CheckPoint.156-315.81.v2024-08-24.q369

Exam Code:	156-315.81
Exam Name:	Check Point Certified Security Expert R81
Certification Provider:	CheckPoint
Free Question Number:	369
Version:	v2024-08-24
# of views:	1899
# of Questions views:	3690
https://www.freeqas.com/qa/CheckPoint/156-315.81/CheckPoint.156-315.81.v2024-08-24.q369.html	

NEW QUESTION: 1
Which components allow you to reset a VPN tunnel?
A. vpn tu command or SmartView monitor
B. delete vpn ike sa or vpn she11 command
C. vpn tunnelutil or delete vpn ike sa command
D. SmartView monitor only
Answer: (SHOW ANSWER)
Explanation
The vpn tu command and the SmartView Monitor are two components that allow you to reset a VPN tunnel.
The vpn tu command is a command-line tool that lets you view and manage the status of VPN tunnels on a Security Gateway or cluster member. The SmartView Monitor is a graphical tool that lets you monitor the network and security performance, view VPN tunnel status, and reset VPN tunnels. Both components can be used to reset a VPN tunnel by selecting the option to delete IKE SA or IPsec SA for a specific peer or all peers. References: R81 VPN Administration Guide, page 29-30; R81 SmartConsole R81 Resolved Issues, sk170114

NEW QUESTION: 2
IF the first packet of an UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), what message is sent back through the kernel?
A. TCP FIN
B. Nothing
C. ICMP unreachable
D. TCP RST
Answer: (SHOW ANSWER)

NEW QUESTION: 3
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)
Explanation
According to the Check Point R81 training course, the medium path is available only when CoreXL is enabled. CoreXL is a performance-enhancing technology that allows multiple CPU cores to process traffic simultaneously. The medium path handles packets that require deeper inspection or content awareness, such as IPS, Anti-Virus, or URL Filtering. The other paths are either available regardless of CoreXL or not valid terms. References: Certified Security Expert (CCSE) R81.20 Course Overview

NEW QUESTION: 4
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?
A. None, Security Management Server would be installed by itself.
B. SmartConsole
C. SecureClient
D. Security Gateway
E. SmartEvent
Answer: D (LEAVE A REPLY)
Explanation
When doing a Stand-Alone Installation, you would install the Security Management Server with the Security Gateway as the other Check Point architecture component. A Stand-Alone Installation is where the Security Management Server and the Security Gateway are installed on the same machine2. The other options are either not Check Point architecture components, or not suitable for a Stand-Alone Installation. References: Check Point R81 Installation and Upgrade Guide

NEW QUESTION: 5
Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?
A. The CoreXL FW instances assignment mechanism is based on IP Protocol type
B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
C. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
When using the Mail Transfer Agent, where are the debug logs stored?
A. $CPDIR/log/emaild elg
B. $FWDIR/log/mtad elg

C. $FWDIR/bin/emaild.mta. elg
D. /var/log/mail.mta elg
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Automation and Orchestration differ in that:
A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
B. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
C. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.
Answer: A (LEAVE A REPLY)
Explanation
Automation and Orchestration differ in that automation relates to codifying tasks, whereas orchestration relates to codifying processes. Automation is the process of converting manual tasks into executable scripts or programs that can be run by machines or software agents. Orchestration is the process of coordinating multiple automated tasks into a coherent workflow that achieves a desired outcome or goal. Orchestration can also involve integrating different systems, tools, and services through web service interactions such as XML and JSON. References: Check Point Security Expert R81 Course, Automation & Orchestration Administration Guide

NEW QUESTION: 8
Which view is NOT a valid CPVIEW view?
A. IDA
B. RAD
C. PDP
D. VPN
Answer: C (LEAVE A REPLY)
Explanation
PDP is not a valid CPVIEW view. CPVIEW is a command-line tool that shows the status of different system parameters, such as CPU, memory, disk, network, and firewall. The valid views are IDA, RAD, VPN, FW, QoS, and others. PDP is a process that handles identity awareness and authentication. References: Check Point R81 Gaia Administration Guide, Check Point Identity Awareness Administration Guide R81

NEW QUESTION: 9
What solution is Multi-queue intended to provide?
A. Improve the efficiency of traffic handling by SecureXL SNDs
B. Improve the efficiency of CoreXL Kernel Instances
C. Reduce the performance of network interfaces
D. Reduce the confusion for traffic capturing in FW Monitor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
You can access the ThreatCloud Repository from:
A. R81.20 SmartConsole and Application Wiki
B. Threat Prevention and Threat Tools
C. Threat Wiki and Check Point Website
D. R81.20 SmartConsole and Threat Prevention
Answer: (SHOW ANSWER)
Explanation
According to the Check Point R81 release notes, you can access the ThreatCloud Repository from R81.20 SmartConsole and Threat Prevention. The ThreatCloud Repository is a cloud-based service that provides real-time threat intelligence and updates to Check Point products. The other options are either outdated or nonexistent.
References: Check Point R81

NEW QUESTION: 11
Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI.
Which command should he use in CLI? (Choose the correct answer.)
A. remove database lock
B. The database feature has one command lock database override.
C. override database lock
D. The database feature has two commands lock database override and unlock database. Both will work.
Answer: (SHOW ANSWER)
Explanation
Ken can use either of the two commands lock database override or unlock database to obtain a configuration lock from another administrator on R81 Security Management Server via CLI. These commands allow him to override the existing lock and gain exclusive access to the database. He can also use the WebUI to perform the same action.
References: Training & Certification | Check Point Software, New Courses and Certificates for R81.10 - Check Point CheckMates

NEW QUESTION: 12
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 SmartConsole. Objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories, such as Network Object, Host, Gateway, Service, Time Object, Custom Application / Site, Limit, and Group.
A resource is a type of object that represents an application or content that is accessible through HTTP or HTTPS protocols. A resource can be used to define access rules for users who connect through Identity Awareness or Mobile Access blades.

NEW QUESTION: 13
You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?
A. import backup
B. migrate import
C. restore_backup
D. cp_merge
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?
A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
B. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OFF. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
D. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.
Answer: A (LEAVE A REPLY)
Explanation
The best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic is: Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON.
She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures. SecureXL is a technology that accelerates network traffic processing by offloading intensive operations from the Firewall kernel to a dedicated SecureXL device. However, this also means that some traffic might not be seen by fw monitor, which is a tool that captures packets at different inspection points in the Firewall kernel. Therefore, to ensure that fw monitor captures all traffic, SecureXL should be turned OFF before using fw monitor. The other suggestions are either incorrect or less effective in capturing traffic.

NEW QUESTION: 15
You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column How to fix it?
A. The Mobile Access Policy Source under Gateway properties Is set to Legacy Policy and not to Unified Access Policy.
B. The Mobile Access Blade is not enabled under Gateway properties.
C. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
D. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which is the correct order of a log flow processed by SmartEvent components?
A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client
Answer: D (LEAVE A REPLY)
Explanation
The correct order of a log flow processed by SmartEvent components is: Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client. The Firewall generates logs for traffic and security events. The Log Server receives and stores the logs from the Firewall. The Correlation Unit analyzes the logs and generates SmartEvent events based on predefined or custom rules. The SmartEvent Server Database stores the events generated by the Correlation Unit. The SmartEvent Client displays the events and reports from the SmartEvent Server Database. References: : Check Point Resource Library, Certified Security Expert (CCSE) R81.20 Course Overview, page 12; : Check Point Software, Training & Certification, SmartEvent Introduction.

NEW QUESTION: 17
What happen when IPS profile is set in Detect Only Mode for troubleshooting?
A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control

Answer: C (LEAVE A REPLY)
It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.
During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION: 18
Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?
A. Windows Management Instrumentation (WMI)
B. Hypertext Transfer Protocol Secure (HTTPS)
C. Lightweight Directory Access Protocol (LDAP)
D. Remote Desktop Protocol (RDP)
Answer: A (LEAVE A REPLY)
Explanation
Windows Management Instrumentation (WMI) is a protocol that allows remote management and monitoring of Windows systems. It is used by AD Query to connect to the Active Directory Domain Controllers and query them for user and computer information. AD Query uses WMI to get real-time updates on user logon events, group membership changes, and computer status changes. WMI is not the same as LDAP, which is a protocol for accessing and modifying directory services. HTTPS and RDP are also different protocols that are not used by AD Query.
References: Check Point R81 Identity Awareness Administration Guide, page 17

NEW QUESTION: 19
Fill in the blank: An identity server uses a _____ for user authentication.
A. One-time password
B. Shared secret
C. Certificate
D. Token
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Which statement is false in respect of the SmartConsole after upgrading the management server to R81.10?
A. Yes. You can download the SmartConsole directly from the Download Center
B. As far as you use version R80.40, no upgrade is needed due to compatibility mode
C. Yes, using CPUSE you can make the installer available in the Web Portal of the Management Server
D. Yes, the SmartConsole Upgrade package can be installed using CPUSE
Answer: B (LEAVE A REPLY)
Explanation
The statement that is false in respect of the SmartConsole after upgrading the management server to R81.10 is that as far as you use version R80.40, no upgrade is needed due to compatibility mode. This is false because SmartConsole R80.40 is not compatible with R81.10 management server and you need to upgrade your

SmartConsole to R81.10 as well. The other statements are true and valid ways to obtain the SmartConsole upgrade package. References: [Check Point Security Expert R81 Installation and Upgrade Guide], page 18.

NEW QUESTION: 21
Which features are only supported with R81.10 Gateways but not R77.x?
A. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. 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.
D. Time object to a rule to make the rule active only during specified times.
Answer: C (LEAVE A REPLY)
Explanation
The features that are only supported with R81.10 Gateways and not with R77.x are described in option C:
"C. 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."
This feature, known as Rule Base Layers, allows for greater flexibility and control in organizing and prioritizing security rules within the rule base.
Options A, B, and D do not specifically pertain to features introduced in R81.10 and are available in earlier versions as well.
References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 22
What is required for a certificate-based VPN tunnel between two gateways with separate management systems?
A. Mutually Trusted Certificate Authorities
B. Shared User Certificates
C. Shared Secret Passwords
D. Unique Passwords
Answer: A (LEAVE A REPLY)
Explanation
A certificate-based VPN tunnel between two gateways with separate management systems requires mutually trusted certificate authorities. This means that each gateway must have a certificate issued by a certificate authority (CA) that the other gateway trusts. The CA can be either an internal CA or an external CA. The CA issues certificates that contain the public key and identity information of the gateway. The gateway uses its private key to sign and encrypt the VPN traffic. The other gateway can verify the signature and decrypt the traffic using the public key in the certificate. This ensures the authenticity, integrity, and confidentiality of the VPN tunnel.
References:
Remote Access VPN R81.20 Administration Guide, page 12
DeepDive Webinar - R81.20 Seamless VPN Connection to Public Cloud, slide 9

NEW QUESTION: 23

What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?

A. new host name "New Host" ip-address "192.168.0.10"

B. set host name "New Host" ip-address "192.168.0.10"

C. create host name "New Host" ip-address "192.168.0.10"

D. add host name "New Host" ip-address "192.168.0.10"

Answer: D (LEAVE A REPLY)

Explanation

The API command to create a new host with the name "New Host" and IP address "192.168.0.10" is:

This command adds a host object with the specified name and IP address to the Check Point configuration.

References: Check Point documentation or training materials related to API commands.

NEW QUESTION: 24

Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine

B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine

C. Size of the $FWDIR/log folder of the target machine must be at least 30% of the size of the $FWDIR/log directory on the source machine

D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B (LEAVE A REPLY)

Explanation

One of the requirements for a successful upgrade using the Advanced Upgrade with Database Migration is that the size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine. This is to ensure that there is enough space to copy the log files from the source machine to the target machine during the upgrade process. References: Advanced Upgrade with Database Migration

NEW QUESTION: 25

Which of the following is NOT an internal/native Check Point command?

A. fwaccel on

B. fw ct1 debug

C. tcpdump

D. cphaprob

Answer: C (LEAVE A REPLY)

Explanation

The command tcpdump is not an internal/native Check Point command. It is a common command-line tool that captures and analyzes network traffic. The other commands are internal/native Check Point commands that perform various functions. For example:
fwaccel on enables SecureXL acceleration on the Security Gateway.
fw ctl debug sets the debug flags for the Firewall kernel module.
cphaprob displays the status and information about ClusterXL or VRRP members.
References: Check Point R81 CLI Reference Guide, pages 11, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27; Check Point R81 Gaia Administration Guide, page 9

NEW QUESTION: 26
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 basis. The Advanced Networking Blade is a software blade that provides advanced routing capabilities for Check Point Security Gateways. It supports dynamic routing protocols such as OSPF, BGP, RIP, and PIM, as well as features such as Policy-Based Routing (PBR), Multicast Routing, and IPv6 support. The Advanced Networking Blade is included in the Next Generation Firewall (NGFW) package and does not require a separate license.

NEW QUESTION: 27
Firewall polices must be configured to accept VRRP packets on the GAiA platform if it Firewall software. The Multicast destination assigned by the internet Assigned Number Authority (IANA) for VRRP is:
A. 224.0.0.18
B. 224 00 5
C. 224.0.0.102
D. 224.0.0.22
Answer: (SHOW ANSWER)
Explanation
The multicast destination assigned by the Internet Assigned Numbers Authority (IANA) for VRRP is 224.0.0.18. This is a reserved multicast address that is used by VRRP routers to communicate with each other and announce their priority and state. Firewall policies must be configured to accept VRRP packets on the Gaia platform if it runs Firewall software. Otherwise, VRRP packets will be dropped by default. References:
[Configuring VRRP on Gaia]

NEW QUESTION: 28
Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances.

Which the following command is NOT related to redundancy and functions?

A. cphaprob -a if

B. cphaprob all show stat

C. cphaprob -l list

D. cphaprob stat

Answer: B (LEAVE A REPLY)

NEW QUESTION: 29

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

A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt

B. mgmt_cli add host name "Server_1" ip-address "10.15.123.10" --format json

C. mgmt_cli add object-host "Server_1" ip-address "10.15.123.10" --format json

D. mgmt._cli add object "Server-1" ip-address "10.15.123.10" --format json

Answer: (SHOW ANSWER)

Explanation

Example:

mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json

* "--format json" is optional. By default the output is presented in plain text.

References:

NEW QUESTION: 30

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____

.

A. User Directory

B. Captive Portal

C. UserCheck

D. Captive Portal and Transparent Kerberos Authentication

Answer: D (LEAVE A REPLY)

NEW QUESTION: 31

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
The correct way to enable Identity Captive Portal for a specific rule is to right click Accept in the rule, select "More", and then check 'Enable Identity Captive Portal'. This will allow guest users to see the splash page and accept the Terms of Service before accessing the Internet. Identity Captive Portal is a feature that enables identity awareness for guest users who are not authenticated by other methods, such as Active Directory or Identity Agent. Identity Captive Portal can be enabled globally or per rule, depending on the security policy requirements.

NEW QUESTION: 32
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?
A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud
Answer: (SHOW ANSWER)
Explanation
Mobile Access is not part of the SandBlast component. Mobile Access is a software blade that provides secure remote access to corporate resources from various devices, such as smartphones, tablets, and laptops. Mobile Access supports different connectivity methods, such as SSL VPN, IPsec VPN, and Mobile Enterprise Application Store (MEAS). Mobile Access also integrates with Mobile Threat Prevention (MTP) to protect mobile devices from malware and network attacks. References: Check Point Security Expert R81 Course, Mobile Access Administration Guide, SandBlast Mobile Datasheet

NEW QUESTION: 33
When using CPSTAT, what is the default port used by the AMON server?
A. 18191
B. 18194
C. 18192
D. 18190
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
Which application should you use to install a contract file?

A. SmartUpdate
B. WebUI
C. SmartView Monitor
D. SmartProvisioning
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
What kind of information would you expect to see when using the "sim affinity -l" command?
A. Overview over SecureXL templated connections
B. The VMACs used in a Security Gateway cluster
C. Affinity Distribution
D. The involved firewall kernel modules in inbound and outbound packet chain
Answer: C (LEAVE A REPLY)
Explanation
The "sim affinity -l" command is a command that displays the affinity distribution of the Security Gateway's interfaces. Affinity distribution is the assignment of CPU cores to handle the traffic from different interfaces.
The "sim affinity -l" command shows the following information for each interface:
The interface name, such as eth0, eth1, etc.
The interface index, such as 0, 1, 2, etc.
The interface type, such as physical, bond, VLAN, etc.
The interface state, such as up or down
The interface speed, such as 1000 Mbps, 10000 Mbps, etc.
The interface MTU, such as 1500, 9000, etc.
The interface MAC address, such as 00:11:22:33:44:55
The interface IP address, such as 192.168.1.1, 10.0.0.1, etc.
The interface affinity mask, such as 0x00000001, 0x00000002, etc. The affinity mask is a hexadecimal value that represents the CPU cores that are assigned to handle the traffic from the interface. For example, 0x00000001 means that only CPU core 0 is assigned, 0x00000003 means that CPU cores 0 and 1 are assigned, and so on.
The "sim affinity -l" command can help you to monitor and optimize the performance of your Security Gateway by showing you how the traffic load is distributed among the CPU cores. You can also use the "sim affinity" command with other options to change the affinity settings of the interfaces or the firewall instances.
For more information, you can refer to the Check Point R81.20 (Titan) Resolved Issues and Enhancements1 or the Solved: Sim Affinity - Check Point CheckMates2.

NEW QUESTION: 36
To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?
A. NAT Template

B. Accept Template
C. Deny Template
D. Drop Template
Answer: (SHOW ANSWER)

NEW QUESTION: 37
John is using Management HA. Which Security Management Server should he use for making changes?
A. secondary Smartcenter
B. active SmartConsole
C. connect virtual IP of Smartcenter HA
D. primary Log Server
Answer: (SHOW ANSWER)
Explanation
In Management HA, you should use the active SmartConsole for making changes. The active SmartConsole is connected to the Primary Security Management Server, which is responsible for synchronizing the configuration with the Secondary Security Management Server. If you use the secondary SmartCenter, your changes will not be replicated to the primary SmartCenter and will be lost in case of a failover.
References: Check Point Resource Library, page 9

NEW QUESTION: 38
NAT rules are prioritized in which order?
1. Automatic Static NAT
2. Automatic Hide NAT
3. Manual/Pre-Automatic NAT
4. Post-Automatic/Manual NAT rules
A. 1, 4, 2, 3
B. 4, 3, 1, 2
C. 1, 2, 3, 4
D. 3, 1, 2, 4
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?
A. Topology, and you are defining the Internal network
B. Internal network(s) you are defining your networks
C. Internal addresses you are defining the gateways
D. Network, and defining your Class A space
Answer: (SHOW ANSWER)

NEW QUESTION: 40

The Check Point installation history feature in provides the following:
A. View install changes and install specific version
B. Policy Installation Date only
C. Policy Installation Date, view install changes and install specific version
D. View install changes
Answer: (SHOW ANSWER)
See the revisions that were installed on the Security Gateway and who installed the Policy. See the changes that were installed and who made the changes. Revert to a specific version, and install the last "good" Policy.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Policy-Installation-History.htm

NEW QUESTION: 41
A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?
A. run fw unloadlocal" on the relevant gateway and check the ping again
B. run "cpstop" on the relevant gateway and check the ping again
C. run "fw log" on the relevant gateway
D. run "fw ctl zdebug drop" on the relevant gateway
Answer: D (LEAVE A REPLY)
Explanation
The solution to troubleshoot the issue of some Internet resources being unavailable is to run fw ctl zdebug drop on the relevant gateway1. This command lists all dropped packets in real time and explains the reasons for the drop2. It is a powerful tool that can help diagnose connectivity problems and firewall policy issues3. To use this command, you need to access the gateway in expert mode and run fw ctl zdebug + drop2. You can also filter the output by using grep with an IP address or a keyword, for example: fw ctl zdebug + drop | grep 10.10.10.10 or fw ctl zdebug + drop | grep SYN3. This command is a wrapper for the full debugs, and it will run the debug commands for you and will allow you to run debug from one debug module only4. By default, it will use a small debug buffer but if you wish, you can provide the -buf option to use your own size4. To stop the command, press Ctrl+C and then run fw ctl debug 0 to reset the debug state3.
Note: Running this command may affect the performance of the firewall, so use it with caution and only when necessary3. References: Solved: is it possible /supported to run fw ctl zdebug on ... - Check ..., How to use the fw ctl zdebug command to view drops on the Security Gateway, Troubleshooting dropped packets in Checkpoint using zdebug, "fw ctl zdebug" - Helpful Command Combinations - Check Point CheckMates

NEW QUESTION: 42
What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?
A. set host name "New Host" ip-address "192.168.0.10"
B. new host name "New Host" ip-address "192.168.0.10"
C. add host name "New Host" ip-address "192.168.0.10"
D. create host name "New Host" ip-address "192.168.0.10"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
What two ordered layers make up the Access Control Policy Layer?
A. Network and Application Control
B. Network and Threat Prevention
C. URL Filtering and Network
D. Application Control and URL Filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Fill in the blank: Authentication rules are defined for _____ .
A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database
Answer: A (LEAVE A REPLY)
Explanation
Authentication rules are defined for user groups, not individual users or all users in the database.
Authentication rules allow you to control which user groups can access specific resources or services through the Security Gateway. You can define different authentication methods and schemes for different user groups, such as Check Point Password, OS Password, RADIUS, TACACS, SecurID, LDAP, or Certificate. You can also define different session timeouts and source restrictions for different user groups. Authentication rules are processed before the network access rules in the rule base.

NEW QUESTION: 45
The admin is connected via ssh lo the management server. He wants to run a mgmt_dl command but got a Error 404 message. To check the listening ports on the management he runs netstat with the results shown below. What can be the cause for the issue?

A. Wrong Management API Access setting^for Ihe client IP To correct it go to SmartConsole / Management & Settings / Blades / Management API and press "Advanced Settings..' and choose GUI clients or ALL IP's.
B. The API didn't run on the default port check it with api status' and add '-port 4434' to the mgmt_clt command.
C. The management permission in the user profile is mrssing. Go to SmartConsole / Management & Settings I Permissions & Administrators / Permission Profiles. Select the profile of the user and enable 'Management API Login' under Management Permissions

D. The API is not running, the services shown by netstat are the gaia services. To start the API run 'api start'
Answer: (SHOW ANSWER)
Explanation
The error message "Error 404. The Management API server is not available. Please check that the Management API server is up and running." indicates that the API is not running on the Management Server.
The netstat command shows that there is no process listening on port 4434, which is the default port for the API. To start the API, the command 'api start' should be used. The other options are not relevant to this issue.
References: Check Point R81 Installation and Upgrade Guide, page 18.

NEW QUESTION: 46
Which command lists all tables in Gaia?
A. fw tab -t
B. fw tab -list
C. fw-tab -s
D. fw tab -1
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Choose the correct syntax to add a new host named "emailserver1" with IP address 10.50.23.90 using GAiA Management CLI?
A. mgmt_cli add host name ip-address 10.50.23.90
B. mgmt_cli add host name "emailserver1" ip-address 10.50.23.90
C. mgmt_cli add host name "myHost12 ip" address 10.50.23.90
D. mgmt_cli add host "emailserver1" address 10.50.23.90
Answer: (SHOW ANSWER)

NEW QUESTION: 48
What are possible Automatic Reactions in SmartEvent?
A. Mail. SNMP Trap, Block Source. Block Event Activity, External Script
B. Web Mail. Block Destination, SNMP Trap. SmartTask
C. Web Mail, Block Service. SNMP Trap. SmartTask, Geo Protection
D. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script
Answer: A (LEAVE A REPLY)

Explanation
The possible Automatic Reactions in SmartEvent are Mail, SNMP Trap, Block Source, Block Event Activity, and External Script1. Automatic Reactions are actions that SmartEvent can perform automatically when a specific event occurs2. They can help you respond quickly and efficiently to security incidents and threats2. The Automatic Reactions are1:
Mail: This reaction sends an email notification to a specified recipient with the details of the event. You can customize the subject and the body of the email, and use variables to include relevant information.
SNMP Trap: This reaction sends an SNMP trap to a specified SNMP server with the details of the event. You can customize the OID and the community string of the trap, and use variables to include relevant information.
Block Source: This reaction blocks the source IP address of the event from accessing your network for a specified duration. You can choose to block the source on all gateways or on specific gateways. You can also choose to block the source on a specific port or service.
Block Event Activity: This reaction blocks the specific activity that triggered the event from occurring again for a specified duration. You can choose to block the activity on all gateways or on specific gateways. You can also choose to block the activity on a specific port or service.
External Script: This reaction runs an external script on a specified server with the details of the event as arguments. You can use any script that can be executed by the operating system of the server, such as bash, perl, python, etc. You can use variables to include relevant information in the script arguments.
References: SmartEvent R81.10 Administration Guide - Check Point Software, SmartEvent - Check Point Software

NEW QUESTION: 49
Which statement is NOT TRUE about Delta synchronization?
A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members.
Answer: A (LEAVE A REPLY)
Explanation
The statement that is not true about Delta synchronization is Using UDP Multicast or Broadcast on port 8161. Delta synchronization is a mechanism that transfers only the changes in the kernel tables between cluster members, instead of sending the entire tables. It uses UDP Multicast or Broadcast on port 8116, not 81612.
The other statements are true about Delta synchronization. References: Check Point R81 ClusterXL Administration Guide

NEW QUESTION: 50
What is the best sync method in the ClusterXL deployment?
A. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
B. Use 1 dedicated sync interface
C. Use 2 clusters +1st sync + 2nd sync
D. Use 1 cluster + 1st sync
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Which of the following is NOT a type of Endpoint Identity Agent?
A. Full
B. Light
C. Terminal
D. Custom
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
Which of the following statements about Site-to-Site VPN Domain-based is NOT true?
A. Route-based- The Security Gateways will have a Virtual Tunnel Interface (VTI) for each VPN Tunnel with a peer VPN Gateway. The Routing Table can have routes to forward traffic to these VTIs. Any traffic routed through a VTI is automatically identified as VPN Traffic and is passed through the VPN Tunnel associated with the VTI.
B. Domain-based- VPN domains are pre-defined for all VPN Gateways.
When the Security Gateway encounters traffic originating from one VPN Domain with the destination to a VPN Domain of another VPN Gateway, that traffic is identified as VPN traffic and is sent through the VPN Tunnel between the two Gateways.
C. Domain-based- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway.
D. Domain-based- VPN domains are pre-defined for all VPN Gateways.
A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?
A. Lagging
B. Collision
C. Synchronized
D. Never been synchronized
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Tom has been tasked to install Check Point R81 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?
A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
B. One machine
C. Two machines
D. Three machines
Answer: (SHOW ANSWER)
Explanation

One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION: 55
To fully enable Dynamic Dispatcher on a Security Gateway:
A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
B. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
C. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu.
D. run fw multik set_mode 1 in Expert mode and then reboot.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.
A. cpm
B. fwd
C. cpd
D. fwm
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
UserCheck objects in the Application Control and URL Filtering rules allow the gateway to communicate with the users. Which action is not supported in UserCheck objects?
A. Inform
B. Drop
C. Reject
D. Ask
Answer: (SHOW ANSWER)

NEW QUESTION: 58
How can SmartView application accessed?
A. http://<Security Management IP Address>/smartview
B. http://<Security Management IP Address>:4434/smartview/
C. https://<Security Management IP Address>/smartview/
D. https://<Security Management host name>:4434/smartview/
Answer: C (LEAVE A REPLY)
Explanation
SmartView is a web-based application that allows you to view and analyze logs, reports, and events from multiple Check Point products. You can access SmartView by using the following URL:

```
https://<Security Management IP Address>/smartview/
```

You need to use HTTPS protocol and the default port 443. You also need to enter the IP address of the Security Management Server that hosts the SmartView application. You cannot use the host name of the Security Management Server or a different port number. References: SmartView R81 Administration Guide

NEW QUESTION: 59
What is Dynamic Balancing?
A. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
B. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
C. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.
D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces
Answer: B (LEAVE A REPLY)

NEW QUESTION: 60
Which command can you use to verify the number of active concurrent connections?
A. fw conn all
B. fw ctl pstat
C. show all connections
D. show connections
Answer: (SHOW ANSWER)
Explanation
The command fw ctl pstat can be used to verify the number of active concurrent connections on a gateway.
This command displays various statistics about the firewall kernel, such as memory usage, CPU utilization, packet rates, and connection table information. The output of this command includes a line that shows the current number of connections and the peak number of connections since the last reboot. For example:

```
Connections all in all: 1234/8192 (15%) at peak: 2345
```

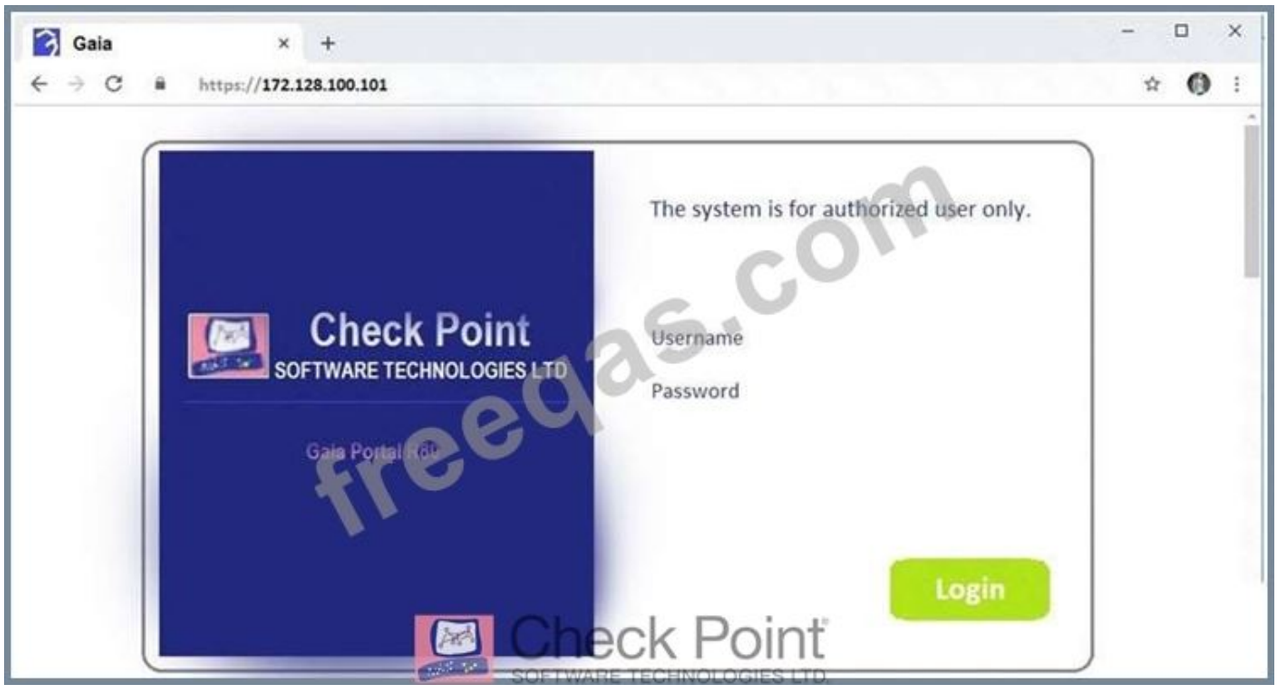
This means that there are currently 1234 active connections out of a maximum of 8192 connections, which is 15% of the connection table capacity. The peak number of connections since the last reboot was 2345.

NEW QUESTION: 61
How can you switch the active log file?
A. Run fw logswitch on the gateway
B. Run fwm logswitch on the Management Server
C. Run fwm logswitch on the gateway
D. Run fw logswitch on the Management Server
Answer: D (LEAVE A REPLY)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/CLI/fw-logswitch.htm

NEW QUESTION: 62
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:
A. All UDP packets
B. All IPv6 Traffic
C. All packets that match a rule whose source or destination is the Outside Corporate Network
D. CIFS packets
Answer: D (LEAVE A REPLY)
Explanation
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions: CIFS packets. SecureXL is a technology that accelerates network traffic processing by offloading intensive operations from the Firewall kernel to a dedicated SecureXL device. However, some packets cannot be accelerated by SecureXL due to various reasons, such as unsupported features, security policy settings, or protocol limitations. One example of packets that cannot be accelerated by SecureXL are CIFS packets, which are used for file sharing and access over SMB protocol. CIFS packets are not accelerated by SecureXL because they require stateful inspection by the Firewall kernel.

NEW QUESTION: 63
What is the command switch to specify the Gaia API context?
A. No need to specify a context, since it defaults to the Gaia API context.
B. mgmt_cli --context gaia_api <Command>
C. You have to specify it in the YAML file api.yml which is located underneath the /etc directory of the security management server
D. You have to change to the zsh-Shell which defaults to the Gaia API context.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 64
Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



A. set web ssl-port <new port number>
B. set Gaia-portal port <new port number>
C. set Gaia-portal https-port <new port number>
D. set web https-port <new port number>
Answer: A (LEAVE A REPLY)
Explanation
The CLISH command to change the default Gaia WebUI Portal port number is set web ssl-port <new port number>. This command will change the port that the WebUI listens on for HTTPS connections. After changing the port, you need to save the configuration with save config and verify that the change was applied with show web ssl-port. You also need to update the Main URL in the Platform Portal section of the gateway object in SmartConsole and install the policy.

NEW QUESTION: 65
In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?
A. If the Action of the matching rule is Accept the gateway will drop the packet
B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
D. If the rule does not matched in the Network policy it will continue to other enabled polices
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_R81_SecMGMT/126197

NEW QUESTION: 66

What are the two high availability modes?
A. Load Sharing and Legacy
B. Traditional and New
C. Active and Standby
D. New and Legacy
Answer: D (LEAVE A REPLY)
Explanation
The two high availability modes are New and Legacy. High availability (HA) is a feature that allows you to create a cluster of two or more Security Gateways that act as a single entity to provide redundancy and reliability for your network traffic. HA ensures that if one Security Gateway fails or becomes unavailable, another Security Gateway in the cluster takes over its role seamlessly and continues to process the traffic. HA also provides load balancing and synchronization of the cluster members. The New mode is the recommended mode for HA clusters, as it provides better performance, scalability, and stability than the Legacy mode. The New mode uses the ClusterXL mechanism to manage the cluster members and the state synchronization. The Legacy mode uses the High Availability Security Extension (HASE) mechanism to manage the cluster members and the state synchronization. The Legacy mode is supported for backward compatibility with older versions of Check Point products, but it has some limitations and disadvantages compared to the New mode.

NEW QUESTION: 67
Which command shows actual allowed connections in state table?
A. fw tab -t StateTable
B. fw tab -t connections
C. fw tab -t connection
D. fw tab connections
Answer: B (LEAVE A REPLY)
Explanation
The correct command to show actual allowed connections in the state table is option B: fw tab -t connections.
This command displays the contents of the "connections" table, which contains information about the active connections being tracked by the firewall.
Option A (fw tab -t StateTable) is incorrect as there is no "StateTable" table; it should be "connections." Option C (fw tab -t connection) is also incorrect, as it should be "connections." Option D (fw tab connections) is not the correct syntax for the command.
References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 68
You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?
A. In CLISH run set interface eth2 hw-addr 11 11 11:11:11 11
B. In expert-mode run ifconfig eth1 hw 11:11:11:11 11 11
C. In expert-mode run: ethtool -4 eth2 mac 11 11:11:11:11:11
D. In CLISH run: set interface eth2 mac-addr 11:11:11:11:11:11

Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
How can you grant GAiAAPI Permissions for a newly created user?
A. Assign the user a permission profile in SmartConsole
B. Assign the user the admin RBAC role in dish
C. No need to grant access since every user has access by default.
D. In bash, use the following command: "gaia_api access --user Tom -enable true"
Answer: A (LEAVE A REPLY)
Explanation
To grant GAiAAPI permissions for a newly created user, you need to assign the user a permission profile in SmartConsole. A permission profile defines the access level and scope of actions that a user can perform using the GAiAAPI. You can choose from predefined permission profiles or create your own custom profiles. You cannot grant GAiAAPI permissions using dish or bash commands. References: [Check Point Security Expert R81 API Reference Guide], page 9.

NEW QUESTION: 70
Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R81.
What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?
A. Unsupported version on UTM-1 570 series appliance
B. Unsupported appliances on remote locations
C. Missing an installed R77.20 Add-on on Security Management Server
D. Unsupported firmware on UTM-1 Edge-W appliance
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
What is the valid range for VRID value in VRRP configuration?
A. 1 - 254
B. 1 - 255
C. 0 - 254
D. 0 - 255
Answer: B (LEAVE A REPLY)
Explanation
The valid range for VRID value in VRRP configuration is 1 - 255. VRID stands for Virtual Router ID, and it is a number that identifies a virtual router in a VRRP cluster. A VRRP cluster consists of one or more routers that share a virtual IP address and provide redundancy and load balancing for network traffic. Each router in the cluster must have a unique

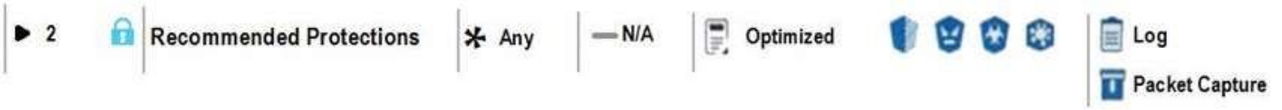
VRID value, and the VRID value must match the VRID value configured on the interface that connects to the VRRP cluster. The VRID value can be any number from 1 to 255, inclusive.

NEW QUESTION: 72
If a "ping"-packet is dropped by FW1 Policy -on how many inspection Points do you see this packet in "fw monitor"?
A. "i", "I" and "o"
B. I don't see it in fw monitor
C. "i" only
D. "i" and "I"
Answer: (SHOW ANSWER)
Explanation
If a "ping"-packet is dropped by FW1 Policy, you will see this packet in "fw monitor" on one inspection point only: "i". The "i" inspection point represents the inbound traffic before any rule processing. Since the packet is dropped by FW1 Policy, it will not pass through any other inspection points, such as "I" (after rule processing), "o" (outbound before rule processing), or "O" (outbound after rule processing). References: :
Check Point Software, Getting Started, fw monitor.

NEW QUESTION: 73
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: C (LEAVE A REPLY)
Explanation
Sticky Decision Function (SDF) is required to prevent asymmetric routing in an Active-Active cluster.
Asymmetric routing occurs when packets from a source to a destination follow a different path than packets from the destination to the source. This can cause problems with stateful inspection and NAT. SDF ensures that packets from the same connection are handled by the same cluster member1. References: Check Point R81 ClusterXL Administration Guide

NEW QUESTION: 74
When Configuring Endpoint Compliance Settings for Applications and Gateways within Mobile Access, which of the three approaches will allow you to configure individual policies for each application?
A. Strong Approach
B. Medium Approach
C. Very Advanced Approach
D. Basic Approach
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



A. The current administrator has read-only permissions to Threat Prevention Policy.
B. Another user has locked the rule for editing.
C. Configuration lock is present. Click the lock symbol to gain read-write access.
D. The current administrator is logged in as read-only because someone else is editing the policy.
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_R81_SecMGMT/124265

NEW QUESTION: 76
What are the correct steps upgrading a HA cluster (M1 is active, M2 is passive) using Multi-Version Cluster(MVC)Upgrade?
A. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on
2) Upgrade the passive node M2 to R81.20
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism
B. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on
2) Upgrade the passive node M2 to R81.20
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy
C. 1) In SmartConsole, change the version of the cluster object
2) Upgrade the passive node M2 to R81.20
3) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 #cphaconf mvc on
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsole, change the version of the cluster object
D. 1) Upgrade the passive node M2 to R81.20
2) Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 #cphaconf mvc on
3) In SmartConsole, change the version of the cluster object
4) Install the Access Control Policy

5) After examine the cluster states upgrade node M1 to R81.20
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.20
Answer: C (LEAVE A REPLY)
Explanation
The correct steps upgrading a HA cluster (M1 is active, M2 is passive) using Multi-Version Cluster (MVC) Upgrade are:
In SmartConsole, change the version of the cluster object to R81.20.
Upgrade the passive node M2 to R81.20 using CPUSE or CLI.
Enable the MVC mechanism on the upgraded R81.20 Cluster Member M2 using the command cphaconf mvc on.
Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails by selecting Continue installing on other Gateways in the Policy Installation Settings dialog box.
After examining the cluster states using cphaprob stat and verifying that both members are synchronized, upgrade node M1 to R81.20 using CPUSE or CLI.
On each Cluster Member, disable the MVC mechanism using the command cphaconf mvc off and Install the Access Control Policy3.
References: Check Point R81 Installation and Upgrade Guide

NEW QUESTION: 77
Which of these statements describes the Check Point ThreatCloud?
A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network
Answer: D (LEAVE A REPLY)
Explanation
The Check Point ThreatCloud is a worldwide collaborative security network that collects and analyzes threat data from millions of sensors, security gateways, and other sources, and delivers real-time threat intelligence and protection to Check Point products. References: Check Point ThreatCloud

NEW QUESTION: 78

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop
2	Management	net_10.28.0.0	GW-R7730	* Any	https ssh	Accept
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop
4	DNS	net_10.28.0.0	* Any	* Any	dns	Accept
5	Web	net_10.28.0.0	* Any	* Any	http https	Accept
6	DMZ Access	net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp AP-Defender	Accept
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop

You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
What does this mean?
A. This rule No. 6 has been marked for deletion in another Management session.
B. This rule No. 6 has been marked for editing in your Management session.
C. This rule No. 6 has been marked for editing in another Management session.
D. This rule No. 6 has been marked for deletion in your Management session.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
What is considered Hybrid Emulation Mode?
A. Manual configuration of file types on emulation location.
B. Load sharing of emulation between an on premise appliance and the cloud.
C. Load sharing between OS behavior and CPU Level emulation.
D. High availability between the local SandBlast appliance and the cloud.
Answer: B (LEAVE A REPLY)
Explanation
Hybrid Emulation Mode is a mode of operation that allows load sharing of emulation between an on premise appliance and the cloud. Emulation is a process that analyzes files for malicious behavior by running them in a virtual sandbox. Hybrid Emulation Mode enables you to optimize the performance and scalability of your Threat Emulation solution by distributing the emulation workload between your local SandBlast appliance and the Check Point cloud service.
References: Check Point Security Expert R81 Course, Threat Emulation Administration Guide

NEW QUESTION: 80
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.
A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.

D. This statement is false because encrypted traffic cannot be inspected.

Answer: C (LEAVE A REPLY)

Explanation

SecureXL is a performance-enhancing technology used in Check Point firewalls. It improves the throughput of both non-encrypted firewall traffic and encrypted VPN traffic. The statement in option C is true because SecureXL does improve both types of traffic by offloading processing to dedicated hardware acceleration, optimizing firewall and VPN operations.

Option C correctly states that SecureXL improves this traffic, making it the verified answer.

References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 81

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____ .

A. User Directory

B. Captive Portal and Transparent Kerberos Authentication

C. Captive Portal

D. UserCheck

Answer: B (LEAVE A REPLY)

Explanation

Browser-based Authentication is a method of acquiring identities from unidentified users by sending them to a web page where they can log in and authenticate. Browser-based Authentication uses two techniques to acquire identities: Captive Portal and Transparent Kerberos Authentication1.

Captive Portal is a simple method that attempts authentication through a web interface before granting a user access to Intranet resources. When a user tries to access a protected resource, they are redirected to a web page where they have to enter their credentials. The credentials are verified by the Identity Awareness Security Gateway or an external authentication server. If the authentication is successful, the user's identity is associated with their IP address and they are allowed to access the resource12.

Transparent Kerberos Authentication is a more seamless method that leverages the existing Kerberos infrastructure in the network. When a user tries to access a protected resource, the Identity Awareness Security Gateway intercepts the Kerberos ticket request and extracts the user's identity from it. The user's identity is then associated with their IP address and they are allowed to access the resource without any additional prompts. This method requires that the Identity Awareness Security Gateway is configured as a trusted proxy in the Active Directory domain12.

Therefore, the correct answer is B. Browser-based Authentication sends users to a web page to acquire identities using Captive Portal and Transparent Kerberos Authentication.

References:

1, THE IMPORTANCE OF ACCESS ROLES - Check Point Software, page 2

2, Browser-based Authentication Check Point - Bing

3, How to Configure Client Authentication - Check Point Software, page 1

4, Identity Sources - Check Point Software

5, Configuring Browser-Based Authentication - Check Point Software

6, Two Factor Authentication - Check Point Software

NEW QUESTION: 82
What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?
A. Manually, Scheduled, Automatic
B. Manually, Automatic, Disabled
C. Manually, Scheduled, Disabled
D. Manually, Scheduled, Enabled
Answer: A (LEAVE A REPLY)
Explanation
The available options for downloading Check Point hotfixes in Gaia WebUI (CPUSE) are Manually, Scheduled, and Automatic. These options can be configured in the CPUSE Settings tab of the Gaia Portal. The Manual option lets you download hotfixes manually from the Check Point Cloud or a local Deployment Agent when you need them. The Scheduled option lets you download hotfixes automatically at a specified time interval (daily, weekly, or monthly). The Automatic option lets you download hotfixes automatically as soon as they are available.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/ html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

NEW QUESTION: 83
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.20 SmartConsole application?
A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
B. Firewall, IPS, Threat Emulation, Application Control.
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.
Answer: C (LEAVE A REPLY)
Explanation
The Threat Prevention profile in Check Point R81.20 SmartConsole application allows you to enforce the following software blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation, and Threat Extraction. These software blades provide comprehensive protection against various types of threats, such as network attacks, malware, ransomware, phishing, and zero-day exploits. You can configure the profile settings for each software blade, such as the action to take, the protection scope, and the exceptions. References: Check Point Security Expert R81 Course, Threat Prevention Administration Guide

NEW QUESTION: 84
When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?
A. RADIUS
B. Remote Access and RADIUS
C. AD Query
D. AD Query and Browser-based Authentication
Answer: D (LEAVE A REPLY)
Explanation

When Identity Awareness is enabled, AD Query and Browser-based Authentication are used as identity sources for Application Control. AD Query allows the Security Gateway to query Active Directory servers for identity information based on IP addresses. Browser-based Authentication allows the Security Gateway to redirect unidentified users to a captive portal where they can authenticate with their credentials. These identity sources provide accurate and up-to-date identity information for Application Control, which can enforce granular policies based on user, group, machine, and domain objects. References: R81 Identity Awareness Administration Guide, page 9.

NEW QUESTION: 85
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
Secure Network Distributor (SND) is a relevant feature of the Security Gateway because it is used to distribute packets among Firewall instances. SND is a technology that improves the performance and scalability of the Security Gateway by using multiple cores to handle concurrent connections. SND consists of two components:
SND driver and Firewall instances. SND driver is responsible for receiving packets from network interfaces and distributing them to Firewall instances based on a load balancing algorithm. Firewall instances are responsible for inspecting packets according to security policies and forwarding them to their destinations. The other options are either incorrect or not related to SND.

NEW QUESTION: 86
Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.
A. Better understand the behavior of the Access Control Policy
B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
C. Automatically rearrange Access Control Policy based on Hit Count Analysis
D. Analyze a Rule Base - You can delete rules that have no matching connections
Answer: C (LEAVE A REPLY)
Explanation
Hit Count is a feature to track the number of connections that each rule matches, which can help to optimize the Rule Base efficiency and analyze the network traffic behavior. The benefit that is not provided by Hit Count is automatically rearrange Access Control Policy based on Hit Count Analysis. Hit Count does not change the order of the rules automatically, but it allows the administrator to manually move the rules up or down based on the hit count statistics. The administrator can also use the SmartOptimize feature to get suggestions for improving the Rule Base order and performance. References: R81 Security Management Administration Guide, page 97.

NEW QUESTION: 87
Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?

A. fw accel stat
B. fwaccel stat
C. fw acces stats
D. fwaccel stats
Answer: (SHOW ANSWER)
Explanation
The fwaccel stat command displays the status of SecureXL, and its enabled templates and features. The other commands are either incorrect or incomplete. References: [SecureXL Commands]

NEW QUESTION: 88
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?
A. In expert mode run #netstat -tulnp | grep httpd to see if httpd is up and to get the port number. In dish run >show web daemon-enable to see if the web daemon is enabled.
B. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use. In expert mode run #netstat -anp | grep httpd to see if the httpd is up
C. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use. In expert mode run #netstat -anp | grep httpd2 to see if the httpd2 is up
D. In expert mode run #netstat -tulnp | grep httpd2 to see if httpd2 is up and to get the port number. In dish run >show web daemon-enable to see if the web daemon is enabled.
Answer: (SHOW ANSWER)
Explanation
The correct way to check if the web service is enabled, running and which port is used is to use option C. In dish, run show web ssl-port to see if the web daemon is enabled and which port is in use. In expert mode, run netstat -anp | grep httpd2 to see if the httpd2 is up1. The httpd2 service is responsible for the Gaia Web Management Interface2. If the web daemon is disabled, you can enable it by running set web daemon-enable on in dish3. If the httpd2 service is down, you can start it by running service httpd2 start in expert mode4.
References: Gaia WebUI and CLI - Check Point CheckMates, Gaia R81.20 Administration Guide - Check Point Software, Gaia R81 Administration Guide - Check Point Software, How to restart Gaia Portal (WebUI) process - Check Point Software

NEW QUESTION: 89
What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?
A. 1-254
B. 1-255
C. 0-254
D. 0 - 255
Answer: B (LEAVE A REPLY)
Explanation

The valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration is 1-255. The VRID is a unique number that identifies a virtual router in a VRRP group. It is used to associate routers and their virtual IP addresses. The VRID must be the same for all routers in the same VRRP group. References: [Configuring VRRP on Gaia]

NEW QUESTION: 90
Return oriented programming (ROP) exploits are detected by which security blade?
A. Data Loss Prevention
B. Check Point Anti-Virus / Threat Emulation
C. Application control
D. Intrusion Prevention Software
Answer: B (LEAVE A REPLY)
Explanation
Return-oriented programming (ROP) exploits are detected by Check Point Anti-Virus / Threat Emulation blade. ROP exploits are a type of code reuse attack that bypasses common exploit mitigation techniques such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Check Point Anti-Virus / Threat Emulation blade can detect and prevent ROP exploits using its behavioral analysis engine that monitors the execution flow of processes and identifies malicious patterns. References: [Check Point Security Expert R81 Threat Prevention Administration Guide], page 17.

NEW QUESTION: 91
Which command would disable a Cluster Member permanently?
A. set clusterXL down-p
B. cphaprob_admin down
C. clusterXL_admin down-p
D. clusterXL_admin down
Answer: C (LEAVE A REPLY)

NEW QUESTION: 92
What are the main stages of a policy installation?
A. Verification, Commit, Installation
B. Initiation, Conversion and Save
C. Initiation, Conversion and FWD REXEC

D. Verification Compilation, Transfer and Commit
Answer: (SHOW ANSWER)

NEW QUESTION: 93
When synchronizing clusters, which of the following statements is FALSE?
A. Only cluster members running on the same OS platform can be synchronized.
B. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
C. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
When users connect to the Mobile Access portal they are unable to open File Shares.
Which log file would you want to examine?
A. cvpnd.elg
B. httpd.elg
C. vpnd.elg
D. fw.elg
Answer: A (LEAVE A REPLY)
Explanation
When users connect to the Mobile Access portal they are unable to open File Shares.
The log file that you would want to examine is . This log file contains information about the Mobile Access VPN daemon, which handles the connections from the Mobile Access portal to the internal resources, such as File Shares, Web Applications, etc. The log file is located in the directory $FWDIR/log/ on the Security Gateway. You can use the command fw log -f cvpnd.elg to view the log file in real time.
References: R81 Mobile Access Administration Guide, page 255.

NEW QUESTION: 95
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?
A. Pentagon
B. Combined
C. Meshed
D. Star
Answer: D (LEAVE A REPLY)
Explanation
A star VPN community is a type of VPN community that allows a central gateway to create VPN tunnels with multiple satellite gateways or hosts, but does not allow satellite gateways or hosts to create VPN tunnels with each other. This

type of community is suitable for hub-and-spoke topologies, where the central gateway acts as the hub and the satellite gateways or hosts act as the spokes. The central gateway can initiate or terminate VPN traffic to any satellite member, but the satellite members can only initiate or terminate VPN traffic to the central gateway.

NEW QUESTION: 96
In what way are SSL VPN and IPSec VPN different?
A. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.
B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
C. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
D. IPSec VPN does not support two factor authentication, SSL VPN does support this
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Which one of the following is true about Threat Extraction?
A. Always delivers a file to user
B. Works on all MS Office, Executables, and PDF files
C. Can take up to 3 minutes to complete
D. Delivers file only if no threats found
Answer: A (LEAVE A REPLY)
Explanation
Threat Extraction is a software blade that always delivers a file to user. Threat Extraction removes or sanitizes the active content from the files and converts them to PDF format, which is safer and more compatible. Threat Extraction can also work together with Threat Emulation to provide both clean and original files to the users.
Threat Extraction works on MS Office, PDF, and archive files, but not on executables. Threat Extraction can take up to 3 minutes to complete, depending on the file size and complexity. References: Check Point Security Expert R81 Course, Threat Extraction Administration Guide

NEW QUESTION: 98
How long may verification of one file take for Sandblast Threat Emulation?
A. up to 3 minutes
B. up to 5 minutes
C. within seconds cleaned file will be provided
D. up to 1 minutes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Which of the following is NOT a VPN routing option available in a star community?
A. To center only.
B. To center, or through the center to other satellites, to Internet and other VPN targets.
C. To satellites through center only.
D. To center and to other satellites through center.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 100
SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:
A. 19090,22
B. 19009,443
C. 18190,80
D. 19190,22
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Which packet info is ignored with Session Rate Acceleration?
A. source port ranges
B. same info from Packet Acceleration is used
C. source ip
D. source port
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
Which TCP port does the CPM process listen on?
A. 18191
B. 18190
C. 8983
D. 19009
Answer: D (LEAVE A REPLY)
Explanation
The TCP port that the CPM process listens on is 19009. The CPM process is the Check Point Management process that handles all management operations on the Security Management Server, such as policy installation, database synchronization, logging, etc. It communicates with other processes and clients using TCP port 19009. The other ports are used by different processes or services. TCP port 18191 is used by the FWM process for management communication. TCP port 18190 is used by the CPD process for inter-process communication. TCP port 8983 is used by the Solr process for SmartLog indexing. References: [Check Point Ports]

NEW QUESTION: 103
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?
A. Fast Path
B. Accelerated Path
C. Medium Path
D. Slow Path
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
What is the responsibility of SOLR process on R81.10 management server?
A. Validating all data before it's written into the database
B. It generates indexes of data written to the database
C. Writing all information into the database
D. Communication between SmartConsole applications and the Security Management Server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?
A. $FWDIR/conf/client.scv
B. $CPDIR/conf/local.scv
C. $CPDIR/conf/client.svc
D. $FWDIR/conf/local.scv
Answer: D (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION: 106
Which command shows actual allowed connections in state table?
A. fw tab -t connections
B. fw tab -t connection
C. fw tab connections
D. fw tab -t StateTable
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
When using the Mail Transfer Agent, where are the debug logs stored?
A. $FWDIR/bin/emaild.mta. elg
B. $CPDIR/log/emaild elg

C. $FWDIR/log/mtad elg
D. /var/log/mail.mta elg
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
What is the main difference between Threat Extraction and Threat Emulation?
A. Threat Extraction always delivers a file and takes less than a second to complete.
B. Threat Emulation never delivers a file that takes less than a second to complete.
C. Threat Extraction never delivers a file and takes more than 3 minutes to complete.
D. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
By default how often updates are checked when the CPUSE Software Updates Policy is set to Automatic?
A. Six times per day
B. Seven times per day
C. Every two hours
D. Every three hours
Answer: (SHOW ANSWER)
Explanation
By default, when the CPUSE Software Updates Policy is set to Automatic, updates are checked every three hours3. This means that the CPUSE agent will automatically download and install updates that match the policy settings every three hours. The other options are not the default values for the CPUSE Software Updates Policy. References: 3: Check Point Software, Getting Started, CPUSE Software Updates Policy.

NEW QUESTION: 110
The Compliance Blade allows you to search for text strings in many windows and panes, to search for a value in a field, what would your syntax be?
A. name field:string
B. field name:string
C. name_field:string
D. field_name:string
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
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 is enabled by default on the Global Properties.
B. Yes, since 'Switch to higher priority cluster member' option on the cluster object properties is enabled by default.
C. No, since 'maintain' current active 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)

NEW QUESTION: 112
Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?
A. Severity
B. Automatic reactions
C. Policy
D. Threshold
Answer: C (LEAVE A REPLY)
Explanation
An event is a notification that something significant has occurred on a Check Point product or network. Events are generated by various sources, such as blades, gateways, servers, SmartEvent, etc. You can view and manage events in SmartConsole by using the Events tab in the Logs & Monitor view. Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane.
The configurable properties include:
Severity: The level of importance or urgency of the event. You can change the severity of an event by selecting a different value from the drop-down list.
Automatic reactions: The actions that are triggered when an event occurs. You can add, edit, or delete automatic reactions for an event by clicking on the + icon or the pencil icon.
Threshold: The minimum number or frequency of occurrences of an event that triggers an automatic reaction. You can change the threshold of an event by entering a different value in the text box.
The policy is not an option to adjust or configure for an event. The policy is a set of rules that define how to handle events based on their source, type, severity, etc. You can create and manage policies in SmartEvent by using the Policies tab in the Logs & Monitor view. References: R81 Logging and Monitoring Administration Guide

NEW QUESTION: 113
Which command collects diagnostic data for analyzing customer setup remotely?
A. cpinfo
B. migrate export
C. sysinfo
D. cpview
Answer: A (LEAVE A REPLY)
Explanation
CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

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

NEW QUESTION: 114
Which command shows the current Security Gateway Firewall chain?
A. fw ctl chain
B. fw ctl firewall-chain
C. show firewall chain
D. show current chain
Answer: A (LEAVE A REPLY)

NEW QUESTION: 115
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
In the Check Point Security Management Architecture, both the Security Management Server and Security Gateway can store logs. The Security Management Server stores logs related to management activities, while the Security Gateway stores logs related to network traffic1. References: Check Point Resource Library, page
3.

NEW QUESTION: 116
What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?
A. test_connectivity_ad -d <domain>
B. test_ldap_connectivity -d <domain>
C. test_ad_connectivity -d <domain>
D. ad_connectivity_test -d <domain>
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/
CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/
CP_R81.30_CLI_ReferenceGuide/200877

NEW QUESTION: 117
What is not a component of Check Point SandBlast?
A. Threat Simulator
B. Threat Emulation

C. Threat Extraction
D. Threat Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 118
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. Run cprestart from clish
B. After upgrading the hardware, increase the number of kernel instances using cpconfig
C. Hyperthreading must be enabled in the bios to use CoreXL
D. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?
A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
B. Create a separate Security Policy package for each remote Security Gateway.
C. Create network objects that restricts all applicable rules to only certain networks.
D. Run separate SmartConsole instances to login and configure each Security Gateway directly.
Answer: B (LEAVE A REPLY)
Explanation
To simplify security administration when working with multiple Security Gateways enforcing an extensive number of rules, you would choose to create a separate Security Policy package for each remote Security Gateway. A Security Policy package is a set of rules and objects that can be assigned to one or more Security Gateways. This allows you to manage different policies for different gateways from the same Management Server1. The other options are either not effective or not feasible for simplifying security administration.
References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 120
What destination versions are supported for a Multi-Version Cluster Upgrade?
A. R81.40 and later
B. R76 and later
C. R70 and Later
D. R81.20 and Later
Answer: D (LEAVE A REPLY)
Explanation
The destination versions that are supported for a Multi-Version Cluster Upgrade are R81.20 and later. This means that the cluster members can be upgraded from any supported version to R81.20 or higher using the Multi-Version Cluster

mode. R81.40, R76, and R70 are not supported destination versions for a Multi-Version Cluster Upgrade.
References: : Check Point Software, Getting Started, Supported Upgrade Paths

NEW QUESTION: 121
When users connect to the Mobile Access portal they are unable to open File Shares.
Which log file would you want to examine?
A. cvpnd.elg
B. httpd.elg
C. vpnd.elg
D. fw.elg
Answer: A (LEAVE A REPLY)
Explanation
When users connect to the Mobile Access portal they are unable to open File Shares.
The log file that you would want to examine is cvpnd.elg. This log file contains information about the Mobile Access VPN daemon, which handles the connections from the Mobile Access portal to the internal resources, such as File Shares, Web Applications, etc. The log file is located in the directory $FWDIR/log/ on the Security Gateway. You can use the command fw log -f cvpnd.elg to view the log file in real time.
References: R81 Mobile Access Administration Guide, page 255.

NEW QUESTION: 122
If you needed the Multicast MAC address of a cluster, what command would you run?
A. cphaprob -a if
B. cphaconf ccp multicast
C. cphaconf debug data
D. cphaprob igmp
Answer: (SHOW ANSWER)
Explanation
The command cphaprob igmp can be used to display the Multicast MAC address of a cluster. This command shows the IGMP (Internet Group Management Protocol) information for each cluster interface, including the VRID (Virtual Router ID), the Multicast IP address, and the Multicast MAC address3. The other commands do not show the Multicast MAC address information. References: Check Point R81 ClusterXL Administration Guide

NEW QUESTION: 123

While using the Gaia CLI. what is the correct command to publish changes to the management server?
A. json publish
B. mgmt publish
C. mgmt_cli commit
D. commit
Answer: B (LEAVE A REPLY)
Explanation
While using the Gaia CLI, the correct command to publish changes to the management server is mgmt publish. This command publishes all changes made by all administrators since the last publish operation. The json publish command is not valid in Gaia CLI. The mgmt_cli commit command is used to publish changes made by a specific administrator session. The commit command is used to save configuration changes in Gaia CLI.
References: Publishing Changes

NEW QUESTION: 124
Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?
A. Remote Desktop Protocol (RDP)
B. Hypertext Transfer Protocol Secure (HTTPS)
C. Windows Management Instrumentation (WMI)
D. Lightweight Directory Access Protocol (LDAP)
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Session unique identifiers are passed to the web api using which http header option?
A. Proxy-Authorization
B. Accept-Charset
C. Application
D. X-chkp-sid
Answer: (SHOW ANSWER)

NEW QUESTION: 126
You need to see which hotfixes are installed on your gateway, which command would you use?
A. cpinfo -o hotfix
B. cpinfo -y all
C. cpinfo -h all
D. cpinfo -l hotfix
Answer: B (LEAVE A REPLY)

NEW QUESTION: 127
What is the correct Syntax for adding an access-rule via R80 API?
A. add access-rule layer "Network" action "Allow"
B. add access-rule layer "Network" position 1 name "Rule 1" service. 1 "SMTP" service.2 "hup"

C. add access-rule <CR> and follow the wizard
D. add rule position 1 name "Rule 1" policy-package "Standard" add service "http"
Answer: B (LEAVE A REPLY)
Explanation
The correct syntax for adding an access-rule via R80 API is to use the add access-rule command with the layer, position, name, and service parameters. The layer parameter specifies the name of the access control policy layer where the rule will be added. The position parameter specifies the ordinal number in which to place the rule in the rulebase. The name parameter specifies the name of the rule. The service parameter specifies one or more services that match this rule. References: [Check Point Security Expert R81 API Reference Guide], page 18.

NEW QUESTION: 128
Which is the correct order of a log flow processed by SmartEvent components?
A. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
C. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client
Answer: (SHOW ANSWER)

NEW QUESTION: 129
Which 3 types of tracking are available for Threat Prevention Policy?
A. SMS Alert, Log, SNMP alert
B. Syslog, None, User-defined scripts
C. None, Log, Syslog
D. Alert, SNMP trap, Mail
Answer: D (LEAVE A REPLY)
Explanation
https://supportcenter.checkpoint.com/supportcenter/portal?

NEW QUESTION: 130
When attempting to start a VPN tunnel, in the logs the error "no proposal chosen" is seen numerous times. No other VPN-related entries are present.
Which phase of the VPN negotiations has failed?
A. IKE Phase 1
B. IPSEC Phase 2
C. IKE Phase 2
D. IPSEC Phase 1
Answer: (SHOW ANSWER)

NEW QUESTION: 131
What is the purpose of extended master key extension/session hash?
A. UDP VOIP protocol extension

B. Special TCP handshaking extension
C. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
D. Supplement DLP data watermark
Answer: C (LEAVE A REPLY)

NEW QUESTION: 132
What is the name of the secure application for Mail/Calendar for mobile devices?
A. Capsule Workspace
B. Capsule Mail
C. Capsule VPN
D. Secure Workspace
Answer: A (LEAVE A REPLY)
Explanation
The secure application for Mail/Calendar for mobile devices in Check Point is called "Capsule Workspace." Capsule Workspace provides secure access to email and calendar data on mobile devices while maintaining security policies and controls.
References: Check Point Certified Security Expert R81 documentation and learning resources.

NEW QUESTION: 133
What are the services used for Cluster Synchronization?
A. 256H-CP tor Full Sync and 8116/UDP for Delta Sync
B. 8116/UDP for Full Sync and Delta Sync
C. TCP/256 for Full Sync and Delta Sync
D. No service needed when using Broadcast Mode
Answer: A (LEAVE A REPLY)
Explanation
Cluster Synchronization is a mechanism that allows cluster members to share state information and maintain a consistent security policy. Cluster Synchronization uses two types of synchronization: Full Synchronization and Delta Synchronization. Full Synchronization transfers the entire Security Policy and state tables from one cluster member to another. Delta Synchronization transfers only the changes in the state tables. Cluster Synchronization uses two services for communication: TCP port 256 (CPHA) for Full Synchronization and UDP port 8116 for Delta Synchronization3. Therefore, the correct answer is A.
References: 3: Cluster Synchronization

NEW QUESTION: 134
Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.
What will happen to the changes already made?
A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.

C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom will have to reboot his SmartConsole computer, clear to cache, and restore changes.
Answer: (SHOW ANSWER)
Explanation
Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work. This is because SmartConsole has a feature called Concurrent Administration, which allows multiple administrators to work on the same Security Policy simultaneously, without blocking each other or creating conflicts. Concurrent Administration uses a locking mechanism to prevent multiple administrators from modifying the same rule or object at the same time. When an administrator clicks on a rule or an object, it becomes locked and a lock icon appears next to it. The lock icon shows the name of the administrator who is working on that rule or object, and prevents other administrators from editing it until it is unlocked12.
Concurrent Administration also has a feature called Session Persistence, which preserves the changes made by an administrator in case of a network failure or a SmartConsole crash. When an administrator reconnects to the Management Server after a network failure or a SmartConsole crash, they can resume their work from where they left off, without losing any changes. The changes are stored locally on the administrator's machine until they are published to the Management Server13.
Therefore, if Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity, his changes will not be lost.
They will be stored locally on his machine and he can resume his work when he reconnects to the Management Server.

NEW QUESTION: 135
What CLI command compiles and installs a Security Policy on the target's Security Gateways?
A. fwm fetch
B. fwm load
C. fwm compile
D. fwm install
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
Fill in the blank: The "fw monitor" tool can be best used to troubleshoot _____.
A. AV issues
B. VPN errors
C. Network traffic issues
D. Authentication issues
Answer: (SHOW ANSWER)
Explanation
https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NEW QUESTION: 137
Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .
A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install
Answer: C (LEAVE A REPLY)
Explanation
The IPS policy for pre-R81 gateways is installed during the Anti-bot policy install. The Anti-bot policy install includes both Anti-bot and IPS protections for pre-R81 gateways, since they share the same inspection engine.
For R81 and above gateways, the IPS policy is installed separately as part of the Threat Prevention policy install, which also includes Anti-virus and Threat Emulation protections. References: R81 Threat Prevention Administration Guide, page 15.

NEW QUESTION: 138
Which command lists firewall chain?
A. fwctl chain
B. fw list chain
C. fw chain module
D. fw tab -t chainmod
Answer: A (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION: 139
Which Queue in the Priority Queue has the maximum priority?
A. Heavy Data Queue
B. High Priority
C. Control
D. Routing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140

SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

A. Analyzes each log entry as it arrives at the log server according to the Event Policy. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.

B. Correlates all the identified threats with the consolidation policy.

C. Collects syslog data from third party devices and saves them to the database.

D. Connects with the SmartEvent Client when generating threat reports.

Answer: A (LEAVE A REPLY)

Explanation

The Correlation Unit in SmartEvent architecture has the function of analyzing each log entry as it arrives at the log server according to the Event Policy. When it identifies a threat pattern, it forwards an event to the SmartEvent Server. This is an essential function in threat detection and analysis, as it helps in identifying and alerting about security threats based on the configured policies.

Option A correctly describes the function of the Correlation Unit, making it the verified answer.

References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 141

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

A. Reset SIC on all gateways.

B. Remove the local ACL lists.

C. No effect.

D. Remove the installed Security Policy.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 142

You have used the SmartEvent GUI to create a custom Event policy. What is the best way to display the correlated Events generated by SmartEvent Policies?

A. Open SmartView Monitor and select the SmartEvent Window from the main menu.

B. In the SmartConsole / Logs & Monitor --> open the Logs View and use type:Correlated as query filter.

C. In the SmartConsole / Logs & Monitor -> open a new Tab and select External Apps / SmartEvent.

D. Select the Events tab in the SmartEvent GUI or use the Events tab in the SmartView web interface.

Answer: C (LEAVE A REPLY)
Explanation
The best way to display the correlated events generated by SmartEvent policies is to open a new tab in the SmartConsole / Logs & Monitor and select External Apps / SmartEvent. This will launch the SmartEvent GUI, which provides a comprehensive view of the network security events, including charts, reports, and timelines. The SmartEvent GUI can also be accessed from a web browser using the SmartView web interface1. References: Check Point R81 SmartEvent Administration Guide

NEW QUESTION: 143
In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?
A. Little o
B. Big O
C. Big I
D. Little i
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?
A. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.
B. Pamela should check SecureXL status on DMZ Security gateway and if it's turned ON. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
D. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OFF. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
How would you enable VMAC Mode in ClusterXL?
A. Cluster Object -> Edit -> ClusterXL and VRRP -> Use Virtual MAC
B. fw ctl set int vmac_mode 1
C. cphaconf vmac_mode set 1
D. Cluster Object -> Edit -> Cluster Members -> Edit -> Use Virtual MAC
Answer: A (LEAVE A REPLY)
Explanation

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk50840

NEW QUESTION: 146
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?
A. Kerberos Ticket Renewed
B. Kerberos Ticket Timed Out
C. Account Logon
D. Kerberos Ticket Requested
Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?
A. fwaccel stats
B. fw accel stat
C. fwaccel stat
D. fw acces stats
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
Which one of the following is true about Threat Emulation?
A. Works on MS Office and PDF files only
B. Takes less than a second to complete
C. Takes minutes to complete (less than 3 minutes)
D. Always delivers a file
Answer: (SHOW ANSWER)

NEW QUESTION: 149
What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?
A. Specific VPN Communities
B. Remote Access VPN Switch
C. Mobile Access VPN Domain
D. Network Access VPN Domain
Answer: (SHOW ANSWER)
Explanation
The "Network Access VPN Domain" feature allows remote-access VPN users to access resources across a site-to-site VPN tunnel. This feature allows remote users to securely access internal network resources as if they were physically connected to the network. This is achieved by adding the remote-access VPN users to a "VPN Domain" that has access to the internal network resources via a site-to-site VPN tunnel. This VPN Domain is also referred to as a "Network Access VPN Domain".

NEW QUESTION: 150
What does the Log "Views" tab show when SmartEvent is Correlating events?
A. A list of common reports
B. Reports for customization
C. Top events with charts and graphs
D. Details of a selected logs
Answer: D (LEAVE A REPLY)
Explanation
The Log "Views" tab shows the details of a selected log when SmartEvent is correlating events. You can select a log from the Logs tab and click on the Views tab to see more information about the log, such as source, destination, service, action, blade, rule number, etc. You can also customize the columns and filters in the Views tab to display only the relevant fields for your analysis. References: [SmartEvent User Guide]

NEW QUESTION: 151
You have enabled "Full Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?
A. Data Awareness is not enabled.
B. Logs are arriving from Pre-R81 gateways.
C. Identity Awareness is not enabled.
D. Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 152
Which statement is WRONG regarding the usage of the Central Deployment in SmartConsole?
A. You can install Hotfixes with the Central Deployment in SmartConsole
B. You can install Jumbo Hotfix accumulators with the Central Deployment in SmartConsole.
C. Only be installed Hotfixes can with the Central Deployment in SmartConsole
D. You can upgrade your cluster without user intervention with the Central Deployment in SmartConsole from R80.40 to R81.10.
Answer: C (LEAVE A REPLY)
Explanation

The statement that is wrong regarding the usage of the Central Deployment in SmartConsole is that only be installed Hotfixes can with the Central Deployment in SmartConsole. This is wrong because Central Deployment can also be used to install Jumbo Hotfix accumulators, upgrade clusters, and perform other operations on multiple gateways simultaneously. Central Deployment simplifies and automates the deployment process and reduces human errors and downtime. References: [Check Point Security Expert R81 Administration Guide], page 23.

NEW QUESTION: 153
Alice wants to upgrade the current security management machine from R80.40 to R81.10 and she wants to check the Deployment Agent status over the GAIA CLISH. Which of the following GAIACLISH command is true?
A. show installer status
B. show uninstaller status
C. show installer packages
D. show agent status
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
DLP and Geo Policy are examples of what type of Policy?
A. Standard Policies
B. Shared Policies
C. Inspection Policies
D. Unified Policies
Answer: B (LEAVE A REPLY)
Explanation
DLP and Geo Policy are examples of Shared Policies. Shared Policies are policies that can be applied to multiple gateways or clusters, regardless of their Access Control policy. Shared Policies allow administrators to manage common security settings across different gateways or clusters, such as Data Loss Prevention, Geo Protection, Threat Prevention, HTTPS Inspection, etc. References: R81 Security Management Administration Guide, page 31.

NEW QUESTION: 155
How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?
A. By dropping traffic from websites identified through ThreatCloud Verification and URL Caching
B. By matching logs against ThreatCloud information about the reputation of the website
C. By dropping traffic that is not proven to be from clean websites in the URL Filtering blade
D. By allowing traffic from websites that are known to run Antivirus Software on servers regularly
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156
What is the minimum number of CPU cores required to enable CoreXL?
A. 1
B. 6
C. 2

D. 4
Answer: (SHOW ANSWER)
Explanation
CoreXL is a technology that improves the performance of the Security Gateway by utilizing multiple CPU cores for processing traffic. CoreXL creates multiple instances of the firewall kernel (fwk) that run in parallel on different CPU cores. The number of kernel instances can be configured using the cpconfig command on the Security Gateway3. The minimum number of CPU cores required to enable CoreXL is 2, as one core is reserved for SND (Secure Network Distributor) and one core is used for running a kernel instance4. If the Security Gateway has only one CPU core, CoreXL cannot be enabled. Therefore, the correct answer is C.
References: 3: CoreXL Administration Guide 4: [CoreXL Frequently Asked Questions (FAQ)]

NEW QUESTION: 157
What is the correct order of the default "fw monitor" inspection points?
A. I, i, O, o
B. i, o, I, O
C. i, I, o, O
D. 1, 2, 3, 4
Answer: (SHOW ANSWER)

NEW QUESTION: 158
In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?
A. If the Action of the matching rule is Accept the gateway will drop the packet
B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
D. If the rule does not matched in the Network policy it will continue to other enabled polices
Answer: C (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION: 159
What is the purpose of a SmartEvent Correlation Unit?
A. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
B. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
C. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?
A. SFWDIR/smartevent/conf
B. $RTDIR/smartevent/conf
C. $RTDIR/smartview/conf
D. $FWDIR/smartview/conf
Answer: C (LEAVE A REPLY)
Explanation
To add the company logo to reports, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to the $RTDIR/smartview/conf directory on the SmartEvent server. The $RTDIR is an environment variable that points to the runtime directory of the SmartEvent server, which is usually /opt/CPrt-R81. The smartview/conf directory contains the configuration files for SmartView, which is a web-based interface for viewing reports and dashboards generated by SmartEvent. References: SmartEvent Administration Guide, SK120193 - How to add a company logo to SmartView reports

NEW QUESTION: 161
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. In the Captive Portal screen of Global Properties, check 'Enable Identity Captive Portal'.
B. On the firewall object, Legacy Authentication screen, check 'Enable Identity Captive Portal'.
C. On the Security Management Server object, check the box 'Identity Logging'.
D. Right click Accept in the rule, select "More", and then check 'Enable Identity Captive Portal'.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
Which utility allows you to configure the DHCP service on Gaia from the command line?
A. cpconfig
B. ifconfig
C. dhcp_ofg
D. sysconfig
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following process pulls application monitoring status?
A. fwd

B. fwm
C. cpwd
D. cpd
Answer: D (LEAVE A REPLY)
Explanation
The process that pulls application monitoring status is cpd. cpd is a daemon that runs on Check Point products and performs various tasks related to management communication, policy installation, license verification, logging, etc. cpd also monitors the status of other processes and applications on the system and reports it to the management server. cpd uses SNMP to collect information from various sources, such as blades, gateways, servers, etc. You can view the application monitoring status in SmartConsole by using the Gateways & Servers tab in the Logs & Monitor view. References: Check Point Processes and Daemons

NEW QUESTION: 164
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. fwd
B. fwm
C. cpwd
D. cpd
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
Check Point ClusterXL Active/Active deployment is used when:
A. Only when there is Unicast solution set up.
B. Only when there is Multicast solution set up.
C. There is High Availability solution set up.
D. There is Load Sharing solution set up.
Answer: (SHOW ANSWER)

NEW QUESTION: 166
What is the base level encryption key used by Capsule Docs?
A. SHA-256
B. RSA 1024
C. RSA 2048
D. AES
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
To fully enable Dynamic Dispatcher on a Security Gateway:
A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
B. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu.
C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
D. run fw multik set_mode 1 in Expert mode and then reboot.
Answer: A (LEAVE A REPLY)
Explanation
To fully enable Dynamic Dispatcher on a Security Gateway, you need to run the following command in Expert mode then reboot:

```
fw ctl multik set_mode 9
```

This command sets the multi-core mode to 9, which means that Dynamic Dispatcher is enabled without Firewall Priority Queues. Dynamic Dispatcher is a feature that optimizes the performance of Security Gateways with multiple CPU cores by dynamically allocating traffic to different cores based on their load and priority. Dynamic Dispatcher can improve the throughput and scalability of the Security Gateway, especially for traffic that is not accelerated by SecureXL. The other commands are not valid or do not enable Dynamic Dispatcher. References: R81 Performance Tuning Administration Guide

NEW QUESTION: 168
Where you can see and search records of action done by R81 SmartConsole administrators?
A. In SmartAuditLog View
B. In the Logs & Monitor view, select "Open Audit Log View"
C. In SmartView Tracker, open active log
D. In Smartlog, all logs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 169
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. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
C. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
D. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
SmartEvent does NOT use which of the following procedures to identify events:

A. Matching a log against each event definition
B. Create an event candidate
C. Matching a log against local exclusions
D. Matching a log against global exclusions
Answer: C (LEAVE A REPLY)
Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:
* Matching a Log Against Global Exclusions
* Matching a Log Against Each Event Definition
* Creating an Event Candidate
* When a Candidate Becomes an Event

NEW QUESTION: 171
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.
A. Formal; corporate
B. Local; formal
C. Local; central
D. Central; local
Answer: (SHOW ANSWER)
Explanation
A central license requires an administrator to designate a gateway for attachment whereas a local license is automatically attached to a Security Gateway. A central license is managed by a Security Management Server or a Multi-Domain Security Management Server and can be attached to any gateway that is managed by that server. A local license is managed by a local license server on each gateway and cannot be moved to another gateway. Central licenses are more flexible and scalable than local licenses, as they can be easily transferred between gateways without generating new licenses.

NEW QUESTION: 172
What will SmartEvent automatically define as events?
A. Firewall
B. VPN
C. IPS
D. HTTPS
Answer: C (LEAVE A REPLY)
Explanation
SmartEvent automatically defines events based on IPS (Intrusion Prevention System) alerts. IPS is a feature that detects and prevents malicious network traffic based on predefined or custom signatures. IPS alerts are generated when IPS detects an attack or an anomaly that matches a signature. SmartEvent collects and correlates IPS alerts from different gateways and displays them as events in SmartEventWeb. The other options are not automatically defined as events by SmartEvent.

NEW QUESTION: 173
Fill in the blank: The R81 utility fw monitor is used to troubleshoot _____.
A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiations
Answer: C (LEAVE A REPLY)
Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

NEW QUESTION: 174
What could NOT be a reason for synchronization issues in a Management HA environment?
A. Accidentally, you have configured unique IP addresses per Management Server which invalidates the CA Certificate
B. Servers are in Collision Mode. Two servers, both in active state cannot be synchronized either automatically or manually.
C. There is a network connectivity failure between the servers
D. The products installed on the servers do not match: one device is a Standalone Server while the other is only a Security Management server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Which Check Point daemon monitors the other daemons?
A. fwm
B. cpd
C. cpwd
D. fwssd
Answer: (SHOW ANSWER)
Explanation
The Check Point daemon that monitors the other daemons is cpwd (Check Point Watchdog). It is responsible for monitoring the health and status of various Check Point daemons and processes running on the Security Gateway. If any daemon or process stops responding or encounters an issue, cpwd can restart it to ensure the continued operation of the Security Gateway.
References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 176
VPN Link Selection will perform the following when the primary VPN link goes down?
A. The Firewall will drop the packets.
B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.

C. The Firewall will send out the packet on all interfaces.
D. The Firewall will inform the client that the tunnel is down.
Answer: B (LEAVE A REPLY)
Explanation
VPN Link Selection is a feature that allows the Security Gateway to select the best link for each VPN tunnel based on the network topology and the Link Selection configuration1. When the primary VPN link goes down, the Firewall can update the Link Selection entries to start using a different link for the same tunnel, as long as the remote peer supports this feature and has multiple IP addresses configured2. This way, the VPN tunnel can be maintained without interruption or renegotiation. The other options are not correct because:

Firewall
A). The Firewall will not drop the packets, but will try to send them over another link if possible.

Firewall
C). The Firewall will not send out the packet on all interfaces, but will use the routing table to determine the best interface for each destination.

Firewall
D). The Firewall will not inform the client that the tunnel is down, but will try to keep the tunnel up by switching to another link.
References: IPSec VPN - Link Selection, Outgoing VPN Link Selection on a gateway with multiple external interfaces

NEW QUESTION: 177
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?
A. Threat Emulation
B. Advanced Networking Blade
C. Application Control
D. Anti-Virus

Answer: (SHOW ANSWER)

NEW QUESTION: 178
After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?
A. You will find it in the home directory of your user account (e.g. /home/admin/)
B. You can locate the file via SmartConsole > Command Line.
C. You have to launch the WebUI and go to "Config" -> "Export Config File" and specifiy the destination directory of your local file system.
D. You cannot locate the file in the file system since Clish does not have any access to the bash file system
Answer: (SHOW ANSWER)
Explanation
You will find the config.txt file in the home directory of your user account (e.g. /home/admin/)1. The save configuration config.txt command is a Clish command that saves the current Gaia configuration to a text file2. The file is stored in the home directory of the user who executed the command, and it can be accessed by using the cat or less commands in expert mode1. The file can also be transferred to another machine by using the scp or sftp commands1. The config.txt file contains the Clish commands that are needed to restore the Gaia configuration to the same state as when the file was saved2. The file can be used for backup, migration, or troubleshooting purposes2.
References: How to backup and restore Gaia configuration - Check Point Software, Gaia R81.10 Administration Guide - Check Point Software

NEW QUESTION: 179
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)

NEW QUESTION: 180
GAiA Software update packages can be imported and installed offline in situation where:
A. Security Gateway with GAiA does NOT have SSH access to Internet.
B. The desired CPUSE package is ONLY available in the Check Point CLOUD.
C. Security Gateway with GAiA does NOT have access to Internet.
D. Security Gateway with GAiA does NOT have SFTP access to Internet
Answer: (SHOW ANSWER)

NEW QUESTION: 181
Which Check Point software blade provides Application Security and identity control?
A. URL Filtering
B. Identity Awareness

C. Application Control
D. Data Loss Prevention
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all the following except:
A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution
Answer: (SHOW ANSWER)
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
* Use an automated script to perform common tasks
* Integrate Check Point products with 3rd party solutions
* Create products that use and enhance the Check Point solution

NEW QUESTION: 183
What two ordered layers make up the Access Control Policy Layer?
A. URL Filtering and Network
B. Network and Threat Prevention
C. Application Control and URL Filtering
D. Network and Application Control
Answer: D (LEAVE A REPLY)
Explanation
What two ordered layers make up the Access Control Policy Layer? Network and Application Control are the two ordered layers that make up the Access Control Policy Layer. The Network layer controls network access based on source, destination, service, time, etc. The Application Control layer controls application access based on users, groups, applications, content categories, etc. The Network layer is always processed before the Application Control layer. References: R81 Security Management Administration Guide, page 29.

NEW QUESTION: 184

One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?
A. A lock icon shows that a rule or an object is locked and will be available.
B. A lock icon next to a rule informs that any Administrator is working on this particular rule.
C. AdminA and AdminB are editing the same rule at the same time.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 185
What are valid authentication methods for mutual authenticating the VPN gateways?
A. PKI Certificates and Kerberos Tickets
B. PKI Certificates and DynamicID OTP
C. Pre-Shared Secrets and Kerberos Ticket
D. Pre-shared Secret and PKI Certificates
Answer: (SHOW ANSWER)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/Topics-VPNRG/User-and-Client-Authentication.htm

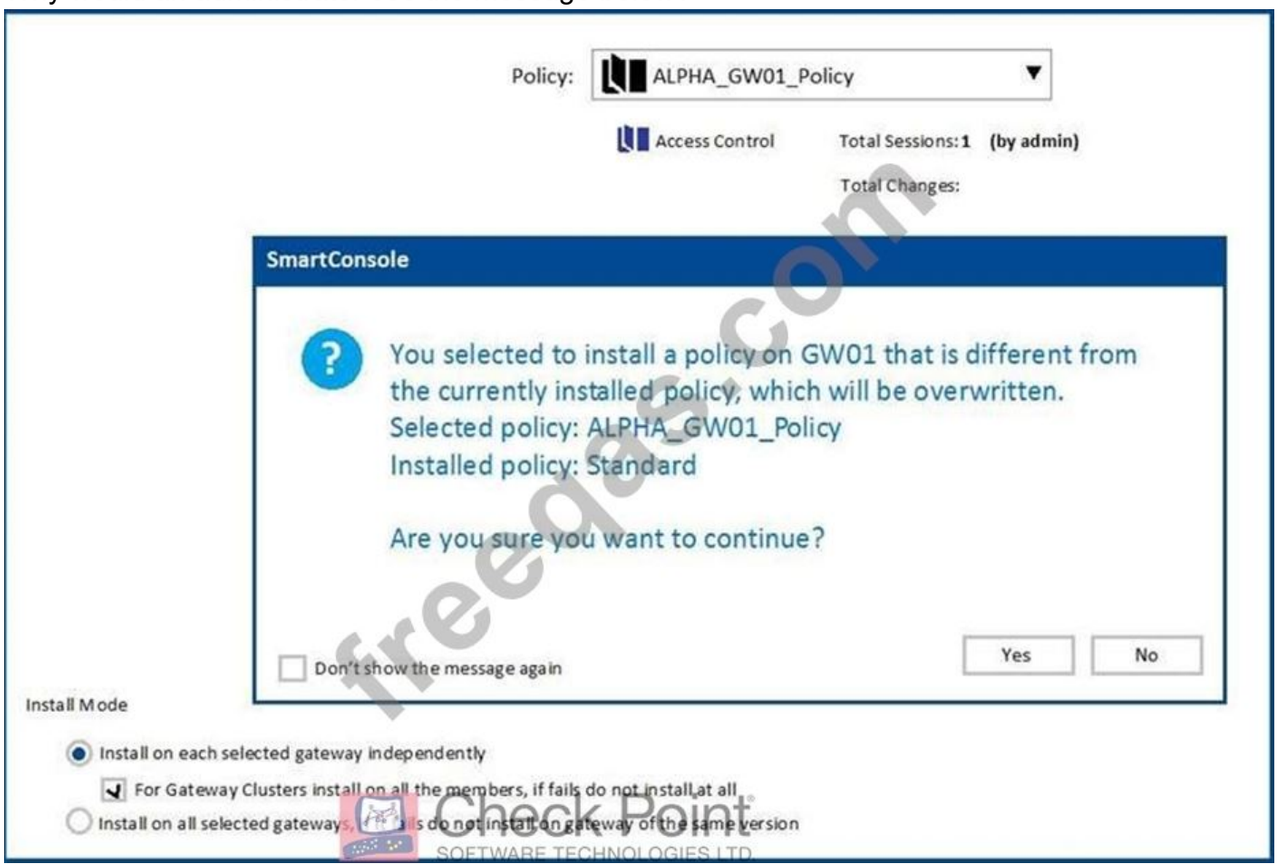
NEW QUESTION: 186
Which web services protocol is used to communicate to the Check Point R81 Identity Awareness Web API?
A. SOAP
B. REST
C. XLANG
D. XML-RPC
Answer: B (LEAVE A REPLY)
The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NEW QUESTION: 187
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?
A. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy
B. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
C. Go to clash-Run cpstop | Run cpstart
D. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
What does the Log "Views" tab show when SmartEvent is Correlating events?

A. Top events with charts and graphs
B. Reports for customization
C. Details of a selected logs
D. A list of common reports
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
Why would an administrator see the message below?



A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.
Answer: B (LEAVE A REPLY)
Explanation
A Policy Package is a set of rules and settings that define how a Security Gateway enforces security on traffic that passes through it. A Policy Package can be created on either the Management Server or the Security Gateway, but it must be installed on both to take effect. When a new Policy Package is created on the Management Server, it must be installed on an existing Security Gateway that has a different Policy Package installed. The message below warns the administrator that installing a new Policy Package will overwrite the existing one on the Security Gateway.

https://www.bing.com/images/blob?bcid=qMoRhR0dzSkGmg
The message also advises the administrator to back up their existing configuration before proceeding with the installation.

NEW QUESTION: 190
Which of the following will NOT affect acceleration?
A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)
Answer: B (LEAVE A REPLY)
Explanation
Check Point's SecureXL technology, which is responsible for acceleration, has certain limitations and conditions under which acceleration may not occur. In this context, the question is asking about factors that will NOT affect acceleration.
Option B, "A 5-tuple match," will not affect acceleration. A 5-tuple match refers to the matching of source IP, source port, destination IP, destination port, and protocol. SecureXL can accelerate traffic that matches these criteria, but it's not a factor that hinders acceleration.
Options A, C, and D can all affect acceleration:
Option A mentions "Connections destined to or originated from the Security gateway," which implies that SecureXL acceleration can apply to these connections.
Option C mentions "Multicast packets," and SecureXL may have limitations in handling multicast traffic efficiently.
Option D mentions "Connections that have a Handler (ICMP, FTP, H.323, etc.)," and certain protocols (such as FTP) may require special handling and might not be fully accelerated by SecureXL.
References: Check Point Certified Security Expert R81 Study Guide

NEW QUESTION: 191
SmartEvent does NOT use which of the following procedures to identify events:
A. Matching a log against each event definition
B. Create an event candidate
C. Matching a log against local exclusions
D. Matching a log against global exclusions
Answer: C (LEAVE A REPLY)
Explanation
SmartEvent does not use matching a log against local exclusions to identify events. Local exclusions are filters that are applied to logs before they are sent to the SmartEvent server. They are used to reduce the amount of logs that are forwarded by the Security Gateways or Log Servers, and to avoid sending irrelevant or sensitive logs. Local exclusions do not affect the event detection process, which is performed by the SmartEvent Correlation Unit on the SmartEvent server. References: Check Point Security Expert R81 Course, SmartEvent Administration Guide, SK120193 - How to configure Local Log Filtering on Security Gateway / Cluster / VSX

NEW QUESTION: 192
Which of the following is a task of the CPD process?
A. Invoke and monitor critical processes and attempts to restart them if they fail
B. Transfers messages between Firewall processes
C. Log forwarding
D. Responsible for processing most traffic on a security gateway
Answer: B (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

NEW QUESTION: 193
What component of Management is used tor indexing?
A. DBSync
B. API Server
C. fwm
D. SOLR
Answer: D (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Multi-DomainSecurityManag

NEW QUESTION: 194
What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)

A. There is a blade reporting a problem.
B. VPN software blade is reporting a malfunction.
C. Security Gateway's MGNT NIC card is disconnected.
D. SmartCenter Server cannot reach this Security Gateway.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 195
Which of the following is NOT a type of Check Point API available in R81.x?
A. Management
B. Identity Awareness Web Services
C. Mobile Access

D. OPSEC SDK
Answer: (SHOW ANSWER)

NEW QUESTION: 196
Fill in the blanks: Gaia can be configured using the _____ or _____ .
A. GaiaUI; command line interface
B. Gaia Interface; GaiaUI
C. Command line interface; WebUI
D. WebUI; Gaia Interface
Answer: C (LEAVE A REPLY)

NEW QUESTION: 197
How many layers make up the TCP/IP model?
A. 2
B. 6
C. 7
D. 4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 198
Which blades and or features are not supported in R81?
A. Identity Awareness
B. SmartConsole Toolbars
C. SmartEvent Maps
D. SmartEvent
Answer: (SHOW ANSWER)

NEW QUESTION: 199
How many interfaces can you configure to use the Multi-Queue feature?
A. 10 interfaces
B. 3 interfaces
C. 4 interfaces
D. 5 interfaces

Answer: D (LEAVE A REPLY)
Explanation
Note -
References:

NEW QUESTION: 200
To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?
A. 5 Network; Host; Objects; Services; API
B. 3 Incoming; Outgoing; Network
C. 2 Internal; External
D. 4 Incoming; Outgoing; Internal; Other
Answer: D (LEAVE A REPLY)
Explanation
To help SmartEvent determine whether events originated internally or externally, you must define the traffic direction using the Initial Settings under General Settings in the Policy Tab. There are four options available to calculate the traffic direction: Incoming, Outgoing, Internal, and Other. Incoming means the source is external and the destination is internal. Outgoing means the source is internal and the destination is external.
Internal means both the source and the destination are internal. Other means both the source and the destination are external. References: SmartEvent R81 Administration Guide

NEW QUESTION: 201
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

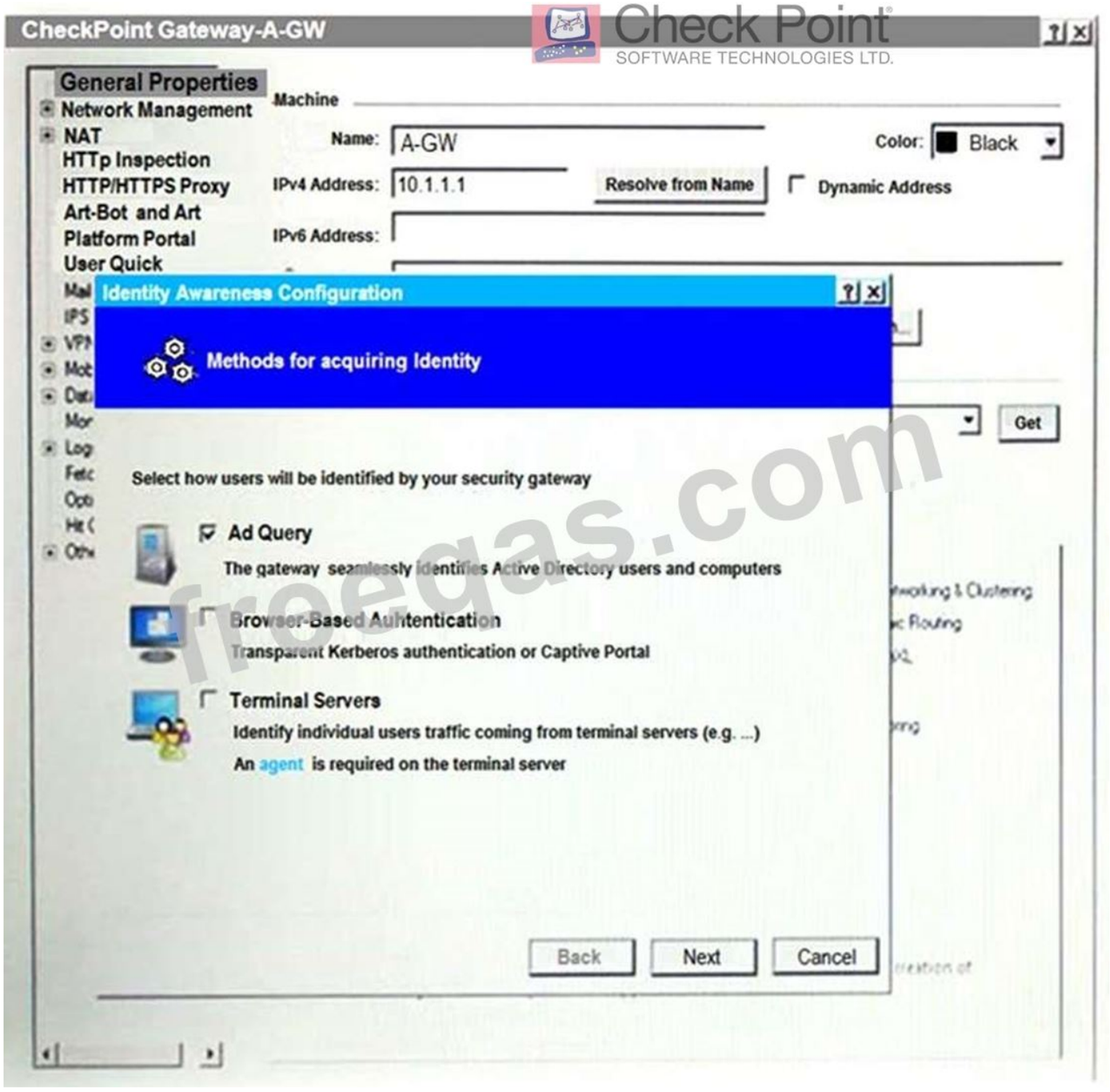
A. Right click Accept in the rule, select "More", and then check 'Enable Identity Captive Portal'.
B. On the firewall object, Legacy Authentication screen, check 'Enable Identity Captive Portal'.
C. In the Captive Portal screen of Global Properties, check 'Enable Identity Captive Portal'.
D. On the Security Management Server object, check the box 'Identity Logging'.
Answer: A (LEAVE A REPLY)
Explanation
The correct way to enable Identity Captive Portal for a specific rule is to right click Accept in the rule, select "More", and then check 'Enable Identity Captive Portal'. This will allow guest users to see the splash page and accept the Terms of Service before accessing the Internet. Identity Captive Portal is a feature that enables identity awareness for guest users who are not authenticated by other methods, such as Active Directory or Identity Agent. Identity Captive Portal can be enabled globally or per rule, depending on the security policy requirements.

NEW QUESTION: 202

Return oriented programming (ROP) exploits are detected by which security blade?
A. Intrusion Prevention Software
B. Check Point Anti-Virus / Threat Emulation
C. Data Loss Prevention
D. Application control
Answer: B (LEAVE A REPLY)
Explanation
Return-oriented programming (ROP) exploits are detected by Check Point Anti-Virus / Threat Emulation blade. ROP exploits are a type of code reuse attack that bypasses common exploit mitigation techniques such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Check Point Anti-Virus / Threat Emulation blade can detect and prevent ROP exploits using its behavioral analysis engine that monitors the execution flow of processes and identifies malicious patterns. References: [Check Point Security Expert R81 Threat Prevention Administration Guide], page 17.

NEW QUESTION: 203
SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:
A. ping, traceroute, netstat, and route
B. ping, nslookup, Telnet, and route
C. ping, whois, nslookup, and Telnet
D. ping, traceroute, netstat, and nslookup
Answer: (SHOW ANSWER)
Explanation
The default commands that appear when right-clicking the IP address, source or destination, in an event in SmartEvent are ping, whois, nslookup, and Telnet. SmartEvent is a unified security event management solution that provides visibility, analysis, and reporting of security events across multiple Check Point products. SmartEvent has a feature that allows administrators to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands that can be executed on the IP address of the active cell. The default commands are ping, whois, nslookup, and Telnet. Ping is a command that tests the connectivity and latency between two hosts by sending packets and measuring the response time. Whois is a command that queries a database for information about the owner and registrar of a domain name or an IP address. Nslookup is a command that queries a DNS server for information about a domain name or an IP address, such as its IP address, name server, mail server, etc. Telnet is a command that establishes a remote connection to another host using the Telnet protocol.

NEW QUESTION: 204
On the following picture an administrator configures Identity Awareness:



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

A. Obligatory usage of Captive Portal.

B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.

C. Kerberos SSO which will be working for Active Directory integration

D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: (SHOW ANSWER)

NEW QUESTION: 205

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop
2	Management	net_10.28.0.0	GW-R7730	* Any	https ssh	Accept
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop
4	DNS	net_10.28.0.0	* Any	* Any	dns	Accept
5	Web	net_10.28.0.0	* Any	* Any	http https	Accept
6	DMZ Access	net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp AP-Defender	Accept
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop

You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
What does this mean?

A. This rule No. 6 has been marked for deletion in your Management session.
B. This rule No. 6 has been marked for deletion in another Management session.
C. This rule No. 6 has been marked for editing in your Management session.
D. This rule No. 6 has been marked for editing in another Management session.

Answer: C (LEAVE A REPLY)

Explanation

You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
This means that rule No.6 has been marked for editing in your Management session. In R81, every administrator works in a session that is independent of other administrators. Changes made by one administrator are not visible to others until they are published. When you edit a rule, it is marked with a pencil icon to indicate that it has been modified in your session. You can also lock a rule to prevent other administrators from editing it until you unlock it or publish your session. References: R81 Security Management Administration Guide, page 43.

NEW QUESTION: 206

Which two Cluster Solutions are available under R81.10?

A. ClusterXL and NSRP
B. VRRPandHSRP
C. VRRP and IP Clustering
D. ClusterXL and VRitP

Answer: D (LEAVE A REPLY)

Explanation

ClusterXL and VRRP are the two cluster solutions that are available under R81.10. According to the ClusterXL R81.10 Administration Guide1, ClusterXL is a Check Point software-based clustering solution that provides high availability and load sharing for Check Point Security Gateways and Cluster Members.

ClusterXL supports two modes: High Availability and Load Sharing. In High Availability mode, all Cluster Members are connected to the same network segment and share a virtual IP address. One member is active and handles all traffic, while the others are in standby mode and ready to take over in case of a failure. In Load Sharing mode, all Cluster Members are active and share the traffic load according to a predefined algorithm. ClusterXL supports both unicast and multicast modes for Load Sharing1.
VRRP (Virtual Router Redundancy Protocol) is an industry standard protocol that provides high availability for routers or firewalls by creating a virtual router with a virtual IP address that is shared by a group of routers or firewalls. One router or firewall is elected as the master and handles all traffic directed to the virtual IP address, while the others are backups that monitor the master and take over if it fails. VRRP can be used with Check Point Security Gateways to provide redundancy and failover for external interfaces1.
NSRP (NetScreen Redundancy Protocol) is a proprietary protocol developed by Juniper Networks that provides high availability and load balancing for NetScreen firewalls. NSRP is not supported by Check Point products2.
HSRP (Hot Standby Router Protocol) is a Cisco proprietary protocol that provides high availability for routers by creating a virtual router with a virtual IP address that is shared by a group of routers. One router is elected as the active router and handles all traffic directed to the virtual IP address, while another router is elected as the standby router and monitors the active router and takes over if it fails. HSRP is not supported by Check Point products.
IP Clustering is a feature of Linux Virtual Server (LVS) that provides high availability and load balancing for IP-based services by creating a cluster of real servers that are accessed through a virtual IP address. The cluster is managed by a director that routes requests to the real servers according to a scheduling algorithm. IP Clustering is not supported by Check Point products.
References: : ClusterXL R81.10 Administration Guide : Check Point R81.10 : Solved: R81.10 - Check Point CheckMates : [Hot Standby Router Protocol - Wikipedia] : [Linux Virtual Server - Wikipedia]

NEW QUESTION: 207
What is the default shell for the command line interface?
A. Expert
B. Clish
C. Admin
D. Normal
Answer: (SHOW ANSWER)
The default shell of the CLI is called clish

NEW QUESTION: 208
What is false regarding prerequisites for the Central Deployment usage?
A. The administrator must have write permission on SmartUpdate
B. Security Gateway must have the latest CPUSE Deployment Agent
C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
D. The Security Gateway must have a policy installed
Answer: C (LEAVE A REPLY)
Explanation

Establishing SIC between gateways and the management server is a prerequisite for Central Deployment usage, as the CDT tool will not take care of this automatically1. The administrator must have write permission on SmartUpdate, the Security Gateway must have the latest CPUSE Deployment Agent, and the Security Gateway must have a policy installed2. These are the basic requirements for using the Central Deployment Tool (CDT), which is a utility that lets you manage a deployment of software packages from your Management Server to the multiple managed Security gateways and cluster members at the same time2. The CDT can perform various actions, such as installation of software packages, taking snapshots, running shell scripts, pushing/pulling files, and automating the RMA backup and restore process2. The CDT is supported on Check Point Appliances with R80.40 and higher versions2. References: How to keep your Security Gateways up to date - Check Point Software, Central Deployment Tool (CDT) - Check Point CheckMates.

NEW QUESTION: 209
When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?
A. IP
B. SIC
C. NAT
D. FQDN
Answer: C (LEAVE A REPLY)
Explanation
NAT (Network Address Translation) is one item that will not be configured on the R81 Security Management Server when setting up an externally managed log server. NAT is a technique that allows devices with private IP addresses to communicate with devices with public IP addresses by translating the private addresses to public ones. NAT is not relevant for configuring an externally managed log server, which requires only the IP address, SIC (Secure Internal Communication), and FQDN (Fully Qualified Domain Name) of the log server.
References: Check Point Security Expert R81 Course, Logging and Monitoring Administration Guide

NEW QUESTION: 210
What is mandatory for ClusterXL to work properly?
A. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members
B. The Sync interface must not have an IP address configured
C. The Magic MAC number must be unique per cluster node
D. The number of cores must be the same on every participating cluster node
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
In which formats can Threat Emulation forensics reports be viewed in?
A. TXT, XML and CSV
B. PDF and TXT
C. PDF, HTML, and XML

D. PDF and HTML
Answer: (SHOW ANSWER)
Explanation
The formats in which Threat Emulation forensics reports can be viewed in are PDF, HTML, and XML. Threat Emulation is a feature that detects and prevents zero-day attacks by emulating files in a sandbox environment and analyzing their behavior. Threat Emulation generates forensics reports that provide detailed information about the emulated files, such as verdict, severity, activity summary, screenshots, network activity, registry activity, file activity, and process activity. These reports can be viewed in PDF, HTML, or XML formats from SmartConsole or SmartView.

NEW QUESTION: 212
What traffic does the Anti-bot feature block?
A. Network traffic that is directed to unknown or malicious servers
B. Command and Control traffic to servers with reputation for hosting malware
C. Network traffic to hosts that have been identified as infected
D. Command and Control traffic from hosts that have been identified as infected
Answer: D (LEAVE A REPLY)

NEW QUESTION: 213
Can multiple administrators connect to a Security Management Server at the same time?
A. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
B. Yes, all administrators can modify a network object at the same time
C. No, only one can be connected
D. Yes, but only one has the right to write.
Answer: (SHOW ANSWER)

NEW QUESTION: 214
Which packet info is ignored with Session Rate Acceleration?
A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used
Answer: C (LEAVE A REPLY)

Explanation
Identifies connections by five attributes
- source address
- destination address
- source port
- destination port
- protocol

NEW QUESTION: 215
On what port does the CPM process run?
A. TCP 857
B. TCP 18192
C. TCP 900
D. TCP 19009
Answer: (SHOW ANSWER)
Explanation
The port that the CPM process runs on is TCP 19009. CPM stands for Check Point Management, and it is the main process that runs on the Security Management Server and interacts with SmartConsole clients. CPM is responsible for managing policies, objects, logs, tasks, and other management functions. CPM listens on TCP port 19009 for incoming connections from SmartConsole clients. The other ports are either used by other processes or not related to CPM.

NEW QUESTION: 216
Alice was asked by Bob to implement the Check Point Mobile Access VPN blade - therefore are some basic configuration steps required - which statement about the configuration steps is true?
A. 1. Add a rule in the Access Control Policy and install policy
2. Configure Mobile Access parameters in Security Gateway object
3. Enable Mobile Access blade on the Security Gateway object and complete the wizard
4. Connect to the Mobile Access Portal
B. 1. Connect to the Mobile Access Portal
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Configure Mobile Access parameters in Security Gateway object
4. Add a rule in the Access Control Policy and install policy
C. 1. Configure Mobile Access parameters in Security Gateway object
2. Enable Mobile Access blade on the Security Gateway object and complete the wizard
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal
D. 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard
2. Configure Mobile Access parameters in Security Gateway object
3. Add a rule in the Access Control Policy and install policy
4. Connect to the Mobile Access Portal

Answer: D (LEAVE A REPLY)

Explanation

The verified answer is D. 1. Enable Mobile Access blade on the Security Gateway object and complete the wizard 2. Configure Mobile Access parameters in Security Gateway object 3. Add a rule in the Access Control Policy and install policy 4. Connect to the Mobile Access Portal The basic configuration steps for the Check Point Mobile Access VPN blade are as follows1:

Enable Mobile Access blade on the Security Gateway object and complete the wizard: This step activates the Mobile Access blade on the selected gateway and guides you through the initial configuration, such as defining the portal name, the certificate, and the authentication methods.

Configure Mobile Access parameters in Security Gateway object: This step allows you to customize the Mobile Access settings, such as defining the supported applications, the access roles, the client settings, and the advanced options.

Add a rule in the Access Control Policy and install policy: This step creates a rule that allows the traffic from the Mobile Access portal to the protected resources and installs the policy on the gateway.

Connect to the Mobile Access Portal: This step verifies that the Mobile Access portal is accessible and functional from a web browser or a mobile device.

The other options are incorrect because they do not follow the correct order or include the necessary steps.

References:

Mobile Access Administration Guide R81 - Check Point Software1

NEW QUESTION: 217

What are possible Automatic Reactions in SmartEvent?

A. Web Mail, Block Service. SNMP Trap. SmartTask, Geo Protection

B. Web Mail. Block Destination, SNMP Trap. SmartTask

C. Mail. SNMP Trap, Block Source. Block Event Activity, External Script

D. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Answer: C (LEAVE A REPLY)

NEW QUESTION: 218

When gathering information about a gateway using CPINFO, what information is included or excluded when using the "-x" parameter?

A. Output excludes connection table

B. Gets information about the specified Virtual System

C. Includes the registry

D. Does not resolve network addresses

Answer: B (LEAVE A REPLY)

NEW QUESTION: 219

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

A. Centos Linux

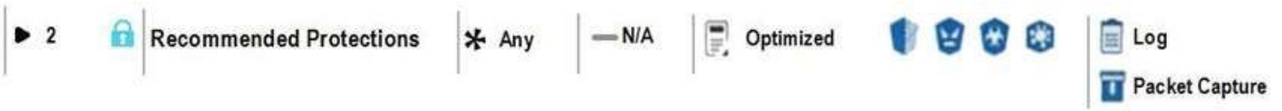
B. Gaia embedded.
C. Gaia
D. Red Hat Enterprise Linux version 5
Answer: B (LEAVE A REPLY)
"These appliances run an embedded version of the Gaia operating system."
https://sc1.checkpoint.com/documents/SMB_R80.20.20/AdminGuides/Locally_Managed/EN/Topics/Quantum-Spark-1500-1600-1800-Appliance-Series-Overview.htm

NEW QUESTION: 220
What is the minimum number of CPU cores required to enable CoreXL?
A. 1
B. 6
C. 2
D. 4
Answer: C (LEAVE A REPLY)
Default number of CoreXL IPv4 FW instances:
Note: The real number of CoreXL FW instances depends on the current CoreXL license.
Number of
CPU cores Default number of
CoreXL IPv4
FW instances Default number of
Secure Network Distributors
(SNDs)
1 1
Note: CoreXL is disabled 0
Note: CoreXL is disabled
2 2 2
4 3 1
6 - 20 [Number of CPU cores] - 2 2
More than 20 (1) [Number of CPU cores] - 4 4

NEW QUESTION: 221
When performing a minimal effort upgrade, what will happen to the network traffic?
A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.
B. All connections that were initiated before the upgrade will be handled by the active gateway
C. All connections that were initiated before the upgrade will be handled normally
D. All connections that were initiated before the upgrade will be handled by the standby gateway
Answer: B (LEAVE A REPLY)
Explanation
All connections that were initiated before the upgrade will be handled by the active gateway. According to the Check Point documentation1, a minimal effort upgrade is a procedure that allows you to upgrade each Security Gateway

individually, without affecting the cluster operation. The active gateway continues to handle the traffic while the standby gateway is upgraded, and then they switch roles. This way, there is no network downtime and no need to synchronize the cluster members before or after the upgrade1. However, some connections may be dropped during the switch-over, so it is recommended to use a connectivity upgrade or a zero downtime upgrade for mission-critical environments2.
References: : Best Practices - Security Gateway Performance - Check Point Software : Checkpoint Cluster Firmware Upgrade - Check Point CheckMates

NEW QUESTION: 222
Which of the following is a new R81 Gateway feature that had not been available in R77.X and older?
A. The rule base can be built of layers, each containing a set of the security 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.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. Time object to a rule to make the rule active only during specified times.
D. Sub Policies ae 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.
Answer: D (LEAVE A REPLY)
Explanation
Sub Policies are a new R81 Gateway feature that had not been available in R77.X and older. 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. This allows for more granular and modular control over the policy. The other features were already available in previous versions . References: Check Point R81 Security Management Administration Guide, Check Point R77 Security Management Administration Guide, Check Point R77 Gaia Administration Guide, Check Point R77 Security Gateway Technical Administration Guide

NEW QUESTION: 223
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)


A. The current administrator has read-only permissions to Threat Prevention Policy.
B. Another user has locked the rule for editing.
C. Configuration lock is present. Click the lock symbol to gain read-write access.
D. The current administrator is logged in as read-only because someone else is editing the policy.
Answer: B (LEAVE A REPLY)
Explanation
The lock symbol in the left column of the rule means that another user has locked the rule for editing. This is to prevent multiple users from editing the same rule at the same time and causing conflicts. References: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Top

NEW QUESTION: 224

What is a best practice before starting to troubleshoot using the "fw monitor" tool?
A. Run the command: fw monitor debug on
B. Clear the connections table
C. Disable CoreXL
D. Disable SecureXL
Answer: (SHOW ANSWER)
Explanation
A best practice before starting to troubleshoot using the fw monitor tool is to disable SecureXL. SecureXL is a performance acceleration solution that optimizes the packet flow through the Security Gateway. However, SecureXL can also bypass some inspection points and cause some packets to be invisible to fw monitor.
Therefore, disabling SecureXL can ensure that fw monitor captures all the relevant packets for troubleshooting purposes. References: Check Point Security Expert R81 Course, fw monitor, SecureXL

NEW QUESTION: 225
As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?
A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
B. Fill Layer4 VPN -SSL VPN that gives users network access to all mobile applications.
C. Full Layer3 VPN -IPSec VPN that gives users network access to all mobile applications.
D. You can make sure that documents are sent to the intended recipients only.
Answer: C (LEAVE A REPLY)
Explanation
The feature that provides Full Layer3 VPN -IPSec VPN, giving users network access to all mobile applications, is the correct answer.
Capsule Connect/VPN is used to establish secure VPN connections for mobile devices, and the Full Layer3 VPN (IPSec VPN) option provides comprehensive network access.
References: Check Point documentation or training materials related to Mobile Access Methods and VPN configurations.

NEW QUESTION: 226
Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?
A. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type
Answer: (SHOW ANSWER)
Explanation
The statement that is most correct regarding about "CoreXL Dynamic Dispatcher" is: The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores. CoreXL Dynamic Dispatcher is a feature that allows

the Security Gateway to dynamically assign connections to the most available CoreXL FW instance, based on the CPU core utilization. This improves the performance and load balancing of the Security Gateway, especially when handling connections with different processing requirements. The other statements are either incorrect or describe the CoreXL Static Dispatcher mechanism, which assigns connections based on a hash function of the Source IP, Destination IP, and IP Protocol type.

NEW QUESTION: 227
From SecureXL perspective, what are the tree paths of traffic flow:
A. Initial Path; Medium Path; Accelerated Path
B. Layer Path; Blade Path; Rule Path
C. Firewall Path; Accept Path; Drop Path
D. Firewall Path; Accelerated Path; Medium Path
Answer: D (LEAVE A REPLY)
Explanation
SecureXL is a technology that improves the performance of Security Gateway by offloading the processing of some packets from the Firewall kernel to the SecureXL device driver1. SecureXL can handle packets in three different paths, depending on the type and state of the packet2:
Firewall Path: This is the slowest path, where packets are processed by the Firewall kernel and all the inspection blades. This path is used for packets that require full inspection, such as the first packet of a connection, packets that match a rule with a UTM blade, or packets that are not eligible for acceleration.
Accelerated Path: This is the fastest path, where packets are processed by the SecureXL device driver and bypass the Firewall kernel. This path is used for packets that belong to an established connection that is marked for acceleration, and do not require any further inspection by the Firewall or other blades.
Medium Path: This is a hybrid path, where packets are processed by both the SecureXL device driver and the Firewall kernel, but skip some inspection steps. This path is used for packets that belong to an established connection that is not marked for acceleration, but do not require full inspection by all the blades.
The other options are not correct because:
A: Initial Path; Medium Path; Accelerated Path: There is no such thing as Initial Path in SecureXL terminology. The initial packet of a connection is always handled by the Firewall Path.
B: Layer Path; Blade Path; Rule Path: These are not paths of traffic flow, but components of the unified policy in R80 and above versions. The Layer Path refers to the order of layers in the policy, the Blade Path refers to the order of blades within a layer, and the Rule Path refers to the order of rules within a blade3.

C: Firewall Path; Accept Path; Drop Path: These are not paths of traffic flow, but possible actions that the Firewall can take on a packet. The Firewall Path is one of the paths of traffic flow, but the Accept Path and Drop Path are not. The Accept Path means that the packet is allowed to pass through the Firewall, and the Drop Path means that the packet is blocked by the Firewall4.
References: Part 3 - SecureXL, What is CoreXL & SecureXL, SecureXL Fast Accelerator (fw fast_accel) for R80.20 and above, QUANTUM 7000 SECURITY GATEWAY

NEW QUESTION: 228
Which packet info is ignored with Session Rate Acceleration?
A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used
Answer: (SHOW ANSWER)
Explanation
Session Rate Acceleration is a SecureXL feature that accelerates the establishment of new connections by bypassing the inspection of the first packet of each session. Session Rate Acceleration ignores the source port information of the packet, as well as the destination port ranges, protocol type, and VPN information. The other packet info is used by Packet Acceleration, which is another SecureXL feature that accelerates the forwarding of subsequent packets of an established connection. References: SecureXL Mechanism

NEW QUESTION: 229
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?
A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
B. mgmt_cli add host name "Server_1" ip-address "10.15.123.10" --format json
C. mgmt_cli add object-host "Server_1" ip-address "10.15.123.10" --format json
D. mgmt._cli add object "Server-1" ip-address "10.15.123.10" --format json
Answer: B (LEAVE A REPLY)
Explanation
The correct syntax to import a host object using mgmt_cli is mgmt_cli add host name <name> ip-address <ip-address> --format <format>1. The name and ip-address parameters are mandatory, while the format parameter is optional and can be either json or txt. The other options are incorrect because they either use wrong parameters, wrong hyphens, or wrong object types. References: 1: Check Point Resource Library2

NEW QUESTION: 230
Which of these is an implicit MEP option?
A. Round robin
B. Load Sharing
C. Source address based
D. Primary-backup
Answer: (SHOW ANSWER)

NEW QUESTION: 231
Alice wants to upgrade the current security management machine from R80.40 to R81.10 and she wants to check the Deployment Agent status over the GAIA CLISH. Which of the following GAIACLISH command is true?
A. show agent status
B. show uninstaller status
C. show installer packages
D. show installer status
Answer: D (LEAVE A REPLY)
Explanation
The correct command for checking the Deployment Agent status over the GAIA CLISH is "show installer status". This command displays information about the Deployment Agent such as its version, status, last update time, and last operation result. The other commands are either invalid or irrelevant for this purpose.
References: [Check Point Security Expert R81 Installation and Upgrade Guide], page 23.

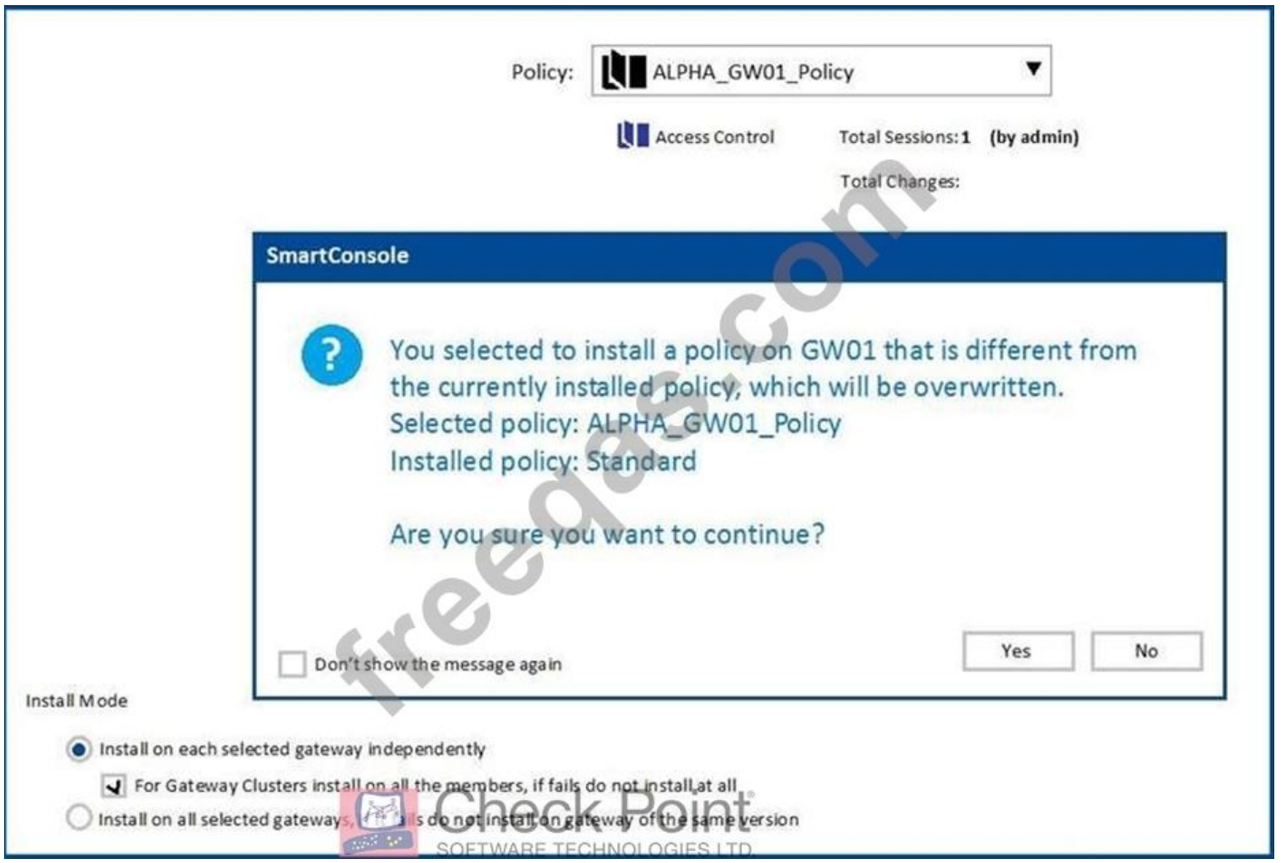
NEW QUESTION: 232
What is the most recommended way to install patches and hotfixes?
A. Software Update Service
B. CPUSE Check Point Update Service Engine
C. UnixinstallScript
D. rpm -Uv
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
What is the correct description for the Dynamic Balancing / Split feature?
A. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
B. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
C. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's. The interface must support Multi-Queue. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
D. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
Answer: D (LEAVE A REPLY)
Explanation
The correct description for the Dynamic Balancing / Split feature is:
Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load. It is only available on Quantum Appliances (not on Quantum Spark or Open Server) The Dynamic Balancing / Split feature is a performance-enhancing daemon that balances the load between CoreXL SNDs and CoreXL Firewalls. It

monitors the average CPU utilization of CoreXL Firewall and SND instances and automatically increases or decreases the number of CoreXL Firewall instances. The Dynamic Balancing Daemon (dsd) has three stages in each iteration: Examine the current CPU utilization, Calculate the optimal split, and Apply the new split1.
The Dynamic Balancing / Split feature is supported on Check Point Appliances, such as Quantum Appliances, Quantum Maestro, Quantum Security Gateways, and Quantum LightSpeed Appliances in KPPAK mode2. It is not supported on Quantum Spark appliances, which are designed for small and medium businesses. It is also not supported on Open Server platforms, which are general-purpose servers that run Check Point software on top of third-party operating systems.
References: Dynamic Balancing for CoreXL; Maestro and Dynamic Balancing (Dynamic Split); Dynamic Balancing available on R80.40; [Quantum Spark Appliances]; [Open Server]

NEW QUESTION: 234
What are valid authentication methods for mutual authenticating the VPN gateways?
A. PKI Certificates and Kerberos Tickets
B. PKI Certificates and DynamicID OTP
C. Pre-Shared Secrets and Kerberos Ticket
D. Pre-shared Secret and PKI Certificates
Answer: D (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/T

NEW QUESTION: 235
Why would an administrator see the message below?



A. A new Policy Package created on the Management is going to be installed to the existing Gateway.
B. A new Policy Package created on the Gateway 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.
C. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
D. A new Policy Package created on the Gateway is going to be installed on the existing Management.
Answer: (SHOW ANSWER)

NEW QUESTION: 236
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
The correct way to enable Identity Captive Portal for a specific rule is to right click Accept in the rule, select

"More", and then check 'Enable Identity Captive Portal'. This will allow guest users to see the splash page and accept the Terms of Service before accessing the Internet. Identity Captive Portal is a feature that enables identity awareness for guest users who are not authenticated by other methods, such as Active Directory or Identity Agent. Identity Captive Portal can be enabled globally or per rule, depending on the security policy requirements.

NEW QUESTION: 237
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 192.168.80.200 255.255.255.0set 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 24add 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. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
Answer: D (LEAVE A REPLY)

NEW QUESTION: 238
Which command will allow you to see the interface status?
A. cphaprob interface
B. cphaprob -I interface
C. cphaprob -a if
D. cphaprob stat
Answer: C (LEAVE A REPLY)
Explanation
The cphaprob -a if command displays the interface status of all cluster members, including the interface name, IP address, state, monitor mode, and sync status. References: cphaprob - Check Point Support Center

NEW QUESTION: 239
What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?
A. Advanced Upgrade only
B. CPUSE offline upgrade only
C. Advanced upgrade or CPUSE offline upgrade
D. SmartUpdate offline upgrade
Answer: C (LEAVE A REPLY)

NEW QUESTION: 240
Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?
A. The Standby Member

B. The Active Member
C. The Primary Member
D. The Secondary Member
Answer: A (LEAVE A REPLY)
Explanation
In a Zero downtime upgrade, you should upgrade the Standby Member first. This is because the Standby Member does not process traffic and can be upgraded without affecting the cluster availability. After upgrading the Standby Member, you can perform a failover and make it the Active Member. Then you can upgrade the original Active Member, which becomes the Standby Member after the failover.
References: Getting Started - Check Point Software, section "Upgrading Cluster Members with Zero Downtime"

NEW QUESTION: 241
What is the command to show SecureXL status?
A. fwaccel status
B. fwaccel stats -m
C. fwaccel -s
D. fwaccel stat
Answer: D (LEAVE A REPLY)
Explanation
The command to show SecureXL status is fwaccel stat. This command displays information about SecureXL acceleration, such as the number of accelerated and non-accelerated connections, the reason for non-acceleration, and the SecureXL device name and mode. The other commands are either invalid or show different statistics.

NEW QUESTION: 242
Which process handles connection from SmartConsole R81?
A. fwm
B. cpmd
C. cpm
D. cpd
Answer: C (LEAVE A REPLY)
Explanation
The CPM process handles connection from SmartConsole R81. The CPM process is the main process of the Security Management Server and the Multi-Domain Security Management Server. It is responsible for managing the database,

handling policy installation, communicating with SmartConsole clients, and providing REST API services. The CPM process runs on port 19009 and uses the CPD process as a proxy for communication with other processes.
References:
Check Point Processes and Daemons, section "CPM"
Check Point R81, section "SmartConsole"
Check Point R81.20, section "REST API"

NEW QUESTION: 243
When simulating a problem on ClusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?
A. cphaprob -d STOP unregister
B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob -d unregister STOP
Answer: (SHOW ANSWER)
Explanation
When simulating a problem on a ClusterXL cluster with the command "cphaprob -d STOP -s problem -t 0 register" to initiate a failover on an active cluster member, you can use the command "cphaprob -d STOP unregister" to remove the problematic state and return the cluster to normal operation.
Option A correctly identifies the command that allows you to remove the problematic state, making it the verified answer.
References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 244
What destination versions are supported for a Multi-Version Cluster Upgrade?
A. R81.40 and later
B. R76 and later
C. R70 and Later
D. R81.10 and Later
Answer: D (LEAVE A REPLY)
Explanation
The destination versions that are supported for a Multi-Version Cluster Upgrade are R81.10 and later. This means that the cluster members can be upgraded from any supported version to R81.10 or higher using the Multi-Version Cluster mode. R81.40, R76, and R70 are not supported destination versions for a Multi-Version Cluster Upgrade.
References: : Check Point Software, Getting Started, Supported Upgrade Paths

NEW QUESTION: 245
Which is the command to identify the NIC dnver before considering about the employment of the Multi-Queue feature?
A. ifconfig -i eth0 verbose
B. ip show Int eth0
C. ethtool A eth0

D. show interface eth0 mq
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?
A. Check Point Remote User
B. Check Point Capsule Workspace
C. Check Point Mobile Web Portal
D. Check Point Capsule Remote
Answer: (SHOW ANSWER)
Explanation
Check Point Mobile Web Portal is a Mobile Access Application that allows a secure container on mobile devices to give users access to internal websites, file shares and emails. The Mobile Web Portal is a web-based application that can be accessed from any browser on any device. It provides a user-friendly interface to access various resources on the corporate network without requiring a VPN client or additional software installation.
The Mobile Web Portal supports authentication methods such as user name and password, certificate, one-time password (OTP), etc. The Mobile Web Portal also supports security features such as encryption, data leakage prevention (DLP), threat prevention, etc. References: R81 Mobile Access Administration Guide

NEW QUESTION: 247
You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?
A. edit fwaffinity.conf; reboot required
B. cpconfig; reboot required
C. edit fwaffinity.conf; reboot not required
D. cpconfig; reboot not required
Answer: B (LEAVE A REPLY)
Explanation
To change the number of firewall instances used by CoreXL, the cpconfig command must be used, followed by a reboot. CoreXL is a technology that improves the performance of the Security Gateway by using multiple cores to handle concurrent connections. The number of firewall instances determines how many cores are dedicated to CoreXL. The cpconfig command allows the administrator to configure various settings on the Security Gateway, including the number of firewall instances. After changing this setting, a reboot is required for the changes to take effect. The other commands are either incorrect or do not require a reboot.

NEW QUESTION: 248
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Stateful Mode configuration, chain modules marked with _____ will not apply.
A. 1
B. 3

C. ffff
D. 2
Answer: (SHOW ANSWER)

NEW QUESTION: 249
What command verifies that the API server is responding?
A. api stat
B. api status
C. show api_status
D. app_get_status
Answer: (SHOW ANSWER)
Explanation
The API server is a service that runs on the Security Management Server and enables external applications to communicate with the Check Point management database using REST APIs. You can verify that the API server is responding by using the following command in Expert mode:

```
api status
```

This command will display the current status of the API server, such as running, stopped, or initializing. It will also show the API version, port number, and SSL certificate information. References: Check Point R81 REST API Reference Guide

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 Management Server name cannot be changed in SmartConsole without re-establishing trust.
C. The Security Gateway name cannot be changed in command line without re-establishing trust.
D. The Security Management Server IP-address cannot be changed without re-establishing the trust.
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which Queue in the Priority Queue has the maximum priority?
A. High Priority
B. Control
C. Routing
D. Heavy Data Queue
Answer: C (LEAVE A REPLY)
Explanation
The Priority Queue is a feature that allows the firewall to prioritize certain types of traffic over others, such as control and routing traffic, when the CPU load is high. The Priority Queue has four levels of priority: Control, Routing, High Priority and Heavy Data Queue1. The Control level has the highest priority and is reserved for firewall control traffic,

such as policy installation and synchronization. The Routing level has the second highest priority and is used for routing protocols, such as OSPF and BGP. The High Priority level has the third highest priority and is used for user-defined traffic that needs to be prioritized, such as VoIP or video conferencing. The Heavy Data Queue level has the lowest priority and is used for bulk data transfer, such as FTP or HTTP2. Therefore, the correct answer is C. References: 1: Firewall Priority Queues 2: Firewall Priority Queues setting

NEW QUESTION: 252
What is the benefit of Manual NAT over Automatic NAT?
A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy.
B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
C. You have the full control about the priority of the NAT rules
D. On IPSO and GAIA Gateways, it is handled in a stateful manner
Answer: C (LEAVE A REPLY)
Explanation
The benefit of Manual NAT over Automatic NAT is that you have full control over the priority of the NAT rules. Manual NAT allows you to create NAT rules that are independent of the security policy and specify the order in which they are applied. Automatic NAT creates NAT rules based on the objects' NAT properties and places them according to predefined criteria. The other options are not benefits of Manual NAT over Automatic NAT. References: : Check Point Software, Getting Started, NAT Rule Base.

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

NEW QUESTION: 254
Which of the following will NOT affect acceleration?
A. Connections that have a Handler (ICMP, FTP, H.323, etc.)
B. A 5-tuple match
C. Connections destined to or originated from the Security gateway
D. Multicast packets
Answer: B (LEAVE A REPLY)

NEW QUESTION: 255
Which feature is NOT provided by all Check Point Mobile Access solutions?
A. Support for IPv6
B. Granular access control

C. Strong user authentication
D. Secure connectivity
Answer: A (LEAVE A REPLY)
Explanation
The feature that is not provided by all Check Point Mobile Access solutions is support for IPv6. Check Point Mobile Access is a comprehensive solution that provides secure remote access to corporate applications and resources using various methods, such as SSL VPN, IPsec VPN, clientless VPN, and mobile VPN. However, not all of these methods support IPv6, which is the latest version of the Internet Protocol that uses 128-bit addresses. According to the Check Point Mobile Access R81 Administration Guide1, only the following Mobile Access methods support IPv6:
SSL Network Extender (SNX) - a thin client that enables remote users to connect securely to the corporate network using SSL/TLS VPN.
Mobile VPN - a full VPN client that enables remote users to connect securely to the corporate network using IPsec VPN.
Capsule Connect - a mobile VPN app for iOS and Android devices that enables remote users to connect securely to the corporate network using IPsec VPN.
The following Mobile Access methods do not support IPv6:
Clientless VPN - a web-based method that enables remote users to access web applications and services using a web browser without installing any software on their devices.
Endpoint Security VPN - a full VPN client that enables remote users to connect securely to the corporate network using IPsec VPN and also provides endpoint security features such as firewall, anti-virus, anti-malware, etc.
Capsule Workspace - a mobile app for iOS and Android devices that enables remote users to access email, calendar, contacts, and corporate applications securely without requiring a VPN connection.

NEW QUESTION: 256
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. cpd
B. cpwd
C. fwd
D. fwm
Answer: D (LEAVE A REPLY)

NEW QUESTION: 257

Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with _____ will not apply.

A. 00000001

B. ffffffff

C. 00000003

D. 00000002

Answer: (SHOW ANSWER)

NEW QUESTION: 258

Is it possible to establish a VPN before the user login to the Endpoint Client?

A. yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_password attribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway

B. no, the user must login first.

C. yes. you had to set neo_always_connected to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_always_connected attribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway

D. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console

Answer: (SHOW ANSWER)

Explanation

You can establish a VPN before the user login to the Endpoint Client by enabling Machine Authentication in the Gateway object of the Smart Console1. Machine Authentication is a feature that allows you to authenticate with a machine certificate and establish a VPN tunnel before the Windows Logon2. This feature provides the following benefits2:

It enhances the security of the VPN connection by verifying the identity of the machine before allowing access to the network.

It simplifies the user experience by eliminating the need to enter credentials twice (once for the VPN and once for the Windows Logon).

It enables seamless connectivity to the network resources and domain services, such as Group Policy, login scripts, and mapped drives. Machine Authentication is supported on Check Point Endpoint Security Client for Windows with E80.71 and higher versions2. It requires a hotfix on top of R77.30 jumbo 286 on the Security Gateway2. To configure Machine Authentication, you need to do the following steps2:

Generate and distribute machine certificates to the Endpoint machines using a trusted Certificate Authority (CA).

Enable Machine Authentication in the Gateway object of the Smart Console and select the CA that issued the machine certificates.

Install policy on the Security Gateway and reboot it.

Enable Machine Authentication in the Endpoint Security Client and select the machine certificate to use.

NEW QUESTION: 259

Which of the following is true regarding the Proxy ARP feature for Manual NAT?

A. The local.arp file must always be configured
B. Automatic proxy ARP configuration can be enabled
C. fw ctl proxy should be configured
D. Translate Destination on Client Side should be configured
Answer: (SHOW ANSWER)
Explanation
The verified answer is B. Automatic proxy ARP configuration can be enabled.
Proxy ARP is a feature that allows a gateway to respond to ARP requests on behalf of another IP address that is not on the same network segment. Proxy ARP is required for manual NAT rules when the NATed IP addresses are not routed to the gateway1.
By default, proxy ARP for manual NAT rules has to be configured manually by editing the local.arp file or using the CLISH commands on the gateway2. However, since R80.10, there is an option to enable automatic proxy ARP configuration for manual NAT rules by modifying the files $CPDIR/tmp/.CPprofile.sh and $CPDIR/tmp/.CPprofile.csh on the gateway3.
fw ctl proxy is a command that displays the proxy ARP table on the gateway, but it does not configure proxy ARP4.
Translate Destination on Client Side is a NAT option that determines whether the destination IP address is translated before or after the routing decision. It does not affect proxy ARP.
References:
Configuring Proxy ARP for Manual NAT - Check Point Software1
R80.10: Automatic Proxy ARP with Manual NAT rules - checkpoint<dot>engineer2 Automatic creation of Proxy ARP for Manual NAT rules on Security Gateway R80.103 fw ctl proxy - Check Point Software NAT Properties - Check Point Software

NEW QUESTION: 260
You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?
A. cpconfig; reboot required
B. cpconfig; reboot not required
C. edit fwaffinity.conf; reboot required
D. edit fwaffinity.conf; reboot not required
Answer: A (LEAVE A REPLY)

NEW QUESTION: 261
To find records in the logs that shows log records from the Application & URL Filtering Software Blade where traffic was dropped, what would be the query syntax?
A. blada: application control AND action:drop
B. blade;"application control AND action:drop
C. (blade: application control AND action;drop)
D. blade."application control AND action;drop
Answer: (SHOW ANSWER)

NEW QUESTION: 262

Which of these statements describes the Check Point ThreatCloud?
A. A worldwide collaborative security network
B. Prevents or controls access to web sites based on category
C. Blocks or limits usage of web applications
D. Prevents Cloud vulnerability exploits
Answer: A (LEAVE A REPLY)

NEW QUESTION: 263
What is required for a site-to-site VPN tunnel that does not use certificates?
A. Unique Passwords
B. RSA Token
C. SecureID
D. Pre-Shared Secret
Answer: D (LEAVE A REPLY)

NEW QUESTION: 264
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:
A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment
Answer: (SHOW ANSWER)
Explanation
For packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are dropped with logs and without sending a negative acknowledgment. Firewall Kernel Inspection is the process of applying security policies and rules to network traffic by the Firewall kernel module. If a packet does not match any rule or matches a rule with an action of Drop or Reject, the packet is dropped by the Firewall kernel module. The difference between Drop and Reject is that Drop silently discards the packet without informing the sender, while Reject discards the packet and sends a negative acknowledgment (such as an ICMP message) to the sender. However, both Drop and Reject actions generate logs that record the details of the dropped packets, such as source, destination, protocol, port, rule number, etc. The other options are either incorrect or describe different scenarios.

NEW QUESTION: 265
What is the port used for SmartConsole to connect to the Security Management Server?
A. CPMI port 18191/TCP
B. CPM port/TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 266
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.
A. Inspect/Bypass
B. Inspect/Prevent
C. Prevent/Bypass
D. Detect/Bypass
Answer: (SHOW ANSWER)
Explanation
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines an Inspect or Bypass action for the file types. The Inspect action means that the file will be sent to the Threat Emulation engine for analysis, and the Bypass action means that the file will not be sent and will be allowed or blocked based on other Threat Prevention blades1. The other options are not valid actions for file types in Threat Prevention profiles. References: Check Point R81 Threat Prevention Administration Guide

NEW QUESTION: 267
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?
A. cphaconf set int fwha_vmac_global_param_enabled 1
B. cphaprob set int fwha_vmac_global_param_enabled 1
C. clusterXL set int fwha_vmac_global_param_enabled 1
D. fw ctl set int fwha_vmac_global_param_enabled 1
Answer: D (LEAVE A REPLY)
Explanation
To enable VMAC mode on a cluster member, you need to set the value of the global kernel parameter fwha_vmac_global_param_enabled to 1. This can be done on-the-fly using the command fw ctl set int fwha_vmac_global_param_enabled 1 on all cluster members. This command does not require a reboot or a policy installation. VMAC mode allows the cluster to use a virtual MAC address for its virtual IP addresses, which reduces the number of gratuitous ARP packets sent upon failover and avoids ARP cache issues on some routers and switches. References: How to enable ClusterXL Virtual MAC (VMAC) mode

NEW QUESTION: 268
What is the purpose of the CPCA process?
A. Generating and modifying certificates.
B. Sending and receiving logs.
C. Monitoring the status of processes.
D. Communication between GUI clients and the SmartCenter server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 269
What information is NOT collected from a Security Gateway in a Cpinfo?
A. System message logs

B. Configuration and database files

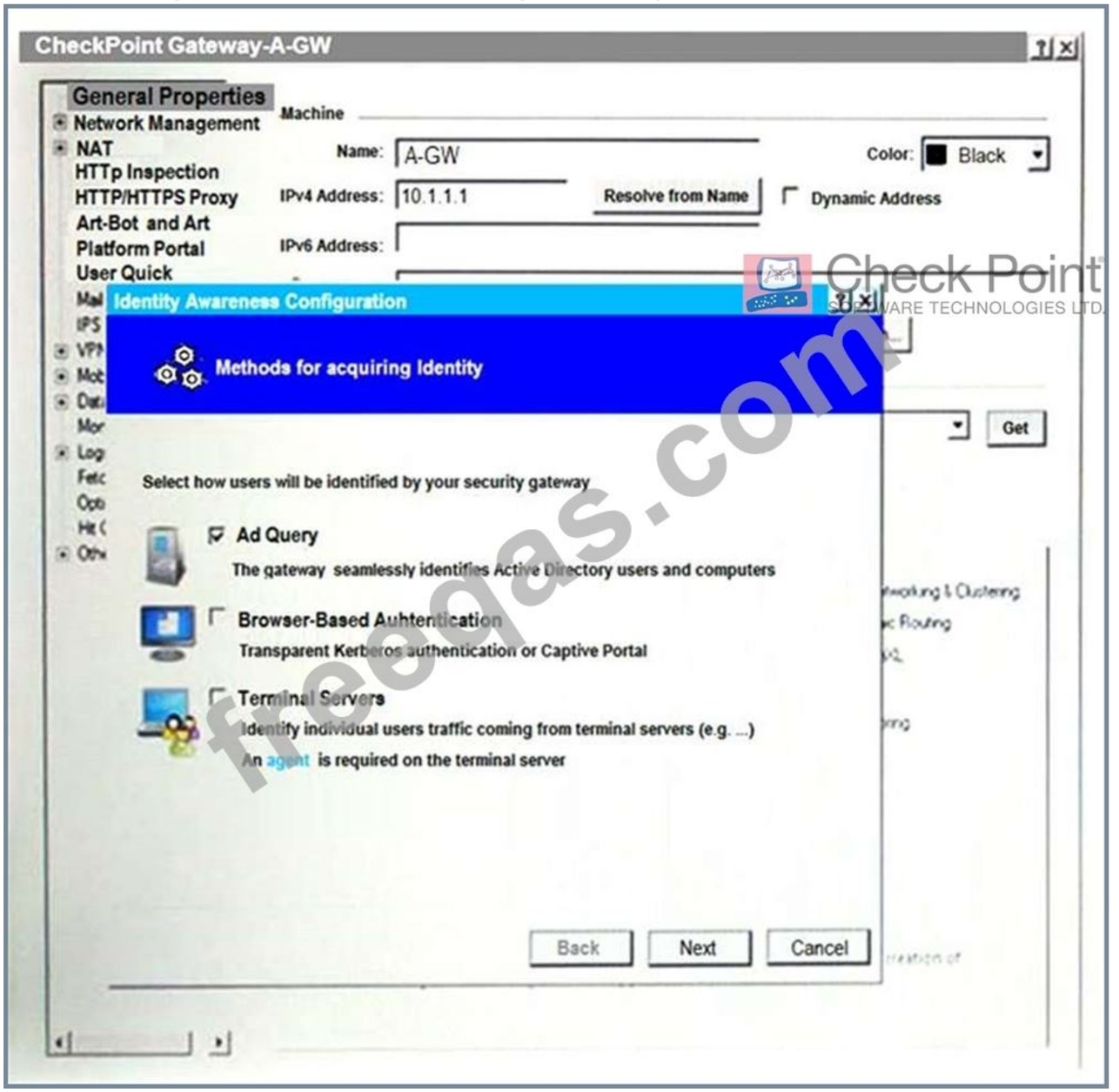
C. OS and network statistics

D. Firewall logs

Answer: D (LEAVE A REPLY)

NEW QUESTION: 270

On the following picture an administrator configures Identity Awareness:



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

A. Obligatory usage of Captive Portal.

B. Kerberos SSO which will be working for Active Directory integration

C. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

D. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 271
To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?
A. 5 Network; Host; Objects; Services; API
B. 3 Incoming; Outgoing; Network
C. 2 Internal; External
D. 4 Incoming; Outgoing; Internal; Other
Answer: D (LEAVE A REPLY)

NEW QUESTION: 272
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?
A. Slow Path
B. Fast Path
C. Medium Path
D. Accelerated Path
Answer: D (LEAVE A REPLY)
Explanation
The traffic is handled by the Accelerated Path. According to the R81.x Security Gateway Architecture (Logical Packet Flow)1, the Accelerated Path is the fastest path for processing packets, as it bypasses most of the inspection and uses SecureXL to accelerate the traffic. The Accelerated Path is used for connections that are established, compliant with the security policy, and do not require any content inspection or NAT1.
The Application Control blade inspects the traffic based on the application identity, which is determined by the Application Control Software Blade in the Medium Path1. However, once the application identity is established, the connection can be offloaded to SecureXL and handled by the Accelerated Path2. This way, the Application Control blade can improve performance and reduce CPU consumption2.
The other paths are not used for this traffic because:

The Slow Path is used for packets that are not compliant with the security policy, require stateful inspection or NAT, or are not supported by SecureXL1. This path involves the most inspection and processing, and is therefore the slowest3.
The Fast Path is used for packets that are trusted and do not require any inspection or NAT. This path bypasses both SecureXL and the Firewall kernel, and uses a kernel module called simfast to forward the packets directly to the network interface driver4. This path is not enabled by default, and requires manual configuration of rules to define which traffic can use it4.
The Medium Path is used for packets that require content inspection, such as IPS, Anti-Virus, Anti-Bot, URL Filtering, or Application Control1. This path uses SecureXL to accelerate some parts of the inspection, but still involves some processing by the Firewall kernel3. This path is only used for the first few packets of a connection until the application identity is established, and then the connection can be offloaded to the Accelerated Path2.
References: : Control SecureXL / CoreXL Paths - Check Point CheckMates : What is CoreXL & SecureXL - jermsmit.com : R81.x Security Gateway Architecture (Logical Packet Flow) : SecureXL and Application Control Layer - Check Point CheckMates

NEW QUESTION: 273
Which one of the following is NOT a configurable Compliance Regulation?
A. GLBA
B. CJIS
C. SOCI
D. NCIPA
Answer: C (LEAVE A REPLY)
Explanation
The Check Point Compliance Blade is a security management tool that monitors the compliance status of the Security Gateways and Security Management Servers with various regulatory standards1. The Compliance Blade supports the following regulatory standards2:
GLBA: The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of
1999, is a US federal law that requires financial institutions to protect the privacy and security of their customers' personal information.
CJIS: The Criminal Justice Information Services Division, also known as CJIS, is a division of the US Federal Bureau of Investigation that provides criminal justice information services to law enforcement, national security, and intelligence agencies. CJIS has a set of security policies and requirements that govern the access, use, and protection of the CJIS data.
NCIPA: The National Counterintelligence and Security Center Insider Threat Program Maturity Framework, also known as NCIPA, is a US government framework that provides guidance and best practices for establishing and enhancing insider threat programs within federal agencies. NCIPA defines five levels of maturity for insider threat programs, from initial to optimized.
SOCI: This is not a valid option for a configurable Compliance Regulation. There is no such regulatory standard with this acronym. However, there is a similar acronym, SOC 2, which stands for Service Organization Control 2, which is a set of standards and criteria for auditing the security, availability, processing integrity, confidentiality, and privacy of service providers that store, process, or transmit customer data3.

Therefore, the correct answer is C, as SOCI is not a configurable Compliance Regulation.
References: 1: ATRG: Compliance Blade (R80.10 and higher) - Check Point Software 3 2: Check Point R81 - Check Point Software 1 3: SOC 2 Compliance Checklist: What You Need to Know - Varonis

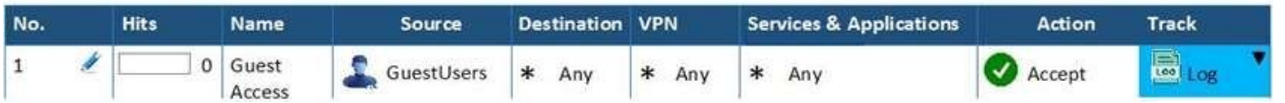
NEW QUESTION: 274
What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?
A. test_connectivity_ad -d <domain>
B. test_ldap_connectivity -d <domain>
C. test_ad_connectivity -d <domain>
D. ad_connectivity_test -d <domain>
Answer: (SHOW ANSWER)
Explanation
The CLI utility that runs connectivity tests from a Security Gateway to an AD domain controller is test_ad_connectivity -d <domain>. This command tests the connectivity between the gateway and the domain controller using LDAP, Kerberos, and WMI protocols. It also verifies the identity awareness configuration and shows the relevant logs3. The other options are not valid commands for testing AD connectivity. References: 3: Check Point Software, Getting Started, Testing Active Directory Connectivity.

NEW QUESTION: 275
With SecureXL enabled, accelerated packets will pass through the following:
A. Network Interface Card, OSI Network Layer, and the Acceleration Device
B. Network Interface Card, Check Point Firewall Kernal, and the Acceleration Device
C. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
D. Network Interface Card and the Acceleration Device
Answer: D (LEAVE A REPLY)

NEW QUESTION: 276
In Threat Prevention, you can create new or clone profiles but you CANNOT change the out-of-the-box profiles of:
A. Basic, Optimized, Strict
B. Basic, Optimized, Severe
C. General, Escalation, Severe
D. General, purposed, Strict
Answer: (SHOW ANSWER)
Explanation
Threat Prevention has three out-of-the-box profiles: Basic, Optimized, and Strict. These profiles define the default actions for different threat prevention blades, such as Anti-Virus, Anti-Bot, IPS, etc. You cannot change the settings of these profiles, but you can clone them and create new profiles with customized settings.
References: Training & Certification | Check Point Software, CCSE section

NEW QUESTION: 277

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?



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

NEW QUESTION: 278
Why is a Central License the preferred and recommended method of licensing?
A. Central Licensing actually not supported with Gaia.
B. Central Licensing is the only option when deploying Gala.
C. 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.
D. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?
A. cphaprob set int fwha_vmac_global_param_enabled 1
B. clusterXL set int fwha_vmac_global_param_enabled 1
C. fw ctl set int fwha_vmac_global_param_enabled 1
D. cphaconf set int fwha_vmac_global_param_enabled 1
Answer: C (LEAVE A REPLY)
Explanation
To enable VMAC mode on a cluster member, you need to set the value of the global kernel parameter fwha_vmac_global_param_enabled to 1. This can be done on-the-fly using the command fw ctl set int fwha_vmac_global_param_enabled 1 on all cluster members. This command does not require a reboot or a policy installation. VMAC mode allows the cluster to use a virtual MAC address for its virtual IP addresses, which reduces the number of gratuitous ARP packets sent upon failover and avoids ARP cache issues on some routers and switches. References: How to enable ClusterXL Virtual MAC (VMAC) mode

NEW QUESTION: 280
If SecureXL is disabled which path is used to process traffic?
A. Passive path
B. Medium path
C. Firewall path

D. Accelerated path
Answer: C (LEAVE A REPLY)
Explanation
If SecureXL is disabled, which means that packet acceleration is not available, the traffic is processed by the Firewall path. The Firewall path is the slowest path in the Check Point architecture, as it involves a full inspection of each packet by the Firewall kernel and all the enabled Software Blades. The Firewall path is also known as the F2F (Firewall to Firewall) path or the INSPECT path. References: Check Point Architecture

NEW QUESTION: 281
What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?
A. 4 Interfaces - an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
B. 3 Interfaces - an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
C. 1 Interface - an interface leading to the organization and the Internet, and configure for synchronization.
D. 2 Interfaces - a data interface leading to the organization and the Internet, a second interface for synchronization.
Answer: (SHOW ANSWER)
Explanation
According to the Check Point R81 Mobile Access Administration Guide, the recommended number of physical network interfaces in a Mobile Access cluster deployment is . One interface should be connected to the organization network, one interface should be connected to the Internet, and one interface should be used for synchronization between cluster members. This configuration provides optimal performance and security for Mobile Access traffic.

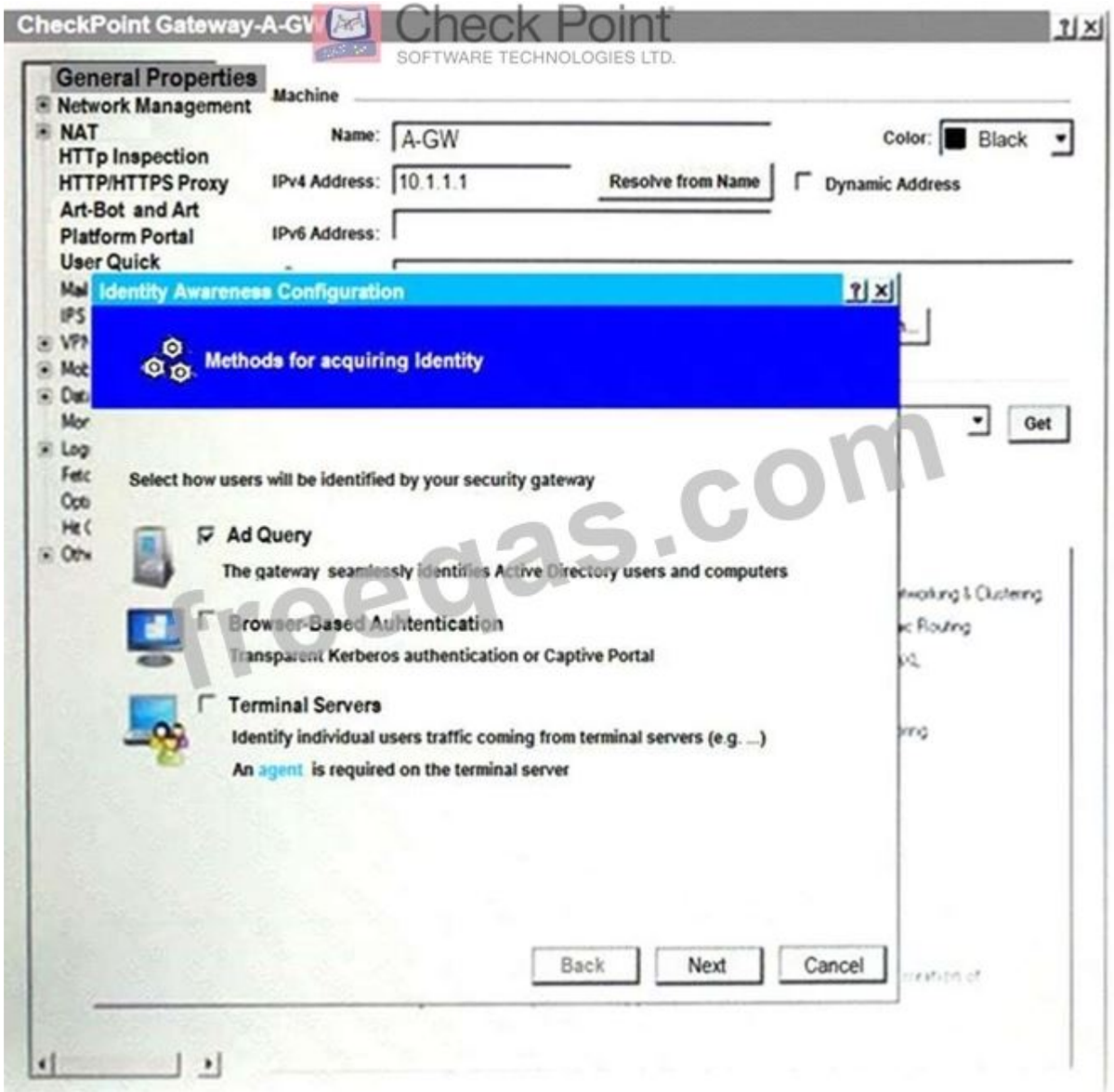
NEW QUESTION: 282
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every
A. 30 sec
B. 60 sec
C. 5 sec
D. 15 sec
Answer: B (LEAVE A REPLY)

NEW QUESTION: 283
Which GUI client is supported in R81?
A. SmartLog
B. SmartView Monitor
C. SmartProvisioning
D. SmartView Tracker
Answer: (SHOW ANSWER)

NEW QUESTION: 284
What are the two ClusterXL Deployment options?

A. Distributed and Full High Availability
B. Broadcast and Multicast Mode
C. Distributed and Standalone
D. Unicast and Multicast Mode
Answer: A (LEAVE A REPLY)
Explanation
The two ClusterXL Deployment options are Distributed and Full High Availability. Distributed deployment means that each cluster member has its own Security Management Server and synchronizes with other members. Full High Availability deployment means that one cluster member is active and handles all traffic, while the other members are in standby mode and ready to take over in case of a failure. The other options are not valid ClusterXL Deployment options, but rather ClusterXL Modes or ClusterXL Load Sharing Methods.
References: [Check Point Security Expert R81 ClusterXL Administration Guide], page 6.

NEW QUESTION: 285
On the following picture an administrator configures Identity Awareness:



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

A. Kerberos SSO which will be working for Active Directory integration

B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.

C. Obligatory usage of Captive Portal.

D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: B (LEAVE A REPLY)

Explanation

After clicking "Next", the above configuration is supported by Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user. This is a feature of Identity Awareness that allows the Security Gateway to identify users and machines on the network and enforce security policies based on their identity. The administrator can configure Identity Awareness to use various methods for acquiring identity, including Active Directory integration, browser-based authentication, terminal servers, and transparent authentication1.

References: Check Point Resource Library, page 3.

NEW QUESTION: 286
Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?
A. cphaprob stat
B. cphaprob -l list
C. cphaprob all show stat
D. cphaprob -a if
Answer: (SHOW ANSWER)

NEW QUESTION: 287
Which NAT rules are prioritized first?
A. Post-Automatic/Manual NAT rules
B. Manual/Pre-Automatic NAT
C. Automatic Hide NAT
D. Automatic Static NAT
Answer: (SHOW ANSWER)
Explanation
The NAT rules that are prioritized first are . NAT stands for Network Address Translation, and it is a feature that allows Security Gateways to modify the source or destination IP addresses or ports of packets that pass through them. NAT rules are the rules that define how NAT is applied to traffic that matches certain criteria. There are three types of NAT rules: Manual/Pre-Automatic NAT, Automatic NAT, and Manual/Post-Automatic NAT. Manual/Pre-Automatic NAT rules are the rules that are manually created by administrators and placed before the automatic NAT rules in the rulebase. These rules have the highest priority and are processed first by the Security Gateway. Automatic NAT rules are the rules that are automatically generated by the Security Gateway based on the NAT properties of network objects. These rules have the second highest priority and are processed after the manual/pre-automatic NAT rules. Manual/Post-Automatic NAT rules are the rules that are manually created by administrators and placed after the automatic NAT rules in the rulebase. These rules have the lowest priority and are processed last by the Security Gateway.

NEW QUESTION: 288
What SmartEvent component creates events?

A. SmartEvent GUI
B. Correlation Unit
C. Consolidation Policy
D. SmartEvent Policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 289
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?
A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart
Answer: B (LEAVE A REPLY)
Explanation
The cvpnd_restart command is used to restart the daemon after making modifications to the $CVPNDIR/conf/cvpnd.C file. The cvpnd daemon is responsible for managing the communication between the Check Point components and the Content Vectoring Protocol (CVP) server. The CVP server is an external server that provides content inspection and filtering services for Check Point gateways. The $CVPNDIR/conf/cvpnd.C file contains the configuration settings for the cvpnd daemon, such as the CVP server IP address, port number, timeout value, and debug level. References: Check Point Security Expert R81 Course, Content Inspection Using ICAP, cvpnd daemon debug file

NEW QUESTION: 290
Which of the following is NOT a type of Check Point API available in R81.x?
A. Identity Awareness Web Services
B. OPSEC SDK
C. Mobile Access
D. Management
Answer: C (LEAVE A REPLY)
Explanation
Check Point API is a set of web services that enable the usage of functions and commands in a dynamic and automated fashion. Check Point API is available in different types, each serving a different purpose and functionality. According to the Check Point Resource Library1, the following are the types of Check Point API available in R81.x:
Identity Awareness Web Services: This type of API allows external applications to send identity and location information to the Security Gateway, which can then use this information for policy enforcement. Identity Awareness Web Services can be used for scenarios such as guest registration, captive portal, identity agents, etc.
OPSEC SDK: This type of API provides a framework for developing applications that interact with Check Point products using the OPSEC (Open Platform for Security) protocol. OPSEC SDK can be used for scenarios such as log export, event management, anti-virus integration, etc.

Management: This type of API allows external applications to perform management operations on the Check Point Management server using RESTful web services. Management API can be used for scenarios such as policy installation, object creation, configuration backup, etc.
Mobile Access is not a type of Check Point API, but rather a feature that provides secure remote access to corporate resources from various devices. Mobile Access uses SSL VPN technology and supports different authentication methods and access scenarios.
References: What is an API Gateway?, How to use Check Point API with Postman quick guide, Home - Check Point Developers, Introduction to RESTful APIs and JSON format, Checkpoint API tutorial, part 1 - getting started

NEW QUESTION: 291
Which of these statements describes the Check Point ThreatCloud?
A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network
Answer: D (LEAVE A REPLY)
Explanation
The Check Point ThreatCloud is a worldwide collaborative security network that collects and analyzes threat data from millions of sensors, security gateways, and other sources, and delivers real-time threat intelligence and protection to Check Point products.

NEW QUESTION: 292
John is using Management HA.
Which Security Management Server should he use for making changes?
A. connect virtual IP of Smartcenter HA
B. primary Log Server
C. active SmartConsole
D. secondary Smartcenter
Answer: (SHOW ANSWER)

NEW QUESTION: 293
In R81 spoofing is defined as a method of:
A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.
Answer: D (LEAVE A REPLY)
Explanation
IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

References:

NEW QUESTION: 294
How can you switch the active log file?
A. Run fw logswitch on the gateway
B. Run fwm logswitch on the Management Server
C. Run fwm logswitch on the gateway
D. Run fw logswitch on the Management Server
Answer: D (LEAVE A REPLY)
Explanation
You can switch the active log file by running fw logswitch on the Management Server1. This command closes the current log file and creates a new one2. It is useful for archiving or backing up log files, or for creating a new log file for a specific time period2. You can also schedule the log switch to occur automatically at a regular interval, such as daily, weekly, or monthly2. To run this command, you need to access the Management Server in expert mode and run fw logswitch1. You can also use the SmartView Tracker to switch the active log file from the GUI. To do this, go to the Network & Endpoint tab, click on the File menu, and select Switch Active File...3.
References: How to switch the active log file - Check Point Software, fw logswitch - Check Point Software, Troubleshooting Check Point logging issues when Security Management Server / Log Server is not receiving logs from Security Gateway - Check Point Software

NEW QUESTION: 295
What is the default size of NAT table fwx_alloc?
A. 35000
B. 10000
C. 25000
D. 20000
Answer: C (LEAVE A REPLY)

NEW QUESTION: 296
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:
A. Dropped without logs and without sending a negative acknowledgment
B. Dropped with logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped without sending a negative acknowledgment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 297
What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)

A. SmartCenter Server cannot reach this Security Gateway.
B. There is a blade reporting a problem.
C. VPN software blade is reporting a malfunction.
D. Security Gateway's MGNT NIC card is disconnected.
Answer: (SHOW ANSWER)
Explanation
If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem. The red exclamation mark indicates that one or more blades on the gateway have an issue that needs attention. The issue could be related to configuration, license, policy, or other factors. Deyra can hover over the icon to see more details about the problem. References: Training & Certification | Check Point Software, New Courses and Certificates for R81.10 - Check Point CheckMates

NEW QUESTION: 298
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: A (LEAVE A REPLY)
Explanation
The correct steps to configure the HTTPS Inspection Policy in Check Point R81 are as follows1:
Go to Manage&Settings > in SmartDashboard.
Enable HTTPS Inspection and select the
Create a new HTTPS Inspection Layer
Define the rules for inspecting HTTPS traffic based on the source, destination, service, and action.
Install the policy on the relevant gateways.
The other options are incorrect because they either use wrong blade names, wrong menu options, or wrong configuration steps. References: 1: LAB:25 How to Configure HTTPS Inspection in Check Point Firewall R81(https://www.youtube.com/watch?v=NCvV7-R9ZgU)

NEW QUESTION: 299
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: (SHOW ANSWER)
Explanation
Proxy ARP is a technique that allows a device to respond to ARP requests on behalf of another IP address.
Proxy ARP is required for Manual Static NAT when the translated IP address does not belong to one of the firewall's interfaces. This is because the firewall needs to intercept the packets destined to the translated IP address and forward them to the original IP address after applying the NAT rule. Without Proxy ARP, the packets would not reach the firewall and the NAT would not work. Proxy ARP is not required for Automatic Static NAT or Automatic Hide NAT, because these types of NAT use IP addresses that belong to the firewall's interfaces. Proxy ARP is also not required for Manual Hide NAT, because this type of NAT does not change the destination IP address of the packets, only the source IP address. References: Check Point R81 Security Management Administration Guide, page 115

NEW QUESTION: 300
What is considered Hybrid Emulation Mode?
A. High availability between the local SandBlast appliance and the cloud.
B. Manual configuration of file types on emulation location.
C. Load sharing of emulation between an on premise appliance and the cloud.
D. Load sharing between OS behavior and CPU Level emulation.
Answer: (SHOW ANSWER)

NEW QUESTION: 301
What is the minimum amount of RAM needed for a Threat Prevention Appliance?
A. 4 GB
B. 6 GB
C. It depends on the number of software blades enabled
D. 8GB with Gaia in 64-bit mode
Answer: A (LEAVE A REPLY)

NEW QUESTION: 302
Which of the following is NOT an attribute of packet acceleration?
A. Destination port
B. Protocol
C. VLAN Tag
D. Source address
Answer: C (LEAVE A REPLY)

NEW QUESTION: 303
Bob is asked by Alice to disable the SecureXL mechanism temporary tor further diagnostic by their Check Point partner. Which of the following Check Point Command is true:
A. fwaccel suspend
B. fwaccel standby
C. fwaccel off
D. fwaccel templates
Answer: C (LEAVE A REPLY)
Explanation
You can disable the SecureXL mechanism temporarily for further diagnostic by running fwaccel off on the Security Gateway1. This command disables SecureXL, which is an acceleration solution that maximizes the performance of the Firewall by offloading CPU-intensive operations to the SecureXL device2. Disabling SecureXL can help you troubleshoot connectivity or policy issues, as it forces all traffic to go through the Firewall kernel and bypass the SecureXL device1. To run this command, you need to access the Security Gateway in expert mode and run fwaccel off1. To enable SecureXL again, you can run fwaccel on1. Note that disabling SecureXL may affect the performance of the Security Gateway, so use it with caution and only when necessary1.
References: How to enable/disable Check Point SecureXL via CLI - Check Point Software, SecureXL - Check Point Software

NEW QUESTION: 304
Automation and Orchestration differ in that:
A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
B. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.
C. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
D. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305

Which view is NOT a valid CPVIEW view?

A. IDA

B. PDP

C. RAD

D. VPN

Answer: B (LEAVE A REPLY)

NEW QUESTION: 306

The fwd process on the Security Gateway sends logs to the fwd process on the Management Server, where it is forwarded to_____via_____

A. cpd, fwm

B. cpm, cpd

C. fwm, cpd

D. cpwd, fwssd

Answer: C (LEAVE A REPLY)

Explanation

The fwd process on the Security Gateway sends logs to the fwd process on the Management Server, where it is forwarded to fwm via cpd. The fwm process is responsible for managing the log files and the cpd process is responsible for communication between processes. The other options are incorrect because they involve processes that are not related to logging or communication. References: Check Point Certified Security Expert R81.20 Course Overview, sk163413: Support, Support Requests, Training ... - Check Point Software, Check Point Certified Security Expert R81.20

NEW QUESTION: 307

The Check Point installation history feature in provides the following:

A. View install changes and install specific version

B. Policy Installation Date only

C. Policy Installation Date, view install changes and install specific version

D. View install changes

Answer: C (LEAVE A REPLY)

Explanation

See the revisions that were installed on the Security Gateway and who installed the Policy. See the changes that were installed and who made the changes. Revert to a specific version, and install the last "good" Policy. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION: 308

CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

A. MySQL

B. Postgres SQL

C. MarisDB

D. SOLR
Answer: (SHOW ANSWER)
Explanation
CPM process stores objects, policies, users, administrators, licenses and management data in a Postgres SQL database. This database is located in $FWDIR/conf and can be accessed using the pg_client command2. The other options are not the correct database type for CPM. References: Check Point R81 Security Management Administration Guide

NEW QUESTION: 309
Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?
A. fwm
B. fwd
C. cpd
D. logd
Answer: B (LEAVE A REPLY)

NEW QUESTION: 310
Which two Identity Awareness daemons are used to support identity sharing?
A. Policy Activation Point (PAP) and Policy Decision Point (PDP)
B. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
C. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
D. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
Answer: D (LEAVE A REPLY)
Source:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/Topics-IDAG/Identity-Awareness-Config-Identity-Sharing.htm

NEW QUESTION: 311
You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.
What must you do to get SIC to work?
A. Create a rule at the top in your Check Point firewall to bypass the Geo-Protection
B. Nothing - Check Point control connections function regardless of Geo-Protection policy
C. Create a rule at the top in the Sydney firewall to allow control traffic from your network
D. Remove Geo-Protection, as the IP-to-country database is updated externally, and you have no control of this.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 312

Bob has finished io setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?
A. cpprod_util MgmtIsPrimary
B. cpprod_util FwIsSecondary
C. cpprod_util MgmtIsSecondary
D. cpprod_util FwIsPrimary
Answer: A (LEAVE A REPLY)
Explanation
The cpprod_util command is a utility that provides information about the installed Check Point products and their versions. The cpprod_util MgmtIsPrimary option checks if the Security Management Server is installed as a primary or a secondary server in a High Availability cluster2. If the server is primary, the command returns "yes". If the server is secondary, the command returns "no". Therefore, Bob can use this command to verify the provisioning of the secondary Security Management Server.
References: 2: cpprod_util

NEW QUESTION: 313
What must you do first if "fwm sic_reset" could not be completed?
A. Reset SIC from Smart Dashboard
B. Cpstop then find keyword "certificate" in objects_5_0.C and delete the section
C. Change internal CA via cpconfig
D. Reinitialize SIC on the security gateway then run "fw unloadlocal"
Answer: C (LEAVE A REPLY)

NEW QUESTION: 314
What is the name of the secure application for Mail/Calendar for mobile devices?
A. Capsule VPN
B. Capsule Mail
C. Capsule Workspace
D. Secure Workspace
Answer: (SHOW ANSWER)

NEW QUESTION: 315
You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?
A. Check Point Capsule Cloud
B. Sandblast Mobile Protect
C. SecuRemote
D. SmartEvent Client Info
Answer: (SHOW ANSWER)
Explanation

SandBlast Mobile Protect is a lightweight app for iOS and Android that gathers data and helps analyze threats to devices in your environment.
https://www.checkpoint.com/downloads/products/how-sandblast-mobile-works-solution-brief.pdf

NEW QUESTION: 316
Which feature is NOT provided by all Check Point Mobile Access solutions?
A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity
Answer: A (LEAVE A REPLY)
Explanation
Types of Solutions
All of Check Point's Remote Access solutions provide:

NEW QUESTION: 317
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?
A. Destination Address
B. Source Address
C. Source Port
D. TCP Acknowledgment Number
Answer: D (LEAVE A REPLY)

NEW QUESTION: 318
When using CPSTAT, what is the default port used by the AMON server?
A. 18191
B. 18192
C. 18194
D. 18190
Answer: (SHOW ANSWER)
Explanation

The default port used by the AMON server when using CPSTAT is 18192. CPSTAT is a command-line tool that allows administrators to monitor various statistics and status information about Check Point products and components, such as CPU usage, memory usage, policy installation, cluster state, etc. CPSTAT uses AMON (Advanced Monitoring) protocol to communicate with AMON server, which is a daemon that runs on Security Gateways or Management Servers and collects and provides AMON data. By default, AMON server listens on TCP port 18192 for incoming CPSTAT requests.

NEW QUESTION: 319
What cloud-based SandBlast Mobile application is used to register new devices and users?
A. Management Dashboard
B. Behavior Risk Engine
C. Check Point Protect Application
D. Check Point Gateway
Answer: D (LEAVE A REPLY)

NEW QUESTION: 320
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. The traffic is originating from the gateway itself.
B. Acceleration is not enabled.
C. There is a virus found. Traffic is still allowed but not accelerated.
D. The connection required a Security server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 321
Customer's R81 management server needs to be upgraded to R81.20. What is the best upgrade method when the management server is not connected to the Internet?
A. Export R81 configuration, clean install R81.20 and import the configuration
B. CPUSE offline upgrade
C. CPUSE online upgrade
D. SmartUpdate upgrade
Answer: (SHOW ANSWER)
Explanation
CPUSE offline upgrade is the best upgrade method when the management server is not connected to the Internet.
CPUSE (Check Point Upgrade Service Engine) is a tool that automates the process of upgrading and installing software packages on Check Point devices. CPUSE can work in online mode or offline mode.
Online mode requires an Internet connection to download the packages from Check Point servers. Offline mode allows you to download the packages manually from another device and transfer them to the management server using a USB drive or SCP. References: Check Point Security Expert R81 Course, CPUSE Administration Guide

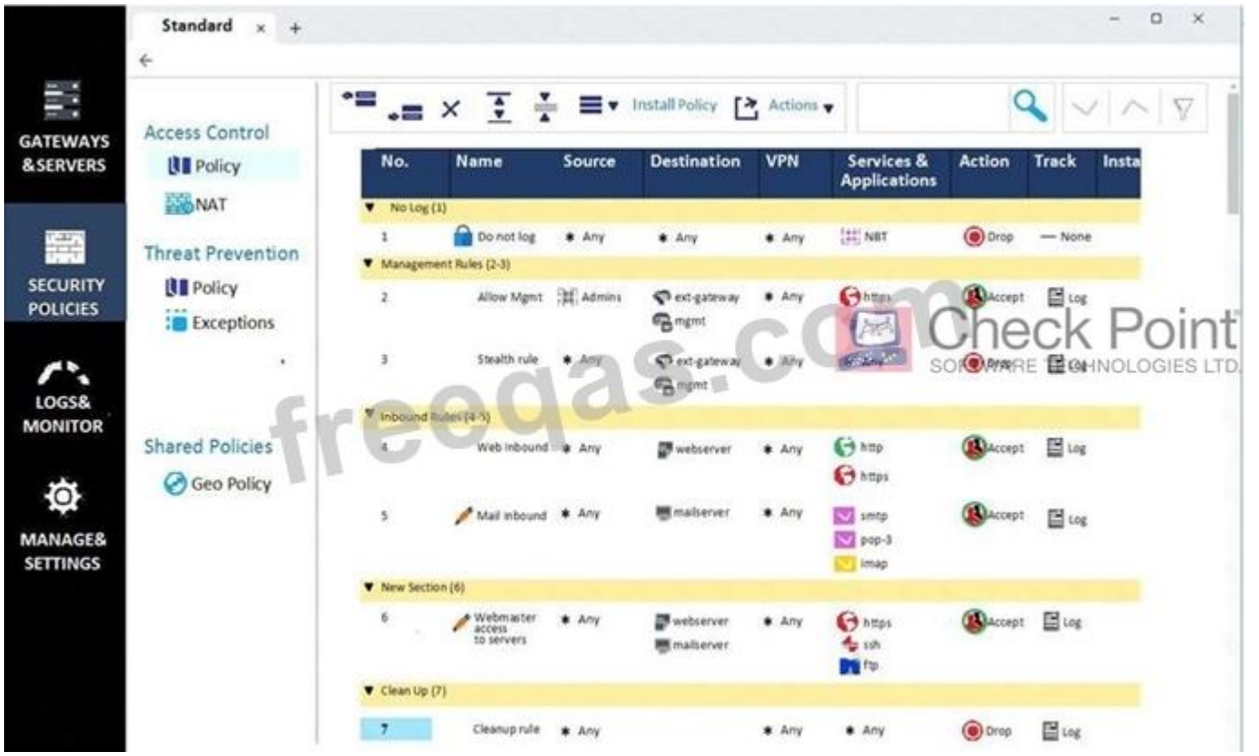
NEW QUESTION: 322
From SecureXL perspective, what are the three paths of traffic flow:
A. Initial Path; Medium Path; Accelerated Path
B. Layer Path; Blade Path; Rule Path
C. Firewall Path; Accelerated Path; Medium Path
D. Firewall Path; Accept Path; Drop Path
Answer: (SHOW ANSWER)
Explanation
From SecureXL perspective, the three paths of traffic flow are Firewall Path, Accelerated Path, and Medium Path. Firewall Path is the path that handles packets that are not processed by SecureXL and are sent to the Firewall kernel for inspection. Accelerated Path is the path that handles packets that are processed by SecureXL and bypass the Firewall kernel. Medium Path is the path that handles packets that are partially processed by SecureXL and partially by the Firewall kernel1. References: Check Point R81 Performance Tuning Administration Guide

NEW QUESTION: 323
By default, how often does Threat Emulation update the engine on the Security Gateway?
A. Once per day
B. Once an hour
C. Once a week
D. Twice per day
Answer: (SHOW ANSWER)
Explanation
By default, Threat Emulation updates the engine on the Security Gateway once per day. This is the recommended frequency for optimal performance and security. However, the admin can change the update frequency to a different value, such as once an hour, once a week, or twice per day, depending on the network needs and resources. The admin can also manually update the engine at any time using the SmartConsole or the command line interface. References: Threat Emulation Engine Release Updates - Check Point Software, Check Point R81.20 Gaia Fresh Install and upgrade

NEW QUESTION: 324
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?
A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode
Answer: C (LEAVE A REPLY)
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that

do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

NEW QUESTION: 325



What can we infer about the recent changes made to the Rule Base?

A. Rule 7 was created by the 'admin' administrator in the current session

B. 8 changes have been made by administrators since the last policy installation

C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator

D. Rule 1 and object webserver are locked by another administrator

Answer: D (LEAVE A REPLY)

Explanation

Based on the image provided by the user, we can infer that rule 1 and object webserver are locked by another administrator. This is because they have red lock icons next to them, which indicate that they are being edited by another administrator in another session. The lock icons prevent other administrators from modifying these objects until the changes are published or discarded by the original administrator. The lock icons also show the name of the administrator who locked the objects when hovered over with the mouse cursor.

The other options are incorrect because:

Rule 7 was not created by the 'admin' administrator in the current session, but by another administrator in another session. This is because it has a blue lock icon next to it, which indicates that it was added by another administrator in another session. The blue lock icon prevents other administrators from deleting this rule until the changes are published or discarded by the original administrator.

8 changes have not been made by administrators since the last policy installation, but in the current session by the 'admin' administrator. This is because there is a yellow number 8 next to the Install Policy button, which indicates that

there are 8 unpublished changes in the current session by the 'admin' administrator. These changes will be published or discarded when the 'admin' administrator clicks on Publish or Discard buttons.
The rules 1, 5 and 6 can be edited by the 'admin' administrator, but only after unlocking them from another administrator who locked them in another session. This is because they have red lock icons next to them, which indicate that they are being edited by another administrator in another session. The
'admin' administrator can unlock these rules by right-clicking on them and selecting Unlock from the menu. However, this will discard the changes made by the original administrator who locked them.

NEW QUESTION: 326
Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?
A. $FWDIR/conf/fwauthd.conf
B. $FWDIR/conf/fwauth.conf
C. $FWDIR/database/fwauthd.conf
D. $FWDIR/state/fwauthd.conf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 327
Which command is used to display status information for various components?
A. sysmess all
B. show system messages
C. show all systems
D. show sysenv all
Answer: (SHOW ANSWER)

NEW QUESTION: 328
Using Web Services to access the API, which Header Name-Value had to be in the HTTP Post request after the login?
A. X-chkp-sid Session Unique Identifier
B. API-Key
C. user-uid
D. uuid Universally Unique Identifier
Answer: A (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/latest/APIs/?#web/introduction~v1.9%20 HTTP Headers content-Type: application/json x-chkp-sid: <session ID token as returned by the login command> The x-chkp-sid header is mandatory in all API calls except the login API.

NEW QUESTION: 329
How is communication between different Check Point components secured in R81? As with all questions, select the BEST answer.

A. By using IPSEC
B. By using SIC
C. By using ICA
D. By using 3DES
Answer: B (LEAVE A REPLY)
Explanation
Communication between different Check Point components is secured by using SIC, which stands for secure internal communication. SIC is a certificate-based channel that uses standards-based TLS 1.2 for creating secure connections and AES128 for encryption. SIC ensures that only authorized components can communicate with each other and that the communication is protected from eavesdropping and tampering. SIC is established by using a one-time password (OTP) that is generated when a Check Point component is created or installed. The OTP is used to initialize the trust relationship between the component and the Security Management Server, which acts as an internal certificate authority (ICA) that issues and revokes certificates for the components.

NEW QUESTION: 330
What does Backward Compatibility mean upgrading the Management Server and how can you check it?
A. The Management Server is able to manage older Gateways. The lowest supported version is documented in the Installation and Upgrade Guide
B. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes
C. You will be able to connect to older Management Server with the SmartConsole. The lowest supported version is documented in the Installation and Upgrade Guide
D. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes
Answer: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RN/Topics-RN/Backward-Co

NEW QUESTION: 331
Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?
A. Severity
B. Policy
C. Automatic reactions
D. Threshold
Answer: B (LEAVE A REPLY)

NEW QUESTION: 332
When performing a minimal effort upgrade, what will happen to the network traffic?
A. All connections that were initiated before the upgrade will be dropped, causing network downtime
B. All connections that were initiated before the upgrade will be handled normally
C. All connections that were initiated before the upgrade will be handled by the active gateway
D. All connections that were initiated before the upgrade will be handled by the standby gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 333
There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?
A. Using Web Services
B. Using Mgmt_cli tool
C. Using SmartConsole GUI console
D. Using CLISH
E. Events are collected with SmartWorkflow from Trouble Ticket systems
Answer: E (LEAVE A REPLY)

NEW QUESTION: 334
What component of R81 Management is used for indexing?
A. DBSync
B. API Server
C. fwm
D. SOLR
Answer: (SHOW ANSWER)
Explanation
The component of R81 Management that is used for indexing is SOLR. SOLR is an open-source enterprise search platform that provides fast and scalable indexing and searching capabilities. SOLR is used by SmartConsole to index the objects and rules in the security policy, as well as the logs and events in SmartLog and SmartEvent. SOLR enables quick and easy access to the relevant information in the management database.
References: Check Point Security Expert R81 Course, SOLR Troubleshooting

NEW QUESTION: 335
What does Backward Compatibility mean upgrading the Management Server and how can you check it?
A. The Management Server is able to manage older Gateways. The lowest supported version is documented in the Installation and Upgrade Guide

B. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes
C. You will be able to connect to older Management Server with the SmartConsole. The lowest supported version is documented in the Installation and Upgrade Guide
D. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes
Answer: (SHOW ANSWER)
Explanation
Backward Compatibility means that the Management Server is able to manage older Gateways. The lowest supported version is documented in the Release Notes of each version. The Installation and Upgrade Guide only provides information about how to install or upgrade the Management Server and the Gateways, not about the compatibility between them. References: Check Point R81 Release Notes, page 6.

NEW QUESTION: 336
If SecureXL is disabled which path is used to process traffic?
A. Medium path
B. Accelerated path
C. Firewall path
D. Passive path
Answer: (SHOW ANSWER)

NEW QUESTION: 337
What is the port used for SmartConsole to connect to the Security Management Server?
A. CPMI port 18191/TCP
B. CPM port/TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP
Answer: A (LEAVE A REPLY)
Explanation
The port used for SmartConsole to connect to the Security Management Server is CPMI port 18191/TCP.
CPMI stands for Check Point Management Interface, which is a proprietary protocol that enables secure communication between the SmartConsole and the Security Management Server. CPMI uses SSL encryption and authentication to protect the data exchange. References: Check Point Security Expert R81 Course, SK52421 - Ports used by Check Point software

NEW QUESTION: 338
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. The option that can be added to each Log, Detailed Log and Extended Log is Accounting/Suppression.
Accounting/Suppression is a feature that allows administrators to control how often logs are generated for certain rules or connections. Accounting means that logs are generated periodically based on a specified interval or volume. Suppression means that logs are generated only for the first and last packet of a connection or session. Accounting/Suppression can be added to any tracking option to reduce the number of logs and save disk space.

NEW QUESTION: 339
Alice wants to upgrade the current security management machine from R80.40 to R81.20 and she wants to check the Deployment Agent status over the GAIA CLISH. Which of the following GAIACLISH command is true?
A. show agent status
B. show uninstaller status
C. show installer packages
D. show installer status
Answer: (SHOW ANSWER)
Explanation
The correct command for checking the Deployment Agent status over the GAIA CLISH is "show installer status". This command displays information about the Deployment Agent such as its version, status, last update time, and last operation result. The other commands are either invalid or irrelevant for this purpose.
References: [Check Point Security Expert R81 Installation and Upgrade Guide], page 23.

NEW QUESTION: 340
You can access the ThreatCloud Repository from:
A. R81.10 SmartConsole and Threat Prevention
B. Threat Wiki and Check Point Website
C. Threat Prevention and Threat Tools
D. R81.10 SmartConsole and Application Wiki
Answer: A (LEAVE A REPLY)

NEW QUESTION: 341
Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?
A. enable DLP and select.exe and .bat file type
B. enable .exe & .bat protection in IPS Policy
C. create FW rule for particular protocol
D. tecli advanced attributes set prohibited_file_types exe.bat
Answer: A (LEAVE A REPLY)

NEW QUESTION: 342

You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?
A. UDP port 8116
B. TCP port 257
C. TCP port 443
D. TCP port 256
Answer: (SHOW ANSWER)

NEW QUESTION: 343
You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.
What is the first step to run management API commands on GAIA's shell?
A. mgmt_admin@teabag > id.txt
B. mgmt_login
C. login user admin password teabag
D. mgmt_cli login user "admin" password "teabag" > id.txt
Answer: B (LEAVE A REPLY)
Explanation
You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.
The first step to run management API commands on GAIA's shell is mgmt_login. This command allows you to login to the management server and obtain a session ID, which is required for running other management API commands. You can also specify the user name and password as parameters, or enter them interactively.
The session ID is stored in the file $CPDIR/tmp/.api_session by default, unless you specify a different file name.
References: R81 Management API Reference Guide, page 15.

NEW QUESTION: 344
In R81 spoofing is defined as a method of:
A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.
Answer: (SHOW ANSWER)
IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION: 345
Which command gives us a perspective of the number of kernel tables?
A. fw tab -t
B. fw tab -s

C. fw tab -n
D. fw tab -k
Answer: B (LEAVE A REPLY)
Explanation
The command "fw tab -s" is used to display information about the state of various kernel tables in a Check Point firewall. It provides a perspective on the number and status of these tables, which can be helpful for troubleshooting and monitoring firewall performance.
Option B correctly identifies the command that gives a perspective of the number of kernel tables, making it the verified answer.
References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

NEW QUESTION: 346
What is the difference between an event and a log?
A. Events are generated at gateway according to Event Policy
B. A log entry becomes an event when it matches any rule defined in Event Policy
C. Events are collected with SmartWorkflow form Trouble Ticket systems
D. Log and Events are synonyms
Answer: (SHOW ANSWER)
Explanation
The difference between an event and a log is that a log entry becomes an event when it matches any rule defined in Event Policy. A log entry is a record of a network activity that is generated by a Security Gateway or a Management Server. An event is a log entry that meets certain criteria and triggers an action or a notification. The other options are either not true or not accurate definitions of events and logs. References:
Check Point R81 Logging and Monitoring Administration Guide

NEW QUESTION: 347
Under which file is the proxy arp configuration stored?
A. $FWDIR/state/proxy_arp.conf on the management server
B. $FWDIR/conf/local.arp on the management server
C. $FWDIR/state/_tmp/proxy.arp on the security gateway
D. $FWDIR/conf/local.arp on the gateway
Answer: D (LEAVE A REPLY)
Explanation

The proxy ARP configuration is stored under the following file:
D: $FWDIR/conf/local.arp on the gateway
This file, local.arp, contains the proxy ARP configuration for the Security Gateway. It is used to configure ARP (Address Resolution Protocol) settings for network communication.
References: Check Point Certified Security Expert R81 Study Guide, Check Point documentation on proxy ARP.

NEW QUESTION: 348
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.
A. True, CLI is the prefer method for Licensing
B. False, Central Licenses are installed via Gaia on Security Gateways
C. False, Central License are handled via Security Management Server
D. True, Central License can be installed with CPLIC command on a Security Gateway
Answer: D (LEAVE A REPLY)

NEW QUESTION: 349
Security Checkup Summary can be easily conducted within:
A. Summary
B. Reports
C. Views
D. Checkups
Answer: C (LEAVE A REPLY)

NEW QUESTION: 350
Which of the following is NOT an option to calculate the traffic direction?
A. Incoming
B. Outgoing
C. Internal
D. External
Answer: (SHOW ANSWER)

NEW QUESTION: 351
What are the correct sleps upgrading a HA cluster (Ml is active. M2 is passive) using Multi-Version Cluster(MVC) Upgrade?
A. 1) Enable the MVC mechanism on both cluster members wcphaprob mvc on
2) Upgrade the passive node M2 to R81.10
3) In SmartConsole. change the version of the cluster object
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.10
6) On each Cluster Member, disable the MVC mechanism
B. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on

2) Upgrade the passive node M2 to R81.10
3) In SmartConsole. change the version of the cluster object
4) Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.10
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy
C. 1) In SmartConsole. change the version of the cluster object
2) Upgrade the passive node M2 to R81.10
3) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 Wcphaconf mvc on
4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails
5) After examine the cluster states upgrade node M1 to R81.10
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsole. change the version of the cluster object
D. 1) Upgrade the passive node M2 to R81.10
2) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 ttcphaconf mvc on
3) In SmartConsole, change the version of the cluster object 4} Install the Access Control Policy
5) After examine the cluster states upgrade node M1 to R81.10
6) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.10
Answer: (SHOW ANSWER)
Explanation
The correct steps for upgrading a HA cluster using MVC are as follows:
Upgrade the passive node M2 to R81.10 using CPUSE or CLI.
Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 using the command cphaconf mvc on.
In SmartConsole, change the version of the cluster object to R81.10.
Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails.
After examining the cluster states, upgrade node M1 to R81.10 using CPUSE or CLI.
On each Cluster Member, disable the MVC mechanism using the command cphaconf mvc off and install the Access Control Policy.
References: : Multi-Version Cluster (MVC) Upgrade

NEW QUESTION: 352
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____.
A. TCP Port 18209
B. TCP Port 18190
C. TCP port 19009
D. TCP Port 18191
Answer: C (LEAVE A REPLY)

NEW QUESTION: 353
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?
A. Combined
B. Pentagon
C. Star
D. Meshed
Answer: (SHOW ANSWER)

NEW QUESTION: 354
What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?
A. CPUSE offline upgrade only
B. Advanced upgrade or CPUSE offline upgrade
C. Advanced Upgrade only
D. SmartUpdate offline upgrade
Answer: B (LEAVE A REPLY)
Explanation
The best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet is either Advanced upgrade or CPUSE offline upgrade. Advanced upgrade is a manual procedure that involves backing up the current configuration, installing the new version from an ISO image, and restoring the configuration. CPUSE offline upgrade is an automated procedure that involves downloading the upgrade package from the Check Point User Center, transferring it to the Security Management Server, and installing it using CPUSE. SmartUpdate offline upgrade is not a valid option, as SmartUpdate is a tool for managing licenses and software packages on multiple gateways and servers1. References: 1: Check Point Software, Getting Started, Upgrading Security Management Servers.

NEW QUESTION: 355
What is the Implicit Clean-up Rule?
A. Another name for the Clean-up Rule.
B. A setting that is configured per Policy Layer.
C. Automatically created when the Clean-up Rule is defined.
D. A setting is defined in the Global Properties for all policies.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 356
Gaia has two default user accounts that cannot be deleted. What are those user accounts?
A. Admin and Default
B. Expert and Clish
C. Control and Monitor
D. Admin and Monitor

Answer: D (LEAVE A REPLY)

Explanation

Gaia has two default user accounts that cannot be deleted: Admin and Monitor. Admin is a superuser account that has full access to all Gaia features and commands. Monitor is a read-only account that can view Gaia configuration and status but cannot make any changes. Both accounts have predefined passwords that can be changed by the Admin user. References: [Check Point R81 Gaia Administration Guide], page 29 SRC: GAIA R81.20 Administration Guide User Management -> Users These users are created by default and cannot be deleted: admin and monitor

NEW QUESTION: 357

What traffic does the Anti-bot feature block?

A. Command and Control traffic from hosts that have been identified as infected

B. Command and Control traffic to servers with reputation for hosting malware

C. Network traffic that is directed to unknown or malicious servers

D. Network traffic to hosts that have been identified as infected

Answer: (SHOW ANSWER)

Explanation

The traffic that the Anti-bot feature blocks is command and control traffic from hosts that have been identified as infected. Anti-bot is a blade that detects and prevents botnet attacks by using a cloud-based service that provides up-to-date threat intelligence. When Anti-bot detects a host that is communicating with a malicious command and control server, it blocks the traffic and generates an alert2. The other options are not the types of traffic that Anti-bot blocks. References: 2: Check Point Software, Getting Started, Anti-Bot.

NEW QUESTION: 358

What is the base level encryption key used by Capsule Docs?

A. RSA 2048

B. RSA 1024

C. SHA-256

D. AES

Answer: A (LEAVE A REPLY)

Explanation

The base level encryption key used by Capsule Docs is RSA 2048. This means that Capsule Docs uses a 2048-bit RSA public key encryption algorithm to encrypt and decrypt documents. RSA is an asymmetric encryption algorithm that uses two keys: a public key that can be shared with anyone, and a private key that must be kept secret. AES, SHA-256, and RSA 1024 are not the base level encryption keys used by Capsule Docs. References: : Check Point Software, Getting Started, Capsule Docs Encryption.

NEW QUESTION: 359

Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up.

B. There is Load Sharing solution set up.

C. Only when there is Unicast solution set up.

D. There is High Availability solution set up.

Answer: (SHOW ANSWER)

Explanation

Check Point ClusterXL Active/Active deployment is used when there is Load Sharing solution set up. Load Sharing is a ClusterXL mode that allows distributing the network traffic between all cluster members, while still providing high availability in case of failures. Load Sharing can be configured as either Unicast or Multicast, depending on the network topology and switches support. References: R81 ClusterXL Administration Guide, page 9.

NEW QUESTION: 360

What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

A. CCP and 18190

B. CCP and 257

C. CCP and 8116

D. CPC and 8116

Answer: C (LEAVE A REPLY)

Explanation

ClusterXL is a clustering technology that provides high availability and load sharing for Security Gateways. ClusterXL uses a proprietary protocol called Check Point Cluster Protocol (CCP) to communicate between cluster members. CCP has two main functions: Health Check and State Synchronization. Health Check is the mechanism that monitors the status and availability of each cluster member and determines which member is the active one. State Synchronization is the mechanism that synchronizes the connection and NAT tables between cluster members to ensure a smooth failover in case of a member failure. CCP uses UDP port 8116 for both Health Check and State Synchronization messages. The other options are not correct because:

A). CCP and 18190: This option is incorrect because CCP does not use port 18190. Port 18190 is used by Secure Internal Communication (SIC) between Security Gateways and Management Servers.

B). CCP and 257: This option is incorrect because CCP does not use port 257. Port 257 is used by Check Point Security Management Protocol (CPM) for communication between SmartConsole and Management Servers.

D). CPC and 8116: This option is incorrect because there is no such protocol as CPC in ClusterXL.

References: ClusterXL R81.20 Administration Guide, ClusterXL Administration Guide R80.40, sk25977 - Ports used by Check Point software

NEW QUESTION: 361

What are possible Automatic Reactions in SmartEvent?

A. Mail. SNMP Trap, Block Source. Block Event Activity, External Script

B. Web Mail. Block Destination, SNMP Trap. SmartTask

C. Web Mail, Block Service. SNMP Trap. SmartTask, Geo Protection

D. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Answer: (SHOW ANSWER)

Explanation

The possible Automatic Reactions in SmartEvent are Mail, SNMP Trap, Block Source, Block Event Activity, and External Script1. Automatic Reactions are actions that SmartEvent can perform automatically when a specific event

occurs2. They can help you respond quickly and efficiently to security incidents and threats2. The Automatic Reactions are1:
Mail: This reaction sends an email notification to a specified recipient with the details of the event. You can customize the subject and the body of the email, and use variables to include relevant information.
SNMP Trap: This reaction sends an SNMP trap to a specified SNMP server with the details of the event. You can customize the OID and the community string of the trap, and use variables to include relevant information.
Block Source: This reaction blocks the source IP address of the event from accessing your network for a specified duration. You can choose to block the source on all gateways or on specific gateways. You can also choose to block the source on a specific port or service.
Block Event Activity: This reaction blocks the specific activity that triggered the event from occurring again for a specified duration. You can choose to block the activity on all gateways or on specific gateways. You can also choose to block the activity on a specific port or service.
External Script: This reaction runs an external script on a specified server with the details of the event as arguments. You can use any script that can be executed by the operating system of the server, such as bash, perl, python, etc. You can use variables to include relevant information in the script arguments.
References: SmartEvent R81.20 Administration Guide - Check Point Software, SmartEvent - Check Point Software

NEW QUESTION: 362
Alice & Bob are going to deploy Management Data Plane Separation (MDPS) for all their Check Point Security Gateway(s)/Cluster(s). Which of the following statement is true?
A. Each network environment is dependent and includes interfaces, routes, sockets, and processes
B. Management Plane - To access, provision and monitor the Security Gateway
C. Data Plane - To access, provision and monitor the Security Gateway
D. Management Plane - for all other network traffic and processing
Answer: B (LEAVE A REPLY)
Explanation
Management Data Plane Separation (MDPS) is a feature that allows the separation of the management plane and the data plane on a Security Gateway or a cluster. The management plane is responsible for accessing, provisioning and monitoring the Security Gateway, while the data plane is responsible for all other network traffic and processing. Each network environment is independent and includes interfaces, routes, sockets, and processes1. References: Check Point R81 Administration Guide

NEW QUESTION: 363

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

A. Clientless remote access

B. Direct access

C. Client-based remote access

D. Clientless direct access

Answer: A (LEAVE A REPLY)

NEW QUESTION: 364

SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

A. 19090,22

B. 19190,22

C. 18190,80

D. 19009,443

Answer: D (LEAVE A REPLY)

Explanation

To use SmartConsole R81 for managing SmartEvent R81, you need to have the following ports open:

Port 19009 for communication over HTTPS (443)

Port 19009 for communication over HTTP (80)

These ports are necessary for the SmartConsole to communicate with SmartEvent for management and monitoring purposes.

References: Check Point Certified Security Expert R81 documentation and learning resources.

NEW QUESTION: 365

Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

A. Security Gateway Clusters in Load Sharing mode

B. Dedicated Log Server

C. Dedicated SmartEvent Server

D. Security Gateways/Clusters in ClusterXL HA new mode

Answer: A (LEAVE A REPLY)

Explanation

Security Gateway Clusters in Load Sharing mode are not supported by the Central Deployment feature in R81.10 SmartConsole. According to the Check Point R81.10 Known Limitations article1, Central Deployment in SmartConsole does not support:

Connection from SmartConsole Client to the Management Server through a proxy server. In this case, use the applicable API command ClusterXL in Load Sharing mode VRRP Cluster Installation of a package on a VSX VSLS Cluster that contains more than 3 members.

On Multi-Domain Servers: Global Domain, or the MDS context

Standalone server

Standby Security Management Server or Multi-Domain Security Management

Scalable Platforms 40000 / 60000

SMB Appliances
The other options are supported by the Central Deployment feature in R81.10 SmartConsole. Dedicated Log Server, Dedicated SmartEvent Server, and Security Gateways/Clusters in ClusterXL HA new mode can be selected as targets for installing packages using the Central Deployment wizard.

NEW QUESTION: 366
Kurt is planning to upgrade his Security Management Server to R81.X. What is the lowest supported version of the Security Management he can upgrade from?
A. R75 Gaia
B. R75 Splat
C. R76 Splat
D. R77.X Gaia
Answer: A (LEAVE A REPLY)

NEW QUESTION: 367
You have existing dbedit scripts from R77. Can you use them with R81.10?
A. dbedit is not supported in R81.10
B. dbedit is fully supported in R81.10
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
D. dbedit scripts are being replaced by mgmt_cli in R81.10
Answer: D (LEAVE A REPLY)

NEW QUESTION: 368
In the Firewall chain mode FFF refers to:
A. Stateful Packets
B. No Match
C. All Packets
D. Stateless Packets
Answer: (SHOW ANSWER)
Explanation
In the Firewall chain mode FFF refers to all packets. Firewall chain mode is a feature that allows administrators to define how packets are processed by different firewall kernel modules in inbound and outbound directions. FFF is one of the predefined chain modes that applies all firewall kernel modules (Firewall, VPN, IPS, etc.) to all packets, regardless of their state or connection. This mode provides maximum security, but also consumes more CPU resources.

NEW QUESTION: 369
Which tool is used to enable ClusterXL?
A. sysconfig
B. SmartConsole
C. SmartUpdate

D. cpconfig
Answer: (SHOW ANSWER)