156-215.77 Q&As

Check Point Certified Security Administrator

Pass CheckPoint 156-215.77 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/156-215-77.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John\\'s desktop which is assigned a static IP address 10.0.0.19.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy. 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web

Server from any machine and from any location.

What should John do when he cannot access the web server from a different personal computer?

A. John should lock and unlock his computer

B. Investigate this as a network connectivity issue

C. The access should be changed to authenticate the user instead of the PC

D. John should install the Identity Awareness Agent

Correct Answer: C

QUESTION 2

What gives administrators more flexibility when configuring Captive Portal instead of LDAP query for Identity Awareness authentication?

A. Captive Portal is more secure than standard LDAP

B. Nothing, LDAP query is required when configuring Captive Portal

C. Captive Portal works with both configured users and guests

D. Captive Portal is more transparent to the user

Correct Answer: C

QUESTION 3

During which step in the installation process is it necessary to note the fingerprint for first- time verification?

A. When configuring the Gateway in the WebUI

B. When configuring the Security Management Server using cpconfig

C. When establishing SIC between the Security Management Server and the Gateway

D. When configuring the Security Gateway object in SmartDashboard

Correct Answer: B

QUESTION 4

The R77 fw monitor utility is used to troubleshoot which of the following problems?

A. Traffic issues

B. Log Consolidation Engine

C. User data base corruption

D. Phase two key negotiation

Correct Answer: A

QUESTION 5

Identity Awareness is implemented to manage access to protected resources based on a user\\'s _____.

A. Application requirement

B. Computer MAC address

C. Identity

D. Time of connection

Correct Answer: C

QUESTION 6

Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism, when logging in to a remote server with Telnet?

A. Manual Sign On

B. Agent Automatic Sign On

C. Partially Automatic Sign On

D. Standard Sign On

Correct Answer: C

QUESTION 7

When you use the Global Properties\\' default settings on R77, which type of traffic will be dropped if NO explicit rule allows the traffic?

A. SmartUpdate connections

B. Outgoing traffic originating from the Security Gateway

C. Firewall logging and ICA key-exchange information

D. RIP traffic

Correct Answer: D

QUESTION 8

Your organization\\'s disaster recovery plan needs an update to the backup and restore section to reap the new distributed R77 installation benefits. Your plan must meet the following required and desired objectives:

Required ObjectivE. The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired ObjectivE. The R77 components that enforce the Security Policies should be backed up at least once a week.

Desired ObjectivE. Back up R77 logs at least once a week.

Your disaster recovery plan is as follows:

-Use the cron utility to run the command upgrade_export each night on the Security Management Servers.

-

Configure the organization\\'s routine back up software to back up the files created by the command upgrade_export.

-

Configure the GAiA back up utility to back up the Security Gateways every Saturday night.

-Use the cron utility 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. Upon evaluation, your plan:

A.

Meets the required objective and only one desired objective.

B.

Meets the required objective but does not meet either desired objective.

C.

Does not meet the required objective.

D.

Meets the required objective and both desired objectives.

Correct Answer: D

QUESTION 9

Which NAT option applicable for Automatic NAT applies to Manual NAT as well?

A. Allow bi-directional NAT

B. Automatic ARP configuration

C. Translate destination on client-side

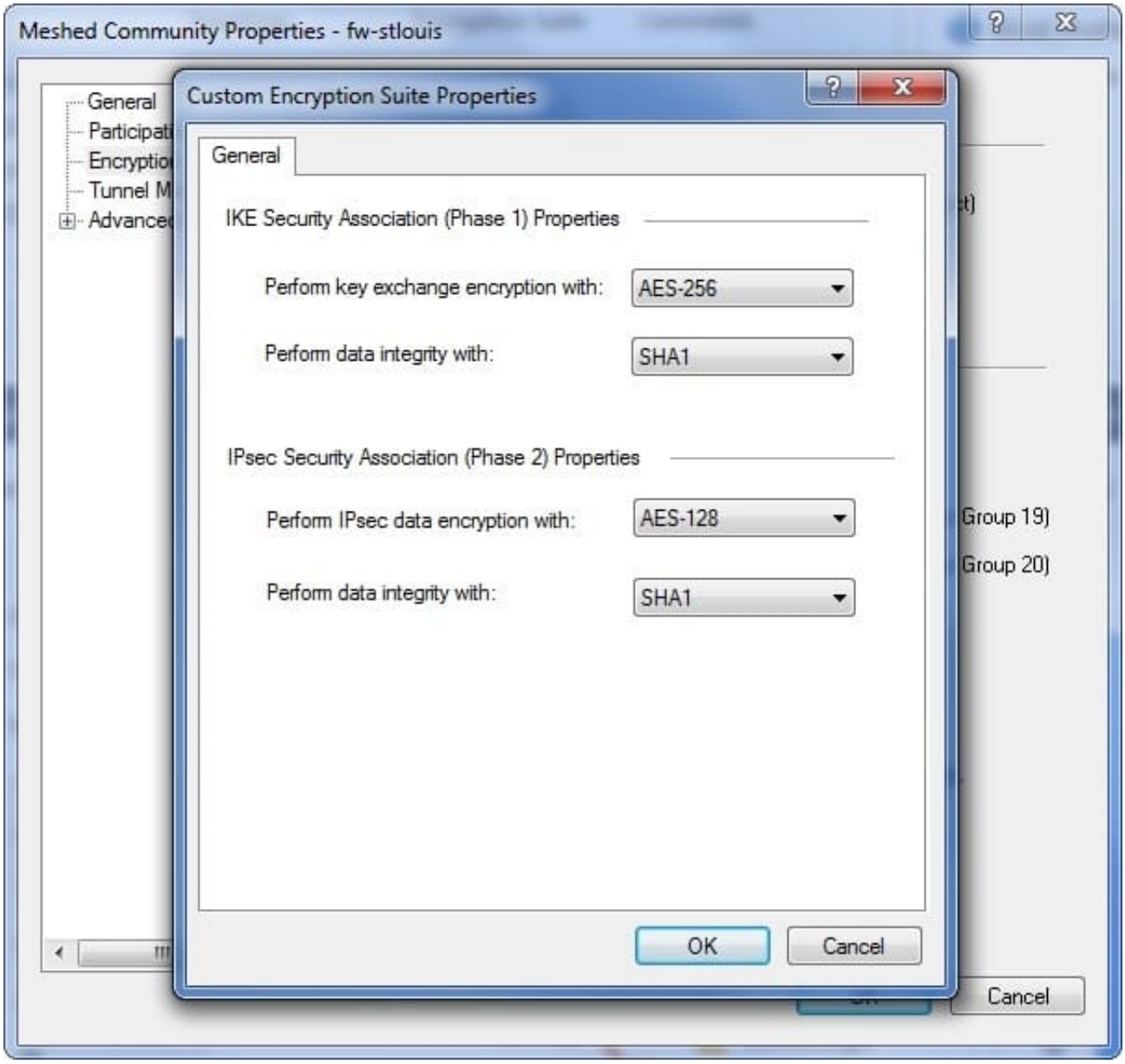
D. Enable IP Pool NAT

Correct Answer: C

QUESTION 10

You have a mesh VPN Community configured to create a site-to-site VPN. Given the displayed VPN properties, what can you conclude about this community?

Exhibit:



A. The VPN Community will perform IKE Phase 1 key-exchange encryption using the longest key Security Gateway R77 supports.

B. Changing the setting Perform key exchange encryption with from AES-256 to 3DES will enhance the VPN Community\\'s security , and reduce encryption overhead.

C. Change the data-integrity setting for this VPN Community because MD5 is incompatible with AES.

D. Changing the setting Perform IPsec data encryption with from AES-128 to 3Des will increase the encryption overhead.

Correct Answer: D

QUESTION 11

You receive a notification that long-lasting Telnet connections to a mainframe are dropped after an hour of

inactivity. Reviewing SmartView Tracker shows the packet is dropped with the error:

Unknown established connection

How do you resolve this problem without causing other security issues? Choose the BEST answer.

A. Increase the service-based session timeout of the default Telnet service to 24-hours.

B. Ask the mainframe users to reconnect every time this error occurs.

C. Increase the TCP session timeout under Global Properties > Stateful Inspection.

D. Create a new TCP service object on port 23 called Telnet-mainframe. Define a service- based session timeout of 24-hours. Use this new object only in the rule that allows the Telnet connections to the mainframe.

Correct Answer: D

QUESTION 12

You are a Security Administrator who has installed Security Gateway R77 on your network. You need to

allow a specific IP address range for a partner site to access your intranet Web server. To limit the

partner\\'s access for HTTP and FTP only, you did the following:

1) Created manual Static NAT rules for the Web server.

2) Cleared the following settings in the Global Properties > Network Address Translation screen:

-Allow bi-directional NAT

-

Translate destination on client side Do the above settings limit the partner\\'s access?

A.

Yes. This will ensure that traffic only matches the specific rule configured for this traffic, and that the Gateway translates the traffic after accepting the packet.

B.

No. The first setting is not applicable. The second setting will reduce performance.

C.

Yes. Both of these settings are only applicable to automatic NAT rules.

D.

No. The first setting is only applicable to automatic NAT rules. The second setting will force translation by the kernel on the interface nearest to the client.

Correct Answer: D

QUESTION 13

You are a Security Administrator using one Security Management Server managing three different firewalls. One firewall does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is a possible cause?

A. The firewall has failed to sync with the Security Management Server for 60 minutes.

B. The firewall object has been created but SIC has not yet been established.

C. The firewall is not listed in the Policy Installation Targets screen for this policy package.

D. The license for this specific firewall has expired.

Correct Answer: C

QUESTION 14

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

A. 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.

B. Two mesh and one star Community: Each mesh Community is set up for each site between headquarters their branches. The star Community has New York as the center and London as its satellite.

C. Two star communities and one mesh: A star community for each city with headquarters as center, and branches as satellites. Then one mesh community for the two headquarters.

D. 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 center Gateways? option checked; all London branch offices defined in one satellite window; but, all New York branch offices defined in another satellite window.

Correct Answer: C

QUESTION 15

How do you configure an alert in SmartView Monitor?

A. An alert cannot be configured in SmartView Monitor.

B. By choosing the Gateway, and Configure Thresholds.

C. By right-clicking on the Gateway, and selecting Properties.

D. By right-clicking on the Gateway, and selecting System Information.

Correct Answer: B

156-215.77 PDF Dumps 156-215.77 Practice Test 156-215.77 Study Guide