kYour company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?  
1) Use same hard drive for database directory, log files, and temporary directory.  
2) Use Consolidation Rules.  
3) Limit logging to blocked traffic only.  
4) Use Multiple Database Tables.  
**A. 2, 4**  
**B. 1, 3, 4**  
**C. 1, 2, 4**  
**D. 1, 2**

To help organize events, SmartReporter uses filtered queries. Which of the following is NOT an SmartEvent event property you can query?  
**A. Event: Critical, Suspect, False Alarm**  
**B. TimE. Last Hour, Last Day, Last Week**  
**C. TypE. Scans, Denial of Service, Unauthorized Entry**  
**D. StatE. Open, Closed, False Alarm**

When migrating the SmartEvent data base from one server to another, the first step is to back up the files on the original server. Which of the following commands should you run to back up the SmartEvent data base?  
**A. migrate export**  
**B. eva\_db\_backup**  
**C. snapshot**  
**D. backup**

When migrating the SmartEvent data base from one server to another, the last step is to save the files on the new server. Which of the following commands should you run to save the SmartEvent data base files on the new server?

**A. cp**

**B. restore**

**C. migrate import**

**D. eva\_db\_restore**

In a UNIX environment, SmartReporter Data Base settings could be modified in:  
**A. $CPDIR/Database/conf/conf.C**  
**B. $RTDIR/Database/conf/my.cnf**  
**C. $ERDIR/conf/my.cnf**  
**D. $FWDIR/Eventia/conf/ini.C**

In a Windows environment, SmartReporter Data Base settings could be modified in:  
**A. $FWDIR/Eventia/conf/ini.C**  
**B. $ERDIR/conf/my.cnf**  
**C. %RTDIR%\Database\conf\my.ini**  
**D. $CPDIR/Database/conf/conf.C**

Which specific R77 GUI would you use to view the length of time a TCP connection was open?  
**A. SmartReporter**  
**B. SmartView Status**  
**C. SmartView Monitor**  
**D. SmartView Tracker**

SmartReporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT:  
**A. Analyzing traffic patterns against public resources.**  
**B. Possible worm/malware activity.**  
**C. Analyzing access attempts via social-engineering.**  
**D. Tracking attempted port scans.**

What is the best tool to produce a report which represents historical system information?  
**A. SmartReporter-Standard Reports**  
**B. SmartView Tracker**  
**C. Smartview Monitor**  
**D. SmartReporter-Express Reports**

If Jack was concerned about the number of log entries he would receive in the SmartReporter system, which policy would he need to modify?  
**A. Log Sequence Policy**  
**B. Report Policy**  
**C. Log Consolidator Policy**  
**D. Consolidation Policy**

You have selected the event Port Scan from Internal Network in SmartEvent, to detect an event when 30 port scans have occurred within 60 seconds. You also want to detect two port scans from a host within 10 seconds of each other. How would you accomplish this?  
**A. Define the two port-scan detections as an exception.**  
**B. You cannot set SmartEvent to detect two port scans from a host within 10 seconds of each other.**  
**C. Select the two port-scan detections as a sub-event.**  
**D. Select the two port-scan detections as a new event.**

When do modifications to the Event Policy take effect?  
**A. As soon as the Policy Tab window is closed.**  
**B. When saved on the SmartEvent Server and installed to the Correlation Units.**  
**C. When saved on the Correlation Units, and pushed as a policy.**  
**D. When saved on the SmartEvent Client, and installed on the SmartEvent Server.**

To back up all events stored in the SmartEvent Server, you should back up the contents of which folder(s)?  
**A. $FWDIR/distrib**  
**B. $FWDIR/distrib\_db and $FWDIR/events**  
**C. $RTDIR/distrib and $RTDIR/events\_db**  
**D. $RTDIR/events\_db**

To clean the system of all SmartEvent events, you should delete the files in which folder(s)?  
**A. $RTDIR/events\_db**  
**B. $FWDIR/distrib\_db and $FWDIR/events**  
**C. $RTDIR/distrib and $RTDIR/events\_db**  
**D. $FWDIR/distrib**

What SmartConsole application allows you to change the SmartReporter Policy?  
**A. SmartDashboard**  
**B. SmartReporter**  
**C. SmartEvent Server**  
**D. SmartUpdate**

Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in SmartReporter?  
**A. In SmartDashboard, the SmartView Monitor page in the R77 Security Gateway object**  
**B. In SmartReporter, under Express > Network Activity**  
**C. In SmartReporter, under Standard > Custom**  
**D. In SmartView Monitor, under Global Properties > Log and Masters**

What access level cannot be assigned to an Administrator in SmartEvent?  
**A. Read only**  
**B. Write only**  
**C. No Access**  
**D. Events Database**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ manages Standard Reports and allows the administrator to specify automatic uploads of reports to a central FTP server.  
**A. SmartReporter Database**  
**B. SmartReporter**  
**C. SmartDashboard Log Consolidator**  
**D. Security Management Server**

\_\_\_\_\_\_\_\_\_\_\_\_\_ generates a SmartEvent Report from its SQL database.  
**A. Security Management Server**  
**B. SmartReporter**  
**C. SmartEvent Client**  
**D. SmartDashboard Log Consolidator**

Which SmartReporter report type is generated from the SmartView Monitor history file?  
**A. Standard**  
**B. Traditional**  
**C. Express**  
**D. Custom**

Which Check Point product is used to create and save changes to a Log Consolidation Policy?  
**A. SmartEvent Server**  
**B. SmartDashboard Log Consolidator**  
**C. SmartReporter Client**  
**D. Security Management Server**

Which Check Point product implements a Consolidation Policy?  
**A. SmartLSM**  
**B. SmartView Tracker**  
**C. SmartView Monitor**  
**D. SmartReporter**

How many pre-defined exclusions are included by default in SmartEvent R77 as part of the product installation?  
**A. 5**  
**B. 0**  
**C. 10**  
**D. 3**

What is the purpose of the pre-defined exclusions included with SmartEvent R77?  
**A. To allow SmartEvent R77 to function properly with all other R71 devices.**  
**B. To avoid incorrect event generation by the default IPS event definition; a scenario that may occur in deployments that include Security Gateways of versions prior to R71.**  
**C. As a base for starting and building exclusions.**  
**D. To give samples of how to write your own exclusion.**

What is the benefit to running SmartEvent in Learning Mode?  
**A. There is no SmartEvent Learning Mode**  
**B. To generate a report with system Event Policy modification suggestions**  
**C. To run SmartEvent, with a step-by-step online configuration guide for training/setup purposes**  
**D. To run SmartEvent with preloaded sample data in a test environment**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is NOT an SmartEvent event-triggered Automatic Reaction.  
**A. SNMP Trap**  
**B. Block Access**  
**C. Mail**  
**D. External Script**

A tracked SmartEvent Candidate in a Candidate Pool becomes an Event. What does NOT happen in the Analyzer Server?  
**A. SmartEvent provides the beginning and end time of the Event.**  
**B. The Event is kept open, but condenses many instances into one Event.**  
**C. The Correlation Unit keeps adding matching logs to the Event.**  
**D. SmartEvent stops tracking logs related to the Candidate.**

You are reviewing computer information collected in ClientInfo. You can NOT:  
**A. Run Google.com search using the contents of the selected cell.**  
**B. Enter new credential for accessing the computer information.**  
**C. Save the information in the active tab to an .exe file.**  
**D. Copy the contents of the selected cells.**

Which of the following is NOT a SmartEvent Permission Profile type?  
**A. No Access**  
**B. Events Database**  
**C. View**  
**D. Read/Write**

What is the SmartEvent Correlation Unit’s function?  
**A. Analyze log entries, looking for Event Policy patterns.**  
**B. Display received threats and tune the Events Policy.**  
**C. Assign severity levels to events.**  
**D. Invoke and define automatic reactions and add events to the database.**

What is the SmartEvent Analyzer’s function?  
**A. Generate a threat analysis report from the Analyzer database.**  
**B. Display received threats and tune the Events Policy.**  
**C. Assign severity levels to events.**  
**D. Analyze log entries, looking for Event Policy patterns.**

What is the SmartEvent Client’s function?  
**A. Assign severity levels to events.**  
**B. Invoke and define automatic reactions and add events to the database.**  
**C. Generate a threat analysis report from the Reporter database.**  
**D. Display received threats and tune the Events Policy.**

What are the 3 main components of the SmartEvent Software Blade?  
1) Correlation Unit  
2) Correlation Client  
3) Correlation Server  
4) Analyzer Server  
5) Analyzer Client  
6) Analyzer Unit  
**A. 1, 3, 4**  
**B. 1, 4, 5**  
**C. 1, 2, 3**  
**D. 4, 5, 6**

How many Events can be shown at one time in the Event preview pane?  
**A. 5,000**  
**B. 15,000**  
**C. 30,000**  
**D. 1,000**

The SmartEvent Server:  
**A. displays the received events**  
**B. deletes events from the events database**  
**C. analyzes each IPS log entry as it enters the Log server**  
**D. invokes defined automatic reactions**

The SmartEvent Correlation Unit:  
**A. forwards what is identified as an event to the SmartEvent server.**  
**B. adds events to the events database.**  
**C. assigns a severity level to an event.**  
**D. displays the received events.**

The SmartEvent Correlation Unit:  
**A. looks for patterns according to the installed Event Policy.**  
**B. assigns a severity level to an event.**  
**C. adds events to the events database.**  
**D. displays the received events.**

Which of the following log files contains verbose information regarding the negotiation process and other encryption failures?  
**A. ike.elg**  
**B. vpn.elg**  
**C. iked.elg**  
**D. vpnd.elg**

What is the most common cause for a Quick mode packet 1 failing with the error “No Proposal Chosen” error?  
**A. The encryption strength and hash settings of one peer does not match the other.**  
**B. The previously established Permanent Tunnel has failed.**  
**C. There is a network connectivity issue.**  
**D. The OS and patch level of one gateway does not match the other.**

Which component receives events and assigns severity levels to the events; invokes any defined automatic reactions, and adds the events to the Events Data Base?  
**A. SmartEvent Correlation Unit**  
**B. SmartEvent Server**  
**C. SmartEvent Analysis DataServer**  
**D. SmartEvent Client**

The \_\_\_\_\_\_\_\_\_\_\_\_\_\_ contains the Events Data Base.  
**A. SmartEvent Server**  
**B. SmartEvent DataServer**  
**C. SmartEvent Client**  
**D. SmartEvent Correlation Unit**

The SmartEvent Correlation Unit:  
**A. analyzes each IPS log entry as it enters the Log server.**  
**B. assigns a severity level to an event.**  
**C. adds events to the events database.**  
**D. displays the received events.**

The SmartEvent Server:  
**A. assigns a severity level to an event.**  
**B. forwards what is known as an event to the SmartEvent Server.**  
**C. analyzes each IPS log entry as it enters the Log server.**  
**D. displays the received events.**

The SmartEvent Client:  
**A. adds events to the events database.**  
**B. analyzes each IPS log entry as it enters the Log server.**  
**C. assigns a severity level to an event.**  
**D. displays the received events.**

What is the command to show OSPF adjacencies?  
**A. show ospf summary-address**  
**B. show ospf interface**  
**C. show ospf neighbors**  
**D. show running-config**

A VPN Tunnel Interface (VTI) is defined on GAiA as: vpn shell interface add numbered 10.10.0.1 10.10.0.2 madrid.cp  
What do you know about this VTI?  
**A. 10.10.0.1 is the local Gateway’s internal interface, and 10.10.0.2 is the internal interface of the remote Gateway.**  
**B. The peer Security Gateway’s name is madrid.cp.**  
**C. The VTI name is madrid.cp.**  
**D. The local Gateway’s object name is madrid.cp.**

Which type of VPN routing relies on a VPN Tunnel Interface (VTI) to route traffic?  
**A. Host-based VPN**  
**B. Route-based VPN**  
**C. Domain-based VPN**  
**D. Subnet-based VPN**

You have three Gateways in a mesh community. Each gateway’s VPN Domain is their internal network as defined on the Topology tab setting All IP Addresses behind Gateway based on Topology information.  
You want to test the route-based VPN, so you created VTIs among the Gateways and created static route entries for the VTIs. However, when you test the VPN, you find out the VPN still go through the regular domain IPsec tunnels instead of the routed VTI tunnels.  
What is the problem and how do you make the VPN use the VTI tunnels?  
**A. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, remove the Gateways out of the mesh community and replace with a star community**  
**B. Domain VPN takes precedence over the route-based VTI. To make the VPN go through VTI, use an empty group object as each Gateway’s VPN Domain**  
**C. Route-based VTI takes precedence over the Domain VPN. To make the VPN go through VTI, use dynamic-routing protocol like OSPF or BGP to route the VTI address to the peer instead of static routes**  
**D. Route-based VTI takes precedence over the Domain VPN. Troubleshoot the static route entries to insure that they are correctly pointing to the VTI gateway IP.**

When configuring a Permanent Tunnel between two gateways in a Meshed VPN community, in what object is the tunnel managed?  
**A. VPN Community object**  
**B. Only the local Security Gateway object**  
**C. Each participating Security Gateway object**  
**D. Security Management Server**

Which of the following log files contains only information about the negotiation process for encryption?  
**A. iked.elg**  
**B. ike.elg**  
**C. vpn.elg**  
**D. vpnd.elg**

Which of the following statements is TRUE concerning MEP VPN’s?  
**A. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.**  
**B. MEP VPN’s are not restricted to the location of the gateways.**  
**C. MEP Security Gateways cannot be managed by separate Management Servers.**  
**D. State synchronization between Security Gateways is required.**

Which of the following statements is TRUE concerning MEP VPN’s?  
**A. MEP Security Gateways can be managed by separate Management Servers.**  
**B. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.**  
**C. State synchronization between Security Gateways is required.**  
**D. MEP VPN’s are restricted to the location of the gateways.**

Which of the following statements is TRUE concerning MEP VPN’s?  
**A. State synchronization between Security Gateways is NOT required.**  
**B. The VPN Client is assigned a Security Gateway to connect to based on a priority list, should the first connection fail.**  
**C. MEP Security Gateways cannot be managed by separate Management Servers.**  
**D. MEP VPN’s are restricted to the location of the gateways.**

Which of the following statements is TRUE concerning MEP VPN’s?  
**A. The VPN Client selects which Security Gateway takes over, should the first connection fail.**  
**B. MEP VPN’s are restricted to the location of the gateways.**  
**C. State synchronization betweened Security Gateways is required.**  
**D. MEP Security Gateways cannot be managed by separate Management Servers.**

At what router prompt would you save your OSPF configuration?  
**A. localhost.localdomain(config-router-ospf)#**  
**B. localhost.localdomain(config-if)#**  
**C. localhost.localdomain(config)#**  
**D. localhost.localdomain#**

Your organization maintains several IKE VPN’s. Executives in your organization want to know which mechanism Security Gateway R77 uses to guarantee the authenticity and integrity of messages. Which technology should you explain to the executives?  
**A. Certificate Revocation Lists**  
**B. Application Intelligence**  
**C. Key-exchange protocols**  
**D. Digital signatures**

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:  
**A. Assign links to specific VPN communities.**  
**B. Probe links for availability.**  
**C. Use links based on authentication method.**  
**D. Use links based on Day/Time.**

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:  
**A. Assign links to use Dynamic DNS.**  
**B. Use Load Sharing to distribute VPN traffic.**  
**C. Use links based on Day/Time.**  
**D. Use links based on authentication method.**

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:  
**A. Assign links to specific VPN communities.**  
**B. Use links based on services.**  
**C. Prohibit Dynamic DNS.**  
**D. Assign links to use Dynamic DNS.**

There are times when you want to use Link Selection to manage high-traffic VPN connections. With Link Selection you can:  
**A. Assign links to specific VPN communities.**  
**B. Assign links to use Dynamic DNS.**  
**C. Set up links for Remote Access.**  
**D. Use links based on Day/Time.**

What type of object may be explicitly defined as a MEP VPN?  
**A. Star VPN Community**  
**B. Any VPN Community**  
**C. Mesh VPN Community**  
**D. Remote Access VPN Community**

MEP VPN’s use the Proprietary Probing Protocol to send special UDP RDP packets to port \_\_\_\_ to discover if an IP is accessible.  
**A. 259**  
**B. 256**  
**C. 264**  
**D. 201**

Which statement defines Public Key Infrastructure? Security is provided:  
**A. by authentication.**  
**B. via both private and public keys, without the use of digital Certificates.**  
**C. by Certificate Authorities, digital certificates, and public key encryption.**  
**D. by Certificate Authorities, digital certificates, and two-way symmetric-key encryption.**

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 exported CA keys and use them to create a new server object to represent your partner’s Certificate Authority (CA).**  
**B. Create a new logical-server object to represent your partner’s CA.**  
**C. Manually import your partner’s Access Control List.**  
**D. Manually import your partner’s Certificate Revocation List.**

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. internal\_clear > All\_communities**  
**B. Internal\_clear > External\_Clear**  
**C. Communities > Communities**  
**D. internal\_clear > All\_GwToGw**

If you need strong protection for the encryption of user data, what option would be the BEST choice?  
**A. Use Diffie-Hellman for key construction and pre-shared keys for Quick Mode. Choose SHA in Quick Mode and encrypt with AES. Use AH protocol. Switch to Aggressive Mode.**  
**B. When you need strong encryption, IPsec is not the best choice. SSL VPN’s are a better choice.**  
**C. Use certificates for Phase 1, SHA for all hashes, AES for all encryption and PFS, and use ESP protocol.**  
**D. Disable Diffie-Hellman by using stronger certificate based key-derivation. Use AES-256 bit on all encrypted channels and add PFS to QuickMode. Use double encryption by implementing AH and ESP as protocols.**

Review the following list of actions that Security Gateway R75 can take when it controls packets. The Policy Package has been configured for Simplified Mode VPN. Select the response below that includes the available actions:  
**A. Accept, Reject, Encrypt, Drop**  
**B. Accept, Hold, Reject, Proxy**  
**C. Accept, Drop, Reject, Client Auth**  
**D. Accept, Drop, Encrypt, Session Auth**

What is used to validate a digital certificate?  
**A. IPsec**  
**B. CRL**  
**C. PKCS**  
**D. S/MIME**

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?  
**A. VTIs can use an already existing physical-interface IP address**  
**B. VTIs cannot share IP addresses**  
**C. VTIs are assigned only local addresses, not remote addresses**  
**D. VTIs are supported on SecurePlatform Pro**

When configuring numbered VPN Tunnel Interfaces (VTIs) in a clustered environment, what issues need to be considered?  
1) Each member must have a unique source IP address.  
2) Every interface on each member requires a unique IP address.  
3) All VTI’s going to the same remote peer must have the same name.  
4) Cluster IP addresses are required.  
**A. 1, 2, and 4**  
**B. 2 and 3**  
**C. 1, 2, 3 and 4**  
**D. 1, 3, and 4**

How do you verify a VPN Tunnel Interface (VTI) is configured properly?  
**A. vpn shell display interface detailed <VTI name>**  
**B. vpn shell show <VTI name> detailed**  
**C. vpn shell display <VTI name> detailed**  
**D. vpn shell show interface detailed <VTI name>**

If both domain-based and route-based VPN’s are configured, which will take precedence?  
**A. Route-based**  
**B. Must be chosen/configured manually by the Administrator in the Policy > Global Properties**  
**C. Domain-based**  
**D. Must be chosen/configured manually by the Administrator in the VPN community object**

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?  
**A. They are supported on the GAiA Operating System.**  
**B. Local IP addresses are not configured, remote IP addresses are configured.**  
**C. VTIs can only be physical, not loopback.**  
**D. VTIs cannot be assigned a proxy interface.**

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?  
**A. VTIs must be assigned a proxy interface.**  
**B. VTIs are only supported on SecurePlatform.**  
**C. VTIs can only be physical, not loopback.**  
**D. Local IP addresses are not configured, remote IP addresses are configured.**

Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?  
**A. Local IP addresses are not configured, remote IP addresses are configured**  
**B. VTIs cannot be assigned a proxy interface**  
**C. VTI specific additional local and remote IP addresses are not configured**  
**D. VTIs are only supported on SecurePlatform**

Which of the following is TRUE concerning numbered VPN Tunnel Interfaces (VTIs)?  
**A. VTIs are assigned only local addresses, not remote addresses**  
**B. VTIs cannot share IP addresses**  
**C. VTIs are only supported on IPSO**  
**D. VTIs cannot use an already existing physical-interface IP address**

After Travis added new processing cores on his server, CoreXL did not use them. What would be the most plausible reason why? Travis did not:  
**A. edit Gateway Properties and increase the kernel instances.**  
**B. edit Gateway Properties and increase the number of CPU cores.**  
**C. run cpconfig to increase the firewall instances.**  
**D. run cpconfig to increase the number of CPU cores.**

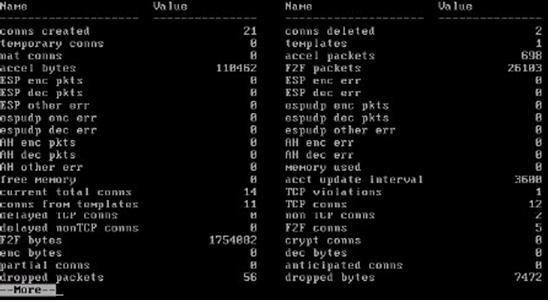
A SmartProvisioning Gateway could be a member of which VPN communities?  
1) Center in Star Topology  
2) Satellite in Star Topology  
3) Center in Remote Access Community  
4) Meshed Community  
**A. 2 only**  
**B. 2 and 3**  
**C. 1, 2 and 3**  
**D. All**

What process manages the dynamic routing protocols (OSPF, RIP, etc.) on GAiA?  
**A. gated**  
**B. There’s no separate process, but the Linux default router can take care of that.**  
**C. routerd**  
**D. arouted**

Which statement is TRUE for route-based VPN’s?  
**A. IP Pool NAT must be configured on each Gateway.**  
**B. Dynamic-routing protocols are not required.**  
**C. Route-based VPN’s are a form of partial overlap VPN Domain.**  
**D. Route-based VPN’s replace domain-based VPN’s.**

VPN routing can also be configured by editing which file?  
**A. $FWDIR/VPN/route\_conf.c**  
**B. $FWDIR/conf/vpn\_route.conf**  
**C. $FWDIR/bin/vpn\_route.conf**  
**D. $FWDIR/conf/vpn\_route.c**

The following graphic illustrates which command being issued on GAiA?  
Exhibit:



**A. fwsecurexl stats**  
**B. fwaccel stats**  
**C. fw securexl stats**  
**D. fw accel stats**

Which of the following services will cause SecureXL templates to be disabled?  
**A. HTTPS**  
**B. LDAP**  
**C. FTP**  
**D. TELNET**

How do you enable SecureXL (command line) on GAiA?  
**A. fwaccel on**   
**B. fw securexl**   
**C. fw accel on**   
**D. fwsecurexl on**

Which of the following is NOT supported by CoreXL?  
**A. Route-based VPN**  
**B. SmartView Tracker**  
**C. IPS**  
**D. IPV4**

If the number of kernel instances for CoreXL shown is 6, how many cores are in the physical machine?  
**A. 6**  
**B. 8**  
**C. 3**  
**D. 4**

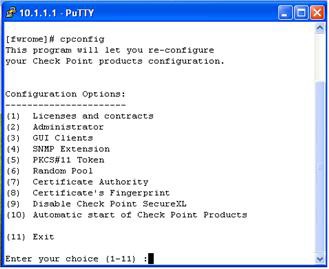
Which of the following is NOT accelerated by SecureXL?  
**A. SSH**  
**B. HTTPS**  
**C. FTP**  
**D. Telnet**

How can you disable SecureXL via the command line (it does not need to survive a reboot)?  
**A. fw ctl accel off**  
**B. securexl off**  
**C. fwaccel off**  
**D. fw xl off**

Which of these is a type of acceleration in SecureXL?  
**A. QoS**  
**B. FTP**  
**C. connection rate**  
**D. GRE**

The CoreXL SND (Secure Network Distributor) is responsible for:  
**A. distributing non-accelerated packets among kernel instances.**  
**B. accelerating VPN traffic.**  
**C. shutting down cores when they are not needed.**  
**D. changing routes to distribute the load across multiple firewalls.**

Your customer asks you about the Performance Pack. You explain to him that a Performance Pack is a software acceleration product which improves the performance of the Security Gateway. You may enable or disable this acceleration by either:  
1) the command: cpconfig



2) the command: fwaccel on¦off



What is the difference between these two commands?  
**A. The fwaccel command determines the default setting. The command cpconfig can dynamically change the setting, but after the reboot it reverts to the default setting.**  
**B. Both commands function identically.**  
**C. The command cpconfig works on the Security Platform only. The command fwaccel can be used on all platforms.**  
**D. The cpconfig command enables acceleration. The command fwaccel can dynamically change the setting, but after the reboot it reverts to the default setting.**

Your customer complains of the weak performance of his systems. He has heard that Connection Templates accelerate traffic. How do you explain to the customer about template restrictions and how to verify that they are enabled?  
**A. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the source port. To test if connection templates are enabled, use the command fw ctl templates.**  
**B. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the source port. To test if connection templates are enabled, use the command fwaccel stat.**  
**C. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the destination port. To test if connection templates are enabled, use the command fwacel templates.**  
**D. To enhance connection-establishment acceleration, a mechanism attempts to "group together" all connections that match a particular service and whose sole discriminating element is the destination port. To test if connection templates are enabled, use the command fw ctl templates.**

Frank is concerned with performance and wants to configure the affinities settings. His gateway does not have the Performance Pack running. What would Frank need to perform in order configure those settings?  
**A. Edit affinity.conf and change the settings.**  
**B. Run fw affinity and change the settings.**  
**C. Edit $FWDIR/conf/fwaffinity.conf and change the settings.**  
**D. Run sim affinity and change the settings.**

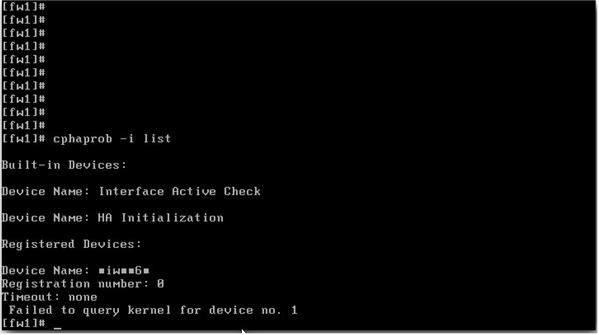
You are concerned that the processor for your firewall running R71 SecurePlatform may be overloaded. What file would you view to determine the speed of your processor(s)?  
**A. cat /etc/sysconfig/cpuinfo**  
**B. cat /proc/cpuinfo**  
**C. cat /etc/cpuinfo**  
**D. cat /var/opt/CPsuite-R71/fw1/conf/cpuinfo**

Which of the following is NOT a restriction for connection template generation?  
**A. SYN Defender**  
**B. UDP services with no protocol type or source port mentioned in advanced properties**  
**C. ISN Spoofing**  
**D. VPN Connections**

In CoreXL, what process is responsible for processing incoming traffic from the network interfaces, securely accelerating authorized packets, and distributing non-accelerated packets among kernel instances?  
**A. NAD (Network Accelerator Daemon)**  
**B. SNP (System Networking Process)**  
**C. SND (Secure Network Distributor)**  
**D. SSD (Secure System Distributor)**

Due to some recent performance issues, you are asked to add additional processors to your firewall. If you already have CoreXL enabled, how are you able to increase Kernel instances?  
**A. Use cpconfig to reconfigure CoreXL.**  
**B. Once CoreXL is installed you cannot enable additional Kernel instances without reinstalling R75.**  
**C. In SmartUpdate, right-click on Firewall Object and choose Add Kernel Instances.**  
**D. Kernel instances are automatically added after process installed and no additional configuration is needed.**

What is the reason for the following error?  
Exhibit:



**A. A third-party cluster solution is implemented.**  
**B. Cluster membership is not enabled on the gateway.**  
**C. Device Name contains non-ASCII characters.**  
**D. Objects.C does not contain a cluster object.**

In which ClusterXL Load Sharing mode, does the pivot machine get chosen automatically by ClusterXL?  
**A. Hot Standby Load Sharing**  
**B. Multicast Load Sharing**  
**C. Unicast Load Sharing**  
**D. CCP Load Sharing**

What configuration change must you make to change an existing ClusterXL cluster object from Multicast to Unicast mode?  
**A. Change the cluster mode to Unicast on the cluster object. Reinstall the Security Policy.**  
**B. Change the cluster mode to Unicast on each of the cluster-member objects.**  
**C. Run cpstop and cpstart, to re-enable High Availability on both objects. Select Pivot mode in cpconfig.**  
**D. Reset Secure Internal Communications (SIC) on the cluster-member objects. Reinstall the Security Policy.**

In a R77 ClusterXL Load Sharing configuration, which type of ARP related problem can force the use of Unicast Mode (Pivot) configuration due to incompatibility on some adjacent routers and switches?  
**A. MGCP MAC address response to a Multicast IP request**  
**B. Multicast MAC address response to a Unicast IP request**  
**C. Unicast MAC address response to a Multicast IP request**  
**D. Multicast MAC address response to a RARP request**

How do new connections get established through a Security Gateway with SecureXL enabled?  
**A. New connections are always inspected by the firewall and if they are accepted, the subsequent packets of the same connection will be passed through SecureXL**  
**B. New connection packets never reach the SecureXL module.**  
**C. The new connection will be first inspected by SecureXL and if it does not match the drop table of SecureXL, then it will be passed to the firewall module for a rule match.**  
**D. If the connection matches a connection or drop template in SecureXL, it will either be established or dropped without performing a rule match, else it will be passed to the firewall module for a rule match.**

You are establishing a ClusterXL environment, with the following topology:  
VIP internal cluster IP = 172.16.10.3; VIP external cluster IP = 192.168.10.3  
Cluster Member 1: 4 NICs, 3 enableD. hme0: 192.168.10.1/24, hme1: 10.10.10.1/24, qfe2: 172.16.10.1/24  
Cluster Member 2: 5 NICs, 3 enabled; hme3: 192.168.10.2/24, hme1: 10.10.10.2/24, hme2: 172.16.10.2/24  
External interfaces 192.168.10.1 and 192.168.10.2 connect to a VLAN switch. The upstream router connects to the same VLAN switch. Internal interfaces 172.16.10.1 and 172.16.10.2 connect to a hub. 10.10.10.0 is the synchronization network. The Security Management Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?  
**A. The Cluster interface names must be identical across all cluster members.**  
**B. Cluster members cannot use the VLAN switch. They must use hubs.**  
**C. The Security Management Server must be in the dedicated synchronization network, not the internal network.**  
**D. There is an IP address conflict.**

In a R75 Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when:  
**1. The Security Policy is installed.  
2. The Security Policy is saved.  
3. The Security Administrator logs in to the seconday Security Management Server and changes its status to Active.  
4. A scheduled event occurs.  
5. The user data base is installed.**Select the BEST response for the synchronization trigger.  
**A. 1, 2, 4**  
**B. 1, 3, 4**  
**C. 1, 2, 5**  
**D. 1, 2, 3, 4**

What is a requirement for setting up R77 Management High Availability?  
**A. All Security Management Servers must reside in the same LAN.**  
**B. State synchronization must be enabled on the secondary Security Management Server.**  
**C. All Security Management Servers must have the same operating system.**  
**D. All Security Management Servers must have the same number of NICs.**

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use three machines with the following configurations:  
Cluster Member 1: OS – GAiA; NICs – QuadCard; Memory – 1 GB; Security Gateway – version: R71 and primary Security Management Server installed, version: R77  
Cluster Member 2: OS – GAiA; NICs – 4 Intel 3Com; Memory – 1 GB; Security Gateway only, version: R77  
Cluster Member 3: OS – GAiA; NICs – 4 other manufacturers; Memory – 512 MB; Security Gateway only, version: R77  
Are these machines correctly configured for a ClusterXL deployment?  
**A. No, Cluster Member 3 does not have the required memory.**  
**B. Yes, these machines are configured correctly for a ClusterXL deployment.**  
**C. No, the Security Management Server is not running the same operating system as the cluster members.**  
**D. No, the Security Gateway cannot be installed on the Security Management Server.**

You are preparing computers for a new ClusterXL deployment. For your cluster, you plan to use four machines with the following configurations:  
Cluster Member 1: OS – GAiA; NICs – QuadCard; Memory – 1 GB; Security Gateway only, version: R77  
Cluster Member 2: OS – GAiA; NICs – 4 Intel 3Com; Memory – 1 GB; Security Gateway only, version: R77  
Cluster Member 3: OS – GAiA; NICs – 4 other manufacturers; Memory: 512 MB; Security Gateway only, version: R77  
Security Management Server: MS Windows 2008; NIC – Intel NIC (1); Security Gateway and primary Security Management Server installed, version: R77  
Are these machines correctly configured for a ClusterXL deployment?  
**A. No, Cluster Member 3 does not have the required memory.**  
**B. No, the Security Gateway cannot be installed on the Security Management Pro Server.**  
**C. No, the Security Management Server is not running the same operating system as the cluster members.**  
**D. Yes, these machines are configured correctly for a ClusterXL deployment.**

The customer wishes to install a cluster. In his network, there is a switch which is incapable of forwarding multicast. Is it possible to install a cluster in this situation?  
**A. No, the customer needs to replace the switch with a new switch, which supports multicast forwarding.**  
**B. Yes, you can toggle on ClusterXL between broadcast and multicast using the command cphaconf set\_ccp broadcast/multicast.**  
**C. Yes, the ClusterXL changes automatically to the broadcast mode if the multicast is not forwarded.**  
**D. Yes, you can toggle on ClusterXL between broadcast and multicast by setting the multicast mode using the command cphaconf set\_ccp multicast on¦off. The default setting is broadcast.**

What could be a reason why synchronization between primary and secondary Security Management Servers does not occur?  
**A. If the set of installed products differ from each other, the Security Management Servers do not synchronize the database to each other.**  
**B. You have installed both Security Management Servers on different server systems (e. g. one machine on HP hardware and the other one on DELL).**  
**C. You are using different time zones.**  
**D. You did not activate synchronization within Global Properties.**

What is the proper command for importing users into the R77 User Database?  
**A. fwm importusrs**  
**B. fwm dbimport**  
**C. fwm import**  
**D. fwm importdb**

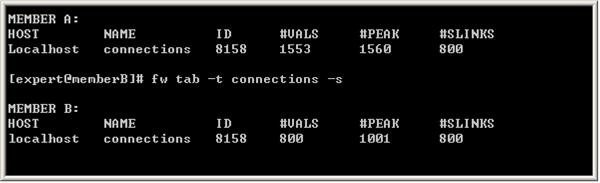
Exhibit:

https://vceguide.com/wp-content/uploads/2017/05/156-315.77-Check-Point-Certified-Security-Expert-CCSE-R77_Image_015.jpg  
What cluster mode is represented in this case?  
**A. 3rd party cluster**  
**B. HA (New mode)**  
**C. Load Sharing Unicast (Pivot) mode**  
**D. Load Sharing (multicast mode)**

Which load-balancing method below is NOT valid?  
**A. Domain**  
**B. They are all valid**  
**C. Round Trip**  
**D. Random**

Which method of load balancing describes “Round Robin”?  
**A. Assigns service requests to servers at random.**  
**B. Ensures that incoming requests are handled by the server with the fastest response time.**  
**C. Measures the load on each server to determine which server has the most available resources.**  
**D. Assigns service requests to the next server in a series.**

State Synchronization is enabled on both members in a cluster, and the Security Policy is successfully installed. No protocols or services have been unselected for selective sync.

  
Review the fw tab -t connections -s output from both members. Is State Synchronization working properly between the two members?  
**A. Members A and B are synchronized, because ID for both members is identical in the connections table.**  
**B. Members A and B are not synchronized, because #VALS in the connections table are not close.**  
**C. Members A and B are synchronized, because #SLINKS are identical in the connections table.**  
**D. Members A and B are not synchronized, because #PEAK for both members is not close in the connections table.**

You want to upgrade a cluster with two members to R77. The Security Management Server and both members are version NGX R65, with the latest Hotfix Accumulator. What is the correct upgrade procedure?  
**1. Change the version in the General Properties of the Gateway-cluster object.**  
**2. Upgrade the Security Management Server, and reboot.**  
**3. Run cpstop on one member, while leaving the other member running. Upgrade one member at a time and reboot after upgrade.**  
**4. Install the Security Policy.**  
**A. 3, 2, 1, 4**  
**B. 2, 4, 3, 1**  
**C. 2, 3, 1, 4**  
**D. 1, 3, 2, 4**

Included in the client’s network are some switches, which rely on IGMP snooping. You must find a solution to work with these switches. Which of the following answers does NOT lead to a successful solution?  
**A. Set the value of fwha\_enable\_igmp\_snooping module configuration parameter to 1.**  
**B. Disable IGMP registration in switches that rely on IGMP packets**  
**C. ClusterXL supports IGMP snooping by default. There is no need to configure anything.**  
**D. Configure static CAMs to allow multicast traffic on specific ports.**

Which of the following would be a result of having more than one active Security Management Server in a Management High Availability (HA) configuration?  
**A. An error notification will popup during SmartDashboard login if the two machines can communicate indicating Collision status.**  
**B. The need to manually synchronize the secondary Security Management Server with the Primary Security Management Server is eliminated.**  
**C. Allows for faster seamless failover: from active-to-active instead of standby-to-active.**  
**D. Creates a High Availability implementation between the Gateways installed on the Security Management Servers.**

When Load Sharing Multicast mode is defined in a ClusterXL cluster object, how are packets being handled by cluster members?  
**A. Only one member at a time is active. The active cluster member processes all packets.**  
**B. All members receive all packets. All members run an algorithm which determines which member processes packets further and which members delete the packet from memory.**  
**C. The pivot machine will handle it.**  
**D. All cluster members process all packets and members synchronize with each other.**

Which of the following does NOT happen when using Pivot Mode in ClusterXL?  
**A. The Pivot forwards the packet to the appropriate cluster member.**  
**B. The Pivot’s Load Sharing decision function decides which cluster member should handle the packet.**  
**C. The Security Gateway analyzes the packet and forwards it to the Pivot.**  
**D. The packet is forwarded through the same physical interface from which it originally came, not on the sync interface.**

When distributing IPSec packets to gateways in a Load Sharing Multicast mode cluster, which valid Load Sharing method will consider VPN information?  
**A. Load Sharing based on SPIs**  
**B. Load Sharing based on IP addresses, ports, and serial peripheral interfaces**  
**C. Load Sharing based on IP addresses, ports, and security parameter indexes**  
**D. Load Sharing based on ports, VTI, and IP addresses**

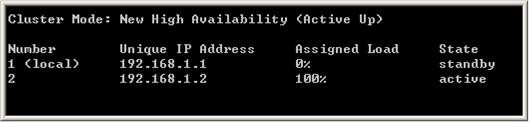
By default, the Cluster Control Protocol (CCP) uses this to send delta sync messages to other cluster members.  
**A. Multicast**  
**B. Unicast**  
**C. Anycast**  
**D. Broadcast**

Exhibit:

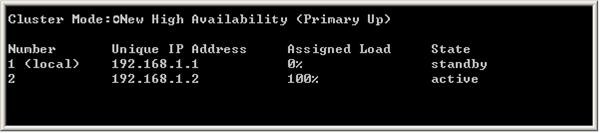
https://vceguide.com/wp-content/uploads/2017/05/156-315.77-Check-Point-Certified-Security-Expert-CCSE-R77_Image_014.jpg  
What cluster mode is represented in this case?  
**A. HA (New mode).**  
**B. 3rd party cluster**  
**C. Load Sharing (multicast mode)**  
**D. Load Sharing Unicast (Pivot) mode**

What is the behavior of ClusterXL in a High Availability environment?  
**A. The active member responds to the virtual address and is the only member that passes traffic.**  
**B. Both members respond to the virtual address and both members pass traffic.**  
**C. Both members respond to the virtual address but only the active member is able to pass traffic.**  
**D. The active member responds to the virtual address and, using sync network forwarding, both members pass traffic.**

Review the cphaprob state command output from one New Mode High Availability ClusterXL member.

  
Which member will be active after member 192.168.1.2 fails over and is rebooted?  
**A. Both members’ state will be in collision.**  
**B. Both members’ state will be active.**  
**C. 192.168.1.1**  
**D. 192.168.1.2**

Review the cphaprob state command output from a New Mode High Availability cluster member. Which machine has the highest priority?  
Exhibit:

  
**A. This output does not indicate which machine has the highest priority.**  
**B. 192.168.1.1, because it is <local>**  
**C. 192.168.1.2, because its state is active**  
**D. 192.168.1.1, because its number is 1**

By default Check Point High Availability components send updates about their state every:  
**A. 0.5 second.**  
**B. 1 second.**  
**C. 5 seconds.**  
**D. 0.1 second.**

You have just upgraded your Load Sharing gateway cluster (both members) from NGX R65 to R77. cphaprob stat shows:  
Cluster Mode: New High Availability (Active Up)  
Member Unique Address Assigned Load State  
1 (local) 172.16.185.21 100% Active  
2 172.16.185.22 0% Ready  
Which of the following is NOT a possible cause of this?  
**A. Member 1 is at a lower version than member 2**  
**B. You have not run cpconfig on member 2 yet.**  
**C. You have a different number of cores defined for CoreXL between the two members**  
**D. Member 1 has CoreXL disabled and member 2 does not**

In Management High Availability, what is an Active SMS?  
**A. Active Security Master Server**  
**B. Active Smart Master Server**  
**C. Active Smart Management Server**  
**D. Active Security Management Server**

For Management High Availability, if an Active SMS goes down, does the Standby SMS automatically take over?  
**A. Yes, if you set up VRRP**  
**B. Yes, if you set up ClusterXL**  
**C. No, the transition should be initiated manually**  
**D. Yes, if you set up SecureXL**

For Management High Availability synchronization, what does the Advance status mean?  
**A. The peer SMS has not been synchronized properly.**  
**B. The peer SMS is properly synchronized.**  
**C. The peer SMS is more up-to-date.**  
**D. The active SMS and its peer have different installed policies and databases.**

You are the MegaCorp Security Administrator. This company uses a firewall cluster, consisting of two cluster members. The cluster generally works well but one day you find that the cluster is behaving strangely. You assume that there is a connectivity problem with the cluster synchronization link (crossover cable). Which of the following commands is the BEST for testing the connectivity of the crossover cable?  
**A. ifconfig -a**  
**B. arping <IP address of the synchronization interface on the other cluster member>**  
**C. telnet <IP address of the synchronization interface on the other cluster member>**  
**D. ping <IP address of the synchronization interface on the other cluster member>**

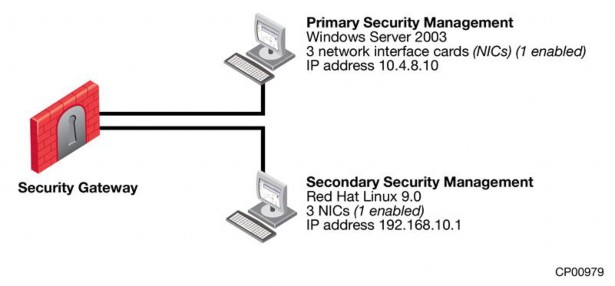
You have a High Availability ClusterXL configuration. Machines are not synchronized. What happens to connections on failover?  
**A. Open connections are lost but can be reestablished.**  
**B. It is not possible to configure High Availability that is not synchronized.**  
**C. Connections cannot be established until cluster members are fully synchronized.**  
**D. Open connections are lost but are automatically recovered whenever the failed machine recovers.**

When using ClusterXL in Load Sharing, what is the default sharing method based on?  
**A. IPs**  
**B. IPs, SPIs**  
**C. IPs, Ports**  
**D. IPs, Ports, SPIs**

If ClusterXL Load Sharing is enabled with state synchronization enabled, what will happen if one member goes down?  
**A. The processing of all connections handled by the faulty machine is immediately taken over by the other member(s).**  
**B. The processing of all connections handled by the faulty machine is dropped, so all connections need to be re-established through the other machine (s).**  
**C. There is no state synchronization on Load Sharing, only on High Availability.**  
**D. The connections are dropped as Load Sharing does not support High Availability.**

What is a Sticky Connection?  
**A. A Sticky Connection is one in which a reply packet returns through the same gateway as the original packet.**  
**B. A Sticky Connection is a connection that remains the same.**  
**C. A Sticky Connection is a VPN connection that remains up until you manually bring it down.**  
**D. A Sticky Connection is a connection that always chooses the same gateway to set up the initial connection.**

Review the R77 configuration. Is it correct for Management High Availability?  
Exhibit:

  
**A. No, the Security Management Servers must reside on the same network.**  
**B. No, the Security Management Servers do not have the same number of NICs.**  
**C. No, the Security Management Servers must be installed on the same operating system.**  
**D. No, a R77 Security Management Server cannot run on Red Hat Linux 9.0.**

Check Point New Mode HA is a(n) \_\_\_\_\_\_\_\_\_ solution.  
**A. primary-domain**  
**B. hot-standby**  
**C. acceleration**  
**D. load-balancing**

When synchronizing clusters, which of the following statements is NOT true?  
**A. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.**  
**B. In the case of a failover, accounting information on the failed member may be lost despite properly working synchronization.**  
**C. Only cluster members running on the same OS platform can be synchronized.**  
**D. The state of connections using resources is maintained by a Security Server, so these connections cannot be synchronized.**

When synchronizing clusters, which of the following statements is NOT true?  
**A. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.**  
**B. An SMTP resource connection using CVP will be maintained by the cluster.**  
**C. User Authentication connections will be lost by the cluster.**  
**D. Only cluster members running on the same OS platform can be synchronized.**

When a failed cluster member recovers, which of the following actions is NOT taken by the recovering member?  
**A. It will not check for any updated policy and load the last installed policy with a warning message indicating that the Security Policy needs to be installed from the Security Management Server.**  
**B. It will try to take the policy from one of the other cluster members.**  
**C. It compares its local policy to the one on the Security Management Server.**  
**D. If the Security Management Server has a newer policy, it will be retrieved, else the local policy will be loaded.**

Organizations are sometimes faced with the need to locate cluster members in different geographic locations that are distant from each other. A typical example is replicated data centers whose location is widely separated for disaster recovery purposes. What are the restrictions of this solution?  
**A. There are two restrictions: 1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss. 2. The synchronization network may only include switches and hubs.**  
**B. There is one restriction: The synchronization network must guarantee no more than 150 ms latency (ITU Standard G.114).**  
**C. There is one restriction: The synchronization network must guarantee no more than 100 ms latency.**  
**D. There are no restrictions.**

In ClusterXL, \_\_\_\_\_\_\_ is defined by default as a critical device.  
**A. fw.d**  
**B. vpnd**  
**C. Filter**  
**D. cpd**

Included in the customer’s network are some firewall systems with the Performance Pack in use. The customer wishes to use these firewall systems in a cluster (Load Sharing mode). He is not sure if he can use the Sticky Decision Function in this cluster. Explain the situation to him.  
**A. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to configure it with the clusterXL\_SDF\_enable command.**  
**B. ClusterXL always supports the Sticky Decision Function in the Load Sharing mode.**  
**C. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to enable the Sticky Decision Function in the SmartDashboard cluster object in the ClusterXL page, Advanced Load Sharing Configuration window.**  
**D. Sticky Decision Function is not supported when employing either Performance Pack or a hardware-based accelerator card. Enabling the Sticky Decision Function disables these acceleration products.**

A connection is said to be Sticky when:  
**A. A copy of each packet in the connection sticks in the connection table until a corresponding reply packet is received from the other side.**  
**B. A connection is not terminated by either side by FIN or RST packet.**  
**C. All the connection packets are handled, in either direction, by a single cluster member.**  
**D. The connection information sticks in the connection table even after the connection has ended.**

How does a cluster member take over the VIP after a failover event?  
**A. Gratuitous ARP**  
**B. Broadcast storm**  
**C. arp -s**  
**D. Ping the sync interface**

Check Point Clustering protocol, works on:  
**A. UDP 18184**  
**B. TCP 8116**  
**C. UDP 8116**  
**D. TCP 18184**

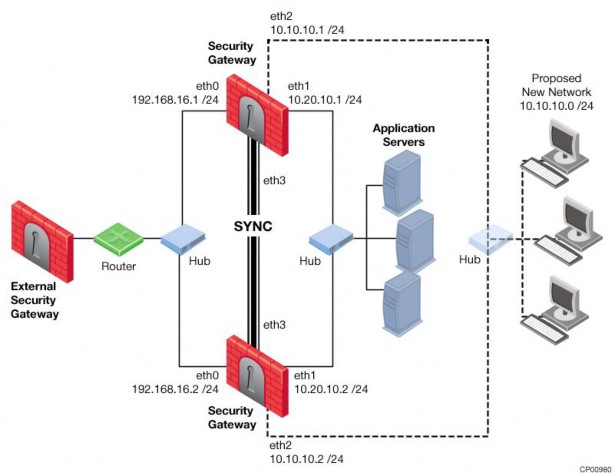
A customer called to report one cluster member’s status as Down. What command should you use to identify the possible cause?  
**A. tcpdump/snoop**  
**B. cphaprob list**  
**C. fw ctl pstat**  
**D. fw ctl debug -m cluster + forward**

A customer calls saying that a Load Sharing cluster shows drops with the error First packet is not SYN. Complete the following sentence. You will recommend:  
**A. turning off SDF (Sticky Decision Function).**  
**B. switch to Multicast Mode.**  
**C. turning on SDF (Sticky Decision Function).**  
**D. configuring flush and ack.**

In ClusterXL, \_\_\_\_\_\_\_ is defined by default as a critical device.  
**A. fwm**  
**B. assld**  
**C. cpp**  
**D. fwd**

\_\_\_\_\_\_\_\_\_\_ is a proprietary Check Point protocol. It is the basis for Check Point ClusterXL inter-module communication.  
**A. CPP**  
**B. CPHA**  
**C. CKPP**  
**D. CCP**

After you add new interfaces to a cluster, how can you check if the new interfaces and the associated virtual IP address are recognized by ClusterXL?  
Exhibit:

  
**A. By running the command cphaprob -I list on both members**  
**B. By running the command cphaprob -a if on both members**  
**C. By running the command cpconfig on both members**  
**D. By running the command cphaprob state on both members**

Which of the following is a supported Sticky Decision Function of Sticky Connections for Load Sharing?  
**A. Support for SecureClient/SecuRemote/SSL Network Extender encrypted connections**  
**B. Multi-connection support for VPN-1 cluster members**  
**C. Support for all VPN deployments (except those with third-party VPN peers)**  
**D. Support for Performance Pack acceleration**

By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:  
**A. The Security Policy is installed.**  
**B. The user data base is installed.**  
**C. The standby Security Management Server starts for the first time.**  
**D. The Security Policy is saved.**

The \_\_\_\_\_\_\_\_ Check Point ClusterXL mode must synchronize the virtual IP and MAC addresses on all clustered interfaces.  
**A. HA Mode Legacy**  
**B. HA Mode New**  
**C. Mode Unicast Load Sharing**  
**D. Mode Multicast Load Sharing**

Which process is responsible for delta synchronization in ClusterXL?  
**A. fwd on the Security Gateway**  
**B. fw kernel on the Security Gateway**  
**C. Clustering on the Security Gateway**  
**D. cpd on the Security Gateway**

Which process is responsible for full synchronization in ClusterXL?  
**A. cpd on the Security Gateway**  
**B. fwd on the Security Gateway**  
**C. fw kernel on the Security Gateway**  
**D. Clustering on the Security Gateway**

Which process is responsible for kernel table information sharing across all cluster members?  
**A. cpd**  
**B. fwd daemon**  
**C. CPHA**  
**D. fw kernel**

What is the supported ClusterXL configuration when configuring a cluster synchronization network on a VLAN interface?  
**A. It is supported on the lowest VLAN tag of the VLAN interface.**  
**B. It is not supported on a VLAN tag.**  
**C. It is supported on VLAN tag 4095.**  
**D. It is supported on VLAN tag 4096.**

While authorization for users managed by SmartDirectory is performed by the gateway, the authentication mostly occurs in \_\_\_\_\_\_\_\_\_\_.  
**A. ldapauth**  
**B. cpauth**  
**C. ldapd**  
**D. cpShared**

When troubleshooting user authentication, you may see the following entries in a debug of the user authentication process. In which order are these messages likely to appear?  
**A. make\_au, au\_auth, au\_fetchuser, au\_auth\_auth, cpLdapCheck, cpLdapGetUser**  
**B. make\_au, au\_auth, au\_fetchuser, cpLdapGetUser, cpLdapCheck, au\_auth\_auth**  
**C. cpLdapGetUser, au\_fetchuser, cpLdapCheck, make\_au, au\_auth, au\_auth\_auth**  
**D. au\_fetchuser, make\_au, au\_auth, cpLdapGetUser, au\_auth\_auth, cpLdapCheck**

\_\_\_\_\_\_\_\_\_\_ is NOT a ClusterXL mode.  
**A. Legacy**  
**B. Unicast**  
**C. Broadcast**  
**D. New**

In a Cluster, some features such as VPN only function properly when:  
**A. all cluster members have the same number of interfaces configured.**  
**B. all cluster members’ clocks are synchronized.**  
**C. all cluster members have the same policy.**  
**D. all cluster members have the same Hot Fix Accumulator pack installed.**

The process \_\_\_\_\_\_\_\_\_\_ is responsible for the authentication for Remote Access clients.  
**A. fwm**  
**B. vpnd**  
**C. cvpnd**  
**D. cpd**

The process that performs the authentication for SSL VPN Users is:  
**A. cpd**  
**B. cvpnd**  
**C. fwm**  
**D. vpnd**

The process that performs the authentication for legacy session authentication is:  
**A. cvpnd**  
**B. fwm**  
**C. vpnd**  
**D. fwssd**

How are cached usernames and passwords cleared from the memory of a Security Gateway?  
**A. By using the Clear User Cache button in SmartDashboard**  
**B. Usernames and passwords only clear from memory after they time out C. By retrieving LDAP user information using the command fw fetchldap**  
**D. By installing a Security Policy**

When an Endpoint user is able to authenticate but receives a message from the client that it is unable to enforce the desktop policy, what is the most likely scenario?  
**A. The gateway could not locate the user in SmartDirectory and is allowing the connection with limitations based on a generic profile.**  
**B. The user’s rights prevent access to the protected network.**  
**C. A Desktop Policy is not configured.**  
**D. The user is attempting to connect with the wrong Endpoint client.**

When using a template to define a user in SmartDirectory, the user’s password should be defined in the \_\_\_\_\_\_\_\_\_\_\_\_\_\_ object.  
**A. VPN Community**  
**B. LDAP**  
**C. Template**  
**D. User**

When configuring an LDAP Group object, select the option \_\_\_\_\_\_\_\_\_\_\_\_ if you want the gateway to reference all groups defined on the LDAP server for authentication purposes.  
**A. Only Sub Tree**  
**B. Only Group in Branch**  
**C. OU Accept and select appropriate domain**  
**D. All Account-Unit’s Users**

When configuring an LDAP Group object, select option \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ if you want the gateway to reference a specific group defined on the LDAP server for authentication purposes.  
**A. Group Agnostic**  
**B. All Account-Unit’s Users**  
**C. Only Sub Tree  
D. Only Group in Branch**

EXPLICACION: **Groups Scope**

There are three possible ways of defining a User Directory group, based on the users defined on the Account Unit:

* **All Account-Unit's Users**
* **Only Sub Tree ([optional prefix], branch)** - you must select a specific Account Unit branch from the drop-down list.
* **Only Group in Branch (DN prefix) -**you must select a specific group of the Account Unit.

The process \_\_\_\_\_\_\_ executes the authentication for logging in to SmartDashboard.  
**A. fwm**  
**B. vpnd**  
**C. cpd**  
**D. cvpnd**

Which of the following is a valid Active Directory designation for user John Doe in the Sales department of AcmeCorp.com?  
**A. Cn=john\_doe,ca=Sales,ou=acmecorp,dc=com**  
**B. Cn=john\_doe,ou=Sales,ou=acmecorp,dc=com**  
**C. Cn=john\_doe,ou=Sales,dc=acmecorp,dc=com**  
**D. Cn=john\_doe,ca=Sales,dc=acmecorp,dc=com**

Which of the following is a valid Active Directory designation for user Jane Doe in the MIS department of AcmeCorp.com?  
**A. Cn=jane\_doe,ou=MIS,dc=acmecorp,dc=com**  
**B. Cn= jane\_doe,ou=MIS,cn=acmecorp,dc=com**  
**C. Cn= jane\_doe,ca=MIS,dc=acmecorp,dc=com**  
**D. Cn= jane\_doe,ca=MIS,cn=acmecorp,dc=com**

You can NOT use SmartDashboard’s SmartDirectory features to connect to the LDAP server. What should you investigate?  
**1. Verify you have read-only permissions as administrator for the operating system.  
2. Verify there are no restrictions blocking SmartDashboard’s User Manager from connecting to the LDAP server.  
3. Check that the login Distinguished Name configured has at least write permission in the access control configuration of the LDAP server.  
A. 2 and 3**  
**B. 1, 2, and 3**  
**C. 1 and 2**  
**D. 1 and 3**

If you are experiencing LDAP issues, which of the following should you check?  
**A. Domain name resolution**  
**B. Secure Internal Communications (SIC)**  
**C. Overlapping VPN Domains**  
**D. Connectivity between the Gateway and LDAP server**

Where do you verify that SmartDirectory is enabled?  
**A. Global properties > Authentication > Use SmartDirectory (LDAP) for Security Gateways is checked**  
**B. Gateway properties > Smart Directory (LDAP) > Use SmartDirectory (LDAP) for Security Gateways is checked**  
**C. Gateway properties > Authentication > Use SmartDirectory (LDAP) for Security Gateways is checked**  
**D. Global properties > Smart Directory (LDAP) > Use SmartDirectory (LDAP) for Security Gateways is checked**

Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?  
**A. fwm**  
**B. fwd**  
**C. vpnd**  
**D. cvpnd**

Remote clients are using SSL VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?  
**A. vpnd**  
**B. cvpnd**  
**C. fwm**  
**D. fwd**

Which of the following is NOT a LDAP server option in SmartDirectory?  
**A. Standard\_DS**  
**B. Novell\_DS**  
**C. Netscape\_DS**  
**D. OPSEC\_DS**

An Account Unit is the interface between the \_\_\_\_\_\_\_\_\_\_ and the \_\_\_\_\_\_\_\_\_\_.  
**A. System, Database**  
**B. Clients, Server**  
**C. Users, Domain**  
**D. Gateway, Resources**

When using Captive Portal to send unidentified users to a Web portal for authentication, which of the following is NOT a recommended use for this method?  
**A. For deployment of Identity Agents**  
**B. Identity-based enforcement for non-AD users (non-Windows and guest users)**  
**C. Leveraging identity in Internet application control**  
**D. Basic identity enforcement in the internal network**

Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). Which of the following is NOT a recommended use  
for this method?  
**A. Leveraging machine name or identity**  
**B. When accuracy in detecting identity is crucial**  
**C. Identity based enforcement for non-AD users (non-Windows and guest users)**  
**D. Protecting highly sensitive servers**

Which of the following access options would you NOT use when configuring Captive Portal?  
**A. From the Internet**  
**B. Through all interfaces**  
**C. Through internal interfaces**  
**D. Through the Firewall policy**

Which describes the function of the account unit?  
**A. An Account Unit is the Check Point account that SmartDirectory uses to access an (LDAP) server**  
**B. An Account Unit is a system account on the Check Point gateway that SmartDirectory uses to access an (LDAP) server**  
**C. An Account Unit is the administration account on the LDAP server that SmartDirectory uses to access to (LDAP) server**  
**D. An Account Unit is the interface which allows interaction between the Security Management server and Security Gateways, and the SmartDirectory (LDAP) server.**

An organization may be distributed across several SmartDirectory (LDAP) servers. What provision do you make to enable a Gateway to use all available resources? Each SmartDirectory (LDAP) server must be:  
**A. a member in the LDAP group.**  
**B. represented by a separate Account Unit.**  
**C. represented by a separate Account Unit that is a member in the LDAP group.**  
**D. a member in a group that is associated with one Account Unit.**

Which is NOT a method through which Identity Awareness receives its identities?  
**A. AD Query**  
**B. Group Policy**  
**C. Identity Agent**  
**D. Captive Portal**

If using AD Query for seamless identity data reception from Microsoft Active Directory (AD), which of the following methods is NOT Check Point recommended?  
**A. Identity-based enforcement for non-AD users (non-Windows and guest users)**  
**B. Basic identity enforcement in the internal network**  
**C. Leveraging identity in Internet application control**  
**D. Identity-based auditing and logging**

Where multiple SmartDirectory servers exist in an organization, a query from one of the clients for user information is made to the servers based on a priority. By what category can this priority be defined?  
**A. Location or Account Unit**  
**B. Gateway or Domain**  
**C. Gateway or Account Unit**  
**D. Location or Domain**

Each entry in SmartDirectory has a unique \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ?  
**A. Container**  
**B. Distinguished Name**  
**C. Organizational Unit**  
**D. Schema**

With the User Directory Software Blade, you can create R77 user definitions on a(n) \_\_\_\_\_\_\_\_\_ Server.  
**A. RSA ACE/Authentication Manager**  
**B. Radius**  
**C. NT Domain**  
**D. LDAP**

When using SmartDashboard to manage existing users in SmartDirectory, when are the changes applied?  
**A. At database synchronization**  
**B. Instantaneously**  
**C. Never, you cannot manage users through SmartDashboard**  
**D. At policy installation**

In SmartDirectory, what is each LDAP server called?  
**A. Account Server**  
**B. LDAP Unit**  
**C. Account Unit**  
**D. LDAP Server**

When defining SmartDirectory for High Availability (HA), which of the following should you do?  
**A. Configure Secure Internal Communications with each server and fetch branches from each.**  
**B. Replicate the same information on multiple Active Directory servers.**  
**C. Configure a SmartDirectory Cluster object.**  
**D. Configure the SmartDirectory as a single object using the LDAP cluster IP. Actual HA functionality is configured on the servers.**

The set of rules that governs the types of objects in the directory and their associated attributes is called the:  
**A. Schema**  
**B. SmartDatabase**  
**C. Access Control List**  
**D. LDAP Policy**

Which of the following commands do you run on the AD server to identify the DN name before configuring LDAP integration with the Security Gateway?  
**A. dsquery user -name administrator**  
**B. query ldap -name administrator**  
**C. ldapquery -name administrator**  
**D. cpquery -name administrator**

There are several SmartDirectory (LDAP) features that can be applied to further enhance SmartDirectory (LDAP) functionality, which of the following is NOT one of those features?  
**A. Support many Domains under the same account unit**  
**B. Support multiple SmartDirectory (LDAP) servers on which many user databases are distributed**  
**C. High Availability, where user information can be duplicated across several servers**  
**D. Encrypted or non-encrypted SmartDirectory (LDAP) Connections usage**

Choose the BEST sequence for configuring user management in SmartDashboard, using an LDAP server.  
**A. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.**  
**B. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.**  
**C. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an LDAP resource object.**  
**D. Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.**

The User Directory Software Blade is used to integrate which of the following with a R77 Security Gateway?  
**A. UserAuthority server**  
**B. RADIUS server**  
**C. Account Management Client server**  
**D. LDAP server**

Your users are defined in a Windows 2008 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?  
**A. LDAP group**  
**B. All Users**  
**C. External-user group**  
**D. A group with a generic user**

What is NOT a valid LDAP use in Check Point SmartDirectory?  
**A. Retrieve gateway CRL’s**  
**B. Enforce user access to internal resources**  
**C. External users management**  
**D. Provide user authentication information for the Security Management Server**

Steve is troubleshooting a connection problem with an internal application. If he knows the source IP address is 192.168.4.125, how could he filter this traffic?  
**A. Run fw monitor -e "accept src-ip=192.168.4.125;"**  
**B. Run fw monitor -e "accept src=192.168.4.125;"**  
**C. Run fw monitor -e "accept dst-ip=192.168.4.125;"**  
**D. Run fw monitor -e "accept ip=192.168.4.125;"**

Check Point support has asked Tony for a firewall capture of accepted packets. What would be the correct syntax to create a capture file to a filename called monitor.out?  
**A. Run fw monitor -e "accept;" -f monitor.out**  
**B. Run fw monitor -e "accept;" -c monitor.out**  
**C. Run fw monitor -e "accept;" -o monitor.out**  
**D. Run fw monitor -e "accept;" -m monitor.out**

When upgrading a cluster in Full Connectivity Mode, the first thing you must do is see if all cluster members have the same products installed. Which command should you run?  
**A. fw fcu**  
**B. cpconfig**  
**C. cphaprob fcustat**  
**D. fw ctl conn –a**

A Minimal Effort Upgrade of a cluster:  
**A. Is only supported in major releases (R70 to R71, R71 to R77).**  
**B. Requires breaking the cluster and upgrading members independently.**  
**C. Treats each individual cluster member as an individual gateway.**  
**D. Upgrades all cluster members except one at the same time.**

A Zero Downtime Upgrade of a cluster:  
**A. Upgrades all cluster members except one at the same time.**  
**B. Is only supported in major releases (R70 to R71, R71 to R77).**  
**C. Requires breaking the cluster and upgrading members independently.**  
**D. Treats each individual cluster member as an individual gateway.**

A Full Connectivity Upgrade of a cluster:  
**A. Treats each individual cluster member as an individual gateway.**  
**B. Requires breaking the cluster and upgrading members independently.**  
**C. Is only supported in minor version upgrades (R70 to R71, R71 to R77).**  
**D. Upgrades all cluster members except one at the same time.**

How does Check Point recommend that you secure the sync interface between gateways?  
**A. Use a dedicated sync network.**  
**B. Configure the sync network to operate within the DMZ.**  
**C. Secure each sync interface in a cluster with Endpoint.**  
**D. Encrypt all sync traffic between cluster members.**

How would you set the debug buffer size to 1024?  
**A. Run fw ctl kdebug 1024**  
**B. Run fw ctl set buf 1024**  
**C. Run fw ctl set int print\_cons 1024**  
**D. Run fw ctl debug -buf 1024**

Typically, when you upgrade the Security Management Server, you install and configure a fresh R77 installation on a new computer and then migrate the database from the original machine. What is the correct order of the steps below to successfully complete this procedure?  
1) Export databases from source.  
2) Connect target to network.  
3) Prepare the source machine for export.  
4) Import databases to target.  
5) Install new version on target.  
6) Test target deployment.  
**A. 3, 1, 5, 4, 2, 6**  
**B. 5, 2, 6, 3, 1, 4**  
**C. 3, 5, 1, 4, 6, 2**  
**D. 6, 5, 3, 1, 4, 2**

During a Security Management Server migrate export, the system:  
**A. Creates a backup file that includes the SmartEvent database.**  
**B. Creates a backup archive for all the Check Point configuration settings.**  
**C. Saves all system settings and Check Point product configuration settings to a file.**  
**D. Creates a backup file that includes the SmartReporter database.**

If no flags are defined during a back up on the Security Management Server, where does the system store the \*.tgz file?  
**A. /var/backups**  
**B. /var/CPbackup/backups**  
**C. /var/opt/backups**  
**D. /var/tmp/backups**

Which is NOT a valid option when upgrading Cluster Deployments?  
**A. Fast path Upgrade**  
**B. Minimal Effort Upgrade**  
**C. Full Connectivity Upgrade**  
**D. Zero Downtime**

John is upgrading a cluster from NGX R65 to R77. John knows that you can verify the upgrade process using the pre-upgrade verifier tool. When John is running Pre-Upgrade Verification, he sees the warning message:  
Title: Incompatible pattern.  
What is happening?  
**A. The actual configuration contains user defined patterns in IPS that are not supported in R77. If the patterns are not fixed after upgrade, they will not be used with R77 Security Gateways.**  
**B. R77 uses a new pattern matching engine. Incompatible patterns should be deleted before upgrade process to complete it successfully.**  
**C. Pre-Upgrade Verification tool only shows that message but it is only informational.**  
**D. Pre-Upgrade Verification process detected a problem with actual configuration and upgrade will be aborted.**

Which command would you use to save the interface information before upgrading a GAiA Gateway?  
**A. ipconfig -a > [filename].txt**  
**B. cp /etc/sysconfig/network.C [location]**  
**C. netstat -rn > [filename].txt**  
**D. ifconfig > [filename].txt**

Which command would you use to save the IP address and routing information before upgrading a GAiA Gateway?  
**A. netstat -rn > [filename].txt**  
**B. ipconfig -a > [filename].txt**  
**C. cp /etc/sysconfig/network.C [location]**  
**D. ifconfig > [filename].txt**

Which command would you use to save the routing information before upgrading a Windows Gateway?  
**A. cp /etc/sysconfig/network.C [location]**  
**B. ifconfig > [filename].txt**  
**C. ipconfig -a > [filename].txt**  
**D. netstat -rn > [filename].txt**

Check Point recommends that you back up systems running Check Point products. Run your backups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend before major changes, such as upgrades?  
**A. upgrade\_export**  
**B. migrate export**  
**C. snapshot**  
**D. Backup**

Check Point recommends that you back up systems running Check Point products. Run your backups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend every couple of months, depending on how frequently you make changes to the network or policy?  
**A. migrate export**  
**B. upgrade\_export**  
**C. snapshot**  
**D. Backup**

Check Point recommends that you back up systems running Check Point products. Run your backups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend anytime outside a maintenance window?  
**A. snapshot**  
**B. backup**  
**C. backup\_export**  
**D. migrate Export**

The file snapshot generates is very large, and can only be restored to:  
**A. The device that created it, after it has been upgraded.**  
**B. A device having exactly the same Operating System and hardware as the device that created the file.**  
**C. Individual members of a cluster configuration.**  
**D. Windows Server class systems.**

Restoring a snapshot-created file on one machine that was created on another requires which of the following to be the same on both machines?  
**A. Windows version, objects database, patch level, and interface configuration**  
**B. State, SecurePlatform version, and patch level**  
**C. State, SecurePlatform version, and objects database**  
**D. Windows version, interface configuration, and patch level**

When restoring a Security Management Server from a backup file, the restore package can be retrieved from which source?  
**A. Local folder, TFTP server, or Disk**  
**B. Disk, SCP server, or TFTP server**  
**C. HTTP server, FTP server, or TFTP server**  
**D. Local folder, TFTP server, or FTP server**

When using migrate to upgrade a Secure Management Server, which of the following is included in the migration?  
**A. System interface configuration**  
**B. SmartEvent database**  
**C. classes.C file**  
**D. SmartReporter database**

Typically, when you upgrade the Security Management Server, you install and configure a fresh R77 installation on a new computer and then migrate the database from the original machine. When doing this, what is required of the two machines? They must both have the same:  
**A. Products installed.**  
**B. Interfaces configured.**  
**C. State.**  
**D. Patch level.**

Your primary Security Management Server runs on GAiA. What is the fastest way to back up your Security Gateway R77 configuration, including routing and network configuration files?  
**A. Copying the directories $FWDIR/conf and $FWDIR/lib to another location.**  
**B. Use the command snapshot.**  
**C. Using the command upgrade\_export.**  
**D. Using the native GAiA back up utility from command line or in the Web-based user interface.**

You need to back up the routing, interface, and DNS configuration information from your R77 GAiA Security Gateway. Which backup-and-restore solution do you use?  
**A. Manual copies of the directory $FWDIR/conf**  
**B. GAiA back up utilities**  
**C. Database Revision Control**  
**D. Commands upgrade\_export and upgrade\_import**

Which of the following methods will provide the most complete backup of an R77 configuration?  
**A. Database Revision Control**  
**B. Policy Package Management**  
**C. The command migrate\_export**  
**D. Copying the directories $FWDIR\conf and $CPDIR\conf to another server**

When restoring R77 using the command upgrade\_import, which of the following items are NOT restored?  
**A. Route tables**  
**B. Gateway topology**  
**C. Licenses**  
**D. User db**

You are running a R77 Security Gateway on GAiA. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What backup method could be used to quickly put the secondary firewall into production?  
**A. backup**  
**B. snapshot**  
**C. migrate\_import**  
**D. manual backup**

An administrator has installed the latest HFA on the system for fixing traffic problems after creating a backup file. A large number of routes were added or modified, causing network problems. The Check Point configuration has not been changed. What would be the most efficient way to revert to a working configuration?  
**A. A back up cannot be restored, because the binary files are missing.**  
**B. The restore is not possible because the backup file does not have the same build number (version).**  
**C. Select Snapshot Management from the SecurePlatform boot menu.**  
**D. Use the command restore and select the appropriate backup file.**

Your R77 enterprise Security Management Server is running abnormally on Windows 2008 Server. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?  
**A. 1. Insert the R77 CD-ROM and select the option to export the configuration using the latest upgrade utilities.**  
2. Complete steps suggested by upgrade\_verification and re-export the configuration if needed.  
3. Save the exported file \*.tgz to a local directory c:/temp.  
4. Uninstall all packages using Add/Remove Programs and reboot.  
5. Install again using the R77 CD-ROM as a primary Security Managment Server and reboot.  
6. Run upgrade\_import to import configuration.  
**B. 1. Download the latest utility upgrade\_export and run from directory c:temp to export the configuration to a \*.tgz file.**  
2. Complete steps suggested by upgrade\_verification.  
3. Uninstall all packages using Add/Remove Programs and reboot.  
4. Use SmartUpdate to reinstall the Security Management Server and reboot.  
5. Transfer file \*.tgz back to local directory /temp.  
6. Run upgrade\_import to import configuration.  
**C. 1. Download the latest utility upgrade\_export and run from directory c:temp to export the configuration to a \*.tgz file.**  
2. Skip upgrade\_verification warnings since you are not upgrading.  
3. Transfer file \*.tgz to another networked machine.  
4. Download and run utility cpclean and reboot.  
5. Use the R77 CD-ROM to select option upgrade\_import to import the configuration.  
**D. 1. Create a data base revision control back up using SmartDashboard.**  
2. Create a compressed archive of the directories %FWDIR%/conf and %FWDIR%/lib and copy them to another networked machine.  
3. Uninstall all packages using Add/Remove Programs and reboot.  
4. Install again using the R77 CD-ROM as a primary Security Managment Server and reboot.  
5. Restore the two archived directories over the top of the new installation, choosing to overwrite existing files.

Security server configuration settings are stored in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .  
**A. $FWDIR/conf/fwauthd.conf**  
**B. $FWDIR/conf/AMT.conf**  
**C. $FWDIR/conf/fwopsec.conf**  
**D. $FWDIR/conf/Fwauth.c**

User definitions are stored in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .  
**A. $FWDIR/conf/users.NDB**  
**B. $FWDIR/conf/fwmuser.conf**  
**C. $FWDIR/conf/fwusers.conf**  
**D. $FWDIR/conf/fwauth.NDB**

Jon is explaining how the inspection module works to a colleague. If a new connection passes through the inspection module and the packet matches the rule, what is the next step in the process?  
**A. Verify if another rule exists.**  
**B. Verify if any logging or alerts are defined.**  
**C. Verify if the packet should be moved through the TCP/IP stack.**  
**D. Verify if the packet should be rejected.**

Which of the following statements accurately describes the migrate command?  
**A. upgrade\_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.**  
**B. Used primarily when upgrading the Security Management Server, migrate stores all object databases and the conf directories for importing to a newer version of the Security Gateway.**  
**C. Used when upgrading the Security Gateway, upgrade\_export includes modified files, such as in the directories /lib and /conf.**  
**D. upgrade\_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.**

What step should you take before running migrate\_export?  
**A. Install policy and exit SmartDashboard.**  
**B. Disconnect all GUI clients.**  
**C. Run a cpstop on the Security Management Server.**  
**D. Run a cpstop on the Security Gateway.**

A snapshot delivers a complete backup of GAiA. How do you restore a local snapshot named MySnapshot.tgz?  
**A. Reboot the system and call the start menu. Select option Snapshot Management, provide the Expert password and select [L] for a restore from a local file. Then, provide the correct file name.**  
**B. As Expert user, type command snapshot – R to restore from a local file. Then, provide the correct file name.**  
**C. As Expert user, type command revert –file MySnapshot.tgz.**  
**D. As Expert user, type command snapshot -r MySnapshot.tgz.**

What is the primary benefit of using upgrade\_export over either backup or snapshot?  
**A. upgrade\_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.**  
**B. upgrade\_export is operating system independent and can be used when backup or snapshot is not available.**  
**C. upgrade\_export has an option to backup the system and SmartView Tracker logs while backup and snapshot will not.**  
**D. The commands backup and snapshot can take a long time to run whereas upgrade\_export will take a much shorter amount of time.**

Your R7x-series Enterprise Security Management Server is running abnormally on Windows Server 2008 R2. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?  
**A. 1. Insert the R77 CD-ROM and select the option to export the configuration using the latest upgrade utilities.**  
2. Follow steps suggested by upgrade\_verification and re-export the configuration if needed.  
3. Save the exported file \*.tgz to a local directory c:/temp.  
4. Uninstall all packages using Add/Remove Programs and reboot.  
5. Install again using the R77 CD-ROM as a primary Security Management Server and reboot.  
6. Run upgrade\_import to import the configuration.  
**B. 1. Create a data base revision control back up using SmartDashboard.**  
2. Create a compressed archive of the directories %FWDIR%/conf and %FWDIR%/lib and copy them to another networked machine.  
3. Uninstall all packages using Add/Remove Programs and reboot.  
4. Install again as a primary Security Management Server using the R77 CD-ROM.  
5. Reboot and restore the two archived directories over the top of the new installation, choosing to overwrite existing files.  
**C. 1. Download the latest utility upgrade\_export and run from a local directory c:/temp to export the configuration into a \*.tgz file.**  
2. Skip any upgrade\_verification warnings since you are not upgrading.  
3. Transfer the file \*.tgz to another networked machine.  
4. Download and run the utility cpclean and reboot.  
5. Use the R77 CD-ROM to select option upgrade\_import to import the configuration.  
**D. 1. Download the latest utility upgrade\_export and run from directory c:/temp to export the configuration into a \*.tgz file.**  
2. Follow steps suggested by upgrade\_verification.  
3. Uninstall all packages using Add/Remove Programs and reboot.  
4. Use SmartUpdate to reinstall the Security Management Server and reboot.  
5. Transfer file \*.tgz back to local directory /temp.  
6. Run upgrade\_import to import the configuration.

Anytime a client initiates a connection to a server, the firewall kernel signals the FWD process using a trap. FWD spawns the \_\_\_\_\_\_\_\_ child service, which runs the security server.  
**A. FWSD**  
**B. FWD**  
**C. In.httpd**  
**D. FWSSD**

The process \_\_\_\_\_\_\_\_ is responsible for Policy compilation.  
**A. FWM**  
**B. CPD**  
**C. FWCMP**  
**D. CPLMD**

The process \_\_\_\_\_\_\_\_ is responsible for Management High Availability synchronization.  
**A. CPD**  
**B. FWSYNC**  
**C. CPLMD**  
**D. FWM**

\_\_\_\_\_\_\_\_\_ is the called process that starts when opening SmartView Tracker application.  
**A. FWM**  
**B. CPLMD**  
**C. logtrackerd**  
**D. fwlogd**

The process \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ compiles $FWDIR/conf/\*.W files into machine language.  
**A. fwd**  
**B. fw gen**  
**C. cpd**  
**D. fwm**

Which of the following is NOT part of the policy installation process?  
**A. Initiation**  
**B. Validation**  
**C. Code compilation**  
**D. Code generation**

When, during policy installation, does the atomic load task run?  
**A. Immediately after fwm load runs on the SmartCenter.**  
**B. Before CPD runs on the Gateway.**  
**C. It is the last task during policy installation.**  
**D. It is the first task during policy installation.**

What process is responsible for transferring the policy file from SmartCenter to the Gateway?  
**A. CPD**  
**B. FWM**  
**C. CPRID**  
**D. FWD**

What firewall kernel table stores information about port allocations for Hide NAT connections?  
**A. NAT\_dst\_any\_list**  
**B. NAT\_alloc**  
**C. NAT\_src\_any\_list**  
**D. fwx\_alloc**

Where do you define NAT properties so that NAT is performed either client side or server side? In SmartDashboard under:  
**A. Gateway Setting**  
**B. NAT Rules**  
**C. Global Properties > NAT definition**  
**D. Implied Rules**

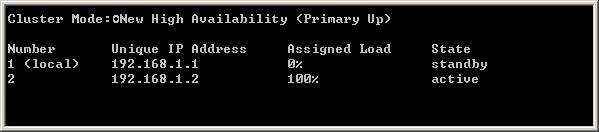
The process \_\_\_\_\_\_\_\_\_\_\_ is responsible for all other security server processes run on the Gateway.  
**A. CPD**  
**B. FWM**  
**C. FWD**  
**D. FWSSD**

The process \_\_\_\_\_\_\_\_ is responsible for GUIClient communication with the SmartCenter.  
**A. CPGUI**  
**B. CPD**  
**C. FWD**  
**D. FWM**

If Bob wanted to create a Management High Availability configuration, what is the minimum number of Security Management servers required in order to achieve his goal?  
**A. Two**  
**B. One**  
**C. Four**  
**D. Three**

David wants to manage hundreds of gateways using a central management tool. What tool would David use to accomplish his goal?  
**A. SmartDashboard**  
**B. SmartBlade**  
**C. SmartLSM**  
**D. SmartProvisioning**

Exhibit:

  
From the following output of cphaprob state, which ClusterXL mode is this?  
**A. Unicast mode  
B. Multicast mode**  
**C. New mode**  
**D. Legacy mode**

Which of the following is NOT a feature of ClusterXL?  
**A. Transparent upgrades  
B. Zero downtime for mission-critical environments with State Synchronization**  
**C. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1 gateway)**  
**D. Transparent failover in case of device failures**

EXPLICACION: ClusterXL provides:

* Transparent failover in case of machine failures
* Zero downtime for mission-critical environments (when using State Synchronization)
* Enhanced throughput (in Load Sharing modes)
* Transparent upgrades

In which case is a Sticky Decision Function relevant?  
**A. Load Balancing – Forward  
B. High Availability**  
**C. Load Sharing – Multicast**  
**D. Load Sharing – Unicast**

You configure a Check Point QoS Rule Base with two rules: an HTTP rule with a weight of 40, and the Default Rule with a weight of 10. If the only traffic passing through your QoS Module is HTTP traffic, what percent of bandwidth will be allocated to the HTTP traffic?  
**A. 80%**  
**B. 50%  
C. 40%**  
**D. 100%**

You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?  
**A. fw purge active**  
**B. fw purge policy  
C. fw fetch policy**  
**D. fw unloadlocal**

How do you verify the Check Point kernel running on a firewall?  
**A. fw ver -k**  
**B. fw ctl pstat**  
**C. fw ctl get kernel**  
**D. fw kernel**

To bind a NIC to a single processor when using CoreXL on GAiA, you would use the command

RESPUESTA = sim affinity

Fill in the blank. To verify SecureXL statistics, you would use the command \_\_\_\_\_\_\_\_

RESPUESTA = fwaccel stats

Fill in the blank. To verify the SecureXL status, you would enter command \_\_\_\_\_\_\_\_\_\_\_\_\_

RESPUESTA = fwaccel stat

Fill in the blank. To enter the router shell, use command \_\_\_\_\_\_\_\_\_\_ .

RESPUESTA = cligated

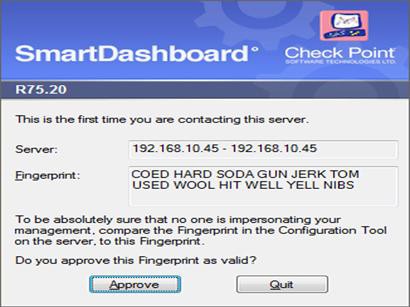
Fill in the blank. To save your OSPF configuration in GAiA, enter the command \_\_\_\_\_\_\_\_\_\_\_ .

RESPUESTA = save config

Fill in the blank. To remove site-to-site IKE and IPSEC keys you would enter command \_\_\_\_ \_\_\_ and select the option to delete all IKE and IPSec SA’s.

RESPUESTA = vpn tu

How could you compare the Fingerprint shown to the Fingerprint on the server? Run cpconfig and select:  
Exhibit:

  
**A. the Certificate Authority option and view the fingerprint.**  
**B. the GUI Clients option and view the fingerprint.**  
**C. the Certificate’s Fingerprint option and view the fingerprint.**  
**D. the Server Fingerprint option and view the fingerprint.**

Control connections between the Security Management Server and the Gateway are not encrypted by the VPN Community. How are these connections secured?  
**A. They are not secured.**  
**B. They are not encrypted, but are authenticated by the Gateway**  
**C. They are encrypted and authenticated using SIC.**  
**D. They are secured by PPTP**

Type the command and syntax that you would use to view the virtual cluster interfaces of a ClusterXL environment.

RESPUESTA = cphaprob -a if

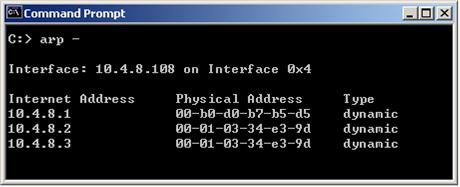
Type the command and syntax to view critical devices on a cluster member in a ClusterXL environment.

RESPUESTA = cphaprob -ia list

Type the command and syntax to configure the Cluster Control Protocol (CCP) to use Broadcast.

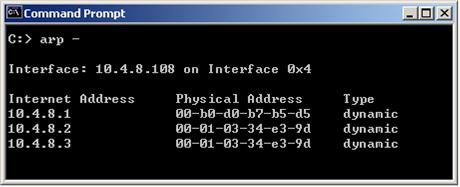
RESPUESTA = cphaconf set\_ccp broadcast

Fill in the blank. In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2 Internal host 10.4.8.108 pings 10.4.8.3, and receives replies.

  
Review the ARP table from the internal Windows host 10.4.8.108. According to the output, which member is the standby machine?

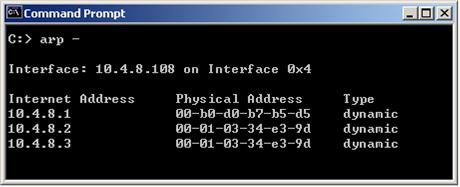
RESPUESTA = 10.4.8.1

Fill in the blank. In New Mode HA, the internal cluster IP VIP address is 10.4.8.3. An internal host 10.4.8.108 successfully pings its Cluster and receives replies.

  
Review the ARP table from the internal Windows host 10.4.8.108. Based on this information, what is the active cluster member’s IP address?

RESPUESTA = 10.4.8.2

Fill in the blank. In Load Sharing Unicast mode, the internal cluster IP address is 10.4.8.3. The internal interfaces on two members are 10.4.8.1 and 10.4.8.2. Internal host 10.4.8.108 Pings 10.4.8.3, and receives replies. The following is the ARP table from the internal Windows host 10.4.8.108.

  
Review the exhibit and type the IP address of the member serving as the pivot machine in the space below.

RESPUESTA = 10.4.8.2

To stop acceleration on a GAiA Security Gateway, enter command:

RESPUESTA = fwaccel off

Which of the following is NOT an advantage of SmartLog?  
**A. SmartLog has a “Top Results” pane showing things like top sources, rules, and users.**  
**B. SmartLog displays query results across multiple log files, reducing the need to open previous files to view results.**  
**C. SmartLog requires less disk space by consolidating log entries into fewer records.**  
**D. SmartLog creates an index of log entries, increasing query speed.**

Write the full fw command and syntax that you would use to troubleshoot ClusterXL sync issues.

RESPUESTA = fw tab -s -t connections

Type the full cphaprob command and syntax that will show full synchronization status.

RESPUESTA = cphaprob -i list

Type the full fw command and syntax that will show full synchronization status

RESPUESTA = fw ctl pstat

Type the full fw command and syntax that allows you to disable only sync on a cluster firewall member.

RESPUESTA = fw ctl setsync off

Type the command and syntax you would use to verify that your Check Point cluster is functioning correctly.

RESPUESTA = cphaprobe state

The connection to the ClusterXL member ‘A’ breaks. The ClusterXL member ‘A’ status is now ‘down’. Afterwards the switch admin set a port to ClusterXL member ‘B’ to ‘down’. What will happen?  
**A. ClusterXL member ‘B’ also left the cluster.**  
**B. ClusterXL member ‘B’ stays active as last member.**  
**C. Both ClusterXL members share load equally.**  
**D. ClusterXL member ‘A’ is asked to come back to cluster.**

Which command will only show the number of entries in the connection table?  
**A. fw tab -t connections -s**  
**B. fw tab -t connections -u**  
**C. fw tab -t connections**  
**D. fw tab**

Which statements about Management HA are correct?  
1) Primary SmartCenter describes first installed SmartCenter  
2) Active SmartCenter is always used to administrate with SmartConsole  
3) Active SmartCenter describes first installed SmartCenter  
4) Primary SmartCenter is always used to administrate with SmartConsole  
**A. 1 and 4**  
**B. 2 and 3**  
**C. 1 and 2**  
**D. 3 and 4**

Which process should you debug if SmartDashboard login fails?  
**A. sdm**  
**B. cpd**  
**C. fwd**  
**D. fwm**

Paul has just joined the MegaCorp security administration team. Natalie, the administrator, creates a new administrator account for Paul in SmartDashboard and installs the policy. When Paul tries to login it fails. How can Natalie verify whether Paul’s IP address is predefined on the security management server?  
**A. Login to Smart Dashboard, access Properties of the SMS, and verify whether Paul’s IP address is listed.**  
**B. Type cpconfig on the Management Server and select the option “GUI client List” to see if Paul’s IP address is listed.**  
**C. Login in to Smart Dashboard, access Global Properties, and select Security Management, to verify whether Paul’s IP address is listed.**  
**D. Access the WEBUI on the Security Gateway, and verify whether Paul’s IP address is listed as a GUI client.**

MultiCorp has bought company OmniCorp and now has two active AD domains. How would you deploy Identity Awareness in this environment?  
**A. You must run an ADquery for every domain.**  
**B. Identity Awareness can only manage one AD domain.**  
**C. Only one ADquery is necessary to ask for all domains.**  
**D. Only Captive Portal can be used.**

Which of the following is the preferred method for adding static routes in GAiA?  
**A. In the CLI with the command “route add”**  
**B. In Web Portal, under Network Management > IPv4 Static Routes**  
**C. In the CLI via sysconfig**  
**D. In SmartDashboard under Gateway Properties > Topology**

Which command will erase all CRL’s?  
**A. vpn crladmin**  
**B. cpstop/cpstart**  
**C. vpn crl\_zap**  
**D. vpn flush**

How frequently does CPSIZEME run by default?  
**A. weekly**  
**B. 12 hours**  
**C. 24 hours**  
**D. 1 hour**

How do you run “CPSIZEME” on SPLAT?  
**A. [expert@HostName]#>./cpsizeme -h**  
**B. [expert@HostName]# ./cpsizeme -R**  
**C. This is not possible on SPLAT**  
**D. [expert@HostName]# ./cpsizeme**

How do you check the version of “CPSIZEME” on GAiA?  
**A. [expert@HostName]# ./cpsizeme.exe -v**  
**B. [expert@HostName]# ./cpsizeme.exe -version**  
**C. [expert@HostName]# ./cpsizeme -V**  
**D. [expert@HostName]# ./cpsizeme –version**

How do you upload the results of “CPSIZEME” to Check Point when using a PROXY server with authentication?  
**A. [expert@HostName]# ./cpsizeme.exe -a username:password@proxy\_address:port**  
**B. [expert@HostName]# ./cpsizeme -p username:password@proxy\_address:port**  
**C. [expert@HostName]# ./cpsizeme -a username:password@proxy\_address:port**  
**D. [expert@HostName]# ./cpsizeme.exe -p username:password@proxy\_address:port**

By default, what happens to the existing connections on a firewall when a new policy is installed?  
**A. All existing data connections will be kept open until the connections have ended.**  
**B. Existing connections are always allowed**  
**C. All existing control and data connections will be kept open until the connections have ended.**  
**D. All existing connections not allowed under the new policy will be terminated.**

Which protocol can be used to provide logs to third-party reporting?  
**A. CPMI (Check Point Management Interface)**  
**B. LEA (Log Export API)**  
**C. AMON (Application Monitoring)**  
**D. ELA (Event Logging API)**

Can the smallest appliance handle all Blades simultaneously?  
**A. Depends on the number of protected clients and throughput.**  
**B. Depends on number of concurrent sessions.**  
**C. Firewall throughput is the only relevant factor.**  
**D. It depends on required SPU for customer environment.**

The process \_\_\_\_\_\_\_ provides service to access the GAIA configuration database.  
**A. configdbd**  
**B. confd**  
**C. fwm**  
**D. ipsrd**

Which CLI tool helps on verifying proper ClusterXL sync?  
**A. fw stat**  
**B. fw ctl sync**  
**C. fw ctl pstat**  
**D. cphaprob stat**

If your firewall is performing a lot of IPS inspection and the CPUs assigned to fw\_worker\_thread are at or near 100%, which of the following could you do to improve performance?  
**A. Add more RAM to the system.**  
**B. Add more Disk Drives.**  
**C. Assign more CPU cores to CoreXL**  
**D. Assign more CPU cores to SecureXL.**

Which of the following CLISH commands would you use to set the admin user’s shell to bash?  
**A. set user admin shell bash**  
**B. set user admin shell /bin/bash**  
**C. set user admin shell = /bin/bash**  
**D. set user admin /bin/bash**

What is Check Point’s CoreXL?  
**A. A way to synchronize connections across cluster members**  
**B. TCP-18190**  
**C. Multiple core interfaces on the device to accelerate traffic**  
**D. Multi Core support for Firewall Inspection**

Fill in the blank. What is the correct command and syntax used to view a connection table summary on a Check Point Firewall?

RESPUESTA = fw tab -t connections -s

Does Check Point recommend generating an upgrade\_export on standby SmartCenters?  
**A. Yes. This is the only way to get the upgrade\_export**  
**B. No. All Check Point processes are stopped.**  
**C. No. There is no way to verify the actual configuration.**  
**D. Yes. All information is available at both SmartCenters.**

The challenges to IT involve deployment, security, management, and what else?  
**A. Assessments**  
**B. Maintenance**  
**C. Transparency**  
**D. Compliance**

What is the correct policy installation process order?  
1.Verification  
2.Code generation and compilation  
3.Initiation  
4.Commit  
**5. Conversion  
6. CPTA  
A. 1, 2, 3, 4, 5, 6**  
**B. 3, 1, 5, 2, 6, 4**  
**C. 4, 2, 3, 5, 6, 1**  
**D. 6, 5, 4, 3, 2, 1**

What is the offline CPSIZEME upload procedure?  
**A. Find the cpsizeme\_of\_<gwname>.pdf, attach it to an e-mail and send it to cpsizeme\_upload@checkpoint.com**  
**B. Use the webbrowser version of cpsizeme and fax it to Check Point.**  
**C. Find the cpsizeme\_of\_<gwname>.xml, attach it to an e-mail and send it to cpsizeme\_upload@checkpoint.com**  
**D. There is no offline upload method.**

MultiCorp is located in Atlanta. It has a branch office in Europe, Asia, and Africa. Each location has its own AD controller for local user login. How many ADqueries have to be configured?

RESPUESTA = 4

Fill in the blank. The command that typically generates the firewall application, operating system, and hardware specific drivers is \_\_\_\_\_\_\_\_\_ .

RESPUESTA = snapshot

Fill in the blanks. To view the number of concurrent connections going through your firewall, you would use the command and syntax \_\_ \_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ \_\_ .

RESPUESTA = fw tab -t connections -s

Fill in the blanks. To view the number of concurrent connections going through core 0 on the firewall, you would use the command and syntax \_\_ \_\_ \_\_\_\_ \_\_ \_\_\_\_\_\_\_\_\_\_\_ \_\_ .

RESPUESTA = fw -i 0 tab -t connections -s

Which Check Point tool allows you to open a debug file and see the VPN packet exchange details.  
**A. PacketDebug.exe**  
**B. VPNDebugger.exe**  
**C. IkeView.exe**  
**D. IPSECDebug.exe**

When a packet is flowing through the security gateway, which one of the following is a valid inspection path?  
**A. Acceleration Path**  
**B. Small Path**  
**C. Firewall Path**  
**D. Medium Path**

To run GAiA in 64bit mode, which of the following is true?  
1) Run set edition default 64-bit.  
2) Install more than 4 GB RAM.  
3) Install more than 4 TB of Hard Disk.  
**A. 1 and 3**  
**B. 1 and 2**  
**C. 2 and 3**  
**D. 1, 2, and 3**

Which two processes are responsible on handling Identity Awareness?  
**A. pdp and lad**  
**B. pdp and pdp-11**  
**C. pep and lad**  
**D. pdp and pep**

Which three of the following are ClusterXL member requirements?  
1) same operating systems  
2) same Check Point version  
3) same appliance model  
4) same policy  
**A. 1, 3, and 4**  
**B. 1, 2, and 4**  
**C. 2, 3, and 4**  
**D. 1, 2, and 3**

Fill in the blank. You can set Acceleration to ON or OFF using command syntax \_\_\_\_\_\_\_\_\_\_\_ .

RESPUESTA = fwaccel off/on

You run cphaprob -a if. When you review the output, you find the word DOWN. What does DOWN mean?  
**A. The cluster link is down.**  
**B. The physical interface is administratively set to DOWN.**  
**C. The physical interface is down.**  
**D. CCP pakets couldn’t be sent to or didn’t arrive from neighbor member.**

Which three of the following components are required to get a SmartEvent up and running?  
1) SmartEvent SIC  
2) SmartEvent Correlation Unit  
3) SmartEvent Server  
4) SmartEvent Analyzer  
5) SmartEvent Client  
**A. 2, 3, and 5**  
**B. 1, 2, and 4**  
**C. 1, 2, and 3**  
**D. 3, 4, and 5**

MegaCorp is using SmartCenter Server with several gateways. Their requirements result in a heavy log load. Would it be feasible to add the SmartEvent Correlation Unit and SmartEvent Server to their SmartCenter Server?  
**A. No. SmartCenter SIC will interfere with the function of SmartEvent.**  
**B. No. If SmartCenter is already under stress, the use of a separate server for SmartEvent is recommended.**  
**C. No, SmartEvent and Smartcenter cannot be installed on the same machine at the same time.**  
**D. Yes. SmartEvent must be installed on your SmartCenter Server.**

Fill in the blank. To verify that a VPN Tunnel is properly established, use the command \_\_\_\_\_\_\_\_

RESPUESTA = vpn tunnelutil

MultiCorp is running Smartcenter R71 on an IPSO platform and wants to upgrade to a new Appliance with R77. Which migration tool is recommended?  
**A. Download Migration Tool R77 for IPSO and Splat/Linux from Check Point website.**  
**B. Use already installed Migration Tool.**  
**C. Use Migration Tool from CD/ISO**  
**D. Fetch Migration Tool R71 for IPSO and Migration Tool R77 for Splat/Linux from CheckPoint website**

MegaCorp is running Smartcenter R70, some Gateways at R65 and some other Gateways with R60. Management wants to upgrade to the most comprehensive IPv6 support. What should the administrator do first?  
**A. Upgrade Smartcenter to R77 first.**  
**B. Upgrade R60-Gateways to R65.**  
**C. Upgrade every unit directly to R77.**  
**D. Check the ReleaseNotes to verify that every step is supported.**

MicroCorp experienced a security appliance failure. (LEDs of all NICs are off.) The age of the unit required that the RMA-unit be a different model. Will a revert to an existing snapshot bring the new unit up and running?  
**A. There is no dynamic update at reboot.**  
**B. No. The revert will most probably not match to hard disk.**  
**C. Yes. Everything is dynamically updated at reboot.**  
**D. No. At installation the necessary hardware support is selected. The snapshot saves this state**

Which is the lowest Gateway version manageable by SmartCenter R77?  
**A. R65**  
**B. S71**  
**C. R55**  
**D. R60A**

Can you implement a complete R77 IPv6 deployment without IPv4 addresses?  
**A. No. SmartCenter cannot be accessed from everywhere on the Internet.**  
**B. Yes. Only one TCP stack (IPv6 or IPv4) can be used at the same time.**  
**C. Yes, There is no requirement for managing IPv4 addresses.**  
**D. No. IPv4 addresses are required for management.**

A ClusterXL configuration is limited to \_\_\_ members.  
**A. There is no limit.**  
**B. 16**  
**C. 6**  
**D. 2**

Select the command set best used to verify proper failover function of a new ClusterXL configuration.  
**A. reboot**  
**B. cphaprob -d failDevice -s problem -t 0 register / cphaprob -d failDevice unregister**  
**C. clusterXL\_admin down / clusterXL\_admin up**  
**D. cpstop/cpstart**

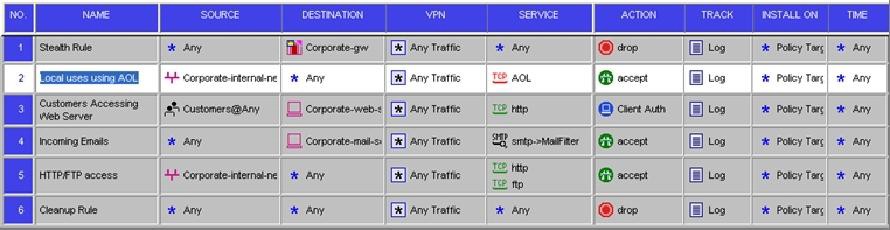
You are troubleshooting a HTTP connection problem. You’ve started fw monitor -o http.pcap. When you open http.pcap with Wireshark there is only one line. What is the most likely reason?  
**A. fw monitor was restricted to the wrong interface.**  
**B. Like SmartView Tracker only the first packet of a connection will be captured by fw monitor.**  
**C. By default only SYN pakets are captured.**  
**D. Acceleration was turned on and therefore fw monitor sees only SYN.**

In the following cluster configuration; if you reboot sglondon\_1 which device will be active when sglondon\_1 is back up and running? Why?  
**A. sglondon\_1 because it the first configured object with the lowest IP.**  
**B. sglondon\_2 because sglondon\_1 has highest IP.**  
**C. sglondon\_1, because it is up again, sglondon\_2 took over during reboot.**  
**D. sglondon\_2 because it has highest priority.**

You find that Gateway fw2 can NOT be added to the cluster object.

  
What are possible reasons for that?  
1) fw2 is a member in a VPN community.  
2) ClusterXL software blade is not enabled on fw2.  
3) fw2 is a DAIP Gateway.  
**A. 2 or 3**  
**B. 1 or 2**  
**C. 1 or 3**  
**D. All**

Review the Rule Base displayed.

  
For which rules will the connection templates be generated in SecureXL?  
**A. Rules 2 and 5**  
**B. Rules 2 through 5**  
**C. Rule 2 only**  
**D. All rules except Rule 3**

EXPLICACION: In general, Connections Templates will be created only for plain UDP or TCP connections. The following restrictions apply for Connection Template generation:

Global restrictions:

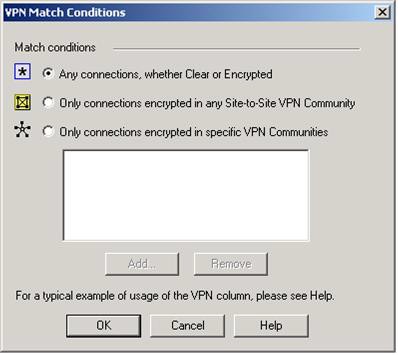
* SYN Defender — Connection Templates for TCP connections will not be created
* VPN connections
* Complex connections (H323, FTP, SQL)
* NetQuotas
* ISN Spoofing

If the Rule Base contains a rule regarding one of the following components, the Connection Templates will be disabled for connections matching this rule, and for all of the following rules:

* Security Server connections.
* Time objects in the rules.
* Dynamic Objects and/or Domain Objects.
* Services of type "other" with a match expression.
* User/Client/Session Authentication actions.
* Services of type RPC/DCERPC/DCOM.

When installing a policy containing restricted rules, you will receive console messages indicating that Connection Templates will not be created due to the rules that have been defined. The warnings should be used as a recommendation that will assist you to fine-tune your policy in order to optimize performance.

You are trying to configure Directional VPN Rule Match in the Rule Base. But the Match column does not have the option to see the Directional Match. You see the following window. What must you enable to see the Directional Match?  
Exhibit:

  
**A. directional\_match (true) in the objects\_5\_0.C file on Security Management Server**  
**B. VPN Directional Match on the Gateway object’s VPN tab**  
**C. VPN Directional Match on the VPN advanced window, in Global Properties**  
**D. Advanced Routing on each Security Gateway**

Which file defines the fields for each object used in the file objects.C (color, num/string, default  
value…)?

**A. $FWDIR/conf/classes.C**

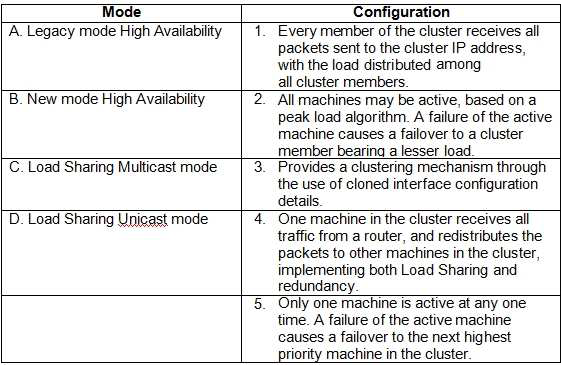
**B. $FWDIR/conf/scheam.C**

**C. $FWDIR/conf/fields.C**

**D. $FWDIR/conf/table.C**

Match the ClusterXL modes with their configurations

Exhibit



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

**B. A-2, B-3, C-1, D-5**

**C. A-3, B-5, C-1, D-4**

**D. A-5, B-2, C-4, D-1**

Your expanding network currently includes ClusterXL running Multicast mode on two members, as shown in this topology: You need to add interfaces: 10.10.10.1/24 on Member  
A, and 10.10.10.2/24 on Member b. The virtual IP address for these interfaces is  
10.10.10.3/24. Both cluster gateways have a Quad card with an available eth3 interface.  
What is the correct procedure to add these interfaces?

**A.**

**1. Disable “Cluster membership” from one Gateway via cpconfig.**

**2. Configure the new interface via sysconfig from the “non-member” Gateway.**

**3. Re-enable “Cluster membership” on the Gateway.**

**4. Perform the same steps on the other Gateway.**

**5. Update the topology in the cluster object.**

**6. Install the Security Policy.**

**B.**

**1. Configure the new interface on both members using WebUI.**

**2. Update the new topology in the cluster object from SmartDashboard.**

**3. Define virtual IP in the Dashboard**

**4. Install the Security Policy.**

**C.**

**1. Use WebUI to configure the new interfaces on both member.**

**2. Update the topology in the cluster object.**

**3. Reboot both gateways.**

**4. Install the Security Policy.**

**D.**

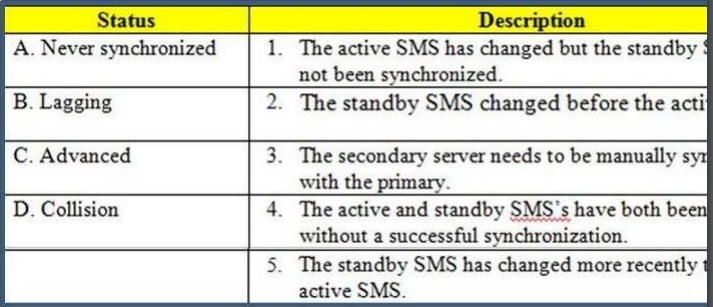
**1. Use the command ifconfig to configure and enable the new interface on both   
members.**

**2. Update the topology in the cluster object for the cluster and both members.**

**3. Install the Security Policy.**

**4. Reboot the gateway.**

Use the table to match the BEST Management High Availability synchronication-status  
descriptions for your Security Management Server (SMS).



**A. A-3, B-5, C-2, D-4**

**B. A-3, B-1, C-5, D-4**

**C. A-5, B-3, C-1, D-2**

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

MegaCorps’ disaster recovery plan is past due for an update to the backup and restore section to enjoy the benefits of the new distributed R77 installation. You must propose a plan that meets the following required and desired objectives:  
Required. Security Policy repository must be backed up no less frequently than every 24 hours.  
Desired. Back up R77 components enforcing the Security Policies at least once a week.  
Desired. Back up R77 logs at least once a week.  
You develop a disaster recovery plan proposing the following:  
\* Use the utility cron to run the command upgrade\_export each night on the Security ManagementServers.  
\* Configure the organization’s routine backup software to back up files created by the command upgrade\_export.  
\* Configure GAiA back up utility to back up Security Gateways every Saturday night.  
\* Use the utility cron to run the command upgrade\_export each Saturday night on the log servers.  
\* Configure an automatic, nightly logswitch.  
\* Configure the organization’s routine back up software to back up the switched logs every night.  
The corporate IT change review committee decides your plan:

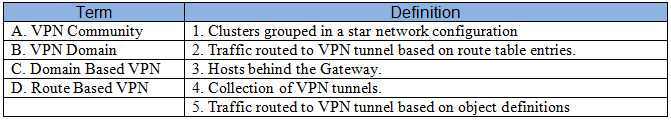
**A. meets the required objective and only one desired objective.**

**B. meets the required objective and both desired objectives.**

**C. meets the rquired objective but does not meet either deisred objective.**

**D. does not meet the required objective.**

Match the VPN-related terms with their definitions. Each correct term is only used once.



**A. A-3, B-4, C-1, D-5**

**B. A-4, B-3, C-5, D-2**

**C. A-2, B-5, C-4, D-1**

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

To provide full connectivity upgrade status, use command

RESPUESTA: cphaprob fcustat

In a zero downtime firewall cluster environment, what command syntax do you run to avoid  
switching problems around the cluster for command cphaconf?

RESPUESTA: set\_ccp broadcast

In a zero downtime scenario, which command do you run manually after all cluster members are upgraded?

RESPUESTA: cphaconf set\_ccp Multicast

Complete this statement. To save interface information before upgrading a Windows Gateway,  
use command

RESPUESTA: ipconfig -a > [filename].txt

Fill in the blank with a numeric value. The default port number for standard TCP connections with the LDAP server is

**A. 389**

**B. 388**

**C. 387**

**D. 386**

Fill in the blank with a numeric value. The default port number for Secure Sockets Layer (SSL)  
connections with the LDAP Server is

**A. 636**

**B. 635**

**C. 634**

**D. 633**

The command useful for debugging by capturing packet information, including verifying LDAP  
authentication on all Check Point platforms is

RESPUESTA: fw monitor

In GAiA, if one is unsure about a possible command, what command lists all possible commands.

**A. show commands**

**B. show all |grep commands**

**C. get all commands**

**D. show configuration**

Fred is troubleshooting a NAT issue and wants to check to see if the inbound connection from this internal network is being translated across the interface in the firewall correctly. He decides to use the fw monitor to capture the traffic from the source 192.168.3.5 or the destination of 10.1.1.25 on his Security Gateway. Green that has an IP of 192.168.4.5. What command captures this traffic in a file that he can download and review with WireShark?

**A. Expert@Green# fwmonitor -e "accept src=192.168.3.5 or dst=10.1.1.25;" -o monitor.out**

**B. Expert@Green# fwmonitor -e "accept src=192.168.3.5 and dst=10.1.1.25;" -o monitor.out**

**C. Expert@Green# fw monitor -e "accept src=192.168.3.5 and dst=10.1.1.25;" -o monitor.out**

**D. Expert@Green# fw monitor -e "accept src=192.168.3.5 or dst=10.1.1.25;" -o monitor.out**

Which components allow you to reset a VPN tunnel?

**A. vpn tu command or SmartView monitor**

**B. SmartView monitor only**

**C. vpn tunnelutil or delete vpn ike sa command**

**D. delete vpn ike sa or vpn shell command**

Select the right answer to export IPS profiles to copy to another management server?

**A. IPS profile exports is not allowed**

**B. fwm dbexport -p <profile-name>**

**C. SmartDashboard - IPS tab - Profiles - select profile + right click and select "export profile"**

**D. ips\_export\_import export <profile-name>**

Which of the following is NOT a valid way to view interface's IP address settings in GAiA?

**A. Using the command ethtool in Expert Mode**

**B. Viewing the file /config/active**

**C. Via the Gaia WebUI**

**D. Via the command show configuration in CLISH**

What utility would you use to configure route-based VPNs?

**A. vpn set\_slim\_server**

**B. vpn tu**

**C. vpn shell**

**D. vpn sw\_topology**

MegaCorp has two different types of hardware with Check Point GAiA installed and set up as gateways. The Administrator wants to provide redundancy in case one of them fails. Choose the best approach

**A. Configure ClusterXL**

**B. Configure Gateway HA**

**C. Configure Management HA for gateways**

**D. Configure VRRP**

In a Check Point gateway cluster, are VRRP and ClusterXL mutually exclusive?

**A. Yes**

**B. No, you need to install GAiA if you want to use both technologies simultaneously.**

**C. No, both gateways should have SPLAT installed.**

**D. No, only IPSO able to enable both technologies simultaneously**

What is the proper CLISH syntax to configure a default route via 192.168.255.1 in GAiA?

**A. set static-route default nexthop gateway address 192.168.255.1 priority 1 on**

**B. set static-route 192.168.255.0/24 nexthop gateway logical ethl on**

**C. set static-route 192.168.255.0/24 nexthop gateway address 192.168.255.1 priority 1 on**

**D. set static-route nexthop default gateway logical 192.168.255.1 priority 1 on**

A ClusterXL configuration is limited to \_\_\_\_\_ members

**A. 16**

**B. There is not limit**

**C. 2**

**D. 8**

CPD is a core Check Point process that does all of the following EXCEPT

**A. Policy installation**

**B. SIC (Secure Internal Communication) functions**

**C. Management High Availability (HA) sync**

**D. AMON status pull from the Gateway**

What process manages the dynamic routing protocols (OSPF, RIP, etc.) on GAiA?

**A. routerd**

**B. routed**

**C. There's no separate process, but the Linux default router can take care of that**

**D. arouted**

In Gaia, the operating system can be changed to 32-bit or 64-bit, provided the processor supports 64-bit. What command toggles to 64-bit

**A. set bitrate 64**

**B. set edition default 64**

**C. set edition default 64-bit**

**D. configure edition 64-bit**

What does the command vpn crl\_zap do?

**A. Nothing, it is not a valid command**

**B. Erases all CRL's from the gateway cache**

**C. Erases VPN certificates from cache**

**D. Erases CRL's from the management server cache**

The "MAC Magic" value must be modified under the following condition:

**A. There is more than one cluster connected to the same VLAN**

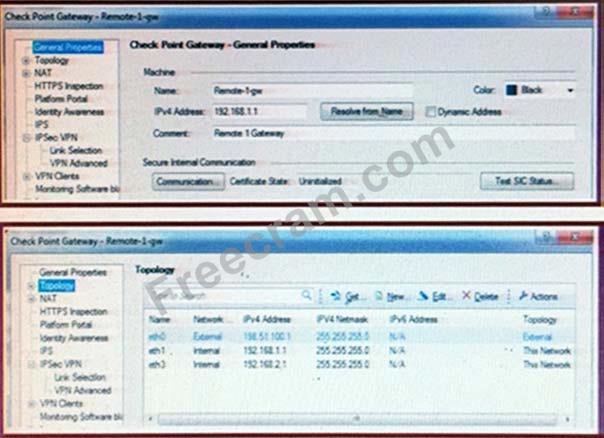
**B. A firewall cluster is configured to use Multicast for CCP traffic**

**C. There are more than two members in a firewall cluster**

**D. A firewall cluster is configured to use Broadcast for CCP traffic**

EXPLICACION: To remind you briefly, "magic mac" is an artificial MAC address used in CCP, Cluster Control Protocol, responsible for probing, messaging and sync communications in ClusterXL. Once you have more than one cluster in the same network, you have to change magic mac settings starting from the second cluster and up.

You have configured a site to site VPN but the tunnel in not coming up. Review the following screen shots. What is a likely cause?



**A. Link selection is set to use Main address**

**B. General Properties IP address is required to be the external interface**

**C. Nothing, it is configured properly**

Which of the following is NOT an internal/native Check Point command?

**A. fw ctl debug  
B. cphaprob**

**C. tcpdump**

**D. fwaccell on**

A Threat Prevention profile is a set of configurations based on the following. Select the right answer

**A. Anti-Virus settings, Anti-Bot settings, Threat Emulation settings**

**B. Anti-Virus settings, Anti-Bot settings, Threat Emulation settings, Intrusion-prevention settings**

**C. Anti-Virus settings, Anti-Bot settings, Threat Emulation settings, Intrusion-prevention settings, HTTPS inspection settings**

**D. Anti-Bot settings, Threat Emulation settings, Intrusion-prevention settings, HTTPS inspection settings**

Katie has enabled User Directory and applied the license to Security Management Server, Green. Her supervisor has asked her to configure the Password Strength options of the least one digit, one symbol, 8 characters long and include an uppercase character. How should she accomplish this?

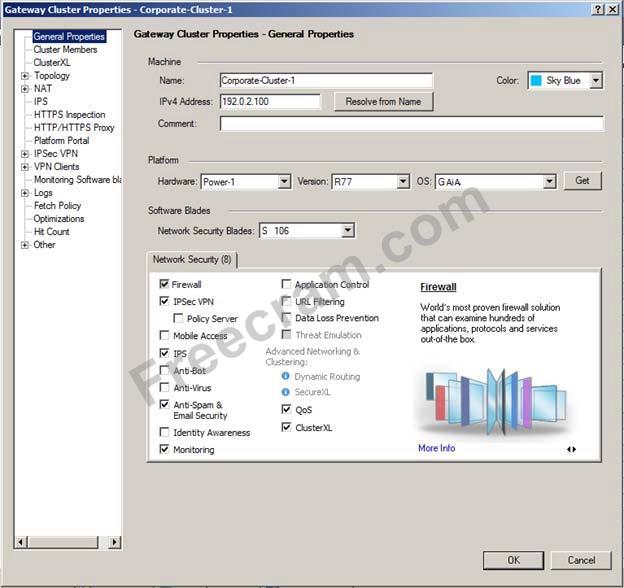
**A. Open the SmartDashboard, Select Global properties, select User Authority; check the boxes for Password must include an upper character, Password must include a digit and Password must include a symbol**

**B. Open the SmartDashboard, Select Global Properties, select User Directory, check the boxes for Password must include an uppercase character, Password must include a digit, and Password must include a symbol.**

**C. Open the SmartDashboard, Select Global Properties, select User Directory, check the boxes for Password must include an uppercase character, Password must include a digit, Password must include a symbol and change the password length to 8 characters.**

**D. Open the SmartDashboard, Select Global properties, select Identity Awareness; check the boxes for Password must include an upper character, Password must include a digit, Password must include a symbol and change the password length to 8 characters.**

John is configuring a new R77 Gateway cluster but he cannot configure the cluster as Third Party IP Clustering because this option is not available in Gateway Cluster Properties. What's happening?  
Exhibit:



**A. ClusterXL needs to be unselected to permit third party clustering configuration**

**B.** **John has an invalid ClusterXL license**

**C.** **Third Party Clustering is not available for R77 Security Gateways**

**D. John is not using third party hardware as IP Clustering is part of Check Point's IP Appliance**

MegaCorp plans to upgrade all of its firewalls. Currently the corporation is a mixture of SecurePlatform and IPSO machines running R71, to the latest code level of GAiA. Many of the firewalls are using VTIs to allow advanced routing configuration to propagate through all the networks. What will the Acme company need to do to make sure VTIs will work once moved to GAiA?

**A. Move to Domain based routing as GAiA does not support VTIs.**

**B. Convert all the Secure Platform replacements to unnumbered VTIs.**

**C. Nothing specific as GAiA supports both numbered and unnumbered VTIs.**

**D. Convert all of the IPSO replacements to numbered VTIs.**

Lilly has generated an IKE debug on her Security Gateway. She has asked Jack to transfer the file to Support. Where is the file located?

**A. $FWDIR/opt/ike.elg**

**B. $FWDIR/opt/vpnd.elg**

**C. $FWDIR/log/vpnd.elg**

**D. $FWDIR/log/ike.elg**

What can you do to see the current number of kernel instances in a system with CoreXL enabled?

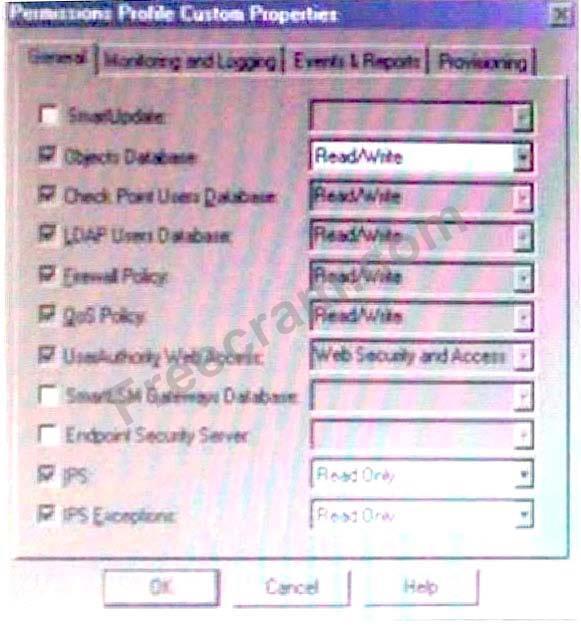
**A. Only Check Point support personnel can access that information**

**B. Run command cpconfig**

**C. Execute SmartDashboard client.**

**D. Browse to Secure Platform Web GUI.**

UserA is able to create a SmartLSM Security Cluster Profile, you must select the correct justification



**A. Not enough information to determine. You must know the user's Provisioning permissions to determine whether they are able to create a SmartLSM Security Cluster Profile**

**B. False The user must have Read/Write permissions for the SmartLSM Gateways Database**

**C. True Only Object Database Read/Write permissions are required to create SmartLSM Profiles**

**D. False. The user must have at least Read permissions for the SmartLSM Gateways Database**

What command will stop all (and only) Management Portal services?

**A. smartportalstop**

**B. spstop**

**C. sportalstop**

**D. cpstop**

Your organization has many VPN-1 Edge gateways at various branch offices, to allow VPN-1 Secure Client users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the VPN-1 Edge gateways first be inspected by your headquarters' VPN-1 Pro Security Gateway.  
How do you configure VPN routing in this star VPN Community?

**A. To the center only**

**B. To the center; or through the center to other satellites, then to the Internet and other VPN targets**

**C. To the center and other satellites, through the center**

**D. To the Internet and other targets only**

**Your customer wishes to install SmartWorkflow on top of R70 Security Management Server (Windows system). What is the required disk space?**

**A. 880 MB**

**B. 1256 MB**

**C. 512 MB**

**D. 1 GB**

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

**A. URI**

**B. AMON**

**C. UFP**

**D. CVP**

**E. LEA**

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



**A. 20%**

**B. 5%**

**C. 8%**

**D. 14%**

**In cryptography, the Rivest, Shamir, Adelman (RSA) scheme has which of the following? Select all that apply.**

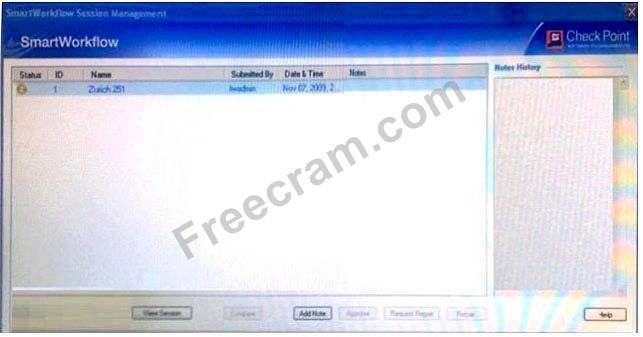
**A. A symmetric-cipher system**

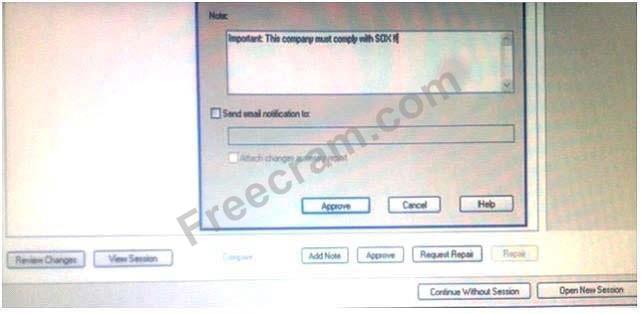
**B. An asymmetric-cipher system**

**C. A secret-key encryption-algorithm system**

**D. A public-key encryption-algorithm system**

John is the MultiCorp Security Administrator. If he suggests a change in the firewall configuration, he must submit his proposal to David, a security manager. One day David is out of the office and john submits his proposal to peter. Surprisingly, Peter is not able to approve the proposal because the system does not permit him to do so?





Both David and Peter have accounts as administrators in the Security Management server and both have the Read/Write ALL permission. What is the reason for this difference?

**A. There were some Hardware/Software issues at Security Management server on the first day.**

**B. The specific SmartWorkflow read/Write permission were assigned to David only.**

**C. The attribute Manage Administrator was not assigned to Peter**

**D. Peter was no logged on to system for a longer time**

**When you add a resource service to a rule, which ONE of the following actions occur?**

**A. VPN-1 Secure Client users attempting to connect to the object defined in the Destination column of the rule will receive a new Desktop Policy from the resource**

**B. All packets matching the resource service rule are analyzed or authenticated, based on the resource properties.**

**C. All packets that match the resource in the rule will be dropped.**

**D. All packets matching that rule are either encrypted or decrypted by the defined resource.**

**E. Users attempting to connect to the destination of the rule will be required to authenticate**

**Which Check Point QoS feature marks the ToS byte in the IP header?**

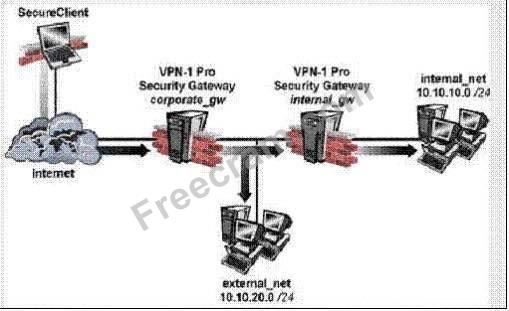
**A. Low Latency Queuing**

**B. Weighted Fair Queuing**

**C. Differentiated Services**

**D. Guarantees**

The following diagram illustrates how a VPN-1 SecureClient user tries to establish a VPN with hosts in the external\_net and internal\_net from the Internet.  
How is the Security Gateway VPN Domain created?



**A. Internal Gateway VPN Domain = internal\_net;**

**External VPN Domain = external net + external gateway object + internal\_net**

**B. Internal Gateway VPN Domain = internal\_net.**

**External Gateway VPN Domain = internal VPN Domain + internal gateway object + external\_net**

**C. Internal Gateway VPN Domain = internal\_net;**

**External Gateway VPN Domain = internal\_net + external\_net**

**D. Internal Gateway VPN Domain = internal\_net.**

**External Gateway VPN Domain = external\_net + internal gateway object**

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

**A. Apply rule only to encrypted traffic**

**B. Rule limit**

**C. Rule guarantee**

**D. Guarantee Allocation**

**E. Rule weight**

What is the lowest possible version a Security Gateway may be running in order to use it as an LSM enabled Gateway?

**A.NGX R71**

**B. NGXR65HFA\_50**

**C. NG-AI R55 HFAJ7**

**D. NGX R60**

DShield is a Check Point feature used to block which of the following threats?

**A. DDOS**

**B. Trojan horses**

**C. Cross Site Scripting**

**D. Buffer overflows**

**E. SQL injection**

VPN access control would fall under which VPN component?

**A. Performance**

**B. Security**

**C. QoS**

**D. Management**

Where is the encryption domain for a SmartLSM Security Gateway configured in R71?

**A. Inside the SmartLSM Security Gateway object in the SmartProvisioning GUI**

**B. Inside the SmartLSM Security Gateway object in the SmartDashboard GUI**

**C. Inside the SmartLSM Security Gateway profile in the SmartProvisioning GUI**

**D. Inside the SmartLSM Security Gateway profile in the SmartDashboard GUI**

When configuring a Web Application for SSL VPN remote access, you have given the following definition for the application along with its protection level.  
Which of the following is the best match for the above application?



**A. hr.dmz.example.com/intranet**

**B. dmz.example.com/extranet**

**C. www.dmz.example/extranet**

**D. www.example.com/intranet**

Which of the following are valid PKI architectures?

**A. Hierarchical architecture**

**B. Gateway architecture**

**C. mesh architecture**

**D. Bridge architecture**

How can you completely tear down a specific VPN tunnel in an intranet IKE VPN deployment?

**A. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec Sas for ALL peers and users".**

**B. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".**

**C. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec Sas for a given user (Client)".**

**D. Run the command vpn tu on the Security Gateway, and choose the option "Delete all IPSec+IKE SAs for a given peer (GW)".**

**E. Run the command vpn tu on the SmartCenter Server, and choose the option "Delete all IPSec+IKE SAs for ALL peers and users".**

Which of the following files is used to allow only specific IPs or networks to access the Management Portal?

**A. hosts. Allow**

**B. portal.ips**

**C. allowedips.portal**

**D. cpportal\_allowips**

You want only RAS signals to pass through H.323 Gatekeeper and other H.323 protocols, passing directly between end points.  
Which routing mode in the VoIP Domain Gatekeeper do you select?

**A. Direct**

**B. Call Setup**

**C. Direct and Call Setup**

**D. Call Setup and Call Control**

You are a Security Administrator preparing to deploy a new HFA (Hot fix Accumulator) to ten Security Gateways at five geographically separated locations.  
What is the BEST method to implement this HFA?

**A. Use a SSH connection to SCP the HFA to each Security Gateway.Once copied locally, initiate a remote installation command and monitor the installation progress with SmartView Monitor.**

**B. Use SmartUpdate to install the packages to each of the Security Gateways remotely**

**C. Send a CDROM 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**

You want to block corporate internal-net and localnet from accessing Web sites containing inappropriate content. You are using WebTrends for URL filtering.  
You have disabled VPN- 1 Control connections in the Global properties.  
Review the diagram and the Security Policies for GW\_A and GW\_B in the exhibit provided.

Corporate users and localnet users receive message "Web cannot be displayed". In SmartView Tracker, you see the connections are dropped with message "content security is not reachable".  
What is the problem, and how do you fix it?

**A. The connection from GW\_B to the WebTrend server is not allowed in the Policy. Fix: Add a rule in GW\_B's Policy with Source GW\_B, destination WebTrends server, service TCP port 18182, and action accept.**

**B. The connection from GW\_B to the internal WebTrends server is not allowed in the Policy. Fix: Add a rule in GW\_A's Policy to allow source WebTrends Server, destination GW\_B, service TCP port 18182, and action accept.**

**C. The connection from GW\_Ato the WebTrends server is not allowed in the Policy. Fix: Add a rule in GW\_B's Policy with source WebTrends server, destination GW\_A, service TCP port 18182, and action accept.**

**D. The connection from GW\_A to the WebTrends server is not allowed in the Policy. Fix: Add a rule in GW\_A's Policy to allow source GW\_A, destination WebTrends server, service TCP port 18182, and action accept.**

**E. The connection from GW\_A to the WebTrends server is not allowed in the Policy. Fix: Add a rule in GW\_B's Policy with source GW\_A, destination: WebTrends server, service TCP port 18182, and action accept.**

Jacob is using a mesh VPN Community to create a site-to-site VPN. The VPN properties in this mesh Community display in this graphic:



Which of the following statements is TRUE?

**A. Jacob must change the data integrity settings for this VPN Community. MD5 is incompatible with AES.**

**B. If Jacob changes the setting "Perform IPSec data encryption with" from "AES-128" to "3DES", he will increase the encryption overhead.**

**C. Jacob's VPN Community will perform IKE Phase 1 key-exchange encryption, using the longest key VPN-1 NGX supports.**

**D. If Jacob changes the setting, "Perform key exchange encryption with" from "3DES" to "DES", he will enhance the VPN Community's security and reduce encryption overhead.**

What is a possible reason for the grayed out Restore Version button in the screenshot of the Database Revision Control while trying to restore Old Structure?

**A. Old Structure was not approved in SmartWorkflow.**

**B. No SmartWorkflow session is started.**

**C. With SmartWorkflow active, only SmartWorkflow revisions could be restored.**

**D. Self-created versions cannot be restored if there are newer versions created in SmartWorkflow.**

Which of the following are valid reasons for beginning with a fresh installation VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65? Select all that apply.

**A. Objects and rules' naming conventions have changed over time.**

**B. Your Security Policy includes rules and objects whose purpose you do not know.**

**C. You see a more logical way to organize your rules and objects**

**D. You want to keep your Check Point configuration.**

When synchronizing clusters, which of the following statements are true? Select all that apply.

**A. Only cluster members running on the same OS platform can be synchronized.**

**B. Client Auth or Session Auth connections through a cluster member will be lost of the cluster member fails.**

**C. The state of connections using resources is maintained by a Security Server, so these connections cannot be synchronized.**

**D. In the case of a failover, accounting information on the failed member may be lost despite a properly**

Wayne configures an HTTP Security Server to work with the content vectoring protocol to screen forbidden sites. He has created a URI resource object using CVP with the following settings:  
Use CVP  
Allow CVP server to modify content  
Return data after content is approved  
He adds two rules to his Rule Base: one to inspect HTTP traffic going to known forbidden sites, the other to allow all other HTTP traffic.  
Wayne sees HTTP traffic going to those problematic sites is not prohibited.  
What could cause this behavior?

**A. The Security Server is not configured correctly.**

**B. The Security Server Rule is after the general HTTP Accept Rule.**

**C. The Security Server is communicating with the CVP server, but no restriction is defined in the CVP server.**

**D. The Security Server is not communicating with the CVP server.**

What is the command to upgrade a SecurePlatform NG with Application Intelligence (Al) R55 SmartCenter Server to VPN-1 NGX using a CD?

**A. patch add cd**

**B. cd patch add**

**C. fwm upgrade\_tool**

**D. patch add**

**E. cppkg add**

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. None**

**B. Hide NAT**

**C. Hide NAT**

**D. Static NAT**

**E. Manual NAT**

Which of the following explains Role Segregation?

**A. SmartWorkflow can be configured so that managers can only view their assigned sessions**

**B. Different tasks within SmartDashboard are divided according to firewall administrator permissions.**

**C. Changes made by an administrator in a SmartWorkflow session must have managerial approval prior to commitment.**

**D. Administrators have different abilities than managers within SmartWorkflow.**

What is the command to upgrade an NG with Application Intelligence R55 Smart Center running on SecurePlatform to VPN-1 NGX R65?

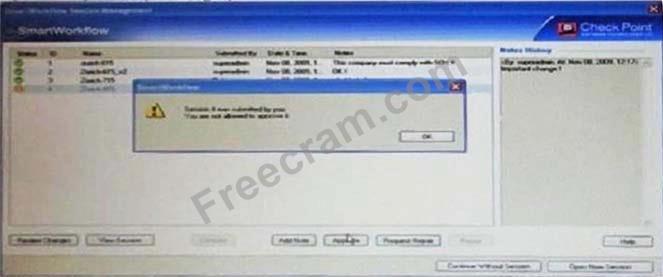
**A. fw install\_mgmt**

**B. upgrade\_mgmt**

**C. patch add cd**

**D. fwm upgrade\_tool**

David is the MultiCorp Security Manager and approves the proposals submitted by the Security Administrator Peter. One day, David believes he has detected a vulnerability in the Security Policy. He submits a change proposal and tries to approve his own submission. The system does not allow him to perform this procedure.



What is the reason for this behavior?

**A. The company does not allow David to submit and approve the same policy change. The setting Manager cannot approve their submitted sessions in Global Properties was set to On.**

**B. The proposal contains some logical contradictions. The Check Point verification control does not permit this change to be carried out.**

**C. The company does not allow David to submit and approve the same policy change. The setting Manager cannot approve their submitted sessions in the SmartWorkflow section of the Firewall object properties was set to On.**

**D. The company does not allow David to submit and also approve the same policy change. David was assigned the Approve only permission (instead of Submit and Approve).**

What port is used for Administrator access for your SSL VPN?

**A. 4433**

**B. 80**

**C. 443**

**D. 4434**

Damon enables an SMTP resource for content protection.

He notices that mail seems to slow down on occasion, sometimes being delivered late.  
Which of the following might improve throughput performance?

**A. Configuring the SMTP resource to bypass the CVP resource**

**B. Configuring the SMTP resource to only allow mail with Damon's company's domain name in the header**

**C. Configuring the CVP resource to return the mail to the Gateway**

**D. Configuring the Content Vector Protocol (CVP) resource to forward the mail to the internal SMTP server, without waiting for a response from the Security Gateway**

**E. Increasing the Maximum number of mail messages in the Gateway's spool directory**

How does ClusterXL Unicast mode handle new traffic?

**A. All cluster members' process all packets and members synchronize with each other. The pivot is responsible for the master sync catalog**

**B. The pivot machine receives and inspects all new packets then synchronizes the connections with other members**

**C. The pivot machine receives all the packets and runs an algorithm to determine which member should process the packets**

**D. All members receive all packets. The Security Management Server decides which member will process the packets. Other members delete the packets from memory.**

If a SmartUpdate upgrade or distribution operation fails on SecurePlatform, how is the system recovered?

**A. The Administrator must reinstall the last version via the command cprinstall revert <object name><file name>.**

**B. The Administrator must remove the rpm packages manually, and reattempt the upgrade.**

**C. The Administrator can only revert to a previously created snapshot (if there is one) with the command cprinstall snapshot <object name><filename>.**

**D. SecurePlatform will reboot and automatically revert to the last snapshot version prior to upgrade.**

Central License management allows a Security Administrator to perform which of the following? Select all that apply.

**A. Attach and/or delete only NGX Central licenses to a remote module (not Local licenses)**

**B. Attach both NGX Central and Local licenses to a remote module**

**C. Add or remove a license to or from the license repository**

**D. Check for expired licenses**

**E. Sort licenses and view license properties**

**F. Delete both NGX Local licenses and Central licenses from a remote module**

Your VPN Community includes three Security Gateways. Each Gateway has its own internal network defined as a VPN Domain. You must test the VPN-1 NGX route-based VPN feature, without stopping the VPN. What is the correct order of steps?

**A. 1. Add a new interface on each Gateway.**

**2. Remove the newly added network from the current VPN Domain in each gateway object.**

**3. Create VPN Tunnel Interfaces (VTI) on each gateway object, to point to the other two peers.**

**4. Add static routes on three Gateways, to route the new network to each peer's VTI interface.**

**B. 1. Add a new interface on each Gateway.**

**2. Add the newly added network into the existing VPN Domain for each Gateway.**

**3. Create VTIs on each gateway object, to point to the other two peers.**

**4. Enable advanced routing on all three Gateways.**

**C. 1. Add a new interface on each Gateway.**

**2. Add the newly added network into the existing VPN Domain for each gateway object.**

**3. Create VTIs on each gateway object, to point to the other two peers.**

**4. Add static routes on three Gateways, to route the new networks to each peer's VTI interface.**

**D. 1. Add a new interface on each Gateway.**

**2. Remove the newly added network from the current VPN Domain for each Gateway.**

**3. Create VTIs on each Gateway, to point to the other two peers**

**4. Enable advanced routing on all three Gateways.**

Which of the following does IPSec use during IPSec key negotiation?

**A. ISAKMP SA**

**B. IPSec SA**

**C. Diffie-Hellman exchange**

**D. RSA Exchange**

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

**A. SMTP**

**B. FTP**

**C. rlogin**

**D. Telnet**

**E. HTTP**

How does a standby SmartCenter Server receive logs from all Security Gateways, when an active SmartCenter Server fails over?

**A. On the Log Servers screen (from the Logs and Masters tree on the gateway object's General Properties screen), add the secondary SmartCenter Server object as the additional log server. Reinstall the Security Policy.**

**B. The secondary Server's host name and IP address must be added to the Masters file, on the remote Gateways.**

**C. Establish Secure Internal Communications (SIC) between the primary and secondary Servers. The secondary Server can then receive logs from the Gateways, when the active Server fails over.**

**D. Create a Check Point host object to represent the standby SmartCenter Server. Then select "Secondary SmartCenter Server" and Log Server", from the list of Check Point Products on the General properties screen.**

**E. The remote Gateways must set up SIC with the secondary SmartCenter Server, for logging.**

Using the Backup Target functionality in SmartProvisioning, what targets are available?

i) FTP

ii) TFTP

iii) SFTP

iv) SCP

v) Locally

**A. ii, iv, v**

**B. i**

**C. i, ii, iv**

**D. i, ii, iii, iv**

Which is NOT a method through which Identity Awareness receives its identities?

**A. Group Policy**

**B. Captive Portal**

**C. Identity Agent**

**D. AD Query**

Your current VPN-1 NG with Application Intelligence (Al) R55standalone VPN-1 Pro Gateway and SmartCenter Server run on SecurePlatform.

You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the SmartCenter Server, and a new machine will be the VPN-1 Pro Gateway only.

You need to migrate the NG with Al R55 SmartCenter Server configuration, including such items as Internal Certificate Authority files, databases, and Security Policies.

How do you request a new license for this VPN-1 NGX upgrade?

**A. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new central license for the NGX VPN-1 Pro Gateway.**

**B. Request a VPN-1 NGX SmartCenter Server license, using the new machine's IP address. Request a new local license for the NGX VPN-1 Pro Gateway.**

**C. Request a new VPN-1 NGX SmartCenter Server license, using the NG with Al SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway.**

**D. Request a VPN-1 NGX SmartCenter Server license, using the NG with Al SmartCenter Server IP address. Request a new central license for the NGX VPN-1 Pro Gateway, licensed for the existing SmartCenter Server IP address.**

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. MD5 Hash Completion**

**B. DES Key Reset**

**C. Perfect Forward Secrecy**

**D. SHA1 Hash Completion**

**E. Phase 3 Key Revocation**

If traffic requires preferential treatment by other routers on the network, in addition to the QoS module, which Check Point QoS feature should be used?

**A. Differentiated Services**

**B. Low Latency Queuing**

**C. Weighted Fair Queuing**

**D. Guarantees**

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

**A. After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the Package Repository on the SmartCenter Server.**

**B. After selecting "Packages: Add... from CD", the selected package is copied to the Package Repository on the SmartCenter Server.**

**C. After selecting "Packages: Add... from CD", the selected package is copied to the packages directory on the selected remote Security Gateway.**

**D. After selecting "Packages: Add... from CD", the entire contents of the CD are copied to the packages directory on the selected remote Security Gateway.**

From the following output of cphaprob state,



Which ClusterXL mode is this?

**A. Multicast mode**

**B. Legacy mode**

**C. New mode**

**D. Unicast mode**

**E. Load Balancing Mode**

What tool exports the Management Configuration into a single file?

**A. CPConfig\_Export**

**B. Backup**

**C. migrate export**

**D. Upgrade\_Export**

Identify the correct step performed by SmartUpdate to upgrade a remote Security Gateway.

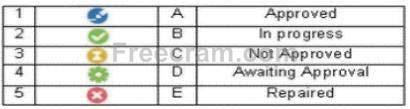
**A. After selecting "Packages > Distribute..." and choosing the target gateway, the SmartUpdate wizard walks the Administrator through a Distributed Installation.**

**B. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the Package Repository on the SmartCenter to the Security Gateway but the installation IS NOT performed.**

**C. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the CDROM of the SmartUpdate PC directly to the Security Gateway and the installation IS performed.**

**D. After selecting "Packages > Distribute..." and choosing the target gateway, the selected package is copied from the Package Repository on the SmartCenter to the Security Gateway and the installation IS performed.**

Match the SmartDashboard session status icons with the appropriate SmartWorkflow session status:



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

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

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

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

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

**A. Low Latency Queuing**

**B. Differentiated Services**

**C. Weighted Fair Queuing**

**D. Guarantees**

What happens when an Administrator activates the DLP Portal for Self Incident Handling and enters its fully qualified domain name (DNS name)?

**A. User Check is activated.**

**B. Connections created between the user and the DLP Gateway when clicking links within e-mail notifications to send or discard quarantined e-mails (matched for an Ask User rule) are encrypted.**

**C. The DLP Gateway can now notify Data Owners about DLP incidents.**

**D. The daemon running DLP Portal starts to run and can cater requests from users' browsers (following links from e-mail notifications) and from Check Point User Check.**

Which version is the minimum requirement for SmartProvisioning?

**A. R70**

**B. R71**

**C. R65 HFA 40**

**D. R70.20**

What is the consequence of clearing the "Log VoIP Connection" box in Global Properties?

**A. The log field setting in rules for VoIP protocols are ignored.**

**B. Dropped VoIP traffic is logged, but accepted VoIP traffic is not logged.**

**C. IP addresses are used, instead of object names, in log entries that reference VoIP Domain objects.**

**D. The SmartCenter Server stops importing logs from VoIP servers.**

**E. VoIP protocol-specific log fields are not included in SmartView Tracker entries.**

Which of the following can NOT be modified by editing the cp\_httpd\_admin.conf file?

**A. Administrative Access Level**

**B. Modifying Web server certificate attributes**

**C. The web server port**

**D. Toggling HTTP or HTTPS protocol use**

For a dedicated DLP Gateway that runs in inline bridge mode, why is it important to properly define the topology?

**A. Topology definition is necessary for correct anti-spoofing.**

**B. Topology definition is used for VPN communities definition.**

**C. Topology is used for Hide NAT.**

**D. By default. My Organization is defined by the internal interfaces of a DLP Gateway.**

You have an internal FTP server, and you allow downloading, but not uploading.  
Assume Network Address Translation is set up correctly, and you want to add an inbound rule with:  
Source: Any  
Destination: FTP server  
Service: FTP resources object.  
How do you configure the FTP resource object and the action column in the rule to achieve this goal?

**A. Enable only the "Get" method in the FTP Resource Properties and use it in the rule, with action drop.**

**B. Disable "Get" and "Put" methods in the FTP Resource Properties and use it in the rule, with action accept.**

**C. Enable only the "Get" method in the FTP Resource Properties, and use this method in the rule, with action accept.**

**D. Enable both "Put" and "Get" methods in the FTP Resource Properties and use them in the rule, with action drop.**

**E. Enable only the "Put" method in the FTP Resource Properties and use it in the rule, with action accept.**

When configuring site-to-site VPN High Availability (HA) with MEP, which of the following is correct?

**A. MEP Gateways must be managed by the same SmartCenter Server.**

**B. The decision on which MEP Gateway to use is made on the MEP Gateway's side of the tunnel.**

**C. If one MEP Security Gateway fails, the connection is lost and the backup Gateway picks up the next connection.**

**D. MEP Gateways cannot be geographically separated machines.**

What action CANNOT be run from SmartUpdate NGX R65?

**A. Get all Gateway Data**

**B. Preinstall verifier**

**C. Reboot gateway**

**D. Fetch sync status**

In SmartWorkflow, what is NOT a valid possibility?

**A. Task Flow with Session but without Role Segregation**

**B. Task Flow without Session but with Role Segregation**

**C. Task Flow without Session and without Role Segregation**

**D. Task Flow with Session and with Role Segregation**

A user cannot authenticate to SSL VPN. You have verified the user is assigned a user group and reproduced the problem, confirming a failed-login session. You do not see an indication of this attempt in the traffic log. The user is not using a client certificate for login.  
To debug this error, where in the authentication process could the solution be found?

**A. cpauth**

**B. cvpnd**

**C. admin**

**D. apache**

What is the maximum number of cores supported by CoreXL?

**A. 12**

**B. 6**

**C. 8**

**D. 4**

How would you configure a rule in a Security Policy to allow SIP traffic from end point Net\_Ato end point Net\_B, through an NGX Security Gateway?

**A. Net\_A/Net\_BM3lP/accept**

**B. Net\_A/Net\_B/VolP\_any/accept**

**C. Net\_A/Net\_B/sip and sip\_any/accept**

**D. Net\_A/Net\_B/sip/accept**

SmartProvisioning uses different types of profiles to manage and provision the gateways.  
These types are:

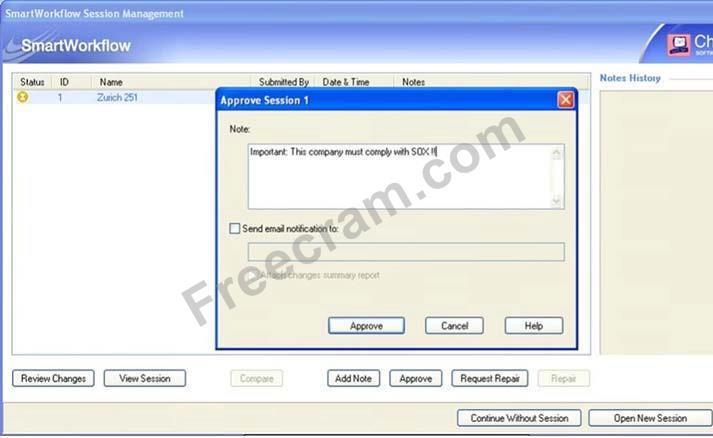
**A. Provisioning Profiles and Gateways Profiles**

**B. SmartLSM Security Profiles and Provisioning Profiles**

**C. SmartLSM Security Profiles and SmartDashboard Profiles**

**D. SmartConsole Profiles and SmartFilter Profiles**

When a security administrator logs in to SmartDashboard and selects Continue without session from the following window,what kind of access will be granted to him in SmartDashboard?



**A. No access will be granted, he will be logged out of SmartDashboard.**

**B. He will get read-only access to the policy, network objects and session management.**

**C. A new session will automatically be created with a default session name along with date and time. All changes made by the manager will be saved in this new session.**

**D. He will get read-only access to the policy and network objects; however, he can still manage the sessions, i.e. Approve, Request Repair etc.**

What is the greatest benefit derived from VPNs compared to frame relay, leased lines any other types of dedicated networks?

**A. lower cost**

**B. Greater performance**

**C. stronger authentication**

**D. Less failure/downtime**

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

**A. Burst traffic matching the Default Rule is exhausting the Check Point QoS global packet buffers.**

**B. The Constant Bit Rate for a Low Latency Class has been exceeded by greater than 10%, and the Maximal Delay is set below requirements.**

**C. The guarantee of one of the rule's sub-rules exceeds the guarantee in the rule itself.**

**D. The number of guaranteed connections is exceeded. The rule's action properties are not set to accept additional connections.**

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

**A. The related end points domain specifies an address range.**

**B. The VoIP gateway object must be added to the group, before the VoIP Domain SIP object is eligible to be added to the group.**

**C. VoIP Domain SIP objects cannot be placed in simple groups.**

**D. The installed VoIP gateways specify host objects.**

**E. The VoIP Domain SIP object's name contains restricted characters.**

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 "Puzzles", and Support IKE DoS protection from unidentified source to "Stateless".**

**B. Set Support IKE DoS protection from identified source to "Stateless", and Support IKE DoS protection from unidentified source to "None".**

**C. Set Support IKE Dos Protection from identified source, and Support IKE DoS protection from unidentified source to "Puzzles".**

**D. Set Support IKE DoS protection from identified source to "Stateless," and Support IKE DoS protection from unidentified source to "Puzzles".**

**E. Set "Support IKE DoS protection" from identified source, and "Support IKE DoS protection" from unidentified source to "Stateless".**

Which Protection Mode does not exist in IPS?

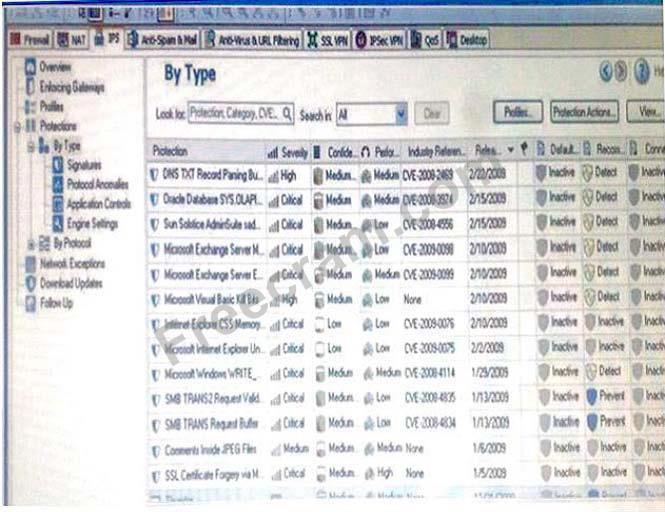
**A. Detect**

**B. Inactive**

**C. Allow**

**D. Prevent**

Laura notices the Microsoft Visual Basic Bits Protection is set to inactive. She wants to set the Microsoft Visual Basic Kill Bits Protection and all other Low Performance Impact Protections to Prevent. She asks her manager for approval and stated she can turn theses on.  
But he wants Laura to make sure no high Performance Impacted Protections are turned on while changing this setting.



Using the out below, how would Laura change the Default\_Protection on Performance Impact Protections classified as low from inactive to prevent until meeting her other criteria?

**A. Go to Profiles / Default\_Protection and select Do not activate protections with performance impact to low or above**

**B. Go to Profiles / Default\_Protection and uncheck Do not activate protections with performance impact to medium or above**

**C. Go to Profiles / Default\_Protection and uncheck Do not activate protections with performance impact to high or above**

**D. Go to Profiles / Default\_Protection and select Do not activate protections with performance impact to medium or above**

What action can be run from SmartUpdate NGX R65?

**A. mds\_backup**

**B. upgrade\_export**

**C. cpinfo**

**D. remote\_uninstall\_verifier**

Your current stands alone VPN-1 NG with Application Intelligence (Al) R55 installation is running on SecurePlatform. You plan to implement VPN-1 NGX in a distributed environment, where the existing machine will be the VPN-1 Pro Gateway. An additional machine will serve as the SmartCenter Server. The new machine runs on a Windows Server 2003.  
You need to upgrade the NG with Al R55 SmartCenter Server configuration to VPN-1 NGX.  
How do you upgrade to VPN-1 NGX?

**A. Run the backup command in the existing SecurePlatform machine, to create a backup file.**

**Copy the file to the Windows Server 2003.**

**Uninstall all Check Point products on SecurePlatform by running rpm CPsuite.**

**R55 command.**

**Reboot.**

**Install new VPN-1 NGX on the existing SecurePlatform machine.**

**Run sysconfig, select VPN-1 Pro Gateway, and reboot.**

**Use VPN-1 NGX CD to install primary SmartCenter Server on the Windows Server 2003.**

**Import the backup file.**

**B. Run backup command on the existing SecurePlatform machine to create a backup file.**

**Copy the file to the Windows Server 2003.**

**Uninstall the primary SmartCenter Server package from NG with Al R55 SecurePlatform using sysconfig.**

**Reboot.**

**Install the NGX primary SmartCenter Server and import the backup file.**

**Open the NGX SmartUpdate, and select "upgrade all packages" on the NG with Al R55 Security Gateway.**

**C. Insert the NGX CD in the existing NGwithAI R55 SecurePlatform machine, and answer yes to backup the configuration.**

**Copy the backup file to the Windows Server 2003.**

**Continue the upgrade process.**

**Reboot after upgrade is finished.**

**After SecurePlatform NGX reboots, run sysconfig, select VPN-1 Pro Gateway, and finish the sysconfig process.**

**Reboot again.**

**Use the NGX CD to install the primary SmartCenter on the Windows Server 2003.**

**Import the backup file.**

**D. Copy the $FWDIR\conf and $FWDIR\lib files from the existing SecurePlatform machine.**

**Create a tar.gzfile, and copy it to the Windows Server 2003.**

**Use VPN-1 NGX CD on the existing SecurePlatform machine to do a new installation.**

**Reboot.**

**Run sysconfig and select VPN-1 Pro Gateway.**

**Reboot.**

**Use the NGX CD to install the primary SmartCenter Server on the Windows Server 2003.**

**On the Windows Server 2003, run upgradeimport command to import $FWDIR\conf and $FWDIR\lib from the SecurePlatform machine.**

How is change approved for implementation in SmartWorkflow?

**A. The change is submitted for approval and is manually installed by the original submitter the next time he logs in after approval of the change.**

**B. The change is submitted for approval and is automatically installed by the original submitter the next time he logs in after approval of the change.**

**C. The change is submitted for approval and is automatically installed by the approver once Approve is clicked.**

**D. The change is submitted for approval and is manually installed by the approver once Approve is clicked.**

What happens in relation to the CRL cache after a cpstop;spstart has been initiated?

**A. The gateway continues to use the old CRL even if it is not valid, until a new CRL is cached**

**B. The gateway issues a crl\_zap on startup, which empties the cache and forces Certificate retrieval.**

**C. The gateway continues to use the old CRL, as long as it is valid.**

**D. The gateway retrieves a new CRL on startup, then discards the old CRL as invalid.**

Which encryption scheme provides in-place encryption?

**A. SKIP**

**B. DES**

**C. AES**

**D. IKE**

Which of the following items can be provisioned via a Profile through SmartProvisioning?  
i) Backup Schedule  
ii) DNS Entries  
iii) Hosts Table  
iv) Domain Name  
v) Interface IP's

**A. i, ii, iv**

**B. i, ii, iii, iv**

**C. i, ii, iii, iv, v**

**D. i**

Concerning these products: SecurePlatform, VPN-1 Pro Gateway, UserAuthority Server, Nokia OS, UTM-1, Eventia Reporter, and Performance Pack, which statement is TRUE?

**A. All can be upgraded to VPN-1 NGX R65 with SmartUpdate.**

**B. All but Performance Pack can be upgraded to VPN-1 NGX R65 with SmartUpdate.**

**C. All but the Nokia OS can be upgraded to VPN-1 NGX R65 with SmartUpdate.**

**D. All but the UTM-1 can be upgraded to VPN-1 NGX R65 with SmartUpdate.**

What is the advantage for deploying SSL VPN in a DMZ, versus a LAN?

**A. SSL VPN adds another layer of access security to internal resources, when it resides in a DMZ.**

**B. Traffic is in clear text when forwarded to internal servers, but the back connection is encrypted for remote users**

**C. Traffic is authenticated without hiding behind Connectra's IP address**

**D. SSL Network Extender is ineffective in a LAN deployment.**

You receive an alert indicating a suspicious FTP connection is trying to connect to one of your internal hosts. How do you block the connection in real time and verify the connection is successfully blocked?

**A. Highlight the suspicious connection in SmartView Tracker > Active mode.**

**Block the connection using Tools > Block Intruder menu.**

**Use Active mode to confirm that the suspicious connection is dropped.**

**B. Highlight the suspicious connection in SmartView Tracker > Log mode.**

**Block the connection using Tools > Block Intruder menu.**

**Use Log mode to confirm that the suspicious connection does not reappear.**

**C. Highlight the suspicious connection in SmartView Tracker > Log mode.**

**Block the connection using Tools > Block Intruder menu.**

**Use the Log mode to confirm that the suspicious connection is dropped.**

**D. Highlight the suspicious connection in SmartView Tracker > Active mode.**

**Block the connection using the Tools > Block Intruder menu.**

**Use the Active mode to confirm that the suspicious connection does not reappear.**

For object-based VPN routing to succeed, what must be configured?

**A. No rules need to be created, implied rules that cover inbound and outbound traffic on the central (HUB) Gateway are already in place from Policy > Properties > Accept VPN-1 Control Connections.**

**B. At least two rules in the Rule Base must created, one to cover traffic inbound and the other to cover traffic outbound on the central (HUB) Security Gateway.**

**C. VPN routing is not configured in the Rule Base or Community objects. Only the native- routing mechanism on each Gateway can direct the traffic via its VTI configured interfaces.**

**D. A single rule in the Rule Base must cover traffic in both directions, inbound and outbound on the central (HUB) Security Gateway.**

What does it mean when a Security Gateway is labeled Untrusted in the SmartProvisioning Status view?

**A. SmartProvisioning is not enabled on the Security Gateway.**

**B. The Security Gateway is down.**

**C. cpd is not running at the Security Gateway.**

**D. SIC has not been established between the Security Gateway and the Security Management.**

Your customer wishes to install the SmartWorkflow Software Blade on a R70 Security Management server (Secure Platform).  
Which is the correct method?

**A. The SmartWorkflow Software Blade is included in the standard R70 version. You need to enable it via cpconfig.**

**B. The SmartWorkflow works directly on the version R70. Install the SmartWorkflow as an add-on. The version of the Management server remains R70.**

**C. You must upgrade the Management Server to the version R70.1 first before you start the installation of the SmartWorkflow Software Blade plug-in.**

**D. When you install the R70.1 package on an R70 Security Management server, it will be upgraded to version R70.1 with SmartWorkflow.**

Where is the ideal place to deploy your SSL VPN?

**A. Anywhere**

**B. In front of the external interface on the gateway**

**C. SSL VPN enabled on the gateway**

**D. Deployed in DMZ**

A cluster contains two members, with external interfaces 172.28.108.1 and 172.28.108.2. The internal interfaces are 10.4.8.1 and 10.4.8.2. The external cluster's IP address is 172.28.108.3, and the internal cluster's IP address is 10.4.8.3. The synchronization interfaces are 192.168.1.1 and 192.168.1.2. The Security Administrator discovers State Synchronization is not working properly, cphaprob if command output displays as follows:

What is causing the State Synchronization problem?

**A. The synchronization interface on the cluster member object's Topology tab is enabled with "Cluster Interface". Disable this interface.**

**B. Interfaces 192.168.1.1 and 192.168.1.2 have defined 192.168.1.3 as a sub. interface.**

**C. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.**

**D. The synchronization network has a cluster, with IP address 192.168.1.3 defined in the gateway-cluster object. Remove the 192.168.1.3 VIP interface from the cluster topology.**

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

**A. If a guarantee is defined in a sub-rule, then a guarantee must be defined for the rule above it.**

**B. If both a rule limit and a per connection limit are defined for a rule, the per connection limit must not be greater than the rule limit.**

**C. If both a limit and a guarantee per rule are defined in a QoS rule, then the limit must be smaller than the guarantee.**

**D. A rule guarantee must not be less than the sum the guarantees defined in its sub-rules.**

What happens to the session information after they are approved and a policy installation is done?

**A. Session information can only be deleted before a policy is installed.**

**B. Session information is never deleted from the database.**

**C. An option is given to retain the session information, default being deletion of session information from the database.**

**D. It depends on the SmartWorkflow settings in Global Properties.**

What physical machine must have access to the UserCenter public IP when checking for new packages with SmartUpdate?

**A. VPN-1 Security Gateway getting the new upgrade package**

**B. SmartUpdate GUI PC**

**C. SmartUpdate installed SmartCenter Server PC**

**D. SmartUpdate Repository SQL database Server**

You are responsible for the IPS configuration of your Check Point firewall. Inside the Denial of service section you need to set the protection parameters against the Teardrop attack tool with high severity. How would you characterize this attack tool? Give the BEST answer.



**A. Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Sending two IP fragments, the latter entirely contained inside the former, causes the server to allocate too much memory and crash. Teardrop is a widely available attack tool that exploits this vulnerability.**

**B. A remote attacker may attack a system by sending a specially crafted RPC request to execute arbitrary code on a vulnerable system. Teardrop is a widely available attack tool that exploits this vulnerability.**

**C. Hackers can send high volumes of non-TCP traffic in an effort to fill up a firewall State Table. This results in a Denial of Service by preventing the firewall from accepting new connections. Teardrop is a widely available attack tool that exploits this vulnerability.**

**D. Some implementations of TCP/IP are vulnerable to packets that are crafted in a particular way (a SYN packet in which the source address and port are the same as the destination, i.e., spoofed). Teardrop is a widely available attack tool that exploits this vulnerability**

To change the default port of the Management Portal:

**A. Re-initialize SIC**

**B. Modify the file cp\_httpd\_admin .conf.**

**C. Edit the masters. conf file on the Portal server.**

**D. Run sysconfig and change the management interface**

Which of the following is a TRUE statement concerning contract verification?

**A. Your contract file is stored on the User Center and fetched by the Gateway as needed.**

**B. Your contract file is stored on the SmartCenter Server and downloaded to the Security Gateway.**

**C. Your contract file is stored on the SmartConsole and downloaded to the SmartCenter Server.**

**D. Your contract file is stored on the SmartConsole and downloaded to the Gateway.**

Which is the BEST configuration option to protect internal users from malicious Java code, without stripping Java scripts?

**A. Use the URI resource to block Java code**

**B. Use the URI resource to strip ActiveX tags**

**C. Use the URI resource to strip applet tags**

**D. Use CVP in the URI resource to block Java code**

Which type of service should a Security Administrator use in a Rule Base to control access to specific shared partitions on target machines?

**A. CIFS**

**B. URI**

**C. HTTP**

**D. Telnet**

**E. FTP**

What is NOT true about Management Portal?

**A. Management Portal could be reconfigured for using HTTP instead of HTTPS**

**B. Choosing Accept control connections in Implied Rules includes Management Portal access**

**C. Management Portal requires a license**

**D. Default Port for Management Portal access is 4433**

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

**A. Star**

**B. Mesh**

**C. Map**

**D. Remote Access**

What is the bit size of DES?

**A. 32**

**B. 56**

**C. 128**

**D. 112**

**E. 168**

**F. 64**

Management Portal should be installed on:

(i) Management Server  
(ii) Security Gateway  
(iii) Dedicated Server

**A. (i) or (ii) only**

**B. All are possible solutions**

**C. (ii) only**

**D. (iii) only**

What is the significance of the depicted icon in the SmartWorkflow toolbar?



**A. Session has been approved.**

**B. Overall status information: Everything is OK.**

**C. Check the consistency of SmartWorkflow sessions.**

**D. Submit for Approval**

Which file can you modify to change settings of the Management Portal?

For example: changing the webserver port or to use HTTP instead of HTTPS.

**A. cp\_http\_admin.conf**

**B. cp\_http.conf**

**C. cp\_httpd\_admin.conf**

**D. cp\_httpd.conf**

Which network port does PPTP use for communication?

**A. 1723/tcp**

**B. 25/tcp**

**C. 25/udp**

**D. 1723/udp**

Your customer wishes to use SmartWorkflow Software Blade, but he also wishes to install a policy during an emergency without an approval. Is it possible?

**A. Yes, it is possible but the administrator must receive special administrator permission, i.e., Can install in emergency. You can use the new GUI to set the administration security setting.**

**B. No, if a customer uses the SmartWorkflow Software Blade, a policy must be approved.**

**C. Yes, it is possible, but this feature must be configured in Global Properties and the administrator must provide a special password.**

**D. Yes, it is possible, but this feature must be configured in the Global Properties. The administrator must provide a special password and the reason for this emergency installation.**

SmartProvisioning can provision the Operating System and network settings on which of the following?

**A. NGX Security Appliances**

**B. IPSO 4.2 Security Gateways**

**C. Edge firmware 6.x and above**

**D. R65 HFA 40 Security Gateways arid above**

The Management Portal Software Blade allows users to

**A. Add/Delete rules**

**B. Monitor traffic flows**

**C. Create/Modify objects**

**D. View Security Policies**

Which of the following is part of the PKI? Select all that apply.

**A. Public-key certificate**

**B. User certificate**

**C. Attribute Certificate**

**D. Certificate Revocation Lists**

Robert has configured a Common Internet File System (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 shared partition, 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 do not allow administrative locks.**

**C. Null CIFS sessions are blocked.**

**D. Access violations are not logged.**

**E. Remote registry access is blocked.**

Problems sometimes occur when distributing IPSec packets to a few machines in a Load Sharing Multicast mode cluster, even though the machines have the same source and destination IP addresses. What is the best Load Sharing method for preventing this type of problem?

**A. Load Sharing based on IP addresses, ports, and serial peripheral interfaces (SPI)**

**B. Load Sharing based on SPIs and ports only**

**C. Load Sharing based on IP addresses and ports**

**D. Load Sharing based on IP addresses only**

**E. Load Sharing based on SPIs only**

Which procedure will create an Internal User?

**A. From the SSL VPN tab, click Users and Authentication I Internal Users I Users and click New User I Default**

**B. In the General Properties of the gateway, click the SSL VPN check box. The SSL VPN Blade Wizard will launch and Step 2 will allow adding new users who will be imported from a RADIUS server.**

**C. In the Users and Administrators tab, click User Groups I Clientless-vpn-user and add the SSL VPN user to the Clientless-vpn-user group**

**D. In the Users and Administrators tab, right click Users and click SSL VPN User**

After installing VPN-1 Pro NGQ R65, you discover that one port on your Intel Quad NIC on the Security Gateway is not fetched by a get topology request. What is the most likely cause and solution?

**A. If an interface is not configured, it is not recognized. Assign an IP and subnet mask using the Web UI.**

**B. The NIC is faulty. Replace it and reinstall.**

**C. Your NIC driver is installed but was not recognized. Apply the latest Secure PlatformR65 Hotfix Accumulator (HFA).**

**D. Make sure the driver for you particular NIC is available, and reinstall. You will be prompted for the driver.**

In Company XYZ, the DLP Administrator defined a new Keywords Data Type that contains a list of secret project names; i.e., Ayalon, Yarkon, Yarden. The threshold is set to At least 2 keywords or phrases. Based on this information, which of the following scenarios will be a match to the Rule Base?

**A. An MS Excel file that contains the following text Mort resources for Yarkon project..**

**Are you certain this is about Yarden?**

**B. A PDF file that contains the following text**

**Yarkon1 can be the code name for the new product.**

**Yardens list of protected sites**

**C. A word file that contains the following text will match:**

**Ayalon**

**ayalon**

**AYALON**

**D. A password protected MS Excel file that contains the following text Ayalon Yarkon Yarden**

One profile in SmartProvisioning can update:

**A. Only Clustered Gateways.**

**B. Potentially hundreds and thousands of gateways.**

**C. Profiles are not used for updating, just reporting.**

**D. Specific gateways.**

What can be said about RSA algorithms? Select all that apply.

**A. Short keys can be used for RSA efficiency.**

**B. RSA is faster to compute than DES**

**C. Long keys can be used in RSA for enhances security**

**D. RSA's key length is variable.**

Cody is notified by blacklist.org that his site has been reported as a spam relay, due to his SMTP 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 allow only mail to or from names, within Cody's corporate domain.**

**B. Configure the SMTP Security Server to perform filtering, based on IP address and SMTP protocols.**

**C. Configure the SMTP Security Server to work with an OPSEC based product, for content checking.**

**D. Configure the SMTP Security Server to perform MX resolving.**

**E. Configure the SMTP Security Server to apply a generic "from" address to all outgoing mail.**

You are configuring the VoIP Domain object for a Skinny Client Control Protocol (SCCP) environment protected by VPN-1 NGX. Which VoIP Domain object type can you use?

**A. Proxy**

**B. Gatekeeper**

**C. CallManager**

**D. Transmission Router**

**E. Gateway**

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 clear text.  
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", and put FTP and HTTP in the 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.**

**C. 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.**

**D. 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.**

Which of these components does NOT require a VPN-1 NGX R65 license?

**A. SmartUpdate upgrading/patching**

**B. Check Point Gateway**

**C. SmartCenter Server**

**D. SmartConsole**

In ClusterXL, which of the following processes are defined by default as critical devices?

**A. fwd**

**B. cphad**

**C. fwm**

**D. fwd.proc**

What GUI client would you use to view an IPS packet capture?

**A. SmartView Monitor.**

**B. SmartView Tracker.**

**C. Smart Update.**

**D. Smart Reporter.**

Which of the following is supported with Office Mode?

**A. Secure mode**

**B. SSL Network Extender**

**C. Secure Client**

**D. Connect Mode**

You just upgraded to R71 and are using the IPS Software Blade.  
You want to enable all critical protections while keeping the rate of false positive very low.  
How can you achieve this?

**A. This can't be achieved; activating any IPS system always causes a high rate of false positives.**

**B. As in SmartDefense, this can be achieved by activating all the critical checks manually.**

**C. new IPS system is based on policies, but it has no ability to calculate or change the confidence level, so it always has a high rate of false positives.**

**D. The new IPS system is based on policies and gives you the ability to activate all checks with critical severity and a high confidence level.**

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

**A. IKE VPNs: AES encryption for IKE Phase 1, and AES encryption for Phase 2; SHA1 hash**

**B. IKE VPNs: AES encryption for IKE Phase 1, and DES encryption for Phase 2; SHA1 hash**

**C. IKE VPNs: DES encryption for IKE Phase 1, and 3DES encryption for Phase 2; MD5 hash**

**D. IKE VPNs: SHA1 encryption for IKE Phase 1, and MD5 encryption for Phase 2; AES hash**

**E. IKE VPNs: CAST encryption for IKE Phase 1, and SHA1 encryption for Phase 2; DES hash**

You are running the license\_upgrade tool on your SecurePlatform Gateway.  
Which of the following can you NOT do with the upgrade tool?

**A. View the licenses in the SmartUpdate License Repository.**

**B. Simulate the license-upgrade process.**

**C. View the status of currently installed licenses.**

**D. Perform the actual license-upgrade process.**

Public keys and digital certificates provide which of the following? Select three.

**A. Non repudiation**

**B. Data integrity**

**C. Availability**

**D. Authentication**

VPN traffic control would fall under which VPN component?

**A. QoS**

**B. Security**

**C. Management**

**D. Performance**

Using SmartProvisioning Profiles, which of the following could be configured for both Secure Platform and UTM-1 Edge devices?  
(i) Backup  
(ii) Routing  
(iii) Interfaces  
(iv) Hosts  
(v) NTP server  
(vi) DNS

**A. (ii), (iii), (iv) and (vi)**

**B. none of these options are available for both.**

**C. (i), (ii) and (iv)**

**D. (i), (iii), (iv) and (vi)**

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

**A. guaranteed per connection**

**B. Low latency class**

**C. Weighted Fair queuing**

**D. guaranteed per VoIP rule**

When upgrading to NGX R65, which Check Point products do not require a license upgrade to be current?

**A. VPN-1 NGX (R60) and later**

**B. None, all versions require a license upgrade**

**C. VPN-1 NG with Application Intelligence (R54) and later**

**D. VPN-1 NGX (R64) and later**

Which of the following SSL Network Extender server-side prerequisites are correct? Select all that apply.

**A. The specific VPN-1 Security Gateway must be configured as a member of the VPN-1 Remote Access Community.**

**B. There are distinctly separate access rules required for Secure Client users vs. SSL Network Extender users.**

**C. The VPN1-Gateway must be configured to work with Visitor Mode**

**D. To use Integrity Clientless Security (ICS), you must install the ICS server or configuration tool.**

Which of the following can NOT approve a change in a SmartWorkflow session?

**A. Provider-1Super users**

**B. CustomerSuper users**

**C. FirewallAdministrators**

**D. FirewallManagers**

Mark the configuration options that are available for Data Loss Prevention in R71.

**A. The DLP as an integrated software blade which can be enabled on a Check Point Security Gateway running other software blades such as firewall, IPS and Management.**

**B. The DLP Gateway running only the Firewall Software Blade**

**C. The DLP Gateway running only the Management Server on the same machine.**

**D. A Dedicated DLP Gateway running only the DLP Software Blade.**

When does the SmartWorkflow Policy Installation window appear?

**A. When the administrator installs an approved policy**

**B. When the administrator installs an unapproved policy**

**C. When the manager approves a session**

**D. When the administrator submits a session for approval**

Which of the following are supported with the office mode? Select all that apply.

**A. SSL Network Extender**

**B. SecureClient**

**C. L2TP**

**D. Transparent Mode**

**E. Gopher**

You plan to install a VPN-1 Pro Gateway for VPN-1 NGX at your company's headquarters.  
You have a single Sun SPARC Solaris 9 machine for VPN-1 Pro enterprise implementation.  
You need this machine to inspect traffic and keep configuration files.  
Which Check Point software package do you install?

**A. SmartCenter Server**

**B. Policy Server and primary SmartCenter Server**

**C. VPN-1 Pro Gateway**

**D. VPN-1 Pro Gateway and primary SmartCenter Server**

**E. ClusterXL and SmartCenter Server**

Which statement about LDAP and Active Directory (AD) with SSL VPN is TRUE?

**A. SSL VPN is capable of administering or creating users and groups directly on an LDAP server.**

**B. SSL VPN never stores the user records of LDAP/AD groups.**

**C. By default. SSL VPN sends username and password credentials to LDAP servers in UTF-8 encoding**

**D. SSL VPN does not support LDAP password remediation.**

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

**A. SmartLSM**

**B. Security Gateway**

**C. SmartCenter Server**

**D. VPN-1 Certificate Manager**

**E. Policy Server**

If a digital signature is used to achieve both data-integrity checking and verification of sender, digital signatures are only used when implementing:

**A. An asymmetric-encryption algorithm**

**B. Triple DES**

**C. A symmetric-encryption algorithm**

**D. CBL-DES**

Rachel is the Security Administrator for a university. The university's FTP servers have old hardware and software. Certain FTP commands cause the FTP servers to malfunction.  
Upgrading the FTP servers is not an option at this time.  
Which of the following options will allow Rachel to control which FTP commands pass through the Security Gateway protecting the FTP servers?

**A. FTP Service Object > Advanced > Blocked FTP Commands**

**B. Web Intelligence > Application Layer > FTP Settings**

**C. Rule Base > Action Field > Properties**

**D. Global Properties > Security Server > Allowed FTP Commands**

**E. SmartDefense > Application Intelligence > FTP Security Server**

The following rule contains an FTP resource object in the Service field:  
Source: local\_net  
Destination: Any  
Service: FTP-resource object  
Action: Accept  
How do you define the FTP Resource Properties > Match tab to prevent internal users from receiving corporate files from external FTP servers, while allowing users to send files?

**A. Enable the "Get" method on the Match tab.**

**B. Enable "Put" and "Get" methods.**

**C. Enable the "Put" method only on the Match tab.**

**D. Disable the "Put" method globally.**

**E. Disable "Get" and "Put" methods on the Match tab.**

Which Security Servers can perform Content Security tasks, but CANNOT perform authentication tasks?

**A. Telnet**

**B. FTP**

**C. HTTP**

**D. SMTP**

If SmartWorkflow is configured to work without Sessions or Role Segregation, how does the SmartDashboard function?

**A. The SmartDashboard functions as if SmartWorkflow is not enabled but an automatic session exists in the background and full SmartView tracker and audit trail functionality will be available.**

**B. The SmartDashboard will function without SmartWorkflow, with no session and no audit trail functionality.**

**C. The SmartDashboard will have no session but SmartView Tracker and audit trail will be available.**

In a distributed VPN-1 Pro NGX environment, where is the Internal Certificate Authority (ICA) installed?

**A. On the Security Gateway**

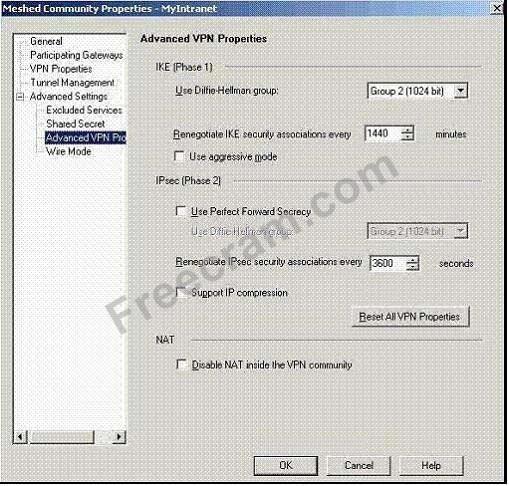
**B. On the Policy Server**

**C. Certificate Manager Server**

**D. On the primary SmartCenter Server**

**E. On the Smart View Monitor**

Stephanie wants to reduce the encryption overhead and improve performance for her mesh VPN Community. The Advanced VPN Properties screen below displays adjusted page settings:



What can Stephanie do to achieve her goal?

**A. Change the setting "Use Diffie. Hellman group" to "Group 5 (1536 bit)"**

**B. Check the box "Use Perfect Forward Secrecy"**

**C. Reduce the setting "Renegotiate IKE security associations every" to "720"**

**D. Check the box "Support IP compression"**

**E. Check the box "Use aggressive mode"**

The Management Portal allows all of the following EXCEPT:

**A. View the status of Check Point products**

**B. Manage firewall logs**

**C. Schedule policy installation**

**D. View administrator activity**

Which of the following can NOT be done on the Management Portal?

**A. Run the Management Portal on a port other than the default port 4433**

**B. Set the Management Portal to use HTTP instead of HTTPS**

**C. Configure Management Portal to bypass authentication when connecting from a specific IP address**

**D. Restrict hosts / networks that can access the portal**

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

**A. 1. Synchronize the two SmartCenter Servers.**

**2. Perform an advanced upgrade on the primary SmartCenter Server.**

**3. Configure the primary SmartCenter Server host object to version VPN-1 NGX.**

**4. Synchronize the two Servers again.**

**5. Upgrade the secondary SmartCenter Server.**

**6. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.**

**7. Synchronize the Servers again.**

**B. 1. Perform an advanced upgrade on the primary SmartCenter Server.**

**2. Configure the primary SmartCenter Server host object to version VPN-1 NGX.**

**3. Synchronize the primary with the secondary SmartCenter Server.**

**4. Upgrade the secondary SmartCenter Server.**

**5. Configure the secondary SmartCenter Server host object to version VPN-1 NGX.**

**6. Synchronize the Servers again.**

**C. 1. Synchronize the two SmartCenter Servers.**

**2. Upgrade the secondary SmartCenter Server.**

**3. Upgrade the primary SmartCenter Server.**

**4. Configure both SmartCenter Server host objects version to VPN-1 NGX.**

**5. Synchronize the Servers again.**

**D. 1. Synchronize the two SmartCenter Servers.**

**2. Perform an advanced upgrade on the primary SmartCenter Server.**

**3. Upgrade the secondary SmartCenter Server.**

**4. Configure both SmartCenter Server host objects to version VPN-1 NGX.**

**5. Synchronize the Servers again.**

What's true about Troubleshooting option in the IPS profile properties?

**A. Temporary changes the active protection profile to "Default\_Protection"**

**B. Temporary sets all protections to track (log) in SmartView Tracker**

**C. Temporary will disable IPS kernel engine**

**D. Temporary sets all active protections to detect**

Check Point recommends deploying SSL VPN:

**A. In parallel to the firewall**

**B. In a DMZ**

**C. On the Primary cluster member**

**D. In front of the firewall with a LAN connection**

Which operating system is NOT supported by VPN-1 Secure Client?

**A. IPSO 3.9**

**B. Windows 2000 Professional**

**C. RedHat Linux 8.0**

**D. MacOSX**

**E. Windows XP SP2**

You need to determine if your company's Web servers are accessed an excessive number of times from the same host. How would you configure this in the IPS tab?

**A. Successive DoS attacks**

**B. Successive alerts**

**C. HTTP protocol inspection**

**D. Successive multiple connections**

You are using SmartUpdate to fetch data and perform a remote upgrade of an NGX Security Gateway.  
Which of the following statements is FALSE?

**A. If SmartDashboard is open during package upload and upgrade, the upgrade will fail.**

**B. A remote installation can be performed without the SVN Foundation package installed on a remote NG with Application Intelligence Security Gateway**

**C. SmartUpdate can query the SmartCenter Server and VPN-1 Gateway for product information**

**D. SmartUpdate can query license information running locally on the VPN-1 Gateway**

Which of the following is an example of the hash function?

**A. SHA and 3DES**

**B. MD5 and SHA-1**

**C. DAC and MAC**

**D. DES and CBC**

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

**A. SCCP**

**B. MGCP**

**C. SIP**

**D. H.323**

**E. MEGACO**

Provisioning Profiles can NOT be applied to:

**A. IP Appliances**

**B. UTM-1 EDGE Appliances**

**C. Power-1 Appliances**

**D. UTM-1 Appliances**

You want to upgrade an NG with Application Intelligence R55 Security Gateway running on SecurePlatform to VPN-1 NGX R65 via SmartUpdate.  
Which package(s) is(are) needed in the Repository prior to upgrade?

**A. SecurePlatform NGX R65 package**

**B. SVN Foundation and VPN-1 Power/UTM packages**

**C. SecurePlatform and VPN-1 Power/UTM NGX R65 packages**

**D. VPN-1 Power/UTM NGX R65 package**

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

**A. Yes. IPS will limit the traffic impact from the scans, and identify if the pattern of the traffic matches any known worms.**

**B. No. The logs and alert can provide some level of information, but determining whether the attack is intentional or a worm, requires further research.**

**C. No. To verify if this is a worm or an active attack, you must also enable TCP attack defenses.**

**D. No. These IPS protections will only block the traffic, but it will not provide a detailed analysis of the traffic.**

What proprietary Check Point protocol is the basis of the functionality of Check Point ClusterXL inter- module communication?

**A. CKPP**

**IPSec**

**C. HA OPCODE**

**D. RDP**

**E. CCP**

Which of the following uses the same key to decrypt as it does to encrypt?

**A. static encryption**

**B. dynamic encryption**

**C. Certificate-based encryption**

**D. Symmetric encryption**

**E. Asymmetric encryption**

When two or more DLP rules are matched, the action taken is the most restrictive action.  
Rank the following items from the lowest restriction level (1) to the highest (4).  
1 . Ask User  
2 . Prevent  
3 . Detect  
4 . Inform User

**A. 4,3,1,2**

**B. 4,1,3,2**

**C. 3,4,1,2**

**D. 3,1,4,2**

You need to verify the effectiveness of your IPS configuration for your Web server farm.  
You have a colleague run penetration tests to confirm that the Web servers are secure against traffic hijacks.  
Of the following, which would be the best configuration to protect from a traffic hijack attempt?

**A. Configure TCP defenses such as Small PMTU size.**

**B. Enable the Web intelligence > SQL injection setting.**

**C. Activate the Cross-Site Scripting property.**

**D. Create resource objects for the Web farm servers and configure rules for the Web farm.**

SmartWorkflow has been enabled with the following configuration:  
If a security administrator opens a new session and after making changes to policy, submits the session for approval will be displayed as:

**A. Not Approved**

**B. Approved**

**C. Awaiting Approval**

**D. In progress**

Which protocol is not supported for DLP?

**A. smtp**

**B. ftp**

**C. https**

**D. http**

John is the MegaCorp Security Administrator, and is using Check Point R71. Malcolm is the Security Administrator of a partner company and is using a different vendor's product and both have to build a VPN tunnel between their companies. Both are using clusters with Load Sharing for their firewalls and John is using ClusterXL as a Check Point clustering solution.  
While trying to establish the VPN, they are constantly noticing problems and the tunnel is not stable and then Malcolm notices that there seems to be 2 SPIs with the same IP from the Check Point site. How can they solve this problem and stabilize the tunnel?

**A. This can be solved when using clusters; they have to use single firewalls.**

**B. This can be solved by running the command Sticky VPN on the Check Point CLI. This keeps the VPN Sticky to one member and the problem is resolved.**

**C. This is surely a problem in the ISPs network and not related to the VPN configuration.**

**D. This can easily be solved by using the Sticky decision function in ClusterXL.**

VPN-1 NGX includes a resource mechanism for working with the Common Internet File System (CIFS).  
However, this service only provides a limited level of actions for CIFS security.  
Which of the following services is NOT provided by a CIFS resource?

**A. Log mapped shares**

**B. Log access shares**

**C. Block Remote Registry Access**

**D. Allow MS print shares**

You have to uninstall the Check Point SmartWorkflow Software Blade on a Secure Platform system. How can you perform this procedure?

**A. To uninstall the SmartWorkflow Software Blade, you must first connect to your Security Management System on the command line level. Then in the directory /opt/CPuninstall/Check\_Point\_Workflow, run the command ./UnixInstallScript -u.**

**B. To uninstall the SmartWorkflow Software Blade you can connect to the Secure Platform Web UI ( <IP of the Security Management Server>) and select: Device > Upgrade. You will be asked if you want uninstall the SmartWorkflow Software Blade.**

**C. To uninstall the SmartWorkflow Software Blade you must first connect to your Security Management System on command line level. Then in the directory /opt/CPUninstall/Check\_Point\_Workflow, run the command ./UnixInstallScript -u. Afterwards, follow the screen instructions and change to the directory / opt/CPUninstall/R70\_HFA\_10 and repeat the previous command.**

**D. To uninstall the SmartWorkflow Software Blade, you use SmartUpdate. Click on the symbol of the Security Management Server, right-click, select Get Gateway Data, select SmartWorkflow, right -click uninstall SmartWorkflow. You will see the progress in the Opera rationStatus windows.**

What is the most typical type of configuration for VPNs with several externally managed Gateways?

**A. Hybrid community**

**B. star community**

**C. mesh community**

**D. SAT community**

**E. domain community**

Which of the following TCP port numbers is used to connect the VPN-1 Gateway to the Content Vector Protocol (CVP) server?

**A. 18180**

**B. 18182**

**C. 7242**

**D. 1456**

**E. 18181**

Your current VPN-1 NG with Application Intelligence (AI) R55 stand-alone VPN-1 Pro Gateway and SmartCenter Server runs on SecurePlatform.  
You plan to implement VPN-1 NGX R65 in a distributed environment, where the new machine will be the SmartCenter Server, and the existing machine will be the VPN-1 Pro Gateway only.  
You need to migrate the NG with AI R55 SmartCenter Server configuration, including licensing.  
How do you handle licensing for this NGX R65 upgrade?

**A. Request an NGX R65 SmartCenter Server license, using the new server's IP address. Request a new central NGX R65 VPN-1 Gateway license also licensed to the new SmartCenter Server's IP address.**

**B. Request an NGX R65 SmartCenter Server license, using the new server's IP address. Request a new central NGX R65 VPN-1 Gateway license for the existing gateway server's IP address.**

**C. Request an NGX R65 SmartCenter Server license, using the existing gateway machine's IP address.**

**Request a new local license for the NGX R65 VPN-1 Gateway using the new server's IP address.**

**D. Leave the current license on the gateway to be upgraded during the software upgrade. Purchase a new license for the VPN-1 NGX R65 SmartCenter Server.**

You are preparing to deploy a VPN-1 Pro Gateway for VPN-1 NGX.  
You have five systems to choose from for the new Gateway, and you must conform to the following requirements:  
Operating-system vendor's license agreement  
Check Point's license agreement  
Minimum operating-system hardware specification  
Minimum Gateway hardware specification  
Gateway installed on a supported operating system (OS)  
Which machine meets ALL of the following requirements?

**A. Processor: 1.67 GHz RAM: 128 MB Hard disk: 5 GB OS: FreeBSD**

**B. Processor: 1.5 GHz RAM: 256 MB Hard disk: 20 GB OS: Red Hat Linux 8.0**

**C. Processor: 1.1 GHz RAM: 512MB Hard disk: 10 GB OS: Windows 2000 Workstation**

**D. Processor: 2.0 GHz RAM: 512MB Hard disk: 10 GB OS: Windows ME**

**E. Processor: 2.2 GHz RAM: 256 MB Hard disk: 20 GB OS: Windows 2000 Server**

Your customer asks you about Check Point SmartWorkflow. His company must comply with various laws and regulations and therefore it is important for him to be able to see the changes made to a specific object.  
How can the customer receive the required information?

**A. The customer can use the Check Point's SmartViewTracker to view the required information. He selects the log category Changed Objects.**

**B. The customer can check compliance. This function compares the logs with the compliance requirements and automatically reports which part of the selected compliance is fulfilled and which is not.**

**C. The customer can use the Check Point's SmartView Tracker directly to receive the required information. He selects the log category SmartWorkflow.**

**D. The customer can use the Record Details. This feature enables administrators to track changes that have been made to objects over an extended period of time. These changes are recorded in SmartView Tracker as audit logs.**

What port is used for communication to the UserCenter with SmartUpdate?

**A. CPMI**

**B. TCP 8080**

**C. HTTP**

**D. HTTPS**

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 the patch utility is upgraded using this command**

**B. Only the OS**

**C. Only VPN-1 Pro Security Gateway**

**D. Both the operating system (OS) and all Check Point products**

**E. All products, except the Policy Server**

What tools CANNOT be launched from SmartUpdate NGX R65?

**A. cpinfo**

**B. Nokia Voyager**

**C. snapshot**

**D. SecurePlatform Web UI**

When using IPS, what does Geo protection do?

**A. To block traffic from and to a specific person**

**B. To block traffic from and to a specific company**

**C. To block traffic from and to a specific city**

**D. To block traffic from and to a specific country**

The We-Make-Widgets company has purchased twenty UTM-1 Edge appliances for their remote offices.  
Kim decides the best way to manage those appliances is to use SmartProvisioning and create a profile they can all use. List the order of steps Kim would go through to add the Dallas Edge appliance to the Remote Office profile using the output below.  
1 . Enter the name of the profile called "Remote Offices"  
2 . Change the provisioning profile to "Remote Offices"  
3 . Click File, then select New, then Provisioning Profile  
4 . Click on the Devices Tab  
5 . Highlight the Dallas Edge appliance, click Edit, then edit Gateway  
6 . Click on the Profiles Tab

**A. 6, 3, 1, 4, 5, 2**

**B. 4, 1, 3, 6, 5, 2**

**C. 6, 1, 3, 4, 5, 2**

**D. 4, 3, 1, 6, 5, 2**

Which of the following is NOT a supported browser for Management Portal?

**A. Mozilla**

**B. Firefox**

**C. Safari**

**D. Internet Explorer**

You are preparing to configure your VoIP Domain Gatekeeper object.  
Which two other objects should you have created first?

**A. An object to represent the PSTN phone network, AND an object to represent the IP phone network**

**B. An object to represent the call manager, AND an object to represent the host on which the transmission router is installed**

**C. An object to represent the IP phone network, AND an object to represent the host on which the proxy is installed**

**D. An object to represent the Q.931 service origination host, AND an object to represent the H.245 termination host**

**E. An object to represent the IP phone network, AND an object to represent the host on which the gatekeeper is installed**

You want to upgrade a SecurePlatform NG with Application Intelligence (Al) R55 Gateway to SecurePlatform NGX R60 via SmartUpdate.  
Which package is needed in the repository before upgrading?

**A. VPN-1 Pro/Express NGXR60**

**B. VPN-1 and Firewall-1**

**C. SecurePlatform NGX R60**

**D. SVN Foundation and VPN-1 Express/Pro**

**E. SVN Foundation 3**

Your network traffic requires preferential treatment by other routers on the network, in addition to the QoS Module, which Check Point QoS feature should you use?

**A. Weighted Fair Queuing**

**B. Low Latency Queuing**

**C. Limits**

**D. Guarantees**

**E. Differentiated Services**

What could the following regular expression be used for in a DLP rule?  
\$([0-9]\*,[0-9] [0-9] [0-9]. [0-9] [0-9]  
Select the best answer.

**A. As a Data Type to prevent programmers from leaking code outside the company**

**B. As a Data Type to prevent the Finance Department from leaking salary information to employees**

**C. As a compound data type representation.**

**D. As a Data Type to prevent employees from sending an email that contains a complete price-list of nine products.**

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

**A. The standard six-packet IKE Phase 2 exchange is replaced by a three-packet exchange.**

**B. The standard six-packet IKE Phase 1 exchange is replaced by a twelve-packet exchange.**

**C. The standard three-packet IKE Phase 2 exchange is replaced by a six-packet exchange.**

**D. The standard three-packet IKE Phase 1 exchange is replaced by a six-packet exchange.**

**E. The standard six-packet IKE Phase 1 exchange is replaced by a three-packet exchange.**

Which Name Resolution protocols are supported in SSL VPN?

**A. DNS, hosts**

**B. DNS, hosts, WINS**

**C. DNS, hosts, Imhosts**

**D. DNS, hosts, Imhosts, WINS**

You start the configuration of SmartWorkflow. SmartWorkflow is enabled, but you are not able to select Open New Session because it is greyed out.  
What must be done to open a new session? Choose the BEST answer.

**A. A rule which allows the SmartWorkflow traffic must be placed on the top of the Rule Base.**

**B. The Work with sessions in Global Properties must be set.**

**C. The use of sessions must be enabled by the CLI command: SWF\_session start.**

**D. Sessions in the Manage menu of SmartDashboard must be selected and enabled.**

Consider the following actions that VPN-1 NGX can take when it control packets. The Policy Package has been configured for Traditional Mode VPN.  
Identify the options that includes the available actions. Select four.

**A. Drop**

**B. Encrypt**

**C. Client auth**

**D. Decrypt**

**E. Reject**

**F. Allow**

**G. Hold**

**H. Proxy**

**I. Accept**

How should Check Point packages be uninstalled?

**A. In any order, CP suite must be the last package uninstalled**

**B. In the opposite order in which the installation wrapper initially installed them.**

**C. In the same order in which the installation wrapper initially installed from.**

**D. In any order as long as all packages are removed**

Barak is a Security Administrator for an organization that has two sites using pershared 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 pershared 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 "PreShared 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 Security Gateways.

**A. 1, 2, 3, 5**

**B. 1, 2, 4, 5**

**C. 1, 2, 3, 4**

**D. 1, 3, 4, 5**

**E. 1, 2, 5**

Which service type does NOT invoke a Security Server?

**A. FTP**

**B. SMTP**

**C. Telnet**

**D. CIFS**

**E. HTTP**

What is the best method for scheduling backup's on multiple firewalls?

**A. SmartUpdate**

**B. Smart Dashboard**

**C. WebUI**

**D. SmartProvisioning**

What type of packet does a VPN-1 SecureClient send to its Policy Server, to report its Secure Configuration Verification status?

**A. TCP keep alive**

**B. ICMP Port Unreachable**

**C. UDP keep alive**

**D. ICMP Destination Unreachable**

**E. IKE Key Exchange**

Which application is used to create a File-Share Application?

**A. SSL VPN Portal WebUI (File-Share Tab)**

**B. SmartPortal WebUI (File-Share Tab)**

**C. SmartDashboard (SSL VPN Tab)**

**D. Provider-1 MDG (Global VPNs Tab)**

Public-key cryptography is considered which of the following?

**A. one-key/symmetric**

**B. one-key/asymmetric**

**C. two-key/symmetric**

**D. two-key/asymmetric**

The relay mail server configured under Email Notifications is used by the DLP Gateway to: (Choose the BEST answer.)

**A. If User Check is configured, there is no need to configure this relay server if there are no Ask User rules and there is no need to notify any Data Owners.**

**B. Send e-mail notifications to users and Data Owners.**

**C. Synchronize with other mail servers in the network.**

**D. Define My Organization / DLP Gateway and scan only e-mails that originate from this relay server.**

Where can a Security Administrator adjust the unit of measurement (bps, Kbps or Bps), for Check Point QoS bandwidth?

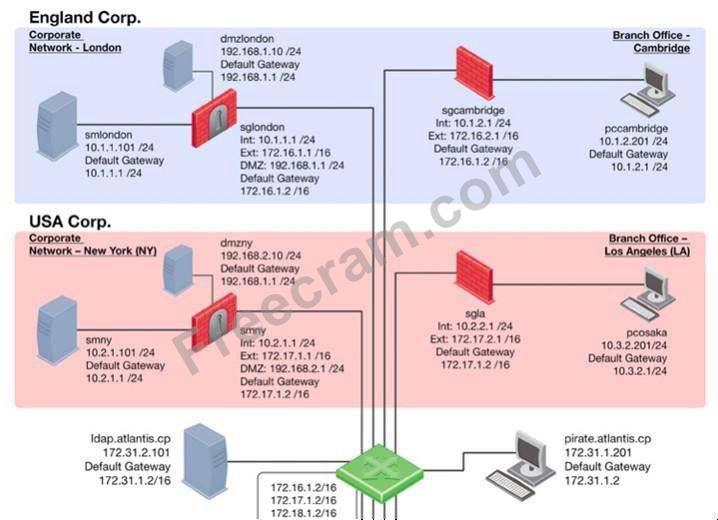
**A. Global Properties**

**B. QoS Class objects**

**C. Check Point gateway object properties**

**D. $CPDIR/conf/qos\_props.pf**

Refer to the to the network topology below.



You have IPS software Blades active on security Gateways sglondon, sgla, and sgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?

**A. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-tuned anomaly algorithms. Even if this is accomplished, no technology can offer 100% protection.**

**B. Since other Gateways do not have IPS activated, attacks may originate from their networks without any noticing.**

**C. The attacker may have used a bunch of evasion techniques like using escape sequences instead of clear text commands. It is also possible that there are entry points not shown in the network layout, like rouge access points.**

**D. All of these options are possible.**

When selecting a backup target using SmartProvisioning, which target is NOT available?

**A. TFTP**

**B. FTP**

**C. Locally on device**

**D. SCP**