

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

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

Answer: A

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)

How can SmartView application accessed?

- A. `http://<Security Management IP Address>/smartview`
- B. `http://<Security Management IP Address>:4434/smartview/`
- C. `https://<Security Management IP Address>/smartview/`
- D. `https://<Security Management host name>:4434/smartview/`

Answer: C

NEW QUESTION 4

- (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 5

- (Exam Topic 1)

In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

- A. `fw ctl sdstat`
- B. `fw ctl affinity -l -a -r -v`
- C. `fw ctl multik stat`
- D. `cpinfo`

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

- A. `fw ctl multik dynamic_dispatching on`
- B. `fw ctl multik dynamic_dispatching set_mode 9`
- C. `fw ctl multik set_mode 9`
- D. `fw ctl multik pq enable`

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

- A. SmartEvent Client Info
- B. SecuRemote
- C. Check Point Protect
- D. Check Point Capsule Cloud

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

Which CLI command will reset the IPS pattern matcher statistics?

- A. ips reset pmstat
- B. ips pstats reset
- C. ips pmstats refresh
- D. ips pmstats reset

Answer: D

NEW QUESTION 9

- (Exam Topic 1)

Which command can you use to verify the number of active concurrent connections?

- A. fw conn all
- B. fw ctl pstat
- C. show all connections
- D. show connections

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

Which TCP-port does CPM process listen to?

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

Answer: D

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)

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 15

- (Exam Topic 1)

Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?

- A. Severity
- B. Automatic reactions
- C. Policy
- D. Threshold

Answer: C

NEW QUESTION 20

- (Exam Topic 1)

Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 23

- (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 28

- (Exam Topic 1)

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 protection mechanism which starts a counter-attack against known Command & Control Centers
- C. Anti-Bot is the only signature-based method of malware protection.
- D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Answer: D

NEW QUESTION 31

- (Exam Topic 1)

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

Explanation:

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

NEW QUESTION 34

- (Exam Topic 1)

Which command would disable a Cluster Member permanently?

- A. clusterXL_admin down
- B. cphaprob_admin down
- C. clusterXL_admin down-p
- D. set clusterXL down-p

Answer: C

NEW QUESTION 38

- (Exam Topic 1)

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: D

NEW QUESTION 42

- (Exam Topic 1)

Connections to the Check Point R81 Web API use what protocol?

- A. HTTPS
- B. RPC
- C. VPN
- D. SIC

Answer: A

NEW QUESTION 44

- (Exam Topic 1)

What is not a component of Check Point SandBlast?

- A. Threat Emulation
- B. Threat Simulator
- C. Threat Extraction
- D. Threat Cloud

Answer: B

NEW QUESTION 46

- (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 -l

Answer: C

NEW QUESTION 50

- (Exam Topic 1)

What is the difference between an event and a log?

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

Answer: B

NEW QUESTION 51

- (Exam Topic 1)

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 I
- B. Little o
- C. Little i
- D. Big O

Answer: A

NEW QUESTION 54

- (Exam Topic 1)

R81.10 management server can manage gateways with which versions installed?

- A. Versions R77 and higher
- B. Versions R76 and higher
- C. Versions R75.20 and higher
- D. Versions R75 and higher

Answer: C

NEW QUESTION 59

- (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 62

- (Exam Topic 1)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application

- C. Typing API commands using Gaia's secure shell(clish)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 67

- (Exam Topic 1)

In R81 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

Answer: D

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.

NEW QUESTION 70

- (Exam Topic 1)

You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore_backup
- B. import backup
- C. cp_merge
- D. migrate import

Answer: D

NEW QUESTION 71

- (Exam Topic 1)

What is true about VRRP implementations?

- A. VRRP membership is enabled in cpconfig
- B. VRRP can be used together with ClusterXL, but with degraded performance
- C. You cannot have a standalone deployment
- D. You cannot have different VRIDs in the same physical network

Answer: C

NEW QUESTION 72

- (Exam Topic 1)

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

- A. MySQL
- B. Postgres SQL
- C. MarisDB
- D. SOLR

Answer: B

NEW QUESTION 74

- (Exam Topic 2)

Which of these is an implicit MEP option?

- A. Primary-backup
- B. Source address based
- C. Round robin
- D. Load Sharing

Answer: A

NEW QUESTION 78

- (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 83

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 85

- (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 88

- (Exam Topic 2)

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: D

Explanation:

Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that require direct GUI access, such as SmartEvent, It provides the following:

- GUI Client communication
- Database manipulation
- Policy Compilation
- Management HA sync

NEW QUESTION 91

- (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 93

- (Exam Topic 2)

You need to see which hotfixes are installed on your gateway, which command would you use?

- A. cpinfo -h all
- B. cpinfo -o hotfix
- C. cpinfo -l hotfix
- D. cpinfo -y all

Answer: D

NEW QUESTION 95

- (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. Fill Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
- C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
- D. You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 98

- (Exam Topic 2)

Which of the following will NOT affect acceleration?

- A. Connections destined to or originated from the Security gateway
- B. A 5-tuple match
- C. Multicast packets
- D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

Answer: B

NEW QUESTION 100

- (Exam Topic 2)

What is the purpose of a SmartEvent Correlation Unit?

- A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
- B. The SmartEvent Correlation Unit's task is to assign severity levels to the identified events.
- C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
- D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

Answer: C

NEW QUESTION 103

- (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 105

- (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 106

- (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 108

- (Exam Topic 2)

What information is NOT collected from a Security Gateway in a Cpinfo?

- A. Firewall logs
- B. Configuration and database files
- C. System message logs
- D. OS and network statistics

Answer: A

NEW QUESTION 111

- (Exam Topic 2)

What is the purpose of extended master key extension/session hash?

- A. UDP VOIP protocol extension
- B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
- C. Special TCP handshaking extension
- D. Supplement DLP data watermark

Answer: B

NEW QUESTION 113

- (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 118

- (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 123

- (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 127

- (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 131

- (Exam Topic 2)

Which command shows the current connections distributed by CoreXL FW instances?

- A. fw ctl multik stat
- B. fw ctl affinity -l
- C. fw ctl instances -v
- D. fw ctl iflist

Answer: A

NEW QUESTION 132

- (Exam Topic 2)

What is a best practice before starting to troubleshoot using the “fw monitor” tool?

- A. Run the command: fw monitor debug on
- B. Clear the connections table
- C. Disable CoreXL
- D. Disable SecureXL

Answer: D

NEW QUESTION 137

- (Exam Topic 2)

Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

- A. enable DLP and select.exe and .bat file type
- B. enable .exe & .bat protection in IPS Policy
- C. create FW rule for particular protocol
- D. tecli advanced attributes set prohibited_file_types exe.bat

Answer: A

NEW QUESTION 138

- (Exam Topic 2)

Which Check Point daemon monitors the other daemons?

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

Answer: C

NEW QUESTION 141

- (Exam Topic 2)

The Correlation Unit performs all but the following actions:

- A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
- B. Generates an event based on the Event policy.
- C. Assigns a severity level to the event.
- D. 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.

Answer: C

NEW QUESTION 143

- (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 147

- (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 149

- (Exam Topic 2)

What scenario indicates that SecureXL is enabled?

- A. Dynamic objects are available in the Object Explorer
- B. SecureXL can be disabled in cpconfig
- C. fwaccel commands can be used in clish
- D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 150

- (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 152

- (Exam Topic 2)

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

- A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
- B. mgmt_cli add host name "Server_1" ip-address "10.15.123.10" --format json
- C. mgmt_cli add object-host "Server_1" ip-address "10.15.123.10" --format json
- D. mgmt_cli add object "Server-1" ip-address "10.15.123.10" --format json

Answer: B

Explanation:

Example:

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

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

NEW QUESTION 155

- (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 159

- (Exam Topic 2)

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

- A. Threat Emulation
- B. HTTPS
- C. QOS
- D. VoIP

Answer: D

NEW QUESTION 163

- (Exam Topic 2)

John detected high load on sync interface. Which is most recommended solution?

- A. For short connections like http service – delay sync for 2 seconds
- B. Add a second interface to handle sync traffic
- C. For short connections like http service – do not sync
- D. For short connections like icmp service – delay sync for 2 seconds

Answer: A

NEW QUESTION 168

- (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 172

- (Exam Topic 2)

To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

- A. fw ctl Dyn_Dispatch on
- B. fw ctl Dyn_Dispatch enable
- C. fw ctl multik set_mode 4
- D. fw ctl multik set_mode 1

Answer: C

NEW QUESTION 176

- (Exam Topic 2)

Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.10 SmartConsole application?

- A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
- B. Firewall, IPS, Threat Emulation, Application Control.
- C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.

D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

Answer: C

NEW QUESTION 177

- (Exam Topic 2)

Automation and Orchestration differ in that:

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

Answer: A

NEW QUESTION 182

- (Exam Topic 2)

SandBlast appliances can be deployed in the following modes:

- A. using a SPAN port to receive a copy of the traffic only
- B. detect only
- C. inline/prevent or detect
- D. as a Mail Transfer Agent and as part of the traffic flow only

Answer: C

NEW QUESTION 187

- (Exam Topic 2)

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

- A. Accept Template
- B. Deny Template
- C. Drop Template
- D. NAT Template

Answer: B

NEW QUESTION 192

- (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 196

- (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 199

- (Exam Topic 3)

When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

- A. All UDP packets
- B. All IPv6 Traffic
- C. All packets that match a rule whose source or destination is the Outside Corporate Network
- D. CIFS packets

Answer: D

NEW QUESTION 200

- (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 201

- (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 202

- (Exam Topic 3)

Which file gives you a list of all security servers in use, including port number?

- A. \$FWDIR/conf/conf.conf
- B. \$FWDIR/conf/servers.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/conf/serversd.conf

Answer: C

NEW QUESTION 205

- (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 208

- (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 211

- (Exam Topic 3)

Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

- A. The CoreXL FW instanxcex 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 CoreXI FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type

Answer: B

NEW QUESTION 212

- (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 217

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 221

- (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 is the minimum amount of RAM needed for a Threat Prevention Appliance?

- A. 6 GB
- B. 8GB with Gaia in 64-bit mode
- C. 4 GB
- D. It depends on the number of software blades enabled

Answer: C

NEW QUESTION 227

- (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 228

- (Exam Topic 3)

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

Answer: D

NEW QUESTION 232

- (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)

Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

Answer:

B

NEW QUESTION 236

- (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 239

- (Exam Topic 3)

What kind of information would you expect to see using the sim affinity command?

- A. The VMACs used in a Security Gateway cluster
- B. The involved firewall kernel modules in inbound and outbound packet chain
- C. Overview over SecureXL templated connections
- D. Network interfaces and core distribution used for CoreXL

Answer: D

NEW QUESTION 240

- (Exam Topic 3)

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 is an automatic procedure but Security Management Server failover is a manual procedure.
- B. Security Gateway failover as well as Security Management Server failover is a manual procedure.
- C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
- D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

Answer: A

NEW QUESTION 244

- (Exam Topic 3)

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

- A. Security Gateway IP-address cannot be changed without re-establishing the trust.
- B. The Security Gateway name cannot be changed in command line without re-establishing trust.
- C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust.
- D. The Security Management Server IP-address cannot be changed without re-establishing the trust.

Answer: A

NEW QUESTION 247

- (Exam Topic 3)

You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?

- A. edit fwaffinity.conf; reboot required
- B. cpconfig; reboot required
- C. edit fwaffinity.conf; reboot not required
- D. cpconfig; reboot not required

Answer: B

NEW QUESTION 248

- (Exam Topic 3)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CApp

Answer: B

NEW QUESTION 252

- (Exam Topic 3)

Which of the following is NOT a VPN routing option available in a star community?

- A. To satellites through center only.
- B. To center, or through the center to other satellites, to Internet and other VPN targets.
- C. To center and to other satellites through center.

D. To center only.

Answer: AD

NEW QUESTION 256

- (Exam Topic 3)

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, username Password, Path, Comment, Member

Answer: C

NEW QUESTION 258

- (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 foun
- 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 262

- (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 264

- (Exam Topic 3)

How many layers make up the TCP/IP model?

- A. 2
- B. 7
- C. 6
- D. 4

Answer: D

NEW QUESTION 265

- (Exam Topic 3)

When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

- A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
- B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
- C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
- D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Answer: D

NEW QUESTION 269

- (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 271

- (Exam Topic 3)

What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

- A. 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
- B. 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
- C. 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
- D. 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

Answer: B

NEW QUESTION 273

- (Exam Topic 3)

Which is NOT an example of a Check Point API?

- A. Gateway API
- B. Management API
- C. OPSEC SDK
- D. Threat Prevention API

Answer: A

NEW QUESTION 278

- (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 281

- (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 283

- (Exam Topic 3)

With SecureXL enabled, accelerated packets will pass through the following:

- A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
- B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
- C. Network Interface Card and the Acceleration Device
- D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Answer: C

NEW QUESTION 287

- (Exam Topic 3)

When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

Answer: A

NEW QUESTION 291

- (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 296

- (Exam Topic 4)

What are the minimum open server hardware requirements for a Security Management Server/Standalone in R81?

- A. 2 CPU cores, 4GB of RAM and 15GB of disk space
- B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
- C. 4 CPU cores, 8GB of RAM and 500GB of disk space
- D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

NEW QUESTION 299

- (Exam Topic 4)

What is the default size of NAT table fw_x_alloc?

- A. 20000
- B. 35000
- C. 25000
- D. 10000

Answer: C

NEW QUESTION 300

- (Exam Topic 4)

If SecureXL is disabled which path is used to process traffic?

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

Answer: C

NEW QUESTION 302

- (Exam Topic 4)

Which command lists firewall chain?

- A. fwctl chain
- B. fw list chain
- C. fw chain module
- D. fw tab -t chainmod

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 307

- (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 311

- (Exam Topic 4)

The back end database for Check Point R81 Management uses:

- A. DBMS
- B. MongoDB
- C. PostgreSQL
- D. MySQL

Answer: C

NEW QUESTION 314

- (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 318

- (Exam Topic 4)

Which feature is NOT provided by all Check Point Mobile Access solutions?

- A. Support for IPv6
- B. Granular access control
- C. Strong user authentication
- D. Secure connectivity

Answer: A

Explanation:

Types of Solutions

All of Check Point's Remote Access solutions provide:

NEW QUESTION 323

- (Exam Topic 4)

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 Emulation
- B. SandBlast Agent
- C. Check Point Protect
- D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 328

- (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 329

- (Exam Topic 4)

When defining QoS global properties, which option below is not valid?

- A. Weight
- B. Authenticated timeout
- C. Schedule
- D. Rate

Answer: D

NEW QUESTION 330

- (Exam Topic 4)

After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

- A. You will find it in the home directory of your user account (e.
- B. /home/admin/)
- C. You can locate the file via SmartConsole > Command Line.
- D. You have to launch the WebUI and go to "Config" -> "Export Config File" and specify the destination directory of your local file system.
- E. You cannot locate the file in the file system since Clish does not have any access to the bash file system

Answer: A

NEW QUESTION 333

- (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 GAIAClsh 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)

Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

- A. cphaprob-aif
- B. cp hap rob state
- C. cphaprob list
- D. probcpha -a if

Answer: A

NEW QUESTION 341

- (Exam Topic 4)

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: D

NEW QUESTION 342

- (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 345

- (Exam Topic 4)

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

Answer: D

NEW QUESTION 346

- (Exam Topic 4)

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 list all Process IDs for all running services.
- D. You can check whether the IPS default setting is set to Detect or Prevent mode

Answer: A

NEW QUESTION 349

- (Exam Topic 4)

What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

- A. Mutually Trusted Certificate Authorities
- B. Shared User Certificates
- C. Shared Secret Passwords
- D. Unique Passwords

Answer: A

NEW QUESTION 351

- (Exam Topic 4)

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

- A. Check Point Update Service Engine
- B. Check Point Software Update Agent
- C. Check Point Remote Installation Daemon (CPRID)
- D. Check Point Software Update Daemon

Answer: A

NEW QUESTION 355

- (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 358

- (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 363

- (Exam Topic 4)

Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

- A. On all satellite gateway to satellite gateway tunnels
- B. On specific tunnels for specific gateways
- C. On specific tunnels in the community
- D. On specific satellite gateway to central gateway tunnels

Answer: C

NEW QUESTION 364

- (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 365

- (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 366

- (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 368

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 371

- (Exam Topic 4)

Which Correction mechanisms are available with ClusterXL under R81.10?

- A. Correction Mechanisms are only available of Maestro Hyperscale Orchestrators
- B. Pre-Correction and SDF (Sticky Decision Function)
- C. SDF (Sticky Decision Function) and Flush and ACK
- D. Dispatcher (Early Correction) and Firewall (Late Correction)

Answer: C

NEW QUESTION 376

- (Exam Topic 4)

SecureXL is able to accelerate the Connection Rate using templates. Which attributes are used in the template to identify the connection?

- A. Source address . Destination address
- B. Source Port, Destination port
- C. Source address . Destination address
- D. Destination port
- E. Source address . Destination address
- F. Destination port
- G. Protocol
- H. Source address . Destination address
- I. Source Port, Destination port
- J. Protocol

Answer: D

NEW QUESTION 380

- (Exam Topic 4)

The Compliance Blade allows you to search for text strings in many windows and panes, to search for a value in a field, what would your syntax be?

- A. field_name:string
- B. name field:string
- C. name_field:string
- D. field name:string

Answer: A

NEW QUESTION 383

- (Exam Topic 4)

What should the admin do in case the Primary Management Server is temporary down?

- A. Use the VIP in SmartConsole you always reach the active Management Server.
- B. The Secondary will take over automatically Change the IP in SmartConsole to logon to the private IP of the Secondary Management Server.
- C. Run the 'promote_util' to activate the Secondary Management server
- D. Logon with SmartConsole to the Secondary Management Server and choose "Make Active' under Actions in the HA Management Menu

Answer: A

NEW QUESTION 384

- (Exam Topic 4)

The WebUI offers several methods for downloading hotfixes via CPUSE except:

- A. Automatic
- B. Force override
- C. Manually
- D. Scheduled

Answer: B

NEW QUESTION 389

- (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 393

- (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. 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 tas
- E. Check Point will make use of the newly installed CPU and Cores.

Answer: A

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/ 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 394

- (Exam Topic 4)

What is the correct order of the default “fw monitor” inspection points?

- A. i, l, o, O
- B. 1, 2, 3, 4
- C. i, o, l, O
- D. l, i, O, o

Answer: C

NEW QUESTION 397

- (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 398

- (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)

Which 3 types of tracking are available for Threat Prevention Policy?

- A. SMS Alert, Log, SNMP alert
- B. Syslog, None, User-defined scripts
- C. None, Log, Syslog
- D. Alert, SNMP trap, Mail

Answer: B

NEW QUESTION 400

- (Exam Topic 4)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

NEW QUESTION 403

- (Exam Topic 4)

Bob has finished to 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 MgmtlsPrimary
- B. cpprod_util FwlsSecondary
- C. cpprod_util MgmtlsSecondary
- D. cpprod_util FwlsPrimary

Answer: A

NEW QUESTION 405

- (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 410

- (Exam Topic 4)

By default, the R81 web API uses which content-type in its response?

- A. Java Script
- B. XML
- C. Text
- D. JSON

Answer: D

NEW QUESTION 412

- (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 415

- (Exam Topic 4)

True or False: In R81, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.
- D. False, only one administrator can login with write permission.

Answer: B

NEW QUESTION 417

- (Exam Topic 4)
DLP and Geo Policy are examples of what type of Policy?

- A. Standard Policies
- B. Shared Policies
- C. Inspection Policies
- D. Unified Policies

Answer: B

NEW QUESTION 420

- (Exam Topic 4)
Is it possible to establish a VPN before the user login to the Endpoint Client?

- A. yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_passwordattribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
- B. no, the user must login first.
- C. ye
- D. 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 thetrac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
- E. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console

Answer: D

NEW QUESTION 423

- (Exam Topic 4)
Which one is not a valid Package Option In the Web GUI for CPUSE?

- A. Clean Install
- B. Export Package
- C. Upgrade
- D. Database Conversion to R81.10 only

Answer: B

NEW QUESTION 425

- (Exam Topic 4)
What two ordered layers make up the Access Control Policy Layer?

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

Answer: D

NEW QUESTION 430

- (Exam Topic 4)
What state is the Management HA in when both members have different policies/databases?

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

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/98838

NEW QUESTION 431

- (Exam Topic 4)
Which of the following processes pulls the application monitoring status from gateways?

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

Answer: A

NEW QUESTION 435

- (Exam Topic 4)
If there are two administration logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available or other administrators? (Choose the BEST answer.)

- A. Publish or discard the session.
- B. Revert the session.
- C. Save and install the Policy.
- D. Delete older versions of database.

Answer: A

NEW QUESTION 437

- (Exam Topic 4)

What is false regarding prerequisites for the Central Deployment usage?

- A. The administrator must have write permission on SmartUpdate
- B. Security Gateway must have the latest CPUSE Deployment Agent
- C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
- D. The Security Gateway must have a policy installed

Answer: D

NEW QUESTION 439

- (Exam Topic 4)

An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

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

Answer: D

NEW QUESTION 440

- (Exam Topic 4)

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. Ask
- B. Drop
- C. Inform
- D. Reject

Answer: D

NEW QUESTION 442

- (Exam Topic 4)

How can you see historical data with cpview?

- A. cpview -f <timestamp>
- B. cpview -e <timestamp>
- C. cpview -t <timestamp>
- D. cpview -d <timestamp>

Answer: C

NEW QUESTION 445

- (Exam Topic 4)

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 nod
- B. Connect both Sync interfaces without using a switch.
- C. Use a group of bonded interface
- D. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define a Virtual IP for the Sync interface.
- E. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per nod
- F. Use two different Switches to connect both Sync interfaces.
- G. Use a group of bonded interfaces connected to different switch
- H. Define a dedicated sync interface, only one interface per node using the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management.

Answer: C

NEW QUESTION 448

- (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 452

- (Exam Topic 4)

What are possible Automatic Reactions in SmartEvent?

- A. Mai
- B. SNMP Trap, Block Sourc
- C. Block Event Activity, External Script
- D. Web Mai
- E. Block Destination, SNMP Tra
- F. SmartTask
- G. Web Mail, Block Servic
- H. SNMP Tra
- I. SmartTask, Geo Protection
- J. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Answer: A

NEW QUESTION 457

- (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-Queu
- 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-Queu
- 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 459

- (Exam Topic 4)

What are the two modes for SNX (SSL Network Extender)?

- A. Network Mode and Application Mode
- B. Visitor Mode and Office Mode
- C. Network Mode and Hub Mode
- D. Office Mode and Hub Mode

Answer: A

NEW QUESTION 464

- (Exam Topic 4)

Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

- A. \$FWDIR/conf/client.scv
- B. \$CPDIR/conf/local.scv
- C. \$CPDIR/conf/client.svc
- D. \$FWDIR/conf/local.scv

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION 466

- (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 470

- (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 472

- (Exam Topic 4)

What are the three SecureXL Templates available in R81.10?

- A. PEP Template
- B. QoS Template
- C. VPN Templates
- D. Accept Template
- E. Drop Template
- F. NAT Templates
- G. Accept Template
- H. Drop Template
- I. Reject Templates
- J. Accept Template
- K. PDP Template
- L. PEP Templates

Answer: B

NEW QUESTION 475

- (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 477

- (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 478

.....

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 FirstTry
- * 156-315.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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