CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

A. Both License (.lic) and Contract (.xml) files
B. cp.macro
C. Contract file (.xml)
D. license File (.lie)

Answer: B

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

NEW QUESTION 2
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. RADIUS
B. Check Point password
C. Security questions
D. SecurID

Answer: C

NEW QUESTION 3
What are the two types of NAT supported by the Security Gateway?

A. Destination and Hide
B. Hide and Static
C. Static and Source
D. Source and Destination

Answer: B

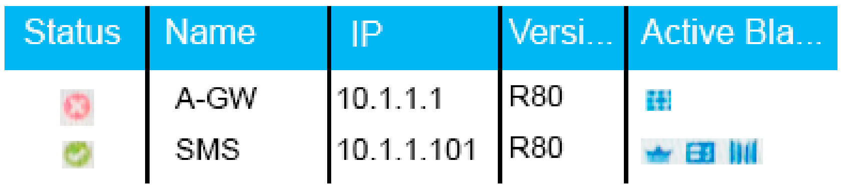
Explanation:
A Security Gateway can use these procedures to translate IP addresses in your network:

NEW QUESTION 4
In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

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

Answer: B

NEW QUESTION 5
What does it mean if Deyra sees the gateway status:



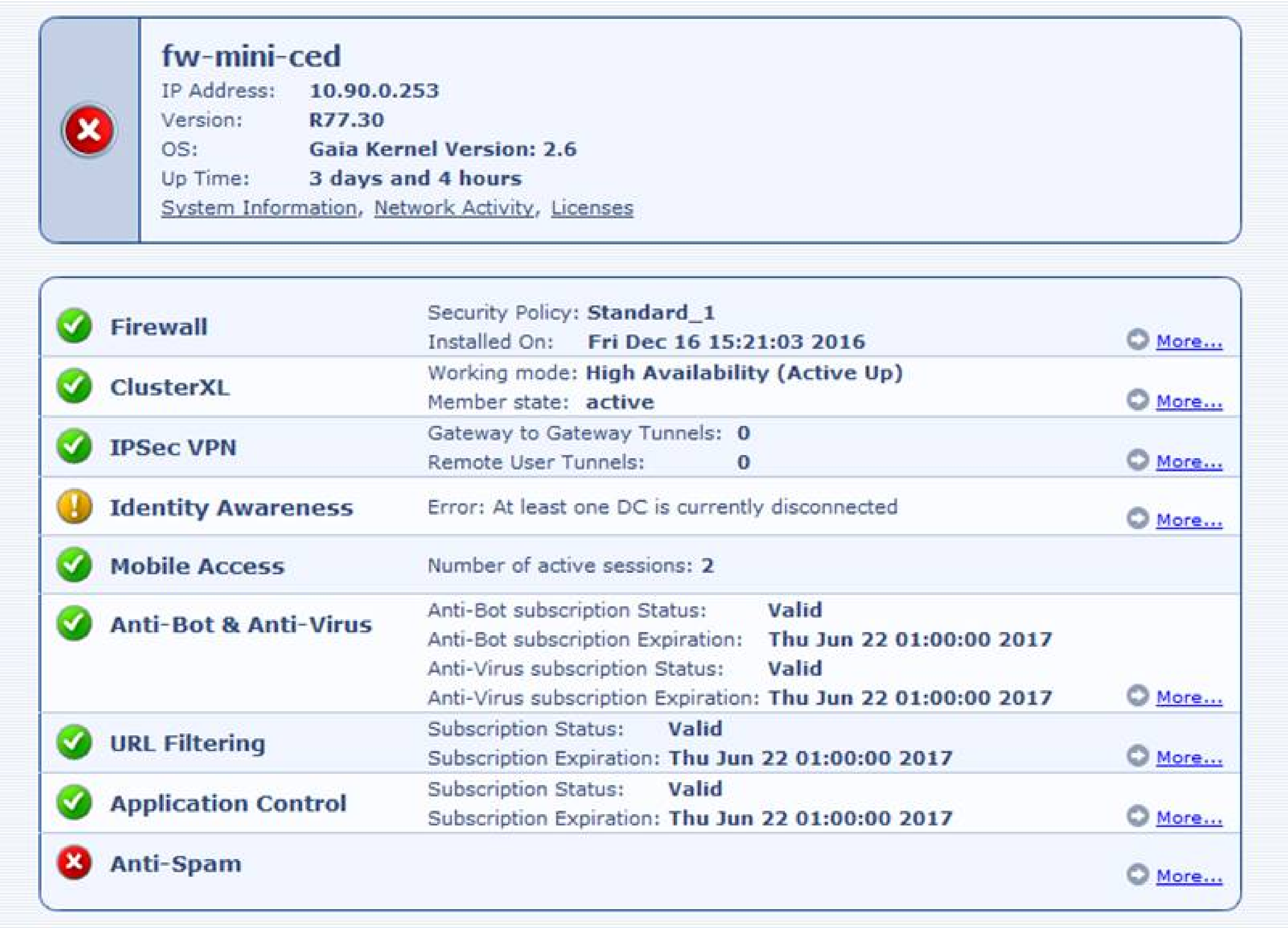
Status	Name	IP	Versi...	Active Bla...
✗	A-GW	10.1.1.1	R80	▦
✓	SMS	10.1.1.101	R80	▦ ▦ ▦

Choose the BEST answer.

A. SmartCenter Server cannot reach this Security Gateway
B. There is a blade reporting a problem
C. VPN software blade is reporting a malfunction
D. Security Gateway’s MGNT NIC card is disconnected.

Answer: B

Explanation:



✗ **fw-mini-ced**

IP Address:	**10.90.0.253**
Version:	**R77.30**
OS:	**Gaia Kernel Version: 2.6**
Up Time:	**3 days and 4 hours**

System Information, Network Activity, Licenses

✓	**Firewall**	Security Policy: **Standard_1** Installed On: **Fri Dec 16 15:21:03 2016**	More...
✓	**ClusterXL**	Working mode: **High Availability (Active Up)** Member state: **active**	More...
✓	**IPSec VPN**	Gateway to Gateway Tunnels: **0** Remote User Tunnels: **0**	More...
!	**Identity Awareness**	Error: At least one DC is currently disconnected	More...
✓	**Mobile Access**	Number of active sessions: **2**	
✓	**Anti-Bot & Anti-Virus**	Anti-Bot subscription Status: **Valid** Anti-Bot subscription Expiration: **Thu Jun 22 01:00:00 2017** Anti-Virus subscription Status: **Valid** Anti-Virus subscription Expiration: **Thu Jun 22 01:00:00 2017**	More...
✓	**URL Filtering**	Subscription Status: **Valid** Subscription Expiration: **Thu Jun 22 01:00:00 2017**	More...
✓	**Application Control**	Subscription Status: **Valid** Subscription Expiration: **Thu Jun 22 01:00:00 2017**	More...
✗	**Anti-Spam**		More...

NEW QUESTION 6
Which of the following is NOT a component of a Distinguished Name?

A. Common Name
B. Country
C. User container
D. Organizational Unit

Answer: C

NEW QUESTION 7
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. 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 8
Fill in the blank: The ______ feature allows administrators to share a policy with other policy packages.

A. Concurrent policy packages
B. Concurrent policies
C. Global Policies
D. Shared policies

Answer: D

Explanation:
"The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

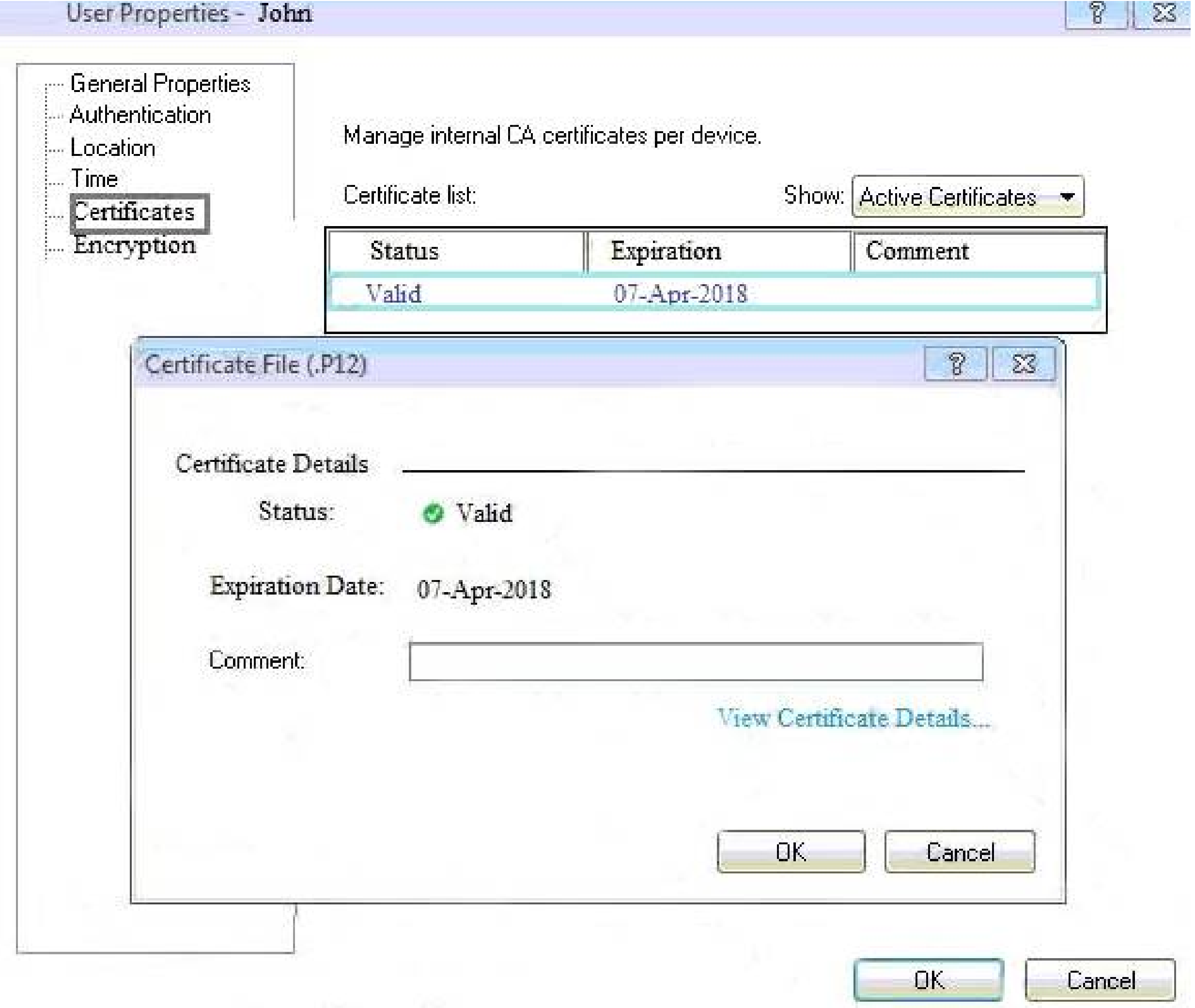
NEW QUESTION 9
When enabling tracking on a rule, what is the default option?

A. Accounting Log
B. Extended Log

C. Log
D. Detailed Log

Answer: C

NEW QUESTION 10
You can see the following graphic:



User Properties - John

Manage internal CA certificates per device.

Certificate list:

Show: Active Certificates

Status	Expiration	Comment
Valid	07-Apr-2018	

Certificate File (.P12)

Certificate Details

Status: Valid

Expiration Date: 07-Apr-2018

Comment:

What is presented on it?

A. Properties of personal .p12 certificate file issued for user John.
B. Shared secret properties of John’s password.
C. VPN certificate properties of the John’s gateway.
D. Expired .p12 certificate properties for user John.

Answer: A

NEW QUESTION 10
You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

A. Open SmartLog and connect remotely to the wireless controller
B. Open SmartEvent to see why they are being blocked
C. Open SmartDashboard and review the logs tab
D. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.

Answer: D

NEW QUESTION 14
What is the purpose of the CPCA process?

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

Answer: D

NEW QUESTION 18
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 21

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

A. Cache the data to speed up its own function.
B. Share the data to the ThreatCloud for use by other Threat Prevention blades.
C. Log the traffic for Administrator viewing.
D. Delete the data to ensure an analysis of the data is done each time.

Answer: B

Explanation:
Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades. src https://infosec.co.il/wp-content/uploads/2020/06/12-GAiA-R80.40-Threat-Prevention.pdf page 28.

NEW QUESTION 26
John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

A. Logout of the session
B. File > Save
C. Install database
D. Publish the session

Answer: D

Explanation:
Installing and Publishing
It is important to understand the differences between publishing and installing. You must do this:
After you did this: Publish
Opened a session in SmartConsole and made changes.
The Publish operation sends all SmartConsole modifications to other administrators, and makes the changes you made in a private session public.
Install the database
Modified network objects, such as servers, users, services, or IPS profiles, but not the Rule Base. Updates are installed on management servers and log servers.
Install a policy Changed the Rule Base.
The Security Management Server installs the updated policy and the entire database on Security Gateways (even if you did not modify any network objects).

NEW QUESTION 31
Which single Security Blade can be turned on to block both malicious files from being downloaded as well as block websites known to host malware?

A. Anti-Bot
B. None - both Anti-Virus and Anti-Bot are required for this
C. Anti-Virus
D. None - both URL Filtering and Anti-Virus are required for this.

Answer: C

Explanation:
Prevent Access to Malicious Websites
The Antivirus Software Blade scans outbound URL requests and ensures users do not visit websites that are known to distribute malware.
Stop Incoming Malicious Files
Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network.
https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf

NEW QUESTION 35
In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT _________.

A. Upgrade the software version
B. Open WebUI
C. Open SSH
D. Open service request with Check Point Technical Support

Answer: C

NEW QUESTION 37
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

Answer: C

NEW QUESTION 38
What is the main difference between Static NAT and Hide NAT?

A. Static NAT only allows incoming connections to protect your network.

B. Static NAT allow incoming and outgoing connection
C. Hide NAT only allows outgoing connections.
D. Static NAT only allows outgoing connection
E. Hide NAT allows incoming and outgoing connections.
F. Hide NAT only allows incoming connections to protect your network.

Answer: B

Explanation:
Hide NAT only translates the source address to hide it behind a gateway.

NEW QUESTION 42
Fill in the blanks: The _______ collects logs and sends them to the _______.

A. Log server; Security Gateway
B. Log server; security management server
C. Security management server; Security Gateway
D. Security Gateways; log server

Answer: D

Explanation:
Gateways send their logs to the log server.

NEW QUESTION 45
Which two Identity Awareness daemons are used to support identity sharing?

A. Policy Activation Point (PAP) and Policy Decision Point (PDP)
B. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
C. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
D. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)

Answer: D

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

NEW QUESTION 47
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

NEW QUESTION 48
Can multiple administrators connect to a Security Management Server at the same time?

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

Answer: C

NEW QUESTION 53
In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?

A. "Inspect", "Bypass"
B. "Inspect", "Bypass", "Categorize"
C. "Inspect", "Bypass", "Block"
D. "Detect", "Bypass"

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 57
What is the BEST method to deploy Identity Awareness for roaming users?

A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways

D. Use captive portal

Answer: B

Explanation:
Using Endpoint Identity Agents give you:

NEW QUESTION 59
Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

Answer: D

NEW QUESTION 60
In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

A. Logging & Monitoring
B. None - the data is available by default
C. Monitoring Blade
D. SNMP

Answer: C

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

NEW QUESTION 64
What is the default tracking option of a rule?

A. Tracking
B. Log
C. None
D. Alert

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 68
SmartEvent does NOT use which of the following procedures to identity 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

NEW QUESTION 69
Which is a suitable command to check whether Drop Templates are activated or not?

A. fw ctl get int activate_drop_templates
B. fwaccel stat
C. fwaccel stats
D. fw ctl templates –d

Answer: B

NEW QUESTION 71
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don’t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 76
Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

A. SmartEvent
B. SmartView Tracker
C. SmartLog
D. SmartView Monitor

Answer: A

Explanation:
https://www.checkpoint.com/downloads/products/smartevent-datasheet.pdf

NEW QUESTION 78
Where is the “Hit Count” feature enabled or disabled in SmartConsole?

A. On the Policy Package
B. On each Security Gateway
C. On the Policy layer
D. In Global Properties for the Security Management Server

Answer: B

Explanation:
References:

NEW QUESTION 81
Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish and install the policy.
B. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.
C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.
D. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway’s external IP.3. Publish the policy.

Answer: C

NEW QUESTION 82
What Identity Agent allows packet tagging and computer authentication?

A. Endpoint Security Client
B. Full Agent
C. Light Agent
D. System Agent

Answer: B

Explanation:
Identity Agent Description Full
Default Identity AgentClosed that includes packet tagging and computer authentication. It applies to all users on the computer on which it is installed. Administrator permissions are required to use the Full Identity Agent type. For the Full Identity Agent, you can enforce IP spoofing protection. In addition, you can leverage computer authentication if you specify computers in Access Roles.
Light
Default Identity Agent that does not include packet tagging and computer authentication. You can install this Identity Agent individually for each user on the target computer. Light Identity Agent type does not require Administrator permissions.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 85
What is a reason for manual creation of a NAT rule?

A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway’s external IP

Answer: D

NEW QUESTION 90
Which of the following is a new R80.10 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 are 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 93
What is the purpose of Captive Portal?

A. It manages user permission in SmartConsole
B. It provides remote access to SmartConsole
C. It authenticates users, allowing them access to the Internet and corporate resources
D. It authenticates users, allowing them access to the Gaia OS

Answer: C

Explanation:
Captive Portal is a simple method that authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminG

NEW QUESTION 95
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 97
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 100
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 101
In which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to a 2200 Appliance
B. From a 4400 Appliance to an HP Open Server
C. From an IBM Open Server to an HP Open Server
D. From an IBM Open Server to a 2200 Appliance

Answer: A

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

NEW QUESTION 103
What two ordered layers make up the Access Control Policy Layer?

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

Answer: D

NEW QUESTION 104
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 even if the Track option is set to “None”?

A. No, it will not work independentl
B. Hit Count will be shown only for rules with Track options 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 107
Which of the following commands is used to verify license installation?

A. Cplic verify license
B. Cplic print
C. Cplic show
D. Cplic license

Answer: B

NEW QUESTION 110
Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

A. IPS blade
B. IPSEC VPN Blade
C. Identity Awareness Blade
D. Firewall Blade

Answer: A

NEW QUESTION 111
Fill in the blank: When a policy package is installed, _______ are also distributed to the target installation Security Gateways.

A. User and objects databases
B. Network databases
C. SmartConsole databases
D. User databases

Answer: A

Explanation:
A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:
The installation process:
If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

NEW QUESTION 112
Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

A. Application Control
B. Threat Emulation
C. Logging and Status
D. Monitoring

Answer: D

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

NEW QUESTION 115
What is the purpose of a Stealth Rule?

A. A rule used to hide a server's IP address from the outside world.
B. A rule that allows administrators to access SmartDashboard from any device.
C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

Answer: C

NEW QUESTION 118
Fill in the blank: Each cluster, at a minimum, should have at least _______ interfaces.

A. Five
B. Two
C. Three
D. Four

Answer: C

NEW QUESTION 121
One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
B. AdminA and AdminB are editing the same rule at the same time.
C. AdminB sees a pencil icon next the rule that AdminB is currently editing.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: B

NEW QUESTION 122
Which of the following is used to extract state related information from packets and store that information in state tables?

A. STATE Engine
B. TRACK Engine
C. RECORD Engine
D. INSPECT Engine

Answer: D

Explanation:
Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over.
It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts.

NEW QUESTION 123
When dealing with rule base layers, what two layer types can be utilized?

A. Ordered Layers and Inline Layers
B. Inbound Layers and Outbound Layers
C. R81.10 does not support Layers
D. Structured Layers and Overlap Layers

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 124
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 125
When configuring LDAP with User Directory integration, changes applied to a User Directory template are:

A. Not reflected for any users unless the local user template is changed.
B. Not reflected for any users who are using that template.
C. Reflected for ail users who are using that template and if the local user template is changed as well.
D. Reflected immediately for all users who are using that template.

Answer: D

Explanation:
You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 127
Where can administrator edit a list of trusted SmartConsole clients?

A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
B. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
C. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients, via cpconfig on a Security Gateway.
D. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.

Answer: B

NEW QUESTION 132
Which of the following commands is used to monitor cluster members in CLI?

A. show cluster state
B. show active cluster
C. show clusters
D. show running cluster

Answer: A

NEW QUESTION 134
What kind of NAT enables Source Port Address Translation by default?

A. Automatic Static NAT
B. Manual Hide NAT
C. Automatic Hide NAT
D. Manual Static NAT

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 138
The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?

A. The SmartLicensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.
D. The cpinfo command must be run on the firewall with the switch -online-license-activation.

Answer: C

Explanation:
"Online activation: this method of activation is available for Check Point manufactured appliances. These appliances should be configured to have internet connectivity during the completion of the First Time Configuration Wizard for software version R77 and below. Customers using R80 and higher will be able to use this feature during or after the completion of the First Time Configuration Wizard."
https://supportcenter.checkpoint.com/supportcenter/portal?eventsubmit_dogoviewsolutiondetails=&solutionid=s

NEW QUESTION 143
Which two of these Check Point Protocols are used by ?

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

Answer: B

NEW QUESTION 146
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 enable which path is handling the traffic?

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

Answer: A

NEW QUESTION 150
When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packer Filtering?

A. Stateful Inspection offers unlimited connections because of virtual memory usage.
B. Stateful Inspection offers no benefits over Packet Filtering.
C. Stateful Inspection does not use memory to record the protocol used by the connection.
D. Only one rule is required for each connection.

Answer: D

NEW QUESTION 152
Which of the following is used to initially create trust between a Gateway and Security Management Server?

A. Internal Certificate Authority
B. Token
C. One-time Password
D. Certificate

Answer: C

Explanation:
To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 154
You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

A. backup
B. logswitch
C. Database Revision
D. snapshot

Answer: D

Explanation:
The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.
Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.
The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 155
Which icon in the WebUI indicates that read/write access is enabled?

A. Pencil
B. Padlock
C. Book
D. Eyeglasses

Answer: A

NEW QUESTION 160
To view the policy installation history for each gateway, which tool would an administrator use?

A. Revisions
B. Gateway installations
C. Installation history
D. Gateway history

Answer: C

NEW QUESTION 161
True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

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

Answer: B

Explanation:
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

NEW QUESTION 165
Is it possible to have more than one administrator connected to a Security Management Server at once?

A. Yes, but only if all connected administrators connect with read-only permissions.
B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
C. No, only one administrator at a time can connect to a Security Management Server
D. Yes, but only one of those administrators will have write-permission
E. All others will have read-only permission.

Answer: B

NEW QUESTION 167
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 170
What Check Point technologies deny or permit network traffic?

A. Application Control, DLP
B. Packet Filtering, Stateful Inspection, Application Layer Firewall.
C. ACL, SandBlast, MPT
D. IPS, Mobile Threat Protection

Answer: B

NEW QUESTION 174
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up
B. There is Load Sharing solution set up
C. Only when there is Unicast solution set up
D. There is High Availability solution set up

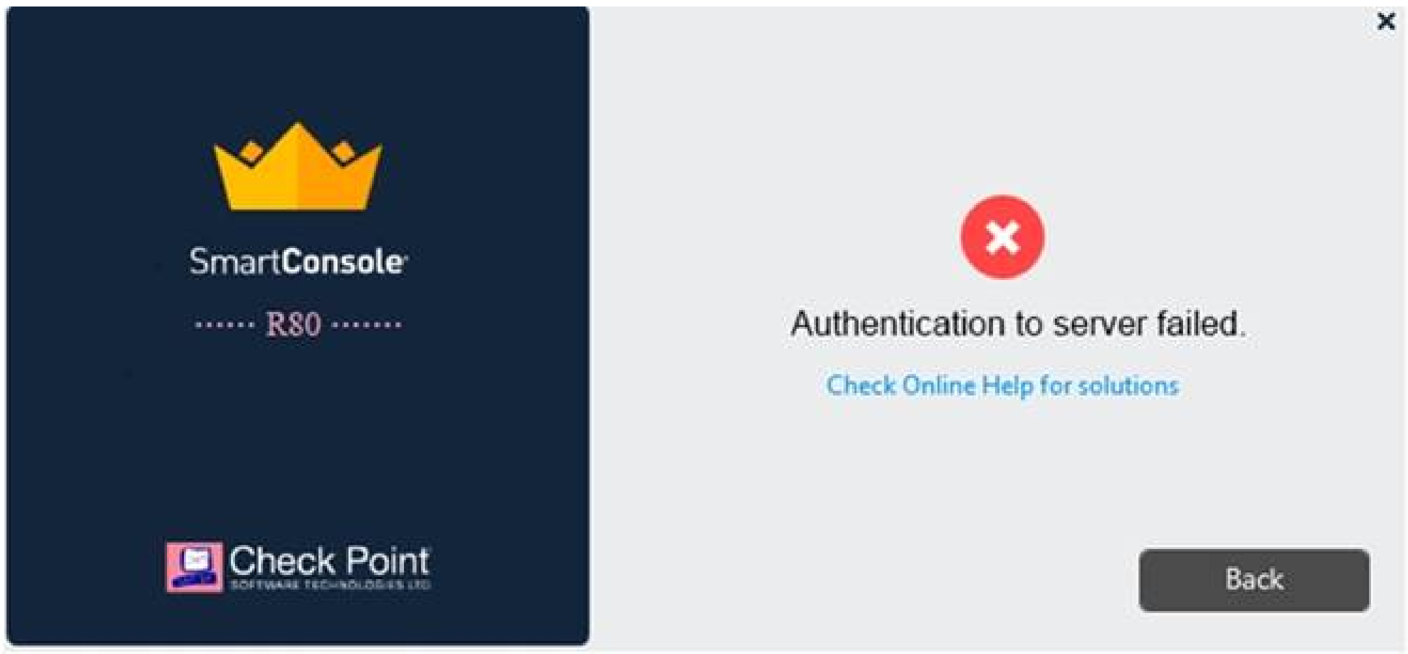
Answer: D

NEW QUESTION 177
When changes are made to a Rule base, it is important to _______ to enforce changes.

A. Publish database
B. Activate policy
C. Install policy
D. Save changes

Answer: C

NEW QUESTION 179
Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



Authentication to server failed.

Check Online Help for solutions

What is the most likely reason?

A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsol
B. Check that the correct key details are used.
C. Check Point Management software authentication details are not automatically the same as the Operating System authentication detail
D. Check that she is using the correct details.
E. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
F. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Answer: B

NEW QUESTION 184
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

A. Remote Access
B. Cloud IdP (Identity Provider)
C. Active Directory Query

D. RADIUS

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 185
There are four policy types available for each policy package. What are those policy types?

A. Access Control, Threat Prevention, Mobile Access and HTTPS Inspection
B. Access Control, Custom Threat Prevention, Autonomous Threat Prevention and HTTPS Inspection
C. There are only three policy types: Access Control, Threat Prevention and NAT.
D. Access Control, Threat Prevention, NAT and HTTPS Inspection

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 187
A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

A. The zone is based on the network topology and determined according to where the interface leads to.
B. Security Zones are not supported by Check Point firewalls.
C. The firewall rule can be configured to include one or more subnets in a zone.
D. The local directly connected subnet defined by the subnet IP and subnet mask.

Answer: A

Explanation:
The Interface window opens. The Topology area of the General pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface Leads To.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 189
A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _________ .

A. Two; Security Management and Endpoint Security
B. Two; Endpoint Security and Security Gateway
C. Three; Security Management, Security Gateway, and Endpoint Security
D. Three; Security Gateway, Endpoint Security, and Gateway Management

Answer: C

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref:
https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 193
Which of the following technologies extracts detailed information from packets and stores that information in state tables?

A. INSPECT Engine
B. Next-Generation Firewall
C. Packet Filtering
D. Application Layer Firewall

Answer: A

Explanation:
Check Point FireWall-1's Stateful Inspection overcomes the limitations of the previous two approaches by providing full application-layer awareness without breaking the client/server model. With Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over. It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. This provides a solution which is highly secure and offers maximum performance, scalability, and extensibility.

NEW QUESTION 196
Which of the following is NOT supported by Bridge Mode on the Check Point Security Gateway?

A. Data Loss Prevention
B. Antivirus
C. Application Control
D. NAT

Answer: D

Explanation:

NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 201
When using Automatic Hide NAT, what is enabled by default?

A. Source Port Address Translation (PAT)
B. Static NAT
C. Static Route
D. HTTPS Inspection

Answer: A

Explanation:
Hiding multiple IP addresses behind one, gateway, IP address requires PAT to differentiate between traffic.

NEW QUESTION 204
Which GUI tool can be used to view and apply Check Point licenses?

A. cpconfig
B. Management Command Line
C. SmartConsole
D. SmartUpdate

Answer: D

Explanation:
SmartUpdate GUI is the recommended way of managing licenses.

NEW QUESTION 209
Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

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

Answer: C

NEW QUESTION 211
What default layers are included when creating a new policy layer?

A. Application Control, URL Filtering and Threat Prevention
B. Access Control, Threat Prevention and HTTPS Inspection
C. Firewall, Application Control and IPSec VPN
D. Firewall, Application Control and IPS

Answer: B

NEW QUESTION 214
When a Security Gateway sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge Mode
D. Targeted

Answer: A

NEW QUESTION 217
What object type would you use to grant network access to an LDAP user group?

A. Access Role
B. User Group
C. SmartDirectory Group
D. Group Template

Answer: B

NEW QUESTION 218
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 221
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R80 configuration, clean install R80.10 and import the configuration
B. CPUSE online upgrade
C. CPUSE offline upgrade
D. SmartUpdate upgrade

Answer: C

NEW QUESTION 223
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 (clash)19+
D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 228
Which default Gaia user has full read/write access?

A. admin
B. superuser
C. monitor
D. altuser

Answer: A

Explanation:
Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish. This user has a User ID of 0, and therefore has all of the privileges of a root user. monitor Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 232
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 (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?

A. The Gateway is an SMB device
B. The checkbox “Use only Shared Secret for all external members” is not checked
C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS
D. Pre-shared secret is already configured in Global Properties

Answer: C

NEW QUESTION 237
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: B

NEW QUESTION 238
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 240
Fill in the blank: It is Best Practice to have a _____ rule at the end of each policy layer.

A. Explicit Drop
B. Implied Drop
C. Explicit CleanUp
D. Implicit Drop

Answer: C

NEW QUESTION 245
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 249
Which of the following is the most secure means of authentication?

A. Password
B. Certificate
C. Token
D. Pre-shared secret

Answer: B

NEW QUESTION 254
In which deployment is the security management server and Security Gateway installed on the same appliance?

A. Standalone
B. Remote
C. Distributed
D. Bridge Mode

Answer: A

Explanation:
https://www.youtube.com/watch?v=BFNnBKQz5HA

NEW QUESTION 258
The SIC Status “Unknown” means

A. There is connection between the gateway and Security Management Server but it is not trusted.
B. The secure communication is established.
C. There is no connection between the gateway and Security Management Server.
D. The Security Management Server can contact the gateway, but cannot establish SIC.

Answer: C

Explanation:
SIC Status
After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

NEW QUESTION 261
What is the most recommended installation method for Check Point appliances?

A. SmartUpdate installation
B. DVD media created with Check Point ISOMorphic
C. USB media created with Check Point ISOMorphic
D. Cloud based installation

Answer: C

NEW QUESTION 266
In which scenario will an administrator need to manually define Proxy ARP?

A. When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
B. When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
C. When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
D. When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.

Answer: C

NEW QUESTION 271

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

A. Application Control
B. Data Awareness
C. Identity Awareness
D. Threat Emulation

Answer: A

NEW QUESTION 272
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

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

Answer: A

NEW QUESTION 275
Which of the following is NOT an advantage to using multiple LDAP servers?

A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
B. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
C. Information on a user is hidden, yet distributed across several servers.
D. You gain High Availability by replicating the same information on several servers

Answer: C

NEW QUESTION 280
Most Check Point deployments use Gaia but which product deployment utilizes special Check Point code (with unification in R81.10)?

A. Enterprise Network Security Appliances
B. Rugged Appliances
C. Scalable Platforms
D. Small Business and Branch Office Appliances

Answer: A

NEW QUESTION 283
Security Zones do no work with what type of defined rule?

A. Application Control rule
B. Manual NAT rule
C. IPS bypass rule
D. Firewall rule

Answer: B

Explanation:
https://community.checkpoint.com/t5/Management/Workaround-for-manual-NAT-when-security-zones-are-use

NEW QUESTION 284
What are the three deployment considerations for a secure network?

A. Distributed, Bridge Mode, and Remote
B. Bridge Mode, Remote, and Standalone
C. Remote, Standalone, and Distributed
D. Standalone, Distributed, and Bridge Mode

Answer: A

NEW QUESTION 285
Fill in the blank: An Endpoint identity agent uses a _______ for user authentication.

A. Shared secret
B. Token
C. Username/password or Kerberos Ticket
D. Certificate

Answer: C

Explanation:
Two ways of auth: Username/Password in Captive Portal or Transparent Kerberos Auth through Kerberos Ticket.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 287
Name the utility that is used to block activities that appear to be suspicious.

A. Penalty Box
B. Drop Rule in the rulebase
C. Suspicious Activity Monitoring (SAM)
D. Stealth rule

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG

NEW QUESTION 291
Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

A. Formal
B. Central
C. Corporate
D. Local

Answer: D

Explanation:
Local licensing is associated with the IP address of the Security Gateway, to which the license will be applied.
Each time the IP address of the Security Gateway changes, a new license must be generated and installed.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 295
To view statistics on detected threats, which Threat Tool would an administrator use?

A. Protections
B. IPS Protections
C. Profiles
D. ThreatWiki

Answer: D

NEW QUESTION 298
What are the three main components of Check Point security management architecture?

A. SmartConsole, Security Management, and Security Gateway
B. Smart Console, Standalone, and Security Management
C. SmartConsole, Security policy, and Logs & Monitoring
D. GUI-Client, Security Management, and Security Gateway

Answer: A

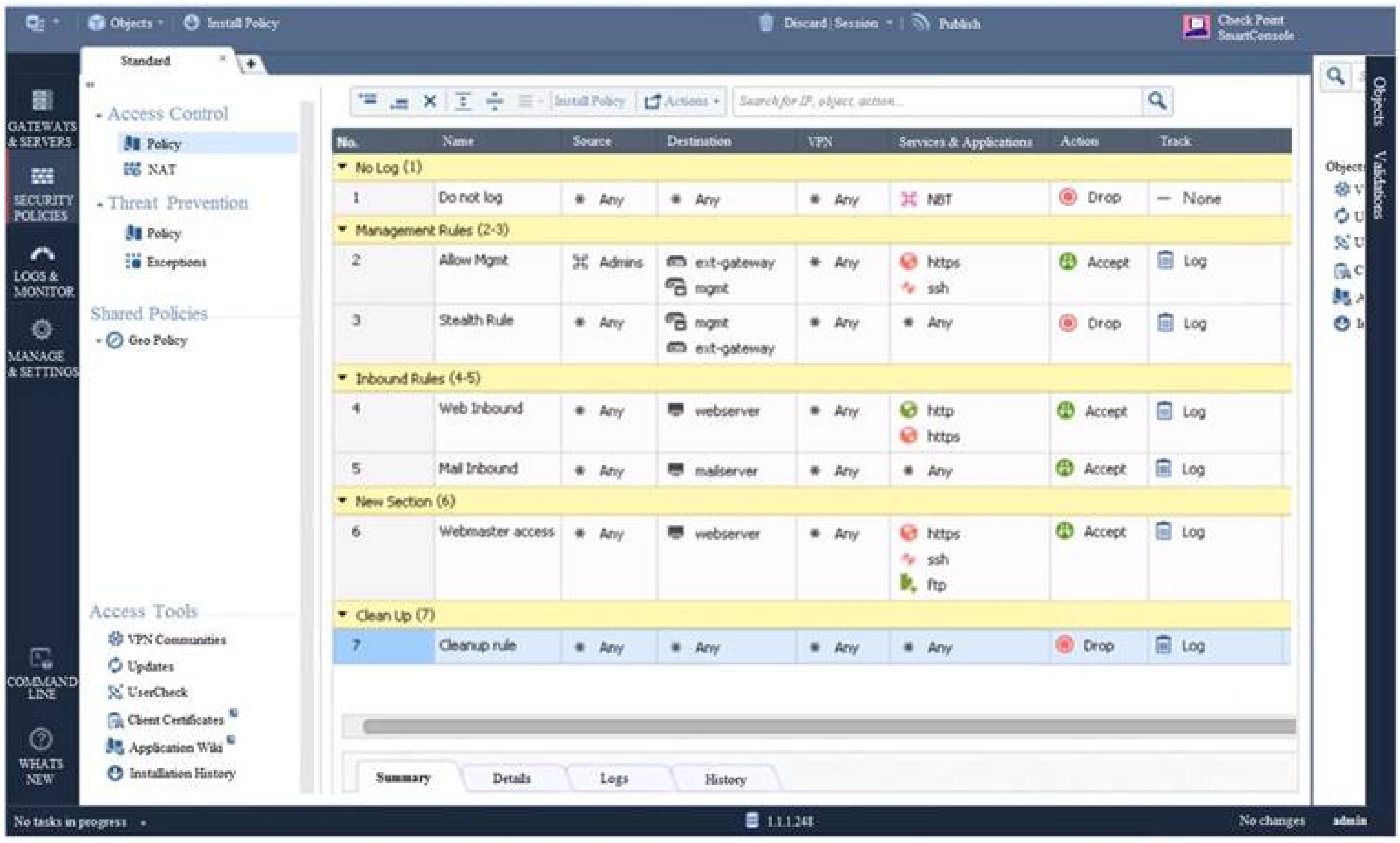
NEW QUESTION 299
When configuring Anti-Spoofing, which tracking options can an Administrator select?

A. Log, Alert, None
B. Log, Allow Packets, Email
C. Drop Packet, Alert, None
D. Log, Send SNMP Trap, Email

Answer: A

Explanation:
Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected: Log - Create a log entry (default)
Alert - Show an alert None - Do not log or alert
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 301
Examine the sample Rule Base.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept	Log
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	Any	webserver	Any	http https	Accept	Log
5	Mail Inbound	Any	mailserver	Any	Any	Accept	Log
New Section (6)							
6	Webmaster access	Any	webserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

What will be the result of a verification of the policy from SmartConsole?

A. No errors or Warnings
B. Verification Erro
C. Empty Source-List in Rule 5 (Mail Inbound)
D. Verification Erro
E. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)
F. Verification Erro
G. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

Answer: C

NEW QUESTION 306
What is the main difference between Threat Extraction and Threat Emulation?

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

Answer: B

NEW QUESTION 310
Fill in the blank: To create policy for traffic to or from a particular location, use the ______ .

A. DLP shared policy
B. Geo policy shared policy
C. Mobile Access software blade
D. HTTPS inspection

Answer: B

Explanation:
Shared Policies
The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. T are shared between all Policy packages.
Shared policies are installed with the Access Control Policy. Software Blade
Description Mobile Access
Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP
Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy
Create a policy for traffic to or from specific geographical or political locations.

NEW QUESTION 313
What is a role of Publishing?

A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
B. The Security Management Server installs the updated policy and the entire database on Security Gateways
C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

Answer: A

NEW QUESTION 315
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

Explanation:
The first rule is the automatic rule for the Accept All Encrypted Traffic feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.
* 2. Site to site VPN - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.
* 3. Remote access - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

NEW QUESTION 319
Identity Awareness allows the Security Administrator to configure network access based on which of the following?

A. Name of the application, identity of the user, and identity of the machine
B. Identity of the machine, username, and certificate
C. Network location, identity of a user, and identity of a machine
D. Browser-Based Authentication, identity of a user, and network location

Answer: C

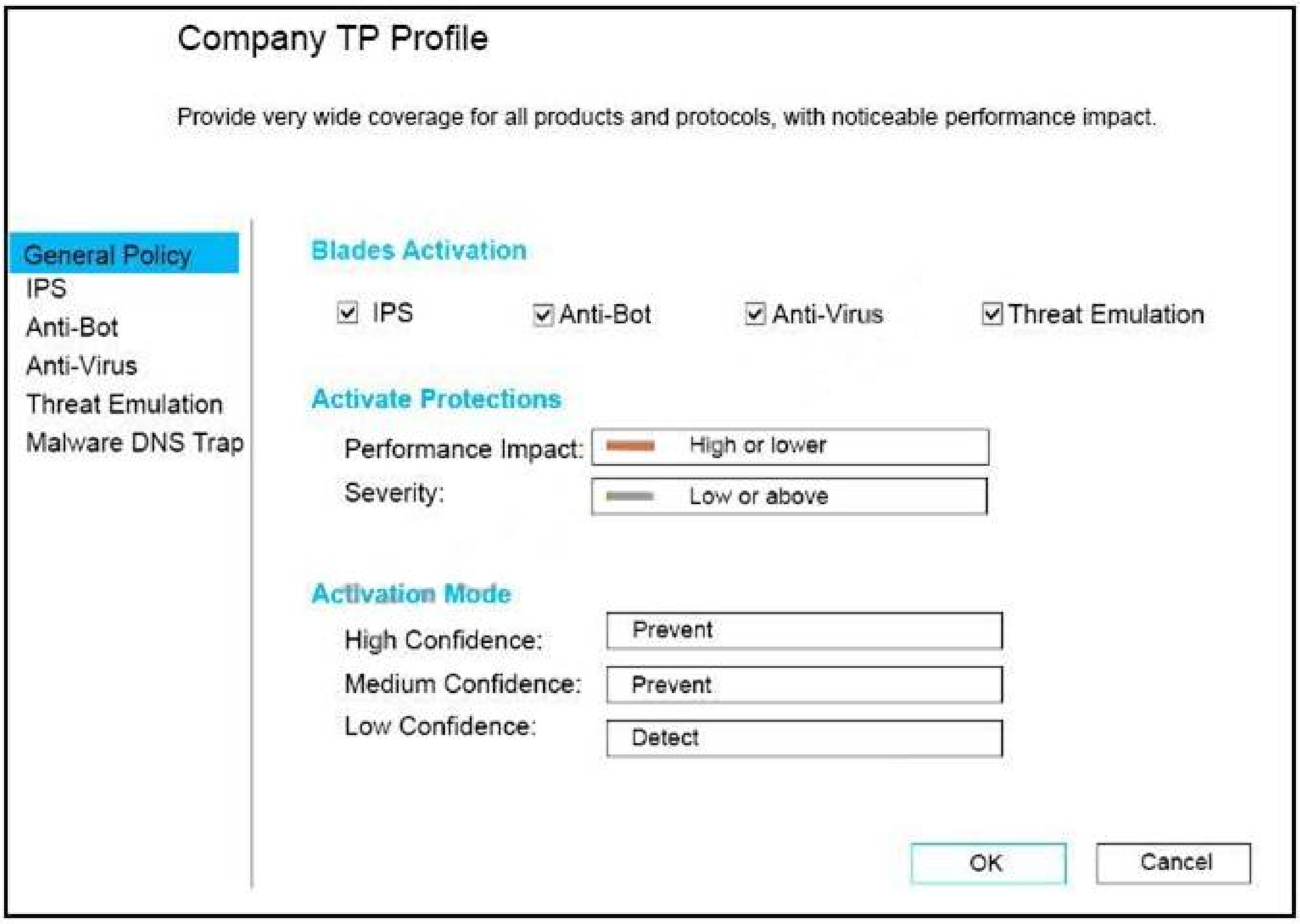
NEW QUESTION 320
Which policy type is used to enforce bandwidth and traffic control rules?

A. Access Control
B. Threat Emulation
C. Threat Prevention
D. QoS

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_fram

NEW QUESTION 322
CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings. The following Threat Prevention Profile has been created.



Company TP Profile

Provide very wide coverage for all products and protocols, with noticeable performance impact.

Blades Activation

☑ IPS ☑ Anti-Bot ☑ Anti-Virus ☑ Threat Emulation

Activate Protections

Performance Impact: High or lower
Severity: Low or above

Activation Mode

High Confidence: Prevent
Medium Confidence: Prevent
Low Confidence: Detect

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

A. Set High Confidence to Low and Low Confidence to Inactive.
B. Set the Performance Impact to Medium or lower.
C. The problem is not with the Threat Prevention Profil
D. Consider adding more memory to the appliance.
E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 327
The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal
Communication (SIC)?

A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 331
When using Monitored circuit VRRP, what is a priority delta?

A. When an interface fails the priority changes to the priority delta
B. When an interface fails the delta claims the priority
C. When an interface fails the priority delta is subtracted from the priority
D. When an interface fails the priority delta decides if the other interfaces takes over

Answer: C

NEW QUESTION 335
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 340
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

Explanation:
Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

NEW QUESTION 344
What is NOT an advantage of Stateful Inspection?

A. High Performance
B. Good Security
C. No Screening above Network layer
D. Transparency

Answer: A

NEW QUESTION 349
What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point INSPECT Engine
B. Check Point Upgrade Service Engine
C. Check Point Update Engine
D. Check Point Upgrade Installation Service

Answer: B

NEW QUESTION 353
Which of the following is NOT a policy type available for each policy package?

A. Threat Emulation
B. Access Control
C. Desktop Security
D. Threat Prevention

Answer: A

Explanation:
References:

NEW QUESTION 356
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade

Answer: B

NEW QUESTION 357
You want to verify if there are unsaved changes in GAiA that will be lost with a reboot. What command can be used?

A. show unsaved
B. show save-state
C. show configuration diff
D. show config-state

Answer: D

NEW QUESTION 362
When installing a dedicated R80 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 20 GB
D. At least 20GB

Answer: D

NEW QUESTION 363
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 366
Name the authentication method that requires token authenticator.

A. SecureID
B. Radius
C. DynamicID
D. TACACS

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 368
......