# CheckPoint.156-215.82.v2026-05-01.q141

| | |
|---|---|
| **Exam Code:** | 156-215.82 |
| **Exam Name:** | Check Point Certified Security Administrator - R82 |
| **Certification Provider:** | CheckPoint |
| **Free Question Number:** | 141 |
| **Version:** | v2026-05-01 |
| **# of views:** | 102 |
| **# of Questions views:** | 1413 |
| https://www.freecram.net/torrent/CheckPoint.156-215.82.v2026-05-01.q141.html | |

**NEW QUESTION: 1**
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: (SHOW ANSWER)**
Application Control is the software blade that enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine. Application Control allows you to define granular rules for applications, web sites, web categories, web content types, and users. You can also use Application Control to monitor and block risky applications and web usage. [Application Control Administration Guide R80.40]

**NEW QUESTION: 2**
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: (SHOW ANSWER)**

Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS. This is because certificate based authentication provides stronger security and easier management than pre-shared secret authentication. The other options are either incorrect or irrelevant for this scenario. [Check Point R80.10 - Part 6 - Certificate Based Authentication]

**NEW QUESTION: 3**
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: (SHOW ANSWER)**
When changes are made to a Rule base, it is important toPublish databaseto enforce changes5. Publishing database saves the changes to the database and makes them available to other administrators. Installing policy applies the changes to the Security Gateways. Check Point R81 Security Management Administration Guide, [Check Point R81 SmartConsole R81 Resolved Issues], [Check Point R81 Firewall Administration Guide]

**NEW QUESTION: 4**
Which of the following is an authentication method used for Identity Awareness?
**A.** SSL
**B.** Captive Portal
**C.** PKI
**D.** RSA
**Answer: (SHOW ANSWER)**
Captive Portal is an authentication method used for Identity Awareness4. Captive Portal is a web-based authentication method that redirects users to a browser-based login page when they try to access the network. Users must provide their credentials to access the network resources.Captive Portal can be used for guest users or users who are not identified by other methods4. SSL, PKI, and RSA are not authentication methods used for Identity Awareness, but rather encryption or certificate technologies. Identity Awareness Reference Architecture and Best Practices

**NEW QUESTION: 5**
DLP and Geo Policy are examples of what type of Policy?
**A.** Inspection Policies
**B.** Shared Policies
**C.** Unified Policies
**D.** Standard Policies
**Answer: (SHOW ANSWER)**

DLP and Geo Policy are examples ofShared Policies. Shared Policies are policies that can be shared with other policy packages to save time and effort when managing multiple gateways with similar security requirements. Shared Policies can be applied to Access Control, Threat Prevention, and HTTPS Inspection layers. Other types of policies include Inspection Policies, Unified Policies, and Standard Policies. [Check Point R81 Security Management Administration Guide], [Check Point R81 SmartConsole R81 Resolved Issues]

**NEW QUESTION: 6**
How do logs change when the "Accounting" tracking option is enabled on a traffic rule?
**A.** Involved traffic logs will be forwarded to a log server.
**B.** Provides log details view email to the Administrator.
**C.** Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.
**D.** Provides additional information to the connected user.
**Answer: (SHOW ANSWER)**
The Accounting tracking option is used to monitor the amount of data that passes through a connection. When this option is enabled on a traffic rule, the involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.This information can be used for billing or auditing purposes3. Check Point R81 Logging and Monitoring Administration Guide

**NEW QUESTION: 7**
Which of the following is NOT a valid deployment option for R80?
**A.** All-in-one (stand-alone)
**B.** Log server
**C.** SmartEvent
**D.** Multi-domain management server
**Answer: (SHOW ANSWER)**
Multi-domain management server is a valid deployment option for R81, not R80.R80 supports multi-domain security management, which is a centralized management solution for large-scale, distributed environments with many different domain networks1. Multi-Domain Security Management Administration Guide R80

**NEW QUESTION: 8**
How are the backups stored in Check Point appliances?
**A.** Saved as*.tar under /var/log/CPbackup/backups
**B.** Saved as*tgz under /var/CPbackup
**C.** Saved as*tar under /var/CPbackup
**D.** Saved as*tgz under /var/log/CPbackup/backups
**Answer: (SHOW ANSWER)**

The backups are stored in Check Point appliances as *.tgz files under /var/CPbackup. This is the default location for backup files created by the backup command. Therefore, the correct answer is B. Saved as *.tgz under /var/CPbackup

**NEW QUESTION: 9**
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 (LEAVE A REPLY)**
The two types of NAT supported by the Security Gateway are hide NAT and static NAT. Hide NAT translates many source IP addresses into one IP address, usually the external interface of the gateway.Static NAT translates one source IP address into another IP address, usually a public IP address34. The other options are not valid types of NAT. Network Address Translation (NAT),Check Point CCSA - R81: Practice Test & Explanation

**NEW QUESTION: 10**
A SAM rule Is implemented to provide what function or benefit?
**A.** Allow security audits.
**B.** Handle traffic as defined in the policy.
**C.** Monitor sequence activity.
**D.** Block suspicious activity.
**Answer: (SHOW ANSWER)**
A SAM (Suspicious Activity Monitoring) rule is implemented to provide the function or benefit of blocking suspicious activity. A SAM rule is a rule that defines an action to be taken by the firewall when it detects a suspicious activity, such as an attack, a scan, or a policy violation. The action can be blocking, dropping, rejecting, or logging the traffic that triggered the suspicious activity. A SAM rule can be created manually or automatically by other security features, such as IPS, Anti-Bot, or SmartEvent.[SAM Rules], [Suspicious Activity Rules]

**NEW QUESTION: 11**
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway
**A.** True, CLI is the prefer method for Licensing
**B.** False, Central License are handled via Security Management Server
**C.** False, Central License are installed via Gaia on Security Gateways
**D.** True, Central License can be installed with CPLIC command on a Security Gateway
**Answer: (SHOW ANSWER)**
In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway using the CPLIC command1.This command allows you to install a license from a file or from the

User Center1. Therefore, the correct answer is D.True, Central License can be installed with CPLIC command on a Security Gateway.

**NEW QUESTION: 12**
Name the pre-defined Roles included in Gaia OS.
**A.** AdminRole, and MonitorRole
**B.** ReadWriteRole, and ReadyOnly Role
**C.** AdminRole, cloningAdminRole, and Monitor Role
**D.** AdminRole
**Answer: (SHOW ANSWER)**
The pre-defined Roles included in Gaia OS are AdminRole and MonitorRole. AdminRole is the role that has full access to all Gaia features and commands.MonitorRole is the role that has read-only access to Gaia features and commands1. The other options are not valid pre-defined Roles in Gaia OS.

**NEW QUESTION: 13**
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?
**A.** SND is a feature to accelerate multiple SSL VPN connections
**B.** SND is an alternative to IPSec Main Mode, using only 3 packets
**C.** SND is used to distribute packets among Firewall instances
**D.** SND is a feature of fw monitor to capture accelerated packets
**Answer: (SHOW ANSWER)**
The Secure Network Distributor (SND) is a feature of the Security Gateway that is used to distribute packets among Firewall instances . It improves the performance and scalability of the Firewall by utilizing multiple CPU cores. The other options are not related to SND. [Check Point Security Gateway Architecture and Packet Flow], [Free Check Point CCSA Sample Questions and Study Guide]

**NEW QUESTION: 14**
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: (SHOW ANSWER)**
The Sticky Decision Function (SDF) can only be changed for Load Sharing implementations, not for High Availability implementations4. Check Point ClusterXL R81 Administration Guide

**NEW QUESTION: 15**
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

**A.** All Connections (Clear or Encrypted)
**B.** Accept all encrypted traffic
**C.** Specific VPN Communities
**D.** All Site-to-Site VPN Communities
**Answer: (SHOW ANSWER)**
The option that allows traffic to VPN gateways in specific VPN communities is Specific VPN Communities4. This option enables you to define which VPN communities are allowed in the rule. All Connections (Clear or Encrypted) allows traffic to any destination, regardless of whether it is encrypted or not. Accept all encrypted traffic allows traffic to any encrypted destination, regardless of the VPN community.All Site-to-Site VPN Communities allows traffic to any site-to-site VPN gateway, regardless of the VPN community4. Therefore, the correct answer is C.Specific VPN Communities.

**NEW QUESTION: 16**
Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?
**A.** Both License (.lic) and Contract (.xml) files
**B.** cp.macro
**C.** Contract file (.xml)
**D.** license File (.lie)
**Answer: (SHOW ANSWER)**
The file that is an electronically signed file used by Check Point to translate the features in the license into a code is cp.macro. This file contains a list of macros that define the license features and their values. It is located in the $FWDIR/conf directory on the Security Management Server or Security Gateway.[Check Point R81 Licensing Guide], [Check Point R80.40 Licensing Guide]



**NEW QUESTION: 17**
Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?
**A.** SmartEvent
**B.** SmartView Tracker
**C.** SmartLog

**D.** SmartView Monitor

**Answer: (SHOW ANSWER)**

SmartEvent is a unified security management solution that provides real-time visibility into security events across the network. SmartEvent shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns, as well as generate reports and alerts based on predefined or customized indicators. SmartView Tracker, SmartLog, and SmartView Monitor are other SmartConsole applications that can show logs, search queries, and network statistics respectively, but they do not provide the same level of correlation and analysis as SmartEvent. [Check Point R81 SmartEvent Administration Guide]

**NEW QUESTION: 18**

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: (SHOW ANSWER)**

When an encrypted packet is decrypted, this happens in the security policy4. The security policy is a set of rules that defines how the Security Gateway inspects and secures traffic. The security policy includes VPN rules that specify which traffic should be encrypted or decrypted. The inbound and outbound chains are part of the inspection framework that processes packets according to the security policy. Check Point R81 VPN Administration Guide

**NEW QUESTION: 19**

Which default Gaia user has full read/write access?

**A.** admin

**B.** superuser

**C.** monitor

**D.** altuser

**Answer: (SHOW ANSWER)**

The default Gaia user that has full read/write access isadmin3. The admin user is the superuser that can perform any administrative task on the Gaia system, such as configuring network settings, installing software updates, managing licenses, creating snapshots, and more. The admin user can also access the Gaia Portal, which is a web-based interface for managing Gaia settings and features. Check Point R81 Gaia Administration Guide

**NEW QUESTION: 20**

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: D (LEAVE A REPLY)**
The Advanced Networking Blade is NOT subscription-based and therefore does not have to be renewed on a regular basis1011.The Advanced Networking Blade provides advanced routing capabilities such as BGP, OSPF, VRRP, and multicast routing10.The other blades are subscription-based and require annual renewal to receive updates and support from Check Point1012.

**NEW QUESTION: 21**
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.
**A.** SHA-256
**B.** SHA-200
**C.** MD5
**D.** SHA-128
**Answer: (SHOW ANSWER)**
By default, the SIC certificates issued by R80 Management Server are based on the SHA-256 algorithm1. SHA-256 is a secure hash algorithm that produces a 256-bit digest. SHA-200, MD5, and SHA-128 are not valid algorithms for SIC certificates. SHA-1 and SHA-256 certificates in Check Point Internal CA (ICA)

**NEW QUESTION: 22**
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: (SHOW ANSWER)**
The answer is B because in R80 and above, more than one administrator can login to the Security Management Server with write permission at the same time. Every administrator works in a session that is independent of the other administrators.This is called concurrent administration and it allows multiple administrators to work on the same policy package simultaneously34Check Point R80.10 Concurrent Administration,Check Point R80.40 Security Management Administration Guide

**NEW QUESTION: 23**
Fill in the blanks: The Application Layer Firewalls inspect traffic through the _____ layer(s) of the TCP/IP model and up to and including the _____ layer.

**A.** Upper; Application
**B.** First two; Internet
**C.** Lower; Application
**D.** First two; Transport
**Answer: (SHOW ANSWER)**
The Application Layer Firewalls inspect traffic through theLowerlayer(s) of the TCP/IP model and up to and including theApplicationlayer. The lower layers are the Physical, Data Link, and Network layers, which deal with the transmission and routing of packets. The Application layer is the highest layer of the TCP/IP model, which provides services and protocols for specific applications such as HTTP, FTP, SMTP, etc. The Application Layer Firewalls can inspect the content and context of the traffic and enforce granular security policies based on various criteria such as user identity, application identity, content type, etc. [Check Point R81 Firewall Administration Guide]

**NEW QUESTION: 24**
Fill in the blank: An identity server uses a _____ for user authentication.
**A.** Shared secret
**B.** Certificate
**C.** One-time password
**D.** Token
**Answer: (SHOW ANSWER)**
The answer is A because an identity server uses a shared secret for user authentication. A shared secret is a passphrase that is known by both the identity server and the user. The identity server sends a challenge to the user, who encrypts it with the shared secret and sends it back.The identity server then verifies the response and authenticates the user12Check Point R81 Identity Awareness Administration Guide,Check Point R81 Identity Server

**NEW QUESTION: 25**
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: (SHOW ANSWER)**
The answer is B because Geo policy shared policy is used to create policy for traffic to or from a particular location based on the source or destination country. DLP shared policy is used to prevent data loss by inspecting files and data for sensitive information. Mobile Access software blade is used to provide secure remote access to corporate resources from various devices.HTTPS inspection is used to inspect encrypted web traffic for threats and compliance4Check Point R81 Geo Policy Administration Guide, [Check Point R81 Data Loss

Prevention Administration Guide], [Check Point R81 Mobile Access Administration Guide], [Check Point R81 HTTPS Inspection Administration Guide]

**NEW QUESTION: 26**
Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?
**A.** All Site-to-Site VPN Communities
**B.** Accept all encrypted traffic
**C.** All Connections (Clear or Encrypted)
**D.** Specific VPN Communities
**Answer: (SHOW ANSWER)**
The option that allows all encrypted and non-VPN traffic that matches the rule is Accept all encrypted traffic.This option enables you to allow traffic to any destination that is encrypted, regardless of whether it is part of a VPN community or not2. Therefore, the correct answer is B.Accept all encrypted traffic.

**NEW QUESTION: 27**
What is the purpose of the Clean-up Rule?
**A.** To log all traffic that is not explicitly allowed or denied in the Rule Base
**B.** To clean up policies found inconsistent with the compliance blade reports
**C.** To remove all rules that could have a conflict with other rules in the database
**D.** To eliminate duplicate log entries in the Security Gateway
**Answer: (SHOW ANSWER)**
The purpose of the Clean-up Rule is to log all traffic that is not explicitly allowed or denied in the Rule Base78.The Clean-up Rule is the last rule in the rulebase and is used to drop and log explicitly unmatched traffic97.To improve the rulebase performance, noise traffic that is logged in the Clean-up rule should be included in the Noise rule so it is matched and dropped higher up in the rulebase8. The other options are not valid purposes of the Clean-up Rule.

**NEW QUESTION: 28**
Which of the following is NOT a tracking option? (Select three)
**A.** Partial log
**B.** Log
**C.** Network log
**D.** Full log
**Answer: (SHOW ANSWER)**
The options that are not tracking options are Partial log, Network log, and Full log. Tracking options are settings that determine how the Security Gateway handles traffic that matches a rule in the security policy. The valid tracking options are Log, Detailed Log, Extended Log, Alert, Mail, SNMP trap, User Defined Alert, and None. The other options are incorrect. Log is a tracking option that records basic information about the traffic, such as source, destination, service, action,

etc. Detailed Log is a tracking option that records additional information about the traffic, such as NAT details, data amount, etc. Extended Log is a tracking option that records even more information about the traffic, such as matched IPS protections, application details, etc. [Logging and Monitoring Administration Guide R80 - Check Point Software]

**NEW QUESTION: 29**
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: (SHOW ANSWER)**
Service blades must be attached to a Security Gateway. A Security Gateway is a device that enforces security policies on traffic that passes through it. A service blade is a software module that provides a specific security function, such as firewall, VPN, IPS, etc. A Security Gateway can have one or more service blades attached to it, depending on the license and hardware capabilities. The other options are incorrect. A management container is a virtualized environment that hosts a Security Management Server or a Log Server. A management server is a device that manages security policies and distributes them to Security Gateways. A Security Gateway container is not a valid term in Check Point terminology. [Check Point R81 Security Management Administration Guide], [Check Point R81 CloudGuard Administration Guide]

**NEW QUESTION: 30**
Under which file is the proxy arp configuration stored?
**A.** $FWDIR/state/proxy_arp.conf on the management server
**B.** $FWDIR/conf/local.arp on the management server
**C.** $FWDIR/state/_tmp/proxy.arp on the security gateway
**D.** $FWDIR/conf/local.arp on the gateway
**Answer: (SHOW ANSWER)**
The file that stores the proxy arp configuration is$FWDIR/conf/local.arpon the gateway3. The other files are not related to proxy arp configuration. How to configure Proxy ARP for Manual NAT on Security Gateway, [Check Point CCSA - R81: Practice Test & Explanation]

**NEW QUESTION: 31**
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: (SHOW ANSWER)**

The command cplic print is used to verify license installation. It displays the installed licenses and their expiration dates . [Check Point R81 Command Line Interface Reference Guide],Check Point :: Pearson VUE



**NEW QUESTION: 32**
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: (SHOW ANSWER)**
Plug-and-play (Trial) and Evaluation licenses are considered temporary because they expire after a certain period of time3. Plug-and-play licenses are valid for 15 days, while Evaluation licenses are valid for 30 days. Check Point Licensing and Contract Operations User Guide

**NEW QUESTION: 33**
How can the changes made by an administrator before publishing the session be seen by a superuser administrator?
**A.** By impersonating the administrator with the 'Login as...' option
**B.** They cannot be seen
**C.** From the SmartView Tracker audit log
**D.** From Manage and Settings > Sessions, right click on the session and click 'View Changes...'
**Answer: (SHOW ANSWER)**
The changes made by an administrator before publishing the session can be seen by a superuser administrator from Manage and Settings > Sessions, right click on the session and click 'View Changes...'.This option allows the superuser to review the changes made by another administrator in a pending session1. Check Point R81 Security Management Administration Guide

**NEW QUESTION: 34**
How many layers make up the TCP/IP model?
**A.** 2

**B.** 7
**C.** 6
**D.** 4
**Answer: (SHOW ANSWER)**
The TCP/IP model is made up of four layers: Application, Transport, Internet, and Network Interface1, p. 10. The TCP/IP model is a simplified version of the OSI model, which has seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical. Check Point CCSA - R81: Practice Test & Explanation, [TCP/IP Model Explained]

**NEW QUESTION: 35**
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: (SHOW ANSWER)**
SmartConsole, SmartEvent GUI client, andSmartView Web Applicationallow viewing of billions of consolidated logs and shows them as prioritized security events1.SmartView Web Application is a web-based interface that provides access to SmartEvent reports and dashboards2. Check Point R81 Security Management Administration Guide,Check Point R81 SmartEvent Administration Guide

**NEW QUESTION: 36**
Which back up method uses the command line to create an image of the OS?
**A.** System backup
**B.** Save Configuration
**C.** Migrate
**D.** snapshot
**Answer: D (LEAVE A REPLY)**
According to the Hewlett Packard Enterprise Support Center3, the snapshot command uses the command line to create an image of the OS. A snapshot is a point-in-time copy of a disk partition that can be used to restore the system in case of a failure or corruption. Hewlett Packard Enterprise Support Center

**NEW QUESTION: 37**
Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?
**A.** Formal
**B.** Central
**C.** Corporate

**D.** Local

**Answer: (SHOW ANSWER)**

Check Point licenses are divided into two types: central and local. Central licenses are managed by a Security Management Server and can be attached to any Security Gateway managed by that server. Local licenses are tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address. Formal and corporate are not types of Check Point licenses. [Check Point R81 Licensing and Contract Administration Guide]

**NEW QUESTION: 38**

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: (SHOW ANSWER)**

The ports to which the Client Authentication daemon listens on by default are 259 and 900. Client Authentication is a method that allows users to authenticate with the Security Gateway before they are allowed access to protected resources. The Client Authentication daemon (fwauthd) runs on the Security Gateway and listens for authentication requests on TCP ports 259 and 900 . [Check Point R81 Remote Access VPN Administration Guide], [Check Point R81 Quantum Security Gateway Guide]

**NEW QUESTION: 39**

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: (SHOW ANSWER)**

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using a complete CLI and API interface using SSH and custom CPCode integration. This allows you to automate tasks, integrate with third-party tools, and create custom scripts . 3rd Party integration of CLI and API for Gateways or Management prior to R80 is not relevant for R80 Management. A complete CLI and API interface for Management with 3rd Party integration is not a specific option. [Check Point R81 Security Management Administration Guide], [Check Point Learning and Training Frequently Asked Questions (FAQs)]

**NEW QUESTION: 40**

Which path below is available only when CoreXL is enabled?

**A.** Slow path

**B.** Firewall path

**C.** Medium path
**D.** Accelerated path
**Answer: (SHOW ANSWER)**
The path that is available only when CoreXL is enabled is the medium path. The medium path is used to handle packets that require deeper inspection by the Firewall and IPS blades, but do not need to go through the slow path . The slow path is used to handle packets that require stateful or out-of-state inspection by other blades, such as Application Control or VPN . The firewall path and the accelerated path are available regardless of CoreXL status . [CoreXL R81 Administration Guide], [Check Point CCSA - R81: Practice Test & Explanation], [Check Point Security Gateway Architecture and Packet Flow], [Free Check Point CCSA Sample Questions and Study Guide]

**NEW QUESTION: 41**
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: (SHOW ANSWER)**
Suspicious Activity Monitoring (SAM) is the utility that is used to block activities that appear to be suspicious.SAM allows administrators to block connections from specific IP addresses or network objects for a specified period of time3. Penalty Box is a feature of SAM that automatically blocks connections from sources that generate too many log entries. Drop Rule in the rulebase is a firewall action that discards packets that match certain criteria. Stealth rule is a firewall rule that prevents direct access to the Security Gateway from external sources.

**NEW QUESTION: 42**
What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?
**A.** A host route to route to the destination IP
**B.** Use the file local.arp to add the ARP entries for NAT to work
**C.** Nothing, the Gateway takes care of all details necessary
**D.** Enabling 'Allow bi-directional NAT' for NAT to work correctly
**Answer: (SHOW ANSWER)**
If the NAT property 'Translate destination on client side' is not enabled in Global properties, nothing needs to be configured on the client side, because the Gateway takes care of all details necessary. The Gateway translates the destination IP address before sending the packet to the client, so the client does not need to know about the NAT rule or add any host route or ARP entry.

**NEW QUESTION: 43**
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: (SHOW ANSWER)**
The back up solution that should be used to ensure your database can be restored on that device is snapshot . A snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system. A snapshot can be used to restore a Security Gateway or Security Management Server to its previous state at any time . Therefore, the correct answer is D. snapshot.

**NEW QUESTION: 44**
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 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 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: (SHOW ANSWER)**
The commands you could use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1 after the initial installation on Check Point appliance are:
set interface Mgmt ipv4-address 192.168.80.200 mask-length 24. This command sets the IPv4 address and subnet mask of the Management interface.
set static-route default nexthop gateway address 192.168.80.1 on. This command sets the default gateway for IPv4 routing.
save config. This command saves the configuration changes.

**NEW QUESTION: 45**
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 (LEAVE A REPLY)**
One of the major features in R80.x SmartConsole is concurrent administration, which allows multiple administrators to work on the same Security Policy at the same time12. However, only one administrator can edit a rule at a time.If AdminA and AdminB are editing the same rule at the same time, it will cause a conflict and prevent them from saving their changes12. Therefore, the correct answer is B.AdminA and AdminB are editing the same rule at the same time.

**NEW QUESTION: 46**
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: (SHOW ANSWER)**
Identity Awareness allows the Security Administrator to configure network access based on network location, identity of a user, and identity of a machine1.These are the three main identity sources that Identity Awareness supports1. Identity Awareness R80.40 Administration Guide



**NEW QUESTION: 47**
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: (SHOW ANSWER)**
The default port numbers for an LDAP server are 389 for standard connections and 636 for SSL connections. LDAP (Lightweight Directory Access Protocol) is a protocol that allows access to directory services over TCP/IP. Therefore, the correct answer is B. 389, 636.

**NEW QUESTION: 48**

What is the default shell for the command line interface?

**A.** Clish

**B.** Admin

**C.** Normal

**D.** Expert

**Answer: (SHOW ANSWER)**

Clish is the default shell for the command line interface. It is a user-friendly shell that provides a menu-based and a command-line mode.Admin, Normal, and Expert are not valid shell names1.

**NEW QUESTION: 49**

Name the authentication method that requires token authenticator.

**A.** SecureID

**B.** Radius

**C.** DynamicID

**D.** TACACS

**Answer: (SHOW ANSWER)**

SecureID is the authentication method that requires token authenticator2. SecureID is a two-factor authentication method that uses a hardware or software token to generate a one-time password. The user must enter the token code along with their username and password to authenticate. Check Point R81 Identity Awareness Administration Guide

**NEW QUESTION: 50**

What are the three deployment options available for a security gateway?

**A.** Standalone, Distributed, and Bridge Mode

**B.** Bridge Mode, Remote, and Standalone

**C.** Remote, Standalone, and Distributed

**D.** Distributed, Bridge Mode, and Remote

**Answer: (SHOW ANSWER)**

A security gateway is a device that enforces the security policy on the traffic that passes through it. There are three deployment options available for a security gateway: Standalone, Distributed, and Bridge Mode. Standalone means that the security gateway and the security management server are installed on the same machine. Distributed means that the security gateway and the security management server are installed on separate machines.Bridge Mode means that the security gateway acts as a transparent bridge between two network segments, without changing the IP addressing scheme1. Check Point R81 Security Gateway Technical Administration Guide

**NEW QUESTION: 51**

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: (SHOW ANSWER)**

Security Zones are a feature of Application Control and Identity Awareness that allow you to define groups of network objects based on their level of trust.Security Zones do not work with Manual NAT rules, because Manual NAT rules are applied before the Application Control and Identity Awareness policy is enforced1. Check Point R81 Security Management Administration Guide

**NEW QUESTION: 52**

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: (SHOW ANSWER)**

In R80, IPS is managed by the Threat Prevention Policy567.The Threat Prevention Policy defines how to protect the network from malicious traffic using IPS, Anti-Bot, Anti-Virus, and Threat Emulation software blades5.The IPS layer in the Threat Prevention Policy allows configuring IPS protections and actions for different network segments5. The other options are not true about the IPS-Blade. Check Point IPS Datasheet,Check Point IPS Software Blade,Quantum Intrusion Prevention System (IPS)

**NEW QUESTION: 53**

True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

**A.** True, every administrator works on a different database that Is independent of the other administrators

**B.** False, this feature has to be enabled in the Global Properties.

**C.** True, every administrator works in a session that is independent of the other administrators

**D.** False, only one administrator can login with write permission

**Answer: (SHOW ANSWER)**

SmartConsole is a unified graphical user interface that allows administrators to manage multiple Check Point security products from a single console. More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time. Every administrator works in a session that is independent of the other administrators.The changes made by one administrator are not visible to others until they are published2. Check Point R81 SmartConsole R81 User Guide

**NEW QUESTION: 54**

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: (SHOW ANSWER)**
The tracking actions that can be selected when configuring Spoof Tracking areLog, alert, none. Spoof Tracking is a feature that detects packets with spoofed source IP addresses and logs them in SmartView Tracker. The administrator can choose to log only, log and alert, or do nothing when spoofed packets are detected. The other options are not valid tracking actions for Spoof Tracking, as they are either not available or not relevant for this feature.

**NEW QUESTION: 55**
Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI?
**A.** hostname 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: (SHOW ANSWER)**
The correct syntax for adding a host using GAiA management CLI ismgmt add host name <name> ip-address <ip-address>2. Check Point GAiA R81 Command Line Interface Reference Guide

**NEW QUESTION: 56**
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: (SHOW ANSWER)**
There are two default users on Gaia Platform and neither can be deleted. The two default users are admin and monitor. The admin user has full access to the Gaia configuration and management tools, such as CLI and WebUI. The monitor user has read-only access to the Gaia configuration and management tools, and can only view the system status and settings. These two users cannot be deleted, but their passwords can be changed.[Gaia Administration Guide], [Gaia Overview]

**NEW QUESTION: 57**
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: (SHOW ANSWER)**
Authentication rules are defined foruser groupsrather than individual users1. To define authentication rules, you must first define users and groups.You can define users with the Check Point user database, or with an external server, such as LDAP1.UserCheck is a feature that enables user interaction with security events2. Individual users and all users in the database are not valid options for defining authentication rules. How to Configure Client Authentication,UserCheck

**NEW QUESTION: 58**
What is the best sync method in the ClusterXL deployment?
**A.** Use 1 cluster + 1st sync
**B.** Use 1 dedicated sync interface
**C.** Use 3 clusters + 1st sync + 2nd sync + 3rd sync
**D.** Use 2 clusters + 1st sync + 2nd sync
**Answer: (SHOW ANSWER)**
The best sync method in the ClusterXL deployment is to use one dedicated sync interface56. This method provides optimal performance and reliability for synchronization traffic.Using multiple sync interfaces is not recommended as it increases CPU load and does not provide 100% sync redundancy5. Using multiple clusters is not a sync method, but a cluster topology. Sync Redundancy in ClusterXL,Best Practice for HA sync interface

**NEW QUESTION: 59**
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: (SHOW ANSWER)**
A reason for manual creation of a NAT rule is when the public IP-address is different from the gateway's external IP.This can happen when the gateway is behind another NAT device or firewall3. Check Point R81 Security Gateway Administration Guide,Check Point CCSA - R81: Practice Test & Explanation

**NEW QUESTION: 60**
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: (SHOW ANSWER)**
The difference between the Install Policy button on the SmartConsole's tab and the Install Policy within a specific policy is that the former installs all the policies that are selected in the Install Policy window, while the latter pre-selects the installation for only the current policy and for the applicable gateways5. The other options are not accurate differences. Installing Policies, [Check Point CCSA - R81: Practice Test & Explanation]

**NEW QUESTION: 61**
Which Check Point software blade provides Application Security and identity control?
**A.** Identity Awareness
**B.** Data Loss Prevention
**C.** URL Filtering
**D.** Application Control
**Answer: (SHOW ANSWER)**
The Check Point software blade that provides Application Security and identity control is Application Control3.Application Control enables network administrators to identify, allow, block, or limit usage of thousands of applications and millions of websites3. Therefore, the correct answer is D.Application Control

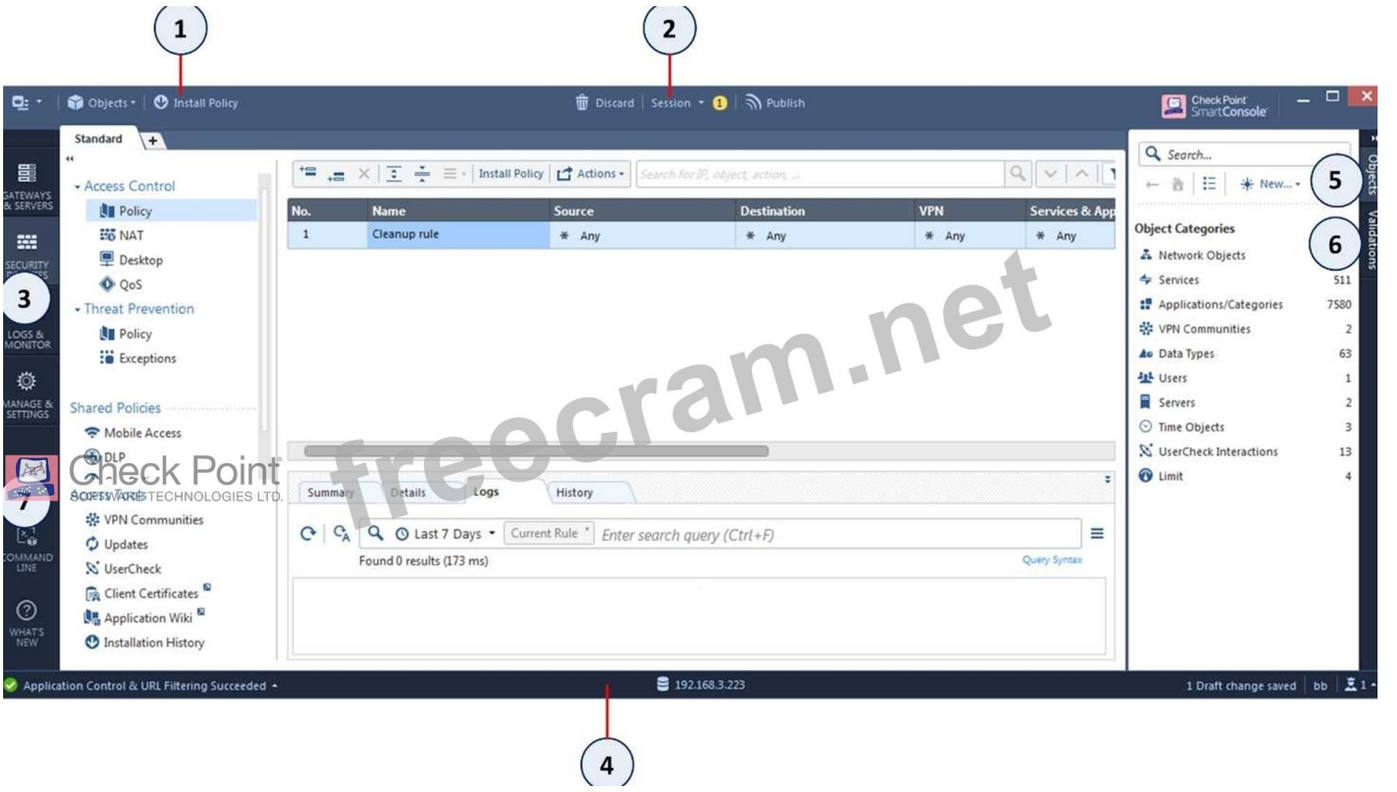


**NEW QUESTION: 62**
When configuring Anti-Spoofing, which tracking options can an Administrator select?
**A.** Log, Alert, None
**B.** Log, Allow Packets, Email
**C.** Drop Packet, Alert, None
**D.** Log, Send SNMP Trap, Email
**Answer: (SHOW ANSWER)**
Log, Alert, and None are the tracking options that an Administrator can select when configuring Anti-Spoofing. Log means that the packet will be logged in SmartView Tracker. Alert means that

the packet will trigger an alert in SmartView Monitor.None means that no action will be taken2. The other options are not valid tracking options.

**NEW QUESTION: 63**
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: (SHOW ANSWER)**
When URL Filtering is set, only the host part of the URL is sent to the Check Point Online Web Service for analysis. The host part is the part of the URL that identifies the web server, such as www.example.com. The Check Point Online Web Service uses this information to categorize the URL and return the appropriate action to the Security Gateway. The other options are not sent to the Check Point Online Web Service for analysis, as they may contain sensitive or irrelevant data.

**NEW QUESTION: 64**
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: (SHOW ANSWER)**
Manage and Command Line is not a valid application navigation tab in the R80 SmartConsole, as it does not exist in the interface.The image shows the navigation toolbar of the R80 SmartConsole, which has four tabs: Security Policies, Logs & Monitor, Gateways & Servers, and Manage & Settings1.The Command Line Interface button is located in the system information area, not in the navigation toolbar1.






**NEW QUESTION: 65**

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

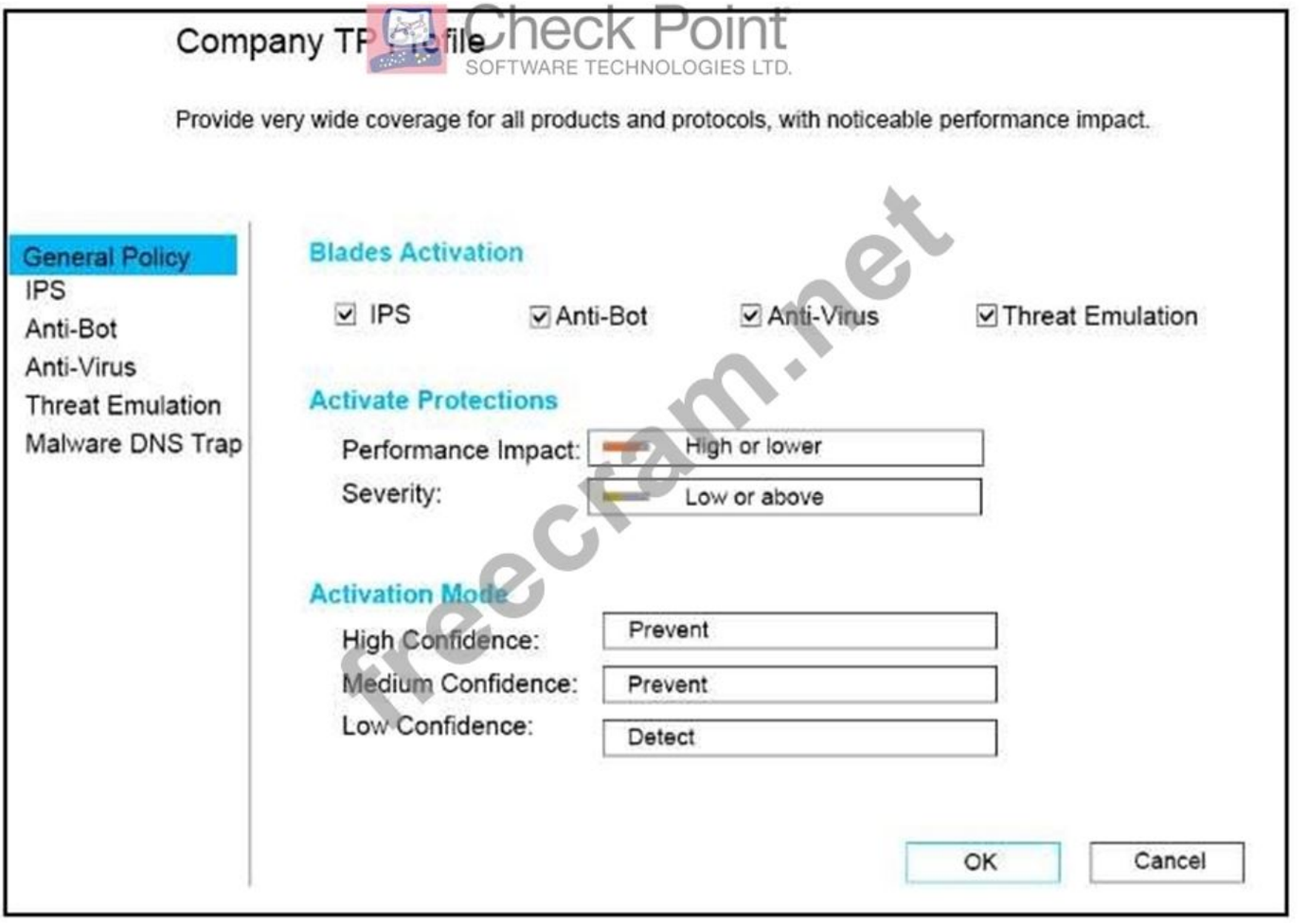
**Answer: (SHOW ANSWER)**

An Endpoint identity agent uses a username/password or Kerberos ticket for user authentication3, p. 28. An Endpoint identity agent is a lightweight client installed on endpoint computers that communicates with Identity Awareness gateways and provides reliable identity information. An Endpoint identity agent does not use a shared secret, a token, or a certificate for user authentication. Check Point CCSA - R81: Practice Test & Explanation, [Check Point Identity Awareness Administration Guide R81]

**NEW QUESTION: 66**

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.




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 Profile. Consider adding more memory to the appliance.

**D.** Set the Performance Impact to Very Low Confidence to Prevent.

**Answer: (SHOW ANSWER)**

The BEST way to tune the profile in order to lower the CPU load still maintaining security at good level is to set the Performance Impact toMedium or lower. This will reduce the number of packets that are inspected by the Threat Prevention blades, while still providing a high level of protection . Setting High Confidence to Low and Low Confidence to Inactive will lower the security level, as it will allow more traffic that may be malicious. The problem is likely with the Threat Prevention Profile, as it can have a significant impact on the CPU utilization of the Security Gateway. Adding more memory to the appliance will not solve the problem, as memory is not the bottleneck in this case. Setting the Performance Impact to Very Low Confidence to Prevent will increase the CPU load, as it will inspect more packets and block more traffic that may be false positives.

**NEW QUESTION: 67**

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: (SHOW ANSWER)**

The function that can NOT be performed in the Unified SmartConsole Gateways and Servers tab isOpen SSH. SSH is a secure shell protocol that allows remote access to a device via command line interface. The Unified SmartConsole does not provide an option to open SSH from the Gateways and Servers tab, as it is not a graphical user interface. The other functions can be performed in the Unified SmartConsole Gateways and Servers tab, such as upgrading the software version, opening WebUI, or opening service request with Check Point Technical Support.

**NEW QUESTION: 68**

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: (SHOW ANSWER)**

The steps you will need to do in SmartConsole in order to get the connection working behind the Internet Security Gateway are:

Define an accept rule in Security Policy. This rule allows the traffic from your internal networks to pass through the Security Gateway.

Define automatic NAT for each network to NAT the networks behind a public IP. This option translates the private IP addresses of your internal networks to a public IP address assigned by your ISP router. This way, your internal networks can communicate with the Internet using a valid IP address.

Publish and install the policy. This step applies the changes you made to the Security Gateway and activates the security and NAT rules.

**NEW QUESTION: 69**

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: (SHOW ANSWER)**
The R80.10 management server can manage gateways with versions R76 and higher34. Versions lower than R76 are not supported by the R80.10 management server. Check Point R80.10 Release Notes,Free Ceck Point CCSA Sample Questions and Study Guide

**NEW QUESTION: 70**
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: (SHOW ANSWER)**
Access roles allow the firewall administrator to configure network access according to remote access clients, a combination of computer or computer groups and networks, and users and user groups12. Therefore, the correct answer is D.

**NEW QUESTION: 71**
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: (SHOW ANSWER)**
When tunnel test packets no longer invoke a response, SmartView Monitor displaysDownfor the given VPN tunnel1. This means that the VPN tunnel is not operational and there is no IKE or IPsec traffic passing through it. No Response, Inactive, and Failed are not valid statuses for VPN tunnels in SmartView Monitor. Smart View Monitor displays status for all S2S VPN tunnels - Phase1 UP

**NEW QUESTION: 72**
What protocol is specifically used for clustered environments?
**A.** Clustered Protocol
**B.** Synchronized Cluster Protocol
**C.** Control Cluster Protocol
**D.** Cluster Control Protocol
**Answer: (SHOW ANSWER)**

The protocol that is specifically used for clustered environments is Cluster Control Protocol (CCP). CCP is a proprietary Check Point protocol that is used for communication between cluster members and for cluster administration. CCP enables cluster members to exchange state information, synchronize connections, monitor interfaces, and perform failover operations. The other options are incorrect. Clustered Protocol, Synchronized Cluster Protocol, and Control Cluster Protocol are not valid terms in Check Point terminology. [Cluster Control Protocol (CCP) - Check Point Software]

**NEW QUESTION: 73**
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: (SHOW ANSWER)**
The way that the objects can be manipulated using the new API integration in R80 Management is JSON. JSON (JavaScript Object Notation) is a lightweight data-interchange format that is easy for humans and machines to read and write. The R80 Management API uses JSON as the primary data format for requests and responses. Therefore, the correct answer is B. JSON.

**NEW QUESTION: 74**
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: (SHOW ANSWER)**
The default layers that are included when creating a new policy layer are Access Control, Threat Prevention, and HTTPS Inspection. Access Control is the layer that defines the basic firewall rules. Threat Prevention is the layer that enables the protection against various types of attacks, such as IPS, Anti-Virus, Anti-Bot, etc.HTTPS Inspection is the layer that allows the inspection of encrypted traffic1. The other options are not the default layers that are included when creating a new policy layer.

**NEW QUESTION: 75**
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: (SHOW ANSWER)**
The actions available in the "Actions" column of a rule in HTTPS Inspection policy are "Inspect" and "Bypass". "Inspect" means that the HTTPS traffic will be decrypted and inspected according to the Access Control policy."Bypass" means that the HTTPS traffic will not be decrypted and will be allowed without inspection1. The other options are not valid actions for HTTPS Inspection policy.

**NEW QUESTION: 76**
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: (SHOW ANSWER)**
Detailed Log is not a valid tracking log option in R80.x3.The tracking log options in R80.x are Log, Full Log, and Extended Log45. Where is 'full log' option in track column,LOGGINGAND MONITORING R80,Logging and Monitoring Administration Guide R80.20



**NEW QUESTION: 77**
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: (SHOW ANSWER)**
The VPN Domains configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear.The VPN Domain is the set of hosts and networks that are allowed to communicate securely with the gateway12. The firewall topologies, NAT rules, and the rule base do not directly affect the VPN encryption decision. Check Point R81 Security Gateway Technical Administration Guide,CCSA/CCSE Exam Tips & Content - R80.X vs. R81.X - Check Point CheckMates

**NEW QUESTION: 78**
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: (SHOW ANSWER)**
The BEST immediate action to take when you have discovered suspicious activity in your network is to create a suspicious action rule to block that traffic.A suspicious action rule is a special type of rule that is triggered when a predefined condition is met, such as a malicious file download, a ransomware attack, or a data exfiltration attempt13. A suspicious action rule can block the traffic, quarantine the source, or send an alert to the administrator. Creating a policy rule to block the traffic may not be effective if the traffic does not match the rule criteria or if the policy installation is delayed. Waiting until traffic has been identified before making any changes may allow the threat to spread or cause more damage. Contacting ISP to block the traffic may not be feasible or timely, and may also affect legitimate traffic. Check Point R81 Security Gateway Technical Administration Guide,Check Point CCSA - R81: Practice Test & Explanation | Udemy

**NEW QUESTION: 79**
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: (SHOW ANSWER)**
To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity.The administrator should install theThreat Prevention Policyafter Publishing the changes3.The Threat Prevention Policy defines how the Security Gateway inspects and protects against threats such as port scans, bot attacks, and zero-day exploits4. Check Point R81 Firewall Administration Guide,Check Point R81 Threat Prevention Administration Guide

**NEW QUESTION: 80**
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: (SHOW ANSWER)**

The Check Point Upgrade Service Engine (CPUSE) is a tool that automates the process of upgrading and installing Check Point products on Gaia OS1.It can also be used to update the Gaia OS itself2. The other options are not valid tools for this purpose. Check Point Upgrade Service Engine (CPUSE) - Gaia Deployment Agent,Check Point R81 Gaia Installation and Upgrade Guide

**NEW QUESTION: 81**

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 (LEAVE A REPLY)**

The three components for Check Point Capsule are Capsule Workspace, Capsule Docs, and Capsule Cloud123.Capsule Workspace provides a secure container on the mobile device that isolates business data and applications from personal data and applications2.Capsule Docs protects business documents everywhere they go with encryption and access control1.Capsule Cloud provides cloud-based security services to protect mobile users from threats3. Check Point Capsule,Check Point Capsule Workspace,Mobile Secure Workspace with Capsule

**NEW QUESTION: 82**

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: (SHOW ANSWER)**

CPUSE - Check Point Upgrade Service Engine is the tool that allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS.CPUSE is a web-based tool that simplifies the installation of software updates, hotfixes, and upgrade packages on Gaia OS2. The other options are not valid tools for updating Gaia OS and Check Point products.

**NEW QUESTION: 83**

Which Threat Prevention profile uses sanitization technology?

**A.** Cloud/data Center

**B.** perimeter

**C.** Sandbox

**D.** Guest Network

**Answer: (SHOW ANSWER)**

Threat Prevention is a comprehensive solution that protects networks from malicious attacks by using multiple security blades, such as Anti-Bot, Anti-Virus, IPS, Threat Emulation, and Threat Extraction. A Threat Prevention profile defines the actions and settings for each blade and can be applied to different network segments or scenarios. The Perimeter profile is one of the predefined profiles that uses sanitization technology to protect users from malicious files and links. Sanitization technology includes Threat Emulation and Threat Extraction blades, which can detect and remove malware from files and web content. [Check Point R81 Threat Prevention Administration Guide]

**NEW QUESTION: 84**

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: (SHOW ANSWER)**

To optimize drops, you can use Priority Queues and fully enable Dynamic Dispatcher on the Security Gateway23. Priority Queues are a mechanism that prioritizes part of the traffic when the Security Gateway is stressed and needs to drop packets. Dynamic Dispatcher is a feature that dynamically assigns new connections to a CoreXL FW instance based on the utilization of CPU cores.To enable both features, you need to run the commandfw ctl multik set_mode 9on the Security Gateway4. Therefore, the correct answer is C.fw ctl multik set_mode 9. CoreXL Dynamic Dispatcher - Check Point Software,Firewall Priority Queues in R80.x / R81.x - Check Point Software,Separate Config for Dynamic Dispatcher and Priority Queues

**NEW QUESTION: 85**

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: (SHOW ANSWER)**

The correct answer is A because a pencil icon in a rule means that you have changed this rule3. The pencil icon indicates that the rule has been modified but not published yet.You can hover over the pencil icon to see who made the change and when3. The other options are not related to the pencil icon. Check Point Learning and Training Frequently Asked Questions (FAQs)

**NEW QUESTION: 86**
The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to "None"?
**A.** No, it will not work independently. Hit Count will be shown only for rules with Track options set as Log or alert
**B.** Yes, it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway
**C.** No, it will not work independently because hit count requires all rules to be logged
**D.** Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways
**Answer: (SHOW ANSWER)**
The Hit count feature will work independently from logging and track the hits even if the Track option is set to "None"1, p. 23.When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways and displays the number of connections that each rule matches in SmartConsole3. Check Point CCSA - R81: Practice Test & Explanation,Check Point Security Management Administration Guide R81

**NEW QUESTION: 87**
Which of the following is NOT supported by Bridge Mode Check Point Security Gateway
**A.** Antivirus
**B.** Data Loss Prevention
**C.** NAT
**D.** Application Control
**Answer: (SHOW ANSWER)**
Bridge Mode Check Point Security Gateway does not support NAT. Bridge Mode is a deployment option that allows the Security Gateway to inspect traffic without being a routing hop.In Bridge Mode, the Security Gateway does not have an IP address and cannot perform NAT1. Therefore, the correct answer is C.NAT.

**NEW QUESTION: 88**
Which of the following are types of VPN communities?
**A.** Pentagon, star, and combination
**B.** Star, octagon, and combination
**C.** Combined and star
**D.** Meshed, star, and combination
**Answer: (SHOW ANSWER)**
The types of VPN communities are Meshed, Star, and Combination. A Meshed community is a group of Security Gateways that have VPN connections between every pair of members. A Star community has one Security Gateway as the center and other Security Gateways or hosts as

satellites. A Combination community is a group of Meshed and Star communities. [Check Point R81 Site-to-Site VPN Administration Guide]

**NEW QUESTION: 89**
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: (SHOW ANSWER)**
Resource is NOT an objects category in SmartConsole1, p. 18. The objects categories in SmartConsole are Network Object, Host, Network, Group, Gateway, Cluster, VPN Community, Service, Time Object, Access Role, Custom Application / Site, Data Center Object, Limit. Check Point CCSA - R81: Practice Test & Explanation, [Check Point SmartConsole R81 Help]

**NEW QUESTION: 90**
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: (SHOW ANSWER)**
The three deployment considerations for a secure network are Remote, Standalone, and Distributed3. Remote deployment means that the Security Management Server and Security Gateway are installed on different machines. Standalone deployment means that the Security Management Server and Security Gateway are installed on the same machine.Distributed deployment means that there are multiple Security Gateways managed by one or more Security Management Servers3. Therefore, the correct answer is C.Remote, Standalone, and Distributed.

**NEW QUESTION: 91**
Which type of attack can a firewall NOT prevent?
**A.** Network Bandwidth Saturation
**B.** Buffer Overflow
**C.** SYN Flood
**D.** SQL Injection
**Answer: (SHOW ANSWER)**
A firewall can NOT prevent a network bandwidth saturation attack, which is a type of denial-of-service (DoS) attack that aims to consume all the available bandwidth of a target network or device1, p. 9.A firewall can prevent other types of attacks, such as buffer overflow, SYN flood,

and SQL injection, by inspecting packets and applying security rules2, p. 11-12. Check Point CCSA - R81: Practice Test & Explanation,156-315.81 Checkpoint Exam Info and Free Practice Test



**NEW QUESTION: 92**
The SIC Status "Unknown" means
**A.** There is connection between the gateway and Security Management Server but it is not trusted.
**B.** The secure communication is established.
**C.** There is no connection between the gateway and Security Management Server.
**D.** The Security Management Server can contact the gateway, but cannot establish SIC.
**Answer: (SHOW ANSWER)**
The SIC Status "Unknown" means that there is no connection between the gateway and Security Management Server.This can happen if the gateway is down, unreachable, or has not been initialized yet12. Check Point R81 Security Management Administration Guide,Free Check Point CCSA Sample Questions and Study Guide

**NEW QUESTION: 93**
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: (SHOW ANSWER)**
The SOLR database is used for full text search and enables powerful matching capabilities3. SOLR is an open source enterprise search platform that provides fast and scalable indexing and searching of data. It supports advanced features such as faceting, highlighting, spell checking, synonyms, etc.The SOLR database is used by Check Point products such as SmartLog and SmartEvent to store and query logs and events3. The other options are incorrect. Option B is false, as SOLR does not write data to the database, but only reads data from it. Option C is false, as SOLR does not serve GUI, but only provides a RESTful API for queries. Option D is false, as

SOLR does not enable powerful matching capabilities and write data to the database, but only enables powerful matching capabilities. SOLR - Check Point Software, [Apache Solr]

**NEW QUESTION: 94**
To view the policy installation history for each gateway, which tool would an administrator use?
**A.** Revisions
**B.** Gateway installations
**C.** Installation history
**D.** Gateway history
**Answer: (SHOW ANSWER)**
To view the policy installation history for each gateway, an administrator would use the Installation history tool1, p. 22.The Installation history tool shows the date and time of each policy installation, the name of the administrator who installed it, and the status of the installation3. Revisions, Gateway installations, and Gateway history are not valid tools in SmartConsole. Check Point CCSA - R81: Practice Test & Explanation,Check Point SmartConsole R81 Help

**NEW QUESTION: 95**
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: (SHOW ANSWER)**
Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use Gaia embedded as the operating system.Gaia embedded is a lightweight version of Gaia that is designed for small and medium businesses1. Centos Linux, Gaia, and Red Hat Enterprise Linux version 5 are not the operating systems used by Rugged appliances.

**NEW QUESTION: 96**
Which repositories are installed on the Security Management Server by SmartUpdate?
**A.** License and Update
**B.** Package Repository and Licenses
**C.** Update and License & Contract
**D.** License & Contract and Package Repository
**Answer: (SHOW ANSWER)**
According to the Managing and Installing license via SmartUpdate2, there are two repositories installed on the Security Management Server by SmartUpdate: License & Contract and Package Repository. The License & Contract repository stores all licenses available and all of the assigned licenses. The Package Repository stores all packages downloaded from the Check Point Cloud or uploaded from a local device. Managing and Installing license via SmartUpdate

**NEW QUESTION: 97**
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: (SHOW ANSWER)**
Upgrading the Security Gateway does not require a new license to be generated and installed. The license is tied to the IP address or hostname of the Security Gateway, not the software version.However, if the IP address or hostname changes, the existing license expires, or the license is upgraded, a new license must be generated and installed12Check Point R81,Managing and Installing license via SmartUpdate

**NEW QUESTION: 98**
How would you determine the software version from the CLI?
**A.** fw ver
**B.** fw stat
**C.** fw monitor
**D.** cpinfo
**Answer: (SHOW ANSWER)**
The command that can be used to determine the software version from the CLI is fw ver.This command displays the version of the firewall module and the build number3. fw stat, fw monitor, and cpinfo are not commands for software version identification. Check Point R81 Command Line Interface Reference Guide, [156-315.81 Checkpoint Exam Info and Free Practice Test - ExamTopics]

**NEW QUESTION: 99**
In which scenario will an administrator need to manually define Proxy ARP?
**A.** When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
**B.** When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
**C.** When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
**D.** When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.
**Answer: (SHOW ANSWER)**
NAT (Network Address Translation) is a technique that modifies the IP addresses or ports of packets that pass through a security gateway. NAT can be configured in two ways: Automatic or Manual. Automatic NAT means that the NAT rules are generated automatically by the security

gateway based on the NAT properties of network objects. Manual NAT means that the NAT rules are defined explicitly by the administrator in the NAT policy. Proxy ARP (Address Resolution Protocol) is a technique that allows a security gateway to answer ARP requests on behalf of other hosts. Proxy ARP is needed when a host on one network segment tries to communicate with a host on another network segment that has a different IP address than its own. In some scenarios, an administrator will need to manually define Proxy ARP for NAT to work properly.One such scenario is when they configure a Manual Static NAT which translates to an IP address that does not belong to one of the firewall's interfaces2. Check Point R81 Network Address Translation Administration Guide

**NEW QUESTION: 100**

Which of the following is used to enforce changes made to a Rule Base?

**A.** Publish database

**B.** Save changes

**C.** Install policy

**D.** Activate policy

**Answer: C (LEAVE A REPLY)**

The option that is used to enforce changes made to a Rule Base is Install policy.Installing policy is the process of sending the security policy and the network objects from the Security Management Server to the Security Gateway1, p. 22.Publishing database and saving changes are options that are used to save changes made to a Rule Base, but they do not enforce them on the Security Gateway2. Activating policy is not a valid option in SmartConsole. Check Point CCSA - R81: Practice Test & Explanation,Check Point SmartConsole R81 Help

**NEW QUESTION: 101**

Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

**A.** Kerberos Ticket Renewed

**B.** Kerberos Ticket Requested

**C.** Account Logon

**D.** Kerberos Ticket Timed Out

**Answer: (SHOW ANSWER)**

The Windows Security Event that will NOT map a username to an IP address in Identity Awareness isKerberos Ticket Timed Out. This event occurs when a Kerberos ticket expires and is not renewed, which means that the user is no longer active on the network. Identity Awareness does not use this event to map a username to an IP address, as it does not indicate a valid user session. The other events are used by Identity Awareness to map a username to an IP address, as they indicate a successful user authentication or activity on the network.

**NEW QUESTION: 102**

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

**A.** Networks
**B.** Users
**C.** Time
**D.** Machines
**Answer: (SHOW ANSWER)**
The following cannot be configured in an Access Role Object:Time4.An Access Role Object is a way to define a group of users based on four criteria: Networks, Users, Machines, and Locations5. Networks are IP addresses or network objects that represent the source or destination of the traffic. Users are user accounts or user groups from an identity source such as LDAP or RADIUS. Machines are endpoints that are identified by MAC addresses or certificates. Locations are geographical regions based on IP addresses. Check Point R81 Firewall Administration Guide,Check Point R81 Identity Awareness Administration Guide

**NEW QUESTION: 103**
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: (SHOW ANSWER)**
URL Filtering employs a technology called UserCheck, which educates users on web usage policy in real time. UserCheck is a feature that allows the firewall to interact with the users and inform them about the web usage policy and its violations. UserCheck can also allow users to request access to blocked websites or report false positives. UserCheck helps users understand and comply with the web usage policy and reduces the workload of the administrators.

**NEW QUESTION: 104**
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: (SHOW ANSWER)**
The default Threat Prevention Profiles in R80 Management are Basic, Optimized, and Strict1. There is no Recommended profile by default. You can create a custom profile and name it

Recommended, but it is not included by default. Check Point R81 Threat Prevention Administration Guide

**NEW QUESTION: 105**
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: (SHOW ANSWER)**
Identity Awareness is a blade that enables administrators to define access rules based on the identity of users and machines, rather than just IP addresses. Identity Awareness allows easy configuration for network access and auditing based on three items: network location, the identity of a user, and the identity of a machine. Network location refers to the source or destination network segment of the traffic. The identity of a user refers to the username or group membership of the user who initiates or receives the traffic. The identity of a machine refers to the hostname or certificate of the machine that initiates or receives the traffic. [Check Point R81 Identity Awareness Administration Guide]

**NEW QUESTION: 106**
Which of the following is NOT a role of the SmartCenter:
**A.** Status monitoring
**B.** Policy configuration
**C.** Certificate authority
**D.** Address translation
**Answer: (SHOW ANSWER)**
Address translation is not a role of the SmartCenter, as it is performed by the Security Gateway based on the NAT policy configured in the SmartConsole5.The other options are roles of the SmartCenter, as it is responsible for status monitoring, policy configuration, and certificate authority for the Security Gateways5.

**NEW QUESTION: 107**
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or_____.
**A.** On all satellite gateway to satellite gateway tunnels
**B.** On specific tunnels for specific gateways
**C.** On specific tunnels in the community
**D.** On specific satellite gateway to central gateway tunnels
**Answer: (SHOW ANSWER)**
Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, oron specific tunnels in the community. This option allows the administrator to select which tunnels should be permanent and which should be established on demand. The other options are not valid, as they do not match the available choices in the VPN community settings.

**NEW QUESTION: 108**
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 (LEAVE A REPLY)**
The components of Check Point Capsule are Capsule Docs, Capsule Cloud, and Capsule Workspace123. There is no Capsule Enterprise component. Capsule Docs protects business documents everywhere they go. Capsule Cloud protects mobile users outside the enterprise security perimeter. Capsule Workspace creates a secure business environment on mobile devices. Check Point Capsule Datasheet,Check Point Capsule Workspace Datasheet,Mobile Secure Workspace with Capsule

**NEW QUESTION: 109**
Can multiple administrators connect to a Security Management Server at the same time?
**A.** No, only one can be connected
**B.** Yes, all administrators can modify a network object at the same time
**C.** Yes, every administrator has their own username, and works in a session that is independent of other administrators
**D.** Yes, but only one has the right to write
**Answer: (SHOW ANSWER)**
Multiple administrators can connect to a Security Management Server at the same time, and each administrator has their own username and works in a session that is independent of other administrators1. This allows concurrent administration and prevents conflicts between different administrators. The other options are incorrect. Only one administrator can be connected is false. All administrators can modify a network object at the same time is false, as only one administrator can lock and edit an object at a time. Only one has the right to write is false, as all administrators

have write permissions unless they are restricted by roles or permissions. Security Management Server - Check Point Software

**NEW QUESTION: 110**

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: (SHOW ANSWER)**

Gaia can be configured using the command line interface (CLI) or the WebUI. The CLI is a text-based interface that allows you to configure and manage Gaia settings using commands and scripts. The WebUI is a graphical interface that allows you to configure and manage Gaia settings using a web browser. Gaia Interface and GaiaUI are not valid terms for Gaia configuration tools. [Gaia Administration Guide], [Gaia Overview]

**NEW QUESTION: 111**

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: (SHOW ANSWER)**

The answer is B because querying logs now is very fast because the Indexing Engine indexes logs for faster search results. The Indexing Engine is a component of the Smart-1 appliance that creates indexes for log fields and values, such as source, destination, action, and time. The indexes enable quick and efficient searches of large amounts of log data.[Check Point R81 Logging and Monitoring Administration Guide], [Check Point R81 Indexing Engine]

**NEW QUESTION: 112**

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

**A.** show unsaved

**B.** show save-state

**C.** show configuration diff

**D.** show config-state

**Answer: D (LEAVE A REPLY)**

The commandshow cnfig-statecan beused to verify if there are unsaved changes in GAiA that will be lost with a reboot . The other commands are not valid in GAiA. [Check Point GAiA Administration Guide], [Check Point CCSA - R81: Practice Test & Explanation]

**NEW QUESTION: 113**
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: (SHOW ANSWER)**
Extended Log is a tracking option that enables administrators to see additional information about the traffic that matches a security rule, such as data type, file name, file size, etc. However, to see any data type information, Content Awareness must be enabled on the Security Gateway. Content Awareness is a blade that inspects files based on their type, size, name, and data.Content Awareness is required for Extended Log to work properly3. Check Point R81 Content Awareness Administration Guide

**NEW QUESTION: 114**
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: (SHOW ANSWER)**
The position of an implied rule is manipulated in the Global Properties window. Implied rules are predefined rules that are not displayed in the rule base. They allow or block traffic for essential services such as communication with Check Point servers, logging, and VPN traffic.The position of an implied rule can be changed in the Global Properties > Firewall > Implied Rules section56. How to view Implied Rules in R80.x / R81.x SmartConsole,Implied Rules

**NEW QUESTION: 115**
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: (SHOW ANSWER)**
The scenario where it is a valid option to transfer a license from one hardware device to another is from a 4400 Appliance to a 2200 Appliance. This is because both appliances are Check Point products and have the same license type (Central License).You can transfer a license from one hardware device to another if they have the same license type and vendor3. Therefore, the correct answer is A.From a 4400 Appliance to a 2200 Appliance.

**NEW QUESTION: 116**
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: (SHOW ANSWER)**
The three types of UserCheck messages are inform, ask, and block. Inform messages notify users about security events and do not require any user action. Ask messages prompt users to choose whether to allow or block an action.Block messages prevent users from performing an action and display a reason1. Check Point R81 Logging and Monitoring Administration Guide

**NEW QUESTION: 117**
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: (SHOW ANSWER)**
The Stealth Rule is used to prevent users from directly connecting to a Security Gateway.It is usually placed at the top of the rule base, before any other rule that allows traffic to the Security Gateway1, p. 32. Check Point CCSA - R81: Practice Test & Explanation

**NEW QUESTION: 118**
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: (SHOW ANSWER)**
The correct answer is D because the commandsave onfiguration <filename>storesthe Gaia configuration in a file for later reference1.The oter commands are not valid in Gaia Clish1. Gaia R81.10 Administration Guide

**NEW QUESTION: 119**
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: (SHOW ANSWER)**
The method to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server is Save Policy.Saving a policy updates the trusted log server with the latest policy and configuration changes3. Check Point R81 Logging and Monitoring Administration Guide

**NEW QUESTION: 120**
URL Filtering cannot be used to:
**A.** Control Bandwidth issues
**B.** Control Data Security
**C.** Improve organizational security
**D.** Decrease legal liability
**Answer: (SHOW ANSWER)**
URL Filtering is a blade that enables administrators to control access to millions of websites by category, users, groups, and machines. URL Filtering can be used to improve organizational security, decrease legal liability, and control data security by preventing users from accessing malicious or inappropriate websites.However, URL Filtering cannot be used to control bandwidth issues, such as limiting the amount of traffic or prioritizing certain applications over others3. For that purpose, other blades such as QoS (Quality of Service) or SecureXL are more suitable. Check Point R81 URL Filtering Administration Guide

**NEW QUESTION: 121**
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: (SHOW ANSWER)**
The "Hit Count" feature is enabled or disabled on the Policy layer in SmartConsole1. To enable or disable the "Hit Count" feature, right-click on the Policy layer and select "Edit Layer".Then, check or uncheck the "Enable Hit Count" option1. Solved: Hit Count in R80.x

**NEW QUESTION: 122**
Security Gateway software blades must be attached to what?
**A.** Security Gateway
**B.** Security Gateway container
**C.** Management server
**D.** Management container
**Answer: (SHOW ANSWER)**
Security Gateway software blades must be attached to a Security Gateway container. A Security Gateway container is a logical object that represents a physical or virtual machine that runs the Security Gateway software. A software blade is a modular security feature that can be enabled or disabled eway container. A software blade can provide functions such as firewall, VPN, IPS, anti-virus, anti-bot, application control, URL filtering, etc.[Security Gateway Containers], [Software Blades]

**NEW QUESTION: 123**
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: (SHOW ANSWER)**
When logging in for the first time to a Security Management Server through SmartConsole, a fingerprint is saved to the SmartConsole cache and is available for future Security Management Server authentications. The fingerprint is a unique identifier of the Security Management Server that is used to verify its identity and prevent man-in-the-middle attacks. The SmartConsole cache is a local folder on the client machine that stores temporary files and settings.

**NEW QUESTION: 124**
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?
**A.** Any size
**B.** Less than 20GB
**C.** More than 10GB and less than 20 GB
**D.** At least 20GB
**Answer: (SHOW ANSWER)**

The correct answer is D because the recommended size of the root partition for a dedicated R80 SmartEvent server is at least 20GB2. Any size, less than 20GB, or more than 10GB and less than 20GB are not sufficient for the SmartEvent server. Check Point R80.40 Installation and Upgrade Guide

**NEW QUESTION: 125**
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?
**A.** Export R80 configuration, clean install R80.10 and import the configuration
**B.** CPUSE online upgrade
**C.** CPUSE offline upgrade
**D.** SmartUpdate upgrade
**Answer: C (LEAVE A REPLY)**
The best upgrade method when the management server is not connected to the Internet is CPUSE offline upgrade . This method allows you to download the upgrade package from another source and install it manually on the management server. The other methods require Internet connection or are not supported for R80.10. [R80.10 Upgrade Verification and FAQ], [Check Point CCSA - R81: Practice Test & Explanation]

**NEW QUESTION: 126**
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: (SHOW ANSWER)**
Gaia has two default user accounts that cannot be deleted. They are Admin and Monitor. Admin is the user account that has full administrative privileges and can access both WebUI and CLI.Monitor is the user account that has read-only privileges and can access only WebUI2. The other options are not default user accounts in Gaia.

**NEW QUESTION: 127**
What command would show the API server status?
**A.** cpm status
**B.** api restart
**C.** api status
**D.** show api status
**Answer: (SHOW ANSWER)**
The commandapi statusshows the API server status, including whether it is enabled or not, the port number, and the API version1. Check Point R81 API Reference Guide

**NEW QUESTION: 128**
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: (SHOW ANSWER)**
Browser-Based Authentication is the best method for enabling Identity Awareness on the Check Point firewalls for users who use company issued or personal laptops. Browser-Based Authentication redirects users to a web page where they enter their credentials to access the network resources. This method does not require any installation or configuration on the user's device and supports any operating system and browser. AD Query is a method that queries Active Directory servers for user login events and maps them to IP addresses. This method does not work for personal laptops that are not joined to the domain. Identity Agents are software agents that run on Windows or macOS devices and provide user and machine identity information to the firewall. This method requires installation and management of the agents on each device, which may not be feasible for personal laptops. Terminal Servers Agent is a method that identifies users who connect to Windows Terminal Servers or Citrix servers via RDP or ICA protocols.This method does not apply to laptops that connect directly to the network910Identity Awareness Reference Architecture and Best Practices,Part 10 - Identity

**NEW QUESTION: 129**
What is NOT an advantage of Stateful Inspection?
**A.** High Performance
**B.** Good Security
**C.** No Screening above Network layer
**D.** Transparency
**Answer: (SHOW ANSWER)**
The option that is NOT an advantage of Stateful Inspection isNo Screening above Network layer. Stateful Inspection is a firewall technology that inspects packets at all layers of the OSI model, from layer 3 (Network) to layer 7 (Application). Stateful Inspection provides screening above Network layer, such as checking TCP flags, sequence numbers, ports, and application protocols . The other options are advantages of Stateful Inspection, as it provides high performance, good security, and transparency for legitimate traffic.

**NEW QUESTION: 130**
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: (SHOW ANSWER)**
When using Automatic Hide NAT,Source Port Address Translation (PAT)is enabled by default1. This means that the source IP address and port number are translated to a different IP address and port number. This allows multiple hosts to share a single IP address for outbound connections. Check Point R81 Firewall Administration Guide

**NEW QUESTION: 131**
Is it possible to have more than one administrator connected to a Security Management Server at once?
**A.** Yes, but only if all connected administrators connect with read-only permissions.
**B.** Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
**C.** No, only one administrator at a time can connect to a Security Management Server
**D.** Yes, but only one of those administrators will have write-permissions. All others will have read-only permission.
**Answer: (SHOW ANSWER)**
It is possible to have more than one administrator connected to a Security Management Server at once, but objects edited by one administrator will be locked for editing by others until the session is published. This feature is called concurrent administration and it allows multiple administrators to work on the same security policy at the same time. However, when one administrator edits an object, such as a gateway, a rule, or a network, that object is locked for other administrators until the change is published or discarded. The lock icon shows which objects are being edited by other administrators and prevents conflicts or overwrites.[Concurrent Administration], [SmartConsole Overview]

**NEW QUESTION: 132**
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: (SHOW ANSWER)**
Back up and restores can be accomplished throughSmartConsole, WebUI, or CLI12.These are the methods to perform system backup and restore, which save and restore the Gaia OS configuration and the Security Management Server database1.WebUI, CLI, or SmartUpdate are not valid methods, as SmartUpdate is used to install software packages and patches, not to back up or restore the system3.CLI, SmartUpdate, or SmartBackup are not valid methods, as SmartBackup is a feature of SmartProvisioning that allows backing up and restoring the configuration of Security Gateways and VSX clusters4.SmartUpdate, SmartBackup, or

SmartConsole are not valid methods, as SmartConsole is used to configure and manage the Security Policy, not to back up or restore the system5.

**NEW QUESTION: 133**

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: (SHOW ANSWER)**

If Deyra sees the gateway status as shown in the image, it means thatthere is a blade reporting a problem. The red "X" in the status column indicates that one or more blades on the Security Gateway have a problem that requires attention. The other options are not correct, as they do not match the status shown in the image. If the SmartCenter Server cannot reach this Security Gateway, the status column would show a yellow triangle with an exclamation mark. If the VPN software blade is reporting a malfunction, the blades column would show a red "X" on the VPN icon. If the Security Gateway's MGNT NIC card is disconnected, the IP column would show "N/A" instead of the IP address.


**NEW QUESTION: 134**

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

**A.** STATE Engine

**B.** TRACK Engine

**C.** RECORD Engine

**D.** INSPECT Engine

**Answer: (SHOW ANSWER)**

The INSPECT Engine is the core component of Check Point's Stateful Inspection technology. It is used to extract state related information from packets and store that information in state tables.The INSPECT Engine also evaluates the security policy and enforces it on the packets1. Check Point R81 Security Gateway Technical Administration Guide

**NEW QUESTION: 135**

Which of the following is NOT a component of a Distinguished Name?

**A.** Common Name

**B.** Country

**C.** User container

**D.** Organizational Unit

**Answer: (SHOW ANSWER)**

A Distinguished Name (DN) is a unique identifier for an entry in an LDAP directory. A DN consists of a sequence of relative distinguished names (RDNs) separated by commas. Each RDN is composed of an attribute type and an attribute value, such as cn=John Smith or ou=Sales. A DN can have different components depending on the structure and schema of the LDAP directory, but some common components are: Common Name (cn), Country , Organizational Unit (ou), Organization (o), State or Province (st), and Locality (l).User container is not a component of a DN3. Check Point R81 Identity Awareness Administration Guide

**NEW QUESTION: 136**

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: (SHOW ANSWER)**

Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for licensed Check Point products for the Gaia operating system and the Gaia operating system itself. CPUSE is an advanced tool that automates software updates and upgrades on Gaia platforms. It can download and install packages such as hotfixes, Jumbo Hotfix Accumulators,

minor versions, major versions, and OS updates.[CPUSE - Gaia Software Updates (including Gaia Software Updates Agent)], [Check Point R81]



**NEW QUESTION: 137**
Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?
**A.** AES-GCM-256
**B.** AES-CBC-256
**C.** AES-GCM-128
**Answer: B (LEAVE A REPLY)**
The answer is B because AES-CBC-256 is not a supported encryption algorithm for IPsec Security Associations (Phase 2) in R81.The supported encryption algorithms are AES-GCM-128, AES-GCM-256, AES-CBC-128, 3DES, and NULL3Check Point R81 VPN Administration Guide

**NEW QUESTION: 138**
When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:
**A.** Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
**B.** The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
**C.** The entire Management Database and all sessions and other administrators can connect only as Read-only.
**D.** Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.
**Answer: (SHOW ANSWER)**
The answer is D because in R80 and above, the first administrator to connect to the Management Server using SmartConsole gets a lock on only the objects being modified in his session of the Management Database. Other administrators can connect to make changes using different sessions, but they cannot modify the same objects as the first administrator until he publishes his changes.This is called concurrent administration and it allows multiple administrators to work on

the same policy package simultaneously12Check Point R80.10 Concurrent Administration,Check Point R80.40 Security Management Administration Guide

**NEW QUESTION: 139**
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: (SHOW ANSWER)**
SmartView Monitor is the tool that allows you to monitor the top bandwidth on SmartConsole. SmartView Monitor is a graphical tool that displays real-time network and security performance data, such as traffic, throughput, connections, CPU usage, memory usage, etc. You can use SmartView Monitor to identify the top bandwidth consumers and optimize your network performance.[SmartView Monitor], [Monitoring Network Traffic]

**NEW QUESTION: 140**
What Identity Agent allows packet tagging and computer authentication?
**A.** Endpoint Security Client
**B.** Full Agent
**C.** Light Agent
**D.** System Agent
**Answer: (SHOW ANSWER)**
The Full Identity Agent allows packet tagging and computer authentication2. Packet tagging is a feature that enables the Security Gateway to identify the source user and machine of each packet, regardless of NAT or routing. Computer authentication is a feature that enables the Security Gateway to authenticate machines that are not associated with any user, such as servers or unattended workstations. The other options are incorrect. Endpoint Security Client is not an Identity Agent, but a software that provides endpoint security features such as firewall, antivirus, VPN, etc. Light Agent is an Identity Agent that does not require installation and runs on a web browser, but it does not support packet tagging or computer authentication. System Agent is not an Identity Agent, but a software that provides system information and health monitoring for endpoints. Check Point Identity Agent for Microsoft Windows 10

**NEW QUESTION: 141**
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: A (LEAVE A REPLY)**

From the Gaia web interface, the operation that CANNOT be performed on a Security Management Server is Verify a Security Policy.This operation can only be done from SmartConsole4. Check Point R81 SmartConsole Online Help