



Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

- A. vpn tu
- B. vpn ipsec remove -l
- C. vpn debug ipsec
- D. fw ipsec tu

Answer: A

Explanation:

vpn tu

Description Launch the TunnelUtil tool which is used to control VPN tunnels.

Usage vpn tu vpn tunnelutil Example vpn tu Output

NEW QUESTION 2

- (Exam Topic 1)

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS and Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

Explanation:

SandBlast Zero-Day Protection

Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day exploit protection from Check Point provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users.

NEW QUESTION 3

- (Exam Topic 1)

You have enabled "Full Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

Answer: A

Explanation:

The most likely reason for the logs data to stop is the low disk space on the logging device, which can be the Management Server or the Gateway Server.

NEW QUESTION 4

- (Exam Topic 1)

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

- A. SmartView Monitor
- B. SmartEvent
- C. SmartUpdate
- D. SmartDashboard

Answer: B

Explanation:

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

NEW QUESTION 5

- (Exam Topic 1)

What are the three essential components of the Check Point Security Management Architecture?

- A. SmartConsole, Security Management Server, Security Gateway
- B. SmartConsole, SmartUpdate, Security Gateway
- C. Security Management Server, Security Gateway, Command Line Interface

D. WebUI, SmartConsole, Security Gateway

Answer: A

Explanation:

Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.

Distributed deployment - Security Gateway and the Security Management server are installed on different machines.

Deployments

Basic deployments:

Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.

You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.

There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

NEW QUESTION 6

- (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 7

- (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 8

- (Exam Topic 1)

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

- A. UserCheck
- B. Active Directory Query
- C. Account Unit Query
- D. User Directory Query

Answer: B

Explanation:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 9

- (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 10

- (Exam Topic 1)

Which default user has full read/write access?

- A. Monitor
- B. Altuser
- C. Administrator
- D. Superuser

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiation

Answer: C

Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

NEW QUESTION 15

- (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 16

- (Exam Topic 1)

Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

- A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.

- B. On both firewalls, the same encryption is used for SI
- C. This is AES-GCM-256.
- D. The Firewall Administrator can choose which encryption suite will be used by SIC.
- E. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

Answer: A

Explanation:

Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

NEW QUESTION 21

- (Exam Topic 1)

Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?

- A. Machine Hide NAT
- B. Address Range Hide NAT
- C. Network Hide NAT
- D. Machine Static NAT

Answer: BC

Explanation:

SmartDashboard organizes the automatic NAT rules in this order:

Static NAT rules for Firewall, or node (computer or server) objects

Hide NAT rules for Firewall, or node objects

Static NAT rules for network or address range objects

Hide NAT rules for network or address range objects

References:

NEW QUESTION 24

- (Exam Topic 1)

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

Answer: B

Explanation:

The default shell of the CLI is called clish References:

NEW QUESTION 26

- (Exam Topic 1)

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

- A. Security questions
- B. Check Point password
- C. SecurID
- D. RADIUS

Answer: A

Explanation:

Authentication Schemes :- Check Point Password

- Operating System Password

- RADIUS

- SecurID

- TACAS

- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

NEW QUESTION 29

- (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 32

- (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 36

- (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 via CLI. Which command should be used 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 database
- 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 37

- (Exam Topic 1)

Choose what BEST describes the Policy Layer Traffic Inspection.

- A. If a packet does not match any of the inline layers, the matching continues to the next Layer.
- B. If a packet matches an inline layer, it will continue matching the next layer.
- C. If a packet does not match any of the inline layers, the packet will be matched against the Implicit Clean-up Rule.
- D. If a packet does not match a Network Policy Layer, the matching continues to its inline layer.

Answer: B

NEW QUESTION 38

- (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 42

- (Exam Topic 1)

Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

- A. NT domain
- B. SMTP
- C. LDAP
- D. SecurID

Answer: C

NEW QUESTION 43

- (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 46

- (Exam Topic 1)

What are the three authentication methods for SIC?

- A. Passwords, Users, and standards-based SSL for the creation of security channels
- B. Certificates, standards-based SSL for the creation of secure channels, and 3DES or AES128 for encryption
- C. Packet Filtering, certificates, and 3DES or AES128 for encryption
- D. Certificates, Passwords, and Tokens

Answer: B

Explanation:

Secure Internal Communication (SIC)

Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install polices on gateways and to send logs between gateways and management servers.

These security measures make sure of the safety of SIC:

Certificates for authentication

Standards-based SSL for the creation of the secure channel

3DES for encryption

References:

NEW QUESTION 47

- (Exam Topic 1)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

Explanation:

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a 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 Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

NEW QUESTION 48

- (Exam Topic 1)

Fill in the blank: The ____ is used to obtain identification and security information about network users.

- A. User Directory
- B. User server
- C. UserCheck
- D. User index

Answer: A

NEW QUESTION 49

- (Exam Topic 1)

Fill in the blanks: VPN gateways authenticate using _____ and _____.

- A. Passwords; tokens
- B. Certificates; pre-shared secrets
- C. Certificates; passwords
- D. Tokens; pre-shared secrets

Answer: B

Explanation:

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

NEW QUESTION 51

- (Exam Topic 1)

Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

- A. UDP
- B. TDP
- C. CCP
- D. HTTP

Answer: A

Explanation:

Parameters:

NEW QUESTION 53

- (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 54

- (Exam Topic 1)

In R80 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION 57

- (Exam Topic 1)

Packages and licenses are loaded from all of these sources EXCEPT

- A. Download Center Web site
- B. UserUpdate
- C. User Center
- D. Check Point DVD

Answer: B

Explanation:

the Download Center web site (packages)
the Check Point DVD (packages)
the User Center (licenses)
by importing a file (packages and licenses)
by running the cplic command line

Packages and licenses are loaded into these repositories from several sources: References:

NEW QUESTION 60

- (Exam Topic 1)

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

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

- 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 64

- (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 68

- (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 71

- (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 74

- (Exam Topic 1)

The security Gateway is installed on GAiA 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 75

- (Exam Topic 1)

With which command can you view the running configuration of Gaia-based system.

- A. show conf-active
- B. show configuration active
- C. show configuration
- D. show running-configuration

Answer: C

NEW QUESTION 80

- (Exam Topic 1)

What are the three conflict resolution rules in the Threat Prevention Policy Layers?

- A. Conflict on action, conflict on exception, and conflict on settings
- B. Conflict on scope, conflict on settings, and conflict on exception
- C. Conflict on settings, conflict on address, and conflict on exception
- D. Conflict on action, conflict on destination, and conflict on settings

Answer: C

NEW QUESTION 83

- (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

NEW QUESTION 85

- (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 88

- (Exam Topic 1)

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

Answer: C

Explanation:

It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

NEW QUESTION 91

- (Exam Topic 1)

Which feature is NOT provided by all Check Point Mobile Access solutions?

- A. Support for IPv6
- B. Granular access control

- C. Strong user authentication
- D. Secure connectivity

Answer: A

Explanation:

Types of Solutions

Enterprise-grade, secure connectivity to corporate resources.

Strong user authentication.

Granular access control. References:

NEW QUESTION 96

- (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:

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 100

- (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 102

- (Exam Topic 1)

What are the two types of address translation rules?

- A. Translated packet and untranslated packet
- B. Untranslated packet and manipulated packet
- C. Manipulated packet and original packet
- D. Original packet and translated packet

Answer: D

Explanation:

NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

Original Packet

Translated Packet References:

NEW QUESTION 106

- (Exam Topic 1)

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.

Where can the administrator check for more information on these errors?

- A. The Log and Monitor section in SmartConsole
- B. The Validations section in SmartConsole
- C. The Objects section in SmartConsole
- D. The Policies section in SmartConsole

Answer: B

Explanation:

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

NEW QUESTION 109

- (Exam Topic 1)

In which deployment is the security management server and Security Gateway installed on the same appliance?

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

Answer: C

Explanation:

Installing Standalone

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

NEW QUESTION 111

- (Exam Topic 1)

Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What as an 'Open Server'?

- A. Check Point software deployed on a non-Check Point appliance.
- B. The Open Server Consortium approved Server Hardware used for the purpose of Security and Availability.
- C. A check Point Management Server deployed using the Open Systems Interconnection (OSI) Server and Security deployment model.
- D. A check Point Management Server software using the Open SSL.

Answer: A

Explanation:

NEW QUESTION 112

- (Exam Topic 2)

What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

- A. degrades performance as the Security Policy grows in size
- B. requires additional Check Point appliances
- C. requires additional software subscription
- D. increases cost

Answer: A

NEW QUESTION 115

- (Exam Topic 2)

Mesh and Star are two types of VPN topologies. Which statement below is TRUE about these types of communities?

- A. A star community requires Check Point gateways, as it is a Check Point proprietary technology.
- B. In a star community, satellite gateways cannot communicate with each other.
- C. In a mesh community, member gateways cannot communicate directly with each other.
- D. In a mesh community, all members can create a tunnel with any other member.

Answer: D

NEW QUESTION 116

- (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 120

- (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 125

- (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 126

- (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 130

- (Exam Topic 2)

Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

- A. Accept; redirect
- B. Accept; drop
- C. Redirect; drop
- D. Drop; accept

Answer: D

NEW QUESTION 133

- (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 137

- (Exam Topic 2)

Why would an administrator see the message below?

- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 141

- (Exam Topic 2)

Fill in the blank: A _____ is used by a VPN gateway to send traffic as if it were a physical interface.

- A. VPN Tunnel Interface
- B. VPN community

- C. VPN router
- D. VPN interface

Answer: A

Explanation:

Route Based VPN

VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

NEW QUESTION 144

- (Exam Topic 2)

Which of these components does NOT require a Security Gateway R77 license?

- A. Security Management Server
- B. Check Point Gateway
- C. SmartConsole
- D. SmartUpdate upgrading/patching

Answer: C

NEW QUESTION 149

- (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 153

- (Exam Topic 2)

MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server. What can you do in this case?

- A. Use manual NAT rule to make an exception
- B. Use the NAT settings in the Global Properties
- C. Disable NAT inside the VPN community
- D. Use network exception in the Alpha-internal network object

Answer: D

NEW QUESTION 157

- (Exam Topic 2)

Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

- A. Firewall drop
- B. Explicit
- C. Implicit accept
- D. Implicit drop
- E. Implied

Answer: E

Explanation:

This is the order that rules are enforced:

First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.

Explicit Rules: These are rules that you create.

Before Last Implied Rules: These implied rules are applied before the last explicit rule.

Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.

Last Implied Rules: Implied rules that are configured as Last in Global Properties.

Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 162

- (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 165

- (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 166

- (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 171

- (Exam Topic 2)

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Firewall
- B. Application Control
- C. Anti-spam and Email Security
- D. Antivirus

Answer: D

Explanation:

The enhanced Check Point Antivirus Software Blade uses real-time virus signatures and anomaly-based protections from ThreatCloud™, the first collaborative network to fight cybercrime, to detect and block malware at the gateway before users are affected.

NEW QUESTION 173

- (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 175

- (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 180

- (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 183

- (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 188

- (Exam Topic 2)

Which policy type is used to enforce bandwidth and traffic control rules?

- A. Threat Emulation
- B. Access Control
- C. QoS
- D. Threat Prevention

Answer: C

Explanation:

Check Point's QoS Solution

QoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software.

NEW QUESTION 193

- (Exam Topic 2)

Which SmartConsole component can Administrators use to track changes to the Rule Base?

- A. WebUI
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartReporter

Answer: B

NEW QUESTION 196

- (Exam Topic 2)

Look at the screenshot below. What CLISH command provides this output?

- A. show configuration all
- B. show confd configuration
- C. show confd configuration all
- D. show configuration

Answer: D

NEW QUESTION 197

- (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 198

- (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 199

- (Exam Topic 2)

What happens if the identity of a user is known?

- A. If the user credentials do not match an Access Role, the system displays the Captive Portal.
- 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 traffic is automatically dropped.
- D. If the user credentials match an Access Role, the rule is applied and traffic is accepted or dropped based on the defined action.

Answer: D

NEW QUESTION 201

- (Exam Topic 2)

NAT can NOT be configured on which of the following objects?

- A. HTTP Logical Server
- B. Gateway
- C. Address Range
- D. Host

Answer: A

NEW QUESTION 202

- (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 203

- (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 206

- (Exam Topic 2)

Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

Answer: B

Explanation:

Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

NEW QUESTION 211

- (Exam Topic 2)

The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

- A. R80 Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- B. R80 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- C. R80 Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R80.
- D. R80 Management cannot manage earlier versions of Check Point Gateways prior to R80. Only R80 and above Gateways can be manage
- E. Consult the R80 Release Notes for more information.

Answer: A

NEW QUESTION 213

- (Exam Topic 2)

The most important part of a site-to-site VPN deployment is the _____.

- A. Internet
- B. Remote users
- C. Encrypted VPN tunnel
- D. VPN gateways

Answer: C

Explanation:

Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

NEW QUESTION 217

- (Exam Topic 2)

Which information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes
- B. application information
- C. destination port
- D. data type information

Answer: D

Explanation:

Network Log - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.

Log - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.

Full Log - Equivalent to the log option, but also records data for each URL request made.

If suppression is not selected, it generates a complete log (as defined in pre-R80 management).

If suppression is selected, it generates an extended log(as defined in pre-R80 management).

None - Do not generate a log.

NEW QUESTION 219

- (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 222

- (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 226

- (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 229

- (Exam Topic 2)

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

- A. Phase two key negotiation
- B. Address translation
- C. Log Consolidation Engine
- D. User data base corruption

Answer: B

NEW QUESTION 232

- (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 237

- (Exam Topic 2)

Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

- A. Shared policy packages
- B. Shared policies
- C. Concurrent policy packages
- D. Concurrent policies

Answer: A

NEW QUESTION 239

- (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 243

- (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 246

- (Exam Topic 3)

Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

- A. Change the Rule Base and install the Policy to all Security Gateways
- B. Block Intruder feature of SmartView Tracker
- C. Intrusion Detection System (IDS) Policy install
- D. SAM – Suspicious Activity Rules feature of SmartView Monitor

Answer: B

NEW QUESTION 247

- (Exam Topic 3)

What is the mechanism behind Threat Extraction?

- A. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
- B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient
- C. This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring).
- D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast

Answer: D

NEW QUESTION 251

- (Exam Topic 3)

As you review this Security Policy, what changes could you make to accommodate Rule 4?

- A. Remove the service HTTP from the column Service in Rule 4.
- B. Modify the column VPN in Rule 2 to limit access to specific traffic.
- C. Nothing at all
- D. Modify the columns Source or Destination in Rule 4

Answer: B

NEW QUESTION 255

- (Exam Topic 3)

Which is the correct order of a log flow processed by SmartEvent components:

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 257

- (Exam Topic 3)

Where do you verify that UserDirectory is enabled?

- A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
- B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked.
- C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.
- D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.

Answer: D

NEW QUESTION 259

- (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 263

- (Exam Topic 3)

Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is BEST to accomplish this task?

- A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port
- B. Then, export the corresponding entries to a separate log file for documentation.
- C. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocol
- D. Apply the alert action or customized messaging.
- E. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.
- F. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Answer: A

NEW QUESTION 265

- (Exam Topic 3)

Which of the below is the MOST correct process to reset SIC from SmartDashboard?

- A. Run cpconfig, and click Reset.
- B. Click the Communication button for the firewall object, then click Reset
- C. Run cpconfig on the gateway and type a new activation key.
- D. Run cpconfig, and select Secure Internal Communication > Change One Time Password.
- E. Click Communication > Reset on the Gateway object, and type a new activation key.

Answer: B

NEW QUESTION 268

- (Exam Topic 3)

Choose the correct statement regarding Implicit Rules.

- A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
- B. Implied rules are fixed rules that you cannot change.
- C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
- D. You can edit the Implicit rules but only if requested by Check Point support personnel.

Answer: A

NEW QUESTION 272

- (Exam Topic 3)

How many packets does the IKE exchange use for Phase 1 Main Mode?

- A. 12
- B. 1
- C. 3
- D. 6

Answer: D

NEW QUESTION 275

- (Exam Topic 3)

What is also referred to as Dynamic NAT?

- A. Automatic NAT
- B. Static NAT
- C. Manual NAT
- D. Hide NAT

Answer: D

NEW QUESTION 276

- (Exam Topic 3)

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

- A. There is a virus found
- B. Traffic is still allowed but not accelerated
- C. The connection required a Security server
- D. Acceleration is not enabled
- E. The traffic is originating from the gateway itself

Answer: D

NEW QUESTION 277

- (Exam Topic 3)

To fully enable Dynamic Dispatcher on a Security Gateway:

- A. run `fw ctl multik set_mode 9` in Expert mode and then reboot
- B. Using `cpconfig`, update the Dynamic Dispatcher value to “full” under the CoreXL menu
- C. Edit `/proc/interrupts` to include `multik set_mode 1` at the bottom of the file, save, and reboot
- D. run `fw ctl multik set_mode 1` in Expert mode and then reboot

Answer: A

NEW QUESTION 281

- (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 283

- (Exam Topic 3)

Which command can you use to verify the number of active concurrent connections?

- A. `fw conn all`
- B. `fw ctl pst pstat`
- C. `show all connections`
- D. `show connections`

Answer: B

NEW QUESTION 287

- (Exam Topic 3)

Which of the following is NOT an option for internal network definition of Anti-spoofing?

- A. Specific – derived from a selected object
- B. Route-based – derived from gateway routing table
- C. Network defined by the interface IP and Net Mask

D. Not-defined

Answer: B

NEW QUESTION 292

- (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 294

- (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 296

- (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 300

- (Exam Topic 3)

Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

- A. Dynamic ID
- B. RADIUS
- C. Username and Password
- D. Certificate

Answer: A

NEW QUESTION 301

- (Exam Topic 3)

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

- A. Secure Internal Communications (SIC) not configured for the object.
- B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
- C. Anti-spoofing not configured on the interfaces on the Gateway object.
- D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B

NEW QUESTION 302

- (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 307

- (Exam Topic 3)

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the

following should you remember?

- A. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
- B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
- C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
- D. You can limit the authentication attempts in the User Properties' Authentication tab.

Answer: B

NEW QUESTION 310

- (Exam Topic 3)

As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this? Enable the Refreshable Timeout setting:

- A. in the user object's Authentication screen.
- B. in the Gateway object's Authentication screen.
- C. in the Limit tab of the Client Authentication Action Properties screen.
- D. in the Global Properties Authentication screen.

Answer: C

NEW QUESTION 312

- (Exam Topic 3)

On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

NEW QUESTION 313

- (Exam Topic 3)

You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

- A. Manual copies of the directory \$FWDIR/conf
- B. upgrade_export command
- C. Database Revision Control
- D. GAIa backup utilities

Answer: C

NEW QUESTION 314

- (Exam Topic 3)

There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console

Answer: C

NEW QUESTION 319

- (Exam Topic 3)

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

- A. Create a new logical-server object to represent your partner's CA
- B. Exchange exported CA keys and use them to create a new server object to represent your partner's Certificate Authority (CA)
- C. Manually import your partner's Certificate Revocation List.
- D. Manually import your partner's Access Control List.

Answer: B

NEW QUESTION 323

- (Exam Topic 3)

While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

- 1) Select Active Mode tab in SmartView Tracker.
- 2) Select Tools > Block Intruder.
- 3) Select Log Viewing tab in SmartView Tracker.
- 4) Set Blocking Timeout value to 60 minutes.
- 5) Highlight connection that should be blocked.

- A. 1, 2, 5, 4
- B. 3, 2, 5, 4
- C. 1, 5, 2, 4
- D. 3, 5, 2, 4

Answer: C

NEW QUESTION 324

- (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 327

- (Exam Topic 3)

Which one of the following is true about Threat Extraction?

- A. Always delivers a file to user
- B. Works on all MS Office, Executables, and PDF files
- C. Can take up to 3 minutes to complete
- D. Delivers file only if no threats found

Answer: B

NEW QUESTION 329

- (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 334

- (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 339

- (Exam Topic 3)

You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicion?

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

Answer: D

NEW QUESTION 342

- (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 345

- (Exam Topic 3)

Which NAT rules are prioritized first?

- A. Post-Automatic/Manual NAT rules
- B. Manual/Pre-Automatic NAT
- C. Automatic Hide NAT
- D. Automatic Static NAT

Answer: B

NEW QUESTION 350

- (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 351

- (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 356

- (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 361

- (Exam Topic 3)

When using GAIA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

- A. As expert user, issue these commands:# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
- B. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field(conf:(conns:(conn:hwaddr ("00:0C:29:12:34:56"))
- C. As expert user, issue the command:# IP link set eth0 addr 00:0C:29:12:34:56
- D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

NEW QUESTION 363

- (Exam Topic 3)

What are types of Check Point APIs available currently as part of R80.10 code?

- A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
- B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
- C. OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API
- D. CPML API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 368

- (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 372

- (Exam Topic 3)

What happens when you run the command: fw sam -J src [Source IP Address]?

- A. Connections from the specified source are blocked without the need to change the Security Policy.
- B. Connections to the specified target are blocked without the need to change the Security Policy.
- C. Connections to and from the specified target are blocked without the need to change the Security Policy.
- D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Answer: A

NEW QUESTION 374

- (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 376

- (Exam Topic 3)

You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.

Unfortunately, you get the message:

“There are no machines that contain Firewall Blade and SmartView Monitor”.

What should you do to analyze the packet size distribution of your traffic? Give the BEST answer.

- A. Purchase the SmartView Monitor license for your Security Management Server.
- B. Enable Monitoring on your Security Management Server.
- C. Purchase the SmartView Monitor license for your Security Gateway.
- D. Enable Monitoring on your Security Gateway.

Answer: D

NEW QUESTION 377

- (Exam Topic 4)

What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

- A. S
- B. W
- C. C
- D. Space bar

Answer: B

NEW QUESTION 380

- (Exam Topic 4)

Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

- A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of this work.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom will have to reboot his SmartConsole computer, clear the cache and restore changes.

Answer: A

NEW QUESTION 384

- (Exam Topic 4)

The CDT utility supports which of the following?

- A. Major version upgrades to R77.30
- B. Only Jumbo HFA's and hotfixes
- C. Only major version upgrades to R80.10
- D. All upgrades

Answer: D

NEW QUESTION 388

- (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 391

- (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 392

- (Exam Topic 4)

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

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

Answer: A

NEW QUESTION 396

- (Exam Topic 4)

What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?

- A. A host route to route to the destination IP
- B. Use the file local.arp to add the ARP entries for NAT to work
- C. Nothing, the Gateway takes care of all details necessary
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

NEW QUESTION 399

- (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 400

- (Exam Topic 4)

What does it mean if Deyra sees the gateway status

Choose the BEST answer.

- A. SmartCenter Server cannot reach this Security Gateway
- B. There is a blade reporting a problem
- C. VPN software blade is reporting a malfunction
- D. Security Gateway s MGNT NIC card is disconnected

Answer: A

NEW QUESTION 403

- (Exam Topic 4)

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R80 configuration, clean install R80.10 and import the configuration
- B. CPUSE online upgrade
- C. CPUSE offline upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 408

- (Exam Topic 4)

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

Answer: C

NEW QUESTION 412

- (Exam Topic 4)

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Answer: B

NEW QUESTION 417

- (Exam Topic 4)

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 420

- (Exam Topic 4)

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

- A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
- B. Windows registry is available for future Security Management Server authentications.
- C. there is no memory used for saving a fingerprint anyway.
- D. SmartConsole cache is available for future Security Management Server authentications.

Answer: D

NEW QUESTION 425

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for ____ .

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

Answer: A

NEW QUESTION 426

- (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 428

- (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 429

- (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 433

- (Exam Topic 4)

Fill in the blank: In Security Gateways R75 and above, SIC uses ____ for encryption.

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

Answer: A

NEW QUESTION 438

- (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 441

- (Exam Topic 4)

The SIC Status “Unknown” means

- A. There is connection between the gateway and Security Management Server but it is not trusted.
- B. The secure communication is established.

- C. There is no connection between the gateway and Security Management Server.
- D. The Security Management Server can contact the gateway, but cannot establish SIC.

Answer: C
Explanation: SIC Status

Explanation:

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:
Communicating - The secure communication is established.
Unknown - There is no connection between the gateway and Security Management Server.
Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

NEW QUESTION 445

- (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 Setting
- D. Security Policies

Answer: B

NEW QUESTION 449

- (Exam Topic 4)

How would you determine the software version from the CLI?

- A. fw ver
- B. fw stat
- C. fw monitor
- D. cpinfo

Answer: A

NEW QUESTION 452

- (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 456

- (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 461

- (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 465

- (Exam Topic 4)

SmartEvent does NOT use which of the following procedures to identify 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 466

- (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 471

- (Exam Topic 4)

Fill in the blank: To create policy for traffic to or from a particular location, use the_____ .

- A. DLP shared policy
- B. Geo policy shared policy
- C. Mobile Access software blade
- D. HTTPS inspection

Answer: B

Explanation:

Shared Policies

The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. T are shared between all Policy packages.

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. References:

NEW QUESTION 472

- (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 474

- (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 476

- (Exam Topic 4)

When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

- A. Reflected immediately for all users who are using template.
- B. Not reflected for any users unless the local user template is changed.
- C. Reflected for all users who are using that template and if the local user template is changed as well.
- D. Not reflected for any users who are using that template.

Answer: A

Explanation:

The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local.

You can change the User Directory templates. Users

associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 478

- (Exam Topic 4)

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

Answer: B

NEW QUESTION 479

- (Exam Topic 4)

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

- A. Three; security management
- 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 481

- (Exam Topic 4)

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge

Answer: A

NEW QUESTION 485

- (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 multik pq enable

Answer: C

NEW QUESTION 486

- (Exam Topic 4)

You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore_backup
- B. import backup
- C. cp_merge
- D. migrate import

Answer: A

NEW QUESTION 490

- (Exam Topic 4)

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

Answer: D

NEW QUESTION 492

- (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 493

- (Exam Topic 4)

When an encrypted packet is decrypted, where does this happen?

- A. Security policy
- B. Inbound chain
- C. Outbound chain
- D. Decryption is not supported

Answer: A

NEW QUESTION 494

- (Exam Topic 4)

Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

- A. All options stop Check Point processes
- B. backup
- C. migrate export
- D. snapshot

Answer: D

NEW QUESTION 498

- (Exam Topic 4)

Choose what BEST describes the reason why querying logs now is very fast.

- A. New Smart-1 appliances double the physical memory install
- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

Answer: B

NEW QUESTION 499

- (Exam Topic 4)

In the Check Point Security Management Architecture, which component(s) can store logs?

- A. SmartConsole
- B. Security Management Server and Security Gateway
- C. Security Management Server
- D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 504

- (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 507

- (Exam Topic 4)

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

- A. Security Gateway IP-address cannot be changed without re-establishing the trust
- B. The Security Gateway name cannot be changed in command line without re-establishing trust
- C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
- D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Answer: A

NEW QUESTION 508

- (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 509

- (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 514

- (Exam Topic 4)

Which GUI tool can be used to view and apply Check Point licenses?

- A. cpconfig
- B. Management Command Line
- C. SmartConsole
- D. SmartUpdate

Answer: D

Explanation:

SmartUpdate GUI is the recommended way of managing licenses. References:

NEW QUESTION 516

- (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 520

- (Exam Topic 4)

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

- A. AES-GCM-256
- B. AES-CBC-256
- C. AES-GCM-128

Answer: B

NEW QUESTION 521

- (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 524

- (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 526

- (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 528

- (Exam Topic 4)

How Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications
- C. Capsule Workspace can provide access to any application
- D. Capsule Connect provides Business data isolation
- E. Capsule Connect does not require an installed application at client

Answer: A

NEW QUESTION 530

.....

Relate Links

100% Pass Your 156-215.80 Exam with Exambible Prep Materials

<https://www.exambible.com/156-215.80-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>