Checkpoint

Exam 156-215

Check Point Certified Security Administrator NGX

Version: 5.0

[Total Questions: 146]

Topic 0, A

A

Question No : 1 - (Topic 0)

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 from the 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 anti-spoofing is enabled.

Answer: D

Question No : 2 - (Topic 0)

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

A. NGX takes the common-name value from the Certificate subject, and searches the LDAP 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 DN 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 external LDAP user database.

Answer: B

Question No : 3 - (Topic 0)

Gary is a Security Administrator in a small company. He needs to determine if the company's Web servers are accessed for an excessive number of times from the same host. How would he configure this setting in SmartDefense?

A. Successive multiple connections
B. HTTP protocol inspection
C. Successive alerts
D. General HTTP worm catcher
E. Successive DoS attacks

Answer: A

Question No : 4 - (Topic 0)

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

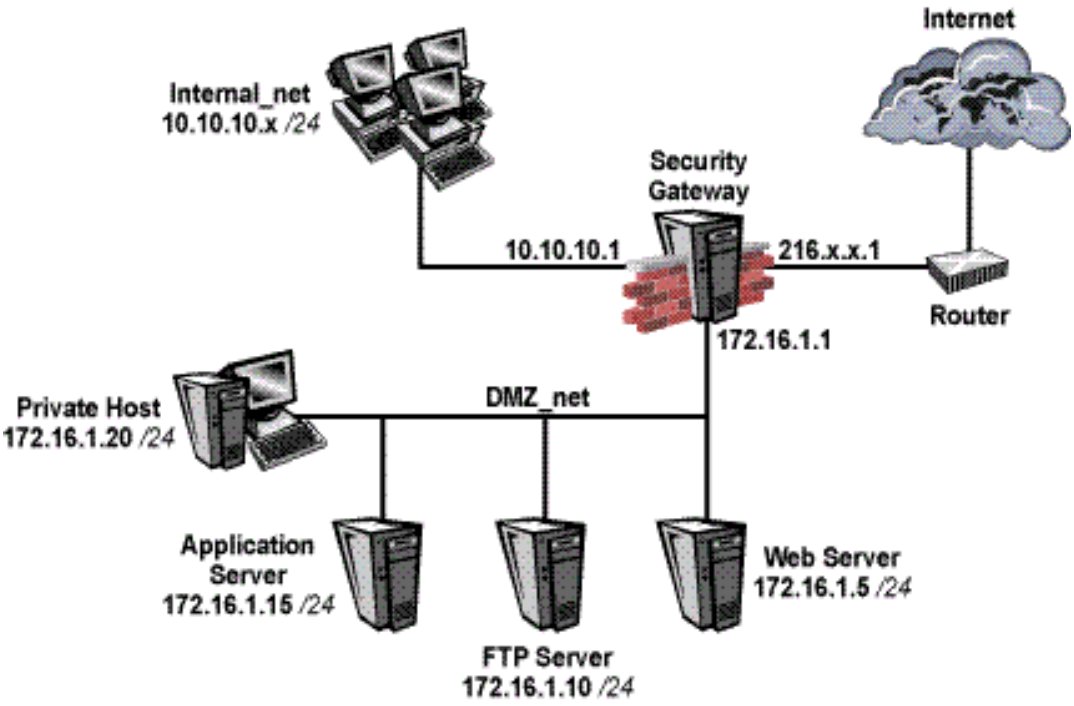
A. Define a secondary SmartCenter Server as a log server, to transfer the old logs.
B. Configure a script to archive old logs to another directory, before old log files are deleted.
C. Do nothing. Old logs are deleted, until free space is restored.
D. Use the fwm logexport command to export the old log files to other location.
E. Do nothing. The SmartCenter Server archives old logs to another directory.

Answer: B

Question No : 5 - (Topic 0)

Brianna has three servers located in a DMZ, using private IP addresses. She wants internal users from 10.10.10.x to access the DMZ servers by public IP addresses. Internal_net 10.10.10.x is configured for Hide NAT behind the Security Gateway's external interface.

What is the best configuration for 10.10.10.x users to access the DMZ servers, using the DMZ servers' public IP addresses?



A. Configure automatic Static NAT rules for the DMZ servers.
B. Configure manual Static NAT rules to translate the DMZ servers, when connecting to the Internet.
C. Configure manual static NAT rules to translate the DMZ servers, when the source is the internal network 10.10.10.x.
D. Configure Hide NAT for the DMZ network behind the DMZ interface of the Security Gateway, when connecting to internal network 10.10.10.x.
E. Configure Hide NAT for 10.10.10.x behind DMZ's interface, when trying to access DMZ servers.

Answer: C

Question No : 6 - (Topic 0)

You are setting up a Virtual Private Network, and must select an encryption scheme. Network performance is a critical issue - even more so than the security of the packet. Which encryption scheme would you select?

A. In-place encryption
B. Tunneling mode encryption
C. Either one will work without compromising performance

Answer: A

Question No : 7 - (Topic 0)

Larry is the Security Administrator for a software-development company. To isolate the corporate network from the developers' network, Larry installs an internal Security Gateway. Larry 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 No : 8 - (Topic 0)

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. ESP.
D. An asymmetric encryption algorithm.
E. Triple DES.

Answer: D

Question No : 9 - (Topic 0)

Ellen is performing penetration tests against SmartDefense for her Web server farm. She needs to verify that the Web servers are secure against traffic hijacks. She has selected the "Products > Web Server" box on each of the node objects. What other settings would be appropriate? Ellen:

A. needs to configure TCP defenses such as "Small PMTU" size.
B. should enable all settings in Web Intelligence.
C. needs to create resource objects for the web farm servers and configure rules for the web farm.
D. must activate the Cross-Site Scripting property.
E. should also enable the Web intelligence > SQL injection setting.

Answer: D

Question No : 10 - (Topic 0)

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

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

Answer: E

Question No : 11 - (Topic 0)

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

Question No : 12 - (Topic 0)

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

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

Answer: E

Question No : 13 - (Topic 0)

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

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

Answer: A

Question No : 14 - (Topic 0)

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 No : 15 - (Topic 0)

Which of the following is the final step in an NGX backup?

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: A

Question No : 16 - (Topic 0)

Which SmartConsole tool verifies the installed Security Policy name?

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

Answer: E

Question No : 17 - (Topic 0)

If the LDAP scheme is not updated on the LDAP server, which Check Point user settings are stored locally in the Check Point user template?

A. Time settings, Authentication type, Location settings
B. Location settings, Authentication type, Password
C. Authentication type, Time settings, Password
D. Password, Authentication type, Time settings

Answer: A

Question No : 18 - (Topic 0)

Choose the BEST sequence for configuring user management on SmartDashboard, 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

Question No : 19 - (Topic 0)

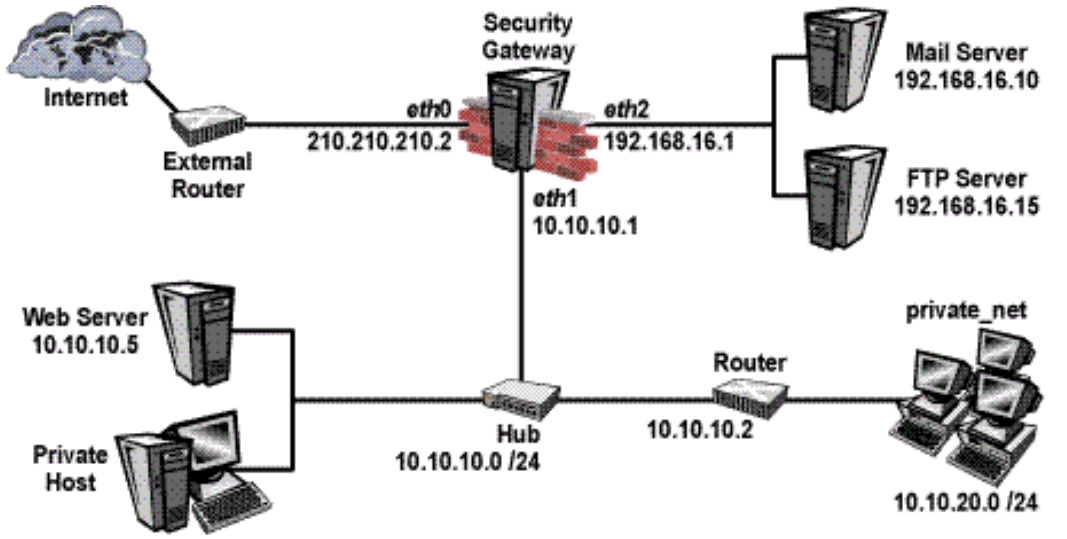
By default, when you click File > Switch Active File from SmartView Tracker, the SmartCenter Server:

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 No : 20 - (Topic 0)

You create implicit and explicit rules for the following network. The group object "internal-networks" includes networks 10.10.10.0 and 10.10.20.0. Assume "Accept ICMP requests" is enabled as before last in the Global Properties.Based on these rules, what happens if you Ping from host 10.10.10.5 to a host on the Internet, by IP address? ICMP will be:



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

A. dropped by rule 0.
B. dropped by rule 2, the Cleanup Rule.
C. accepted by rule 1.
D. dropped by the last implicit rule.

E. accepted by the implicit rule.

Answer: C

Question No : 21 - (Topic 0)

Jack's project is to define the backup and restore section of his organization's disaster recovery plan for his organization's distributed NGX installation. Jack must meet the following required and desired objectives:

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

Desired Objective: The 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:

Use the cron utility to run the upgrade_export command each night on the SmartCenter Servers. Configure the organization's routine backup software to back up the files created by the upgrade_export command.

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

Use the cron utility to run the upgrade_export command each Saturday night on the Log Servers. Configure an automatic, nightly logswitch. Configure the organization's routine backup software to back up the switched logs every night.

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