Checkpoint 156-215

Check Point 156-215.65 Check Point Security Administration I NGX

Practice Test

Version 1.4

QUESTION NO: 1

What are the results of the command: fw sam [Target IP Address]?

A. Connections to the specified target are blocked without the need to change the Security Policy
B. Connections to and from the specified target are blocked without the need to change the Security Policy
C. The Security Policy is compiled and installed on the target's embedded VPN/FireWall Modules
D. Connections from the specified target are blocked without the need to change the Security Policy

Answer: B

QUESTION NO: 2

The command fw fetch causes the:

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

Answer: C

QUESTION NO: 3

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

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

Answer: D

QUESTION NO: 4

Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services. The Gateway does not allow Telnet service to itself from any location. How

would you set up the authentication method? With a:

A. Session Authentication rule
B. Client Authentication rule using the manual sign-on method, using HTTP on port 900
C. Client Authentication for fully automatic sign on
D. Client Authentication rule, using partially automatic sign on

Answer: B

QUESTION NO: 5

You must set up SIP with a proxy for your network. IP phones are in the 172.16.100.0 network. The Registrar and Proxy are installed on the host, 172.16.101.100. To allow handover enforcement for outbound calls from SIP-net to the Internet, you have defined the following objects:

Network object: SIP-net: 172.16.100.0/24

SIP-gateway: 172.16.101.100

VoIP Domain object: VoIP_domain_A

End-point domain: SIP-net

VoIP gateway installed at: SIP-gateway host object

How would you configure the rule?

A. VoIP_domain_A / any / sip_any / accept
B. VoIP_Gateway_A / any / sip / accept
C. Unsupported because the SIP Registrar and the SIP Proxy are installed on the same host. Separate and create two VoIP Domain objects.
D. SIP-net & SIP-gateway / any / sip / accept

Answer: A

QUESTION NO: 6

A _____ rule is used to prevent all traffic going to the VPN-1 NGX Security Gateway

A. Stealth

B. Cleanup
C. SmartDefense
D. Reject

Answer: A

QUESTION NO: 7

An advantage of using central vs local licensing is:

A. Only one IP address is used for all licenses.
B. Licenses are automatically attached to their respective Security Gateways.
C. The license must be renewed when changing the IP address of a Security Gateway.
D. A license can be taken from oneSmartCenter Server and given to SmartCenter Server.

Answer: A

QUESTION NO: 8

Which command allows verification of the Security Policy name and install date on a Security Gateway?

A. fw ver -p
B. fw show policy
C. fw stat -l
D. fw ctl pstat -policy

Answer: C

QUESTION NO: 9

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

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

Answer: C

QUESTION NO: 10

When configuring objects in SmartMap, it is helpful to _____ the objects so that they are properly defined for use in a policy rule.

A. Save
B. Actualize
C. Physically connect to
D. Expand

Answer: B

QUESTION NO: 11

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

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

Answer: D

QUESTION NO: 12

During which step in the installation process is it necessary to note the fingerprint for first-time verification?

A. When configuring theSmartCenter Server using cpconfig
B. When configuring the Gateway in theWebUI
C. When configuring the Security Gateway object inSmartDashboard
D. When establishing SIC between theSmartCenter Server and the Gateway

Answer: A

QUESTION NO: 13

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

A. cpstat fwd
B. fw stat
C. fw ver
D. fw ctl pstat

Answer: B

QUESTION NO: 14

The command fw fetch causes the:

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

Answer: C

QUESTION NO: 15

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

A. If a guarantee is defined in a sub-rule, then a guarantee must be defined for the rule above it.
B. If both a limit and a guarantee per rule are defined in aQoS rule, then the limit must be smaller than the guarantee.
C. A rule guarantee must not be less than the sum the guarantees defined in its sub-rules.
D. If both a rule limit and a per connection limit are defined for a rule, the per connection limit must not be greater than the rule limit.

Answer: B

QUESTION NO: 16

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

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

Answer: D

QUESTION NO: 17

Where can an administrator specify the notification action to be taken by the firewall in the event that available disk space drops below 15%?

A. Real Time Monitor: Gateway Settings: Status Monitor
B. SmartView Tracker: Audit Tab: Gateway Counters
C. This can only be monitored by a user-defined script
D. SmartView Monitor: Gateway Status: Threshold Settings

Answer: D

QUESTION NO: 18

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 server object for the LDAP Account Unit, and create an LDAP resource object.
C. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.

Answer: A

QUESTION NO: 19

Which option or utility includes only Security and NAT, QoS, and Desktop Security settings?

A. Policy Package Management
B. Database Revision Control
C. Backup

D. File > Save fromSmartDashboard

Answer: A

QUESTION NO: 20

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

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

Answer: A

QUESTION NO: 21

Which of the following Global Properties NAT options applies to Manual Network Address Translation rules only?

A. Automatic ARP configuration
B. Translate destination on client-side
C. Enable IP Pool NAT
D. Allow bi-directional NAT

Answer: B

QUESTION NO: 22

You have blocked an IP address via the Block Intruder feature of SmartView Tracker. How can you see the addresses you have blocked?

A. InSmartView Tracker, click the Active tab, and the actively blocked connections display.
B. InSmartView Monitor, select the Blocked Intruder option from the query tree view.
C. Runfwm blocked_view.
D. InSmartView Monitor, select Suspicious Activity Rules from the Tools menu and select the relevant Security Gateway from the list.

Answer: D

QUESTION NO: 23

Assume you are a Security Administrator for ABCTech. You have allowed authenticated access to users from Mkting_net to Finance_net. But in the user's properties, connections are only permitted within Mkting_net. What is the best way to resolve this conflict?

A. Select "Intersect with user database" in the action-properties window.
B. Permit access toFinance_net.
C. Select "Intersect with user database" or "Ignore Database" in the action properties window.
D. Select "Ignore Database" in the action properties window.

Answer: C

QUESTION NO: 24

Which type of VPN-1 NGX R65 Security Server does not provide User Authentication?

A. SMTP Security Server
B. FTP Security Server
C. HTTP Security Server
D. HTTPS Security Server

Answer: A

QUESTION NO: 25

VPN-1 NGX R65 supports VoIP traffic in all of the following environments, except which environment?

A. H.323
B. SCCP
C. H.509-b
D. MGCP

Answer: C

QUESTION NO: 26

Your users are defined in a Windows 2003 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 R65?

A. All Users
B. External-user group
C. A group with generic* user
D. LDAP group

Answer: D

QUESTION NO: 27

Another Administrator without access to SmartDashboard installed a new VPN-1 NGX R65 Security Gateway, using SecurePlatform, over the weekend. You want to confirm communication between the Security Gateway and the SmartCenter Server by installing the Security Policy on the Security Gateway. What might prevent you from installing the Policy on the Security Gateway?

A. You first need to run thefw unloadlocal command on the new Security Gateway.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway andSmartCenter Server. You must initialize SIC on the SmartCenter Server.
C. You first need to run thefw unloadlocal command on the SmartCenter Server.
D. You have not established Secure Internal Communications (SIC) between the Security Gateway andSmartCenter Server. You must initialize SIC on both the Security Gateway and the SmartCenter Server.

Answer: D

QUESTION NO: 28

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

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

Answer: A

QUESTION NO: 29

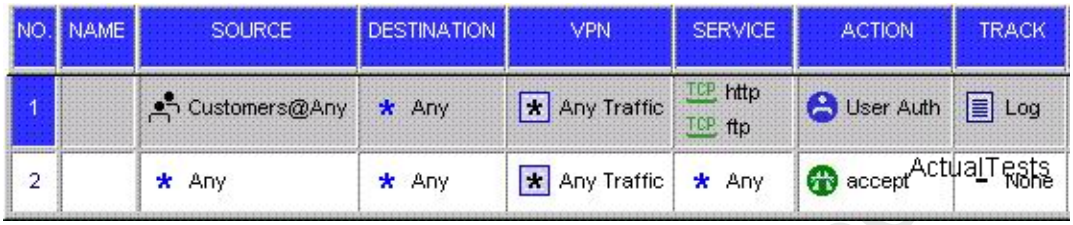
How can you prevent delay-sensitive applications, such as video and voice traffic, from being dropped due to long queue using Check Point QoS solution?

A. guaranteed per connection
B. Weighted Fair queuing
C. Low latency class
D. guaranteed per VoIP rule

Answer: C

QUESTION NO: 30

Review the following rules. Assume domain UDP is enabled in the implied rules:What happens when a user from the internal network tries to browse to the Internet using HTTP? The:



A. user's connection is dropped by the last implied rule.
B. user can connect to the Internet successfully after being authenticated successfully.
C. user can go to the Internet, without being prompted for authentication.
D. user is prompted three times before connecting to the Internet successfully.

Answer: C

QUESTION NO: 31

Your company's Security Policy forces users to authenticate to the Gateway explicitly, before they can use any services. The Gateway does not allow Telnet service to itself from any location. How would you set up the authentication method? With a:

A. Client Authentication rule, using partially automatic sign on
B. Client Authentication rule using the manual sign-on method, using HTTP on port 900
C. Session Authentication rule
D. Client Authentication for fully automatic sign on

Answer: B

QUESTION NO: 32

Which of the following features in SmartDefense, CANNOT be configured per profile?

A. Successive Events
B. Blocked FTP Commands
C. Report toDShield
D. Spoofed Reset Protection

Answer: B

QUESTION NO: 33

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

A. InSmartDefense SMTP settings
B. In the Security Server window in Global Properties
C. In the gateway object's SMTP settings in the Advanced window
D. In thesmtp.conf file on the SmartCenter Server

Answer: C

QUESTION NO: 34

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

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

Answer: B

QUESTION NO: 35

What information is found in the SmartView Tracker audit log?

A. Policy Package rule modification date/time stamp
B. Destination IP address
C. Historical reports log
D. ClusterXL sync failure

Answer: A

QUESTION NO: 36

Which utility is necessary for reestablishing SIC??

A. sysconfig
B. vconfig
C. cplic
D. cpconfig

Answer: D

QUESTION NO: 37

Which of the following statements accurately describes the snapshot command?

A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of aSecurePlatform Security Gateway.
B. snapshot creates a full system-level backup of theSmartCenter Server on any OS.
C. snapshot stores only the system-configuration settings on the Gateway.
D. A gateway snapshot includes configuration settings and Check Point product information from the remoteSmartCenter Server.

Answer: A

QUESTION NO: 38

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

A. SmartView Monitor
B. SmartUpdate
C. SmartView Status
D. Eventia Analyzer

Answer: A

QUESTION NO: 39

You administer a large, geographically distributed network. The Internet connection at a remote site failed during the weekend, and the Security Gateway logged locally for over 48 hours. It is possible that the logs may have consumed most of the free space on the Gateway's hard disk. Which SmartConsole application displays the percent of free hard-disk space on the remote

Security Gateway?

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

Answer: D

QUESTION NO: 40

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

A. The VPN-1 Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
B. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
C. You can limit the authentication attempts in the Authentication tab of the User Properties screen.
D. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.

Answer: A

QUESTION NO: 41

Which column in the Rule Base is used to define authentication parameters?

A. Track
B. Source
C. Service
D. Action

Answer: D

QUESTION NO: 42

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your NGX Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every 1 minute, a search through the SmartView tracker for GRE traffic only shows one entry for the whole day (early in the morning

after a policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.

If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.

Which of the following is the best explanation of this behavior?

A. The Log Server "log unification process" unifies all log entries from the Security Gateway on a specific connection into only one log entry in theSmartView Tracker. GRE trafic has a 10 minute session timeout thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
B. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt. Because it is encrypted, the NGX Security Gateway cannot distinguish between GRE sessions. This is a known issue with GRE. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
C. The Log Server is failing to log GREtrafic properly because it is VPN trafic. Turn off all VPN configuration to the partner site to enable proper logging.
D. The setting "Log" does not capture this level of detail for GRE. Set the rule tracking action to AUDIT since certain types of traffic can only be tracked this way.

Answer: A

QUESTION NO: 43

You are Security Administrator for a large call center. The management team 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, configured to drop peer-to-peer file-sharing traffic. How do you determine the number of packets dropped by each Gateway?

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

Answer: D

QUESTION NO: 44

Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism when logging in to a remote server with Telnet?

A. Agent Automatic Sign On
B. Manual Sign On
C. Standard Sign On
D. Partially Automatic Sign On

Answer: D

QUESTION NO: 45

It is possible to export SmartMap to which type of file(s)?

A. Adobe Photoshop and JPEG
B. SmartMap cannot be exported in NGX R60 through R65
C. Microsoft Visio and GIF
D. Microsoft Visio, bitmap, or JPEG

Answer: D

QUESTION NO: 46

How does the Get Address button, found on the Host Node Object - General Properties page retrieve the address?

A. Address resolution (ARP, RARP)
B. Name resolution (hosts file, DNS, cache)
C. SNMP Get
D. Route Table

Answer: B

QUESTION NO: 47

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

A. In Global Properties > Reporting Tools check the box "Enable tracking all rules (including rules marked as 'None' in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.

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

Answer: A

QUESTION NO: 48

When troubleshooting the behavior of Check Point Stateful Inspection, it is important to consider "inbound" vs "outbound" packet inspection from the point of view of the _____.

A. Internet
B. Administrator
C. Logical Topology
D. Security Gateway

Answer: D

QUESTION NO: 49

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

A. Are used for securing internal network communications between theSmartDashboard and the SmartCenter Server.
B. For NGX R65 Security Gateways are created during theSmartCenter Server installation.
C. Uniquely identify Check Point enabled machines; they have the same function as VPN Certificates.
D. Decrease network security by securing administrative communication among theSmartCenter Servers and the Security Gateway.

Answer: C

QUESTION NO: 50

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

A. Guarantees

B. Low Latency Queuing
C. Differentiated Services
D. Weighted Fair Queuing

Answer: B

QUESTION NO: 51

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

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

Answer: B

QUESTION NO: 52

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

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

Answer: D

QUESTION NO: 53

Which of the following statements BEST describes Hide Mode Translation?

A. Translates non-routable internal IP addresses to one routable IP address only
B. Allows you to hide an entire network behind a pool of IP addresses, selected randomly
C. Allows you to hide any entire network or IP range behind one routable IP address only
D. Allows you to hide any entire network or IP range behind one IP address

Answer: D

QUESTION NO: 54

What information is found in the SmartView Tracker audit log?

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

Answer: A

QUESTION NO: 55

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

A. Determined by the Global Properties configuration: Logs defined in the Log and Alerts section, rules with tracking set to Account or SNMP trap.
B. Determined by the "Dshield Storm Center Logging" setting in "Logs and Masters" of the SmartCenter Server object: rules with tracking set to Log or None.
C. Determined inSmartDefense > Network Security > Dshield Storm Center configuration: SmartCenter sends logs from rules with tracking set to either "Alert" or one of the specific "User Defined Alerts".
D. Determined by how Web Intelligence > Information Disclosure is configured: rules with tracking set to User Defined Alerts or SNMP trap.

Answer: C

QUESTION NO: 56

SmartView Tracker logs the following Security Administrator activities, EXCEPT:

A. Object creation, deletion, and editing.
B. Administrator login and logout.
C. Rule Base changes.
D. Tracking SLA compliance.

Answer: D

QUESTION NO: 57

The customer has a small Check Point installation which includes one Window 2003 server working as SmartConsole and SmartCenter with a second server running SecurePlatform working

as Security Gateway. This is an example of:

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

Answer: A

QUESTION NO: 58

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

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

Answer: C

QUESTION NO: 59

Your SmartCenter Server fails and does not reboot. One of your remote Security Gateways managed by the SmartCenter Server reboots. What happens to that remote Gateway after reboot?

A. Since theSmartCenter Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, all traffic is allowed through the Gateway.
B. The remote Gateway fetches the last installed Security Policy locally, and passes traffic normally. The Gateway will log locally, since theSmartCenter Server is not available.
C. Since theSmartCenter Server is not available, the remote Gateway uses the local Security Policy, but does not log traffic.
D. Since theSmartCenter Server is not available, the remote Gateway cannot fetch the Security Policy. Therefore, no traffic is allowed through the Gateway.

Answer: B

QUESTION NO: 60

Your Security Gateways are running near performance capacity and will get upgraded hardware next week, which of the following would be best to quickly drop all connections from a specific attacker's IP at a peak time of day?

A. Intrusion Detection System (IDS) policy install
B. Change the Rule Base and install the policy to all security gateways
C. SAM ?Block Intruder feature ofSmartView Tracker
D. SAM ?Suspicious Activity Rules feature ofSmartView Monitor

Answer: D

QUESTION NO: 61

You are about to test some rule and object changes suggested in an NGX newsgroup. Which backup solution should you use, to ensure the easiest restoration of your Security Policy to its previous configuration, after testing the changes?

A. upgrade_export command
B. Database Revision Control
C. SecurePlatform backup utilities
D. Manual copies of the $FWDIR/conf directory

Answer: B

QUESTION NO: 62

What does it indicate when a Check Point product name includes the word "SMART"?

A. This Check Point product is a GUI Client
B. The Check Point product includes Artificial Intelligence
C. Security Management Architecture
D. Stateful Management of all Routed Traffic

Answer: C

QUESTION NO: 63

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

Answer: A

QUESTION NO: 64

Assuming the Cleanup Rule is included in a Rule Base, in which position in the Rule Base should the "Accept ICMP requests" implied rule have no effect?

A. After Stealth Rule
B. First
C. Before Last
D. Last

Answer: D

QUESTION NO: 65

If a user is configured for partially automatic Client Authentication and attempts to authenticate remotely using FTP, which authentication method will be invoked for the first connection from the users IP?

A. Client Authentication
B. User Authentication
C. Manual Sign On
D. Session Authentication

Answer: B

QUESTION NO: 66

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

A. Per Connection Guarantee
B. Rule weight
C. Rule guarantee
D. Apply rule only to encrypted traffic

Answer: A

QUESTION NO: 67

Which of the following describes the behavior of an NGX Security Gateway?

A. IP protocol types listed as "secure" are allowed by default. ICMP, TCP, UDP sessions are inspected.
B. All traffic is expressly permitted via explicit rules.
C. Traffic is filtered using controlled port scanning.
D. Traffic not explicitly permitted is dropped.

Answer: D

QUESTION NO: 68

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

A. Runfw fetch from the Security Gateway.
B. Reinstall the Security Policy.
C. Select install database from the Policy menu.
D. Select save from the file menu.

Answer: B

QUESTION NO: 69

You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify the security administration task, which one of the following would you choose to do?

A. Run separateSmartConsole instances to login and configure each Security Gateway directly
B. Create a separate Security Policy Package for each remote Security Gateway
C. Create Network Range objects that restrict all applicable rules to only certain networks
D. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules

Answer: B

QUESTION NO: 70

Your internal network is using 10.1.1.0/24. This network is behind your perimeter VPN-1 NGX R65 Gateway, which connects to your ISP provider. How do you configure the Gateway to allow this network to go out to the Internet?

A. Use automatic Static NAT for network 10.1.1.0/24.

B. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.
C. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
D. Use Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter Gateway.

Answer: D

QUESTION NO: 71

Which specific VPN-1 NGX R65 GUI would you use to view the length of time a TCP connection was open?

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

Answer: B

QUESTION NO: 72

You want to display log entries containing information from a specific column in the SmartView Tracker. If you want to see ONLY those entries, what steps would you take?

A. Left-click column, Specific, Add, Apply Filter
B. Right-click column, Search? Add string, Apply Filter
C. Right-click column, Edit Filter, Specific, Add, OK
D. Left-click column, Search, Add string, Apply Filter

Answer: C

QUESTION NO: 73

Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. Configure the Security Gateway protecting the Web servers as a Web server.

B. Check the "Products > Web Server" box on the host node objects representing your Web servers.
C. Check the "Web Intelligence" box in theSmartDefense > HTTP Protocol Inspection.
D. The penetration software you are using is malfunctioning and is reporting a false-positive.

Answer: C

QUESTION NO: 74

You have just been hired as the Security Administrator for a public relations company. Your manager asks you to investigate ways to improve the performance of the firm's perimeter Security Gateway. You 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:

You initially recommend the following changes to the Gateway's configuration:
?Replace all domain objects with network and group objects.
?Stop logging Domain Name over UDP (queries).
?Use Global Properties, instead of explicit rules, to control ICMP, VRRP, and RIP.

When you test these changes, what do you conclude about meeting the required and desired results?

A. The actions meet the required results, and one of the desired results.
B. The actions meet none of the required results.
C. The actions meet all required results, and none of the desired results.
D. The actions meet all required and desired results.

Answer: D

QUESTION NO: 75

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

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

Answer: B

QUESTION NO: 76

All of the following are VPN-1 control connections defined by default implied rules, EXCEPT:

A. Specific traffic that facilitates functionality, such as logging, management, and key exchange.
B. Acceptance of IKE and RDP traffic for communication and encryption purposes.
C. Exclusion of specific services for reporting purposes.
D. Communication with server types, such as RADIUS, CVP, UFP, TACACS, and LDAP.

Answer: C

QUESTION NO: 77

Your company plans to stream training videos provided by a third party on the Internet. You get to configure the corporate security to facilitate this effort.

?You configure NGX R65 so each department ONLY views Webcasts specific to its department.

?You create and configure multicast restrictions for all interfaces.

?You configure the interface multicast restrictions to "Drop all multicast packets except those whose destination is in the list".

Initial tests reveal no multicast transmissions coming from the NGX Security Gateway. What is a possible cause for the connection problem?

A. You still have to create the necessary "to and through" rules, defining how NGX R65 will handle the multicast traffic.
B. Multicast groups are configured improperly on the external interface properties of the Security Gateway object.

C. NGX R65 does not support multicast routing protocols and streaming media through the Security Gateway.
D. The Multicast Rule is below the Stealth Rule. NGX R65 can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule.

Answer: A

QUESTION NO: 78

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

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

Answer: C

QUESTION NO: 79

Your VPN-1 NGX R65 primary SmartCenter Server is installed on SecurePlatform. You plan to schedule the SmartCenter Server to run fw logswitch automatically every 48 hours. How do you create this schedule?

A. Create a time object, and add 48 hours as the interval. Open the Security Gateway object's Logs and Masters window, enable "Schedule log switch", and select the time object.
B. On aSecurePlatform SmartCenter Server, this can only be accomplished by configuring the fw logswitch command via the cron utility.
C. Create a time object, and add 48 hours as the interval. Select that time object's Global Properties > Logs and Masters window, to schedule alogswitch.
D. Create a time object, and add 48 hours as the interval. Open the primarySmartCenter Server object's Logs and Masters window, enable "Schedule log switch", and select the Time object.

Answer: D

QUESTION NO: 80

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

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

Answer: D

QUESTION NO: 81

As a Security Administrator, you must refresh the Client Authentication authorization time-out every time a new user connection is authorized. How do you do this? Enable the:

A. "Refreshable Timeout" setting, in the gateway object's Authentication screen.
B. "Refreshable Timeout", in the user object's Authentication screen.
C. "Refreshable Timeout" setting, in the Limit tab of the Client Authentication Action properties screen.
D. "Refreshable timeout", in the Global Properties Authentication screen.

Answer: C

QUESTION NO: 82

You are configuring the VoIP Domain object for an SCCP environment protected by VPN-1 NGX R65. Which VoIP Domain object type can you use?

A. Gatekeeper
B. Proxy
C. CallManager
D. Transmission Router

Answer: C

QUESTION NO: 83

Which specific VPN-1 NGX R65 GUI would you use to add an address translation rule?

A. SmartView Monitor
B. SmartDashboard
C. SmartNAT
D. SmartConsole

Answer: B

QUESTION NO: 84

Which of the following are authentication methods that VPN-1 NGX uses to validate connection attempts? Select the response below that includes the most complete list of valid authentication methods

A. User, Client, Session
B. Connection, User, Client
C. Connection,Proxied, Session
D. Proxied, User, Dynamic, Session

Answer: A

QUESTION NO: 85

The customer has a small Check Point installation which includes one Linux Enterprise 3.0 server working as SmartConsole and a second server running Windows 2003 working as both SmartCenter server and the Security Gateway. This is an example of:

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

Answer: B

QUESTION NO: 86

When you add a resource object to a rule, which ONE of the following occurs?

A. All packets matching that rule are either encrypted or decrypted by the defined resource
B. Users attempting to connect to the Destination of the rule will be required to authenticate
C. All packets matching the resource service are analyzed through an application-layer proxy
D. All packets that match the resource will be dropped

Answer: C

QUESTION NO: 87

Which antivirus scanning method does not work if the Gateway is connected as a node in proxy mode?

A. Scan by IP Address
B. Scan by Server
C. Scan by File Type
D. Scan by Direction

Answer: D

QUESTION NO: 88

Which of the following statements about Bridge mode are TRUE?

A. Assuming a new installation, bridge mode requires changing the existing IP routing of the network.
B. A bridge must be configured with a pair of interfaces.
C. When managing a Security Gateway in Bridge mode, it is possible to use a bridge interface for Network Address Translation.
D. AllClusterXL modes are supported.

Answer: B

QUESTION NO: 89

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

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

Answer: B

QUESTION NO: 90

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

A. SmartDashboard: Security Gateway Object: Advanced Properties Tab

B. SmartDashboard: Policy Package Manager
C. SmartView Monitor: Global Thresholds
D. SmartView Tracker: Audit Log

Answer: C

QUESTION NO: 91

Which of the below is the MOST correct process to reset SIC?

A. Runcpconfig, and select "Secure Internal Communication > Change One Time Password".
B. Click Reset in the Communication window of the Gateway object, and type a new activation key.
C. Runcpconfig, and click Reset.
D. Click the Communication button for the firewall object, then click Reset. Run cpconfig and type a new activation key.

Answer: D

QUESTION NO: 92

Your Rule Base includes a Client Authentication rule, with partial authentication and standard sign on for HTTP, Telnet, and FTP services. The rule was working, until this morning. Now users are not prompted for authentication, and they see error "page cannot be displayed" in the browser. In SmartView Tracker, you discover the HTTP connection is dropped when the Gateway is the destination. What caused Client Authentication to fail?

A. You enabled Static NAT on the problematic machines.
B. You added the Stealth Rule before the Client Authentication rule.
C. You disabled NGX Control Connections in Global Properties.
D. You added a rule below the Client Authentication rule, blocking HTTP from the internal network.

Answer: B

QUESTION NO: 93

You are configuring the VoIP Domain object for a SIP environment, protected by VPN-1 NGX R65. Which VoIP Domain object type can you use?

A. Call Agent
B. Proxy

C. Gateway
D. Call Manager

Answer: B

QUESTION NO: 94

You are configuring SmartDefense to block the CWD and FIND commands. What should you do before you install the Security Policy to keep the Security Gateway from continuing to pass the commands?

A. Set the radio button on theSmartDefense > Application Intelligence > FTP Security Server screen to "Configurations apply to all connections".
B. Include CWD and FIND in the FTP Service Object > Advanced > Blocked FTP Commands list.
C. Delete the rule accepting FTP to any source, and from any destination from the Rule Base.
D. Check the Global Properties > Security Server > "Control FTP Commands" box.

Answer: A

QUESTION NO: 95

You are a firewall administrator with one SmartCenter Server managing three different firewalls. One of the firewalls does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is a possible cause?

A. The firewall is not listed in the "policy installation targets" screen for this policy package
B. The firewall has failed to sync with theSmartCenter Server for 60 minutes
C. The license for this specific firewall has expired
D. The firewall object has been created but SIC has not yet been established

Answer: A

QUESTION NO: 96

A _____ rule is designed to drop all other communication that does not match another rule.

A. Stealth
B. Cleanup
C. Reject
D. Anti-Spoofing

Answer: B

QUESTION NO: 97

You are creating rules and objects to control VoIP traffic in your organization, through a VPN-1 NGX R65 Security Gateway. You create VoIP Domain SIP Proxy objects to represent each of your organization's three SIP gateways. You then create a simple group to contain the VoIP Domain SIP Proxy objects. When you attempt to add the VoIP Domain SIP objects to the group, they are not listed. What is the problem?

A. The related end-points domain specifies an address range. Simple groups cannot contain address range objects even if imbedded in a VoIP object.
B. VoIP Domain SIP Proxy objects cannot be placed in simple groups.
C. The VoIP gateway object must be added to the group, before the VoIP Domain SIP Proxy object is eligible to be added to the group.
D. The VoIP Domain Proxy object contains a "SIP Gateway" field populated with a VPN-1 Security Gateway object. Simple groups cannot contain Security Gateways even if imbedded in a VoIP object.

Answer: B

QUESTION NO: 98

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

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

Answer: C

QUESTION NO: 99

The third-shift Administrator was updating SmartCenter Access settings in Global Properties. He managed to lock all of the administrators out of their accounts. How should you unlock these accounts?

A. Delete the fileadmin.lock in the $FWDIR/tmp/ directory of the SmartCenter Server.
B. Reinstall theSmartCenter Server and restore using upgrade_import.
C. Login toSmartDashboard as the special "cpconfig_admin" user account; right-click on each administrator object and select "unlock".

D. Typefwm lock_admin a from the command line of the SmartCenter Server

Answer: D

QUESTION NO: 100

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

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

Answer: C

QUESTION NO: 101

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

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

Answer: C

QUESTION NO: 102

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

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

Answer: C

QUESTION NO: 103

Which of the following statements BEST describes Hide Mode Translation?

A. Allows you to hide any entire network or IP range behind one IP address
B. Translates non-routable internal IP addresses to one routable IP address only
C. Allows you to hide an entire network behind a pool of IP addresses, selected randomly
D. Allows you to hide any entire network or IP range behind one routable IP address only

Answer: A

QUESTION NO: 104

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

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

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

Answer: C

QUESTION NO: 105

You cannot use SmartDashboard's SmartDirectory features to connect to the LDAP server. What should you investigate?

1. Verify you have read-only permissions as administrator for the operating system.

2. Verify there are no restrictions blocking SmartDashboard's User Manager from connecting to the LDAP server.

3. Check that the Login Distinguished Name configured has root (Administrator) permission (or at least write permission) in the access control configuration of the LDAP server.

A. 1 and 3
B. 1, 2, and 3
C. 2 and 3
D. 1 and 2

Answer: C

QUESTION NO: 106

What is the difference between Standard and Specific Sign On methods?

A. Standard Sign On requires the user toreauthenticate for each service and each host to which he is trying to connect. Specific Sign On allows the user to sign on only to a specific IP address.
B. Standard Sign On allows the user to be automatically authorized for all services that the rule allows. Specific Sign On requires that the userreauthenticate for each service and each host to which he is trying to connect.
C. Standard Sign On allows the user to be automatically authorized for all services that the rule allows. Specific Sign On requires that the userreauthenticate for each service specifically defined in the "Specific Action Properties" window.
D. Standard Sign On allows the user to be automatically authorized for all services that the rule allows, butreauthenticate for each host to which he is trying to connect. Specific Sign On requires that the user reauthenticate for each service.

Answer: B

QUESTION NO: 107

As a Security Administrator, you must refresh the Client Authentication authorization time-out every time a new user connection is authorized. How do you do this? Enable the:

A. "Refreshable timeout", in the Global Properties Authentication screen.
B. "Refreshable Timeout" setting, in the Limit tab of the Client Authentication Action properties screen.
C. "Refreshable Timeout", in the user object's Authentication screen.
D. "Refreshable Timeout" setting, in the gateway object's Authentication screen.

Answer: B

QUESTION NO: 108

You are configuring the VoIP Domain object for an H.323 environment, protected by VPN-1 NGX R65. Which VoIP Domain object type can you use?

A. Gatekeeper
B. Proxy
C. Transmission Router
D. Call Agent

Answer: A

QUESTION NO: 109

One of your remote 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 an error message. What is the problem?

A. The time on theSmartCenter Server's clock has changed, which invalidates the remote Gateway's Certificate.
B. The Internal Certificate Authority for theSmartCenter object has been removed from objects_5_0.C.
C. The remote Gateway's IP address has changed, which invalidates the SIC Certificate.
D. There is no connection between theSmartCenter Server and the remote Gateway. Rules or routing may block the connection.

Answer: D

QUESTION NO: 110

How do you configure a VPN-1 NGX R65 Security Gateway's kernel memory settings, without manually modifying the configuration files in $FWDIR\lib? By configuring the settings on the:

A. Global Properties Capacity Optimization screen
B. gateway object's Capacity Optimization screen
C. SmartCenter Server object's Advanced screen
D. Gateway object's Advanced screen

Answer: B

QUESTION NO: 111

Anti-Spoofing is typically set up on which object types?

A. Security Gateway
B. Host
C. Domain
D. Network

Answer: A

QUESTION NO: 112

Web Filtering can make exceptions for specific sites by being enforced:

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

Answer: C

QUESTION NO: 113

Which option or utility includes Security Policies and Global Properties settings?

A. File > Save fromSmartDashboard
B. Backup
C. Database Revision Control
D. Policy Package Management

Answer: C

QUESTION NO: 114

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

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

Answer: B

QUESTION NO: 115

It is possible to configure Network Address Translation in all of the following areas, EXCEPT:

A. Dynamic Object Properties
B. Object Properties
C. Global Properties
D. Address-translation rules

Answer: A

QUESTION NO: 116

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

A. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections.
B. Burst traffic matching the Default Rule is exhausting the Check PointQoS global packet buffers.
C. The guarantee of one of the rule's sub-rules exceeds the guarantee in the rule itself.
D. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements.

Answer: A

QUESTION NO: 117

You are configuring SmartDefense to block the CWD and FIND commands. What should you do before you install the Security Policy to keep the Security Gateway from continuing to pass the commands?

A. Include CWD and FIND in the FTP Service Object > Advanced > Blocked FTP Commands list.
B. Delete the rule accepting FTP to any source, and from any destination from the Rule Base.
C. Check the Global Properties > Security Server > "Control FTP Commands" box.

D. Set the radio button on theSmartDefense > Application Intelligence > FTP Security Server screen to "Configurations apply to all connections".

Answer: D

QUESTION NO: 118

A Security Policy installed by another Security Administrator has blocked all SmartDashboard connections to the stand-alone installation of VPN-1 NGX R65. After running the fw unloadlocal command, you are able to reconnect with SmartDashboard and view all changes. Which of the following change is the most likely cause of the block?

A. A Stealth Rule has been configured for the NGX R65 Gateway.
B. The Allow VPN-1 Control Connections setting in Policy>Global Properties has been unchecked.
C. The Gateway Object representing your gateway was configured as an Externally Managed VPN-1 Gateway.
D. The Security policy installed to the Gateway had no rules in it.

Answer: B

QUESTION NO: 119

You are working with multiple Security Gateways that enforce a common set of rules. To minimize the number of policy packages, which one of the following would you choose to do?

A. Create a separate Security Policy Package for each remote Security Gateway and specify "InstallOn?Gateways"
B. Install a separate localSmartCenter Server and SmartConsole for each remote Security Gateway
C. Create a single Security Policy Package with "Installon?Target" defined whenever a unique rule is required for a specific gateway
D. Run separateSmartDashboard instances to login and configure each Security Gateway directly

Answer: C

QUESTION NO: 120

An unprotected SMTP Server causes your site to be reported as a spam relay. Which of the following is the most efficient configuration method to implement an SMTP Security Server to prevent this?

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

Answer: B

QUESTION NO: 121

Spoofing is a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins.
D. Making packets appear as if they come from an authorized IP address.

Answer: D

QUESTION NO: 122

You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After awhile, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Restore the entire database, except the user database.
B. Runfwm dbexport filename. Restore the database. Then, run fwm dbimport filename to import the users.
C. Runfwm_dbexport to export the user database. Select "restore the entire database" in the Database Revision screen. Then, run fwm_dbimport.
D. Restore the entire database, except the user database, and then create the new user and user group.

Answer: A

QUESTION NO: 123

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

A. fw delete all.all
B. cpstop
C. fw unloadlocal
D. fw unload policy

Answer: C

QUESTION NO: 124

What information is found in the SmartView Tracker audit log?

A. Historical reports log
B. ClusterXL sync failure
C. Destination IP address
D. Policy Package rule modification date/time stamp

Answer: D

QUESTION NO: 125

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

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

Answer: D

QUESTION NO: 126

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

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

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

Answer: D

QUESTION NO: 127

A third-shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. How would you check this using SmartConsole?

A. SmartView Monitor
B. This information can only be viewed withfw ctl pstat command from the CLI.
C. Eventia Analyzer
D. SmartView Tracker

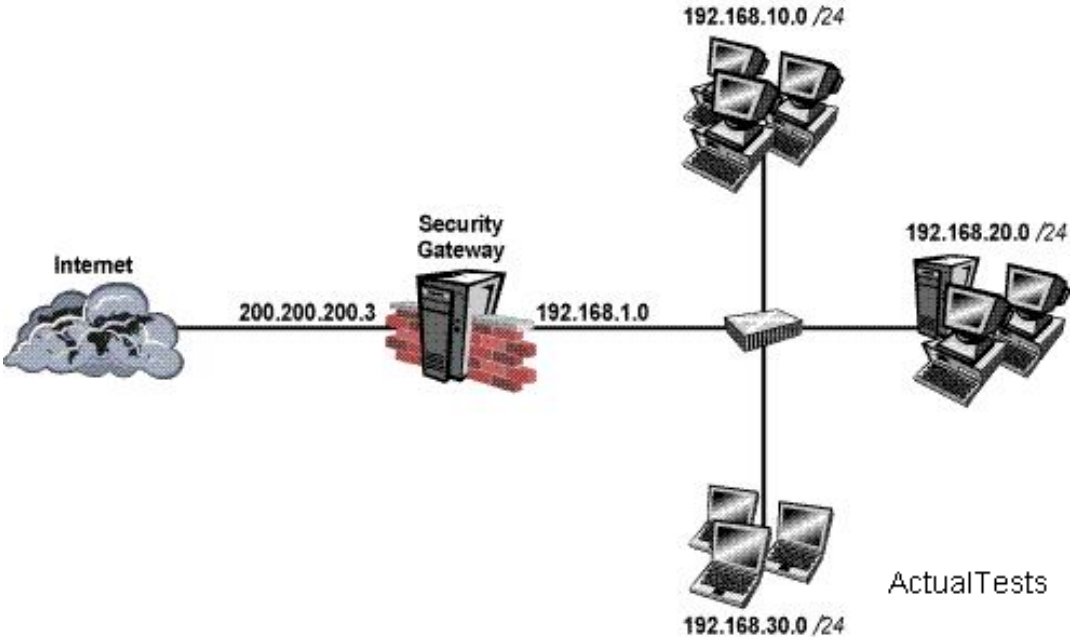
Answer: A

QUESTION NO: 128

Your perimeter Security Gateway's external IP is 200.200.200.3. Your network diagram shows:Required: Allow only network 192.168.10.0 and 192.168.20.0 to go out to Internet, using 200.200.200.5.

The local network 192.168.1.0/24 needs to use 200.200.200.3 to go out to the Internet.

Assuming you enable all the settings in the NAT page of Global Properties, how do you achieve this requirement?



A. Create two network objects: 192.168.10.0/24 and 192.168.20.0/24. Add the two network objects to a group object. Create a manual NAT rule like the following: Original source - group object; Destination ?any; Service ?any; Translated source - 200.200.200.5; Destination ?original; Service ?original.
B. Create an Address Range object, starting from 192.168.10.1 to 192.168.20.254. Enable Hide NAT on the NAT page of the Address range object. Enter Hiding IP address 200.200.200.5. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
C. Create a network object 192.168.0.0/16. Enable Hide NAT on the NAT page. Enter 200.200.200.5 as hiding IP address. Add an ARP entry for 200.200.200.5 for the MAC address of 200.200.200.3.
D. Create network objects for 192.168.10.0/24 and 192.168.20.0/24. Enable Hide NAT on both network objects, using 200.200.200.5 as hiding IP address. Add an ARP entry for 200.200.200.3 for the MAC address of 200.200.200.5.

Answer: B

QUESTION NO: 129

You have just been hired as the Security Administrator for the Insure-It-All insurance company. Your manager gives you the following requirements for controlling DNS traffic:

Required Result #1: Accept domain-name-over-TCP traffic (zone-transfer traffic).

Required Result #2: Log domain-name-over-TCP traffic (zone-transfer traffic).

Desired Result #1: Accept domain-name-over-UDP traffic (queries traffic).

Desired Result #2: Do not log domain-name-over-UDP traffic (queries traffic).

Desired Result #3: Do not clutter the Rule Base by creating explicit rules for traffic that can be controlled using Global Properties.

To begin, you make the following configuration changes, and install the Security Policy:

?Select the box "Accept Domain Name over TCP (Zone Transfer)" in Global Properties.
?Select the box "Accept Domain Name over UDP (Queries)" in Global Properties.
?Select the box "Log Implied Rules" in Global Properties.

Do your initial actions meet the required and desired results?

A. The actions meet all required results, and none of the desired results.
B. The actions meet the required results, and two of the desired results.
C. The actions meet all required and desired results.
D. The actions meet not meet the required results.

Answer: B

QUESTION NO: 130

You find a suspicious FTP connection trying to connect to one of your internal hosts. How do you block it in real time and verify it is successfully blocked?

A. Highlight the suspicious connection inSmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection is listed in this SmartView Tracker view as "dropped".
B. Highlight the suspicious connection inSmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection does not appear again in this SmartView Tracker view.
C. Highlight the suspicious connection inSmartView Tracker > Log mode. Block it using Tools > Block Intruder menu. Observe in the Log mode that the suspicious connection does not appear again in this SmartView Tracker view.
D. Highlight the suspicious connection inSmartView Tracker > Log mode. Block it using Tools > Block Intruder menu. Observe in the Log mode that the suspicious connection is listed in this SmartView Tracker view as "dropped".

Answer: B

QUESTION NO: 131

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

A. Hidden rules are already effectively disabled from Security Gateway enforcement.
B. Right-click on the Hidden rule place-holder bar in the Rule Base and select "Disable Rule(s)".
C. Right-click on the Hidden rule place-holder bar in the Rule Base and uncheck "hide", then right-click and select "Disable Rule(s)", re-hide the rule.
D. Use the search utility in theSmartDashboard to view all hidden rules. Select the relevant rule and select "Disable Rule (s)".

Answer: C

QUESTION NO: 132

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

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

Answer: C

QUESTION NO: 133

Which of the following commands can provide the most complete restore of an NGX R65 configuration?

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

Answer: A

QUESTION NO: 134

You want to implement Static Destination NAT in order to provide external, Internet users access to an internal Web Server that has a reserved (RFC 1918) IP address. You have an unused valid IP address on the network between your Security Gateway and ISP router. You control the router that sits between the external interface of the firewall and the Internet.

What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?

A. Place a static host route on the ISP router from the valid IP address to the firewall's external address
B. Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address
C. Place a static host route on the firewall from the valid IP address to the internal web server
D. Publish a proxy ARP entry on the internal web server instead of the firewall for the valid IP address

Answer: A

QUESTION NO: 135

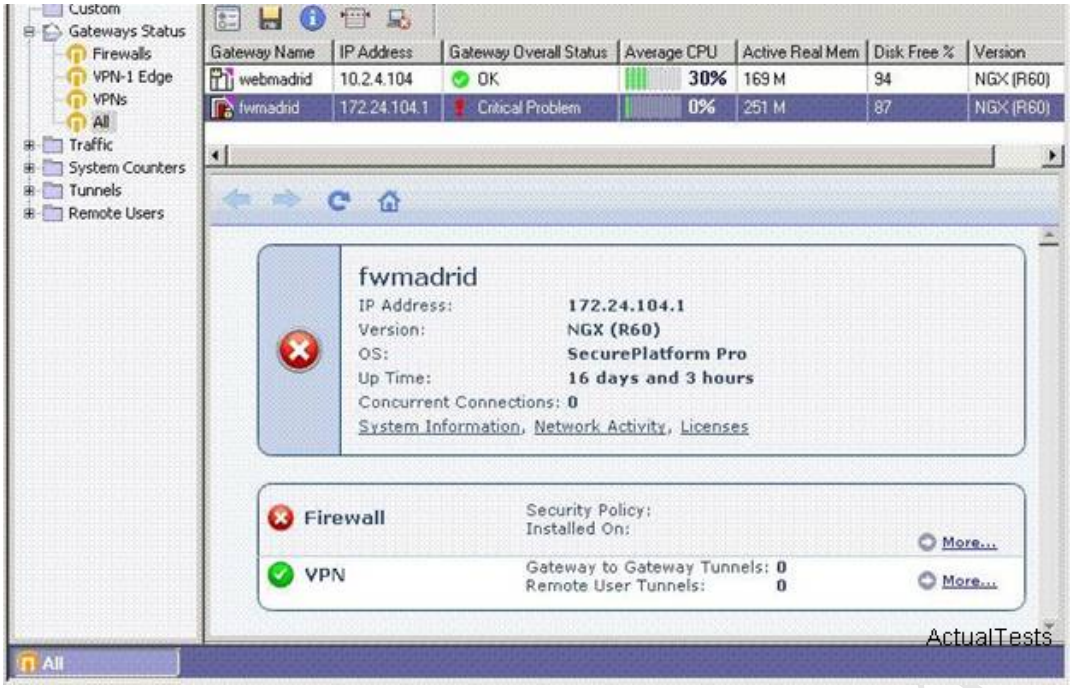
Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status. You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks. The penetration testing indicated the Web servers were still vulnerable. You have checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?

A. The penetration software you are using is malfunctioning and is reporting a false-positive.
B. Configure the Security Gateway protecting the Web servers as a Web server.
C. Check the "Products > Web Server" box on the host node objects representing your Web servers.
D. Check the "Web Intelligence" box in theSmartDefense > HTTP Protocol Inspection.

Answer: D

QUESTION NO: 136

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



A. No Security Policy installed on the Security Gateway
B. Time not synchronized between theSmartCenter Server and Security Gateway
C. No Secure Internal Communications established between theSmartCenter Server and Security Gateway
D. Version mismatch between theSmartCenter Server and Security Gateway

Answer: A

QUESTION NO: 137

Which of the following statements accurately describes the upgrade_export command?

A. upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
B. upgrade_export stores network-configuration data, all settings configured by the WebUI, and the database of user settings prior to upgrading the SmartCenter Server.
C. Used when upgrading the Security Gateway,upgrade_export includes modified files, such as in the /lib directory.
D. Used primarily when upgrading theSmartCenter Server, upgrade_export stores all object databases and the conf directories for importing to a newer version of VPN-1.

Answer: D

QUESTION NO: 138

What are the results of the command: fw sam [Target IP Address]?

A. Connections from the specified target are blocked without the need to change the Security Policy
B. Connections to the specified target are blocked without the need to change the Security Policy
C. The Security Policy is compiled and installed on the target's embedded VPN/FireWall Modules
D. Connections to and from the specified target are blocked without the need to change the Security Policy

Answer: D

QUESTION NO: 139

In a distributed management environment, the administrator has removed the default check from "Accept VPN-1 Power/UTM Control Connections" under the Policy > Global Properties > Firewall tab. In order for the SmartCenter Server to install a policy to the Firewall an explicit rule must be created to allow the SmartCenter Server to communicate to the Security Gateway on port _____

A. 900
B. 259
C. 256
D. 80

Answer: C

QUESTION NO: 140

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

A. Select save from the file menu.
B. Reinstall the Security Policy.
C. Select install database from the Policy menu.
D. Runfw fetch from the Security Gateway.

Answer: B

QUESTION NO: 141

Of the three mechanisms Check Point uses for controlling traffic, which enables firewalls to incorporate
layer 4 awareness in packet inspection?

A. Stateful Inspection
B. SmartDefense
C. Application Intelligence
D. Packet filtering

Answer: A

QUESTION NO: 142

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

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

Answer: D

QUESTION NO: 143

Which statement below is TRUE about management plug-ins?

A. The plug-in is a package installed on the Security Gateway.
B. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.
C. A management plug-in interacts with aSmartCenter Server to provide new features and support for new products.
D. Installing a management plug-in is just like an upgrade process. (It overwrites existing components.)

Answer: C

QUESTION NO: 144

It is required to completely reboot the OS after which of the following changes are made on the Security
Gateway?

i.e. cprestart command is not sufficient

1. Adding a hot-swappable NIC to the OS for the first time.
2. Uninstalling the VPN-1 Power/UTM package.

3. Installing the VPN-1 Power/UTM package.
4. Re-establishing SIC to the SmartCenter Server.
5. Doubling the maximum number of connections accepted by the Security Gateway

A. 1, 2, 3 only
B. 3 only
C. 3, 4, and 5 only
D. 1, 2, 3, 4, and 5

Answer: A

QUESTION NO: 145

In a "Stand-Alone Installation" the functionality of the SmartCenter Server would be installed together with which other Check Point architecture component?

A. SecureClient
B. SmartConsole
C. Security Gateway
D. None,SmartCenter Server would be installed by itself

Answer: C

QUESTION NO: 146

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a
central license for one remote Security Gateway. You must request a central license:

A. Using yourSmartCenter Server's IP address, attach the license to the remote Gateway via SmartUpdate.
B. Using the remote Gateway's IP address, attach the license to the remote Gateway viaSmartUpdate.
C. Using each of the Gateways' IP addresses, apply the licenses on theSmartCenter Server with the cprlic
put command.
D. Using the remote Gateway's IP address, apply the license locally with thecplic put command.

Answer: A

QUESTION NO: 147

You are installing a SmartCenter server. Your security plan calls for three administrators for this particular server. How many can you create during installation?

A. As many as you want
B. Depends on the license installed on theSmartCenter Server
C. Only one with full access and one with read-only access
D. Only one

Answer: D

QUESTION NO: 148

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

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

Answer: C

QUESTION NO: 149

Your bank's distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartUpdate
B. SmartPortal
C. SmartDashboard
D. SmartView Tracker

Answer: A

QUESTION NO: 150

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway.
You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to

upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

A. SmartView Monitor and SmartUpdate
B. SmartLSM and SmartUpdate
C. SmartView Tracker and SmartView Monitor
D. SmartDashboard and SmartView Tracker

Answer: A

QUESTION NO: 151

Which of the following are available SmartConsole clients which can be installed from the R65 NGX
Windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker, CPINFO, SmartUpdate
B. Security Policy Editor, Log Viewer, Real Time Monitor GUI
C. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
D. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor

Answer: D

QUESTION NO: 152

Which R65 SmartConsole tool would you use to verify the current installed Security Policy name on a
Security Gateway?

A. SmartView Status
B. SmartUpdate
C. SmartView Monitor
D. None,SmartConsole applications only communicate with the SmartCenter Server.

Answer: C

QUESTION NO: 153

Which R65 SmartConsole tool would you use to verify the installed Security Policy name on a Security
Gateway?

A. SmartUpdate
B. None,SmartConsole applications only communicate with the SmartCenter Server.
C. SmartView Server
D. SmartView Tracker

Answer: D

QUESTION NO: 154

Which SmartConsole tool would you use to see the last policy pushed in the audit log?

A. SmartView Status
B. SmartView Server
C. SmartView Monitor
D. SmartView Tracker

Answer: D

QUESTION NO: 155

VPN-1 NGX R65's INSPECT Engine inserts itself into the kernel between which two layers of the OSI
model?

A. Presentation and Application
B. Session and Transport
C. Data and Network
D. Physical and Data

Answer: C

QUESTION NO: 156

Your current security scenario gives you the option to choose between a stand-alone installation and a distributed installation. Which of the following factors would cause you to decide in favor of the distributed installation?

A. You are forced to use Windows as operating system.
B. You cannot upgrade software packages on a stand-alone Security Gateway viaSmartUpdate.
C. Clientless VPN would not work in a stand-alone installation.
D. TheSmartCenter Server must be a secondary server. You are forced to install a separate primary server.

Answer: B

QUESTION NO: 157

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

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

Answer: A

QUESTION NO: 158

UDP packets are delivered if they are _____.

A. bypassing the kernel by the "forwarding layer" ofClusterXL
B. a legal response to an allowed request on the inverse UDP ports and IP
C. astateful ACK to a valid SYN-SYN/ACK on the inverse UDP ports and IP
D. referenced in the SAM related dynamic tables

Answer: B

QUESTION NO: 159

UDP packets are delivered if they are _____.

A. a new client > server packet allowed by the Rule Base
B. a new server > client packet allowed by the Rule Base
C. astateful ACK to a valid SYN-SYN/ACK on the inverse UDP ports and IP
D. any UDP packet in any direction (client > server; server > client) allowed by the Rule Base

Answer: A

QUESTION NO: 160

Once installed, the VPN-1 NGX R65 kernel resides directly below what layer of the TCP/IP stack? Note: Application is the top and Physical is the bottom of the IP stack.

A. Data Link
B. Network
C. Session
D. Transport

Answer: B

QUESTION NO: 161

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

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

Answer: C