CheckPoint.156-215.81.v2024-07-09.q411

Exam Code:	156-215.81
Exam Name:	Check Point Certified Security Administrator R81
Certification Provider:	CheckPoint
Free Question Number:	411
Version:	v2024-07-09
# of views:	1776
# of Questions views:	4110
https://www.freeqas.com/qa/CheckPoint/156-215.81/CheckPoint.156-215.81.v2024-07-09.q411.html	

NEW QUESTION: 1
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. On the firewall object, Legacy Authentication screen, check "Enable Identity Captive Portal"
B. Right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"
C. In the Captive Portal screen of Global Properties, check "Enable Identity Captive Portal"
D. On the Security Management Server object, check the box "Identity Logging"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
What is a reason for manual creation of a NAT rule?
A. The public IP-address is different from the gateway's external IP
B. In R81 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
C. Network Address Translation is desired for some services, but not for others.
D. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
Answer: A (LEAVE A REPLY)

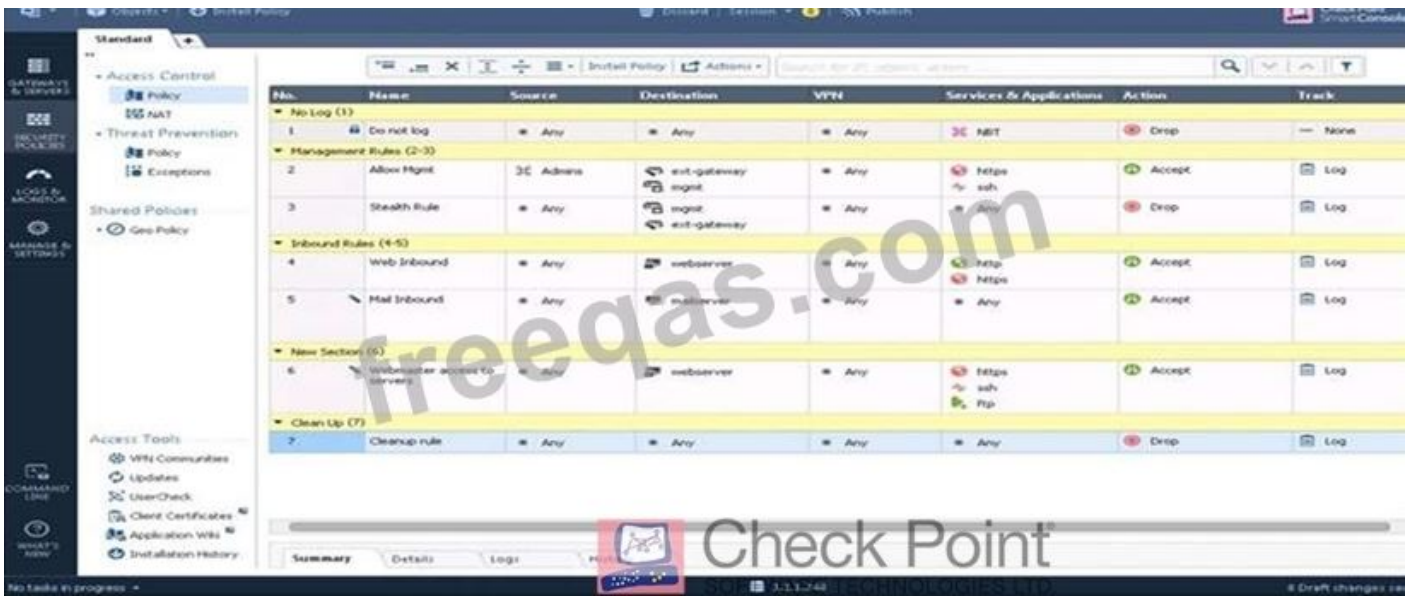
NEW QUESTION: 3
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?
A. Accounting
B. Suppression

C. Accounting/Suppression
D. Accounting/Extended
Answer: C (LEAVE A REPLY)
Explanation
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. You can add Accounting and/or Suppression to each of these options1. Accounting enables you to track the amount of data that is sent or received by a specific rule. Suppression enables you to reduce the number of logs that are generated by a specific rule. Therefore, the correct answer is C. Accounting/Suppression. References: Logging and Monitoring Administration Guide R80 - Check Point Software

NEW QUESTION: 4
Secure Internal Communication (SIC) is handled by what process?
A. CPM
B. HTTPS
C. FWD
D. CPD
Answer: D (LEAVE A REPLY)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

NEW QUESTION: 5
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?
A. ifconfig -a
B. show interfaces
C. show interfaces detail
D. show configuration interface
Answer: (SHOW ANSWER)
Explanation
The BEST command to view configuration details of all interfaces in Gaia CLISH is show configuration interface3. This command displays the interface name, IP address, netmask, state, MTU, and other parameters for each interface. ifconfig -a, show interfaces, and show interfaces detail are not valid commands in Gaia CLISH. References: How to configure static routes in CLISH on Gaia OS and IPSO OS, GAIA CLISH Commands - Fir3net, Gaia Administration Guide R80 - Check Point Software, Gaia Clish commands including User Defined (Extended) commands

NEW QUESTION: 6
Examine the sample Rule Base.



What will be the result of a verification of the policy from SmartConsole?

A. Verification Error. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)

B. No errors or Warnings

C. Verification Error. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

D. Verification Error. Empty Source-List in Rule 5 (Mail Inbound)

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

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

A. Accounting/Suppression

B. Accounting/Extended

C. Suppression

D. Accounting

Answer: A (LEAVE A REPLY)

NEW QUESTION: 8

What are two basic rules Check Point recommending for building an effective security policy?

A. Accept Rule and Drop Rule

B. Cleanup Rule and Stealth Rule

C. Explicit Rule and Implied Rule

D. NAT Rule and Reject Rule

Answer: B (LEAVE A REPLY)

Explanation

Two basic rules that Check Point recommends for building an effective security policy are Cleanup Rule and Stealth Rule. A Cleanup Rule is a rule that is placed at the end of the rule base and drops or logs any traffic that does not match any of the previous rules2. A Stealth Rule is a rule that is placed at the top of the rule base and protects the Security Gateway from direct access by unauthorized users3. The other options are not basic rules for building a security policy, but rather types or categories of rules.

NEW QUESTION: 9
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.
A. Concurrent policy packages
B. Concurrent policies
C. Global Policies
D. Shared policies
Answer: D (LEAVE A REPLY)
Explanation
The Shared policies feature allows administrators to share a policy with other policy packages3. This can save time and effort when managing multiple gateways with similar security requirements. Shared policies can be applied to Access Control, Threat Prevention, and HTTPS Inspection layers4. References: Check Point R81 Security Management Administration Guide, Check Point R81 SmartConsole R81 Resolved Issues

NEW QUESTION: 10
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.
A. MD5
B. SHA-128
C. SHA-200
D. SHA-256
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
What is the default tracking option of a rule?
A. Tracking
B. Log
C. None
D. Alert
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Tracking-Options.htm

NEW QUESTION: 12
There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A's interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?
A. No, since "maintain current active cluster member" option on the cluster object properties is enabled by default
B. No, since "maintain current active cluster member" option is enabled by default on the Global Properties
C. Yes, since "Switch to higher priority cluster member" option on the cluster object properties is enabled by default

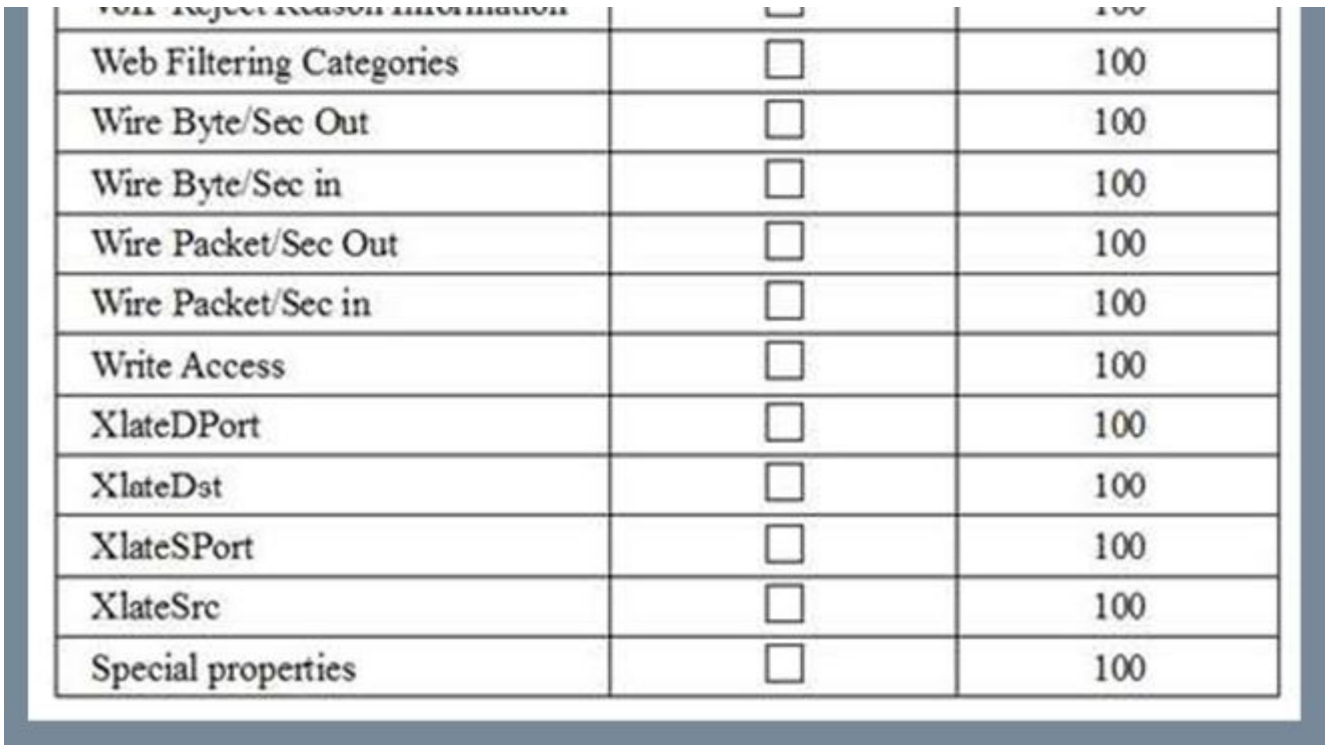
D. Yes, since "Switch to higher priority cluster member" option is enabled by default on the Global Properties
Answer: (SHOW ANSWER)
What Happens When a Security Gateway Recovers?
In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:
* Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
* Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

NEW QUESTION: 13
What is the purpose of the Stealth Rule?
A. To hide the gateway from the Internet.
B. To reduce the number of rules in the database.
C. To prevent users from directly connecting to a Security Gateway.
D. To reduce the amount of logs for performance issues.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?
A. The SmartLicensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.
D. The cpinfo command must be run on the firewall with the switch -online-license-activation.
Answer: C (LEAVE A REPLY)
"Online activation: this method of activation is available for Check Point manufactured appliances. These appliances should be configured to have internet connectivity during the completion of the First Time Configuration Wizard for software version R77 and below. Customers using R80 and higher will be able to use this feature during or after the completion of the First Time Configuration Wizard." https://supportcenter.checkpoint.com/supportcenter/portal?eventsubmit_dogoviewsolutiondetails=&solutionid=sk11054

NEW QUESTION: 15
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100



Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateDPort
B. XlateDst
C. XlateSrc
D. XlateSPort
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following is a new R81.10 Gateway feature that had not been available in R77.X and older?
A. Time object to a rule to make the rule active only during specified times.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.
D. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
To enforce the Security Policy correctly, a Security Gateway requires:

A. awareness of the network topology
B. a routing table
C. a Demilitarized Zone
D. a Security Policy install
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible explanation for this?
A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
B. Another administrator is logged into the Management and currently editing the DNS Rule.
C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.
Answer: B (LEAVE A REPLY)
Explanation
The padlock sign next to the DNS rule in the Rule Base indicates that another administrator is logged into the Management and currently editing the DNS Rule1. This is a feature of R80 that allows multiple administrators to work on the same policy simultaneously. The padlock sign prevents other administrators from modifying the same rule until the editing administrator publishes or discards the changes2. The other options are not valid explanations for the padlock sign. References: 156-215.80 : Check Point Certified Security Administrator (CCSA R80) : Part 19, Multi-User Policy Editing

NEW QUESTION: 19
When enabling tracking on a rule, what is the default option?
A. Extended Log
B. Log
C. Detailed Log
D. Accounting Log
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
What data MUST be supplied to the SmartConsole System Restore window to restore a backup?
A. Server, Protocol, Username, Password, Path
B. Username, Password, Path, Version

C. Server, Username, Password, Path, Version

D. Server, Protocol, Username, Password, Destination Path

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

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

A. Connections to and from the specified target are blocked without the need to change the Security Policy.

B. Connections from the specified source are blocked without the need to change the Security Policy.

C. Connections to 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: (SHOW ANSWER)

NEW QUESTION: 22

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 (LEAVE A REPLY)

Explanation

To ensure that VMAC mode is enabled, you should run the command fw ctl get int fwha_vmac_global_param_enabled on all cluster members and check that the result of the command returns the value 11. This command shows the current value of the global kernel parameter fwha_vmac_global_param_enabled, which controls whether VMAC mode is enabled or disabled. VMAC mode is a feature that associates a Virtual MAC address with each Virtual IP address of the cluster, which reduces the need for Gratuitous ARP packets and improves failover performance1. The other options are incorrect. Option A is not a valid command. Option C is a command to show the status of cluster interfaces, not VMAC mode2. Option D is a command to show the value of a different global kernel parameter, fwha_vmac_global_param_enabled, which controls whether VMAC mode is enabled for all interfaces or only for non-VLAN interfaces1. References: How to enable ClusterXL Virtual MAC (VMAC) mode, cphaprob

NEW QUESTION: 23

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: D (LEAVE A REPLY)

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: 24
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 (LEAVE A REPLY)
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: 25
Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?
A. Microsoft Publisher
B. JSON
C. Microsoft Word
D. RC4 Encryption
Answer: B (LEAVE A REPLY)
Explanation
The way that the objects can be manipulated using the new API integration in R80 Management is JSON.
JSON (JavaScript Object Notation) is a lightweight data-interchange format that is easy for humans and machines to read and write.
The R80 Management API uses JSON as the primary data format for requests and responses. Therefore, the correct answer is B. JSON.

NEW QUESTION: 26
Which is a suitable command to check whether Drop Templates are activated or not?
A. fw ctl get int activate_drop_templates
B. fwaccel stat
C. fw ctl templates -d
D. fwaccel stats
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following is NOT a tracking log option in R80.x?
A. Extended Log
B. Log
C. Detailed Log
D. Full Log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

Which rule is responsible for the user authentication failure?

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

A. Rule 3

B. Rule 4

C. Rule 5

D. Rule 6

Answer: A (LEAVE A REPLY)

NEW QUESTION: 29

Aggressive Mode in IKEv1 uses how many packages for negotiation?

A. 6

B. 3

C. depends on the make of the peer gateway

D. 5

Answer: B (LEAVE A REPLY)

Explanation

Aggressive Mode in IKEv1 uses three packets for negotiation, with all data required for the SA passed by the initiator1. The responder sends the proposal, key material, and ID, and authenticates the session in the next packet. The initiator replies and authenticates the session1.

The other answers are not correct because they either refer to the Main Mode in IKEv1, which uses six packets for negotiation2, or they are irrelevant to the number of packets used in Aggressive Mode.

* Understand IPsec IKEv1 Protocol - Cisco

* Negotiation modes for phase 1 - IBM

* FAQ-What are the differences between IKEv1 and IKEv2- Huawei

NEW QUESTION: 30

How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

A. Involved traffic logs will be forwarded to a log server.

B. Provides log details view email to the Administrator.

C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.

D. Provides additional information to the connected user.

Answer: (SHOW ANSWER)

Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Tracking-Options.htm

NEW QUESTION: 31
Core Protections are installed as part of what Policy?
A. Desktop Firewall Policy
B. Mobile Access Policy.
C. Threat Prevention Policy.
D. Access Control Policy.
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following is the most secure means of authentication?
A. Password
B. Certificate
C. Token
D. Pre-shared secret
Answer: (SHOW ANSWER)
Explanation
Certificate is the most secure means of authentication among the given options2. A certificate is a digital document that contains information about the identity of a user or a device, and is signed by a trusted authority. A certificate can be used to prove the identity of a user or a device without revealing any sensitive information, such as passwords or tokens. Password, token, and pre-shared secret are less secure means of authentication because they can be easily compromised, stolen, or guessed by attackers.
References: Secure User Authentication Methods - freeCodeCamp.org, What is the Most Secure Authentication Method for Your Organization ...

NEW QUESTION: 33
What are the two elements of address translation rules?
A. Original packet and translated packet
B. Manipulated packet and original packet
C. Translated packet and untranslated packet
D. Untranslated packet and manipulated packet
Answer: (SHOW ANSWER)

Explanation
Address translation rules are used to map an IP address space into another by modifying network address information in the IP header of packets. Address translation rules have two elements: original packet and translated packet6. The original packet is the packet before it undergoes address translation, and the translated packet is the packet after it undergoes address translation. The original packet and the translated packet may have different source and destination IP addresses, depending on the type and direction of address translation.

NEW QUESTION: 34
Which command is used to add users to or from existing roles?
A. add rba user <User Name> roles <List>
B. add user <User Name>
C. add rba user <User Name>
D. add user <User Name> roles <List>
Answer: A (LEAVE A REPLY)
Explanation
The command add rba user <User Name> roles <List> is used to add users to or from existing roles. RBA stands for Role-Based Administration, which is a feature that allows administrators to assign different permissions and access levels to users based on their roles2.
References: 2: Check Point R81 Security Management Administration Guide, page 20.

NEW QUESTION: 35
Can a Check Point gateway translate both source IP address and destination IP address in a given packet?
A. No.
B. Yes.
C. Yes, but only when using Automatic NAT.
D. Yes, but only when using Manual NAT.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
What is the default shell of Gaia CLI?
A. Monitor
B. Bash
C. Read-only
D. CLI.sh
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
To view statistics on detected threats, which Threat Tool would an administrator use?
A. ThreatWiki
B. IPS Protections
C. Protections
D. Profiles

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
What is the user ID of a user that have all the privileges of a root user?
A. User ID 99
B. User ID 2
C. User ID 1
D. User ID 0
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers?
A. Anti-bot
B. Anti-Malware
C. Anti-Spam
D. IPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40
You are asked to check the status of several user-mode processes on the management server and gateway.
Which of the following processes can only be seen on a Management Server?
A. fwm
B. cpwd
C. fwd
D. cpd
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
Name the utility that is used to block activities that appear to be suspicious.
A. Suspicious Activity Monitoring (SAM)
B. Drop Rule in the rulebase
C. Stealth rule
D. Penalty Box
Answer: (SHOW ANSWER)

NEW QUESTION: 42
What is the command to see cluster status in cli expert mode?
A. clusterXL status
B. clusterXL stat
C. cphaprob stat
D. fw ctl stat

Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
Which command shows the installed licenses in Expert mode?
A. print cplic
B. show licenses
C. fwlic print
D. cplic print
Answer: (SHOW ANSWER)
Explanation
The command that shows the installed licenses in Expert mode is cplic print. This command displays information about the licenses that are installed on the local machine or a remote machine1. The other commands are not valid for showing licenses in Expert mode.

NEW QUESTION: 44
Which statement is NOT TRUE about Delta synchronization?
A. Quicker than Full sync
B. Transfers changes in the Kernel tables between cluster members
C. Using UDP Multicast or Broadcast on port 8116
D. Using UDP Multicast or Broadcast on port 8161
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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 (LEAVE A REPLY)
Explanation
The components of Check Point Capsule are Capsule Docs, Capsule Cloud, and Capsule Workspace123.
There is no Capsule Enterprise component. Capsule Docs protects business documents everywhere they go.
Capsule Cloud protects mobile users outside the enterprise security perimeter. Capsule Workspace creates a secure business environment on mobile devices. References: Check Point Capsule Datasheet, Check Point Capsule Workspace Datasheet, Mobile Secure Workspace with Capsule

NEW QUESTION: 46
When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packer Filtering?
A. Stateful Inspection does not use memory to record the protocol used by the connection.
B. Stateful Inspection offers unlimited connections because of virtual memory usage.
C. Only one rule is required for each connection.
D. Stateful Inspection offers no benefits over Packet Filtering.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
In order to modify Security Policies the administrator can use which of the following tools? (Choose the best answer.)
A. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
B. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
C. SmartConsole and WebUI on the Security Management Server.
D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
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 (LEAVE A REPLY)
These are basic access control rules we recommend for all Rule Bases:
There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION: 49
What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?
A. Verification tool
B. Verification licensing
C. Automatic licensing and Verification tool
D. Automatic licensing
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Fill in the blanks: The Application Layer Firewalls inspect traffic through the _____ layer(s) of the TCP/IP model and up to and including the _____ layer.
A. Upper; Application
B. First two; Internet
C. Lower; Application

D. First two; Transport

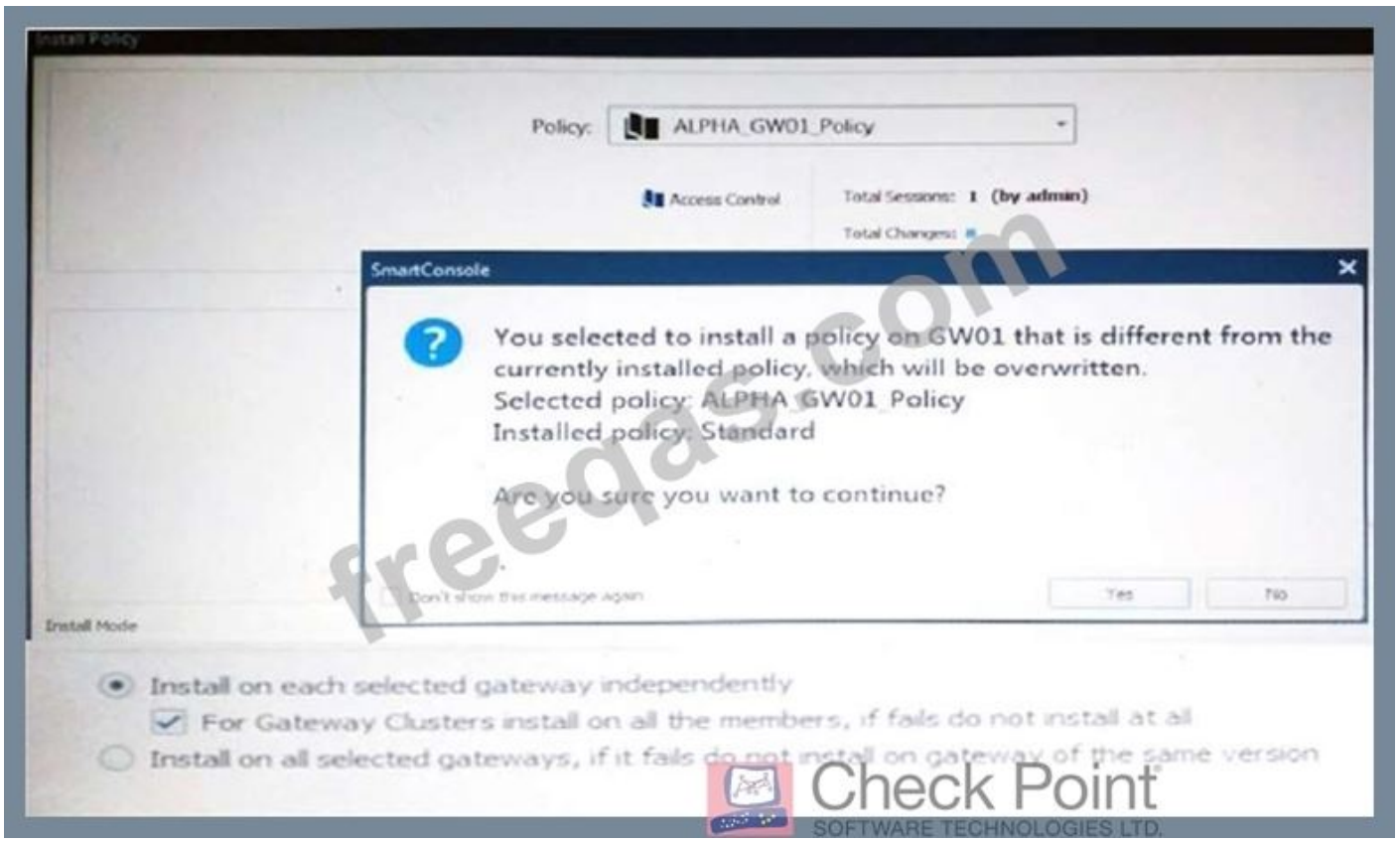
Answer: C (LEAVE A REPLY)

Explanation

The Application Layer Firewalls inspect traffic through the Lower layer(s) of the TCP/IP model and up to and including the Application layer. The lower layers are the Physical, Data Link, and Network layers, which deal with the transmission and routing of packets. The Application layer is the highest layer of the TCP/IP model, which provides services and protocols for specific applications such as HTTP, FTP, SMTP, etc. The Application Layer Firewalls can inspect the content and context of the traffic and enforce granular security policies based on various criteria such as user identity, application identity, content type, etc. References:
[Check Point R81 Firewall Administration Guide]

NEW QUESTION: 51

Why would an administrator see the message below?



A. A new Policy Package created on the Gateway is going to be installed on the existing Management.

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 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: (SHOW ANSWER)

NEW QUESTION: 52

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, Protocol, Username, Password, Path, Comment, All Members

C. Server, TFTP, Username, Password, Path, Comment, All Members

D. Server, Protocol, Username, Password, Path, Comment, Member

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53

Fill in the blank: In Office mode, a Security Gateway assigns a remote client to an IP address once_____.

A. the user connects and authenticates

B. office mode is initiated

C. the user connects

D. the user requests a connection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 54

What is the purpose of Captive Portal?

A. It manages user permission in SmartConsole

B. It provides remote access to SmartConsole

C. It authenticates users, allowing them access to the Internet and corporate resources

D. It authenticates users, allowing them access to the Gaia OS

Answer: C (LEAVE A REPLY)

Explanation

Captive Portal is a feature of Identity Awareness that allows you to authenticate users through a web browser before they access the Internet or corporate resources. Captive Portal can be used for various authentication methods, such as user name and password, one-time password (OTP), or certificate3. Captive Portal does not manage user permission in SmartConsole, provide remote access to SmartConsole, or authenticate users to the Gaia OS. Those are different functions that are not related to Captive Portal.

References: Check Point R81 Identity Awareness Administration Guide

NEW QUESTION: 55

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)

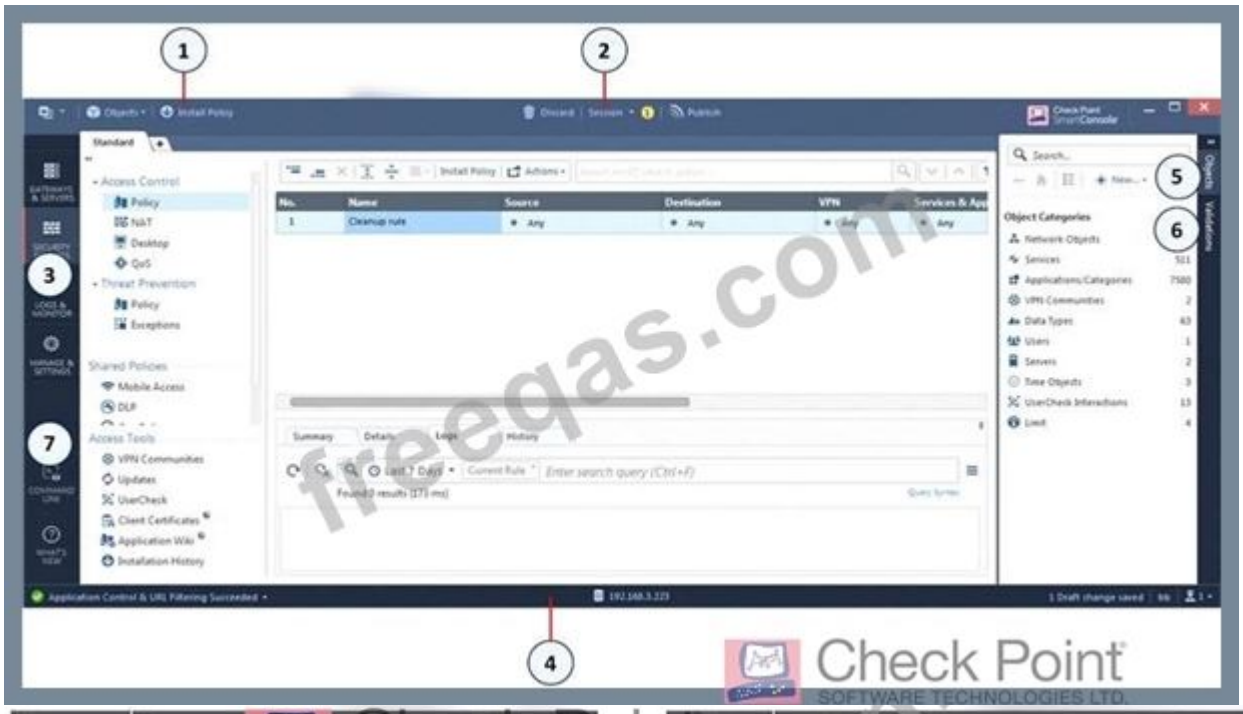
Explanation

Manage and Command Line is not a valid application navigation tab in the R80 SmartConsole, as it does not exist in the interface.

The image shows the navigation toolbar of the R80 SmartConsole, which has four tabs:

Security Policies, Logs & Monitor, Gateways & Servers, and Manage & Settings1. The Command Line Interface button is located in the system information area, not in the navigation toolbar1.

References: Application Control and URL Filtering - Check Point Software



Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

NEW QUESTION: 56
One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?
A. AdminB sees a pencil icon next the rule that AdminB is currently editing.
B. AdminA and AdminB are editing the same rule at the same time.
C. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
Which two of these Check Point Protocols are used by ?
A. FWD and CPLOG
B. FWD and LEA
C. ELA and CPD
D. ELA and CPLOG
Answer: (SHOW ANSWER)
NEW QUESTION: 58

A layer can support different combinations of blades What are the supported blades:
A. Firewall (Network Access Control). Application & URL Filtering and Content Awareness
B. Firewall (Network Access Control). Application & URL Filtering. Content Awareness and Mobile Access
C. Firewall. URLF, Content Awareness and Mobile Access
D. Firewall. NAT, Content Awareness and Mobile Access
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
What statement is true regarding Visitor Mode?
A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
B. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
C. All VPN traffic is tunneled through UDP port 4500.
D. Only ESP traffic is tunneled through port TCP 443.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
Log query results can be exported to what file format?
A. Text (txt)
B. Word Document (docx)
C. Comma Separated Value (csv)
D. Portable Document Format (pdf)
Answer: (SHOW ANSWER)

NEW QUESTION: 61
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: (SHOW ANSWER)
Explanation
Threat Extraction delivers PDF versions of original files with active content removed, such as macros, embedded objects, and scripts. This ensures that users receive clean and safe files in seconds12.
References: Check Point SandBlast Zero-Day Protection, Check Point Threat Extraction

NEW QUESTION: 62
Fill in the blank: Service blades must be attached to a _____.
A. Security Gateway
B. Management container
C. Management server
D. Security Gateway container
Answer: (SHOW ANSWER)
Explanation
Service blades must be attached to a Security Gateway. A Security Gateway is a device that enforces security policies on traffic that passes through it. A service blade is a software module that provides a specific security function, such as firewall, VPN, IPS, etc. A Security Gateway can have one or more service blades attached to it, depending on the license and hardware capabilities. The other options are incorrect. A management container is a virtualized environment that hosts a Security Management Server or a Log Server. A management server is a device that manages security policies and distributes them to Security Gateways. A Security Gateway container is not a valid term in Check Point terminology. References: [Check Point R81 Security Management Administration Guide], [Check Point R81 CloudGuard Administration Guide]

NEW QUESTION: 63
What is the RFC number that act as a best practice guide for NAT?
A. RFC 1939
B. RFC 1950
C. RFC 793
D. RFC 1918
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?
A. Detects and blocks malware by correlating multiple detection engines before users are affected.
B. Configure rules to limit the available network bandwidth for specified users or groups.
C. Use UserCheck to help users understand that certain websites are against the company's security policy.
D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A because detecting and blocking malware by correlating multiple detection engines before users are affected is not a feature of the Check Point URL Filtering and Application Control Blade3. This feature is part of the Check Point Anti-Virus and Anti-Bot Blades3. The other options are features of the Check Point URL Filtering and Application Control Blade3. References: Check Point R81 URL Filtering and Application Control Administration Guide

NEW QUESTION: 65

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

A. Active Directory Query

B. User Directory Query

C. Account Unit Query

D. UserCheck

Answer: (SHOW ANSWER)

Explanation

Active Directory Query is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers. Active Directory Query enables the Security Gateway to query the Active Directory Domain Controllers for user and computer information, such as IP addresses, group memberships, and login events.

References: : Check Point R81 Identity Awareness Administration Guide, page 14.

NEW QUESTION: 66

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

A. show interface (interface) -chain

B. tcpdump /snoop

C. fw monitor

D. tcpdump

Answer: C (LEAVE A REPLY)

NEW QUESTION: 67

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

A. The VPN Domains

B. The Rule Base

C. NAT Rules

D. The firewall topologies

Answer: (SHOW ANSWER)

NEW QUESTION: 68

Which encryption algorithm is the least secured?

A. 3DES

B. AES-128

C. DES

D. AES-256

Answer: (SHOW ANSWER)

Explanation

This answer is correct because DES (Data Encryption Standard) is the least secured encryption algorithm among the options given. DES uses a 56-bit key, which is too short and can be easily cracked by brute force attacks1. DES also suffers from other weaknesses, such as weak keys, complementation property, and linear cryptanalysis2.

The other answers are not correct because they are more secured encryption algorithms than DES. 3DES (Triple DES) is an

improvement over DES that applies DES three times with different keys, resulting in a
168-bit key3. AES-128 and AES-256 are variants of AES (Advanced Encryption Standard) that use 128-bit and 256-bit keys respectively. AES is considered to be the most secure symmetric encryption algorithm and is widely used for data protection.
* What is DES encryption, and why was it replaced?
* Data Encryption Standard - Wikipedia
* What is 3DES encryption?
* [What is AES encryption and how does it work?]

NEW QUESTION: 69
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?
A. At least 20GB
B. More than 10GB and less than 20 GB
C. Any size
D. Less than 20GB
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
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. Custom Application / Site
B. Resource
C. Limit
D. Network Object
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or_____.
A. On all satellite gateway to satellite gateway tunnels
B. On specific tunnels for specific gateways
C. On specific tunnels in the community
D. On specific satellite gateway to central gateway tunnels
Answer: C (LEAVE A REPLY)
Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:
NEW QUESTION: 72
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 and install the policy.

B. 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.

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 Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish the policy.

Answer: (SHOW ANSWER)

Explanation

The steps you will need to do in SmartConsole in order to get the connection working behind the Internet Security Gateway are:

* Define an accept rule in Security Policy. This rule allows the traffic from your internal networks to pass through the Security Gateway.

* Define automatic NAT for each network to NAT the networks behind a public IP. This option translates

* the private IP addresses of your internal networks to a public IP address assigned by your ISP router.

This way, your internal networks can communicate with the Internet using a valid IP address.

* Publish and install the policy. This step applies the changes you made to the Security Gateway and activates the security and NAT rules.

References: Check Point R81 Quantum Security Gateway Guide

NEW QUESTION: 73

What component of R81 Management is used for indexing?

A. API Server

B. fwm

C. SOLR

D. DBSync

Answer: C (LEAVE A REPLY)

NEW QUESTION: 74

What technologies are used to deny or permit network traffic?

A. Firewall Blade. URL/Application Blade and IPS

B. Packet Filtenng. Stateful Inspection, and Application Layer Firewall

C. Stateful Inspection. Firewall Blade, and URL'Application Blade

D. Stateful Inspection. URL/Application Blade, and Threat Prevention

Answer: C (LEAVE A REPLY)

NEW QUESTION: 75

In which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to a 2200 Appliance

B. From a 4400 Appliance to an HP Open Server
C. From an IBM Open Server to an HP Open Server
D. From an IBM Open Server to a 2200 Appliance
Answer: A (LEAVE A REPLY)
Explanation
The scenario where it is a valid option to transfer a license from one hardware device to another is from a 4400 Appliance to a 2200 Appliance. This is because both appliances are Check Point products and have the same license type (Central License). You can transfer a license from one hardware device to another if they have the same license type and vendor3. Therefore, the correct answer is A. From a 4400 Appliance to a 2200 Appliance.

NEW QUESTION: 76
From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?
A. Open a terminal shell
B. Verify a Security Policy
C. View Security Management GUI Clients
D. Add a static route
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n) _____ Server.
A. SecurID
B. LDAP
C. NT domain
D. SMTP
Answer: B (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/LDAP-and-User-Directory.htm

NEW QUESTION: 78
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 R81 security management?
A. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

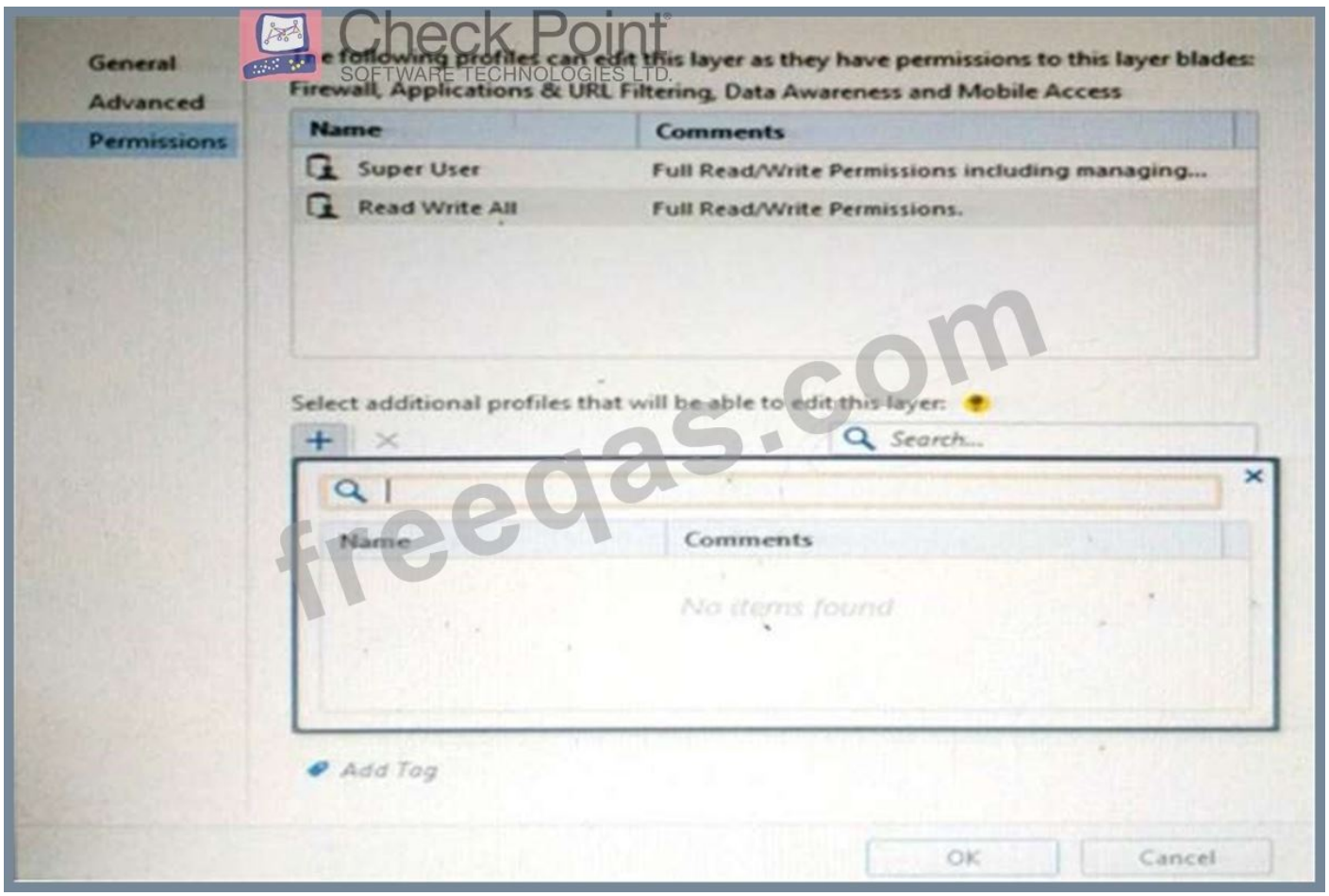
B. Create a text-file with DBEDIT script that creates all objects and policies. Run the file in the command line of the management server using command dbedit -f.
C. Create a text-file with mgmt_cli script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.
D. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command load configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
What action can be performed from SmartUpdate R77?
A. remote_uninstall_verifier
B. fw stat -1
C. upgrade_export
D. cpinfo
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
When using Automatic Hide NAT, what is enabled by default?
A. Source Port Address Translation (PAT)
B. Static NAT
C. Static Route
D. HTTPS Inspection
Answer: A (LEAVE A REPLY)
Explanation
When using Automatic Hide NAT, Source Port Address Translation (PAT) is enabled by default1. This means that the source IP address and port number are translated to a different IP address and port number. This allows multiple hosts to share a single IP address for outbound connections. References: Check Point R81 Firewall Administration Guide

NEW QUESTION: 81
How can the changes made by an administrator before publishing the session be seen by a superuser administrator?
A. They cannot be seen
B. From the SmartView Tracker audit log
C. From Manage and Settings > Sessions, right click on the session and click 'View Changes...'
D. By impersonating the administrator with the 'Login as...' option
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything.
What is the most likely cause of this problem? Select the BEST answer.



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

NEW QUESTION: 83
Fill in the blanks: The _____ collects logs and sends them to the _____.
A. Log server; Security Gateway
B. Log server; security management server
C. Security management server; Security Gateway
D. Security Gateways; log server
Answer: D (LEAVE A REPLY)
Gateways send their logs to the log server.

NEW QUESTION: 84
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. Then, export the corresponding entries to a separate log file for documentation.

B. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.
C. 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.
D. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocols. Apply the alert action or customized messaging.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
Fill in the blank Once a license is activated, a_____should be installed.
A. Security Gateway Contract file
B. Service Contract file
C. License Management file
D. License Contract file
Answer: B (LEAVE A REPLY)
Explanation
Once a license is activated, a Service Contract file should be installed. This file contains information about the license expiration date, support level, and other details3. The other options are not valid file names.
References: 3: Check Point R81 Security Management Administration Guide, page 15.

NEW QUESTION: 86
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 (LEAVE A REPLY)
Explanation
The command to restore a backup of Check Point configurations without the OS information is restore_backup4. This command restores the Gaia OS configuration and the firewall database from a compressed file. The other commands are not valid for this purpose. import backup is not a valid command. cp_merge is a command to merge policies or objects from different databases. migrate import is a command to import a previously exported database using migrate export. References: System Backup and Restore feature in Gaia, [cp_merge], [migrate import]

NEW QUESTION: 87
When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?
A. Incorrect routing to reach the gateway.
B. The gateway is not powered on.
C. The Admin would need to login to Read-Only mode
D. Another Admin has made an edit to that object and has yet to publish the change.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?
A. The zone is based on the network topology and determined according to where the interface leads to.
B. Security Zones are not supported by Check Point firewalls.
C. The firewall rule can be configured to include one or more subnets in a zone.
D. The local directly connected subnet defined by the subnet IP and subnet mask.
Answer: A (LEAVE A REPLY)
Explanation
A security zone is a group of one or more network interfaces from different centrally managed gateways that have the same security requirements. The zone is based on the network topology and determined according to where the interface leads to. For example, a zone can be defined as internal, external, DMZ, VPN, etc.
Security zones are supported by Check Point firewalls and can be used to simplify security policies and network segmentation. The firewall rule can be configured to include one or more zones as source or destination objects. The local directly connected subnet defined by the subnet IP and subnet mask is not considered part of the zone, but rather a property of the interface.References: [Security Zones], [Security Zones Best Practices]

NEW QUESTION: 89
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal Communication (SIC)?
A. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.
B. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
C. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
D. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
Fill in the blank: Authentication rules are defined for _____.
A. Users using UserCheck
B. Individual users
C. User groups
D. All users in the database
Answer: (SHOW ANSWER)

NEW QUESTION: 91
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?
A. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs

performance and does not add security due to a shorter key in phase 1.
B. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
C. The two algorithms do not have the same key length and so don't work together. You will get the error ... No proposal chosen...
D. All is fine and can be used as is.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
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 SmartEvent to see why they are being blocked
B. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.
C. Open SmartLog and connect remotely to the wireless controller
D. Open SmartDashboard and review the logs tab
Answer: (SHOW ANSWER)

NEW QUESTION: 93
Which of the following is NOT an option for internal network definition of Anti-spoofing?
A. Not-defined
B. Specific - derived from a selected object
C. Network defined by the interface IP and Net Mask
D. Route-based - derived from gateway routing table
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
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 Limit tab of the Client Authentication Action Properties screen.
B. in the user object's Authentication screen.
C. in the Gateway object's Authentication screen.
D. in the Global Properties Authentication screen.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
Stateful Inspection compiles and registers connections where?
A. Connection Cache
B. State Cache
C. State Table
D. Network Table
Answer: C (LEAVE A REPLY)
Explanation
Stateful Inspection compiles and registers connections in the State Table. The State Table is a database that stores information about active connections and sessions on the Security Gateway. The other options are not valid names for the database that stores connection information.
References: 1: Policy Types 2: CPUSE 3: SIC : [Software Containers] : [Stateful Inspection]

NEW QUESTION: 96
Check Point licenses come in two forms. What are those forms?
A. Security Gateway and Security Management.
B. On-premise and Public Cloud
C. Central and Local.
D. Access Control and Threat Prevention.
Answer: C (LEAVE A REPLY)
Explanation
This answer is correct because these are the two forms of Check Point licenses that are used to activate the software blades on the Security Gateways and the Security Management Servers1. A central license is a license that is attached to a Security Management Server and can be used to manage multiple Security Gateways1. A local license is a license that is attached to a specific Security Gateway and can only be used by that gateway1.
The other answers are not correct because they are either irrelevant or inaccurate options for Check Point licenses forms. Security Gateway and Security Management are not license forms, but software components that provide firewall, VPN, and other security features2. On-premise and Public Cloud are not license forms, but deployment options for Check Point products3. Access Control and Threat Prevention are not license forms, but software blades that provide different security functions.
* Check Point License Guide
* Check Point Software Blade Quick Licensing Guide
* Check Point CloudGuard Network Security
* [Check Point Software Blades]

NEW QUESTION: 97
What type of NAT is a one-to-one relationship where each host is translated to a unique address?
A. Source
B. Static
C. Hide
D. Destination
Answer: B (LEAVE A REPLY)

Explanation
The type of NAT that is a one-to-one relationship where each host is translated to a unique address is Static NAT. Static NAT maps an unregistered IP address to a registered IP address on a one-to-one basis3. This means that for each internal host, there is a corresponding external address that represents it3. Therefore, the correct answer is B

NEW QUESTION: 98
Which of the following are types of VPN communities?
A. Pentagon, star, and combination
B. Star, octagon, and combination
C. Combined and star
D. Meshed, star, and combination
Answer: D (LEAVE A REPLY)
Explanation
The types of VPN communities are Meshed, Star, and Combination. A Meshed community is a group of Security Gateways that have VPN connections between every pair of members. A Star community has one Security Gateway as the center and other Security Gateways or hosts as satellites. A Combination community is a group of Meshed and Star communities. References: [Check Point R81 Site-to-Site VPN Administration Guide]

NEW QUESTION: 99
Which of the following is NOT a policy type available for each policy package?
A. Threat Emulation
B. Access Control
C. Desktop Security
D. Threat Prevention
Answer: (SHOW ANSWER)
Explanation
References: Threat Emulation is not a policy type available for each policy package. Threat Emulation is a software blade that is part of the Threat Prevention policy type. The other options are valid policy types that can be configured for each policy package.
References: [Threat Prevention Administration Guide R80.40],
[Security Policies Administration Guide R80.40]

NEW QUESTION: 100
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.
A. Captive Portal and Transparent Kerberos Authentication
B. UserCheck
C. User Directory
D. Captive Portal
Answer: A (LEAVE A REPLY)
Explanation
Browser-based Authentication sends users to a web page to acquire identities using Captive Portal and Transparent Kerberos

Authentication. Captive Portal is a web page that prompts users to enter their credentials. Transparent Kerberos Authentication is a method that automatically authenticates users who have a valid Kerberos ticket from the Active Directory domain controller2. UserCheck is a feature that allows users to interact with the security policy, not a method of authentication. User Directory is a component that integrates with external user databases, not a web page for authentication. Captive Portal alone is not enough to fill in the blank, as it is only one of the methods used by Browser-based Authentication.

NEW QUESTION: 101
Fill in the blank: Each cluster, at a minimum, should have at least _____ interfaces.
A. Five
B. Two
C. Three
D. Four
Answer: C (LEAVE A REPLY)
Explanation
Each cluster, at a minimum, should have at least three interfaces4. These are:
A sync interface for synchronizing state information between cluster members.
A cluster interface for sending and receiving cluster control packets.
A production interface for handling regular traffic that passes through the cluster4. References: Check Point R80.20 - How to configure Cluster firewalls - First Time Setup

NEW QUESTION: 102
URL Filtering cannot be used to:
A. Control Bandwidth issues
B. Control Data Security
C. Improve organizational security
D. Decrease legal liability
Answer: D (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Creating-Application-Control-and-URL-Filtering-Rules.htm

NEW QUESTION: 103
In SmartConsole, on which tab are Permissions and Administrators defined?
A. Manage and Settings
B. Logs and Monitor
C. Security Policies
D. Gateways and Servers
Answer: (SHOW ANSWER)
Explanation
Permissions and Administrators are defined on the Manage and Settings tab in SmartConsole3. This tab allows you to create and manage administrator accounts, roles, permissions, and authentication methods for accessing SmartConsole and other Check Point management interfaces. References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 104
What is the default shell for the command line interface?
A. Clish
B. Admin
C. Normal
D. Expert
Answer: A (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/Gaia-Clish-Commands.htm

NEW QUESTION: 105
Which of the following is NOT a method used by Identity Awareness for acquiring identity?
A. Remote Access
B. Cloud IdP (Identity Provider)
C. Active Directory Query
D. RADIUS
Answer: B (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Introduction-Identity-Sources.htm?tocpath=Introduction%20to%20Identity%20Awareness%7CIdentity%20Sources%7C_____0

NEW QUESTION: 106
Fill in the blanks: A security Policy is created in _____ , stored in the _____ , and Distributed to the various _____ .
A. The Check Point database, SmartConsole, Security Gateways
B. Rule base, Security Management Server, Security Gateways
C. SmartConsole, Security Management Server, Security Gateways
D. SmartConsole, Security Gateway, Security Management Servers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
Which command can you use to verify the number of active concurrent connections?
A. show all connections
B. fw conn all
C. show connections

D. fw ctl pst pstat
Answer: (SHOW ANSWER)

NEW QUESTION: 108
How would you determine the software version from the CLI?
A. cpinfo
B. fw ver
C. fw monitor
D. fw stat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Which application is used for the central management and deployment of licenses and packages?
A. SmartProvisioning
B. SmartLicense
C. SmartUpdate
D. Deployment Agent
Answer: (SHOW ANSWER)
Explanation
SmartUpdate is the application that is used for the central management and deployment of licenses and packages. SmartUpdate allows administrators to manage licenses, software updates, and hotfixes for multiple Security Gateways and cluster members from one central location2. SmartProvisioning is an application that enables centralized management of network devices. SmartLicense is a feature that simplifies license management by using a cloud-based portal. Deployment Agent is a component that enables automatic deployment of software packages3.

NEW QUESTION: 110
Application Control/URL filtering database library is known as:
A. Application database
B. AppWiki
C. Application-Forensic Database
D. Application Library
Answer: B (LEAVE A REPLY)
Explanation
Application Control/URL filtering database library is known as AppWiki. AppWiki is an application classification and identification database that enables administrators to control access to thousands of applications and millions of websites. References: [Check Point R81 Application Control Administration Guide], [Check Point AppWiki]
NEW QUESTION: 111
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____.
A. User Center
B. User Directory
C. UserCheck

D. User Administration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
Fill in the blank RADIUS protocol uses_____to communicate with the gateway
A. UDP
B. TDP
C. HTTP
D. CCP
Answer: (SHOW ANSWER)

NEW QUESTION: 113
What is the purpose of Priority Delta in VRRP?
A. When a box is up, Effective Priority = Priority + Priority Delta
B. When a box fails, Effective Priority = Priority - Priority Delta
C. When an Interface fails, Effective Priority = Priority - Priority Delta
D. When an Interface is up, Effective Priority = Priority + Priority Delta
Answer: (SHOW ANSWER)

NEW QUESTION: 114
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. 3DES and MD5
C. Certificates and IPsec
D. Certificates and pre-shared secret
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?
A. Microsoft Publisher
B. RC4 Encryption
C. JSON
D. Microsoft Word
Answer: C (LEAVE A REPLY)
NEW QUESTION: 116
Fill in the blanks: There are _____ types of software containers _____.
A. Three; security management, Security Gateway, and endpoint security
B. Two; endpoint security and Security Gateway
C. Three; Security gateway, endpoint security, and gateway management
D. Two; security management and endpoint security

Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
What Check Point tool is used to automatically update Check Point products for the Gaia OS?
A. Check Point INSPECT Engine
B. Check Point Upgrade Service Engine
C. Check Point Update Engine
D. Check Point Upgrade Installation Service
Answer: B (LEAVE A REPLY)
Explanation
The Check Point Upgrade Service Engine (CPUSE) is a tool that automates the process of upgrading and installing Check Point products on Gaia OS1. It can also be used to update the Gaia OS itself2. The other options are not valid tools for this purpose.
References: Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent, Check Point R81 Gaia Installation and Upgrade Guide

NEW QUESTION: 118
Which of the following is NOT an alert option?
A. Mail
B. High alert
C. SNMP
D. User defined alert
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
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 collected with SmartWorkflow from Trouble Ticket systems
C. Logs and Events are synonyms
D. Events are generated at gateway according to Event Policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
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)
Explanation
The backups are stored in Check Point appliances as *.tgz files under /var/CPbackup. This is the default location for backup files created by the backup command. Therefore, the correct answer is B. Saved as *.tgz under /var/CPbackup

NEW QUESTION: 121
When configuring Anti-Spoofing, which tracking options can an Administrator select?
A. Log, Alert, None
B. Log, Allow Packets, Email
C. Drop Packet, Alert, None
D. Log, Send SNMP Trap, Email
Answer: (SHOW ANSWER)
Explanation
Log, Alert, and None are the tracking options that an Administrator can select when configuring Anti-Spoofing. Log means that the packet will be logged in SmartView Tracker. Alert means that the packet will trigger an alert in SmartView Monitor. None means that no action will be taken2. The other options are not valid tracking options.

NEW QUESTION: 122
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?
A. The Gateway is an SMB device
B. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS
C. The checkbox "Use only Shared Secret for all external members" is not checked
D. Pre-shared secret is already configured in Global Properties
Answer: B (LEAVE A REPLY)

NEW QUESTION: 123
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway
A. True, Central License can be installed with CPLIC command on a Security Gateway
B. False, Central License are installed via Gaia on Security Gateways
C. False, Central License are handled via Security Management Server
D. True, CLI is the prefer method for Licensing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124

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: (SHOW ANSWER)
Explanation
When a Security Gateway sends its logs to an IP address other than its own, it means that the Security Gateway and the Log Server are installed on different machines. This is a characteristic of a Distributed deployment3. Therefore, the correct answer is A

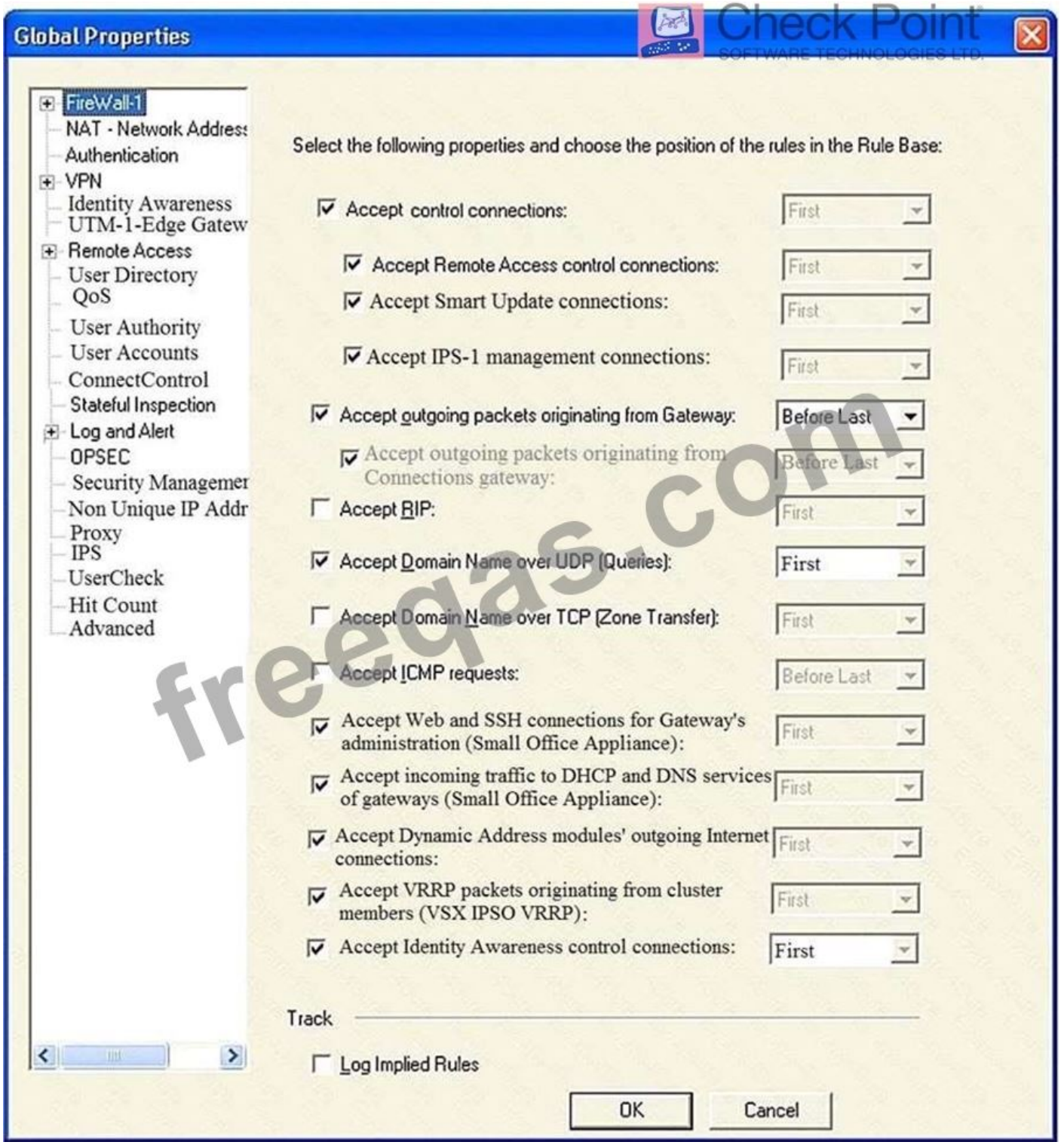
NEW QUESTION: 125
What are the types of Software Containers?
A. Smart Console, Security Management, and Security Gateway
B. Security Management, Security Gateway, and Endpoint Security
C. Security Management, Log & Monitoring, and Security Policy
D. Security Management, Standalone, and Security Gateway
Answer: B (LEAVE A REPLY)
Explanation
The types of Software Containers are Security Management, Security Gateway, and Endpoint Security.
Software Containers are virtual environments that run on top of Gaia OS and allow multiple instances of Check Point products to coexist on the same physical machine. The other options are not valid types of Software Containers.

NEW QUESTION: 126
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?
A. SmartManager
B. SmartConsole
C. Security Gateway
D. Security Management Server
Answer: D (LEAVE A REPLY)
Explanation
The Security Management Server is the component that changes most often and should be backed up most frequently, because it stores all the security policies and configurations for the Check Point components in your network. The other components are either clients or gateways that do not change as frequently.
References: Check Point Security Management Administration Guide R81, p. 9
NEW QUESTION: 127
What default layers are included when creating a new policy layer?
A. Application Control, URL Filtering and Threat Prevention
B. Access Control, Threat Prevention and HTTPS Inspection
C. Firewall, Application Control and IPSec VPN
D. Firewall, Application Control and IPS
Answer: (SHOW ANSWER)
Explanation

The default layers that are included when creating a new policy layer are Access Control, Threat Prevention, and HTTPS Inspection. Access Control is the layer that defines the basic firewall rules. Threat Prevention is the layer that enables the protection against various types of attacks, such as IPS, Anti-Virus, Anti-Bot, etc. HTTPS Inspection is the layer that allows the inspection of encrypted traffic1. The other options are not the default layers that are included when creating a new policy layer.

NEW QUESTION: 128
When changes are made to a Rule base, it is important to _____ to enforce changes.
A. Activate policy
B. Save changes
C. Install policy
D. Publish database
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Consider the Global Properties following settings:



The selected option "Accept Domain Name over UDP (Queries)" means:

A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.

B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Answer: A (LEAVE A REPLY)

Explanation
The selected option "Accept Domain Name over UDP (Queries)" means that UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy. This option enables the Security Gateway to accept DNS queries from external hosts and forward them to internal DNS servers. The queries are accepted by an implied rule that is applied before the explicit rules in the Security Policy. The implied rule only allows queries from interfaces that have external anti-spoofing groups defined . References: Check Point R81 Quantum Security Gateway Guide, Implied Rules

NEW QUESTION: 130
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump.
How can you achieve this requirement?
A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and assign role to the user.
B. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.
C. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 131
In which scenario will an administrator need to manually define Proxy ARP?
A. When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
B. When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
C. When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
D. When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.
Answer: C (LEAVE A REPLY)
Explanation
NAT (Network Address Translation) is a technique that modifies the IP addresses or ports of packets that pass through a security gateway. NAT can be configured in two ways: Automatic or Manual. Automatic NAT means that the NAT rules are generated automatically by the security gateway based on the NAT properties of network objects. Manual NAT means that the NAT rules are defined explicitly by the administrator in the NAT policy. Proxy ARP (Address Resolution Protocol) is a technique that allows a security gateway to answer ARP requests on behalf of other hosts. Proxy ARP is needed when a host on one network segment tries to communicate with a host on another network segment that has a different IP address than its own. In some scenarios, an administrator will need to manually define Proxy ARP for NAT to work properly. One such scenario is when they configure a Manual Static NAT which translates to an IP address that does not belong to one of the firewall's interfaces2. References: Check Point R81 Network Address Translation Administration Guide
NEW QUESTION: 132

Which of the following technologies extracts detailed information from packets and stores that information in state tables?
A. INSPECT Engine
B. Next-Generation Firewall
C. Packet Filtering
D. Application Layer Firewall
Answer: B (LEAVE A REPLY)
Check Point FireWall-1's Stateful Inspection overcomes the limitations of the previous two approaches by providing full application-layer awareness without breaking the client/server model. With Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over. It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. This provides a solution which is highly secure and offers maximum performance, scalability, and extensibility.

NEW QUESTION: 133
Which two Identity Awareness commands are used to support identity sharing?
A. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
C. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
D. Policy Activation Point (PAP) and Policy Decision Point (PDP)
Answer: C (LEAVE A REPLY)

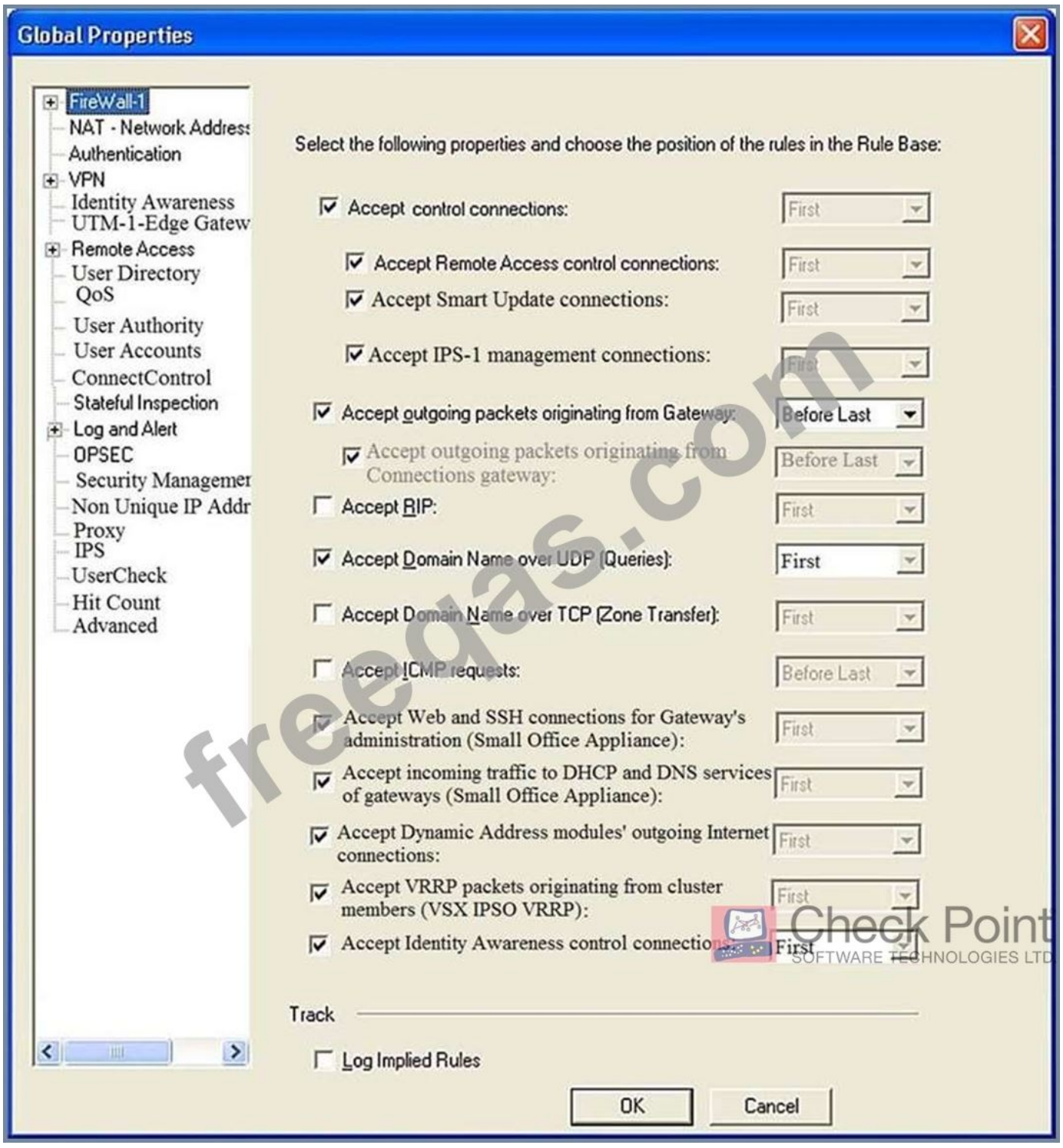
NEW QUESTION: 134
Which of the following commands is used to monitor cluster members in CLI?
A. show active cluster
B. show cluster state
C. show running cluster
D. show clusters
Answer: B (LEAVE A REPLY)

NEW QUESTION: 135
Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.
A. Main
B. Authentication
C. Quick
D. High Alert
Answer: A (LEAVE A REPLY)
Phase I modes
Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

NEW QUESTION: 136
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. No, it will not work independently. Hit Count will be shown only for rules with Track options set as Log or alert
B. Yes, it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway
C. No, it will not work independently because hit count requires all rules to be logged
D. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways
Answer: D (LEAVE A REPLY)
Explanation
The Hit count feature will work independently from logging and track the hits even if the Track option is set to "None"1, p. 23. When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways and displays the number of connections that each rule matches in SmartConsole3. References: Check Point CCSA - R81: Practice Test & Explanation, Check Point Security Management Administration Guide R81

NEW QUESTION: 137
Consider the Global Properties following settings:



The selected option "Accept Domain Name over UDP (Queries)" means:

A. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

C. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

D. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.

Answer: (SHOW ANSWER)

NEW QUESTION: 138
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 Limit tab of the Client Authentication Action Properties screen.
B. in the Gateway object's Authentication screen.
C. in the user object's Authentication screen.
D. in the Global Properties Authentication screen.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?
A. Blue > add local backup
B. Blue > set backup local
C. Blue > add backup local
D. Expert&Blue#add local backing
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Examine the sample Rule Base.

What will be the result of a verification of the policy from SmartConsole?
A. Verification Error. Empty Source-List in Rule 5 (Mail Inbound)
B. No errors or Warnings
C. Verification Error. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)
D. Verification Error. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule
Answer: C (LEAVE A REPLY)

NEW QUESTION: 141
Access roles allow the firewall administrator to configure network access according to:
A. a combination of computer groups and network

B. users and user groups
C. all of above
D. remote access clients
Answer: C (LEAVE A REPLY)
To create an access role:
The Access Role window opens.
Your selection is shown in the Networks node in the Role Preview pane.
A window opens. You can search for Active Directory entries or select them from the list.
You can search for AD entries or select them from the list.
The access role is added to the Users and Administrators tree.

NEW QUESTION: 142
Choose what BEST describes a Session.
A. Sessions ends when policy is pushed to the Security Gateway.
B. Starts when an Administrator publishes all the changes made on SmartConsole.
C. Starts when an Administrator logs in to the Security Management Server through SmartConsole and ends when it is published.
D. Sessions locks the policy package for editing.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
How are the backups stored in Check Point appliances?
A. Saved as*tar under /var/CPbackup
B. Saved as*tgz under /var/log/CPbackup/backups
C. Saved as*tgz under /var/CPbackup
D. Saved as*.tar under /var/log/CPbackup/backups
Answer: C (LEAVE A REPLY)

NEW QUESTION: 144
Fill in the blank RADIUS Accounting gets_____data from requests generated by the accounting client
A. Payload
B. Destination
C. Location
D. Identity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?
A. All Connections (Clear or Encrypted)
B. Accept all encrypted traffic
C. Specific VPN Communities
D. All Site-to-Site VPN Communities

Answer: C (LEAVE A REPLY)
Explanation
The option that allows traffic to VPN gateways in specific VPN communities is Specific VPN Communities4.
This option enables you to define which VPN communities are allowed in the rule. All Connections (Clear or Encrypted) allows traffic to any destination, regardless of whether it is encrypted or not. Accept all encrypted traffic allows traffic to any encrypted destination, regardless of the VPN community. All Site-to-Site VPN Communities allows traffic to any site-to-site VPN gateway, regardless of the VPN community4. Therefore, the correct answer is C. Specific VPN Communities.

NEW QUESTION: 146
Which of the following is NOT a policy type available for each policy package?
A. Threat Prevention
B. Desktop Security
C. Threat Emulation
D. Access Control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 147
Fill in the blank: The_____is used to obtain identification and security information about network users.
A. User index
B. UserCheck
C. User Directory
D. User server
Answer: (SHOW ANSWER)
Explanation
The User Directory is used to obtain identification and security information about network users. It can be integrated with external user databases such as LDAP, RADIUS, or TACACS+. References: Certified Security Administrator (CCSA) R81.20 Course Overview, page 9.

NEW QUESTION: 148
What is the mechanism behind Threat Extraction?
A. 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
B. 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
C. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
D. 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).
Answer: B (LEAVE A REPLY)
NEW QUESTION: 149
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?
A. SND is a feature to accelerate multiple SSL VPN connections

B. SND is an alternative to IPSec Main Mode, using only 3 packets
C. SND is used to distribute packets among Firewall instances
D. SND is a feature of fw monitor to capture accelerated packets
Answer: C (LEAVE A REPLY)
Explanation
The Secure Network Distributor (SND) is a feature of the Security Gateway that is used to distribute packets among Firewall instances . It improves the performance and scalability of the Firewall by utilizing multiple CPU cores. The other options are not related to SND. References: [Check Point Security Gateway Architecture and Packet Flow], [Free Check Point CCSA Sample Questions and Study Guide]

NEW QUESTION: 150
Can multiple administrators connect to a Security Management Server at the same time?
A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
D. Yes, but only one has the right to write
Answer: C (LEAVE A REPLY)
Explanation
Multiple administrators can connect to a Security Management Server at the same time, and each administrator has their own username and works in a session that is independent of other administrators1. This allows concurrent administration and prevents conflicts between different administrators. The other options are incorrect. Only one administrator can be connected is false. All administrators can modify a network object at the same time is false, as only one administrator can lock and edit an object at a time. Only one has the right to write is false, as all administrators have write permissions unless they are restricted by roles or permissions. References: Security Management Server - Check Point Software

NEW QUESTION: 151
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: 152
Which of the following is NOT a role of the SmartCenter:
A. Status monitoring
B. Policy configuration
C. Certificate authority
D. Address translation
Answer: (SHOW ANSWER)
Explanation
Address translation is not a role of the SmartCenter, as it is performed by the Security Gateway based on the NAT policy configured in the SmartConsole5. The other options are roles of the SmartCenter, as it is responsible for status monitoring, policy configuration, and certificate authority for the Security Gateways5.
References: Gaia R81.10 Administration Guide, QUANTUM SECURITY MANAGEMENT R81, Remote Access VPN R81 Administration Guide

NEW QUESTION: 153
How do you manage Gaia?
A. Through CLI and WebUI
B. Through CLI only
C. Through SmartDashboard only
D. Through CLI, WebUI, and SmartDashboard
Answer: D (LEAVE A REPLY)
Explanation
Gaia can be managed through CLI, WebUI, and SmartDashboard1, p. 17-18. CLI is a command-line interface that allows administrators to configure and monitor Gaia using commands and scripts. WebUI is a web-based interface that allows administrators to configure and monitor Gaia using a browser. SmartDashboard is a graphical user interface that allows administrators to manage security policies and objects for Gaia devices.
References: Check Point CCSA - R81: Practice Test & Explanation, [Check Point Gaia Administration Guide R81], [Check Point Security Management Administration Guide R81]

NEW QUESTION: 154
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. Limit
B. Resource
C. Custom Application / Site
D. Network Object
Answer: B (LEAVE A REPLY)
Explanation
Resource is NOT an objects category in SmartConsole1, p. 18. The objects categories in SmartConsole are Network Object, Host, Network, Group, Gateway, Cluster, VPN Community, Service, Time Object, Access Role, Custom Application / Site, Data Center Object, Limit. References: Check Point CCSA - R81: Practice Test & Explanation, [Check Point SmartConsole R81 Help]

NEW QUESTION: 155
Security Gateway software blades must be attached to what?
A. Security Gateway
B. Security Gateway container
C. Management server
D. Management container
Answer: B (LEAVE A REPLY)
Explanation
Security Gateway software blades must be attached to a Security Gateway container. A Security Gateway container is a logical object that represents a physical or virtual machine that runs the Security Gateway software. A software blade is a modular security feature that can be enabled or disabled on a Security Gateway container. A software blade can provide functions such as firewall, VPN, IPS, anti-virus, anti-bot, application control, URL filtering, etc.References: [Security Gateway Containers], [Software Blades]

NEW QUESTION: 156
Fill in the blank: By default, the SIC certificates issued by R81 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: 157
When you upload a package or license to the appropriate repository in SmartUpdate. where is the package or license stored?
A. SmartConsole installed device
B. Check Point user center
C. Security Management Server
D. Security Gateway
Answer: C (LEAVE A REPLY)
Explanation
When you upload a package or license to the appropriate repository in SmartUpdate, the package or license is stored on the Security Management Server. SmartUpdate is a tool that allows you to centrally manage software updates and licenses for all Check Point products on your network.
References: : Check Point R81 Security Management Administration Guide, page 16.

NEW QUESTION: 158
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. Create a Suspicious Activity Rule in Smart Monitor.
C. Select Block intruder from the Tools menu in SmartView Tracker.

D. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 159
How many users can have read/write access in Gaia Operating System at one time?
A. One
B. Three
C. Two
D. Infinite
Answer: A (LEAVE A REPLY)
if another user has r/w access, you need to use "lock database override" or "unlock database" to claim r/w access. Ref: https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/html_frameset.htm?topic=documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/162435

NEW QUESTION: 160
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 miltik pq enable
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl multik dynamic_dispatching on
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
Which information is included in the "Extended 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: (SHOW ANSWER)
Explanation
Application information is included in the "Extended Log" tracking option, but is not included in the "Log" tracking option4. The "Extended Log" option provides additional information about the application, such as name, category, risk, and technology4.
References: LOGGINGAND MONITORING R80

NEW QUESTION: 162
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.

To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
4) Install policy.
Ms McHanry tries to access the resource but is unable.
What should she do?
A. Have the security administrator select the Action field of the Firewall Rule "Redirect HTTP connections to an authentication (captive) portal".
B. Have the security administrator select Any for the Machines tab in the appropriate Access Role.
C. Install the Identity Awareness agent on her iPad.
D. Have the security administrator reboot the firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 163
The SmartEvent R80 Web application for real-time event monitoring is called:
A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView
Answer: D (LEAVE A REPLY)
Explanation
SmartView is the web application for real-time event monitoring in SmartEvent R80 and above. It provides a unified view of security events across the network and allows for quick investigation and response34.
References: SmartEvent R80.40 Administration Guide, SmartView

NEW QUESTION: 164
Which icon in the WebUI indicates that read/write access is enabled?
A. Pencil
B. Eyeglasses
C. Padlock
D. Book
Answer: (SHOW ANSWER)

NEW QUESTION: 165
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?
A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.
C. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and

assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?
A. Configure rules to limit the available network bandwidth for specified users or groups.
B. Use UserCheck to help users understand that certain websites are against the company's security policy.
C. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.
D. Detects and blocks malware by correlating multiple detection engines before users are affected.
Answer: (SHOW ANSWER)

NEW QUESTION: 167
How is communication between different Check Point components secured in R81? As with all questions, select the best answer.
A. By using ICA
B. By using 3DES
C. By using SIC
D. By using IPSEC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
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. snapshot
B. logswitch
C. Database Revision
D. backup
Answer: (SHOW ANSWER)

NEW QUESTION: 169
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, and if the session is saved, rule will be available

B. Rule is locked by AdminA, because the save bottom has not been press.
C. Rule is locked by AdminA, and will make it available if session is published.
D. Rule is locked by AdminA, because an object on that rule is been edited.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
Which one of the following is TRUE?
A. Ordered policy is a sub-policy within another policy
B. Pre-R80 Gateways do not support ordered layers
C. Inline layer can be defined as a rule action
D. One policy can be either inline or ordered, but not both
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
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. SmartUpdate upgrade
B. CPUSE offline upgrade
C. CPUSE online upgrade
D. Export R80 configuration, clean install R80.10 and import the configuration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172
Which of the following is NOT a method used by Identity Awareness for acquiring identity?
A. Remote Access
B. RADIUS
C. Active Directory Query
D. Certificates
Answer: D (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following is NOT a type of Endpoint Identity Agent?
A. Terminal
B. Light
C. Full
D. Custom
Answer: (SHOW ANSWER)

NEW QUESTION: 174
Session unique identifiers are passed to the web api using which http header option?
A. X-chkp-sid

B. Accept-Charset
C. Proxy-Authorization
D. Application
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A because session unique identifiers are passed to the web api using the X-chkp-sid http header option1. The X-chkp-sid header is used to authenticate and authorize API calls1. The other options are not related to session unique identifiers.
References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 175
When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:
A. The entire Management Database and all sessions and other administrators can connect only as Read-only.
B. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
C. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.
D. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 176
What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
⊗	A-GW	10.1.1.1	R80	
✓	SMS	10.1.1.101	R80	

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)
Explanation
If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem.
The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention.
The other options are not correct, as they do not match the status shown in the image. If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.
References: Remote Access VPN R81 Administration Guide, Check Point R81.10

NEW QUESTION: 177

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 (LEAVE A REPLY)

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: 178

Fill in the blank: An LDAP server holds one or more _____.

A. Server Units

B. Account Units

C. Administrator Units

D. Account Servers

Answer: B (LEAVE A REPLY)

NEW QUESTION: 179

View the rule below. What does the pen-symbol in the left column mean?

A. The configuration lock is present. Click the pen symbol in order to gain the lock.

B. Another user has currently locked the rules for editing.

C. Rules have been edited by the logged in administrator, but the policy has not been published yet.

D. Those rules have been published in the current session.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 180

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 (LEAVE A REPLY)

SIC Status

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:

NEW QUESTION: 181

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

A. secondary Smartcenter

B. active Smartcenter

C. connect virtual IP of Smartcenter HA

D. primary Smartcenter

Answer: B (LEAVE A REPLY)

Explanation

The SmartCenter that should be connected to for making changes is the active SmartCenter. The active SmartCenter is the one that is currently synchronizing its configuration with the secondary SmartCenter and handling the communication with the gateways . The primary SmartCenter is the one that was initially configured as the main server, but it may become inactive if a failover occurs. The virtual IP of SmartCenter HA is used to access the SmartConsole, not to make changes. References: [Security Management Server High Availability (HA) R81 Administration Guide], [Check Point CCSA - R81: Practice Test & Explanation], [How to configure ClusterXL High Availability on Security Management Server]

NEW QUESTION: 182
What command would show the API server status?
A. cpm status
B. api restart
C. api status
D. show api status
Answer: D (LEAVE A REPLY)
Explanation
The command api status shows the API server status, including whether it is enabled or not, the port number, and the API version1.
References: Check Point R81 API Reference Guide

NEW QUESTION: 183
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet.
How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"
B. On the firewall object, Legacy Authentication screen, check "Enable Identity Captive Portal"
C. In the Captive Portal screen of Global Properties, check "Enable Identity Captive Portal"
D. On the Security Management Server object, check the box "Identity Logging"
Answer: A (LEAVE A REPLY)
Explanation
Identity Captive Portal is a Check Point Identity Awareness web portal, to which users connect with their web browser to log in and authenticate, when using Browser-Based Authentication2. To enable Identity Captive Portal for a specific rule, you need to right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"3. References: Identity Awareness Administration Guide R80, Identity awareness with captive portal in Checkpoint R80

NEW QUESTION: 184
When configuring Anti-Spoofing, which tracking options can an Administrator select?
A. Log, Alert, None
B. Drop Packet, Alert, None
C. Log, Allow Packets, Email

D. Log, Send SNMP Trap, Email
Answer: A (LEAVE A REPLY)

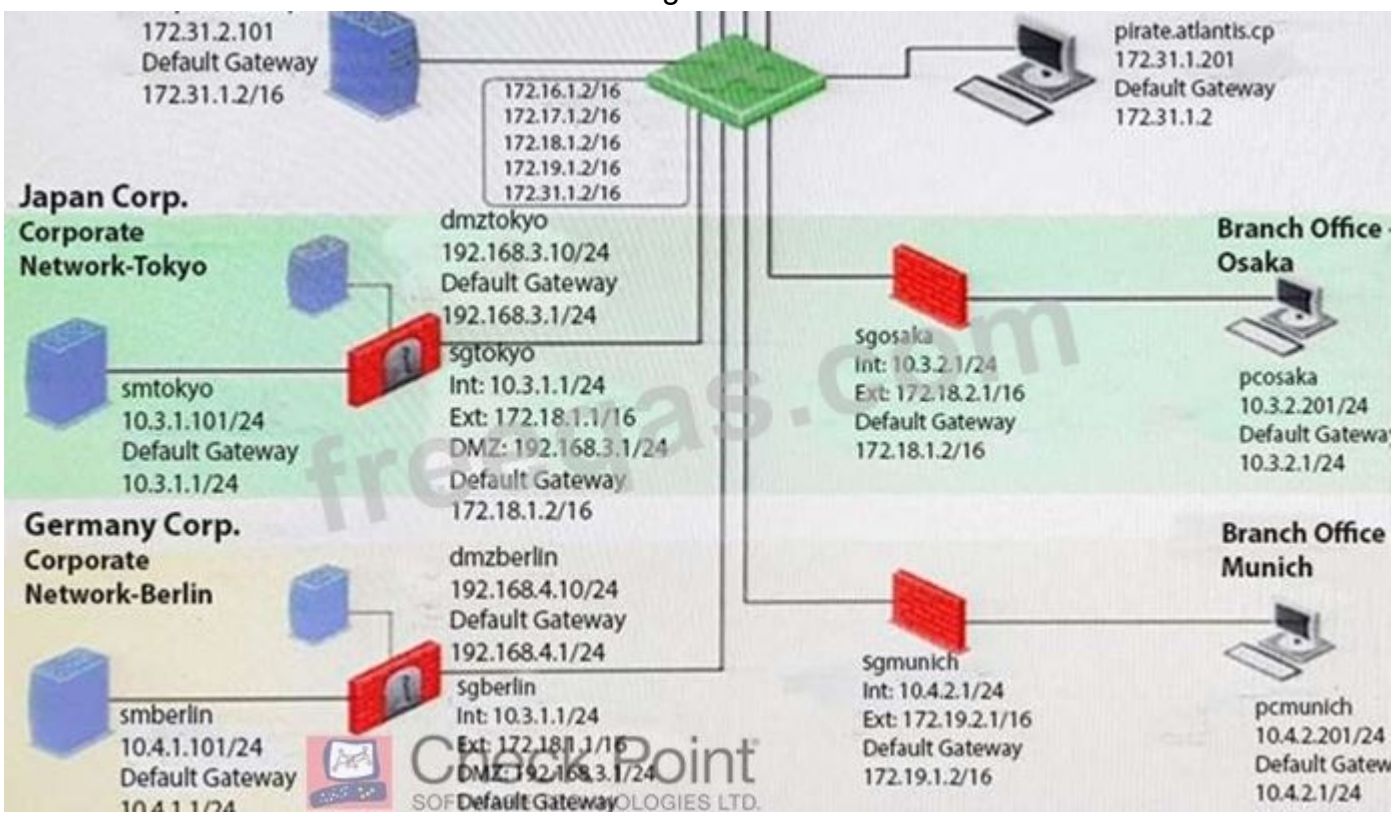
NEW QUESTION: 185
Which type of attack can a firewall NOT prevent?
A. Network Bandwidth Saturation
B. Buffer Overflow
C. SYN Flood
D. SQL Injection
Answer: A (LEAVE A REPLY)
Explanation
A firewall can NOT prevent a network bandwidth saturation attack, which is a type of denial-of-service (DoS) attack that aims to consume all the available bandwidth of a target network or device1, p. 9. A firewall can prevent other types of attacks, such as buffer overflow, SYN flood, and SQL injection, by inspecting packets and applying security rules2, p. 11-12. References: Check Point CCSA - R81: Practice Test & Explanation, 156-315.81 Checkpoint Exam Info and Free Practice Test

NEW QUESTION: 186
An administrator can use section titles to more easily navigate between large rule bases. Which of these statements is FALSE?
A. Section titles are not sent to the gateway side.
B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.
C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.
D. Sectional Titles do not need to be created in the SmartConsole.
Answer: (SHOW ANSWER)
Section titles are only for visual categorization of rules.

NEW QUESTION: 187
Is it possible to have more than one administrator connected to a Security Management Server at once?
A. Yes, but only if all connected administrators connect with read-only permissions.
B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
C. No, only one administrator at a time can connect to a Security Management Server
D. Yes, but only one of those administrators will have write-permissions. All others will have read-only permission.
Answer: B (LEAVE A REPLY)
Explanation
It is possible to have more than one administrator connected to a Security Management Server at once, but objects edited by one administrator will be locked for editing by others until the session is published. This feature is called concurrent administration and it allows multiple administrators to work on the same security policy at the same time. However, when one administrator edits an object, such as a gateway, a rule, or a network, that object is locked for other administrators until the change is published or discarded. The lock icon shows which objects are being edited by other administrators and prevents conflicts or overwrites.References: [Concurrent Administration], [SmartConsole Overview]

NEW QUESTION: 188

You want to reset SIC between smberlin and sgosaka.



In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the menu.

When trying to establish a connection, instead of a working connection, you receive this error message:

What is the reason for this behavior?

A. The check Point services on the Gateway were not restarted because you are still in the cpconfig utility.

B. You must first initialize the Gateway object in SmartDashboard (i.e., right-click on the object, choose Basic Setup > Initialize).

C. The Gateway was not rebooted, which is necessary to change the SIC key.

D. The activation key contains letters that are on different keys on localized keyboards. Therefore, the activation can not be typed in a matching fashion.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 189

What is a role of Publishing?

A. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base
B. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
C. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
D. The Security Management Server installs the updated policy and the entire database on Security Gateways
Answer: C (LEAVE A REPLY)

NEW QUESTION: 190
Full synchronization between cluster members is handled by Firewall Kernel.
Which port is used for this?
A. TCP port 256
B. UDP port 256
C. UDP port 265
D. TCP port 265
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
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. Anti-Virus
Answer: D (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/The_Check_Point_ThreatCloud.htm

NEW QUESTION: 192
Identity Awareness lets an administrator easily configure network access and auditing based on three items Choose the correct statement.
A. Network location, the identity of a user and the active directory membership.
B. Network location, the identity of a user and the identity of a machine.
C. Network location, the telephone number of a user and the UID of a machine
D. Geographical location, the identity of a user and the identity of a machine
Answer: (SHOW ANSWER)
Explanation
Identity Awareness is a software blade that lets an administrator easily configure network access and auditing based on three items: network location, the identity of a user, and the identity of a machine. These items are used to identify and authenticate users and machines, and to enforce identity-based policies. Network location refers to the IP address or subnet of the source or destination of the traffic. The identity of a user can be obtained from various sources, such as Active Directory, LDAP, or Captive Portal. The identity of a machine can be verified by using Secure Domain Logon or Identity Agent.

NEW QUESTION: 193
When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?
A. Log, allow packets, email
B. Log, alert, none
C. Log, send snmp trap, email
D. Drop packet, alert, none
Answer: B (LEAVE A REPLY)
Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

NEW QUESTION: 194
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. AD Query
B. Terminal Servers Endpoint Identity Agent
C. Endpoint Identity Agent and Browser-Based Authentication
D. RADIUS and Account Logon
Answer: C (LEAVE A REPLY)
Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary. The Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

NEW QUESTION: 195
Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?
A. SmartDashboard
B. SmartEvent
C. SmartView Monitor
D. SmartUpdate
Answer: B (LEAVE A REPLY)
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. Ref: https://www.checkpoint.com/products/smartevent/

NEW QUESTION: 196
Fill in the blank: Licenses can be added to the License and Contract repository _____ .
A. From a file, manually, or from SmartView Monitor
B. From the User Center, from a file, or manually
C. From SmartView Monitor, from the User Center, or from a file
D. Manually, from SmartView Monitor, or from the User Center
Answer: B (LEAVE A REPLY)

NEW QUESTION: 197
Where can administrator edit a list of trusted SmartConsole clients?
A. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
B. 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.
C. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients, via cpconfig on a Security Gateway.
D. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 198
When changes are made to a Rule base, it is important to _____ to enforce changes.
A. Publish database
B. Save changes
C. Install policy
D. Activate policy
Answer: (SHOW ANSWER)

NEW QUESTION: 199
Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?
A. All Site-to-Site VPN Communities
B. All Connections (Clear or Encrypted)
C. Accept all encrypted traffic
D. Specific VPN Communities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 200
What is the purpose of Captive Portal?
A. It manages user permission in SmartConsole
B. It provides remote access to SmartConsole
C. It authenticates users, allowing them access to the Internet and corporate resources
D. It authenticates users, allowing them access to the Gaia OS
Answer: (SHOW ANSWER)
Captive Portal is a simple method that authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminGuide/html_frameset.htm?

topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminGuide/148468

NEW QUESTION: 201
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:
A. 3rd Party integration of CLI and API for Management prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. A complete CLI and API interface for Management with 3rd Party integration.
D. 3rd Party integration of CLI and API for Gateways prior to R80.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 202
Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI?
A. hostname myHost12 ip-address 10.50.23.90
B. mgmt add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt add host name emailserver1 ip-address 10.50.23.90
Answer: D (LEAVE A REPLY)
Explanation
The correct syntax for adding a host using GAiA management CLI is mgmt add host name <name> ip-address <ip-address>2. References: Check Point GAiA R81 Command Line Interface Reference Guide

NEW QUESTION: 203
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 set_mode 9
B. fw ctl miltik pq enable
C. fw ctl multik dynamic_dispatching on
D. fw ctl multik dynamic_dispatching set_mode 9
Answer: A (LEAVE A REPLY)

NEW QUESTION: 204
Which option in tracking allows you to see the amount of data passed in the connection?
A. Data
B. Accounting
C. Logs
D. Advanced
Answer: (SHOW ANSWER)
Explanation
Accounting is the option in tracking that allows you to see the amount of data passed in the connection.

Accounting tracks the number of bytes and packets for each connection and generates reports based on the collected data.
References: Certified Security Administrator (CCSA) R81.20 Course Overview, page 14.

NEW QUESTION: 205
Using ClusterXL, what statement is true about the Sticky Decision Function?
A. Can only be changed for Load Sharing implementations
B. All connections are processed and synchronized by the pivot
C. Is configured using cpconfig
D. Is only relevant when using SecureXL
Answer: A (LEAVE A REPLY)
Explanation
The Sticky Decision Function (SDF) can only be changed for Load Sharing implementations, not for High Availability implementations4. References: Check Point ClusterXL R81 Administration Guide

NEW QUESTION: 206
In SmartConsole, on which tab are Permissions and Administrators defined?
A. Security Policies
B. Logs and Monitor
C. Gateways and Servers
D. Manage and Settings
Answer: D (LEAVE A REPLY)

NEW QUESTION: 207
Fill in the blank: An identity server uses a _____ for user authentication.
A. Shared secret
B. Certificate
C. One-time password
D. Token
Answer: A (LEAVE A REPLY)
Explanation
The answer is A because an identity server uses a shared secret for user authentication. A shared secret is a passphrase that is known by both the identity server and the user. The identity server sends a challenge to the user, who encrypts it with the shared secret and sends it back. The identity server then verifies the response and authenticates the user12 References: Check Point R81 Identity Awareness Administration Guide, Check Point R81 Identity Server

NEW QUESTION: 208
What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
	A-GW	10.1.1.1	R80	
	SMS	10.1.1.101	R80	

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)
Explanation
If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem.
The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention.
The other options are not correct, as they do not match the status shown in the image. If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.
References: Remote Access VPN R81 Administration Guide, Check Point R81.10

NEW QUESTION: 209
What is the best sync method in the ClusterXL deployment?
A. Use 2 clusters + 1st sync + 2nd sync
B. Use 1 dedicated sync interface
C. Use 1 cluster + 1st sync
D. Use 3 clusters + 1st sync + 2nd sync + 3rd sync

Answer: B (LEAVE A REPLY)

NEW QUESTION: 210
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. When Joe logs in, Bob will be log out automatically.
B. If Joe tries to make changes, he won't, database will be locked.
C. Since they both are log in on different interfaces, they both will be able to make changes.
D. Bob will be prompt that Joe logged in.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 211
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?
A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with UID 0 and assign role to the user.
C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.
Answer: A (LEAVE A REPLY)
Explanation
To achieve the requirement of giving the Network Operations Center administrator access to Check Point Security devices mostly for troubleshooting purposes, but not to the expert mode, and still allowing her to run tcpdump, you need to:
Add tcpdump to CLISH using add command. This command adds a new command to the Command Line Interface Shell (CLISH) that allows running tcpdump without entering the expert mode .
Create a new access role. This option defines a set of permissions and commands that can be assigned to a user or a group of users.
Add tcpdump to the role. This option grants the permission to run tcpdump to the role.
Create new user with any UID and assign role to the user. This option creates a new user account with any User ID (UID) and assigns the role that has tcpdump permission to the user.
References: [How to add a new command to CLISH], [Check Point R81 Gaia Administration Guide], [Check Point R81 Identity Awareness Administration Guide]

NEW QUESTION: 212
Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?
A. Application Control
B. Data Awareness
C. Identity Awareness
D. Threat Emulation
Answer: A (LEAVE A REPLY)
Explanation
Application Control is the software blade that enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine. Application Control allows you to define granular rules for applications, web sites, web categories, web content types, and users. You can also use Application Control to monitor and block risky applications and web usage. References: [Application Control Administration Guide R80.40]

NEW QUESTION: 213
What are the two types of NAT supported by the Security Gateway?
A. Destination and Hide
B. Hide and Static
C. Static and Source
D. Source and Destination
Answer: B (LEAVE A REPLY)
Explanation
The two types of NAT supported by the Security Gateway are hide NAT and static NAT. Hide NAT translates many source IP addresses into one IP address, usually the external interface of the gateway. Static NAT translates one source IP address into another IP address, usually a public IP address34. The other options are not valid types of NAT. References: Network Address Translation (NAT), Check Point CCSA - R81:
Practice Test & Explanation

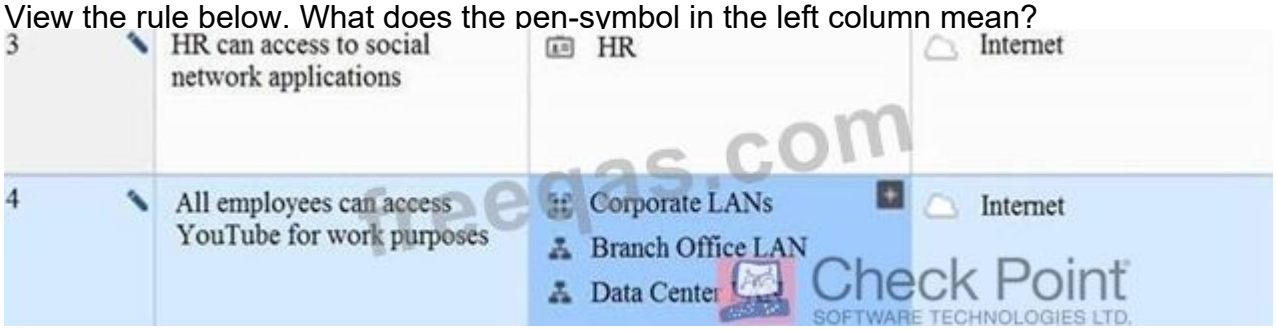
NEW QUESTION: 214
Look at the following screenshot and select the BEST answer.


A. Internal clients can upload and download archive-files to FTP_Ext server using FTP.
B. Internal clients can upload and download any-files to FTP_Ext-server using FTP.
C. Clients external to the Security Gateway can download archive files from FTP_Ext server using FTP.
D. Clients external to the Security Gateway can upload any files to the FTP_Ext-server using FTP.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 215
Using ClusterXL, what statement is true about the Sticky Decision Function?
A. Is only relevant when using SecureXL

B. All connections are processed and synchronized by the pivot
C. Is configured using cpconfig
D. Can only be changed for Load Sharing implementations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 216
View the rule below. What does the pen-symbol in the left column mean?



A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is present. Click the pen symbol in order to gain the lock.
Answer: B (LEAVE A REPLY)
Explanation
The pen-symbol in the left column means that the rules have been edited by the logged in administrator, but the policy has not been published yet. It indicates that the changes are not yet effective and can be discarded.References: Policy Editor, Publishing Changes

NEW QUESTION: 217
What are the three tabs available in SmartView Tracker?
A. Predefined, All Records, Custom Queries
B. Endpoint, Active, and Custom Queries
C. Network & Endpoint, Management, and Active
D. Network, Endpoint, and Active
Answer: A (LEAVE A REPLY)

NEW QUESTION: 218
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 (LEAVE A REPLY)
Explanation
When an encrypted packet is decrypted, this happens in the security policy4. The security policy is a set of rules that defines how the Security Gateway inspects and secures traffic. The security policy includes VPN rules that specify which traffic should be encrypted or decrypted. The inbound and outbound chains are part of the inspection framework that processes packets according to the security

policy. References: Check Point R81 VPN Administration Guide

NEW QUESTION: 219
Choose what BEST describes users on Gaia Platform.
A. There is one default user that cannot be deleted.
B. There are two default users that cannot be deleted and one SmartConsole Administrator.
C. There are two default users and one cannot be deleted.
D. There is one default user that can be deleted.
Answer: (SHOW ANSWER)

NEW QUESTION: 220
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal Communication (SIC)?
A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.
Answer: A (LEAVE A REPLY)
Explanation
The statement that best describes Secure Internal Communication (SIC) is: After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA. SIC is a mechanism that ensures secure communication between Check Point components by using certificates that are issued by an Internal Certificate Authority (ICA)3. The other statements are not accurate descriptions of SIC.

NEW QUESTION: 221
When configuring LDAP with User Directory integration, changes applied to a User Directory template are:
A. Not reflected for any users unless the local user template is changed.
B. Not reflected for any users who are using that template.
C. Reflected for ail users who are using that template and if the local user template is changed as well.
D. Reflected immediately for all users who are using that template.
Answer: (SHOW ANSWER)
You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Managing-Users-on-User-Directory-Server.htm

NEW QUESTION: 222
What is the main objective when using Application Control?
A. To filter out specific content.
B. To assist the firewall blade with handling traffic.

C. To see what users are doing.

D. Ensure security and privacy of information.

Answer: (SHOW ANSWER)

https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/

NEW QUESTION: 223

With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

A. The complete communication is sent for inspection.

B. The IP address of the source machine.

C. The end user credentials.

D. The host portion of the URL.

Answer: B (LEAVE A REPLY)

"A local cache that gives answers to 99% of URL categorization requests. When the cache does not have an answer, only the host name is sent to the Check Point Online Web Service for categorization. "

https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/24853/FILE/CP_R77_ApplicationControlURLFiltering_AdminGuide.pdf

NEW QUESTION: 224

How do you configure an alert in SmartView Monitor?

A. An alert cannot be configured in SmartView Monitor.

B. By right-clicking on the Gateway, and selecting Properties.

C. By right-clicking on the Gateway, and selecting System Information.

D. By choosing the Gateway, and Configure Thresholds.

Answer: (SHOW ANSWER)

NEW QUESTION: 225

What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard

B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy

C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy

D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C (LEAVE A REPLY)

Explanation

The steps to configure the HTTPS Inspection Policy are as follows34:

Go to Manage & Settings > Blades > HTTPS Inspection > Policy.

Click on New HTTPS Inspection Rule or select an existing rule and click on Edit Rule.

Define the Source, Destination for the rule. The action can be either Inspect, Bypass, or Ask.

Click on OK and then on Install Policy to apply the changes. References: HTTPS Inspection R81 Administration Guide, Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 226

Which of the following is NOT a type of Endpoint Identity Agent?

A. Custom
B. Terminal
C. Full
D. Light
Answer: A (LEAVE A REPLY)
Explanation
There are three types of Endpoint Identity Agents: Full, Light, and Terminal. Custom is not a valid type2.
References: 2: Check Point R81 Endpoint Security Administration Guide, page 18.

NEW QUESTION: 227
Which of the following is NOT a tracking option? (Select three)
A. Partial log
B. Full log
C. Network log
D. Log
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 228
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect.
Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.
A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config
Answer: (SHOW ANSWER)
Explanation
The commands you could use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1 after the initial installation on Check Point appliance are:
set interface Mgmt ipv4-address 192.168.80.200 mask-length 24. This command sets the IPv4 address and subnet mask of the

Management interface.
set static-route default nexthop gateway address 192.168.80.1 on. This command sets the default gateway for IPv4 routing.
save config. This command saves the configuration changes.
References: [Check Point R81 Gaia CLI Reference Guide], [Check Point R81 Gaia Administration Guide]

NEW QUESTION: 229
What are the steps to configure the HTTPS Inspection Policy?
A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy
Answer: C (LEAVE A REPLY)
Explanation
The steps to configure the HTTPS Inspection Policy are as follows34:
Go to Manage & Settings >
Click on New HTTPS Inspection Rule or select an existing rule and click on Edit Rule.
Define the Source, Destination for the rule. The action can be either Inspect, Bypass, or Ask.
Click on OK and then on Install Policy to apply the changes. References: HTTPS Inspection R81 Administration Guide, Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 230
Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?
A. All Site-to-Site VPN Communities
B. Accept all encrypted traffic
C. All Connections (Clear or Encrypted)
D. Specific VPN Communities
Answer: B (LEAVE A REPLY)
Explanation
The option that allows all encrypted and non-VPN traffic that matches the rule is Accept all encrypted traffic. This option enables you to allow traffic to any destination that is encrypted, regardless of whether it is part of a VPN community or not2. Therefore, the correct answer is B. Accept all encrypted traffic.

NEW QUESTION: 231
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: (SHOW ANSWER)

NEW QUESTION: 232

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

A. The Security Gateway is upgraded.

B. The existing license expires.

C. The license is upgraded.

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

Answer: A (LEAVE A REPLY)

Explanation

Upgrading the Security Gateway does not require a new license to be generated and installed. The license is tied to the IP address or hostname of the Security Gateway, not the software version. However, if the IP address or hostname changes, the existing license expires, or the license is upgraded, a new license must be generated and installed12 References: Check Point R81, Managing and Installing license via SmartUpdate

NEW QUESTION: 233

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. Accelerated Path

B. Slow Path

C. Medium Path

D. Fast Path

Answer: B (LEAVE A REPLY)

NEW QUESTION: 234

In order to modify Security Policies, the administrator can use which of the following tools? (Choose the best answer.)

A. SmartConsole and WebUI on the Security Management Server.

B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.

C. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.

D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Answer: B (LEAVE A REPLY)

Explanation

In order to modify Security Policies, the administrator can use SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed. SmartConsole is a graphical tool that allows the administrator to create, edit, and manage security policies using a web browser. mgmt_cli (API) is a command-line tool that allows the administrator to perform the same tasks using commands and scripts. Both tools can connect to the Security Management Server remotely from any computer that has SmartConsole installed.References: [SmartConsole Overview], [mgmt_cli (API)]

NEW QUESTION: 235

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

A. No Response

B. Down

C. Failed

D. Inactive
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?
A. backup
B. Database Revision
C. snapshot
D. migrate export
Answer: C (LEAVE A REPLY)
Snapshot Management
The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.
Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.
The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be saved.

NEW QUESTION: 237
What key is used to save the current CPView page in a filename format cpview_"cpview process ID". cap"number of captures"?
A. C
B. W
C. S
D. Space bar
Answer: A (LEAVE A REPLY)

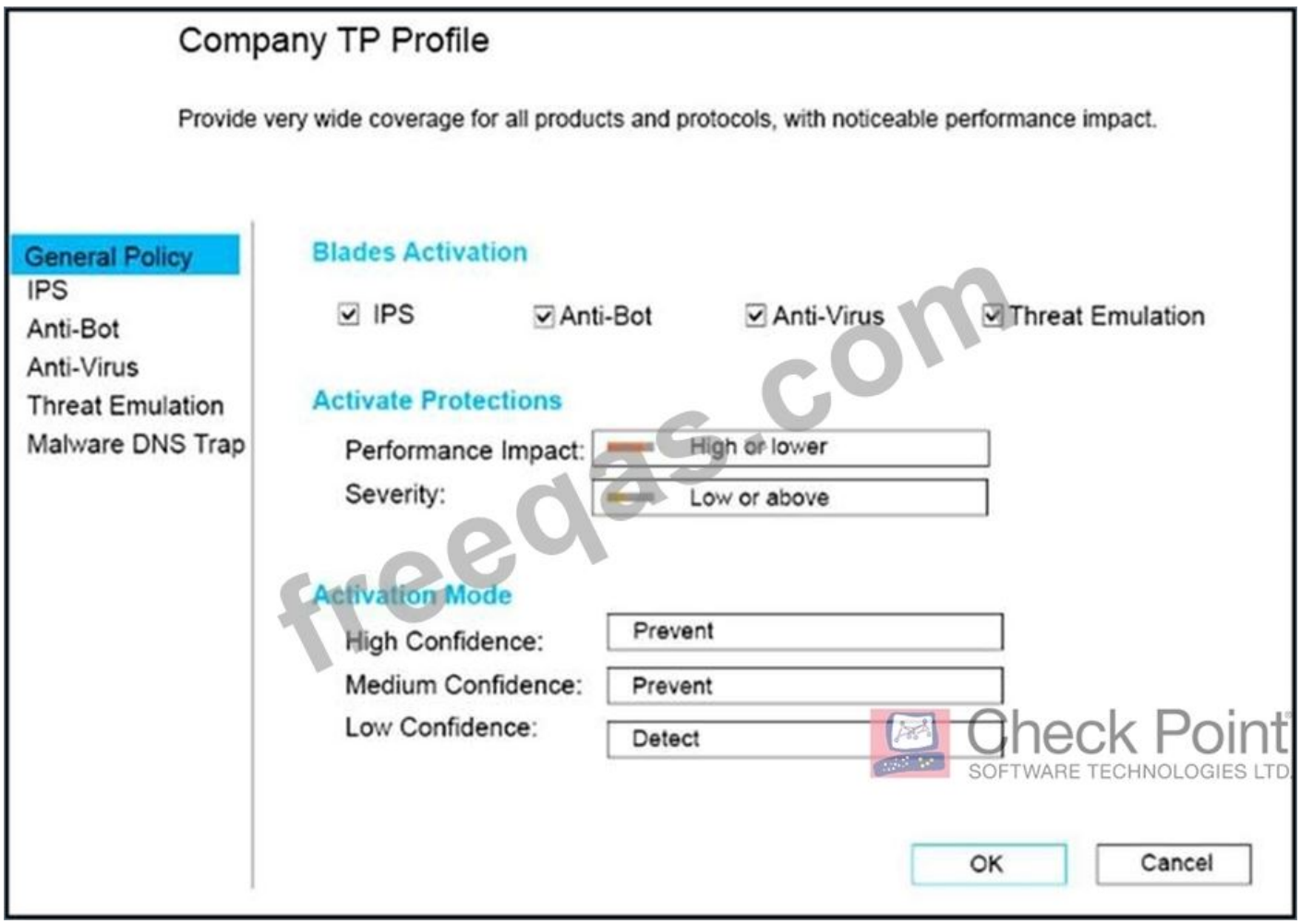
NEW QUESTION: 238
Which backup utility captures the most information and tends to create the largest archives?
A. snapshot
B. migrate export
C. backup
D. Database Revision
Answer: A (LEAVE A REPLY)

NEW QUESTION: 239
URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?
A. WebCheck
B. UserCheck
C. Harmony Endpoint
D. URL categorization

Answer: B (LEAVE A REPLY)
UserCheck alerts users while attemping to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION: 240
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: (SHOW ANSWER)
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: 241
CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings.
The following Threat Prevention Profile has been created.



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 the Performance Impact to Very Low Confidence to Prevent.

B. Set the Performance Impact to Medium or lower.

C. Set High Confidence to Low and Low Confidence to Inactive.

D. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 242

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 (LEAVE A REPLY)
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: 243
If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?
A. Log Implied Rule was not set correctly on the track column on the rules base.
B. Track log column is set to Log instead of Full Log.
C. Track log column is set to none.
D. Log Implied Rule was not selected on Global Properties.
Answer: D (LEAVE A REPLY)
Explanation
If there is an Accept Implied Policy set to "First", Jorge cannot see any logs because Log Implied Rule was not selected on Global Properties. The Log Implied Rule option enables logging for all implied rules, such as DHCP, anti-spoofing, and cleanup rules.
References: : Check Point R81 Security Management Administration Guide, page 103.

NEW QUESTION: 244
If an administrator wants to restrict access to a network resource only allowing certain users to access it, and only when they are on a specific network what is the best way to accomplish this?
A. Create an inline layer where the destination is the target network resource Define sub-rules allowing only specific sources to access the target resource
B. Create an Access Role object, with specific users or user groups specified, and specific networks defined Use this access role as the "Source" of an Access Control rule
C. Use a "New Legacy User At Location", specifying the LDAP user group that the users belong to, at the desired location
D. Create a rule allowing only specific source IP addresses access to the target network resource.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 245
What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
	A-GW	10.1.1.1	R80	
	SMS	10.1.1.101	R80	

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)
Explanation
If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem.
The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention.
The other options are not correct, as they do not match the status shown in the image. If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.
References: Remote Access VPN R81 Administration Guide. Check Point R81.10

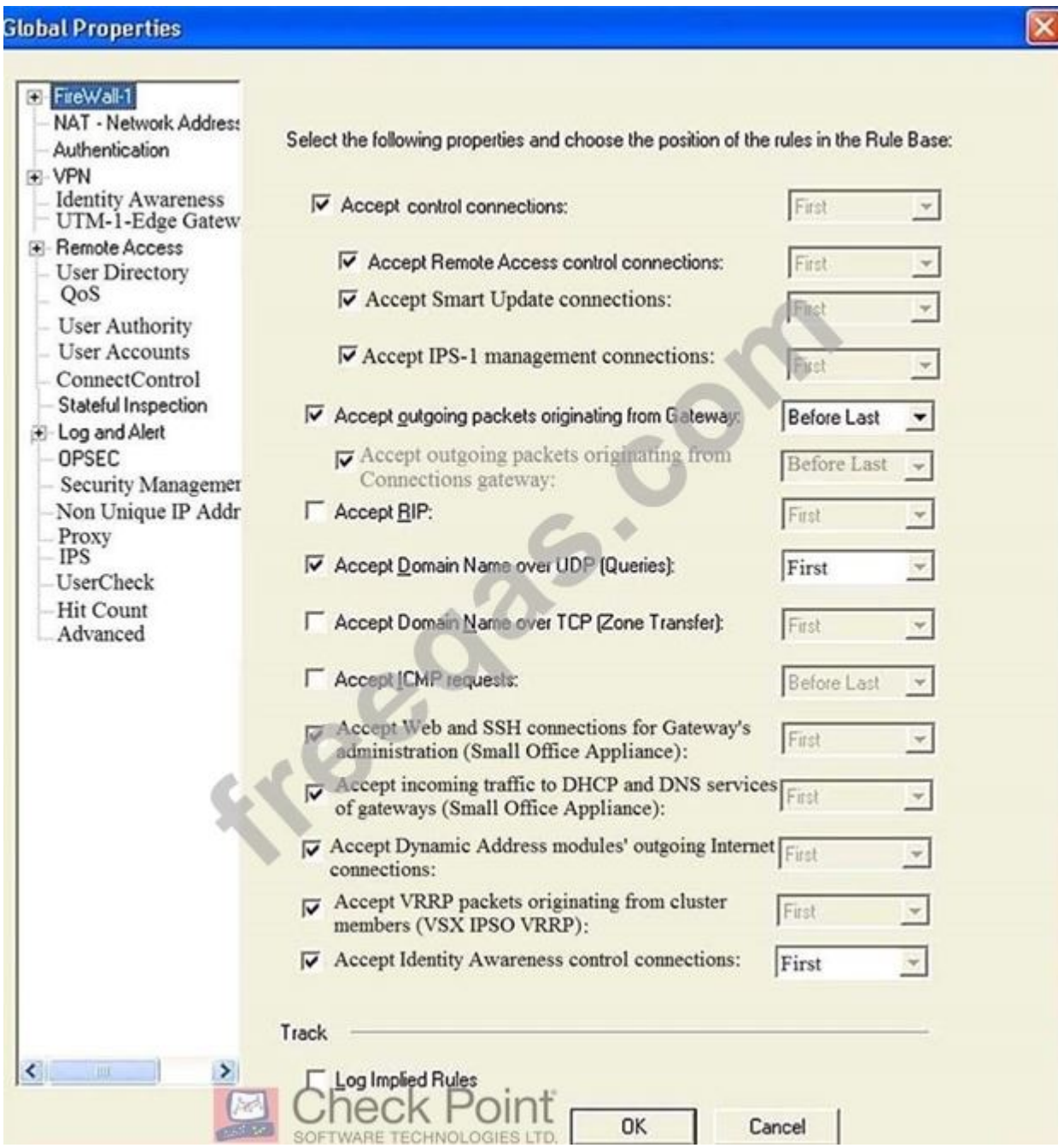
NEW QUESTION: 246
In SmartEvent, a correlation unit (CU) is used to do what?
A. Collect security gateway logs, Index the logs and then compress the logs.
B. Receive firewall and other software blade logs in a region and forward them to the primary log server.
C. Analyze log entries and identify events.
D. Send SAM block rules to the firewalls during a DOS attack.
Answer: C (LEAVE A REPLY)
Explanation

A correlation unit (CU) is a component of SmartEvent that analyzes log entries on log servers and identifies events based on predefined or custom rules1. A CU receives logs from one or more log servers and forwards them to the SmartEvent server, where they are stored in the events database

NEW QUESTION: 247
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. Anti-Virus
Answer: D (LEAVE A REPLY)
Explanation
Anti-Virus is the Check Point software blade that prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud. Anti-Virus scans files and email attachments for viruses, worms, trojans, and other types of malware. It also uses ThreatCloud, a collaborative network that delivers real-time dynamic security intelligence, to detect unknown malware based on their behavior. Firewall is a software blade that enforces security policy by inspecting and controlling network traffic. Application Control is a software blade that enables administrators to control access to web applications. Anti-spam and Email Security is a software blade that protects email infrastructure from spam, phishing, and malware attacks.

NEW QUESTION: 248
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. Formal
B. Central
C. Corporate
D. Local
Answer: (SHOW ANSWER)
Explanation
Check Point licenses are divided into two types: central and local. Central licenses are managed by a Security Management Server and can be attached to any Security Gateway managed by that server. Local licenses are tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address. Formal and corporate are not types of Check Point licenses. References: [Check Point R81 Licensing and Contract Administration Guide]

NEW QUESTION: 249
Consider the Global Properties following settings:



The selected option "Accept Domain Name over UDP (Queries)" means:

A. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

C. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.

D. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 250

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: (SHOW ANSWER)
Explanation
The answer is A because changing the Security Gateway IP-address requires re-establishing the trust with the Security Management Server by initializing the Secure Internal Communication (SIC). Changing the Security Gateway name in command line or changing the Security Management Server name or IP-address in SmartConsole does not require re-establishing the trust, but it may require updating the topology and pushing the policy.References: [Check Point R81 Security Management Administration Guide], [Check Point R81 Security Gateway Administration Guide]

NEW QUESTION: 251
Which key is created during Phase 2 of a site-to-site VPN?
A. Pre-shared secret
B. Diffie-Hellman Public Key
C. Symmetrical IPSec key
D. Diffie-Hellman Private Key
Answer: C (LEAVE A REPLY)
Explanation
The key that is created during Phase 2 of a site-to-site VPN is a symmetrical IPSec key3. This key is used to encrypt and decrypt the data that is exchanged between the VPN peers3. The symmetrical IPSec key is derived from the shared secret and the Diffie-Hellman public keys that are exchanged during Phase 13.
References: Site to Site VPN in R80.x - Tutorial for Beginners

NEW QUESTION: 252
Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?
A. Kerberos Ticket Requested
B. Account Logon
C. Kerberos Ticket Renewed
D. Kerberos Ticket Timed Out
Answer: D (LEAVE A REPLY)

NEW QUESTION: 253
Which of the following technologies extracts detailed information from packets and stores that information in state tables?
A. INSPECT Engine
B. Application Layer Firewall
C. Packet Filtering
D. Next-Generation Firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 254

Fill in the blanks: A Security Policy is created in_____, stored in the_____ and Distributed to the various

A. Rule base. Security Management Server Security Gateways

B. The Check Point database. SmartConsole, Security Gateways

C. SmartConsole, Security Gateway, Security Management Servers

D. SmartConsole, Security Management Server, Security Gateways

Answer: (SHOW ANSWER)

Explanation

A Security Policy is created in SmartConsole, stored in the Security Management Server, and distributed to the various Security Gateways. SmartConsole is a graphical user interface that allows administrators to create and edit security policies. The Security Management Server is a central server that stores and manages the security policies. The Security Gateways are devices that enforce the security policies on the network traffic.

References: : Check Point R81 Security Gateway Administration Guide, page 9.

NEW QUESTION: 255

What does it mean if Deyra sees the gateway status:

Choose the BEST answer.

A. Security Gateway's MGNT NIC card is disconnected.

B. There is a blade reporting a problem

C. VPN software blade is reporting a malfunction

D. SmartCenter Server cannot reach this Security Gateway

Answer: B (LEAVE A REPLY)

NEW QUESTION: 256

Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.

A. Main

B. Authentication

C. Quick

D. High Alert

Answer: A (LEAVE A REPLY)

Explanation

Phase 1 of the two-phase negotiation process conducted by IKE operates in Main mode or Aggressive mode12. Main mode is more secure than Aggressive mode, as it protects the identities of the peers and uses six messages to establish the IKE SA13. Authentication, Quick, and High Alert are not valid modes for IKE phase 1.

References: Understand IPsec IKEv1 Protocol, Internet Key Exchange for IPsec VPNs Configuration Guide, Internet Key Exchange

NEW QUESTION: 257
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 (LEAVE A REPLY)
Explanation
The Security Management Server and the Security Gateway are the components that can store logs in the Check Point Security Management Architecture. The Security Management Server stores logs in a database and can also forward them to external log servers. The Security Gateway can store logs locally in a buffer or a local log file, and can also send them to the Security Management Server or a log server.
References: Check Point Security Management Administration Guide R81, p. 11-12

NEW QUESTION: 258
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?
A. RADIUS
B. Check Point password
C. Security questions
D. SecurID
Answer: (SHOW ANSWER)
Explanation
Security questions are not an authentication scheme used for accounts created through SmartConsole4. The available authentication schemes are Check Point password, RADIUS, TACACS, SecurID, LDAP, and Certificate. References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 259
Which of the following is NOT a method used by Identity Awareness for acquiring identity?
A. Remote Access
B. Cloud IdP (Identity Provider)
C. Active Directory Query
D. RADIUS
Answer: B (LEAVE A REPLY)
Explanation
Identity Awareness uses several methods for acquiring identity, such as Active Directory Query, Identity Agent, Browser-Based Authentication, Terminal Servers, Captive Portal, and RADIUS12. Cloud IdP (Identity Provider) is not a method used by Identity

Awareness12. Therefore, the correct answer is B. Cloud IdP (Identity Provider).

NEW QUESTION: 260
How do you configure the Security Policy to provide uses access to the Captive Portal through an external (Internet) interface?
A. No action is necessary. This access is available by default.
B. Change the gateway settings to allow Captive Portal access via an external interface.
C. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 261
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 (LEAVE A REPLY)
Explanation
The answer is B because querying logs now is very fast because the Indexing Engine indexes logs for faster search results. The Indexing Engine is a component of the Smart-1 appliance that creates indexes for log fields and values, such as source, destination, action, and time. The indexes enable quick and efficient searches of large amounts of log data.References: [Check Point R81 Logging and Monitoring Administration Guide],
[Check Point R81 Indexing Engine]

NEW QUESTION: 262
In which scenario is it a valid option to transfer a license from one hardware device to another?
A. From an IBM Open Server to an HP Open Server
B. From a 4400 Appliance to an HP Open Server
C. From a 4400 Appliance to a 2200 Appliance
D. From an IBM Open Server to a 2200 Appliance
Answer: (SHOW ANSWER)

NEW QUESTION: 263
You had setup the VPN Community NPN-Stores' with 3 gateways. There are some issues with one remote gateway(I .1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways.
A. action:"Key Install" AND 1.1.1.1 AND Quick Mode
B. Blade:"VPN"AND VPN-Stores AND Main Mode
C. action:"Key Install" AND 1.1.1.1 AND Main Mode
D. Blade:"VPN"AND VPN-Stores AND Quick Mode
Answer: A (LEAVE A REPLY)
Explanation

This log filter will show only the logs that have the action of "Key Install", which means that the Security Gateway installed a new encryption key for the VPN tunnel1. It will also show only the logs that have the IP address of 1.1.1.1, which is the remote gateway that has some issues. Finally, it will show only the logs that have the Quick Mode, which is the IKE Phase 2 negotiation that establishes the agreed networks for both gateways2.
The other log filters are not correct because they either include the Main Mode, which is the IKE Phase 1 negotiation that establishes the secure channel between the gateways2, or they do not specify the IP address of the remote gateway.
* Logging and Monitoring R81.20 Administration Guide
* Remote Access VPN R81.20 Administration Guide
* Remote Access VPN R81 Administration Guide

NEW QUESTION: 264
View the rule below. What does the pen-symbol in the left column mean?

A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is present. Click the pen symbol in order to gain the lock.
Answer: B (LEAVE A REPLY)
Explanation
The pen-symbol in the left column means that the rules have been edited by the logged in administrator, but the policy has not been published yet. It indicates that the changes are not yet effective and can be discarded.References: Policy Editor, Publishing Changes

NEW QUESTION: 265
To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?
A. Protections
B. IPS Protections
C. ThreatWiki
D. Profiles
Answer: (SHOW ANSWER)

NEW QUESTION: 266
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 (LEAVE A REPLY)

NEW QUESTION: 267
What is the default shell of Gaia CLI?
A. clish
B. Monitor
C. Read-only
D. Bash
Answer: A (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/CLI-Reference-_interface_.htm

NEW QUESTION: 268
Which authentication scheme requires a user to possess a token?
A. TACACS
B. RADIUS
C. SecurID
D. Check Point password
Answer: (SHOW ANSWER)

NEW QUESTION: 269
Which one of the following is TRUE?
A. Ordered policy is a sub-policy within another policy
B. One policy can be either inline or ordered, but not both
C. Inline layer can be defined as a rule action
D. Pre-R80 Gateways do not support ordered layers
Answer: C (LEAVE A REPLY)
Explanation
The answer is C because inline layer can be defined as a rule action in a policy layer. Inline layer is a sub-policy that contains additional rules that are applied only if the parent rule matches. Ordered layer is a policy layer that contains rules that are applied in order, from top to bottom. One policy can be either inline or ordered, but not both. Pre-R80 Gateways do support ordered layers, but not inline layers5 References: Check Point R81 Policy Layers and Sub-Policies, [Check Point R81 Security Gateway Administration Guide]

NEW QUESTION: 270
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 (LEAVE A REPLY)
Explanation
The Next Generation Threat Emulation software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware1, p. 41. It emulates files in a virtual environment and inspects their behavior for malicious activity3. References: Check Point CCSA - R81: Practice Test & Explanation, Check Point Threat Emulation Administration Guide R81

NEW QUESTION: 271
You have enabled "Extended 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. Identity Awareness is not enabled.
B. Log Trimming is enabled.
C. Logging has disk space issues
D. Content Awareness is not enabled.
Answer: D (LEAVE A REPLY)
Explanation
Extended Log is a tracking option that enables administrators to see additional information about the traffic that matches a security rule, such as data type, file name, file size, etc. However, to see any data type information, Content Awareness must be enabled on the Security Gateway. Content Awareness is a blade that inspects files based on their type, size, name, and data. Content Awareness is required for Extended Log to work properly3. References: Check Point R81 Content Awareness Administration Guide

NEW QUESTION: 272
What is the BEST method to deploy Identity Awareness for roaming users?
A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways
D. Use captive portal
Answer: (SHOW ANSWER)
Explanation
The BEST method to deploy Identity Awareness for roaming users is to use identity agents, which are software components installed on endpoints that provide user and machine identity information to the Security Gateway45. Identity agents are more secure and reliable than other methods, as they do not require network changes or user interaction4. Office Mode, sharing user identities between gateways, and using captive portal are not methods to deploy Identity Awareness, but rather features or options that can be used with Identity Awareness46.

References: Identity Awareness Reference Architecture and Best Practices, Identity Awareness PDP Broker, Identity Awareness Datasheet

NEW QUESTION: 273
Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?
A. Dynamic ID
B. Username and Password
C. RADIUS
D. Certificate
Answer: A (LEAVE A REPLY)

NEW QUESTION: 274
What are the three deployment options available for a security gateway?
A. Standalone, Distributed, and Bridge Mode
B. Bridge Mode, Remote, and Standalone
C. Remote, Standalone, and Distributed
D. Distributed, Bridge Mode, and Remote
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

NEW QUESTION: 275
John is using Management HA.
Which Smartcenter should be connected to for making changes?
A. secondary Smartcenter
B. active Smartcenter
C. connect virtual IP of Smartcenter HA
D. primary Smartcenter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 276
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?
A. Logging & Monitoring
B. None - the data is available by default
C. Monitoring Blade
D. SNMP
Answer: C (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Monitoring-Blade.htm

NEW QUESTION: 277

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. No, it will not work independently because hit count requires all rules to be logged
D. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways
Answer: (SHOW ANSWER)

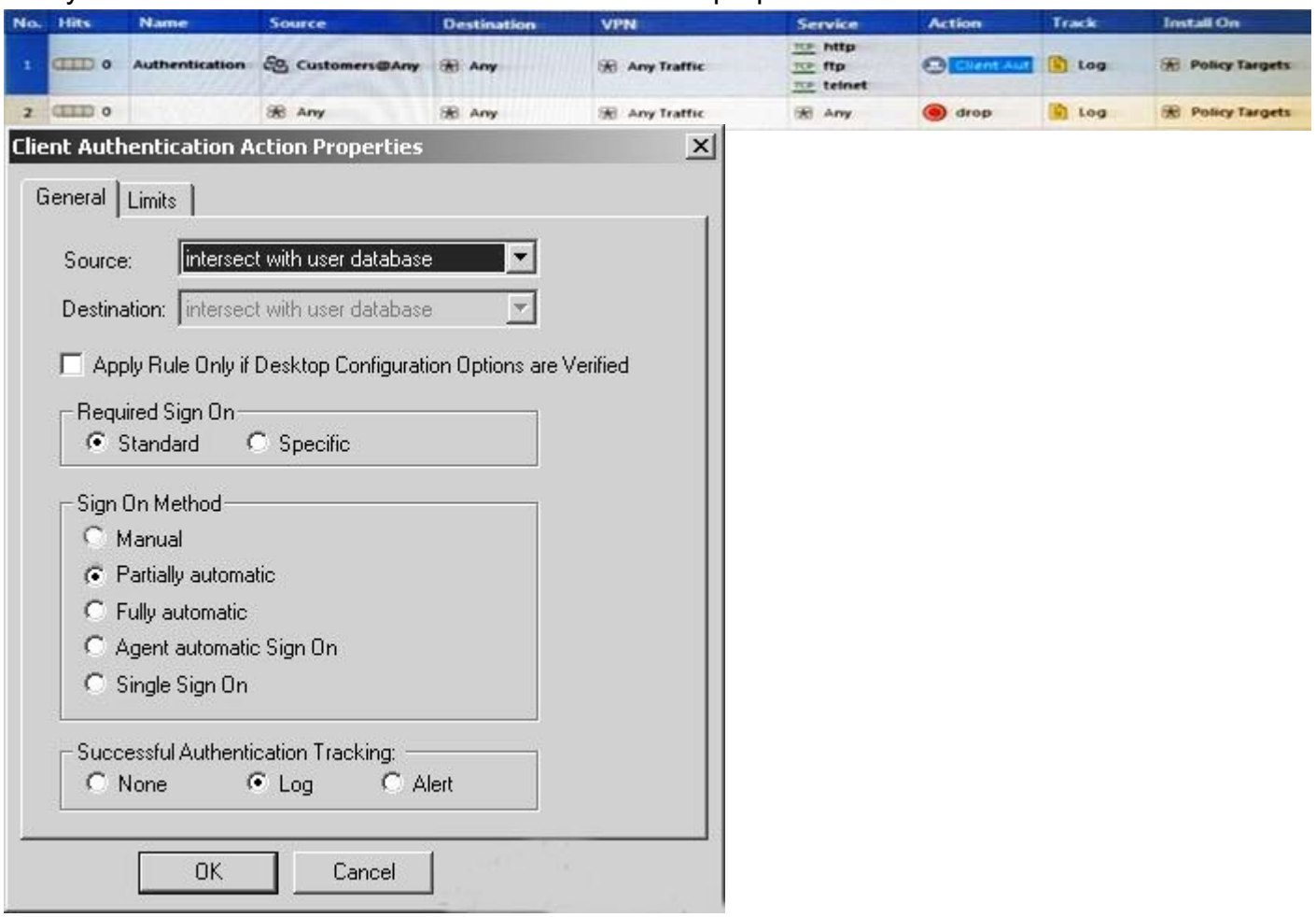
NEW QUESTION: 278
An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).
Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.
If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.
Which of the following is the BEST for this behavior?
A. The Log Server is failing to log GRE traffic properly because it is VPN traffic. Disable all VPN configuration to the partner site to enable proper logging.
B. The setting Log does not capture this level of detail for GRE. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
C. The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracker. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
D. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE sessions. This is a known issue with GRE. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279
Fill in the blank: _____information is included in the "Full Log" tracking option, but is not included in the "Log" tracking option?
A. destination port
B. data type
C. file attributes
D. application
Answer: B (LEAVE A REPLY)
NEW QUESTION: 280
Which of the following is NOT a component of Check Point Capsule?
A. Capsule Enterprise
B. Capsule Docs
C. Capsule Workspace
D. Capsule Cloud

Answer: (SHOW ANSWER)

NEW QUESTION: 281
A SAM rule Is implemented to provide what function or benefit?
A. Allow security audits.
B. Handle traffic as defined in the policy.
C. Monitor sequence activity.
D. Block suspicious activity.
Answer: (SHOW ANSWER)
Explanation
A SAM (Suspicious Activity Monitoring) rule is implemented to provide the function or benefit of blocking suspicious activity. A SAM rule is a rule that defines an action to be taken by the firewall when it detects a suspicious activity, such as an attack, a scan, or a policy violation. The action can be blocking, dropping, rejecting, or logging the traffic that triggered the suspicious activity. A SAM rule can be created manually or automatically by other security features, such as IPS, Anti-Bot, or SmartEvent.References: [SAM Rules], [Suspicious Activity Rules]

NEW QUESTION: 282
Study the Rule base and Client Authentication Action properties screen.

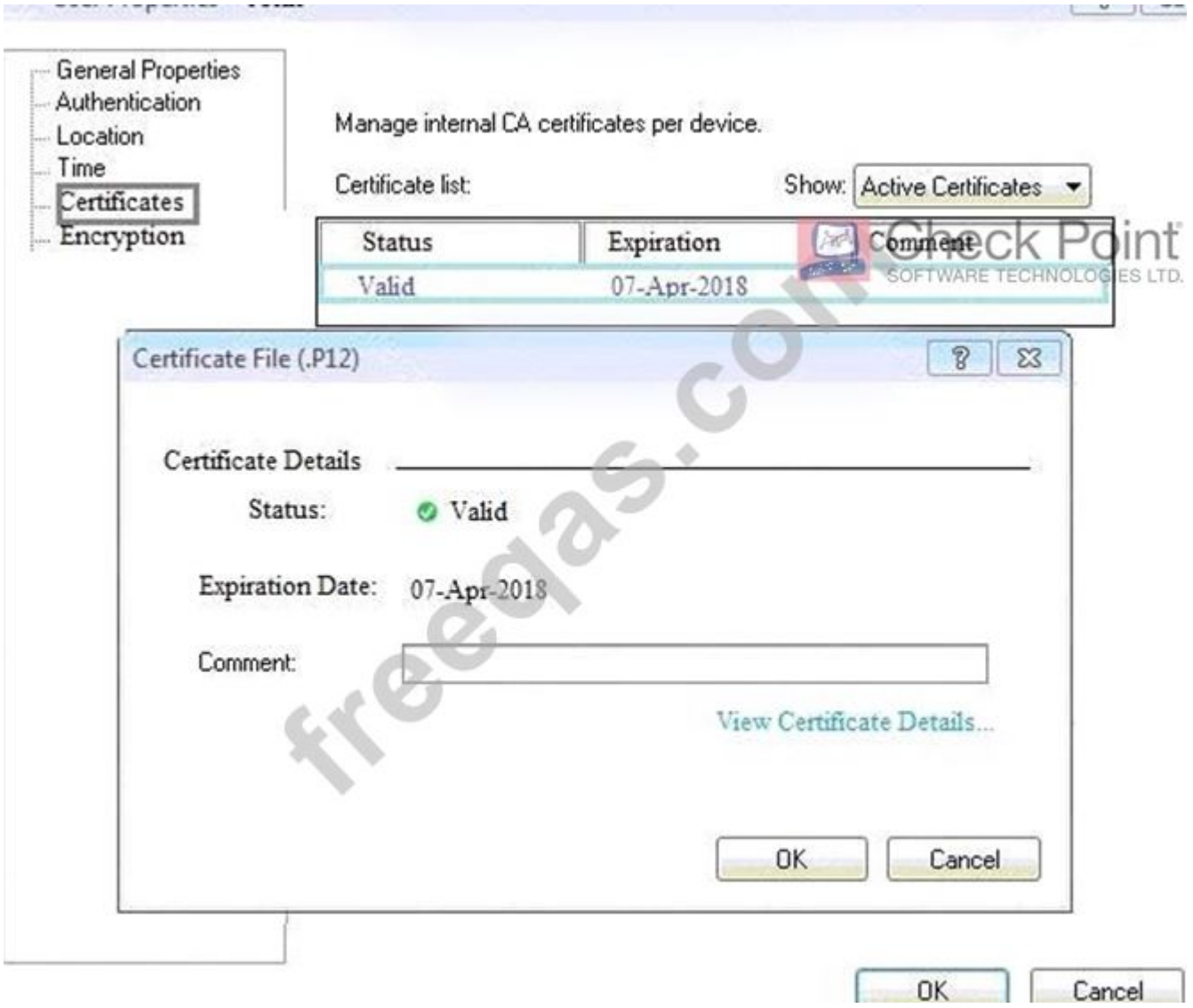


After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site.
What happens when the user tries to FTP to another site using the command line? The:
A. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client

Authentication
B. FTP data connection is dropped after the user is authenticated successfully.
C. FTP connection is dropped by Rule 2.
D. user is prompted for authentication by the Security Gateways again.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 283
R80 Security Management Server can be installed on which of the following operating systems?
A. Gaia only
B. Gaia, SPLAT, Windows Server only
C. Gaia, SPLAT, Windows Server and IPSO only
D. Gaia and SPLAT only
Answer: (SHOW ANSWER)
R80 can be installed only on GAIA OS.
Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:
* Security Management Server
* Multi-Domain Security Management Server
* Log Server
* Multi-Domain Log Server
* SmartEvent Server

NEW QUESTION: 284
You can see the following graphic:



What is presented on it?

A. Properties of personal. p12 certificate file issued for user John.

B. Shared secret properties of John's password.

C. VPN certificate properties of the John's gateway.

D. Expired. p12 certificate properties for user John.

Answer: A (LEAVE A REPLY)

Explanation

The answer is A because the graphic shows the properties of a personal .p12 certificate file issued for user John. A .p12 file is a file format that contains a user's private key and public key certificate. The graphic shows that the certificate file is valid and has an expiration date of 07-Apr-2018. The graphic also shows that the certificate file is issued by an internal CA, which is a Check Point component that manages certificates for users and gateways.References: Check Point R81 Certificate Management, Check Point R81 Internal CA

NEW QUESTION: 285

What is the default tracking option of a rule?

A. Tracking

B. Log

C. None

D. Alert

Answer: B (LEAVE A REPLY)

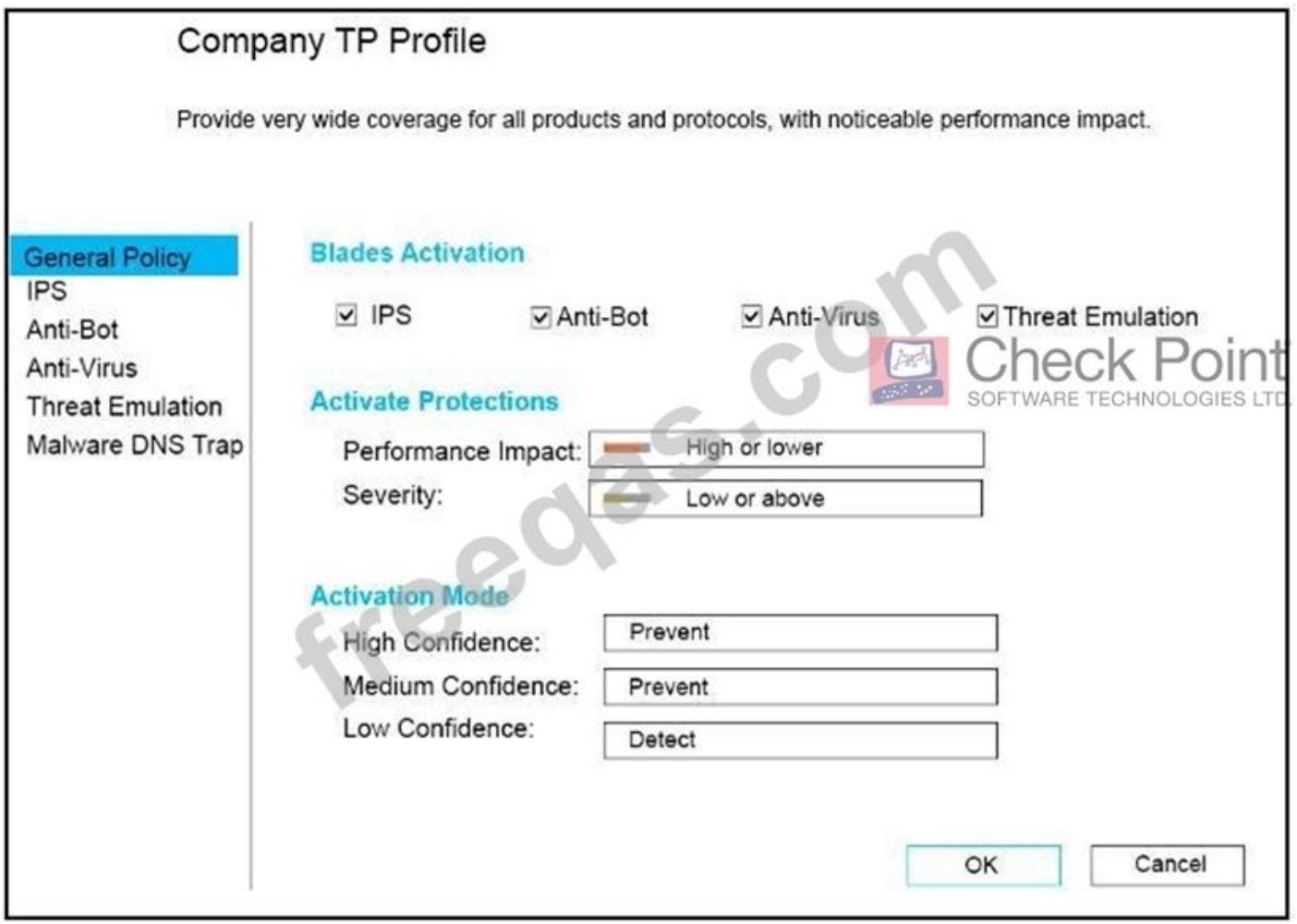
Explanation

The default tracking option of a rule is Log3. This means that the Security Gateway will generate a log entry for every connection that matches the rule. The log entry will contain information such as source, destination, service, action, and time. Other tracking options include None, Alert, Mail, SNMP Trap, User Alert, and Accounting. References: Check Point R81 Firewall Administration Guide

NEW QUESTION: 286

CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings.

The following Threat Prevention Profile has been created.



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 Profile. Consider adding more memory to the appliance.

D. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B (LEAVE A REPLY)

Explanation

The BEST way to tune the profile in order to lower the CPU load still maintaining security at good level is to set the Performance Impact to Medium or lower. This will reduce the number of packets that are inspected by the Threat Prevention blades, while still providing a high level of protection . Setting High Confidence to Low and Low Confidence to Inactive will lower the security level, as it will allow more traffic that may be malicious. The problem is likely with the Threat Prevention Profile, as it can have a significant

impact on the CPU utilization of the Security Gateway. Adding more memory to the appliance will not solve the problem, as memory is not the bottleneck in this case. Setting the Performance Impact to Very Low Confidence to Prevent will increase the CPU load, as it will inspect more packets and block more traffic that may be false positives.
References: Threat Prevention Administration Guide, Check Point R81.10

NEW QUESTION: 287
If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?
A. Log Implied Rule was not selected on Global Properties.
B. Log Implied Rule was not set correctly on the track column on the rules base.
C. Track log column is set to none.
D. Track log column is set to Log instead of Full Log.
Answer: A (LEAVE A REPLY)
Implied Rules are configured only on Global Properties.

NEW QUESTION: 288
What is the best sync method in the ClusterXL deployment?
A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
D. Use 2 clusters + 1st sync + 2nd sync
Answer: B (LEAVE A REPLY)
Explanation
The best sync method in the ClusterXL deployment is to use one dedicated sync interface56. This method provides optimal performance and reliability for synchronization traffic. Using multiple sync interfaces is not recommended as it increases CPU load and does not provide 100% sync redundancy5. Using multiple clusters is not a sync method, but a cluster topology. References: Sync Redundancy in ClusterXL, Best Practice for HA sync interface

NEW QUESTION: 289
What is the purpose of the Stealth Rule?
A. To prevent users from directly connecting to a Security Gateway.
B. To reduce the number of rules in the database.
C. To reduce the amount of logs for performance issues.
D. To hide the gateway from the Internet.
Answer: (SHOW ANSWER)

Explanation
The Stealth Rule is used to prevent users from directly connecting to a Security Gateway. It is usually placed at the top of the rule base, before any other rule that allows traffic to the Security Gateway1, p. 32.
References: Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 290
Which one of the following is TRUE?
A. Inline layer can be defined as a rule action
B. Ordered policy is a sub-policy within another policy
C. Pre-R81 Gateways do not support ordered layers
D. One policy can be either inline or ordered, but not both
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
When changes are made to a Rule base, it is important to _____ to enforce changes.
A. Publish database
B. Activate policy
C. Install policy
D. Save changes
Answer: A (LEAVE A REPLY)
Explanation
When changes are made to a Rule base, it is important to to enforce changes5. Publishing database saves the changes to the database and makes them available to other administrators. Installing policy applies the changes to the Security Gateways.
References: Check Point R81 Security Management Administration Guide, [Check Point R81 SmartConsole R81 Resolved Issues], [Check Point R81 Firewall Administration Guide]

NEW QUESTION: 292
Fill in the blank: Once a license is activated, a _____ should be installed.
A. Security Gateway Contract file
B. Service Contract file
C. License Contract file
D. License Management file
Answer: (SHOW ANSWER)
NEW QUESTION: 293
How many users can have read/write access in Gaia at one time?
A. Two
B. Three
C. One
D. Infinite
Answer: C (LEAVE A REPLY)

NEW QUESTION: 294
Which tool allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS?
A. CPUSE - Check Point Upgrade Service Engine
B. CPDAS - Check Point Deployment Agent Service
C. CPAUE - Check Point Automatic Update Engine
D. CPASE - Check Point Automatic Service Engine
Answer: (SHOW ANSWER)

NEW QUESTION: 295
R80.10 management server can manage gateways with which versions installed?
A. Versions R77 and higher
B. Versions R75.20 and higher
C. Versions R76 and higher
D. Version R75 and higher
Answer: C (LEAVE A REPLY)

NEW QUESTION: 296
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 (LEAVE A REPLY)
Explanation
When tunnel test packets no longer invoke a response, SmartView Monitor displays Down for the given VPN tunnel1. This means that the VPN tunnel is not operational and there is no IKE or IPsec traffic passing through it. No Response, Inactive, and Failed are not valid statuses for VPN tunnels in SmartView Monitor.
References: Smart View Monitor displays status for all S2S VPN tunnels - Phase1 UP

NEW QUESTION: 297
True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.
A. True, every administrator works on a different database that Is independent of the other administrators
B. False, this feature has to be enabled in the Global Properties.
C. True, every administrator works in a session that is independent of the other administrators
D. False, only one administrator can login with write permission
Answer: C (LEAVE A REPLY)
Multiple R/W admins can log into SmartConsole and edit rules but they can't edit a rule that is being worked on by another admin.

NEW QUESTION: 298

Name the pre-defined Roles included in Gaia OS.

A. AdminRole, and MonitorRole

B. ReadWriteRole, and ReadyOnly Role

C. AdminRole, cloningAdminRole, and Monitor Role

D. AdminRole

Answer: A (LEAVE A REPLY)

Explanation

The pre-defined Roles included in Gaia OS are AdminRole and MonitorRole. AdminRole is the role that has full access to all Gaia features and commands. MonitorRole is the role that has read-only access to Gaia features and commands1. The other options are not valid pre-defined Roles in Gaia OS.

NEW QUESTION: 299

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible explanation for this?

A. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

B. Another administrator is logged into the Management and currently editing the DNS Rule.

C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.

Answer: (SHOW ANSWER)

NEW QUESTION: 300

URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

A. WebCheck

B. UserCheck

C. Harmony Endpoint

D. URL categorization

Answer: B (LEAVE A REPLY)

Explanation

URL Filtering employs a technology called UserCheck, which educates users on web usage policy in real time. UserCheck is a feature that allows the firewall to interact with the users and inform them about the web usage policy and its violations. UserCheck can also allow users to request access to blocked websites or report false positives. UserCheck helps users understand and comply with the web usage policy and reduces the workload of the administrators.

NEW QUESTION: 301
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 SmartLog and query for the IP address of the Manager's tablet
B. Open SmartLog and connect remotely to the IP of the wireless controller
C. Open SmartView Tracker and filter the logs for the IP address of the tablet
D. Open SmartView Tracker and check all the IP logs for the tablet
Answer: (SHOW ANSWER)
Explanation
SmartLog is a unified log viewer that provides fast and easy access to logs from all Check Point components3. It allows the administrator to query for any log field, such as the IP address of the tablet, and filter the results by time, severity, blade, action, and more4. SmartView Tracker is a legacy tool that displays network activity logs from Security Gateways and other Check Point devices. It does not support remote connection to the wireless controller or querying for specific IP addresses. References: SmartLog, SmartLog Queries, [SmartView Tracker]

NEW QUESTION: 302
Fill in the blank: It is Best Practice to have a _____ rule at the end of each policy layer.
A. Explicit Drop
B. Implicit Drop
C. Explicit CleanUp
D. Implied Drop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 303
Fill in the blank: The position of an implied rule is manipulated in the _____ window.
A. NAT
B. Firewall
C. Global Properties
D. Object Explorer
Answer: C (LEAVE A REPLY)
Explanation
The position of an implied rule is manipulated in the Global Properties window. Implied rules are predefined rules that are not

displayed in the rule base. They allow or block traffic for essential services such as communication with Check Point servers, logging, and VPN traffic. The position of an implied rule can be changed in the Global Properties > Firewall > Implied Rules section56.
References: How to view Implied Rules in R80.x / R81.x SmartConsole, Implied Rules

NEW QUESTION: 304
Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.
A. Main
B. Quick
C. High Alert
D. Authentication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
Which command can you use to enable or disable multi-queue per interface?
A. Cpmq config
B. cpmq set
C. Set cpmq enable
D. Cpmqueue set
Answer: B (LEAVE A REPLY)

NEW QUESTION: 306
Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for what components?
A. The Security Gateway (SG) and Security Management Server (SMS) software and the CPUSE engine.
B. Licensed Check Point products for the Gala operating system and the Gaia operating system itself.
C. The CPUSE engine and the Gaia operating system.
D. The Gaia operating system only.
Answer: B (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/CPUSE.htm

NEW QUESTION: 307
Which of the following is NOT a valid deployment option for R81?
A. Bridge Mode
B. All-in-one (stand-alone)
C. CloudGuard
D. Distributed
Answer: (SHOW ANSWER)

NEW QUESTION: 308
After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?
A. The gateways can only send logs to an SMS and cannot send logs to a Log Server. Log Servers are proprietary log archive servers.
B. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log

Server.
C. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
D. Logs are not automatically forwarded to a new Log Server. SmartConsole must be used to manually configure each gateway to send its logs to the server.
Answer: D (LEAVE A REPLY)
Explanation
Logs are not automatically forwarded to a new Log Server. SmartConsole must be used to manually configure each gateway to send its logs to the server. After adding a new Log Server and establishing the SIC trust with the SMS, the administrator must use SmartConsole to assign the Log Server to each gateway in the Logs and Masters section of the gateway properties2. The other options are not correct, as gateways can send logs to both SMS and Log Server, Log Servers are not proprietary log archive servers, and gateways will not detect the new Log Server after the next policy install.

NEW QUESTION: 309
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. Explicit
B. Firewall drop
C. Implied
D. Implicit accept
E. Implicit drop
Answer: C (LEAVE A REPLY)

NEW QUESTION: 310
To fully enable Dynamic Dispatcher on a Security Gateway:
A. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot
B. run fw ctl multik set_mode 1 in Expert mode and then reboot
C. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu
D. run fw ctl multik set_mode 9 in Expert mode and then reboot
Answer: D (LEAVE A REPLY)

NEW QUESTION: 311
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.
A. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
B. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?
A. Protections
B. IPS Protections
C. Profiles
D. ThreatWiki
Answer: (SHOW ANSWER)
Explanation
According to the Learn More About Threat Signatures4, to quickly review when Threat Prevention signatures were last updated, you can use the IPS Protections tool. This tool shows you the date and time of the last update, as well as the number of signatures and their categories. References: Learn More About Threat Signatures

NEW QUESTION: 313
In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?
A. Rule 1
B. Cleanup Rule
C. Blank field under Rule Number
D. Rule 0
Answer: D (LEAVE A REPLY)

NEW QUESTION: 314
What are the two types of NAT supported by the Security Gateway?
A. Hide and Static
B. Destination and Hide
C. Static and Source
D. Source and Destination
Answer: A (LEAVE A REPLY)

NEW QUESTION: 315
In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?
A. "Inspect", "Bypass"
B. "Inspect", "Bypass", "Categorize"
C. "Inspect", "Bypass", "Block"
D. "Detect", "Bypass"
Answer: A (LEAVE A REPLY)
Explanation
The actions available in the "Actions" column of a rule in HTTPS Inspection policy are "Inspect" and "Bypass". "Inspect" means that the HTTPS traffic will be decrypted and inspected according to the Access Control policy. "Bypass" means that the HTTPS traffic will not be decrypted and will be allowed without inspection1. The other options are not valid actions for HTTPS Inspection policy.

NEW QUESTION: 316

In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

A. Different computers or appliances.

B. The same computer or appliance.

C. Both on virtual machines or both on appliances but not mixed.

D. In Azure and AWS cloud environments.

Answer: (SHOW ANSWER)

"The Security Management ServerClosed (1) and the Security GatewayClosed (3) are installed on different computers, with a network connection (2)." https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Getting-Started.htm

NEW QUESTION: 317

Fill in the blanks: A Security Policy is created in_____, stored in the_____ and Distributed to the various

A. SmartConsole, Security Gateway, Security Management Servers

B. Rule base. Security Management Server Security Gateways

C. The Check Point database. SmartConsole, Security Gateways

D. SmartConsole, Security Management Server, Security Gateways

Answer: D (LEAVE A REPLY)

NEW QUESTION: 318

Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

A. SmartEvent

B. SmartView Tracker

C. SmartLog

D. SmartView Monitor

Answer: A (LEAVE A REPLY)

Explanation

SmartEvent is a unified security management solution that provides real-time visibility into security events across the network. SmartEvent shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns, as well as generate reports and alerts based on predefined or customized indicators.

SmartView Tracker, SmartLog, and SmartView Monitor are other SmartConsole applications that can show logs, search queries, and network statistics respectively, but they do not provide the same level of correlation and analysis as SmartEvent. References: [Check Point R81 SmartEvent Administration Guide]

NEW QUESTION: 319
Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?
A. Manual NAT can offer more flexibility than Automatic NAT.
B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
D. Automatic NAT can offer more flexibility than Manual NAT.
Answer: A (LEAVE A REPLY)
Explanation
Manual NAT can offer more flexibility than Automatic NAT because it allows the administrator to define the NAT rules in any order and position1. Automatic NAT creates the NAT rules automatically and places them at the top or bottom of the NAT Rule Base2.
References: Check Point R81 Firewall Administration Guide, Check Point R81 Security Management Administration Guide

NEW QUESTION: 320
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: (SHOW ANSWER)
Explanation
The SIC Status "Unknown" means that there is no connection between the gateway and Security Management Server. This can happen if the gateway is down, unreachable, or has not been initialized yet12.
References: Check Point R81 Security Management Administration Guide, Free Check Point CCSA Sample Questions and Study Guide

NEW QUESTION: 321
Which icon in the WebUI indicates that read/write access is enabled?
A. Pencil
B. Padlock
C. Book
D. Eyeglasses
Answer: A (LEAVE A REPLY)
Explanation
The icon in the WebUI that indicates that read/write access is enabled is the Pencil icon . The Pencil icon appears next to the name of the device when it is in Read/Write mode, which allows making changes to the configuration. The Padlock icon indicates that read-only access is enabled, which prevents making changes to the configuration. The Book icon indicates that online help is available, which provides information and guidance on using the WebUI. The Eyeglasses icon indicates that a view-only mode is enabled, which allows viewing the configuration without logging in.
References: Gaia R81.10 Administration Guide, WebUI Overview

NEW QUESTION: 322

To view statistics on detected threats, which Threat Tool would an administrator use?
A. Protections
B. IPS Protections
C. Profiles
D. ThreatWiki
Answer: D (LEAVE A REPLY)
Explanation
ThreatWiki is a web-based tool that provides statistics on detected threats, such as attack types, sources, destinations, and severity. It also allows the administrator to search for specific threats and view their details and mitigation methods. The other options are not tools for viewing statistics on detected threats. References:
[ThreatWiki], [ThreatWiki - Threat Emulation]

NEW QUESTION: 323
Which of the following is NOT a back up method?
A. Save backup
B. System backup
C. snapshot
D. Migrate
Answer: A (LEAVE A REPLY)
The built-in Gaia backup procedures:
Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.

NEW QUESTION: 324
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. Intrusion Detection System (IDS) Policy install
C. SAM - Suspicious Activity Rules feature of SmartView Monitor
D. Block Intruder feature of SmartView Tracker
Answer: D (LEAVE A REPLY)

NEW QUESTION: 325
Which one of the following is a way that the objects can be manipulated using the new API integration in R81 Management?
A. RC4 Encryption
B. JSON
C. Microsoft Word
D. Microsoft Publisher
Answer: (SHOW ANSWER)

NEW QUESTION: 326

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

A. Phase two key negotiation

B. User data base corruption

C. Address translation

D. Log Consolidation Engine

Answer: (SHOW ANSWER)

NEW QUESTION: 327

How Capsule Connect and Capsule Workspace differ?

A. Capsule Connect does not require an installed application at client

B. Capsule Workspace can provide access to any application

C. Capsule Connect provides Business data isolation

D. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications

Answer: D (LEAVE A REPLY)

NEW QUESTION: 328

What is the default shell for the command line interface?

A. Clish

B. Admin

C. Normal

D. Expert

Answer: (SHOW ANSWER)

NEW QUESTION: 329

How many layers make up the TCP/IP model?

A. 2

B. 7

C. 4

D. 6

Answer: (SHOW ANSWER)

NEW QUESTION: 330

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 (LEAVE A REPLY)

Explanation

If the NAT property 'Translate destination on client side' is not enabled in Global properties, nothing needs to be configured on the client side, because the Gateway takes care of all details necessary. The Gateway translates the destination IP address before

sending the packet to the client, so the client does not need to know about the NAT rule or add any host route or ARP entry.
References: Check Point Security Engineering Study Guide, p. 136-137

NEW QUESTION: 331
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. Create a Suspicious Activity Rule in Smart Monitor.
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. Add a temporary rule using SmartDashboard and select hide rule.
Answer: (SHOW ANSWER)

NEW QUESTION: 332
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. Traffic is still allowed but not accelerated
B. The traffic is originating from the gateway itself
C. The connection required a Security server
D. Acceleration is not enabled
Answer: (SHOW ANSWER)

NEW QUESTION: 333
One of major features in R81.x SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?
A. AdminA, AdminB and AdminC are editing three different rules at the same time.
B. AdminA and AdminB are editing the same rule at the same time.
C. AdminB sees a pencil icon next the rule that AdminB is currently editing.
D. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
You want to store the GAiA configuration in a file for later reference.
What command should you use?
A. write mem <filename>
B. show config -f <filename>
C. save config -o <filename>
D. save configuration <filename>
Answer: (SHOW ANSWER)

NEW QUESTION: 335
In which deployment is the security management server and Security Gateway installed on the same appliance?
A. Standalone
B. Remote
C. Distributed
D. Bridge Mode
Answer: A (LEAVE A REPLY)
Explanation
A standalone deployment is when the security management server and Security Gateway are installed on the same appliance. This is suitable for small or branch office environments1

NEW QUESTION: 336
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: 337
R81 is supported by which of the following operating systems:
A. Gaia, SecurePlatform, and Windows
B. SecurePlatform only

C. Windows only
D. Gaia only
Answer: D (LEAVE A REPLY)

NEW QUESTION: 338
Which of the following commands is used to monitor cluster members?
A. cphaprob state
B. cphaprob status
C. cphaprob
D. cluster state
Answer: A (LEAVE A REPLY)

NEW QUESTION: 339
Fill in the blanks: The _____ collects logs and sends them to the _____.
A. Log server; Security Gateway
B. Log server; security management server
C. Security management server; Security Gateway
D. Security Gateways; log server
Answer: (SHOW ANSWER)
Explanation
The Security Gateways collect logs and send them to the log server. The Security Gateways are the components that enforce the security policy on network traffic and generate logs for each connection that matches a rule with a tracking option. The log server is the component that receives and stores the logs from the Security Gateways and provides a centralized interface for viewing and analyzing them. The log server can be either a dedicated server or integrated with the Security Management Server. References: [Check Point R81 Security Management Administration Guide]

NEW QUESTION: 340
What are types of Check Point APIs available currently as part of R81.10 code?
A. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API
B. OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API
C. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
D. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
Answer: (SHOW ANSWER)

NEW QUESTION: 341
If an administrator wants to restrict access to a network resource only allowing certain users to access it, and only when they are on a specific network what is the best way to accomplish this?
A. Create an inline layer where the destination is the target network resource Define sub-rules allowing only specific sources to access the target resource
B. Use a "New Legacy User at Location", specifying the LDAP user group that the users belong to, at the desired location
C. Create a rule allowing only specific source IP addresses access to the target network resource.

D. Create an Access Role object, with specific users or user groups specified, and specific networks defined Use this access role as the "Source" of an Access Control rule

Answer: D (LEAVE A REPLY)

Explanation

The best way to restrict access to a network resource only allowing certain users to access it, and only when they are on a specific network, is to create an Access Role object, with specific users or user groups specified, and specific networks defined. Then, use this access role as the "Source" of an Access Control rule. This allows for granular control over network traffic based on user identity and location3.

References: 3: Check Point R81 Security Gateway Administration Guide, page 13.

NEW QUESTION: 342

What Identity Agent allows packet tagging and computer authentication?

A. Endpoint Security Client

B. Full Agent

C. Light Agent

D. System Agent

Answer: B (LEAVE A REPLY)

Explanation

The Full Identity Agent allows packet tagging and computer authentication2. Packet tagging is a feature that enables the Security Gateway to identify the source user and machine of each packet, regardless of NAT or routing. Computer authentication is a feature that enables the Security Gateway to authenticate machines that are not associated with any user, such as servers or unattended workstations. The other options are incorrect.

Endpoint Security Client is not an Identity Agent, but a software that provides endpoint security features such as firewall, antivirus, VPN, etc. Light Agent is an Identity Agent that does not require installation and runs on a web browser, but it does not support packet tagging or computer authentication. System Agent is not an Identity Agent, but a software that provides system information and health monitoring for endpoints.

References: Check Point Identity Agent for Microsoft Windows 10

NEW QUESTION: 343

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

A. Symmetrical IPSec key

B. Pre-shared secret

C. Diffie-Hellman Private Key

D. Diffie-Hellman Public Key

Answer: (SHOW ANSWER)

NEW QUESTION: 344

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 suspicious?

A. SmartView Tracker

B. SmartView Status
C. SmartUpdate
D. SmartDashboard
Answer: (SHOW ANSWER)

NEW QUESTION: 345
What are the advantages of a "shared policy" in R81?
A. Allows the administrator to share a policy so that it is available to use in another Policy Package
B. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway
C. Allows the administrator to share a policy between all the users identified by the Security Gateway
D. Allows the administrator to share a policy between all the administrators managing the Security Management Server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 346
What port is used for communication to the User Center with SmartUpdate?
A. CPMI 200
B. TCP 8080
C. HTTPS 443
D. HTTP 80
Answer: (SHOW ANSWER)

NEW QUESTION: 347
Secure Internal Communication (SIC) is handled by what process?
A. CPM
B. HTTPS
C. FWD
D. CPD
Answer: D (LEAVE A REPLY)
Explanation
Secure Internal Communication (SIC) is handled by the CPD process3. CPD is the Check Point Daemon that runs on all Check Point modules and handles internal licensing and SIC operations. SIC is a mechanism that ensures secure communication between Check Point components using certificates and encryption.
References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 348
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?
A. Threat Emulation
B. Threat Cloud
C. Mail Transfer Agent
D. Mobile Access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 349
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. Database Revision Control
C. GAiA backup utilities
D. upgrade_export command
Answer: (SHOW ANSWER)

NEW QUESTION: 350
The CDT utility supports which of the following?
A. Only major version upgrades to R81.10
B. All upgrades
C. Only Jumbo HFA's and hotfixes
D. Major version upgrades to R77.30
Answer: B (LEAVE A REPLY)

NEW QUESTION: 351
What is the default shell of Gaia CLI?
A. clish
B. Monitor
C. Read-only
D. Bash
Answer: (SHOW ANSWER)
Explanation
The default shell of Gaia CLI is clish, which stands for Check Point command line interface shell1. It provides a user-friendly interface to configure and manage Check Point products. References: Check Point Gaia Administration Guide

NEW QUESTION: 352
What is the purpose of a Stealth Rule?
A. A rule that allows administrators to access SmartDashboard from any device.
B. A rule used to hide a server's IP address from the outside world.

C. A rule at the end of your policy to drop any traffic that is not explicitly allowed.
D. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 353
Fill in the blank: Back up and restores can be accomplished through_____.
A. WebUI, CLI, or SmartUpdate
B. SmartUpdate, SmartBackup, or SmartConsole
C. SmartConsole, WebUI, or CLI
D. CLI, SmartUpdate, or SmartBackup
Answer: C (LEAVE A REPLY)

NEW QUESTION: 354
Which of the following is NOT an identity source used for Identity Awareness?
A. Remote Access
B. UserCheck
C. AD Query
D. RADIUS
Answer: (SHOW ANSWER)
Explanation
UserCheck is not an identity source used for Identity Awareness. UserCheck is a feature that allows you to interact with users when they trigger Data Loss Prevention or Threat Prevention incidents2. Identity Awareness uses different methods to acquire identities, such as AD Query, Identity Agent, Browser-Based Authentication, Terminal Servers, Captive Portal, and RADIUS3 . Therefore, the correct answer is B: UserCheck.

NEW QUESTION: 355
You want to set up a VPN tunnel to a external gateway. You had to make sure that the IKE P2 SA will only be established between two subnets and not all subnets defined in the default VPN domain of your gateway.
A. In the SmartConsole create a dedicated VPN Community for both Gateways. On the Management add the following line to the $FWDIR/conf/user.def.FWI file subnet_for_range_and_peer = {
<peerGW_IP,first_IP_in_range1,last_IP_in_the_range1; subnet_mask>);
B. In the SmartConsole create a dedicated VPN Community for both Gateways. Selecting the local gateway in the Community you can set the VPN Domain to 'User defined' and put in the local network.
C. In the SmartConsole create a dedicated VPN Community for both Gateways. On the Gateway add the following line to the $FWDIR/cont/user.def.FW1 file subnet_for_range_and_peer = {
<peerGW_IP,first_IP_in_range1,last_IP_in_the_range1;subnet_mask> };
D. In the SmartConsole create a dedicated VPN Community for both Gateways. Go to Security Policies / Access Control and create an in-line layer rule with source and destination containing the two networks used for the IKE P2 SA. Put the name of the Community in the VPN column.
Answer: B (LEAVE A REPLY)
Explanation

This answer is correct because this is the recommended way to configure a VPN tunnel between two subnets and not all subnets defined in the default VPN domain of your gateway1. By creating a dedicated VPN Community, you can specify the VPN peers and the encryption settings for the VPN tunnel2. By selecting the local gateway in the Community, you can set the VPN Domain to 'User defined' and put in the local network that you want to include in the VPN tunnel1. This way, you can limit the VPN traffic to the subnets that you want and avoid unnecessary encryption and decryption of other traffic.
The other answers are not correct because they are either outdated or incorrect ways to configure a VPN tunnel between two subnets. Answer A and C are outdated methods that involve editing the user.def file, which is not recommended and can cause problems with the VPN configuration3. Answer D is incorrect because creating an in-line layer rule with source and destination containing the two networks used for the IKE P2 SA will not affect the VPN tunnel establishment, but only the access control policy4. The VPN column in the rule is used to specify the VPN direction, not the VPN Community name4.
* How to configure a Site-to-Site VPN with a universal tunnel
* Site to Site VPN R81 Administration Guide - Check Point Software
* How to configure a Site-to-Site VPN with a 3rd-party remote gateway
* Access Control Policy R81 Administration Guide - Check Point Software

NEW QUESTION: 356
The competition between stateful inspection and proxies was based on performance, protocol support, and security. Considering stateful Inspections and Proxies, which statement is correct?
A. Stateful Inspection is limited to Layer 3 visibility, with no Layer 4 to Layer 7 visibility capabilities.
B. When it comes to performance, proxies were significantly faster than stateful inspection firewalls.
C. Proxies offer far more security because of being able to give visibility of the payload (the data).
D. When it comes to performance, stateful inspection was significantly faster than proxies.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 357
Which application is used for the central management and deployment of licenses and packages?
A. SmartProvisioning
B. SmartLicense
C. SmartUpdate
D. Deployment Agent
Answer: C (LEAVE A REPLY)
Reference:
topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_Installation_and_Upgrade_Guide/206206

NEW QUESTION: 358
Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?
A. IPS blade
B. Firewall Blade
C. IPSEC VPN Blade
D. Identity Awareness Blade
Answer: (SHOW ANSWER)

NEW QUESTION: 359
If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?
A. Track log column is set to none.
B. Track log column is set to Log instead of Full Log.
C. Log Implied Rule was not selected on Global Properties.
D. Log Implied Rule was not set correctly on the track column on the rules base.
Answer: (SHOW ANSWER)

NEW QUESTION: 360
What is true about the IPS-Blade?
A. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same
B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. in R80, IPS is managed by the Threat Prevention Policy
D. in R80, IPS Exceptions cannot be attached to "all rules"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 361
One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?
A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
B. AdminA and AdminB are editing the same rule at the same time.
C. AdminB sees a pencil icon next the rule that AdminB is currently editing.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.
Answer: A (LEAVE A REPLY)
In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions.
Reference:
http://downloads.checkpoint.com/dc/download.htm?ID=65846

NEW QUESTION: 362
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?
A. Accept all encrypted traffic

B. All Site-to-Site VPN Communities
C. All Connections (Clear or Encrypted)
D. Specific VPN Communities
Answer: (SHOW ANSWER)

NEW QUESTION: 363
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.
A. Symmetric routing
B. Failovers
C. Asymmetric routing
D. Anti-Spoofing
Answer: B (LEAVE A REPLY)
Explanation
The Sticky Decision Function (SDF) is required to prevent failovers in an Active-Active cluster. The SDF ensures that the same cluster member handles all connections that belong to a certain session. If the SDF is not enabled, different cluster members may handle different connections of the same session, which may cause a failover or a drop12. References: ClusterXL Administration Guide R81, Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 364
Which of the following is NOT an identity source used for Identity Awareness?
A. UserCheck
B. Remote Access
C. AD Query
D. RADIUS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 365
What technologies are used to deny or permit network traffic?
A. Stateful Inspection. Firewall Blade, and URL'Application Blade
B. Packet Filtenng. Stateful Inspection, and Application Layer Firewall
C. Firewall Blade. URL/Application Blade and IPS
D. Stateful Inspection. URL/Application Blade, and Threat Prevention
Answer: A (LEAVE A REPLY)
Explanation
The technologies that are used to deny or permit network traffic are Stateful Inspection, Firewall Blade, and URL/Application Blade. Stateful Inspection is a technology that inspects network traffic at the packet level and maintains the state and context of each connection. Firewall Blade is a software blade that enforces security policy and prevents unauthorized access to protected resources. URL/Application Blade is a software blade that enables administrators to control access to millions of websites and applications based on users, groups, and machines.
References: : Check Point R81 Security Gateway Administration Guide, page 9. : Check Point R81 Security Gateway Administration Guide, page 10. : Check Point R81 Security Gateway Administration Guide, page 12.

NEW QUESTION: 366
What is a reason for manual creation of a NAT rule?
A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway's external IP
Answer: D (LEAVE A REPLY)
Explanation
A reason for manual creation of a NAT rule is when the public IP-address is different from the gateway's external IP. This can happen when the gateway is behind another NAT device or firewall3 . References: Check Point R81 Security Gateway Administration Guide, Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 367
Fill in the blank: A(n)_____rule is created by an administrator and configured to allow or block traffic based on specified criteria.
A. Inline
B. Explicit
C. Implicit drop
D. Implicit accept
Answer: (SHOW ANSWER)
Explanation
An explicit rule is created by an administrator and configured to allow or block traffic based on specified criteria. Explicit rules are displayed in the Rule Base and can be modified by the administrator. References: Certified Security Administrator (CCSA) R81.20 Course Overview, page 12.

NEW QUESTION: 368
Fill in the blank: _____ is the Gaia command that turns the server off.
A. sysdown
B. exit
C. halt
D. shut-down
Answer: C (LEAVE A REPLY)
Explanation
halt is the Gaia command that turns the server off. This command shuts down the operating system and powers off the machine. Other commands that can be used to shut down the server are shutdown and poweroff.
References: [Gaia Administration Guide R80.40]

NEW QUESTION: 369
Which of the following is NOT a set of Regulatory Requirements related to Information Security?
A. PCI
B. HIPPA
C. Sarbanes Oxley (SOX)

D. ISO 37001
Answer: (SHOW ANSWER)

NEW QUESTION: 370
In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?
A. "Inspect", "Bypass"
B. "Inspect", "Bypass", "Categorize"
C. "Inspect", "Bypass", "Block"
D. "Detect", "Bypass"
Answer: A (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/HTTPS-Inspection.htm#HTTPS_Inspection_Policy

NEW QUESTION: 371
How many users can have read/write access in Gaia Operating System at one time?
A. One
B. Three
C. Two
D. Infinite
Answer: A (LEAVE A REPLY)
Explanation
Only one user can have read/write access in Gaia Operating System at one time2. This is to prevent conflicts and errors when multiple users try to modify the same configuration settings. References: Check Point Gaia Administration Guide

NEW QUESTION: 372
Which command shows the installed licenses?
A. cplic print
B. print cplic
C. fwlic print
D. show licenses
Answer: A (LEAVE A REPLY)
Explanation
The command that shows the installed licenses is cplic print. This command displays the license information on a Check Point server or Security Gateway. It shows the license type, expiration date, attached blades, etc.
The other options are incorrect. print cplic is not a valid command. fwlic print is not a valid command. show licenses is not a valid command. References: [How to check license status on SecurePlatform / Gaia from CLI]

NEW QUESTION: 373
Why is a Central License the preferred and recommended method of licensing?
A. Central Licensing is actually not supported with Gaia.
B. Central Licensing is the only option when deploying Gaia

C. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
D. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/The_Check_Point_ThreatCloud.htm

NEW QUESTION: 374
Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?
A. Threat Emulation
B. Logging and Status
C. Application Control
D. Monitoring
Answer: D (LEAVE A REPLY)

NEW QUESTION: 375
The IT Management team is interested in the new features of the Check Point R81 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R81 because it is so different.
As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?
A. R81 Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R81.
B. R81 Management cannot manage earlier versions of Check Point Gateways prior to R81. Only R81 and above Gateways can be managed. Consult the R81 Release Notes for more information.
C. R81 Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R81. Consult the R81 Release Notes for more information.
D. R81 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R81. Consult the R81 Release Notes for more information.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 376
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?
A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade
Answer: (SHOW ANSWER)
Explanation
The Advanced Networking Blade is NOT subscription-based and therefore does not have to be renewed on a regular basis1011. The Advanced Networking Blade provides advanced routing capabilities such as BGP, OSPF, VRRP, and multicast routing10. The other blades are subscription-based and require annual renewal to receive updates and support from Check Point1012.
References: Check Point License Guide, IPS Software Blade contracts, Product Catalog

NEW QUESTION: 377
AdminA and AdminB are both logged in on SmartConsole What does it mean if AdmmB sees a lock icon on a rule? Choose the BEST answer.
A. Rule is locked by AdminA and will be made available if the session is published
B. Rule is locked by AdminA because the rule is currently being edited
C. Rule is locked by AdminA and if the session is saved, the rule will be made available
D. Rule is locked by AdminA because the save button has not been pressed
Answer: (SHOW ANSWER)
Explanation
If AdminB sees a lock icon on a rule, it means that the rule is locked by AdminA and will be made available if the session is published. A session is a set of changes made by an administrator in SmartConsole. A session can be published to save and share the changes with other administrators, or discarded to cancel the changes and unlock the objects1.
References: 1: Check Point R81 Security Management Administration Guide, page 18.

NEW QUESTION: 378
Fill in the blank: To create policy for traffic to or from a particular location, use the _____.
A. DLP shared policy
B. HTTPS inspection
C. Geo policy shared policy
D. Mobile Access software blade
Answer: C (LEAVE A REPLY)

NEW QUESTION: 379
Which component functions as the Internal Certificate Authority for R77?
A. SmartLSM
B. Management Server
C. Policy Server
D. Security Gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 380
John is the administrator of a R81 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole.

To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

A. Publish the session

B. Install database

C. File > Save

D. Logout of the session

Answer: A (LEAVE A REPLY)

NEW QUESTION: 381

Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

A. Specific VPN Communities

B. All Connections (Clear or Encrypted)

C. Accept all encrypted traffic

D. All Site-to-Site VPN Communities

Answer: A (LEAVE A REPLY)

NEW QUESTION: 382

Check Point licenses come in two forms. What are those forms?

A. Central and Local.

B. Access Control and Threat Prevention.

C. On-premise and Public Cloud.

D. Security Gateway and Security Management.

Answer: (SHOW ANSWER)

Explanation

Check Point licenses come in two forms: central and local. Central licenses are attached to the Security Management Server and are distributed to managed Security Gateways. Local licenses are attached directly to a specific Security Gateway.

NEW QUESTION: 383

Which single Security Blade can be turned on to block both malicious files from being downloaded as well as block websites known to host malware?

A. Anti-Virus

B. Anti-Bot

C. None - both URL Filtering and Anti-Virus are required for this.

D. None - both Anti-Virus and Anti-Bot are required for this

Answer: C (LEAVE A REPLY)

NEW QUESTION: 384

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 (LEAVE A REPLY)
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:

NEW QUESTION: 385
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?
A. show interfaces
B. show interfaces detail
C. show configuration interface
D. ifconfig -a
Answer: C (LEAVE A REPLY)

NEW QUESTION: 386
Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client
A. Destination
B. Identity
C. Payload
D. Location
Answer: B (LEAVE A REPLY)
How RADIUS Accounting Works with Identity Awareness
RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.

NEW QUESTION: 387
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.
A. Concurrent policy packages
B. Concurrent policies
C. Global Policies
D. Shared policies
Answer: (SHOW ANSWER)
"The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/SmartConsole-Toolbars-Shared-Policies.htm

NEW QUESTION: 388
Name one limitation of using Security Zones in the network?
A. Security zones will not work in Automatic NAT rules
B. Security zone will not work in Manual NAT rules
C. Security zones will not work in firewall policy layer
D. Security zones cannot be used in network topology
Answer: (SHOW ANSWER)

Explanation
One limitation of using Security Zones in the network is that Security Zones will not work in Manual NAT rules. Manual NAT rules are rules that explicitly define how to translate the source and destination IP addresses and ports of each connection. Manual NAT rules do not support using Security Zones as objects, only network objects or groups. Automatic NAT rules are rules that automatically define how to translate the source and destination IP addresses and ports of each connection based on the network objects or groups properties. Automatic NAT rules support using Security Zones as objects. Security Zones can also work in firewall policy layer and network topology.References: [Security Zones Best Practices], [NAT Methods]

NEW QUESTION: 389
Which of the following is NOT a valid deployment option for R80?
A. All-in-one (stand-alone)
B. Log server
C. Multi-domain management server
D. SmartEvent
Answer: C (LEAVE A REPLY)

NEW QUESTION: 390
What object type would you use to grant network access to an LDAP user group?
A. SmartDirectory Group
B. Access Role
C. User Group
D. Group Template
Answer: C (LEAVE A REPLY)

NEW QUESTION: 391
Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n) _____ Server.
A. SecurID
B. LDAP
C. NT domain
D. SMTP
Answer: B (LEAVE A REPLY)
Explanation
With the User Directory Software Blade, you can create user definitions on a(n) LDAP Server2. LDAP stands for Lightweight Directory Access Protocol and is a protocol for accessing and managing user information stored in a directory service. The User Directory Software Blade enables integration with LDAP servers such as Microsoft Active Directory, Novell eDirectory, and OpenLDAP.
References: Check Point R81 Identity Awareness Administration Guide

NEW QUESTION: 392
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.
A. Shared policy packages
B. Concurrent policy packages
C. Concurrent policies
D. Shared policies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 393
Which of the following is NOT an advantage to using multiple LDAP servers?
A. Information on a user is hidden, yet distributed across several servers
B. You gain High Availability by replicating the same information on 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)

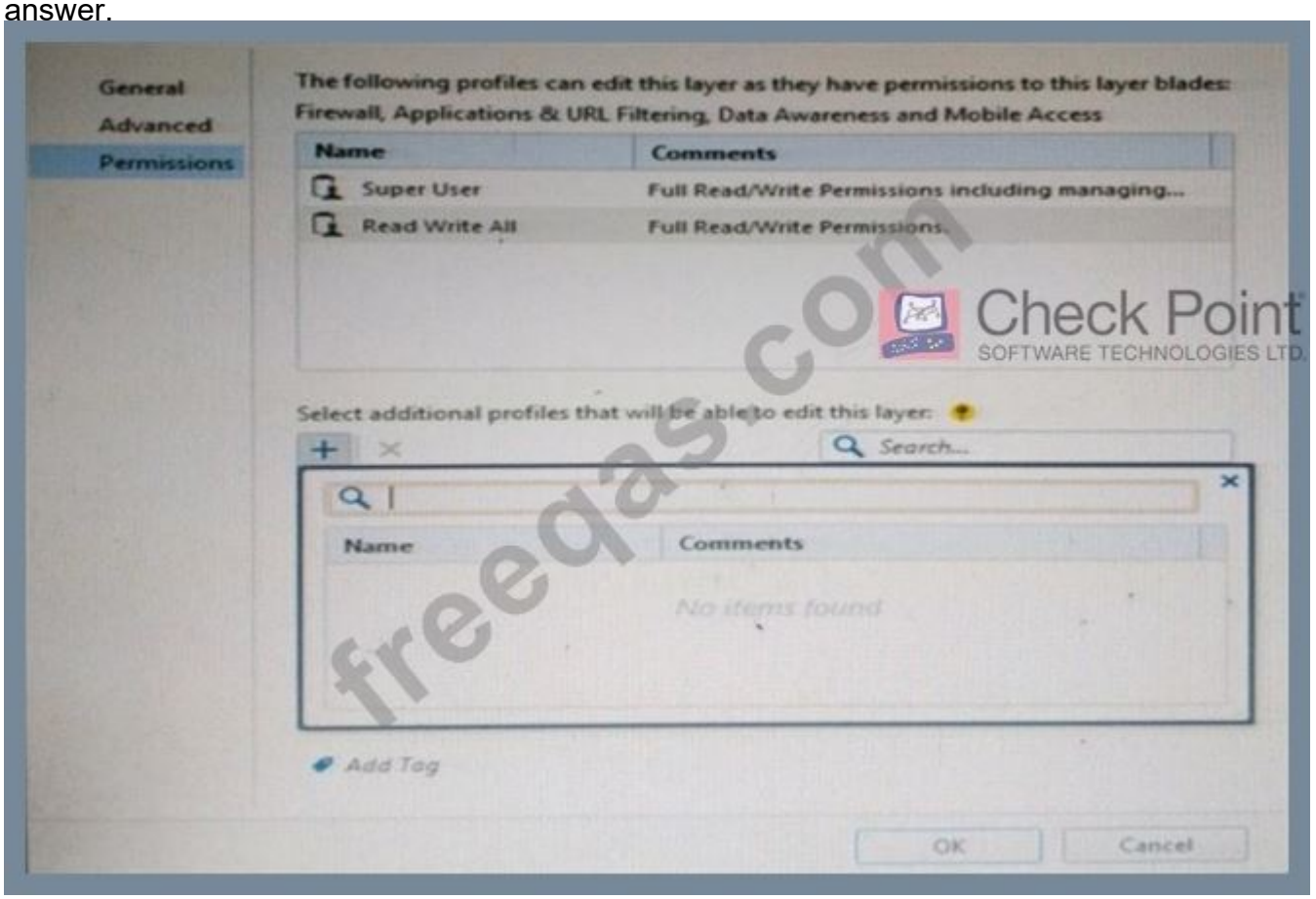
NEW QUESTION: 394
The Captive Portal tool:
A. Acquires identities from unidentified users.
B. Is deployed from the Identity Awareness page in the Global Properties settings.
C. Is only used for guest user authentication.
D. Allows access to users already identified.
Answer: (SHOW ANSWER)

NEW QUESTION: 395
If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer
A. Save and install the Policy
B. Delete older versions of database
C. Revert the session.
D. Publish or discard the session
Answer: (SHOW ANSWER)
Explanation
If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, the administrator who locked the objects must publish or discard the session to make them available to other administrators. Publishing or discarding the session will save or discard the changes made by the administrator and unlock the objects for editing by others3.

References: 3: Check Point R81 Security Management Administration Guide, page 18.

NEW QUESTION: 396
Which of the following is NOT a valid option when configuring access for Captive Portal?
A. According to the Firewall Policy
B. Through internal interfaces
C. From the Internet
D. Through all interfaces
Answer: C (LEAVE A REPLY)

NEW QUESTION: 397
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. There are no permission profiles available and you need to create one first.
B. All permission profiles are in use.
C. "Edit layers by Software Blades" is unselected in the Permission Profile
D. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.
Answer: (SHOW ANSWER)

NEW QUESTION: 398
Fill in the blank: An Endpoint identity agent uses a _____ for user authentication.

A. Shared secret
B. Token
C. Username/password or Kerberos Ticket
D. Certificate
Answer: (SHOW ANSWER)
Explanation
An Endpoint identity agent uses a username/password or Kerberos ticket for user authentication3, p. 28. An Endpoint identity agent is a lightweight client installed on endpoint computers that communicates with Identity Awareness gateways and provides reliable identity information. An Endpoint identity agent does not use a shared secret, a token, or a certificate for user authentication.
References: Check Point CCSA - R81:
Practice Test & Explanation, [Check Point Identity Awareness Administration Guide R81]

NEW QUESTION: 399
What is the SOLR database for?
A. Enables powerful matching capabilities and writes data to the database
B. Writes data to the database and full text search
C. Used for full text search and enables powerful matching capabilities
D. Serves GUI responsible to transfer request to the DLE server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 400
Access roles allow the firewall administrator to configure network access according to:
A. remote access clients.
B. a combination of computer or computer groups and networks.
C. users and user groups.
D. All of the above.
Answer: (SHOW ANSWER)
Explanation
Access roles allow the firewall administrator to configure network access according to remote access clients, a combination of computer or computer groups and networks, and users and user groups12. Therefore, the correct answer is D.

NEW QUESTION: 401
Which path below is available only when CoreXL is enabled?
A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path
Answer: C (LEAVE A REPLY)

NEW QUESTION: 402
Which of the following uses the same key to decrypt as it does to encrypt?

A. Certificate-based encryption
B. Symmetric encryption
C. Asymmetric encryption
D. Dynamic encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 403
Which GUI tool can be used to view and apply Check Point licenses?
A. cpconfig
B. Management Command Line
C. SmartConsole
D. SmartUpdate
Answer: (SHOW ANSWER)
SmartUpdate GUI is the recommended way of managing licenses.

NEW QUESTION: 404
AdminA and AdminB are both logged in on SmartConsole What does it mean if AdmmB sees a lock icon on a rule? Choose the BEST answer.
A. Rule is locked by AdminA because the rule is currently being edited
B. Rule is locked by AdminA and if the session is saved, the rule will be made available
C. Rule is locked by AdminA because the save button has not been pressed
D. Rule is locked by AdminA and will be made available if the session is published
Answer: D (LEAVE A REPLY)

NEW QUESTION: 405
Core Protections are installed as part of what Policy?
A. Access Control Policy.
B. Desktop Firewall Policy
C. Mobile Access Policy.
D. Threat Prevention Policy.
Answer: (SHOW ANSWER)
Explanation
Core Protections are installed as part of the Threat Prevention Policy. Core Protections are a set of IPS protections that are essential for securing your network against malicious traffic4. The other policies do not include Core Protections.
References: 1: Check Point CLI Reference Card 2: Anti-Spoofing 3: SmartView Tracker 4: Core Protections

NEW QUESTION: 406
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 (LEAVE A REPLY)

Explanation

To enforce the Security Policy correctly, a Security Gateway requires awareness of the network topology.

This means that the gateway knows which networks and interfaces are internal and external, and how to route packets between them . References: [Check Point R81 Security Gateway Technical Administration Guide], Check Point CCSA - R81: Practice Test & Explanation

NEW QUESTION: 407

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

A. SmartUpdate > Edit Security Management Server Object > SIC

B. SmartUpdate > Edit Gateway Object > Communication

C. SmartDashboard > Edit Security Management Server Object > SIC

D. SmartDashboard > Edit Gateway Object > General Properties > Communication

Answer: (SHOW ANSWER)

NEW QUESTION: 408

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"

B. On the firewall object, Legacy Authentication screen, check "Enable Identity Captive Portal"

C. In the Captive Portal screen of Global Properties, check "Enable Identity Captive Portal"

D. On the Security Management Server object, check the box "Identity Logging"

Answer: A (LEAVE A REPLY)

NEW QUESTION: 409

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 task. Check Point will make use of the newly installed CPU and Cores
D. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy
Answer: (SHOW ANSWER)

NEW QUESTION: 410
View the rule below. What does the pen-symbol in the left column mean?

A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is present. Click the pen symbol in order to gain the lock.
Answer: B (LEAVE A REPLY)
Explanation
The pen-symbol in the left column means that the rules have been edited by the logged in administrator, but the policy has not been published yet. It indicates that the changes are not yet effective and can be discarded.References: Policy Editor, Publishing Changes

NEW QUESTION: 411
To view the policy installation history for each gateway, which tool would an administrator use?
A. Gateway history
B. Revisions
C. Gateway installations
D. Installation history
Answer: D (LEAVE A REPLY)