

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

What are the different command sources that allow you to communicate with the API server?

- A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
- B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
- C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
- D. API_cli Tool, Gaia CLI, Web Services

Answer: B

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

Which view is NOT a valid CPVIEW view?

- A. IDA
- B. RAD
- C. PDP
- D. VPN

Answer: C

NEW QUESTION 4

- (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 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)

Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

- A. 15 sec
- B. 60 sec
- C. 5 sec
- D. 30 sec

Answer: B

NEW QUESTION 7

- (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 8

- (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 9

- (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 10

- (Exam Topic 1)

On R81.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

NEW QUESTION 10

- (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 14

- (Exam Topic 1)

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. CPM allows the GUI client and management server to communicate via web services using _____.

- A. TCP port 19009
- B. TCP Port 18190
- C. TCP Port 18191
- D. TCP Port 18209

Answer: A

NEW QUESTION 16

- (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 18

- (Exam Topic 1)

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265

- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Answer: D

Explanation:

Synchronization works in two modes:

Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.

Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.

NEW QUESTION 22

- (Exam Topic 1)

During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

- A. Host having a Critical event found by Threat Emulation
- B. Host having a Critical event found by IPS
- C. Host having a Critical event found by Antivirus
- D. Host having a Critical event found by Anti-Bot

Answer: D

NEW QUESTION 24

- (Exam Topic 1)

There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console
- E. Events are collected with SmartWorkflow from Trouble Ticket systems

Answer: E

NEW QUESTION 27

- (Exam Topic 1)

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

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 31

- (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 33

- (Exam Topic 1)

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

- A. Synchronized
- B. Never been synchronized

- C. Lagging
- D. Collision

Answer: D

NEW QUESTION 38

- (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 43

- (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 48

- (Exam Topic 1)

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

NEW QUESTION 53

- (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 56

- (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 58

- (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 61

- (Exam Topic 1)

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. Security Gateway
- E. SmartEvent

Answer: D

NEW QUESTION 65

- (Exam Topic 1)

Where you can see and search records of action done by R81 SmartConsole administrators?

- A. In SmartView Tracker, open active log
- B. In the Logs & Monitor view, select "Open Audit Log View"
- C. In SmartAuditLog View
- D. In Smartlog, all logs

Answer: B

NEW QUESTION 67

- (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 69

- (Exam Topic 1)

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

- A. RADIUS server
- B. Username and password (internal, LDAP)
- C. SecurID
- D. TACACS+

Answer: D

NEW QUESTION 71

- (Exam Topic 1)

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

Answer: B

NEW QUESTION 75

- (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 79

- (Exam Topic 1)

What command verifies that the API server is responding?

- A. api stat
- B. api status
- C. show api_status
- D. app_get_status

Answer: B

NEW QUESTION 84

- (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 89

- (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 90

- (Exam Topic 2)
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

- A. This statement is true because SecureXL does improve all traffic.
- B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
- C. This statement is true because SecureXL does improve this traffic.
- D. This statement is false because encrypted traffic cannot be inspected.

Answer: C

Explanation:

SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 94

- (Exam Topic 2)
Which GUI client is supported in R81?

- A. SmartProvisioning
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartLog

Answer: C

NEW QUESTION 95

- (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 97

- (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 98

- (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 102

- (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 105

- (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 106

- (Exam Topic 2)

Which of the following is NOT a type of Check Point API available in R81.x?

- A. Identity Awareness Web Services
- B. OPSEC SDK
- C. Mobile Access
- D. Management

Answer: C

NEW QUESTION 110

- (Exam Topic 2)

What is the command to see cluster status in cli expert mode?

- A. fw ctl stat
- B. clusterXL stat
- C. clusterXL status
- D. cphaprob stat

Answer: D

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 114

- (Exam Topic 2)

You have existing dbedit scripts from R77. Can you use them with R81.10?

- A. dbedit is not supported in R81.10
- B. dbedit is fully supported in R81.10
- C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
- D. dbedit scripts are being replaced by mgmt_cli in R81.10

Answer: D

NEW QUESTION 116

- (Exam Topic 2)

Which encryption algorithm is the least secured?

- A. AES-128
- B. AES-256

- C. DES
- D. 3DES

Answer: C

NEW QUESTION 120

- (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 123

- (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 127

- (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 131

- (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 134

- (Exam Topic 2)

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

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

Answer: C

Explanation:

Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

- Matching a Log Against Global Exclusions
- Matching a Log Against Each Event Definition
- Creating an Event Candidate
- When a Candidate Becomes an Event References:

NEW QUESTION 136

- (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 138

- (Exam Topic 2)

Which directory below contains log files?

- A. /opt/CPsmartlog-R81/log
- B. /opt/CPshrd-R81/log
- C. /opt/CPsuite-R81/fw1/log
- D. /opt/CPsuite-R81/log

Answer: C

NEW QUESTION 142

- (Exam Topic 2)

Which one of the following is true about Capsule Connect?

- A. It is a full layer 3 VPN client
- B. It offers full enterprise mobility management
- C. It is supported only on iOS phones and Windows PCs
- D. It does not support all VPN authentication methods

Answer: A

NEW QUESTION 144

- (Exam Topic 2)

Customer's R81 management server needs to be upgraded to R81.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R81 configuration, clean install R81.10 and import the configuration
- B. CPUSE offline upgrade
- C. CPUSE online upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 146

- (Exam Topic 2)

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: A

NEW QUESTION 150

- (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 154

- (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 158

- (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 159

- (Exam Topic 2)

Which web services protocol is used to communicate to the Check Point R81 Identity Awareness Web API?

- A. SOAP
- B. REST
- C. XLANG
- D. XML-RPC

Answer: B

Explanation:

The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NEW QUESTION 161

- (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 164

- (Exam Topic 2)

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

- A. Analyzes each log entry as it arrives at the log server according to the Event Policy.
- B. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.
- C. Correlates all the identified threats with the consolidation policy.
- D. Collects syslog data from third party devices and saves them to the database.
- E. Connects with the SmartEvent Client when generating threat reports.

Answer: A

NEW QUESTION 167

- (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 172

- (Exam Topic 2)

How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

- A. cphaprob set int fwaha_vmac_global_param_enabled 1
- B. clusterXL set int fwaha_vmac_global_param_enabled 1
- C. fw ctl set int fwaha_vmac_global_param_enabled 1
- D. cphaconf set int fwaha_vmac_global_param_enabled 1

Answer: C

NEW QUESTION 174

- (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 175

- (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 176

- (Exam Topic 3)

Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users from AD.

- A. WMI
- B. Eventvwr
- C. XML
- D. Services.msc

Answer: A

NEW QUESTION 177

- (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 179

- (Exam Topic 3)

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 181

- (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 185

- (Exam Topic 3)

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Setting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

Answer: D

NEW QUESTION 186

- (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 191

- (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 195

- (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 197

- (Exam Topic 3)

Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R81.

What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?

- A. Missing an installed R77.20 Add-on on Security Management Server
- B. Unsupported firmware on UTM-1 Edge-W appliance
- C. Unsupported version on UTM-1 570 series appliance
- D. Unsupported appliances on remote locations

Answer: A

NEW QUESTION 199

- (Exam Topic 3)

Check Point security components are divided into the following components:

- A. GUI Client, Security Gateway, WebUI Interface
- B. GUI Client, Security Management, Security Gateway
- C. Security Gateway, WebUI Interface, Consolidated Security Logs
- D. Security Management, Security Gateway, Consolidate Security Logs

Answer: B

NEW QUESTION 204

- (Exam Topic 3)

What command lists all interfaces using Multi-Queue?

- A. cpmq get
- B. show interface all
- C. cpmq set
- D. show multiqueue all

Answer: A

NEW QUESTION 208

- (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 212

- (Exam Topic 3)

What is UserCheck?

- A. Messaging tool used to verify a user's credentials.
- B. Communication tool used to inform a user about a website or application they are trying to access.
- C. Administrator tool used to monitor users on their network.
- D. Communication tool used to notify an administrator when a new user is created.

Answer: B

NEW QUESTION 216

- (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 219

- (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 224

- (Exam Topic 3)

Which Check Point feature enables application scanning and the detection?

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

Answer: B

NEW QUESTION 228

- (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 229

- (Exam Topic 3)

What is the command to show SecureXL status?

- A. fwaccel status
- B. fwaccel stats -m
- C. fwaccel -s
- D. fwaccel stat

Answer: D

Explanation:

To check overall SecureXL status: [Expert@HostName]# fwaccel stat References:

NEW QUESTION 230

- (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 232

- (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 235

- (Exam Topic 3)

Which command would you use to set the network interfaces' affinity in Manual mode?

- A. sim affinity -m
- B. sim affinity -l
- C. sim affinity -a
- D. sim affinity -s

Answer: D

NEW QUESTION 239

- (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 241

- (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 242

- (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 247

- (Exam Topic 3)

What is the valid range for VRID value in VRRP configuration?

- A. A.-1 - 254B.1 - 255C.0 - 254D.0 - 255

Answer: B

Explanation:

Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.

NEW QUESTION 250

- (Exam Topic 4)

How would you enable VMAC Mode in ClusterXL?

- A. Cluster Object -> Edit -> ClusterXL and VRRP -> Use Virtual MAC
- B. fw ctl set int vmac_mode 1
- C. cphaconf vmac_mode set 1
- D. Cluster Object -> Edit -> Cluster Members -> Edit -> Use Virtual MAC

Answer: A

Explanation:

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

NEW QUESTION 255

- (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 of 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 260

- (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 264

- (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 268

- (Exam Topic 4)

Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?

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

Answer: C

NEW QUESTION 270

- (Exam Topic 4)

A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

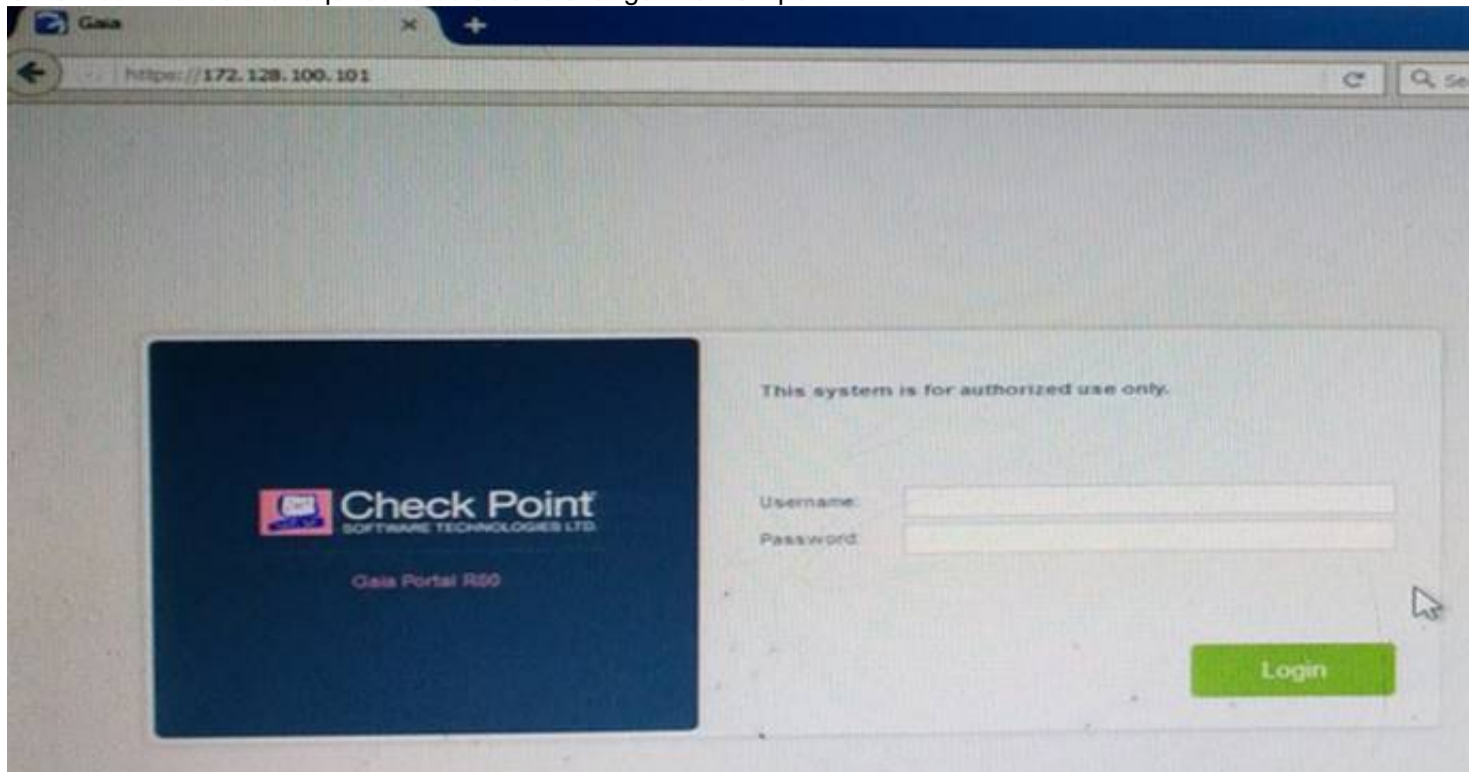
- A. run fw unloadlocal" on the relevant gateway and check the ping again
- B. run "cpstop" on the relevant gateway and check the ping again
- C. run "fw log" on the relevant gateway
- D. run "fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 275

- (Exam Topic 4)

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



- A. set web ssl-port <new port number>
- B. set Gaia-portal port <new port number>
- C. set Gaia-portal https-port <new port number>
- D. set web https-port <new port number>

Answer: A

NEW QUESTION 276

- (Exam Topic 4)

Which components allow you to reset a VPN tunnel?

- A. vpn tu command or SmartView monitor
- B. delete vpn ike sa or vpn she11 command
- C. vpn tunnelutil or delete vpn ike sa command
- D. SmartView monitor only

Answer: D

NEW QUESTION 281

- (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 283

- (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 284

- (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 289

- (Exam Topic 4)

The customer has about 150 remote access user with a Windows laptops. Not more than 50 Clients will be connected at the same time. The customer want to use multiple VPN Gateways as entry point and a personal firewall. What will be the best license for him?

- A. He will need Capsule Connect using MEP (multiple entry points).
- B. Because the customer uses only Windows clients SecuRemote will be sufficient and no additional license is needed
- C. He will need Harmony Endpoint because of the personal firewall.
- D. Mobile Access license because he needs only a 50 user license, license count is per concurrent use

Answer: D

NEW QUESTION 291

- (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 296

- (Exam Topic 4)

Kurt is planning to upgrade his Security Management Server to R81.X. What is the lowest supported version of the Security Management he can upgrade from?

- A. R76 Splat
- B. R77.X Gaia
- C. R75 Splat
- D. R75 Gaia

Answer: D

NEW QUESTION 297

- (Exam Topic 4)

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

- A. All Connections (Clear or Encrypted)
- B. Accept all encrypted traffic
- C. Specific VPN Communities
- D. All Site-to-Site VPN Communities

Answer: B

NEW QUESTION 298

- (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 300

- (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 302

- (Exam Topic 4)

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly

modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor.

Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS AND Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

NEW QUESTION 306

- (Exam Topic 4)

Which of the following is NOT a valid type of SecureXL template?

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

Answer: B

NEW QUESTION 307

- (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 308

- (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 311

- (Exam Topic 4)

Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

- A. Better understand the behavior of the Access Control Policy
- B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
- C. Automatically rearrange Access Control Policy based on Hit Count Analysis
- D. Analyze a Rule Base - You can delete rules that have no matching connections

Answer: C

NEW QUESTION 312

- (Exam Topic 4)

In Threat Prevention, you can create new or clone profiles but you CANNOT change the out-of-the-box profiles of:

- A. Basic, Optimized, Strict
- B. Basic, Optimized, Severe
- C. General, Escalation, Severe
- D. General, purposed, Strict

Answer: A

NEW QUESTION 313

- (Exam Topic 4)

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

- A. For FTP connections – do not sync
- 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 314

- (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 319

- (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 320

- (Exam Topic 4)

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

Answer: D

Explanation:

Identity Awareness gets identities from these acquisition sources:

NEW QUESTION 323

- (Exam Topic 4)

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

- A. Pentagon
- B. Combined
- C. Meshed
- D. Star

Answer: D

NEW QUESTION 328

- (Exam Topic 4)

What solution is Multi-queue intended to provide?

- A. Improve the efficiency of traffic handling by SecureXL SNDs
- B. Reduce the confusion for traffic capturing in FW Monitor
- C. Improve the efficiency of CoreXL Kernel Instances
- D. Reduce the performance of network interfaces

Answer: C

NEW QUESTION 329

- (Exam Topic 4)

Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?

- A. Yes, but they need to have a mutually trusted certificate authority
- B. Yes, but they have to have a pre-shared secret key
- C. No, they cannot share certificate authorities
- D. No, Certificate based VPNs are only possible between Check Point devices

Answer:

A

NEW QUESTION 334

- (Exam Topic 4)

By default how often updates are checked when the CPUSE Software Updates Policy is set to Automatic?

- A. Six times per day
- B. Seven times per day
- C. Every two hours
- D. Every three hours

Answer: D

Explanation:

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

NEW QUESTION 337

- (Exam Topic 4)

According to out of the box SmartEvent policy, which blade will automatically be correlated into events?

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

Answer: C

NEW QUESTION 342

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 346

- (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 347

- (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 349

- (Exam Topic 4)

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server.

Answer: D

NEW QUESTION 352

- (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 355

- (Exam Topic 4)

Which component is NOT required to communicate with the Web Services API?

- A. API key
- B. session ID token
- C. content-type
- D. Request payload

Answer: A

NEW QUESTION 356

- (Exam Topic 4)

John is using Management HA. Which Security Management Server should he use for making changes?

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

Answer: B

NEW QUESTION 360

- (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 365

- (Exam Topic 4)

Packet acceleration (SecureXL) identifies connections by several attributes- Which of the attributes is NOT used for identifying connection?

- A. Source Address
- B. Destination Address
- C. TCP Acknowledgment Number
- D. Source Port

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 366

- (Exam Topic 4)

What is false regarding a Management HA environment?

- A. Only one Management Server should be active, while any others be in standby mode
- B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
- C. SmartConsole can connect to any management server in Readonly mode.

D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Answer: B

NEW QUESTION 368

- (Exam Topic 4)

When synchronizing clusters, which of the following statements is FALSE?

- A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
- B. Only cluster members running on the same OS platform can be synchronized.
- C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
- D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D

NEW QUESTION 373

- (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 377

- (Exam Topic 4)

Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

- A. https://<Device_IP_Address>
- B. http://<Device_IP_Address>:443
- C. https://<Device_IP_Address>:10000
- D. https://<Device_IP_Address>:4434

Answer: A

NEW QUESTION 378

- (Exam Topic 4)

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

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

Answer: B

NEW QUESTION 381

- (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 383

- (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 388

- (Exam Topic 4)

According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them into a temporary directory. Which process is true for receiving these Tiles;

- A. FWD
- B. CPD
- C. FWM
- D. RAD

Answer: A

NEW QUESTION 393

- (Exam Topic 4)

Which software blade does NOT accompany the Threat Prevention policy?

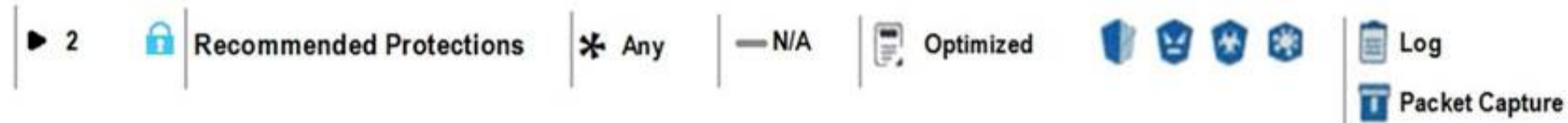
- A. Anti-virus
- B. IPS
- C. Threat Emulation
- D. Application Control and URL Filtering

Answer: D

NEW QUESTION 394

- (Exam Topic 4)

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



- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION 398

- (Exam Topic 4)

You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column. How to fix it?

- A. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
- B. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
- C. The Mobile Access Policy Source under Gateway properties is set to Legacy Policy and not to Unified Access Policy.
- D. The Mobile Access Blade is not enabled under Gateway properties.

Answer: C

NEW QUESTION 403

- (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 407

- (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 412

- (Exam Topic 4)

How can you switch the active log file?

- A. Run fw logswitch on the gateway
- B. Run fwm logswitch on the Management Server
- C. Run fwm logswitch on the gateway
- D. Run fw logswitch on the Management Server

Answer: D

NEW QUESTION 413

- (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 by the active gateway
- C. All connections that were initiated before the upgrade will be handled normally
- D. All connections that were initiated before the upgrade will be handled by the standby gateway

Answer: B

NEW QUESTION 415

- (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 419

- (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 424

- (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 429

- (Exam Topic 4)

What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

- A. test_connectivity_ad -d <domain>
- B. test_ldap_connectivity -d <domain>
- C. test_ad_connectivity -d <domain>
- D. ad_connectivity_test -d <domain>

Answer: C

Explanation:

<https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/>

[CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/200877](https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/200877)

NEW QUESTION 433

- (Exam Topic 4)

What are possible Automatic Reactions in SmartEvent?

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

Answer: A

NEW QUESTION 436

- (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 load
- 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's
- 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's
- 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 load
- J. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

Answer: D

NEW QUESTION 439

- (Exam Topic 4)

Which command is used to add users to or from existing roles?

- A. Add rba user <User Name> roles <List>
- B. Add rba user <User Name>
- C. Add user <User Name> roles <List>
- D. Add user <User Name>

Answer: A

NEW QUESTION 443

- (Exam Topic 4)

What is "Accelerated Policy Installation"?

- A. Starting R81, the Desktop Security Policy installation process is accelerated thereby reducing the duration of the process significantly
- B. Starting R81, the QoS Policy installation process is accelerated thereby reducing the duration of the process significantly
- C. Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly
- D. Starting R81, the Threat Prevention Policy installation process is accelerated thereby reducing the duration of the process significantly

Answer: C

NEW QUESTION 447

- (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 451

- (Exam Topic 4)

What command is used to manually failover a cluster during a zero downtime upgrade?

- A. set cluster member down
- B. cpstop
- C. clusterXL_admin down
- D. set clusterXL down

Answer: C

NEW QUESTION 452

- (Exam Topic 4)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

NEW QUESTION 453

- (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 457

- (Exam Topic 4)

Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R81/CP_R81BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 461

- (Exam Topic 4)

CoreXL is NOT supported when one of the following features is enabled: (Choose three)

- A. Route-based VPN
- B. IPS
- C. IPv6
- D. Overlapping NAT

Answer: ACD

Explanation:

CoreXL does not support Check Point Suite with these features:

- > Check Point QoS (Quality of Service)
- > Route-based VPN
- > IPv6 on IPSO
- > Overlapping NAT

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

NEW QUESTION 464

- (Exam Topic 4)

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

- A. show interface eth0 mq
- B. ethtool A eth0
- C. ifconfig -i eth0 verbose
- D. ip show Int eth0

Answer: A

NEW QUESTION 465

- (Exam Topic 4)

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C

NEW QUESTION 468

- (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 469

- (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 470

- (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 475

- (Exam Topic 4)

What are the two types of tests when using the Compliance blade?

- A. Policy-based tests and Global properties
- B. Global tests and Object-based tests
- C. Access Control policy analysis and Threat Prevention policy analysis
- D. Tests conducted based on the IoC XMfchfile and analysis of SOLR documents

Answer: D

NEW QUESTION 479

.....

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](#)