Check Point Certified Security Expert

1. 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 is surely a problem in the ISPs network and not related to the VPN configuration.

B. This can easily be solved by using the Sticky decision function in ClusterXL.

C. This can be solved when using clusters; they have to use single firewalls.

D. 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.

Answer(s): B

---

2. What is the most typical type of configuration for VPNs with several externally managed Gateways?

A. mesh community

B. Hybrid community

C. SAT community

D. domain community

E. star community

Answer(s): E

---

3. VPN access control would fall under which VPN component?

A. Performance

B. Security

C. Management

D. QoS

Answer(s): B

---

4. 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. snapshot

B. backup

C. migrate export

D. eva_db_backup

Answer(s): D

---

5. What is a "sticky" connection?

A. A Sticky Connection is a VPN connection that remains up until you manually bring it down.

B. A Sticky Connection is a connection that always chooses the same gateway to set up the initial connection.

C. A Sticky Connection is one in which a reply packet returns through the same gateway as the original packet.

D. A Sticky Connection is a connection that remains the same.

Answer(s): C

---

6. Your current VPN-1 NG with Application Intelligence (AI) R55 stand alone 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 AI R55 SmartCenter Server configuration, including such items as Internal Certificate Authority files, databases, and Security Policies.

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

C. 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.

D. 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.

Answer(s): B

---

7. 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. upgrade_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.

D. Used when upgrading the Security Gateway, upgrade_export includes modified files, such as in the directories /lib and /conf.

Answer(s): B

---

8. In R71, how would you define a rule to block all traffic sent to or from Germany?

A. Create a country specific policy within IPS Geo Protections with Germany as the country, block as the action, and from and to country for direction.

B. Create a policy rule with destination being a custom dynamic object representing Germany and action block. You must also create a rule in the opposite direction.

C. Go to Policy / Global Properties / Geographical Protection Enforcement and add Germany to the blocked countries list.

D. This action is not possible.

Answer(s): A

---

9. Which Security Servers can perform Content Security tasks, but CANNOT perform authentication tasks?

A. FTP

B. HTTP

C. Telnet

D. SMTP

Answer(s): D

---

10. How is Smart Workflow disabled?

A. In SmartView Tracker, click on SmartWorkflow > Disable Smart Workflow

B. In cpconfig, choose Disable Smart Workflow from the menu

C. In SmartDashboard, click on View > Smart Workflow > Disable Smart Workflow

D. Open Smart Workflow as admin. Create new session and name it Disable Smart Workflow. In SmartDashboard click Smart Workflow > Disable Smart Workflow, click OK in the warning box, click

Save and Continue

Answer(s): D

---

11. With is the SmartEvent Correlation Unit's function?

A. Display received threats and tune the Events Policy

B. Invoke and define automatic reactions and add events to the database.

C. Analyze log entries, looking for Event Policy patterns.

D. Assign severity levels to events.

Answer(s): C

---

12. 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.

A. 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).

B. 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.

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

Answer(s): B

---

13. The SmartEvent Correlation Unit:

A. displays the received events.

B. assigns a severity level to an event.

C. adds events to the events database.

D. forwards what is identified as an event to the SmartEvent server.

Answer(s): D

---

14. 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 perform filtering, based on IP address and SMTP protocols.

B. Configure the SMTP Security Server to perform MX resolving.

C. Configure the SMTP Security Server to allow only mail to or from names, within Cody's corporate domain.

D. Configure the SMTP Security Server to work with an OPSEC based product, for content checking.

E. Configure the SMTP Security Server to apply a generic "from" address to all outgoing mail.

Answer(s): C

---

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

D. All cluster members process all packets and members synchronize with each other.

Answer(s): B

---

16. 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/sip and sip_any/accept

C. Net_A/Net_B/VolP_any/accept

D. Net_A/Net_B/sip/accept

Answer(s): D

---

17. Which command can be used to verify SecureXL statistics?

A. fw ctl pstat

B. fwaccel stats

C. cphaprob stat

D. fwaccel top

Answer(s): B

---

18. SmartProvisioning is an integral part of the Security Management or Provider-1 CMA. To enable SmartProvisioning on the Security Management server:

A. Obtain a SmartProvisioning license, add the License to the Security Management server or CMA, turn on SmartProvisioning on each Gateway to be controlled.

B. Obtain a SmartProvisioning license, add the License to the Security Management server or CMA, disable SecureXL.

C. Obtain a SmartProvisioning license, add the License to the Security Management server or CMA, select the box under Policy for SmartProvisioning.

D. Obtain a SmartProvisioning license, add the License to the Security Management server or CMA.

Answer(s): D

---

19. What SmartConsole application allows you to change the Log Consolidation Policy?

A. SmartDashboard

B. SmartUpdate

C. SmartEvent Server

D. SmartReporter

Answer(s): D

---

20. 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 installed VoIP gateways specify host objects.

B. VoIP Domain SIP objects cannot be placed in simple groups.

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

D. The related end points domain specifies an address range.

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

Answer(s): B