# Exam Questions 156-215.77

Check Point Certified Security Administrator – GAiA

**https://www.2passeasy.com/dumps/156-215.77/**

**NEW QUESTION 1**
Several Security Policies can be used for different installation targets. The Firewall protecting Human Resources' servers should have its own Policy Package. These rules must be installed on this machine and not on the Internet Firewall.
How can this be accomplished?

A. A Rule Base is always installed on all possible target
B. The rules to be installed on a Firewall are defined by the selection in the Rule Base row Install On.
C. When selecting the correct Firewall in each line of the Rule Base row Install On, only this Firewall is shown in the list of possible installation targets after selecting Policy > Install on Target.
D. In the menu of SmartDashboard, go to Policy > Policy Installation Targets and select the correct firewall via Specific Targets.
E. A Rule Base can always be installed on any Check Point Firewall objec
F. It is necessary to select the appropriate target directly after selecting Policy > Install on Target.

**Answer:** C

**NEW QUESTION 2**
An internal host initiates a session to the Google.com website and is set for Hide NAT behind the Security Gateway. The initiating traffic is an example of .

A. client side NAT
B. source NAT
C. destination NAT
D. None of these

**Answer:** B

**NEW QUESTION 3**
Which of the following can be found in cpinfo from an enforcement point?

A. Everything NOT contained in the file r2info
B. VPN keys for all established connections to all enforcement points
C. The complete file objects_5_0.c
D. Policy file information specific to this enforcement point

**Answer:** D

**NEW QUESTION 4**
After filtering a fw monitor trace by port and IP, a packet is displayed three times; in the i, I, and o inspection points, but not in the O inspection point.
Which is the likely source of the issue?

A. The packet has been sent out through a VPN tunnel unencrypted.
B. An IPSO ACL has blocked the packet's outbound passage.
C. A SmartDefense module has blocked the packet.
D. It is due to NAT.

**Answer:** D

**NEW QUESTION 5**
The third-shift Administrator was updating Security Management Server access settings in Global Properties and testing. He managed to lock himself out of his account.
How can you unlock this account?

A. Type fwm unlock_admin from the Security Management Server command line.
B. Type fwm unlock_admin -u from the Security Gateway command line.
C. Type fwm lock_admin -u <account name> from the Security Management Server command line.
D. Delete the file admin.lock in the Security Management Server directory $FWDIR/tmp/.

**Answer:** C

**NEW QUESTION 6**
You are a Security Administrator who has installed Security Gateway R77 on your network. You need to allow a specific IP address range for a partner site to access your intranet Web server. To limit the partner's access for HTTP and FTP only, you did the following:
1) Created manual Static NAT rules for the Web server.
2) Cleared the following settings in the Global Properties > Network Address Translation screen:
- Allow bi-directional NAT
- Translate destination on client side
Do the above settings limit the partner's access?

A. Ye
B. This will ensure that traffic only matches the specific rule configured for this traffic, and that the Gateway translates the traffic after accepting the packet.
C. N
D. The first setting is not applicabl
E. The second setting will reduce performance.
F. Ye
G. Both of these settings are only applicable to automatic NAT rules.
H. N
I. The first setting is only applicable to automatic NAT rule

J. The second setting will force translation by the kernel on the interface nearest to the client.

**Answer:** D

**NEW QUESTION 7**
Your internal network is configured to be 10.1.1.0/24. This network is behind your perimeter R77 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 Hide NAT for network 10.1.1.0/24 behind the external IP address of your perimeter Gateway.
B. Use Hide NAT for network 10.1.1.0/24 behind the internal interface of your perimeter Gateway.
C. Use automatic Static NAT for network 10.1.1.0/24.
D. Do nothing, as long as 10.1.1.0 network has the correct default Gateway.

**Answer:** A

**NEW QUESTION 8**
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

**Answer:** D

**NEW QUESTION 9**
Many companies have defined more than one administrator. To increase security, only one administrator should be able to install a Rule Base on a specific Firewall.
How do you configure this?

A. Define a permission profile in SmartDashboard with read/write privileges, but restrict it to all other firewalls by placing them in the Policy Targets fiel
B. Then, an administrator with this permission profile cannot install a policy on any Firewall not listed here.
C. Put the one administrator in an Administrator group and configure this group in the specific Firewall object in Advanced > Permission to Install.
D. In the object General Properties representing the specific Firewall, go to the Software Blades product list and select Firewal
E. Right-click in the menu, select Administrator to Install to define only this administrator.
F. Right-click on the object representing the specific administrator, and select that Firewall in Policy Targets.

**Answer:** B

**NEW QUESTION 10**
Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want 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 the Internet?

A. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service.
B. Configure Automatic Static NAT on network 10.10.20.0/24.
C. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
D. Configure Automatic Hide NAT on network 10.10.20.0/24 and then edit the Service column in the NAT Rule Base on the automatic rule.

**Answer:** C

**NEW QUESTION 10**
You just installed a new Web server in the DMZ that must be reachable from the Internet. You create a manual Static NAT rule as follows:
Source: Any || Destination: web_public_IP || Service: Any || Translated Source: original || Translated Destination: web_private_IP || Service: Original
“web_public_IP” is the node object that represents the new Web server’s public IP address. “web_private_IP” is the node object that represents the new Web site’s private IP address. You enable all settings from Global Properties > NAT.
When you try to browse the Web server from the Internet you see the error “page cannot be displayed”.
Which of the following is NOT a possible reason?

A. There is no Security Policy defined that allows HTTP traffic to the protected Web server.
B. There is no ARP table entry for the protected Web server’s public IP address.
C. There is no route defined on the Security Gateway for the public IP address to the Web server’s private IP address.
D. There is no NAT rule translating the source IP address of packets coming from the protected Web server.

**Answer:** A

**NEW QUESTION 13**
After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your DMZ, you notice that any NATed connections to that machine are being dropped by anti-spoofing protections. Which of the following is the MOST LIKELY cause?

A. The Global Properties setting Translate destination on client side is unchecke
B. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
C. Check the Global Properties setting Translate destination on client side.
D. The Global Properties setting Translate destination on client side is unchecke
E. But the topology on the external interface is set to Others +. Change topology to External.
F. The Global Properties setting Translate destination on client side is checke
G. But the topology on the external interface is set to Externa

H. Change topology to Others +.
I. The Global Properties setting Translate destination on client side is checke
J. But the topology on the DMZ interface is set to Internal - Network defined by IP and Mas
K. Uncheck the Global Properties setting Translate destination on client side.

**Answer:** A

**NEW QUESTION 17**
Secure Internal Communications (SIC) is completely NAT-tolerant because it is based on:

A. IP addresses.
B. SIC is not NAT-tolerant.
C. SIC names.
D. MAC addresses.

**Answer:** C

**NEW QUESTION 18**
Which SmartConsole tool would you use to see the last policy pushed in the audit log?

A. SmartView Tracker
B. None, SmartConsole applications only communicate with the Security Management Server.
C. SmartView Status
D. SmartView Server

**Answer:** A

**NEW QUESTION 21**
When restoring R77 using the command upgrade_import, which of the following items are NOT restored?

A. SIC Certificates
B. Licenses
C. Route tables
D. Global properties

**Answer:** C

**NEW QUESTION 22**
By default, when you click File > Switch Active File in SmartView Tracker, the Security Management Server:

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

**Answer:** A

**NEW QUESTION 25**
Which of the following statements BEST describes Check Point's Hide Network Address Translation method?

A. Translates many destination IP addresses into one destination IP address
B. One-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation
C. Translates many source IP addresses into one source IP address
D. Many-to-one NAT which implements PAT (Port Address Translation) for accomplishing both Source and Destination IP address translation

**Answer:** C

**NEW QUESTION 27**
Which R77 feature or command allows Security Administrators to revert to earlier Security Policy versions without changing object configurations?

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

**Answer:** C

**NEW QUESTION 31**
Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

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

**Answer:** A

**NEW QUESTION 35**
SmartView Tracker R77 consists of three different modes. They are:

A. Log, Active, and Audit
B. Log, Active, and Management
C. Network and Endpoint, Active, and Management
D. Log, Track, and Management

**Answer:** C

**NEW QUESTION 38**
What happens when you select File > Export from the SmartView Tracker menu?

A. Current logs are exported to a new *.log file.
B. Exported log entries are not viewable in SmartView Tracker.
C. Logs in fw.log are exported to a file that can be opened by Microsoft Excel.
D. Exported log entries are deleted from fw.log.

**Answer:** C

**NEW QUESTION 41**
You are the Security Administrator for ABC-Corp. A Check Point Firewall is installed and in use on GAiA. You are concerned that the system might not be retaining your entries for the
interfaces and routing configuration. You would like to verify your entries in the corresponding file(s) on GAiA. Where can you view them? Give the BEST answer.

A. /etc/sysconfig/netconf.C
B. /etc/conf/route.C
C. /etc/sysconfig/network-scripts/ifcfg-ethx
D. /etc/sysconfig/network

**Answer:** A

**NEW QUESTION 45**
You have created a Rule Base for firewall, websydney. Now you are going to create a new policy package with security and address translation rules for a second Gateway. What is TRUE about the new package's NAT rules?
Exhibit:

| NO. | ORIGINAL PACKET | | | TRANSLATED PACKET | | | INSTALL ON |
|---|---|---|---|---|---|---|---|
| | SOURCE | DESTINATION | SERVICE | SOURCE | DESTINATION | SERVICE | |
| 1 | websydney | Any | Any | websydney (Hid | Original | Original | fwsydney |
| 2 | net_singapore | net_singapore | Any | Original | Original | Original | All |
| 3 | net_singapore | Any | Any | net_singapore (H | Original | Original | All |
| 4 | Any | websydney | Any | Original | websydney | Original | Policy Targets |
| 5 | Any | websingapore | HTTP_and_HTTPS | Original | Original | http | Policy Targets |

A. Rules 1, 2, 3 will appear in the new package.
B. Only rule 1 will appear in the new package.
C. NAT rules will be empty in the new package.
D. Rules 4 and 5 will appear in the new package.

**Answer:** A

**NEW QUESTION 46**
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After awhile, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database.
How can you do this?

A. Run fwm dbexport -l filenam
B. Restore the databas
C. Then, run fwm dbimport -l filename to import the users.
D. Run fwm_dbexport to export the user databas
E. Select restore the entire database in the Database Revision scree
F. Then, run fwm_dbimport.
G. Restore the entire database, except the user database, and then create the new user and user group.
H. Restore the entire database, except the user database.

**Answer:** D

**NEW QUESTION 49**
You plan to create a backup of the rules, objects, policies, and global properties from an R77 Security Management Server. Which of the following backup and restore solutions can you use?

1. `upgrade_export` and `upgrade_import` utilities
2. Database revision control
3. SecurePlatform backup utilities
4. Policy package management
5. Manual copies of the `$CPDIR/conf` directory

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

**Answer:** C

**NEW QUESTION 50**
How many packets does the IKE exchange use for Phase 1 Aggressive Mode?

A. 12
B. 6
C. 3
D. 1

**Answer:** C

**NEW QUESTION 52**
Exhibit:

1. Run `cpconfig` on the Gateway, select **Secure Internal Communication**, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the **Communication** button in the Gateway object's **General** screen, enter the activation key, and click **Initialize** and **OK**.
5. Install the Security Policy.

You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to ship to another Administrator at a MegaCorp hub office.
What is the correct order for pushing SIC certificates to the Gateway before shipping it?

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

**Answer:** B

**NEW QUESTION 53**
Which of the following is a viable consideration when determining Rule Base order?

A. Grouping IPS rules with dynamic drop rules
B. Placing more restrictive rules before more permissive rules
C. Grouping authentication rules with QOS rules
D. Grouping reject and drop rules after the Cleanup Rule

**Answer:** B

**NEW QUESTION 58**
Security Gateway R77 supports User Authentication for which of the following services? Select the response below that contains the MOST correct list of supported services.

A. SMTP, FTP, TELNET
B. SMTP, FTP, HTTP, TELNET
C. FTP, HTTP, TELNET
D. FTP, TELNET

**Answer:** C

**NEW QUESTION 61**
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

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

**Answer:** B

**NEW QUESTION 63**
Which of the following are authentication methods that Security Gateway R77 uses to validate connection attempts? Select the response below that includes the MOST complete list of valid authentication methods.

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

**Answer:** C

**NEW QUESTION 68**
You are troubleshooting NAT entries in SmartView Tracker. Which column do you check to view the new source IP?
Exhibit:

| | | |
|---|---|---|
| URL List Version | ☐ | 100 |
| Unreachable directories | ☐ | 100 |
| Update Service | ☐ | 100 |
| Update Source | ☐ | 100 |
| Update Status | ☐ | 100 |
| User Action Comment | ☐ | 100 |
| User Additional Information | ☐ | 100 |
| User Check | ☐ | 1 |
| User DN | ☐ | 100 |
| User Directory | ☐ | 100 |
| User Display Name | ☐ | 100 |
| User Group | ☐ | 100 |
| User Reported Wrong Category | ☐ | 100 |
| User Response | ☐ | 50 |
| User SID | ☐ | 100 |
| User UID | ☐ | 100 |
| User's IP | ☐ | 100 |
| UserCheck ID | ☐ | 100 |
| UserCheck Interaction Name | ☐ | 100 |
| UserCheck Message to User | ☐ | 100 |
| UserCheck Scope | ☐ | 100 |
| UserCheck User Input | ☐ | 100 |
| VLAN ID | ☐ | 100 |
| VPN Feature | ☐ | 100 |
| VPN Peer Gateway | ☐ | 100 |
| Version | ☐ | 100 |
| Virtual Link | ☐ | 100 |
| Virus Name | ☐ | 100 |
| VoIP Duration | ☐ | 100 |
| VoIP Log Type | ☐ | 100 |
| VoIP Reject Reason | ☐ | 100 |
| VoIP Reject Reason Information | ☐ | 100 |
| Web Filtering Categories | ☐ | 100 |
| Wire Byte/Sec Out | ☐ | 100 |
| Wire Byte/Sec in | ☐ | 100 |
| Wire Packet/Sec Out | ☐ | 100 |
| Wire Packet/Sec in | ☐ | 100 |
| Write Access | ☐ | 100 |
| XlateDPort | ☐ | 100 |
| XlateDst | ☐ | 100 |
| XlateSPort | ☐ | 100 |
| XlateSrc | ☐ | 100 |
| special properties | ☐ | 100 |

A. XlateDPort
B. XlateDst
C. XlateSPort
D. XlateSrc

**Answer:** D

**NEW QUESTION 71**
Captive Portal is a that allows the gateway to request login information from the user.

A. Pre-configured and customizable web-based tool
B. Transparent network inspection tool
C. LDAP server add-on
D. Separately licensed feature

**Answer:** A

**NEW QUESTION 73**

The Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). What is not a recommended usage of this method?

A. When accuracy in detecting identity is crucial
B. Leveraging identity for Data Center protection
C. Protecting highly sensitive servers
D. Identity based enforcement for non-AD users (non-Windows and guest users)

**Answer:** D

**NEW QUESTION 76**
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

A. Secure Internal Communications (SIC) not configured for the object.
B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
C. Anti-spoofing not configured on the interfaces on the Gateway object.
D. A Gateway object created using the Check Point > Security Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

**Answer:** D

**NEW QUESTION 80**
Which of the following describes the default behavior of an R77 Security Gateway?

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

**Answer:** A

**NEW QUESTION 85**
Which of the following is an authentication method used by Identity Awareness?

A. SSL
B. Captive Portal
C. RSA
D. PKI

**Answer:** B

**NEW QUESTION 86**
In the Rule Base displayed, user authentication in Rule 4 is configured as fully automatic.
Eric is a member of the LDAP group, MSD_Group.

| No. | Hits | Name | Source | Destination | VPN | Service | Action | Track | Install On |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | NetBIOS | Any | Any | Any Traffic | NBT | drop | Log | Policy Targets |
| 2 | 0 | Management | webSingapore | fwsingapore | Any Traffic | ssh<br>https | accept | None | Policy Targets |
| 3 | 0 | Stealth | Any | fwsingapore | Any Traffic | Any | drop | Log | Policy Targets |
| 4 | 0 | Authentication | MSAD_Group@net_singapore | Any | Any Traffic | http | User Auth | Log | Policy Targets |
| 5 | 0 | Partner City | net_singapore<br>net_frankfurt | net_frankfurt<br>net_singapore | frankfurt_singapore | Any | accept | Log | Policy Targets |
| 6 | 0 | Network Traffic | net_singapore<br>net_sydney | Any | Any Traffic | ftp<br>icmp-proto<br>https<br>http<br>dns | accept | Log | Policy Targets |
| 7 | 0 | Cleanup | Any | Any | Any Traffic | Any | drop | Log | Policy Targets |

What happens when Eric tries to connect to a server on the Internet?

A. None of these things will happen.
B. Eric will be authenticated and get access to the requested server.
C. Eric will be blocked because LDAP is not allowed in the Rule Base.
D. Eric will be dropped by the Stealth Rule.

**Answer:** B

**NEW QUESTION 89**
Which rule is responsible for the installation failure? Exhibit:

| NO. | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON |
|---|---|---|---|---|---|---|---|---|
| 1 | NetBIOS Rule | Any | Any | Any Traffic | NBT | drop | None | Policy Targets |
| 2 | Mgmt Rule | websingapore | fwsingapore | Any Traffic | ssh<br>https | accept | None | Policy Targets |
| 3 | Web Server Rule | Any | websingapore | Any Traffic | http | Client Auth | Log | Policy Targets |
| 4 | Stealth Rule | Any | fwsingapore | Any Traffic | Any | drop | Log | Policy Targets |
| 5 | Partner City Rule | net_singapore<br>net_rome | net_singapore<br>net_rome | Rome_Singapore | http | accept | Log | Policy Targets |
| 6 | Network Traffic Rule | net_singapore<br>net_sydney | Any | Any Traffic | dns<br>icmp-proto<br>ftp<br>https<br>http | accept | Log | Policy Targets |
| 7 | Network Traffic Rule | websydney | Any | Any Traffic | ftp | reject | Log | Policy Targets |
| 8 | Cleanup Rule | Any | Any | Any Traffic | Any | drop | Log | Policy Targets |

A. Rule 3
B. Rule 4
C. Rule 6
D. Rule 5

**Answer:** C

**NEW QUESTION 94**
Which of the following allows administrators to allow or deny traffic to or from a specific network based on the user's credentials?

A. Access Policy
B. Access Role
C. Access Rule
D. Access Certificate

**Answer:** B

**NEW QUESTION 99**
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

A. The two algorithms do not have the same key length and so don't work togethe
B. You will get the error …. No proposal chosen….
C. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
D. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
E. All is fine and can be used as is.

**Answer:** C

**NEW QUESTION 102**
Users with Identity Awareness Agent installed on their machines login with , so that when the user logs into the domain, that information is also used to meet Identity Awareness credential requests.

A. Key-logging
B. ICA Certificates
C. SecureClient
D. Single Sign-On

**Answer:** D

**NEW QUESTION 103**
Which of the following actions do NOT take place in IKE Phase 1?

A. Peers agree on encryption method.
B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
C. Peers agree on integrity method.
D. Each side generates a session key from its private key and the peer's public key.

**Answer:** B

**NEW QUESTION 105**
You would use the Hide Rule feature to:

A. View only a few rules without the distraction of others.
B. Hide rules from read-only administrators.
C. Hide rules from a SYN/ACK attack.
D. Make rules invisible to incoming packets.

**Answer:** A

**NEW QUESTION 108**
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.
To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
Ms. McHanry tries to access the resource but is unable. What should she do?

A. Have the security administrator select the Action field of the Firewall Rule “Redirect HTTP connections to an authentication (captive) portal?
B. Have the security administrator reboot the firewall
C. Have the security administrator select Any for the Machines tab in the appropriate Access Role
D. Install the Identity Awareness agent on her iPad

**Answer:** A

**NEW QUESTION 109**
You have installed a R77 Security Gateway on GAiA. To manage the Gateway from the enterprise Security Management Server, you create a new Gateway object and Security Policy. When you install the new Policy from the Policy menu, the Gateway object does not appear in the Install Policy window as a target. What is the problem?

A. The object was created with Node > Gateway.
B. No Masters file is created for the new Gateway.
C. The Gateway object is not specified in the first policy rule column Install On.
D. The new Gateway's temporary license has expired.

**Answer:** A

**NEW QUESTION 112**
Certificates for Security Gateways are created during a simple initialization from ____.

A. sysconfig
B. The ICA management tool
C. SmartUpdate
D. SmartDashboard

**Answer:** D

**NEW QUESTION 113**
How can you activate the SNMP daemon on a Check Point Security Management Server?

A. Using the command line, enter snmp_install.
B. From cpconfig, select SNMP extension.
C. Any of these options will work.
D. In SmartDashboard, right-click a Check Point object and select Activate SNMP.

**Answer:** B

**NEW QUESTION 116**
Which of the following commands can be used to remove site-to-site IPsec Security Association (SA)?

A. vpn debug ipsec
B. vpn ipsec
C. fw ipsec tu
D. vpn tu

**Answer:** D

**NEW QUESTION 120**
How many packets are required for IKE Phase 2?

A. 12
B. 2
C. 6
D. 3

**Answer:** D

**NEW QUESTION 121**
The User Directory Software Blade is used to integrate which of the following with Security Gateway R77?

A. RADIUS server
B. Account Management Client server
C. UserAuthority server
D. LDAP server

**Answer:** D

**NEW QUESTION 126**
Which type of R77 Security Server does not provide User Authentication?

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

**Answer:** A

**NEW QUESTION 129**
Identify the ports to which the Client Authentication daemon listens by default.

A. 259, 900
B. 256, 600
C. 80, 256
D. 8080, 529

**Answer:** A

**NEW QUESTION 130**
John is the Security Administrator in his company. He installs a new R77 Security Management Server and a new R77 Gateway. He now wants to establish SIC between them. After entering the activation key, he gets the following message in SmartDashboard -
“Trust established?”
SIC still does not seem to work because the policy won’t install and interface fetching does not work. What might be a reason for this?

A. SIC does not function over the network.
B. It always works when the trust is established
C. The Gateway’s time is several days or weeks in the future and the SIC certificate is not yet valid.
D. This must be a human error.

**Answer:** C

**NEW QUESTION 134**
Match the following commands to their correct function. Each command has one function only listed.
Exhibit:

| Command | Function |
|---|---|
| C1 `cp_admin_convert` | F1: export and import different revisions of the database. |
| C2 `cpca_client` | F2: export and import policy packages. |
| C3 `cp_merge` | F3: transfer Log data to an external database. |
| C4 `cpwd_admin` | F4: execute operations on the ICA. |
| | F5: invokes and monitors critical processes such as Check Point daemons on the local machine. |
| | F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard. |

A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F2; C2>F1; C3>F6; C4>F4
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F4; C2>F6; C3>F3; C4>F2

**Answer:** A

**NEW QUESTION 139**
An Administrator without access to SmartDashboard installed a new IPSO-based R77 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway applianc
B. Resolve by running the command fw unloadlocal on the local Security Gateway.
C. You first need to run the command fw unloadlocal on the R77 Security Gateway appliance in order to remove the restrictive default policy.
D. You first need to create a new Gateway object in SmartDashboard, establish SIC via the Communication button, and define the Gateway’s topology.
E. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Serve
F. You must initialize SIC on the Security Management Server.

**Answer:** C

**NEW QUESTION 143**
When using LDAP as an authentication method for Identity Awareness, the query:

A. Requires client and server side software.
B. Prompts the user to enter credentials.
C. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.
D. Is transparent, requiring no client or server side software, or client intervention.

**Answer:** D

**NEW QUESTION 146**
If a Security Gateway enforces three protections, LDAP Injection, Malicious Code Protector, and Header Rejection, which Check Point license is required in SmartUpdate?

A. IPS
B. SSL: VPN
C. SmartEvent Intro
D. Data Loss Prevention

**Answer:** A

**NEW QUESTION 151**
You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

A. You checked the cache password on desktop option in Global Properties.
B. Another rule that accepts HTTP without authentication exists in the Rule Base.
C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
D. Users must use the SecuRemote Client, to use the User Authentication Rule.

**Answer:** B

**NEW QUESTION 154**
Several Security Policies can be used for different installation targets. The firewall protecting Human Resources' servers should have a unique Policy Package. These rules may only be installed on this machine and not accidentally on the Internet firewall. How can this be configured?

A. When selecting the correct firewall in each line of the row Install On of the Rule Base, only this firewall is shown in the list of possible installation targets after selecting Policy > Install.
B. A Rule Base can always be installed on any Check Point firewall objec
C. It is necessary to select the appropriate target directly after selecting Policy > Install.
D. In the SmartDashboard policy, select the correct firewall to be the Specific Target of the rule.
E. A Rule Base is always installed on all possible target
F. The rules to be installed on a firewall are defined by the selection in the row Install On of the Rule Base.

**Answer:** C

**NEW QUESTION 159**
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
B. If the user credentials do not match an Access Role, the system displays a sandbox.
C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

**Answer:** C

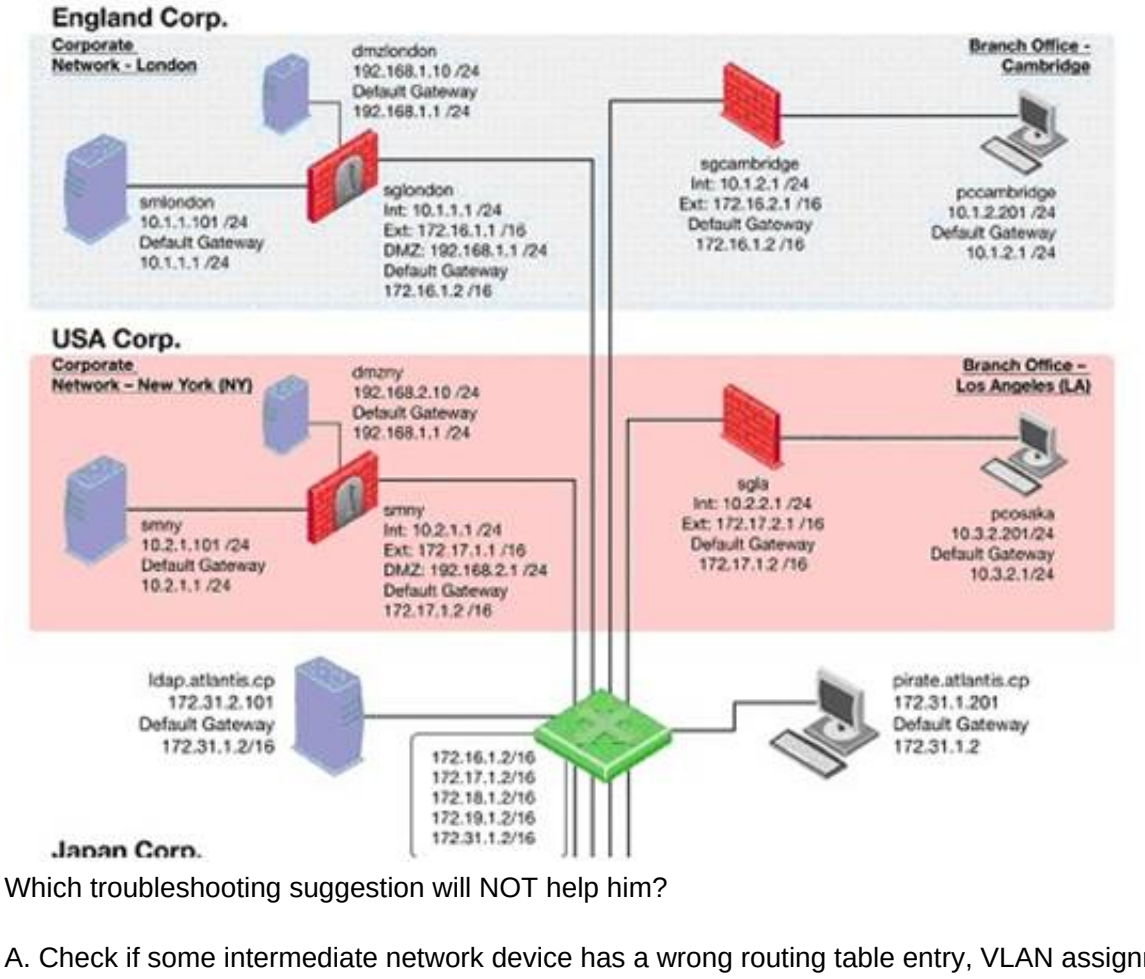
**NEW QUESTION 160**
As you review this Security Policy, what changes could you make to accommodate Rule 4? Exhibit:

| No. | Hits | Name | Source | Destination | VPN | Service | Action |
|---|---|---|---|---|---|---|---|
| | Limit Access to Gateways (Rule 1) | | | | | | |
| 1 | 0 | Stealth | Corporate-internal-net | GW-group | Any Traffic | Any | drop |
| | VPN Access Rules (Rules 2-5) | | | | | | |
| 2 | 0 | Site-to-Site | Any | Any | Any Traffic | CIFS<br>ftp-port<br>http<br>https<br>smtp | accept |
| 3 | 0 | Remote Access | Mobile-vpn-user@Any | Any | RemoteAccess | CIFS<br>http<br>https<br>imap | accept |
| 4 | 0 | Clientless VPN | Clientless-vpn-user@Any | Corporate-WA-proxy-server | Any Traffic | https | User Auth |
| 5 | 0 | Web Server | L2TP-vpn-user@Any<br>Customers@Any | Remote-1-web-server | Any Traffic | http | accept |

A. Remove the service HTTP from the column Service in Rule 4.
B. Modify the column VPN in Rule 2 to limit access to specific traffic.
C. Nothing at all
D. Modify the columns Source or Destination in Rule 4.

**Answer:** B

**NEW QUESTION 164**
The London Security Gateway Administrator has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect.




Which troubleshooting suggestion will NOT help him?

A. Check if some intermediate network device has a wrong routing table entry, VLAN assignment, duplex-mismatch, or trunk issue.
B. Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.
C. Verify the SIC initialization.
D. Verify that the Rule Base explicitly allows management connections.

**Answer:** D

**NEW QUESTION 167**
The Security Gateway is installed on GAiA R77 The default port for the Web User Interface is .

A. TCP 18211
B. TCP 443
C. TCP 4433
D. TCP 257

**Answer:** B

**NEW QUESTION 169**
You have included the Cleanup Rule in your Rule Base. Where in the Rule Base should the Accept ICMP Requests implied rule have no effect?

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

**Answer:** A

**NEW QUESTION 172**
Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway. After selecting Packages > Distribute and Install Selected Package and choosing the target Gateway, the:

A. selected package is copied from the Package Repository on the Security Management Server to the Security Gateway and the installation IS performed.
B. SmartUpdate wizard walks the Administrator through a distributed installation.
C. selected package is copied from the Package Repository on the Security Management Server to the Security Gateway but the installation IS NOT performed.
D. selected package is copied from the SmartUpdate PC CD-ROM directly to the Security Gateway and the installation IS performed.

**Answer:** A

**NEW QUESTION 175**
In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule must be created to allow the server to communicate to the Security Gateway on port _____

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

**Answer:** C

**NEW QUESTION 180**
What physical machine must have access to the User Center public IP address when checking for new packages with SmartUpdate?

A. A Security Gateway retrieving the new upgrade package
B. SmartUpdate installed Security Management Server PC
C. SmartUpdate GUI PC
D. SmartUpdate Repository SQL database Server

**Answer:** C

**NEW QUESTION 184**
Which rule position in the Rule Base should hold the Cleanup Rule? Why?

A. Firs
B. It explicitly accepts otherwise dropped traffic.
C. Las
D. It explicitly drops otherwise accepted traffic.
E. Las
F. It serves a logging function before the implicit drop.
G. Before last followed by the Stealth Rule.

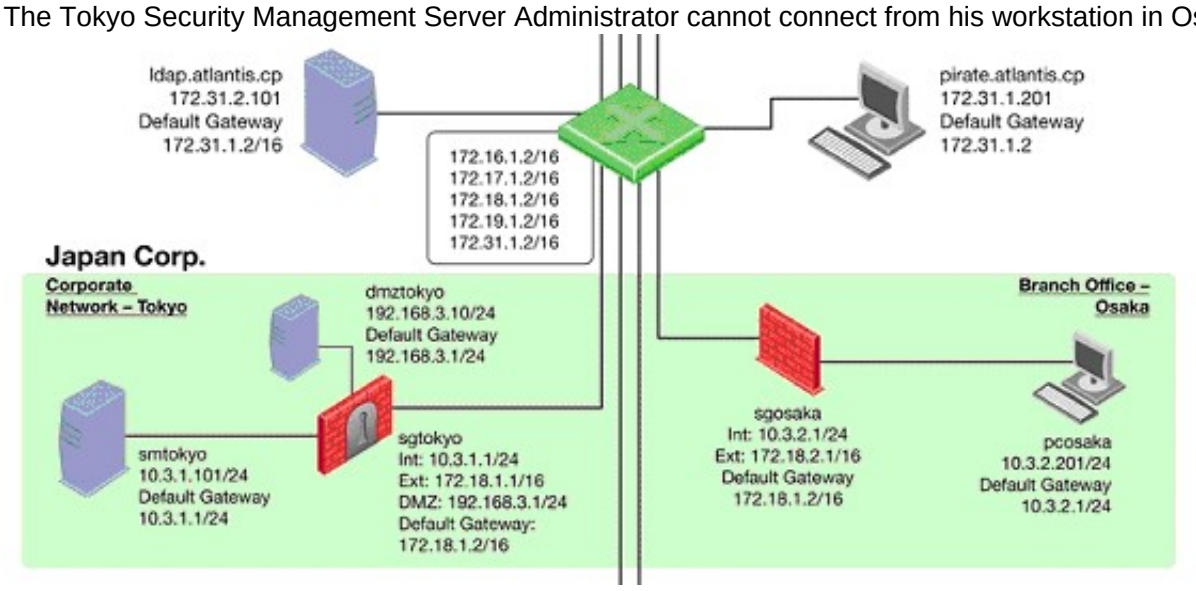
**Answer:** C

**NEW QUESTION 186**
You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? (i.e. the command cprestart is not sufficient.)
1. Adding a hot-swappable NIC to the Operating System for the first time.
2. Uninstalling the R77 Power/UTM package.
3. Installing the R77 Power/UTM package.
4. Re-establishing SIC to the Security Management Server.
5. Doubling the maximum number of connections accepted by the Security Gateway.

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

**Answer:** C

**NEW QUESTION 188**
The Tokyo Security Management Server Administrator cannot connect from his workstation in Osaka.




Which of the following lists the BEST sequence of steps to troubleshoot this issue?

A. Check for matching OS and product versions of the Security Management Server and the clien
B. Then, ping the Gateways to verify connectivit
C. If successful, scan the log filesfor any denied management packets.
D. Verify basic network connectivity to the local Gateway, service provider, remote Gateway, remote network and target machin
E. Then, test for firewall rules that deny management access to the targe
F. If successful, verify that pcosaka is a valid client IP address.
G. Check the allowed clients and users on the Security Management Serve
H. If pcosaka and your user account are valid, check for network problem
I. If there are no network related issues, this is likely to be a problem with the server itsel
J. Check for any patches and upgrade
K. If still unsuccessful, open a case with Technical Support.
L. Call Tokyo to check if they can ping the Security Management Server locall
M. If so, login to sgtokyo, verify management connectivity and Rule Bas
N. If this looks okay, ask your provider if they have some firewall rules that filters out your management traffic.

**Answer:** B

**NEW QUESTION 189**
All of the following are Security Gateway control connections defined by default implied rules, EXCEPT:

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

**Answer:** A

**NEW QUESTION 194**
Where do you verify that UserDirectory is enabled?

A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > UseUserDirectory (LDAP) for Security Gateways is checked
D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked

**Answer:** D

**NEW QUESTION 196**
How do you configure the Security Policy to provide user access to the Captive Portal through an external (Internet) interface?

A. Change the gateway settings to allow Captive Portal access via an external interface.
B. No action is necessar
C. This access is available by default.
D. Change the Identity Awareness settings under Global Properties to allow Captive Portal access on all interfaces.
E. Change the Identity Awareness settings under Global Properties to allow Captive Portal access for an external interface.

**Answer:** A

**NEW QUESTION 199**
What action CANNOT be run from SmartUpdate R77?

A. Fetch sync status
B. Reboot Gateway
C. Preinstall verifier
D. Get all Gateway Data

**Answer:** A

**NEW QUESTION 202**
You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify security administration, which one of the following would you choose to do?

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

**Answer:** D

**NEW QUESTION 204**
Central license management allows a Security Administrator to perform which of the following functions?
1. Check for expired licenses.
2. Sort licenses and view license properties.
3. Attach both R77 Central and Local licesnes to a remote module.
4. Delete both R77 Local Licenses and Central licenses from a remote module.
5. Add or remove a license to or from the license repository.
6. Attach and/or delete only R77 Central licenses to a remote module (not Local licenses).

A. 1, 2, 5, & 6
B. 2, 3, 4, & 5
C. 2, 5, & 6
D. 1, 2, 3, 4, & 5

**Answer:** D

**NEW QUESTION 207**
What CANNOT be configured for existing connections during a policy install?

A. Keep all connections
B. Keep data connections
C. Re-match connections
D. Reset all connections

**Answer:** D

**NEW QUESTION 209**

Suppose the Security Gateway hard drive fails and you are forced to rebuild it. You have a snapshot file stored to a TFTP server and backups of your Security Management Server.
What is the correct procedure for rebuilding the Gateway quickly?

A. Reinstall the base operating system (i.e., GAiA). Configure the Gateway interface so that the Gateway can communicate with the TFTP serve
B. Revert to the stored snapshot image, and install the Security Policy.
C. Run the command revert to restore the snapshot, establish SIC, and install the Policy.
D. Run the command revert to restore the snapsho
E. Reinstall any necessary Check Point product
F. Establish SIC and install the Policy.
G. Reinstall the base operating system (i.e., GAia). Configure the Gateway interface so that the Gateway can communicate with the TFTP serve
H. Reinstall any necessary Check Point products and previously applied hotfixe
I. Revert to the stored snapshot image, and install the Policy.

**Answer:** A

**NEW QUESTION 212**
What command syntax would you use to see accounts the gateway suspects are service accounts?

A. pdp check_log
B. pdp show service
C. adlog check_accounts
D. adlog a service_accounts

**Answer:** D

**NEW QUESTION 216**
What statement is true regarding Visitor Mode?

A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
B. Only ESP traffic is tunneled through port TCP 443.
C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
D. All VPN traffic is tunneled through UDP port 4500.

**Answer:** A

**NEW QUESTION 221**
SmartUpdate is mainly for which kind of work –
1. Monitoring Performance and traffic
2. Provision Package
3. Managing licenses
4. Creating a Rule Base

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

**Answer:** A

**NEW QUESTION 225**
Which of the following is NOT an option for internal network definition of Anti-spoofing?

A. Specific – derived from a selected object
B. Route-based – derived from gateway routing table
C. Network defined by the interface IP and Net Mask
D. Not-defined

**Answer:** B

**NEW QUESTION 229**
What action can be performed from SmartUpdate R77?

A. upgrade_export
B. fw stat -l
C. cpinfo
D. remote_uninstall_verifier

**Answer:** C

**NEW QUESTION 230**
A third-shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. Which SmartConsole component would you use to verify this?

A. Eventia Analyzer
B. SmartView Tracker

C. SmartView Monitor
D. This information can only be viewed with the command fw ctl pstat from the CLI.

**Answer:** C

**NEW QUESTION 231**
Is it possible to see user activity in SmartView Tracker?

A. Yes, seeing user activity is enabled when using the Identity Awareness blade.
B. No, a Check Point Gateway can only see IP addresses.
C. Yes, but you have to enable the option: See user information in SmartView Tracker.
D. Yes, but you need to use the SPLAT operating system.

**Answer:** A

**NEW QUESTION 232**
What is also referred to as Dynamic NAT?

A. Automatic NAT
B. Static NAT
C. Manual NAT
D. Hide NAT

**Answer:** D

**NEW QUESTION 237**
Choose the correct statement regarding Stealth Rules:

A. The Stealth Rule is a default rule that always exists when using Check Point products.
B. The Stealth Rule is part of the Implicit rules.
C. Check Point recommends you include a Stealth Rule as a best practice.
D. The Stealth Rule is a rule that hides your internal networks.

**Answer:** C

**NEW QUESTION 242**
Which command displays the installed Security Gateway kernel version?

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

**Answer:** C

**NEW QUESTION 245**
Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

A. She needs to edit /etc/SSHd/SSHd_config and add the Standard Mode account.
B. She needs to run sysconfig and restart the SSH process.
C. She needs to edit /etc/scpusers and add the Standard Mode account.
D. She needs to run cpconfig to enable the ability to SCP files.

**Answer:** C

**NEW QUESTION 246**
Complete this statement. The block Intruder option in the Active log is available _____.

A. in the SmartView Monitor client
B. in the SmartView Tracker client
C. since R75.40 release
D. only if you have the IPS blade enabled at least in one gateway

**Answer:** B

**NEW QUESTION 247**
Which tool CANNOT be launched from SmartUpdate R77?

A. IP Appliance Voyager
B. snapshot
C. GAiA WebUI
D. cpinfo

**Answer:** B

**NEW QUESTION 249**
What is the difference between Standard and Specific Sign On methods?

A. Standard Sign On allows the user to be automatically authorized for all services that the rule allow
B. Specific Sign On requires that the user re-authenticate for each service specifically defined in the window Specific Action Properties.
C. Standard Sign On allows the user to be automatically authorized for all services that the rule allows, but re-authenticate for each host to which he is trying to connec
D. Specific Sign On requires that the user re-authenticate for each service.
E. Standard Sign On allows the user to be automatically authorized for all services that the rule allow
F. Specific Sign On requires that the user re-authenticate for each service and each host to which he is trying to connect.
G. Standard Sign On requires the user to re-authenticate for each service and each host to which he is trying to connec
H. Specific Sign On allows the user to sign on only to a specific IP address.

**Answer:** C

**NEW QUESTION 252**
You are a Security Administrator preparing to deploy a new HFA (Hotfix Accumulator) to ten Security Gateways at five geographically separate locations. What is the BEST method to implement this HFA?

A. Use a SSH connection to SCP the HFA to each Security Gatewa
B. Once copied locally, initiate a remote installation command and monitor the installation progress with SmartView Monitor.
C. Send a CD-ROM with the HFA to each location and have local personnel install it.
D. Send a Certified Security Engineer to each site to perform the update.
E. Use SmartUpdate to install the packages to each of the Security Gateways remotely.

**Answer:** D

**NEW QUESTION 255**
Lily has completed the initial setup of her Management Server with an IP address of 192.168.12.12. She must now run the First Time Configuration Wizard via the Gaia Portal to finish the setup. Lily knows she must use a browser to access the device, but it unsure of the correct URL to enter; which one below will she need to use?

A. http://192.168.12.12
B. https://192.168.12.12:4433
C. https://192.168.12.12
D. http://192.168.12.12:8080

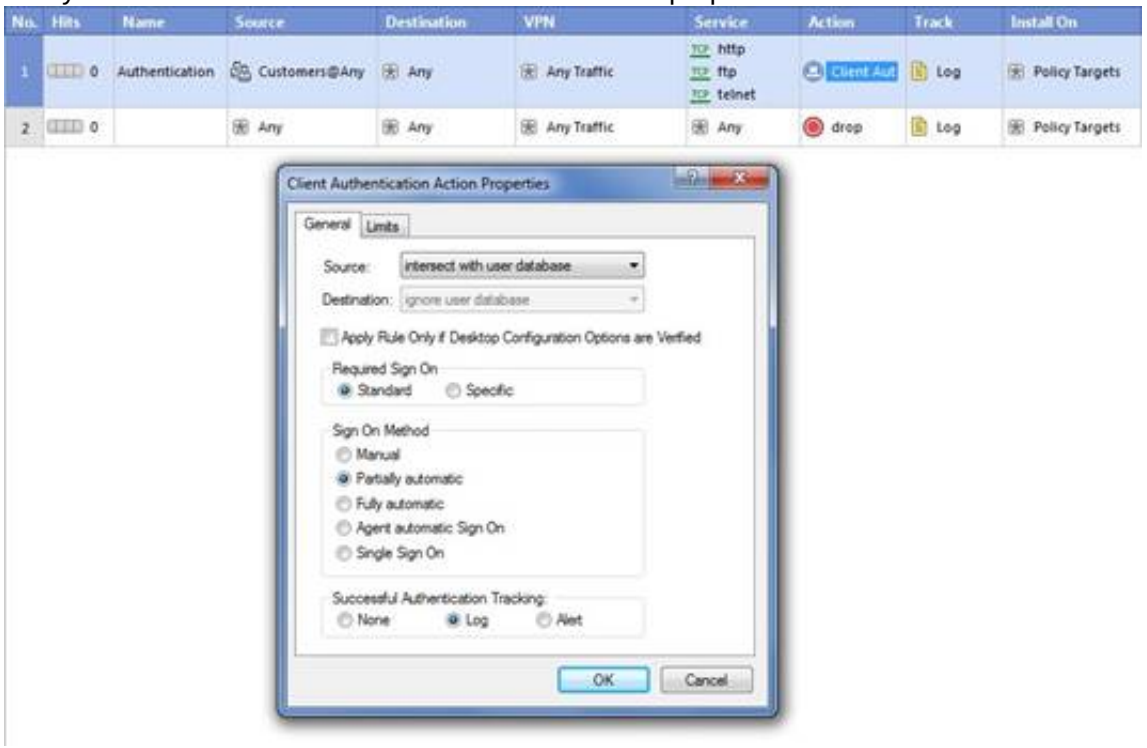
**Answer:** C

**NEW QUESTION 258**
In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

A. Rule 0
B. Blank field under Rule Number
C. Rule 1
D. Cleanup Rule

**Answer:** A

**NEW QUESTION 259**
Study the Rule base and Client Authentication Action properties screen -




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?

A. user is prompted for authentication by the Security Gateway again.
B. FTP data connection is dropped after the user is authenticated successfully.

C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication.
D. FTP connection is dropped by Rule 2.

**Answer:** C

**Explanation:**
Manual Users must use either telnet to port 259 on the firewall, or use a Web browser to connect to port 900 on the firewall to authenticate before being granted access.
# Partially Automatic If user authentication is configured for the service the user is attempting to access and they pass this authentication, then no further client authentication is required. For example, if HTTP is permitted on a client authentication rule, the user will be able to transparently authenticate since FireWall-1 has a security server for HTTP.Then, if
this setting is chosen, users will not have to manually authenticate for this connection. Note that this applies to all services for which FireWall-1 has built-in security servers (HTTP, FTP, telnet, and rlogin).
# Fully Automatic If the client has the session authentication agent installed, then no further client authentication is required (see session authentication below). For HTTP, FTP, telnet, or rlogin, the firewall will authenticate via user authentication, and then session authentication will be used to authenticate all other services.
http://www.syngress.com
Figure 6.19 Client Authentication Action Properties 278 Chapter 6 • Authenticating Users
# Agent Automatic Sign On Uses session authentication agent to provide transparent authentication (see session authentication below).
# Single Sign-On System Used in conjunction with UserAuthority servers to provide enhanced application level security. Discussion of UserAuthority is beyond the scope of this book.

**NEW QUESTION 261**
What information is found in the SmartView Tracker Management log?

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

**Answer:** A

**NEW QUESTION 263**
Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

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

**Answer:** A

**NEW QUESTION 267**
Is it possible to track the number of connections each rule matches in a Rule Base?

A. Yes, but you need SPLAT operating system to enable the feature Hits Count in the SmartDashboard client.
B. Yes, since R75 40 you can use the feature Hits Count in the SmartDashboard client.
C. Yes, but you need Gala operating system to enable the feature Hits Count in the SmartDashboard client.
D. No, due to an architecture limitation it is not possible to track the number of connections each rule matches.

**Answer:** B

**NEW QUESTION 269**
Jack has been asked do enable Identify Awareness.
What are the three methods for Acquiring Identify available in the Identify Awareness Configuration Wizard?

A. LDAP Query, Terminal Servers, Light-weight Identity Agent
B. AD Query, Browser-Based Authentication, Light-Weight Identity Agent
C. AD Query, Browser-Based Authentication, Terminal Servers
D. LDAP Query, Browser-Based Authentication, Terminal Servers

**Answer:** C

**NEW QUESTION 273**
What information is found in the SmartView Tracker Management log?

A. Historical reports log
B. Policy rule modification date/time stamp
C. Destination IP address
D. Most accessed Rule Base rule

**Answer:** B

**NEW QUESTION 278**
Which NAT option is available for Manual NAT as well as Automatic NAT?

A. Allow bi-directional NAT

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

**Answer:** C

**NEW QUESTION 282**
Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

A. Yes.
B. No.
C. Yes, but only when using Automatic NAT.
D. Yes, but only when using Manual NAT.

**Answer:** A

**NEW QUESTION 284**
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 Security Management Server, and Policy installation is not affected. When you click the Test SIC status button in the problematic Gateway object, you receive an error message. What is the problem?

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

**Answer:** D

**NEW QUESTION 285**
Which R77 GUI would you use to see the number of packets accepted since the last policy install?

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

**Answer:** A

**NEW QUESTION 290**
For remote user authentication, which authentication scheme is NOT supported?

A. Check Point Password
B. RADIUS
C. TACACS
D. SecurID

**Answer:** C

**NEW QUESTION 295**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.77 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.77 Product From:

**https://www.2passeasy.com/dumps/156-215.77/**

## Money Back Guarantee

### 156-215.77 Practice Exam Features:

* 156-215.77 Questions and Answers Updated Frequently

* 156-215.77 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.77 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.77 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year