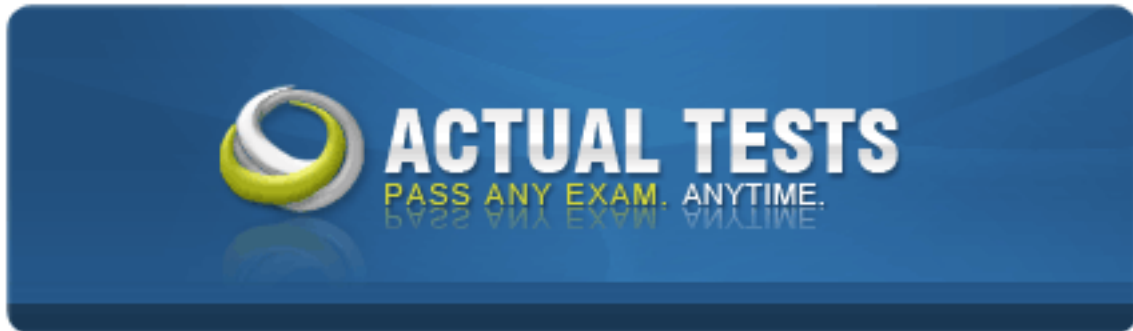


Checkpoint 156-315-71



Check Point Security Expert R71

Practice Test

Version: 5.0

QUESTION NO: 1

You need to publish SecurePlatform routes using the ospf routing protocol. What is the correct command structure, once entering the route command, to implement ospf successfully?

- A. Run cpconfig utility to enable ospf routing
- B. ip route ospf
ospf network1
ospf network2
- C. Enable
Configure terminal
Router ospf [id]
Network [network] [wildmask] area [id]
- D. Use DBedit utility to either the objects_5_0.c file

Answer: C

Explanation:

QUESTION NO: 2

Control connections between the Security Management Server and the Gateway are not encrypted by the VPN Community. How are these 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 PPTP
- D. They are not secured.

Answer: A

Explanation:

QUESTION NO: 3

How does a cluster member take over the VIP after a failover event?

- A. Ping the sync interface
- B. if list -renew
- C. Broadcast storm
- D. Gratuitous ARP

Answer: D

Explanation:

QUESTION NO: 4

You want to verify that your Check Point cluster is working correctly. Which command line tool can you use?

- A. cphaconf state
- B. cphaprob state
- C. cphainfo-s
- D. cphastart -status

Answer: B

Explanation:

QUESTION NO: 5

_____ is a proprietary Check Point protocol, it is the basis for Check Point ClusterXL inter-module communication.

- A. RDP
- B. CCP
- C. CKPP
- D. HA OPCODE

Answer: B

Explanation:

QUESTION NO: 6

John is configuring a New R71 Gateway cluster but he cannot configure the cluster as Third Party IP Clustering because his option is not available in Gateway Cluster Properties.

What's happening?

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

Answer: A

Explanation:

QUESTION NO: 7

You are MegaCorp Security Administrator. This company uses a firewall cluster, consisting of two cluster members. The cluster generally works well but one day you find that the cluster is behaving strangely. You assume that there is a connectivity problem with the cluster synchronization cluster link (cross-over cable).

Which of the following commands is the best for testing the connectivity of the crossover cable?

- A. telnet <IP address of the synchronization interface on the other cluster member>
- B. arping <IP address of the synchronization interface on the other cluster member>
- C. ifconfig -a
- D. Ping <IP address of the synchronization interface on the other cluster member>

Answer: D

Explanation:

QUESTION NO: 8

Organizations are sometimes faced with the need to locate cluster members in different geographic locations that are distant from each other. A typical example is replicated data centers whose location is widely separated for disaster recovery purposes.

What are the restrictions of this solution?

- A. There are no restrictions.
- B. There is one restriction: The synchronization network must guarantee no more than 150 ms latency (ITU Standard G.114).
- C. There is one restriction: The synchronization network must guarantee no more than 100 ms latency.
- D. There are two restrictions: 1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss. 2. The synchronization network may only include switches and hubs.

Answer: D

Explanation:

QUESTION NO: 9

You are establishing a ClusterXL environment, with the following topology:

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 Security Management 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. The Security Management Server must be in the dedicated synchronization network, not the internal network.
- C. The Cluster interface names must be identical across all cluster members.
- D. Cluster members cannot use the VLAN switch. They must use hubs.

Answer: B

Explanation:

QUESTION NO: 10

Match the ClusterXL Modes with their configurations:

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

Answer: C

Explanation:

QUESTION NO: 11

Check point Clustering protocol, works on:

- A. UDP 8116
- B. UDP 500
- C. TCP 8116
- D. TCP 19864

Answer: A

Explanation:

QUESTION NO: 12

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

- A. fw ctl setsync 0
- B. fw ctl sysnstat stop
- C. fw ctl sysnstat off
- D. fw ctl setsyns off

Answer: D

Explanation:

QUESTION NO: 13

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

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

Answer: C

Explanation:

QUESTION NO: 14

Which procedure creates a new administrator in SmartWorkflow?

- A. Run cpconfig, supply the Login Name. Profile Properties, Name, Access Applications and Permissions.
- B. In SmartDashboard, click SmartWorkflow / Enable SmartWorkflow and the Enable SmartWorkflow wizard will start. Supply the Login Name, Profile Properties, Name, Access Applications and Permissions when prompted.
- C. On the Provider-1 primary MDS, run cpconfig, supply the Login Name, Profile Properties, Name, Access Applications and Permissions.
- D. In SmartDashboard, click Users and Administrators right click Administrators / New Administrator and supply the Login Name. Profile Properties, Name, Access Applications and Permissions.

Answer: D

Explanation:

QUESTION NO: 15

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. IPS Web Intelligence is enabled to check on the host.

Answer: B

Explanation:

QUESTION NO: 16

Which external user authentication protocols are supported in SSL VPN?

- A. LDAP, Active Directory, SecurID
- B. DAP, SecurID, Check Point Password, OS Password, RADIUS, TACACS
- C. LDAP, RADIUS, Active Directory, SecurID
- D. LDAP, RADIUS, TACACS, SecurID

Answer: B

Explanation:

QUESTION NO: 17

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: 18

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: A

Explanation:

QUESTION NO: 19

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

- A. Smart Dashboard Log Consolidator
- B. Security Management Server
- C. Smart Reporter Database
- D. Smart Reporter

Answer: D

Explanation:

QUESTION NO: 20

What is a task of the SmartEvent Correlation Unit?

- A. Add events to the events database.
- B. Look for patterns according to the installed Event Policy.
- C. Assign a severity level to an event
- D. Display the received events.

Answer: D

Explanation:

QUESTION NO: 21

Based on the following information, which of the statements below is FALSE?

A DLP Rule Base has the following conditions:

Data Type =Password Protected File

Source=My Organization

Destination=Outside My Organization

Protocol=Any

Action=Ask User

Exception:Data Type=Any,

Source=Research and Development (R&D)

Destination=Pratner1.com

Protocol=Any

All other rules are set to Detect. UserCheck is enabled and installed on all client machines.

- A.** When a user from R&D sends an e-mail with a password protected PDF file as an attachment to xyz@partner1 .com, he will be prompted by UserCheck.
- B.** When a user from Finance sends an e-mail with an encrypted ZIP file as an attachment to. He will be prompted by UserCheck.
- C.** Another rule is added: Source = R&D, Destination = partner1.com, Protocol = Any, Action = Inform. When a user from R&D sends an e-mail with an encrypted ZIP file as an attachment to, he will be prompted by UserCheck.
- D.** When a user from R&D sends an e-mail with an encrypted ZIP file as an attachment to , he will NOT be prompted by UserCheck.

Answer: B

Explanation:

QUESTION NO: 22

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

```
vpn shell 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 Gateway.

Answer: A

Explanation:

QUESTION NO: 23

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, on 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: 24

When running DIP Wizard for the first time, which of the following is a mandatory configuration?

- A. Mail Server
- B. E-mail Domain in My Organization
- C. DLP Portal URL
- D. Active Directory

Answer: B

Explanation:

QUESTION NO: 25

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: D

Explanation:

QUESTION NO: 26

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

- A. SmartReporter
- B. SmartView Monitor
- C. SmartView Status
- D. SmartView Tracker

Answer: D

Explanation:

QUESTION NO: 27

What is not available for Express Reports compared to Standard Reports?

- A. Filter
- B. Period
- C. Content
- D. Schedule

Answer: A

Explanation:

QUESTION NO: 28

Based on the following information, which of the statements below is TRUE?

A DLP Rule Base has the following conditions:

Data Type = Large file (> 500KB)

Source = My Organization

Destination = Free Web Mails

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 UserCheck
- B. When a user sends an e-mail with a small body and 5 attachments, each of 200 KB to, he will

be prompted by UserCheck.

C. When a user sends an e-mail with an attachment larger than 500 KB to, he will be prompted by UserCheck.

D. When a user sends an e-mail with an attachment larger than 500KB to, he will be prompted by UserCheck.

Answer: A

Explanation:

QUESTION NO: 29

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: 30

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 incidents, the portal authenticates the user using only AD/LDAP.

B. Check Point UserCheck client authentication is based on AD.

C. For SMTP traffic, each recipient e-mail address is translated using AD/LDAP to a user name and group that is checked vs. the destination column of the DLP rule base.

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 rule base.

Answer: B

Explanation:

QUESTION NO: 31

You are running R71 and using the new IPS Software Blade. To maintain the highest level of security, you are doing IPS updates regularly- What kind of problems can be caused by the

automatic updates?

- A. None; updates will not add any new security checks causing problematic behavior on the systems.
- B. None, all new updates will be implemented in Detect only mode to avoid unwanted traffic interruptions. They have to be activated manually later
- C. None, all the checks will be activated from the beginning, but will only detect attacks and not disturb any non-malicious traffic in the network.
- D. All checks will be activated from the beginning and might cause unwanted traffic outage due to false positives of the new checks and non-RFC compliant self-written applications.

Answer: B

Explanation:

QUESTION NO: 32

Which of the following deployment scenarios CANNOT be managed by Check Point QoS?

- A. Two lines connected to a single router, and the router is connected directly to the Gateway
- B. Two lines connected to separate routers, and each router is connected to separate interfaces on the Gateway
- C. One LAN line and one DMZ line connected to separate Gateway interfaces
- D. Two lines connected directly to the Gateway through a hub

Answer: A

Explanation:

QUESTION NO: 33

Given the following protection detailed and the enforcing gateways list, is the Too many DNS queries with the RD flag set protection enabled on the Gateway R71? Please choose the answer with the correct justification.

- A. yes because it is set to prevent on the Default_Protection, which R71 gateway has applied.
- B. No because the protection is only supported on IPS-1 Sensor
- C. No enough information to determine one way or other
- D. No, because the Too many DNS queries with the flag set protection is not a valid protection in R71

Answer: A

Explanation:

QUESTION NO: 34

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

- A. SmartProvisioning
- B. SmartBlade
- C. SmartDashboard
- D. SmartLSM

Answer: A

Explanation:

QUESTION NO: 35

Which technology is responsible for assembling packet streams and passing ordered data to the protocol parsers in IPS?

- A. Pattern Matcher
- B. Content Management Infrastructure
- C. Accelerated INSPECT
- D. Packet Streaming Layer

Answer: D

Explanation:

QUESTION NO: 36

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

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

Answer: D

Explanation:

QUESTION NO: 37

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic is passing through the QoS Module matches both rules, which of the following statements is TRUE?

- A. Each H.323 connection will receive at least 512 Kbps of bandwidth.
- B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
- C. 50% of available bandwidth will be allocated to the Default Rule.
- D. Neither rule will be allocated more than 10% of available bandwidth.

Answer: B

Explanation:

QUESTION NO: 38

Which method of load balancing describes "Round Robin"?

- A. Assigns service requests to the next server in a series.
- B. Ensures that incoming requests are handled by the server with the fastest response time.
- C. Measures the load on each server to determine which server has the most available resources.
- D. Assigns service requests to servers at random.

Answer: A

Explanation:

QUESTION NO: 39

For Management High Availability synchronization, what does the Advance status mean?

- A. The Active SMS and its peer have different installed policies and databases.
- B. The peer SMS is properly synchronized.
- C. The peer SMS has not been synchronized properly.
- D. The peer SMS is more up-to-date.

Answer: D

Explanation:

QUESTION NO: 40

In Load Sharing Unicast mode, the internal cluster IP 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 pivot machine?

- A. 10.4.8.2
- B. 10.4.8.1
- C. 10.4.8.3
- D. The pivot machine cannot be determined by this test.

Answer: A

Explanation:

QUESTION NO: 41

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

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

Answer: D

Explanation:

QUESTION NO: 42

How is SmartWorkflow enabled?

- A. In SmartView Monitor, click on SmartWorkflow / Enable SmartWorkflow. The Enabling SmartWorkflow wizard launches and prompts for SmartWorkflow Operation Mode. Once a mode is selected, the wizard finishes.
- B. In SmartView Tracker, click on SmartWorkflow / Enable SmartWorkflow. The Enabling SmartWorkflow wizard launches and prompts for SmartWorkflow Operation Mode Once a mode is selected, the wizard finishes.
- C. In SmartDashboard, click on SmartWorkflow / Enable SmartWorkflow The Enabling SmartWorkflow wizard launches and prompts for SmartWorkflow Operation Mode. Once a mode is

selected, the wizard finishes.

D. In SmartEvent, click on SmartWorkflow/ Enable SmartWorkflow. The Enabling SmartWorkflow wizard launches and prompts for SmartWorkflow Operation Mode. Once a mode is selected, the wizard finishes.

Answer: C

Explanation:

QUESTION NO: 43

A SmartProvisioning Gateway could be a member of which VPN communities?

- (i) Center In Star Topology
- (ii) Satellite in Star Topology
- (iii) Carter in Remote Access Community
- (iv) Meshed Community

- A.** (ii) and (iii)
- B.** (ii) only
- C.** All
- D.** (i), (ii), (iii)

Answer: A

Explanation:

QUESTION NO: 44

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

$\$([0-9]^*, [0-9] [0-9] [0-9]. [0-9] [0-9])$

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 Finance Department from leaking salary information to employees

Answer: B

Explanation:

QUESTION NO: 45

True or False User A is able to create a SmartLSM Security Cluster Profile e, 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 Profiles
- 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: D

Explanation:

QUESTION NO: 46

Which Check Point QoS feature is used to dynamically allocate relative portions of available bandwidth?

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

Answer: B

Explanation:

QUESTION NO: 47

Which SmartReporter report type is generated from the SmartView Monitor history file?

- A. Express
- B. Standard
- C. Custom
- D. Traditional

Answer: A

Explanation:

QUESTION NO: 48

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

- A.** The new connection will be 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 or 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: 49

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

- A.** fw ctl get kernel
- B.** fw ctl pstat
- C.** fw kernel
- D.** fw ver -k

Answer: D

Explanation:

QUESTION NO: 50

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. 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: 51

John is the MegaCorp Security Administrator, and is using Check Point R71. 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 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.
- B.** This is surely a problem in the ISPs network and not related to the VPN configuration.
- C.** This can be solved when using clusters; they have to use single firewalls.
- D.** This can easily be solved by using the Sticky decision function in ClusterXL.

Answer: D

Explanation:

QUESTION NO: 52

The following is cphaprob state command output from one New Mode High Availability ClusterXL cluster member

```
Cluster Mode: New High Availability <Active Up>
Number      Unique IP Address  Assigned Load  State
1 <local>    192.168.1.1       0%            standby
2           192.168.1.2       100%          active
```

Which member will be active after member 192.168.12 fails over and is rebooted?

- A. 92.168.12
- B. Both members' state will be active.
- C. 192168.1.1
- D. Both members' state will be in collision

Answer: C

Explanation:

QUESTION NO: 53

Laura notices the Microsoft Visual Basic Bits Protection is set to inactive. She wants to set the Microsoft Visual Basic Kill Bits Protection and all other Low Performance Impact Protections to Prevent. She asks her manager for approval and stated she can turn these on. But he wants Laura to make sure no high Performance Impacted Protections are turned on while changing this setting.

Using the out below, how would Laura change the Default_Protection on Performance Impact Protections classified as low from inactive to prevent until meeting her other criteria?

- A. Go to Profiles / 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 uncheck Do not activate protections with performance impact to high or above

Answer: C

Explanation:

QUESTION NO: 54

The following graphic illustrates which command being issued on SecurePlatform?

When a security administrator selects Repair for a 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: 55

Refer to the to the network topology below. You have IPS software Blades active on security Gateways sglondon, sgla, and sgny, 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. Attacker may have used a touch of evasion techniques like using escape sequences instead of clear text commands. It is also possible that there are entry points not shown in the network layout, like rouge access points.
- C. Since other Gateways do not have IPS activated, attacks may originate from their networks without any noticing
- D. An IPS may combine different technologies, but is dependent on regular signature updates and well-turned automatically algorithms. Even if this is accomplished, no technology can offer 100% protection.

Answer: A

Explanation:

QUESTION NO: 56

Which Check Point product implements Consolidation policy?

- A. SmartView Monitor
- B. SmartLSM
- C. SmartView Tracker
- D. SmartReporter

Answer: D

Explanation:

QUESTION NO: 57

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: A

Explanation:

QUESTION NO: 58

You have installed SecurePlatform R71 as Security Gateway operating system. As company requirements changed, you need the VTI features of R71 would you do?

- A. Only IPSO 3.9 supports VTI feature, so you have to replace your Security Gateway with Nokia appliances.
- B. Type pro enable on your Security Gateway and reboot it.
- C. You have to re-install your Security Gateway with SecurePlatform Pro R71, as SecurePlatform R71 does not support VTIs.
- D. In SmartDashboard click on the OS drop down menu and choose SecurePlatform Pro. You have to reboot the Security Gateway in order for the change to take effect.

Answer: B

Explanation:

QUESTION NO: 59

How is change approved for implementation in SmartWorkflow?

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

Answer: C

Explanation:

QUESTION NO: 60

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: 61

What is a task of the SmartEvent Correlation Unit?

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

Answer: C

Explanation:

QUESTION NO: 62

Provisioning Profiles can NOT be applied to:

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

Answer: C

Explanation:

QUESTION NO: 63

What is the lowest possible version a Security Gateway may be running in order to use it as an LSM enabled Gateway?

- A. NG-AI R55 HFAJ7
- B. NGX R60
- C. NGXR65HFA_50
- D. NGX R71

Answer: A

Explanation:

QUESTION NO: 64

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: 65

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: 66

One profile in SmartProvisioning can update:

- A. Potentially hundreds and thousands of gateways.

- B. Only Clustered Gateways.
- C. Specific gateways.
- D. Profiles are not used for updating, just reporting.

Answer: A

Explanation:

QUESTION NO: 67

What cluster mode is represented in this case?

1 (local)172.168.1.1100\$active

2 172.14*.1.2 0\$standby

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

Answer: B

Explanation:

QUESTION NO: 68

Check Point recommends deploying SSL VPN:

- A. In parallel to the firewall
- B. In a DMZ
- C. In front of the firewall with a LAN connection
- D. On the Primary cluster member

Answer: C

Explanation:

QUESTION NO: 69

Which type of routing relies on a VPN Tunnel Interface (VTI) to route traffic?

- A. Subnet-based VPN

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

Answer: B

Explanation:

QUESTION NO: 70

What are the SmartProvisioning Provisioning Profile indicators?

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

Answer: B

Explanation:

QUESTION NO: 71

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. SmartEvent Client
- B. SmartEvent Server
- C. SmartEvent Correlation Unit
- D. SmartEvent Analysis Data Server

Answer: B

Explanation:

QUESTION NO: 72

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: 73

Which of the following can NOT be modified by editing the cp_httpd_admin.conf file?

- A. Toggling HTTP or HTTPS protocol use
- B. The web server port
- C. Modifying Web server certificate attributes
- D. Administrative Access Level

Answer: B

Explanation:

QUESTION NO: 74

John is upgrading a cluster from NGX R65 to R71. John knows that you can verify the upgrade process using the pre-upgrade verifier tool. When John is running Pre-Upgrade Verification, he sees this warning message: Title: Incompatible pattern. What's happening?

- A. The actual configuration contains user defined patterns in IPS that are not supported in R71. If the patterns are not fixed after upgrade, they will not be used with R71 Security Gateways.
- B. R71 uses a new pattern matching engine. Incompatible patterns should be deleted before upgrade process to complete it successfully.
- C. Pre-Upgrade Verification tool only shows that message but it is only informational.
- D. Pre-Upgrade Verification process detected a problem with actual configuration and upgrade will be aborted.

Answer: A

Explanation:

QUESTION NO: 75

SmartWorkflow has been enabled with the following configuration.

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

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

Answer: B

Explanation:

QUESTION NO: 76

If traffic requires preferential treatment by other routers on the network, in addition to the QoS module, which Check Point QoS feature should be used?

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

Answer: B

Explanation:

QUESTION NO: 77

You are concerned that the processor for your firewall running NGX R71 SecurePlatform may be overloaded. What file would you view to determine the speed of your processors)?

- A. cat /etc/cpuinfo
- B. cat /var/opt/CPsuite-R71/fw1/conf/cpuinfo
- C. cat /etc/sysconfig/cpuinfo
- D. cat /proc/cpuinfo

Answer: D

Explanation:

QUESTION NO: 78

In Company XYZ, the DLP Administrator defined a new Keywords Data Type that contains a list of secret project names; i.e. Ayalon, Yarkon, 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. A PDF file that contains the following text
Yarkon1 can be the code name 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 will match:
Ayalon
ayalon
AYALON
- D. A password protected MS Excel file that contains the following text
Ayalon
Yarkon
Yarden

Answer: B

Explanation:

QUESTION NO: 79

With SmartEvent, what is the Client's function?

- A. Display received threats and tune the Events Policy
- B. Generate a threat analysis report from the Reporter database.
- C. Assign severity levels to events.
- D. Invoke and define automatic reactions and add events to the database

Answer: A

Explanation:

QUESTION NO: 80

Which Name Resolution protocols are supported in SSL VPN?

- A. DNS, hosts, lmhosts, WINS
- B. DNS, hosts, lmhosts
- C. DNS, hosts, WINS
- D. DNS, hosts

Answer: D

Explanation:

QUESTION NO: 81

Which statement about LDAP and Active Directory (AD) with SSL VPN is TRUE?

- A. SSL VPN does not support LDAP password remediation.
- B. SSL VPN is capable of administering or creating users and groups directly on an LDAP server.
- C. SSL VPN never stores the user records of LDAP/AD groups.
- D. By default, SSL VPN sends username and password credentials to LDAP servers in UTF-8 encoding

Answer: B

Explanation:

QUESTION NO: 82

To configure the Cluster Control Protocol (CCP) to use Broadcast, the following command is run:

- A. set_ccp cpcluster broadcast:
- B. cphaconf set_ccp broadcast
- C. ccp broadcast
- D. clusterconfig set_ccp broadcast

Answer: B

Explanation:

QUESTION NO: 83

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

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

Answer: A

Explanation:

QUESTION NO: 84

Which 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: 85

How does ClusterXL Unicast mode handle new traffic?

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

Answer: C

Explanation:

QUESTION NO: 86

When do modifications to the Event Policy take effect?

- A.** As soon as the Policy Tab window is closed.
- B.** When saved on the SmartEvent Server and installed to the Correlation Units.
- C.** When saved on the SmartEvent Client, and installed on the SmartEvent Server.
- D.** When saved on the Correlation Units, and pushed as a policy

Answer: C

Explanation:

QUESTION NO: 87

Which of the following explains Role Segregation?

- A.** Administrators have different abilities than managers within SmartWorkflow.
- B.** Different tasks within SmartDashboard are divided according to firewall administrator permissions.
- C.** Changes made by an administrator in a SmartWorkflow session must have managerial approval prior to commitment.
- D.** SmartWorkflow can be configured so that managers can only view their assigned sessions

Answer: C

Explanation:

QUESTION NO: 88

To clean the system of all events, you should delete the files in which folders?

- A. \$FWDIR/distrib
- B. \$FWDIR/ events_db
- C. \$FWDIR/distrib and \$PWDIR/events_db
- D. \$FWDIR/distrib db and \$FWDIR/events

Answer: C

Explanation:

QUESTION NO: 89

A user cannot authenticate to SSL VPN. You have verified the user is assigned a user group and reproduced the problem, confirming a failed-login session. You do not see an indication of this attempt in the traffic log. The user is not using a client certificate for login. To debug this error, where in the authentication process could the solution be found?

- A. apache
- B. admin
- C. cvpnd
- D. cpauth

Answer: C

Explanation:

QUESTION NO: 90

Which Protection Mode does not exist in IPS?

- A. Allow
- B. Detect
- C. Prevent
- D. Inactive

Answer: D

Explanation:

QUESTION NO: 91

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: 92

Which of the following does NOT happen when using Pivot Mode in ClusterXL?

- A.** The Pivot forwards the packet to the appropriate cluster member.
- B.** The Pivot's Load Sharing decision function decides which cluster member should handle the packet.
- C.** The Security Gateway analyzes the packet and forwards it to the Pivot.
- D.** The packet is forwarded through the same physical interface from which it originally came, not on the sync interface

Answer: C

Explanation:

QUESTION NO: 93

Which of the following actions is most likely to improve the performance of Check Point QoS?

- A. Put the most frequently used rules at the bottom of the QoS Rule Base.
- B. Define Check Point QoS only on the external interfaces of the QoS Module.
- C. Turn per rule limits into per connection limits
- D. Turn per rule guarantees into per connection guarantees.

Answer: B

Explanation:

QUESTION NO: 94

Where is the encryption domain for a SmartLSM Security Gateway configured in R71?

- A. Inside the SmartLSM Security Gateway object in the SmartDashboard GUI
- B. Inside the SmartLSM Security Gateway profile in the SmartProvisioning GUI
- C. Inside the SmartLSM Security Gateway object in the SmartProvisioning GUI
- D. Inside the SmartLSM Security Gateway profile in the SmartDashboard GUI

Answer: B

Explanation:

QUESTION NO: 95

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 because the system does not permit him to do so?

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 this difference?

- A. There were some Hardware/Software issues at Security Management server on the first day.
- B. Peter was not logged on to system for a longer time
- C. The attribute Manage Administrator was not assigned to Peter
- D. The specific SmartWorkflow read/Write permission were assigned to David only.

Answer: C

Explanation:

QUESTION NO: 96

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: A

Explanation:

QUESTION NO: 97

From the following output of chaprob state, which ClusterXL mode is this?

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

Answer: C

Explanation:

QUESTION NO: 98

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

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

Answer: D

Explanation:

QUESTION NO: 99

When load sharing Multicast mode is defined in a ClusterXL cluster object, how are packets being

handled by cluster members?

- A. only one member at a time is active. The active cluster member processes all packets.
- B. All members receive all packets. All members run an algorithm which determines which member processes packets further and which members delete the packet from memory.
- C. AB cluster members process all packets and members synchronize with each other.
- 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: B

Explanation:

QUESTION NO: 100

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

- A. SSL VPN adds another layer of access security to internal resources, when it resides in a DMZ.
- 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: 101

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 (ii) only

Answer: D

Explanation:

QUESTION NO: 102

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-initialize SIC

Answer: B

Explanation:

QUESTION NO: 103

What is the proper command for importing users into the R71 User Database?

- A. fwm import
- B. fwm importusrs
- C. fwm importdb
- D. fwm dbimport

Answer: D

Explanation:

QUESTION NO: 104

What port is used for Administrator access for your SSL VPN?

- A. 80
- B. 4433
- C. 4434
- D. 443

Answer: D

Explanation:

QUESTION NO: 105

You have just upgraded your HA gateway cluster (both members) from NGX R65 to R71.

cphaprob stat shows:

Which of the following is not a possible cause of this?

- A. You have not run cpconfig on member 2 yet.
- B. Member 1 has CoreXL disabled and member 2 does not
- C. Member 1 is at a lower version than member 2
- D. You have a different number of cores defined for CoreXL between the two members

Answer: C

Explanation:

QUESTION NO: 106

What is the behavior of ClusterXL in a High Availability environment?

- A. Both members respond to the virtual address and both members pass traffic.
- B. Both members respond to the virtual address but only the active member is able to pass traffic
- C. The active member responds to the virtual address and is the only member that passes traffic.
- D. The active member responds to the virtual address and, using sync network forwarding, both members pass traffic

Answer: C

Explanation:

QUESTION NO: 107

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

- 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: 108

What is the command to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 SmartCenter Server to VPN-1 NGX using a CD?

- A. cd patch add
- B. fwm upgrade_tool
- C. cppkg add
- D. patch add
- E. patch add cd

Answer: E

Explanation:

QUESTION NO: 109

You have a production implementation of Management High Availability, at version VPN-1 NG with Application Intelligence R55. You must upgrade your two SmartCenter Servers to VPN-1 NGX. What is the correct procedure?

- A. 1. Synchronize the two SmartCenter Servers.
2. Upgrade the secondary SmartCenter Server.
3. Upgrade the primary SmartCenter Server.
4. Configure both SmartCenter Server host objects version to VPN-1 NGX.
5. Synchronize the Servers again.
- B. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Upgrade the secondary SmartCenter Server.
4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
5. Synchronize the Servers again.
- C. 1. Perform an advanced upgrade on the primary SmartCenter Server.
2. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
3. Synchronize the primary with the secondary SmartCenter Server.
4. Upgrade the secondary SmartCenter Server.
5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
6. Synchronize the Servers again.
- D. 1. Synchronize the two SmartCenter Servers.
2. Perform an advanced upgrade on the primary SmartCenter Server.
3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
4. Synchronize the two Servers again.
5. Upgrade the secondary SmartCenter Server.
6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.
7. Synchronize the Servers again.

Answer: B

Explanation:

QUESTION NO: 110

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Pro 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, without making any changes to the existing primary SmartCenter Server? (Changes can include uninstalling and reinstalling.)

- A.** You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- B.** The new machine cannot be installed as the Internal Certificate Authority on its own.
- C.** The secondary Server cannot be installed on a SecurePlatform Pro machine alone.
- D.** Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server.

Answer: A

Explanation:

QUESTION NO: 111

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: 256 MB, Security Gateway version: VPN-1 NGX

Cluster Member 2: OS: SecurePlatform, NICs: four Intel 3Com, memory: 512 MB, Security Gateway version: VPN-1 NGX

Cluster Member 3: OS: SecurePlatform, NICs: four other manufacturers, memory: 128 MB, Security Gateway version: VPN-1 NGX

SmartCenter Pro Server: MS Windows Server 2003, NIC: Intel NIC (one), Security Gateway and primary SmartCenter Server installed version: VPN-1 NGX

Are these machines correctly configured for a ClusterXL deployment?

- A.** No, the SmartCenter Pro Server is not using the same operating system as the cluster members.
- B.** Yes, these machines are configured correctly for a ClusterXL deployment.
- C.** No, Cluster Member 3 does not have the required memory.
- D.** No, the SmartCenter Pro Server has only one NIC.

Answer: B

Explanation:

QUESTION NO: 112

You set up a mesh VPN Community, so your internal networks can access your partner's network, and vice versa. Your Security Policy encrypts only FTP and HTTP traffic through a VPN tunnel. All other traffic among your internal and partner networks is sent in clear text. How do you configure the VPN Community?

- A.** Disable "accept all encrypted traffic", and put FTP and HTTP in the Excluded services in the Community object. Add a rule in the Security Policy for services FTP and http, with the Community object in the VPN field.
- B.** Disable "accept all encrypted traffic" in the Community, and add FTP and HTTP services to the Security Policy, with that Community object in the VPN field.
- C.** Enable "accept all encrypted traffic", but put FTP and HTTP in the Excluded services in the Community. Add a rule in the Security Policy, with services FTP and http, and the Community object in the VPN field.
- D.** Put FTP and HTTP in the Excluded services in the Community object. Then add a rule in the Security Policy to allow Any as the service, with the Community object in the VPN field.

Answer: B

Explanation:

QUESTION NO: 113

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

- A.** The remote Gateways must set up SIC with the secondary SmartCenter Server, for logging.
- B.** 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.
- C.** On the Log Servers screen (from the Logs and Masters tree on the gateway object's General Properties screen), add the secondary SmartCenter Server object as the additional log server. Reinstall the Security Policy.
- 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 screen.
- E.** The secondary Server's host name and IP address must be added to the Masters file, on the remote Gateways.

Answer: C

Explanation:

QUESTION NO: 114

You want only RAS signals to pass through H.323 Gatekeeper and other H.323 protocols, passing directly between end points. Which routing mode in the VoIP Domain Gatekeeper do you select?

- A. Direct
- B. Direct and Call Setup
- C. Call Setup
- D. Call Setup and Call Control

Answer: A

Explanation:

QUESTION NO: 115

Which component functions as the Internal Certificate Authority for VPN-1 NGX?

- A. VPN-1 Certificate Manager
- B. SmartCenterServer
- C. SmartLSM
- D. Policy Server
- E. Security Gateway

Answer: B

Explanation:

QUESTION NO: 116

You are configuring the VoIP Domain object for a Skinny Client Control Protocol (SCCP) environment protected by VPN-1 NGX. Which VoIP Domain object type can you use?

- A. CallManager
- B. Gatekeeper
- C. Gateway
- D. Proxy
- E. Transmission Router

Answer: A

Explanation:

QUESTION NO: 117

What type of packet does a VPN-1 SecureClient send to its Policy Server, to report its Secure Configuration Verification status?

- A. ICMP Port Unreachable
- B. TCP keep alive
- C. IKE Key Exchange
- D. ICMP Destination Unreachable
- E. UDP keep alive

Answer: E

Explanation:

QUESTION NO: 118

Which Security Servers can perform Content Security tasks, but CANNOT perform authentication tasks?

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

Answer: C

Explanation:

QUESTION NO: 119

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?

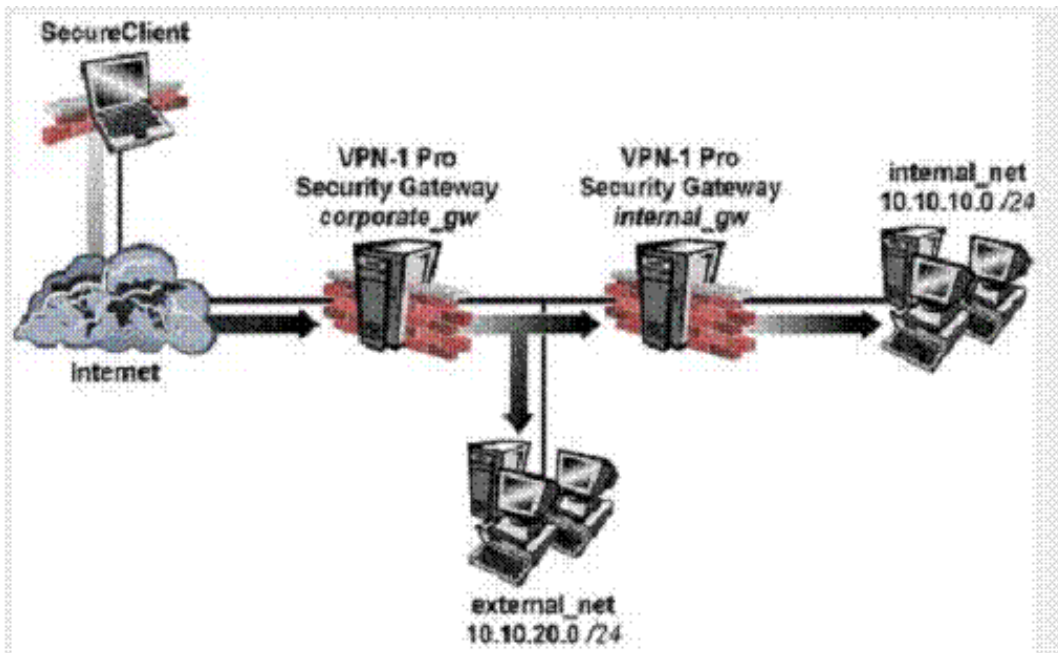
- A. internal_clear > All_GwToGw
- B. Communities > Communities
- C. Internal_clear > External_Clear
- D. Internal_clear > Communities
- E. internal_clear > All communities

Answer: E

Explanation:

QUESTION NO: 120

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external_net and internal_net from the Internet. How is the Security Gateway VPN Domain created?



- A. Internal Gateway VPN Domain = internal_net;
External VPN Domain = external net + external gateway object + internal_net.
- B. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = external_net + internal gateway object
- C. Internal Gateway VPN Domain = internal_net;
External Gateway VPN Domain = internal_net + external_net
- D. Internal Gateway VPN Domain = internal_net.
External Gateway VPN Domain = internal VPN Domain + internal gateway object + external_net

Answer: D

Explanation:

QUESTION NO: 121

A 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's IP address is 172.28.108.3, and the internal cluster's IP 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, cphaprob if command output displays as follows: What is causing the State Synchronization problem?

```
Required interfaces: 3
Required secured interfaces: 1
eth0CUP (sync, secured) multicast
eth1 UP non sync (non secured) multicast
eth2 UP non sync (non secured), multicast
Virtual cluster interfaces: 3
eth0 192.168.1.3
eth1 172.28.108.3
eth2 10.4.8.3
```

- A. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.
- B. Interfaces 192.168.1.1 and 192.168.1.2 have defined 192.168.1.3 as a suB. interface.
- C. The synchronization interface on the cluster member object's Topology tab is enabled with "Cluster Interface". Disable this interface.
- D. The synchronization network has a cluster, with IP address 192.168.1.3 defined in the gateway-cluster object. Remove the 192.168.1.3 VIP interface from the cluster topology.

Answer: D

Explanation:

QUESTION NO: 122

How can you completely tear down a specific VPN tunnel in an intranet IKE VPN deployment?

- A. Run the command `vpn tu` on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
- B. Run the command `vpn tu` on the SmartCenter Server, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".
- C. Run the command `vpn tu` on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for a given peer (GW)".
- D. Run the command `vpn tu` on the Security Gateway, and choose the option "Delete all IPSec SAs for a given user (Client)".
- E. Run the command `vpn tu` on the Security Gateway, and choose the option "Delete all IPSec SAs for ALL peers and users".

Answer: C

Explanation:

QUESTION NO: 123

How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queues when using a Check Point QoS solution?

- A. Low latency class
- B. DiffServrule
- C. guaranteed per connection
- D. Weighted Fair Queuing
- E. guaranteed per VoIP rule

Answer: A

Explanation:

QUESTION NO: 124

You are preparing to deploy a VPN-1 Pro Gateway for VPN-1 NGX. You have five systems to choose from for the new Gateway, and you must conform to the following requirements:

- Operating-system vendor's license agreement
- Check Point's license agreement
- Minimum operating-system hardware specification
- Minimum Gateway hardware specification
- Gateway installed on a supported operating system (OS)

Which machine meets ALL of the following requirements?

- A. Processor: 1.1 GHz RAM: 512MB Hard disk: 10 GB OS: Windows 2000 Workstation
- B. Processor: 2.0 GHz RAM: 512MB Hard disk: 10 GB OS: Windows ME
- C. Processor: 1.5 GHz RAM: 256 MB Hard disk: 20 GB OS: Red Hat Linux 8.0
- D. Processor: 1.67 GHz RAM: 128 MB Hard disk: 5 GB OS: FreeBSD
- E. Processor: 2.2 GHz RAM: 256 MB Hard disk: 20 GB OS: Windows 2000 Server

Answer: E

Explanation:

QUESTION NO: 125

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.

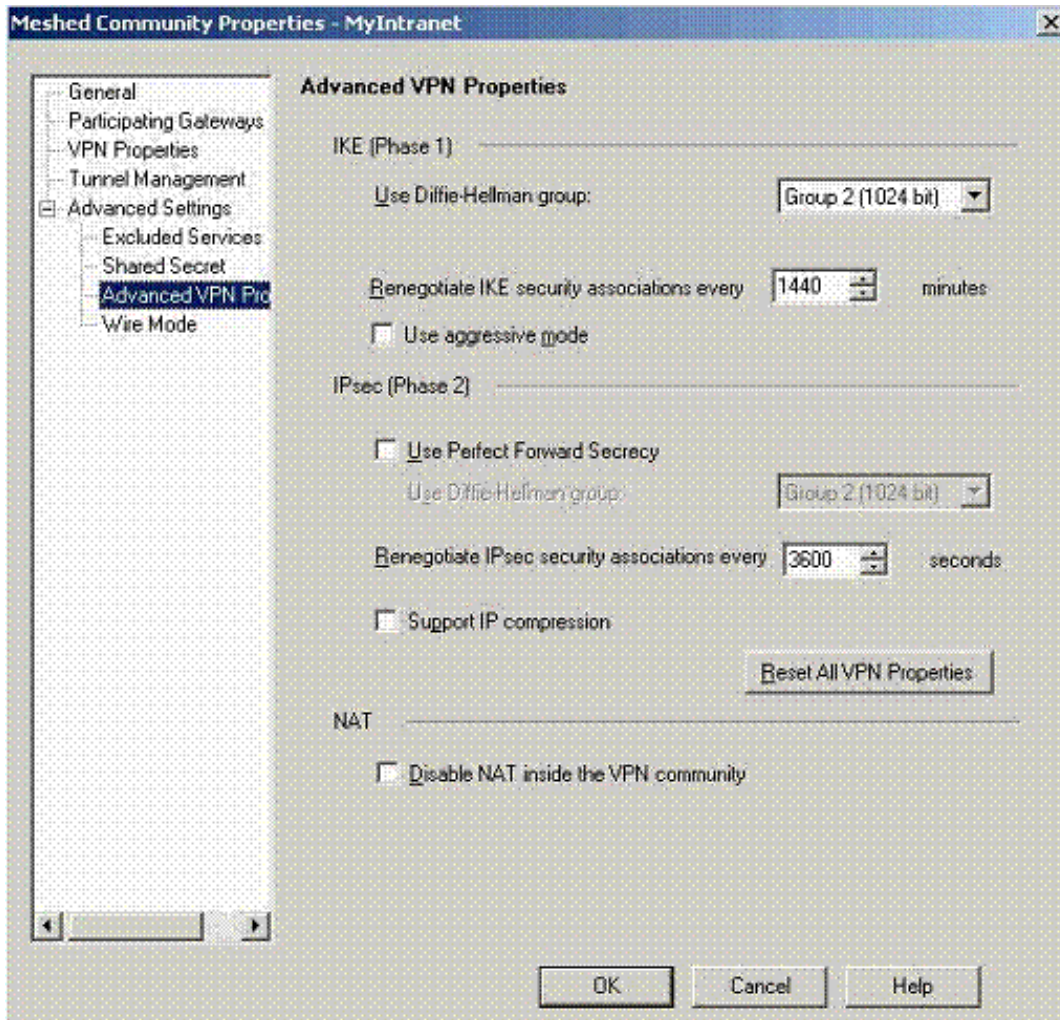
- A. 1, 2, 3
- B. 1, 2, 3, 4
- C. 1, 3, 4
- D. 1, 2, 5
- E. 1, 2, 4

Answer: E

Explanation:

QUESTION NO: 126

Stephanie wants to reduce the encryption overhead and improve performance for her mesh VPN Community. The Advanced VPN Properties screen below displays adjusted page settings: What can Stephanie do to achieve her goal?



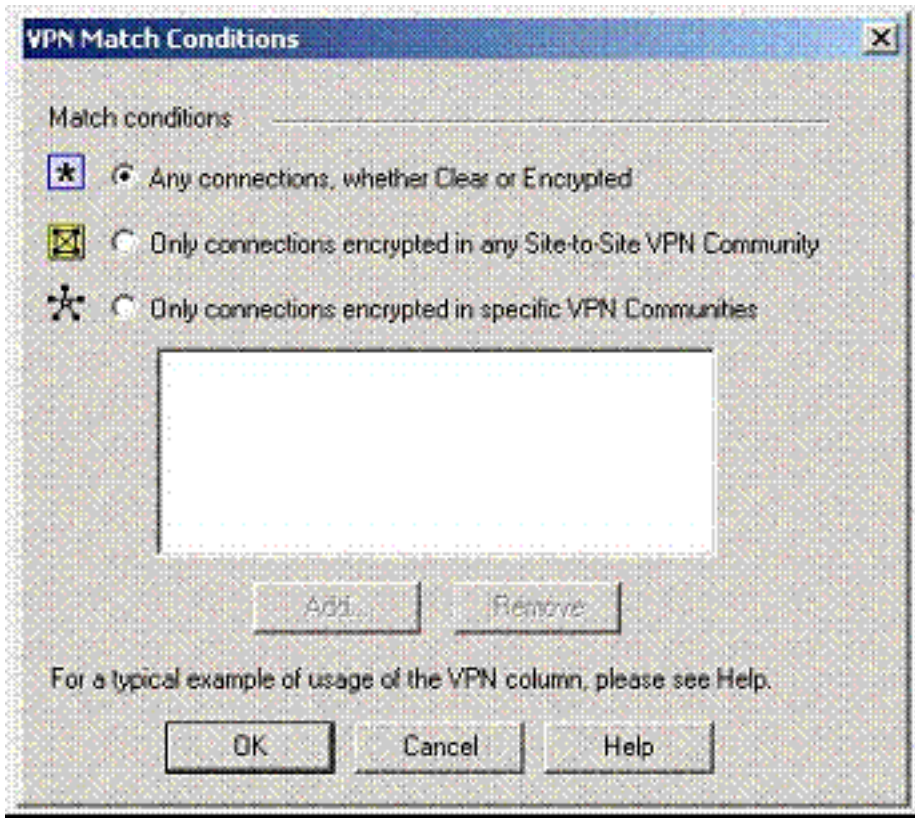
- A. Check the box "Use Perfect Forward Secrecy".
- B. Change the setting "Use Diffie. Hellman group" to "Group 5 (1536 bit)".
- C. Check the box "Use aggressive mode".
- D. Check the box "Support IP compression"
- E. Reduce the setting "Renegotiate IKE security associations every" to "720".

Answer: D

Explanation:

QUESTION NO: 127

Steve tries to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. Steve sees the following screen. What is the problem?



- A. Steve must enable `directional_match(true)` in the `objects_5_0.C` file on SmartCenter Server.
- B. Steve must enable Advanced Routing on each Security Gateway.
- C. Steve must enable VPN Directional Match on the VPN Advanced screen, in Global properties.
- D. Steve must enable a dynamic routing protocol, such as OSPF, on the Gateways.
- E. Steve must enable VPN Directional Match on the gateway object's VPN tab.

Answer: C

Explanation:

QUESTION NO: 128

Jerry is concerned that a denial-of-service (DoS) attack may affect his VPN Communities. He decides to implement IKE DoS protection. Jerry needs to minimize the performance impact of implementing this new protection. Which of the following configurations is MOST appropriate for Jerry?

- A. Set Support IKE DoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless".
- B. Set Support IKE DoS Protection from identified source, and Support IKE DoS protection from unidentified source to "Puzzles".
- C. Set Support IKE DoS protection from identified source to "Stateless," and Support IKE DoS protection from unidentified source to "Puzzles".
- D. Set "Support IKE DoS protection" from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".

E. Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None".

Answer: D

Explanation:

QUESTION NO: 129

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. Check Point gateway object properties
- D. \$CPDIR/conf/qos_props.pf
- E. Advanced Action options in each QoS rule

Answer: A

Explanation:

QUESTION NO: 130

You are configuring the VoIP Domain object for an H.323 environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?

- A. Transmission Router
- B. Gatekeeper
- C. Call Manager
- D. Proxy
- E. Call Agent

Answer: B

Explanation:

QUESTION NO: 131

Problems sometimes occur when distributing IPSec packets to a few machines in a Load Sharing Multicast mode cluster, even though the machines have the same source and destination IP addresses. What is the best Load Sharing method for preventing this type of problem?

- A. Load Sharing based on IP addresses, ports, and serial peripheral interfaces (SPI)

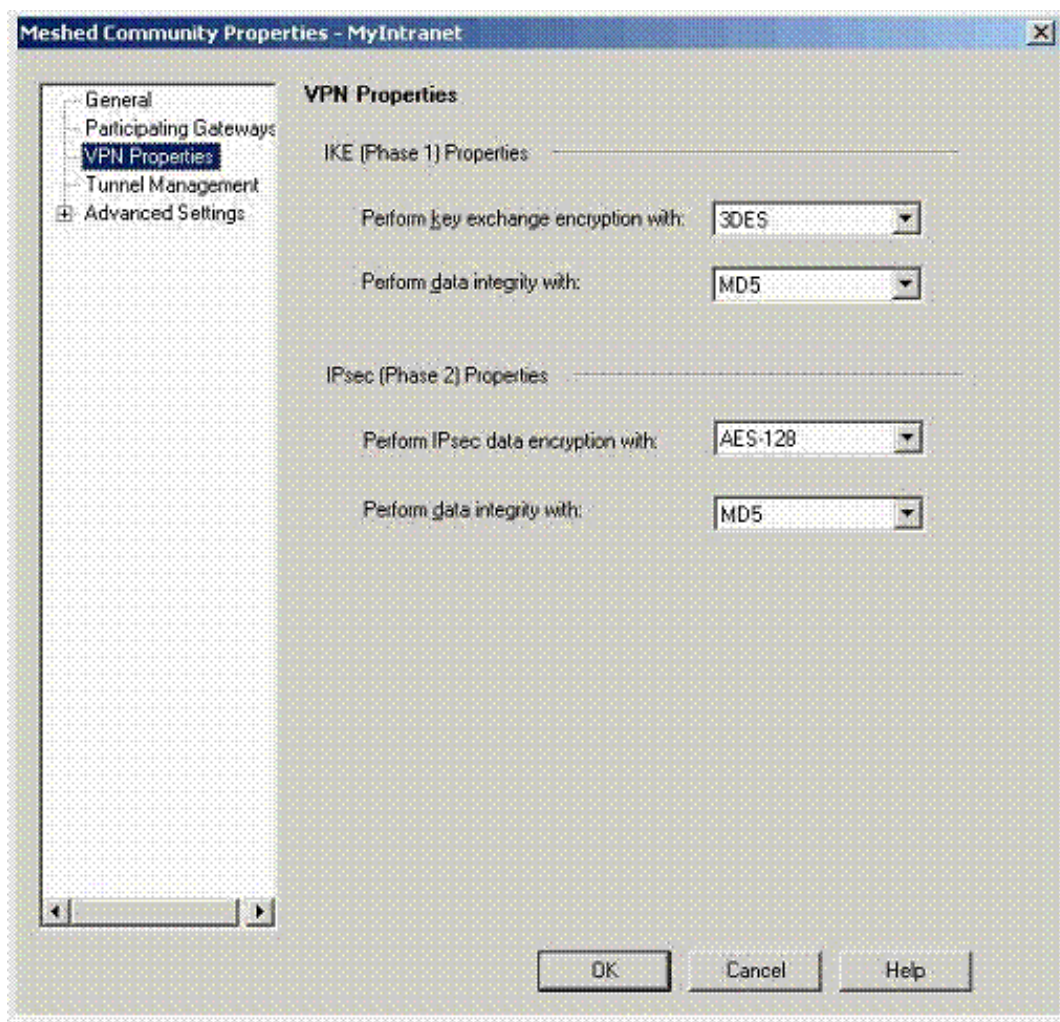
- B. Load Sharing based on SPIs only
- C. Load Sharing based on IP addresses only
- D. Load Sharing based on SPIs and ports only
- E. Load Sharing based on IP addresses and ports

Answer: E

Explanation:

QUESTION NO: 132

Jacob is using a mesh VPN Community to create a site-to-site VPN. The VPN properties in this mesh Community display in this graphic: Which of the following statements is TRUE?



- A. If Jacob changes the setting, "Perform key exchange encryption with" from "3DES" to "DES", he will enhance the VPN Community's security and reduce encryption overhead.
- B. Jacob must change the data integrity settings for this VPN Community. MD5 is incompatible with AES.
- C. If Jacob changes the setting "Perform IPsec data encryption with" from "AES-128" to "3DES",

he will increase the encryption overhead.

D. Jacob's VPN Community will perform IKE Phase 1 key-exchange encryption, using the longest key VPN-1 NGX supports.

Answer: C

Explanation:

QUESTION NO: 133

Rachel is 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. Which of the following options will allow Rachel to control which FTP commands pass through the Security Gateway protecting the FTP servers?

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

Answer: B

Explanation:

QUESTION NO: 134

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.** Manually import your partner's Access Control List.
- B.** Exchange a shared secret, before importing Certificates.
- C.** Create a new logical-server object, to represent your partner's CA.
- D.** Manually import your partner's Certificate Revocation List.
- E.** Exchange exported CAkeys and use them to create a new server object, to represent your partner's Certificate Authority (CA).

Answer: E

Explanation:

QUESTION NO: 135

You are reviewing SmartView Tracker entries, and see a Connection Rejection on a Check Point QoS rule. What causes the Connection Rejection?

- A. No QOS rule exists to match the rejected traffic.
- B. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections.
- C. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements.
- D. Burst traffic matching the Default Rule is exhausting the Check Point QoS global packet buffers.
- E. The guarantee of one of the rule's sub rules exceeds the guarantee in the rule itself.

Answer: B

Explanation:

QUESTION NO: 136

Wayne configures an HTTP Security Server to work with the content vectoring protocol to screen forbidden sites. He has created a URI resource object using CVP with the following settings:

Use CVP

Allow CVP server to modify content

Return data after content is approved

He adds two rules to his Rule Base: one to inspect HTTP traffic going to known forbidden sites, the other to allow all other HTTP traffic.

Wayne sees HTTP traffic going to those problematic sites is not prohibited.

What could cause this behavior?

- A. The Security Server Rule is after the general HTTP Accept Rule.
- B. The Security Server is not communicating with the CVP server.
- C. The Security Server is not configured correctly.
- D. The Security Server is communicating with the CVP server, but no restriction is defined in the CVP server.

Answer: A

Explanation:

QUESTION NO: 137

You have two Nokia Appliances: one IP530 and one IP380. Both Appliances have IPSO 3.9 and

VPN-1 Pro NGX installed in a distributed deployment. Can they be members of a gateway cluster?

- A. No, because the Gateway versions must not be the same on both security gateways
- B. Yes, as long as they have the same IPSO version and the same VPN-1 Pro version
- C. No, because members of a security gateway cluster must be installed as standalone deployments
- D. Yes, because both gateways are from Nokia, whether they have the same VPN-1 PRO version or not
- E. No, because the appliances must be of the same model (Both should be IP530 or IP380.)

Answer: B

Explanation:

QUESTION NO: 138

You want to block corporatE. internal-net and localnet from accessing Web sites containing inappropriate content. You are using WebTrends for URL filtering. You have disabled VPN-1 Control connections in the Global properties. Review the diagram and the Security Policies for GW_A and GW_B in the exhibit provided.

Security Policy installed on GW_A

NO	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	Management GW_A	Management GW_A	Management GW_A	Any Traffic	TCP CPD TCP CPD_amon TCP FWI TCP FWI_CPRID TCP FWI_ica_pull TCP FWI_ica_push TCP FWI_ica_services TCP FWI_key TCP FWI_log TCP FWI_lognt TCP FWI_sam	accept	None	Policy Targets
2	localnet Corporate-internal-net	Any	Any	Any Traffic	HTTP http-voas-sites	drop	Log	Policy Targets
3	localnet Corporate-internal-net	Any	Any	Any Traffic	TCP http	accept	None	Policy Targets
4	Corporate-internal-net	Corporate-internal-net localnet	Corporate-internal-net localnet	Any Traffic	Any	accept	None	Policy Targets
5	Any	Any	Any	Any Traffic	Any	drop	Log	Policy Targets

Security Policy installed on GW B

NO	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	Management GW_A	Management GW_A	Management GW_A	Any Traffic	TCP CPD TCP CPD_amon TCP FWI TCP FWI_CPRID TCP FWI_ica_pull TCP FWI_ica_push	accept	None	Policy Targets

Corporate users and localnet users receive message "Web cannot be displayed". In SmartView Tracker, you see the connections are dropped with message "content security is not reachable". What is the problem, and how do you fix it?

- A.** The connection from GW_B to the internal WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_A's Policy to allow source WebTrends Server, destination GW_B, service TCP port 18182, and action accept.
- B.** The connection from GW_B to the WebTrend server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with Source GW_B, destination WebTrends server, service TCP port 18182, and action accept.
- C.** The connection from GW_A to the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with source WebTrends server, destination GW_A, service TCP port 18182, and action accept.
- D.** The connection from GW_A to the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_B's Policy with source GW_A, destination: WebTrends server, service TCP port 18182, and action accept.
- E.** The connection from GW_A to the WebTrends server is not allowed in the Policy.
Fix: Add a rule in GW_A's Policy to allow source GW_A, destination WebTrends server, service TCP port 18182, and action accept.

Answer: E

Explanation:

QUESTION NO: 139

VPN-1 NGX includes a resource mechanism for working with the Common Internet File System (CIFS). However, this service only provides a limited level of actions for CIFS security. Which of the following services is NOT provided by a CIFS resource?

- A.** Log access shares
- B.** Block Remote Registry Access
- C.** Log mapped shares
- D.** Allow MS print shares

Answer: D

Explanation:

QUESTION NO: 140

Your organization has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 Secure Client 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 only
- D. To the center; or through the center to other satellites, then to the Internet and other VPN targets

Answer: D

Explanation:

QUESTION NO: 141

Robert has configured a Common Internet File System (CIFS) resource to allow access to the public partition of his company's file server, on \\erisco\goldenapple\files\public. Robert receives reports that users are unable to access the shared partition, unless they use the file server's IP address. Which of the following is a possible cause?

- A. Mapped shares do not allow administrative locks.
- B. The CIFS resource is not configured to use Windows name resolution
- C. Access violations are not logged.
- D. Remote registry access is blocked.
- E. Null CIFS sessions are blocked.

Answer: B

Explanation:

QUESTION NO: 142

You want to create an IKE VPN between two VPN-1 NGX Security Gateways, to protect two networks. The network behind one Gateway is 10.15.0.0/16, and network 192.168.9.0/24 is behind the peer's Gateway. Which type of address translation should you use, to ensure the two networks access each other through the VPN tunnel?

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

Answer: D

Explanation:

QUESTION NO: 143

Jennifer wants to protect internal users from malicious Java code, but she does not want to strip Java scripts. Which is the BEST configuration option?

- 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 ActiveX tags
- D. Use the URI resource to strip applet tags
- E. Use the URI resource to strip script tags

Answer: A

Explanation:

QUESTION NO: 144

Your VPN Community includes three Security Gateways. Each Gateway has its own internal network defined as a VPN Domain. You must test the VPN-1 NGX route-based VPN feature, without stopping the VPN. What is the correct order of steps?

- A. 1. Add a new interface on each Gateway.
2. Remove the newly added network from the current VPN Domain for each Gateway.
3. Create VTIs on each Gateway, to point to the other two peers
4. Enable advanced routing on all three Gateways.
- B. 1. Add a new interface on each Gateway.
2. Remove the newly added network from the current VPN Domain in each gateway object.
3. Create VPN Tunnel Interfaces (VTI) on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new network to each peer's VTI interface.
- C. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each Gateway.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Enable advanced routing on all three Gateways.
- D. 1. Add a new interface on each Gateway.
2. Add the newly added network into the existing VPN Domain for each gateway object.
3. Create VTIs on each gateway object, to point to the other two peers.
4. Add static routes on three Gateways, to route the new networks to each peer's VTI interface.

Answer: B

Explanation:

QUESTION NO: 145

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

- A. Telnet
- B. HTTP
- C. rlogin
- D. FTP
- E. SMTP

Answer: C

Explanation:

QUESTION NO: 146

You are running a VPN-1 NG with Application Intelligence R54 SecurePlatform VPN-1 Pro Gateway. The Gateway also serves as a Policy Server. When you run patch add cd from the NGX CD, what does this command allow you to upgrade?

- A. Only VPN-1 Pro Security Gateway
- B. Both the operating system (OS) and all Check Point products
- C. All products, except the Policy Server
- D. Only the patch utility is upgraded using this command
- E. Only the OS

Answer: B

Explanation:

QUESTION NO: 147

Which type of service should a Security Administrator use in a Rule Base to control access to specific shared partitions on target machines?

- A. Telnet
- B. CIFS
- C. HTTP
- D. FTP
- E. URI

Answer: B

Explanation:

QUESTION NO: 148

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

- A. Phase 3 Key Revocation
- B. Perfect Forward Secrecy
- C. MD5 Hash Completion
- D. SHA1 Hash Completion
- E. DES Key Reset

Answer: B

Explanation:

QUESTION NO: 149

How would you configure a rule in a Security Policy to allow SIP traffic from end point Net_A to end point Net_B, through an NGX Security Gateway?

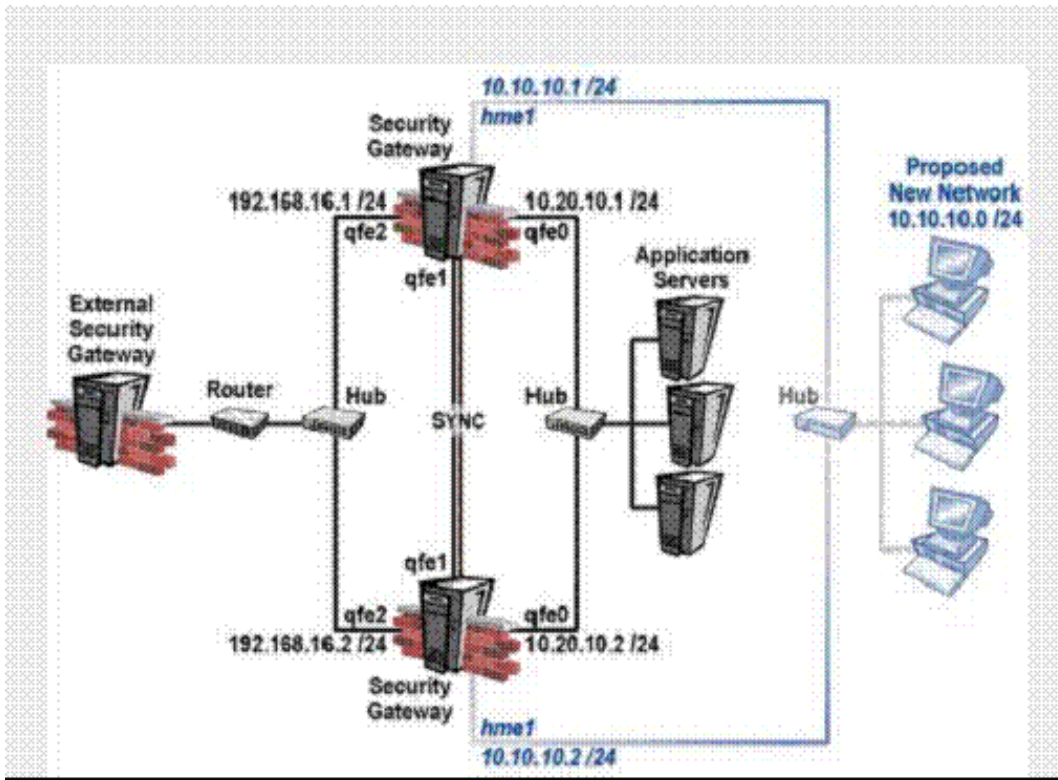
- A. Net_A/Net_B/sip/accept
- B. Net_A/Net_B/sip and sip_any/accept
- C. Net_A/Net_B/VoIP_any/accept
- D. Net_A/Net_B/M3IP/accept

Answer: A

Explanation:

QUESTION NO: 150

After you add new interfaces to this cluster, how can you check if the new interfaces and associated virtual IP address are recognized by ClusterXL?



- A. By running the cphaprob state command on both members
- B. By running the cphaprob. a if command on both members
- C. By running the cphaprob. l list command on both members
- D. By running the fw ctl iflist command on both members
- E. By running the cpconfig command on both members

Answer: B

Explanation:

QUESTION NO: 151

Barak is a Security Administrator for an organization that has two sites using prE. shared secrets in its VPN. The two sites are Oslo and London. Barak has just been informed that a new office is opening in Madrid, and he must enable all three sites to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server, behind the Oslo Security Gateway. Barak decides to switch from prE. shared secrets to Certificates issued by the Internal Certificate Authority (ICA). After creating the Madrid gateway object with the proper VPN Domain, what are Barak's remaining steps?

1. Disable "PrE. Shared Secret" on the London and Oslo gateway objects
2. Add the Madrid gateway object into the Oslo and London's mesh VPN Community
3. Manually generate ICA Certificates for all three Security Gateways.

4. Configure "Traditional mode VPN configuration" in the Madrid gateway object's VPN screen
5. Reinstall the Security Policy on all three Security Gateways.

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

Answer: A

Explanation:

QUESTION NO: 152

You have an internal FTP server, and you allow downloading, but not uploading. Assume Network Address Translation is set up correctly, and you want to add an inbound rule with:

Source: Any

Destination: FTP server

Service: FTP resources object.

How do you configure the FTP resource object and the action column in the rule to achieve this goal?

- A. Enable only the "Get" method in the FTP Resource Properties, and use this method in the rule, with action accept.
- B. Enable only the "Get" method in the FTP Resource Properties and use it in the rule, with action drop.
- C. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.
- D. Disable "Get" and "Put" methods in the FTP Resource Properties and use it in the rule, with action accept.
- E. Enable only the "Put" method in the FTP Resource Properties and use it in the rule, with action accept.

Answer: A

Explanation:

QUESTION NO: 153

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. Yes, these machines are configured correctly for a ClusterXL deployment.
- B. No, QuadCards are not supported with ClusterXL.
- C. No, all machines in a cluster must be running on the same OS.
- D. No, a cluster must have an even number of machines.
- E. No, ClusterXL is not supported on Red Hat Linux.

Answer: C

Explanation:

QUESTION NO: 154

Damon enables an SMTP resource for content protection. He notices that mail seems to slow down on occasion, sometimes being delivered late. Which of the following might improve throughput performance?

- A. Configuring the SMTP resource to bypass the CVP resource
- B. Increasing the Maximum number of mail messages in the Gateway's spool directory
- C. Configuring the Content Vector Protocol (CVP) resource to forward the mail to the internal SMTP server, without waiting for a response from the Security Gateway
- D. Configuring the CVP resource to return the mail to the Gateway
- E. Configuring the SMTP resource to only allow mail with Damon's company's domain name in the header

Answer: C

Explanation:

QUESTION NO: 155

What is the consequence of clearing the "Log VoIP Connection" box in Global Properties?

- A. Dropped VoIP traffic is logged, but accepted VoIP traffic is not logged.
- B. VoIP protocol-specific log fields are not included in SmartView Tracker entries.
- C. The log field setting in rules for VoIP protocols are ignored.
- D. IP addresses are used, instead of object names, in log entries that reference VoIP Domain objects.
- E. The SmartCenter Server stops importing logs from VoIP servers.

Answer: B

Explanation:

QUESTION NO: 156

VPN-1 NGX includes a resource mechanism for working with the Common Internet File System (CIFS). However, this service only provides a limited level of actions for CIFS security. Which of the following services is provided by a CIFS resource?

- A. Allow Unix file sharing.
- B. Allow MS print shares
- C. Logging Mapped Shares
- D. Access Violation logging.

Answer: C

Explanation:

QUESTION NO: 157

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

- A. Two stars and one mesh Community; each star Community is set up for each site, with headquarters as the center of the Community, and branches as satellites. The mesh Communities are between the New York and London headquarters
- B. Three mesh Communities: one for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.
- C. Two mesh Communities, one for each headquarters and their branch offices; and one star

Community, in which London is the center of the Community and New York, is the satellite.

D. Two mesh Communities, one for each headquarters and their branch offices; and one star Community, where New York is the center of the Community and London is the satellite.

Answer: A

Explanation:

QUESTION NO: 158

You are preparing to configure your VoIP Domain Gatekeeper object. Which two other objects should you have created first?

- A.** An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed
- B.** An object to represent the PSTN phone network, AND an object to represent the IP phone network
- C.** An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed
- D.** An object to represent the Q.931 service origination host, AND an object to represent the H.245 termination host
- E.** An object to represent the call manager, AND an object to represent the host on which the transmission router is installed

Answer: C

Explanation:

QUESTION NO: 159

Yoav is a Security Administrator preparing to implement a VPN solution for his multi-site organization. To comply with industry regulations, Yoav's VPN solution must meet the following requirements:

Portability: Standard

Key management: Automatic, external PKI

Session keys: Changed at configured times during a connection's lifetime

Key length: No less than 128-bit

Data integrity: Secure against inversion and brute force attacks

What is the most appropriate setting Yoav should choose?

- A. IKE VPNs: AES encryption for IKE Phase 1, and DES encryption for Phase 2; SHA1 hash
- B. IKE VPNs: SHA1 encryption for IKE Phase 1, and MD5 encryption for Phase 2; AES hash
- C. IKE VPNs: CAST encryption for IKE Phase 1, and SHA1 encryption for Phase 2; DES hash
- D. IKE VPNs: AES encryption for IKE Phase 1, and AES encryption for Phase 2; SHA1 hash
- E. IKE VPNs: DES encryption for IKE Phase 1, and 3DES encryption for Phase 2; MD5 hash

Answer: D

Explanation:

QUESTION NO: 160

Which of the following commands shows full synchronization status?

- A. cphaproB. i list
- B. cphastop
- C. fw ctl pstat
- D. cphaproB. a if
- E. fw hastat

Answer: A

Explanation:

QUESTION NO: 161

In a distributed VPN-1 Pro NGX environment, where is the Internal Certificate Authority (ICA) installed?

- A. On the Security Gateway
- B. Certificate Manager Server
- C. On the Policy Server
- D. On the Smart View Monitor
- E. On the primary SmartCenter Server

Answer: E

Explanation:

QUESTION NO: 162

You must set up SIP with a proxy for your network. IP phones are in the 172.16.100.0 network. The Registrar and proxy are installed on host 172.16.100.100. To allow handover enforcement for outbound calls from SIP-net to network Net_B on the Internet, you have defined the following objects:

Network object: SIP-net: 172.16.100.0/24

SIP-gateway: 172.16.100.100

VoIP Domain object: VoIP_domain_A

1. EnD. point domain: SIP-net

2. VoIP gateway installed at: SIP-gateway host object

How would you configure the rule?

- A. SIP-Gateway/Net_B/sip_any/accept
- B. VoIP_domain_A/Net_B/sip/accept
- C. SIP-Gateway/Net_B/sip/accept
- D. VoIP_domain_A/Net_B/sip_any, and sip/accept
- E. VoIP_Gateway_M/Net_B/sip_any/accept

Answer: B

Explanation:

QUESTION NO: 163

What is the behavior of ClusterXL in a High Availability environment?

- A. Both members respond to the virtual IP address, and both members pass traffic when using their physical addresses.
- B. Both members respond to the virtual IP address, but only the active member is able to pass traffic.
- C. The active member responds to the virtual IP address and both members pass traffic when using their physical addresses.
- D. The active member responds to the virtual IP address and is the only member that passes traffic
- E. The passive member responds to the virtual IP address, and both members route traffic when using their physical addresses.

Answer: D

Explanation:

QUESTION NO: 164

Which Check Point QoS feature marks the Type of Service (ToS) byte in the IP header?

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

Answer: C

Explanation:

QUESTION NO: 165

You plan to incorporate OPSEC servers, such as Websense and Trend Micro, to do content filtering. Which segment is the BEST location for these OPSEC servers, when you consider Security Server performance and data security?

- A. On the Security Gateway
- B. Internal network, where users are located
- C. On the Internet
- D. DMZ network, where application servers are located
- E. Dedicated segment of the network

Answer: E

Explanation:

QUESTION NO: 166

The following rule contains an FTP resource object in the Service field:

Source: local_net

Destination: Any

Service: FTP-resource object

Action: Accept

How do you define the FTP Resource Properties > Match tab to prevent internal users from receiving corporate files from external FTP servers, while allowing users to send files?

- A. Enable "Put" and "Get" methods.
- B. Disable the "Put" method globally.
- C. Enable the "Put" method only on the Match tab.
- D. Enable the "Get" method on the Match tab.

E. Disable "Get" and "Put" methods on the Match tab.

Answer: C

Explanation:

QUESTION NO: 167

VPN-1 NGX supports VoIP traffic in all of the following environments, EXCEPT which environment?

- A. H.323
- B. SIP
- C. MEGACO
- D. SCCP
- E. MGCP

Answer: C

Explanation:

QUESTION NO: 168

Cody is notified by blacklist.org that his site has been reported as a spam relay, due to his SMTP Server being unprotected. Cody decides to implement an SMTP Security Server, to prevent the server from being a spam relay. Which of the following is the most efficient configuration method?

- A. Configure the SMTP Security Server to perform MX resolving.
- B. Configure the SMTP Security Server to perform filtering, based on IP address and SMTP protocols.
- C. Configure the SMTP Security Server to work with an OPSEC based product, for content checking.
- D. Configure the SMTP Security Server to apply a generic "from" address to all outgoing mail.
- E. Configure the SMTP Security Server to allow only mail to or from names, within Cody's corporate domain.

Answer: E

Explanation:

QUESTION NO: 169

You want to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 Gateway to SecurePlatform NGX R60 via SmartUpdate. Which package is needed in the repository before upgrading?

- A. SVN Foundation and VPN-1 Express/Pro
- B. VPN-1 and Firewall-1
- C. SecurePlatform NGX R60
- D. SVN Foundation 3 E. VPN-1 Pro/Express NGXR60

Answer: C

Explanation:

QUESTION NO: 170

Your current stand. alone VPN-1 NG with Application Intelligence (AI) R55 installation is running on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the VPN-1 Pro Gateway. An additional machine will serve as the SmartCenter Server. The new machine runs on a Windows Server 2003. You need to upgrade the NG with AI R55 SmartCenter Server configuration to VPN-1 NGX.

How do you upgrade to VPN-1 NGX?

- A.** Insert the NGX CD in the existing NGwithAI R55 SecurePlatform machine, and answer yes to backup the configuration. Copy the backup file to the Windows Server 2003. Continue the upgrade process. Reboot after upgrade is finished. After SecurePlatform NGX reboots, run sysconfig, select VPN-1 Pro Gateway, and finish the sysconfig process. Reboot again. Use the NGX CD to install the primary SmartCenter on the Windows Server 2003. Import the backup file.
- B.** Run the backup command in the existing SecurePlatform machine, to create a backup file. Copy the file to the Windows Server 2003. Uninstall all Check Point products on SecurePlatform by running rpm CPsuitE. R55 command. Reboot. Install new VPN-1 NGX on the existing SecurePlatform machine. Run sysconfig, select VPN-1 Pro Gateway, and reboot. Use VPN-1 NGX CD to install primary SmartCenter Server on the Windows Server 2003. Import the backup file.
- C.** Copy the \$FWDIR\conf and \$FWDIR\lib files from the existing SecurePlatform machine. Create a tar.gzfile, and copy it to the Windows Server 2003. Use VPN-1 NGX CD on the existing SecurePlatform machine to do a new installation. Reboot. Run sysconfig and select VPN-1 Pro Gateway. Reboot. Use the NGX CD to install the primary SmartCenter Server on the Windows Server 2003. On the Windows Server 2003, run upgradeimport command to import \$FWDIR\conf and \$FWDIR\lib from the SecurePlatform machine.
- D.** Run backup command on the existing SecurePlatform machine to create a backup file. Copy the file to the Windows Server 2003. Uninstall the primary SmartCenter Server package from NG with AI R55 SecurePlatform using sysconfig. Reboot. Install the NGX primary SmartCenter Server and import the backup file. Open the NGX SmartUpdate, and select "upgrade all packages" on the NG with AI R55 Security Gateway.

Answer: A

Explanation:

QUESTION NO: 171

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

- A. The standard three packet IKE Phase 1 exchange is replaced by a six-packet exchange.
- B. The standard six-packet IKE Phase 2 exchange is replaced by a three packet exchange.
- C. The standard three packet IKE Phase 2 exchange is replaced by a six-packet exchange.
- D. The standard six-packet IKE Phase 1 exchange is replaced by a three packet exchange.
- E. The standard six-packet IKE Phase 1 exchange is replaced by a twelve packet exchange.

Answer: D

Explanation:

QUESTION NO: 172

DSShield is a Check Point feature used to block which of the following threats?

- A. Cross Site Scripting
- B. SQL injection
- C. DDOS
- D. Buffer overflows
- E. Trojan horses

Answer: C

Explanation:

QUESTION NO: 173

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

- A. In the Security Server window in Global Properties
- B. In SmartDefense SMTP settings
- C. In the smtp.conf file on the SmartCenter Server
- D. In the gateway object's SMTP settings in the Advanced window
- E. In the SMTP resource object

Answer: D

Explanation:

QUESTION NO: 174

Greg is creating rules and objects to control VoIP traffic in his organization, through a VPN-1 NGX Security Gateway. Greg creates VoIP Domain SIP objects to represent each of his organization's

three SIP gateways. Greg then creates a simple group to contain the VoIP Domain SIP objects. When Greg attempts to add the VoIP Domain SIP objects to the group, they are not listed. What is the problem?

- A. The related enD. points domain specifies an address range.
- B. VoIP Domain SIP objects cannot be placed in simple groups.
- C. The installed VoIP gateways specify host objects.
- D. The VoIP gateway object must be added to the group, before the VoIP Domain SIP object is eligible to be added to the group.
- E. The VoIP Domain SIP object's name contains restricted characters.

Answer: B

Explanation:

QUESTION NO: 175

You plan to install a VPN-1 Pro Gateway for VPN-1 NGX at your company's headquarters. You have a single Sun SPARC Solaris 9 machine for VPN-1 Pro enterprise implementation. You need this machine to inspect traffic and keep configuration files. Which Check Point software package do you install?

- A. VPN-1 Pro Gateway and primary SmartCenter Server
- B. Policy Server and primary SmartCenter Server
- C. ClusterXL and SmartCenter Server
- D. VPN-1 Pro Gateway
- E. SmartCenter Server

Answer: A

Explanation:

QUESTION NO: 176

```
Cluster Mode:New High Availability (Active Up)
Number      Unique IP Address  Assigned Load  State
1 <local>   192.168.1.1        0%             down
2           192.168.1.2        100%           active
```

The following is cphaprob state command output from a New Mode High Availability cluster member. Which machine has the highest priority?

- A. 192.168.1.2, since its number is 2

- B. 192.168.1.1, because its number is 1
- C. This output does not indicate which machine has the highest priority.
- D. 192.168.1.2, because its state is active

Answer: B

Explanation:

QUESTION NO: 177

Which service type does NOT invoke a Security Server?

- A. HTTP
- B. FTP
- C. Telnet
- D. CIFS
- E. SMTP

Answer: D

Explanation:

QUESTION NO: 178

Your current VPN-1 NG with Application Intelligence (AI) R55 stand alone VPN-1 Pro Gateway and SmartCenter Server run on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the SmartCenter Server, and a new machine will be the VPN-1 Pro Gateway only. You need to migrate the NG with AI R55 SmartCenter Server configuration, including such items as Internal Certificate Authority files, databases, and Security Policies.

How do you request a new license for this VPN-1 NGX upgrade?

- A. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new local license for the NGX VPN-1 Pro Gateway.
- B. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new central license for the NGX VPN-1 Pro Gateway.
- C. Request a new VPN-1 NGX SmartCenter Server license, using the NG with AI SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway.
- D. Request a VPN-1 NGX SmartCenter Server license, using the NG with AI SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway, licensed for the existing SmartCenter Server IP address.

Answer: D

Explanation:

QUESTION NO: 179

What is a requirement for setting up Management High Availability?

- A. All SmartCenter Servers must reside in the same Local Area Network (LAN).
- B. All SmartCenter Servers must have the same amount of memory.
- C. You can only have one Secondary SmartCenter Server.
- D. All SmartCenter Servers must have the BIOS release.
- E. All SmartCenter Servers must have the same operating system.

Answer: E

Explanation:

QUESTION NO: 180

Which of the following TCP port numbers is used to connect the VPN-1 Gateway to the Content Vector Protocol (CVP) server?

- A. 18182
- B. 18180
- C. 18181
- D. 7242
- E. 1456

Answer: C

Explanation:

QUESTION NO: 181

Which operating system is NOT supported by VPN-1 Secure Client?

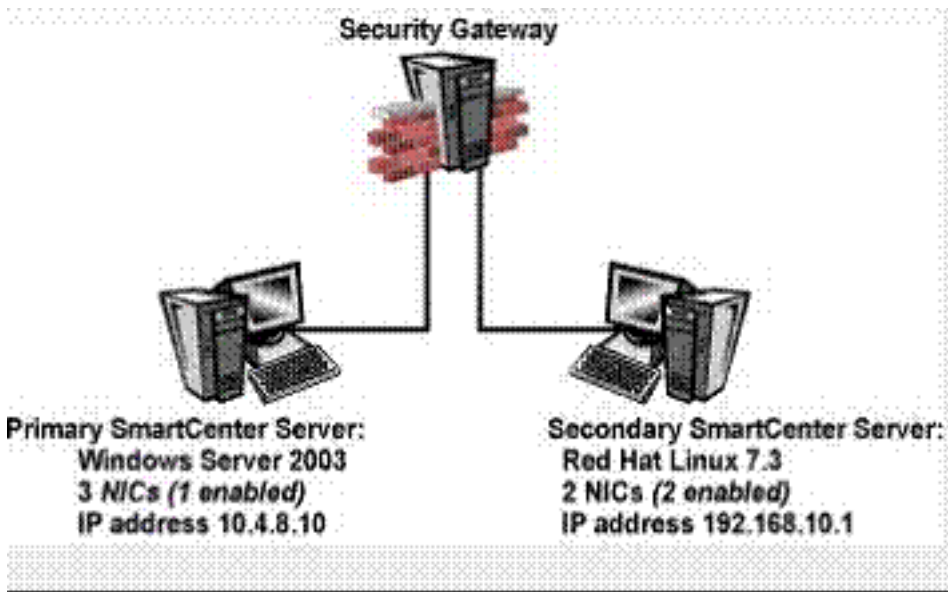
- A. IPSO 3.9
- B. Windows XP SP2
- C. Windows 2000 Professional
- D. RedHat Linux 8.0
- E. MacOSX

Answer: A

Explanation:

QUESTION NO: 182

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



- A. No, the SmartCenter Servers must be installed on the same operating system.
- B. No, a VPN-1 NGX SmartCenter Server cannot run on Red Hat Linux 7.3.
- C. No, the SmartCenter Servers must reside on the same network.
- D. No, A VPN-1 NGX SmartCenter Server can only be in a Management HA configuration, if the operating system is Solaris.
- E. No, the SmartCenter Servers do not have the same number of NICs.

Answer: A

Explanation:

QUESTION NO: 183

You are preparing a lab for a ClusterXL environment, with the following topology:

Vip internal cluster IP = 172.16.10.1; Vip external cluster IP = 192.168.10.3

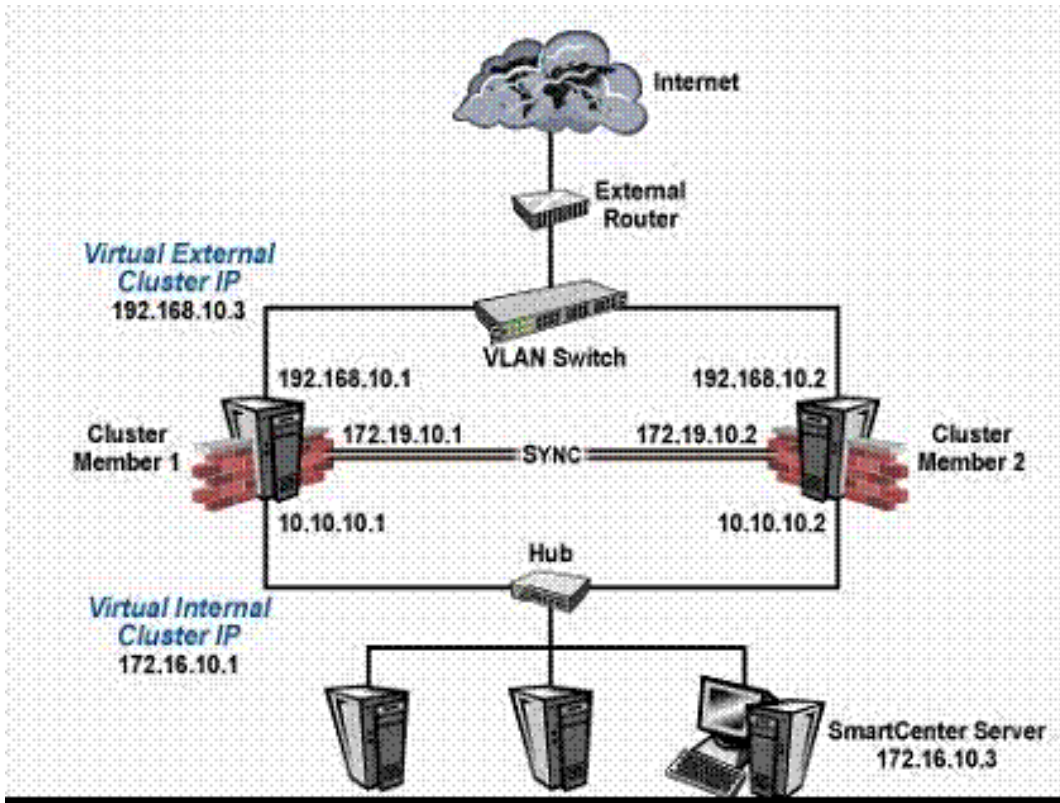
Cluster Member 1: four NICs, three enabled: qfe0: 192.168.10.1/24, qfel: 10.10.10.1/24, qfe2: 172.16.10.1/24

Cluster Member 2: five NICs, three enabled; hme0: 192.168.10.2/24, ethi: 10.10.10.2/24, eth2: 172.16.10.2/24

Member Network tab on internal-cluster interface: is 10.10.10.0, 255.255.255.0

SmartCenter Pro Server: 172.16.10.3

External interfaces 192.168.10.1 and 192.168.10.2 connect to a Virtual Local Area Network (VLAN) switch. The upstream router connects to the same VLAN switch. Internal interfaces 10.10.10.1 and 10.10.10.2 connect to a hub. There is no other machine in the 10.10.10.0 network. 172.19.10.0 is the synchronization network. What is the problem with this configuration?



- A. The SmartCenter Pro Server cannot be in the synchronization network.
- B. There is no problem with this configuration. It is correct.
- C. Members do not have the same number of NICs.
- D. The internal network does not have a third cluster member.
- E. Cluster members cannot use the VLAN switch. They must use hubs.

Answer: B

Explanation:

QUESTION NO: 184

Which VPN Community object is used to configure VPN routing within the SmartDashboard?

- A. Star
- B. Mesh
- C. Remote Access
- D. Map

Answer: A

Explanation:

QUESTION NO: 185

You want to upgrade a cluster with two members to VPN-1 NGX. 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. 3, 2, 1, 4
- B. 2, 4, 3, 1
- C. 1, 3, 2, 4
- D. 2, 3, 1, 4
- E. 1, 2, 3, 4

Answer: D

Explanation:

QUESTION NO: 186

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

- A. The Security Policy is installed.
- B. The Security Policy is saved.
- C. The user database is installed.
- D. The Security Administrator logs in to the standby SmartCenter Server, for the first time.
- E. The standby SmartCenter Server starts for the first time.

Answer: A

Explanation:

QUESTION NO: 187

VPN-1 NGX supports VoIP traffic in all of the following environments, except which environment?

- A. H509-D
- B. SIP
- C. MGCP
- D. H.323
- E. SCCP

Answer: A

Explanation:

QUESTION NO: 188

You receive an alert indicating a suspicious FTP connection is trying to connect to one of your internal hosts. How do you block the connection in real time and verify the connection is successfully blocked?

- A. Highlight the suspicious connection in SmartView Tracker > Active mode. Block the connection using the Tools > Block Intruder menu. Use the Active mode to confirm that the suspicious connection does not reappear.
- B. Highlight the suspicious connection in SmartView Tracker > Log mode. Block the connection using Tools > Block Intruder menu. Use Log mode to confirm that the suspicious connection does not reappear.
- C. Highlight the suspicious connection in SmartView Tracker > Active mode. Block the connection using Tools > Block Intruder menu. Use Active mode to confirm that the suspicious connection is dropped.
- D. Highlight the suspicious connection in SmartView Tracker > Log mode. Block the connection using Tools > Block Intruder menu. Use the Log mode to confirm that the suspicious connection is dropped.

Answer: A

Explanation:

QUESTION NO: 189

Which of the following QoS ruleE. action properties is an Advanced action type, only available in Traditional mode?

- A. Guarantee Allocation
- B. Rule weight
- C. Apply rule only to encrypted traffic
- D. Rule limit
- E. Rule guarantee

Answer: A

Explanation:

QUESTION NO: 190

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

- A. LEA
- B. URI
- C. UFP
- D. AMON
- E. CVP

Answer: C

Explanation:

QUESTION NO: 191

Regarding QoS guarantees and limits, which of the following statements is FALSE?

- A. The guarantee of a suB. rule cannot be greater than the guarantee defined for the rule above it.
- B. If a guarantee is defined in a suB. rule, a guarantee must be defined for the rule above it.
- C. A rule guarantee must not be less than the sum defined in the guarantees' suB. rules.
- D. If both a rule and per-connection limit are defined for a rule, the per-connection limit must not be greater than the rule limit.
- E. If both a limit and guarantee per rule are defined in a QoS rule, the limit must be smaller than the guarantee.

Answer: E

Explanation:

QUESTION NO: 192

Your network includes ClusterXL running Multicast mode on two members, as shown in this topology:Your network is expanding, and you need to add new interfaces: 10.10.10.1/24 on Member A, and 10.10.10.2/24 on Member B. The virtual IP address for interface 10.10.10.0/24 is 10.10.10.3. What is the correct procedure to add these interfaces?

- A. 1. Use the ifconfig command to configure and enable the new interface.
2. Run cpstop and cpstart on both members at the same time.

3. Update the topology in the cluster object for the cluster and both members.

4. Install the Security Policy.

B. 1. Disable "Cluster membership" from one Gateway via cpconfig.

2. Configure the new interface via sysconfig from the "non-member" Gateway.

3. RE. enable "Cluster membership" on the Gateway.

4. Perform the same step on the other Gateway.

5. Update the topology in the cluster object for the cluster and members.

6. Install the Security Policy.

C. 1. Run cpstop on one member, and configure the new interface via sysconfig.

2. Run cpstart on the member. Repeat the same steps on another member.

3. Update the new topology in the cluster object for the cluster and members.

4. Install the Security Policy.

D. 1. Use sysconfig to configure the new interfaces on both members.

2. Update the topology in the cluster object for the cluster and both members.

3. Install the Security Policy.

Answer: C

Explanation:

QUESTION NO: 193

You are configuring the VoIP Domain object for a SIP environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?

A. Call Manager

B. Gateway

C. Call Agent

D. Gatekeeper

E. Proxy

Answer: E

Explanation:

QUESTION NO: 194

When you add a resource service to a rule, which ONE of the following actions occur?

A. VPN-1 Secure Client users attempting to connect to the object defined in the Destination column of the rule will receive a new Desktop Policy from the resource.

B. All packets that match the resource in the rule will be dropped.

C. All packets matching the resource service rule are analyzed or authenticated, based on the resource properties.

D. Users attempting to connect to the destination of the rule will be required to authenticate.

E. All packets matching that rule are either encrypted or decrypted by the defined resource.

Answer: C

Explanation:

QUESTION NO: 195

To change an existing ClusterXL cluster object from Multicast to Unicast mode, what configuration change must be made?

- A. Change the cluster mode to Unicast on the cluster object Reinstall the Security Policy.
- B. Reset Secure Internal Communications (SIC) on the cluster-member objects. Reinstall the Security Policy.
- C. Run cpstop and cpstart, to rE. enable High Availability on both objects. Select Pivot mode in cpconfig.
- D. Change the cluster mode to Unicast on the cluster-member object.
- E. Switch the internal network's default Security Gateway to the pivot machine's IP address.

Answer: A

Explanation:

QUESTION NO: 196

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

```
MEMBER A:
HOST      NAME      ID      #UALS    #PEAK    #SLINKS
localhost connections 8158    1553     1560     800

[expert@memberB]# fw tab -t connections -s

MEMBER B:
HOST      NAME      ID      #UALS    #PEAK    #SLINKS
localhost connections 8158    800      1001     800
```

- A. Members A and B are synchronized, because ID for both members is identical in the connections table.
- B. The connections-table output is incomplete. You must run the cphaprob state command, to determine if members A and B are synchronized.
- 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 #SLINKS are identical in the connections table.
- E. Members A and B are not synchronized, because #VALS in the connections table are not close.

Answer: E

Explanation:

QUESTION NO: 197

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

Number	Unique IP Address	Assigned Load	State
1 (local)	192.168.1.1	30%	active
2	192.168.1.2	70%	active

- A. Load Balancing Mode
- B. Multicast mode
- C. Unicastmode
- D. New mode
- E. Legacy mode

Answer: C

Explanation:

QUESTION NO: 198

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps, and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic passing through the QoS Module matches both rules, which of the following statements is true?

- A. Neither rule will be allocated more than 10% of available bandwidth.
- B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
- C. 50% of available bandwidth will be allocated to the H.323 rule.
- D. 0% of available bandwidth will be allocated to the Default Rule.
- E. Each H.323 connection will receive at least 512 Kbps of bandwidth.

Answer: B

Explanation:

QUESTION NO: 199

You plan to migrate a VPN-1 NG with Application Intelligence (AI) R55 SmartCenter Server to VPN-1 NGX. 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. Upgrade the SmartCenter Server and the five remote Gateways via SmartUpdate, at the same time.
- B. 1. Copy the \$FWDIR\conf directory from the SmartCenter Server.
2. Save directory contents to another directory.
3. Uninstall the SmartCenter Server, and install a new SmartCenter Server.
4. Move directory contents to \$FWDIR\conf.
5. Reinstall all gateways using NGX and install a policy.
- C. 1. From the VPN-1 NGX CD in the SmartCenter Server, select "advance upgrade".
2. After importing the SmartCenter configuration into the new NGX SmartCenter, reboot.
3. Upgrade all licenses and software on all five remote Gateways via SmartUpdate.
- D. 1. Upgrade the five remote Gateways via SmartUpdate.
2. Upgrade the SmartCenter Server, using the VPN-1 NGX CD.
- E. 1. Upgrade the SmartCenter Server, using the VPN-1 NGX CD. 2. Reinstall and update the licenses of the five remote Gateways.

Answer: C

Explanation:

QUESTION NO: 200

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

- A. FTP
- B. SMTP
- C. Telnet
- D. HTTP
- E. rlogin

Answer: B

Explanation:

QUESTION NO: 201

You are configuring the VoIP Domain object for an H.323 environment, protected by VPN-1 NGX. Which VoIP Domain object type can you use?

- A. Transmission Router
- B. Gatekeeper
- C. Call Manager
- D. Proxy
- E. Call Agent

Answer: B

Explanation:

QUESTION NO: 202

Your network traffic requires preferential treatment by other routers on the network, in addition to the QoS Module, which Check Point QoS feature should you use?

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

Answer: C

Explanation:

QUESTION NO: 203

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

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

Answer: B

Explanation:

QUESTION NO: 204

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

- A. SmartConsole

- B. Check Point Gateway
- C. SmartCenter Server
- D. SmartUpdate upgrading/patching

Answer: A

Explanation:

QUESTION NO: 205

Which of the following is a TRUE statement concerning contract verification?

- A. Your contract file is stored on the User Center and fetched by the Gateway as needed.
- B. Your contract file is stored on the SmartConsole and downloaded to the SmartCenter Server.
- C. Your contract file is stored on the SmartConsole and downloaded to the Gateway.
- D. Your contract file is stored on the SmartCenter Server and downloaded to the Security Gateway.

Answer: D

Explanation:

QUESTION NO: 206

Your current VPN-1 NG with Application Intelligence (AI) R55 stand-alone VPN-1 Pro Gateway and SmartCenter Server runs on SecurePlatform. You plan to implement VPN-1 NGX R65 in a distributed environment, where the new machine will be the SmartCenter Server, and the existing machine will be the VPN-1 Pro Gateway only. You need to migrate the NG with AI R55 SmartCenter Server configuration, including licensing.

How do you handle licensing for this NGX R65 upgrade?

- A. Request an NGX R65 SmartCenter Server license, using the new server's IP address. Request a new central NGX R65 VPN-1 Gateway license also licensed to the new SmartCenter Server's IP address.
- B. Leave the current license on the gateway to be upgraded during the software upgrade. Purchase a new license for the VPN-1 NGX R65 SmartCenter Server.
- C. Request an NGX R65 SmartCenter Server license, using the existing gateway machine's IP address. Request a new local license for the NGX R65 VPN-1 Gateway using the new server's IP address.
- D. Request an NGX R65 SmartCenter Server license, using the new server's IP address. Request a new central NGX R65 VPN-1 Gateway license for the existing gateway server's IP address.

Answer: A

Explanation:

QUESTION NO: 207

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

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

Answer: B

Explanation:

QUESTION NO: 208

What action can be run from SmartUpdate NGX R65?

- A. remote_uninstall_verifier
- B. upgrade_export
- C. mds_backup
- D. cpinfo

Answer: D

Explanation:

QUESTION NO: 209

What tools CANNOT be launched from SmartUpdate NGX R65?

- A. cpinfo
- B. SecurePlatform Web UI
- C. Nokia Voyager
- D. snapshot

Answer: D

Explanation:

QUESTION NO: 210

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

Answer: B

Explanation:

QUESTION NO: 211

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

Answer: B

Explanation:

QUESTION NO: 212

You are using SmartUpdate to fetch data and perform a remote upgrade of an NGX Security Gateway.

Which of the following statements is FALSE?

- A. If SmartDashboard is open during package upload and upgrade, the upgrade will fail.
- B. A remote installation can be performed without the SVN Foundation package installed on a remote NG with Application Intelligence Security Gateway
- C. SmartUpdate can query the SmartCenter Server and VPN-1 Gateway for product information
- D. SmartUpdate can query license information running locally on the VPN-1 Gateway

Answer: B

Explanation:

QUESTION NO: 213

What port is used for communication to the UserCenter with SmartUpdate?

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

Answer: B

Explanation:

QUESTION NO: 214

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

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

Answer: D

Explanation:

QUESTION NO: 215

What action CANNOT be run from SmartUpdate NGX R65?

- A. Get all Gateway Data
- B. Reboot gateway
- C. Preinstall verifier...

D. Fetch sync status

Answer: D

Explanation:

QUESTION NO: 216

You want to upgrade an NG with Application Intelligence R55 Security Gateway running on SecurePlatform to VPN-1 NGX R65 via SmartUpdate. Which package(s) is(are) needed in the Repository prior to upgrade?

- A. SecurePlatform NGX R65 package
- B. VPN-1 Power/UTM NGX R65 package
- C. SecurePlatform and VPN-1 Power/UTM NGX R65 packages
- D. SVN Foundation and VPN-1 Power/UTM packages

Answer: A

Explanation:

QUESTION NO: 217

Why should the upgrade_export configuration file (.tgz) be deleted after you complete the import process?

- A. It will prevent a future successful upgrade_export since the .tgz file cannot be overwritten.
- B. It will conflict with any future upgrades run from SmartUpdate.
- C. SmartUpdate will start a new installation process if the machine is rebooted.
- D. It contains your security configuration, which could be exploited.

Answer: D

Explanation:

QUESTION NO: 218

Concerning these products: SecurePlatform, VPN-1 Pro Gateway, UserAuthority Server, Nokia OS, UTM-1, Eventia Reporter, and Performance Pack, which statement is TRUE?

- A. All but the Nokia OS can be upgraded to VPN-1 NGX R65 with SmartUpdate.
- B. All but Performance Pack can be upgraded to VPN-1 NGX R65 with SmartUpdate.
- C. All can be upgraded to VPN-1 NGX R65 with SmartUpdate.
- D. All but the UTM-1 can be upgraded to VPN-1 NGX R65 with SmartUpdate.

Answer: C

Explanation:

QUESTION NO: 219

If a SmartUpdate upgrade or distribution operation fails on SecurePlatform, how is the system recovered?

- A.** SecurePlatform will reboot and automatically revert to the last snapshot version prior to upgrade.
- B.** The Administrator must remove the rpm packages manually, and reattempt the upgrade.
- C.** The Administrator can only revert to a previously created snapshot (if there is one) with the command `cprinstall snapshot <object name> <filename>`.
- D.** The Administrator must reinstall the last version via the command `cprinstall revert <object name> <file name>`.

Answer: A

Explanation:

QUESTION NO: 220

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

- A.** After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the packages directory on the selected remote Security Gateway.
- B.** After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the Package Repository on the SmartCenter Server.
- C.** After selecting "Packages: Add... from CD", the selected package is copied to the packages directory on the selected remote Security Gateway.
- D.** After selecting "Packages: Add... from CD", the selected package is copied to the Package Repository on the SmartCenter Server.

Answer: D

Explanation:

QUESTION NO: 221

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

- A.** After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the Package Repository on the SmartCenter to the Security Gateway but

the installation IS NOT performed.

- B.** After selecting "Packages > Distribute..." and choosing the target gateway, the SmartUpdate wizard walks the Administrator through a Distributed Installation.
- C.** After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the Package Repository on the SmartCenter to the Security Gateway and the installation IS performed.
- D.** After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the CDROM of the SmartUpdate PC directly to the Security Gateway and the installation IS performed.

Answer: A

Explanation:

QUESTION NO: 222

What happens in relation to the CRL cache after a cpstop;spstart has been initiated?

- A.** The gateway continues to use the old CRL even if it is not valid, until a new CRL is cached
- B.** The gateway continues to use the old CRL, as long as it is valid.
- C.** The gateway issues a crl_zap on startup, which empties the cache and forces Certificate retrieval.
- D.** The gateway retrieves a new CRL on startup, then discards the old CRL as invalid.

Answer: B

Explanation:

QUESTION NO: 223

Public-key cryptography is considered which of the following?

- A.** two-key/symmetric
- B.** one-key/asymmetric
- C.** two-key/asymmetric
- D.** one-key/symmetric

Answer: C

Explanation:

QUESTION NO: 224

What is the greatest benefit derived from VPNs compared to frame relay, leased lines any other types of dedicated networks?

- A. lower cost
- B. stronger authentication
- C. Less failure/downtime
- D. Greater performance

Answer: A

Explanation:

QUESTION NO: 225

What is the bit size of DES?

- A. 56
- B. 112
- C. 168
- D. 128
- E. 32
- F. 64

Answer: A

Explanation:

QUESTION NO: 226

In cryptography, the Rivest, Shamir, Adelman (RSA) scheme has which of the following? Select all that apply.

- A. A symmetric-cipher system
- B. A secret-key encryption-algorithm system
- C. A public-key encryption-algorithm system
- D. An asymmetric-cipher system

Answer: C,D

Explanation:

QUESTION NO: 227

Which of the following are supported with the office mode? Select all that apply.

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

Answer: A,B,E

Explanation:

QUESTION NO: 228

Which network port does PPTP use for communication?

- A. 1723/tcp
- B. 1723/udp
- C. 25/udp
- D. 25/tco

Answer: A

Explanation:

QUESTION NO: 229

VPN access control would fall under which VPN component?

- A. QoS
- B. Performance
- C. Management
- D. Security

Answer: D

Explanation:

QUESTION NO: 230

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

- A. fwm
- B. cphad
- C. fw.d
- D. fwd.proc

Answer: B

Explanation:

QUESTION NO: 231

If a digital signature is used to achieve both data-integrity checking and verification of sender, digital signatures are only used when implementing:

- A. A symmetric-encryption algorithm
- B. CBL-DES
- C. Triple DES
- D. An asymmetric-encryption algorithm

Answer: D

Explanation:

QUESTION NO: 232

Which of the following is supported with Office Mode?

- A. SecuRemote
- B. SecureClient
- C. SSL Network Extender
- D. Connect Mode

Answer: A

Explanation:

QUESTION NO: 233

When synchronizing clusters, which of the following statements are true?

Select all that apply.

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

Answer: A,B,C

Explanation:

QUESTION NO: 234

VPN traffic control would fall under which VPN component?

- A. Performance
- B. Management
- C. Security
- D. QoS

Answer: D

Explanation:

QUESTION NO: 235

Which of the following is an example of the hash function?

- A. DES and CBC
- B. DAC and MAC
- C. SHA and 3DES
- D. MD5 and SHA-1

Answer: D

Explanation:

QUESTION NO: 236

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. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.
- C. MEP Gateways must be managed by the same SmartCenter Server.
- 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: 237

Consider the following actions that VPN-1 NGX can take when it control packets. The Policy Package has been configured for Traditional Mode VPN. Identify the options that includes the available actions. Select four.

- A. Allow
- B. Reject
- C. Client auth
- D. Decrypt
- E. Accept
- F. Drop
- G. Encrypt
- H. Hold
- I. Proxy

Answer: B,E,F,G

Explanation:

QUESTION NO: 238

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 SecureClient/SecuRemote/SSL Network Extended encrypted connections.
- C. Support for all VPN deployments (except those with third-party VPN peers)
- D. Support for Performance Pack acceleration

Answer: B

Explanation:

QUESTION NO: 239

Which of the following does IPSec use during IPSec key negotiation?

- A. IPSec SA
- B. RSA Exchange
- C. ISAKMP SA
- D. Diffie-Hellman exchange

Answer: D

Explanation:

QUESTION NO: 240

Which of the following SSL Network Extender server-side prerequisites are correct? Select all that apply.

- A. The VPN1-Gateway must be configured to work with Visitor Mode
- B. The specific VPN-1 Security Gateway must be configured as a member of the VPN-1 Remote Access Community.
- C. There are distinctly separate access rules required for SecureClient users vs. SSL Network Extender users.
- D. To use Integrity Clientless Security (ICS), you must install the ICS server or configuration tool.

Answer: A,B,D

Explanation:

QUESTION NO: 241

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

Answer: C

Explanation:

QUESTION NO: 242

Which of the following provides a unique user ID for a digital Certificate?

- A. Username
- B. User-message digest
- C. User e-mail
- D. User organization

Answer: B

Explanation:

QUESTION NO: 243

For object-based VPN routing to succeed, what must be configured?

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

Answer: C

Explanation:

QUESTION NO: 244

What proprietary Check Point protocol is the basis of the functionality of Check Point ClusterXL inter-module communication?

- A.** RDP
- B.** IPSec
- C.** CCP
- D.** HA OPCODE
- E.** CKPP

Answer: C

Explanation:

QUESTION NO: 245

Which of the following is part of the PKI? Select all that apply.

- A.** User certificate
- B.** Attribute Certificate
- C.** Certificate Revocation Lists

D. Public-key certificate

Answer: A,C,D

Explanation:

QUESTION NO: 246

Which of the following are valid PKI architectures?

- A. mesh architecture
- B. Bridge architecture
- C. Gateway architecture
- D. Hierarchical architecture

Answer: A,C,D

Explanation:

QUESTION NO: 247

Which of the following are valid reasons for beginning with a fresh installation VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65? Select all that apply.

- 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 over time.

Answer: A,C,D

Explanation:

QUESTION NO: 248

Public keys and digital certificates provide which of the following? Select three.

- A. Non repudiation
- B. Data integrity
- C. Availability
- D. Authentication

Answer: A,B,D

Explanation:

QUESTION NO: 249

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

- A. dynamic encryption
- B. Certificate-based encryption
- C. static encryption
- D. Symmetric encryption
- E. Asymmetric encryption

Answer: D

Explanation:

QUESTION NO: 250

Which of the following happen when using Pivot Mode in ClusterXL? Select all that apply.

- A. The Pivot forwards the packet to the appropriate cluster member.
- B. The Security Gateway analyzes the packet and forwards it to the Pivot.
- C. The packet is forwarded through the same physical interface from which it originally came, not on the sync interface.
- D. The Pivot's Load Sharing decision function decides which cluster member should handle the packet.

Answer: A,C,D

Explanation:

QUESTION NO: 251

Central License management allows a Security Administrator to perform which of the following? Select all that apply.

- A. Attach and/or delete only NGX Central licenses to a remote module (not Local licenses)
- B. Check for expired licenses
- C. Add or remove a license to or from the license repository
- D. Sort licenses and view license properties
- E. Delete both NGX Local licenses and Central licenses from a remote module
- F. Attach both NGX Central and Local licenses to a remote module

Answer: A,B,C,D

Explanation:

QUESTION NO: 252

How should Check Point packages be uninstalled?

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

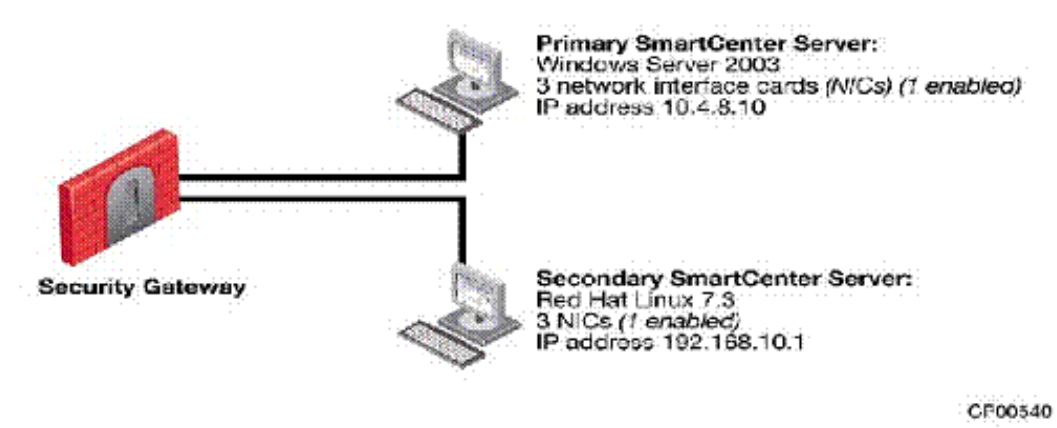
Answer: B

Explanation:

QUESTION NO: 253

The following configuration is for VPN-1 NGX 65.

:Is this configuration correct for Management High Availability (HA)?



- A. No, a NGX 65 SmartCenter Server cannot run on Red Hat Linux 7.3.
- B. No, the SmartCenter Servers must be installed on the same operating system.
- C. No, the SmartCenter Servers must reside on the same network.
- D. No, the SmartCenter Servers do not have the same number of NICs.

Answer: B

Explanation:

QUESTION NO: 254

When distributing IPSec packets to gateways in a Load Sharing Multicast mode cluster, which valid Load Sharing method will consider VPN information in the decision function?

- A. Load Sharing based on SPIs
- B. Load Sharing based on ports, VTI, and IP addresses
- C. Load Sharing based on IP addresses, ports, and serial peripheral interfaces.
- D. Load Sharing based on IP addresses, ports, and security parameter indexes.

Answer: D

Explanation:

QUESTION NO: 255

Which encryption scheme provides in-place encryption?

- A. DES
- B. SKIP
- C. AES
- D. IKE

Answer: B

Explanation:

QUESTION NO: 256

Which of the following can be said about numbered VPN Tunnel Interfaces (VTIs)?

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

Answer: A

Explanation:

QUESTION NO: 257

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

- A. fw install_mgmt

- B. upgrade_mgmt
- C. patch add cd
- D. fwm upgrade_tool

Answer: C

Explanation:

QUESTION NO: 258

What can be said about RSA algorithms? Select all that apply.

- A. Long keys can be used in RSA for enhances security
- B. Short keys can be used for RSA efficiency.
- C. RSA is faster to compute than DES
- D. RSA's key length is variable.

Answer: A,B,D

Explanation:

QUESTION NO: 259

By default Check Point High Availability components send updates about their state every...

- A. 1 second
- B. 2 seconds
- C. 5 seconds
- D. 0.1 seconds
- E. 0.5 seconds

Answer: D

Explanation:

QUESTION NO: 260

What is the most typical type of configuration for VPNs with several externally managed Gateways?

- A. star community
- B. mesh community
- C. domain community
- D. Hybrid community

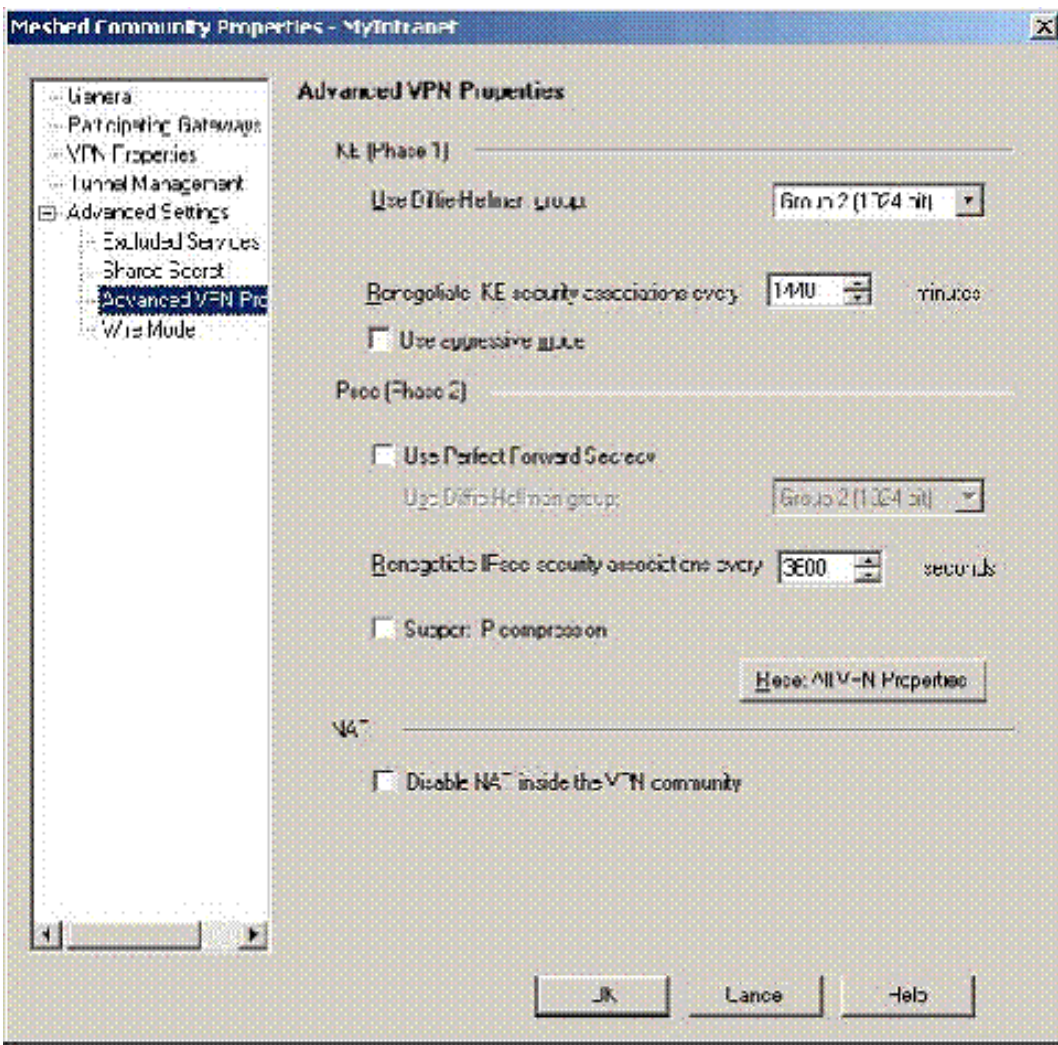
E. SAT community

Answer: A

Explanation:

QUESTION NO: 261

Exhibit:



You study the Advanced Properties exhibit carefully. What settings can you change to reduce the encryption overhead and improve performance for your mesh VPN Community?

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

Answer: A

Explanation:

QUESTION NO: 262

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

```
vpn shell interface add numbered 10.10.0.1 10.10.0.2 Helsinki.cp
```

What do you know about this VTI?

- A. The VTI name is "Helsinki.cp"
- B. The local Gateway's object name is "Helsinki.cp"
- C. The peer Security Gateway's name is "Helsinki.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: C

Explanation:

QUESTION NO: 263 DRAG DROP

ABC.com has two sites using certificates-based VPN issued by the ICA. The two sites, Tokyo and Paris, are configured using a simplified VPN policy. You are trying to integrate a new office opening in New Delhi. You must enable all three sites to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server behind the Paris Security Gateway.

After creating the Dubai Gateway object with the proper VPN domain, what must you do?

Steps Select from here

Steps place here

- Add the Dubai Gateway object into the mesh VPN Community shared by Paris and Tokyo
- Reinstall the Security Policy on all three Gateways
- Configure "Traditional mode VPN configuration" option in the Dubai Gateway object's VPN screen. Ensure that the "Support Authentication Methods: Public key Signatures" is checked
- Verify the Rules Bases which will be installed on all three gateways allows the desired source and destination VPN traffic
- Manually generate an ICA Certificate on the VPN tab of the of the Dubai Gateway object by clicking the Add ... button.

- Place first step here*
- Place first step here*
- Place third step, if any, here*
- Place fourth step, if any, here*
- Place 5th step, if any, here*

Answer:

Steps Select from here

Steps place here

- Add the Dubai Gateway object into the mesh VPN Community shared by Paris and Tokyo
- Reinstall the Security Policy on all three Gateways
- Configure "Traditional mode VPN configuration" option in the Dubai Gateway object's VPN screen. Ensure that the "Support Authentication Methods: Public key Signatures" is checked
- Verify the Rules Bases which will be installed on all three gateways allows the desired source and destination VPN traffic
- Manually generate an ICA Certificate on the VPN tab of the of the Dubai Gateway object by clicking the Add ... button.

- Verify the Rules Bases which will be installed on all three gateways allows the desired source and destination VPN traffic
- Add the Dubai Gateway object into the mesh VPN Community shared by Paris and Tokyo
- Reinstall the Security Policy on all three Gateways
- Place fourth step, if any, here*
- Place 5th step, if any, here*

QUESTION NO: 264 DRAG DROP

Match the ClusterXL Modes with their configurations.

Steps Select from here

New mode High Availability

Load Sharing Multicast mode

Load Sharing Unicast mode

Legacy mode High Availability

Definitions

Provides a clustering mechanism through the use of cloned interface configuration details.

Every member of the cluster receives all packets sent to the cluster IP address, with the load distributed optimally among all cluster members.

One machine in the cluster receives all traffic from a router, and redistributes the packets to other machines in the cluster, implementing both Load Sharing and redundancy

Only one machine is active at any one time. A failure of the active machine causes a failover to the next highest priority machine in the cluster

Options, place here

Place here

Place here

Place here

Place here

Answer:

Steps Select from here

New mode High Availability

Load Sharing Multicast mode

Load Sharing Unicast mode

Legacy mode High Availability

Definitions

Provides a clustering mechanism through the use of cloned interface configuration details.

Every member of the cluster receives all packets sent to the cluster IP address, with the load distributed optimally among all cluster members.

One machine in the cluster receives all traffic from a router, and redistributes the packets to other machines in the cluster, implementing both Load Sharing and redundancy

Only one machine is active at any one time. A failure of the active machine causes a failover to the next highest priority machine in the cluster

Options, place here

New mode High Availability

Load Sharing Multicast mode

Load Sharing Unicast mode

Legacy mode High Availability

QUESTION NO: 265 DRAG DROP

Match the Terms with their definitions.

Options, select from these

VPN Site

VPN Community

VPN Domain

VPN Community member

Definitions

Hosts behind the Gateway

Place here

Community member plus VPN domain

Place here

Collection of VPN tunnels

Place here

Gateway at one end of a VPN tunnel

Place here

Answer:

Options, select from these

VPN Site

VPN Community

VPN Domain

VPN Community member

Definitions

Hosts behind the Gateway

VPN Community

Community member plus VPN domain

VPN Site

Collection of VPN tunnels

VPN Community

Gateway at one end of a VPN tunnel

VPN Community member

QUESTION NO: 266 DRAG DROP

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically. Select the best response for the synchronization sequence.

Select Steps from here	Steps place here
A scheduled event occurs.	Place first step here
The Security Policy is saved.	Place second step, if any, here
The user database is installed	Place third step, if any, here
The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active .	Place fourth step, if any, here
The Security Policy is installed	Place 5th step, if any, here

Answer:

Select Steps from here	Steps place here
A scheduled event occurs.	The Security Policy is installed
The Security Policy is saved.	The Security Policy is saved.
The user database is installed	A scheduled event occurs.
The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active .	Place fourth step, if any, here
The Security Policy is installed	Place 5th step, if any, here

QUESTION NO: 267 DRAG DROP

Match the remote-access VPN connection mode features with their descriptions.

Auto connect	Hub mode
Office Mode	Visitor Mode

Definitions

All traffic routed through the Gateway	Place here
E-mail client tries to access an IMAP server behind the SecurityGateway. SecureClient prompts the user to initiate a tunnel to that Gateway.	Place here
Tunnels client-to-Gateway traffic via TCP on port 433	Place here
Resolves routing issues between the client and the Gateway	Place here

Answer:

Auto connect	Hub mode
Office Mode	Visitor Mode

Definitions

All traffic routed through the Gateway	Hub mode
E-mail client tries to access an IMAP server behind the SecurityGateway. SecureClient prompts the user to initiate a tunnel to that Gateway.	Auto connect
Tunnels client-to-Gateway traffic via TCP on port 433	Visitor Mode
Resolves routing issues between the client and the Gateway	Office Mode

QUESTION NO: 268

Which of the following commands can be used to bind a NIC to a single processor when using a

Performance Pack on SecurePlatform?

- A. fw fat path nic
- B. splat proc
- C. sim affinity
- D. set proc

Answer: C

Explanation:

QUESTION NO: 269

What is the maximum number of cores supported by CoreXL?

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

Answer: B

Explanation:

QUESTION NO: 270

Which of the following is NOT a restriction for connection template generation?

- A. ISN Spoofing
- B. SYN Defender
- C. UDP services with no protocol type or source port mentioned in advanced properties
- D. VPN Connections

Answer: C

Explanation:

QUESTION NO: 271

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

Answer: C

Explanation:

QUESTION NO: 272

From the following Rule Base, for which rules will the connection templates be generated in SecureXL?

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Stealth Rule	Any	Corporate-gw	Any Traffic	Any	drop	Log	Policy Tars	Any
2	Local Users Access AOL	Corporate-internal-ne	Any	Any Traffic	AOL	accept	Log	Policy Tars	Any
3	Customers Accessing Web Server	Customers@Any	Corporate-web-s	Any Traffic	Http	Client Auth	Log	Policy Tars	Any
4	Incoming Emails	Any	Corporate-mail-s	Any Traffic	smtp-MailFilter	accept	Log	Policy Tars	Any
5	HTTP/FTP access	Corporate-internal-ne	Any	Any Traffic	Http Ftp	accept	Log	Policy Tars	Any
6	Cleanup Rule	Any	Any	Any Traffic	Any	drop	Log	Policy Tars	Any

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

Answer: C

Explanation:

QUESTION NO: 273

In which ClusterXL Load Sharing mode, does the pivot machine get chosen automatically by ClusterXL?

- A. Unicast Load Sharing
- B. Hot Standby Load Sharing
- C. CCP Load Sharing
- D. Multicast Load Sharing

Answer: A

Explanation:

QUESTION NO: 274

Which Check Point QoS feature allows a Security Administrator to define special classes of service for delay-sensitive applications?

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

Answer: D

Explanation:

QUESTION NO: 275

What is the router command to save your OSPF configuration?

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

Answer: D

Explanation:

QUESTION NO: 276

At what router prompt would you save your OSPF configuration?

- A. localhost.localdomain#
- B. localhost.localdomain(conf ig-if)#
- C. local host. localdomain(conf ig)#
- D. localhost.localdomain(config-router-ospf)#

Answer: A

Explanation:

QUESTION NO: 277

Which of the following operating systems support numbered VTI's?

- A. IPSO 4.0 +
- B. SecurePlatform Pro
- C. Windows Server 2003
- D. Solaris

Answer: B

Explanation:

QUESTION NO: 278

Which statement is TRUE for route-based VPNs?

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

Answer: D

Explanation:

QUESTION NO: 279

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

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

Answer: B

Explanation:

QUESTION NO: 280

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

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

Answer: A

Explanation:

QUESTION NO: 281

What is the reason for the following error? (See Graphic)

```
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}#  
{fw1}# cphaprob -i list  
Built-in Devices:  
Device Name: Interface Active Check  
Device Name: HA Initialization  
Registered Devices:  
Device Name: *iu**B*  
Registration number: 8  
Timeout: none  
Failed to query kernel for device no. 1  
{fw1}#
```

- A. Name contains non-ASCII characters.
- B. Objects.C does not contain a cluster object.
- C. A third-party cluster solution is implemented.
- D. Cluster membership is not enabled on the gateway.

Answer: D

Explanation:

QUESTION NO: 282

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

Answer: B

Explanation:

QUESTION NO: 283

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

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

Answer: D

Explanation:

QUESTION NO: 284

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

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

Answer: B

Explanation:

QUESTION NO: 285

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: 1 GB, Security

Gateway, version: R71 and primary Security Management Server installed, version:

R71

Cluster Member 2: OS: SecurePlatform, NICs: 4 Intel 3Com, memory: 1 GB, Security

Gateway only, version: R71

Cluster Member 3: OS: SecurePlatform, NICs: 4 other manufacturers, memory: 512 MB,

Security Gateway only, version: R71

Are these machines correctly configured for a ClusterXL deployment?

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

Answer: A

Explanation:

QUESTION NO: 286

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

- A. perf_pack off
- B. fw accel off
- C. splat_accel off
- D. fwaccel off

Answer: D

Explanation:

QUESTION NO: 287

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

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

Answer: A

Explanation:

QUESTION NO: 288

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

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

Answer: D

Explanation:

QUESTION NO: 289

After Travis added new processing cores on his server, CoreXL did not use them. What would be the most plausible reason why? Travis did not:

- A. edit the Gateway Properties and increase the number of CPU cores.
- B. run cpconfig to increase the kernel instances.
- C. edit the Gateway Properties and increase the kernel instances.
- D. run cpconfig to increase the number of CPU cores.

Answer: B

Explanation:

QUESTION NO: 290

Check Point New Mode HA is a(n)_____ solution.

- A. hot-standby
- B. primary-domain
- C. acceleration
- D. load-balancing

Answer: A

Explanation:

QUESTION NO: 291

Included in the client's network are some switches, which rely on IGMP snooping. You must find a solution to work with these switches. Which of the following answers does NOT lead to a successful solution?

- A. ClusterXL supports IGMP snooping by default. There is no need to configure anything.
- B. Disable IGMP registration in switches that rely on IGMP packets
- C. Set the value of fwaha_enable_igmp_snooping module configuration parameter to 1.
- D. Configure static CAMs to allow multicast traffic on specific ports.

Answer: A

Explanation:

QUESTION NO: 292

You have two IP Appliances: one IP565 and one IP395. Both appliances have IPSO 6.2 and R71 installed in a distributed deployment. Can they be members of a Gateway Cluster?

- A. Yes, as long as they have the same IPSO and Check Point versions.
- B. No, because IP does not have a cluster option.
- C. No, because the Security Gateways must be installed in a stand-alone installation.
- D. No, because the appliances must be of the same model (both should be IP565 or IP395).

Answer: A

Explanation:

QUESTION NO: 293

What could be a reason why synchronization between primary and secondary Security Management Servers does not occur?

- A. You have installed both Security Management Servers on different server systems (e. g. one machine on HP hardware and the other one on DELL).
- B. You are using different time zones.
- C. You did not activate synchronization within the Global Properties.
- D. If the set of installed products differ from each other, the Security Management Servers do not synchronize the database to each other.

Answer: D

Explanation:

QUESTION NO: 294

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

Answer: B

Explanation:

QUESTION NO: 295

What does it mean when a Security Gateway is labeled Untrusted in the SmartProvisioning Status view?

- A. SIC has not been established between the Security Gateway and the Security Management.
- B. SmartProvisioning is not enabled on the Security Gateway,
- C. cpd is not running at the Security Gateway.
- D. The Security Gateway is down.

Answer: A

Explanation:

QUESTION NO: 296

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

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

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

Answer: C

Explanation:

QUESTION NO: 297

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 to "Remote Offices"
3. Click File, then select New, then Provisioning Profile
4. Click on the Devices Tab
5. Highlight the Dallas Edge appliance, click Edit, then edit Gateway
6. Click on the Profiles Tab

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

Answer: A

Explanation:

QUESTION NO: 298

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

- A. IPSO 4.2 Security Gateways
- B. Edge firmware 6.x and above
- C. R65 HFA 40 Security Gateways and above
- D. NGX Security Appliances

Answer: C

Explanation:

QUESTION NO: 299

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

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

Answer: B

Explanation:

QUESTION NO: 300

Which of the following load-balancing methods is not valid?

- A. Domain
- B. They are all valid
- C. Round trip
- D. Random

Answer: B

Explanation:

QUESTION NO: 301

The relay mail server configured under "Email Notifications" is used by the DLP Gateway to:
(Choose the BEST answer.)

- A. Synchronize with other mail servers in the network.
- B. If UserCheck is configured, there is no need to configure this relay server if there are no Ask User rules and there is no need to notify any Data Owners.
- C. Define My Organization > DLP Gateway and scan only e-mails that originate from this relay server
- D. Release e-mails from quarantine - DLP Gateway will send the released e-mail to this relay mail server.

Answer: D

Explanation:

QUESTION NO: 302

For a dedicated DLP Gateway that runs in inline bridge mode, why is it important to properly define the topology?

- A. Topology definition is necessary for correct anti-spoofing.
- B. Topology is used for Hide NAT.

- C. By default. My Organization is defined by the internal interfaces of a DLP Gateway.
- D. Topology definition is used for VPN communities definition.

Answer: C

Explanation:

QUESTION NO: 303

Which protocol is not supported for DLP?

- A. ftp
- B. https
- C. http
- D. smtp

Answer: B

Explanation:

QUESTION NO: 304

What happens when an Administrator activates the DLP Portal for Self Incident Handling and enters its fully qualified domain name (DNS name)?

- A. Connections created between the user and the DLP Gateway when clicking links within e-mail notifications to send or discard quarantined e-mails (matched for an Ask User rule) are encrypted.
- B. The daemon running DLP Portal starts to run and can cater requests from users' browsers (following links from e-mail notifications) and from Check Point UserCheck.
- C. The DLP Gateway can now notify Data Owners about DLP incidents.
- D. UserCheck is activated.

Answer: B

Explanation:

QUESTION NO: 305

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 positive very low. How can you achieve this?

- A. 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. As in SmartDefense, this can be achieved by activating all the critical checks manually.
- 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. This can't be achieved; activating any IPS system always causes a high rate of false positives.

Answer: C

Explanation:

QUESTION NO: 306

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 a network attack, or a user's system is infected with a worm. Will you get all the information you need from these actions?

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

Answer: D

Explanation:

QUESTION NO: 307

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

Answer: B

Explanation:

QUESTION NO: 308

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

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

Answer: C

Explanation:

QUESTION NO: 309

You are responsible for the IPS configuration of your Check Point firewall. Inside the Denial of service section you need to set the protection parameters against the Teardrop attack tool with high severity. How would you characterize this attack tool? Give the BEST answer.

Protection	Sever.	Confide.	Perfor.	Industry Refe.	Relea.
Teardrop	High	Medium	Vey low	CAN-1999-025	
Ping of Death	Medium	Medium	Vey low	CVE-1999-0129	
LAND	Medium	Medium	Vey low	CVE-1999-0016	
Non-TCP Flooding	High	Medium	Low	None	
Aggressive Aging	Medium	High	Vey low	None	

- A. Hackers can send high volumes of non-TCP traffic in an effort to fill up a firewall State Table. This results in a Denial of Service by preventing the firewall from accepting new connections. Teardrop is a widely available attack tool that exploits this vulnerability.
- B. A remote attacker may attack a system by sending a specially crafted RPC request to execute arbitrary code on a vulnerable system. Teardrop is a widely available attack tool that exploits this vulnerability.
- C. Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination, i.e., spoofed). Teardrop is a widely available attack tool that exploits this vulnerability.
- D. Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. Teardrop is a widely available attack tool that exploits this vulnerability.

Answer: D

Explanation:

QUESTION NO: 310

Which application is used to create a File-Share Application?

- A. SmartDashboard (SSL VPN Tab)
- B. SmartPortal WebUI (File-Share Tab)
- C. SSL VPN Portal WebUI (File-Share Tab)
- D. Provider-1 MDG (Global VPNs Tab)

Answer: A

Explanation:

QUESTION NO: 311

Which procedure will create an Internal User?

- A. In the Users and Administrators tab, right click Users and click SSL VPN User
- B. In the General Properties of the gateway, click the SSL VPN check box. The SSL VPN Blade Wizard will launch and Step 2 will allow adding new users who will be imported from a RADIUS server.
- C. From the SSL VPN tab, click Users and Authentication | Internal Users | Users and click New User | Default
- D. In the Users and Administrators tab, click User Groups | Clientless-vpn-user and add the SSL VPN user to the Clientless-vpn-user group

Answer: C

Explanation:

QUESTION NO: 312

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

- A. External Script
- B. Block Access
- C. SNMP Trap

D. Mail

Answer: B

Explanation:

QUESTION NO: 313

What are the 3 main components of the SmartEvent 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. i, iv, v
- C. i, iii, iv
- D. iv, v, vi

Answer: B

Explanation:

QUESTION NO: 314

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

- A. SmartEvent Server
- B. SmartUpdate
- C. SmartReporter
- D. SmartDashboard

Answer: D

Explanation:

QUESTION NO: 315

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

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

Answer: D

Explanation:

QUESTION NO: 316

Which version is the minimum requirement for SmartProvisioning?

- A. R65 HFA 40
- B. R70
- C. R71
- D. R70.20

Answer: A

Explanation:

QUESTION NO: 317

SmartReporter Data Base settings could be modified in:

- A. \$CPDIR/Database/conf/conf.C
- B. \$ERDIR/conf/my.cnf +f
- C. \$RTDIR/Database/conf/my.ini
- D. \$FWDIR/Eventia/conf/ini.C

Answer: C

Explanation:

QUESTION NO: 318

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

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

Answer: B

Explanation:

QUESTION NO: 319

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

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

Answer: A

Explanation:

QUESTION NO: 320

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

- A. 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.
- B. The SmartDashboard will function without SmartWorkflow, with no session and no audit trail functionality.
- C. The SmartDashboard will have no session but SmartView Tracker and audit trail will be available.
- D. All functions of SmartWorkflow will be available on a per rule basis.

Answer: A

Explanation:

QUESTION NO: 321

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

Answer: A

Explanation:

QUESTION NO: 322

Assuming all connections that are allocated bandwidth in your Check Point QoS Rule Base are open, what would be the corresponding bandwidth percentage of the Kazaa Rule in the following example?

NAME	SOURCE	DESTINATION	SERVICE	ACTION
Site to Site VPN	GW-group	GW-group	CIFS ftp smtp http https	Weight 20
Kazaa	internal-net-group	* Any	KaZaA	Weight 5
Default	* Any	* Any	* Any	Weight 10

- A. 5%
- B. 20%
- C. 8%
- D. 14%

Answer: D

Explanation:

QUESTION NO: 323

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

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

Answer: D

Explanation:

QUESTION NO: 324

SmartProvisioning uses different types of profiles to manage and provision the gateways. These types are:

- A.** SmartLSM Security Profiles and Provisioning Profiles.
- B.** Provisioning Profiles and Gateways Profiles.
- C.** SmartLSM Security Profiles and SmartDashboard Profiles.
- D.** SmartConsole Profiles and SmartFilter Profiles.

Answer: A

Explanation:

QUESTION NO: 325

What is the best method for scheduling backup's on multiple firewalls?

- A.** WebUI
- B.** SmartProvisioning
- C.** Smart Dashboard

D. SmartUpdate

Answer: B

Explanation:

QUESTION NO: 326

The graphic illustrates which command being issued on SecurePlatform?

```

-----
conn created                21      conn deleted                2
temporary conn             0      templates                   1
nat conn                   0      accel packets               698
accel bytes                118462  F2F packets                 26183
ESP enc pkts              0      ESP enc err                 0
ESP dec pkts              0      ESP dec err                 0
ESP other err             0      espudp enc pkts            0
espudp enc err            0      espudp dec pkts            0
espudp dec err            0      espudp other err           0
AH enc pkts               0      AH enc err                 0
AH dec pkts               0      AH dec err                 0
AH other err              0      memory used                 0
free memory               0      acct update interval       3600
current total conn        14      TCP violations              1
conn from templates       11      TCP conn                   12
delayed tcp conn         0      non tcp conn                2
delayed nonTCP conn      0      F2F conn                    5
F2F bytes                 1754802  crypt conn                  0
enc bytes                  0      dec bytes                   0
partial conn              0      anticipated conn            0
dropped packets           56      dropped bytes               7472
-----

```

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

Answer: A

Explanation:

QUESTION NO: 327

What is a "sticky" connection?

- A. A "sticky" connection is one in which a reply packet returns through the same gateway as the original packet.
- B. A "sticky" connection is a VPN connection that remains up until you manually bring it down.
- C. A "sticky" connection is a connection that always chooses the same gateway to set up the initial connection.

D. A "sticky" connection is a connection that remains the same.

Answer: A

Explanation:

QUESTION NO: 328

When two or more DLP rules are matched, the action taken is the most restrictive action. Rank the following items from the lowest restriction level (1) to the highest (4).

1. Ask User
2. Prevent
3. Detect
4. Inform User

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

Answer: A

Explanation:

QUESTION NO: 329

When using IPS, what does Geo protection do?

- A. To block traffic from and to a specific country
- B. To block traffic from and to a specific person
- C. To block traffic from and to a specific company
- D. To block traffic from and to a specific city

Answer: A

Explanation:

QUESTION NO: 330

Which of these is a type of acceleration in SecureXL?

- A. connection rate
- B. GRE
- C. FTP
- D. QoS

Answer: A

Explanation:

QUESTION NO: 331

_____ is a proprietary Check Point protocol. It is the basis for Check Point ClusterXL inter-module communication.

- A. CKPP
- B. CCP
- C. HA OPCODE
- D. RDP

Answer: B

Explanation:

QUESTION NO: 332

The Management Portal allows all of the following EXCEPT:

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

Answer: B

Explanation:

QUESTION NO: 333

Where is the ideal place to deploy your SSL VPN?

- A. Deployed in DMZ
- B. SSL VPN enabled on the gateway
- C. In front of the external interface on the gateway
- D. Anywhere

Answer: A

Explanation:

QUESTION NO: 334

How many events are shown by default in the Event preview pane?

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

Answer: C

Explanation:

QUESTION NO: 335

How is a change approved for implementation in SmartWorkflow?

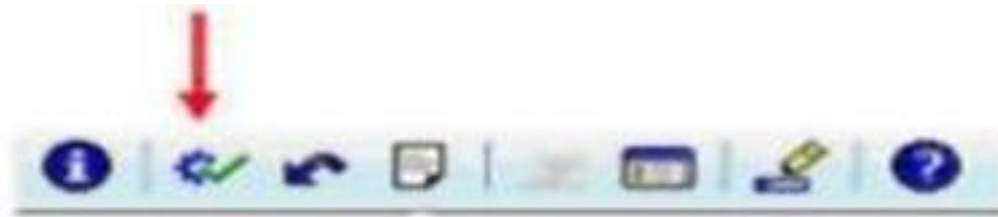
- A. The change is submitted for approval and is manually installed by the approver once the "Approve" button is clicked
- B. The change is submitted for approval and is automatically installed by the original submitter the next time he logs in after approval of the change.
- C. The change is submitted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

Answer: C

Explanation:

QUESTION NO: 336

What is the significance of the depicted icon in the SmartWorkflow toolbar?



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

Answer: A

Explanation:

QUESTION NO: 337

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

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

Answer: B

Explanation:

QUESTION NO: 338

Which of the following can NOT approve a change in a SmartWorkf low session?

- A. FireWall Administrators
- B. FireWall Managers
- C. Provider-1 Superusers

D. Customer Superusers**Answer: A****Explanation:****QUESTION NO: 339**

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

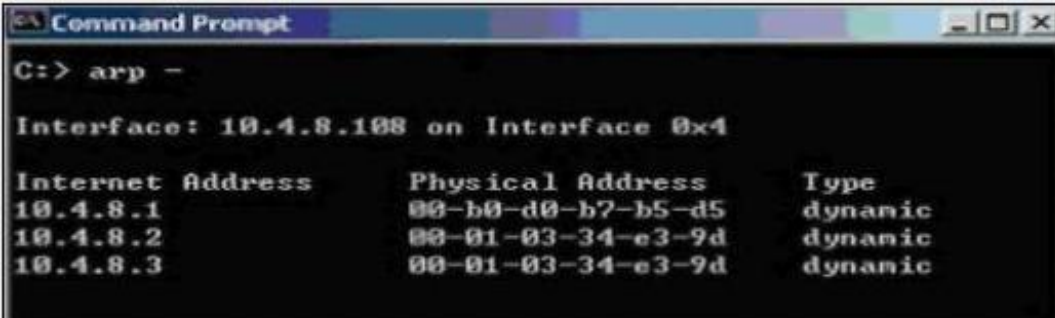
Which actions should be taken to achieve that?

- (i) Use same hard driver for database directory, log files and temporary directory
- (ii) Use Consolidation Rules
- (iii) Limit logging to blocked traffic only
- (iv) Using Multiple Database Tables

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

Answer: C**Explanation:****QUESTION NO: 340**

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. In the graphic is the ARP table from the internal Windows host 10.4.8.108: According to the output, which member is the standby machine?



```
Command Prompt
C:\> arp -

Interface: 10.4.8.108 on Interface 0x4

Internet Address      Physical Address      Type
10.4.8.1              00-b0-d0-b7-b5-d5    dynamic
10.4.8.2              00-01-03-34-e3-9d    dynamic
10.4.8.3              00-01-03-34-e3-9d    dynamic
```

- A. 10.4.8.2
- B. 10.4.8.1
- C. The standby machine cannot be determined by this test.
- D. 10.4.83

Answer: B

Explanation:

QUESTION NO: 341

When a tracked SmartEvent Candidate in a Candidate Pool becomes an Event, what does NOT happen in The Analyzer Server?

- A. The Correlation Unit keeps adding matching logs to the Event.
- B. SmartEvent provides the beginning and end time of the Event.
- C. SmartEvent stops tracking logs related to the Candidate.
- D. The Event is kept open, but condenses many instances into one Event.

Answer: C

Explanation: