Exam : 156-215

Title : Check Point Security Administration NGX (156-215.1)

Ver : 11.27.06

QUESTION 1:

Which VPN-1 NGX feature or command allows Security Administrators to revert to earlier versions of the same Security Policy?

A. Policy Package management
B. cpinfo
C. cpconfig
D. Database Revision Control
E. upgrade_export/import

Answer: D

QUESTION 2:

In SmartView Tracker, you see an entry for an outbound connection showing address translation. But when setting SmartView Tracker to show all entries for that connection, only outbound entries show. What is the possible cause for this?

A. The entry is for a Manual Dynamic NAT connection, from a specific host infected by a worm.
B. The entry is for a Manual Static NAT connection, where inbound traffic is managed by a separate rule.
C. The entry is for a Static NAT connection, from a specific host that has been infected by a worm.
D. The entry is for a Dynamic NAT connection from a specific host.

Answer: B

QUESTION 3:

Which of the following commands is used to restore VPN-1 NGX configuration information?

A. gunzip
B. cpconfig
C. fw ctl pstat
D. cpinfo
E. upgrade_import

Answer: E

QUESTION 4:

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

A. CVP
B. DEFENDER

C. URI
D. FTP
E. UFP

Answer: E

QUESTION 5:

Your organization Certkiller .com's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How would you request and apply the license?

A. Request a central license, using the remote Security Gateway's IP address. Apply he license locally with the fwputlic command.
B. Request a central license, using the SmartCenter Server's IP address. Apply the license locally on the remote Gateway with the fwputlic command.
C. Request a central license, using your SmartCenter Server's IP address. Attach the license to the remote Gateway via SmartUpdate.
D. Request a central license, using the remote Gateway's IP address. Attach the license to the remote Gateway via SmartUpdate.
E. Request local licenses for all Gateways separately. Apply the license locally on the remote Gateways with the fwputlic command.

Answer: C

QUESTION 6:

How do you create more granular control over commands, such as CWD and FIND, in FTP data connections?

A. Use Global Properties > Security Server settings.
B. Use the gateway object's Security Server settings.
C. Use the Service field of the Rule Base.
D. Use an FTP resource object.
E. Use FTP Security Server settings in SmartDefense.

Answer: E

QUESTION 7:

Which of the following is the final step in a VPN-1 NGX backup?

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

E. Run the cpstop command.

Answer: B

QUESTION 8:

Choose the BEST sequence for configuring user management on SmartDashboard, for use with an LDAP server:

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

Answer: C

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

340, Check Point Security Administration NGX I Student Handbook

---

QUESTION 9:

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

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

Answer: B

QUESTION 10:

Yoav is a Security Administrator preparing to implement a VPN solution for his multisite organization. To comply with industry regulations, Yoav's VPN solution must meet the following requirement:
* Portability: Standard
* Key management: Automatic, external PKI
* Session keys: Changed at configured times during a connection's lifetime
* Key length: No less that 128-bit
* Data integrity: Secure against inversion and brute-force attacks
What is the most appropriate setting you should choose?

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

Answer: E

QUESTION 11:

How are cached usernames and passwords cleared from the memory of a VPN-1 NGX Security Gateway?

A. By pushing new user information from the LDAP server.
B. By retrieving LDAP user information, using the fwfetchldap command.
C. By using the Clear User Cache button in SmartDashboard.
D. Usernames and passwords only clear from memory aftere they time out.
E. By installing Security Policy

Answer: E

QUESTION 12:

Which VPN-1 NGX configuration setting forces the Client Authentication authorization time-out refresh, each time a new user connection is authorized? Choose ONE.

A. The "Refreshable Timeout" setting, in the Limit tab of the Client Authentication Action properties screen
B. The Global Properties > Authentication parameters, adjusted to allow for "Regular Client Refreshment"
C. The SmartDefense > Application Intelligence > Client Authentication > Refresh User Timeout option enabled
D. The Time object, with hours restricted and renewable, in the Time field of the Client Authentication rule.
E. The "Time" properties, adjusted on the user objects for each user, in he source of the Client Authentication rule

Answer: A

QUESTION 13:

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

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

Answer: A

QUESTION 14:

Your internal network's internal IP address is 10.1.1.0/24. This network needs to connect to the Internet using the Security Gateway's external (public) IP address. How would you do this?

A. Use Hide NAT on the network object in the 10.1.1.0 network.
B. Use Static Source NAT on the network object.
C. Use Dynamic NAT on network object 10.1.1.0/24.
D. Use Static NAT on the network object in the 10.1.1.0 network.
E. Use Static Destination NAT on the network object.

Answer: A

QUESTION 15:

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

A. Use the URI resource to strip script tags
B. Use the URI resource to block Java code
C. Use the URI resource to strip applet tags
D. Use the URI resource to strip ActiveX tags
E. Use CVP in the URI resource to block Java code

Answer: B

QUESTION 16:

You are the Security Administrator for Certkiller .com. Certkiller .com's Security Policy forces users to authenticate to the Security Gateway explicitly, before they can use any services. You are also reminded that your Gateway does not allow the Telnet service to itself from any location. How would you set up the authentication method?

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

Answer: A

QUESTION 17:

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

A. Run cpstop and cpstart on the SmartCenter Server, then disable the rule.
B. Open the Rule Menu, and select "hide" and "view hidden rules". The select the rule, right-click and select Disable.
C. When a rule is hidden, it is automatically disabled. You do not need to disable the rule again.
D. Clear "Hide" on the drop-down list to make the rule visible, then select "Disable Rule(s)".
E. Uninstall the Security Policy, and then disable the rule.

Answer: D

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

QUESTION 18:

Jeremy manages sites in Tokyo, Calcutta and Dallas, from his office in Chicago. He is trying to create a report for management, detailing the current software level of each Security Gateway. He also wants to create a proposal outline, listing the most cost-effective way to upgrade his Gateways. Which two SmartConsole applications should Jeremy use, to create his report and outline?

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

Answer: B
SmartLSM is a policy manager for enterprise VPN
configs, not a resource monitor, and has nothing to do with viewing
software versions/levels. Smartview Monitor does that.
http://www.checkpoint.com/products/smartcenter/smartlsm.html
http://www.checkpoint.com/products/downloads/svm_datasheet.pdf

---

QUESTION 19:

When restoring VPN-1 NGX using the upgrade_import command, which of the following items are NOT restored?

A. Global properties
B. Objects
C. Route tables
D. Security Policies
E. License

Answer: C

QUESTION 20:

Carol is the Security Administrator for a chain of grocery stores. Each grocery store is protected by a Security Gateway. Carol is generating a report for the information-technology audit department. The report must include the name of the Security Policy installed on each remote Security Gateway, and the date and time the Security Policy was installed. Which SmartConsole application should Carol use to gather this information?

A. SmartView Status
B. SmartView Monitor
C. Smartpdate

D. SmartView Tracker
E. SmartLSM

Answer: B

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

QUESTION 21:

When you check "Web Server" in a host-node object, what happens to the host?

A. More granular controls are added to the host, in addition to Web Intelligence tab settings.
B. SmartDefense Web Intelligence is enabled to check on the host.
C. Automatic Static NAT is enabled on the host.
D. The Web server is enabled on the host.
E. You can specify allowed ports in the Web server's node-object properties. You then do not need to list all allowed ports in the Rule Base.

Answer: A

QUESTION 22:

Your primary SmartCenter Server is on SecurePlattform. What is the easiest way to back up your VPN-1 NGX configuration?

A. By copying the whole $FWDIR to another location.
B. By using upgrade_export command in $FWDIR\bin directory.
C. By executing a conf_merge with an objects_5_0.C from a new NGX installation.
D. By copying the $FWDIR\conf and $FWDIR\lib directory to another location.
E. By using native SecurePlatform backup utility from command line or in Web based interface.

Answer: E

QUESTION 23:

In VPN-1 NGX, what happens if a Distinguished Name (DN) is NOT found in LDAP?

A. VPN-1 NGX takes the common-name value from the Certificate subject, and searches the LDAP account unit for a matching user id.
B. The Security Gateway uses the subject of the Certificate as the DN for the initial lookup.
C. If the first request fails or if branches do not match, NGX tries to map the identity to the user id attribute.
D. When users authenticate with valid Certificates, the Security Gateway tries to map the

identities with user registered in the external LDAP user database.
E. VPN-1 NGX searches the internal database for the username.

Answer: A

QUESTION 24:

Jane needs to create a backup of the routing, interface, and DNS configuration information from her VPN-1 NGX SecurePlatform Pro Security Gateway. Which backup-and-restore solution do you recommend for Jane?

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

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

QUESTION 25:

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. Users are now not prompted for authentication, and their browser display "page cannot be displayed". In SmartView Tracker, you discover the HTTP connection is being dropped by the Security Gateway as the destination. What caused Client Authentication to fail?

A. You added the Stealth Rule before the Client Authentication rule.
B. You disabled VPN-1 NGX control connections in Global Properties.
C. You enabled Static NAT on the problematic machines.
D. The browsers' proxy settings have changed.
E. You added a rule below the Client Authentication rule, blocking HTTP from the internal network.

Answer: A

QUESTION 26:

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

BEST long-term security, you should:

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

Answer: B

QUESTION 27:

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

A. Set the position of all implicit rules to "Before Last".
B. Check the "Log Implied Rules" box in Global Properties.
C. Clear all Global Properties check boxes, and use explicit rules instead.
D. Install the "view Implicit Rules" package using SmartUpdate.
E. Use the "Implicit Rules" predefined query in SmartView Tracker.

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

---

QUESTION 28:

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

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

Answer: B

QUESTION 29:

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

A. With SmartView Status
B. With SmartView Tracker in Audit mode
C. With SmartView Tracker in Log mode
D. With SmartView Monitor
E. With SmartView Tracker in Active Mode

Answer: B

QUESTION 30:

Jill is about to test some rule and object changes suggested in a VPN-1 NGX newsgroup. Which backup and restore solution should Jill use, to ensure she can restore her Security Policy to its previous configuration, after testing the changes?

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

Answer: B

QUESTION 31:

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?

A. External-user group
B. ALLUSERS
C. LDAP group
D. LDAP account-unit group
E. A group with generic* user

Answer: C

QUESTION 32:

Ben is the Security Administrator for a university. Ben configured and installed a new Security Policy this morning. An hour after installing the new Security Policy, Ben began receiving complaints that Internet access was very slow. Ben called his Internet Service Provider, who asked Ben how much virtual memory his Security

Gateway had. Which SmartConsole application should Ben use to answer this question?

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

Answer: E

QUESTION 33:

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

A. Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None"
B. Set Support IKE DoS protection from identified source to "None", and Support IKE DoS protection from unidentified source to "Stateless"
C. Set Support IKE DoS protection from identified source to "Puzzles", and Support IKE DoS protection from unidentified sources to "Stateless"
D. Set support IKE DoS protection from identified sources to "Puzzles", and Support IKE DoS protection from unidentified source to "Puzzles"
E. Set support IKE DoS protection from identified sources to "Stateless", and Support IKE DoS protection from unidentified source to "Puzzles"

Answer: E

Explanation: This is the default, and CheckPoint recommended. Refer to the VPN.pdf file on the CP CD, pg 34 & 35.

QUESTION 34:

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

A. VPN Communities comprised of three star Communities: The first one between New York headquarters and its branches. The second star Community is between London headquarters and its branches. The third star Community is between New York and

London headquarters.
B. VPN Communities comprised of two mesh Communities, one for each headquarters and their branch offices; one star Community, where New York is the center of the Community and London is the satellite.
C. VPN Communities comprised of two star and one mesh Community; each star Community is set up for each site, with headquarters as the center of the Community and branches as satellites. The mesh Communities are between the New York and London headquarters.
D. VPN Communities comprised of two mesh Communities for each headquarters and their branch offices; and one star Community, in which London is the center of the Community and New York is the satellite.
E. VPN Communities comprised of three mesh Communities: one for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.

Answer: C

QUESTION 35:

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

A. Reinstall the Security Policy
B. Close SmartDashboard, the reopen it
C. Run cpstop and cpstart on the SmarCenter Gateway.
D. Run cpstop and cpstart on the SmarCenter Server.
E. Do nothing. The changes is made automatically.

Answer: A

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

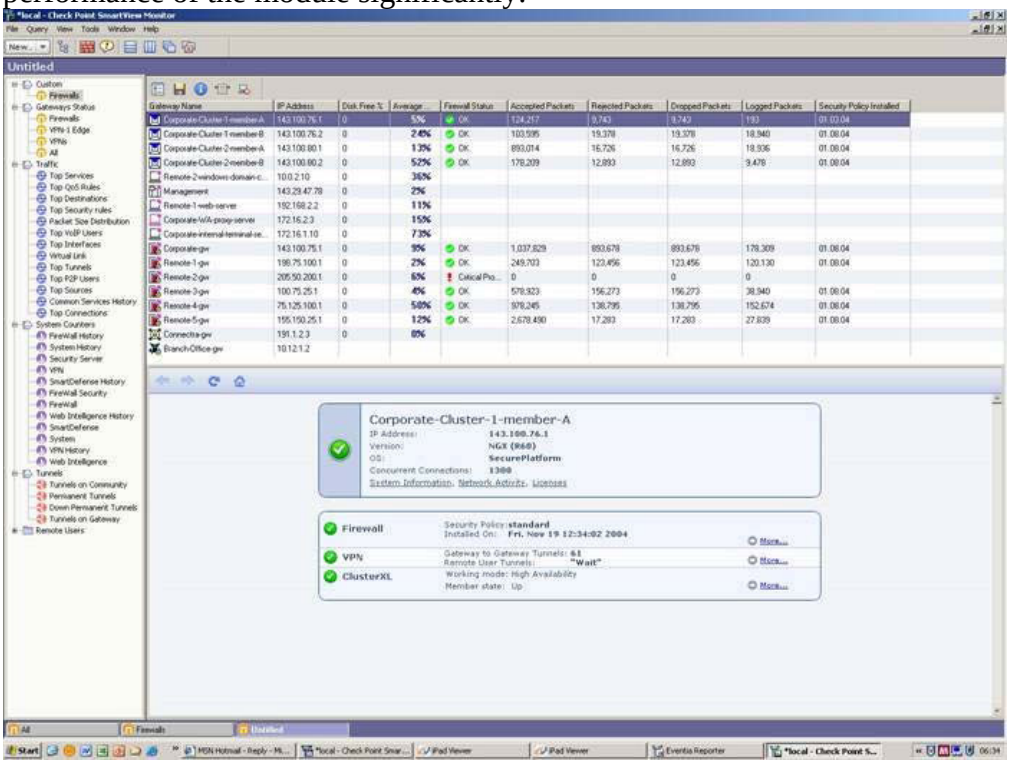
QUESTION 36:

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

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

Answer: B

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



QUESTION 37:

Ilse manages a distributes VPN-1 NGX installation for a large bank. Ilse needs to know which Security Gateways have licenses that will expire within the next 30 days. Which SmartConsole application should Ilse use to gather this information?

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

Answer: A

QUESTION 38:

Which VPN-1 NGX logs can you configure to send to DShield.org?

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

Answer: C

QUESTION 39:

Brianna has three servers located in a DMZ, using public IP addresses that need to be accessed by her internal networks. Brianna's internal network use class B IP addresses, per RFC 1918. Internal networks access the Internet, using Dynamic NAT behind the external IP address of her Security Gateway. What is the best way to configure access for the DMZ servers?

A. Configure Manual NAT rules to translate the internal networks, when connecting to the DMZ servers.
B. Configure Dynamic NAT for the DMZ interface of the Security Gateway.
C. Configure Static NAT rules for the DMZ servers.
D. Configure Manual NAT rules to translate the DMZ servers, when connecting to the internet.

Answer: A

Explanation:
Between internal network and dmz network there's no need for NAT, because Security Gateway has routes for both so routing should be enough.
So the Address Translation should look like this:
Original PacketTranslated Packet
Source Destination Service Source Destination Service
internal_net dmz_netAny Original Original Original

QUESTION 40:

How do you prevent malware from scanning specific ports in SmartDefense?

A. By enabling Malware Scan protection
B. By enabling Malicious Code Protector
C. By enabling Host port Scan
D. By enabling Sweep Scan protection
E. By enabling Network port scan

Answer: D

Explanation:
The question is tricky and a play on words, a 'sweep' is a scan on specific ports across multiple servers - which fits the answer.

QUESTION 41:

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

A. Run fw unloadlocal on the Security Gateway.
B. Run fw uninstall localhost on the Security Gateway.
C. Run fw unlocklocal on the SmartCenter Server.
D. Run cpstop on the SmartCenter Server.
E. Run cpstop on the Security Gateway.

Answer: A

QUESTION 42:

Doug wants to know who installed a Security Policy blocking all traffic from the corporate network. Which SmartView Tracker selection is best suited for this?

A. SmartView Tracker Active tab
B. SmartView Tracker Audit tab
C. SmartView Tracker custom filter
D. SmartVew Tracker Records pane
E. SmartView Tracker log connections

Answer: B

QUESTION 43:

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

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

Answer: E

QUESTION 44:

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

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

Answer: C

QUESTION 45:

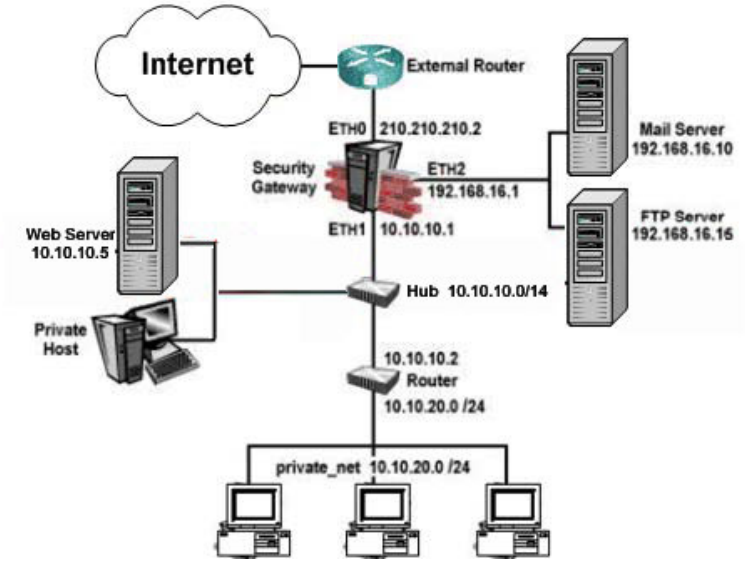
What does schema checking do?

A. Issues Certificates, and register the Certificates with the VPN-1 NGX Internal Certificate Authority
B. Maps LDAP objects to objects in the VPN-1 NGX objects.c file
C. Provides topology downloads for SecuRemote and SecureClient users authenticated by an LDAP server
D. Authenticates users attempting to access resources protected by a VPN-1 NGX Security Gateway
E. Verifies that every object class, and its associated attributes, is defined in the directory schema

Answer: E

QUESTION 46:

As a Security Administrator, you must configure anti-spoofing on Secure Gateway interfaces, to protect your internal networks. What is the correct anti-spoofing setting on interface ETH1 in this network diagram?
NOTE: In the DMZ, mail server 192.168.16.10 is statically translated to the object "mail_valid", with IP address 210.210.210.3. FTP server 192.168.16.15 is statically translated to the object "ftp_valid", with IP address 210.210.210.5.



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

Answer: A

QUESTION 47:

When you use the Global Properties' default settings, which type of traffic will be dropped, if no explicit rule allows the traffic?

A. IKE and rDP traffic
B. Outgoing traffic originating from the Security gateway.
C. SmartUpdate connections
D. Firewall logging and ICA key-exchange information.
E. RIP traffic

Answer: E

QUESTION 48:

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

A. Purges the current log, and prompts you for the new log's mode.
B. Prompts you to enter a file name, then saves the log file.
C. Saves the current log file, names the log file by date and time, and starts a new log file.

D. Opens a new window with a previously saved log file.
E. Purges the current log file, and starts a new log file.

Answer: C

QUESTION 49:

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

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

Answer: A

QUESTION 50:

Jordan's company is streaming training videos provided by a third party on the Internet. Jordan configures VPN-1 NGX, so that each department ONLY views webcasts specific to its department. Jordan created and configured the multicast groups for all interfaces, and configures them to "Drop all multicast packets except those whose destination is in the list". But no multicast transmissions are coming from the Internet. What is possible causes fro the connection problem?

A. Multicast groups are configured improperly on the external interface properties of the Security Gateway object.
B. Anti-spoofing is enabled. VPN-1 NGX cannot pass multicast traffic, if anti-spoofing is enabled.
C. Jordan did not create the necessary "to and through" rules, defining how VPN-1 NGX will handle the multicast traffic.
D. VPN-1 NGX does not support multicast routing protocols and streaming media through the Security Gateway.
E. The Multicast Rule is below the Stealth Rule. VPN-1 NGX can only pass multicast traffic, if the Multicast Rule is above the Stealth Rule.

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

QUESTION 51:

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 the SmartCenter Server is not available, the remote Gateway cannot fetch the

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

Answer: E

QUESTION 52:

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

A. SmartConsole
B. SmartCenter Server
C. Policy Server
D. SmartLSM
E. Security Gateway

Answer: B

QUESTION 53:

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

A. the CIFS resource is not configured to use Windows name resolution
B. Mapped shares are not configured to log.
C. Null CIFS sessions are configured to be blocked
D. Remote registry access is configured to be blocked.
E. Access violations are not configured to log.

Answer: A

QUESTION 54:

Barak
is a Security Administrator for an organization that has two sites using pre-shared secrets in its VPN. The two sites are Oslo and London. Barak has just been informed that a new office is opening in Madrid, and he must enable all three sites

to connect via the VPN to each other. Three Security Gateways are managed by the same SmartCenter Server, behind the Oslo Security Gateway. Barak decides to switch from pre-shared secrets to Certificates issued by the Internal Certificate Authority (ICA). After creating the Madrid gateway object with the proper VPN Domain, what are Barak's remaining steps?

1. Disable "Pre-Shared Secret" on the London and Oslo gateway objects.
2. Add the Madrid gateway object into the Oslo and London's mesh VPN Community.
3. Manually generate ICA Certificates for all three Security Gateways.
4. Configure "Traditional mode VPN configuration" in the Madrid gateway object's VPN screen.
5. Reinstall the Security Policy on all three Gateways.

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

Answer: E

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

QUESTION 55:

You want to establish a VPN, using Certificates. Your VPN will exchange Certificates with an external partner. Which of the following activities should you do first?

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

Answer: C

QUESTION 56:

There is a Web server behind your perimeter Security Gateway. You need to protect the server from network attackers, who creates scripts that force your Web server to send user credentials or identities to other Web servers. Which box do you check in the Web Intelligence tab in SmartDashboard?

A. Command Injection protection

B. SQL Injection protection
C. HTTP header format checking
D. HTTP protocol inspection protection
E. Cross Site Scripting protection

Answer: E
See screenshot from the actual Smartdefense description for Cross-site scripting defense:

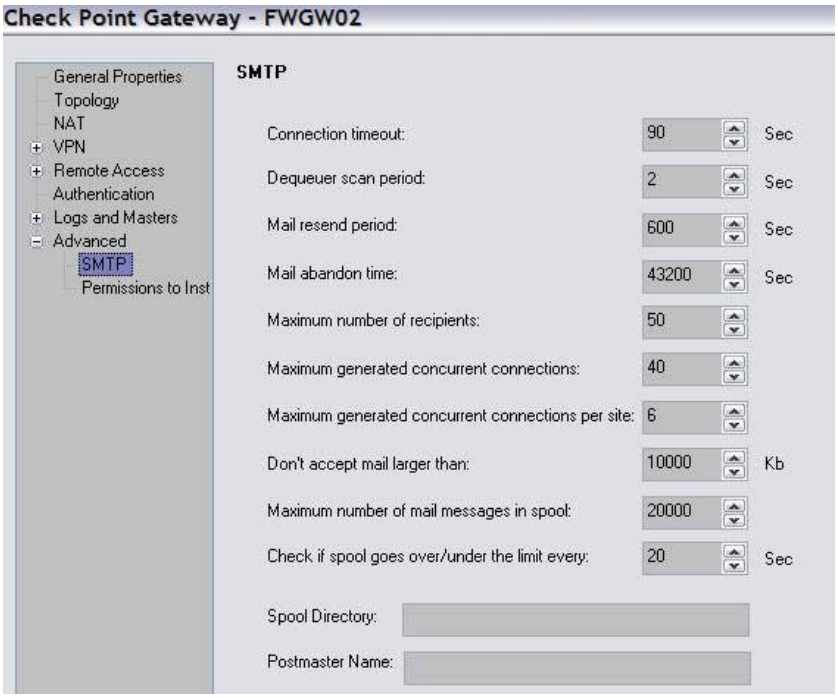
QUESTION 57:

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

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

Answer: C
It's an option in the SMTP security server settings from the gateway object. See

screenshot:



QUESTION 58:

Quinton is the Security Administrator for a chain of retail stores. In a recent security newsletter, Quinton read about an attack where a client fools a server into sending large amount of data, using small packets. Quinton is concerned that this company's servers might be vulnerable to this type of attack. Which smartDefense option should Quinton use to protect the servers?

A. Application Intelligence > DNS > Cache poisoning
B. Network Security > Successive events > DoS
C. Network Security > TCP > Small PMTU
D. Application Intelligence > Microsoft Networks > File and Print Sharing
E. Network Security > Denial of Service > LAND

Answer: C

QUESTION 59:

In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

A. Rule 999
B. Rule 0
C. Rule 1
D. Cleanup Rule
E. Stealth Rule

Answer: B
Rule 0 means the action was not taken because of a rule but rather for some other reason (for example, anti-spoofing or authentication was applied).
Found @ http://www.checkpoint.com/support/technical/online_ug/logview.html

---

QUESTION 60:

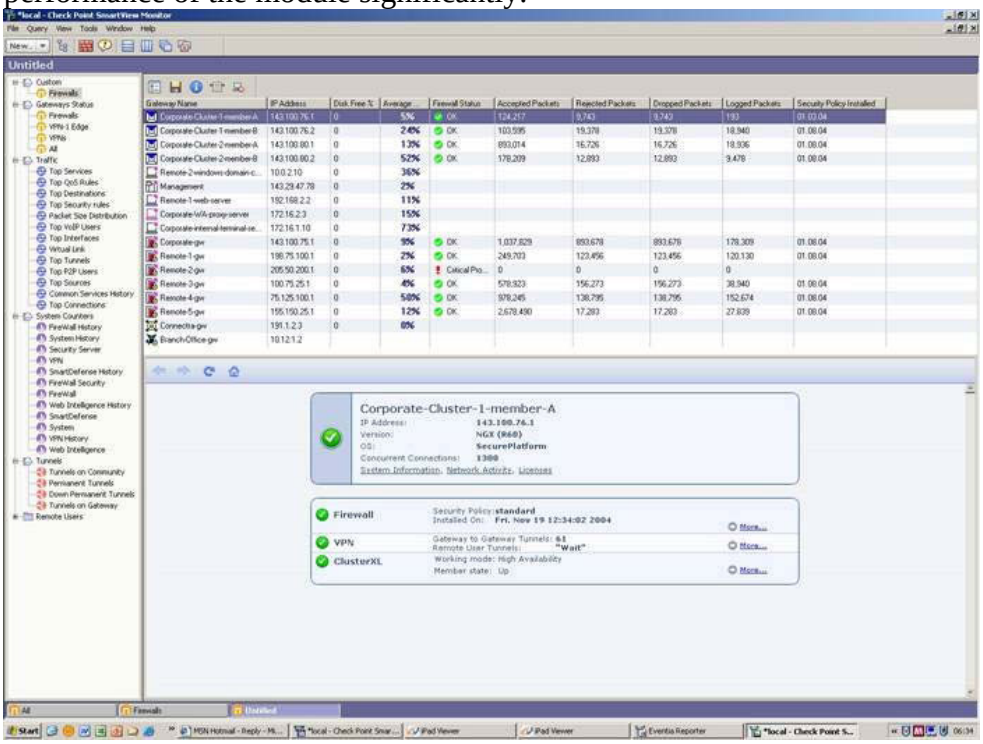
Sonny is the Security Administrator for a company with a large call center. The management team in the center is concerned that employees may be installing and attempting to use peer-to-peer file-sharing utilities, during their lunch breaks. The call center's network is protected by an internal Security Gateway, configured to drop peer-to-peer file-sharing traffic. The call-center management team wants to know if the Security Gateway protecting the call center drops more packets than other internal Security Gateways in the corporate network. Which application should Sonny use, determine the number of packets dropped by each Gateway?

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

Answer: B

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

performance of the module significantly.



QUESTION 61:

Katie is the Security Administrator for an insurance company. Her manager gives Katie 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.
Katie makes the following configuration changes, and installs the Security Policy:
1. She selects the box "Accept Domain Name over TCP (Zone transfer)" in Global Properties.
2. She selects the box "Accept Domain Name over UDP (Queries)" in Global Properties.
3. She selects the box "Log Implied Rules" in Global Properties
Does Katie's solution meet the required and desired results?

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

Answer: E

QUESTION 62:

David is a consultant for a software-deployment company. David is working at a customer's site this week. David's ask is to create a map of the customer's VPN tunnels, including down and destroyed tunnels. Which SmartConsole application will provide David with the information needed to create this map?

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

Answer: C

QUESTION 63:

Gail is the Security Administrator for a marketing firm. Gail is working with the networking team, to troubleshoot user complaints regarding access to audio-streaming material from the Internet. The networking team asks Gail to check he configuration settings for the perimeter Security Gateway. Which SmartConsole application should Gail use to check the configuration settings?

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

Answer: D

QUESTION 64:

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 "unknown". What is the problem?

A. The time on the SmartCenter Server's clock has changed, which invalidates the remote Gateway's Certificate.
B. The remote Gateway's IP address has changed, which invalidates the SIC Certificate.
C. The Security Gateway is NG with Application Intelligence, and the SmartCenter Server is NGX.
D. The Internal Certificate Authority for the SmartCenter object has been removed from objects_5_0.c.

E. There is no connection between the SmartCenter Server and the remote Gateway. Rules or routing may block the connection.

Answer: E

QUESTION 65:

Frank wants to know why users on the corporate network cannot receive multicast transmissions from the Internet. A VPN-1 NGX Security Gateway protects the corporate network from the Internet. Which of the following is a possible cause for the connection problem?

A. VPN-1 NGX does not support multicast routing protocols and streaming media through the Security Gateway.
B. The Multicast Rule is below the Stealth Rule. VPN-1 NGX can only pass multicast traffic, it the Multicast Rule is above the Stealth Rule.
C. Multicast restrictions are configured improperly on the external interface properties of the Security Gateway object.
D. Anti-spoofing is enabled. VPN-1 NGX cannot pass multicast traffic, if anti-spoofing is enabled.
E. Frank did not install the necessary multicast license with SmartUpdate, when upgrading the VPN-1 NGX.

Answer: C

QUESTION 66:

You are concerned that a message may have been intercepted and retransmitted, thus compromising the security of the communications. You attach a code to the electronically transmitted message that uniquely identifies the sender. This code is known as a:

A. Digital signature
B. Tag
C. Private key
D. AES flag
E. Diffie-Helman verification

Answer: A

QUESTION 67:

A user attempts authentication using SecureClient. The user's password is rejected, even though it is correctly defined in the LDAP directory.
Which of the following is a valid cause?

A. The LDAP server has insufficient memory
B. The LDAP and Security Gateway databases are not synchronized.
C. The SmartCenter Server cannot communicate with the LDAP server.
D. The user has defined the wrong encryption scheme.
E. The user is defined in both the NGX user database and the LDAP directory

Answer: B

Explanation:
The LDAP and Security gateway data base are not synchronized.

QUESTION 68:

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

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

Answer: E

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

---

QUESTION 69:

Exhibit: *** MISSING ***
Review the following rules and note the Client Authentication Action properties screen as displayed in the exhibit,
After being authenticated by the Security Gateway, when a user starts an HPPT connection to a Web site, the user tries to FTP antother site using the command line.
What happens to the user?
The...

A. FTP session is dropped by the implicit Cleanup Rule.
B. User is prompted from that FTP site only, and does not need to enter username and password for Client Authentication.
C. FTP connection is dropped by rule 2.

D. FTP data connection is dropped, after the user is authenticated successfully.
E. User is prompted for authentication bye the Security Gateway again.

Answer:

QUESTION 70:

Diffie-Hellman uses which type of key exchange?

A. Adaptive
B. Asymmetric
C. Symmetric
D. Static
E. Dynamic

Answer: B

QUESTION 71:

Certkiller's main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. Certkiller also has a small network 10.10-.20.0/24 behind the internal router. Jack wants to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services.
Which of the following configurations will allow this network to access Internet?

A. Automatic Static NAT on network 10.10.20.0/24
B. Manual Hide NAT rules for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
C. Manual Static NAT rules for network 10.10.20.0/24,
D. Automatic Hide NAT for network 10.10.20.0/24.
E. No change is necessarey.

Answer: A

Explanation:
It is specified that the network addresses are translated only when they try to access HTTP,SMTP and FTP.
Original Packet Translated Packet
No Source Destination Service Source Destination Service
1 internal_net Any HTTP firewall(hide) Original Original
2 internal_net Any FTP firewall(hide) Original Original
3 internal_net Any SMTP firewall(hide) Original Original

QUESTION 72:

With SmartDashboard´s Smart Directory, you can create NGX user definitions on

a(n) _____ Server.

A. NT Domain
B. LDAP
C. Provider-1
D. SecureID
E. Radius

Answer: B

QUESTION 73:

Jens notices a large amount of traffic from a specific internal IP address. He needs to verify if it is a network attack, or a user's system infected with a worm. He has enabled Sweep Scan Protection and Host port scan in SmartDefense. Will Jens get all the information he needs from these actions?

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

Answer: B

QUESTION 74:

Which NGX feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

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

Answer: C

QUESTION 75:

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

A. the settings on the Gateway object's Capacity Optimization screen
B. the settings on the Global Properties Capacity Optimization screen
C. the Settings on the Gateway object's Advanced screen
D. the settings on the SmartCenter Server object's Advanced screen
E. SmartDefense Kernel Defender options

Answer: A

QUESTION 76:

Which of the following is NOT a feature or quality of a hash function?

A. Encrypted with the sender's RSA private key, the hash function forms the digital signature.
B. It is mathematically infeasible to derive the original message from the message digest.
C. The hash function forms a two-way, secure communication.
D. The hash function is irreversible.
E. It is mathematically infeasible for two different messages to produce the same message digest.

Answer: C

Explanation:
The hash function does not provide a two way secure communication, it's simply a function which when used in conjuction with a digital certificate ensures the integrity and unique identity of a sender.

QUESTION 77:

You are a Security Administrator configuring Static NAT on an internal host-node object. You clear the box "Translate destination on client side", accessed from Global Properties > NAT settings > Automatic NAT. Assuming all other Global Properties NAT settings are selected, what else must be configured for automatic Static NAT to work?

A. The NAT IP address must be added to the anti-spoofing group of the external Gateway interface
B. Two address-translation rules in the Rule Base
C. No extra configuring needed
D. A proxy ARP entry, to ensure packets destined for the public IP address will reach the Security Gateway's external interface

E. A static route, to ensure packets destined for the public NAT IP address will reach the Gateway's internal interface

Answer: E

Explanation:
if you clear the box "Translate destination on client side" the nat will be performed on the internal interface side of your firewall, rather than the external interface and packets will not get to the firewalls internal interface as the routing on the firewall would send packets bound for public IP to the external interface. So you need to add a static route to point the nat rules public ip to the internal interface of the firewall so that the nat can be performed.
From ChechkPoint Online Help:
Translate destination on client side applies to packets originating at the client, with the server as its destination. Static NAT for the server is performed on the client side.
In Check Point Gateways prior to version NG, Static NAT for the server ("Static Destination Mode NAT") was performed on the server side of the gateway, which required special handling for anti-spoofing and internal routing.

QUESTION 78:

Which encryption scheme provides "In-place" encryption?

A. IKE
B. Manual IPSec
C. DES
D. SKIP
E. AES

Answer: C

Explanation:
DES (and FWZ1 and RC4) is an encryption algorithm that is used to encrypt the data portion of a packet.
The relationship between the components of the encryption schemes, as implemented in FireWall-1, is described in the following table.

Encryption Schemes

encryption scheme	FWZ	Manual IPSec	SKIP
authentication algorithm	MD5	MD5, SHA-1, CBC-DES MAC	MD5, SHA-1, CBC-DES MAC
encryption algorithm	DES, FWZ1	DES, RC4	DES (triple DES for key encryption), RC4
encryption is ...	in-place	encapsulated	encapsulated

Not B, D: Manual IPSec and SKIP are an examples of encapsulated encryption, where the entire packet is encrypted.

QUESTION 79:

After importing the NGX schema into an LDAP server, what should you enable?

A. Schema checking
B. Encryption
C. UserAuthority
D. ConnectControl
E. Secure Internal Communications

Answer: A

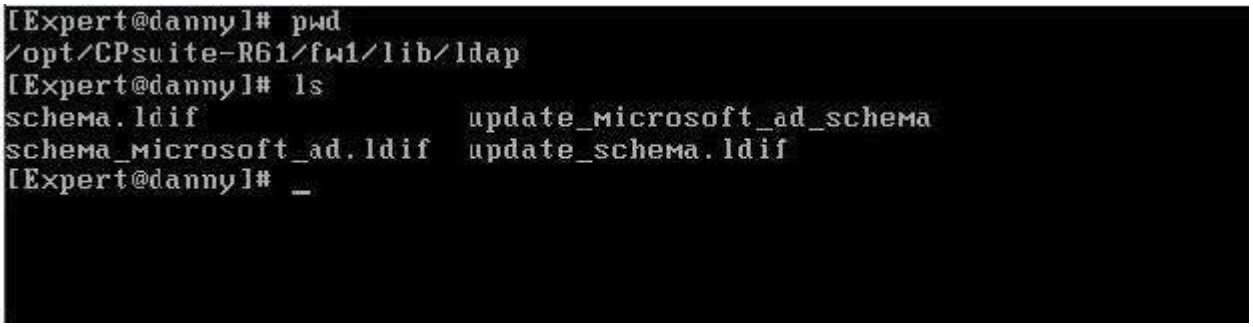
QUESTION 80:

Which ldif file must you modify to extend the schema of a Windows 2000 domain?

A. In NGX you do not need to modify any .ldif file
B. The appropriate .ldif file is located in the Security Gateway:
$FWDIR/conf/ldif/Microsoft_ad_schema.ldif
C. The appropriate .ldif file is located in the SmartCenter Server:
$FWDIR/lib/ldap/schema_microsoft_ad.ldif
D. The appropriate .ldif file is located in the Security Gateway:
$FWDIR/lib/ldif/Microsoft_ad_schema.ldif
E. The appropriate .ldif file is located in the SmartCenter Server:
$FWDIR/conf/ldif/Microsoft_ad_schema.ldif

Answer: C

Explanation:
Page 226 of the SmartCenter_UserGuide.pdf from Check Point says
"The definitions of all VPN-1 Pro attributes in LDIF format are contained in the file 'scheme_microsoft_ad.ldif' located in $FWDIR/lib/ldap directory."
http://www.checkpoint.com/support/technical/documents/docs_r61.html
Also screenshot from SecurePlatform confirms this

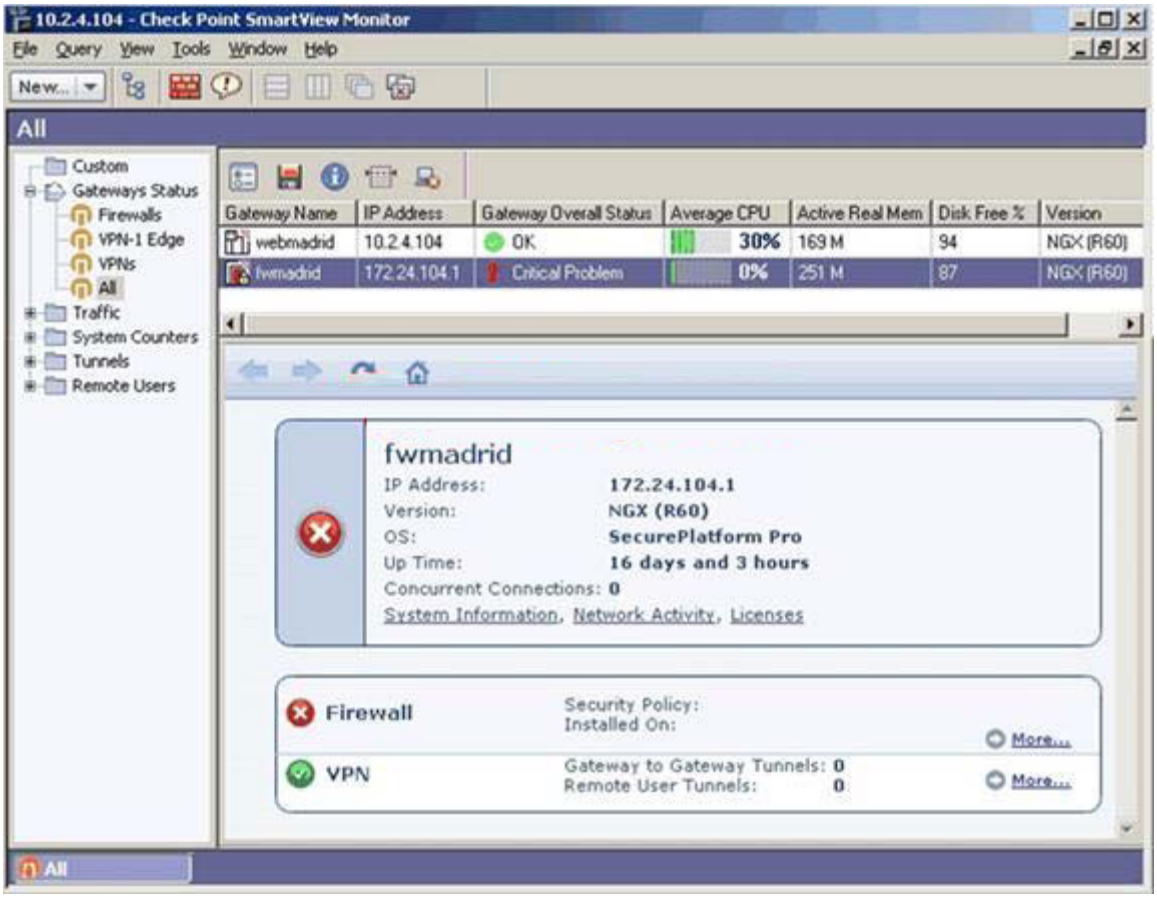


Not B, D, E: All of thefilenames/locations in answers B,D,E are invalid - it can't be those

---

QUESTION 81:

What is the reason for the Critical Problem notification in this SmartView Monitor example?



A. Active real memory shortage on the Gateway
B. No Security Policy installed on the Security Gateway
C. Version mismatch between the SmartCenter Server and Security Gateway
D. Time not synchronized between the SmartCenter Server and Security Gateway
E. No Secure Internal Communications established between the SmartCenter Server and Security Gateway

Answer: B

QUESTION 82:

Your standby SmartCenter Server's status is collision. What does that mean, and how do you synchronize the Server and its peer?

A. The standby and active Servers have two Internal Certificate Authority (ICA) Certificates. Uninstall and reinstall the standby Server.
B. The active Server detected a keep-alive packet from the standby Server.
C. The peer Server has not been properly synchronized. Manually synchronize both Servers again.
D. The peer Server is more up-to-date. Manually synchronize both Servers again.
E. The active SmartCenter Server and its peer have different Security Policies and databases. Manually synchronize the Servers, and decide which Server's configuration to overwrite.

Answer: E

Explanation:
This description is taken from the help menu in SmartDashboard in an article titled "The Management High Availability Solution".
The possible synchronization statuses are:
(several other status codes) ... then
Collision - the Active SmartCenter Server and its peer have different installed policies and databases. The administrator must perform manual synchronization and decide which of the SCSs to overwrite.
In this case, both SmartCenter Server A and B have some information which is not synchronized with its peer. In order to remedy the collision state, one of the SmartCenter Servers will need to be overwritten. The SmartCenter Server which is found to have the dominant or significant changes should be the SmartCenter Server on which manual synchronization is initiated.
At this point the system administrator needs to decide which of the SmartCenter Server's should become the Standby SCS, and change its status, if necessary.

QUESTION 83:

Sarah is the Security Administrator for Certkiller . Sarah has configured SmartDefense to block the CWD and FIND commands. Sarah installs the Security Policy, but the Security Gateway continues to pass the commands. Which of the following could be the cause of the problem?

A. The Rule Base includes a rule accepting FTP to any source, from any destination.
B. The SmartDefense > Application Intelligence > FTP Security Server screen does not have the radio button set to "Configurations apply to all connections".
C. The FTP Service Object > Advanced > Blocked FTP Commands list does not include CWD and FIND.
D. The Web Intelligence > Application Layer > FTP Settings list is configured to allow, rather than exlude, CW and FIND commands.
E. The Global Properties > Security Server > "Control FTP Commands" box is not checked.

Answer: B

QUESTION 84:

Your NGX enterprise SmartCenter Server is working normally. However, you must reinstall the SmartCenter Server, but keep the SmartCenter Server configuration (for example, all Security Policies, databases, etc.) How would you reinstall the Server and keep its configuration?

A. 1. Run the latest upgrade_export utility to export the configuration.
2. Keep the exported file in the same location.
3. Use SmartUpdate to reinstall the SmartCenter Server.
4. Run upgrade_import to import the configuration.
B. 1. Run the latest upgrade_export utility to export the configuration.
2. Leave the exported .tgz file in $FWDIR.
3. Install the primary SmartCenter Server on top of the current installation.
4. Run upgrade_import to import the configuration.
C. 1. Insert the NGX CD-ROM, and select the option to export the configuration into a .tgz file.
2. Transfer the .tgz file to another networked machine.
3. Uninstall all NGX packages, and reboot.
4. Use the NGX CD-ROM to select the upgrade_import option to import the configuration.
D. 1. Download the latest upgrade_export utility, and run it from $FWDIR\bin to export the configuration into a .tgz file.
2. Transfer the .tgz file to another networked machine.
3. Uninstall all NGX packages, and reboot.
4. Install a new primary SmartCenter Server.
5. Run upgrade_import to import the configuration.

Answer: D

Explanation:
Note: correct path will be $FWDIR/bin/upgrade_tools

QUESTION 85:

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

A. Run the command fwm sic_reset to reinitialize the Internal Certificate Authority (ICA) of the SmartCenter Server. Then retype the activation key on the Security Gateway from SmartDashboard.
B. From cpconfig on the SmartCenter Server, choose the Secure Internal Communication option and retype the activation key. Next, retype the same key in the gateway object in

SmartDashboard and reinitialize Secure Internal Communications (SIC).
C. From the SmartCenter Server's command line type fw putkey -p <IP Address of SmartCenter Server>.
D. From the SmartCenter Server's command line type fw putkey -p <IP Address of Security Gateway>.
E. Reinstall the Security Gateway.

Answer: B

Explanation:
Note: The B option (Secure Internal Communication) is available in NG R55. We don't have something like this in NGX R60 or NGX R61.
Incorrect answers:
A: A deletes the certificates, although this would work it's not needed just to reset SIC.
C,D,E are irrelevant.

QUESTION 86:

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

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

Answer: C

QUESTION 87:

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 activated the Cross-Site Scripting property. What other settings would be appropriate? Ellen:

A. should also enable the Web intelligence > SQL injection setting.
B. must select the "Products > Web Server" box on each of the node objects.
C. should enable all settings in Web Intelligence.
D. needs to configure TCP defenses such as "Small PMTU" size.
E. needs to create resource objects for the web farm servers and configure rules for the web farm.

Answer: B

QUESTION 88:

William is a Security Administrator who has added address translation for his internal Web server to be accessible by external clients. Due to poor network design by his predecessor, William sets up manual NAT rules for this server, while his FTP server and SMTP server are both using automatic NAT rules. All traffic from his FTP and SMTP servers are passing through the Security Gateway without a problem, but traffic from the Web server is dropped because of anti-spoofing settings. What is causing this?

A. "Allow bi-directional NAT" is not checked in Global Properties.
B. "Translate destination on client side" is not checked in Global Properties under "Manual NAT Rules".
C. "Translate destination on client side" is not checked in Global Properties > Automatic NAT Rules.
D. Routing is not configured correctly.
E. Manual NAT rules are not configured correctly.

Answer: B

Explanation: Checkpoint asks this question for making relation between antispoofing and "translate destination on client site" properties.. Questions emphasizes this with the last sentence "., but the traffic from web server is dropped because of antispoofing settings..".

QUESTION 89:

You are a security consultant for a hospital. You are asked to create some type of authentication rule on the NGX Security Gateway, to allow doctors to update patients' records via HTTP from various workstations. Which authentication method should you use?

A. Client Authentication
B. LDAP Authentication
C. SecureID Authentication
D. TACAS Authentication
E. User Authentication

Answer: E

QUESTION 90:

Certkiller is the Security Administrator for an online bookstore. Customers connect to a variety of Web servers to place orders, change orders, and check status of their orders. Mrs. Bill checked every box in the Web Intelligence tab, and installed the

Security Policy, She ran penetration test through the Security Gateway, to determine if the Web servers were protected from cross-site scripting attacks. The penetration test indicated the Web servers were still vulnerable. Which of the following might correct the problem?

A. The penetration software Certkiller is using is malfunctioning and is reporting a false-positive.
B. Certkiller must create resource objects, and use them in the rule allowing HTTP traffic to the Web servers.
C. Certkiller needs to check the "Products > Web Server" box on the host node objects representing his Web servers.
D. Certkiller needs to check the "Web Intelligence" box in the SmartDefense > HTTP Properties.
E. Certkiller needs to configure the Security Gateway protecting the Web servers as a Web server.

Answer: C

Explanation: Jack check everything on web intelligence and what she must to next is to check product-->web server to activate the rules.

QUESTION 91:

You create two Policy Packages for two NGX Security Gateways. For the first Policy Package, you select Security and Address Translation and QoS Policy. For the second Policy Package, you selected Security and Address Translation and Desktop Security Policy. In the first Policy Package, you enable host-based port scan from the SmartDefense tab. You save and install the policy to the relevant Gateway object. How is the port scan configured on the second Policy Package's SmartDefense tab?

A. Host-based port scan is disabled by default.
B. Host-based port scan is enabled, because SmartDefense settings are global.
C. Host-based port scan is enabled but it is not highlighted.
D. There is no SmartDefense tab in the second Policy Package.

Answer: B

Explanation:
Smart defense setting are global.

QUESTION 92:

A digital signature:

A. Uniquely encodes the receiver of the key.

B. Provides a secure key exchange mechanism over the Internet.
C. Guarantees the authenticity and integrity of a message.
D. Automatically changes the shared keys.
E. Decrypts data to its original form.

Answer: C

QUESTION 93:

You are setting up a Virtual Private Network, and must select an encryption scheme. Your data is extremely business sensitive and you want maximum security for your data communications. Which encryption scheme would you select?

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

Answer: A

Explanation:
It says you want maximum security, in this case you would use tunnel encryption which encrypts all of the packet not just the payload (more secure). C is wrong because tunnel encryption puts more of a processing overhead on the server than in-place encryption.

QUESTION 94:

You have just started a new job as the Security Administrator for Certkiller . Your boss has asked you to ensure that peer-to-peer file sharing is not allowed past the corporate Security Gateway. Where should you configure this?

A. SmartDashboard > SmartDefense
B. SmartDashboard > WebDefense
C. By editing the file $FWDIR/conf/application_intelligence.C
D. SmartDashboard > Policy > Global Properties > Malicious Activity Detection
E. SmartDashboard > Web Intelligence

Answer: A

QUESTION 95:

Amy is configuring a User Authentication rule for the technical-support department to access an intranet server. What is the correct statement?

A. The Security Server first checks if there is any rule tat does not require authentication for this type of connection.

B. The User Authentication rule must be placed above the Stealth Rule.
C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
D. Amy can only use the rule for Telnet, FTP, and rlogin services.
E. Amy can limit the authentication attempts in the Authentication tab of the User Properties screen.

Answer: A

Explanation: Answer A is correct since you can have a rule below the User Authentication rule that allows the communication and the user will never get prompted for a login.
Page 350 of the Official Student guide (NGX version 1.1)
"The fact that a user successfully connects does not necessarily mean that the user was first authenticated. The authenticating Security Server first checks if the connection can be allowed by a rule that does not require authentication. If one exists, the user will be connected through the less-restrictive rule, bypassing the User Authentication rule."
Not B: Rules with User or Session Authentication as the action can be placed below the Stealth Rule. All Client Authentication rules must be place above the Stealth rule, so they have access to the Secure Gateway.
Checkpoint Student Handbook Official courseware NGX I Rev 156.215.1 page 382
Not D:User Authentication supports HTTP and HTTPS along with Telnet, FTP and rlogin

---

QUESTION 96:

How can you unlock an administrator's account, which was been locked due to SmartCenter Access settings in Global Properties?

A. Type fwm lock_admin -ua from the command line of the SmartCenter Server.
B. Clear the "locked" box from the user's General Properties in SmartDashboard.
C. Type fwm unlock_admin -ua from the command line of the SmartCenter Server.
D. Type fwm unlock_admin -ua from the command line of the Security Gateway.
E. Delete the file admin.lock in the $FWDIR/tmp/ directory of the SmartCenter Server.

Answer: A

Explanation:
You can unlock administrator just using "fwm lock_admin
"
The options are:
[-v] # view names of all locked Administrators
[-u Administrator] # unlock a single Administrator
[-ua] # unlock all locked Administrators
Thus, the correct answer is A.
Example:
[Expert@cpmodule]# fwm lock_admin -ua

Operation finished successfully
[Expert@cpmodule]# fwm lock_admin -va
No Administrators are currently locked.
Not C: The command "fwm unlock_admin -ua" does not exist.

QUESTION 97:

How many administrators can be created during installation of the SmartCenter Server?

A. Only one
B. Only one with full access and one with read-only access
C. As many as you want
D. Depends on the license installed on the SmartCenter Server
E. Specified in the Global Properties

Answer: A

QUESTION 98:

Which SmartConsole tool verifies the installed Security Policy name?

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

Answer: E

QUESTION 99:

Ilse manages a distributed NGX installation for Certkiller .com. Ilse needs to know which Security Gateways have licenses that will expire within the next 30 days. Which SmartConsole application should Ilse use to gather this information?

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

Answer: B

QUESTION 100:

Herman is attempting to configure a site-to-site VPN with one of his firm's business partner. Herman thinks Phase 2 negotiations are failing. Which SmartConsole application should Herman use to confirm his suspicions?

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

Answer: C

QUESTION 101:

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

A. Launch cpconfig and select "Administrators".
B. Launch SmartDashboard, click the admin user account, and overwrite the existing Check Point Password.
C. Type cpm -a, and provide the existing administration account name. Reset the Security Administrator's password.
D. Export the user database into an ASCII file with fwm dbexport. Open this file with an editor, and delete the "Password" portion of the file. The log in to the account without password. You will be prompted to assign a new password.
E. Launch cpconfig and delete the Administrator's account. Recreate the account with the same name.

Answer: E

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

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

QUESTION 102:

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

A. It is not possible to export an old log file, only save and switch in SmartView Tracker.
B. Current logs are exported to a new *.log file.
C. Exported log entries are still viewable in SmartView Tracker.
D. Exported log entries are deleted from fw.log.
E. Logs in fw.log are exported to a file that can be opened by Microsoft Excel.

Answer: C

QUESTION 103:

Which type of TCP attack is a bandwidth attack, where a client fools a server into sending large amount of data, using small packets?

A. SMURF
B. Small PMTU
C. Host System Hogging
D. LAN
E. SYN-Flood

Answer: B

QUESTION 104:

What is the proper command for exporting users in LDAP format?

A. fw dbexport -f c:\temp\users.txt

B. fw dbimport -f c:\temp\users.ldif -l -s "o=YourCity.com,c=YourCountry"
C. fw dbimport -f c:\temp\users.ldap
D. fw dbexport -f c:\temp\users.ldap -l -s
E. fw dbexport -f c:\temp\users.ldif -l -s "o=YourCity.com,c=YourCountry"

Answer: E

Explanation:
In check point Security administration NGX1 1.1 on page 417 in Chapter 9: LDAP User Management with SMARTDIRECTORY (official courseware/book)
A typical command looks like the following example; Fwm dbexport -f c:\temp\users.ldif -l -s "o=yourcity.com,c=yourcountry"
This command exports all attributes for all users to the users.ldif file, in LDF format.
Export allows users to be imported into an LDAP server.

QUESTION 105:

Shauna is troubleshooting a Security Gateway that is dropping all traffic whenever the most recent Security Policy is installed. Working at the Security Gateway, Shauna needs to uninstall the Policy, but keep the processes running so she can see if there is an issue with the Gateway's firewall tables. Which of the following commands will do this?

A. fw dbload 10.1.1.5
B. fw unload 10.1.1.5
C. cprestart
D. fw tab -x -u
E. cpstop

Answer: D

Explanation:
tab -x -u displays kernel table content.
You want to uninstall not to load something.
Incorrect answers:
Not A, B: The question did not tell us anything about node 10.1.1.5.
Not A: Definitely wouldn't be A as fw dbload is used to download user/network objects to specific targets, and it specifically says in the question she wants to uninstall the security policy.

QUESTION 106:

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

A. In SmartView Status click the Blocked Intruder tab.

B. Run fwm blocked_view.
C. Run fw sam -va.
D. Run fw tab -t sam_blocked_ips.
E. In SmartView Tracker, click the Active tab, and the actively blocked connections display.

Answer: D

QUESTION 107:

Your internal Web server in the DMZ has IP address 172.16.10.1/24. A particular network from the Internet tries to access this Web server. You need to set up some type of Network Address Translation (NAT), so that NAT occurs only from the HTTP service, and only from the remote network as the source. The public IP address for the Web server is 200.200.200.1. All properties in the NAT screen of Global Properties are enabled.
Select the correct NAT rules, so NAT happens ONLY between "web_dallas" and the remote network.

A. 1. Create another node object named "web_dallas_valid", and enter "200.200.200.1" in the General Properties screen.
2. Create two manual NAT rules above the automatic Hide NAT rules for the 172.16.10.0 network.
3. Select "HTTP" in the Service column of both manual NAT rules.
4. Enter an ARP entry and route on the Security Gateway's OS.
B. 1. Enable NAT on the web_dallas object, select "static", and enter "200.200.200.1" in the General Properties screen.
2. Specify "HTTP" in the automatic Static Address Translation rules.
3. Create incoming and outgoing rules for the web_dallas server, for the HTTP service only.
C. 1. Enable NAT on the web_dallas object, select "hide", and enter "200.200.200.1" for the Hide NAT IP address.
2. Specify "HTTP" in the Address Translation rules that are generated automatically.
3. Create incoming and outgoing rules for the web_dallas server, for the HTTP service only.
D. 1. Create another node object named "web_dallas_valid", and enter "200.200.200.1" in the General Properties screen.
2. Create two manual NAT rules below the Automatic Hide NAT rules for network 172.16.10.0, in the Address Translation Rule Base.
3. Select "HTTP" in the Service column of both manual NAT rules.
4. Enter an ARP entry and route on the Security Gateway's OS.

Answer: A

Explanation: Note Automatic NAT has defined order for placing rules into the rule base. The gateway installs Static NAT rules first, then Hide NAT rules. Within

Static and NAT rules, node objects are first,then address ranges, and finally networks.
See configuring _check_point_NGX_VPN-1_Firewall-1-R page 235

QUESTION 108:

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

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

Answer: D

Explanation:
The question is tricky and a play on words, a 'sweep' is a scan on specific ports across multiple servers - which fits the answer.

QUESTION 109:

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. Administrators should be able to view backed up logs in SmartView Tracker.
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 logexport. Configure the organization's routine backup software to back up the export log every night.
Jack's plan:

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

D. Does not meet the required objective.

Answer: B

Explanation: Logs can be viewed after exported.

QUESTION 110:

Anna is working at Certkiller .com, together with three other Security Administrators. Which SmartConsole tool should she use to check changes to rules or object properties other administrators made?

A. SmartDashboard
B. SmartView Tracker
C. Eventia Tracker
D. Eventia Monitor
E. SmartView Monitor

Answer: B

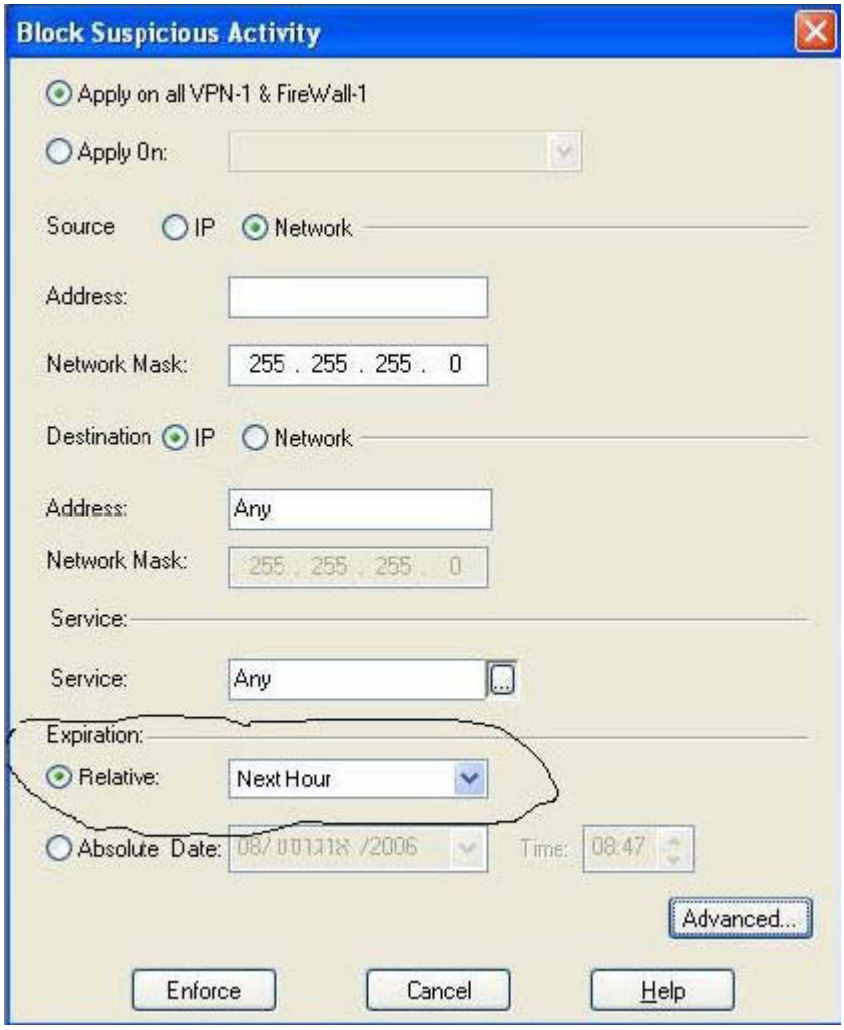
QUESTION 111:

When you find a suspicious connection from a problematic host, you want to block everything from that whole network, not just the host. You want to block this for an hour, but you do not want to add any rules to the Rule Base. How do you achieve this?

A. Create a Suspicious Activity rule in SmartView Tracker.
B. Create a Suspicious Activity Rule in SmartView.
C. Create an "FW SAM" rule in SmartView Monitor.
D. Select "block intruder" from the Tools menu in the SmartView Tracker.

Answer: B

Explanation:
They want to block the whole network not from specific node.
It is indeed possible to block for an hour using the Suspicious Activity Rule. See screenshot:



Not D: Block intruder block the source only.

QUESTION 112:

Your internal network is using 10.1.1.0/24. This network is behind your perimeter NGX VPN-1 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. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
C. Use manual Static NAT on the client side for network 10.1.1.0/24
D. Use Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter Gateway.
E. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.

Answer: D

QUESTION 113:

Which of these changes to a Security Policy optimizes Security Gateway performance?

A. Using domain objects in rules when possible
B. Using groups within groups in the manual NAT Rule Base
C. Putting the least-used rule at the top of the Rule Base
D. Logging rules as much as possible
E. Removing old or unused Security Policies from Policy Packages

Answer: E

QUESTION 114:

Nelson is a consultant. He is at a customer's site reviewing configuration and logs as a part of a security audit. Nelson sees logs accepting POP3 traffic, but he does not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause? The POP3:

A. service is a VPN-1 Control Connection.
B. rule is hidden.
C. service is accepted in Global Properties.
D. service cannot be controlled by NGX.
E. rule is disabled.

Answer: B

QUESTION 115:

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

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

Answer: E

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

QUESTION 116:

Mary is the IT auditor for a bank. One of her responsibilities is reviewing the Security Administrators activity and comparing it to the change log. Which application should Mary use to view Security Administrator activity?

A. NGX cannot display Security Administrator activity
B. SmartView Tracker in Real-Time Mode
C. SmartView Tracker in Audit Mode
D. SmartView Tracker in Log Mode
E. SmartView Tracker in Activity Mode

Answer: C

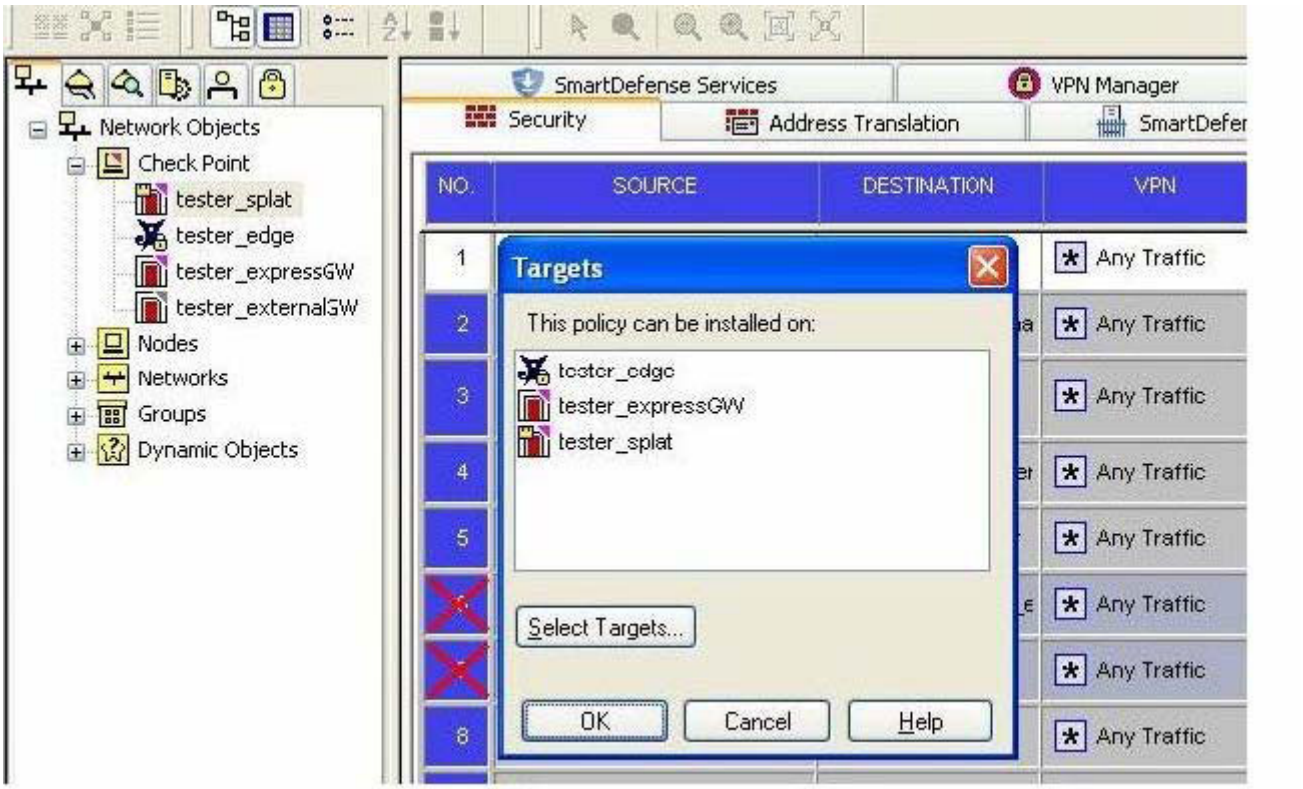
QUESTION 117:

Andrea has created a new gateway object that she will be managing at a remote location. She attempts to install the Security Policy to the new gateway object, but the object does not appear in the "install on" box. Which of the following is the most likely cause?

A. Andrea has created the object using "New Check Point > VPN-1 Edge Embedded Gateway"
B. Andrea created the gateway object using the "New Check Point > Externally Managed VPN Gateway" option from the Network Objects dialog box.
C. Andrea has not configured anti-spoofing on the interfaces on the gateway object.
D. Andrea has not configure Secure Internal Communications (SIC) for the oject.
E.
Andrea created the Object using "New Check Point > VPN-1 Pro/Express Security Gateway" option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B

Explanation:
Anti-spoofing configuration does not affect the ability to install the security policy on a gatway. No SIC configuration is required to install the security policy on a gateway. Both VPN-1 Edge gateways and VPN-1 Pro/Express gateways will appear in the list of selectable targets in SmartDashboard, but gateways created as externally managed will not (see screenshot)



QUESTION 118:

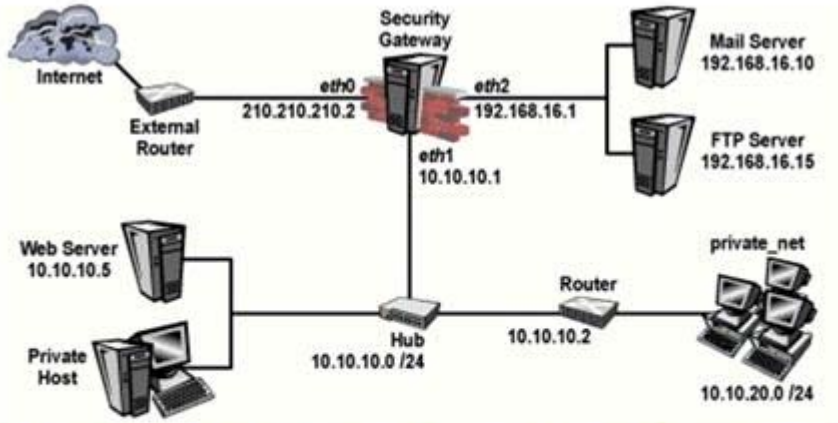
Certkiller is recently hired as the Security Administrator for Certkiller .com. Jack Bill's manager has asked her to investigate ways to improve the performance of the firm's perimeter Security Gateway. Certkiller must propose a plan based on the following required and desired results:
Required Result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

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

Answer: E

QUESTION 119:

You create implicit and explicit rules for the following network. The group object "internal-networks" include networks 10.10.10.0 and 10.10.20.0. Assume "Accept ICMP requests" is enabled as before last in the Global Properties.



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	smtp dns	accept	Log
3		Any	Any	Any Traffic	Any	drop	Log

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:

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 120:

What does schema checking do?

A.Authenticates users attempting to access resources protected by an NGX Security Gateway.

B. Verifies that every object class, and its associated attributes, is defined in the directory schema.
C. Maps LDAP objects to objects in the NGX objects_5_0.c files.
D. Verifies the Certificate Revocation List for Certificate Validity.
E. Provides topology downloads for SecuRemote and SecureClient users authenticated by an LDAP server.

Answer: B

QUESTION 121:

Jill is about to test some rule and object changes suggested in an NGX newsgroup. Which backup and restore solution should Jill use, to ensure she can most easily restore her Security Policy to its previous configuration, after testing the changes?

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

Answer: E

QUESTION 122:

You want VPN traffic to match packets from internal interfaces. You also want the traffic to exit the Security Gateway, bound for all site-to-site VPN Communities, including Remote Access Communities.
How should you configure the VPN match rule

A. internalclear>All-GwToGw
B. Communities>Communities
C. Internalclear>ExternalClear
D. Internalclear>Communities
E. Internalclear>Allcommunities

Answer: E

QUESTION 123:

Review the following rules and note the Client Authentication Action properties screen, as shown in the exhibit.
After being authenticated by the Security Gateway when a user starts an HTTP connection to a Web site the user tries to FTP to another site using the command line. What happens to the user?
The....

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

Answer: B

QUESTION 124:

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

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

Answer: D

Explanation:
cplic print - prints details of Check Point licenses on the local machine. On a Module, this command will print all licenses that are installed on the local machine - both Local and Central licenses.
P456, .
NG COMMAND LINE INTERFACE
Advanced Technical Reference Guide - NG FP3

QUESTION 125:

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

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

Answer: A

QUESTION 126:

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

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

Answer: B

Explanation:

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

427, Check Point Security Administration NGX I Student Handbook

---

QUESTION 127:

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

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

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

QUESTION 128:

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

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

Answer: D

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

QUESTION 129:

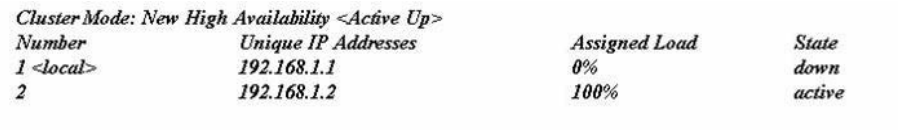
Which command allows you to view the contents of an NGX table?

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

Answer: B

QUESTION 130:

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



Cluster Mode: New High Availability <Active Up>

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

Which machine has the highest priority?

A. 192.168.1.2,since its number is 2
B. 192.168.1.1,because its number is 1
C. This output does not indicate which machine has the highest priority
D. 192.168.1.2, because its state is active

Answer: B

QUESTION 131:

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

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

Answer: D

QUESTION 132:

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

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

Answer: E

QUESTION 133:

Which of the following commands shows full synchronizalion status?

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

Answer: C

QUESTION 134:

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

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

Answer: A

QUESTION 135:

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

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

Answer: D

QUESTION 136:

Which operating system is not supported byVPN-1 SecureClient?

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

Answer: A

QUESTION 137:

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

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

Answer: D

QUESTION 138:

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

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

Answer: B

QUESTION 139:

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

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

Answer: A

QUESTION 140:

Certkiller is the Security Administrator for a software-development company. To isolate the corporate network from the developer's network, Certkiller installs an internal Security Gateway. Jack wants to optimize the performance of this Gateway. Which of the following actions is most likely to improve the Gateway's performance?

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

Answer: A

QUESTION 141:

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

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

Answer: E

QUESTION 142:

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

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

Address of SmartCenter Server>-.
D. From the SmartCenter Server's command line type fw putkey -p <shared key>- <IP Address of security Gateway>-.
E. Re-install the Security Gateway

Answer: B

QUESTION 143:

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

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

Answer: B

QUESTION 144:

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

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

Answer: D

QUESTION 145:

Certkiller is recently hired as the Security Administrator for a public relations company. Certkiller's manager has asked her to investigate ways to improve the performance of the firm's perimeter Security Gateway. Certkiller must propose a plan based on the following required and desired results
Required Result #1: Do not purchase new hardware
Required Result #2: Use configuration changes 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:
Certkiller recommends the following changes to the Gateway's configuration:
1. Replace all domain objects with network and group objects.
2. Stop logging Domain Name over UDP (queries)
3. Use Global Properties, instead of explicit rules, to control ICMP. VRRP, and RIP.
Does Certkiller's proposed solution meet the required and desired result s?

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

Answer: A

QUESTION 146:

What is a Consolidation Policy?

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

Answer: B

QUESTION 147:

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

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

Answer: A