

## CheckPoint.156-215.81.v2022-11-21.q106

<b>Exam Code:</b>	156-215.81
<b>Exam Name:</b>	Check Point Certified Security Administrator R81
<b>Certification Provider:</b>	CheckPoint
<b>Free Question Number:</b>	106
<b>Version:</b>	v2022-11-21
<b># of views:</b>	4155
<b># of Questions views:</b>	1060
<a href="https://www.freepdfdumps.com/CheckPoint.156-215.81.v2022-11-21.q106.html">https://www.freepdfdumps.com/CheckPoint.156-215.81.v2022-11-21.q106.html</a>	

### NEW QUESTION: 1

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

- A. Add a temporary rule using SmartDashboard and select hide rule.
- B. Use dbedit to script the addition of a rule directly into the Rule Bases\_5\_0.fws configuration file.
- C. Select Block intruder from the Tools menu in SmartView Tracker.
- D. Create a Suspicious Activity Rule in Smart Monitor.

**Answer: (SHOW ANSWER)**

### NEW QUESTION: 2

John is using Management HA. Which Smartcenter should be connected to for making changes?

- A. connect virtual IP of Smartcenter HA
- B. active Smartcenter
- C. secondary Smartcenter
- D. primary Smartcenter

**Answer: (SHOW ANSWER)**

### NEW QUESTION: 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 > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client

D. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 4**

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

**Answer:** D ([LEAVE A REPLY](#))

**NEW QUESTION: 5**

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

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

**Answer:** D ([LEAVE A REPLY](#))

**NEW QUESTION: 6**

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. 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.
- B. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
- C. You can limit the authentication attempts in the User Properties' Authentication tab.
- D. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.

**Answer:** A ([LEAVE A REPLY](#))

**NEW QUESTION: 7**

When should you generate new licenses?

- A. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
- B. After a device upgrade.

- C. Only when the license is upgraded.
- D. Before installing contract files.

**Answer: B (LEAVE A REPLY)**

#### **NEW QUESTION: 8**

How are the backups stored in Check Point appliances?

- A. Saved as\*.tar under /var/log/CPbackup/backups
- B. Saved as\*tgz under /var/CPbackup
- C. Saved as\*tar under /var/CPbackup
- D. Saved as\*tgz under /var/log/CPbackup/backups

**Answer: B (LEAVE A REPLY)**

Backup configurations are stored in: /var/CPbackup/backups/

#### **NEW QUESTION: 9**

In what way are SSL VPN and IPSec VPN different?

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

**Answer: B (LEAVE A REPLY)**

#### **NEW QUESTION: 10**

Choose the correct statement regarding Implicit Rules.

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

**Answer: (SHOW ANSWER)**

#### **NEW QUESTION: 11**

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. Fast Path
- C. Medium Path
- D. Accelerated Path

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 12**

You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

- A. backup
- B. logswitch
- C. Database Revision
- D. snapshot

**Answer: (SHOW ANSWER)**

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

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

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

**NEW QUESTION: 13**

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

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

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 14**

From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

- A. Add a static route
- B. Verify a Security Policy
- C. View Security Management GUI Clients
- D. Open a terminal shell

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 15**

How do you manage Gaia?

- A. Through CLI and WebUI
- B. Through SmartDashboard only
- C. Through CLI only
- D. Through CLI, WebUI, and SmartDashboard

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 16**

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X in standalone mode and setup MTA
- B. You can utilize only Check Point Cloud Services for this scenario
- C. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance
- D. Install appliance TE250X on SpanPort on LAN switch in MTA mode

**Answer: B (LEAVE A REPLY)**

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

#### **NEW QUESTION: 17**

Which of the following licenses are considered temporary?

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

**Answer: B (LEAVE A REPLY)**

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

#### **NEW QUESTION: 18**

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway.

How do you apply the license?

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 19**

What is the purpose of the CPCA process?

- A. Generating and modifying certificates
- B. Sending and receiving logs
- C. Communication between GUI clients and the SmartCenter server
- D. Monitoring the status of processes

**Answer: A ([LEAVE A REPLY](#))**

**NEW QUESTION: 20**

The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to "None"?

- A. Yes, it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway
- B. No, it will not work independently. Hit Count will be shown only for rules with Track options set as Log or alert
- C. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways
- D. No, it will not work independently because hit count requires all rules to be logged

**Answer: C ([LEAVE A REPLY](#))**

**NEW QUESTION: 21**

What command would show the API server status?

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

**Answer: C ([LEAVE A REPLY](#))**

**NEW QUESTION: 22**

Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

- A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish the policy.
- B. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish and install the policy.
- C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.

D. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 23**

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

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

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 24**

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. Enable Monitoring on your Security Gateway.
- D. Purchase the SmartView Monitor license for your Security Gateway.

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 25**

Which of the following is NOT an advantage to using multiple LDAP servers?

- A. You gain High Availability by replicating the same information on several servers
- B. Information on a user is hidden, yet distributed across several servers
- C. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- D. You achieve a faster access time by placing LDAP servers containing the database at remote sites

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 26**

Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is \_\_\_\_\_.

- A. Sent to the Security Administrator.
- B. Stored on the Security Management Server.
- C. Sent to the Internal Certificate Authority.

D. Stored on the Certificate Revocation List.

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 27**

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

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

**Answer: D** ([LEAVE A REPLY](#))

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

**NEW QUESTION: 28**

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

- A. Since they both are log in on different interfaces, they both will be able to make changes.
- B. If Joe tries to make changes, he won't, database will be locked.
- C. When Joe logs in, Bob will be log out automatically.
- D. Bob will be prompt that Joe logged in.

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 29**

Which information is included in the "Extended Log" tracking option, but is not included in the "Log" tracking option?

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

**Answer: C** ([LEAVE A REPLY](#))

**NEW QUESTION: 30**

Anti-Spoofing is typically set up on which object type?

- A. Host
- B. Security Gateway
- C. Security Management object
- D. Network

**Answer: B ([LEAVE A REPLY](#))**

**NEW QUESTION: 31**

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

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

**Answer: B ([LEAVE A REPLY](#))**

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (**414 Q&As Dumps, 30%OFF Special Discount: Freepdfdumps**)

**NEW QUESTION: 32**

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

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

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 33**

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

- A. Profiles
- B. Protections
- C. IPS Protections
- D. ThreatWiki

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 34**

Which of the following is a hash algorithm?

- A. IDEA

- B. DES
- C. MD5
- D. 3DES

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 35**

Fill in the blank: \_\_\_\_\_ is the Gaia command that turns the server off.

- A. shut-down
- B. exit
- C. halt
- D. sysdown

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 36**

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers?

- A. Anti-Malware
- B. IPS
- C. Anti-bot
- D. Anti-Spam

**Answer: C (LEAVE A REPLY)**

Anti-Bot

The Need for Anti-Bot

There are two emerging trends in today's threat landscape:

Both of these trends are driven by bot attacks.

A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

**NEW QUESTION: 37**

Which of the following is NOT a tracking option? (Select three)

- A. Network log
- B. Full log
- C. Log
- D. Partial log

**Answer: A,B,D (LEAVE A REPLY)**

**NEW QUESTION: 38**

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

- A. Gateway
- B. HTTP Logical Server

C. Address Range

D. Host

**Answer: B ([LEAVE A REPLY](#))**

#### **NEW QUESTION: 39**

Which of the following situations would not require a new license to be generated and installed?

A. The Security Gateway is upgraded.

B. The IP address of the Security Management or Security Gateway has changed.

C. The existing license expires.

D. The license is upgraded.

**Answer: ([SHOW ANSWER](#))**

#### **NEW QUESTION: 40**

What is also referred to as Dynamic NAT?

A. Manual NAT

B. Hide NAT

C. Automatic NAT

D. Static NAT

**Answer: ([SHOW ANSWER](#))**

#### **NEW QUESTION: 41**

What is the purpose of a Stealth Rule?

A. A rule used to hide a server's IP address from the outside world.

B. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

C. A rule that allows administrators to access SmartDashboard from any device.

D. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.

**Answer: ([SHOW ANSWER](#))**

#### **NEW QUESTION: 42**

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

A. Source Port

B. Source Address

C. Destination Address

D. TCP Acknowledgment Number

**Answer: D ([LEAVE A REPLY](#))**

#### **NEW QUESTION: 43**

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

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

**Answer: D (LEAVE A REPLY)**

#### **NEW QUESTION: 44**

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

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

**Answer: D (LEAVE A REPLY)**

#### **NEW QUESTION: 45**

You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

- A. Open SmartDashboard and review the logs tab
- B. Open SmartEvent to see why they are being blocked
- C. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.
- D. Open SmartLog and connect remotely to the wireless controller

**Answer: C (LEAVE A REPLY)**

#### **NEW QUESTION: 46**

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

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

**Answer: A (LEAVE A REPLY)**

Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

**NEW QUESTION: 47**

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

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

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 48**

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.

- A. There is no object on the database with that name or that IP address.
- B. Object does not have a NAT IP address.
- C. Search detailed is missing the subnet mask.
- D. There is no object on the database with that IP address.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 49**

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 (LEAVE A REPLY)**

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:

The LAN Settings window opens.

The settings for the Internet Explorer proxy server are configured.

If you chose to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

**NEW QUESTION: 50**

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Asymmetric routing
- B. Symmetric routing
- C. Anti-Spoofing
- D. Failovers

**Answer: D ([LEAVE A REPLY](#))**

**NEW QUESTION: 51**

Which key is created during Phase 2 of a site-to-site VPN?

- A. Diffie-Hellman Public Key
- B. Diffie-Hellman Private Key
- C. Pre-shared secret
- D. Symmetrical IPSec key

**Answer: D ([LEAVE A REPLY](#))**

**NEW QUESTION: 52**

Which of the following are types of VPN communities?

- A. Pentagon, star, and combination
- B. Meshed, star, and combination
- C. Star, octagon, and combination
- D. Combined and star

**Answer: B ([LEAVE A REPLY](#))**

**NEW QUESTION: 53**

Which firewall daemon is responsible for the FW CLI commands?

- A. cpm
- B. fwd
- C. fwm
- D. cpd

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 54**

Identity Awareness allows the Security Administrator to configure network access based on which of the following?

- A. Name of the application, identity of the user, and identity of the machine
- B. Network location, identity of a user, and identity of a machine
- C. Identity of the machine, username, and certificate
- D. Browser-Based Authentication, identity of a user, and network location

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 55**

What Identity Agent allows packet tagging and computer authentication?

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

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 56**

Which of the following is used to initially create trust between a Gateway and Security Management Server?

- A. Internal Certificate Authority
- B. Token
- C. One-time Password
- D. Certificate

**Answer: C (LEAVE A REPLY)**

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

**NEW QUESTION: 57**

What is the appropriate default Gaia Portal address?

- A. HTTPS://[IPADDRESS]
- B. HTTPS://[IPADDRESS]:8080
- C. HTTPS://[IPADDRESS]:4434
- D. HTTP://[IPADDRESS]

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 58**

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: B (LEAVE A REPLY)**

**NEW QUESTION: 59**

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 (LEAVE A REPLY)**

These users are created by default and cannot be deleted:

#### **NEW QUESTION: 60**

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

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

**Answer: C (LEAVE A REPLY)**

#### **NEW QUESTION: 61**

Which back up method uses the command line to create an image of the OS?

- A. System backup
- B. Save Configuration
- C. snapshot
- D. Migrate

**Answer: C (LEAVE A REPLY)**

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

#### **NEW QUESTION: 62**

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

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 63**

Which rule is responsible for the user authentication failure?

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

**Answer: (**[SHOW ANSWER](#)**)**

**NEW QUESTION: 64**

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

**Answer: A (**[LEAVE A REPLY](#)**)**

**NEW QUESTION: 65**

Which of the following is considered to be the more secure and preferred VPN authentication method?

- A. Pre-shared secret
- B. Certificate
- C. MD5
- D. Password

**Answer: B (**[LEAVE A REPLY](#)**)**

**NEW QUESTION: 66**

What is the difference between an event and a log?

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

**Answer: A (**[LEAVE A REPLY](#)**)**

**NEW QUESTION: 67**

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

**Answer: B (**[LEAVE A REPLY](#)**)**

In Action, select:

**NEW QUESTION: 68**

You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

- A. Open SmartView Tracker and filter the logs for the IP address of the tablet
- B. Open SmartView Tracker and check all the IP logs for the tablet
- C. Open SmartLog and query for the IP address of the Manager's tablet
- D. Open SmartLog and connect remotely to the IP of the wireless controller

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 69**

What SmartEvent component creates events?

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

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 70**

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. Package Repository and Licenses
- B. License & Contract and Package Repository
- C. Update and License & Contract
- D. License and Update

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 71**

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

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

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 72**

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:** ([SHOW ANSWER](#))

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: 73**

Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

- A. Blue > set backup local
- B. Blue > add local backup
- C. Expert&Blue#add local backing
- D. Blue > add backup local

**Answer:** ([SHOW ANSWER](#))

### **NEW QUESTION: 74**

The Captive Portal tool:

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

**Answer:** ([SHOW ANSWER](#))

### **NEW QUESTION: 75**

Which message indicates IKE Phase 2 has completed successfully?

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

**Answer:** A ([LEAVE A REPLY](#))

### **NEW QUESTION: 76**

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories.

Which of the following is NOT an objects category?

- A. Network Object
- B. Limit
- C. Resource
- D. Custom Application / Site

**Answer: C (LEAVE A REPLY)**

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

#### **NEW QUESTION: 77**

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

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

**Answer: C (LEAVE A REPLY)**

#### **NEW QUESTION: 78**

Fill in the blank: Each cluster, at a minimum, should have at least \_\_\_\_\_ interfaces.

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

**Answer: C (LEAVE A REPLY)**

#### **NEW QUESTION: 79**

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

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

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 80**

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

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

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 81**

You want to verify if there are unsaved changes in GAIa that will be lost with a reboot. What command can be used?

- A. show unsaved
- B. show config-state
- C. show save-state
- D. show configuration diff

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 82**

Which component functions as the Internal Certificate Authority for R77?

- A. SmartLSM
- B. Policy Server
- C. Security Gateway
- D. Management Server

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 83**

How would you determine the software version from the CLI?

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

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 84**

Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

- A. Manage and Command Line
- B. Logs and Monitor
- C. Security Policies

D. Gateway and Servers

Answer: A ([LEAVE A REPLY](#))

**NEW QUESTION: 85**

Message digests use which of the following?

- A. SHA-1 and MD5
- B. DES and RC4
- C. IDEA and RC4
- D. SSL and MD4

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 86**

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

Answer: B ([LEAVE A REPLY](#))

**NEW QUESTION: 87**

Which of the following describes how Threat Extraction functions?

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

Answer: D ([LEAVE A REPLY](#))

**NEW QUESTION: 88**

Fill in the blank: Authentication rules are defined for \_\_\_\_\_.

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

Answer: ([SHOW ANSWER](#))

**NEW QUESTION: 89**

Where can administrator edit a list of trusted SmartConsole clients in R80?

- A.** In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients.
- B.** cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
- C.** Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- D.** WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients, via cpconfig on a Security Gateway.

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 90**

The default method for destination NAT is \_\_\_\_\_, where NAT occurs on the Inbound interface closest to the client.

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

**Answer:** **D** ([LEAVE A REPLY](#))

**NEW QUESTION: 91**

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

- A.** SmartLSM and SmartUpdate
- B.** SmartView Monitor and SmartUpdate
- C.** SmartDashboard and SmartView Tracker
- D.** SmartView Tracker and SmartView Monitor

**Answer:** **B** ([LEAVE A REPLY](#))

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have**

**been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

**NEW QUESTION: 92**

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

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

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 93**

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 (LEAVE A REPLY)**

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: 94**

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

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

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 95**

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

- A. Is only relevant when using SecureXL
- B. Is configured using cpconfig
- C. Can only be changed for Load Sharing implementations

D. All connections are processed and synchronized by the pivot

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 96**

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

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

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

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

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

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 97**

Why would an administrator see the message below?

- A. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- B. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- C. 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.
- D. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 98**

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the \_\_\_\_\_ algorithm.

- A. SHA-200
- B. SHA-128
- C. MD5
- D. SHA-256

**Answer: D ([LEAVE A REPLY](#))**

#### **NEW QUESTION: 99**

All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

- A. SMTP
- B. HTTP
- C. FTP
- D. RLOGIN

**Answer: ([SHOW ANSWER](#))**

#### **NEW QUESTION: 100**

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

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

**Answer: C ([LEAVE A REPLY](#))**

#### **NEW QUESTION: 101**

To view statistics on detected threats, which Threat Tool would an administrator use?

- A. Profiles
- B. IPS Protections
- C. Protections
- D. ThreatWiki

**Answer: D ([LEAVE A REPLY](#))**

#### **NEW QUESTION: 102**

What is the best sync method in the ClusterXL deployment?

- A. Use 1 dedicated sync interface
- B. Use 1 cluster + 1st sync
- C. Use 2 clusters + 1st sync + 2nd sync
- D. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 103**

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SecureClient
- C. SmartEvent
- D. SmartConsole

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 104**

Which type of attack can a firewall NOT prevent?

- A. Network Bandwidth Saturation
- B. SQL Injection
- C. Buffer Overflow
- D. SYN Flood

**Answer: ([SHOW ANSWER](#))**

**NEW QUESTION: 105**

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

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

**Answer: A ([LEAVE A REPLY](#))**

**NEW QUESTION: 106**

What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

- A. Automatic licensing
- B. Verification licensing
- C. Automatic licensing and Verification tool
- D. Verification tool

**Answer: ([SHOW ANSWER](#))**

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine

here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

**Valid 156-215.81 Dumps** shared by Actual4test.com for Helping Passing 156-215.81 Exam! Actual4test.com now offer the **newest 156-215.81 exam dumps**, the Actual4test.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 156-215.81 dumps with Test Engine here: [https://www.actual4test.com/156-215.81\\_examcollection.html](https://www.actual4test.com/156-215.81_examcollection.html) (414 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)