Checkpoint

Exam 156-215.70

Check Point Certified Security Administrator R70

Version: 10.1

[Total Questions: 546]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	152
Topic 3: Volume C	100
Topic 4: Volume D	99
Topic 5: Volume E	95

Topic 1, Volume A

Question No : 1 - (Topic 1)

Your organization has many Edge Gateways at various branch offices allowing users to access company resources. For security reasons, your organization's Security Policy requires all Internet traffic initiated behind the Edge Gateways first be inspected by your headquarters' R70 Security Gateway. How do you configure VPN routing in this star VPN Community?

A. To Internet and other targets only
B. To center or through the center to other satellites, to Internet and other VPN targets
C. To center and other satellites, through center
D. To center only

Answer: B

Question No : 2 - (Topic 1)

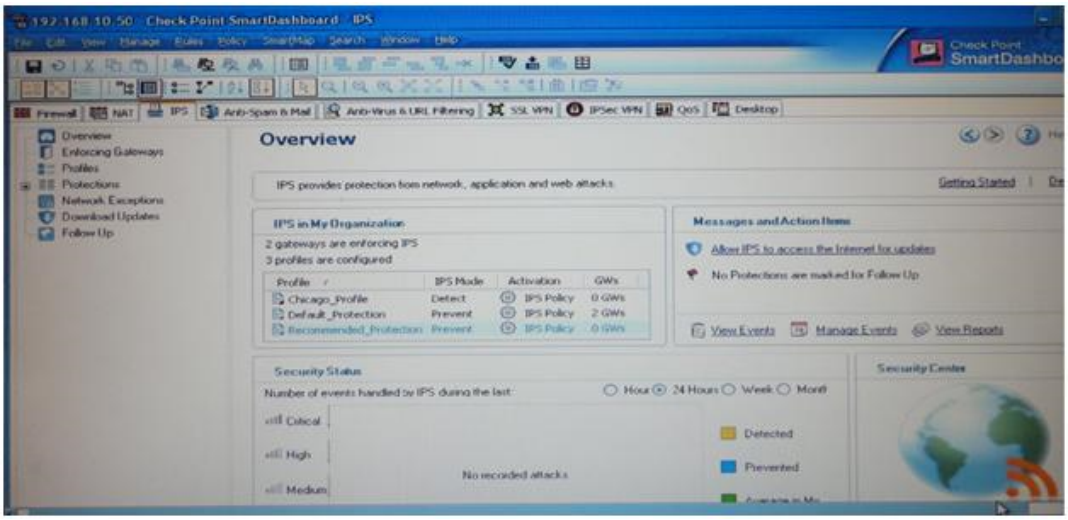
Which of the following are available SmartConsole clients which can be installed from the R70 Windows CD? Read all answers and select the most complete and valid list.

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

Answer: B

Question No : 3 - (Topic 1)

The TotallyCoolSecurity Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-chicago using Detect mode. After reviewing logs, Matt noticed that fw-chicago is not detecting any of the IPS protections that Bob had previously setup. Analyze the output below and determine how can correct the problem.



A. Matt should re-create the Chicago_Profile and select Activate protections manually Instead of per the IPS Policy
B. Matt should activate the Chicago_Profile as it is currently not activated
C. Matt should assign the fw-chicago Security Gateway to the Chicago_Profile
D. Matt should change the Chicago_Profile to use Protect mode because Detect mode will not work.

Answer: C

Question No : 4 - (Topic 1)

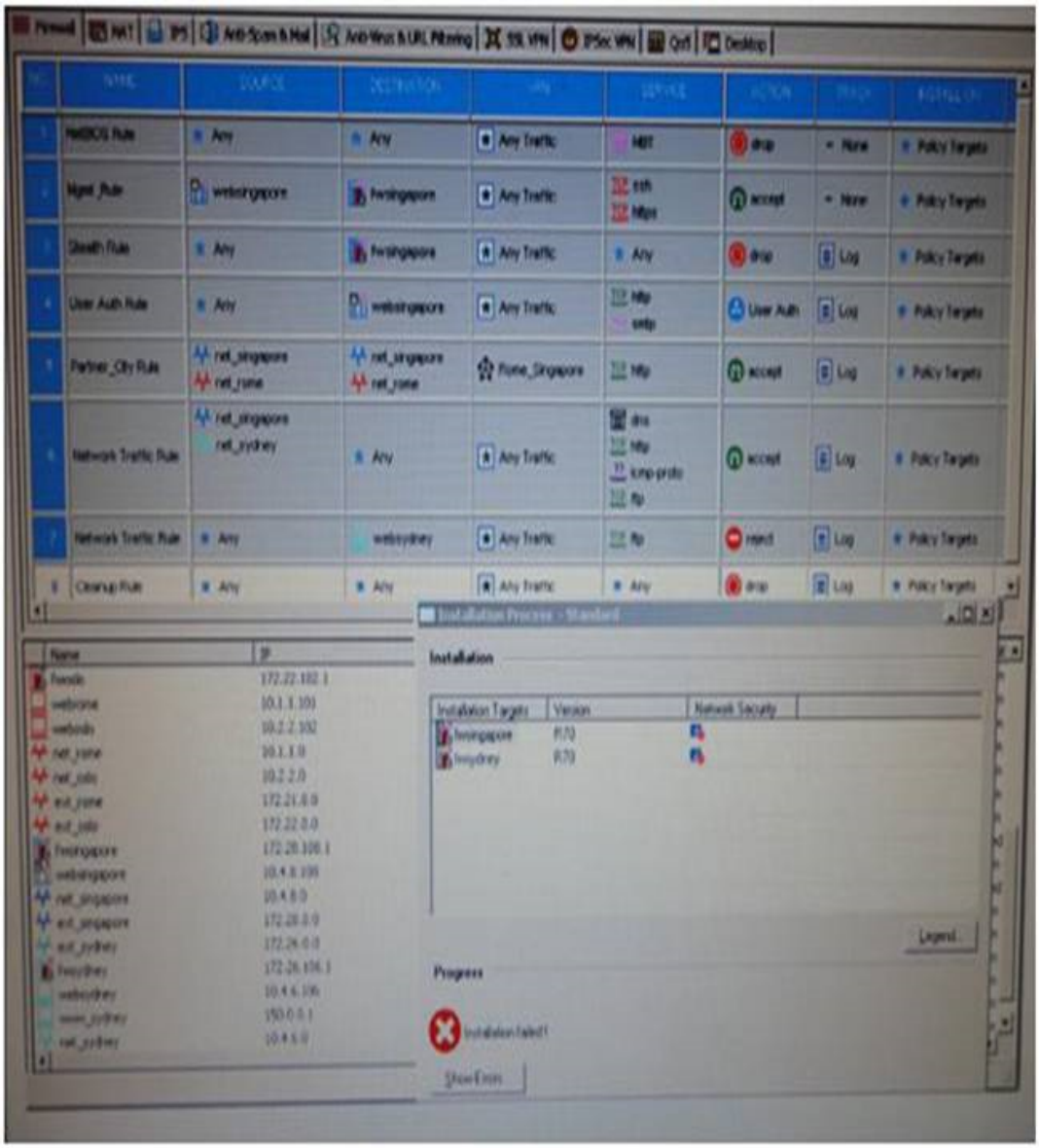
Certificates for Security Gateways are created during a simple initialization from_____.

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

Answer: D

Question No : 5 - (Topic 1)

Which rule is responsible for the installation failure?



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

Answer: B

Question No : 6 - (Topic 1)

Which of the following is true regarding configuration of clustering nodes?

A. Cluster nodes do not have to run exactly the same version of CheckPoint package

B. Each node must have exactly the same set of packages as all the other nodes
C. Each cluster node must run exactly the same version of R70
D. You must enable state synchronization
E. You must install R70 as an enforcement module (only) on each node

Answer: B,C,D,E

Question No : 7 - (Topic 1)

Your company has two headquarters, one in London, and one in New York Each office includes several branch offices. The branch offices need to rate with the headquarters in their country, not with each other, and only the headquarters need to communicate directly. What is the BEST configuration for establishing VPN Communities for this company? VPN Communities comprised of:

A. Two star and one mesh Community: One star Community is set up for each site, with headquarters as the center of the Community and its branches as satellites The mesh Community includes only New York and London Gateways.
B. One star Community with the option to "mesh" the center of the star: New York and London Gateways added to the center of the star with the mesh canter Gateways option checked, all London branch offices defined m one satellite window, but all New York branch offices defined m another satellite window.
C. Two mesh and one star Community One mesh Community is set up for each of the headquarters and its branch offices The star Community is configured with London as the center of the Community and New York is the satellite.
D. Three mesh Communities: One for London headquarters and its branches, one for New York headquarters and its branches, and one for London and New York headquarters.

Answer: A

Question No : 8 - (Topic 1)

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

A. Highlight the suspicious connection in SmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection is listed in this SmartView Tracker view as "dropped".
B. Highlight the suspicious connection in SmartView Tracker > Active mode. Block it using Tools > Block Intruder menu. Observe in the Active mode that the suspicious connection

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

Answer: B

Question No : 9 - (Topic 1)

What is the desired outcome when running the command cpinfo -z -o cpinfo.out?

A. Send output to a file called cpinfo. out in compressed format.
B. Send output to a file called cpinfo. out in usable format for the CP InfoView utility.
C. Send output to a file called cpinfo. out without address resolution.
D. Send output to a file called cpinfo. out and provide a screen print at the same time.

Answer: A

Question No : 10 - (Topic 1)

R70's INSPECT Engine inserts itself into the kernel between which tow layers of the OSl model?

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

Answer: D

Question No : 11 - (Topic 1)

In a distributed management environment, the administrator has removed the default check from Accept Control Connections under the Policy > Global Properties > FireWall tab. In order for the Security Management Server to install a policy to the Firewall, an explicit rule

must be created to allow the server to communicate to the Security Gateway on port_____.

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

Answer: A

Question No : 12 - (Topic 1)

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

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

Answer: D

Question No : 13 - (Topic 1)

An Administrator without access to SmartDashboard installed a new IPSO-based R70 Security Gateway over the weekend. He e-mailed you the SIC activation key. You want to confirm communication between the Security Gateway and the Management Server by installing the Policy. What might prevent you from installing the Policy?

A. You first need to create a new UTM-1 Gateway object, establish SIC via the Communication button, and define the Gateway's topology.
B. You have not established Secure Internal Communications (SIC) between the Security Gateway and Management Server You must initialize SIC on the Security Management Server.
C. An intermediate local Security Gateway does not allow a policy install through it to the remote new Security Gateway appliance Resolve by running the tw unloadlocal command on the local Security Gateway.
D. You first need to run the fw unloadlocal command on the R70 Security Gateway

appliance in order to remove the restrictive default policy.

Answer: B

Question No : 14 - (Topic 1)

Which opponent functions as the Internet Certificate Authority for R70?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: B

Question No : 15 - (Topic 1)

What CANNOT be configured for existing connections during a policy install?

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

Answer: C

Question No : 16 - (Topic 1)

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

A. Log sites from blocked categories.
B. Redirect users to a new URL.
C. Block sites only once.
D. Alert the Administrator to block a suspicious site

Answer: A

Question No : 17 - (Topic 1)

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

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

Answer: C

Question No : 18 - (Topic 1)

Which of the following SSL Network Extender server-side prerequisites is NOT correct?

A. The Gateway must be configured to work with Visitor Mode.
B. There are distinctly separate access rules required for SecureClient users vs. SSL Network Extender users.
C. To use Integrity Clientless Security (ICS), you must install the IC3 server or configuration tool.
D. The specific Security Gateway must be configured as a member of the Remote Access Community

Answer: B

Question No : 19 - (Topic 1)

In previous version, the full TCP three-way handshake was sent to the firewall kernel for inspection. How is this improved in current Flows/SecureXL?

A. Only the initial SYN packet is inspected The rest are handled by IPSO
B. Packets are offloaded to a third-party hardware card for near-line inspection
C. Packets are virtualized to a RAM drive-based FW VM
D. Resources are proactively assigned using predictive algorithmic techniques

Answer: A