CheckPoint.156-315.81.v2023-11-23.q259

Exam Code:	156-315.81
Exam Name:	Check Point Certified Security Expert R81
Certification Provider:	CheckPoint
Free Question Number:	259
Version:	v2023-11-23
# of views:	1545
# of Questions views:	60254
https://www.freecram.net/torrent/CheckPoint.156-315.81.v2023-11-23.q259.html	

NEW QUESTION: 1
What is Dynamic Balancing?
A. 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.
B. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
C. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces
Answer: (SHOW ANSWER)

NEW QUESTION: 2
What is the most recommended way to install patches and hotfixes?
A. CPUSE Check Point Update Service Engine
B. Software Update Service
C. rpm -Uv
D. UnixinstallScript
Answer: (SHOW ANSWER)

NEW QUESTION: 3
What API command below creates a new host object with the name "My Host" and IP address of "192 168 0 10"?
A. new host name "My Host" ip-address "192 168.0.10"
B. set host name "My Host" ip-address "192.168.0.10"
C. mgmt.cli -m <mgmt ip> add host name "My Host" ip-address "192.168.0 10"
D. create host name "My Host" ip-address "192.168 0.10"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?
A. Transfers messages between Firewall processes
B. Restart Daemons if they fail
C. Secure Internal Communication (SIC)
D. Pulls application monitoring status
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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.
A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.
C. 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.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Capsule Connect and Capsule Workspace both offer secured connection for remote users who are using their mobile devices. However, there are differences between the two.
Which of the following statements correctly identify each product's capabilities?
A. Workspace supports ios operating system, Android, and WP8, whereas Connect supports ios operating system and Android only
B. For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connect offers both jailbreak/root detection and MDM cooperative enforcement.
C. Workspace can support any application, whereas Connect has a limited number of application types which it will support.
D. For credential protection, Connect uses One-time Password login support and has no SSO support, whereas Workspace offers both One-Time Password and certain SSO login support.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
What are the Threat Prevention software components available on the Check Point Security Gateway?
A. IPS, Threat Emulation and Threat Extraction

B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
D. IDS, Forensics, Anti-Virus, Sandboxing
Answer: (SHOW ANSWER)
Explanation
To challenge today's malware landscape, Check Point's comprehensive Threat Prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to detect and block modern malware.
For more information, see the R81 Threat Prevention Administration Guide.
These Software Blades provide Threat Prevention:
Anti-Bot Software Blade
Anti-Virus Software Blade
Threat Extraction Software Blade
Threat Emulation Software Blade
IPS Software Blade

NEW QUESTION: 8
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?
A. it is not possible.
B. Use Multi-Domain Management Server.
C. Install Management and SmartEvent on different machines.
D. Choose different setting for log storage and SmartEvent db
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which of the following is NOT an option to calculate the traffic direction?
A. External
B. Outgoing
C. Internal
D. Incoming
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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)

NEW QUESTION: 11
Which Check Point feature enables application scanning and the detection?
A. Application Dictionary
B. AppWiki
C. CPApp
D. Application Library
Answer: (SHOW ANSWER)

NEW QUESTION: 12
You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?
A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
B. ifconfig eth1 hw 11:11:11:11:11:11; expert
C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
D. ethtool -i eth2 mac 11:11:11:11:11:11; expert
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of these statements describes the Check Point ThreatCloud?
A. Blocks or limits usage of web applications
B. Prevents Cloud vulnerability exploits
C. Prevents or controls access to web sites based on category
D. A worldwide collaborative security network
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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/Extended
B. Accounting
C. Accounting/Suppression
D. Suppression
Answer: (SHOW ANSWER)

NEW QUESTION: 15
There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?
A. Using SmartConsole GUI console
B. Using Mgmt_cli tool
C. Events are collected with SmartWorkflow from Trouble Ticket systems
D. Using Web Services

E. Using CLISH
Answer: (SHOW ANSWER)

NEW QUESTION: 16
What is the command to show SecureXL status?
A. fwaccel status
B. fwaccel stats -m
C. fwaccel -s
D. fwaccel stat
Answer: (SHOW ANSWER)
Explanation
To check overall SecureXL status:
[Expert@HostName]# fwaccel stat
References:

NEW QUESTION: 17
You need to see which hotfixes are installed on your gateway, which command would you use?
A. cpinfo -l hotfix
B. cpinfo -o hotfix
C. cpinfo -h all
D. cpinfo -y all
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?
A. cpwd
B. fwd
C. cpd
D. fwm
Answer: (SHOW ANSWER)

Explanation
Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that requite direct GUI access, such as SmartEvent, It provides the following:
- GUI Client communication
- Database manipulation
- Policy Compilation
- Management HA sync

NEW QUESTION: 19
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)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_RemoteAccessVPN_AdminGuide/T

NEW QUESTION: 20
Which Check Point software blade provides protection from zero-day and undiscovered threats?
A. Application Control
B. Threat Emulation
C. Firewall
D. Threat Extraction
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which CLI command will reset the IPS pattern matcher statistics?
A. ips pstats reset
B. ips pmstats reset
C. ips reset pmstat
D. ips pmstats refresh
Answer: (SHOW ANSWER)

NEW QUESTION: 22
The Firewall kernel is replicated multiple times, therefore:
A. The Firewall kernel only touches the packet if the connection is accelerated
B. The Firewall can run different policies per core
C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
D. The Firewall can run the same policy on all cores.
Answer: (SHOW ANSWER)

Explanation
On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.
References:

NEW QUESTION: 23
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways
A. action:"Key Install" AND 1.1.1.1 AND Main Mode
B. action:"Key Install- AND 1.1.1.1 ANDQuick Mode
C. Blade:"VPN" AND VPN-Stores AND Quick Mode
D. Blade:"VPN" AND VPN-Stores AND Main Mode
Answer: (SHOW ANSWER)

NEW QUESTION: 24
What are the three components for Check Point Capsule?
A. Capsule Workspace, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Docs, Capsule Connect
C. Capsule Docs, Capsule Cloud, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which command will allow you to see the interface status?
A. cphaprob -a if
B. cphaprob -I interface
C. cphaprob interface
D. cphaprob stat
Answer: (SHOW ANSWER)

NEW QUESTION: 26
John is using Management HA. Which Security Management Server should he use for making changes?
A. active SmartConsole
B. primary Log Server
C. connect virtual IP of Smartcenter HA
D. secondary Smartcenter
Answer: (SHOW ANSWER)

NEW QUESTION: 27
In R81, how do you manage your Mobile Access Policy?
A. Through the Mobile Console
B. From the Dedicated Mobility Tab
C. From SmartDashboard
D. Through the Unified Policy
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____
.
A. Captive Portal and Transparent Kerberos Authentication
B. User Directory
C. UserCheck
D. Captive Portal
Answer: (SHOW ANSWER)

NEW QUESTION: 29
What is required for a site-to-site VPN tunnel that does not use certificates?
A. RSA Token
B. SecureID
C. Unique Passwords
D. Pre-Shared Secret
Answer: (SHOW ANSWER)

NEW QUESTION: 30
Which component is NOT required to communicate with the Web Services API?
A. Request payload
B. API key
C. content-type
D. session ID token
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of these is an implicit MEP option?
A. Round robin
B. Primary-backup
C. Load Sharing
D. Source address based
Answer: (SHOW ANSWER)

NEW QUESTION: 32
The Correlation Unit performs all but the following actions:
A. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.
B. Assigns a severity level to the event.
C. Generates an event based on the Event policy.
D. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
In which deployment is the security management server and Security Gateway installed on the same appliance?
A. Standalone
B. Remote
C. Distributed
D. Bridge Mode
Answer: (SHOW ANSWER)
Explanation
SRC: Installation and Upgrade Guide R81 In a Standalone deployment, a Check Point computer runs both the Security Gateway and Security Management Server products.

NEW QUESTION: 34
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?
A. UDP port 265
B. TCP port 265
C. UDP port 256
D. TCP port 256
Answer: (SHOW ANSWER)
Explanation
Synchronization works in two modes:

Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.
Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.
References:

NEW QUESTION: 35
SmartEvent Security Checkups can be run from the following Logs and Monitor activity:
A. Checkups
B. Reports
C. Advanced
D. Views
Answer: (SHOW ANSWER)

NEW QUESTION: 36
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?
A. Host having a Critical event found by IPS
B. Host having a Critical event found by Antivirus
C. Host having a Critical event found by Threat Emulation
D. Host having a Critical event found by Anti-Bot
Answer: (SHOW ANSWER)

NEW QUESTION: 37
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)
Explanation
"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-S

NEW QUESTION: 38
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 "cpstop" on the relevant gateway and check the ping again

B. run "fw ctl zdebug drop" on the relevant gateway
C. run fw unloadlocal" on the relevant gateway and check the ping again
D. run "fw log" on the relevant gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which tool is used to enable ClusterXL?
A. SmartUpdate
B. SmartConsole
C. cpconfig
D. sysconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following commands shows the status of processes?
A. cpwd admin_list
B. cpwd_admin -l
C. cpwd_admin list
D. cpwd -l
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What is the purpose of the command "ps aux | grep twd"?
A. You can check the Process ID and the processing time of the twd process.
B. You can convert the log file into Post Script format.
C. You can check whether the IPS default setting is set to Detect or Prevent mode
D. You can list all Process IDs for all running services.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
What is the correct order of the default "fw monitor" inspection points?
A. i, o, I, O
B. i, I, o, O
C. 1, 2, 3, 4
D. I, i, O, o
Answer: (SHOW ANSWER)
Explanation
https://community.checkpoint.com/t5/General-Topics/Check-Point-Inspection-points-iIoO/td-p/34938 The default order of the "fw monitor" inspection points is:
i (input): this is the first inspection point, where packets enter the firewall.

I (local): this is the second inspection point, where packets are processed locally by the firewall, before being forwarded to the next hop.
o (output): this is the third inspection point, where packets are sent out to their final destination.
O (offload): this is the fourth inspection point, where packets are offloaded to hardware acceleration for faster processing.

NEW QUESTION: 43
Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.
A. FWD
B. CPVIEWD
C. DASSERVICE
D. CPD
Answer: (SHOW ANSWER)

NEW QUESTION: 44
Which command collects diagnostic data for analyzing customer setup remotely?
A. cpinfo
B. migrate export
C. sysinfo
D. cpview
Answer: (SHOW ANSWER)
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: 45
Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?
A. ethtool A eth0
B. ip show Int eth0
C. ifconfig -i eth0 verbose
D. show interface eth0 mq
Answer: (SHOW ANSWER)

NEW QUESTION: 46

The SmartEvent R81 Web application for real-time event monitoring is called:
A. SmartView Monitor
B. There is no Web application for SmartEvent
C. SmartView
D. SmartEventWeb
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
Which of the following is NOT an alert option?
A. User defined alert
B. High alert
C. SNMP
D. Mail
Answer: (SHOW ANSWER)

NEW QUESTION: 48
What is the least amount of CPU cores required to enable CoreXL?
A. 6
B. 2
C. 4
D. 1
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Which one of the following is NOT a configurable Compliance Regulation?
A. SOCI
B. NCIPA
C. CJIS
D. GLBA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50

What solution is Multi-queue intended to provide?

A. Improve the efficiency of CoreXL Kernel Instances
B. Reduce the performance of network interfaces
C. Improve the efficiency of traffic handling by SecureXL SNDs
D. Reduce the confusion for traffic capturing in FW Monitor
Answer: (SHOW ANSWER)

NEW QUESTION: 51
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 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.
D. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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 Capsule Workspace
B. Check Point Capsule Remote
C. Check Point Remote User
D. Check Point Mobile Web Portal
Answer: (SHOW ANSWER)

NEW QUESTION: 53
The Event List within the Event tab contains:

A. events generated by a query.
B. a list of options available for running a query.
C. the details of a selected event.
D. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?
A. fwd via cpm
B. cpm via cpd
C. fwm via fwd
D. fwd via cpd
Answer: (SHOW ANSWER)

NEW QUESTION: 55
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)
Explanation
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION: 56
How can SmartView application accessed?
A. https://<Security Management host name>:4434/smartview/
B. http://<Security Management IP Address>/smartview
C. https://<Security Management IP Address>/smartview/
D. http://<Security Management IP Address>:4434/smartview/
Answer: (SHOW ANSWER)

NEW QUESTION: 57
You can access the ThreatCloud Repository from:
A. R81.10 SmartConsole and Threat Prevention
B. R81.10 SmartConsole and Application Wiki
C. Threat Wiki and Check Point Website
D. Threat Prevention and Threat Tools
Answer: (SHOW ANSWER)

NEW QUESTION: 58

Connections to the Check Point R81 Web API use what protocol?
A. HTTPS
B. RPC
C. VPN
D. SIC
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which features are only supported with R81.10 Gateways but not R77.x?
A. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
B. Time object to a rule to make the rule active only during specified times.
C. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
D. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

A. Check Point Software Update Agent
B. Check Point Remote Installation Daemon (CPRID)
C. Check Point Update Service Engine
D. Check Point Software Update Daemon
Answer: (SHOW ANSWER)

NEW QUESTION: 61
What Is the difference between Updatable Objects and Dynamic Objects
A. Dynamic Objects are maintained automatically by the Threat Cloud. For Dynamic Objects there rs no need to install policy for the changes to take effect. Updatable Objects are created and maintained locally.
B. Updatable Objects is a Threat Cloud Service. The provided Objects are updated automatically. Dynamic Objects are created and maintained locally For Dynamic Objects there is no need to install policy for the changes to take effect.
C. Dynamic Objects ate maintained automatically by the Threat Cloud. Updatable Objects are created and maintained locally. In both cases there is no need to install policy for the changes to take effect.
D. Updatable Objects is a Threat Cloud Service. The provided Objects are updated automatically. Dynamic Objects are created and maintained locally In both cases there is no need to install policy for the changes to take effect.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
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)
Explanation
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION: 63
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. Correlates all the identified threats with the consolidation policy.
B. Collects syslog data from third party devices and saves them to the database.
C. Connects with the SmartEvent Client when generating threat reports.
D. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.
What is one of the requirements for his success?
A. 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
B. 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
C. Size of the /var/log folder of the target machine must be at least 25GB or more
D. 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

Answer: (SHOW ANSWER)

NEW QUESTION: 65
What technologies are used to deny or permit network traffic?
A. Packet Filtering, Stateful Inspection, and Application Layer Firewall
B. Stateful Inspection, URL/Application Blade, and Threat Prevention
C. Firewall Blade, URL/Application Blade, and IPS
D. Stateful Inspection, Firewall Blade, and URL/Application Blade
Answer: (SHOW ANSWER)

NEW QUESTION: 66
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: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION: 67
If a "ping"-packet is dropped by FW1 Policy -on how many inspection Points do you see this packet in "fw monitor"?
A. "i" only
B. I don't see it in fw monitor
C. "i", "I" and "o"
D. "i" and "I"
Answer: (SHOW ANSWER)

NEW QUESTION: 68
From SecureXL perspective, what are the three paths of traffic flow:
A. Firewall Path; Accept Path; Drop Path
B. Firewall Path; Accelerated Path; Medium Path
C. Initial Path; Medium Path; Accelerated Path
D. Layer Path; Blade Path; Rule Path
Answer: (SHOW ANSWER)

NEW QUESTION: 69

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

A. Failovers

B. Asymmetric routing

C. Symmetric routing

D. Anti-Spoofing

Answer: (SHOW ANSWER)

NEW QUESTION: 70

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

A. All connections are processed and synchronized by the pivot

B. Is only relevant when using SecureXL

C. Is configured using cpconfig

D. Can only be changed for Load Sharing implementations

Answer: (SHOW ANSWER)

NEW QUESTION: 71

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: 72

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

A. Hypertext Transfer Protocol Secure (HTTPS)

B. Lightweight Directory Access Protocol (LDAP)

C. Windows Management Instrumentation (WMI)

D. Remote Desktop Protocol (RDP)

Answer: (SHOW ANSWER)

NEW QUESTION: 73

How often does Threat Emulation download packages by default?

A. Once a week
B. Once per day
C. Once an hour
D. Twice per day
Answer: (SHOW ANSWER)

NEW QUESTION: 74
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. Big O
B. Little i
C. Big I
D. Little o
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
You pushed a policy to your gateway and you cannot access the gateway remotely any more. What command should you use to remove the policy from the gateway by logging in through console access?
A. "fw unloadpolicy"
B. "fwundo"
C. "fw cpstop"
D. "fw unloadlocal"
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Fill in the blank: _____ information is included in "Full Log" tracking option, but is not included in "Log" tracking option?
A. Application
B. File attributes
C. Data type
D. Destination port
Answer: (SHOW ANSWER)

NEW QUESTION: 77
What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?
A. Security Gateway failover as well as Security Management Server failover is a manual procedure.
B. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
C. Security Gateway failover as well as Security Management Server failover is an automatic procedure.
D. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
With SecureXL enabled, accelerated packets will pass through the following:
A. Network Interface Card, Check Point Firewall Kernal, and the Acceleration Device
B. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
C. Network Interface Card, OSI Network Layer, and the Acceleration Device
D. Network Interface Card and the Acceleration Device
Answer: (SHOW ANSWER)

NEW QUESTION: 79
The following command is used to verify the CPUSE version:
A. [Expert@HostName:0]#show installer status
B. [Expert@HostName:0]#show installer status build
C. HostName:0>show installer build
D. HostName:0>show installer status build
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

A. Both License (.lic) and Contract (.xml) files
B. Contract file (.xml)
C. license File (.lic)
D. cp.macro
Answer: (SHOW ANSWER)

NEW QUESTION: 81
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 number of cores must be the same on every participating cluster node
C. The Sync interface must not have an IP address configured
D. The Magic MAC number must be unique per cluster node
Answer: (SHOW ANSWER)

NEW QUESTION: 82
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 (not on Quantum Spark or Open Server)
B. 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)
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 and Open Server (not on Quantum Spark)
D. 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)
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which view is NOT a valid CPVIEW view?
A. IDA
B. PDP
C. RAD
D. VPN
Answer: (SHOW ANSWER)

NEW QUESTION: 84
What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?
A. Anti-Bot is the only countermeasure against unknown malware
B. Anti-Bot is the only signature-based method of malware protection.
C. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.
D. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85

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

NEW QUESTION: 86
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: (SHOW ANSWER)
Explanation
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.
References:

NEW QUESTION: 87
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____ .
A. TCP Port 18209
B. TCP Port 19009
C. TCP Port 18191
D. TCP Port 18190
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?
A. fwm
B. cpd
C. cpwd
D. cpm
Answer: (SHOW ANSWER)

NEW QUESTION: 89
What Factor preclude Secure XL Templating?
A. ClusterXL in load sharing Mode
B. Source Port Ranges/Encrypted Connections

C. CoreXL
D. IPS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 90
VPN Link Selection will perform the following when the primary VPN link goes down?
A. The Firewall will inform the client that the tunnel is down.
B. The Firewall will drop the packets.
C. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
D. The Firewall will send out the packet on all interfaces.
Answer: (SHOW ANSWER)

NEW QUESTION: 91
SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their dat a.
Which component is NOT part of the SandBlast Mobile solution?
A. Behavior Risk Engine
B. Personal User Storage
C. Management Dashboard
D. Gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Besides fw monitor, what is another command that can be used to capture packets?
A. ping
B. traceroute
C. arp
D. tcpdump
Answer: (SHOW ANSWER)

NEW QUESTION: 93
DLP and Geo Policy are examples of what type of Policy?

A. Inspection Policies
B. Standard Policies
C. Unified Policies
D. Shared Policies
Answer: (SHOW ANSWER)

NEW QUESTION: 94
The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to "None"?
A. No, it will work independently. Hit Count will be shown only for rules Track option set as Log or alert.
B. Yes it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways.
C. No, it will not work independently because hit count requires all rules to be logged.
D. Yes it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway.
Answer: (SHOW ANSWER)

NEW QUESTION: 95
What command verifies that the API server is responding?
A. api status
B. api stat
C. show api_status
D. app_get_status
Answer: (SHOW ANSWER)

NEW QUESTION: 96
What is the difference between an event and a log?
A. A log entry becomes an event when it matches any rule defined in Event Policy
B. Events are generated at gateway according to Event Policy
C. Log and Events are synonyms
D. Events are collected with SmartWorkflow form Trouble Ticket systems
Answer: (SHOW ANSWER)

NEW QUESTION: 97
After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?
A. You have to launch the WebUI and go to "Config" -> "Export Config File" and specifiy the destination directory of your local file system.
B. You cannot locate the file in the file system since Clish does not have any access to the bash file system
C. You can locate the file via SmartConsole > Command Line.
D. You will find it in the home directory of your user account (e.g. /home/admin/)
Answer: (SHOW ANSWER)

NEW QUESTION: 98
What traffic does the Anti-bot feature block?
A. Command and Control traffic to servers with reputation for hosting malware
B. Network traffic to hosts that have been identified as infected
C. Network traffic that is directed to unknown or malicious servers
D. Command and Control traffic from hosts that have been identified as infected
Answer: (SHOW ANSWER)

NEW QUESTION: 99
What has to be taken into consideration when configuring Management HA?
A. SmartConsole must be closed prior to synchronized changes in the objects database
B. For Management Server synchronization, only External Virtual Switches are supported. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.
C. The Database revisions will not be synchronized between the management servers
D. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpredundant to pass before the Firewall Control Connections.
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?
A. Dedicated SmartEvent Server
B. Security Gateway Clusters in Load Sharing mode
C. Security Gateways/Clusters in ClusterXL HA new mode
D. Dedicated Log Server
Answer: (SHOW ANSWER)

NEW QUESTION: 101
Which is NOT an example of a Check Point API?
A. OPSC SDK
B. Management API
C. Gateway API
D. Threat Prevention API
Answer: (SHOW ANSWER)

NEW QUESTION: 102
The WebUI offers several methods for downloading hotfixes via CPUSE except:
A. Automatic
B. Manually
C. Scheduled
D. Force override

Answer: (SHOW ANSWER)

NEW QUESTION: 103
An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?
A. He can use the fwaccel stat command on the gateway
B. He can use the fwaccel stat command on the Security Management Server.
C. He can use the fw accel stat command on the gateway.
D. He can use the fw accel statistics command on the gateway.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
How can you see historical data with cpview?
A. cpview -d <timestamp>
B. cpview -e <timestamp>
C. cpview -t <timestamp>
D. cpview -f <timestamp>
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?
A. Source Address
B. Destination Address
C. TCP Acknowledgment Number
D. Source Port
Answer: (SHOW ANSWER)
Explanation
https //sc1.checkpoint.com/documents/R77/CP R77_Firewall_WebAdmm/92711.htm

NEW QUESTION: 106
Which Check Point daemon monitors the other daemons?
A. cpd
B. fwm
C. cpwd
D. fwssd
Answer: (SHOW ANSWER)

NEW QUESTION: 107
Customer's R81 management server needs to be upgraded to R81.10. What is the best upgrade method when the management server is not connected to the Internet?
A. Export R81 configuration, clean install R81.10 and import the configuration
B. SmartUpdate upgrade
C. CPUSE offline upgrade
D. CPUSE online upgrade
Answer: (SHOW ANSWER)

NEW QUESTION: 108
What is the name of the secure application for Mail/Calendar for mobile devices?
A. Capsule Workspace
B. Secure Workspace
C. Capsule Mail
D. Capsule VPN
Answer: (SHOW ANSWER)

NEW QUESTION: 109
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. IPSEC Phase 1
B. IPSEC Phase 2
C. IKE Phase 2
D. IKE Phase 1
Answer: (SHOW ANSWER)

NEW QUESTION: 110
What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

A. The corresponding feature is new to R81.10 and is called "Management Data Plane Separation"
B. The corresponding feature is called "Dynamic Dispatching"
C. The corresponding feature is called "Dynamic Split"

D. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?
A. Never been synchronized
B. Synchronized
C. Collision
D. Lagging
Answer: (SHOW ANSWER)

NEW QUESTION: 112
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?
A. Publish changes
B. Install database
C. Install policy
D. Save changes
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Which of the following is NOT a type of Endpoint Identity Agent?
A. Full
B. Terminal
C. Custom
D. Light
Answer: (SHOW ANSWER)

NEW QUESTION: 114
What is required for a certificate-based VPN tunnel between two gateways with separate management systems?
A. Unique Passwords
B. Mutually Trusted Certificate Authorities
C. Shared Secret Passwords
D. Shared User Certificates
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Installations and upgrades with CPUSE require that the CPUSE agent is up-to-date. Usually the latest build is downloaded automatically. How can you verify the CPUSE agent build?

A. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer status build
B. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer agent
C. In WebUI Status and Actions page or by running the following command in CLISH: show installer status build
D. In WebUI Status and Actions page or by running the following command in CLISH: show installer status version
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Security Checkup Summary can be easily conducted within:
A. Checkups
B. Views
C. Summary
D. Reports
Answer: (SHOW ANSWER)

NEW QUESTION: 117
What are the two types of tests when using the Compliance blade?
A. Policy-based tests and Global properties
B. Global tests and Object-based tests
C. Access Control policy analysis and Threat Prevention policy analysis
D. Tests conducted based on the IoC XMfcfile and analysis of SOLR documents
Answer: (SHOW ANSWER)
Explanation
The Check Point Compliance Blade has a library of Check Point-defined tests to use as a baseline for good gateway and policy configuration. A Best Practice test is related to specified regulations in different regulatory standards. It describes compliance status and recommends corrective steps. Global Tests - Examine all applicable configuration settings in the organization. Object-based Tests - Examine the configuration settings for specified objects (gateways, profiles and other objects)
https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION: 118
In the Firewall chain mode FFF refers to:
A. Stateful Packets
B. Stateless Packets
C. No Match
D. All Packets
Answer: (SHOW ANSWER)

NEW QUESTION: 119
The back end database for Check Point R81 Management uses:
A. MySQL
B. DBMS
C. PostgreSQL
D. MongoDB
Answer: (SHOW ANSWER)

NEW QUESTION: 120
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Port
B. Destination Address
C. TCP Acknowledgment Number
D. Source Address
Answer: (SHOW ANSWER)

NEW QUESTION: 121
What is the recommended way to have a redundant Sync connection between the cluster nodes?
A. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per node. Connect both Sync interfaces without using a switch.
B. Use a group of bonded interfaces. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define a Virtual IP for the Sync interface.
C. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per node. Use two different Switches to connect both Sync interfaces.
D. Use a group of bonded interfaces connected to different switches. Define a dedicated sync interface, only one interface per node using the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management.
Answer: (SHOW ANSWER)
Explanation
The recommended way to have a redundant Sync connection between the cluster nodes is to use a group of bonded interfaces connected to different switches. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management, you should define a dedicated sync interface, only one interface per node.

NEW QUESTION: 122
What is not a purpose of the deployment of Check Point API?
A. Execute an automated script to perform common tasks
B. Create a customized GUI Client for manipulating the objects database
C. Create products that use and enhance the Check Point solution
D. Integrate Check Point products with 3rd party solution
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Bob is going to prepare the import of the exported R81.10 management database. Now he wants to verify that the installed tools on the new target security management machine are able to handle the R81.10 release.
Which of the following Check Point command is true?
A. $FWDIR/scripts/migrate_server print_installed_tools -v R77.30
B. $CPDIR/scripts/migrate_server print_installed_tools -v R81.10
C. $FWDIR/scripts/migrate_server print_installed_tools -v R81.10
D. $FWDIR/scripts/migrate_server print_uninstalled_tools -v R81.10
Answer: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_CLI_ReferenceGuide/Topics-
To export the management database and configuration: [Expert@MGMT:0]# cd $FWDIR/scripts/
[Expert@MGMT:0]# ./migrate_server export -v R81.10 [-skip_upgrade_tools_check] [-l | -x]
[--include-uepm-msi-files] [--exclude-uepm-postgres-db] [--ignore_warnings] /<Full Path>/<Name of Exported File>

NEW QUESTION: 124
What does the "unknown" SIC status shown on SmartConsole mean?
A. SIC activation key requires a reset
B. Administrator input the wrong SIC key
C. The management can contact the Security Gateway but cannot establish Secure Internal Communication
D. There is no connection between the Security Gateway and Security Management Server
Answer: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION: 125
Which command is used to add users to or from existing roles?
A. Add user <User Name> roles <List>

B. Add rba user <User Name> roles <List>
C. Add user <User Name>
D. Add rba user <User Name>
Answer: (SHOW ANSWER)

NEW QUESTION: 126
Is it possible to establish a VPN before the user login to the Endpoint Client?
A. no, the user must login first.
B. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console
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 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
Answer: (SHOW ANSWER)

NEW QUESTION: 127
Check Point ClusterXL Active/Active deployment is used when:
A. There is Load Sharing solution set up.
B. Only when there is Unicast solution set up.
C. There is High Availability solution set up.
D. Only when there is Multicast solution set up.
Answer: (SHOW ANSWER)

NEW QUESTION: 128
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. Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.
D. Identity Awareness is not enabled.
Answer: (SHOW ANSWER)

NEW QUESTION: 129
What statement best describes the Proxy ARP feature for Manual NAT in R81.10?
A. local.arp file must always be configured
B. fw ctl proxy should be configured
C. Automatic proxy ARP configuration can be enabled
D. Translate Destination on Client Side should be configured

Answer: (SHOW ANSWER)

NEW QUESTION: 130

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. Mail Transfer Agent
B. Threat Emulation
C. Threat Cloud
D. Mobile Access
Answer: (SHOW ANSWER)

NEW QUESTION: 131

At what point is the Internal Certificate Authority (ICA) created?
A. During the primary Security Management Server installation process.
B. When an administrator initially logs into SmartConsole.
C. Upon creation of a certificate.
D. When an administrator decides to create one.
Answer: (SHOW ANSWER)

NEW QUESTION: 132

Which of the following is NOT a type of Check Point API available in R81.x?
A. Mobile Access
B. Management
C. Identity Awareness Web Services
D. OPSEC SDK
Answer: (SHOW ANSWER)

NEW QUESTION: 133

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 web https-port <new port number>
C. set Gaia-portal port <new port number>
D. set Gaia-portal https-port <new port number>
Answer: (SHOW ANSWER)

NEW QUESTION: 134

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: C (LEAVE A REPLY)
Explanation
One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION: 135
What command would show the API server status?
A. api status
B. show api status
C. cpm status
D. api restart
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which command is used to set the CCP protocol to Multicast?
A. cphaconf set_ccp no_broadcast
B. cphaprob set_ccp multicast
C. cphaprob set_ccp no_broadcast
D. cphaconf set_ccp multicast
Answer: (SHOW ANSWER)

NEW QUESTION: 137
Which one is not a valid Package Option In the Web GUI for CPUSE?
A. Clean Install
B. Upgrade
C. Export Package
D. Database Conversion to R81.10 only
Answer: (SHOW ANSWER)

NEW QUESTION: 138
You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores.
How many cores can be used in a Cluster for Firewall-kernel on the new device?
A. 4
B. 3
C. 2
D. 1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 139
You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?
A. SecuRemote
B. SmartEvent Client Info
C. Check Point Capsule Cloud
D. Check Point Protect
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Which encryption algorithm is the least secured?
A. AES-256
B. 3DES
C. AES-128
D. DES
Answer: D (LEAVE A REPLY)

NEW QUESTION: 141
To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:
A. fw ctl multik set_mode 4
B. fw ctl Dyn_Dispatch on
C. fw ctl multik set_mode 1
D. fw ctl Dyn_Dispatch enable
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Alice & Bob are going to use Management Data Plane Separation and therefore the routing separation needs to be enabled. Which of the following command is true for enabling the Management Data Plane Separation (MDPS):
A. set mdps split brain on

B. set mdps data plane off
C. set mdps mgmt plane on
D. set mdps split plane on
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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. After upgrading the hardware, increase the number of kernel instances using cpconfig
B. Hyperthreading must be enabled in the bios to use CoreXL
C. Run cprestart from dish
D. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores.
Answer: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG
R81
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/T
cpconfig -> Enter the number of the Check Point CoreXL option. (Enter 1 to select Change the number of firewall instances. OR Enter 2 for the option Change the number of IPv6 firewall instances.) -> Enter the total number of IPv4 (IPv6) CoreXL Firewall instances you wish the Security Gateway to run. Follow the instructions on the screen. -> Exit from the cpconfig menu. - Reboot the Security Gateway.

NEW QUESTION: 144
What is not a component of Check Point SandBlast?
A. Threat Extraction
B. Threat Emulation
C. Threat Simulator
D. Threat Cloud
Answer: (SHOW ANSWER)

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

NEW QUESTION: 146

What is the correct command to observe the Sync traffic in a VRRP environment?
A. fw monitor -e "accept port(6118;"
B. fw monitor -e "accept[12:4,b]=224.0.0.18;"
C. fw monitor -e "accept dst=224.0.0.18;"
D. fw monitor -e "accept proto=mcVRRP;"
Answer: (SHOW ANSWER)

NEW QUESTION: 147
What does the Log "Views" tab show when SmartEvent is Correlating events?
A. Top events with charts and graphs
B. Details of a selected logs
C. A list of common reports
D. Reports for customization
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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 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
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 httpd2 to see if the httpd2 is up
C. 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.
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: B (LEAVE A REPLY)

NEW QUESTION: 149
D18912E1457D5D1DDCBD40AB3BF70D5D
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 based and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?
A. The packet is the second in an established TCP connection
B. The connection required a Security server
C. The packets are not multicast
D. The connection is destined for a server within the network
Answer: (SHOW ANSWER)

NEW QUESTION: 150
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)
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: 151
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: 152
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: (SHOW ANSWER)
Explanation

SRC: GAIA R81.10 Administration Guide User Management -> Users These users are created by default and cannot be deleted: admin and monitor

NEW QUESTION: 153
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
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

NEW QUESTION: 154
What is UserCheck?
A. Administrator tool used to monitor users on their network.
B. Messaging tool used to verify a user's credentials.
C. Communication tool used to inform a user about a website or application they are trying to access.
D. Communication tool used to notify an administrator when a new user is created.
Answer: (SHOW ANSWER)

NEW QUESTION: 155
Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?
A. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type
B. The CoreXL FW instances assignment mechanism is based on IP Protocol type
C. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
D. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?
A. Fast Path
B. Accelerated Path
C. Slow Path
D. Medium Path
Answer: (SHOW ANSWER)

NEW QUESTION: 157
You want to store the GAIA configuration in a file for later reference. What command should you use?
A. show config -f <filename>
B. save configuration <filename>
C. write mem <filename>
D. save config -o <filename>
Answer: (SHOW ANSWER)

NEW QUESTION: 158
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: (SHOW ANSWER)
Explanation
ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION: 159
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: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ClusterXL_AdminGuide/Topics-CX

NEW QUESTION: 160
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

A. Combined
B. Star
C. Meshed
D. Pentagon
Answer: (SHOW ANSWER)

NEW QUESTION: 161
For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision
B. Never been synchronized
C. Lagging
D. Down
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Which Remote Access Client does not provide an Office-Mode Address?
A. Check Point Mobile
B. Endpoint Security Suite
C. Endpoint Security VPN
D. SecuRemote
Answer: (SHOW ANSWER)

NEW QUESTION: 163
What is the default size of NAT table fwx_alloc?
A. 20000
B. 25000
C. 10000
D. 35000
Answer: (SHOW ANSWER)

NEW QUESTION: 164
By default, the R81 web API uses which content-type in its response?
A. Java Script
B. Text
C. XML
D. JSON
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Session unique identifiers are passed to the web api using which http header option?
A. Accept-Charset
B. Application
C. Proxy-Authorization
D. X-chkp-sid
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
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. Yes, since 'Switch to higher priority cluster member' option is enabled by default on the Global Properties.
B. No, since 'maintain' current active cluster member' option is enabled by default on the Global Properties.
C. Yes, since 'Switch to higher priority cluster member' option on the cluster object properties is enabled by default.
D. No, since 'maintain' current active cluster member' option on the cluster object properties is enabled by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 167
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: (SHOW ANSWER)
Explanation
Types of Solutions
All of Check Point's Remote Access solutions provide:

NEW QUESTION: 168
What are the attributes that SecureXL will check after the connection is allowed by Security Policy?
A. Source address, Destination address, Source port, Destination port, Protocol
B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
C. Source address, Destination address, Destination port, Protocol
D. Source address, Destination address, Source port, Destination port
Answer: (SHOW ANSWER)

NEW QUESTION: 169

You have used the "set inactivity-timeout 120" command to prevent the session to be disconnected after 10 minutes of inactivity. However, the Web session is being disconnected after 10 minutes. Why?
A. The idle timeout for the web session is specified with the "set web session-timeout" command.
B. The number specified is the amount of the idle timeout in seconds rather than in minutes. So you have to use the command "set inactivity-timeout 600" instead.
C. Probably, you have forgotten to make sure that nobody is accessing the management server via the SmartConsole which locks the management database.
D. The number of minutes is correct. Probably, you have forgotten to save this setting with the "save config" command.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
What is false regarding a Management HA environment?
A. SmartConsole can connect to any management server in Readonly mode.
B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
C. Synchronization will occur automatically with each Publish event if the Standby servers are available.
D. Only one Management Server should be active, while any others be in standby mode
Answer: (SHOW ANSWER)

NEW QUESTION: 171
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 FwlsSecondary
B. cpprod_util MgmtlsPrimary
C. cpprod_util MgmtlsSecondary
D. cpprod_util FwlsPrimary
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?
A. Yes, but they have to have a pre-shared secret key
B. Yes, but they need to have a mutually trusted certificate authority
C. No, they cannot share certificate authorities
D. No, Certificate based VPNs are only possible between Check Point devices
Answer: (SHOW ANSWER)

NEW QUESTION: 173
What is the command to check the status of Check Point processes?
A. cphaprob list

B. cpwd_admin list
C. cptop
D. top
Answer: B (LEAVE A REPLY)

NEW QUESTION: 174
Which of the following is NOT a valid type of SecureXL template?
A. Accept Template
B. Drop Template
C. NAT Template
D. Deny template
Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Which of the following processes pulls the application monitoring status from gateways?
A. fwm
B. cpwd
C. cpm
D. cpd
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Which firewall daemon is responsible for the FW CLI commands?
A. cpd
B. cpm
C. fwd
D. fwm
Answer: (SHOW ANSWER)

NEW QUESTION: 177
What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?
A. Idle <20%
B. SYS <20%
C. Wait <20%
D. USR <20%
Answer: (SHOW ANSWER)

NEW QUESTION: 178
You find one of your cluster gateways showing "Down" when you run the "cphaprob stat" command. You then run the "clusterXL_admin up" on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

A. cpstat -f all
B. cphaprob -f register
C. cphaprob -a list
D. cphaprob -d -s report
Answer: (SHOW ANSWER)

NEW QUESTION: 179
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. Drop
B. Ask
C. Reject
D. Inform
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Automation and Orchestration differ in that:
A. 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.
B. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
C. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 181
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?
A. Network and Application
B. Virtual Adapter and Mobile App
C. Application and Client Service
D. Network and Layers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 182
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.
A. Accept; drop
B. Accept; redirect
C. Redirect; drop
D. Drop; accept
Answer: (SHOW ANSWER)

NEW QUESTION: 183
What is the benefit of "tw monitor" over "tcpdump"?
A. "fw monitor" can be used from the CLI of the Management Server to collect information from multiple gateways.
B. With "fw monitor", you can see the inspection points, which cannot be seen in "tcpdump"
C. "fw monitor" is also available for 64-Bit operating systems.
D. "fw monitor" reveals Layer 2 information, while "tcpdump" acts at Layer 3.
Answer: (SHOW ANSWER)

NEW QUESTION: 184
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, 2, 3, 4
B. 4, 3, 1, 2
C. 3, 1, 2, 4
D. 1, 4, 2, 3
Answer: (SHOW ANSWER)

NEW QUESTION: 185
Which command will reset the kernel debug options to default settings?
A. fw ctl dbg resetall
B. fw ctl debug set 0
C. fw ctl dbg -a 0
D. fw ctl debug 0
Answer: D (LEAVE A REPLY)

NEW QUESTION: 186
Which blades and or features are not supported in R81?
A. SmartEvent Maps
B. SmartConsole Toolbars
C. Identity Awareness
D. SmartEvent
Answer: (SHOW ANSWER)

NEW QUESTION: 187
Which upgrade method you should use upgrading from R80.40 to R81.10 to avoid any downtime?
A. Zero Downtime Upgrade (ZDU)
B. Connectivity Upgrade (CU)
C. Minimal Effort Upgrade (ME)
D. Multi-Version Cluster Upgrade (MVC)
Answer: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION: 188
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)
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: 189
What are the methods of SandBlast Threat Emulation deployment?
A. Cloud, OpenServer and Vmware
B. Cloud, Smart-1 and Hybrid
C. Cloud, Appliance and Private
D. Cloud, Appliance and Hybrid
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following links will take you to the SmartView web application?

A. https://<Security Management Server IP Address>/smartview
B. https://<Security Management Server host name>/smartviewweb/
C. https://<Security Management Server host name>smartviewweb
D. https://<Security Management Server IP Address>/smartview/
Answer: (SHOW ANSWER)

NEW QUESTION: 191
Please choose the path to monitor the compliance status of the Check Point R81.10 based management.
A. Security & Policies --> New Tab --> Compliance View
B. Gateways & Servers --> Compliance View
C. Logs & Monitor --> New Tab --> Open compliance View
D. Compliance blade not available under R81.10
Answer: (SHOW ANSWER)

NEW QUESTION: 192
John detected high load on sync interface. Which is most recommended solution?
A. For short connections like http service - do not sync
B. Add a second interface to handle sync traffic
C. For short connections like icmp service - delay sync for 2 seconds
D. For FTP connections - do not sync
Answer: (SHOW ANSWER)

NEW QUESTION: 193
Main Mode in IKEv1 uses how many packages for negotiation?
A. depends on the make of the peer gateway
B. 6
C. 4
D. 3
Answer: (SHOW ANSWER)

NEW QUESTION: 194
SandBlast appliances can be deployed in the following modes:
A. as a Mail Transfer Agent and as part of the traffic flow only
B. inline/prevent or detect
C. detect only
D. using a SPAN port to receive a copy of the traffic only
Answer: B (LEAVE A REPLY)

NEW QUESTION: 195
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file,

she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.
Which component of SandBlast protection is her company using on a Gateway?
A. SandBlast Threat Extraction
B. SandBlast Agent
C. SandBlast Threat Emulation
D. Check Point Protect
Answer: (SHOW ANSWER)

NEW QUESTION: 196
In what way are SSL VPN and IPSec VPN different?
A. IPSec VPN does not support two factor authentication, SSL VPN does support this
B. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.
C. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
D. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
Answer: (SHOW ANSWER)

NEW QUESTION: 197
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 R81.10
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 #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 R81.10
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 #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 R81.10
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
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION: 198
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. Unsupported firmware on UTM-1 Edge-W appliance
D. Missing an installed R77.20 Add-on on Security Management Server
Answer: (SHOW ANSWER)

NEW QUESTION: 199
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 used to distribute packets among Firewall instances
C. SND is a feature of fw monitor to capture accelerated packets
D. SND is an alternative to IPSec Main Mode, using only 3 packets
Answer: (SHOW ANSWER)

NEW QUESTION: 200

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

A. C

B. S

C. W

D. Space bar

Answer: (SHOW ANSWER)

NEW QUESTION: 201

Return oriented programming (ROP) exploits are detected by which security blade?

A. Check Point Anti-Virus / Threat Emulation

B. Intrusion Prevention Software

C. Application control

D. Data Loss Prevention

Answer: (SHOW ANSWER)

NEW QUESTION: 202

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. Direct access

B. Client-based remote access

C. Clientless direct access

D. Clientless remote access

Answer: (SHOW ANSWER)

NEW QUESTION: 203

SmartConsole R81 x requires the following ports to be open for SmartEvent.

A. 19009, 18190 & 443

B. 18190 & 443

C. 19009, 19004 & 18190

D. 19009, 19090 & 443

Answer: (SHOW ANSWER)

NEW QUESTION: 204

Which of the following authentication methods ARE NOT used for Mobile Access?

A. SecurID

B. Username and password (internal, LDAP)

C. TACACS+

D. RADIUS server

Answer: (SHOW ANSWER)

NEW QUESTION: 205
What two ordered layers make up the Access Control Policy Layer?
A. Network and Application Control
B. Application Control and URL Filtering
C. URL Filtering and Network
D. Network and Threat Prevention
Answer: (SHOW ANSWER)

NEW QUESTION: 206
Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____ .
A. Stored on the Security Management Server.
B. Sent to the Security Administrator.
C. Stored on the Certificate Revocation List.
D. Sent to the Internal Certificate Authority.
Answer: (SHOW ANSWER)

NEW QUESTION: 207
When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?
A. Any size
B. At least 20GB
C. Less than 20GB
D. More than 10GB and less than 20GB
Answer: (SHOW ANSWER)

NEW QUESTION: 208
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, whois, nslookup, and Telnet
B. ping, traceroute, netstat, and nslookup
C. ping, traceroute, netstat, and route
D. ping, nslookup, Telnet, and route
Answer: (SHOW ANSWER)

NEW QUESTION: 209
When defining QoS global properties, which option below is not valid?
A. Schedule
B. Rate

C. Authenticated timeout
D. Weight
Answer: (SHOW ANSWER)

NEW QUESTION: 210
What are the main stages of a policy installation?
A. Verification Compilation, Transfer and Commit
B. Verification, Commit, Installation
C. Initiation, Conversion and FWD REXEC
D. Initiation, Conversion and Save
Answer: (SHOW ANSWER)

NEW QUESTION: 211
Under which file is the proxy arp configuration stored?
A. $FWDIR/conf/local.arp on the gateway
B. $FWDIR/state/proxy_arp.conf on the management server
C. $FWDIR/conf/local.arp on the management server
D. $FWDIR/state/_tmp/proxy.arp on the security gateway
Answer: (SHOW ANSWER)

NEW QUESTION: 212
What is the minimum amount of RAM needed for a Threat Prevention Appliance?
A. 6 GB
B. It depends on the number of software blades enabled
C. 8GB with Gaia in 64-bit mode
D. 4 GB
Answer: (SHOW ANSWER)

NEW QUESTION: 213
Which command shows the current connections distributed by CoreXL FW instances?
A. fw ctl iflist
B. fw ctl multik stat

C. fw ctl affinity -l
D. fw ctl instances -v
Answer: (SHOW ANSWER)

NEW QUESTION: 214
What is the mechanism behind Threat Extraction?
A. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient.
B. This a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender.
C. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.
D. This is a new mechanism to identify the IP address of the sender of malicious codes and put it into the SAM database (Suspicious Activity Monitoring).
Answer: C (LEAVE A REPLY)

NEW QUESTION: 215
To fully enable Dynamic Dispatcher on a Security Gateway:
A. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
B. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
C. run fw multik set_mode 1 in Expert mode and then reboot.
D. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu.
Answer: (SHOW ANSWER)

NEW QUESTION: 216
Which statement is true about ClusterXL?
A. Supports Dynamic Routing (Unicast and Multicast)
B. Supports Dynamic Routing (Unicast Only)
C. Supports Dynamic Routing (Multicast Only)
D. Does not support Dynamic Routing
Answer: (SHOW ANSWER)

NEW QUESTION: 217
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.10 SmartConsole application?
A. Firewall, IPS, Threat Emulation, Application Control.
B. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
C. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.
D. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?
A. Super User
B. Full Access
C. Auditor
D. Read Only All
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?
A. Kerberos Ticket Timed Out
B. Kerberos Ticket Renewed
C. Account Logon
D. Kerberos Ticket Requested
Answer: (SHOW ANSWER)

NEW QUESTION: 220
Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

A. Random Pool
B. CA Authority
C. Certificate's Fingerprint
D. Certificate Authority
Answer: D (LEAVE A REPLY)

NEW QUESTION: 221
Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?
A. https://<Device_IP_Address>:4434
B. https://<Device_IP_Adress>
C. http://<Device IP_Address>:443
D. https://<Device_IP_Address>:10000
Answer: (SHOW ANSWER)

NEW QUESTION: 222
Which TCP port does the CPM process listen on?
A. 18190

B. 18191
C. 19009
D. 8983
Answer: (SHOW ANSWER)

NEW QUESTION: 223
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
References:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/T

NEW QUESTION: 224
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?
A. sim erdos -e 1
B. sim erdos -x 1
C. sim erdos -v 1
D. sim erdos - m 1
Answer: (SHOW ANSWER)

NEW QUESTION: 225
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 -l list
B. cphaprob -a if
C. cphaprob stat
D. cphaprob all show stat
Answer: (SHOW ANSWER)

NEW QUESTION: 226
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?
A. 50%
B. 80%
C. 15%

D. 75%
Answer: (SHOW ANSWER)

NEW QUESTION: 227
What processes does CPM control?
A. DLEServer, Object-Store, CP Process and database changes
B. web_services, dle_server and object_Store
C. web-services, CPMI process, DLEserver, CPM process
D. Object-Store, Database changes, CPM Process and web-services
Answer: B (LEAVE A REPLY)

NEW QUESTION: 228
What is the main objective when using Application Control?
A. To filter out specific content.
B. To assist the firewall blade with handling traffic.
C. To see what users are doing.
D. Ensure security and privacy of information.
Answer: (SHOW ANSWER)
Explanation
https://digitalguardian.com/blog/what-application-control

NEW QUESTION: 229
The "MAC magic" value must be modified under the following condition:
A. A firewall cluster is configured to use Broadcast for CCP traffic
B. There are more than two members in a firewall cluster
C. There is more than one cluster connected to the same VLAN
D. A firewall cluster is configured to use Multicast for CCP traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Office mode means that:

A. SecurID client assigns a routable MAC address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
B. Users authenticate with an Internet browser and use secure HTTPS connection.
C. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
D. Allows a security gateway to assign a remote client an IP address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
Answer: (SHOW ANSWER)

NEW QUESTION: 231
In which scenario will an administrator need to manually define Proxy ARP?
A. When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
B. When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
C. When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
D. When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.
Answer: C (LEAVE A REPLY)
Explanation
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION: 232
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. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
C. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
D. Go to clash-Run cpstop | Run cpstart
Answer: (SHOW ANSWER)

NEW QUESTION: 233
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. Accelerated Path
B. Slow Path
C. Medium Path

D. Fast Path
Answer: (SHOW ANSWER)

NEW QUESTION: 234
Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?
A. fw tab -t connections -f
B. fw tab -t connections -c
C. fw tab -t connections -s
D. fw tab -t connections
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?
A. /var/opt/CPshrd-R81/conf/local.arp
B. /opt/CPshrd-R81/conf/local.arp
C. $FWDIR/conf/local.arp
D. $CPDIR/conf/local.arp
Answer: (SHOW ANSWER)

NEW QUESTION: 236
Which two of these Check Point Protocols are used by SmartEvent Processes?
A. FWD and CPLOG
B. ELA and CPD
C. FWD and LEA
D. ELA and CPLOG
Answer: (SHOW ANSWER)

NEW QUESTION: 237
Which Check Point software blade provides Application Security and identity control?
A. Identity Awareness
B. Application Control
C. Data Loss Prevention
D. URL Filtering
Answer: (SHOW ANSWER)

NEW QUESTION: 238
Which two Cluster Solutions are available under R81.10?

A. VRRP and IP Clustering
B. ClusterXL and VRitP
C. VRRPandHSRP
D. ClusterXL and NSRP
Answer: (SHOW ANSWER)

NEW QUESTION: 239
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: (SHOW ANSWER)
Explanation
The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.
References:

NEW QUESTION: 240
What is the command switch to specify the Gaia API context?
A. You have to specify it in the YAML file api.yml which is located underneath the /etc directory of the security management server
B. No need to specify a context, since it defaults to the Gaia API context.
C. mgmt_cli --context gaia_api <Command>
D. You have to change to the zsh-Shell which defaults to the Gaia API context.
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Which command gives us a perspective of the number of kernel tables?
A. fw tab -k
B. fw tab -s
C. fw tab -t
D. fw tab -n
Answer: (SHOW ANSWER)

NEW QUESTION: 242
Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:
A. ReverseProxy
B. ReverseProxyCLI
C. ReverseCLIProxy
D. ProxyReverseCLI
Answer: A (LEAVE A REPLY)

NEW QUESTION: 243
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: (SHOW ANSWER)
Explanation
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk50840

NEW QUESTION: 244
According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them Into a temporary directory. Which process is true for receiving these Tiles;
A. FWD
B. FWM
C. RAD
D. CPD
Answer: (SHOW ANSWER)

NEW QUESTION: 245
By default, which port does the WebUI listen on?
A. 4434
B. 8080
C. 443
D. 80
Answer: (SHOW ANSWER)

NEW QUESTION: 246
What is the purpose of extended master key extension/session hash?
A. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
B. Special TCP handshaking extension
C. UDP VOIP protocol extension
D. Supplement DLP data watermark
Answer: (SHOW ANSWER)

NEW QUESTION: 247
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: (SHOW ANSWER)
Explanation
https://sc1.checkpoint.com/documents/R81/CP_R81BC_ThreatPrevention/html_frameset.htm?topic=documents/

NEW QUESTION: 248
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 i
B. Big O
C. Big I
D. Little o
Answer: (SHOW ANSWER)

NEW QUESTION: 249
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: (SHOW ANSWER)
Explanation
Note -
References:

NEW QUESTION: 250
What are the different command sources that allow you to communicate with the API server?
A. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
B. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
C. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
D. API_cli Tool, Gaia CLI, Web Services
Answer: (SHOW ANSWER)

NEW QUESTION: 251
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?
A. SmartConsole
B. None, Security Management Server would be installed by itself.
C. SmartEvent
D. Security Gateway
E. SecureClient
Answer: D (LEAVE A REPLY)

NEW QUESTION: 252
How many policy layers do Access Control policy support?
A. 2
B. 4
C. 1
D. 3
Answer: (SHOW ANSWER)
Explanation
Two policy layers:
- Network Policy Layer
- Application Control Policy Layer

NEW QUESTION: 253
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 installer packages
C. show uninstaller status
D. show installer status
Answer: (SHOW ANSWER)

NEW QUESTION: 254

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:
A. Threat Emulation
B. QOS
C. HTTPS
D. VoIP
Answer: (SHOW ANSWER)

NEW QUESTION: 255
In ClusterXL Load Sharing Multicast Mode:
A. every member of the cluster received all of the packets sent to the cluster IP address
B. only the primary member received packets sent to the cluster IP address
C. only the secondary member receives packets sent to the cluster IP address
D. packets sent to the cluster IP address are distributed equally between all members of the cluster
Answer: (SHOW ANSWER)

NEW QUESTION: 256
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 with negative acknowledgment
C. Dropped without logs and without sending a negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment
Answer: (SHOW ANSWER)

NEW QUESTION: 257
What command can you use to have cpinfo display all installed hotfixes?
A. cpinfo -hf
B. cpinfo -y all
C. cpinfo -get hf
D. cpinfo installed_jumbo
Answer: (SHOW ANSWER)

NEW QUESTION: 258
What is the protocol and port used for Health Check and State Synchronization in ClusterXL?
A. CPC and 8116
B. CCP and 257
C. CCP and 18190
D. CCP and 8116
Answer: (SHOW ANSWER)

NEW QUESTION: 259
When using the Mail Transfer Agent, where are the debug logs stored?
A. $FWDIR/bin/emaild.mta. elg
B. /var/log/mail.mta elg
C. $FWDIR/log/mtad elg
D. $CPDIR/log/emaild elg
Answer: (SHOW ANSWER)