Checkpoint 156-215-71

Check Point Certified Security Administrator R71

Practice Test

Version: 4.5

QUESTION NO: 1

If you check the box Use Aggressive Mode in the IKE Properties dialog box, the standard:

A. three-packet IKE Phase 2 exchange Is replaced by a six-packet exchange
B. three-packet IKE Phase 2 exchange is replaced by a two-packet exchange
C. six-packet IKE Phase 1 exchange is replaced by a three-packet exchange
D. three-packet IKE Phase 1 exchange is replaced by a six-packet exchange

Answer: C
Explanation:

QUESTION NO: 2

Of the following, what parameters will not be preserved when using Database Revision Control?

1) Simplified mode Rule Bases

2) Traditional mode Rule Bases

3) Secure Platform WebUI Users

4) SIC certificates

5) SmartView Tracker audit logs

6) SmartView Tracker traffic logs

7) Implied Rules

8) IPS Profiles

9) Blocked connections

10) Manual NAT rules

11) VPN communities

12) Gateway route table

13) Gateway licenses

A. 3, 4, 5, 6, 9, 12, 13
B. 5, 6, 9, 12, 13
C. 1, 2, 8, 10, 11

D. 2, 4, 7, 10, 11

Answer: B

Explanation:

QUESTION NO: 3

You believe Phase 2 negotiations are railing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicions?

A. SmartDashboard
B. SmartView Tracker
C. SmartUpdate
D. SmartView Status

Answer: B

Explanation:

QUESTION NO: 4

You are running a R71 Security Gateway on SecurePlatform, in case of a hardware failure. You have a server with the exact same hardware and firewall version Installed. What backup method could be used to quickly put the secondary firewall into production?

A. Upgrade_export
B. Manual backup
C. Snapshot
D. Backup

Answer: C

Explanation:

QUESTION NO: 5

What happens hi relation to the CRL cache after a cpstop and cpstart have been initiated?

A. The Gateway retrieves a new CRL on startup, and then discards the old CRL as invalid
B. The Gateway continues to use the old CRL, as long as it is valid.

C. The Gateway continues to use the old CRL even if it is not valid, until a new CRL is cached
D. The Gateway issues a crl_zap on startup, which empties the cache and forces Certificate retrieval

Answer: B
Explanation:

QUESTION NO: 6

What physical machine must have access to the User Center public IP address when checking for new packages with smartUpdate?

A. SmartUpdate GUI PC
B. SmartUpdate Repository SQL database Server
C. A Security Gateway retrieving the new upgrade package
D. SmartUpdate installed Security Management Server PC

Answer: A
Explanation:

QUESTION NO: 7

In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

A. Blank field under Rule Number
B. Rule 0
C. Cleanup Rule
D. Rule 1

Answer: B
Explanation:

QUESTION NO: 8

The URL Filtering Policy can be configured to monitor URLs in order to:

A. Log sites from blocked categories.
B. Redirect users to a new URL.

C. Block sites only once.
D. Alert the Administrator to block a suspicious site.

Answer: A
Explanation:

QUESTION NO: 9

The Customer has a small Check Point installation which includes one Windows XP workstation as SmartConsole, one Solaris server working as security Management Server, and a third server running SecurePlatform as Security Gateway. This is an Example of a (n):

A. Stand-Alone Installation.
B. Unsupported configuration
C. Distributed Installation
D. Hybrid Installation.

Answer: A
Explanation:

QUESTION NO: 10

You want to implement Static Destination NAT in order to provide external. Internet users access to an internal Webserver that has a reserved (RFC 1918) IP address You have an unused valid IP address on the network between your Security Gateway and ISP router. You control the router that sits between the external interface of the firewall and the Internet. What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?

A. Place a static host route on the firewall for the valid IP address to the internal Web server.
B. Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.
C. Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
D. Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.

Answer: C
Explanation:

QUESTION NO: 11

The third-shift Administrator was updating Security Management Server access settings in global properties. He managed to lock all of the administrators out of their accounts. How should you unlock these accounts?

A. Login to SmartDashboard as the special cpconfig_admin user account, right click on administrator object and select Unlock.
B. Type fwm lock_admin -ua from the command line of the Security Manager server.
C. Reinstall the Security Management Server and restore using upgrade_import.
D. Delete the file admin.lock in the $fwDIR/tmp/ directory of the Security Management server.

Answer: B
Explanation:

QUESTION NO: 12

You find a suspicious connection from a problematic host. You decide that you want to block everything from the whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the rule base. How do you achieve this?

A. Add a “temporary” rule using SmartDashboard and select hide rule.
B. Create a Suspicious Activity Rule in SmartView Monitor
C. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0. fws configuration file.
D. Select block intruder from the tools menu in SmartView Tracker.

Answer: B
Explanation:

QUESTION NO: 13

The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?

A. Session and Network layers
B. Application and Presentation layers
C. Physical and Data link layers
D. Network and Data link layers

Answer: D

Explanation:

QUESTION NO: 14

Phase 1 uses_____.

A. Conditional
B. Sequential
C. Asymmetric
D. Symmetric

Answer: D
Explanation:

QUESTION NO: 15

An advantage of using central instead of local licensing is:

A. A license can be taken from one Security Management server and given to another Security Management Server.
B. Only one IP address is used for all licenses.
C. Licenses are automatically attached to their respective Security Gateways.
D. The license must be renewed when changing the IP address of security Gateway. Each module's license has a unique IP address.

Answer: B
Explanation:

QUESTION NO: 16

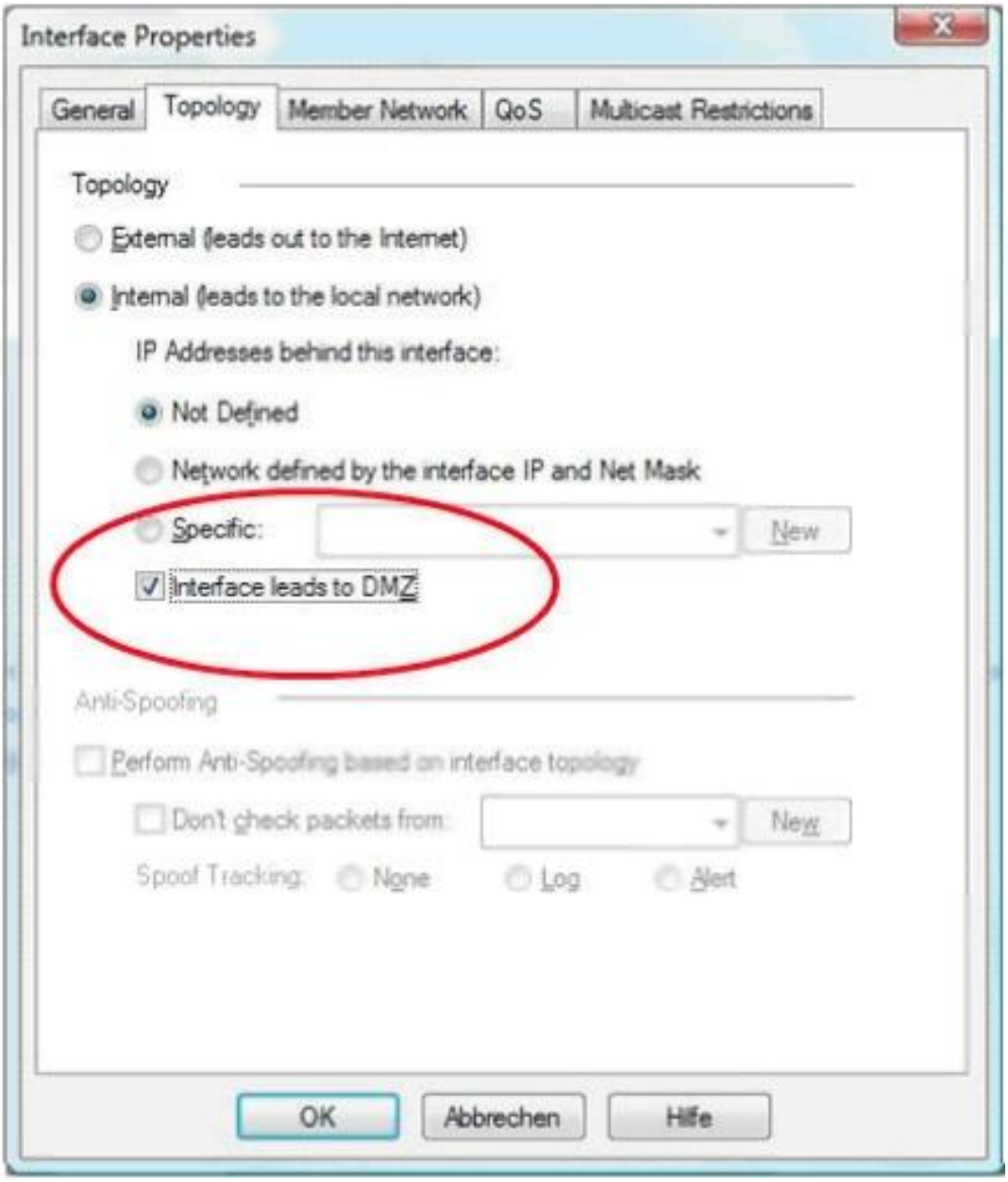
Which of the following uses the same key to decrypt as it does to encrypt?

A. Asymmetric encryption
B. Symmetric encryption
C. Certificate-based encryption
D. Dynamic encryption

Answer: B
Explanation:

QUESTION NO: 17

When configuring the network interfaces of a checkpoint Gateway, the direction can be defined as Internal or external. What is meaning of interface leading to DMZ?



A. It defines the DMZ Interface since this information is necessary for Content Control.
B. Using restricted Gateways, this option automatically turns off the counting of IP Addresses originating from this interface
C. When selecting this option. Ann-Spoofing is configured automatically to this net.
D. Activating this option automatically turns this interface to External

Answer: A

Explanation:

QUESTION NO: 18

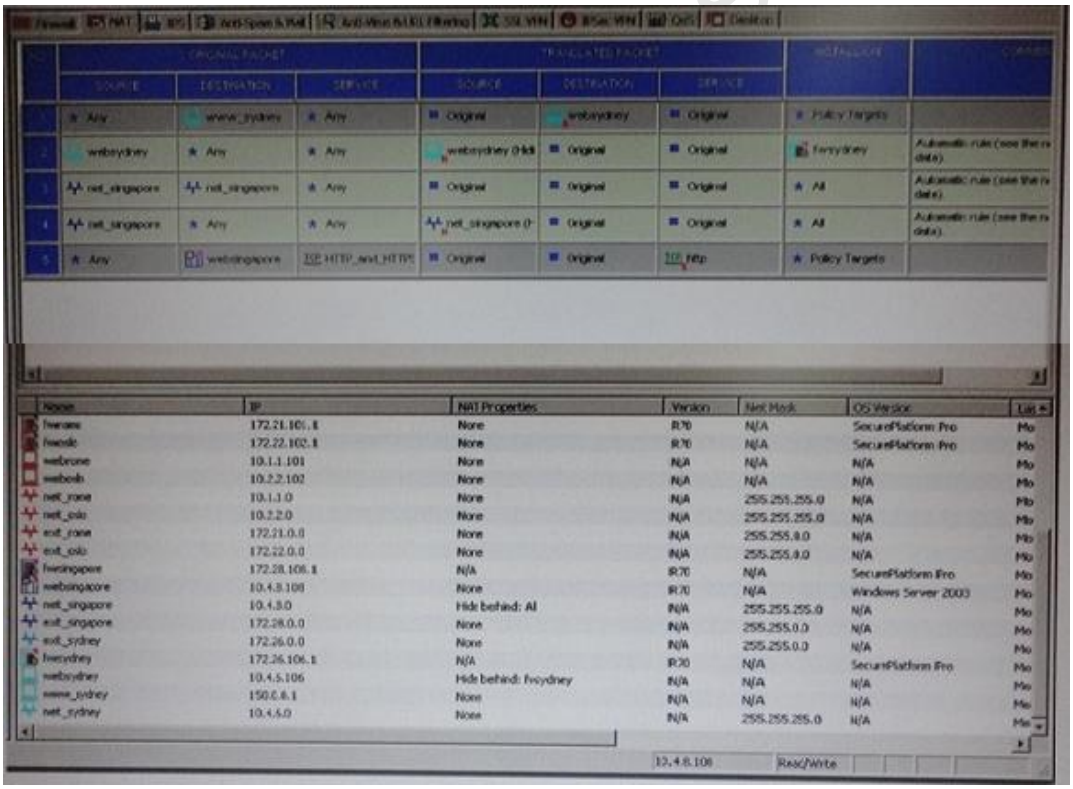
Which service is it NOT possible to configure user authentication?

A. HTTPS
B. FTP
C. SSH
D. Telnet

Answer: C
Explanation:

QUESTION NO: 19

You have created a rule Base Firewall, websydney. Now you are going to create a new policy package with security and address transaction rules for a secured gateway. What is true about the new package's NAT rules?



A. Rules 1 and 5 will be appear in the new package
B. Rules 1, 3.A and 5 will appear in the new package

C. Rules 2, 3 and 4 will appear in the new package
D. NAT rules will be empty in the new package

Answer: D
Explanation:

QUESTION NO: 20

You run cpconfig to reset SIC on the Security Gateway. After the SIC reset operation is complete, the policy that will be installed is the

A. Last policy that was installed
B. Default filter
C. Standard policy
D. Initial policy

Answer: D
Explanation:

QUESTION NO: 21

What can NOT be selected for VPN tunnel sharing?

A. One tunnel per subnet pair
B. One tunnel per Gateway pair
C. One tunnel per pair of hosts
D. One tunnel per VPN domain pair

Answer: D
Explanation:

QUESTION NO: 22

Which answers are TRUE? Automatic Static NAT CANNOT be used when:

i) NAT decision is based on the destination port

ii) Source and Destination IP both have to be translated

iii) The NAT rule should only be installed on a dedicated Gateway only

iv) NAT should be performed on the server side

A. (i), (ii), and (iii)
B. (i), and (ii)
C. ii) and (iv)
D. only (i)

Answer: A
Explanation:

QUESTION NO: 23

Security Gateway R71 supports User Authentication for which of the following services? Select the response below that contains the most complete list of supported services.

A. FTP, HTTP, TELNET
B. FTP, TELNET
C. SMTP, FTP, HTTP, TELNET
D. SMTP, FTP, TELNET

Answer: A
Explanation:

QUESTION NO: 24

Which of these security policy changes optimize Security Gateway performance?

A. Use Automatic NAT rules instead of Manual NAT rules whenever possible
B. Putting the least-used rule at the top of the Rule Base
C. Using groups within groups in the manual NAT Rule Base
D. Using domain objects in rules when possible

Answer: D
Explanation:

QUESTION NO: 25

A Web server behind the Security Gateway is set to Automatic Static NAT Client side NAT is not checked in the Global Properties. A client on the Internet initiates a session to the Web Server.

Assuming there is a rule allowing this traffic, what other configuration must be done to allow the traffic to reach the Web server?

A. Automatic ARP must be unchecked in the Global Properties.
B. A static route must be added on the Security Gateway to the internal host.
C. Nothing else must be configured.
D. A static route for the NAT IP must be added to the Gateway's upstream router.

Answer: A

Explanation:

QUESTION NO: 26

Latency has lost SIC communication with her Security Gateway and she needs to re establish SIC. What would be the correct order of steps needed to perform this task?

1) Create a new activation key on the Security Gateway, then exit cpconfig.

2) Click the Communication tab on the Security Gateway object, and then click Reset.

3) Run the cpconfig tool, and then select Secure Internal Communication to reset.

4) Input the new activation key in the Security Gateway object, and then click initialize

5) Run the cpconfig tool, then select source Internal Communication to reset.

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

Answer: A

Explanation:

QUESTION NO: 27

Which type of resource could a Security Administrator use to control access to specific share on target machines?

A. URI
B. CIFS

C. Telnet
D. FTP

Answer: B
Explanation:

QUESTION NO: 28

Which port must be allowed to pass through enforcement points in order to allow packet logging to operate correctly?

A. 514
B. 256
C. 257
D. 258

Answer: C
Explanation:

QUESTION NO: 29

While in Smart View Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 but cannot remember all the steps. What is the correct order of steps needed to perform this?

1) Select the Active Mode tab In Smart view Tracker

2) Select Tools > Block Intruder

3) Select the Log Viewing tab in SmartView Tracker

4) Set the Blocking Time out value to 60 minutes

5) Highlight the connection he wishes to block

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

Answer: C
Explanation:

QUESTION NO: 30

A rule _____ is designed to log and drop all other communication that does not match another rule?

A. Stealth
B. Cleanup
C. Reject
D. Anti-Spoofing

Answer: B
Explanation:

QUESTION NO: 31

Which the following statement is TRUE about management plug-ins?

A. The plug-in is a package installed on the Security Gateway
B. A management plug-in interacts with a Security Management Server to provide new features and support for new products
C. Using a plug m offers full central management only if special licensing is applied to specific features of the plug-in
D. Installing a management plug-in is just like an upgrade process (It overwrites existing components)

Answer: B
Explanation:

QUESTION NO: 32

For normal packet transaction of an accepted communication to a host protocol by a Security Gate Way how many lines per packet are recorded on a packet analyzer like wire Shark using fw monitor?

A. 2
B. 4
C. 3
D. None

Answer: B

Explanation:

QUESTION NO: 33

Your R71 enterprise Security Management Server is running abnormally on Windows 2003 Server. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings impact (i.e , all security policies database, SIC, licensing etc). What is the BEST method to reinstall the Server and keep its critical configuration?

A. 1) Run the latest upgrade_export utility to export the configuration
2) Leave the exported - tgz file in %FWDIR\bin.
3) Install the primary security Management Server on top of the current installation
4) Run upgrade_import to Import the configuration.
B. 1) Insert the R71 CD-ROM. and select the option to export the configuration into a . tgz file
2) Skip any upgrade verification warnings since you are not upgrading.
3) Transfer the. tgz file to another networked machine.
4) Download and run the cpclean utility and reboot.
5) Use the R71 CD_ROM to select the upgrade__import option to import the c
C. 1) Download the latest upgrade_export utility and run it from a \ temp directory to export the Configuration.
2) Perform any requested upgrade verification suggested steps.
3) Uninstall all R71 packages via Add/Remove Programs and reboot
4) Use smartUpdate to reinstall the Security Management server and reboot
5) Transfer the .tgz file back to the local \ temp.
6) Run upgrade_import to import the configuration.
D. 1) Download the latest upgrade_export utility and run it from a \ temp directory to export the Configuration.
2) Transferee .tgz file to another network machine
3) Uninstall all R71 packages via Add/Remove Programs and reboot
4) Install again using the R71 CD ROM as a primary security management server
5) Reboot and than transfer the .tgz file back to the local\ tem p
6) Run upgcade_import to import the configuration.

Answer: C

Explanation:

QUESTION NO: 34

Which of the following are authentication methods that Security Gateway R7Tuses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

A. Proxied, User, Dynamic, Session
B. Connection, User, Client
C. User, Client, Session
D. Connection, Proxied, Session

Answer: C
Explanation:

QUESTION NO: 35

Which Security Servers can perform authentication tasks, but CANNOT perform content security tasks?

A. HTTPS
B. Telnet
C. FTP
D. HTTP

Answer: B
Explanation:

QUESTION NO: 36

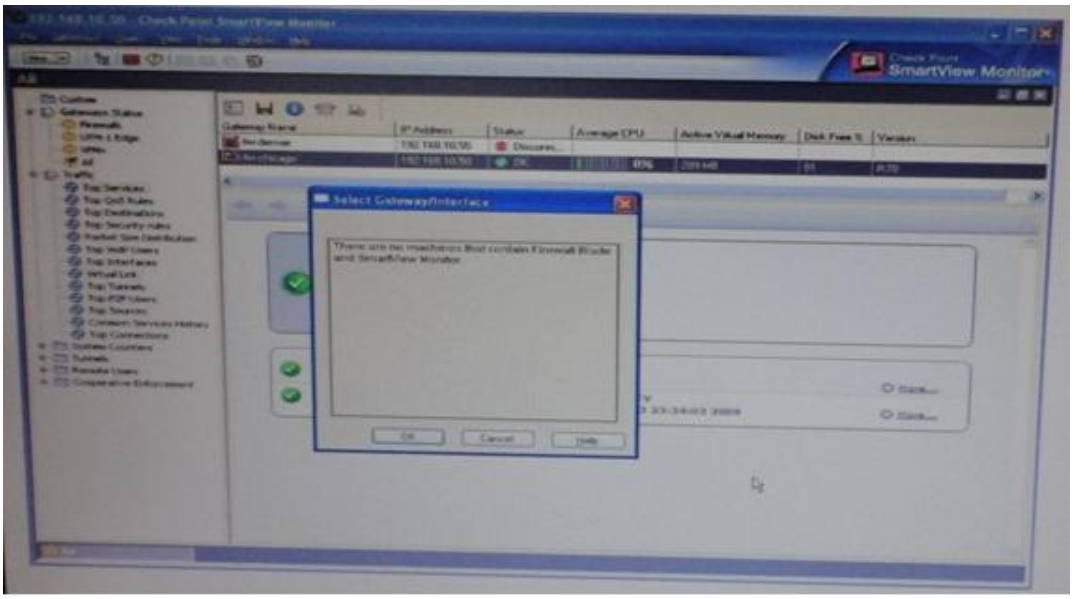
How would you create a temporary user bypass to the URL Filtering policy in Security Gateway?

A. By adding an exception in URL Filtering / Advanced I Network Exceptions
B. By enabling it in URL Filtering /Advanced / Bypass
C. By creating an authentication rule in the Firewall
D. It is not possible

Answer: A
Explanation:

QUESTION NO: 37

Cara wants to monitor the tap services on her Security Gateway (fw-chicago), but she is getting an error message. Other security gateways are reporting except a new security gateway just recently deployed. Analyze the error message from the out put below and determine what Care can do to correct the problem?



A. She should create a firewall rule to allow the CPMI traffic back to her Smart Console.
B. She should re-install the Security Policy on her Security Gateway since it was using the default rule Base.
C. She should edit the Security gateway object and enable the monitoring Software Blade.
D. She should let the monitoring run longer in order for it to collect sampled data.

Answer: C
Explanation:

QUESTION NO: 38

The Internal Certificate Authority (ICA) CANNOT be used for:

A. Virtual Private Network (VPN) Certificates for gateways
B. NAT rules
C. Remote-access users
D. SIC connections

Answer: B
Explanation:

QUESTION NO: 39

Which of the following commands can provide the most complete restore of an R71 configuration?

A. Cpconfig
B. Upgrade_import
C. fwm db_import -p <export file>
D. cpinfo -recover

Answer: B
Explanation:

QUESTION NO: 40

When using the Anti-Virus Content Security, how are different file types analyzed?

A. They are analyzed by their un-encoded format.
B. They are analyzed by their magic number.
C. They are analyzed by the MIME header.
D. They are analyzed by their file extension (i.e. .bat, .exe. .doc)

Answer: B
Explanation:

QUESTION NO: 41

Because of pre-existing design constraints, you set up manual NAT rules for HTTP server are both using automatic NAT rules. All traffic from your FTP and SMTP servers are passing through a Security Gateway Way without a problem, but traffic from the Web server is dropped on rule 0 because of anti-spoofing settings. What is causing this?

A. Allow bi-directional NAT is not checked in Global Properties.
B. Manual NAT rules are not configured correctly.
C. Translate destination on client side is not checked in Global Properties under manual NAT rules.
D. Routing is not configured correctly.

Answer: C
Explanation:

QUESTION NO: 42

You are creating an output file with the following command:

Fw monitor -e "accept (arc=10 . 20 . 30 . 40 or dst=10 , 20 , 30 - 40) ; " -o ~/output

Which tools do you use to analyze this file?

A. You can analyze it with Wireshark or Ethereal
B. You can analyze the output file with any ASCI editor.
C. The output file format is CSV. so you can use MS Excel to analyze it
D. You cannot analyze it with any tool as the syntax should be: fw monitor -e accept ([12, b] = 10.20.30.40 or [16, b]=10.20.30.40); -0 ~/output

Answer: A
Explanation:

QUESTION NO: 43

URL filtering policy can make exceptions for specific sites by being enforced:

A. Only for specific sources and destinations.
B. For all traffic, except on specific sources and destinations.
C. For alt traffic, except blocked sites.
D. For all traffic. There are no exceptions.

Answer: B
Explanation:

QUESTION NO: 44

When doing a stand-alone installation, you should install the security Management which other checkpoint architecture component?

A. Secure Client
B. Security Gateway
C. Smart Console
D. None, Security Management Server would install itself

Answer: B
Explanation:

QUESTION NO: 45

Which of the following is a hash algorithm?

A. DES
B. IDEA
C. MD5
D. 3DES

Answer: C
Explanation:

QUESTION NO: 46

Which component functions as the Internal Certificate Authority for R71?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: B
Explanation:

QUESTION NO: 47

The SIC certificate is stored in the_____ directory.

A. $FUIDIR/conf
B. $CPDIR/conf
C. $FWDIR/database
D. $CPDIR/registry

Answer: C
Explanation:

QUESTION NO: 48

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-

effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

A. SmartLSM and SmartUpdate
B. SmartView Tracker and SmartView Monitor
C. SmartView Monitor and SmartUpdate
D. SmartDashboard and SmartView Tracker

Answer: C
Explanation:

QUESTION NO: 49

When you hide a rule in a Rule Base, how can you then disable the rule?

A. Use the search utility in SmartDashboard to view all hidden rules Select the relevant rule and click Disable Rule(s).
B. Right-click on the hidden rule place-holder bar and select Disable Rule(s).
C. Right-click on the hidden rule place-holder bar and uncheck Hide, then right-click and select Disable Rule(s), re-hide the rule.
D. Hidden rules are already effectively disabled from Security Gateway enforcement.

Answer: C
Explanation:

QUESTION NO: 50

Which of the following can be found in cpinfo from an enforcement point?

A. The complete file objects_5_0. c
B. Policy file information specific to this enforcement point
C. Everything NOT contained in the file r2info
D. VPN keys for all established connections to all enforcement points

Answer: A
Explanation:

QUESTION NO: 51

Which antivirus scanning method does not work if the Gateway is connected as a node in proxy

mode?

A. Scan by Direction
B. Scan by File Type
C. Scan by Server
D. Scan by IP Address

Answer: A
Explanation:

QUESTION NO: 52

Which of the following is a CLI command for Security Gateway R71?

A. fwm policy_print <policyname>
B. fw shutdown
C. fw merge
D. fw tab –u

Answer: D
Explanation:

QUESTION NO: 53

You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify Security administration, which one of the following would you choose to do?

A. Create a separate Security Policy package for each remote Security Gateway.
B. Run separate SmartConsole instances to login and configure each Security Gateway directly.
C. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
D. Create network objects that restrict all applicable rules to only certain networks.

Answer: A
Explanation:

QUESTION NO: 54

The customer has a small Check Point installation which includes one Windows 2003 server as

the Smart Console and a second server running secure Platform as both Security Management Server and the Security Gateway. This is an example of a (n):

A. Unsupported configuration.
B. Hybrid Installation.
C. Distributed Installation.
D. Stand-Alone Installation.

Answer: C
Explanation:

QUESTION NO: 55

Which set of objects have an Authentication tab?

A. Networks. Hosts
B. Users, Networks
C. Users, User Groups
D. Templates, Users

Answer: C
Explanation:

QUESTION NO: 56

Which operating system is NOT supported by Endpoint Connect R71?

A. MacOS X
B. Windows XP SP2 O C.
C. Windows Vista 64-bit SP1
D. Windows 2000 SP1

Answer: D
Explanation:

QUESTION NO: 57

Security Servers can perform authentication tasks, but CANNOT perform content security tasks?

A. RHV HTTPS
B. FTP
C. RLOGIN
D. HTTP

Answer: C
Explanation:

QUESTION NO: 58

When launching SmartDashboard, what information is required to log into R7?

A. User Name, Management Server IP, certificate fingerprint file
B. User Name, Password. Management Server IP
C. Password. Management Server IP
D. Password, Management Server IP, LDAP Server IP

Answer: B
Explanation:

QUESTION NO: 59

SmartView Tracker R71 consists of three different modes. They are

A. Log, Active, and Audit
B. Log, Active, and Management
C. Log, Track, and Management
D. Network & Endpoint, Active, and Management

Answer: D
Explanation:

QUESTION NO: 60

Can you upgrade a clustered deployment with zero downtime?

A. No, this is not possible.
B. Yes, if you select the option zero downtime, it will keep one member active
C. No, you must bring all gateways down.

D. Yes, this is the default setting.

Answer: B

Explanation:

QUESTION NO: 61

What action CANNOT be run from SmartUpdate R71?

A. Get all Gateway Data
B. Fetch sync status
C. Reboot Gateway
D. Preinstall verifier

Answer: D

Explanation:

QUESTION NO: 62

When john first installed the system, he forgot to configure DNS server security Gateway. How could john configure DNS servers now that his security gateway is in production?

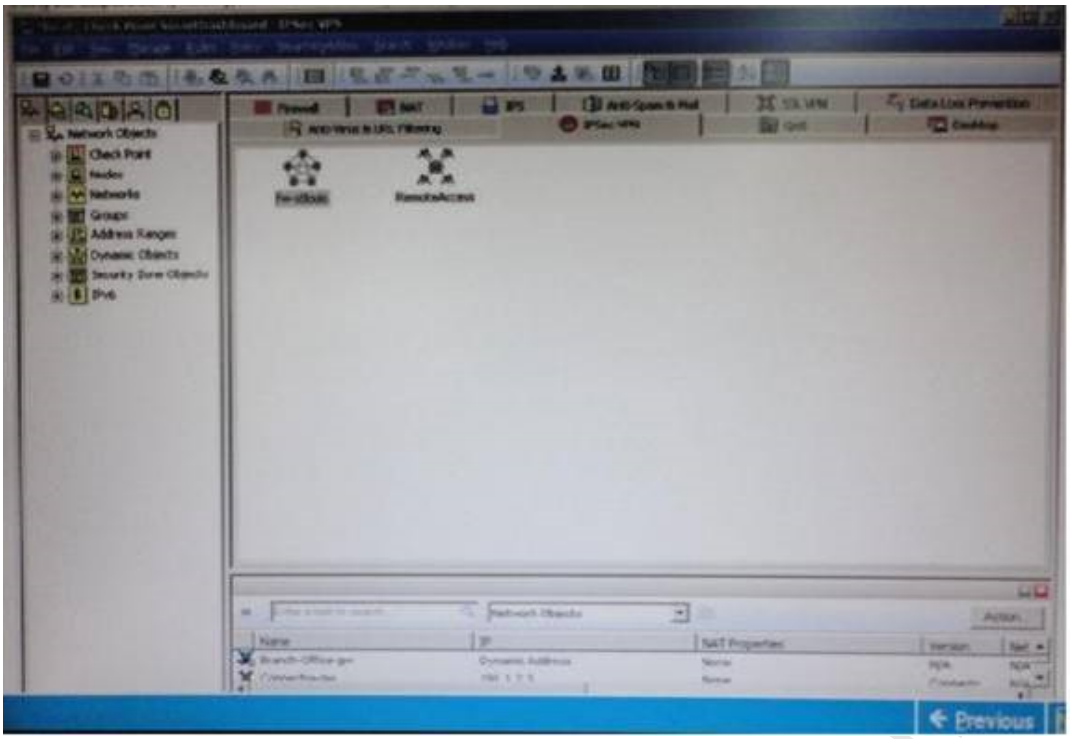
A. Login to the firewall using SSH and run cpconfig, then select Domain Name Servers.
B. Login to the firewall using SSH and run fwm, then select System Configuration and Domain Name Servers.
C. Login to the SmartDashboard, edit the firewall Gateway object, and select the tab Interface, than domain name servers.
D. Login to the firewall using SSH and run aysconfig, then select Domain Name Servers.

Answer: D

Explanation:

QUESTION NO: 63

Using the out put below, what type of VPN is configured for fw-stlouis?



A. Traditional
B. Meshed
C. Domain-Based
D. Star

Answer: B
Explanation:

QUESTION NO: 64

A clean up rule is used to:

A. Drop without logging connections that would otherwise be dropped and logged fry default
B. Log connections that would otherwise be accepted without logging by default.
C. Log connections that would otherwise be dropped without logging by default.
D. Drop without logging connections that would otherwise be accepted and logged by default

Answer: C
Explanation:

QUESTION NO: 65

When check point translation method allows an administrator to use fewer ISP-assigned IP

addresses then the number of internal hosts requiring internet connectivity?

A. Static Destination
B. Hide
C. Dynamic Destination
D. Static Source

Answer: B
Explanation:

QUESTION NO: 66

Your bank's distributed R71 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartView Tracker
B. Smart Portal
C. SmartUpdate
D. SmartDashboard

Answer: B
Explanation:

QUESTION NO: 67

If you were NOT using IKE aggressive mode for your IPsec tunnel, how many packets would you see for normal Phase 1 exchange?

A. 6
B. 2
C. 3
D. 9

Answer: A
Explanation:

QUESTION NO: 68

Identify the correct step performed by SmartUpdate a remote Security Gateway. After selecting packages Select / Add from CD, the:

A. entire contents of the CD-ROM arc copied to the packages directory on the selected remote Security Gateway
B. selected package is copied to the Package Repository on the Security Management: Server
C. entire contents of the CD-ROM are copied to the Package Repository on the Security Management Server
D. selected package is copied to the packages directory on the selected remote Security Gateway

Answer: B
Explanation:

QUESTION NO: 69

You are reviving the security administrator activity for a bank and comparing it to the change log. How do you view Security Administrator activity?

A. SmartView Tracker cannot display Security Administrator activity: instead, view the system logs on the Security Management Server's Operating System
B. SmartView Tracker in Management Mode
C. SmartView Tracker in Active Mode
D. SmartView Tracker in Network and Endpoint Mode

Answer: D
Explanation:

QUESTION NO: 70

You would use the Hide Rule feature to:

A. Make rules invisible to incoming packets.
B. View only a few rules without the distraction of others
C. Hide rules from read-only administrators.
D. Hide rules from a SYN/ACK attack.

Answer: A
Explanation:

QUESTION NO: 71

Which of the following methods will provide the most complete backup of an R71 configuration?

A. Policy Package Management
B. Copying the $PWDIR\conf and $CPDIR\conf directories to another server
C. upgrade_export command
D. Database Revision Control

Answer: B

Explanation:

QUESTION NO: 72

To monitor all traffic between a network and the internet on a Security Platform Gateway, what is the best utility to use?

A. Snoop
B. Cpinfo
C. Infoview
D. Tcpdump

Answer: D

Explanation:

QUESTION NO: 73

Where are automatic NAT rules added to the Rule Base?

A. Before last
B. Middle
C. First
D. Last

Answer: D

Explanation:

QUESTION NO: 74

Which R71 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

A. SmartView Status
B. SmartView Monitor
C. None, SmartConsole applications only communicate with the Security Management Server.
D. SmartUpdate

Answer: C

Explanation:

QUESTION NO: 75

You are responsible for configuration of Meg a Corn's Check Point Firewall. You need to allow two NAT rules to match a connection. Is it possible? Give the best answer

A. Yes. it is possible to have two NAT rules which match a connection, but only when using Automatic NAT(bidirectional NAT)
B. No, it is not possible to have more one NAT rule matching a connection. When the firewall receives a packet belonging to a concentration, it compares it against the first rule in the Rule Base, then the second rule, and so on When it finds a rule that matches, it stops checking and applies that rule.
C. Yes, it is possible to have two NAT rules which match a connection, but only in using Manual NAT (bidirectional NAT)
D. Yes, there are always as many active NAT rules as there are connections.

Answer: D

Explanation:

QUESTION NO: 76

On of your licenses is set for an IP address no longer in use. What happens to this license during the licenser-upgrade process?

A. It is upgraded with new available features but the IP remains the same
B. It remains untouched.
C. It is upgraded with the previous features using the new IP address
D. It is dropped

Answer: A

Explanation:

QUESTION NO: 77

External commands can be included in SmartView Tracker via the menu Tools / Custom commands. The security management server is running under SecurePlatform, and the GUI is on a system running Microsoft Windows. How do you run the command trecert.exe to the list?

A. Use the program GUI dbedit to add the command trace route to the properties of the security management Server.
B. Go to the menu Tools I Custom Commands and configure the Windows command trecert.exe to the list.
C. There is no possibility to expand the three pre-defined options ping, whois, and nslookup.
D. Go to the menu. Tools / Custom Commands and configure the Linux command trace route to the list.

Answer: B
Explanation:

QUESTION NO: 78

What is used to validate a digital certificate?

A. IPsec
B. CRL
C. S/MIME
D. PKCS

Answer: C
Explanation:

QUESTION NO: 79

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R71 Security Gateway to a partner site. Rules for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every one minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a policy install).

If your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets every minute interval.

If GRE encapsulation is turned off on the router. SmartView Tracker shows a log entry for the UDP keep-alive packet every minute. Which of the following is the BEST explanation for this behavior?

A. The Log Server log unification process unifies all log entries from the Security Gateway on specific connection into only one log entry in the SmartView Tracker. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged. connection at the beginning of the day
B. The Log Server is failing to log GRE traffic property because it is VPN traffic. Disable all VPN configurations to the partner site to enable proper logging.
C. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt. Because it is encrypted, the R71 Security Gateway cannot distinguish between GRE sessions. This is a known issue with the GRE. Use IPSEC instead of the non GRE protocol for encapsulation.
D. The setting Log does not capture this level of details for GRE Set the rule tracking a action to audit since certain types of traffic can only tracked this way.

Answer: A
Explanation:

QUESTION NO: 80

Which do you configure to give remote access VPN users a local IP address?

A. Office mode IP pool
B. NAT pool
C. Encryption domain pool
D. Authentication pool

Answer: A
Explanation:

QUESTION NO: 81

You need to plan the company's new security system. The company needs a very high level of security and also high performance and high through put for their applications. You need to turn on most of the integrated IPS checks while maintain high throughput. What would be the best solution for this scenario?

A. The IPS does not run when Core XL is enabled
B. You need to buy a strong multi-core machine and run R71 or later on Secure Platform with

CoreXL technology enabled.
C. The IPS system does not affect the firewall performance and CoreXL is not needed in this scenario.
D. Bad luck, both together can not be achieved.

Answer: B
Explanation:

QUESTION NO: 82

Which can an administrator configure the notification action of a policy install time change?

A. SmartView Tracker I Audit Log
B. SmartView Monitor/ Gateways I Thresholds Settings
C. SmartDashboard / Security Gateway Object I Advanced Properties Tail
D. SmartDashboard / Policy Package Manager

Answer: B
Explanation:

QUESTION NO: 83

You intend to upgrade a Check Point Gateway from R65 to R71. Prior to upgrading, you want to backup the gateway should there be any problems with the upgrade of the following allows for the gateway configuration to be completely backup into a manageable size in the least amount of time?

A. Backup
B. Snapshot
C. Upgrade_export
D. Database_revision

Answer: B
Explanation:

QUESTION NO: 84

Which of the following describes the default behavior of an R71 Security Gateway?

A. Traffic is filtered using controlled port scanning.
B. All traffic is expressly permitted via explicit rules.
C. Traffic not explicitly permitted is dropped.
D. IP protocol types listed as secure are allowed by default, i.e ICMP, TCP, UDP sessions are inspected.

Answer: C
Explanation:

QUESTION NO: 85

Which R71 GUI would you use to see the number of packets accepted since the last policy install?

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

Answer: C
Explanation:

QUESTION NO: 86

A digital signature:

A. Provides a secure key exchange mechanism over the Internet
B. Automatically exchanges shared keys.
C. Guarantees the authenticity and integrity of a message.
D. Decrypts data to its original form.

Answer: A
Explanation:

QUESTION NO: 87

Which of the following statements accurately describes the upgrade_export command?

A. Upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included before exporting.

B. Used when upgrading the Security Gateway, upgrade_export includes modified files directory.
C. Upgrade_export stores network-configuration data, objects, global properties, and the data base revisions prior to upgrading the security Management Server.
D. Used primarily when upgrading the Security Management Server. Upgrade_export stores all object database and the conf directions for importing to a newer version of the Security Gateway.

Answer: A

Explanation:

QUESTION NO: 88

What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security gateway?

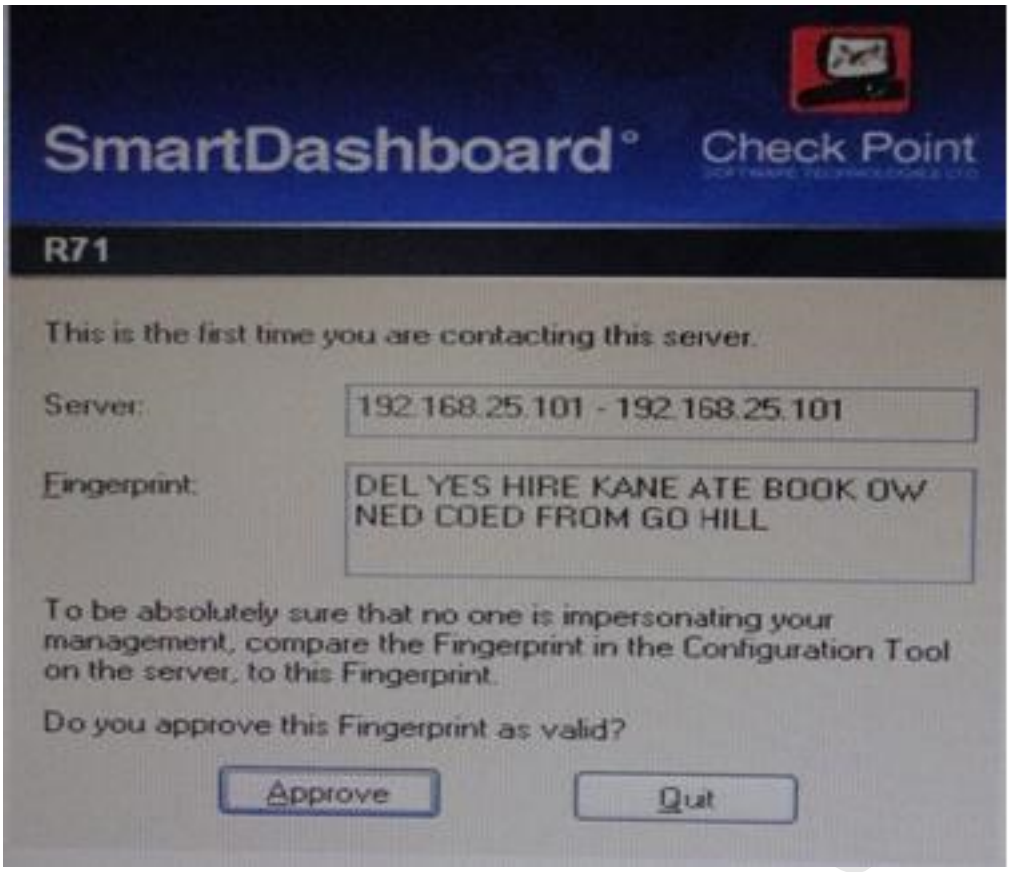
A. Install the View Implicit Rules package using SmartUpdate.
B. In Global Properties / Reporting Tools check the box Enable tracking all rules (including rules marked as none in the track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.
C. Check the Log Implied Rules Globally box on the R71 Gateway object.
D. Define two log servers on the R71 Gateway object. Enable Log Implied Rules on the first log server. Enable log rule Base on the second log server. Use Smart Reporter to merge the two log server records into the same database for HIPPA log audits.

Answer: B

Explanation:

QUESTION NO: 89

From the output below, where is the fingerprint generated?



A. SmartUpdate
B. Security Management Server
C. SmartDashboard
D. SmartConsole

Answer: B

Explanation:

QUESTION NO: 90

Which of the following statements BEST describes Check Point's Hide Network Checkpoints Address Translation method?

A. Translates many source IP addresses into one source IP address
B. Many-to-one NAT which implements PAT (Port Address Translation) for accomplishing both secure and destination IP address translation.
C. Translates many destination IP addresses into one destination IP address
D. One-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Secure and Destination IUP address translation.

Answer: A

Explanation:

QUESTION NO: 91

How can you reset the password of the Security Administrator that was created during initial installation of the security management sever on Secure Platform?

A. Type fwm -a, and provide the existing administrator's account name. Reset the Security administrator's password.
B. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the password portion of the file. Then log in to the account without a password You will be prompted to assign a new password.
C. Type cpm -a, and provide the existing administrator's account name. Reset the Security administrator's password.
D. Launch SmartDashboard in the User Management screen, and edit the cpconfig administrator.

Answer: D
Explanation:

QUESTION NO: 92

Match each of the following command to there correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy packages.
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in cpconfig to SmartDashboard.

A. C1>F2, C2>F1, C3>F6, C4>F4
B. C1>F6, C2>F4, C3>F2, C4>F5
C. C1>F2, C4>F4, C3>F1, C4>F5
D. C1>F4, C2>F6, C3>F3, C4>F2

Answer: B

Explanation:

QUESTION NO: 93

Which of the following statement about bridge mode is TRUE?

A. When managing a Security Gateway m Bridge mode. It is possible to use a bridge interlace for Network Address Translation
B. Assuming a new installation, bridge mode requires changing the existing IP routing of the network
C. All ClusterXL modes arc supported
D. A bridge must be configured with a pair of interfaces.

Answer: D

Explanation:

QUESTION NO: 94

Beginning with R71 Software Blades was introduced. One of the Software Blades is the IPS Software Blade as a replacement for Smart Defense. When buyers are upgrading to a bundle, some blades are included, e.g. FW, VPN, IPS in SG103. Which statement is NOT true?

A. The license price includes IPS Updates for the first year.
B. The IPS Software Blade can be used for an unlimited time.
C. There is no need to renew the service contract after one year.
D. After one year, it is mandatory to renew the service contract for the IPS Software Blade because it has been bundled with the license when perchased.

Answer: D

Explanation:

QUESTION NO: 95

What is the desired outcome when running the command op info - z -o cpinfo -out?

A. Send output to a file called cpinfo. out in compressed format
B. Send output to a file called cpinfo. out in usable format for the CP Info View utility IOC.
C. Send output to a file called cpinfo. out without address resolution.

D. Send output to a file called cpinfo. out and provide a screen print at the same time

Answer: A

Explanation:

QUESTION NO: 96

Which of the following are available SmartConsole clients which can be installed from the R71 windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker. CPINFO. SmartUpdate
B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
C. SmartView Tracker. SmartDashboard, CPINFO. SmartUpdate, SmartView Status
D. Security Policy Editor, Log Viewer. Real Time Monitor GUI

Answer: B

Explanation:

QUESTION NO: 97

Antivirus protection on a checkpoint gateway is available for all of the following protocols, EXCEPT:

A. FTP
B. SMTP
C. HTTP
D. TELNET

Answer: D

Explanation:

QUESTION NO: 98

Message digests use which of the following?

A. SHA-1 and MD5
B. IDEA and RC4
C. SSL and MD4
D. DES and RC4

Answer: A
Explanation:

QUESTION NO: 99

Which fw monitor utility would be best to troubleshoot which of the following problems?

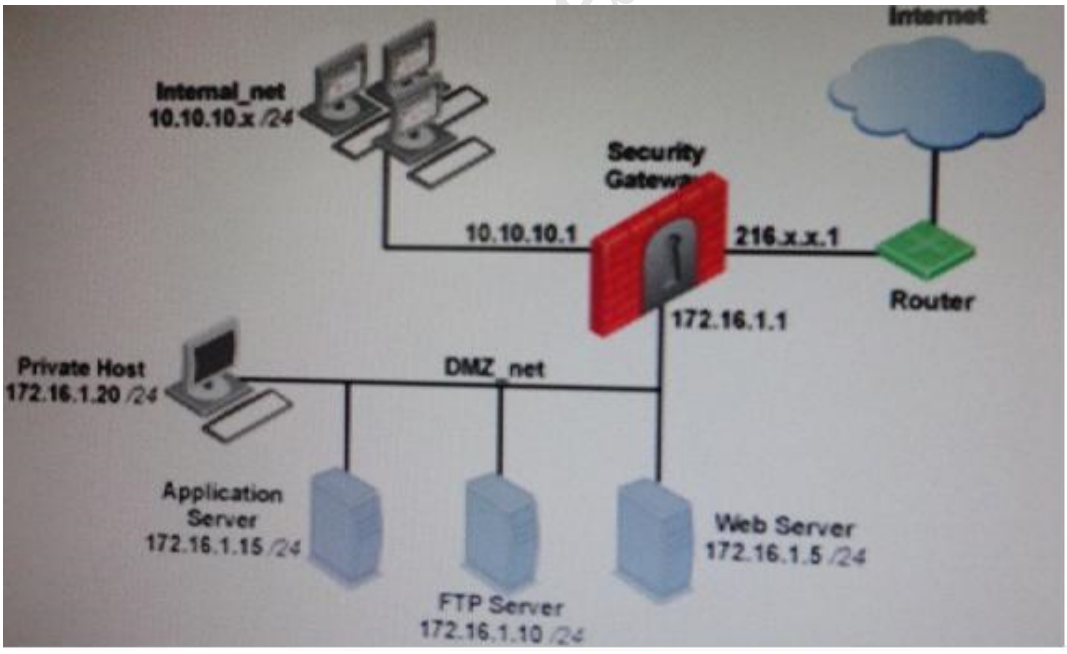
A. An error occurs when editing a network object in SmartDashboard
B. A statically NATed Web server behind a Security Gateway cannot be reached from the Internet
C. You get an invalid ID error in SmartView Tracker for phase 2 IKE key negotiations.
D. A user in the user database is corrupt.

Answer: B
Explanation:

QUESTION NO: 100

You have three servers located in DMZ address. You want internal users from 10.10.10x10 to access the DMZ servers by public IP addresses. Internet.net 10.10.10xis configured for the NAT behind the security gateway external interface.

What is the best configuration for 10.10.10xusers to access the DMZ servers, using the DMZ server public IP address?



A. When connecting to the Internet, configure manual Static NAT rules to translate the DMZ

servers
B. When the source is the internal network 10.10.10xt configure manual static NAT rules to translate the DMZ servers
C. When connecting to internal network 10 10.10 x. configure Hide NAT for the DMZ servers.
D. When connecting to the internal network 10.10.10x, configure Hide Nat for the DMZ network behind the DMZ interface of the Security Gateway

Answer: A
Explanation:

QUESTION NO: 101

What information is found in the SmartView Tracker Management log?

A. Rule author
B. TCP handshake average duration
C. TCP source port
D. Top used QOS rule

Answer: A
Explanation:

QUESTION NO: 102

If you run fw monitor without any parameters, what does the output display?

A. In /var/adm/monitor. Out
B. On the console
C. In /tmp/log/monitor – out
D. In / var/log/monitor. out

Answer: A
Explanation:

QUESTION NO: 103

Which statement defines Public Key Infrastructure? Security is provided:

A. By authentication

B. By Certificate Authorities, digital certificates, and two-way symmetric- key encryption
C. By Certificate Authorities, digital certificates, and public key encryption.
D. Via both private and public keys, without the use of digital Certificates.

Answer: D
Explanation:

QUESTION NO: 104

As a Security Administrator, you are required to create users for authentication. When you create a user for user authentication, the data is stored in the _____.

A. SmartUpdate repository
B. User Database
C. Rules Database
D. Objects Database

Answer: B
Explanation:

QUESTION NO: 105

Why are certificates preferred over pre-shared keys in an IPsec VPN?

A. Weak scalability: PSKs need to be set on each and every Gateway
B. Weak performance: PSK takes more time to encrypt than Drffie-Hellman
C. Weak security: PSKs can only have 112 bit length.
D. Weak Security. PSK are static and can be brute-forced

Answer: D
Explanation:

QUESTION NO: 106

If you are experiencing LDAP issues, which of the following should you check?

A. Domain name resolution
B. Overlapping VPN Domains
C. Secure Internal Communications (SIC)

D. Connectivity between the R71 Gateway and LDAP server

Answer: D
Explanation:

QUESTION NO: 107

Jeff wanted to upgrade his Security Gateway to R71, but he remembers that he needs to have a contract file from the user centre before he can start the upgrade. If Jeff wants to download the contracts file from the User Center, what is the correct order of steps needed to perform this?

1) Select Update Contracts from User Center.

2) Enter your Username for your User Center account.

3) Enter your Password for your User Center account.

4) Click the Browse button to specify the path to your download contracts file.

5) Enter your Username and Password for your Security Gateway.

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

Answer: A
Explanation:

QUESTION NO: 108

Choose the BEST sequence for configuring user management in SmartDashboard, Using an LDAP server.

A. Enable LDAP in Global Properties; configure a host-node object for the LDAP server, a Unit.
B. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.

Answer: B
Explanation:

QUESTION NO: 109

You have configured automatic static NAT on an internal host-node object. You clear the box Translate destination on client site from global properties Nat. assuming all other settings on all properties are selected, what else must be configured so that a host on internet can initiate an inbound connection to this host.

A. A static route to ensure packets destined for the public NAT IP address will reach the Gateway's internal interface.
B. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface.
C. The NAT IP address must be added to the anti-spoofing group of the external gateway interface
D. No extra configuration is needed

Answer: B
Explanation:

QUESTION NO: 110

Which VPN Community object is used to configure Hub Mode VPN routing in SmartDashboard?

A. Mesh
B. Star
C. Routed
D. Remote Access

Answer: B
Explanation:

QUESTION NO: 111

You have blocked an IP address via the Block Intruder feature of SmartView Tracker How can you view the blocked addresses'?

A. Run f wm blockedview.
B. In SmartView Monitor, select the Blocked Intruder option from the query tree view
C. In SmartView Monitor, select Suspicious Activity Rules from the Tools menu and select the relevant Security Gateway from the list
D. In SmartView Tracker, click the Active tab. and the actively blocked connections displays

Answer: C
Explanation:

QUESTION NO: 112

John is the Security Administrator in his company He installs a new R71 Security Management Server and a new R71 Gateway He now wants to establish SIC between them. After entering the activation key, the message "Trust established" is displayed in SmartDashboard, but SIC still does not seem to work because the policy won't install and interface fetching still does not work. What might be a reason for this?

A. This must be a human error.
B. The Gateway's time is several days or weeks in the future and the SIC certificate is not yet valid.
C. SIC does not function over the network.
D. It always works when the trust is established.

Answer: B
Explanation:

QUESTION NO: 113

What are you required to do before running upgrade__ export?

A. Run cpconfig and set yourself up as a GUI client.
B. Run a cpstop on the Security Management Server
C. Run a cpstop on the Security Gateway.
D. Close all GUI clients

Answer: B,C,D
Explanation:

QUESTION NO: 114

You are installing a Security Management Server Your security plan calls for three administrators for this particular server. How many can you create during installation'?

A. Depends on the license installed on the Security Management Server
B. Only one with full access and one with read-only access
C. One
D. As many as you want

Answer: C

Explanation:

QUESTION NO: 115

You are installing your R71Security Gateway. Which is NOT a valid option for the hardware platform?

A. Crossbeam
B. Solaris
C. Windows
D. IPSO

Answer: B

Explanation:

QUESTION NO: 116

A Security Policy installed by another Security Administrator has blocked all SmartDashboard connections to the stand-alone installation of R71. After running the fw unloadlocal command, you are able to reconnect with SmartDashboard and view all changes. Which of the following change is the most likely cause of the block?

A. A Stealth Rule has been configured for the R71 Gateway.
B. The Allow control connections setting in Policy > Global Properties has been unchecked.
C. The Security Policy installed to the Gateway had no rules in it
D. The Gateway Object representing your Gateway was configured as an Externally Managed VPN Gateway.

Answer: B

Explanation:

QUESTION NO: 117

In previous version, the full TCP three-way handshake was sent to the firewall kernel for inspection. How is this improved in current Flows/SecureXL?

A. Only the initial SYN packet is inspected The rest are handled by IPSO
B. Packets are offloaded to a third-party hardware card for near-line inspection

C. Packets are virtualized to a RAM drive-based FW VM
D. Resources are proactively assigned using predictive algorithmic techniques

Answer: A
Explanation:

QUESTION NO: 118

Which command displays the installed Security Gateway version?

A. fw stat
B. cpstat -gw
C. fw ver
D. tw printver

Answer: C
Explanation:

QUESTION NO: 119

What is a Consolidation Policy?

A. The collective name of the Security Policy, Address Translation, and IPS Policies.
B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
C. The collective name of the logs generated by SmartReporter.
D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Answer: B
Explanation:

QUESTION NO: 120

What CANNOT be configured for existing connections during a policy install?

A. Keep all connections
B. Keep data connections
C. Reset all connections
D. Re-match connections

Answer: C
Explanation:

QUESTION NO: 121

Which OPSEC server can be used to prevent users from accessing certain Web sites?

A. LEA
B. AMON
C. UFP
D. CVP

Answer: C
Explanation:

QUESTION NO: 122

Assume an intruder has compromised your current IKE Phase 1 and Phase 2 keys. Which of the following options will end the intruder's access after the next Phase 2 exchange occurs?

A. Perfect Forward Secrecy
B. SHA1 Hash Completion
C. Phase 3 Key Revocation
D. M05 Hash Completion

Answer: A
Explanation:

QUESTION NO: 123

You are trying to save a custom log query in R71 SmartView Tracker, but getting the following error "Could not save 'query-name' (Error Database is Read only).

Which of the following is a likely explanation for this?

A. You have read-only rights to the Security Management Server database.
B. You do not have the explicit right to save a custom query in your administrator permission profile under SmartConsole customization
C. You do not have OS write permissions on the local SmartView Tracker PC in order to save the custom query locally
D. Another administrator is currently connected to the Security Management Server with read/write

permissions which impacts your ability to save custom log queries to the Security Management Server.

Answer: A

Explanation:

QUESTION NO: 124

Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services. The Gateway does not allow the Telnet service to itself from any location. How would you configure authentication on the Gateway? With a:

A. Client Authentication for fully automatic sign on
B. Client Authentication rule using the manual sign-on method, using HTTP on port 900
C. Client Authentication rule, using partially automatic sign on
D. Session Authentication rule

Answer: B

Explanation:

QUESTION NO: 125

In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port_____.

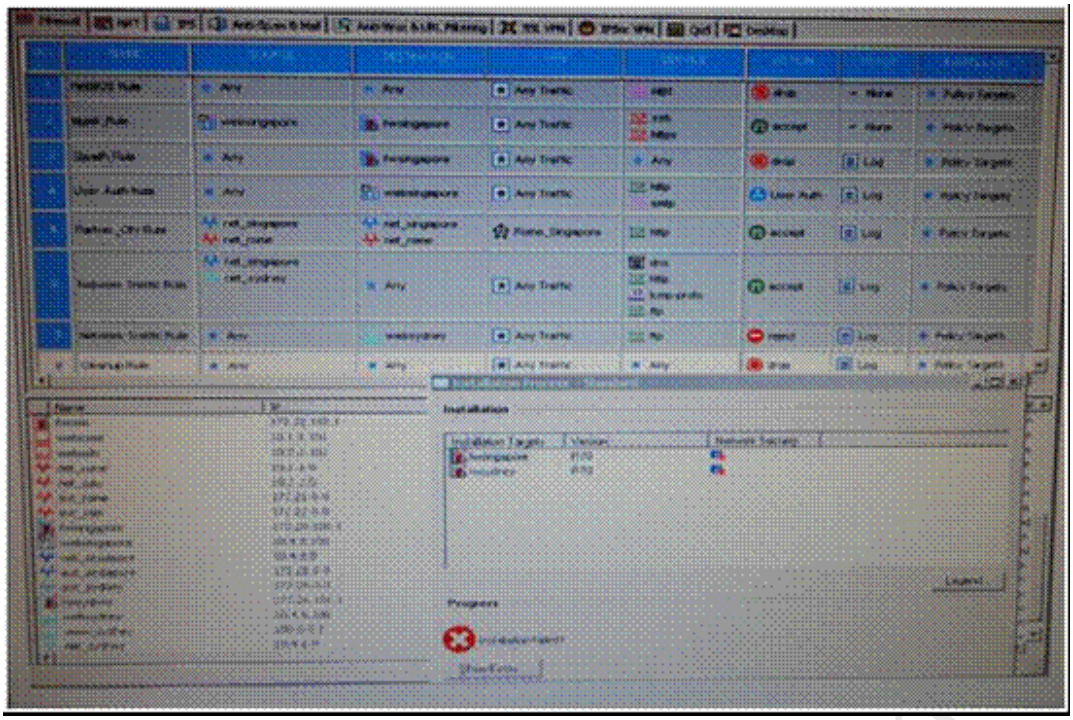
A. 256
B. 80
C. 900
D. 259

Answer: A

Explanation:

QUESTION NO: 126

Which rule is responsible for the installation failure?



A. Rule 4
B. Rule 3
C. Rule 5
D. Rule 6

Answer: A
Explanation:

QUESTION NO: 127

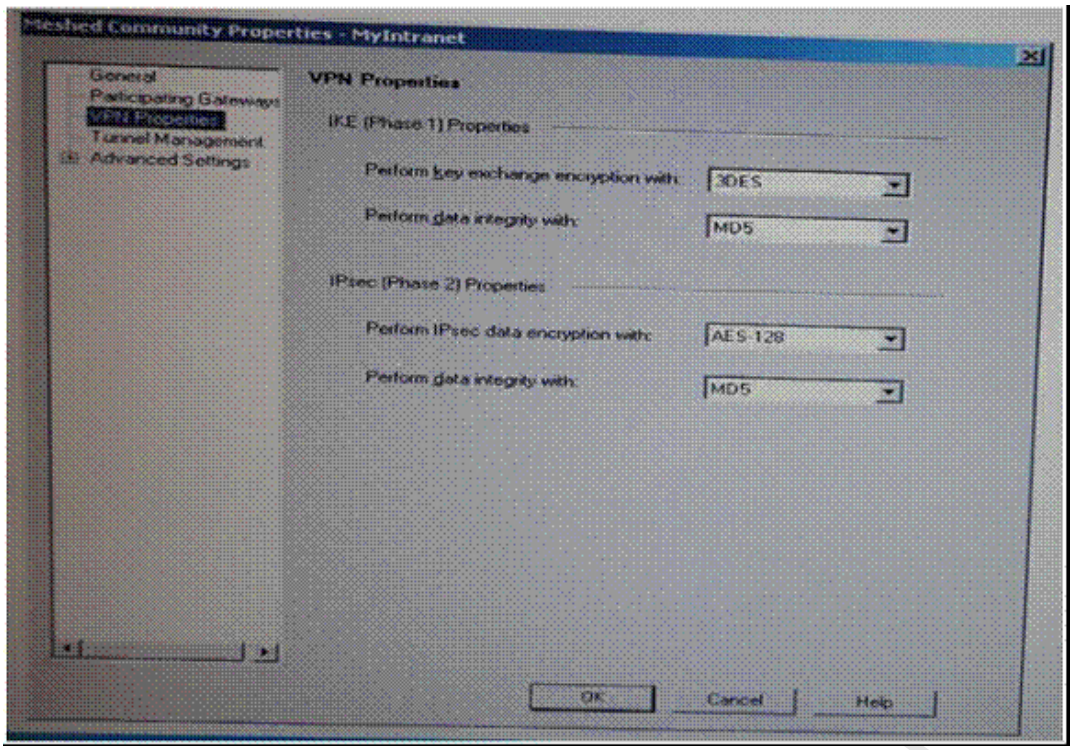
If you experience unwanted traffic from a specific IP address, how can you stop it most quickly?

A. Check anti-spoofing settings
B. Configure a rule to block the address
C. Create a SAM rule
D. Activate an IPS protection

Answer: C
Explanation:

QUESTION NO: 128

You are evaluating the configuration of a mesh VPN Community used to create a site-to-site VPN. This graphic displays the VPN properties in this mesh Community



Which of the following would be a valid conclusion?

A. The VPN Community will perform IKE Phase 1 key-exchange encryption using the longest key Security Gateway R71 supports.
B. Changing the setting Perform IPsec data encryption with from AES-128 to 3DES will increase the encryption overhead.
C. Changing the setting Perform key exchange encryption with 3DES to DES will enhance the VPN Community's security, and reduce encryption overhead.
D. Change the data-integrity settings for this VPN CommunitybecauseMD5 is incompatible with AES.

Answer: A
Explanation:

QUESTION NO: 129

You just installed a new Web server in the DMZ that must be reachable from the Internet You create a manual Static NAT rule as follows:

Source:	Any
Destination:	web_public_IP
Service:	Any
Translated Source:	original
Translated Destination:	web_private_IP
Service:	original

“web_publicIP" is the node Object that represents the public IP address of the new Web server. "web_privateIP" is the node object that represents the new Web site's private P address You enable all settings from Global Properties > NAT.

When you try to browse the Web server from the Internet, you see the error 'page cannot be displayed" Which of the following is NOT a possible reason?

A. There is no route defined on the Security Gateway for the public IP address to the private IP address of the Web server.
B. There is no Security Policy defined that allows HTTP traffic to the protected Web server.
C. There is an ARP entry on the Gateway but the settings Merge Manual proxy ARP and Automatic ARP configuration are enabled in Global Properties. The Security Gateway ignores manual ARP entries.
D. There is no ARP table entry for the public IP address of the protected Web server

Answer: A
Explanation:

QUESTION NO: 130

Which of the following SSL Network Extender server-side prerequisites is NOT correct?

A. The Gateway must be configured to work with Visitor Mode.
B. There are distinctly separate access rules required for SecureClient users vs. SSL Network Extender users.

C. To use Integrity Clientless Security (ICS), you must install the IC3 server or configuration tool.
D. The specific Security Gateway must be configured as a member of the Remote Access Community

Answer: B
Explanation:

QUESTION NO: 131

You need to determine if your company's Web servers are accessed an excessive number of times from the same host. How would you configure this in the IPS tab?

A. Successive multiple connections
B. Successive alerts
C. Successive DoS attacks
D. HTTP protocol inspection

Answer: A
Explanation:

QUESTION NO: 132

What does it indicate when a Check Point product name includes the word "SMART"?

A. Stateful Management of all Routed Traffic.
B. This Check Point product is a GUI Client.
C. Security Management Architecture.
D. The Check Point product includes Artificial Intelligence.

Answer: C
Explanation:

QUESTION NO: 133

How many times is the firewall kernel invoked for a packet to be passed through a VPN connection?

A. Three times
B. Twice

C. Once
D. None The IPSO kernel handles it

Answer: C
Explanation:

QUESTION NO: 134

When attempting to connect with SecureClient Mobile the following error message is received. The certificate provided is invalid. Please provide the username and password.

What is the probable cause of the error?

A. The certificate provided is invalid.
B. The user's credentials are invalid.
C. The user attempting to connect is not configured to have an office mode IP address so the connection failed.
D. There is no connection to the server, and the client disconnected.

Answer: A
Explanation:

QUESTION NO: 135

The fw stat -l command includes all of the following except:

A. The number of packets that have been inspected
B. The date and time of the policy that is installed.
C. The number of times the policy has been installed
D. The number of packets that have been dropped

Answer: A
Explanation:

QUESTION NO: 136

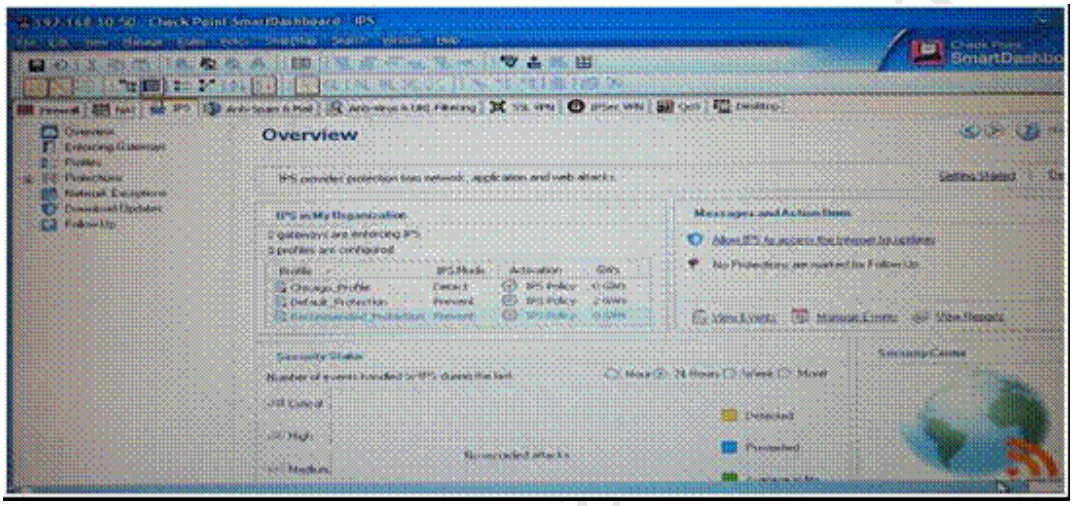
Although SIC was already established and running, Joe reset SIC between the Security Management Server and a remote Gateway. He set a new activation key on the Gateway's side with the cpconfig command and put in the same activation key in the Gateway's object on the Security Management Server Unfortunately SIC cannot be established. What is a possible reason for the problem?

A. The installed policy blocks the communication.
B. Joe forgot to reboot the Gateway.
C. Joe forgot to exit from cpconfig.
D. The old Gateway object should have been deleted and recreated.

Answer: C
Explanation:

QUESTION NO: 137

The TotallyCoolSecurity Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-chicago using Detect mode. After reviewing logs, Matt noticed that fw-chicago is not detecting any of the IPS protections that Bob had previously setup. Analyze the output below and determine how can correct the problem.



A. Matt should re-create the Chicago_Profile and select Activate protections manually Instead of per the IPS Policy
B. Matt should activate the Chicago_Profile as it is currently not activated
C. Matt should assign the fw-chicago Security Gateway to the Chicago_Profile
D. Matt should change the Chicago_Profile to use Protect mode because Detect mode will not work.

Answer: C
Explanation:

QUESTION NO: 138

Which statement below describes the most correct strategy for implementing a Rule Base?

A. Add the Stealth Rule before the last rule.
B. Umit grouping to rules regarding specific access.
C. Place the most frequently used rules at the top of the Policy and the ones that are not frequently used further down.
D. Place a network-traffic rule above the administrator access rule.

Answer: C
Explanation:

QUESTION NO: 139

An Administrator without access to SmartDashboard installed a new IPSO-based R71 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. You first need to create a new UTM-1 Gateway object, establish SIC via the Communication button, and define the Gateway's topology.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server You must initialize SIC on the Security Management Server.
C. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway appliance Resolve by running the tw unloadlocal command on the local Security Gateway.
D. You first need to run the fw unloadlocal command on the R71 Security Gateway appliance in order to remove the restrictive default policy.

Answer: B
Explanation:

QUESTION NO: 140

Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. diag
B. cpinfo -o date.cpinfo.txt
C. netstat > date.netstat.txt
D. cpstat > date.cpatat.txt

Answer: B
Explanation:

QUESTION NO: 141

R71's INSPECT Engine inserts itself into the kernel between which tow layers of the OSI model?

A. Physical and Data
B. Session and Transport
C. Presentation and Application
D. Data and Network

Answer: C
Explanation:

QUESTION NO: 142

After filtering a fw monitor trace by port and IP, a packet is displayed three times; in the “I”, “I”, and 'o' inspection points, but not in the 'O' inspection. Which is the likely source of the issue?

A. The packet has been sent out through a VPN tunnel unencrypted.
B. An IPSO ACL has blocked the outbound passage of the packet.
C. A SmartDefense module has blocked the packet
D. It is an issue with NAT

Answer: D
Explanation:

QUESTION NO: 143

Your company has two headquarters, one in London, and one in New York Each office includes several branch offices. The branch offices need to rate with the headquarters in their country, not with each other, and only the headquarters need to communicate directly. What is the BEST configuration for establishing VPN Communities for this company? VPN Communities comprised of:

A. Two star and one mesh Community: One star Community is set up for each site, with headquarters as the center of the Community and its branches as satellites The mesh Community includes only New York and London Gateways.
B. One star Community with the option to "mesh" the center of the star: New York and London Gateways added to the center of the star with the mesh canter Gateways option checked, all London branch offices defined m one satellite window, but all New York branch offices defined m another satellite window.
C. Two mesh and one star Community One mesh Community is set up for each of the

headquarters and its branch offices The star Community is configured with London as the center of the Community and New York is the satellite.
D. Three mesh Communities: One for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.

Answer: A
Explanation:

QUESTION NO: 144

How can you configure an application to automatically launch on the Security Management Server when traffic is dropped Security Policy?

A. Pop-up alert script
B. User-defined alert script
C. Custom scripts cannot be executed through alert scripts
D. SNMP trap alert script

Answer: B
Explanation:

QUESTION NO: 145

The command fw fetch causes the:

A. Security Management Server to retrieve the IP addresses of the target Security Gateway.
B. Security Gateway to retrieve the compiled policy and inspect code from the Security Management Server and install it to the kernel
C. Security Gateway to retrieve the user database information from the tables on the Security Management Server
D. Security Management Server to retrieve the debug logs of the target Security Gateway

Answer: B
Explanation:

QUESTION NO: 146

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credential. What must happen after authentication that

allows the client to connect to the Security Gateway's VPN domain?

A. Active-X must be allowed on the client.
B. An office mode address must be obtained by the client.
C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
D. The SNX client application must be installed on the client.

Answer: A
Explanation:

QUESTION NO: 147

Which authentication type requires specifying a contact agent in the Rule Base?

A. Client Authentication with Partially Automatic Sign On
B. User Authentication
C. Session Authentication
D. Client Authentication with Manual Sign On

Answer: C
Explanation:

QUESTION NO: 148

You find a suspicious FTP connection trying to connect to one of your internal hosts. How do you block it m real time and verify it is successfully blocked?

A. Highlight the suspicious connection in SmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection is listed in this SmartView Tracker view as "dropped".
B. Highlight the suspicious connection in SmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection does not appear again in this SmartView Tracker view.
C. Highlight the suspicious connection in SmartView Tracker > Log mode. Block it using Tools > Block Intruder menu. Observe in the Log mode that the suspicious connection does not appear again in this SmartView Tracker view.
D. Highlight the suspicious connection in SmartView Tracker > Log mode. Block it using Tools > Block Intruder menu. Observe in the Log mode that the suspicious connection is listed in this SmartView Tracker view as "dropped".

Answer: B
Explanation:

QUESTION NO: 149

Your network includes a SecurePlatform machine running NG with Application Intelligence (Al) R55. This configuration acts as both the primary Security Management Server and VPN-1 Pro Gateway. You add one machine, so you can implement Security Gateway R71 in a distributed environment. The new machine is an Intel CoreDuo processor, with 2 GB RAM and a 500-GB hard drive. How do you use these two machines to successfully migrate the NG with Al R55 configuration?

A. 1. On the existing machine, export the NG with AJ R55 configuration to a network share.
2. Insert the R71 CD-ROM in the old machine Install the R7D Security Gateway only while reinstalling the SecurePlatform OS over the top of the existing installation. Complete sysconfig.
3. On the new machine, install SecurePlatform as the primary Security Management Server only.
4. Transfer the exported. tgz file into the new machine, import the configuration, and then reboot
5. Open SmartDashboard, change the Gateway object to the new version, and reset SIC for the Gateway object.
B. 1. Export the configuration on the existing machine to a tape drive
2. Uninstall the Security Management Server from the existing machine, using sysconfig.
3. Insert the R71 CD-ROM. run the patch add CD-ROM command to upgrade the existing machine to the R71 Security Gateway, and reboot
4. Install a new primary Security Management Server on the new machine
5. Change the Gateway object to the new version, and reset SIC
C. 1. Export the configuration on the existing machine to a network share
2. Uninstall the Security Gateway from the existing machine, using sysconfig
3. Insert the R71 CD ROM. and run the patch add CD-HGM command to upgrade the Security Management Server to Security Gateway R 70
4. Select upgrade with imported file, and reboot
5. Install a new R71 Security Gateway as the only module on the new machine, and reset SIC to the new Gateway
D. 1. Export the configuration on the existing machine as a backup only
2. Edit $FWDIR\product. conf on the existing machine, to disable the VPN-1 Pro Gateway package
3. Reboot the existing machine
4. Perform an in place upgrade on the Security Management Server using the command "patch odd cd"
5. On the new machine, install SecurePlatform as the R71 Security Gateway only
6. Run sysconfig to complete the configuration
7. From SmartDashboard, reconfigure the Gateway object to the new version, and reset SIC

Answer: A

Explanation:

QUESTION NO: 150

How can you access the Certificate Revocation List (CRL) on the firewall, if you have configured a Stealth Rule as the first explicit rule?

A. You can access the Revocation list by means of a browser using the URL: <https: //IP-FW: 18264/ICA_CRLI.crl> provided the implied rules are activated per default
B. The CRL is encrypted, so it is useless to attempt to access it.
C. You cannot access the CRL, since the Stealth Rule will drop the packets
D. You can only access the CRI via the Security Management Server as the internal CA is located on that server

Answer: A
Explanation:

QUESTION NO: 151

What port is used for communication to the User Center with SmartUpdate?

A. CPMI200
B. HTTPS443
C. HTTP 80
D. TCP 8080

Answer: B
Explanation:

QUESTION NO: 152

You are the Security Administrator in a large company called ABC. A Check Point Firewall is installed and in use on SecurePlatform. You are concerned that the system might not be retaining your entries for the interface and routing configuration. You would like to verify your entries in the corresponding file(s) on SecurePlatform. Where can you view them? Give the BEST answer.

A. /etc/conf/route.C
B. /etc/sysconfig/netconf.C
C. /etc/sysconfig/network-scripts/ifcfg-ethx
D. /etc/sysconfig/network

Answer: B
Explanation:

QUESTION NO: 153

You are Security Administrator preparing to deploy a new HFA (HOTfix Accumulator) to ten Security Gateways at five geographically separate locations.

What is the BEST method to implement this HFA?

A. Send a Certified Security Engineer to each site to perform the update.
B. Use SmartUpdate to install the packages to each of the Security Gateways remotely
C. Use a SSH connection to SCP the HFA to each Security Gateway. Once copied locally, imitate a remote installation command and monitor the installation progress with SmartView Monitor
D. Send a CD-ROM with the HFA to each location and have local personnel install it.

Answer: B
Explanation:

QUESTION NO: 154

You want to generate a cpinfo file via CLI on a system running SecurePlatform. This will take about 40 minutes since the log files are also needed. What action do you need to take regarding timeout?

A. Log in as the default user expert and start cpinfo.
B. No action is needed because cpshell has a timeout of one hour by default.
C. Log in as Administrator, set the timeout to one hour with the command idle 60 and start cpinfo.
D. Log in as admin, switch to expert mode, set the timeout to one hour with the command, idle 60, then start cpinto.

Answer: C
Explanation:

QUESTION NO: 155

Which feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

A. Policy Package management
B. dbexport/dbimport
C. Database Revision Control
D. upgrade_export/upgrade_import

Answer: C

Explanation:

QUESTION NO: 156

Your Gateways are running near performance capacity and will get upgraded hardware next week. Which of the following would be MOST effective for quickly dropping all connections from a specific attacker's IP at a peak time of day?

A. SAM - Block Intruder feature of SmartView Tracker
B. Intrusion Detection System (IDS) Policy install
C. SAM - Suspicious Activity Rules feature of SmartView Monitor
D. Change the Rule Base and install the Policy to all Security Gateways

Answer: C

Explanation:

QUESTION NO: 157

Which of the following statements about the Port Scanning feature of IPS is TRUE?

A. The default scan detection is when more than 500 open inactive ports are open for a period of 120 seconds
B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. Port Scanning does not block scanning; it detects port scans with one of three levels of detection sensitivity.
D. When a port scan is detected, only a log is issued, never an alert

Answer: C

Explanation:

QUESTION NO: 158

Certificates for Security Gateways are created during a simple initialization from_____.

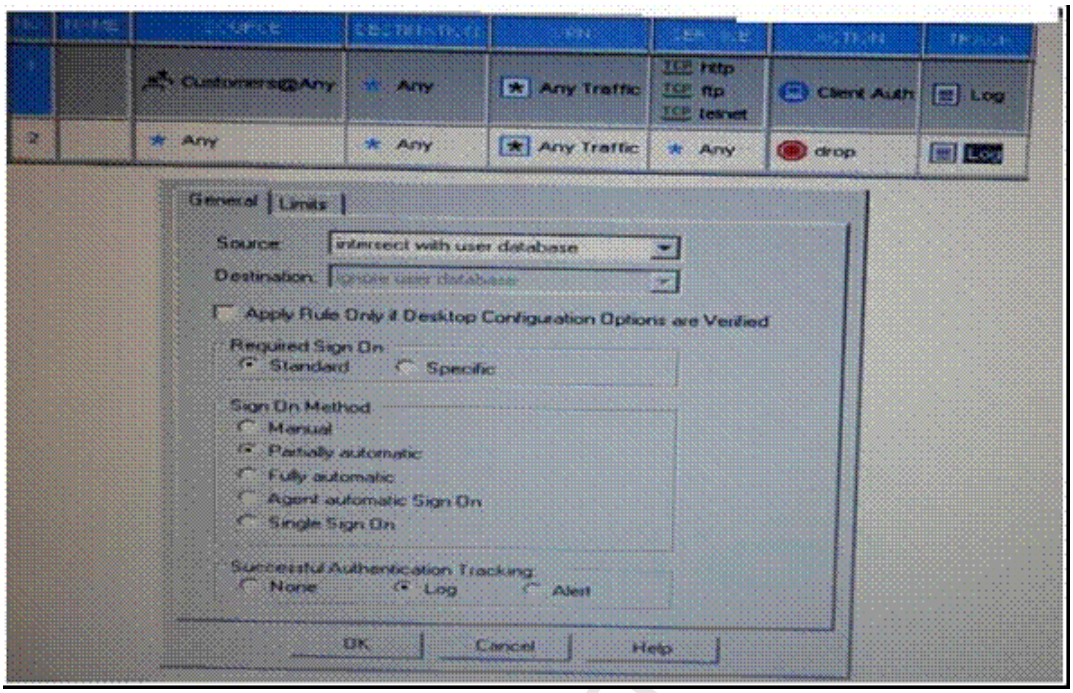
A. SmartUpdate
B. sysconfig
C. The ICA management tool.
D. SmartDashboard

Answer: D

Explanation:

QUESTION NO: 159

Reviews the following rules and note the Client Authentication Action properties screen, as shown below:



After being authenticated by the Security Gateway, when a user starts an HTTP connection to a Web site, the user tries to FTP to another site using the command line. What happens to the user? The:

A. User is prompted from that FPT site only, and does not need to enter his user name and password for Client Authentication.
B. User is prompted for Authentication by the Security Gateway again.
C. FTP data connection is dropped after the user is authenticated successfully.
D. FTP connection is dropped by rules 2.

Answer: A

Explanation:

QUESTION NO: 160

A Web server behind the Security Gateway is set 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 occurs on which inspection point?

A. I B. O
B. o
C. i

Answer: B
Explanation:

QUESTION NO: 161

Which of the following statements about file-type recognition in Content Inspection is TRUE?

A. Antivirus status is monitored using SrnartView Tracker.
B. A scan failure will only occur if the antivirus engine fails to initialize.
C. All file types are considered "at risk", and are not configurable by the Administrator or the Security Policy.
D. The antivirus engine acts as a proxy, caching the scanned file before delivering it to the client.

Answer: D
Explanation:

QUESTION NO: 162

Which Security Gateway R71 configuration setting forces the Client Authentication authorization time-out to refresh, each time a new user is authenticated? The:

A. Global Properties > Authentication parameters, adjusted to allow for Regular Client Refreshment
B. Time properties, adjusted on the user objects for each user, in the source of the Client Authentication rule
C. IPS > Application Intelligence > Client Authentication > Refresh User Timeout option enabled
D. Refreshable Timeout setting, in the Limits tab of the Client Authentication Action Properties screen

Answer: D
Explanation:

QUESTION NO: 163

What information is found in the SmartView Tracker Management log?

A. Most accessed Rule Base rule
B. Number of concurrent IKE negotiations
C. SIC revoke certificate event
D. Destination IP address

Answer: C
Explanation:

QUESTION NO: 164

When configuring objects in SmartMap, it helps if you_____ the objects so that they may be used in a policy rule.

A. Expand
B. Actualize
C. Physically connect to
D. Save

Answer: B
Explanation:

QUESTION NO: 165

You have included the Cleanup Rule in your Rule Base. Where in the Rule Base should the Accept ICMP Requests implied rule have no effect?

A. First
B. Before Last
C. Last
D. After Stealth Rule

Answer: C
Explanation:

QUESTION NO: 166

Your organization’s disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R71 installation. Your plan must meet the following required and desired objectives:

Required Objective: The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired Objective: The R71 components that enforce the Security Polices should be blocked up at least once a week.

Desired Objective: Back up R71 logs at least once a week

Your disaster recovery plan is as follows:

Use the cron utility to run the upgrade_ export command each night on the Security Management Servers.

Configure the organization's routine backup software to back up the files created by the upgrade_ export command.

Configure the SecurePlatform backup utility to back up the Security Gateways every Saturday night

Use the cron utility to run the upgrade export: command each Saturday niqht on the log servers

Configure an automatic, nightly loqswitch

Configure the organization's routine backup software to back up the switched logs every night

Upon evaluation, your plan:

A. Meets the required objective but does not meet either desired objective.
B. Does not meet the required objective.
C. Meets the required objective and only one desired objective.
D. Meets the required objective and both desired objectives.

Answer: D
Explanation:

QUESTION NO: 167

Your Rule Base includes a Client Authentication rule, using partial authentication and standard sign-on for HTTP, Telnet, and FTP services. The rule was working, until this morning. Now users are not prompted for authentication, and they see error "page cannot be displayed" in the browser. In SmartView Tracker, you discover the HTTP connection is dropped when the Gateway is the destination. What caused Client Authentication to fail?

A. You added a rule below the Client Authentication rule, blocking HTTP from the internal network.

B. You added the Stealth Rule before the Client Authentication rule.
C. You disabled R71 Control Connections in Global Properties.
D. You enabled Static NAT on the problematic machines.

Answer: B
Explanation:

QUESTION NO: 168

Which SmartConsole component can Administrators use to track remote administrative activities?

A. WebUI
B. Eventia Reporter
C. SmartView Monitor
D. SmartView Tracker

Answer: D
Explanation:

QUESTION NO: 169

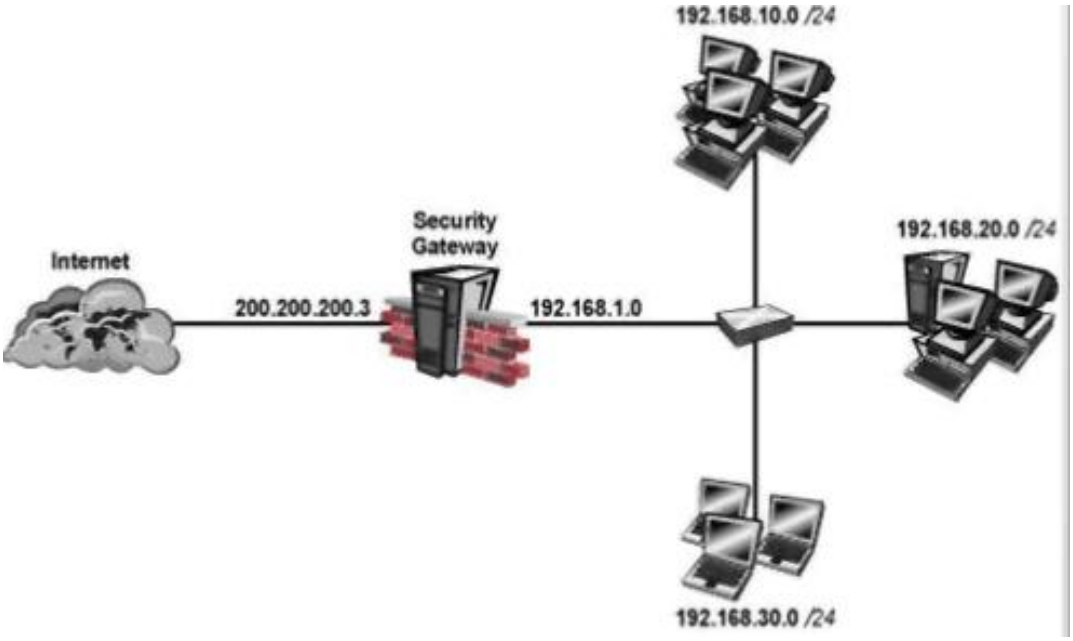
Which of the following statements regarding SecureXL and CoreXL is TRUE?

A. SecureXL is an application for accelerating connections.
B. CoreXL enables multi-core processing for program interfaces.
C. SecureXL is only available in R71.
D. CoreXL is included in SecureXL.

Answer: A
Explanation:

QUESTION NO: 170

Your perimeter Security Gateway's external IP is 200 200.200.3. Your network diagram shows:



Required: Allow only network 192.168.10.0 and 192.168.20.0 to go out to the Internet, using 200. 200.200.5.

The local network 192.168.1.0/24 needs to use 200.200.200.3 to go out to the Internet.

Assuming you enable all the settings in the NAT page of Global Properties, how could you achieve these requirements?

A. Create a network object 192.168.0.0/16. Enable Hide NAT on the NAT page. Enter 200.200.200.5 as the hiding IP address. Add and ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
B. Create network objects for 192.168.10.0/24 and 192.168.20.0/24. Enable Hide NAT on both network objects, using 200.200.200.5 as hiding IP address Add an ARP entry for 200.200.200.3 for the MAC address of 200.200.200.5.
C. Create an address Range object, starting from 192.168.10.1 to 192.168.20.254. Enable Hide NAT page of the address range object. Enter Hiding IP address 200.200.200.5. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
D. Create two network objects: 192.168.10.0/24. and 192.168.20.0/24. Add the two network objects. Create a manual NAT rule like the following Original source –group object; Destination – any Service – any, Translated source – 200.200.200.5; Destination – original, Service – original.

Answer: C
Explanation:

QUESTION NO: 171

During which step in the installation process is it necessary to note the fingerprint for first-time verification?

A. When establishing SIC between the Security Management Server and the Gateway
B. When configuring the Security Management Server using cpconfig
C. When configuring the Security Gateway object in SmartDashboard
D. When configuring the Gateway in the WebUI

Answer: B
Explanation:

QUESTION NO: 172

What's the difference between the SmartView Tracker Tool section in R71 and NGX R65?

A. Tools section in R71 is exactly the same as the tools section in R65
B. Using R71. You can choose a program to view captured packets.
C. Enable Warning Dialogs option is not available in R71
D. R71 adds a new option to send ICMP packets to the source/destination address of the log event

Answer: B
Explanation:

QUESTION NO: 173

Your organization has many Edge Gateways at various branch offices allowing users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the Edge Gateways first be inspected by your headquarters' R71 Security Gateway. How do you configure VPN routing in this star VPN Community?

A. To Internet and other targets only
B. To center or through the center to other satellites, to Internet and other VPN targets
C. To center and other satellites, through center
D. To center only

Answer: B
Explanation:

QUESTION NO: 174

Several Security Policies can be used for different installation targets. The firewall protecting Human Resources' servers should have a unique Policy Package. These rules may only be installed on this machine and not accidentally on the Internet firewall. How can this be configured?

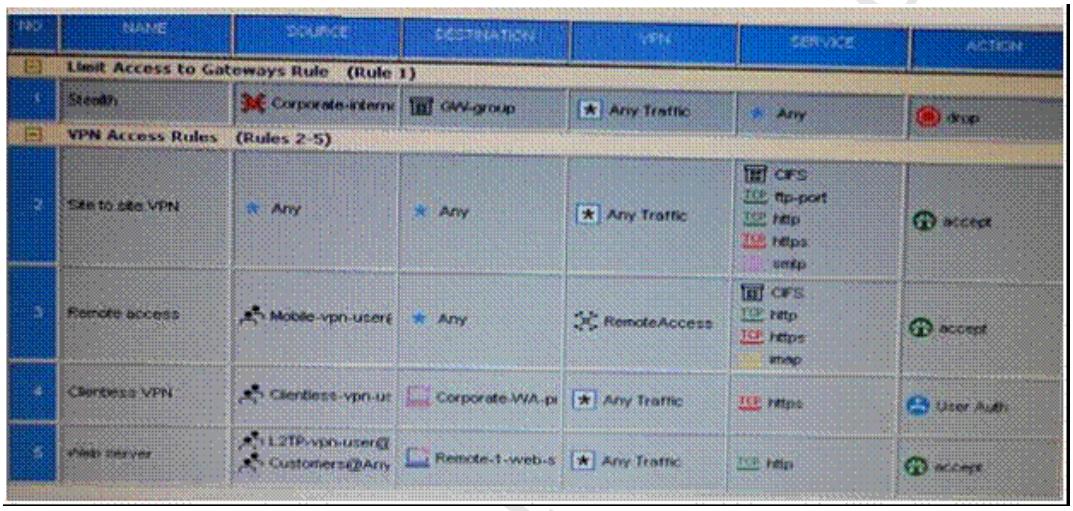
A. A Rule Base is always installed on all possible targets. The rules to be installed on a firewall are defined by the selection in the row Install On of the Rule Base.
B. When selecting the correct firewall in each line of the row Install On of the Rule Base, only this firewall is shown in the list of possible installation targets after selecting Policy > Install.
C. In the SmartDashboard main menu go to Policy > Policy Installation > Targets and select the correct firewall to be put into the list via Specific Targets
D. A Rule Base can always be installed on any Check Point firewall object It is necessary to select the appropriate target directly after selecting Policy > Install.

Answer: C

Explanation:

QUESTION NO: 175

Examine the following Security Policy. What, if any, changes could be made to accommodate Rule 4?



A. Nothing at all
B. Modify the Source 01 Destination columns in Rule 4
C. Remove the service HTTPS from the Service column in Rule A
D. Modify the VPN column in Rule 2 to limit access to specific traffic

Answer: D

Explanation:

QUESTION NO: 176

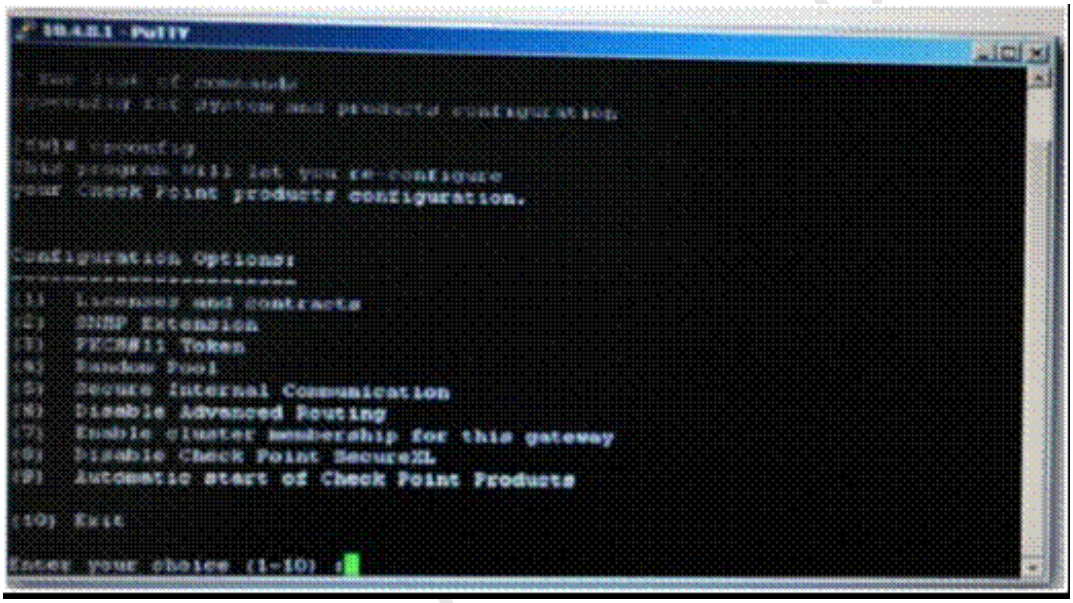
After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your DMZ, you notice that any NATed connections to that machine are being dropped by anti-spoofing protections. Which of the following is the MOST LIKELY cause?

A. The Global Properties setting Translate destination on client side is checked. But the topology on the external interface is set to External.Change topology to Others +.
B. The Global Properties setting Translate destination on client side is unchecked. But the topology on the external interface is set to Others +. Change topology to External
C. The Global Properties setting Translate destination on client side is checked But the topology on the DMZ interface is set to Internal -Network defined by IP and Mask Uncheck the Global Properties setting Translate destination on client side
D. The Global Properties setting Translate destination on client side is unchecked But the topology on the DMZ interface is set to Internal -Network defined by IP and Mask Check the Global Properties setting Translate destination on client side.

Answer: D
Explanation:

QUESTION NO: 177

What information is provided from the options in this screenshot?



(i)Whether a SIC certificate was generated for the Gateway

(ii)Whether the operating system is SecurePlatform or SecurePlatform Pro

(iii)Whether this is a standalone or distributed installation

A. (i), (ii) and (iii)
B. (i) and (iii)
C. (i) and (ii)
D. (ii) and (iii)

Answer: D
Explanation:

QUESTION NO: 178

Which type of R71 Security Server does not provide User Authentication?

A. FTP Security Server
B. SMTP Security Server
C. HTTP Security Server
D. HTTPS Security Server

Answer: B
Explanation:

QUESTION NO: 179

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 R71
D. You must enable state synchronization
E. You must install R71 as an enforcement module (only) on each node

Answer: B,C,D,E
Explanation:

QUESTION NO: 180

Using the Backup and Restore operation on R71, it is possible to:

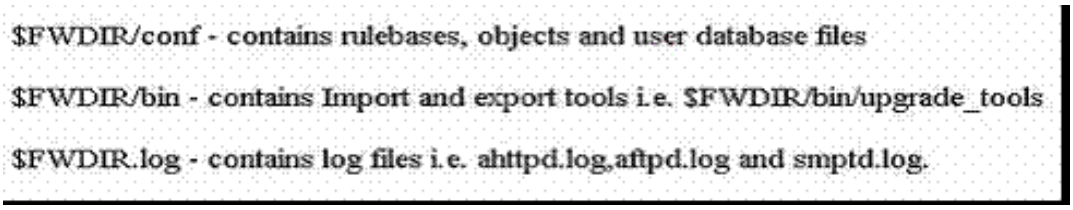
A. Link the all cluster members for failover
B. Upgrade the SmartDashboard
C. Maintain a backup of the SmartCenter Management Server to be used in case of failover
D. Replace the original SmartCenter Management Server with another clone SmartCenter Management Server, while the original is being serviced
E. Upgrade the SmartCenter Management Server

Answer: C,D,E

Explanation:

QUESTION NO: 181

What directory in R71 contains all of the Rule Bases, objects, and the user database files?



A. $FWDIR/bin directory
B. Winnt/Config directory
C. $FWDIR/etc directory
D. $FWDIR/conf directory
E. $FWDIR/bin/etc directory

Answer: D
Explanation:

QUESTION NO: 182

Platforms IP290, IP390 and IP560 are flash-based, diskless platforms. And what do you have to do prior to upgrading their images to R71?

A. Backup old images
B. Do nothing
C. Delete old images
D. Backup their images
E. Restore old images

Answer: C
Explanation:

QUESTION NO: 183

You have not performed software upgrade to NGX R71. 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
Explanation:

QUESTION NO: 184

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. R71 is not running on the system you are adding
C. The IP address should be the real IP address of a cluster interface
D. R71 is running on the system you are adding
E. The existing nodes must be running R71 and firewall monitoring is enabled on them

Answer: B,E
Explanation:

QUESTION NO: 185

When carrying out a backup operation on R71, 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
Explanation:

QUESTION NO: 186

Which tool will you use prior to installation to reduce the risk of incompatibility with the deployment to R71?

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

Answer: D
Explanation:

QUESTION NO: 187

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
Explanation:

QUESTION NO: 188

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

Explanation:

QUESTION NO: 189

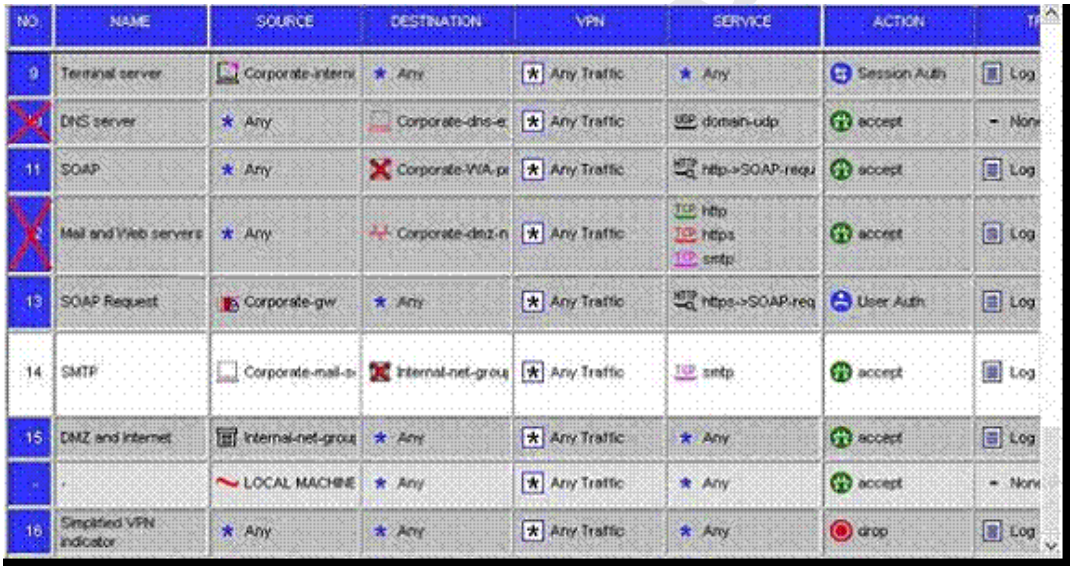
How will you install a rule base? Choose the best answer.

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

Answer: B
Explanation:

QUESTION NO: 190

How would you disable a rule?



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

Explanation:

QUESTION NO: 191

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

Explanation:

QUESTION NO: 192

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.

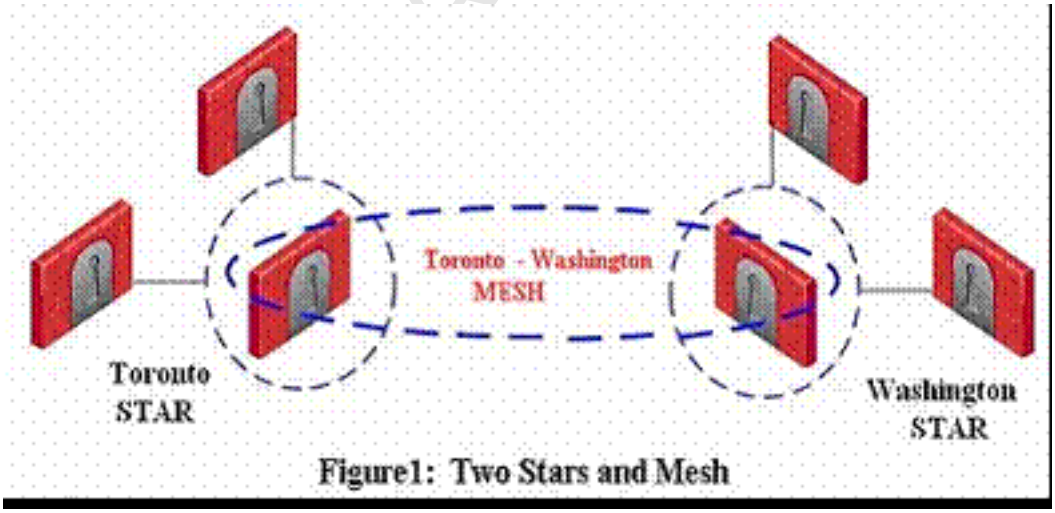


Figure1: Two Stars and Mesh

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 two mesh
D. You need to define three stars and two meshes
E. You need to define a star and a mesh

Answer: A
Explanation:

QUESTION NO: 193

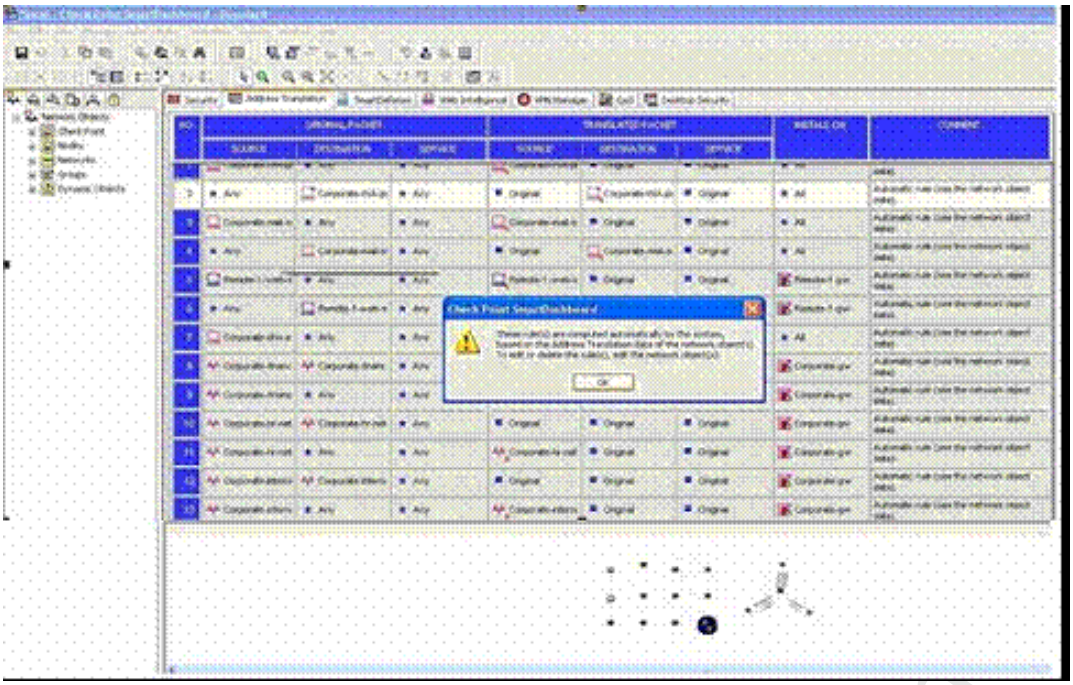
The negotiation prior to the establishment of a VPN tunnel might result in the production of large packets. Some NAT devices may not fragment large packets correctly making the connection impossible. Which of the following is true as to the resolving this issue?

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
Explanation:

QUESTION NO: 194

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



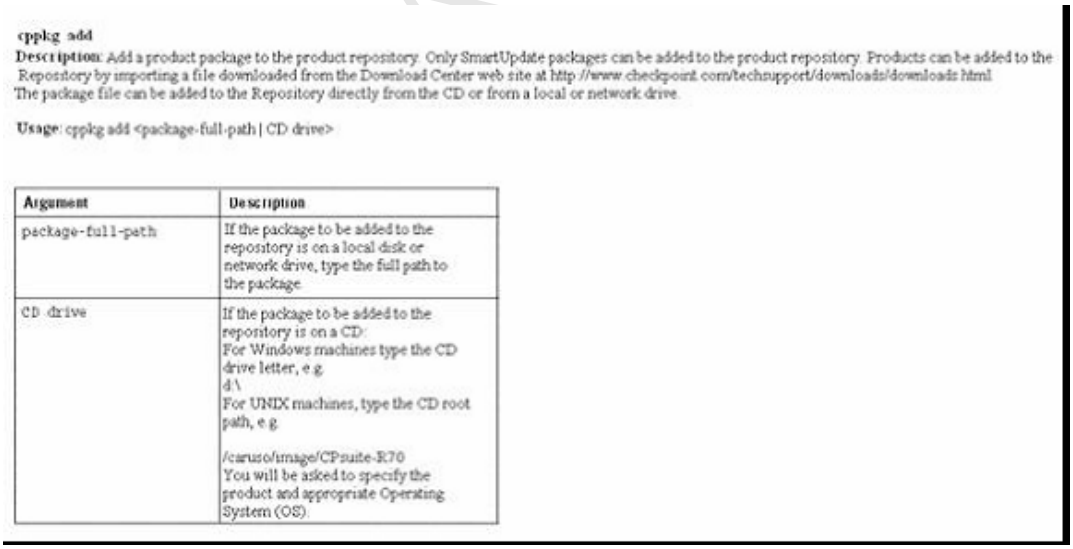
A. By highlighting the rule, click on Rules menu and select delete
B. By highlighting the rule and hit Delete button on your keyboard
C. By highlighting the rule, right-click and select Delete option from the emerging menu
D. By highlighting the rule, click on Edit menu and select delete
E. By modifying the object's configuration

Answer: E

Explanation:

QUESTION NO: 195

The SmartUpdate command line "cprinstall get" will:



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 $FWROOT.

Usage: cppkg get

cppkg getroot

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

Usage: cppkg getroot

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

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 cpprinstall 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:\FWroot and on UNIX it is /var/FWroot. 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 $FWROOT 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 string).

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 $FWROOT 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 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 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][-o
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
- cpinstall 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: aa6uwkuDc-CE6CRtjhr-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.

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
CK01234567890ab
```

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.
-P 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-z98N7Cc3m (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

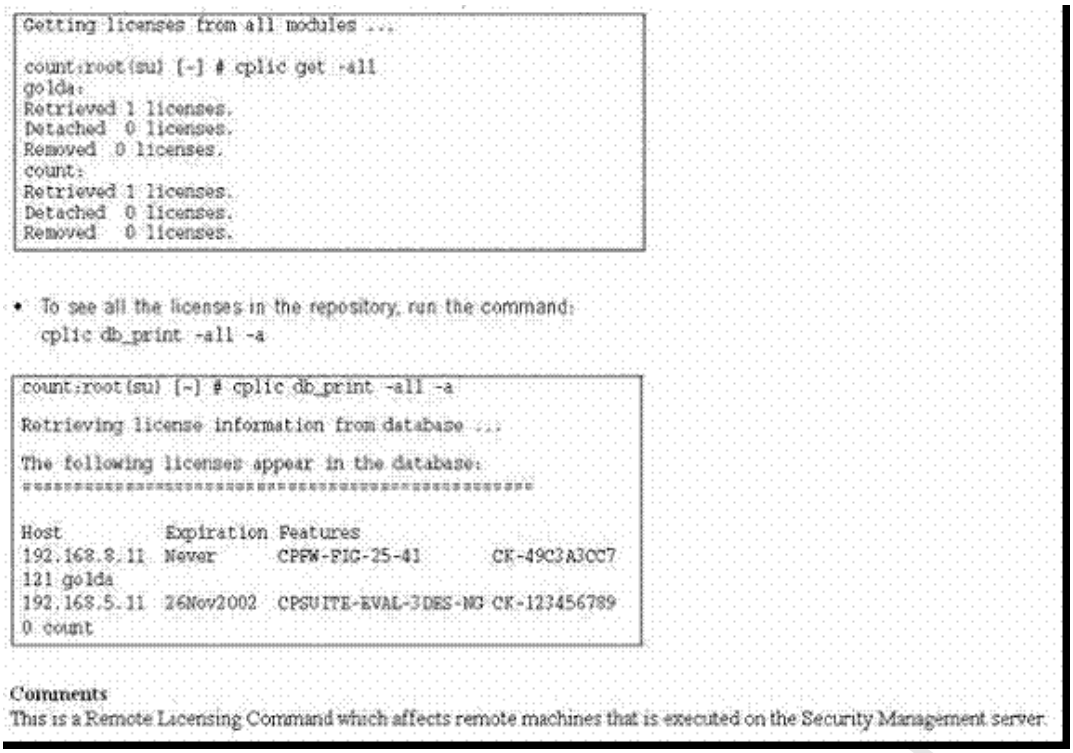
Description: Use the cplic upgrade command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.

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:



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
Explanation:

QUESTION NO: 196

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
Explanation:

QUESTION NO: 197

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 cplic del command to detach the license then re-run the cplic db_rm Command

Answer: E
Explanation:

QUESTION NO: 198

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
Explanation:

QUESTION NO: 199

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
Explanation:

QUESTION NO: 200

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
Explanation:

QUESTION NO: 201

What will the command "d:\winnt\fw1\ng\bin] cppkg add C:\CPsuite-R71" 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
Explanation:

QUESTION NO: 202

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

Explanation:

QUESTION NO: 203

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?

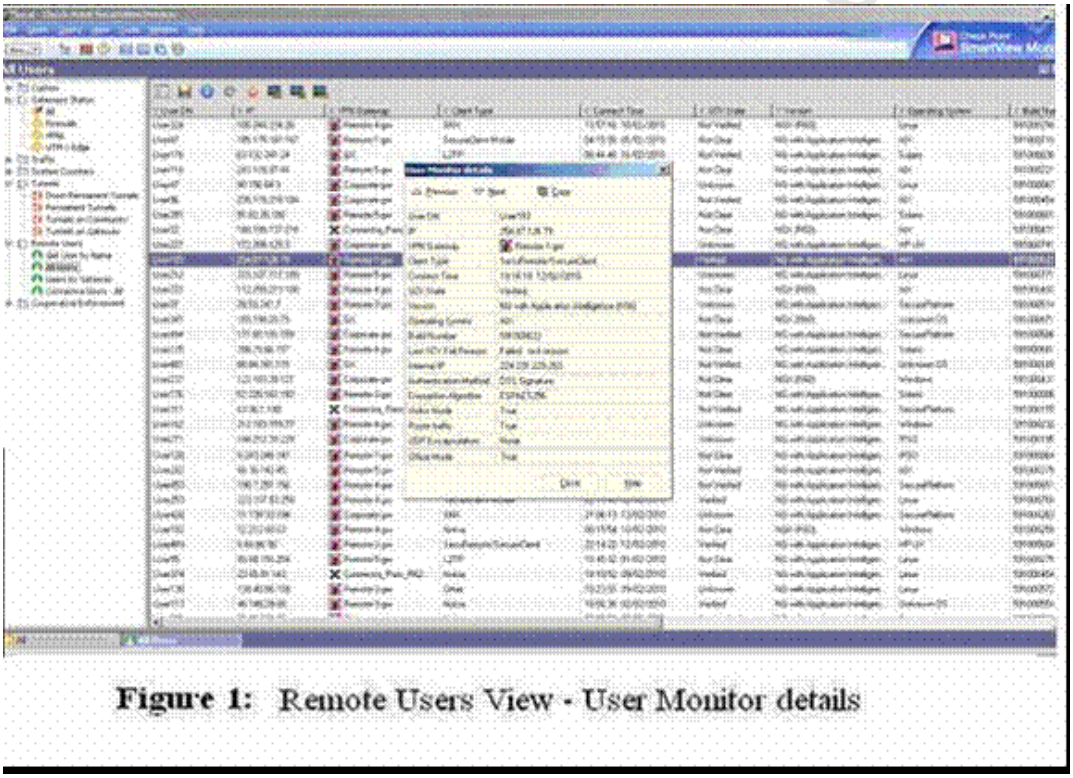


Figure 1: Remote Users View - User Monitor details

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

Answer: C

Explanation:

QUESTION NO: 204

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).

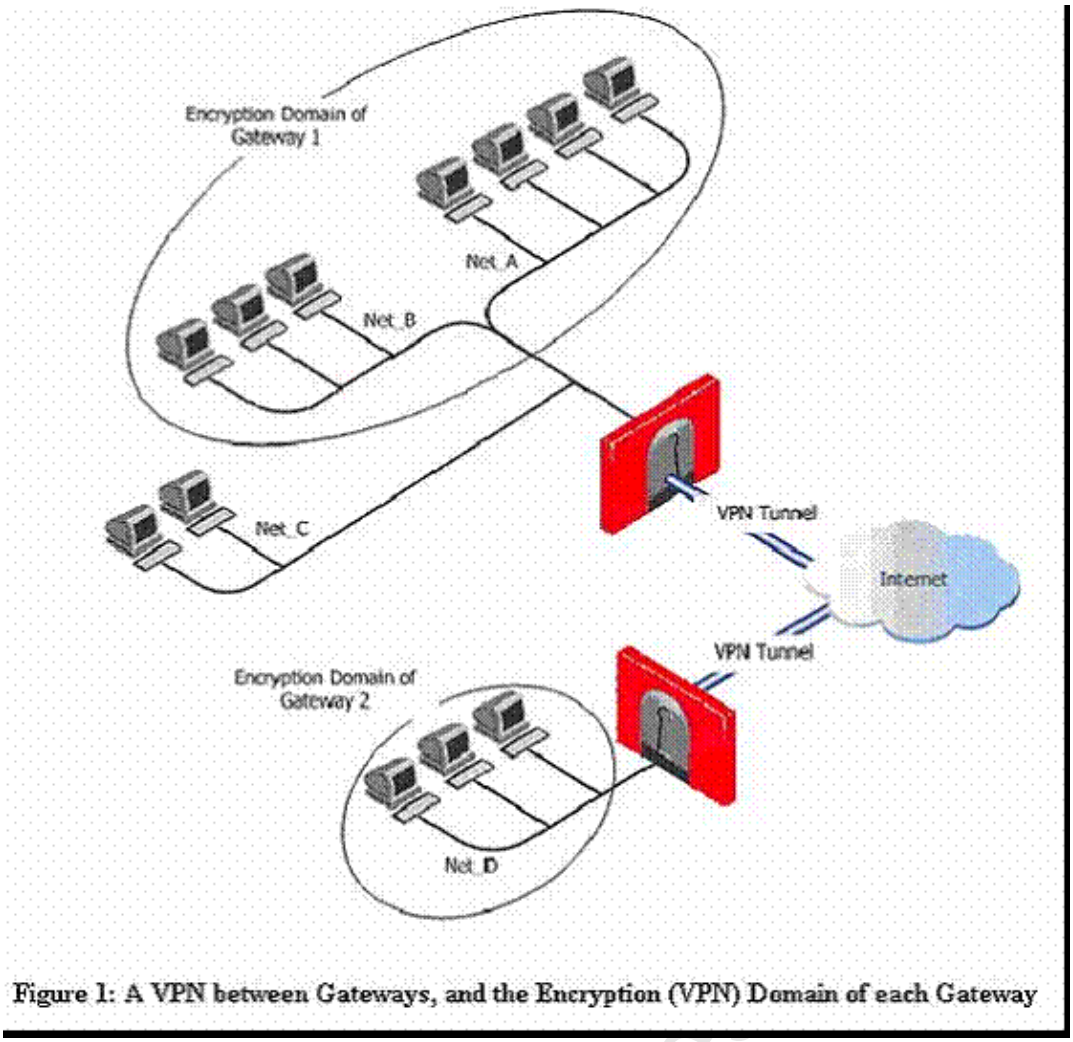


Figure 1: A VPN between Gateways, and the Encryption (VPN) Domain of each Gateway

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

Answer: B

Explanation:

QUESTION NO: 205

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

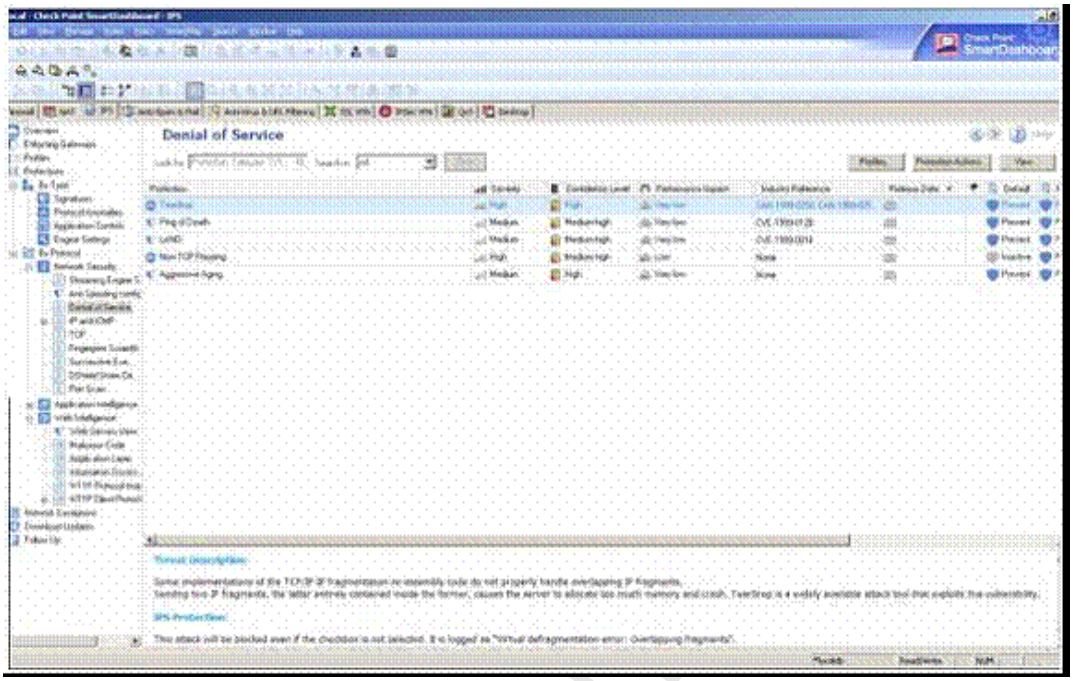
A. The use of authentication algorithm
B. Support of Multiple SmartDirectory (LDAP) Vendors using Profiles
C. Support of multiple SmartDirectory (LDAP) servers
D. High Availability
E. The use of encrypted or non-encrypted SmartDirectory (LDAP) Connections

Answer: B,C,D,E

Explanation:

QUESTION NO: 206

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



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 vulnerability Specially 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 fragmented PING 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

Explanation:

QUESTION NO: 207

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

Explanation:

QUESTION NO: 208

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?

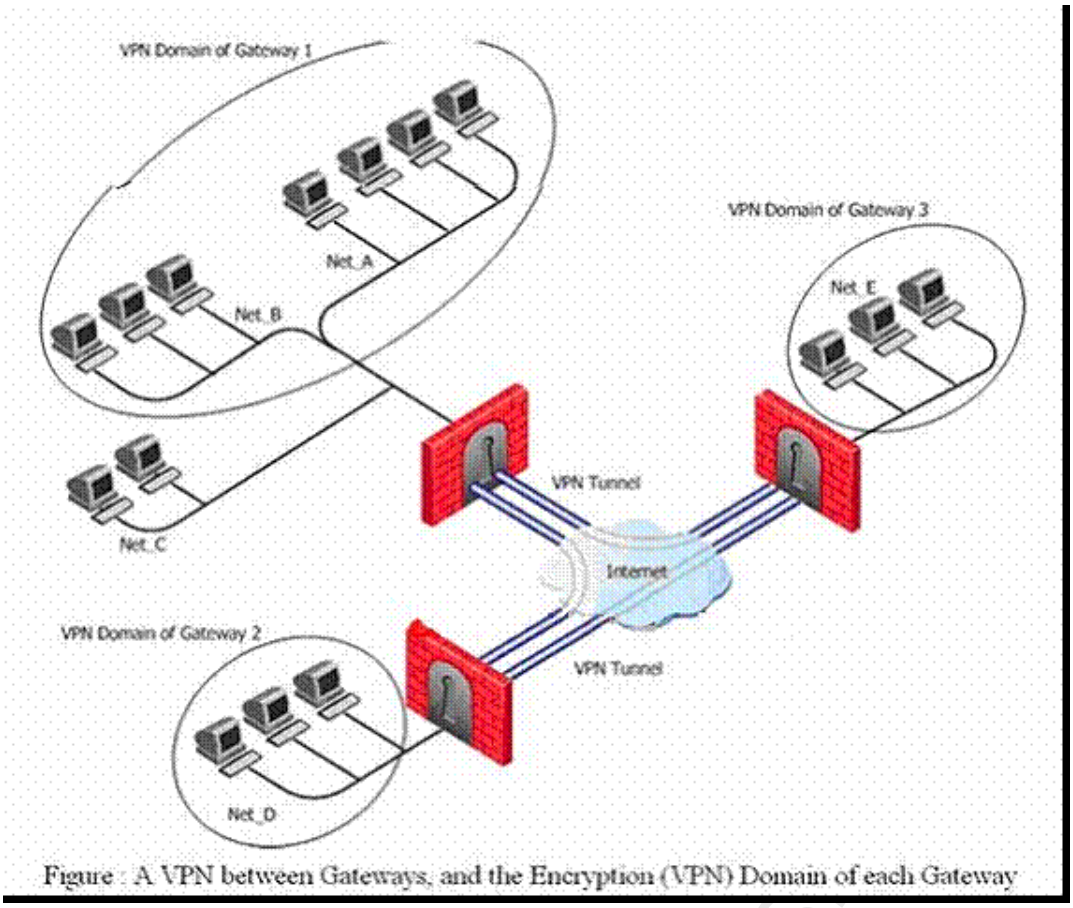


Figure : A VPN between Gateways, and the Encryption (VPN) Domain of each Gateway

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

Explanation:

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: 209

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
Explanation:

QUESTION NO: 210

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
Explanation:

QUESTION NO: 211

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

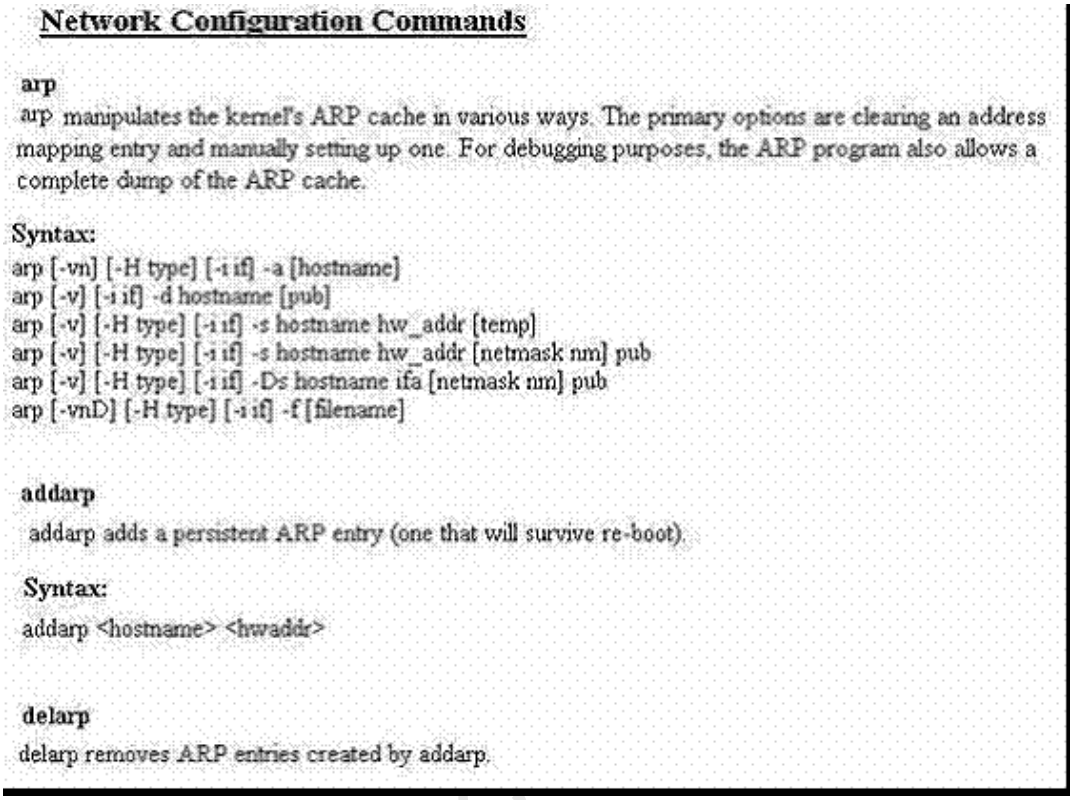
D. HTTP
E. HTTPS

Answer: A

Explanation:

QUESTION NO: 212

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 the 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

Explanation:

QUESTION NO: 213

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
Explanation:

QUESTION NO: 214

What command will you use to configure network interfaces settings?

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

Answer: E
Explanation:

QUESTION NO: 215

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

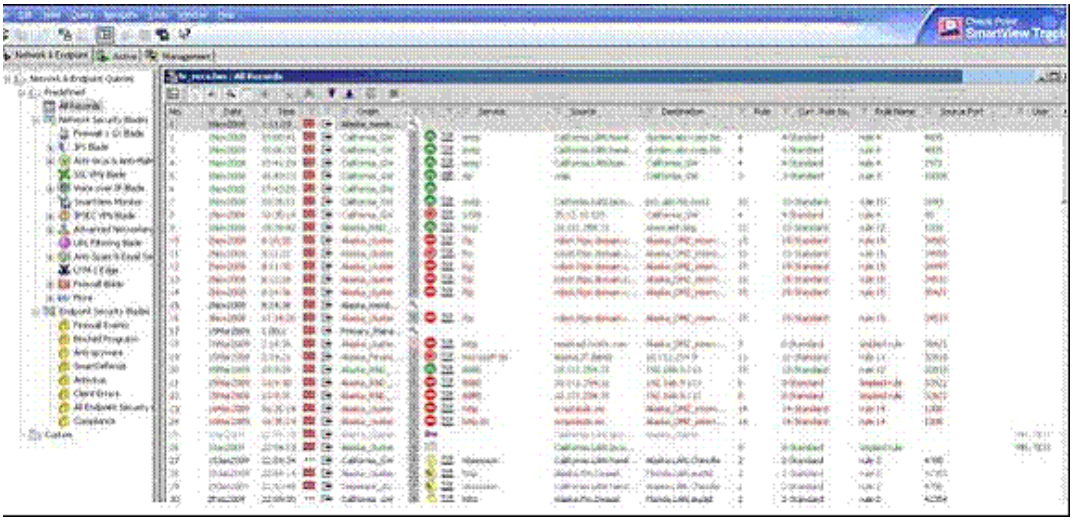
A. Nothing is wrong.
B. The authentication type should be changed to session authentication.
C. The user was TELNET- ing at wrong port. The user should use port 295.
D. The user was TELNET- ing at the wrong port. The user should use port 259.
E. The authentication type should be changed to user authentication.

Answer: E
Explanation:

QUESTION NO: 216

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

Explanation:

QUESTION NO: 217

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

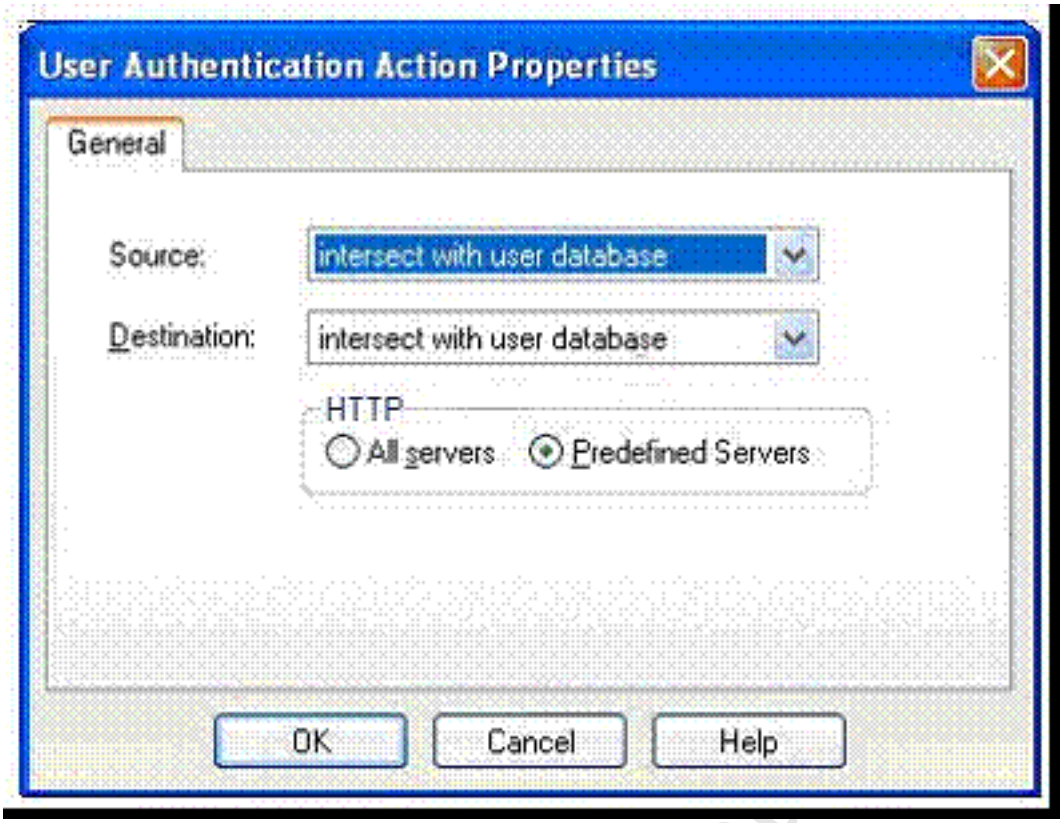
Answer: D

Explanation:

QUESTION NO: 218

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:



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

Explanation:

QUESTION NO: 219

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

Explanation:

QUESTION NO: 220

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

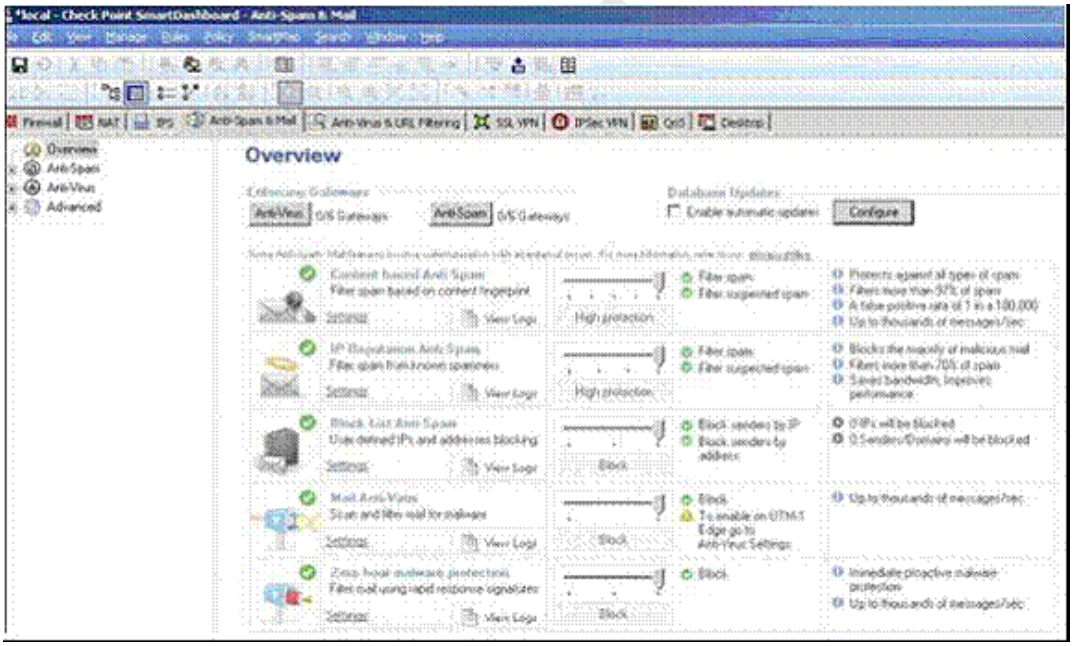
A. No available answer
B. In some situations
C. In some rear situations
D. In all situations
E. Not in any situation

Answer: D

Explanation:

QUESTION NO: 221

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



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

Explanation:

QUESTION NO: 222

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

Explanation:

QUESTION NO: 223

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

Explanation:

UESTION NO: 224

Which of the following are external authentication scheme that are supported by R71? 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: 224

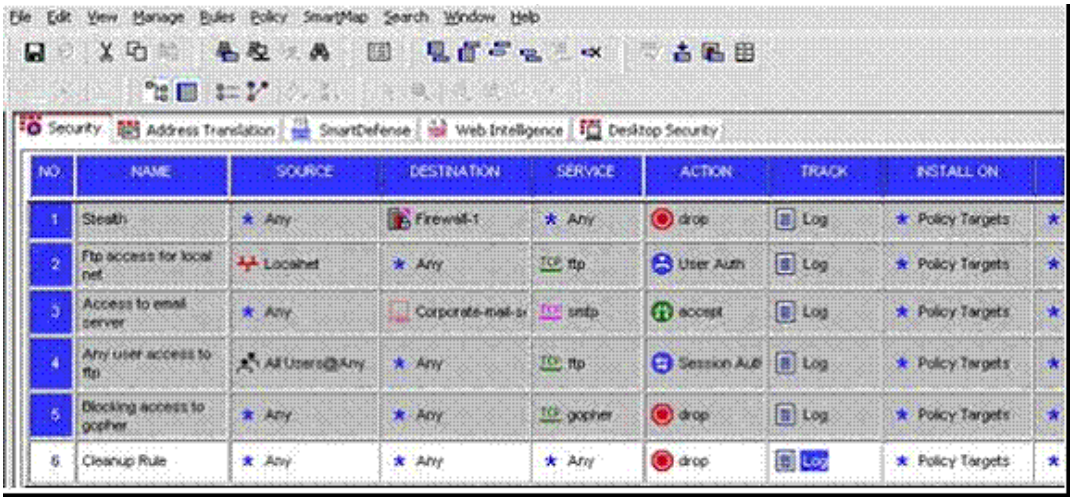
VPN routing provides a way of controlling how VPN traffic is directed. There are two methods for doing this. Which of these two methods will Route VPN traffic based on the encryption domain behind each Gateway in the community?

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

Answer: B
Explanation:

QUESTION NO: 225

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?



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

Answer: D
Explanation:

QUESTION NO: 226

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

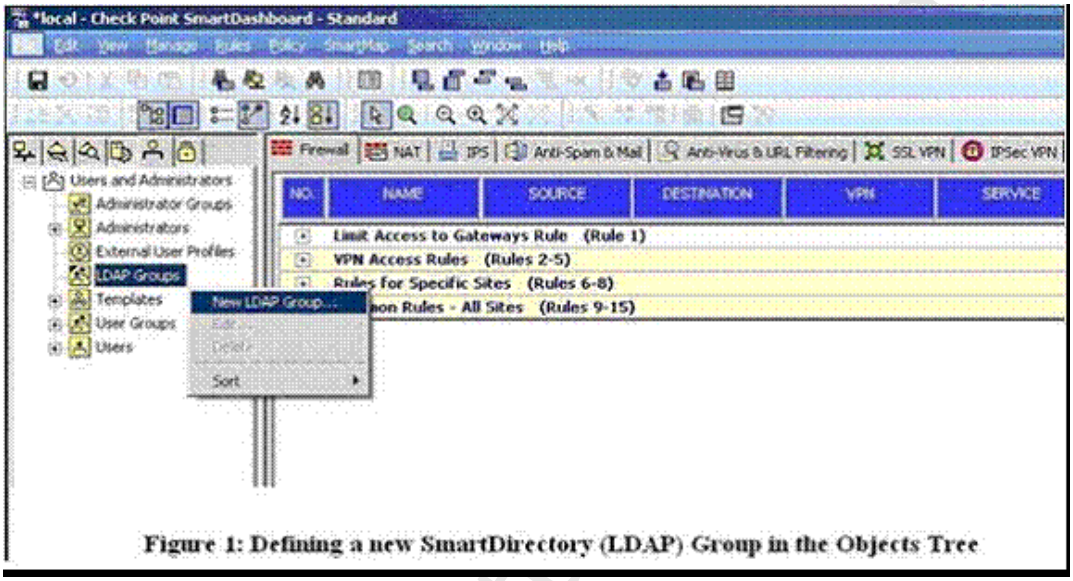


Figure 1: Defining a new SmartDirectory (LDAP) Group in the Objects Tree

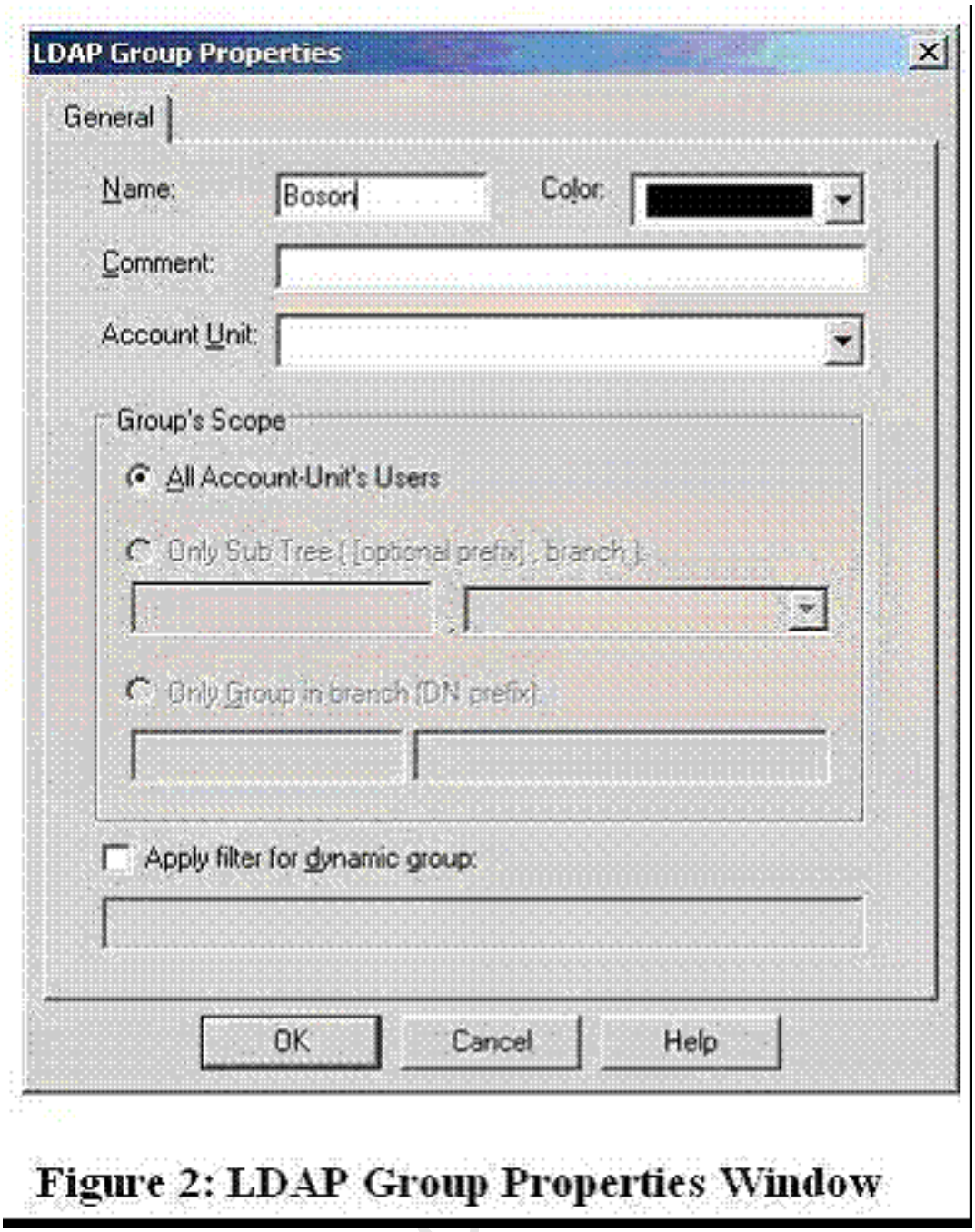


Figure 2: LDAP Group Properties Window

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 are created, they can be applied in various policy rules

Answer: A,B,D,E

Explanation:

UESTION NO: 228

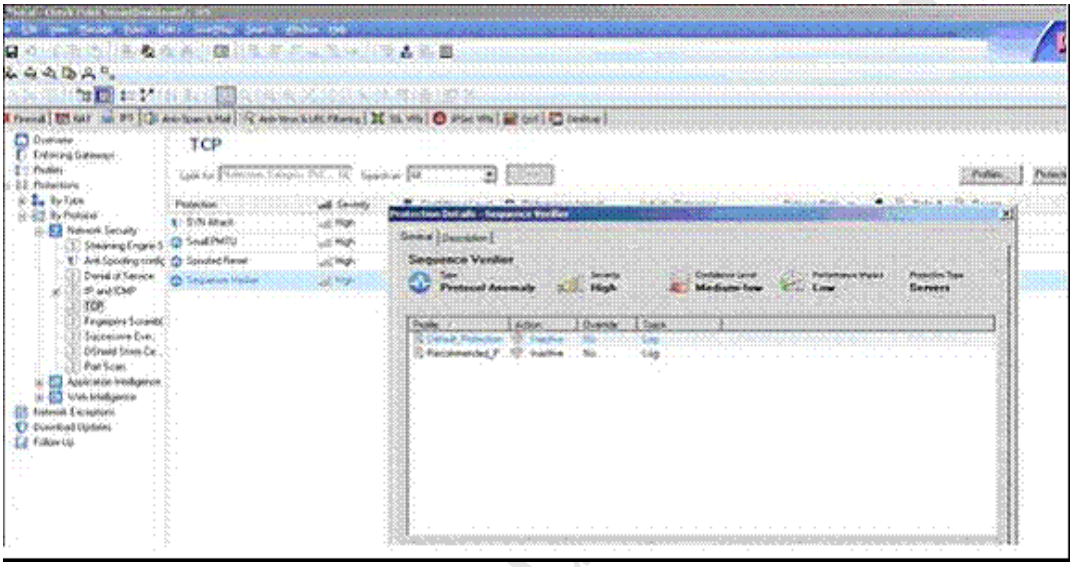
The default cluster administrator user name is:

A. Supervisor
B. Adminstrator
C. cadmin
D. Admin
E. clusterAdmin

Answer: C

QUESTION NO: 227

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



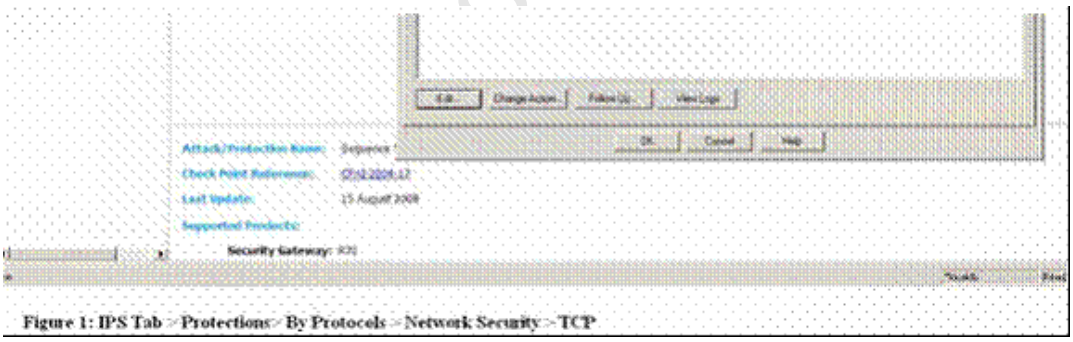


Figure 1: IPS Tab > Protections > By Protocols > Network Security > TCP

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: 228

You are responsible for the configuration of MegaCorp's Firewall you need to allow two NA rules to match a connection. Is it possible? Give the best answer

A. Yes it is possible to have the NAT rules which match a connection, but only in using manual NAT (bidirectional NAT)
B. No, it is not possible to have more one NAT rule matching a connection. When the firewall receives a packet belonging to a connection, it compares it against the first rule in the rule base, and then the second rule, and so on. When it finds a rule that matches, it stops checking and applies that rule.
C. Yes, there are always as many active NAT rules as there are connections.
D. Yes it is possible to have two NAT rules which match a connection, but only when using Automatic NAT (Bidirectional NAT)

Answer: D
Explanation:

QUESTION NO: 229

A third shift Security Administrator configured and installed a new Security Policy early this morning when you arrive he tells you that he has been Receiving complaints that Internet very slow. You suspect the security Gateway virtual memory might be the problem. Which smart console component would you use to verify this?

A. SmartView Tracker
B. SmartView Monitor
C. This information can only be viewed with fw ctl pstat command from the CLI
D. Eventia Analyzer

Answer: B
Explanation:

QUESTION NO: 230

Which of the following is NOT true for Clientless VPN?

A. The Gateway accepts any encryption method that is proposed by the client and supported in the VPN
B. Secure communication is provided between clients and servers that support HTTP
C. User Authentication is supported
D. The Gateway can enforce the use of strong encryption

Answer: B

Explanation:

QUESTION NO: 231

A rule_____ is designed to log and drop nil other communication that does not match another rule.

A. Stealth
B. Cleanup
C. Reject
D. Ann-Spoor

Answer: B

Explanation:

QUESTION NO: 232

You currently do not have a Check Point software subscription for one of your products. What will happen if you attempt to upgrade the license for this product?

A. The license will be upgraded with a warning
B. It is deleted
C. It is upgraded with new available features, but cannot be activated
D. The license is not upgraded

Answer: D

Explanation:

QUESTION NO: 233

Which could be an appropriate solution for assigning a unique office mode IP address to secure client users?

A. Configure a DHCP server with IP reservation using the information gathered by the utility vpn

macutil.
B. Edit $ PWDIA/conf/SCM_ assignment. conf on the management server with the correct user name and office mode ip address
C. Create a DHCP resource with the fixed IP address to use name mapping.
D. Fixed office mode IP can be configured as a user property in smart dash board

Answer: A
Explanation:

QUESTION NO: 234

How are cached usernames and passwords cleared from the memory of a R71 Security Gateway?

A. By retrieving LDAP user information using the command fw f etchldap
B. By using the Clear User Cache button in Smart Dashboard
C. Usernames and password only clear from memory after they time out
D. By installing a Security Policy

Answer: D
Explanation:

QUESTION NO: 235

When you use the Global Properties default settings on R71. Which type of traffic will be dropped?

A. RIP traffic
B. Smart Update connections
C. Outgoing traffic originating from the Security Gateway
D. Firewall logging and ICA key-exchange information

Answer: A
Explanation:

QUESTION NO: 236

URL Filtering Policy ran make exceptions for specific sites by being enforced?

A. Only for specific sources and destinations
B. For all traffic, except on specific sources and destinations
C. For all traffic, except blocked sites
D. For all traffic, There are no exceptions

Answer: B
Explanation:

QUESTION NO: 237

You are the Security Administrate for university The University's FTP servers have old hardware and software. Certain FTP command causes the FTP servers to malfunction Upgrading the FTP servers is not an optional this time. Where you can define blocked FTP commands passing through the Security Gateway protecting the FTP servers?

A. IPS > Protections > By Protocol > IPS Software Blade > Application Intelligence > FTP > FTP advanced protections>FTP Commands
B. FTP Service Object > Advanced > Blocked FTP Commands
C. Global Properties > Firewall > Security Server > Allowed FTP Commands
D. Rule Base > Service Field > Edit Properties

Answer: A
Explanation:

QUESTION NO: 238

Spoofing is a method of:

A. Hiding your firewall from unauthorized users.
B. Disguising an illegal IP address behind an authorized IP address through port address Translation.
C. Making packets appear as if they come from an authorized IP address
D. Detecting people using false or wrong authentication logins.

Answer: C
Explanation:

QUESTION NO: 239

You plan to migrate a Windows NG with Application Intelligence (Ai) R55 SmartCener server to R71. You also plan to upgrade four VPN-1 pro Gateways at remote offices and one local VPN-1 pro gateway at your company's head quarter to R71. The management server configuration must be migrated. What is the correct procedure to migrate the configuration?

A. 1. Upgrade the remote gateway via smartUpdate.

2. upgrade the security management server, using the R71 CD
B. 1. From the R71 CD-ROM on the security management server, select Upgrade
2. Reboot after installation and upgrade all licenses via SmartUpdate
3. Reinstall all gateways using R 70 and install a policy
C. 1. Copy the $PWDIR\ conf directory from the security management server
2. Save directory contents to another file server
3. Uninstall the security management server, and install anew security management server
4. Move the saved directory contents to $ PWDIR\conf replacing the default installation files
5. Reinstall all gateways using R71 and install a security policy
D. 1. From the R71 CD- ROM in the security management server, select export
2. Install R 70 on a new PC using the option installation using imported configuration
3. Reboot after installation and update all licenses via smartUpdate
4. Upgrade software on all five remote Gateway via SmartUpdate

Answer: D
Explanation:

QUESTION NO: 240

When john first installed the system, he forgets to configure DNS servers on the security Gateway. How could John configure DNS servers now that his security gateway is in production?

A. Login to the firewall using SSH and run cpconfig, than select domain name servers
B. Login to the firewall using SSH and run fwn, than select system configuration and domain name servers.
C. Login to the smart dashboard, edit the firewall gate object, select the tab interface, than domain name servers
D. Login to the firewall using SSH and run sysconfig, then select domain name servers.

Answer: D
Explanation:

QUESTION NO: 241

You have an NGX R65 have gateway running on Security platform. The Gateway also serves as a Policy Server. When you run patch add CD from security Gateway R71 CD-ROM. what does this command allow you to upgrade?

A. Only the R71 Security Gateway
B. Only the patch utility is upgraded using this command
C. All products, except the Policy Server
D. Both the operating system and all Check Point products

Answer: D
Explanation:

QUESTION NO: 242

Which of the following explanations best describes the command fw logswitch {-h taeget} {+ 1 -} {oldlog}

A. Display a remote machine's log-file list.
B. Control Kernel
C. Display protocol Hosts
D. Create a new Log file. The old log has moved

Answer: D
Explanation:

QUESTION NO: 243

Which of the following uses the same key to decrypt as it does to encrypt?

A. Asymmetric encryption
B. Symmetric encryption
C. Certificate-based encryption
D. Dynamic encryption

Answer: B
Explanation:

QUESTION NO: 244

NAT can be implemented on which of the following lists of objects?

A. Domain network
B. Host network
C. Host user
D. Network, Dynamic Object

Answer: B
Explanation:

QUESTION NO: 245

Which security servers can perform authentication task, but CANNOT perform content security tasks?

A. FTP
B. HTTP
C. Telnet
D. HTTPS

Answer: C
Explanation:

QUESTION NO: 246

Central license management allows a Security Administrator to perform which of the following functions?

1) Check for expired licenses.

2) Sort licenses and view license properties

3) Attach both R71 Central and Local licenses to a remote module

4) Delete both R71 Local licenses and Central licenses from a remote module

5) Add or remove a license to or from the license repository

6) Attach and/or delete only R71 Central licenses to a remote module (not local licenses)

A. 2.5.&6
B. 2.3.4.&5
C. L 2. 5.& 6
D. 1.2.3.4.&5

Answer: D
Explanation:

QUESTION NO: 247

Which smear view tracker selection would most effectively show who installed a security policy blocking all traffic from the corporate network?

A. Custom filter

B. Network and Endpoint tab
C. Management Tab
D. Active tab

Answer: C
Explanation:

QUESTION NO: 248

Identify the ports to which the Client authentication daemon listens default?

A. 256, 600
B. 80, 256
C. 8080, 529
D. 259, 900

Answer: D
Explanation:

QUESTION NO: 249

Select the correct statement about secure internal communication (S|C) certificates, S|C certificates?

A. Increase network security by securing administrative communication with a two factor challenge response authentication.
B. Uniquely identify the machines installed with check point software only. They have the same function as RSA authentication certificates.
C. Are for security Gateways created during the security management server installation.
D. Can be used for securing internal network communication between the security gateway and an OPSEC device.

Answer: D
Explanation:

QUESTION NO: 250

What is the syntax for uninstalling a package using newpkg?

A. –s (pathname of package)
B. –u (pathname of package)

C. Newpkg CANNOT be used to install
D. –i (full pathname of package)

Answer: C
Explanation:

QUESTION NO: 251

An internal host initiates a session to www.google.com http://www.google.com/ and is set for hide NAT behind the security gateway. The initiating traffic is an example of _____.

A. Client side NAT
B. Destination NAT
C. Source NAT
D. None of these

Answer: C
Explanation:

QUESTION NO: 252

The user directory software blade is use to integrate which of the following with security gateway R71?

A. RADIUS server
B. Account management client server
C. User authority server
D. LDAP server

Answer: C
Explanation:

QUESTION NO: 253

What is the officially accepted diagnostic tool for IP appliance support?

A. Ipsinfo

B. Uag-diag
C. CST
D. cpinfo

Answer: C
Explanation:

QUESTION NO: 254

There are three options available for configuring a firewall policy on the Secure Client Mobile device. Which of the following is NOT an option?

A. Configured on endpoint client
B. No
C. Configured on server
D. yes

Answer: B
Explanation:

QUESTION NO: 255

You are connected that a message may have been increased and retransmitted, thus compromising the security of the communication. You attach a code to the electronically transmitted message that uniquely identifies the sender. This code is known as a (n):

A. diffie-Helman verification
B. digital signature
C. private key
D. AES flag

Answer: A
Explanation:

QUESTION NO: 256

If you were NOT using IKE aggressive mode for your IPSec tunnel, how many packets would you see for normal phase exchange?

A. 6

B. 2
C. 3
D. 9

Answer: A
Explanation:

QUESTION NO: 257

In order to have full control you decide to use manual NAT entries instead of automatic NAT rules. Which of the following is NOT true?

A. When using dynamic hide NAT with an address that is not configured on a gateway interface, you need to add proxy ARP entry for that.
B. When using static NAT, you must add proxy ARP entries for the gateway on the hosts that are using the NAT gateway with the gateway internal
C. When using static NAT, you must add proxy ARP entries to the Gateway for all hiding addresses
D. If you choice Automatic NAT instead, all necessary entries are done for you.

Answer: A
Explanation:

QUESTION NO: 258

Which antivirus scanning method does not work if the gateway is connected as a node in proxy mode?

A. Scan by direction
B. Scan by file type
C. Scan by server
D. Scan by IP address

Answer: A
Explanation:

QUESTION NO: 259

How can | verify the policy version locally instead on the firewall?

A. Fw ver

B. Fw ctl iflist
C. Fw ver –k
D. Fw stat

Answer: C

QUESTION NO: 260

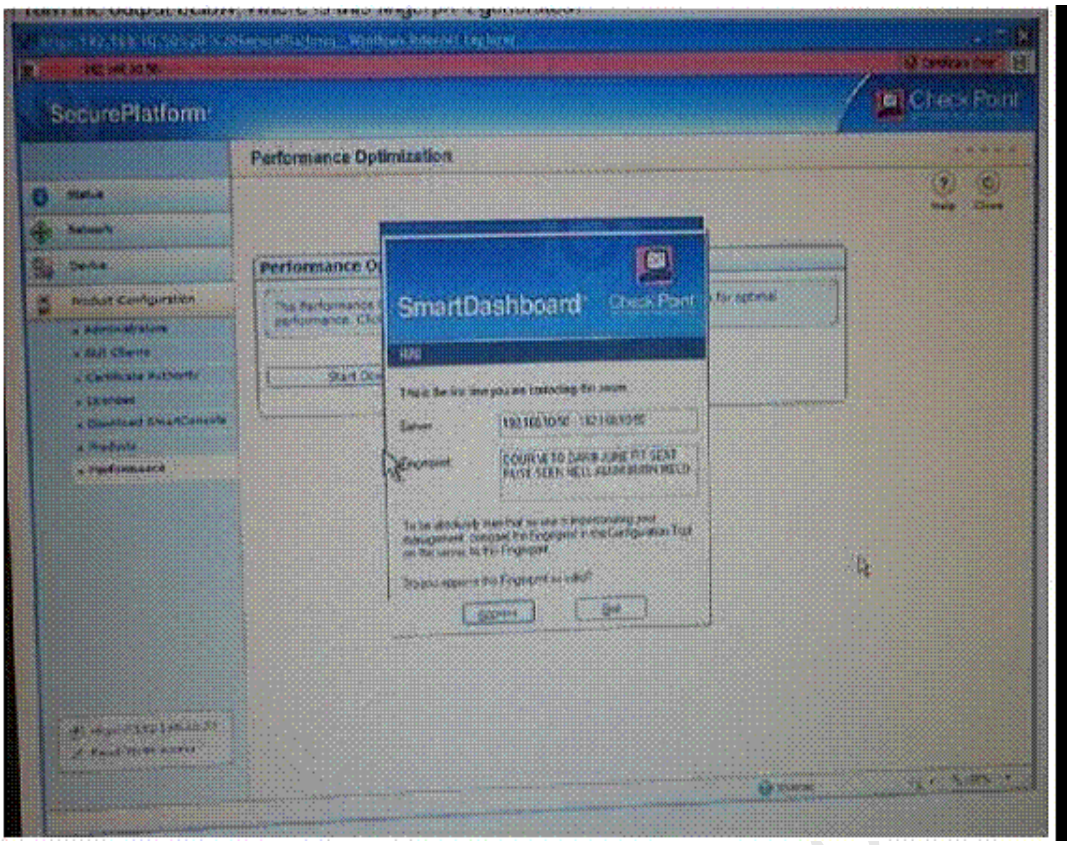
The third shift administrator was updating security management server access setting in global properties. He managed to lock the entire Administrator out of their accounts. How should you unlock these accounts?

A. Logging to smart dash board as special cpconfig_admin account. Right click on each administrator object and select Unlock.
B. Type fwm lock_admin –ua from the command line of the security management server
C. Reinstall the security management Server and restore using upgrade _imort
D. Delete the file admin .lock in the sfwdir/ tmp/directory of the security managem,ent server.

Answer: C
Explanation:

QUESTION NO: 261

From the output below, where is the fingerprint generated?



A. Security management server
B. SmartUpdate
C. SmartDashboard
D. SmartConsole

Answer: A

Explanation:

QUESTION NO: 262

What do you use to view a R71 security Gateway's status, including CPU use, amount of virtual memory, percent of free hard disk space, version?

A. Only possible via command line tools
B. SmartView Tracker
C. SmartView Monitor
D. SmartUpdate

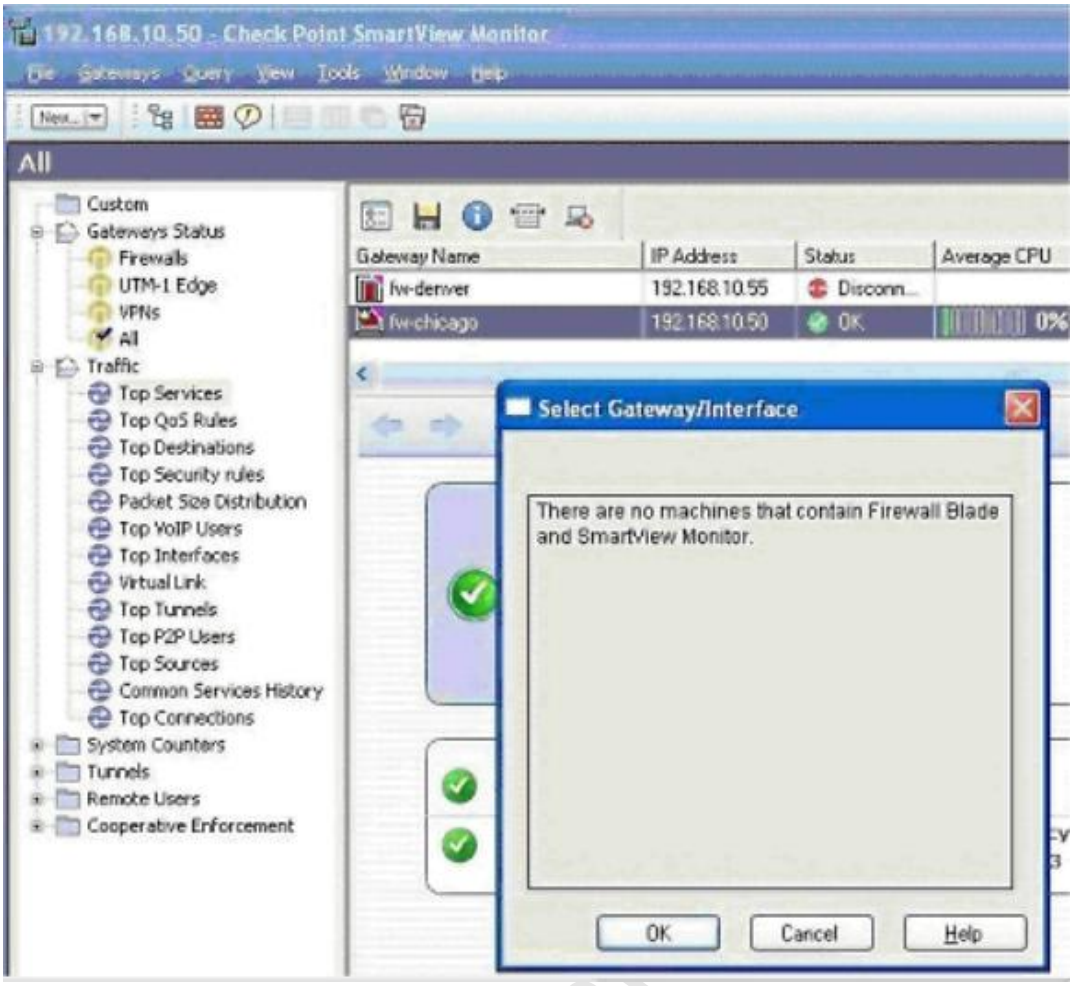
Answer: C

Explanation:

QUESTION NO: 263

Cara wants to monitor the top services on her security Gateway (fw-chicago), but she is getting an

error message. Other security gateways are reporting time information except a new security gateway that was just recently deployed. Analyze the error message from the out below and determine what Cara can do to correct the problem?



A. She should re-install the security policy on the security Gateway since it was using the default rule base
B. She should create a firewall rule to allow the CPMI traffic back to her smart console.
C. She should let the monitoring run longer in order for it to collect sampled data
D. She should edit the security Gateway object and enable the monitoring Software Blade.

Answer: D
Explanation:

QUESTION NO: 264

How do you recover communications between your security management server and security gateway if you “LOCK” yourself via a rule or policy mis-configuration?

A. Fw delete all. all@local host

B. Cpstop
C. Fw unloadlocal
D. Fw unload policy

Answer: C
Explanation:

QUESTION NO: 265

What are the approved methods of modifying objects_5_0 .c?

A. Windows WordPad
B. Windows notepad
C. dbedit
D. cpconfig

Answer: C
Explanation:

QUESTION NO: 266

After implementing static address translation to allow internet traffic to an internal web server on your DMZ. You notice that any NAted connections to that machine are being dropped by anti-spoofing protection which of the following is most likely cause?

A. The global properties settings translation on client side is checked. But the topology on the external change topology to others+
B. The global properties settings translation on client side is unchecked. But the topology on the external interface is set to others + change topology is external
C. The global properties settings translation on client side is checked. But the topology on the DMZ interface is set to be internal-network defined by IP and mask. Uncheck the Global properties setting Translation on Client side.
D. The global properties settings translation on client side is unchecked. But the topology on the DMZ interface is set to be internal-network defined by IP and mask. Click the Global properties setting Translation on Client side.

Answer: D
Explanation:

QUESTION NO: 267

Which of the following is NOT supported with office mode?

A. Transparent mode
B. L2TP
C. Secure Client
D. SSL Network Extender

Answer: A
Explanation:

QUESTION NO: 268

Which component functions as the internal certificate authority for R71?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLsm

Answer: B
Explanation:

QUESTION NO: 269

You are the security administrator in a large company called ABC. A Check point firewall is installed and is in use on secure platform. You are concerned. That the system might not be retaining your entries for the interfaces and routing configurations. You would like to verify your entries in the corresponding Files(s) on secure platform. Where can you view them? Give the best answer

A. / etc / conf /route . c
B. / etc / sysconfig / netconf .c
C. / ets / sysconfig / netconf-scripts / ifcfg-ethx
D. / etc / sysconfid / network

Answer: B
Explanation:

QUESTION NO: 270
When you change an implicit rule's order from last to first in global properties, how do you make

the change take effect?

A. Select save from the file menu
B. Reinstall the security policy
C. Select install database from the policy menu
D. Run fw fetch from the security gateway

Answer: B

Explanation:

QUESTION NO: 271

Your R71 security management server is installed on secure platform. You plan to schedule the security management server to run Log switch automatically every 48 hours. How do you create the schedule?

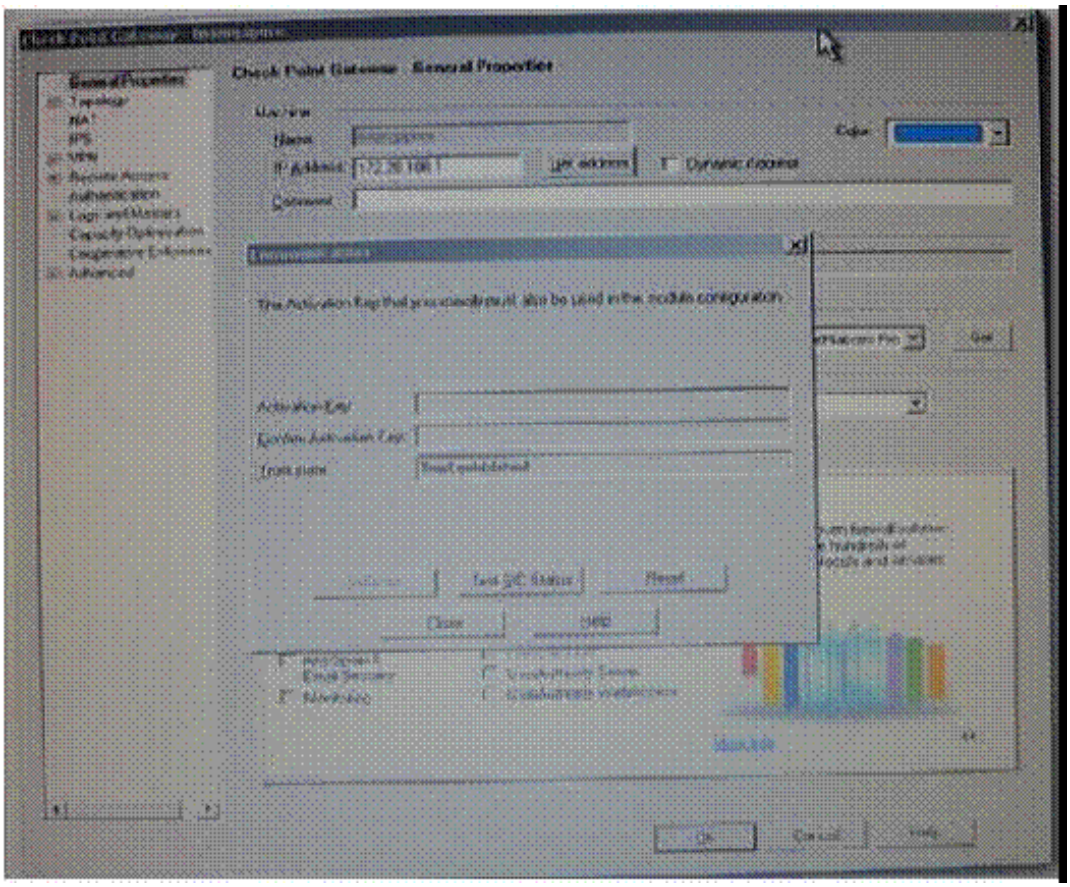
A. Create time object, and add 48 hours as the interval. Select the time object's global properties >logs and master window, to schedule a log switch
B. Create time object, and add 48 hours as the interval. Open the primary security management object's logs and master window, enable schedule log switch, and select the time object
C. Create time object, and add 48 hours as the interval. Open the security Gateway objects logs and masters window, enable schedule log switch, and select the time object
D. On a secure platform Security management Server, this can only the accomplished by configuring the fw logswitch command via the cron utility

Answer: B

Explanation:

QUESTION NO: 272

What will happen when Reset is pressed and confirmed?



A. The gateway certificate will be revoked on the security management server only
B. SIC will be reset on the Gateway only
C. The Gateway certificate will be revoked on the security management server and SIC will be reset on the Gateway
D. The gateway certificate on the gateway only

Answer: B

Explanation:

QUESTION NO: 273

How do you use Smartview monitor to compile traffic statistics for your campany's internet activity during production hours?

A. View total packets passed through the security gateway
B. Use the traffic counters setting and Smartview monitor to generate a graph showing the total HTTP traffic for the day
C. Select the Tunnels view, and generate a report on the statistics
D. Configure a suspicious activity rule which triggers an alert when HTTP traffic pass through gateway

Answer: B

Explanation:

QUESTION NO: 274

Which of the following is viable consideration when determining rule base order?

A. Grouping functionality related rules together
B. Grouping rules by date of creation
C. Grouping authentication rules with address translation rules
D. Grouping reject and drop rules after the cleanup rule

Answer: A
Explanation:

QUESTION NO: 275

You are about the integrated RSA SecurID users into to the check point infrastructure. What kind of users are to be defined via SmartDashboard?

A. internet user group
B. a group wit generic user
C. LDAP account unit Group
D. All users

Answer: A
Explanation:

QUESTION NO: 276

What is the primary benefit of using upgrade_export over either backup of snapshot?

A. The backup and snapshot commands can take long time to run whereas upgrade_export will take a much shorter amount of time.
B. upgrade_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.
C. upgrade_export is operating system independent and can be used when backup of snapshot is not available.
D. upgrade_export has an option to backup the system and SmartView tracker logs while back and snapshot will not.

Answer: A

Explanation:

QUESTION NO: 277

Which of the following actions do not place in IKE phase 1?

A. Each side generates a session key from its private key and peer's public key
B. Peers agree on integrity method
C. Diffie-Hellman key is combined with the key material to produce the symmetrical IPSec key.
D. Peers agree on encryption method

Answer: C
Explanation:

QUESTION NO: 278

The customer has small Checkpoint installation which includes one windows 2003 server as the SmartConsole and second server running SecurePlatform as both Management Server and Security Gateway. This is an example of a(n):

A. Unsupported configuration
B. Hybrid installation
C. Distributed installation
D. Stand-Alone installation

Answer: C
Explanation:

QUESTION NO: 279

A marketing firm's networking team is typing to troubleshoot user complaints regarding access audio-streaming material from the internet. The networking team asks you to check the object and rule configuration settings for perimatre security Gateway. Which SmartConsole application should you use to check these object and rules?

A. Smart View Tracker
B. SmartView Status
C. SmartView Monitor
D. Smart Dashboard

Answer: D

Explanation:

QUESTION NO: 280

Multi-corp must comply with industry regulations in implementing VPN solutions among Multiple defines the following requirements:

Portability Standard

Key management Automatic, external PKI

Session keys changed at configured times during a connection's lifetime

Key length No less than 128-bit

Data integrity Secure against inversion and brute-force attacks

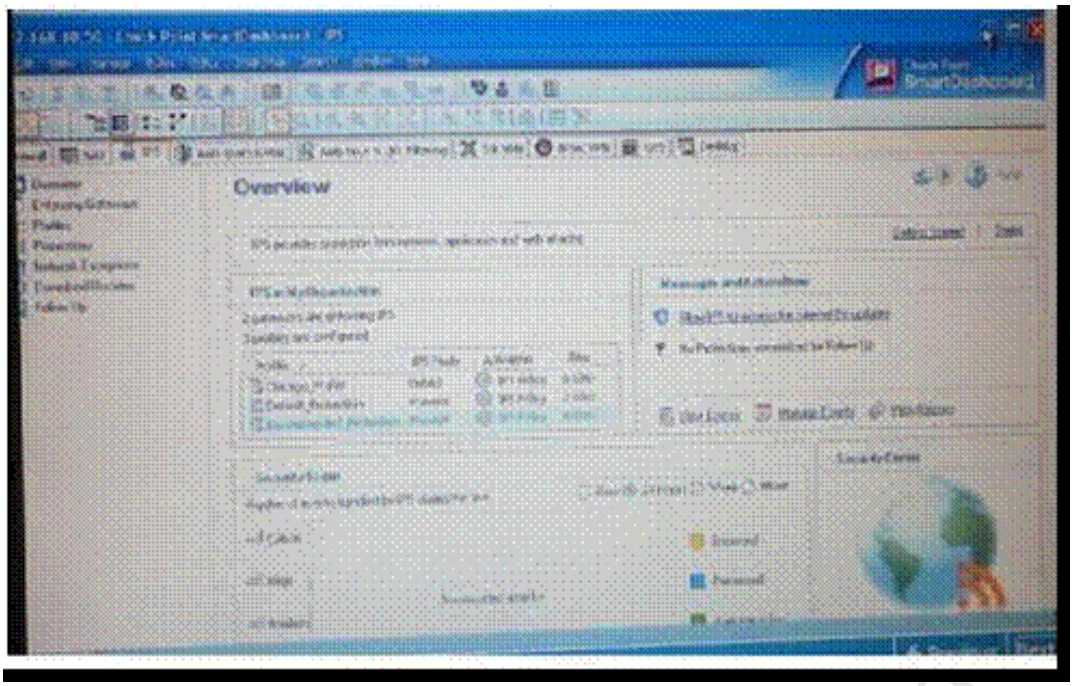
What is the most appropriate setting to comply with theses requirements?

A. IKE VPNs: SHA1 encryption for IKE Phase 1, and MD5 encryption for phase 2, AES hash
B. IKE VPNs: DES encryption for IKE phase 1, and 3DES encryption for phase 2, MD 5 hash
C. IKE VPNs: CAST encryption for IKE Phase 1, and SHA 1 encryption for phase 2, DES hash
D. IKE VPNs: AES encryption for IKE Phase 1, and MD5 encryption for phase 2, SHA 1 hash

Answer: B
Explanation:

QUESTION NO: 281

Totally cool security company has a large security staff. Bob configured a new IPS Chicago_ Profile for fw_ chicago using Delete mode. After reviewing Matt noticed that Fw_ chicago is not directing any of the IP protection that Bob had previously setup. Analyze the output below and determine how matt correct the problem.



A. Matt should re-create the Chicago_Profile and select activate protections manually instead of per the IPS policy.
B. Matt should re-create the Chicago_Profile as it is currently not activated.
C. Matt should assign the fw_Chicago Security Gateway to the Chicago Profile
D. Matt should re-create the Chicago_Profile to use protect mode because detect mode will not work

Answer: C
Explanation:

QUESTION NO: 282

For information to phase security between security management Server and another Checkpoint component, what would not be required?

A. The communication must be authenticated
B. The communication must use two factor or biometric authentication
C. The communication must be encrypted
D. The component must be time-and-date synchronized with the security management server.

Answer: B
Explanation:

QUESTION NO: 283

The security gateway is installed on Secure Platform R71. The default port for the web user is _____.

A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D
Explanation:

QUESTION NO: 284

You are creating an out put file with the following command:

Fw monitor -e “accept (src=10.20.30.40 or dst=10.20.30.40); “ -0 ~/ output

Which tool do you use to analyze this file?

A. You can analyze it with Wireshark or Ethernet
B. You can analyze the output file with any ASCII editor
C. The output file format is CSV, so you can use MS Excel to analyze it
D. You can analyze it with any tool as the Syntax should be:
Fw monitor -e “accept ([12, b]=10.2.30.40 or [16, b]=10.20.30.40); -0 ~/ output.

Answer: A
Explanation:

QUESTION NO: 285

How do you define a service object for a TCP port range?

A. Manage services>New TCP, provide name and define port x-y
B. Manage services>New group, provide name and add all services ports for range individually to the group object
C. Manage services>New other, provide name and define protocol: 17, Range: x-y
D. Manage services>New other, provide name and define protocol: x-y

Answer: A
Explanation:

QUESTION NO: 286

Your online bookstore has customers connecting to a variety of Web Services to place or change orders and check order status. You ran penetration tests through the security gateway to determine if the Web Servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated to web servers were still Vulnerable. You have checked every box in the web intelligence tab, and installed the security policy. What else might you do to reduce the vulnerability?

A. Configure the security gateway protecting the web servers as a web server.
B. Check the products> Webserver box on the host node representing you
C. Add port (TCP 443) as an additional port on the Webserver tab for the host node
D. The presentation software you are using is malfunctioning and is reporting a false-po

Answer: C
Explanation:

QUESTION NO: 287

What would be the benefit of upgrading from smart defense to IPS r 70?

A. The Smart Defense is replaced by the technology of IPS-1
B. The Smart defense technology expands IPS -1 to IPS R 70.
C. Completely rewritten engine provides improved security performance and reporting.
D. There is no difference-IPS R71 is new name

Answer: C
Explanation:

QUESTION NO: 288

What physical machine must have access to the user Centre center public IP address when checking for new packages with SmartUpdates?

A. Smart Update GUI PC
B. SmartUpdate Repository SQL database server
C. A security gateway retrieving the new Upgrade Package
D. SmartUpdate installed security management server PC

Answer: D
Explanation:

QUESTION NO: 289

Which rule should be cleanup Rule in the Rule Base?

A. Last, it servers a logging function before the implicit drop.
B. Last, it explicitly drops otherwise accepted traffic
C. Before last followed by the Stealth Rule.
D. First, it explicitly accepts otherwise dropped traffic.

Answer: A
Explanation:

QUESTION NO: 290

In smart dash Board, Translation destination on client side is checked in global properties. When network Address translation is used:

A. It is necessary to add a static route to the gateways routing tables
B. The security gateway's ARP file must be modified
C. It is necessary to add a static route to the gateway's routing table
D. VLAN tagging cannot be defined for any hosts protected by the gateway

Answer: B
Explanation:

QUESTION NO: 291

Assume you are a security administrator ABCTech. You have allowed authenticated access to users from Mkting_net to Finance_net. But in the user's properties, connections are only permitted within Mkting_net. What is the BEST way to resolve this conflict?

A. Permit access to Finance_net
B. Select ignore database in action properties wibndow
C. Select intersect with user database in the action properties window
D. Select intersect with user database or ignore database in the action

Answer: C
Explanation:

QUESTION NO: 292

UDP packets are delivered if they are _____.

A. A legal response to an allowed request on the inverse UDP ports and IP
B. A Stateful ACK to a valid SYN-SYN-/ACK on the inverse UDP ports and IP
C. Reference in the SAM related Dynamic tables
D. Bypassing the Kernel by the “forwarding layer” of clusterXL

Answer: A
Explanation:

QUESTION NO: 293

Whitfield Diffie and martin Hellman gave their names to what standard?

A. An encryption scheme that makes pre-shared keys obsolete
B. An algorithm that is used in IPsec QuickMode and as an additional option in IPsec QuickMode (PFS)
C. A key exchange protocol for the advanced Encryption Standard
D. A key agreement/ derivation protocols the constructs secure keys over an insecure channel

Answer: D
Explanation:

QUESTION NO: 294

What happens in relation to the CRL cache after a cpstop and cpstart have been initiated?

A. The Gateway retrieves a new CRL on startup, and discards the old CRL as invalid.
B. The Gateway continuous to use the old CRL, as long as it is valid.
C. The Gateway continuous to use the old CRL even if it is not valid, until a new CRL is cashed.
D. The Gateway issues a crl_zap on startup, which empties the cache and forces certificate retrieval.

Answer: B

QUESTION NO: 295

What information is found in the Smartview Tracker management log?

A. Rule author
B. TCP handshake average duration
C. TCP source port
D. Top used QOS rule

Answer: C

Explanation:

QUESTION NO: 296

What rulers send log information to Dshield .org when strom centre is configured?

A. Determine in IPS, Dshield storm center configuration. Security management server sends logs from rules with tracking set to either alert or one of the specific User Defined Alerts
B. Determine by the global properties configuration: log defined in the Log and Alerts section, rules with tracking set to account or SNMP trap
C. Determine the Web intelligence, configuration: information Disclosure is configured; rules with tracking sets to User defined Alerts or SNMP trap
D. Determined by the Dshield Storm Center Logging setting in the Logs and Masters of the security Management server object rules with tracking set to Log or None

Answer: A

Explanation:

QUESTION NO: 297

Your current checkpoint Enterprise consists of one Management Server and Four Gateways in four different locations with the following versions.

All devices are running secure platform. You are upgrading your enterprise to R71. Place the required tasks from the following list in the correct order for upgrading your enterprise to R71.

1) Upgrade all gateways to R71

2) Upgrade all gateways 3 and 4 to R 65

3) Upgrade all gateways 2, 3, and 4 to R 65

4) Upgrade all gateway 4 to R 65

5) Perform pre-upgrade verifier on Security management server

6) Perform pre-upgrade verifier on all Gateways

7) Perform License upgrade checker on Gateway 2

8) Perform License upgrade checker on Gateway 3

9) Perform License upgrade checker on Gateway 4

10) Perform License upgrade checker on Security Management Server

11) Perform License upgrade checker on all devices

12) Upgrade security management server to R 70

A. 11, 5, 12, 3, 1
B. 9, 4, 5, 12, 1
C. 5, 6, 12, 1
D. 11, 5, 12, 2, 1

Answer: C
Explanation:

QUESTION NO: 298

Which of these security policy Changes Optimize security Gateway performances?

A. Use automatic NAT rules instead of manual NAT rules when ever possible
B. Putting the Least-Used rule at the top o of the rule Base
C. Using groups within groups in the manual Nat Rule Base
D. Using Domain objects in rules when possible

Answer: D
Explanation:

QUESTION NO: 299

How can you most quickly reset secure internal communication (SIC) between a security management server and security Gateway

A. Run the command fwm sic-reset to initialize the internal certificate authority (ICA) of the security gateway. This will automatically Sync SIC to both the Security management
B. activation key on the security gateway from the SmartDashboard
C. From cpconfig in the Gateway, choose the Secure Internal Communication option and retype the activation key. Next retype the same key in the gateway object in the SmartDashboard and reinitialize secure internal communication (SIC)
D. From the Security Management Server's command line, Type fw putkey –p <shared key> < IP Address of security Gateway>.

Answer: C
Explanation:

QUESTION NO: 300

You installed security management server in a computer using SecurePlatform in the Mega corp home office. You use IP address 10.1.1.1. You also installed the security Gateway on a second secure platform computer, which you plan to ship to an other administrator at a mega corp Hub office. What is in the correct order for pushing SIC certificates to the Gateway before shipping it

1) Run cpconfig on the gateway, set secure internal communication, enter the activation key and reconfirm.

2) Initialize internal certificate authority (ICA) on the security Management server.

3) Confirm the gateway object with the host name and IP address for the remote site.

4) Click the communication button in the gateway object's general screen, enter the activation key, and click initialize and ok.

5) Install the security policy.

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

Answer: B
Explanation:

QUESTION NO: 301

Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is best to accomplish this task?

A. Watch his IP in SmartView monitor by setting an alert action to any packet that matches your Rule base and his IP Address for inbound and outbound traffic.
B. Use Smart View tracker to follow his actions by filtering log entries that feature the WinSCP source or destination port. Then, export the corresponding entries to a separate log file for documentation.
C. Use SmartDashboard to add a rule in the firewall rule Base that matches his IP address and those of potential target and suspucious9 protocols. Apply the alert action or customized messaging.
D. Send the suspect an email with a key logging Trojan attached, to get direct information about his wrong doing

Answer: A
Explanation:

QUESTION NO: 302

Security Gateway R71 supports user authentication for which of the following services? Select the response below that contains the most complete lost of supported services.

A. FTP, HTTP, TELNET
B. FTP, TELNET
C. SMTP, FTP, HTTP, TELNET
D. SMTP, FTP, TELNET

Answer: A
Explanation:

QUESTION NO: 303

In a distributed management environment, the administrator has removed all default check boxes from the Policy > Global Properties > Firewall tab. In order for the Security Gateway to send logs to the Security Management Server, an explicit rule must be created to allow the SeiNrity Gateway to communicate to the Security Management Server on port_____.

A. 259
B. 257
C. 900
D. 256

Answer: B
Explanation:

NEW QUESTIONS

QUESTION NO: 304

You need to plan the company's new security system. The company needs a very high level of security and also high performance and high throughput for their applications. You need to turn on most of the integrated IPS checks while maintaining high throughput. What would be the BEST solution for this scenario?

A. You need to buy a strong multi-core machine and run R70 or later on SecurePlatform with CoreXL technology enabled.
B. Bad luck, both together can not be achieved.
C. The IPS does not run when CoreXL is enabled.
D. The IPS system does not affect the firewall performance and CoreXL is not needed in this scenario.

Answer: A
Explanation:

QUESTION NO: 305

Once installed, the R71 kernel resides directly below which layer of the OSI model?

Note: Application is the top and Physical is the bottom of the IP stack.

A. Network
B. Transport
C. Data Link
D. Session

Answer: A
Explanation:

QUESTION NO: 306

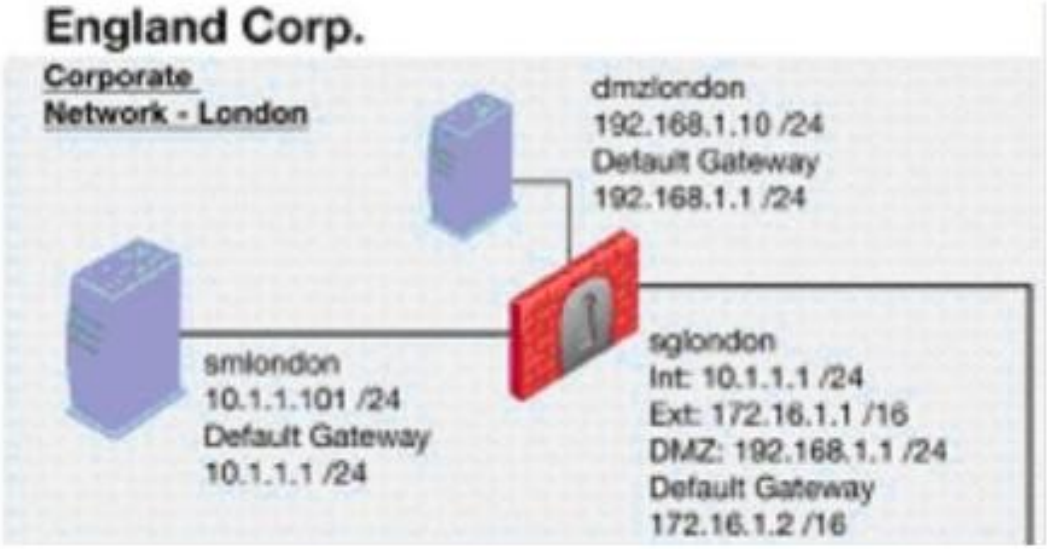
How can you reset the password of the Security Administrator that was created during initial installation of the Security Management Server on SecurePlatform?

A. Type cpm -a, and provide the existing administrator's account name. Reset the Security Administrator's password.
B. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the "Password" portion of the file. Then log in to the account without a password. You will be prompted to assign a new password.
C. Launch SmartDashboard in the User Management screen, and edit the cpconfig administrator.
D. Type fwm -a, and provide the existing administrator's account name. Reset the Security Administrator's password.

Answer: D
Explanation:

QUESTION NO: 307

The Administrator of the London Security Gateway has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect. Which troubleshooting suggestion will NOT help him?



A. Verify that the Rule Base explicitly allows management connections.
B. Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.
C. Verify the SIC initialization.
D. Check if some intermediate network device has a wrong routing table entry, VLAN assignment, duplex-mismatch, or trunk issue.

Answer: A
Explanation:

QUESTION NO: 308

When restoring R71 using the upgrade_ import command, which of the following items is NOT restored?

A. Licenses
B. Global properties
C. SIC Certificates
D. Route tables

Answer: D

Explanation:

QUESTION NO: 309

Which operating systems are supported by a Check Point Security Gateway on an open server?

A. Check Point SecurePlatform and Microsoft Windows
B. Sun Solaris, Red Hat Enterprise Linux, Check Point SecurePlatform, IPSO, Microsoft Windows
C. Check Point SecurePlatform, IPSO, Sun Solaris, Microsoft Windows
D. Microsoft Windows, Red Hat Enterprise Linux, Sun Solaris, IPSO

Answer: A
Explanation:

QUESTION NO: 310

Your network is experiencing connectivity problems and you want to verify if routing problems are present. You need to disable the firewall process but still allow routing to pass through the Gateway running on an IP Appliance running IPSO. What command do you need to run after stopping the firewall service?

A. fw fwd routing
B. ipsofwd on admin
C. fw load routed
D. ipsofwd slowpath

Answer: B
Explanation:

QUESTION NO: 311

ALL of the following options are provided by the SecurePlatform sysconf ig utility, EXCEPT:

A. DHCP Server configuration
B. GUI Clients
C. Time & Date
D. Export setup

Answer: B

Explanation:

QUESTION NO: 312

Your company is running Security Management Server R71 on SecurePlatform, which has been migrated through each version starting from Check Point 4.1. How do you add a new administrator account?

A. Using SmartDashboard, under Users, select Add New Administrator
B. Using the Web console on SecurePlatform under Product configuration, select Administrators
C. Using SmartDashboard or cpconf ig
D. Using cpconftg on the Security Management Server, choose Administrators

Answer: A

Explanation:

QUESTION NO: 313

The command fw fetch causes the:

A. Security Gateway to retrieve the user database information from the tables on the Security Management Server.
B. Security Gateway to retrieve the compiled policy and inspect code from the Security C. Management Server and install it to the kernel.
C. Security Management Server to retrieve the debug logs of the target Security Gateway.
D. Security Management Server to retrieve the IP addresses of the target Security Gateway.

Answer: B

Explanation:

QUESTION NO: 314

Which of the following provides confidentiality services for data and messages in a Check Point VPN?

A. Cryptographic checksums
B. Digital signatures

C. Asymmetric Encryption
D. Symmetric Encryption

Answer: D

Explanation:

QUESTION NO: 315

You wish to configure an IKE VPN between two R71 Security Gateways, to protect two networks. The network behind one Gateway is 10.15.0.0/16, and network 192.168.9.0/24 is behind the peer's Gateway. Which type of address translation should you use to ensure the two networks access each other through the VPN tunnel?

A. Hide NAT
B. Static NAT
C. Manual NAT
D. None

Answer: D

Explanation:

QUESTION NO: 316

Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

A. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
B. All is fine and can be used as is.
C. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
D. The 2 algorithms do not have the same key length and so don't work together. You will get the error ".... No proposal chosen...."

Answer: C

Explanation:

QUESTION NO: 317

For VPN routing to succeed, what must be configured?

A. VPN routing is not configured in the Rule Base or Community objects. Only the native-routing mechanism on each Gateway can direct the traffic via its VTI configured interfaces.
B. No rules need to be created; implied rules that cover inbound and outbound traffic on the central (HUB) Gateway are already in place from Policy > Properties > Accept VPN-1 Control Connections.
C. At least two rules in the Rule Base must be created, one to cover traffic inbound and the other to cover traffic outbound on the central (HUB) Security Gateway.
D. A single rule in the Rule Base must cover all traffic on the central (HUB) Security Gateway for the VPN domain.

Answer: D
Explanation:

QUESTION NO: 318

If Henry wanted to configure Perfect Forward Secrecy for his VPN tunnel, in which phase would he be configuring this?

A. Aggressive Mode
B. Diffie-Hellman
C. Phase 2
D. Phase 1

Answer: C
Explanation:

QUESTION NO: 319

You enable Automatic Static NAT on an internal host node object with a private IP address of 10.10.10.5, which is NATed into 216.216.216.5. (You use the default settings in Global Properties > NAT.)

When you run fw monitor on the R71 Security Gateway and then start a new HTTP connection from host 10.10.10.5 to browse the Internet, at what point in the monitor output will you observe

the HTTP SYN-ACK packet translated from 216.216.216.5 back into 10.10.10.5?

A. i=inbound kernel, before the virtual machine
B. O=outbound kernel, after the virtual machine
C. o=outbound kernel, before the virtual machine
D. I=inbound kernel, after the virtual machine

Answer: D
Explanation:

QUESTION NO: 320

Which command allows verification of the Security Policy name and install date on a Security Gateway?

A. fw show policy
B. fw ctl pstat -policy
C. fw stat -l
D. fwver-p

Answer: C
Explanation:

QUESTION NO: 321

Which answers are TRUE? Automatic Static NAT CANNOT be used when:

(i) NAT decision is based on the destination port.

(ii) Source and Destination IP both have to be translated.

(iii) The NAT rule should only be installed on a dedicated Gateway.

(iv) NAT should be performed on the server side.

A. (iii) and (iv)
B. (i), (iii) and (iv)
C. (ii) and (iii)
D. only (i)

Answer: D

Explanation:

QUESTION NO: 322

When translation occurs using automatic Hide NAT, what also happens?

A. Nothing happens.
B. The source port is modified.
C. The destination port is modified.
D. The destination is modified.

Answer: B
Explanation:

QUESTION NO: 323

Which of the following statements BEST describes Check Point's Hide Network Address Translation method?

A. Many-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation
B. Translates many destination IP addresses into one destination IP address
C. Translates many source IP addresses into one source IP address
D. One-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation

Answer: C
Explanation:

QUESTION NO: 324

Which R71 feature or command allows Security Administrators to revert to earlier versions of the Security Policy without changing object configurations?

A. fwm dbexport/fwm dbimport
B. Policy Package management
C. upgrade_export/upgrade„import
D. Database Revision Control

Answer: B

Explanation:

QUESTION NO: 325

A Hide NAT rule has been created which includes a source address group often (10) networks and three (3) other group objects (containing 4, 5, and 6 host objects respectively). Assuming all addresses are non-repetitive, how many effective rules have you created?

A. 1
B. 25
C. 2
D. 13

Answer: B

Explanation:

QUESTION NO: 326

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

A. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
B. Anti-spoofing not configured on the interfaces on the Gateway object.
C. A Gateway object created using the Check Point > Security Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.
D. Secure Internal Communications (SIC) not configured for the object.

Answer: A

Explanation:

QUESTION NO: 327

You have configured a remote site Gateway that supports your boss's access from his home office using a DSL dialup connection. Everything worked fine yesterday, but today all connectivity is lost. Your initial investigation results in "nobody has touched anything", which you can support by

taking a look in SmartView Tracker Management. What is the problem and what can be done about it?

A. You cannot use NAT and a dialup connection.
B. The NAT configuration is not correct; you can only use private IP addresses in a static NAT setup.
C. A static NAT setup may not work with DSL, since the external IP may change. Hide NAT behind the Gateway is the preferred method here.
D. According to published limitations of Security Gateway R71, there's a bug with NAT. A restart of the Gateway will help here.

Answer: C
Explanation:

QUESTION NO: 328

A host on the Internet initiates traffic to the Static NAT IP of your Web server behind the Security Gateway. With the default settings in place for NAT, the initiating packet will translate the_____.

A. source on client side
B. destination on server side
C. destination on client side
D. source on server side

Answer: C
Explanation:

QUESTION NO: 329

When you use the Global Properties' default settings on R71, which type of traffic will be dropped if no explicit rule allows the traffic?

A. SmartUpdate connections
B. Firewall logging and ICA key-exchange information
C. Outgoing traffic originating from the Security Gateway
D. RIP traffic

Answer: D
Explanation:

QUESTION NO: 330

A Stealth rule is used to:

A. Use the Security Gateway to hide the border router from internal attacks.
B. Cloak the type of Web server in use behind the Security Gateway.
C. Prevent communication to the Security Gateway itself.
D. Prevent tracking of hosts behind the Security Gateway.

Answer: C
Explanation:

QUESTION NO: 331

SmartView Tracker logs the following Security Administrator activities, EXCEPT:

A. Administrator login and logout
B. Object creation, deletion, and editing
C. Tracking SLA compliance
D. Rule Base changes

Answer: C
Explanation:

QUESTION NO: 332

You are working with three other Security Administrators. Which SmartConsole component can be used to monitor changes to rules or object properties made by the other administrators?

A. Eventia Monitor
B. SmartView Monitor
C. SmartView Tracker
D. Eventia Tracker

Answer: C
Explanation:

QUESTION NO: 333

Which SmartView Tracker mode allows you to read the SMTP e-mail body sent from the Chief Executive Officer (CEO) of a company?

A. This is not a SmartView Tracker feature.
B. Display Payload View
C. Display Capture Action
D. Network and Endpoint Tab

Answer: A
Explanation:

QUESTION NO: 334

One of your remote Security Gateway's suddenly stops sending logs, and you cannot install the Security Policy on the Gateway. All other remote Security Gateways are logging normally to the Security Management Server, and Policy installation is not affected. When you click the Test SIC status button in the problematic Gateway object you receive an error message. What is the problem?

A. There is no connection between the Security Management Server and the remote Gateway. Rules or routing may block the connection.
B. The remote Gateway's IP address has changed, which invalidates the SIC Certificate.
C. The time on the Security Management Server's clock has changed, which invalidates the remote Gateway's Certificate.
D. The Internal Certificate Authority for the Security Management Server object has been removed from objects_5_0.C.

Answer: A
Explanation:

QUESTION NO: 335

Where can an administrator specify the notification action to be taken by the firewall in the event that available disk space drops below 15%?

A. Real Time Monitor > Gateway Settings > Status Monitor

B. SmartView Tracker > Audit Tab > Gateway Counters
C. This can only be monitored by a user-defined script.
D. SmartView Monitor > Gateway Status > Threshold Settings

Answer: D
Explanation:

QUESTION NO: 336

Which R71 component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

A. Smart Event
B. SmartView Monitor
C. SmartView Status
D. SmartUpdate

Answer: B
Explanation:

QUESTION NO: 337

For which protocol is anti-virus not available?

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

Answer: C
Explanation:

QUESTION NO: 338

For remote user authentication, which authentication scheme is NOT supported?

A. SecurID
B. TACACS

C. Check Point Password
D. RADIUS

Answer: B
Explanation:

QUESTION NO: 339

What happens to evaluation licenses during the license-upgrade process?

A. They are dropped.
B. They remain untouched, but may not activate all features of a new version.
C. They automatically expire.
D. They are upgraded with new available features.

Answer: B
Explanation:

QUESTION NO: 340

Which of the following statements about service contracts, i.e., Certificate, software subscription, or support contract, is FALSE?

A. A service contract can apply only for a single set of Security Gateways managed by the same Security Management Server.
B. The contract file is stored on the Security Management Server and downloaded to all Security Gateways during the upgrade process.
C. Most software-subscription contracts are permanent, and need not be renewed after a certain time passes.
D. Service Contracts can apply for an entire User Center account.

Answer: C
Explanation:

QUESTION NO: 341

All R71 Security Servers can perform authentication with the exception of one. Which of the Security Servers cannot perform authentication?

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

Answer: C
Explanation:

QUESTION NO: 342

What is the difference between Standard and Specific Sign On methods?

A. Standard Sign On allows the user to be automatically authorized for all services that the rule allows, but re-authenticate for each host to which he is trying to connect. Specific Sign On requires that the user re-authenticate for each service.
B. Standard Sign On requires the user to re-authenticate for each service and each host to which he is trying to connect. Specific Sign On allows the user to sign on only to a specific IP address.
C. Standard Sign On allows the user to be automatically authorized for all services that the rule allows. Specific Sign On requires that the user re-authenticate for each service and each host to which he is trying to connect.
D. Standard Sign On allows the user to be automatically authorized for all services that the rule allows. Specific Sign On requires that the user re-authenticate for each service specifically defined in the window Specific Action Properties.

Answer: C
Explanation:

QUESTION NO: 343

Which column in the Rule Base is used to define authentication parameters?

A. Source
B. Action
C. Track
D. Service

Answer: B
Explanation:

QUESTION NO: 344

Identify the ports to which the Client Authentication daemon listens by default.

A. 8080, 529
B. 259,900
C. 80, 256
D. 256,600

Answer: C
Explanation:

QUESTION NO: 345

If a Security Gateway enforces three protections, LDAP Injection, Malicious Code Protector, and Header Rejection, which Check Point license is required in SmartUpdate?

A. Data Loss Prevention
B. SmartEvent Intro
C. SSL: VPN
D. IPS

Answer: D
Explanation:

QUESTION NO: 346

R7Ts INSPECT Engine inserts itself into the kernel between which two layers of the OSI model?

A. Presentation and Application
B. Physical and Data
C. Session and Transport
D. Data and Network

Answer: A
Explanation:

QUESTION NO: 347

Your R71 primary Security Management Server is installed on SecurePlatform. You plan to schedule the Security Management Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Open the primary Security Management Server object's Logs and Masters window, enable Schedule log switch, and select the Time object.
B. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masters window, enable Schedule log switch, and select the Time object.
C. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.
D. On a SecurePlatform Security Management Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.

Answer: A
Explanation:

QUESTION NO: 348

Which command is used to uninstall the Security Policy directly from the Security Gateway?

A. fwm unload.local
B. cpstop
C. fwm load <gtwynames-IP> NULL
D. fw unloadlocal

Answer: D
Explanation:

QUESTION NO: 349

Which of these attributes would be critical for a site-to-site VPN?

A. Strong authentication
B. Centralized management
C. Strong data encryption
D. Scalability to accommodate user groups

Answer: C
Explanation:

QUESTION NO: 350

What statement is true regarding Visitor Mode?

A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
B. All VPN traffic is tunneled through UDP port 4500.
C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
D. Only ESP traffic is tunneled through port TCP 443.

Answer: A
Explanation:

QUESTION NO: 351

How does the Get Address button, found on the Host Node Object > General Properties page retrieve the address?

A. Route Table
B. SNMP Get
C. Address resolution (ARP. RARP)
D. Name resolution (hosts file, DNS, cache)

Answer: D
Explanation:

QUESTION NO: 352

Static NAT connections, by default, translate on which inspection point of the firewall kernel?

A. Outbound
B. Eitherbound
C. Inbound
D. Post-inbound

Answer: C
Explanation:

QUESTION NO: 353

You are about to test some rule and object changes suggested in an R71 newsgroup. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. upgrade export command
B. Manual copies of the SFWDIR/conf directory
C. SecurePlatform backup utilities
D. Database Revision Control

Answer: D
Explanation:

QUESTION NO: 354

Which Check Point address translation method is necessary if you want to connect from a host on the Internet via HTTP to a server with a reserved (RFC 1918) IP address on your DMZ?

A. Static Destination Address Translation
B. Port Address Translation
C. Dynamic Source Address Translation
D. Hide Address Translation

Answer: A
Explanation:

QUESTION NO: 355

You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error: "Unknown established connection"

How do you resolve this problem without causing other security issues? Choose the BEST answer.

A. Increase the service-based session timeout of the default Telnet service to 24-hours.
B. Create a new TCP service object on port 23 called Telnet-mainframe. Define a service-based

session Timeout of 24-hours. Use this new object only in the rule that allows the Telnet connections to the mainframe.
C. Ask the mainframe users to reconnect every time this error occurs.
D. Increase the TCP session timeout under Global Properties > Stateful Inspection.

Answer: B
Explanation:

QUESTION NO: 356

After installing Security Gateway R71, you discover that one port on your Intel Quad NIC on the Security Gateway is not fetched by a Get Topology request. What is the most likely cause and solution?

A. Your NIC driver is installed but was not recognized. Apply the latest SecurePlatform R71 Hotfix Accumulator (HFA).
B. The NIC is faulty. Replace it and reinstall.
C. Make sure the driver for your particular NIC is available, and reinstall. You will be prompted for the driver.
D. If an interface is not configured, it is not recognized. Assign an IP address and subnet mask using the WebUI.

Answer: D
Explanation:

QUESTION NO: 357

Which of the following objects is a valid source in an authentication rule?

A. User@Network
B. User@Any
C. Host@Any
D. User_group@Network

Answer: D
Explanation:

QUESTION NO: 358

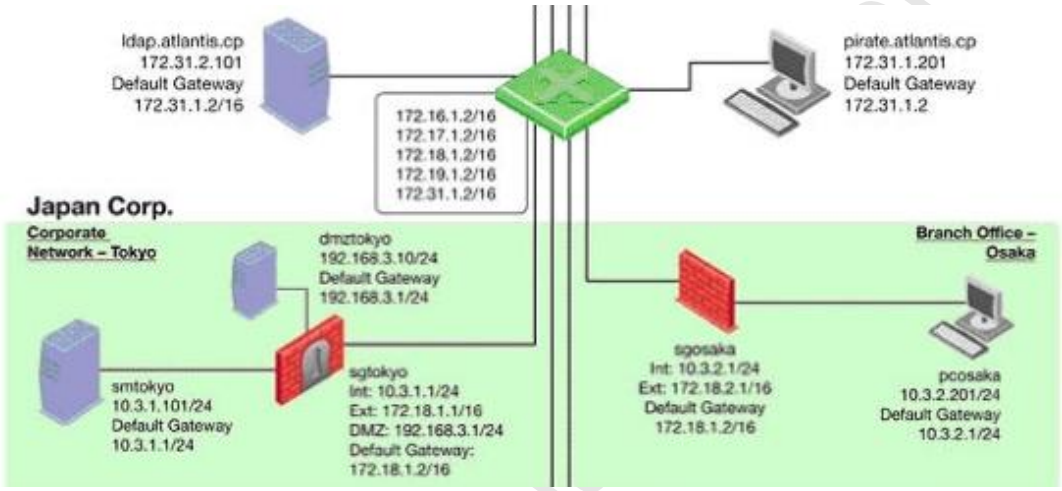
Which of these components does NOT require a Security Gateway R71 license?

A. SmartUpdate upgrading/patching
B. Security Management Server
C. SmartConsole
D. Check Point Gateway

Answer: C
Explanation:

QUESTION NO: 359

The Administrator of the Tokyo Security Management Server cannot connect from his workstation in Osaka. Which of the following lists the BEST sequence of steps to troubleshoot this issue?



A. Check for matching OS and product versions of the Security Management Server and the client. Then, ping the Gateways to verify connectivity. If successful, scan the log files for any denied management packets.
B. Call Tokyo to check if they can ping the Security Management Server locally. If so, login to sgtokyo, verify management connectivity and Rule Base. If this looks okay, ask your provider if they have some firewall rules that filters out your management traffic.
C. Verify basic network connectivity to the local Gateway, service provider, remote Gateway, remote network and target machine. Then, test for firewall rules that deny management access to the target. If successful, verify that pcosaka is a valid client IP address.
D. Check the allowed clients and users on the Security Management Server. If pcosaka and your user account are valid, check for network problems. If there are no network related issues, this is likely to be a problem with the server itself. Check for any patches and upgrades. If still unsuccessful, open a case with Technical Support.

Answer: C
Explanation:

QUESTION NO: 360

How many inspection capture points are shown in fw monitor?

A. 2
B. 1
C. Depends on the number of interfaces on the Gateway
D. 4

Answer: D
Explanation:

QUESTION NO: 361

Looking at an fw monitor capture in Wireshark, the initiating packet in Hide NAT translates on_____.

A. I
B. O
C. o
D. i

Answer: B
Explanation:

QUESTION NO: 362

Which of the following statements accurately describes the snapshot command?

A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a SecurePlatform Security Gateway.
B. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.
C. snapshot creates a full system-level backup of the Security Management Server on any OS
D. snapshot stores only the system-configuration settings on the Gateway.

Answer: A

Explanation:

QUESTION NO: 363

What is a possible reason for the IKE failure shown in this screenshot?

A. Mismatch in VPN Domains.
B. Mismatch in Diffie-Hellman group.
C. Mismatch in encryption schemes.
D. Mismatch in preshared secrets.

Answer: D

Explanation:

QUESTION NO: 364

Which statement is TRUE about implicit rules?

A. They are derived from Global Properties and explicit object properties.
B. The Gateway enforces implicit rules that enable outgoing packets only.
C. You create them in SmartDashboard.
D. Changes to the Security Gateway's default settings do not affect implicit rules.

Answer: A

Explanation:

QUESTION NO: 365

Which item below in a Security Policy would be enforced first?

A. Administrator-defined Rule Base
B. Network Address Translation
C. IP spoofing/IP options
D. Security Policy "First" rule

Answer: C

Explanation:

QUESTION NO: 366

Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services. Which of the following configurations will allow this network to access the Internet?

A. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service
B. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24
C. Configure Automatic Hide NAT on network 10.10.20.0/24 and then edit the Service column in the NAT Rule Base on the automatic rule
D. Configure Automatic Static NAT on network 10.10.20.0/24

Answer: B

Explanation:

QUESTION NO: 367

Review the rules in the graphic. Assume domain UDP is enabled in the implied rules.

What happens when a user from the internal network tries to browse to the Internet using HTTP? The user:

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Customers@Any	* Any	* Any Traffic	TCP http TCP ftp	User Auth	Log
2		* Any	* Any	* Any Traffic	* Any	accept	- None

A. is prompted three times before connecting to the Internet successfully.
B. can go to the Internet after Telnetting to the client auth daemon port 259.
C. can connect to the Internet successfully after being authenticated.
D. can go to the Internet, without being prompted for authentication.

Answer: D

Explanation: