

Exam Questions 156-215.80

Check Point Certified Security Administrator

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



NEW QUESTION 1

- (Exam Topic 1)

What does the “unknown” SIC status shown on SmartConsole mean?

- A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
- B. SIC activation key requires a reset.
- C. The SIC activation key is not known by any administrator.
- D. There is no connection between the Security Gateway and SMS.

Answer: D

Explanation:

The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

NEW QUESTION 2

- (Exam Topic 1)

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C

Explanation:

To configure Security Management Server on Gaia:

Open a browser to the WebUI: <https://<Gaia management IP address>>

NEW QUESTION 3

- (Exam Topic 1)

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?

- A. Security Gateways is not part of the Domain
- B. SmartConsole machine is not part of the domain
- C. SMS is not part of the domain
- D. Identity Awareness is not enabled on Global properties

Answer: B

Explanation:

To enable Identity Awareness:

Log in to SmartDashboard.

From the Network Objects tree, expand the Check Point branch.

Double-click the Security Gateway on which to enable Identity Awareness.

In the Software Blades section, select Identity Awareness on the Network Security tab. 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).

See Choosing Identity Sources.

Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

Click Next.

The Integration With Active Directory window opens.

When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with all of the domain controllers in the organization's Active Directory.

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)

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

- A. Security Gateway
- B. Check Point user center
- C. Security Management Server
- D. SmartConsole installed device

Answer: C

Explanation:

SmartUpdate installs two repositories on the Security Management server:

License & Contract Repository, which is stored on all platforms in the directory \$FWDIR\conf\.

Package Repository, which is stored:

on Windows machines in C:\SUroot.

on UNIX machines in /var/suroot.

The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

NEW QUESTION 6

- (Exam Topic 1)

DLP and Geo Policy are examples of what type of Policy?

- A. Standard Policies
- B. Shared Policies
- C. Inspection Policies
- D. Unified Policies

Answer: B

Explanation:

The Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy	Create a policy for traffic to or from specific geographical or political locations.
HTTPS Policy	The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. To launch the HTTPS Policy, click Manage & Settings > Blades > HTTPS Inspection > Configure in SmartDashboard

NEW QUESTION 7

- (Exam Topic 1)

ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.



How will you describe the new “Publish” button in R80 Management Console?

- A. The Publish button takes any changes an administrator has made in their management session, publishes a copy to the Check Point of R80, and then saves it to the R80 database.
- B. The Publish button takes any changes an administrator has made in their management session and publishes a copy to the Check Point Cloud of R80 and but does not save it to the R80
- C. The Publish button makes any changes an administrator has made in their management session visible to all other administrator sessions and saves it to the Database.
- D. The Publish button makes any changes an administrator has made in their management session visible to the new Unified Policy session and saves it to the Database.

Answer: C

Explanation:

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

The following graphic shows:

[illegible]

- A. View from SmartLog for logs initiated from source address 10.1.1.202
B. View from SmartView Tracker for logs of destination address 10.1.1.202
C. View from SmartView Tracker for logs initiated from source address 10.1.1.202
D. View from SmartView Monitor for logs initiated from source address 10.1.1.202

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Which of the following is NOT an integral part of VPN communication within a network?

- A. VPN key
B. VPN community
C. VPN trust entities
D. VPN domain

Answer: A

Explanation:

VPN key (to not be confused with pre-shared key that is used for authentication).

VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.

VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.

VPN Community - A named collection of VPN domains, each protected by a VPN gateway. References:

http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

NEW QUESTION 10

- (Exam Topic 1)

Fill in the blank: Gaia can be configured using the _____ or _____.

- A. Gaia; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

Answer: C

Explanation:

Configuring Gaia for the First Time In This Section:

Running the First Time Configuration Wizard in WebUI Running the First Time Configuration Wizard in CLI

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

NEW QUESTION 13

- (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 15

- (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 19

- (Exam Topic 1)

Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

- A. upgrade_import
- B. cpconfig
- C. fwm dbimport -p <export file>
- D. cpinfo -recover

Answer: A

Explanation:

(Should be "migrate import")

"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " upgrade_import ".

NEW QUESTION 22

- (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 23

- (Exam Topic 1)

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only

- B. Read/Write, Read only, None
- C. Read/Write, None
- D. Read Only, None

Answer: B

Explanation:

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (readonly) access to other features, and no access to other features.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

NEW QUESTION 27

- (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 28

- (Exam Topic 1)

Fill in the blank: The tool ____ generates a R80 Security Gateway configuration report.

- A. infoCP
- B. infoview
- C. cpinfo
- D. fw cpinfo

Answer: C

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPinfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPinfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

NEW QUESTION 30

- (Exam Topic 1)

When attempting to start a VPN tunnel, in the logs the error 'no proposal chosen' is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

Answer: D

NEW QUESTION 33

- (Exam Topic 1)

What is NOT an advantage of Packet Filtering?

- A. Low Security and No Screening above Network Layer
- B. Application Independence
- C. High Performance
- D. Scalability

Answer: A

Explanation:

Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

NEW QUESTION 34

- (Exam Topic 1)

Fill in the blank: Each cluster has _____ interfaces.

- A. Five
- B. Two
- C. Three
- D. Four

Answer: C

Explanation:

Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each direction are connected via a switch, router, or VLAN switch.

NEW QUESTION 36

- (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 38

- (Exam Topic 1)

You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:

APP	PID	STAT	#START	START_TIME	MON	COMMAND
CPVIEW	1078	E	1	[16:26:34] 5/5/2016	N	cpviewd
CPD	0	T	1	[17:13:37] 6/5/2016	N	cpd
FWD	21761	E	1	[17:13:31] 6/5/2016	N	fwd -c
CPM	0	T	1	[16:32:23] 6/5/2016	N	/opt/CPsuite-R80/fw1/scripts/cpm.sh -v
FWM	0	T	1	[17:13:45] 6/5/2016	N	fwm
SSL	7873	E	1	[16:32:32] 5/5/2016	N	LogCore
SMARTVIEW	7884	E	1	[16:32:32] 5/5/2016	N	SmartView
INDEXER	7894	E	1	[16:32:33] 5/5/2016	N	/opt/CPsuite-R80/log_indexer/log_indexer
SMARTLOG_SERVER	7977	E	1	[16:32:33] 5/5/2016	N	/opt/CPsuite-R80/smartlog_server
SVR	8045	E	1	[16:32:34] 5/5/2016	N	SVRServer
DASERVICE	8094	E	1	[16:32:34] 5/5/2016	N	DAService_script
CPDM	0	T	0	[17:17:02] 6/5/2016	N	cpstat_monitor

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

- A. CDP is down
- B. SVR is down
- C. FWM is down
- D. CPSM is down

Answer: C

Explanation:

The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.).

STATE is T (Terminate = Down)

Symptoms

SmartDashboard fails to connect to the Security Management server.

Verify if the FWM process is running. To do this, run the command:

[Expert@HostName:0]# ps -aux | grep fwm

If the FWM process is not running, then try force-starting the process with the following command: [Expert@HostName:0]# cpwd_admin start -name FWM -path "\$FWDIR/bin/fwm" -command "fwm" [Expert@HostName:0]# ps -aux | grep fwm

[Expert@HostName:0]# cpwd_admin start -name FWM -path "\$FWDIR/bin/fwm" -command "fwm"

NEW QUESTION 40

- (Exam Topic 1)

Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

- A. High Availability
- B. Load Sharing Multicast
- C. Load Sharing Pivot
- D. Master/Backup

Answer: B

Explanation:

ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

NEW QUESTION 42

- (Exam Topic 2)

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: D

Explanation:

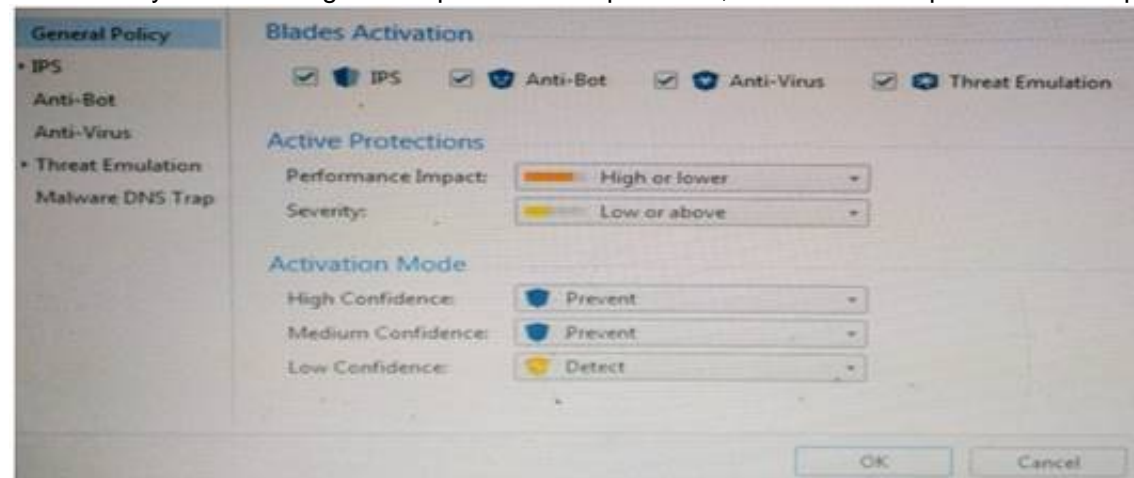
SandBlast Threat Emulation

As part of the Next Generation Threat Extraction software bundle (NGTX), the SandBlast Threat Emulation capability prevents infections from undiscovered exploits zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network.

NEW QUESTION 45

- (Exam Topic 2)

Provide very wide coverage for all products and protocols, with noticeable performance impact.



How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

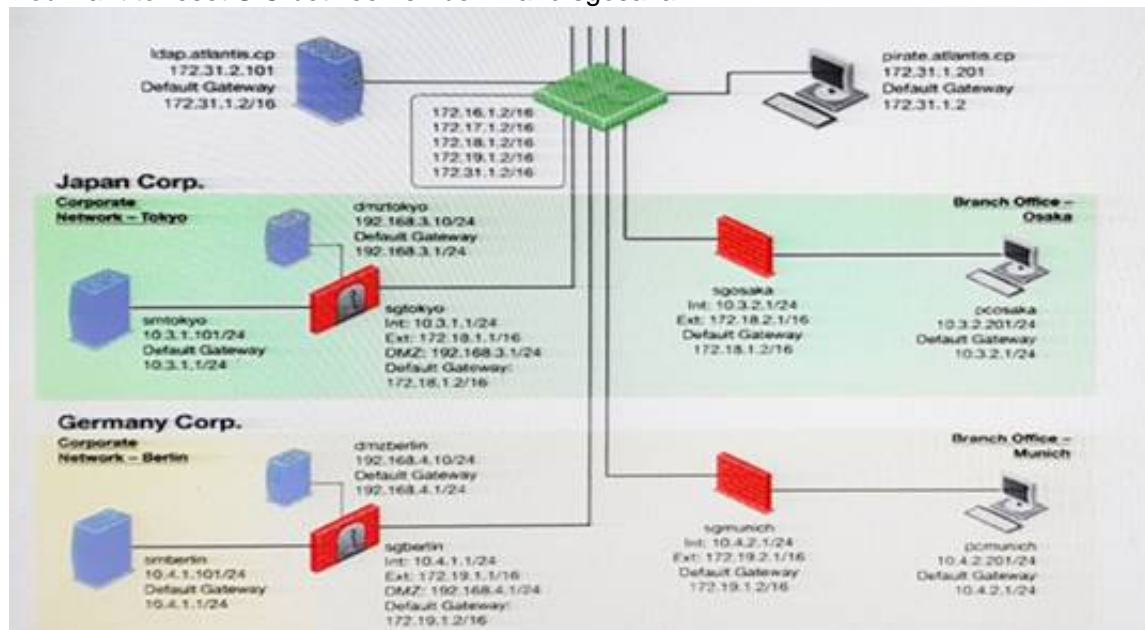
- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profil
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 46

- (Exam Topic 2)

You want to reset SIC between smberlin and sgosaka.



In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the menu. When trying to establish a connection, instead of a working connection, you receive this error message:



What is the reason for this behavior?

- A. The Gateway was not rebooted, which is necessary to change the SIC key.
- B. You must first initialize the Gateway object in SmartDashboard (i.e., right-click on the object, choose Basic Setup > Initialize).
- C. The check Point services on the Gateway were not restarted because you are still in the cpconfig utility.
- D. The activation key contains letters that are on different keys on localized keyboard
- E. Therefore, the activation can not be typed in a matching fashion.

Answer: C

NEW QUESTION 47

- (Exam Topic 2)

Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

- A. "Encrypt" action in the Rule Base
- B. Permanent Tunnels
- C. "VPN" column in the Rule Base
- D. Configuration checkbox "Accept all encrypted traffic"

Answer: A

Explanation:

Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:

- Simplified mode to all new Firewall Policies
- Traditional or Simplified per new Firewall Policy

2. Click OK.

3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.

4. Click New.

The New Policy window opens.

5. Give a name to the new policy and select Access Control.

In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

NEW QUESTION 48

- (Exam Topic 2)

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, Username, Password, Path, Comment, member

Answer: C

NEW QUESTION 53

- (Exam Topic 2)

Which of the following is NOT defined by an Access Role object?

- A. Source Network
- B. Source Machine
- C. Source User
- D. Source Server

Answer: D

NEW QUESTION 56

- (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 61

- (Exam Topic 2)

Where do we need to reset the SIC on a gateway object?

- A. SmartDashboard > Edit Gateway Object > General Properties > Communication
- B. SmartUpdate > Edit Security Management Server Object > SIC
- C. SmartUpdate > Edit Gateway Object > Communication
- D. SmartDashboard > Edit Security Management Server Object > SIC

Answer: A

NEW QUESTION 62

- (Exam Topic 2)

Which of the following is NOT a VPN routing option available in a star community?

- A. To satellites through center only
- B. To center, or through the center to other satellites, to Internet and other VPN targets
- C. To center and to other satellites through center
- D. To center only

Answer: A

Explanation:

SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

On the Star Community window, in the:

Center Gateways section, select the Security Gateway that functions as the "Hub".

Satellite Gateways section, select Security Gateways as the "spokes", or satellites.

On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:

To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.

To center, or through the center to other satellites, to internet and other VPN targets - This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.

Create an appropriate Access Control Policy rule.

NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

NEW QUESTION 66

- (Exam Topic 2)

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, gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP.

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 the 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. 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.
- 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.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

- A. John should install the identity Awareness Agent
- B. The firewall admin should install the Security Policy
- C. John should lock and unlock the computer
- D. Investigate this as a network connectivity issue

Answer: C

NEW QUESTION 68

- (Exam Topic 2)

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

- A. Pentagon
- B. Combined
- C. Meshed
- D. Star

Answer: D

Explanation:

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN connections between each Security Gateway. In a Star community, satellites have a VPN connection with the center Security Gateway, but not to each other.

NEW QUESTION 71

- (Exam Topic 2)

Fill in the blank: The ____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

- A. Application Control
- B. Data Awareness
- C. URL Filtering
- D. Threat Emulation

Answer: A

NEW QUESTION 72

- (Exam Topic 2)

Fill in the blanks: A Check Point software license consists of a _____ and _____.

- A. Software container; software package
- B. Software blade; software container
- C. Software package; signature
- D. Signature; software blade

Answer: B

Explanation:

Check Point's licensing is designed to be scalable and modular. To this end, Check Point offers both predefined packages as well as the ability to custom build a solution tailored to the needs of the Network Administrator. This is accomplished by the use of the following license components:

Software Blades
Container

NEW QUESTION 74

- (Exam Topic 2)

Fill in the blanks: A security Policy is created in _____, stored in the _____, and Distributed to the various _____.

- A. Rule base, Security Management Server, Security Gateways
- B. SmartConsole, Security Gateway, Security Management Servers
- C. SmartConsole, Security Management Server, Security Gateways
- D. The Check Point database, SmartConsole, Security Gateways

Answer: C

NEW QUESTION 75

- (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 77

- (Exam Topic 2)

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Answer: B

Explanation:

Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the R76 VPN Administration Guide.

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

NEW QUESTION 82

- (Exam Topic 2)

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

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering

Answer: B

Explanation:

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

NEW QUESTION 87

- (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 90

- (Exam Topic 2)

Choose what BEST describes users on Gaia Platform.

- A. There is one default user that cannot be deleted.
- B. There are two default users and one cannot be deleted.
- C. There is one default user that can be deleted.
- D. There are two default users that cannot be deleted and one SmartConsole Administrator.

Answer: B

Explanation:

These users are created by default and cannot be deleted:

admin — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.

monitor — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 93

- (Exam Topic 2)

Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____.

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 96

- (Exam Topic 2)

What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

- A. show interface (interface) –chain
- B. tcpdump
- C. tcpdump /snoop
- D. fw monitor

Answer: D

NEW QUESTION 98

- (Exam Topic 2)

In the R80 SmartConsole, on which tab are Permissions and Administrators defined?

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

Answer: C

NEW QUESTION 102

- (Exam Topic 2)

You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

- A. The POP3 rule is disabled.
- B. POP3 is accepted in Global Properties.
- C. The POP3 rule is hidden.
- D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Answer: C

NEW QUESTION 103

- (Exam Topic 2)

Which of the following licenses are considered temporary?

- A. Perpetual and Trial
- B. Plug-and-play and Evaluation
- C. Subscription and Perpetual
- D. Evaluation and Subscription

Answer: B

Explanation:

Should be Trial or Evaluation, even Plug-and-play (all are synonyms). Answer B is the best choice.

NEW QUESTION 107

- (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.

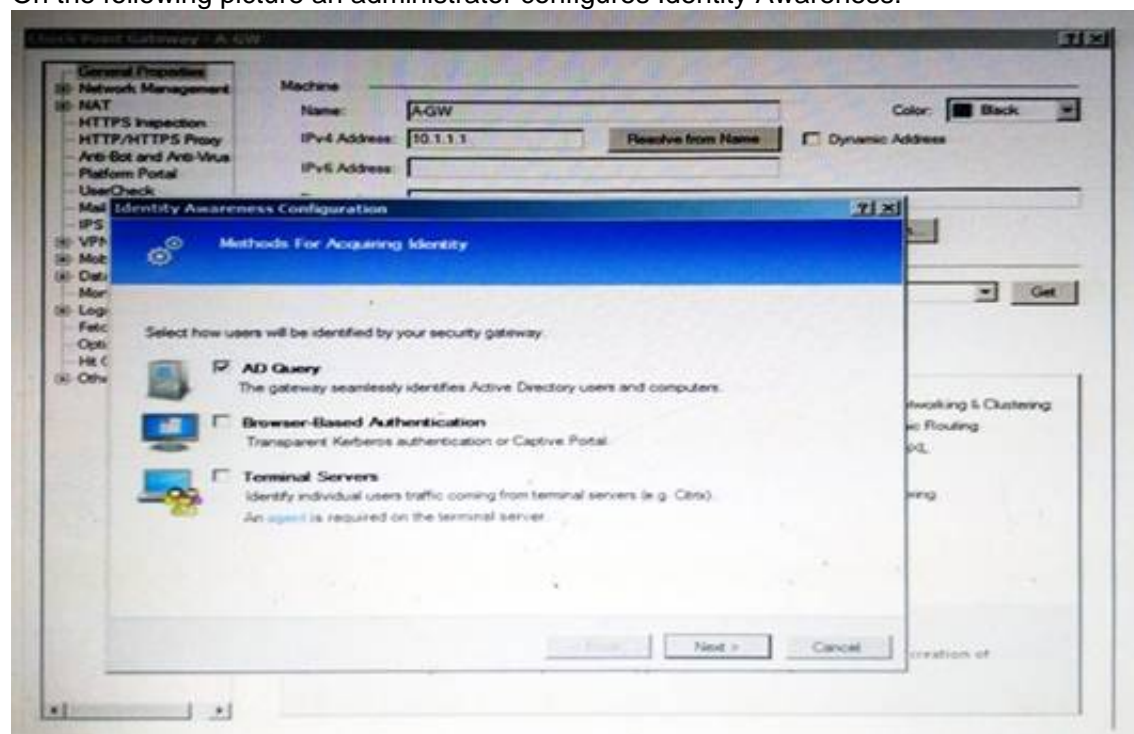
- A. Rule is locked by AdminA, because the save bottom has not been press.
- B. Rule is locked by AdminA, because an object on that rule is been edited.
- C. Rule is locked by AdminA, and will make it available if session is published.
- D. Rule is locked by AdminA, and if the session is saved, rule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

Answer: C

NEW QUESTION 112

- (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 116

- (Exam Topic 2)

How many users can have read/write access in Gaia at one time?

- A. Infinite

- B. One
- C. Three
- D. Two

Answer: B

NEW QUESTION 120

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

- A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
- B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
- C. IPSec VPN does not support two factor authentication, SSL VPN does support this
- D. IPSec VPN uses an additional virtual adapter, SSL VPN uses the client network adapter only

Answer: D

NEW QUESTION 124

- (Exam Topic 3)

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

- A. Interoperable Device
- B. Network Node
- C. Externally managed gateway
- D. Gateway

Answer: A

NEW QUESTION 126

- (Exam Topic 3)

Which rule is responsible for the user authentication failure?

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NET	drop	None
2	0	Management	webSingapore	fwSingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwSingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome net_singapore net_sydney	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic		Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

- A. Rule 4
- B. Rule 6
- C. Rule 3
- D. Rule 5

Answer: C

NEW QUESTION 131

- (Exam Topic 3)

Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:

- A. Create new dashboards to manage 3rd party task
- B. Create products that use and enhance 3rd party solutions
- C. Execute automated scripts to perform common tasks
- D. Create products that use and enhance the Check Point Solution

Answer: A

NEW QUESTION 136

- (Exam Topic 3)

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow from Trouble Ticket systems
- D. Logs and Events are synonyms

Answer: B

NEW QUESTION 140

- (Exam Topic 3)

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 142

- (Exam Topic 3)

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- A. Dropped without sending a negative acknowledgment
- B. Dropped without logs and without sending a negative acknowledgment
- C. Dropped with negative acknowledgment
- D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 147

- (Exam Topic 3)

Where does the security administrator activate Identity Awareness within SmartDashboard?

- A. Gateway Object > General Properties
- B. Security Management Server > Identity Awareness
- C. Policy > Global Properties > Identity Awareness
- D. LDAP Server Object > General Properties

Answer: A

NEW QUESTION 148

- (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 150

- (Exam Topic 3)

Where would an administrator enable Implied Rules logging?

- A. In Smart Log Rules View
- B. In SmartDashboard on each rule
- C. In Global Properties under Firewall
- D. In Global Properties under log and alert

Answer: B

NEW QUESTION 152

- (Exam Topic 3)

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

- A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- C. Using the remote Gateway's IP address, and applying the license locally with command cplic put.
- D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

Answer: B

NEW QUESTION 156

- (Exam Topic 3)

What port is used for communication to the User Center with SmartUpdate?

- A. CPMI 200
- B. TCP 8080
- C. HTTP 80
- D. HTTPS 443

Answer: D

NEW QUESTION 161

- (Exam Topic 3)

What is the benefit of Manual NAT over Automatic NAT?

- A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy
- B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
- C. You have the full control about the priority of the NAT rules
- D. On IPSO and GAIA Gateways, it is handled in a Stateful manner

Answer: C

NEW QUESTION 162

- (Exam Topic 3)

When defining QoS global properties, which option below is not valid?

- A. Weight
- B. Authenticated timeout
- C. Schedule
- D. Rate

Answer: C

NEW QUESTION 164

- (Exam Topic 3)

Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

- A. Source Address
- B. Destination Address
- C. TCP Acknowledgment Number
- D. Source Port

Answer: C

NEW QUESTION 168

- (Exam Topic 3)

What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

- A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging histor
- B. Use your normal log server for standard logging for troubleshooting.
- C. Install the View Implicit Rules package using SmartUpdate.
- D. Define two log servers on the R77 Gateway objec
- E. Lof Implied Rules on the first log serve
- F. Enable Log Rule Base on the second log serve
- G. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.
- H. Check the Log Implied Rules Globally box on the R77 Gateway object.

Answer: A

NEW QUESTION 170

- (Exam Topic 4)

To enforce the Security Policy correctly, a Security Gateway requires:

- A. a routing table
- B. awareness of the network topology
- C. a Demilitarized Zone
- D. a Security Policy install

Answer: B

Explanation:

The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

- Correctly enforce the Security Policy.
- Ensure the validity of IP addresses for inbound and outbound traffic.
- Configure a special domain for Virtual Private Networks.

NEW QUESTION 171

- (Exam Topic 4)

Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 173

- (Exam Topic 4)

Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

- A. ADQuery
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

Answer: D

NEW QUESTION 176

- (Exam Topic 4)

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 179

- (Exam Topic 4)

Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays ____ for the given VPN tunnel.

- A. Down
- B. No Response
- C. Inactive
- D. Failed

Answer: A

NEW QUESTION 181

- (Exam Topic 4)

Which message indicates IKE Phase 2 has completed successfully?

- A. Quick Mode Complete
- B. Aggressive Mode Complete
- C. Main Mode Complete
- D. IKE Mode Complete

Answer: A

NEW QUESTION 183

- (Exam Topic 4)

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 188

- (Exam Topic 4)

Which back up utility captures the most information and tends to create the largest archives?

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

Answer: B

NEW QUESTION 190

- (Exam Topic 4)

What Identity Agent allows packet tagging and computer authentication?

- A. Endpoint Security Client
- B. Full Agent
- C. Light Agent
- D. System Agent

Answer: B

NEW QUESTION 191

- (Exam Topic 4)

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
- D. Yes, but only one has the right to write

Answer: C

NEW QUESTION 196

- (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 199

- (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 204

- (Exam Topic 4)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell (clash)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 209

- (Exam Topic 4)

Which of the following is an authentication method used for Identity Awareness?

- A. SSL
- B. Captive Portal
- C. PKI
- D. RSA

Answer: B

NEW QUESTION 211

- (Exam Topic 4)

Which command shows the installed licenses?

- A. cplic print
- B. print cplic
- C. fwlic print
- D. show licenses

Answer: A

NEW QUESTION 216

- (Exam Topic 4)

Fill in the blanks. There are _____ types of software containers _____

- A. Three; security managemen

- B. Security Gateway and endpoint security.
- C. Three; Security Gateway, endpoint Security, and gateway management.
- D. Two; security management and endpoint security
- E. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 217

- (Exam Topic 4)

How many sessions can be opened on the Management Server at the same time?

- A. Unlimited, One per each licensed Gateway
- B. One
- C. Unlimited, Multiple per administrator
- D. Unlimited, One per administrator

Answer: D

NEW QUESTION 221

- (Exam Topic 4)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 223

- (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 225

- (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 226

- (Exam Topic 4)

What Check Point technologies deny or permit network traffic?

- A. Application Control DLP
- B. Packet Filtering, Stateful Inspection, Application Layer Firewall
- C. ACL SandBlast, MPT
- D. IPS, Mobile Threat Protection

Answer: B

NEW QUESTION 230

- (Exam Topic 4)

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats
- B. Proactively detects threats
- C. Delivers file with original content
- D. Delivers PDF versions of original files with active content removed

Answer: B

NEW QUESTION 231

- (Exam Topic 4)

Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

- A. The firewall topologies
- B. NAT Rules
- C. The Rule Base
- D. The VPN Domains

Answer: C

NEW QUESTION 232

- (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 236

- (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 238

- (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 240

- (Exam Topic 4)

What command would show the API server status?

- A. cpm status
- B. api restart
- C. api status
- D. show api status

Answer: D

NEW QUESTION 244

- (Exam Topic 4)

Which two Identity Awareness commands are used to support identity sharing?

- A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
- C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
- D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

Answer: A

NEW QUESTION 245

- (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 250

- (Exam Topic 4)

To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

- A. fw ctl set int fwha vmac global param enabled
- B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
- C. cphaprob -a if
- D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 253

.....

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