

Checkpoint

Exam 156-210

Check Point NG with Application Intelligence - Management I

Version: 3.2

[Total Questions: 241]

Question No : 1

Once you have installed Secure Internal Communications (SIC) for a host-node object and issued a certificate for it. Which of the following can you perform? Choose two.

- A. Rename the object
- B. Rename the certificate
- C. Edit the object properties
- D. Rest SIC
- E. Edit the object type

Answer: A,C

Explanation: Explanation: Object can be renamed and the properties can be edited even after establishing the SIC and issue the certificate

Question No : 2

You are a Security Administrator preparing to implement Hide NAT. You must justify your decision. Which of the following statements justifies implementing a Hide NAT solution? Choose two.

- A. You have more internal hosts than public IP addresses
- B. Your organization requires internal hosts, with RFC 1918-compliant addresses to be assessable from the Internet.
- C. Internally, your organization uses an RFC 1918-compliant addressing scheme.
- D. Your organization does not allow internal hosts to access Internet resources
- E. Internally, you have more public IP addresses than hosts.

Answer: A,C

Question No : 3

Which critical files and directories need to be backed up? Choose three

- A. \$FWDIR/conf directory
- B. rulebase_5_0.fws
- C. objects_5_0.c
- D. \$CPDIR/temp directory
- E. \$FWDIR/state directory

Answer: A,B,C

Question No : 4

Which of the following statements about the General HTTP Worm Catches is FALSE?

- A. The General HTTP Worm Catcher can detect only worms that are part of a URI.
- B. Security Administrators can configure the type of notification that will take place, if a worm is detected.
- C. SmartDefense allows you to configure worm signatures, using regular expressions.
- D. The General HTTP Worm Catcher's detection takes place in the kernel, and does not require a Security Server.
- E. Worm patterns cannot be imported from a file at this time.

Answer: A

Question No : 5

You are a Security Administrator attempting to license a distributed VPN-1/Firewall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which of the following must be considered when licensing the deployment? Choose two.

- A. Local licenses are IP specific.
- B. A license can be installed and removed on a VPN-1/Firewall-1 version 4.1, using SmartUpdate.
- C. You must contact Check Point via E-mail or telephone to create a license for an Enforcement Module.
- D. Licenses cannot be installed through SmartUpdate.
- E. Licenses are obtained through the Check Point User Center

Answer: A,E

Question No : 6

Which of the following are tasks performed by a VPN-1/FireWall-1 SmartCenter Server? Choose three.

- A. Examines all communications according to the Enterprise Security Policy.
- B. Stores VPN-1/FirWall-1 logs.
- C. Manages the User Database.
- D. Replicates state tables for high availability.
- E. Compiles the Rule Base into an enforceable Security Policy.

Answer: B,C,E

Question No : 7

You are a Security Administrator preparing to implement an address translation solution for Certpaper.com.

The solution you choose must meet the following requirements:

- ✍ RFC 1918-compliant internal addresses must be translated to public, external addresses when packets exit the Enforcement Module.
- ✍ Public, external addresses must be translated to internal, RFC 1918-compliant addresses when packets enter the Enforcement Module.

Which address translation solution BEST meets your requirements?

- A. Hide NAT
- B. The requirements cannot be met with any address translation solution.
- C. Dynamic NAT
- D. IP Pool Nat
- E. Static NAT

Answer: E

Question No : 8

Which of the following suggestions regarding Security Policies will NOT improve performance?

- A. If most incoming connections are HTTP, but the rule that accepts HTTP at the bottom of the Rule Base, before the Cleanup Rule
- B. Use a network object, instead of multiple host-node objects.
- C. Do not log unnecessary connections.
- D. Keep the Rule Base simple.
- E. Use IP address-range objects in rules, instead of a set of host-node objects.

Answer: A

Question No : 9

You are a Security Administrator attempting to license a distributed VPN-1/Firwall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which license type is the BEST for your deployment?

- A. Discretionary
- B. Remote
- C. Central
- D. Local
- E. Mandatory

Answer: C

Question No : 10

Network attacks attempt to exploit vulnerabilities in network applications, rather than targeting firewalls directly.

What does this require of today's firewalls?

Checkpoint 156-210 : Practice Test

- A. Firewalls should provide network-level protection, by inspecting packets all layers of the OSI model.
- B. Firewall should not inspect traffic below the Application Layer of the OSI model, because such inspection is no longer relevant.
- C. Firewalls should understand application behavior, to protect against application attacks and hazards.
- D. Firewalls should provide separate proxy processes for each application accessed through the firewall.
- E. Firewalls should be installed on all Web servers, behind organizations' intranet.

Answer: C

Question No : 11

What function does the Audit mode of SmartView Tracker perform?

- A. It tracks detailed information about packets traversing the Enforcement Modules.
- B. It maintains a detailed log of problems with VPN-1/FireWall-1 services on the SmartCenter Server.
- C. It is used to maintain a record of the status of each Enforcement Module and SmartCenter server.
- D. It maintains a detailed record of status of each Enforcement Module and SmartCenter Server.
- E. It tracks changes and Security Policy installations, per Security Administrator, performed in SmartDashboard.

Answer: E

Question No : 12

In the SmartView Tracker, what is the difference between the FireWall-1 and VPN-1 queries? Choose three.

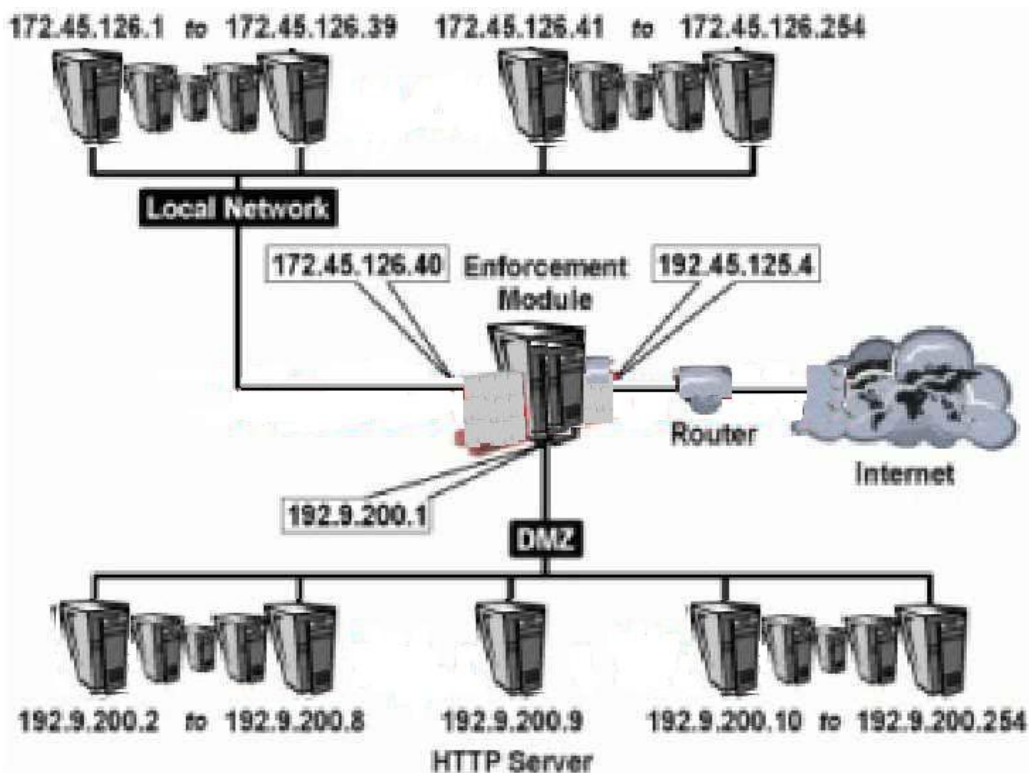
- A. A VPV-1 query only displays encrypted and decrypted traffic.
- B. A FireWall-1 query displays all traffic matched by rules, which have logging activated.
- C. A FireWall-1 query displays all traffic matched by all rules.
- D. A FireWall-1 query also displays encryption and decryption information.

E. Implied rules, when logged, are viewed using the VPN-1 query.

Answer: A,B,D

Question No : 13

Network topology exhibit



You want hide all localnet and DMZ hosts behind the Enforcement Module, except for the HTTP Server (192.9.200.9). The HTTP Server will be providing public services, and must be accessible from the Internet.

Select the two BEST Network Address Translation (NAT) solutions for this scenario,

- A. To hide Local Network addresses, set the address translation for 192.9.0.0
- B. To hide Local Network addresses, set the address translation for 192.9.200.0
- C. Use automatic NAT rule creation to hide both DMZ and Local Network.
- D. To hide Local Network addresses, set the address translation for privatenet.
- E. Use automatic NAT rule creation, to statically translate the HTTP Server address.

Answer: C,E

Question No : 14

The SmartDefense Storm Center Module agent receives the Dshield.org Block List, and:

- A. Populates CPDShield with blocked address ranges, every three hours.
- B. Generates logs from rules tracking internal traffic.
- C. Submits the number of authentication failures, and drops, rejects, and accepts.
- D. Generates regular and compact log digest.
- E. Populates the firewall daemon with log trails.

Answer: A

Question No : 15

What are the advantages of central licensing? Choose three.

- A. Only the IP address of a SmartCenter Server is needed for all licences.
- B. A central licence can be removed from one Enforcement Module, and installed on another Enforcement Module.
- C. Only the IP address of an Enforcement Module is needed for all licences.
- D. A central license remains valid, when you change the IP address of an Enforcement Module.
- E. A central license can be converted into a local license.

Answer: A,B,D

Question No : 16

A security Administrator wants to review the number of packets accepted by each of the Enforcement modules. Which of the following viewers is the BEST source for viewing this information?

- A. SmartDashboard
- B. SmartUpdate

- C. SmartMap
- D. SmartView Status
- E. SmartView Tracker

Answer: D

Question No : 17

Hidden (or masked) rules are used to:

- A. Hide rules from administrators with lower privileges.
- B. View only a few rules, without distraction of others.
- C. Temporarily disable rules, without having to reinstall the Security Policy.
- D. Temporarily convert specifically defined rules to implied rules.
- E. Delete rules, without having to reinstall the Security Policy.

Answer: B

Question No : 18

Which of the following characteristics BEST describes the behaviour of Check Point NG with Application Intelligence?

- A. Traffic not expressly permitted is prohibited.
- B. All traffic is expressly permitted by explicit rules.
- C. Secure connections are authorized by default. Unsecured connections are not.
- D. Traffic is filtered using controlled ports.
- E. TELNET, HTTP; and SMTP are allowed by default.

Answer: A

Question No : 19

SmartUpdate CANNOT be used to:

Checkpoint 156-210 : Practice Test

- A. Track installed versions of Check Point and OPSEC products.
- B. Manage licenses centrally.
- C. Update installed Check Point and OPSEC software remotely, from a centralized location.
- D. Uninstall Check Point and OPSEC software remotely, from a centralized location.
- E. Remotely install NG with Application Intelligence for the first time, on a new machine.

Answer: E

Question No : 20

Which of the following statements about Client Authentication is FALSE?

- A. In contrast to User Authentication that allows access per user. Client Authentication allows access per IP address.
- B. Client Authentication is more secure than User Authentication, because it allows multiple users and connections from an authorized IP address or host.
- C. Client Authentication enables Security Administrators to grant access privileges to a specific IP address, after successful authentication.
- D. Authentication is by user name and password, but it is the host machine (client) that is granted access.
- E. Client Authentication is not restricted to a limited set of protocols.

Answer: B

Question No : 21

Why is Application Layer particularly vulnerable to attacks? Choose three

- A. Malicious Java, ActiveX, and VB Scripts can exploit host system simply by browsing.
- B. The application Layer performs access-control and legitimate-use checks.
- C. Defending against attacks at the Application Layer is more difficult, than at lower layers of the OSI model.
- D. The Application Layer does not perform unauthorized operations.
- E. The application Layer supports many protocols.

Answer: A,C,E