

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

Which statement is true regarding redundancy?

- A. System Administrators know when their cluster has failed over and can also see why it failed over by using the `cphaprob -f` if command.
- B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
- C. Machines in a ClusterXL High Availability configuration must be synchronized.
- D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

Which of the SecureXL templates are enabled by default on Security Gateway?

- A. Accept
- B. Drop
- C. NAT
- D. None

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

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. Application and Client Service
- B. Network and Application
- C. Network and Layers
- D. Virtual Adapter and Mobile App

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.

- A. Inspect/Bypass
- B. Inspect/Prevent
- C. Prevent/Bypass
- D. Detect/Bypass

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

Which command is used to set the CCP protocol to Multicast?

- A. `cphaprob set_ccp multicast`
- B. `cphaconf set_ccp multicast`
- C. `cphaconf set_ccp no_broadcast`
- D. `cphaprob set_ccp no_broadcast`

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

Which features are only supported with R81.10 Gateways but not R77.x?

- A. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
- B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- C. The rule base can be built of layers, each containing a set of the security rule
- D. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- E. Time object to a rule to make the rule active only during specified times.

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

Fill in the blank: The R81 utility `fw monitor` is used to troubleshoot .

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues

D. Phase two key negotiations

Answer: C

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.

NEW QUESTION 8

- (Exam Topic 1)

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

- A. Secure Internal Communication (SIC)
- B. Restart Daemons if they fail
- C. Transfers messages between Firewall processes
- D. Pulls application monitoring status

Answer: D

NEW QUESTION 9

- (Exam Topic 1)

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: D

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.

NEW QUESTION 10

- (Exam Topic 1)

Fill in the blank: The command _____ provides the most complete restoration of a R81 configuration.

- A. upgrade_import
- B. cpconfig
- C. fwm dbimport -p <export file>
- D. cpinfo -recover

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

- A. infoCP
- B. infoview
- C. cpinfo
- D. fw cpinfo

Answer: C

NEW QUESTION 12

- (Exam Topic 1)

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network objects that restricts all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Answer: B

NEW QUESTION 16

- (Exam Topic 1)

What Factor preclude Secure XL Templating?

- A. Source Port Ranges/Encrypted Connections
- B. IPS
- C. ClusterXL in load sharing Mode
- D. CoreXL

Answer: A

NEW QUESTION 17

- (Exam Topic 1)

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Answer: C

NEW QUESTION 21

- (Exam Topic 1)

Advanced Security Checkups can be easily conducted within:

- A. Reports
- B. Advanced
- C. Checkups
- D. Views
- E. Summary

Answer: A

NEW QUESTION 23

- (Exam Topic 1)

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: B

NEW QUESTION 28

- (Exam Topic 1)

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 data. Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

Answer: C

NEW QUESTION 32

- (Exam Topic 1)

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. fwm via fwd
- C. cpm via cpd
- D. fwd via cpd

Answer: A

NEW QUESTION 33

- (Exam Topic 1)

To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

- A. fw ctl multik set_mode 1
- B. fw ctl Dynamic_Priority_Queue on
- C. fw ctl Dynamic_Priority_Queue enable
- D. fw ctl multik set_mode 9

Answer: D

NEW QUESTION 35

- (Exam Topic 1)

Which command shows actual allowed connections in state table?

- A. fw tab -t StateTable
- B. fw tab -t connections
- C. fw tab -t connection
- D. fw tab connections

Answer: B

NEW QUESTION 37

- (Exam Topic 1)

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

- A. R81 Management API
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

Answer: C

NEW QUESTION 42

- (Exam Topic 1)

The Event List within the Event tab contains:

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

Answer: C

NEW QUESTION 47

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 52

- (Exam Topic 1)

Which command lists all tables in Gaia?

- A. fw tab -t
- B. fw tab -list
- C. fw-tab -s
- D. fw tab -1

Answer: C

NEW QUESTION 53

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 55

- (Exam Topic 1)

How many images are included with Check Point TE appliance in Recommended Mode?

- A. 2(OS) images
- B. images are chosen by administrator during installation
- C. as many as licensed for
- D. the most new image

Answer: A

NEW QUESTION 60

- (Exam Topic 1)

What is the correct command to observe the Sync traffic in a VRRP environment?

- A. fw monitor -e "accept[12:4,b]=224.0.0.18;"
- B. fw monitor -e "accept port(6118;"
- C. fw monitor -e "accept proto=mcVRRP;"
- D. fw monitor -e "accept dst=224.0.0.18;"

Answer: D

NEW QUESTION 63

- (Exam Topic 1)

To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 65

- (Exam Topic 1)

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, Source port, Destination port
- D. Source address, Destination address, Destination port, Protocol

Answer: A

NEW QUESTION 70

- (Exam Topic 2)

Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

- A. cphaprob stat
- B. cphaprob -a if
- C. cphaprob -l list
- D. cphaprob all show stat

Answer: D

NEW QUESTION 73

- (Exam Topic 2)

What are the blades of Threat Prevention?

- A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
- B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
- C. IPS, AntiVirus, AntiBot
- D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Answer: D

NEW QUESTION 77

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 80

- (Exam Topic 2)

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
- B. Threat Extraction always delivers a file and takes less than a second to complete.
- C. Threat Emulation never delivers a file that takes less than a second to complete.
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete.

Answer: B

NEW QUESTION 82

- (Exam Topic 2)

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 fw accel stat command on the gateway.
- B. He can use the fw accel statistics command on the gateway.
- C. He can use the fwaccel stat command on the Security Management Server.
- D. He can use the fwaccel stat command on the gateway

Answer: D

NEW QUESTION 84

- (Exam Topic 2)

Which of the following describes how Threat Extraction functions?

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

Answer: B

NEW QUESTION 86

- (Exam Topic 2)

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

- A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
- B. Full Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
- C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
- D. You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 88

- (Exam Topic 2)

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. cphaprob -f register
- B. cphaprob -d -s report
- C. cpstat -f all
- D. cphaprob -a list

Answer: D

NEW QUESTION 90

- (Exam Topic 2)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 93

- (Exam Topic 2)

You are investigating issues with two gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

- A. TCP port 443
- B. TCP port 257
- C. TCP port 256
- D. UDP port 8116

Answer: C

NEW QUESTION 94

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 99

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 104

- (Exam Topic 2)

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

- A. Collision
- B. Down
- C. Lagging
- D. Never been synchronized

Answer: B

NEW QUESTION 108

- (Exam Topic 2)

How often does Threat Emulation download packages by default?

- A. Once a week
- B. Once an hour
- C. Twice per day
- D. Once per day

Answer: D

NEW QUESTION 109

- (Exam Topic 2)

What is the name of the secure application for Mail/Calendar for mobile devices?

- A. Capsule Workspace
- B. Capsule Mail
- C. Capsule VPN
- D. Secure Workspace

Answer: A

NEW QUESTION 113

- (Exam Topic 2)

In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _____ will not apply.

- A. ffff
- B. 1
- C. 2
- D. 3

Answer: B

NEW QUESTION 115

- (Exam Topic 2)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: B

NEW QUESTION 118

- (Exam Topic 2)

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

- A. Capsule Docs

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

Answer: C

NEW QUESTION 120

- (Exam Topic 2)

Which command shows detailed information about VPN tunnels?

- A. cat \$FWDIR/conf/vpn.conf
- B. vpn tu tlist
- C. vpn tu
- D. cpview

Answer: B

NEW QUESTION 121

- (Exam Topic 2)

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: B

NEW QUESTION 126

- (Exam Topic 2)

What is mandatory for ClusterXL to work properly?

- A. The number of cores must be the same on every participating cluster node
- B. The Magic MAC number must be unique per cluster node
- C. The Sync interface must not have an IP address configured
- D. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members

Answer: B

NEW QUESTION 128

- (Exam Topic 2)

What is the purpose of Priority Delta in VRRP?

- A. When a box up, Effective Priority = Priority + Priority Delta
- B. When an Interface is up, Effective Priority = Priority + Priority Delta
- C. When an Interface fail, Effective Priority = Priority – Priority Delta
- D. When a box fail, Effective Priority = Priority – Priority Delta

Answer: C

Explanation:

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will begin to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP. References:

NEW QUESTION 131

- (Exam Topic 2)

Which one of the following is true about Threat Extraction?

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

Answer: A

NEW QUESTION 132

- (Exam Topic 2)

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

Answer: A

NEW QUESTION 133

- (Exam Topic 2)

When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

- A. IP
- B. SIC
- C. NAT
- D. FQDN

Answer: C

NEW QUESTION 136

- (Exam Topic 2)

What is the command to check the status of the SmartEvent Correlation Unit?

- A. fw ctl get int cpsead_stat
- B. cpstat cpsead
- C. fw ctl stat cpsemd
- D. cp_conf get_stat cpsemd

Answer: B

NEW QUESTION 138

- (Exam Topic 2)

Where do you create and modify the Mobile Access policy in R81?

- A. SmartConsole
- B. SmartMonitor
- C. SmartEndpoint
- D. SmartDashboard

Answer: A

NEW QUESTION 140

- (Exam Topic 2)

What is considered Hybrid Emulation Mode?

- A. Manual configuration of file types on emulation location.
- B. Load sharing of emulation between an on premise appliance and the cloud.
- C. Load sharing between OS behavior and CPU Level emulation.
- D. High availability between the local SandBlast appliance and the cloud.

Answer: B

NEW QUESTION 144

- (Exam Topic 2)

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resilient VPN client.
- B. SSL VPN requires installation of a resident VPN client.
- C. SSL VPN and IPSec VPN are the same.
- D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser.

Answer: D

NEW QUESTION 148

- (Exam Topic 2)

When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20GB
- D. At least 20GB

Answer: D

NEW QUESTION 151

- (Exam Topic 2)

What is the benefit of "fw monitor" over "tcpdump"?

- A. "fw monitor" reveals Layer 2 information, while "tcpdump" acts at Layer 3.
- B. "fw monitor" is also available for 64-Bit operating systems.
- C. With "fw monitor", you can see the inspection points, which cannot be seen in "tcpdump"

D. "fw monitor" can be used from the CLI of the Management Server to collect information from multiple gateways.

Answer: C

NEW QUESTION 155

- (Exam Topic 2)

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

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

Answer: A

NEW QUESTION 160

- (Exam Topic 2)

Which one of the following is true about Threat Emulation?

- A. Takes less than a second to complete
- B. Works on MS Office and PDF files only
- C. Always delivers a file
- D. Takes minutes to complete (less than 3 minutes)

Answer: D

NEW QUESTION 164

- (Exam Topic 2)

Which command gives us a perspective of the number of kernel tables?

- A. fw tab -t
- B. fw tab -s
- C. fw tab -n
- D. fw tab -k

Answer: B

NEW QUESTION 165

- (Exam Topic 2)

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 170

- (Exam Topic 2)

The following command is used to verify the CPUSE version:

- A. HostName:0>show installer status build
- B. [Expert@HostName:0]#show installer status
- C. [Expert@HostName:0]#show installer status build
- D. HostName:0>show installer build

Answer: A

NEW QUESTION 174

- (Exam Topic 3)

What cloud-based SandBlast Mobile application is used to register new devices and users?

- A. Check Point Protect Application
- B. Management Dashboard
- C. Behavior Risk Engine
- D. Check Point Gateway

Answer: D

NEW QUESTION 178

- (Exam Topic 3)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 182

- (Exam Topic 3)

Which is NOT a SmartEvent component?

- A. SmartEvent Server
- B. Correlation Unit
- C. Log Consolidator
- D. Log Server

Answer: C

NEW QUESTION 187

- (Exam Topic 3)

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 source machine must be at least 25% of the size of the /var/log directory on the target machine
- B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
- C. Size of the \$FWDIR/log folder of the target machine must be at least 30% of the size of the \$FWDIR/log directory on the source machine
- D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B

NEW QUESTION 189

- (Exam Topic 3)

Please choose the path to monitor the compliance status of the Check Point R81.10 based management.

- A. Gateways & Servers --> Compliance View
- B. Compliance blade not available under R81.10
- C. Logs & Monitor --> New Tab --> Open compliance View
- D. Security & Policies --> New Tab --> Compliance View

Answer: C

NEW QUESTION 192

- (Exam Topic 3)

What will SmartEvent automatically define as events?

- A. Firewall
- B. VPN
- C. IPS
- D. HTTPS

Answer: C

NEW QUESTION 196

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 199

- (Exam Topic 3)

The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

- A. ccp
- B. cphaconf
- C. cphad
- D. cphastart

Answer: A

NEW QUESTION 204

- (Exam Topic 3)
How many policy layers do Access Control policy support?

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

Answer: A

Explanation:

Two policy layers:
- Network Policy Layer
- Application Control Policy Layer

NEW QUESTION 207

- (Exam Topic 3)
What is the Implicit Clean-up Rule?

- A. A setting is defined in the Global Properties for all policies.
- B. A setting that is configured per Policy Layer.
- C. Another name for the Clean-up Rule.
- D. Automatically created when the Clean-up Rule is defined.

Answer: C

NEW QUESTION 211

- (Exam Topic 3)
What is true of the API server on R81.10?

- A. By default the API-server is activated and does not have hardware requirements.
- B. By default the API-server is not active and should be activated from the WebUI.
- C. By default the API server is active on management and stand-alone servers with 16GB of RAM (or more).
- D. By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more).

Answer: D

NEW QUESTION 214

- (Exam Topic 3)
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. 3
- B. 2
- C. 1
- D. 4

Answer: D

NEW QUESTION 216

- (Exam Topic 3)
Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

- A. The CoreXL FW instances assignment mechanism is based on Source MAC addresses, Destination MAC addresses
- B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
- C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
- D. The CoreXL FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type

Answer: B

NEW QUESTION 219

- (Exam Topic 3)
GAiA Software update packages can be imported and installed offline in situation where:

- A. Security Gateway with GAiA does NOT have SFTP access to Internet
- B. Security Gateway with GAiA does NOT have access to Internet.
- C. Security Gateway with GAiA does NOT have SSH access to Internet.
- D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 220

- (Exam Topic 3)
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting

- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 222

- (Exam Topic 3)

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. /opt/CPshrd-R81/conf/local.arp
- B. /var/opt/CPshrd-R81/conf/local.arp
- C. \$CPDIR/conf/local.arp
- D. \$FWDIR/conf/local.arp

Answer: D

NEW QUESTION 223

- (Exam Topic 3)

What command would show the API server status?

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

Answer: C

NEW QUESTION 228

- (Exam Topic 3)

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

- A. Three; security management, Security Gateway, and endpoint security
- B. Three; Security Gateway, endpoint security, and gateway management
- C. Two; security management and endpoint security
- D. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 230

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 233

- (Exam Topic 3)

In which formats can Threat Emulation forensics reports be viewed in?

- A. TXT, XML and CSV
- B. PDF and TXT
- C. PDF, HTML, and XML
- D. PDF and HTML

Answer: C

NEW QUESTION 234

- (Exam Topic 3)

SandBlast agent extends 0 day prevention to what part of the network?

- A. Web Browsers and user devices
- B. DMZ server
- C. Cloud
- D. Email servers

Answer: A

NEW QUESTION 239

- (Exam Topic 3)

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: B

NEW QUESTION 243

- (Exam Topic 3)

What CLI command compiles and installs a Security Policy on the target's Security Gateways?

- A. fwm compile
- B. fwm load
- C. fwm fetch
- D. fwm install

Answer: B

NEW QUESTION 246

- (Exam Topic 3)

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: B

NEW QUESTION 250

- (Exam Topic 3)

After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
- B. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0 0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0 0.0.0.0 gw 192.168.80.1 onsave config
- D. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 252

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

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

Answer: D

NEW QUESTION 257

- (Exam Topic 3)

What is the SandBlast Agent designed to do?

- A. Performs OS-level sandboxing for SandBlast Cloud architecture
- B. Ensure the Check Point SandBlast services is running on the end user's system
- C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
- D. Clean up email sent with malicious attachments

Answer: C

NEW QUESTION 261

- (Exam Topic 3)

When using CPSTAT, what is the default port used by the AMON server?

- A. 18191
- B. 18192
- C. 18194
- D. 18190

Answer: B

NEW QUESTION 263

- (Exam Topic 3)

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

What is the most likely reason that the traffic is not accelerated?

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

Answer: B

NEW QUESTION 266

- (Exam Topic 3)

SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:

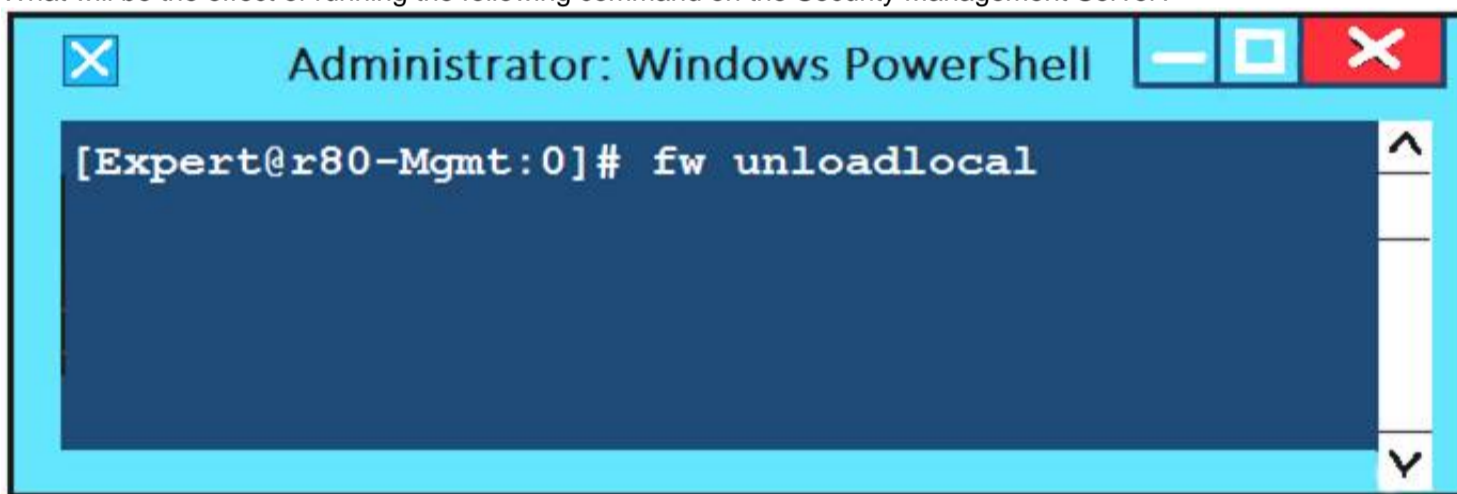
- A. ping, traceroute, netstat, and route
- B. ping, nslookup, Telnet, and route
- C. ping, whois, nslookup, and Telnet
- D. ping, traceroute, netstat, and nslookup

Answer: C

NEW QUESTION 267

- (Exam Topic 3)

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



- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

Answer: A

NEW QUESTION 272

- (Exam Topic 3)

Which path below is available only when CoreXL is enabled?

- A. Slow path
- B. Firewall path
- C. Medium path
- D. Accelerated path

Answer: C

NEW QUESTION 274

- (Exam Topic 3)

For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

- A. 20 minutes
- B. 15 minutes
- C. Admin account cannot be unlocked automatically
- D. 30 minutes at least

Answer: D

NEW QUESTION 279

- (Exam Topic 3)

What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

- A. Lagging
- B. Synchronized
- C. Never been synchronized
- D. Collision

Answer: B

NEW QUESTION 281

- (Exam Topic 3)

Which of the following is NOT an alert option?

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

Answer: B

NEW QUESTION 283

- (Exam Topic 3)

What are the methods of SandBlast Threat Emulation deployment?

- A. Cloud, Appliance and Private
- B. Cloud, Appliance and Hybrid
- C. Cloud, Smart-1 and Hybrid
- D. Cloud, OpenServer and Vmware

Answer: A

NEW QUESTION 287

- (Exam Topic 4)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

NEW QUESTION 291

- (Exam Topic 4)

Firewall polices must be configured to accept VRRP packets on the GAiA platform if it Firewall software. The Multicast destination assigned by the internet Assigned Number Authority (IANA) for VRRP is:

- A. 224.0.0.18
- B. 224 00 5
- C. 224.0.0.102
- D. 224.0.0.22

Answer: A

NEW QUESTION 296

- (Exam Topic 4)

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. Certificate's Fingerprint
- B. Random Pool
- C. CA Authority
- D. Certificate Authority

Answer: D

NEW QUESTION 301

- (Exam Topic 4)

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 304

- (Exam Topic 4)

After finishing installation admin John likes to use top command in expert mode. John has to set the expert-password and was able to use top command. A week later John has to use the top command again, He detected that the expert password is no longer valid. What is the most probable reason for this behavior?

- A. "write memory" was not issued on clish
- B. changes are only possible via SmartConsole
- C. "save config" was not issued in expert mode
- D. "save config" was not issued on clish

Answer: D

NEW QUESTION 309

- (Exam Topic 4)

There are multiple types of licenses for the various VPN components and types. License type related to management and functioning of Remote Access VPNs are - which of the following license requirement statement is NOT true:

- A. MobileAccessLicense ° This license is required on the Security Gateway for the following Remote Access solutions
- B. EndpointPolicyManagementLicense ° The Endpoint Security Suite includes blades other than the Remote Access VPN, hence this license is required to manage the suite
- C. EndpointContainerLicense ° The Endpoint Software Blade Licenses does not require an Endpoint Container License as the base
- D. IPSecVPNLicense • This license is installed on the VPN Gateway and is a basic requirement for a Remote Access VPN solution

Answer: C

NEW QUESTION 313

- (Exam Topic 4)

What is the SOLR database for?

- A. Used for full text search and enables powerful matching capabilities
- B. Writes data to the database and full text search
- C. Serves GUI responsible to transfer request to the DLE server
- D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 316

- (Exam Topic 4)

When using the Mail Transfer Agent, where are the debug logs stored?

- A. \$FWDIR/bin/emaild.mt
- B. elg
- C. \$FWDIR/log/mtad elg
- D. /var/log/mail.mta elg
- E. \$CPDIR/log/emaild elg

Answer: C

NEW QUESTION 318

- (Exam Topic 4)

Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

- A. Check Point Security Management HA (Secondary): set cluster member mvc on
- B. Check Point Security Gateway Only: set cluster member mvc on
- C. Check Point Security Management HA (Primary): set cluster member mvc on
- D. Check Point Security Gateway Cluster Member: set cluster member mvc on

Answer: D

NEW QUESTION 320

- (Exam Topic 4)

How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?

- A. By dropping traffic from websites identified through ThreatCloud Verification and URL Caching
- B. By dropping traffic that is not proven to be from clean websites in the URL Filtering blade
- C. By allowing traffic from websites that are known to run Antivirus Software on servers regularly
- D. By matching logs against ThreatCloud information about the reputation of the website

Answer: D

NEW QUESTION 322

- (Exam Topic 4)

What are the services used for Cluster Synchronization?

- A. 256H-CP for 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: C

NEW QUESTION 327

- (Exam Topic 4)

True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.

- A. True, CLI is the prefer method for Licensing
- B. False, Central License are handled via Security Management Server
- C. False, Central Licenses are installed via Gaia on Security Gateways
- D. True, Central License can be installed with CPLIC command on a Security Gateway

Answer: D

NEW QUESTION 330

- (Exam Topic 4)

What a valid SecureXL paths in R81.10?

- A. F2F (Slow path). Templated Pat
- B. PQX and F2V
- C. F2F (Slow path). PXL, QXL and F2V
- D. F2F (Slow path), Accelerated Path, PQX and F2V
- E. F2F (Slow path), Accelerated Path, Medium Path and F2V

Answer: D

NEW QUESTION 332

- (Exam Topic 4)

Alice & Bob are concurrently logged In via SSH on the same Check Point Security Gateway as user "admin" however Bob was first logged in and acquired the lock Alice is not aware that Bob is also logged in to the same Security Management Server as she is but she needs to perform very urgent configuration changes - which of the following GAIACLISH command is true for overriding Bobs configuration database lock:

- A. lock database override
- B. unlock override database
- C. unlock database override
- D. database unlock override

Answer: A

NEW QUESTION 336

- (Exam Topic 4)

Choose the correct syntax to add a new host named "emailserver1" with IP address 10.50.23.90 using GAIa Management CLI?

- A. mgmt_cli add host name "myHost12 ip" address 10.50.23.90
- B. mgmt_cli add host name ip-address 10.50.23.90
- C. mgmt_cli add host "emailserver1" address 10.50.23.90
- D. mgmt_cli add host name "emailserver1" ip-address 10.50.23.90

Answer: D

Explanation:

Reference: <https://weekly-geekly.github.io/articles/339924/index.html>

NEW QUESTION 341

- (Exam Topic 4)

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

- A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
- B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
- C. Size of the \$FWDIR/log folder of the target machine must be at least 30% of the size of the \$FWDIR/log directory on the source machine
- D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/90083

NEW QUESTION 345

- (Exam Topic 4)

What command is used to manually failover a Multi-Version Cluster during the upgrade?

- A. clusterXL_admin down in Expert Mode
- B. clusterXL_admin down in Clish
- C. set cluster member state down in Clish
- D. set cluster down in Expert Mode

Answer: B

NEW QUESTION 346

- (Exam Topic 4)

What is required for a site-to-site VPN tunnel that does not use certificates?

- A. Pre-Shared Secret
- B. RSA Token
- C. Unique Passwords
- D. SecureID

Answer: A

NEW QUESTION 349

- (Exam Topic 4)

What is a possible command to delete all of the SSH connections of a gateway?

- A. fw sam -l dport 22
- B. fw ctl conntab -x -dpott=22
- C. fw tab -t connections -x -e 00000016
- D. fwaccel dos config set dport ssh

Answer: A

NEW QUESTION 351

- (Exam Topic 4)

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

- A. ffffffff
- B. 00000001
- C. 00000002
- D. 00000003

Answer: B

NEW QUESTION 356

- (Exam Topic 4)

You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?

- A. In CLISH run: set interface eth2 mac-addr 11:11:11:11:11:11
- B. In expert-mode run ifconfig eth1 hw 11:11:11:11 11 11
- C. In CLISH run set interface eth2 hw-addr 11 11 11:11:11 11
- D. In expert-mode run: ethtool -4 eth2 mac 11 11:11:11:11:11

Answer: A

NEW QUESTION 359

- (Exam Topic 4)

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 363

- (Exam Topic 4)

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Run cprestart from clish
- B. After upgrading the hardware, increase the number of kernel instances using cpconfig
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores

E. Hyperthreading must be enabled in the bios to use CoreXL

Answer: B

NEW QUESTION 368

- (Exam Topic 4)

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: B

NEW QUESTION 371

- (Exam Topic 4)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 375

- (Exam Topic 4)

On R81.10 the IPS Blade is managed by:

- A. Threat Protection policy
- B. Anti-Bot Blade
- C. Threat Prevention policy
- D. Layers on Firewall policy

Answer: C

NEW QUESTION 377

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

- A. 18191
- B. 18190
- C. 8983
- D. 19009

Answer: D

NEW QUESTION 379

- (Exam Topic 4)

Which of the following statements about SecureXL NAT Templates is true?

- A. NAT Templates are generated to achieve high session rate for NA
- B. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- C. These are enabled by default and work only if Accept Templates are enabled.
- D. DROP Templates are generated to achieve high session rate for NA
- E. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- F. These are disabled by default and work only if NAT Templates are disabled.
- G. NAT Templates are generated to achieve high session rate for NA
- H. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- I. These are disabled by default and work only if Accept Templates are disabled.
- J. ACCEPT Templates are generated to achieve high session rate for NA
- K. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase looku
- L. These are disabled by default and work only if NAT Templates are disabled.

Answer: A

NEW QUESTION 381

- (Exam Topic 4)

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

- A. Accept; redirect

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

Answer: D

NEW QUESTION 383

- (Exam Topic 4)

Which of the following is NOT supported by CPUSE?

- A. Automatic download of full installation and upgrade packages
- B. Automatic download of hotfixes
- C. Installation of private hotfixes
- D. Offline installations

Answer: D

Explanation:

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

NEW QUESTION 387

- (Exam Topic 4)

If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

- A. Nothing - the proxy ARP is automatically handled in the R81 version
- B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
- C. Add the proxy ARP configurations in a file called \$FWDIR/conf/local.arp
- D. Add the proxy ARP configurations in a file called \$CPDIR/conf/local.arp

Answer: D

NEW QUESTION 389

- (Exam Topic 4)

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

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

Answer: B

NEW QUESTION 390

- (Exam Topic 4)

Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

- A. cpm
- B. fwd
- C. cpd
- D. fwmD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: D

NEW QUESTION 391

- (Exam Topic 4)

Which command is used to obtain the configuration lock in Gaia?

- A. Lock database override
- B. Unlock database override
- C. Unlock database lock
- D. Lock database user

Answer: A

Explanation:

Obtaining a Configuration Lock

NEW QUESTION 396

- (Exam Topic 4)

What are the two high availability modes?

- A. Load Sharing and Legacy

- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION 399

- (Exam Topic 4)

When users connect to the Mobile Access portal they are unable to open File Shares. Which log file would you want to examine?

- A. cvpnd.elg
- B. httpd.elg
- C. vpnd.elg
- D. fw.elg

Answer: A

NEW QUESTION 404

- (Exam Topic 4)

When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

- A. Syslog
- B. SNMPTrap
- C. Block Source
- D. Mail

Answer: B

NEW QUESTION 408

- (Exam Topic 4)

What is the default shell for the command line interface?

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

Answer: B

Explanation:

The default shell of the CLI is called clish References:

NEW QUESTION 409

- (Exam Topic 4)

What is the purpose of the CPCA process?

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

Answer: D

NEW QUESTION 412

- (Exam Topic 4)

What Is the difference between Updatable Objects and Dynamic Objects

- A. Dynamic Objects ate maintained automatically by the Threat Clou
- B. Updatable Objects are created and maintained locall
- C. In both cases there is no need to install policy for the changes to take effect.
- D. Updatable Objects is a Threat Cloud Servic
- E. The provided Objects are updated automaticall
- F. Dynamic Objects are created and maintained locally For Dynamic Objectsthere is no need to install policy for the changes to take effect.
- G. Updatable Objects is a Threat Cloud Servic
- H. The provided Objects are updated automaticall
- I. Dynamic Objects are created and maintained locally In both cases there is noneed to install policy for the changes to take effect.
- J. Dynamic Objects are maintained automatically by the Threat Clou
- K. For Dynamic Objects there rs no need to install policy for the changes to take effec
- L. Updatable Objects are created and maintained locally.

Answer: B

NEW QUESTION 416

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 417

- (Exam Topic 4)

When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

- A. Network, and defining your Class A space
- B. Topology, and you are defining the Internal network
- C. Internal addresses you are defining the gateways
- D. Internal network(s) you are defining your networks

Answer: D

NEW QUESTION 421

- (Exam Topic 4)

How many users can have read/write access in Gaia at one time?

- A. Infinite
- B. One
- C. Three
- D. Two

Answer: B

NEW QUESTION 422

- (Exam Topic 4)

When performing a minimal effort upgrade, what will happen to the network traffic?

- A. All connections that were initiated before the upgrade will be dropped, causing network downtime
- B. All connections that were initiated before the upgrade will be handled normally
- C. All connections that were initiated before the upgrade will be handled by the standby gateway
- D. All connections that were initiated before the upgrade will be handled by the active gateway

Answer: A

NEW QUESTION 427

- (Exam Topic 4)

What is the benefit of Manual NAT over Automatic NAT?

- A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy.
- B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
- C. You have the full control about the priority of the NAT rules
- D. On IPSO and GAIA Gateways, it is handled in a stateful manner

Answer: C

NEW QUESTION 430

- (Exam Topic 4)

Besides fw monitor, what is another command that can be used to capture packets?

- A. arp
- B. traceroute
- C. tcpdump
- D. ping

Answer: C

NEW QUESTION 434

- (Exam Topic 4)

Which software blade does NOT accompany the Threat Prevention policy?

- A. Anti-virus
- B. IPS
- C. Threat Emulation
- D. Application Control and URL Filtering

Answer: D

NEW QUESTION 436

- (Exam Topic 4)

Which of the following is a task of the CPD process?

- A. Invoke and monitor critical processes and attempts to restart them if they fail
- B. Transfers messages between Firewall processes
- C. Log forwarding
- D. Responsible for processing most traffic on a security gateway

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

NEW QUESTION 441

- (Exam Topic 4)

What component of Management is used for indexing?

- A. DBSync
- B. API Server
- C. fwm
- D. SOLR

Answer: D

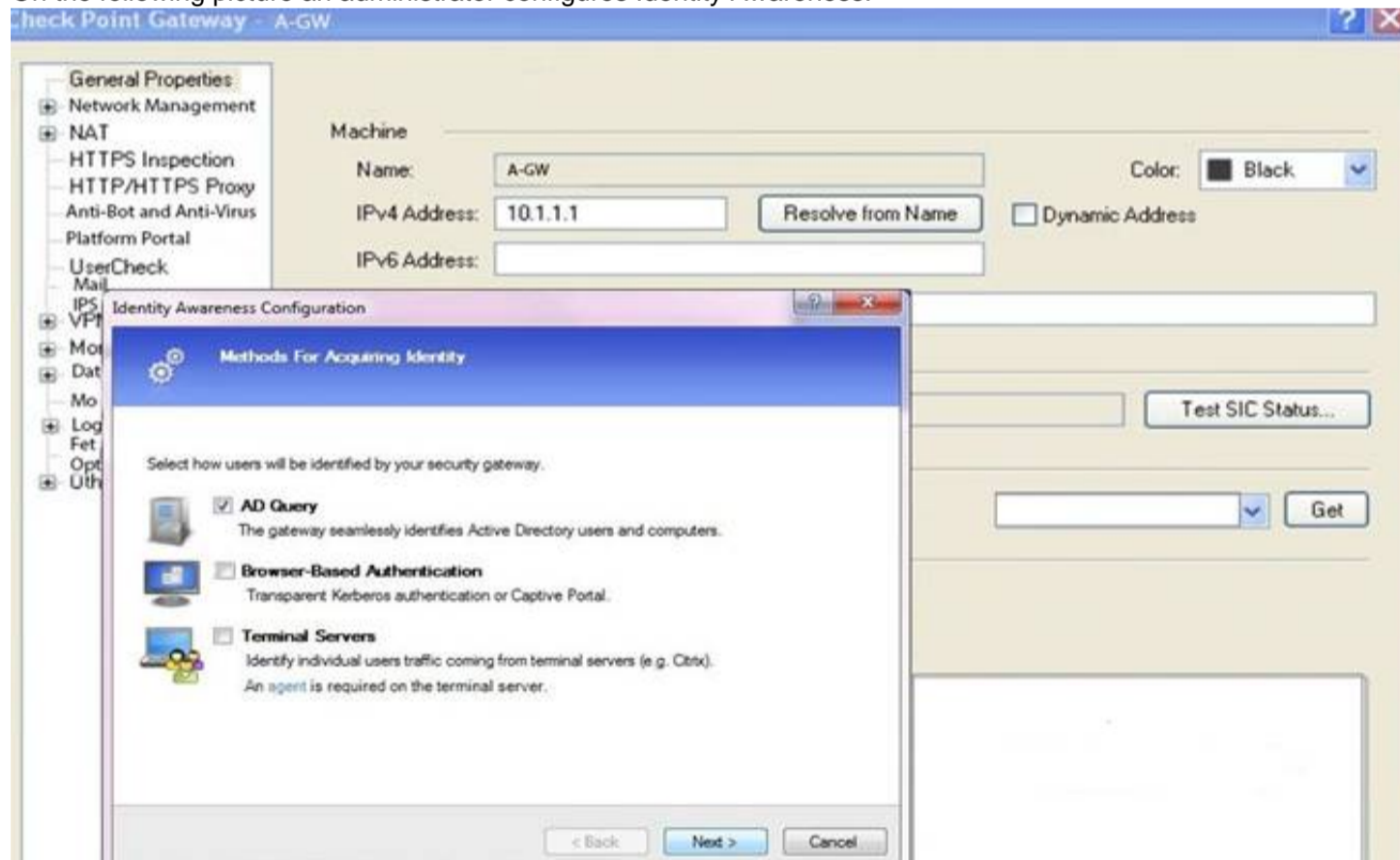
Explanation:

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Multi-DomainSecurityManag

NEW QUESTION 446

- (Exam Topic 4)

On the following picture an administrator configures Identity Awareness:



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

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
- C. Obligatory usage of Captive Portal.
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: B

NEW QUESTION 447

- (Exam Topic 4)

What destination versions are supported for a Multi-Version Cluster Upgrade?

- A. R81.40 and later
- B. R76 and later
- C. R70 and Later
- D. R81.10 and Later

Answer: D

NEW QUESTION 448

- (Exam Topic 4)

Which of the following is NOT an attribute of packet acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. VLAN Tag

Answer: D

NEW QUESTION 452

- (Exam Topic 4)

What does Backward Compatibility mean upgrading the Management Server and how can you check it?

- A. The Management Server is able to manage older Gateway
- B. The lowest supported version is documented in the Installation and Upgrade Guide
- C. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes
- D. You will be able to connect to older Management Server with the SmartConsol
- E. The lowest supported version is documented in the Installation and Upgrade Guide
- F. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes

Answer: A

NEW QUESTION 457

- (Exam Topic 4)

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. DASSERVICE
- B. FWD
- C. CPVIEWD
- D. CPD

Answer: A

NEW QUESTION 462

- (Exam Topic 4)

You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

- A. fw unloadlocal
- B. fw unloadpolicy
- C. fwm unload local
- D. fwm unload policy

Answer: A

NEW QUESTION 464

- (Exam Topic 4)

After verifying that API Server is not running, how can you start the API Server?

- A. Run command "set api start" in CLISH mode
- B. Run command "mgmt cli set api start" in Expert mode
- C. Run command "mgmt api start" in CLISH mode
- D. Run command "api start" in Expert mode

Answer: B

NEW QUESTION 467

- (Exam Topic 4)

When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

- A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
- B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
- C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
- D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 472

- (Exam Topic 4)

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 loa
- B. 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'

- D. The interface must support Multi-Queue
- E. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
- F. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND'
- G. The interface must support Multi-Queue
- H. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
- I. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current loa
- J. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

Answer: D

NEW QUESTION 476

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 480

- (Exam Topic 4)

What is the amount of Priority Queues by default?

- A. There are 8 priority queues and this number cannot be changed.
- B. There is no distinct number of queues since it will be changed in a regular basis based on its system requirements.
- C. There are 7 priority queues by default and this number cannot be changed.
- D. There are 8 priority queues by default, and up to 8 additional queues can be manually configured

Answer: D

NEW QUESTION 482

- (Exam Topic 4)

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: B

NEW QUESTION 486

- (Exam Topic 4)

SmartEvent uses it's event policy to identify events. How can this be customized?

- A. By modifying the firewall rulebase
- B. By creating event candidates
- C. By matching logs against exclusions
- D. By matching logs against event rules

Answer: D

NEW QUESTION 488

- (Exam Topic 4)

How many interfaces can you configure to use the Multi-Queue feature?

- A. 10 interfaces
- B. 3 interfaces
- C. 4 interfaces
- D. 5 interfaces

Answer: D

NEW QUESTION 493

- (Exam Topic 4)

The "MAC magic" value must be modified under the following condition:

- A. There is more than one cluster connected to the same VLAN
- B. A firewall cluster is configured to use Multicast for CCP traffic
- C. There are more than two members in a firewall cluster
- D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

NEW QUESTION 495

- (Exam Topic 4)

Fill in the blank: _____ information is included in "Full Log" tracking option, but is not included in "Log" tracking option?

- A. Destination port
- B. Data type
- C. File attributes
- D. Application

Answer: B

NEW QUESTION 500

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 501

- (Exam Topic 4)

Which command shows the current Security Gateway Firewall chain?

- A. show current chain
- B. show firewall chain
- C. fw ctl chain
- D. fw ctl firewall-chain

Answer: C

NEW QUESTION 503

- (Exam Topic 4)

Which one of the following is NOT a configurable Compliance Regulation?

- A. GLBA
- B. CJIS
- C. SOCI
- D. NCIPA

Answer: C

NEW QUESTION 505

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

156-315.81 Practice Exam Features:

- * 156-315.81 Questions and Answers Updated Frequently
- * 156-315.81 Practice Questions Verified by Expert Senior Certified Staff
- * 156-315.81 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 156-315.81 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-315.81 Practice Test Here](#)