

Exam Questions 156-215.80

Check Point Certified Security Administrator

<https://www.2passeasy.com/dumps/156-215.80/>



NEW QUESTION 1

- (Exam Topic 1)

Which of the following is NOT a component of a Distinguished Name?

- A. Organization Unit
- B. Country
- C. Common name
- D. User container

Answer: D

Explanation:

Distinguished Name Components

CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name

NEW QUESTION 2

- (Exam Topic 1)

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

Which of the following is NOT a SecureXL traffic flow?

- A. Medium Path
- B. Accelerated Path
- C. Fast Path
- D. Slow Path

Answer: C

Explanation:

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL. Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.

Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

NEW QUESTION 4

- (Exam Topic 1)

The Gaia operating system supports which routing protocols?

- A. BGP, OSPF, RIP
- B. BGP, OSPF, EIGRP, PIM, IGMP
- C. BGP, OSPF, RIP, PIM, IGMP
- D. BGP, OSPF, RIP, EIGRP

Answer: A

Explanation:

The Advanced Routing Suite

The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

NEW QUESTION 5

- (Exam Topic 1)

What does ExternalZone represent in the presented rule?

- A. The Internet.
- B. Interfaces that administrator has defined to be part of External Security Zone.
- C. External interfaces on all security gateways.
- D. External interfaces of specific gateways.

Answer: B

Explanation:

Configuring Interfaces

Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window. To configure the interfaces:

From the Devices window, double-click the Security Gateway 80.

The Security Gateway

window opens.

Select the Interfaces tab.

Select Use the following settings. The interface settings open.

Select the interface and click Edit.

The Edit window opens.

From the IP Assignment section, configure the IP address of the interface:

Select Static IP.

Enter the IP address and subnet mask for the interface.

In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.

References:

NEW QUESTION 6

- (Exam Topic 1)

What will be the effect of running the following command on the Security Management Server?

- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

Answer: A

Explanation:

This command uninstall actual security policy (already installed) References:

NEW QUESTION 7

- (Exam Topic 1)

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.

- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

Answer: B

Explanation:

Administrator Collaboration

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 8

- (Exam Topic 1)

Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

- A. Local
- B. Central
- C. Corporate
- D. Formal

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

- A. remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands: lock database override and unlock databas
- E. Both will work.

Answer: D

Explanation:

Use the database feature to obtain the configuration lock. The database feature has two commands:

lock database [override].

unlock database

The commands do the same thing: obtain the configuration lock from another administrator.

NEW QUESTION 10

- (Exam Topic 1)

Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

- A. /var/log/Cpbackup/backups/backup/backup_fw.tgs
- B. /var/log/Cpbackup/backups/backup/backup_fw.tar
- C. /var/log/Cpbackup/backups/backups/backup_fw.tar
- D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D

Explanation:

Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration. The configuration is saved to a .tgz file in the following directory:

Gaia OS Version Hardware

Local Directory R75.40 - R77.20

Check Point appliances

/var/log/CPbackup/backups/ Open Server

/var/CPbackup/backups/ R77.30

Check Point appliances

/var/log/CPbackup/backups/ Open Server

NEW QUESTION 10

- (Exam Topic 1)

Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?

- A. cpconfig
- B. fw ctl pstat
- C. cpview
- D. fw ctl multik stat

Answer: C

Explanation:

CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.

NEW QUESTION 14

- (Exam Topic 1)

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Answer: A

Explanation:

The order of NAT priorities is:

Static NAT
IP Pool NAT
Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

NEW QUESTION 19

- (Exam Topic 1)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CApp

Answer: B

Explanation:

AppWiki Application Classification Library

AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.

NEW QUESTION 21

- (Exam Topic 1)

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 23

- (Exam Topic 1)

In R80, Unified Policy is a combination of

- A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
- B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.

Answer: D

Explanation:

D is the best answer given the choices. Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

Firewall and VPN
Application Control and URL Filtering
Identity Awareness
Data Awareness
Mobile Access
Security Zones

NEW QUESTION 24

- (Exam Topic 1)

Which one of the following is the preferred licensing model? Select the Best answer.

- A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.
- B. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency of the gateway.
- C. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
- D. Central licensing because it ties the package license to the MAC-address of the Security Management Server Mgmt-interface and has no dependency of the gateway.

Answer: B

Explanation:

Central License

A Central License is a license attached to the Security Management server IP address, rather than the gatewa IP address. The benefits of a Central License are:

Only one IP address is needed for all licenses.

A license can be taken from one gateway and given to another.

The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

NEW QUESTION 26

- (Exam Topic 1)

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

- A. Display policies and logs on the administrator's workstation.
- B. Verify and compile Security Policies.
- C. Processing and sending alerts such as SNMP traps and email notifications.
- D. Store firewall logs to hard drive storage.

Answer: A

NEW QUESTION 28

- (Exam Topic 1)

Fill in the blank: A ____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

- A. Clientless remote access
- B. Clientless direct access
- C. Client-based remote access
- D. Direct access

Answer: A

Explanation:

Clientless - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

NEW QUESTION 29

- (Exam Topic 1)

On the following graphic, you will find layers of policies.

What is a precedence of traffic inspection for the defined polices?

- A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.
- B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer
- C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.
- D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.

Answer: B

Explanation:

To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

For example, when you upgrade to R80 from earlier versions:

Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.

All layers are evaluated in parallel

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

All layers are evaluated in parallel

NEW QUESTION 34

- (Exam Topic 1)

WeBControl Layer has been set up using the settings in the following dialogue:

Consider the following policy and select the BEST answer.

- A. Traffic that does not match any rule in the subpolicy is dropped.
- B. All employees can access only Youtube and Vimeo.
- C. Access to Youtube and Vimeo is allowed only once a day.
- D. Anyone from internal network can access the internet, except the traffic defined in drop rules 5.2, 5.5 and 5.6.

Answer: D

Explanation:

Policy Layers and Sub-Policies

R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators

With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an “accept” action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.

Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.

Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

NEW QUESTION 36

- (Exam Topic 1)

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

- A. Central
- B. Corporate
- C. Formal
- D. Local

Answer: D

NEW QUESTION 37

- (Exam Topic 1)

The security Gateway is installed on GAI A R80 The default port for the WEB User Interface is ____.

- A. TCP 18211
- B. TCP 257
- C. TCP 4433
- D. TCP 443

Answer: D

NEW QUESTION 39

- (Exam Topic 1)

Where can you trigger a failover of the cluster members?

Log in to Security Gateway CLI and run command clusterXL_admin down.

In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

- A. 1, 2, and 3
- B. 2 and 3
- C. 1 and 2
- D. 1 and 3

Answer: C

Explanation:

How to Initiate Failover

NEW QUESTION 43

- (Exam Topic 1)

Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: <https://personal.mymail.com>, which blade will she enable to achieve her goal?

- A. DLP
- B. SSL Inspection
- C. Application Control
- D. URL Filtering

Answer: A

Explanation:

Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

NEW QUESTION 46

- (Exam Topic 1)

Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

- A. Block Port Overflow
- B. Local Interface Spoofing
- C. Suspicious Activity Monitoring
- D. Adaptive Threat Prevention

Answer: C

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation

NEW QUESTION 51

- (Exam Topic 1)

What is the default time length that Hit Count Data is kept?

- A. 3 month
- B. 4 weeks
- C. 12 months
- D. 6 months

Answer: A

Explanation:

Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

NEW QUESTION 53

- (Exam Topic 2)

What statement is true regarding Visitor Mode?

- A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
- B. Only ESP traffic is tunneled through port TCP 443.
- C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
- D. All VPN traffic is tunneled through UDP port 4500.

Answer: A

NEW QUESTION 57

- (Exam Topic 2)

What are the three tabs available in SmartView Tracker?

- A. Network & Endpoint, Management, and Active
- B. Network, Endpoint, and Active
- C. Predefined, All Records, Custom Queries
- D. Endpoint, Active, and Custom Queries

Answer: C

NEW QUESTION 60

- (Exam Topic 2)

Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

- A. Yes.
- B. No.

- C. Yes, but only when using Automatic NAT.
- D. Yes, but only when using Manual NAT.

Answer: A

NEW QUESTION 65

- (Exam Topic 2)

You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the “Select additional profile that will be able edit this layer” you do not see anything. What is the most likely cause of this problem? Select the BEST answer.

- A. “Edit layers by Software Blades” is unselected in the Permission Profile
- B. There are no permission profiles available and you need to create one first.
- C. All permission profiles are in use.
- D. “Edit layers by selected profiles in a layer editor” is unselected in the Permission profile.

Answer: B

NEW QUESTION 67

- (Exam Topic 2)

Which of the following is TRUE about the Check Point Host object?

- A. Check Point Host has no routing ability even if it has more than one interface installed.
- B. When you upgrade to R80 from R77.30 or earlier versions, Check Point Host objects are converted to gateway objects.
- C. Check Point Host is capable of having an IP forwarding mechanism.
- D. Check Point Host can act as a firewall.

Answer: A

Explanation:

A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server. It is not a routing mechanism and is not capable of IP forwarding.

NEW QUESTION 70

- (Exam Topic 2)

What action can be performed from SmartUpdate R77?

- A. upgrade_export
- B. fw stat -1
- C. cpinfo
- D. remote_uninstall_verifier

Answer: C

NEW QUESTION 74

- (Exam Topic 2)

Which directory holds the SmartLog index files by default?

- A. \$SMARTLOGDIR/data
- B. \$SMARTLOG/dir
- C. \$FWDIR/smartlog
- D. \$FWDIR/log

Answer: A

NEW QUESTION 78

- (Exam Topic 2)

Study the Rule base and Client Authentication Action properties screen.

After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site. What happens when the user tries to FTP to another site using the command line? The:

- A. user is prompted for authentication by the Security Gateways again.
- B. FTP data connection is dropped after the user is authenticated successfully.
- C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication
- D. FTP connection is dropped by Rule 2.

Answer: C

NEW QUESTION 80

- (Exam Topic 2)

Choose the SmartLog property that is TRUE.

- A. SmartLog has been an option since release R71.10.
- B. SmartLog is not a Check Point product.
- C. SmartLog and SmartView Tracker are mutually exclusive.
- D. SmartLog is a client of SmartConsole that enables enterprises to centrally track log records and security activity with Google-like search.

Answer: D

NEW QUESTION 83

- (Exam Topic 2)

Administrator wishes to update IPS from SmartConsole by clicking on the option “update now” under the IPS tab. Which device requires internet access for the update to work?

- A. Security Gateway
- B. Device where SmartConsole is installed
- C. SMS
- D. SmartEvent

Answer: B

Explanation:

Updating IPS Manually

You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.

To obtain updates of all the latest protections from the IPS website:

Configure the settings for the proxy server in Internet Explorer.
In Microsoft Internet Explorer, open Tools > Internet Options > Connections tab > LAN Settings.
The LAN Settings window opens.
Select Use a proxy server for your LAN.
Configure the IP address and port number for the proxy server.
Click OK.
The settings for the Internet Explorer proxy server are configured.
In the IPS tab, select Download Updates
and click Update Now.

NEW QUESTION 87

- (Exam Topic 2)

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server

Answer: D

Explanation:

Users
Use the WebUI and CLI to manage user accounts. You can:
Add users to your Gaia system.
Edit the home directory of the user.
Edit the default shell for a user.
Give a password to a user.
Give privileges to users.

NEW QUESTION 90

- (Exam Topic 2)

Which feature in R77 permits blocking specific IP addresses for a specified time period?

- A. Suspicious Activity Monitoring
- B. HTTP Methods
- C. Local Interface Spoofing
- D. Block Port Overflow

Answer: A

NEW QUESTION 93

- (Exam Topic 2)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

Explanation:

This chapter gives an introduction to the Gaia command line interface (CLI). The default shell of the CLI is called clish.

NEW QUESTION 95

- (Exam Topic 2)

What is the default method for destination NAT?

- A. Destination side
- B. Source side
- C. Server side
- D. Client side

Answer: D

NEW QUESTION 96

- (Exam Topic 2)

The Captive Portal tool:

- A. Acquires identities from unidentified users.
- B. Is only used for guest user authentication.
- C. Allows access to users already identified.
- D. Is deployed from the Identity Awareness page in the Global Properties settings.

Answer: A

NEW QUESTION 99

- (Exam Topic 2)

Which authentication scheme requires a user to possess a token?

- A. TACACS
- B. SecurID
- C. Check Point password
- D. RADIUS

Answer: B

Explanation:

SecurID

SecurID requires users to both possess a token authenticator and to supply a PIN or password References:

NEW QUESTION 101

- (Exam Topic 2)

Which of the following statements accurately describes the command snapshot?

- A. snapshot creates a full OS-level backup, including network-interface data, Check Point production information, and configuration settings of a GAiA Security Gateway.
- B. snapshot creates a Security Management Server full system-level backup on any OS
- C. snapshot stores only the system-configuration settings on the Gateway
- D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server

Answer: A

NEW QUESTION 105

- (Exam Topic 2)

AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

- A. Rule is locked by AdminA, because the save bottom has not been press.
- B. Rule is locked by AdminA, because an object on that rule is been edited.
- C. Rule is locked by AdminA, and will make it available if session is published.
- D. Rule is locked by AdminA, and if the session is saved, rule will be available

Answer: C

NEW QUESTION 107

- (Exam Topic 2)

On the following picture an administrator configures Identity Awareness:

After clicking "Next" the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user
- C. Obligatory usage of Captive Portal
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

Answer: B

Explanation:

To enable Identity Awareness:

Log in to R80 SmartConsole.

From the Awareness.

Gateway&s

Servers

view, double-click the Security Gateway on which to enable Identity

On the Network Security tab, select Identity Awareness.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

NEW QUESTION 108

- (Exam Topic 2)

You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

- A. backup
- B. Database Revision
- C. snapshot
- D. migrate export

Answer: C

Explanation:

2. Snapshot Management

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.

The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 111

- (Exam Topic 2)

Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

- A. Create a text-file with mgmt_cli script that creates all objects and policie
- B. Open the file in SmartConsole Command Line to run it.
- C. Create a text-file with Gaia CLI -commands in order to create all objects and policie
- D. Run the file in CLISH with command load configuration.
- E. Create a text-file with DBEDIT script that creates all objects and policie
- F. Run the file in the command line of the management server using command dbedit -f.
- G. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

Answer: A

Explanation:

Did you know: mgmt_cli can accept csv files as inputs using the --batch option.

The first row should contain the argument names and the rows below it should hold the values for these parameters.

So an equivalent solution to the powershell script could look like this:

data.csv:

```
mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>
```

This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

NEW QUESTION 114

- (Exam Topic 3)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: C

NEW QUESTION 117

- (Exam Topic 3)

The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

- A. Six times per day
- B. Seven times per day
- C. Every two hours
- D. Every three hours

Answer: D

NEW QUESTION 120

- (Exam Topic 3)

A Cleanup rule:

- A. logs connections that would otherwise be dropped without logging by default.
- B. drops packets without logging connections that would otherwise be dropped and logged by default.
- C. logs connections that would otherwise be accepted without logging by default.
- D. drops packets without logging connections that would otherwise be accepted and logged by default.

Answer: A

NEW QUESTION 125

- (Exam Topic 3)

Which of these statements describes the Check Point ThreatCloud?

- A. Blocks or limits usage of web applications
- B. Prevents or controls access to web sites based on category
- C. Prevents Cloud vulnerability exploits
- D. A worldwide collaborative security network

Answer: D

NEW QUESTION 127

- (Exam Topic 3)

Which of the following actions do NOT take place in IKE Phase 1?

- A. Peers agree on encryption method.
- B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
- C. Peers agree on integrity method.
- D. Each side generates a session key from its private key and peer's public key.

Answer: B

NEW QUESTION 128

- (Exam Topic 3)

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

- A. External-user group
- B. LDAP group
- C. A group with a generic user
- D. All Users

Answer: B

NEW QUESTION 129

- (Exam Topic 3)

Which remote Access Solution is clientless?

- A. Checkpoint Mobile
- B. Endpoint Security Suite
- C. SecuRemote
- D. Mobile Access Portal

Answer: D

NEW QUESTION 131

- (Exam Topic 3)

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Dynamic encryption
- C. Certificate-based encryption
- D. Symmetric encryption

Answer: D

NEW QUESTION 134

- (Exam Topic 3)

What happens if the identity of a user is known?

- A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
- B. If the user credentials do not match an Access Role, the system displays a sandbox.
- C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
- D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Answer: C

NEW QUESTION 137

- (Exam Topic 3)

Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

- A. Check Point Password
- B. TACACS
- C. LDAP
- D. Windows password

Answer:

C

NEW QUESTION 138

- (Exam Topic 3)

Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

- A. SandBlast Threat Emulation
- B. SandBlast Agent
- C. Check Point Protect
- D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 140

- (Exam Topic 3)

VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

- A. 3DES and MD5
- B. Certificates and IPsec
- C. Certificates and pre-shared secret
- D. IPsec and VPN Domains

Answer: C

NEW QUESTION 143

- (Exam Topic 3)

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

- A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
- B. mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json
- C. mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json
- D. mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json

Answer: A

NEW QUESTION 148

- (Exam Topic 3)

Which of the following is NOT an attribute of packer acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. Application Awareness

Answer: D

NEW QUESTION 149

- (Exam Topic 3)

You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

- A. A group with generic user
- B. All users
- C. LDAP Account Unit Group
- D. Internal user Group

Answer: A

NEW QUESTION 151

- (Exam Topic 3)

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.

Answer: B

NEW QUESTION 154

- (Exam Topic 3)

When launching SmartDashboard, what information is required to log into R77?

- A. User Name, Management Server IP, certificate fingerprint file
- B. User Name, Password, Management Server IP

- C. Password, Management Server IP
- D. Password, Management Server IP, LDAP Server IP

Answer: B

NEW QUESTION 159

- (Exam Topic 3)

Which R77 GUI would you use to see number of packets accepted since the last policy install?

- A. SmartView Monitor
- B. SmartView Tracker
- C. SmartDashboard
- D. SmartView Status

Answer: A

NEW QUESTION 161

- (Exam Topic 3)

Identify the API that is not supported by Check Point currently.

- A. R80 Management API-
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

Answer: C

NEW QUESTION 162

- (Exam Topic 3)

If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client?

- A. Nothing
- B. TCP FIN
- C. TCP RST
- D. ICMP unreachable

Answer: A

NEW QUESTION 167

- (Exam Topic 4)

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

- A. Smart Cloud Services
- B. Load Sharing Mode Services
- C. Threat Agent Solution
- D. Public Cloud Services

Answer: A

NEW QUESTION 171

- (Exam Topic 4)

The SmartEvent R80 Web application for real-time event monitoring is called:

- A. SmartView Monitor
- B. SmartEventWeb
- C. There is no Web application for SmartEvent
- D. SmartView

Answer: B

NEW QUESTION 172

- (Exam Topic 4)

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

Answer: D

NEW QUESTION 173

- (Exam Topic 4)

Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. Gateway and Servers
- B. Logs and Monitor
- C. Manage Seeting
- D. Security Policies

Answer: B

NEW QUESTION 176

- (Exam Topic 4)

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

Answer: A

NEW QUESTION 179

- (Exam Topic 4)

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 181

- (Exam Topic 4)

What is the purpose of the Clean-up Rule?

- A. To log all traffic that is not explicitly allowed or denied in the Rule Base.
- B. To clean up policies found inconsistent with the compliance blade reports.
- C. To remove all rules that could have a conflict with other rules in the database.
- D. To eliminate duplicate log entries in the Security Gateway

Answer: A

NEW QUESTION 186

- (Exam Topic 4)

Which Threat Prevention Profile is not included by default in R80 Management?

- A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
- B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
- C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
- D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

Answer: D

NEW QUESTION 187

- (Exam Topic 4)

SmartEvent does NOT use which of the following procedures to identity events:

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

Answer: C

NEW QUESTION 189

- (Exam Topic 4)

Fill the blank. IT is Best Practice to have a _____ rule at the end of each policy layer.

- A. Explicit Drop
- B. Implied Drop
- C. Explicit Cleanup
- D. Implicit Drop

Answer: A

NEW QUESTION 191

- (Exam Topic 4)

Which deployment adds a Security Gateway to an existing environment without changing IP routing?

- A. Distributed
- B. Bridge Mode
- C. Remote
- D. Standalone

Answer: B

NEW QUESTION 192

- (Exam Topic 4)

In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting
- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 194

- (Exam Topic 4)

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

- A. fw ctl multik dynamic_dispatching on
- B. fw ctl multik dynamic_dispatching set_mode 9
- C. fw ctl multik set_mode 9
- D. fw ctl miltik pq enable

Answer: C

NEW QUESTION 197

- (Exam Topic 4)

What is the SOLR database for?

- A. Used for full text search and enables powerful matching capabilities
- B. Writes data to the database and full text search
- C. Serves GUI responsible to transfer request to the DLE server
- D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 202

- (Exam Topic 4)

When using Monitored circuit VRRP, what is a priority delta?

- A. When an interface fails the priority changes to the priority delta
- B. When an interface fails the delta claims the priority
- C. When an interface fails the priority delta is subtracted from the priority
- D. When an interface fails the priority delta decides if the other interfaces takes over

Answer: C

NEW QUESTION 207

- (Exam Topic 4)

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resident VPN client
- B. SSL VPN requires installation of a resident VPN client
- C. SSL VPN and IPSec VPN are the same
- D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Answer: D

NEW QUESTION 209

- (Exam Topic 4)

Fill in the blank: In order to install a license, it must first be added to the _____. .

- A. User Center
- B. Package repository
- C. Download Center Web site
- D. License and Contract repository

Answer: B

NEW QUESTION 212

- (Exam Topic 4)

Fill in the blanks. In _____ NAT, the _____ is translated.

- A. Hide; source
- B. Static; source
- C. Simple; source
- D. Hide; destination

Answer: B

NEW QUESTION 216

- (Exam Topic 4)

True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.
- D. False, only one administrator can login with write permission.

Answer: B

Explanation:

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

NEW QUESTION 220

- (Exam Topic 4)

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

NEW QUESTION 225

- (Exam Topic 4)

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete
- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer: B

NEW QUESTION 229

- (Exam Topic 4)

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: A

NEW QUESTION 234

- (Exam Topic 4)

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)
- B. Log Server
- C. SmartEvent
- D. Multi-domain management server

Answer: D

NEW QUESTION 235

- (Exam Topic 4)

Which of the following is the most secure means of authentication?

- A. Password
- B. Certificate
- C. Token
- D. Pre-shared secret

Answer: B

NEW QUESTION 240

- (Exam Topic 4)

Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

- A. Format; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

Answer: D

NEW QUESTION 245

- (Exam Topic 4)

Which path below is available only when CoreXL is enabled?

- A. Slow path
- B. Firewall path
- C. Medium path
- D. Accelerated path

Answer: C

NEW QUESTION 247

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.80 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.80 Product From:

<https://www.2passeasy.com/dumps/156-215.80/>

Money Back Guarantee

156-215.80 Practice Exam Features:

- * 156-215.80 Questions and Answers Updated Frequently
- * 156-215.80 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-215.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year