Checkpoint 156-215-70

156-215.70 Check Point Certified Security Administrator R70

Practice Test

Version 3.0

QUESTION NO: 1

QUESTION NO: 2

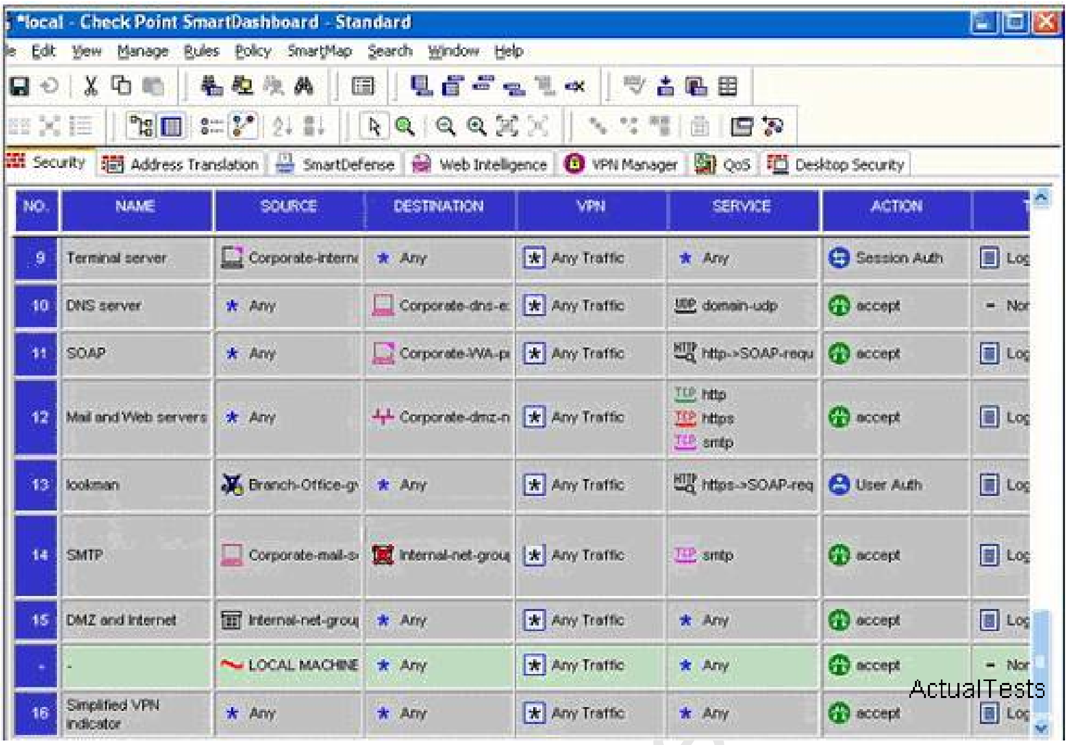
You run a standalone deployment with a machine that runs SecurePlatform NGX R60. You now want to change the configuration to distributed deployment. You get a new machine with high specification in order to implement Security Gateway R70 in a distributed deployment. How would you use these two machines to successfully migrate the NGX R60 configuration?

A. (A) Run R70 CDROM in the old machine to upgrade the existing SecurePlatform R60 to R70 and install the R70 Security Gateway. (B) Run sysconfig to complete configuration. (C) On the new machine, install SecurePlatform as the primary Security Management Server only. (D) Transfer the exported .tgz file into the new machine, import the configuration, and then reboot. (E) Go to the SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
B. (A)On the existing machine, export the NGX R60 configuration to a network share.
(B) Run R70 CDROM in the old machine to upgrade the existing SecurePlatform R60 to R70 and install the R70 Security Gateway. (C) Run cpconfig to complete configuration.
(D) On the new machine, install SecurePlatform as the primary Security Management Server only.
(E) Transfer the exported .tgz file into the new machine, import the configuration, and then reboot.
(F) Go to the SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
C. (A)On the existing machine, export the NGX R60 configuration to a network share.
(B) Run R70 CDROM in the old machine to upgrade the existing SecurePlatform R60 to R70 and install the R70 Security Gateway. (C) Run sysconfig to complete configuration.
(D) On the new machine, install SecurePlatform as the primary Security Management Server only.
(E) Transfer the exported .tgz file into the new machine, import the configuration, and then reboot.
(F) Go to the SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
D. (A) Run R70 CDROM in the old machine to upgrade the existing SecurePlatform R60 to R70 and install the R70 Security Gateway. (B) Run cpconfig to complete configuration. (C) On the new machine, install SecurePlatform as the primary Security Management Server only. (D) Transfer the exported .tgz file into the new machine, import the configuration, and then reboot. E. Go to the SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
E. (A)On the existing machine, export the NGX R60 configuration to a network share. (B) Uninstall the R70 Security Gateway. (C) Run sysconfig to complete configuration.
(D) On the new machine, install SecurePlatform as the primary Security Management Server only.
(E) Transfer the exported .tgz file into the new machine, import the configuration, and then reboot.
(F) Go to the SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.

Answer: C

QUESTION NO: 3

Examine the diagram and answer the question. What do you think is missing from the rule?


*local - Check Point SmartDashboard - Standard
le Edit View Manage Rules Policy SmartMap Search Window Help
Security
Address Translation
SmartDefense
Web Intelligence
VPN Manager
QoS
Desktop Security

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	T
9	Terminal server	Corporate-intern	Any	Any Traffic	Any	Session Auth	Log
10	DNS server	Any	Corporate-dns-e	Any Traffic	domain-udp	accept	- Nor
11	SOAP	Any	Corporate-WA-p	Any Traffic	http->SOAP-requ	accept	Log
12	Mail and Web servers	Any	Corporate-dmz-n	Any Traffic	http https smtp	accept	Log
13	lookman	Branch-Office-g	Any	Any Traffic	https->SOAP-req	User Auth	Log
14	SMTP	Corporate-mail-s	Internal-net-grou	Any Traffic	smtp	accept	Log
15	DMZ and Internet	Internal-net-grou	Any	Any Traffic	Any	accept	Log
-	-	LOCAL MACHINE	Any	Any Traffic	Any	accept	- Nor
16	Simplified VPN indicator	Any	Any	Any Traffic	Any	accept	Log

A. Implicit rule
B. Stealth rule
C. Anti-spoofing rule
D. Pseudo rule
E. Cleanup rule

Answer: E

QUESTION NO: 4

Which of the following would you not test if SIC fails to initialize?

A. Check the date and time at the operating systems and make sure the time is accurate
B. Ensure connectivity between the gateway and Security Management server
C. Verify that Security Management server and SmartDashboard use the different SIC activation key
D. Ensure the Security Management server's IP address andname are in the /etc/hosts file on the gateway
E. On the gateway, type fw unloadlocal to remove the security policy so that all traffic is allowed through

Answer: C

QUESTION NO: 5

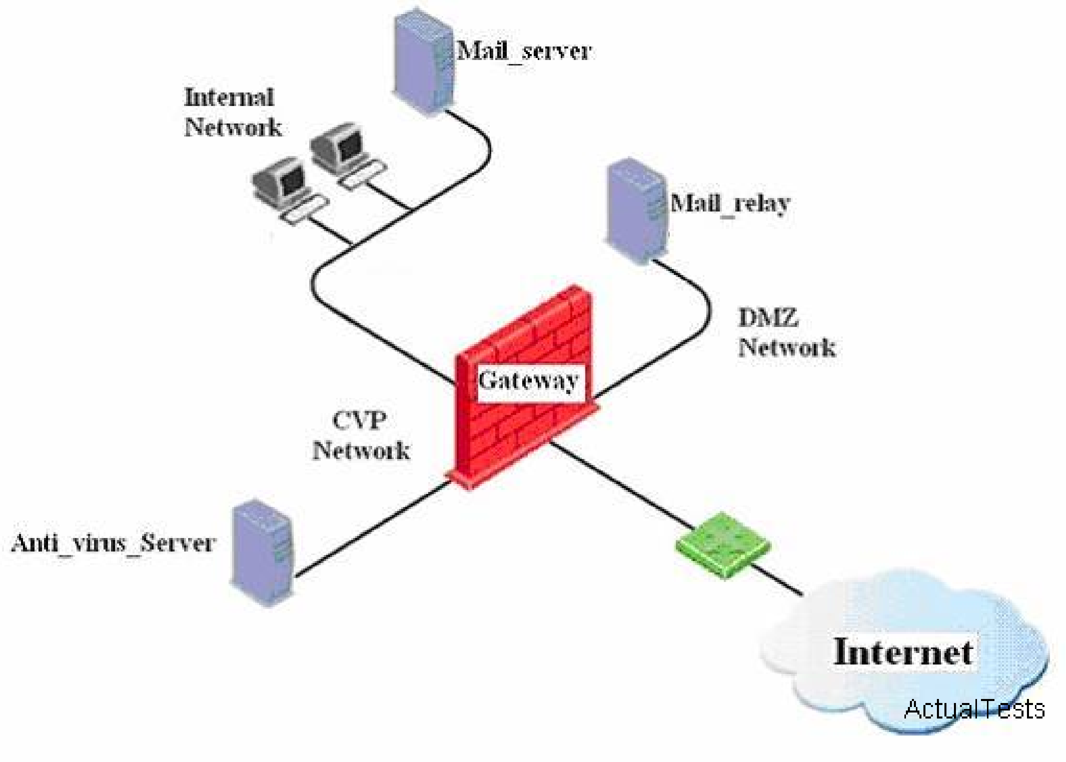
What Dashboard will you go to in Network Voyager in order to get information regarding CPU Utilization and memory Utilization when performing Performance Monitoring?

A. System Dashboard
B. Traffic Dashboard
C. Connection Dashboard
D. Connection Map Dashboard
E. Forwarding Dashboard

Answer: A

QUESTION NO: 6

The diagram shows sample configuration for Anti-Virus Checking for Incoming Email. Which one of the following is not a step to configure Anti-Virus checking for incoming email?



A. Define rules that use the resource
B. Create a gateway object to represent the Security Gateway
C. Create an OPSEC Application object to represent the OPSEC Application server, and associate it with the host object

D. Define an SMTP resource that uses the OPSEC Application object, and associate it with the OPSEC Application object
E. Create a host object for the machine on which the third-party, OPSEC server application is installed

Answer: B

QUESTION NO: 7

You execute series of command in Transaction Mode (Check Point IPSO command-line interface (CLI)), and you see lots of errors. What command will you use to undo the all the changes?

A. set
B. commit
C. undo
D. ignore
E. rollback

Answer: E

QUESTION NO: 8

SmartUpdate installs two repositories on the Security Management server. What folder does Package repository use a storage on Unix platform?

A. C:\Suroot
B. /var/log
C. /var/suroot
D. /var/etc
E. /var/bin

Answer: C

QUESTION NO: 9

Which of the following are limitations of a Bridge Mode?

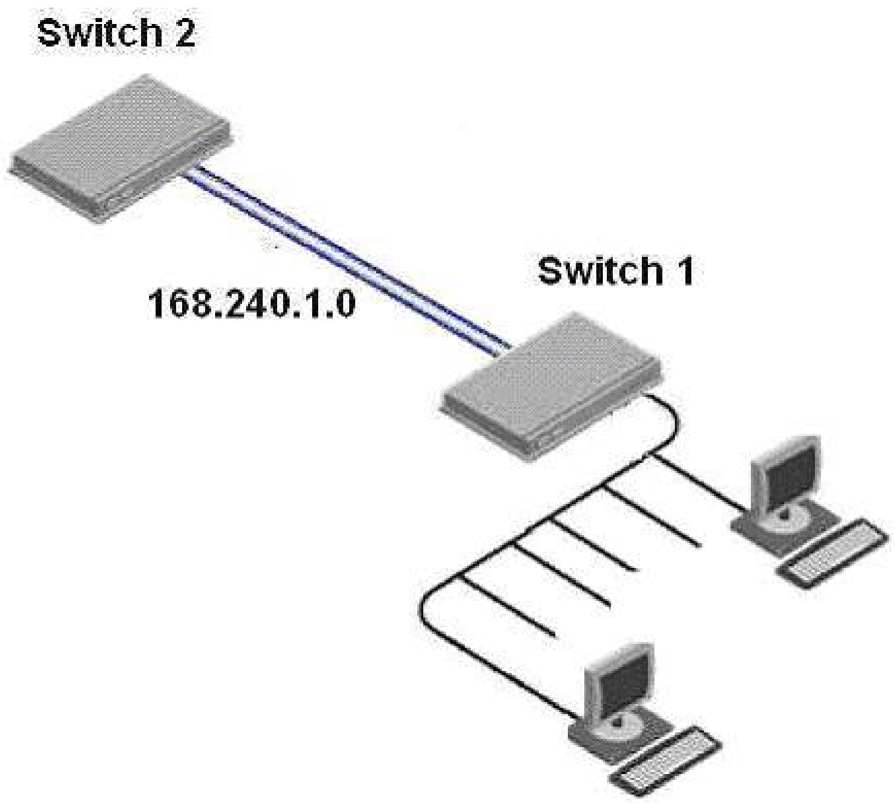


Figure 1: Network without bridge mode deployment

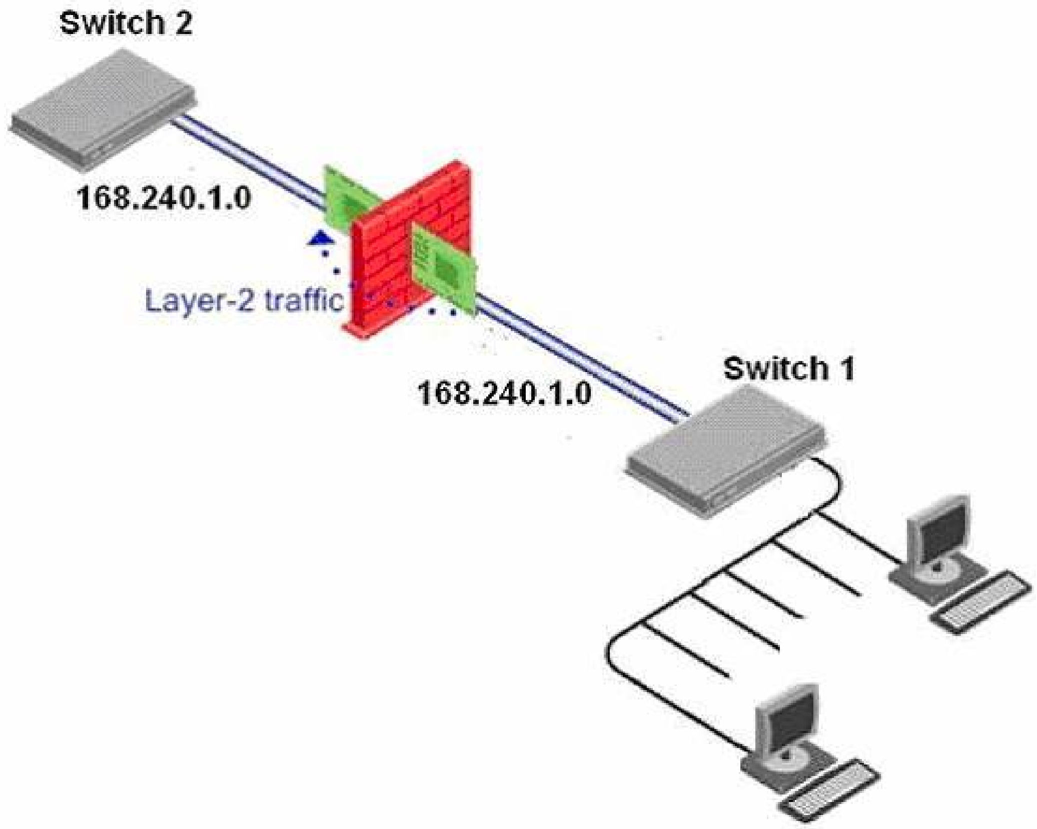


Figure 2: Deploying a Single VPN-1 gateway in bridge mode

A. Cluster configurations are not supported

B. Bridge mode is only supported on the Nokia platforms

C. Clustering has to be in place prior to the deployment of bridge mode

D. Network Address Translation is not supported

E. A bridge must be configured with a pair of interfaces

Answer: A,D,E

QUESTION NO: 10

What does the command ipscti allows you to do?

A. Allows you modify the stored configuration

B. Allows you modify the running configuration

C. Allows you to reboot your Nokia device

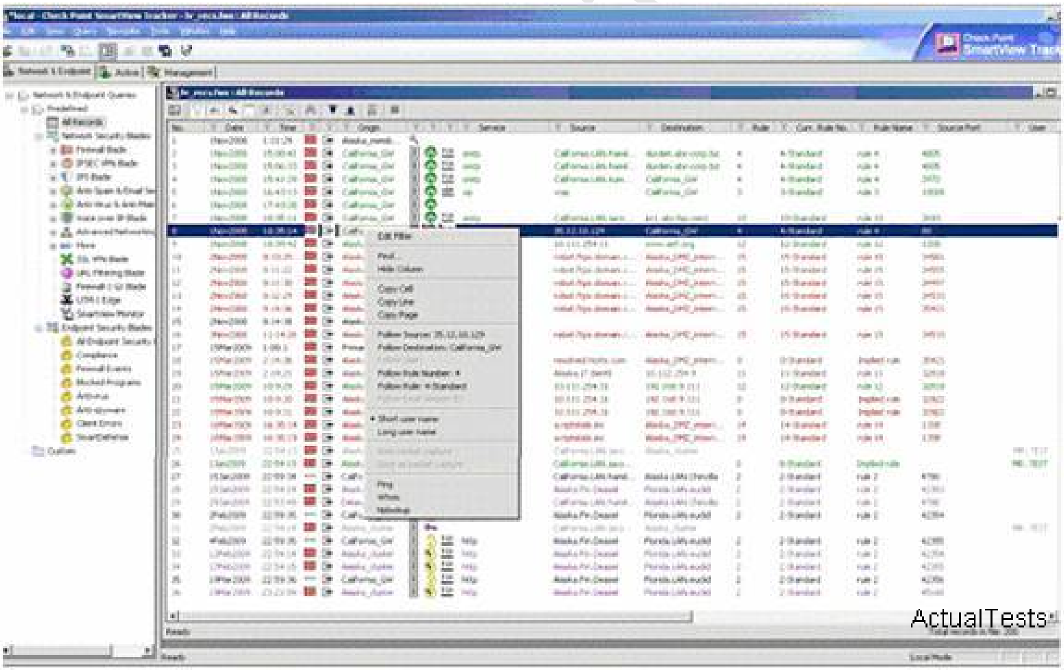
D. Allows you monitor system status

E. Allows you save delete the running configuration

Answer: B

QUESTION NO: 11

To hide a data field in the SmartView Tracker, what would you do?



A. You will choose Select menu, then select Hide Column option from the data field sub menu

B. Left-click the data field (column) that you are hiding and select Hide Columnoption from the emerging menu

C. There is now way you can do this

D. You will choose Select menu and choose Hide option

E. Right-click the data field (column) that you are hiding and select Hide Columnoption from the emerging menu

Answer: E

QUESTION NO: 12

When dealing with IP Appliances, where would you go to check information regarding: File system mounts and unmount; upgrade; reboot, backup etc..?

A. log under logfile

B. log under audit

C. log under system

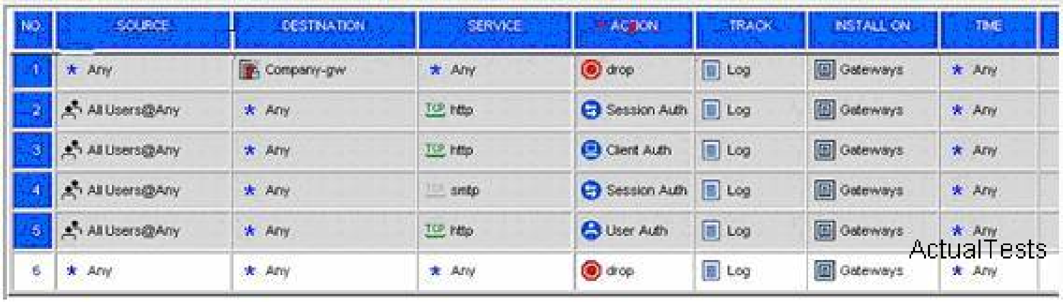
D. log under logSystem

E. log under syslog

Answer: E

QUESTION NO: 13

Study the diagram and answer the question below. Which rule will prevent a user from performing Client Authentication?



NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Any	Company-gw	Any	drop	Log	Gateways	Any
2	All Users@Any	Any	TCP http	Session Auth	Log	Gateways	Any
3	All Users@Any	Any	TCP http	Client Auth	Log	Gateways	Any
4	All Users@Any	Any	TCP smtp	Session Auth	Log	Gateways	Any
5	All Users@Any	Any	TCP http	User Auth	Log	Gateways	Any
6	Any	Any	Any	drop	Log	Gateways	Any

A. Rule 3

B. Rule 2

C. Rule 6

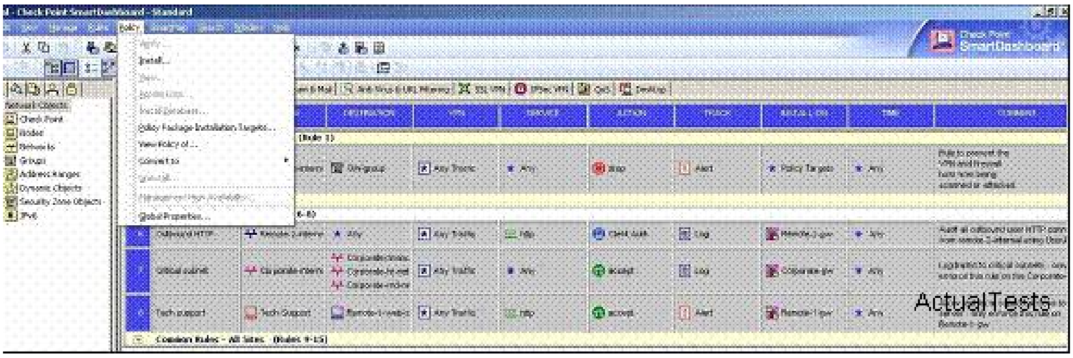
D. Rule 1

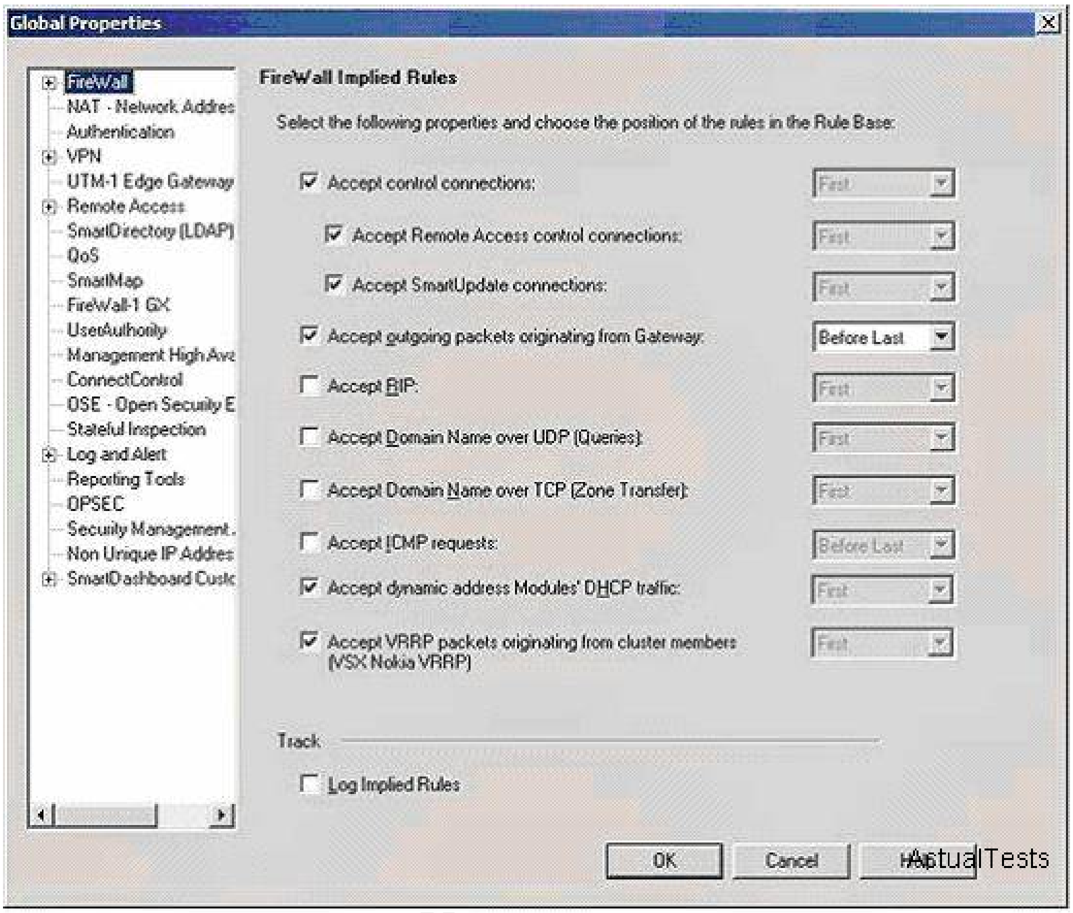
E. Rule 5

Answer: D

QUESTION NO: 14

What menu would you select in SmartDashboard to access Global Properties screen? Note: If wrong answer(s) is/are chosen, see the diagram for correct answer.





FireWall Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept control connections: First

☑ Accept Remote Access control connections: First

☑ Accept SmartUpdate connections: First

☑ Accept outgoing packets originating from Gateway: Before Last

☐ Accept RIP: First

☐ Accept Domain Name over UDP (Queries): First

☐ Accept Domain Name over TCP (Zone Transfer): First

☐ Accept ICMP requests: Before Last

☑ Accept dynamic address Modules' DHCP traffic: First

☑ Accept VRRP packets originating from cluster members (VSX Nokia VRRP): First

Track

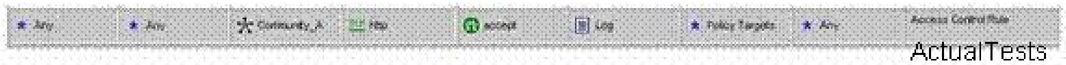
☐ Log Implied Rules

A. Rules
B. Policy
C. Topology
D. File
E. Manage

Answer: B

QUESTION NO: 15

Which of the following are true of Access Control within VPN Communities?



Any	Any	Community_A	Http	accept	Log	Policy Targets	Any	Access Control Rule

Figure 1: Access Control Rule

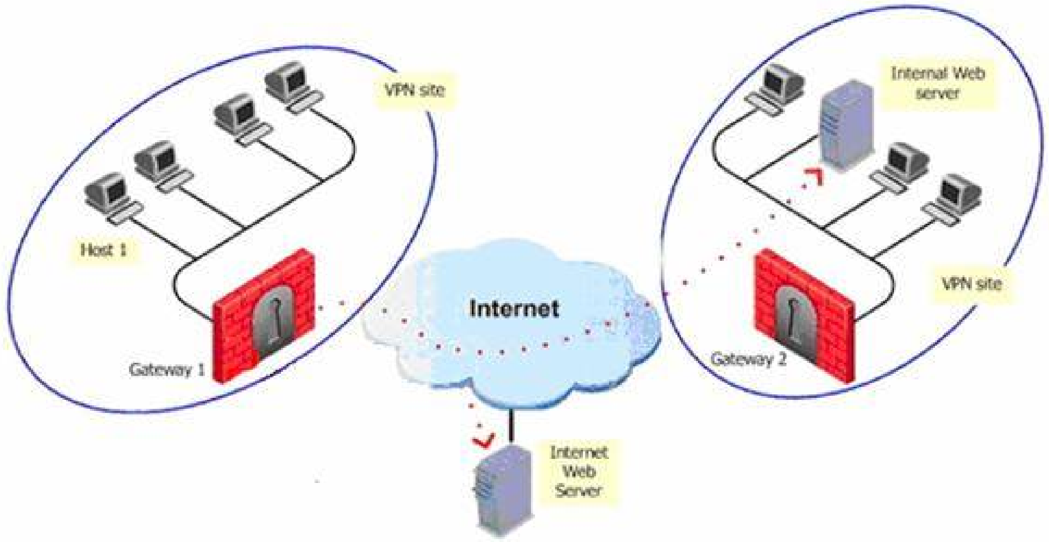
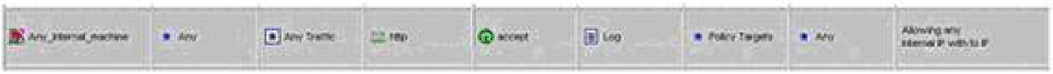


Figure 2: Access control in VPN communities



Any_internal_machine	Any	Any Traffic	Http	accept	Log	Policy Targets	Any	Allowing any internal IP with/to IP

Figure 3: Allowing any internal IP to any IP

A. The fact that two gateways belong to the same VPN community does automatically mean the gateways have access to each other

B. Using the Global Properties, it is possible to create access control rules that apply only to members of a VPN community

C. The configuration of the gateways into a VPN community means that if these gateways are allowed to communicate via an access control policy, then that communication is encrypted

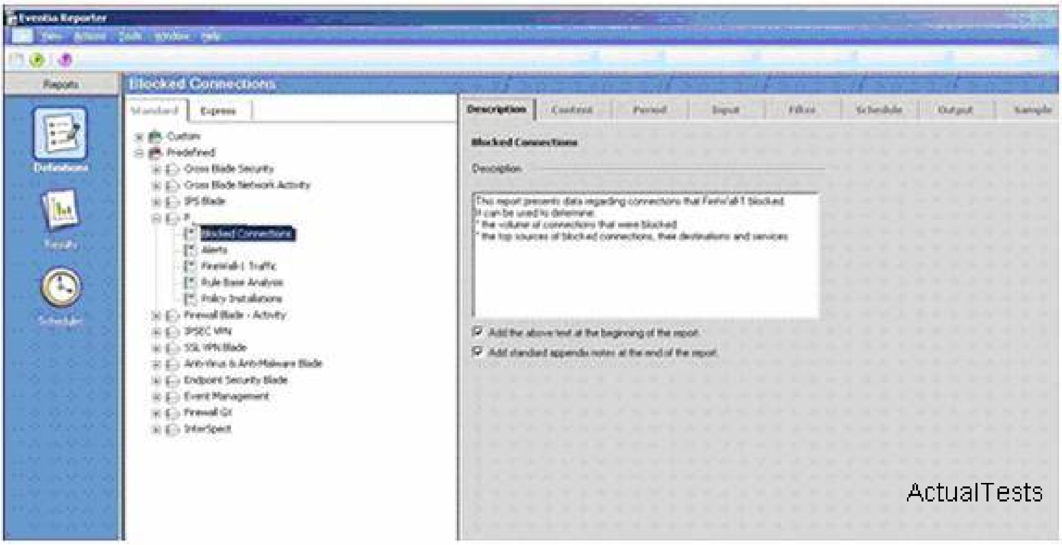
D. Using the VPN column of the Security Policy Rule Base, it is possible to create access control rules that apply only to members of a VPN community

E. The fact that two gateways belong to the same VPN community does not mean the gateways have access to each other

Answer: C,D,E

QUESTION NO: 16

If you are in Eventia Reporter and need to see all blocked connections, what reports would you switch to under the Standard tab?



This report presents data regarding connections that FireWall-1 blocked
It can be used to determine:
* the volume of connections that were blocked
* the top sources of blocked connections, their destinations and services

☑ Add the above text at the beginning of the report
☑ Add standard appendix notes at the end of the report

A. Firewall GX

B. Firewall Blade - Monitor

C. INTERSPECT

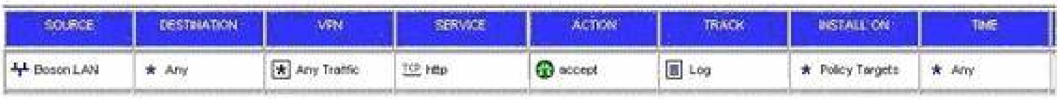
D. IPSEC VPN

E. Firewall Blade - Security

Answer: E

QUESTION NO: 17

Which of the following is true regarding the Rule Base?



SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
Boson LAN	Any	Any Traffic	TCP http	accept	Log	Policy Targets	Any

Figure 1: Access Control Rule

A. A security policy is implemented by means of ordered set of rules in the security Rule Base

B. Rule parameters include the source and destination of the communication, the services and protocols

C. A well defined security policy is essential to an effective security solution

D. The Rule Base is a collection of rules that determine which communication traffic is permitted

E. The fundamental principle of the Rule Base is that all actions that are not explicitly permitted are not necessarily prohibited

Answer: A,B,C,D

QUESTION NO: 18

When modifying a user template, the users already created based on this template will be:

A. Unaffected
B. Deleted
C. Affected
D. Re-created
E. Created

Answer: A

QUESTION NO: 19

Which of the following are true of User Authentication type?

A. User Authentication grants access on a per host basis
B. User Authentication is a secure form of authentication as the authentication is valid only for one connection.
C. User Authentication grants access on a per user basis
D. User Authentication can be used with any service
E. User Authentication can be used for TELNET,FTP,

Answer: B,C,E

QUESTION NO: 20

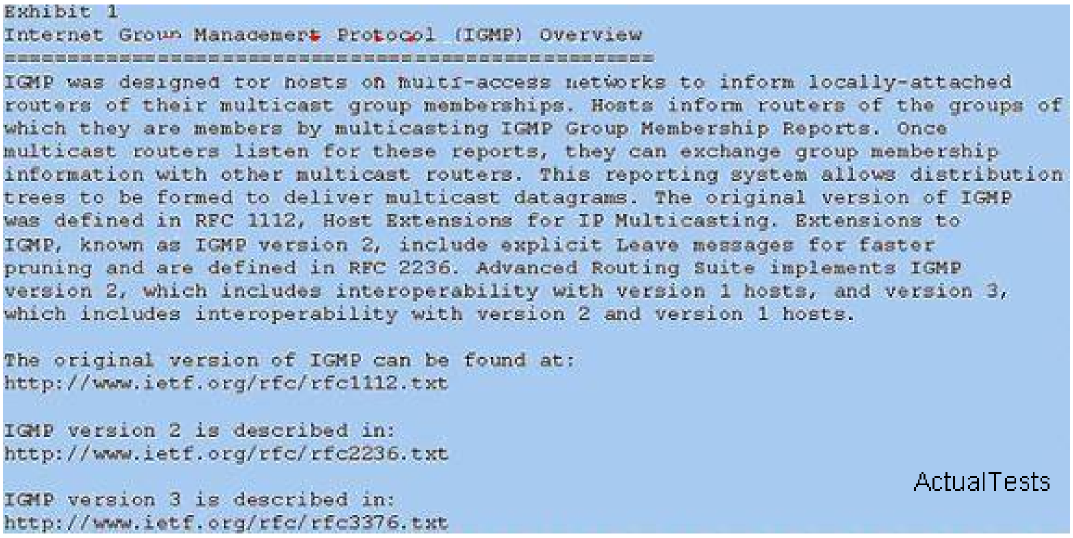
In LDAP, four profiles are defined corresponding to a specific SmartDirectory (LDAP) server,

A. Netscape_DS
B. Linux_AD
C. Novell_DS
D. OPSEC_DS
E. Microsoft_ADand these are:

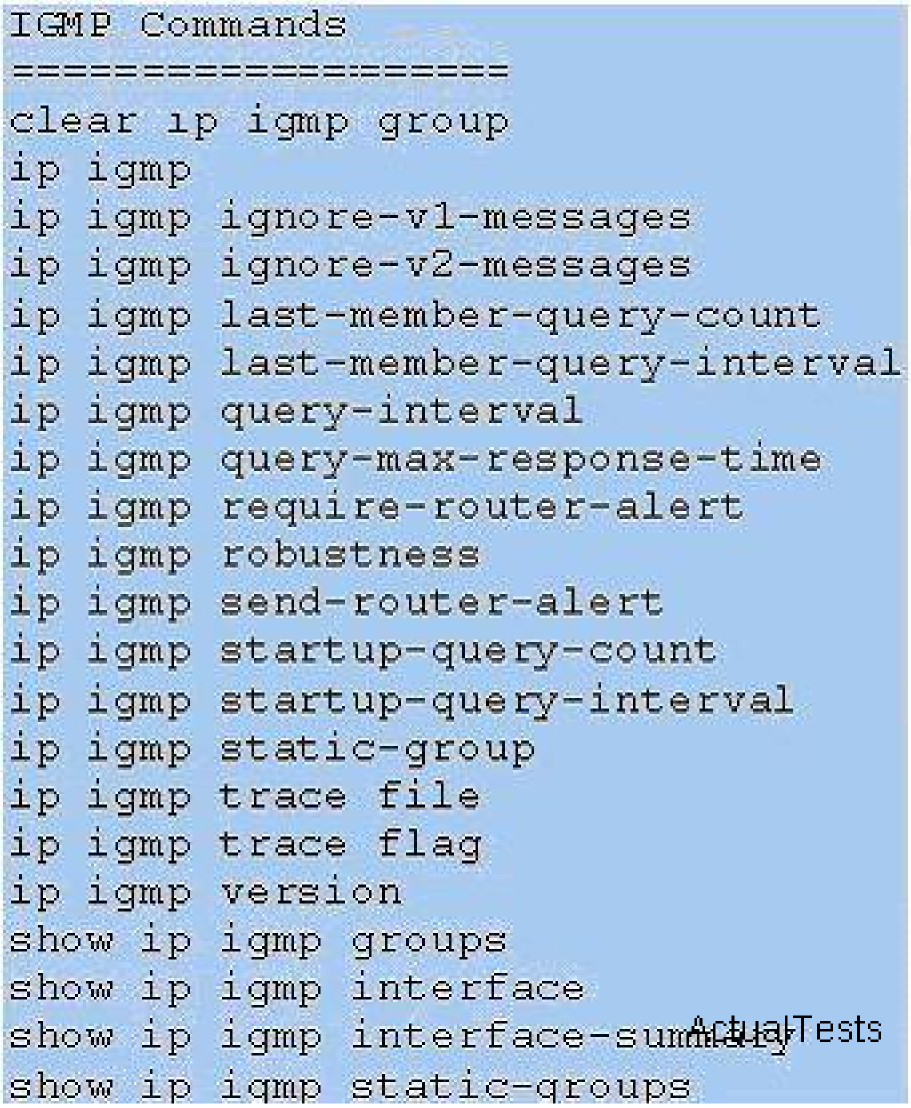
Answer: A,C,D,E

QUESTION NO: 21

Which of the following command will display IGMP information regarding multicast group membership?



```
Exhibit 1
Internet Group Management Protocol (IGMP) Overview
===================================================
IGMP was designed for hosts on multi-access networks to inform locally-attached
routers of their multicast group memberships. Hosts inform routers of the groups of
which they are members by multicasting IGMP Group Membership Reports. Once
multicast routers listen for these reports, they can exchange group membership
information with other multicast routers. This reporting system allows distribution
trees to be formed to deliver multicast datagrams. The original version of IGMP
was defined in RFC 1112, Host Extensions for IP Multicasting. Extensions to
IGMP, known as IGMP version 2, include explicit Leave messages for faster
pruning and are defined in RFC 2236. Advanced Routing Suite implements IGMP
version 2, which includes interoperability with version 1 hosts, and version 3,
which includes interoperability with version 2 and version 1 hosts.

The original version of IGMP can be found at:
http://www.ietf.org/rfc/rfc1112.txt

IGMP version 2 is described in:
http://www.ietf.org/rfc/rfc2236.txt

IGMP version 3 is described in:
http://www.ietf.org/rfc/rfc3376.txt
```



```
IGMP Commands
===================
clear ip igmp group
ip igmp
ip igmp ignore-v1-messages
ip igmp ignore-v2-messages
ip igmp last-member-query-count
ip igmp last-member-query-interval
ip igmp query-interval
ip igmp query-max-response-time
ip igmp require-router-alert
ip igmp robustness
ip igmp send-router-alert
ip igmp startup-query-count
ip igmp startup-query-interval
ip igmp static-group
ip igmp trace file
ip igmp trace flag
ip igmp version
show ip igmp groups
show ip igmp interface
show ip igmp interface-summary
show ip igmp static-groups
```

A. ip igmp robustness

B. show ip igmp groups

C. ip igmp query-max-response-time

D. ip igmp ignore-v1-messages

E. clear ip igmp group

Answer: B

QUESTION NO: 22

IPSO supports a maximum of 1015 VLAN interfaces, and what is the default maximum?

A. 2015
B. 950
C. 1015
D. 1000
E. 2000

Answer: B

QUESTION NO: 23

The advantages of saving consolidated records to a table over multiple database tables include: (Select all the correct answers)

A. You are saved the trouble of moving records between tables
B. You can select the appropriate source table for each report you wish to generate
C. A report is generated based on a single table
D. Reduction in the report generation time
E. All the data is readily accessible

Answer: A,B,C,E

QUESTION NO: 24

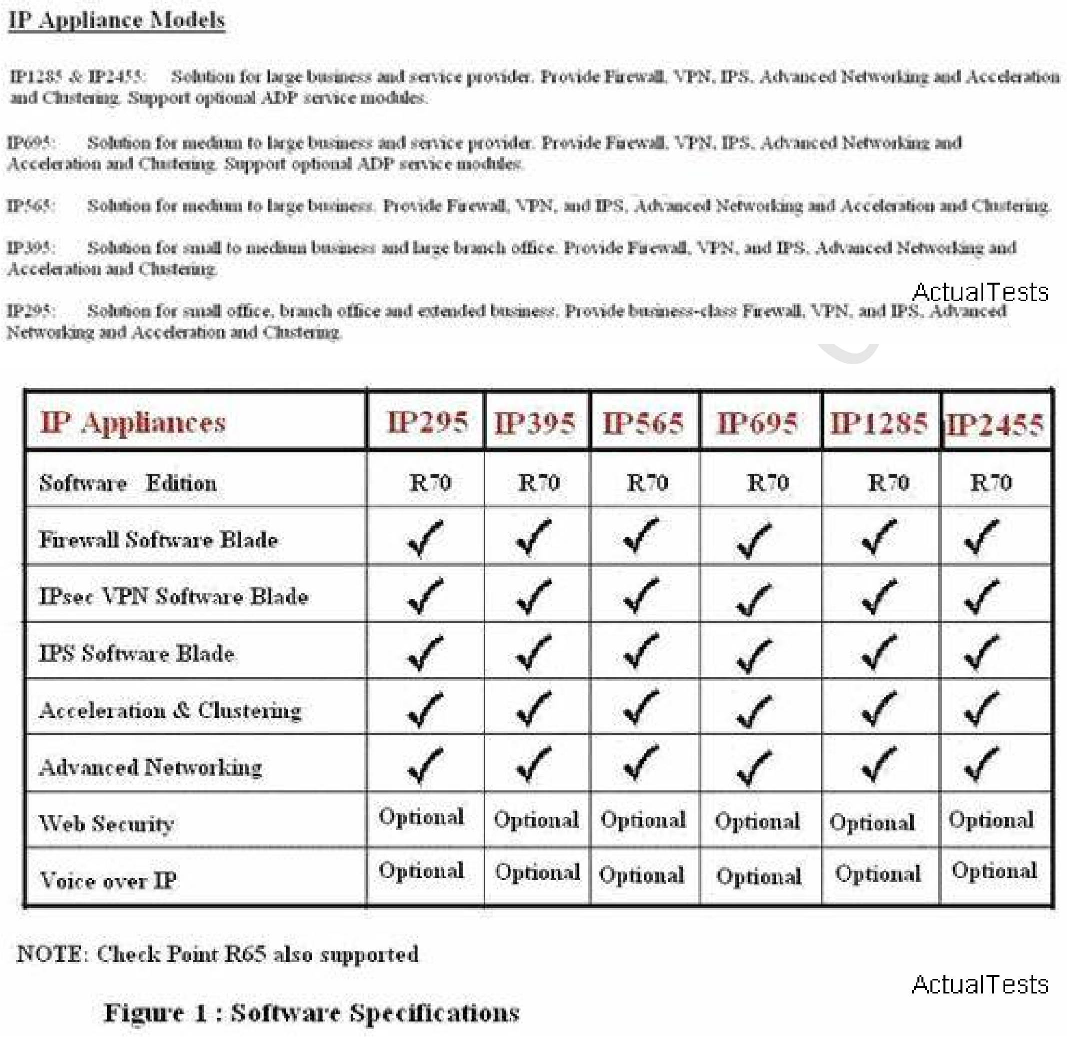
Check Point recommends that you install the latest Hotfix Accumulators (latest HFA) in order to stay current with the latest software and security updates. Based on this, you want to deploy a latest HFA to fifteen Security Gateways at ten geographically separated locations. What is the best way to go about this?

A. Use the SmartDashboard to install the packages to each of the Security Gateways remotely
B. Email the installation files to all the locations, and get the Administrator at each location to carry out the installation
C. Zip the installation files and send the zipped files to all the locations, and get the Administrator at each location to carry out the installation
D. Use the SmartUpdate to install the packages to each of the Security Gateways remotely
E. Send the CDROM to each location, and get the Administrator at each location to carry out the installation

Answer: D

QUESTION NO: 25

John, an IT director for ACME IT Support Ltd., needs an advice regarding which IP Appliance to purchase for his company. He gives the following information: His company can be described as a small size. And George needs to run VPN, FireWall, IPS and clustering. George wants you, a Checkpoint engineer to recommend an Appliance. Which of the following would you recommend? Select all the correct answers.



IP Appliance Models

IP1285 & IP2455: Solution for large business and service provider. Provide Firewall, VPN, IPS, Advanced Networking and Acceleration and Clustering. Support optional ADP service modules.

IP695: Solution for medium to large business and service provider. Provide Firewall, VPN, IPS, Advanced Networking and Acceleration and Clustering. Support optional ADP service modules.

IP565: Solution for medium to large business. Provide Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP395: Solution for small to medium business and large branch office. Provide Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP295: Solution for small office, branch office and extended business. Provide business-class Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP Appliances	IP295	IP395	IP565	IP695	IP1285	IP2455
Software Edition	R70	R70	R70	R70	R70	R70
Firewall Software Blade	✓	✓	✓	✓	✓	✓
IPsec VPN Software Blade	✓	✓	✓	✓	✓	✓
IPS Software Blade	✓	✓	✓	✓	✓	✓
Acceleration & Clustering	✓	✓	✓	✓	✓	✓
Advanced Networking	✓	✓	✓	✓	✓	✓
Web Security	Optional	Optional	Optional	Optional	Optional	Optional
Voice over IP	Optional	Optional	Optional	Optional	Optional	Optional

NOTE: Check Point R65 also supported

Figure 1 : Software Specifications

A. IP295
B. IP695
C. IP565
D. IP395
E. IP1285

Answer: A,D

QUESTION NO: 26

Which of the following is not a hardware requirement for installing SecurePlatform on Intel platform?

A. BootableCD-ROM Drive
B. 512 MB memory
C. One or more supported network adapter cards
D. 1 GB free disk space
E. Intel Pentium III 300+ MHz or equivalent processor

Answer: D

QUESTION NO: 27

there are two modes for IKE phase I: Main Mode and

A. Aggressive Mode
B. Harsh Mode
C. Secret Mode
D. Minor Mode
E. Major Mode

Answer: A

QUESTION NO: 28

You have not performed software upgrade to NGX R70. You have upgraded your license and every time you try to run commands such as cplic print; cpstop, you receive all sort of errors. In order to resolve this you will have to:

A. Remove the software
B. Do nothing. The error will go away with time
C. Remove the upgraded license
D. Upgrade the software to version NGX
E. Re-upgrade the license to the version before the upgrade

Answer: D

QUESTION NO: 29

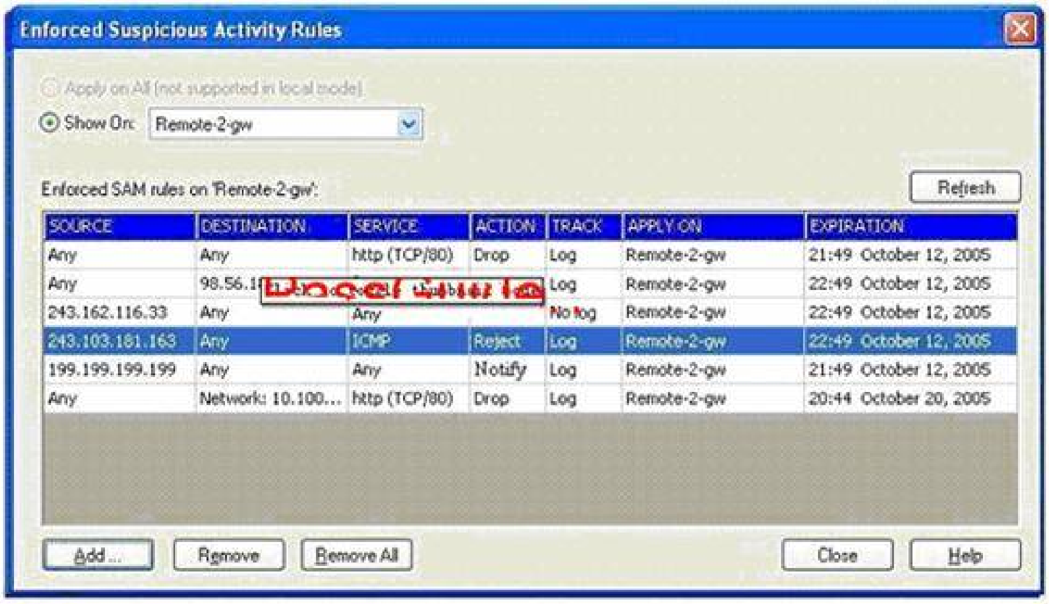
When carrying out Anti-Virus Signature Database Updates, you can either use Automatic or Manual type. What is the default update interval?

A. 120 minutes
B. 120 seconds
C. 120 hours
D. 60 hours
E. 60 minutes

Answer: A

QUESTION NO: 30

Which of the following is true of the highlighted rule in diagram 1? The ICMP type in the rule are types: 0 and 8.



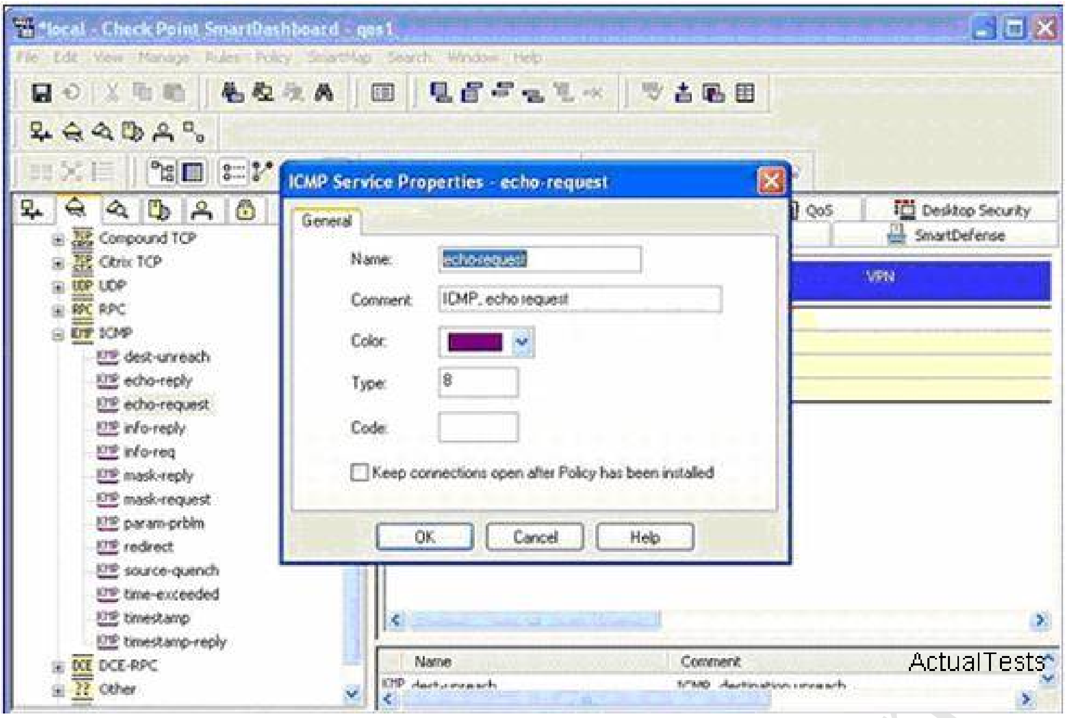
Enforced Suspicious Activity Rules
○ Apply on All (not supported in local mode)
● Show On: Remote-2-gw
Refresh
Add ...
Remove
Remove All
Close
Help

Enforced SAM rules on 'Remote-2-gw':

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	APPLY ON	EXPIRATION
Any	Any	http (TCP/80)	Drop	Log	Remote-2-gw	21:49 October 12, 2005
Any	98.56.1[illegible]	[illegible]	[illegible]	Log	Remote-2-gw	22:49 October 12, 2005
243.162.116.33	Any	Any		No log	Remote-2-gw	22:49 October 12, 2005
243.103.181.163	Any	ICMP	Reject	Log	Remote-2-gw	22:49 October 12, 2005
199.199.199.199	Any	Any	Notify	Log	Remote-2-gw	21:49 October 12, 2005
Any	Network: 10.100...	http (TCP/80)	Drop	Log	Remote-2-gw	20:44 October 20, 2005

Figure 1 Enforced Suspicious Activity Rules window

ActualTests



ICMP Service Properties - echo-request

Name: echo-request

Comment: ICMP, echo request

Color:

Type: 8

Code:

□ Keep connections open after Policy has been installed

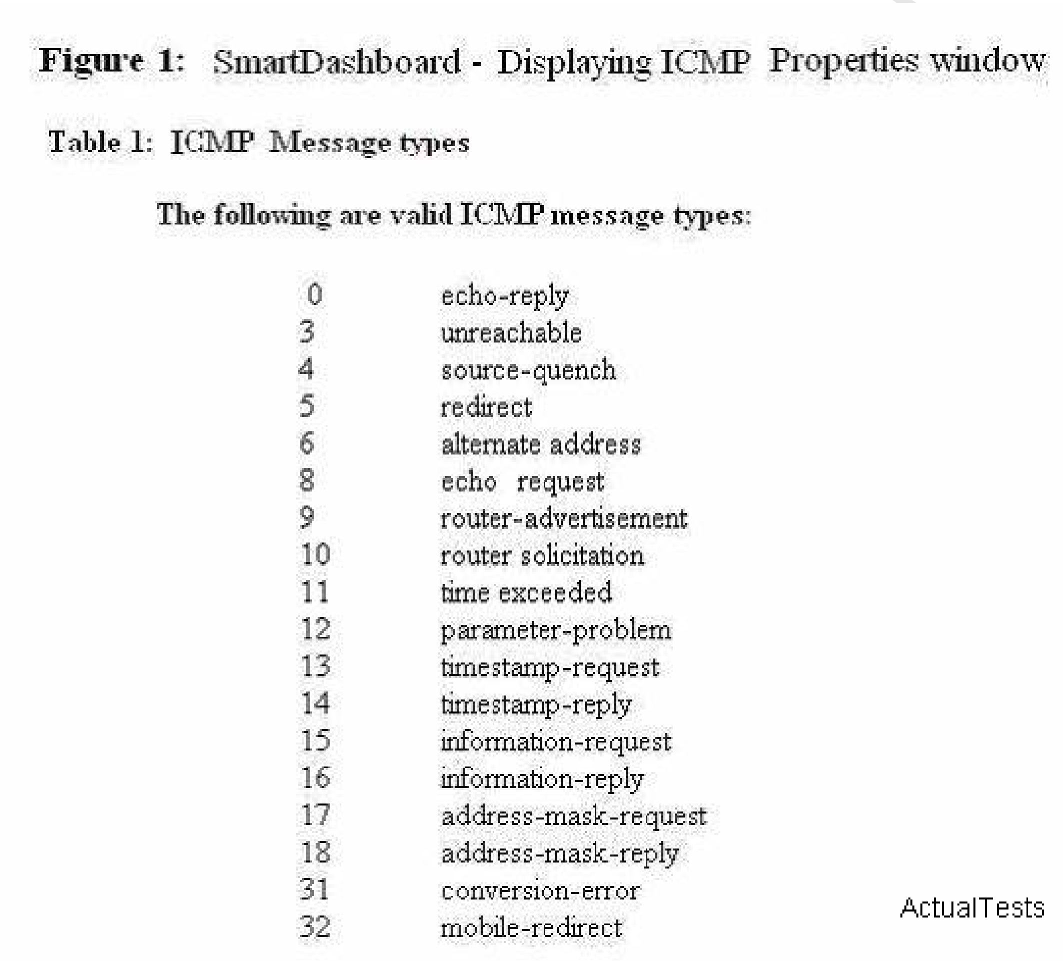


Figure 1: SmartDashboard - Displaying ICMP Properties window

Table 1: ICMP Message types

The following are valid ICMP message types:

0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate address
8	echo request
9	router-advertisement
10	router solicitation
11	time exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	address-mask-request
18	address-mask-reply
31	conversion-error
32	mobile-redirect

A. The host with the IP address 243.103.181.163 will be able to test the connectivity and reachability of any host

B. The host with the IP address 243.103.181.163 will not be able to test the connectivity and reachability of any host

C. In fact the host 243.103.181.163 will not be able to ping any host

D. Any host but host with the IP 199.199.199.199 should be able to ping 243.103.181.163 host
E. The host with the IP address 199.199.199.199 will be able to test the connectivity and reachability of any host

Answer: B,C,D

QUESTION NO: 31

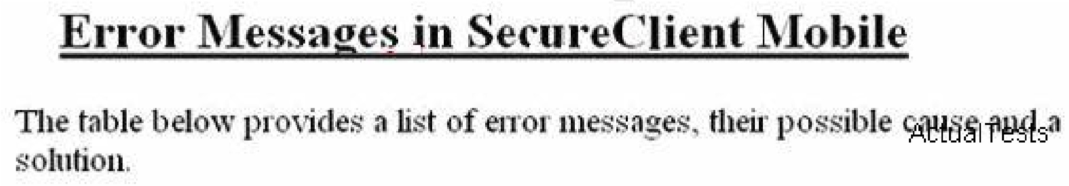
What will happen at the console if I entered the command delete interface log_if_name?

A. The system deletes all the configuration information for a physical interface
B. The system displays all the configuration information for a physical interface
C. The console displays help to delete all the configuration information for a physical interface
D. The system shows all the configuration information for a physical interface
E. The system sets all the configuration information for a physical interface

Answer: C

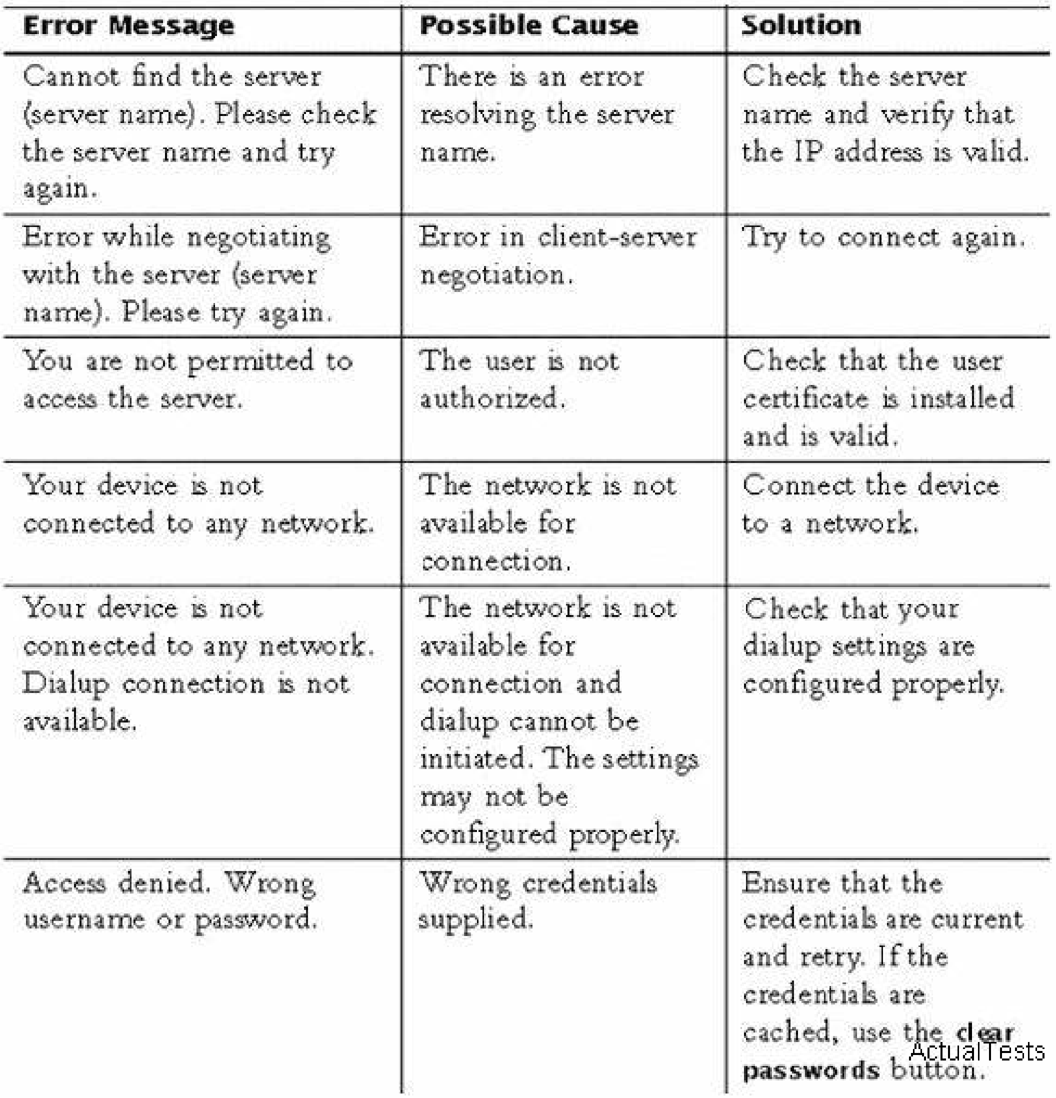
QUESTION NO: 32

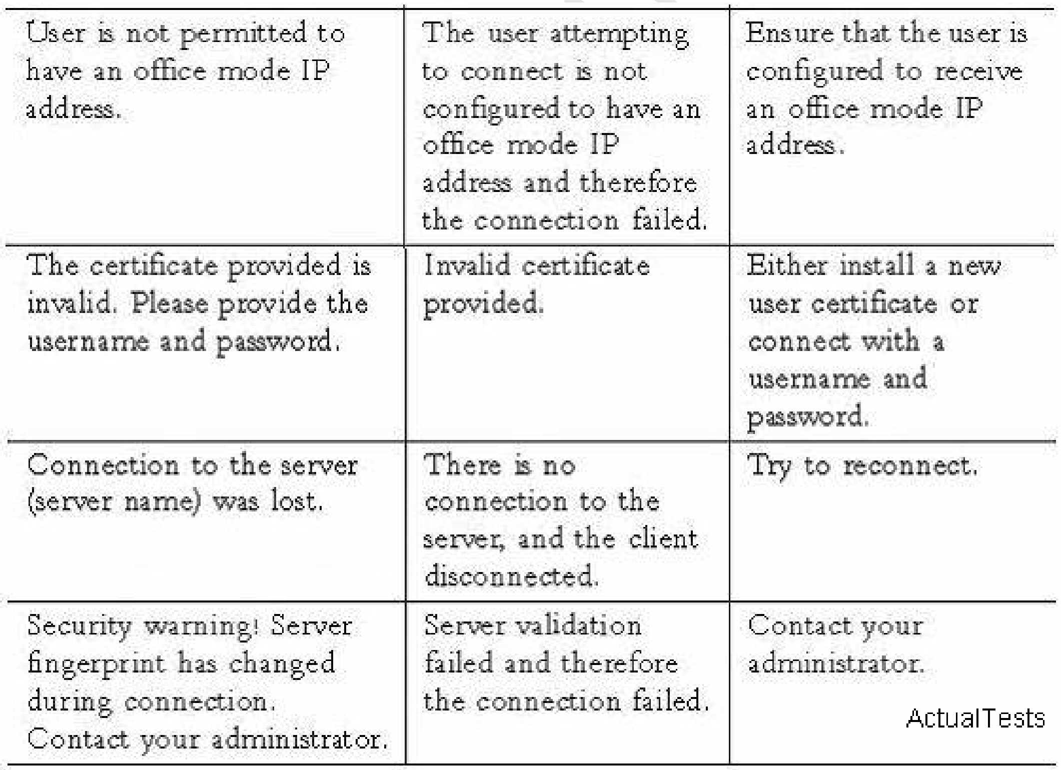
When you tried to connect your SecureClient Mobile, you received the error message "The certificate provided is invalid. Please provide the username and password"?. What is likely to be the reason?



Error Messages in SecureClient Mobile

The table below provides a list of error messages, their possible cause and a solution.





Error Message	Possible Cause	Solution
Cannot find the server (server name). Please check the server name and try again.	There is an error resolving the server name.	Check the server name and verify that the IP address is valid.
Error while negotiating with the server (server name). Please try again.	Error in client-server negotiation.	Try to connect again.
You are not permitted to access the server.	The user is not authorized.	Check that the user certificate is installed and is valid.
Your device is not connected to any network.	The network is not available for connection.	Connect the device to a network.
Your device is not connected to any network. Dialup connection is not available.	The network is not available for connection and dialup cannot be initiated. The settings may not be configured properly.	Check that your dialup settings are configured properly.
Access denied. Wrong username or password.	Wrong credentials supplied.	Ensure that the credentials are current and retry. If the credentials are cached, use the **clear passwords** button.
User is not permitted to have an office mode IP address.	The user attempting to connect is not configured to have an office mode IP address and therefore the connection failed.	Ensure that the user is configured to receive an office mode IP address.
The certificate provided is invalid. Please provide the username and password.	Invalid certificate provided.	Either install a new user certificate or connect with a username and password.
Connection to the server (server name) was lost.	There is no connection to the server, and the client disconnected.	Try to reconnect.
Security warning! Server fingerprint has changed during connection. Contact your administrator.	Server validation failed and therefore the connection failed.	Contact your administrator.

A. There is no connection to the server

B. Invalid certificate is provided

C. The network is not available for connection

D. Server validation failed

E. Wrong credentials supplied

Answer: B

QUESTION NO: 33

Which VPN topology will you configure if want your organization needs to exchange information with networks belonging to external partners?

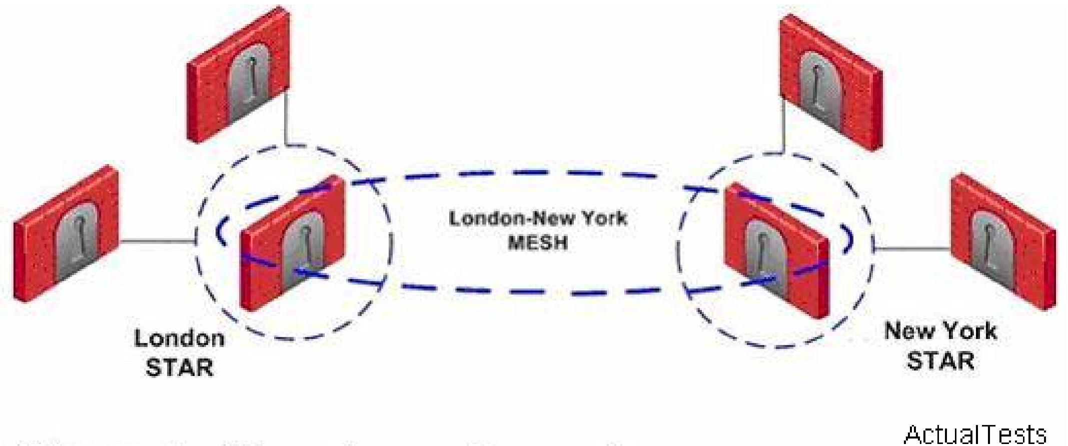


Figure A : Two stars and a mesh

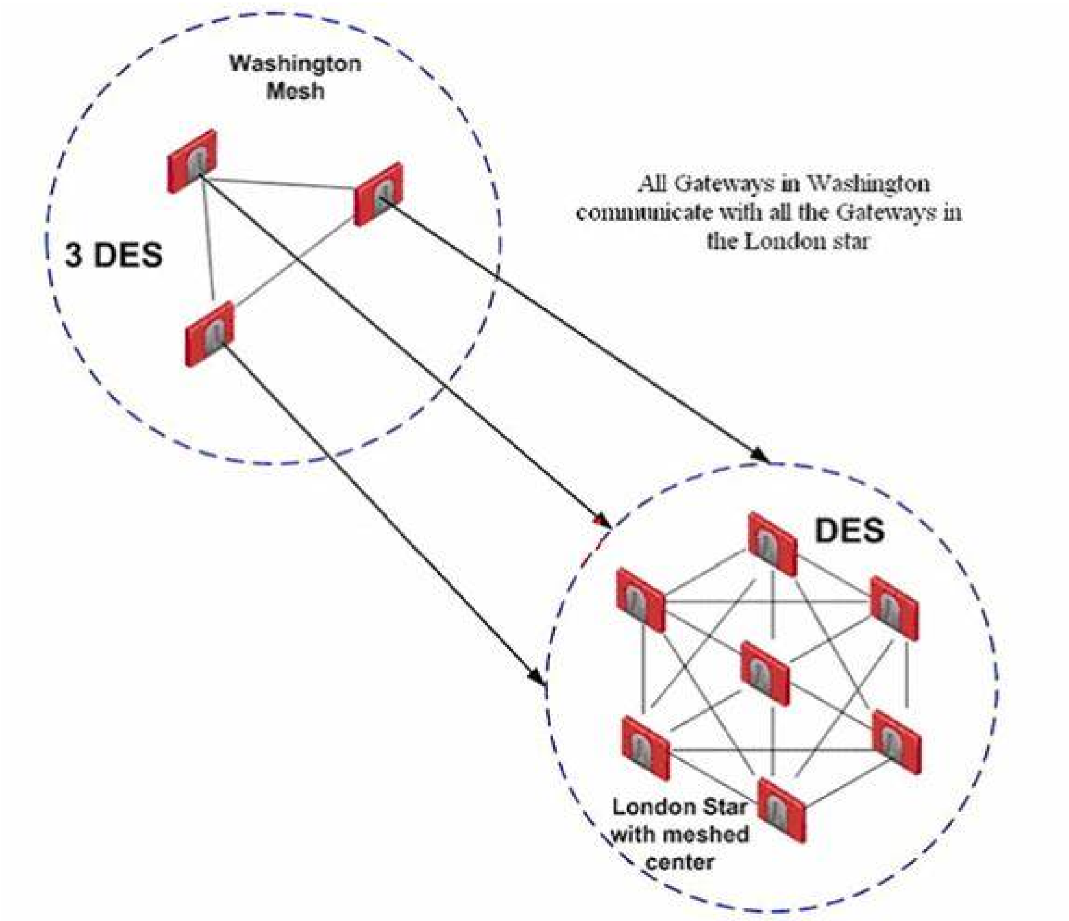

Washington Mesh
3 DES
All Gateways in Washington communicate with all the Gateways in the London star
DES
London Star with meshed center

Figure B: Different means of encryption in separate Mesh communities

A. Star
B. Ring
C. Mesh
D. Cross
E. Meshed

Answer: A

QUESTION NO: 34

For small networks, a single CA may be all that is sufficient and larger enterprise networks may need:

A. CRL
B. Certificate Authority
C. Multiple CA
D. Simple CA
E. Revocation List

Answer: C

QUESTION NO: 35

Your disaster recover strategy needs to be tested in order to ensure that it works as it should. You decide to run a test to achieve two objectives. The first objective - required objective - is to ensure that the Security Policy repository be backed up at least every 24 hours. The second objective - desired objective - to ensure that the R70 components that enforce the Security Policies be backed up at least once a week, and R70 logs should also be backed up at least once a week. You run cron utility to run upgrade_export command each night on the Security Management Servers. You then configure the organization's routine backup software to back the files created by the upgrade_export command. You configure the SecurePlatform backup utility to back the Security Gateways every Friday night. Which of the following is true?

A. Your actions will not meet the required objective but will meet one of the desired objectives
B. Your actions will meet the required objective and none of the desired objectives
C. Your actions will meet the required objective and the two desired objectives
D. Your actions will not meet the required objective but will meet the two desired objectives
E. Your actions will meet the required objective and one desired objective

Answer: E

QUESTION NO: 36

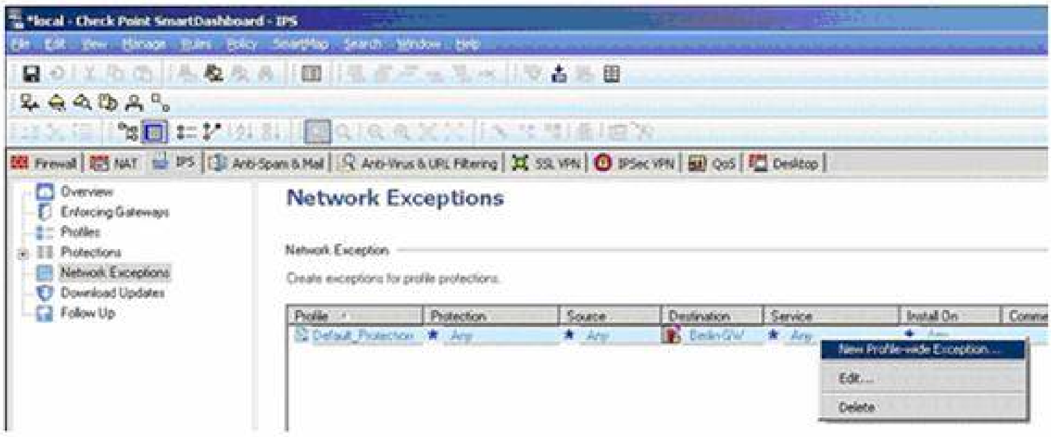
What are the limitations of firewall?

A. A firewall will always protect connections that do not access the firewall
B. A firewall can protect the network against authorized users
C. A firewall can protect connections that do not access the firewall
D. A firewall cannot protect connections that do not access the firewall
E. A firewall cannot protect the network against authorized users

Answer: D,E

QUESTION NO: 37

When using a server that does not comply with RFC standards, then you will have to configure:


*local - Check Point SmartDashboard - IPS
File Edit View Manage Rules Policy SmartMap Search Window Help
Firewall
NAT
IPS
Anti-Spam & Mail
Anti-Virus & URL Filtering
SSL VPN
IPSec VPN
QoS
Desktop
Overview
Enforcing Gateways
Profiles
Protections
Network Exceptions
Download Updates
Follow Up
New Profile-wide Exception...
Edit...
Delete

Network Exceptions

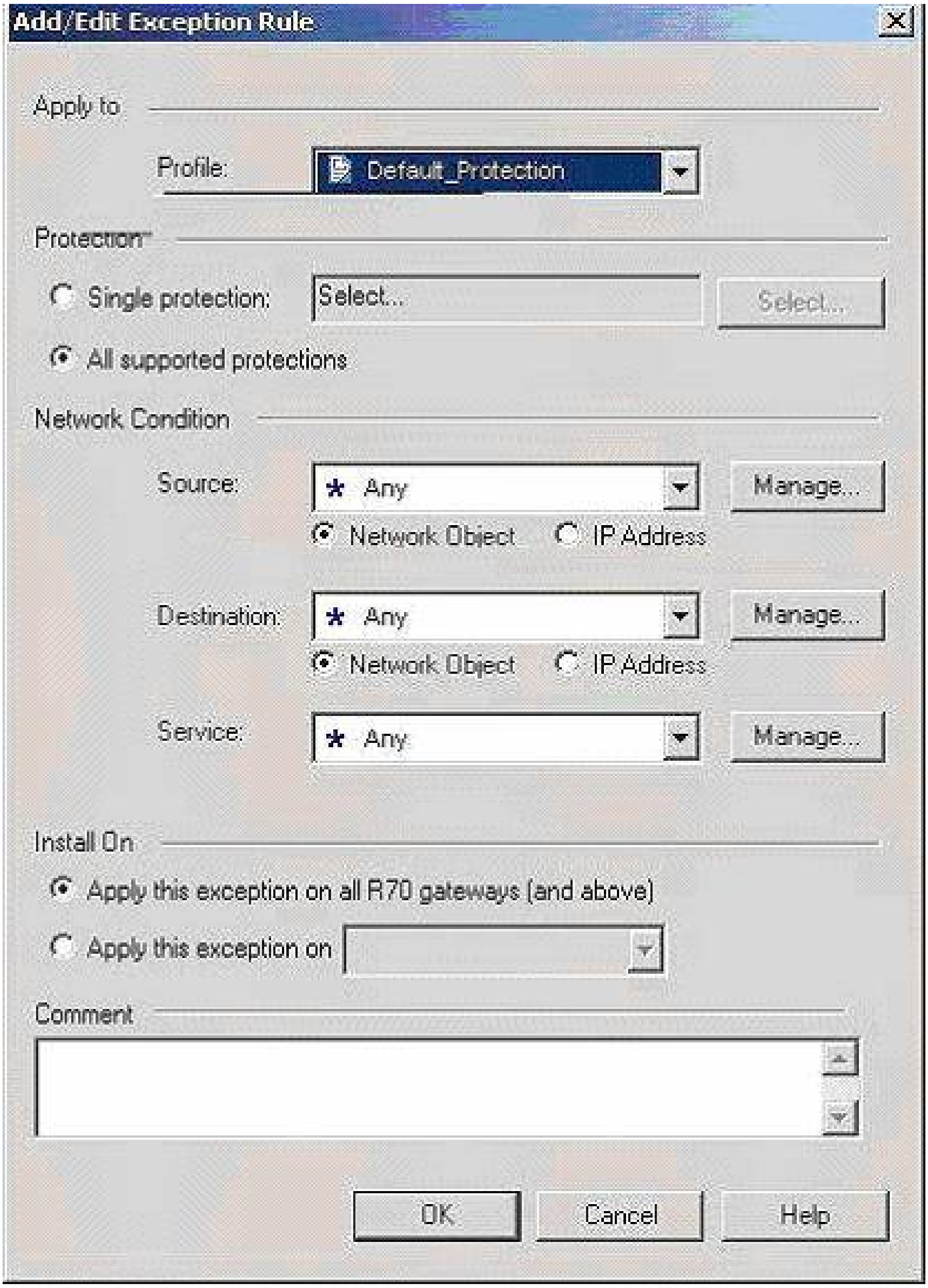
Network Exception

Create exceptions for profile protections.

Profile	Protection	Source	Destination	Service	Install On	Comme
Default_Protection	★ Any	★ Any	BerlinGW	★ Any	★ Any	

Figure 1: IPS Tab - Network Exceptions Page

ActualTests



Add/Edit Exception Rule

Apply to

Profile: Default_Protection

Protection

○ Single protection: Select...

● All supported protections

Network Condition

Source: * Any

● Network Object ○ IP Address

Destination: * Any

● Network Object ○ IP Address

Service: * Any

Install On

● Apply this exception on all R70 gateways (and above)

○ Apply this exception on

Comment

Figure 2: Add/Edit Exception Rule Window

A. Protections

B. Enforcing Gateways

C. Network Exceptions

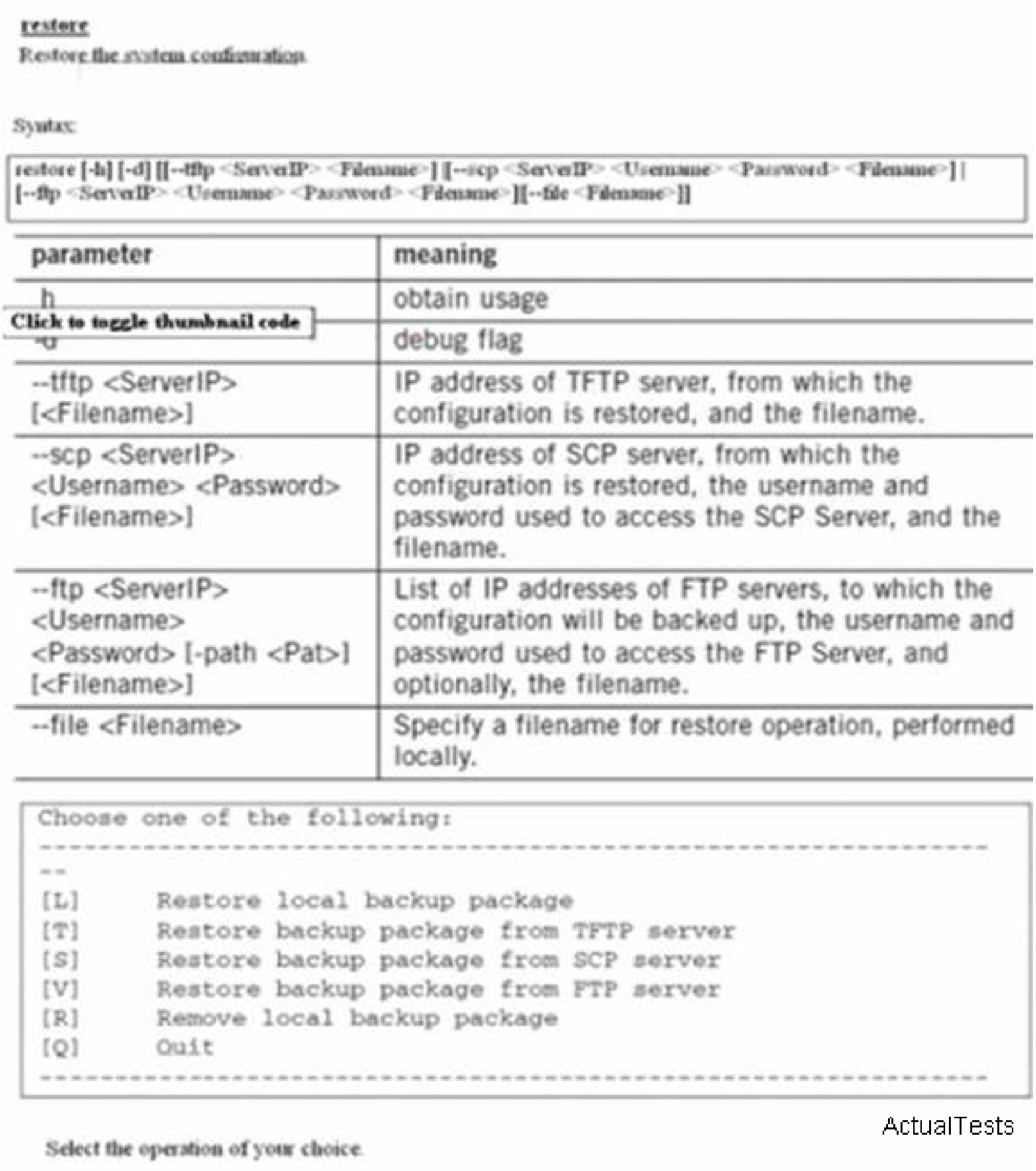
D. Follow Up

E. Download Updates

Answer: C

QUESTION NO: 38

What will the command "restore -scp 192.23.2.3 Admin passwd" do?



restore

Restore the system configuration

Syntax:

```
restore [-h] [-d] [[--tftp <ServerIP> <Filename>] | [--scp <ServerIP> <Username> <Password> <Filename>] |
[--ftp <ServerIP> <Username> <Password> <Filename>][--file <Filename>]]
```

parameter	meaning
h	obtain usage
-d	debug flag
--tftp <ServerIP> [<Filename>]	IP address of TFTP server, from which the configuration is restored, and the filename.
--scp <ServerIP> <Username> <Password> [<Filename>]	IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.
--ftp <ServerIP> <Username> <Password> [-path <Pat>] [<Filename>]	List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.
--file <Filename>	Specify a filename for restore operation, performed locally.

```
Choose one of the following:
-----------------------------------------------------------------
--
[L]     Restore local backup package
[T]     Restore backup package from TFTP server
[S]     Restore backup package from SCP server
[V]     Restore backup package from FTP server
[R]     Remove local backup package
[Q]     Quit
-----------------------------------------------------------------
```

Select the operation of your choice

A. Restore configfile file from SCP server with an IP address 192.23.2.3, and login to it using username Admin and password passwd
B. Restore Admin file from SCP server with an IP address 192.23.2.3, and login to it using username Admin and password configfile
C. Restore configfile file from SCP server with an IP address 192.23.2.3, and login to it using username passwd and password Admin
D. Restore Admin file from TFTP server with an IP address 192.23.2.3, and login to it using username Admin and password configfile
E. Restore configfile file from TFTP server with an IP address 192.23.2.3, and login to it using username Admin and password passwd

Answer: A

QUESTION NO: 39

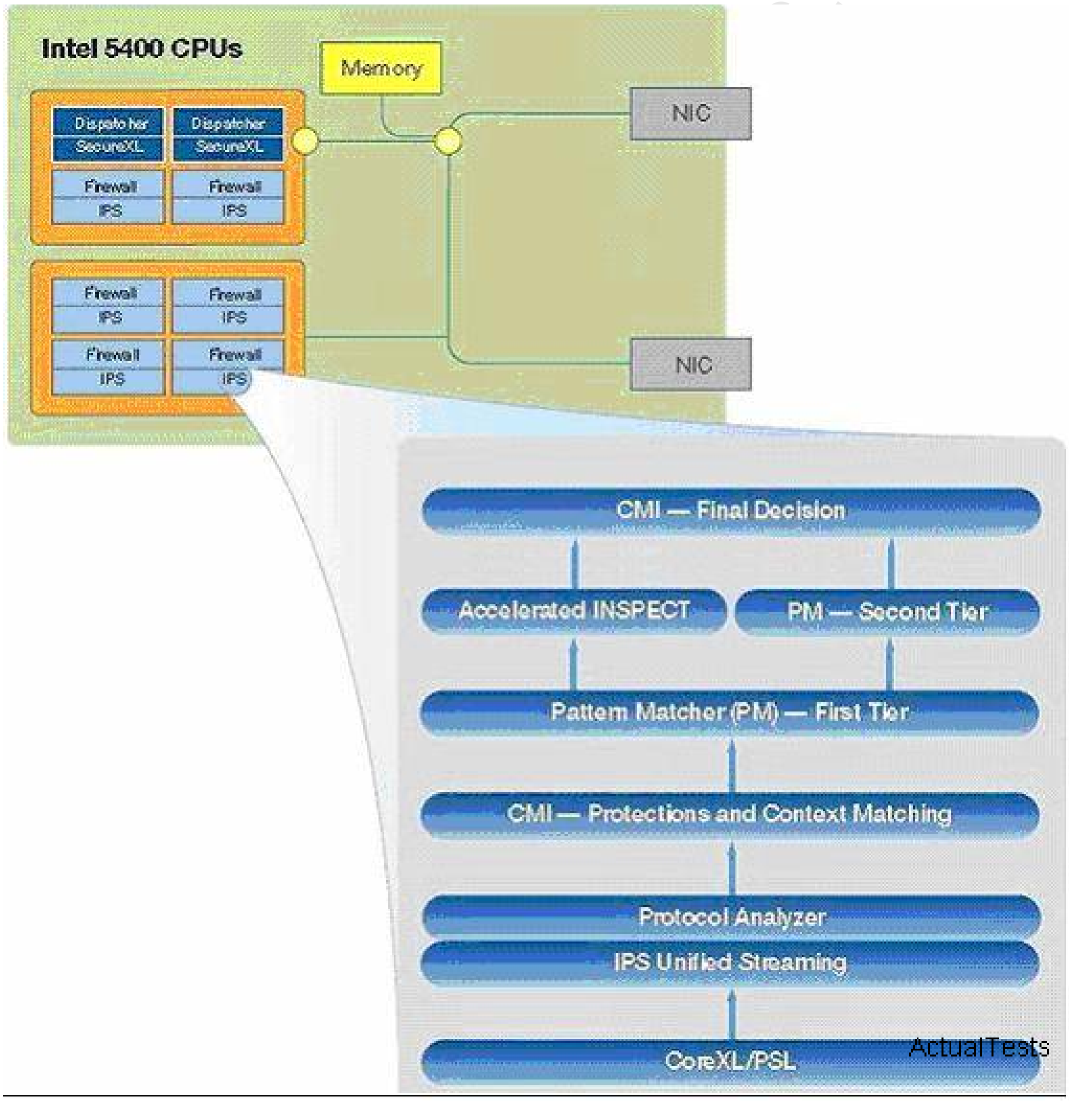
Which of the following will you consult to receive the list of address ranges that are recommended for blocking?

A. DShield Storm Center
B. Address range site
C. SmartView Tracker
D. SmartView Monitor
E. IP Block List site

Answer: A

QUESTION NO: 40

Which architecture component is the "brain" of the IPS engine that coordinates different components, decides which protections should run on a certain packet, decides the final action to be performed on the packet and issues an event log?



A. Passive Streaming Library
B. Context Management Infrastructure
C. Protocol Parsers
D. Compound Signature Identification
E. Pattern Matcher

Answer: B

QUESTION NO: 41

What is technique whereby an intruder attempts to gain unauthorized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges?

A. Encryption
B. IP Spoofing
C. Authentication
D. Tracker
E. NAT

Answer: B

QUESTION NO: 42

Which of the following is true regarding addition of a new Software Blades to your existing hardware?

A. No need to do anything aside from turning on their functionality
B. You will need to update the driver of your existing hardware
C. You will need to update the firmware of your existing hardware
D. There is no way to add a new Software Blades to your existing hardware
E. You will have to add a new hardware to accommodate the change

Answer: A

QUESTION NO: 43

What two conditions must be met when you are manually adding CheckPoint appliances to an existing cluster?

A. You must configure interfaces with IP addresses in each of the networks the cluster will connect to

B. R70 is not running on the system you are adding
C. The IP address should be the real IP address of a cluster interface
D. R70 is running on the system you are adding
E. The existing nodes must be running R70 and firewall monitoring is enabled on them

Answer: B,E

QUESTION NO: 44

The two main branches of Asymmetric encryption are Public key encryption and :

A. LDAP
B. Digital signatures
C. Universal key encryption
D. Privatekey encryption
E. Handshake

Answer: B

QUESTION NO: 45

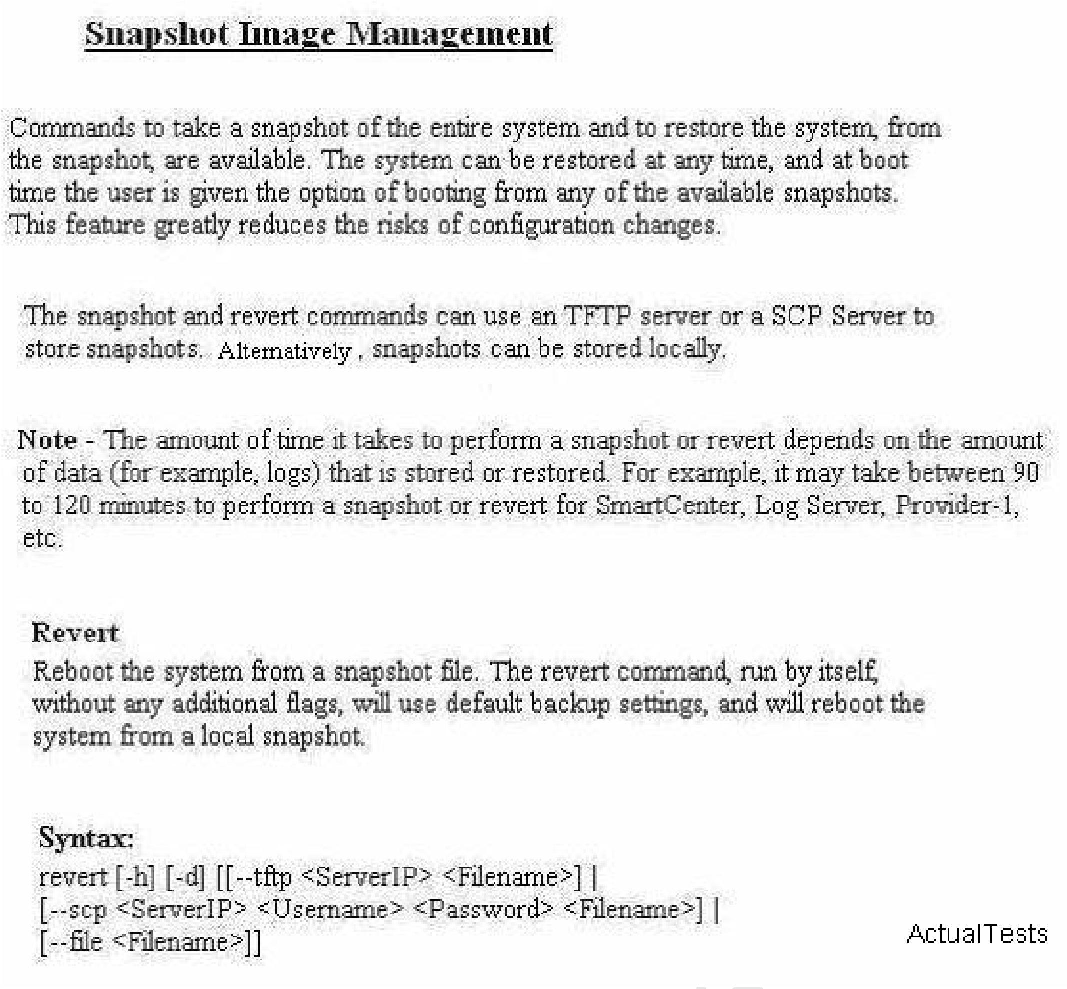
How would you create or define a new user Template?

A. By going to CheckPoint SmartDashboard, select Users menu. In the emerging Users window, click on New button
B. By going to SmartView Status, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button
C. By going to SmartView Tracker, select Clients from Manage menu. In the emerging Users window, click on New button
D. By going to SmartView Tracker, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button
E. By going to CheckPoint SmartDashboard, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button

Answer: E

QUESTION NO: 46

What would the command "revert 192.155.46.56 configfile" achieve in SecurePlatform CLI?



Snapshot Image Management

Commands to take a snapshot of the entire system and to restore the system, from the snapshot, are available. The system can be restored at any time, and at boot time the user is given the option of booting from any of the available snapshots. This feature greatly reduces the risks of configuration changes.

The snapshot and revert commands can use an TFTP server or a SCP Server to store snapshots. Alternatively , snapshots can be stored locally.

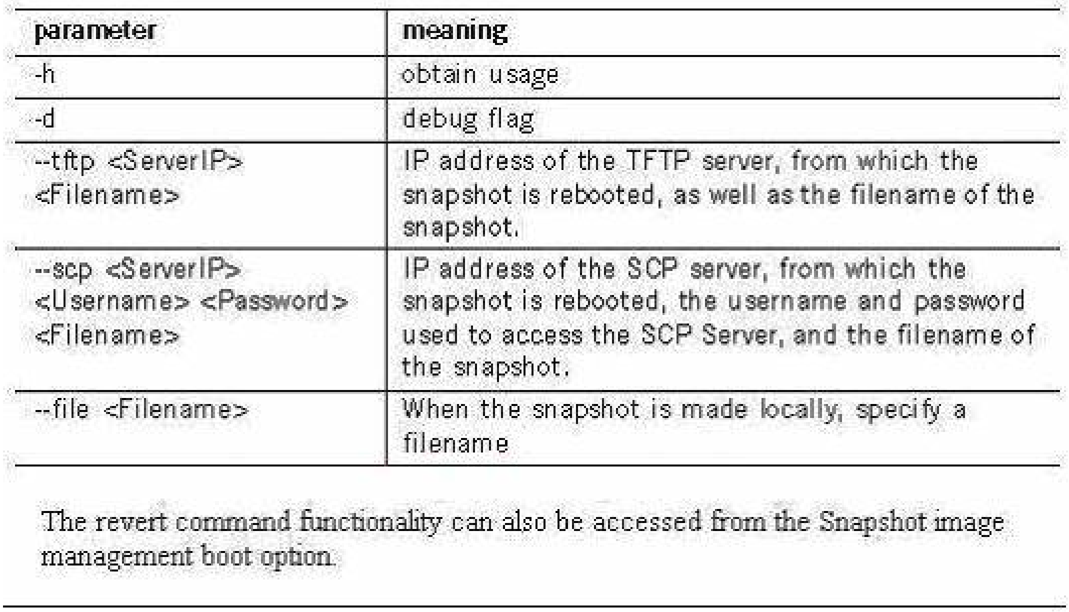
Note - The amount of time it takes to perform a snapshot or revert depends on the amount of data (for example, logs) that is stored or restored. For example, it may take between 90 to 120 minutes to perform a snapshot or revert for SmartCenter, Log Server, Provider-1, etc.

Revert

Reboot the system from a snapshot file. The revert command, run by itself, without any additional flags, will use default backup settings, and will reboot the system from a local snapshot.

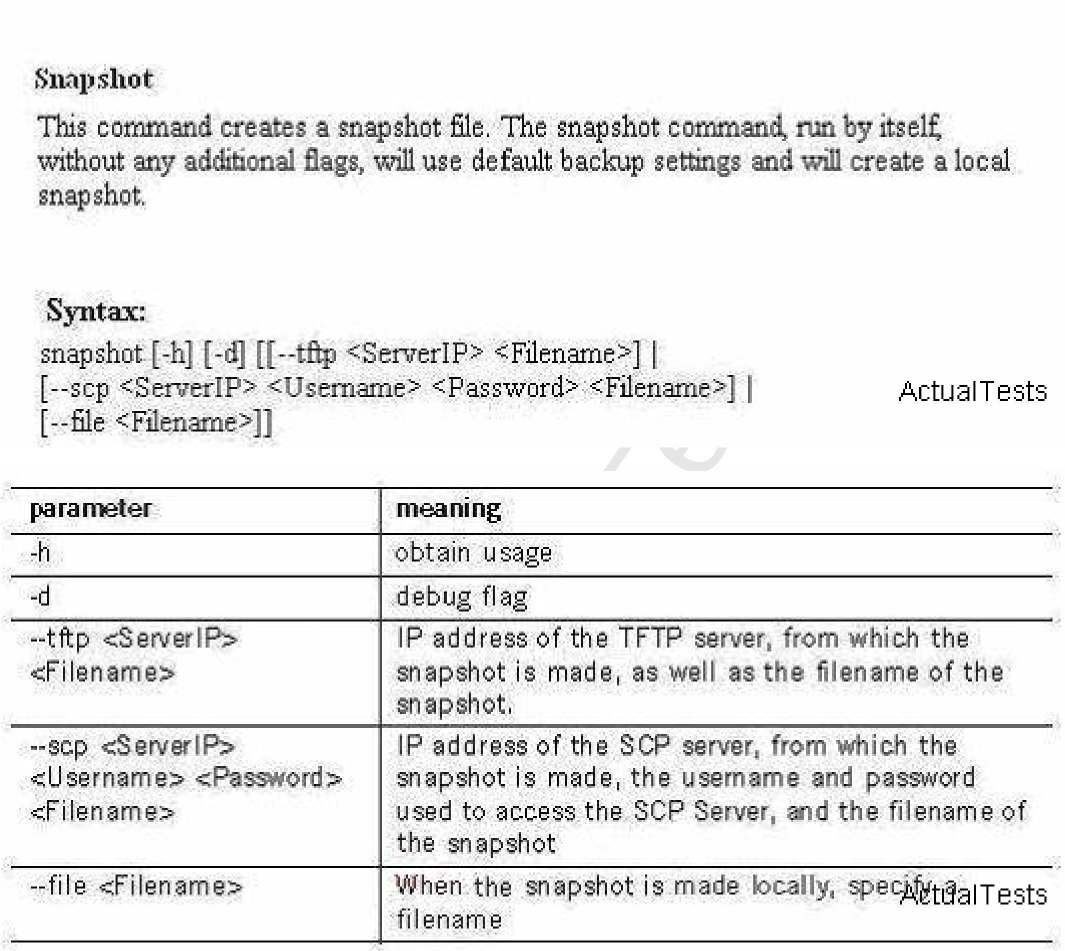
Syntax:

```
revert [-h] [-d] [[--tftp <ServerIP> <Filename>] |
[--scp <ServerIP> <Username> <Password> <Filename>] |
[--file <Filename>]]
```



parameter	meaning
-h	obtain usage
-d	debug flag
--tftp <ServerIP> <Filename>	IP address of the TFTP server, from which the snapshot is rebooted, as well as the filename of the snapshot.
--scp <ServerIP> <Username> <Password> <Filename>	IP address of the SCP server, from which the snapshot is rebooted, the username and password used to access the SCP Server, and the filename of the snapshot.
--file <Filename>	When the snapshot is made locally, specify a filename

The revert command functionality can also be accessed from the Snapshot image management boot option.



Snapshot

This command creates a snapshot file. The snapshot command, run by itself, without any additional flags, will use default backup settings and will create a local snapshot.

Syntax:

```
snapshot [-h] [-d] [[--tftp <ServerIP> <Filename>] |
[--scp <ServerIP> <Username> <Password> <Filename>] |
[--file <Filename>]]
```

parameter	meaning
-h	obtain usage
-d	debug flag
--tftp <ServerIP> <Filename>	IP address of the TFTP server, from which the snapshot is made, as well as the filename of the snapshot.
--scp <ServerIP> <Username> <Password> <Filename>	IP address of the SCP server, from which the snapshot is made, the username and password used to access the SCP Server, and the filename of the snapshot
--file <Filename>	When the snapshot is made locally, specify a filename

A. Ignore the file called configfile from TFTP server with an IP address of 192.155.46.56

B. Reboot the system from a snapshot file called configfile placed in the TFTP server with an IP address of 192.155.46.56

C. Kill the file called configfile from TFTP server with an IP address of 192.155.46.56

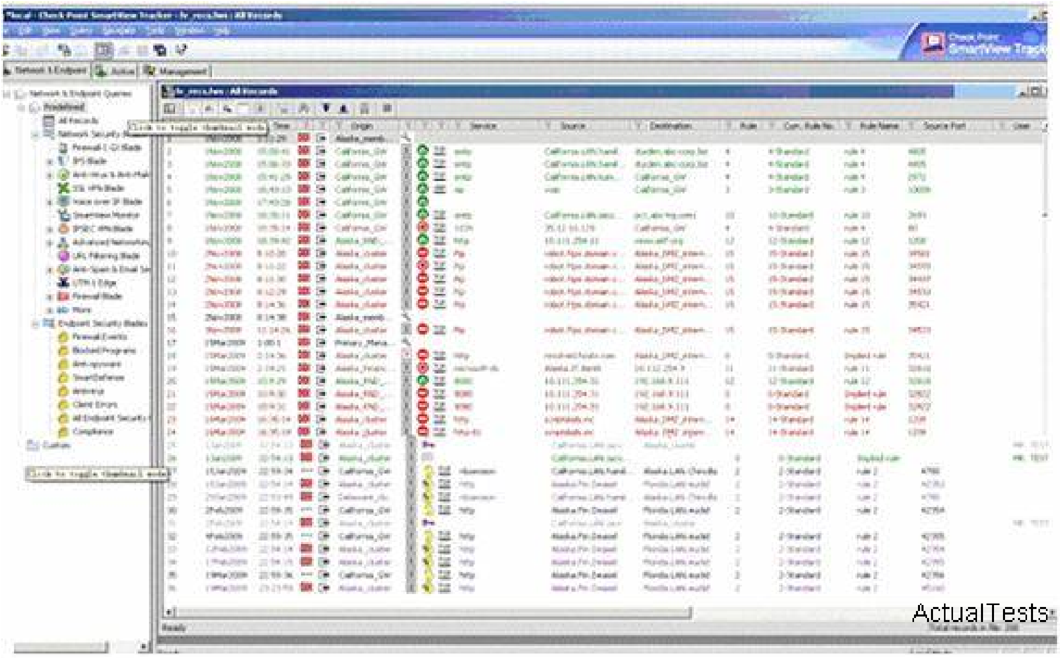
D. Stop the system when booted from a snapshot file called configfile placed in the TFTP server with an IP address of 192.155.46.56

E. Purge the file called configfile from TFTP server with an IP address of 192.155.46.56

Answer: B

QUESTION NO: 47

Study the diagram and answer the question below. What type of client GUI is shown in the diagram?

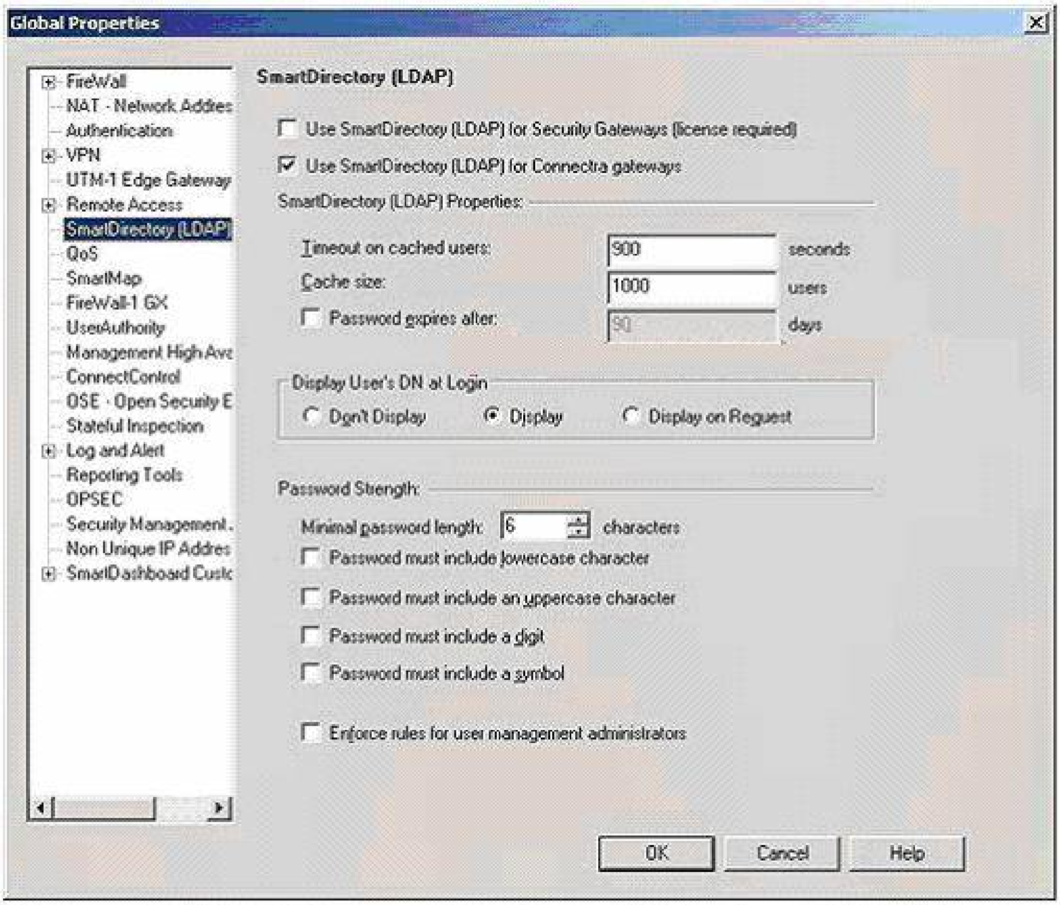


A. SmartView Status
B. Security Status GUI
C. SmartView Tracker
D. Security SmartDashboard
E. Rule Base GUI

Answer: C

QUESTION NO: 48

Where would you go enable SmartDirectory (LDAP) attributes?



SmartDirectory (LDAP)

☐ Use SmartDirectory (LDAP) for Security Gateways (license required)

☑ Use SmartDirectory (LDAP) for Connectra gateways

SmartDirectory (LDAP) Properties:

Timeout on cached users: 900 seconds

Cache size: 1000 users

☐ Password expires after: 90 days

Display User's DN at Login

○ Don't Display ● Display ○ Display on Request

Password Strength:

Minimal password length: 6 characters

☐ Password must include lowercase character

☐ Password must include an uppercase character

☐ Password must include a digit

☐ Password must include a symbol

☐ Enforce rules for user management administrators

Figure 1: Global Properties - SmartDirectory (LDAP) page

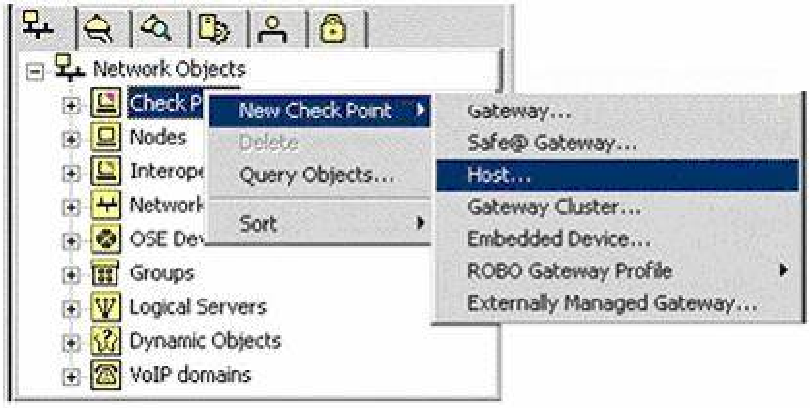


Figure 2: Defining a new SmartDirectory (LDAP) server in the Objects Tree

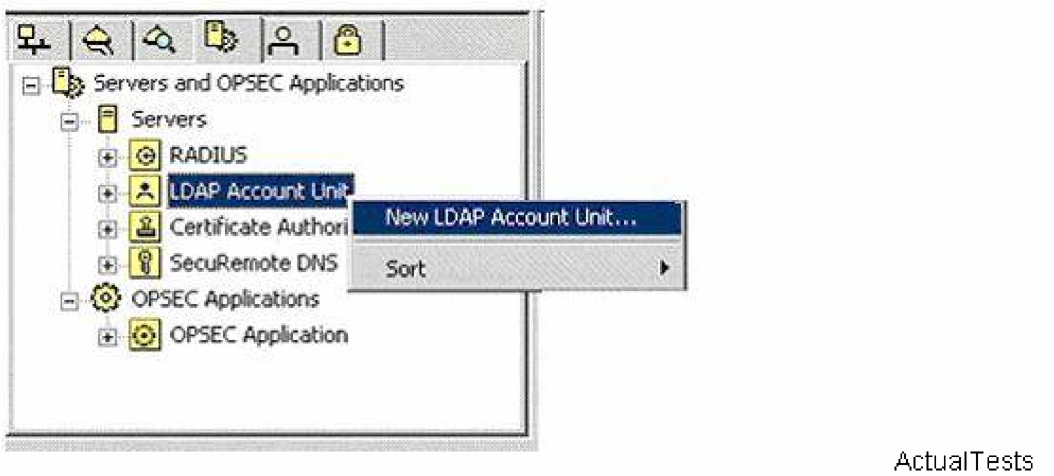


Figure 3: Defining a new SmartDirectory (LDAP) Account Unit in the Objects Tree

A. In the LDAP Properties window, SmartDirectory(LDAP) page
B. In the Gateway Properties window, SmartDirectory(LDAP) page
C. In the Host Properties window, SmartDirectory(LDAP) page
D. In the User Properties window, SmartDirectory(LDAP) page
E. In the Global Properties window, SmartDirectory(LDAP) page

Answer: E

QUESTION NO: 49

When carrying out a backup operation on R70, you will have to backup which of the following files?

A. $FWDIR/conf/objects_5_0.C
B. $FWDIR/conf/rule.fws
C. $FWDIR/database/fwauth.NDB*
D. $FWDIR/conf/rulebases_5_0.fws
E. $FWDIR/database/control.map

Answer: A,C,D

QUESTION NO: 50

Which of the following is true of VPN Tunnel Interfaces (VTI)? Select of all the correct answers.

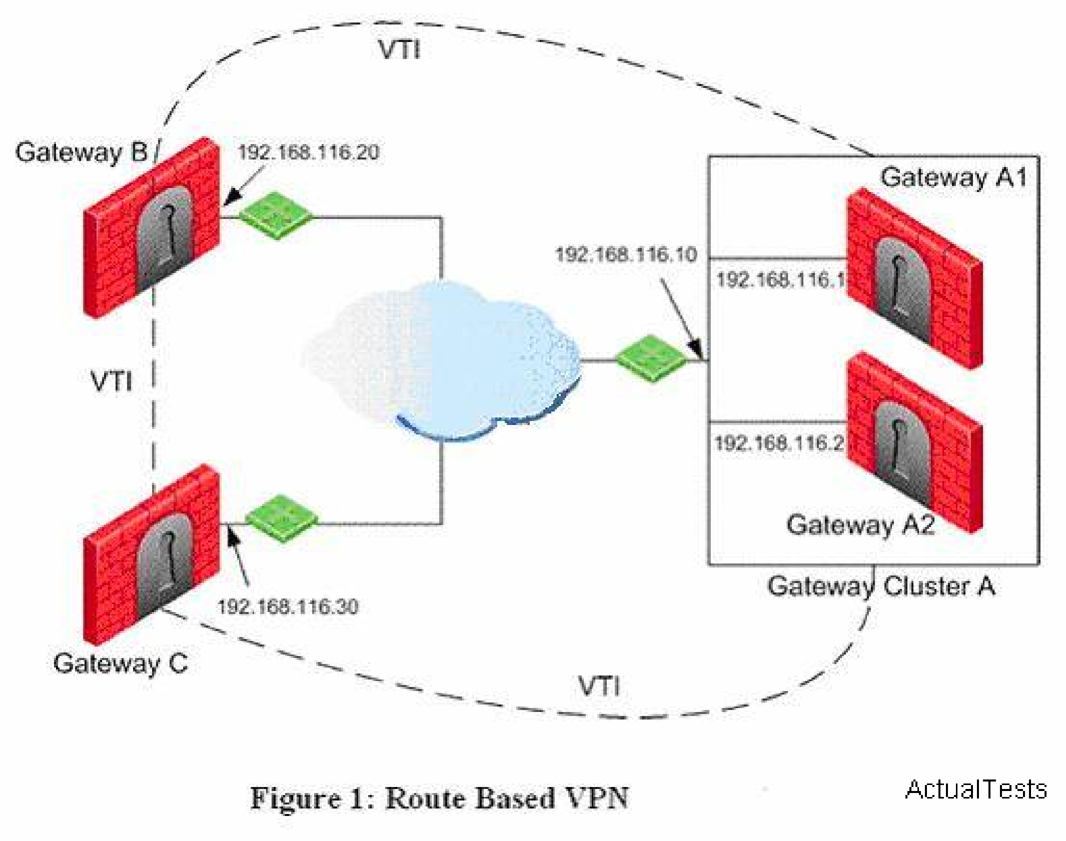


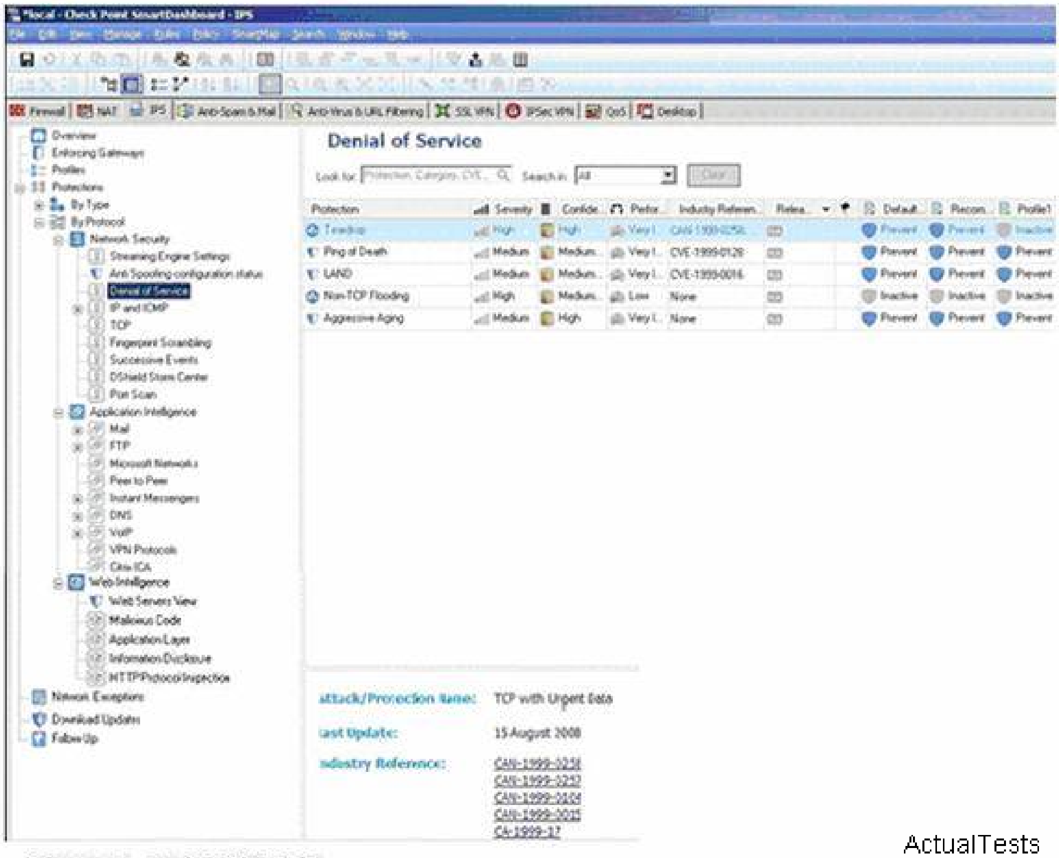
Figure 1: Route Based VPN

A. In Route Based VPN, VTIs are created on the local Gateway. Each VTI is associated with a corresponding VTI on a remote gateway peer
B. The use of VTI introduces a new method of configuring VPNs called Route Based VPN
C. Route Based VPN is supported on SecurePlatform and Nokia IPSO 3.9 platforms and above
D. A VTI is an Operating System level virtual interface that can be used as a Gateway to the encryption domain of the peer gateway.
E. Route Based VPN is supported on all OS platforms

Answer: A,B,C,D

QUESTION NO: 51

To configure various security pertain to POP3 and IMAP, what section would you go to in the Application Intelligence section of the IPS?



Denial of Service

Look for: Protection, Category, CVE... Search in: All Clear

Protection	Severity	Confide...	Perfor...	Industry Referen...	Relea...	Default...	Recom...	Profile1
Teardrop	High	High	Very l...	CAN-1999-0258...		Prevent	Prevent	Inactive
Ping of Death	Medium	Medium...	Very l...	CVE-1999-0128		Prevent	Prevent	Prevent
LAND	Medium	Medium...	Very l...	CVE-1999-0016		Prevent	Prevent	Prevent
Non-TCP Flooding	High	Medium...	Low	None		Inactive	Inactive	Inactive
Aggressive Aging	Medium	High	Very l...	None		Prevent	Prevent	Prevent

Attack/Protection Name: TCP with Urgent Data

Last Update: 15 August 2008

Industry Reference: CAN-1999-0258
CAN-1999-0252
CAN-1999-0104
CAN-1999-0015
CA-1999-17

Figure 1: IPS Tab

A. HTTP section
B. Microsoft Networks section
C. Mail section
D. Denial of Service section
E. FTP section

Answer: C

QUESTION NO: 52

A host listens for router advertisements via the all-hosts multicast IP address. Which of the following is the correct all-hosts multicast IP address?

A. 224.0.0.1
B. 224.0.0.3
C. 224.0.0.13
D. 224.0.0.4
E. 224.0.0.5

Answer: A

QUESTION NO: 53

Refer to the diagram and answer the following questions. To allow the user to access a network resource protected by a security gateway, a VPN tunnel establishment process is initiated. An IKE negotiation takes place between the gateways. At what point can the Client successful connect to the Host 1?

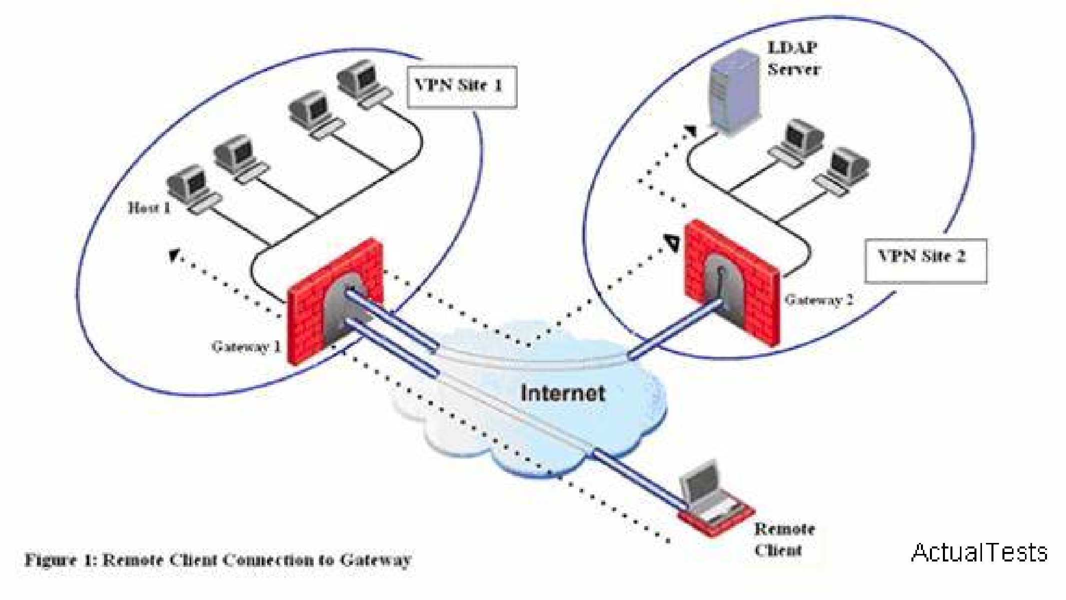


Figure 1: Remote Client Connection to Gateway

A. Once IKE is successfully completed, and before the tunnel is created
B. During the IKE negotiation process
C. Once IKE is successfully completed, and a tunnel is created
D. Before the IKE negotiation process
E. Before the IKE takes place

Answer: C

QUESTION NO: 54

Which of the following tools will you use to manage IP Appliances?

A. SmartView Tracker
B. SmartDashboard
C. SmartProvisioning
D. Network Voyager
E. SmartUpdate

Answer: D

QUESTION NO: 55

With the license_upgrade tool you can:

A. Perform the actual license upgrade process
B. Manage non license issues
C. Simulate the license upgrade process
D. View the status of the currently installed licenses
E. View the licenses installed on your machine

Answer: A,C,D,E

QUESTION NO: 56

What feature would you use to facilitate the creating of new users and to minimize mistakes with users details?

A. user definition
B. Group facility
C. user based
D. User facility
E. User templates

Answer: E

QUESTION NO: 57

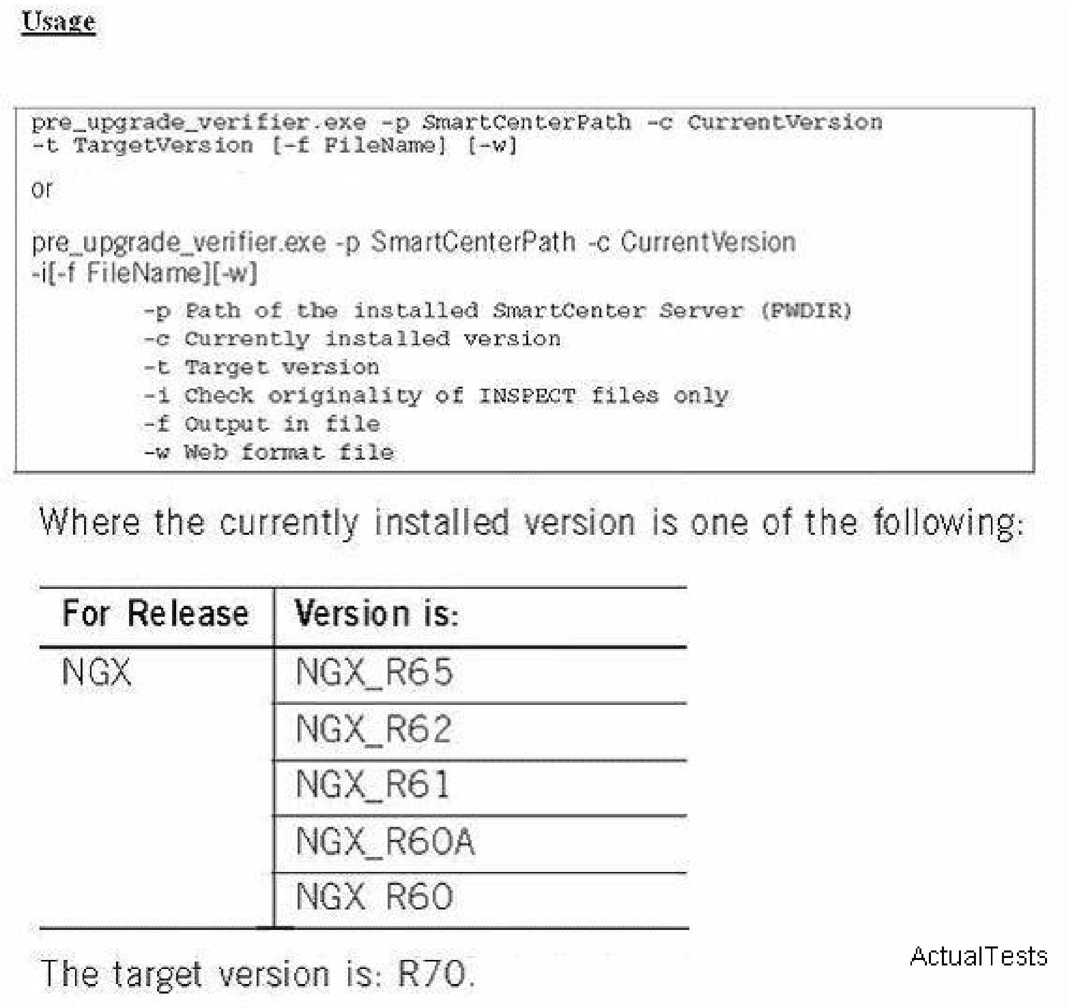
The default settings in the Anti-Virus window have been configured to prevent the Anti- Virus engine from overloading. If the Anti-Virus engine becomes overloaded, you can choose "Whether to block all files". The drawback of this is that choosing this option:

A. May leave you with quicker network response
B. May leave you with slower network response
C. May result in connectivity problems
D. May leave you open to virus attacks
E. May leave you with huge license fee

Answer: C

QUESTION NO: 58

Which tool will you use prior to installation to reduce the risk of incompatibility with the deployment to R70?



Usage

```
pre_upgrade_verifier.exe -p SmartCenterPath -c CurrentVersion
-t TargetVersion [-f FileName] [-w]

or

pre_upgrade_verifier.exe -p SmartCenterPath -c CurrentVersion
-i[-f FileName][-w]
        -p Path of the installed SmartCenter Server (FWDIR)
        -c Currently installed version
        -t Target version
        -i Check originality of INSPECT files only
        -f Output in file
        -w Web format file
```

Where the currently installed version is one of the following:

For Release	Version is:
NGX	NGX_R65
	NGX_R62
	NGX_R61
	NGX_R60A
	NGX R60

The target version is: R70.

A. Compatibility Tool
B. cpconfig
C. Post-Upgrade Verification Tool
D. Pre-Upgrade Verification Tool
E. cpinfo

Answer: D

QUESTION NO: 59

What are the three policy types?

A. Desktop Security
B. QoS
C. Security and Address Translation
D. Module Transition
E. Rule Base Editor

Answer: A,B,C

QUESTION NO: 60

AES, DES, CAST and RC2 are types of what? Note: If wrong answer is chosen, see the diagram for correct answer.

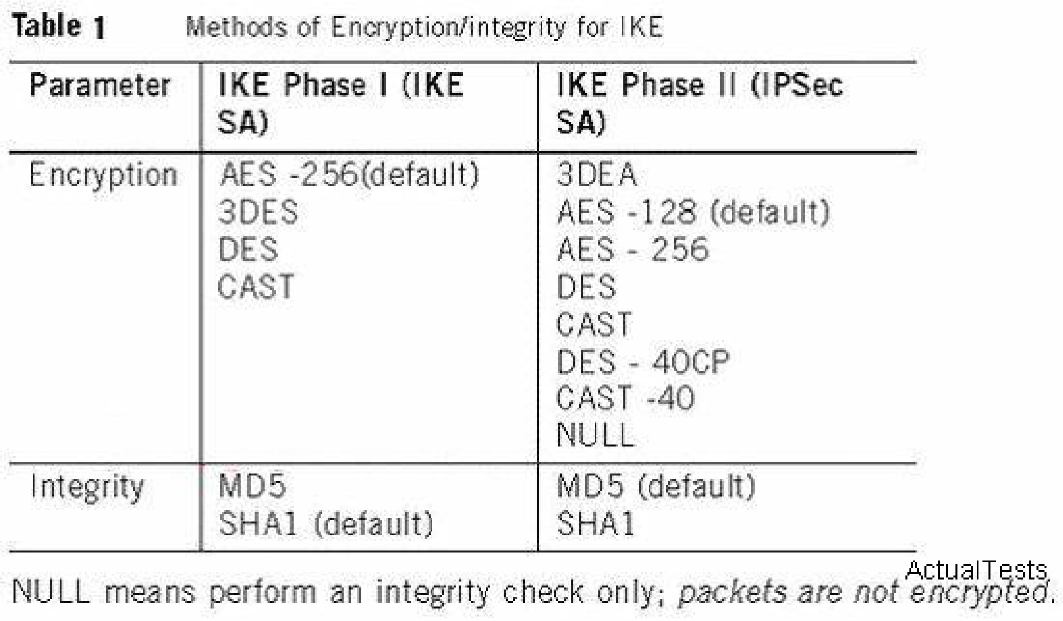


Table 1 Methods of Encryption/integrity for IKE

Parameter	IKE Phase I (IKE SA)	IKE Phase II (IPSec SA)
Encryption	AES -256(default) 3DES DES CAST	3DEA AES -128 (default) AES - 256 DES CAST DES - 40CP CAST -40 NULL
Integrity	MD5 SHA1 (default)	MD5 (default) SHA1

NULL means perform an integrity check only; *packets are not encrypted.*

A. Integrity schemes
B. Authentication algorithms
C. Encryption methods
D. Algorithm methods
E. Integrity methods

Answer: C

QUESTION NO: 61

User authentication cannot provide access privilege for which service(s)?

A. RPC
B. TELNET
C. FTP
D. RLOGIN
E. HTTP

Answer: A

QUESTION NO: 62

One of your remote users usually connects to the corporate network with a single profile. If the user has to connect from different locations e.g. hotels, partners sites etc. What do you have to do as an administrator to resolve this issue?

A. Define different user for each location
B. There is no way to resolve this
C. Configure different machine for each location
D. Define a number of connection profiles
E. Install different machine for each location

Answer: D

QUESTION NO: 63

How is CheckPoint stateful-inspection firewalls provide a security measure against port scanning?

A. By translating the IP to port
B. By filtering the incoming traffic
C. By opening all ports until the specific port is requested
D. By filtering the incoming and outdoing traffic
E. By closing all ports until the specific port is requested

Answer: E

QUESTION NO: 64

On Log File Management, what happens to the current log file when it approaches the default limit?

A. New Log file cannot be created when current file is opened
B. The current file is appended to the new file
C. The current Log file is opened in addition to the new Log file
D. The current Log file is closed and written to disk with a name that contains the current date and time
E. The current file is lost

Answer: D

QUESTION NO: 65

Which of the following events will happen during IKE Phase I? Select three answers

A. A Diffie-Hellman key is created

B. The key material exchanged during IPSEC phase is used for building the IPSec keys
C. The peers authenticate either by certificates or via a pre-shared secret
D. IKE is encrypted according to the keys and methods agreed upon in IKE phases
E. Key material (random bits and other mathematical data) as well as an agreement on methods for IKE phase II are exchanged between the peers

Answer: A,C,E

QUESTION NO: 66

SecureClient will reconnect to the Policy Server to download a new policy when half specified time period has elapsed. If the default time is used, then the time is set to:

A. 50 minutes
B. 70 minutes
C. 60 minutes
D. 80 minutes
E. 40 minutes

Answer: C

QUESTION NO: 67

The advantages of using upgrade_export over other backup tools e.g. snapshot, backup are:

A. It takes longer time to complete a complex operation
B. It can be used in place of snapshot or backup utilities
C. It can backup routing tables
D. It can work on any platform i.e. its operating system independent
E. It takes shorter time to complete an operation

Answer: B,D

QUESTION NO: 68

How would you create NAT rules automatically?

A. By modifying the NAT tab of the Service object Properties window
B. By modifying the NAT tab of the SIC object Properties window
C. None of the available answers
D. By modifying your RuleBase

E. By modifying the NAT tab of the Network object Properties window

Answer: E

QUESTION NO: 69

In the IPS Software Blade, you want to activate all critical protections and minimize the rate of false positive. Do you think this is possible?

A. Partially true, as the IPS gives you the ability to activate all checks with critical severity and cannot allow you to minimize the rate of false positive
B. This is not possible
C. Activating all checks with critical severity comes with high false positive
D. Yes, as the IPS gives you the ability to activate all checks with critical severity and high confidence level
E. Partially true, as the IPS does not give you the ability to activate all checks with critical severity and but does allow you to minimize the rate of false positive

Answer: D

QUESTION NO: 70

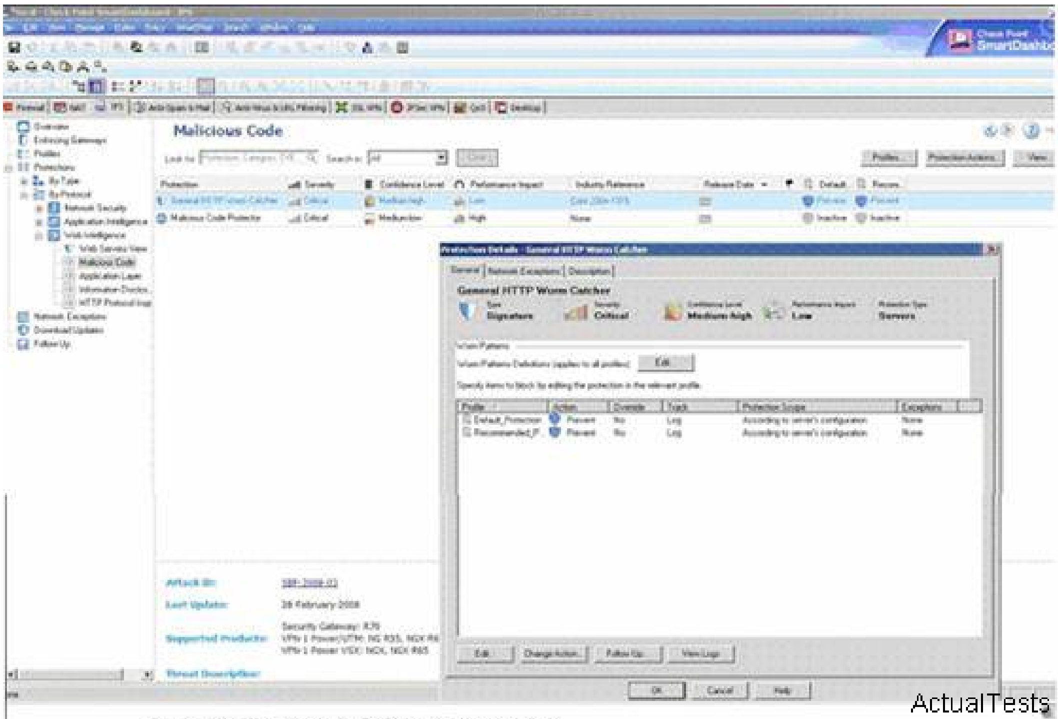
Which Check Point product provides network administrators with the tools they need to monitor traffic and identify bottlenecks as they occur?

A. SmartDashboard
B. SmartView Monitor
C. SmartView Status
D. SmartView Tracker
E. SmartView Dashboard

Answer: B

QUESTION NO: 71

In IPS, each protection is clearly marked with a performance impact setting in terms of:



Malicious Code

Protection	Severity	Confidence Level	Performance Impact	Industry Reference	Release Date	Default	Recom...
General HTTP Worm Catcher	Critical	Medium-high	Low	[illegible]		Prevent	Prevent
Malicious Code Protector	Critical	Medium-low	High	None		Inactive	Inactive

Protection Details - General HTTP Worm Catcher

General HTTP Worm Catcher

Type: Signature
Severity: Critical
Confidence Level: Medium-high
Performance Impact: Low
Protection Type: Servers

Worm Patterns

Worm Patterns Definitions (applies to all profiles)

Specify items to block by editing the protection in the relevant profile.

Profile	Action	Override	Track	Protection Scope	Exceptions
Default_Protection	Prevent	No	Log	According to server's configuration	None
Recommended_P...	Prevent	No	Log	According to server's configuration	None

Attack ID: [illegible]
Last Update: 28 February 2008
Supported Products: Security Gateway: R70
VPN-1 Power/UTM: NG R55, NGX R6...
VPN-1 Power VSX: NGX, NGX R65
Threat Description:

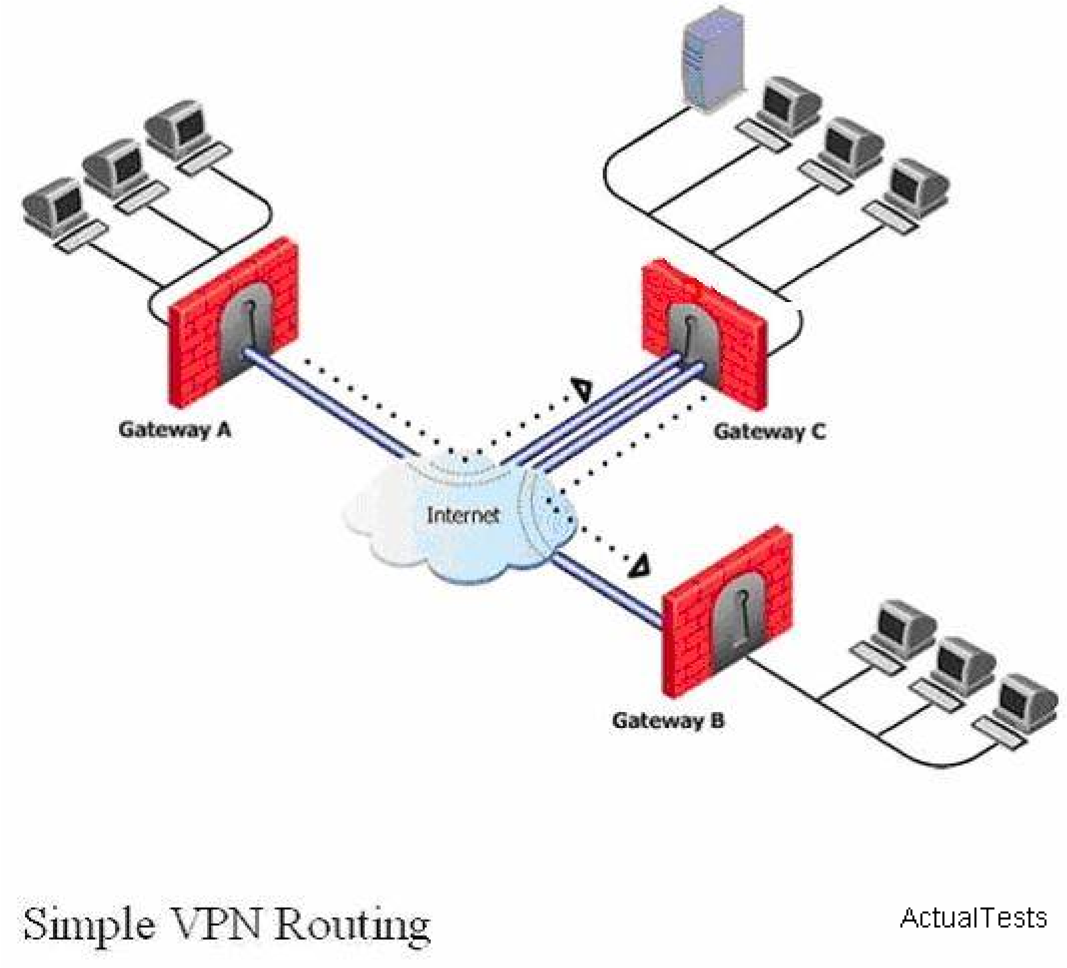
Figure 1: IPS Tab > Protocol > By Protocol > Malicious Code

A. Medium
B. Low
C. High
D. Critical
E. Harsh

Answer: A,B,C,D

QUESTION NO: 72

Which of the following is a method of controlling how VPN traffic is routed between gateway modules and remote access clients within a community?



A. Office Based VPN
B. Route Based VPN
C. Domain Based VPN
D. Remote Based VPN
E. Directional VPN

Answer: C

QUESTION NO: 73

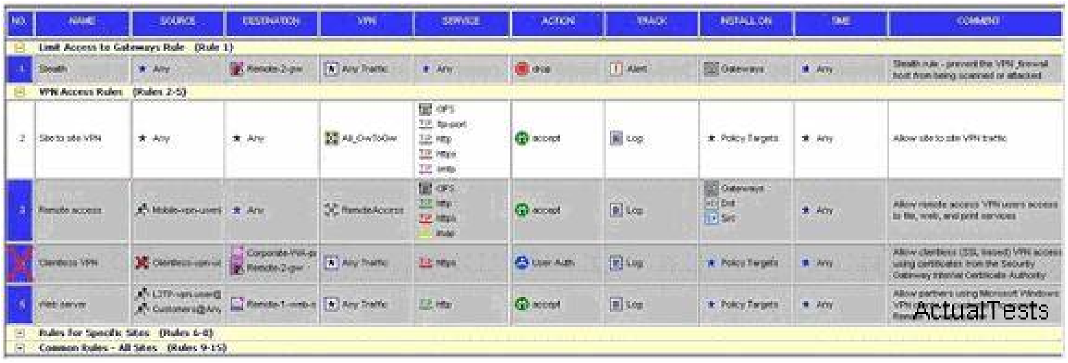
What type of authentication is used to authenticate any service on a per-session basis?

A. Client authentication
B. Session authentication
C. Transparent authentication
D. User authentication
E. Automatic authentication

Answer: B

QUESTION NO: 74

What should the Destination column of Stealth rule be set to?



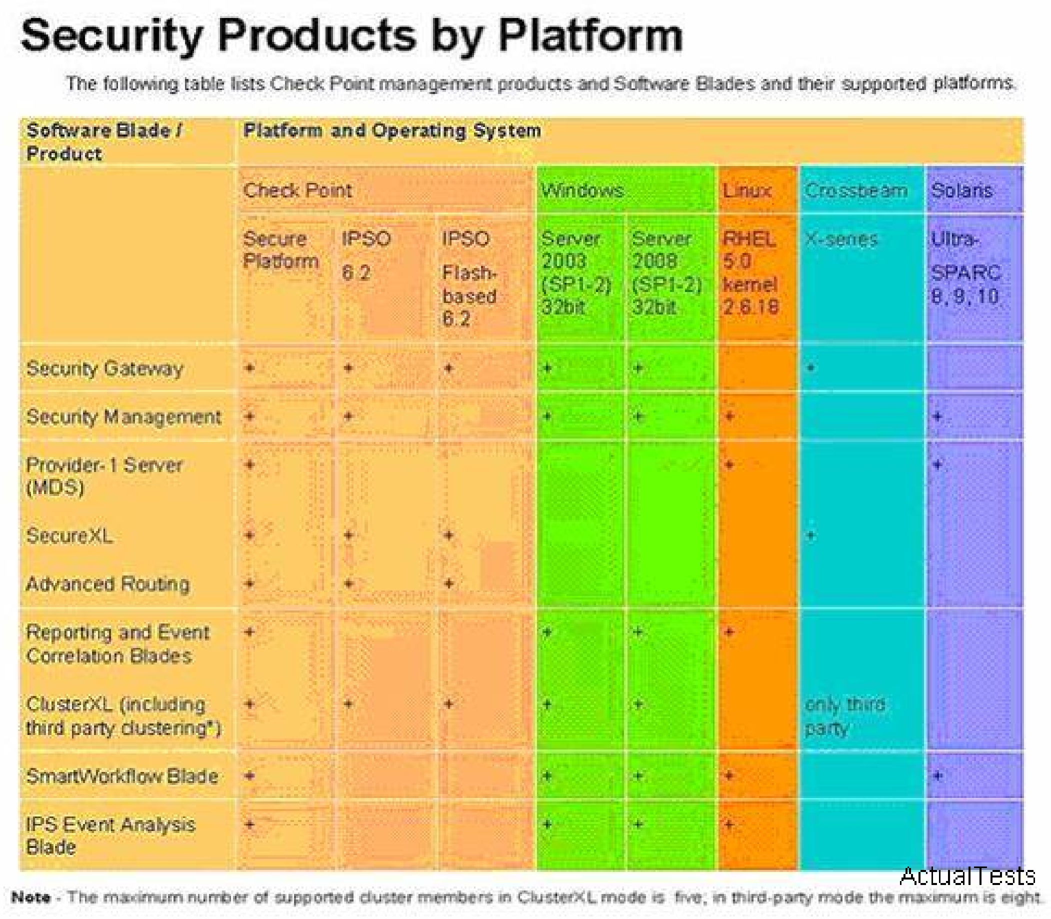
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊟	Limit Access to Gateways Rule (Rule 1)									
1	Stealth	★ Any	Remote-2-gw	Any Traffic	★ Any	drop	Alert	Gateways	★ Any	Stealth rule - prevent the VPN firewall host from being scanned or attacked
⊟	VPN Access Rules (Rules 2-5)									
2	Site to site VPN	★ Any	★ Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	★ Policy Targets	★ Any	Allow site to site VPN traffic
3	Remote access	Mobile-vpn-users	★ Any	RemoteAccess	CIFS http https imap	accept	Log	Gateways Dst Src	★ Any	Allow remote access VPN users access to file, web, and print services
4	Clientless VPN	Clientless-vpn-u	Corporate-WA-g Remote-2-gw	Any Traffic	https	User Auth	Log	★ Policy Targets	★ Any	Allow clientless (SSL based) VPN access using certificates from the Security Gateway Internal Certificate Authority
5	Web server	L2TP-vpn-users@ Customers@Any	Remote-1-web-s	Any Traffic	http	accept	Log	★ Policy Targets	★ Any	Allow partners using Microsoft Windows VPN [illegible]
⊞	Rules for Specific Sites (Rules 6-8)									
⊞	Common Rules - All Sites (Rules 9-15)									

A. Local firewall host
B. Any service
C. Local_network
D. Any
E. Email server

Answer: A

QUESTION NO: 75

A distributed deployment, which is rather complex deployment is where the Security Gateway and the Security Management server are deployed on different machines. In all deployments, whether standalone or distributed, SmartConsole can be installed on any machine. If you want to run SmartConsole GUI on the Linux Enterprise server, and Security Gateway and Security Management server on the Windows Server 2003, then what do you call such configuration?

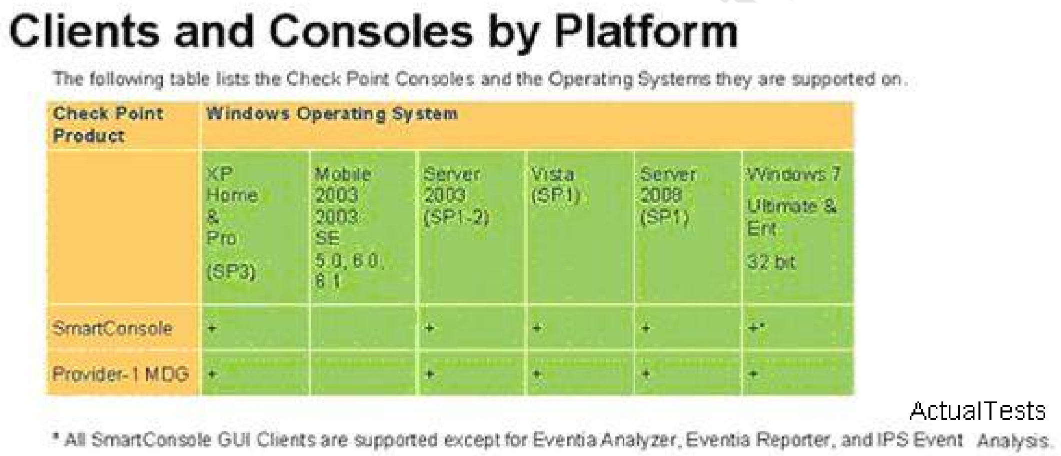


Security Products by Platform

The following table lists Check Point management products and Software Blades and their supported platforms.

Software Blade / Product	Platform and Operating System							
	Check Point			Windows		Linux	Crossbeam	Solaris
	Secure Platform	IPSO 6.2	IPSO Flash-based 6.2	Server 2003 (SP1-2) 32bit	Server 2008 (SP1-2) 32bit	RHEL 5.0 kernel 2.6.18	X-series	Ultra-SPARC 8, 9, 10
Security Gateway	+	+	+	+	+		+	
Security Management	+	+		+	+	+		+
Provider-1 Server (MDS)	+					+		+
SecureXL	+	+	+				+	
Advanced Routing	+	+	+					
Reporting and Event Correlation Blades	+			+	+	+		
ClusterXL (including third party clustering*)	+	+	+	+	+		only third party	
SmartWorkflow Blade	+			+	+	+		+
IPS Event Analysis Blade	+			+	+	+		

Note - The maximum number of supported cluster members in ClusterXL mode is five; in third-party mode the maximum is eight.

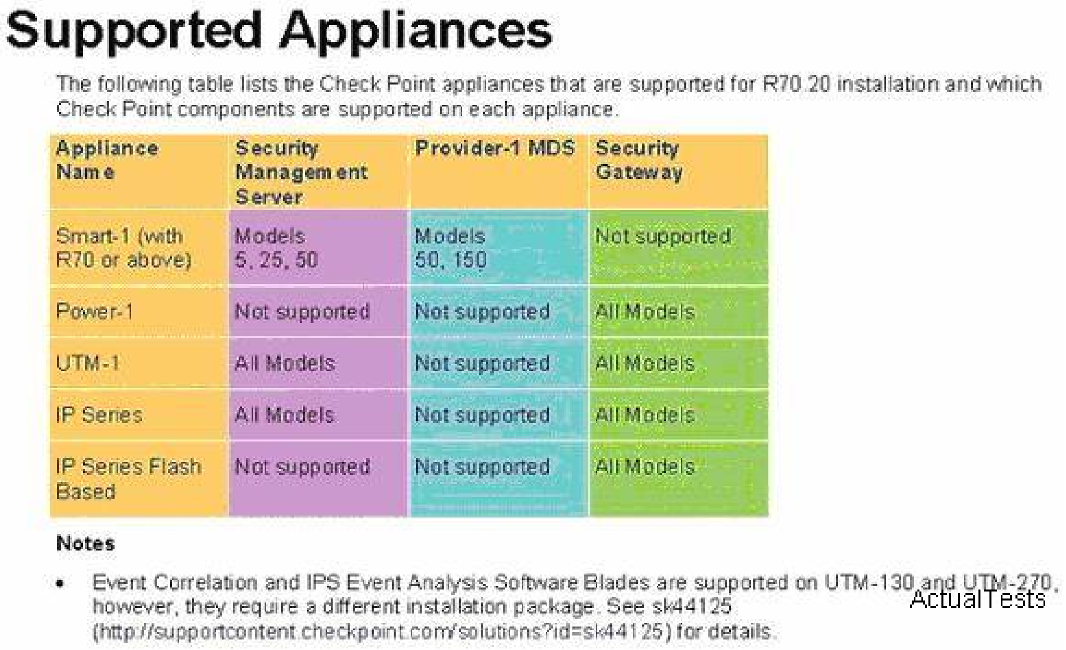


Clients and Consoles by Platform

The following table lists the Check Point Consoles and the Operating Systems they are supported on.

Check Point Product	Windows Operating System					
	XP Home & Pro (SP3)	Mobile 2003 2003 SE 5.0, 6.0, 6.1	Server 2003 (SP1-2)	Vista (SP1)	Server 2008 (SP1)	Windows 7 Ultimate & Ent 32 bit
SmartConsole	+		+	+	+	+*
Provider-1 MDG	+		+	+	+	+

* All SmartConsole GUI Clients are supported except for Eventia Analyzer, Eventia Reporter, and IPS Event Analysis.



Supported Appliances

The following table lists the Check Point appliances that are supported for R70.20 installation and which Check Point components are supported on each appliance.

Appliance Name	Security Management Server	Provider-1 MDS	Security Gateway
Smart-1 (with R70 or above)	Models 5, 25, 50	Models 50, 150	Not supported
Power-1	Not supported	Not supported	All Models
UTM-1	All Models	Not supported	All Models
IP Series	All Models	Not supported	All Models
IP Series Flash Based	Not supported	Not supported	All Models

Notes

- Event Correlation and IPS Event Analysis Software Blades are supported on UTM-130 and UTM-270, however, they require a different installation package. See sk44125 (http://supportcontent.checkpoint.com/solutions?id=sk44125) for details.

A. Unsupported installation or configuration

B. Standalone installation

C. Client - server configuration

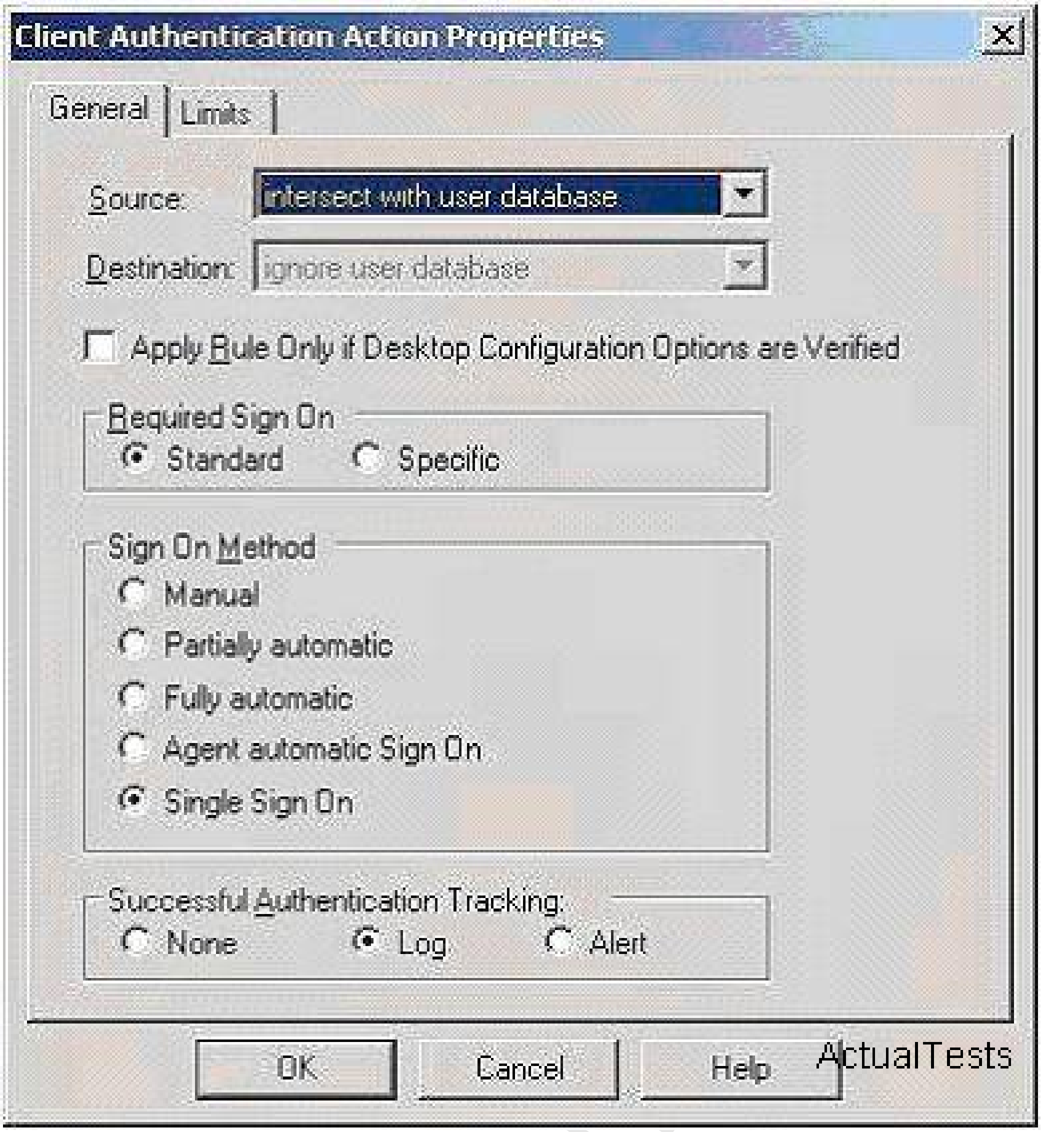
D. Distributed configuration

E. Hybrid configuration

Answer: A

QUESTION NO: 76

Study the diagram on client authentication action properties and answer the question below. To allow users to use all services permitted by the rule for the authorization period without having to perform authentication for each service, which option must you choose?



Client Authentication Action Properties

General | Limits

Source: intersect with user database

Destination: ignore user database

□ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On

● Standard ○ Specific

Sign On Method

○ Manual

○ Partially automatic

○ Fully automatic

○ Agent automatic Sign On

● Single Sign On

Successful Authentication Tracking:

○ None ● Log ○ Alert

A. Required Sign On: Specific

B. Required Sign On: Standard

C. SignOn Method: Fully Automatic

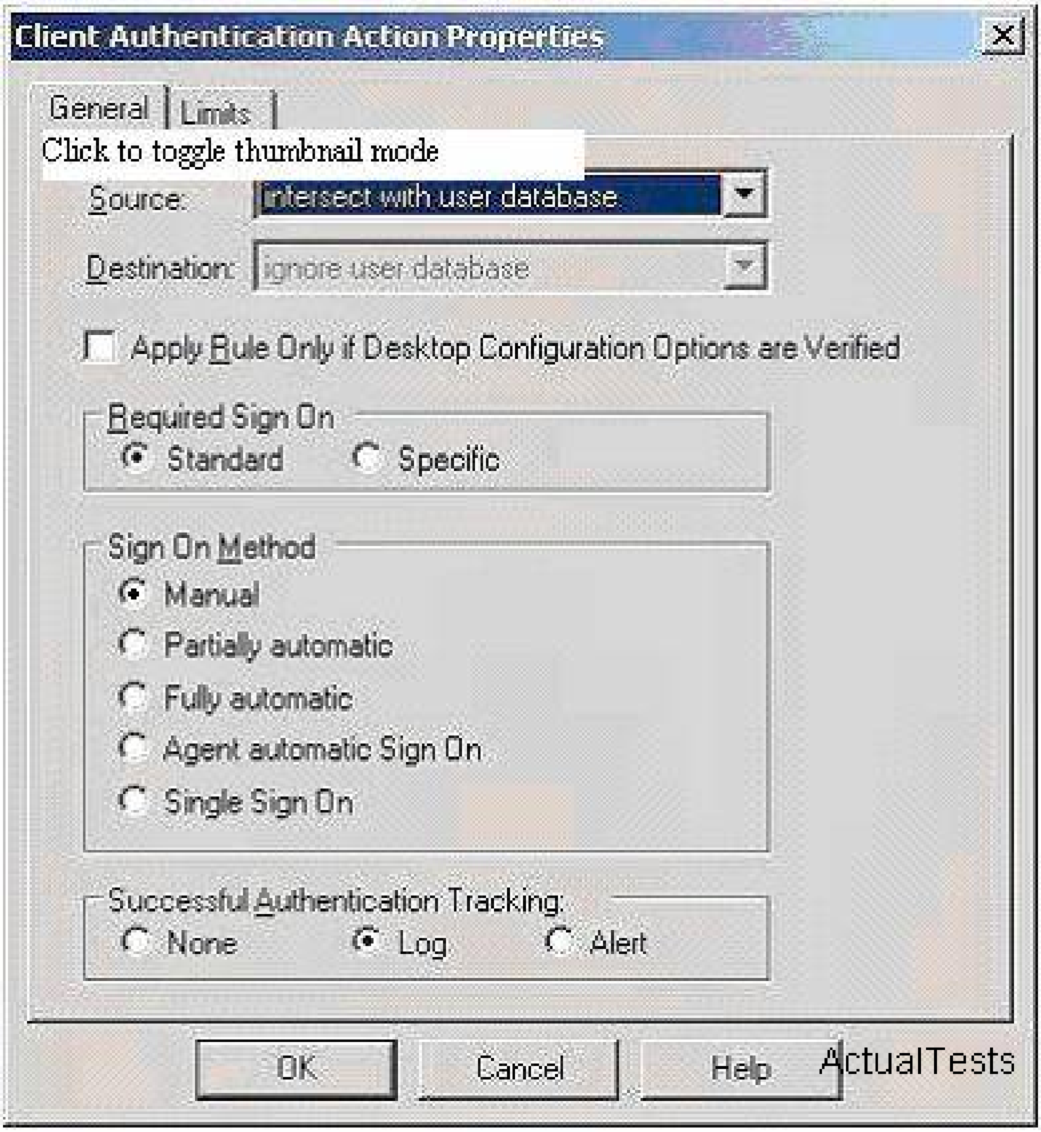
D. SignOn Method: Manual

E. SignOn Method: Partially Automatic

Answer: B

QUESTION NO: 77

If you must use " Fully Automatic Sign On" method when deploying Client Authentication for a non-authenticated service then you must:


Client Authentication Action Properties
General
Limits
Click to toggle thumbnail mode
OK
Cancel
Help

Source: Intersect with user database

Destination: ignore user database

□ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On
● Standard ○ Specific

Sign On Method
● Manual
○ Partially automatic
○ Fully automatic
○ Agent automatic Sign On
○ Single Sign On

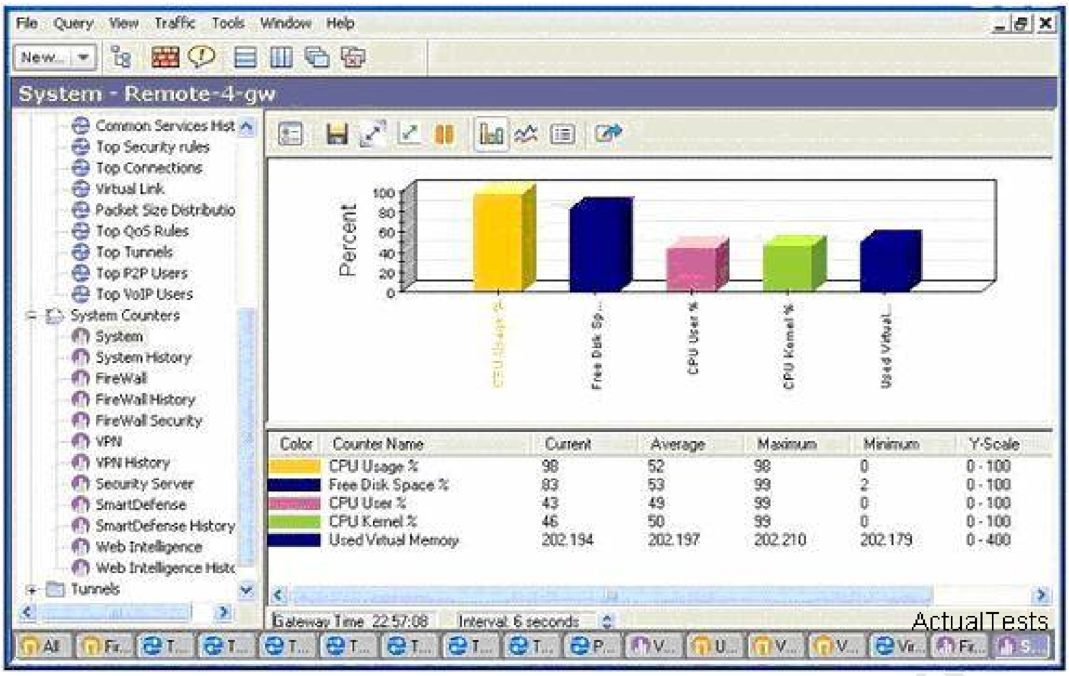
Successful Authentication Tracking:
○ None ● Log ○ Alert

A. Install Session Authentication Agent on the destination server
B. Install Session Authentication Agent on the client
C. Define additional rule in your RuleBase
D. Install Session Authentication Agent on the gateway
E. Allow Implicit rule to handle this

Answer: B

QUESTION NO: 78

The diagram shows the system counter for Remote-4-gw gateway. Which of the following is true of data? Select all the correct answers



Color	Counter Name	Current	Average	Maximum	Minimum	Y-Scale
🟨	CPU Usage %	98	52	98	0	0 - 100
🟦	Free Disk Space %	83	53	99	2	0 - 100
🟪	CPU User %	43	49	99	0	0 - 100
🟩	CPU Kernel %	46	50	99	0	0 - 100
🟦	Used Vitual Memory	202.194	202.197	202.210	202.179	0 - 400

Gateway Time 22:57:08

Interval: 6 seconds

A. The virtual memory needs upgrading

B. The disk space needs upgrading

C. The CPU needs upgrading

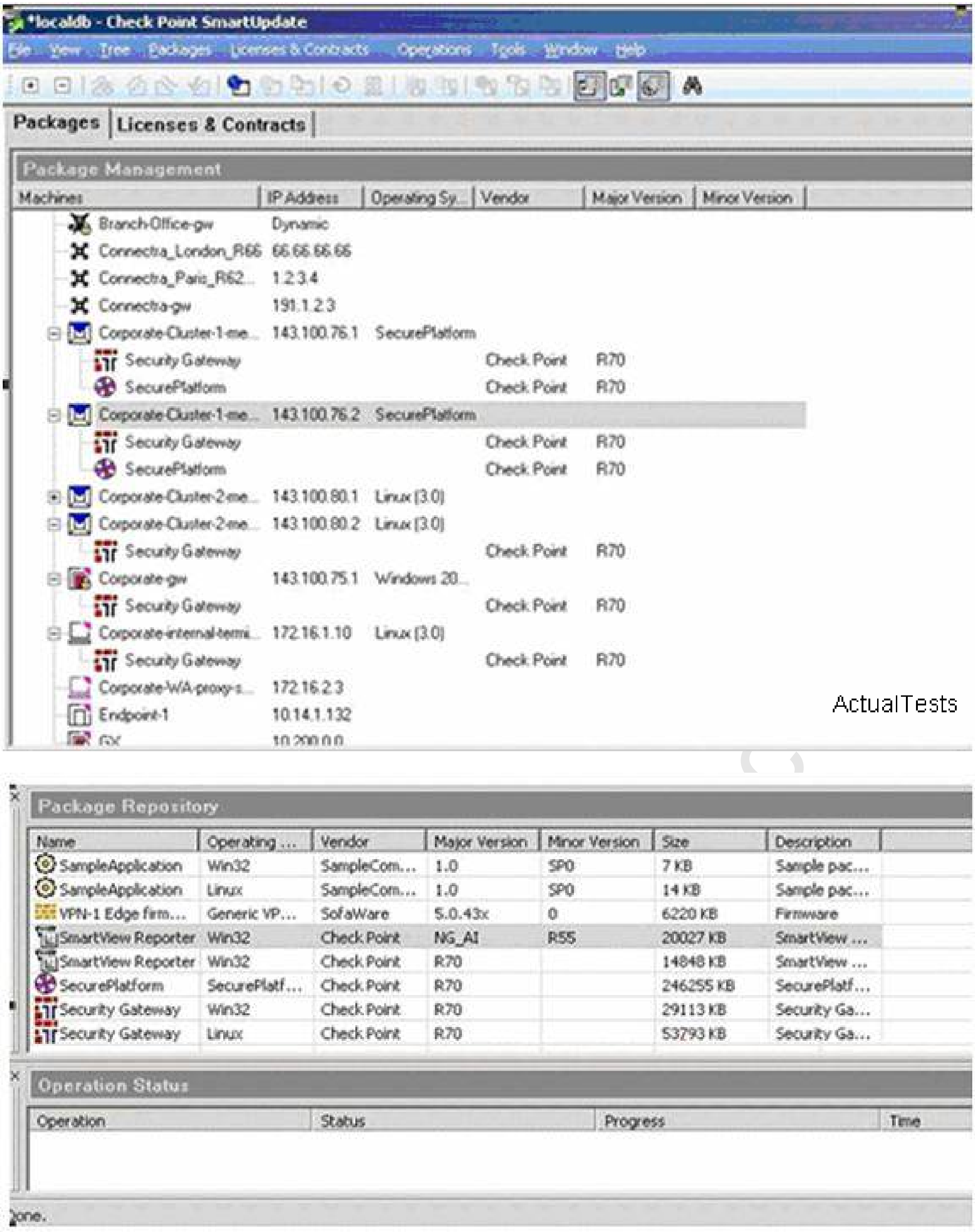
D. The disk space does not need upgrading

E. The memory needs upgrading

Answer: C,D

QUESTION NO: 79

What area would you switch to within SmartUpdate GUI when looking for installations that are presently taking place?



Package Management

Machines	IP Address	Operating Sy...	Vendor	Major Version	Minor Version
Branch-Office-gw	Dynamic				
Connectra_London_R66	66.66.66.66				
Connectra_Paris_R62...	1.2.3.4				
Connectra-gw	191.1.2.3				
Corporate-Cluster-1-me...	143.100.76.1	SecurePlatform			
Security Gateway			Check Point	R70	
SecurePlatform			Check Point	R70	
Corporate-Cluster-1-me...	143.100.76.2	SecurePlatform			
Security Gateway			Check Point	R70	
SecurePlatform			Check Point	R70	
Corporate-Cluster-2-me...	143.100.80.1	Linux [3.0]			
Corporate-Cluster-2-me...	143.100.80.2	Linux [3.0]			
Security Gateway			Check Point	R70	
Corporate-gw	143.100.75.1	Windows 20...			
Security Gateway			Check Point	R70	
Corporate-internal-termi...	172.16.1.10	Linux [3.0]			
Security Gateway			Check Point	R70	
Corporate-WA-proxy-s...	172.16.2.3				
Endpoint-1	10.14.1.132				
GX	10.200.0.0				

Package Repository

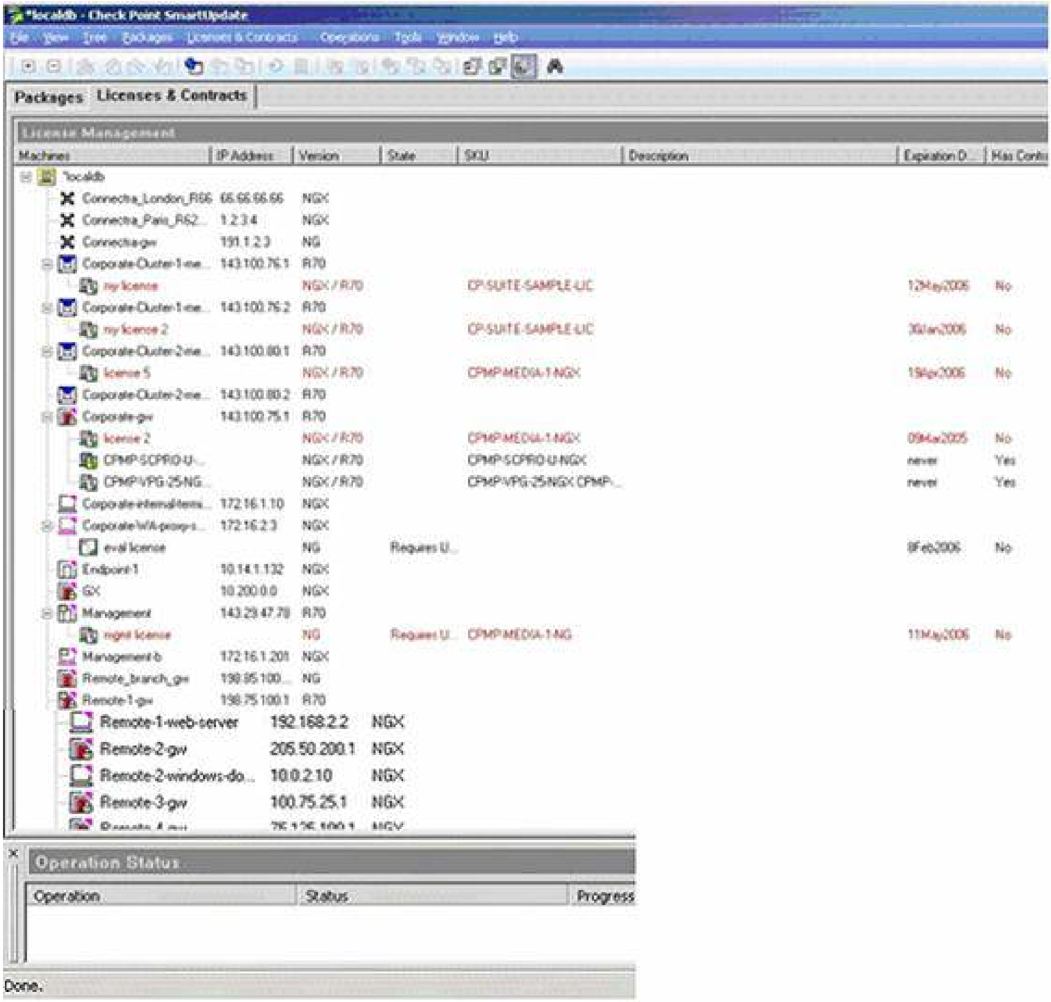
Name	Operating ...	Vendor	Major Version	Minor Version	Size	Description
SampleApplication	Win32	SampleCom...	1.0	SP0	7 KB	Sample pac...
SampleApplication	Linux	SampleCom...	1.0	SP0	14 KB	Sample pac...
VPN-1 Edge firm...	Generic VP...	SofaWare	5.0.43x	0	6220 KB	Firmware
SmartView Reporter	Win32	Check Point	NG_AI	R55	20027 KB	SmartView ...
SmartView Reporter	Win32	Check Point	R70		14848 KB	SmartView ...
SecurePlatform	SecurePlatf...	Check Point	R70		246255 KB	SecurePlatf...
Security Gateway	Win32	Check Point	R70		29113 KB	Security Ga...
Security Gateway	Linux	Check Point	R70		53793 KB	Security Ga...

Operation Status

Operation	Status	Progress	Time

Done.

Figure 1: SmartUpdate - Packages Tab


*localdb - Check Point SmartUpdate
File View Tree Packages Licenses & Contracts Operations Tools Window Help
Packages
Licenses & Contracts
License Management
Operation Status
Operation
Status
Progress
Done.

Machines	IP Address	Version	State	SKU	Description	Expiration D...	Has Conta...
*localdb							
Connectra_London_R66	66.66.66.66	NGX					
Connectra_Paris_R62...	1.2.3.4	NGX					
Connectra-gw	191.1.2.3	NG					
Corporate-Cluster-1-me...	143.100.76.1	R70					
my license		NGX / R70		CP-SUITE-SAMPLE-LIC		12May2006	No
Corporate-Cluster-1-me...	143.100.76.2	R70					
my license 2		NGX / R70		CP-SUITE-SAMPLE-LIC		30Jan2006	No
Corporate-Cluster-2-me...	143.100.80.1	R70					
license 5		NGX / R70		CPMP-MEDIA-1-NGX		19Apr2006	No
Corporate-Cluster-2-me...	143.100.80.2	R70					
Corporate-gw	143.100.75.1	R70					
license 2		NGX / R70		CPMP-MEDIA-1-NGX		09Mar2005	No
CPMP-SCPRO-U-...		NGX / R70		CPMP-SCPRO-U-NGX		never	Yes
CPMP-VPG-25-NG...		NGX / R70		CPMP-VPG-25-NGX CPMP-...		never	Yes
Corporate-internal-termi...	172.16.1.10	NGX					
Corporate-WA-proxy-s...	172.16.2.3	NGX					
eval license		NG	Requires U...			8Feb2006	No
Endpoint-1	10.14.1.132	NGX					
GX	10.200.0.0	NGX					
Management	143.29.47.78	R70					
night license		NG	Requires U...	CPMP-MEDIA-1-NG		11May2006	No
Management-b	172.16.1.201	NGX					
Remote_branch_gw	198.95.100...	NG					
Remote-1-gw	198.75.100.1	R70					
Remote-1-web-server	192.168.2.2	NGX					
Remote-2-gw	205.50.200.1	NGX					
Remote-2-windows-do...	10.0.2.10	NGX					
Remote-3-gw	100.75.25.1	NGX					
Remote-4-gw	75.125.100.1	NGX					

Figure 1: SmartUpdate - Licenses & Contracts Tab

A. Installation status pane
B. Repository Management
C. Operation status Pane
D. Packages Management
E. License Management

Answer: C

QUESTION NO: 80

Packet filter can inspect packets up to the network layer of the OSI model. Choose the statement that is true of the upper four layers of the OSI model.

A. The upper four layers are left examined and disallow packets into internal network on these layers.
B. The upper four layers are left examined and Packet filter allows packets into internal network on these layers.
C. The upper four layers are left unexamined and Packet filter allows packets into internal network on these layers.

D. The packets are forced into lower three layers and hence, examined.
E. The upper four layers are left unexamined and Packet filter disallows packets into internal network on these layers.

Answer: C

QUESTION NO: 81

When upgrading ClusterXL, which of the following options will you choose if network activity is required during the upgrade process?

A. Maximum Effort Upgrade
B. Minimal Effort Upgrade
C. Zero Downtime
D. Full Connectivity Upgrade
E. Full Downtime

Answer: C

QUESTION NO: 82

To install and activate the R70 package on IPSO, what command will you run?

A. patch add cd
B. cpconfig
C. cpinfo
D. UnixInstallScript
E. newpkg

Answer: E

QUESTION NO: 83

Which of the following is true regarding Security servers?

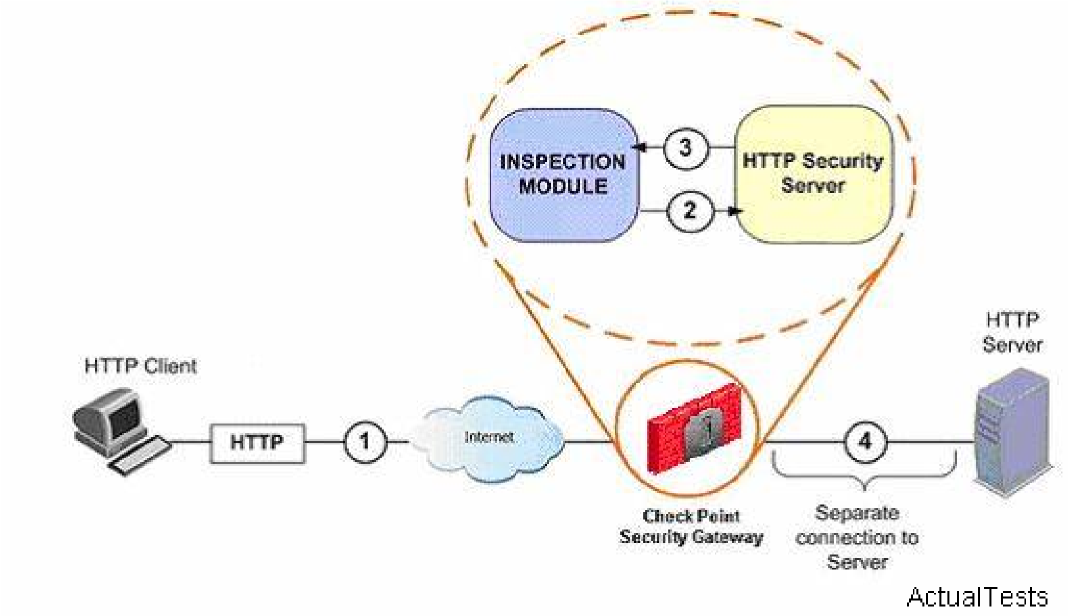


Figure 1: How the Security Server Mediates a Connection

A. Security servers can only provide content security for TCP
B. Security servers can perform authentication
C. Security servers do provide content security for HTTP, SMTP and FTP
D. Security servers can perform NAT
E. Security servers are processes that are integrated into the firewall

Answer: B,C,E

QUESTION NO: 84

The three VPN Components are:

A. VPN Management tools
B. VPN trust entities
C. VPN Tunnel
D. VPN Domain
E. VPN endpoints

Answer: A,B,E

QUESTION NO: 85

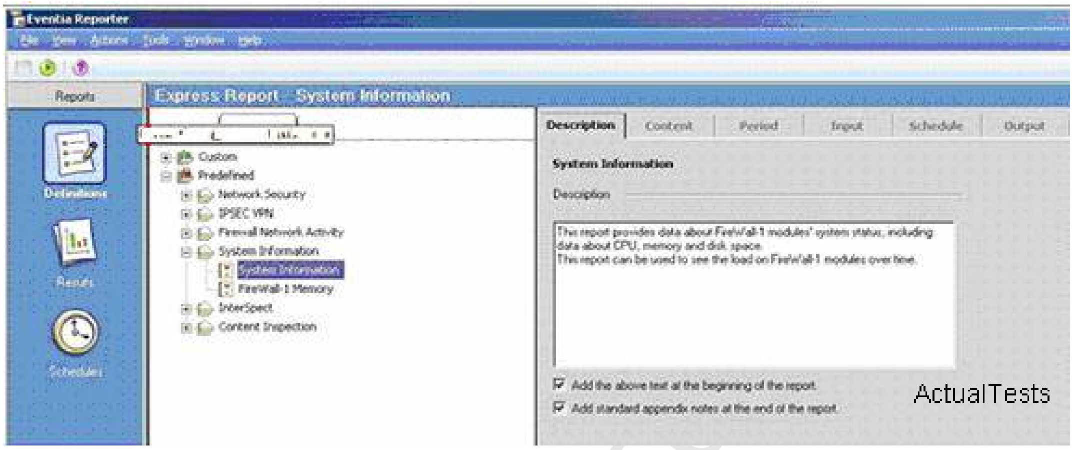
What answer below list the steps for setting up anti-virus inspection? a) define a CVP server (b) define rules in the rule base that specify the action to be taken on connections that invoke each resource (c) define a resource object (d) create a network object representing the IP address of the CVP server

A. d,a,b,c
B. a,c,b,d
C. d,c,b,a
D. d,b,a,c
E. d,a,c,b

Answer: E

QUESTION NO: 86

Which page would you switch to within Eventia reporter (in Express tab) when seeking reports that provides data about gateway system status, including data about CPU, memory and disk space?



System Information

Description

This report provides data about FireWall-1 modules' system status, including data about CPU, memory and disk space.
This report can be used to see the load on FireWall-1 modules over time.

☑ Add the above text at the beginning of the report.
☑ Add standard appendix notes at the end of the report.

Figure 1: Eventia Reporter

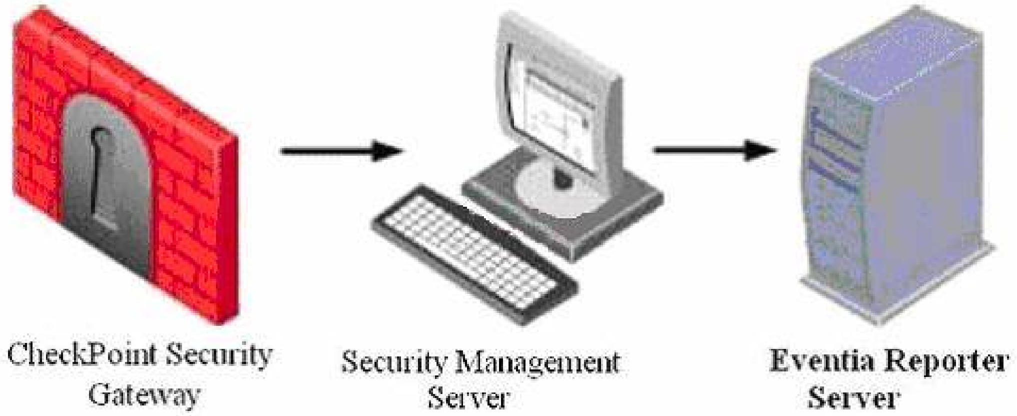


Figure 2: Eventia Reporter Express Report Architecture

A. VPN

B. Network Activity
C. Security
D. InterSpect
E. System Information

Answer: E

QUESTION NO: 87

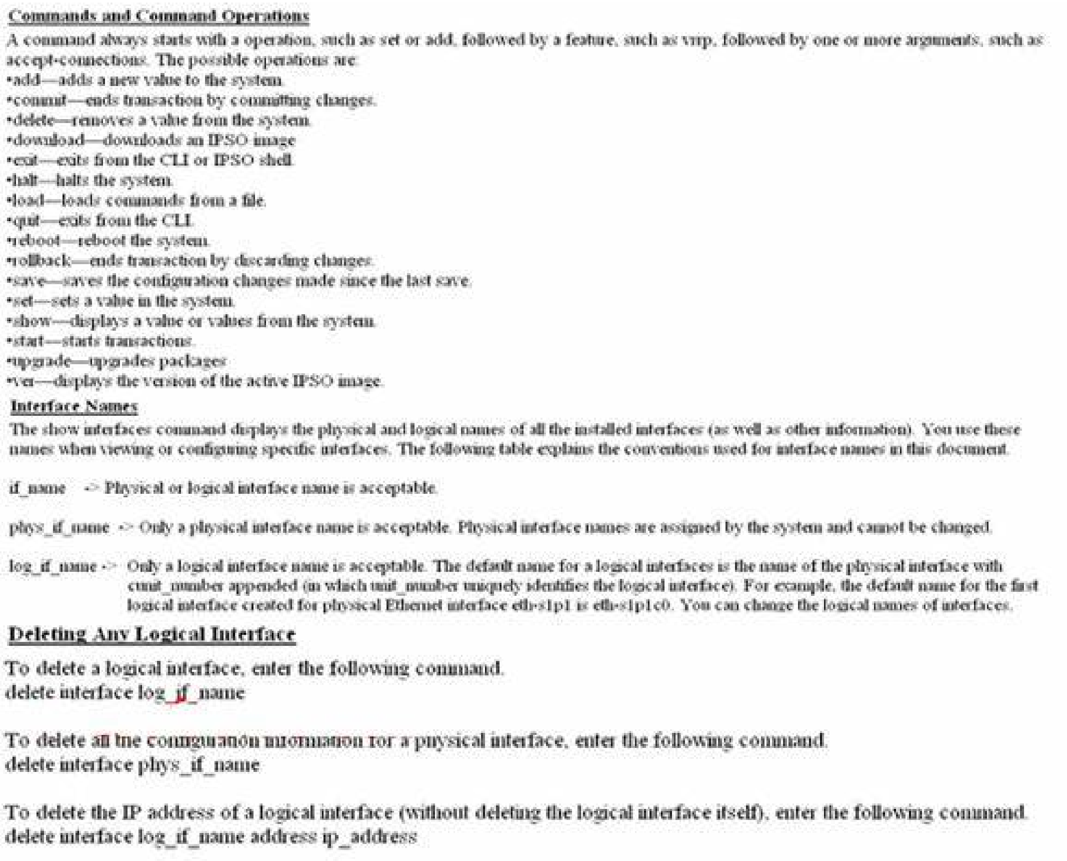
Working in SecurePlatform, what mode would you switch to if you exit from Expert Mode?

A. Administrator
B. Custom
C. Standard
D. host
E. Genius

Answer: C

QUESTION NO: 88

To see a variety of information about all the interfaces in a system, you will use the command:



Commands and Command Operations

A command always starts with a operation, such as set or add, followed by a feature, such as vrrp, followed by one or more arguments, such as accept-connections. The possible operations are:

•add—adds a new value to the system.
•commit—ends transaction by committing changes.
•delete—removes a value from the system.
•download—downloads an IPSO image
•exit—exits from the CLI or IPSO shell.
•halt—halts the system.
•load—loads commands from a file.
•quit—exits from the CLI.
•reboot—reboot the system.
•rollback—ends transaction by discarding changes.
•save—saves the configuration changes made since the last save.
•set—sets a value in the system.
•show—displays a value or values from the system.
•start—starts transactions.
•upgrade—upgrades packages
•ver—displays the version of the active IPSO image.

Interface Names

The show interfaces command displays the physical and logical names of all the installed interfaces (as well as other information). You use these names when viewing or configuring specific interfaces. The following table explains the conventions used for interface names in this document.

if_name -> Physical or logical interface name is acceptable.

phys_if_name -> Only a physical interface name is acceptable. Physical interface names are assigned by the system and cannot be changed.

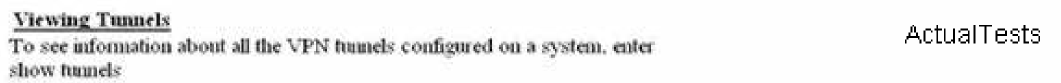
log_if_name -> Only a logical interface name is acceptable. The default name for a logical interfaces is the name of the physical interface with cunit_number appended (in which unit_number uniquely identifies the logical interface). For example, the default name for the first logical interface created for physical Ethernet interface eth-s1p1 is eth-s1p1c0. You can change the logical names of interfaces.

Deleting Any Logical Interface

To delete a logical interface, enter the following command.
delete interface log_if_name

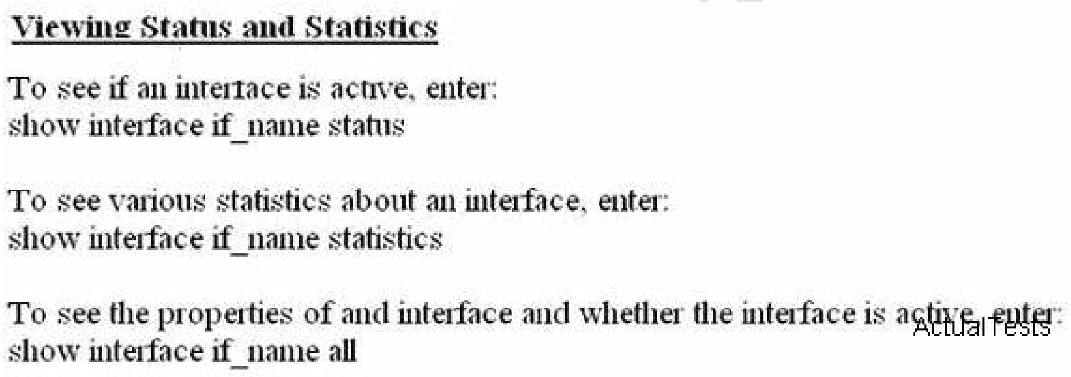
To delete all the configuration information for a physical interface, enter the following command.
delete interface phys_if_name

To delete the IP address of a logical interface (without deleting the logical interface itself), enter the following command.
delete interface log_if_name address ip_address



Viewing Tunnels

To see information about all the VPN tunnels configured on a system, enter
show tunnels

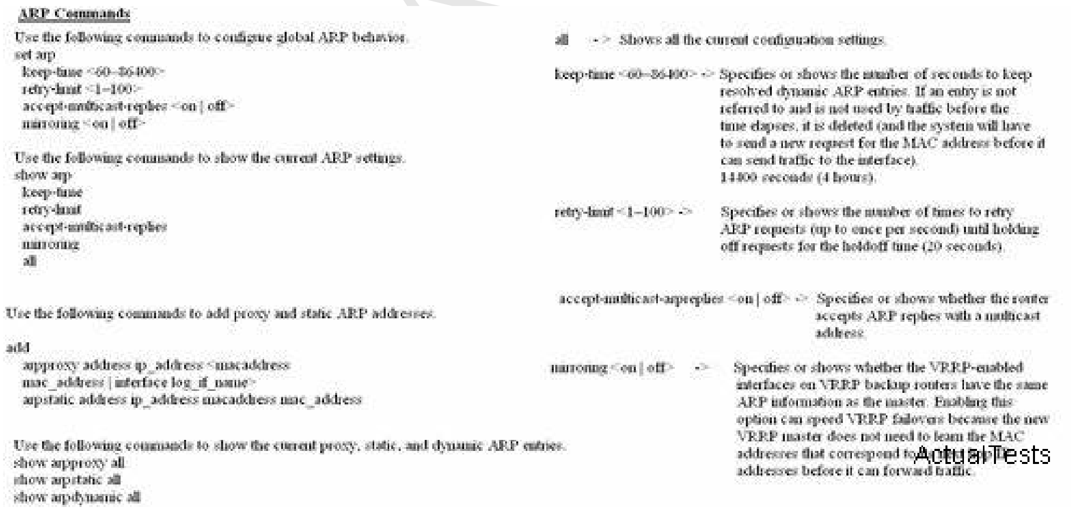


Viewing Status and Statistics

To see if an interface is active, enter:
show interface if_name status

To see various statistics about an interface, enter:
show interface if_name statistics

To see the properties of and interface and whether the interface is active, enter:
show interface if_name all



ARP Commands

Use the following commands to configure global ARP behavior.

```
set arp
  keep-time <60–86400>
  retry-limit <1–100>
  accept-multicast-replies <on | off>
  mirroring <on | off>
```

Use the following commands to show the current ARP settings.

```
show arp
  keep-time
  retry-limit
  accept-multicast-replies
  mirroring
  all
```

Use the following commands to add proxy and static ARP addresses.

```
add
   arpproxy address ip_address <macaddress
   mac_address | interface log_if_name>
   arpstatic address ip_address macaddress mac_address
```

Use the following commands to show the current proxy, static, and dynamic ARP entries.

```
show arpproxy all
show arpstatic all
show arpdynamic all
```

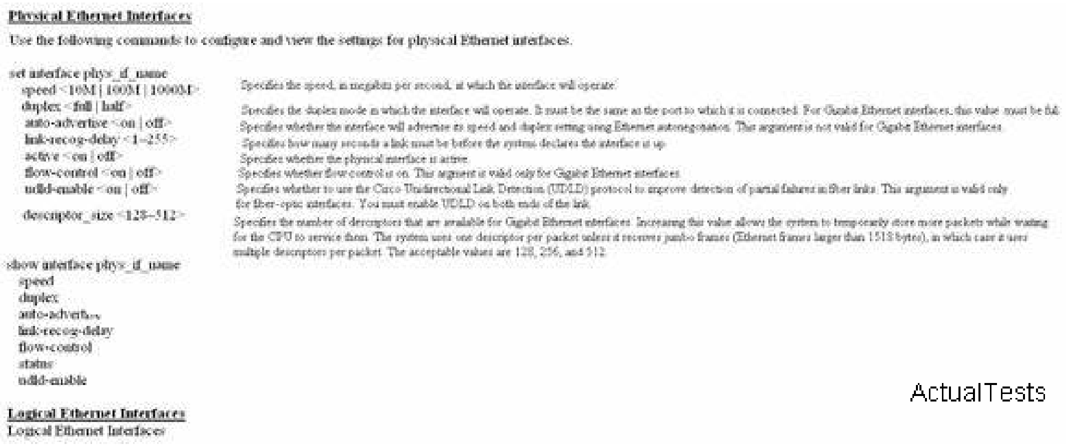
all -> Shows all the current configuration settings.

keep-time <60–86400> -> Specifies or shows the number of seconds to keep resolved dynamic ARP entries. If an entry is not referred to and is not used by traffic before the time elapses, it is deleted (and the system will have to send a new request for the MAC address before it can send traffic to the interface).
14400 seconds (4 hours).

retry-limit <1–100> -> Specifies or shows the number of times to retry ARP requests (up to once per second) until holding off requests for the holdoff time (20 seconds).

accept-multicast-arpreplies <on | off> -> Specifies or shows whether the router accepts ARP replies with a multicast address.

mirroring <on | off> -> Specifies or shows whether the VRRP-enabled interfaces on VRRP backup routers have the same ARP information as the master. Enabling this option can speed VRRP failovers because the new VRRP master does not need to learn the MAC addresses that correspond to its neighbor IP addresses before it can forward traffic.



Physical Ethernet Interfaces

Use the following commands to configure and view the settings for physical Ethernet interfaces.

```
set interface phys_if_name
   speed <10M | 100M | 1000M>
   duplex <full | half>
   auto-advertise <on | off>
   link-recog-delay <1–255>
   active <on | off>
   flow-control <on | off>
   udld-enable <on | off>

   descriptor_size <128–512>
```

Specifies the speed, in megabits per second, at which the interface will operate.

Specifies the duplex mode in which the interface will operate. It must be the same as the port to which it is connected. For Gigabit Ethernet interfaces, this value must be ful

Specifies whether the interface will advertise its speed and duplex setting using Ethernet autonegotiation. This argument is not valid for Gigabit Ethernet interfaces.

Specifies how many seconds a link must be before the system declares the interface is up.

Specifies whether the physical interface is active.

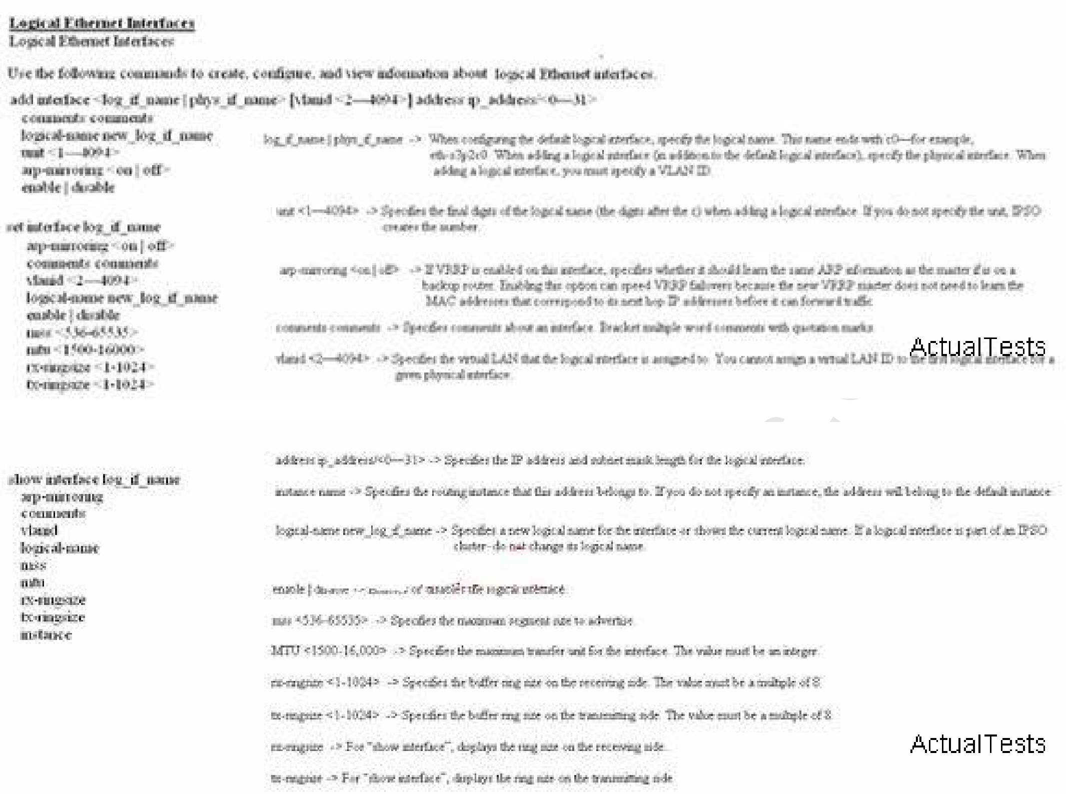
Specifies whether flow control is on. This argument is valid only for Gigabit Ethernet interfaces.

Specifies whether to use the Cisco Unidirectional Link Detection (UDLD) protocol to improve detection of partial failures in fiber links. This argument is valid only for fiber-optic interfaces. You must enable UDLD on both ends of the link.

Specifies the number of descriptors that are available for Gigabit Ethernet interfaces. Increasing this value allows the system to temporarily store more packets while waiting for the CPU to service them. The system uses one descriptor per packet unless it receives jumbo frames (Ethernet frames larger than 1518 bytes), in which case it uses multiple descriptors per packet. The acceptable values are 128, 256, and 512.

```
show interface phys_if_name
  speed
  duplex
  auto-advertise
  link-recog-delay
  flow-control
  status
  udld-enable
```

Logical Ethernet Interfaces
Logical Ethernet Interfaces



Logical Ethernet Interfaces
Logical Ethernet Interfaces

Use the following commands to create, configure, and view information about logical Ethernet interfaces.

```
add interface <log_if_name | phys_if_name> [vlanid <2—4094>] address ip_address/<0—31>
   comments comments
   logical-name new_log_if_name
   unit <1—4094>
   arp-mirroring <on | off>
   enable | disable

set interface log_if_name
    arp-mirroring <on | off>
    comments comments
    vlanid <2—4094>
    logical-name new_log_if_name
    enable | disable
    mss <536-65535>
    mtu <1500-16000>
    rx-ringsize <1-1024>
    tx-ringsize <1-1024>
```

log_if_name | phys_if_name -> When configuring the default logical interface, specify the logical name. This name ends with c0—for example, eth-s3p2c0. When adding a logical interface (in addition to the default logical interface), specify the physical interface. When adding a logical interface, you must specify a VLAN ID.

unit <1—4094> -> Specifies the final digits of the logical name (the digits after the c) when adding a logical interface. If you do not specify the unit, IPSO creates the number.

arp-mirroring <on | off> -> If VRRP is enabled on this interface, specifies whether it should learn the same ARP information as the master if is on a backup router. Enabling this option can speed VRRP failovers because the new VRRP master does not need to learn the MAC addresses that correspond to its next hop IP addresses before it can forward traffic.

comments comments -> Specifies comments about an interface. Bracket multiple word comments with quotation marks.

vlanid <2—4094> -> Specifies the virtual LAN that the logical interface is assigned to. You cannot assign a virtual LAN ID to the first logical interface for a given physical interface.

```
show interface log_if_name
  arp-mirroring
  comments
  vlanid
  logical-name
  mss
  mtu
  rx-ringsize
  tx-ringsize
  instance
```

address ip_address/<0—31> -> Specifies the IP address and subnet mask length for the logical interface.

instance name -> Specifies the routing instance that this address belongs to. If you do not specify an instance, the address will belong to the default instance.

logical-name new_log_if_name -> Specifies a new logical name for the interface or shows the current logical name. If a logical interface is part of an IPSO cluster, do not change its logical name.

enable | disable -> Enables or disables the logical interface.

mss <536-65535> -> Specifies the maximum segment size to advertise.

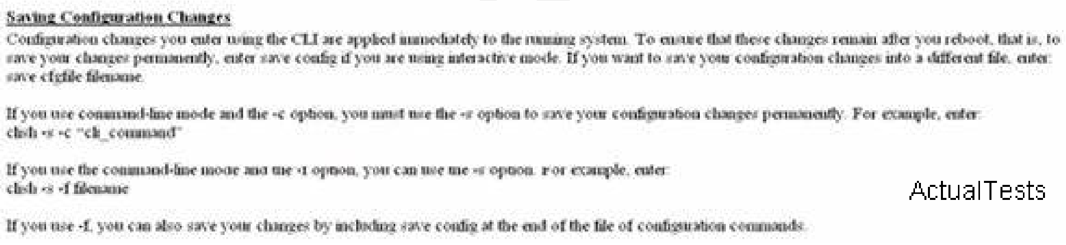
MTU <1500-16,000> -> Specifies the maximum transfer unit for the interface. The value must be an integer.

rx-ringsize <1-1024> -> Specifies the buffer ring size on the receiving side. The value must be a multiple of 8.

tx-ringsize <1-1024> -> Specifies the buffer ring size on the transmitting side. The value must be a multiple of 8.

rx-ringsize -> For "show interface", displays the ring size on the receiving side.

tx-ringsize -> For "show interface", displays the ring size on the transmitting side.



Saving Configuration Changes

Configuration changes you enter using the CLI are applied immediately to the running system. To ensure that these changes remain after you reboot, that is, to save your changes permanently, enter save config if you are using interactive mode. If you want to save your configuration changes into a different file, enter: save cfgfile filename.

If you use command-line mode and the -c option, you must use the -s option to save your configuration changes permanently. For example, enter:
clish -s -c "cli_command"

If you use the command-line mode and the -f option, you can use the -s option. For example, enter:
clish -s -f filename

If you use -f, you can also save your changes by including save config at the end of the file of configuration commands.

A. show interfaces

B. show info

C. display info

D. show config

E. display interfaces info

Answer: A

QUESTION NO: 89

The command "delete interface log_if_name" will delete a logical interface, then what command deletes a physical interface?

A. delete interface phys_if_name
B. delete interface_name
C. delete interface physical__name
D. delete interface phys_name
E. delete interface phys_if_pname

Answer: A

QUESTION NO: 90

What command will you use to save your configuration in order that the changes remain after you reboot, if the filename is configfile?

A. save cfgfile configfile
B. save cfgfile filename
C. save cfgfile
D. save filename
E. CLI save cfgfile

Answer: A

QUESTION NO: 91

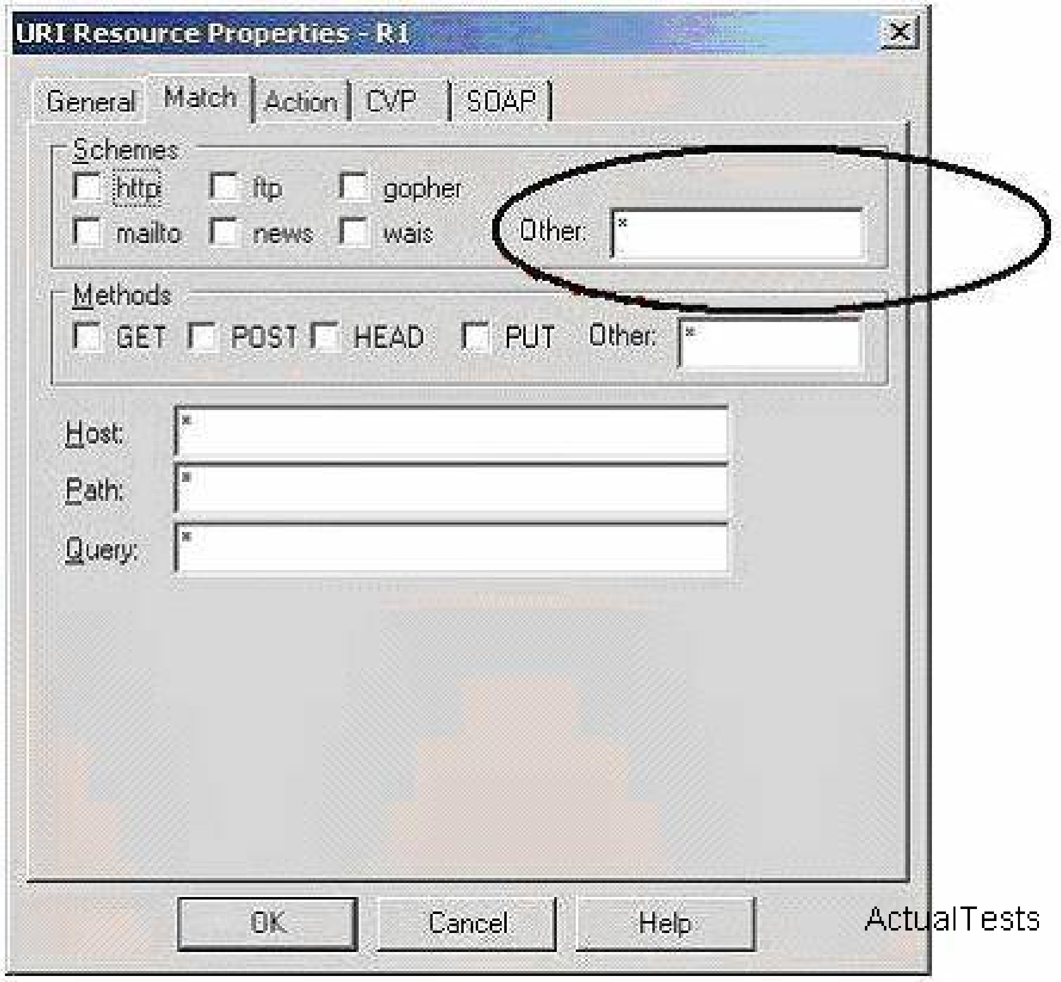
When upgrading Security Management server, the upgrade process checks to see whether a contract file is already present on the server. If not, then you can either download a contracts file from the User Center or:

A. Export a local contract file
B. Cancel the upgrade
C. Continue without contract information (download later using SmartUpdate)
D. Verify a local contract file on Security Management server
E. Import a local contract file

Answer: C,E

QUESTION NO: 92

In the URI Resource Properties window - Match tab, shown in the diagram. What will happen if you select type a wildcard in the box in circle?



Schemes
□ http □ ftp □ gopher
□ mailto □ news □ wais
Other: *

Methods
□ GET □ POST □ HEAD □ PUT Other: *

Host: *
Path: *
Query: *

A. This will mean that the resource cannot be used in the rulebase
B. This will indicate any host
C. This will mean that GET, POST, HEAD and PUT methods will be used
D. This will indicate URI schemes to which this Gateway resource applies
E. This will indicate the Rule Base will make special consideration for specified Resource

Answer: C

QUESTION NO: 93

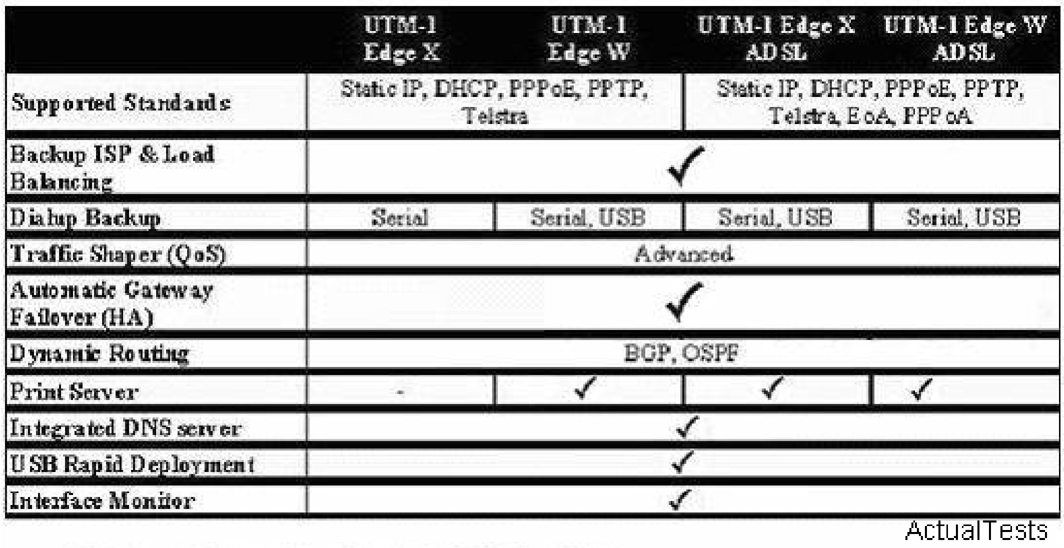
What types of NAT Modes are supported by CheckPoint Security Gateway?

A. Destination Static and Hide
B. Source Static and Hide
C. Static and Hide
D. Source Static and Destination Static
E. Hide

Answer: C

QUESTION NO: 94

Which of the following dynamic routing protocols are supported by UTM-1 Edge (regardless of the type)? Select all the correct answers.



	UTM-1 Edge X	UTM-1 Edge W	UTM-1 Edge X ADSL	UTM-1 Edge W ADSL
Supported Standards	Static IP, DHCP, PPPoE, PPTP, Telstra		Static IP, DHCP, PPPoE, PPTP, Telstra, EoA, PPPoA	
Backup ISP & Load Balancing	✓			
Dialup Backup	Serial	Serial, USB	Serial, USB	Serial, USB
Traffic Shaper (QoS)	Advanced			
Automatic Gateway Failover (HA)	✓			
Dynamic Routing	BGP, OSPF			
Print Server	-	✓	✓	✓
Integrated DNS server	✓			
USB Rapid Deployment	✓			
Interface Monitor	✓			

Figure 1: Networking Data for UTM-1 Edge

A. IS-IS

B. OSPF

C. BGP

D. RIP

E. EIGRP

Answer: B,C

QUESTION NO: 95

Your web server behind the security Gateway is configured to Automatic Static NAT. Client side NAT is enabled in the Global Properties. A client on the Internet initiates a session to the web server. On the initiating packet, NAT is likely to occur on which inspection point?

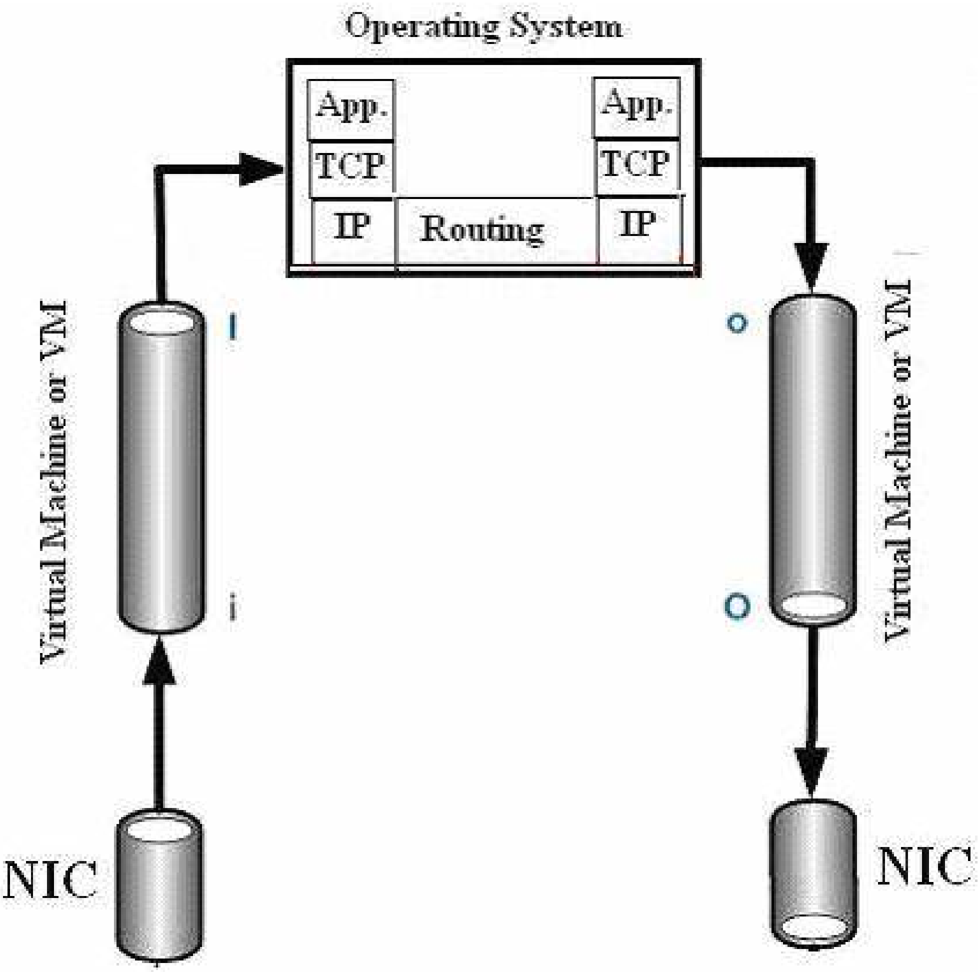
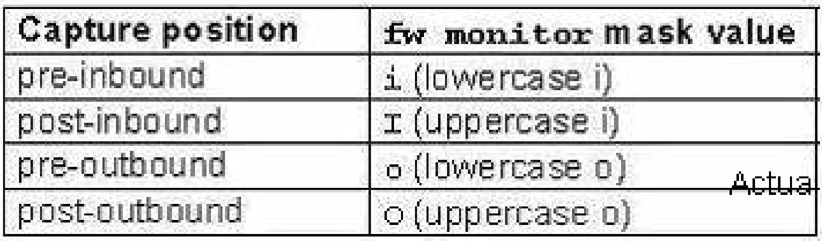


Figure 1

Table 1



Capture position	fw monitor mask value
pre-inbound	i (lowercase i)
post-inbound	I (uppercase i)
pre-outbound	o (lowercase o)
post-outbound	O (uppercase o)

A. I - Post inbound orBig I

B. o - Pre outbound or little o

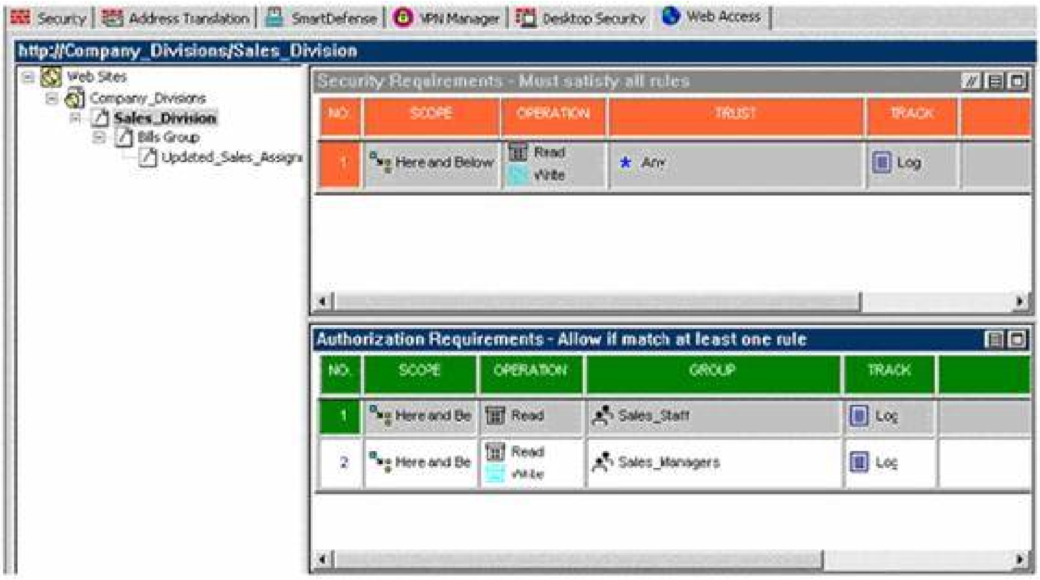
C. O - Post outbound or big O

D. i - Pre inbound or little i

Answer: C

QUESTION NO: 96

The diagram shows two authorization rules. John is a manager in the sales department of a medium-sized company. The first rule states that only Read access is granted to the Sales Staff Group and the second rule states that both Read and Write status can be granted to members of the Sales Managers Group. If John is a member of both groups, what privilege will be granted to him?



Security Requirements - Must satisfy all rules

NO.	SCOPE	OPERATION	TRUST	TRACK
1	Here and Below	Read Write	Any	Log

Authorization Requirements - Allow if match at least one rule

NO.	SCOPE	OPERATION	GROUP	TRACK
1	Here and Be	Read	Sales_Staff	Log
2	Here and Be	Read Write	Sales_Managers	Log

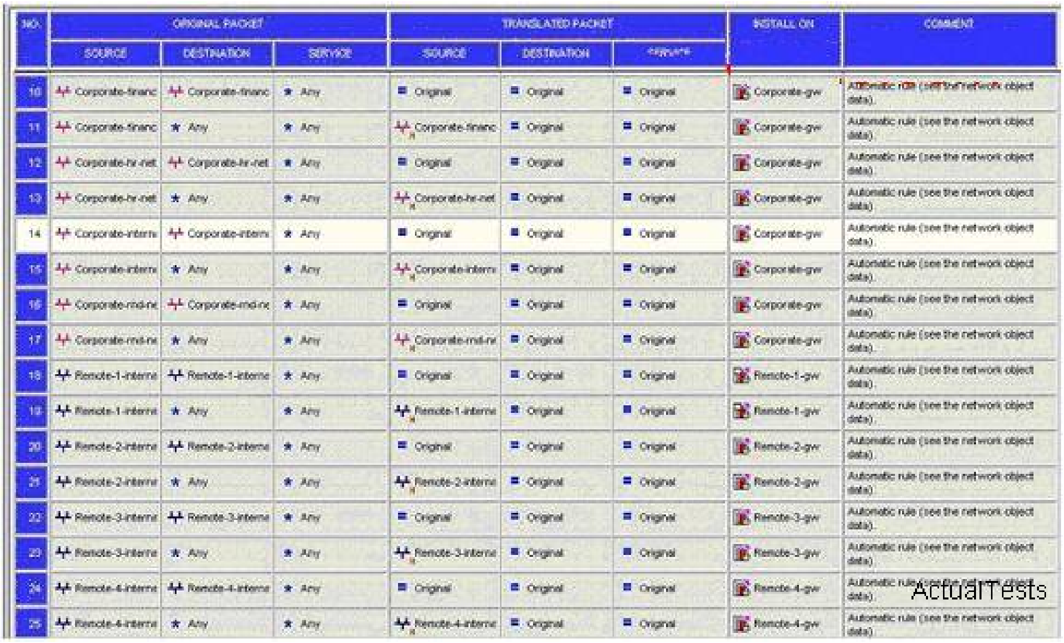
Figure 1: Security and Authorization rule

A. No access
B. Write
C. Read
D. Read and Write
E. Admin

Answer: D

QUESTION NO: 97

Each NAT rule consists of what three elements? Choose all the correct answers.



NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
10	Corporate-financ	Corporate-financ	★ Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data).
11	Corporate-financ	★ Any	★ Any	Corporate-financ	Original	Original	Corporate-gw	Automatic rule (see the network object data).
12	Corporate-hr-net	Corporate-hr-net	★ Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data).
13	Corporate-hr-net	★ Any	★ Any	Corporate-hr-net	Original	Original	Corporate-gw	Automatic rule (see the network object data).
14	Corporate-interni	Corporate-interni	★ Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data).
15	Corporate-interni	★ Any	★ Any	Corporate-interni	Original	Original	Corporate-gw	Automatic rule (see the network object data).
16	Corporate-rnd-ne	Corporate-rnd-ne	★ Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data).
17	Corporate-rnd-ne	★ Any	★ Any	Corporate-rnd-ne	Original	Original	Corporate-gw	Automatic rule (see the network object data).
18	Remote-1-interne	Remote-1-interne	★ Any	Original	Original	Original	Remote-1-gw	Automatic rule (see the network object data).
19	Remote-1-interne	★ Any	★ Any	Remote-1-interne	Original	Original	Remote-1-gw	Automatic rule (see the network object data).
20	Remote-2-interne	Remote-2-interne	★ Any	Original	Original	Original	Remote-2-gw	Automatic rule (see the network object data).
21	Remote-2-interne	★ Any	★ Any	Remote-2-interne	Original	Original	Remote-2-gw	Automatic rule (see the network object data).
22	Remote-3-interne	Remote-3-interne	★ Any	Original	Original	Original	Remote-3-gw	Automatic rule (see the network object data).
23	Remote-3-interne	★ Any	★ Any	Remote-3-interne	Original	Original	Remote-3-gw	Automatic rule (see the network object data).
24	Remote-4-interne	Remote-4-interne	★ Any	Original	Original	Original	Remote-4-gw	Automatic rule (see the network object data).
25	Remote-4-interne	★ Any	★ Any	Remote-4-interne	Original	Original	Remote-4-gw	Automatic rule (see the network object data).

A. Source
B. Destination
C. Policy
D. Action
E. Service

Answer: A,B,E

QUESTION NO: 98

Which of the following is the correct list of the key features of SmartView Monitor? Select all the correct answers.

A. Gateways
B. VPN
C. Tunnels
D. Traffic / Counters
E. Remote Users

Answer: A,C,D,E

QUESTION NO: 99

Querying rules can help you identify the most appropriate place for new rules. You can run queries on which of the following?

A. IPS

B. Access Rule Bases
C. Desktop Security
D. Security
E. NAT

Answer: B,C,D

QUESTION NO: 100

What SmartConsole client allows you to block or terminate any active connection from or to a specific IP address?

A. SmartDashboard
B. SmartView Status
C. RuleBase
D. Security Policy
E. SmartView Tracker

Answer: E

QUESTION NO: 101

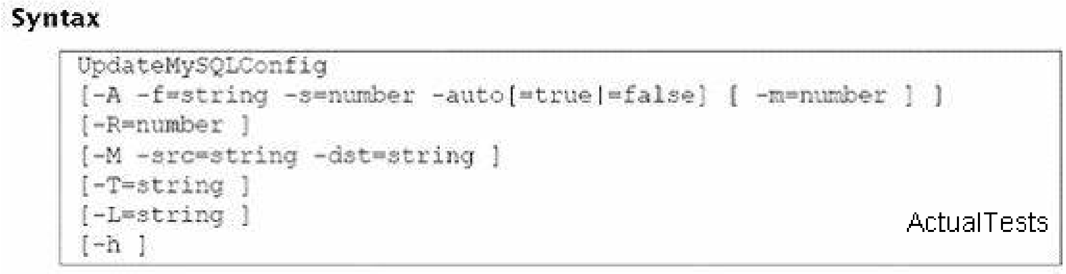
When dealing with IPSO clustering modes, which of the modes will you choose if you want each cluster node to receive every packet sent to the cluster system and decides whether to process it based on information it receives from the master node?

A. Multicast with IGMP mode
B. Multicast with IGMP
C. Multicast mode
D. Forwarding mode
E. Unicast mode

Answer: C

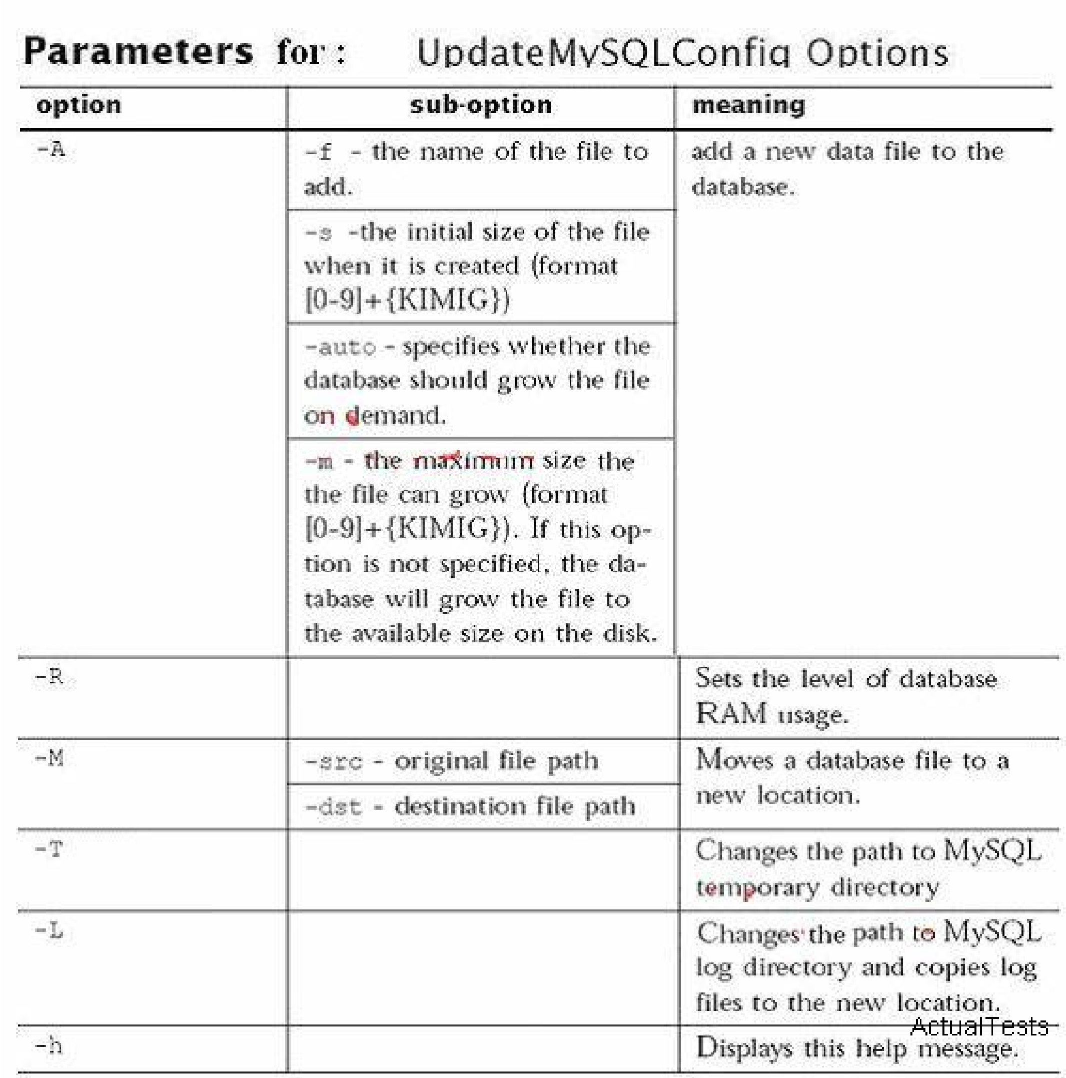
QUESTION NO: 102

Prior to changing Eventia Reporter Database settings using UpdateMySQLConfig application, you must stop all Eventia Reporter services. What command would you run in order to achieve this?



Syntax

```
UpdateMySQLConfig
[-A -f=string -s=number -auto[=true|=false] [ -m=number ] ]
[-R=number ]
[-M -src=string -dst=string ]
[-T=string ]
[-L=string ]
[-h ]
```



Parameters for : UpdateMySQLConfig Options

option	sub-option	meaning
-A	-f - the name of the file to add.	add a new data file to the database.
	-s -the initial size of the file when it is created (format [0-9]+{KIMIG})	
	-auto - specifies whether the database should grow the file on demand.	
	-m - the maximum size the the file can grow (format [0-9]+{KIMIG}). If this option is not specified, the database will grow the file to the available size on the disk.	
-R		Sets the level of database RAM usage.
-M	-src - original file path	Moves a database file to a new location.
	-dst - destination file path	
-T		Changes the path to MySQL temporary directory
-L		Changes the path to MySQL log directory and copies log files to the new location.
-h		Displays this help message.

A. cpstop

B. UpdateMySQLConfig

C. rmdstop

D. rmdstart

E. cpconfig

Answer: C

QUESTION NO: 103

In IPSO Directory structure, which of the following directory contains Checkpoint software package?

A. /opt

B. /config

C. /image

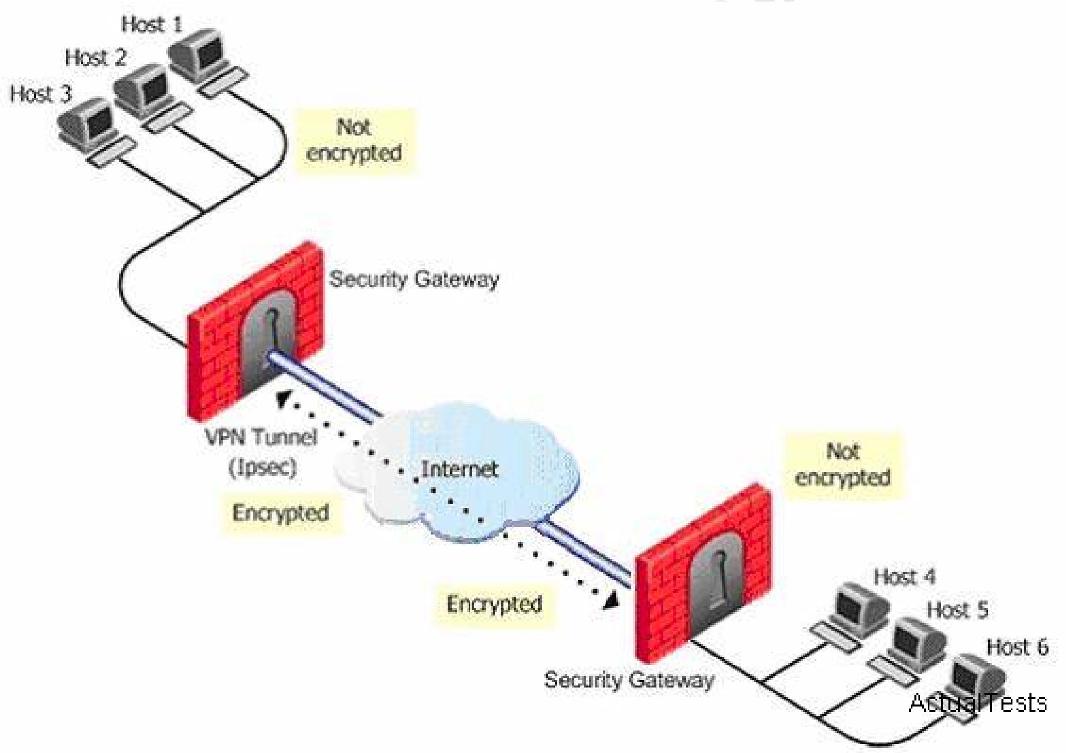
D. /etc

E. /var

Answer: A

QUESTION NO: 104

Your network configuration is shown in the diagram. Host 1 and host 6 need to communicate. A VPN tunnel is established in order that the communication can be encrypted. Which of the following are the correct steps of communication between host 1 and host 6 using the VPN tunnel? 1 A packet leaves the source host and reaches the gateway 2 The gateway encrypts the packet 3 The packet goes down the VPN tunnel to the second gateway. In actual fact, the packets are standard IP packets passing through the Internet. However, because the packets are encrypted, they can be considered as passing through a private "virtual" tunnel 4 The packet is delivered in the clear to the destination host. From the hosts perspective, they are connecting directly 5 The second gateway decrypts the packet



A. 1,2,3,4,5

B. 1,2,5,3,4

C. 1,2,5,4,3

D. 1,2,4,3,5

E. 1,2,3,5,4

Answer: E

QUESTION NO: 105

If the gateways use certificates, the certificates can be issued either by the Internal Certificate Authority (ICA) on the Security Management server, or by a:

A. External Server CA
B. Enforcement Module
C. Third party OPSEC certified CA
D. No Certificate Authority asideICA
E. SecurityGateway CA

Answer: C

QUESTION NO: 106

Which of the following is true regarding IPS Tuning Protections?

A. it is recommended to clone tuning management in order to minimize hard disk space
B. Apply all of the protections as a group to specific gateways
C. It is recommended to create separate profiles for different gateway location types
D. It is recommended to create the same profile for different gateway location types
E. it is recommended to apply different profiles for current gateways and for older Gateways

Answer: B,C,E

QUESTION NO: 107

IPSO file systems are based on which of the following file system type?

A. UFS
B. FAT
C. NTFS
D. FAT32
E. DOS

Answer: A

QUESTION NO: 108

In the RuleBase, which element determines what Firewall should do with a packet?

A. Destination
B. Source
C. Action
D. No
E. Service

Answer: C

QUESTION NO: 109

To distribute or upgrade a package, you must first add it to the Package Repository. You can add packages to the Package Repository from which of the following three locations?

A. User Center
B. Certificate Key
C. Check Point CD
D. Download Center
E. SmartDashboard

Answer: A,C,D

QUESTION NO: 110

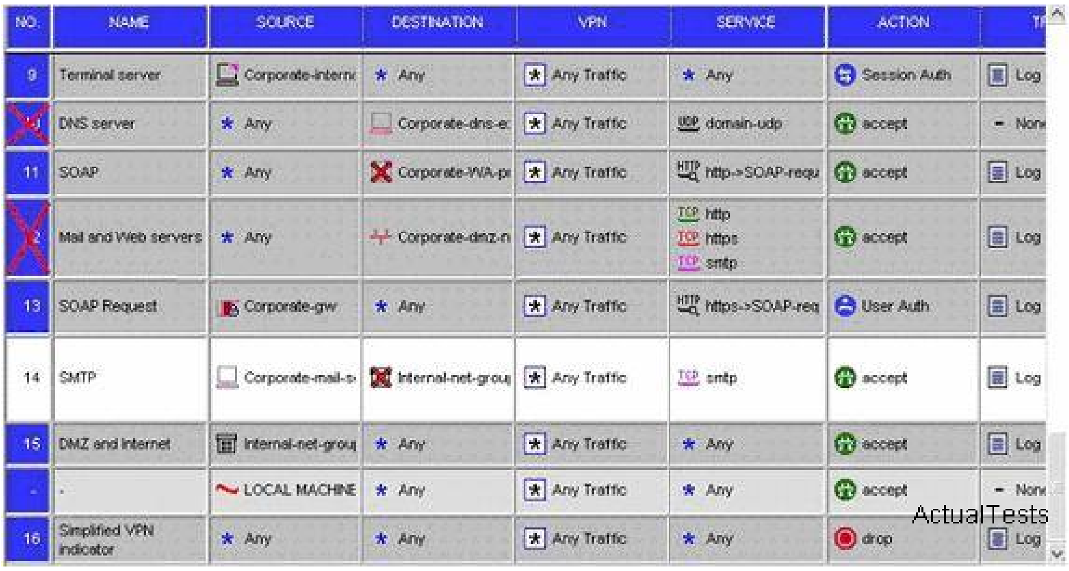
How will you install a rule base? Choose the best answer.

A. After defining your rules inSmartDashboard , choose install from File menu
B. After defining your rules in SmartDashboard, choose Install from Policy menu
C. Before defining your rules inSmartDashboard , choose Install from View menu
D. After defining your rules in SmartDashboard, choose Install from View menu
E. Before defining your rules inSmartDashboard , choose Install from Policy menu

Answer: B

QUESTION NO: 111

How would you disable a rule?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TI
9	Terminal server	Corporate-interne	* Any	Any Traffic	* Any	Session Auth	Log
10	DNS server	* Any	Corporate-dns-e	Any Traffic	UDP domain-udp	accept	- None
11	SOAP	* Any	Corporate-WA-p	Any Traffic	HTTP http->SOAP-requ	accept	Log
12	Mail and Web servers	* Any	Corporate-dmz-n	Any Traffic	TCP http TCP https TCP smtp	accept	Log
13	SOAP Request	Corporate-gw	* Any	Any Traffic	HTTP https->SOAP-req	User Auth	Log
14	SMTP	Corporate-mail-s	Internal-net-grou	Any Traffic	TCP smtp	accept	Log
15	DMZ and Internet	Internal-net-grou	* Any	Any Traffic	* Any	accept	Log
-	-	LOCAL MACHINE	* Any	Any Traffic	* Any	accept	- None
16	Simplified VPN indicator	* Any	* Any	Any Traffic	* Any	drop	Log

A. By selecting the rule, then select "Disable Rule" option from Topology menu in CheckPoint SmartDashboard

B. By selecting the rule, then select "Disable Rule" option from Rules menu in SmartView Tracker

C. By selecting the rule, then select "Disable Rule" option from Rules menu in CheckPoint SmartDashboard

D. By selecting the rule, then select "Disable Rule" option from File menu in CheckPoint SmartDashboard

E. By selecting the rule, then select "Disable Rule" option from Rules menu in SmartView Status

Answer: C

QUESTION NO: 112

Which of the options below best describes the difference between the Drop action and Reject action? (assume TCP is specified in the service column of your rulebase)

A. Drop action is the same as Reject action

B. With Drop action, the sender is not notified but with Reject action, the user is notified

C. Reject action is the same as Drop action

D. With Drop action, the sender is authenticated but with Reject action, the user is not authenticated

E. With Drop action, the sender is notified but with Reject action, the user is not Notified

Answer: B

QUESTION NO: 113

Your company has headquarters in two countries: Toronto (Canada) and Washington (USA). Each headquarter has a number of branch offices. The branch offices only need to communicate with the headquarter in their country, not with each other i.e. no branch office should communicate with another branch office.

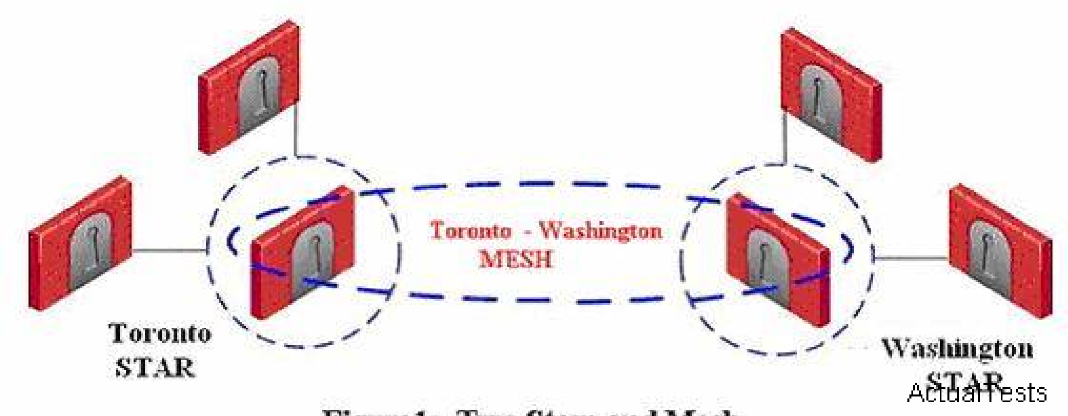


Figure1: Two Stars and Mesh

A. You need to define two stars and a mesh
B. You need to define a star and two meshes
C. You need to define two stars and twomesh
D. You need to define three stars and two meshes
E. You need to define a star and a mesh

Answer: A

QUESTION NO: 114

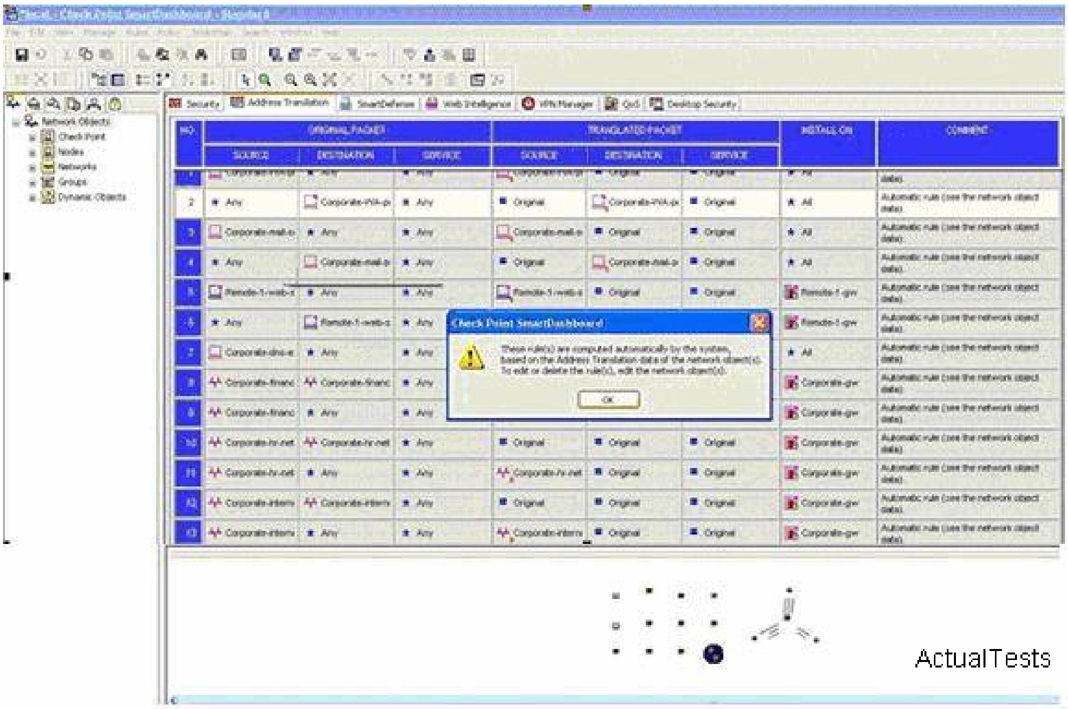
The negotiation prior to the establishment of a VPN tunnel might result in the production of large packets. Some NAT devices may not fragment large packets correctly making the connection impossible. Which of the following is true as to the resolving this issue?

A. IKE over TCP can be used to solve the problem, though this problem is resolved during IKE phase 2
B. If using NAT-T, you can use Aggressive Mode
C. UDP Encapsulation method uses port number 2746 to resolve this problem
D. If using NAT-T, port 4500 must be enabled
E. IKE over TCP can be used to solve the problem, though this problem is resolved during IKE phase I

Answer: C,D,E

QUESTION NO: 115

How can you delete an automatic NAT rule? See the diagram if you choose wrong answer.



NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	[illegible]	Any	Any	[illegible]	Original	Original	All	data)
2	Any	Corporate-IWA-p	Any	Original	Corporate-IWA-p	Original	All	Automatic rule (see the network object data)
3	Corporate-mail-s	Any	Any	Corporate-mail-s	Original	Original	All	Automatic rule (see the network object data)
4	Any	Corporate-mail-s	Any	Original	Corporate-mail-s	Original	All	Automatic rule (see the network object data)
5	Remote-1-web-s	Any	Any	Remote-1-web-s	Original	Original	Remote-1-gw	Automatic rule (see the network object data)
6	Any	Remote-1-web-s	Any				Remote-1-gw	Automatic rule (see the network object data)
7	Corporate-dns-s	Any	Any				All	Automatic rule (see the network object data)
8	Corporate-financ	Corporate-financ	Any				Corporate-gw	Automatic rule (see the network object data)
9	Corporate-financ	Any	Any				Corporate-gw	Automatic rule (see the network object data)
10	Corporate-hr-net	Corporate-hr-net	Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data)
11	Corporate-hr-net	Any	Any	Corporate-hr-net	Original	Original	Corporate-gw	Automatic rule (see the network object data)
12	Corporate-interns	Corporate-interns	Any	Original	Original	Original	Corporate-gw	Automatic rule (see the network object data)
13	Corporate-interns	Any	Any	Corporate-interns	Original	Original	Corporate-gw	Automatic rule (see the network object data)

Check Point SmartDashboard

These rule(s) are computed automatically by the system, based on the Address Translation data of the Network object(s). To edit or delete the rule(s), edit the network object(s).

OK

A. By highlighting the rule, click on Rules menu and select delete

B. By highlighting the rule and hitDelete button on your keyboard

C. By highlighting the rule, right-click and select Delete option from the emerging menu

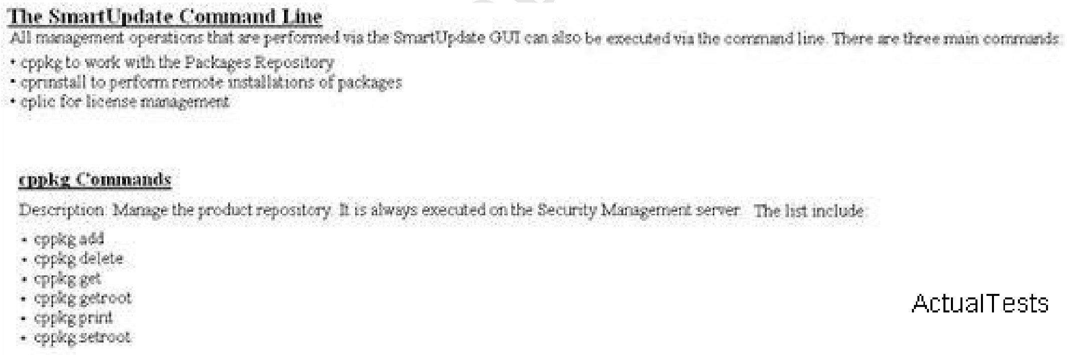
D. By highlighting the rule, click on Edit menu and select delete

E. By modifying the object's configuration

Answer: E

QUESTION NO: 116

The SmartUpdate command line "cprinstall get" will:


ActualTests

The SmartUpdate Command Line

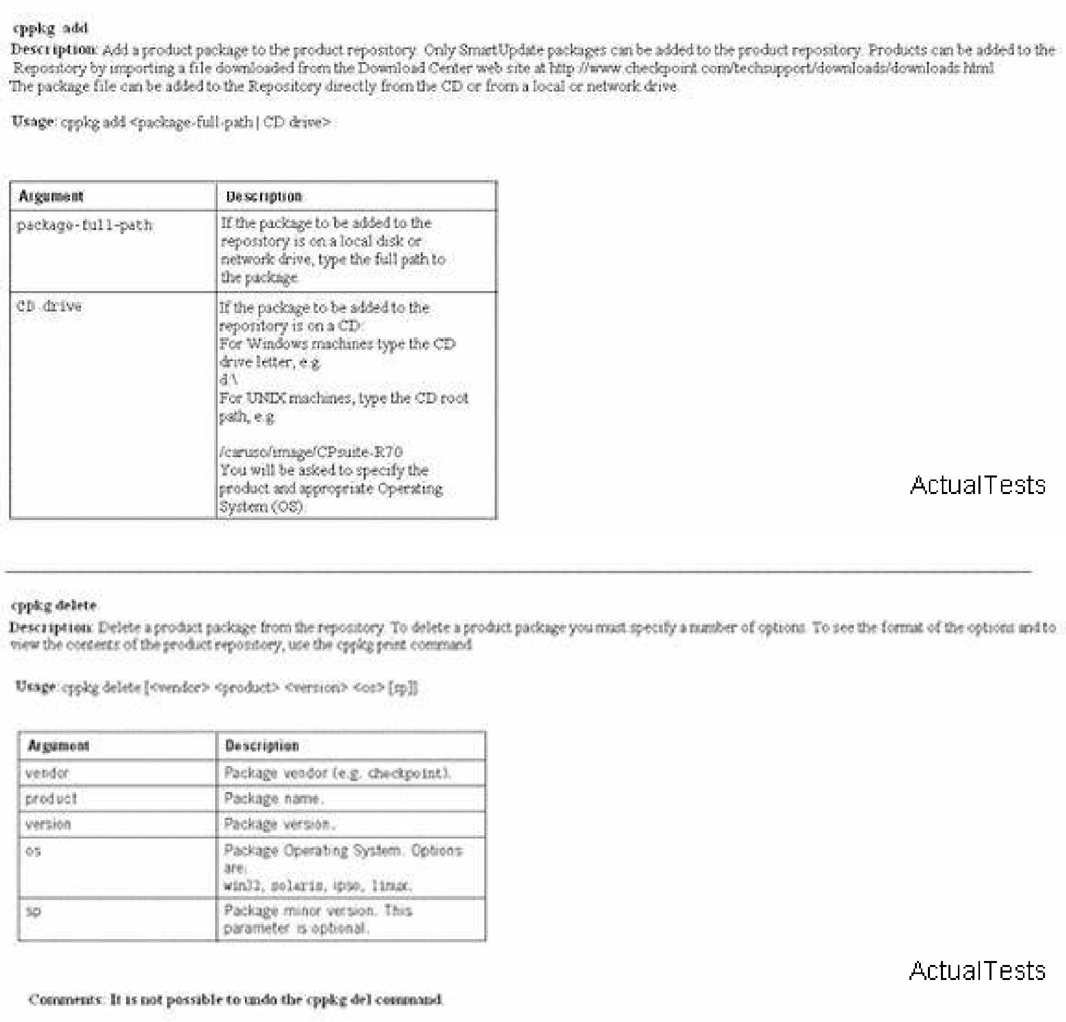
All management operations that are performed via the SmartUpdate GUI can also be executed via the command line. There are three main commands:

- cppkg to work with the Packages Repository
- cprinstall to perform remote installations of packages
- cplic for license management

cppkg Commands

Description: Manage the product repository. It is always executed on the Security Management server. The list include:

- cppkg add
- cppkg delete
- cppkg get
- cppkg getroot
- cppkg print
- cppkg setroot



cppkg add

Description: Add a product package to the product repository. Only SmartUpdate packages can be added to the product repository. Products can be added to the Repository by importing a file downloaded from the Download Center web site at http://www.checkpoint.com/techsupport/downloads/downloads.html
The package file can be added to the Repository directly from the CD or from a local or network drive.

Usage: cppkg add <package-full-path | CD drive>

Argument	Description
package-full-path	If the package to be added to the repository is on a local disk or network drive, type the full path to the package.
CD drive	If the package to be added to the repository is on a CD: For Windows machines type the CD drive letter, e.g. d:\ For UNIX machines, type the CD root path, e.g. /caruso/image/CPsuite-R70 You will be asked to specify the product and appropriate Operating System (OS).

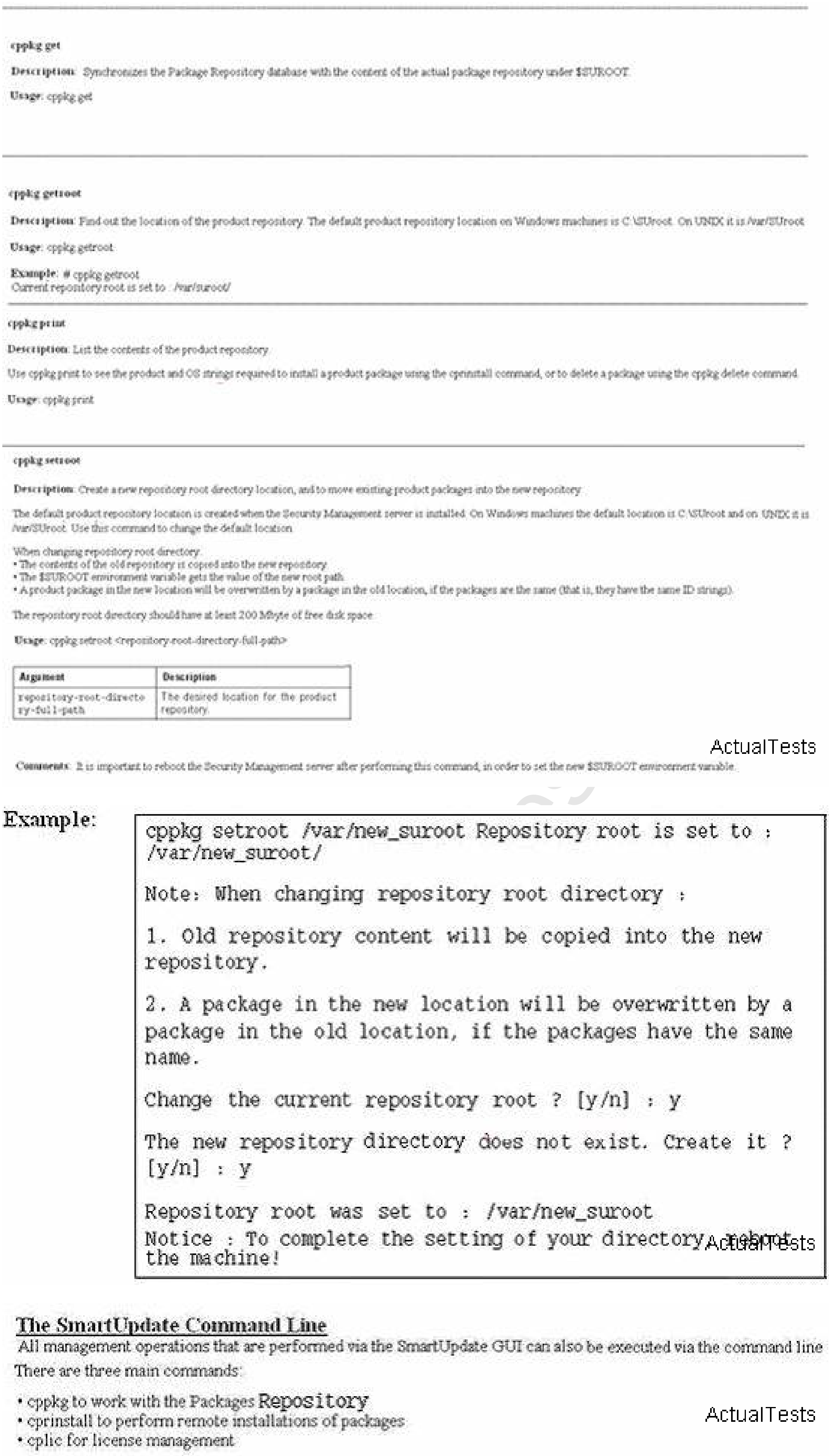
cppkg delete

Description: Delete a product package from the repository. To delete a product package you must specify a number of options. To see the format of the options and to view the contents of the product repository, use the cppkg print command.

Usage: cppkg delete [<vendor> <product> <version> <os> [sp]]

Argument	Description
vendor	Package vendor (e.g. checkpoint).
product	Package name.
version	Package version.
os	Package Operating System. Options are: win32, solaris, ipso, linux.
sp	Package minor version. This parameter is optional.

Comments: It is not possible to undo the cppkg del command.



cppkg get

Description: Synchronizes the Package Repository database with the content of the actual package repository under $SUROOT.

Usage: cppkg get

cppkg getroot

Description: Find out the location of the product repository. The default product repository location on Windows machines is C:\SUroot. On UNIX it is /var/SUroot

Usage: cppkg getroot

Example: # cppkg getroot
Current repository root is set to : /var/suroot/

cppkg print

Description: List the contents of the product repository.

Use cppkg print to see the product and OS strings required to install a product package using the cprinstall command, or to delete a package using the cppkg delete command.

Usage: cppkg print

cppkg setroot

Description: Create a new repository root directory location, and to move existing product packages into the new repository.

The default product repository location is created when the Security Management server is installed. On Windows machines the default location is C:\SUroot and on UNIX it is /var/SUroot. Use this command to change the default location.

When changing repository root directory:
- The contents of the old repository is copied into the new repository.
- The $SUROOT environment variable gets the value of the new root path.
- A product package in the new location will be overwritten by a package in the old location, if the packages are the same (that is, they have the same ID strings).

The repository root directory should have at least 200 Mbyte of free disk space.

Usage: cppkg setroot <repository-root-directory-full-path>

Argument	Description
repository-root-directory-full-path	The desired location for the product repository.

Comments: It is important to reboot the Security Management server after performing this command, in order to set the new $SUROOT environment variable.

Example:

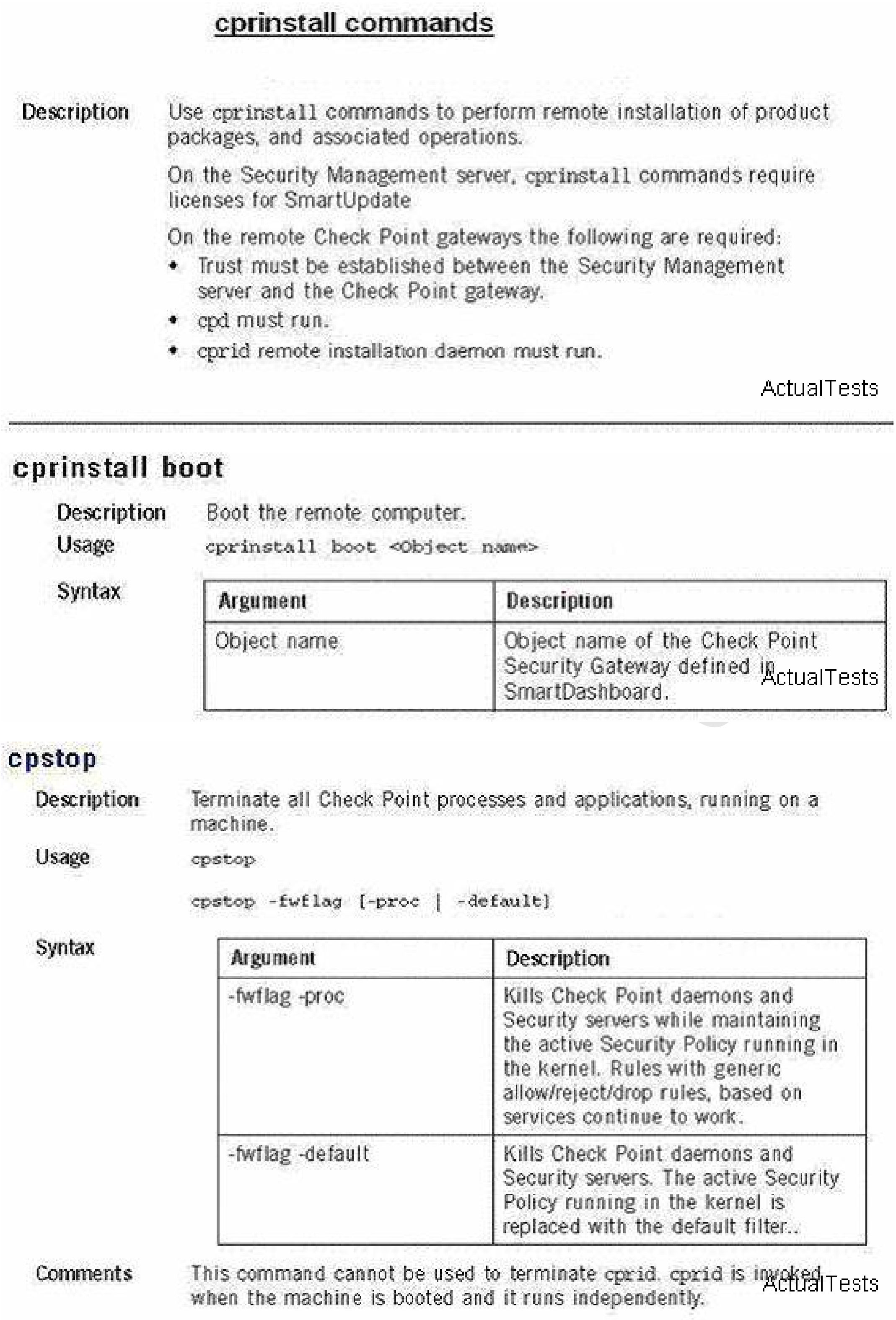
```
cppkg setroot /var/new_suroot Repository root is set to :
/var/new_suroot/

Note: When changing repository root directory :

1. Old repository content will be copied into the new
repository.

2. A package in the new location will be overwritten by a
package in the old location, if the packages have the same
name.

Change the current repository root ? [y/n] : y

The new repository directory does not exist. Create it ?
[y/n] : y

Repository root was set to : /var/new_suroot
Notice : To complete the setting of your directory, reboot
the machine!
```

The SmartUpdate Command Line

All management operations that are performed via the SmartUpdate GUI can also be executed via the command line.

There are three main commands:

- cppkg to work with the Packages Repository
- cprinstall to perform remote installations of packages
- cplic for license management



cprinstall commands

Description

Use `cprinstall` commands to perform remote installation of product packages, and associated operations.

On the Security Management server, `cprinstall` commands require licenses for SmartUpdate

On the remote Check Point gateways the following are required:

- Trust must be established between the Security Management server and the Check Point gateway.
- cpd must run.
- cprid remote installation daemon must run.

cprinstall boot

Description Boot the remote computer.

Usage `cprinstall boot <Object name>`

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.

cpstop

Description Terminate all Check Point processes and applications, running on a machine.

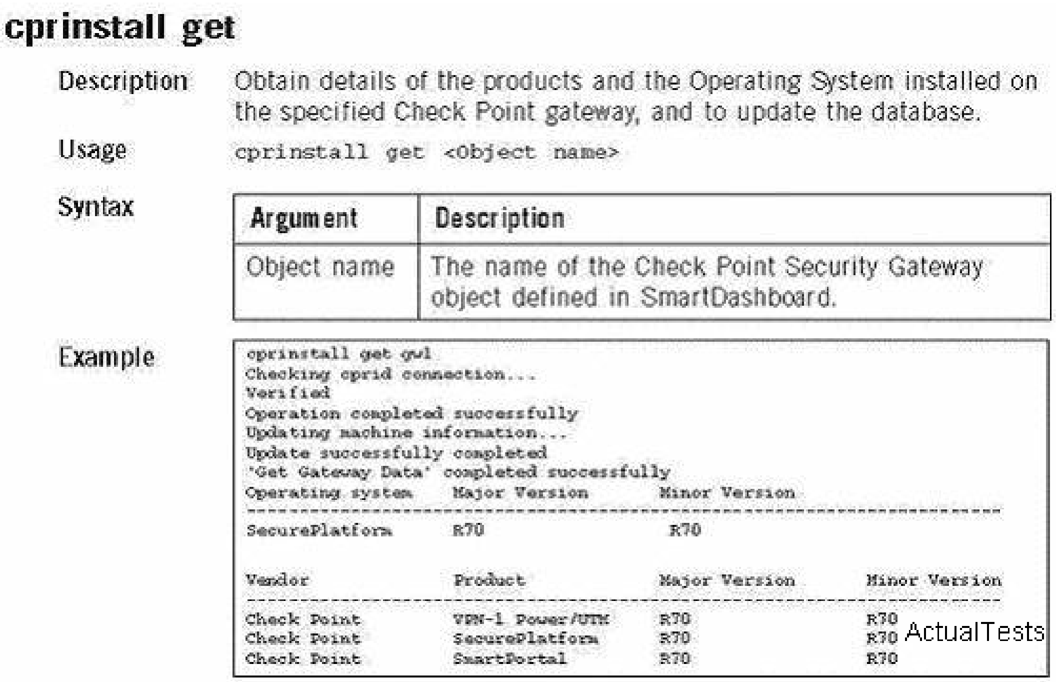
Usage

```
cpstop

cpstop -fwflag [-proc | -default]
```

Syntax

Argument	Description
-fwflag -proc	Kills Check Point daemons and Security servers while maintaining the active Security Policy running in the kernel. Rules with generic allow/reject/drop rules, based on services continue to work.
-fwflag -default	Kills Check Point daemons and Security servers. The active Security Policy running in the kernel is replaced with the default filter..

Comments This command cannot be used to terminate cprid. cprid is invoked when the machine is booted and it runs independently.



cprinstall get

Description Obtain details of the products and the Operating System installed on the specified Check Point gateway, and to update the database.

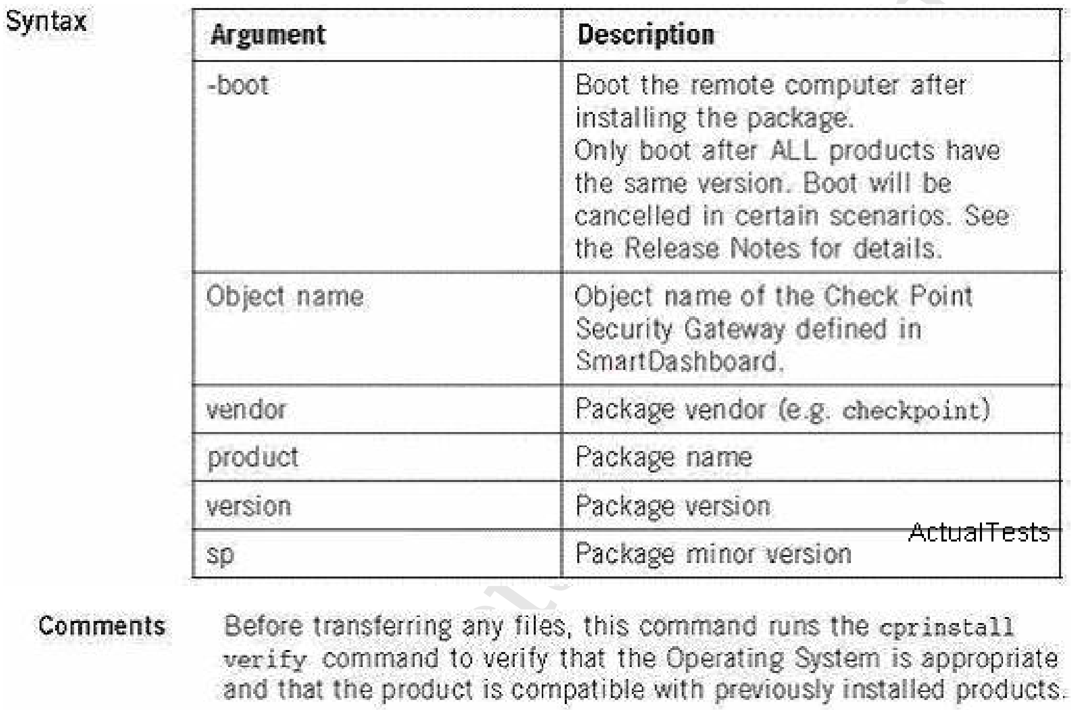
Usage `cprinstall get <Object name>`

Syntax

Argument	Description
Object name	The name of the Check Point Security Gateway object defined in SmartDashboard.

Example

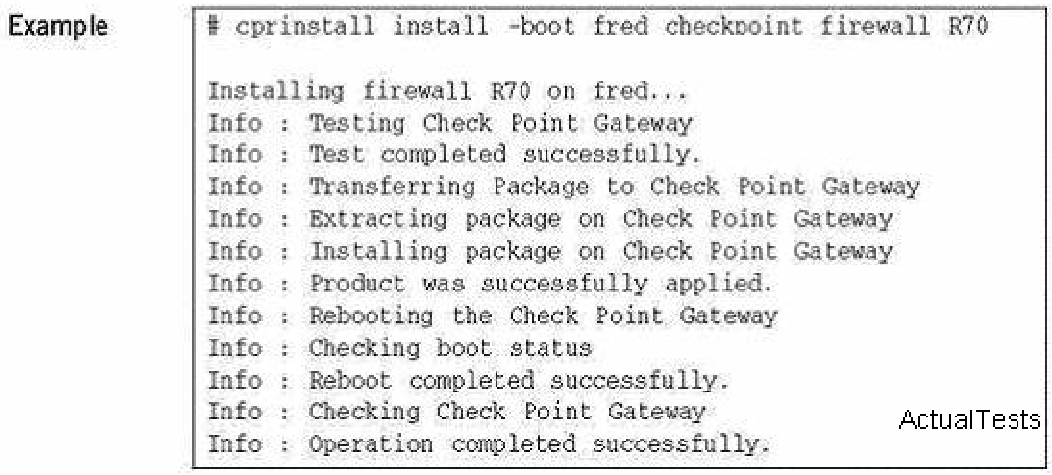
```
cprinstall get gw1
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system    Major Version       Minor Version
----------------------------------------------------------------------
SecurePlatform      R70                  R70

Vendor              Product             Major Version       Minor Version
----------------------------------------------------------------------
Check Point         VPN-1 Power/UTM     R70                 R70
Check Point         SecurePlatform      R70                 R70
Check Point         SmartPortal         R70                 R70
```



Syntax

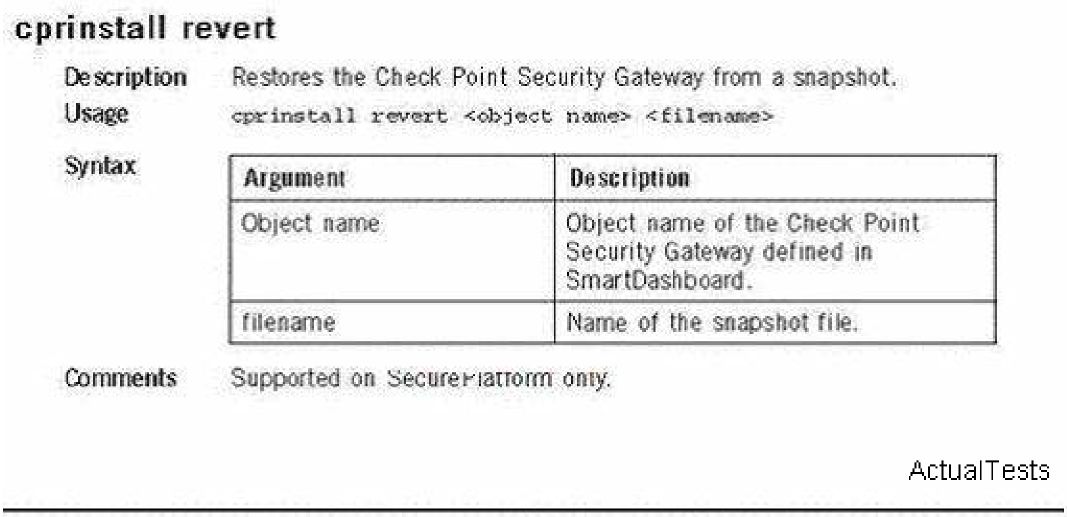
Argument	Description
-boot	Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios. See the Release Notes for details.
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint)
product	Package name
version	Package version
sp	Package minor version

Comments Before transferring any files, this command runs the `cprinstall verify` command to verify that the Operating System is appropriate and that the product is compatible with previously installed products.



Example

```
# cprinstall install -boot fred checkpoint firewall R70

Installing firewall R70 on fred...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
```



cprinstall revert

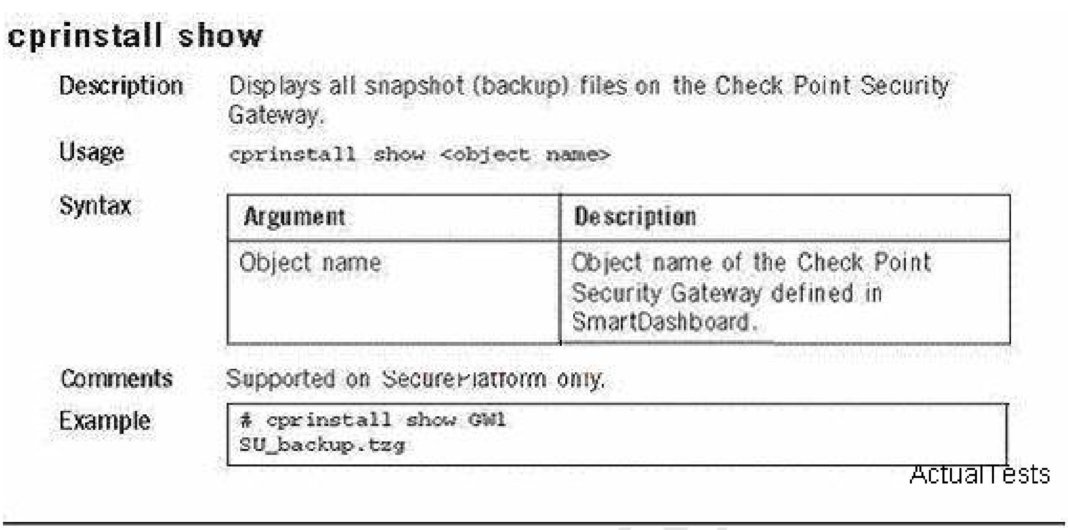
Description Restores the Check Point Security Gateway from a snapshot.

Usage `cprinstall revert <object name> <filename>`

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
filename	Name of the snapshot file.

Comments Supported on SecurePlatform only.



cprinstall show

Description Displays all snapshot (backup) files on the Check Point Security Gateway.

Usage `cprinstall show <object name>`

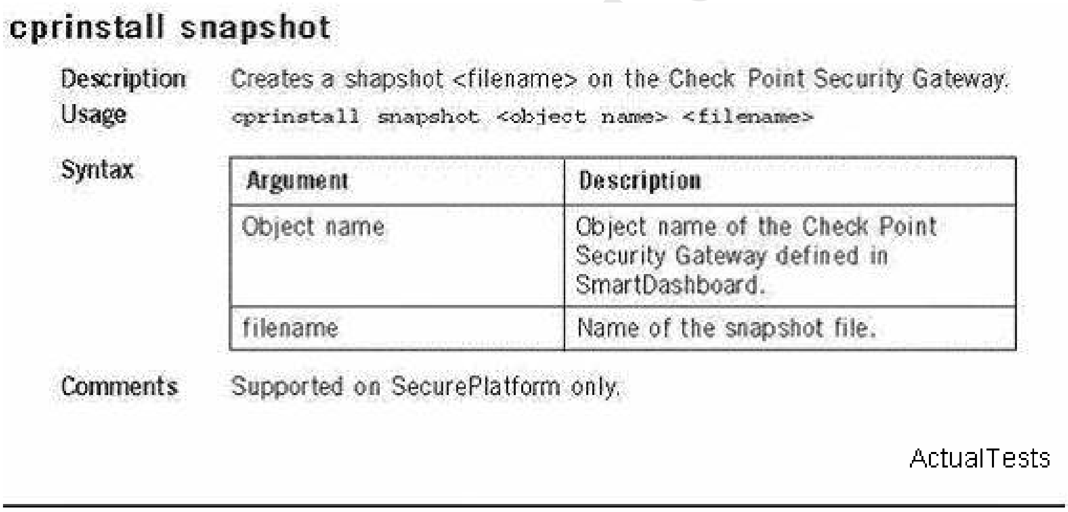
Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.

Comments Supported on SecurePlatform only.

Example

```
# cprinstall show GW1
SU_backup.tzg
```



cprinstall snapshot

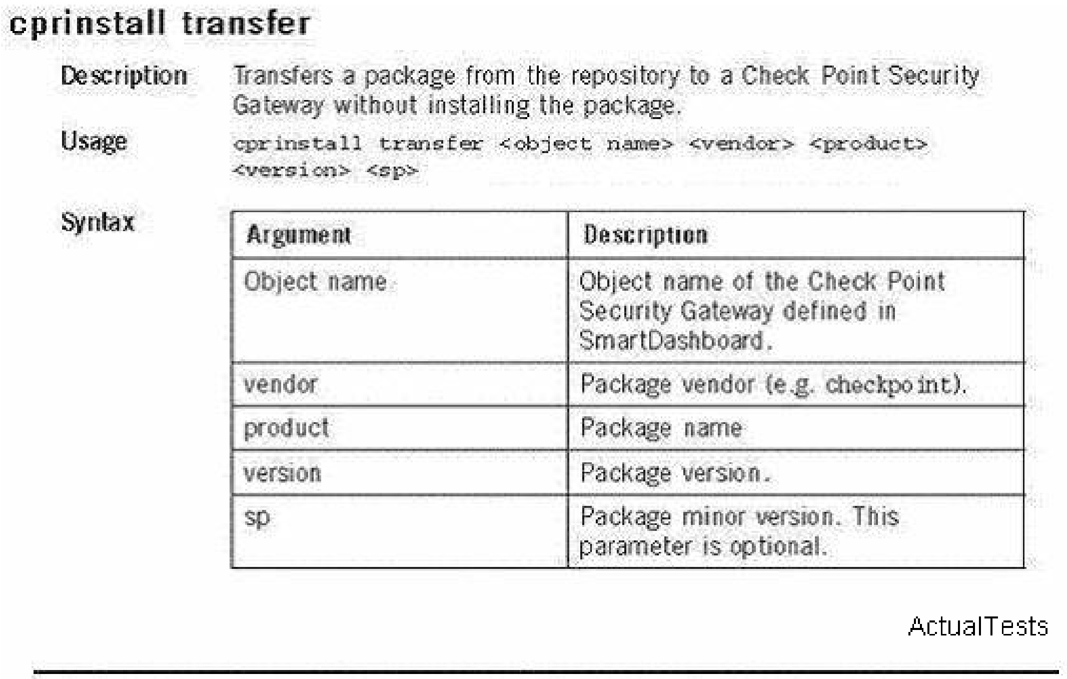
Description Creates a shapshot <filename> on the Check Point Security Gateway.

Usage `cprinstall snapshot <object name> <filename>`

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
filename	Name of the snapshot file.

Comments Supported on SecurePlatform only.



cprinstall transfer

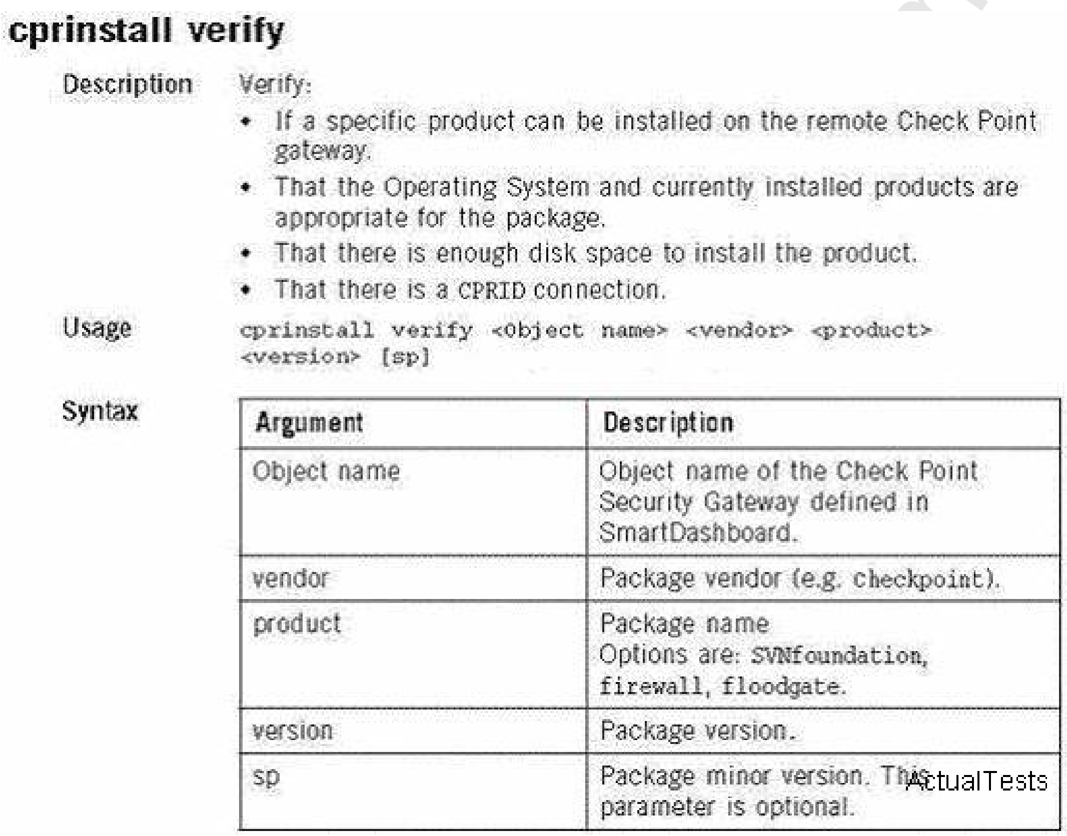
Description Transfers a package from the repository to a Check Point Security Gateway without installing the package.

Usage

```
cprinstall transfer <object name> <vendor> <product>
<version> <sp>
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint).
product	Package name
version	Package version.
sp	Package minor version. This parameter is optional.



cprinstall verify

Description Verify:

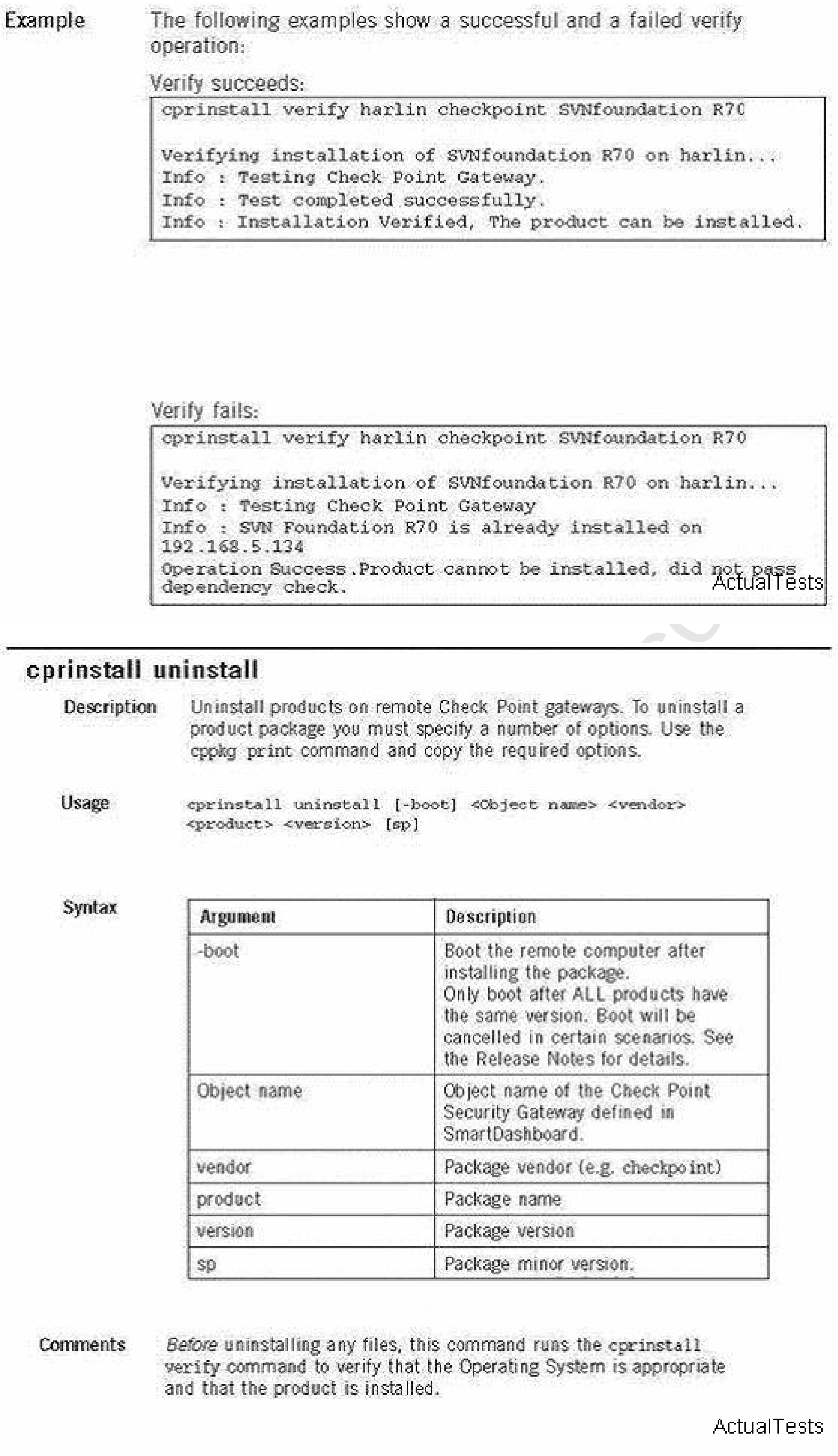
- If a specific product can be installed on the remote Check Point gateway.
- That the Operating System and currently installed products are appropriate for the package.
- That there is enough disk space to install the product.
- That there is a CPRID connection.

Usage

```
cprinstall verify <object name> <vendor> <product>
<version> [sp]
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint).
product	Package name Options are: SVNfoundation, firewall, floodgate.
version	Package version.
sp	Package minor version. This parameter is optional.



Example The following examples show a successful and a failed verify operation:

Verify succeeds:

```
cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info : Testing Check Point Gateway.
Info : Test completed successfuly.
Info : Installation Verified, The product can be installed.
```

Verify fails:

```
cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info : Testing Check Point Gateway
Info : SVN Foundation R70 is already installed on
192.168.5.134
Operation Success.Product cannot be installed, did not pass
dependency check.
```

cprinstall uninstall

Description Uninstall products on remote Check Point gateways. To uninstall a product package you must specify a number of options. Use the cppkg print command and copy the required options.

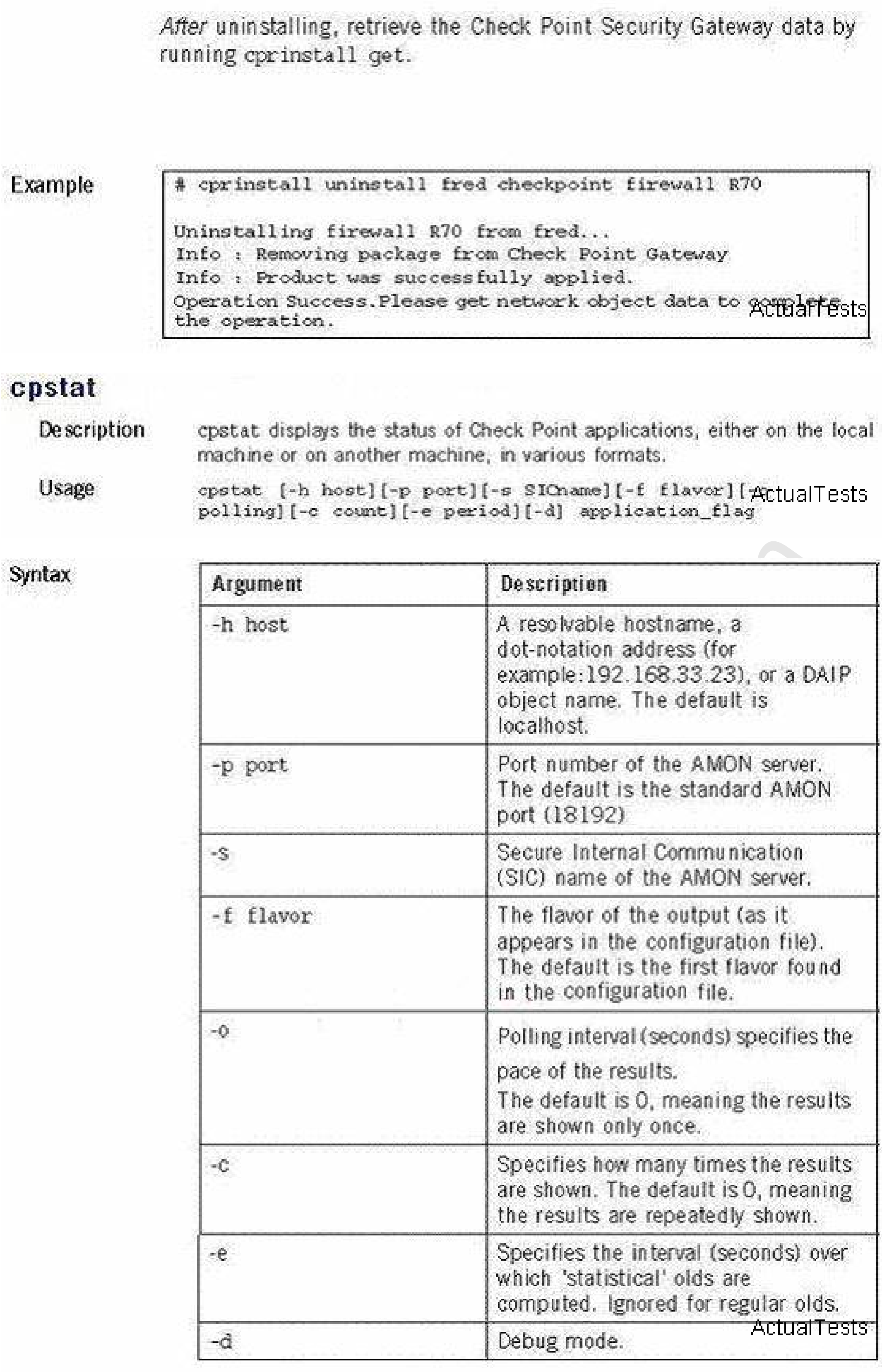
Usage

```
cprinstall uninstall [-boot] <Object name> <vendor>
<product> <version> [sp]
```

Syntax

Argument	Description
-boot	Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios. See the Release Notes for details.
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint)
product	Package name
version	Package version
sp	Package minor version.

Comments *Before* uninstalling any files, this command runs the cprinstall verify command to verify that the Operating System is appropriate and that the product is installed.



After uninstalling, retrieve the Check Point Security Gateway data by running `cprinstall get`.

Example

```
# cprinstall uninstall fred checkpoint firewall R70

Uninstalling firewall R70 from fred...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success.Please get network object data to complete
the operation.
```

cpstat

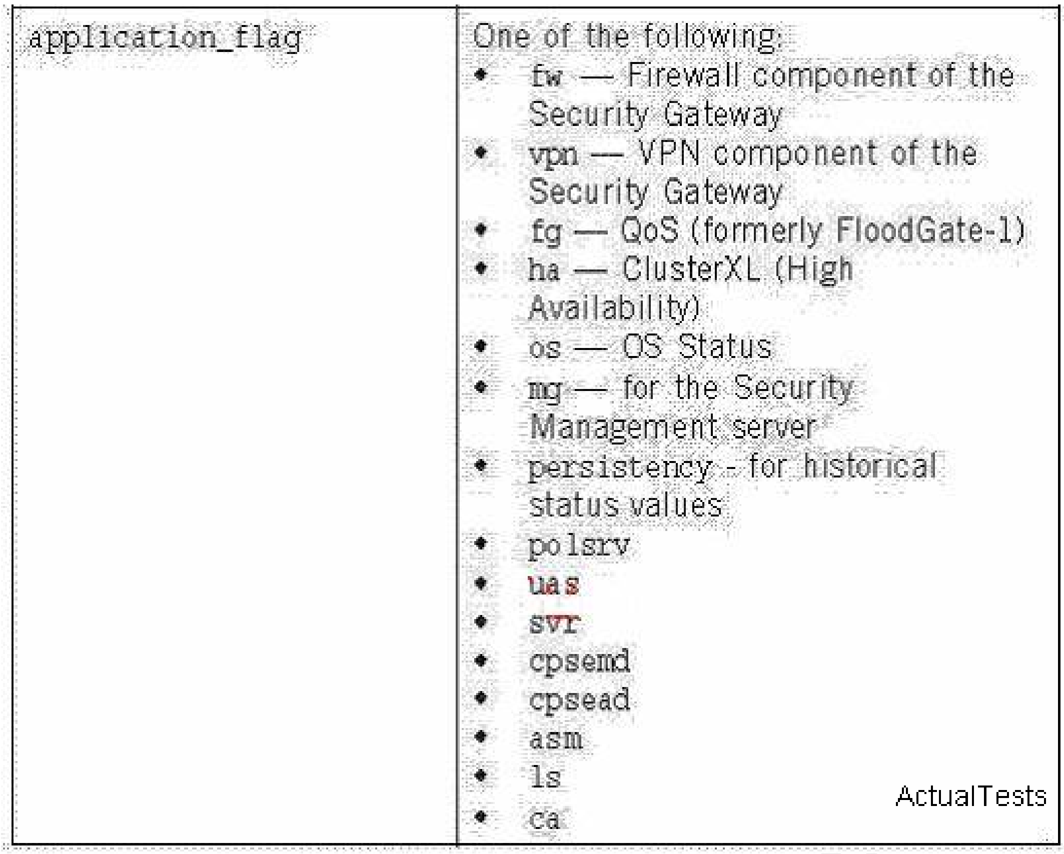
Description cpstat displays the status of Check Point applications, either on the local machine or on another machine, in various formats.

Usage

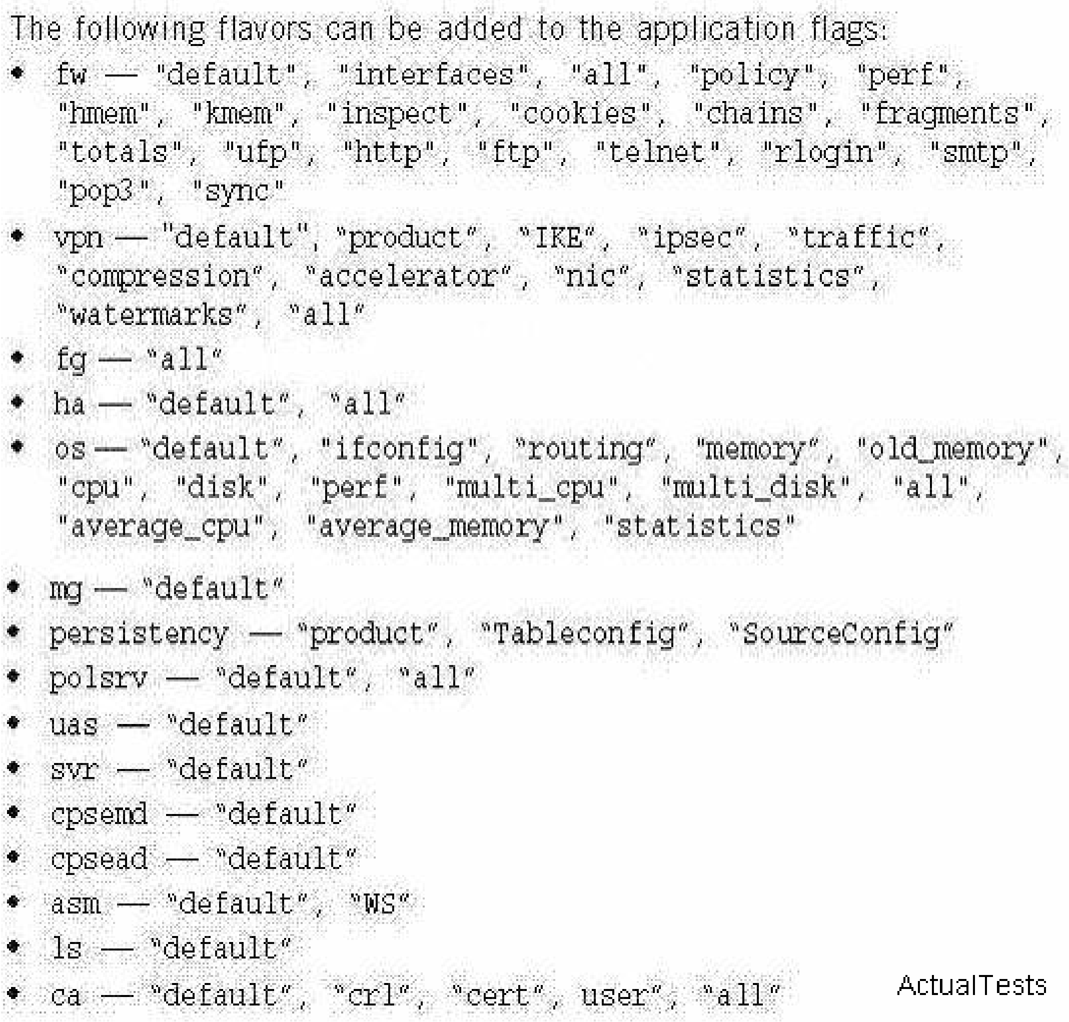
```
cpstat [-h host][-p port][-s SICname][-f flavor][-
polling][-c count][-e period][-d] application_flag
```

Syntax

Argument	Description
-h host	A resolvable hostname, a dot-notation address (for example:192.168.33.23), or a DAIP object name. The default is localhost.
-p port	Port number of the AMON server. The default is the standard AMON port (18192)
-s	Secure Internal Communication (SIC) name of the AMON server.
-f flavor	The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.
-o	Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.
-c	Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.
-e	Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.
-d	Debug mode.

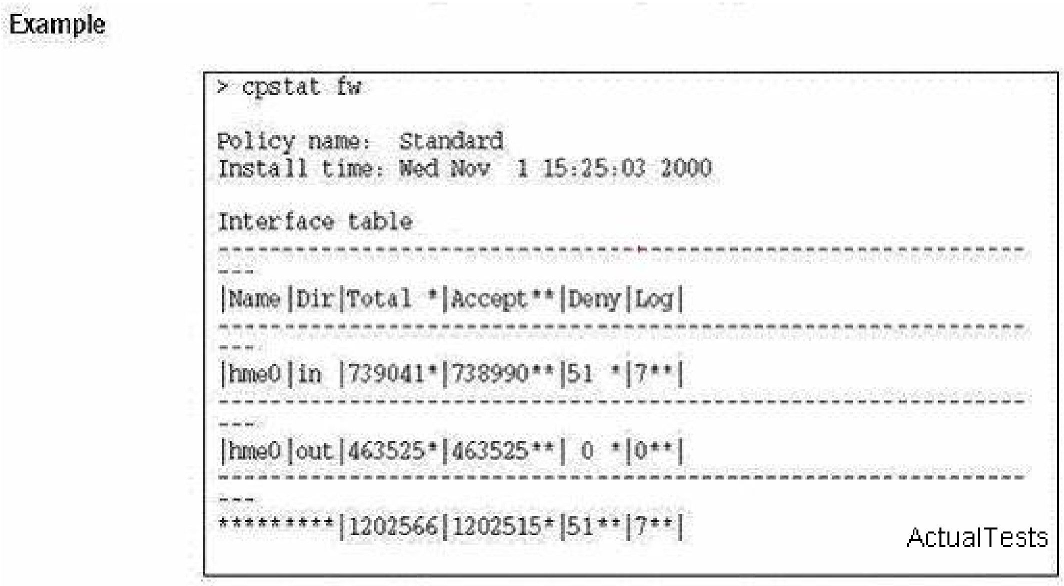


application_flag	One of the following: • fw — Firewall component of the Security Gateway • vpn — VPN component of the Security Gateway • fg — QoS (formerly FloodGate-1) • ha — ClusterXL (High Availability) • os — OS Status • mg — for the Security Management server • persistency - for historical status values • polsrv • uas • svr • cpsemd • cpsead • asm • ls • ca



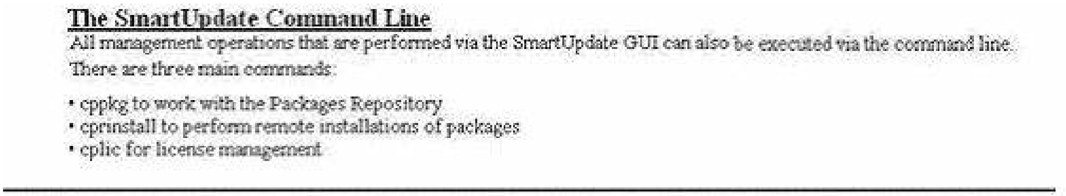
The following flavors can be added to the application flags:

- fw — "default", "interfaces", "all", "policy", "perf", "hmem", "kmem", "inspect", "cookies", "chains", "fragments", "totals", "ufp", "http", "ftp", "telnet", "rlogin", "smtp", "pop3", "sync"
- vpn — "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- fg — "all"
- ha — "default", "all"
- os — "default", "ifconfig", "routing", "memory", "old_memory", "cpu", "disk", "perf", "multi_cpu", "multi_disk", "all", "average_cpu", "average_memory", "statistics"
- mg — "default"
- persistency — "product", "Tableconfig", "SourceConfig"
- polsrv — "default", "all"
- uas — "default"
- svr — "default"
- cpsemd — "default"
- cpsead — "default"
- asm — "default", "WS"
- ls — "default"
- ca — "default", "crl", "cert", user", "all"



Example

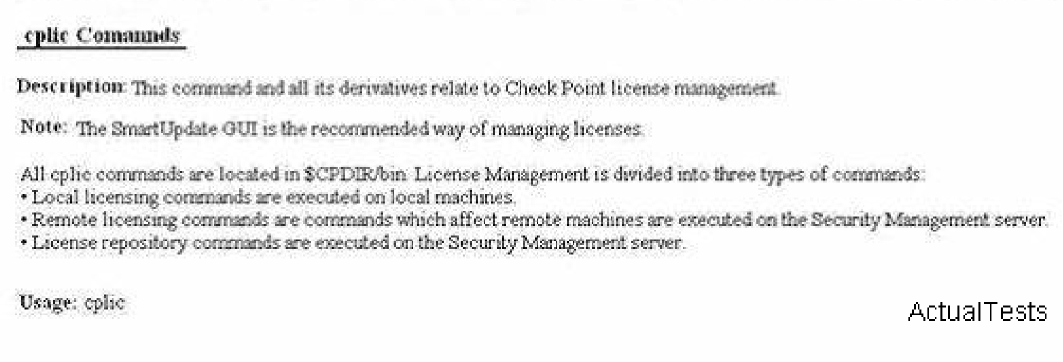
```
> cpstat fw

Policy name:  Standard
Install time: Wed Nov  1 15:25:03 2000

Interface table
-----------------------------------------------------------------
---
|Name|Dir|Total *|Accept**|Deny|Log|
-----------------------------------------------------------------
---
|hme0|in |739041*|738990**|51  *|7**|
-----------------------------------------------------------------
---
|hme0|out|463525*|463525**| 0  *|0**|
-----------------------------------------------------------------
---
*********|1202566|1202515*|51**|7**|
```



The SmartUpdate Command Line

All management operations that are performed via the SmartUpdate GUI can also be executed via the command line. There are three main commands:

- cppkg to work with the Packages Repository
- cprinstall to perform remote installations of packages
- cplic for license management



cplic Commands

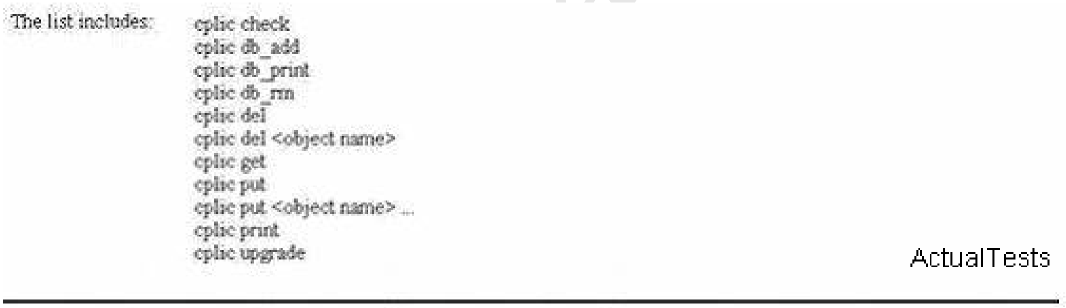
Description: This command and all its derivatives relate to Check Point license management.

Note: The SmartUpdate GUI is the recommended way of managing licenses.

All cplic commands are located in $CPDIR/bin. License Management is divided into three types of commands:

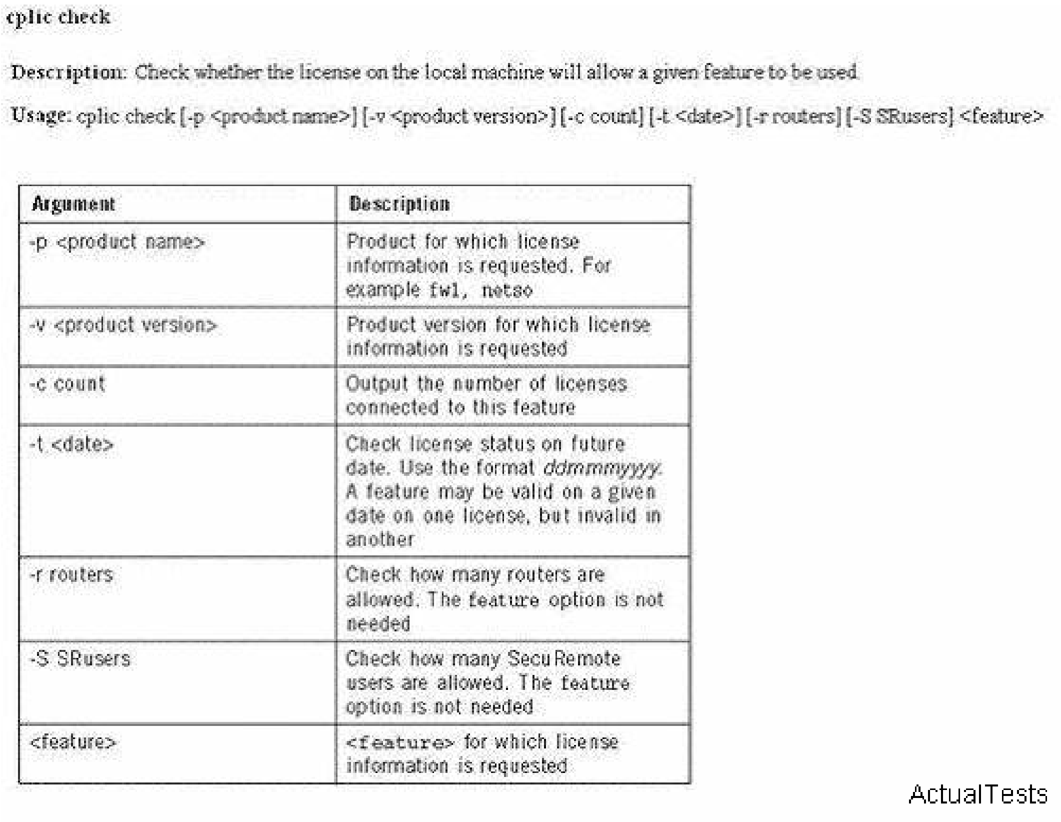
- Local licensing commands are executed on local machines.
- Remote licensing commands are commands which affect remote machines are executed on the Security Management server.
- License repository commands are executed on the Security Management server.

Usage: cplic



The list includes:

cplic check
cplic db_add
cplic db_print
cplic db_rm
cplic del
cplic del <object name>
cplic get
cplic put
cplic put <object name> ...
cplic print
cplic upgrade

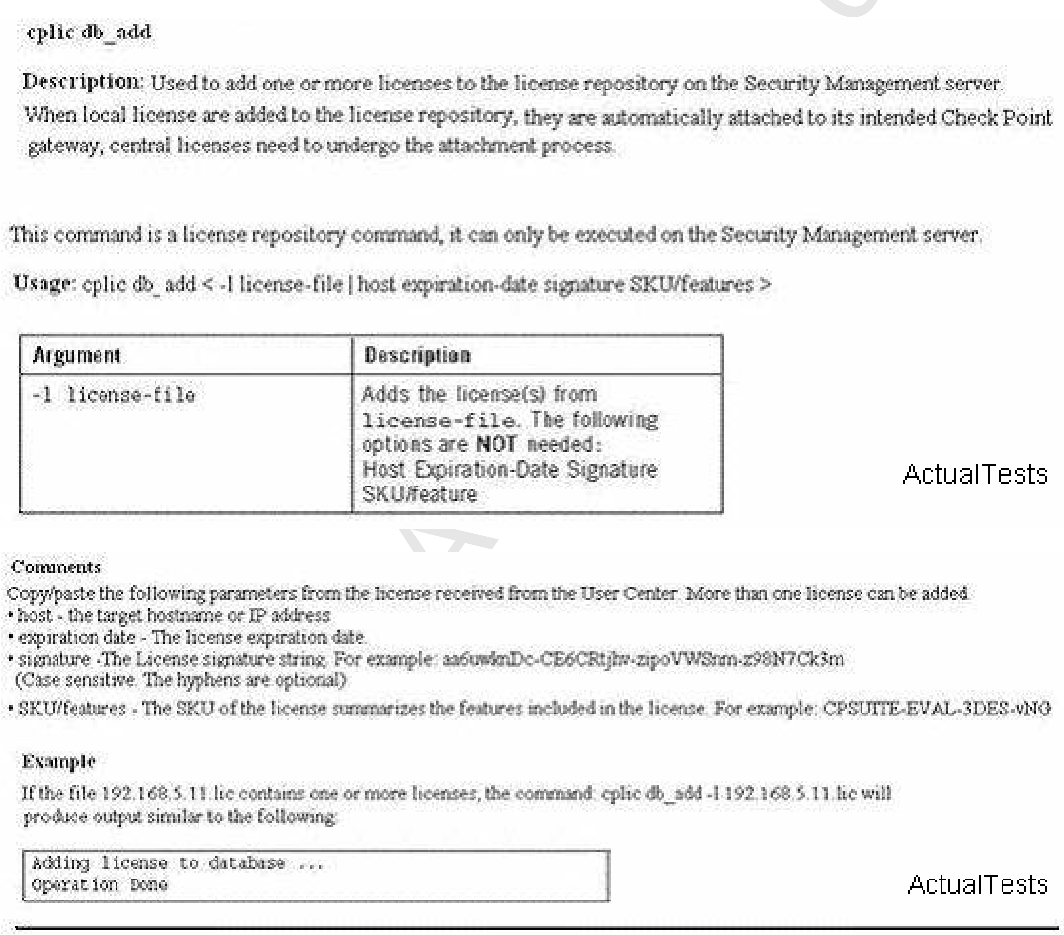


cplic check

Description: Check whether the license on the local machine will allow a given feature to be used.

Usage: cplic check [-p <product name>] [-v <product version>] [-c count] [-t <date>] [-r routers] [-S SRusers] <feature>

Argument	Description
-p <product name>	Product for which license information is requested. For example fw1, netso
-v <product version>	Product version for which license information is requested
-c count	Output the number of licenses connected to this feature
-t <date>	Check license status on future date. Use the format *ddmmmyyyy*. A feature may be valid on a given date on one license, but invalid in another
-r routers	Check how many routers are allowed. The feature option is not needed
-S SRusers	Check how many SecuRemote users are allowed. The feature option is not needed
<feature>	<feature> for which license information is requested



cplic db_add

Description: Used to add one or more licenses to the license repository on the Security Management server. When local license are added to the license repository, they are automatically attached to its intended Check Point gateway, central licenses need to undergo the attachment process.

This command is a license repository command, it can only be executed on the Security Management server.

Usage: cplic db_ add < -l license-file | host expiration-date signature SKU/features >

Argument	Description
-l license-file	Adds the license(s) from license-file. The following options are **NOT** needed: Host Expiration-Date Signature SKU/feature

Comments

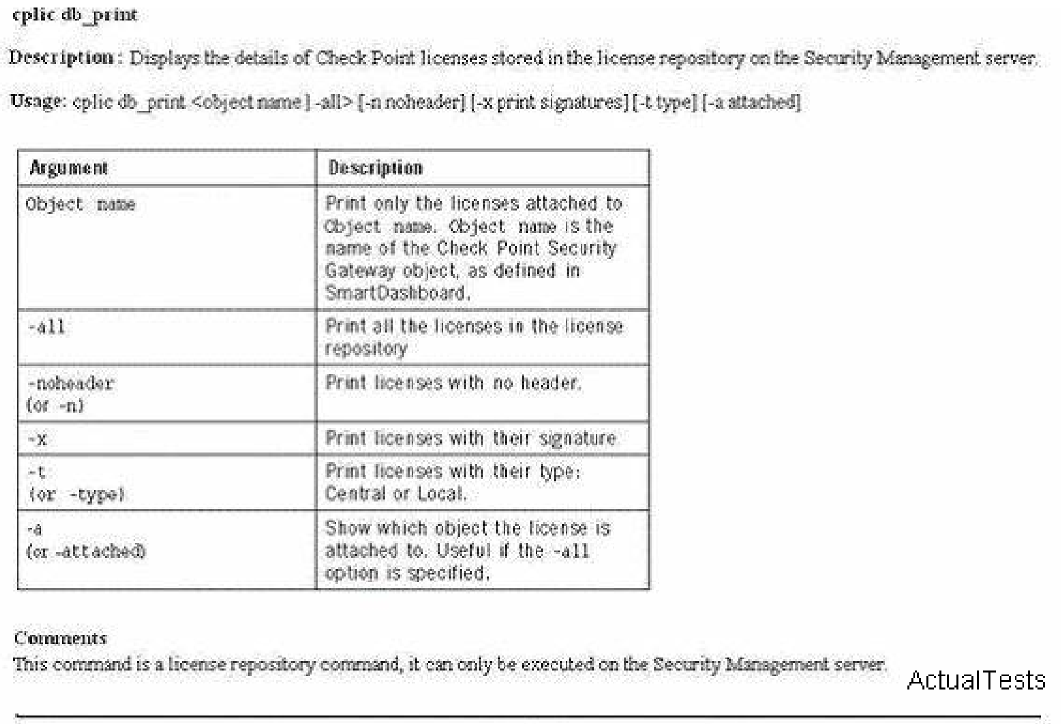
Copy/paste the following parameters from the license received from the User Center. More than one license can be added.

- host - the target hostname or IP address
- expiration date - The license expiration date.
- signature -The License signature string. For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional)
- SKU/features - The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG

Example

If the file 192.168.5.11.lic contains one or more licenses, the command: cplic db_add -l 192.168.5.11.lic will produce output similar to the following:

```
Adding license to database ...
Operation Done
```



cplic db_print

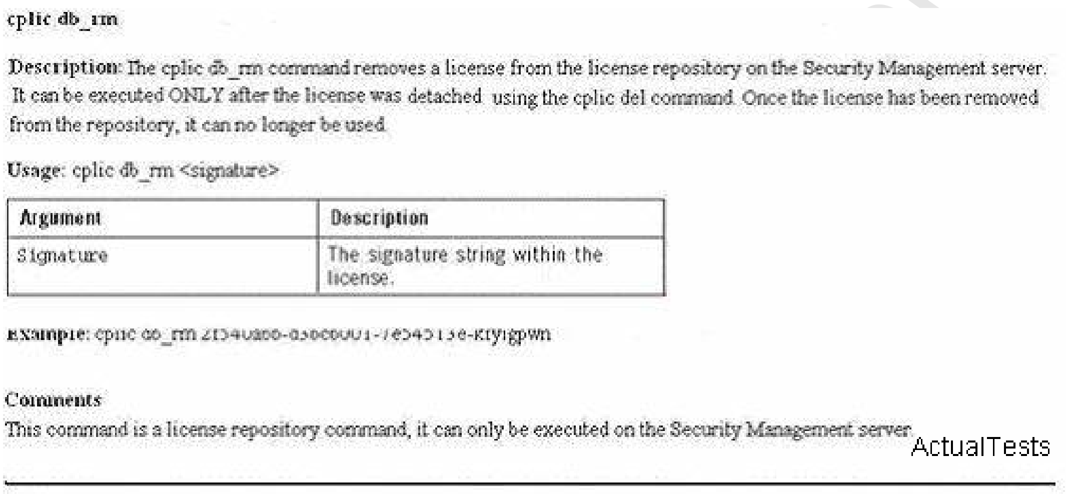
Description : Displays the details of Check Point licenses stored in the license repository on the Security Management server.

Usage: cplic db_print <object name] -all> [-n noheader] [-x print signatures] [-t type] [-a attached]

Argument	Description
Object name	Print only the licenses attached to Object name. Object name is the name of the Check Point Security Gateway object, as defined in SmartDashboard.
-all	Print all the licenses in the license repository
-noheader (or -n)	Print licenses with no header.
-x	Print licenses with their signature
-t (or -type)	Print licenses with their type: Central or Local.
-a (or -attached)	Show which object the license is attached to. Useful if the -all option is specified.

Comments

This command is a license repository command, it can only be executed on the Security Management server.



cplic db_rm

Description: The cplic db_rm command removes a license from the license repository on the Security Management server. It can be executed ONLY after the license was detached using the cplic del command. Once the license has been removed from the repository, it can no longer be used.

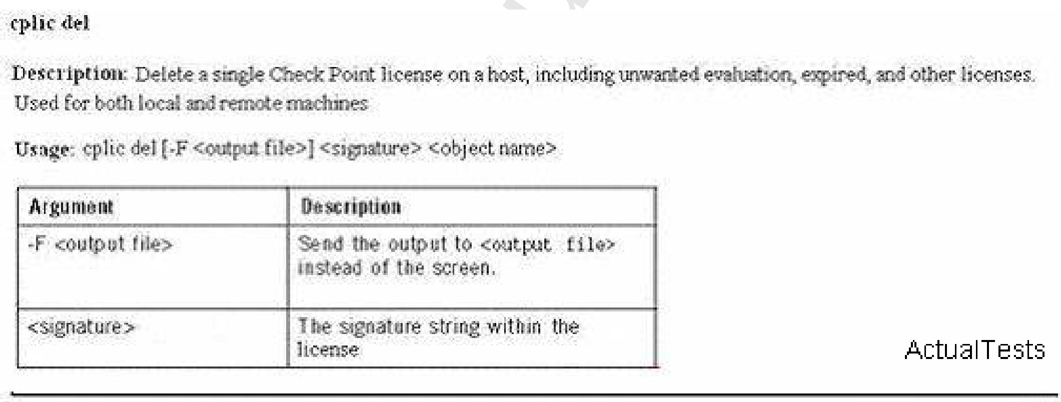
Usage: cplic db_rm <signature>

Argument	Description
Signature	The signature string within the license.

Example: cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn

Comments

This command is a license repository command, it can only be executed on the Security Management server.

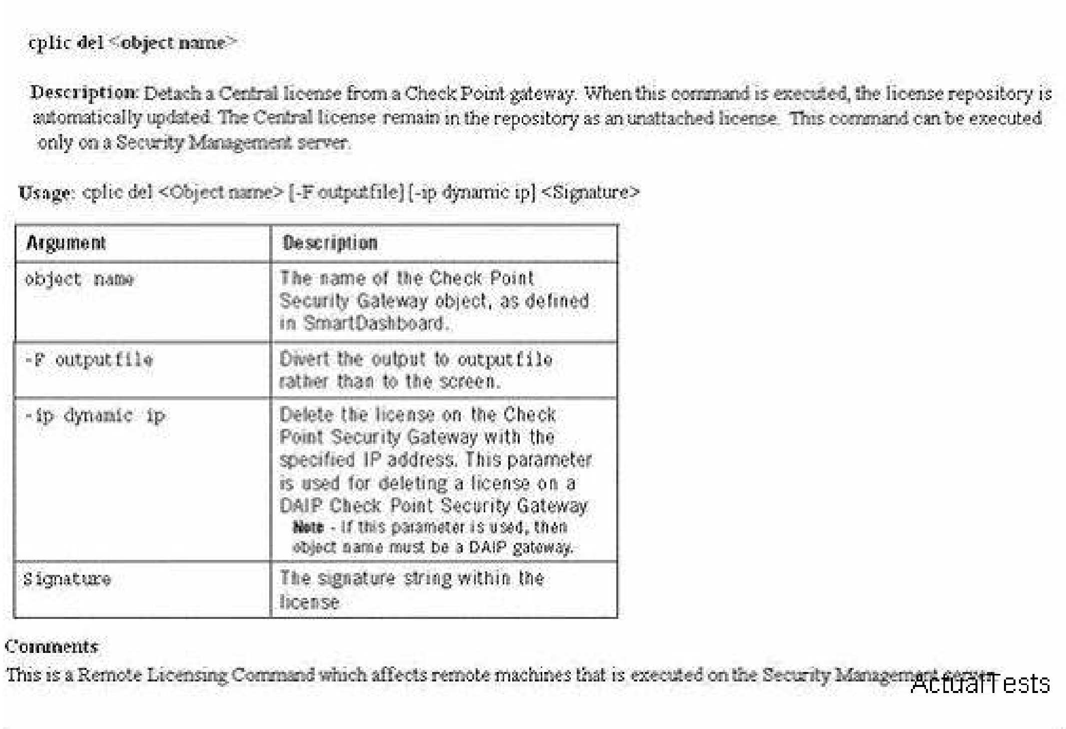


cplic del

Description: Delete a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote machines

Usage: cplic del [-F <output file>] <signature> <object name>

Argument	Description
-F <output file>	Send the output to <output file> instead of the screen.
<signature>	The signature string within the license



cplic del <object name>

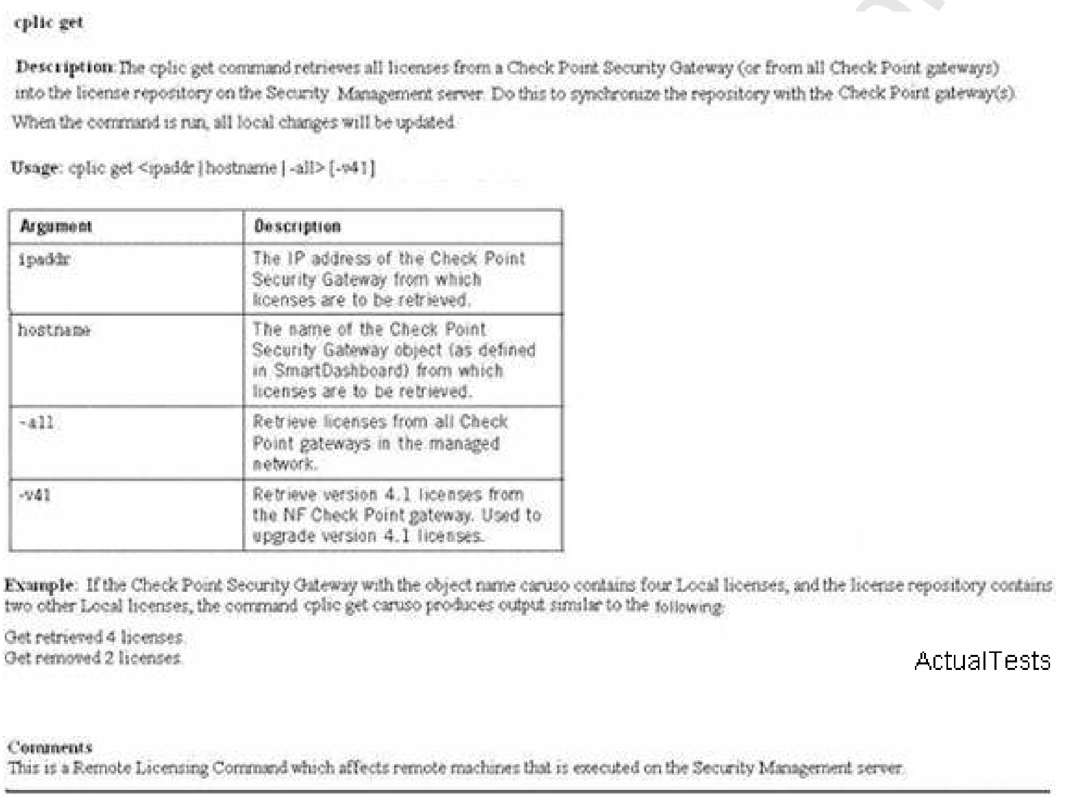
Description: Detach a Central license from a Check Point gateway. When this command is executed, the license repository is automatically updated. The Central license remain in the repository as an unattached license. This command can be executed only on a Security Management server.

Usage: cplic del <Object name> [-F outputfile] [-ip dynamic ip] <Signature>

Argument	Description
object name	The name of the Check Point Security Gateway object, as defined in SmartDashboard.
-F outputfile	Divert the output to outputfile rather than to the screen.
-ip dynamic ip	Delete the license on the Check Point Security Gateway with the specified IP address. This parameter is used for deleting a license on a DAIP Check Point Security Gateway **Note** - If this parameter is used, then object name must be a DAIP gateway.
Signature	The signature string within the license

Comments

This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.



cplic get

Description: The cplic get command retrieves all licenses from a Check Point Security Gateway (or from all Check Point gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Check Point gateway(s). When the command is run, all local changes will be updated.

Usage: cplic get <ipaddr | hostname | -all> [-v41]

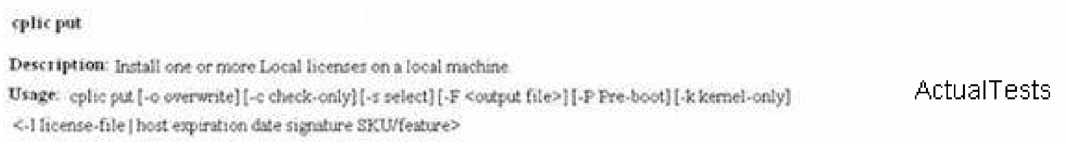
Argument	Description
ipaddr	The IP address of the Check Point Security Gateway from which licenses are to be retrieved.
hostname	The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved.
-all	Retrieve licenses from all Check Point gateways in the managed network.
-v41	Retrieve version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses.

Example: If the Check Point Security Gateway with the object name caruso contains four Local licenses, and the license repository contains two other Local licenses, the command cplic get caruso produces output similar to the following:

```
Get retrieved 4 licenses.
Get removed 2 licenses.
```

Comments

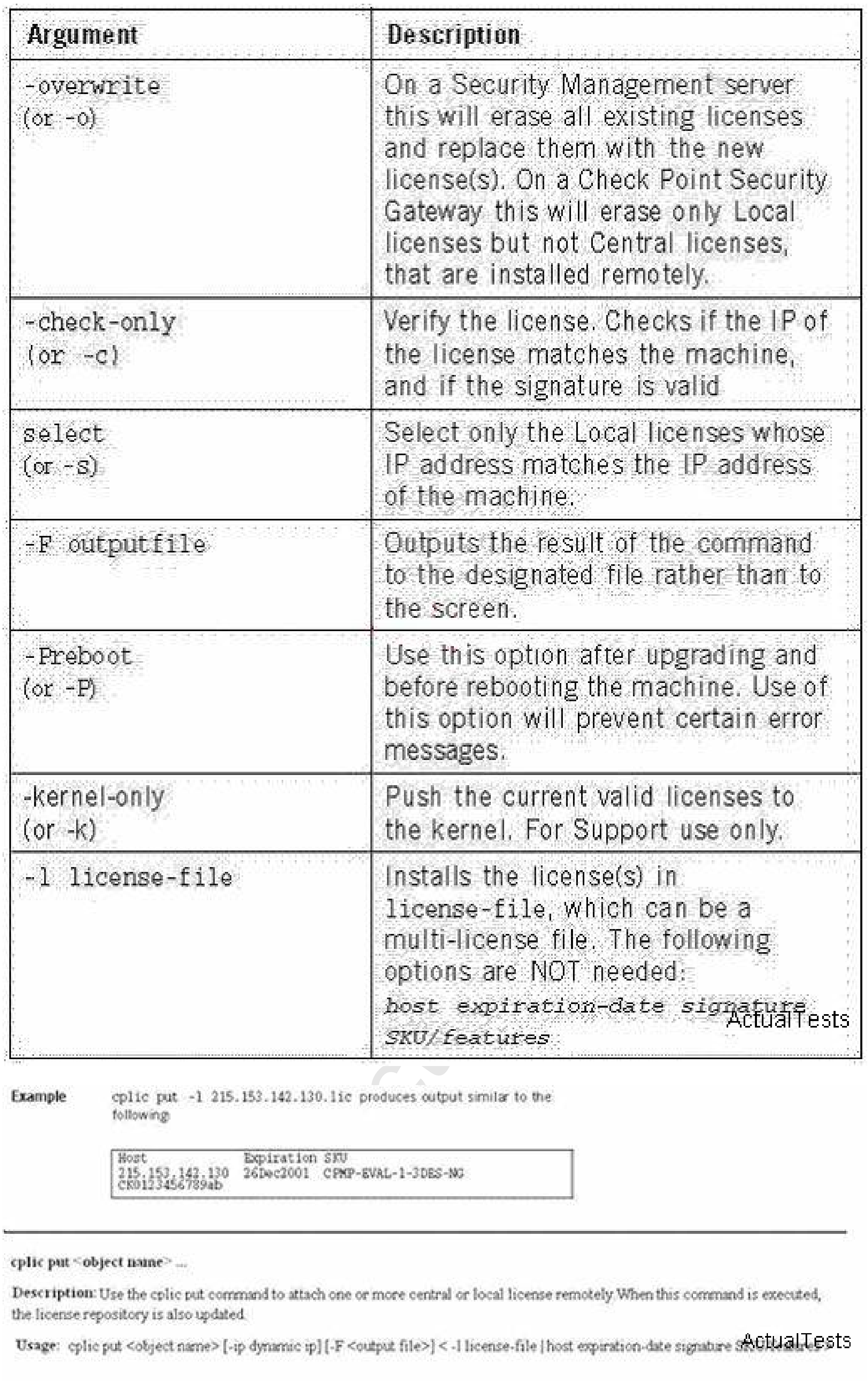
This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.



cplic put

Description: Install one or more Local licenses on a local machine.

Usage: cplic put [-o overwrite] [-c check-only] [-s select] [-F <output file>] [-P Pre-boot] [-k kernel-only] <-l license-file | host expiration date signature SKU/feature>



Argument	Description
-overwrite (or -o)	On a Security Management server this will erase all existing licenses and replace them with the new license(s). On a Check Point Security Gateway this will erase only Local licenses but not Central licenses, that are installed remotely.
-check-only (or -c)	Verify the license. Checks if the IP of the license matches the machine, and if the signature is valid
select (or -s)	Select only the Local licenses whose IP address matches the IP address of the machine.
-F outputfile	Outputs the result of the command to the designated file rather than to the screen.
-Preboot (or -P)	Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages.
-kernel-only (or -k)	Push the current valid licenses to the kernel. For Support use only.
-l license-file	Installs the license(s) in license-file, which can be a multi-license file. The following options are NOT needed: *host expiration-date signature SKU/features*

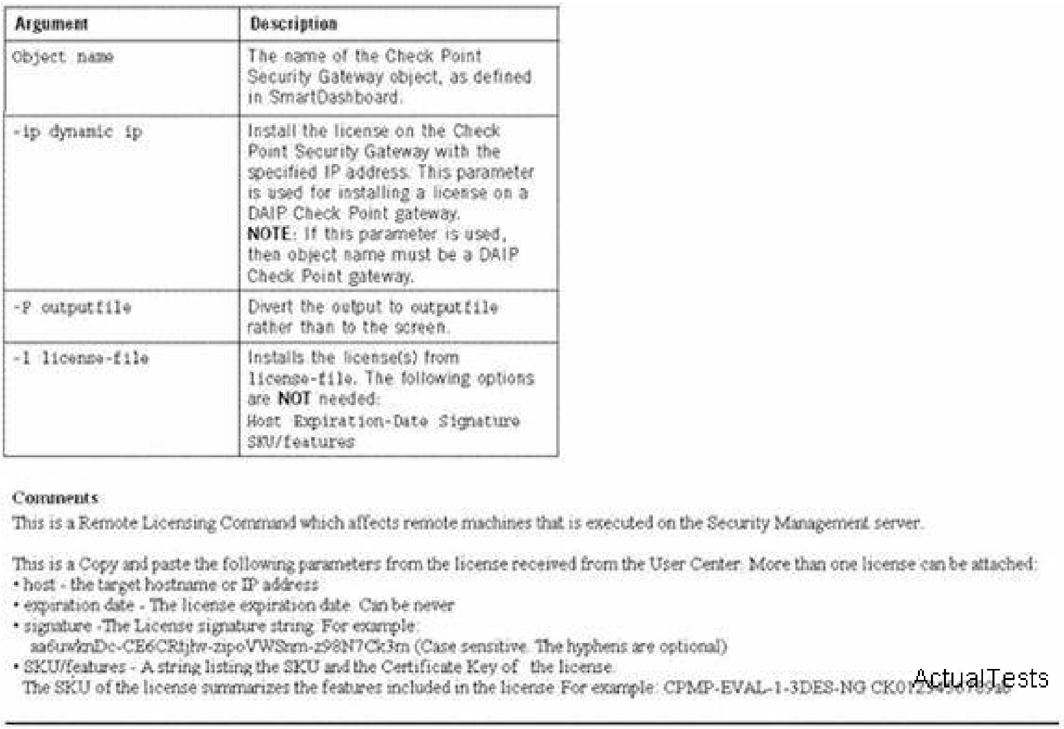
Example cplic put -l 215.153.142.130.lic produces output similar to the following

```
Host             Expiration SKU
215.153.142.130  26Dec2001  CPMP-EVAL-1-3DES-NG
CK0123456789ab
```

cplic put <object name> ...

Description: Use the cplic put command to attach one or more central or local license remotely When this command is executed, the license repository is also updated

Usage: cplic put <object name> [-ip dynamic ip] [-F <output file>] < -l license-file | host expiration-date signature SKU/features >

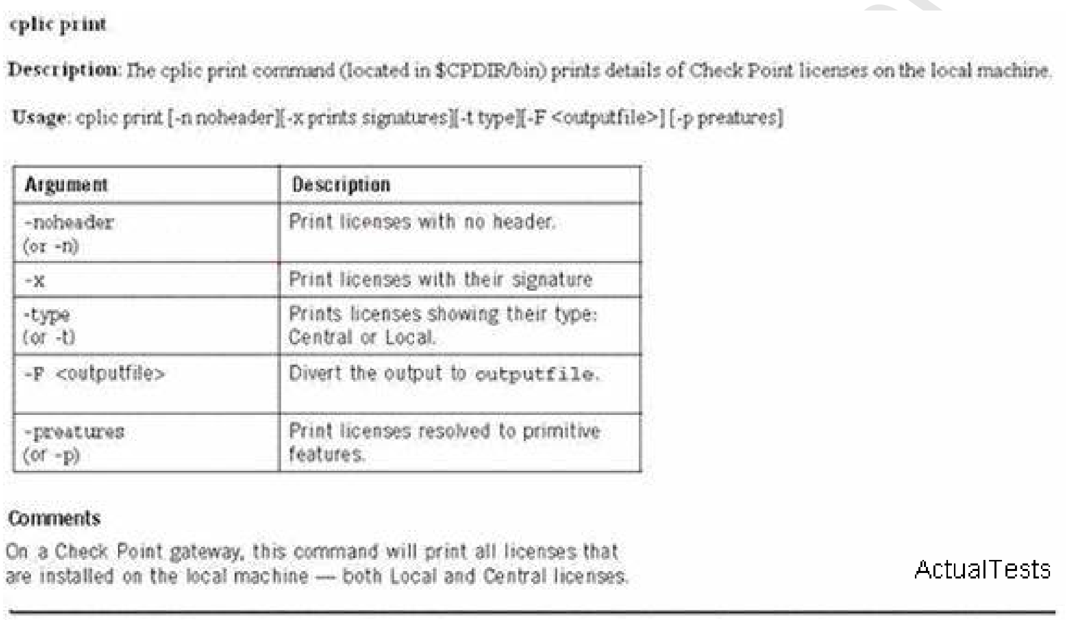


Argument	Description
Object name	The name of the Check Point Security Gateway object, as defined in SmartDashboard.
-ip dynamic ip	Install the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point gateway. **NOTE**: If this parameter is used, then object name must be a DAIP Check Point gateway.
-F outputfile	Divert the output to outputfile rather than to the screen.
-l license-file	Installs the license(s) from license-file. The following options are **NOT** needed: Host Expiration-Date Signature SKU/features

Comments

This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.

This is a Copy and paste the following parameters from the license received from the User Center. More than one license can be attached:
- host - the target hostname or IP address
- expiration date - The license expiration date. Can be never
- signature -The License signature string. For example:
  aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional)
- SKU/features - A string listing the SKU and the Certificate Key of the license.
  The SKU of the license summarizes the features included in the license. For example: CPMP-EVAL-1-3DES-NG CK0123456789ab



cplic print

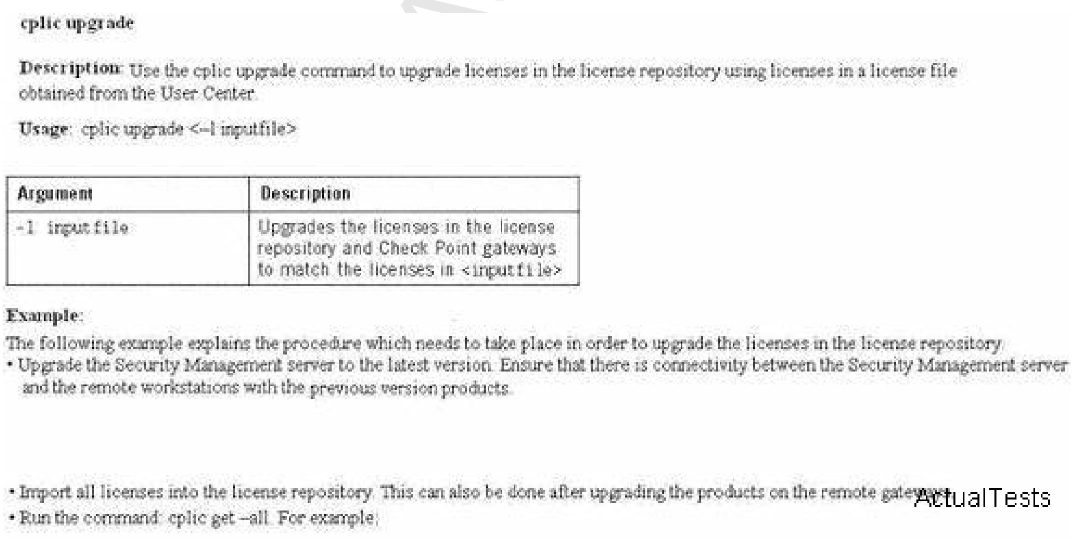
Description: The cplic print command (located in $CPDIR/bin) prints details of Check Point licenses on the local machine.

Usage: cplic print [-n noheader][-x prints signatures][-t type][-F <outputfile>] [-p preatures]

Argument	Description
-noheader (or -n)	Print licenses with no header.
-x	Print licenses with their signature
-type (or -t)	Prints licenses showing their type: Central or Local.
-F <outputfile>	Divert the output to outputfile.
-preatures (or -p)	Print licenses resolved to primitive features.

Comments

On a Check Point gateway, this command will print all licenses that are installed on the local machine — both Local and Central licenses.



cplic upgrade

Description: Use the cplic upgrade command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.

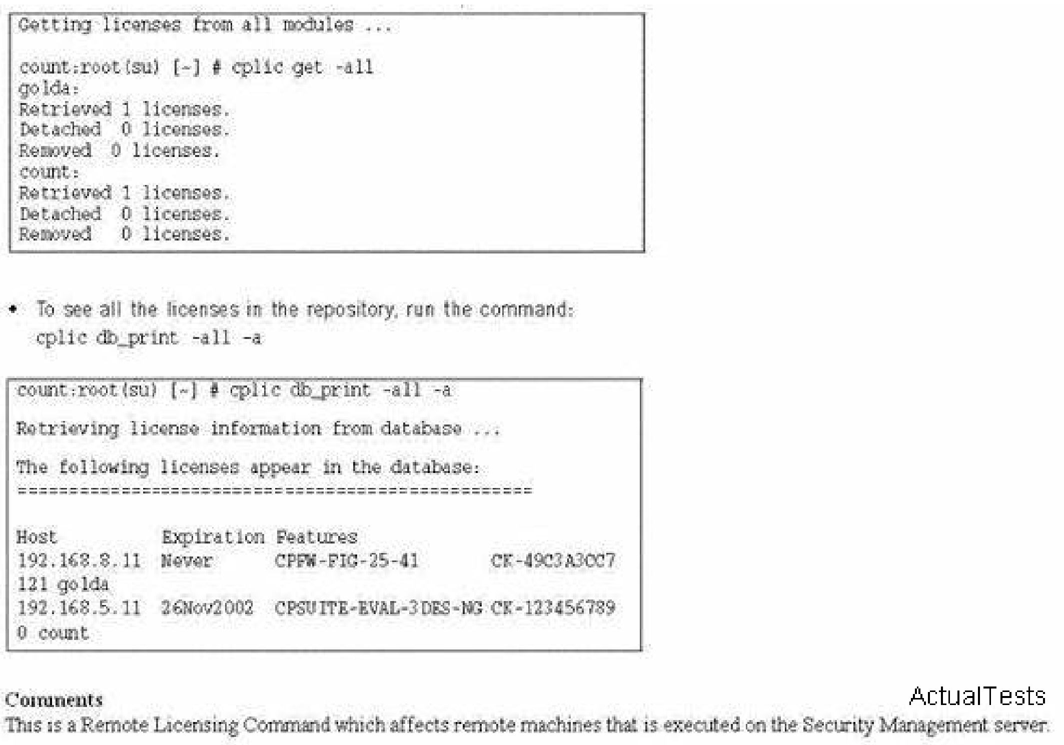
Usage: cplic upgrade <–l inputfile>

Argument	Description
-l inputfile	Upgrades the licenses in the license repository and Check Point gateways to match the licenses in <inputfile>

Example:

The following example explains the procedure which needs to take place in order to upgrade the licenses in the license repository.
- Upgrade the Security Management server to the latest version. Ensure that there is connectivity between the Security Management server and the remote workstations with the previous version products.

- Import all licenses into the license repository. This can also be done after upgrading the products on the remote gateways.
- Run the command: cplic get –all. For example:



```
Getting licenses from all modules ...

count:root(su) [~] # cplic get -all
golda:
Retrieved 1 licenses.
Detached  0 licenses.
Removed  0 licenses.
count:
Retrieved 1 licenses.
Detached  0 licenses.
Removed   0 licenses.
```

- To see all the licenses in the repository, run the command:
  cplic db_print -all -a

```
count:root(su) [~] # cplic db_print -all -a

Retrieving license information from database ...

The following licenses appear in the database:
==================================================

Host          Expiration Features
192.168.8.11  Never      CPFW-FIG-25-41       CK-49C3A3CC7
121 golda
192.168.5.11  26Nov2002  CPSUITE-EVAL-3DES-NG CK-123456789
0 count
```

Comments

This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.

A. Install Check Point products on remote Check Point gateways

B. Verify if a specific product can be installed on the remote Check Point gateway

C. Obtain details of the products and the Operating System installed on the specified Check Point gateway, and to update the database

D. Verify that the Operating System and currently installed products are appropriate for the package

E. Delete Check Point products on remote Check Point gateways

Answer: C

QUESTION NO: 117

You ran a certain SmartUpdate command line in order to find out the location of the product repository, and the result was "Current repository root is set to : /var/suroot/". What is the command likely to be?

A. cppkg delete

B. cppkg getroot

C. cppkg setroot

D. cppkg add

E. cppkg print

Answer: B

QUESTION NO: 118

You use the cplic db_rm command to remove a license from the license repository on the Security Management server and receive an error message stating that only detached licenses can be removed. How will you go about this in order to get license removed?

A. Go to License Tree in the SmartView Monitor, highlight the license to be removed and then detach it, then re- run cplic db_rm command
B. Run cplic db_rm twice to solve the problem
C. Manually detach the license by using the control panel and the re-run the cplic db_rm command
D. Go to License Tree in the SmartDashboard, highlight the license to be removed and then detach it, then re- run cplic db_rm command
E. Firstly, use cplicdel command to detach the license then re-run the cplic db_rm Command

Answer: E

QUESTION NO: 119

What is the difference between the commands cplic db_print and cplic print?

A. cplic print will print licenses on local machine and cplic db_print will display details of licenses in repository on the Security Management server
B. Both commands do the same job
C. cplic db_print will print licenses on local machine and cplic print will display details of licenses in repository on the Security Gateway
D. cplic print will print licenses on local machine and cplic db_print will print details of licenses in repository on any components
E. cplic db_print will display licenses on local machine and cplic print will display details of licenses in repository on the SmartConsole

Answer: A

QUESTION NO: 120

The SmartUpdate command line " cprinstall transfer" will:

A. Transfers a package from the repository to a Check Point Security Gateway without installing the package
B. Verify that the Operating System and currently installed products are appropriate for the package
C. Transfers a package from the repository to a Check Point Security Gateway and install the package

D. Obtain details of the products and the Operating System installed on the specified Check Point gateway, and to update the database
E. Verify if a specific product can be installed on the remote Check Point gateway

Answer: A

QUESTION NO: 121

What command prints the details of the Check Point licenses?

A. Pkgadd -d
B. Setup
C. Print
D. fw print
E. cplic print

Answer: E

QUESTION NO: 122

What will the command "d:\winnt\fw1\ng\bin] cppkg add C:\CPsuite-R70" achieve? Where d:\winnt\fw1\ng\bin is package-full-path?

A. It will purge a product package to the product repository
B. It will kill a product package to the product repository
C. It will add a product package to the product repository
D. It will print a product package to the product repository
E. It will delete a product package to the product repository

Answer: C

QUESTION NO: 123

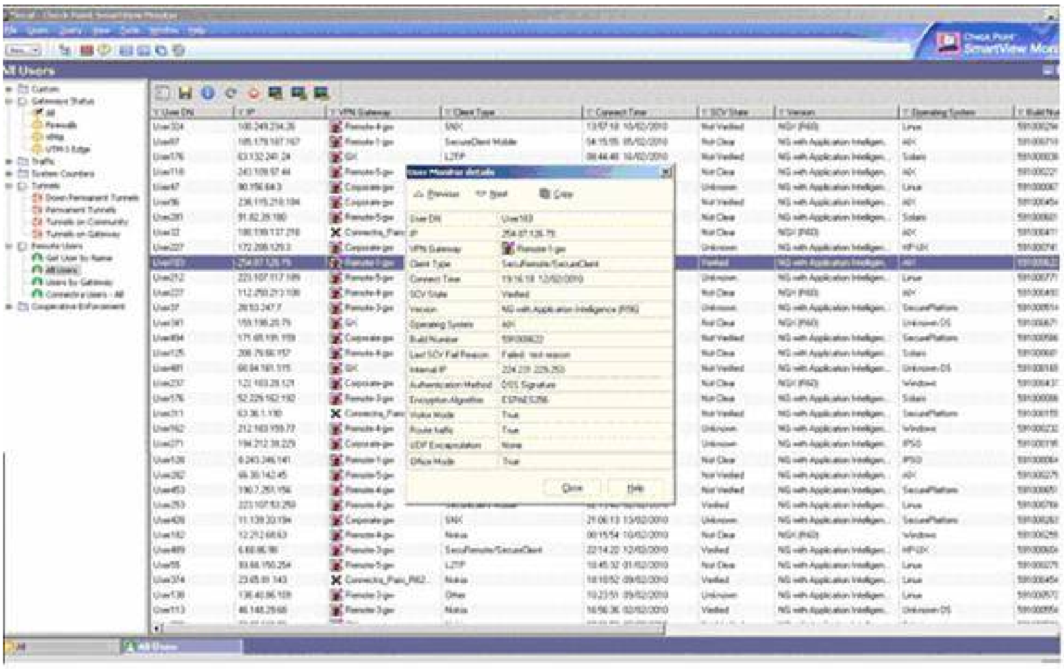
Anti-Spam status is monitored using which of the following tool?

A. Cpconfig
B. SmartView Tracker
C. Eventia Reporter
D. SmartView Monitor
E. SmartDashboard

Answer: D

QUESTION NO: 124

User Monitor details window is shown in the diagram 1 of the SmartView Monitor. Which of the following information you would not get in the window?



User Monitor details

User DN	User183
IP	254.87.126.75
VPN Gateway	Remote-1-gw
Client Type	SecuRemote/SecureClient
Connect Time	19:16:18 12/02/2010
SCV State	Verified
Version	NG with Application Intelligence (R56)
Operating System	AIX
Build Number	591000622
Last SCV Fail Reason	Failed: test reason
Internal IP	224.231.225.253
Authentication Method	DSS Signature
Encryption Algorithm	ESP/AES256
Visitor Mode	True
Route traffic	True
UDP Encapsulation	None
Office Mode	True

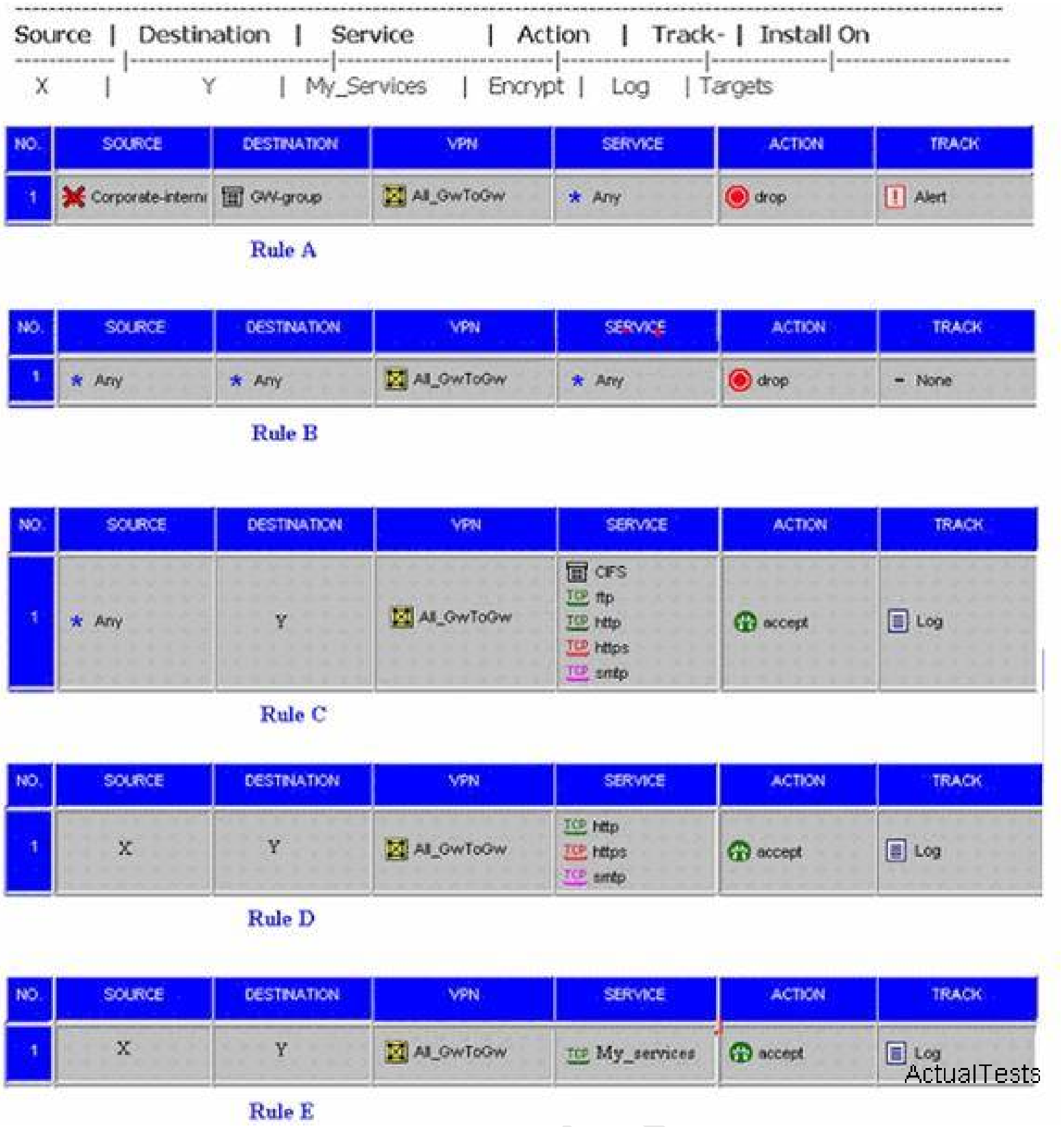
Figure 1: Remote Users View - User Monitor details

A. Internal IP
B. User DN
C. VPN Tunnel
D. Security Gateway
E. Connect Time

Answer: C

QUESTION NO: 125

The rule below shows the Encrypt rule in a Traditional Mode Rule Base. What is likely to be Simplified Mode equivalent if the if the connections originates at X and its destination is Y, within any Site-to-Site Community (i.e. All_GW _to_GW).



Source	Destination	Service	Action	Track-	Install On
X	Y	My_Services	Encrypt	Log	Targets

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Corporate-intern	GW-group	All_GwToGw	Any	drop	Alert

Rule A

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Any	Any	All_GwToGw	Any	drop	None

Rule B

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Any	Y	All_GwToGw	CIFS ftp http https smtp	accept	Log

Rule C

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	X	Y	All_GwToGw	http https smtp	accept	Log

Rule D

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	X	Y	All_GwToGw	My_services	accept	Log

Rule E

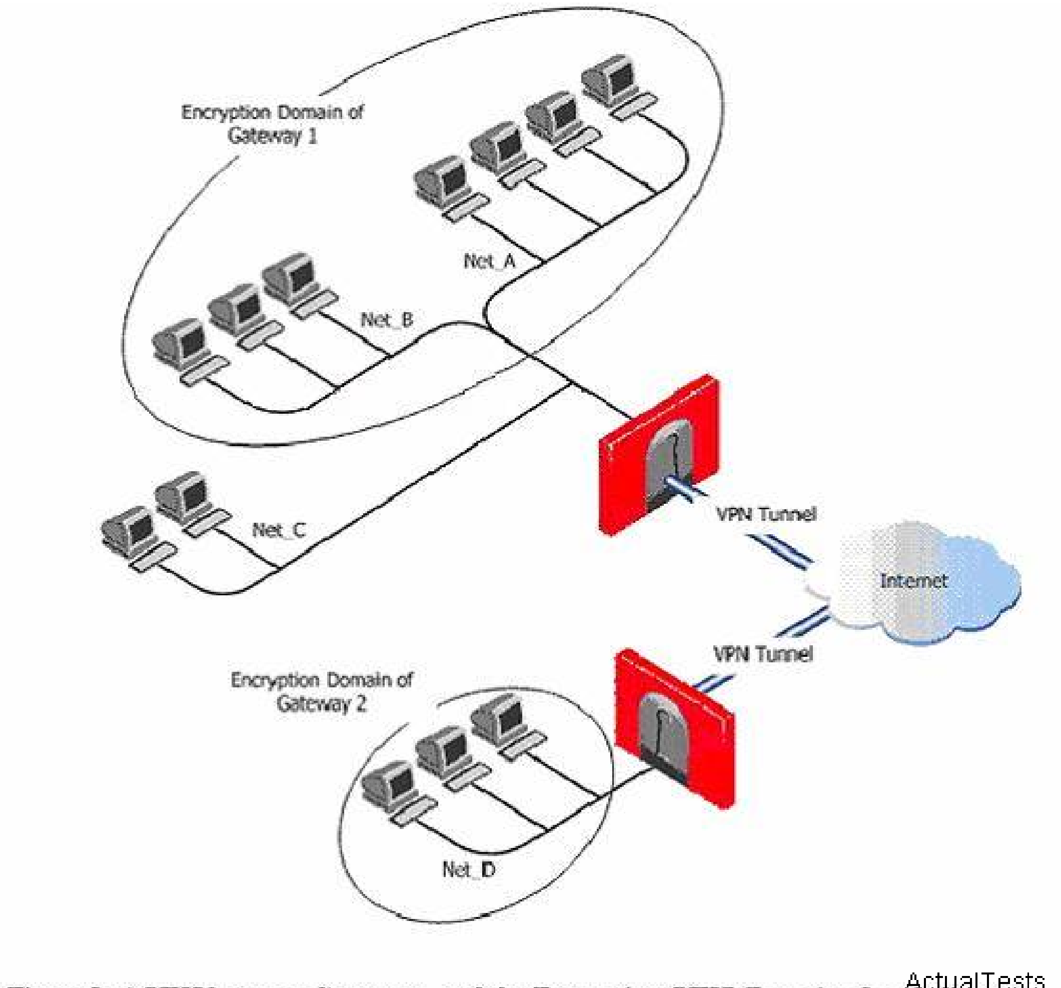

Encryption Domain of Gateway 1
Net_A
Net_B
Net_C
VPN Tunnel
Internet
VPN Tunnel
Encryption Domain of Gateway 2
Net_D
ActualTests

Figure 1: A VPN between Gateways, and the Encryption (VPN) Domain of each Gateway

A. Rule C
B. Rule E
C. Rule A
D. Rule B
E. Rule D

Answer: B

QUESTION NO: 126

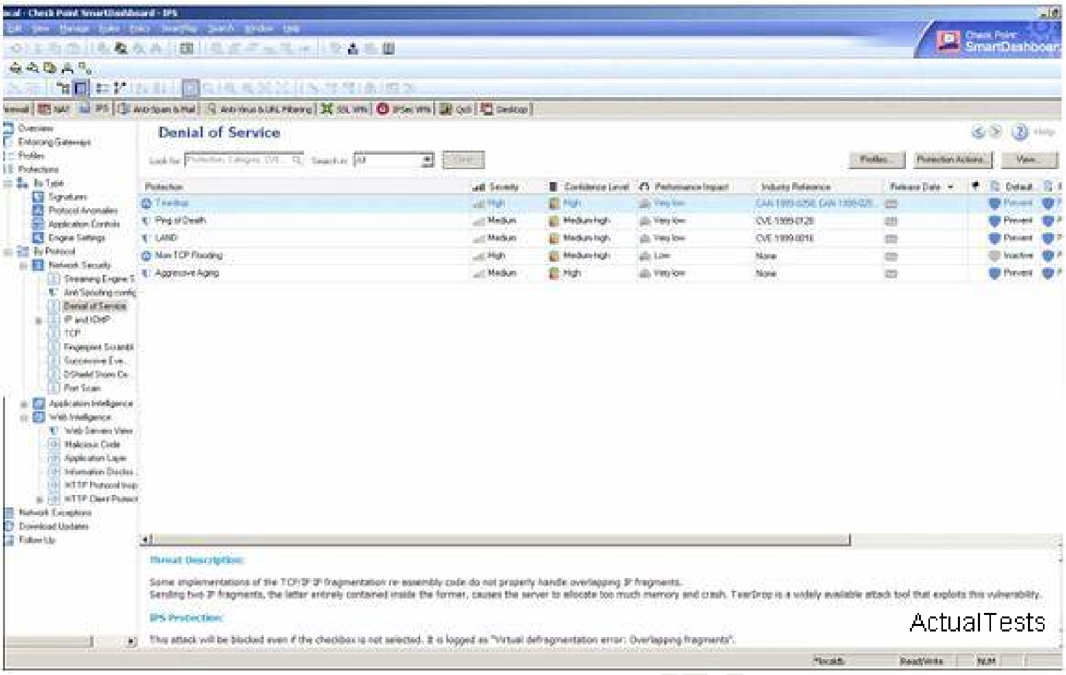
SmartDirectory (LDAP) new features include which of the following? Select the all correct answers.

A. The use of authentication algorithm
B. Support of Multiple SmartDirectory (LDAP) Vendors using Profiles
C. Support of multiple SmartDirectory (LDAP) servers
D. High Availability
E. The use of encrypted or non-encrypted SmartDirectory (LDAP) Connections

Answer: B,C,D,E

QUESTION NO: 127

You are configuring IPS, Denial of Service - Teardrop section. Which of the following is true of Teardrop?



Denial of Service

Protection	Severity	Confidence Level	Performance Impact	Industry Reference	Release Date	Default
Teardrop	High	High	Very low	CAN 1999-0258, CAN 1999-025...		Prevent
Ping of Death	Medium	Medium-high	Very low	CVE 1999-0128		Prevent
LAND	Medium	Medium-high	Very low	CVE 1999-0016		Prevent
Non TCP Flooding	High	Medium-high	Low	None		Inactive
Aggressive Aging	Medium	High	Very low	None		Prevent

Threat Description:

Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments.
Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. TearDrop is a widely available attack tool that exploits this vulnerability.

IPS Protection:

This attack will be blocked even if the checkbox is not selected. It is logged as "Virtual defragmentation error: Overlapping fragments".

A. A denial of service vulnerability has been reported in the Linux Kernel. The vulnerability is due to an error in the Linux Kernel IPv6 over IPv4 tunneling driverthat fails to properly handle crafted network packets. Teardrop is a widely available attack tool that exploits this vulnerability
B. Some implementations of TCP/IP contain fragmentation re-assembly code that does not properly handle overlapping IP fragments. Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. Teardrop is a widely available attack tool that exploits this vulnerability
C. JPEG is a very popular image file format. Teardrop is a widely available attack tool that exploits this vulnerabilitySpecially crafted JPEG files may be used to create a DoS condition and in some cases, arbitrary code execution
D. Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination, i.e., spoofed). Teardrop is a widely available attack tool that exploits this vulnerability
E. The attacker sends a fragmentedPING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash. Teardrop is a widely available attack tool that exploits this vulnerability

Answer: B

QUESTION NO: 128

Which of the following command will you use to export users from the NGX user database?

A. fwm dbexports
B. fw export
C. fwm export
D. fw dbexport
E. fwm dbexport

Answer: E

QUESTION NO: 129

The diagrams show your network and the encrypt rule. If the source and destination are inside the VPN Domain of the same gateway i.e. Source X is in Net_A and Destination Y is in Net_B. The connection originates at X and reaches the gateway, which forwards the response back to Y. Which of the following is true?

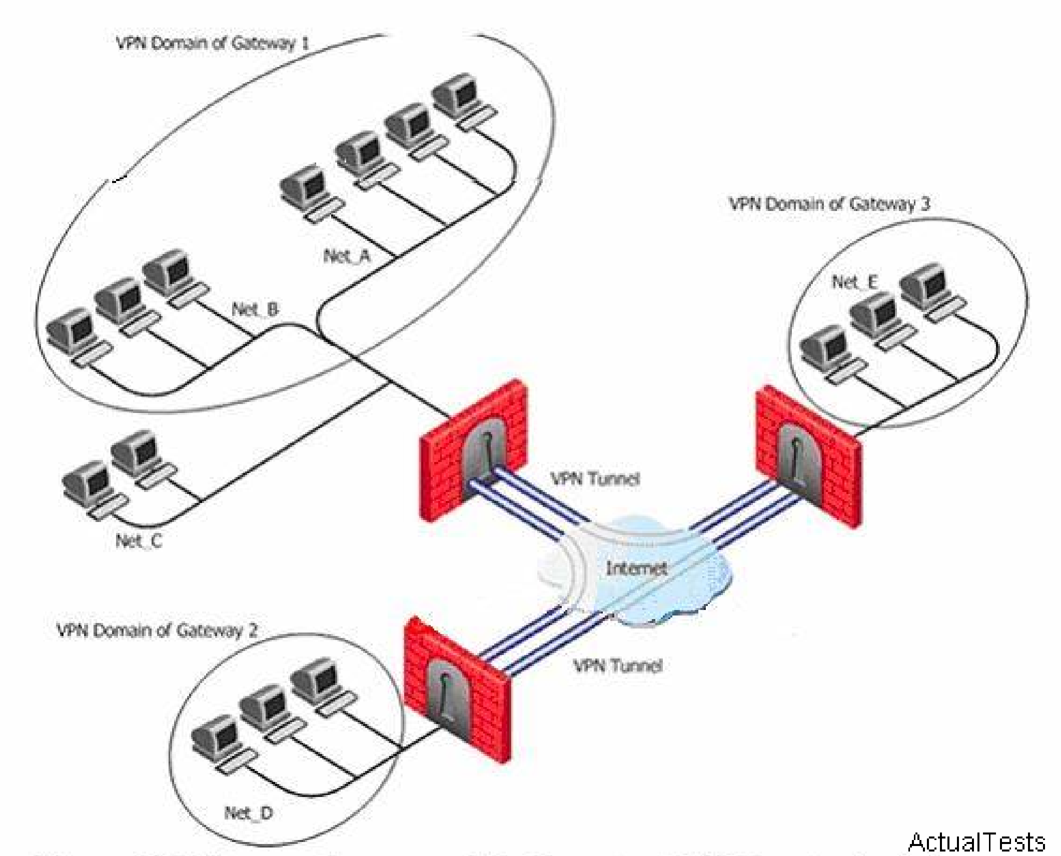
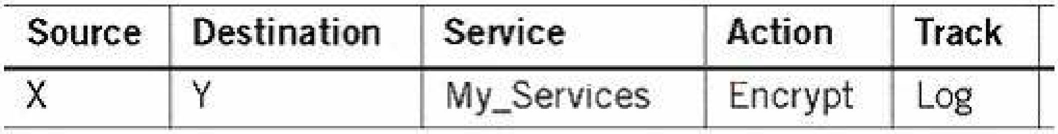


Figure : A VPN between Gateways, and the Encryption (VPN) Domain of each Gateway



Source	Destination	Service	Action	Track
X	Y	My_Services	Encrypt	Log

Figure 2: An Encrypt rule

A. The connection from Net_A to Net_B will be authenticated
B. The gateway 1 will need authentication
C. The connection from Net_A to Net_B will not be encrypted
D. The gateway 1 will drops the connection from Net_A to Net_B
E. The connection from Net_A to Net_B will be encrypted

Answer: C

QUESTION NO: 130

Which type of authentication will require users to TELNET to port port 900 to be authenticated for a service?

A. Session authentication
B. TCP authentication
C. User authentication
D. Client authentication
E. IP authentication

Answer: D

QUESTION NO: 131

The main drawback to tunneling-mode encryption is:

A. The security of the packet size
B. The decrease in the packet size
C. The increase in the packet size
D. The de-cryption of the packet size
E. The quickness of the packet size

Answer: C

QUESTION NO: 132

259 or connect via HTTP at If SecureClient cannot download a new policy from any Policy Server, it will try again after a fixed interval. If the fixed interval is set to default, then the default time is:

A. 8 minutes
B. 4 minutes
C. 5 minutes

D. 3 minutes
E. 10 minutes

Answer: C

QUESTION NO: 133

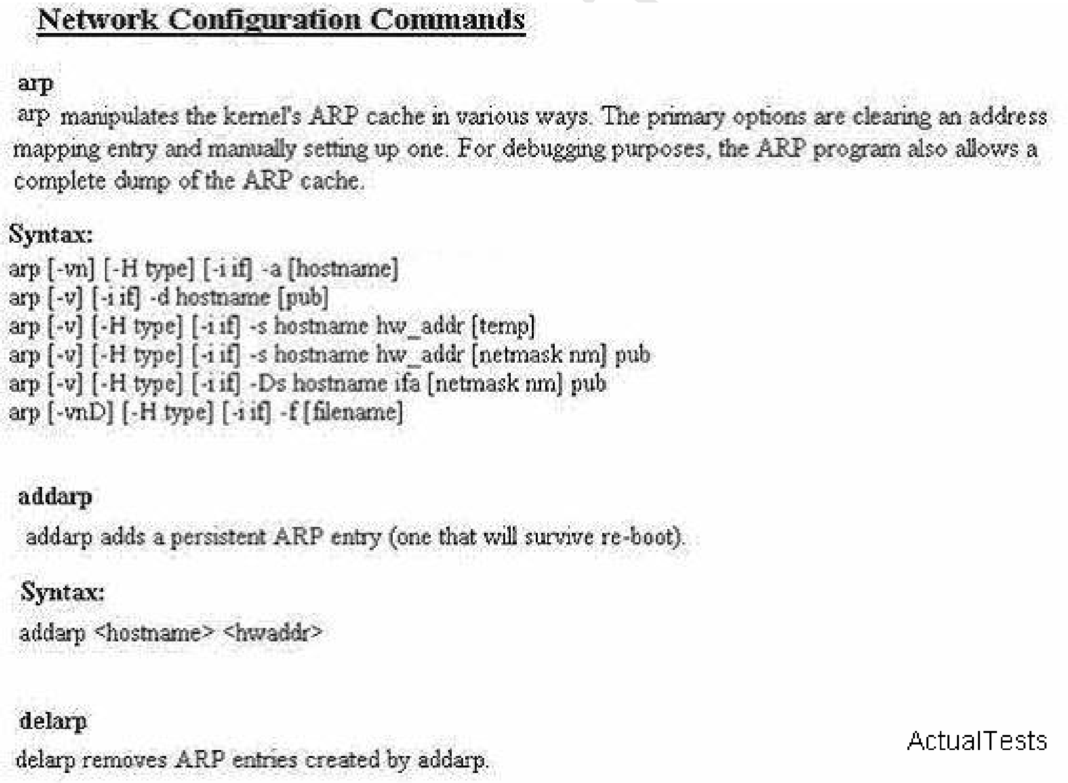
Which of the following Security servers can perform authentication tasks but will not be able perform content security tasks?

A. RLOGIN
B. FTP
C. SMTP
D. HTTP
E. HTTPS

Answer: A

QUESTION NO: 134

Which of the following commands would you use to clear an IP- to- physical address translation table when using SecurePlatform?



Network Configuration Commands

arp

arp manipulates the kernel's ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting up one. For debugging purposes, the ARP program also allows a complete dump of the ARP cache.

Syntax:

```
arp [-vn] [-H type] [-i if] -a [hostname]
arp [-v] [-i if] -d hostname [pub]
arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]
arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub
arp [-v] [-H type] [-i if] -Ds hostname ifa [netmask nm] pub
arp [-vnD] [-H type] [-i if] -f [filename]
```

addarp

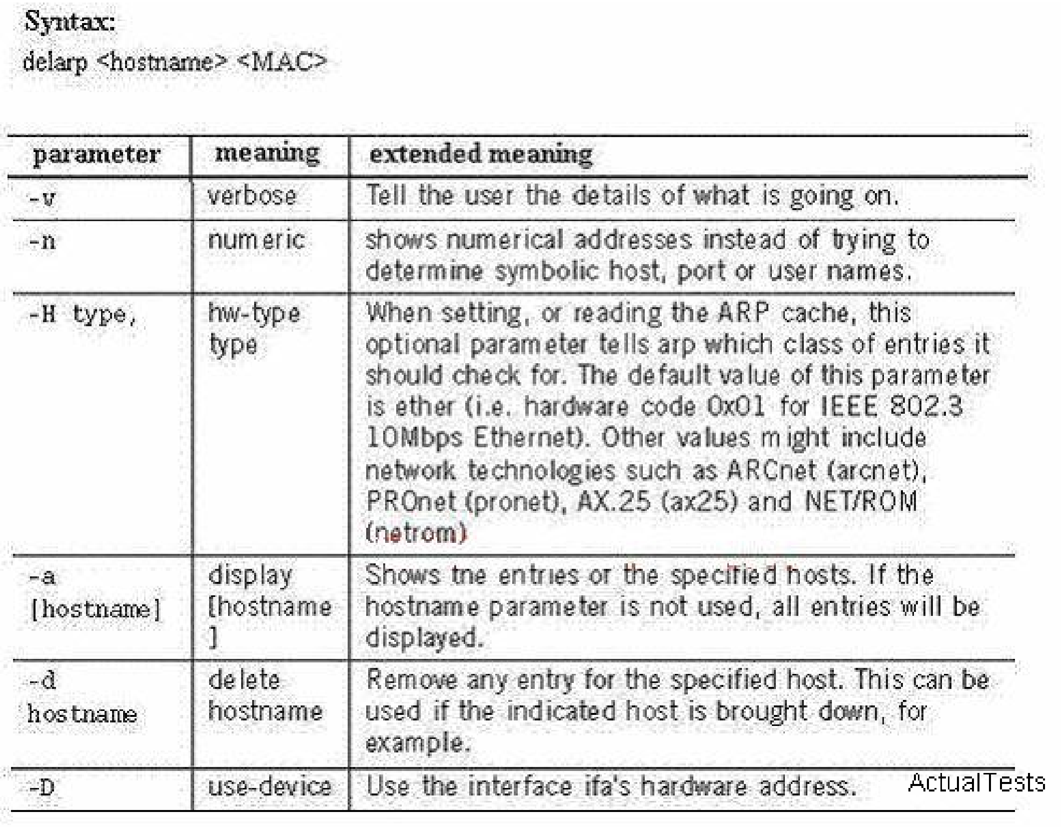
addarp adds a persistent ARP entry (one that will survive re-boot).

Syntax:

```
addarp <hostname> <hwaddr>
```

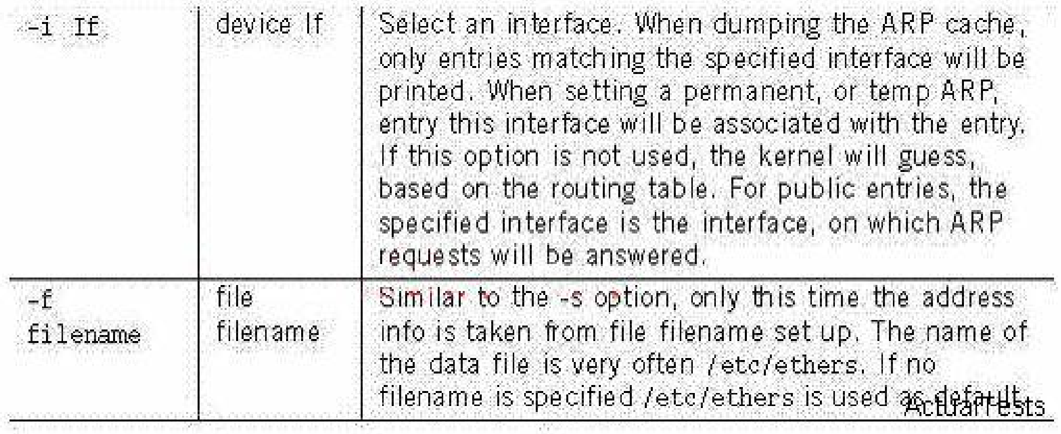
delarp

delarp removes ARP entries created by addarp.

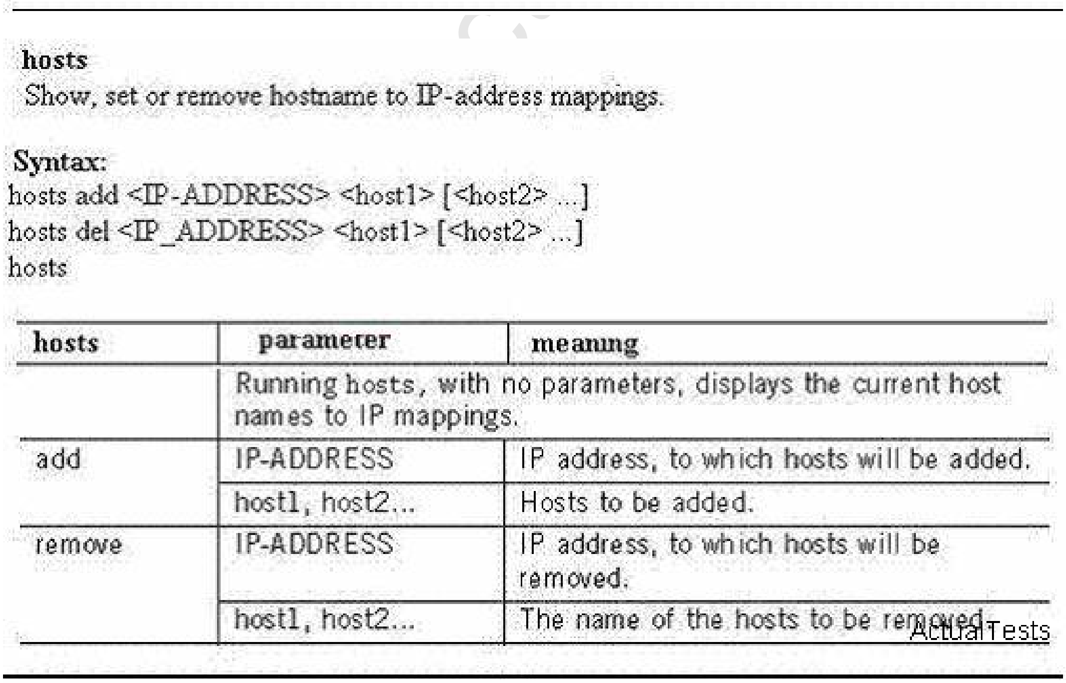


Syntax:
delarp <hostname> <MAC>

parameter	meaning	extended meaning
-v	verbose	Tell the user the details of what is going on.
-n	numeric	shows numerical addresses instead of trying to determine symbolic host, port or user names.
-H type,	hw-type type	When setting, or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet), PROnet (pronet), AX.25 (ax25) and NET/ROM (netrom)
-a [hostname]	display [hostname]	Shows tne entries or the specified hosts. If the hostname parameter is not used, all entries will be displayed.
-d hostname	delete hostname	Remove any entry for the specified host. This can be used if the indicated host is brought down, for example.
-D	use-device	Use the interface ifa's hardware address.



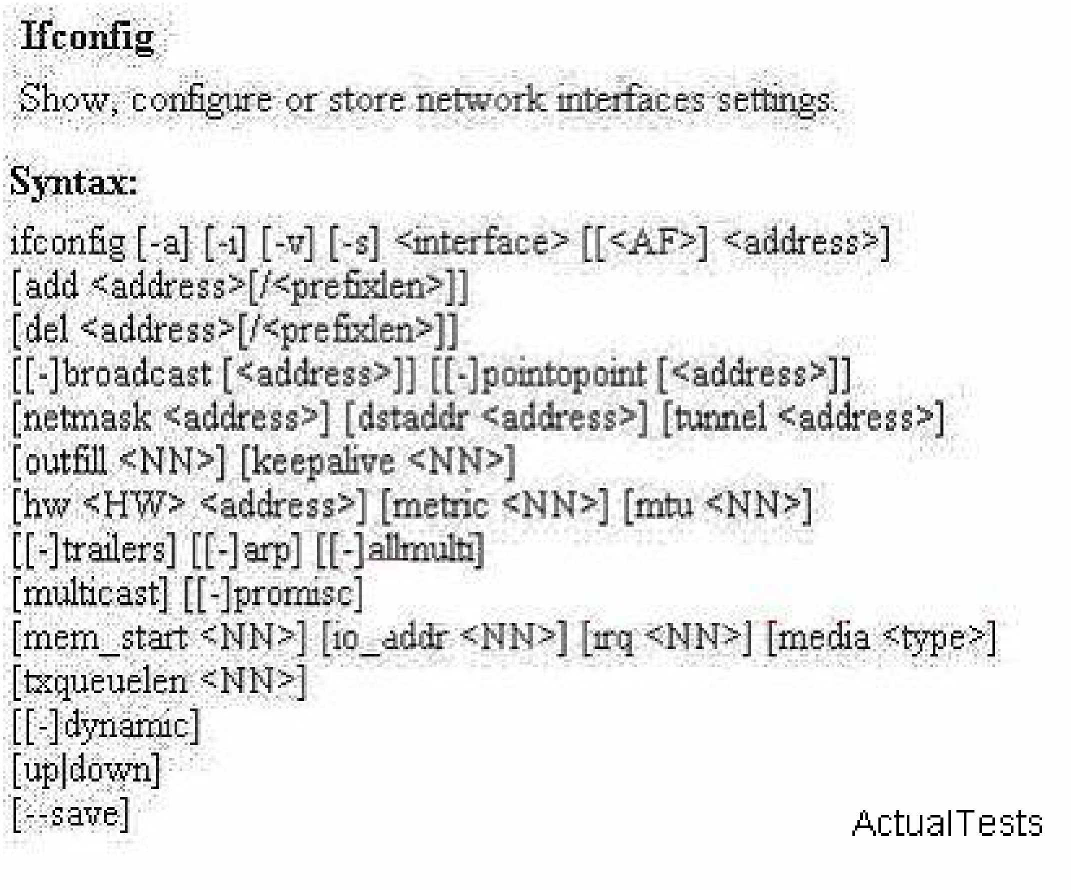
-i If	device If	Select an interface. When dumping the ARP cache, only entries matching the specified interface will be printed. When setting a permanent, or temp ARP, entry this interface will be associated with the entry. If this option is not used, the kernel will guess, based on the routing table. For public entries, the specified interface is the interface, on which ARP requests will be answered.
-f filename	file filename	Similar to the -s option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers. If no filename is specified /etc/ethers is used as default.



hosts
Show, set or remove hostname to IP-address mappings.

Syntax:
hosts add <IP-ADDRESS> <host1> [<host2> ...]
hosts del <IP_ADDRESS> <host1> [<host2> ...]
hosts

hosts	parameter	meaning
	Running hosts, with no parameters, displays the current host names to IP mappings.	
add	IP-ADDRESS	IP address, to which hosts will be added.
	host1, host2...	Hosts to be added.
remove	IP-ADDRESS	IP address, to which hosts will be removed.
	host1, host2...	The name of the hosts to be removed.

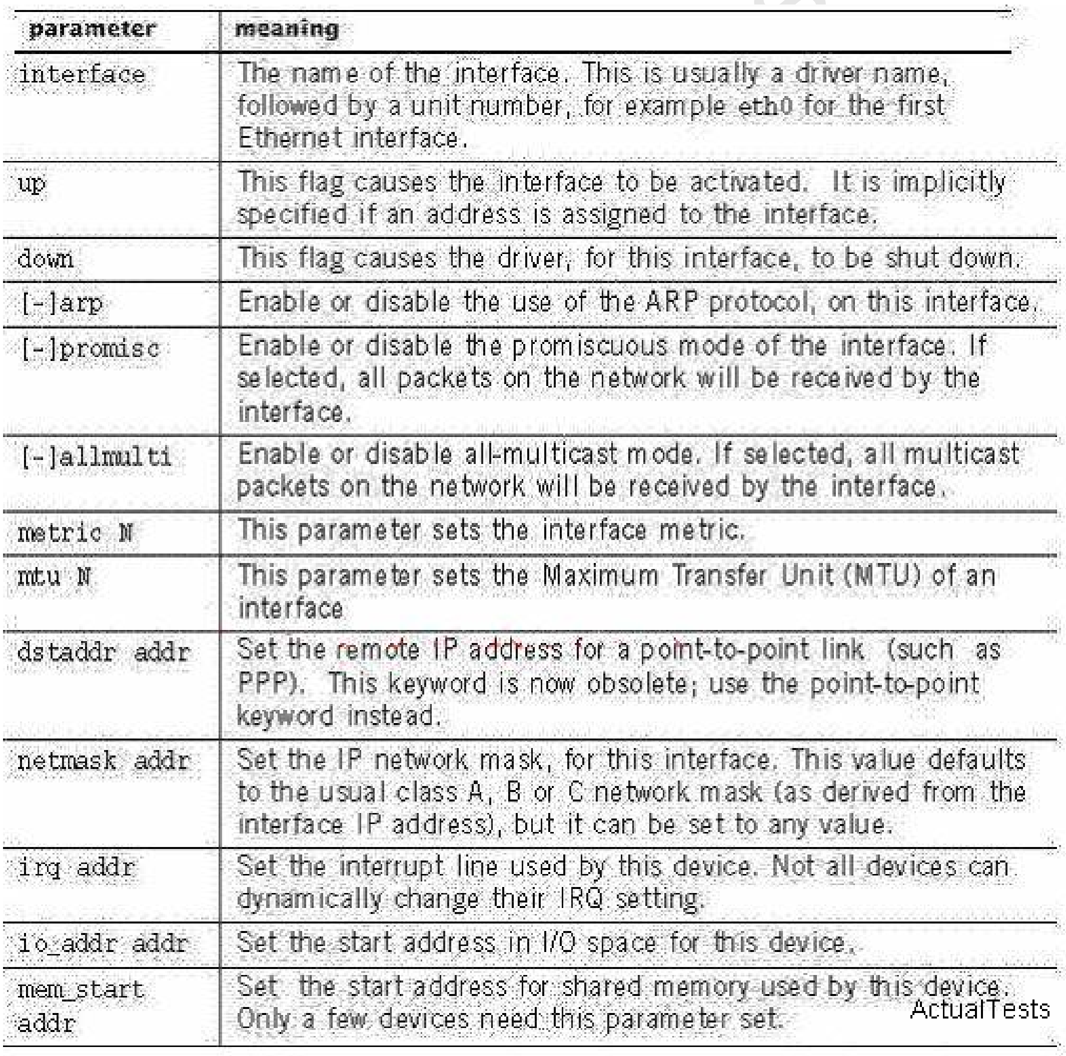


Ifconfig

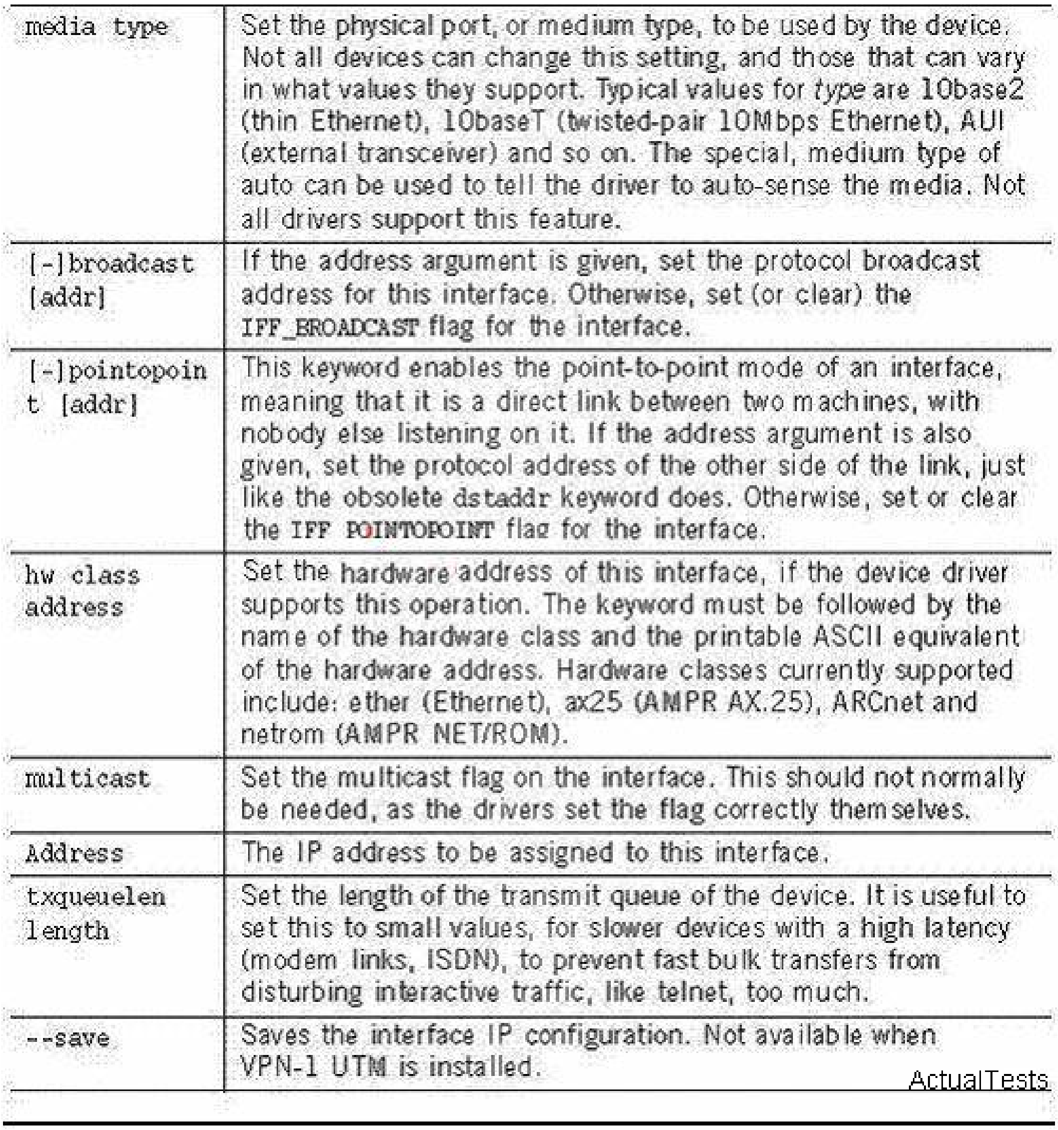
Show, configure or store network interfaces settings.

Syntax:

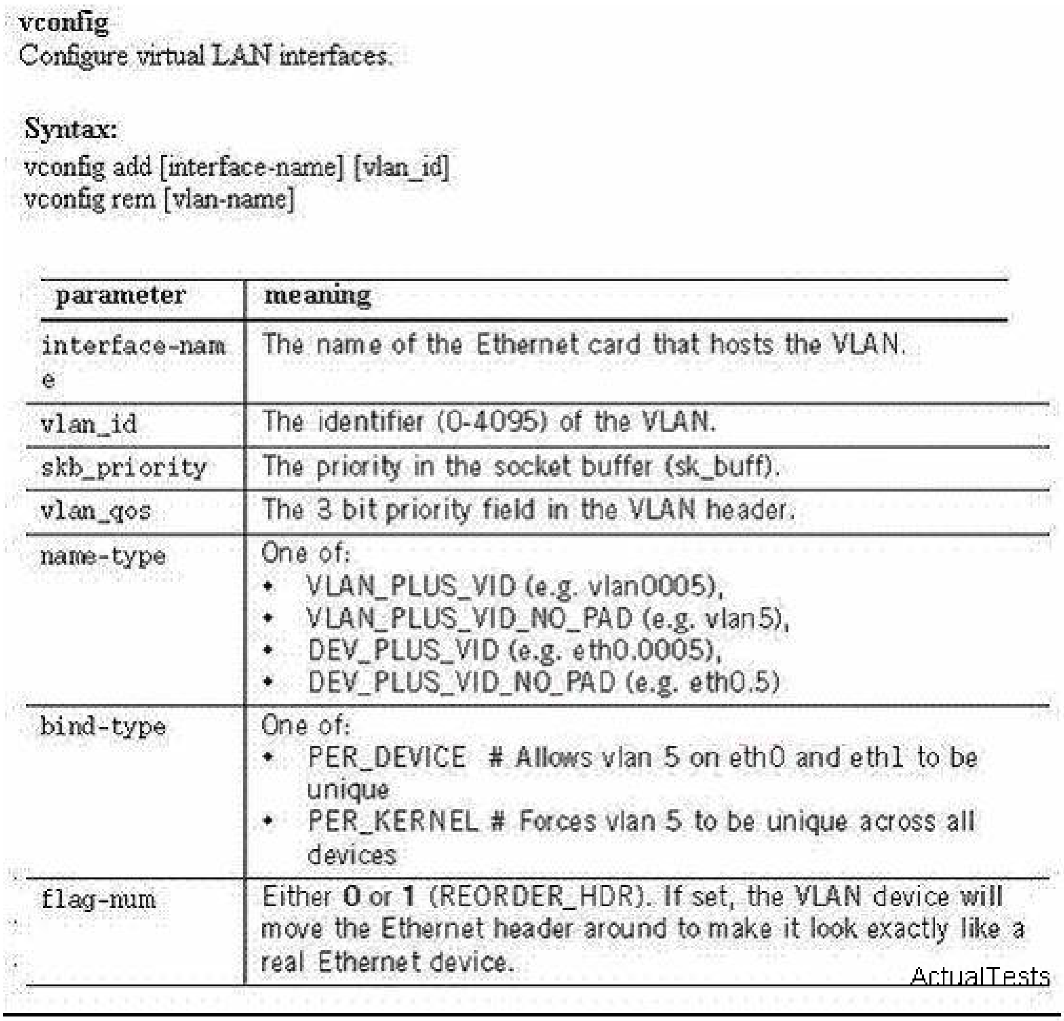
```
ifconfig [-a] [-i] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]] [[-]pointopoint [<address>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [metric <NN>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down]
[--save]
```



parameter	meaning
interface	The name of the interface. This is usually a driver name, followed by a unit number, for example eth0 for the first Ethernet interface.
up	This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.
down	This flag causes the driver, for this interface, to be shut down.
[-]arp	Enable or disable the use of the ARP protocol, on this interface.
[-]promisc	Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.
[-]allmulti	Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.
metric N	This parameter sets the interface metric.
mtu N	This parameter sets the Maximum Transfer Unit (MTU) of an interface
dstaddr addr	Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the point-to-point keyword instead.
netmask addr	Set the IP network mask, for this interface. This value defaults to the usual class A, B or C network mask (as derived from the interface IP address), but it can be set to any value.
irq addr	Set the interrupt line used by this device. Not all devices can dynamically change their IRQ setting.
io_addr addr	Set the start address in I/O space for this device.
mem_start addr	Set the start address for shared memory used by this device. Only a few devices need this parameter set.



media type	Set the physical port, or medium type, to be used by the device. Not all devices can change this setting, and those that can vary in what values they support. Typical values for *type* are 10base2 (thin Ethernet), 10baseT (twisted-pair 10Mbps Ethernet), AUI (external transceiver) and so on. The special, medium type of auto can be used to tell the driver to auto-sense the media. Not all drivers support this feature.
[-]broadcast [addr]	If the address argument is given, set the protocol broadcast address for this interface. Otherwise, set (or clear) the **IFF_BROADCAST** flag for the interface.
[-]pointopoint [addr]	This keyword enables the point-to-point mode of an interface, meaning that it is a direct link between two machines, with nobody else listening on it. If the address argument is also given, set the protocol address of the other side of the link, just like the obsolete dstaddr keyword does. Otherwise, set or clear the **IFF POINTOPOINT** flag for the interface.
hw class address	Set the hardware address of this interface, if the device driver supports this operation. The keyword must be followed by the name of the hardware class and the printable ASCII equivalent of the hardware address. Hardware classes currently supported include: ether (Ethernet), ax25 (AMPR AX.25), ARCnet and netrom (AMPR NET/ROM).
multicast	Set the multicast flag on the interface. This should not normally be needed, as the drivers set the flag correctly themselves.
Address	The IP address to be assigned to this interface.
txqueuelen length	Set the length of the transmit queue of the device. It is useful to set this to small values, for slower devices with a high latency (modem links, ISDN), to prevent fast bulk transfers from disturbing interactive traffic, like telnet, too much.
--save	Saves the interface IP configuration. Not available when VPN-1 UTM is installed.



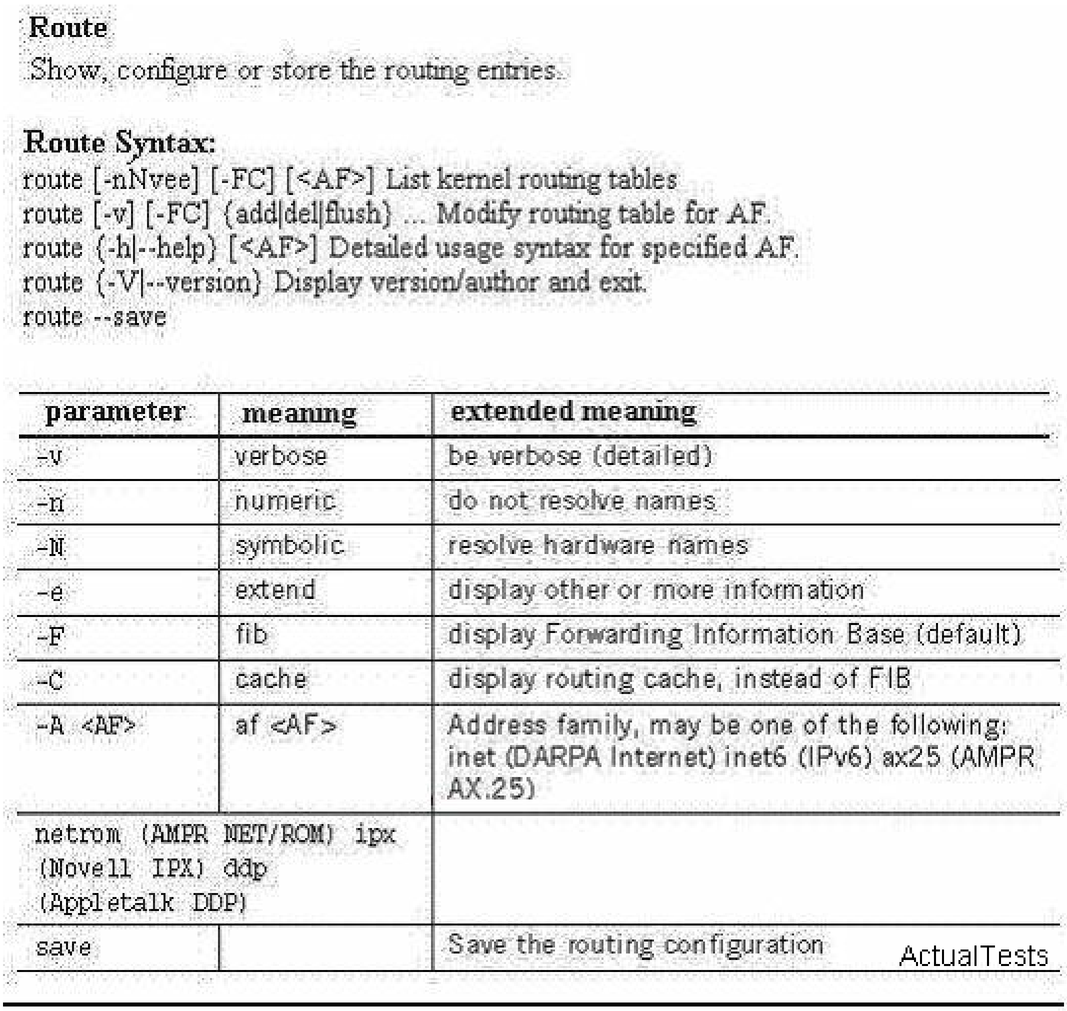
vconfig

Configure virtual LAN interfaces.

Syntax:

```
vconfig add [interface-name] [vlan_id]
vconfig rem [vlan-name]
```

parameter	meaning
interface-name	The name of the Ethernet card that hosts the VLAN.
vlan_id	The identifier (0-4095) of the VLAN.
skb_priority	The priority in the socket buffer (sk_buff).
vlan_qos	The 3 bit priority field in the VLAN header.
name-type	One of: • VLAN_PLUS_VID (e.g. vlan0005), • VLAN_PLUS_VID_NO_PAD (e.g. vlan5), • DEV_PLUS_VID (e.g. eth0.0005), • DEV_PLUS_VID_NO_PAD (e.g. eth0.5)
bind-type	One of: • PER_DEVICE # Allows vlan 5 on eth0 and eth1 to be unique • PER_KERNEL # Forces vlan 5 to be unique across all devices
flag-num	Either **0** or **1** (REORDER_HDR). If set, the VLAN device will move the Ethernet header around to make it look exactly like a real Ethernet device.



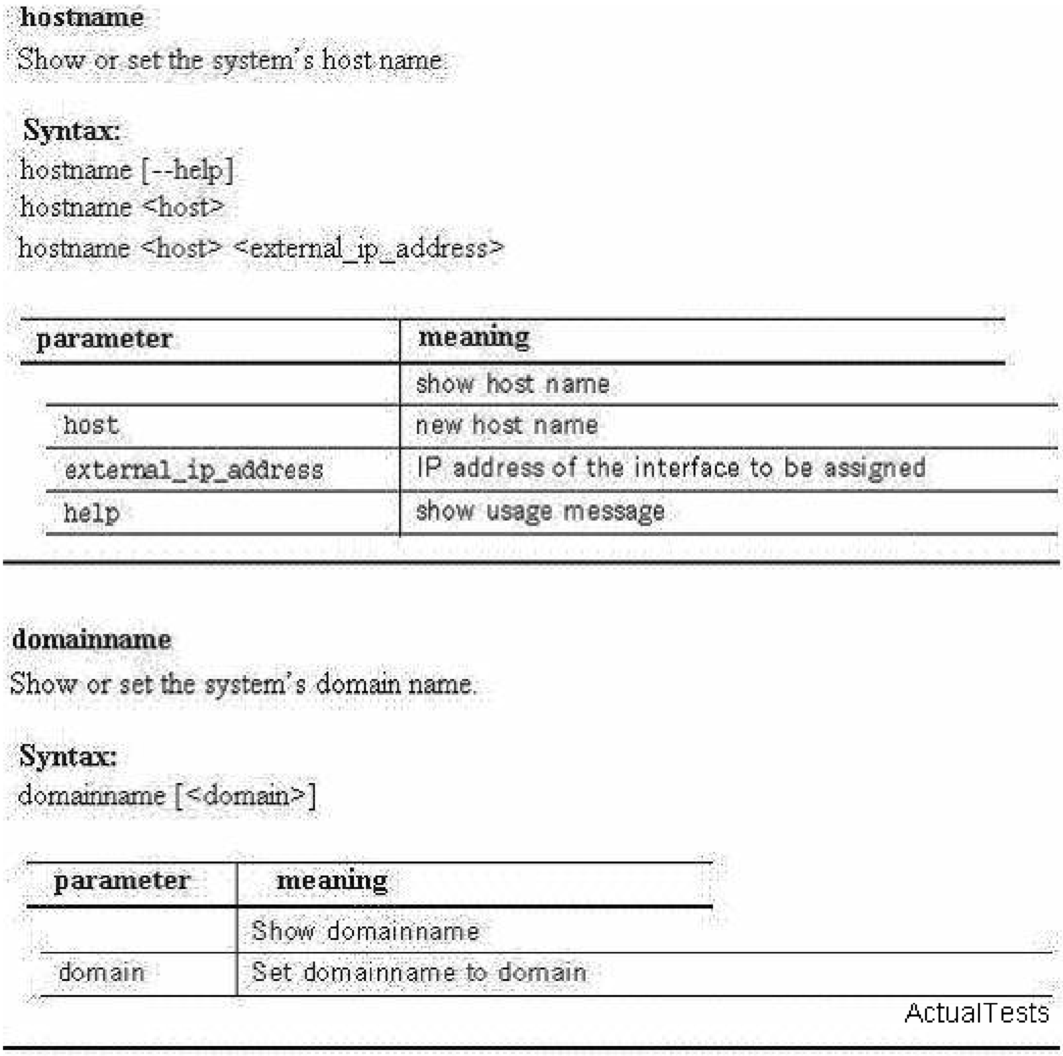
Route

Show, configure or store the routing entries.

Route Syntax:

route [-nNvee] [-FC] [<AF>] List kernel routing tables
route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.
route {-h|--help} [<AF>] Detailed usage syntax for specified AF.
route {-V|--version} Display version/author and exit.
route --save

parameter	meaning	extended meaning
-v	verbose	be verbose (detailed)
-n	numeric	do not resolve names
-N	symbolic	resolve hardware names
-e	extend	display other or more information
-F	fib	display Forwarding Information Base (default)
-C	cache	display routing cache, instead of FIB
-A <AF>	af <AF>	Address family, may be one of the following: inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)		
save		Save the routing configuration



hostname

Show or set the system's host name.

Syntax:

```
hostname [--help]
hostname <host>
hostname <host> <external_ip_address>
```

parameter	meaning
	show host name
host	new host name
external_ip_address	IP address of the interface to be assigned
help	show usage message

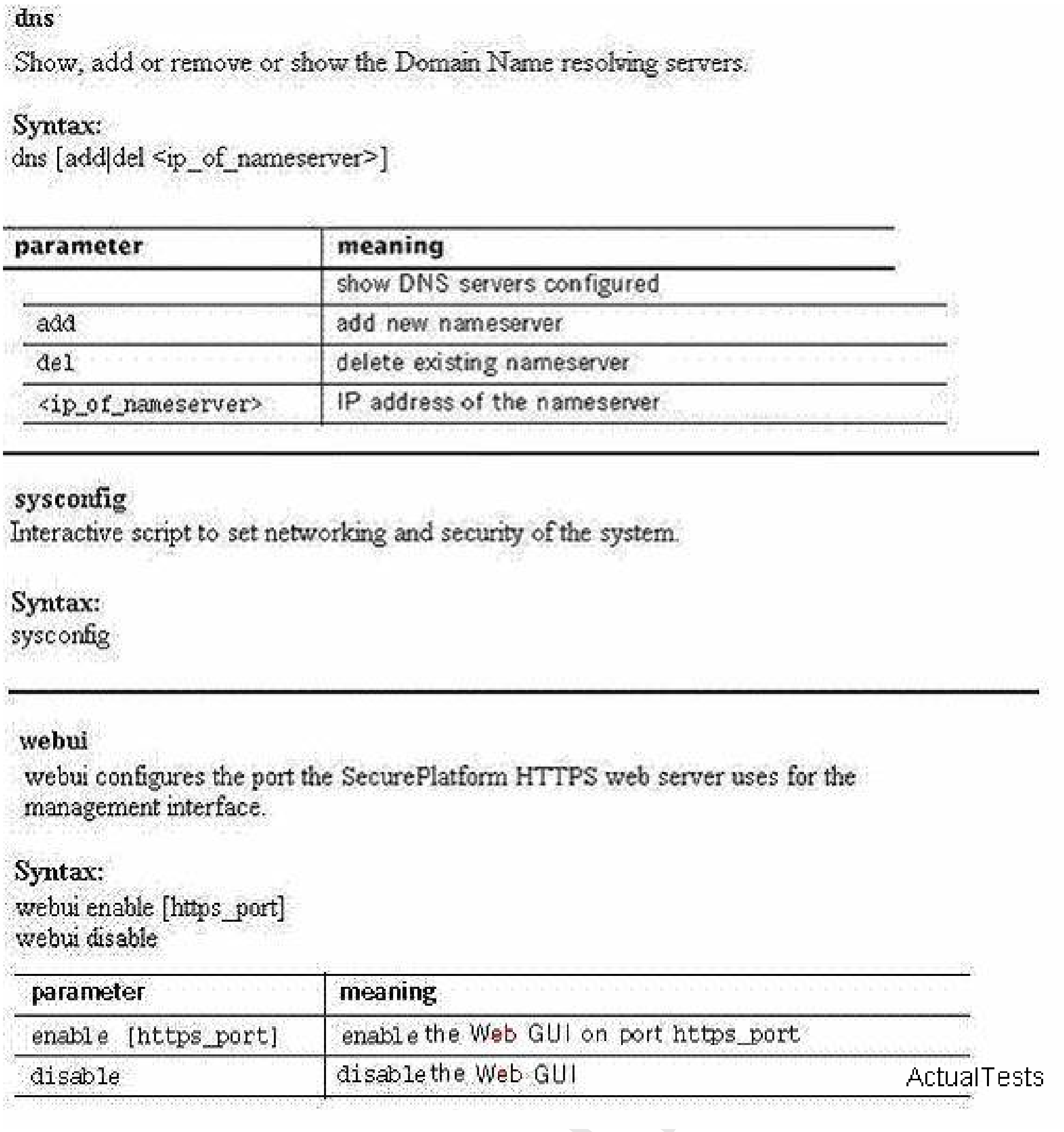
domainname

Show or set the system's domain name.

Syntax:

```
domainname [<domain>]
```

parameter	meaning
	Show domainname
domain	Set domainname to domain



dns

Show, add or remove or show the Domain Name resolving servers.

Syntax:

dns [add|del <ip_of_nameserver>]

parameter	meaning
	show DNS servers configured
add	add new nameserver
del	delete existing nameserver
<ip_of_nameserver>	IP address of the nameserver

sysconfig

Interactive script to set networking and security of the system.

Syntax:

sysconfig

webui

webui configures the port the SecurePlatform HTTPS web server uses for the management interface.

Syntax:

webui enable [https_port]
webui disable

parameter	meaning
enable [https_port]	enable the Web GUI on port https_port
disable	disable the Web GUI

A. hosts
B. arp
C. ipconfig
D. traceroute
E. vconfig

Answer: B

QUESTION NO: 135

You are in SecurePlatform and want to configure a new virtual LAN. If the name of NIC card that host is 3C579 and the Vlan identifier is 10, what command would you use to achieve this? Note: If wrong answer(s) is/are chosen, see the diagram for correct answer(s) and explanation.

A. vconfig [interface-name] [vlan_id]
B. vconfig add 3C579 10
C. vconfigure add [3C579] [10]

D. config add 3C579 10
E. config add [3C579] [10]

Answer: B

QUESTION NO: 136

What command will you use to configure network interfaces settings?

A. configure
B. config
C. ipconfig
D. arp
E. ifconfig

Answer: E

QUESTION NO: 137

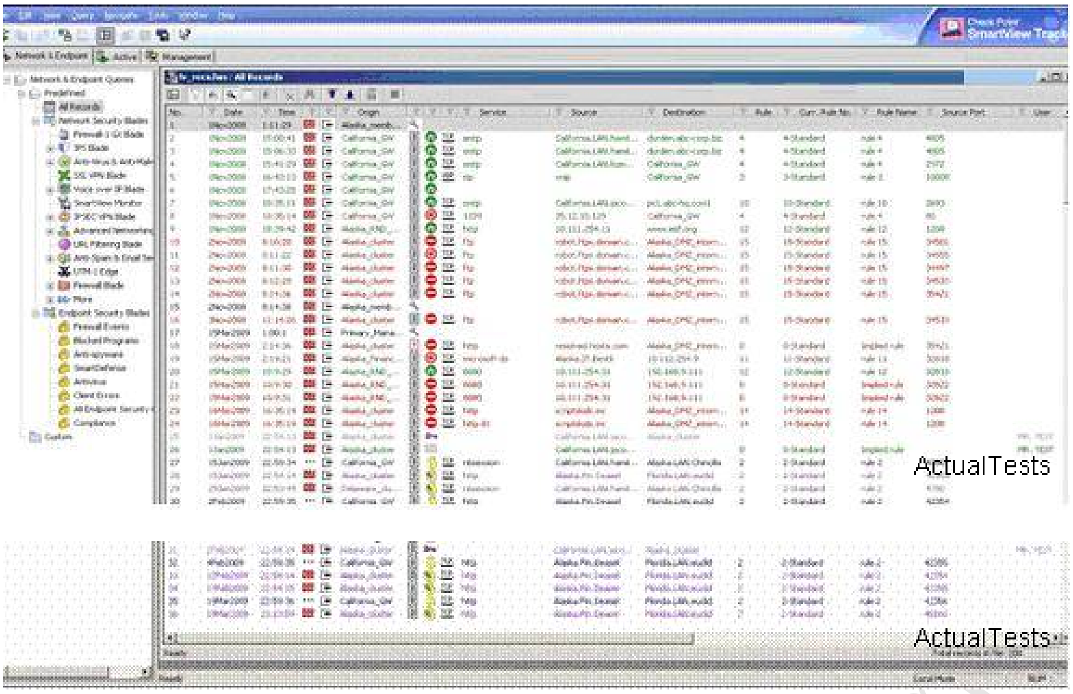
A user was initiating client authentication session by beginning a TELNET session on port 900. What do you think might be wrong?

A. Nothing is wrong.
B. The authentication type should be changed to session authentication.
C. The user was TELNET- ing at wrong port. The user should use port 295.
D. The user was TELNET- ing at the wrong port. The user should use port 259.
E. The authentication type should be changed to user authentication.

Answer: E

QUESTION NO: 138

Study the diagram and answer the question below. What type of client GUI is shown in the diagram?



A. Rule Base GUI
B. SmartView Tracker
C. Security Status GUI
D. Security SmartDashboard
E. SmartView Status

Answer: B

QUESTION NO: 139

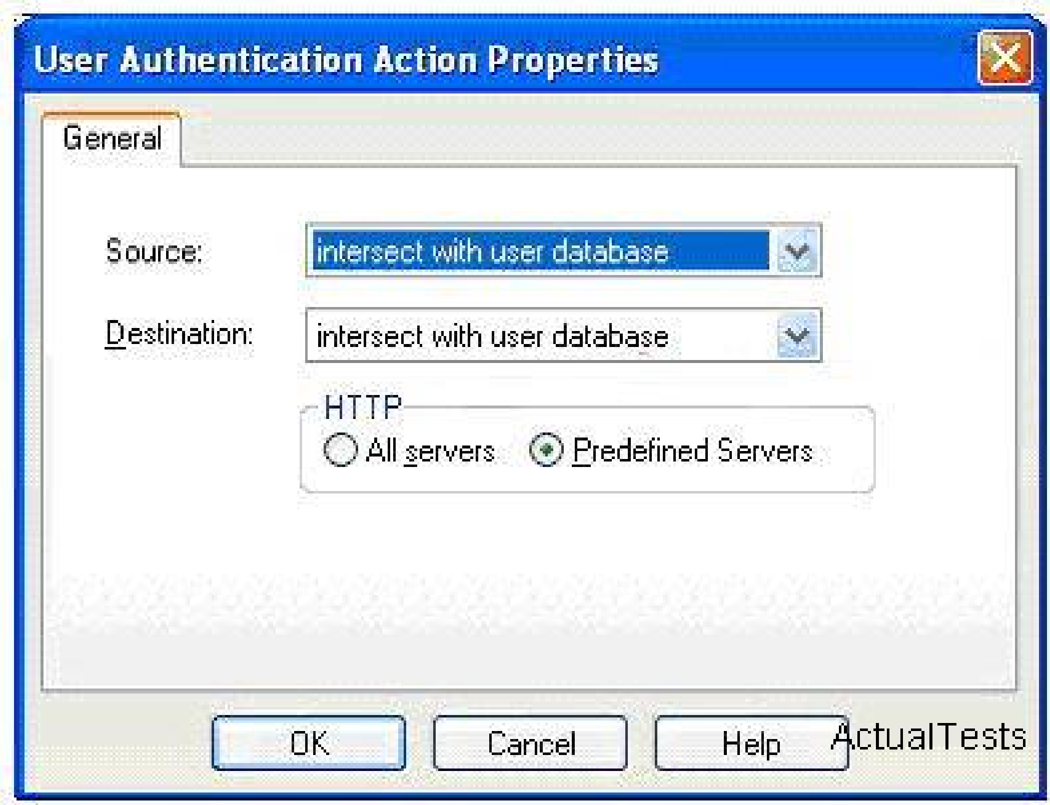
SmartUpdate is the primary tool used for upgrading Check Point gateways. When upgrading your gateway, what feature will you choose if want to upgrade all packages installed on your gateway?

A. Minimal Effort Upgrade
B. Add Package to Repository
C. Upgrading the Gateway
D. Upgrade All Packages
E. Zero Effort

Answer: D

QUESTION NO: 140

The allowed Sources in the Location tab of the User Properties window specify that the user to whom a User Authentication rule is being applied is not allowed access from the source address, while the rule itself allows access. To resolve this conflict, you will have to:



User Authentication Action Properties

Source: intersect with user database

Destination: intersect with user database

HTTP: ○ All servers ● Predefined Servers

A. Create an administrator account in place of the user account
B. Install your rule base
C. Re-create the user object
D. Select Allowed Destinations field in the Network Object Properties
E. Configure User Authentication Action Properties screen

Answer: E

QUESTION NO: 141

What services are supported by client authentication?

A. All services
B. FTP
C. RLOGIN
D. HTTP and FTP
E. TELNET, HTTP and FTP
F. HTTPS, HTTP and FTP

Answer: A

QUESTION NO: 142

In what situation will you consider and deploy policy management conventions?

A. No available answer

B. In some situations

C. In some rear situations

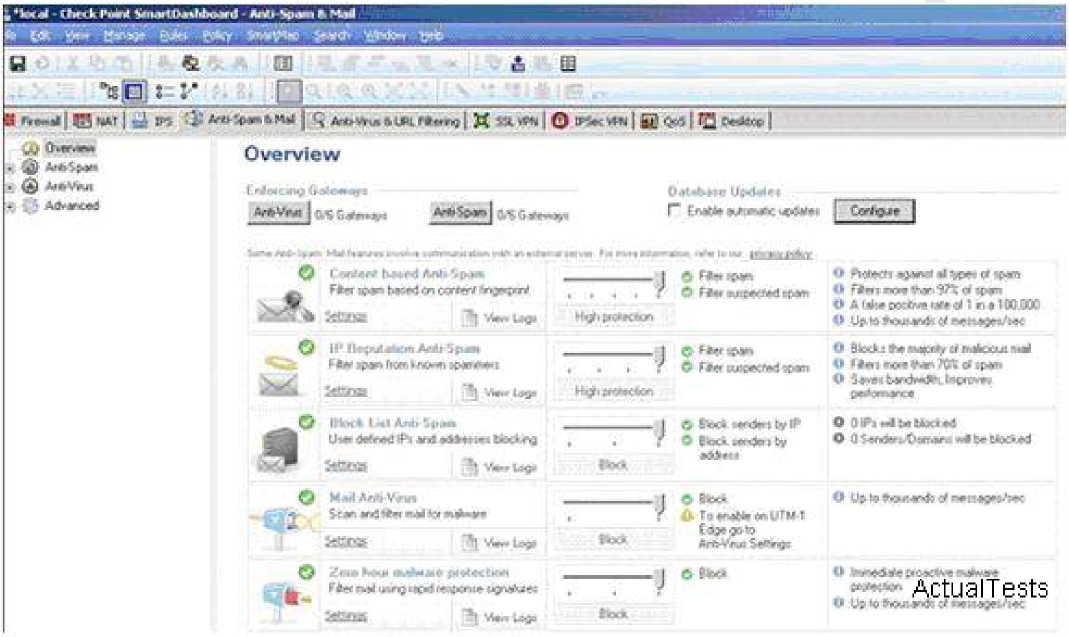
D. In all situations

E. Not in any situation

Answer: D

QUESTION NO: 143

On the Anti-Spam & Mail tab of the SmartDashboard, you can configure which of the following:


*local - Check Point SmartDashboard - Anti-Spam & Mail
File Edit View Manage Rules Policy SmartMap Search Window Help
Firewall
NAT
IPS
Anti-Spam & Mail
Anti-Virus & URL Filtering
SSL VPN
IPSec VPN
QoS
Desktop
Overview
Anti-Spam
Anti-Virus
Advanced
ActualTests

Overview

Enforcing Gateways

Anti-Virus 0/5 Gateways

Anti-Spam 0/5 Gateways

Database Updates

□ Enable automatic updates Configure

Some Anti-Spam Mail features involve communication with an external server. For more information, refer to our privacy policy

Content based Anti-Spam
Filter spam based on content fingerprint
Settings View Logs
High protection
Filter spam
Filter suspected spam
Protects against all types of spam
Filters more than 97% of spam
A false positive rate of 1 in a 100,000
Up to thousands of messages/sec

IP Reputation Anti-Spam
Filter spam from known spammers
Settings View Logs
High protection
Filter spam
Filter suspected spam
Blocks the majority of malicious mail
Filters more than 70% of spam
Saves bandwidth, Improves performance

Block List Anti-Spam
User defined IPs and addresses blocking
Settings View Logs
Block
Block senders by IP
Block senders by address
0 IPs will be blocked
0 Senders/Domains will be blocked

Mail Anti-Virus
Scan and filter mail for malware
Settings View Logs
Block
Block
To enable on UTM-1 Edge go to Anti-Virus Settings
Up to thousands of messages/sec

Zero hour malware protection
Filter mail using rapid response signatures
Settings View Logs
Block
Block
Immediate proactive malware protection
Up to thousands of messages/sec

A. Select gateways that enforce Anti-Virus checking

B. Enable automatic updates

C. View settings and logs

D. Select gateways that enforce Anti-Spam protection

E. View alerts

Answer: A,B,C,D

QUESTION NO: 144

Which of the following is true of Symmetric Encryption?

A. Both communicating parties using Symmetric Encryption use different keys for encryption and decryption

B. The material used to build these keys must be exchanged in a secure manner
C. Both communicating parties using Symmetric Encryption use the same key for encryption and decryption
D. The material used to build these keys does not have to be exchanged in a secure manner
E. Information can be securely exchanged only if the key belongs exclusively to the communicating parties

Answer: B,C,E

QUESTION NO: 145

Your company was unable to obtain more than four legal internet IP addresses from your ISP, and as an administrator you decide to use a single IP address for internet access. What will you implement to allow all your internal users to access the internet with a single IP address?

A. Source Static NAT
B. Undynamic NAT
C. Static NAT
D. Hide NAT
E. Source Destination NAT

Answer: D

QUESTION NO: 146

Which of the following are external authentication scheme that are supported by R70? Select all the correct answers.

A. SecurID
B. Operating System Password
C. TACACS
D. Check Point Password
E. RADIUS

Answer: A,C,E

QUESTION NO: 147

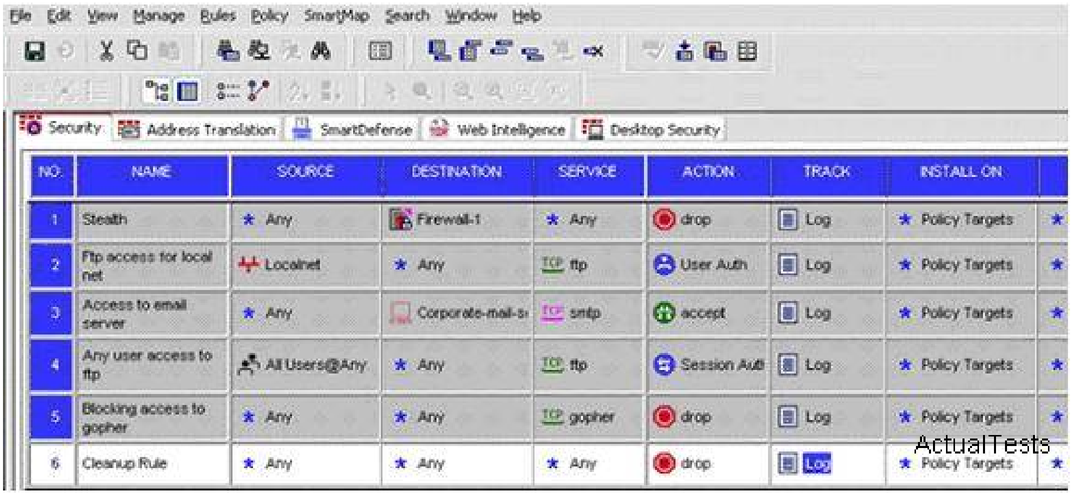
VPN routing provides a way of controlling how VPN traffic is directed. There are two methods for doing this. Which of these two methods will Route VPN traffic based on the encryption domain behind each Gateway in the community?

A. Dynamic Based VPN
B. Domain Based VPN
C. Static Based VPN
D. Route Based VPN
E. Routing Based VPN

Answer: B

QUESTION NO: 148

Study the diagram and answer the question below. What rule would allow access from your local network using FTP service with User Authentication as a method of authentication?



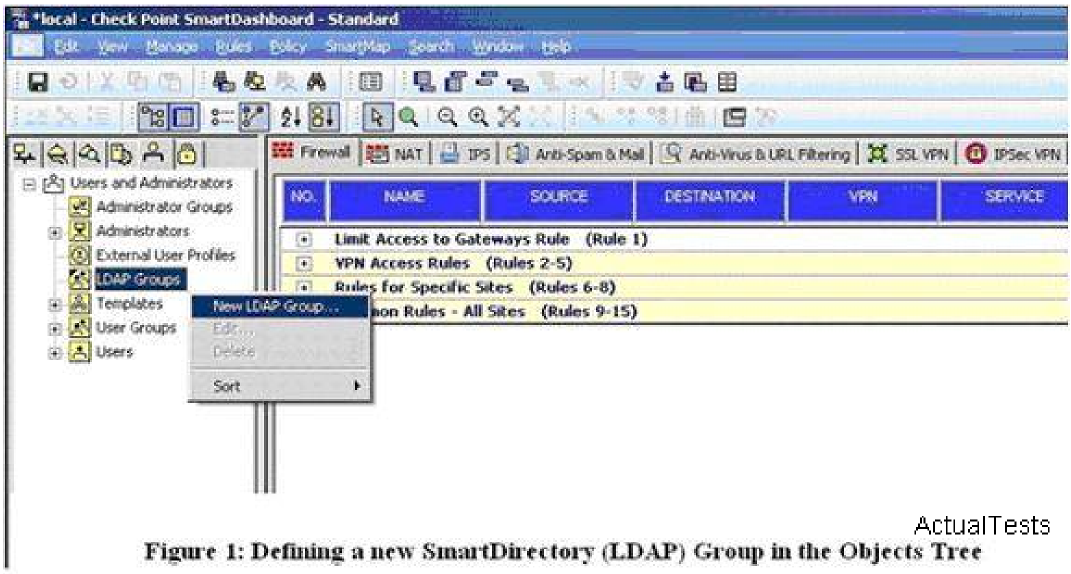
NO.	NAME	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	
1	Stealth	★ Any	Firewall-1	★ Any	drop	Log	★ Policy Targets	★
2	Ftp access for local net	Localnet	★ Any	TCP ftp	User Auth	Log	★ Policy Targets	★
3	Access to email server	★ Any	Corporate-mail-s	TCP smtp	accept	Log	★ Policy Targets	★
4	Any user access to ftp	All Users@Any	★ Any	TCP ftp	Session Auth	Log	★ Policy Targets	★
5	Blocking access to gopher	★ Any	★ Any	TCP gopher	drop	Log	★ Policy Targets	★
6	Cleanup Rule	★ Any	★ Any	★ Any	drop	Log	★ Policy Targets	★

A. 5
B. 1
C. 3
D. 2
E. 4

Answer: D

QUESTION NO: 149

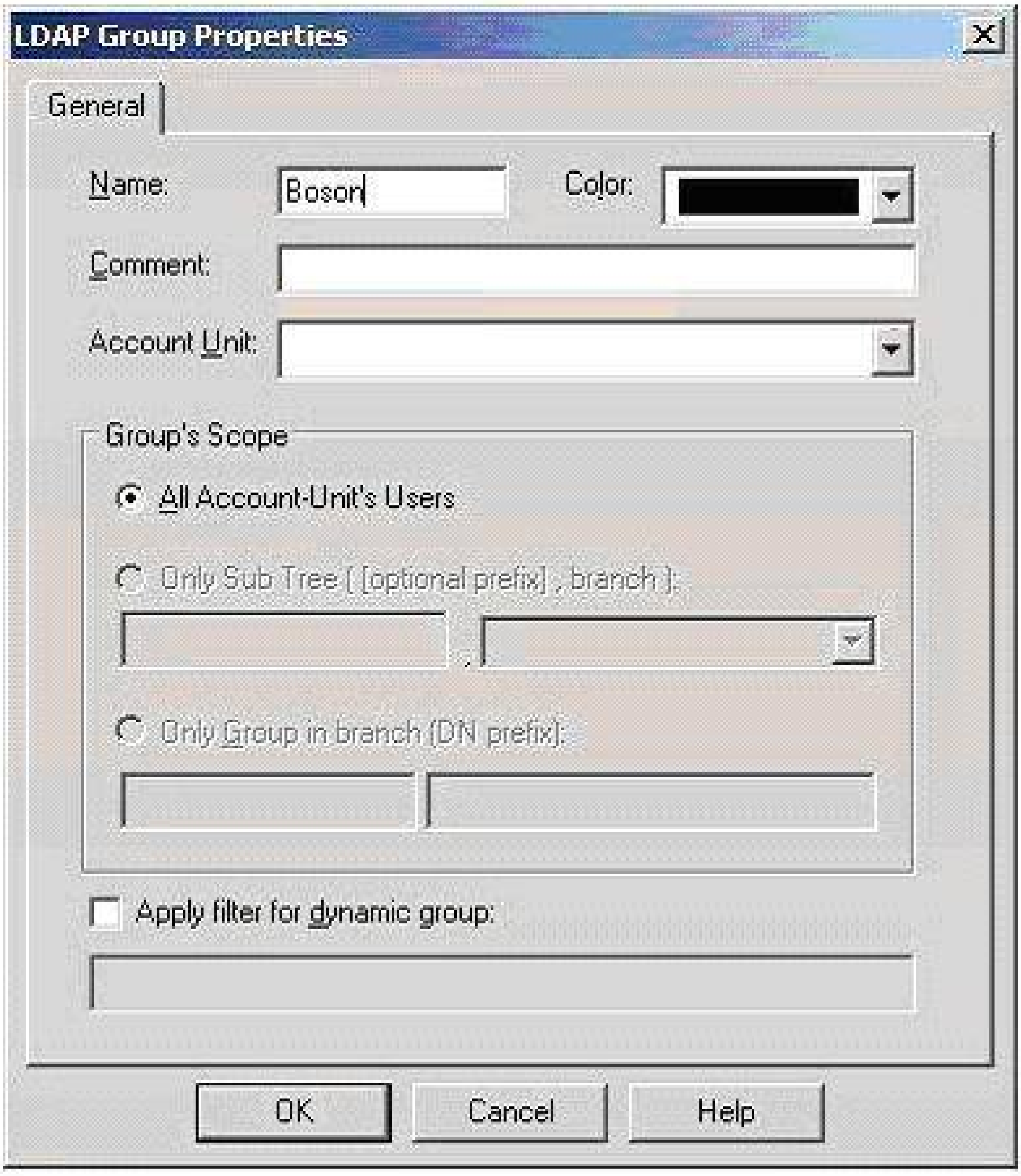
Which of the following is true regarding SmartDirectory (LDAP) Groups? Select all the correct answers.


*local - Check Point SmartDashboard - Standard
File Edit View Manage Rules Policy SmartMap Search Window Help
Firewall NAT IPS Anti-Spam & Mail Anti-Virus & URL Filtering SSL VPN IPSec VPN
Users and Administrators
Administrator Groups
Administrators
External User Profiles
LDAP Groups
Templates
User Groups
Users
New LDAP Group...
Edit...
Delete
Sort

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE

Limit Access to Gateways Rule (Rule 1)
VPN Access Rules (Rules 2-5)
Rules for Specific Sites (Rules 6-8)
...mon Rules - All Sites (Rules 9-15)

Figure 1: Defining a new SmartDirectory (LDAP) Group in the Objects Tree



Name: Boson
Color:
Comment:
Account Unit:

Group's Scope

● All Account-Unit's Users

○ Only Sub Tree [[optional prefix] , branch]:

○ Only Group in branch (DN prefix):

□ Apply filter for dynamic group:

Figure 2: LDAP Group Properties Window

A. SmartDirectory (LDAP) users can be grouped logically

B. SmartDirectory (LDAP) groups are created in order classify users within certain group types

C. SmartDirectory (LDAP) users can be created with SmartView Monitor GUI

D. SmartDirectory (LDAP) users can be grouped dynamically according to a dynamic filter

E. Once SmartDirectory (LDAP) groups arecreated, they can be applied in various policy rules

Answer: A,B,D,E

QUESTION NO: 150

The default cluster administrator user name is:

A. Supervisor

B. Adminstrator

C. cadmin

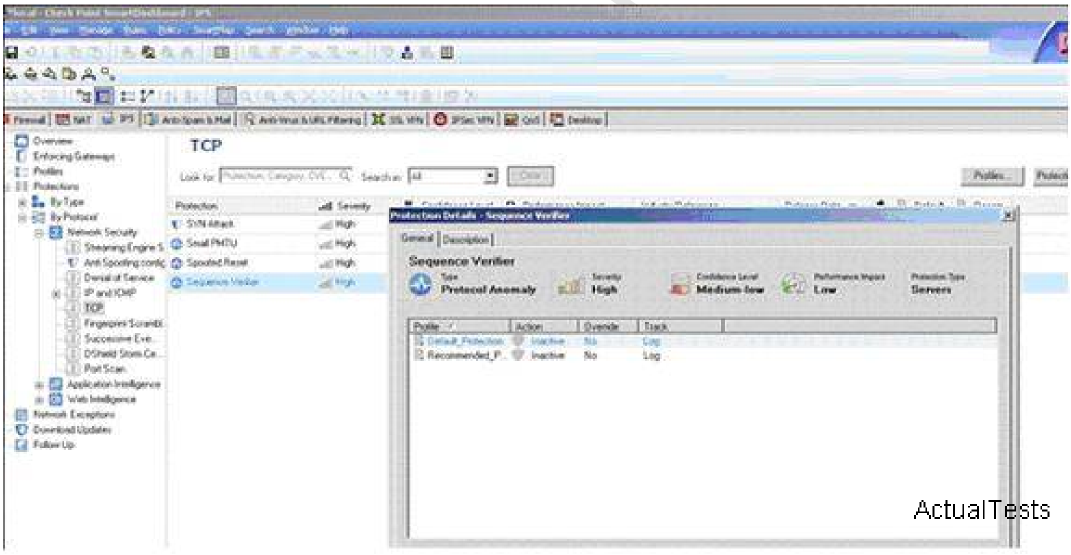
D. Admin

E. clusterAdmin

Answer: C

QUESTION NO: 151

What will be the consequence of disabling TCP state check in the IPS tab?

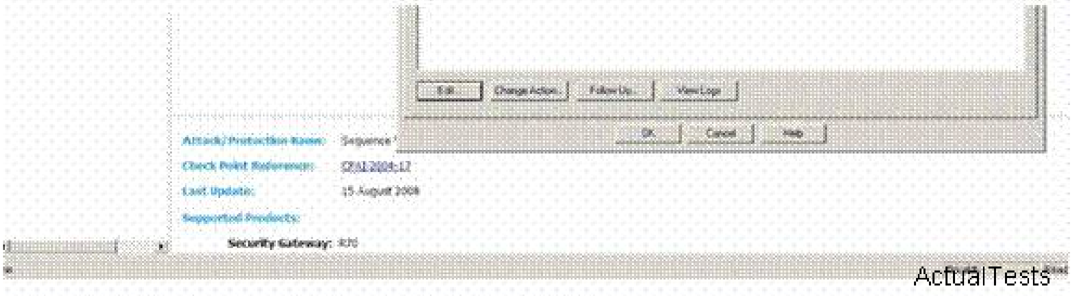


Protection	Severity
SYN Attack	High
Small PMTU	High
Spoofed Reset	High
Sequence Verifier	High

Sequence Verifier

Type: Protocol Anomaly
Severity: High
Confidence Level: Medium-low
Performance Impact: Low
Protection Type: Servers

Profile	Action	Override	Track
Default_Protection	Inactive	No	Log
Recommended_P...	Inactive	No	Log



Attack/Protection Name: Sequence

Check Point Reference: CPAI-2004-17

Last Update: 15 August 2008

Supported Products:

Security Gateway: R70

Figure 1: IPS Tab > Protections > By Protocols > Network Security > TCP

A. This will boost your overall Firewall performance

B. This will disable your IPS

C. This will disable your firewall

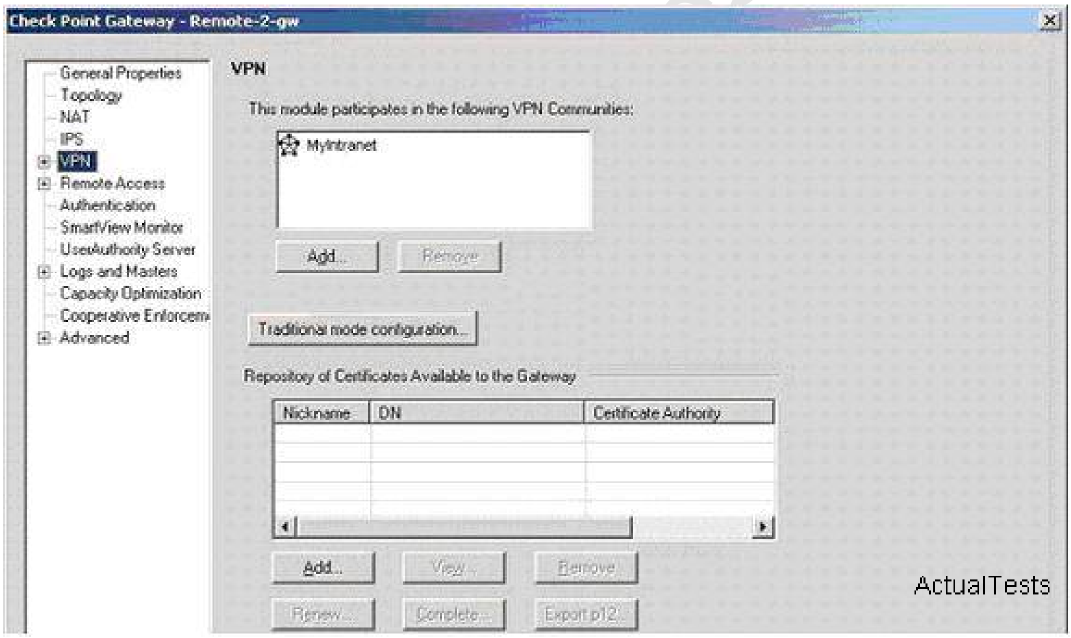
D. This will have adverse effect on your Firewall performance

E. This will degrade your overall Firewall performance

Answer: A

QUESTION NO: 152

The Internal Certificate Authority (ICA) is a fully featured, internal authentication server that is installed on a Security Management Server. The ICA cannot be used in which of the following situations?



VPN

This module participates in the following VPN Communities:

MyIntranet

Repository of Certificates Available to the Gateway

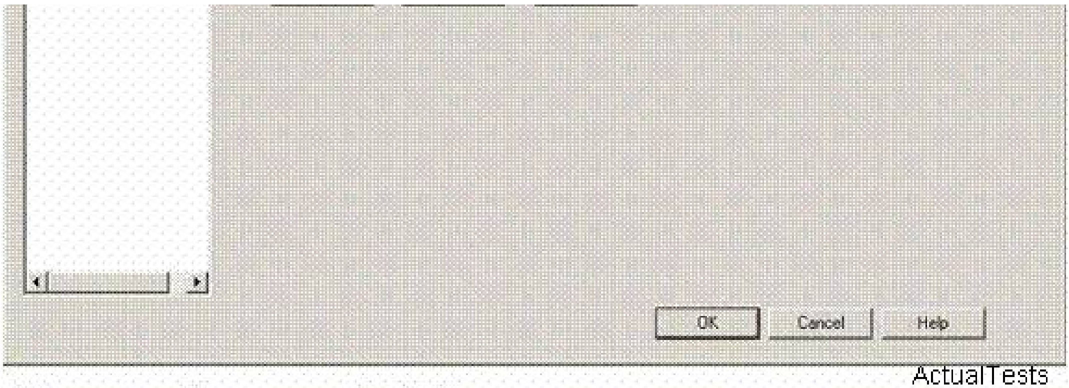
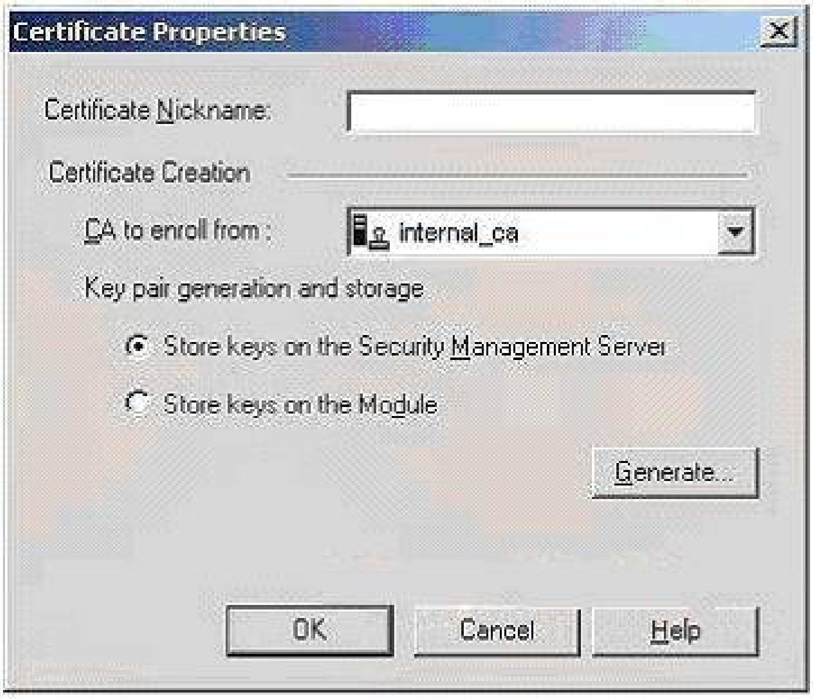


Figure 1: Gateway - VPN Page



Certificate Properties

Certificate Nickname:

Certificate Creation

CA to enroll from : internal_ca

Key pair generation and storage

● Store keys on the Security Management Server

○ Store keys on the Module

Figure 2: Certificate Properties screen

A. The CA creates the profile file and then give it to the user

B. The user logs on the SmartDashboard to request a certificate. If successful the certificate is email to the user

C. The user creates a certificate registration request file, then transfers the file via mail or FTP to the CA

D. The user creates a profile on their workstation using SecureClient

E. The user registers with the CA using a web browser and then exports the certificate and private key for use in other applications

Answer: B

QUESTION NO: 153

Check Point Nodes communicate with other Check Point Nodes by means of control connections. What feature is used by control connections to ensure strong authentication between Check Point Nodes?

A. Implied Rules
B. Diffie-Hellman
C. FireWall Implied Rules
D. Explicit Rules
E. Secure Internal Communication

Answer: E

QUESTION NO: 154

SmartUpdate has two tabs. Which tab will show you the Operating Systems that are installed on the Check Point Security Gateways which are being managed by the Security Management server?

A. Dialogue tab
B. Operating System tab
C. Windows tab
D. Licenses tab
E. Packages tab

Answer: E

QUESTION NO: 155

The Diffie-Hellman algorithm builds an encryption key known as a "shared secret" from the private key of one party and the:

A. Combination of public and private keys of the other
B. Privatekey of the other
C. Encryption key of the other
D. Combination of private and public keys of the other
E. Public key of the other

Answer: E

QUESTION NO: 156

For VPN routing to succeed:

A. A single rule must be created in the Security Policy Rule base and must cover traffic in outbound direction
B. Two rules must be created in the Security Policy Rulebase, one must cover traffic in inbound direction and the other in outbound direction
C. A single rule must be created in the Security Policy Rule base and must cover traffic in both directions
D. A single rule must be created in the Security Policy Rule base and must cover traffic in inbound direction
E. Two rules must be created in the Security Policy Rule base and must cover traffic in both directions

Answer: C

QUESTION NO: 157

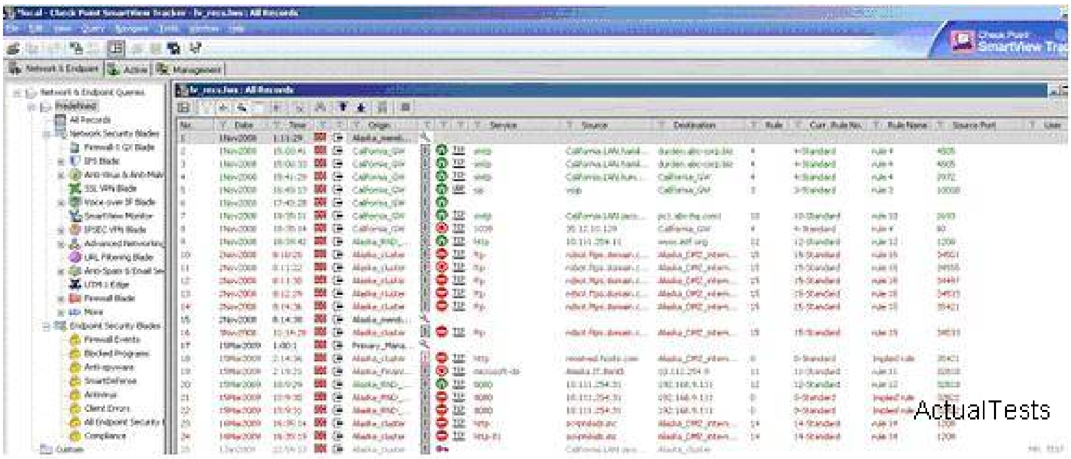
The advantages of Session Authentication over other types of authentication are:

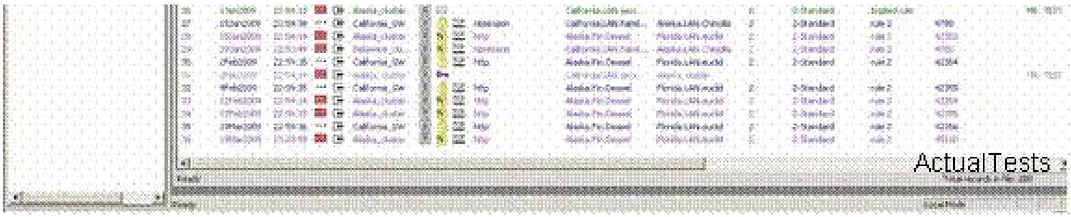
A. Less resource intensive
B. Smoother connection
C. High resource intensive
D. You do not necessarily have install Session Authentication agent
E. Heavy connection

Answer: A,B

QUESTION NO: 158

What are the three pre-defined selection view modes in SmartView Tracker GUI?





A. Active Mode
B. Network & Endpoint Mode
C. Active status
D. Connection Mode
E. Management Mode

Answer: A,B,E

QUESTION NO: 159

How does Gateway implement Transparent Authentication?

A. When a user does not have to explicitly connect to the Gateway to perform the authentication before continuing to the destination
B. When a user authenticated for FTP, HTTP, RLOGIN and TELNET at the same time
C. When a user have to explicitly connect to the Gateway Module to perform the authentication before continuing to the destination
D. When a user have to directly connect to the Gateway to perform the authentication before continuing to the destination
E. When a user authenticated to FTP service only

Answer: A

QUESTION NO: 160

When an entity receives a certificate from another entity, it must: (Select all the correct answers)

A. VPN verifies the validity of the certificate's use
B. Verify the certificate signature
C. Verify that the certificate chain has not expired
D. Verify that the certificate is generated by the internal Security Management Server
E. Verify that the certificate chain is not revoked

Answer: A,B,C,E

QUESTION NO: 161

The scheduling Status pane of the WebUI displays which of the following information?

A. Start at
B. Recur every
C. Backup to
D. Restored from
E. Enabled

Answer: A,B,C,E

QUESTION NO: 162

Security Management server supports two main VPN topologies: Meshed and

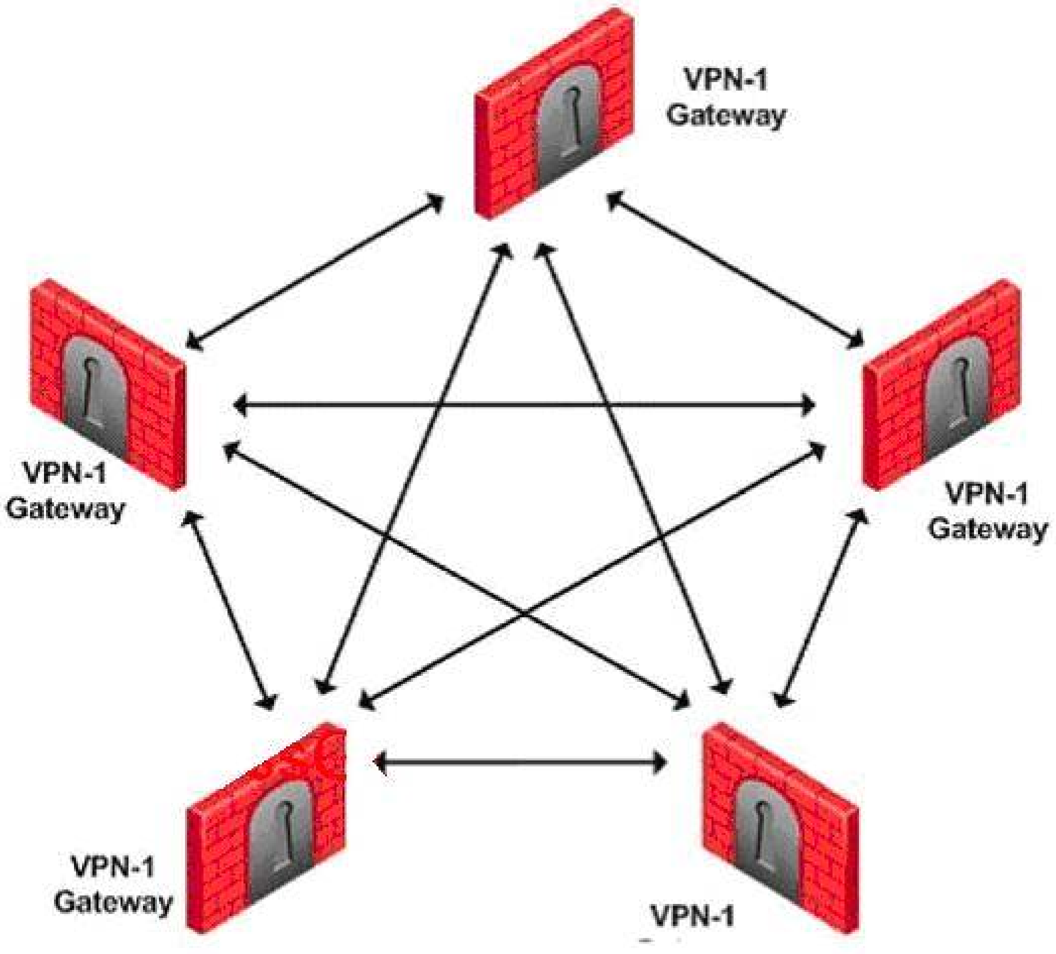


Figure 1: Basic Meshed community

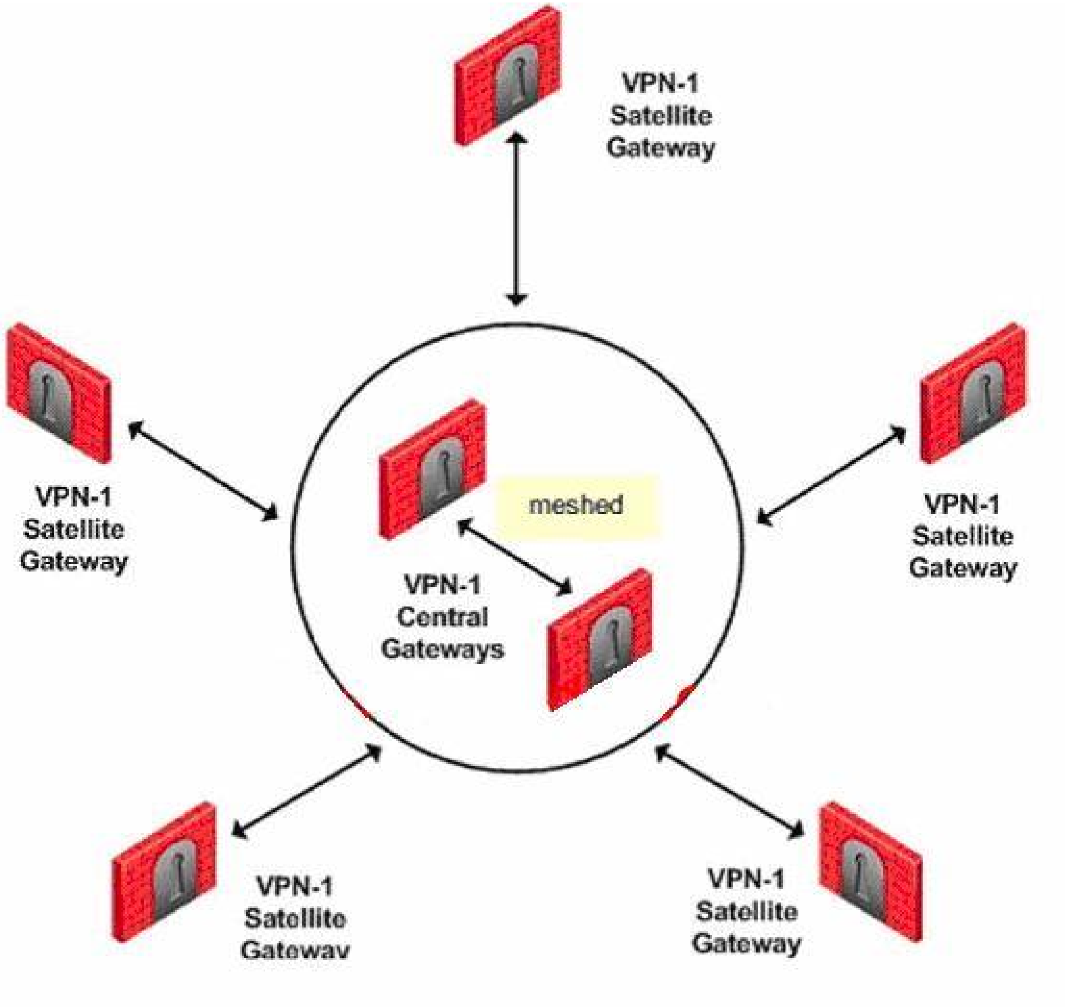
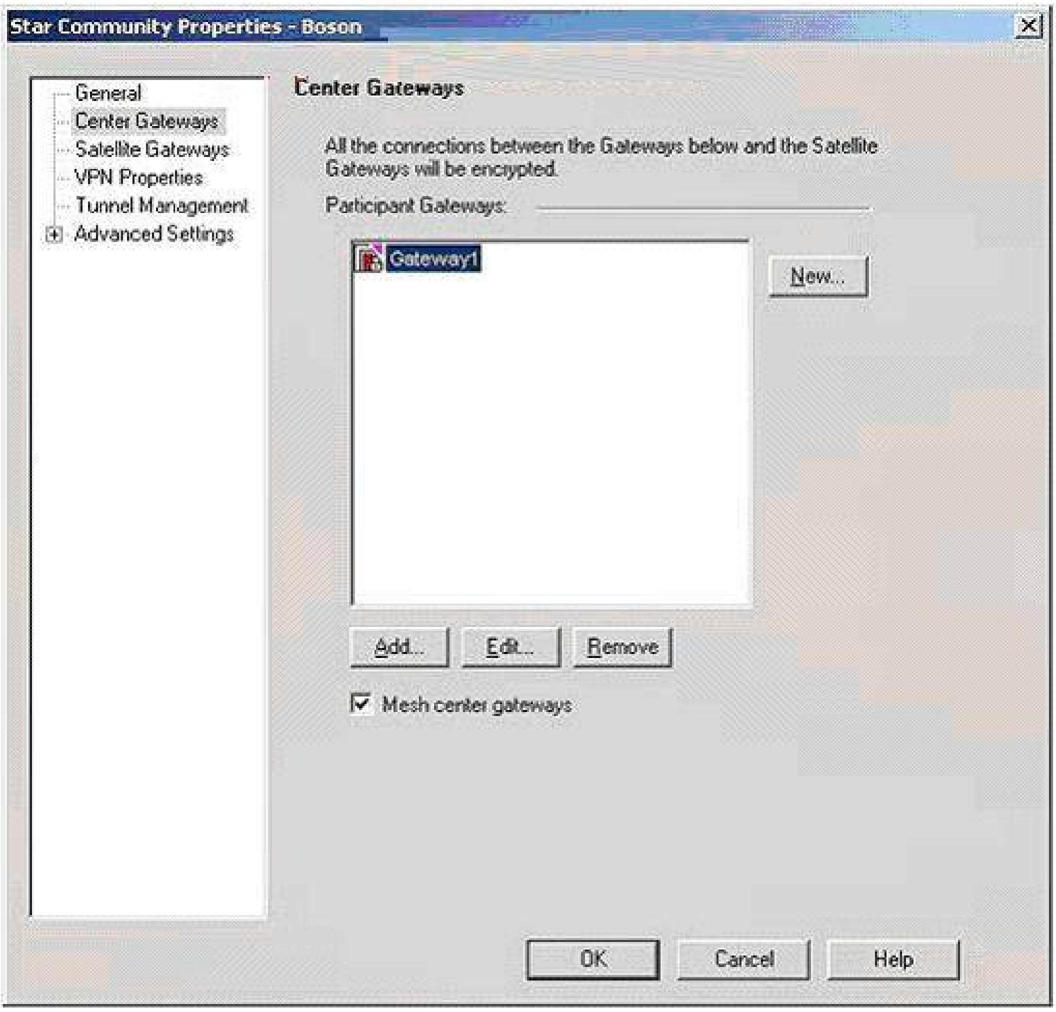


Figure 2: Star VPN community



Center Gateways

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

Participant Gateways:

Gateway1

☑ Mesh center gateways

Figure 3: Star Community Properties window

A. Ethernet

B. Star

C. Token

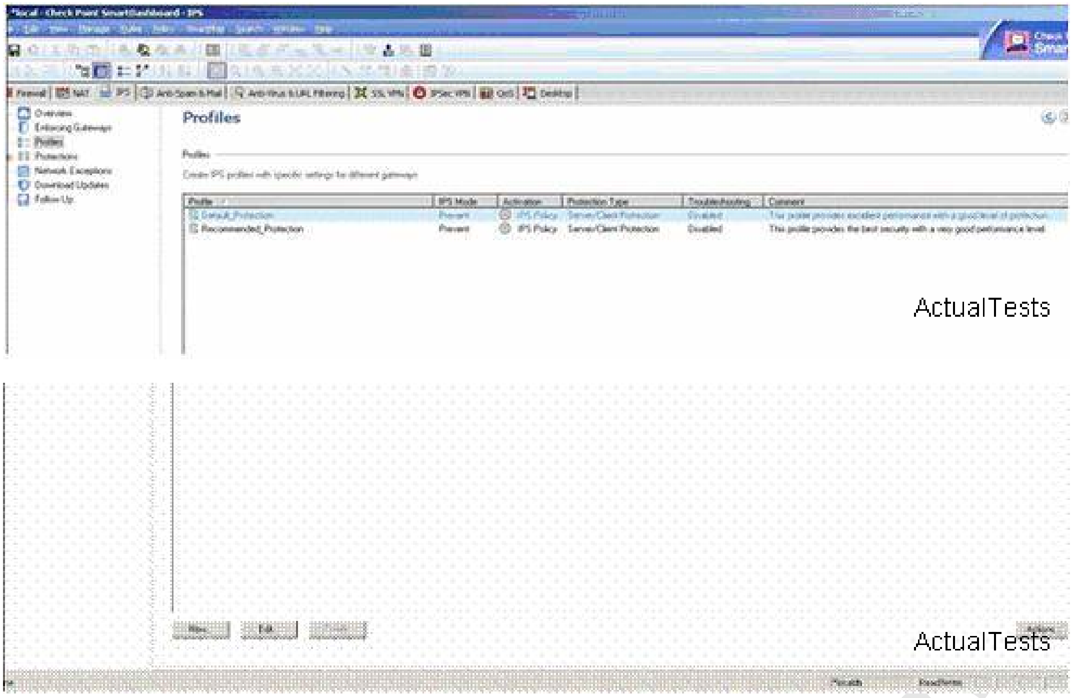
D. Ring

E. Cross

Answer: B

QUESTION NO: 163

If IPS protections are not activated automatically then you will have to consider:



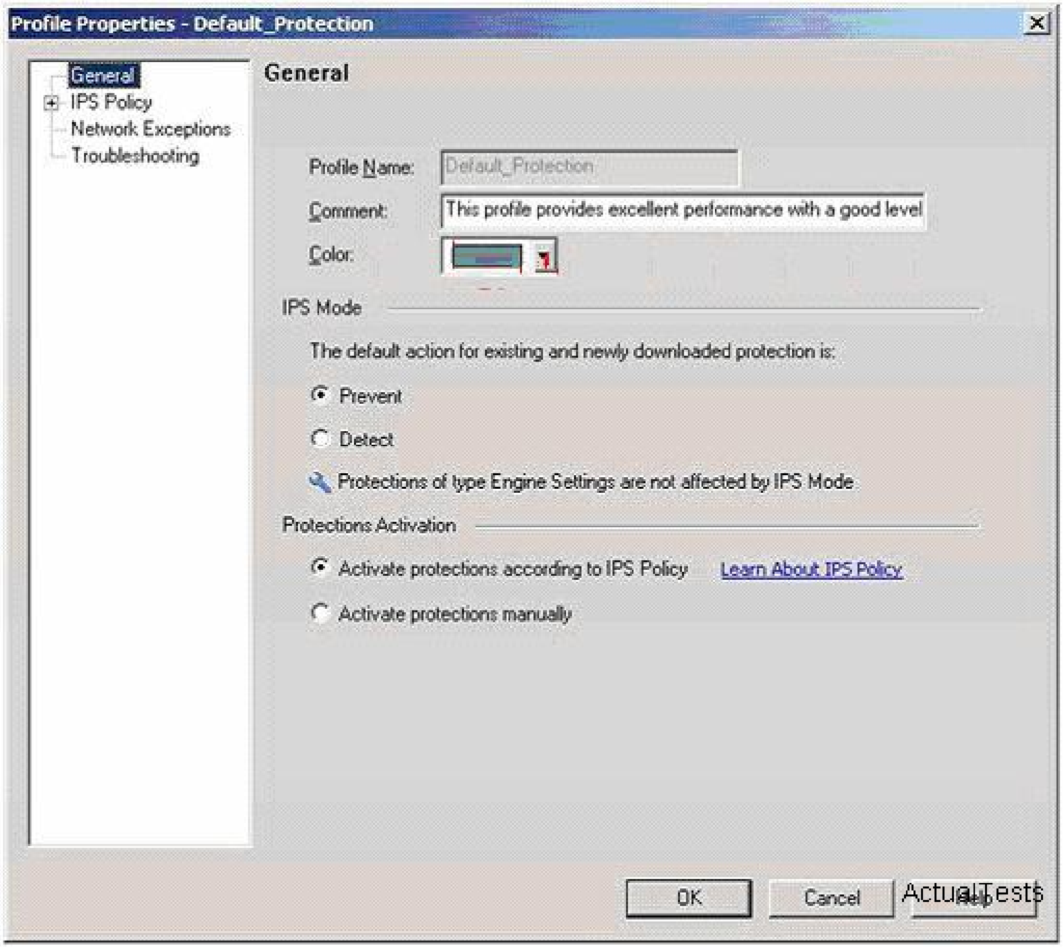
Profiles

Profiles

Create IPS profiles with specific settings for different gateways

Profile	IPS Mode	Activation	Protection Type	Troubleshooting	Comment
Default_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides excellent performance with a good level of protection
Recommended_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides the best security with a very good performance level

Figure 1: IPS Protections



Profile Properties - Default_Protection

General

Profile Name: Default_Protection

Comment: This profile provides excellent performance with a good level

Color:

IPS Mode

The default action for existing and newly downloaded protection is:

● Prevent

○ Detect

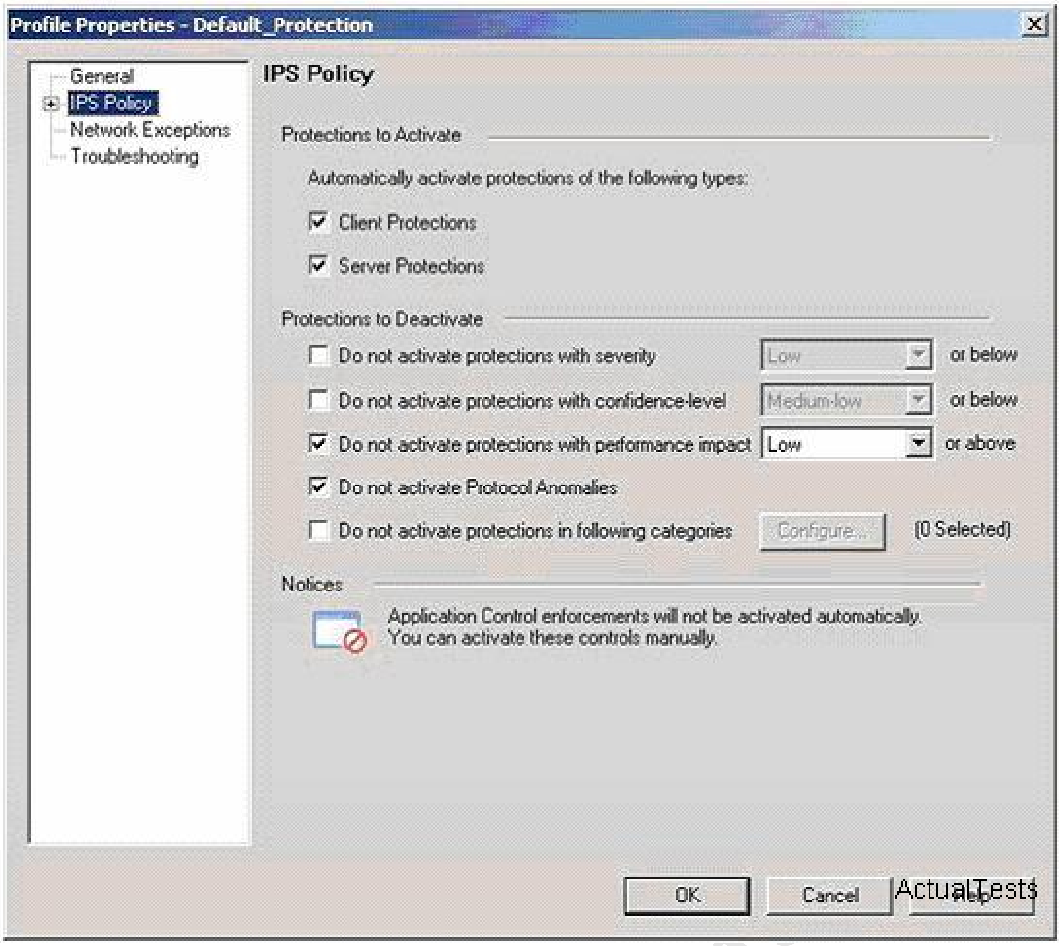
Protections of type Engine Settings are not affected by IPS Mode

Protections Activation

● Activate protections according to IPS Policy Learn About IPS Policy

○ Activate protections manually

Figure 2: Profiles Properties Window - General Page



Profile Properties - Default_Protection

IPS Policy

Protections to Activate

Automatically activate protections of the following types:

☑ Client Protections

☑ Server Protections

Protections to Deactivate

☐ Do not activate protections with severity Low or below

☐ Do not activate protections with confidence-level Medium-low or below

☑ Do not activate protections with performance impact Low or above

☑ Do not activate Protocol Anomalies

☐ Do not activate protections in following categories Configure... (0 Selected)

Notices

Application Control enforcements will not be activated automatically.
You can activate these controls manually.

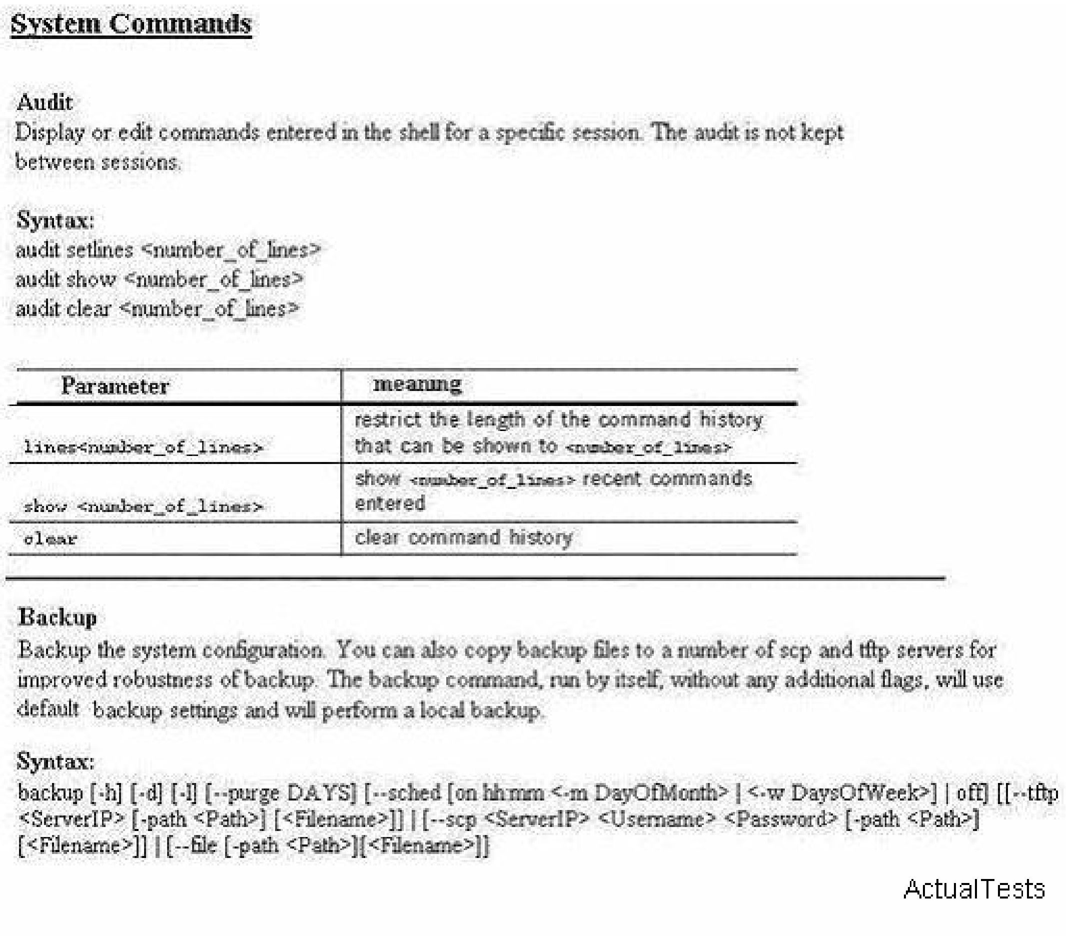
Figure 3 : Profiles Properties Window - IPS Policy Page

A. Redesigning
B. IPSBy Type
C. Manual activation
D. Profiling
E. IPS Profiling

Answer: C

QUESTION NO: 164

What is true of the command "backup -scp ip5 username3 password3 -path mybackup" if you run it on SecurePlatform?



System Commands

Audit

Display or edit commands entered in the shell for a specific session. The audit is not kept between sessions.

Syntax:

```
audit setlines <number_of_lines>
audit show <number_of_lines>
audit clear <number_of_lines>
```

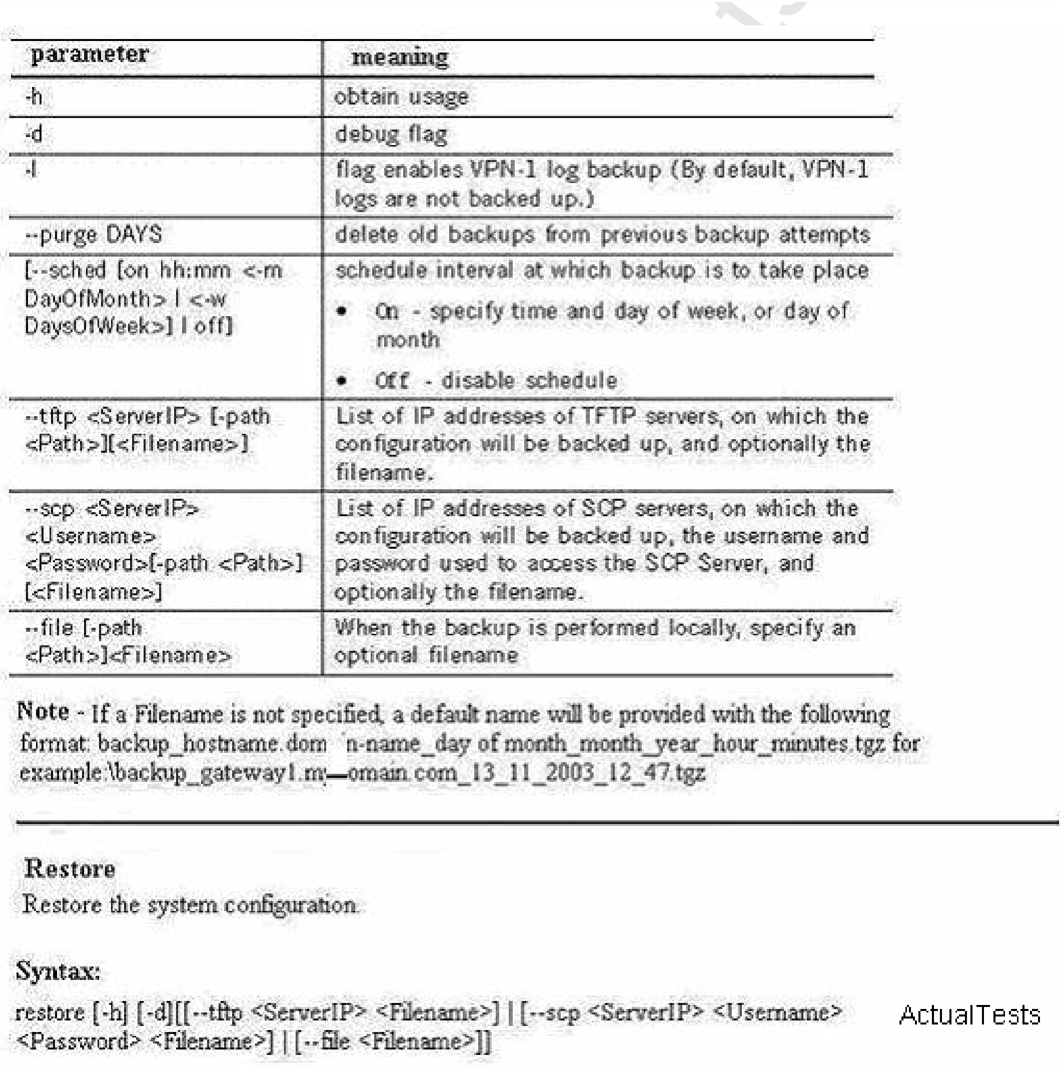
Parameter	meaning
lines<number_of_lines>	restrict the length of the command history that can be shown to <number_of_lines>
show <number_of_lines>	show <number_of_lines> recent commands entered
clear	clear command history

Backup

Backup the system configuration. You can also copy backup files to a number of scp and tftp servers for improved robustness of backup. The backup command, run by itself, without any additional flags, will use default backup settings and will perform a local backup.

Syntax:

```
backup [-h] [-d] [-l] [--purge DAYS] [--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek>] | off] [[--tftp
<ServerIP> [-path <Path>] [<Filename>]] | [--scp <ServerIP> <Username> <Password> [-path <Path>]
[<Filename>]] | [--file [-path <Path>][<Filename>]]
```



parameter	meaning
-h	obtain usage
-d	debug flag
-l	flag enables VPN-1 log backup (By default, VPN-1 logs are not backed up.)
--purge DAYS	delete old backups from previous backup attempts
[--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek>] | off]	schedule interval at which backup is to take place • On - specify time and day of week, or day of month • Off - disable schedule
--tftp <ServerIP> [-path <Path>][<Filename>]	List of IP addresses of TFTP servers, on which the configuration will be backed up, and optionally the filename.
--scp <ServerIP> <Username> <Password>[-path <Path>] [<Filename>]	List of IP addresses of SCP servers, on which the configuration will be backed up, the username and password used to access the SCP Server, and optionally the filename.
--file [-path <Path>]<Filename>	When the backup is performed locally, specify an optional filename

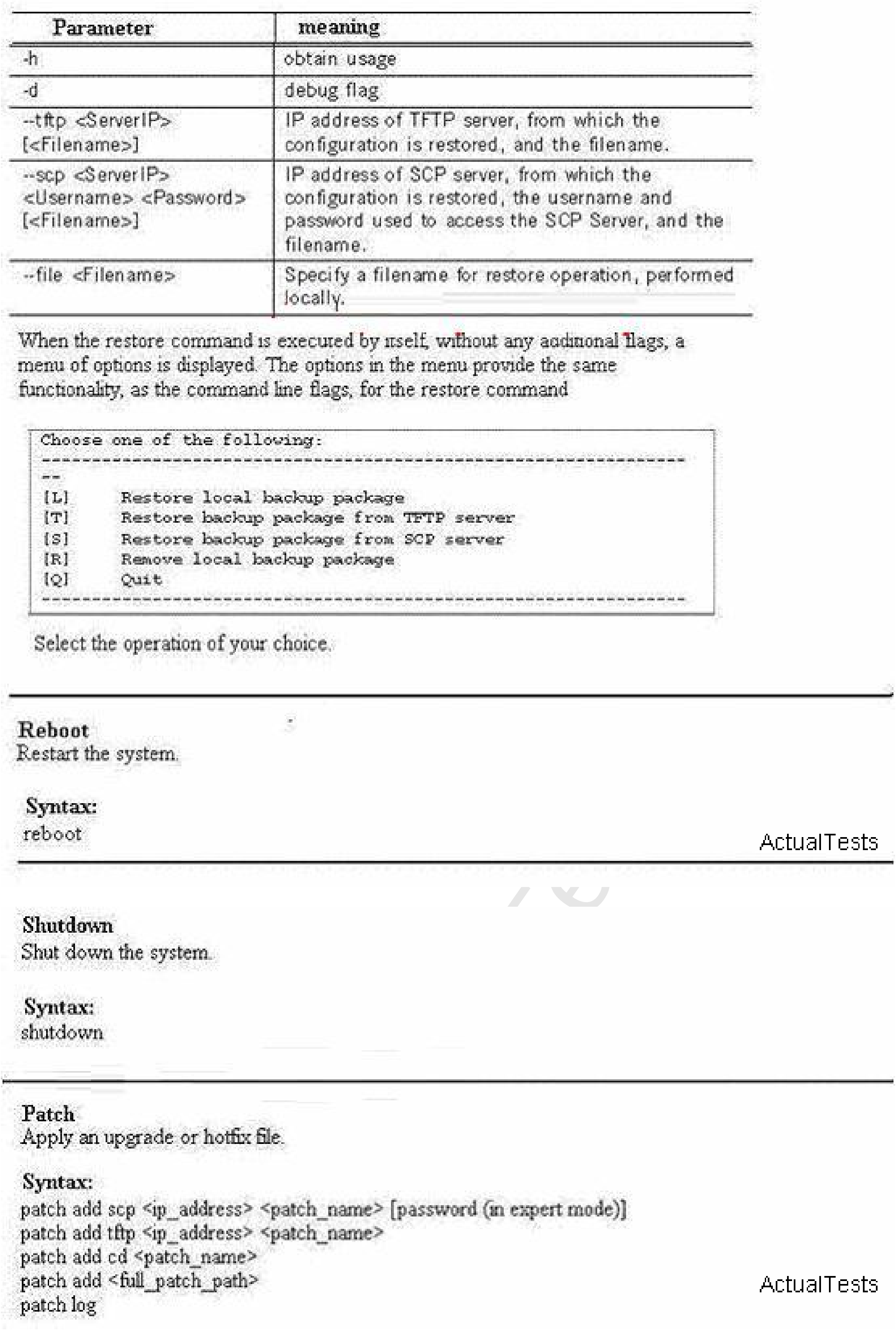
Note - If a Filename is not specified, a default name will be provided with the following format: backup_hostname.dom 'n-name_day of month_month_year_hour_minutes.tgz for example:\backup_gateway1.m;—omain.com_13_11_2003_12_47.tgz

Restore

Restore the system configuration.

Syntax:

```
restore [-h] [-d][[--tftp <ServerIP> <Filename>] | [--scp <ServerIP> <Username>
<Password> <Filename>] | [--file <Filename>]]
```



Parameter	meaning
-h	obtain usage
-d	debug flag
--tftp <ServerIP> [<Filename>]	IP address of TFTP server, from which the configuration is restored, and the filename.
--scp <ServerIP> <Username> <Password> [<Filename>]	IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.
--file <Filename>	Specify a filename for restore operation, performed locally.

When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command

```
Choose one of the following:
-----------------------------------------------------------------
--
[L]     Restore local backup package
[T]     Restore backup package from TFTP server
[S]     Restore backup package from SCP server
[R]     Remove local backup package
[Q]     Quit
-----------------------------------------------------------------
```

Select the operation of your choice.

Reboot
Restart the system.

Syntax:
reboot

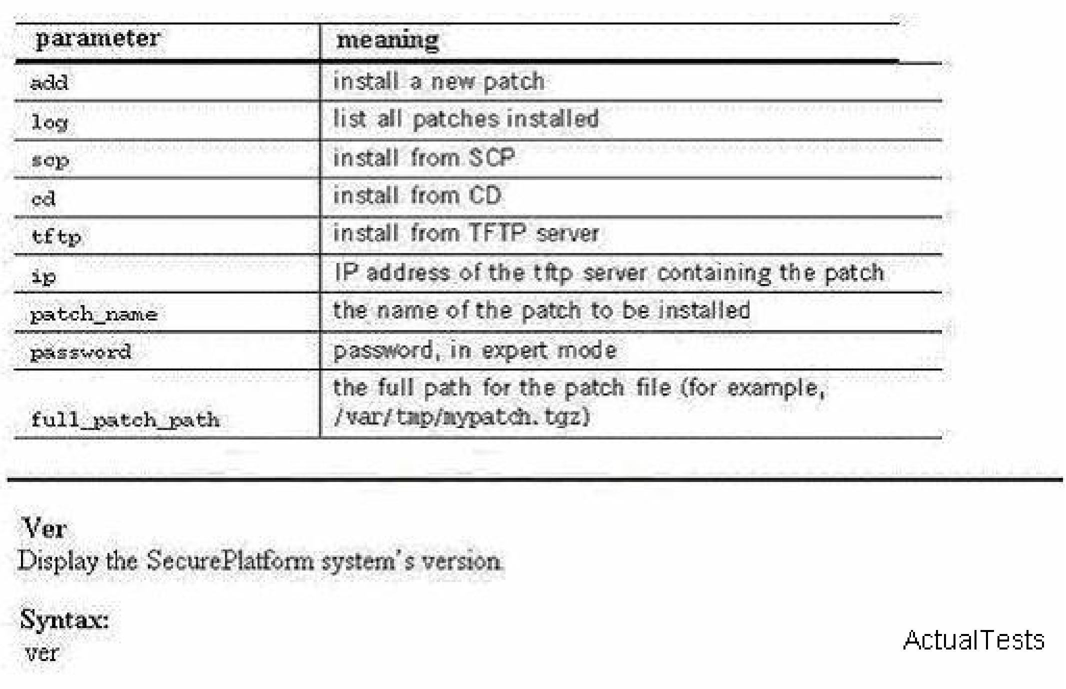
Shutdown
Shut down the system.

Syntax:
shutdown

Patch
Apply an upgrade or hotfix file.

Syntax:

```
patch add scp <ip_address> <patch_name> [password (in expert mode)]
patch add tftp <ip_address> <patch_name>
patch add cd <patch_name>
patch add <full_patch_path>
patch log
```



parameter	meaning
add	install a new patch
log	list all patches installed
scp	install from SCP
cd	install from CD
tftp	install from TFTP server
ip	IP address of the tftp server containing the patch
patch_name	the name of the patch to be installed
password	password, in expert mode
full_patch_path	the full path for the patch file (for example, /var/tmp/mypatch.tgz)

Ver
Display the SecurePlatform system's version

Syntax:
ver

A. The backup file be saved onscp server with ip5 on username3/-path/ with the default backup file name
B. The backup file be saved onscp server on username3/mybackup/ with the default backup file name
C. backup to server withip5 , using username3 password3 as credentials, and with default backup file name
D. The backup file be saved onscp server with ip4 on username3/password3/mybackup/ with the default backup file name
E. The backup file be saved onscp server with ip5 on username3/password3/mybackup/ with the default backup file name

Answer: C

QUESTION NO: 165

The advantages of using IPSO include which of the following? Select all the correct answers.

A. IPSO contains embedded daemons that prevent hacking into the system
B. IPSO is scalable
C. IPSO is based on Windows operating systems
D. IPSO is hardened from the ground up
E. IPSO is used as the secure operating system for firewall and VPN systems

Answer: B,D,E

QUESTION NO: 166

The methods of encryption supported during the IKE phase 1 process are: AES; 3DES; DES; and CAST. The MD5 and SHA1 are method of what?

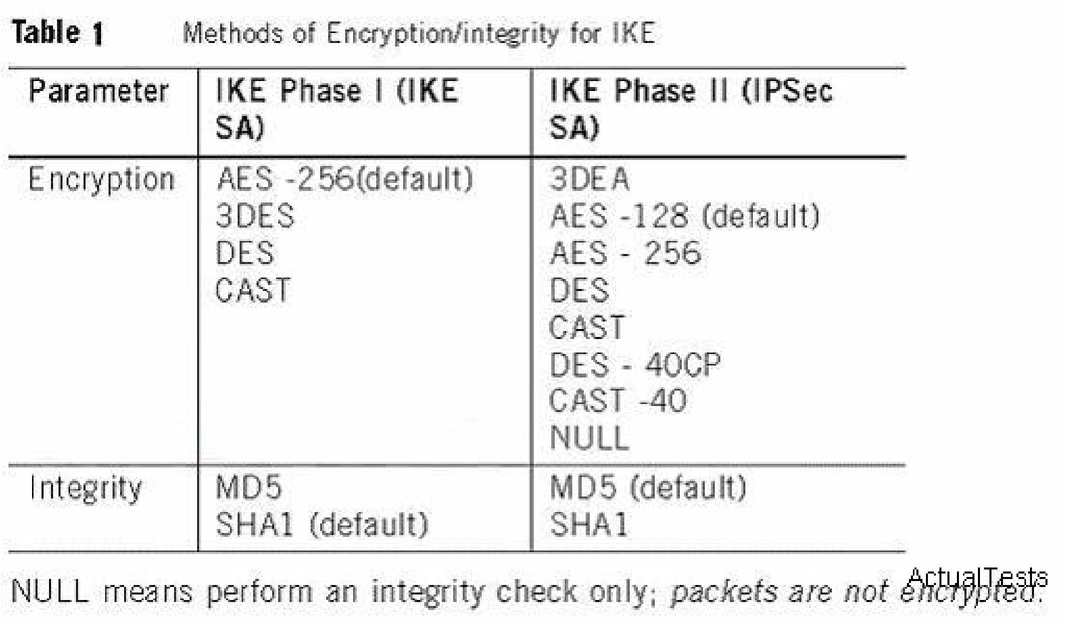


Table 1 Methods of Encryption/integrity for IKE

Parameter	IKE Phase I (IKE SA)	IKE Phase II (IPSec SA)
Encryption	AES -256(default) 3DES DES CAST	3DEA AES -128 (default) AES - 256 DES CAST DES - 40CP CAST -40 NULL
Integrity	MD5 SHA1 (default)	MD5 (default) SHA1

NULL means perform an integrity check only; *packets are not encrypted.*

A. Integrity
B. IPSec SA
C. IPSec Phase
D. Algorithm
E. IPSec

Answer: A

QUESTION NO: 167

By default, UFP uses which of the following port?

A. 18181
B. 18182
C. 443
D. 1900
E. 440

Answer: B

QUESTION NO: 168

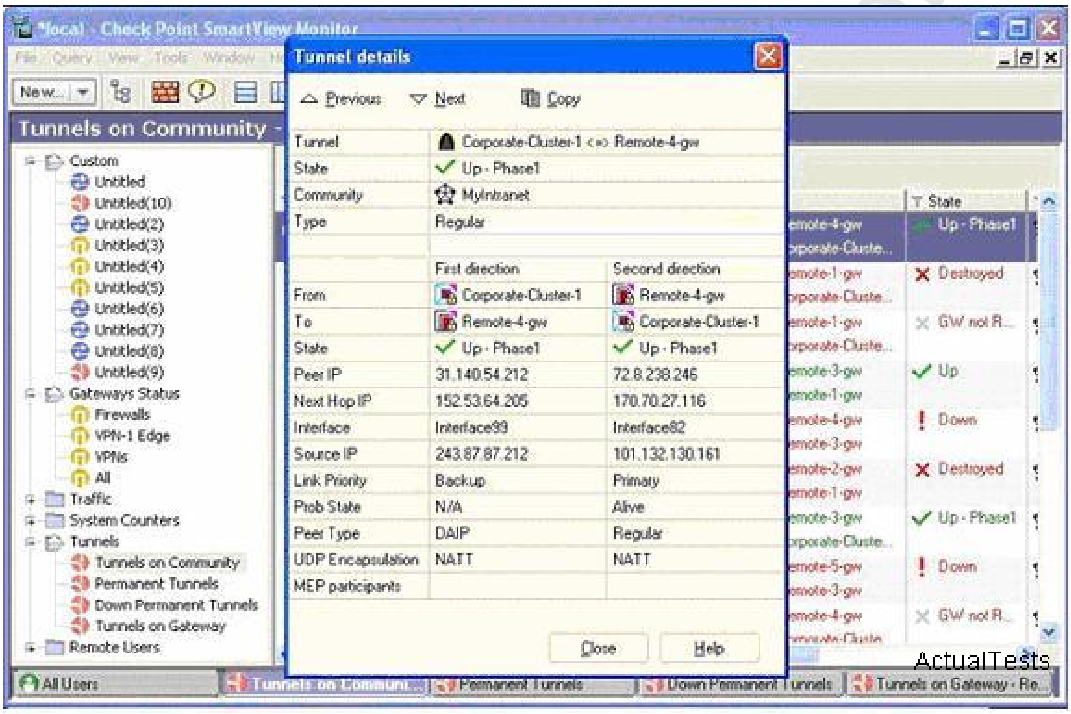
Your web server behind the security Gateway is configured to Automatic Static NAT. Client side NAT is not enabled in the Global Properties. A client on the Internet initiates a session to the web server. You have setup a rule to allow this session. In order for the traffic from the client to reach the web server, what else do you have to do?

A. A static route will be added on the Security Gateway to the web server
B. A automatic route will be added on the Security Gateway to the client
C. Modify the rule base and the Global Properties
D. Nothing else is necessary
E. A automatic route will be added on the Security Gateway to the web server

Answer: A

QUESTION NO: 169

Diagram 1 shows SmartView Monitor: Tunnel View mode with Tunnel details window. Which of the following information can you not get in the window?



Tunnel	Corporate-Cluster-1 <=> Remote-4-gw	
State	✓ Up - Phase1	
Community	MyIntranet	
Type	Regular	
	First direction	Second direction
From	Corporate-Cluster-1	Remote-4-gw
To	Remote-4-gw	Corporate-Cluster-1
State	✓ Up - Phase1	✓ Up - Phase1
Peer IP	31.140.54.212	72.8.238.246
Next Hop IP	152.53.64.205	170.70.27.116
Interface	Interface93	Interface82
Source IP	243.87.87.212	101.132.130.161
Link Priority	Backup	Primary
Prob State	N/A	Alive
Peer Type	DAIP	Regular
UDP Encapsulation	NATT	NATT
MEP participants		

Figure 1: SmartView Monitor - Tunnel View

A. Tunnel
B. Community
C. Prob State
D. State
E. User DN

Answer: E

QUESTION NO: 170

R70 implements privacy by making no one but the intended parties to understand the communication, in the way of data encryption. The encryption is carried out by encryption software and a secret key. What do you need to decrypt the encrypted data?

A. Shared key
B. Hardware key
C. Privatekey
D. Software key
E. combination of Shared key and Network key

Answer: A

QUESTION NO: 171

Which of the following is true of Digital Signature?

A. Is a code that can be used to identify what part of data toencrypt
B. Is a code that can be used to encrypt an electronically transmittedmessage
C. Is a code that can be attached to an electronically transmitted message that uniquely identifies thesender
D. Is a code that can be attached to an electronically transmitted message that uniquely identifies therecipient
E. Is a code that can be used to decrypt an electronically transmittedmessage

Answer: C

QUESTION NO: 172

ISAKMP/Oakley provides a mean to:

A. ISAKMP/Oakley functions in two phases
B. Manage those keys
C. Agree on which protocols, algorithms, and keys to use
D. Exchange keys safely
E. Create a set of IPSec applications

Answer: A,B,C,D

QUESTION NO: 173

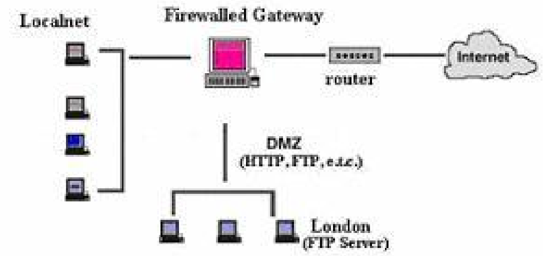
VPN deployments can be two types and these are:

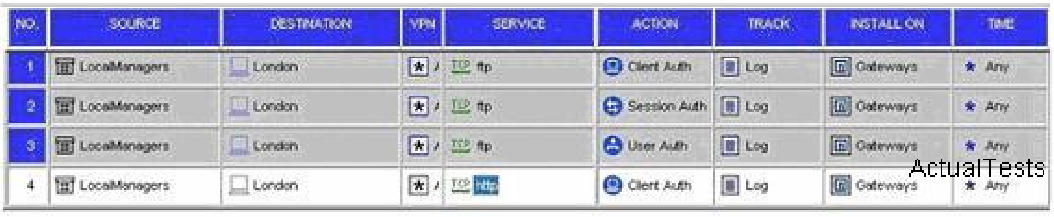
A. Terrestrial VPN
B. Extranet VPN
C. Site to Site VPN
D. Intranet VPN
E. Remote Access VPN

Answer: C,E

QUESTION NO: 174

See the diagrams and answer the question. Your Internal network is called Local net. What rule would allow Local Managers to access London (the FTP server) after successful User Authentication?





NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	LocalManagers	London	★	TCP ftp	Client Auth	Log	Gateways	★ Any
2	LocalManagers	London	★	TCP ftp	Session Auth	Log	Gateways	★ Any
3	LocalManagers	London	★	TCP ftp	User Auth	Log	Gateways	★ Any
4	LocalManagers	London	★	TCP http	Client Auth	Log	Gateways	★ Any

A. Rule 2
B. None of the available answers
C. Rule 1
D. Rule 4
E. Rule 3

Answer: E

QUESTION NO: 175

Which of the following are the disadvantages of symmetric encryption?

A. Symmetric encryption can be cracked through a "brute-force" attack
B. Symmetric encryption also create lesser key-management problems than Asymmetric ciphers
C. Secret channel is necessary for the exchange of the public key
D. Symmetric encryption processing tend to be about "1000 times slower than Asymmetric encryption
E. The key that deciphers the ciphertext is the same as the key enciphers the clear text

Answer: A,C,E

QUESTION NO: 176

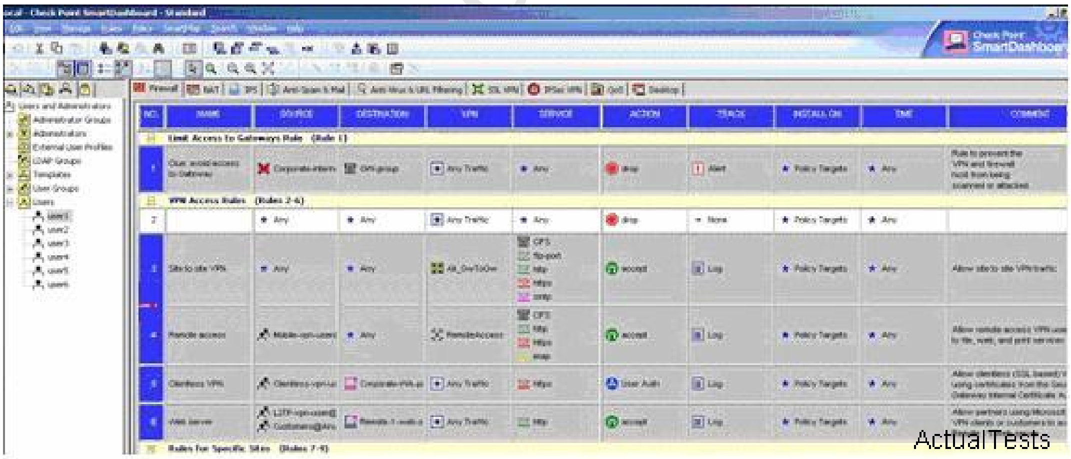
Which of the following question(s) will you raise when planning a VPN topology? 1. Who needs secure/private access? 2. From a VPN point of view, what will be the structure of the organization? 3. Internally managed gateways will authenticate each other using certificates 4. How will externally managed gateways authenticate 5. What VPN topology will be suitable?

A. 1
B. 1,2
C. 1,2,3,4,5
D. 1,2,3
E. 1,2,3,4

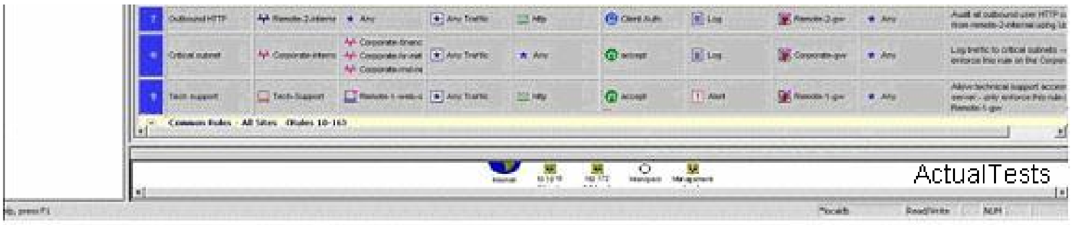
Answer: E

QUESTION NO: 177

The default track column of the newly created Default rule is set to:



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Limit Access to Gateways Rule (Rule 1)										
1	[illegible] access to Gateways	Corporate-intern	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	Rule to prevent the VPN and firewall host from being scanned or attacked
VPN Access Rules (Rules 2-6)										
2		Any	Any	Any Traffic	Any	drop	None	Policy Targets	Any	
3	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any	Allow site to site VPN traffic
4	Remote access	Mobile-vpn-users	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any	Allow remote access VPN use to file, web, and print services
5	Clientless VPN	Clientless-vpn-u	Corporate-WA-p	Any Traffic	https	User Auth	Log	Policy Targets	Any	Allow clientless (SSL based) using certificates from the Sec Gateway Internal Certificate A
6	Web server	L2TP-vpn-users@ Customers@Any	Remote-1-web-s	Any Traffic	http	accept	Log	Policy Targets	Any	Allow partners using Microsoft VPN clients or customers to ac
Rules for Specific Sites (Rules 7-9)										



7	Outbound HTTP	Remote-2-interna	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any	Audit all outbound user HTTP [illegible] from remote-2-internal using [illegible]
8	Critical subnet	Corporate-interna	Corporate-financ Corporate-hr-net Corporate-mail-s	Any Traffic	Any	accept	Log	Corporate-gw	Any	Log traffic to critical subnets -- enforce this rule on the Corpor
9	Tech support	Tech-Support	Remote-1-web-s	Any Traffic	http	accept	Alert	Remote-1-gw	Any	Allow technical support access [illegible] server - only enforce this rule [illegible] Remote-1-gw

Common Rules - All Sites (Rules 10-16)

A. Log

B. Alert

C. Mail

D. User Defined

E. - None

Answer: E

QUESTION NO: 178

A ____________________ ____________________ is a trusted third party that can provide a public key even over an untrusted network such as the Internet.

A. SmartView Tracker

B. Certificate Authority

C. SecuRemote client

D. Smart Update

E. SmartView Monitor

Answer: B

QUESTION NO: 179

What other way can you use to administer Security Policy apart from CheckPoint SmartDashboard?

A. Check Policy Application configuration

B. By command Line options

C. By Check Point Managing Editor

D. By MSDOS command

E. Using pkgrm application

Answer: B

QUESTION NO: 180

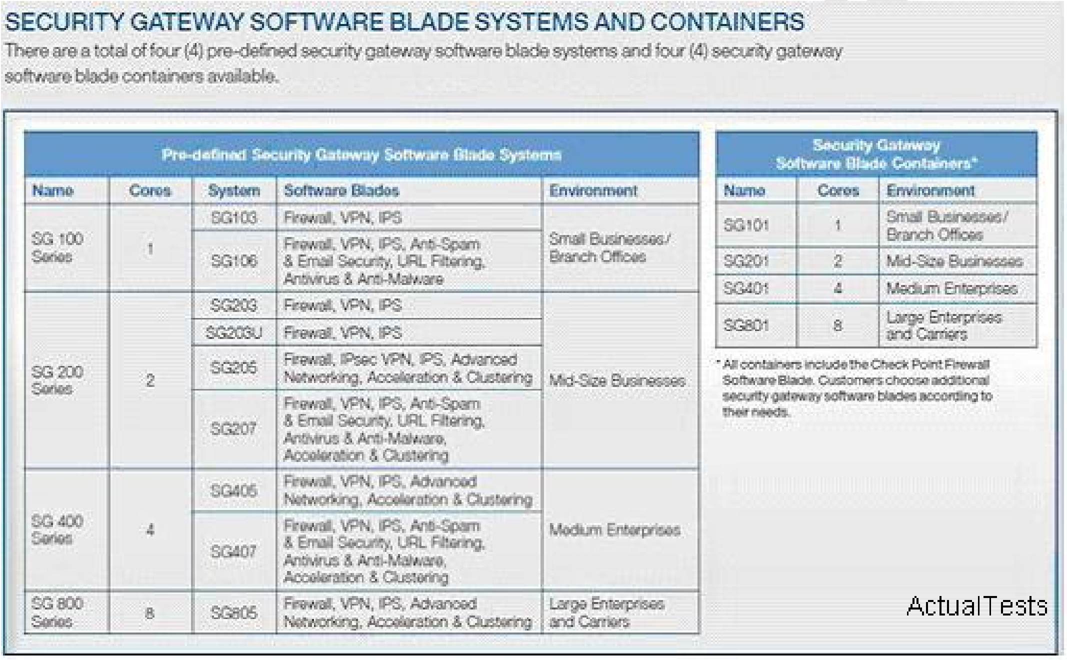
The most recommended and manageable method for authentication among gateways and remote clients is:

A. Pre-shared secrets
B. Gateway Password
C. Digital certificates
D. One Time Password
E. Hybrid Mode

Answer: C

QUESTION NO: 181

You want to configure Software Blade Containers and you have two types which you have to choose from. You run 9 gateways. Which of the containers you have to choose from based on number of gateways?



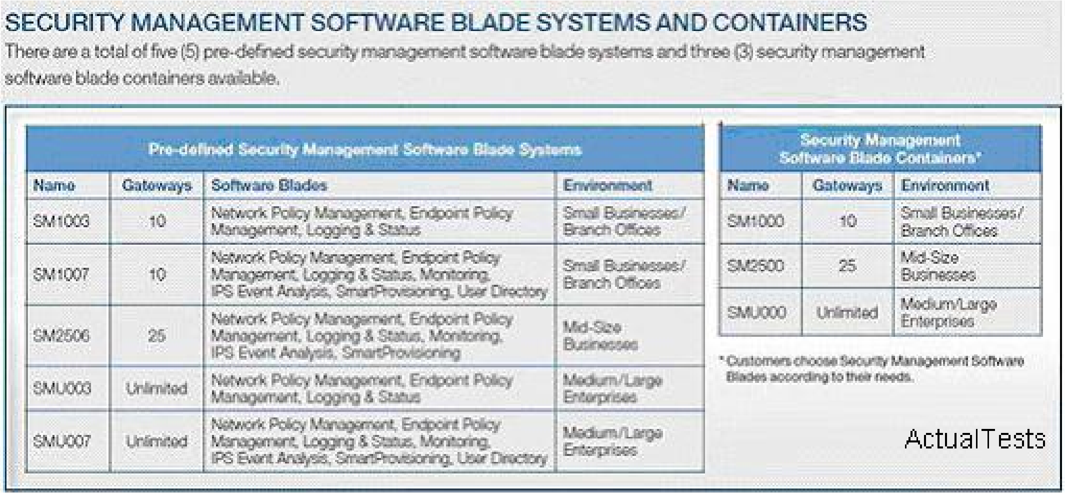
SECURITY GATEWAY SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of four (4) pre-defined security gateway software blade systems and four (4) security gateway software blade containers available.

Pre-defined Security Gateway Software Blade Systems				
Name	Cores	System	Software Blades	Environment
SG 100 Series	1	SG103	Firewall, VPN, IPS	Small Businesses/ Branch Offices
		SG106	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware	
SG 200 Series	2	SG203	Firewall, VPN, IPS	Mid-Size Businesses
		SG203U	Firewall, VPN, IPS	
		SG205	Firewall, IPsec VPN, IPS, Advanced Networking, Acceleration & Clustering	
		SG207	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	
SG 400 Series	4	SG405	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	Medium Enterprises
		SG407	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	
SG 800 Series	8	SG805	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	Large Enterprises and Carriers

Security Gateway Software Blade Containers*		
Name	Cores	Environment
SG101	1	Small Businesses/ Branch Offices
SG201	2	Mid-Size Businesses
SG401	4	Medium Enterprises
SG801	8	Large Enterprises and Carriers

* All containers include the Check Point Firewall Software Blade. Customers choose additional security gateway software blades according to their needs.



SECURITY MANAGEMENT SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of five (5) pre-defined security management software blade systems and three (3) security management software blade containers available.

Pre-defined Security Management Software Blade Systems			
Name	Gateways	Software Blades	Environment
SM1003	10	Network Policy Management, Endpoint Policy Management, Logging & Status	Small Businesses/ Branch Offices
SM1007	10	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Small Businesses/ Branch Offices
SM2506	25	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning	Mid-Size Businesses
SMU003	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status	Medium/Large Enterprises
SMU007	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Medium/Large Enterprises

Security Management Software Blade Containers*		
Name	Gateways	Environment
SM1000	10	Small Businesses/ Branch Offices
SM2500	25	Mid-Size Businesses
SMU000	Unlimited	Medium/Large Enterprises

* Customers choose Security Management Software Blades according to their needs.

A. Network Policy Management

B. Management Portal

C. Endpoint Policy Management

D. Security Gateway Containers

E. Security Management Containers

Answer: E

QUESTION NO: 182

Study the diagram 1 and then answer the question below. Which of the following rule in the diagram would allow connections between the two VPN sites?

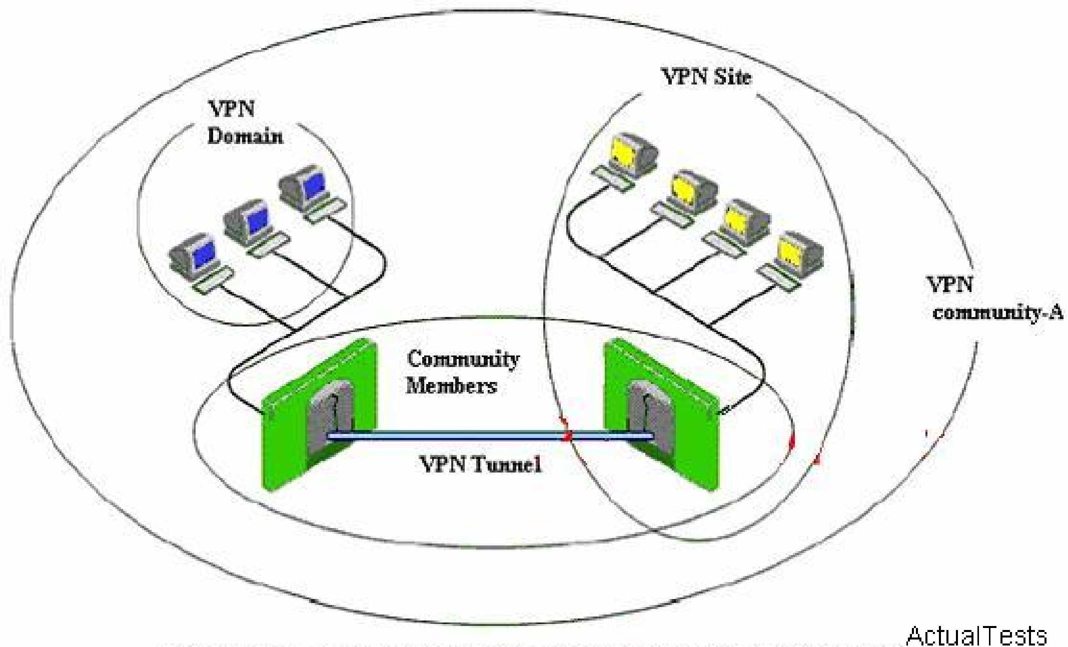
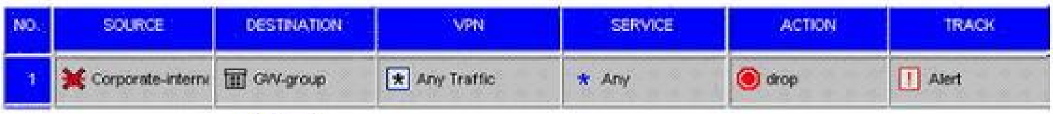
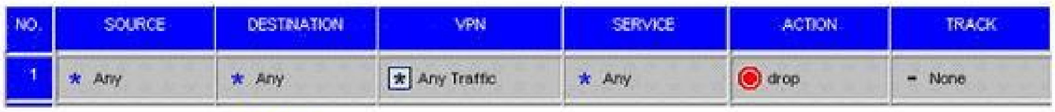


Figure A: Your VPN community(called community-A)



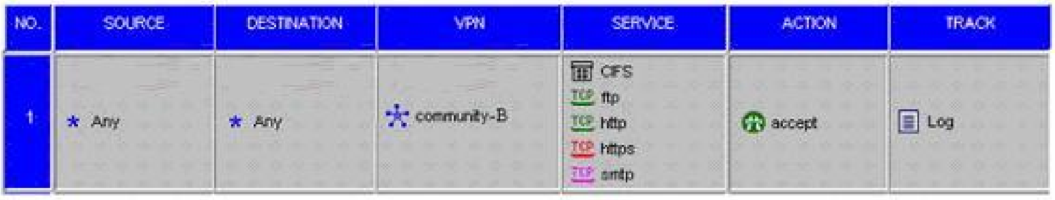
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Corporate-intern	GW-group	Any Traffic	* Any	drop	Alert

Rule A



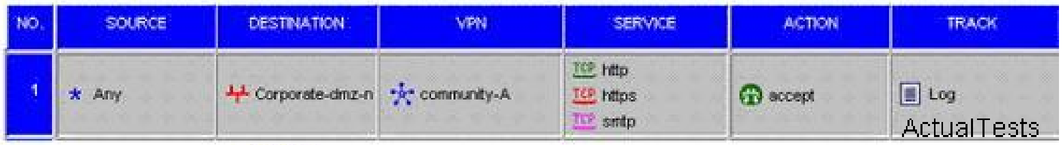
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	Any Traffic	* Any	drop	- None

Rule B



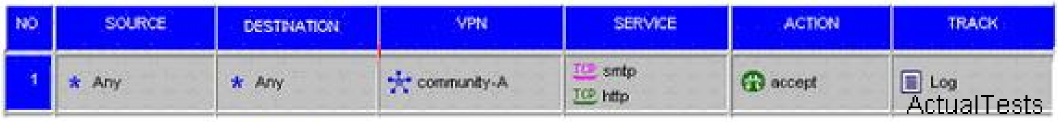
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	community-B	CIFS TCP ftp TCP http TCP https TCP smtp	accept	Log

Rule C



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	Corporate-dmz-n	community-A	TCP http TCP https TCP smtp	accept	Log

Rule D



NO	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	community-A	TCP smtp TCP http	accept	Log

Rule E

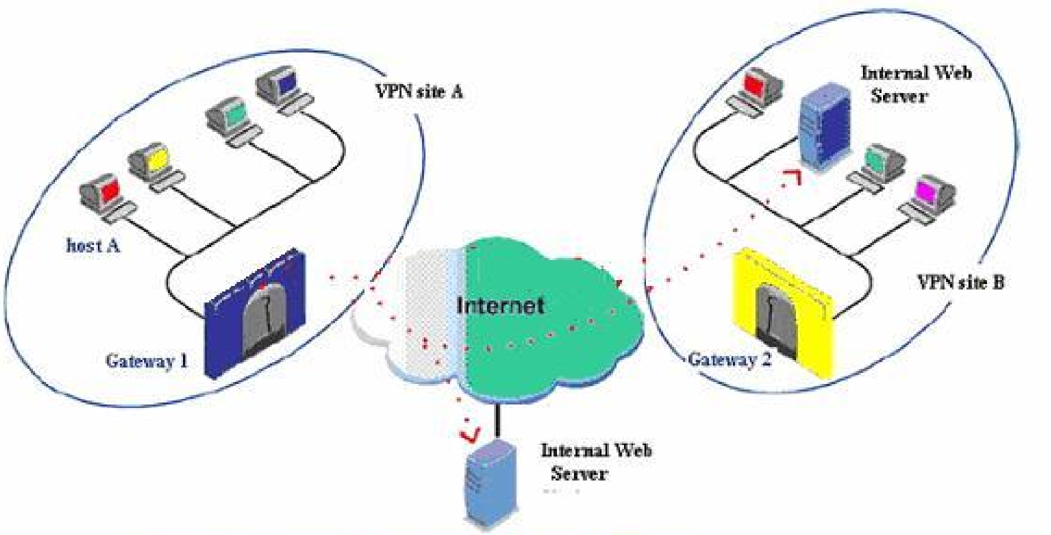


Figure A: Access Control in VPN communities

b

A. Rule C

B. Rule E

C. Rule B

D. Rule A

E. Rule D

Answer: B

QUESTION NO: 183

See the diagram then answer the question. When SmartDirectory (LDAP) servers are queried for user information, they are queried according to their place in a set priority. The closest SmartDirectory (LDAP) server has the first priority. The furthest SmartDirectory (LDAP) server has the last priority.

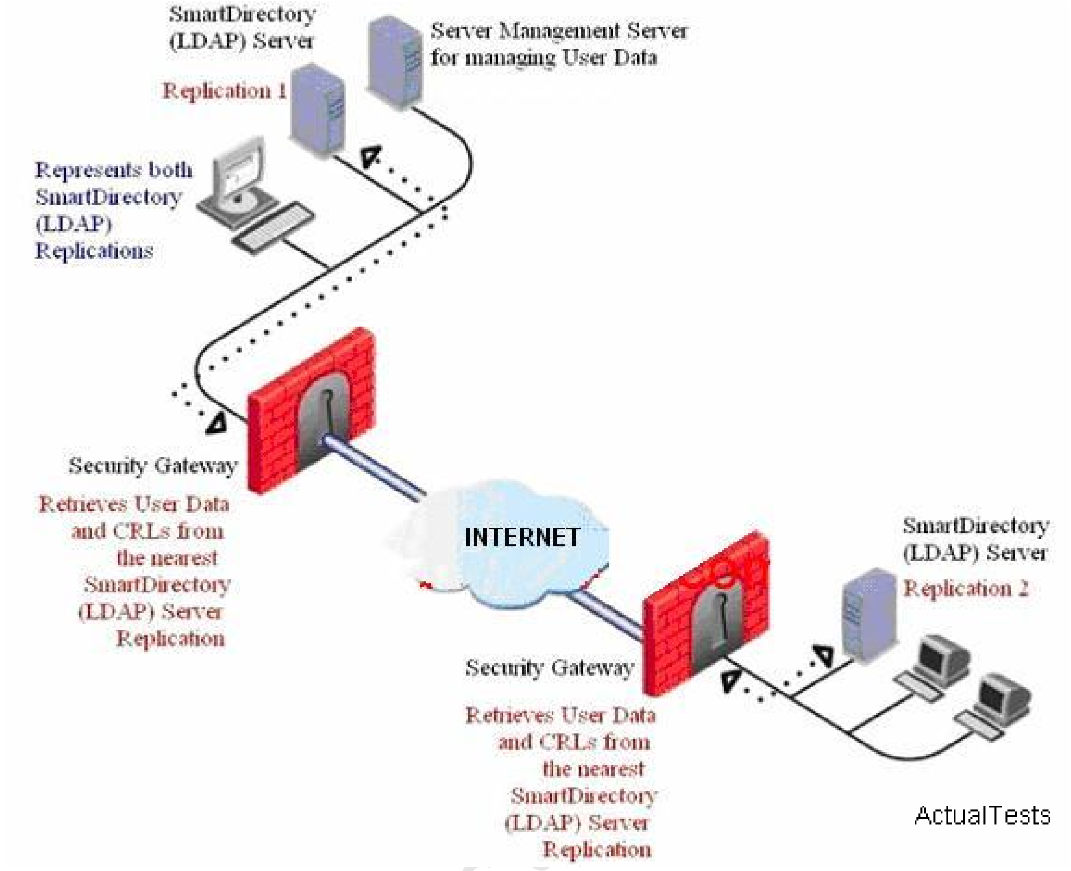

SmartDirectory (LDAP) Server
Replication 1
Server Management Server for managing User Data
Represents both SmartDirectory (LDAP) Replications
Security Gateway
Retrieves User Data and CRLs from the nearest SmartDirectory (LDAP) Server Replication
INTERNET
SmartDirectory (LDAP) Server
Replication 2
Security Gateway
Retrieves User Data and CRLs from the nearest SmartDirectory (LDAP) Server Replication

Figure 1: SmartDirectory (LDAP) Server Replications

A. In a random manner
B. In a round-robin manner
C. According to the distance from the Security Management Server
D. According to the distance from the gateway
E. In a manner based on certain algorithm

Answer: B

QUESTION NO: 184

You are upgrading your remote security gateway using a SmartUpdate. Once you have chosen your package source to be Download Center web, the following step will involve:

A. Copy the package to the repositories on the SmartConsole
B. Copy the package to the repositories on the SmartDashboard
C. Copy the package to the repositories on the Security Gateway
D. Copy the package to the repositories on the Security Management Server
E. Copy the package to the repositories on the SmartUpdate

Answer: D

QUESTION NO: 185

If both Domain Based VPN and Route Based VPN are enabled, which one of the following will take precedence?

A. Domain Based VPN
B. OSP
C. Numbered VTI
D. BGP
E. Route Based VPN

Answer: A

QUESTION NO: 186

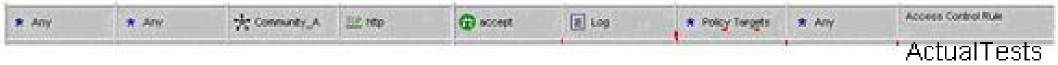
One of the prerequisites for remote upgrades using SmartUpdate is to enable SIC in order to allow secure communications between the Security Management server and remote Check Point Security Gateways. The other prerequisite involve:

A. Ensuring that SmartUpdate connections are allowed in the Global Properties
B. Ensuring that remote upgrades connections are allowed in the gateway property box
C. Ensuring that Suspicious Activity Rule is created on the SmartView Monitor
D. Ensuring that access rule is created on the SmartDashboard
E. Ensuring that access rule is created on the SmartView Tracker

Answer: A

QUESTION NO: 187

Which of the following are true of Access Control within VPN Communities?



Any	Any	Community_A	http	accept	Log	Policy Targets	Any	Access Control Rule

Figure 1: Access Control Rule

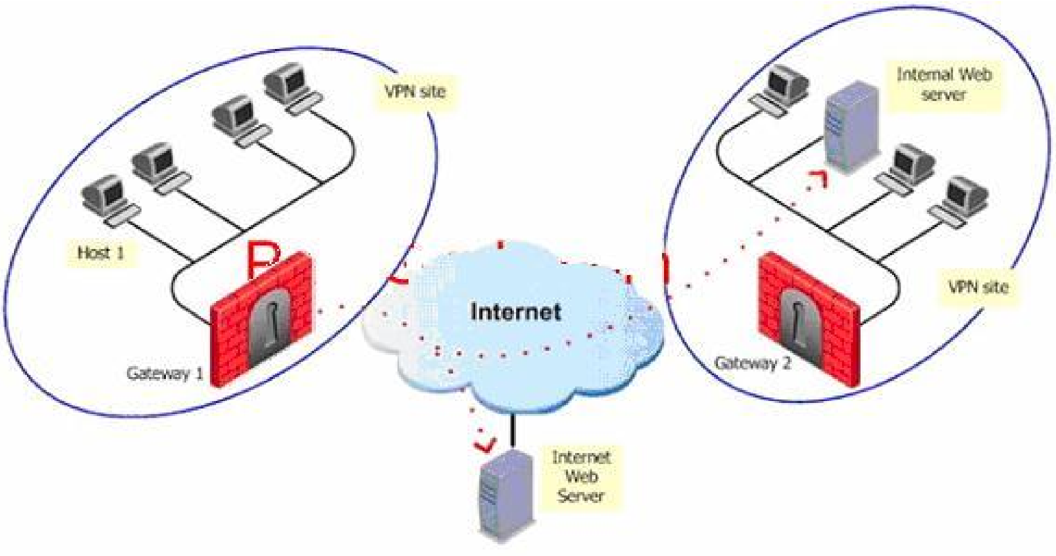
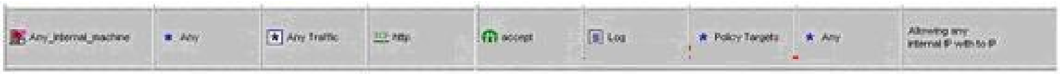


Figure 2: Access control in VPN communities



Any_internal_machine	★ Any	Any Traffic	http	accept	Log	★ Policy Targets	★ Any	Allowing any internal IP with to IP

Figure 3: Allowing any internal IP to any IP

A. The fact that two gateways belong to the same VPN community does automatically mean the gateways have access to each other

B. Using the Global Properties, it is possible to create access control rules that apply only to members of a VPN community

C. Using the VPN column of the Security Policy Rule Base, it is possible to create access control rules that apply only to members of a VPN community

D. The configuration of the gateways into a VPN community means that if these gateways are allowed to communicate via an access control policy, then that communication is encrypted

E. The fact that two gateways belong to the same VPN community does not mean the gateways have access to each other

Answer: C,D,E

QUESTION NO: 188

Which of the following is likely to be the best order for configuring user management in SmartDashboard using SmartDirectory (LDAP)?

A. Enable SmartDirectory (LDAP) attributes in the SmartDirectory page of the Global Properties, define the Check Point host on which the SmartDirectory (LDAP) server resides, and define a SmartDirectory (LDAP) Account Unit

B. Enable the Check Point host on which the SmartDirectory (LDAP) server resides, define SmartDirectory (LDAP) Account Unit,configure SmartDirectory (LDAP) attributes in the SmartDirectory page of the Global Properties

C. Enableconfigure SmartDirectory (LDAP) attributes in the SmartDirectory page of the Global Properties, and configure the obtained license
D. Enable SmartDirectory (LDAP) Account Unit, configure SmartDirectory (LDAP) attributes in the SmartDirectory page of the Global Properties, and define the Check Point host on which the SmartDirectory (LDAP) server resides
E. Enable the Check Point host on which the SmartDirectory (LDAP) server resides, define SmartDirectory (LDAP) Account Unit, configure SmartDirectory (LDAP) attributes in the SmartDirectory page of the Global Properties, and configure the obtained license

Answer: A

QUESTION NO: 189

Which of the following is true of Accounts Units?

A. SIC needs to be configured in order that Accounts Units can securely logon to Security Management Server and SmartDirectory (LDAP)
B. An organization is not allowed to have more than one Account Unit to represent the various SmartDirectory (LDAP) servers
C. When working with SmartDirectory (LDAP) servers, you need to define the Account Unit that represents the organization
D. Account Unit represents one or more branches of the information maintained on the SmartDirectory (LDAP) server
E. Account Unit is the interface which allows interaction between the Security Management server and Security Gateways, and the SmartDirectory (LDAP) servers

Answer: C,D,E

QUESTION NO: 190

Which of the following is true of SOAP?

A. SOAP provides a way for applications to communicate with each other over the Internet
B. SOAP provides a way for applications to communicate with each other over the Internet, dependent of platform
C. CheckPoint Security Gateway checks that only a predefined list of acceptable methods is being passed in the SOAP packet
D. SOAP relies on XML to define the format of the information and then adds the necessary HTTP headers to send it
E. The way that CheckPoint Security Gateway treats SOAP packets is defined in a URI resource that uses HTTP

Answer: A,C,D,E

QUESTION NO: 191

One of the host machines behind Gateway A initiates a connection with a host machine behind Gateway B. For either policy reason, Gateway A cannot establish a VPN tunnel with Gateway B. Using VPN Routing, both Gateways A and B can establish VPN tunnels with Gateway C, so the connection is routed through Gateway C. What VPN routing method would you employ to achieve this?

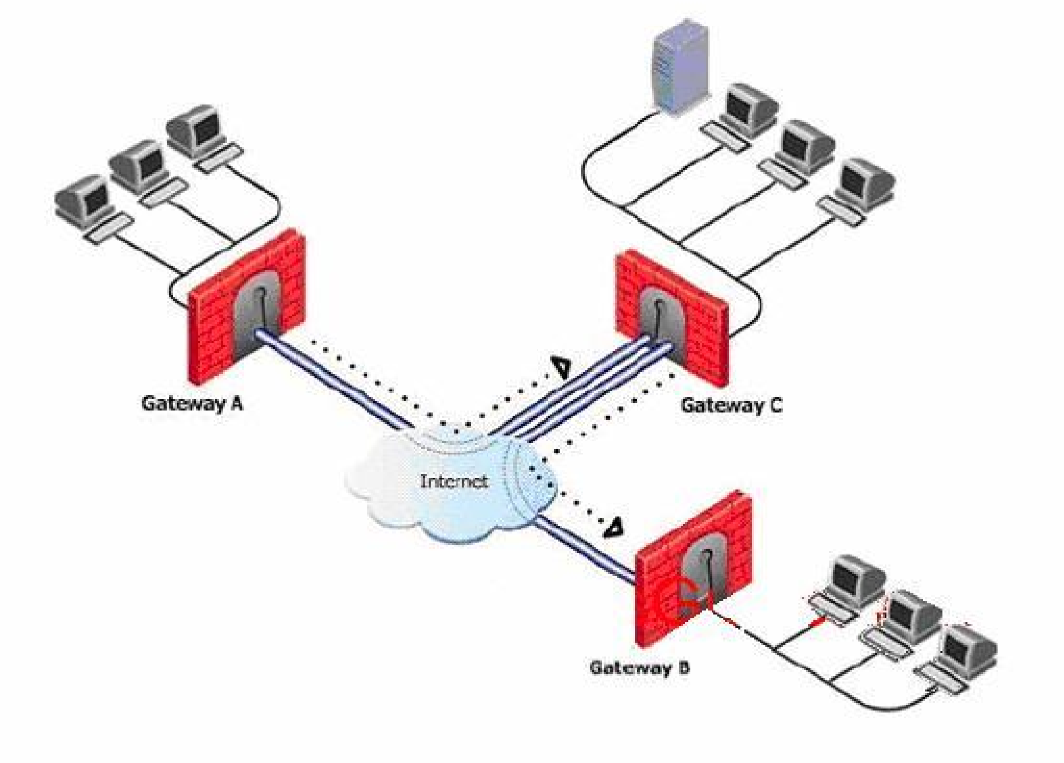


FIGURE 1 Simple VPN routing

ActualTests

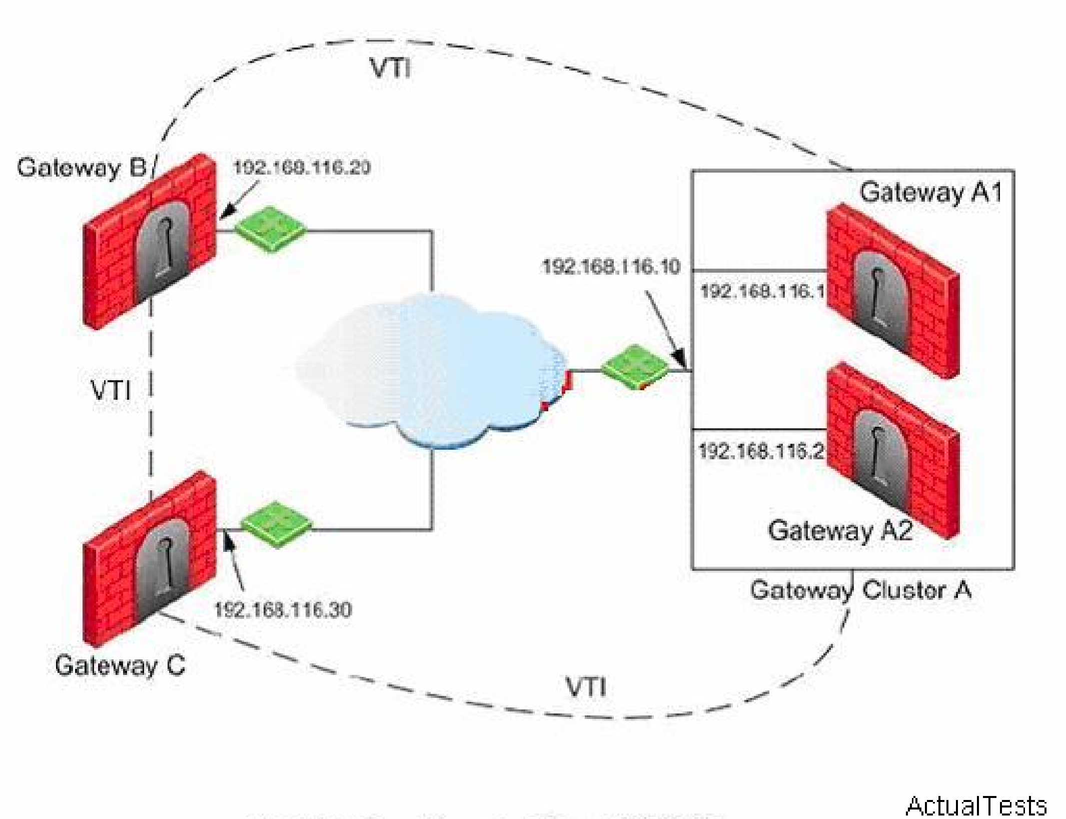


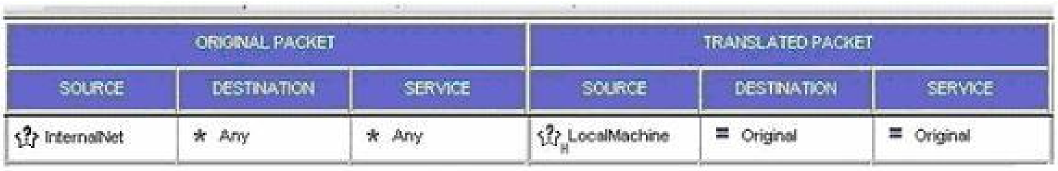
FIGURE 2 Route Based VPN

A. Domain Based VPN
B. Stationary Based VPN
C. Static Based VPN
D. Dynamic Based VPN
E. Gateway Based VPN

Answer: A

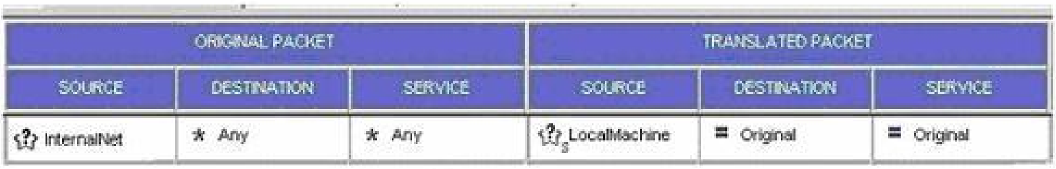
QUESTION NO: 192

Study the diagram and proceed to answer the question. Which of the following rule will hide the InternalNetwork behind the external IP address of the SmartLSM Security Gateway. Note: a) Use the LocalMachine dynamic object to represent the SmartLSM Gateway , b) Use the InternalNet, DMZnet and AuxiliaryNet dynamic objects to represent the respective networks behind the SmartLSM Gateway.



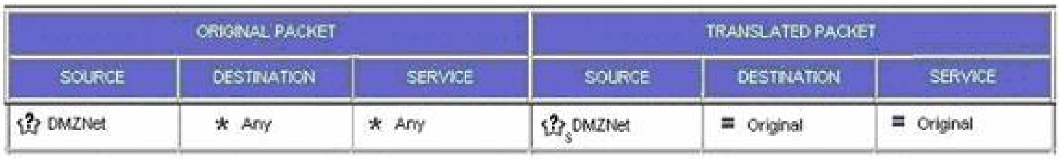
ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
InternalNet	* Any	* Any	H LocalMachine	= Original	= Original

Figure A



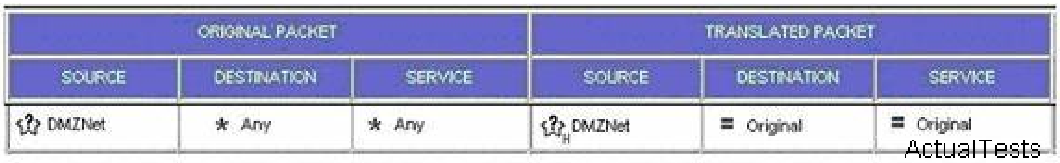
ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
InternalNet	* Any	* Any	S LocalMachine	= Original	= Original

Figure B



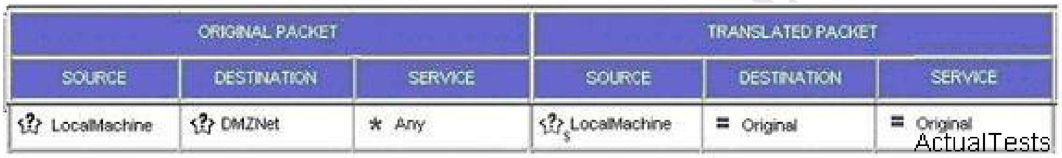
ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
DMZNet	* Any	* Any	S DMZNet	= Original	= Original

Figure C



ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
DMZNet	* Any	* Any	H DMZNet	= Original	= Original

Figure D



ORIGINAL PACKET			TRANSLATED PACKET		
SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE
LocalMachine	DMZNet	* Any	S LocalMachine	= Original	= Original

Figure E

A. FIGURE A

B. FIGURE D

C. FIGURE C

D. FIGURE E

E. FIGURE B

Answer: A

QUESTION NO: 193

Why should User Authentication not be suitable with HTTP sessions?

A. Because User Authentication requires authentication scheme that requires persession authentication

B. Because User Authentication requires authentication scheme that would not work with HTTP authentication

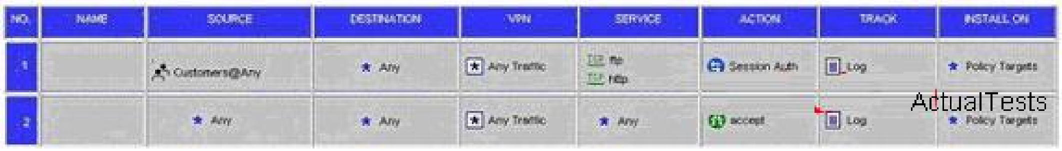
C. Because User Authentication requires authentication on a per-session basis which in contrast to HTTP that requires in many sessions

D. Because User Authentication requires authentication scheme that requires persession authentications
E. Because User Authentication requires authentication on a per-session basis which in contrast to HTTP that requires in one session

Answer: C

QUESTION NO: 194

Study the diagram and and then answer the question. What is likely to happen if a user from the internal network tries to access the Internet using HTTP?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1		Customers@Any	★ Any	Any Traffic	ftp http	Session Auth	Log	★ Policy Targets
2		★ Any	★ Any	Any Traffic	★ Any	accept	Log	★ Policy Targets

A. The user should be able to connect after successfully ftp connection
B. The user will not be able to go to the Internet
C. The user should be able to connect after successfully client- authenticated
D. The user should be able to connect after successfully authenticated
E. The user should be able to go to the Internet without being authenticated

Answer: E

QUESTION NO: 195

When deploying a new IP Appliance to replace an old one, the existing configuration may not necessarily map directly to the new appliance. Which of the following is true regarding the configuration that may not map to the new appliance?

A. The interface-naming convention
B. Some deprecated features
C. CLI
D. Backup - restore feature
E. Appliance might be flash-based while the old one was disk-based

Answer: A,B,E

QUESTION NO: 196

Which of the following are true of mesh and star community? Select all the correct answers.

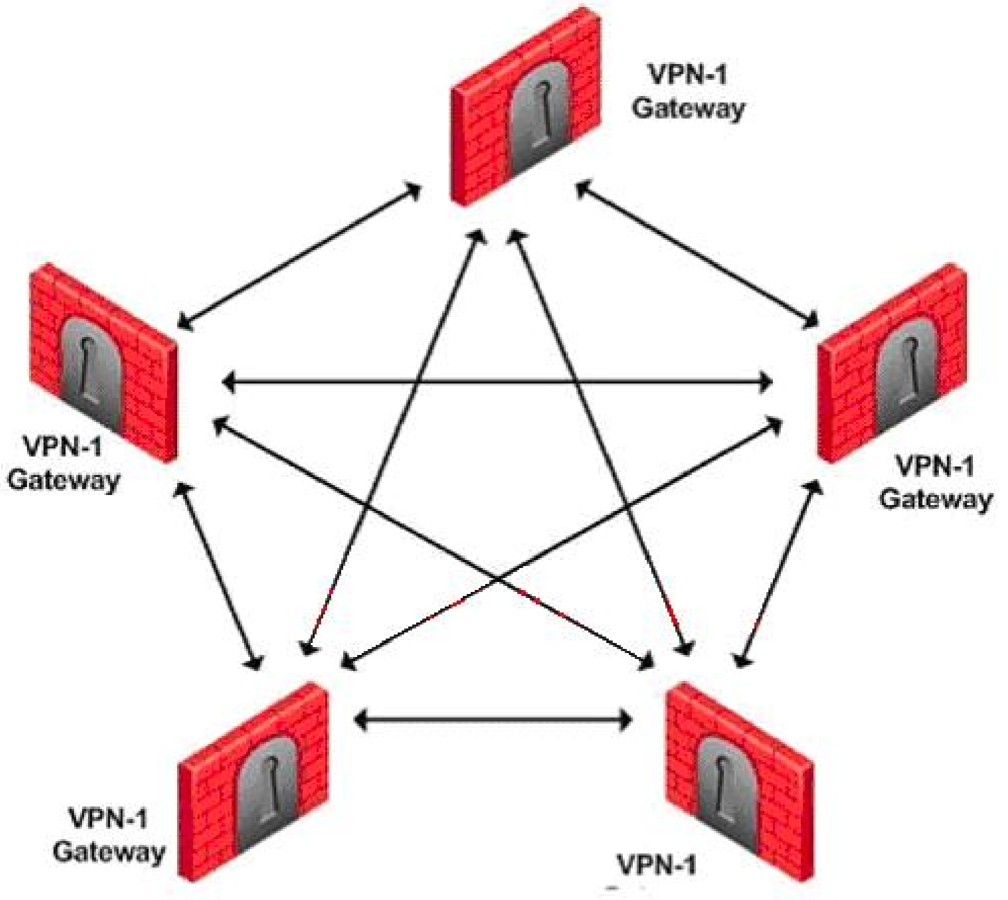


Figure 1: Basic Meshed community

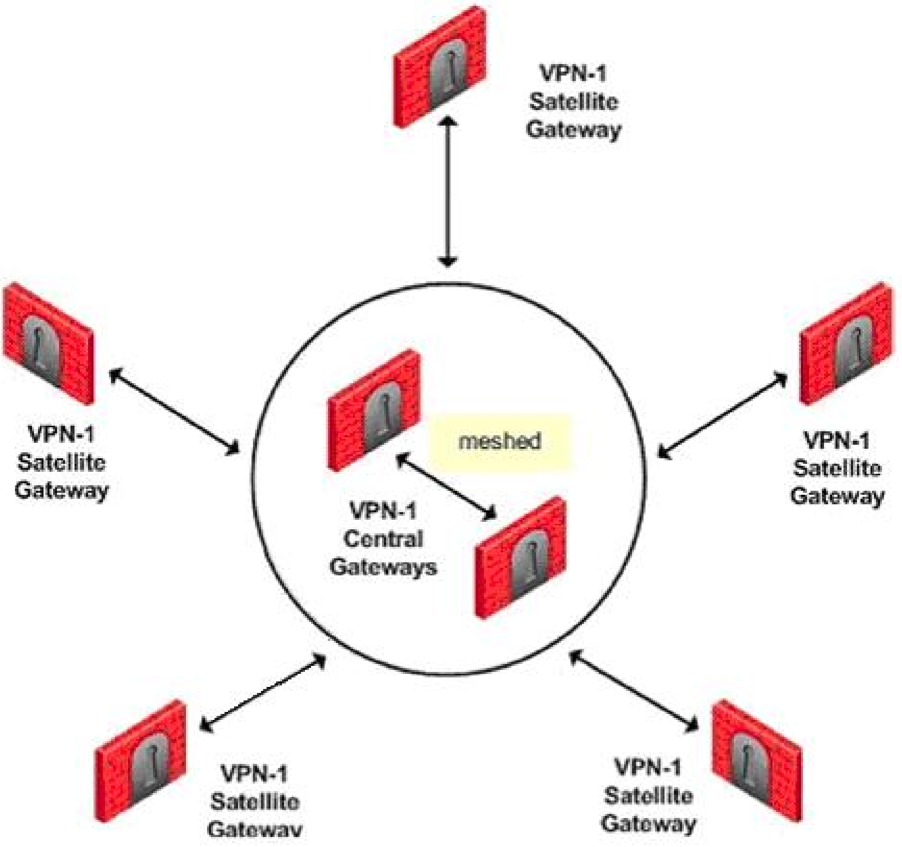
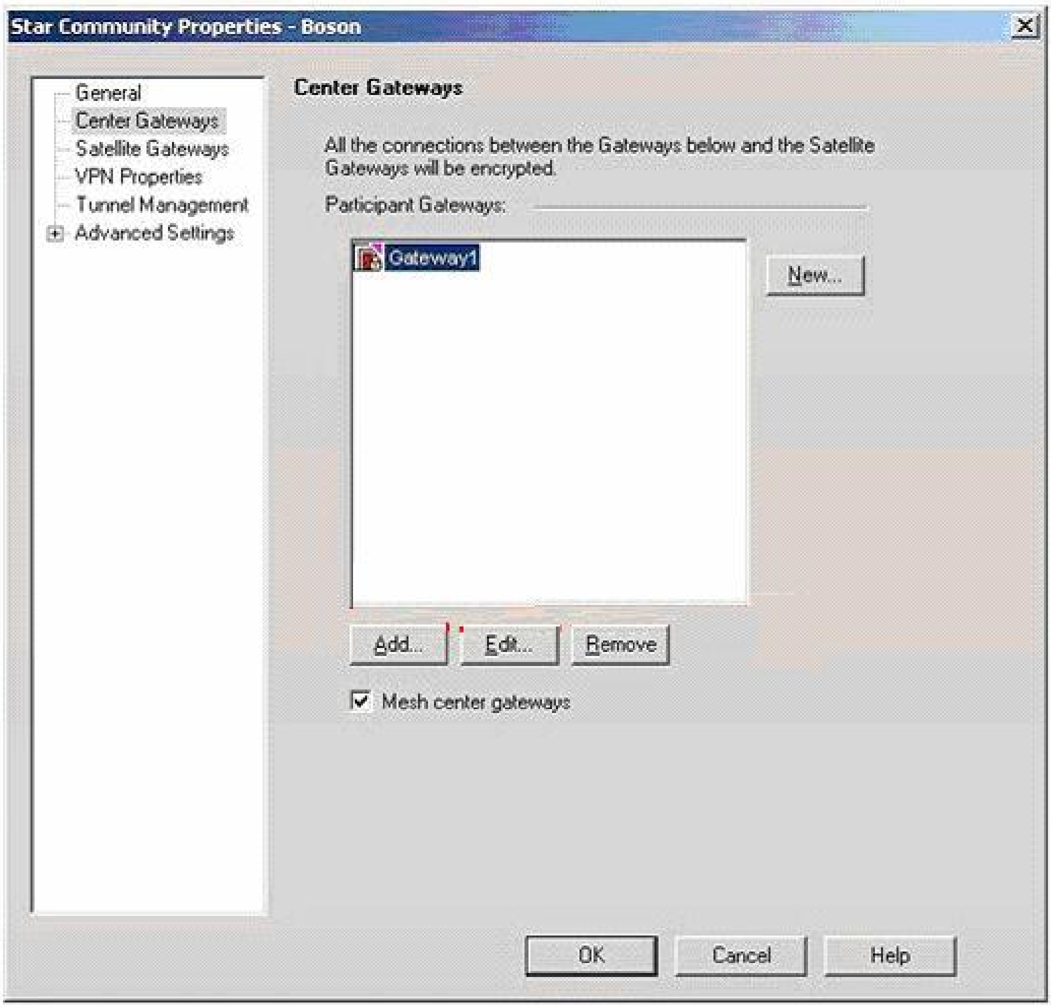


Figure 2: Star VPN community



Center Gateways

All the connections between the Gateways below and the Satellite Gateways will be encrypted.

Participant Gateways:

Gateway1

☑ Mesh center gateways

Figure 3: Star Community Properties window

A. In a mesh community, VPN site can create a VPN tunnel with any other VPN site in the community

B. In a mesh community, VPN site can create a VPN tunnel with any other gateway defined as a management station

C. In a star community, a satellite can create a tunnel only with other sites whose gateways are defined as central.

D. In a star community, a satellite gateway cannot create a VPN tunnel with a gateway that is also defined as a satellite gateway

E. In a star community, a central gateway cannot create a VPN tunnel with a gateway that is also defined as a central gateway

Answer: A,C,D

QUESTION NO: 197

What key in your keyboard provides methods of automatic command-line completion?

A. F1

B. CTRL A
C. Space key
D. Tab key
E. CTRL B

Answer: D

QUESTION NO: 198

What file must you edit to fine-tune your Eventia Reporter for improve performance? Assume you are dealing with Unix system.

A. userc.C
B. my.cnf
C. my.ini
D. userc.conf
E. objects_5_0.C

Answer: B

QUESTION NO: 199

In IPSO file structure, which of the following file enables execution of programs on startup?

A. /etc
B. /var/etc/rc.local
C. /config/db
D. /image
E. /var

Answer: B

QUESTION NO: 200

VPN routing between Gateways (star or mesh) can be configured by editing which of the following configuration file? Note: If wrong answer is chosen, see the diagram for correct answer.

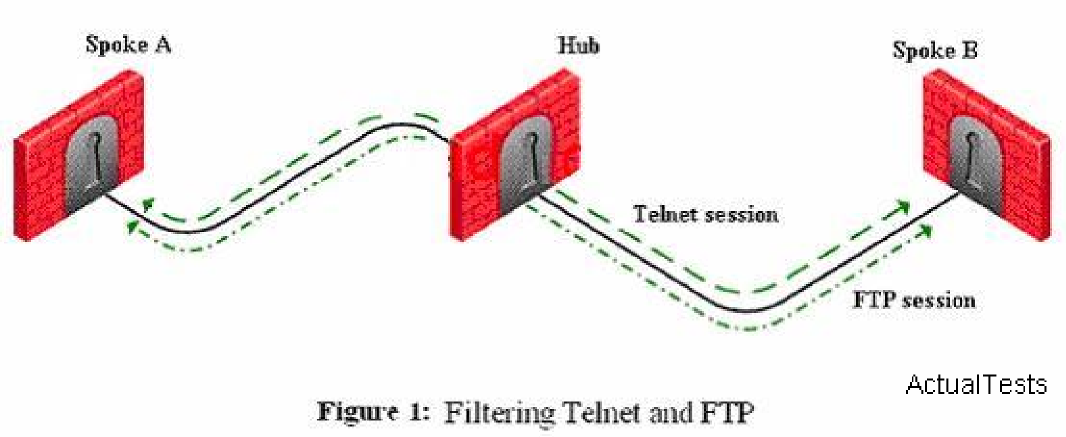


Figure 1: Filtering Telnet and FTP

A. $FWDIR\bin\amon_cpconfig.exe
B. $FWDIR\conf\vpn_route.conf
C. $FWDIR\conf\sic_policy.conf
D. $FWDIR\conf\users.C
E. $FWDIR\bin\cpconfig.exe

Answer: B

QUESTION NO: 201

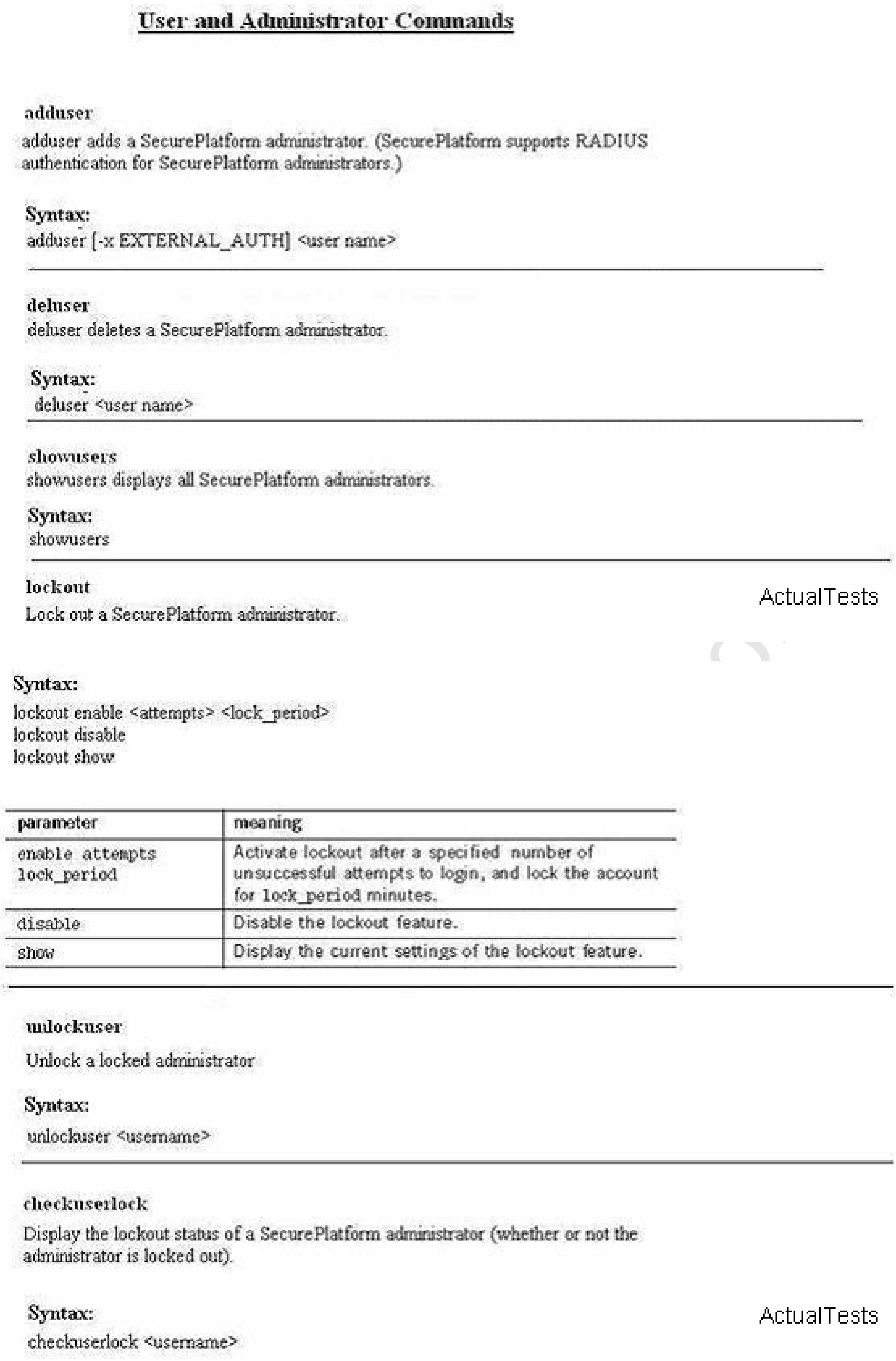
How many phases are involved in the IKE encryption scheme?

A. One phase
B. Five phases
C. Two phases
D. Four phases
E. Three phases

Answer: C

QUESTION NO: 202

Want do you intend to achieve by entering the command "lockout enable 3 30"?



User and Administrator Commands

adduser

adduser adds a SecurePlatform administrator. (SecurePlatform supports RADIUS authentication for SecurePlatform administrators.)

Syntax:

```
adduser [-x EXTERNAL_AUTH] <user name>
```

deluser

deluser deletes a SecurePlatform administrator.

Syntax:

```
deluser <user name>
```

showusers

showusers displays all SecurePlatform administrators.

Syntax:

```
showusers
```

lockout

Lock out a SecurePlatform administrator.

Syntax:

```
lockout enable <attempts> <lock_period>
lockout disable
lockout show
```

parameter	meaning
enable attempts lock_period	Activate lockout after a specified number of unsuccessful attempts to login, and lock the account for lock_period minutes.
disable	Disable the lockout feature.
show	Display the current settings of the lockout feature.

unlockuser

Unlock a locked administrator

Syntax:

```
unlockuser <username>
```

checkuserlock

Display the lockout status of a SecurePlatform administrator (whether or not the administrator is locked out).

Syntax:

```
checkuserlock <username>
```

A. De-activate account lockout after 3 unsuccessful attempts, and lock the account for30 minutes

B. Delete account lockout after 3 unsuccessful attempts, and lock the account for 30 minutes

C. Activate account lockout after 30 unsuccessful attempts, and lock the account for 3 minutes

D. Activate account lockout after 3 unsuccessful attempts, and lock the account for 30 minutes

E. De-activate account lockout after 30 unsuccessful attempts, and lock the account for 3 minutes

Answer: D

QUESTION NO: 203

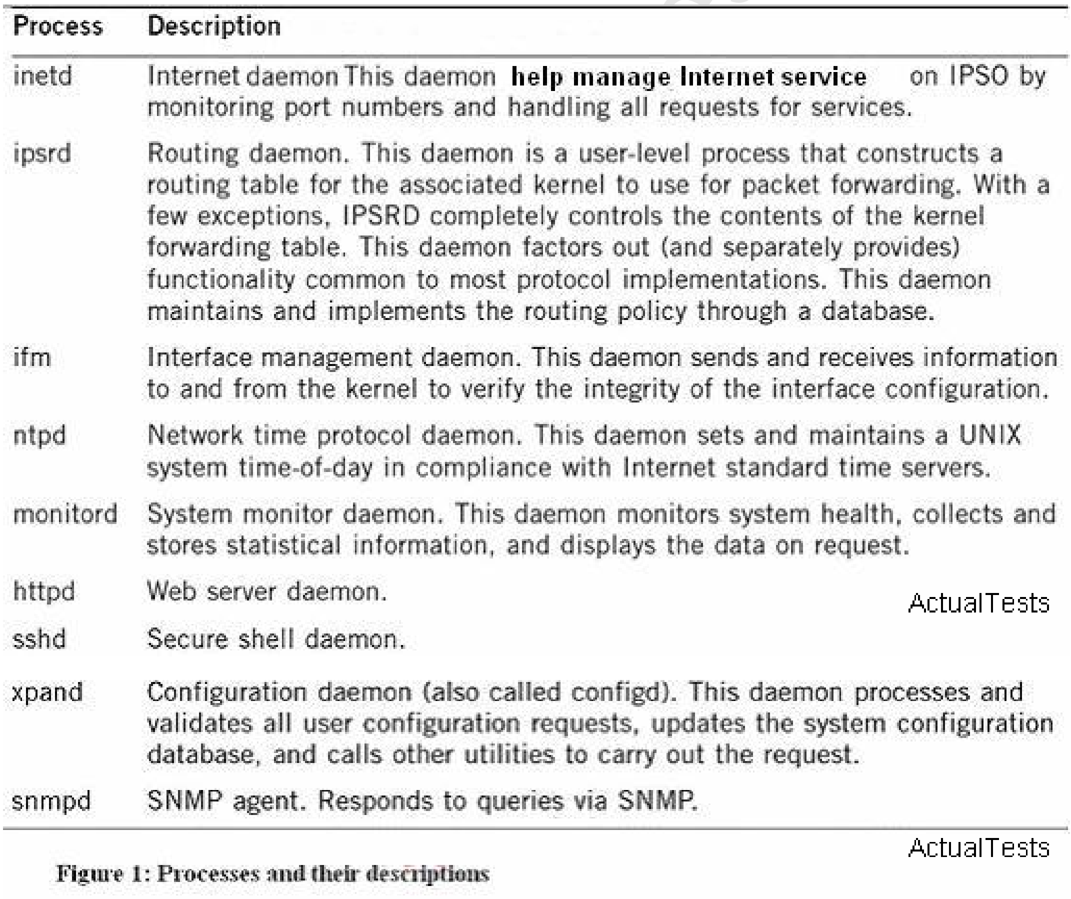
When you run FTP Activity report, you do not receive any datA. What would you do to rectify the issue?

A. For each FTP Activity, create the associated resource
B. For each FTP Activity, create the associated resource and add a rule in the Security Policy whose service column uses this resource
C. Do nothing
D. Configure each FTP Activity on the Global Properties
E. Configure each FTP Activity on the Gateway

Answer: B

QUESTION NO: 204

The process monitor (PM) monitors critical IPSO processes for their statuses and will try to restart any process that has terminated abnormally. If any process fails to start, the PM continues to try to restart it at what regular intervals?



Process	Description
inetd	Internet daemon This daemon **help manage Internet service** on IPSO by monitoring port numbers and handling all requests for services.
ipsrd	Routing daemon. This daemon is a user-level process that constructs a routing table for the associated kernel to use for packet forwarding. With a few exceptions, IPSRD completely controls the contents of the kernel forwarding table. This daemon factors out (and separately provides) functionality common to most protocol implementations. This daemon maintains and implements the routing policy through a database.
ifm	Interface management daemon. This daemon sends and receives information to and from the kernel to verify the integrity of the interface configuration.
ntpd	Network time protocol daemon. This daemon sets and maintains a UNIX system time-of-day in compliance with Internet standard time servers.
monitord	System monitor daemon. This daemon monitors system health, collects and stores statistical information, and displays the data on request.
httpd	Web server daemon.
sshd	Secure shell daemon.
xpand	Configuration daemon (also called configd). This daemon processes and validates all user configuration requests, updates the system configuration database, and calls other utilities to carry out the request.
snmpd	SNMP agent. Responds to queries via SNMP.

Figure 1: Processes and their descriptions

A. Interval of 2 seconds

B. Interval of 10 seconds
C. Interval of 4 seconds
D. Interval of 12 seconds
E. Interval of 8 seconds

Answer: A

QUESTION NO: 205

What is the purpose of Action element in the rule base?

A. The Action element determines when the firewall hosts have to be replaced
B. The Action element determines when the firewall hosts and gateways services need to be rebooted
C. The Action element determines where on host on the external network it needs to forward the packets
D. The Action element determines what firewall needs to do with packets
E. The Action element determines when the firewall hosts and gateways services need to be restarted

Answer: D

QUESTION NO: 206

What is the job of URL Filtering Protocol (UFP) server?3

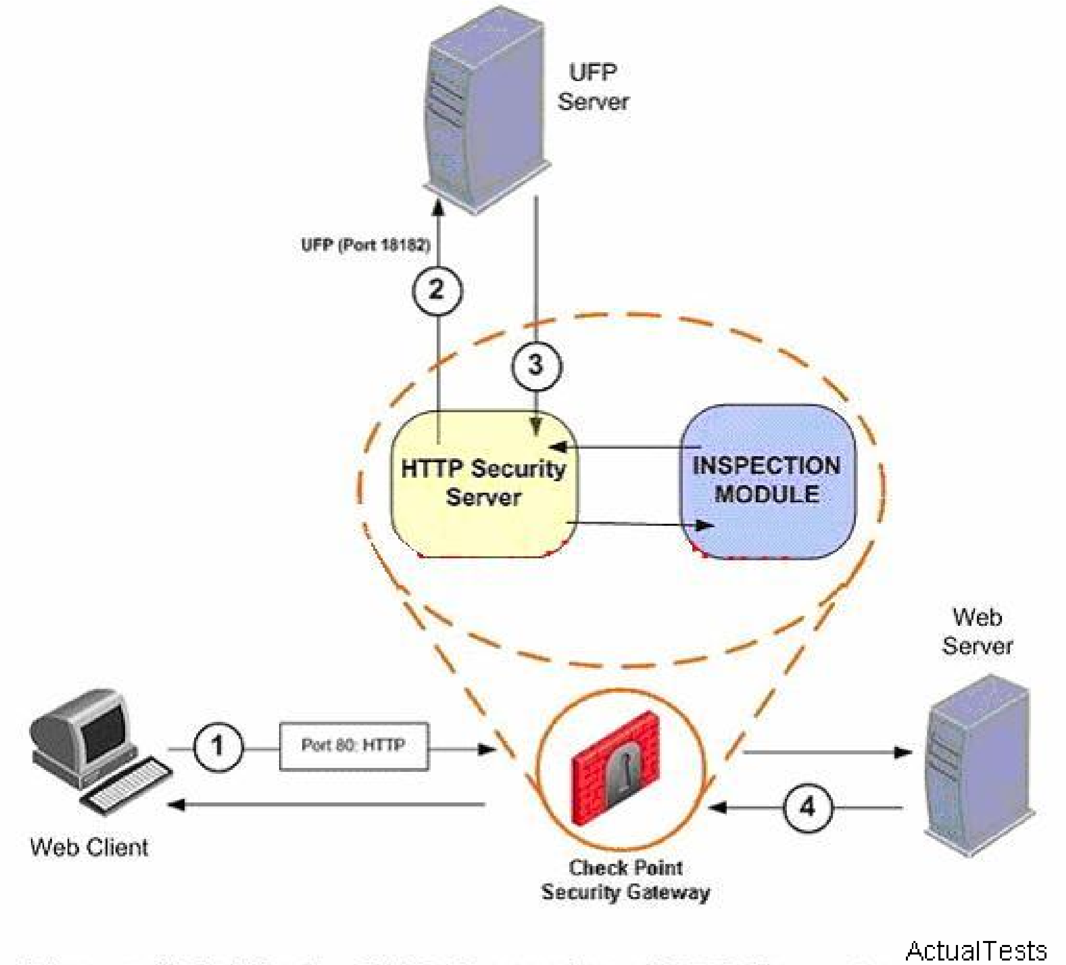


Figure 1: URL Filtering (UFP) Process for an HTTP Connection

A. It blocks the unwanted URL

B. It allows fast secure connections between the CVP servers and the Security Gateway

C. It maintains a list of URLs and their categories

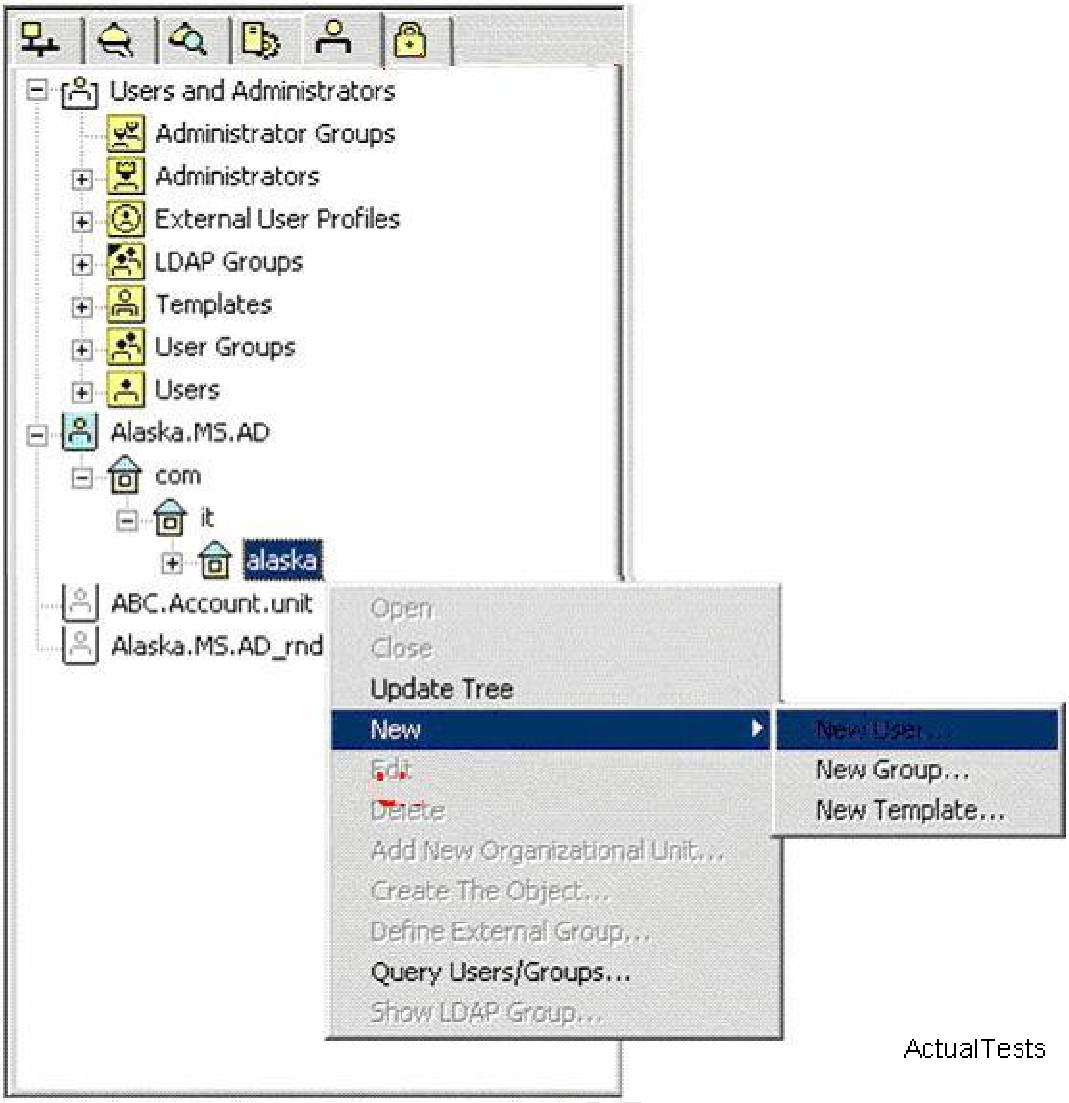
D. It maintains the list of SmartConsole clients that allowto connect to Security Management Server

E. It allows access to resources

Answer: C

QUESTION NO: 207

Which of the following is true of user management on a SmartDirectory (LDAP) server?



A. Changes that are applied to a SmartDirectory (LDAP) template are reflected the next time the users reboot the machines

B. User Management depends on the situation of Accounts Units

C. User management in the SmartDirectory (LDAP) server is done externally

D. User management in the SmartDirectory (LDAP) server is done locally

E. Changes that are applied to a SmartDirectory (LDAP) template are reflected immediately for all users who are using that template

Answer: C,E

QUESTION NO: 208

Which of the following does the Security Gateway R70 use for guaranteeing the integrity and authenticity of messages?

A. Digital signatures

B. Application Intelligence

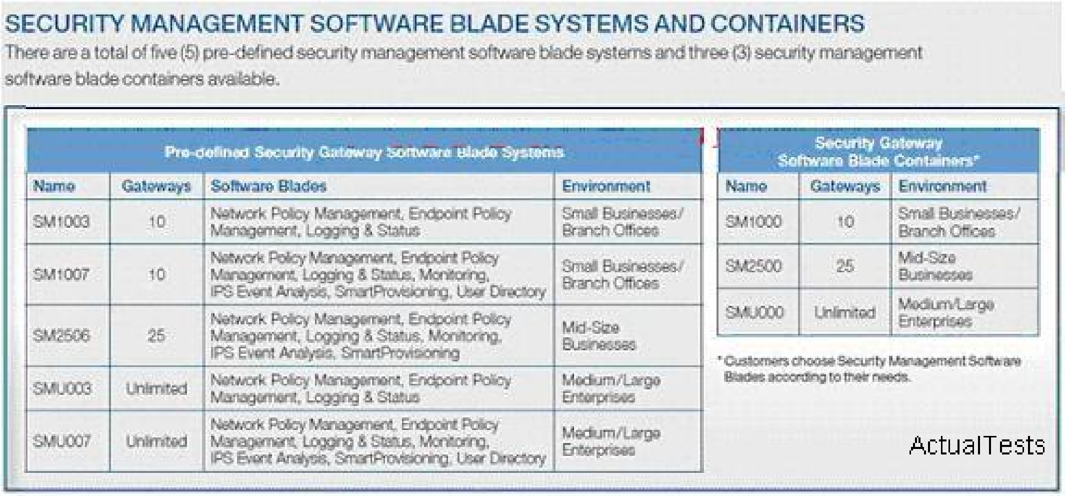
C. IPSec

D. 3DES
E. Web Intelligence

Answer: A

QUESTION NO: 209

You want to configure Software Blade Containers and you have two types which you have to choose from. You run small business and have 30 users. You want to choose a 1core system. Which of the following model are you likely to run? Choose all the correct answers.



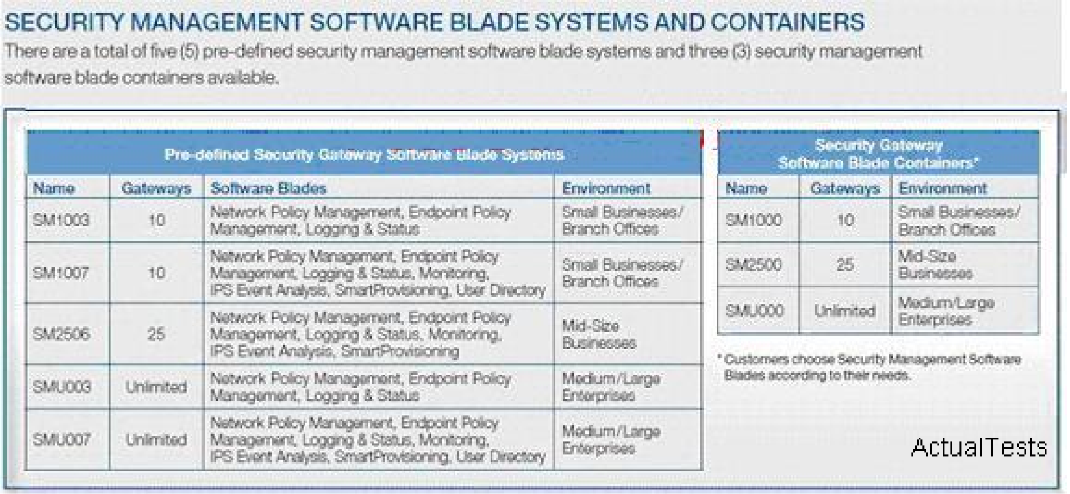
SECURITY MANAGEMENT SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of five (5) pre-defined security management software blade systems and three (3) security management software blade containers available.

Pre-defined Security Gateway Software Blade Systems			
Name	Gateways	Software Blades	Environment
SM1003	10	Network Policy Management, Endpoint Policy Management, Logging & Status	Small Businesses/ Branch Offices
SM1007	10	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Small Businesses/ Branch Offices
SM2506	25	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning	Mid-Size Businesses
SMU003	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status	Medium/Large Enterprises
SMU007	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Medium/Large Enterprises

Security Gateway Software Blade Containers*		
Name	Gateways	Environment
SM1000	10	Small Businesses/ Branch Offices
SM2500	25	Mid-Size Businesses
SMU000	Unlimited	Medium/Large Enterprises

* Customers choose Security Management Software Blades according to their needs.



SECURITY MANAGEMENT SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of five (5) pre-defined security management software blade systems and three (3) security management software blade containers available.

Pre-defined Security Gateway Software Blade Systems			
Name	Gateways	Software Blades	Environment
SM1003	10	Network Policy Management, Endpoint Policy Management, Logging & Status	Small Businesses/ Branch Offices
SM1007	10	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Small Businesses/ Branch Offices
SM2506	25	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning	Mid-Size Businesses
SMU003	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status	Medium/Large Enterprises
SMU007	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Medium/Large Enterprises

Security Gateway Software Blade Containers*		
Name	Gateways	Environment
SM1000	10	Small Businesses/ Branch Offices
SM2500	25	Mid-Size Businesses
SMU000	Unlimited	Medium/Large Enterprises

* Customers choose Security Management Software Blades according to their needs.

ActualTests

A. SG106
B. SG203
C. SG103
D. SG20
E. SG102

Answer: A,C

QUESTION NO: 210

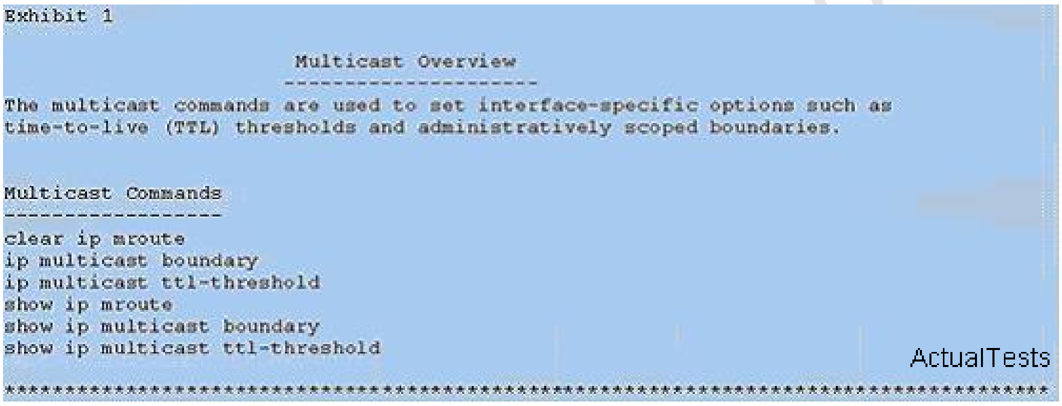
The fundamental concepts of the Security Rule Base is "That which is not explicitly permitted is ____________________".

A. logged
B. prohibited
C. perfected
D. forbidden
E. logging

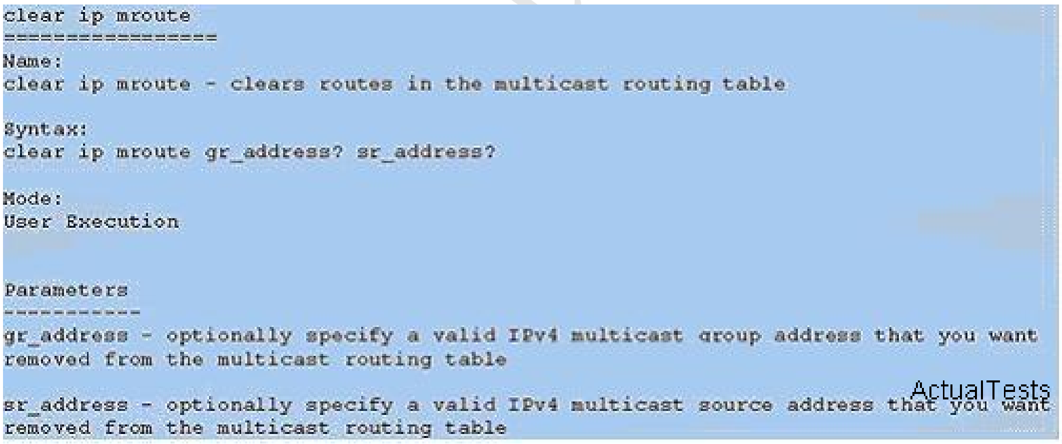
Answer: B

QUESTION NO: 211

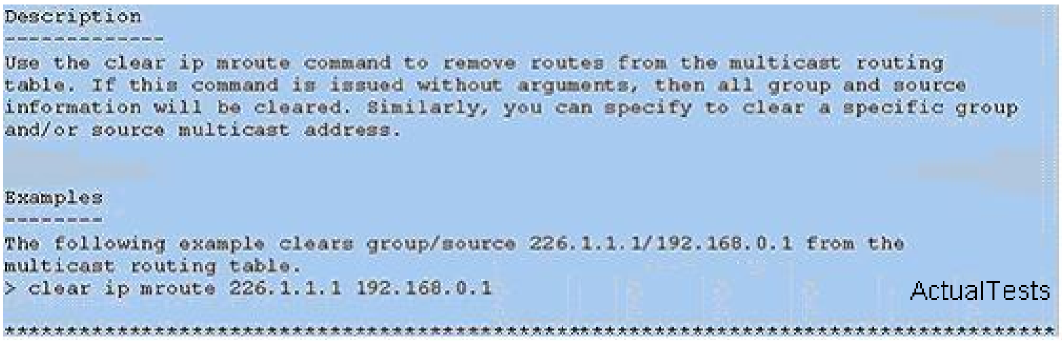
Which of the following multicast commands would you use to remove routes from the multicast routing table?



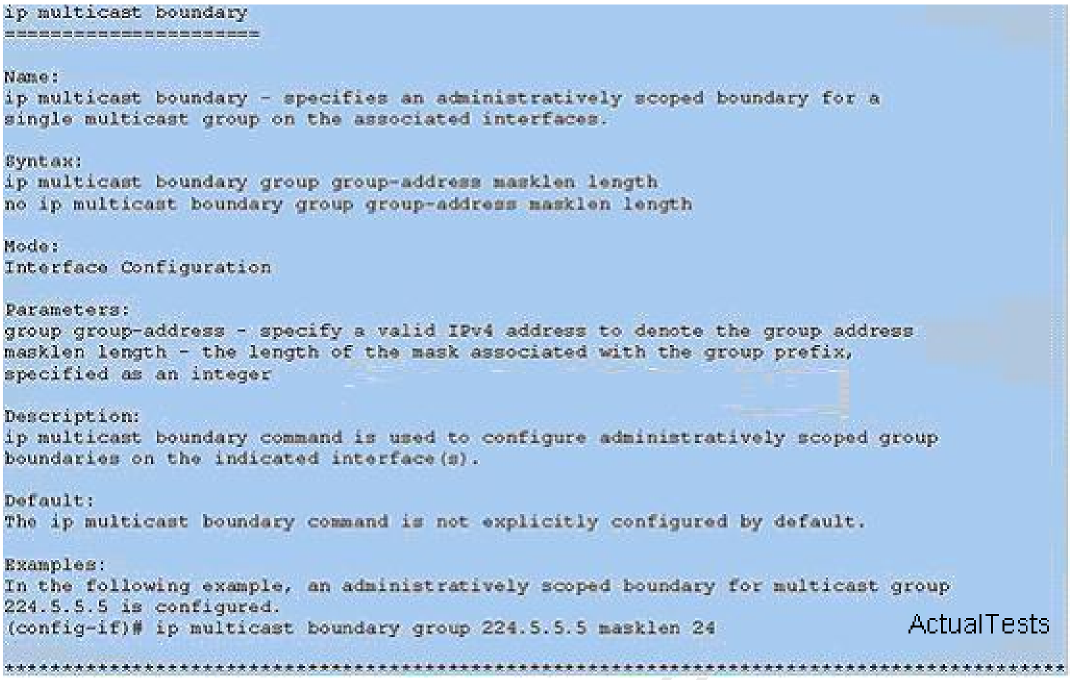
```
Exhibit 1

                         Multicast Overview
                        ----------------------
The multicast commands are used to set interface-specific options such as
time-to-live (TTL) thresholds and administratively scoped boundaries.


Multicast Commands
------------------
clear ip mroute
ip multicast boundary
ip multicast ttl-threshold
show ip mroute
show ip multicast boundary
show ip multicast ttl-threshold

****************************************************************************************
```



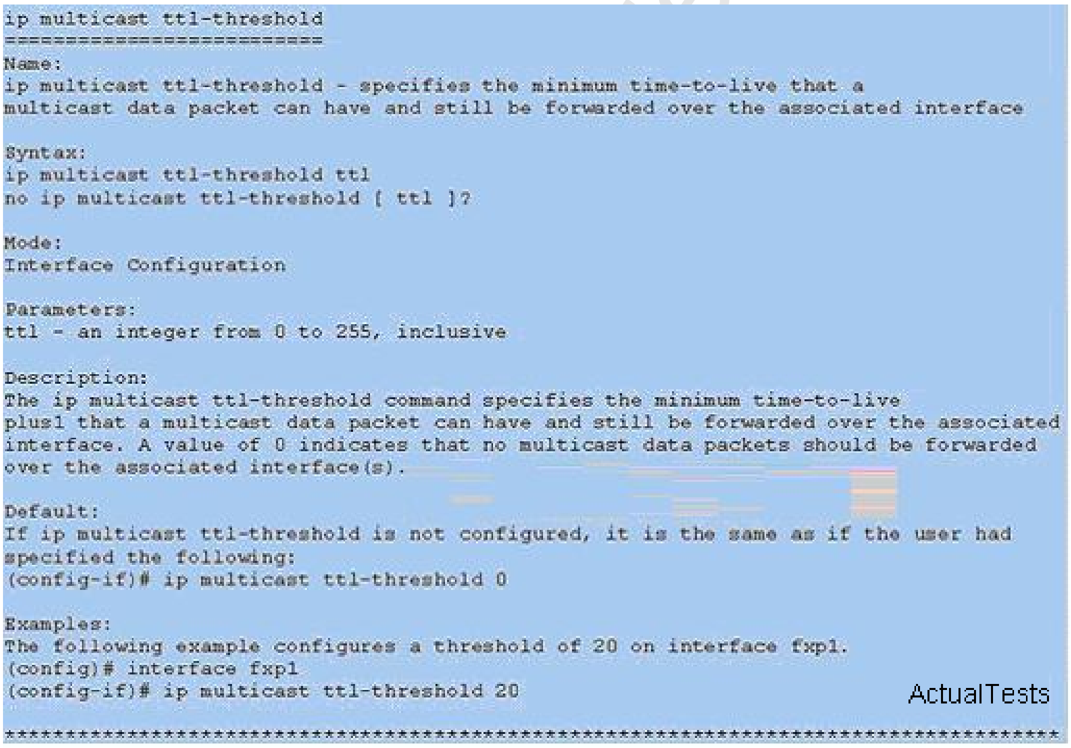
```
clear ip mroute
==================
Name:
clear ip mroute - clears routes in the multicast routing table

Syntax:
clear ip mroute gr_address? sr_address?

Mode:
User Execution


Parameters
-----------
gr_address - optionally specify a valid IPv4 multicast group address that you want
removed from the multicast routing table

sr_address - optionally specify a valid IPv4 multicast source address that you want
removed from the multicast routing table
```



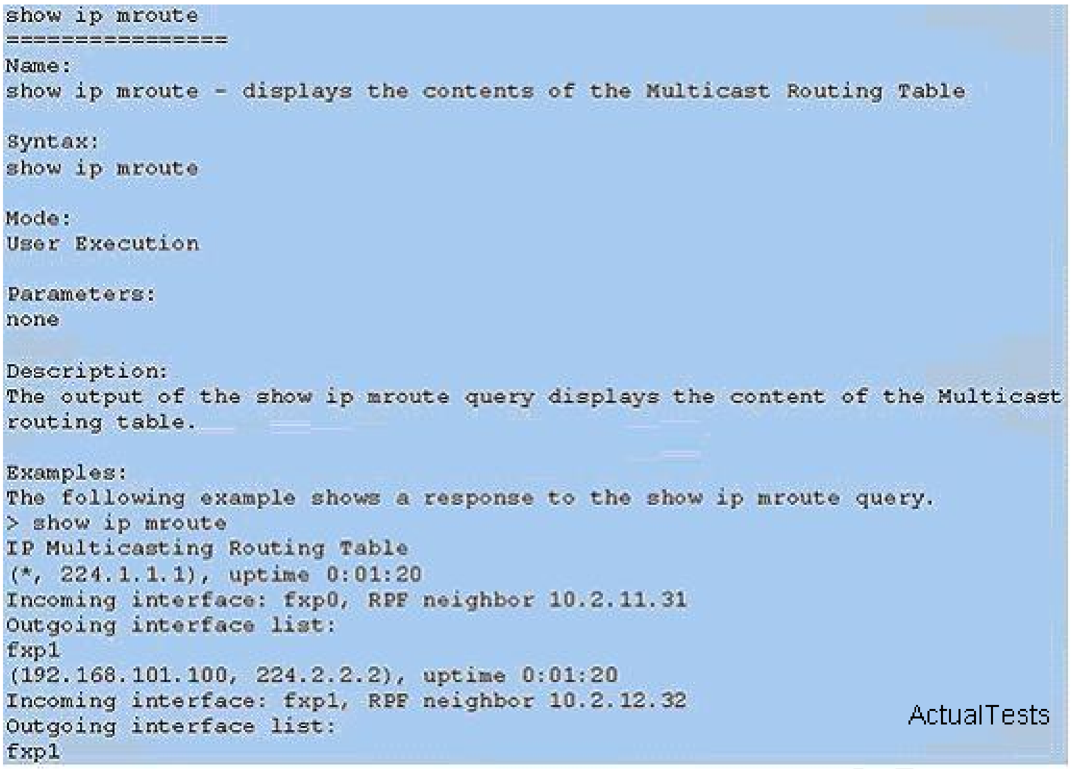
```
Description
-------------
Use the clear ip mroute command to remove routes from the multicast routing
table. If this command is issued without arguments, then all group and source
information will be cleared. Similarly, you can specify to clear a specific group
and/or source multicast address.


Examples
--------
The following example clears group/source 226.1.1.1/192.168.0.1 from the
multicast routing table.
> clear ip mroute 226.1.1.1 192.168.0.1

*****************************************************************************************
```



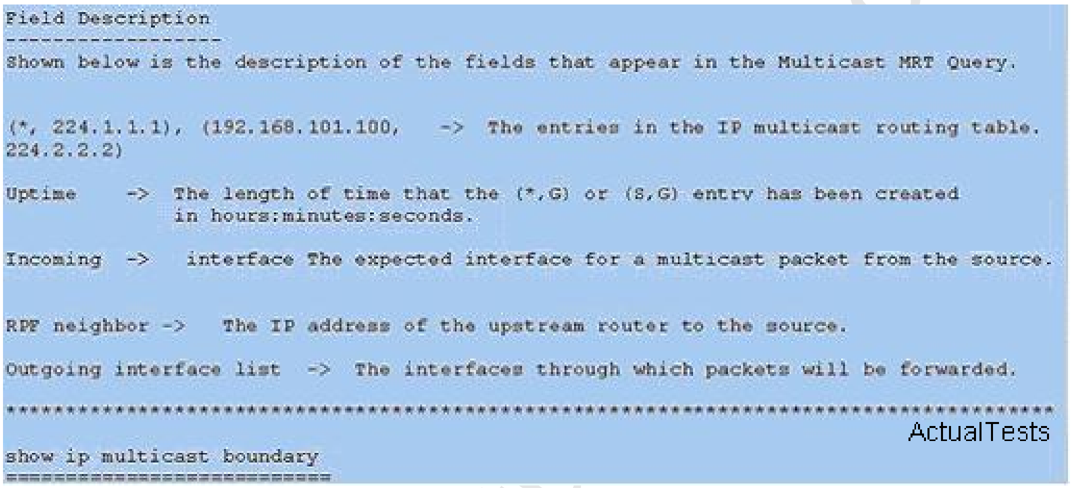
```
ip multicast boundary
======================

Name:
ip multicast boundary - specifies an administratively scoped boundary for a
single multicast group on the associated interfaces.

Syntax:
ip multicast boundary group group-address masklen length
no ip multicast boundary group group-address masklen length

Mode:
Interface Configuration

Parameters:
group group-address - specify a valid IPv4 address to denote the group address
masklen length - the length of the mask associated with the group prefix,
specified as an integer

Description:
ip multicast boundary command is used to configure administratively scoped group
boundaries on the indicated interface(s).

Default:
The ip multicast boundary command is not explicitly configured by default.

Examples:
In the following example, an administratively scoped boundary for multicast group
224.5.5.5 is configured.
(config-if)# ip multicast boundary group 224.5.5.5 masklen 24

*****************************************************************************************
```



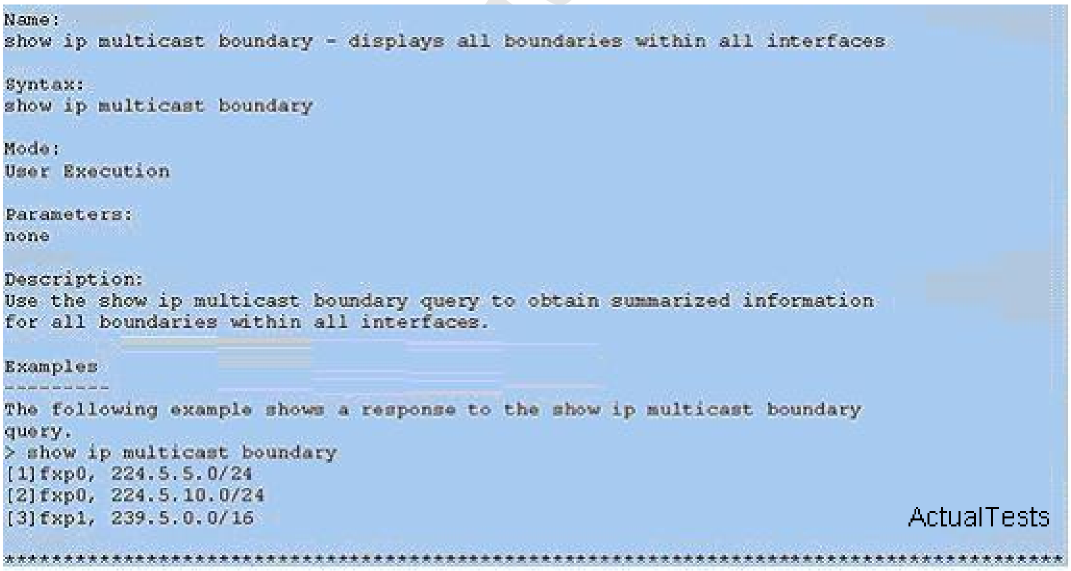
```
ip multicast ttl-threshold
===========================
Name:
ip multicast ttl-threshold - specifies the minimum time-to-live that a
multicast data packet can have and still be forwarded over the associated interface

Syntax:
ip multicast ttl-threshold ttl
no ip multicast ttl-threshold [ ttl ]?

Mode:
Interface Configuration

Parameters:
ttl - an integer from 0 to 255, inclusive

Description:
The ip multicast ttl-threshold command specifies the minimum time-to-live
plus1 that a multicast data packet can have and still be forwarded over the associated
interface. A value of 0 indicates that no multicast data packets should be forwarded
over the associated interface(s).

Default:
If ip multicast ttl-threshold is not configured, it is the same as if the user had
specified the following:
(config-if)# ip multicast ttl-threshold 0

Examples:
The following example configures a threshold of 20 on interface fxp1.
(config)# interface fxp1
(config-if)# ip multicast ttl-threshold 20

*****************************************************************************************
```



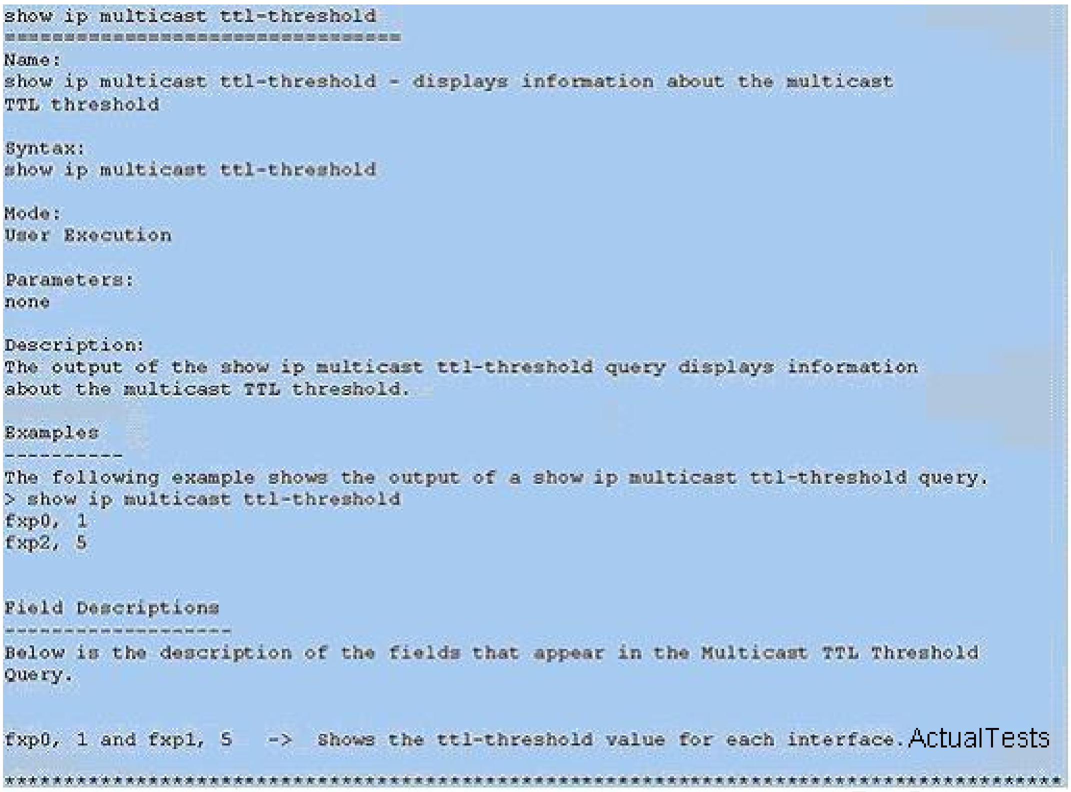
```
show ip mroute
================
Name:
show ip mroute - displays the contents of the Multicast Routing Table

Syntax:
show ip mroute

Mode:
User Execution

Parameters:
none

Description:
The output of the show ip mroute query displays the content of the Multicast
routing table.

Examples:
The following example shows a response to the show ip mroute query.
> show ip mroute
IP Multicasting Routing Table
(*, 224.1.1.1), uptime 0:01:20
Incoming interface: fxp0, RPF neighbor 10.2.11.31
Outgoing interface list:
fxp1
(192.168.101.100, 224.2.2.2), uptime 0:01:20
Incoming interface: fxp1, RPF neighbor 10.2.12.32
Outgoing interface list:
fxp1
```



```
Field Description
------------------
Shown below is the description of the fields that appear in the Multicast MRT Query.


(*, 224.1.1.1), (192.168.101.100,   ->  The entries in the IP multicast routing table.
224.2.2.2)

Uptime     ->  The length of time that the (*,G) or (S,G) entrv has been created
               in hours:minutes:seconds.

Incoming  ->   interface The expected interface for a multicast packet from the source.


RPF neighbor ->   The IP address of the upstream router to the source.

Outgoing interface list   ->  The interfaces through which packets will be forwarded.

*******************************************************************************************

show ip multicast boundary
============================
```



```
Name:
show ip multicast boundary - displays all boundaries within all interfaces

Syntax:
show ip multicast boundary

Mode:
User Execution

Parameters:
none

Description:
Use the show ip multicast boundary query to obtain summarized information
for all boundaries within all interfaces.

Examples
---------
The following example shows a response to the show ip multicast boundary
query.
> show ip multicast boundary
[1]fxp0, 224.5.5.0/24
[2]fxp0, 224.5.10.0/24
[3]fxp1, 239.5.0.0/16

*******************************************************************************************
```



```
show ip multicast ttl-threshold
=================================
Name:
show ip multicast ttl-threshold - displays information about the multicast
TTL threshold

Syntax:
show ip multicast ttl-threshold

Mode:
User Execution

Parameters:
none

Description:
The output of the show ip multicast ttl-threshold query displays information
about the multicast TTL threshold.

Examples
----------
The following example shows the output of a show ip multicast ttl-threshold query.
> show ip multicast ttl-threshold
fxp0, 1
fxp2, 5


Field Descriptions
-------------------
Below is the description of the fields that appear in the Multicast TTL Threshold
Query.


fxp0, 1 and fxp1, 5   ->  Shows the ttl-threshold value for each interface.
**************************************************************************************************
```

A. clear ip mroute

B. ip multicast boundary

C. show ip mroute

D. show ip multicast boundary

E. ip multicast ttl-threshold

Answer: A

QUESTION NO: 212

To display the contents of the Multicast Routing Table, you will use which of the following commands?

A. show ip mroute

B. ip multicast boundary

C. ip multicast ttl-threshold

D. show ip multicast boundary

E. clear ip mroute

Answer: A

QUESTION NO: 213

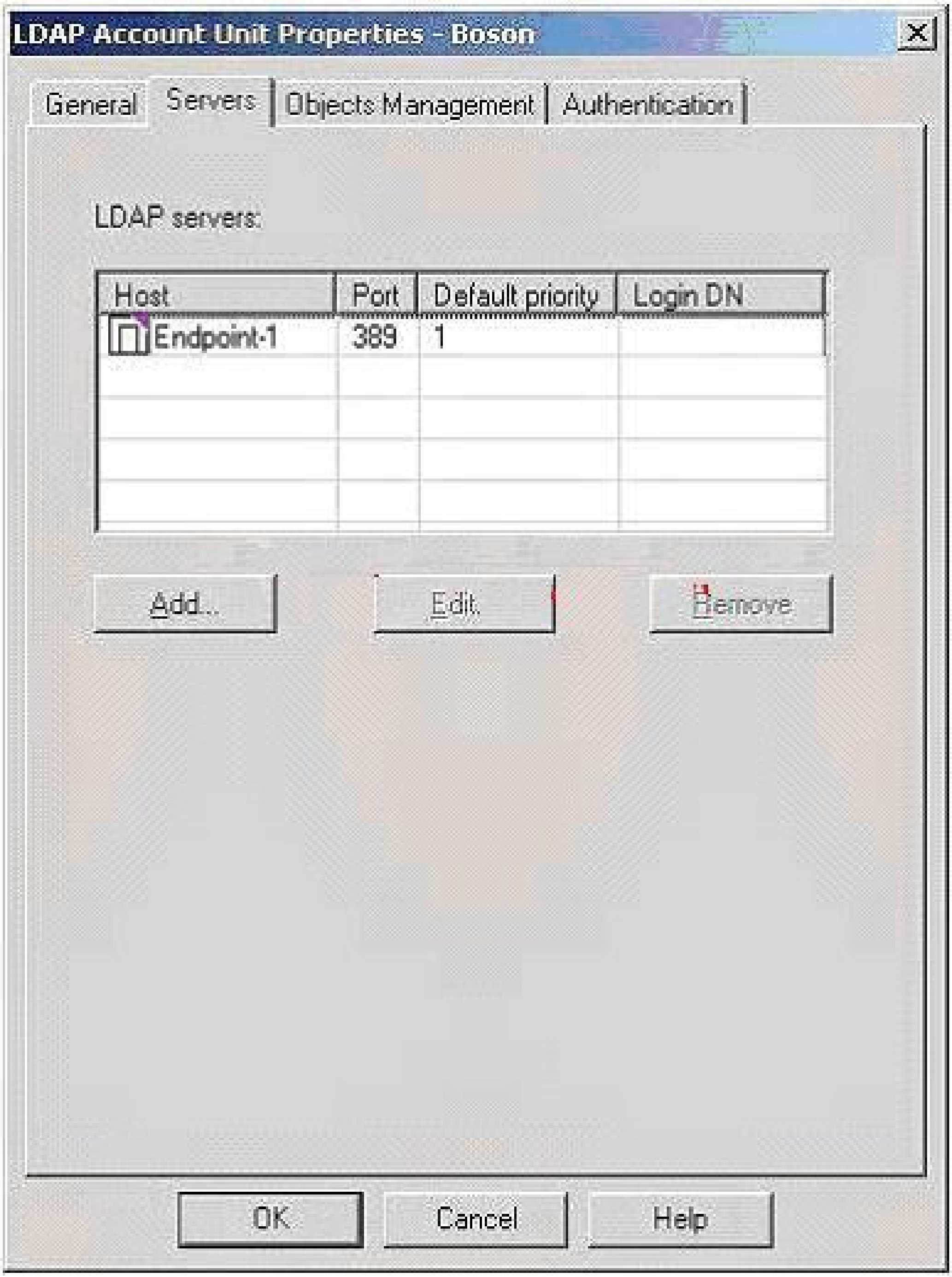
The command " show ip multicast boundary" query will:

A. Display the content of the Multicast routing table
B. Remove routes from the multicast routing table
C. Obtain summarized information for all boundaries within all interfaces
D. Specify the minimum time-to-live plus1 that a multicast data packet can have and still be forwarded over the associated interface
E. Display information about the multicast TTL threshold

Answer: C

QUESTION NO: 214

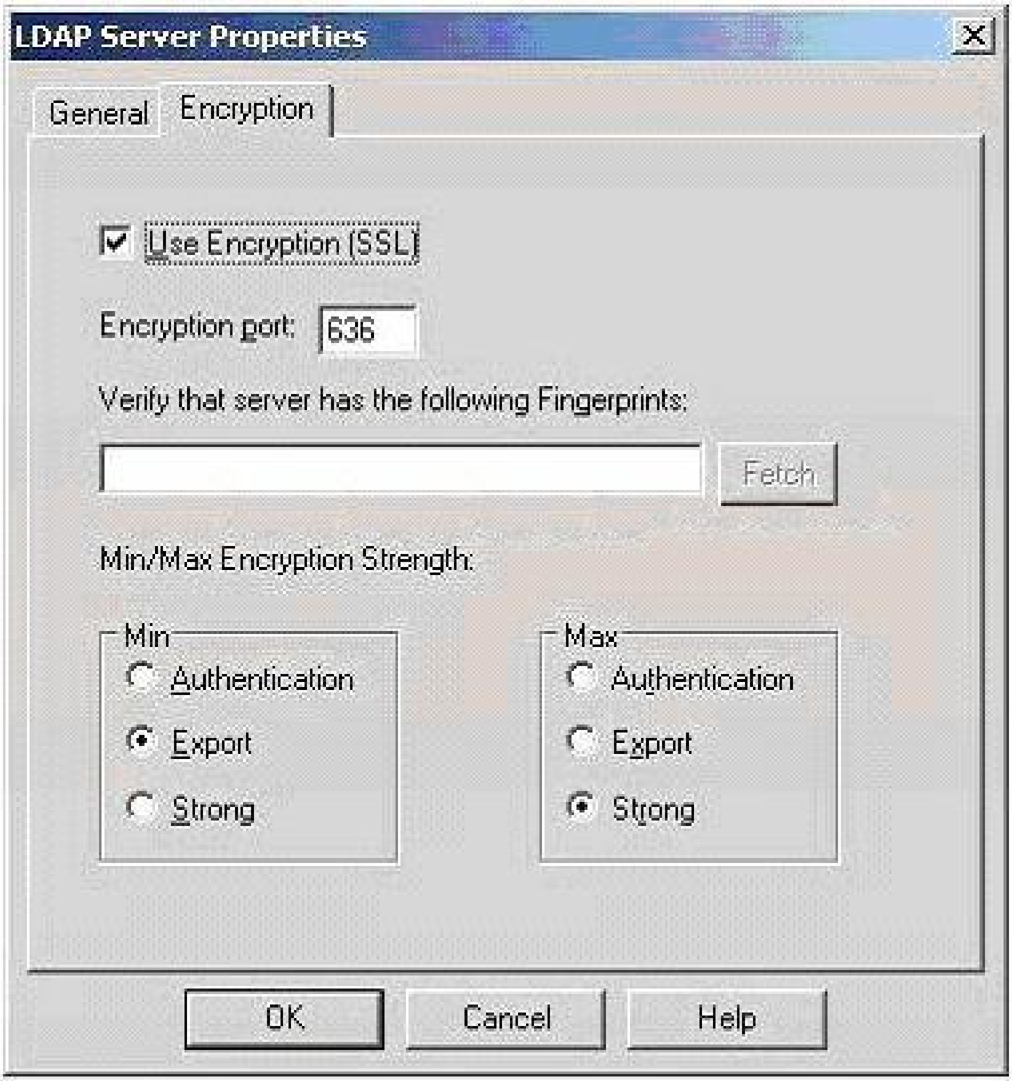
The Security Management server and its gateways can be issued special certificates in order to allow them to communicate with SmartDirectory (LDAP)) server. In addition to this, what parameter must be set in objects_5_0.C file?



LDAP servers:

Host	Port	Default priority	Login DN
Endpoint-1	389	1	

Figure 1: LDAP Account Unit Properties window.



LDAP Server Properties

General | Encryption

☑ Use Encryption (SSL)

Encryption port: 636

Verify that server has the following Fingerprints:

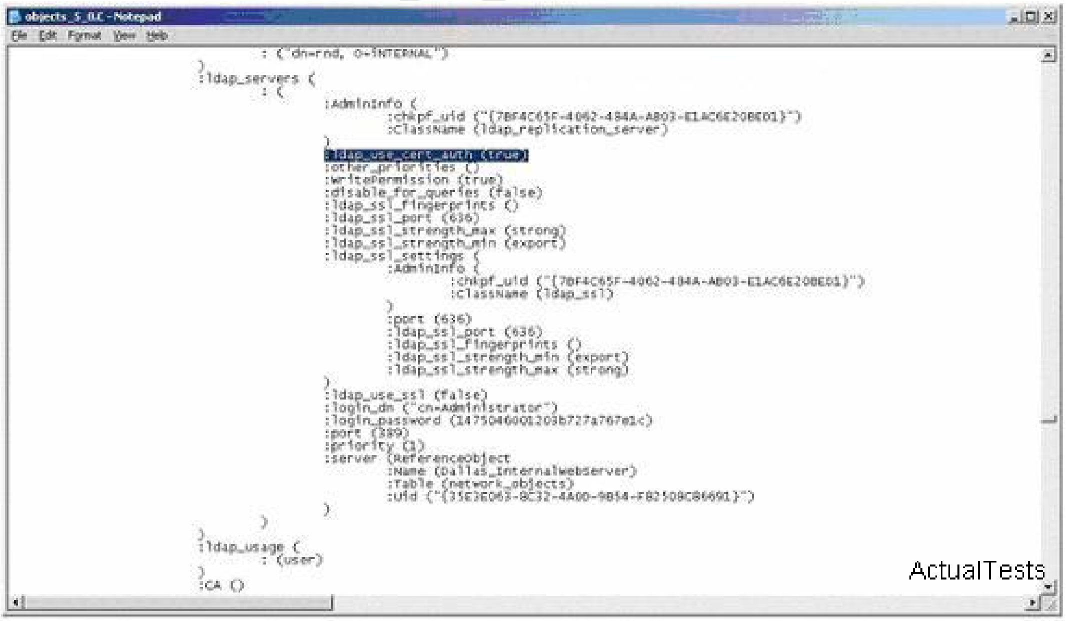
Min/Max Encryption Strength:

Min: ○ Authentication ● Export ○ Strong

Max: ○ Authentication ○ Export ● Strong

Figure 2: LDAP Server Properties Windows

If you click on Server tab, you will get LDAP Server Properties window shown in figure 2.



objects_5_0.C - Notepad

```
                : ("dn=rnd, o=INTERNAL")
        )
        :ldap_servers (
                : (
                        :AdminInfo (
                                :chkpf_uid ("{7BF4C65F-4062-484A-AB03-E1AC6E20BE01}")
                                :ClassName (ldap_replication_server)
                        )
                        :ldap_use_cert_auth (true)
                        :other_priorities ()
                        :writePermission (true)
                        :disable_for_queries (false)
                        :ldap_ssl_fingerprints ()
                        :ldap_ssl_port (636)
                        :ldap_ssl_strength_max (strong)
                        :ldap_ssl_strength_min (export)
                        :ldap_ssl_settings (
                                :AdminInfo (
                                        :chkpf_uid ("{7BF4C65F-4062-484A-AB03-E1AC6E20BE01}")
                                        :ClassName (ldap_ssl)
                                )
                                :port (636)
                                :ldap_ssl_port (636)
                                :ldap_ssl_fingerprints ()
                                :ldap_ssl_strength_min (export)
                                :ldap_ssl_strength_max (strong)
                        )
                        :ldap_use_ssl (false)
                        :login_dn ("cn=Administrator")
                        :login_password (14750460012036727a767e1c)
                        :port (389)
                        :priority (1)
                        :server (ReferenceObject
                                :Name (Dallas_Internalwebserver)
                                :Table (network_objects)
                                :Uid ("{35E3E063-8C32-4A00-9854-FB2508C86691}")
                        )
                )
        )
        :ldap_usage (
                : (user)
        )
        :CA ()
```

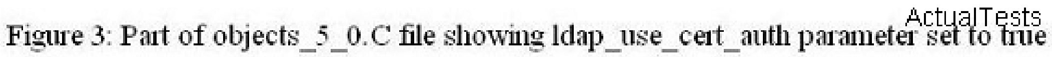


Figure 3: Part of objects_5_0.C file showing ldap_use_cert_auth parameter set to true

ActualTests

A. Set ldap_ssl_ldap_server to false
B. Set ldap_use_cert_auth to true
C. Set ldap_use_ldap_server to true
D. Set ldap_use_ssl to false
E. Set ldap_ssl_fingerprints to true

Answer: B

QUESTION NO: 215

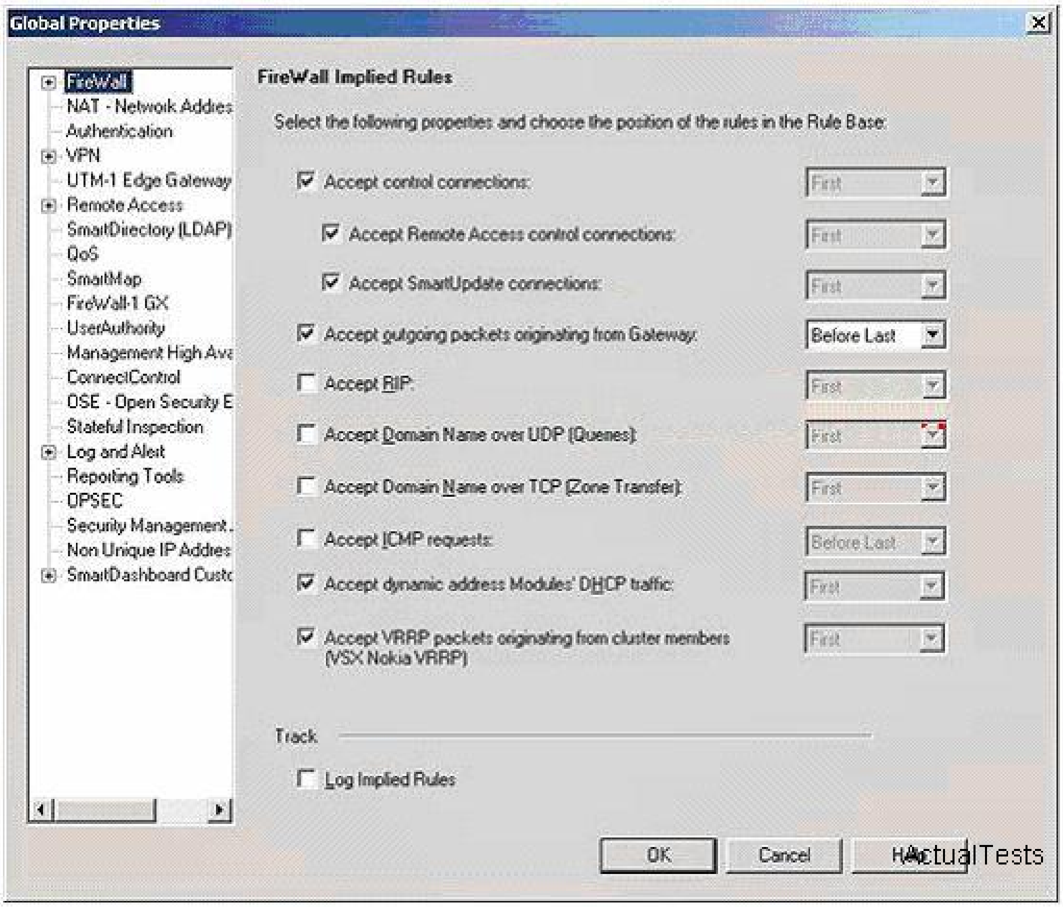
What would happen to the disabled rules if you fail to re-install your security policy after reenabling these disabled rules?

A. The disabled rules will re-install service
B. The disabled rules will enableitself automatically
C. The disabled rules will re-installitself automatically
D. The disabled rules will enforce you to re-install the security policy
E. The disabled rules remain disabled

Answer: E

QUESTION NO: 216

How would you access Global Properties? Choose the best answer.



FireWall Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

- ☑ Accept control connections: First
  - ☑ Accept Remote Access control connections: First
  - ☑ Accept SmartUpdate connections: First
- ☑ Accept outgoing packets originating from Gateway: Before Last
- □ Accept RIP: First
- □ Accept Domain Name over UDP (Queries): First
- □ Accept Domain Name over TCP (Zone Transfer): First
- □ Accept ICMP requests: Before Last
- ☑ Accept dynamic address Modules' DHCP traffic: First
- ☑ Accept VRRP packets originating from cluster members (VSX Nokia VRRP): First

Track

- □ Log Implied Rules

A. FromSmartDashboard , choose the window menu and select Global Properties

B. From SmartDashboard, click on Policy menu and select Global Properties...

C. From SmartView Status, click on Policy menu and select Global Properties...

D. From SmartView Tracker, click on Policy menu and select Properties...

E. From SmartLSM, click on Policy menu and select Global Properties...

Answer: B

QUESTION NO: 217

For SecuRemote/SecureClient to resolve the names of internal hosts behind the Security Gateway with non-unique IP addresses using an internal DNS server, what must you implement?

A. VPN Routing

B. Office Mode

C. IPS

D. Layer Two Transfer Protocol

E. Connect Mode

Answer: B,E

QUESTION NO: 218

You need to setup a new corporate VPN between your head-office and all your branches. You need to choose the strongest and the most secure algorithms for the VPN between the head-office and legal branch office. And for the VPN between the head-office and marketing branch, you must use shorter keylength encryption algorithm e.g. DES. How would you about the setup?

A. Create a star type VPN community and choose head-office as central gateway and the two branches as satellite gateways
B. You will setup three different communities.One community between the legal and headoffice. One community between marketing and head-office. One community between legal and marketing. You have the option of using either traditional VPN mode or simplified VPN mode configuration
C. You will setup one community to encompass legal, marketing and head-office. You have the option of using either traditional VPN mode or simplified VPN mode configuration
D. This cannot be achieved as the same encryption algorithm has to be used in the two communities
E. You will setup two different communities and the head-office as the center for both communities. You have the option of using either traditional VPN mode or simplified VPN mode configuration

Answer: E

QUESTION NO: 219

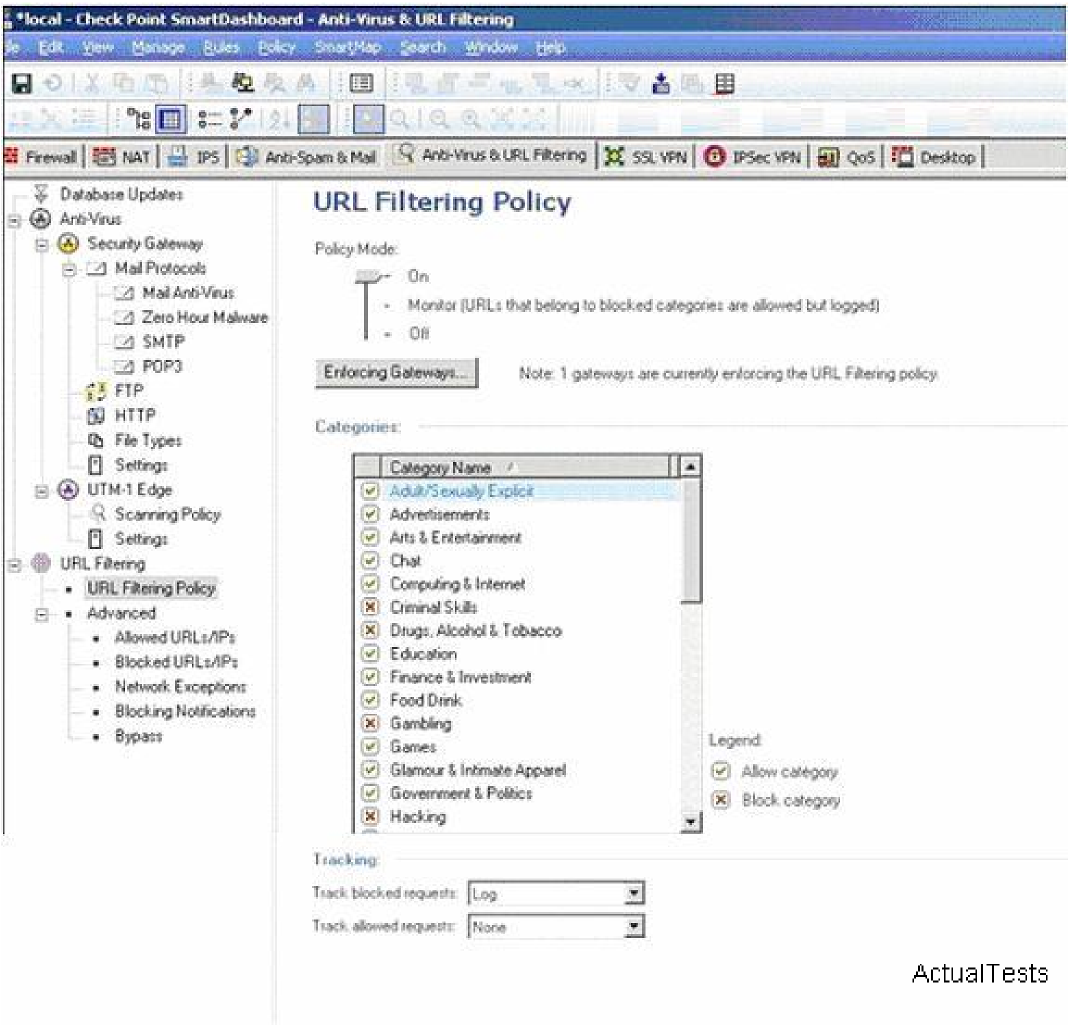
NAT Generated Rule question: The rule that specifies that for connections that originate in the external network, the destination address of the packet is translated and this is known as:

A. Hide Rule
B. Destination Hide Rule
C. Source Hide Rule
D. Static Rule
E. Destination Static Rule

Answer: E

QUESTION NO: 220

The URL is allowed or blocked based on categories in the predefined database and/or the Web Filter Allow/Block Lists. if the URL address you are accessing matches two or more categories, and one of them is blocked then what is likely to happen?



URL Filtering Policy

Policy Mode:

- On
- Monitor (URLs that belong to blocked categories are allowed but logged)
- Off

Note: 1 gateways are currently enforcing the URL Filtering policy.

Categories:

Category Name
☑ Adult/Sexually Explicit
☑ Advertisements
☑ Arts & Entertainment
☑ Chat
☑ Computing & Internet
☒ Criminal Skills
☒ Drugs, Alcohol & Tobacco
☑ Education
☑ Finance & Investment
☑ Food Drink
☒ Gambling
☑ Games
☑ Glamour & Intimate Apparel
☑ Government & Politics
☒ Hacking

Legend:

☑ Allow category

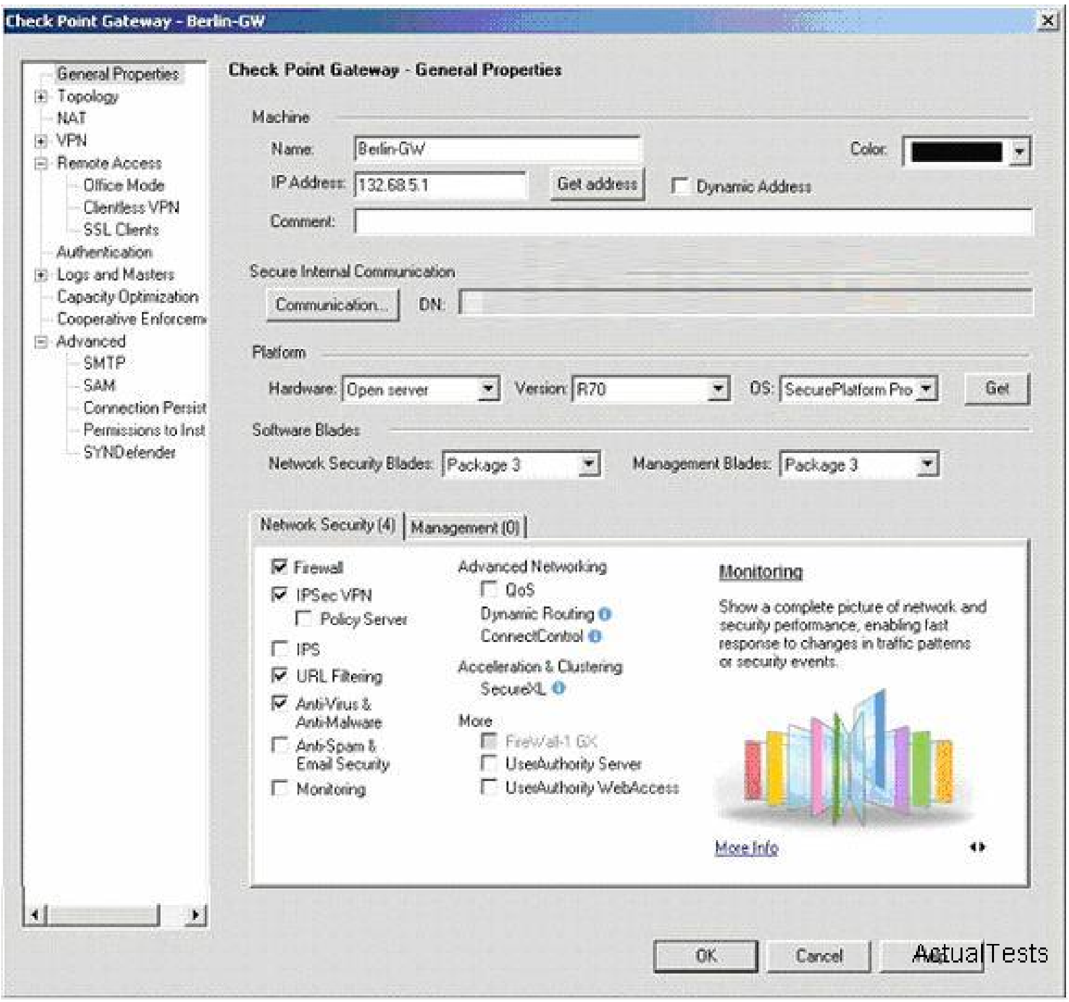
☒ Block category

Tracking:

Track blocked requests: Log

Track allowed requests: None

Figure 1: SmartDashboard - Anti-Virus & URL Filtering tab



Check Point Gateway - General Properties

Machine

Name: Berlin-GW

IP Address: 132.68.5.1

□ Dynamic Address

Color:

Comment:

Secure Internal Communication

DN:

Platform

Hardware: Open server Version: R70 OS: SecurePlatform Pro

Software Blades

Network Security Blades: Package 3 Management Blades: Package 3

Network Security (4) | Management (0)

☑ Firewall
☑ IPSec VPN
□ Policy Server
□ IPS
☑ URL Filtering
☑ Anti-Virus & Anti-Malware
□ Anti-Spam & Email Security
□ Monitoring

Advanced Networking
□ QoS
Dynamic Routing
ConnectControl

Acceleration & Clustering
SecureXL

More
□ FireWall-1 GX
□ UserAuthority Server
□ UserAuthority WebAccess

Monitoring

Show a complete picture of network and security performance, enabling fast response to changes in traffic patterns or security events.

More Info

Figure 2: CheckPoint Gateway - General Properties page

A. The URL address you are accessing will be allowed

B. The URL address you are accessing will be directed to the Security Gateway

C. The URL address you are accessing will be denied

D. The URL address you are accessing will be directed to the Security Management Server

E. The URL address you are accessing will be directed to the Security Management Server and Security Gateway

Answer: C

QUESTION NO: 221

Sharon wishes to communicate with George. During the exchange of public key between Sharon and George, Craig is able to intercept the key. And as soon as the communications begins, Craig is able to intercept the message to George, forges it and sends it to him. What sort of attack is this and what would you deploy to defend against this?

A. Anti-spoofing attack, and the defense is Public key infrastructures

B. Man-in-the-middle attack, and the defense is Public key infrastructures

C. Denial of serviceattack, and the defense is Digital Certificate

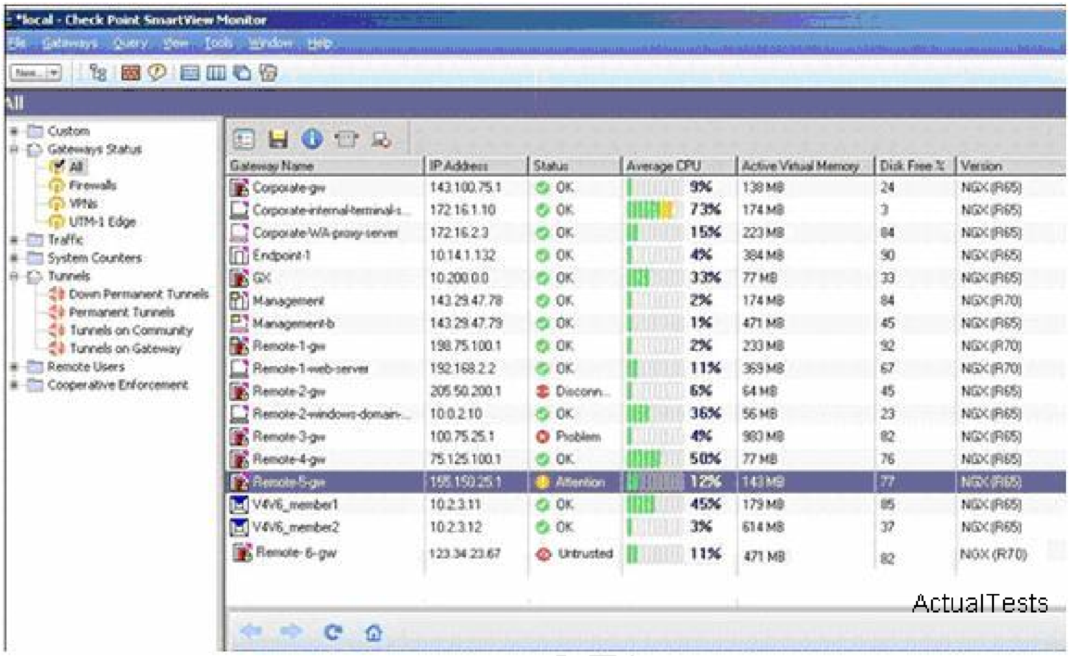
D. Malicious code, and the defense is Public key infrastructures

E. Man-in-the-middle attack, and the defense is Syndefense

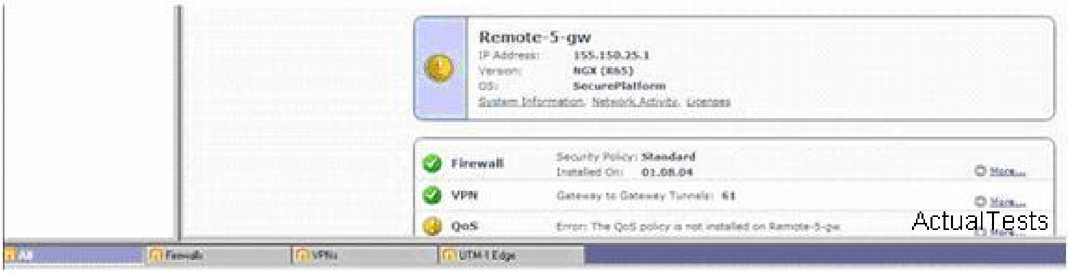
Answer: B

QUESTION NO: 222

Examine diagram 1 and answer the question. The status of Remote-6-gw gateway shows Untrusted. What is likely to be the problem? Diagram 2 shed more light on the answer.



Gateway Name	IP Address	Status	Average CPU	Active Virtual Memory	Disk Free %	Version
Corporate-gw	143.100.75.1	OK	9%	138 MB	24	NGX (R65)
Corporate-internal-terminal-s...	172.16.1.10	OK	73%	174 MB	3	NGX (R65)
Corporate-WA-proxy-server	172.16.2.3	OK	15%	223 MB	84	NGX (R65)
Endpoint-1	10.14.1.132	OK	4%	384 MB	90	NGX (R65)
GX	10.200.0.0	OK	33%	77 MB	33	NGX (R65)
Management	143.29.47.78	OK	2%	174 MB	84	NGX (R70)
Management-b	143.29.47.79	OK	1%	471 MB	45	NGX (R65)
Remote-1-gw	198.75.100.1	OK	2%	233 MB	92	NGX (R70)
Remote-1-web-server	192.168.2.2	OK	11%	369 MB	67	NGX (R70)
Remote-2-gw	205.50.200.1	Disconn...	6%	64 MB	45	NGX (R65)
Remote-2-windows-domain-...	10.0.2.10	OK	36%	56 MB	23	NGX (R65)
Remote-3-gw	100.75.25.1	Problem	4%	983 MB	82	NGX (R65)
Remote-4-gw	75.125.100.1	OK	50%	77 MB	76	NGX (R65)
Remote-5-gw	155.150.25.1	Attention	12%	143 MB	77	NGX (R65)
V4V6_member1	10.2.3.11	OK	45%	179 MB	85	NGX (R65)
V4V6_member2	10.2.3.12	OK	3%	614 MB	37	NGX (R65)
Remote- 6-gw	123.34.23.67	Untrusted	11%	471 MB	82	NGX (R70)



Remote-5-gw

IP Address: 155.150.25.1

Version: NGX (R65)

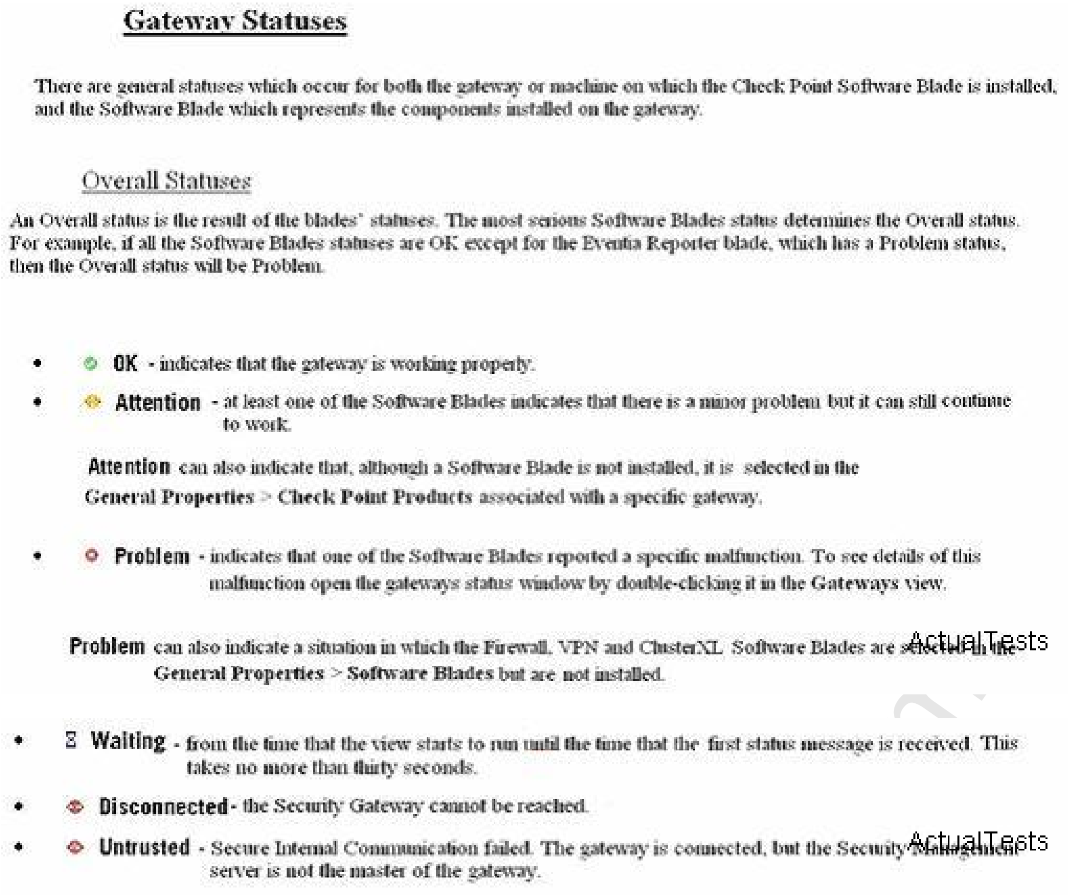
OS: SecurePlatform

System Information, Network Activity, Licenses

Firewall Security Policy: Standard Installed On: 01.08.04 More...

VPN Gateway to Gateway Tunnels: 61 More...

QoS Error: The QoS policy is not installed on Remote-5-gw More...



Gateway Statuses

There are general statuses which occur for both the gateway or machine on which the Check Point Software Blade is installed, and the Software Blade which represents the components installed on the gateway.

Overall Statuses

An Overall status is the result of the blades' statuses. The most serious Software Blades status determines the Overall status. For example, if all the Software Blades statuses are OK except for the Eventia Reporter blade, which has a Problem status, then the Overall status will be Problem.

- **OK** - indicates that the gateway is working properly.
- **Attention** - at least one of the Software Blades indicates that there is a minor problem but it can still continue to work.

Attention can also indicate that, although a Software Blade is not installed, it is selected in the **General Properties > Check Point Products** associated with a specific gateway.

- **Problem** - indicates that one of the Software Blades reported a specific malfunction. To see details of this malfunction open the gateways status window by double-clicking it in the **Gateways** view.

Problem can also indicate a situation in which the Firewall, VPN and ClusterXL Software Blades are selected in the **General Properties > Software Blades** but are not installed.

- **Waiting** - from the time that the view starts to run until the time that the first status message is received. This takes no more than thirty seconds.
- **Disconnected** - the Security Gateway cannot be reached.
- **Untrusted** - Secure Internal Communication failed. The gateway is connected, but the Security Management server is not the master of the gateway.

A. The Security Gateway cannot be reached

B. The Software Blade is not installed

C. Secure Internal Communication failed

D. The gateway is working properly

E. Waiting problem

Answer: C

QUESTION NO: 223

If the SIC status on the gateway shows "Unknown" then:

A. The gateway has received the certificate fromICA

B. The gateway has not received the certificate fromICA

C. There is no connection between the Gateway and the Security Management server

D. There is connection between the Gateway and the Security Management server

E. Connection is established between

Answer: C

QUESTION NO: 224

What is likely to be the advantage of Continuous Download of scanned file?

A. If a virus is present in the opened part of the file that is being delivered,then it could infect the client computer
B. The issue of short delay
C. Continuous Download starts sending information to the client while Anti-Virus scanning is still taking place
D. The user may experience a long delay before the file is delivered
E. The issue of time-out

Answer: C

QUESTION NO: 225

When performing an upgrade that involves a new installation and manually importing a previously exported configuration to new machine, what tools will you to achieve this?

A. upgrade_import tool
B. Pre-Upgrade Verification tool
C. upgrade_export tool only
D. Pre-Upgrade Verification tool and upgrade_import tool
E. upgrade_export tool and upgrade_import tool

Answer: E

QUESTION NO: 226

Which command displays the status of the bridge configuration?

A. brctl show
B. bridge conf
C. bridge conf show
D. bridge show
E. conf bridge

Answer: A

QUESTION NO: 227

In IPS, the protection parameters are: (select all the correct answers).

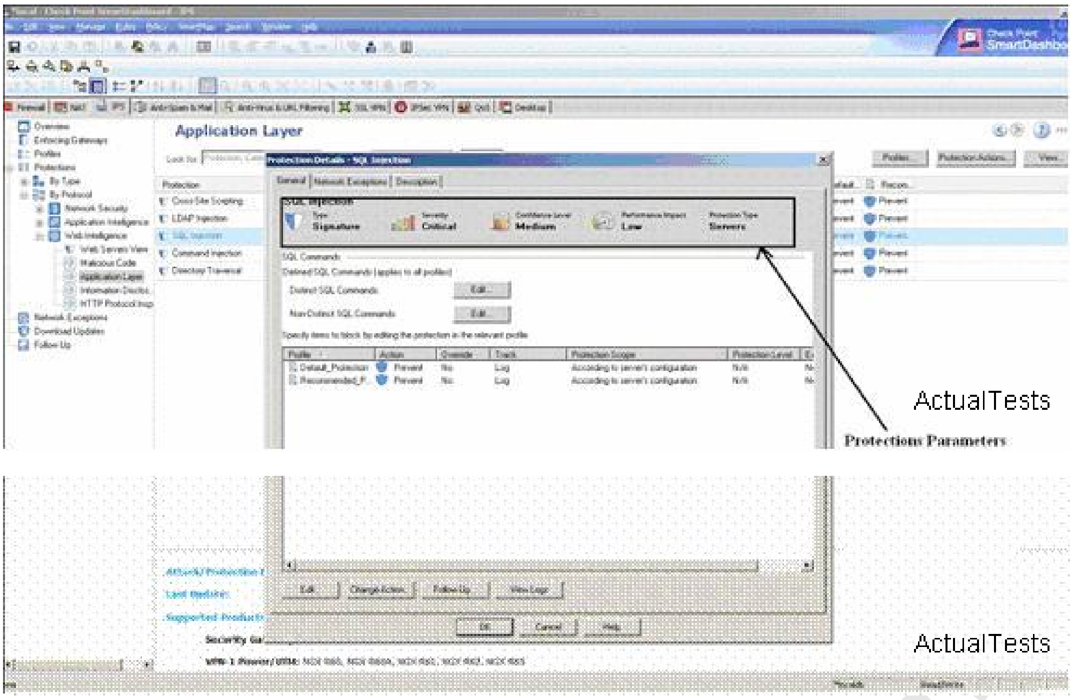
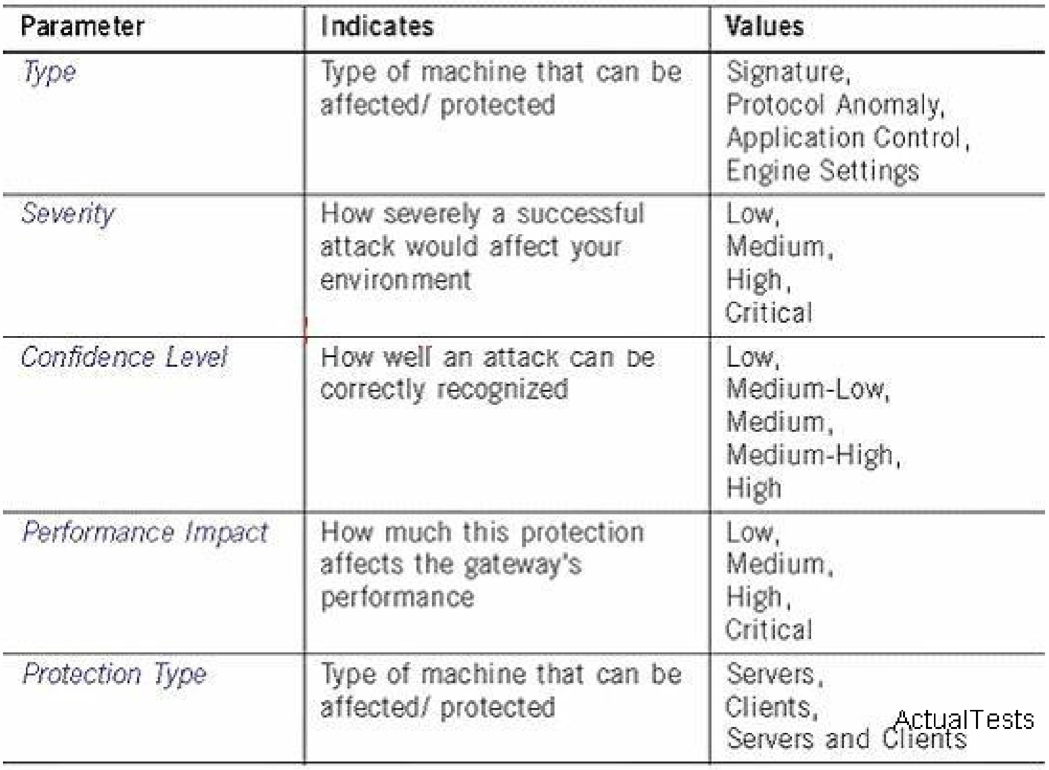
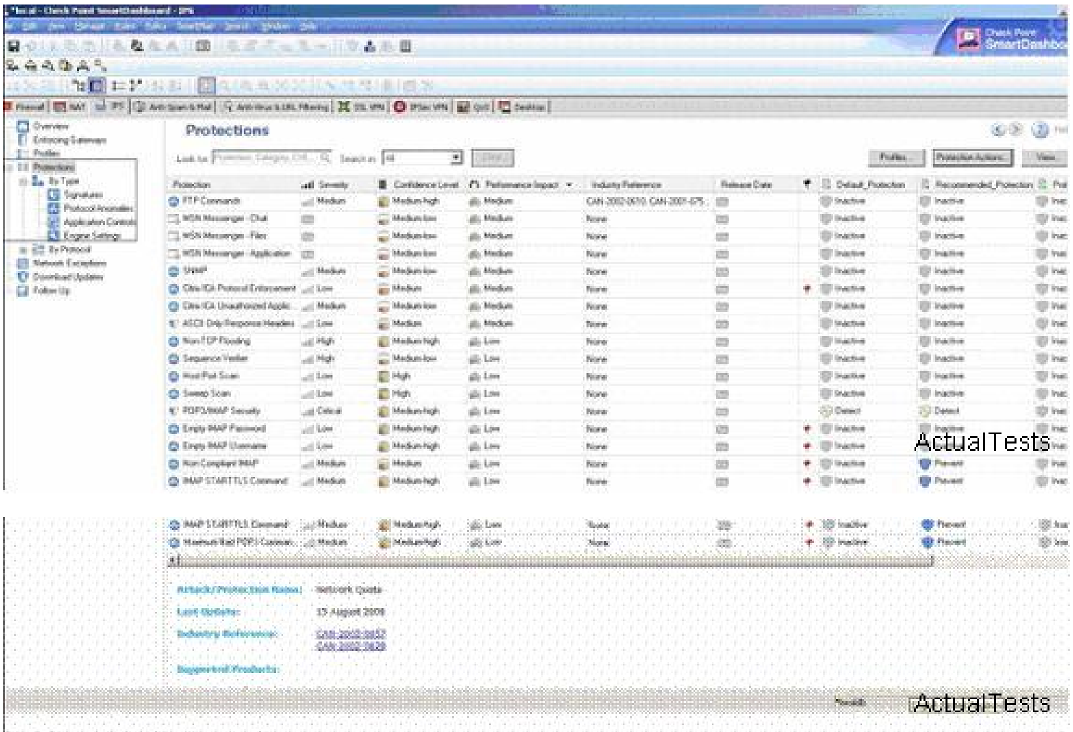


Figure 1: Protection Parameters

Table 1: Explanation of Protection Parameters



Parameter	Indicates	Values
Type	Type of machine that can be affected/ protected	Signature, Protocol Anomaly, Application Control, Engine Settings
Severity	How severely a successful attack would affect your environment	Low, Medium, High, Critical
Confidence Level	How well an attack can be correctly recognized	Low, Medium-Low, Medium, Medium-High, High
Performance Impact	How much this protection affects the gateway's performance	Low, Medium, High, Critical
Protection Type	Type of machine that can be affected/ protected	Servers, Clients, Servers and Clients



Look for: Protection, Category, CVE... Search in: All

Protection	Severity	Confidence Level	Performance Impact	Industry Reference	Release Date	⚑	Default_Protection	Recommended_Protection	Pol
FTP Commands	Medium	Medium-high	Medium	CAN-2002-0610, CAN-2001-075...			Inactive	Inactive	Inac
MSN Messenger - Chat		Medium-low	Medium	None			Inactive	Inactive	Inac
MSN Messenger - Files		Medium-low	Medium	None			Inactive	Inactive	Inac
MSN Messenger - Application		Medium-low	Medium	None			Inactive	Inactive	Inac
SNMP	Medium	Medium-low	Medium	None			Inactive	Inactive	Inac
Citrix ICA Protocol Enforcement	Low	Medium	Medium	None		⚑	Inactive	Inactive	Inac
Citrix ICA Unauthorized Applic...	Medium	Medium-low	Medium	None			Inactive	Inactive	Inac
ASCII Only Response Headers	Low	Medium	Medium	None			Inactive	Inactive	Inac
Non-TCP Flooding	High	Medium-high	Low	None			Inactive	Inactive	Inac
Sequence Verifier	High	Medium-low	Low	None			Inactive	Inactive	Inac
Host Port Scan	Low	High	Low	None			Inactive	Inactive	Inac
Sweep Scan	Low	High	Low	None			Inactive	Inactive	Inac
POP3/IMAP Security	Critical	Medium-high	Low	None			Detect	Detect	Inac
Empty IMAP Password	Low	Medium-high	Low	None		⚑	Inactive	Inactive	Inac
Empty IMAP Username	Low	Medium-high	Low	None		⚑	Inactive	[illegible]	Inac
Non Compliant IMAP	Medium	Medium	Low	None		⚑	Inactive	Prevent	Inac
IMAP STARTTLS Command	Medium	Medium-high	Low	None		⚑	Inactive	Prevent	Inac
IMAP STARTTLS Command	Medium	Medium-high	Low	None		⚑	Inactive	Prevent	Inac
Maximum Bad POP3 Comman...	Medium	Medium-high	Low	None		⚑	Inactive	Prevent	Inac

Attack/Protection Name: Network Quota

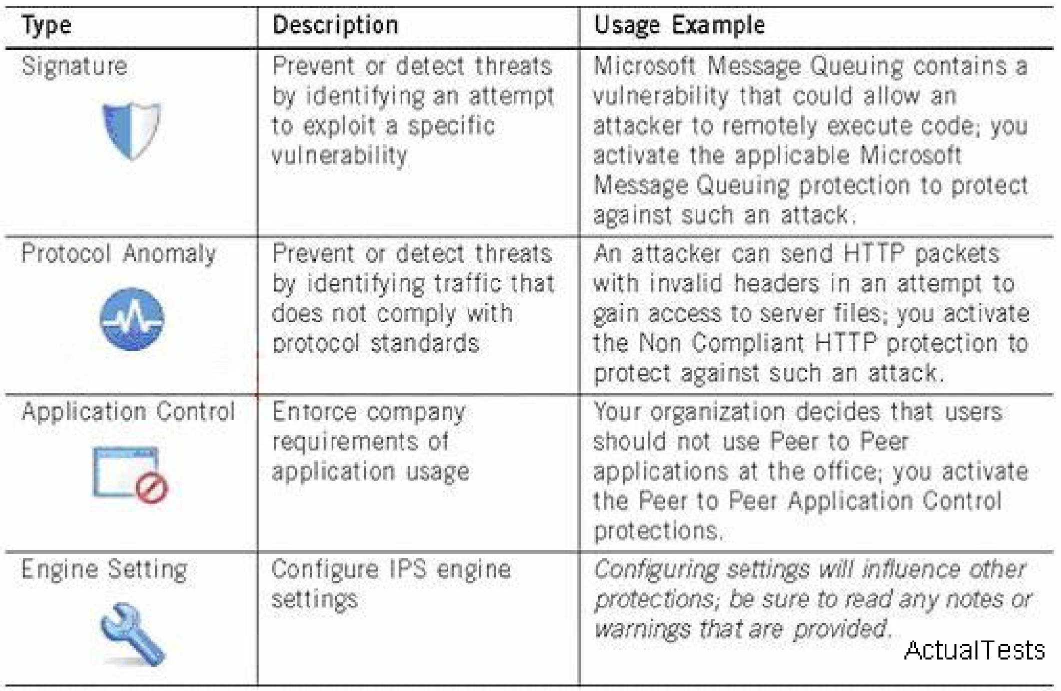
Last Update: 15 August 2008

Industry Reference: CAN-2002-0657
CAN-2002-0628

Supported Products:

Figure 2: IPS Tab - Protection Page

Table 2: Types



Type	Description	Usage Example
Signature	Prevent or detect threats by identifying an attempt to exploit a specific vulnerability	Microsoft Message Queuing contains a vulnerability that could allow an attacker to remotely execute code; you activate the applicable Microsoft Message Queuing protection to protect against such an attack.
Protocol Anomaly	Prevent or detect threats by identifying traffic that does not comply with protocol standards	An attacker can send HTTP packets with invalid headers in an attempt to gain access to server files; you activate the Non Compliant HTTP protection to protect against such an attack.
Application Control	Enforce company requirements of application usage	Your organization decides that users should not use Peer to Peer applications at the office; you activate the Peer to Peer Application Control protections.
Engine Setting	Configure IPS engine settings	*Configuring settings will influence other protections; be sure to read any notes or warnings that are provided.*

A. Confidence Level
B. Severity
C. Rigorous
D. Type
E. Performance Impact

Answer: A,B,D,E

QUESTION NO: 228

Which of the following is not a reason for integrating SmartDirectory (LDAP) Entities with Security Management server and Security Gateways?

A. To enable User management
B. To enable CRL retrieval
C. To encrypt the users directory database
D. To authenticate users
E. To query user information

Answer: C

QUESTION NO: 229

Which utility is used to automatically backup your configuration when performing upgrade?

A. upgrade_import command
B. backup export command
C. upgrade_export command
D. restore command
E. backup command

Answer: C

QUESTION NO: 230

Which of the following is true difference between SmartView Monitor and SmartView Tracker? Select all the correct answers.

A. SmartView Monitor provides real-time monitoring while SmartView Tracker provides realtime visual tracking
B. SmartView Tracker is useful for reducing the time required to troubleshoot configuration errors
C. There is no difference between the two
D. SmartView Tracker provides real-time monitoring while SmartView Monitor provides realtime visual tracking
E. SmartView Monitor helps to maximize performance of customers' networks and manage costs

Answer: A,B,E

QUESTION NO: 231

The diagram shows your network. Host X behind gateway A want to initiate a connection with a host Y machine behind gateway B. Gateway A cannot establish a VPN tunnel with gateway B directly due to political reason. Gateways A and B can only establish VPN tunnels with gateway C. This configuration is known as what?

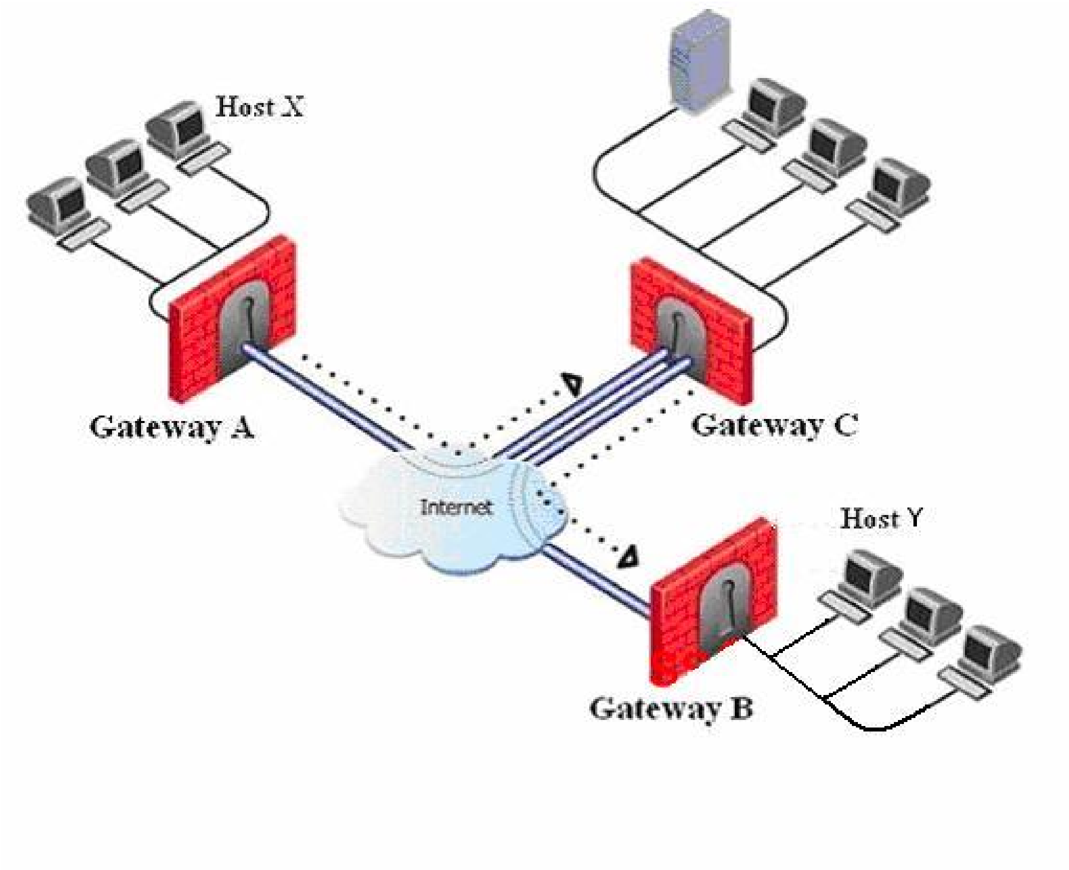


Figure 1: VPN Routing

A. Domain Based VPN
B. Route Based VPN
C. vpn_route.conf
D. VPN Routing
E. IP VPN Routing

Answer: A

QUESTION NO: 232

The Internal Certificate Authority (ICA) is a fully featured, internal authentication server that is installed on a Security Management Server. The ICA cannot be used in which of the following situations?

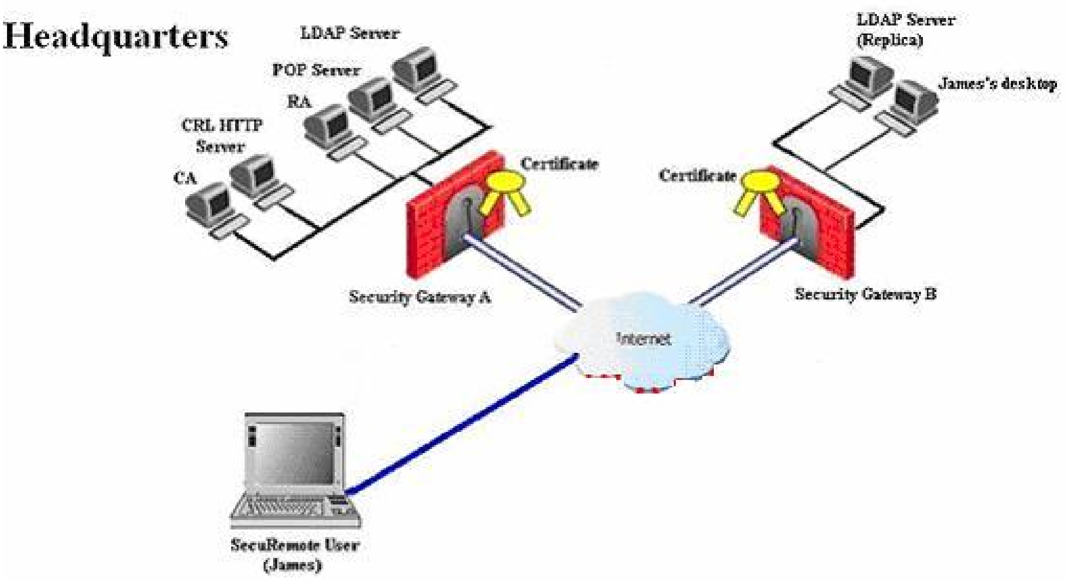


Figure 1: Local Certificate Authority

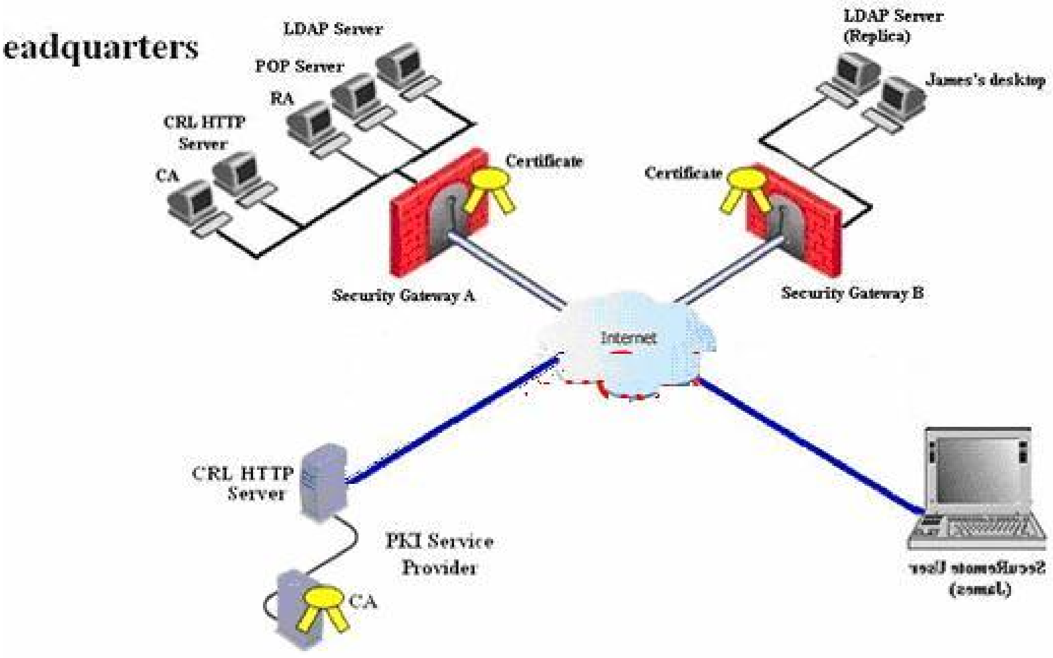


Figure 2: CA service via the Internet

A. Establishing site-to-site VPNs between Gateways

B. Using a certificate over the Internet

C. Authenticating SecuRemote and SecureClient traffic to Gateways for VPN capabilities

D. Using Hybrid Mode RAS VPN for authenticating Gateways to SecuRemote and SecureClient users

E. Providing certificates for users and security administrators

Answer: B

QUESTION NO: 233

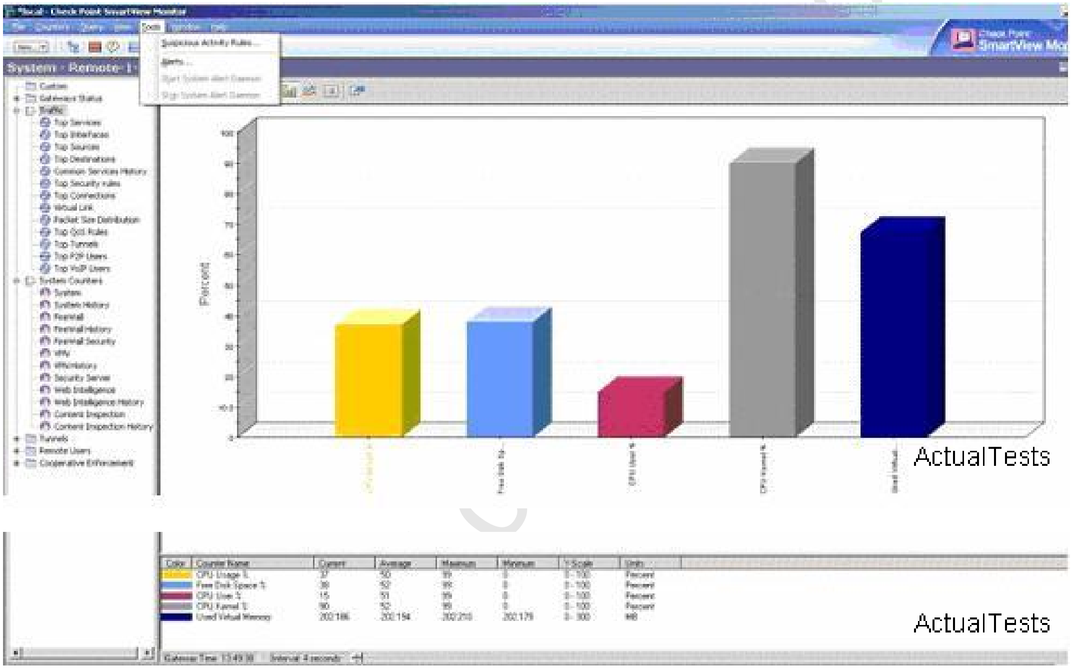
A system administrator wants to find out list of users currently connected and number of bytes being transferred by each user. Which SmartView Tracker GUI mode do you think the administrator should use?

A. Active Mode
B. Active Connections
C. Management Mode
D. Active Log
E. Network & Endpoint Mode

Answer: A

QUESTION NO: 234

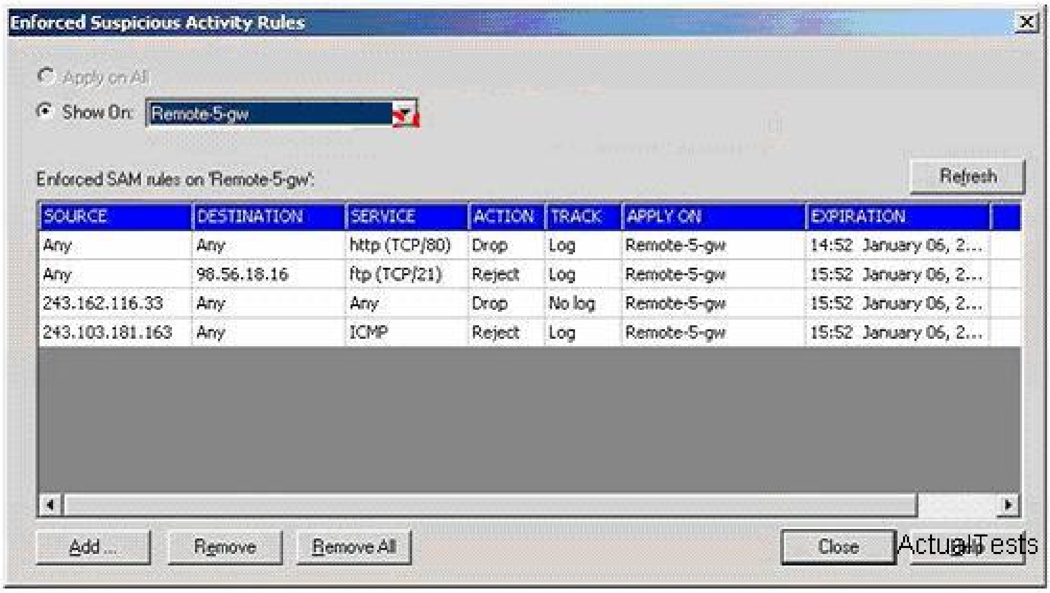
To create a Suspicious Activity Rule in the SmartView Monitor, what menu will you select?



Color	Counter Name	Current	Average	Maximum	Minimum	Y Scale	Units
🟨	CPU Usage %	37	50	99	0	0 - 100	Percent
🟦	Free Disk Space %	38	52	99	0	0 - 100	Percent
🟥	CPU User %	15	51	99	0	0 - 100	Percent
⬜	CPU Kernel %	90	52	99	0	0 - 100	Percent
🟦	Used Virtual Memory	202 186	202 194	202 210	202 179	0 - 300	MB

Gateway Time: 13:49:38 Interval: 4 seconds

Figure 1 : SmartView Monitor - Tools Menu



Enforced Suspicious Activity Rules

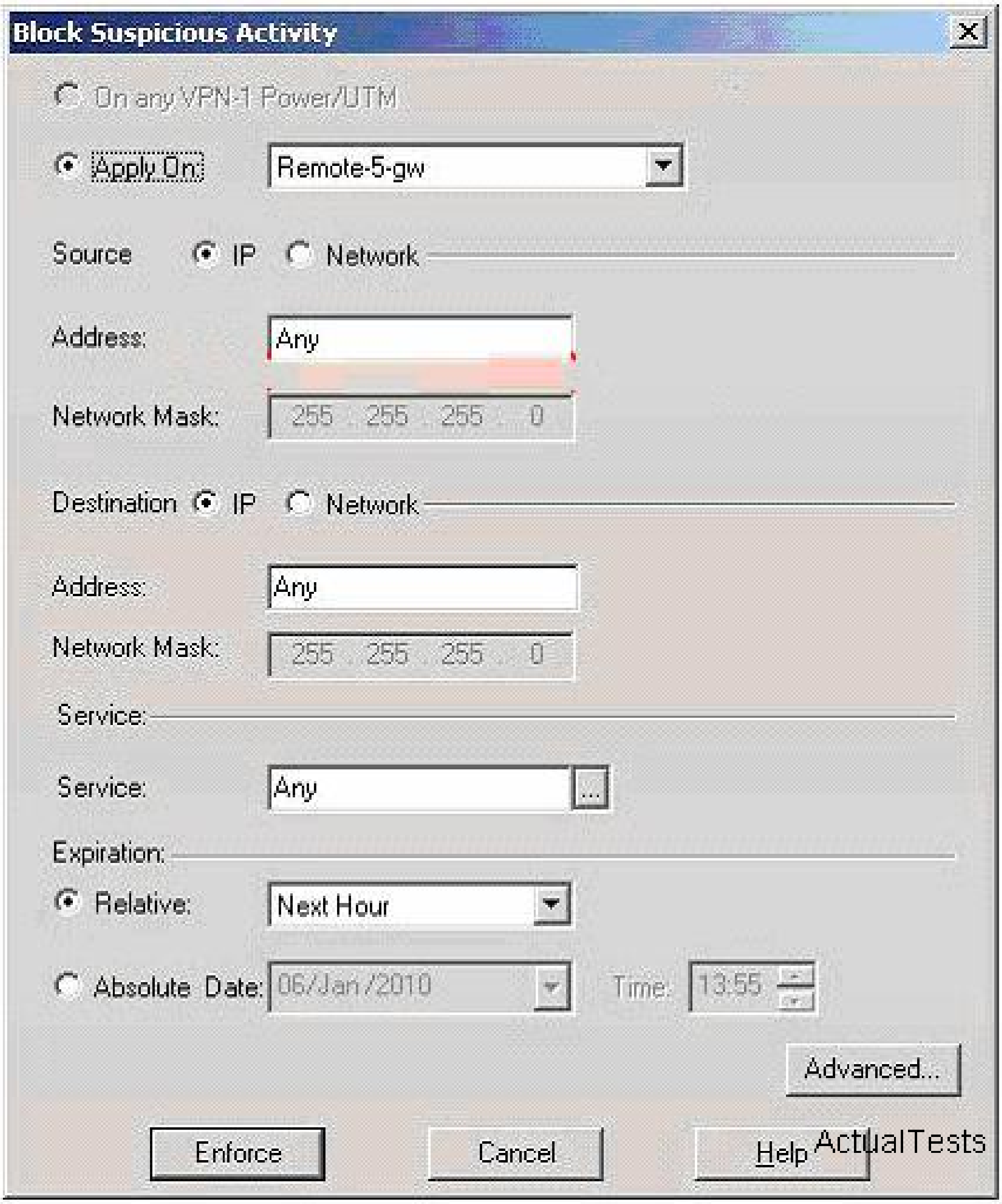
○ Apply on All

● Show On: Remote-5-gw

Enforced SAM rules on 'Remote-5-gw':

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	APPLY ON	EXPIRATION
Any	Any	http (TCP/80)	Drop	Log	Remote-5-gw	14:52 January 06, 2...
Any	98.56.18.16	ftp (TCP/21)	Reject	Log	Remote-5-gw	15:52 January 06, 2...
243.162.116.33	Any	Any	Drop	No log	Remote-5-gw	15:52 January 06, 2...
243.103.181.163	Any	ICMP	Reject	Log	Remote-5-gw	15:52 January 06, 2...

Figure 2: Enforced Suspicious Activity Rules



Block Suspicious Activity

○ On any VPN-1 Power/UTM

● Apply On: Remote-5-gw

Source ● IP ○ Network

Address: Any

Network Mask: 255 . 255 . 255 . 0

Destination ● IP ○ Network

Address: Any

Network Mask: 255 . 255 . 255 . 0

Service:

Service: Any

Expiration:

● Relative: Next Hour

○ Absolute Date: 06/Jan /2010 Time: 13:55

Figure 3: Block Suspicious Activity box

A. View
B. Tools
C. Traffic
D. Query
E. File

Answer: B

QUESTION NO: 235

When modifying a user template, the users already created based on this template will be:

A. Affected
B. Unaffected
C. Re-created
D. Created
E. Deleted

Answer: B

QUESTION NO: 236

What SmartView Tracker mode would you switch to when terminating an active connection using the Block Intruder window?

A. Intruder
B. Active
C. Any mode
D. Network & Endpoint
E. Management

Answer: B

QUESTION NO: 237

What is the purpose of Stealth rule?

A. To disable a firewall
B. To allow any connection to the firewall

C. To prevent any user from scanning or attacking the firewall
D. To specify users that should be prevented from connecting to the firewall
E. To specify users that should be allowed to connect to the firewall

Answer: C

QUESTION NO: 238

Match each of the following commands to their correct function.

(A) cp_admin_convert
(B) cpwd_admin
(C) cpca_client
(D) cp_merge
(E) cpwd_admin start

1- This command and all its derivatives are used to execute operations on the ICA.
2- Automatically export administrator definitions that were created in cpconfig to SmartDashboard.
3- Export and import of policy packages
4- This utility is used to show the status of processes, and to configure cpwd on local machine
5- Start a new process by cpwd (cpwd also known as WatchDog)

A. A -> 2, B.-> 4,C -> 1,D.-> 5,E.-> 3
B. A -> 2, B.-> 3,C -> 4,D.-> 1,E.-> 5
C. A -> 5, B.-> 4,C -> 1,D.-> 3,E.-> 2
D. A -> 2, B.-> 4,C -> 1,D.-> 3,E.-> 5
E. A -> 4, B.-> 2,C -> 1,D.-> 3,E.-> 5

Answer: D

QUESTION NO: 239

Which of the following steps must you take in order to maximize the performance of your Eventia Reporter Server? Select all the correct answers.

A. Use the fastest disk available with the highest RPM (Revolutions per Minute) and a large buffer size
B. Configure the SIC between the Eventia Reporter Server machine and the SmartCenter, or the Log server, to the optimal speed
C. Configure the network connection between the Eventia Reporter Server machine and the SmartCenter, or the Log server, to the optimal speed

D. Adjust the database configuration file and consolidation memory buffers to use the additional memory
E. Use a computer that matches the minimum hardware requirements, as specified in the Release Notes

Answer: A,C,D,E

QUESTION NO: 240

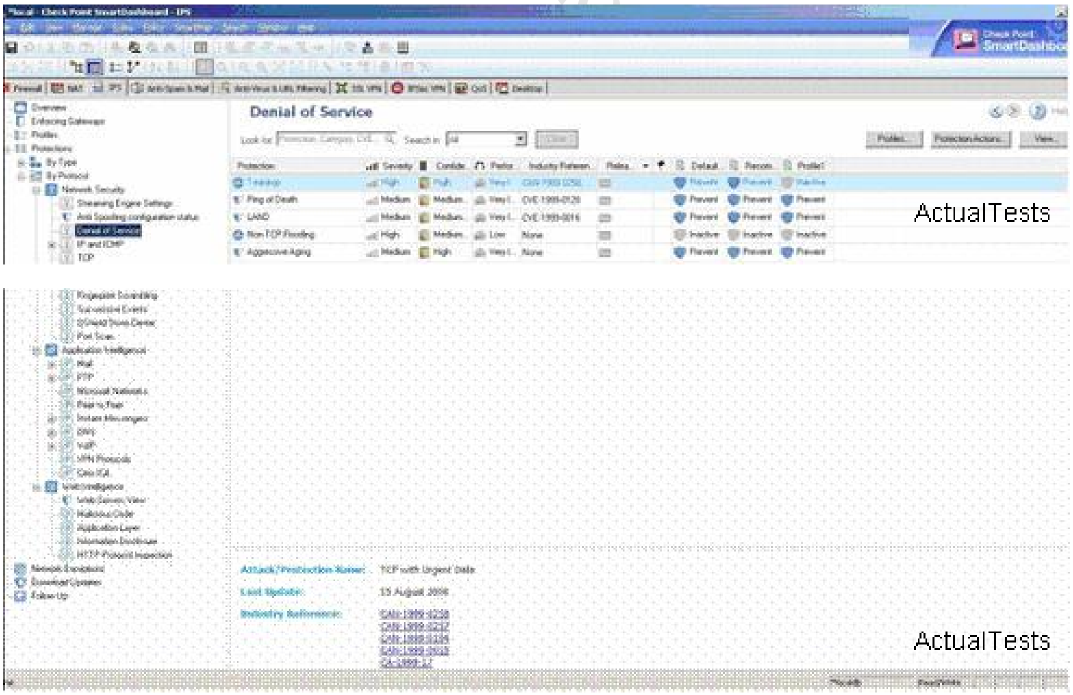
When two entities try to establish a VPN tunnel, each side supplies its peer with random information signed by its private key and with the certificate that contains the:

A. Diffie-Hellman
B. Algorithm
C. Public key
D. Privatekey
E. Authentication

Answer: C

QUESTION NO: 241

The diagram shows IPS Protection, Network Security section. Where will you go to configure protection against improper use of the TCP or UDP protocols?



Denial of Service

Protection	Severity	Confide...	Perfor...	Industry Referen...	Relea...		Default...	Recom...	Profile1
Teardrop	High	High	Very l...	CAN-1999-0258			Prevent	Prevent	Inactive
Ping of Death	Medium	Medium...	Very l...	CVE-1999-0128			Prevent	Prevent	Prevent
LAND	Medium	Medium...	Very l...	CVE-1999-0016			Prevent	Prevent	Prevent
Non TCP Flooding	High	Medium...	Low	None			Inactive	Inactive	Inactive
Aggressive Aging	Medium	High	Very l...	None			Prevent	Prevent	Prevent

Attack/Protection Name: TCP with Urgent Data
Last Update: 15 August 2008
Industry Reference: CAN-1999-0258
CAN-1999-0212
CAN-1999-0116
CAN-1999-0653
CA-1998-12

Figure 1: IPS Tab

A. Denial of Service
B. Finger Scrambling
C. Streaming Engine Settings
D. Anti-Spoofing Configuration Status
E. IP and ICMP

Answer: C

QUESTION NO: 242

You can choose to hide your internal IP addresses in which of the following ways?

A. Hide behind a virtual IP address
B. Hide behind an imaginary IP address
C. Hide behind 255.255.255.255
D. Hide behind 0.0.0.0
E. Hide behind the IP address of the gateway's internal interface

Answer: A,D

QUESTION NO: 243

The Eventia Reporter Database system consists of a set of files that to be backed up. Which of the following file will specify entire data directory tree?

A. UpdateMySQLConfig
B. conf
C. objects.C
D. objects_5_0.C
E. my.ini

Answer: E

QUESTION NO: 244

When using CLI, what keystroke combinations move you to the beginning of the line?

A. Alt-D
B. Alt-B
C. Ctrl-A
D. Ctrl-B

E. Ctrl-C

Answer: C

QUESTION NO: 245

Before Gateways can exchange encryption keys and build VPN tunnels, they first need to authenticate to each other using one of the following credentials:

A. Certificates, SIC
B. Pre-shared secret,Internal CA
C. Pre-shared secret, SIC
D. Certificates, Pre-shared secret
E. Certificates, SVN

Answer: D

QUESTION NO: 246

Successful and unsuccessful authentication attempts can be monitored in SmartView Tracker. Where will you go to configure failed authentication attempts?

A. In the Authentication page of a gateway object
B. In the Action column of any rule
C. In the Encryption page of a gateway object
D. In the Track column of any rule
E. In the Client Authentication Action Properties window

Answer: A

QUESTION NO: 247

Which of the following is true of spanning tree protocol(STP) Protocol?

A. STP provides path redundancy and prevents undesirable loops between switches
B. Check Point supports the per-VLAN STP
C. A Security Gateway in Bridge mode will not support the spanning tree protocol
D. SNMP has to run when running STP to control the network
E. STP monitors for device failure and controls which switches the traffic passes through

Answer: A,B,E

QUESTION NO: 248

Which of the following events will happen during IKE Phase I? Select three answers

A. IKE is encrypted according to the keys and methods agreed upon in IKE phases
B. A Diffie-Hellman key is created
C. The peers authenticate, either by certificates or via a pre-shared secret
D. Key material (random bits and other mathematical data) as well as an agreement on methods for IKE phase II are exchanged between the peers
E. The key material exchanged during IPSEC phase is used for building the IPSec keys

Answer: B,C,D

QUESTION NO: 249

Which of the following enforces security policies on the security gateway on which they reside?

A. SVN
B. VPN
C. SIC
D. INSPECT Engine
E. SmartDashboard

Answer: D

QUESTION NO: 250

The Log Consolidator process continuously adds new records into the database as they are generated from the security gateway. Eventually, the space allocated for the database will fill up. To manually archive or delete older record, you will implement:

A. Record Maintenance
B. Automatic Maintenance
C. Ordinary Maintenance
D. Manual Maintenance
E. Cyclic Maintenance

Answer: B

QUESTION NO: 251

Below is the Basic Concepts and Terminology. 1. Administrators are the designated managers of SmartConsole 2. In a standalone deployment, the Security Management server, and the gateway are installed on the same machine 3. Objects are defined and managed in SmartView Track. 4. A Policy Package - is a set of Policies that are enforced on selected gateways 5. A Log Server is the repository for log entries generated on gateway. Which of the following Basic Concepts and Terminology are true?

(A) 1,2,3,4 and 5 are correct
(B) 2,3 and 4 are correct
(C) 1,2,3 and 4 are correct
(D) 1,2,4 and 5 are correct
(E) 1,3,4 and 5 are correct

A. B
B. A
C. C
D. D
E. E

Answer: D

QUESTION NO: 252

Which of the following is true of Internal User Database and LDAP? Select four answers.

A. Changes that are applied to a SmartDirectory (LDAP) template are reflected immediately for all users who are using that template
B. User management in the SmartDirectory (LDAP) server is done externally and not locally
C. User management in the SmartDirectory (LDAP) server is done internally or locally
D. For Internal User Database, the Security Gateway can store a static password in its local user database for each user configured in Security Management server
E. Internal User Database is done internally or locally

Answer: A,B,D,E

QUESTION NO: 253

What is a collection of VPN enabled gateways capable of communicating via VPN tunnels

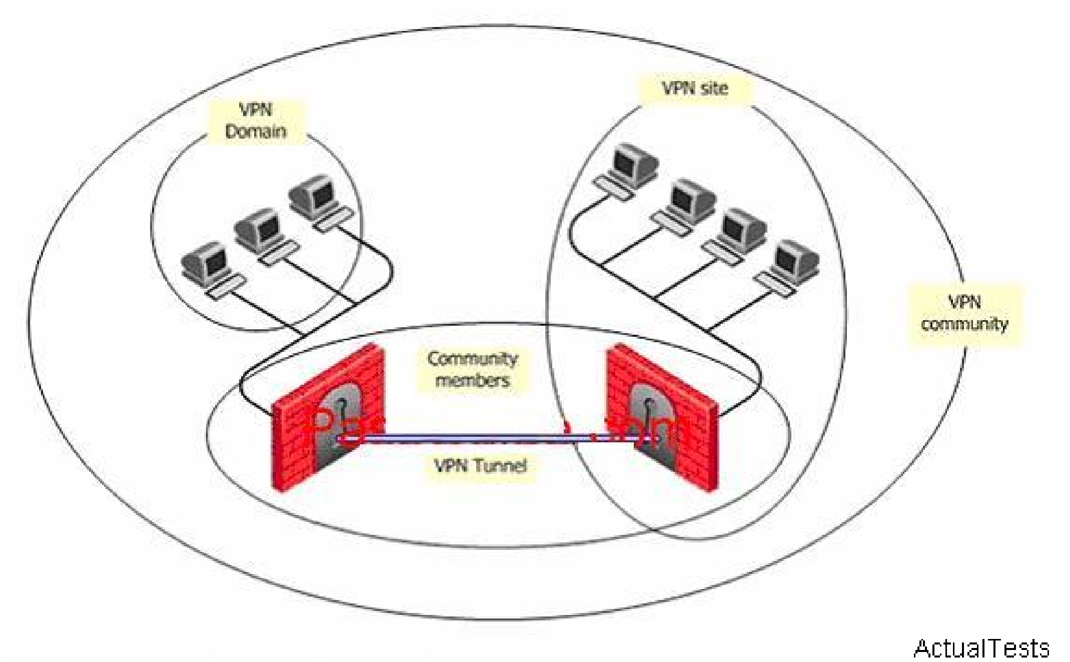


Figure 1: VPN Terminology

A. VPN domain
B. Domain Based VPN
C. VPN Community member
D. Route Based VPN
E. VPN Community

Answer: E

QUESTION NO: 254

Sharon wishes to communicate with George. During the exchange of public key between Sharon and George, Craig is able to intercept the key. And as soon as the communications begins, Craig is able to intercept the message to George, forges it and sends it to him. What sort of attack is this and what would you deploy to defend against this?

A. Man-in-the-middle attack, and the defense is Syndefense
B. Anti-spoofing attack, and the defense is Public key infrastructures
C. Malicious code, and the defense is Public key infrastructures
D. Denial of serviceattack, and the defense is Digital Certificate
E. Man-in-the-middle attack, and the defense is Public key infrastructures

Answer: E

QUESTION NO: 255

Which of the following is true of IPSO?

A. IPSO is based on FreeBSD

B. IPSO is ideal for internetworking with customers' IP networks

C. IPSO is customized to support CheckPoint enhanced routing capabilities and security gateways

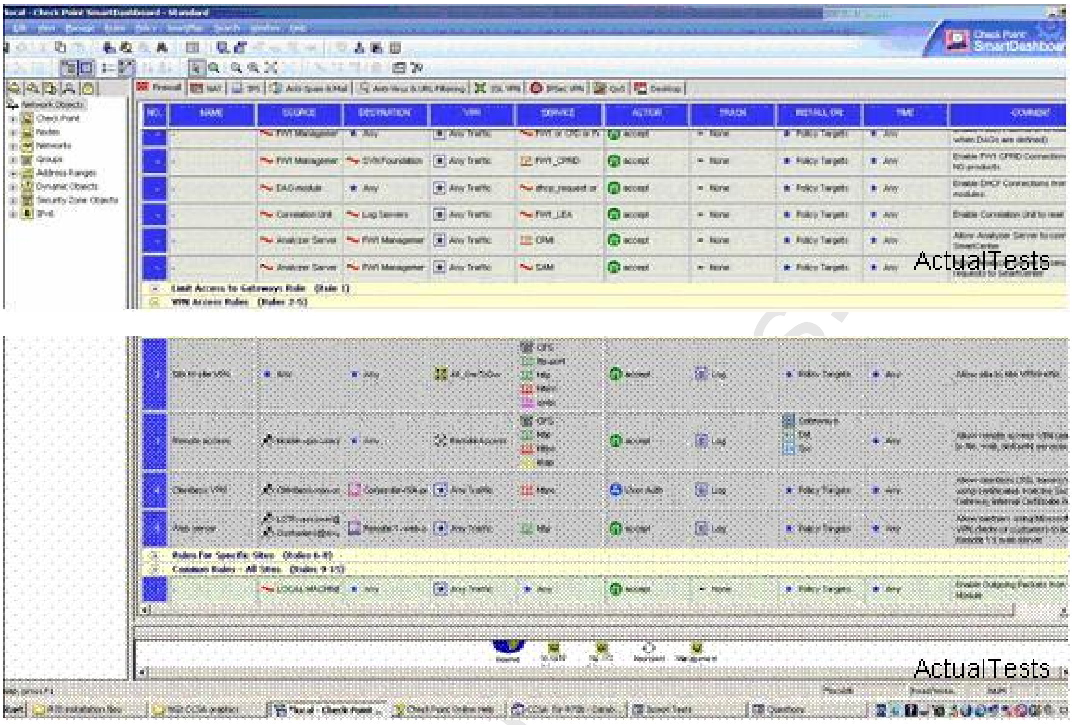
D. IP is not compliant to IPv6 standards

E. IPSO is a unique operating system kernel that is optimized with hardened security

Answer: A,B,C,E

QUESTION NO: 256

Study the diagram. What are the rules with numbers in the diagram called?


Check Point SmartDashboard
NO.
NAME
SOURCE
DESTINATION
VPN
SERVICE
ACTION
TRACK
INSTALL ON
TIME
COMMENT
Limit Access to Gateways Rule (Rule 1)
VPN Access Rules (Rules 2-5)
Rules For Specific Sites (Rules 6-8)
Common Rules - All Sites (Rules 9-15)
ActualTests
ActualTests

A. Explicit rule

B. Stealth rule

C. Cleanup rule

D. Semi rule

E. Implicit rule

Answer: A

QUESTION NO: 257

What is a Firewall? (Choose the best answer)

A. A system designed to allow influx of externalusers access to or from an internal network

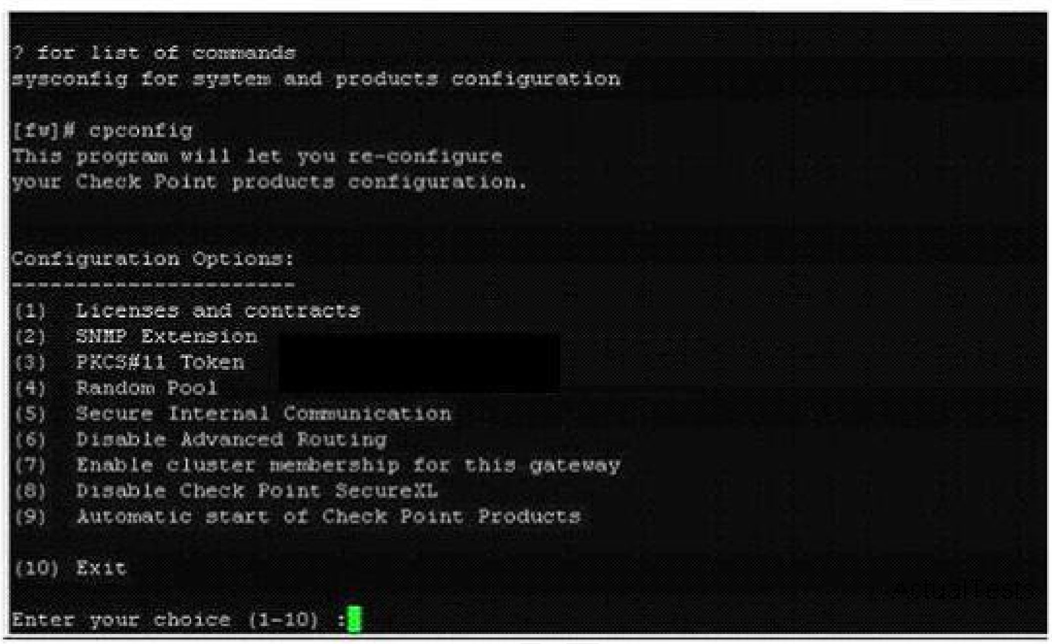
B. A system designed to connect to the internets and control communications between separate servers

C. A system designed to allow unauthorized access to or from an internal network
D. A system designed to connect to the intranets and control communications between separate servers
E. A system designed to prevent unauthorized access to or from an internal network

Answer: E

QUESTION NO: 258

The diagram shows the part of the sysconfig. What information can you deduce from the diagram? Select all the correct answers.



```
? for list of commands
sysconfig for system and products configuration

[fw]# cpconfig
This program will let you re-configure
your Check Point products configuration.


Configuration Options:
----------------------
(1)  Licenses and contracts
(2)  SNMP Extension
(3)  PKCS#11 Token    [redacted]
(4)  Random Pool
(5)  Secure Internal Communication
(6)  Disable Advanced Routing
(7)  Enable cluster membership for this gateway
(8)  Disable Check Point SecureXL
(9)  Automatic start of Check Point Products

(10) Exit

Enter your choice (1-10) :
```

A. cpinfo is the configuration tool
B. The operating system is Windows
C. The operating system is SecurePlatform or SecurePlatform Pro
D. The deployment is a distributed installation
E. The deployment is a stand-alone installation

Answer: C,D

QUESTION NO: 259

In SmartView Monitor, you can use Traffic Monitoring to: Select all the correct answers.

A. Detect and monitor suspicious activity
B. Analyze network traffic patterns
C. Suggest where Clustering can be useful

D. Identify who generates the most traffic and the times of peak activity
E. Audit and estimate costs of network use

Answer: A,B,D,E

QUESTION NO: 260

Which of the following is true of Cluster Management?

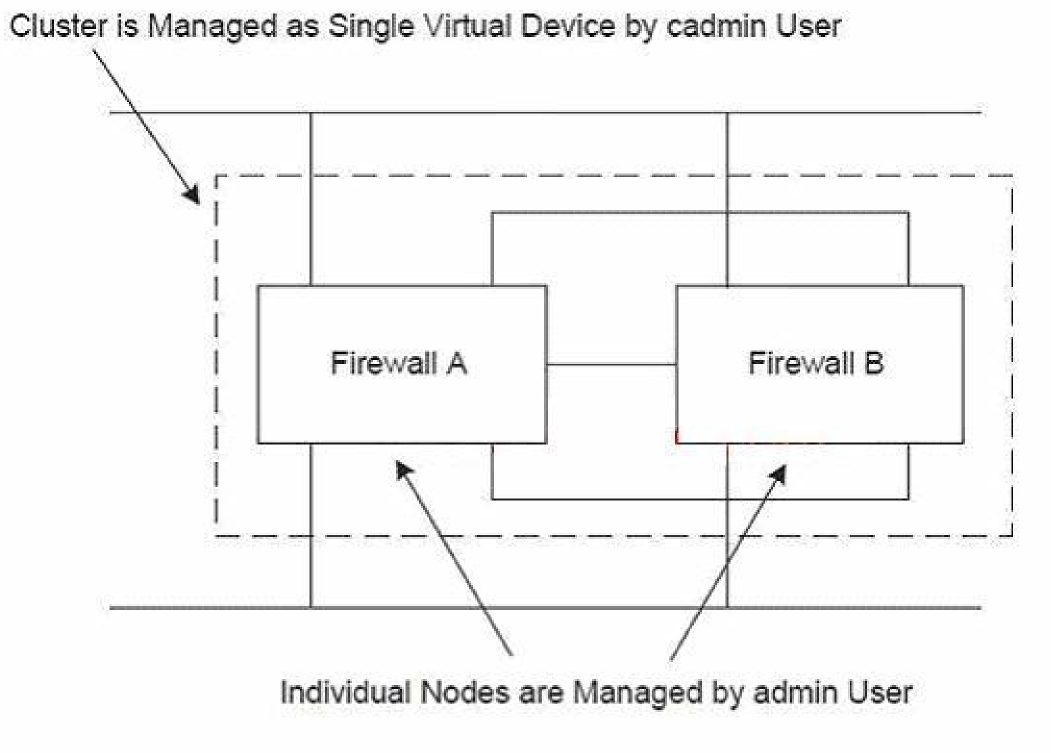

Cluster is Managed as Single Virtual Device by cadmin User
Firewall A
Firewall B
Individual Nodes are Managed by admin User
ActualTests

Figure 1: Clustering System

A. Cluster Voyager and the cluster CLI manage multiple clustered IPSO systems as if they are a single system
B. Voyager and Cluster Voyager do the same job
C. Cluster Voyager and the cluster CLI do the same job
D. Cluster Voyager and the cluster CLI manage is designed to manage a single system
E. Voyager and the CLI manage a single IPSO system

Answer: A,C,E

QUESTION NO: 261

Using third party PKI involves creating a certificate for the user and:

A. A certificate for the User Group

B. A certificate for the NT Server

C. A certificate for the Security Management Server

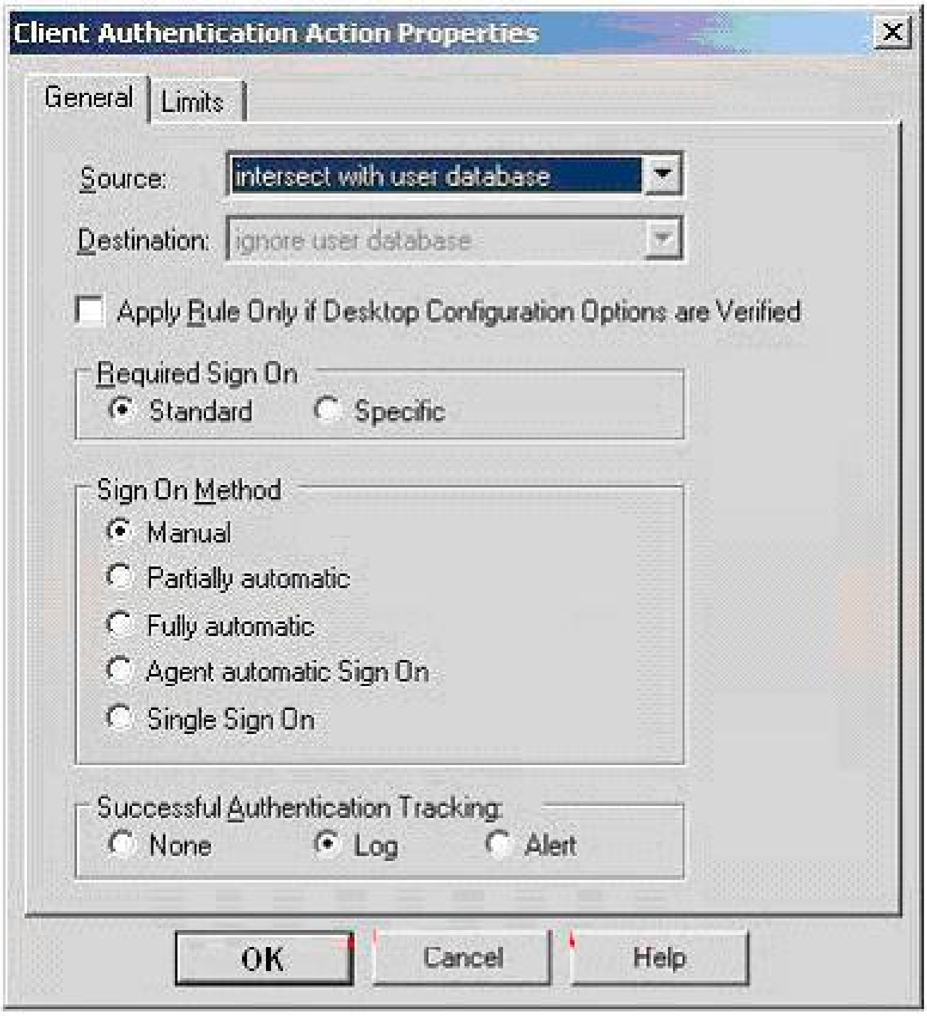
D. A certificate for the gateway

E. A certificate for the Policy Server

Answer: D

QUESTION NO: 262

How would you treat a Authentication user when the allowed location in the User definition is different than the location allowed to the user in the Rule in Client Authentication?



Client Authentication Action Properties

Source: intersect with user database

Destination: ignore user database

☐ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On: ● Standard ○ Specific

Sign On Method:
- ● Manual
- ○ Partially automatic
- ○ Fully automatic
- ○ Agent automatic Sign On
- ○ Single Sign On

Successful Authentication Tracking: ○ None ● Log ○ Alert

Figure 1: Client Authentication Action Properties box

A. Configure Any Authentication Method scheme

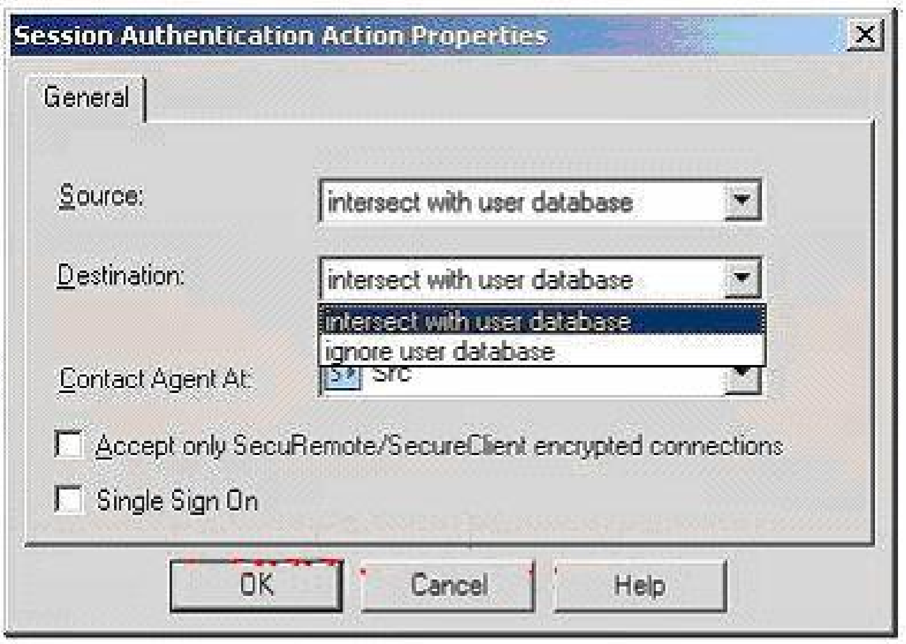
B. Configure Authentication Method scheme

C. Configure Session Authentication Action Properties
D. Configure User Authentication Action Properties
E. Configure Client Authentication Action Properties

Answer: E

QUESTION NO: 263

How would you treat a user access when the allowed location of the user is different than the location allowed to the user in the Rule in the Session Authentication?



Session Authentication Action Properties

General

Source: intersect with user database

Destination: intersect with user database

intersect with user database
ignore user database

Contact Agent At: Src

□ Accept only SecuRemote/SecureClient encrypted connections

□ Single Sign On

Figure 1: Session Authentication Action Properties

A. Configure Any Authentication Method scheme
B. Configure Authentication Method scheme
C. Configure Client Authentication Action Properties
D. Configure Session Authentication Action Properties
E. Configure User Authentication Action Properties

Answer: D

QUESTION NO: 264

The remote access clients connect with gateways using Connect mode. The Connect mode offers which of the following features? Select all the correct answers.

A. VPN Tunnel mode
B. Office mode
C. Visitor mode
D. User profiles
E. Routing all traffic through Gateway (Hub mode)

Answer: B,C,D,E

QUESTION NO: 265

The benefits of upgrading from SmartDefense to IPS R70 Include:

A. IPS R70 engine is completely re-written to provide better reporting
B. IPS R70 engine is completely re-written to provide improved security performance
C. The license fee of IPS R70 is lot cheaper than SmartDefense
D. Upgrading does not provide any visible benefits
E. IPS R70 provides easy upgrade

Answer: A,B

QUESTION NO: 266

You are in SecurePlatform and you want to make temporary change to one of the network interface card. You need to change the MAC address of the interface eth0 to "00:2B:40:23:45:07". You want this change to be temporary in that after re-starting the network, you want the old MAC address to be active. How would you go about this?

A. You will edit the /etc/sysconfig/netconf.C and input the MAC address in the field
B. You will login as expert user and enter the following commands: # ip link set eth0 down # ip link set eth0 up
C. You will login as expert user and enter the following commands: # ip link set eth0 down # ip link set eth0 addr 00:2B:40:23:45:07 # ip link set eth0 up
D. You will login as standard user and enter the following commands: # ip link set eth0 down # ip link set eth0 addr 00:2B:40:23:45:07 # ip link set eth0 up
E. You will login as standard user and enter the following commands: # ip link set eth0 addr 00:2B:40:23:45:07

Answer: C

QUESTION NO: 267

Which of these authenticates users for specific services?

A. Implicit session authentication

B. Session authentication

C. Client authentication

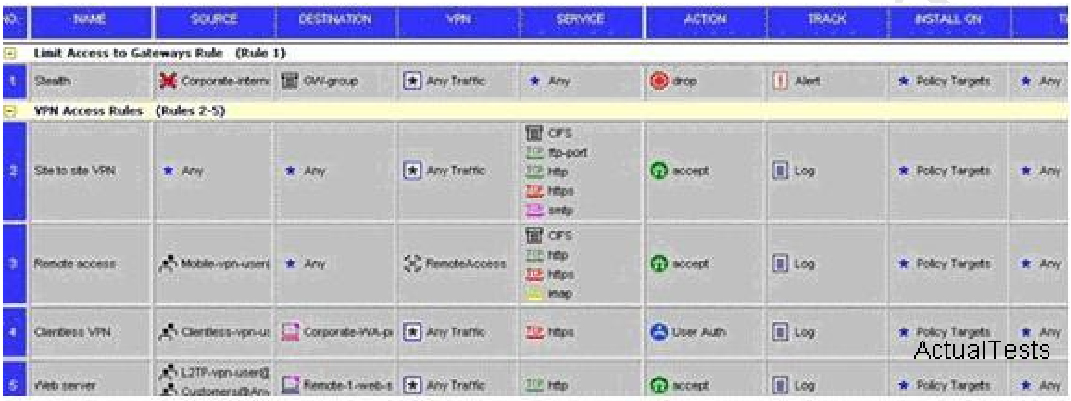
D. User authentication

E. Implicit client authentication

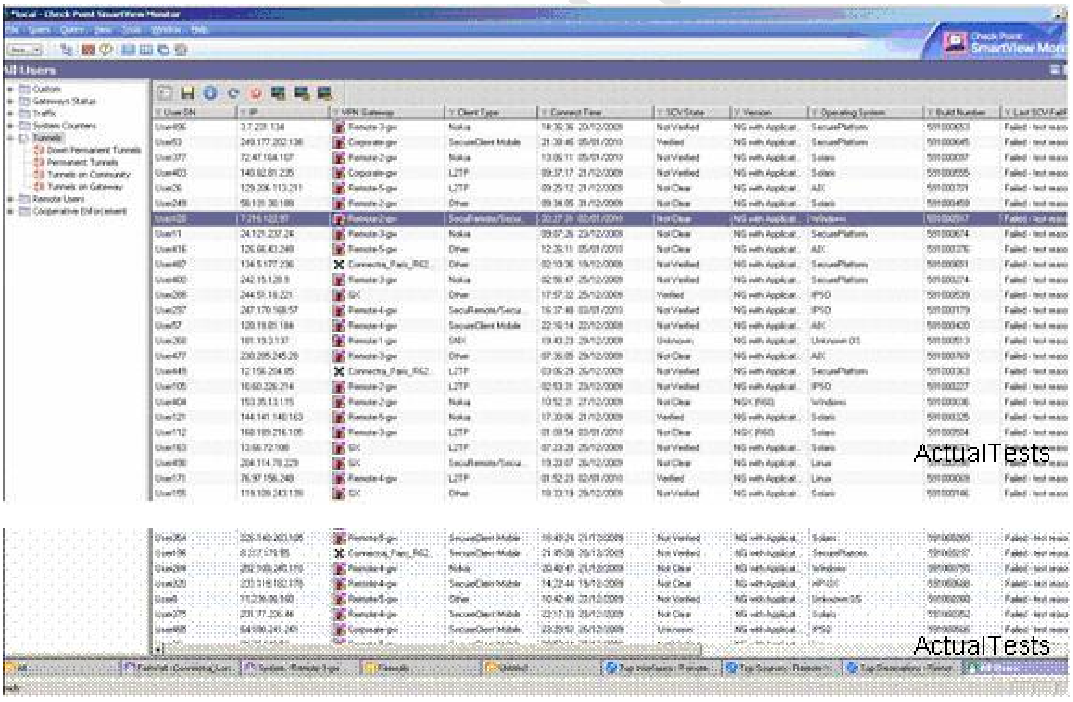
Answer: D

QUESTION NO: 268

Examine the diagram and then answer the question. Which of the following rules will hinder rule 4?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	T
	Limit Access to Gateways Rule (Rule 1)								
1	Stealth	Corporate-intern	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any
	VPN Access Rules (Rules 2-5)								
2	Site to site VPN	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any
3	Remote access	Mobile-vpn-users	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any
4	Clientless VPN	Clientless-vpn-us	Corporate-WA-p	Any Traffic	https	User Auth	Log	Policy Targets	Any
5	Web server	L2TP-vpn-user@ Customers@Any	Remote-1-web-s	Any Traffic	http	accept	Log	Policy Targets	Any



A. Rule 3

B. Rule 1

C. No rule hinders rule 4

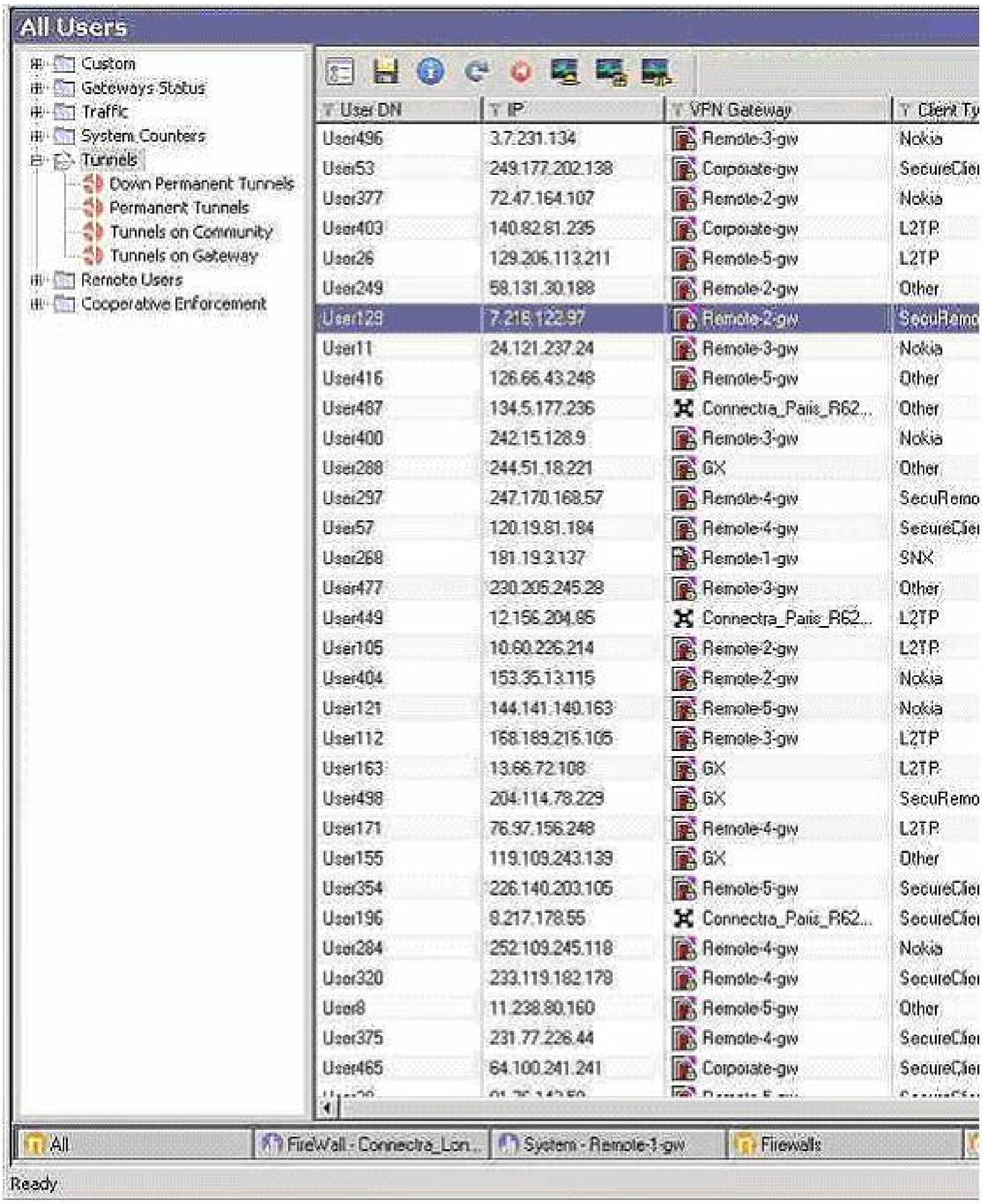
D. Rule 5

E. Rule 2

Answer: E

QUESTION NO: 269

When a Tunnel view is run, the results appear in the SmartView Monitor SmartConsole. A Tunnels view can be created and run for which of the following options?



User DN	IP	VPN Gateway	Client Ty
User496	3.7.231.134	Remote-3-gw	Nokia
User53	249.177.202.138	Corporate-gw	SecureClie
User377	72.47.164.107	Remote-2-gw	Nokia
User403	140.82.81.235	Corporate-gw	L2TP
User26	129.206.113.211	Remote-5-gw	L2TP
User249	58.131.30.188	Remote-2-gw	Other
User129	7.218.122.97	Remote-2-gw	SecuRemo
User11	24.121.237.24	Remote-3-gw	Nokia
User416	126.66.43.248	Remote-5-gw	Other
User487	134.5.177.236	Connectra_Paris_R62...	Other
User400	242.15.128.9	Remote-3-gw	Nokia
User288	244.51.18.221	GX	Other
User297	247.170.168.57	Remote-4-gw	SecuRemo
User57	120.19.81.184	Remote-4-gw	SecureClie
User268	181.19.3.137	Remote-1-gw	SNX
User477	230.205.245.28	Remote-3-gw	Other
User449	12.156.204.85	Connectra_Paris_R62...	L2TP
User105	10.60.226.214	Remote-2-gw	L2TP
User404	153.35.13.115	Remote-2-gw	Nokia
User121	144.141.140.163	Remote-5-gw	Nokia
User112	168.189.216.105	Remote-3-gw	L2TP
User163	13.66.72.108	GX	L2TP
User498	204.114.78.229	GX	SecuRemo
User171	76.97.156.248	Remote-4-gw	L2TP
User155	119.109.243.139	GX	Other
User354	226.140.203.105	Remote-5-gw	SecureClie
User196	8.217.178.55	Connectra_Paris_R62...	SecureClie
User284	252.109.245.118	Remote-4-gw	Nokia
User320	233.119.182.178	Remote-4-gw	SecureClie
User8	11.238.80.160	Remote-5-gw	Other
User375	231.77.226.44	Remote-4-gw	SecureClie
User465	64.100.241.241	Corporate-gw	SecureClie

A. Tunnel Users

B. Down Permanent Tunnels

C. Tunnels on Community

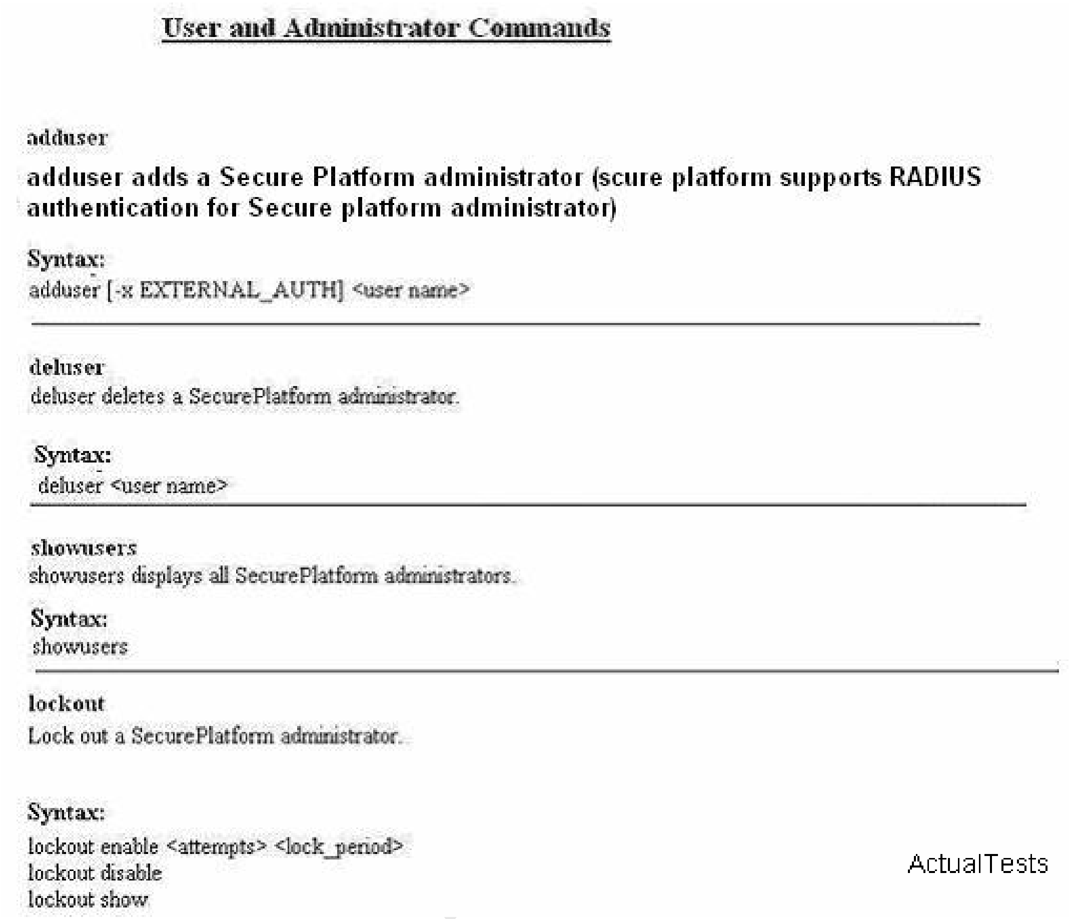
D. Permanent Tunnels

E. Tunnels on Gateway

Answer: B,C,D,E

QUESTION NO: 270

To unlock a SecurePlatform Administrator account called kate, you will use the command:



User and Administrator Commands

adduser

adduser adds a Secure Platform administrator (scure platform supports RADIUS authentication for Secure platform administrator)

Syntax:

adduser [-x EXTERNAL_AUTH] <user name>

deluser

deluser deletes a SecurePlatform administrator.

Syntax:

deluser <user name>

showusers

showusers displays all SecurePlatform administrators.

Syntax:

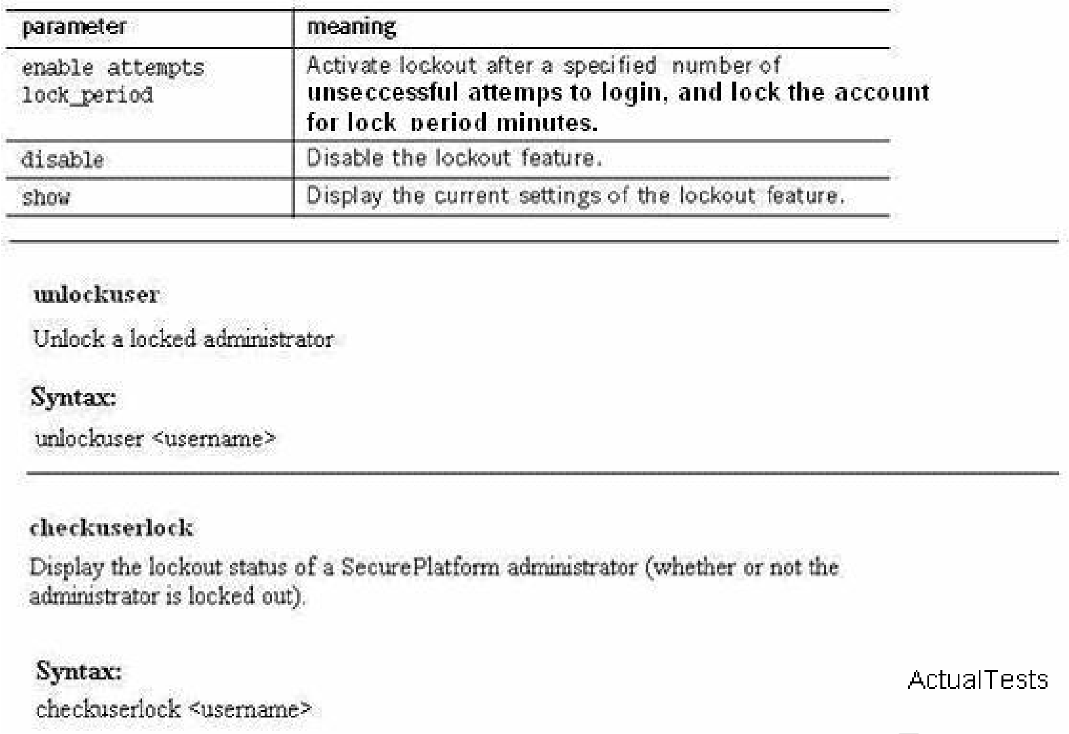
showusers

lockout

Lock out a SecurePlatform administrator.

Syntax:

lockout enable <attempts> <lock_period>
lockout disable
lockout show



parameter	meaning
enable attempts lock_period	Activate lockout after a specified number of **unseccessful attemps to login, and lock the account for lock period minutes.**
disable	Disable the lockout feature.
show	Display the current settings of the lockout feature.

unlockuser

Unlock a locked administrator

Syntax:

unlockuser <username>

checkuserlock

Display the lockout status of a SecurePlatform administrator (whether or not the administrator is locked out).

Syntax:

checkuserlock <username>

A. releasekate

B. unlockuserkate

C. unlock username

D. unlockuser usernamekate

E. unlockkate

Answer: B

QUESTION NO: 271

There are situations in which a computer does not yet have a Security Policy installed, and is vulnerable. Two features that provide security when security policy has not been installed and activated are: Boot Security - which secures communication during the boot period , and the Initial Policy -

A. Which provides security after a Security Policy is installed for the first time

B. Which allows control of IPforwarding

C. Which disables IP forwarding in the OSkernel

D. Which allows allcommunications

E. Which provides security before a Security Policy is installed for the first time

Answer: E

QUESTION NO: 272

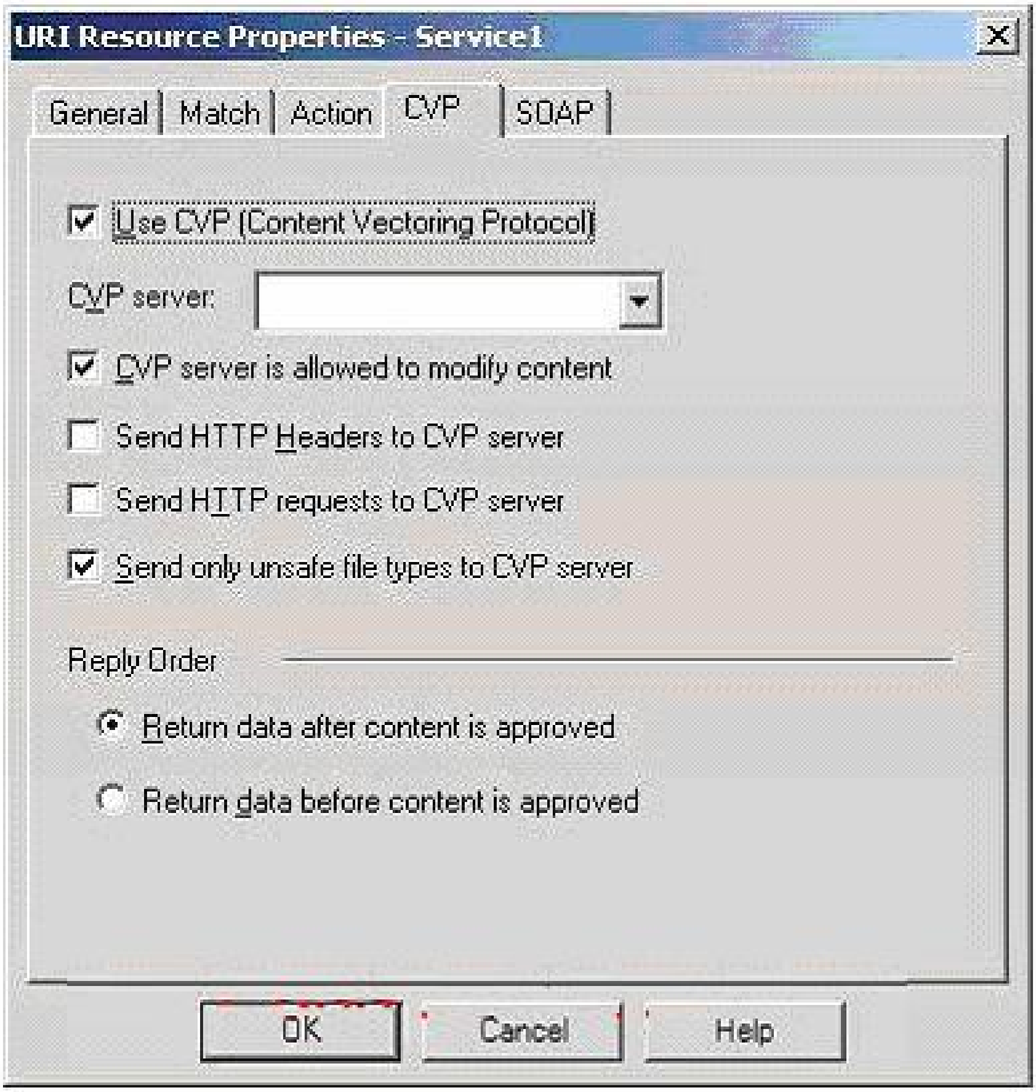
You run a Distributed deployment. Your Security Management Server is down and cannot be re-booted for some reasons. The remote Security Gateway that is being managed by the Security Management Server suddenly reboots. What is likely to happen once the Security Gateway finishes rebooting?

A. The remote Security Gateway will allow all traffic and will also log locally
B. The remote Security Gateway will fetch the last Security Policy locally and will not pass the traffic, and will log locally
C. The remote Security Gateway will block all traffic and will also log locally
D. The remote Security Gateway will fetch the last Security Policy locally and will pass the traffic normally, and will also log locally
E. The remote Security Gateway will fetch the last Security Policy from the Security Management Server and will pass the traffic normally, and will also log locally

Answer: D

QUESTION NO: 273

One of differences between the "Enhanced UFP Performance Mode" and "URL Filtering Using the HTTP Security Server" lie in the fact that with the: Note:The diagram is part of the explanation.



URI Resource Properties - Service1

☑ Use CVP (Content Vectoring Protocol)

CVP server:

☑ CVP server is allowed to modify content

□ Send HTTP Headers to CVP server

□ Send HTTP requests to CVP server

☑ Send only unsafe file types to CVP server

Reply Order

● Return data after content is approved

○ Return data before content is approved

Figure 1: URI Resource Properties

A. "URL Filtering Using the HTTP Security Server" requires Security gateway to mediate connections

B. The are no differences between the two

C. "Enhanced UFP Performance Mode", the users browsing websites experience significantly improved response times

D. "Enhanced UFP Performance Mode" requires Security gateway to mediate connections

E. "URL Filtering Using the HTTP Security Server", the users browsing websites experience significantly improved response times

Answer: C

QUESTION NO: 274

You contact the SmartView Tracker about ftp connections to a ftp server called boson that keep dropping after an two hours of idleness. The SmartView Tracker shows "Unknown established error" entry for this connection. How would you resolve this error without causing any other security problems?

A. You will create a new TCP service object on port 21 which you can name as ftpboson, then configure the Global Properties. You will then use the new object only in the rule that allows the ftp connections to the boson
B. Go to the Global Properties window, increase the ftp connections to 24 hours
C. You will create a new TCP service object on port 21 which you can name as ftpboson. You will then use the new object only in the rule that allows the ftp connections to the boson
D. You will create a new TCP service object on port 21 which you can name as ftpboson, then define a service-based session timeout of 24 hours. You will then use the new object only in the rule that allows the ftp connections to the boson
E. Go to the Global Properties window, increase the TCP connections to 24 hours

Answer: D

QUESTION NO: 275

Why would an administrator want to disable a rule ?

A. Only when verifying a security policy without affecting the actualfirewalled network
B. Only when enforcing a security policy without affecting the actualfirewalled network
C. Only when testing a security policy on external network without affecting the actualfirewalled network
D. Only when installing a security policy without affecting the actualfirewalled network
E. Only when troubleshooting a firewall problem

Answer: E

QUESTION NO: 276

Application Intelligence feature of the IPS prevent and defend attacks of which of the OSI layer?

A. Session
B. Network
C. Transport
D. Application
E. Data Link

Answer: D

QUESTION NO: 277

Which mode would you run your IPSO appliance if you want it to function as a layer 2 bridge?

A. Transparent Mode
B. Layer 2 Mode
C. Masking Mode
D. Packet Forwarding Mode
E. Routing Mode

Answer: A

QUESTION NO: 278

If aggressive mode is selected for your IPSec tunnel, the gateway performs the IKE negotiation using how many packets during phase 1 exchange?

A. 9
B. 2
C. 3
D. 6
E. 12

Answer: C

QUESTION NO: 279

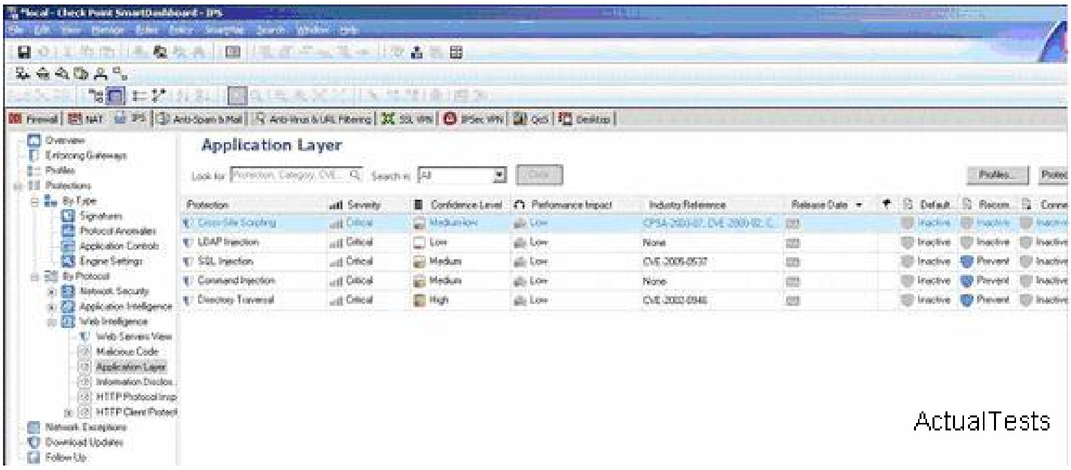
You want to download a contracts file from Checkpoint User Center website (when upgrading your Security Gateway from R65 to R70), which of the following options below lists the correct steps you will take to achieve this?

A. Enter your credentials,then choose your contracts from the site
B. Choose upgrade contracts from the site, then enter your username then follow by your password
C. Navigate to the contracts file, then enter your username then follow by your password
D. Browse to the contracts file from the list of files, then enter your username then follow by your password
E. Enter your Security Gateway information, then enter your username then follow by your password

Answer: B

QUESTION NO: 280

You need to configure IPS in order to protect your network against traffic hijack attempts. Which of the following will you configure?



Protection	Severity	Confidence Level	Performance Impact	Industry Reference	Release Date		Default...	Recom...	Conne
Cross-Site Scripting	Critical	Medium-low	Low	CPSA-2003-07, CVE-2000-02, C...			Inactive	Inactive	Inactive
LDAP Injection	Critical	Low	Low	None			Inactive	Inactive	Inactive
SQL Injection	Critical	Medium	Low	CVE-2005-0537			Inactive	Prevent	Inactive
Command Injection	Critical	Medium	Low	None			Inactive	Prevent	Inactive
Directory Traversal	Critical	High	Low	CVE-2002-0946			Inactive	Prevent	Inactive

Figure 1: Application layer > Cross-Site Scripting

A. Cross-Site Scripting
B. Directory Traversal
C. Command Injection
D. SQL Injection
E. LDAP Injection

Answer: A

QUESTION NO: 281

You are using Command Line Editing keys in the SecurePlatform. What will ^a or Home key will allow you to achieve?

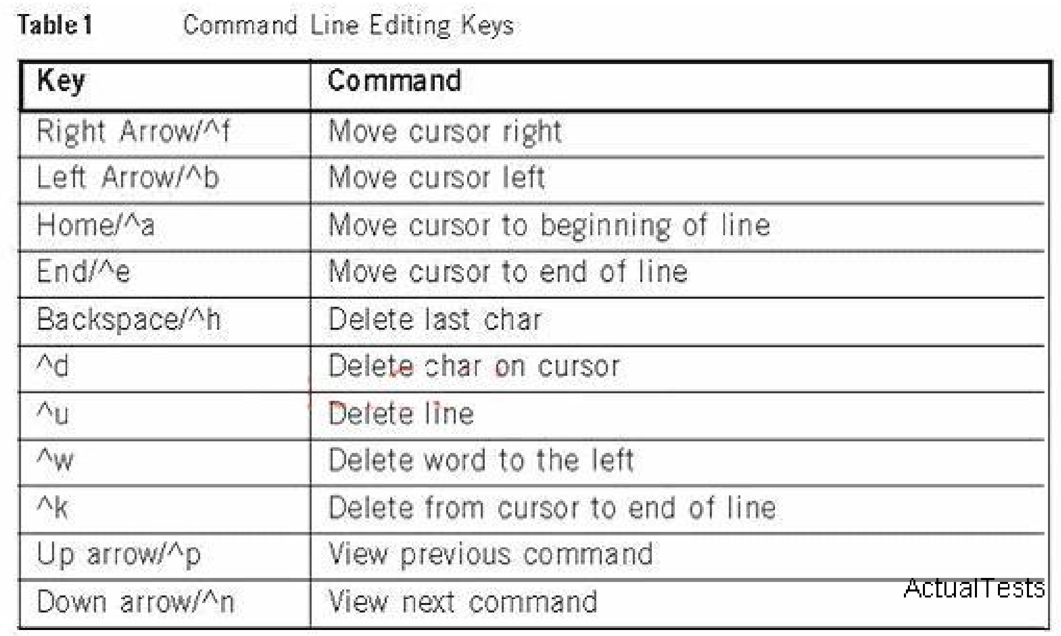


Table 1 Command Line Editing Keys

Key	Command
Right Arrow/^f	Move cursor right
Left Arrow/^b	Move cursor left
Home/^a	Move cursor to beginning of line
End/^e	Move cursor to end of line
Backspace/^h	Delete last char
^d	Delete char on cursor
^u	Delete line
^w	Delete word to the left
^k	Delete from cursor to end of line
Up arrow/^p	View previous command
Down arrow/^n	View next command

A. Move cursor to end of line
B. Delete word to the left
C. Delete word to the right
D. Move cursor to beginning of line
E. Move cursor to middle of line

Answer: D

QUESTION NO: 282

Establishing Remote Access VPN requires configuration on both the gateway side and the:

A. Hosts behind the Gateway
B. Interface leading to Gateway
C. Permanent tunnels
D. Adminstrator computer
E. Remote user side

Answer: E

QUESTION NO: 283

The policy should allow the desktop users to work as freely as possible, but at the same time makes it hard to attack the remote users' desktop. Which of the following points must you consider when defining these plans? Select all the correct answers.

A. Allow only POP3, IMAP and HTTP and block all the rest

B. Implement outbound policy to use rules in order to block specific problematic services and allow the rest
C. Outbound connections to the encryption domain of the organization must always be encrypted, even if the outbound rule for the service specifies "accept"
D. It should be borne in mind that the implied rules may allow or block services which were not explicitly handled in previous rules
E. You should not explicitly allow any service to be opened to the SecureClient

Answer: B,C,D,E

QUESTION NO: 284

Your remote Security Gateway is configured to support remote users access from their homes. These users use DSL dialup connection. Some of these users keep complaining of lost of connections. In order to resolve the problem, you go to the SmartView Tracker and notice that there is no indication that their (users) configurations have been tamper with. The remote Security Gateway is setup with static NAT. Which of the following is true? Select all the correct answers.

A. Static NAT setup may work with DSL connection because the external IP may change
B. Advice the management to change the DSL to Broadband
C. Hide NAT is likely resolve the problem
D. Static NAT setup may not work with DSL connection because the external IP may change
E. Modify the remote Security Gateway using DHCP

Answer: C,D

QUESTION NO: 285

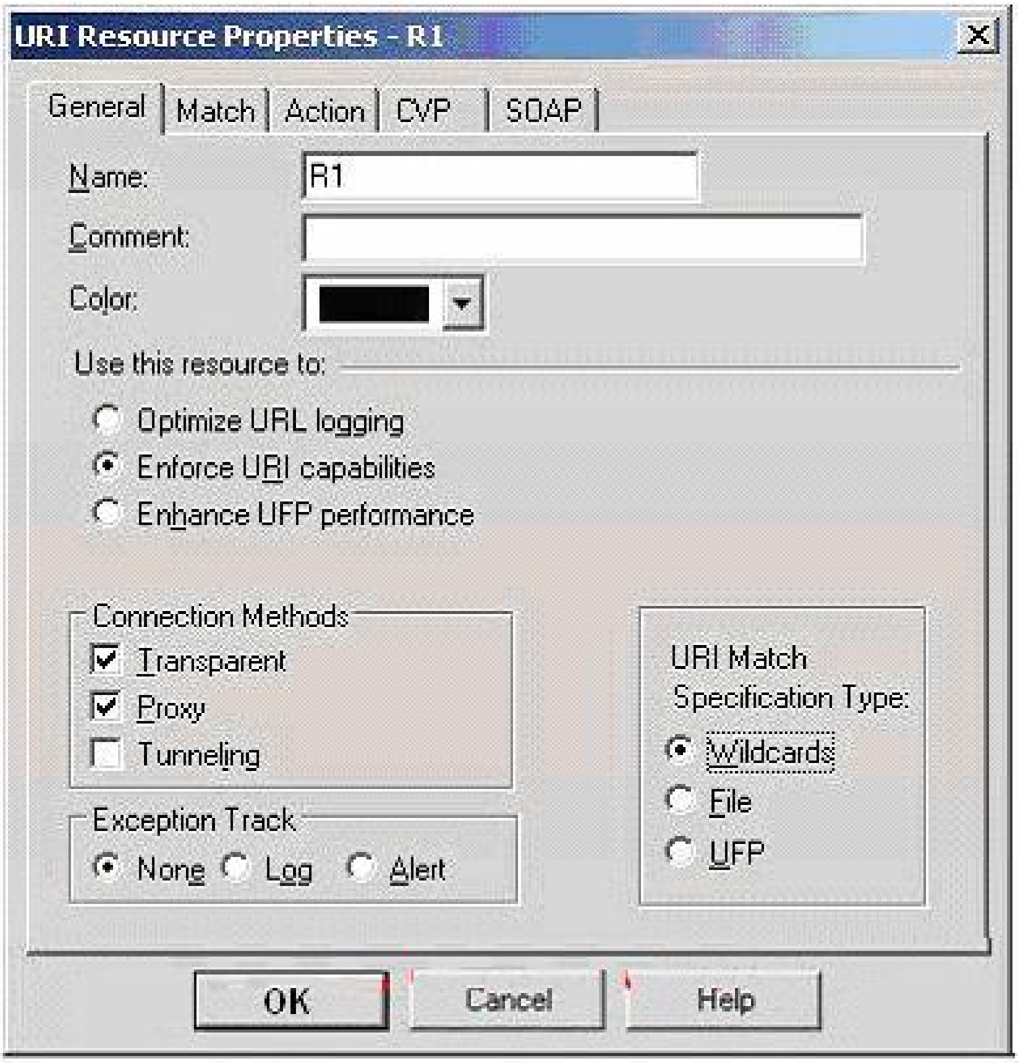
You create a file config.txt that contains a series of CLI commands. To execute the commands in file from the IPSO shell (not the CLI) you would enter which of the following command?

A. clish -f config.txt
B. set -f config.txt
C. run -f config.txt
D. load -f config.txt
E. execute -f config.txt

Answer: A

QUESTION NO: 286

In the URI Resource Properties window (see figure 1or 2 or 3), what do you think will happen if Tunneling box is checked?



Name: R1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging
● Enforce URI capabilities
○ Enhance UFP performance

Connection Methods

☑ Transparent
☑ Proxy
□ Tunneling

Exception Track

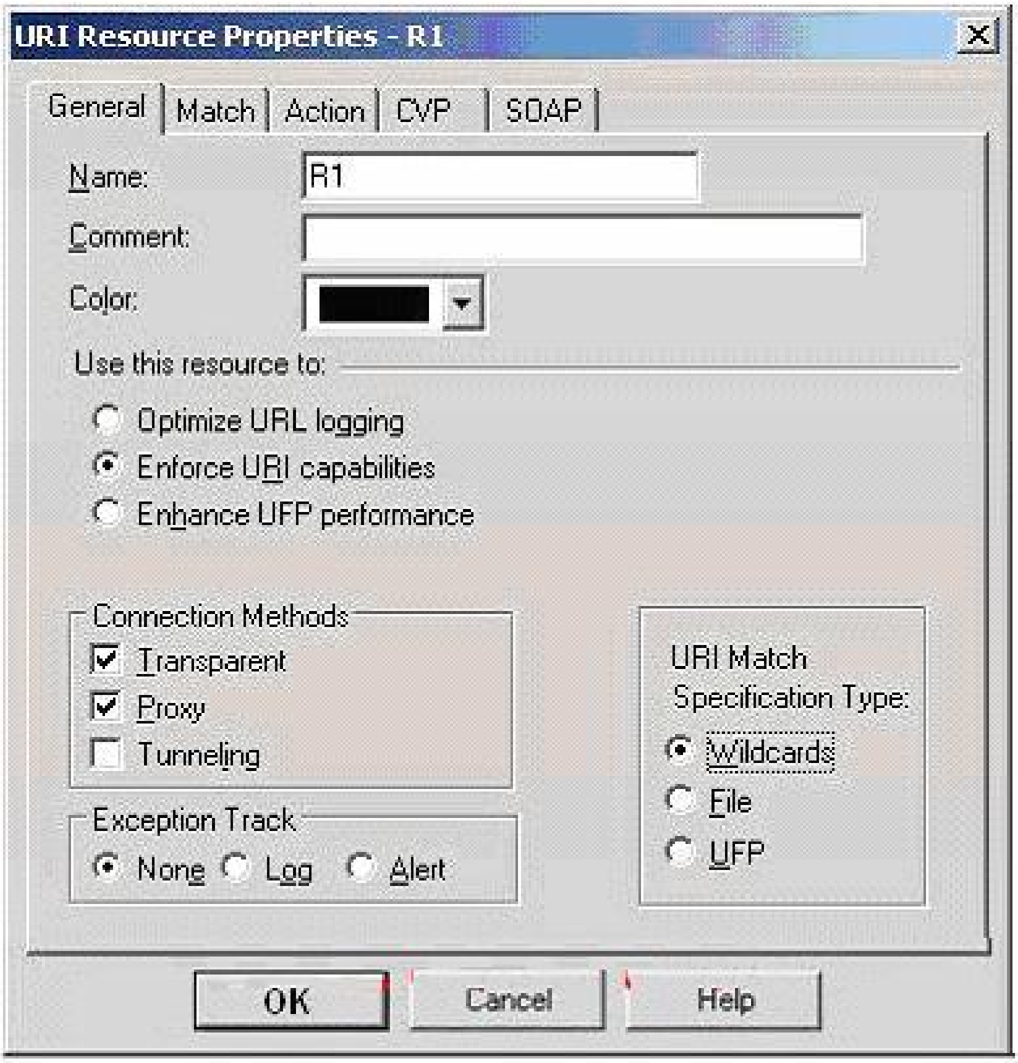
● None ○ Log ○ Alert

URI Match Specification Type:

● Wildcards
○ File
○ UFP

Figure 1: URI Resource Properties

The URI Match Specification Type section is set to :Wildcards



Name: R1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging
● Enforce URI capabilities
○ Enhance UFP performance

Connection Methods

☑ Transparent
☑ Proxy
□ Tunneling

Exception Track

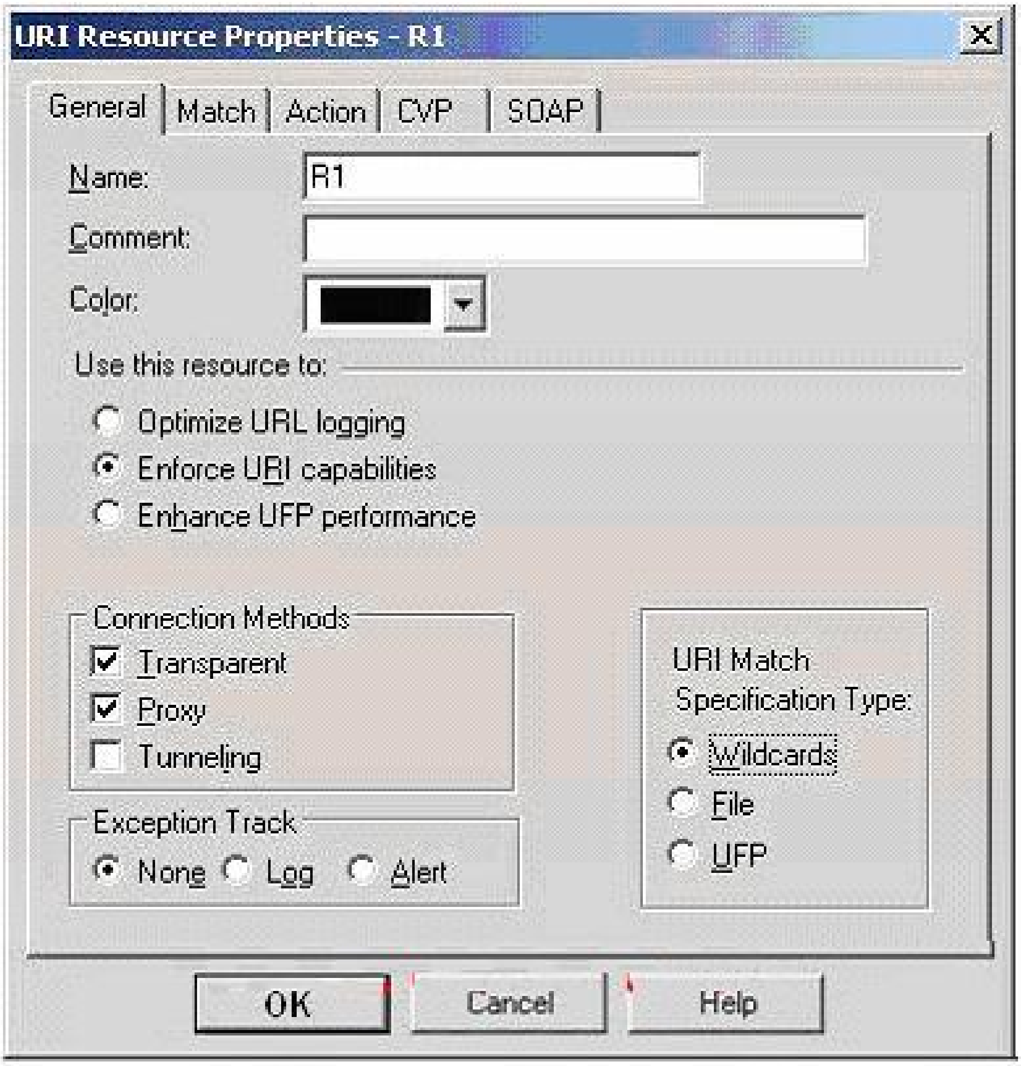
● None ○ Log ○ Alert

URI Match Specification Type:

● Wildcards
○ File
○ UFP

Figure 2 : URI Resource Properties

The URI Match Specification Type section is set to :File



Name: R1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging
● Enforce URI capabilities
○ Enhance UFP performance

Connection Methods

☑ Transparent
☑ Proxy
□ Tunneling

Exception Track

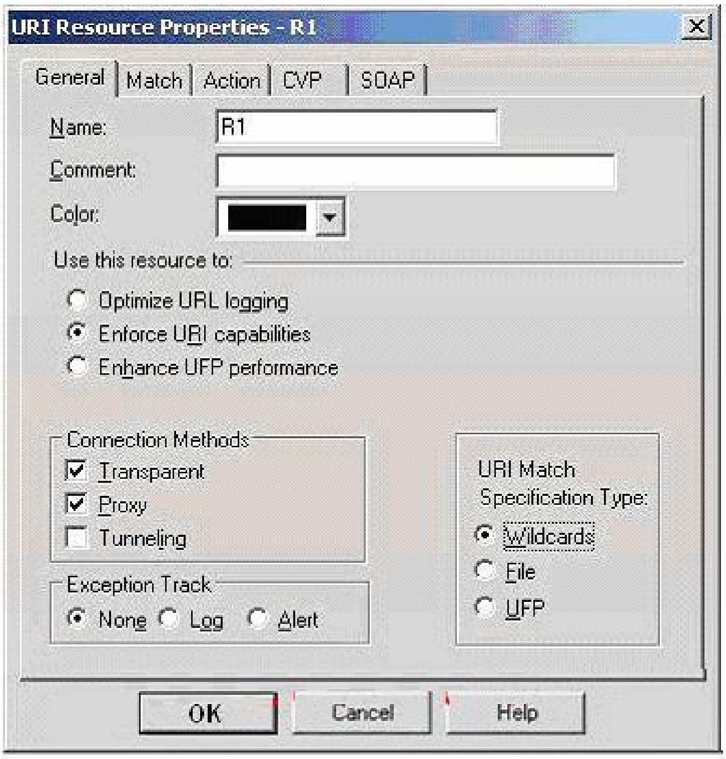
● None ○ Log ○ Alert

URI Match Specification Type:

● Wildcards
○ File
○ UFP

Figure 3 : URI Resource Properties

The URI Match Specification Type section is set to :UFP



URI Resource Properties - R1

Name: R1

Comment:

Color:

Use this resource to:

○ Optimize URL logging
● Enforce URI capabilities
○ Enhance UFP performance

Connection Methods

☑ Transparent
☑ Proxy
☐ Tunneling

Exception Track

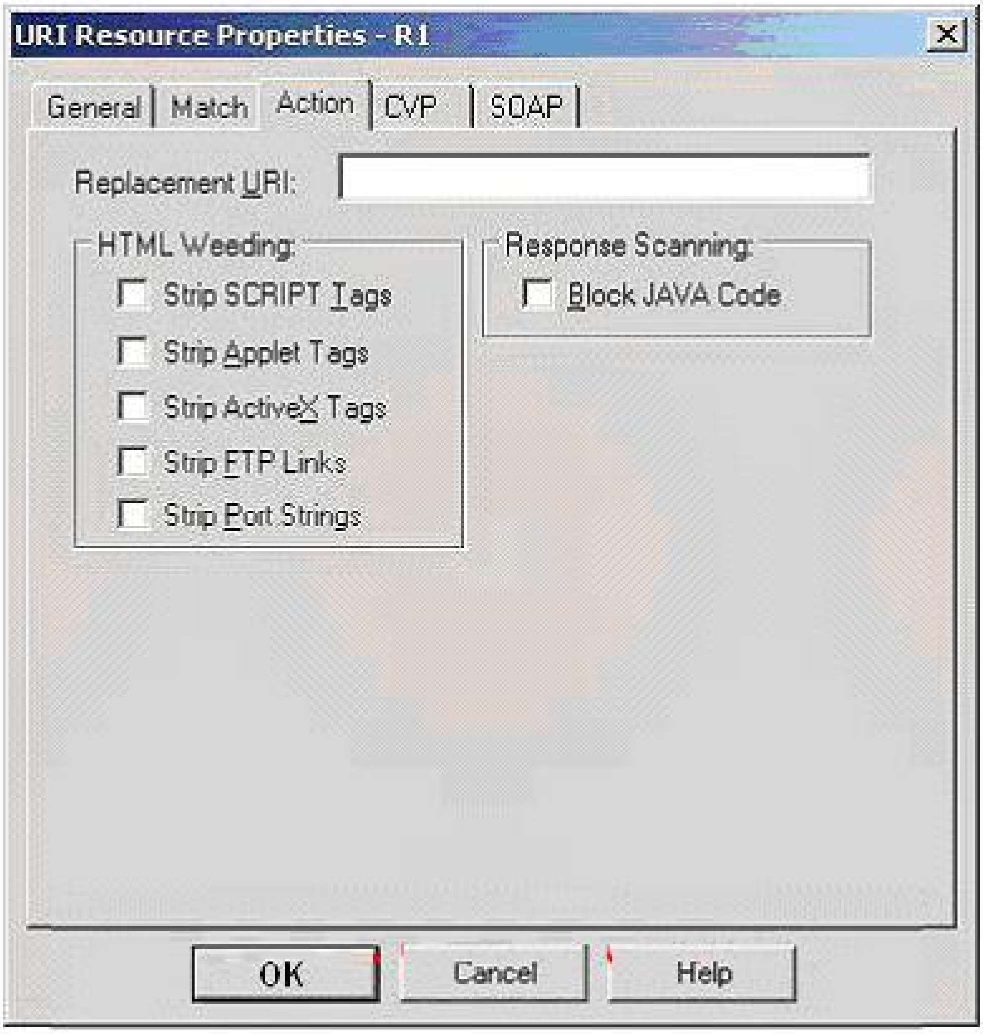
● None ○ Log ○ Alert

URI Match Specification Type:

● Wildcards
○ File
○ UFP

Figure 4 : URI Resource Properties - Tunneling Box Checked

ActualTests



Replacement URI:

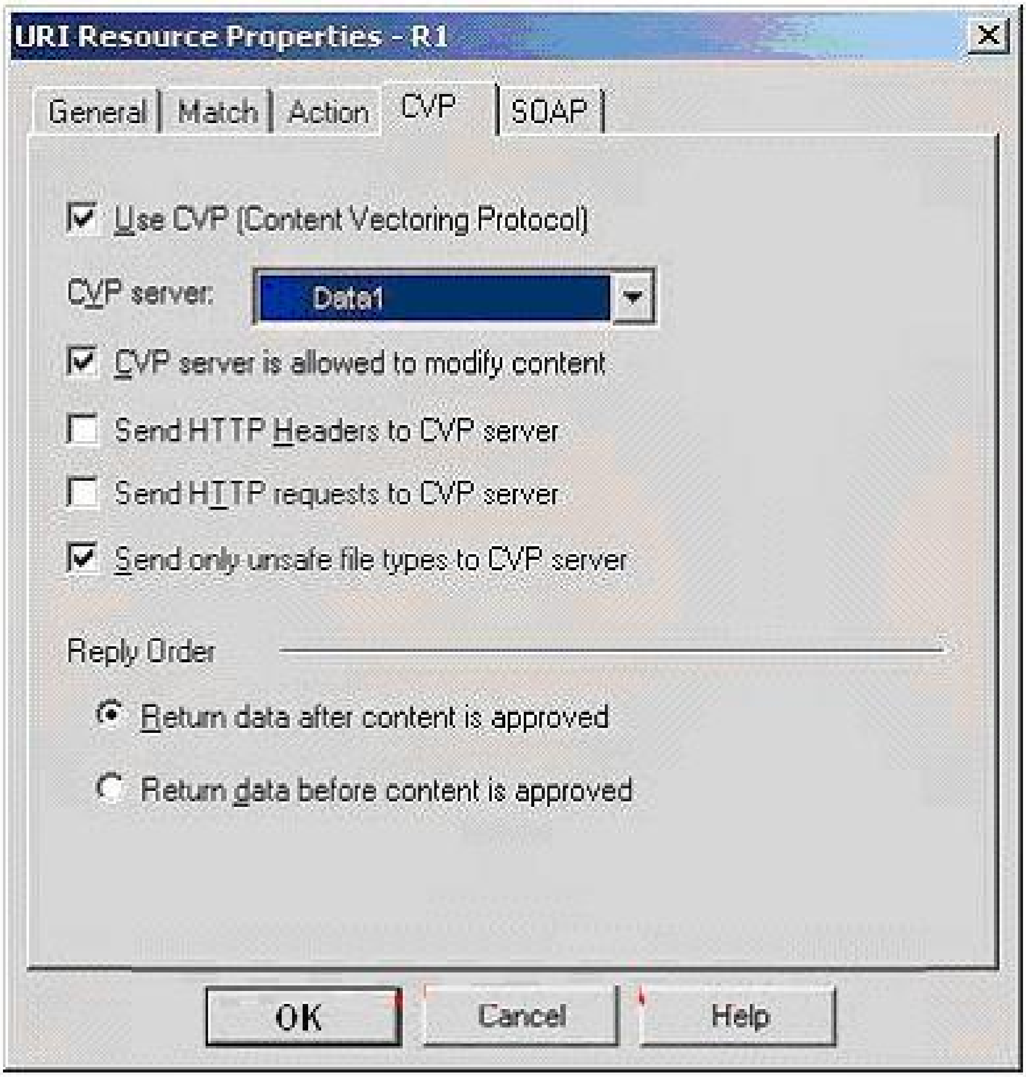
HTML Weeding:

- □ Strip SCRIPT Tags
- □ Strip Applet Tags
- □ Strip ActiveX Tags
- □ Strip FTP Links
- □ Strip Port Strings

Response Scanning:

- □ Block JAVA Code

Figure 5: URI Resource Properties - Action tab



URI Resource Properties - R1

☑ Use CVP (Content Vectoring Protocol)

CVP server: Data1

☑ CVP server is allowed to modify content

☐ Send HTTP Headers to CVP server

☐ Send HTTP requests to CVP server

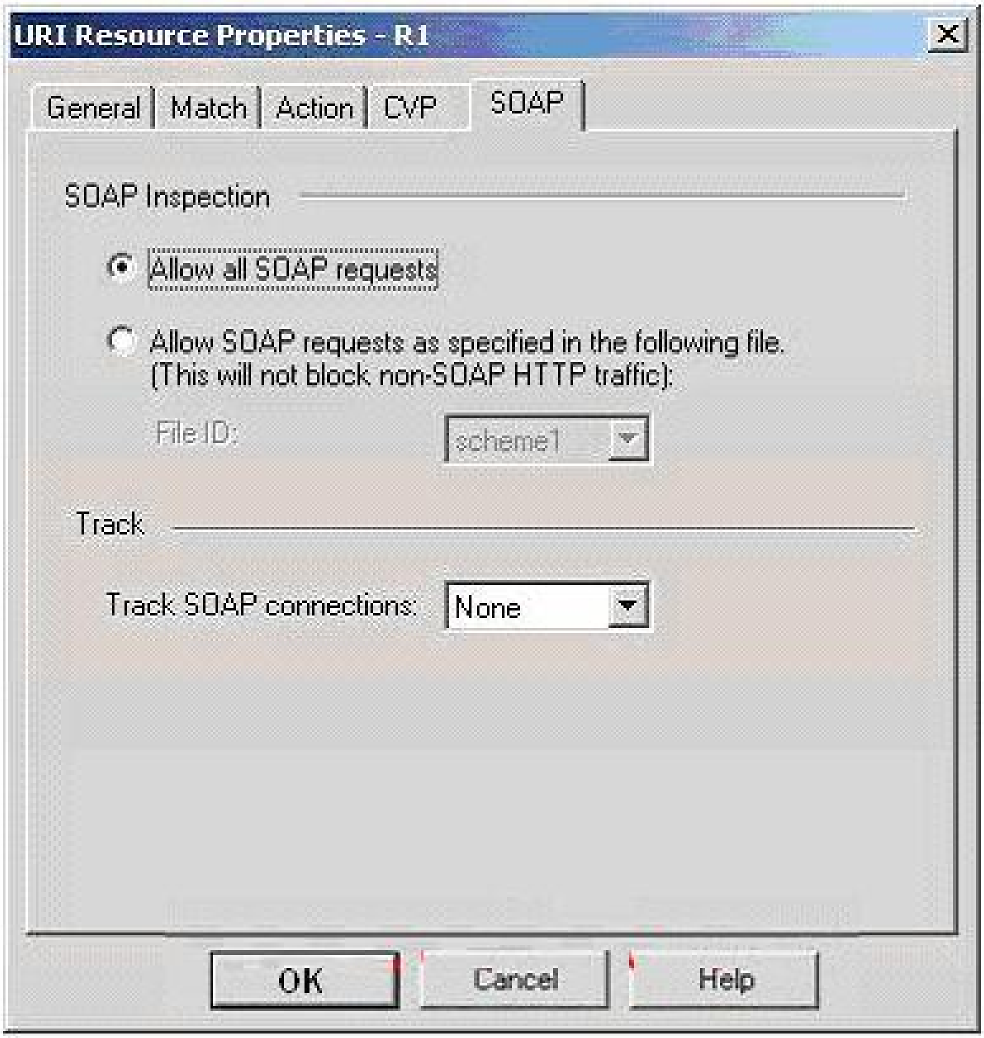
☑ Send only unsafe file types to CVP server

Reply Order

● Return data after content is approved

○ Return data before content is approved

Figure 6: URI Resource Properties - CVP tab



URI Resource Properties - R1

SOAP Inspection

● Allow all SOAP requests

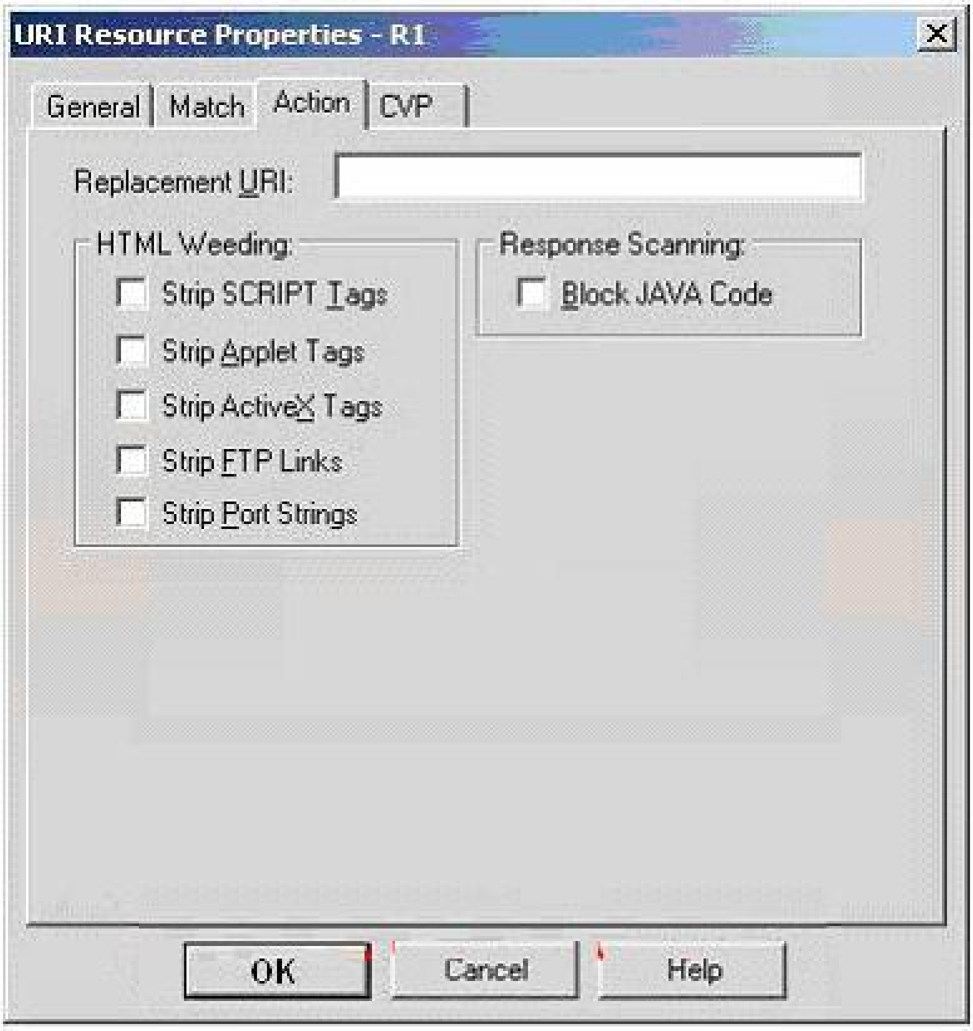
○ Allow SOAP requests as specified in the following file.
(This will not block non-SOAP HTTP traffic):

File ID: scheme1

Track

Track SOAP connections: None

Figure 7: URI Resource Properties - SOAP tab



URI Resource Properties - R1

Replacement URI:

HTML Weeding:

□ Strip SCRIPT Tags

□ Strip Applet Tags

□ Strip ActiveX Tags

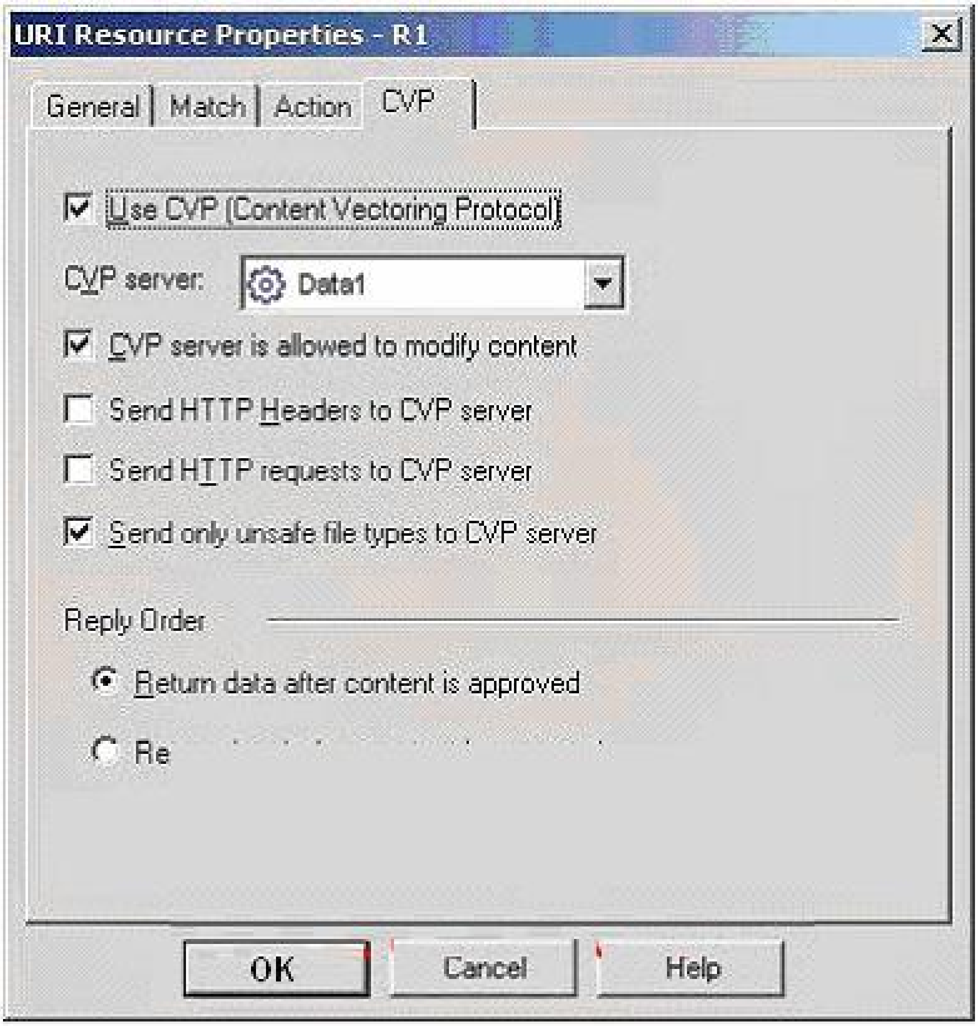
□ Strip FTP Links

□ Strip Port Strings

Response Scanning:

□ Block JAVA Code

Figure 8 : URI Resource Properties - Action tab



☑ Use CVP (Content Vectoring Protocol)

CVP server: Data1

☑ CVP server is allowed to modify content

□ Send HTTP Headers to CVP server

□ Send HTTP requests to CVP server

☑ Send only unsafe file types to CVP server

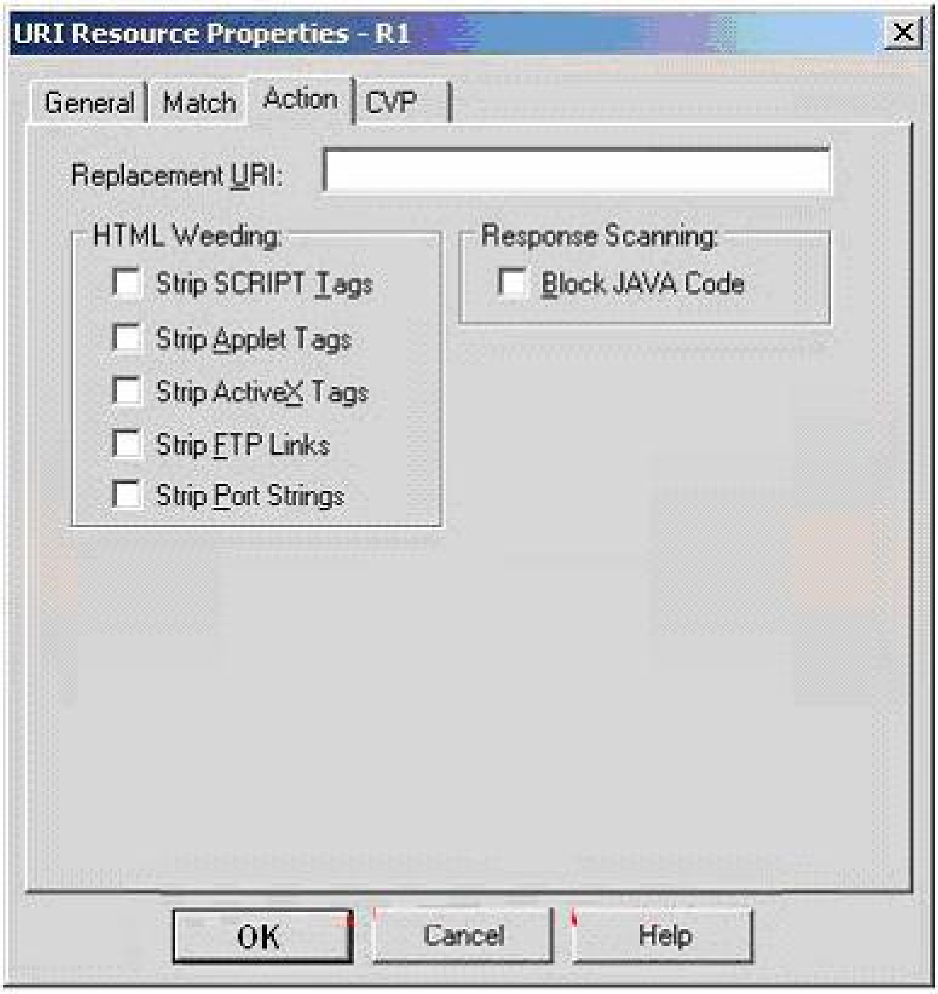
Reply Order

● Return data after content is approved

○ Re

Figure 9 : URI Resource Properties - CVP tab

If File button is selected and Tunneling box is not checked in figure 2, figure 2 show what the tabs will look like



Replacement URI:

HTML Weeding:

☐ Strip SCRIPT Tags

☐ Strip Applet Tags

☐ Strip ActiveX Tags

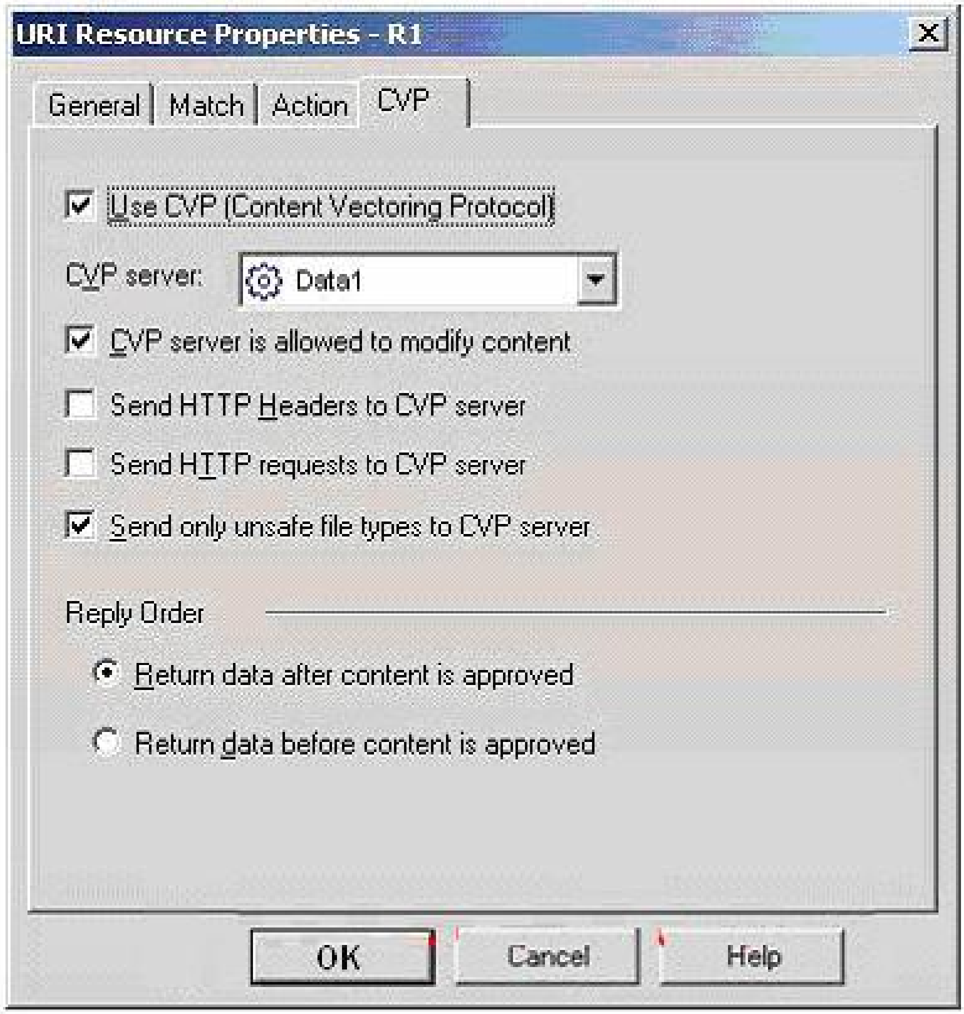
☐ Strip FTP Links

☐ Strip Port Strings

Response Scanning:

☐ Block JAVA Code

Figure 10 : URI Resource Properties - Action tab



URI Resource Properties - R1

☑ Use CVP (Content Vectoring Protocol)

CVP server: Data1

☑ CVP server is allowed to modify content

□ Send HTTP Headers to CVP server

□ Send HTTP requests to CVP server

☑ Send only unsafe file types to CVP server

Reply Order

● Return data after content is approved

○ Return data before content is approved

Figure 11 : URI Resource Properties - CVP tab

If UFP button is selected and Tunneling box is not checked in figure 3 , figures 10 and 11 show what the tabs will look like

A. You will not be allowed to use URI File

B. The Action and CVP tabs are disabled

C. The SOAP tab is disabled

D. You will not be allowed to use UFP specifications and URI File

E. You will not be allowed to use UFP specifications

Answer: B

QUESTION NO: 287

Where must you place Client authentication rule in the Rule Base in order to have access to the firewall?

A. Any where in the rulebase

B. Above the Stealth rule

C. Above Cleanup rule
D. Below Stealth rule
E. Below Cleanup rule

Answer: B

QUESTION NO: 288

You are using Command Line Editing keys in the SecurePlatform. What will ^e allow you to achieve?

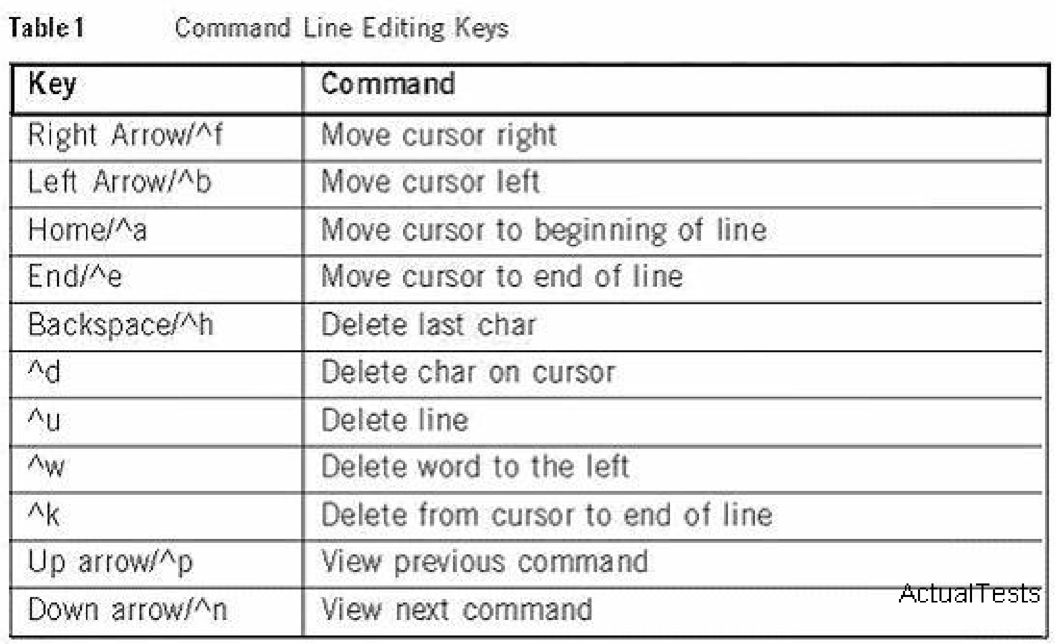


Table 1 Command Line Editing Keys

Key	Command
Right Arrow/^f	Move cursor right
Left Arrow/^b	Move cursor left
Home/^a	Move cursor to beginning of line
End/^e	Move cursor to end of line
Backspace/^h	Delete last char
^d	Delete char on cursor
^u	Delete line
^w	Delete word to the left
^k	Delete from cursor to end of line
Up arrow/^p	View previous command
Down arrow/^n	View next command

A. Move cursor to beginning of line
B. Delete word to the left
C. Delete word to the right
D. Move cursor to middle of line
E. Move cursor to end of line

Answer: E

QUESTION NO: 289

Which of these are true of the FTP Security server?

A. Implement FTP security server with an SMTP resource
B. Implement FTP security server with an FTP resource
C. FTP security server provides authentication services and content security based on FTP commands (PUT/GET)

D. Anti-virus checking for files
E. File name restrictions

Answer: B,C,D,E

QUESTION NO: 290

CI has a built-in File Type recognition engine that enables you to define a per-type policy for handling files of a given type. Which of he following file types operations can be configured? Select all the correct answers.

A. Inspect
B. Detect
C. Block
D. Pass
E. Scan

Answer: C,D,E

QUESTION NO: 291

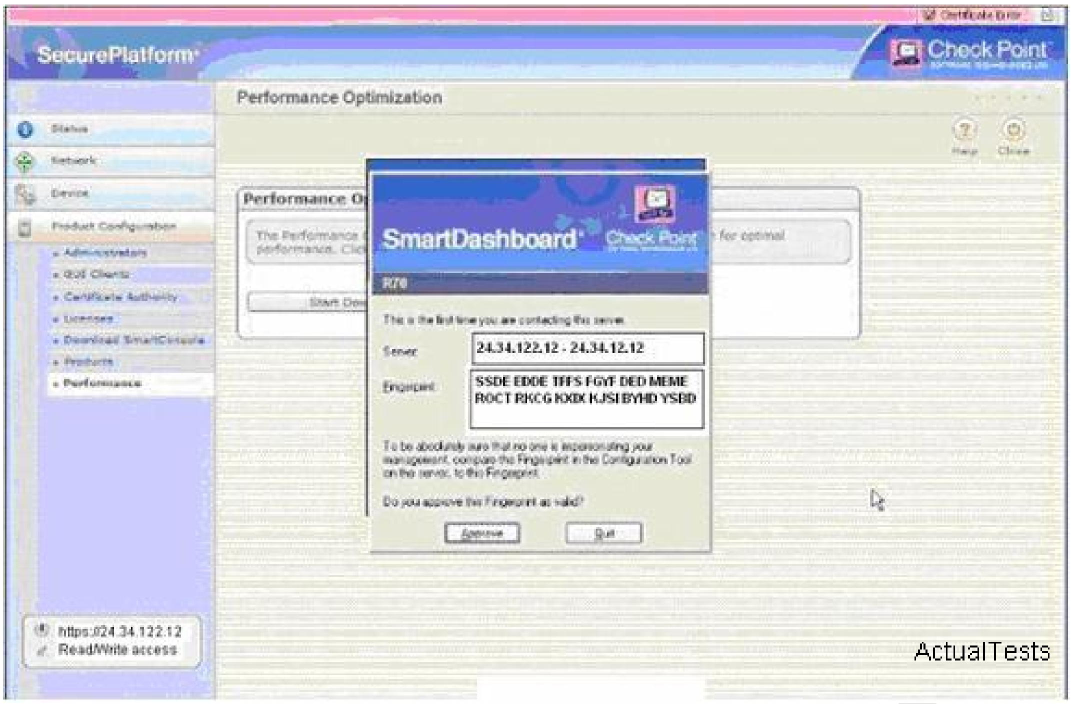
Which of the following is not an Authentication Schemes for SecureClient Mobile?

A. One Time Password
B. Legacy
C. Certificate
D. Certificate with enrollment
E. Mixed

Answer: A

QUESTION NO: 292

Examine the diagram and answer the question. Where is the fingerprint is likely to be generated?



This is the first time you are contacting this server.

Server: 24.34.122.12 - 24.34.12.12

Fingerprint: SSDE EDDE TFFS FGYF DED MEME ROCT RKCG KXDK KJSI BYHD YSBD

To be absolutely sure that no one is impersonating your management, compare the Fingerprint in the Configuration Tool on the server, to this Fingerprint.

Do you approve this Fingerprint as valid?

A. Security Management Server
B. SmartView Tracker
C. SmartConsole
D. SmartView Monitor
E. Security Gateway

Answer: A

QUESTION NO: 293

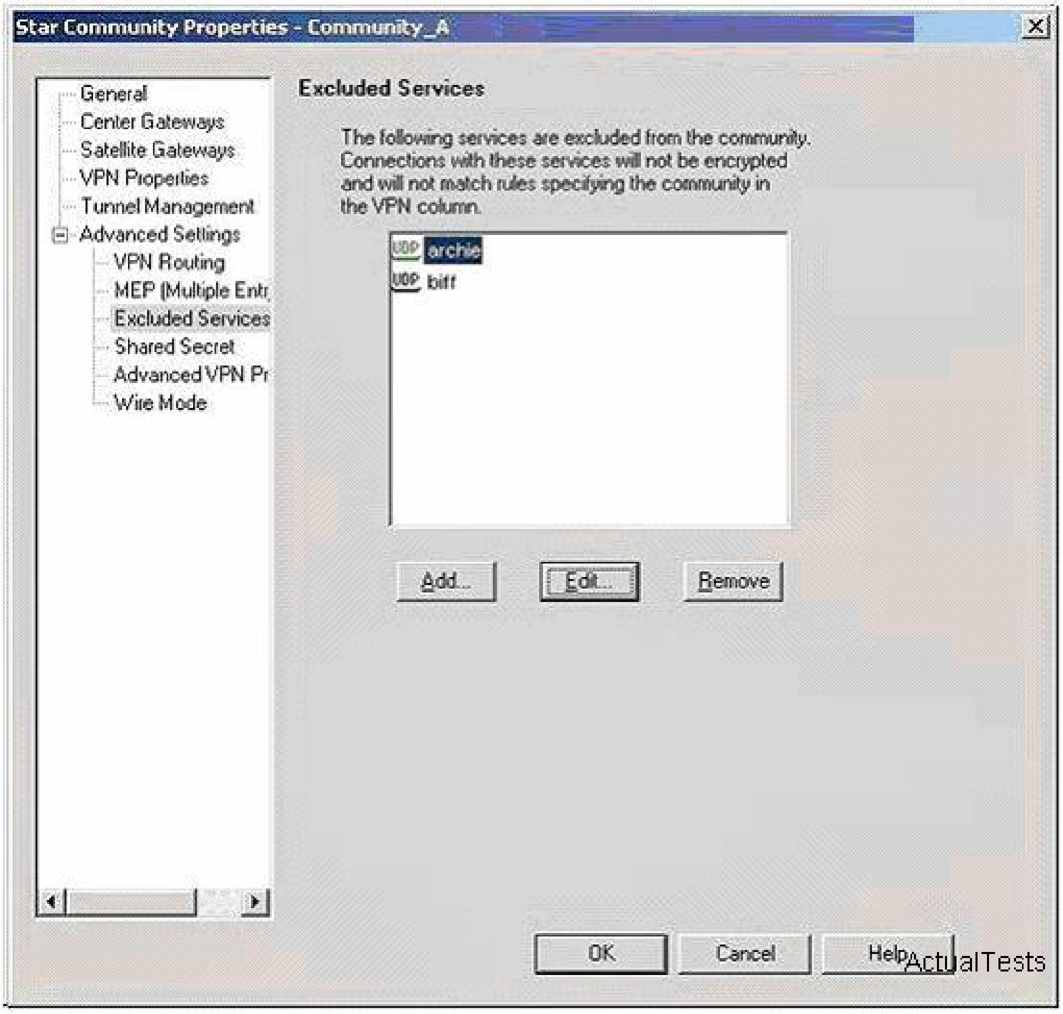
Which if the following is true of Link Aggregation feature?

A. Combination of Ethernet ports offer greater bandwidth per logical interface and load balancing across the ports
B. Combination of Ethernet ports does not necessarily offer greater bandwidth per logical interface and load balancing across the ports
C. IPSO appliances allow you to combine Ethernet ports so that they function as one logical port
D. if one of the physical links in an aggregation group fails, the traffic is redistributed to the remaining physical links
E. You can aggregate as many as four ports in one aggregation group

Answer: A,C,D,E

QUESTION NO: 294

In the VPN Communities Properties window, which page will you go prevent certain services from being encrypted?

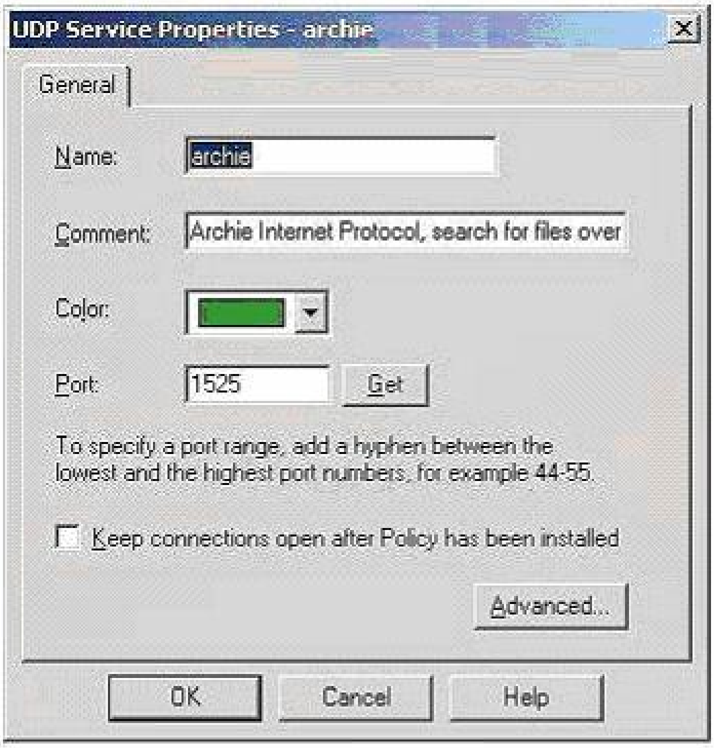


Excluded Services

The following services are excluded from the community. Connections with these services will not be encrypted and will not match rules specifying the community in the VPN column.

To edit any listed services, highlight and click it and its properties window will emerge e.g. if you click archie service. the window in figure 2 will pop up.

Figure 1: Star Community Properties Window - Excluded Services Page



UDP Service Properties - archie

General

Name: archie

Comment: Archie Internet Protocol, search for files over

Color: 🟩

Port: 1525

To specify a port range, add a hyphen between the lowest and the highest port numbers, for example 44-55.

□ Keep connections open after Policy has been installed

Figure 2: UDP Service Properties Window

A. Center Gateways

B. VPN Routing

C. Excluded Services

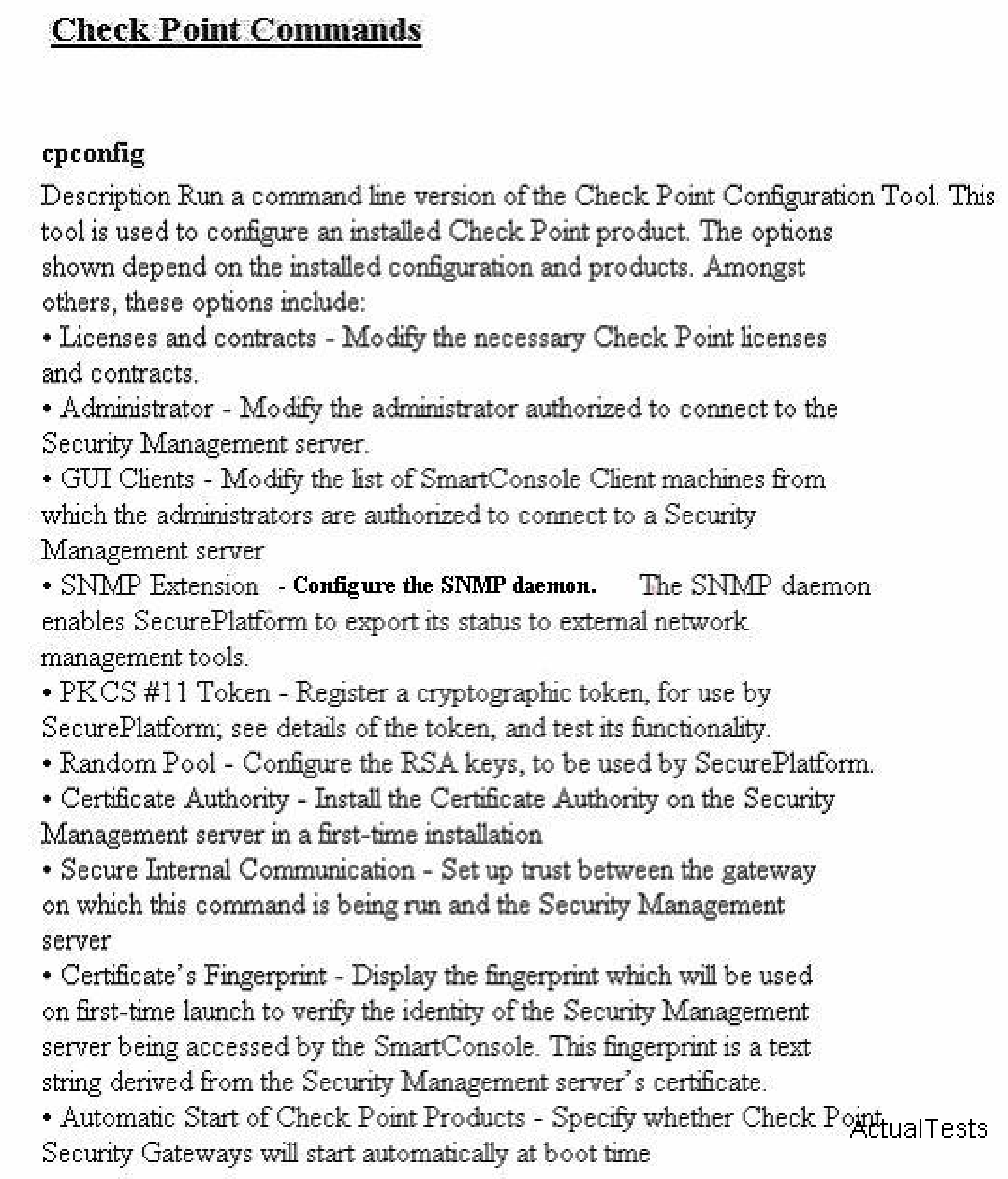
D. Wire Mode

E. Shared Secret

Answer: C

QUESTION NO: 295

What tool will you use to configure an installed Check Point product?

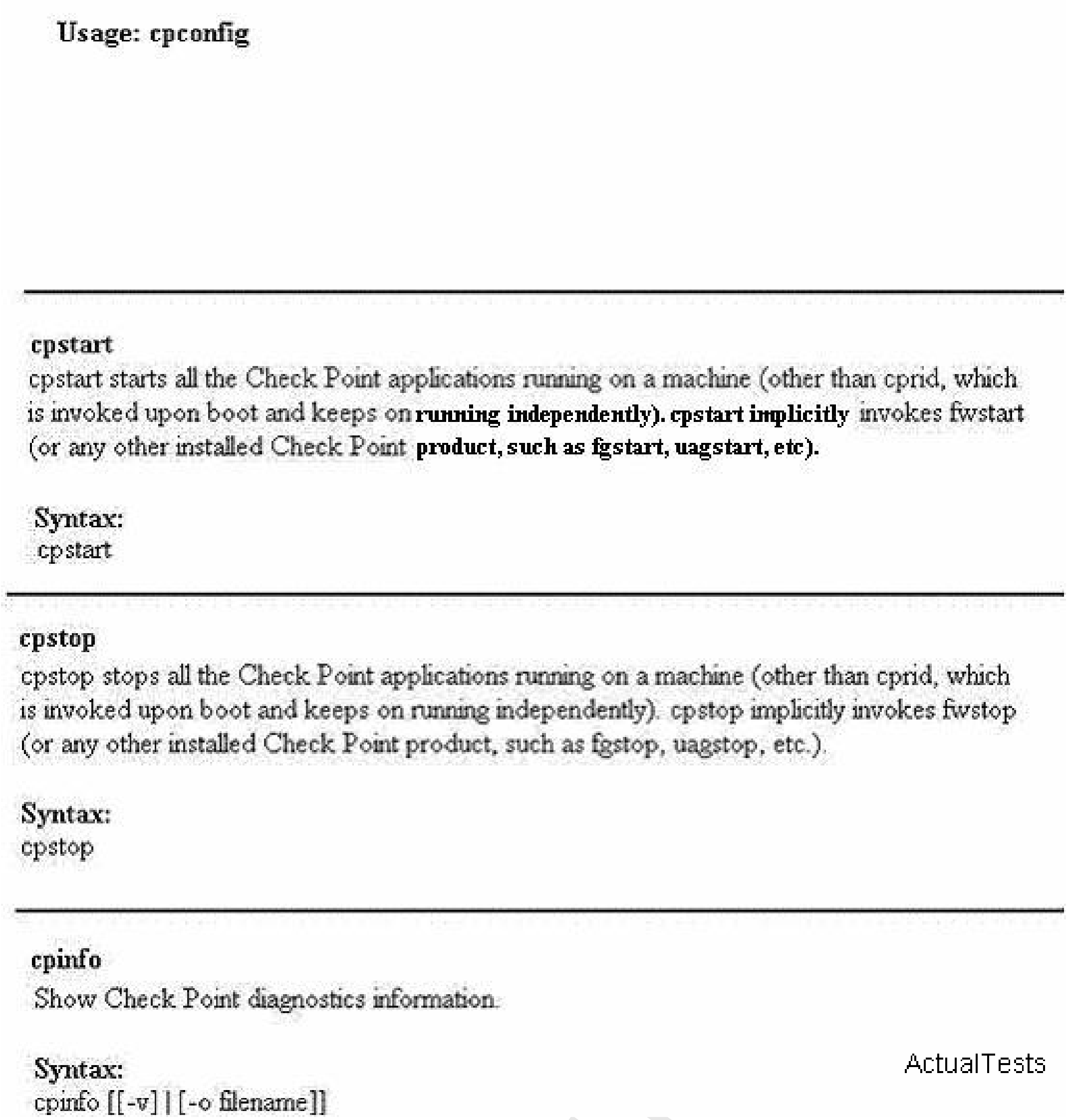


Check Point Commands

cpconfig

Description Run a command line version of the Check Point Configuration Tool. This tool is used to configure an installed Check Point product. The options shown depend on the installed configuration and products. Amongst others, these options include:

- Licenses and contracts - Modify the necessary Check Point licenses and contracts.
- Administrator - Modify the administrator authorized to connect to the Security Management server.
- GUI Clients - Modify the list of SmartConsole Client machines from which the administrators are authorized to connect to a Security Management server
- SNMP Extension - **Configure the SNMP daemon.** The SNMP daemon enables SecurePlatform to export its status to external network management tools.
- PKCS #11 Token - Register a cryptographic token, for use by SecurePlatform; see details of the token, and test its functionality.
- Random Pool - Configure the RSA keys, to be used by SecurePlatform.
- Certificate Authority - Install the Certificate Authority on the Security Management server in a first-time installation
- Secure Internal Communication - Set up trust between the gateway on which this command is being run and the Security Management server
- Certificate's Fingerprint - Display the fingerprint which will be used on first-time launch to verify the identity of the Security Management server being accessed by the SmartConsole. This fingerprint is a text string derived from the Security Management server's certificate.
- Automatic Start of Check Point Products - Specify whether Check Point Security Gateways will start automatically at boot time



Usage: cpconfig

cpstart

cpstart starts all the Check Point applications running on a machine (other than cprid, which is invoked upon boot and keeps on **running independently). cpstart implicitly** invokes fwstart (or any other installed Check Point **product, such as fgstart, uagstart, etc).**

Syntax:

cpstart

cpstop

cpstop stops all the Check Point applications running on a machine (other than cprid, which is invoked upon boot and keeps on running independently). cpstop implicitly invokes fwstop (or any other installed Check Point product, such as fgstop, uagstop, etc.).

Syntax:

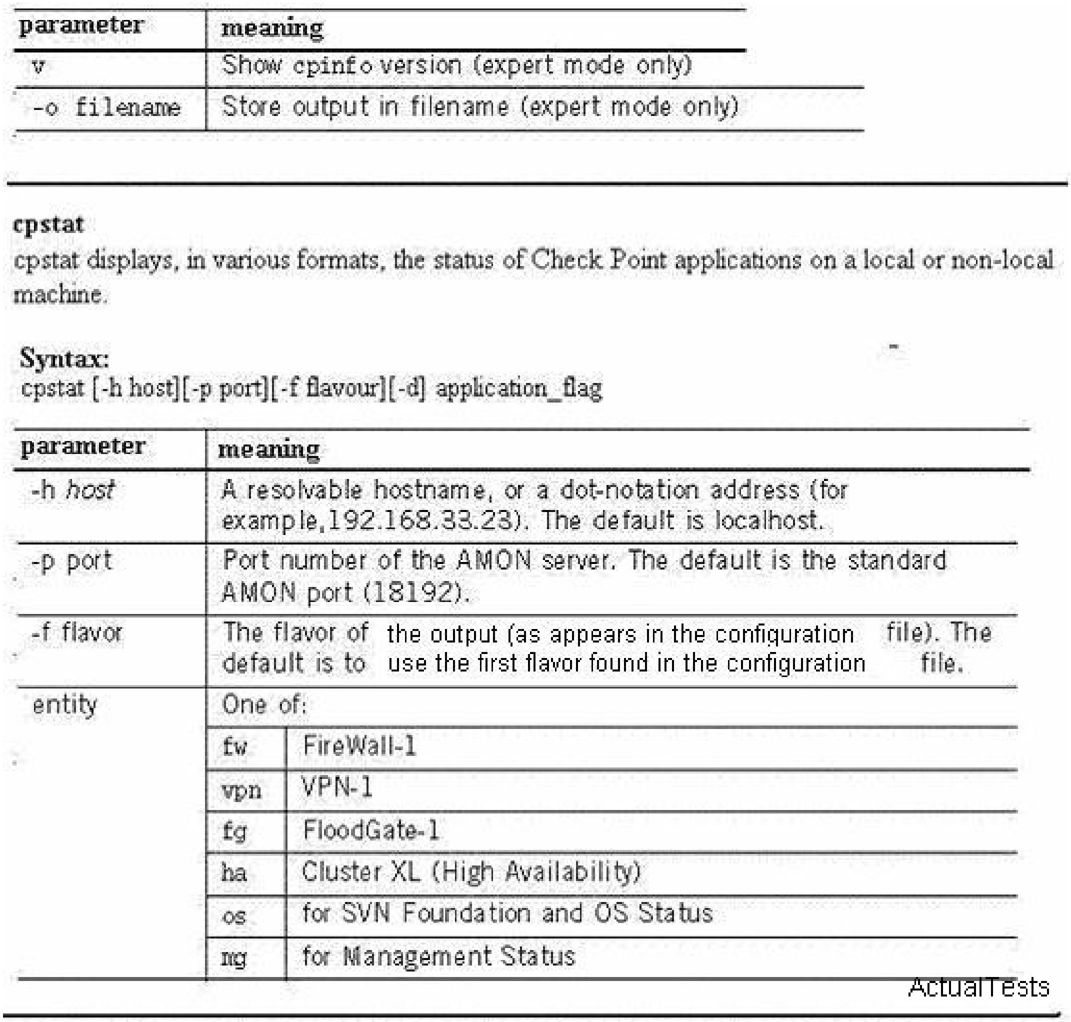
cpstop

cpinfo

Show Check Point diagnostics information.

Syntax:

cpinfo [[-v] | [-o filename]]



parameter	meaning
v	Show cpinfo version (expert mode only)
-o filename	Store output in filename (expert mode only)

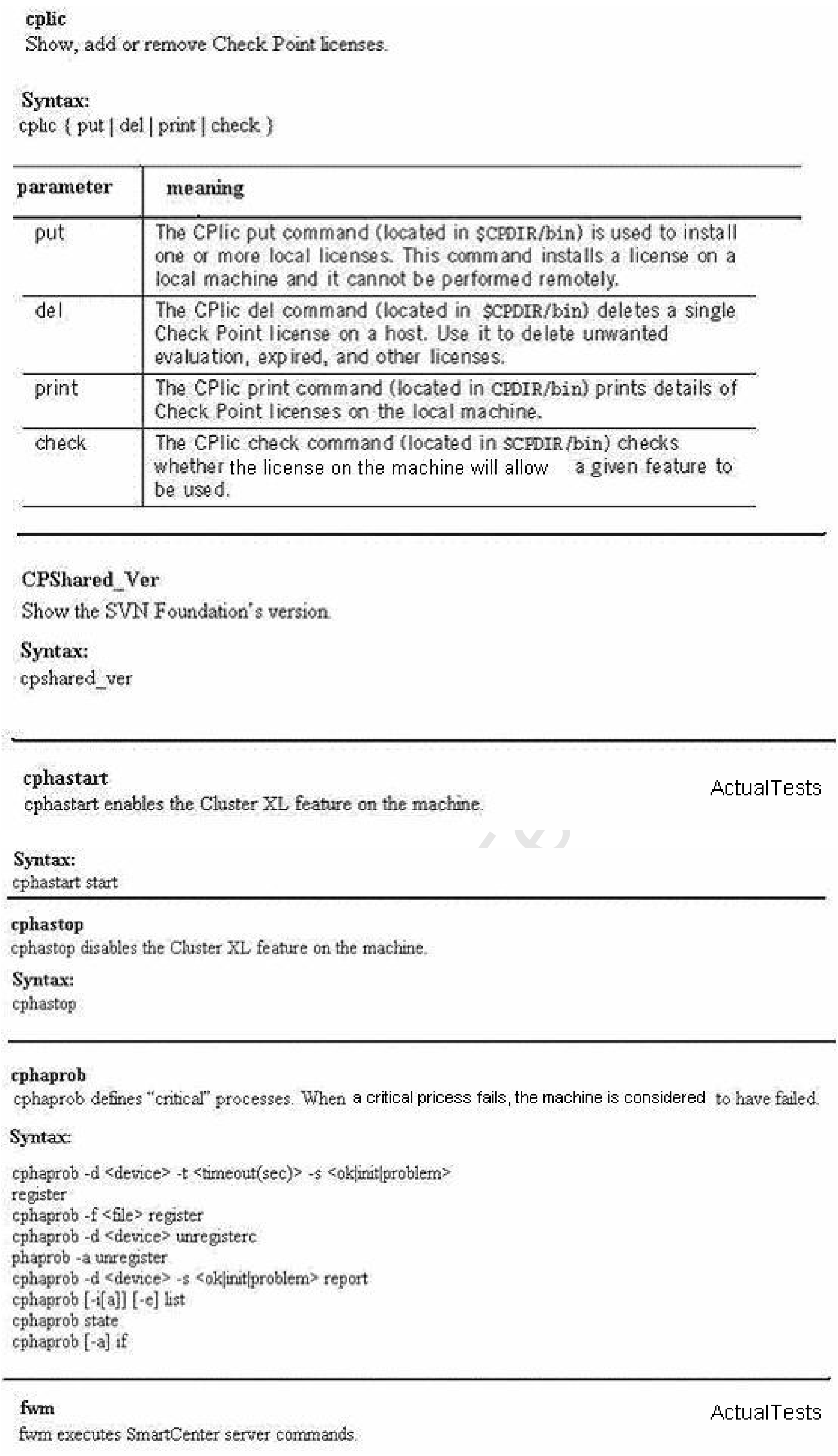
cpstat

cpstat displays, in various formats, the status of Check Point applications on a local or non-local machine.

Syntax:

cpstat [-h host][-p port][-f flavour][-d] application_flag

parameter	meaning	
-h *host*	A resolvable hostname, or a dot-notation address (for example,192.168.33.23). The default is localhost.	
-p port	Port number of the AMON server. The default is the standard AMON port (18192).	
-f flavor	The flavor of the output (as appears in the configuration file). The default is to use the first flavor found in the configuration file.	
entity	One of:	
	fw	FireWall-1
	vpn	VPN-1
	fg	FloodGate-1
	ha	Cluster XL (High Availability)
	os	for SVN Foundation and OS Status
	mg	for Management Status



cplic

Show, add or remove Check Point licenses.

Syntax:

cplic { put | del | print | check }

parameter	meaning
put	The CPlic put command (located in $CPDIR/bin) is used to install one or more local licenses. This command installs a license on a local machine and it cannot be performed remotely.
del	The CPlic del command (located in $CPDIR/bin) deletes a single Check Point license on a host. Use it to delete unwanted evaluation, expired, and other licenses.
print	The CPlic print command (located in CPDIR/bin) prints details of Check Point licenses on the local machine.
check	The CPlic check command (located in $CPDIR/bin) checks whether the license on the machine will allow a given feature to be used.

CPShared_Ver

Show the SVN Foundation's version.

Syntax:

cpshared_ver

cphastart

cphastart enables the Cluster XL feature on the machine.

Syntax:

cphastart start

cphastop

cphastop disables the Cluster XL feature on the machine.

Syntax:

cphastop

cphaprob

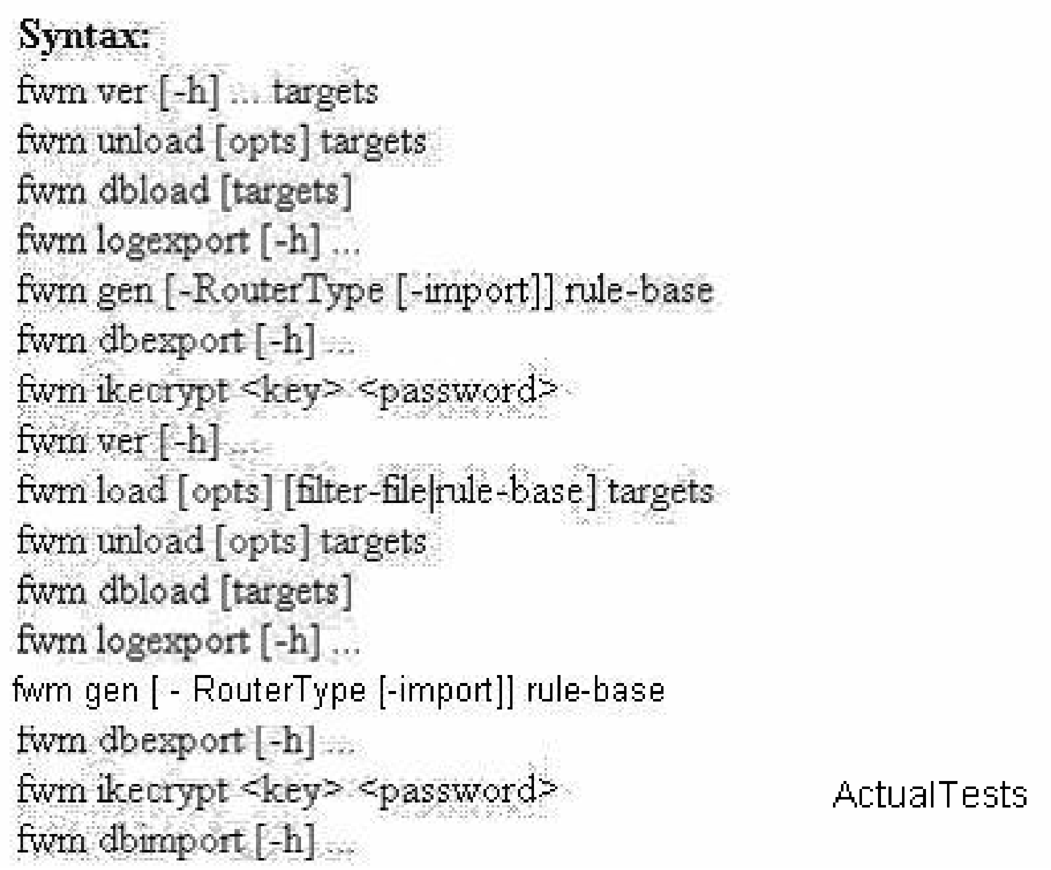
cphaprob defines "critical" processes. When a critical pricess fails, the machine is considered to have failed.

Syntax:

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem>
register
cphaprob -f <file> register
cphaprob -d <device> unregisterc
phaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

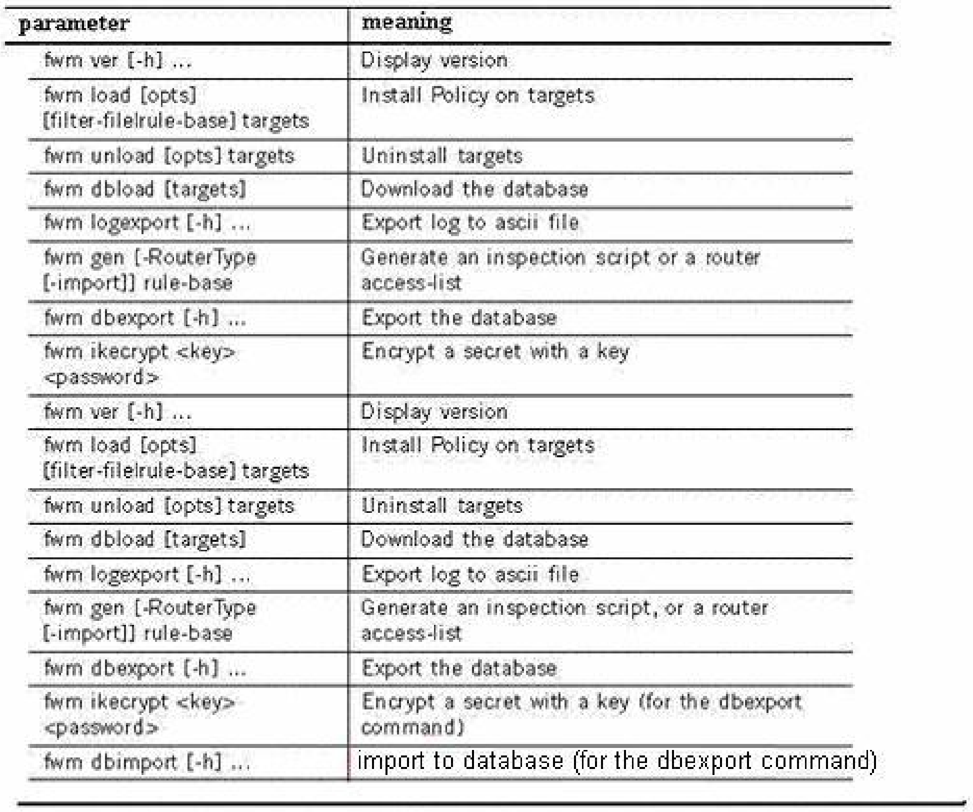
fwm

fwm executes SmartCenter server commands.

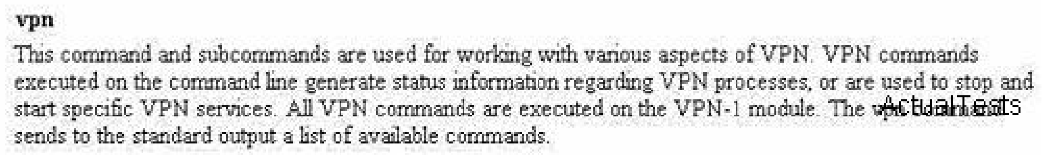


Syntax:

```
fwm ver [-h] ... targets
fwm unload [opts] targets
fwm dbload [targets]
fwm logexport [-h] ...
fwm gen [-RouterType [-import]] rule-base
fwm dbexport [-h] ...
fwm ikecrypt <key> <password>
fwm ver [-h] ...
fwm load [opts] [filter-file|rule-base] targets
fwm unload [opts] targets
fwm dbload [targets]
fwm logexport [-h] ...
fwm gen [ - RouterType [-import]] rule-base
fwm dbexport [-h] ...
fwm ikecrypt <key> <password>
fwm dbimport [-h] ...
```

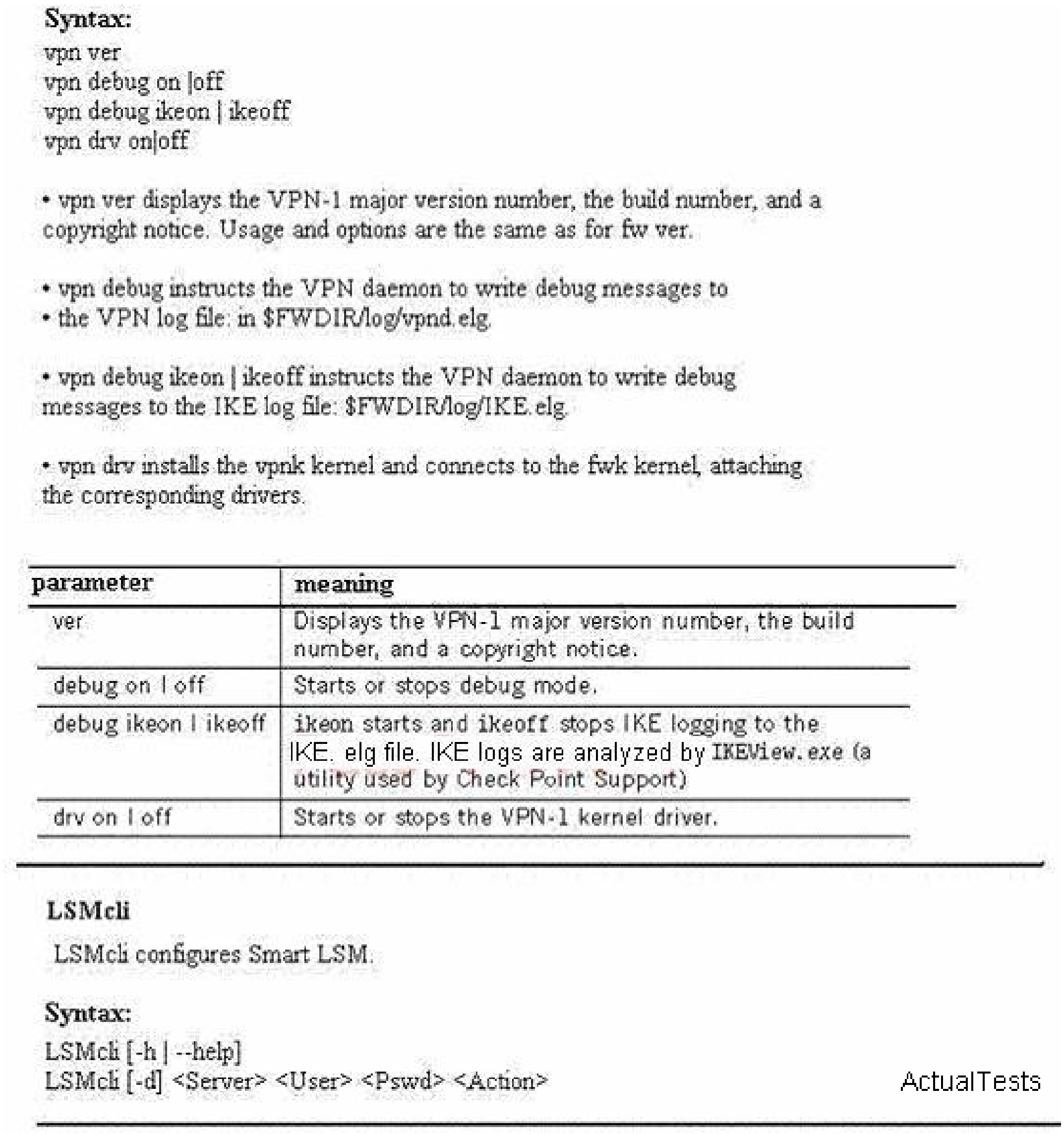


parameter	meaning
fwm ver [-h] ...	Display version
fwm load [opts] [filter-filelrule-base] targets	Install Policy on targets
fwm unload [opts] targets	Uninstall targets
fwm dbload [targets]	Download the database
fwm logexport [-h] ...	Export log to ascii file
fwm gen [-RouterType [-import]] rule-base	Generate an inspection script or a router access-list
fwm dbexport [-h] ...	Export the database
fwm ikecrypt <key> <password>	Encrypt a secret with a key
fwm ver [-h] ...	Display version
fwm load [opts] [filter-filelrule-base] targets	Install Policy on targets
fwm unload [opts] targets	Uninstall targets
fwm dbload [targets]	Download the database
fwm logexport [-h] ...	Export log to ascii file
fwm gen [-RouterType [-import]] rule-base	Generate an inspection script, or a router access-list
fwm dbexport [-h] ...	Export the database
fwm ikecrypt <key> <password>	Encrypt a secret with a key (for the dbexport command)
fwm dbimport [-h] ...	import to database (for the dbexport command)



vpn

This command and subcommands are used for working with various aspects of VPN. VPN commands executed on the command line generate status information regarding VPN processes, or are used to stop and start specific VPN services. All VPN commands are executed on the VPN-1 module. The vpn command sends to the standard output a list of available commands.



Syntax:

```
vpn ver
vpn debug on |off
vpn debug ikeon | ikeoff
vpn drv on|off
```

• vpn ver displays the VPN-1 major version number, the build number, and a copyright notice. Usage and options are the same as for fw ver.

• vpn debug instructs the VPN daemon to write debug messages to

• the VPN log file: in $FWDIR/log/vpnd.elg.

• vpn debug ikeon | ikeoff instructs the VPN daemon to write debug messages to the IKE log file: $FWDIR/log/IKE.elg.

• vpn drv installs the vpnk kernel and connects to the fwk kernel, attaching the corresponding drivers.

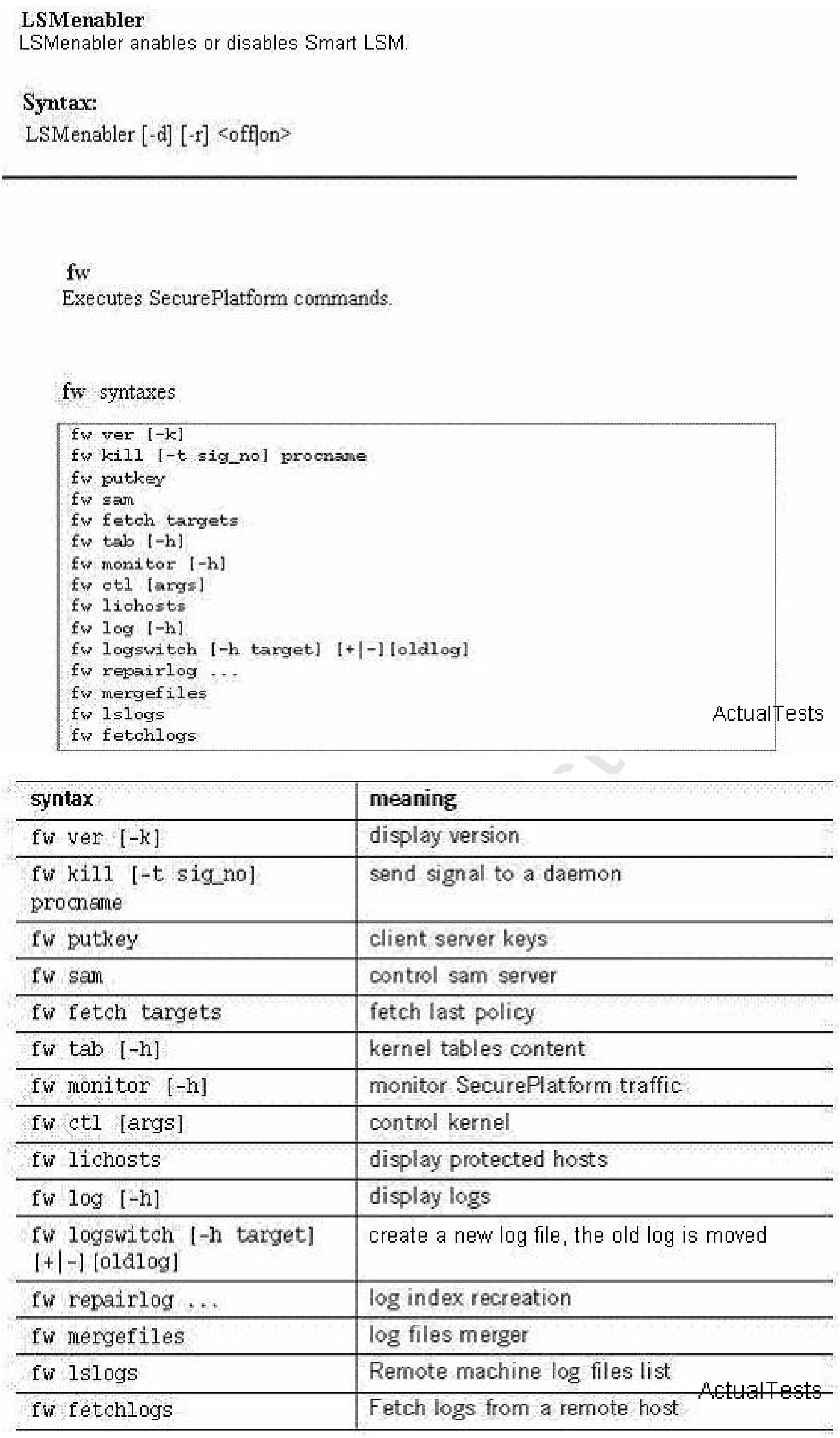
parameter	meaning
ver	Displays the VPN-1 major version number, the build number, and a copyright notice.
debug on I off	Starts or stops debug mode.
debug ikeon I ikeoff	ikeon starts and ikeoff stops IKE logging to the IKE. elg file. IKE logs are analyzed by IKEView.exe (a utility used by Check Point Support)
drv on I off	Starts or stops the VPN-1 kernel driver.

LSMcli

LSMcli configures Smart LSM.

Syntax:

```
LSMcli [-h | --help]
LSMcli [-d] <Server> <User> <Pswd> <Action>
```



LSMenabler

LSMenabler anables or disables Smart LSM.

Syntax:

LSMenabler [-d] [-r] <off|on>

fw

Executes SecurePlatform commands.

fw syntaxes

```
fw ver [-k]
fw kill [-t sig_no] procname
fw putkey
fw sam
fw fetch targets
fw tab [-h]
fw monitor [-h]
fw ctl [args]
fw lichosts
fw log [-h]
fw logswitch [-h target] [+|-][oldlog]
fw repairlog ...
fw mergefiles
fw lslogs
fw fetchlogs
```

syntax	meaning
fw ver [-k]	display version
fw kill [-t sig_no] procname	send signal to a daemon
fw putkey	client server keys
fw sam	control sam server
fw fetch targets	fetch last policy
fw tab [-h]	kernel tables content
fw monitor [-h]	monitor SecurePlatform traffic
fw ctl [args]	control kernel
fw lichosts	display protected hosts
fw log [-h]	display logs
fw logswitch [-h target] [+|-] [oldlog]	create a new log file, the old log is moved
fw repairlog ...	log index recreation
fw mergefiles	log files merger
fw lslogs	Remote machine log files list
fw fetchlogs	Fetch logs from a remote host

A. ifconfig

B. config tool

C. cpconfig

D. ipconfig
E. configure tool

Answer: C

QUESTION NO: 296

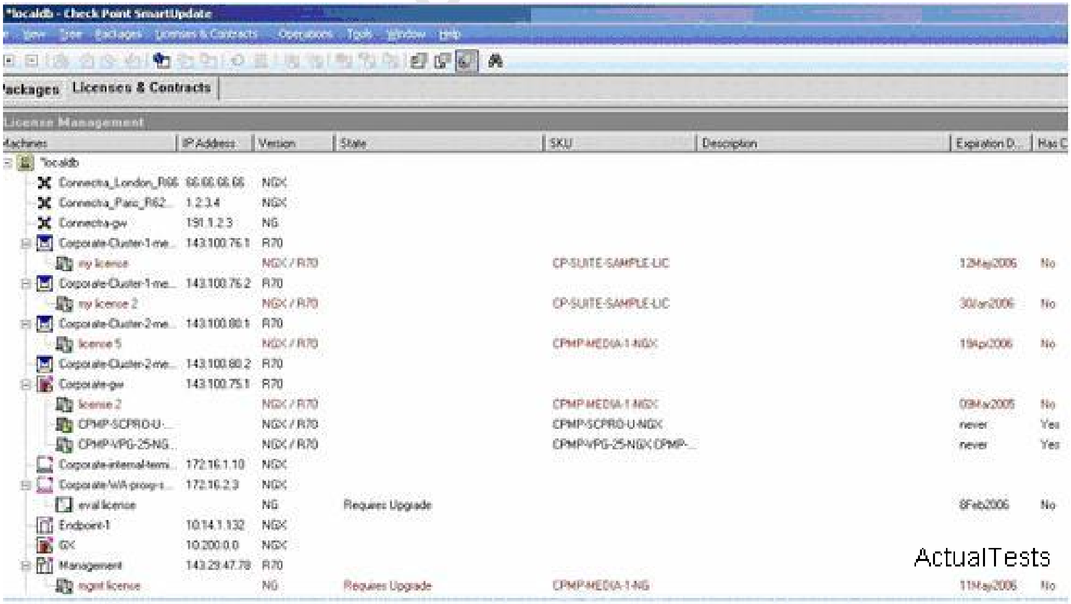
You are in SmartView Tracker GUI and you want to create a Network Object of the type fw.boson.com. How would you achieve this with minimal effort (without having to shut down SmartView Tracker GUI)?

A. You will have to shut down SmartView Tracker GUI, and launch SmartView Status, then select Manage menu. From Manage menu you will select Network objects.
B. You will have to shut down SmartView Tracker GUI, and launchSmartDashboard , then select Manage menu. From Manage menu you will select Network objects.
C. From SmartView Tracker GUI you will choose Policy Menu and select SmartDashboard. In SmartDashboard GUI, you will choose Manage menu and the select Network Objects
D. From SmartView Tracker GUI you will choose File Menu and select SmartDashboard. In SmartDashboard GUI, you will choose Manage menu and then select Network Objects
E. From SmartView Tracker GUI you will choose Window Menu and select SmartDashboard. In SmartDashboard GUI, you will choose Manage menu and then select Network Objects

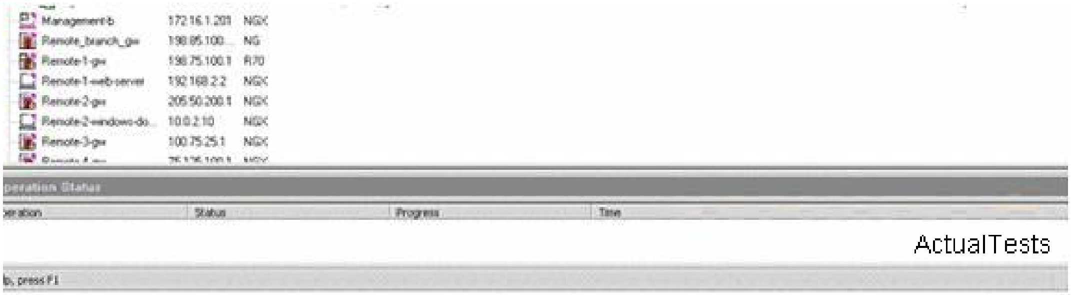
Answer: E

QUESTION NO: 297

Once you have successfully upgraded Security Management server, what tool will you use to manage your contracts?



Machines	IP Address	Version	State	SKU	Description	Expiration D...	Has C
*localdb							
Connecticut_London_R66	66.66.66.66	NGX					
Connecticut_Paris_R62...	1.2.3.4	NGX					
Connecticut-gw	191.1.2.3	NG					
Corporate-Cluster-1-me...	143.100.76.1	R70					
my licence		NGX / R70		CP-SUITE-SAMPLE-LIC		12May2006	No
Corporate-Cluster-1-me...	143.100.76.2	R70					
my licence 2		NGX / R70		CP-SUITE-SAMPLE-LIC		30Jan2006	No
Corporate-Cluster-2-me...	143.100.80.1	R70					
licence 5		NGX / R70		CPMP-MEDIA-1-NGX		19Apr2006	No
Corporate-Cluster-2-me...	143.100.80.2	R70					
Corporate-gw	143.100.75.1	R70					
licence 2		NGX / R70		CPMP-MEDIA-1-NGX		09Mar2005	No
CPMP-SCPRO-U-...		NGX / R70		CPMP-SCPRO-U-NGX		never	Yes
CPMP-VPG-25-NG...		NGX / R70		CPMP-VPG-25-NGX CPMP-...		never	Yes
Corporate-internal-termi...	172.16.1.10	NGX					
Corporate-WA-proxy-s...	172.16.2.3	NGX					
eval licence		NG	Requires Upgrade			8Feb2006	No
Endpoint-1	10.14.1.132	NGX					
GX	10.200.0.0	NGX					
Management	143.29.47.78	R70					
mgmt licence		NG	Requires Upgrade	CPMP-MEDIA-1-NG		11May2006	No



```
Management-b             172.16.1.201   NGX
Remote_branch_gw         198.85.100...  NG
Remote-1-gw              198.75.100.1   R70
Remote-1-web-server      192.168.2.2    NGX
Remote-2-gw              205.50.200.1   NGX
Remote-2-windows-do...   10.0.2.10      NGX
Remote-3-gw              100.75.25.1    NGX
```

Figure 1: SmartUpdate

A. SmartView Monitor

B. SmartView Tracker

C. SmartUpdate

D. SmartDashboard

E. Eventia Reporter

Answer: C

QUESTION NO: 298

At what point does policy get downloaded from a policy server?

A. when the SecureClient machine boots up

B. when the security gateway initializes

C. when the SecureClient machine connects to Security Management server

D. when the Policy Server initializes

E. when the SecureClient machine connects to the site

Answer: E

QUESTION NO: 299

The log file for the Eventia Reporter server can be found in the in which location?

A. $RTDIR/log/log

B. $RTDIR/bin/Server.log

C. $RTDIR/log/SVRServer.log

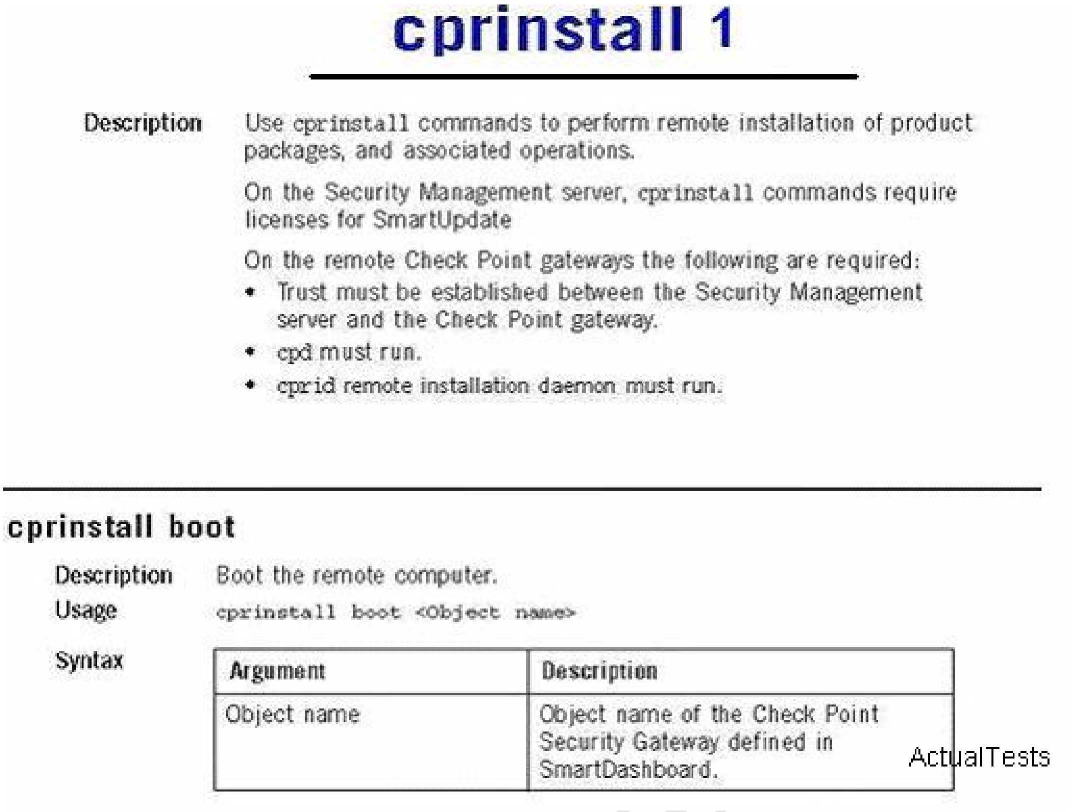
D. $RTDIR/log/vpn_route.conf

E. $RTDIR/util/adtlog

Answer: C

QUESTION NO: 300

The cprinstall install command is used to install Check Point products on remote modules. When running this command with the -boot option, then the:



cprinstall 1

Description Use `cprinstall` commands to perform remote installation of product packages, and associated operations.

On the Security Management server, `cprinstall` commands require licenses for SmartUpdate

On the remote Check Point gateways the following are required:

- Trust must be established between the Security Management server and the Check Point gateway.
- cpd must run.
- cprid remote installation daemon must run.

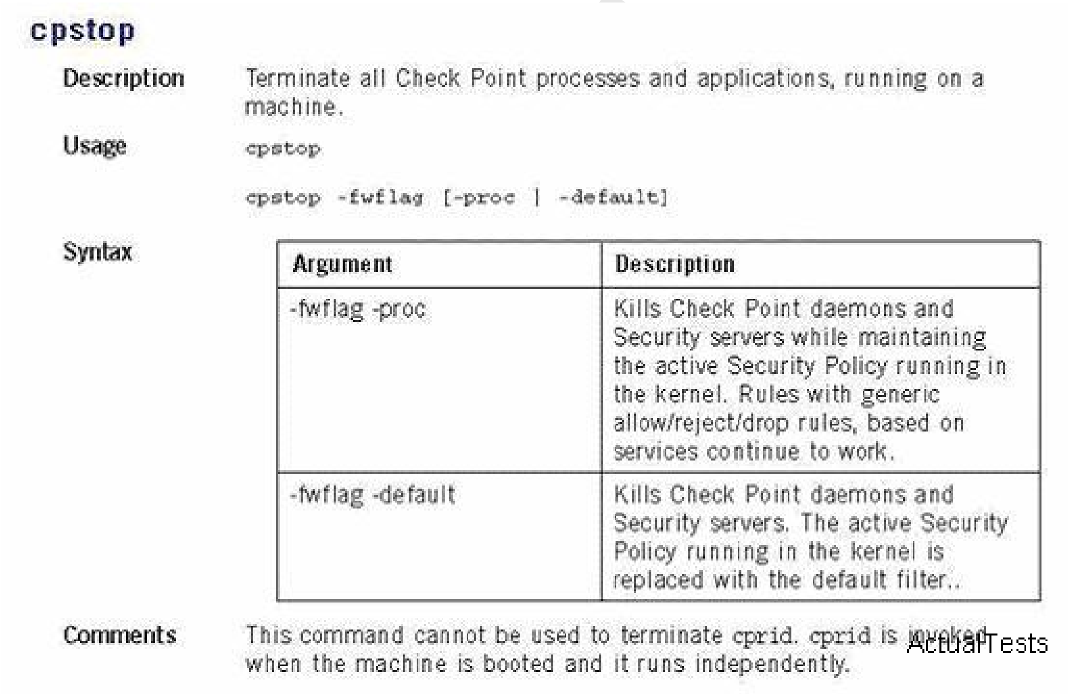
cprinstall boot

Description Boot the remote computer.

Usage `cprinstall boot <Object name>`

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.



cpstop

Description Terminate all Check Point processes and applications, running on a machine.

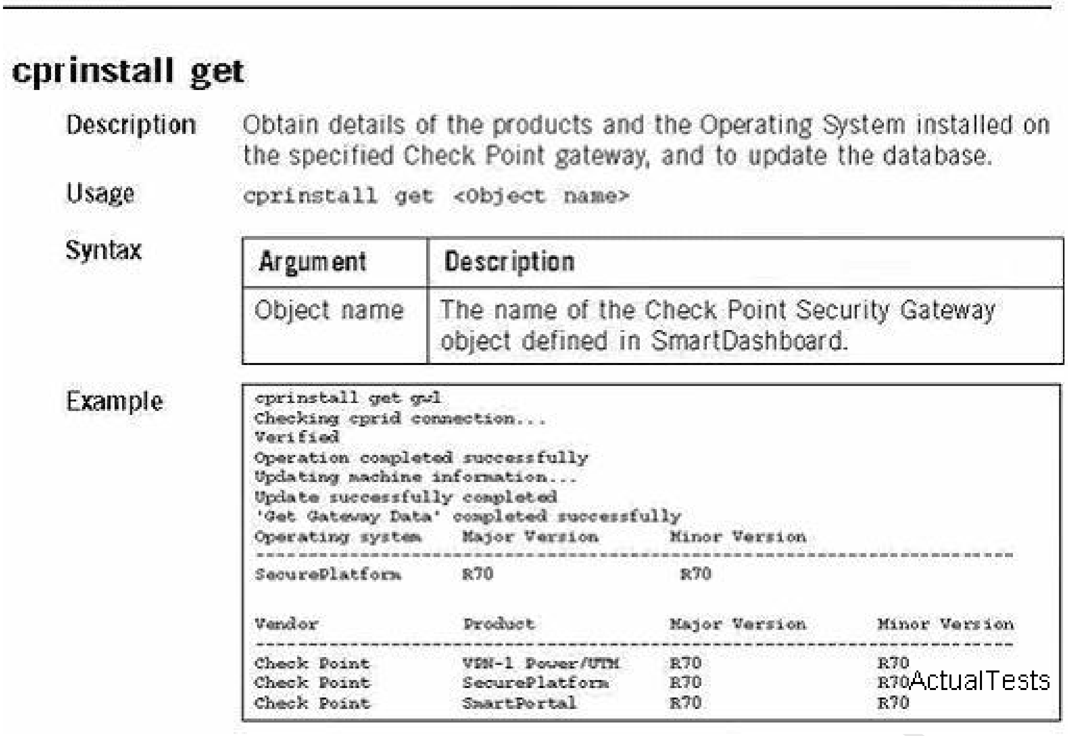
Usage

```
cpstop
cpstop -fwflag [-proc | -default]
```

Syntax

Argument	Description
-fwflag -proc	Kills Check Point daemons and Security servers while maintaining the active Security Policy running in the kernel. Rules with generic allow/reject/drop rules, based on services continue to work.
-fwflag -default	Kills Check Point daemons and Security servers. The active Security Policy running in the kernel is replaced with the default filter..

Comments This command cannot be used to terminate cprid. cprid is invoked when the machine is booted and it runs independently.



cprinstall get

Description Obtain details of the products and the Operating System installed on the specified Check Point gateway, and to update the database.

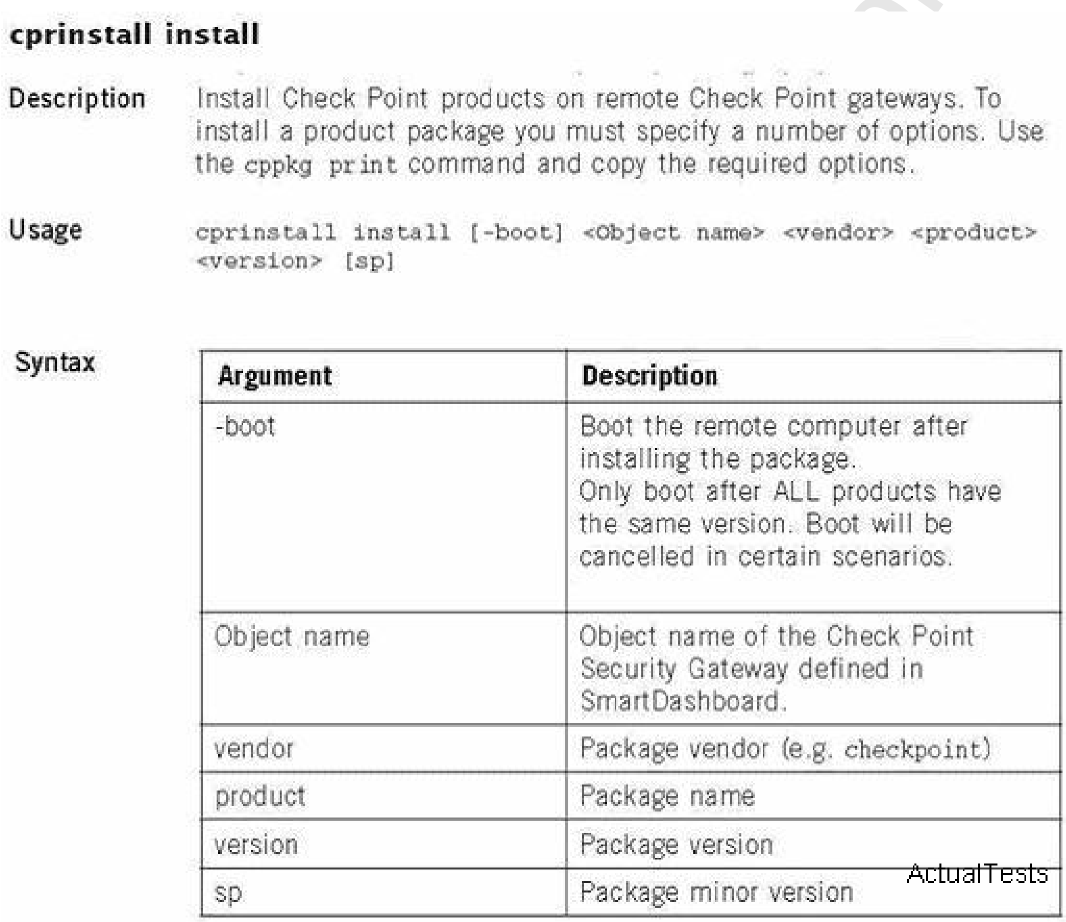
Usage `cprinstall get <Object name>`

Syntax

Argument	Description
Object name	The name of the Check Point Security Gateway object defined in SmartDashboard.

Example

```
cprinstall get gw1
Checking cprid connection...
Verified
Operation completed successfully
Updating machine information...
Update successfully completed
'Get Gateway Data' completed successfully
Operating system    Major Version          Minor Version
------------------------------------------------------------------------
SecurePlatform      R70                     R70


Vendor              Product                Major Version         Minor Version
------------------------------------------------------------------------
Check Point         VPN-1 Power/UTM        R70                   R70
Check Point         SecurePlatform         R70                   R70
Check Point         SmartPortal            R70                   R70
```



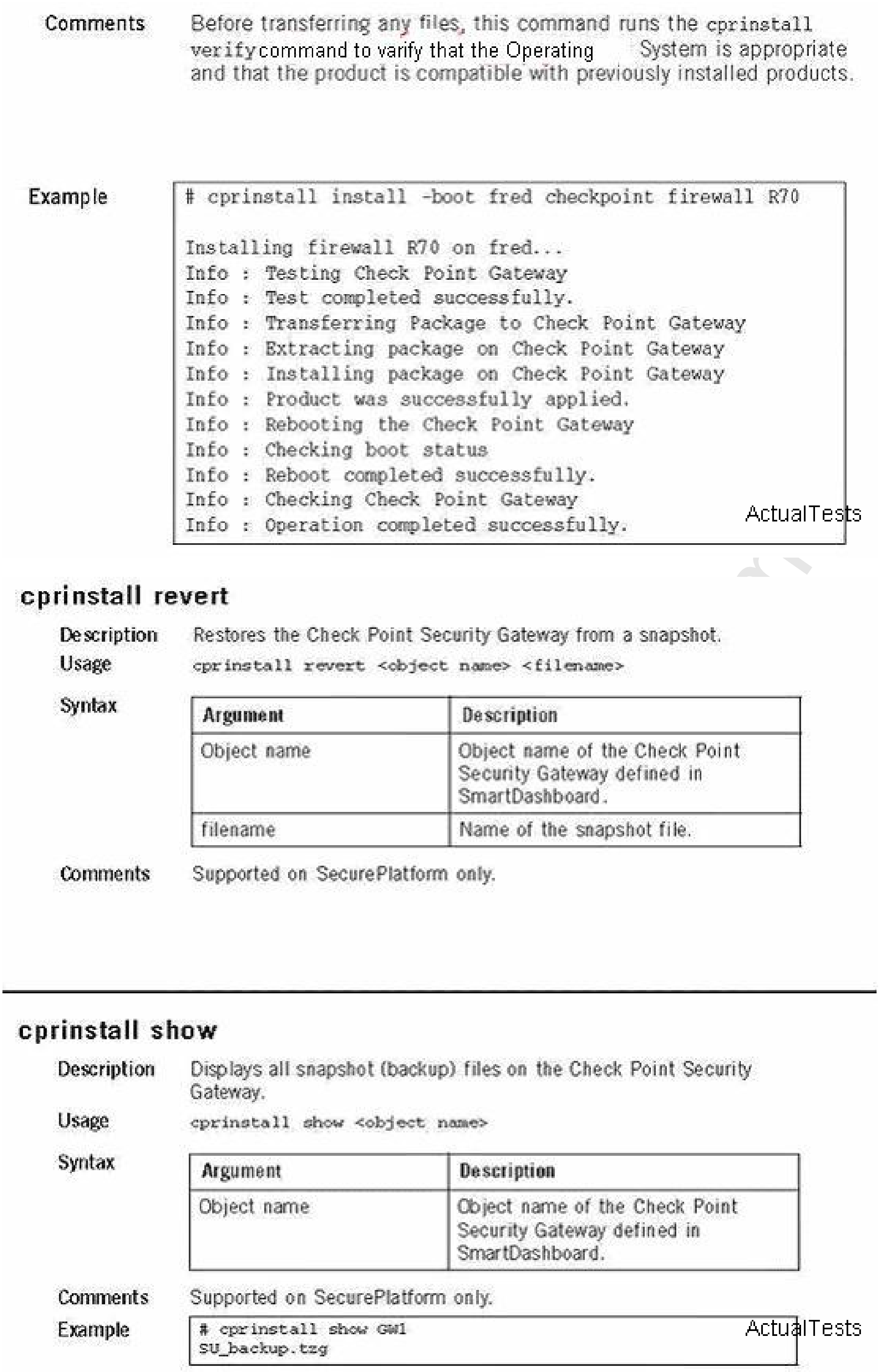
cprinstall install

Description Install Check Point products on remote Check Point gateways. To install a product package you must specify a number of options. Use the `cppkg print` command and copy the required options.

Usage `cprinstall install [-boot] <Object name> <vendor> <product> <version> [sp]`

Syntax

Argument	Description
-boot	Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios.
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint)
product	Package name
version	Package version
sp	Package minor version



Comments Before transferring any files, this command runs the `cprinstall verify` command to varify that the Operating System is appropriate and that the product is compatible with previously installed products.

Example

```
# cprinstall install -boot fred checkpoint firewall R70

Installing firewall R70 on fred...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
```

cprinstall revert

Description Restores the Check Point Security Gateway from a snapshot.

Usage `cprinstall revert <object name> <filename>`

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
filename	Name of the snapshot file.

Comments Supported on SecurePlatform only.

cprinstall show

Description Displays all snapshot (backup) files on the Check Point Security Gateway.

Usage `cprinstall show <object name>`

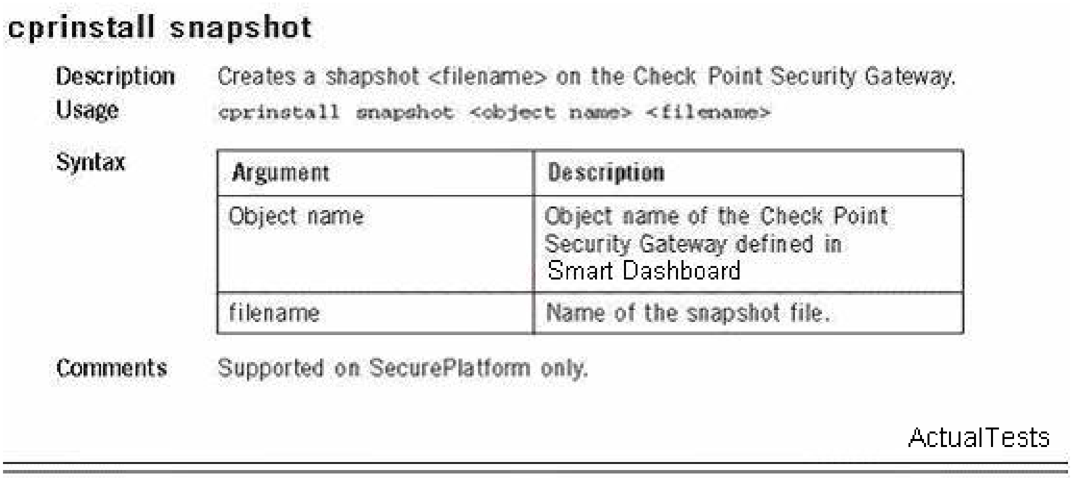
Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.

Comments Supported on SecurePlatform only.

Example

```
# cprinstall show GW1
SU_backup.tzg
```



cprinstall snapshot

Description Creates a shapshot <filename> on the Check Point Security Gateway.

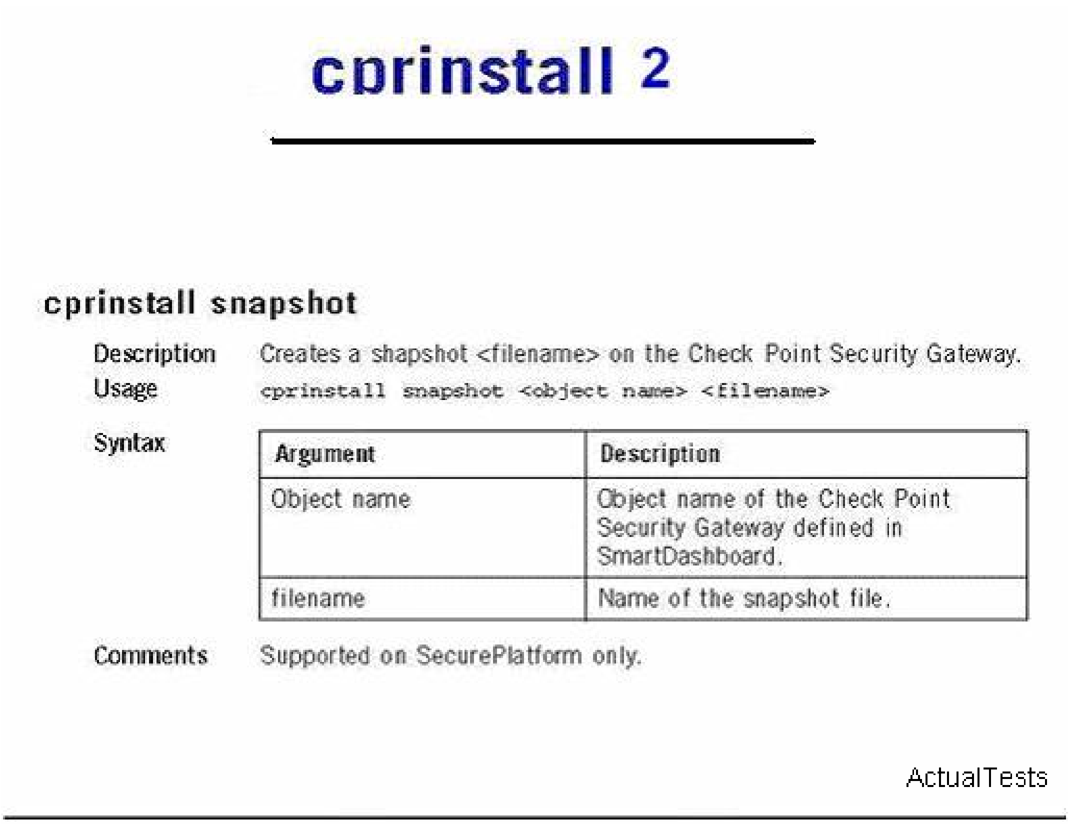
Usage

```
cprinstall snapshot <object name> <filename>
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in Smart Dashboard
filename	Name of the snapshot file.

Comments Supported on SecurePlatform only.



cprinstall 2

cprinstall snapshot

Description Creates a shapshot <filename> on the Check Point Security Gateway.

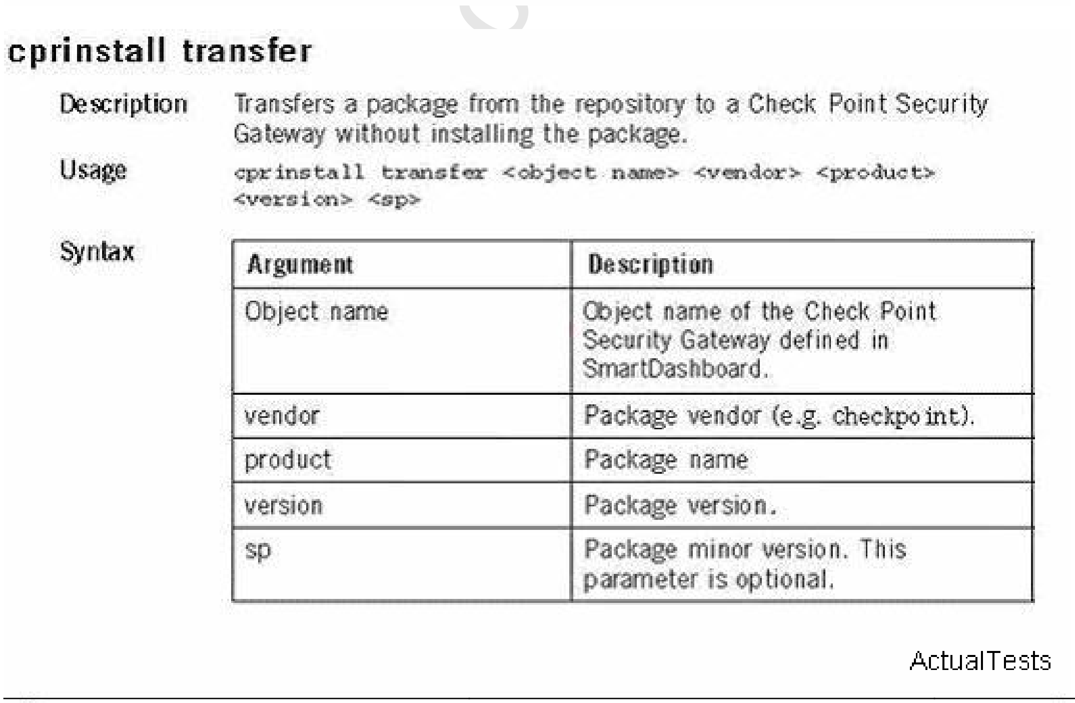
Usage

```
cprinstall snapshot <object name> <filename>
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
filename	Name of the snapshot file.

Comments Supported on SecurePlatform only.



cprinstall transfer

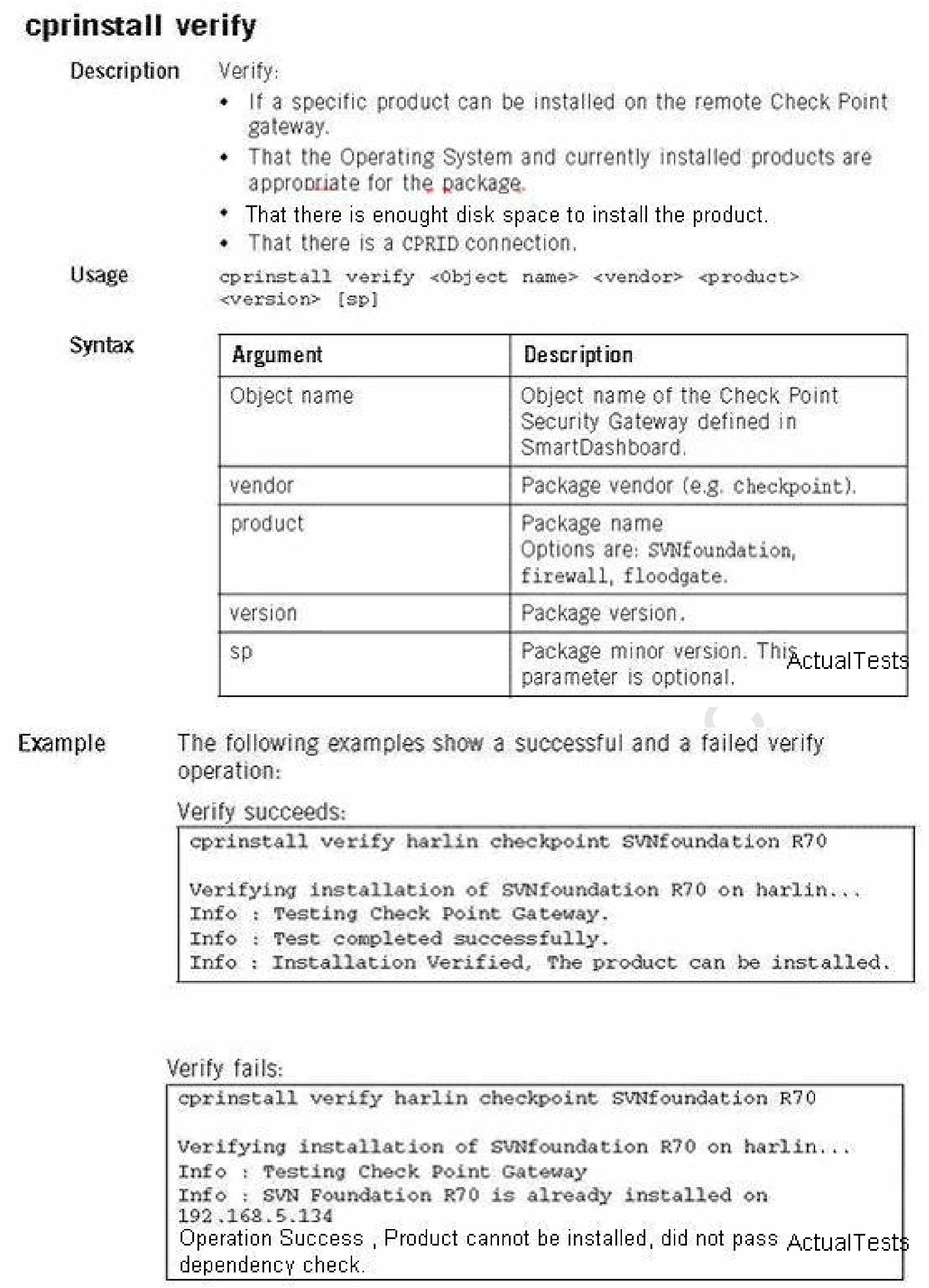
Description Transfers a package from the repository to a Check Point Security Gateway without installing the package.

Usage

```
cprinstall transfer <object name> <vendor> <product>
<version> <sp>
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint).
product	Package name
version	Package version.
sp	Package minor version. This parameter is optional.



cprinstall verify

Description

Verify:

- If a specific product can be installed on the remote Check Point gateway.
- That the Operating System and currently installed products are appropriate for the package.
- That there is enought disk space to install the product.
- That there is a CPRID connection.

Usage

```
cprinstall verify <Object name> <vendor> <product>
<version> [sp]
```

Syntax

Argument	Description
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. `checkpoint`).
product	Package name Options are: `SVNfoundation`, `firewall`, `floodgate`.
version	Package version.
sp	Package minor version. This parameter is optional.

Example

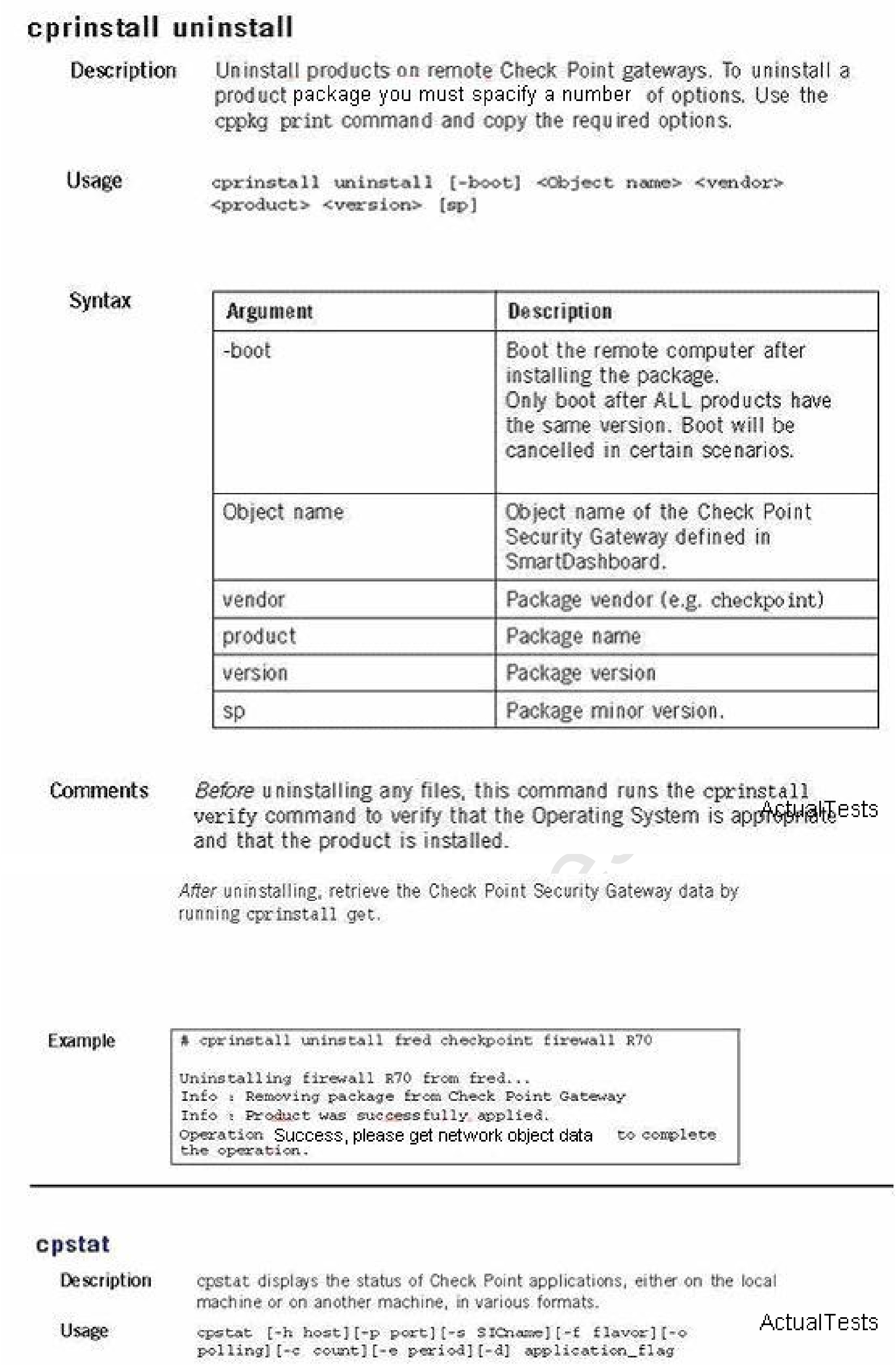
The following examples show a successful and a failed verify operation:

Verify succeeds:

```
cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
```

Verify fails:

```
cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info : Testing Check Point Gateway
Info : SVN Foundation R70 is already installed on
192.168.5.134
Operation Success , Product cannot be installed, did not pass
dependency check.
```



cprinstall uninstall

Description Uninstall products on remote Check Point gateways. To uninstall a product package you must spacify a number of options. Use the cppkg print command and copy the required options.

Usage

```
cprinstall uninstall [-boot] <Object name> <vendor>
<product> <version> [sp]
```

Syntax

Argument	Description
-boot	Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios.
Object name	Object name of the Check Point Security Gateway defined in SmartDashboard.
vendor	Package vendor (e.g. checkpoint)
product	Package name
version	Package version
sp	Package minor version.

Comments *Before* uninstalling any files, this command runs the cprinstall verify command to verify that the Operating System is appropriate and that the product is installed.

After uninstalling, retrieve the Check Point Security Gateway data by running cprinstall get.

Example

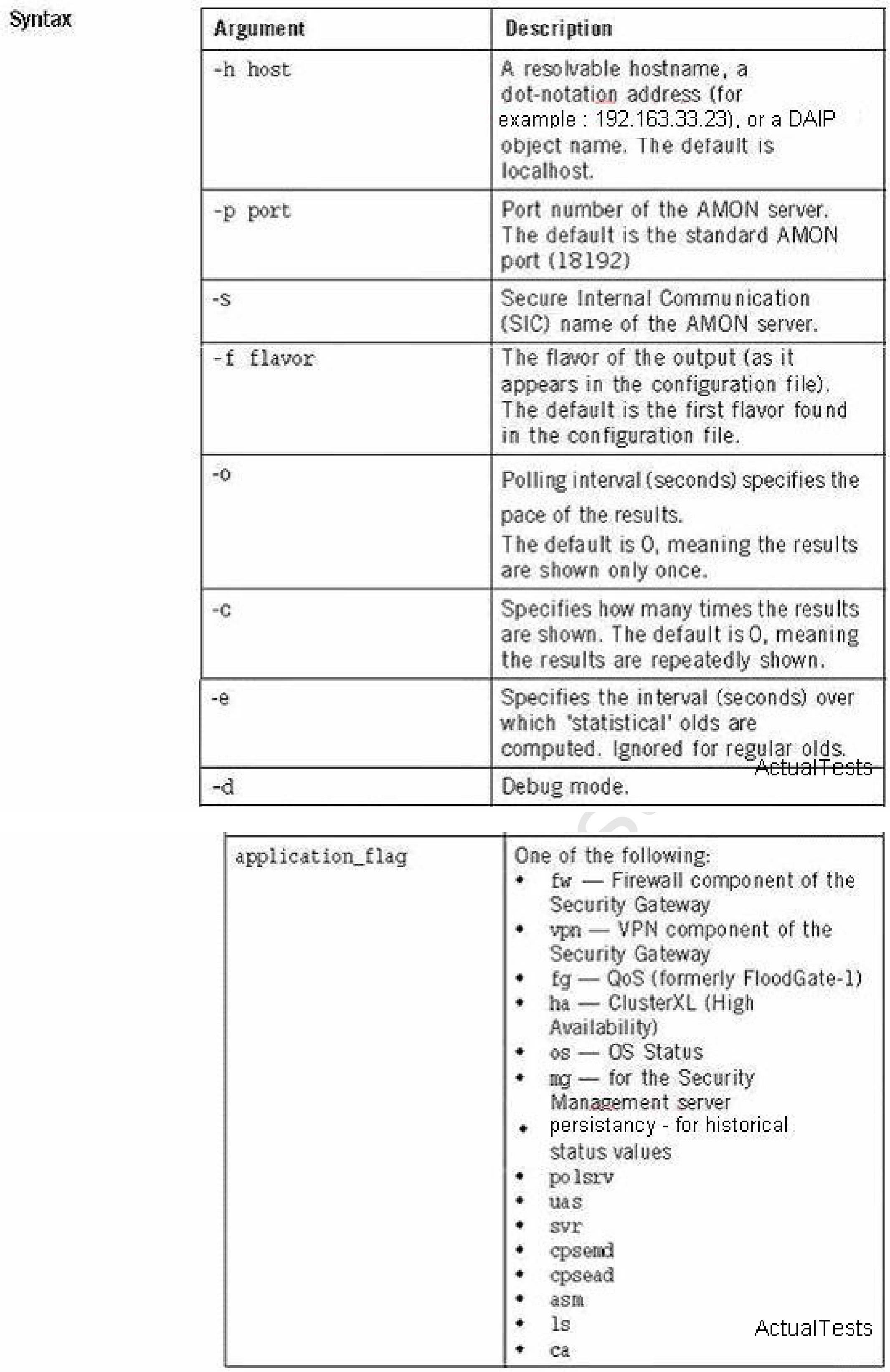
```
# cprinstall uninstall fred checkpoint firewall R70

Uninstalling firewall R70 from fred...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success, please get network object data  to complete
the operation.
```

cpstat

Description cpstat displays the status of Check Point applications, either on the local machine or on another machine, in various formats.

Usage

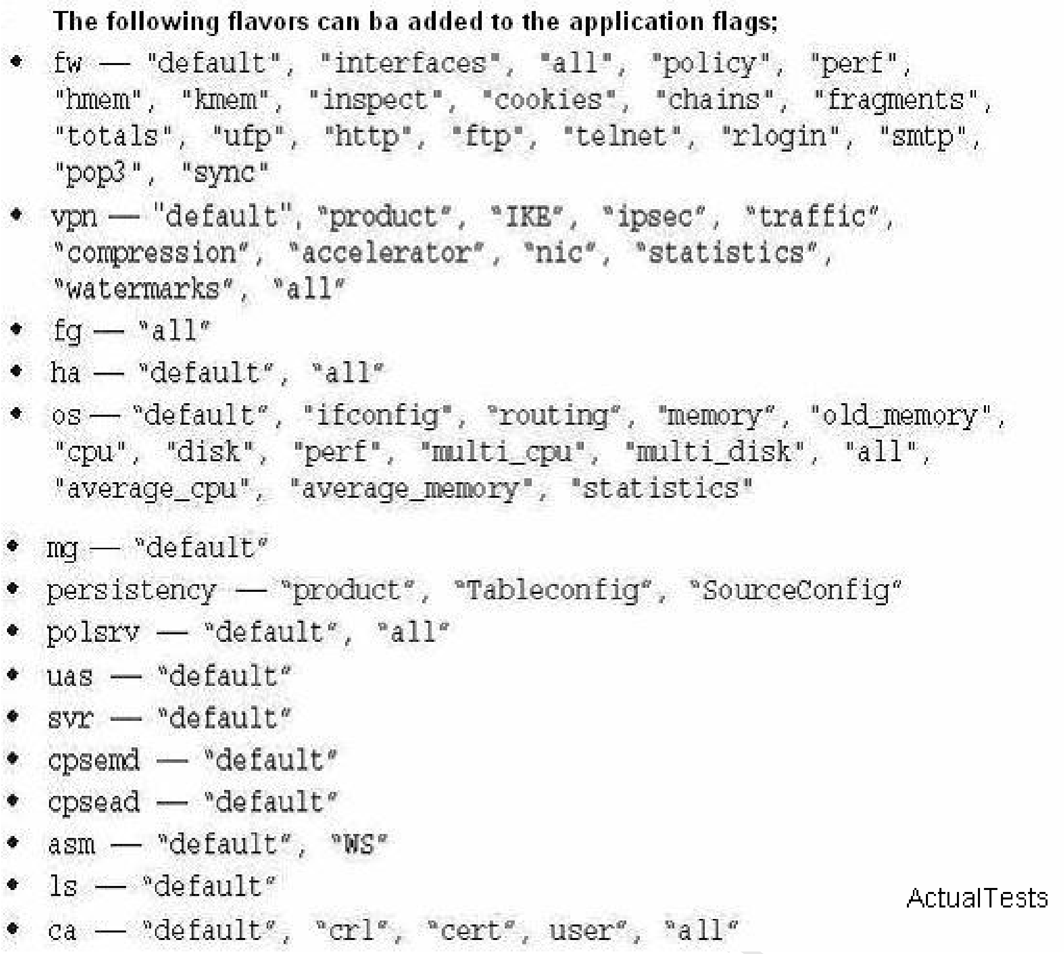
```
cpstat [-h host][-p port][-s SICname][-f flavor][-o
polling][-c count][-e period][-d] application_flag
```



Syntax

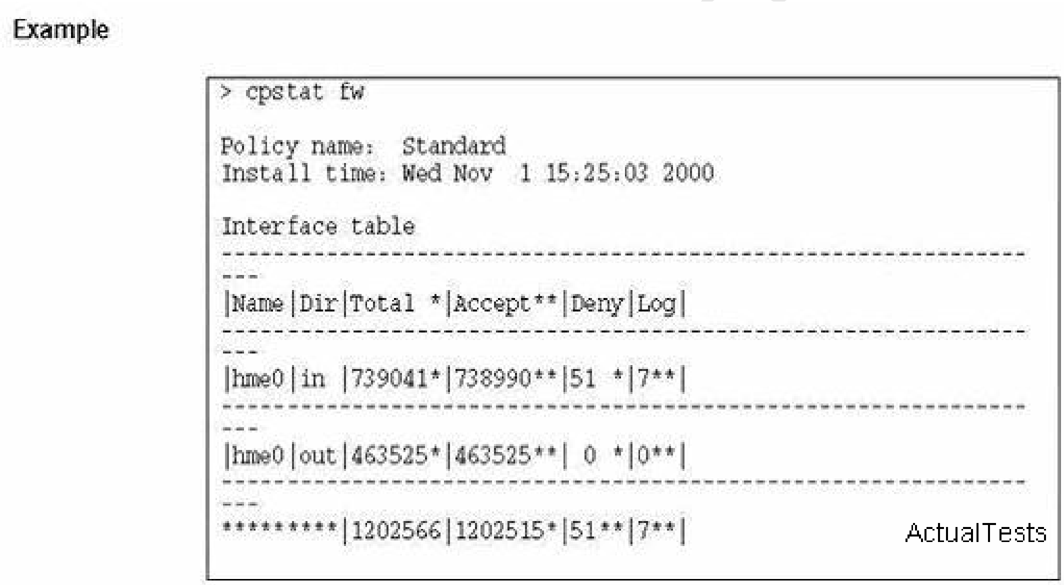
Argument	Description
-h host	A resolvable hostname, a dot-notation address (for example : 192.163.33.23), or a DAIP object name. The default is localhost.
-p port	Port number of the AMON server. The default is the standard AMON port (18192)
-s	Secure Internal Communication (SIC) name of the AMON server.
-f flavor	The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.
-o	Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.
-c	Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.
-e	Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds.
-d	Debug mode.

application_flag	One of the following: • fw — Firewall component of the Security Gateway • vpn — VPN component of the Security Gateway • fg — QoS (formerly FloodGate-1) • ha — ClusterXL (High Availability) • os — OS Status • mg — for the Security Management server • persistancy - for historical status values • polsrv • uas • svr • cpsemd • cpsead • asm • ls • ca



The following flavors can ba added to the application flags;

- fw — "default", "interfaces", "all", "policy", "perf", "hmem", "kmem", "inspect", "cookies", "chains", "fragments", "totals", "ufp", "http", "ftp", "telnet", "rlogin", "smtp", "pop3", "sync"
- vpn — "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- fg — "all"
- ha — "default", "all"
- os — "default", "ifconfig", "routing", "memory", "old_memory", "cpu", "disk", "perf", "multi_cpu", "multi_disk", "all", "average_cpu", "average_memory", "statistics"
- mg — "default"
- persistency — "product", "Tableconfig", "SourceConfig"
- polsrv — "default", "all"
- uas — "default"
- svr — "default"
- cpsemd — "default"
- cpsead — "default"
- asm — "default", "WS"
- ls — "default"
- ca — "default", "crl", "cert", user", "all"



Example

```
> cpstat fw

Policy name:  Standard
Install time: Wed Nov  1 15:25:03 2000

Interface table
--------------------------------------------------------------
---
|Name|Dir|Total *|Accept**|Deny|Log|
--------------------------------------------------------------
---
|hme0|in |739041*|738990**|51 *|7**|
--------------------------------------------------------------
---
|hme0|out|463525*|463525**| 0 *|0**|
--------------------------------------------------------------
---
*********|1202566|1202515*|51**|7**|
```

A. Remote computer will reboot before installing the package

B. Local computer will reboot before installing the package

C. Local computer will reboot after installing the package

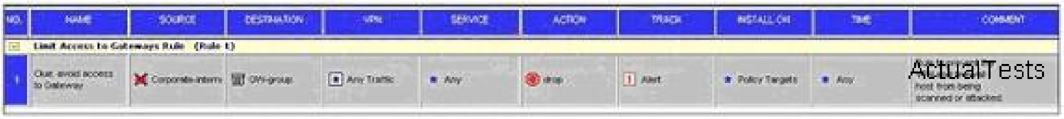
D. Remote computer will reboot during the installation of the package

E. Remote computer will reboot after installing the package

Answer: E

QUESTION NO: 301

Study the diagram and answer the question below. What rule is shown in the diagram?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Limit Access to Gateways Rule (Rule 1)										
1	Clue: avoid access to Gateway	Corporate-interns	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	[illegible] host from being scanned or attacked

A. NAT Rule

B. Cleanup Rule

C. Anti-Spoofing

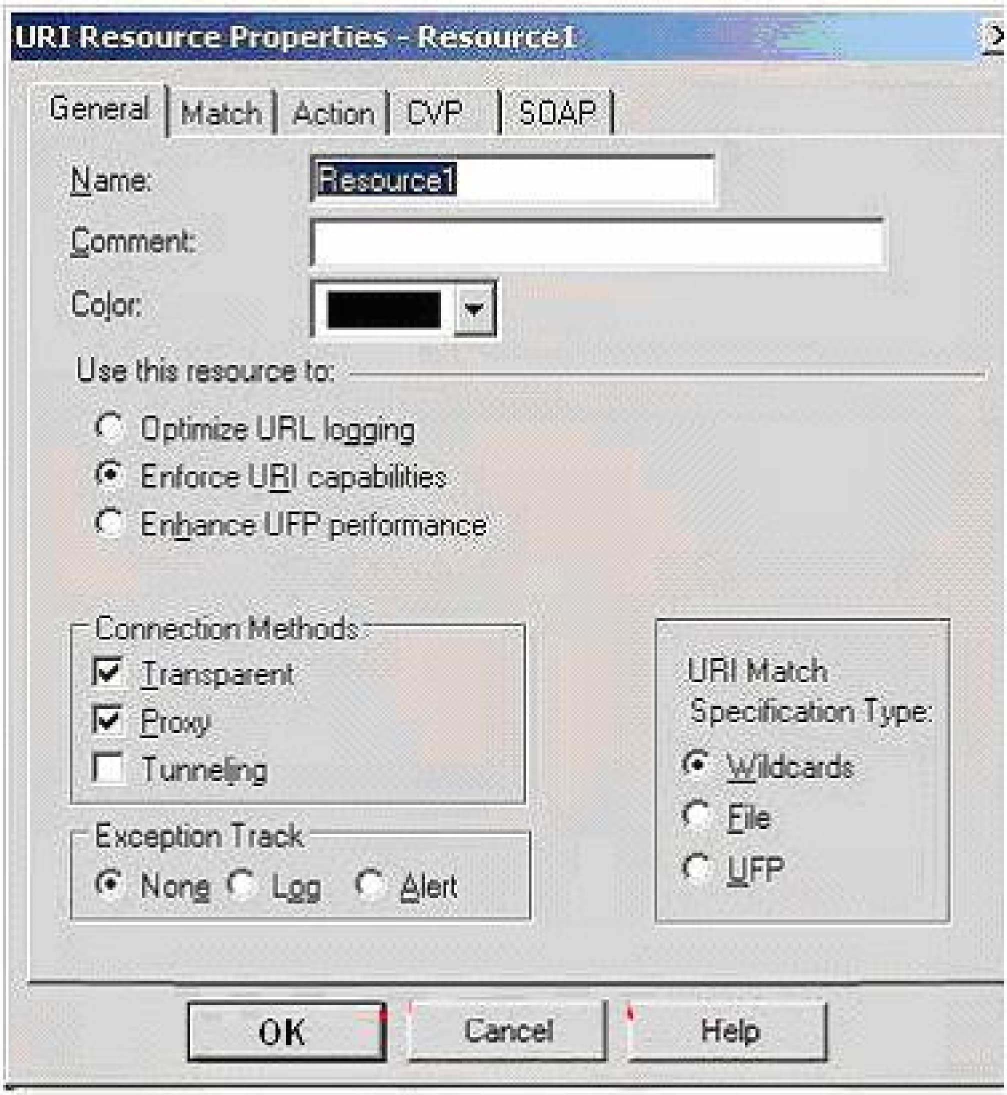
D. Stealth Rule

E. Default Rule

Answer: D

QUESTION NO: 302

From the answer options below, select all the URI Match Specification type you can choose from in the General tab of URI Resource Properties screen



URI Resource Properties - Resource1

Name: Resource1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging

● Enforce URI capabilities

○ Enhance UFP performance

Connection Methods

☑ Transparent

☑ Proxy

□ Tunneling

Exception Track

● None ○ Log ○ Alert

URI Match Specification Type:

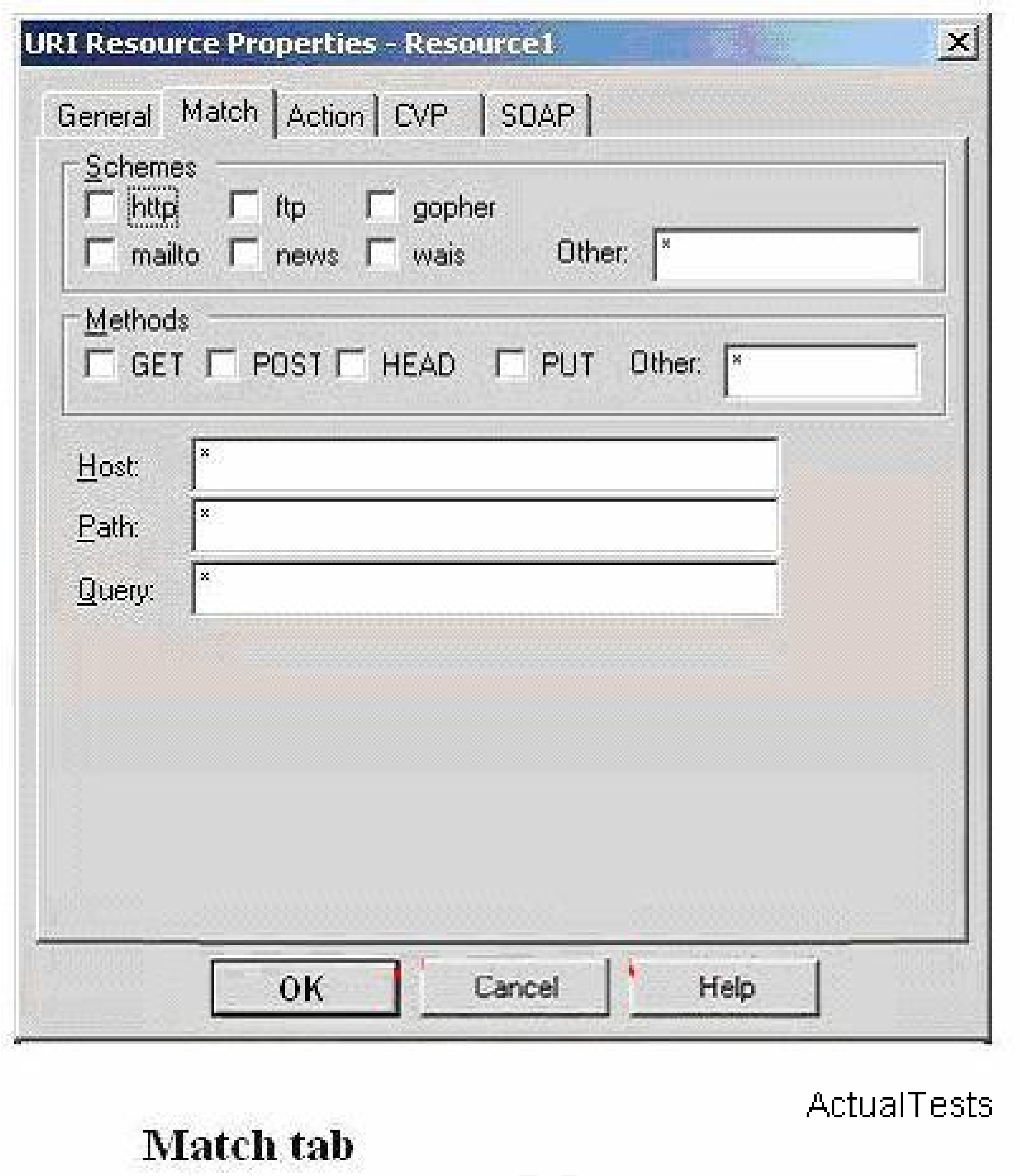
● Wildcards

○ File

○ UFP

General Tab

ActualTests



URI Resource Properties - Resource1

Schemes

□ http □ ftp □ gopher
□ mailto □ news □ wais Other: *

Methods

□ GET □ POST □ HEAD □ PUT Other: *

Host: *

Path: *

Query: *

Match tab

A. Resources

B. Wild Cards

C. CVP

D. File

E. UFP

Answer: B,D,E

QUESTION NO: 303

External User Profiles can be defined as:

A. Users who are not defined in the internalusers database but on LDAP server

B. Users who are defined in the internalusers database or on an LDAP server

C. Users that are defined on SmartDashboard

D. Users who are not defined in the internalusers database or on an LDAP server
E. Users that are defined on LDAP server

Answer: D

QUESTION NO: 304

Why must Client Authentication rule be placed above Stealth rule in the Rulebase?

A. In order that they can have access to the SmartDashboard
B. In order that they can have access to the local Security Management server
C. In order that they can have access to the Security Management server
D. In order that they can have access to the OS
E. In order that they can have access to the local Gateway

Answer: E

QUESTION NO: 305

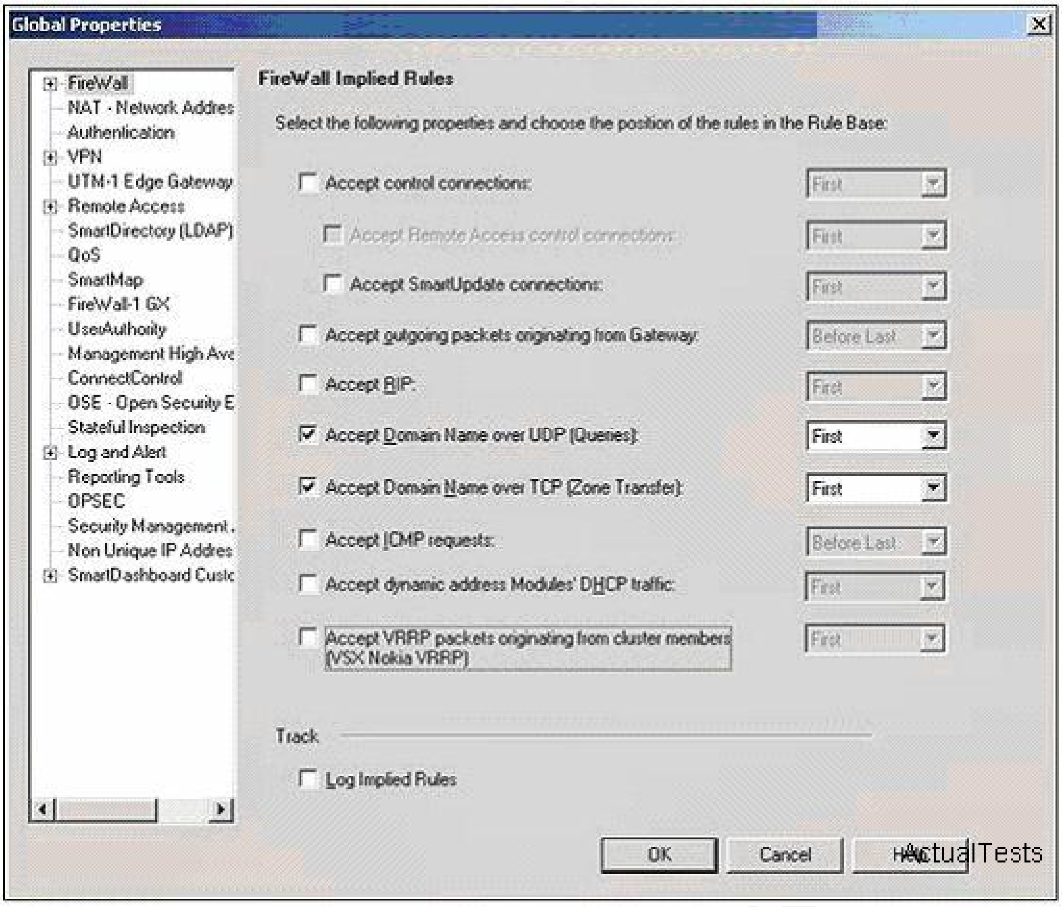
Which of the following is true regarding UTM-1 Edge appliances?

A. There is a limitation on the file size that can be scanned by antivirus gateway
B. They come with integrated gateway antivirus
C. They support standard email protocols (POP3, IMAP, and SMTP), including Webbased email
D. They support best-of-breed URL Filtering based onan 3rd party URL filtering services
E. They provide solutions for blocking spam and Malware

Answer: B,C,D,E

QUESTION NO: 306

Your IT boss gives you the following requirements which are classified as mandatory requirements and optional requirements. Mandatory requirements 1: Accept domain-name-over-TCP traffic (zone-transfer traffic) Mandatory requirements 2: Log domain-name-over-TCP traffic (zone-transfer traffic) Optional requirements 1: Accept domain-name-over-UDP traffic (queries traffic) Optional requirements 2: Do not log domain-name-over-UDP traffic (queries traffic) Optional requirements 3: Do not clutter the Rule Base by creating explicit rules for traffic that can be controlled using Global Properties. In order to achieve these objectives, you:



FireWall Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

- □ Accept control connections: First
- □ Accept Remote Access control connections: First
- □ Accept SmartUpdate connections: First
- □ Accept outgoing packets originating from Gateway: Before Last
- □ Accept RIP: First
- ☑ Accept Domain Name over UDP (Queries): First
- ☑ Accept Domain Name over TCP (Zone Transfer): First
- □ Accept ICMP requests: Before Last
- □ Accept dynamic address Modules' DHCP traffic: First
- □ Accept VRRP packets originating from cluster members (VSX Nokia VRRP): First

Track

- □ Log Implied Rules

A. Go to the Global Properties and select "Accept Domain Name overTCP(Zone Transfer) box
B. Go to the Global Properties and select "Accept Domain Name over UDP (Queries)" box
C. Go to the Global Properties and select "Log Implied Rules" Would your procedures achieve the mandatory requirements and optional requirements?
D. Your procedures will achieve the two mandatory requirements and two optional requirements
E. Your procedures will achieve all the mandatory requirements and none of the optional requirements
F. Your procedures will achieve neither the mandatory requirements nor the optional requirements
G. Your procedures will achieve all the mandatory requirements and one optional requirement
H. Your procedures will achieve all the mandatory requirements and optional Requirements

Answer: A

QUESTION NO: 307

Which tool is ideal management utility for distributed installation with multiple security gateways, where specific policies are created for specific security gateway?

A. Rule Grouping Tool
B. Database Revision Control
C. Policy Package Management
D. Rule Base Management

E. Rule Coded Tool

Answer: C

QUESTION NO: 308

To perform an advanced upgrade on SecurePlatform using R70 CDROM, what command will you enter at the command prompt?

A. UnixInstallScript
B. cpinfo
C. patch add cd
D. LinuxInstallScript
E. cpconfig

Answer: C

QUESTION NO: 309

Your disaster recover strategy needs to be tested in order to ensure that it works as it should. You decide to run a test to achieve two objectives. The first objective - required objective - is to ensure that the Security Policy repository be backed up at least every 24 hours. The second objective - desired objective - to ensure that the R70 components that enforce the Security Policies be backed up at least once a week, and R70 logs should also be backed up at least once a week. You run cron utility to run upgrade_export command each night on the Security Management Servers. You then configure the organization's routine backup software to back the files created by the upgrade_export command. You configure the SecurePlatform backup utility to back the Security Gateways every Friday night. You use the cron utility to run the upgrade_export command each Friday night on the log servers. You configure the automatic nightly logswitch. You also configure the organization's routine backup software to back up the switched logs every night. Which of the following is true?

A. Your actions will meet the required objective and one desired objective
B. Your actions will not meet the required objective but will meet one of the desired objectives
C. Your actions will meet the required objective and none of the desired objectives
D. Your actions will not meet the required objective but will meet the two desired objectives
E. Your actions will meet the required objective and the two desired objectives

Answer: E

QUESTION NO: 310

You are performing an upgrade of your Security Management server using " Migrate and Upgrade to a New Security Management server" method. What is the use of the production server?

A. There is no need to use a production server
B. Is the off-line machine
C. Is the destination machine whose configuration you need to copyfrom
D. Is the destination machine whose configuration you need tocopy
E. Is the source machine whose configuration you need tocopy

Answer: E

QUESTION NO: 311

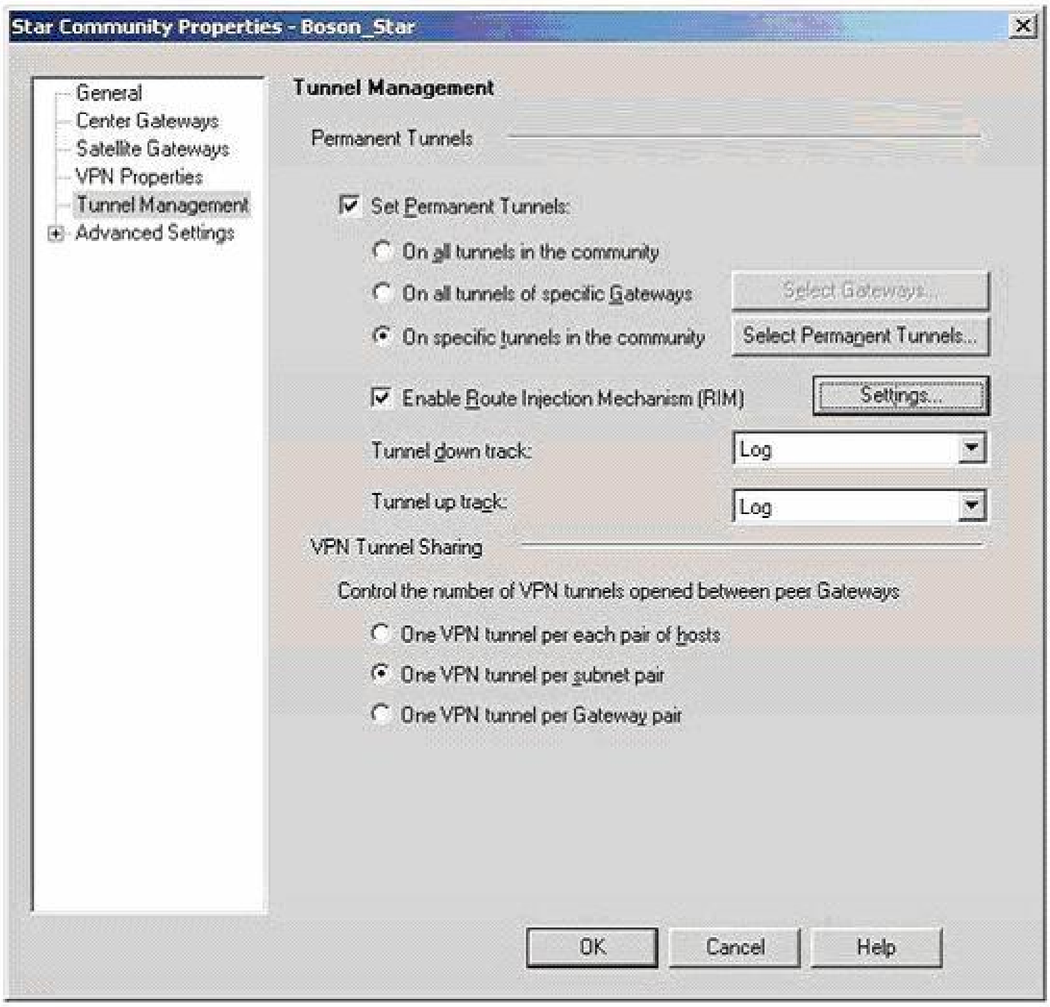
Which of he following is true regarding SmartUpdate and management of licenses?

A. With Central Licensing, you only need one IP address for all licenses
B. With Local Licensing, license can be taken from one gateway and given to another
C. Attaching a license to a gateway involves installing the license on the remote gateway, and associating
D. A Local License is a license attached to the Security Management server IP address,rather than the gateway IP address
E. Detaching a license from a gateway involves uninstalling the license from the remote gateway and making the license in the License & Contract Repository available to any gateway

Answer: A,C,E

QUESTION NO: 312

Which of the following is true regarding Permanent Tunnels?



Star Community Properties - Boson_Star

- General
- Center Gateways
- Satellite Gateways
- VPN Properties
- Tunnel Management
- Advanced Settings

Tunnel Management

Permanent Tunnels

☑ Set Permanent Tunnels:

○ On all tunnels in the community

○ On all tunnels of specific Gateways [Select Gateways...]

● On specific tunnels in the community [Select Permanent Tunnels...]

☑ Enable Route Injection Mechanism (RIM) [Settings...]

Tunnel down track: Log

Tunnel up track: Log

VPN Tunnel Sharing

Control the number of VPN tunnels opened between peer Gateways

○ One VPN tunnel per each pair of hosts

● One VPN tunnel per subnet pair

○ One VPN tunnel per Gateway pair

ActualTests

Figure 1: Community Properties Window

A. Permanent Tunnels provide greater interoperability and scalability between gateways

B. Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued

C. Permanent Tunnels can only be established between Check Point gateways

D. Each VPN tunnel in the community may be set to be a Permanent Tunnel

E. Permanent Tunnels control the number of VPN tunnels created between peer Gateways

Answer: B,C,D

QUESTION NO: 313

Anti-Virus protection is available for which of the following protocols?

A. HTTP

B. FTP

C. SNMP

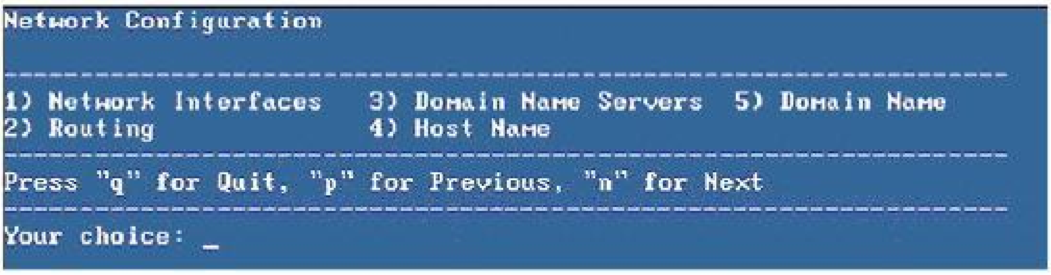
D. SMTP

E. POP3

Answer: A,B,D,E

QUESTION NO: 314

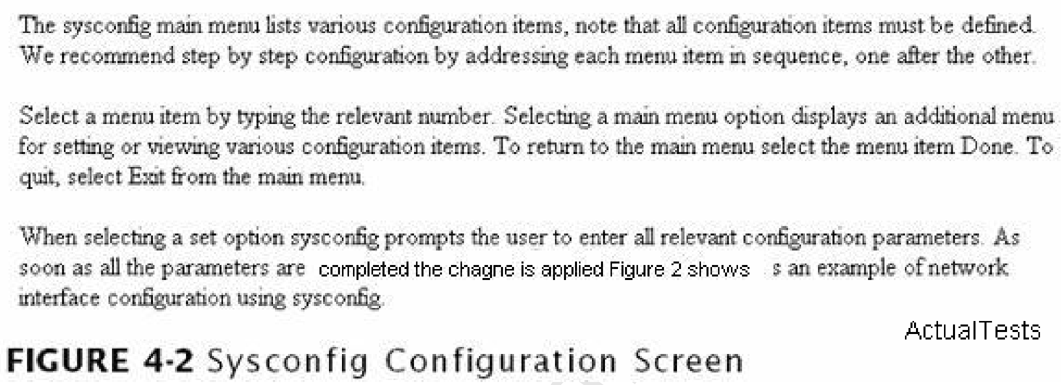
After installing SecurePlatform, what tool would you use to configure it?



```
Network Configuration

--------------------------------------------------------------------
1) Network Interfaces   3) Domain Name Servers   5) Domain Name
2) Routing              4) Host Name
--------------------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
--------------------------------------------------------------------
Your choice: _
```

Figure 1: Sysconfig Main Menu

.

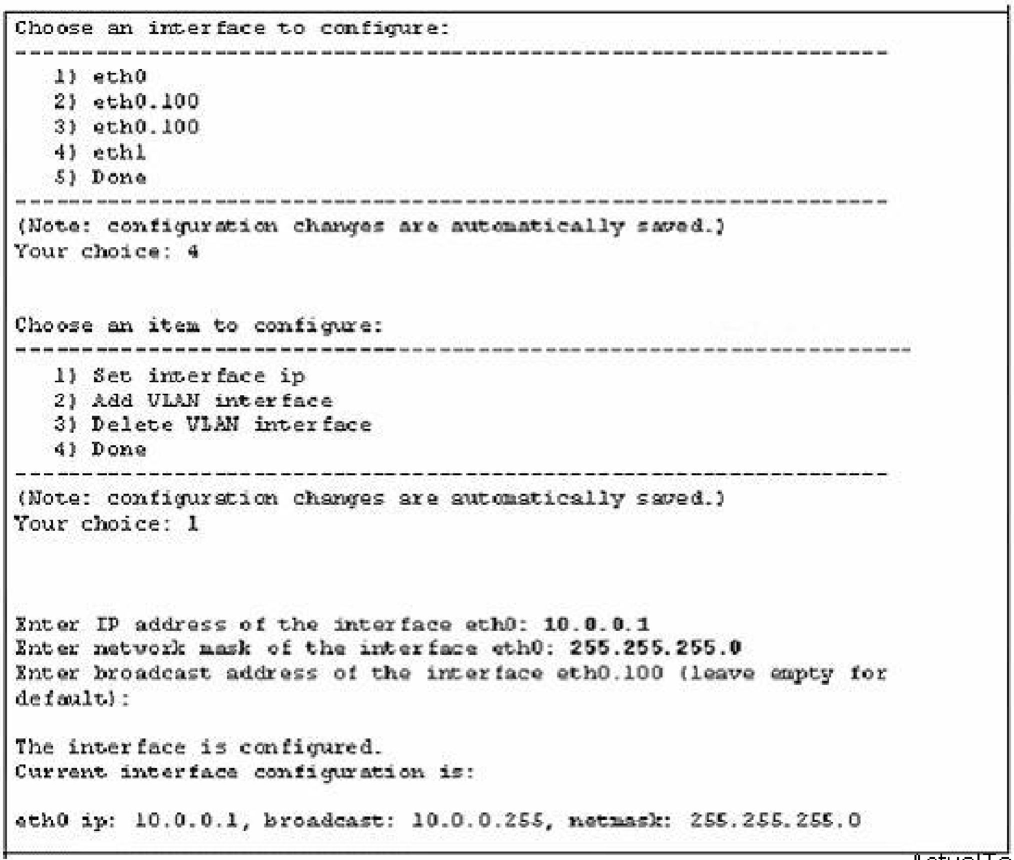


The sysconfig main menu lists various configuration items, note that all configuration items must be defined. We recommend step by step configuration by addressing each menu item in sequence, one after the other.

Select a menu item by typing the relevant number. Selecting a main menu option displays an additional menu for setting or viewing various configuration items. To return to the main menu select the menu item Done. To quit, select Exit from the main menu.

When selecting a set option sysconfig prompts the user to enter all relevant configuration parameters. As soon as all the parameters are completed the chagne is applied Figure 2 shows s an example of network interface configuration using sysconfig.

FIGURE 4-2 Sysconfig Configuration Screen

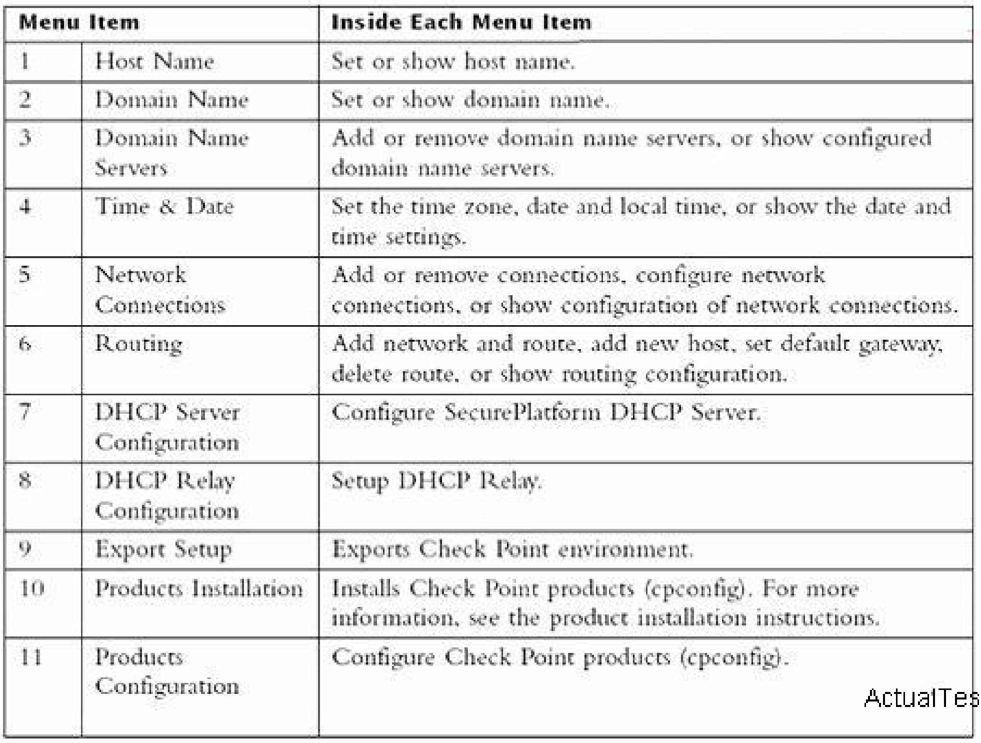


```
Choose an interface to configure:
------------------------------------------------------------------
   1) eth0
   2) eth0.100
   3) eth0.100
   4) eth1
   5) Done
------------------------------------------------------------------
(Note: configuration changes are automatically saved.)
Your choice: 4


Choose an item to configure:
--------------------------------------------------------------------
   1) Set interface ip
   2) Add VLAN interface
   3) Delete VLAN interface
   4) Done
------------------------------------------------------------------
(Note: configuration changes are automatically saved.)
Your choice: 1



Enter IP address of the interface eth0: 10.0.0.1
Enter network mask of the interface eth0: 255.255.255.0
Enter broadcast address of the interface eth0.100 (leave empty for
default):

The interface is configured.
Current interface configuration is:

eth0 ip: 10.0.0.1, broadcast: 10.0.0.255, netmask: 255.255.255.0
```

Figure 2: Sysconfig Configuration Screen

The following table summarizes the various configuration options:

TABLE 4-1 Sysconfig Configuration Options



Menu Item		Inside Each Menu Item
1	Host Name	Set or show host name.
2	Domain Name	Set or show domain name.
3	Domain Name Servers	Add or remove domain name servers, or show configured domain name servers.
4	Time & Date	Set the time zone, date and local time, or show the date and time settings.
5	Network Connections	Add or remove connections, configure network connections, or show configuration of network connections.
6	Routing	Add network and route, add new host, set default gateway, delete route, or show routing configuration.
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.
9	Export Setup	Exports Check Point environment.
10	Products Installation	Installs Check Point products (cpconfig). For more information, see the product installation instructions.
11	Products Configuration	Configure Check Point products (cpconfig).

A. config

B. SecurePlatformconfig

C. systemconfig

D. ipconfig
E. sysconfig

Answer: E

QUESTION NO: 315

A __________ __________ is a set of Policies that are enforced on selected Enforcement modules. These Policies may include different types of policies, such as a Security Policy or a QoS policy.

A. Security Policy
B. Objects
C. Policy Package
D. Enforcement module
E. Security Management server

Answer: C

QUESTION NO: 316

Once you have created a template, any user you create based on the template will inherit all of the template's properties, including membership in groups. If you modify this template's properties, the changes will affect all the users created from the template in the future. Do you think the changes will also affect the users you have created in the past based on this template?

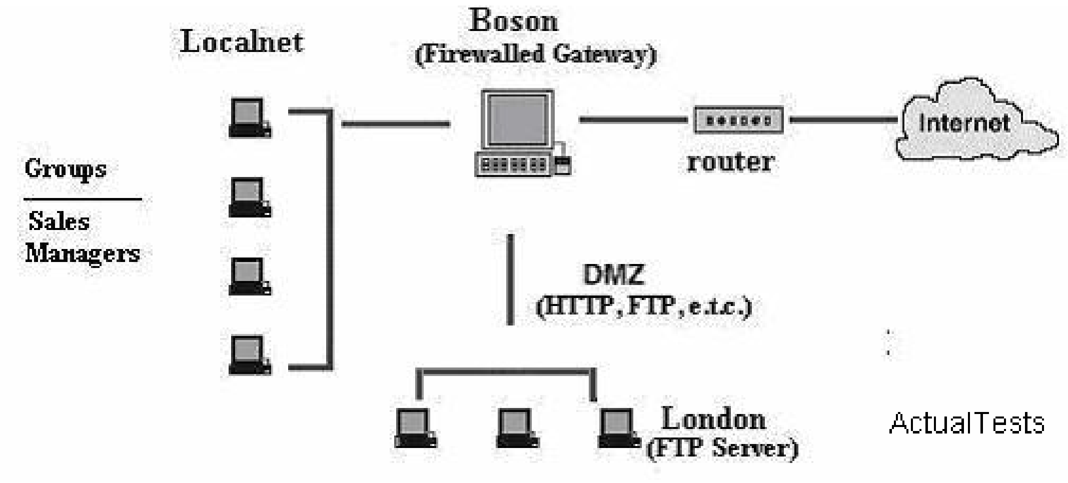
A. No, the new changes will not affect the users you have created in the past based on this template
B. Yes, the new changes will affect the users you will create in the future and also the users you have created in the past based on this template
C. No, the new changes will not affect the users you will create in the future and also the users you have created in the past based on this template
D. None of the available answers
E. Yes, the new changes will also affect the users you have created in the past based on this template

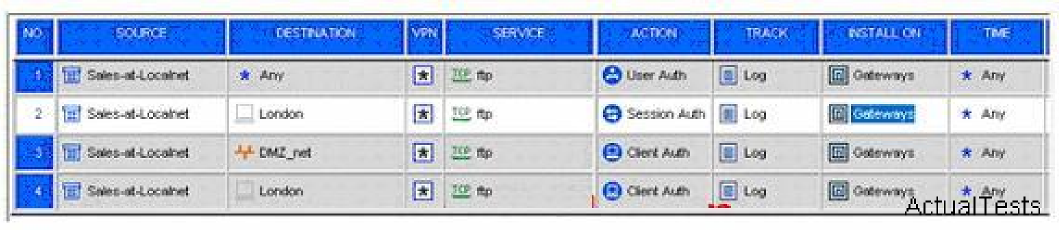
Answer: A

QUESTION NO: 317

Study the diagram and answer the question. Your Internal network is called Local net. In order to grant different accesses to the users in your network, you created two different groups: Sales and

Managers. You will now need to modify your rule to allow Sales team access FTP access to any location. What rule would allow Sales team FTP access to any location?





NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Sales-at-Localnet	Any	★	TCP ftp	User Auth	Log	Gateways	Any
2	Sales-at-Localnet	London	★	TCP ftp	Session Auth	Log	Gateways	Any
3	Sales-at-Localnet	DMZ_net	★	TCP ftp	Client Auth	Log	Gateways	Any
4	Sales-at-Localnet	London	★	TCP ftp	Client Auth	Log	Gateways	Any

A. Rule 1
B. None of the available answers
C. Rule 2
D. Rule 4
E. Rule 3

Answer: A

QUESTION NO: 318

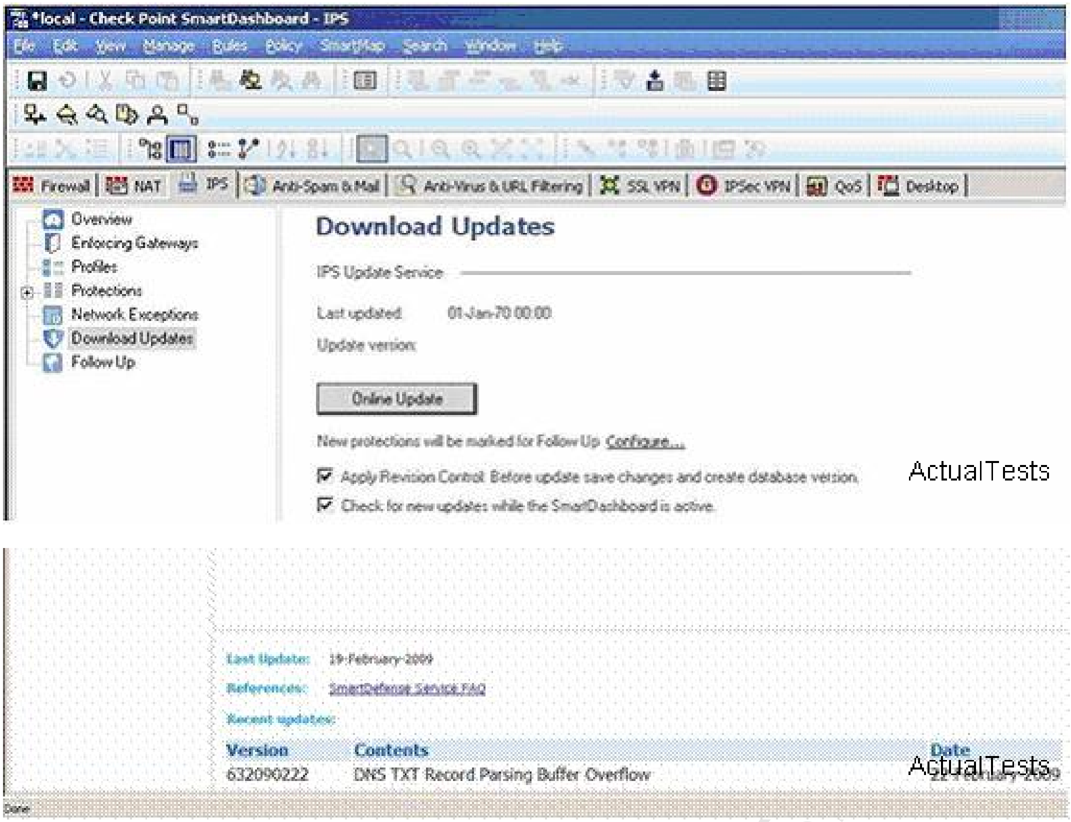
What are the three types of authentication?

A. Non-Transparent Authentication
B. Transparent Authentication
C. User Authentication
D. Client Authentication
E. Session Authentication

Answer: C,D,E

QUESTION NO: 319

Which page will you go in the IPS tab in order to download IPS updates?


*local - Check Point SmartDashboard - IPS
File Edit View Manage Rules Policy SmartMap Search Window Help
Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS | Desktop
Overview
Enforcing Gateways
Profiles
Protections
Network Exceptions
Download Updates
Follow Up
Online Update
Done

Download Updates

IPS Update Service

Last updated: 01-Jan-70 00:00

Update version:

New protections will be marked for Follow Up Configure...

☑ Apply Revision Control: Before update save changes and create database version.

☑ Check for new updates while the SmartDashboard is active.

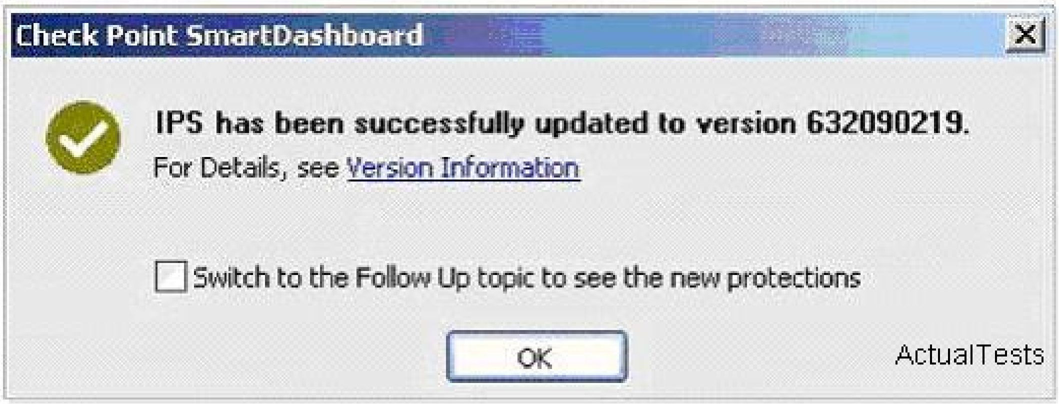
Last Update: 19-February-2009

References: SmartDefense Service FAQ

Recent updates:

Version	Contents	Date
632090222	DNS TXT Record Parsing Buffer Overflow	22-February-2009

Figure 1: IPS Tab - Download Updates Page



IPS has been successfully updated to version 632090219.
For Details, see Version Information

☐ Switch to the Follow Up topic to see the new protections

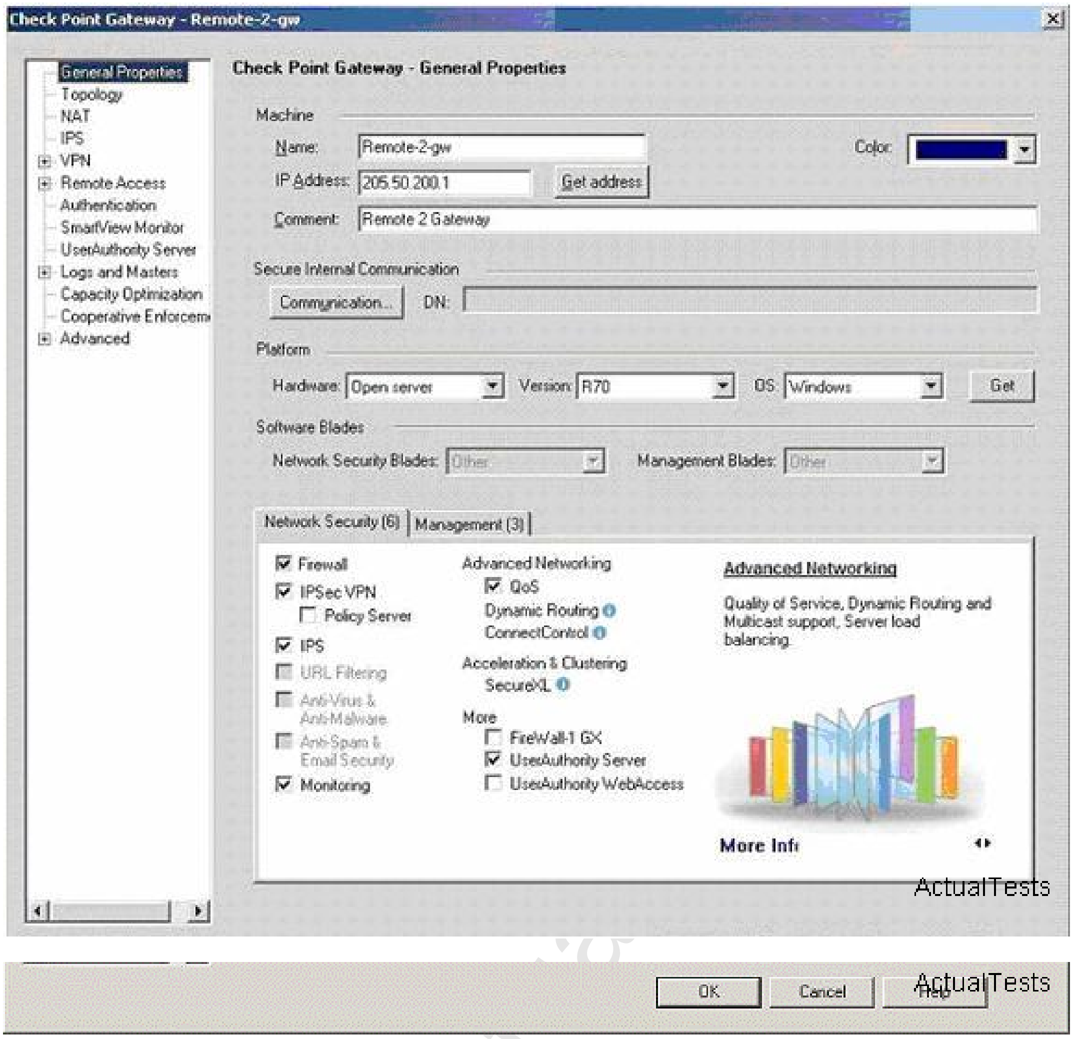
Figure 2: Successful Update Window

A. Download Updates page
B. Protections page
C. Network Exceptions page
D. Profiles page
E. Enforcing Gateways page

Answer: A

QUESTION NO: 320

You are deploying Software blades and you have two options to choose from. You want to deploy software that allows you to deploy Access Control, Authentication, NAT, VPN and IPS?



Check Point Gateway - General Properties

Machine

Name: Remote-2-gw

IP Address: 205.50.200.1

Color:

Comment: Remote 2 Gateway

Secure Internal Communication

DN:

Platform

Hardware: Open server Version: R70 OS: Windows

Software Blades

Network Security Blades: Other Management Blades: Other

Network Security (6) | Management (3)

- ☑ Firewall
- ☑ IPSec VPN
  - □ Policy Server
- ☑ IPS
- □ URL Filtering
- □ Anti-Virus & Anti-Malware
- □ Anti-Spam & Email Security
- ☑ Monitoring

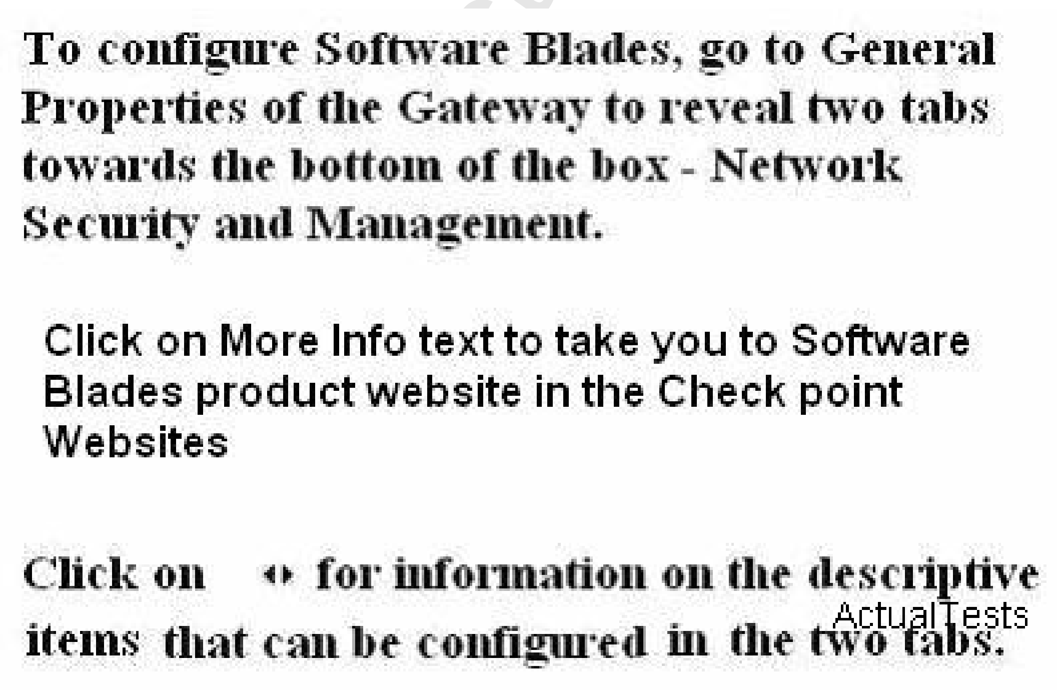
Advanced Networking
- ☑ QoS
- Dynamic Routing
- ConnectControl

Acceleration & Clustering
- SecureXL

More
- □ FireWall-1 GX
- ☑ UserAuthority Server
- □ UserAuthority WebAccess

Advanced Networking

Quality of Service, Dynamic Routing and Multicast support, Server load balancing

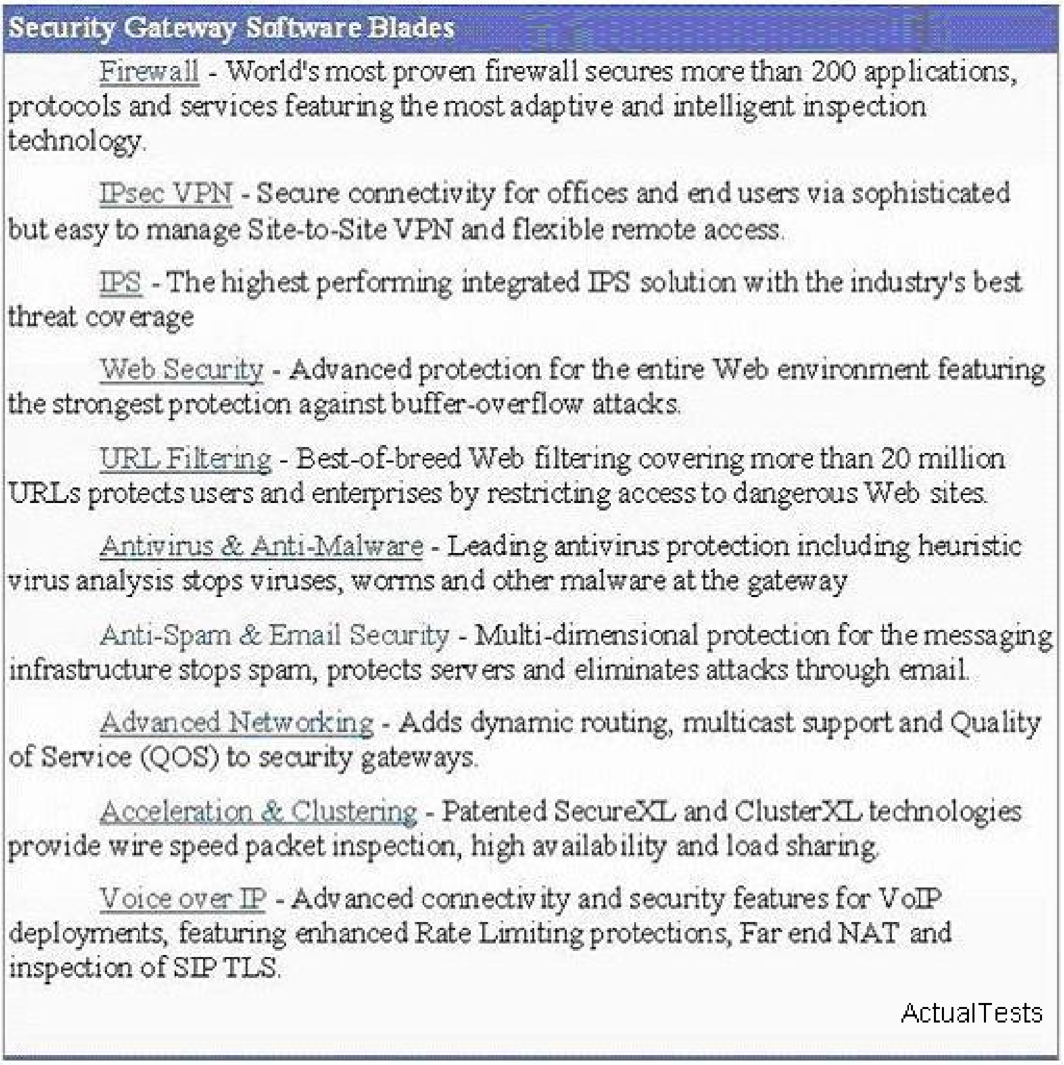


To configure Software Blades, go to General Properties of the Gateway to reveal two tabs towards the bottom of the box - Network Security and Management.

Click on More Info text to take you to Software Blades product website in the Check point Websites

Click on ◂▸ for information on the descriptive items that can be configured in the two tabs.

Figure 1: Network Security tab



Security Gateway Software Blades

Firewall - World's most proven firewall secures more than 200 applications, protocols and services featuring the most adaptive and intelligent inspection technology.

IPsec VPN - Secure connectivity for offices and end users via sophisticated but easy to manage Site-to-Site VPN and flexible remote access.

IPS - The highest performing integrated IPS solution with the industry's best threat coverage

Web Security - Advanced protection for the entire Web environment featuring the strongest protection against buffer-overflow attacks.

URL Filtering - Best-of-breed Web filtering covering more than 20 million URLs protects users and enterprises by restricting access to dangerous Web sites.

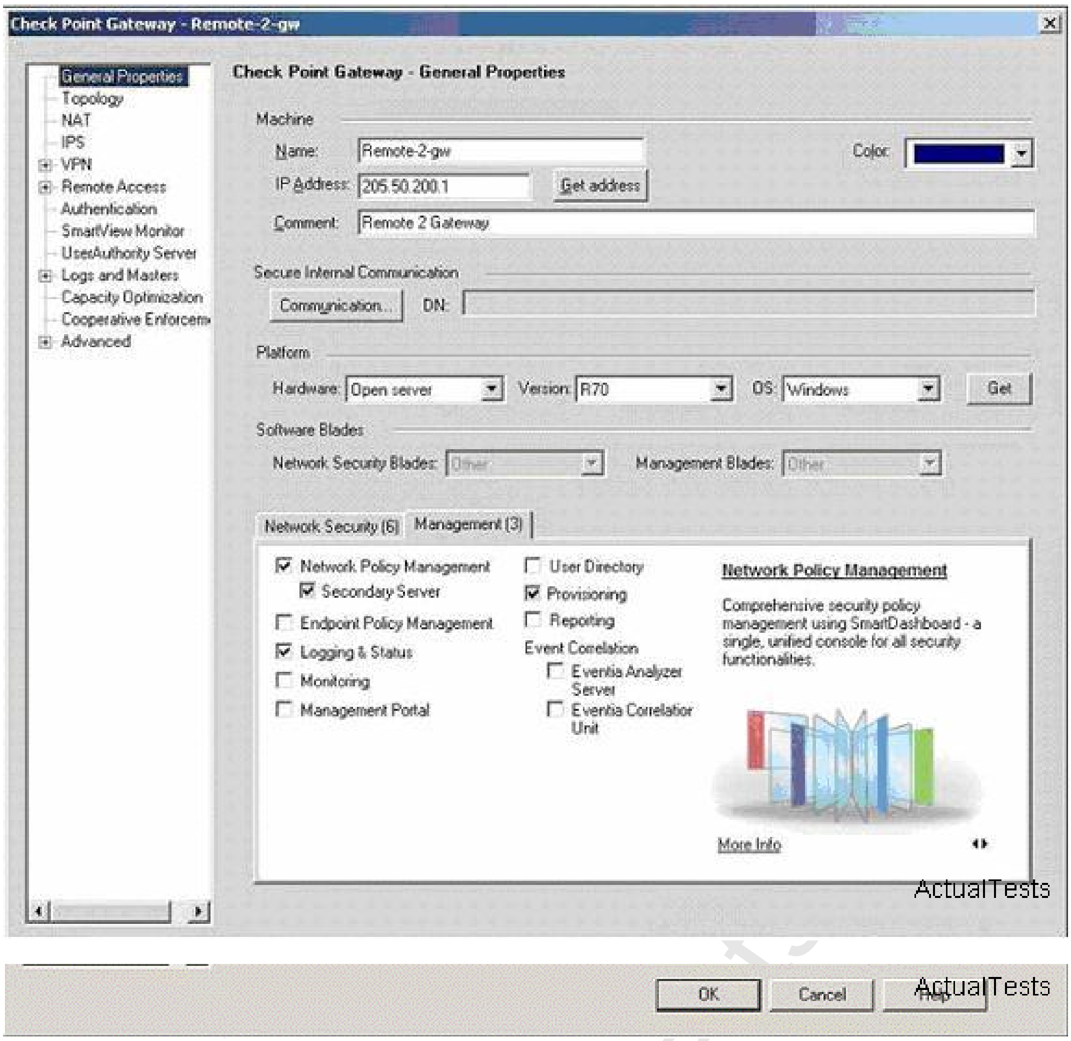
Antivirus & Anti-Malware - Leading antivirus protection including heuristic virus analysis stops viruses, worms and other malware at the gateway

Anti-Spam & Email Security - Multi-dimensional protection for the messaging infrastructure stops spam, protects servers and eliminates attacks through email.

Advanced Networking - Adds dynamic routing, multicast support and Quality of Service (QOS) to security gateways.

Acceleration & Clustering - Patented SecureXL and ClusterXL technologies provide wire speed packet inspection, high availability and load sharing.

Voice over IP - Advanced connectivity and security features for VoIP deployments, featuring enhanced Rate Limiting protections, Far end NAT and inspection of SIP TLS.



Check Point Gateway - Remote-2-gw

Check Point Gateway - General Properties

Machine

Name: Remote-2-gw

IP Address: 205.50.200.1

Comment: Remote 2 Gateway

Secure Internal Communication

DN:

Platform

Hardware: Open server

Version: R70

OS: Windows

Software Blades

Network Security Blades: Other

Management Blades: Other

Network Security (6) | Management (3)

☑ Network Policy Management

☑ Secondary Server

□ Endpoint Policy Management

☑ Logging & Status

□ Monitoring

□ Management Portal

□ User Directory

☑ Provisioning

□ Reporting

Event Correlation

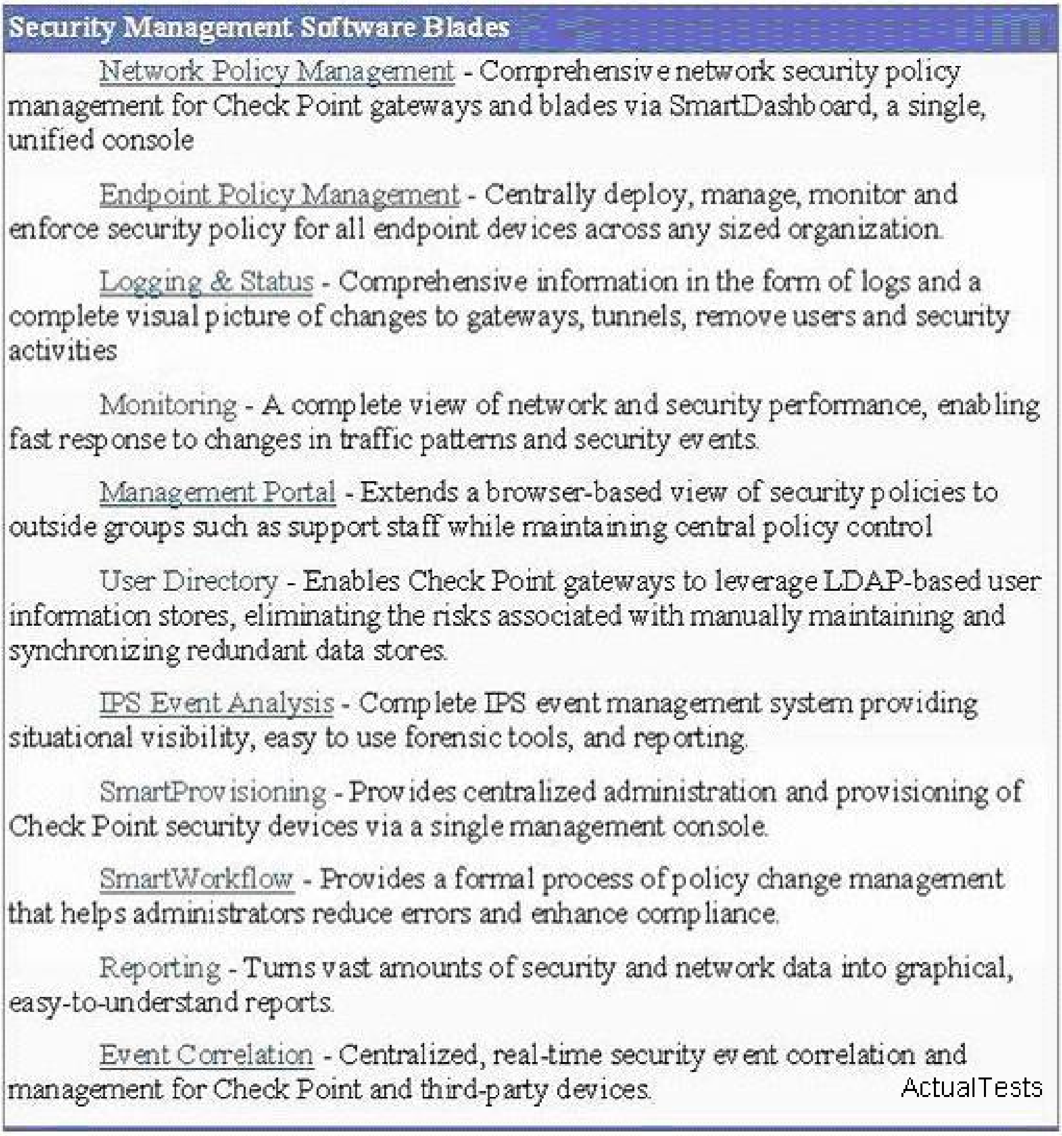
□ Eventia Analyzer Server

□ Eventia Correlation Unit

Network Policy Management

Comprehensive security policy management using SmartDashboard - a single, unified console for all security functionalities.

Figure 2: Management tab



Security Management Software Blades

Network Policy Management - Comprehensive network security policy management for Check Point gateways and blades via SmartDashboard, a single, unified console

Endpoint Policy Management - Centrally deploy, manage, monitor and enforce security policy for all endpoint devices across any sized organization.

Logging & Status - Comprehensive information in the form of logs and a complete visual picture of changes to gateways, tunnels, remove users and security activities

Monitoring - A complete view of network and security performance, enabling fast response to changes in traffic patterns and security events.

Management Portal - Extends a browser-based view of security policies to outside groups such as support staff while maintaining central policy control

User Directory - Enables Check Point gateways to leverage LDAP-based user information stores, eliminating the risks associated with manually maintaining and synchronizing redundant data stores.

IPS Event Analysis - Complete IPS event management system providing situational visibility, easy to use forensic tools, and reporting.

SmartProvisioning - Provides centralized administration and provisioning of Check Point security devices via a single management console.

SmartWorkflow - Provides a formal process of policy change management that helps administrators reduce errors and enhance compliance.

Reporting - Turns vast amounts of security and network data into graphical, easy-to-understand reports.

Event Correlation - Centralized, real-time security event correlation and management for Check Point and third-party devices.

A. Security Network Software Blades

B. Security Endpoint Software Blades

C. Security IPSEC Software Blades

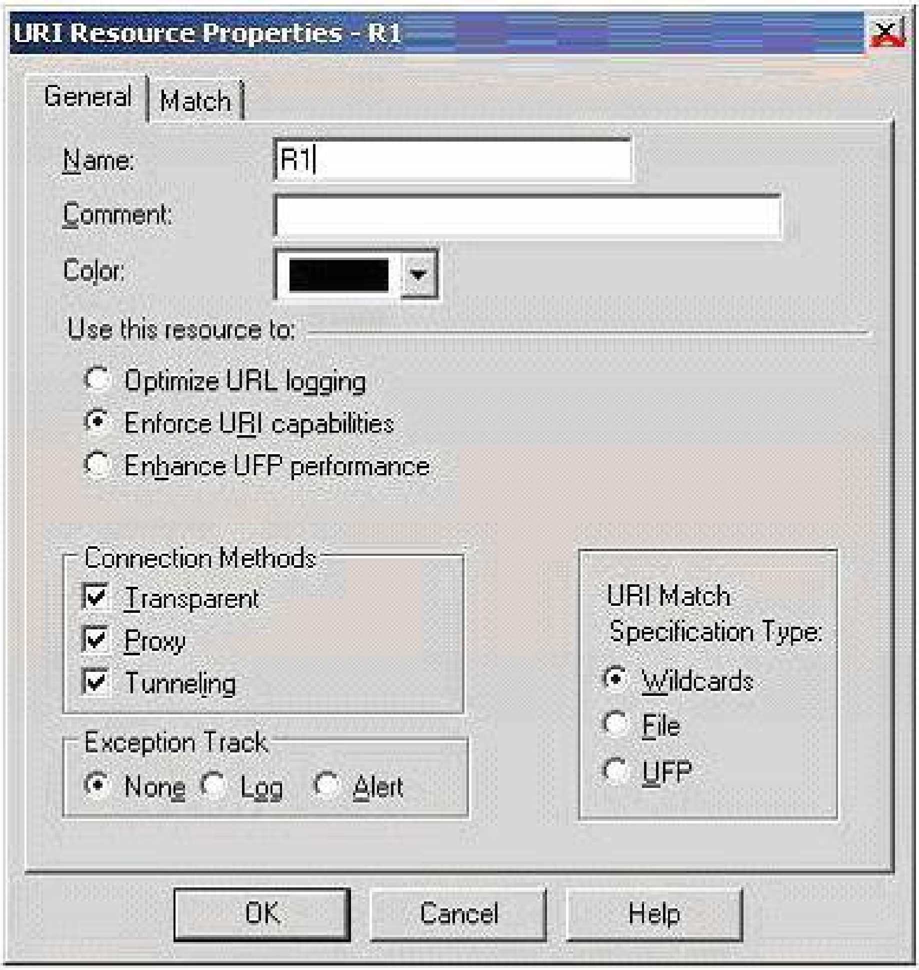
D. Security Gateway Software Blades

E. Security Management Software Blades

Answer: D

QUESTION NO: 321

Host (on the Match tab of the URI Resource Properties window if "Wildcards" button is selected in the URI Match Specification Type section)specifies the host and port of a known HTTPS server e.g. https server host:443. If you specify a wildcard (i.e. *) instead, then what is likely to be the result?



URI Resource Properties - R1

General | Match

Name: R1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging

● Enforce URI capabilities

○ Enhance UFP performance

Connection Methods

☑ Transparent

☑ Proxy

☑ Tunneling

Exception Track

● None ○ Log ○ Alert

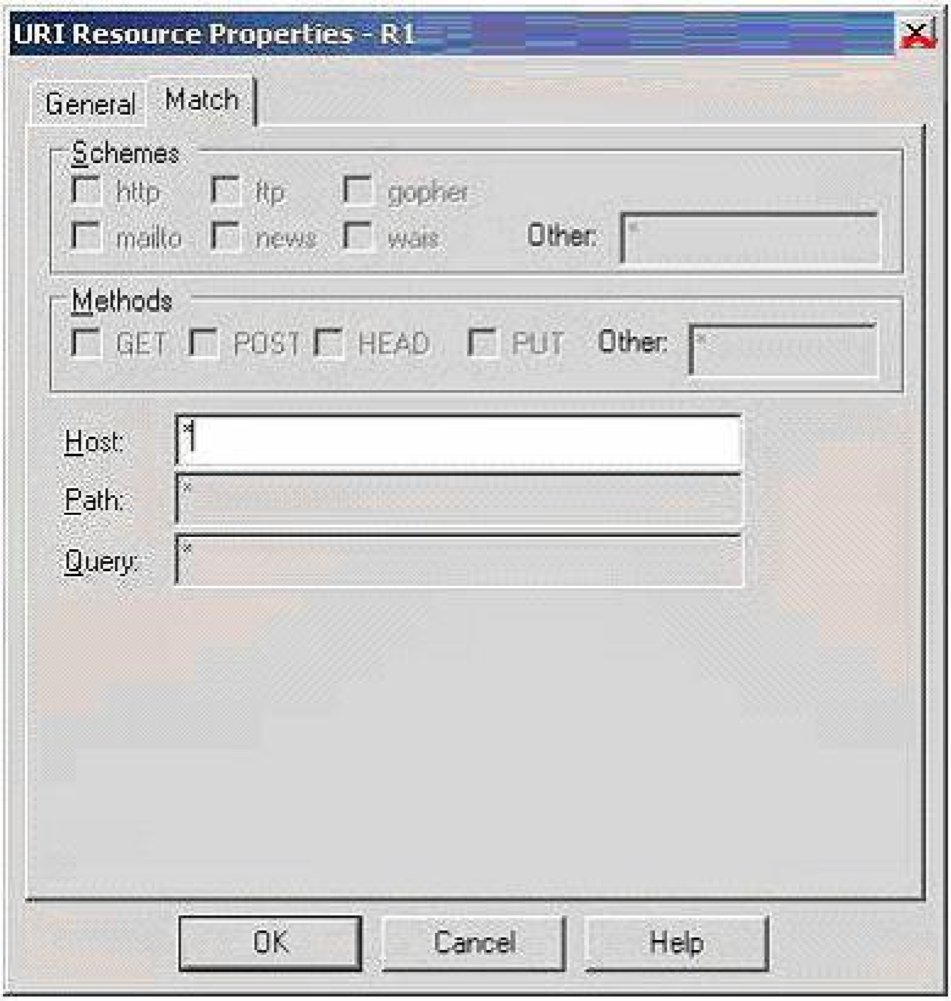
URI Match Specification Type:

● Wildcards

○ File

○ UFP

Figure 1:URI Resource Properties - General tab



URI Resource Properties - R1

General | Match

Schemes

□ http □ ftp □ gopher

□ mailto □ news □ wais Other: *

Methods

□ GET □ POST □ HEAD □ PUT Other: *

Host: *

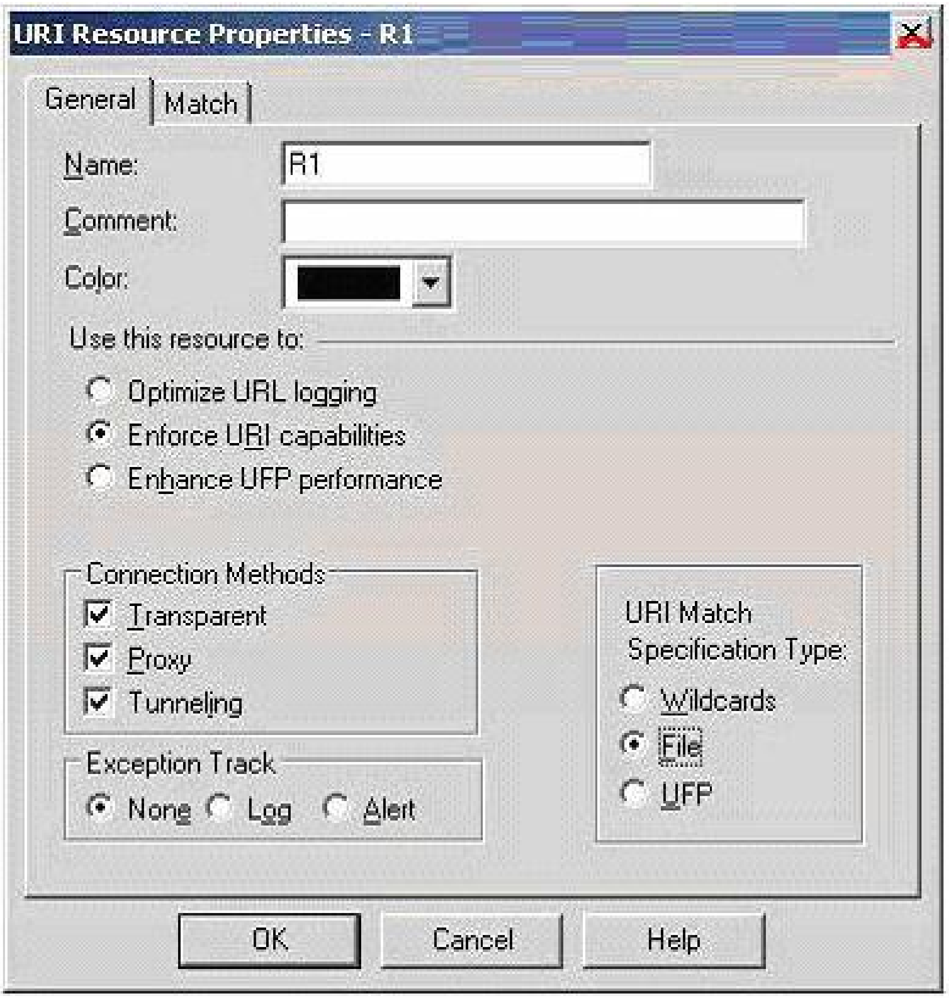
Path: *

Query: *

Figure 2:URI Resource Properties - Match tab

If Wildcards is selected in General tab

Tunneling box is checked in General tab



URI Resource Properties - R1

Name: R1

Comment:

Color:

Use this resource to:

○ Optimize URL logging

● Enforce URI capabilities

○ Enhance UFP performance

Connection Methods

☑ Transparent

☑ Proxy

☑ Tunneling

Exception Track

● None ○ Log ○ Alert

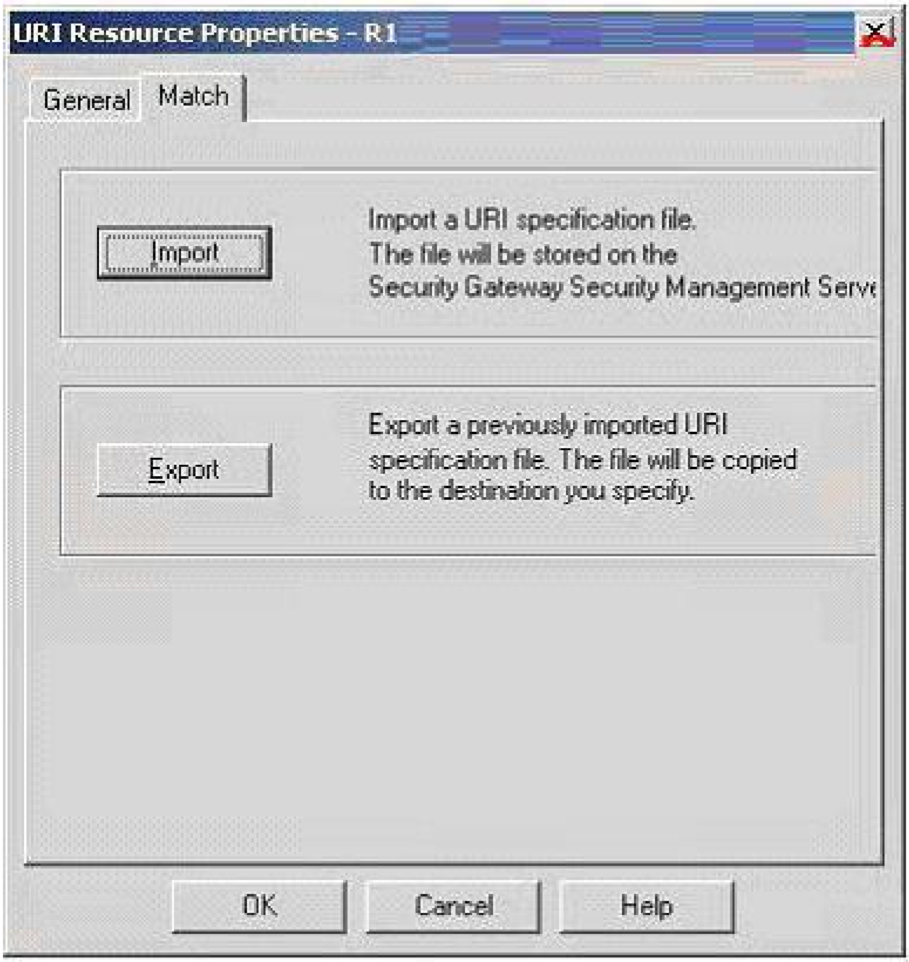
URI Match Specification Type:

○ Wildcards

● File

○ UFP

Figure 3 :URI Resource Properties - General tab



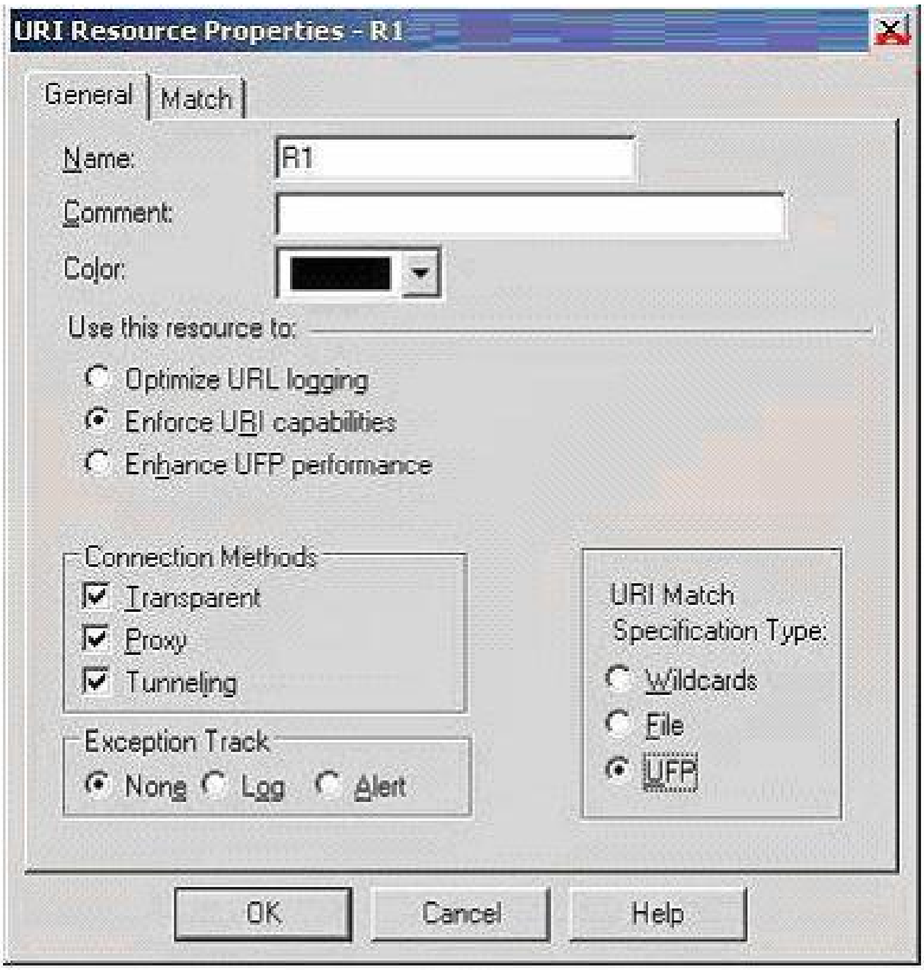
Import a URI specification file. The file will be stored on the Security Gateway Security Management Serve

Export a previously imported URI specification file. The file will be copied to the destination you specify.

Figure 4:URI Resource Properties - Match tab

If Wildcards is selected in General tab

Tunneling box is checked in General tab



URI Resource Properties - R1

General | Match

Name: R1

Comment:

Color: ■

Use this resource to:

○ Optimize URL logging

● Enforce URI capabilities

○ Enhance UFP performance

Connection Methods

☑ Transparent

☑ Proxy

☑ Tunneling

Exception Track

● None ○ Log ○ Alert

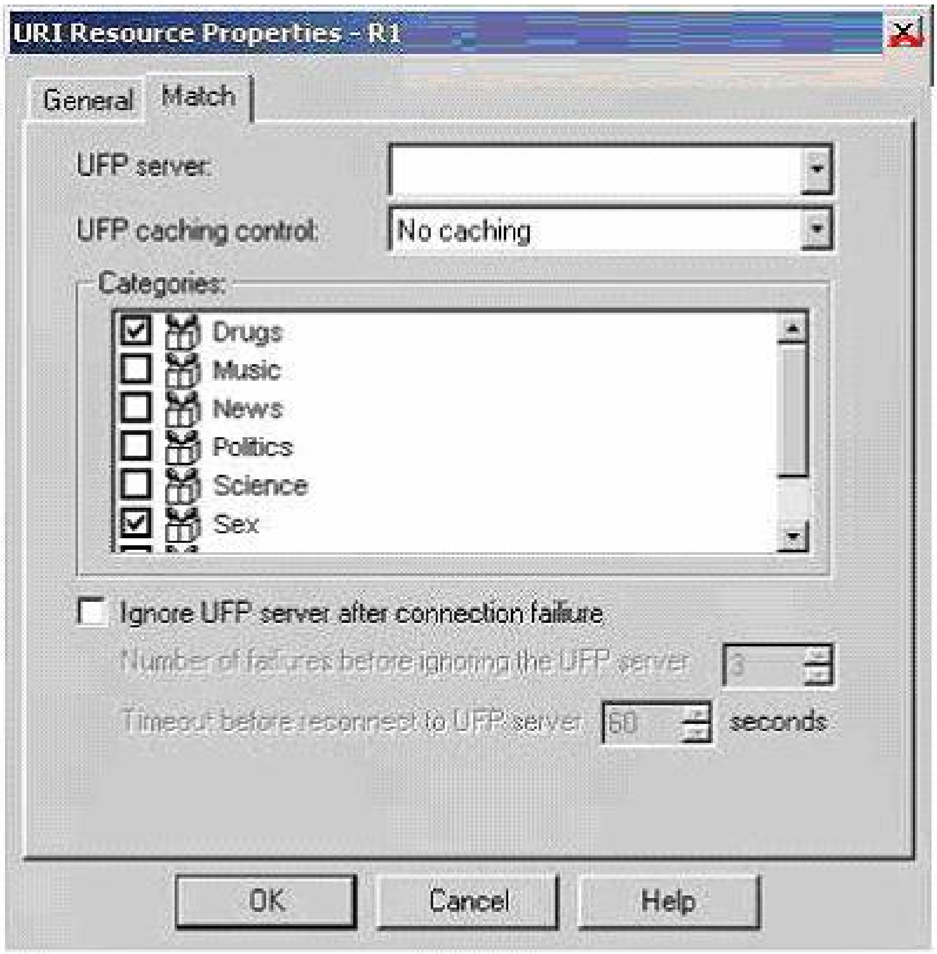
URI Match Specification Type:

○ Wildcards

○ File

● UFP

Figure 5:URI Resource Properties - General tab



UFP server:

UFP caching control: No caching

Categories:

- ☑ Drugs
- □ Music
- □ News
- □ Politics
- □ Science
- ☑ Sex

□ Ignore UFP server after connection failure

Number of failures before ignoring the UFP server: 3

Timeout before reconnect to UFP server: 60 seconds

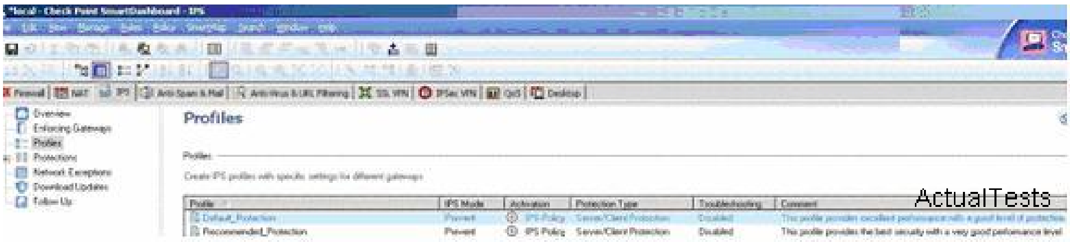
Figure 6 : URI Resource Properties - Match tab
If Wildcards is selected in General tab
Tunneling box is checked in General tab

A. That will indicate the Rule Base will make special consideration for specified resource
B. That will indicate all ports
C. The Action and CVP tabs will be disabled
D. That will indicate any host or any port
E. That will indicate any host

Answer: D

QUESTION NO: 322

Activating a large number of protections to include those with low severity or a low confidence level protects against a wide range of attacks but the disadvantage of this is that:



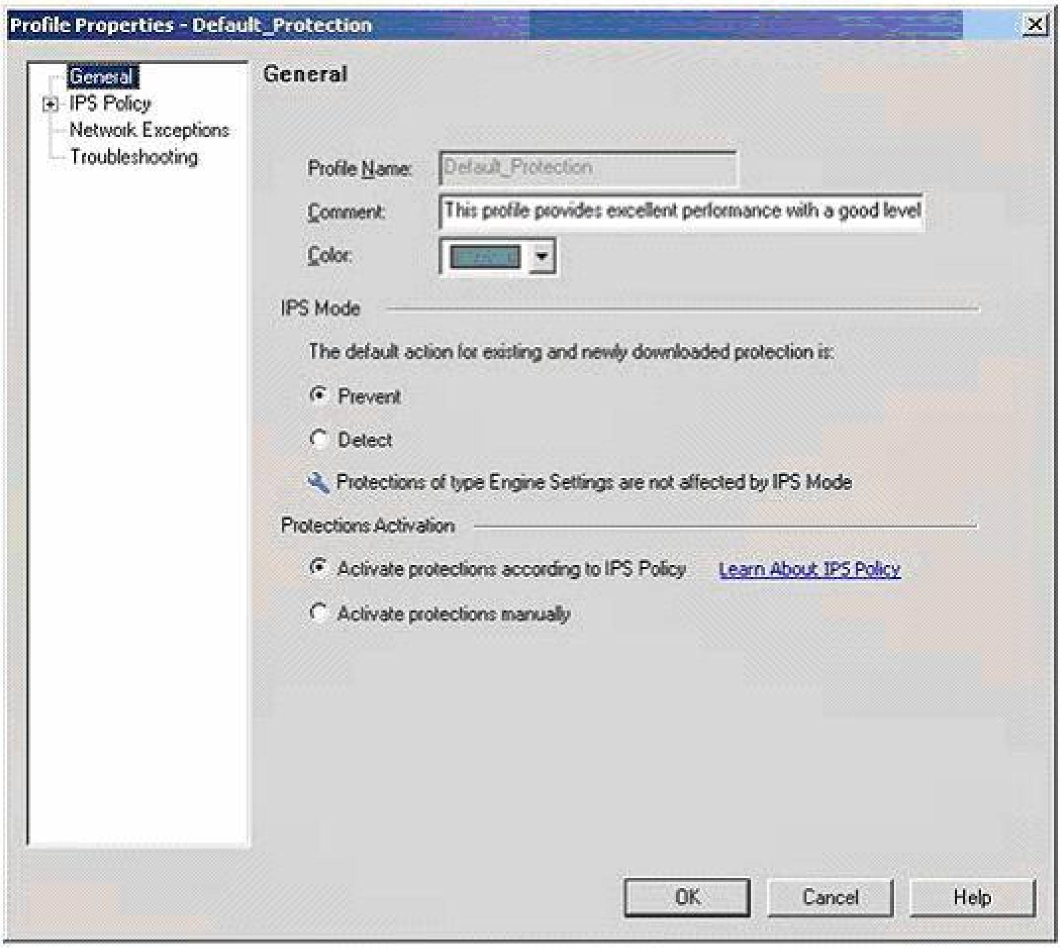
Profiles

Profiles

Create IPS profiles with specific settings for different gateways

Profile	IPS Mode	Activation	Protection Type	Troubleshooting	Comment
Default_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides excellent performance with a good level of protection
Recommended_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides the best security with a very good performance level

Figure 1: IPS Protections



Profile Properties - Default_Protection

General

Profile Name: Default_Protection

Comment: This profile provides excellent performance with a good level

Color:

IPS Mode

The default action for existing and newly downloaded protection is:

● Prevent

○ Detect

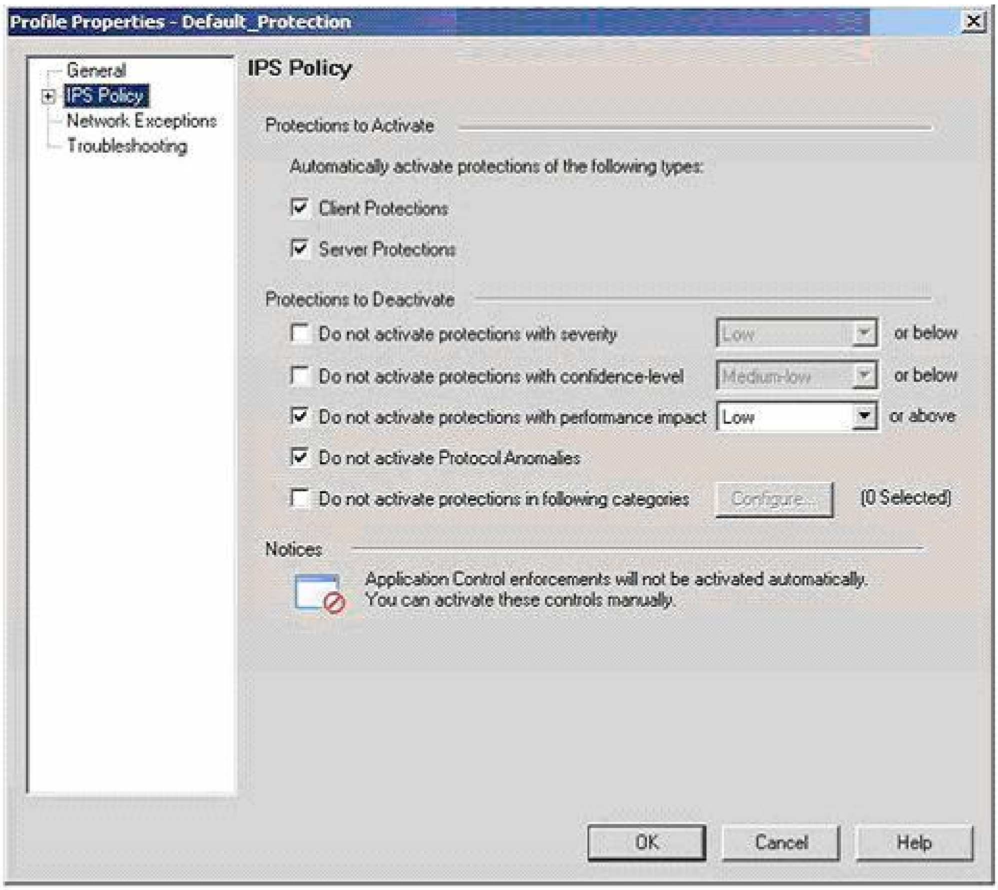
Protections of type Engine Settings are not affected by IPS Mode

Protections Activation

● Activate protections according to IPS Policy Learn About IPS Policy

○ Activate protections manually

Figure 2: Profiles Properties Window - General Page



IPS Policy

Protections to Activate

Automatically activate protections of the following types:

☑ Client Protections

☑ Server Protections

Protections to Deactivate

☐ Do not activate protections with severity Low or below

☐ Do not activate protections with confidence-level Medium-low or below

☑ Do not activate protections with performance impact Low or above

☑ Do not activate Protocol Anomalies

☐ Do not activate protections in following categories Configure... (0 Selected)

Notices

Application Control enforcements will not be activated automatically.
You can activate these controls manually.

Figure 3 : Profiles Properties Window - IPS Policy Page

A. SmartView Tracker may not be available to manage the IPS

B. This can also create a volume of logs and alerts that is difficult to manage

C. The protections with high security will be difficult to manage

D. The protections with low security will be difficult to manage

E. The performance will degrade

Answer: B

QUESTION NO: 323

SecurID, Check Point Password, OS Password, RADIUS and TACACS are types of what?

A. VPN schemes

B. Firewall schemes

C. Encryption schemes

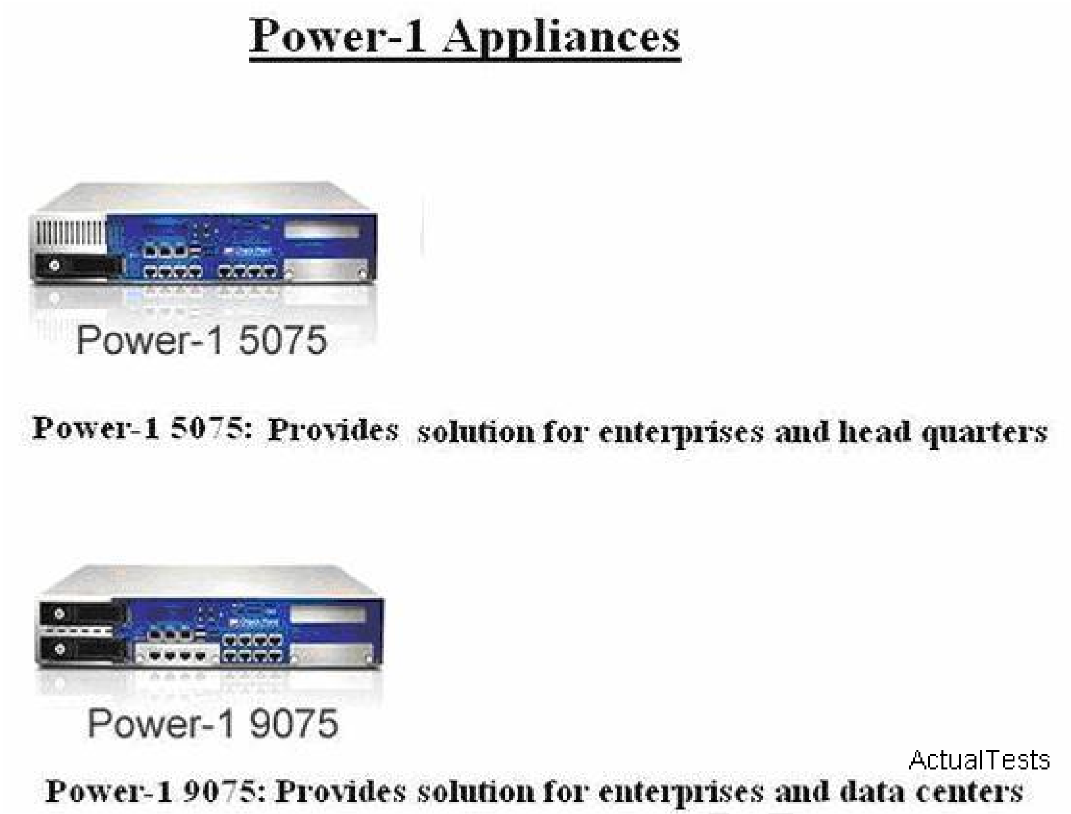
D. Authentication schemes

E. Authentication types

Answer: D

QUESTION NO: 324

Which of the Power-1 model will you choose for a large enterprise? Select all the correct answers.

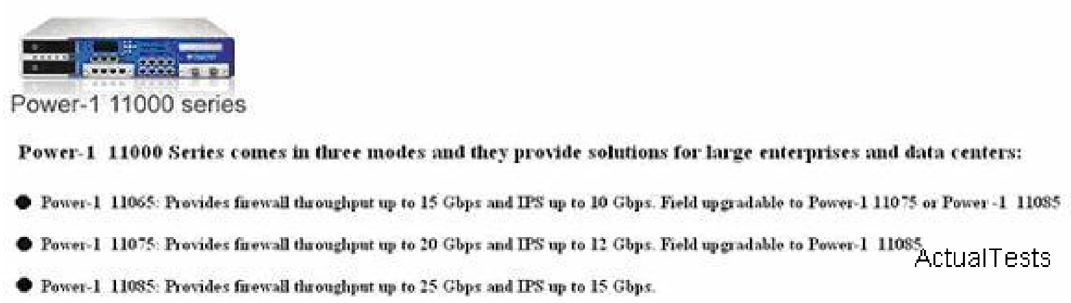


Power-1 5075
Power-1 9075

Power-1 Appliances

Power-1 5075: Provides solution for enterprises and head quarters

Power-1 9075: Provides solution for enterprises and data centers



Power-1 11000 series

Power-1 11000 Series comes in three modes and they provide solutions for large enterprises and data centers:

- Power-1 11065: Provides firewall throughput up to 15 Gbps and IPS up to 10 Gbps. Field upgradable to Power-1 11075 or Power -1 11085
- Power-1 11075: Provides firewall throughput up to 20 Gbps and IPS up to 12 Gbps. Field upgradable to Power-1 11085
- Power-1 11085: Provides firewall throughput up to 25 Gbps and IPS up to 15 Gbps.

A. 9075
B. 5075
C. 11085
D. 11025
E. 11065

Answer: C,E

QUESTION NO: 325

You can add licenses to the License & Contract Repository in which of the following ways?

A. Add License Details from CD

B. Add License Details Manually
C. DownloadFrom the User Center
D. Importing License Files
E. DownloadFrom the SmartDashboard

Answer: B,C,D

QUESTION NO: 326

R70 only supports which version of IPSO?

A. 5.0
B. 3.5
C. 6.0
D. 3.8
E. 4.0

Answer: C

QUESTION NO: 327

What are the benefits of Central Licensing?

A. The new license remains valid when changing the gateway IP address
B. Only one IP address is needed for all licenses
C. Multiple IP address are needed for all licenses
D. The licenses are revoked when changing the IP address of a Module
E. A license can be removed from one gateway and installed on another Module

Answer: A,B,E

QUESTION NO: 328

Which of the following is correct regarding R70 Licensing? Select all the correct answers.

A. License is required for SmartConsole management clients
B. Licenses are imported using the Check Point Configuration Tool or SmartUpdate
C. You can obtain a license key from theCheck Point User Center
D. Licenses are required for the Security Management server and security gateways
E. The Check Point software is activated using a certificate key, which is located on the back of the software media pack

Answer: B,C,D,E

QUESTION NO: 329

When performing Automatic Maintenance operation in Eventia Reporter, what is the recommended percentage you will specify for High Watermark?

A. 90%
B. 80%
C. 70%
D. 95%
E. 60%

Answer: B

QUESTION NO: 330

You are remote access user using SecureClient. You receive an IP of 10.1.1.1 which is entered into the headers of the IPSec packet. The packet is NATed. The packet's new source IP is 192.168.17.25. The Gateway decapsulates the NATed IP and decrypts the packet. The IP address is reverted to its original source IP of 10.1.1.1. There is an internal host with the same IP, and anti-spoofing is turned on the corporate LAN. Due to IP address duplicate, all your packets are dropped. To correct the this issue what Check Point Security Gateway feature will you implement?

A. IP address pool
B. Desktop Security
C. VPN Routing
D. Office Mode
E. SecuRemote

Answer: D

QUESTION NO: 331

Why do you not have to backup your configuration using upgrade_export.exe when performing an upgrade on SecurePlatform?

A. Because the Backup utility automatically does it for you during the upgrade
B. Because the Import utility automatically does it for you during the upgrade
C. Because you will have to run backup command at the end of the upgrade
D. Because the Export utility automatically does it for you during the upgrade

E. Because you will have to run restore command at the end of the upgrade

Answer: D

QUESTION NO: 332

How would you create or define a new user Template?

A. By going to SmartViewTracker , select Clients from Manage menu. In the emerging Users window, click on New button
B. By going to CheckPoint SmartDashboard, select Users menu. In the emerging Users window, click on New button
C. By going to CheckPoint SmartDashboard, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button
D. By going to SmartView Status, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button
E. By going to SmartView Tracker, select "Users and Administrators" from Manage menu. In the emerging Users window, click on New button

Answer: C

QUESTION NO: 333

How would you uninstall the Security Policy on the selected modules?

A. By choosing Uninstall from the Policy menu of SmartView Status GUI to uninstall the Security Policy on the selected modules
B. By choosing Uninstall from the Policy menu of SmartDashboard GUI to uninstall the Security Policy on the selected modules
C. By choosing Uninstall from the Manage menu of SmartDashboard to uninstall the Security Policy on the selected modules
D. By choosing Uninstall from the Policy menu of SmartView Tracker GUI to uninstall the Security Policy on the selected modules
E. By choosing Uninstall from the Window menu of SmartDashboard to uninstall the Security Policy on the selected modules

Answer: B

QUESTION NO: 334

Once you have finished configuring "CVP or UFP Inspection on any TCP Service", what is last step you will make to complete the implementation?

A. Install the security policy
B. Create a new service
C. Configured TCP resource
D. Install a resource
E. Create OPSEC Application

Answer: A

QUESTION NO: 335

Temporary loss of connection with the CRL repository or slight differences between clocks on the different machines may cause valid of CRLs to be considered invalid and hence, the certificates. To overcome this shortcoming, the VPN offers the:

A. Third Party PKI
B. CRL Grace Period
C. Certificates Removal List
D. Certificates Revocation List
E. PKI solutions

Answer: B

QUESTION NO: 336

Which of these authentication types is used to grant access on a per host basis?

A. Client authentication
B. Implicit Session authentication
C. Session authentication
D. User authentication
E. Transparent Session authentication

Answer: A

QUESTION NO: 337

What is a Security policy?

A. It's a set of rules that define your external network objects
B. It's a set of rules that define only your external network security
C. It's a set of rules that define your internal network objects

D. It's a set of rules that define your external network security

E. It's a set of rules that define your network security

Answer: E

QUESTION NO: 338

To prevent delays while large email files are scanned for Spam, what tool or feature will transfer email to the recipient while Anti-Spam detection takes place?

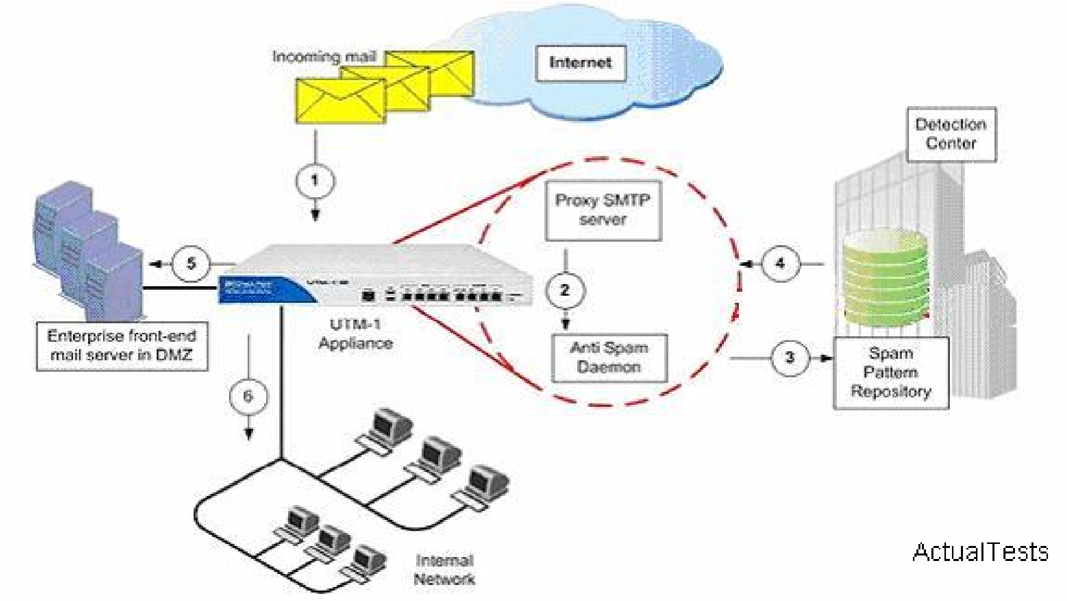


Figure 1: Mail Architecture

A. Adaptive Continuous Download

B. Pre-shared Secret

C. Anti-Spam Notification

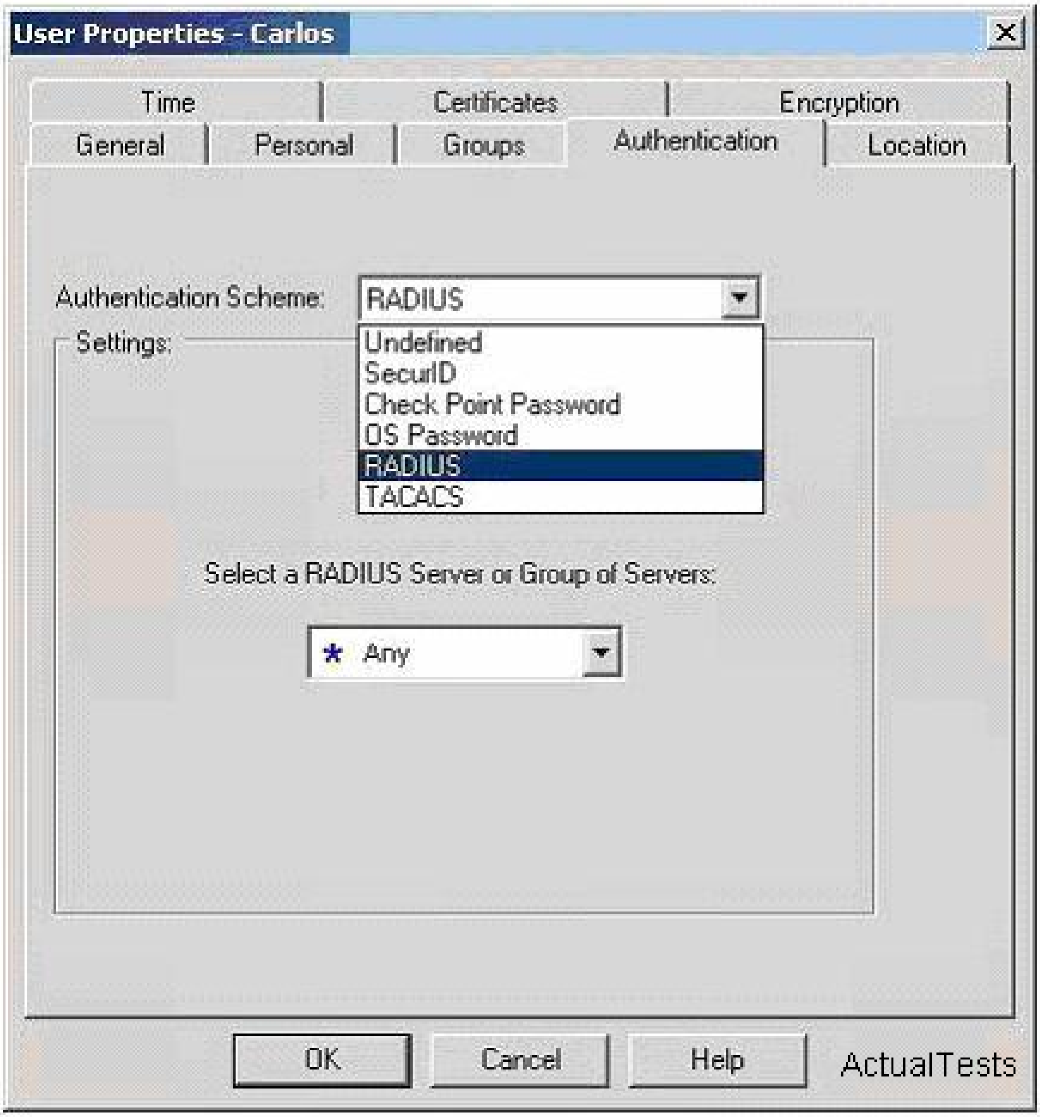
D. Anti-Spam Architecture

E. SmartDashboard

Answer: A

QUESTION NO: 339

How would you define an Authentication Scheme for a certain user?


User Properties - Carlos

Authentication Scheme: RADIUS

Settings:

Undefined
SecurID
Check Point Password
OS Password
RADIUS
TACACS

Select a RADIUS Server or Group of Servers: Any

A. Authentication scheme is defined for every user by SecurityGateway, no input is needed from the Administrator

B. By going to the FireWall Properties for that user, select the Authentication tab, and choose the desired scheme

C. By creating a workstation object to represent the PC that the user would log on from to perform the authentication, then select the Authentication tab, and choose the desired scheme

D. By going to the Workstation Properties of that user, select the Authentication tab, and choose the desired scheme

E. By going to the user Properties for that user, select the Authentication tab, and choose the desired scheme

Answer: E

QUESTION NO: 340

You are in the process of upgrading the licenses of your CheckPoint products, but you have not subscribed to one of these products. What is likely to happen to the upgrade?

A. All the licenses will be upgraded

B. All the licenses will be deleted

C. The license of the product that you have not subscribed to will be upgraded

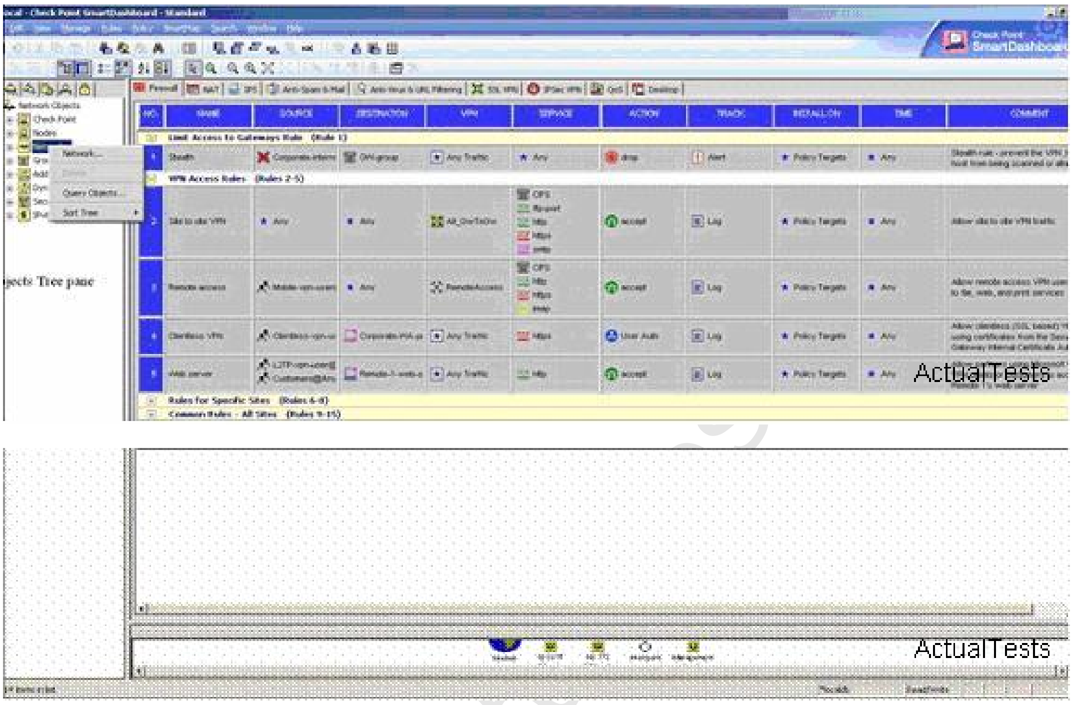
D. The license of the product that you have not subscribed to will not be upgraded

E. All the licenses will not be upgraded

Answer: D

QUESTION NO: 341

What would you use to create Security Policy rule?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Limit Access to Gateways Rule (Rule 1)										
1	Stealth	Corporate-intern	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	Stealth rule - prevent the VPN host from being scanned or att
VPN Access Rules (Rules 2-5)										
2	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any	Allow site to site VPN traffic
3	Remote access	Mobile-vpn-users	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any	Allow remote access VPN users to file, web, and print services
4	Clientless VPN	Clientless-vpn-u	Corporate-PIA-p	Any Traffic	https	User Auth	Log	Policy Targets	Any	Allow clientless (SSL based) using certificates from the Secu Gateway Internal Certificate Au
5	Web server	L2TP-vpn-users@ Customers@Any	Remote-1-web-s	Any Traffic	http	accept	Log	Policy Targets	Any	[illegible] Remote 1's web server
Rules for Specific Sites (Rules 6-8)										
Common Rules - All Sites (Rules 9-15)										

A. Firewall server Editor

B. SmartView Tracker

C. SmartDashboard

D. Firewall module Editor

E. SmartView Monitor

Answer: C

QUESTION NO: 342

Bidirectional NAT applies to which rules in the NAT Rule Base?

A. Hidden NAT rules

B. Automatic NAT rules

C. Manual NAT rules

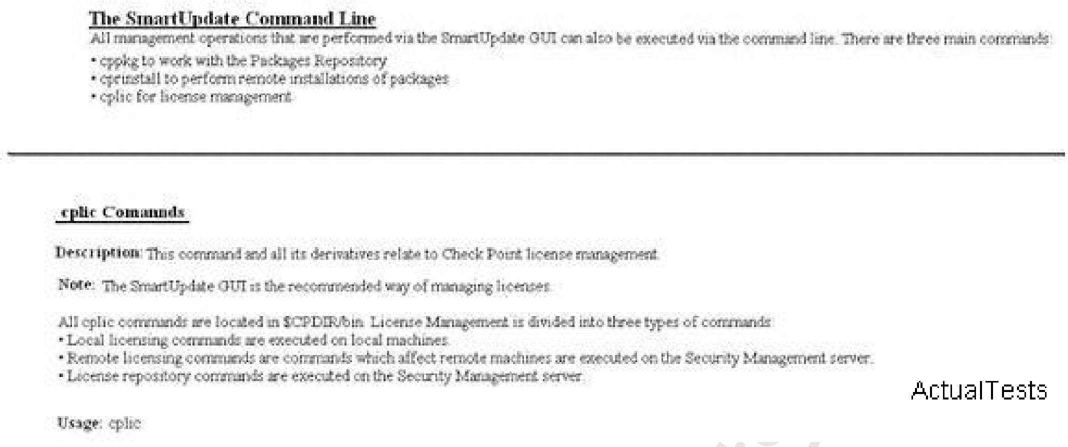
D. Implied rules

E. Static NAT rules

Answer: B

QUESTION NO: 343

What command will you use to retrieve licenses from the host 123.34.45.68?



The SmartUpdate Command Line

All management operations that are performed via the SmartUpdate GUI can also be executed via the command line. There are three main commands:

- cppkg to work with the Packages Repository
- cprinstall to perform remote installations of packages
- cplic for license management

cplic Comannds

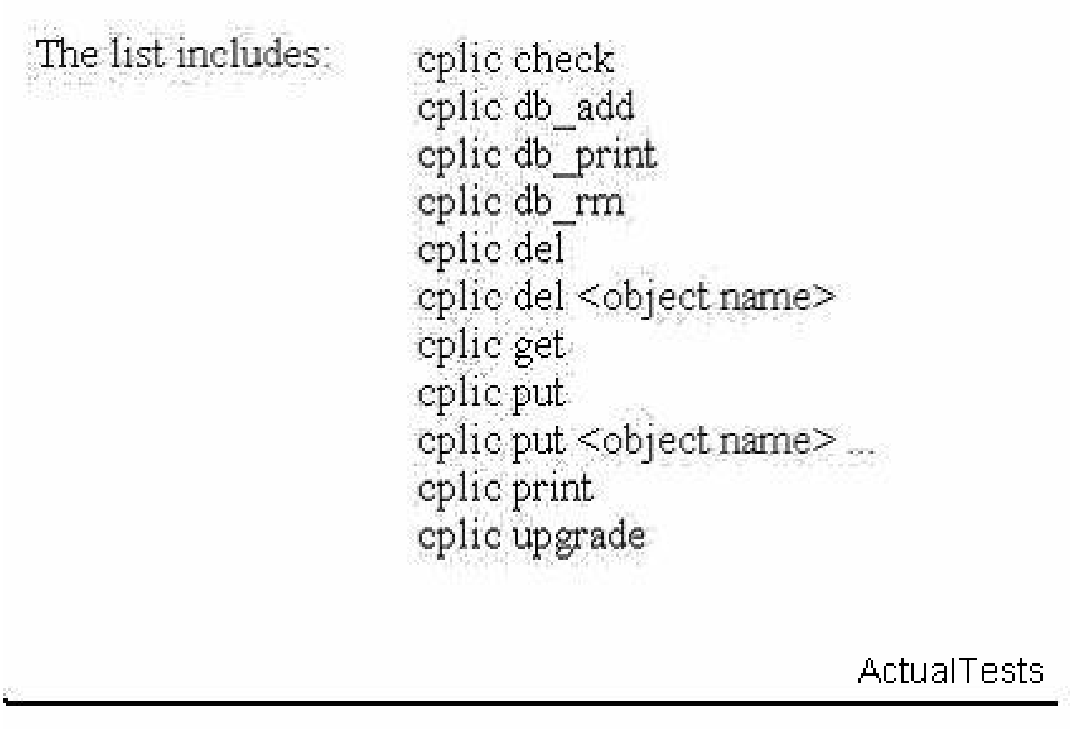
Description: This command and all its derivatives relate to Check Point license management.

Note: The SmartUpdate GUI is the recommended way of managing licenses.

All cplic commands are located in $CPDIR/bin. License Management is divided into three types of commands:

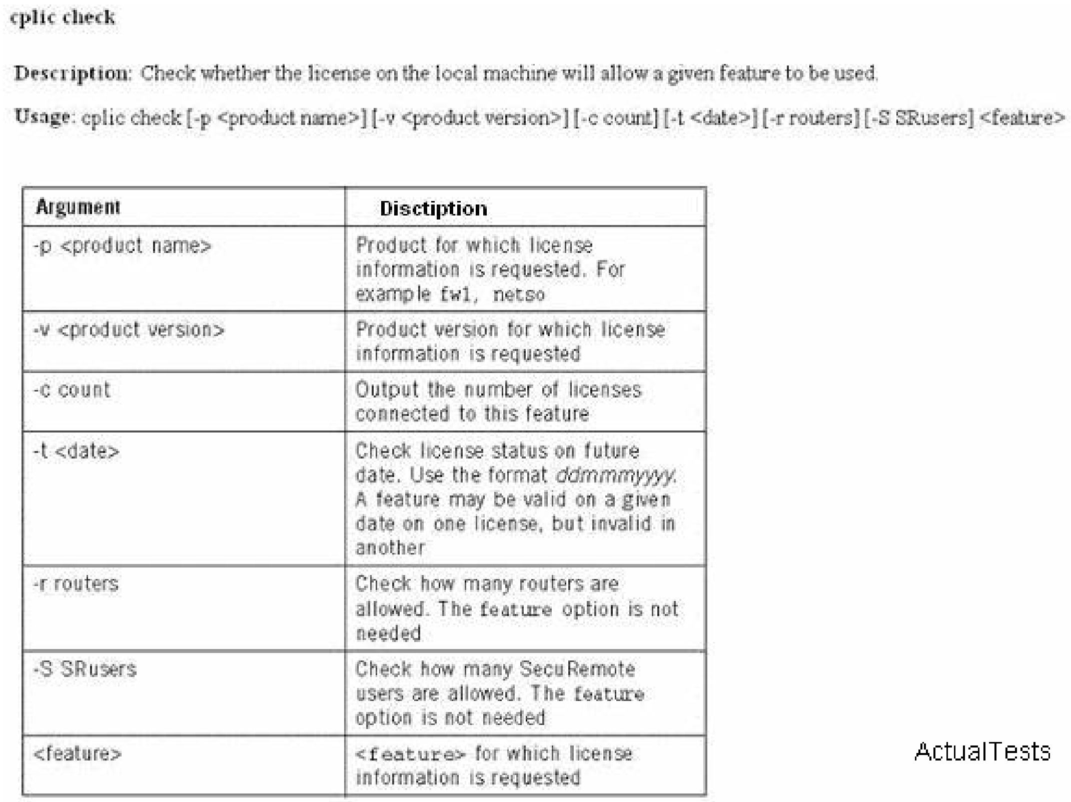
- Local licensing commands are executed on local machines.
- Remote licensing commands are commands which affect remote machines are executed on the Security Management server.
- License repository commands are executed on the Security Management server.

Usage: cplic



The list includes:

```
cplic check
cplic db_add
cplic db_print
cplic db_rm
cplic del
cplic del <object name>
cplic get
cplic put
cplic put <object name> ...
cplic print
cplic upgrade
```

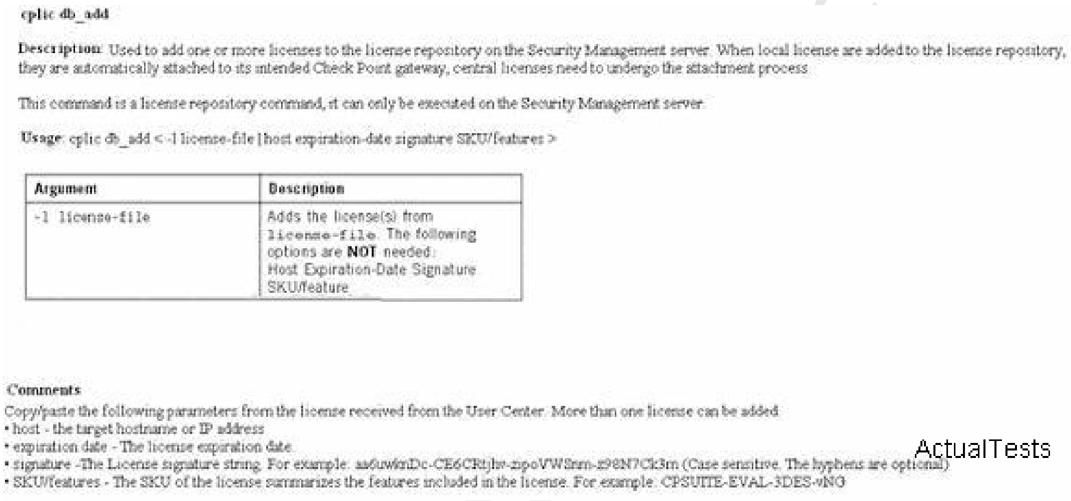


cplic check

Description: Check whether the license on the local machine will allow a given feature to be used.

Usage: cplic check [-p <product name>] [-v <product version>] [-c count] [-t <date>] [-r routers] [-S SRusers] <feature>

Argument	Disctiption
-p <product name>	Product for which license information is requested. For example fw1, netso
-v <product version>	Product version for which license information is requested
-c count	Output the number of licenses connected to this feature
-t <date>	Check license status on future date. Use the format *ddmmmyyyy.* A feature may be valid on a given date on one license, but invalid in another
-r routers	Check how many routers are allowed. The feature option is not needed
-S SRusers	Check how many SecuRemote users are allowed. The feature option is not needed
<feature>	<feature> for which license information is requested



cplic db_add

Description: Used to add one or more licenses to the license repository on the Security Management server. When local license are added to the license repository, they are automatically attached to its intended Check Point gateway, central licenses need to undergo the attachment process.

This command is a license repository command, it can only be executed on the Security Management server.

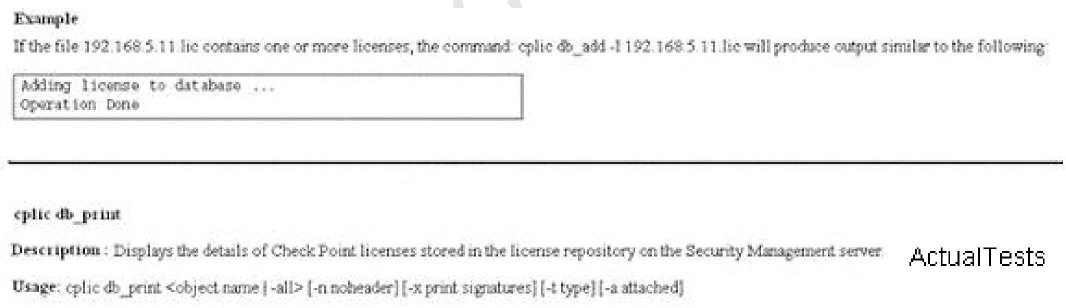
Usage: cplic db_add < -l license-file | host expiration-date signature SKU/features >

Argument	Description
-l license-file	Adds the license(s) from license-file. The following options are **NOT** needed: Host Expiration-Date Signature SKU/feature

Comments

Copy/paste the following parameters from the license received from the User Center. More than one license can be added.

- host - the target hostname or IP address
- expiration date - The license expiration date.
- signature -The License signature string. For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional)
- SKU/features - The SKU of the license summarizes the features included in the license. For example: CPSUITE-EVAL-3DES-vNG



Example

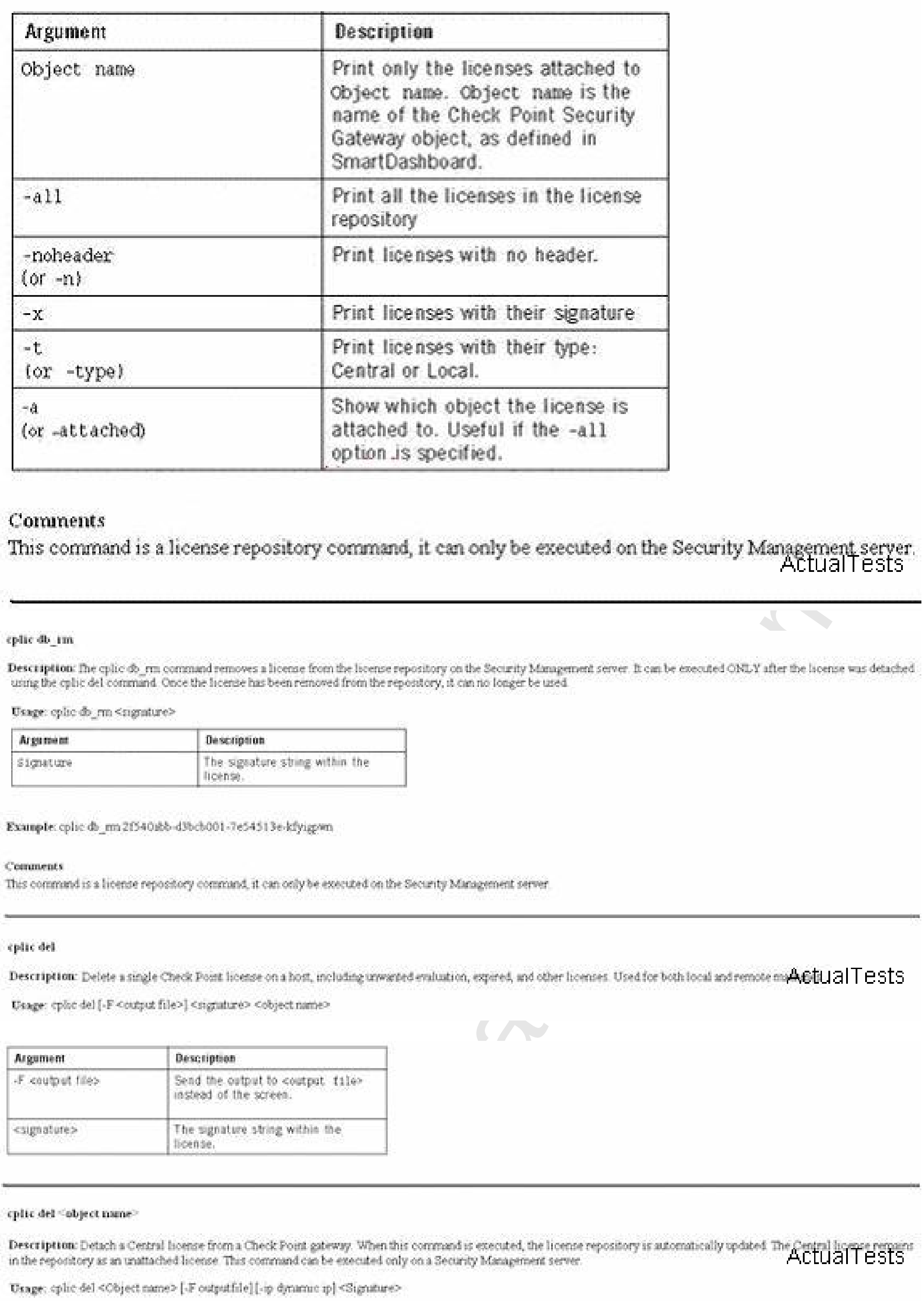
If the file 192.168.5.11.lic contains one or more licenses, the command: cplic db_add -l 192.168.5.11.lic will produce output similar to the following:

```
Adding license to database ...
Operation Done
```

cplic db_print

Description : Displays the details of Check Point licenses stored in the license repository on the Security Management server.

Usage: cplic db_print <object name | -all> [-n noheader] [-x print signatures] [-t type] [-a attached]



Argument	Description
Object name	Print only the licenses attached to Object name. Object name is the name of the Check Point Security Gateway object, as defined in SmartDashboard.
-all	Print all the licenses in the license repository
-noheader (or -n)	Print licenses with no header.
-x	Print licenses with their signature
-t (or -type)	Print licenses with their type: Central or Local.
-a (or -attached)	Show which object the license is attached to. Useful if the -all option is specified.

Comments

This command is a license repository command, it can only be executed on the Security Management server.

cplic db_rm

Description: The cplic db_rm command removes a license from the license repository on the Security Management server. It can be executed ONLY after the license was detached using the cplic del command. Once the license has been removed from the repository, it can no longer be used

Usage: cplic db_rm <signature>

Argument	Description
Signature	The signature string within the license.

Example: cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn

Comments

This command is a license repository command, it can only be executed on the Security Management server

cplic del

Description: Delete a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote management

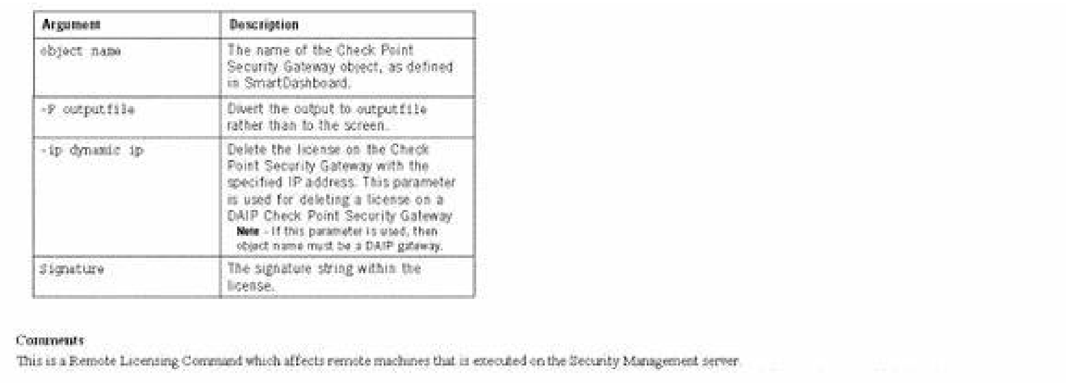
Usage: cplic del [-F <output file>] <signature> <object name>

Argument	Description
-F <output file>	Send the output to <output file> instead of the screen.
<signature>	The signature string within the license.

cplic del <object name>

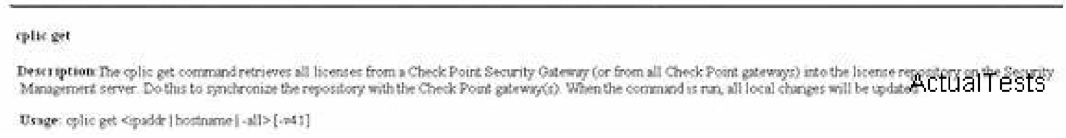
Description: Detach a Central license from a Check Point gateway. When this command is executed, the license repository is automatically updated. The Central license remains in the repository as an unattached license. This command can be executed only on a Security Management server.

Usage: cplic del <Object name> [-F outputfile] [-ip dynamic ip] <Signature>



Argument	Description
object name	The name of the Check Point Security Gateway object, as defined in SmartDashboard.
-F outputfile	Divert the output to outputfile rather than to the screen.
-ip dynamic ip	Delete the license on the Check Point Security Gateway with the specified IP address. This parameter is used for deleting a license on a DAIP Check Point Security Gateway **Note** - If this parameter is used, then object name must be a DAIP gateway.
Signature	The signature string within the license.

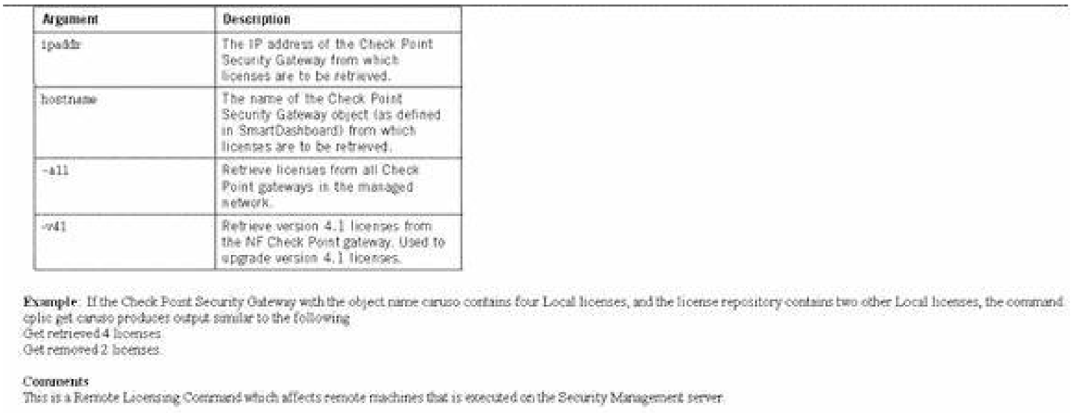
Comments
This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.



cplic get

Description The cplic get command retrieves all licenses from a Check Point Security Gateway (or from all Check Point gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Check Point gateway(s). When the command is run, all local changes will be update

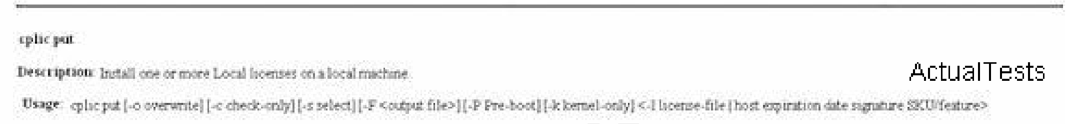
Usage: cplic get <ipaddr | hostname | -all> [-v41]



Argument	Description
ipaddr	The IP address of the Check Point Security Gateway from which licenses are to be retrieved.
hostname	The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved.
-all	Retrieve licenses from all Check Point gateways in the managed network.
-v41	Retrieve version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses.

Example: If the Check Point Security Gateway with the object name caruso contains four Local licenses, and the license repository contains two other Local licenses, the command cplic get caruso produces output similar to the following
Get retrieved 4 licenses.
Get removed 2 licenses.

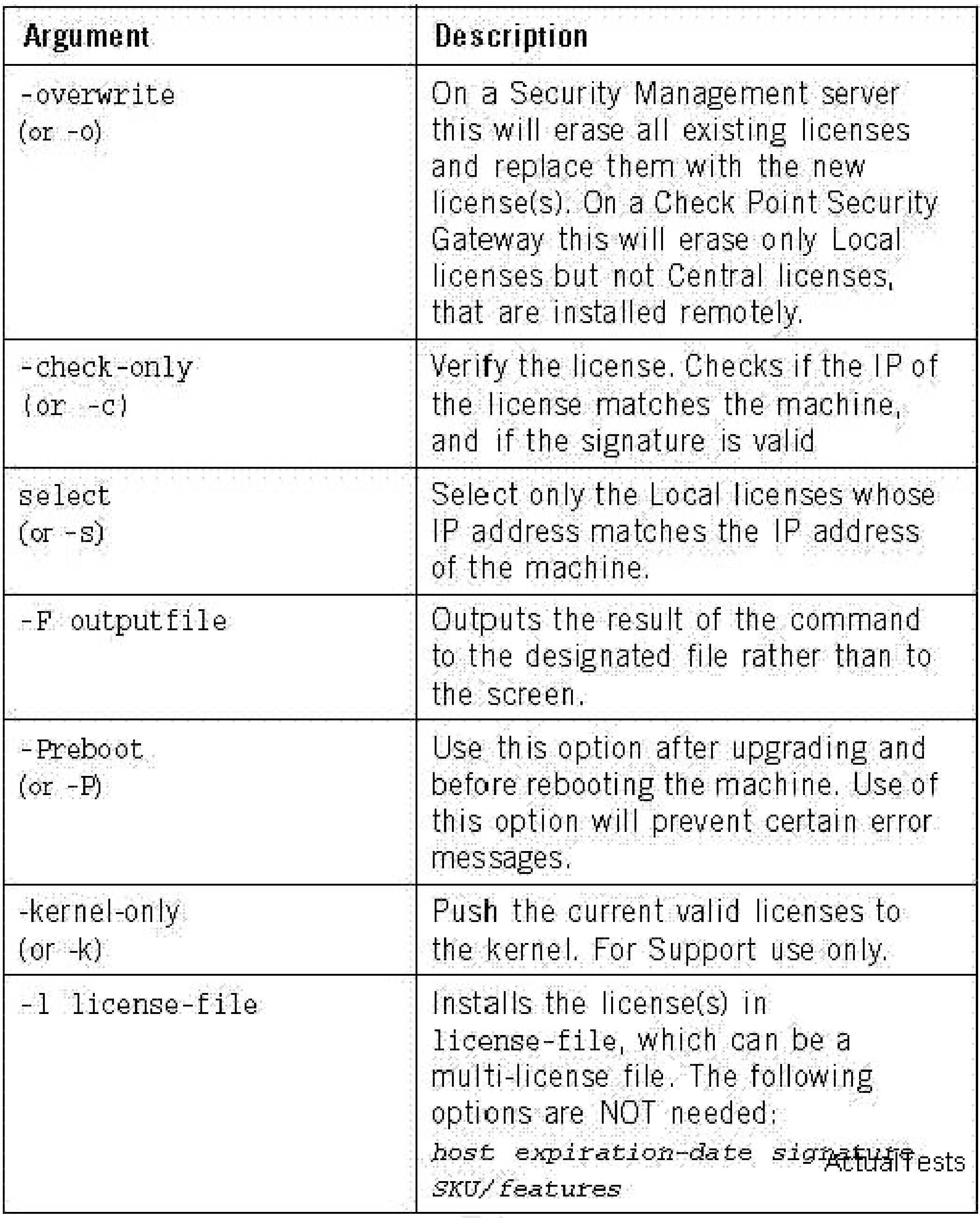
Comments
This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.



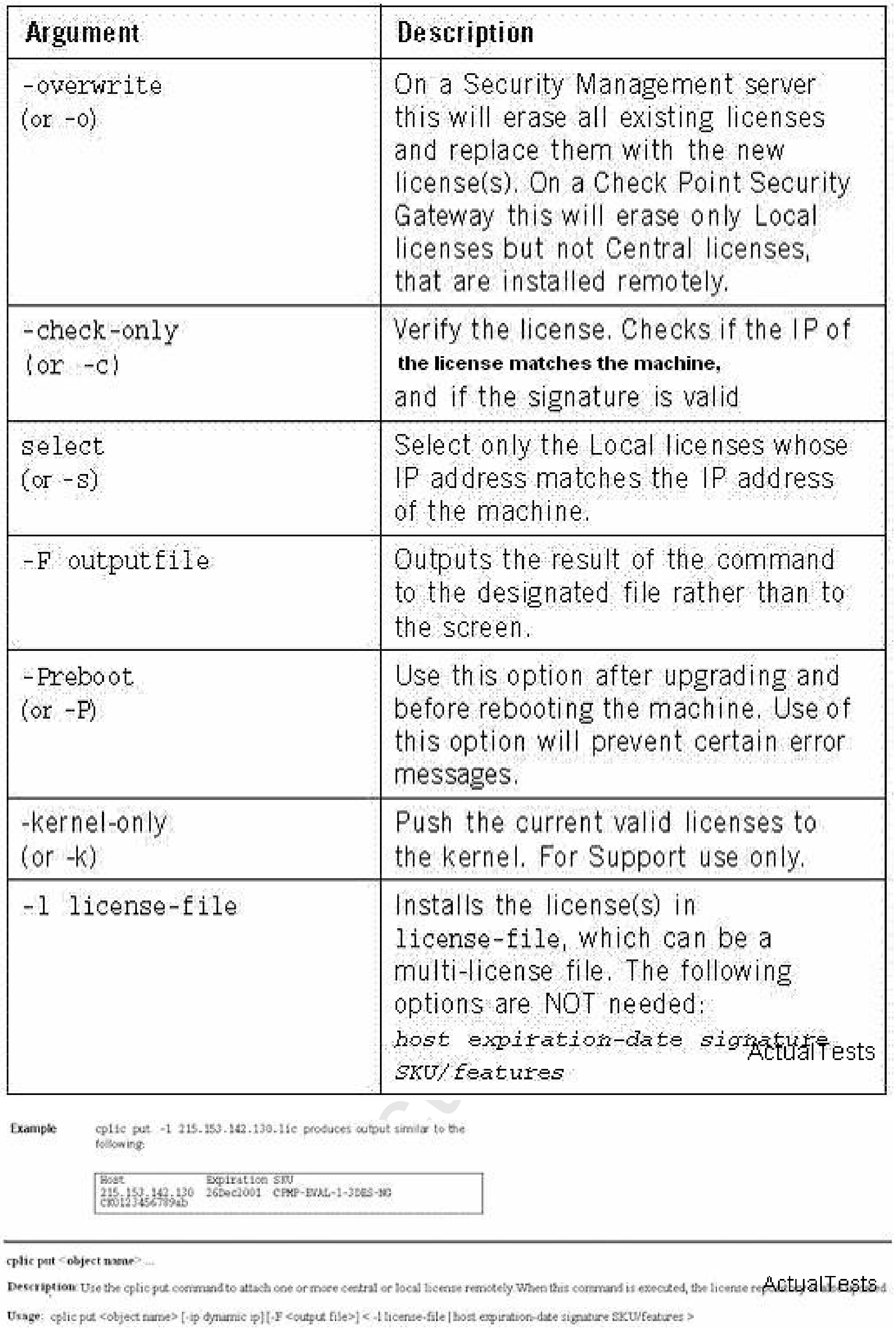
cplic put

Description: Install one or more Local licenses on a local machine.

Usage: cplic put [-o overwrite] [-c check-only] [-s select] [-F <output file>] [-P Pre-boot] [-k kernel-only] <-l license-file | host expiration date signature SKU/feature>



Argument	Description
-overwrite (or -o)	On a Security Management server this will erase all existing licenses and replace them with the new license(s). On a Check Point Security Gateway this will erase only Local licenses but not Central licenses, that are installed remotely.
-check-only (or -c)	Verify the license. Checks if the IP of the license matches the machine, and if the signature is valid
select (or -s)	Select only the Local licenses whose IP address matches the IP address of the machine.
-F outputfile	Outputs the result of the command to the designated file rather than to the screen.
-Preboot (or -P)	Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages.
-kernel-only (or -k)	Push the current valid licenses to the kernel. For Support use only.
-l license-file	Installs the license(s) in license-file, which can be a multi-license file. The following options are NOT needed: *host expiration-date signature SKU/features*



Argument	Description
-overwrite (or -o)	On a Security Management server this will erase all existing licenses and replace them with the new license(s). On a Check Point Security Gateway this will erase only Local licenses but not Central licenses, that are installed remotely.
-check-only (or -c)	Verify the license. Checks if the IP of **the license matches the machine,** and if the signature is valid
select (or -s)	Select only the Local licenses whose IP address matches the IP address of the machine.
-F outputfile	Outputs the result of the command to the designated file rather than to the screen.
-Preboot (or -P)	Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages.
-kernel-only (or -k)	Push the current valid licenses to the kernel. For Support use only.
-l license-file	Installs the license(s) in license-file, which can be a multi-license file. The following options are NOT needed: *host expiration-date signature SKU/features*

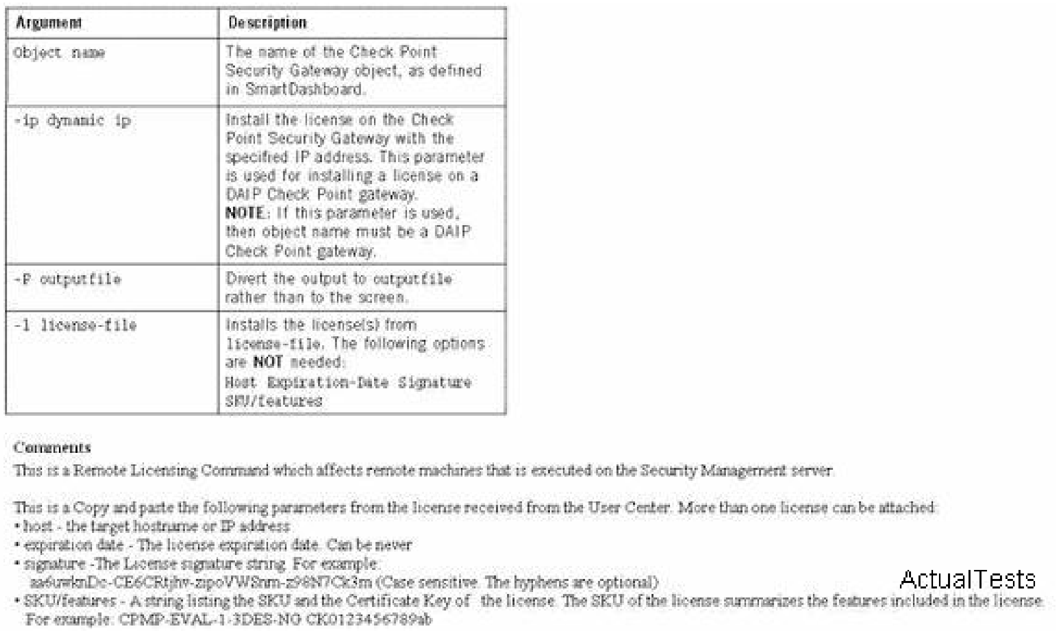
Example cplic put -l 215.153.142.130.lic produces output similar to the following:

```
Host             Expiration SKU
215.153.142.130  26Dec2001  CPMP-EVAL-1-3DES-NG
CK0123456789ab
```

cplic put <object name> ...

Description: Use the cplic put command to attach one or more central or local license remotely. When this command is executed, the license re[illegible]

Usage: cplic put <object name> [-ip dynamic ip] [-F <output file>] < -l license-file | host expiration-date signature SKU/features >



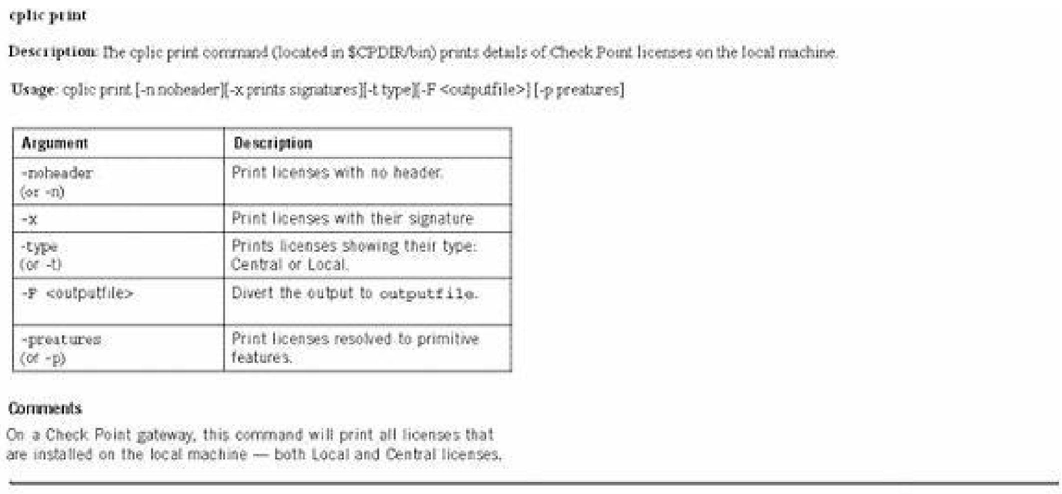
Argument	Description
Object name	The name of the Check Point Security Gateway object, as defined in SmartDashboard.
-ip dynamic ip	Install the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point gateway. **NOTE**: If this parameter is used, then object name must be a DAIP Check Point gateway.
-F outputfile	Divert the output to outputfile rather than to the screen.
-l license-file	Installs the license(s) from license-file. The following options are **NOT** needed: Host Expiration-Date Signature SKU/features

Comments

This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.

This is a Copy and paste the following parameters from the license received from the User Center. More than one license can be attached:

- host - the target hostname or IP address
- expiration date - The license expiration date. Can be never
- signature -The License signature string. For example: aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m (Case sensitive. The hyphens are optional)
- SKU/features - A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: CPMP-EVAL-1-3DES-NG CK0123456789ab



cplic print

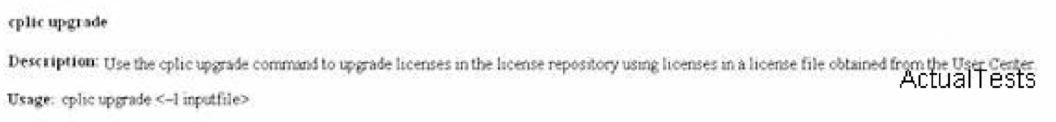
Description: The cplic print command (located in $CPDIR/bin) prints details of Check Point licenses on the local machine.

Usage: cplic print [-n noheader][-x prints signatures][-t type][-F <outputfile>] [-p preatures]

Argument	Description
-noheader (or -n)	Print licenses with no header.
-x	Print licenses with their signature
-type (or -t)	Prints licenses showing their type: Central or Local.
-F <outputfile>	Divert the output to outputfile.
-preatures (or -p)	Print licenses resolved to primitive features.

Comments

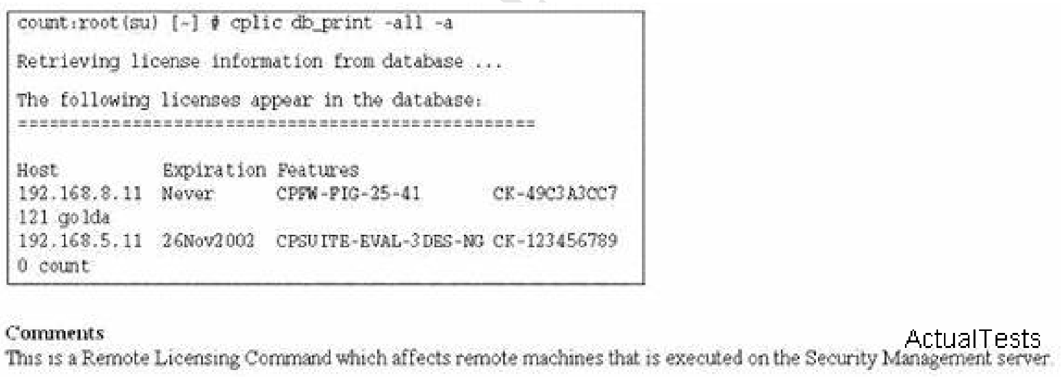
On a Check Point gateway, this command will print all licenses that are installed on the local machine — both Local and Central licenses.



cplic upgrade

Description: Use the cplic upgrade command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.

Usage: cplic upgrade <–l inputfile>



```
count:root(su) [-] # cplic db_print -all -a

Retrieving license information from database ...

The following licenses appear in the database:
==================================================

Host          Expiration Features
192.168.8.11  Never      CPFW-FIG-25-41       CK-49C3A3CC7
121 golda
192.168.5.11  26Nov2002  CPSUITE-EVAL-3DES-NG CK-123456789
0 count
```

Comments

This is a Remote Licensing Command which affects remote machines that is executed on the Security Management server.

A. cplic retrieve 123.34.45.68

B. cplic catch 123.34.68.45

C. cplic get 123.34.45.68

D. cplicdel 123.34.45.68

E. cplic out 123.34.45.68

Answer: C

QUESTION NO: 344

_______________ is a technique where an intruder attempts to gain unauthorized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges.

A. Services
B. IP Spoofing
C. SYNDefender
D. NAT
E. Anti-spoofing

Answer: B

QUESTION NO: 345

During the process of upgrading your gateway using SmartUpdate, what tool will display the list of gateways that can or cannot be upgraded?

A. newpkg
B. UnixInstallScript
C. cpconfig
D. cpinfo
E. Upgrade Verification

Answer: E

QUESTION NO: 346

What two services or protocols does the Client Authentication use to initiate connection to the firewall?

A. HTTP and HTTPS
B. HTTP and TCP
C. TELNET and RPC
D. HTTP and UDP
E. TELNET and HTTP

Answer: E

QUESTION NO: 347

When SecureClient is started, and before it connects to the Policy Server, it enforces a "default policy", which consists of the rules defined for all users in the last policy downloaded from the Policy Server. At what point does the default Policy cease to be enforced?

A. When the user reboots his/her laptop
B. When the Security Gateway initializes
C. There should be never a time when default policy ceases to enforce policy
D. When the user downloads an updated policy from a Security Management server
E. When the user downloads an updated policy from a Policy server

Answer: E

QUESTION NO: 348

Which of the following regarding Rule Base order is feasible?

A. Group accessed rules based on their creation dates
B. Place more frequently accessed rules before less frequently accessed rules
C. Always install the Rule Base frequently
D. Group similar accessed rules together
E. Place less frequently accessed rules before more frequently accessed rules

Answer: B

QUESTION NO: 349

What authentication type is not restricted to specific services, but provides a mechanism for authenticating any application, be it standard or custom?

A. User authentication
B. Data authentication
C. Session authentication
D. Client authentication
E. Transparent authentication

Answer: D

QUESTION NO: 350

If aggressive mode is not selected for your IPSec tunnel, the gateway defaults to main mode, performing the IKE negotiation using how many packets during phase 1 exchange?

A. 2
B. 3
C. 9
D. 12
E. 6

Answer: E

QUESTION NO: 351

To perform a new installation and manually import the configuration on Linux and Solaris, what tool will you run?

A. template
B. UnixInstallScript
C. cpinfo
D. cpconfig
E. LinuxInstallScript

Answer: B

QUESTION NO: 352

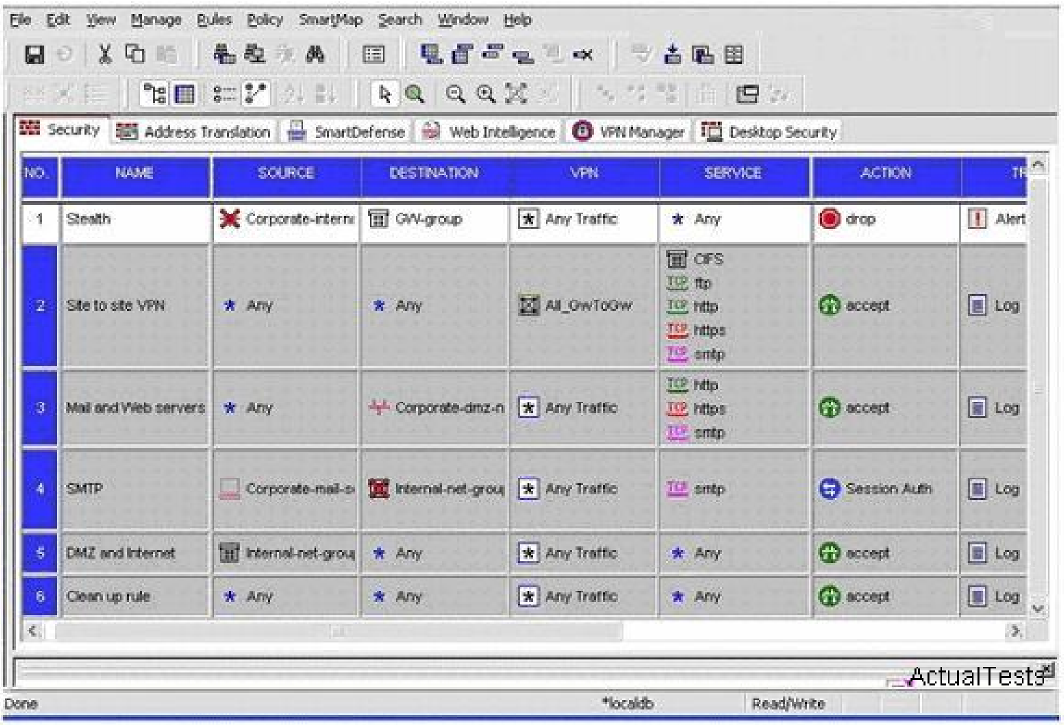
At present you run Traditional mode VPN configuration on all Gateways and policies. Your boss now decides to migrate or convert to simplified mode VPN due to its advantages. You want to implement this without any downtime. What is the easiest way to achieve this?

A. You will convert Gateway policies by using the simplified VPN wizard, and thenmigrate Gateway per Gateway
B. You will manually re-create Gateway for Gateway using Simple Mode wizard, then completely re-write the policies then install this on simplified VPN
C. There is now way to migrate without downtime
D. You will manually re-create Gateway for Gateway using SmartMap, then completely rewrite the policies then install this on simplified VPN
E. You will manually migrate each Gateway,then completely re-write the policies then install this on simplified VPN

Answer: A

QUESTION NO: 353

Examine the diagram and answer the question that follows. The action column on rule number4 is set to session Authentication. For session Authentication to work, what must be installed on user's PCs making connection?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TR
1	Stealth	Corporate-interna	GW-group	Any Traffic	Any	drop	Alert
2	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp http https smtp	accept	Log
3	Mail and Web servers	Any	Corporate-dmz-n	Any Traffic	http https smtp	accept	Log
4	SMTP	Corporate-mail-s	Internal-net-grou	Any Traffic	smtp	Session Auth	Log
5	DMZ and Internet	Internal-net-grou	Any	Any Traffic	Any	accept	Log
6	Clean up rule	Any	Any	Any Traffic	Any	accept	Log

A. System module
B. Checkpoint Client Authentication program
C. Checkpoint Session Authentication Agent
D. User Authentication program
E. Checkpoint Client Authentication Agent

Answer: C

QUESTION NO: 354

What mode in the SmartView Tracker enables you track changes made to objects in the RuleBase, and tracks general SmartDashboard usage?

A. Management Mode
B. Track Mode
C. Network & Endpoint Mode
D. Track Mode

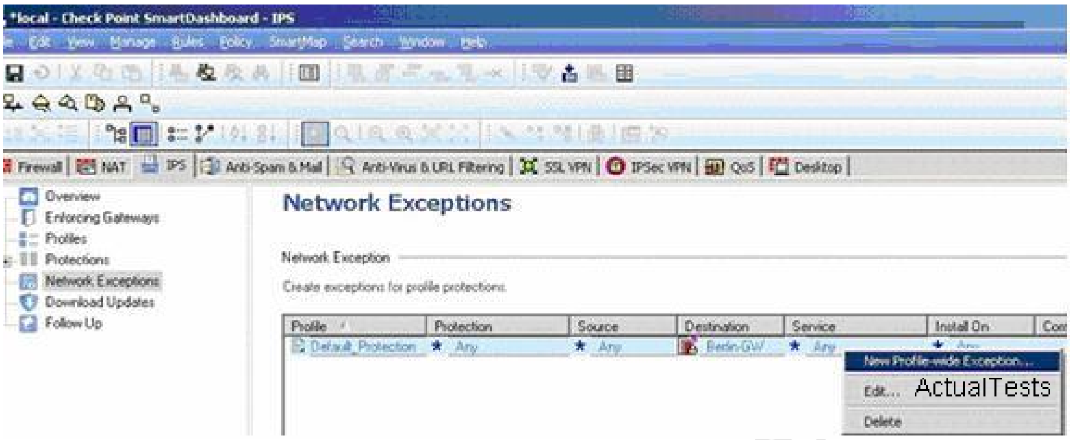
E. Active Mode

F. Connection Mode

Answer: A

QUESTION NO: 355

If you are creating a Network Exception rule and set the Source, Destination, and Service to Any, then you are:


*local - Check Point SmartDashboard - IPS
File Edit View Manage Rules Policy SmartMap Search Window Help
Firewall
NAT
IPS
Anti-Spam & Mail
Anti-Virus & URL Filtering
SSL VPN
IPSec VPN
QoS
Desktop
Overview
Enforcing Gateways
Profiles
Protections
Network Exceptions
Download Updates
Follow Up
New Profile-wide Exception...
Edit...
Delete

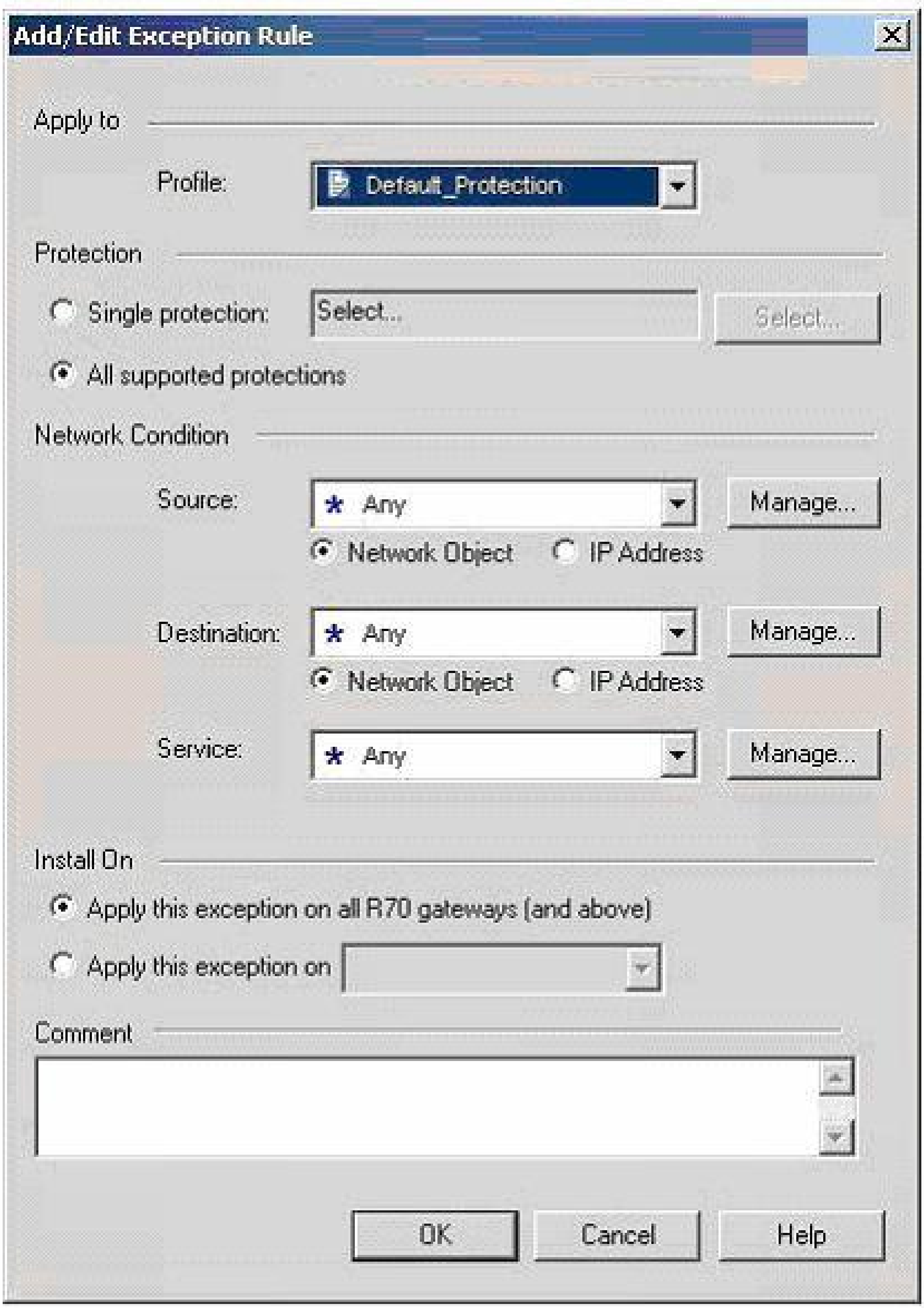
Network Exceptions

Network Exception

Create exceptions for profile protections.

Profile	Protection	Source	Destination	Service	Install On	Con
Default_Protection	★ Any	★ Any	Berlin-GW	★ Any	★ Any	

Figure 1: IPS Tab - Network Exceptions Page



Add/Edit Exception Rule

Apply to

Profile: Default_Protection

Protection

○ Single protection: Select...

● All supported protections

Network Condition

Source: * Any
● Network Object ○ IP Address

Destination: * Any
● Network Object ○ IP Address

Service: * Any

Install On

● Apply this exception on all R70 gateways (and above)

○ Apply this exception on

Comment

Figure 2: Add/Edit Exception Rule Window

A. In effect decipher the protection
B. In effect reset the protection
C. In effect rebooting the protection
D. In effect deactivating the protection
E. In effect installing the protection

Answer: D

QUESTION NO: 356

After running the converter wizard to convert a traditional mode VPN to a simplified mode VPN, what do you have to do ensure that the security policy is maintained?

A. Install the conversion
B. Review the Security Rule Base
C. Re-write the Rule Base
D. Verify the conversion
E. Review the conversion

Answer: B

QUESTION NO: 357

You place a new Gateway in your existing network which requires that you reconfigure your IP routing tables. You want all traffic that going from the one router to the other, first enters the first interface of gateway, and then passes to the other interface before been forwarded to the other router. Which of the following would you deploy to achieve this?

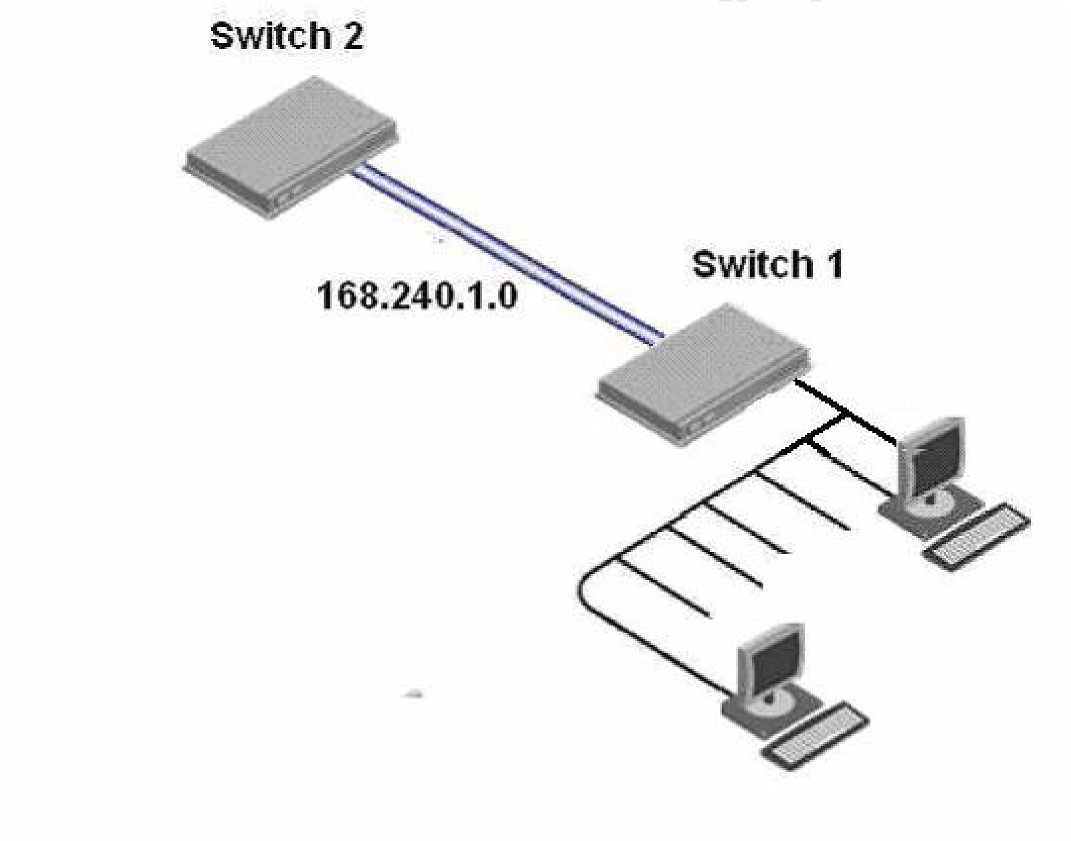


Figure 1: Network without bridge mode deployment

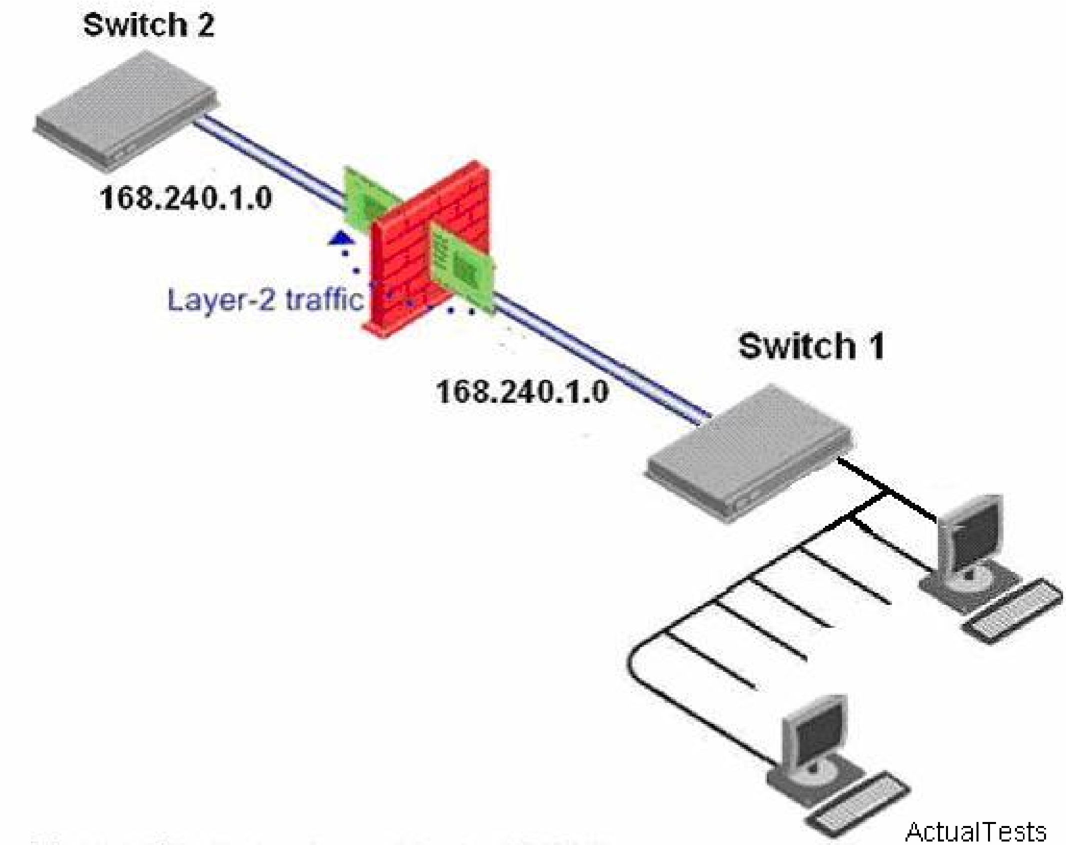


Figure 2: Deploying a Single VPN-1 gateway in bridge mode

A. Cluster Mode

B. Firewall Mode

C. Secure Mode

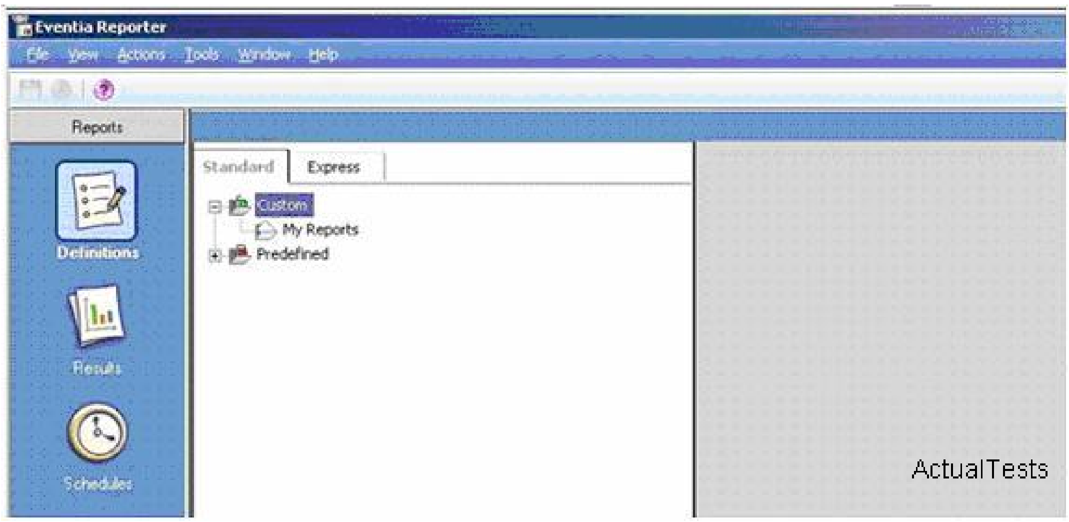
D. Hot Swipe Mode

E. Bridge Mode

Answer: E

QUESTION NO: 358

Which one of the following feature in the Eventia Reporter can you customize to your needs?



A. FireWall GX
B. Express
C. Standard
D. Database
E. My Reports

Answer: E

QUESTION NO: 359

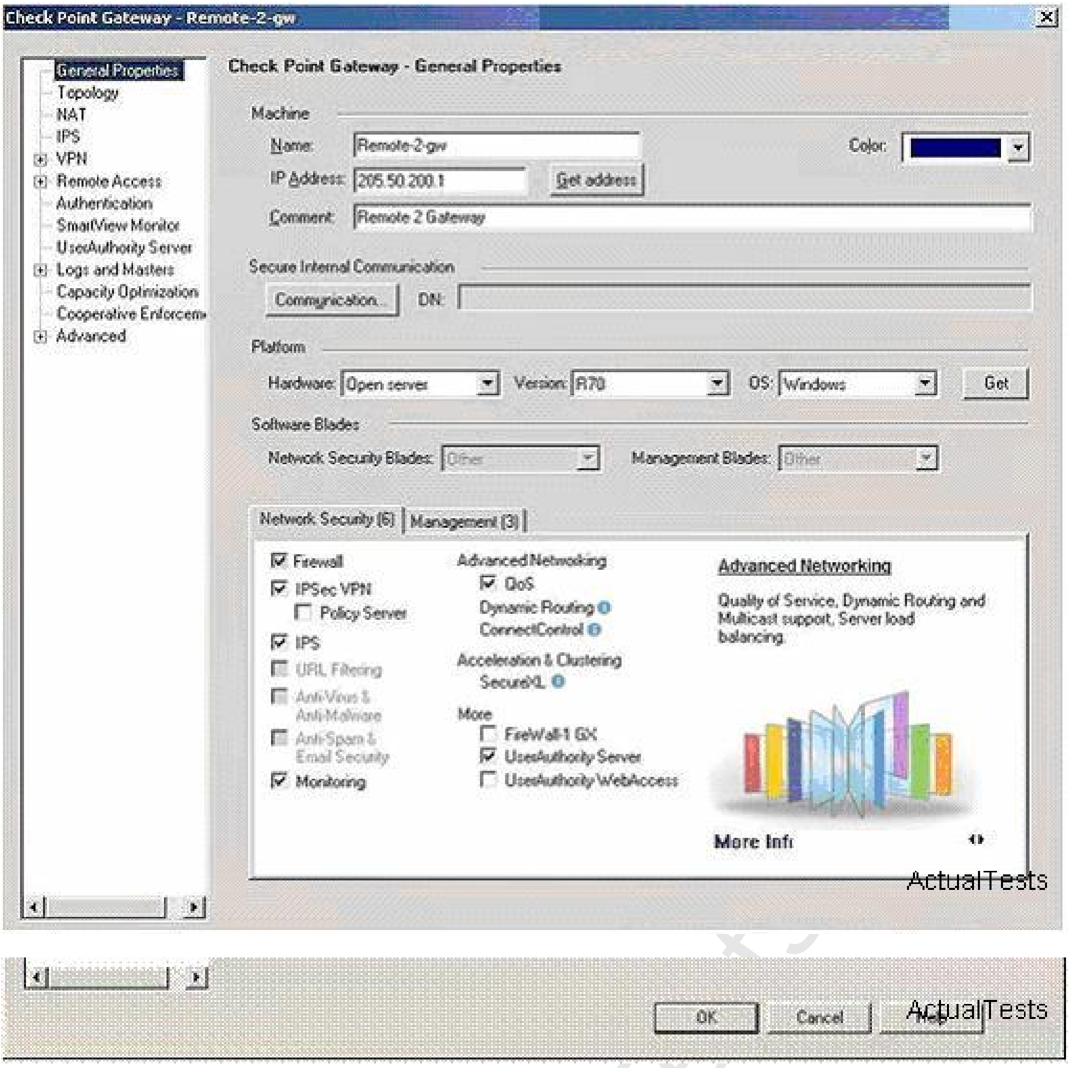
Before gateways can exchange encryption keys and build VPN tunnels, they first need to authenticate to each other. Gateways authenticate to each other either presenting a certificate or using:

A. Agreed Secret
B. Diffie-Hellman key
C. SVN
D. Pre-shared secret
E. SIC

Answer: D

QUESTION NO: 360

Which of the following is true regarding deployment of Software Blades? Select all the correct answers.



Check Point Gateway - Remote-2-gw

Check Point Gateway - General Properties

Machine

Name: Remote-2-gw

IP Address: 205.50.200.1

Comment: Remote 2 Gateway

Color:

Secure Internal Communication

DN:

Platform

Hardware: Open server

Version: R70

OS: Windows

Software Blades

Network Security Blades: Other

Management Blades: Other

Network Security (6) | Management (3)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ IPS
□ URL Filtering
□ Anti-Virus & Anti-Malware
□ Anti-Spam & Email Security
☑ Monitoring

Advanced Networking
☑ QoS
Dynamic Routing
ConnectControl

Acceleration & Clustering
SecureXL

More
□ FireWall-1 GX
☑ UserAuthority Server
□ UserAuthority WebAccess

Advanced Networking

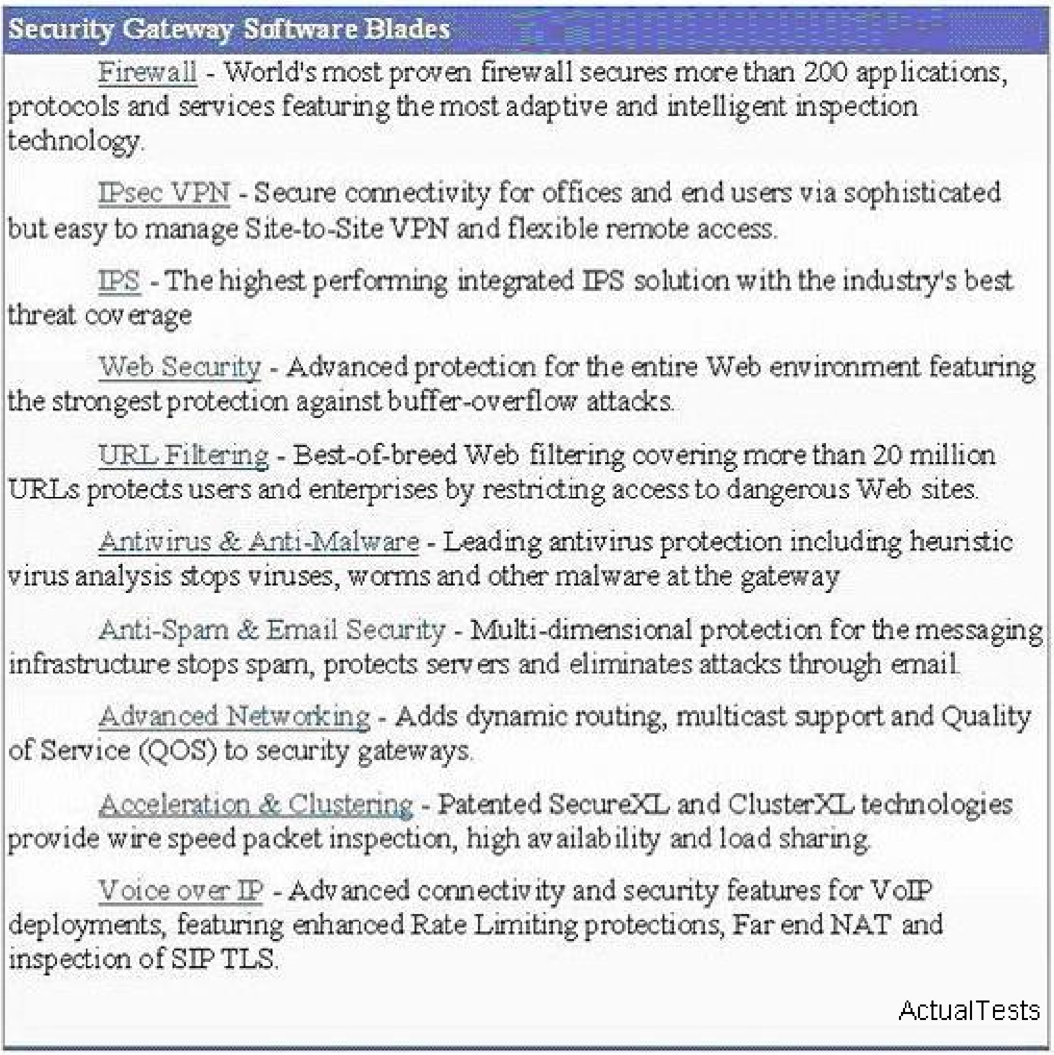
Quality of Service, Dynamic Routing and Multicast support, Server load balancing.

To configure Software Blades, go to General Properties of the Gateway to reveal two tabs towards the bottom of the box - Network Security and Management.

Click on More Info text to take you to Software Blades product website in the Check Point websites.

Click on ◂▸ for information on the descriptive items that can be configured in the two tabs.

Figure 1: Network Security tab



Security Gateway Software Blades

Firewall - World's most proven firewall secures more than 200 applications, protocols and services featuring the most adaptive and intelligent inspection technology.

IPsec VPN - Secure connectivity for offices and end users via sophisticated but easy to manage Site-to-Site VPN and flexible remote access.

IPS - The highest performing integrated IPS solution with the industry's best threat coverage

Web Security - Advanced protection for the entire Web environment featuring the strongest protection against buffer-overflow attacks.

URL Filtering - Best-of-breed Web filtering covering more than 20 million URLs protects users and enterprises by restricting access to dangerous Web sites.

Antivirus & Anti-Malware - Leading antivirus protection including heuristic virus analysis stops viruses, worms and other malware at the gateway

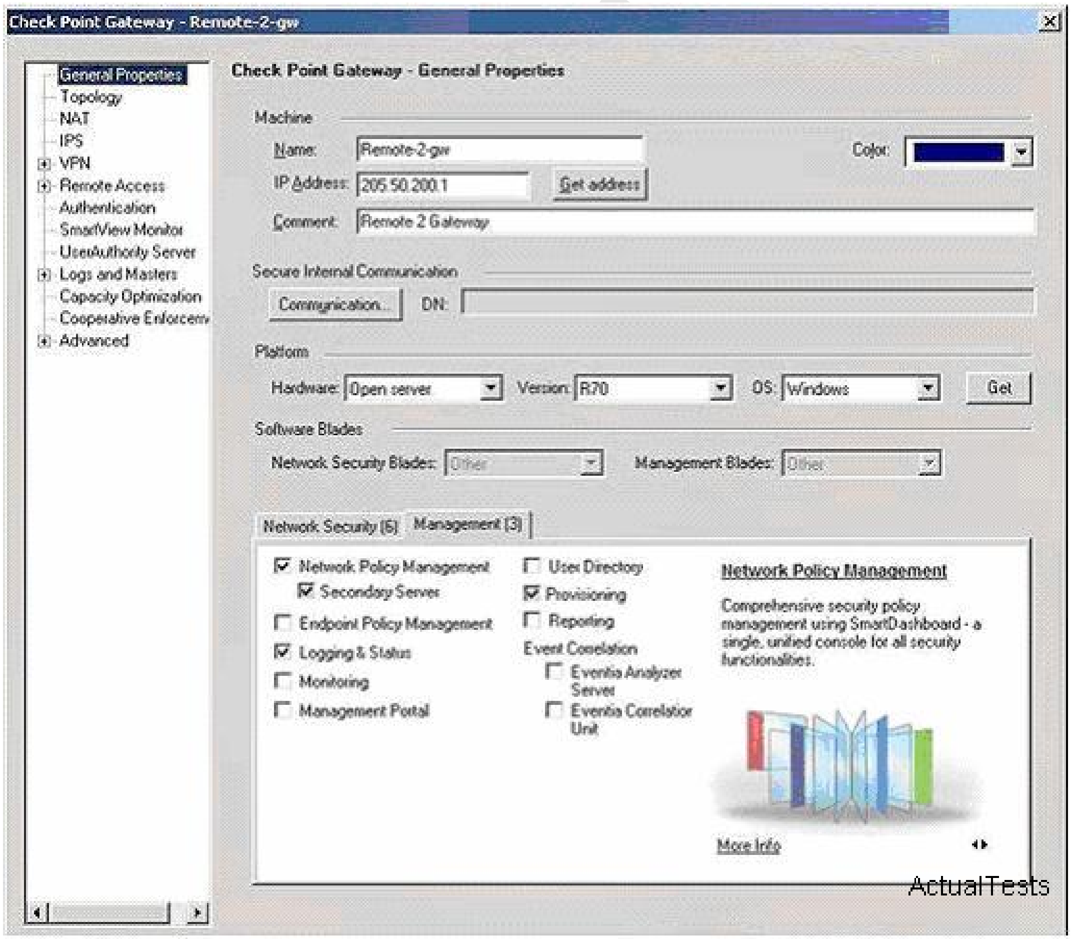
Anti-Spam & Email Security - Multi-dimensional protection for the messaging infrastructure stops spam, protects servers and eliminates attacks through email.

Advanced Networking - Adds dynamic routing, multicast support and Quality of Service (QOS) to security gateways.

Acceleration & Clustering - Patented SecureXL and ClusterXL technologies provide wire speed packet inspection, high availability and load sharing.

Voice over IP - Advanced connectivity and security features for VoIP deployments, featuring enhanced Rate Limiting protections, Far end NAT and inspection of SIP TLS.

ActualTests



Check Point Gateway - General Properties

Machine

Name: Remote-2-gw

IP Address: 205.50.200.1 Get address

Comment: Remote 2 Gateway

Color:

Secure Internal Communication

Communication... DN:

Platform

Hardware: Open server Version: R70 OS: Windows Get

Software Blades

Network Security Blades: Other Management Blades: Other

Network Security (6) Management (3)

☑ Network Policy Management

☑ Secondary Server

☐ Endpoint Policy Management

☑ Logging & Status

☐ Monitoring

☐ Management Portal

☐ User Directory

☑ Provisioning

☐ Reporting

Event Correlation

☐ Eventia Analyzer Server

☐ Eventia Correlation Unit

Network Policy Management

Comprehensive security policy management using SmartDashboard - a single, unified console for all security functionalities.

More Info

ActualTests

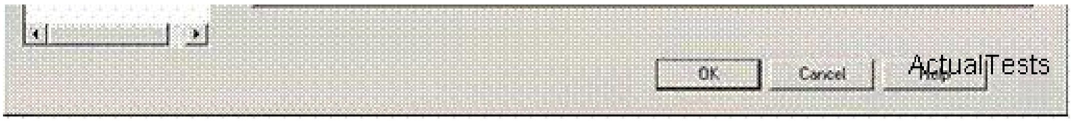
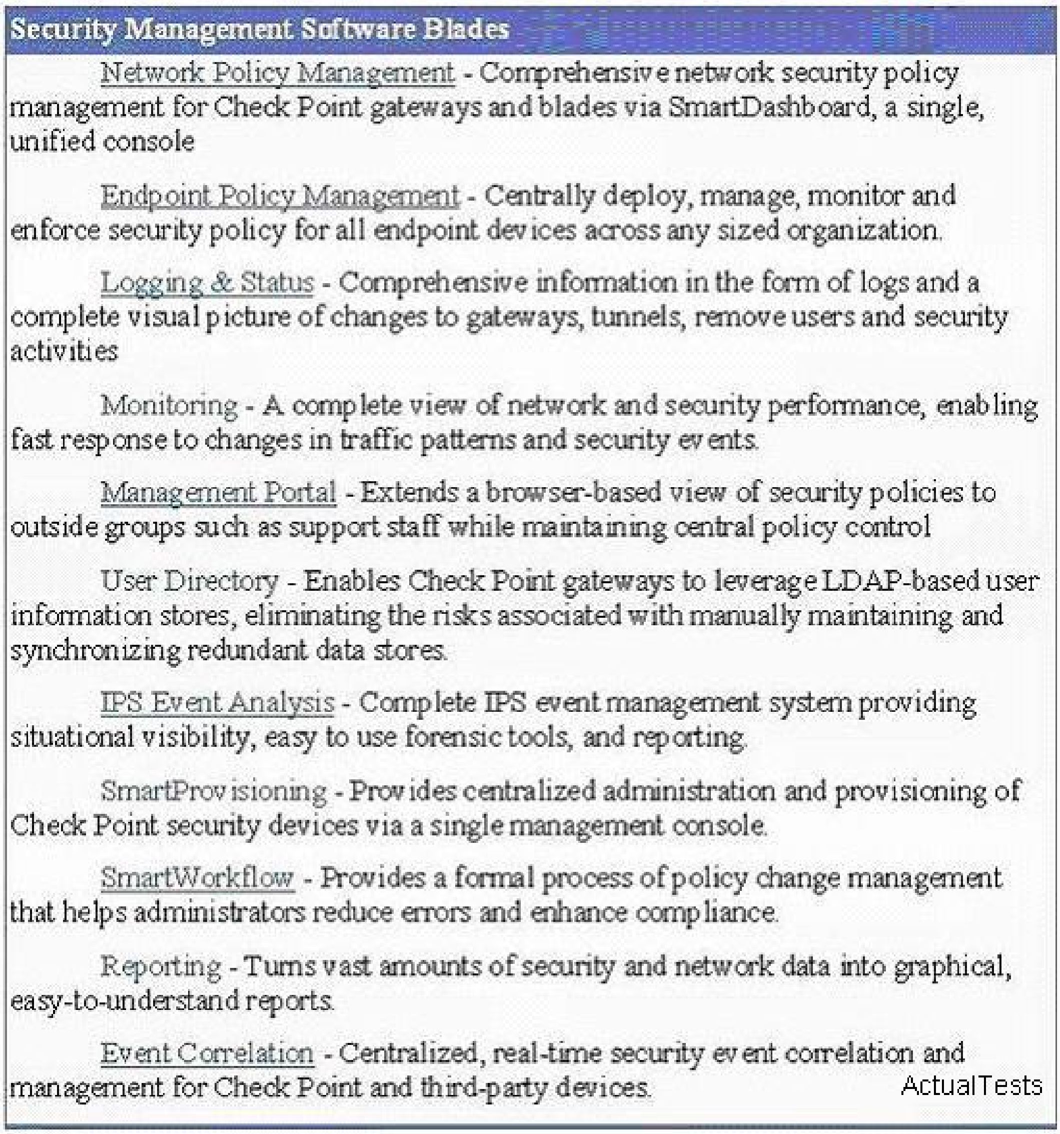


Figure 2: Management tab



Security Management Software Blades

Network Policy Management - Comprehensive network security policy management for Check Point gateways and blades via SmartDashboard, a single, unified console

Endpoint Policy Management - Centrally deploy, manage, monitor and enforce security policy for all endpoint devices across any sized organization.

Logging & Status - Comprehensive information in the form of logs and a complete visual picture of changes to gateways, tunnels, remove users and security activities

Monitoring - A complete view of network and security performance, enabling fast response to changes in traffic patterns and security events.

Management Portal - Extends a browser-based view of security policies to outside groups such as support staff while maintaining central policy control

User Directory - Enables Check Point gateways to leverage LDAP-based user information stores, eliminating the risks associated with manually maintaining and synchronizing redundant data stores.

IPS Event Analysis - Complete IPS event management system providing situational visibility, easy to use forensic tools, and reporting.

SmartProvisioning - Provides centralized administration and provisioning of Check Point security devices via a single management console.

SmartWorkflow - Provides a formal process of policy change management that helps administrators reduce errors and enhance compliance.

Reporting - Turns vast amounts of security and network data into graphical, easy-to-understand reports.

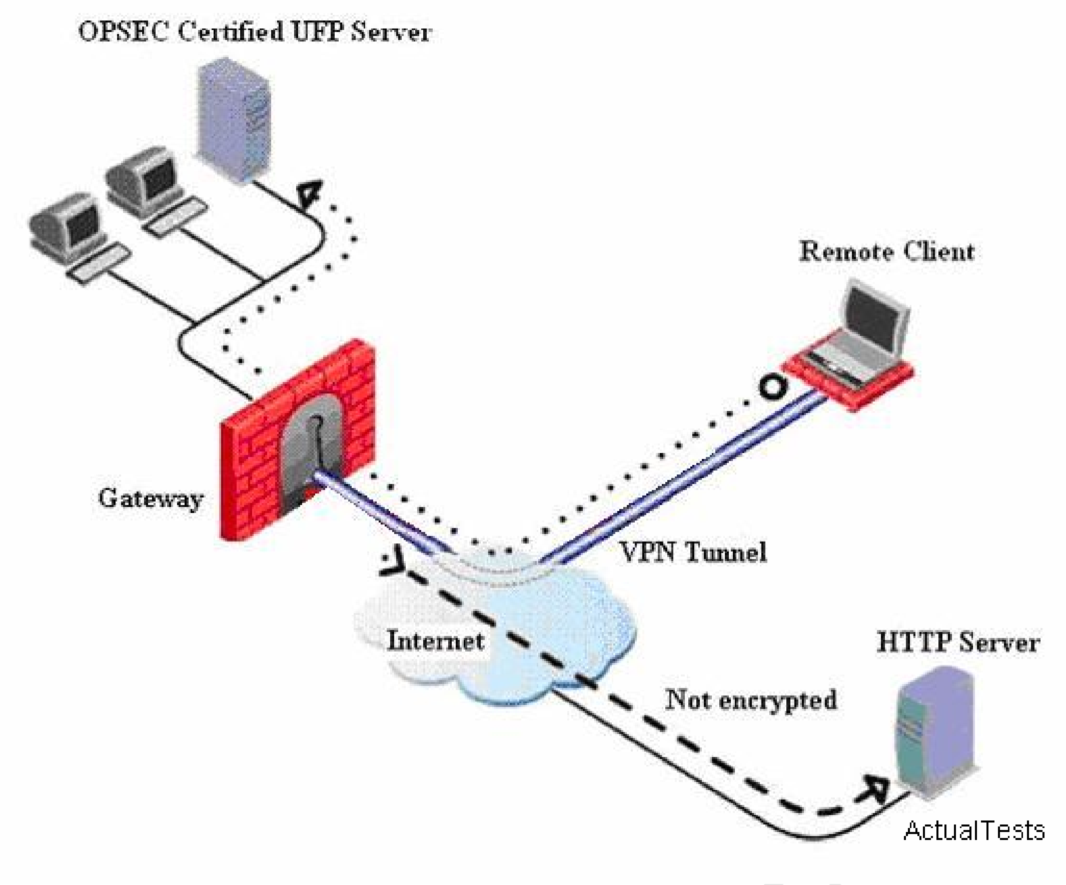
Event Correlation - Centralized, real-time security event correlation and management for Check Point and third-party devices.

A. When addinga software blades, upgrading the existing drivers must be done
B. Software blades can be deployed on UTM-1
C. Software blades can be deployed on open servers
D. Software blades can be deployed on Power-1
E. New software blades can be easily added to the existing hardware platform by simply turning on their functionality

Answer: B,C,D,E

QUESTION NO: 361

A remote client needs to access an HTTP server on the Internet as shown in the diagram. What will be the consequence If you NAT-ed the address of the remote client behind the Gateway?



A. The NAT-ing prevents the HTTP server on the Internet from replying directly to the client
B. The NAT-ing prevents the Anti-spoofing law from been enforced on the client
C. The NAT-ing prevents the Anti-spoofing law from been enforced on the Security Gateway
D. There should not be any consequence if NAT-ed
E. The NAT-ing allows the HTTP server on the Internet to reply directly to the client

Answer: A

QUESTION NO: 362

The diagram shows CVP Inspection process during an FTP Connection. The communication normally, should take place at port 21. What is likely to happen if the client initiates a data transfer over port 20? Choose the best answer.

FIGURE 12-3 CVP Inspection process during an FTP Connection

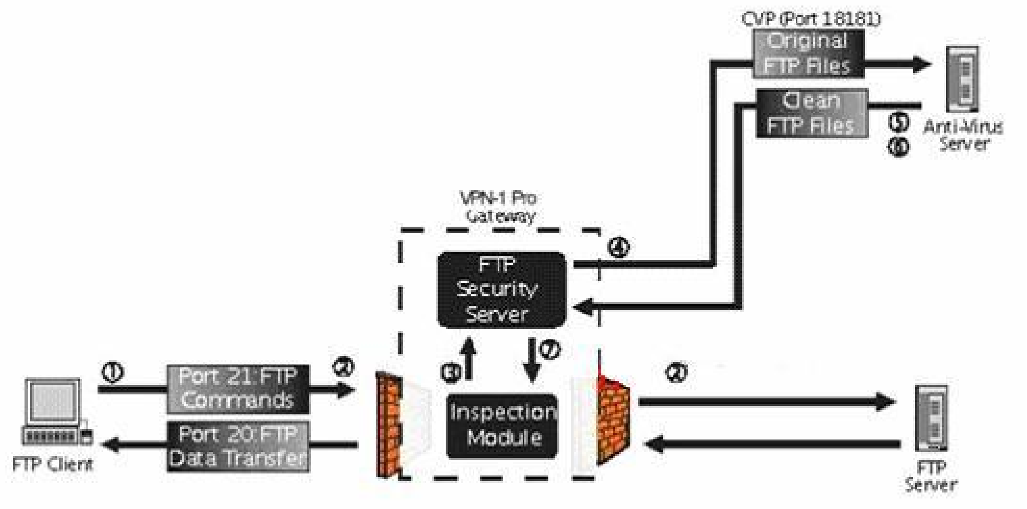


FIGURE 1: CVP Inspection process during an FTP Connection

A. The Inspection Module sends ACK to the client

B. The Inspection Module folds or diverts the connection into the FTP Security Server

C. The Inspection Module drops the connection

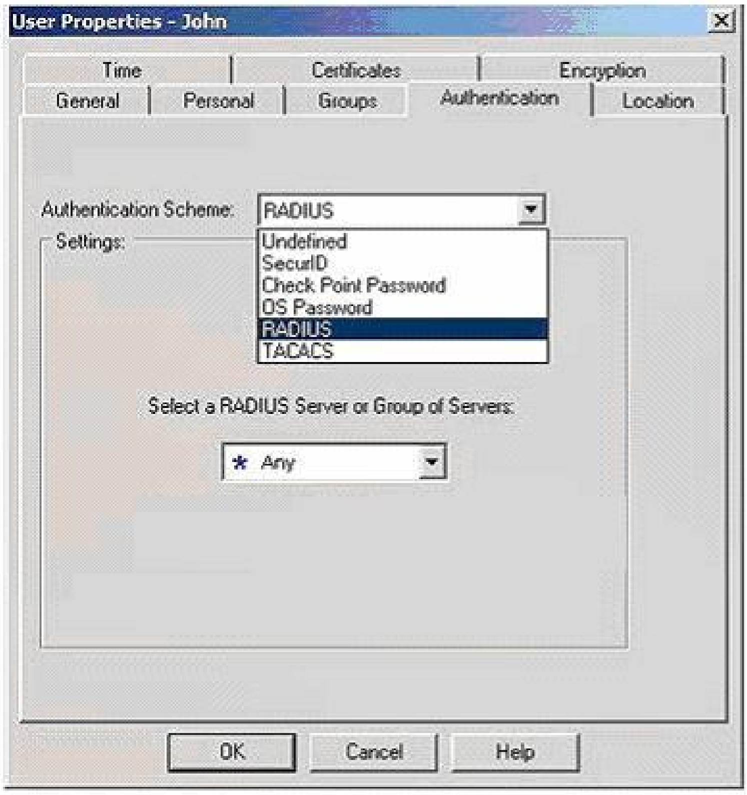
D. The Firewall block the connection

E. The Inspection Module sends SYC/ACK to the client

Answer: B

QUESTION NO: 363

Your new System Administrator is setting up User Authentication for the very first time. After the setting up she tests it but does not work. You then ask her to follow the CheckPoint recommendation for troubleshooting. What is the Checkpoint recommended way to troubleshoot this?



User Properties - John

Authentication Scheme: RADIUS

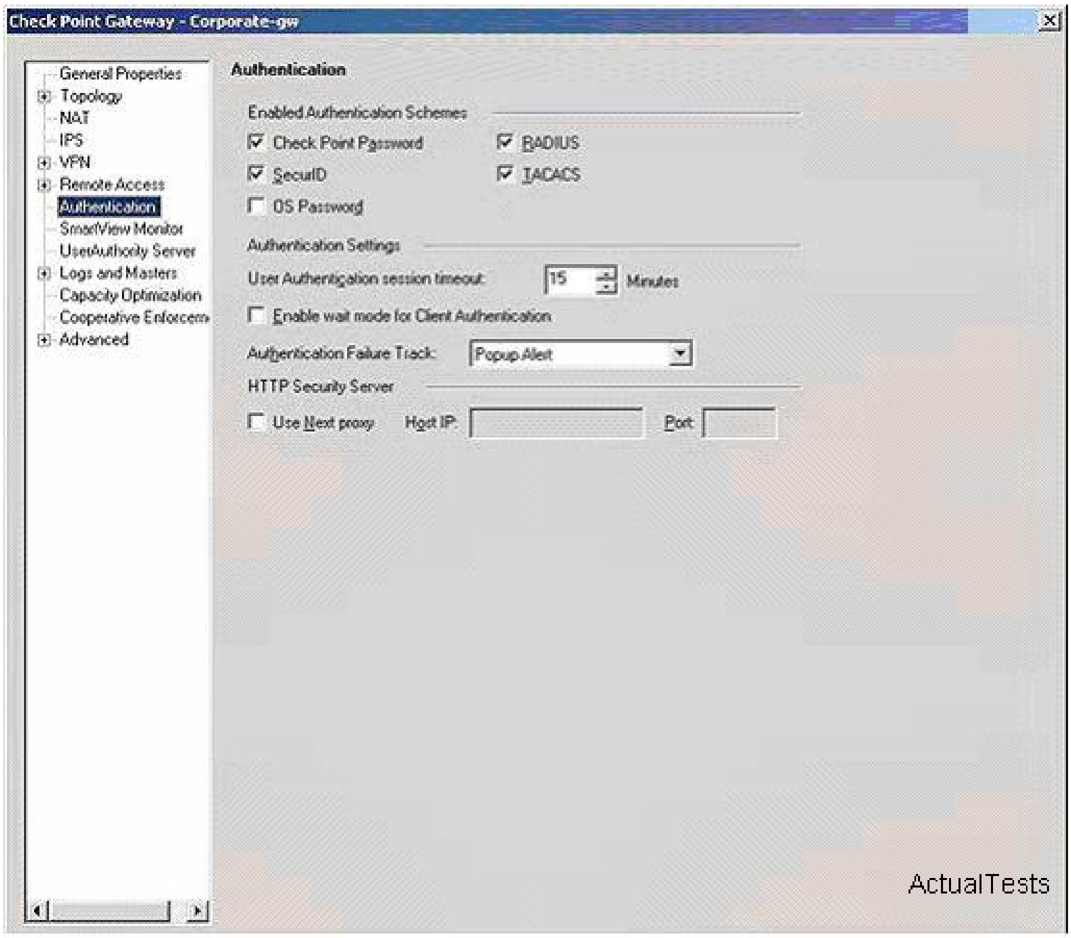
Settings:

Select a RADIUS Server or Group of Servers:

* Any

You will drop the arrow down to select Authentication scheme, and this has to correspond with Authentication scheme you choose for the network object for your firewall machine (as in diagram 2

Figure 1: User Properties Screen - Authentication tab



Check Point Gateway - Corporate-gw

Authentication

Enabled Authentication Schemes

☑ Check Point Password ☑ RADIUS

☑ SecurID ☑ TACACS

□ OS Password

Authentication Settings

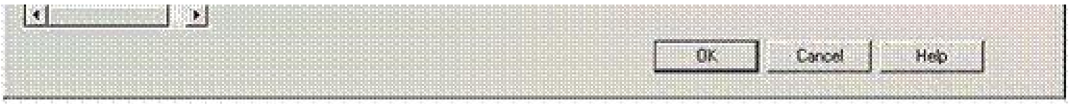
User Authentication session timeout: 15 Minutes

□ Enable wait mode for Client Authentication

Authentication Failure Track: Popup Alert

HTTP Security Server

□ Use Next proxy Host IP: Port:



ActualTests

Figure B: Check Point Gateway Properties Screen - Authentication Page

A. To delete the users and groups objects, re-create them and define new Authentication scheme for them
B. To verify that Authentication type you setup for the Firewall Module is the same that you setup for the Security Management server
C. Configure your Firewall Module and set up new Authentication type and new Authentication scheme
D. To verify the properties for the user attempting Authentication (this to include Authentication scheme), and to verify that the same Authentication scheme is selected in the Authentication properties of the network object for your firewall machine
E. Re-install Firewall Module and set up new Authentication type

Answer: D

QUESTION NO: 364

When dealing with IPSO clustering modes, which of the following is true of the forwarding mode?

A. In this mode, each node receives every packet sent to the cluster and decides whether to process it based on information it receives from the master node
B. In this mode, each cluster node receives every packet sent to the cluster and decides whether to process it based on information it receives from the master node
C. in this mode, each cluster interface joins an IP multicast group
D. In this mode, the master cluster node initially receives all the packets sent to the cluster and decides which node should process the packet
E. if the routers and switches on either side of the cluster do not support multicast MAC addresses then forwarding mode is suitable

Answer: D,E

QUESTION NO: 365

In IPSO directory structure, what does config folder contain?

A. The kernel image
B. Execution programs on startup
C. The software packages

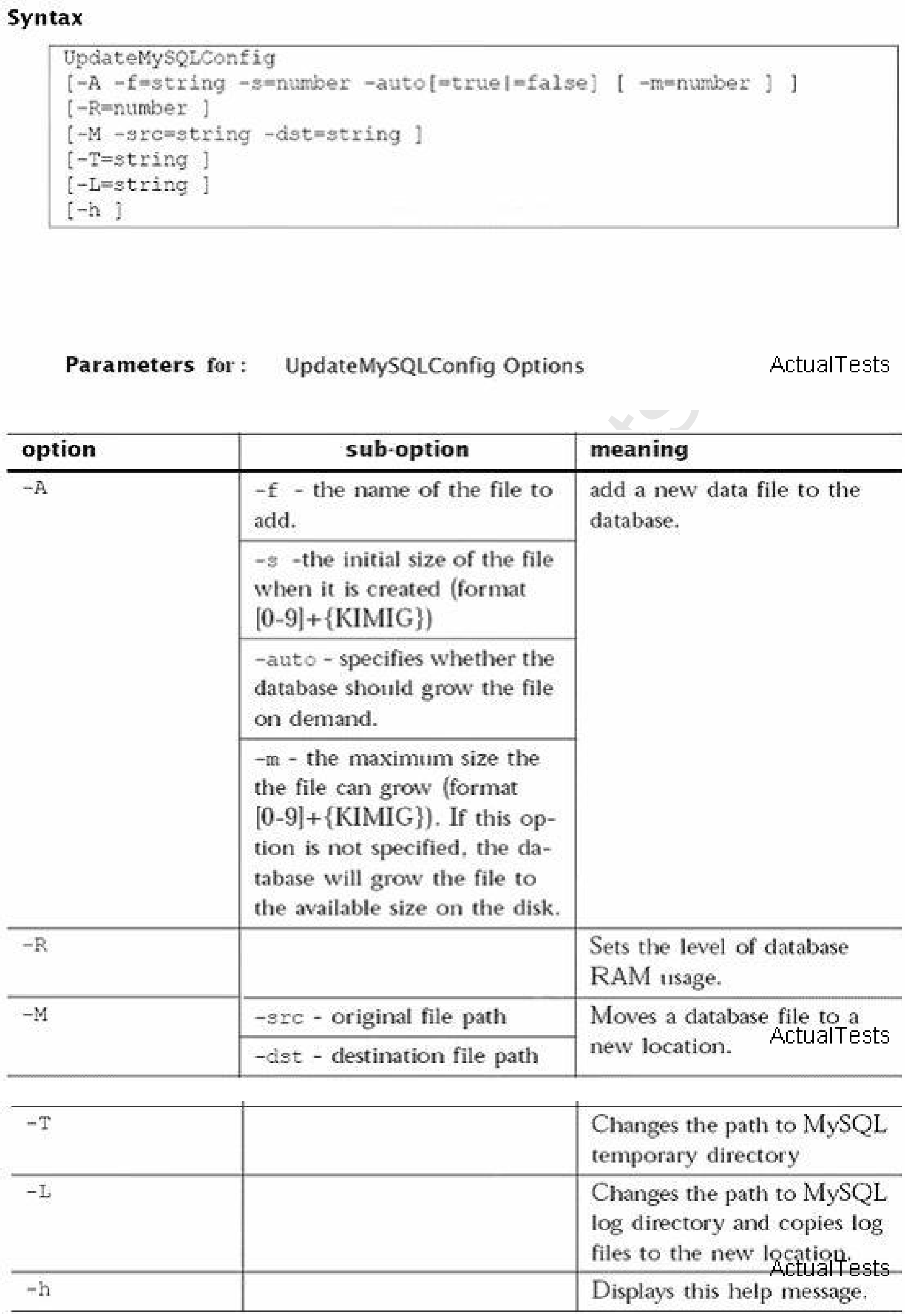
D. IPSO configuration file

E. System log files

Answer: D

QUESTION NO: 366

What application would you run in order to modify Eventia Reporter Database settings?



Syntax

```
UpdateMySQLConfig
[-A -f=string -s=number -auto[=true|=false] [ -m=number ] ]
[-R=number ]
[-M -src=string -dst=string ]
[-T=string ]
[-L=string ]
[-h ]
```

Parameters for : UpdateMySQLConfig Options

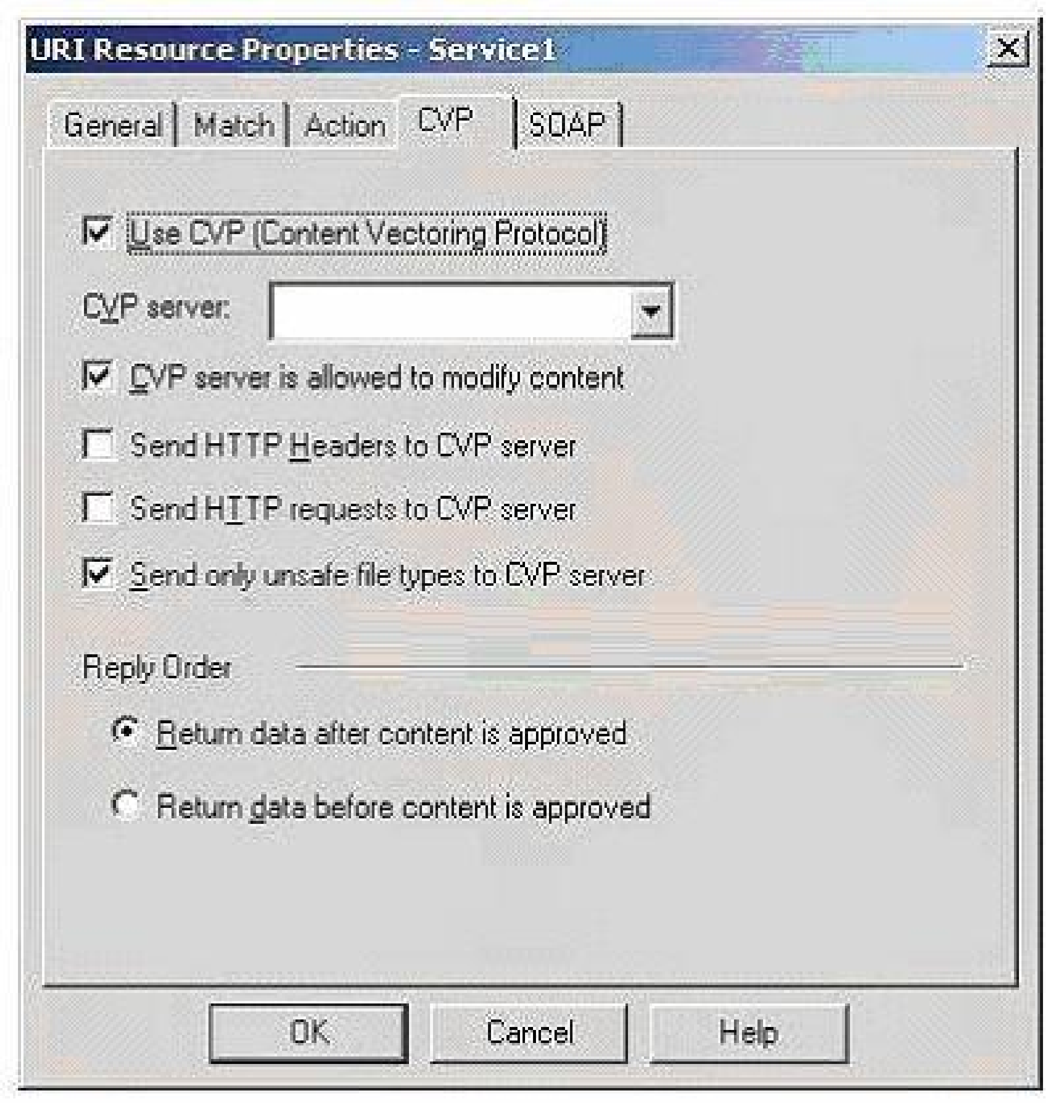
option	sub-option	meaning
-A	-f - the name of the file to add.	add a new data file to the database.
	-s -the initial size of the file when it is created (format [0-9]+{KIMIG})	
	-auto - specifies whether the database should grow the file on demand.	
	-m - the maximum size the the file can grow (format [0-9]+{KIMIG}). If this option is not specified, the database will grow the file to the available size on the disk.	
-R		Sets the level of database RAM usage.
-M	-src - original file path	Moves a database file to a new location.
	-dst - destination file path	
-T		Changes the path to MySQL temporary directory
-L		Changes the path to MySQL log directory and copies log files to the new location.
-h		Displays this help message.

A. ModifyMyERDConfig
B. rmdstop
C. UpdateMySQLConfig
D. cpconfig
E. UpdateMyERDConfig

Answer: C

QUESTION NO: 367

The performance of the CVP server when inspecting HTTP connections can be enhanced by:


URI Resource Properties - Service1

☑ Use CVP (Content Vectoring Protocol)

CVP server:

☑ CVP server is allowed to modify content

□ Send HTTP Headers to CVP server

□ Send HTTP requests to CVP server

☑ Send only unsafe file types to CVP server

Reply Order

● Return data after content is approved

○ Return data before content is approved

Figure 1: URI Resource Properties

A. Making sure that all file typesare sent to the CVP server
B. Making surethat two Security Management Servers are run in parallel
C. Making surethat two Security Gateways are run in parallel

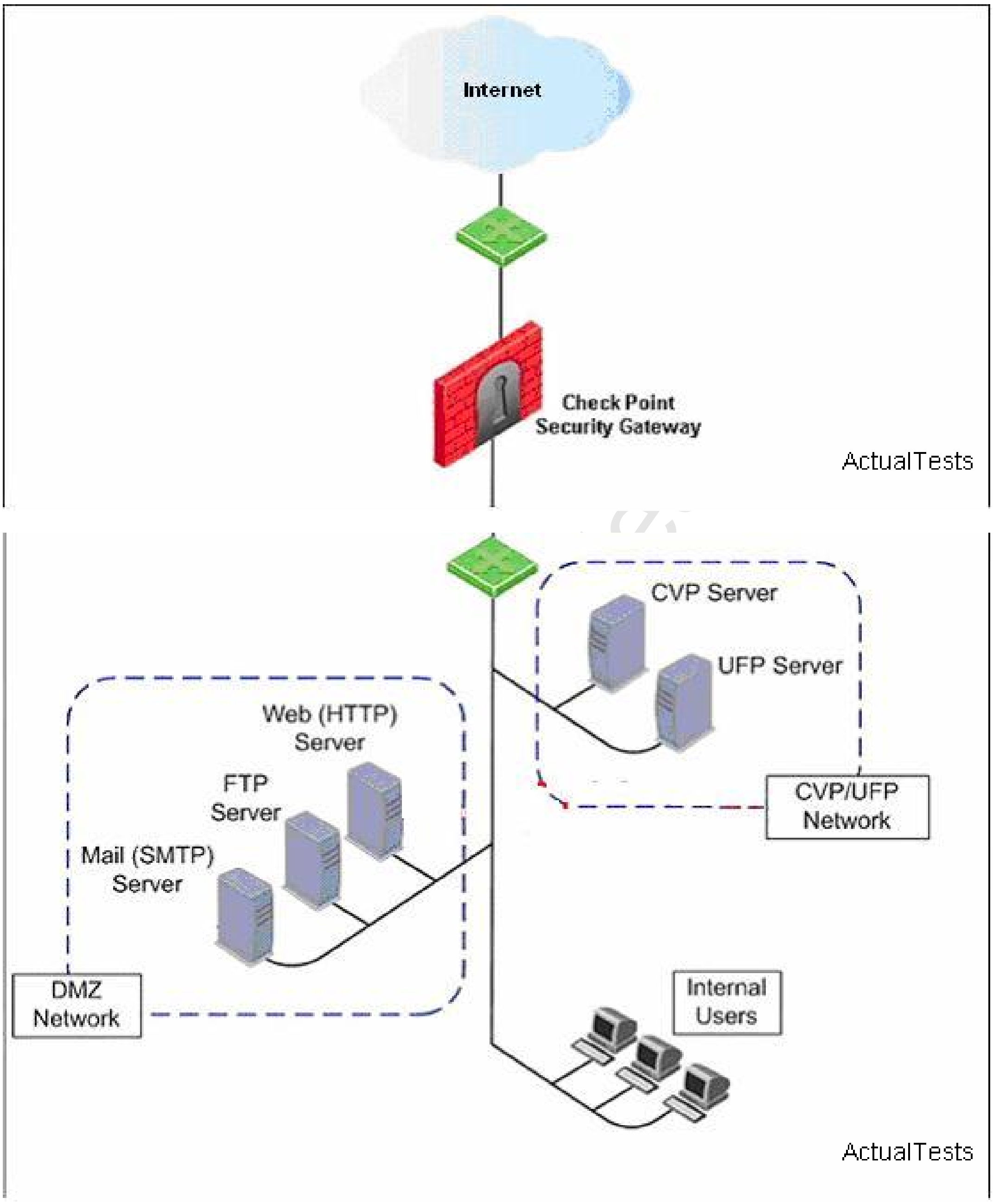
D. Making sure that URI Resourcesare run

E. Making sure that only unsafe file types are sent to the CVP server

Answer: E

QUESTION NO: 368

CVP and UFP servers are typically deployed on dedicated servers. Where should they be placed in a network?



A. Demilitarized Zone

B. Virtual Network Zone

C. Decommissioned Network

D. Server

E. VPN

Answer: A

QUESTION NO: 369

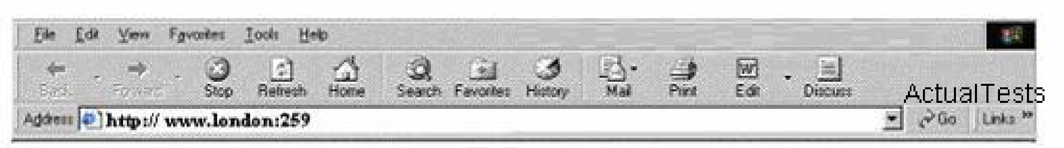
When connecting to a Gateway, you automatically logon to the Policy Server residing behind that Gateway. If you define an alternative policy server in the connection profile, then Policy Server High Availability functionality is activated. What file would you need to configure Policy Server High Availability?

A. vpn_config.conf
B. product.ini
C. users.c
D. cpd.pid
E. userc.c

Answer: E

QUESTION NO: 370

Study the diagram and answer the question below. George was initiating a client authentication session by beginning an HTTP session on port 259 with the gateway named london as shown. What do you think might be wrong with the address George specified in the browser?



Address http:// www.london:259

A. The user should use Session Authentication method to successfully connect to the destination server.
B. The user should be able to connect, since he was using the right port.
C. The user should bypass the firewall at port 259 to connect successfully.
D. The user was using the wrong port. He needs to use port 900 to connect successfully.
E. The user should bypass the firewall at port 900 to connect successfully.

Answer: D

QUESTION NO: 371

At what point does the SecureClient download its policy from a Policy Server?

A. When install the SecuRemote software on the SecuRemote machine

B. When install the SecureClient software on the SecureClient machine

C. When the SecuRemote machine reboots

D. When the SecureClient machine connects to the site

E. When the SecureClient machine reboots

Answer: D

QUESTION NO: 372

The diagram shows your network. The gateway A will want to start IKE negotiation with gateway B to build a VPN tunnel for the control connection as both gateways do belong to the same community. What is likely to be the consequence of turning off implicit rules?

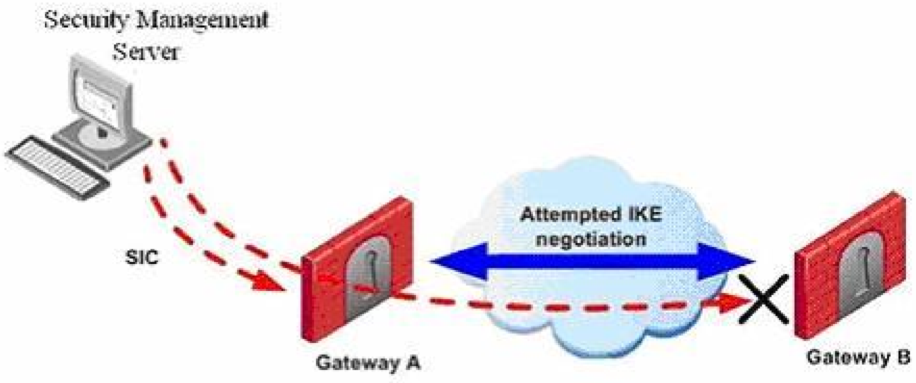


Figure 1: Turning off control connections can cause Policy installation to fail

A. You will not be able to install a Policy on a Remote gateway A

B. The gateway B will have to re-configured

C. You will not be able to install a Policy on both gateways A and B

D. You will not be able to install a Policy on a Remote gateway B

E. You will be able to install a Policy on both gateways A and B

Answer: D

QUESTION NO: 373

Which of the following is true of IPS-1 Management Server, Alerts Concentrators and Management Dashboard?

A. They must always be of the different version

B. They must always be of the same version

C. They can only be managed via CLI
D. They must always be managed remotely
E. They must not reside on the same machine

Answer: B

QUESTION NO: 374

What must you have before upgrading your gateways or Security management server to the NGX R65 or newer?

A. Downloadable
B. Contract
C. Wrapper
D. Service
E. File

Answer: B

QUESTION NO: 375

SmartUpdate installs two repositories on the Security Management server. What folder does License repository use a storage on Windows platform?

A. $FWDIR\bin
B. $FWDIR\conf
C. $FWDIR\log
D. $FWDIR\network
E. $FWDIR\dir

Answer: B

QUESTION NO: 376

On Log File Management, what happens to the current log file when it approaches the default limit?

A. The current Log file is opened in addition to the new Log file.
B. The current file is appended to the new file.
C. The current file is lost.
D. New Log file cannot be created when current file is opened.

E. The current Log file is closed and written to disk with a name that contains the current date and time.

Answer: E

QUESTION NO: 377

What are the reasons for using NAT?

A. To map NetBIOS names to IP addresses in internal network
B. To conceal a network's internal IP address from the internet for security reasons
C. To reveal a network's internal IP address from the internet for security reasons
D. To translate invalid addresses to Valid or legaladdresses , and vice versa
E. To map hardware addresses to IP addresses in internal network

Answer: B,D

QUESTION NO: 378

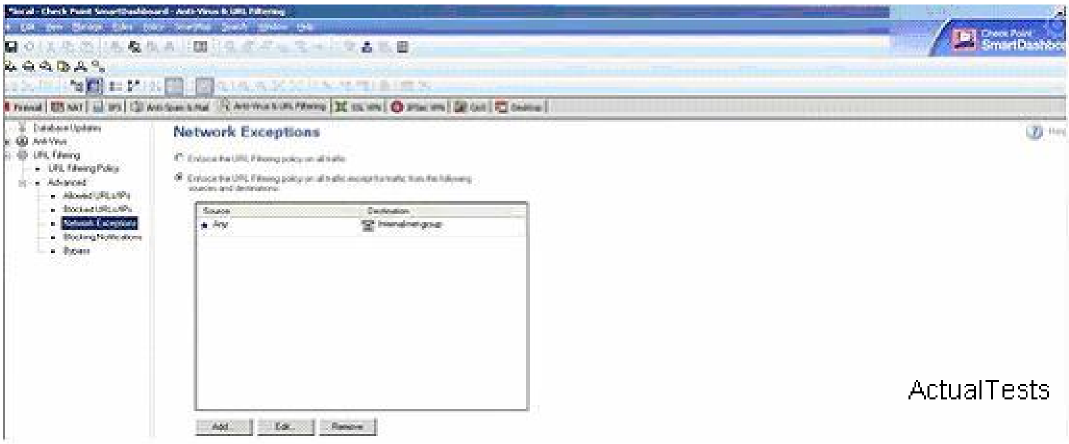
How many log file(s) can be opened in the SmartView Tracker GUI at a time?

A. Two
B. Five
C. Three
D. One
E. Four

Answer: D

QUESTION NO: 379

You are in Network Exceptions page shown in the diagram, selecting the button on right side window will:



Network Exceptions

○ Enforce the URL Filtering policy on all traffic

● Enforce the URL Filtering policy on all traffic except for traffic from the following sources and destinations:

Source	Destination
Any	Internal-net-group

Add... Edit... Remove

A. Create a list of the networks connections(or specific source and destination) through which traffic should be inspected

B. Create a list of the networks connections(or specific source and destination) through which traffic should not be inspected

C. Enforce the URL Filtering Policy on all traffic

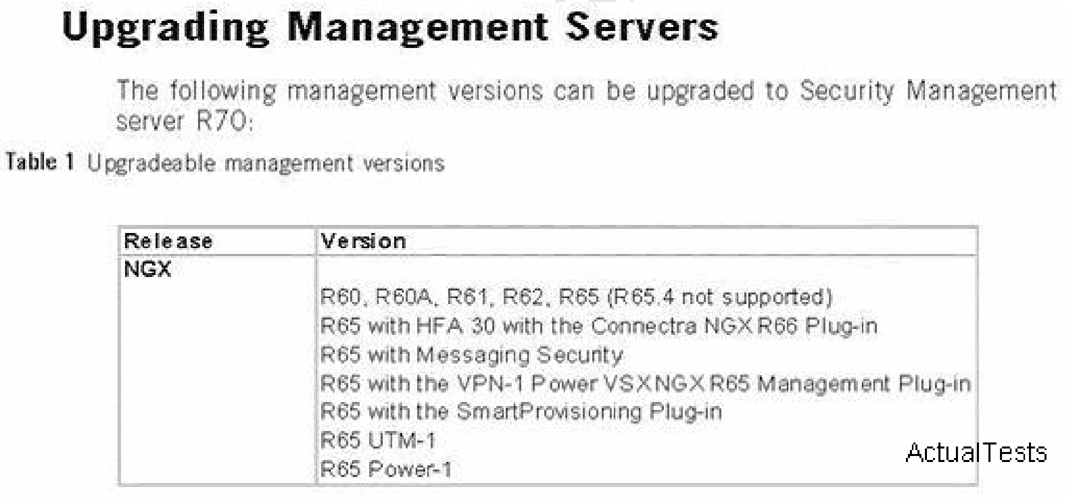
D. Have no effect

E. Enforce the URL Filtering Policy on specific traffic

Answer: B

QUESTION NO: 380

Which of The following management versions cannot be upgraded to Security Management server R70?

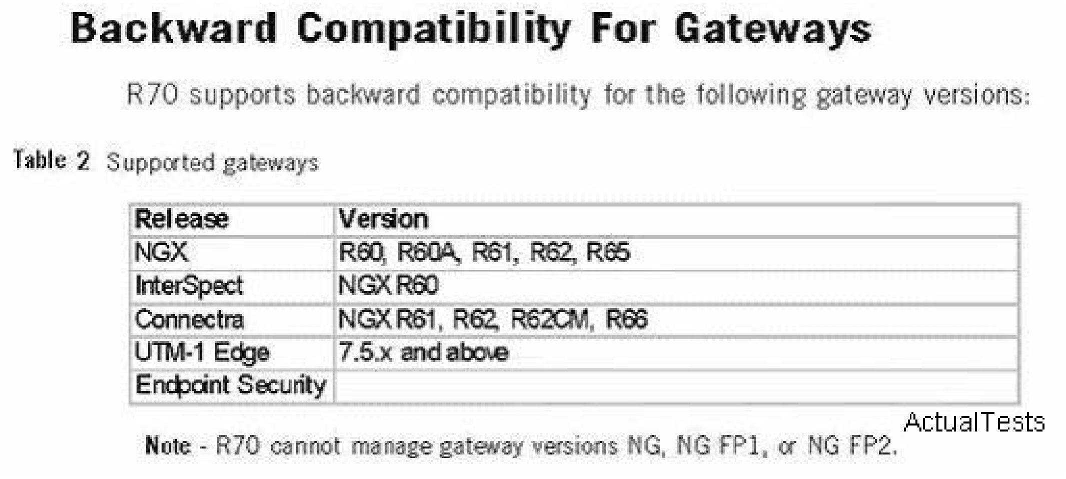

ActualTests

Upgrading Management Servers

The following management versions can be upgraded to Security Management server R70:

Table 1 Upgradeable management versions

Release	Version
NGX	R60, R60A, R61, R62, R65 (R65.4 not supported) R65 with HFA 30 with the Connectra NGX R66 Plug-in R65 with Messaging Security R65 with the VPN-1 Power VSX NGX R65 Management Plug-in R65 with the SmartProvisioning Plug-in R65 UTM-1 R65 Power-1



Backward Compatibility For Gateways

R70 supports backward compatibility for the following gateway versions:

Table 2 Supported gateways

Release	Version
NGX	R60, R60A, R61, R62, R65
InterSpect	NGX R60
Connectra	NGX R61, R62, R62CM, R66
UTM-1 Edge	7.5.x and above
Endpoint Security	

Note - R70 cannot manage gateway versions NG, NG FP1, or NG FP2.

A. R65
B. R62
C. R61
D. NG
E. R60

Answer: D

QUESTION NO: 381

You modify your Rule Base to allow some new groups access to the Internet. After the modification, you install the security policy. The members of these groups keep contact you saying that the connection to the Internet is too slow. You think that the Security Gateway virtual memory might be the problem. Which tool will you contact to get information about your Security Gateway virtual memory?

A. SmartProvisioning
B. SmartDashboard
C. SmartView Monitor
D. SmartUpdate
E. SmartView Tracker

Answer: C

QUESTION NO: 382

10 new users are being employed by your company as roaming tradesmen. They will be connecting to your VPN community from anywhere in the world. You need to implement a technology that can be used with a standard Web browser and can provide accesses to resources from many locations. What technology will you implement?

A. IKE VPN

B. SSH VPN

C. Specialized VPN client software

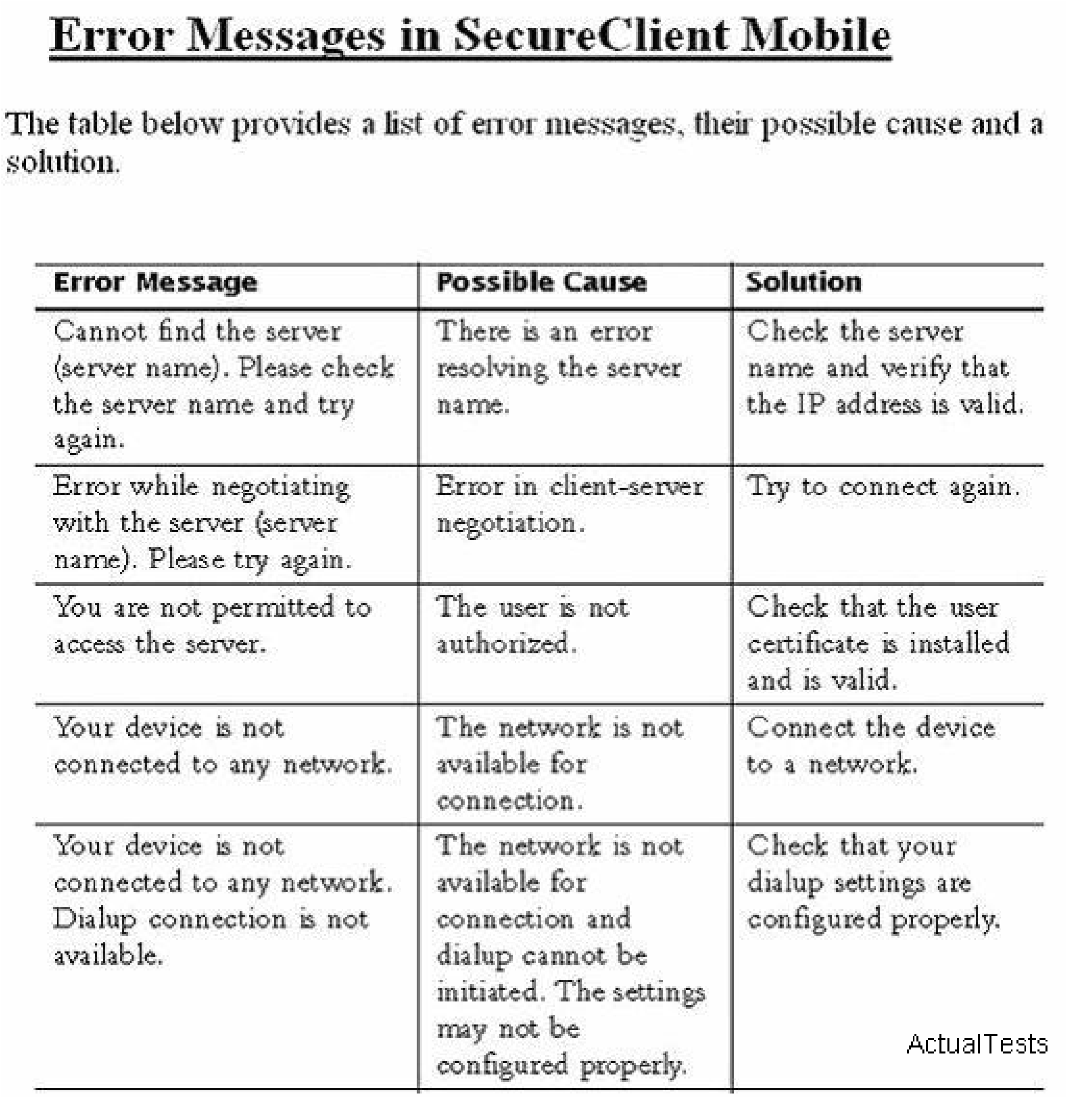
D. IPSEC VPN

E. SSL VPN

Answer: E

QUESTION NO: 383

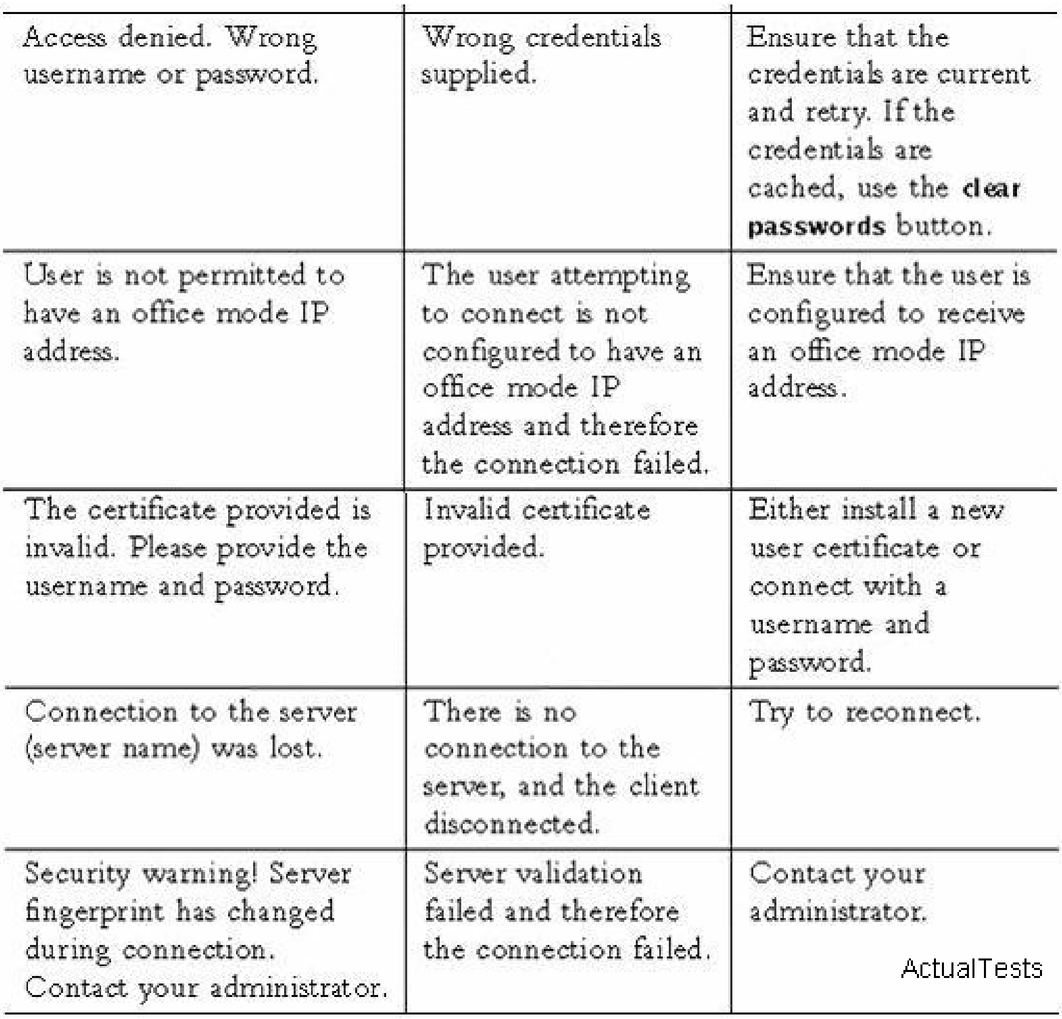
When you tried to connect your SecureClient Mobile, you received the error message "Error while negotiating with the server"? What is likely to be the possible cause and how will you resolve it?



Error Messages in SecureClient Mobile

The table below provides a list of error messages, their possible cause and a solution.

Error Message	Possible Cause	Solution
Cannot find the server (server name). Please check the server name and try again.	There is an error resolving the server name.	Check the server name and verify that the IP address is valid.
Error while negotiating with the server (server name). Please try again.	Error in client-server negotiation.	Try to connect again.
You are not permitted to access the server.	The user is not authorized.	Check that the user certificate is installed and is valid.
Your device is not connected to any network.	The network is not available for connection.	Connect the device to a network.
Your device is not connected to any network. Dialup connection is not available.	The network is not available for connection and dialup cannot be initiated. The settings may not be configured properly.	Check that your dialup settings are configured properly.



Access denied. Wrong username or password.	Wrong credentials supplied.	Ensure that the credentials are current and retry. If the credentials are cached, use the **clear passwords** button.
User is not permitted to have an office mode IP address.	The user attempting to connect is not configured to have an office mode IP address and therefore the connection failed.	Ensure that the user is configured to receive an office mode IP address.
The certificate provided is invalid. Please provide the username and password.	Invalid certificate provided.	Either install a new user certificate or connect with a username and password.
Connection to the server (server name) was lost.	There is no connection to the server, and the client disconnected.	Try to reconnect.
Security warning! Server fingerprint has changed during connection. Contact your administrator.	Server validation failed and therefore the connection failed.	Contact your administrator.

A. Wrong credentials supplied. Check the server name and verify that the IP address is valid to resolve

B. There is an error resolving the server name. Check the server name and verify that the IP address is valid to resolve

C. Invalid certificate is provided. Try to connect again to resolve

D. The network is not available for connection. Check that your dialup settings are configured properly to resolve

E. Error in client-server negotiation. Try to connect again to resolve

Answer: E

QUESTION NO: 384

Which of these are true of the FTP Security server?

A. Implement FTP security server with an SMTP resource

B. FTP security server provides authentication services and content security based on FTP commands (PUT/GET)

C. Implement FTP security server with an FTP resource

D. File name restrictions
E. Anti-virus checking for files

Answer: B,C,D,E

QUESTION NO: 385

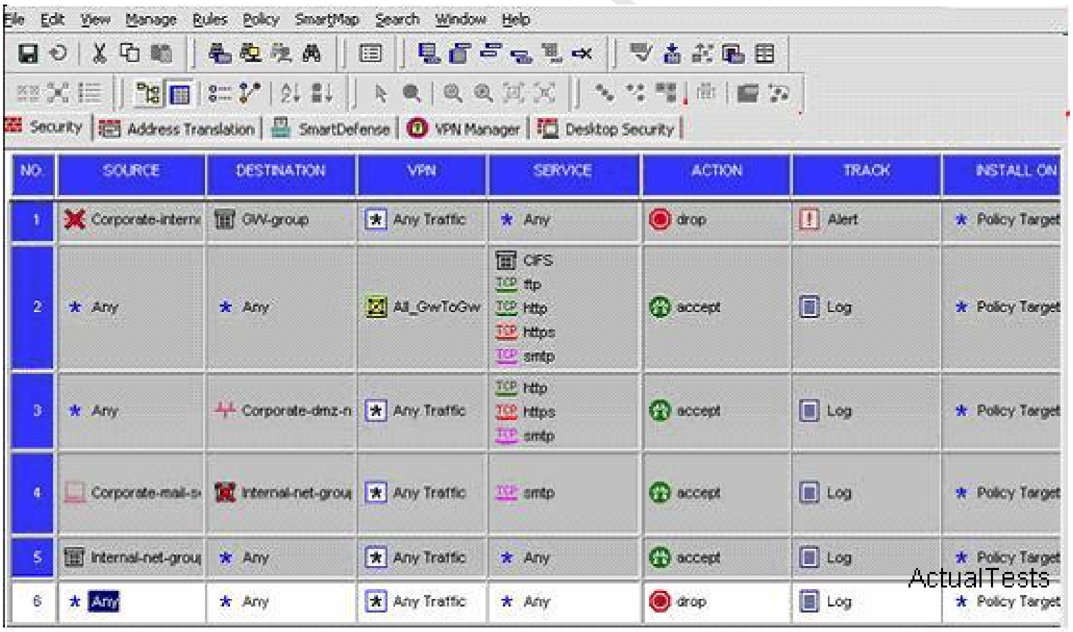
10 new users are being employed by your company as roaming tradesmen. They will be connecting to your VPN community from anywhere in the world. You need to implement a technology that can be used with a standard Web browser and can provide accesses to resources from many locations. What technology will you implement?

A. Specialized VPN client software
B. IPSEC VPN
C. SSL VPN
D. SSH VPN
E. IKE VPN

Answer: C

QUESTION NO: 386

Why would an administrator want to negate a selected object in the Rule Base?



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	Corporate-intern	GW-group	Any Traffic	Any	drop	Alert	Policy Target
2	Any	Any	All_GwToGw	CIFS ftp http https smtp	accept	Log	Policy Target
3	Any	Corporate-dmz-n	Any Traffic	http https smtp	accept	Log	Policy Target
4	Corporate-mail-s	Internal-net-grou	Any Traffic	smtp	accept	Log	Policy Target
5	Internal-net-grou	Any	Any Traffic	Any	accept	Log	Policy Target
6	Any	Any	Any Traffic	Any	drop	Log	Policy Target

A. To connect to any destination using http service
B. To nest a specific object or user
C. To connect to any destination using ftp service
D. To include all objects or users and exclude a specific object or user

E. To include a specific object or user

Answer: D

QUESTION NO: 387

Secure communication channels between Check Point modules (such as Security Management Server, Enforcement modules or OPSEC modules) can be set up using _____

A. SIC
B. SVM
C. eBusiness Application
D. Management Application
E. Secure Virtual Network Architecture

Answer: A

QUESTION NO: 388

How would create a user object from the SmartView Tracker GUI without having to shut it down and start SmartDashboard?

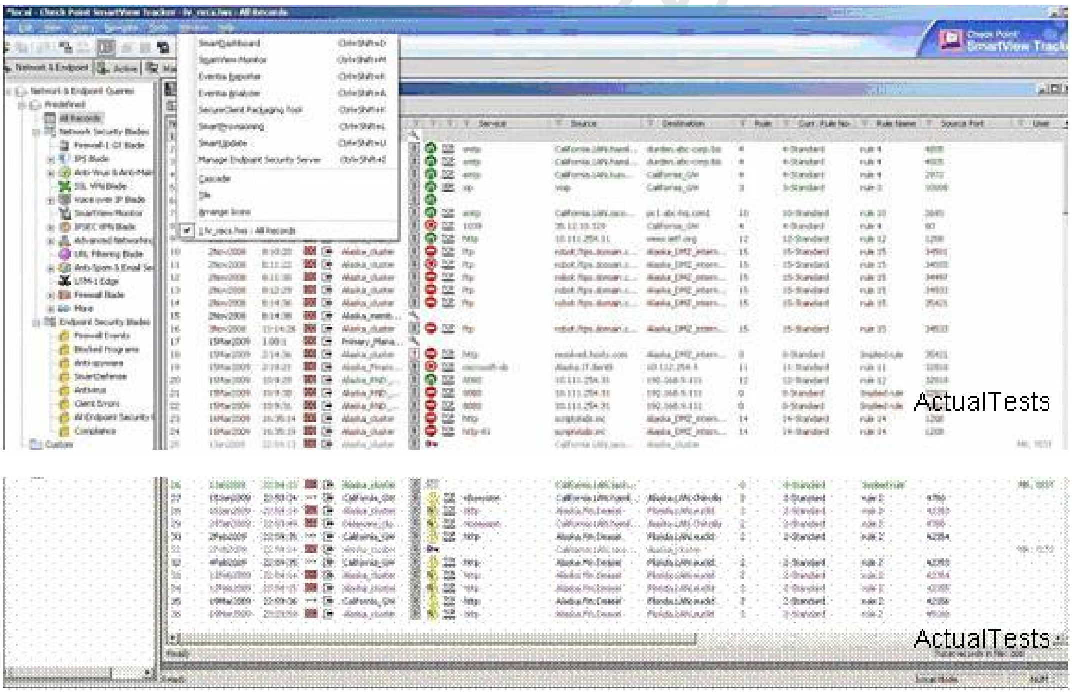


Figure 1: SmartView Tracker

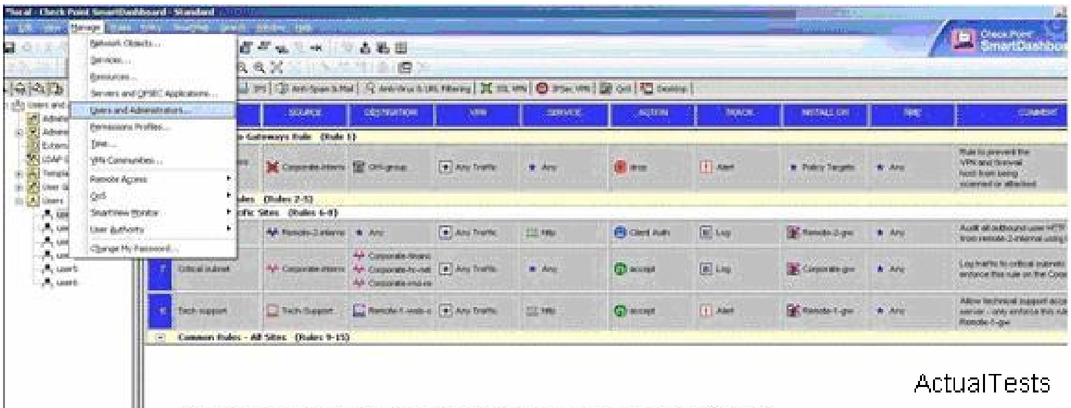


Figure 2 : Manage Menu - selecting Users and Administrators...

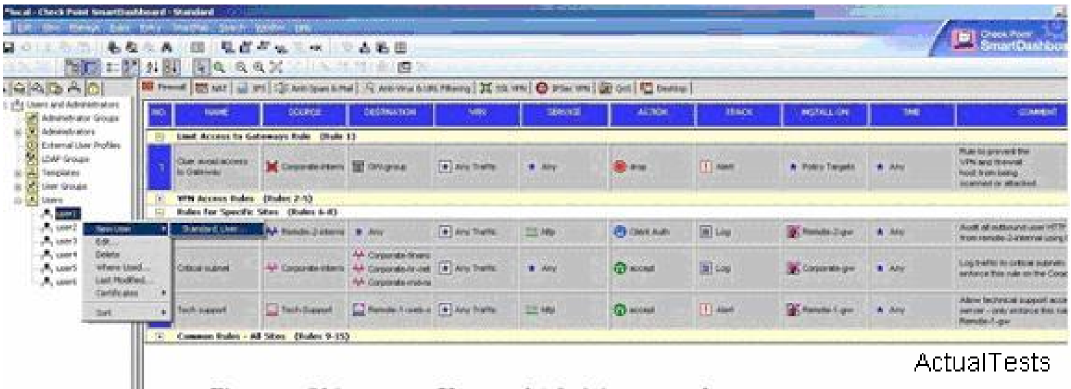


Figure 3 : Objects tree - Users and Administrators tab

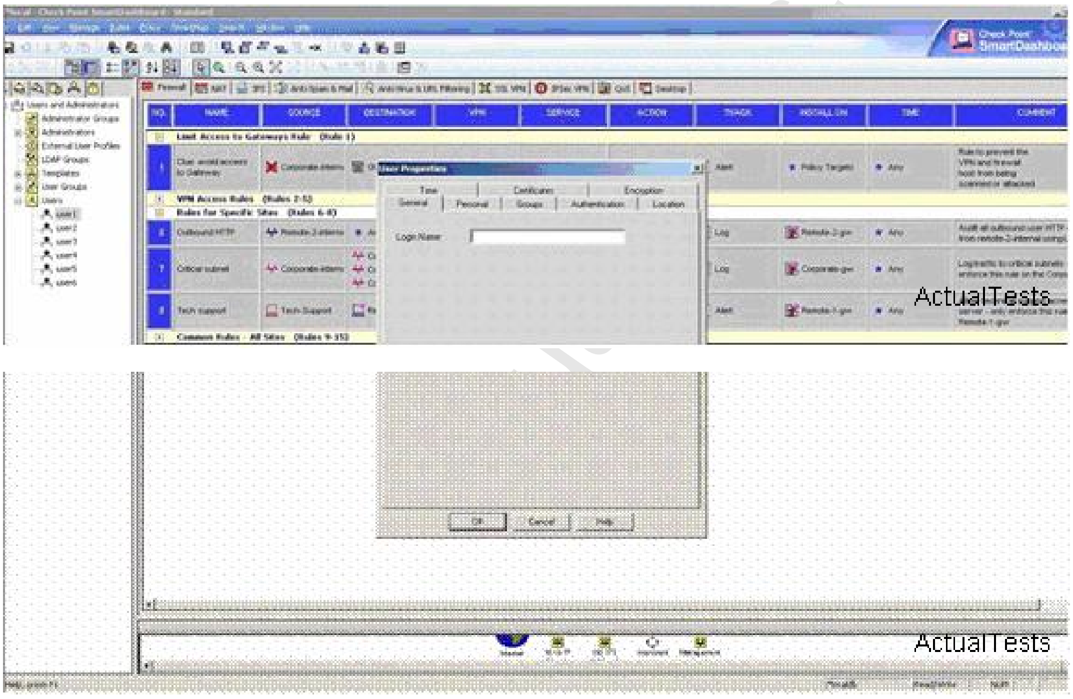


Figure 4: User Properties window

A. You will choose Window Menu and select SmartDashboarD. In SmartDashboard GUI, you will choose Manage menu and then select Users and Administrators...

B. You will choose File Menu and select SmartDashboarD. In the SmartDashboard GUI, you will choose Manage menu and then select User and Administrator...

C. You will choose Window Menu and select SmartView Tracker. In the SmartView Tracker GUI, you will choose Manage menu and then select User and Administrator...
D. You will choose Window Menu and select SmartDashboar
E. In the SmartDashboard GUI you will choose Manage menu and then Network Objects
F. There is now way to do this without shutting down from the GUI and then launch the SmartDashboard GUI

Answer: A

QUESTION NO: 389

What is the difference between Cleanup and Stealth rule? Choose the best answer.

A. Stealth rule is an extension of Cleanup rule
B. Stealth rule is used to prevent external users from connecting to the Gateway while Cleanup rule allows the Gateway to accept all traffic not described by other rules
C. Stealth rule is the same as Cleanup rule
D. Stealth rule is used to prevent any user from connecting to the Gateway while Cleanup rule drops all traffic not permitted by previous rules
E. Stealth rule is used to prevent external users from connecting to the Gateway while Cleanup rule allows the Gateway to drop al traffic not described by other rules

Answer: D

QUESTION NO: 390

To manually perform a pre-upgrade verification, which of the following file would you run?

A. license_upgradE. exe
B. pre_upgrade_Verifier.exe
C. upgrade_export.exe
D. verify_packagE. exe
E. update_download_helper.exe

Answer: B

QUESTION NO: 391

Which of the following is true of Software Blade? Select all the correct answers.

A. It is security building block that is independent, modular and can be centrally managed

B. It can be easily administered
C. As the needs of the company change, additional software blades can be easily activated to extend security to an existing configuration on the same security hardware
D. It delivers rivaled security integration to allow the right level of security at some of the layers of the network
E. It can be quickly enabled and configured on any gateway or management system

Answer: A,C,E

QUESTION NO: 392

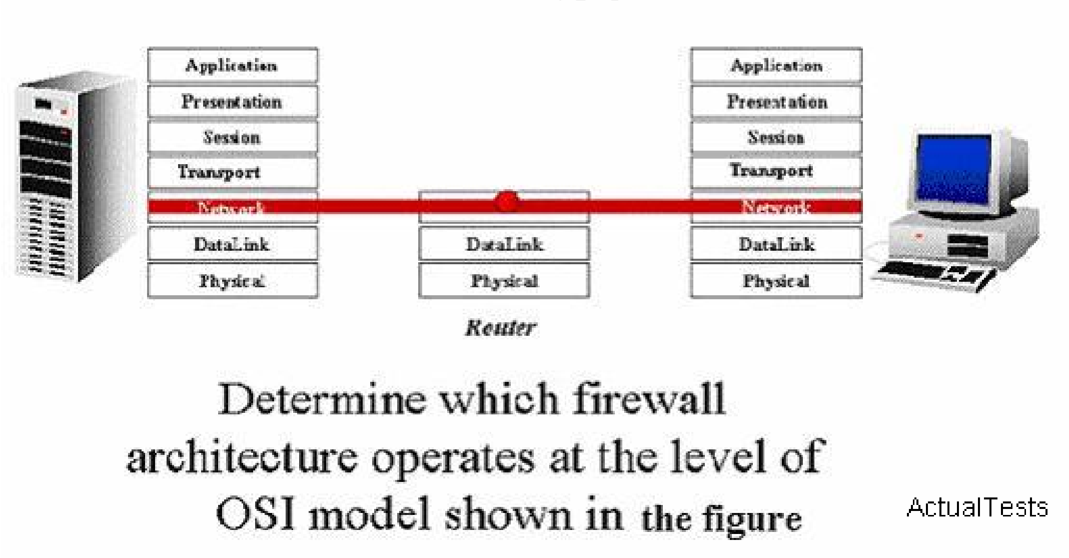
Which of the following feature provides high availability by avoiding a single point of failure?

A. Command Line Interface
B. Ipsilon Routing Daemon
C. Disk Mirroring
D. Exterior Gateway Protocol
E. IP Clustering

Answer: E

QUESTION NO: 393

Look at exhibit 1. What type of firewall is shown in the diagram?



Determine which firewall architecture operates at the level of OSI model shown in the figure

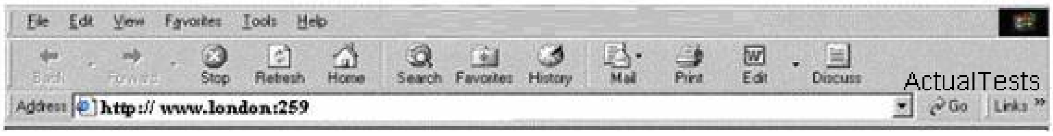
A. Firewall
B. Network layer firewall
C. Packet filtering
D. Proxies

E. Application Layer

Answer: C

QUESTION NO: 394

Study the diagram and answer the question below. George was initiating a client authentication session by beginning an HTTP session on port 259 with the gateway named london as shown. What do you think might be wrong with the address George specified in the browser?



http:// www.london:259

A. The user should use Session Authentication method to successfully connect to the destination server.
B. The user should bypass the firewall at port 259 to connect successfully.
C. The user should be able to connect, since he was using the right port.
D. The user was using the wrong port. He needs to use port 900 to connect successfully.
E. The user should bypass the firewall at port 900 to connect successfully.

Answer: D

QUESTION NO: 395

What secure protocol provides secure connection to a SecurePlatform system?

A. SSH
B. RSV
C. RSH
D. TCP
E. IP

Answer: A

QUESTION NO: 396

Which folder or directory contains the list of IP addresses of machines designated as Masters?

A. bin
B. log
C. conf

D. util

E. lib

Answer: C

QUESTION NO: 397

The command line to use when monitoring system status is:

A. show interface monitor

B. show system status

C. monitor system status

D. show system

E. show status

Answer: A

QUESTION NO: 398

Why would an Administrator want to verify a security policy? Choose all the correct answers.

A. To identify the conflicting rules present in your Security Policy

B. To ensure all rules in a security policy are placed accurately

C. To create a security policy but not install it on a firewalled computer

D. To verify the implicit rule created from new rule

E. To test a security policy before installing it on a firewalled computer

Answer: A,B,C,E

QUESTION NO: 399

While you are working in Network Voyager, which keys or operations are not recommended in your browser?

A. Avoid using Backspace key as a way to commit a change in the Network Voyager pages

B. Your browser's space tab

C. Avoid using Enter key as a way to commit a change in the Network Voyager pages

D. Your browser'sBack and Forward buttons

E. Avoid using bookmarks as a way of navigating to Network Voyager pages

Answer: D,E

QUESTION NO: 400

What application, a support tool, gathers into one text file a wide range of data concerning the Check Point packages in your system?

A. CPInfo
B. SmartUpdate
C. Management Portal
D. Cpconfig
E. SmartLSM

Answer: A

QUESTION NO: 401

If system's performance is of utmost importance, what deployment type would you implement for Eventia Reporter?

A. Server/Server Model
B. Standalone Paradigm
C. Standalone Deployment
D. Client/Client Model
E. Distributed Deployment

Answer: E

QUESTION NO: 402

Anti-Virus Scanning methods are Scan by IP and:

A. Scan by Direction
B. Scan by Network
C. Scan by MAC Address
D. Scan by ARP
E. Scan by Source

Answer: A

QUESTION NO: 403

How many disks do you need to implement Disk Mirroring (RAID 1)?

A. 4
B. 8
C. 2
D. 10
E. 6

Answer: C

QUESTION NO: 404

Which of the following is the rule base file?

A. control.map
B. fwauth.NDB*
C. objects_5_0.C
D. rulebases_5_0.fws
E. rulE. fws

Answer: D

QUESTION NO: 405

Which of the following may be true when dealing with Access Control and two gateways in the same VPN Community? Select all the correct answers.

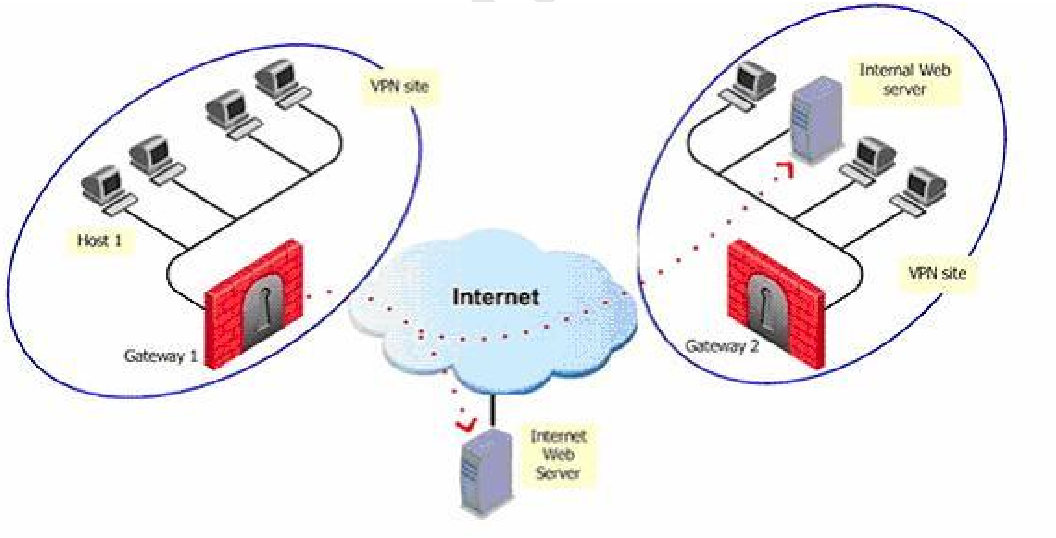


FIGURE 1 Access control in VPN communities

A. The configuration of the two Gateways into a VPN community means that if these Gateways are allowed to communicate via an access control policy, then that communication is encrypted

B. Configuring VPN page in the Global Properties, it is possible to create access control rules that apply only to members of a VPN community
C. Configuring the two Gateways into a VPN community does not create a de facto access control policy between the Gateways
D. Configuring the two Gateways into a VPN community creates a de facto access control policy between the Gateways
E. With VPN column of the Security Policy Rule Base, it is possible to create access control rules that apply only to members of a VPN community

Answer: A,C,E

QUESTION NO: 406

The CheckPoint Open Performance Architecture security software running on Intel® multicore processors was designed to solve which of the following problems?

A. Trade-off between the performance and security
B. Trade-off between the system fine-tuning and Application-layer threats combat
C. Degradation of security
D. Degradation of performance
E. Transparency

Answer: A

QUESTION NO: 407

Which of the following is true regarding Transparent Mode?

A. It allows your IPSO appliance to behave like a layer 2 device
B. It allows you to maintain your current local area network configuration
C. It allows you to maintain your existing IP address with your ISP
D. Traffic between transparent mode interfaces is inspected at layer 3
E. You can configure some interfaces to use transparent mode while other interfaces on the same platform are configured normally

Answer: A,C,E

QUESTION NO: 408

One of the problem of the asymmetric encryption is proving that a public key is authentic and has not been tampered with. Which of the following is the solution to this problem? Select all the correct answers.

A. Pretty Good Privacy (PGP)
B. Universal key encryption
C. Public-key infrastructure (PKI)
D. Digital Signature
E. Privatekey encryption

Answer: A,C

QUESTION NO: 409

What deployment is said to be implemented If the gateway and the Security Management server are deployed on separate machines?

A. Model
B. Server/Server
C. Distributed deployment
D. Client/Client
E. Firewall

Answer: C

QUESTION NO: 410

If you choose to do backup with Network Voyager manually, which of the following directory will get backed-up?

A. /cron)
B. /conf
C. /config
D. /etc)
E. /image

Answer: A,C,D

QUESTION NO: 411

When restoring backups of older versions of SecurePlatform such as NG AI, which of the following settings are likely to be restored? Select all the correct answers.

A. user accounts
B. routes

C. hostname
D. upgrade history
E. WebUI port

Answer: A,B,C,E

QUESTION NO: 412

There are a number of factors that can improve performance of the Eventia Reporter's database and these include setting the amounts of RAM to buffer datA. To do this, you will use UpdateMySQLConfig utility. Which of the following flags will you use in conjunction with UpdateMySQLConfig application?

A. -R
B. -L
C. -N
D. -T
E. -M

Answer: A

QUESTION NO: 413

Before the advent of Checkpoint's Stateful Inspection technology, what types of traditional firewall technology were in use? Choose the correct answer(s).

A. OSI layers gateways
B. Packet filtering
C. Stateful inspection gateways
D. Packet proxies
E. Application layer gateways

Answer: B,E

QUESTION NO: 414

How would you verify a security policy?

A. By selecting Verify from Policy menu in SmartDashboard
B. By selecting Verify from File menu in SmartDashboard
C. By selecting Verify from Edit menu in SmartDashboard

D. By selecting Verify from Window menu in SmartDashboard
E. By selecting Verify from Manage menu in SmartDashboard

Answer: A

QUESTION NO: 415

You have just taken over as an Administrator of a very large insurance company. Your Manager asks you to review all the Security Policies and rules installed on your Enforcement modulE. What tool would you use to achieve this?

A. SmartDashboard
B. SmartView Tracker
C. SmartView Monitor
D. SVN
E. SIC

Answer: A

QUESTION NO: 416

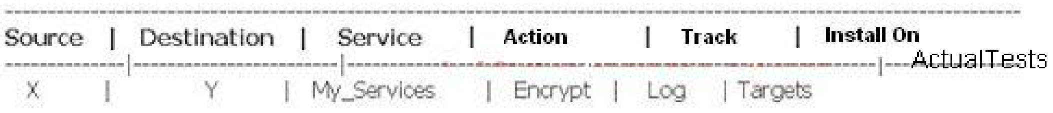
What are the ways by which you can improve NGX performance? Choose all the appropriate options

A. Keep the RuleBase simple
B. Include unnecessary services in the RuleBase
C. Disable Accounting and Active connections mode in the SmartView Tracker GUI
D. You can add services to the RuleBase as needed
E. Use faster hardware
F. Position the most applied rules first in the RuleBase

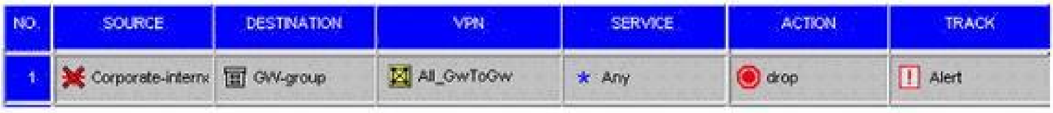
Answer: A,C,E,F

QUESTION NO: 417

The rule below shows the Encrypt rule in a Traditional Mode Rule Base. What is likely to be Simplified Mode equivalent if the if the connections originates at X and its destination is Y, within any Site-to-Site Community (i.e. All_GW _to_GW).

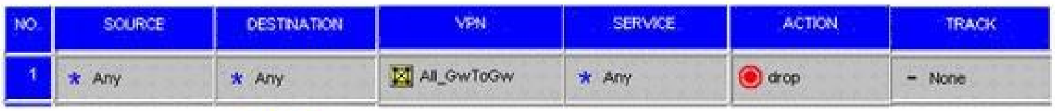


Source	Destination	Service	Action	Track	Install On
X	Y	My_Services	Encrypt	Log	Targets



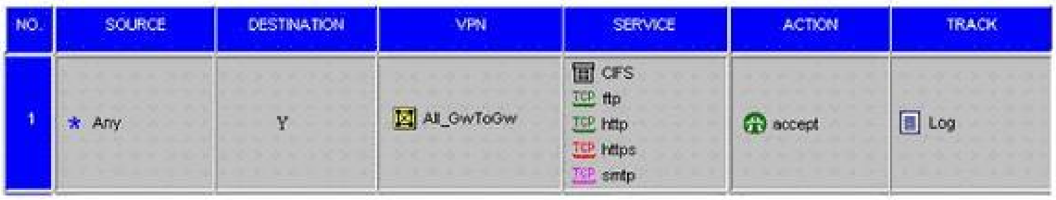
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Corporate-intern	GW-group	All_GwToGw	* Any	drop	Alert

Rule A



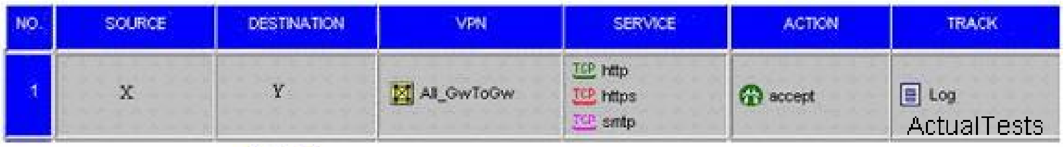
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	* Any	All_GwToGw	* Any	drop	- None

Rule B



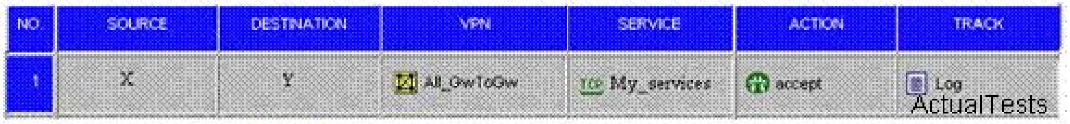
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	* Any	Y	All_GwToGw	CIFS TCP ftp TCP http TCP https TCP smtp	accept	Log

Rule C



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	X	Y	All_GwToGw	TCP http TCP https TCP smtp	accept	Log

Rule D



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	X	Y	All_GwToGw	TCP My_services	accept	Log

Rule E

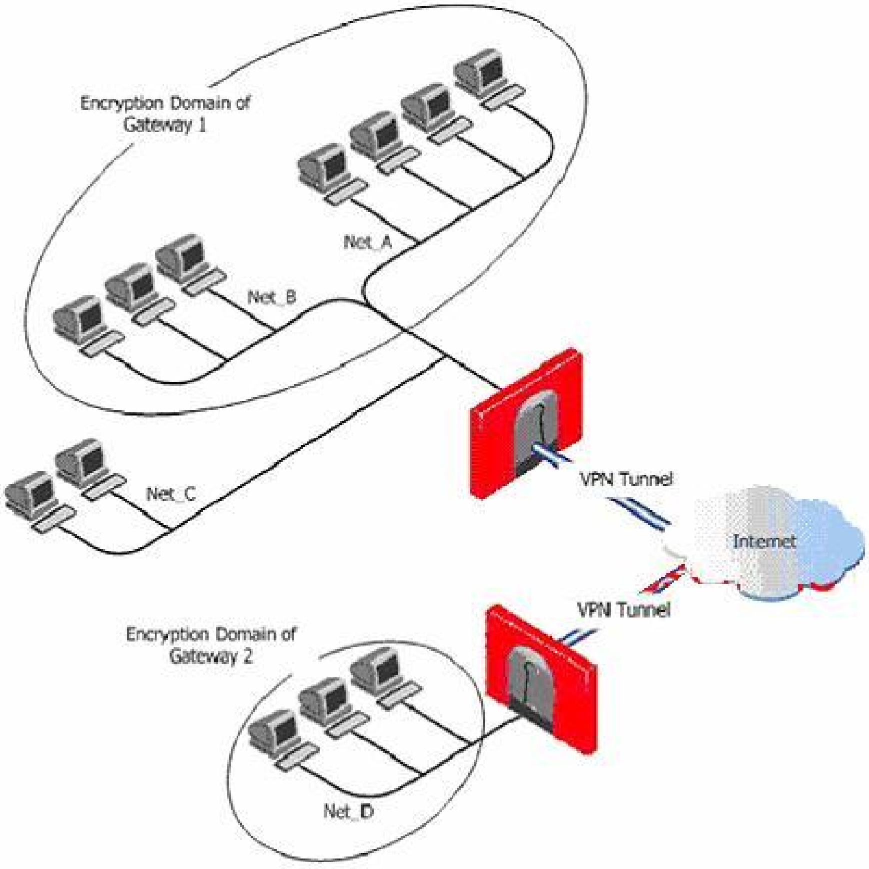

Encryption Domain of Gateway 1
Net_A
Net_B
Net_C
VPN Tunnel
Internet
VPN Tunnel
Encryption Domain of Gateway 2
Net_D

Figure 1: A VPN between Gateways, and the Encryption (VPN) Domain of each Gateway

A. Rule D

B. Rule B

C. Rule E

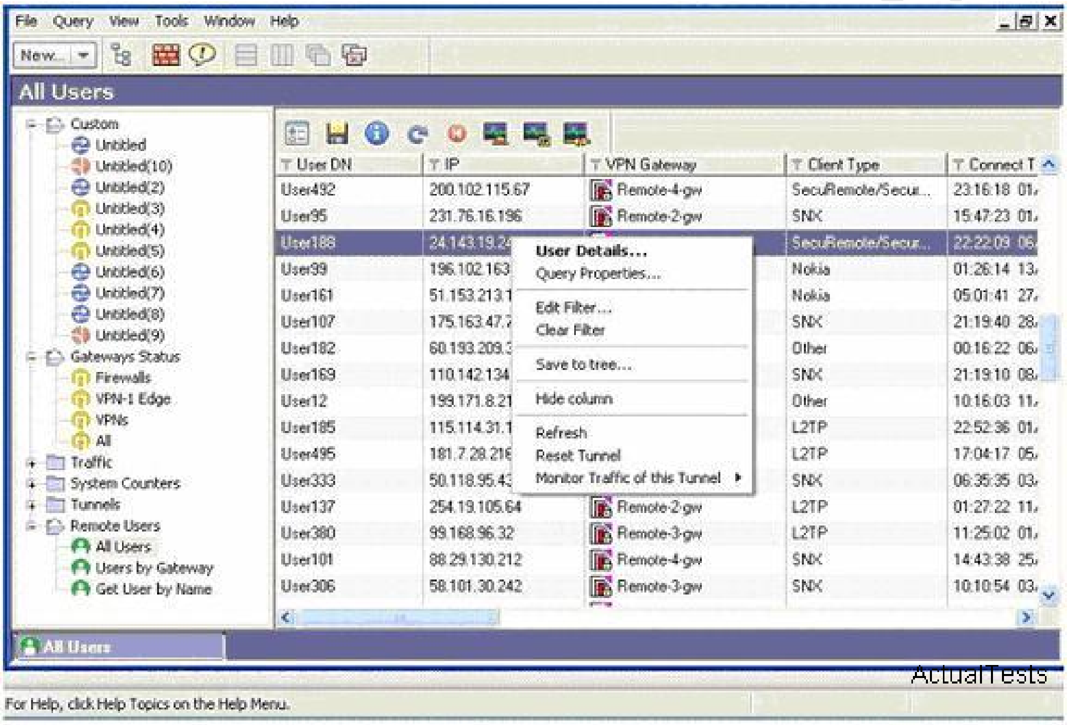
D. Rule A

E. Rule C

Answer: C

QUESTION NO: 418

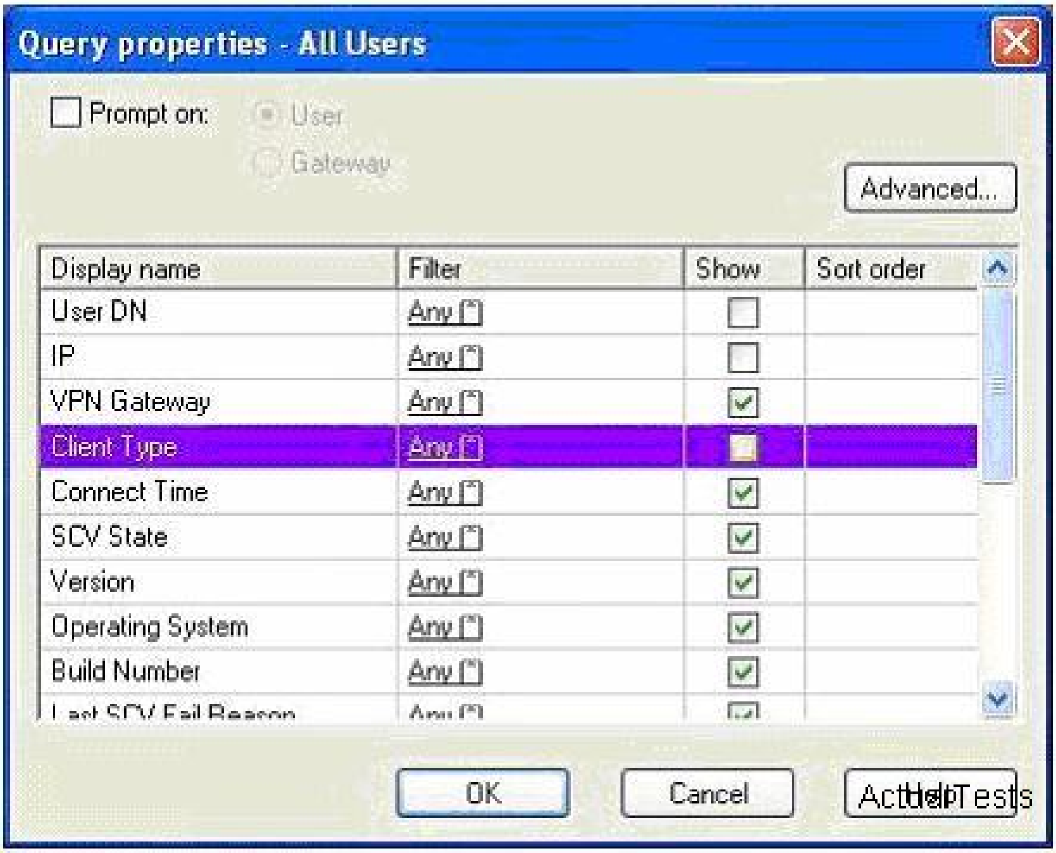
Diagram 1 shows SmartView Monitor, Remote Users view, All Users pagE. You highlighted a desired entry and right click to call the menu (shown in the diagram), you then select Hide Column option to hide any desired column. To reveal all the hidden column, what option must you select in the menu?



User DN	IP	VPN Gateway	Client Type	Connect T
User492	200.102.115.67	Remote-4-gw	SecuRemote/Secu...	23:16:18 01,
User95	231.76.16.196	Remote-2-gw	SNX	15:47:23 01,
User188	24.143.19.2		SecuRemote/Secu...	22:22:09 06,
User99	196.102.163		Nokia	01:26:14 13,
User161	51.153.213.1		Nokia	05:01:41 27,
User107	175.163.47.7		SNX	21:19:40 28,
User182	60.193.209.3		Other	00:16:22 06,
User169	110.142.134		SNX	21:19:10 08,
User12	199.171.8.21		Other	10:16:03 11,
User185	115.114.31.1		L2TP	22:52:36 01,
User495	181.7.28.216		L2TP	17:04:17 05,
User333	50.118.95.43		SNX	06:35:35 03,
User137	254.19.105.64	Remote-2-gw	L2TP	01:27:22 11,
User380	99.168.96.32	Remote-3-gw	L2TP	11:25:02 01,
User101	88.29.130.212	Remote-4-gw	SNX	14:43:38 25,
User306	58.101.30.242	Remote-3-gw	SNX	10:10:54 03,

For Help, click Help Topics on the Help Menu.

Figure 1: SmartView Monitor window: Remote Users View - All Users page



Query properties - All Users

□ Prompt on: ● User ○ Gateway

Display name	Filter	Show	Sort order
User DN	Any [*]	□	
IP	Any [*]	□	
VPN Gateway	Any [*]	☑	
Client Type	Any [*]	□	
Connect Time	Any [*]	☑	
SCV State	Any [*]	☑	
Version	Any [*]	☑	
Operating System	Any [*]	☑	
Build Number	Any [*]	☑	
Last SCV Fail Reason	Any [*]	☑	

Figure 2: Query Properties Window

A. Clear Filter
B. User Details
C. Edit Filter
D. Query Properties
E. Reset Tunnel

Answer: D

QUESTION NO: 419

How would you navigate from one SmartConsole GUI to another?

A. Select window menu from the GUI you are working on, then choose the client GUI you are switching to
B. Reboot the Client machinE. Log on into themachine, choose the programs, Firewall and client you want to switch to
C. Select file menu from the GUI you are working on, then choose the client GUI you are switching to
D. Not possible to navigate
E. Select policy menu from the GUI you are working on, then choose the client GUI you are switching to

Answer: A

QUESTION NO: 420

Using the Network Voyager to monitor your system health check, which of the following statistics can you not view there?

A. Interface Queue Statistics
B. Interface Traffic Statistics
C. SecureXL Connection Statistics
D. System Statistics
E. SecurePlatform Connection Statistics

Answer: E

QUESTION NO: 421

You are carrying out Tunnel testing. You configure one gateway as pinger and the other gateway as responder. What port must you configure the responder gateway to listen on for the communication?

A. 18234
B. 1834
C. 443
D. 80
E. 1024

Answer: A

QUESTION NO: 422

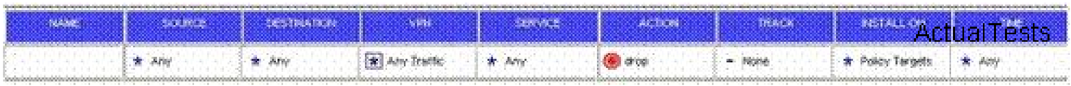
When you run FTP Activity report, you do not receive any datA. What would you do to rectify the issue?

A. Configure each FTP Activity on the Global Properties
B. Configure each FTP Activity on the Gateway
C. For each FTP Activity, create the associated resource
D. Do nothing
E. For each FTP Activity, create the associated resource and add a rule in the Security Policy whose service column uses this resource

Answer: E

QUESTION NO: 423

What rule is displayed when you add a rule to the RuleBase?



NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
	* Any	* Any	☒ Any Traffic	* Any	● drop	- None	* Policy Targets	* Any

A. Anti-Spoofing

B. Stealth Rule

C. NAT rule

D. Default rule

E. Cleanup rule

Answer: D

QUESTION NO: 424

How can a Security Gateway protect your internal network against a connection that does not pass through it?

A. By rejecting the connection

B. By rejecting the connection, advise the source to reconnect and make sure the new connection pass through it

C. It cannot

D. By redirecting the connection towards it and authenticate the connection

E. By accepting the connection

Answer: C

QUESTION NO: 425

Which of the following is true regarding configuration of clustering nodes?

A. Cluster nodes do not have to run exactly the same version of CheckPoint package

B. Each node must have exactly the same set of packages as all the other nodes

C. Each cluster node must run exactly the same version of R70

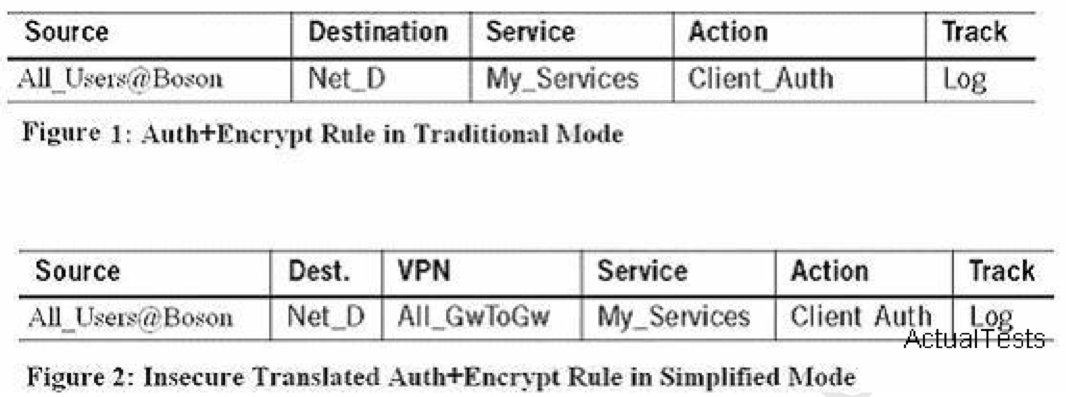
D. You must enable state synchronization

E. You must install R70 as an enforcement module (only) on each node

Answer: B,C,D,E

QUESTION NO: 426

Conversion of Auth+Encrypt Rules in Traditional Mode cannot be automatically translated in such a way that the translated Rule Base is at least as restrictive as the original rulE. The Converter wizard translates Auth+Encrypt rules (in Traditional Mode) to a single rule (in Simplified Mode) without adequate restriction or security. To correct this problem in the translated rule in the Simplified Mode you will have to:



Source	Destination	Service	Action	Track
All_Users@Boson	Net_D	My_Services	Client_Auth	Log

Figure 1: Auth+Encrypt Rule in Traditional Mode

Source	Dest.	VPN	Service	Action	Track
All_Users@Boson	Net_D	All_GwToGw	My_Services	Client Auth	Log

Figure 2: Insecure Translated Auth+Encrypt Rule in Simplified Mode

A. Add an encryption rule
B. Add a drop rule
C. Add an authentication + encryption rule
D. Add an accept rule
E. Add an authentication rule

Answer: B

QUESTION NO: 427

Which of the following is true of Eventia Reporter Licensing?

A. License is installed on a per Security Management Server basis
B. If you have a license for Security Gateway then you do not need a separate license for Eventia Reporter
C. License is installed on a per gateway basis
D. Up to 5 UTM-1 Edge devices are considered a single gateway
E. If you have three gateways and you buy three licenses, you do not have to select the gateways because the system knows that you only have three

Answer: C,D,E

QUESTION NO: 428

What view in the SmartView Monitor will you go to in order to view Information concerning the status, activities and hardware of the firewall currently being run by your company?

A. Tunnel View
B. Traffic View
C. Custom View
D. Remote User View
E. System Counters View

Answer: E

QUESTION NO: 429

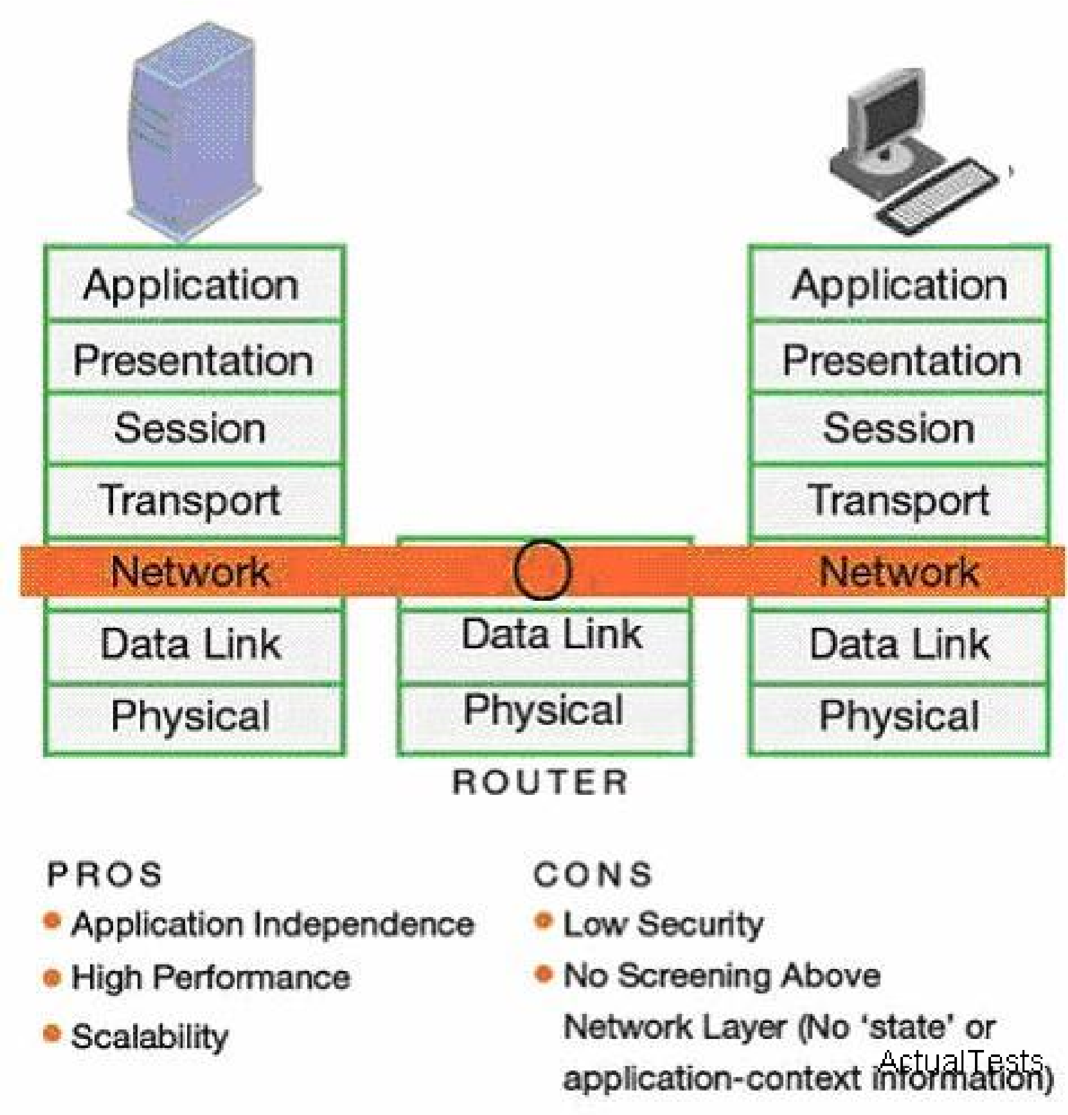
What command can be used to create disk mirror set?

A. add diskmirror set
B. create mirror set
C. add diskmirror
D. create diskmirror
E. create diskmirror set

Answer: C

QUESTION NO: 430

A typical packet filter rule base will include which of the following elements? Select all the correct answers.



A. Destination port
B. Destination address
C. Source port
D. State tables
E. Source address

Answer: A,B,C,E

QUESTION NO: 431

Using the Backup and Restore operation on R70, it is possible to:

A. Link the all cluster members for failover
B. Upgrade the SmartDashboard
C. Maintain a backup of the SmartCenter Management Server to be used in case of failover
D. Replace the original SmartCenter Management Server with another clone SmartCenter Management Server, while the original is being serviced

E. Upgrade the SmartCenter Management Server

Answer: C,D,E

QUESTION NO: 432

If security policy is enforced by more than two firewalled objects, how many rule bases would you need?

A. Three rule bases
B. Only one rule base
C. No rule base is needed to implement your security policy
D. Two rule bases
E. One rule base each for each number of network objects there

Answer: B

QUESTION NO: 433

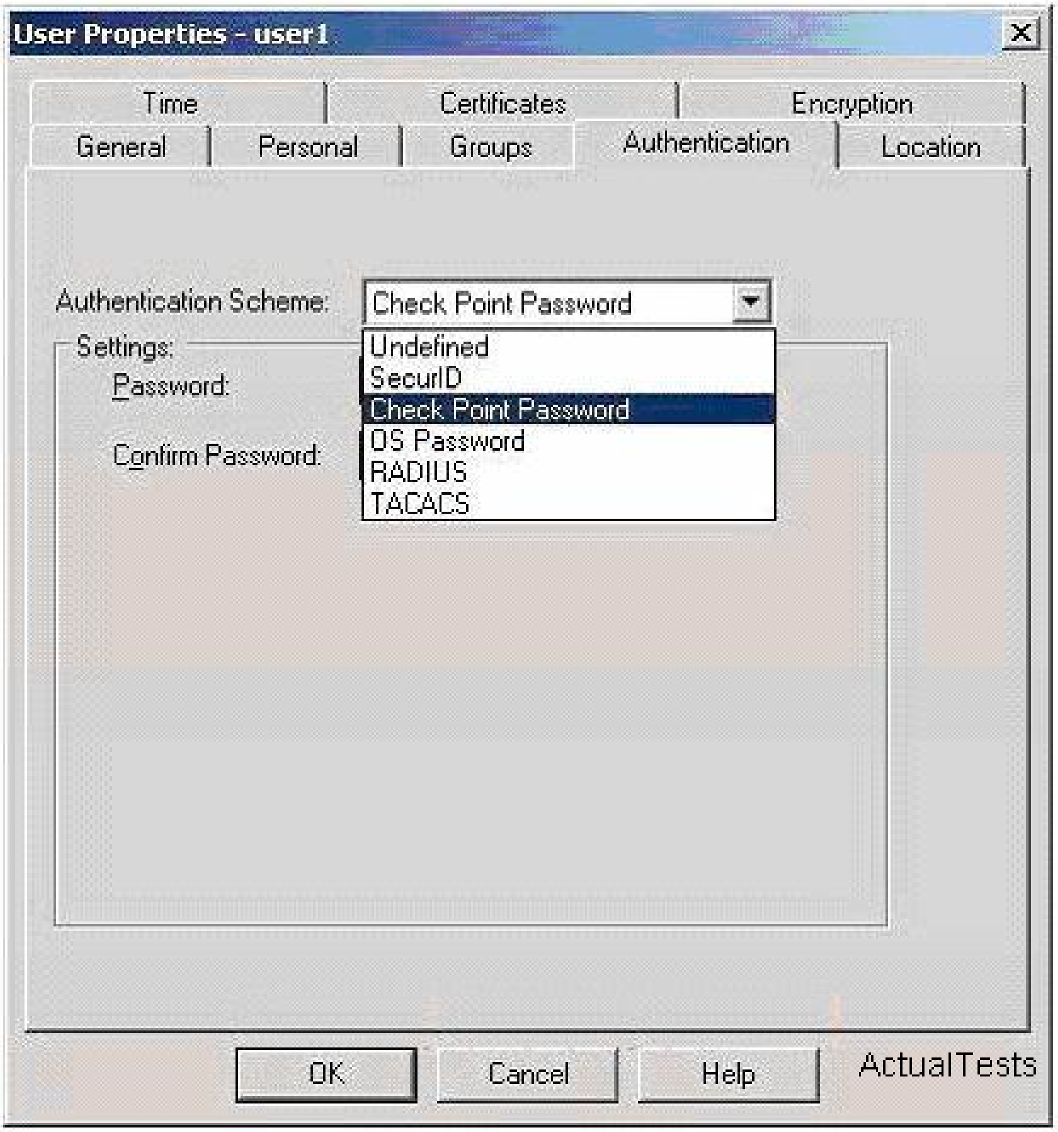
Which SmartConsole clients allows you to view captured packet from IPS?

A. SmartDashboard
B. Eventia Reporter
C. SmartUpdate
D. SmartView Tracker
E. SmartView Monitor

Answer: D

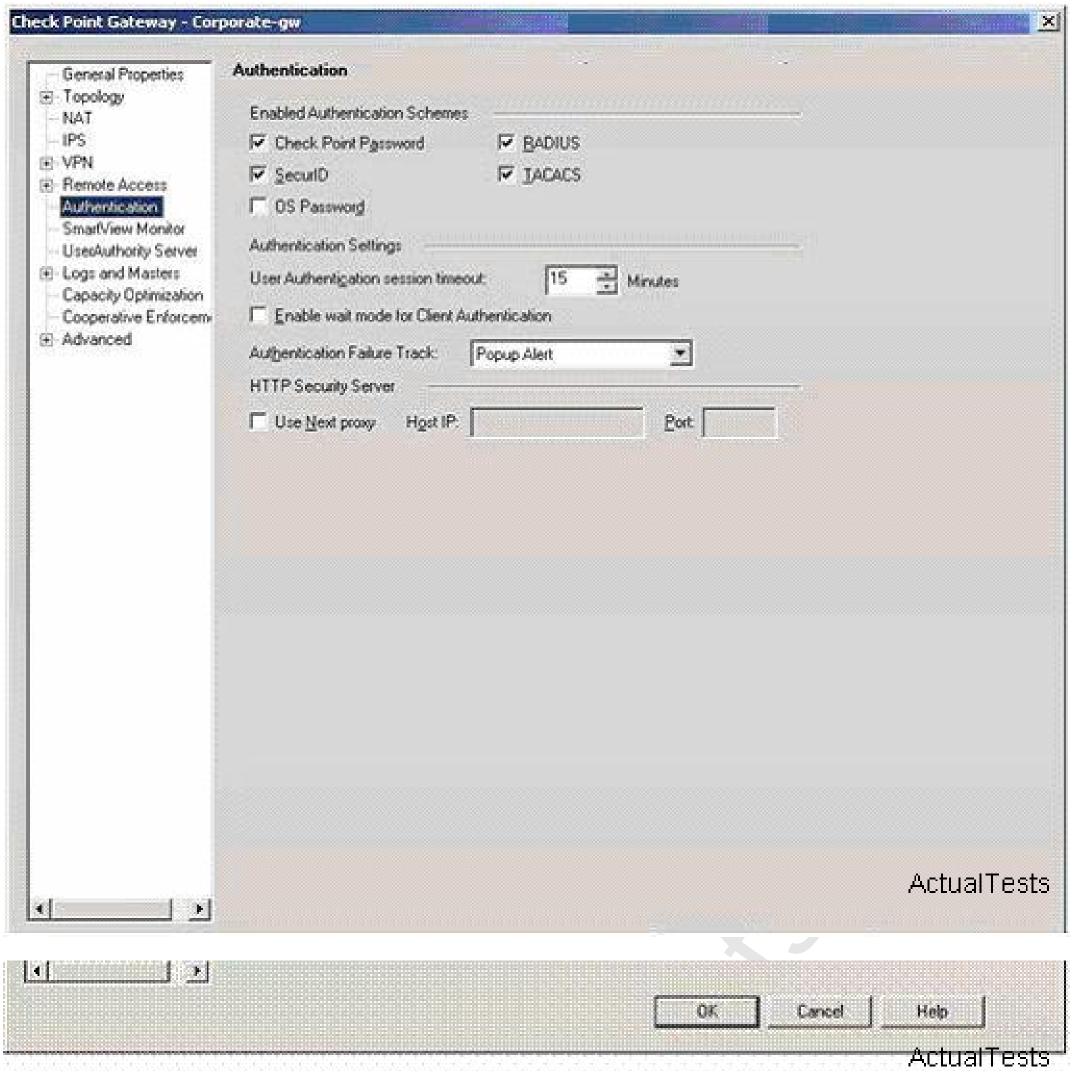
QUESTION NO: 434

Your new System Administrator is setting up User Authentication for the very first timE. After the setting up she tests it but does not work. You then ask her to follow the CheckPoint recommendation for troubleshooting. What is the Checkpoint recommended way to troubleshoot this?



Authentication Scheme: Check Point Password

Figure 1: User Properties window - Authentication tab



Authentication

Enabled Authentication Schemes

☑ Check Point Password ☑ RADIUS

☑ SecurID ☑ TACACS

□ OS Password

Authentication Settings

User Authentication session timeout: 15 Minutes

□ Enable wait mode for Client Authentication

Authentication Failure Track: Popup Alert

HTTP Security Server

□ Use Next proxy Host IP: Port:

Figure 2: Check Point Gateway Properties window - Authentication page

A. To delete the users and groups objects, re-create them and define new Authentication scheme for them

B. To verify the properties for the user attempting Authentication (this to include Authentication scheme), and to verify that the same Authentication scheme is selected in the Authentication properties of the network object for your firewall machine

C. To verify that Authentication type you setup for the Firewall Module is the same that you setup for the SmartCenter Management Server

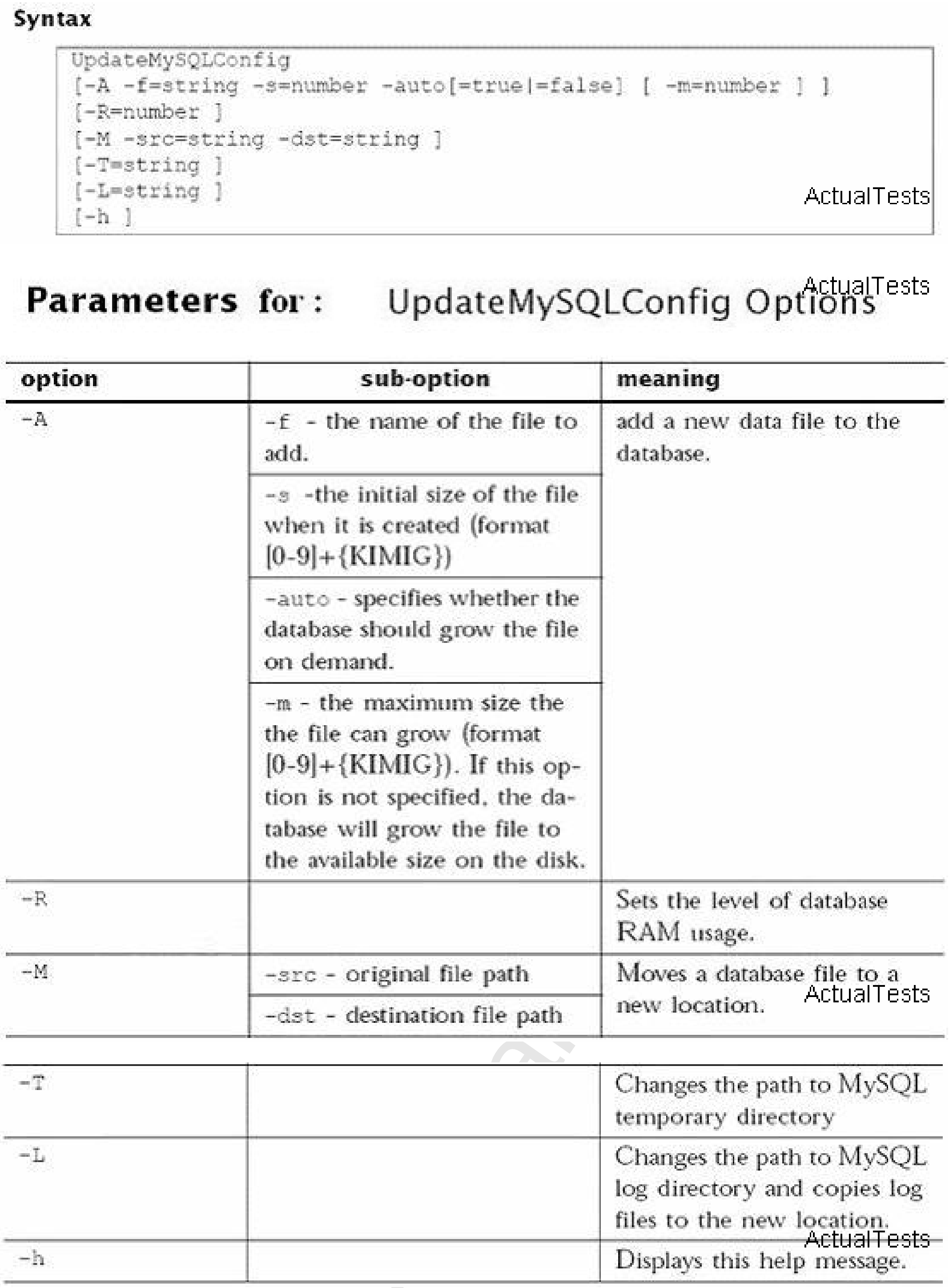
D. Configure your Firewall Module and set up new Authentication type and new Authentication scheme

E. Re-install Firewall Module and set up new Authentication type

Answer: B

QUESTION NO: 435

What file must edit in order to change the Eventia Reporter Database settings?



Syntax

```
UpdateMySQLConfig
[-A -f=string -s=number -auto[=true|=false] [ -m=number ] ]
[-R=number ]
[-M -src=string -dst=string ]
[-T=string ]
[-L=string ]
[-h ]
```

Parameters for : UpdateMySQLConfig Options

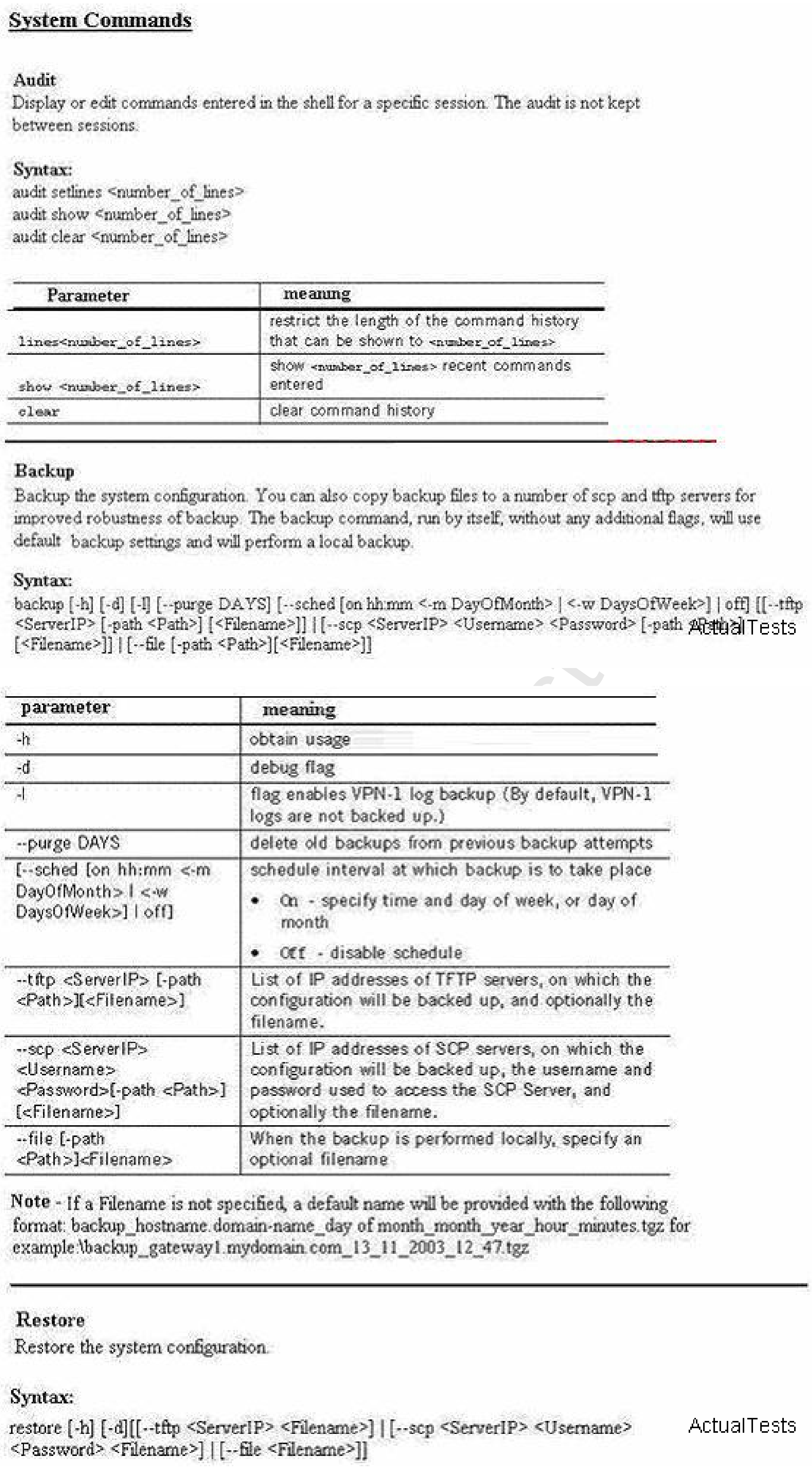
option	sub-option	meaning
-A	-f - the name of the file to add.	add a new data file to the database.
	-s -the initial size of the file when it is created (format [0-9]+{KIMIG})	
	-auto - specifies whether the database should grow the file on demand.	
	-m - the maximum size the the file can grow (format [0-9]+{KIMIG}). If this option is not specified, the database will grow the file to the available size on the disk.	
-R		Sets the level of database RAM usage.
-M	-src - original file path	Moves a database file to a new location.
	-dst - destination file path	
-T		Changes the path to MySQL temporary directory
-L		Changes the path to MySQL log directory and copies log files to the new location.
-h		Displays this help message.

A. objects_5_0.C
B. userC. C
C. my.cnf
D. userC. conf
E. my.ini

Answer: E

QUESTION NO: 436

The command line in SecurePlatform to reboot a system is:



System Commands

Audit

Display or edit commands entered in the shell for a specific session. The audit is not kept between sessions.

Syntax:

audit setlines <number_of_lines>
audit show <number_of_lines>
audit clear <number_of_lines>

Parameter	meaning
lines<number_of_lines>	restrict the length of the command history that can be shown to <number_of_lines>
show <number_of_lines>	show <number_of_lines> recent commands entered
clear	clear command history

Backup

Backup the system configuration. You can also copy backup files to a number of scp and tftp servers for improved robustness of backup. The backup command, run by itself, without any additional flags, will use default backup settings and will perform a local backup.

Syntax:

backup [-h] [-d] [-l] [--purge DAYS] [--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek>] | off] [[--tftp <ServerIP> [-path <Path>] [<Filename>]] | [--scp <ServerIP> <Username> <Password> [-path <Path>] [<Filename>]] | [--file [-path <Path>][<Filename>]]

parameter	meaning
-h	obtain usage
-d	debug flag
-l	flag enables VPN-1 log backup (By default, VPN-1 logs are not backed up.)
--purge DAYS	delete old backups from previous backup attempts
[--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek>] | off]	schedule interval at which backup is to take place • On - specify time and day of week, or day of month • Off - disable schedule
--tftp <ServerIP> [-path <Path>][<Filename>]	List of IP addresses of TFTP servers, on which the configuration will be backed up, and optionally the filename.
--scp <ServerIP> <Username> <Password>[-path <Path>] [<Filename>]	List of IP addresses of SCP servers, on which the configuration will be backed up, the username and password used to access the SCP Server, and optionally the filename.
--file [-path <Path>]<Filename>	When the backup is performed locally, specify an optional filename

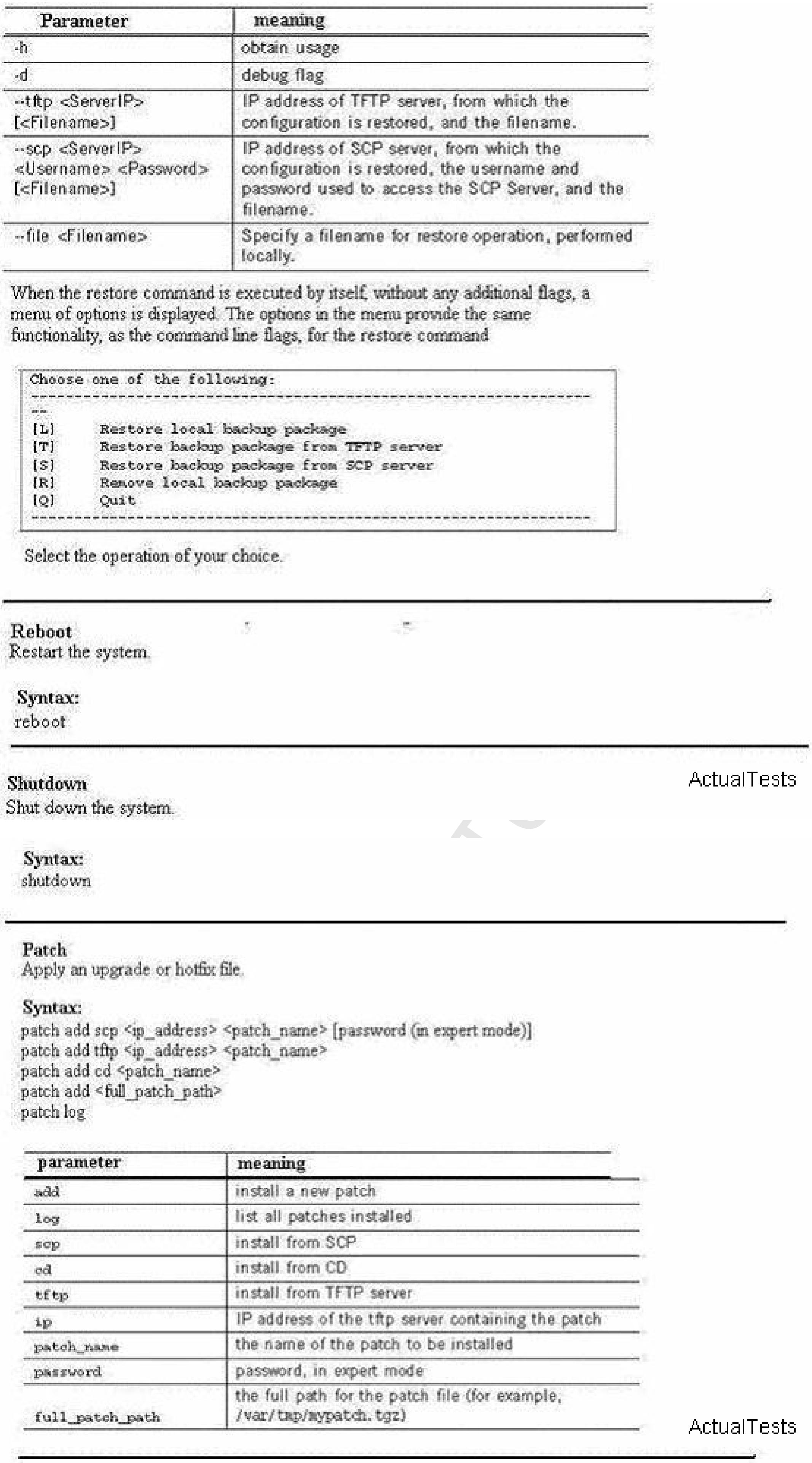
Note - If a Filename is not specified, a default name will be provided with the following format: backup_hostname.domain-name_day of month_month_year_hour_minutes.tgz for example:\backup_gateway1.mydomain.com_13_11_2003_12_47.tgz

Restore

Restore the system configuration.

Syntax:

restore [-h] [-d][[--tftp <ServerIP> <Filename>] | [--scp <ServerIP> <Username> <Password> <Filename>] | [--file <Filename>]]



Parameter	meaning
-h	obtain usage
-d	debug flag
--tftp <ServerIP> [<Filename>]	IP address of TFTP server, from which the configuration is restored, and the filename.
--scp <ServerIP> <Username> <Password> [<Filename>]	IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.
--file <Filename>	Specify a filename for restore operation, performed locally.

When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command

```
Choose one of the following:
-----------------------------------------------------------------------
--
[L]      Restore local backup package
[T]      Restore backup package from TFTP server
[S]      Restore backup package from SCP server
[R]      Remove local backup package
[Q]      Quit
-----------------------------------------------------------------------
```

Select the operation of your choice.

Reboot
Restart the system.

Syntax:
reboot

Shutdown
Shut down the system.

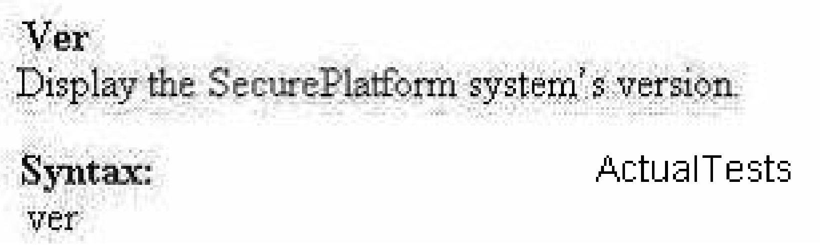
Syntax:
shutdown

Patch
Apply an upgrade or hotfix file.

Syntax:

```
patch add scp <ip_address> <patch_name> [password (in expert mode)]
patch add tftp <ip_address> <patch_name>
patch add cd <patch_name>
patch add <full_patch_path>
patch log
```

parameter	meaning
add	install a new patch
log	list all patches installed
scp	install from SCP
cd	install from CD
tftp	install from TFTP server
ip	IP address of the tftp server containing the patch
patch_name	the name of the patch to be installed
password	password, in expert mode
full_patch_path	the full path for the patch file (for example, /var/tmp/mypatch.tgz)



Ver

Display the SecurePlatform system's version.

Syntax:

ver

A. boot

B. restart

C. reboot

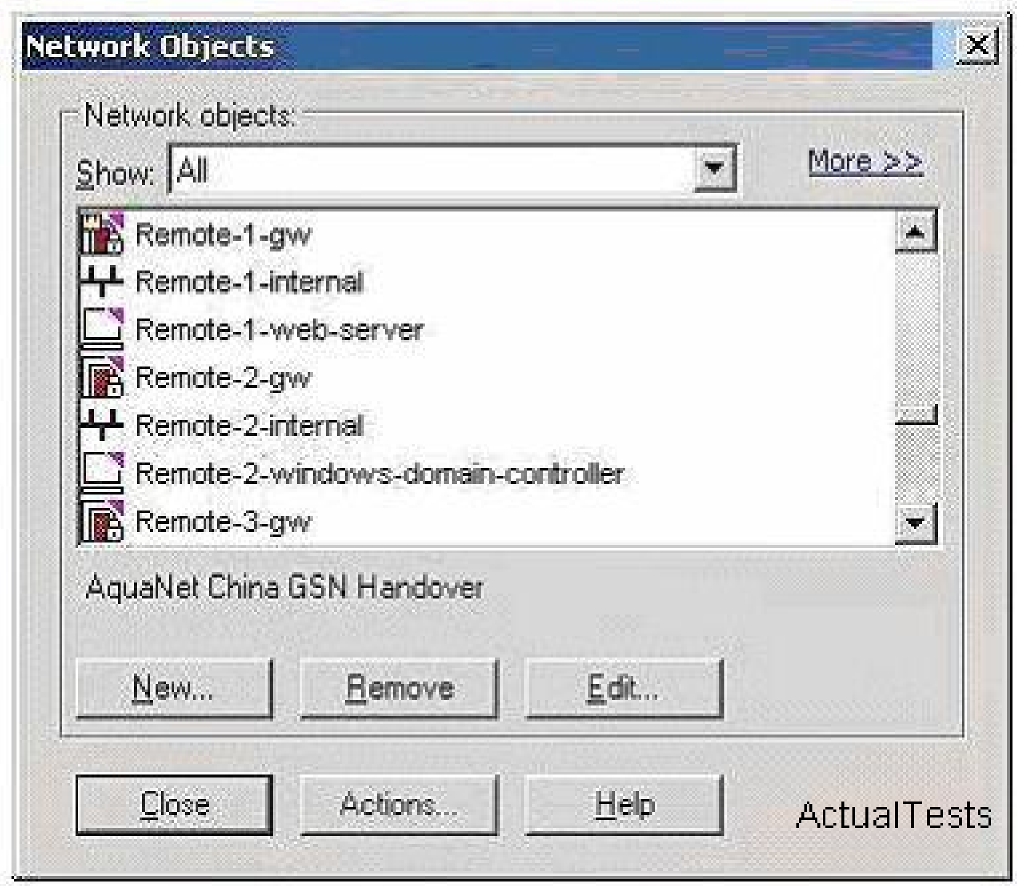
D. start

E. startup

Answer: C

QUESTION NO: 437

What option would you select in the Topology tab of Interface Property box when configuring anti-spoofing protection, to ensure that anti-spoofing verification does not occur for addresses coming from internal networks into the external interface?



Network Objects

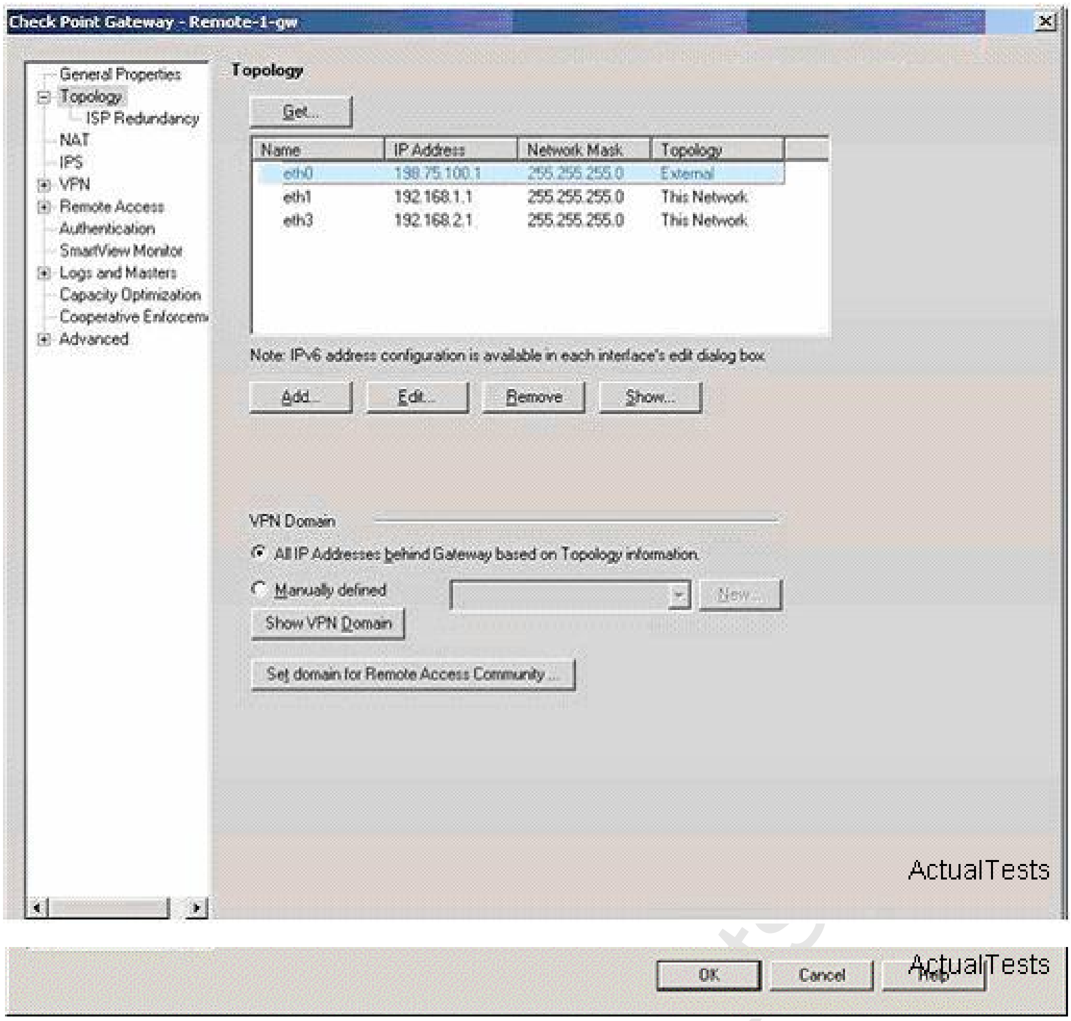
Network objects:

Show: All

- Remote-1-gw
- Remote-1-internal
- Remote-1-web-server
- Remote-2-gw
- Remote-2-internal
- Remote-2-windows-domain-controller
- Remote-3-gw

AquaNet China GSN Handover

Figure 1: Network Objects box



Check Point Gateway - Remote-1-gw

Topology

Name	IP Address	Network Mask	Topology
eth0	198.75.100.1	255.255.255.0	External
eth1	192.168.1.1	255.255.255.0	This Network
eth3	192.168.2.1	255.255.255.0	This Network

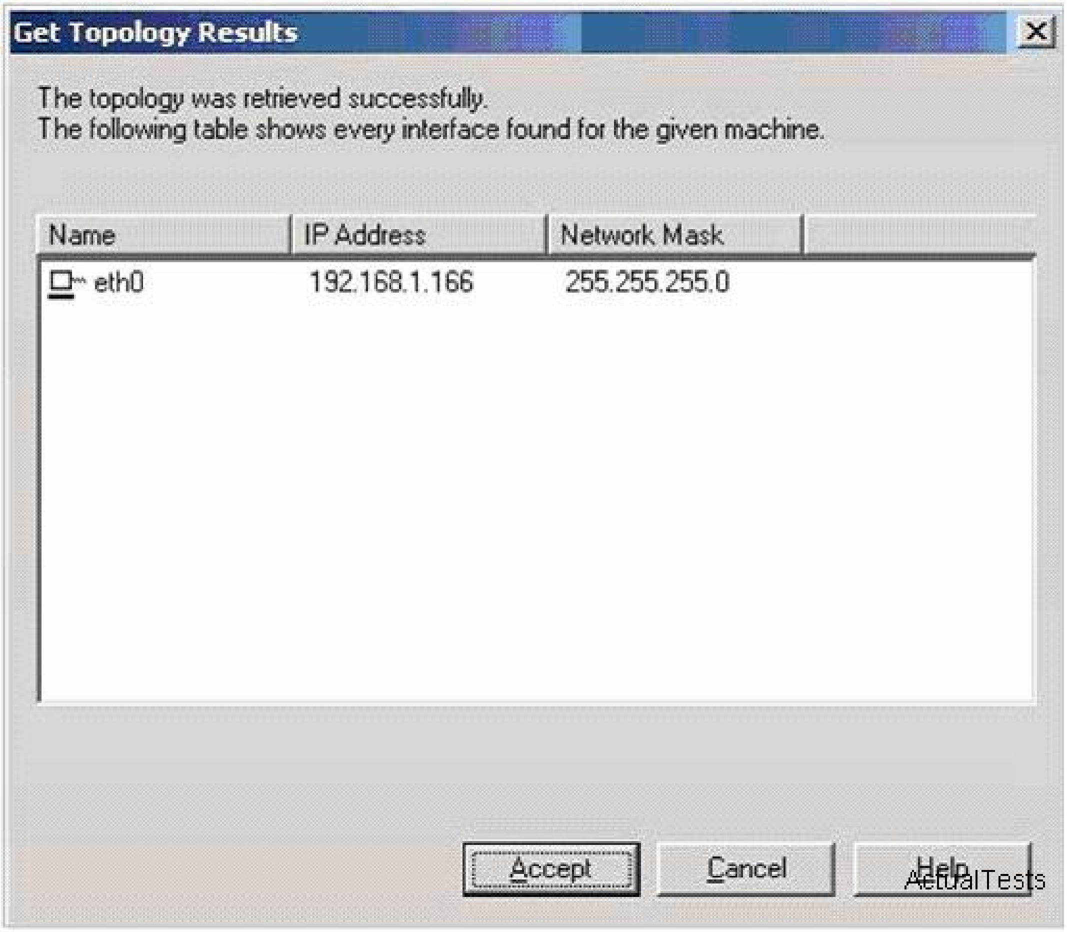
Note: IPv6 address configuration is available in each interface's edit dialog box.

VPN Domain

● All IP Addresses behind Gateway based on Topology information.

○ Manually defined

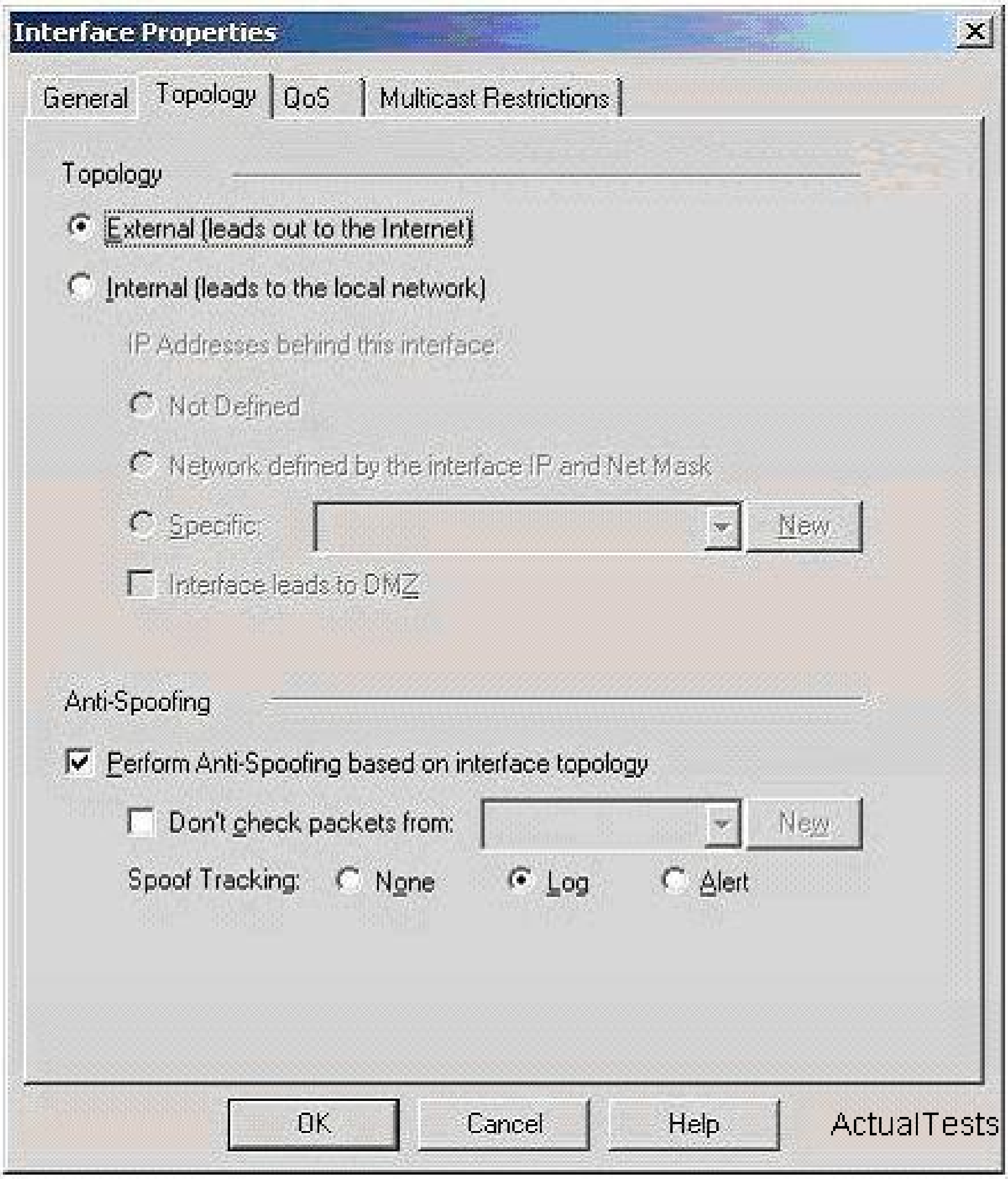
Figure 2: CheckPoint Gateway Properties box



The topology was retrieved successfully.
The following table shows every interface found for the given machine.

Name	IP Address	Network Mask
eth0	192.168.1.166	255.255.255.0

Figure 3: Get Topology Results box



Interface Properties

Topology

● External (leads out to the Internet)

○ Internal (leads to the local network)

IP Addresses behind this interface

○ Not Defined

○ Network defined by the interface IP and Net Mask

○ Specific:

□ Interface leads to DMZ

Anti-Spoofing

☑ Perform Anti-Spoofing based on interface topology

□ Don't check packets from:

Spoof Tracking: ○ None ● Log ○ Alert

Figure 4: Interface Properties box

A. External (leads out to the Internet)
B. Interface leads to DMZ
C. IP addresses behind this interface
D. Internal (leads to the local network)
E. Perform Anti-Spoofing based on Interface topology

Answer: E

QUESTION NO: 438

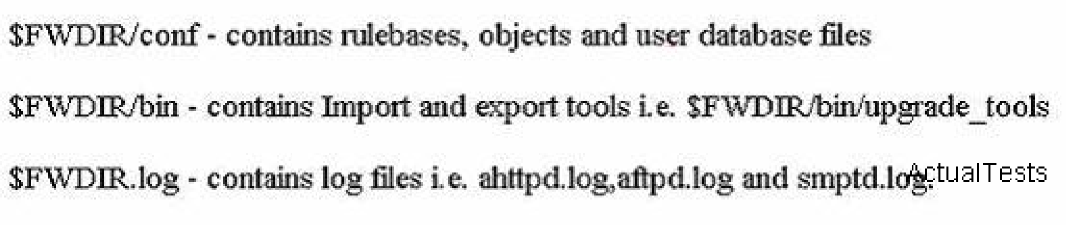
In IPSO directory structure, what does image folder contain?

A. System log files
B. The kernel image
C. The software packages
D. Execution programs on startup
E. IPSO configuration file

Answer: B

QUESTION NO: 439

What directory in R70 contains all of the Rule Bases, objects, and the user database files?



$FWDIR/conf - contains rulebases, objects and user database files

$FWDIR/bin - contains Import and export tools i.e. $FWDIR/bin/upgrade_tools

$FWDIR.log - contains log files i.e. ahttpd.log,aftpd.log and smptd.log.

A. $FWDIR/bin directory
B. Winnt/Config directory
C. $FWDIR/etc directory
D. $FWDIR/conf directory
E. $FWDIR/bin/etc directory

Answer: D

QUESTION NO: 440

The diagram 1 shows the custom view of SmartView Monitor with list of IP addresses. The highlighted entry shows Ip address whose destination you want to block. You will receive Block Suspicious Activity window shown in diagram 2 when you select Block Destination in the menu (by right-clicking the highlighted IP address entry). Which of the following is true of this blocked connection?

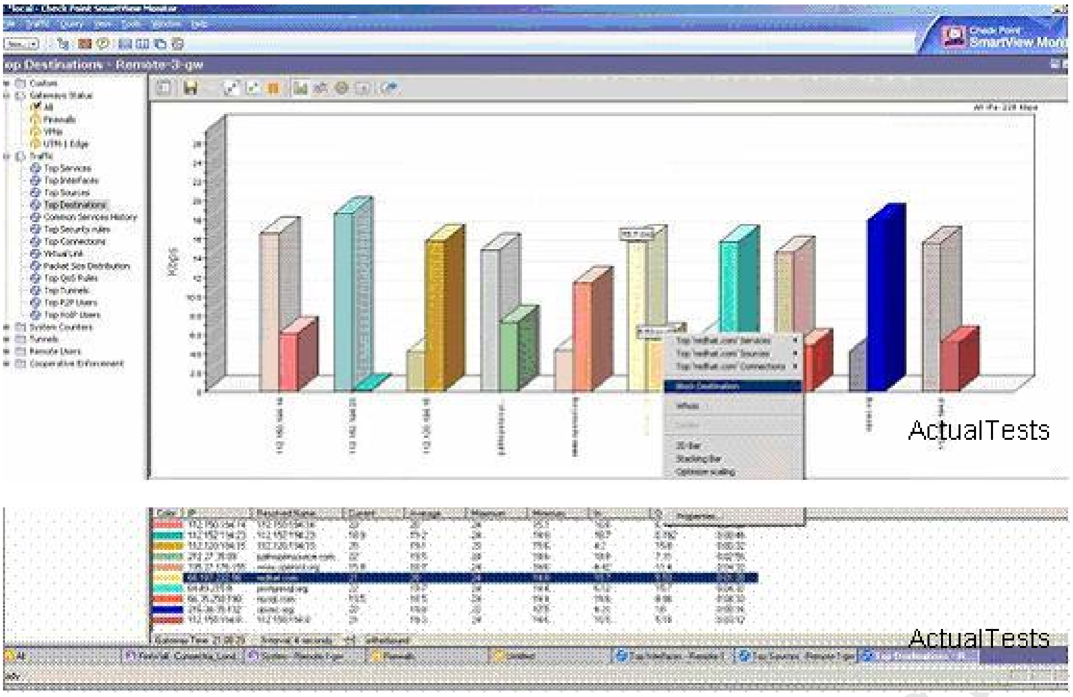
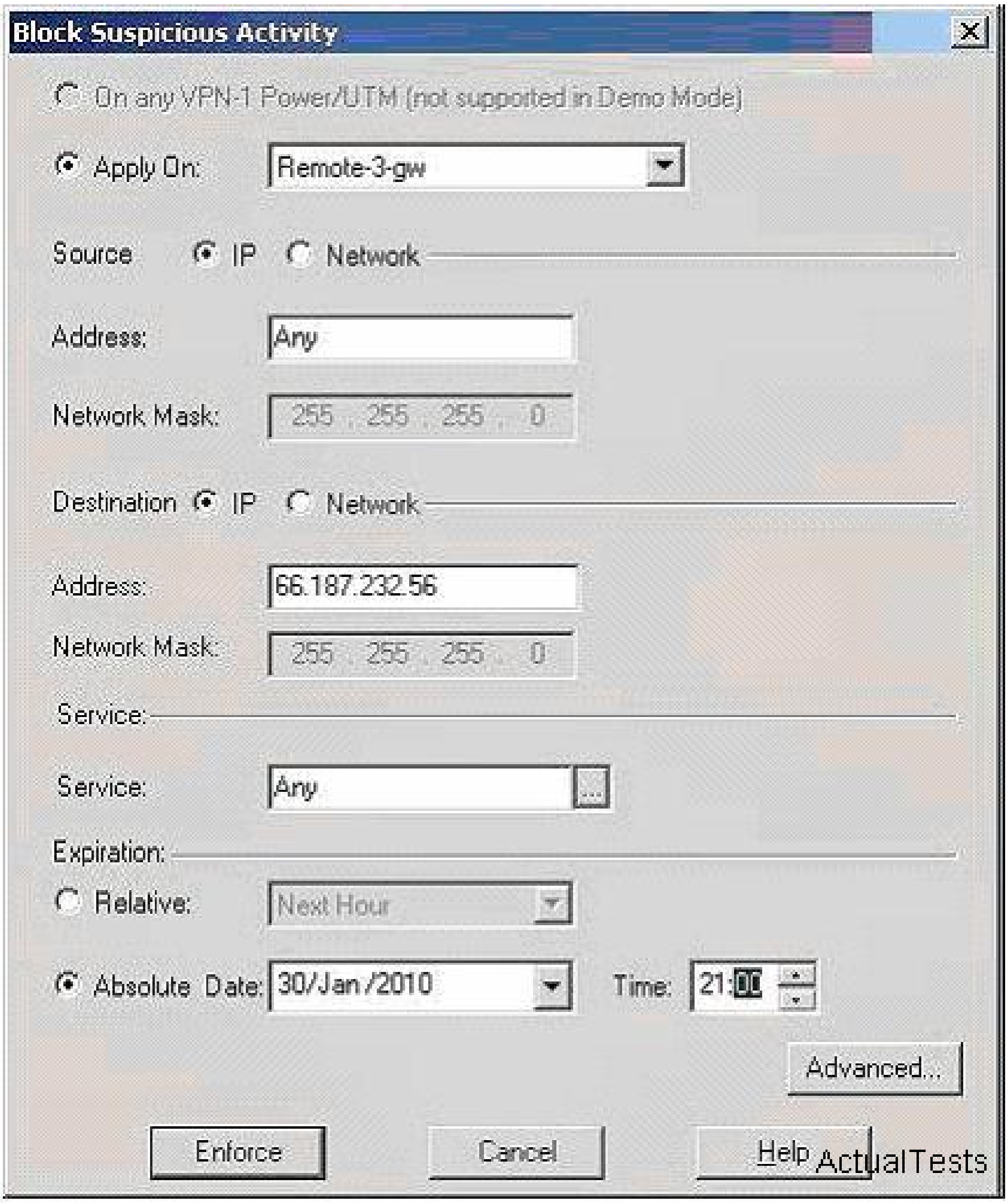


Figure 1: SmartView Monitor



Block Suspicious Activity

○ On any VPN-1 Power/UTM (not supported in Demo Mode)

● Apply On: Remote-3-gw

Source ● IP ○ Network

Address: Any

Network Mask: 255 . 255 . 255 . 0

Destination ● IP ○ Network

Address: 66.187.232.56

Network Mask: 255 . 255 . 255 . 0

Service:

Service: Any

Expiration:

○ Relative: Next Hour

● Absolute Date: 30/Jan/2010 Time: 21:00

Figure 2: Block Suspicious Activity window

A. Once you click enforce button, the redhat.com is inaccessible

B. Any connection from any source, from11 Oct 2005 should be able to access redhat.com

C. Any connection from any source, after30 Jan 2010 should be able to access redhat.com

D. Any service to this destination is blocked

E. Once you click enforce button, source address connecting to the redhat.com isBlocked

Answer: A,C,D

QUESTION NO: 441

What is the role of the IPSRD?

A. To ensure that the business information is delivered in a secure a manner

B. To support a wide array of routing protocols

C. To support NGX functionality

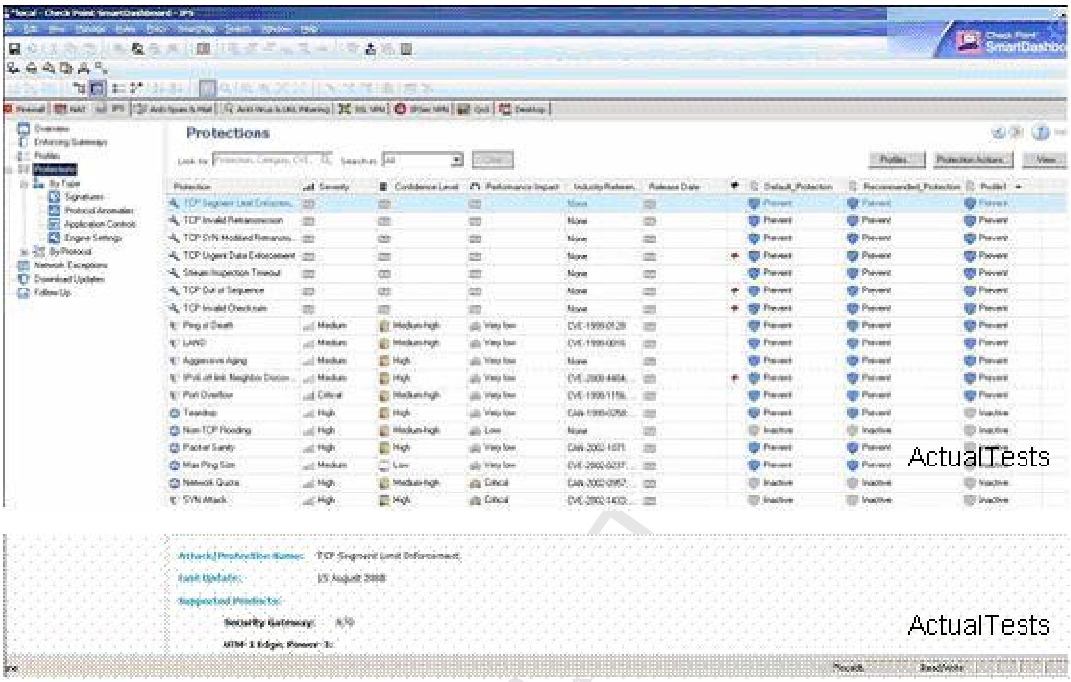
D. To harden a network security

E. To dynamically compute paths or routes to remote networks

Answer: E

QUESTION NO: 442

In IPS, you can export the Protections list as a text filE. What sort of file is this?



Protections

Protection	Severity	Confidence Level	Performance Impact	Industry Referen...	Release Date	⚑	Default_Protection	Recommended_Protection	Profile1
TCP Segment Limit Enforcem...				None			Prevent	Prevent	Prevent
TCP Invalid Retransmission				None			Prevent	Prevent	Prevent
TCP SYN Modified Retransmis...				None			Prevent	Prevent	Prevent
TCP Urgent Data Enforcement				None		⚑	Prevent	Prevent	Prevent
Stream Inspection Timeout				None			Prevent	Prevent	Prevent
TCP Out of Sequence				None		⚑	Prevent	Prevent	Prevent
TCP Invalid Checksum				None		⚑	Prevent	Prevent	Prevent
Ping of Death	Medium	Medium-high	Very low	CVE-1999-0128			Prevent	Prevent	Prevent
LAND	Medium	Medium-high	Very low	CVE-1999-0016			Prevent	Prevent	Prevent
Aggressive Aging	Medium	High	Very low	None			Prevent	Prevent	Prevent
IPv6 off-link Neighbor Discov...	Medium	High	Very low	CVE-2008-4404...		⚑	Prevent	Prevent	Prevent
Port Overflow	Critical	Medium-high	Very low	CVE-1999-1156...			Prevent	Prevent	Prevent
Teardrop	High	High	Very low	CAN-1999-0258...			Prevent	Prevent	Inactive
Non-TCP Flooding	High	Medium-high	Low	None			Inactive	Inactive	Inactive
Packet Sanity	High	High	Very low	CAN-2002-1071			Prevent	Prevent	[illegible]
Max Ping Size	Medium	Low	Very low	CVE-2002-0237...			Prevent	Prevent	[illegible]
Network Quota	High	Medium-high	Critical	CAN-2002-0957...			Inactive	Inactive	Inactive
SYN Attack	High	High	Critical	CVE-2002-1403...			Inactive	Inactive	Inactive

Attack/Protection Name: TCP Segment Limit Enforcement

Last Update: 15 August 2008

Supported Products:

Security Gateway: N/A

UTM-1 Edge, Power-1:

Figure 1: IPS Tab - Protections Page

A. PDF extension file

B. Template file

C. Word document file

D. Adobe acrobat file

E. Comma-delimited file

Answer: E

QUESTION NO: 443

Roger is a Security Administrator that is troubleshooting a connectivity problem. The diagram of his network is shown in the diagram. Roger is using a packet capture equipment for troubleshooting and the equipment shows that the packets are arriving at Ie0 interface, but a packet capture on the internal network localnet do not show that the packets are leaving the Gateway. He checks the security Policy and that seems to be okay. He now checks routing configuration and that seems to be okay too. What is likely to be the cause of the problem?

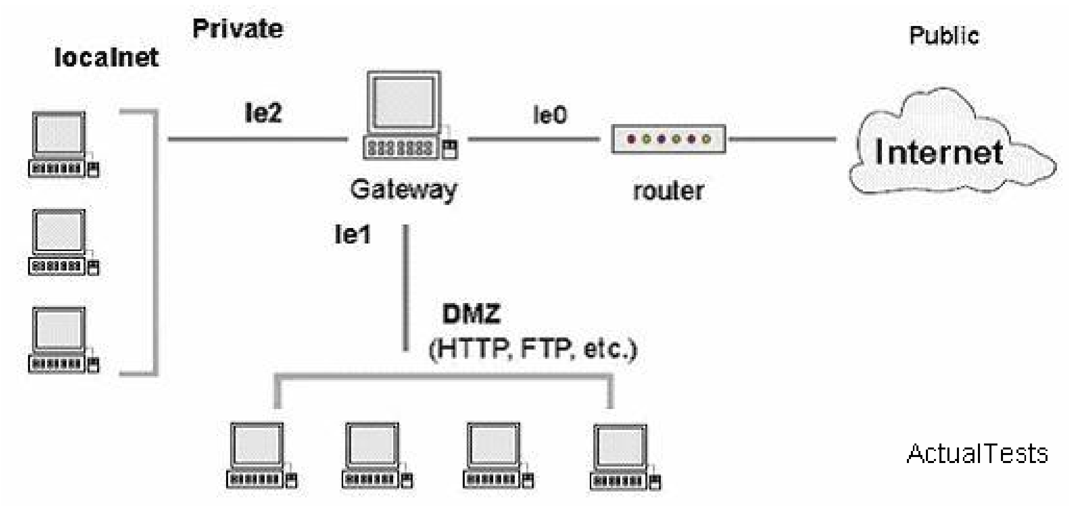


Figure 1: Connectivity Problem

A. The Ie2 might be faulty
B. The routing might be incorrectly configured
C. The Ie1 might be faulty
D. The Ie0 might be faulty
E. The stealth rule might be the problem

Answer: A

QUESTION NO: 444

In SmartView Tracker GUI, what option do you select to delete all records in the active Log File?

A. Purge Active File
B. Remove Active File
C. Kill Active File
D. Cut Active File
E. Delete Active File

Answer: A

QUESTION NO: 445

Where would you go to configure Migration from Traditional Mode to Simplified Mode?

A. Global Properties > Firewall page
B. Global Properties > VPN page
C. Global Properties > Traditional to Simplified page
D. Global Properties > Simplified page
E. Global Properties > Traditional page

Answer: B

QUESTION NO: 446

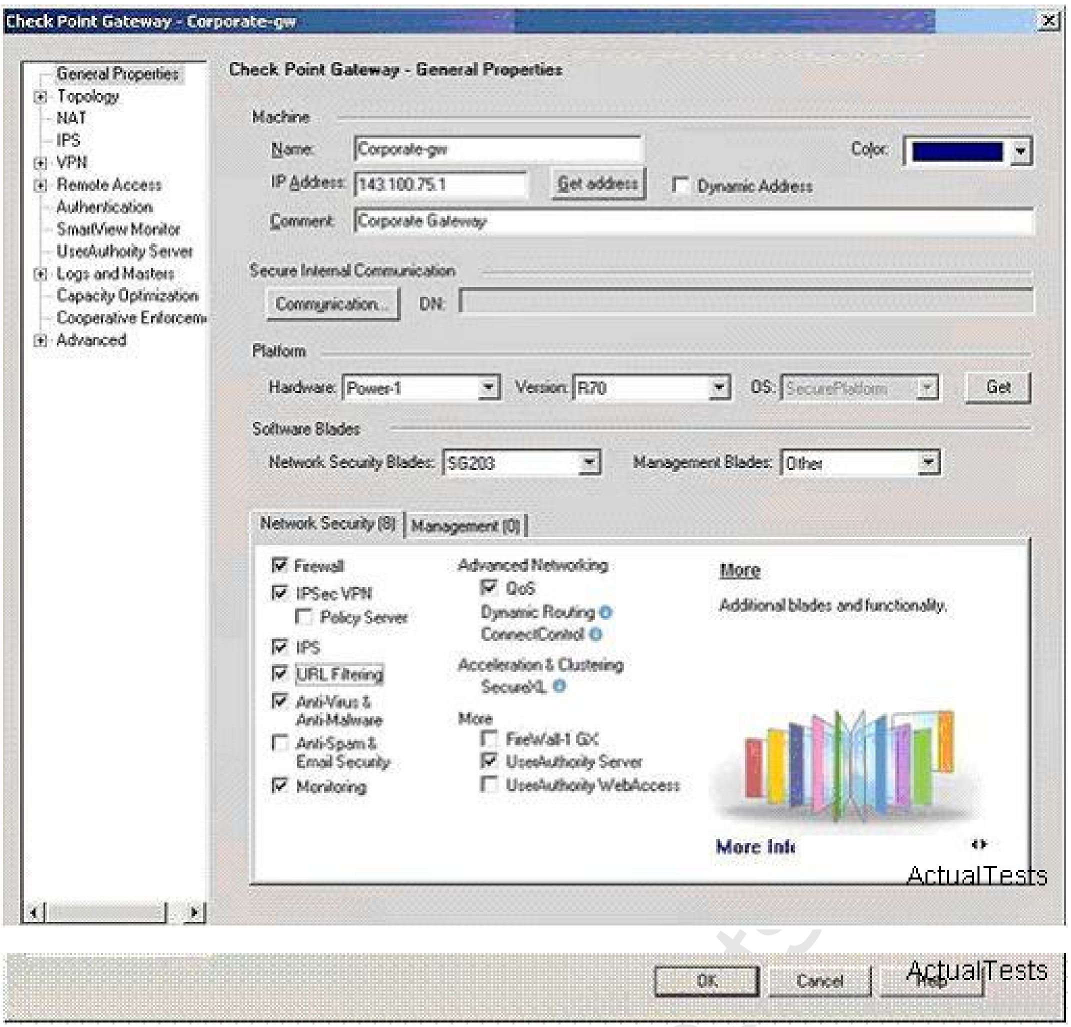
What tool will you use to configure a freshly installed IPSO?

A. CLI
B. SmartDashboard
C. cpconfig
D. cpstop
E. cpstart

Answer: C

QUESTION NO: 447

To configure integrated Anti-Virus scanning, you will go to: (see the diagram if you failed the question).



Check Point Gateway - Corporate-gw

Check Point Gateway - General Properties

Machine

Name: Corporate-gw

Color:

IP Address: 143.100.75.1

□ Dynamic Address

Comment: Corporate Gateway

Secure Internal Communication

DN:

Platform

Hardware: Power-1

Version: R70

OS: SecurePlatform

Software Blades

Network Security Blades: SG203

Management Blades: Other

Network Security (8) | Management (0)

☑ Firewall

☑ IPSec VPN

□ Policy Server

☑ IPS

☑ URL Filtering

☑ Anti-Virus & Anti-Malware

□ Anti-Spam & Email Security

☑ Monitoring

Advanced Networking

☑ QoS

Dynamic Routing

ConnectControl

Acceleration & Clustering

SecureXL

More

□ FireWall-1 GX

☑ UserAuthority Server

□ UserAuthority WebAccess

More

Additional blades and functionality.

A. Service Properties window

B. Global Properties

C. User Properties window

D. The Software Blades section in the General Properties page of the Gateway

E. Anti-virus scanning page in the Global Properties

Answer: D

QUESTION NO: 448

Which of the following provides you with easiest and most efficient method of upgrade of NGX across distributed installations?

A. Using SecureClient Packaging Tool GUI

B. Using upgrade_import tool

C. Using NGX CDROM for manual installation

D. Using SmartUpdate GUI

E. Using SmartCenter

Answer: D

QUESTION NO: 449

Version Operations are performed via the Database Revision Control window. With this window you can:

A. Revert to a saved version
B. Create a new version of the current policy manually
C. Delete a selected version
D. View a saved version
E. Clone a selected version

Answer: A,B,C,D

QUESTION NO: 450

Following the implied rule base order, what rule is processed last?

A. Implicit Drop Rule
B. Default Rule
C. Direct Rule
D. Explicit Rule
E. Stealth Rule

Answer: A

QUESTION NO: 451

Diagram 1 depicts Wire Mode with Route Based VPN configuration. Gateway A and B are satellite gateways and gateway C is a center gateway. Wire mode is enabled on Center Gateway C. Host 1 residing behind Satellite Gateway A wishes to open a connection through a VPN tunnel with Host 2 behind Satellite Gateway B. Which of the following is true of the configuration?

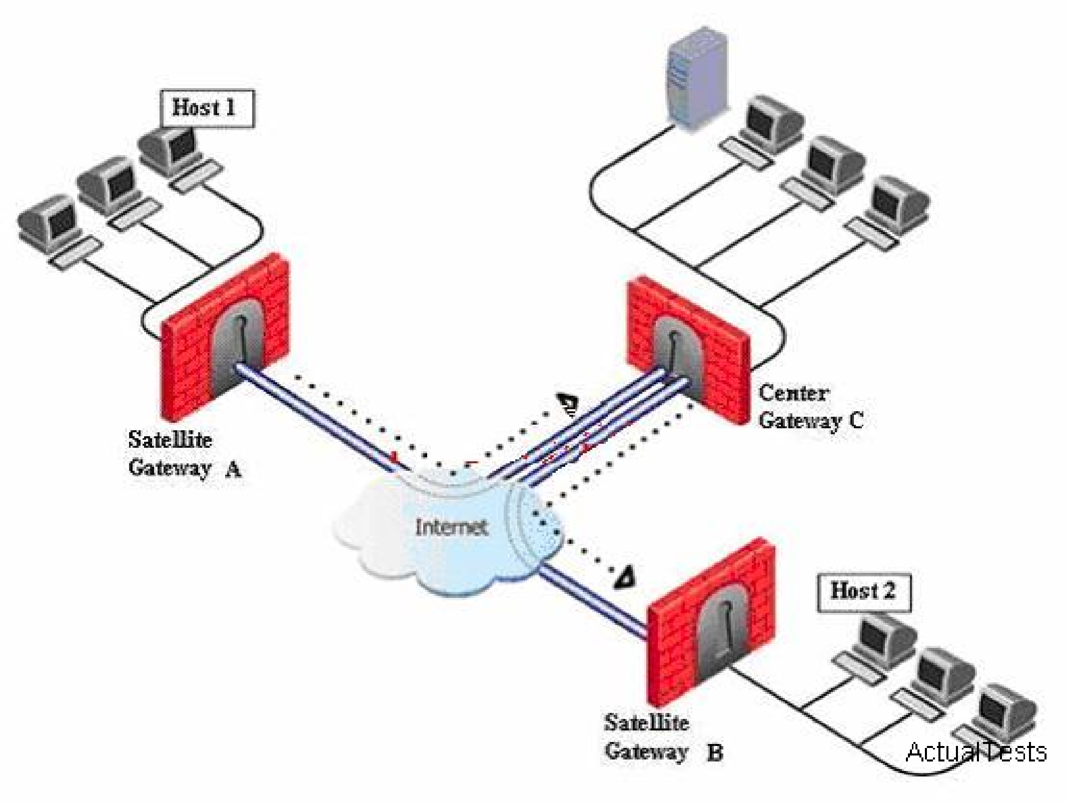


Figure 1: Wire Mode in a Satellite Community

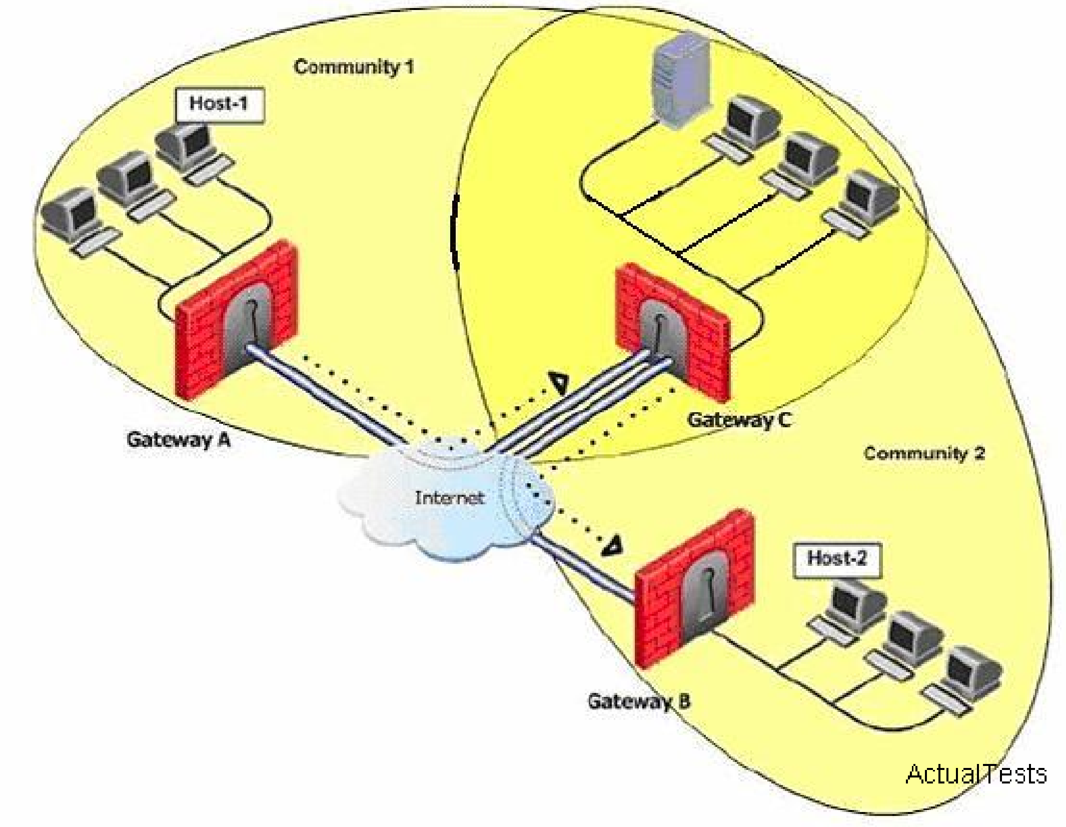


FIGURE 2: Wire Mode Between Two VPN Communities

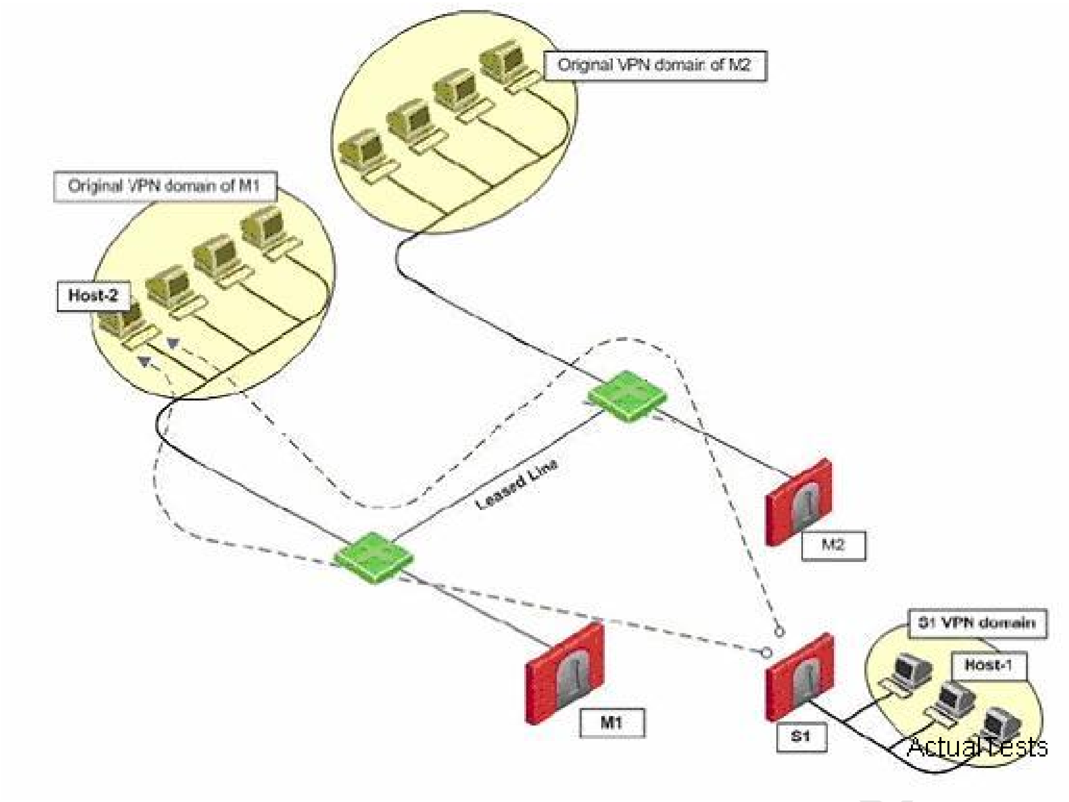


FIGURE 3: Wire Mode in MEP scenario

A. Satellite Gateway B is used to route traffic between Satellite Gateways A and B within the community
B. Center Gateway C is used to route traffic between Satellite Gateways A and B within the community
C. If traffic is going from Satellite gateway A to B, then the Satellite gateway A will start to assume the role of Center Gateway and start to route the traffic
D. Any satellite gateways in the configuration can switch role to Center Gateway
E. Satellite Gateway A is used to route traffic between Satellite Gateways A and B within the community

Answer: B

QUESTION NO: 452

Which of the following is true of Multicast IP? Select all the correct answers.

A. Multicast is used to transmit a single message to a select group of recipients
B. Multicast enabled routers use multicast routing protocols to communicate multicast group information with each other
C. Multicast enabled routers use Internet Group Management Protocol (IGMP) to communicate multicast group information with each other

D. Internet Group Management Protocol (IGMP) is defined in RFC 1112
E. IP Multicasting applications send one copy of each datagram (IP packet) and address it to a group of computers that want to receive it

Answer: A,B,D,E

QUESTION NO: 453

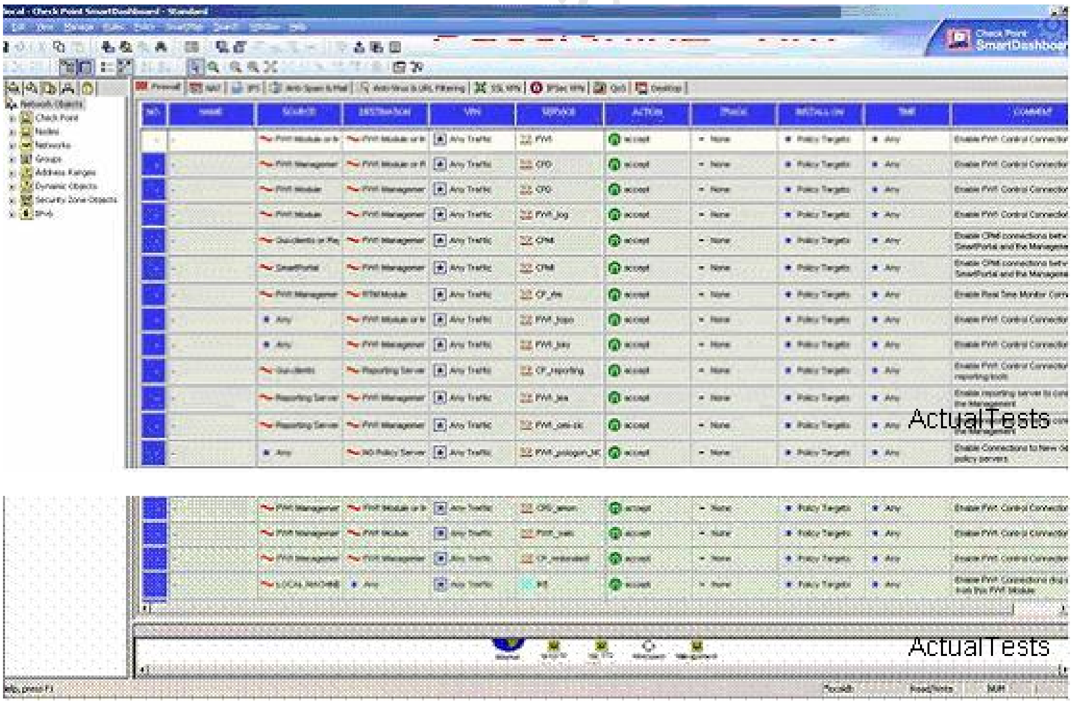
In a standalone deployment, all Eventia Reporter server components (the Log Consolidator Engine, the Eventia Reporter Database and the Eventia Reporter server) are installed on the which machine?

A. Security Gateway
B. Firewall
C. SmartConsole
D. Enforcement Pro
E. Security Management server

Answer: E

QUESTION NO: 454

Study the diagram in the picture and answer the question below. What are the rules without numbering called?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
[illegible]	-	FW1 Module or H	FW1 Module or H	Any Traffic	FW1	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	FW1 Management	FW1 Module or H	Any Traffic	CPD	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	FW1 Module	FW1 Management	Any Traffic	CPD	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	FW1 Module	FW1 Management	Any Traffic	FW1_log	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	Gui clients or Re	FW1 Management	Any Traffic	CPMI	accept	None	Policy Targets	Any	Enable CPMI connections betw SmartPortal and the Manageme
[illegible]	-	SmartPortal	FW1 Management	Any Traffic	CPMI	accept	None	Policy Targets	Any	Enable CPMI connections betw SmartPortal and the Manageme
[illegible]	-	FW1 Management	RTM Module	Any Traffic	CP_rtm	accept	None	Policy Targets	Any	Enable Real Time Monitor Conn
[illegible]	-	Any	FW1 Module or H	Any Traffic	FW1_topo	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	Any	FW1 Management	Any Traffic	FW1_key	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	Gui clients	Reporting Server	Any Traffic	CP_reporting	accept	None	Policy Targets	Any	Enable FW1 Control Connectio reporting tools
[illegible]	-	Reporting Server	FW1 Management	Any Traffic	FW1_lea	accept	None	Policy Targets	Any	Enable reporting server to con the Management
[illegible]	-	Reporting Server	FW1 Management	Any Traffic	FW1_omi-sic	accept	None	Policy Targets	Any	[illegible] the Management
[illegible]	-	Any	NG Policy Server	Any Traffic	FW1_pslogon_NG	accept	None	Policy Targets	Any	Enable Connections to New St policy servers
[illegible]	-	FW1 Management	FW1 Module or H	Any Traffic	CPD_amon	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	FW1 Management	FW1 Module	Any Traffic	FW1_sds	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	FW1 Management	FW1 Management	Any Traffic	CP_redundant	accept	None	Policy Targets	Any	Enable FW1 Control Connectio
[illegible]	-	LOCAL_MACHINE	Any	Any Traffic	IKE	accept	None	Policy Targets	Any	Enable FW1 Connections that o from this FW1 Module

A. Stealth rule

B. Cleanup rule
C. Implicit rule
D. Explicit rule
E. Semi rule

Answer: C

QUESTION NO: 455

To begin using your IPS subscription, where would you input your subscription information?

A. SmartView Tracker
B. SmartView Monitor
C. SmartDashboard
D. Eventia Reporter
E. SmartUpdate

Answer: E

QUESTION NO: 456

How would you reveal all Hidden Rules?

A. By selecting Rules menu, select Hide-> Unhide All
B. By selecting File menu, select Hide-> Unhide All
C. By selecting Policy menu, select Hide-> Unhide All
D. By selecting Manage menu, select Hide-> Unhide All
E. By selecting Rules menu, selectUnhide all

Answer: A

QUESTION NO: 457

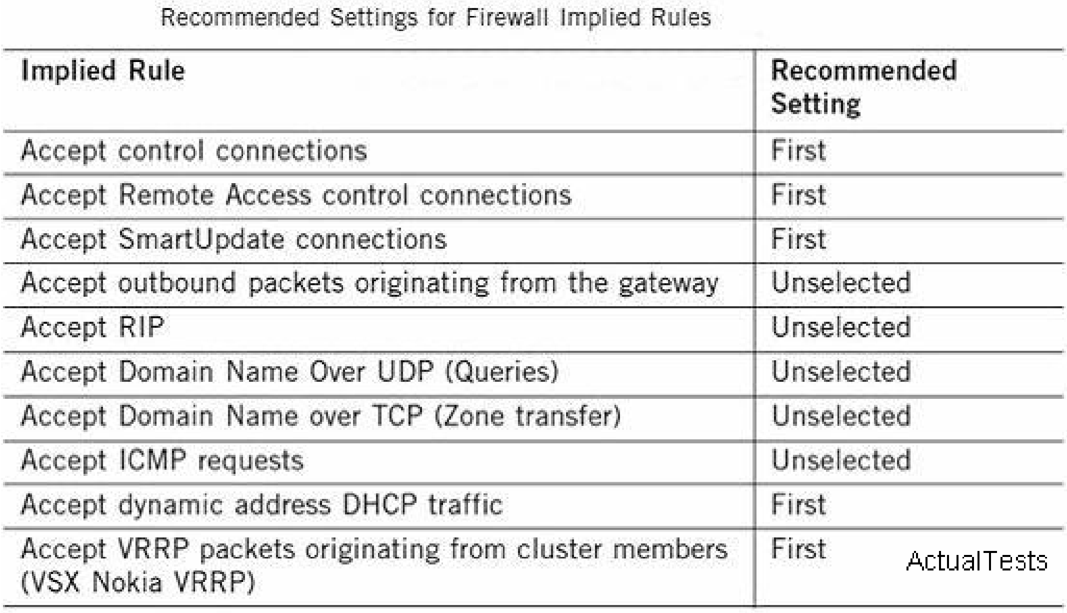
What do you acquire in order that other users cannot make configuration changes to your appliance while you logon to it?

A. Configuration key
B. Security password
C. Supervisor password
D. Adminstrator password
E. Configuration lock

Answer: E

QUESTION NO: 458

Which of the following is true of the Implied Rules?



Recommended Settings for Firewall Implied Rules

Implied Rule	Recommended Setting
Accept control connections	First
Accept Remote Access control connections	First
Accept SmartUpdate connections	First
Accept outbound packets originating from the gateway	Unselected
Accept RIP	Unselected
Accept Domain Name Over UDP (Queries)	Unselected
Accept Domain Name over TCP (Zone transfer)	Unselected
Accept ICMP requests	Unselected
Accept dynamic address DHCP traffic	First
Accept VRRP packets originating from cluster members (VSX Nokia VRRP)	First

A. Implied rules prevents direct access to Gateway

B. Implied rules cannot be logged

C. Implied rules are placed first, last, or before last in the Rule Base

D. Security Gateway creates implied rules from the Policy > Global Properties definitions

E. Implied rules enable certain connections to occur to and from the gateway

Answer: C,D,E

QUESTION NO: 459

The differences between Traditional VPN Mode and Simplified VPN Mode are that:

A. In Simplified VPN Mode, a single rule, with the Encrypt rule action, deals with both access control and encryption

B. In Traditional VPN Mode, the Security Rule Base deals only with access control

C. In Traditional VPN Mode, a single rule, with the Encrypt rule action, deals with both access control and encryption

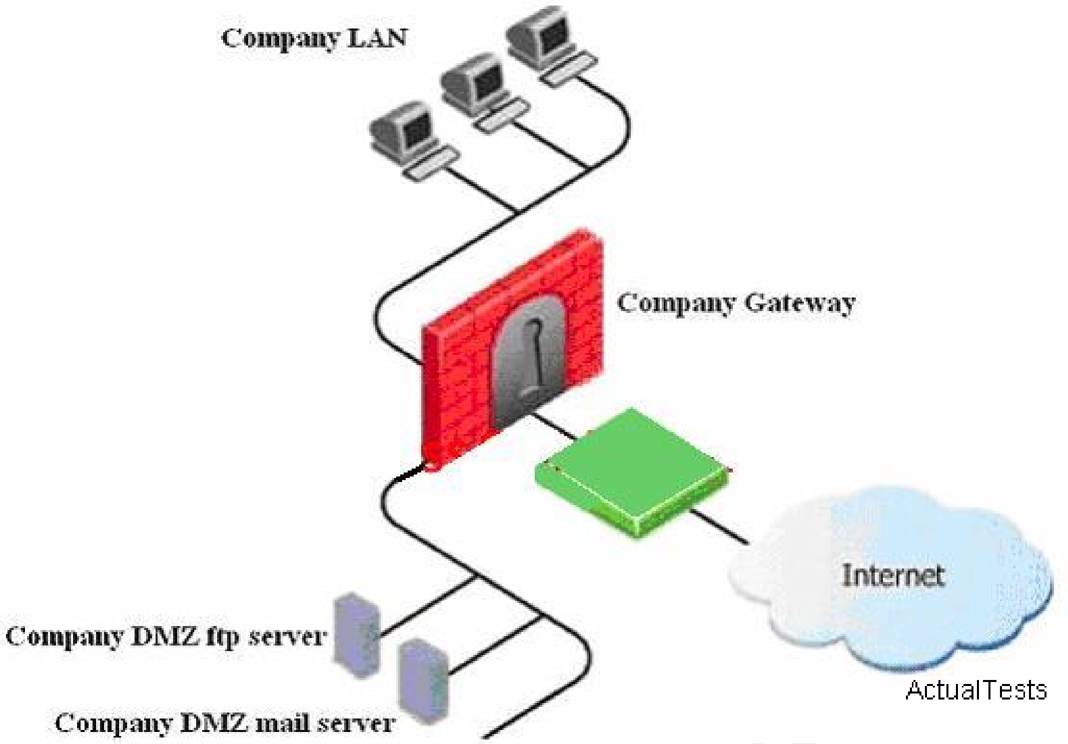
D. In Simplified VPN Mode, the Security Rule Base deals only with access control

E. Traditional policies allow VPNs to be created with greater granularity than Simplified policies

Answer: C,D,E

QUESTION NO: 460

Which of the following is true of INSPECT Engine? Select all the correct answers.



A. The INSPECT Engine enforces Security Policies on any Security Gateway

B. INSPECT Engine is the mechanism used for extracting the state-related information from all application layers

C. The INSPECT Engine is dynamically loaded into the kernel between layer 2 and layer 3 of the OSI

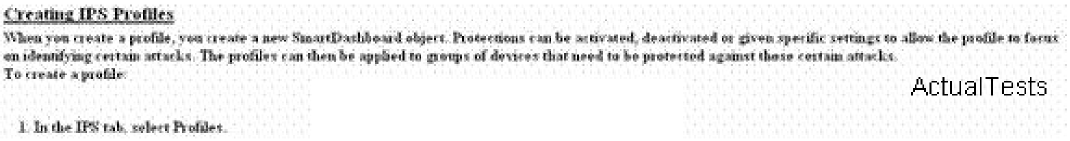
D. The INSPECT Engine enforces Security Policies on the Security Gateway on which they reside

E. INSPECT Engine is the mechanism used for extracting the state-related information from all transport layers

Answer: B,C,D

QUESTION NO: 461

Which of the following tools will you use to create an IPS profiles?

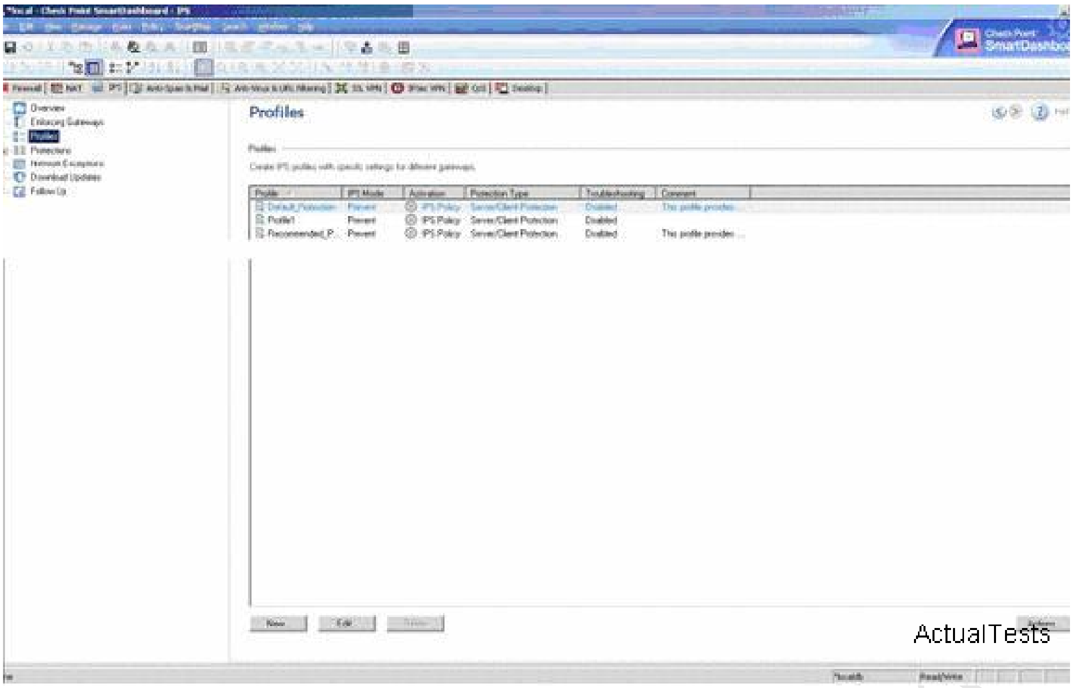


Creating IPS Profiles

When you create a profile, you create a new SmartDashboard object. Protections can be activated, deactivated or given specific settings to allow the profile to focus on identifying certain attacks. The profiles can then be applied to groups of devices that need to be protected against those certain attacks.

To create a profile:

1. In the IPS tab, select Profiles.



Profiles

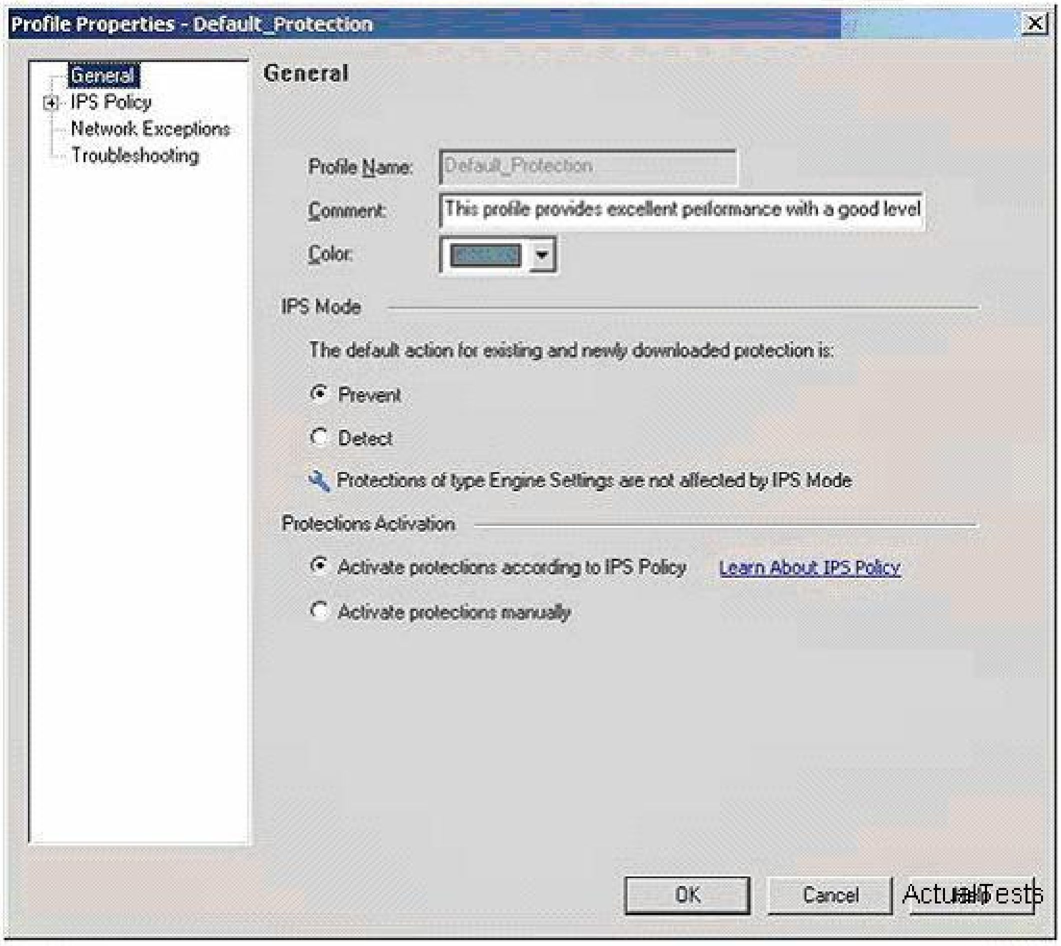
Profiles

Create IPS profiles with specific settings for different gateways.

Profile	IPS Mode	Activation	Protection Type	Troubleshooting	Comment
Default_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	The profile provides ...
Profile1	Prevent	IPS Policy	Server/Client Protection	Disabled	
Recommended_P...	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides ...

2. Click New and choose an option:

- Create New Profile: Opens empty Profile Properties window for new configuration.
- Clone Selected Profile: Creates copy of selected profile. Select the cloned profile and click Edit to make changes (including providing a new name) in the Profile Properties window.



General

Profile Name: Default_Protection

Comment: This profile provides excellent performance with a good level

Color:

IPS Mode

The default action for existing and newly downloaded protection is:

● Prevent

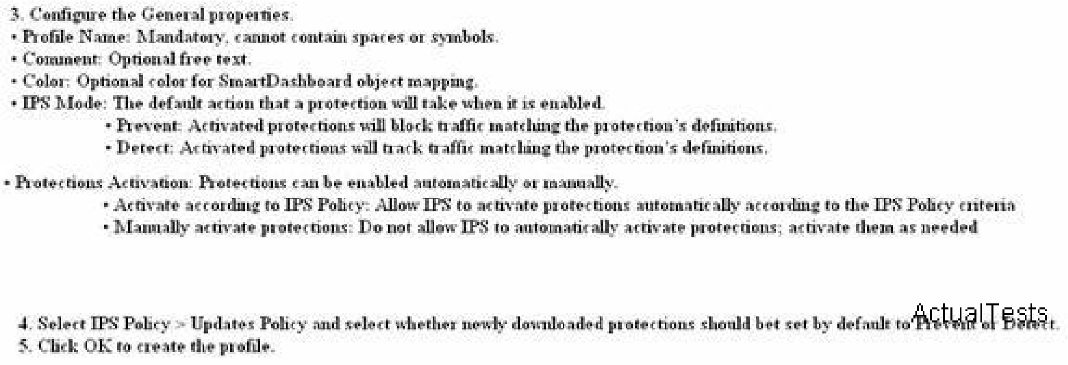
○ Detect

Protections of type Engine Settings are not affected by IPS Mode

Protections Activation

● Activate protections according to IPS Policy   Learn About IPS Policy

○ Activate protections manually



3. Configure the General properties.

- Profile Name: Mandatory, cannot contain spaces or symbols.
- Comment: Optional free text.
- Color: Optional color for SmartDashboard object mapping.
- IPS Mode: The default action that a protection will take when it is enabled.
  - Prevent: Activated protections will block traffic matching the protection's definitions.
  - Detect: Activated protections will track traffic matching the protection's definitions.
- Protections Activation: Protections can be enabled automatically or manually.
  - Activate according to IPS Policy: Allow IPS to activate protections automatically according to the IPS Policy criteria
  - Manually activate protections: Do not allow IPS to automatically activate protections; activate them as needed

4. Select IPS Policy > Updates Policy and select whether newly downloaded protections should bet set by default to Prevent or Detect.
5. Click OK to create the profile.

A. Protections Browser of the IPS tab in the SmartDashboard
B. SmartView Monitor
C. IPS Monitor
D. SmartView Tracker
E. IPS Config

Answer: A

QUESTION NO: 462

Which of the following is true of the hidden rules?

A. Whether they are displayed, or not, hidden rules are displayed when the security Policy is installed
B. None of the available answers
C. Whether they are displayed, or not, hidden rules are made redundant when the security Policy is installed
D. Whether they are displayed, or not, hidden rules numbering would change when the security Policy is installed
E. Whether they are displayed, or not, hidden rules are enforced when the security Policy is installed

Answer: E

QUESTION NO: 463

What advantage does N+1 topology offer over traditional load balancing topology?

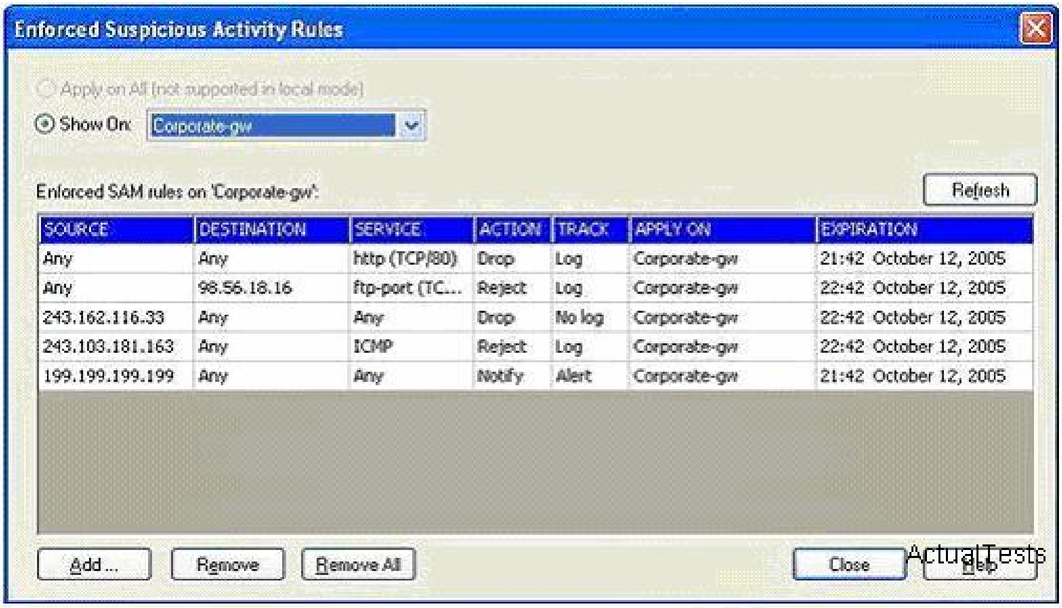
A. By offering a minimum guarantee that certain number of nodes will be active
B. By offering better throughput because it uses the bandwidth of the production networks more efficiently
C. By offering a lower cost
D. By offering a possibility of configuration while cluster is active

E. By offering a possibility of connection while cluster is active

Answer: A

QUESTION NO: 464

What does Enforced Suspicious Activity Rules window provide you with?



○ Apply on All (not supported in local mode)

● Show On: Corporate-gw

Enforced SAM rules on 'Corporate-gw':

SOURCE	DESTINATION	SERVICE	ACTION	TRACK	APPLY ON	EXPIRATION
Any	Any	http (TCP/80)	Drop	Log	Corporate-gw	21:42 October 12, 2005
Any	98.56.18.16	ftp-port (TC...	Reject	Log	Corporate-gw	22:42 October 12, 2005
243.162.116.33	Any	Any	Drop	No log	Corporate-gw	22:42 October 12, 2005
243.103.181.163	Any	ICMP	Reject	Log	Corporate-gw	22:42 October 12, 2005
199.199.199.199	Any	Any	Notify	Alert	Corporate-gw	21:42 October 12, 2005

Figure 1 Enforced Suspicious Activity Rules Window

A. The display of automatically configured enforced rule due to the state of the specified gateway
B. The display of the drafted enforced rules
C. The display of the currently enforced rules
D. Nothing
E. The automatically configured enforced rule due to the state of the specified gateway

Answer: C

QUESTION NO: 465

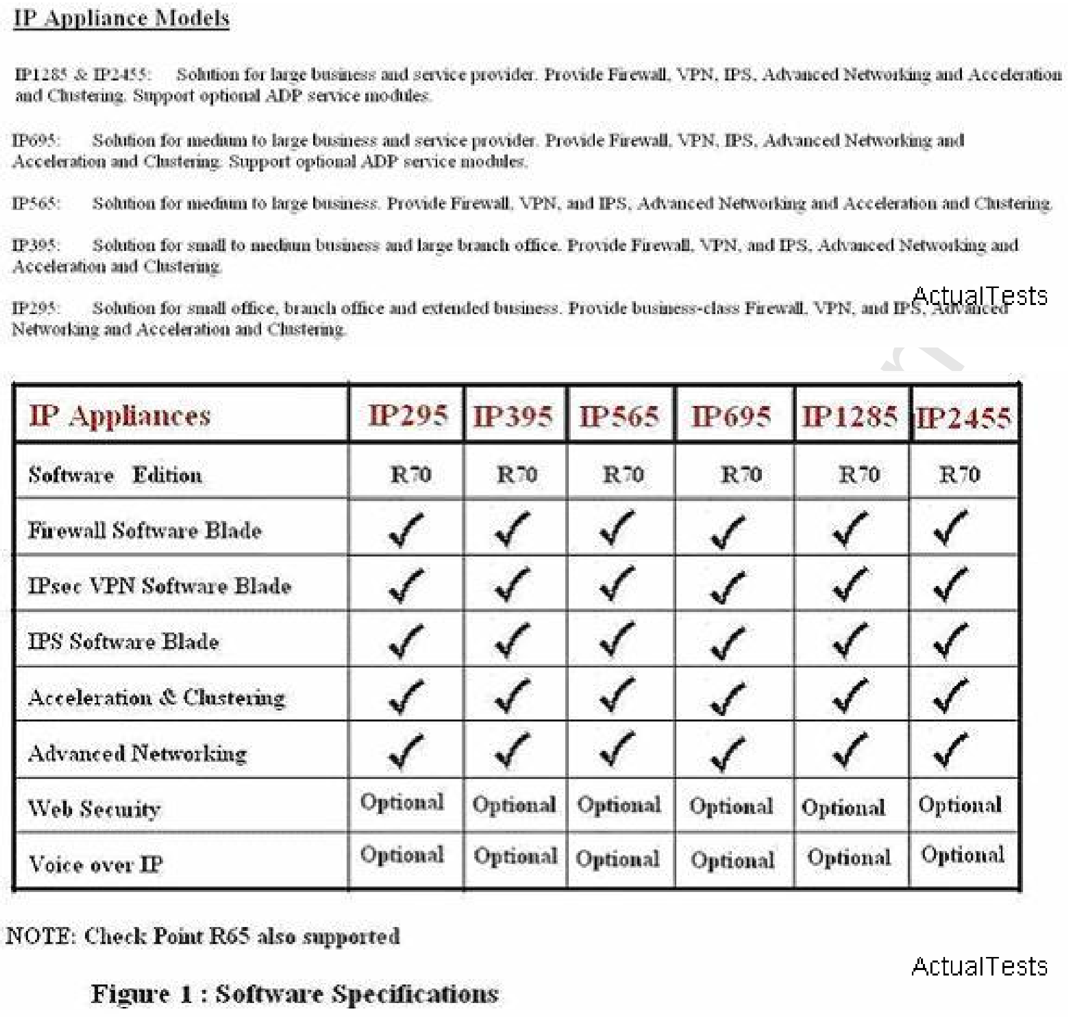
Manually backed-up files are stored in which of the following directories?

A. /sched
B. /image
C. /config
D. /backup
E. /cron

Answer: D

QUESTION NO: 466

Which of the following IP Appliance models are suitable for large enterprises that are service providers? Select all the correct answers.



IP Appliance Models

IP1285 & IP2455: Solution for large business and service provider. Provide Firewall, VPN, IPS, Advanced Networking and Acceleration and Clustering. Support optional ADP service modules.

IP695: Solution for medium to large business and service provider. Provide Firewall, VPN, IPS, Advanced Networking and Acceleration and Clustering. Support optional ADP service modules.

IP565: Solution for medium to large business. Provide Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP395: Solution for small to medium business and large branch office. Provide Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP295: Solution for small office, branch office and extended business. Provide business-class Firewall, VPN, and IPS, Advanced Networking and Acceleration and Clustering.

IP Appliances	IP295	IP395	IP565	IP695	IP1285	IP2455
Software Edition	R70	R70	R70	R70	R70	R70
Firewall Software Blade	✓	✓	✓	✓	✓	✓
IPsec VPN Software Blade	✓	✓	✓	✓	✓	✓
IPS Software Blade	✓	✓	✓	✓	✓	✓
Acceleration & Clustering	✓	✓	✓	✓	✓	✓
Advanced Networking	✓	✓	✓	✓	✓	✓
Web Security	Optional	Optional	Optional	Optional	Optional	Optional
Voice over IP	Optional	Optional	Optional	Optional	Optional	Optional

NOTE: Check Point R65 also supported

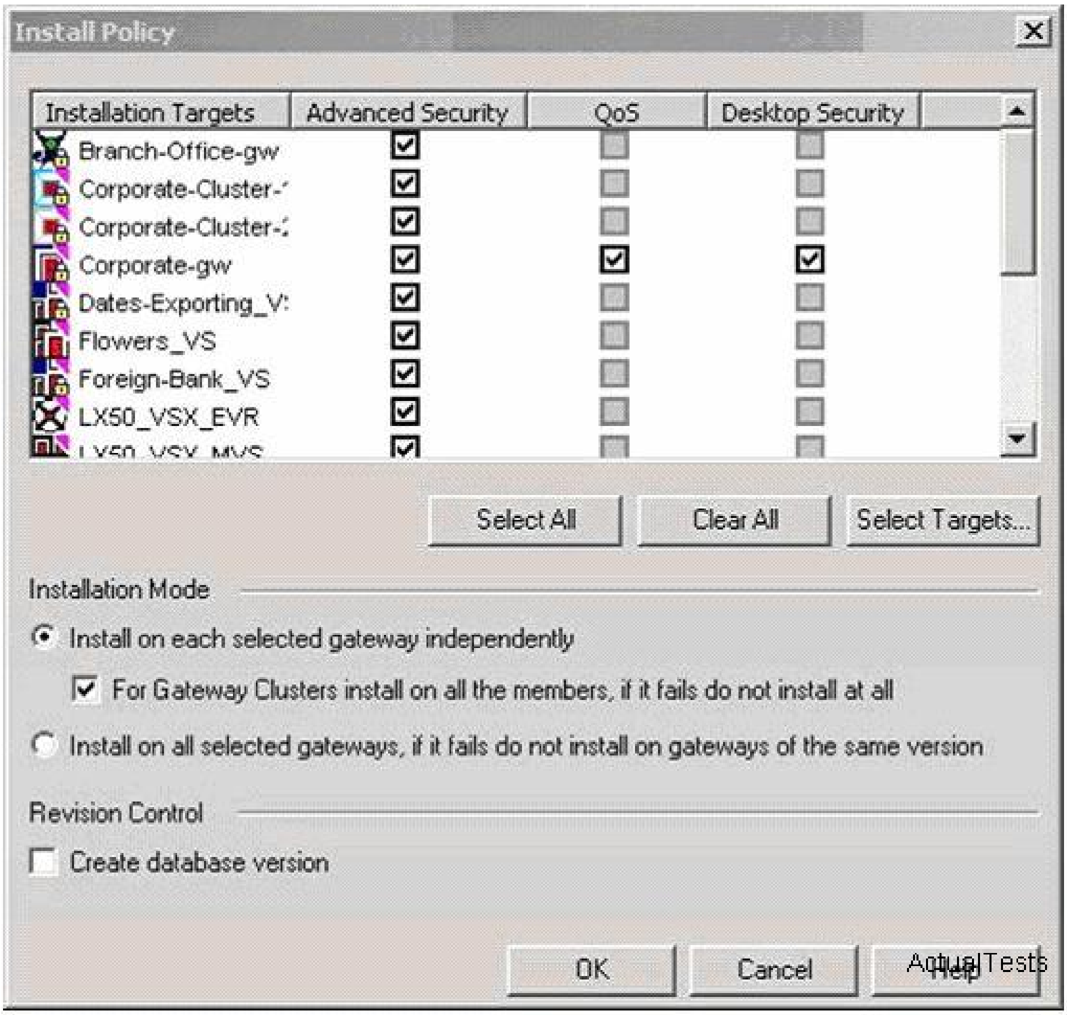
Figure 1 : Software Specifications

A. IP1285
B. IP2455
C. IP695
D. IP565
E. IP395

Answer: A,B,C

QUESTION NO: 467

When installing (and uninstall) Policy Packages in the Install Policy window, what box will you tick in order that the Security Management server can be allowed to manage multiple versions of policies?



Installation Targets	Advanced Security	QoS	Desktop Security
Branch-Office-gw	☑	□	□
Corporate-Cluster-'	☑	□	□
Corporate-Cluster-:	☑	□	□
Corporate-gw	☑	☑	☑
Dates-Exporting_V:	☑	□	□
Flowers_VS	☑	□	□
Foreign-Bank_VS	☑	□	□
LX50_VSX_EVR	☑	□	□
LX50_VSX_MVS	☑	□	□

Installation Mode

● Install on each selected gateway independently

☑ For Gateway Clusters install on all the members, if it fails do not install at all

○ Install on all selected gateways, if it fails do not install on gateways of the same version

Revision Control

□ Create database version

Figure 1: Install Policy Window

A. Verify Object
B. BackupAnd Restore
C. Create Service Object
D. Revision control
E. Create Network Object

Answer: D

QUESTION NO: 468

What would you specify in order to display only entries of interest in the SmartView Tracker, and to hide other entries?

A. Selection
B. Viewer criteria
C. Record criteria
D. Filtering criteria

E. Column criteria

Answer: D

QUESTION NO: 469

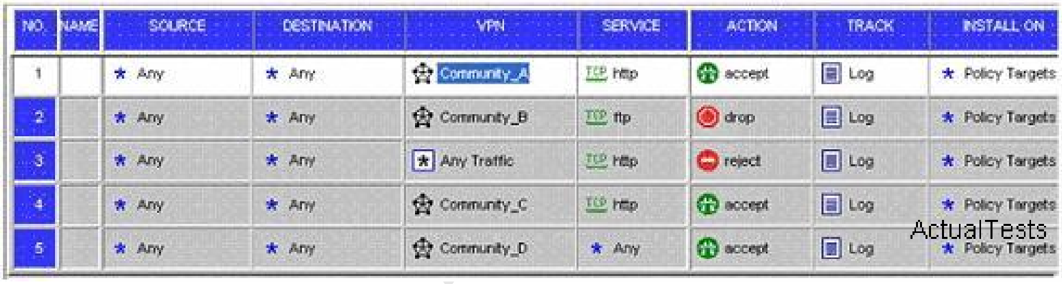
Platforms IP290, IP390 and IP560 are flash-based, diskless platforms. And what do you have to do prior to upgrading their images to R70?

A. Backup old images
B. Do nothing
C. Delete old images
D. Backup their images
E. Restore old images

Answer: C

QUESTION NO: 470

Configuring Gateways into a VPN community does not create a de facto access control policy between the Gateways. And the fact that two Gateways belong to the same VPN community does not mean the Gateways have access to each other. Which of the following rule in diagram 1 will allow communication between gateways in the Community_D if the connection is HTTP?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1		* Any	* Any	Community_A	TCP http	accept	Log	* Policy Targets
2		* Any	* Any	Community_B	TCP ftp	drop	Log	* Policy Targets
3		* Any	* Any	Any Traffic	TCP http	reject	Log	* Policy Targets
4		* Any	* Any	Community_C	TCP http	accept	Log	* Policy Targets
5		* Any	* Any	Community_D	* Any	accept	Log	* Policy Targets

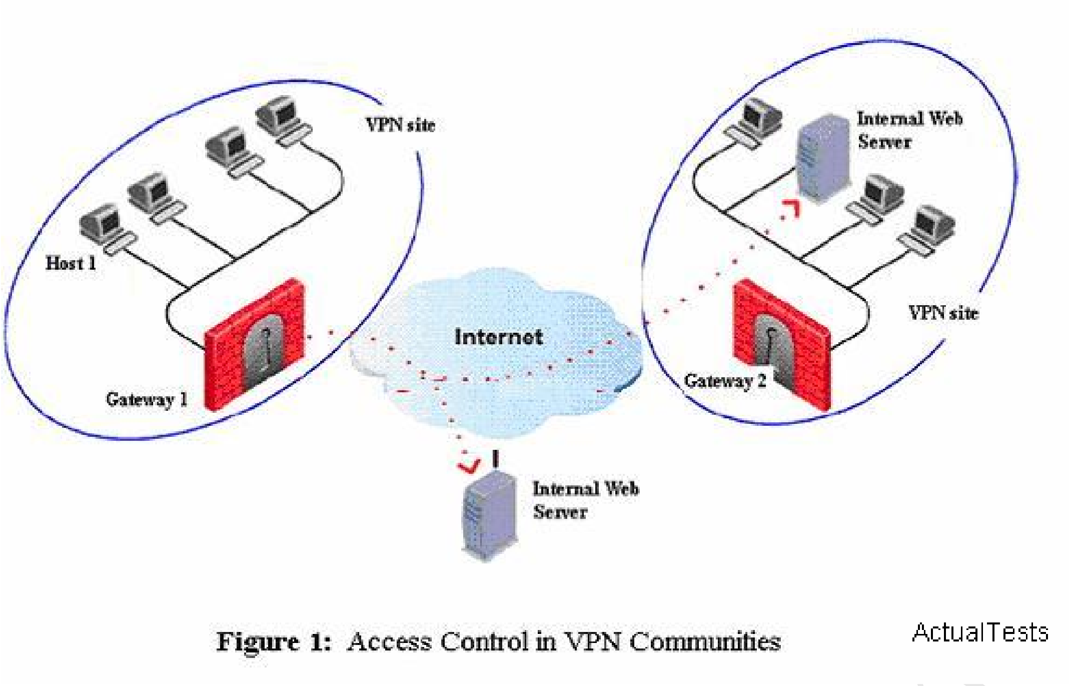


Figure 1: Access Control in VPN Communities

A. Rule 2

B. Rule 5

C. Rule 3

D. Rule 1

E. Rule 4

Answer: B

QUESTION NO: 471

Which of the following is true regarding implementation of DMZ?

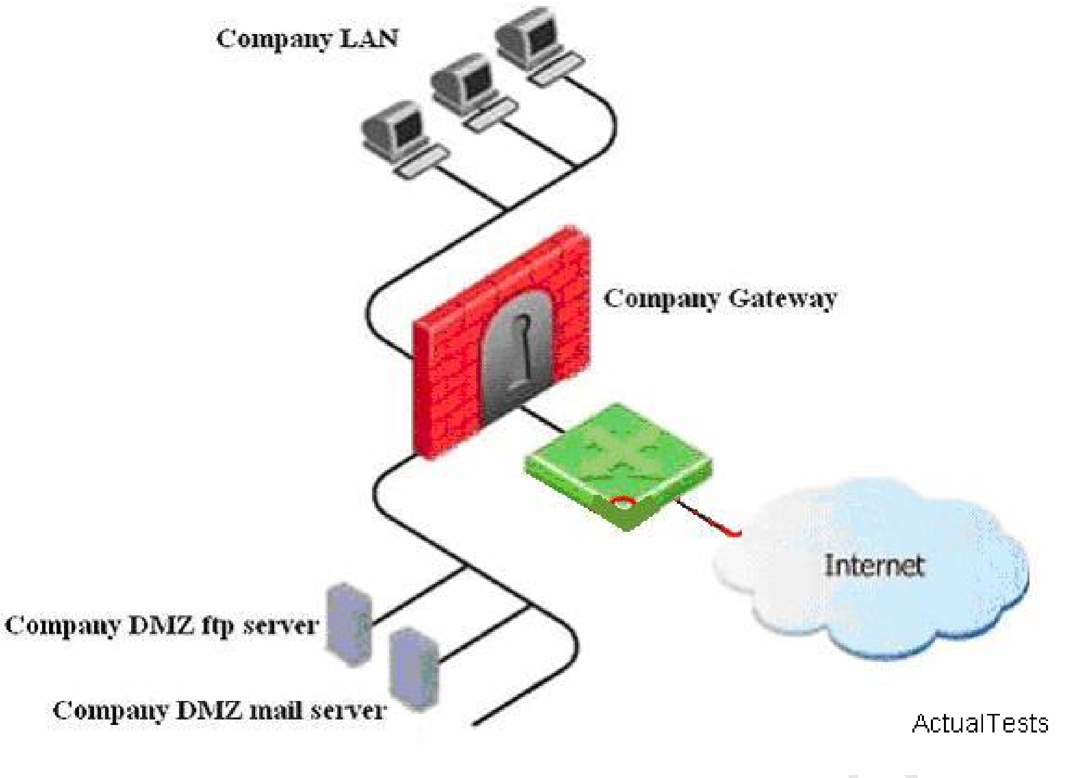


Figure 1: Network with a DMZ implementation

A. The DMZ isolates all servers that are accessible from untrusted sources, such as the Internet

B. If you have servers that are externally accessible from the Internet, it is recommended to create a DMZ

C. Servers in the DMZ should be as secure as possible

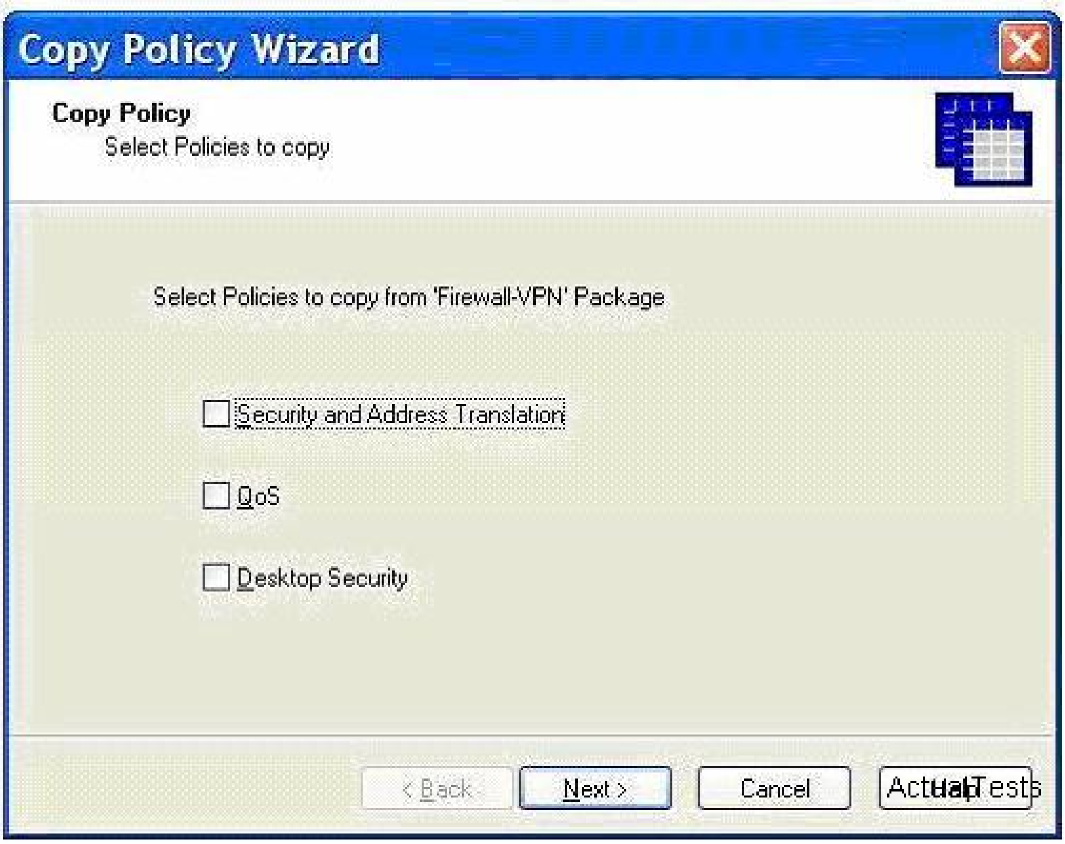
D. Servers in the DMZ are accessible from any network, and all externally accessible servers should be located in the DMZ

E. Do allow the DMZ to initiate connections into the internal network

Answer: A,B,C,D

QUESTION NO: 472

How would you copy the Policy package to an existing policy package? Note: If wrong answer is chosen, see the diagram for correct answer.



Select Policies to copy from 'Firewall-VPN' Package

□ Security and Address Translation

□ QoS

□ Desktop Security

A. By using Cloning Policy Wizard window
B. By using Copy Policy Wizard window
C. By using Wizard window
D. By using Policy window
E. By using Policy Wizard window

Answer: B

QUESTION NO: 473

In Eventia Reporter, Standard Reports are generated from information in Log Consolidator logs to yield relevant analysis of activity. Which of the following are based on data collected by the Check Point system counters and SmartView Monitor history files?

A. Report Tree
B. Contents Tab
C. Section
D. Report
E. Express Reports

Answer: E

QUESTION NO: 474

To guarantee the quality of the available logs in the Eventia Reporter, you must:

A. Adjust your Security Management server
B. Ensure your Security Policy is indeed tracking all events
C. Make sure there is communication between the Enforcement Point and Security Management server
D. Modify your Enforcement Point
E. Make sure there is communication between the SmartConsole and Security Management server

Answer: B

QUESTION NO: 475

What application, a support tool, gathers into one text file a wide range of data concerning the Check Point packages in your system?

A. Management Portal
B. SmartLSM
C. CPInfo
D. Cpconfig
E. SmartUpdate

Answer: C

QUESTION NO: 476

What do you intend to achieve if you run a command "cpinfo -o file2" in the SecurePlatform?

A. Store CheckPoint diagnostics information output to file2
B. Redirect CheckPoint diagnostics information output to filename
C. Compare CheckPoint diagnostics information output to file2
D. Print CheckPoint diagnostics information output to file2
E. Store CheckPoint diagnostics information output to file

Answer: A

QUESTION NO: 477

What do you intend to achieve if you run a command "cpinfo -o file2" in the SecurePlatform?

A. Store CheckPoint diagnostics information output to file2
B. Redirect CheckPoint diagnostics information output to filename
C. Compare CheckPoint diagnostics information output to file2
D. Print CheckPoint diagnostics information output to file2
E. Store CheckPoint diagnostics information output to file

Answer: A

QUESTION NO: 478

Which firewall type examines a packet up to the network layer of OSI model?

A. Proxy
B. Session layer gateways
C. Packet filtering
D. Application layer gateways
E. Firewall

Answer: C

QUESTION NO: 479

How would you convert regular SecurePlatform to SecurePlatformPro using CLI?

A. By entering "upgrade SP" at the expert mode command line
B. By entering "pro enable" at IPSO CLI
C. By entering "upgrade" at the expert mode command line
D. By entering "pro enable" at the expert mode command line
E. By entering "convert SP" at the expert mode command line

Answer: D

QUESTION NO: 480

UTM-1 Edge gateways can participate in two types of VPN communities i.e. Site-to-Site and Remote Access. With Remote Access configuration, UTM-1 Edge gateway will act as a remote client. Which of the following is true of all machines deployed behind the UTM-1 Edge gateway?

A. They will allow all traffic

B. They will function as remote access gateway

C. They will block all traffic

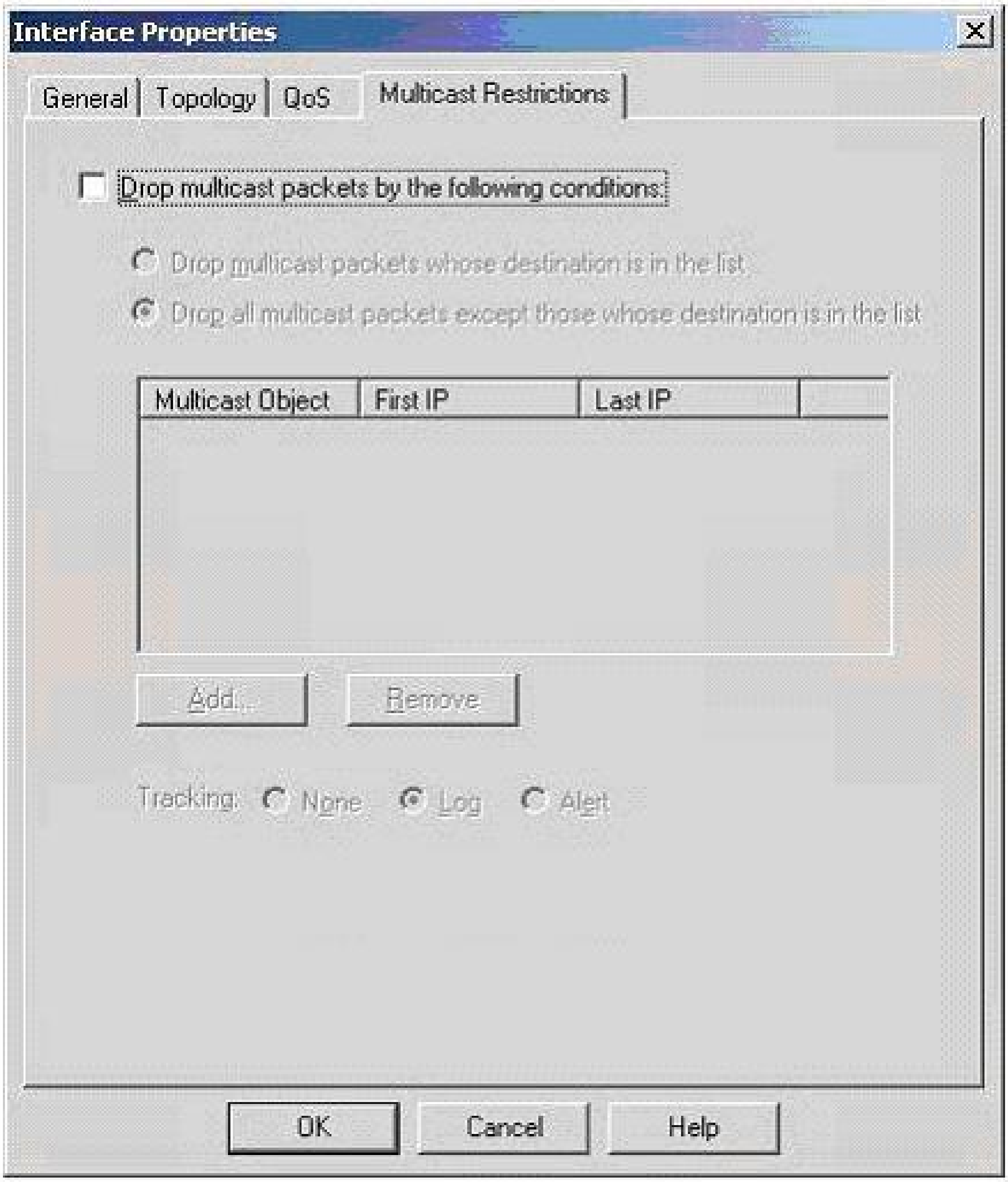
D. They will function as gateway

E. They will function as remote access Client

Answer: E

QUESTION NO: 481

Which of the following is true of multicast access restrictions?



☐ Drop multicast packets by the following conditions:

○ Drop multicast packets whose destination is in the list

● Drop all multicast packets except those whose destination is in the list

Multicast Object	First IP	Last IP

Tracking: ○ None ● Log ○ Alert

Figure 1: Interface Properties - Multicast Restriction s tab

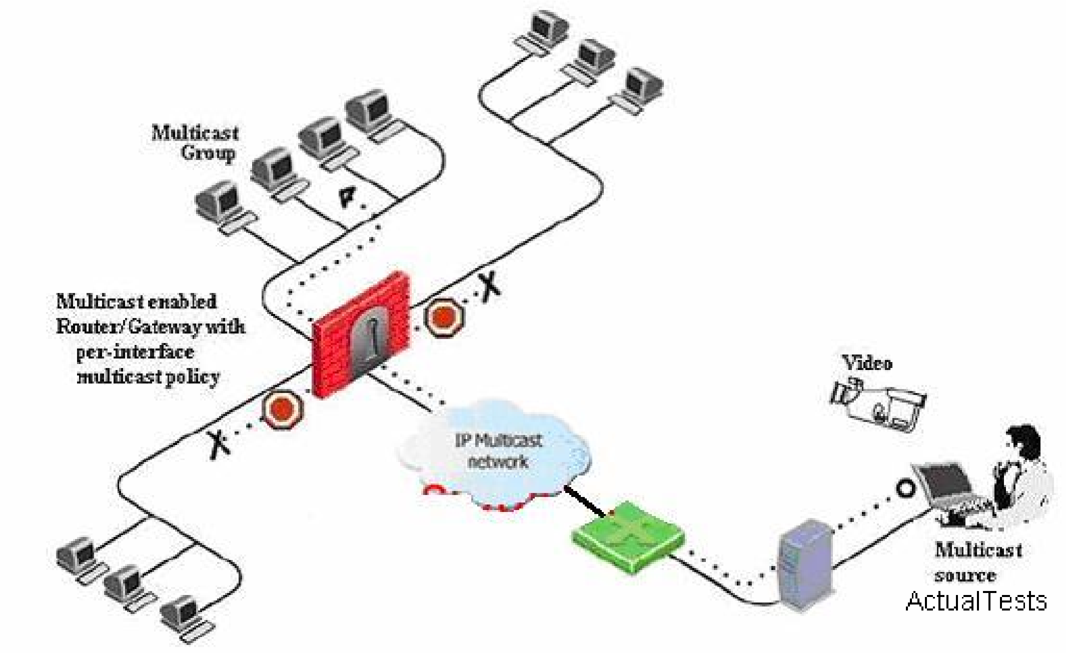

Multicast Group
Multicast enabled Router/Gateway with per-interface multicast policy
IP Multicast network
Video
Multicast source
ActualTests

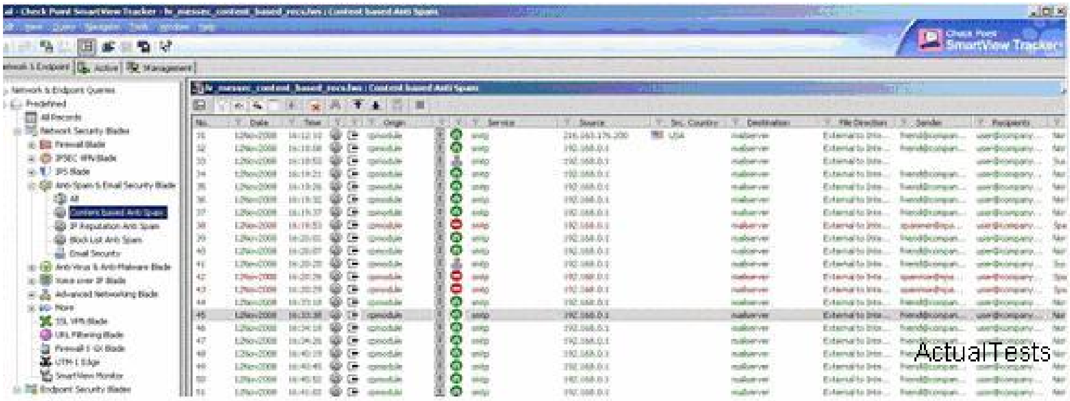
Figure 2: Gateway with per-interface multicast restrictions

A. You can define multicast access restrictions on each interface
B. The restrictions that you define will specify multicast addresses or address ranges to allow or block
C. When no restrictions for multicast datagrams are defined, multicast datagrams entering the gateway on one interface are allowed out of all others
D. When access is denied to a multicast group on an interface in the outbound direction, OSPF packets destined to the group will be denied on that interface in the outbound direction
E. When access is denied to a multicast group on an interface in the outbound direction, IGMP packets destined to the group will be denied on that interface in the inbound direction

Answer: A,B,C,E

QUESTION NO: 482

The sender of an email that is falsely classified as spam will receive an email notification that the email could not be delivered. What would the email contain?



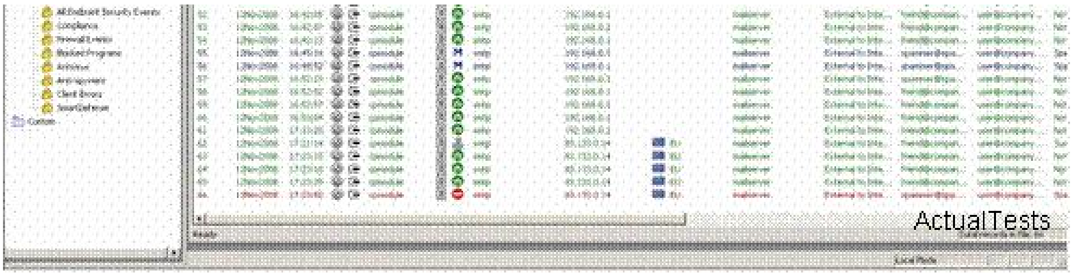


Figure 1: SmartView Tracker - Network & Endpoint Tab

A. Mac Address of the sender

B. Mac Address of the destination

C. Email session ID

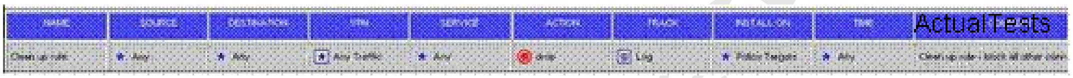
D. IP Address of destination

E. IP Address of source

Answer: C

QUESTION NO: 483

The action field of the Cleanup Rule must be set to:



NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	[illegible]
Clean up rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other com

A. Drop

B. Reject

C. Allow

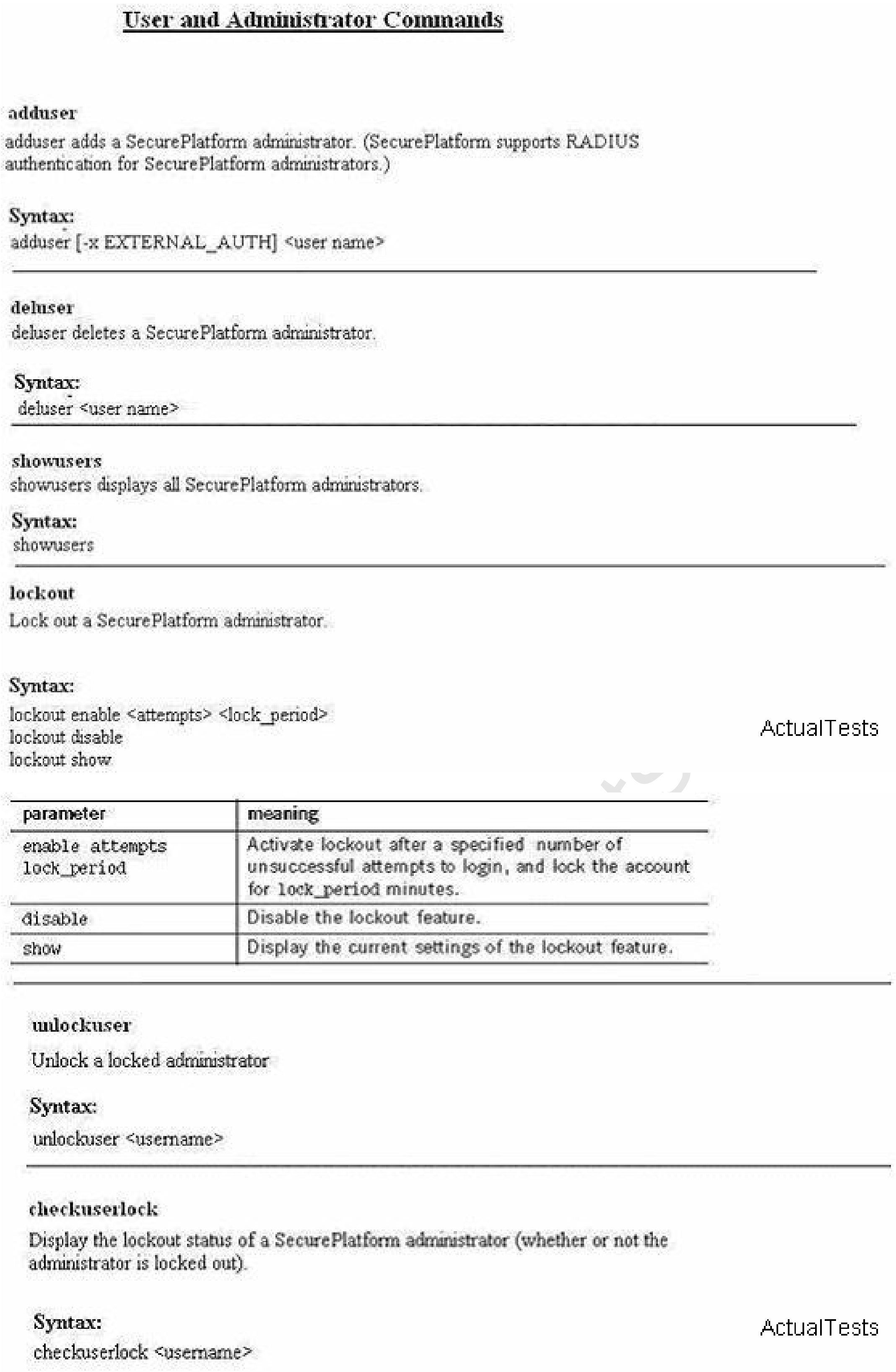
D. Accept

E. User Authentication

Answer: A

QUESTION NO: 484

showusers command will display:



User and Administrator Commands

adduser

adduser adds a SecurePlatform administrator. (SecurePlatform supports RADIUS authentication for SecurePlatform administrators.)

Syntax:

adduser [-x EXTERNAL_AUTH] <user name>

deluser

deluser deletes a SecurePlatform administrator.

Syntax:

deluser <user name>

showusers

showusers displays all SecurePlatform administrators.

Syntax:

showusers

lockout

Lock out a SecurePlatform administrator.

Syntax:

lockout enable <attempts> <lock_period>
lockout disable
lockout show

parameter	meaning
enable attempts lock_period	Activate lockout after a specified number of unsuccessful attempts to login, and lock the account for lock_period minutes.
disable	Disable the lockout feature.
show	Display the current settings of the lockout feature.

unlockuser

Unlock a locked administrator

Syntax:

unlockuser <username>

checkuserlock

Display the lockout status of a SecurePlatform administrator (whether or not the administrator is locked out).

Syntax:

checkuserlock <username>

A. All SecurePlatform administrators

B. All activated Adminstrator accounts

C. All lockout Adminstrator accounts

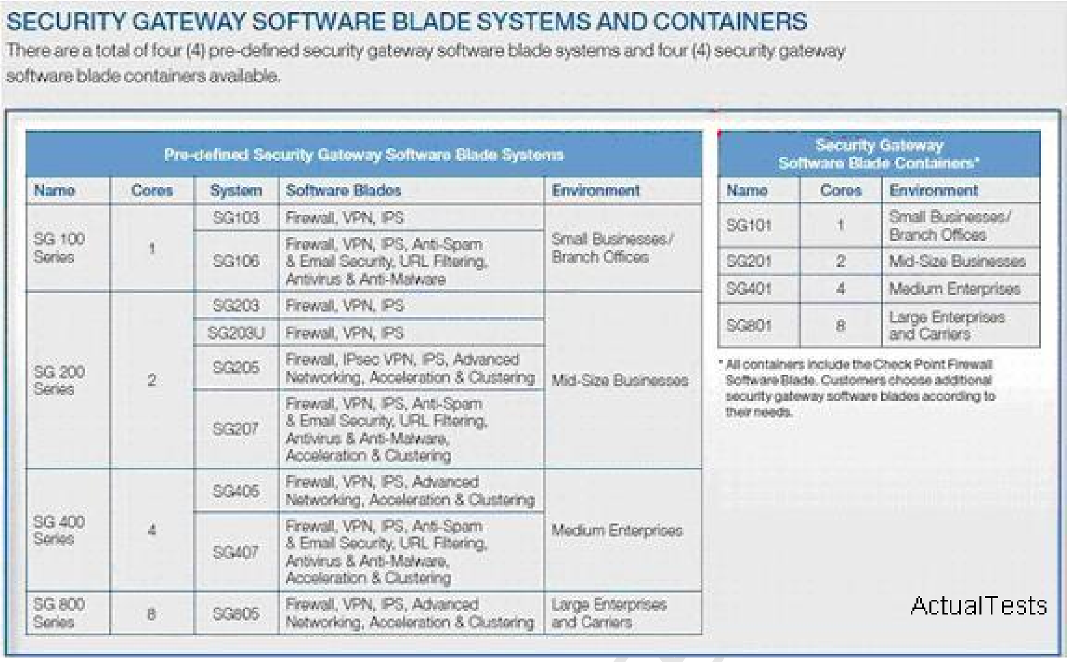
D. All de-activated Adminstrator accounts

E. All lockout accounts

Answer: A

QUESTION NO: 485

Check Point's Software Blade Architecture enables customization of tailored systems or quick selection of predefined turnkey solutions. You run an unlimited number of gateways which be described as a 8 core system. Your organization can also be described as large. You want to deploy security management software blade systems. Which of the following will you deploy?



SECURITY GATEWAY SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of four (4) pre-defined security gateway software blade systems and four (4) security gateway software blade containers available.

Pre-defined Security Gateway Software Blade Systems

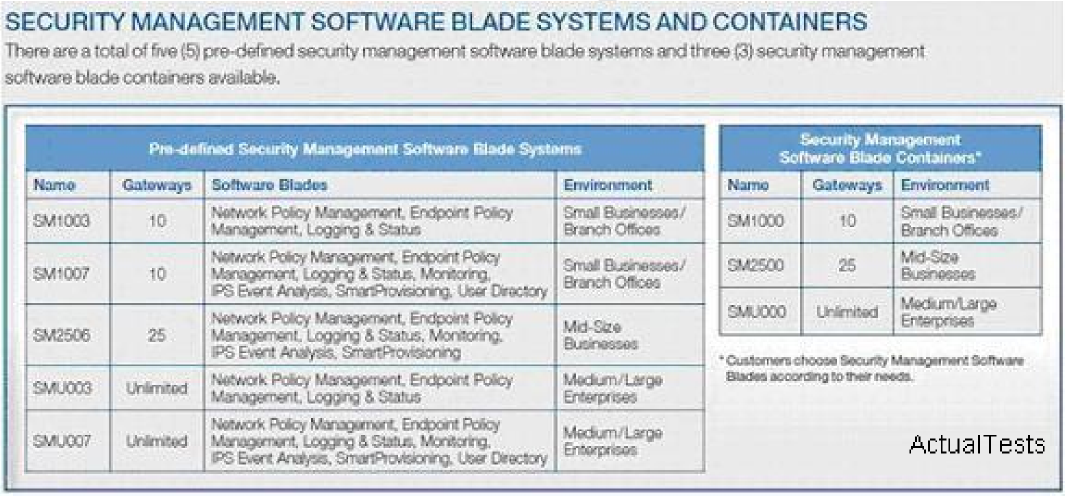
Name	Cores	System	Software Blades	Environment
SG 100 Series	1	SG103	Firewall, VPN, IPS	Small Businesses/ Branch Offices
		SG106	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware	
SG 200 Series	2	SG203	Firewall, VPN, IPS	Mid-Size Businesses
		SG203U	Firewall, VPN, IPS	
		SG205	Firewall, IPsec VPN, IPS, Advanced Networking, Acceleration & Clustering	
		SG207	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	
SG 400 Series	4	SG405	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	Medium Enterprises
		SG407	Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering	
SG 800 Series	8	SG805	Firewall, VPN, IPS, Advanced Networking, Acceleration & Clustering	Large Enterprises and Carriers

Security Gateway Software Blade Containers*

Name	Cores	Environment
SG101	1	Small Businesses/ Branch Offices
SG201	2	Mid-Size Businesses
SG401	4	Medium Enterprises
SG801	8	Large Enterprises and Carriers

* All containers include the Check Point Firewall Software Blade. Customers choose additional security gateway software blades according to their needs.

ActualTests



SECURITY MANAGEMENT SOFTWARE BLADE SYSTEMS AND CONTAINERS

There are a total of five (5) pre-defined security management software blade systems and three (3) security management software blade containers available.

Pre-defined Security Management Software Blade Systems

Name	Gateways	Software Blades	Environment
SM1003	10	Network Policy Management, Endpoint Policy Management, Logging & Status	Small Businesses/ Branch Offices
SM1007	10	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Small Businesses/ Branch Offices
SM2506	25	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning	Mid-Size Businesses
SMU003	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status	Medium/Large Enterprises
SMU007	Unlimited	Network Policy Management, Endpoint Policy Management, Logging & Status, Monitoring, IPS Event Analysis, SmartProvisioning, User Directory	Medium/Large Enterprises

Security Management Software Blade Containers*

Name	Gateways	Environment
SM1000	10	Small Businesses/ Branch Offices
SM2500	25	Mid-Size Businesses
SMU000	Unlimited	Medium/Large Enterprises

* Customers choose Security Management Software Blades according to their needs.

ActualTests

A. SG800
B. SMU007
C. SG400
D. SM2506
E. SM1007

Answer: B

QUESTION NO: 486

Identify Network & Endpoint mode file.

A. 2008-07-27_114327_1.logptr
B. 2008-07-27_114327_1.adtlog
C. 2008-07-27_114327_1.vlog
D. 2008-07-27_114327.vlogptr
E. 2008-07-27_112327.log

Answer: E

QUESTION NO: 487

Which of following is true of objects_5_0.C and objects.C files?

A. dbedit utility must be used to edit the Objects.C
B. objects_5_0.C file has replaced objects.C
C. dbedit utility must be used to edit the Objects_5_0.C
D. Objects_5_0.C is a network object file
E. objects.C file has replaced objects_5_0.C

Answer: B,C,D

QUESTION NO: 488

How can you navigate or open SmartView Monitor GUI from SmartView Tracker GUI?

A. Select SmartView Monitor from view menu.
B. Select SmartView Monitor from file menu.
C. Select SmartView Monitor from select menu.
D. Select SmartView Monitor from edit menu.
E. Select SmartView Monitor from window menu.

Answer: E

QUESTION NO: 489

If you run a fw logswitch command at 4 Jan 2010,0812hrs and taken the second to be 00, what is likely to be the name of the new active file that is being created?

A. $FWDIR/log/01-04-2010_0812.log

B. $FWDIR/log/01-04-2010_081200.log
C. $FWDIR/log/2010-01-04_081200.log
D. $FWDIR/log/2010-01-04_0812.log
E. $FWDIR/log/2010-04-01_081200.log

Answer: C

QUESTION NO: 490

What are the following security measures will ensure the safety of SIC?

A. Standards-based SSL for the creation of the secure channel
B. Certificates for integrity
C. Certificates for authentication
D. DES for encryption
E. 3DES for encryption

Answer: A,C,E

QUESTION NO: 491

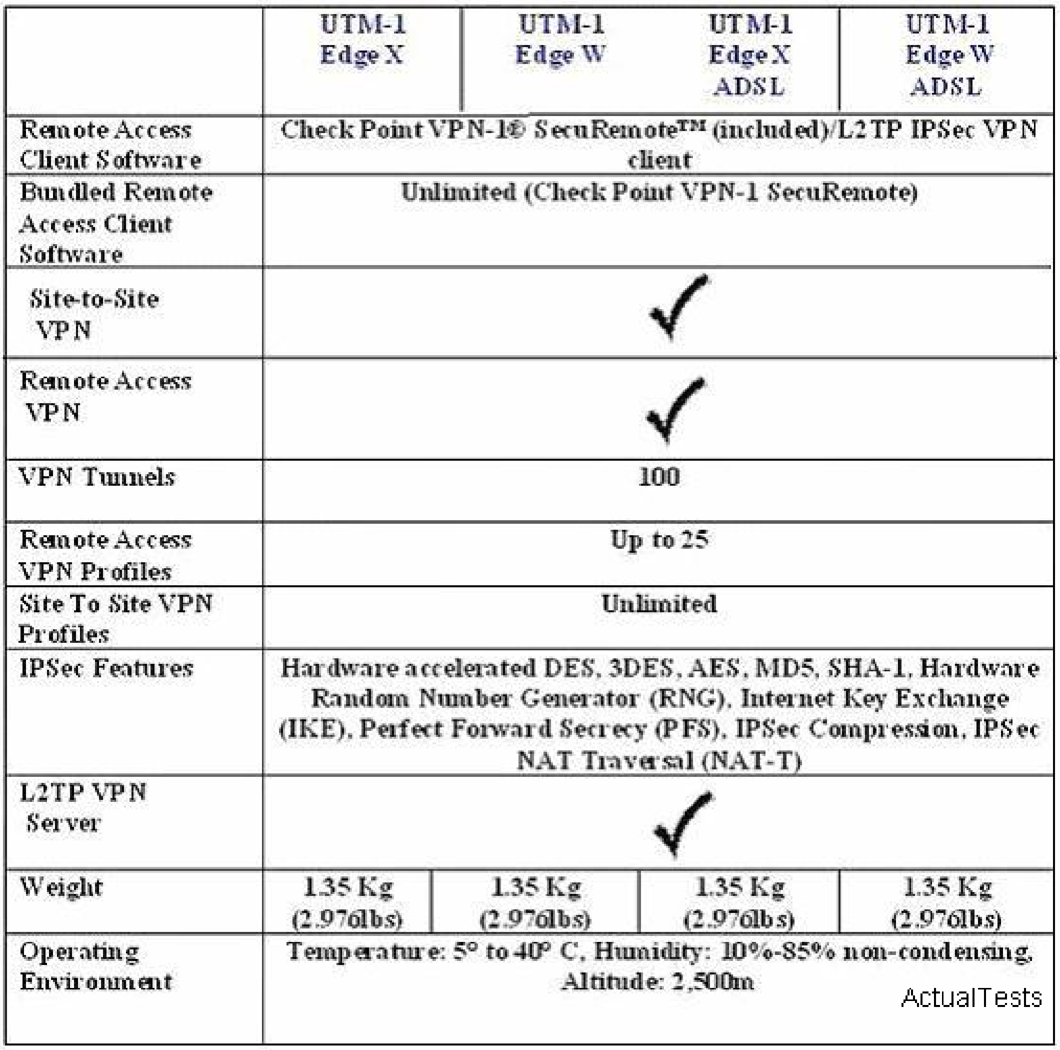
For each kind of Check Point application there is a set of status parameters that can be monitored. When the status of an application is changed or when an event has occurred, predefined actions can be triggered. What must you define in the SmartView Monitor to achieve this?

A. Alerts
B. Predefinition
C. Triggering
D. Thresholds
E. Filtering

Answer: D

QUESTION NO: 492

Which of the following is true regarding UTM-1 Edge appliances type and their VPN functionalities? Select all the correct answers.



	UTM-1 Edge X	UTM-1 Edge W	UTM-1 Edge X ADSL	UTM-1 Edge W ADSL
Remote Access Client Software	Check Point VPN-1® SecuRemote™ (included)/L2TP IPSec VPN client			
Bundled Remote Access Client Software	Unlimited (Check Point VPN-1 SecuRemote)			
Site-to-Site VPN	✓			
Remote Access VPN	✓			
VPN Tunnels	100			
Remote Access VPN Profiles	Up to 25			
Site To Site VPN Profiles	Unlimited			
IPSec Features	Hardware accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSec Compression, IPSec NAT Traversal (NAT-T)			
L2TP VPN Server	✓			
Weight	1.35 Kg (2.976lbs)	1.35 Kg (2.976lbs)	1.35 Kg (2.976lbs)	1.35 Kg (2.976lbs)
Operating Environment	Temperature: 5° to 40° C, Humidity: 10%-85% non-condensing, Altitude: 2,500m			

Figure 1: UTM-1 Edge VPN Data

A. They provide support for various VPN clients including SecureClient, SecuRemote and L2TP VPN clients

B. Perfect Forward Secrecy algorithm is not supported by UTM-1 Edge W

C. They provide support for various VPN clients including SecureClient, SecuRemote aside L2TP VPN clients

D. They do offer remote access connectivity solution

E. They do offer site-to-site connectivity solution

Answer: A,D,E

QUESTION NO: 493

What option would you select in the General Properties tab of the UTM-1 Edge gateway in order to enable Anti Virus protection?

A. Anti-Virus Protection enabled

B. Edge Anti-Virus protection

C. Edge Malware protection

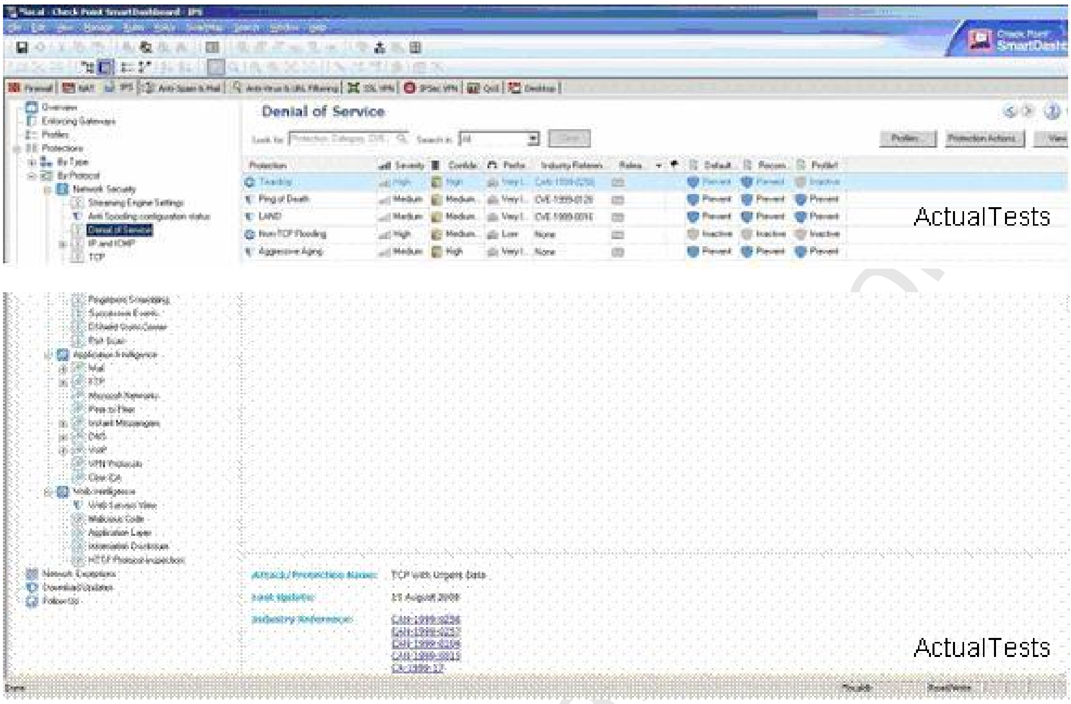
D. Enable Anti-Virus

E. Edge protection

Answer: A

QUESTION NO: 494

Which of these can you not configure in the Application Intelligence section of the IPS?



Protection	Severity	Confide...	Perfo...	Industry Referen...	Releas...	Default...	Recom...	Profile1
Teardrop	High	High	Very l...	CVE-1999-0250		Prevent	Prevent	Inactive
Ping of Death	Medium	Medium...	Very l...	CVE-1999-0128		Prevent	Prevent	Prevent
LAND	Medium	Medium...	Very l...	CVE-1999-0016		Prevent	Prevent	Prevent
Non-TCP Flooding	High	Medium...	Low	None		Inactive	Inactive	Inactive
Aggressive Aging	Medium	High	Very l...	None		Prevent	Prevent	Prevent

Attack/Protection Name: TCP with Urgent Data

Last Update: 11 August 2008

Industry Reference: CAN-1999-0236 CAN-1999-0227 CAN-1999-0108 CAN-1999-0011 CA-1999-17

Figure 1: IPS Tab

A. TCP

B. VoIP

C. Mail

D. FTP

E. DNS

Answer: A

QUESTION NO: 495

How many log file(s) can be opened in the SmartView Tracker GUI at a time?

A. Three

B. One

C. Five

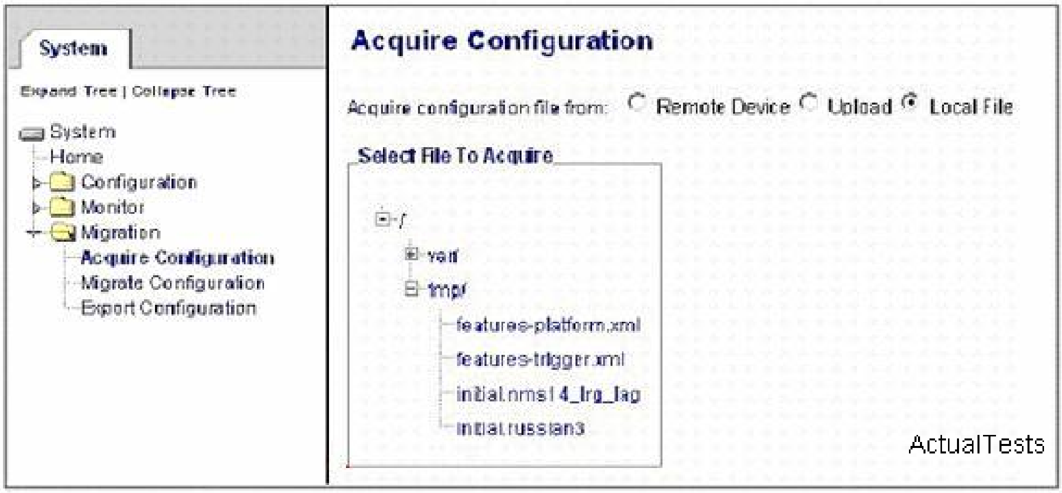
D. Four

E. Two

Answer: B

QUESTION NO: 496

When deploying a new IP Appliance to replace an old one, the existing configuration setting may not necessarily map directly to the new appliance. Which of the following system is designed to address this problem?

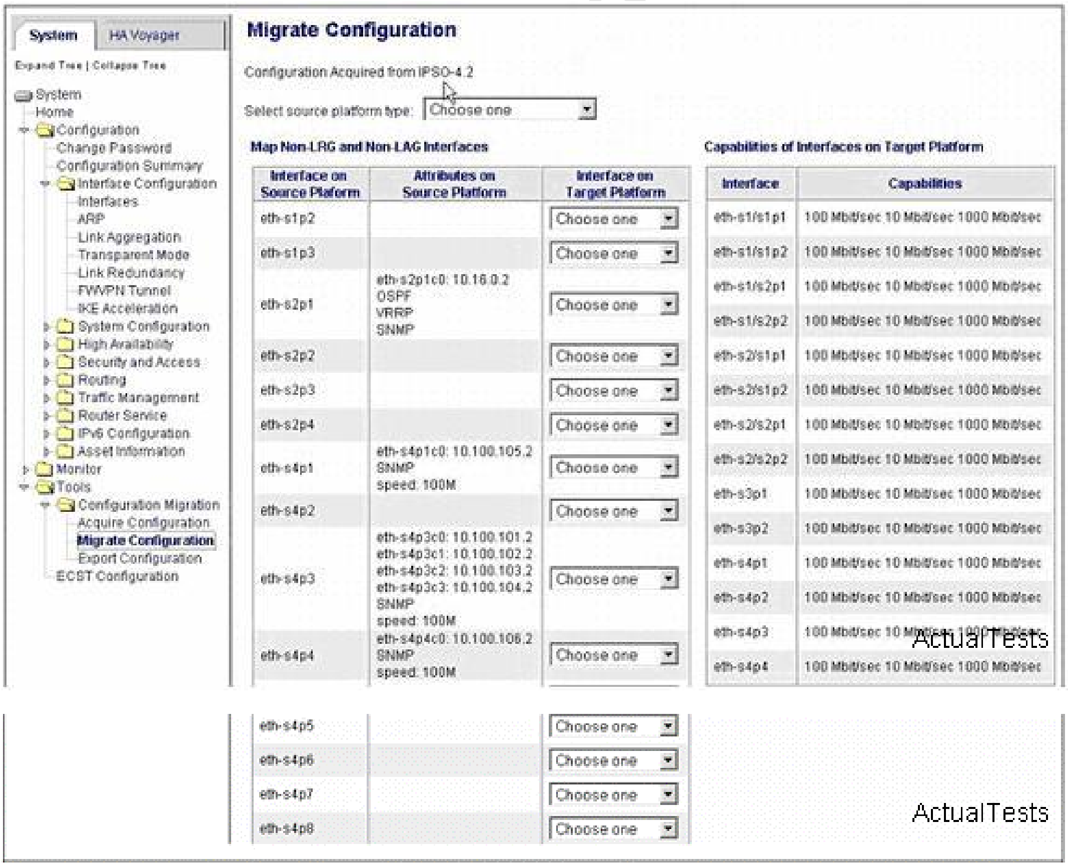


Acquire Configuration

Acquire configuration file from: ○ Remote Device ○ Upload ● Local File

Select File To Acquire

```
⊟ /
  ⊞ var/
  ⊟ tmp/
     features-platform.xml
     features-trigger.xml
     initial.nms14_lrg_lag
     initial.russian3
```



Migrate Configuration

Configuration Acquired from IPSO-4.2

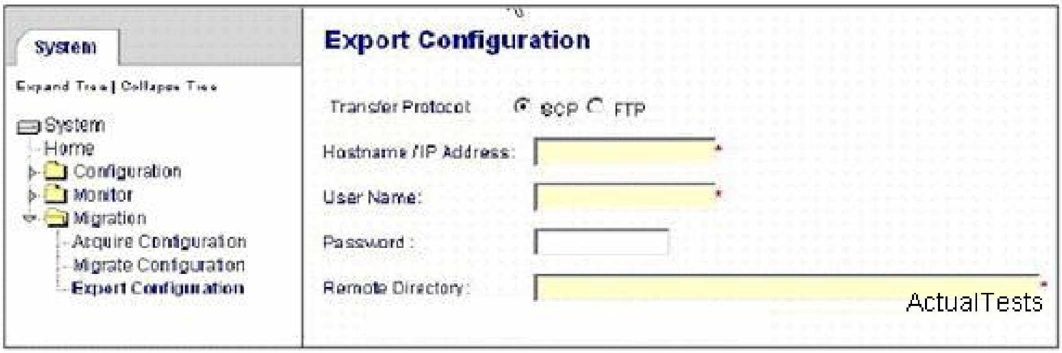
Select source platform type: Choose one

Map Non-LRG and Non-LAG Interfaces

Interface on Source Plaform	Attributes on Source Platform	Interface on Target Platform
eth-s1p2		Choose one
eth-s1p3		Choose one
eth-s2p1	eth-s2p1c0: 10.16.0.2 OSPF VRRP SNMP	Choose one
eth-s2p2		Choose one
eth-s2p3		Choose one
eth-s2p4		Choose one
eth-s4p1	eth-s4p1c0: 10.100.105.2 SNMP speed: 100M	Choose one
eth-s4p2		Choose one
eth-s4p3	eth-s4p3c0: 10.100.101.2 eth-s4p3c1: 10.100.102.2 eth-s4p3c2: 10.100.103.2 eth-s4p3c3: 10.100.104.2 SNMP speed: 100M	Choose one
eth-s4p4	eth-s4p4c0: 10.100.106.2 SNMP speed: 100M	Choose one
eth-s4p5		Choose one
eth-s4p6		Choose one
eth-s4p7		Choose one
eth-s4p8		Choose one

Capabilities of Interfaces on Target Platform

Interface	Capabilities
eth-s1/s1p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s1p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s2p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s1/s2p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s1p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s1p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s2p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s2/s2p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s3p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s3p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p1	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p2	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p3	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec
eth-s4p4	100 Mbit/sec 10 Mbit/sec 1000 Mbit/sec



Export Configuration

Transfer Protocol ● SCP ○ FTP

Hostname /IP Address: *

User Name: *

Password :

Remote Directory: *

A. Configuration migration wizard
B. CLI
C. SmartDashboard
D. IPSO
E. SmartView Tracker

Answer: A

QUESTION NO: 497

When dealing with IPSO clustering modes, which of the following is true of the multicast mode?

A. In this mode, all the nodes of an IPSO cluster share a single multicast MAC for each cluster IP address.
B. In this mode, any device that needs to establish a connection to a cluster IP address must be able to accept ARP replies that contain a multicast MAC address
C. This mode offers the benefits of Multicast with IGMP with an additional improvement
D. In this mode, each cluster node receives every packet sent to the cluster and decides whether to process it based on information it receives from the master node
E. Multicast mode usually offers better throughput because it uses the bandwidth of the production networks more efficiently

Answer: A,B,D,E

QUESTION NO: 498

With Hide NAT, a single public address is shared with multiple computers on your intranet that have private addresses. What is likely to change in order to make each internal computer distinguishable or what CheckPoint Security Gateway uses to distinguish each internal computer when delivering packets?

A. Type of services
B. MAC Address

C. UDP
D. Port numbers
E. IP Address

Answer: D

QUESTION NO: 499

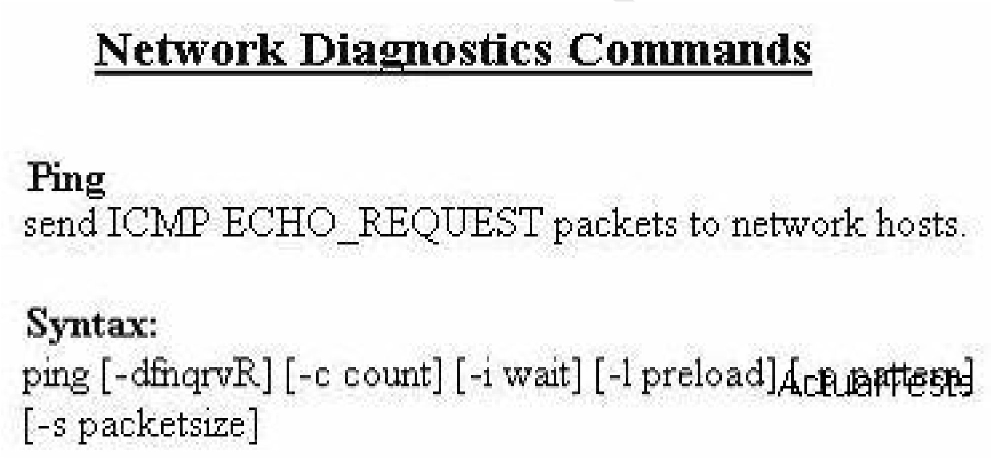
You are creating automatic NAT rules by configuring the necessary network objects. For each object that you configure with Static NAT, how many NAT rules are created?

A. 2
B. 3
C. 5
D. 1
E. 4

Answer: A

QUESTION NO: 500

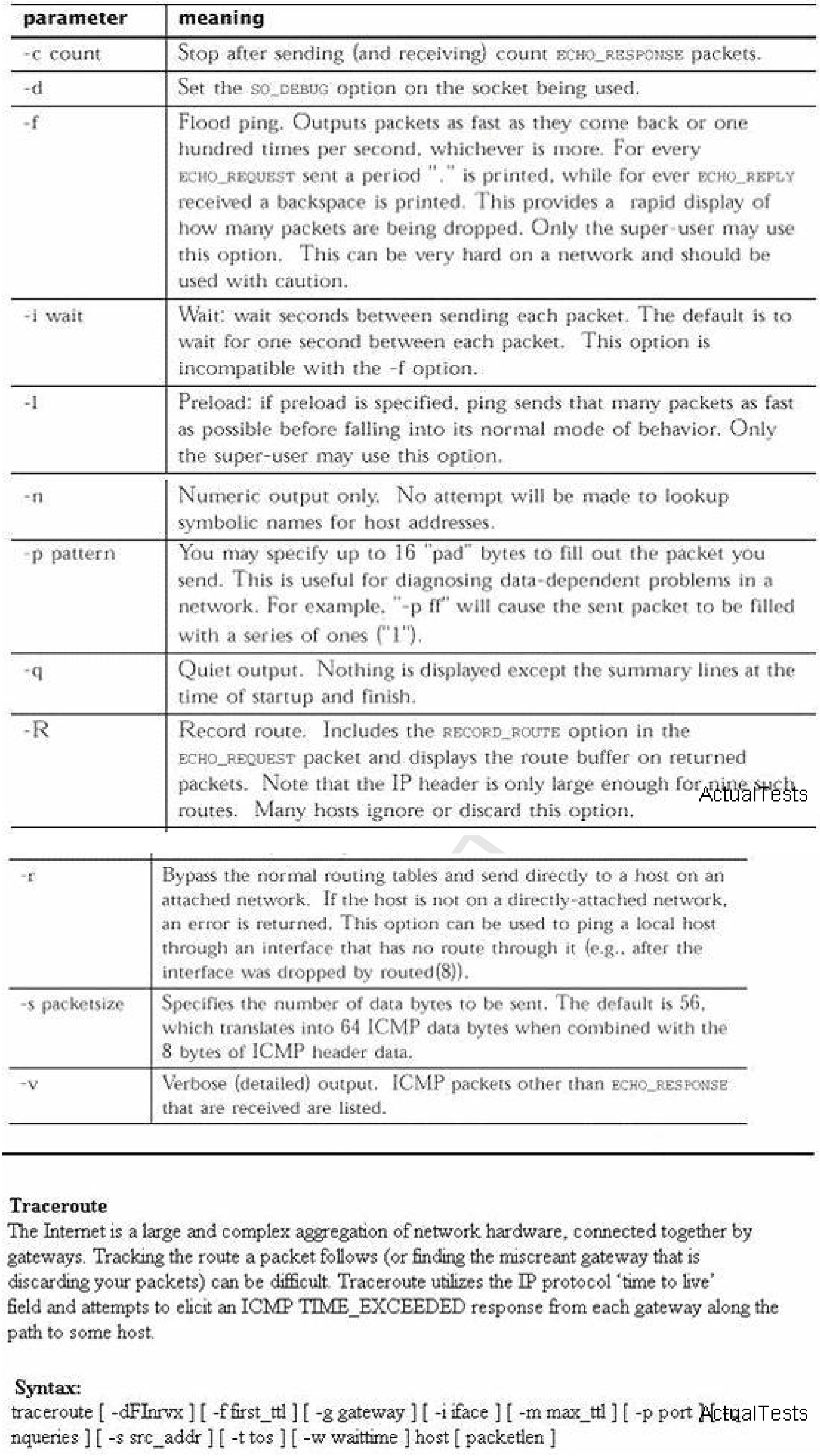
What command would you use (when working in SecurePlatform) in order to discover the path by a data to reach a certain destination?



Network Diagnostics Commands

Ping
send ICMP ECHO_REQUEST packets to network hosts.

Syntax:
ping [-dfnqrvR] [-c count] [-i wait] [-l preload] [-p pattern]
[-s packetsize]



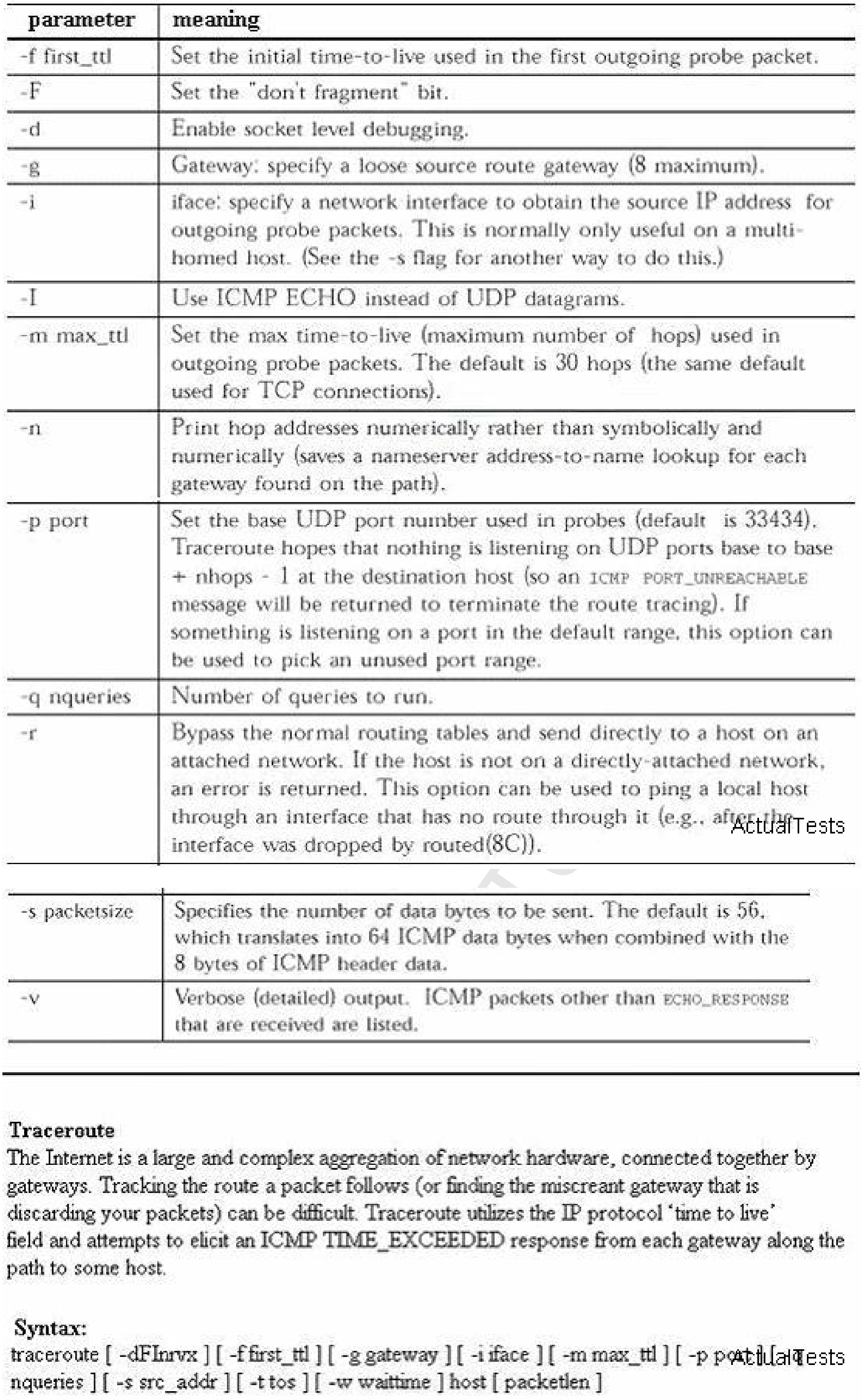
parameter	meaning
-c count	Stop after sending (and receiving) count ECHO_RESPONSE packets.
-d	Set the SO_DEBUG option on the socket being used.
-f	Flood ping. Outputs packets as fast as they come back or one hundred times per second, whichever is more. For every ECHO_REQUEST sent a period "." is printed, while for ever ECHO_REPLY received a backspace is printed. This provides a rapid display of how many packets are being dropped. Only the super-user may use this option. This can be very hard on a network and should be used with caution.
-i wait	Wait: wait seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.
-l	Preload: if preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user may use this option.
-n	Numeric output only. No attempt will be made to lookup symbolic names for host addresses.
-p pattern	You may specify up to 16 "pad" bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, "-p ff" will cause the sent packet to be filled with a series of ones ("1").
-q	Quiet output. Nothing is displayed except the summary lines at the time of startup and finish.
-R	Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.
-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8)).
-s packetsize	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
-v	Verbose (detailed) output. ICMP packets other than ECHO_RESPONSE that are received are listed.

Traceroute

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route a packet follows (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute utilizes the IP protocol 'time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

Syntax:

traceroute [-dFInrvx] [-f first_ttl] [-g gateway] [-i iface] [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos] [-w waittime] host [packetlen]



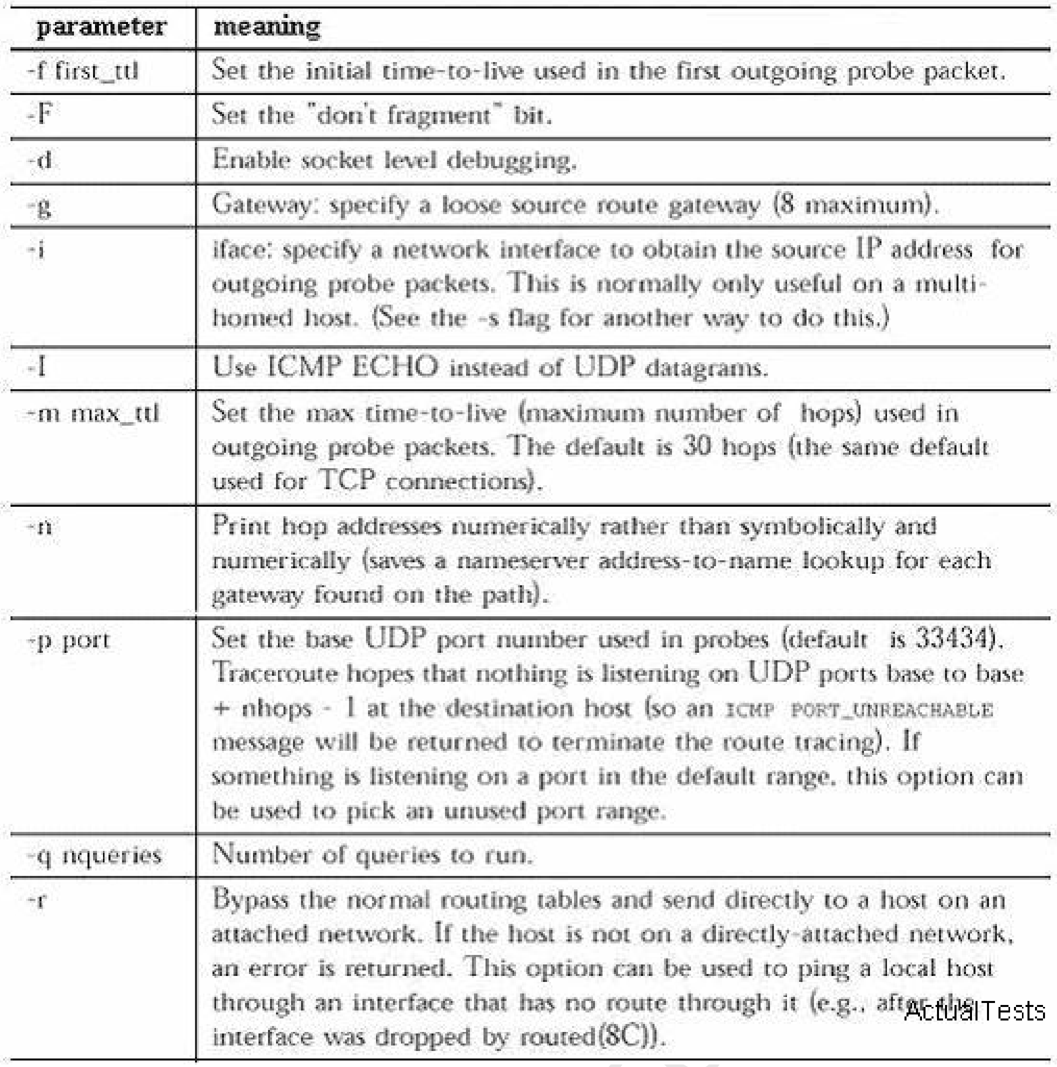
parameter	meaning
-f first_ttl	Set the initial time-to-live used in the first outgoing probe packet.
-F	Set the "don't fragment" bit.
-d	Enable socket level debugging.
-g	Gateway: specify a loose source route gateway (8 maximum).
-i	iface: specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)
-I	Use ICMP ECHO instead of UDP datagrams.
-m max_ttl	Set the max time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
-n	Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).
-p port	Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.
-q nqueries	Number of queries to run.
-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8C)).
-s packetsize	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
-v	Verbose (detailed) output. ICMP packets other than ECHO_RESPONSE that are received are listed.

Traceroute

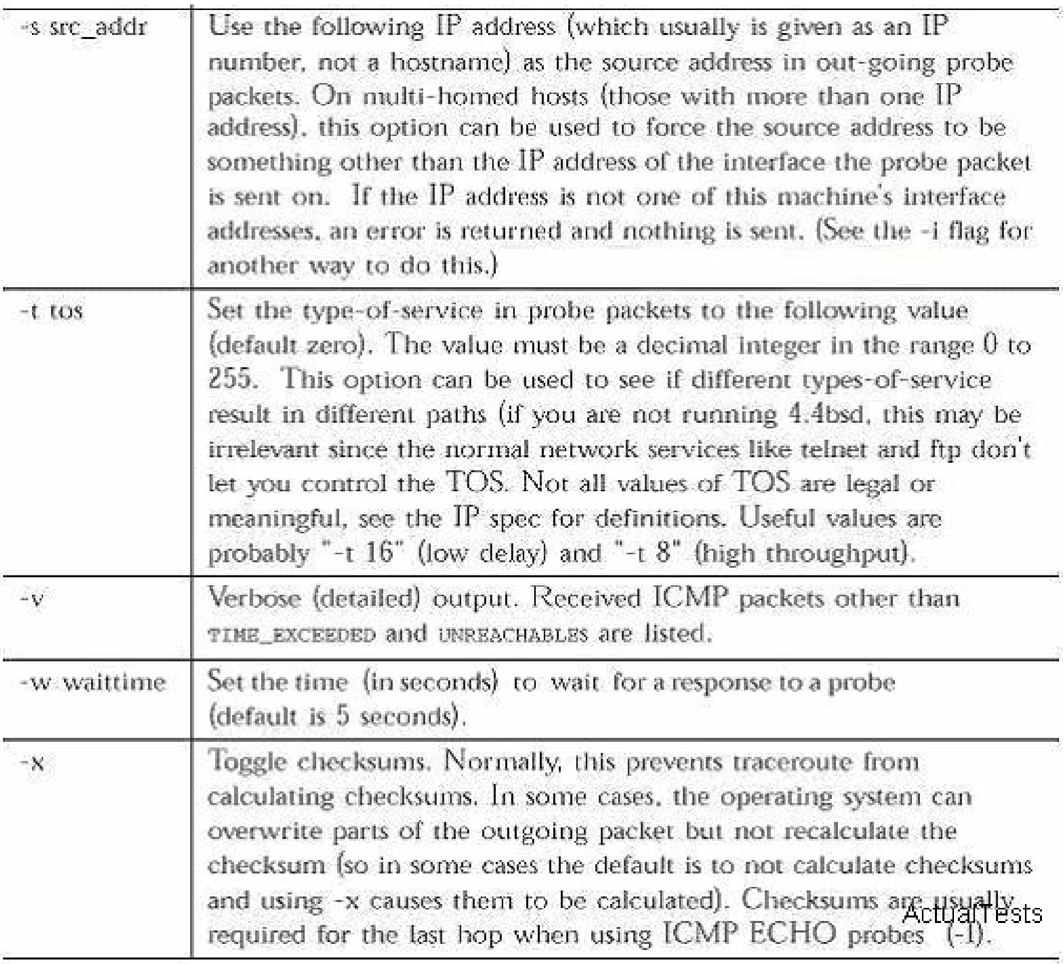
The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route a packet follows (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute utilizes the IP protocol 'time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

Syntax:

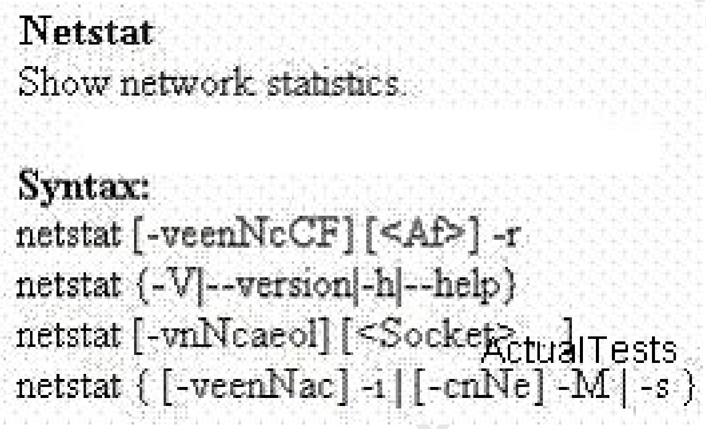
traceroute [-dFInrvx] [-f first_ttl] [-g gateway] [-i iface] [-m max_ttl] [-p port] [-q nqueries] [-s src_addr] [-t tos] [-w waittime] host [packetlen]



parameter	meaning
-f first_ttl	Set the initial time-to-live used in the first outgoing probe packet.
-F	Set the "don't fragment" bit.
-d	Enable socket level debugging.
-g	Gateway: specify a loose source route gateway (8 maximum).
-i	iface: specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)
-I	Use ICMP ECHO instead of UDP datagrams.
-m max_ttl	Set the max time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
-n	Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).
-p port	Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an `ICMP PORT_UNREACHABLE` message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.
-q nqueries	Number of queries to run.
-r	Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (e.g., after the interface was dropped by routed(8C)).



-s src_addr	Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in out-going probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)
-t tos	Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths (if you are not running 4.4bsd, this may be irrelevant since the normal network services like telnet and ftp don't let you control the TOS. Not all values of TOS are legal or meaningful, see the IP spec for definitions. Useful values are probably "-t 16" (low delay) and "-t 8" (high throughput).
-v	Verbose (detailed) output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLES are listed.
-w waittime	Set the time (in seconds) to wait for a response to a probe (default is 5 seconds).
-x	Toggle checksums. Normally, this prevents traceroute from calculating checksums. In some cases, the operating system can overwrite parts of the outgoing packet but not recalculate the checksum (so in some cases the default is to not calculate checksums and using -x causes them to be calculated). Checksums are usually required for the last hop when using ICMP ECHO probes (-I).

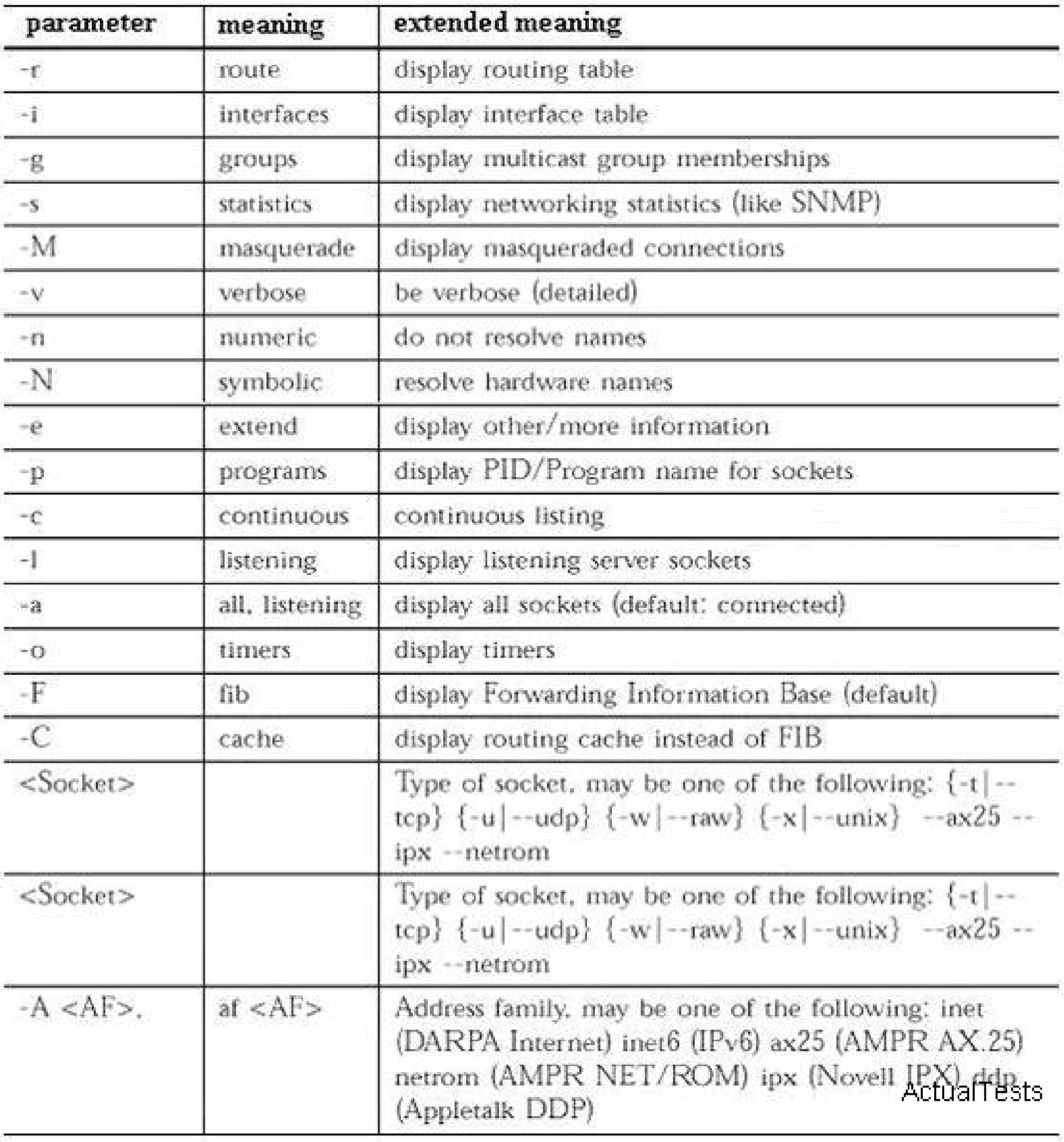


Netstat

Show network statistics.

Syntax:

```
netstat [-veenNcCF] [<Af>] -r
netstat {-V|--version|-h|--help}
netstat [-vnNcaeol] [<Socket> ...]
netstat { [-veenNac] -i | [-cnNe] -M | -s }
```



parameter	meaning	extended meaning
-r	route	display routing table
-i	interfaces	display interface table
-g	groups	display multicast group memberships
-s	statistics	display networking statistics (like SNMP)
-M	masquerade	display masqueraded connections
-v	verbose	be verbose (detailed)
-n	numeric	do not resolve names
-N	symbolic	resolve hardware names
-e	extend	display other/more information
-p	programs	display PID/Program name for sockets
-c	continuous	continuous listing
-l	listening	display listening server sockets
-a	all, listening	display all sockets (default: connected)
-o	timers	display timers
-F	fib	display Forwarding Information Base (default)
-C	cache	display routing cache instead of FIB
<Socket>		Type of socket, may be one of the following: {-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
<Socket>		Type of socket, may be one of the following: {-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
-A <AF>,	af <AF>	Address family, may be one of the following: inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25) netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)

A. Tracert
B. Route
C. Ping
D. Netstat
E. Traceroute

Answer: E

QUESTION NO: 501

If there are multiple protocols with a route to given destination, then these protocols can be ranked to allow a single route to be installed in the forwarding table for the destination. Which of the following allows this?

A. BGP
B. NSP
C. IPSRD

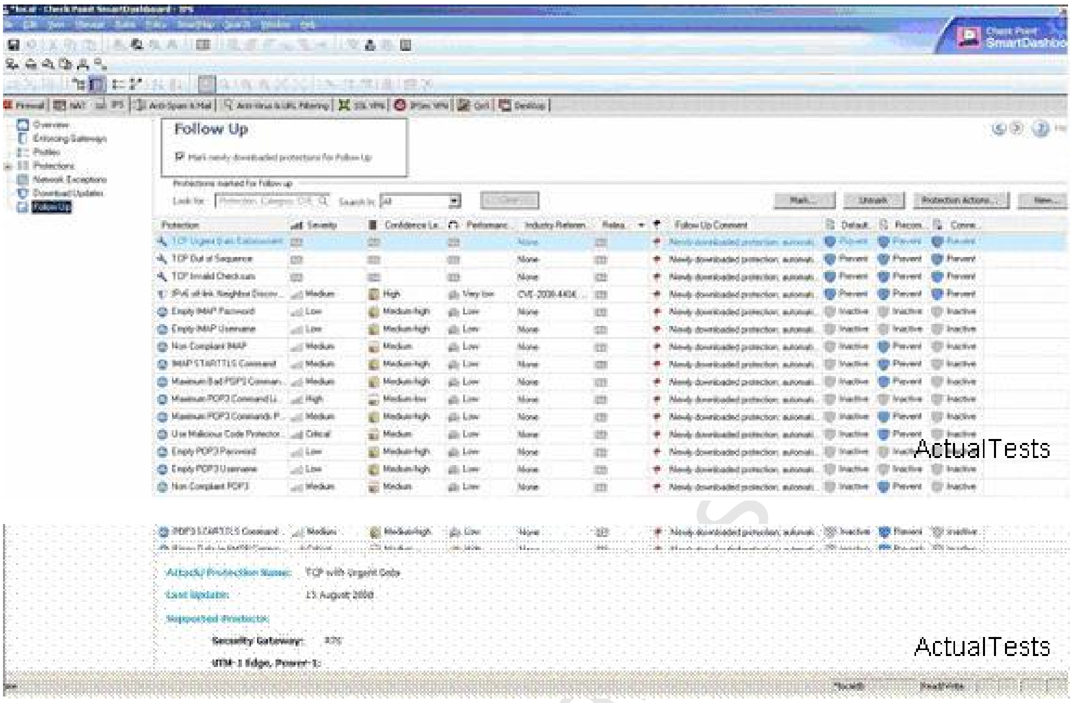
D. NCSP

E. IPSO

Answer: C

QUESTION NO: 502

Which of the following you have to configure prior to downloading the latest IPS protections? Select all the correct answers.



Follow Up

☑ Mark newly downloaded protections for Follow Up

Protections marked for Follow up

Look for: Protection, Category, CVE   Search in: All

Protection	Severity	Confidence Le...	Performanc...	Industry Referen...	Relea...		Follow Up Comment	Default...	Recom...	Conne...
TCP Urgent Data Enforcement	▨	▨	▨	None	▨	✓	Newly downloaded protection; automati...	Prevent	Prevent	Prevent
TCP Out of Sequence	▨	▨	▨	None	▨	✓	Newly downloaded protection; automati...	Prevent	Prevent	Prevent
TCP Invalid Checksum	▨	▨	▨	None	▨	✓	Newly downloaded protection; automati...	Prevent	Prevent	Prevent
IPv6 all-link Neighbor Discov...	Medium	High	Very low	CVE-2008-4404...	▨	✓	Newly downloaded protection; automati...	Prevent	Prevent	Prevent
Empty IMAP Password	Low	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Inactive	Inactive
Empty IMAP Username	Low	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Inactive	Inactive
Non Compliant IMAP	Medium	Medium	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
IMAP STARTTLS Command	Medium	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
Maximum Bad POP3 Comman...	Medium	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
Maximum POP3 Command Li...	High	Medium-low	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Inactive	Inactive
Maximum POP3 Commands P...	Medium	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
Use Malicious Code Protector...	Critical	Medium	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
Empty POP3 Password	Low	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Inacti	Inactive
Empty POP3 Username	Low	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Inactive	Inactive
Non Compliant POP3	Medium	Medium	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive
POP3 STARTTLS Command	Medium	Medium-high	Low	None	▨	✓	Newly downloaded protection; automati...	Inactive	Prevent	Inactive

Attack/Protection Name: TCP with Urgent Data

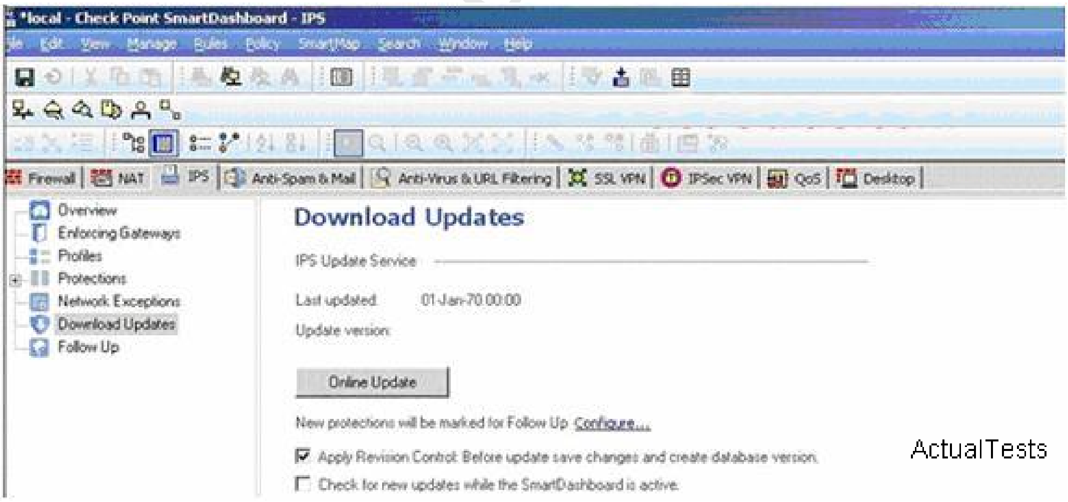
Last Update: 15 August 2008

Supported Products:

Security Gateway: R70

UTM-1 Edge, Power-1:

Figure 1: IPS Tab - Follow Up page



*local - Check Point SmartDashboard - IPS

Download Updates

IPS Update Service

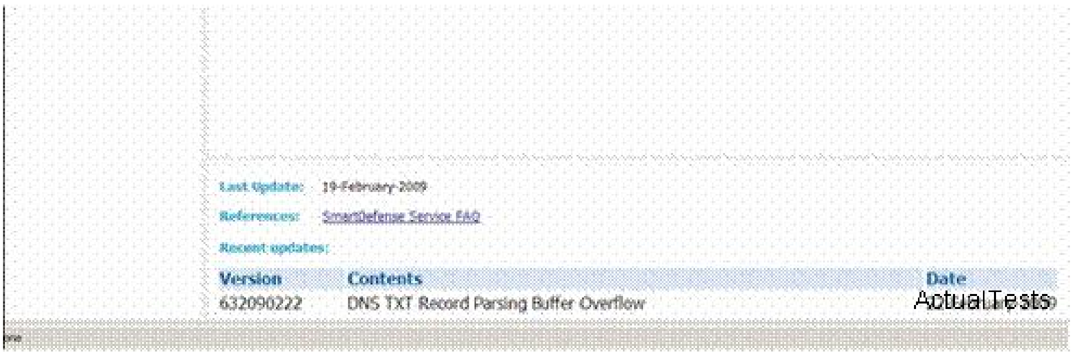
Last updated: 01-Jan-70 00:00

Update version:

New protections will be marked for Follow Up Configure...

☑ Apply Revision Control: Before update save changes and create database version.

□ Check for new updates while the SmartDashboard is active.



Last Update: 19-February-2009

References: SmartDefense Service FAQ

Recent updates:

Version	Contents	Date
632090222	DNS TXT Record Parsing Buffer Overflow	[illegible]

Figure 2: IPS Tab - Download Updates page

A. Click on Online Update button in the Download Updates page in the IPS tab
B. Check for new updates while the SmartView Tracker is lively
C. Configure Database Revision Control
D. Check for new updates while the SmartDashboard is active
E. Mark newly downloaded protections for Follow Up

Answer: C,D,E

QUESTION NO: 503

You successfully setup SSH. Your SSH server is up and running. You configured SSH to use standard port 22. You now try to establish a connection with the server from your client, using correct credentials. You are having problem connecting to the server. What is likely to be the reason why you cannot connect?

A. The public key is not accurate
B. The username or password might be wrong
C. The configured port is wrong
D. The server IP address is wrong
E. The client IP address is incorrect

Answer: A

QUESTION NO: 504

Which view would provide you with feature that allows you to keep track of VPN remote users currently on or any IPSec clients connecting to the gateways?

A. Tunnels
B. System Counters
C. Traffic

D. Remote Users
E. Gateway Status

Answer: D

QUESTION NO: 505

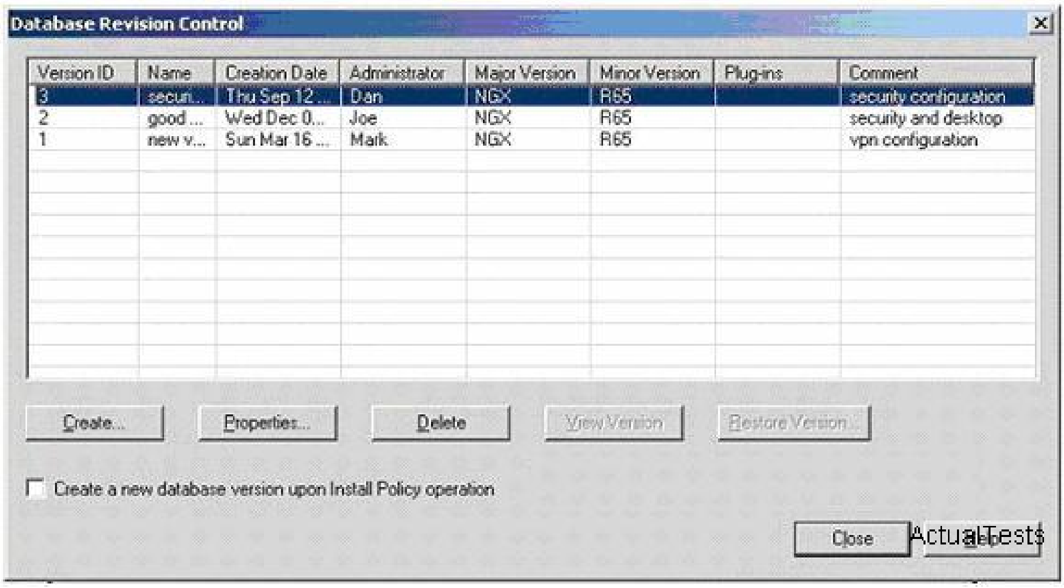
Logging information on the Anti-Virus scan is sent to the Security Management server and can be viewed using which of the following GUI?

A. cpinfo
B. Eventia Reporter
C. SmartView Monitor
D. SmartView Tracker
E. cpconfig

Answer: D

QUESTION NO: 506

Which window must you use to create a new version of the current policy, manually?



Database Revision Control

Version ID	Name	Creation Date	Administrator	Major Version	Minor Version	Plug-ins	Comment
3	secur...	Thu Sep 12 ...	Dan	NGX	R65		security configuration
2	good ...	Wed Dec 0...	Joe	NGX	R65		security and desktop
1	new v...	Sun Mar 16 ...	Mark	NGX	R65		vpn configuration

□ Create a new database version upon Install Policy operation

Figure 1: Database Revision Control window

A. Operations Objects
B. Copy Policy Wizard window
C. QoS Classes
D. Virtual Links

E. Database Revision Control window

Answer: E

QUESTION NO: 507

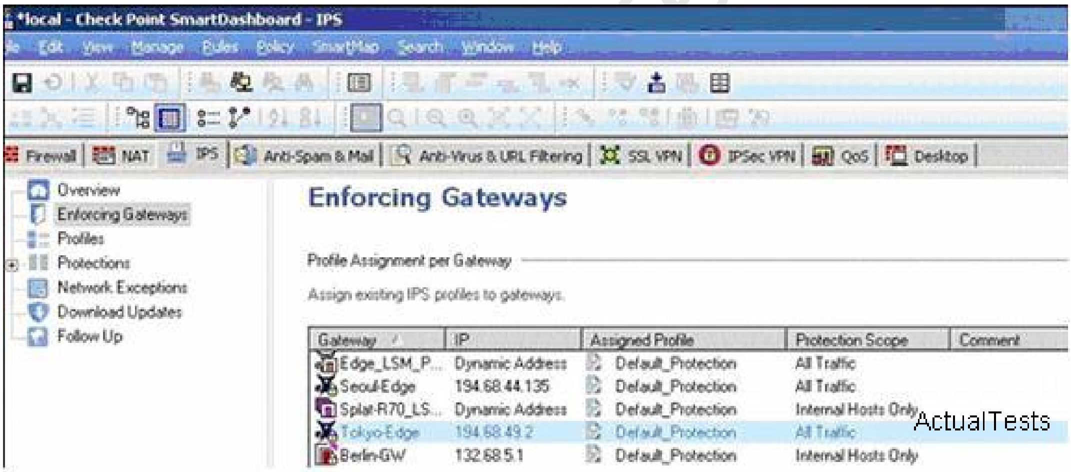
Which of the following is true of Alerts in SmartView Monitor?

A. Alerts are sentIf certain rules or attributes are matched
B. By default an alert is sent as a pop up message only to the administrator's system server when a new alert arrives to SmartView Monitor
C. System Alerts can be defined per product
D. Alerts provide real-time information about vulnerabilities to computer systems and how they can be eliminated
E. Alerts are sent in order to draw theadministrators attention to problematic gateways

Answer: A,C,D,E

QUESTION NO: 508

How will you assign an IPS profile?



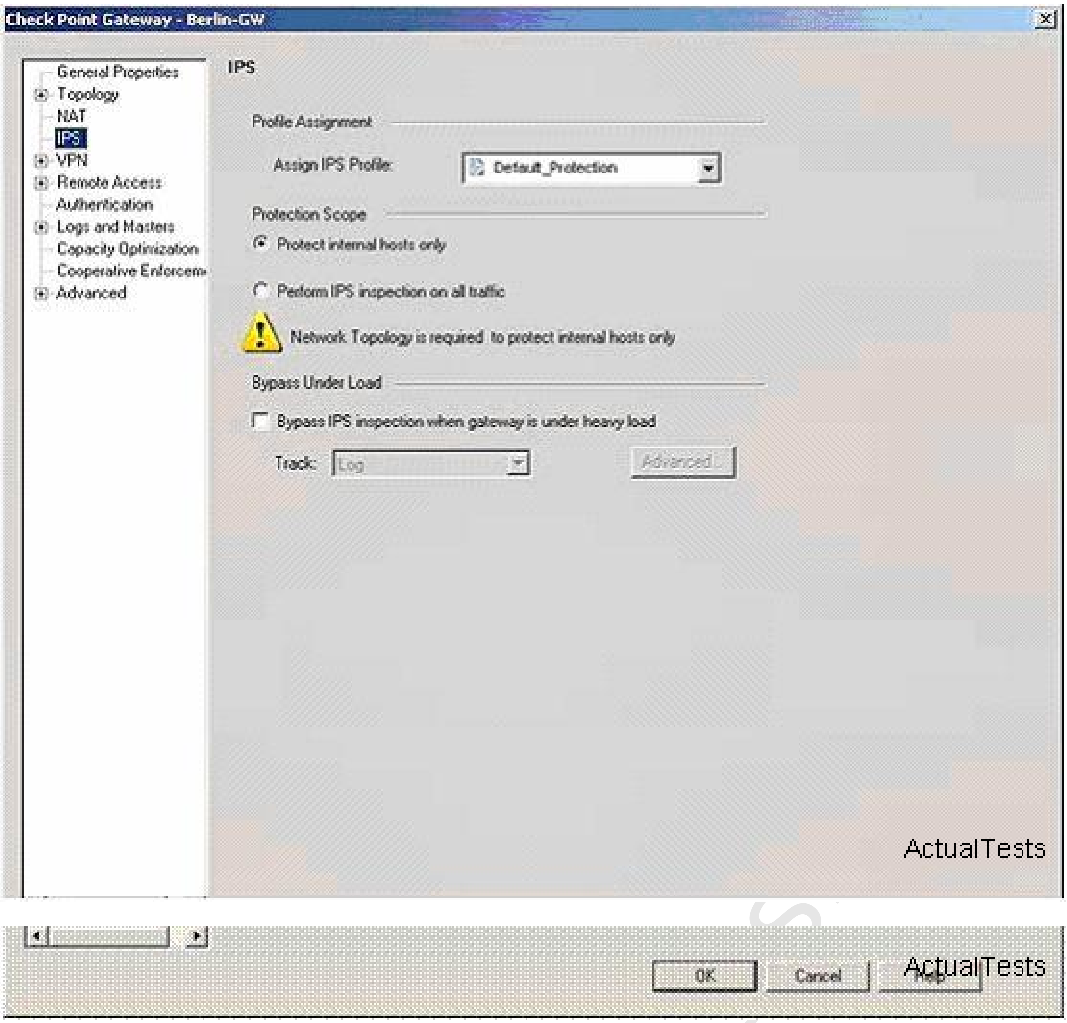
Enforcing Gateways

Profile Assignment per Gateway

Assign existing IPS profiles to gateways.

Gateway	IP	Assigned Profile	Protection Scope	Comment
Edge_LSM_P...	Dynamic Address	Default_Protection	All Traffic	
Seoul-Edge	194.68.44.135	Default_Protection	All Traffic	
Splat-R70_LS...	Dynamic Address	Default_Protection	Internal Hosts Only	
Tokyo-Edge	194.68.49.2	Default_Protection	All Traffic	
Berlin-GW	132.68.5.1	Default_Protection	Internal Hosts Only	

Figure 1: Enforcing Gateways



Check Point Gateway - Berlin-GW

IPS

Profile Assignment

Assign IPS Profile: Default_Protection

Protection Scope

● Protect internal hosts only

○ Perform IPS inspection on all traffic

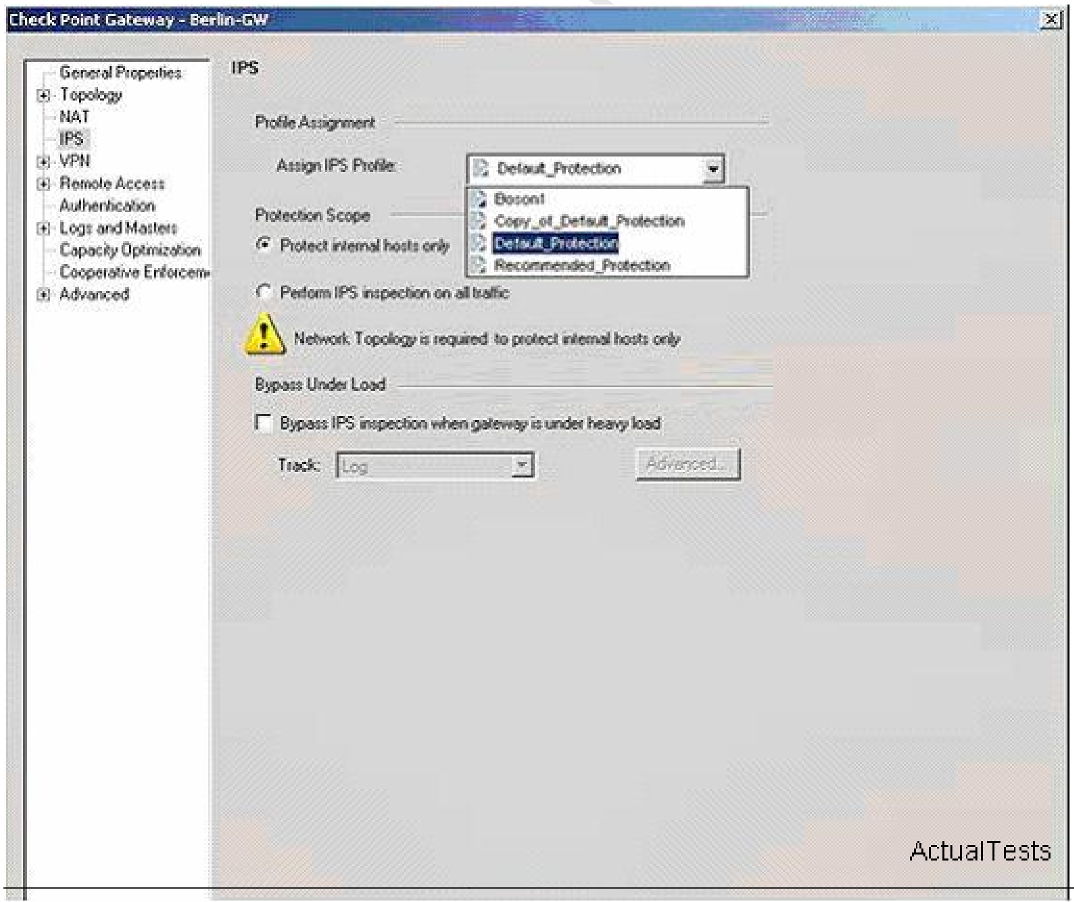
Network Topology is required to protect internal hosts only

Bypass Under Load

□ Bypass IPS inspection when gateway is under heavy load

Track: Log

Figure 2: Gateway Properties Window



Check Point Gateway - Berlin-GW

IPS

Profile Assignment

Assign IPS Profile: Default_Protection

Protection Scope

● Protect internal hosts only

○ Perform IPS inspection on all traffic

Network Topology is required to protect internal hosts only

Bypass Under Load

□ Bypass IPS inspection when gateway is under heavy load

Track: Log

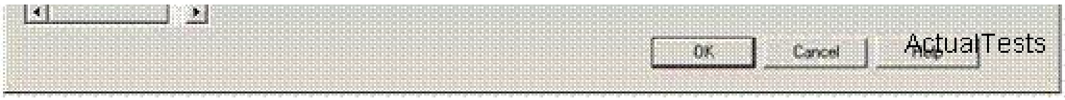
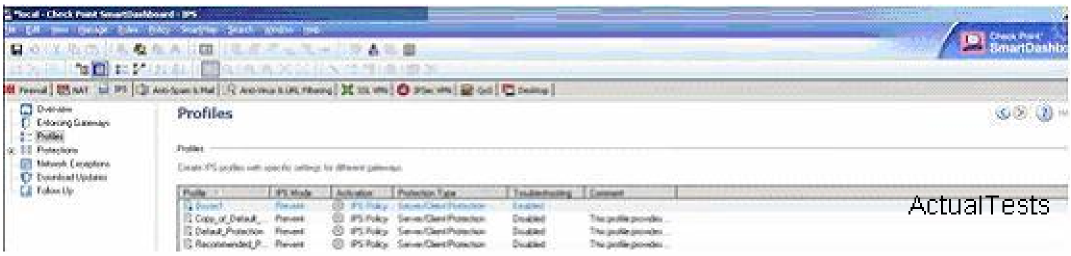


Figure 3: Gateway Properties Window - Assigning a Profile



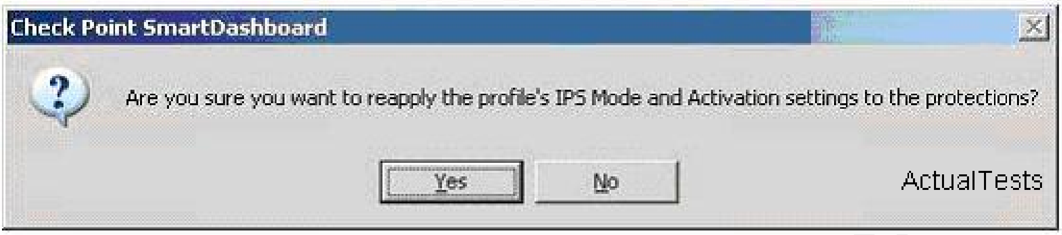
Profiles

Profiles

Create IPS profiles with specific settings for different gateways.

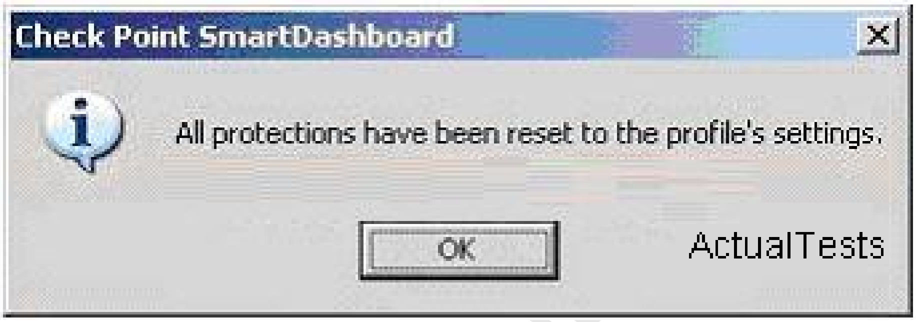
Profile	IPS Mode	Activation	Protection Type	Troubleshooting	Comment
[illegible]	Prevent	IPS Policy	Server/Client Protection	Enabled	
Copy_of_Default_...	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides...
Default_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides...
Recommended_P...	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides...

Figure 4: SmartDashboard - IPS Tab , Showing Action Menu


Check Point SmartDashboard

Are you sure you want to reapply the profile's IPS Mode and Activation settings to the protections?

Figure 5: Re-application of the IPS Mode and Activation settings message


Check Point SmartDashboard

All protections have been reset to the profile's settings.

Figure 6: Reset Message

A. Go to SmartView Monitor, IPS tab, select Enforcing Gateways on left compartment, select the desired Gateway and click Edit button to get the properties of the gateway, and assign the appropriate profile

B. Go to SmartView Tracker, IPS tab, select Enforcing Gateways on left compartment, select the desired Gateway and click Edit button to get the properties of the gateway, and assign the appropriate profile

C. Go to SmartUpdate, IPS tab, select Enforcing Gateways on left compartment, select the desired Gateway and click Edit button to get the properties of the gateway, and assign the appropriate profile

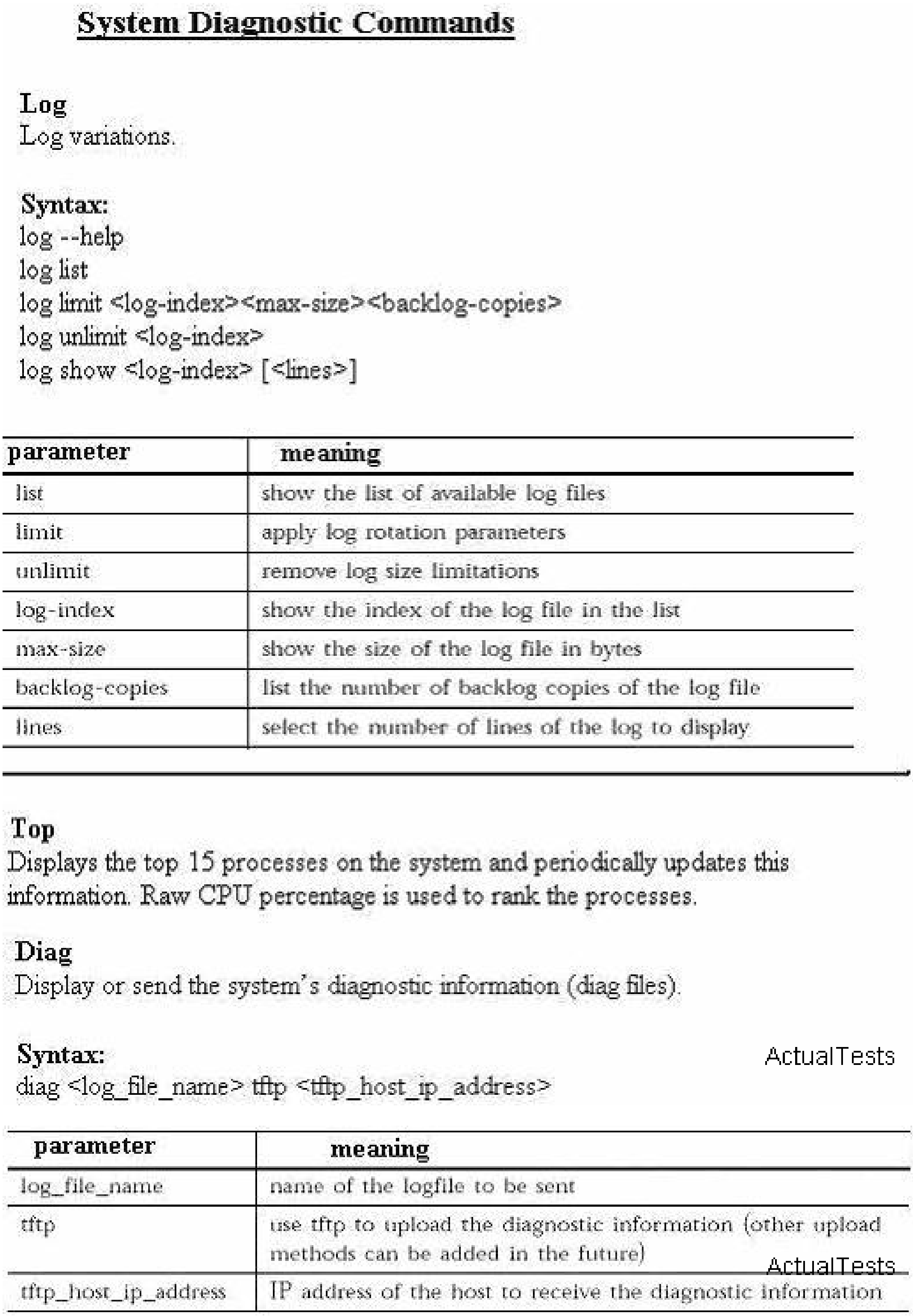
D. Go toSmartDashboard ,IPS tab, select Enforcing Gateways on left compartment, select the desired Gateway and click Edit button to get the properties of the gateway, and assign the appropriate profile

E. Go to Eventia Reporter, IPS tab, select Enforcing Gateways on left compartment, select the desired Gateway and click Edit button to get the properties of the gateway, and assign the appropriate profile

Answer: D

QUESTION NO: 509

What would the command "diag configfile 192.33.45.65" do when using SecurePlatform?



System Diagnostic Commands

Log
Log variations.

Syntax:

```
log --help
log list
log limit <log-index><max-size><backlog-copies>
log unlimit <log-index>
log show <log-index> [<lines>]
```

parameter	meaning
list	show the list of available log files
limit	apply log rotation parameters
unlimit	remove log size limitations
log-index	show the index of the log file in the list
max-size	show the size of the log file in bytes
backlog-copies	list the number of backlog copies of the log file
lines	select the number of lines of the log to display

Top
Displays the top 15 processes on the system and periodically updates this information. Raw CPU percentage is used to rank the processes.

Diag
Display or send the system's diagnostic information (diag files).

Syntax:

```
diag <log_file_name> tftp <tftp_host_ip_address>
```

parameter	meaning
log_file_name	name of the logfile to be sent
tftp	use tftp to upload the diagnostic information (other upload methods can be added in the future)
tftp_host_ip_address	IP address of the host to receive the diagnostic information

A. Send the diagnostic information file called configfile to the tftp host 192.33.45.65
B. Diagnose the diagnostic information file called configfile on the tftp host192.33.45.65
C. Purge the diagnostic information file called configfile on the tftp host 192.33.45.65
D. Revert to the diagnostic information file called configfile on the tftp host 192.33.45.65
E. Kill the diagnostic information file called configfile on the tftp host 192.33.45.65

Answer: A

QUESTION NO: 510

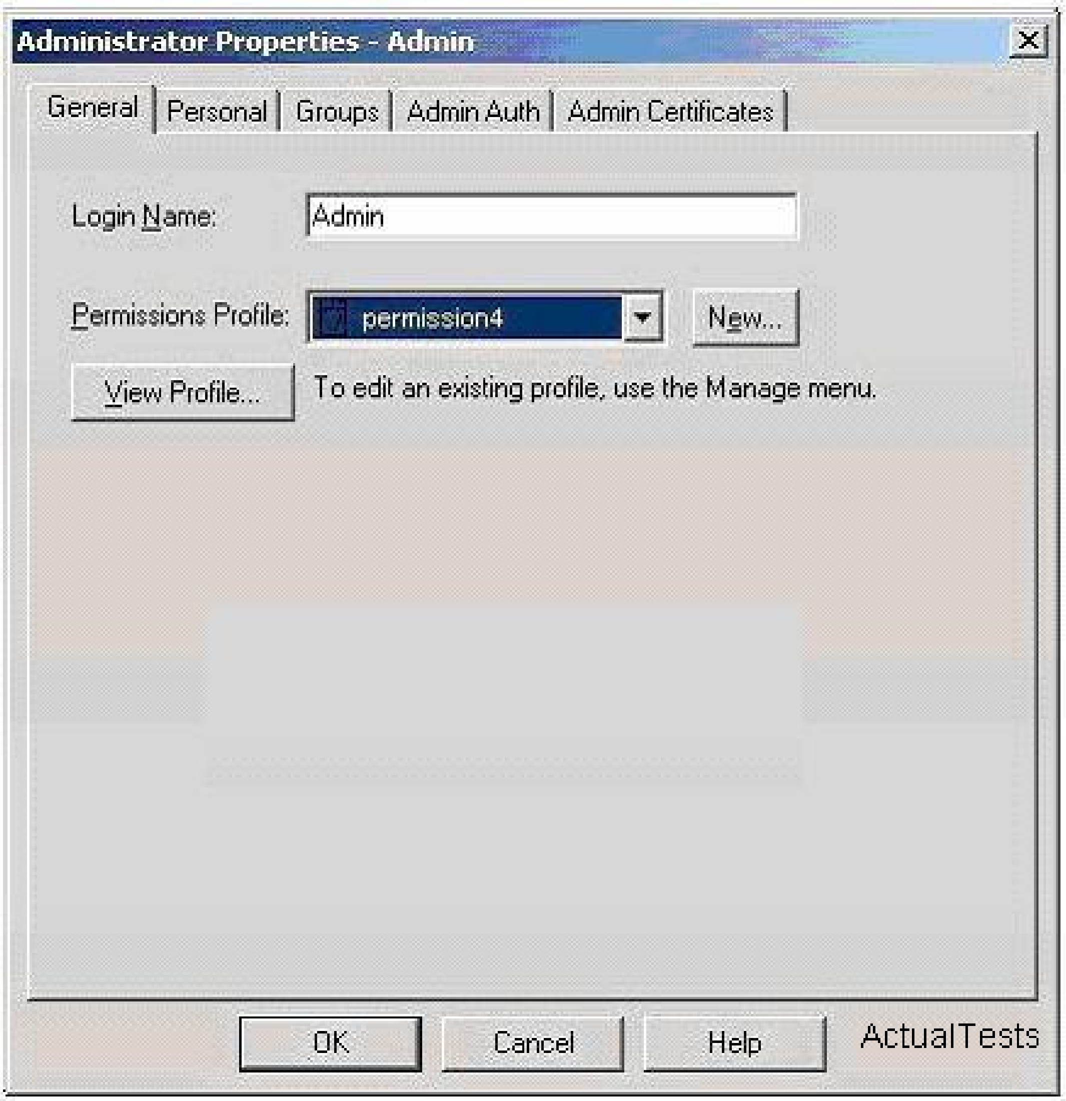
NAT specific question: What are the Hide Mode limitations?

A. Hide Mode cannot be used when the external server must distinguish between clients based on their IP address, since all clients share the same IP address under Hide Mode
B. Hide Mode cannot be used for protocols where the port number cannot be changed
C. Hide Mode must be used for connections initiated by hosts in an internal network, where the host's IP addresses are invalid
D. Hide Mode can be used when the external server must distinguish between clients based on their IP address, since all clients share the same IP address under Hide Mode
E. Hide Mode does not allow access to the "hidden" hosts to be initiated from the outside

Answer: A,B,E

QUESTION NO: 511

What permission would you give an Administrator in order to grant him full access to all Check Point products? Note: If wrong answer(s) is/are chosen, see the diagram for correct answer(s) and explanation.



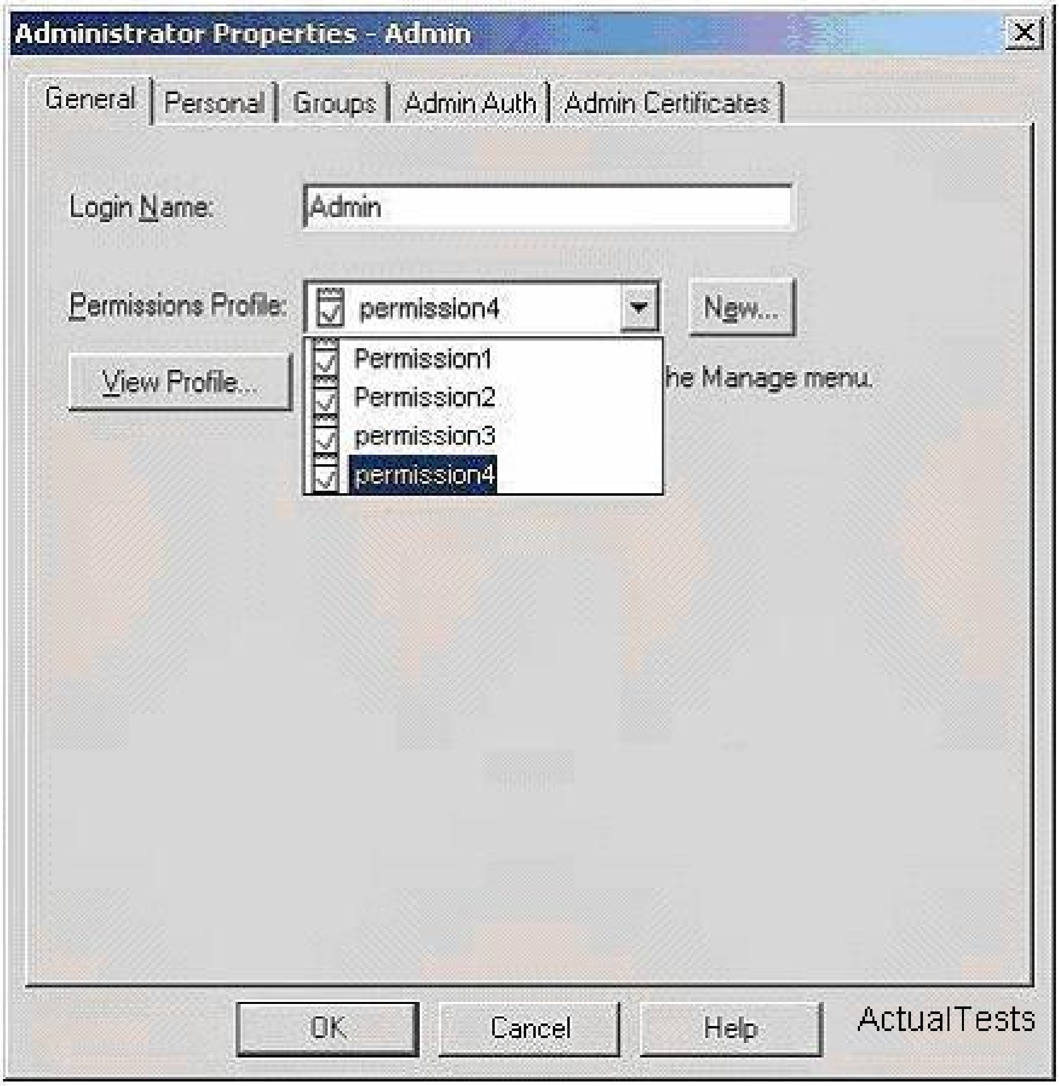
Administrator Properties - Admin

Login Name: Admin

Permissions Profile: permission4

To edit an existing profile, use the Manage menu.

Figure 1: Administrator Properties Windows – selecting Permission 4 profile

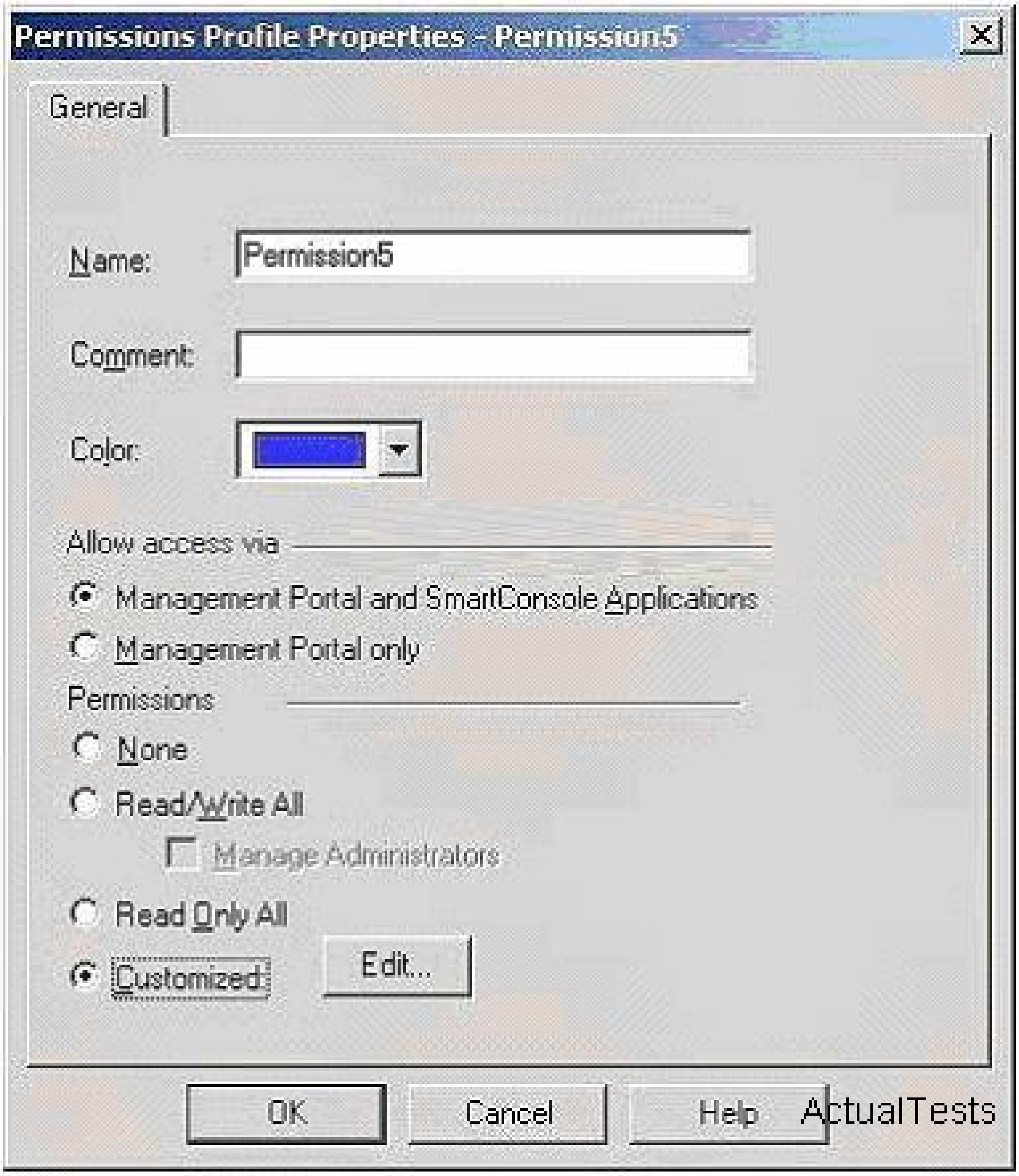


Administrator Properties - Admin

Login Name: Admin

Permissions Profile: permission4

Figure 2 : Administrator Properties Windows - showing four profiles that have been created



Permissions Profile Properties - Permission5

General

Name: Permission5

Comment:

Color: 🟦

Allow access via

● Management Portal and SmartConsole Applications

○ Management Portal only

Permissions

○ None

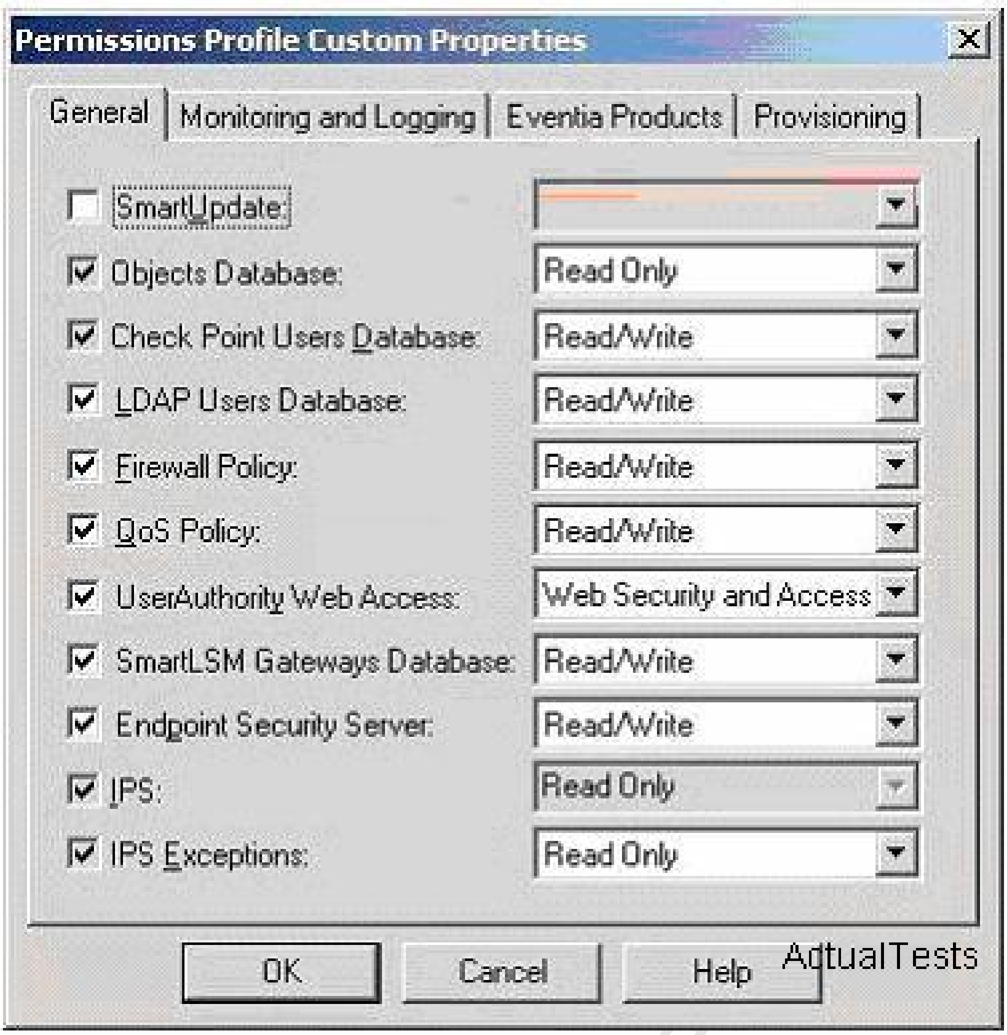
○ Read/Write All

□ Manage Administrators

○ Read Only All

● Customized

Figure 3: Permission Profile Properties box



□ SmartUpdate:

☑ Objects Database: Read Only

☑ Check Point Users Database: Read/Write

☑ LDAP Users Database: Read/Write

☑ Firewall Policy: Read/Write

☑ QoS Policy: Read/Write

☑ UserAuthority Web Access: Web Security and Access

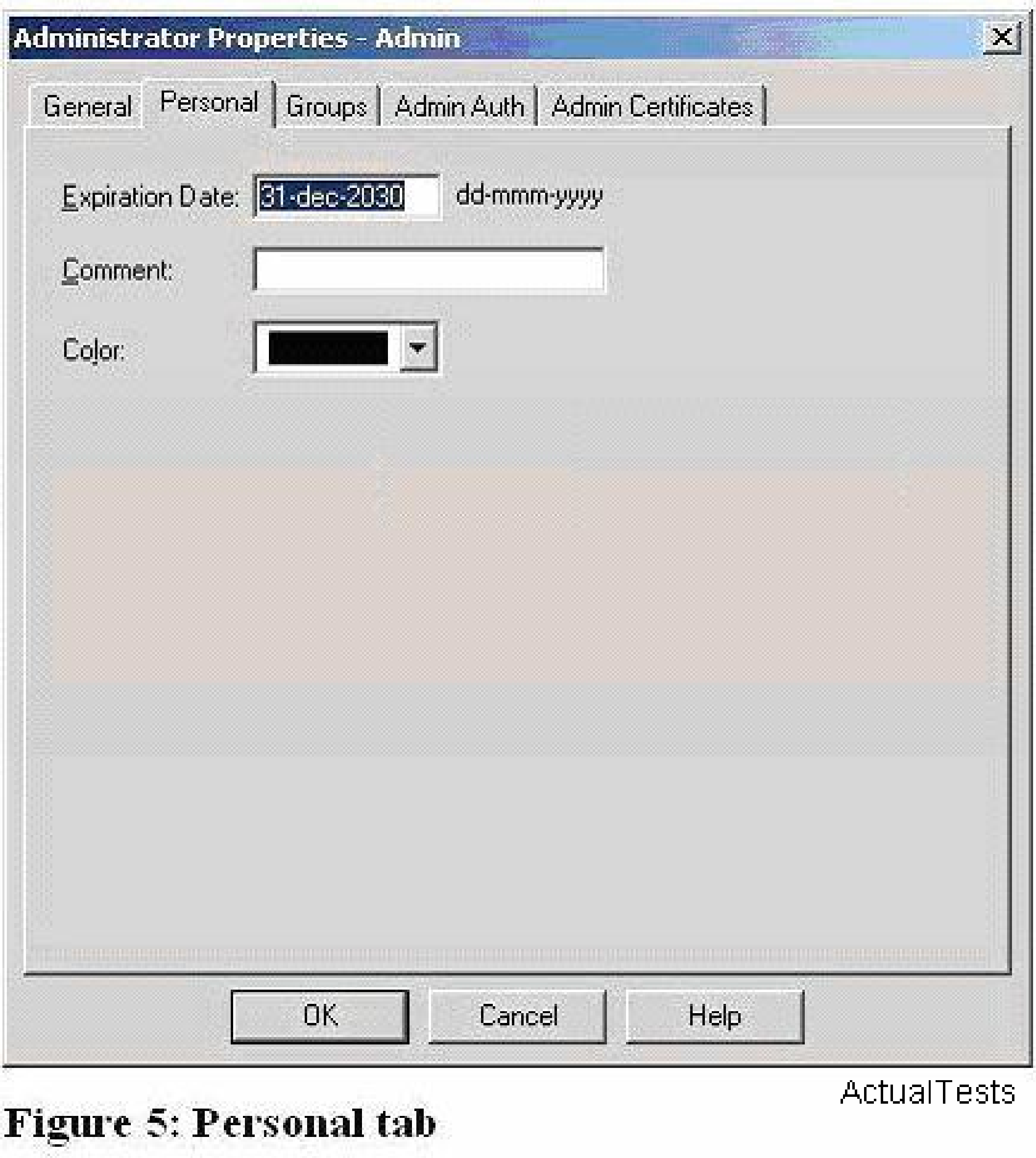
☑ SmartLSM Gateways Database: Read/Write

☑ Endpoint Security Server: Read/Write

☑ IPS: Read Only

☑ IPS Exceptions: Read Only

Figure 4: Permissions Profile Custom Properties box



Expiration Date: 31-dec-2030 dd-mmm-yyyy

Comment:

Color: ■

Figure 5: Personal tab

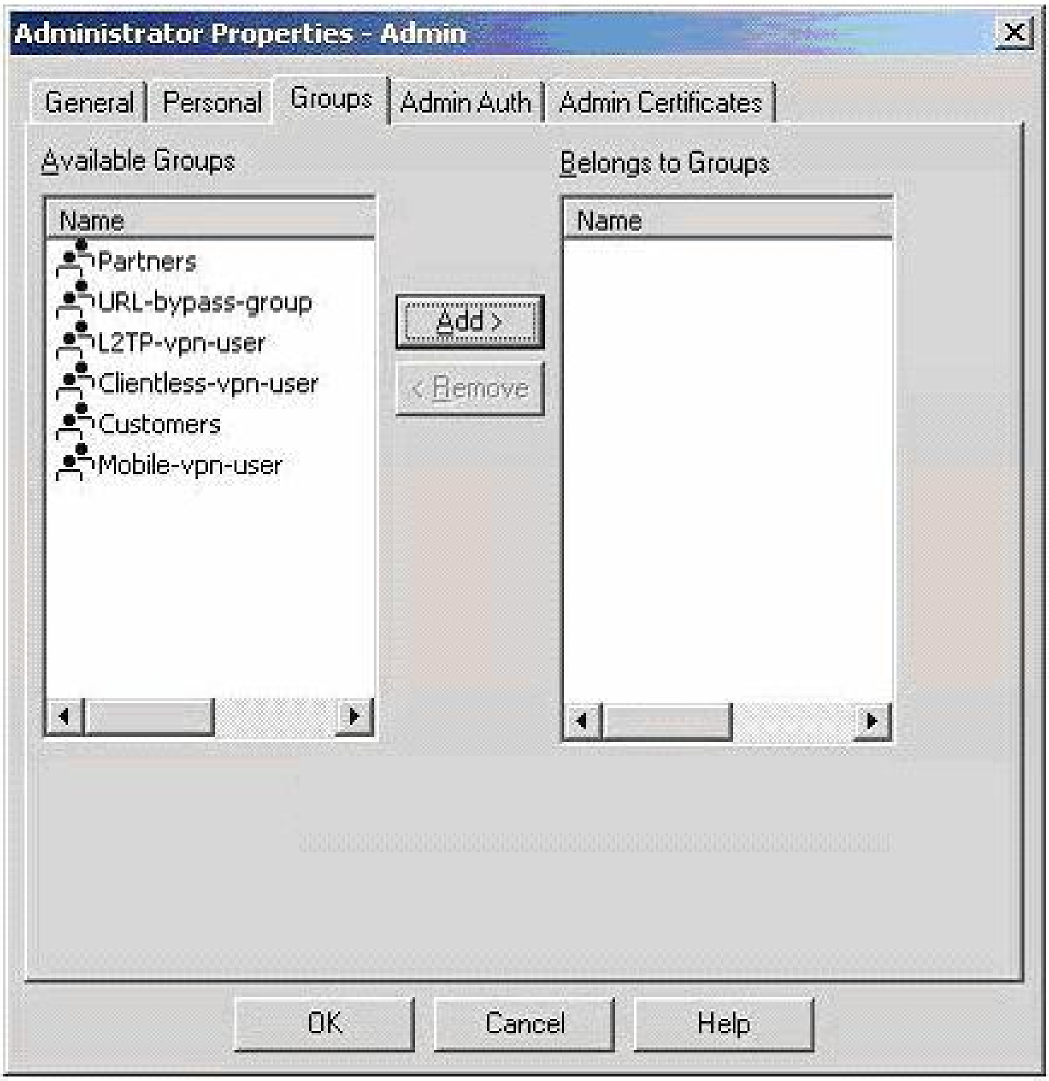
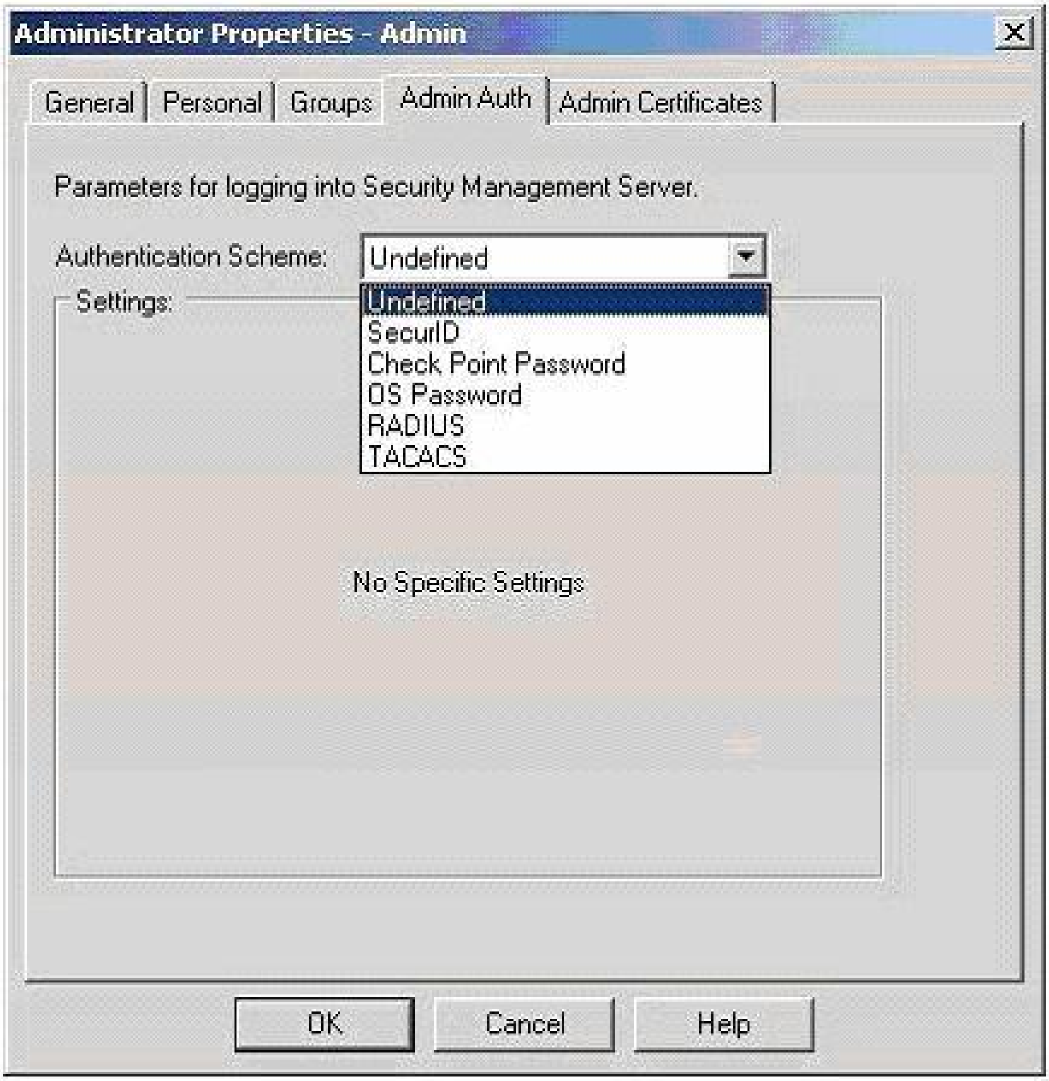


Figure 6: Groups tab



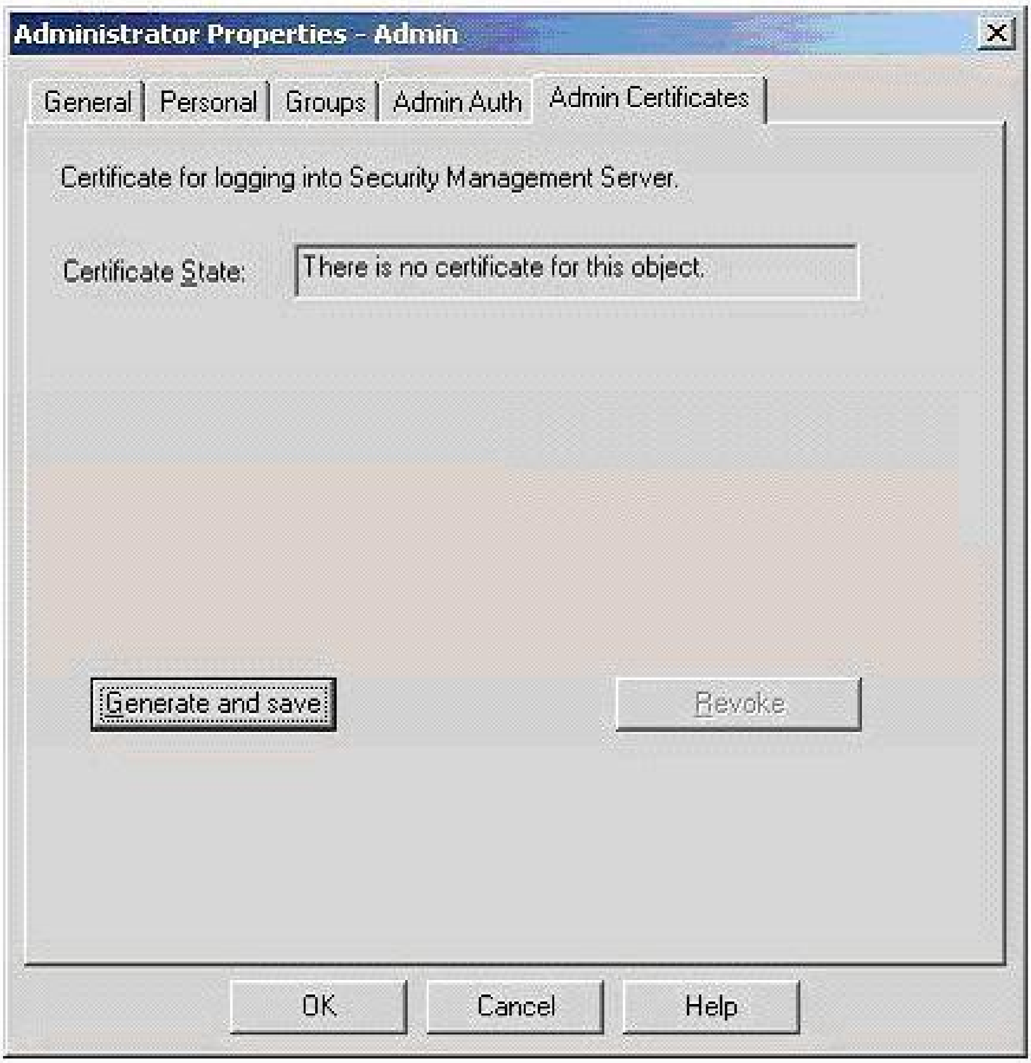
Parameters for logging into Security Management Server.

Authentication Scheme: Undefined

Settings:

No Specific Settings

Figure 7: Admin Authentication tab



Administrator Properties - Admin

Certificate for logging into Security Management Server.

Certificate State: There is no certificate for this object.

Figure 8: Admin Certificates tab

A. Administrator
B. Full Access
C. Read only
D. Supervisor
E. Read / Write All

Answer: E

QUESTION NO: 512

Which of the following enables customization of tailored systems or quick selection of predefined turnkey solutions?

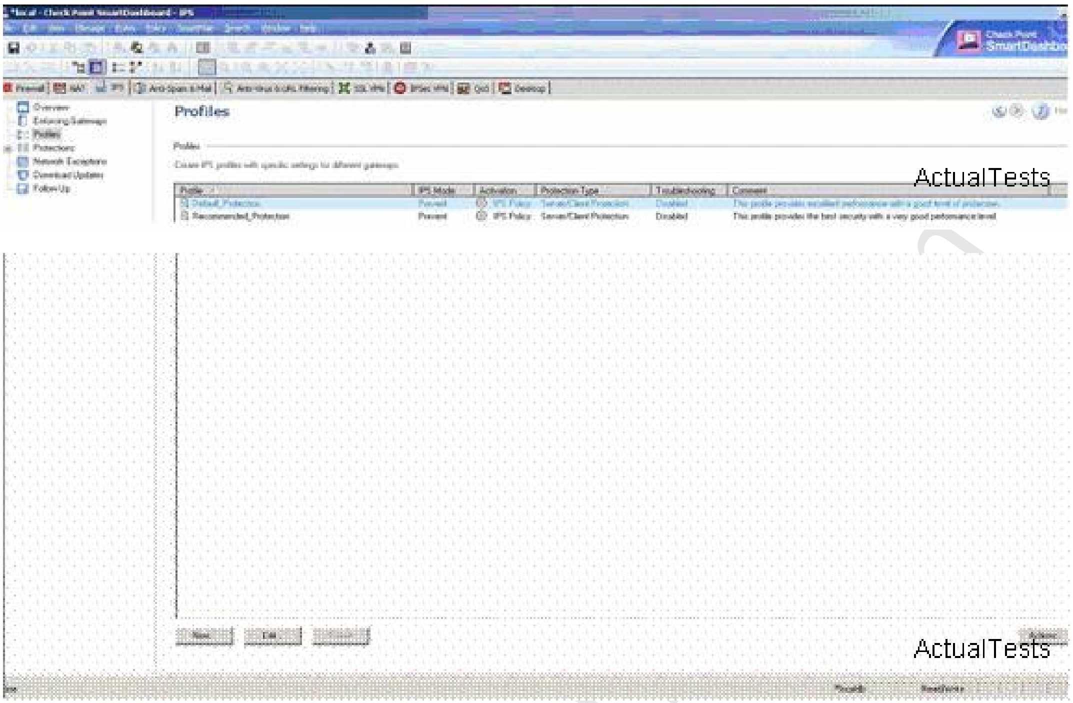
A. Security Gateway Container
B. Endpoint Policy Management
C. Software Blade Architecture
D. Security Management

E. Network Policy Management

Answer: C

QUESTION NO: 513

IPS provides two pre-defined profiles that can be used to immediately implement IPS protection. These are Default_Protection and:



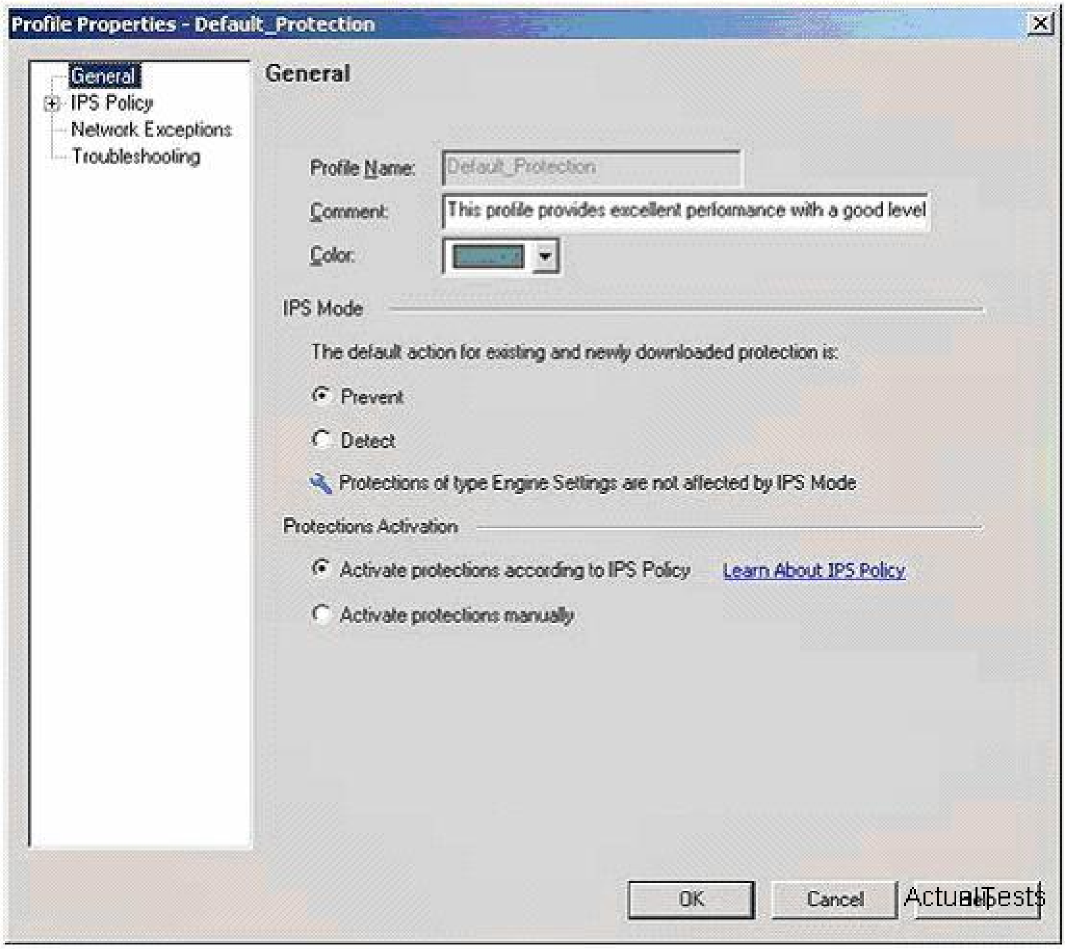
Profiles

Profiles

Create IPS profiles with specific settings for different gateways.

Profile	IPS Mode	Activation	Protection Type	Troubleshooting	Comment
Default_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides excellent performance with a good level of protection.
Recommended_Protection	Prevent	IPS Policy	Server/Client Protection	Disabled	This profile provides the best security with a very good performance level

Figure 1: IPS Protections



General

Profile Name: Default_Protection

Comment: This profile provides excellent performance with a good level

Color:

IPS Mode

The default action for existing and newly downloaded protection is:

● Prevent

○ Detect

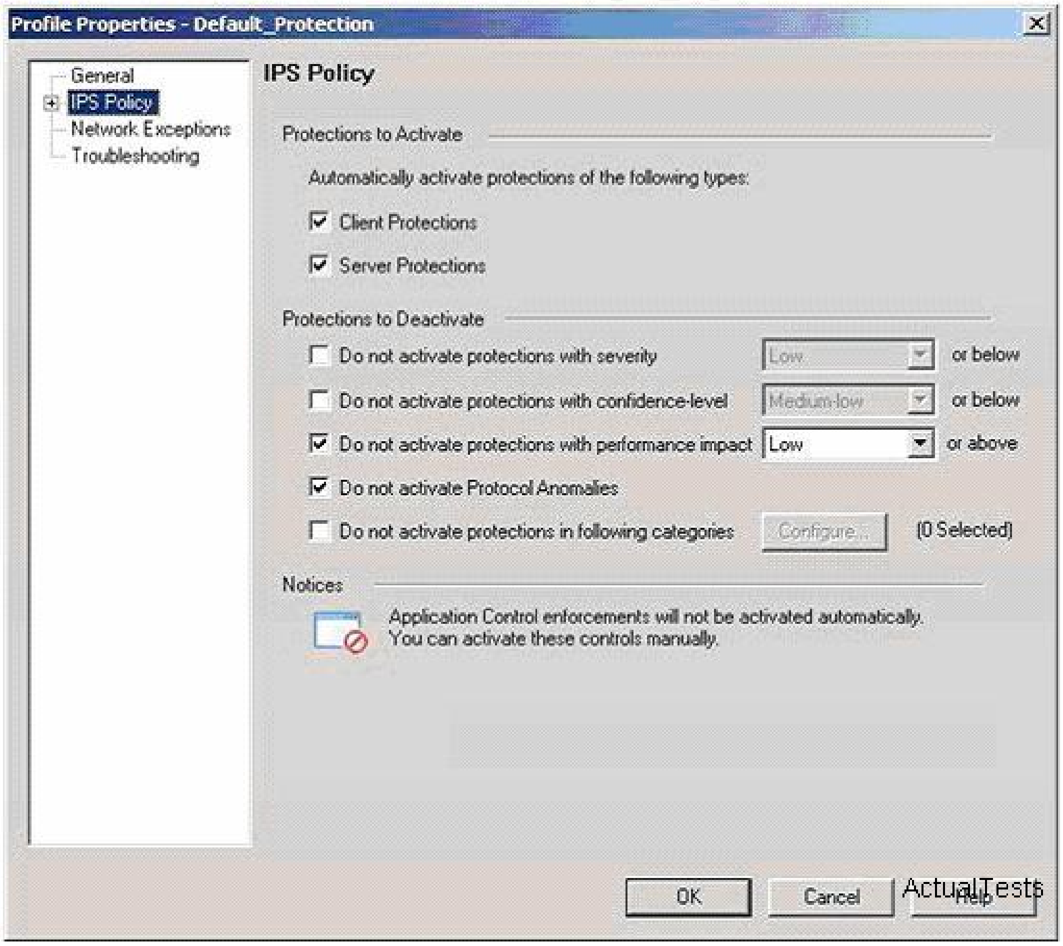
Protections of type Engine Settings are not affected by IPS Mode

Protections Activation

● Activate protections according to IPS Policy   Learn About IPS Policy

○ Activate protections manually

Figure 2: Profiles Properties Window - General Page



IPS Policy

Protections to Activate

Automatically activate protections of the following types:

☑ Client Protections

☑ Server Protections

Protections to Deactivate

□ Do not activate protections with severity Low or below

□ Do not activate protections with confidence-level Medium-low or below

☑ Do not activate protections with performance impact Low or above

☑ Do not activate Protocol Anomalies

□ Do not activate protections in following categories (0 Selected)

Notices

Application Control enforcements will not be activated automatically.
You can activate these controls manually.

Figure 3 : Profiles Properties Window - IPS Policy Page

A. Configured _Protection

B. Attack_Protection

C. Recommended_Protection

D. Customized Protection

E. Customized_Protection

Answer: C