Exam Questions 156-215.81

Check Point Certified Security Administrator R81

https://www.2passeasy.com/dumps/156-215.81/

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
With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

A. The complete communication is sent for inspection.
B. The IP address of the source machine.
C. The end user credentials.
D. The host portion of the URL.

Answer: D

Explanation:
"A local cache that gives answers to 99% of URL categorization requests. When the cache does not have an answer, only the host name is sent to the Check Point Online Web Service for categorization. " https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/24853/FILE/CP_R77_ApplicationControlURL

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
When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

A. The URL and server certificate are sent to the Check Point Online Web Service
B. The full URL, including page data, is sent to the Check Point Online Web Service
C. The host part of the URL is sent to the Check Point Online Web Service
D. The URL and IP address are sent to the Check Point Online Web Service

Answer: C

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

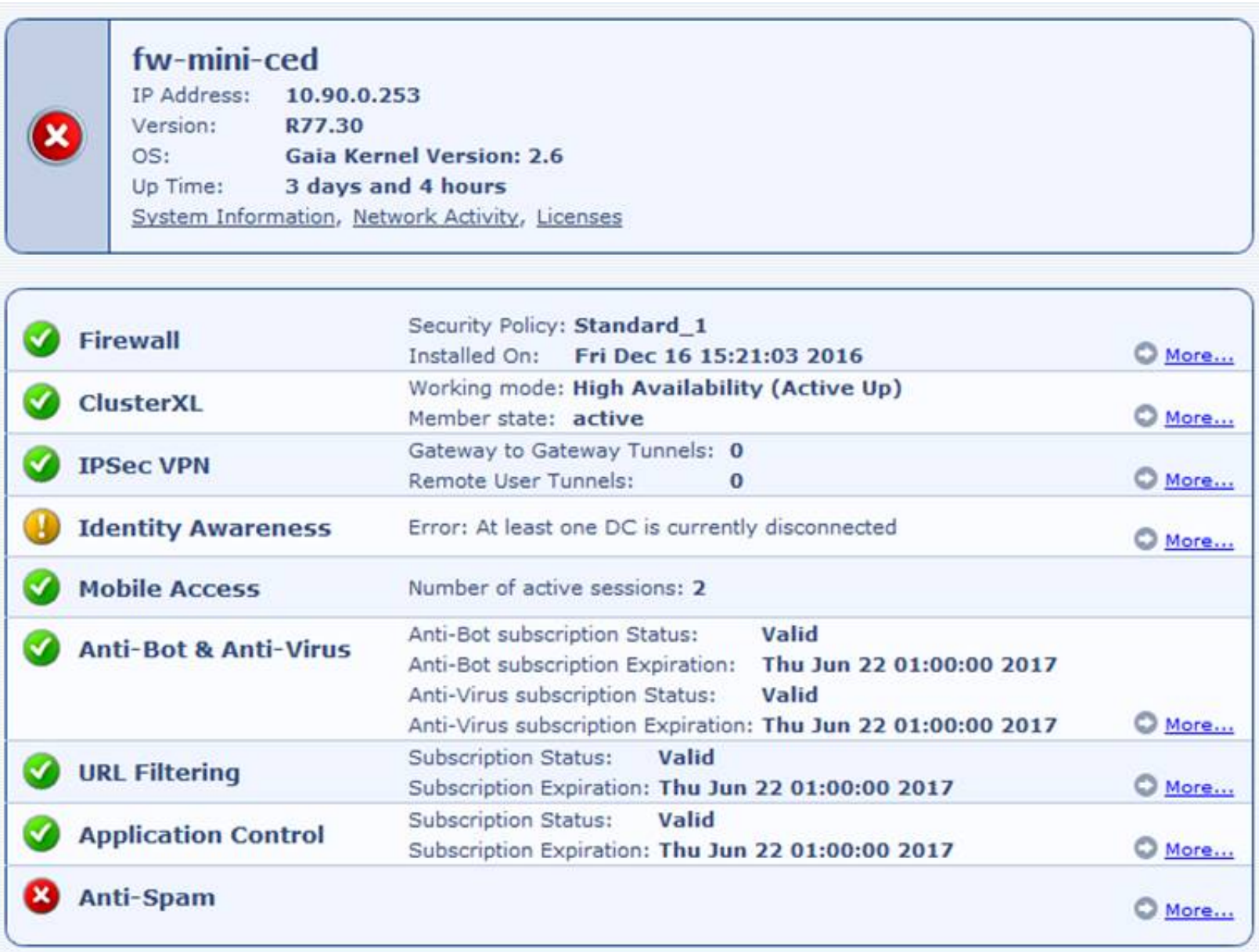
Status	Name	IP	Versi...	Active Bla...
	A-GW	10.1.1.1	R80	
	SMS	10.1.1.101	R80	

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:



NEW QUESTION 6
Fill in the blanks: Gaia can be configured using _____ the _____.

A. Command line interface; WebUI
B. Gaia Interface; GaiaUI
C. WebUI; Gaia Interface
D. GaiaUI; command line interface

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/C

NEW QUESTION 7
In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

A. Different computers or appliances.
B. The same computer or appliance.
C. Both on virtual machines or both on appliances but not mixed.
D. In Azure and AWS cloud environments.

Answer: A

Explanation:
"The Security Management ServerClosed (1) and the Security GatewayClosed (3) are installed on different computers, with a network connection (2)."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 8
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 9
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Createnew user with UID 0 and assign role to the user.
C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.

Answer: A

NEW QUESTION 10
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

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	Any	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	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
B. Another administrator is logged into the Management and currently editing the DNS Rule.
C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

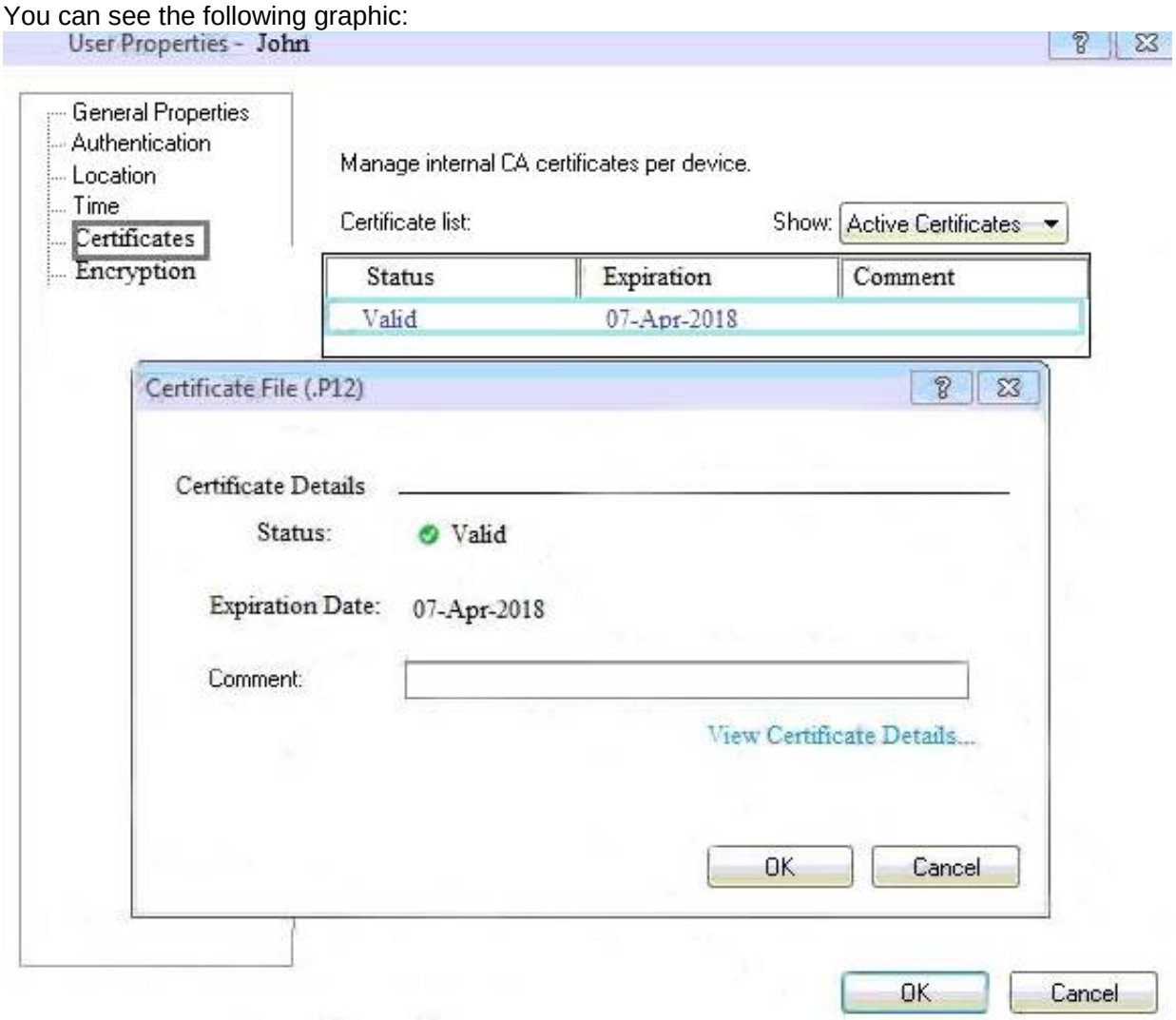
Answer: B

NEW QUESTION 10
Which one of the following is TRUE?

A. Ordered policy is a sub-policy within another policy
B. One policy can be either inline or ordered, but not both
C. Inline layer can be defined as a rule action
D. Pre-R80 Gateways do not support ordered layers

Answer: C

NEW QUESTION 14
You can see the following graphic:



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 19
What are the types of Software Containers?

A. Smart Console, Security Management, and Security Gateway
B. Security Management, Security Gateway, and Endpoint Security
C. Security Management, Log & Monitoring, and Security Policy
D. Security Management, Standalone, and Security Gateway

Answer: B

NEW QUESTION 22
What is the purpose of the Clean-up Rule?

A. To log all traffic that is not explicitly allowed or denied in the Rule Base
B. To clean up policies found inconsistent with the compliance blade reports
C. To remove all rules that could have a conflict with other rules in the database
D. To eliminate duplicate log entries in the Security Gateway

Answer: A

Explanation:
These are basic access control rules we recommend for all Rule Bases:
There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION 25
Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

A. 675, 389
B. 389, 636
C. 636, 290
D. 290, 675

Answer: B

Explanation:
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

NEW QUESTION 27
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

A. All options stop Check Point processes
B. backup
C. migrate export
D. snapshot

Answer: D

NEW QUESTION 30
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 32
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

A. IPS
B. Anti-Virus
C. Anti-Malware
D. Content Awareness

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To "Check Point Antivirus Software Blade prevents

and stops
threats such as malware, viruses, and Trojans from entering and infecting a network"
Also here -https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf

NEW QUESTION 33
John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 37
Identify the ports to which the Client Authentication daemon listens on by default?

A. 259, 900
B. 256, 257
C. 8080, 529
D. 80, 256

Answer: A

NEW QUESTION 39
Fill in the blank: Service blades must be attached to a _____.

A. Security Gateway
B. Management container
C. Management server
D. Security Gateway container

Answer: A

NEW QUESTION 40
How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

A. Involved traffic logs will be forwarded to a log server.
B. Provides log details view email to the Administrator.
C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.
D. Provides additional information to the connected user.

Answer: C

Explanation:
Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

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 46
Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

A. Manual NAT can offer more flexibility than Automatic NAT.
B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
D. Automatic NAT can offer more flexibility than Manual NAT.

Answer: A

Explanation:
"An Auto-NAT rule only uses the source address and port when matching and translating. Manual NAT can match and translate source and destination addresses and ports." https://networkdirection.net/articles/firewalls/firepowermanagementcentre/fmcnatpolicies/

NEW QUESTION 47
Fill in the blank: Back up and restores can be accomplished through _____.

A. SmartConsole, WebUI, or CLI
B. WebUI, CLI, or SmartUpdate
C. CLI, SmartUpdate, or SmartBackup
D. SmartUpdate, SmartBackup, or SmartConsole

Answer: A

Explanation:
Backup and RestoreThese options let you: To back up a configuration:
The Backup window opens.

NEW QUESTION 51
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 55
Which deployment adds a Security Gateway to an existing environment without changing IP routing?

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

Answer: B

NEW QUESTION 59
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 62
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 67
In order to modify Security Policies the administrator can use which of the following tools? (Choose the best answer.)

A. SmartConsole and WebUI on the Security Management Server.
B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
C. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Answer: B

NEW QUESTION 69
What SmartEvent component creates events?

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

D. SmartEvent GUI

Answer: B

NEW QUESTION 72
The SmartEvent R80 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: B

NEW QUESTION 73
What is the purpose of a Clean-up Rule?

A. Clean-up Rules do not server any purpose.
B. Provide a metric for determining unnecessary rules.
C. To drop any traffic that is not explicitly allowed.
D. Used to better optimize a policy.

Answer: C

Explanation:
These are basic access control rules we recommend for all Rule Bases:
There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION 76
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 78
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 83
Fill in the blank: The position of an implied rule is manipulated in the _____ window.

A. NAT
B. Firewall
C. Global Properties
D. Object Explorer

Answer: C

Explanation:
"Note - In addition, users can access the Implied Rules configurations through Global Properties and use the implied policy view below Configuration."
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 85
To increase security, the administrator has modified the Core protection ‘Host Port Scan’ from ‘Medium’ to ‘High’ Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

A. The Access Control and Threat Prevention Policies.
B. The Access Control Policy.
C. The Access Control & HTTPS Inspection Policy.
D. The Threat Prevention Policy.

Answer: D

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubm

NEW QUESTION 86
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 90
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 95
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 97
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 102
What is the most complete definition of the difference between the Install Policy button on the SmartConsole’s tab, and the Install Policy within a specific policy?

A. The Global one also saves and published the session before installation.
B. The Global one can install multiple selected policies at the same time.
C. The local one does not install the Anti-Malware policy along with the Network policy.
D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Answer: D

NEW QUESTION 105
Which of the following is considered to be the more secure and preferred VPN authentication method?

A. Password
B. Certificate
C. MD5
D. Pre-shared secret

Answer: B

Explanation:
References:

NEW QUESTION 107
How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

A. By impersonating the administrator with the 'Login as…' option
B. They cannot be seen
C. From the SmartView Tracker audit log
D. From Manage and Settings > Sessions, right click on the session and click 'View Changes…'

Answer: D

Explanation:
From the Smartconsole, you can possibly view the changes via Manage & setting, Sessions

NEW QUESTION 112
What are the Threat Prevention software components available on the Check Point Security Gateway?

A. IPS, Threat Emulation and Threat Extraction
B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
D. IDS, Forensics, Anti-Virus, Sandboxing

Answer: C

NEW QUESTION 113
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 115
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 116
Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?

A. Microsoft Publisher
B. JSON
C. Microsoft Word
D. RC4 Encryption

Answer: B

NEW QUESTION 120
In SmartConsole, on which tab are Permissions and Administrators defined?

A. Manage and Settings
B. Logs and Monitor
C. Security Policies
D. Gateways and Servers

Answer: A

NEW QUESTION 125
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 129
When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

A. Log, send snmp trap, email
B. Drop packet, alert, none
C. Log, alert, none
D. Log, allow packets, email

Answer: C

Explanation:
Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

NEW QUESTION 133
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 135
Which tool is used to enable ClusterXL?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

NEW QUESTION 136
When should you generate new licenses?

A. Before installing contract files.
B. After a device upgrade.
C. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
D. Only when the license is upgraded.

Answer: C

NEW QUESTION 141
Which of the following situations would not require a new license to be generated and installed?

A. The Security Gateway is upgraded.
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 143
Fill in the blanks: The Application Layer Firewalls inspect traffic through _____ the layer(s) of the TCP/IP model and up to and including the _____ layer.

A. Upper; Application
B. First two; Internet
C. Lower; Application
D. First two; Transport

Answer: C

Explanation:
application firewalls, or application layer firewalls, use a series of configured policies to determine whether to block or allow communications to or from an app.

NEW QUESTION 144
What are the three types of UserCheck messages?

A. inform, ask, and block
B. block, action, and warn
C. action, inform, and ask
D. ask, block, and notify

Answer: A

Explanation:
Inform User Inform
Shows when the action for the ruleClosed is inform. It informs users what the company policy is for that site. Blocked Message
Block
Shows when a request is blocked. Ask User
Ask
Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_DataLossPrevention_AdminGuide/

NEW QUESTION 146
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 151
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

Answer: A

NEW QUESTION 153
Fill in the blanks: There are _____ types of software containers _____.

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

Answer: A

Explanation:
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security.

NEW QUESTION 157
After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?

A. The gateways can only send logs to an SMS and cannot send logs to a Log Serve
B. Log Servers are proprietary log archive servers.
C. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log Server.
D. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
E. Logs are not automatically forwarded to a new Log Serve
F. SmartConsole must be used to manually configure each gateway to send its logs to the server.

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf

NEW QUESTION 159
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 160
Which type of attack can a firewall NOT prevent?

A. Network Bandwidth Saturation
B. Buffer Overflow
C. SYN Flood
D. SQL Injection

Answer: A

NEW QUESTION 164
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

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

Answer: C

NEW QUESTION 167
The competition between stateful inspection and proxies was based on performance, protocol support, and security. Considering stateful Inspections and Proxies, which statement is correct?

A. Stateful Inspection is limited to Layer 3 visibility, with no Layer 4 to Layer 7 visibility capabilities.
B. When it comes to performance, proxies were significantly faster than stateful inspection firewalls.
C. Proxies offer far more security because of being able to give visibility of the payload (the data).
D. When it comes to performance, stateful inspection was significantly faster than proxies.

Answer: C

NEW QUESTION 168
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 171
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 176
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 181
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 183
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 185
Name the pre-defined Roles included in Gaia OS.

A. AdminRole, and MonitorRole
B. ReadWriteRole, and ReadyOnly Role
C. AdminRole, cloningAdminRole, and Monitor Role
D. AdminRole

Answer: A

NEW QUESTION 189
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 190
URL Filtering cannot be used to:

A. Control Bandwidth issues
B. Control Data Security
C. Improve organizational security
D. Decrease legal liability

Answer: D

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

NEW QUESTION 191
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

A. Down
B. No Response
C. Inactive
D. Failed

Answer: A

NEW QUESTION 192
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 193
What key is used to save the current CPView page in a filename format cpview_“cpview process ID”. cap”number of captures”?

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

Answer: C

NEW QUESTION 198
Which of the following is NOT a role of the SmartCenter:

A. Status monitoring
B. Policy configuration
C. Certificate authority
D. Address translation

Answer: C

NEW QUESTION 202
What command from the CLI would be used to view current licensing?

A. license view
B. fw ctl tab -t license -s
C. show license -s
D. cplic print

Answer: D

NEW QUESTION 207
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 208
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 213
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

A. Security Management Server’s /home/.fgpt file and is available for future SmartConsole authentications.
B. Windows registry is available for future Security Management Server authentications.
C. There is no memory used for saving a fingerprint anyway.
D. SmartConsole cache is available for future Security Management Server authentications.

Answer: D

NEW QUESTION 215
Which of the following cannot be configured in an Access Role Object?

A. Networks
B. Users
C. Time

D. Machines

Answer: C

Explanation:
Access Role objects includes one or more of these objects: Networks.
Users and user groups. Computers and computer groups. Remote Access Clients.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 219
Security Gateway software blades must be attached to what?

A. Security Gateway
B. Security Gateway container
C. Management server
D. Management container

Answer: B

Explanation:
Security Management and Security Gateway Software Blades must be attached to a Software Container to be licensed.
https://downloads.checkpoint.com/dc/download.htm?ID=11608

NEW QUESTION 223
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 224
Which tool is used to enable cluster membership on a Gateway?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

Explanation:
References:

NEW QUESTION 227
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 228
What protocol is specifically used for clustered environments?

A. Clustered Protocol
B. Synchronized Cluster Protocol
C. Control Cluster Protocol
D. Cluster Control Protocol

Answer: D

NEW QUESTION 232
Fill in the blanks: In _____ NAT, Only the _____ is translated.

A. Static; source
B. Simple; source
C. Hide; destination

D. Hide; source

Answer: D

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

NEW QUESTION 234
Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
C. 192.168.1.1 AND 172.26.1.1 AND drop
D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Answer: B

NEW QUESTION 235
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

A. Firewall
B. Application Control
C. Anti-spam and Email Security
D. Anti-Virus

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 238
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

A. Formal; corporate
B. Local; formal
C. Local; central
D. Central; local

Answer: D

NEW QUESTION 240
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

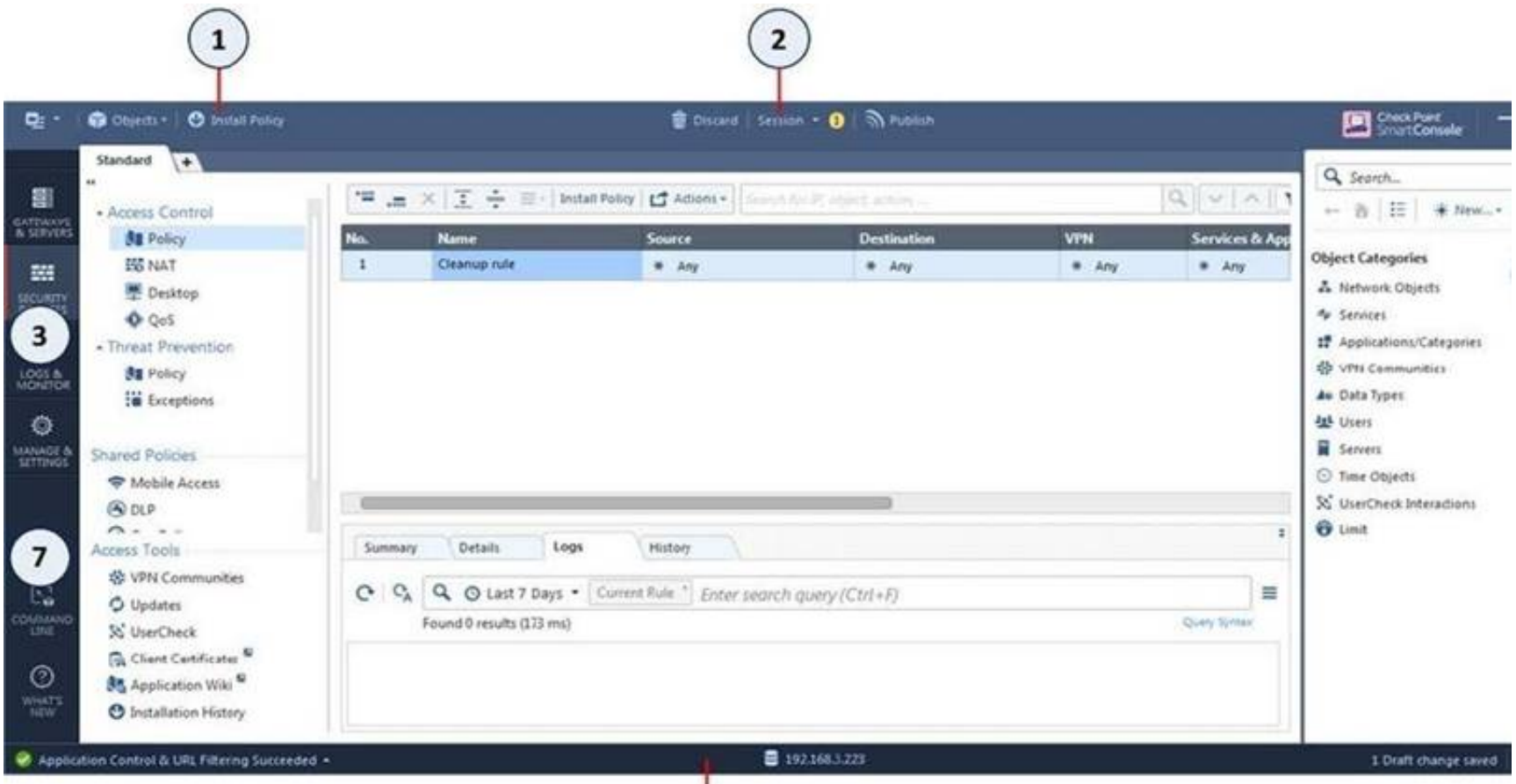
Answer: A

NEW QUESTION 243
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

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

Answer: A

Explanation:



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

NEW QUESTION 247
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 251
Which SmartConsole tab is used to monitor network and security performance?

A. Manage & Settings
B. Security Policies
C. Gateway & Servers
D. Logs & Monitor

Answer: D

NEW QUESTION 253
Which is a main component of the Check Point security management architecture?

A. Identity Collector
B. Endpoint VPN client
C. SmartConsole
D. Proxy Server

Answer: C

Explanation:
https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Part-1-The-Architecture/ba-p/88043 Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and
Threat Prevention capabilities.
Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only.

SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways.

NEW QUESTION 256
How 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 260
In SmartEvent, a correlation unit (CU) is used to do what?

A. Collect security gateway logs, Index the logs and then compress the logs.
B. Receive firewall and other software blade logs in a region and forward them to the primary log server.
C. Analyze log entries and identify events.
D. Send SAM block rules to the firewalls during a DOS attack.

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_Ad

NEW QUESTION 264
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 266
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 267
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 271
Which of the following is NOT a valid configuration screen of an Access Role Object?

A. Users
B. Networks
C. Time
D. Machines

Answer: C

NEW QUESTION 273
How are the backups stored in Check Point appliances?

A. Saved as*.tar under /var/log/CPbackup/backups
B. Saved as*tgz under /var/CPbackup
C. Saved as*tar under /var/CPbackup
D. Saved as*tgz under /var/log/CPbackup/backups

Answer: B

Explanation:
Backup configurations are stored in: /var/CPbackup/backups/

NEW QUESTION 274
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resident 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 276
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 277
Can you use the same layer in multiple policies or rulebases?

A. Yes - a layer can be shared with multiple policies and rules.
B. No - each layer must be unique.
C. No - layers cannot be shared or reused, but an identical one can be created.
D. Yes - but it must be copied and pasted with a different name.

Answer: A

Explanation:
https://community.checkpoint.com/t5/Management/Sharing-a-layer-across-different-policies/td-p/1660

NEW QUESTION 282
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 286
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: C

NEW QUESTION 287

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.81 Product From:

https://www.2passeasy.com/dumps/156-215.81/

Money Back Guarantee

156-215.81 Practice Exam Features:

* 156-215.81 Questions and Answers Updated Frequently

* 156-215.81 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year