Free Questions for 156-315.81 by actualtestdumps

Shared by Carey on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What ports are used for SmartConsole to connect to the Security Management Server?

Options:

A- CPMI (18190)

B- ICA_Pull (18210), CPMI (18190) https (443)

C- CPM (19009), CPMI (18190) https (443)

D- CPM (19009), CPMI (18190) CPD (18191)

Answer:

C

Explanation:

The correct answer is C) CPM (19009), CPMI (18190) https (443).

SmartConsole is a client application that connects to the Security Management Server to manage and configure the security policy and objects. SmartConsole uses three ports to communicate with the Security Management Server1:

CPM (19009): This port is used for the communication between the SmartConsole client and the Check Point Management (CPM) process on the Security Management Server. The CPM process handles the database operations and the policy installation.

CPMI (18190): This port is used for the communication between the SmartConsole client and the Check Point Management Interface (CPMI) process on the Security Management Server. The CPMI process handles the authentication and encryption of the SmartConsole sessions.

https (443): This port is used for the communication between the SmartConsole client and the web server on the Security Management Server. The web server provides the SmartConsole GUI and the SmartConsole extensions.

The other options are incorrect because they either include ports that are not used by SmartConsole or omit ports that are used by SmartConsole.

SmartConsole R81.20 - Check Point Software1

Question 2

Question Type: **MultipleChoice**

Which of the following is true regarding the Proxy ARP feature for Manual NAT?

Options:

A- The local.arp file must always be configured

B- Automatic proxy ARP configuration can be enabled

C- fw ctl proxy should be configured

D- Translate Destination on Client Side should be configured

Answer:

B

Explanation:

The verified answer is B) Automatic proxy ARP configuration can be enabled.

Proxy ARP is a feature that allows a gateway to respond to ARP requests on behalf of another IP address that is not on the same network segment. Proxy ARP is required for manual NAT rules when the NATed IP addresses are not routed to the gateway1.

By default, proxy ARP for manual NAT rules has to be configured manually by editing the local.arp file or using the CLISH commands on the gateway2. However, since R80.10, there is an option to enable automatic proxy ARP configuration for manual NAT rules by modifying the files $CPDIR/tmp/.CPprofile.sh and $CPDIR/tmp/.CPprofile.csh on the gateway3.

fw ctl proxy is a command that displays the proxy ARP table on the gateway, but it does not configure proxy ARP4.

Translate Destination on Client Side is a NAT option that determines whether the destination IP address is translated before or after the routing decision. It does not affect proxy ARP.

Configuring Proxy ARP for Manual NAT - Check Point Software1

R80.10: Automatic Proxy ARP with Manual NAT rules - checkpoint<dot>engineer2

Automatic creation of Proxy ARP for Manual NAT rules on Security Gateway R80.103

fw ctl proxy - Check Point Software

NAT Properties - Check Point Software

Question 3

Question Type: **MultipleChoice**

Alice was asked by Bob to implement the Check Point Mobile Access VPN blade - therefore are some basic configuration steps required - which statement about the configuration steps is true?

Options:

A- 1. Add a rule in the Access Control Policy and install policy
2. Configure Mobile Access parameters in Security Gateway object
3. Enable Mobile Access blade on the Security Gateway object and complete the wizard
4. Connect to the Mobile Access Portal

B- 1. Connect to the Mobile Access Portal
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Configure Mobile Access parameters in Security Gateway object
4. Add a rule in the Access Control Policy and install policy

C- 1. Configure Mobile Access parameters in Security Gateway object
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal

D- 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard
2. Configure Mobile Access parameters in Security Gateway object
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal

Answer:

D

Explanation:

The verified answer is D) 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard 2. Configure Mobile Access parameters in Security Gateway object 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal

The basic configuration steps for the Check Point Mobile Access VPN blade are as follows1:

Enable Mobile Access blade on the Security Gateway object and complete the wizard: This step activates the Mobile Access blade on the selected gateway and guides you through the initial configuration, such as defining the portal name, the certificate, and the authentication methods.

Configure Mobile Access parameters in Security Gateway object: This step allows you to customize the Mobile Access settings, such as defining the supported applications, the access roles, the client settings, and the advanced options.

Add a rule in the Access Control Policy and install policy: This step creates a rule that allows the traffic from the Mobile Access portal to the protected resources and installs the policy on the gateway.

Connect to the Mobile Access Portal: This step verifies that the Mobile Access portal is accessible and functional from a web browser or a mobile device.

The other options are incorrect because they do not follow the correct order or include the necessary steps.

Mobile Access Administration Guide R81 - Check Point Software1

Question 4

Question Type: MultipleChoice

Which command collects diagnostic data for analyzing a customer setup remotely?

Options:

A- cpv

B- cpinfo

C- migrate export

D- sysinfo

Answer:

B

Explanation:

The verified answer is B) cpinfo.

cpinfo is a command that collects diagnostic data for analyzing a customer setup remotely. It is an auto-updatable utility that runs on the customer's machine and uploads the data to Check Point servers. The data includes information about the system, the security policy, the objects, and the logs. Check Point support engineers can use the DiagnosticsView utility to open the cpinfo file and view the

customer's configuration and environment settings1.

migrate export is a command that exports the Check Point configuration and database files to a compressed file. It is used for backup and migration purposes, not for remote analysis2.

sysinfo is a command that displays basic information about the system, such as the hostname, the OS version, the CPU model, and the memory size. It does not collect or upload any data to Check Point servers3.

cpv is not a valid command in Check Point.

Support, Support Requests, Training ... - Check Point Software1

Migrate export - Check Point Software

sysinfo - Check Point Software

Question 5

Question Type: **MultipleChoice**

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

Options:

A- Application Control

B- Firewall

C- Identity Awareness

D- URL Filtering

Answer:

C

Explanation:

The verified answer is C. Identity Awareness.

Identity Awareness is the Check Point software blade that provides detailed visibility of users, groups, and machines, while also providing application and access control through the creation of accurate, identity-based policies1. Identity Awareness allows you to easily configure network access and auditing based on three items: network location, the identity of a user and the identity of a machine1. Identity Awareness integrates with multiple identity sources, such as Microsoft Active Directory, Cisco Identity Services Engine, and RADIUS Accounting23.

Application Control is the Check Point software blade that enables network administrators to identify and control thousands of applications and widgets, and millions of websites, based on categories, risk, and characteristics.

Firewall is the Check Point software blade that provides stateful inspection and enforcement of network traffic, and protects against network and application-level attacks.

URL Filtering is the Check Point software blade that enables secure web access by blocking access to malicious and inappropriate websites, and enforcing compliance with corporate policies.

Identity Awareness - Check Point Software1

Check Point Integrated Security Architecture - Check Point Software2

Cisco Identity Services Engine and Check Point Integration3

Application Control - Check Point Software

Firewall - Check Point Software

URL Filtering - Check Point Software

Question 6

Question Type: **MultipleChoice**

While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

Options:

A- Security Gateway is not part of the Domain

B- SmartConsole machine is not part of the domain

C- Identity Awareness is not enabled on Global properties

D- Security Management Server is not part of the domain

Answer:

B

Explanation:

The verified answer is B) SmartConsole machine is not part of the domain.

The Identity Awareness wizard uses the SmartConsole machine to detect the windows domain by querying the Active Directory server using DCOM protocol1. If the SmartConsole machine is not part of the domain, the query will fail and the wizard will not automatically detect the domain. The user will have to manually enter the domain name and credentials to proceed with the configuration.

The Security Gateway, the Security Management Server, and the Identity Awareness global properties do not affect the domain detection by the wizard. However, they are required for other aspects of the Identity Awareness blade, such as AD Query, Identity Collector, and Browser-Based Authentication2.

Identity Awareness Configuration wizard authentication fails3

Identity Awareness - Check Point Software4

Question 7

Question Type: MultipleChoice

Which of the following cannot be configured in an Access Role Object?

Options:

A- Networks

B- Machines

C- Users

D- Time

Answer:

D

Explanation:

The verified answer is D) Time.

An Access Role object is a logical representation of a set of users, machines, or networks that can be used in the security policy1. An Access Role object can include the following components1:

Networks: IP addresses or network objects that define the source or destination of the traffic.

Machines: Specific hosts or machine groups that are identified by their MAC addresses or certificates.

Users: Specific users or user groups that are authenticated by one or more identity sources, such as Active Directory, LDAP, or Identity Awareness.

Time is not a component of an Access Role object, and it cannot be configured in it. Time is a separate object type that can be used to define the validity period of a rule or a policy2.

LDAP group vs Access role objects - Check Point CheckMates3

THE IMPORTANCE OF ACCESS ROLES - Check Point Software1

Time Objects - Check Point Software2

Question 8

Question Type: MultipleChoice

Identity Awareness lets an administrator easily configure network access and auditing based on three items. Choose the correct statement.

Options:

A- Network location, the identity of a user and the identity of a machine.

B- Geographical location, the identity of a user and the identity of a machine.

C- Network location, the identity of a user and the active directory membership.

D- Network location, the telephone number of a user and the UID of a machine.

Answer:

A

Explanation:

The correct answer is A. Network location, the identity of a user and the identity of a machine.

Identity Awareness allows you to easily configure network access and auditing based on three items: network location, the identity of a user and the identity of a machine1. This enables you to create granular and accurate identity-based policies that control who can access what, when and how. You can also monitor and log user and machine activities for compliance and auditing purposes.

Geographical location, the telephone number of a user and the UID of a machine are not the items that Identity Awareness uses to identify and authorize users and machines.

Identity Awareness - Check Point Software1