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

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

Answer: C

NEW QUESTION 3
What is the purpose of the Stealth Rule?

A. To prevent users from directly connecting to a Security Gateway.
B. To reduce the number of rules in the database.
C. To reduce the amount of logs for performance issues.
D. To hide the gateway from the Internet.

Answer: A

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

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

Answer: B

NEW QUESTION 5
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 6
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 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
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 9
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 10
Choose what BEST describes the reason why querying logs now is very fast.

A. New Smart-1 appliances double the physical memory install
B. Indexing Engine indexes logs for faster search results
C. SmartConsole now queries results directly from the Security Gateway
D. The amount of logs been store is less than the usual in older versions

Answer: B

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

NEW QUESTION 10
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 12
You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

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

Answer: D

NEW QUESTION 14
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 15
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 20
John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

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

Answer: D

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

NEW QUESTION 25
When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

A. SmartView Monitor should be opened and then the SAM rule/s can be applied immediatel
B. Installing policy is not required.
C. The policy type SAM must be added to the Policy Package and a new SAM rule must be applied.Simply Publishing the changes applies the SAM rule on the firewall.
D. The administrator must work on the firewall CLI (for example with SSH and PuTTY) and the command 'sam block' must be used with the right parameters.
E. The administrator should open the LOGS & MONITOR view and find the relevant lo
F. Right clicking on the log entry will show the Create New SAM rule option.

Answer: A

Explanation:
A Security GatewayClosed with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policyClosed. These rules are applied immediately (policy installation is not required).
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 27
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 32
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 35
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 37
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 42
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 43
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 44
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 48
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 51
What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

A. Verification tool

B. Verification licensing
C. Automatic licensing
D. Automatic licensing and Verification tool

Answer: D

NEW QUESTION 56
Which command shows the installed licenses?

A. cplic print
B. print cplic
C. fwlic print
D. show licenses

Answer: A

NEW QUESTION 57
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 59
The Gateway Status view in SmartConsole shows the overall status of Security Gateways and Software Blades. What does the Status Attention mean?

A. Cannot reach the Security Gateway.
B. The gateway and all its Software Blades are working properly.
C. At least one Software Blade has a minor issue, but the gateway works.
D. Cannot make SIC between the Security Management Server and the Security Gateway

Answer: C

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

NEW QUESTION 62
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup
B. import backup
C. cp_merge
D. migrate import

Answer: A

NEW QUESTION 66
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 68
Gaia has two default user accounts that cannot be deleted. What are those user accounts?

A. Admin and Default
B. Expert and Clish
C. Control and Monitor
D. Admin and Monitor

Answer: D

NEW QUESTION 72
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 73
What is the BEST method to deploy Identity Awareness for roaming users?

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

Answer: B

Explanation:
Using Endpoint Identity Agents give you:

NEW QUESTION 75
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 78
Which information is included in the “Extended Log” tracking option, but is not included in the “Log” tracking option?

A. file attributes
B. application information
C. destination port
D. data type information

Answer: B

NEW QUESTION 80
Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

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

Answer: D

NEW QUESTION 81
A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

A. Anti-Bot protection
B. Anti-Malware protection
C. Policy-based routing
D. Suspicious Activity Monitoring (SAM) rules

Answer: D

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

NEW QUESTION 85
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 89
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 90
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 93
What type of NAT is a one-to-one relationship where each host is translated to a unique address?

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

Answer: B

NEW QUESTION 97
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 102
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 105
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 109
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 113
Which type of Check Point license ties the package license to the IP address of the Security Management Server?

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

Answer: A

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

NEW QUESTION 117
R80 is supported by which of the following operating systems:

A. Windows only
B. Gaia only
C. Gaia, SecurePlatform, and Windows
D. SecurePlatform only

Answer: B

NEW QUESTION 118
In which scenario is it a valid option to transfer a license from one hardware device to another?

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

Answer: A

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

NEW QUESTION 122
In _______ NAT, the _______ is translated.

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

Answer: A

NEW QUESTION 125
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 128
Choose what BEST describes users on Gaia Platform.

A. There are two default users and neither can be deleted.
B. There are two default users and one cannot be deleted.
C. There is one default user that can be deleted.
D. There is one default user that cannot be deleted.

Answer: A

Explanation:
These users are created by default and cannot be deleted: admin
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.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/U

NEW QUESTION 133
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 135
Using R80 Smart Console, what does a “pencil icon” in a rule mean?

A. I have changed this rule
B. Someone else has changed this rule
C. This rule is managed by check point’s SOC
D. This rule can’t be changed as it’s an implied rule

Answer: A

NEW QUESTION 139
Which Threat Prevention Profile is not included by default in R80 Management?

A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

Answer: D

NEW QUESTION 142
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 143
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 147
Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

A. The firewall topologies
B. NAT Rules
C. The Rule Base
D. The VPN Domains

Answer: C

NEW QUESTION 148
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 152
One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

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

Answer: B

NEW QUESTION 157
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 160
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 163
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 166
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
C. cphaprob –a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 169
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 170

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 173
Choose what BEST describes the reason why querying logs now are very fast.

A. The amount of logs being stored is less than previous versions.
B. New Smart-1 appliances double the physical memory install.
C. Indexing Engine indexes logs for faster search results.
D. SmartConsole now queries results directly from the Security Gateway.

Answer: B

NEW QUESTION 178
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 180
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 182
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 184
What is the RFC number that act as a best practice guide for NAT?

A. RFC 1939
B. RFC 1950
C. RFC 1918
D. RFC 793

Answer: C

Explanation:
https://datatracker.ietf.org/doc/html/rfc1918

NEW QUESTION 188
When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packer Filtering?

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

Answer: D

NEW QUESTION 191
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 196
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 199
Which icon in the WebUI indicates that read/write access is enabled?

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

Answer: A

NEW QUESTION 204
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 208
To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

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

Answer: B

NEW QUESTION 211
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 215
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 220
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 222
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 223
When changes are made to a Rule base, it is important to _______ to enforce changes.

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

Answer: C

NEW QUESTION 224
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 226
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 229
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 234
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 239
Identity Awareness allows easy configuration for network access and auditing based on what three items?

A. Client machine IP address.
B. Network location, the identity of a user and the identity of a machine.
C. Log server IP address.
D. Gateway proxy IP address.

Answer: B

NEW QUESTION 241
When using Automatic Hide NAT, what is enabled by default?

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

Answer: A

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

NEW QUESTION 245
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 249
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 252
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 257
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 260
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 261
Which two Identity Awareness commands are used to support identity sharing?

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

Answer: A

NEW QUESTION 263
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 268
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 272
What is the main objective when using Application Control?

A. To filter out specific content.
B. To assist the firewall blade with handling traffic.
C. To see what users are doing.
D. Ensure security and privacy of information.

Answer: A

Explanation:
https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/

NEW QUESTION 275
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

A. Symmetric routing

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

Answer: B

NEW QUESTION 280
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 285
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 286
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 290
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 294
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 295
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 299
Access roles allow the firewall administrator to configure network access according to:

A. remote access clients.
B. a combination of computer or computer groups and networks.
C. users and user groups.
D. All of the above.

Answer: D

Explanation:
To create an access role:
The Access Role window opens.
Your selection is shown in the Networks node in the Role Preview pane.
A window opens. You can search for Active Directory entries or select them from the list. You can search for AD entries or select them from the list.
The access role is added to the Users and Administrators tree.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 302
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 305
Name the utility that is used to block activities that appear to be suspicious.

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

Answer: C

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

NEW QUESTION 306
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 308
What are the three main components of Check Point security management architecture?

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

Answer: A

NEW QUESTION 310
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 311
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 312
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 315
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

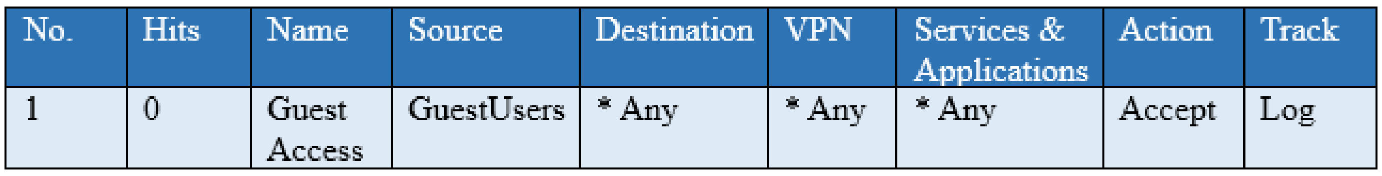
NEW QUESTION 319
Fill in the blank: To create policy for traffic to or from a particular location, use the _______ .

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 323
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 324
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 326
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

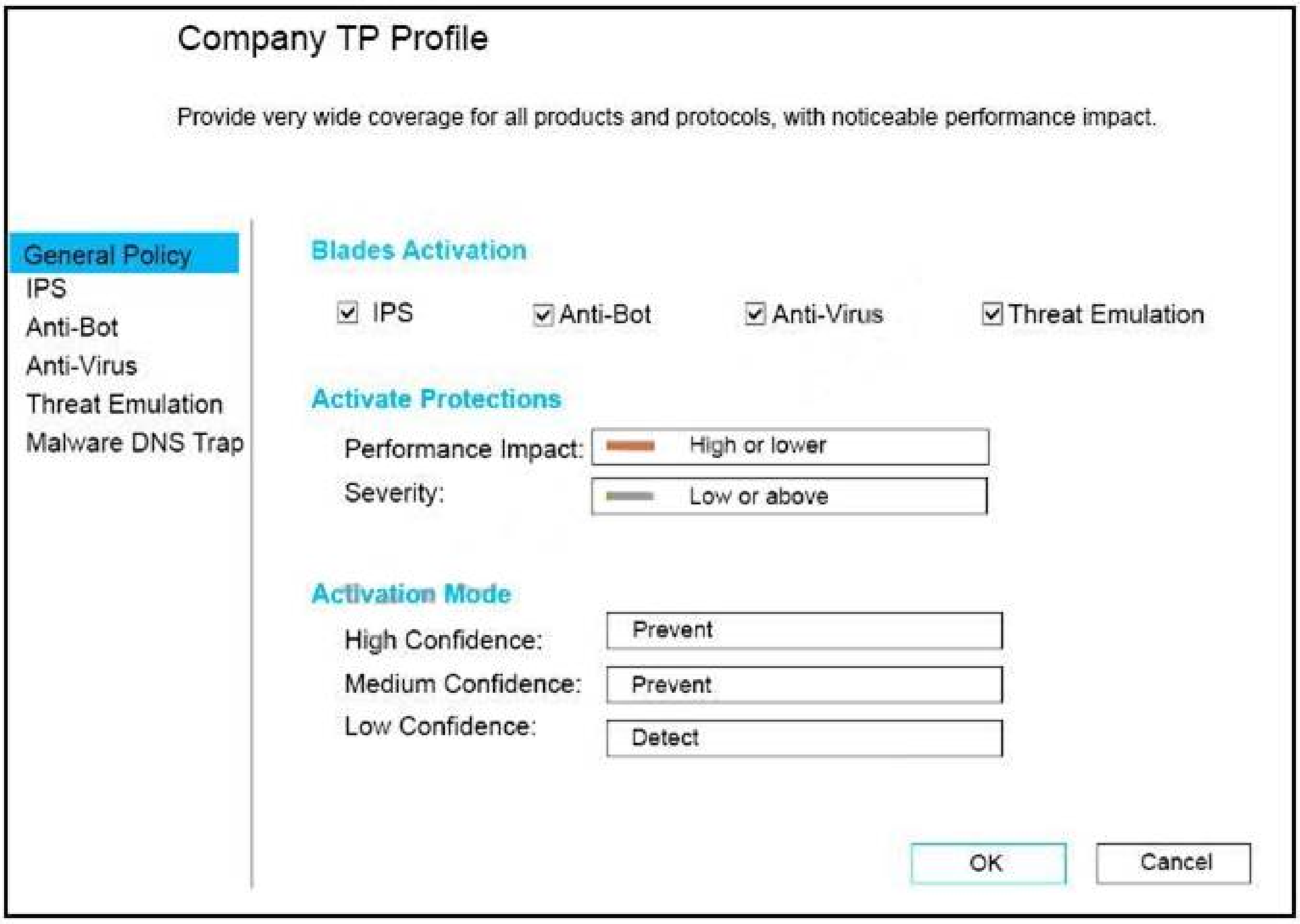
Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_fram

NEW QUESTION 329
Which of the following is NOT an option to calculate the traffic direction?

A. Incoming
B. Internal
C. External
D. Outgoing

Answer: D

NEW QUESTION 332
CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings.
The following Threat Prevention Profile has been created.


Company TP Profile

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

Blades Activation

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

Activate Protections

Performance Impact: High or lower
Severity: Low or above

Activation Mode

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

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

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

Answer: B

NEW QUESTION 336
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 337
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 338
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

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

Answer: B

NEW QUESTION 340
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 344
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 347
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 348
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 350
......