Exam   :   **156-210**

Title   :   Check Point CCSA NG

Version   :   Demo

1.Once you have installed Secure Internal Communcations (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

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

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

4.Which of the following statements about the General HTTP Worm Catcher 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

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

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

7.You are a Security Administrator preparing to implement an address translation solution for Certkiller .com.
The solution you choose must meet the following requirements:

1. RFC 1918-compliant internal addresses must be translated to public, external addresses when packets exit the Enforcement Module.
2. 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

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

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 deployemenet?

A. Discretionary

B. Remote

C.   Central

D. Local

E. Mandatory

Answer: C

10.Network attacks attempt to exploit vulnerabilities in network applications, rather

than targeting firewalls directly.

What does this require of today's firewalls?

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

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.

Instant Download   PDF And VCE   100% Passing Guarantee   100% Money Back Guarantee

----

Answer: E

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

A. A VPN-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

13.Network   topology   exhibit
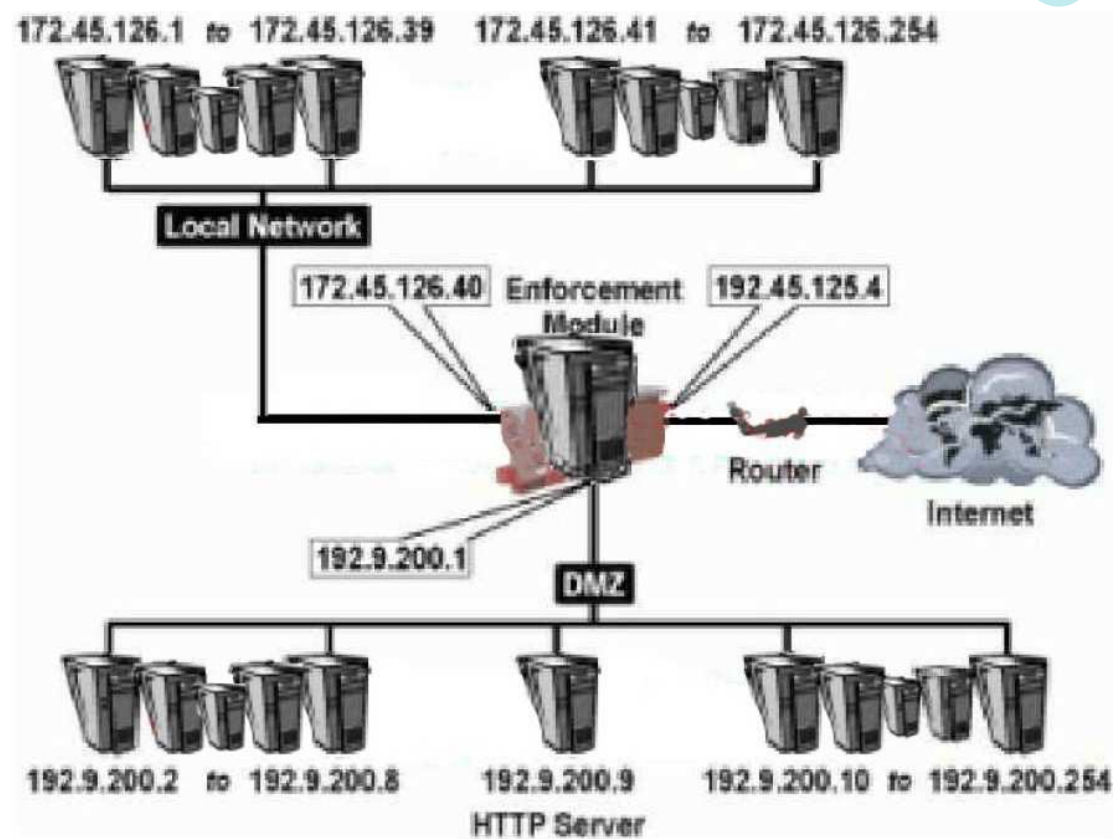
You want hide all localnet and DMZ hosts behind the Enforcemenet Module, except
for the HTTP Server (192.9.200.9). The HTTP Server will be providing public
services, and must be accessible from the Internet.
Select the two BEST Network Address Translation (NAT) solutions for this
scenario,

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

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

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 installe don 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 Enforcemente Module.

E. A central license can be converted into a local license.

Answer: A, B, D

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

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

Instant Download   PDF And VCE   100% Passing Guarantee   100% Money Back Guarantee

----

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 connectdions are not.
D. Traffic is filtered using controlled ports.
E. TELNET, HTTP; and SMTP are allowed by default.
Answer: A

19.SmartUpdate CANNOT be used to:

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

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

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

22.You have created a rule that requires users to be authenticated, when connecting to the Internet using HTTP. Which is the BEST authentication method for users who must use specific computers for Internet access?

A. Client
B. Session
C. User
Answer: A

23.What function does the Active mode of SmartView Tracker perform?

A. It displays the active Security Policy.
B. It displays active Security Administrators currently logged into a SmartCenter Server.
C. It displays current active connections traversing Enforcement Modules.
D. It displays the current log file, as it is stored on a SmartCenter Server.
E. It displays only current connections between VPN-1/FireWall-1 modules.
Answer: C

24.You are importing product data from modules, during a VPN-1/Firwall-1 Enforcement Module upgrade. Which of the following statements are true? Choose two.

A. Upgrading a single Enforcement Module is recommended by Check Point, since there is no chance of mismatch between installed product versions.
B. SmartUpdate queries license information, from the SmartConsole runging locally on the Enforcement Module.
C. SmartUpdate queries the SmartCenter Server and Enforcement Module for product information.
D. If SmartDashboard and all SmartConsoles must be open during input, otherwise the product-data retrieval process will fail
Answer: A, C

25.Which if the following components functions as the Internal Certificate Authority for all modules in the VPN-1/FireWall-1 configuration?

A. Enforcement Module
B. INSPECT Engine
C. SmartCenter Server
D. SmartConsole
E. Policy Server
Answer: C

26.Which of the following is NOT a security benefit of Check Point's Secure Internal Communications (SIC)?

A. Generates VPN certificates for IKE clients.

B. Allows the Security Administrator to confirm that the Security Policy on an Enforcement Module came from an authorized Management Server.

C. Confirms that a SmartConsole is authorized to connect a SmartCenter Server

D. Uses SSL for data encryption.

E. Maintains data privacy and integrity.

Answer: A

27.You are administering one SmartCenter Server that manages three Enforcement Modules. One of the Enforcement Modules does not appear as a target in the Install Policy screen, when you attempt to install the Security Policy. What is causing this to happen?

A. The license for the Enforcement Module has expired.

B. The Enforcement Module requires a reboot.

C. The object representing the Enforcement Module was created as a Node->Gateway.

D. The Enforcement Module was not listed in the Install On column of its rule.

E. No Enforcement Module Master filer was created, designating the SmartCenter Server

Answer: C

28.You are the Security Administrator with one SmartCenter Server managing one Enforcement Moduel. SmartView Status displayes a computer icon with an "I" in the Status column. What does this mean?

A. You have entered the wrong password at SmartView Status login.

B. Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module.

C. The SmartCenter Server cannot contact a gateway.

D. The VPN-1/Firewall-1 Enforcement Module has been compromised and is no longer controlled by this SmartCenter Sever.

E. The Enforcement Module is installed and responding to status checks, but the status is problematic.

Answer: E

29.Check Point's NG with Application Intelligence protects against Network and Transport layer attacks by: (Choose two)

A. Preventing protocol-anomaly detection-

B. Allowing IP fragmentation-

C. Preventing validation of compliance to standards.

D. Preventing non-TCP denial-of-service attacks, and port scanning.

E. Preventing malicious manipulation of Network Layer protocols.

Answer: D, E

30.Which of the following locations is Static NAT processed by the Enforcement Module on packets from an external source to an internal statically translated host? Static NAT occurs.

A. After the inbound kernel, and before routing. B.
After the outbound kernel, and before routing. C.
After the inbound kernel, and aftter routing.
D. Before the inbound kernel, and after routing.
E. Before the outbound kernel, and before routing.
Answer: C

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Get Latest & Actual IT Exam Dumps with VCE and PDF from Pass4itSure.
https://www.Pass4itSure.com