Exam : 156-315
Check Point Security Administration NGX II

Demo Version

To Access Full Version, Please go to

www.itexamworld.com

QUESTION 1:

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

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

Answer: D

Explanation: Bandwidth Allocation and Rules A rule can specify three factors to be applied to bandwidth allocation for classified connections: Weight Weight is the relative portion of the available bandwidth that is allocated to a rule. To calculate what portion of the bandwidth the connections matched to a rule receive, use the following formula: thisrule's portion = this rule's weight / total weight of all rules with open connections For example, if this rule's weight is 12 and the total weight of all the rules under which connections are currently open is 120, then all the connections open under this rule are allocated 12/120 (or 10%) of the available bandwidth. In practice, a rule may get more than the bandwidth allocated by this formula, if other rules are not using their maximum allocated bandwidth. Unless a per connection limit or guarantee is defined for a rule, all connections under a rule receive equal weight. Allocating bandwidth according to weights ensures full utilization of the line even if a specific class is not using all of its bandwidth. In such a case, the left over bandwidth is divided among the remaining classes in accordance with their relative weights. Units are configurable, see "Defining QoS Global Properties" on page 94. Default Rule Chapter 4 Basic QoS Policy Management 35 Guarantees A guarantee allocates a minimum bandwidth to the connections matched with a rule. Guarantees can be defined for: the sum of all connections within a rule A total rule guarantee reserves a minimum bandwidth for all the connections under a rule combined. The actual bandwidth allocated to each connection depends on the number of open connections that match the rule. The total bandwidth allocated to the rule can be no less than the guarantee, but the more connections that are open, the less bandwidth each one receives. individual connections within a rule A per connection guarantee means that each connection that matches the particular rule is guaranteed a minimum bandwidth. Although weights do in fact guarantee the bandwidth share for specific connections, only a guarantee allows you to specify an absolute bandwidth value. Limits A limit specifies the maximum bandwidth that is assigned to all the connections together. A limit defines a point beyond which connections under a rule are not allocated bandwidth, even if there is unused bandwidth available. Limits can also be defined for the sum of all connections within a rule or for individual connections within a rule.

QUESTION 2:

Which operating system is NOT supported by VPN-1 SecureClient?

A. IPSO 3.9
B. Windows XP SP2

C. Windows 2000 Professional
D. RedHat Linux 8.0
E. MacOS X

Answer: A

Explanation:
RedHat 8 is also not currently supported according to the docs, but A is the most correct answer..
http://www.checkpoint.com/products/downloads/vpn-1_clients_datasheet.pdf

QUESTION 3:

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. VNP-1 and FireWall-1
C. SecurePlatform NGX R60
D. SVN Founation
E. VPN-1 Pro/Express NGX R60 Answer: C

Explanation: SmartCenter Upgrade on SecurePlatform R54, R55 and Later Versions Upgrading to NGX R60 over a SecurePlatform operating system requires updating both operating system and software products installed. SecurePlatform users should follow the relevant SecurePlatform upgrade process. The process described in this section will result with an upgrade of all components (Operating System and software packages) in a single upgrade process. No further upgrades are required. Refer to NGX R60 SecurePlatform Guide for additional information. If a situation arises in which a revert to your previous configuration is required refer to "Revert to your Previous Deployment" on page 52 for detailed information. Using a CD ROM The following steps depict how to upgrade SecurePlatform R54 and later versions using a CD ROM drive. 1 Log into SecurePlatform (Expert mode is not necessary). 2 Apply the SecurePlatform NGX R60 upgrade package: # patch add cd. 3 At this point you will be asked to verify the MD5 checksum. 4 Answer the following question: Do you want to create a backup image for automatic revert? Yes/No If you select Yes, a Safe Upgrade will be performed. Safe Upgrade automatically takes a snapshot of the entire system so that the entire system (operating system and installed products) can be restored if something goes wrong during the Upgrade process (for example, hardware incompatibility). If the Upgrade process detects a malfunction, it will automatically revert to the Safe Upgrade image. When the Upgrade process is complete, upon reboot you will be given the option to manually choose to start the SecurePlatform operating system using the upgraded version image or using the image prior to the Upgrade process.

QUESTION 4:

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 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 the 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 the 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: C

Explanation:
Block Intruder
SmartView Tracker allows you to terminate an active connection and block further connections from and to specific IP addresses. Proceed as follows:
1Select the connection you wish to block by clicking it in the Active mode's Records pane.
2From the Tools menu, select Block Intruder.
The Block Intruder window is displayed.
3In Blocking Scope, select the connections that you would like to block:
Block all connections with the same source, destination and service - block the selected connection or any other connection with the same service, source or destination.
Block access from this source - block access from this source. Block all connections that are coming from the machine specified in the Source field.
Block access to this destination - block access to this destination. Block all connections that are headed to the machine specified in the Destination field.
4In Blocking Timeout, select one of the following:
Indefinite blocks all further access
For... minutes blocks all further access attempts for the specified number of minutes
5In Force this blocking, select one of the following:
Only on... blocks access attempts through the indicated VPN-1 Pro module.
On any VPN-1 & FireWall-1 Module blocks access attempts through all VPN-1 Pro modules defined as gateways or hosts on the Log Server.
6Click OK.

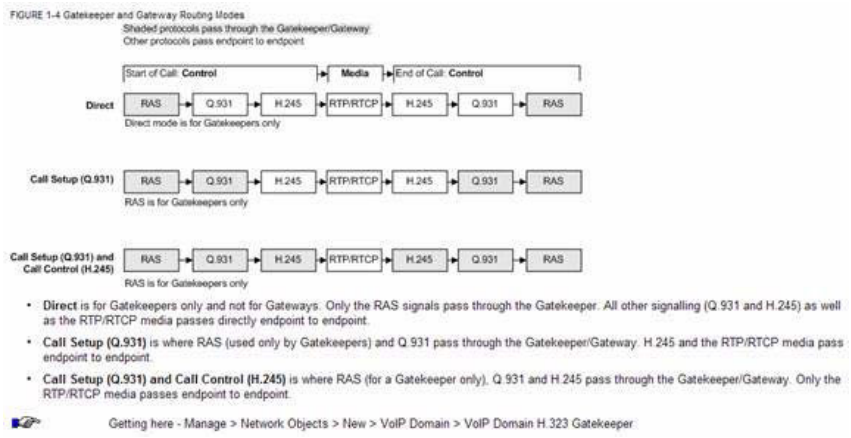
QUESTION 5:

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: From the help section:



QUESTION 6:

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

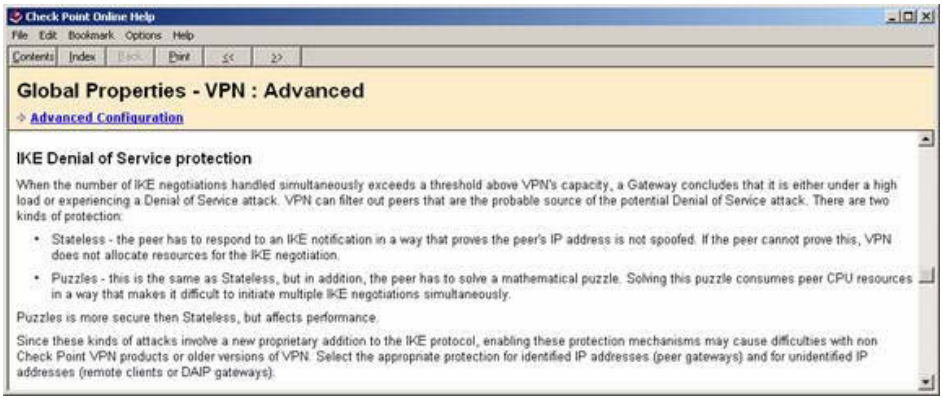
A. Set Support IKE DoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless"
B. Set Support IKE DoS protection from identified source, and Support IKE DoS protection from unidentified soruce to "Puzzles"
C. Set Support IKE DoS protection 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:
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 7:

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

A. 1. Synchronize the two SmartCenter Servers
1. 2. Upgrade the secondary SmartCenter Server.
2. 3. Upgrade the primary SmartCenter Server.
3. 4. Configure both SmartCenter Server host objects version to VPN-1 NGX
4. 5. Synchronize the Servers again.

B. 1. Synchronize the two SmartCenter Servers
1. 2. Perform an advanced upgrade the primary SmartCenter Server.
2. 3. Upgrade the secondary SmartCenter Server.
3. 4. Configure both SmartCenter Server host objects to version VPN-1 NGX.
4. 5. Synchronize the Servers again

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

D. 1. Synchronize the two SmartCenter Servers.
1. 2. Perform an advanced upgrade on the primary SmartCenter Server.
2. 3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.
3. 4. Synchronize the two servers again.
4. 5. Upgrade the secondary SmartCenter Server.
5. 6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.

6. 7. Synchronize the Servers again.

Answer: A

Explanation: Management High Availability Upgrade the Management High Availability Servers 1 Synchronize the Standby SmartCenter Servers (SCSs) with the Active SCS by selectingSynchronize in the Policy > Management High Availability window. 2 Upgrade all the SCSs in the organization. 3 Login to SmartDashboard via the Active SCS. For each Standby SCS, change the softwareversion in Check Point Products listbox of its network objects window. 4 Synchronize the Standby SCSs with the Active SCS. The synchronization status is expectedto be collision. This occurs on account of the Upgrade operation. 5 Make sure that you select the Active SCS as the dominant SCS, in order that all the Standby SCSs will be overwritten. Once again, synchronize the remaining Standby SCSs to the Active SCS. Not D: You can not sync NGX with NG.

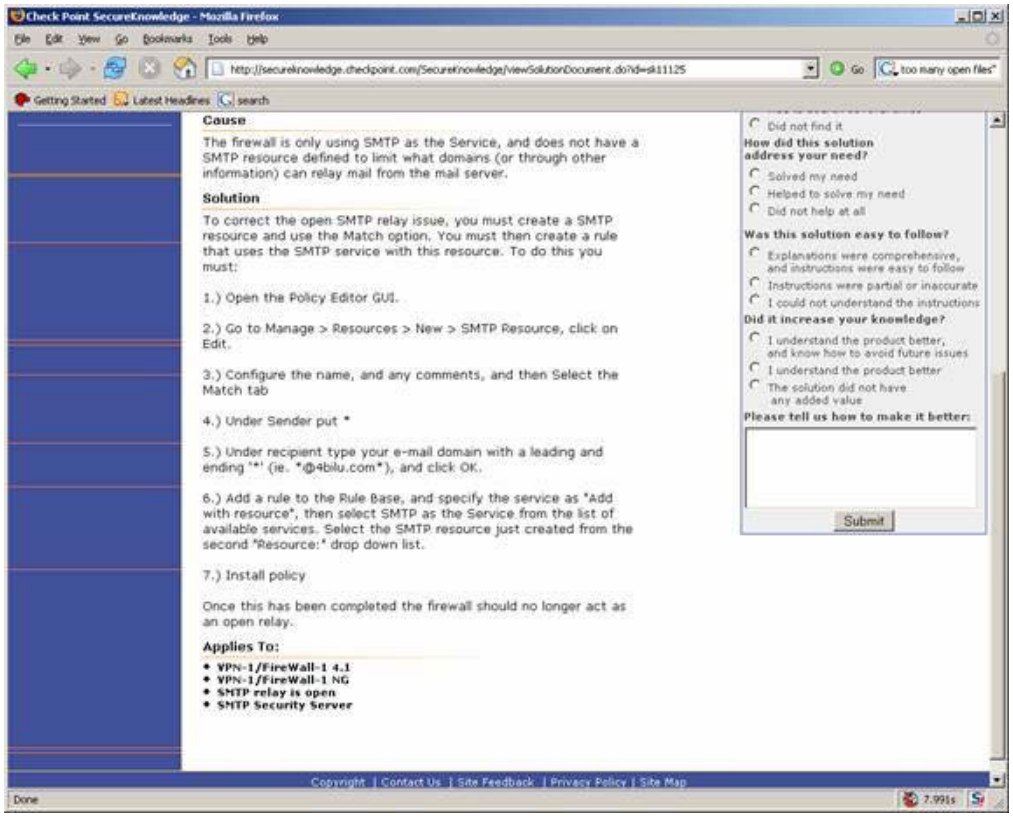
QUESTION 8:

Itexamworld is notified by blacklist.org that her site has been reported as a spam relay, due to her SMTP server being unprotected. Mrs. Bill 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 Jack's corporate domain.

Answer: E

Explanation:
The following screen shot is from the Check Point Secure knowledge base.
It states that
"To correct the open SMTP relay issue, you must create a SMTP resource and use the Match option. You must then create a rule that uses the SMTP service with this resource."
"Under recipient type your e-mail domain with a leading and ending '*' (ie. *@4bilu.com*), and click OK."
"Once this has been completed the firewall should no longer act as an open relay."
Therefore, you are using a match resource on the corporate domain, not filtering which makes the correct answer E.


Check Point SecureKnowledge - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://secureknowledge.checkpoint.com/SecureKnowledge/viewSolutionDocument.do?id=sk11125
Getting Started Latest Headlines search
Cause
The firewall is only using SMTP as the Service, and does not have a SMTP resource defined to limit what domains (or through other information) can relay mail from the mail server.
Solution
To correct the open SMTP relay issue, you must create a SMTP resource and use the Match option. You must then create a rule that uses the SMTP service with this resource. To do this you must:
1.) Open the Policy Editor GUI.
2.) Go to Manage > Resources > New > SMTP Resource, click on Edit.
3.) Configure the name, and any comments, and then Select the Match tab
4.) Under Sender put *
5.) Under recipient type your e-mail domain with a leading and ending '*' (ie. *@4bilu.com*), and click OK.
6.) Add a rule to the Rule Base, and specify the service as "Add with resource", then select SMTP as the Service from the list of available services. Select the SMTP resource just created from the second "Resource:" drop down list.
7.) Install policy
Once this has been completed the firewall should no longer act as an open relay.
Applies To:
VPN-1/FireWall-1 4.1
VPN-1/FireWall-1 NG
SMTP relay is open
SMTP Security Server
Did not find it
How did this solution address your need?
Solved my need
Helped to solve my need
Did not help at all
Was this solution easy to follow?
Explanations were comprehensive, and instructions were easy to follow
Instructions were partial or inaccurate
I could not understand the instructions
Did it increase your knowledge?
I understand the product better, and know how to avoid future issues
I understand the product better
The solution did not have any added value
Please tell us how to make it better:
Submit
Copyright | Contact Us | Site Feedback | Privacy Policy | Site Map
Done
7.991s