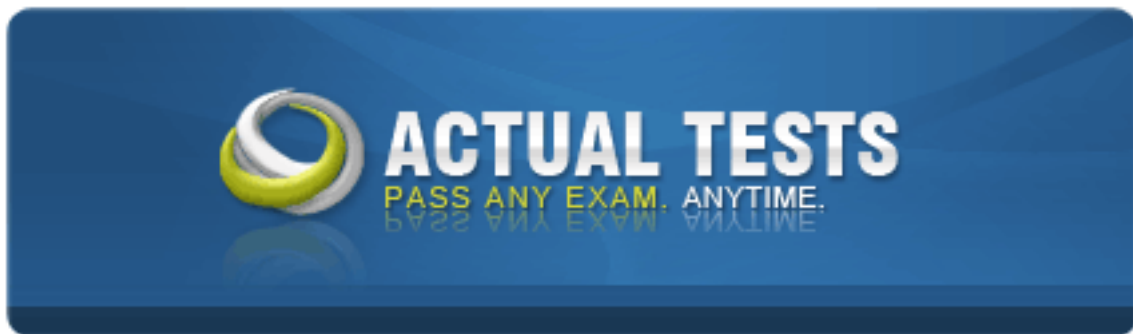


Checkpoint 156-915-71



Check Point Certified Security Expert R71 Update

Practice Test

Version: 4.0

QUESTION NO: 1

Which SmartEvent, what is the Correlation Unit's function?

- A. Invoke and define automatic reactions and add events to the database
- B. Assign severity levels to events
- C. Display received threats and tune the Events Policy
- D. Analyze log entries, looking for Event Policy patterns

Answer: D

Explanation:

QUESTION NO: 2

How do you verify the Check Point kernel running on a firewall?

- A. fw ctrl get kernel
- B. fw ctrl pstat
- C. fwkernel
- D. fwver -k

Answer: D

Explanation:

QUESTION NO: 3

After repairing a SmartWorkflow session:

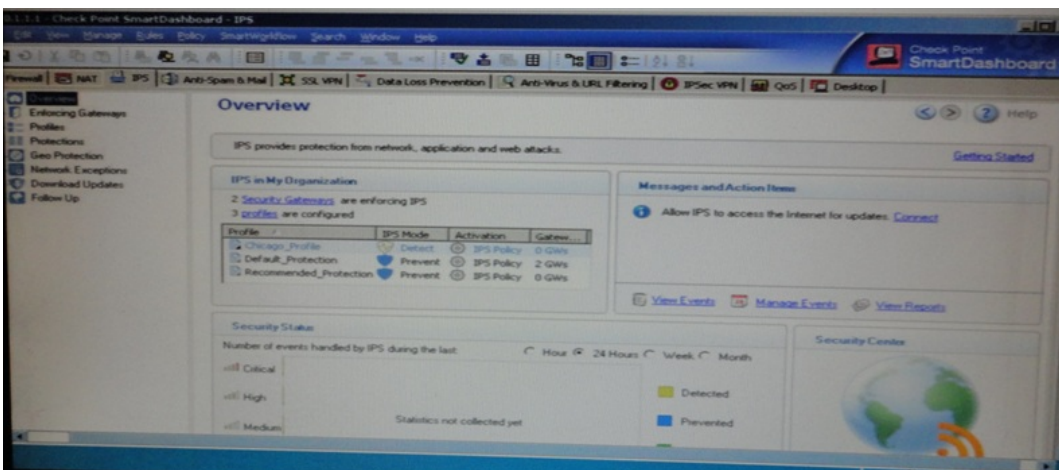
- A. The session moves to status Repaired and a new session can be started
- B. The session moves to status Awaiting Repair and must be resubmitted
- C. The session is continued with status Not approved and a new session must be started
- D. The session is discarded and a new session is automatically started

Answer: B

Explanation:

QUESTION NO: 4

TotallyCoolSecurity Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-Chicagousing Detect mode. After reviewing Matt noticed that fw-Chicagois not detecting any of the IPS protections that Bob had previously setup. Analyze the output below and determine how Mattcorrectsthe problem.



- A. Matt should assign the fw-ChicagoSecurity Gateway to theChicago_Profile.
- B. Matt should theChicago_Profile to useProtect mode because Detect mode
- C. Matt should re-create theChicago_Profile and select Activeprotections manually instead of per theIPSPolicy.
- D. Mattshouldactivatethe Chicago_Profileasitis currently notactivated.

Answer: A

Explanation:

QUESTION NO: 5

Which Remote Desktop protocols are supported natively in SSL VPN?

- A. Microsoft RDP only
- B. AT&T VNC and Microsoft RDP
- C. Citrix ICA and Microsoft RDP
- D. AT&T VNC, Citrix ICA and Microsoft RDP

Answer: D

Explanation:

QUESTION NO: 6

To force clients to use integritySecurity Workspace when accessing sensitive applications, the Administrator can configure Connectra:

- A. Via protection levels
- B. To implement integrity Clientless Security
- C. To force the user to re-authenticate at login
- D. Without a special setting. Secure Workspace is automatically configured.

Answer: A

Explanation:

QUESTION NO: 7

The default port for browser access to the Management Portal is

- A. 4433
- B. 4343
- C. 8080
- D. 443

Answer: A

Explanation:

QUESTION NO: 8

In which case is a Sticky Decision Function relevant?

- A. Load Sharing - Unicast
- B. Load Balancing - Forward
- C. High Availability
- D. Load Sharing - Multicast

Answer: D

Explanation:

QUESTION NO: 9

You just upgraded to R71 and are using the IPS Software Blade. You want to enable all critical protections while keeping the rate of false positives very low. How can you achieve this?

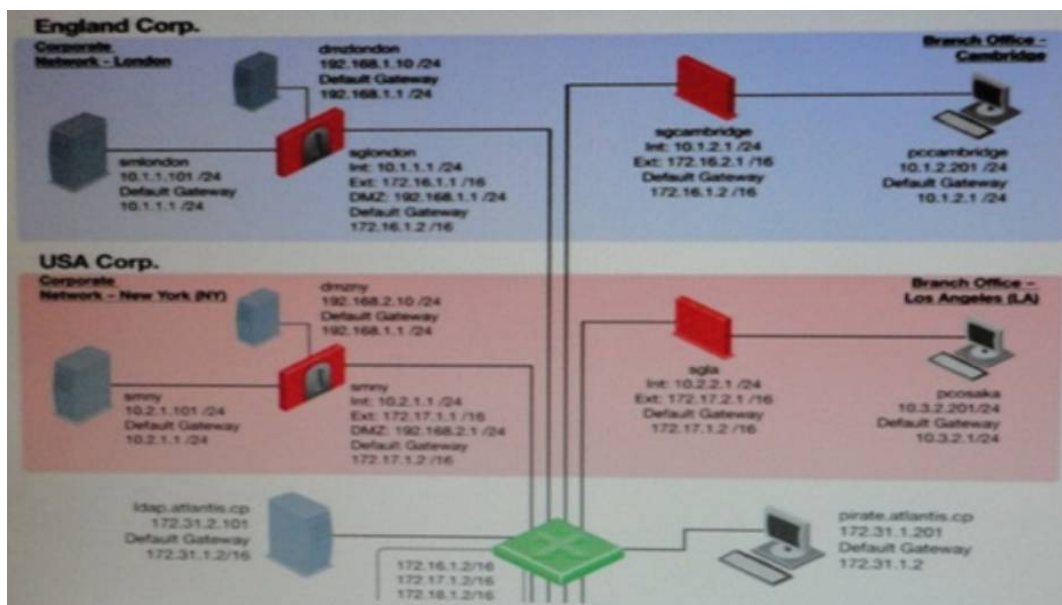
- A. The new IPS system is based on policies, but it has no ability to calculate or change the confidence level, so it always has a high rate of false positives.
- B. This can't be achieved; activating any IPS system always causes a high rate of false positives.
- C. The new IPS system is based on policies and gives you the ability to activate all checks with critical severity and a high confidence level.
- D. As in SmartDefense, this can be achieved by activating all the critical checks manually.

Answer: C

Explanation:

QUESTION NO: 10

Refer to the network topology below. You have IPS Software Blades active on the Security Gateways *sglondon*, *sgla*, and *sgsny*, but still experience attacks on the Web server in the New York DMZ. How is this possible?



- A. All of these options are possible.
- B. The attacker may have used a bunch of evasion techniques like using escape sequence instead of cleartext commands. It is also possible that there are entry points not shown in the network.

layout, like rogue access points.

C. Since other Gateways do not have IPS activated, attacks may originate from their network without anyone noticing.

D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-turned anomaly algorithms. Even if this is accomplished, no technology can offer 100 % protection.

Answer: C

Explanation:

QUESTION NO: 11

Which of the following is NOT an Smartevent event-triggered Automatic Reaction?

A. Mail

B. Block Access

C. External Script

D. SNMP Trap

Answer: B

Explanation:

QUESTION NO: 12

Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?

A. (i), (ii) and (iv)

B. (i), (iii), (iv)

C. (ii) and (iv)

D. (i) and (ii)

Answer: C

Explanation:

QUESTION NO: 13

What SmartConsole application allows you to change the Log Consolidation Policy?

- A. SmartReporter
- B. SmartUpdate
- C. SmartEvent Server
- D. Smart Dashboard

Answer: A

Explanation:

QUESTION NO: 14

In configure a client to property log in to the user portal using a certificate, the Administrator MUST:

- A. Create an internal user in the admin portal.
- B. Install an R71 internal Certificate Authority certificate.
- C. Create a client certificate from Smart Dashboard
- D. Store the client certificate on the SSL VPN Gateway

Answer: C

Explanation:

QUESTION NO: 15

What process manages the dynamic routing protocols (ospf, RIP, etc) on SecurePlatform Pro?

- A. gated
- B. arouted
- C. routerd
- D. There's no separate process, but the Linux default router can take care of that.

Answer: A

Explanation:

QUESTION NO: 16

To change the default port of the Management Portal,

- A. Edit the masters.conf file on the Portal server.

- B. Modify the file cp_httpd_admin.conf.
- C. Run sysconfig and change the management interface
- D. Re-initializeSIC.

Answer: C

Explanation:

QUESTION NO: 17

Where do Gateways managed by SmartProvisioning fetch their assigned profiles?

- A. The Smartview Monitor
- B. The standalone SmartProvisioning server
- C. The Security Management server or CMA
- D. They are fetched locally from the individual device

Answer: C

Explanation:

QUESTION NO: 18

When synchronizing clusters, which of the following statements is NOT true?

- A. Client Auth or Session Auth connections through a cluster member will be lost if the cluster member fails.
- B. The state of connection using resources is maintained by a Security Server, so there connections cannot be synchronized.
- C. Only cluster members running on the same OS platform can be synchronized.
- D. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.

Answer: D

Explanation:

QUESTION NO: 19

What command will allow you to disable sync on a cluster firewall member?

- A. fw ctl setaync 0
- B. fw ctl syncsatat stop
- C. fw ctl syncstat off
- D. fw ctl setsync off

Answer: D

Explanation:

QUESTION NO: 20

By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:

- A. The Security Policy is saved.
- B. The Security Policy is installed.
- C. The user database is installed.
- D. The standby Security Management Server starts for the first time.

Answer: A

Explanation:

QUESTION NO: 21

A customer is calling saying one member's status is Down. What will you check?

- A. cphaprob list (verify what critical device is down)
- B. Fw ctl debug -m cluster + forward(forwarding layer debug)
- C. tcpdump/snoop (CCP traffic)
- D. fw ctlpstat (check sync)

Answer: A

Explanation:

QUESTION NO: 22

You have a High Availability ClusterXL configuration. Machines are not synchronizer. What happens to connections on failover?

- A. It is not possible to configure High Availability that is not synchronized.
- B. Old connections are lost but can be reestablished.
- C. Connection cannot be established until cluster members are fully synchronized.
- D. Old connections are lost but are automatically recovered whenever the failed machine recovers.

Answer: B

Explanation:

QUESTION NO: 23

When using ClusterXL in load sharing, what method is used by default?

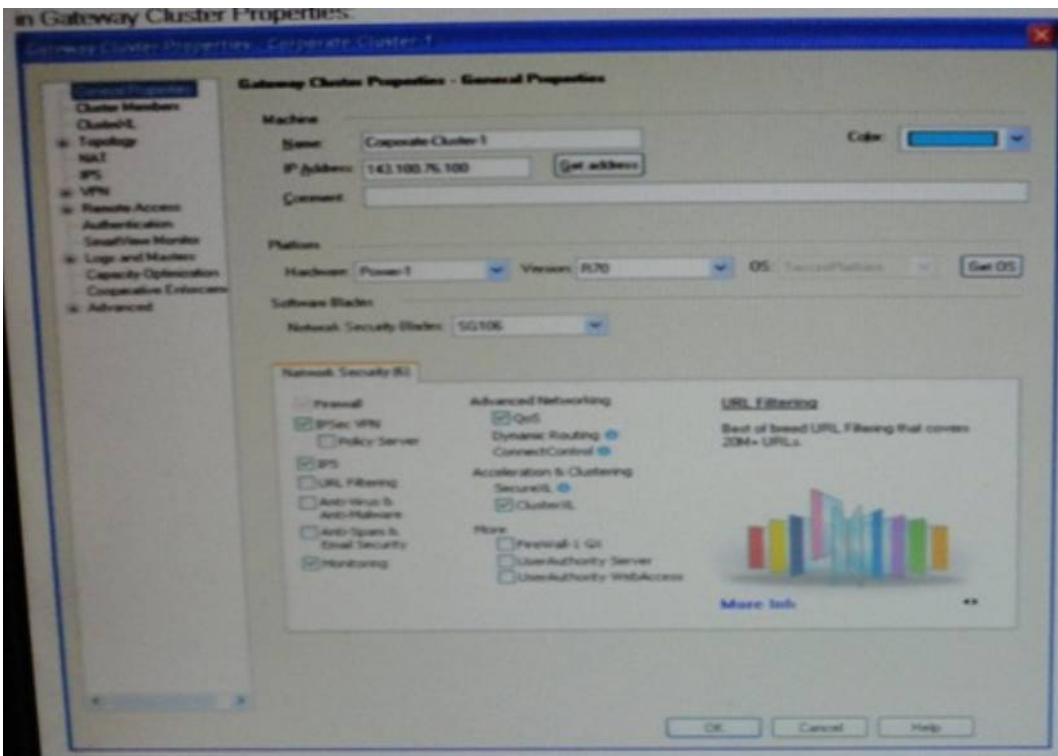
- A. IPs, SPIs
- B. IPs, Ports, SPIs
- C. IPs
- D. IPs, Ports

Answer: C

Explanation:

QUESTION NO: 24

John is configuring a new R17 Gateway cluster but he cannot configure the cluster as Third Party IP Clustering in Gateway Cluster Properties:



What's happening?

- A. John is not using thirdparty hardware as IP Clustering is part of Check Point's IP Appliance.
- B. Third Party Clustering is not available for R71 Security Gateways.
- C. ClusterXL needs to be unselected to permit 3rd party clustering configuration.
- D. John has an invalid ClusterXL license

Answer: C

Explanation:

QUESTION NO: 25

A customer calls saying that a load-sharing cluster shows drops with the error First packet is not SYN. Complete the following sentence. I will recommend:

- A. Change the load on each member.
- B. configuring flush and ack
- C. turning off SDF (Sticky Decision Function)
- D. turning on SDF (Sticky Decision Function)

Answer: D

Explanation:

QUESTION NO: 26

Which at the following commands shows full synchronization status?

- A. cphaprob-illist.
- B. fw ctliflist
- C. Fw hastat
- D. cphaprob-aif

Answer: A

Explanation:

QUESTION NO: 27

If Victor wanted to edit new Signature Protections, what tab would he need to access in Smart Dashboard?

- A. QoS Tab
- B. SmartDefense Tab
- C. IPSec VPN Tab
- D. IPS Tab

Answer: D

Explanation:

QUESTION NO: 28

Due to some recent performance issues, you are asked to add additional processors to your firewall. If you already have CoreXL enabled, how are you able to increase Kernel instances?

- A. Kernel instances are automatically added after process installed and no additional configuration is needed.
- B. In SmartUpdate, right-click on Firewall Object and choose Add Kernel instances.
- C. Once CoreXL is installed you cannot enable additional Kernel instances without reinstalling R71.
- D. Use cpconfig to reconfigure CoreXL.

Answer: D

Explanation:

QUESTION NO: 29

Which of the following is the default port for Management Portal?

- A. 4434
- B. 443
- C. 444
- D. 4433

Answer: D

Explanation:

QUESTION NO: 30

Which of the following is TRUE concerning unnumbered VPNTunnelInterfaces (VTIs)?

- A. VTIs cannot be assigned a proxy interface
- B. Local IP addresses are not configured, remote IP addresses are configured
- C. VTIs can only be physical, not loopback
- D. VTIs are only supported on the IPSO Operating System

Answer: B

Explanation:

QUESTION NO: 31

SSL termination takes place:

- A. In a DMZ and LAN deployment on a Security Gateway
- B. In a DMZ and LAN deployment scenario on a Security Gateway
- C. In a DMZ and LAN deployment scenario on a Connectra Gateway
- D. In a DMZ deployment on a Connectra Gateway

Answer: C

Explanation:

QUESTION NO: 32

Which component functions as the Internal Certificate Authority for R71?

- A. Security Gateway
- B. ManagementServer
- C. Policy Server
- D. SmartLSM

Answer: B

Explanation:

QUESTION NO: 33

Which operating system(s) support(s) unnumbered VPN Tunnel Interface (VTIs) for route-based VPNs?

- A. SecurePlatform for NGX and higher
- B. Solaris 9 and higher
- C. IPSO 3.9 and higher
- D. Red Hat Linux

Answer: A

Explanation:

QUESTION NO: 34

If a Security Gateway enforces these protections, LDAP injection, Malicious Code Protector, and Header Rejection, which Check Point licenses are required in SmartUpdate?

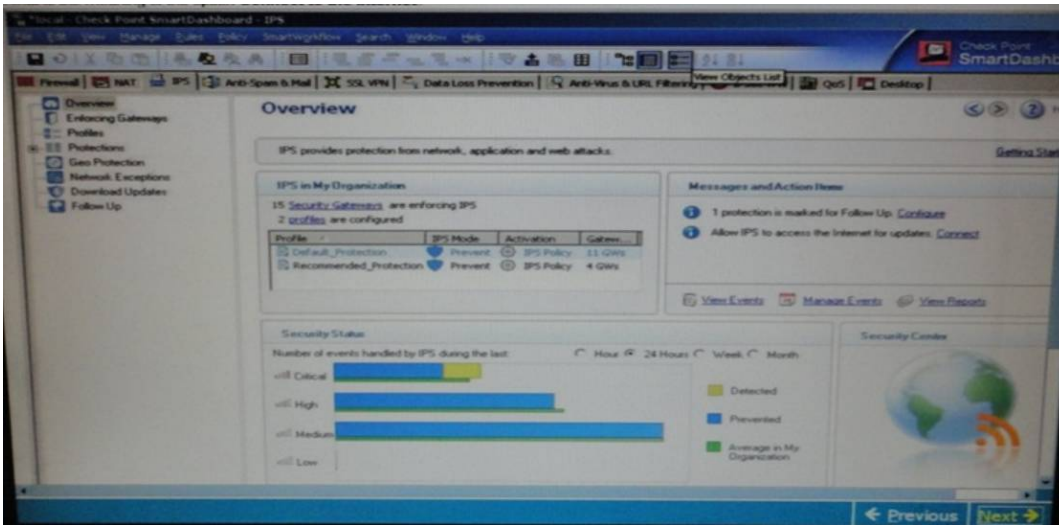
- A. SmartEvent Intro
- B. SSL VPN
- C. Data Loss Prevention
- D. IPS

Answer: D

Explanation:

QUESTION NO: 35

What is meaning of the option Connect to the internet?



- A. Smart Dashboard will retrieve information from Check Point over the Internet. No information will be sent.
- B. Smart Dashboard will retrieve information from Check Point over the Internet. Your information will be sent anonymously to Check Point.
- C. Smart Dashboard will retrieve information from Check Point over the Internet using your User Center login.
- D. Smart Dashboard will retrieve information from Check Point over the Internet.

Answer: C

Explanation:

QUESTION NO: 36

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in SmartReporter?

- A. In SmartReporter, under Express > Network Activity
- B. In SmartReporter, under Standard > Custom
- C. In Smart Dashboard, the SmartView Monitor page in the R71 Security Gateway Object
- D. In SmartView Monitor, under Global Properties > Log and Masters

Answer: C

Explanation:

QUESTION NO: 37

Using IPS, how do you notify the Security Administrator that malware is scanning specific? By enabling:

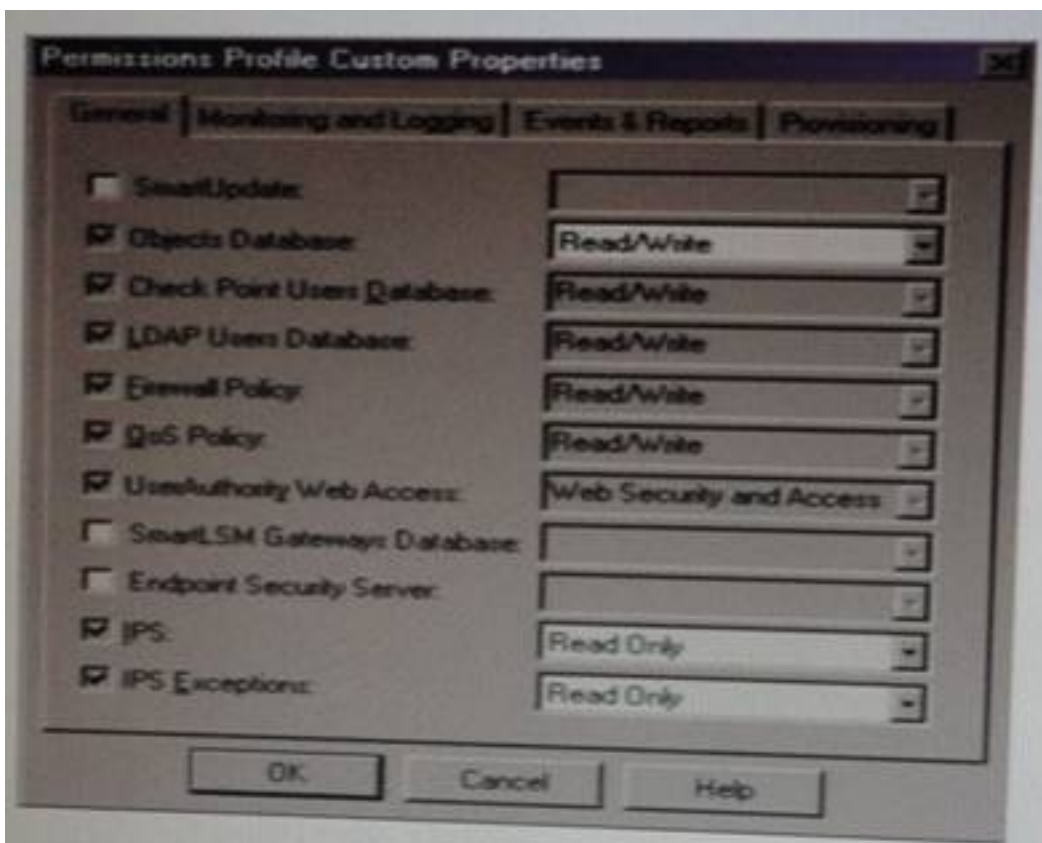
- A. Malware Scan protection
- B. Sweep Scan protection
- C. Host Port Scan
- D. Malicious Codes Protector

Answer: D

Explanation:

QUESTION NO: 38

UserA has the following permissions for SmartConsole:



True or False User A is able to create a SmartLSM Security Cluster Profile. If false, you must select the correct justification.

- A. False. The user must have at least Read permissions for the SmartLSM Gateways Database.

- B. True. Only Object Database Read/Write permissions are required to create SmartLSM Profile.
- C. False. The user must have Read/Write permissions for the SmartLSM Gateways Database.
- D. Not enough information to determine. You must know the user's Provisioning permissions to determine whether they are able to create a SmartLSM Security Cluster Profile

Answer: C

Explanation:

QUESTION NO: 39

Mark the configuration options that are available for Data Loss Prevention in R71.

- A. A Dedicated DLP Gateway running only the DLP Software Blade.
- B. The DLP Gateway running only the Firewall Software Blade.
- C. The DLP Gateway running only the Management Server on the same machine.
- D. the DLP as an integrated software blade, which can be enabled on a Check Point Security Gateway running other software blades such Firewall, IPS and Management.

Answer: A

Explanation:

QUESTION NO: 40

In company XYZ, the DLP Administrator defined a new Keywords Data Type that contains a list of secret project names, i.e. Ayalon, Yarkon, and Yarden. The threshold is set to At least 2 keywords or phrases. Based on this information, which of the following scenarios will be a match to the Rule Base?

- A. PDF file that contains the following text:
Yarkon1 can be the codename for the new product. Yarden's list of protected sites.
- B. An MS Excel file that contains the following text:
More resources for Yarkon project...Are you certain this is about Yarden?
- C. A word file that contains the following text:
Ayalon
ayalon
AYALON
- D. A password protected MS Excel file that contains the following text:
Ayalon
Yarkon
Yarden

Answer: B

Explanation:

QUESTION NO: 41

The CoreXL SND (Secure Network Distributor) is responsible for:

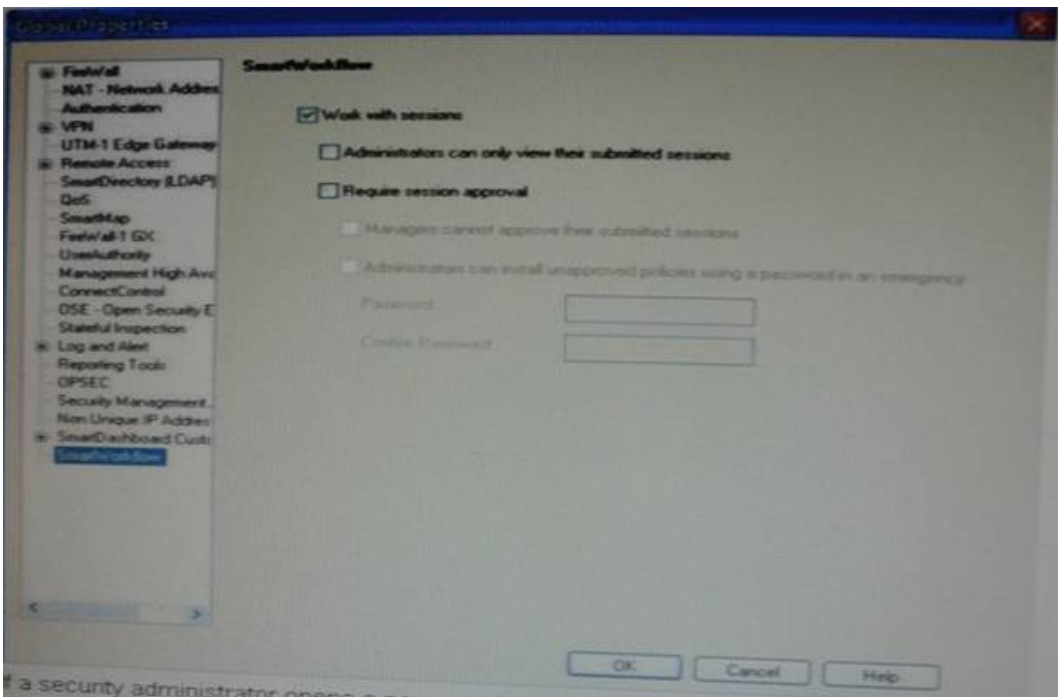
- A. shutting down cores when they are not needed
- B. changing routes to distribute the load across multiple firewalls.
- C. accelerating VPN traffic
- D. distributing non-accelerated packets among kernel instances

Answer: D

Explanation:

QUESTION NO: 42

SmartWorkflow has been enabled with the following configuration:



If a security administrator opens a new session and after making changes to the policy, submits the session for approval. The status of his session will be displayed as:

A. Approved

- B. In progress
- C. Not Approved
- D. Awaiting Approval

Answer: D

Explanation:

QUESTION NO: 43

Which of the following generate a SmartEvent Report from SQL database?

- A. Security Management Server
- B. SmarttEvent Client
- C. SmartReporter
- D. Smart DashboardLog Consolidator

Answer: B

Explanation:

QUESTION NO: 44

What is a task of the SmartEvert Server?

- A. Invoke defined automatic reactions
- B. Analyze each IPS log entry as it enters the Log server
- C. Display the received events
- D. Add events to the events database

Answer: D

Explanation:

QUESTION NO: 45

Among the authentication schemes SSI VPN employs for users, which scheme does Check Point recommended so all servers are replicated?

- A. User certificates
- B. LDAP

- C. Username and password
- D. RADIUS

Answer: B

Explanation:

QUESTION NO: 46

In R71, My Organization e-mail addresses or domains are used for:

- A. Scanning e-mail only if its sender e-mail address is part of this definition, by default
- B. Defining the e-mail address of the SMTP relay server
- C. FTP traffic sent from a user where his e-mail is part of this definition scanned by DLP, by default.
- D. HTTP traffic sent from a user where his e-mail is part of this definition scanned by DLP, by default.

Answer: D

Explanation:

QUESTION NO: 47

A VPN Tunnel Interface (VTI) is defined on SecurePlatform Pro as:

```
Vpn ahell interface add numbered 10.10.0.1 10.10.0.2 madrid.cp
```

What do you know about this VTI?

- A. The peer Security Gateway's name is *madrid.cp*.
- B. The local Gateway's object name is *madrid.cp*.
- C. The VTI name is *madrid.cp*.
- D. 10.10.0.1 is the local Gateway's internal interface, and 10.10.0.2 is the internal interface of the remote Gateway.

Answer: A

Explanation:

QUESTION NO: 48

Which of the following components receives events and assigns severity levels to the events; then

any defined automatic reactions and adds the events to the Events Data Base?

- A. SmartEvent Client
- B. SmartEvent Server
- C. SmartEvent Correlation Unit
- D. SmartEvent Analysis DataServer

Answer: C

Explanation:

QUESTION NO: 49

When deploying dedicated DLP Gateway behind a perimeter firewall on an interface leading to the internal network (there is only one internal network):

- A. The DLP Gateway can inspect SMTP traffic if a MS Exchange server is located on the internal network, and it either sends e-mail directly to the internal using SMTP or sends e-mail to the internal in SMTP via a mail relay that is located on the perimeter's firewall DMZ network.
- B. The DLP Gateway can inspect internal e-mail (e-mail between two users on the internal network) if the organization's internal mail server is located in the internal in the internal network and users are configured to send e-mail to this mail server using SMTP.
- C. User's HTTPS and FTP traffic can be inspected by the R71 DLP Gateway.
- D. The DLP Gateway can inspect e-mail (e-mail between two users on the internal network) if the organization's internal mail server is located on the another network (not the internal network; for instance the DMZ or a different internal network) and users are configured to send e-mail to this mail server using SMTP.

Answer: D

Explanation:

QUESTION NO: 50

Which of the following commands can be used to stop Management Portal services?

- A. fw stopportal
- B. cpportalstop
- C. cpstop/portal
- D. smartportalstop

Answer: D

Explanation:

QUESTION NO: 51

When selecting a backup target using SmartProvisioning, which target is NOT available?

- A. TFTP
- B. Locally on device
- C. SCP
- D. FTP

Answer: A

Explanation:

QUESTION NO: 52

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs must be assigned a proxy interface.
- B. VTIs can only be physical, not loopback
- C. Local IP addresses are not configured, remote IP addresses are configured
- D. VTIs are only supported on SecuredPlatform.

Answer: C

Explanation:

QUESTION NO: 53

To clean the system of all events, you should delete the files in which folder(s)?

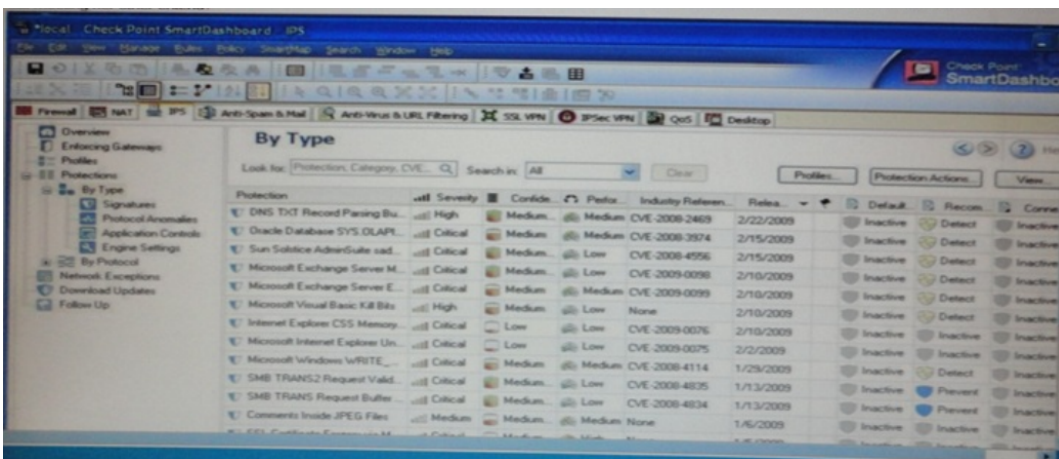
- A. \$PWDIR/distrib
- B. \$FITOIR/events_db
- C. \$PWDIR//distrib and \$PWDIR/events_db
- D. \$FWDIR/distrib_db and \$PVDIR/events

Answer: C

Explanation:

QUESTION NO: 54

Laura notices the Microsoft Visual BasicKill Bits Protection is set to inactive. She wants to set the Microsoft Visual Basic Kill Bits Protection and all other Performance Impact Protections to Prevent. She asks her manager for approval and he started she can turn these on. But he wants Laura to make sure High Performance Impacted Protections are turned on while changing this setting. Using the output below, how would Laura Change the Default_Protection on Performance Impact Protections classified as Low from inactive to Prevent still meeting her other criteria?



- A. GotoProfiles /Default_Protection and uncheck Do not activate protections with performance impact to Medium or Above
- B. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to Low or Above
- C. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to Medium or Above
- D. Go to Profiles / Default_Protection and select Do not activate protections with performance impact to High or Above

Answer: C

Explanation:

QUESTION NO: 55

In the following command LSMcli [-d] <server> <pswd> <action> "server" should be replaced with

- A. Hostname of ROBO gateway
- B. Hostname DAP device
- C. IP address of theSecurity Management server

D. GUclient

Answer: C

Explanation:

QUESTION NO: 56

You use the snapshot feature to store your Connectra SSL VPN configuration. What do you expect to find?

- A. Nothing: snapshot is not supported in Connectra SSL VPN
- B. The management configuration of the current product, a management or stand-alone machine
- C. A complete image of the local file system
- D. Specified directories of the local file system

Answer: C

Explanation:

QUESTION NO: 57

Date type = Large file (>500KB)

Source = My organization

Protocol = any

Action = ask user

All other rules are set to detect. Usercheck is enabled and installed on all client machines.

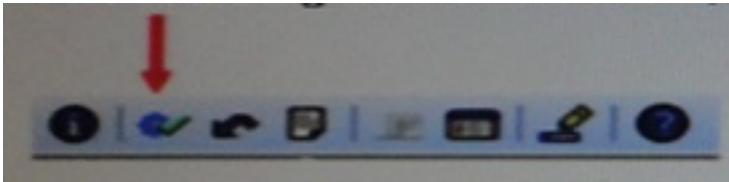
- A. when a user uploads a 600 KB file to his yahoo account via web mail (via his browser), he will be prompted by user check
- B. When a user sends an e-mail with a small point with a small body and 5 attachments, each of 200 KB to, he will be prompted by user check.
- C. When a user sends an email with an attachment larger than 500 KB to, he will be prompted by user check.
- D. When a user sends an email with an attachment larger than 500 KB to, he will be prompted by user check.

Answer: A

Explanation:

QUESTION NO: 58

What is significance of the depicted icon in the Smart Workflow toolbar?



Choose the BEST answer.

- A. Overall status information: Everything is OK.
- B. Session has been approved.
- C. Submit for Approval
- D. Check the consistency of Smart workflow sessions

Answer: C

Explanation:

QUESTION NO: 59

You configure a Check Point QoS rule based with two rules: an HTTP rule with a weight of 40 and the Default Rule with a weight of 10. If only HTTP traffic is passing through your QoS Module, what percent of bandwidth will be allocated to the HTTP traffic?

- A. 80%
- B. 40%
- C. 100%
- D. 50%

Answer: A

Explanation:

QUESTION NO: 60

Which is TRUE for route-based VPNs?

- A. IP Pool NAT must be configured on each Gateway
- B. Route-based VPNs are a form of partial overlap VPN Domain
- C. Dynamic-routing protocols are not required
- D. Route-based VPNs replace domain-based VPNs

Answer: A

Explanation:

QUESTION NO: 61

Which procedure creates a new administrator in smartworkflow?

- A. run the cpconfig, supply the login name, profile properties, name, access applications and permissions.
- B. In smart dashboard, click smartworkflow / enable smartworkflow and the enable smartworkflow wizard will start. Supply the login name, profile properties, name, access applications and prompted.
- C. On the provider-1 primary MDS, run cpconfig, supply the login name, profile properties, name, access applications and permissions.
- D. In the smart dashboard, click user and administrators right click administrators / new administrator and supply the login name, profile properties, access applications and permissions

Answer: D

Explanation:

QUESTION NO: 62

What is a task of the Smart Event Server?

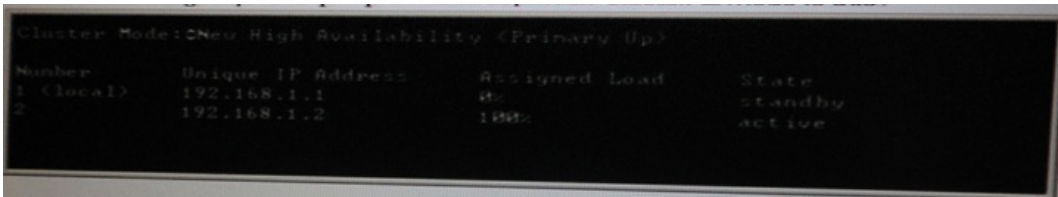
- A. Assign a severity level to an event
- B. Display the received events.
- C. Analyze each IPS log entry as it enters the Log server.
- D. Forward what is known as an event to the Smart Event Server.

Answer: A

Explanation:

QUESTION NO: 63

From the following output of cphaprob state, which clusterXL mode is this?



```
Cluster Mode: New High Availability (Primary Up)
Number Unique IP Address Assigned Load State
1 (local) 192.168.1.1 40% standby
2 192.168.1.2 100% active
```

- A. New mode
- B. Multicast mode
- C. Legacy mode
- D. unicast mode

Answer: D

Explanation:

QUESTION NO: 64

Can endusers be forced to authenticate by using client certificates and username password credentials?

- A. yes, but by manually changing the parameters is password warning to true in the \$ PWDIR/conf/ objects_5_0.c file, to allow for LDAP
- B. No, R71 only supports authentication by client certificates
- C. Yes by editing the protection-level settings
- D. SSL VPN support server certificates

Answer: C

Explanation:

QUESTION NO: 65

Your customer complains of the weak performance of his systems. He has heard that connection templates accelerate traffic. How do you explain to the customer about template restrictions and how to verify that they are enabled?

- A.** To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the destination port. To test if the connection templates are enabled, use the command “fw ct1 templates”
- B.** To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the secure port. To test if the connection templates are enabled, use the command “fw ct1 templates”
- C.** To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the secure port. To test if the connection templates are enabled, use the command “fw ct1 templates”
- D.** To enhance connection-establishment acceleration, a mechanism attempts to “group together” all connections match a particular service and whose sole discriminating element is the destination port. To test if the connection templates are enabled, use the command “fw accel templates”

Answer: D

Explanation:

QUESTION NO: 66

Your customer wishes to install the smart workflow blade on a R70 security management server (secure platform). Which is the correct method? Choose the best answer.

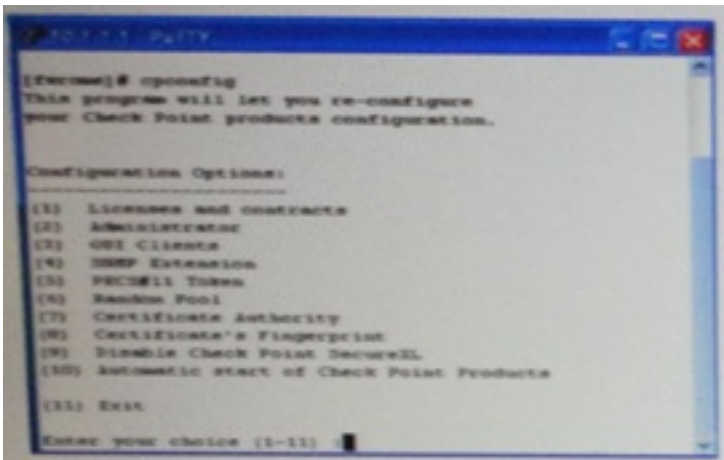
- A.** When you install the R70.1 package on an R70 security management server, it will be upgraded to version R70.1 with smart workflow.
- B.** The smart workflow works directly on the versions R70. Install the smart workflow as an add-on. The version of the management server remains R70.
- C.** You must upgrade the management server to the version R70.1 first before you start the installation of the smart workflow software blade plug-in
- D.** The smart workflow blade is included in the standard R70 version. You need to enable via cpconfig.

Answer: A

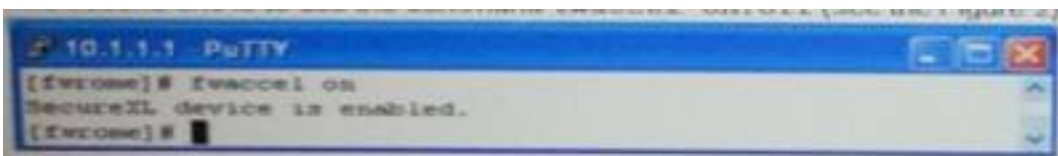
Explanation:

QUESTION NO: 67

Your customer asks you about the performance pack. you explain to him that a performance pack is software acceleration product which improves the performance of the security gateway. There are two ways to enable or disable the acceleration. the first one is to use command cpconfig (see the fig 1)



The second one is to use the command fwaccel on: off (see the figure 2)



What is the difference between those two commands?

- A. The command cpconfig works on the security platform only. The command fwaccel can be used on all platforms.
- B. The fwaccel command determines the default setting. the command cpconfig can dynamically change the setting but after the reboot it reverts to the default setting.
- C. Both the commands have the save function.
- D. The cpconfig command enables acceleration. The command fwaccel can dynamically change the settings, but after reboot it reverts to the default settings.

Answer: D

Explanation:

QUESTION NO: 68

How is a change approved for implementing in smart workflow?

- A. The change is submitted for approval and is automatically installed by the approver once approval is clicked.
- B. The change is submitted for approval and is manually installed by the original submitter the next time he logs in after the approval of the change.
- C. The change is submitted for approval and is manually installed by the approver once approval is clicked.

Answer: B

Explanation:

QUESTION NO: 69

Which statement is TRUE for route-based VPNs?

- A. IP Pool NAT must be configured on each Gateway
- B. Route-based VPNs are a form of partial overlap VPN Domain
- C. Dynamic-routing protocols are not required
- D. Route-based VPNs replace domain-based VPNs

Answer: A

Explanation:

QUESTION NO: 70

Management portal should be installed on:

- (i) management server
- (ii) security gateway
- (iii) dedicated server

- A. All are possible solutions
- B. (ii) only
- C. (iii) only
- D. (i) or (iii) only

Answer: D

Explanation:

QUESTION NO: 71

How many Events can be shown at one time in the Event preview pane?

- A. 5000
- B. 15000
- C. 30000
- D. 1000

Answer: C

Explanation:

QUESTION NO: 72

What access level cannot be assigned to an administrator in a smart event?

- A. Event database
- B. Write only
- C. No access
- D. Read only

Answer: B

Explanation:

QUESTION NO: 73

You need to publish secured platform routes using the OSPF routing protocol. What is the correct command structure, once entering the router command, to implement OSPF successfully?

- A. run the cpconfig utility to enable ospf routing
- B. ip route ospf network 1
ospf network 2.
- C. enable
- D. Configure terminal

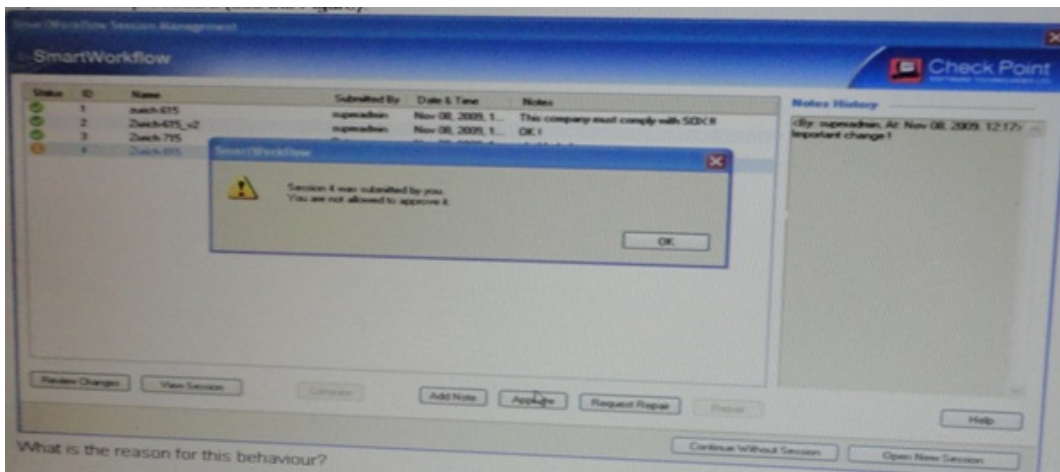
Router ospf terminal
 Router ospf [id]
 Network [network] [wildcradmask] area [id]
 D. use DBedit utility to edit the objects_5_0.c file

Answer: C

Explanation:

QUESTION NO: 74

David is the multicorp security manager and approves the proposals submitted by the security administrator Peter. One day, David believes he has detected a vulnerability in the security policy. He submits a change proposal and tries to approve his own submission. The system does not allow him to perform this procedure.



What is reason of this behavior?

- A. The company does not allow David to submit and also approve the same poln (instead of Submit and Approve).
- B. The company does not allow David to submit and approve the same submitted sessions in Global Properties was set to on
- C. The company does not allow David to submit and approve the same policy cfi submitted sessions in the Smart Workflow section of the Firewall object properties was set to on
- D. The proposal contains some logical contradictions. The Check Point does not permit this change to be carried out.

Answer: D

Explanation:

QUESTION NO: 75

With Smart Event what is the Analyzer function?

- A. Analyze log entries, looking for event Policy patterns.
- B. Generate a threat analysis report from the Analyzer database
- C. Display received threats and tune the Events Policy.
- D. Assign severity levels to events

Answer: A

Explanation:

QUESTION NO: 76

David wants to manage hundreds of gateways using a central management tool. What tool would David use to accomplish his goal?

- A. Smart Provisioning
- B. Smart blade
- B. Smart Dashboard
- C. SmartSM

Answer: C

Explanation:

QUESTION NO: 77

You have received an LDAP account unit and confirmed the apply & fetch branches options works in SSL.VPN, but end users still cannot be authenticated. What is the most LIKELY cause?

- A. The administrator login is incorrect
- B. the LDAP server is incorrectly configured.
- C. The user is not defined in active directory
- D. the LDAP account unit's login distinguished name is incorrectly configured

Answer: D

Explanation:

QUESTION NO: 78

Which of the following services will cause the secure XL templates to be disabled?

- A. TELNET
- B. FTP
- C. LDAP
- D. HTTPS

Answer: D

Explanation:

QUESTION NO: 79

Which of the following statements is FALSE about the DLP software blade and Active Directory (AD) or LDAP?

- A. When a user authenticates in the DLP portal to view all his unhandled, the portal authenticates the user using only AD/LDAP
- B. Check Point user check client authentication is based on AD.
- C. For SMTP traffic, each recipient e-mail address is translated using AD/LDAP to user name and group that is checked vs. the destination column of the LDAP rule.
- D. For SMTP traffic, the sender e-mail address is translated using AD/LDAP to a user name and group that is checked vs. the source column of the DLP base.

Answer: C

Explanation:

QUESTION NO: 80

What are the Smart Provisioning profile indicators?

- A. OK. Needs Attention, Uninitialized, Unknown

- B. OK. Needs Attention. Agent is in local mode,Uninitialized,Unknown
- C. OK. Wating,Unknown. Not Installed. Not Updated. May be out of date
- D. OK. In Use,Out of date, not used

Answer: B

Explanation:

QUESTION NO: 81

Whendoes it mean when a Security Gateway islabeleduntrustedin theSmart provisioning status view?

- A. theSecurity Gateway is down.
- B. SIC has not been established between the Security Gateway and the Security management.
- C. Smart Provisioning is not enabled on the Security Gateway
- D. cpd is not running at the Security Gateway

Answer: B

Explanation:

QUESTION NO: 82

Pushing a SmartPravisioning Profile to a gatewayfailed.Whatare possible reasons for that?

- (i)SIC is not established
- (ii)SSH demon is not running on the gateway.
- (iii)An admin has logged in locally on the gateway.
- (iv) LSM is not enabled on the gateway
- (v)Gateway is in maintenance mode

- A. (i), (iv) or (v)
- B. (i) or (v)
- C. (iii) or (v)
- D. (ii), (iii), (iv)

Answer: B

Explanation:

QUESTION NO: 83

Control connections between the security management server and gateway are not encrypted by VPN community. How are these connections secured?

- A. They are not encrypted, but are authenticated by the Gateway
- B. They are secured by PPTP
- C. They are not secured

Answer: A

Explanation:

QUESTION NO: 84

Which of the following is TRUE concerning numbered VPN Tunnel Warfare's (VTIs)?

- A. VTIs are supported on SecurePlatform Pro
- B. VTTs cannot share IP addresses
- C. VTIs are assigned only local addresses, not remote addresses
- D. VTTs can use an already existing physical-interface IP address

Answer: A

Explanation:

QUESTION NO: 85

Which of the following is NOT accelerated by SecureXL?

- A. FTP
- B. HTTPS
- C. TELNET
- D. SSH

Answer: B

Explanation:

QUESTION NO: 86

Identify the correct step performed by smartupdate to upgrade a remotesecuritygateway. After selecting packages / distribute and install selected package and choosing the target gateway.

- A.** Selected package is copied from the CD-ROM of the smartupdate PC directly to the security gateway and installation is performed.
- B.** Selected package is copied from the package repository on the security management server to the security gateway but the installation is not performed
- C.** Smart update wizard walks the administrator through a distributed package.
- D.** Selected package is copied from the package repository on the security management server to the security gateway and installation is performed.

Answer: D

Explanation:

QUESTION NO: 87

What is NOT true about Management Portal?

- A.** Choosing Accept control connections in Implied Rules includes Management Portal access
- B.** Management Portal requires a license
- C.** Default Port for Management Portal access is 4433
- D.** Management Portal could be reconfigured for using HTTP instead of HTTPS

Answer: D

Explanation:

QUESTION NO: 88

Provisioning Profiles can NOT be applied to:

- A. UTM-EDGE Appliances
- B. UTM-1 Appliances
- C. IP Appliances
- D. Power-1 Appliances

Answer: C

Explanation:

QUESTION NO: 89

Based on the following information, which statement below is TRUE?

DLP rule base has the following conditions:

Date type = Large file (.500KB)

Source =myorganization

Destination =free web mails

Protocol = any

Action = ask user

At other rules are set to detect. Usercheck is enabled and installed on all client machines

- A. a user sent an e-mail that was matched by the large file rule and by another rule with action, detect. As a result the action taken by DLP is detected and the user will not be prompted by user check.
- B. A user sends an e-mail with a small body and an attachment is a 600 KB, ZIP file containing 200 files each with a size of 10 KB (before compression). The user will be prompted by user check.
- C. When a user sends an e-mail with a small body and 5 attachments, each of 200KB to, he will be prompted by user check.
- D. When a user uploads a 600 kB file to his Yahoo account via Web mail (via his browser) he will be prompted by user check

Answer: D

Explanation:

QUESTION NO: 90

Which of the following commands can be used to bind a NIC to a single processor when using a performance pack on a secure platform?

- A. Set proc
- B. Splat proc
- C. Fw fat path nic
- D. Sim affinity

Answer: D

Explanation:

QUESTION NO: 91

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

- A. CPM200
- B. HTTPS443
- C. HTTP80
- D. TCP 8080

Answer: B

Explanation:

QUESTION NO: 92

You are using tracelogger to debug SSL VPN's server and obtain a textual traffic dump. Which type of traffic will you not see in output?

- A. Traffic outbound from internal networks
- B. Traffic to the portal
- C. Traffic outbound to external networks
- D. Traffic inbound from external networks

Answer: B

Explanation:

QUESTION NO: 93

You are using a tracer to debug an SSL VPN's server side and obtain a textual traffic dump. Which type of traffic will you NOT see in the output?

- A. Traffic outbound from the internal networks
- B. Traffic to the portal
- C. Traffic inbound to the external networks
- D. Traffic inbound from the external networks

Answer: B

Explanation:

QUESTION NO: 94

What could the following regular expression be used for in a DLP rule?

`$ 9 [0-9] *, [0-9] [0-9] [0-9],[0-9] [0-9]`

Select the best answer

- A. As a Data Type to prevent programmers from leaking code outside the company
- B. As a compound data type representation.
- C. As a Data Type to prevent employees from sending an email that contains a complete price-list of nine products
- D. As a Data Type to prevent the France Department from leaking salary information to employees

Answer: C

Explanation:

QUESTION NO: 95

Your customer wishes to install Smart Workflow on top of R/O security SERVER (Windows system). What is the required disk space?

- A. 1256 MB
- B. 1 GB
- C. 512 MB

D. 880 MB

Answer: D

Explanation:

QUESTION NO: 96

The following graphic illustrates which command being issued on a Secure Platform?

```

fwaccel stats
total conn          14
conn from templates 11
dropped tcp conn    0
dropped nonTCP conn 0
TCP bytes          1754800
dec bytes           0
partial conn        0
dropped packets     96
total conn          14
conn from templates 11
dropped tcp conn    0
dropped nonTCP conn 0
TCP conn            0
crypt conn          0
dec bytes           0
anticipated conn    0
dropped bytes       7472
  
```

- A. fwsecurexl stats
- B. fwaccel stats
- C. fw accel stats
- D. fw securexl stats

Answer: C

Explanation:

QUESTION NO: 97

If Bob wanted to create a management high availability configuration, what is minimum number of security management servers required in order to achieve this goal?

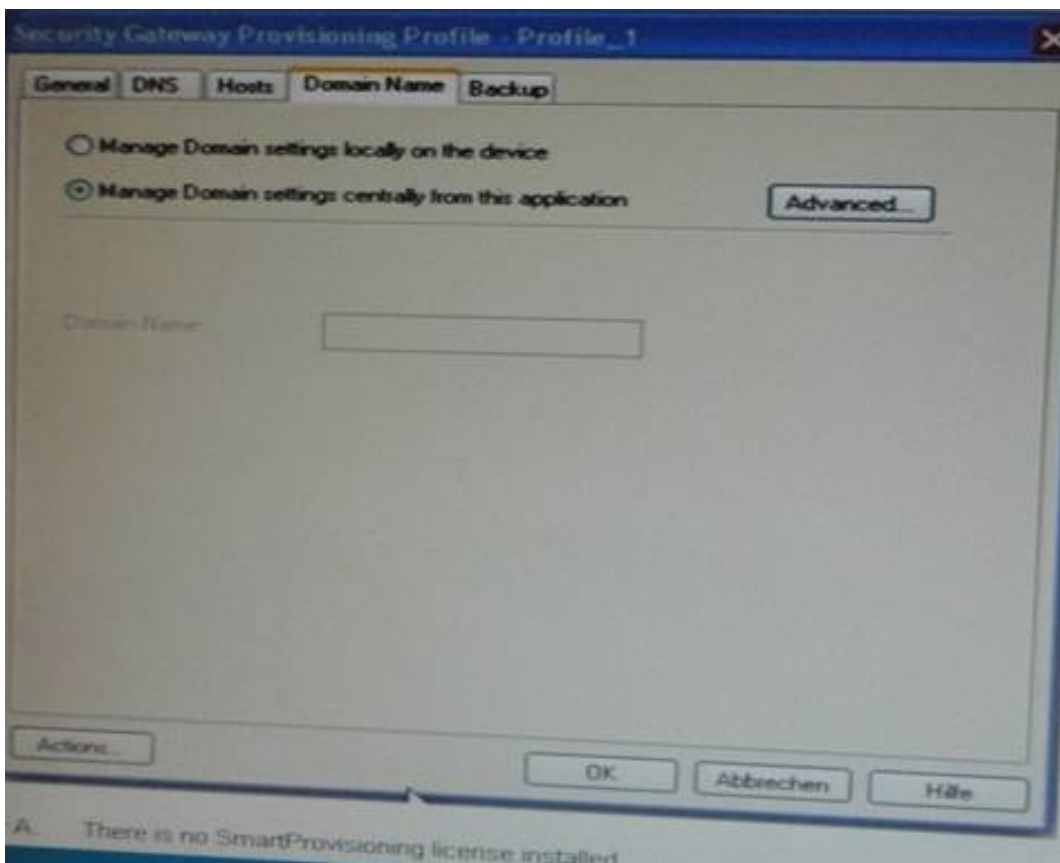
- A. Three
- B. Two
- C. Four
- D. One

Answer: B

Explanation:

QUESTION NO: 98

Domain name can not be changed in smart provisioning and domain name is grayed out what is possible reason for this?



- A. There is no SmartProvisioning license installed.
- B. Profile is not assigned to any Gateway
- C. Domainprofile setting on device level is set to Mandatory.
- D. Domain name settings are always fetched from firewall object

Answer: A

Explanation:

QUESTION NO: 99

To help organize events, smart reporter uses filtered queries. Which of the following is not a smart Event event property you can query?

- A. State Open, Cloacd,Fnlao,Alarm
- B. Type scans, denial of service unauthorized entry
- C. Eventcritical,suspect, false alarm
- D. Time last hour, last day, last week

Answer: B

Explanation:

QUESTION NO: 100

From the following rule base, for which rules will the connection templates be generated in secureXL?

Rule	Source	Destination	Service	Action	Log	Policy Target	...
2	Corporate-internal-ne	Any	Any Traffic	ACL		Policy Target	Any
Customers Accessing Web Service	Customers@any	Corporate-web-s	Any Traffic	http	Client Auth	Log	Policy Target
Incoming Emails	Any	Corporate-mail-s	Any Traffic	smtp-mail/for	accept	Log	Policy Target
HTTP/FTP access	Corporate-internal-ne	Any	Any Traffic	http	accept	Log	Policy Target
Cleanup Rule	Any	Any	Any Traffic	Any	drop	Log	Policy Target

- A. Rule nos 2 to 5
- B. Rule nos 2 and 5
- C. Rule no 2 only
- D. All rules except rule no 3

Answer: C

Explanation:

QUESTION NO: 101

Smart provisioning can provision the Operating System and network settings on which of the following?

- A. R65 HFA 40 Security Gateways and above

- B. IPSO42.Security Gateways
- C. NGX Security Appliances
- D. Edge firmware 6x and above

Answer: D

Explanation:

QUESTION NO: 102

You are using smartupdate and perform a remote upgrade to a R/1 Security Gateway. Which of the following statements is false?

- A. You are using smartupdate and perform a remote upgrade to a R/1 Security Gateway. Which of the following statements is false?
- B. Smart dashboard is open during package upload and upgrade, the upgrade will fail.
- C. Smartupdate can query the Security Management Server and Gateway (or product information)
- D. SmartUpdate can query license information running locally on the Gateway

Answer: B

Explanation:

QUESTION NO: 103

Which is the best configuration option to protect internal users from malicious Java code, without stripping Java scripts?

- A. Use the URI resource to block Java code
- B. Use CVP in the URI resource to block Java code
- C. Use the URI resource to strip applet tags
- D. Use the URI resource to strip ActiveX tags

Answer: B

Explanation:

QUESTION NO: 104

Which of the following is NOT a feature of clusterXL?

- A. Enhanced throughput in all clusterXL modes (2 gateway cluster compared with 1 gateway)
- B. Transparent failover in case of device failures
- C. Zero downtime for mission-critical environments with State Synchronization
- D. Transparent upgrades

Answer: D

Explanation:

QUESTION NO: 105

Which procedure enables the SSL VPN blade on the gateway?

- A. Log into small dashboard, create the new rule with the source and destination addresses of the record remote network set the action to encrypt and push the policy to the gateway.
- B. Log into a small dashboard, edit the properties of the gateway, and select the SSL, VPN check box.
- C. Log into smart dashboard select the VPN communications tab and add the gateway to the appropriate community.
- D. Log into Web UI on the gateway and check the SSL VPN blade check box.

Answer: B

Explanation:

QUESTION NO: 106

Which DLP action would describe the following action: The data transmission event is logged in smart viewtracker Administrators with permission view the data that was sent the traffic is passed.

- A. Detect
- B. AskUser
- C. Informuser
- D. Prevent

Answer: C

Explanation:

QUESTION NO: 107

Which of the following statements about SSL VPN is true?

- A. Traffic is not encrypted in a LAN department. Where clear text requests are forwarded to internal servers
- B. All traffic is always encrypted
- C. Traffic is encrypted, when it is initiated from a LAN
- D. Administration traffic is not encrypted

Answer: A

Explanation:

QUESTION NO: 108

You have installed secured platform R71 as security gateway operating system as company requirements changed. You need the VTI features of R71. What should you do?

- A. Only IPSO 3.9 supports VTI feature, so you have to replace your security gateway with Nokia appliances.
- B. B-Type pro enables on your security gateway and reboots it.
- C. You have to reinstall your security gateway with secured Platform pro R71, as secured platform R71 does not support VTI<S
- D. In smart dashboard click on the OS drop down menu and choose secured platform pro. you have to reboot the security gateway in order for the change to take effect

Answer: B

Explanation:

QUESTION NO: 109

Which tool CANNOT be launched from smart update R71?

- A. Snapshot
- B. SecurePlatform WebUI
- C. Cpinfo
- D. IP Appliance Voyager

Answer: D

Explanation:

QUESTION NO: 110

Which specific R71 GUI would you use to view the length of time a TCP connection was open?

- A. SmartReporter
- B. Smart ViewMonitor
- C. SmartView Status
- D. SmartView Tracker

Answer: D

Explanation:

QUESTION NO: 111

You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?

- A. Fw purge policy
- B. Fw fetch policy
- C. Fw purge active
- D. Fw unload local

Answer: D

Explanation:

QUESTION NO: 112

In smartworkflow, what is not a valid possibility?

- A. TaskFlow without Session and without role segregation.
- B. Task Flow without Session but with Role Segregation
- C. Task Flow with Session but without Role Segregation
- D. Task flow with Session and with Role Segregation

Answer: B

Explanation:

QUESTION NO: 113

What is the benefit to running Eventia Analyzer in Learning Mode?

- A. There is no Eventia Analyzer Learning Mode
- B. To run Eventia Analyzer, with a step-by-step online configuration guide for training/setup purpose
- C. To run Eventia Analyzer with preloaded sample data in a test environment
- D. To generate a report with system Event Policy modification suggestions

Answer: D

Explanation:

QUESTION NO: 114

What is the maximum number of cores supported by CoreXL?

- A. 6
- B. 8
- C. 4
- D. 12

Answer: B

Explanation:

QUESTION NO: 115

Which of the following commands will stop acceleration on a Security Gateway running on Secure Platform?

- A. splat_accel off
- B. fwacceX off
- C. perf_pack off
- D. fwaceel off

Answer: D

Explanation:

QUESTION NO: 116

You want VPN traffic to match packets from internal interfaces- You also want the traffic to exit the Security Gateway bound for all site-to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?

- A. Communities > communities

- B. Internal_clear > External_Clear
- C. Internal_clear > All_GwTogw
- D. Internal_clear > All_communities

Answer: D

Explanation:

QUESTION NO: 117 CORRECT TEXT

The London office just upgraded their DNS Gateway needs with the new settings. What would be the best way for Henry to change the DNS settings for the London's Gateway?

- A>Edit the Canada profile
- B.Edit the gateways DNS settings from the edit gateway, then selecting the DNS tab
- C.DNS settings for that gateway cannot be changed
- D.Edit the Europe profile

Answer: B

QUESTION NO: 118

What are the SmartProvisioning Policy Status indicators?

- A. OK, Down, Up, Synchronized
- B. OK, Waiting, Out of Sync, Not Installed, Not communicating
- C. OK, Unknown, Not Installed, May be out of date
- D. OK, Waiting, Unknown, Not Installed, Not Updated, May be out of date

Answer: D

Explanation:

QUESTION NO: 119

You have selected the event "port scan from internal network in Eventia Analyzer", to detect an event when 30 ports have occurred when 60 seconds. You want to detect two ports scans from a host within 10 seconds of each other. How would you accomplish this?

- A. You cannot set Eventia Analyzer to detect two port scans within 10 seconds of each other.
- B. Select the two port-scan detections as a new event.

- C. Select the two port-scan detections as a sub event.
- D. Select the two port-scan detections as an exception.

Answer: D

Explanation:

QUESTION NO: 120

When checkpoint product is used to create and save changes to a Log consolidation policy?

- A. Security Management Server
- B. Eventia Reporter Client
- C. SmartDashboard Log Consolidator
- D. Eventia Reporter Server

Answer: D

QUESTION NO: 121

Reporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT

- A. Possible worm/malware activity.
- B. Tracking attempted port scans.
- C. Analyzing traffic patterns against public resources.
- D. Analyzing access attempts via social-engineering.

Answer: D

Explanation:

QUESTION NO: 122

Laura notices the Microsoft Visual Basic kill Bits protection is set to inactive. She wants to set the Microsoft Visual Basic Kill bits protection and all other low performance impact protection to prevent. She asks her manager for approval and he stated she can turn these on. But he told Laura to make sure no high performance impact protections are limited on while changing this setting.

Using the output below, how would Laura change the default-protection on performance impact protections classified as low from inactive to prevent while still meeting her other criteria?

- A. Go to profiles > Default_protection and unlock "Do not activate protections with performance impact to medium or above"
- B. Go to profiles > Default_protection and select "Do not activate protections with performance impact to low or above"
- C. Go to profiles > Default_protection and select "Do not activate protections with performance impact to medium or above"
- D. Go to profiles > Default_protection and unlock "Do not activate protections with performance impact to high or above"

Answer: C

Explanation:

QUESTION NO: 123

John is the MultiCorp Security Administrator. If he suggests a change in the firewall configuration, he must submit his proposal to David, a Security manager. One day David is out of the office and John submits his proposal to Peter, surprisingly, Peter is not able to approve the proposal the system does not permit him to do so (See figure below)

Next day David is back and he can carry out this operation.

Both David and Peter have accounts as administrators in the Security management Server and both have the read/write all permission. What is the reason for the difference? Choose the best answer.

- A. There were some hardware/software issues at the Security management Server on the first day.
- B. Peter was not log on to system for a long time.
- C. The attribute manage administrators was not assigned to Peter.
- D. The specific SmartWorkflow read/write permissions were assigned to David only.

Answer: D

Explanation:

QUESTION NO: 124

Which of the following is a supported deployment for Connectra?

- A. IPSO 4.9 build 88

- B. VMWare ESX
- C. Solaris 10
- D. Windows server 2007

Answer: B

Explanation:

QUESTION NO: 125

Which type of routing relies on a VPN Tunnel interface (VT1) to route traffic?

- A. Subnet-based VPN
- B. Route-based VPN
- C. Host-based VPN
- D. Domain-based VPN

Answer: B

Explanation:

QUESTION NO: 126

What is a task of the IPS Event Analysis Server?

- A. Assign a severity level to an event.
- B. Display the received events.
- C. Forward what is known as an event to the IPS Event Analysis server
- D. Analyze each IPS log entry as it enters the Log server.

Answer: D

Explanation:

QUESTION NO: 127

Using IPS, how do you notify the Security Administrator that malware is scanning specific ports?
By enabling:

- A. Malware Scan protection
- B. Sweep Scan protection
- C. Host Port Scan
- D. Malicious Code Protector

Answer: C

Explanation:

QUESTION NO: 128

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

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

Answer: D

Explanation:

QUESTION NO: 129

What is the purpose of the pre-defined exclusions Included with Eventia Analyzer and IPS Event Analysis R7P?

- A. To give samples of how to write your own exclusion.
- B. As a base for starting and building exclusions
- C. To allow Eventia Analyzer and IPS Event Analysis R70 to function property with all other R70 release devices
- D. To avoid incorrect event generation by the default IPS event definition, a scenario that may occur in deployments that include Security Gateways of versions prior to R70

Answer: D

Explanation:

QUESTION NO: 130

You are trying to configure Directional VPN Rule Match in the Rule Base. But the match column does not have the option to see the directional match. You see the following window. What must you enable to see the Directional match?

- A. VPN Directional Match on the Gateway object's VPN tab
- B. Advanced Routing on each Security Gateway

- C. VPN Directional Match on the VPN advanced Window, m Global Properties
- D. Directional_match (True) in the objects_5_0 file on Security management Server

Answer: C

Explanation:

QUESTION NO: 131

You believe Phase 2 negotiations are failing 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: 132

The 'We-Make-Widgets' company has purchased twenty UTM-1 Edge appliances for their remote offices. Kim decides the best way to manage those appliances is to use SmartProvisioning and create a profile they can all use. List the order of steps Kim would go through to add the Dallas Edge appliance to the remote Office profile Using the output below.

1. Enter the name of the profile called "Remote Offices"
2. Change the provisioning profile called "Remote Offices"
3. Click file than select new, than provisioning profile
4. Click on the devices tab
5. Highlight the Dallas Edge appliances, click, than edit gateway
6. Click on the profile tab

- A. 6, 1, 3, 4, 5, 2
- B. 4, 1, 3, 6, 5, 2
- C. 6, 3, 1, 4, 5, 2
- D. 4, 3, 1, 6, 5, 2

Answer: B

Explanation:

QUESTION NO: 133

You are Connectra administrator. Your users complain that their outlook Web Access is running extremely slowly, and their overall browsing experience configures to worsen. You suspect it could be a logging problem. Which of the following log file does CheckPoint recommended you purge?

- A. Httpd*.log
- B. Event_ws.log
- C. Mod_ws_owd.log
- D. Alert_owd.log

Answer: A

Explanation:

QUESTION NO: 134

With Eventia Analyzer, what is the analyzer Server's function?

- A. Generate a threat analysis report from the Analyzer database.
- B. Analyze log entries, looking for Event Policy patterns.
- C. Displays received threats and tune the Events Policy.
- D. Assign severity levels to events.

Answer: B

Explanation:

QUESTION NO: 135

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: B

Explanation:

QUESTION NO: 136

When does the SmartWorkflow Policy Installation window appear?

- A. When the administrator installs an approved policy
- B. When the manager approves a session
- C. When the administrator installs an unapproved policy
- D. When the administrator submits a session for approval

Answer: C

Explanation:

QUESTION NO: 137

Control connections between the security management Server and the Gateway are not encrypted by the VPN community. How are the connections secured?

- A. They are encrypted and authenticated using SIC
- B. They are not encrypted, but are authenticated by the Gateway
- C. They are secured by PPTF
- D. They are not secured

Answer: A

Explanation:

QUESTION NO: 138

Which of the following is NOT an IPS Event Analysis Permission Profile type?

- A. View
- B. Read/Write
- C. No Access
- D. Events Database

Answer: A

Explanation:

QUESTION NO: 139

For an initial installation of Connectra, Which of the following statements is TRUE?

- A. You must configure the Connectra username and password before running the First time Wizard
- B. It is possible to run the First Time Wizard from Expert Mode on the Connectra server.
- C. It is not possible to use the sysconfig and cpconfig utilities, until the First Time Wizard in the Administration Web GUI is successfully completed
- D. It is not necessary to set up the Rule Base before completing Connectra's installation

Answer: A

Explanation:

QUESTION NO: 140

Which of the following statements is FALSE regarding ospf configuration on SecurePlatform Pro?

- A. Router ospf 1 creates the Router ID for the Security Gateway and should be the same ID for all Gateways.
- B. Router ospf 1 creates an ospf routing instance and this process ID should be different for each Security Gateway.
- C. Router ospf 1 creates the Router ID for the Security Gateway and should be different for all Gateways.
- D. Router ospf 1 creates an ospf routing instance and this process ID should be the same on all Gateways.

Answer: C

Explanation:

QUESTION NO: 141

Using the output below, what does the red flag indicate for the MS08-067 Protection?

- A. It indicates it is for follow up.
- B. It indicates this protection is for new 0-day vulnerability.
- C. It indicates the protection's Security Level was modified from the default setting by the administrator.
- D. It indicates this protection is critical.

Answer: A

Explanation:

QUESTION NO: 142

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: 143

Which of the following statements about the Port Scanning feature of IPS Is TRU6?

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

Answer: C

Explanation:

QUESTION NO: 144

Which of the following items can be provisioned via a profile through SmartProvisioning?

- i) Backup Schedule
- ii) DNS Entries
- iii) Hosts Table
- iv) Domain Name
- v) Interface IP'S

- A. i, ii, Iv
- B. i, ii, iii, iv

- C. i
- D. i, ii, iii, iv, v

Answer: B

Explanation:

QUESTION NO: 145

VPN routing can also be configured by editing which file?

- A. \$FWDIR\VPN\ route_conf. c
- B. \$ PWDIR\ bin\ vpn_route. conf
- C. \$FWDIR\conf\vpn_route.c
- D. \$PWDIR\conf \vpn_route. conf

Answer: D

Explanation:

QUESTION NO: 146

Your customer asks you about the Check Point SmartWorkflow. He was informed that it is possible to use the SmartWorkflow Software Blade without using *Sessions* and "Role Segregation". What is the BEST explanation for this?

- A. SmartDashboard works as if SmartWorkflow is not enabled. The administrator can modify and install policies without any intermediate steps The administrator will be asked if he wishes to keep the tracking information of deployed changes to see them later with SmartView Tracker
- B. SmartDashboard works as if SmartWorkflow is not enabled the administrator can modify and install policies without any intermediate steps Changes are not tracked
- C. SmartDashboard works as if SmartWorkflow is not enabled. The administrator can modify and install policies without any intermediate steps. The deployed changes are tracked automatically.
- D. The information is incorrect. If the customer uses SmartWorkflow Software Blade, he must use the "Session" with or without "Role Segregation."

Answer: C

Explanation:

QUESTION NO: 147

SmartProvisioning is an integral part of the security management or provider-1 CMA. To enable SmartProvisioning on the security management server:

- A. Obtain the SmartProvisioning license, add the License to the Security Management server or CMA, turn on SmartProvisioning on each gateway.
- B. Obtain the SmartProvisioning license, add the License to the Security Management server or CMA, disable SecureXL.
- C. Obtain the SmartProvisioning license, add the License to the Security Management server or CMA.
- D. Obtain the SmartProvisioning license, add the License to the Security Management server or CMA, select the box under policy for SmartProvisioning.

Answer: C

Explanation:

QUESTION NO: 148

What rules send log information to Dshield.org when Center is configured?

- A. Determined 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. Determined by the Global Properties configuration Logs defined In the Log and Alerts section, rules tracking set to Account or SNMP tarp.
- C. Determined in Web Intelligence, configuration Information Disclosure is configured, rules with tracking set to user defined alerts or SNMP.
- D. Determined by the Dshield Storm Center Logging suiting in Logs and Masters of the Security Management Server object rules with tracking set to Log or None.

Answer: A

Explanation:

QUESTION NO: 149

Which of the following manages Eventia Reporter Standard Reports and allows the administrator to specify automatic Uploads of reports to a central FTP server?

- A. Security Management Server
- B. Eventia Reporter Client
- C. SmartDashboard Log Consolidator
- D. Eventia Reporter Server

Answer: D

Explanation:

QUESTION NO: 150

How do new connections get established through a Security Gateway with SecureXL enabled?

- A. The new connection will DC first inspected by SecureXL and if it does not match the drop table of SecureXL. Then it will be passed to the firewall module for a rule match.
- B. If the connection matches a connection of drop template in SecureXL. It will either be established or dropped without performing a rule match, else it will be passed to the firewall module for a rule match.
- C. New connections are always inspected by the firewall and if they are accepted, the subsequent packets of the same connection will be passed through SecureXL
- D. New connection packets never reach the SecureXL module

Answer: C

Explanation:

QUESTION NO: 151

To help organize events, Eventia Analyzer uses filtered queries. Which of the following is NOT an Eventia Analyzer event property you can query?

- A. Even Critical, Suspect, False Alarm
- B. Time: Last hour, Last Day, Last Week
- C. State Open, Closed, False Alarm
- D. Type Scans, Denial of Services, Unauthorized Entry

Answer: A

Explanation:

QUESTION NO: 152

Using the Backup Target functionality in SmartProvisioning, what targets are available?

- i) FTP
- ii) TFTP
- iii) SFTP
- iv) SCP
- v) Locally

- A. i
- B. ii, iv,v
- C. i, ii,iv
- D. I, ii,iii, iv

Answer: B

Explanation:

QUESTION NO: 153

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. You plan to take the opportunity to create 0 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: 154

Your online book store has customers connecting to a variety of web servers to place or change orders and check order status. You ran penetration tests through the security Gateway todetermine if the web servers were protected from a recent series of cross site scripting attacks. The penetration testing indicated the 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 Product > Web Server box on the hoist node objects representing your Web servers
- C. Add Port (TCP 443) as an additional port on the Web Server tab for the host node
- D. The penetration software you are using is malfunctioning and is reporting a false-positive

Answer: B

Explanation:

QUESTION NO: 155

What is a task of the IPS Event Correlation Unit?

- A. Analyze each IPS log entry as it enters the Log server.
- B. Assign a severity level to an event.
- C. Add events to the events database
- D. Display the received events.

Answer: A

Explanation:

QUESTION NO: 156

A security of administrators opens a new session, makes changes to the policy and submits the session for Approval. The Security Manager may approve the session or request repair if a manager opens a new session and submits it for approval, can he approve his session as a Security Manager?

- A. It depends on the type of changes made in the session.
- B. It depends on the SmartWorkflow settings in Global Properties.
- C. Yes, he can always approve his own session
- D. No, he can never approve his own session

Answer: D

Explanation:

QUESTION NO: 157

What happens to the session information after they are approved and a policy Installation is done?

- A. Session information is never deleted from the database.
- B. It depends on the SmartWorkflow settings in Global Properties.
- C. An option is given to retain the session information, default facing deletion of session information from the database.
- D. Session information can only be deleted before a policy is installed

Answer: D

Explanation:

QUESTION NO: 158

Wren of the following platforms does NOT support SecureXL?

- A. UTM-1 Appliance
- B. Power-1 Appliance
- C. IP Appliance
- D. UNIX

Answer: D

Explanation:

QUESTION NO: 159

When a security administrator selects Repair for session requested for repair by a Security Manager, Which of the following happens?

- A. The administrator will have to open the old session and make the changes, no note is added automatically, however, the manager adds his notes stating the changes required.
- B. The same session is modified with a note automatically added stating Under repair
- C. The old status is removed and a new session is created with the same name, but with a note stating New session after repair
- D. A new session is created by the name Repairing Session <old id> and the old session status is updated to Repaired with a note stating Repaired by Session <new id>

Answer: D

Explanation:

QUESTION NO: 160

A user accesses the user portal using Integrity Secure Workspace, and attempts to initialize a network application using SSL Network Extender. The application fails to start. What is the MOST LIKELY solution?

- A. Select the option Auto-detect client capabilities
- B. Select the option Enable SSL Network Extender Application Mode only
- C. Select the option Turn off all SSL tunneling clients
- D. Select the option Enable SSL Network Extender Network Mode only

Answer: B

Explanation:

QUESTION NO: 161

While using the SmartProvisioning to create a new profile, you cannot continue because there are

no devices to select. What is the possible reason for this?

- i) All devices already have a profile assigned to them
- ii) Provisioning Blade is not enabled on the devices
- iii) No UTM- 1/Power- 1/Secure Platform devices are defined in SmartDashboard
- iv) SIC is not established on the devices.

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

Answer: B

Explanation:

QUESTION NO: 162

What is a task of the IPS Event Analysis Server?

- A. Invoke defined automatic reactions
- B. Display the received events
- C. Analyze each IPS log entry as it enters the Log server
- D. Add events to the events database

Answer: C

Explanation:

QUESTION NO: 163

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: 164

What are the 3 main components of the IPS Event Analysis software Blade?

- i) Correlation Unit
- ii) Correlation Client
- iii) Correlation Server
- iv) Analyzer Server
- v) Analyzer Client
- vi) Analyzer Unit

- A. i ii iii
- B. iv, v. vi
- C. i, iii, iv
- D. i, iv, v

Answer: D

Explanation:

QUESTION NO: 165

How can you verify that SecureXL is running?

- A. cpstat os
- B. fw ver
- C. securexl stat
- D. fwaccel stat

Answer: D

Explanation:

QUESTION NO: 166

Susan needs to change the DNS settings on the SecurePlatform Gateway. Using the output below, which gateway she could edit from the devices view using Edit gateway, then selecting the DNS tab?

- A. Seoul-Edge
- B. Prague-GW
- C. Berlin-GW
- D. Paris-GW

Answer: D

Explanation:

QUESTION NO: 167

What is the router command to save your OSPF configuration?

- A. Save
- B. write config
- C. save memory
- D. write mem

Answer: B

Explanation:

QUESTION NO: 168

You enable Sweep scan Protection and Host port scan in IPS to determine if a large amount of traffic from a specific internal IP address is network attack, or a user's system is infected with a worm. Will you get all the information you need from these actions?

- A. No. To verify if this is a worm or an active attack, you must also enable TCP attack defenses
- B. No. The logs and alert can provide some level of information, but determining whether the attack is intentional or a worm requires further research.
- C. Yes. IPS will limit the traffic impact from the scans, and identify if the pattern of the traffic matches any known worms
- D. No. These IPS protections will only block the traffic, but it will not provide a detailed analysis of the traffic

Answer: B

Explanation:

QUESTION NO: 169

Using SmartProvisioning Profiles, which of the following could be configured for both SecurePlatform AND UTM-1 Edge devices?

- i) Backup
- ii) Routing
- iii) Interfaces
- iv) Hosts
- v) NTP server
- vi) DNS

- A. ii, iii, iv, and vi
- B. i, iii, iv, and vi
- C. None of these options are available for both.
- D. i, ii, and iv

Answer: C

Explanation:

QUESTION NO: 170

What is the advantage for deploying Connectra in a DMZ, versus a LAN?

- A. Connectra adds another layer of access security to internal resources, when It resides in a DMZ
- B. B.SSL Network Extender is ineffective in a LAN deployment
- C. Traffic is in clear text when forwarded to internal servers, but the back connection is encrypted for remote users
- D. Traffic is authenticated without hiding behind Connectra's IP address

Answer: A

Explanation:

QUESTION NO: 171

Your customer wishes to use SmartWorkflow Software Blade, but he also wishes to install a policy during an emergency without an approval. Is it possible? Select the BEST answer

- A. Yes, it is possible but the administrator must receive special administrator permission i.e, can install in emergency. You can use the new CUI to set the administration security setting.
- B. Yes, it is possible, but this feature must be configured in the Global Properties. The

administrator must provide a special password and the reason for this emergency installation.

C. Yes. It is possible, but this feature must be configured in Global Properties and the administrator must provide a special password.

D. No, if a customer uses the SmartWorkflow Software Blade, a policy must be approved

Answer: C

Explanation:

QUESTION NO: 172

Check Point product implements a Consolidation Policy?

A. Eventia Reporter

B. SmartView Monitor

C. SmartLSM

D. SmartView Tracker

Answer: A

Explanation:

QUESTION NO: 173

Which of the following is not supported by CoreXL?

A. IPV4

B. IPS

C. Route-based VPN

D. SmartView Tracker

Answer: B

Explanation:

QUESTION NO: 174

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting "All IP Addresses behind Gateway based on Topology Information"

You want to test the route based VPN, so you created VTIs among the Gateways and created static route entries for the VTTs However, when you test the VPN. You find out the VPN still go through the regular domain IPsec tunnels instead of the routed VT1 tunnels.

What is the problem and how do you make the VPN use the VTI tunnels?

- A. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP
- B. Domain VPN takes precedence over the route-based VTI to make the VPN go through VTI. use an empty group object as each Gateway's VPN Domain
- C. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI. remove the Gateways out of the mesh community and replace with a star community
- D. Route-based VTI takes precedence over the Domain VPN. To make the VPN go through VTI. Use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes

Answer: B

Explanation:

QUESTION NO: 175

The Management Portal Software Blade allows users to

- A. View Security Policies
- B. Monitor traffic flows
- C. Add/Delete rules
- D. Create/Modify objects

Answer: A

Explanation:

QUESTION NO: 176

You have configured an LDAP account unit and confirmed the Apply & Fetch Branches option works in Connectra, but end users still cannot be authenticated. What is the MOST LIKELY cause?

- A. The Administrator's login is incorrect.
- B. The LOAP server is incorrectly configured
- C. The user is not defined in Active Directory
- D. The LOAP account unit's login Distinguished Name is incorrectly configured

Answer: D

Explanation:

QUESTION NO: 177

After repairing a SmartWorkflow session:

- A. The session moves to status Repaired and a new session can be started.
- B. The session moves to status Awaiting Repair and must be resubmitted.
- C. The session is continued with status not approved and a new session must be started.
- D. The session is discarded and a new session is automatically started.

Answer: A

Explanation:

QUESTION NO: 178

The Management Portal allows all of the following EXCEPT:

- A. View administrator activity
- B. Schedule policy installation
- C. View the status of Check Point products
- D. Manage firewall logs

Answer: B

Explanation:

QUESTION NO: 179

Which of the following functions CANNOT be performed in clinetinfo on computer information collected?

- A. Copy the contents of the selected cells.
- B. Save the information in the active tab to an .exe file.
- C. Enter new credential for accessing the computer information.
- D. Run Google.com search using the contents of the selected cell.

Answer: D

Explanation:

QUESTION NO: 180

Your customer asks you about checkpoint SmartWorkflow. His company must comply with various

laws and regulations and therefore it is important for him to be able to see the changes made to specific object. You explain to him that he can use the SmartWorkflow software Blade to achieve his objective and show him some examples (shown in Figures below). How can the customer receive the required information?

Choose the best answer

- A.** The customer can check compliance. This function compares the logs with the compliance requirements and automatically reports which part of the selected compliance is fulfilled and which is not
- B.** The customer can use the Check Point's SmartView Tracker to view the required information. He selects the log category Changed Objects
- C.** The customer can use the Record Details. This feature enables administrators to track changes that have been made to objects over an extended period of time These changes are recorded in SmartView Tracker as audit togs
- D.** The customer can use the Check Point's SmartView Tracker directly to receive the required information. He selects the log category SmartWorkflow

Answer: B

Explanation:

QUESTION NO: 181

When a security administrator logs in to SmartDashboard and selects Continue without session from the following window, what kind of access will be generated in SmartDashboard?

- A.** He will get read4 only access to the policy, network objects and session management
- B.** He will get read-only access to the policy and network objects; however, He can still manage the sessions, i.e.Approve, Request Repair etc
- C.** A new session will automatically be created with a default session name along with date and time. All changes made by the manager will be saved in this new session
- D.** No access will be granted, he will be logged out of SmartDashboard

Answer: A

Explanation:

QUESTION NO: 182

How do you control the maximum number of mail messages in a spool directory?

- A.** In the Gateway object's SMTP settings under the Advanced window

- B. In the smtp. conf file on the Security Management Server
- C. In the Security Server window in Global Properties
- D. In IPS SMTP settings

Answer: A

Explanation:

QUESTION NO: 183

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs cannot be assigned a proxy interface.
- B. Local IP addresses are not configured, remote IP addresses are configured.
- C. VTIs can only be physical, not loopback
- D. VTIs are only supported on the IPSO Operating System.

Answer: B

Explanation:

QUESTION NO: 184

When using Connectra with endpoint Security Policies, what option is NOT available when configuring DAT enforcement?

- A. Maximum DAT file version
- B. Maximum DAT file age
- C. Minimum DAT file version
- D. Oldest DAT file timestamp

Answer: A

Explanation:

QUESTION NO: 185

When configuring a web Application for SSL. VPN remote access, you have given the following definition for the application along with its protection level?

Which of the following is best match for the above application?

- A. dmz.example.com/extranet
- B. www.dmz.example.com

- C. www.example.com/intranet
- D. hr.dmz.example.com/intranet

Answer: C

Explanation:

QUESTION NO: 186

The SmartProvisioning management concept is based on:

- A. Zones
- B. Groups
- C. Regions
- D. Profiles

Answer: D

Explanation:

QUESTION NO: 187

You start the configuration of SmartWorkflow. SmartWorkflow is enabled, but you are not able to select Open new session because it is grayed out?

What must be done to open a new session?

- A. Sessions in the Manage menu of SmartDashboard must be selected and enabled.
- B. The use of sessions must be enabled by the CU command. SWF_session start.
- C. A rule which allows the SmartWorkflow traffic must be placed on the top of the Rule Base.
- D. The Work with sessions in Global Properties must be set.

Answer: D

Explanation:

QUESTION NO: 188

Which operating system(s) support(s) unnumbered VPN Tunnel Interfaces (VTIs) for route-based VPNs?

- A. SecurePlatform for NGX and higher
- B. Solaris 9 and higher
- C. IPSO 3.9 and higher

D. Red Hat Linux

Answer: A

Explanation:

QUESTION NO: 189

If Bob wanted to create a Management high Availability configuration, what is the minimum number of Security management servers required in order to achieve his goal?

- A. Three
- B. Two
- C. Four
- D. One

Answer: B

Explanation:

QUESTION NO: 190

Match the SmartDashboard session status icons with the appropriate SmartWorkflow sessionstatus:

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

Answer: B

Explanation:

QUESTION NO: 191

What is a task of the IPS Event Analysis Client?

- A. Add events to the events database.
- B. Assign a severity level to an event.
- C. Display the received events.
- D. Analyze each IPS log entry as it enters the Log server

Answer: C

Explanation:

QUESTIONNO: 192

When upgrading to NGX R65, which Check Point products do not require a license upgrade to be current?

- A. None, all versions require a license upgrade
- B. VPN-1 NGX(R64) and later
- C. VPN-1 NGX(R60) and later
- D. VPN-1 NG with Application Intelligence (R54) and later

Answer: C

QUESTION NO: 192

A security audit has determined that your unpatched web application server is revealing the fact that it accesses a SQL server. You believe that you have enabled the proper SmartDefense setting but would like to verify this fact using SmartView Tracker. Which of the following entries confirms the proper blocking of this leaked information to an attacker?

- A. "Fingerprint Scrambling: Changed [SQL] to [Perl]"
- B. "HTTP response spoofing: remove signature [SQL Server]"
- C. "Concealed HTTP response [SQL Server]. (Error Code WSE0160003)"
- D. "ASCII Only Response Header detected: SQL"

Answer: C

Explanation:

QUESTION NO: 193

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in Eventia Reporter?

- A. In SmartDashboard, the SmartView Monitor page in the VPN-1 Security Gateway object
- B. In Eventia Reporter, under Express > Network Activity
- C. In Eventia Reporter, under Standard > Custom
- D. In SmartView Monitor, under Global Properties > Log and Masters

Answer: A

Explanation:

QUESTION NO: 194

Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?

- A. In SmartView Monitor, select Tools > Alerts
- B. In SmartView Tracker, select Tools > Custom Commands
- C. In SmartDashboard, edit the Gateway object, select SmartDefense > Alerts
- D. In SmartDashboard, select Global Properties > Log and Alert > Alert Commands

Answer: A

Explanation:

QUESTION NO: 195

When configuring VPN High Availability (HA) with MEP, which of the following is correct?

- A. The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).
- B. MEP Gateways must be managed by the same SmartCenter Server.
- C. MEP VPN Gateways cannot be geographically separated machines.
- D. If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues

Answer: A

Explanation:

QUESTION NO: 196

Which of the following would NOT be a reason for beginning with a fresh installation of VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65?

- A. You see a more logical way to organize your rules and objects.
- B. YOU want to keep your Check Point configuration.
- C. Your Security Policy includes rules and objects whose purpose you do not know.
- D. Objects and rules' naming conventions have changed overtime.

Answer: B

Explanation:

QUESTION NO: 197

How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?

- A. Use FTP Security Server settings in SmartDefense.
- B. Add the restricted commands to the aftp.conf file in the SmartCenter Server.
- C. Configure the restricted FTP commands in the Security Servers screen of the Global properties.
- D. Enable FTP Bounce checking in SmartDefense.

Answer: A

Explanation:

QUESTION NO: 198

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

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

Answer: A

Explanation:

QUESTION NO: 199

Which NGX R65 logs can you configure to send to DShield.org?

- A. SNMP and account logs
- B. Alert and user-defined alert logs
- C. Account and alert logs
- D. Audit and alert logs

Answer: B

Explanation:

QUESTION NO: 200

The customer has a small Check Point installation which includes one Window XP workstation working as SmartConsole „, one Solaris server working as SmartCenter, and a third server running SecurePlatform working as Security Gateway. This is an example of:

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

Answer: A

Explanation:

QUESTION NO: 201

Which VPN-1 NGX R65 component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

- A. SmarrViewMonitor
- B. SmarrView Status
- C. SmartUpdate
- D. Eventia Analyzer

Answer: D

Explanation:

QUESTION NO: 202

SmartDefense profiles are:

- A. Files that take 3MB of RAM from the user console machine.
- B. Able to be cloned, but only from the command line.
- C. Configurable up to 20 for all VPN-1 R65 Gateways and above.
- D. Configurable from either the SmartDefense tab or from the Gateway itself.

Answer: D

Explanation:

QUESTION NO: 203

What is a Consolidation Policy?

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

Answer: D

Explanation:

QUESTION NO: 204

Match the ClusterXL Modes with their configurations

- A. A2.B3.C4.D 1
- B. A2.B3.C 1.D4
- C. A3,B2,C4,D 1
- D. A3.B2.C 1.D4

Answer: D

Explanation:

QUESTION NO: 205

State Synchronization is enabled on both members in a cluster, and the Security Policy is successfully installed. No protocols or services have been deselected for "selective sync". The following is the fw tab -t connections -s output from both members: Is State Synchronization working properly between the two members?

- A. Members A and B are synchronized, because #SLINKS are identical in the connections table.
- B. Members A and B are not synchronized, because #VALS in the connections table are not close.
- C. Members A and B are not synchronized, because #PEAK for both members is not close in the connections table.
- D. Members A and B are synchronized, because ID for both members is identical in the connections table.

Answer: B

Explanation:

QUESTION NO: 206

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?

- A. VTIs are supported on SecurePlatform Pro.
- B. VTIS cannot share IP addresses
- C. VTIs can use an already existing physical-interface IP address
- D. VTIS are assigned only local addresses, not remote addresses

Answer: A

Explanation:

QUESTION NO: 207

Which of the following is NOT supported with Office Mode?

- A. SSL Network Extender
- B. L2TP
- C. SecureClient
- D. Transparent Mode

Answer: D

Explanation:

QUESTION NO: 208

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 NGX Central and Local licenses to a remote module.
- (4) Delete both NGX 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 NGX Central licenses to a remote module (not Local licenses).

- A. 1,2,3,4,&5
- B. 1.2.5.&6
- C. 2,3,4,&5
- D. 2,5,&6

Answer: A

Explanation:

QUESTION NO: 209

You are the Security Administrator for a university. The university's FTP servers have old hardware and software. Certain FTP commands cause the FTP servers to malfunction. Upgrading the FTP servers is not an option at this time. Where can you define Blocked FTP Commands passing through the Security Gateway protecting the FTP servers?

- A. SmartDefense > Application Intelligence > FTP > FTP Security Server
- B. Rule Base > Action Field > Properties
- C. FTP Service Object > Advanced > Blocked FTP Commands
- D. Global Properties > Security Server > Allowed FTP Commands

Answer: A

Explanation:

QUESTION NO: 210

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the following configurations: Cluster Member 1: OS: SecurePlatform, NICs: QuadCard, memory: 512 MB, Security Gateway, version: VPN-1 NGX R65 and primary SmartCenter Server installed, version: VPN-1 NGX R65 Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65 Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 256 MB, Security Gateway only, and version: VPN-1 NGX R65

- A. No, the Security Gateway cannot be installed on the SmartCenter Pro Server.
- B. No, the SmartCenter Pro Server is not running the same operating system as the cluster members.
- C. Yes, these machines are configured correctly for a ClusterXL deployment.
- D. No, Cluster Member 3 does not have the required memory.

Answer: A

Explanation:

QUESTION NO: 211

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the following configurations: Are these machines correctly configured for a ClusterXL deployment?

- A. No, all machines in a cluster must be running on the same OS.
- B. Yes, these machines are configured correctly for a ClusterXL deployment.
- C. No, QuadCards are not supported with ClusterXL.
- D. No, a cluster may only have two members.

Answer: A

Explanation:

QUESTION NO: 212

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

- A. WebUI
- B. cpconfig
- C. ifconfig
- D. sysconfig

Answer: D

Explanation:

QUESTION NO: 213

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

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

Answer: C

Explanation:

QUESTION NO: 214

An NGXR65 HA cluster contains two members with external interfaces 172.28.108.1 and 172.28.108.2. The internal interfaces are 10.4.8.1 and 10.4.8.2. The external cluster VIP address is 172.28.108.3 and the internal cluster VIP address is 10.4.8.3. The synchronization interfaces are 192.168.1.1 and 192.168.1.2. The Security Administrator discovers State Synchronization is not working properly. The cphaprob if command output displays shows: What is causing the State Synchronization problem?

- A.** The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.
- B.** The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.
- C.** The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.
- D.** Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Answer: A

Explanation:

QUESTION NO: 215

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server?

- A.** Use cpprod_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.
- B.** Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
- C.** You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- D.** Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Answer: C

Explanation:

QUESTION NO: 216

What must a public hospital Security Administrator do to comply with new health-care legislation requirements for logging all traffic accepted through the perimeter Security Gateway?

- A.** Define two log servers on the VPN-1 NGX R65 Gateway object. Enable "Log Implied Rules" on the first log server. Enable "Log Rule Base" on the second log server. Use Eventia Reporter to merge the two log server records into the same database for HIPPA log audits.
- B.** Install the "View Implicit Rules" package using SmartUpdate.
- C.** 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.
- D.** Check the "Log Implied Rules Globally" box on the VPN-1 NGX R65 Gateway object.

Answer: C

Explanation:

QUESTION NO: 217

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when

- (1) The Security Policy is installed.
- (2) The Security Policy is saved.
- (3) The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active.
- (4) A scheduled event occurs.
- (5) The user database is installed.

Select the BEST response for the synchronization sequence. Choose One:

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

Answer: C

Explanation:

QUESTION NO: 218

Which of the following commands is a CLI command for VPN-1 NGX R65?

- A. fw shutdown
- B. fwprint
- C. fw tab -u
- D. fw merge

Answer: C

Explanation:

QUESTION NO: 219

You are running the licensejppgrade tool on your SecurePlatform Gateway. Which of the following can you NOT do with the upgrade tool?

- A. Simulate the license-upgrade process.
- B. Perform the actual license-upgrade process.
- C. View the status of currently installed licenses.
- D. View the licenses in the SmartUpdate License Repository.

Answer: D

Explanation:

QUESTION NO: 220

What tools CANNOT be launched from SmartUpdate NGX R65?

- A. cpinfo
- B. SecurePlatform WebUI
- C. snapshot
- D. Nokia Voyager

Answer: C

Explanation:

QUESTION NO: 221

Your VPN-1 NGX R65 primary SmartCenter Server is installed on SecurePlatform. You plan to schedule the SmartCenter 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. Select that time object's Global Properties > Logs and Masters window, to schedule a logswitch.
- 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. Open the primary SmartCenter Server object's Logs and Masters window, enable "Schedule log switch", and select the Time object.
- D.** On a SecurePlatform SmartCenter Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.

Answer: C

Explanation:

QUESTION NO: 222

You plan to migrate an NG with Application Intelligence (AI) R55 SmartCenter Server on Windows to VPN-1 NGX R65. You also plan to upgrade four VPN-1 Pro Gateways at remote offices, and one local VPN-1 Pro Gateway at your company's headquarters. The SmartCenter Server configuration must be migrated. What is the correct procedure to migrate the configuration?

- A.** 1. Upgrade the five remote Gateways via SmartUpdate.
2. Upgrade the SmartCenter Server, using the NGX R65 CD.
- B.** 1. From the VPN-1 NGX R65 CD on the SmartCenter Server, select "Upgrade".
2. Reboot after installation and upgrade all licenses via SmartUpdate.
3. Reinstall all gateways using NGX R65 and install a policy.
- C.** 1. From the VPN-1 NGX R65 CD in the SmartCenter Server, select "Export".
2. Install VPN-1 NGX R65 on a new PC using the option "Installation using imported configuration".
3. Reboot after installation and upgrade all licenses via SmartUpdate.
4. Upgrade software on all five remote Gateways via SmartUpdate.
- D.** 1. Copy the \$FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another file server.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move the saved directory contents to \$FWDIR\conf replacing the default installation files.
5. Reinstall all gateways using VPN-1 NGX R65 and install a Security Policy.

Answer: C

Explanation:

QUESTION NO: 223

How should Check Point packages be uninstalled?

- A. In the same order in which the installation wrapper initially installed them
- B. In any order as long as all packages are removed
- C. In the opposite order in which the installation wrapper initially installed them
- D. In any order; CPsuite must be the last package uninstalled.

Answer: C

Explanation:

QUESTION NO: 224

You are working in a large hospital, together with three other Security Administrators. How do you use SmartConsole to check changes to rules or object properties other administrators made?

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

Answer: D

Explanation:

QUESTION NO: 225

Which operating system is not supported by SecureClient?

- A. MacOSX
- B. Windows XP SP2
- C. Windows 2003 Professional
- D. IPSO 3.9

Answer: D

Explanation:

QUESTION NO: 226

In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs. What can you do to keep old log files, when free space falls below 45 MB?

- A. Do nothing. Old logs are deleted, until free space is restored.
- B. Do nothing. The SmartCenter Server automatically copies old logs to a backup server before purging.
- C. Use the fwm logexport command to export the old log files to other location.
- D. Configure a script to run fw logswitch and SCP the output file to a separate file server.

Answer: D

Explanation:

QUESTION NO: 227

What happens when you select File > Export from the SmartView Tracker menu?

- A. Exported log entries are deleted from fw.log.
- B. Current logs are exported to a new.log file.
- C. Exported log entries are still viewable in SmartView Tracker.
- D. Logs in fw.log are exported to a file that can be opened by Microsoft Excel

Answer: D

Explanation:

QUESTION NO: 228

When launching SmartDashboard, what information is required to log into VPN-1 NGX R65?

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

Answer: B

Explanation:

QUESTION NO: 229

What is the command to upgrade an NG with Application Intelligence R55 SmartCenter Server running on SecurePlatform to VPN-1 NGX R65?

- A. upgrade_mgmt
- B. fwinstall_mgmt
- C. fwm upgrade_tool

D. patch add cd

Answer: D

Explanation:

QUESTION NO: 230

Which SmartView Tracker mode allows you to read the SMTP email body sent from the Chief Executive Officer (CEO)?

- A. Log Tab
- B. Display Capture Action
- C. This is not a SmartView Tracker feature
- D. Account Query

Answer: B

Explanation:

QUESTION NO: 231

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

- A. Connectivity between the NGX gateway and LDAP server
- B. Secure Internal Communications (SIC)
- C. VPN Load Balancing
- D. Overlapping VPN Domains

Answer: C

Explanation:

QUESTION NO: 232

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

- A. SmartView Tracker
- B. TheWebUI
- C. Eventia Reporter
- D. SmartView Monitor

Answer: B

Explanation:

QUESTION NO: 233

Where can an administrator configure the notification action in the event of a policy install time change?

- A. SmartDashboard: Policy Package Manager
- B. SmartView Tracker: Audit Log
- C. SmartView Monitor: Global Thresholds
- D. SmartDashboard: Security Gateway Object: Advanced Properties Tab

Answer: C

Explanation:

QUESTION NO: 234

Which of the following is the most critical step in a SmartCenter Server NGX R65 backup strategy?

- A. Perform a full system tape backup of both the SmartCenter and Security Gateway machines.
- B. Run the cpstop command prior to running the upgrade_export command
- C. Using the upgradejimport command, attempt to restore the SmartCenter Server to a non-production system
- D. Move the *.tgz upgrade_export file to an offsite location via ftp.

Answer: C

Explanation:

QUESTION NO: 235

In a R70 ClusterXL Load Sharing configuration, which type of ARP related problem sometimes forces the use of Unicast Mode (Pivot) configuration due to incompatibility on some adjacent routers and switches?

- A. Multicast MAC address response to a RARP request
- B. MGCP MAC address response to a Multicast IP request
- C. Unicast MAC address response to a Multicast IP request
- D. Multicast MAC address response to a Unicast IP request

Answer: D

Explanation:

QUESTION NO: 236

How do you verify a VPN Tunnel Interface (VTI) is configured properly?

- A. vpn shell display interface detailed <VTI name>
- B. vpn shell show interface detailed <VTI name*
- C. vpn shell display <VTI name> detailed
- D. vpn shell show<VTI name> detailed

Answer: B

Explanation:

QUESTION NO: 237

What action can be run from SmartUpdate NGX R65?

- A. mds_backup
- B. cpinfo
- C. upgrade_export
- D. remote uninstall verifier

Answer: B

Explanation:

QUESTION NO: 238

Which of the following would NOT be a function of the Check Point license-upgrade tool?

- A. Upgrade locally managed licenses.
- B. Simulate the license-upgrade process.
- C. Manually upgrade a specific license.
- D. View the status of the currently installed licenses.

Answer: C

Explanation:

QUESTION NO: 239

How do you use SmartView Monitor to compile traffic statistics for your company's Internet activity during production hours?

- A. Use the "Traffic Counters" settings and SmartView Monitor to generate a graph showing the total HTTP traffic for the day
- B. Select the "Tunnels" view, and generating a report on the statistics
- C. View total packets passed through the Security Gateway
- D. Configure a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway

Answer: A

Explanation:

QUESTION NO: 240

How do you recover communications between your SmartCenter Server and Security Gateway if you "lock" yourself out via a rule or policy mis-configuration?

- A. cpstop
- B. fw unload policy
- C. fw delete all.all
- D. fwunloadlocal

Answer: D

Explanation:

QUESTION NO: 241

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

- A. fwm unload.local
- B. fw kill policy
- C. cpstop
- D. fwunloadlocal

Answer: D

Explanation:

QUESTION NO: 242

You have two NOKIA Appliances: one IP530 and one IP380. Both appliances have IPSO 3.9 and NGX R65 VPN-1 Power installed in a distributed deployment. Can they be members of a Gateway Cluster?

- A. No, because the appliances must be of the same model (both should be IP530 or IP380)
- B. NO, because NOKIA does not have a cluster option.
- C. Yes, as long as they have the same IPSO and VPN-1 versions.
- D. NO, because the Security Gateways must be installed in a stand-alone installation.

Answer: C

Explanation:

QUESTION NO: 243

Your organization has many VPN-1 Edge Gateways at various branch offices, to allow users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the VPN-1 Edge Gateways first be inspected by your headquarters' VPN-1 Pro Security Gateway. How do you configure VPN routing in this star VPN Community?

- A. To the Internet and other targets only
- B. To the center and other satellites, through the center
- C. To the center; orthrougnthe center to other satellites, then to the Internet and other VPN targets
- D. To the center only

Answer: C

Explanation:

QUESTION NO: 244

Your bank's distributed VPN-1 NGX R65 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. SmartUpdate
- B. SmartView Tracker
- C. SmartDashboard
- D. SmartPortal

Answer: D

Explanation:

QUESTION NO: 245

After installing VPN-1 Pro NGX R65, 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. Make sure the driver for your particular NIC is available, and reinstall. You will be prompted for the driver.
- B. The NIC is faulty. Replace it and reinstall.
- C. If an interface is not configured, it is not recognized. Assign an IP and subnet mask using the WebUI.
- D. Your NIC driver is installed but was not recognized. Apply the latest SecurePlatform R65 Hotfix Accumulator (HFA).

Answer: C

Explanation:

QUESTION NO: 246

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

- A. SmartViewTracker
- B. SmartView Status
- C. SmartView Monitor
- D. SmartDashboard

Answer: B

Explanation:

QUESTION NO: 247

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 access is very slow. You suspect the Security Gateway virtual memory might be the problem. How would you check this using SmartConsole?

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

Answer: A

Explanation:

QUESTION NO: 248

The command fw fetch causes the:

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

Answer: D

Explanation:

QUESTION NO: 249

When configuring Port Scanning, which level of sensitivity detects more than 100 inactive ports are tried for a period of 30 seconds?

- A. LOW
- B. High
- C. None. Such a level does not exist.
- D. Medium

Answer: D

Explanation:

QUESTION NO: 250

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

- A. Manage Services, New Other, Provide name and define Protocol: x-y

- B. Manage Services, New TCP, Provide name and define Port: x-y
- C. Manage Services, New Other, Provide name and define Protocol: 17, Range: x-y
- D. Manage Services, New Group, Provide name and Add all service ports for range individually to the group object

Answer: B

Explanation:

QUESTION NO: 251

Which of these components does NOT require a VPN-1 NGX R65 license?

- A. Check Point Gateway
- B. SmartCenterServer
- C. SmartConsole
- D. SmartUpdate upgrading/patching

Answer: C

Explanation:

QUESTION NO: 252

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

- A. Log sites that are currently being blocked.
- B. Log sites from blocked categories.
- C. Alert the Administrator to block a suspicious site.
- D. Block sites only once.

Answer: B

Explanation:

QUESTION NO: 253

Upon checking SmartView Monitor, you find the following Critical Problem notification. What is the reason?

- A. Version mismatch between the SmartCenter Server and Security Gateway
- B. NO Secure Internal Communications established between the SmartCenter Server and Security Gateway

- C. Time not synchronized between the SmartCenter Server and Security Gateway
- D. No Security Policy installed on the Security Gateway

Answer: D

Explanation:

QUESTION NO: 254

You are administering your company's Clientless VPN connections. How many Security Servers should you be running to support 750 active users?

- A. 3
- B. 7
- C. 5
- D. 1

Answer: C

Explanation:

QUESTION NO: 255

How do you view a Security Administrator's activities, using SmartConsole tools?

- A. SmartView Tracker in Log mode
- B. Eventia Suite
- C. SmartView Monitor using the Administrator Activity filter
- D. SmartView Tracker in Audit mode

Answer: D

Explanation:

QUESTION NO: 256

The _____ Check Point ClusterXL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces

- A. New Mode HA
- B. Legacy Mode HA
- C. Multicast Mode Load Sharing
- D. Pivot Mode Load Sharing

Answer: B

Explanation:

QUESTION NO: 257

In ClusterXL, which of the following processes are defined by default as critical devices?

- A. assld
- B. fwd
- C. fwm
- D. cpp

Answer: B

Explanation:

QUESTION NO: 258

When configuring site-to-site VPN High Availability (HA) with MEP, which of the following is correct?

- A. MEP Gateways cannot be geographically separated machines.
- B. MEP Gateways must be managed by the same SmartCenter Server.
- C. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.
- D. If one MEP Security Gateway fails, the connection is lost and the backup Gateway picks up the next connection.

Answer: D

Explanation:

QUESTION NO: 259

You want to establish a VPN, using Certificates. Your VPN will exchange Certificates with an external partner. Which of the following activities should you do first?

- A. Exchange exported CAkeys and uses them to create a new server object to represent your partner's Certificate Authority (CA).
- B. Manually import your partner's Access Control List.
- C. Manually import your partner's Certificate Revocation List.
- D. Create a new logical-server object to represent your partner's CA.

Answer: A

Explanation:

QUESTION NO: 260

You are establishing a ClusterXL environment, with the following topology: VIP internal cluster IP = 172.16.10.3; VIP external cluster IP = 192.168.10.3 ClusterMember1:4NICs,3enabled: hme(): 192.168.10.1/24, hme1: 10.10.10.1/24, qfe2: 172.16.10.1/24 Cluster Member 2: 5 NICs, 3 enabled; hme3: 192.168.10.2/24, hme1: 10.10.10.2/24, hme2: 172.16.10.2/24 External interfaces 192.168.10.1 and 192.168.10.2 connect to a VLAN switch. The upstream router connects to the same VLAN switch. Internal interfaces 172.16.10.1 and 172.16.10.2 connect to a hub. 10.10.10.0 is the synchronization network. The SmartCenter Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?

- A. There is an IP address conflict.
- B. Cluster members cannot use the VLAN switch. They must use hubs.
- C. The Cluster interface names must be identical across all cluster members.
- D. The SmartCenter Server must be in the dedicated synchronization network, not the internal network.

Answer: A

Explanation:

QUESTION NO: 261

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use four machines with the following configurations: Cluster Member 1: OS: SecurePlatform, NICs: QuadCard, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65

Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 512 MB, Security Gateway only, and version: VPN-1 NGX R65 Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 256 MB, Security Gateway only, and version: VPN-1 NGX R65 SmartCenter Server: MS Windows 2000, NIC: Intel NIC (1), Security Gateway and primary SmartCenter Server installed, version: VPN-1 NGX R65 Are these machines correctly configured for a ClusterXL deployment?

- A. No, Cluster Member 3 does not have the required memory.
- B. NO, the Security Gateway cannot be installed on the SmartCenter Pro Server.
- C. Yes, these machines are configured correctly for a ClusterXL deployment.
- D. NO, the SmartCenter Pro Server is not running the same operating system as the cluster members.

Answer: C

Explanation:

QUESTION NO: 262

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

- A. CPMI
- B. TCP 8080
- C. HTTPS
- D. HTTP

Answer: C

Explanation:

QUESTION NO: 263

Which command line interface utility allows the administrator to verify the name and timestamp of the Security Policy currently installed on a firewall module?

- A. fwver
- B. fw stat
- C. fw ctl pstat
- D. cpstatfwd

Answer: B

Explanation:

QUESTION NO: 264

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

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

Answer: B

Explanation:

QUESTION NO: 265

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

- A. SmartUpdate installed SmartCenter Server PC
- B. SmartUpdate GUI PC
- C. VPN.1 Security Gateway getting the new upgrade package
- D. SmartUpdate Repository SQL database Server

Answer: B

Explanation:

QUESTION NO: 266

Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Why?

- A. Users must use the SecuRemote Client, to use the User Authentication Rule.
- B. YOU have forgotten to place the User Authentication Rule before the Stealth Rule.
- C. You checked the "cache password on desktop" option in Global Properties.
- D. Another rule that accepts HTTP without authentication exists in the Rule Base.

Answer: B

Explanation:

QUESTION NO: 267

When you check "Web Server" in a host.node object, what happens to the host?

- A. The Web server daemon is enabled on the host.
- B. More granular controls are added to the host, in addition to Web Intelligence tab settings.
- C. You can specify allowed ports in the Web server's node.object properties. You then do not need to list all allowed ports in the Rule Base
- D. SmartDefense Web Intelligence is enabled to check on the host.

Answer: B

Explanation:

QUESTION NO: 268

What command displays the version of an already installed Security Gateway?

- A. cpstat-gw
- B. fw printver
- C. fwver
- D. fw stat

Answer: C

Explanation:

QUESTION NO: 269

Multi-Corp wants to implement IKE DoS protection to prevent a denial-of-service (DoS) attack from paralyzing its VPN Communities. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations would BEST enable this new protection with minimal impact to the organization?

- A. Set "Support IKE DoS protection from identified source" to "Puzzles", and "Support IKE DoS protection from unidentified source" to "Stateless".
- B. Set both "Support IKE Dos protection from identified source", and "Support IKE DoS protection from unidentified source" to "Puzzles".
- C. Set both "Support IKE DoS protection from identified source", and "Support IKE DoS protection from unidentified source" to "Stateless"
- D. Set "Support IKE DoS protection from identified source" to "Stateless", and "Support IKE DoS protection from unidentified source" to "None".

Answer: C

Explanation:

QUESTION NO: 270

You are concerned that your company's servers might be vulnerable to an attack where a client fools a server into sending large amounts of data, using small packets. Which SmartDefense option should you use to protect the servers?

- A. Network Security > Denial of Service > Non-TCP Flooding
- B. Network Security > Denial of Service > LAND
- C. Network Security > IP and ICMP > Block Null Payload ICMP
- D. Network Security > TCP > Small PMTU

Answer: D

Explanation:

QUESTION NO: 271

Your organization's disaster recovery plan needs an update to the backup and restore section to realize the benefits of the new distributed VPN-1 NGX R65 installation. You want to document a plan to 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 NGX components that enforce the Security Policies should be backed up no less frequently than once a week? Desired Objective: Back up NGX logs no less frequently than once a week Your disaster recovery plan is as follows:? Use the cron utility to run the upgrade_export command each night on the SmartCenter 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 night on the Log Servers. Configure an automatic, nightly logswitch. Configure the organization's routine backup software to back up the switched logs every night. Upon evaluation, your plan:

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

Answer: D

Explanation:

QUESTION NO: 272

Which of the following generates an Eventia Report from its SQL database?

- A. SmartCenterServer
- B. SmartDashboard Log Consolidator
- C. Eventia Reporter Client
- D. Eventia Reporter Server

Answer: D

Explanation:

QUESTION NO: 273

You want to establish a VPN, using Certificates. Your VPN will exchange Certificates with an external partner. Which of the following activities should you do first?

- A. Exchange exported CA keys and uses them to create a new server object to represent your partner's Certificate Authority (CA).
- B. Manually import your partner's Access Control List.
- C. Manually import your partner's Certificate Revocation List.
- D. Create a new logical-server object to represent your partner's CA.

Answer: A

Explanation:

QUESTION NO: 274

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

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

Answer: A

Explanation:

QUESTION NO: 275

Antivirus protection on a VPN-1 Gateway is available for all of the following protocols, EXCEPT

- A. POP3
- B. TELNET
- C. HTTP
- D. FTP

Answer: B

Explanation:

QUESTION NO: 276

By default, when you click File > Switch Active File from SmartView Tracker, the SmartCenter Server:

- A. Prompts you to enter a filename, then saves the log file.
- B. Saves the current log file, names the log file by date and time, and starts a new log file.

- C. Purges the current log file, and starts a new log file.
- D. Purges the current log, and prompts you for the new log's mode.

Answer: B

Explanation:

QUESTION NO: 277

Choose all correct statements. SmartUpdate, located on a VPN-1 NGX SmartCenter Server, allows you to

- (1) Remotely perform a first time installation of VPN-1 NGX on a new machine.
- (2) Determine OS patch levels on remote machines.
- (3) Update installed Check Point and any OPSEC certified software remotely.
- (4) Update installed Check Point software remotely.
- (5) Track installed versions of Check Point and OPSEC products.
- (6) Centrally manage licenses.

- A. 1.3.4.S6
- B. 1 &4
- C. 4.5.S6
- D. 2,4,5,&6

Answer: D

Explanation:

QUESTION NO: 278

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

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

Answer: D

Explanation:

QUESTION NO: 279

What is the command in SecurePlatform Expert shell used to add routes without the use of sysconfig or the WebUI?

- A. ifroute
- B. ifconfig
- C. sysconfig route
- D. ip route

Answer: D

Explanation:

QUESTION NO: 280

Which of the following is a supported Sticky Decision function of Sticky Connections for Load Sharing?

- A. Multi-connection support for VPN-1 cluster members
- B. Support for Performance Pack acceleration
- C. Support for all VPN deployments (except those with third-party VPN peers)
- D. Support for SecureClient/SecuRemote/SSL Network Extender encrypted connections

Answer: D

Explanation:

QUESTION NO: 281

Look at the Advanced Properties screen exhibit. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?

- A. Check the box "Use aggressive mode"
- B. Change the "Renegotiate IPSec security associations every 3600 seconds" to 7200
- C. Change the setting "Use Diffie-Hellman group:" to "Group 5 (1536 bit)"
- D. Check the box "Use Perfect Forward Secrecy"

Answer: B

Explanation:

QUESTION NO: 282

You are a Security Administrator preparing to deploy a new HFA (Hotfix Accumulator) to ten Security Gateways at five geographically separated 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 a SSH connection to SCP the HFA to each Security Gateway. Once copied locally, initiate a remote installation command and monitor the installation progress with SmartView Monitor.
- C. Use SmartUpdate to install the packages to each of the Security Gateways remotely
- D. Send a CDROM with the HFA to each location and have local personnel install it

Answer: C

Explanation:

QUESTION NO: 283

How does a standby SmartCenter Server receive logs from all Security Gateways, when an active SmartCenter Server fails over?

- A. Establish Secure Internal Communications (SIC) between the primary and secondary Servers. The secondary Server can then receive logs from the Gateways, when the active Server fails over.
- B. Add the secondary SmartCenter Server object as a backup log server in the "Log Servers" window (under the "Logs and Masters" tab on the Gateway object). Reinstall the Security Policy.
- C. The secondary Server's host name and IP address must be added to the Masters file on the remote Gateways.
- D. Create a Check Point host object to represent the standby SmartCenter Server. Then select "Secondary SmartCenter Server" and "Log Server", from the list of Check Point Products on the General Properties window.

Answer: B

Explanation:

QUESTION NO: 284

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: 285

What information is found in the SmartView Tracker audit log?

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

Answer: A

Explanation:

QUESTION NO: 286

You want to upgrade a cluster with two members to VPN-1 NGX R65. The SmartCenter Server and both members are version VPN-1/Firewall-1 NG FP3, with the latest Hotfix. What is the correct upgrade procedure?

- (1) Change the version, in the General Properties of the gateway-cluster object.
- (2) Upgrade the SmartCenter Server, and reboot after upgrade.
- (3) Run cpstop on one member, while leaving the other member running. Upgrade one member
At a time, and reboot after upgrade. (4)Reinstall the Security Policy.

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

Answer: B

Explanation:

QUESTION NO: 287

Your network includes a SecurePlatform machine running NG with Application Intelligence (AI) R55. This configuration acts as both the primary SmartCent Server and VPN-1 Pro Gateway. You add one machine, so you can implement VPN-1 NGX R65 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 AI R55 configuration?

- A.**
1. On the existing machine, export the NG with AI R55 configuration to a network share.
 2. Insert the NGXR65 CD-ROM in the old machine. Install the NGXR65 Security Gateway only while reinstalling the SecurePlatform OS over the top of the existing installation. Complete sysconfig.
 4. On the new machine, install SecurePlatform as the primary SmartCenter Server only.
 5. Transfer the exported .tgzfile into the new machine, import the configuration, and then reboot.
 6. 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 network share.
 2. Uninstall the Security Gateway from the existing machine, using sysconfig.
 3. Insert the NGX R65 CD-ROM, and run the patch add cd command to upgrade the SmartCenter Server to VPN-1 NGX R65.
 4. Select "upgrade with imported file", and reboot.
 5. Install a new NGX R65 Security Gateway as the only module on the new machine, and reset SIC to the new Gateway.
- C.**
1. Export the configuration on the existing machine to a tape drive.
 2. Uninstall the SmartCenter Server from the existing machine, using sysconfig.
 3. Insert the NGX R65 CD-ROM, run the patch add cd command to upgrade the existing machine to the NGX R65 Security Gateway, and reboot.
 4. Install a new primary SmartCenter Server on the new machine.
 5. Change the gateway object to the new version, and reset SIC.
- 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 Pro gateway package.
 3. Reboot the existing machine.
 4. Perform an in-place-upgrade on the SmartCenter using the command "patch add cd".
 5. On the new machine, install SecurePlatform as the NGX R65 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: B

Explanation:

QUESTION NO: 288

Which of the following is NOT true for Management High Availability (HA)?

- A. The HA SmartCenter Servers must all be the same OS and OS Service Pack
- B. The HA SmartCenter Servers must all be the same Check Point Version
- C. If the active SmartCenter Server is down, a standby SmartCenter Servers needs to become active in order to be able to edit and install the Security Policy
- D. The HA SmartCenter Servers are synchronized so matching data is maintained and ready to be used.

Answer: A

Explanation:

QUESTION NO: 289

An internal host 10.4.8.108 successfully pings its Legacy Mode Cluster and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108. Based on this information, what is the active cluster member's IP address?

According to the output, which member is the standby machine?

- A. 10.4.8.2
- B. 10.4.8.3
- C. The active cluster member's IP address cannot be determined by this arp cache
- D. 10.4.8.1

Answer: C

Explanation:

QUESTION NO: 290

The following is cphaprob state command output from one New Mode High Availability ClusterXL cluster member: Which member will be active after member 192.168.1.2 fails over and is rebooted?

- A. Both members' state will be collision.
- B. 192.168.1.1
- C. 192.168.1.2
- D. Both members' state will be active.

Answer: B

Explanation:

QUESTION NO: 291

Match the remote-access VPN Connection mode features with their descriptions:

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

Answer: B

Explanation:

QUESTION NO: 292

The following configuration is for VPN-1 NGX R65:Is this configuration correct for Management High Availability?

- A. No, the SmartCenter Servers must be installed on the same operating system.
- B. No, the SmartCenter Servers do not have the same number of NICs.
- C. No, an NGXR65 SmartCenter Server cannot run on Red Hat Linux 7.3.
- D. NO, the SmartCenter Servers must reside on the same network.

Answer: A

Explanation:

QUESTION NO: 293

In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2. Internal host 10.4.8.108 Pings 10.4.8.3, and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108:According to the output, which member is the standby machine?

- A. 10.4.8.1
- B. The standby machine cannot be determined by this test.
- C. 10.4.8.2

D. 10.4.8.3

Answer: A

Explanation:

QUESTION NO: 294

What is the best tool to produce a report which represents historical system information?

- A. Eventia Reporter-Standard Reports
- B. Smartview Monitor
- C. SmartView Tracker
- D. Eventia Reporter-Express Reports

Answer: D

Explanation:

QUESTION NO: 295

To clean the system of all events, you should delete the files in which folder(s)?

- A. \$FWDIR\distrib
- B. \$FWDIR\events_dp
- C. \$FWDIR\distrib and \$RTDIR/events_db
- D. \$FWDIR/distrib_db and SFWDIR/events

Answer: C

Explanation:

QUESTION NO: 296

John is the MegaCorp Security Administrator, and is using Check Point R70. Malcolm is the Security Administrator of a partner company and is using a different vendor's product and both have to build a VPN tunnel between their companies. Both are using clusters with Load Sharing for their firewalls and John is using ClusterXL as a Check Point clustering solution. While trying to establish the VPN, they are constantly noticing problems and the tunnel is not stable and then Malcolm notices that there seems to be 2 SPIs with the same IP from the Check Point site. How can they solve this problem and stabilize the tunnel?

- A. This can easily be solved by using the Sticky decision function in ClusterXL.
- B. This can be solved by running the command "Sticky VPN" on the Check Point CLI. This keeps

the VPN Sticky to one member and the problem is resolved.

C. This can be solved when using clusters; they have to use single firewalls.

D. This is surely a problem in the ISPs network and not related to the VPN configuration.

Answer: A

Explanation:

QUESTION NO: 297

Which of the following commands can be used to bind a NIC to a single processor when using a Performance Pack on SecurePlatform?

A. sim affinity

B. splat proc

C. set proc

D. fw fat path nic

Answer: A

Explanation:

QUESTION NO: 298

Where can a Security Administrator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?

A. Global Properties

B. QoS Class objects

C. \$CPDIR/conf/qos_props.pf

D. Check Point gateway object properties

Answer: A

Explanation:

QUESTION NO: 299

Which of these four Check Point QoS technologies prevents the transmission of redundant packets when multiple copies of a packet are concurrently queued on the same flow?

- A. Weighted Flow Random Early Drop (WFRED)
- B. Retransmission Detection Early Drop (RDED)
- C. Intelligent Queuing Engine
- D. Stateful Inspection

Answer: B

Explanation:

QUESTION NO: 300

Which of the following components receives events and assigns severity levels to the events; then invokes any defined automatic reactions and adds the events to the Events Data Base?

- A. IPS Event Analysis DataServer
- B. IPS Event Analysis Client
- C. IPS Event Correlation Unit
- D. IPS Event Analysis Server

Answer: D

Explanation:

QUESTION NO: 301

How does ClusterXL Unicast mode handle new traffic?

- A. The pivot machine receives all the packets and runs an algorithm to determine which member should process the packets.
- B. All cluster members process all packets and members synchronize with each other. The pivot is responsible for the master sync catalog.
- C. The pivot machine receives and inspects all new packets then synchronizes the connections with other members.
- D. All members receive all packets. The Security Management Server decides which member will process the packets. Other members delete the packets from memory.

Answer: A

Explanation:

QUESTION NO: 302

In the following command, LSMcli [-d] <server> <user> <pswd> <action> "server" should be replaced with:

- A. Hostname DAIP device
- B. Hostname of ROBO gateway
- C. GUIclient
- D. IP address of the Security Management server

Answer: D

Explanation:

QUESTION NO: 303

You have three Gateways in a mesh community. Each gateway's VPN Domain is their internal network as defined on the Topology tab setting "All IP Addresses behind Gateway based on Topology information."

You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPsec tunnels instead of the routed VTI tunnels.

- A. Route-based VTI takes precedence over the Domain VPN. To make the VPN go through VTI, use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes.
- B. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.
- C. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, use an empty group object as each Gateway's VPN Domain.
- D. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community.

Answer: C

Explanation:

QUESTION NO: 304

Even after configuring central logging on Connectra, Connectra logs are not displaying in SmartView Tracker. What could be the cause of this problem?

- A. R70 does not support a host object with the same IP address as a Management Server used as secondary log server or management station.
- B. You must install the Security Policy, and try again.
- C. You must install the Management Server database.
- D. You must reestablish logging from Connectra to the Management Server, using a dummy log-

server object.

Answer: C

Explanation:

QUESTION NO: 305

How many IPS Events can be shown at one time in the Event preview pane?

- A. 1,000
- B. 30,000
- C. 15,000
- D. 5,000

Answer: B

Explanation:

QUESTION NO: 306

What cluster mode is represented in this case?

- 1 (local) 172.168.1.1 100% active
- 2 172.168.1.2 0% standby

- A. 3rd party cluster
- B. Load Sharing (multicast mode)
- C. Load Sharing Unicast (Pivot) mode
- D. HA (New mode).

Answer: D

Explanation:

QUESTION NO: 307

For best performance in Event Correlation, you should use:

- A. Nothing slows down Event Correlation
- B. Many objects
- C. Large groups
- D. IP address ranges

Answer: D

Explanation:

QUESTION NO: 308

If SmartWorkflow is configured to work without Sessions or Role Segregation, how does the SmartDashboard function?

- A. The SmartDashboard will have no session but SmartView Tracker and audit trail will be available.
- B. The SmartDashboard functions as if SmartWorkflow is not enabled but an automatic session exists in the background and full SmartView tracker and audit trail functionality will be available.
- C. All functions of SmartWorkflow will be available on a per rule basis.
- D. The SmartDashboard will function without SmartWorkflow, with no session and no audit trail functionality.

Answer: B

Explanation:

QUESTION NO: 309

Which Check Point QoS feature marks the ToS byte in the IP header?

- A. Weighted Fair Queuing
- B. Low Latency Queuing
- C. Guarantees
- D. Differentiated Services

Answer: D

Explanation:

QUESTION NO: 310

When configuring a Web Application for SSL VPN remote access, you have given the following definition for the application along with its protection level.

- A. www.dmz.example.com
- B. dmz .example.com/extranet
- C. www.example.com/intranet
- D. hr.dmz.example.com/intranet

Answer: C

Explanation:

QUESTION NO: 311

You need to verify the effectiveness of your IPS configuration for your Web server farm. You have a colleague run penetration tests to confirm that the Web servers are secure against traffic hijacks. Of the following, which would be the best configuration to protect from a traffic hijack attempt?

- A. Create resource objects for the Web farm servers and configure rules for the Web farm.
- B. Enable the Web intelligence > SQL injection setting.
- C. Configure TCP defenses such as Small PMTU size.
- D. Activate the Cross-Site Scripting property.

Answer: D

QUESTION NO: 312

URL Filtering Policy can make exceptions for specific sites by being enforced...

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

Answer: C

Explanation: