CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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)
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 4
- (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 5
- (Exam Topic 1)
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user’s machine via the web browser. What are the two modes of SNX?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is a new R81 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rule
B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
D. Time object to a rule to make the rule active only during specified times.
E. Sub Policies ae sets of rules that can be created and attached to specific rule
F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 7
- (Exam Topic 1)

Which view is NOT a valid CPVIEW view?

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

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
What is true about the IPS-Blade?

A. In R81, IPS is managed by the Threat Prevention Policy
B. In R81, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. In R81, IPS Exceptions cannot be attached to “all rules”
D. In R81, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____.

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

Answer: D

NEW QUESTION 10
- (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 11
- (Exam Topic 1)
Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config
D. St cpmq enable

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
Fill in the blank: The R81 utility fw monitor is used to troubleshoot .

A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiations

Answer: C

Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

NEW QUESTION 17
- (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 21
- (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 23
- (Exam Topic 1)
What is the mechanism behind Threat Extraction?

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

Answer: D

NEW QUESTION 24
- (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 26
- (Exam Topic 1)
Which command will allow you to see the interface status?

A. cphaprob interface
B. cphaprob –I interface
C. cphaprob –a if
D. cphaprob stat

Answer: C

NEW QUESTION 29
- (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 31
- (Exam Topic 1)
Advanced Security Checkups can be easily conducted within:

A. Reports
B. Advanced

C. Checkups
D. Views
E. Summary

Answer: A

NEW QUESTION 36
- (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 41
- (Exam Topic 1)
What happen when IPS profile is set in Detect Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control

Answer: C

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

NEW QUESTION 46
- (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 47
- (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 50
- (Exam Topic 1)
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members.

Answer: A

NEW QUESTION 54
- (Exam Topic 1)

To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?

A. 5 Network; Host; Objects; Services; API
B. 3 Incoming; Outgoing; Network
C. 2 Internal; External
D. 4 Incoming; Outgoing; Internal; Other

Answer: D

NEW QUESTION 57
- (Exam Topic 1)
Which statement is correct about the Sticky Decision Function?

A. It is not supported with either the Performance pack of a hardware based accelerator card
B. Does not support SPI's when configured for Load Sharing
C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
D. It is not required L2TP traffic

Answer: A

NEW QUESTION 60
- (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 65
- (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 68
- (Exam Topic 1)
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

Answer: C

Explanation:
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

NEW QUESTION 69
- (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 73
- (Exam Topic 1)
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect

B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 77
- (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 81
- (Exam Topic 1)
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

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

Answer: C

NEW QUESTION 82
- (Exam Topic 1)
Which command lists all tables in Gaia?

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

Answer: C

NEW QUESTION 87
- (Exam Topic 1)
Which of the following type of authentication on Mobile Access can NOT be used as the first authentication method?

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

Answer: A

NEW QUESTION 90
- (Exam Topic 1)
Which two of these Check Point Protocols are used by SmartEvent Processes?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Answer: D

NEW QUESTION 91
- (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 95
- (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 98
- (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 100
- (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 101
- (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 102
- (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 105
- (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 107
- (Exam Topic 2)
What are the blades of Threat Prevention?

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

Answer: D

NEW QUESTION 111

- (Exam Topic 2)
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: A

NEW QUESTION 116
- (Exam Topic 2)
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

A. SFWDIR/smartevent/conf
B. $RTDIR/smartevent/conf
C. $RTDIR/smartview/conf
D. $FWDIR/smartview/conf

Answer: C

NEW QUESTION 118
- (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 121
- (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 requite direct GUI access, such as SmartEvent, It provides the following:
– GUI Client communication
– Database manipulation
– Policy Compilation
– Management HA sync

NEW QUESTION 124
- (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 126
- (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 127
- (Exam Topic 2)
You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

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

Answer: D

NEW QUESTION 131
- (Exam Topic 2)
You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

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

Answer: C

NEW QUESTION 133
- (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 138
- (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 142
- (Exam Topic 2)
Which encryption algorithm is the least secured?

A. AES-128
B. AES-256
C. DES
D. 3DES

Answer: C

NEW QUESTION 146
- (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 148
- (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 149
- (Exam Topic 2)
How do Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VP
B. Capsule Workspace provides a Desktop with usable applications.
C. Capsule Workspace can provide access to any application.
D. Capsule Connect provides Business data isolation.
E. Capsule Connect does not require an installed application at client.

Answer: A

NEW QUESTION 152
- (Exam Topic 2)
Please choose correct command to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt: add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt: add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 155
- (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 157
- (Exam Topic 2)
What processes does CPM control?

A. Object-Store, Database changes, CPM Process and web-services
B. web-services, CPMI process, DLEserver, CPM process
C. DLEServer, Object-Store, CP Process and database changes
D. web_services, dle_server and object_Store

Answer: D

NEW QUESTION 161
- (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 162
- (Exam Topic 2)
What are the main stages of a policy installations?

A. Verification & Compilation, Transfer and Commit
B. Verification & Compilation, Transfer and Installation
C. Verification, Commit, Installation
D. Verification, Compilation & Transfer, Installation

Answer: A

NEW QUESTION 167

- (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 170
- (Exam Topic 2)
VPN Link Selection will perform the following when the primary VPN link goes down?

A. The Firewall will drop the packets.
B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
C. The Firewall will send out the packet on all interfaces.
D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 171
- (Exam Topic 2)
Which Remote Access Client does not provide an Office-Mode Address?

A. SecuRemote
B. Endpoint Security Suite
C. Endpoint Security VPN
D. Check Point Mobile

Answer: A

NEW QUESTION 174
- (Exam Topic 2)
Which one of the following is true about Threat Extraction?

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

Answer: A

NEW QUESTION 177
- (Exam Topic 2)
What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

A. new host name “New Host” ip-address “192.168.0.10”
B. set host name “New Host” ip-address “192.168.0.10”
C. create host name “New Host” ip-address “192.168.0.10”
D. add host name “New Host” ip-address “192.168.0.10”

Answer: D

NEW QUESTION 180
- (Exam Topic 2)
With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

A. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
B. For end users to access the native applications, they need to install the SSL Network Extender.
C. HTTPS for web-based applications and AES or RSA algorithm for native application
D. For end users to access the native application, they need to install the SSL Network Extender.
E. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
F. For end users to access the native applications, no additional software is required.
G. HTTPS for web-based applications and AES or RSA algorithm for native application
H. For end users to access the native application, no additional software is required.

Answer: A

NEW QUESTION 181
- (Exam Topic 2)
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?

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

Answer: A

NEW QUESTION 183
- (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 185
- (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 189
- (Exam Topic 2)
What is the command to check the status of the SmartEvent Correlation Unit?

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

Answer: B

NEW QUESTION 194
- (Exam Topic 2)
Which statement is true about ClusterXL?

A. Supports Dynamic Routing (Unicast and Multicast)
B. Supports Dynamic Routing (Unicast Only)
C. Supports Dynamic Routing (Multicast Only)
D. Does not support Dynamic Routing

Answer: A

NEW QUESTION 197
- (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 199
- (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 201
- (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 205
- (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 207
- (Exam Topic 2)
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 208
- (Exam Topic 2)
Which of the following links will take you to the SmartView web application?

A. https://<Security Management Server host name>/smartviewweb/
B. https://<Security Management Server IP Address>/smartview/
C. https://<Security Management Server host name>smartviewweb
D. https://<Security Management Server IP Address>/smartview

Answer: B

NEW QUESTION 210
- (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 213
- (Exam Topic 2)
You want to store the GAIA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config –f <filename>
C. save config –o <filename>
D. save configuration <filename>

Answer: D

NEW QUESTION 217
- (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 221
- (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 Polic
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 224
- (Exam Topic 2)
Which one of the following is true about Threat Emulation?

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

Answer: D

NEW QUESTION 225
- (Exam Topic 2)
What component of R81 Management is used for indexing?

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

Answer: D

NEW QUESTION 230
- (Exam Topic 2)
What is the port used for SmartConsole to connect to the Security Management Server?

A. CPMI port 18191/TCP
B. CPM port/TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP

Answer: A

NEW QUESTION 234
- (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 235
- (Exam Topic 2)
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart

Answer: B

NEW QUESTION 236
- (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 239
- (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 242
- (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 245
- (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 247
- (Exam Topic 3)
Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.
What is one of the requirements for his success?

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

Answer: B

NEW QUESTION 252
- (Exam Topic 3)
What statement best describes the Proxy ARP feature for Manual NAT in R81.10?

A. Automatic proxy ARP configuration can be enabled
B. Translate Destination on Client Side should be configured
C. fw ctl proxy should be configured
D. local.arp file must always be configured

Answer: D

NEW QUESTION 257
- (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 260
- (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 261
- (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 265
- (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 266
- (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 271
- (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 272
- (Exam Topic 3)
What is true of the API server on R81.10?

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

Answer: D

NEW QUESTION 276

- (Exam Topic 3)
You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.
What must you do to get SIC to work?

A. Remove Geo-Protection, as the IP-to-country database is updated externally, and you have no control of this.
B. Create a rule at the top in the Sydney firewall to allow control traffic from your network
C. Nothing - Check Point control connections function regardless of Geo-Protection policy
D. Create a rule at the top in your Check Point firewall to bypass the Geo-Protection

Answer: C

NEW QUESTION 280
- (Exam Topic 3)
Which statement is most correct regarding about “CoreXL Dynamic Dispatcher”?

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

Answer: B

NEW QUESTION 283
- (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 288
- (Exam Topic 3)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 293
- (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 296
- (Exam Topic 3)
Fill in the blank: The “fw monitor” tool can be best used to troubleshoot _____.

A. AV issues
B. VPN errors
C. Network traffic issues
D. Authentication issues

Answer: C

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal? eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NEW QUESTION 300
- (Exam Topic 3)
Check Point APIs allow system engineers and developers to make changes to their organization’s security policy with CLI tools and Web Services for all the following except:

A. Create new dashboards to manage 3rd party task

B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution

Answer: A

Explanation:
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
• Use an automated script to perform common tasks
• Integrate Check Point products with 3rd party solutions
• Create products that use and enhance the Check Point solution References:

NEW QUESTION 302
- (Exam Topic 3)
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned O
B. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OF
D. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
E. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
F. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Answer: A

NEW QUESTION 304
- (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 305
- (Exam Topic 3)
One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: C

NEW QUESTION 308
- (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 310
- (Exam Topic 3)
Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____ .

A. Sent to the Internal Certificate Authority.
B. Sent to the Security Administrator.
C. Stored on the Security Management Server.
D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 315
- (Exam Topic 3)
SandBlast agent extends 0 day prevention to what part of the network?

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

Answer: A

NEW QUESTION 316
- (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 317
- (Exam Topic 3)
What CLI command compiles and installs a Security Policy on the target's Security Gateways?

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

Answer: B

NEW QUESTION 322
- (Exam Topic 3)
Which of the following technologies extracts detailed information from packets and stores that information in state tables?

A. INSPECT Engine
B. Stateful Inspection
C. Packet Filtering
D. Application Layer Firewall

Answer: A

NEW QUESTION 324
- (Exam Topic 3)
Which blades and or features are not supported in R81?

A. SmartEvent Maps
B. SmartEvent
C. Identity Awareness
D. SmartConsole Toolbars

Answer: A

NEW QUESTION 328
- (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 332
- (Exam Topic 3)
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

A. User Directory
B. Captive Portal and Transparent Kerberos Authentication
C. Captive Portal
D. UserCheck

Answer: B

NEW QUESTION 337

- (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 341
- (Exam Topic 3)
Which of the following commands shows the status of processes?

A. cpwd_admin -l
B. cpwd -l
C. cpwd admin_list
D. cpwd_admin list

Answer: D

NEW QUESTION 345
- (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 349
- (Exam Topic 3)
In the Firewall chain mode FFF refers to:

A. Stateful Packets
B. No Match
C. All Packets
D. Stateless Packets

Answer: C

NEW QUESTION 353
- (Exam Topic 3)
In what way are SSL VPN and IPSec VPN different?

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

Answer: D

NEW QUESTION 354
- (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 358
- (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 361
- (Exam Topic 3)
With MTA (Mail Transfer Agent) enabled the gateways manages SMTP traffic and holds external email with potentially malicious attachments. What is required in order to enable MTA (Mail Transfer Agent) functionality in the Security Gateway?

A. Threat Cloud Intelligence
B. Threat Prevention Software Blade Package
C. Endpoint Total Protection
D. Traffic on port 25

Answer: B

NEW QUESTION 363
- (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 368
- (Exam Topic 3)
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Answer: D

NEW QUESTION 370
- (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 371
- (Exam Topic 3)
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Stateful Mode configuration, chain modules marked with _____ will not apply.

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

Answer: D

NEW QUESTION 376
- (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 381
- (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 385
- (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 388
- (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 392
- (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 395
- (Exam Topic 4)
Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

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

Answer: D

NEW QUESTION 399
- (Exam Topic 4)
What is the default size of NAT table fwx_alloc?

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

Answer: C

NEW QUESTION 401
- (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 403

- (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 407
- (Exam Topic 4)
Which of the following is NOT a type of Endpoint Identity Agent?

A. Terminal
B. Light
C. Full
D. Custom

Answer: A

NEW QUESTION 412
- (Exam Topic 4)
What is the SOLR database for?

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

Answer: A

NEW QUESTION 417
- (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 419
- (Exam Topic 4)
D18912E1457D5D1DDCBD40AB3BF70D5D
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule based and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

A. The connection is destined for a server within the network
B. The connection required a Security server
C. The packet is the second in an established TCP connection
D. The packets are not multicast

Answer: B

NEW QUESTION 424
- (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 429
- (Exam Topic 4)
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via
e-m ail. 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 433
- (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 438
- (Exam Topic 4)
What are the services used for Cluster Synchronization?

A. 256H-CP tor Full Sync and 8116/UDP for Delta Sync
B. 8116/UDP for Full Sync and Delta Sync
C. TCP/256 for Full Sync and Delta Sync
D. No service needed when using Broadcast Mode

Answer: C

NEW QUESTION 443
- (Exam Topic 4)
Which utility allows you to configure the DHCP service on Gaia from the command line?

A. ifconfig
B. dhcp_ofg
C. sysconfig
D. cpconfig

Answer: C

NEW QUESTION 446
- (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 448
- (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 449
- (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 451
- (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 specifiy 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 455
- (Exam Topic 4)
How long may verification of one file take for Sandblast Threat Emulation?

A. up to 1 minutes
B. within seconds cleaned file will be provided
C. up to 5 minutes
D. up to 3 minutes

Answer: B

NEW QUESTION 457
- (Exam Topic 4)
Which Queue in the Priority Queue has the maximum priority?

A. High Priority
B. Control
C. Routing
D. Heavy Data Queue

Answer: C

NEW QUESTION 459
- (Exam Topic 4)
Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

A. cpexport
B. sysinfo
C. cpsizeme
D. cpinfo

Answer: D

NEW QUESTION 464
- (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 465
- (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. SecurelD

Answer: A

NEW QUESTION 469
- (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 470
- (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 474
- (Exam Topic 4)
What traffic does the Anti-bot feature block?

A. Command and Control traffic from hosts that have been identified as infected
B. Command and Control traffic to servers with reputation for hosting malware
C. Network traffic that is directed to unknown or malicious servers
D. Network traffic to hosts that have been identified as infected

Answer: A

NEW QUESTION 479
- (Exam Topic 4)
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

A. action:"Key Install" AND 1.1.1.1 AND Main Mode
B. action:"Key Install- AND 1.1.1.1 ANDQuick Mode
C. Blade:"VPN" AND VPN-Stores AND Main Mode
D. Blade:"VPN" AND VPN-Stores AND Quick Mode

Answer: C

NEW QUESTION 482
- (Exam Topic 4)
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

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

Answer: B

NEW QUESTION 484
- (Exam Topic 4)
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck
B. Active Directory Query
C. Account Unit Query
D. User Directory Query

Answer: B

Explanation:
Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 489
- (Exam Topic 4)
What are the correct sleps upgrading a HA cluster (Ml is active. M2 is passive) using Multi-Version Cluster(MVC) Upgrade?

A. 1) Enable the MVC mechanism on both cluster members «cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
B. change the version of the cluster object4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism
C. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
D. change the version of the cluster object4) Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy

E. 1) In SmartConsol
F. change the version of the cluster object2) Upgrade the passive node M2 to R81.103) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 Wcphaconf mvc on4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsol
G. change the version of the cluster object
H. 1) Upgrade the passive node M2 to R81.102) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 ttcphaconf mvc on3) In SmartConsole, change the version of the cluster object 4} Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.10

Answer: D

NEW QUESTION 492
- (Exam Topic 4)
Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with _____ will not apply.

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

Answer: B

NEW QUESTION 496
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. Go to clash-Run cpstop | Run cpstart
B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
C. Administrator does not need to perform any tas
D. Check Point will make use of the newly installed CPU and Cores
E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 498
- (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 501
- (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 505
- (Exam Topic 4)
Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____.

A. The license is attached to the wrong Security Gateway.
B. The existing license expires.
C. The license is upgraded.
D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 507
- (Exam Topic 4)
Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password

D. Token

Answer: A

NEW QUESTION 511
- (Exam Topic 4)
You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
B. ifconfig eth1 hw 11:11:11:11:11:11; expert
C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

Answer: A

NEW QUESTION 514
- (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 519
- (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 522
- (Exam Topic 4)
Which of the following is NOT an internal/native Check Point command?

A. fwaccel on
B. fw ct1 debug
C. tcpdump
D. cphaprob

Answer: C

NEW QUESTION 523
- (Exam Topic 4)
Alice works for a big security outsourcing provider company and as she receives a lot of change requests per day she wants to use for scripting daily (asks the API services from Check Point fof the Management API. Firstly she needs to be aware if the API services are running for the management. Which of the following Check Point Command is true:

A. api mgmt status
B. api status
C. status api
D. status mgmt apt

Answer: B

NEW QUESTION 528
- (Exam Topic 4)
How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?

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

Answer: B

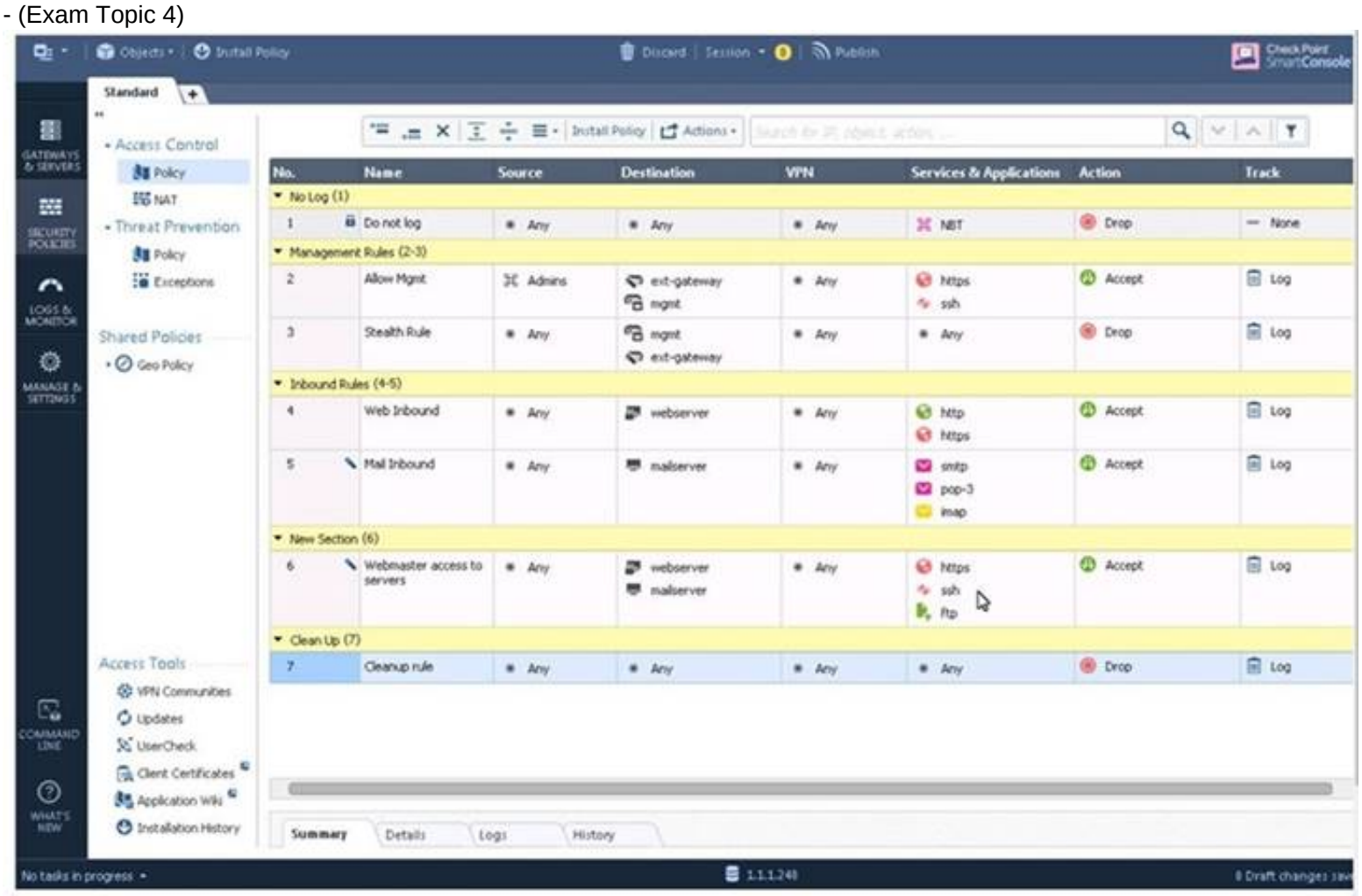
NEW QUESTION 530

- (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 532
- (Exam Topic 4)



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

A. Rule 7 was created by the ‘admin’ administrator in the current session
B. 8 changes have been made by administrators since the last policy installation
C. The rules 1, 5 and 6 cannot be edited by the ‘admin’ administrator
D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 537
- (Exam Topic 4)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 538
- (Exam Topic 4)
What is the base level encryption key used by Capsule Docs?

A. RSA 2048
B. RSA 1024
C. SHA-256
D. AES

Answer: A

NEW QUESTION 539
- (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 542
- (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 546
- (Exam Topic 4)
Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 550
- (Exam Topic 4)
What does the Log "Views" tab show when SmartEvent is Correlating events?

A. A list of common reports
B. Reports for customization
C. Top events with charts and graphs
D. Details of a selected logs

Answer: D

NEW QUESTION 551
- (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 553
- (Exam Topic 4)
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

A. Accept; redirect
B. Accept; drop
C. Redirect; drop
D. Drop; accept

Answer: D

NEW QUESTION 558
- (Exam Topic 4)
What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
D. Use 2 clusters +1st sync + 2nd sync

Answer:

B

NEW QUESTION 561
- (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 562
- (Exam Topic 4)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	Any	Any	Any	NBT	Drop	None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	Any	Any	dns	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	Any	Any	http https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	Any	ftp AP-Defender	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

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

A. This rule N
B. 6 has been marked for deletion in your Management session.
C. This rule N
D. 6 has been marked for deletion in another Management session.
E. This rule N
F. 6 has been marked for editing in your Management session.
G. This rule N
H. 6 has been marked for editing in another Management session.

Answer: C

NEW QUESTION 564
- (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 568
- (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 572
- (Exam Topic 4)
If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

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

Answer: D

NEW QUESTION 576
- (Exam Topic 4)
What is the correct order of the default “fw monitor” inspection points?

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

Answer: C

NEW QUESTION 579
- (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 581
- (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 585
- (Exam Topic 4)
When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

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

Answer: B

NEW QUESTION 587
- (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 592
- (Exam Topic 4)
What is the command used to activated Multi-Version Cluster mode?

A. set cluster member mvc on in Clish
B. set mvc on on Clish
C. set cluster MVC on in Expert Mode
D. set cluster mvc on in Expert Mode

Answer: A

NEW QUESTION 595
- (Exam Topic 4)

What is the default shell for the command line interface?

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

Answer: B

Explanation:
The default shell of the CLI is called clish References:

NEW QUESTION 600
- (Exam Topic 4)
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Use Multi-Domain Management Server.
B. Choose different setting for log storage and SmartEvent db
C. Install Management and SmartEvent on different machines.
D. it is not possible.

Answer: C

NEW QUESTION 602
- (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 605
- (Exam Topic 4)
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select “More”, and then check ‘Enable Identity Captive Portal’.
B. On the firewall object, Legacy Authentication screen, check ‘Enable Identity Captive Portal’.
C. In the Captive Portal screen of Global Properties, check ‘Enable Identity Captive Portal’.
D. On the Security Management Server object, check the box ‘Identity Logging’.

Answer: A

NEW QUESTION 609
- (Exam Topic 4)
What Is the difference between Updatable Objects and Dynamic Objects

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

Answer: B

NEW QUESTION 613
- (Exam Topic 4)
What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

A. Idle <20%
B. USR <20%
C. SYS <20%

D. Wait <20%

Answer: A

NEW QUESTION 614
- (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 616
- (Exam Topic 4)
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

A. Toni? AND 10.0.4.210 NOT 10.0.4.76
B. To** AND 10.0.4.210 NOT 10.0.4.76
C. Ton* AND 10.0.4.210 NOT 10.0.4.75
D. "Toni" AND 10.0.4.210 NOT 10.0.4.76

Answer: D

NEW QUESTION 620
- (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_Adress>
B. http://<Device IP_Address>:443
C. https://<Device_IP_Address>:10000
D. https://<Device_IP_Address>:4434

Answer: A

NEW QUESTION 623
- (Exam Topic 4)
The Check Point history feature in R81 provides the following:

A. View install changes and install specific version
B. View install changes
C. Policy Installation Date, view install changes and install specific version
D. Policy Installation Date only

Answer: D

NEW QUESTION 626
- (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 630
- (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 633
- (Exam Topic 4)
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and

which port is used?

A. In expert mode run #netstat -tulnp | grep httpd to see if httpd is up and to get the port numbe
B. In dish run >show web daemon-enable to see if the web daemon is enabled.
C. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in us
D. In expert mode run #netstat -anp | grep httpd to see if the httpd is up
E. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in us
F. In expert mode run #netstat -anp | grep httpd2 to see if the httpd2 is up
G. In expert mode run #netstat -tulnp | grep httpd2 to see if httpd2 is up and to get the port numbe
H. In dish run >show web daemon-enable to see if the web daemon is enabled.

Answer: C

NEW QUESTION 636
- (Exam Topic 4)
In Advanced Permanent Tunnel Configuration, to set the amount of time the tunnel test runs without a response before the peer host is declared 'down', you would set the ?

A. life sign polling interval
B. life sign timeout
C. life_sign_polling_interval
D. life_sign_timeout

Answer: D

Explanation:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm? topic=documents/R77/CP_R77_VPN_AdminGuide/14018

NEW QUESTION 640
- (Exam Topic 4)
What is the benefit of Manual NAT over Automatic NAT?

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

Answer: C

NEW QUESTION 642
- (Exam Topic 4)
What is Dynamic Balancing?

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

Answer: B

NEW QUESTION 645
- (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 646
- (Exam Topic 4)
To find records in the logs that shows log records from the Application & URL Filtering Software Blade where traffic was dropped, what would be the query syntax?

A. blada: application control AND action:drop
B. blade."application control AND action;drop
C. (blade: application control AND action;drop)
D. blade;"application control AND action:drop

Answer: D

NEW QUESTION 648
- (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 652
- (Exam Topic 4)
Which is the correct order of a log flow processed by SmartEvent components?

A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 656
- (Exam Topic 4)
SandBlast agent extends 0 day prevention to what part of the network?

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

Answer: A

NEW QUESTION 658
- (Exam Topic 4)
Main Mode in IKEv1 uses how many packages for negotiation?

A. 4
B. depends on the make of the peer gateway
C. 3
D. 6

Answer: C

NEW QUESTION 659
- (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 660
- (Exam Topic 4)
What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?

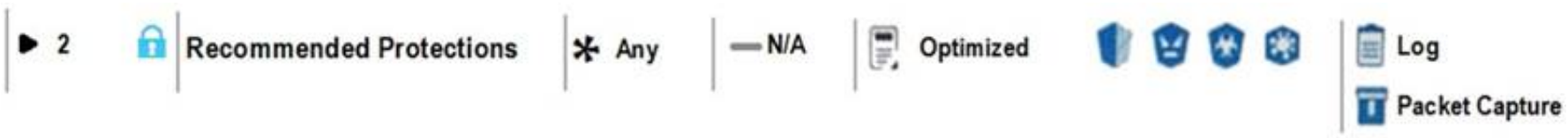
A. Manually, Scheduled, Automatic
B. Manually, Automatic, Disabled
C. Manually, Scheduled, Disabled
D. Manually, Scheduled, Enabled

Answer: A

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 662
- (Exam Topic 4)
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)

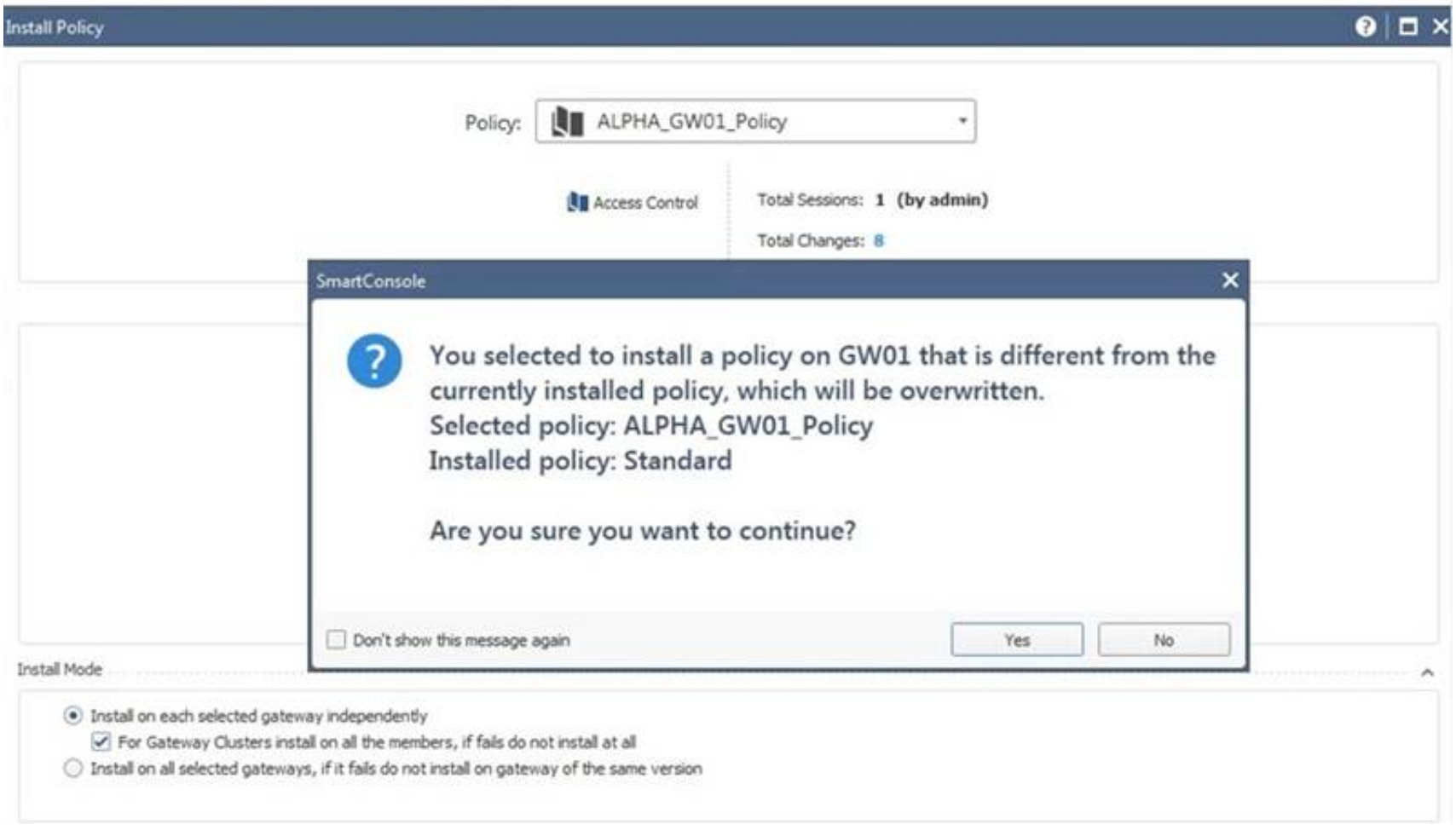


A. The current administrator has read-only permissions to Threat Prevention Policy.
B. Another user has locked the rule for editing.
C. Configuration lock is presen
D. Click the lock symbol to gain read-write access.
E. The current administrator is logged in as read-only because someone else is editing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

Answer: B

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

NEW QUESTION 663
- (Exam Topic 4)
Why would an administrator see the message below?



A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 668
- (Exam Topic 4)
What component of Management is used tor indexing?

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

Answer: D

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

NEW QUESTION 671
- (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 673
- (Exam Topic 4)
What API command below creates a new host object with the name "My Host" and IP address of "192 168 0 10"?

A. set host name "My Host" ip-address "192.168.0.10"
B. new host name "My Host" ip-address "192 168.0.10"
C. create host name "My Host" ip-address "192.168 0.10"
D. mgmt.cli -m <mgmt ip> add host name "My Host" ip-address "192.168.0 10"

Answer: A

NEW QUESTION 678
- (Exam Topic 4)
While using the Gaia CLI. what is the correct command to publish changes to the management server?

A. json publish
B. mgmt publish
C. mgmt_cli commit
D. commit

Answer: B

NEW QUESTION 683
- (Exam Topic 4)
You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Logging has disk space issue
B. Change logging storage options on the logging server or Security Management Server properties and install database.
C. Data Awareness is not enabled.
D. Identity Awareness is not enabled.
E. Logs are arriving from Pre-R81 gateways.

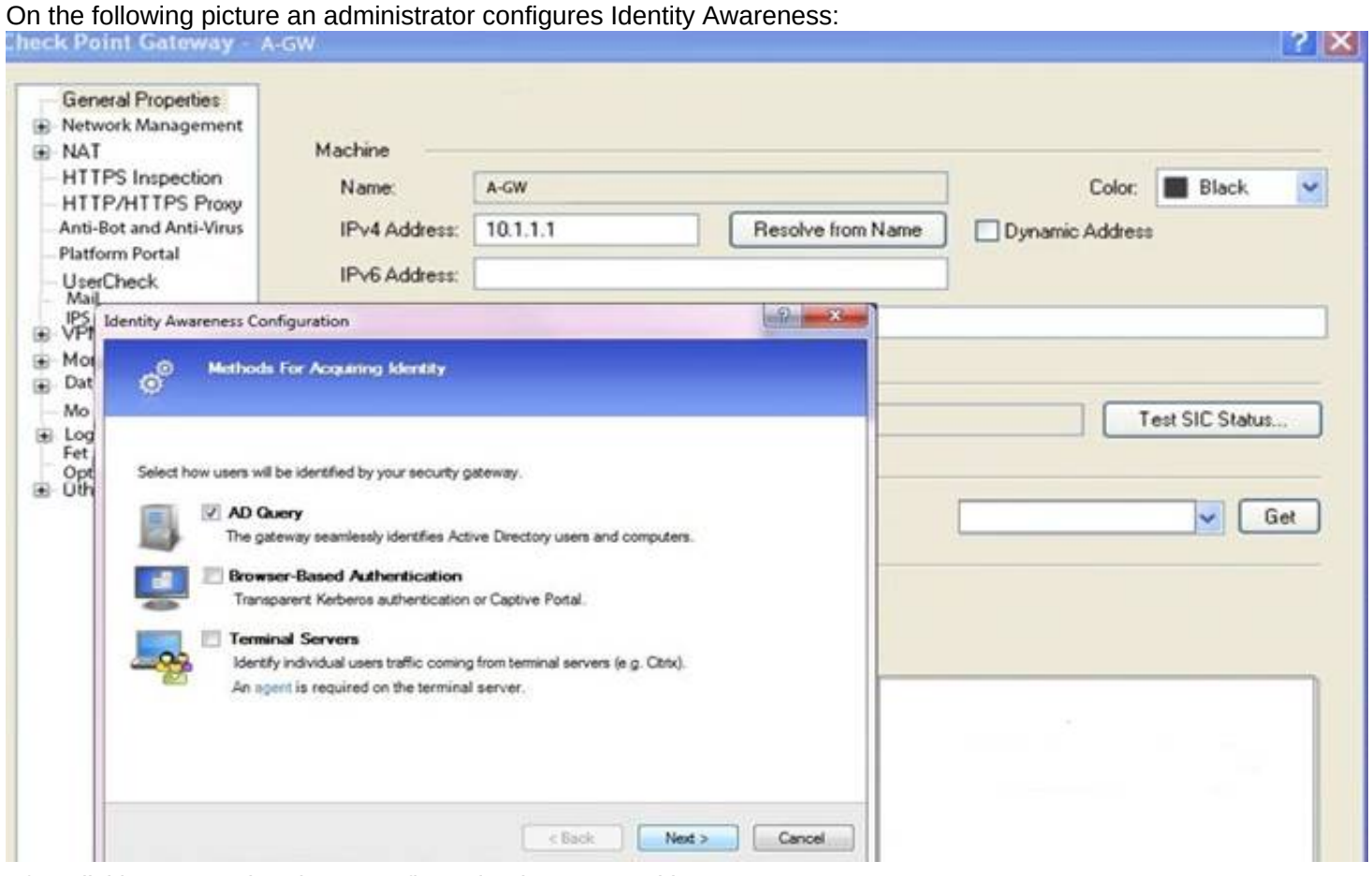
Answer: A

NEW QUESTION 688
- (Exam Topic 4)
Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

A. ReverseCLIProxy
B. ReverseProxyCLI
C. ReverseProxy
D. ProxyReverseCLI

Answer: C

NEW QUESTION 692
- (Exam Topic 4)
On the following picture an administrator configures Identity Awareness:



After clicking “Next” the above configuration is supported by:

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

Answer: B

NEW QUESTION 697
- (Exam Topic 4)
What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

A. CPUSE offline upgrade only
B. Advanced upgrade or CPUSE offline upgrade
C. Advanced Upgrade only
D. SmartUpdate offline upgrade

Answer: B

NEW QUESTION 698
- (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 switche
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 702
- (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 705
- (Exam Topic 4)
Which of the following is NOT an attribute of packet acceleration?

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

Answer: D

NEW QUESTION 706
- (Exam Topic 4)
What does Backward Compatibility mean upgrading the Management Server and how can you check it?

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

Answer: A

NEW QUESTION 710
- (Exam Topic 4)
The log server sends what to the Correlation Unit?

A. Authentication requests
B. CPMI dbsync
C. Logs

D. Event Policy

Answer: C

NEW QUESTION 714
- (Exam Topic 4)
What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

A. The corresponding feature is new to R81.10 and is called "Management Data Plane Separation"
B. The corresponding feature is called "Dynamic Dispatching"
C. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.
D. The corresponding feature is called "Dynamic Split"

Answer: A

NEW QUESTION 717
- (Exam Topic 4)
You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

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

Answer: A

NEW QUESTION 718
- (Exam Topic 4)
SmartConsole R81 x requires the following ports to be open for SmartEvent.

A. 19009, 19090 & 443
B. 19009, 19004 & 18190
C. 18190 & 443
D. 19009, 18190 & 443

Answer: D

NEW QUESTION 719
- (Exam Topic 4)
At what point is the Internal Certificate Authority (ICA) created?

A. Upon creation of a certificate.
B. During the primary Security Management Server installation process.
C. When an administrator decides to create one.
D. When an administrator initially logs into SmartConsole.

Answer: B

NEW QUESTION 721
- (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 723
- (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 725
- (Exam Topic 4)
Which Check Point software blade provides protection from zero-day and undiscovered threats?

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

Answer: B

NEW QUESTION 727
- (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 731
- (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 735
- (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 738
- (Exam Topic 4)
SmartEvent uses it's event policy to identify events. How can this be customized?

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

Answer: D

NEW QUESTION 742
- (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 747
- (Exam Topic 4)
Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

A. Security Gateway Clusters in Load Sharing mode
B. Dedicated Log Server
C. Dedicated SmartEvent Server
D. Security Gateways/Clusters in ClusterXL HA new mode

Answer: D

NEW QUESTION 752
- (Exam Topic 4)
What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

A. set config-lock on override
B. Click the Lock icon in the WebUI
C. "set rbac rw = 1"
D. lock database override

Answer: C

NEW QUESTION 757
- (Exam Topic 4)
Fill in the blank: _____ information is included in “Full Log” tracking option, but is not included in “Log” tracking option?

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

Answer: B

NEW QUESTION 758
- (Exam Topic 4)
Fill in the blank: Authentication rules are defined for _____ .

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

Answer: A

NEW QUESTION 759
- (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 763
- (Exam Topic 4)
Which is the command to identify the NIC dnver 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 766
- (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 770
- (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 773
- (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 XMfcfile and analysis of SOLR documents

Answer: D

NEW QUESTION 778
.....

Relate Links

100% Pass Your 156-315.81 Exam with Exambible Prep Materials

https://www.exambible.com/156-315.81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/