Exam : 156-915

Title : Accelerated CCSE NGX (156-915.1)

Ver : 11-25-08

QUESTION 1:

You have two Nokia Appliances one IP530 and one IP380. Both Appliances have IPSO 39 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 stand-alone 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 IP530orIP380.)

Answer: B

QUESTION 2:

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?

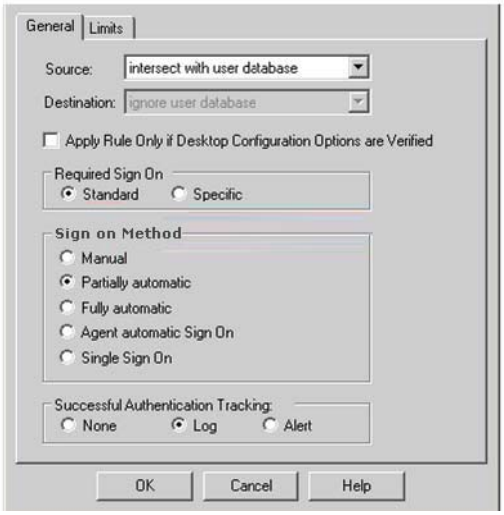
A. Internal_clear>- All_GwToGw
B. Communities >- Communities
C. Internal_clear>- External_Clear
D. Internal_clear>- Communitis
E. Internal_clear>-All_communitis

Answer: E

QUESTION 3:

Review the following rules and note the Client Authentication Action properties screen, as shown in the exhibit.

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Customer@Any	* Any	Any Traffic	TCP http TCP ftp TCP telnet	Client Auth	Log
2		* Any	* Any	Any Traffic	* Any	drop	Log



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

A. FTP session is dropprd by the implicit Cleanup Rule.
B. User is prompted from the FTP site only, and does not need to enter username nad password for the Client Authentication.
C. FTP connection is dropped by rule 2.
D. FTP data connection is dropped, after the user is authenticated successfully.
E. User is prompted for authentication by the Security Gateway again.

Answer: B

QUESTION 4:

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

A. FTP session is dropped by the implicit Cleanup Rule
B. user is prompted from that FTP site on~, and does not need to enter username and password for Client Authentication
C. FTP connection is dropped by rule2
D. FTP data connection is dropped, after the user is authenticated successfully
E. User is prompted for authentication by the Security Gateway aqain

Answer: B

QUESTION 5:

You want to upgrade a SecurePlatform NG with Application Intelligence (AI) R55 Gateway to SecurePlalform 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. SecurePlalform NGX R60
D. SVN Foundation
E. VPN-1 ProfExpress NGX R60

Answer: C

Explanation:
SecurePlatform Upgrade
An IBM e305 server is configured as a SecurePlatform firewall with NG-AI HFA-12. A new VPN-1 Pro/Express Gateway object is created in SmartDashboard. SIC is initialized and NG and NGX licenses are attached to the module.The starting point for the upgrade is illustrated in Figure 13.16.
Figure 13.16 The Package Management View SecurePlatform Pre-Upgrade
The next step is to add the SecurePlatform NGX to the Package Repository using the Add Package From CD option. Insert NGX CD1 containing the SmartUpdate client and click the Add Package From CD button in the toolbar to open a browse window. Select the appropriate drive and the packages are listed as displayed in Figure 13.17. p480, Configuring Check Point NGX VPN-1/FireWall-1, Syngress, 1597490318

QUESTION 6:

What is the command to see the licenses of the Security Gateway Certkiller from your SmartCenter Server?

A. print Certkiller
B. fw licprint Certkiller
C. fw tab -t fwlic Certkiller
D. cplic print Certkiller
E. fw lic print Certkiller

Answer: D

Explanation:
cplic print - prints details of Check Point licenses on the local machine. On a Module, this command will print all licenses that are installed on the local machine - both Local and Central licenses.

P456, .
NG COMMAND LINE INTERFACE
Advanced Technical Reference Guide - NG FP3

QUESTION 7:

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

QUESTION 8:

Ophelia is the security Administrator for a shipping company. Her company uses a custom application to update the distribution database. The custom application includes a service used only to notify remote sites that the distribution database is malfunctioning. The perimeter Security Gateways Rule Base includes a rule to accept this traffic. Ophelia needs to be notified, via atext message to her cellular phone, whenever traffic is accepted on this rule. Which of the following options is MOST appropriate for Ophelia's requirement?

A. User-defined alert script
B. Logging implied rules
C. SmartViewMonitor
D. Pop-up API
E. SNMP trap

Answer: A

QUESTION 9:

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:
QoS rules with the track field set to Log can generate the following types of log events:
QoS rejects a connection when the number of guaranteed connections is exceeded, and/or when the rule's action properties are not set to accept additional connections.
359, accel_ccse_ngx

QUESTION 10:

Choose the BEST sequence for configuring user management on Smart Dash board, for use with an LDAP server

A. Enable LDAP in Global Properties, configure a host-node object for the LDAP Server, and configure a server object for the LDAP Account Unit
B. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties
C. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP server using an OPSEC application
D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object
E. Configure a server object for the LDAP Account Unit, and create an LDAP resource object

Answer: A

Explanation:

1. Confirm the Use LDAP Account Management box is checked in the SmartDashboard Global Properties screen, on the LDAP tab.
2. Confirm User Management is checked on the account unit's General tab.
3. Confirm the LDAP server is accessible from the NGX SmartCenter Server.
4. Confirm there is a host-node object in SmartDashboard, with the IP address of the LDAP server.
5. Confirm there is a server object in SmartDashboard, for an LDAP server using the LDAP Account Unit.
6. In Login DN on the LDAP account unit's General tab, use the same login DN that was created when the LDAP server was installed. The DN is case-sensitive.

340, Check Point Security Administration NGX I Student Handbook

---

QUESTION 11:

Which of the following is the final step in an NGXbackup?

A. Test restoration in a non-production environment, using the upgrade_import command
B. Move the *.tgz file to another location
C. Run the upgrade_export command
D. Copy the conf directory to another location
E. Run the cpstop command

Answer: B

Explanation:

In a production environment, copy this file to a safe off-site archive, and destroy the original.

427, Check Point Security Administration NGX I Student Handbook

---

QUESTION 12:

Gail is the security administrator for a marketing firm. Gail is working with the networking team, to troubleshoot user complaints regarding access to audio-streaming material from the internet. The networking team asks Gail to check the object and rule configuration settings for the perimeter Security Gateway. Which SmartConsole application should Gail use to check these objects and rules?

A. SmartView Monitor
B. SmartUpdate
C. SmartViewTracker
D. SmartDashboard
E. SmartViewStatus

Answer: A

Explanation: Smartview Status was an NG product. It looks like it is now replaced by Smartview Monitor.

QUESTION 13:

Which mechanism is used to export Check Point logs to third party applications?

A. OPSE
B. CPLogManager
C. LEA
D. SmartViewTracker
E. ELA

Answer: C
Explanation; Check Point has made an API (Application Programming Interface) available for these companies to use to communicate with Check Point's product line.The SDK (Software Development Kit) requires knowledge of the C programming language. The SDK contains software to integrate with the following interfaces:
? CVP The Content Vectoring Protocol allows antivirus solutions to talk to FireWall-1.
? UFP The URI Filtering Protocol allows Web filtering to integrate.
? LEA The Log Export API enables you to export log files to third-party log servers.
? ELA The Event Logging API allows Check Point to receive logs from third-party software.
338, Configuring Check Point NGX VPN-1/FireWall-1, Syngress, 1597490318

QUESTION 14:

In NGX, what happens if a Distinguished Name (ON) is NOT found in LADP?

A. NGX takes the common-name value from the Certificate subject, and searches the LADP account unit for a matching user id
B. NGX searches the internal database for the username
C. The Security Gateway uses the subject of the Certificate as the ON for the initial lookup
D. If the first request fails or if branches do not match, NGX tries to map the identity to the user id attribute
E. When users authenticate with valid Certificates, the Security Gateway tries to map the identities with users registered in the extemal LADP user database

Answer: D

Explanation:
Retrieving Information from a SmartDirectory (LDAP) server
When a Gateway requires user information for authentication purposes, it searches

for this information in three different places:
1 The first place that is queried is the internal users database.
2 If the specified user is not defined in this database, the Gateway queries the SmartDirectory (LDAP) servers defined in the Account Unit one at a time, and according to their priority. If for some reason the query against a specified SmartDirectory (LDAP) server fails, for instance the SmartDirectory (LDAP) connection is lost, the SmartDirectory (LDAP) server with the next highest priority is queried. If there is more than one Account Unit, the Account Units are queried concurrently. The results of the query are either taken from the first Account Unit to meet the conditions, or from all the Account Units which meet the conditions. The choice between taking the result of one Account Unit as opposed to many is a matter of Gateway configuration.
3 If the information still cannot be found, the Gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

QUESTION 15:

You are preparing to configure your VolP 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 Q931 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

QUESTION 16:

Certkiller .com 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 star 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

QUESTION 17:

When you change an implicit rule's order from "last" to "first" in Global Properties, how do you make the change effective?

A. Close SmartDashboard, and reopen it
B. Select install database from the Policy menu
C. Select save from the file menu
D. Reinstall the Security Policy
E. Run fw fetch from the Security Gateway

Answer: D

Explanation:
Reinstall policy. When you make changes to a security policy(Implicit or explicit) you have toreinstall policy.

QUESTION 18:

Which command allows you to view the contents of an NGX table?

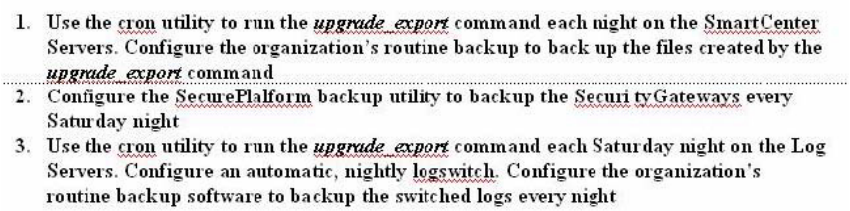
A. fw tab -s <tablename>-
B. fw tab -t <tablename>-
C. fw tab -u <tablename>-
D. fw tab -a <tablename>-
E. fw tab -x <tablename>-

Answer: B

QUESTION 19:

Jack's project is to define the backup and restore section of his organization's disaster recovery plan for his organization's distributed NGX instaliation. Jack must meet the following required and desired objectives .
* Required Objective The security policy repository must be backed up no less

frequent~ than every 24 hours
* Desired Objective The NGX components that enforce the Security Policies should be backed up no less frequently than once a week
* Desired Objective Back up NGX logs no less frequently than once a week
Jack's disaster recovery plan is as follows. See exhibit.


1. Use the cron utility to run the *upgrade_export* command each night on the SmartCenter Servers. Configure the organization's routine backup to back up the files created by the *upgrade_export* command
2. Configure the SecurePlalform backup utility to backup the SecuritGateways every Saturday night
3. Use the cron utility to run the *upgrade_export* command each Saturday night on the Log Servers. Configure an automatic, nightly logswitch. Configure the organization's routine backup software to backup the switched logs every night

Jack's plan:

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

Answer: D

Explanation: Logs can be viewed after exported.

QUESTION 20:

You want to upgrade a cluster with two members to VPN-1 NGK 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

QUESTION 21:

Certkiller needs to back up the routing, interface, and DNS configuration information from her NGX SecurePlatform Pro Security Gateway. Which backup-and-restore solution do you recommend for Certkiller?

A. Database Revision Control
B. Manual copies of the $FWDIR/conf directory
C. upgrade_export and upgrade_import commands
D. SecurePlatformbackup utilities
E. Policy Package management

Answer: D
Upgrade_export and Upgrade_import do NOT
backup/restore routing/dns information. This must be backed up using
the Secureplatform utils.
http://updates.checkpoint.com/fileserver/ID/5516/FILE/CheckPoint_NGX_SecurePlatform_SecurePlatformPro
_

QUESTION 22:

The following is cphaprobstate command output from a New Mode High Availability cluster member:

Cluster Mode: New High Availability <Active Up>

Number	*Unique IP Addresses*	*Assigned Load*	*State*
1 <local>	*192.168.1.1*	*0%*	*down*
2	*192.168.1.2*	*100%*	*active*

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

QUESTION 23:

What do you use to view an NGX Security Gateway's status, including CPU use, amount of virtual memory, percent of free hard-disk space, and version?

A. SmartLSM
B. SmartViewTracker
C. SmartUpdate
D. SmartViewMonitor
E. SmartViewStatus

Answer: D

QUESTION 24:

Which of the following commands is used to restore NGX configuration information?

A. cpcontig
B. cpinfo-i
C. restore
D. fwm dbimport
E. upgrade_import

Answer: E

QUESTION 25:

Eric wants to see all URLs' ful destination path in the SmartView Tracker logs, not just the fully qualified domain name of the web servers. For Example, the information field of a log entry displays the URL http://hp.msn.com/css/home/hpcl1012.css. How can Eric best customize SmartView Tracker to see the logs he wants? Configure the URl resource, and select

A. "transparent" asthe connection method
B. "tunneling"as the connection method
C. "optimize URL logging"; use the URI resource in the rule, with action "accept"
D. "Enforce URI capability"; use the URI resource in the rule,with action "accept"

Answer: C

QUESTION 26:

Which of the following commands shows full synchronizalion status?

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

Answer: C

QUESTION 27:

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

A. Opens a new window with a previously saved log file
B. Purges the current log file, and starts a new log file
C. Purges the current log, and prompts you for the new log's mode
D. Saves the current log file, names the log file by date and time, and starts a new log file
E. Prompts you to enter a filename, then saves the log file

Answer: D

QUESTION 28:

The following is cphaprob state command output from a ClusterXL New mode High Availability member

Cluster Mode: New High Availability <Active Up>

Number	*Unique IP Addresses*	*Assigned Load*	*State*
1 <local>	*192.168.1.1*	*0%*	*standby*
2	*192.168.1.2*	*100%*	*active*

When member 192.168.1.2 fails over and restarts, which member will become actrve?

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

Answer: B

QUESTION 29:

Select the correct statement about Secure Internal Communications (SIC) Certificates? SIC Certificates:

A. for the SmartCenter Server are created during the SmartCenter Server configuration
B. decrease network security by securing administrative communication among the SmartCenter Servers and the Security Gateway
C. for NGX Security Gateways are created during the SmartCenter Server installation
D. uniquely identify Check Point enabled machines; they have the same function as VPN Certificates
E. are used for securing internal network communications between the SmartView Tracker and an OPSEC device

Answer: D

Explanation: Uniquely identify checkpoint enabled machines: they have the same function as authentication certificates

---

QUESTION 30:

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

A. Star
B. Mesh

C. Remote Access
D. Map

Answer: A

QUESTION 31:

How does ClusterXL Unicast mode handle new traffic?

A. The pivot machine receives and inspects all new packets, and synchronizes the connections with other members
B. Only the pivot machine receives all packets. It runs an algorithm to determine which member should process the packets
C. All members receive all packets. The SmartCenter Server decides which member will process the packets. Other members simply drop the packets
D. All cluster members process all packets, and members synchronize with each other

Answer: B

QUESTION 32:

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

A. Secure lnternal Cornrnunicalions(SIC)
B. VPN tunneling
C. Overlapping VPN Domains
D. NGX connectivity
E. VPN Load Balancing

Answer: D

QUESTION 33:

How can you reset the password of the Security Administrator, which was created during initial installation of the SmartCenter Server on SecurePlattform?

A. Launch cpcontig and select "Administrators"
B. Launch SmartDashboard, click the admin user account, and overwrite the existing Check Point Password
C. Type cpm -a, and provide the existing administration account name. Reset the Security Administrator's password
D. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the "Password" portion of the file Then log in to the account withthout password. You will be prompted to assign a new password
E. Launch cpconfig and delete the Administrator's account. Recreate the account with the same name

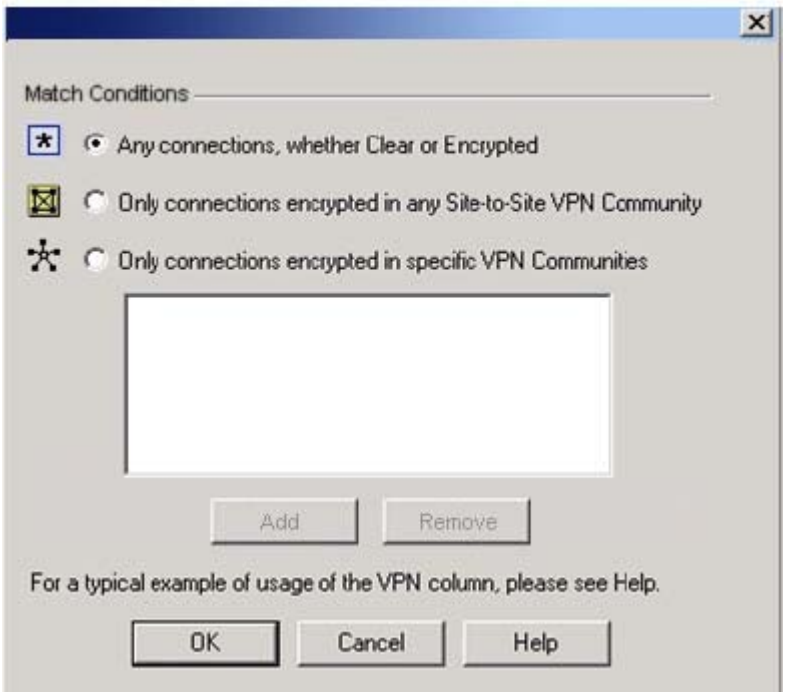
Answer: E

Explanation:
We have validated that Administrator account created during initial installation can not be managed by SmartDashboard.

This is the account we have created during installation.
The only way you can reset the password following instruction on answer E.

QUESTION 34:

Dr Bill 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 Dr Bill sees the following screen. What is the problem?



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

Answer: C
Reference: VPN.pdf page 145

QUESTION 35:

Assume an intruder has compromised your current lKE 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

QUESTION 36:

Ben is the security administrator for a university. Ben configured and installed a new Security Policy this morning. An hour after installing the new security policy. Ben began receiving complaints that internet access was very slow. Ben called his internet Server Provider , who asked Ben how much virtual memory his Security Gateway had. Which SmartConsole application should Ben Use to answer this question?

A. SmartViewTracker
B. SmartLSM
C. SmartUpdate
D. SmartView Monitor
E. SmartView Status

Answer: D

QUESTION 37:

Which operating system is not supported byVPN-1 SecureClient?

A. IPS0 3.9
B. Windows XP SP2
C. Windows 2000 Professional
D. RedHat Linux 7 0
E. MacOS X

Answer: A

QUESTION 38:

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

A. Guarantees
B. Differentiated Services
C. Limits
D. Weighted Fair Queueing
E. Low Latency Queueinq

Answer: D

QUESTION 39:

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

A. Turn "per rule guarantees" into "per connection guarantees"
B. Install Check Point QoS only on the external interfaces of the QoS Module
C. Put the most frequently used rules at the bottom of the QoS Rule Base
D. Turn "per rule limits" into "per connection limits
E. Define weights in the Default Rule in multiples of 10

Answer: B

Explanation: On page 402 of the NGX II 1.1 book the second bullet states, "...will provide you the most functionality and improvements."

QUESTION 40:

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. On~ the patch utility is upgraded using this command
E. Only the OS

Answer: B

QUESTION 41:

Frank wants to know why users on the corporate network cannot receive multicast transmissions from the Internet. An NGX Security Gateway protects the corporate network fromt he Internet Which of the following is a possible cause for the connection problem?

A. NGX does not support multicast routing protocols and streaming media through the Security Gateway
B. Frank did not install the necessary multicast license with SmartUpdate, when he upgraded to NGX
C. The Multicast Rule is below the Stealth Rule. NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule
D. Multicast restrictions are not configured properly on the corporate internal network interface properties of the Security Gateway object
E. Anti-spoofing is enabled. NGX cannot pass multicast traffic, if a nti-spoofing is enabled

Answer: D
Not D: NGX doesn't support multicast? That's quite obviously not true.
http://www.checkpoint.com/ngx/upgrade/top10.html

QUESTION 42:

John is the Security Administrator for a public hospital. New health-care legislation requires logging for all traffic accepted through the perimeter Security Gateway. What must John do, to ensure implied rules meet the new requirement?

A. Use the "Implicit Rules" predefined query in SmartView Tracker
B. Install the "View Implicit Rules" package using SmartUpdate
C. Check the "Log Implied Rules Globally box on the NGX Gateway object
D. Set the position of all implicit rules to "Before Last"
E. Check the "Log Implied Rules" box in Global Properties

Answer: E
Check the "Log Implied Rules" Box in Global Properties. Definetally the answer Go to Global Properties\Firewall-1\Track(At the botom of the screeen)Tick Implied Rules

---

QUESTION 43:

Your primary SmartCenter Server is installed on a SecurePlatform Pro Machine,

which is also a VPN-1 Pro Gateway. You want to implement a 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 (change 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: Based on deploying a management HA, it has to be in a distributed environment so it seems answer "A" would be the answer.

QUESTION 44:

Amanda is compiling traffic statistics for Certkiller .com's Internet activity during production hours. How could she use SmartView Monitor to find this information? By

A. using the "Traffic Counters" settings and SmartView Monitor to generate a graph showing the total HTTP traffic for the day
B. -monitoring each specific user's Web traffic use.
C. Viewing total packets passed through the Security Gateway
D. selecting the "Tunnels" view, and generating a report on the statistics
E. configuring a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway

Answer: A

QUESTION 45:

ASecurity Administrator is notified that some long-lasting Telnet connections to a mainframe are dropped every time after an hour. The Administrator suspect that the the Security Gateway might be blocking these connections. As she reviews the Smart Tracker the Administrator sees the packet is dropped with the error "Unknown established connection". How can she resolve this problem without causing other security issues?
Choose the BEST answer. She can:

A. increase the session time-out in the mainframe's Object Properties
B. create a new TCP service object on port 23, and increase the session time-out for this

object She only uses this new object in the rule that allows the Telnet connections to the mainframe
C. increase the session time-out in the Service Properties of the Telnet service
D. increase the session time-out in the Global Properties
E. ask the mainframe users to reconnect every time this error occurs

Answer: B
Explanation; It is better to change the "Session Timeout" for a specific service than to set it globally for ALL Services.
Checkpoint KBase:
To specify a timeout for a TCP servce that is different from the global TCP timeout (defined in the Stateful Inspection page of the Global Properties window), proceed as follows:
1. Open the TCP Service Properties window for the specific service.
2. Click "Advanced".
3. In the Advanced TCP Service Properties window, select "Other".
4. Specify the timeout.
5. Install the policy.

QUESTION 46:

Your users are defined in a Windows 2000 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in NGX?

A. All Users
B. A group with generic' user
C. External-user group
D. LDAP account-unit group
E. LDAP group

Answer: E

QUESTION 47:

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. Reinstallt he 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

QUESTION 48:

Jordan's company is streaming training videos provided by a third party on the internet. Jordan configures NGX, so that each department only views Webcasts specific to its department. Jordan created and configured the multicast groups for all interfaces, and configures them to "Drop all multicast packets expect those whose destination is in the list". However, no multicast transmissions are coming from the internet. What is a possible cause for the connection problem?

A. The Multicast Rule is below the Stealth Rule. NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule
B. Jordan did not create the necessary "to and through" rules, defining how NGX will handle the multicast traffic
C. Multicast groups are configured improper~ on the external interface properties of the Security Gateway object
D. Anti-spoofing is enabled. NGX cannot pass multicast traffic, if anti-spoofing is enabled
E. NGX does not support multicast routing protocols and streaming media through the Security Gateway

Answer: C
Not E: NGX doesn't support multicast? That's quite obviously not true.
http://www.checkpoint.com/ngx/upgrade/top10.html

QUESTION 49:

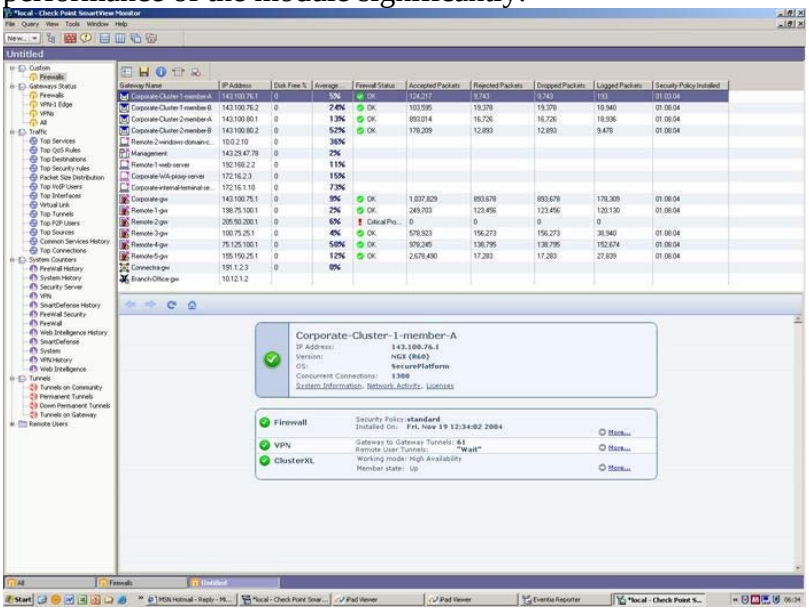
Which NGX component displays the number of packets accepted, rejected, and dropped on a specific Security Gateway, in real time?

A. Reporting Module
B. Eventia Reporter
C. SmartUpdate
D. SmartView Status
E. SmartView Monitor

Answer: E

Explanation:

The SmartView Monitor enables network administrators to monitor Check Point System Counters, traffic on an interface and QoS in real-time. Additionally it is able to create reports on past activities. In Report mode, reports can be made for Check Point System Counters as well as for traffic on an interface.
When you decide to create traffic history reports in the SmartView Monitor, the reports creation process may affect the performance of the module. If you do not intend to use create traffic history reports, you should disable the Traffic options on this page. Other types of reports (such as Check Point System Counter reports) do not affect the performance of the module significantly.



QUESTION 50:

Certkiller .com has many VPN-1 Edge Gateways at various branch offices, t allow VPN-1 SecureClient users to access company resources. For security reasons, Certkiller .com'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 continue 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 otherVPN targets

Answer: D

QUESTION 51:

Certkiller is the Security Administrator for a software-development company. To isolate the corporate network from the developer's network, Certkiller installs an

internal Security Gateway. Jack wants to optimize the performance of this Gateway. Which of the following actions is most likely to improve the Gateway's performance?

A. Remove unused Security Policies from Policy Packages
B. Clear all Global Properties check boxes, and use explicit rules
C. Use groups within groups in the manual NAT Rule Base
D. Put the least-used rules at the top of the Rule Base
E. Use domain objects in rules, where possible

Answer: A

QUESTION 52:

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

QUESTION 53:

Which of these changes to a Security Policy optimizes Security Gate way performance?

A. Using domain objects in rules When possible
B. Using groups within groups in the manual NAT Rule Base
C. Pulling the least-used rule at the top of the Rule Base

D. Logging rules as much as possible
E. Removing old or unused Security Policies from Policy Packages

Answer: E

QUESTION 54:

Certkiller is the Security Administrator for a chain of grocery stores. Each grocery store is protected by a Security Gateway. Certkiller is generating a report for the information-technology audit department. The report must include the name of the Security Policy installed on each remote Security Gateway, the date and time the Security Policy was installed, and general performance statistics (CPU Use, average CPU time, active real memory, etc.).
Which SmartConsole application should Certkiller use to gather this information?

A. SmartUpdate
B. SmartView Status
C. SmartView Tracker
D. SmartLSM
E. SmartView Monitor

Answer: E

QUESTION 55:

You are trying to enter a new user, group, or organizational unit on an LDAP server, and you encounter the error "violates schema". To provide the BEST long-term security, you should

A. Import the schema, and enable schema checking
B. Turn off schema checking, and restart the LDAP server
C. Turn off schema checking, and restart the SmartCenter Server
D. Restart the server
E. Recover the corrupt database

Answer: A

QUESTION 56:

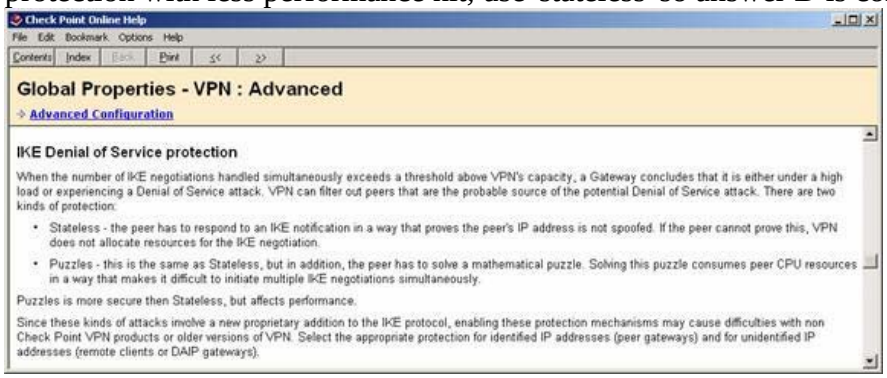
Certkiller is concerned that a denial-of-service (DoS) attack may affect his VPN Communities. Mrs. Bill decides to implement IKE DoS protection. Jack needs to minimize the performance impact of implementing this new protection.
Which of the following configurations is MOST appropriate for Certkiller?

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: C

Explanation:
From the online HELP for NGX R60, (see screen capture below)
The options for DOS on IKE for both identified and unidentified connections are...
Puzzles - best protection, but performance intensive
Stateless - less protection, but not as performance intensive
None - no protection for DOS on IKE
Therefore, answer C will have impact on "unidentified" IKE connections. To provide protection with less performance hit, use 'stateless' so answer D is correct, not C.



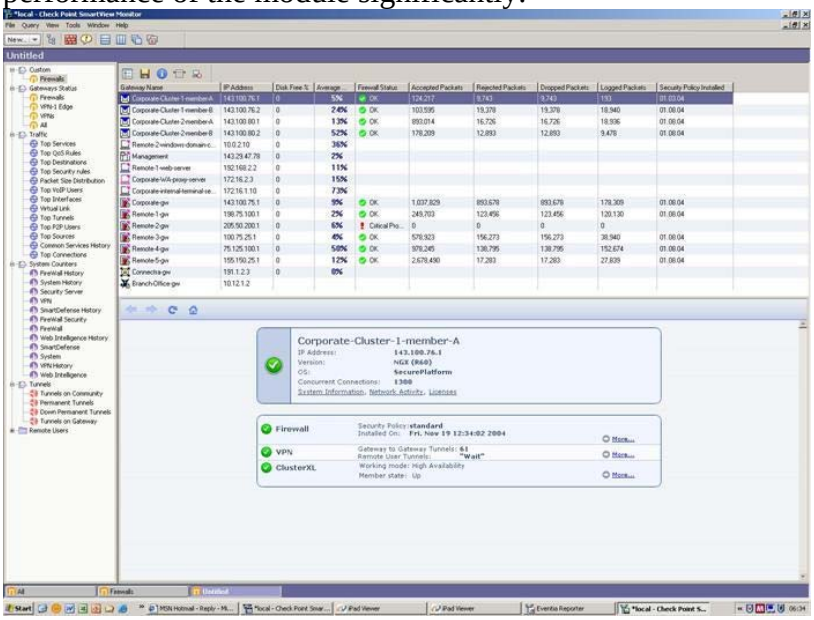
QUESTION 57:

Certkiller is the security Administrator for Certkiller .com with a large call center. The management team in the center is concerned that employees may be installing and attempting to use peer-to-peer file-sharing utilities, during their lunch breaks. The call center's network is protected by an internal Security Gateway, which is configured to drop peer-to-peer file-sharing traffic.
Which application should Jack use, to determine the number of packets dropped by each Gateway?

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

Answer: B

Explanation:
The SmartView Monitor enables network administrators to monitor Check Point System Counters, traffic on an interface and QoS in real-time. Additionally it is able to create reports on past activities. In Report mode, reports can be made for Check Point System Counters as well as for traffic on an interface.
When you decide to create traffic history reports in the SmartView Monitor, the reports creation process may affect the performance of the module. If you do not intend to use create traffic history reports, you should disable the Traffic options on this page. Other types of reports (such as Check Point System Counter reports) do not affect the performance of the module significantly.



QUESTION 58:

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 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

QUESTION 59:

You work as an administrator at Certkiller .com. 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 are allowed in the Action properties. If traffic passing through the QoS Module matches both rules, which of the following statement is true?

A. Neither rule will be allocated more than 10% of available bandwidth
B. The H.323 rulel will consume no more than 2048 Kbps of available bandwidth
C. 50% of available bandwidth will be allocated to the H.323 rule
D. 50% 01 available bandwidth will be allocated to the Default Rule
E. Each H.323 connection will receive at least 512 Kbps of bandwidth

Answer: B

QUESTION 60:

How can you reset Secure Internal Communications (SIC) between a SmartCenter Server and Security Gateway?

A. Run the command fwm sic_reset to reinitialize the Internal Certificate Authority (ICA) of the SmartCenter Server. Then retype the activation key on the Security-Gateway from SmartDashboard
B. From cpconfig on the SmartCenter Server, choose the Secure Internal Communication option and retype the actrvation key Next, retype the same key in the gateway object in SmartDashboard and reinitialize Secure Internal Communications (SIC)
C. From the SmartCenter Server's command line type fw putkey -p <shared key>- <IP Address of SmartCenter Server>-.
D. From the SmartCenter Server's command line type fw putkey -p <shared key>- <IP Address of security Gateway>-.
E. Re-install the Security Gateway

Answer: B

QUESTION 61:

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

A. The remote Gateway's IP address has changed, which invalidates the SIC Certificate
B. The Security Gateway is NG with Application Intelligence, and the SmartCenter Server is NGX

C. The Internal Certfcate Authorty for the SmartCenter object has been removed from objects_5_0 c
D. The time on the SmartCenter Server's clock has changed, which invalidates the remote Gateway's Certificate
E. There is no connection between the SmartCenter Server and the remote Gateway. Rules or routing may block the connection

Answer: E

QUESTION 62:

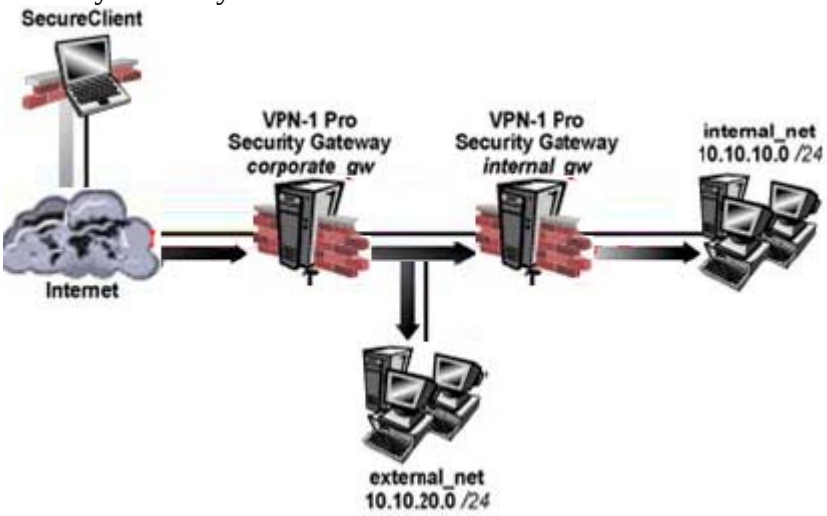
Which NGX feature or command allows Security Administrators to revert to earlier versions of the Security Policy without changing object configurations?

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

Answer: B

QUESTION 63:

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 GatewayVPN Domain = Internal_net
External Gateway VPN Domain = external_net + internal gateway object
C. Internal GatewayVPN Domain = Internal_net
External Gateway VPN Domain = internal_net + external_net

D. Internal GatewayVPN Domain = Internal_net
External Gateway VPN Domain = internal VPN Domain + internal gateway object + external_net

Answer: D

Explanation:
For the remote-access client to make it through to the internal-net, he must first connect to the corporate_gw. From there, he must route and have access to talk with the internal_gw or he will never get into the internal net. Answer A does not include the internal_gw in the "external vpn domain", so the connection would never make it in! Just like the "internal gateway vpn domain" does NOT include the gateway protecting it, the "external gateway vpn domain" doe not need the corporate_gw either.

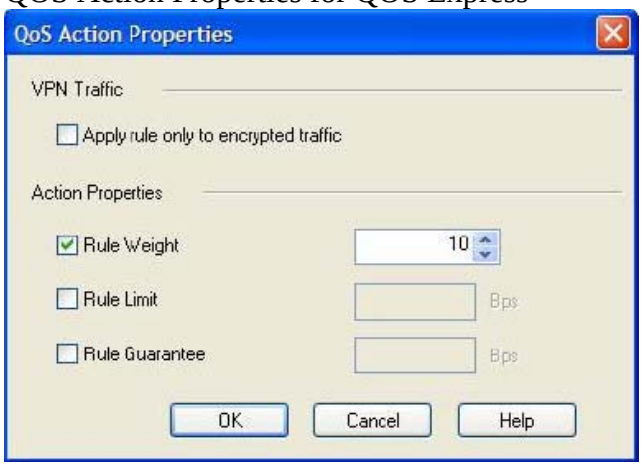
QUESTION 64:

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

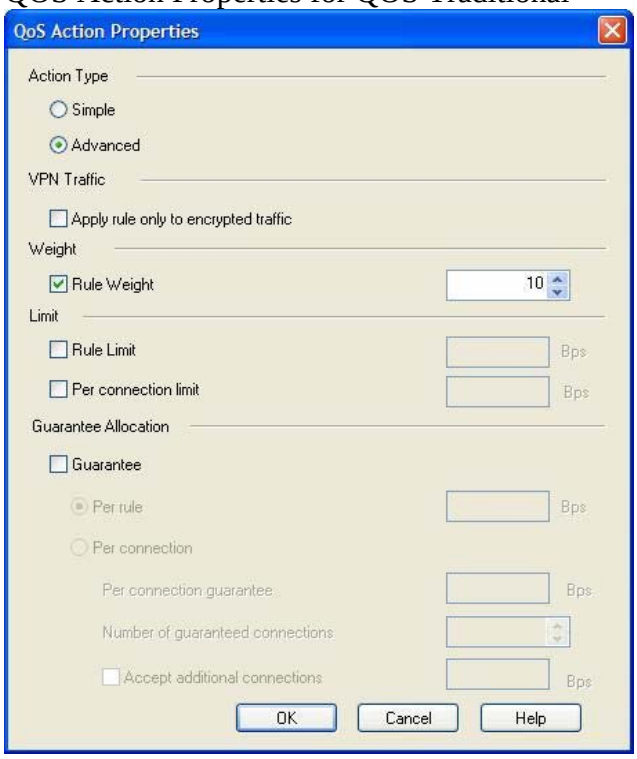
A. Guarantee Allocation
B. Rule weight
C. Apply rule only to encrypted traffic
D. Rule limit
E. Rule guarantee

Answer: A

Explanation:
Create a new policy package and compare.
QOS Action Properties for QOS Express



QOS Action Properties for QOS Traditional



QUESTION 65:

Certkiller is the Security Administrator for Certkiller .com's large geographically distributed network. The internet connection at one of her remote sites failed during the weekend, and the Security Gateway logged locally for over 48 hours. Certkiller is concerned that the logs may have consumed most of the free space on the Gateway's hard disk.
Which SmartConsole application should Certkiller use, to view the percent of free hard-disk space on the remote Security Gateway?

A. SmartView Status
B. SmartView Tracker
C. SmartUpdate
D. SmartView Monitor
E. SmartLSM

Answer: D

QUESTION 66:

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

A. Open the Rule Menu, and select Hide and view hidden rules Select the rule, right-click, and select Disable

B. Uninstall the Security Policy, and then disable the rule
C. When a rule is hidden, it is automatically disabled. You do not need to disable the rule again
D. Run cpstop and cpstart on the SmartCenter Server, then disable the rule
E. Clear Hide from Rules drop-down menu, then right-click and select "Disable Rule (s)"

Answer: E

Explanation:
Not A: A will only let you see the hidden rules but rules are still in hidden state. So it will not let you disable.

QUESTION 67:

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

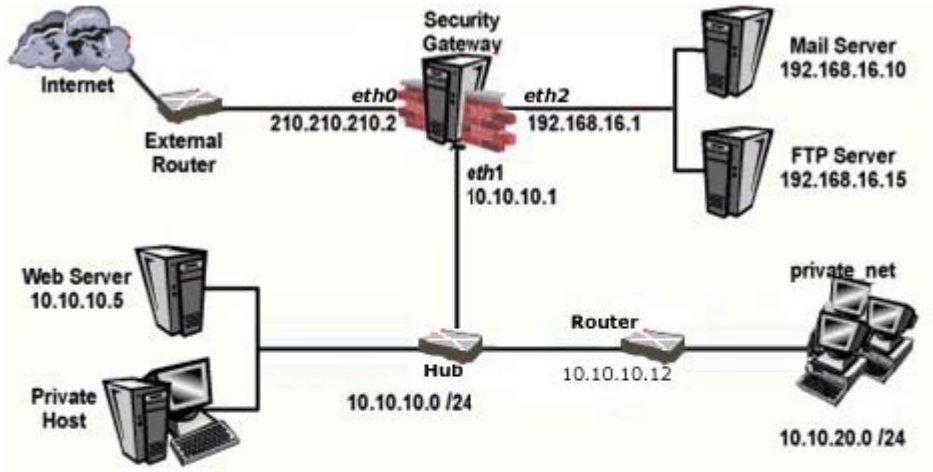
A. Low latency class
B. DiffServ rule
C. guaranteed per connection
D. Weighted Fair queuing
E. guaranteed per VolP rule

Answer: A

Explanation:
In Check Points PDF CheckPoint_R61_QoS_UserGuide.pdf, on page 95, paragraph 4 it says "FloodGate-1 Low Latency Queuing makes it possible to define special Classes of Service for "delay sensitive" applications like voice and video."
This we believe indicates that Low Latency Classes is the best option.

QUESTION 68:

As a Security Administrator, you must configure anti-spoofing on Security Gateway interfaces, to protect your Internal networks. What is the correct anti-spoofing setting on interface ETH1 in this network diagram?



NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		internal-networks	Any	Any Traffic	Any	accept	Log
2		Any	Corporate-mail-server Corporate-dns-ext	Any Traffic	TCP smtp dns	accept	Log
3		Any	Any	Any Traffic	Any	drop	Log

NOTE In the DMZ, mail server 192.168.16.10 is statically translated to the object "mail_valid", with IP address 210.210.210.3. The FTP server 192.168.16.15 is statically translated to the object "flp_valid", with IP address 210.210.210.5

A. A group object that includes the 10.10.0.0/16 and 192.168.16.0/24 networks, and mail_valid and ftp_valid host objects
B. A group object that includes the 10.10.20.0/24 and 10.10.10.0/24networks
C. A group object that includes the 10.10.0.0/16 network object, mail_valid host,and ftp_valid host object
D. A group object that includes the 192.168.16.0/24 and 10.10 0.0/16 networks
E. A group object that includes the 10.10.10.0/24 and 192.168.16.0/24networks

Answer: B

QUESTION 69:

Mary is recently hired as the Security Administrator for a public relations company. Mary's manager has asked her to investigate ways to improve the performance of the firm's perimeter Security Gateway. Mary must propose a plan based on the following required and desired results
Required Result #1: Do not purchase new hardware
Required Result #2: Use configuration changes that do not reduce security
Desired Result #1: Reduce the number of explicit rules in the Rule Base
Desired Result #2: Reduce the volume of logs
Desired Result #3: Improve the Gateway's performance
Proposed Solution:
Mary recommends the following changes to the Gateway's configuration:
1. Replace all domain objects with network and group objects.

2. Stop logging Domain Name over UDP (queries)
3. Use Global Properties, instead of explicit rules, to control ICMP. VRRP, and RIP.
Does Mary's proposed solution meet the required and desired result s?

A. The solution meets the required results, and two of the desired results
B. The solution does not meet the required results
C. The solution meets all required results, and none of the desired results
D. The solution meets all required and desired results
E. The solution meets the required results, and one of the desired results

Answer: A

QUESTION 70:

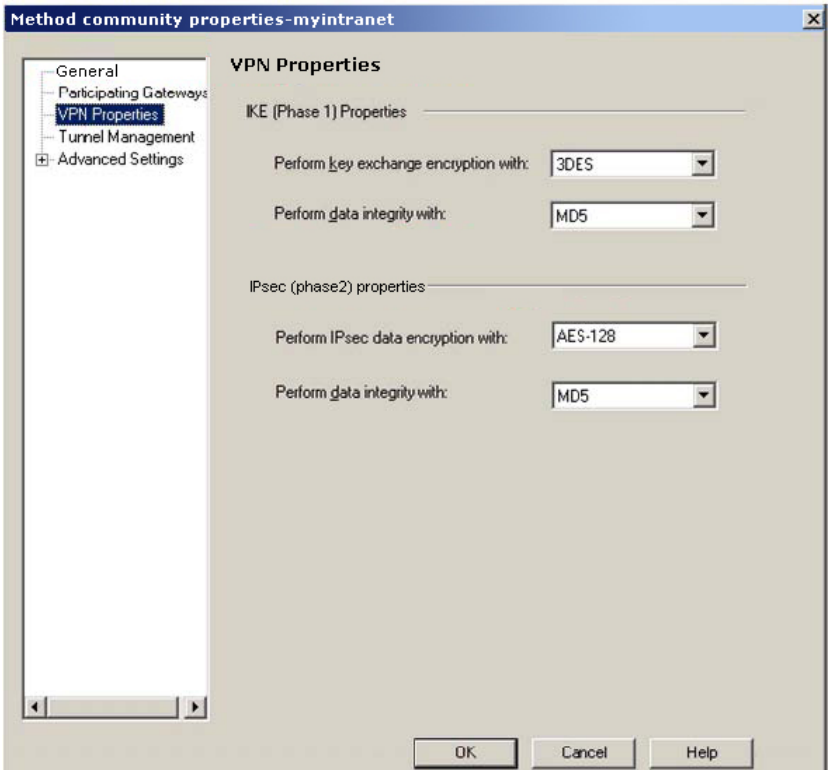
What is a Consolidation Policy?

A. The collective name of the Security Policy, Address Translation, and SmartDefense Policies
B. The specific Policy used by Eventia Reporter to configure log-management practices
C. The state of the Policy once installed on a Security Gateway
D. A Policy created by Eventia Reporter to generate logs
E. The collective name of the logs generated by Eventia Reporter

Answer: B

QUESTION 71:

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
Exbibit:



Which of the following statements isTRUE?

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's VPN Community will perform IKE Phase 1 key-exchanqe encryption, usinq the lonqest key VPN-1 NGX supports
C. Jacob must change the data-integrity settings for this VPN Community. MD5 is incompatible with AES
D. If Jacob changes the setting "Perform IPsec data encryption With" from "AES-128" to "3DES", he will increase the encryption overhead

Answer: D

QUESTION 72:

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
fwtab -t connections - s output from both members:

MEMBER A:

HOST	NAME	ID	#VALS	#PEAK	#SLINKS
Localhost	connections	8158	1553	1560	800

MEMBER B:

HOST	NAME	ID	#VALS	#PEAK	#SLINKS
Localhost	connections	8158	800	1001	800

Is State Synchronization working properly between the two members?

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 #SLlNKS 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:
Debugging State Synchronization
To monitor the synchronization mechanism on ClusterXL or third-party OPSEC certified clustering products, run the following commands on a cluster member.
FW TAB -T CONNECTIONS - S
One quick test to verify if State Synchronization is working properly is by running the fw tab -t connections -s command from cluster members. If the #VALS numbers are very close between cluster members, cluster members are synchronizing properly.
Here is a sample output of fw tab -t connections -s:
HOST NAME ID #VALS #PEAK #SLINKS
localhost connections 8158 4 22 4
If the #VALS numbers are very close between cluster members, it is safe to say State Synchronization is working properly.

The key line is "If the #VALS numbers are very close between cluster members, it is safe to say State Synchronization is working properly."
Reference.
http://www.checkpoint.com/services/education/training/samples/ClusterXL_Sample_Chapter.pdf

---

QUESTION 73:

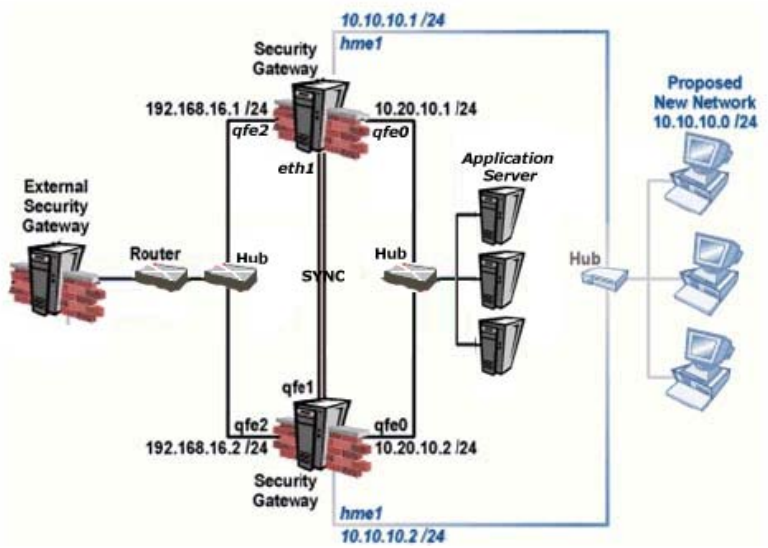
Which Check Point QoS feature marks the Type of Service (ToS) byte in the IP header?

A. Guarantees
B. Low Latency Oueuing
C. Differentiated Services
D. Weighted FairOueueing
E. Limits

Answer: C

QUESTION 74:

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 lP 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 technology 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. Reenable "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 spstart 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 on both membes.
3. Install the Security Policy.

Answer: C

Explanation: It looks like Solaris OStherefore should be ifconfig command not sysconfig.

QUESTION 75:

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 reenable 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

QUESTION 76:

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

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

Answer: B

QUESTION 77:

You have locked yourself out of SmartDashboard With the rules you just installed on your stand alone Security Gateway. Now you cannot access the SmartCenter Server or any SmartConsole tools via SmartDashboard. How can you reconnect to SmartDashboard?

A. Run cpstop on the SmartCenter Server
B. Run fw unlocklocal on the SmartCenter Server
C. Run fw unloadlocal on the Security Gateway
D. Delete the $fwdir/database/manage.lock file and run cprestart.
E. Run fw uninstall localhost on the Security Gateway

Answer: C

QUESTION 78:

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

QUESTION 79:

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
Reference: R60 CheckPointQoS.pdf page 94

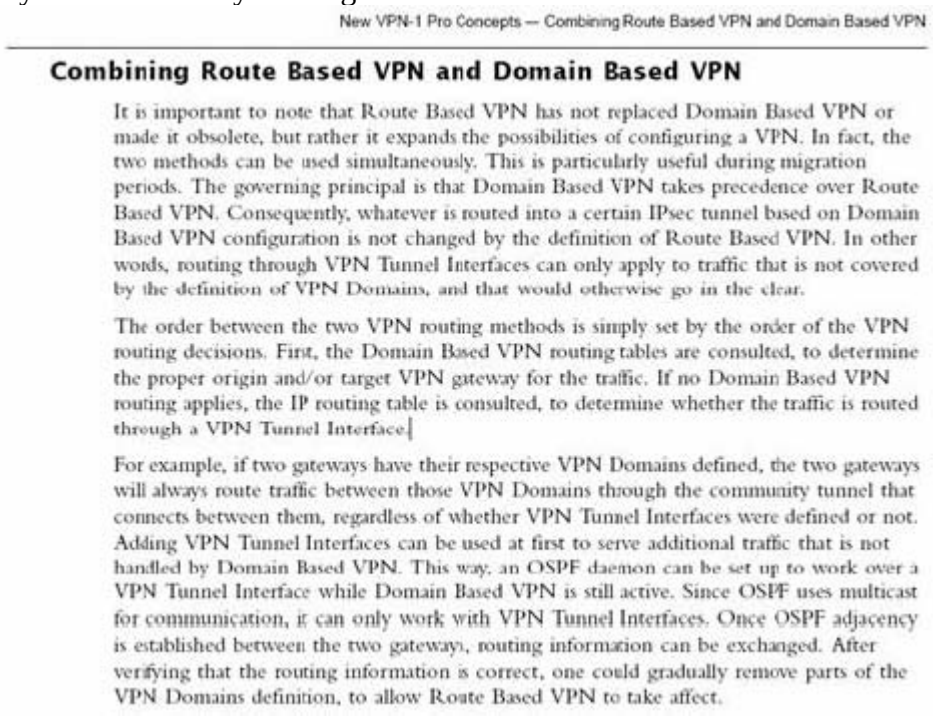
QUESTION 80:

Your VPN Community includes three Security Gateways. Each Gateway has its own intemal 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 anew 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 anew 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.Add static routes on three Gateways, to route the new network to each peer's VTI interface
C.
1.Add anew interface on each gateway
2.Add the newly added network into the exsiting 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.
D.
1.Add anew interface on each gateway
2.Add the newly added network into the exsiting VPN Domain for each Gateway.
3.Create VTIs on each Gateway, 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

Answer: B

Explanation:
In the VPN NGX (R60) Route Based VPN Deployments Documentation (August 30,2005) on page 7 it states that
"The order between the two VPN routing methods is simply set by the order of the VPN routing decisions. First, the Domain Based VPN routing tables are consulted, to determine the proper origin and/or target VPN gateway for the traffic. If no Domain Based VPN routing applies, the IP routing table is consulted, to determine whether the traffic is routed through a VPN Tunnel Interface." (see screen print below)
For this reason, you must 'remove' the new network from the VPN domain or you will never be able to 'test' the route-based VPN feature. Secondly, you must add the static routes, (enabling advanced routing is only for dynamic routing) Therefore, answer C is incorrect and answer B is the correct answer.
Note: This assumes as the question states that the "newly added network" does not have any VPN's currently running on it. VPN's not on this network will continue to run.



QUESTION 81:

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 few 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 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: C

Explanation: Without installing the policy the new setting will not be applied.
BTW it is not necessary/useful to change to traditional mode configuration.

QUESTION 82:

Certkiller is recently hired as the Security Administrator for Certkiller .com. Jack Bill's manager has asked her to investigate ways to improve the performance of the firm's perimeter Security Gateway. Certkiller must propose a plan based on the following required and desired results:
Required Result #1: Do not purchase new hardware.
Required Result #2: Use configuration changes the do not reduce security.
Desired Result #1: Reduce the number of explicit rules in the Rule Base.
Desired Result #2: Reduce the volume of logs.
Desired Result #3: Improve the Gateway's performance.
Proposed solution:
* Replace all domain objects with network and group objects.
* Check "Log implied rules" and "Accept ICMP requests" in Global Properties.
* Use Global Properties, instead of explicit rules, to control ICMP, VRRP, and RIP.
Does Certkiller's proposed solution meet the required and desired results?

A. The solution meets all required and desired results.
B. The solution meets all required, and one of the desired results.
C. The solution meets all required, and two of the desired results.
D. The solution meets all required, and none of the desired results.

E. The solution does not meet the required results.

Answer: E