CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1
An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

A. AD Query
B. Browser-Based Authentication
C. Identity Agents
D. Terminal Servers Agent

Answer: B

NEW QUESTION 2
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 3
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

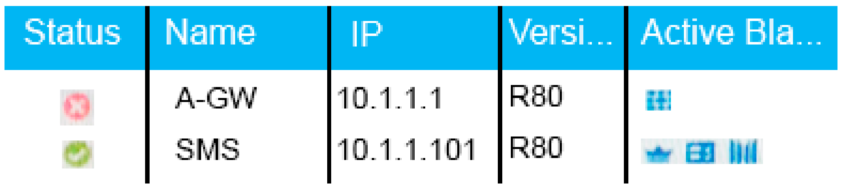
Answer: B

NEW QUESTION 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:



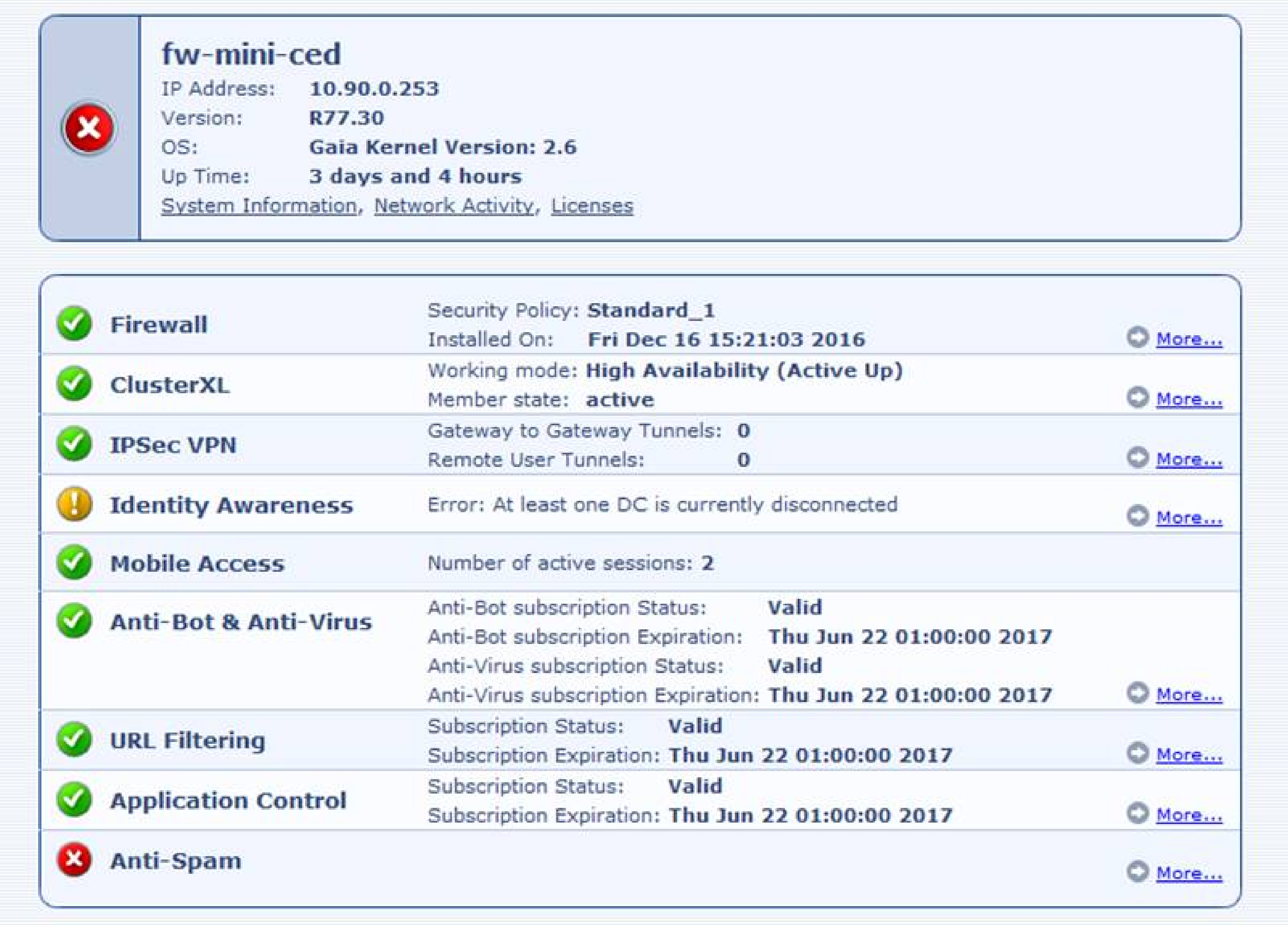
Status	Name	IP	Versi...	Active Bla...
✗	A-GW	10.1.1.1	R80	▦
✓	SMS	10.1.1.101	R80	▦ ▦ ▦

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:



✗ **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
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
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
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 9
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116

C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members

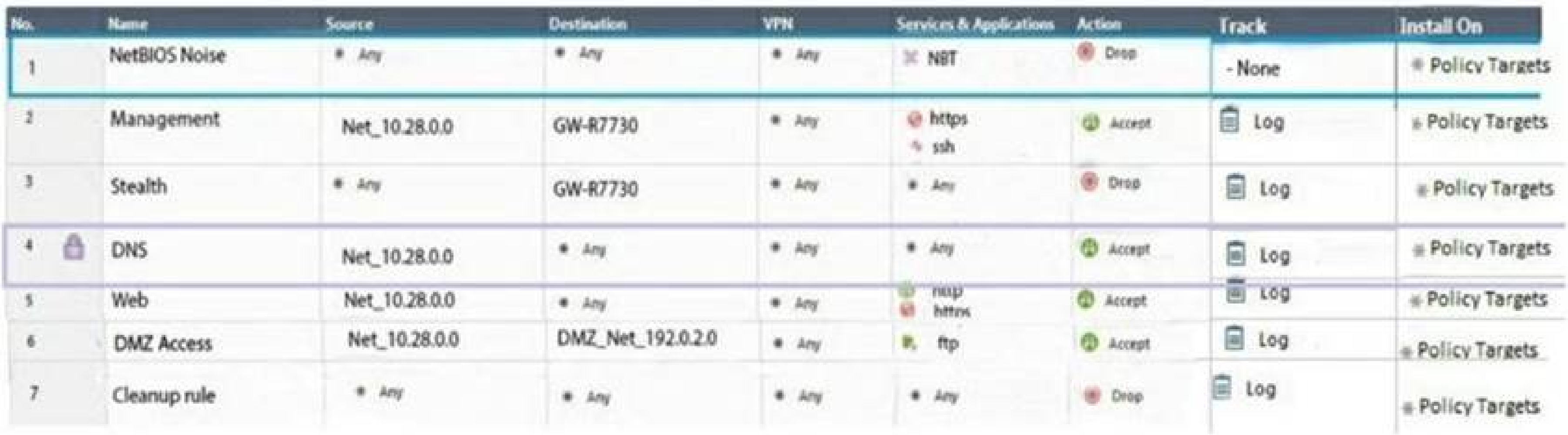
Answer: A

NEW QUESTION 10
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Answer: C

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 11
Name one limitation of using Security Zones in the network?

A. Security zones will not work in Automatic NAT rules
B. Security zone will not work in Manual NAT rules
C. Security zones will not work in firewall policy layer
D. Security zones cannot be used in network topology

Answer: B

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

NEW QUESTION 12
URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

A. WebCheck
B. UserCheck
C. Harmony Endpoint
D. URL categorization

Answer: B

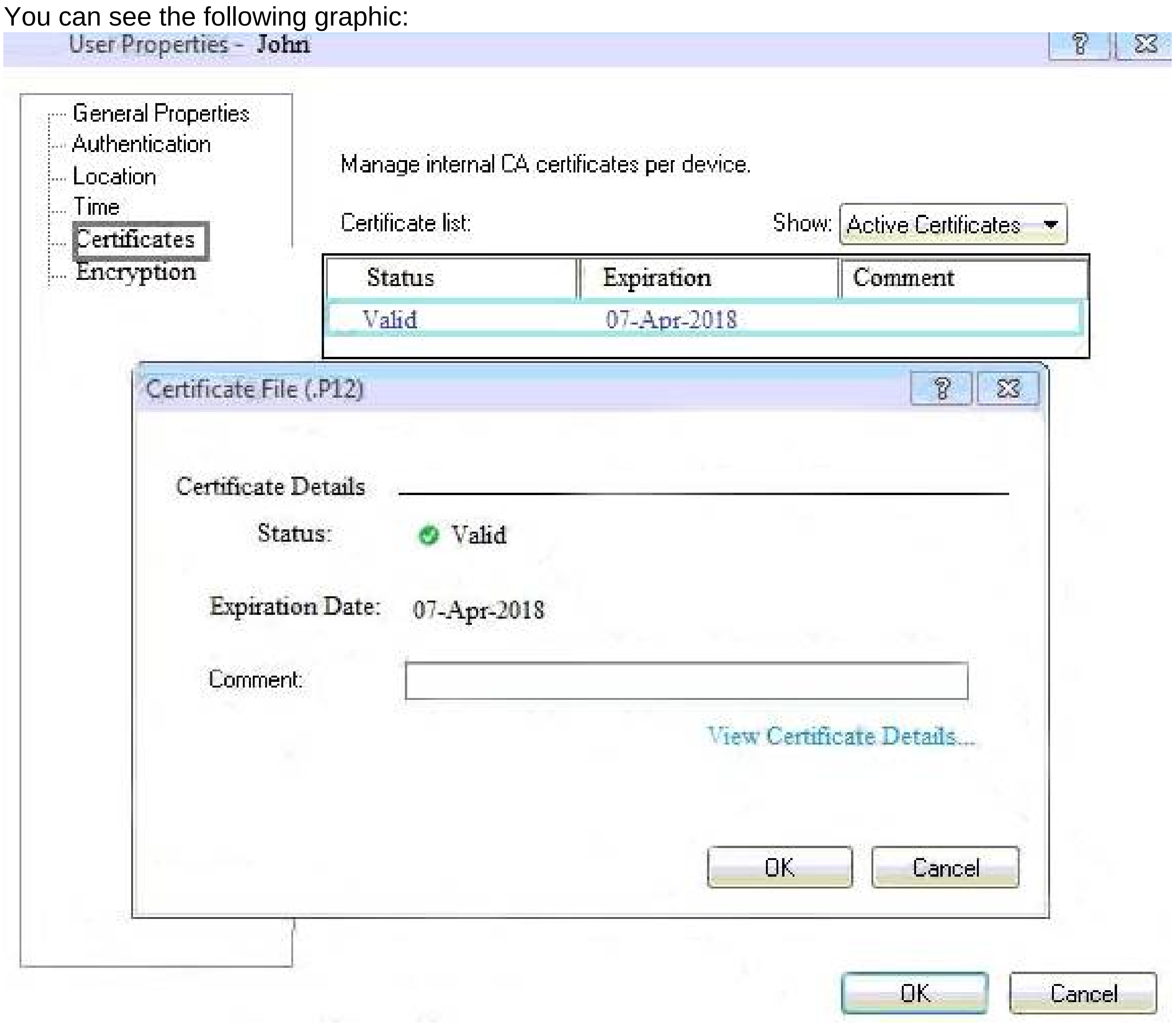
Explanation:
UserCheck alerts users while attemping to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION 16
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 18
You can see the following graphic:



User Properties - John

- General Properties
- Authentication
- Location
- Time
- Certificates
- Encryption

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 22
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 23
Fill in the bank: In Office mode, a Security Gateway assigns a remote client to an IP address once _______ .

A. the user connects and authenticates
B. office mode is initiated
C. the user requests a connection
D. the user connects

Answer: A

Explanation:
Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected.

NEW QUESTION 27
Which tool allows you to monitor the top bandwidth on smart console?

A. Logs & Monitoring
B. Smart Event
C. Gateways & Severs Tab
D. SmartView Monitor

Answer: D

Explanation:

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

NEW QUESTION 32
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as ________.

A. User Center
B. User Administration
C. User Directory
D. UserCheck

Answer: C

Explanation:
User Directory lets you configure:
High Availability, to duplicate user data across multiple servers for backup. See Account Units and High Availability.
Multiple Account Units, for distributed databases.
Define LDAP Account Units, for encrypted User Directory connections. See Modifying the LDAP Server. Profiles, to support multiple LDAP vendors. See User Directory Profiles. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 35
Which of the following is an authentication method used for Identity Awareness?

A. SSL
B. Captive Portal
C. PKI
D. RSA

Answer: B

NEW QUESTION 37
From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

A. Verify a Security Policy
B. Open a terminal shell
C. Add a static route
D. View Security Management GUI Clients

Answer: B

NEW QUESTION 39
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 43
Which of the following is NOT a tracking log option in R80.x?

A. Log
B. Full Log
C. Detailed Log
D. Extended Log

Answer: C

NEW QUESTION 47
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 49
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 51
Core Protections are installed as part of what Policy?

A. Access Control Policy.
B. Desktop Firewall Policy
C. Mobile Access Policy.
D. Threat Prevention Policy.

Answer: A

Explanation:
Core protections - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy. ThreatCloud protections - Updated from the Check Point cloud, (see Updating IPS Protections). These protections are part of the Threat Prevention policy. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 52
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 53
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 55
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 56
What are the advantages of a “shared policy” in R80?

A. Allows the administrator to share a policy between all the users identified by the Security Gateway
B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
C. Allows the administrator to share a policy so that it is available to use in another Policy Package
D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Answer: C

Explanation:

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

NEW QUESTION 58
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 63
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 64
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 69
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 73
What is the SOLR database for?

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

Answer: A

NEW QUESTION 74
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

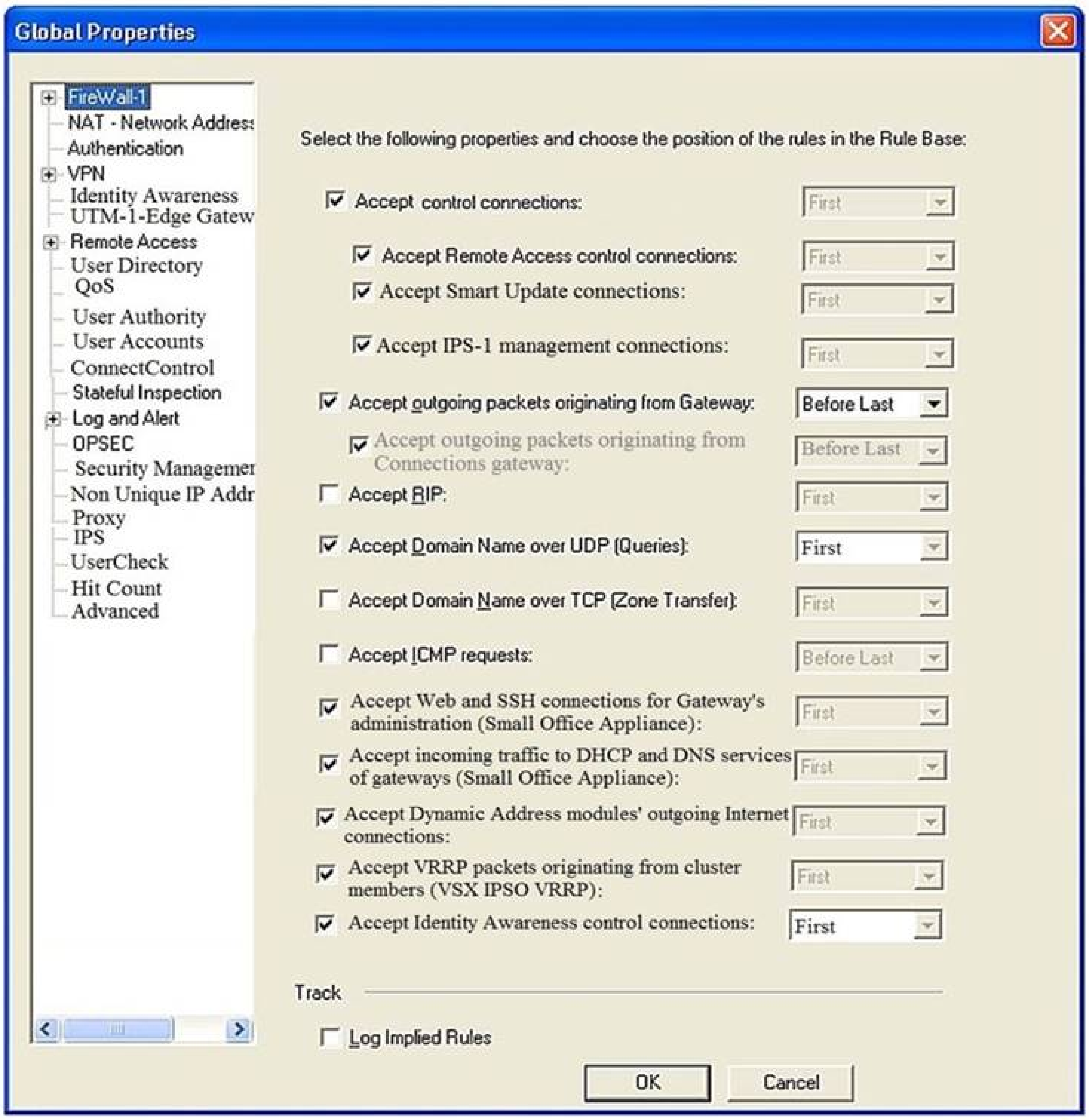
NEW QUESTION 75
Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

A. Centos Linux
B. Gaia embedded
C. Gaia
D. Red Hat Enterprise Linux version 5

Answer: B

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

NEW QUESTION 79
Consider the Global Properties following settings:



Select the following properties and choose the position of the rules in the Rule Base:

- ☑ Accept control connections: First
- ☑ Accept Remote Access control connections: First
- ☑ Accept Smart Update connections: First
- ☑ Accept IPS-1 management connections: First
- ☑ Accept outgoing packets originating from Gateway: Before Last
- ☑ Accept outgoing packets originating from Connections gateway: Before Last
- ☐ Accept RIP: First
- ☑ Accept Domain Name over UDP (Queries): First
- ☐ Accept Domain Name over TCP (Zone Transfer): First
- ☐ Accept ICMP requests: Before Last
- ☑ Accept Web and SSH connections for Gateway's administration (Small Office Appliance): First
- ☑ Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance): First
- ☑ Accept Dynamic Address modules' outgoing Internet connections: First
- ☑ Accept VRRP packets originating from cluster members (VSX IPSO VRRP): First
- ☑ Accept Identity Awareness control connections: First

Track

- ☐ Log Implied Rules

The selected option “Accept Domain Name over UDP (Queries)” means:

A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Answer: A

NEW QUESTION 83
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 85
Stateful Inspection compiles and registers connections where?

A. Connection Cache
B. State Cache
C. State Table
D. Network Table

Answer: C

NEW QUESTION 89
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 94
What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

A. Server, Username, Password, Path, Version
B. Username, Password, Path, Version
C. Server, Protocol, Username, Password, Destination Path
D. Server, Protocol, Username, Password, Path

Answer: D

Explanation:
References:

NEW QUESTION 99
Which backup utility captures the most information and tends to create the largest archives?

A. backup
B. snapshot
C. Database Revision
D. migrate export

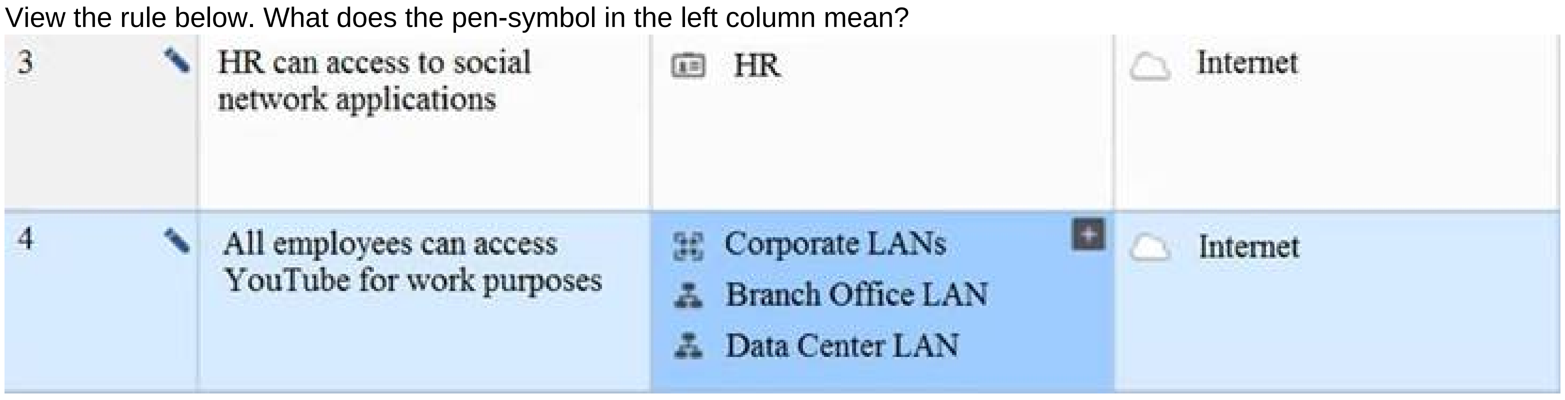
Answer: B

NEW QUESTION 102
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 103
View the rule below. What does the pen-symbol in the left column mean?



3	✎	HR can access to social network applications	HR	Internet
4	✎	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN Data Center LAN	Internet

A. Those rules have been published in the current session.
B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
C. Another user has currently locked the rules for editing.
D. The configuration lock is presen
E. Click the pen symbol in order to gain the lock.

Answer: B

NEW QUESTION 106
You have discovered suspicious activity in your network. What is the BEST immediate action to take?

A. Create a policy rule to block the traffic.
B. Create a suspicious action rule to block that traffic.
C. Wait until traffic has been identified before making any changes.
D. Contact ISP to block the traffic.

Answer: B

NEW QUESTION 107
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 108
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 110
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 114
What is true about the IPS-Blade?

A. in R80, IPS is managed by the Threat Prevention Policy
B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. in R80, IPS Exceptions cannot be attached to “all rules”
D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 119
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 120
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 125
Which of the following is NOT a valid deployment option for R80?

A. All-in-one (stand-alone)
B. CloudGuard
C. Distributed
D. Bridge Mode

Answer: B

NEW QUESTION 130
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 134
When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

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

Answer: A

Explanation:
The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 137
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 138
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 143
In _______ NAT, the _______ is translated.

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

Answer: A

NEW QUESTION 147
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 149
You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

A. Open SmartLog and connect remotely to the IP of the wireless controller
B. Open SmartView Tracker and filter the logs for the IP address of the tablet
C. Open SmartView Tracker and check all the IP logs for the tablet
D. Open SmartLog and query for the IP address of the Manager's tablet

Answer: B

NEW QUESTION 154
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 157
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 159
Which part of SmartConsole allows administrators to add, edit delete, and clone objects?

A. Object Browser
B. Object Editor
C. Object Navigator
D. Object Explorer

Answer: D

NEW QUESTION 161
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 162
Which of these is NOT a feature or benefit of Application Control?

A. Eliminate unknown and unwanted applications in your network to reduce IT complexity and application risk.
B. Identify and control which applications are in your IT environment and which to add to the IT environment.
C. Scans the content of files being downloaded by users in order to make policy decisions.
D. Automatically identify trusted software that has authorization to run

Answer: C

Explanation:
File scanning is a job for ThreatCloud and it sandboxes/scrubs files.

NEW QUESTION 164
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 166
A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

A. In the system SMEM memory pool.
B. In State tables.
C. In the Sessions table.
D. In a CSV file on the firewall hard drive located in $FWDIR/conf/.

Answer: B

Explanation:
The information stored in the state tables provides cumulative data that can be used to evaluate future connections......
https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateful-firewall/

NEW QUESTION 167
Fill in the blank: Authentication rules are defined for ______.

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

Answer: A

NEW QUESTION 172
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 177
How would you determine the software version from the CLI?

A. fw ver
B. fw stat
C. fw monitor
D. cpinfo

Answer: A

NEW QUESTION 179
R80.10 management server can manage gateways with which versions installed?

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

Answer: B

NEW QUESTION 180
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

A. ifconfig -a
B. show interfaces
C. show interfaces detail
D. show configuration interface

Answer: D

NEW QUESTION 182
Application Control/URL filtering database library is known as:

A. Application database
B. AppWiki
C. Application-Forensic Database
D. Application Library

Answer: B

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

NEW QUESTION 187
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 192
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 195
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 200
Fill in the blank: An LDAP server holds one or more ______.

A. Server Units
B. Administrator Units
C. Account Units
D. Account Servers

Answer: C

NEW QUESTION 203
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 207
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 209
What are the three components for Check Point Capsule?

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

Answer: D

NEW QUESTION 213
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 217
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 220
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 222
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 223
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 228
Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

A. SmartDashboard
B. SmartEvent
C. SmartView Monitor
D. SmartUpdate

Answer: B

Explanation:
SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously. Ref: https://www.checkpoint.com/products/smartevent/

NEW QUESTION 233
When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge

Answer: A

NEW QUESTION 237
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 240
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 245
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 250
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 253
Which Threat Prevention profile uses sanitization technology?

A. Cloud/data Center
B. perimeter
C. Sandbox
D. Guest Network

Answer: B

Explanation:
Strict Security for Perimeter Profile & Perimeter Profile use sanitization as a technology in Threat prevention profile

NEW QUESTION 255
Which key is created during Phase 2 of a site-to-site VPN?

A. Pre-shared secret
B. Diffie-Hellman Public Key
C. Symmetrical IPSec key
D. Diffie-Hellman Private Key

Answer: C

NEW QUESTION 257
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 260
When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

A. The gateway is not powered on.
B. Incorrect routing to reach the gateway.
C. The Admin would need to login to Read-Only mode
D. Another Admin has made an edit to that object and has yet to publish the change.

Answer: D

NEW QUESTION 263
In the Check Point Security Management Architecture, which component(s) can store logs?

A. SmartConsole
B. Security Management Server and Security Gateway
C. Security Management Server
D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 266
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 269
True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

A. False, log servers are configured on the Log Server General Properties
B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
C. True, all Security Gateways forward logs automatically to the Security Management Server
D. False, log servers are enabled on the Security Gateway General Properties

Answer: B

NEW QUESTION 272
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 275
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 280
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 285
Which tool allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS?

A. CPASE - Check Point Automatic Service Engine
B. CPAUE - Check Point Automatic Update Engine
C. CPDAS - Check Point Deployment Agent Service
D. CPUSE - Check Point Upgrade Service Engine

Answer: D

Explanation:
Check Point Update Service Engine (CPUSE), also known as Deployment Agent [DA], is an advanced and intuitive mechanism for software deployment on Gaia OS, which supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 288
DLP and Geo Policy are examples of what type of Policy?

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

Answer: B

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

NEW QUESTION 289
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 293
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 298
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 302
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 306
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 307
Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for what components?

A. The Security Gateway (SG) and Security Management Server (SMS) software and the CPUSE engine.
B. Licensed Check Point products for the Gala operating system and the Gaia operating system itself.
C. The CPUSE engine and the Gaia operating system.
D. The Gaia operating system only.

Answer: B

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

NEW QUESTION 310
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 313
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files
C. AppWiki
D. IPS Protections

Answer: A

NEW QUESTION 318
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 323
Which of the following licenses are considered temporary?

A. Plug-and-play (Trial) and Evaluation
B. Perpetual and Trial
C. Evaluation and Subscription
D. Subscription and Perpetual

Answer: A

NEW QUESTION 325
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 327
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 329
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

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

Answer: B

NEW QUESTION 330
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 333
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 334
When should you generate new licenses?

A. Before installing contract files.
B. After an RMA procedure when the MAC address or serial number of the appliance changes.
C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
D. Only when the license is upgraded.

Answer: C

NEW QUESTION 336
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 340
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 342
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 346
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 348
Fill in the blank: SmartConsole, SmartEvent GUI client, and _______ allow viewing of billions of consolidated logs and shows them as prioritized security events.

A. SmartView Web Application
B. SmartTracker
C. SmartMonitor

D. SmartReporter

Answer: A

Explanation:
"The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents"
https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=docume

NEW QUESTION 352
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 355
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 356
When defining group-based access in an LDAP environment with Identity Awareness, what is the BEST object type to represent an LDAP group in a Security Policy?

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

Answer: A

NEW QUESTION 360
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 361
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 364
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 365
In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

Answer: C

NEW QUESTION 369
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

A. Save Policy
B. Install Database
C. Save session
D. Install Policy

Answer: D

NEW QUESTION 372
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 376
Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is _______.

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

Answer: D

NEW QUESTION 377
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 378
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 380
Which of the following is NOT an identity source used for Identity Awareness?

A. Remote Access
B. UserCheck

C. AD Query
D. RADIUS

Answer: B

NEW QUESTION 384
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 389
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 393
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 394
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 397
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 398
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 399
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 400
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

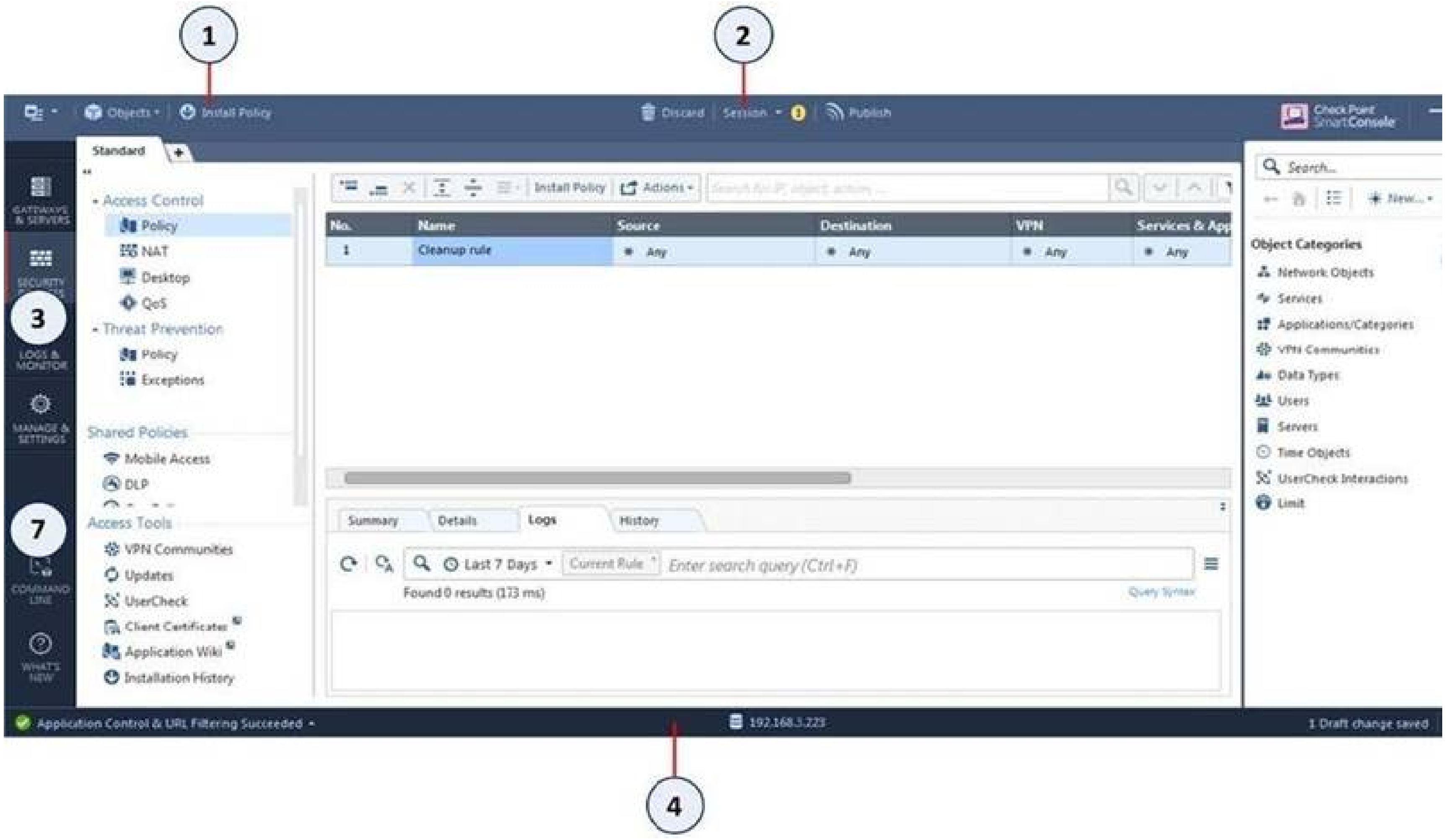
Explanation:
Two ways of auth: Username/Password in Captive Portal or Transparent Kerberos Auth through Kerberos Ticket.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 401
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

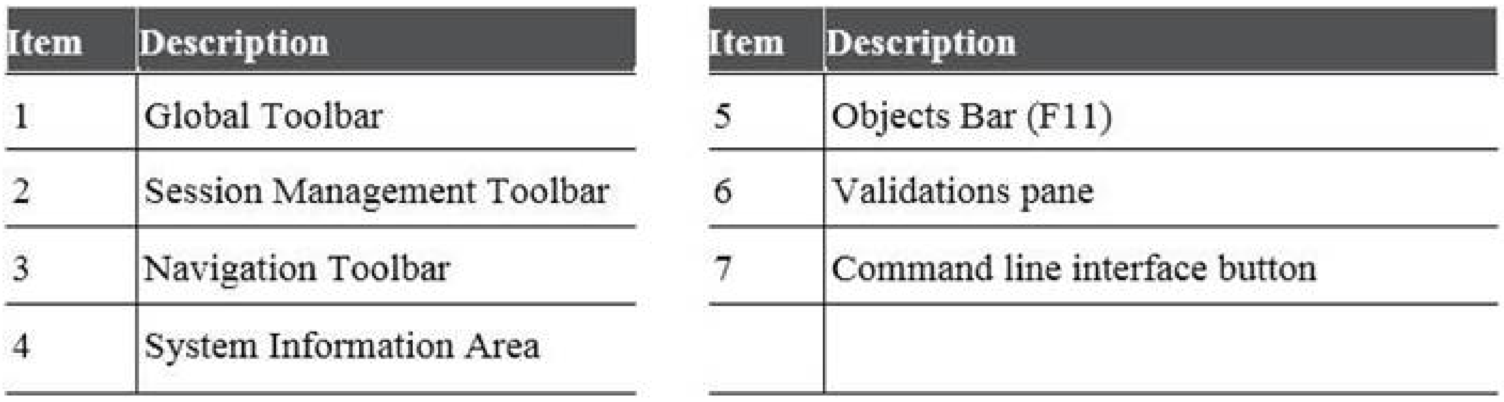
A. Manage and Command Line
B. Logs and Monitor
C. Security Policies
D. Gateway and Servers

Answer: A

Explanation:



No.	Name	Source	Destination	VPN	Services & App
1	Cleanup rule	Any	Any	Any	Any



Item	Description	Item	Description
1	Global Toolbar	5	Objects Bar (F11)
2	Session Management Toolbar	6	Validations pane
3	Navigation Toolbar	7	Command line interface button
4	System Information Area		

NEW QUESTION 402
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 407
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 408
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

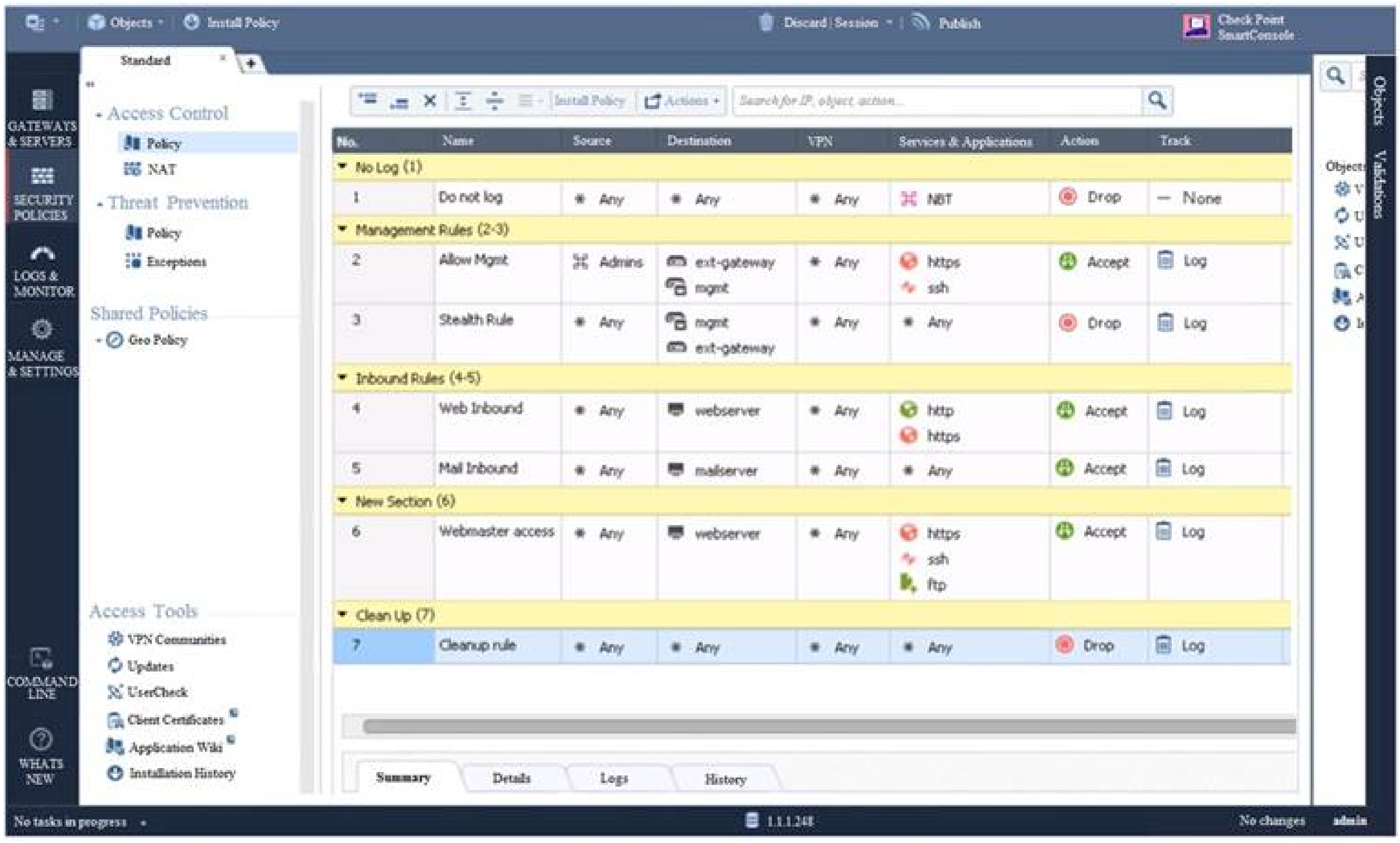
NEW QUESTION 412
Which is a main component of the Check Point security management architecture?

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 417
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 421
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

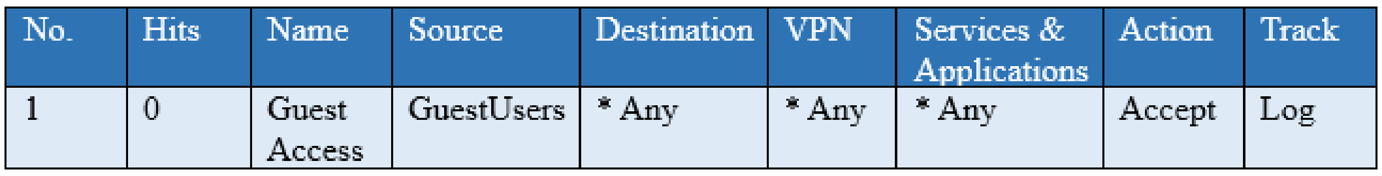
NEW QUESTION 423
Fill in the blank: To create policy for traffic to or from a particular location, use the ______ .

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 425
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 429
Which statement describes what Identity Sharing is in Identity Awareness?

A. Management servers can acquire and share identities with Security Gateways
B. Users can share identities with other users
C. Security Gateways can acquire and share identities with other Security Gateways
D. Administrators can share identifies with other administrators

Answer: C

Explanation:
Identity Sharing
Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.
Set these options on the Identity Awareness > Identity Sharing page of the Security Gateway object:

NEW QUESTION 432
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 436
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 439
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 442
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

NEW QUESTION 445
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 448
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 449
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 450
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 455
You have enabled "Extended Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Identity Awareness is not enabled.
B. Log Trimming is enabled.
C. Logging has disk space issues
D. Content Awareness is not enabled.

Answer: D

NEW QUESTION 458
Phase 1 of the two-phase negotiation process conducted by IKE operates in ______ mode.

A. Main
B. Authentication
C. Quick
D. High Alert

Answer: A

Explanation:
Phase I modes
Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

NEW QUESTION 460
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 461
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 466
Fill in the blank: With the User Directory Software Blade, you can create user definitions on a(n) _______ Server.

A. SecurID
B. LDAP
C. NT domain
D. SMTP

Answer: B

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

NEW QUESTION 469
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 471

What is UserCheck?

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

Answer: B

Explanation:

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

NEW QUESTION 472

......

Relate Links

Contact us