CheckPoint.156-215.80.v2022-07-09.q193

Exam Code:	156-215.80
Exam Name:	Check Point Certified Security Administrator R80
Certification Provider:	CheckPoint
Free Question Number:	193
Version:	v2022-07-09
# of views:	3321
# of Questions views:	1930
https://www.freeqas.com/qa/CheckPoint/156-215.80/CheckPoint.156-215.80.v2022-07-09.q193.html	

NEW QUESTION: 1
Review the following screenshot and select the BEST answer.

A. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.
B. By default all layers are shared with all policies.
C. Data Center Layer is an inline layer in the Access Control Policy.
D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 2
What does the "unknown" SIC status shown on SmartConsole mean?
A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
B. SIC activation key requires a reset.
C. The SIC activation key is not known by any administrator.
D. There is no connection between the Security Gateway and SMS.
Answer: D (LEAVE A REPLY)
The most typical status is Communicating. Any other statusindicates that the SIC communication is problematic.
For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server.
If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

NEW QUESTION: 3
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:
A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517081623_70199443034f806cf2dd0a7ba15f201c&xtn=.pdf

NEW QUESTION: 4
Fill in the blanks: A High Availability deployment is referred to as a _____ cluster and a Load Sharing deployment is referred to as a _____ cluster.
A. Standby/standby; active/active
B. Active/active; standby/standby
C. Active/active; active/standby;
D. Active/standby; active/active
Answer: (SHOW ANSWER)
In a High Availability cluster, only one member is active (Active/Standby operation).
ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle network traffic (Active/Active operation).

NEW QUESTION: 5

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:
A. There is no memory used for saving a fingerprint anyway.
B. SmartConsole cache is available for future Security Management Server authentications.
C. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
D. Windows registry is available for future Security Management Server authentications.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
Which of the following is NOT an alert option?
A. SNMP
B. High alert
C. Mail
D. User defined alert
Answer: B (LEAVE A REPLY)
Explanation
In Action, select:
* none - No alert.
* log - Sends a log entry to the database.
* alert - Opens a pop-up window to your desktop.
* mail - Sends a mail alert to your Inbox.
* snmptrap - Sends an SNMP alert.
* useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

NEW QUESTION: 7
Which Check Point feature enables application scanning and the detection?
A. Application Dictionary
B. AppWiki
C. Application Library
D. CPApp
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
AppWiki Application Classification Library
AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.
Reference: https://www.checkpoint.com/products/application-control-software-blade/

NEW QUESTION: 8

On the following graphic, you will find layers of policies.

What is a precedence of traffic inspection for the defined polices?

A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.

B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer

C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.

D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

For example, when you upgrade to R80 from earlier versions:

- Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

- Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.

All layers are evaluated in parallel

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

NEW QUESTION: 9
Can multiple administrators connect to a Security Management Server at the same time?
A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other
administrators
D. Yes, but only one has the right to write
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
What are the advantages of a "shared policy" in R80?
A. Allows the administrator to share a policy so that it is available to use in another Policy Package
B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
C. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway
D. Allows the administrator to share a policy between all the users identified by the Security Gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
Which default user has full read/write access?
A. Monitor
B. Altuser
C. Administrator
D. Superuser
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 12
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: (SHOW ANSWER)
Explanation
References:

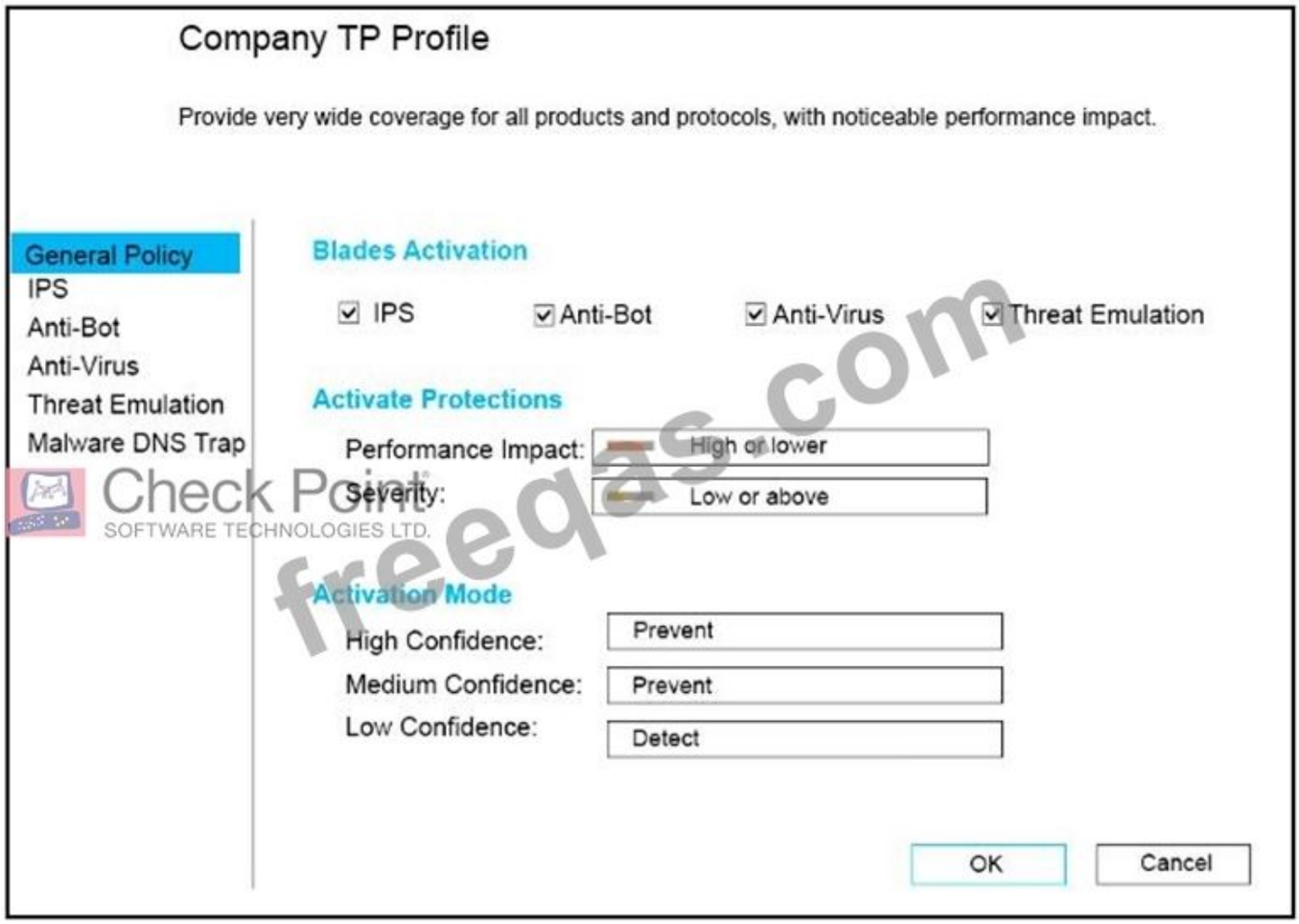
NEW QUESTION: 13
What happens when you run the command: fw sam -J src [Source IP Address]?

A. Connections to the specified target are blocked without the need to change the Security Policy.
B. Connections to and from the specified target are blocked without the need to change the Security Policy.
C. Connections to and from the specified target are blocked with the need to change the Security Policy.
D. Connections from the specified source are blocked without the need to change the Security Policy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 14
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?
A. None, Security Management Server would be installed by itself.
B. SmartEvent
C. SmartConsole
D. SecureClient
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?
A. Auditor
B. Read Only All
C. Super User
D. Full Access
Answer: B (LEAVE A REPLY)
Explanation
To create a new permission profile:
In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
Click New Profile.
The New Profile window opens.
Enter a unique name for the profile.
Select a profile type:
Read/Write All - Administrators can make changes
Auditor (Read Only All) - Administrators can see information but cannot make changes Customized - Configure custom settings Click OK.

NEW QUESTION: 16
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 the Performance Impact to Medium or lower.

B. Set High Confidence to Low and Low Confidence to Inactive.

C. Set the Performance Impact to Very Low Confidence to Prevent.

D. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.

Answer: A (LEAVE A REPLY)

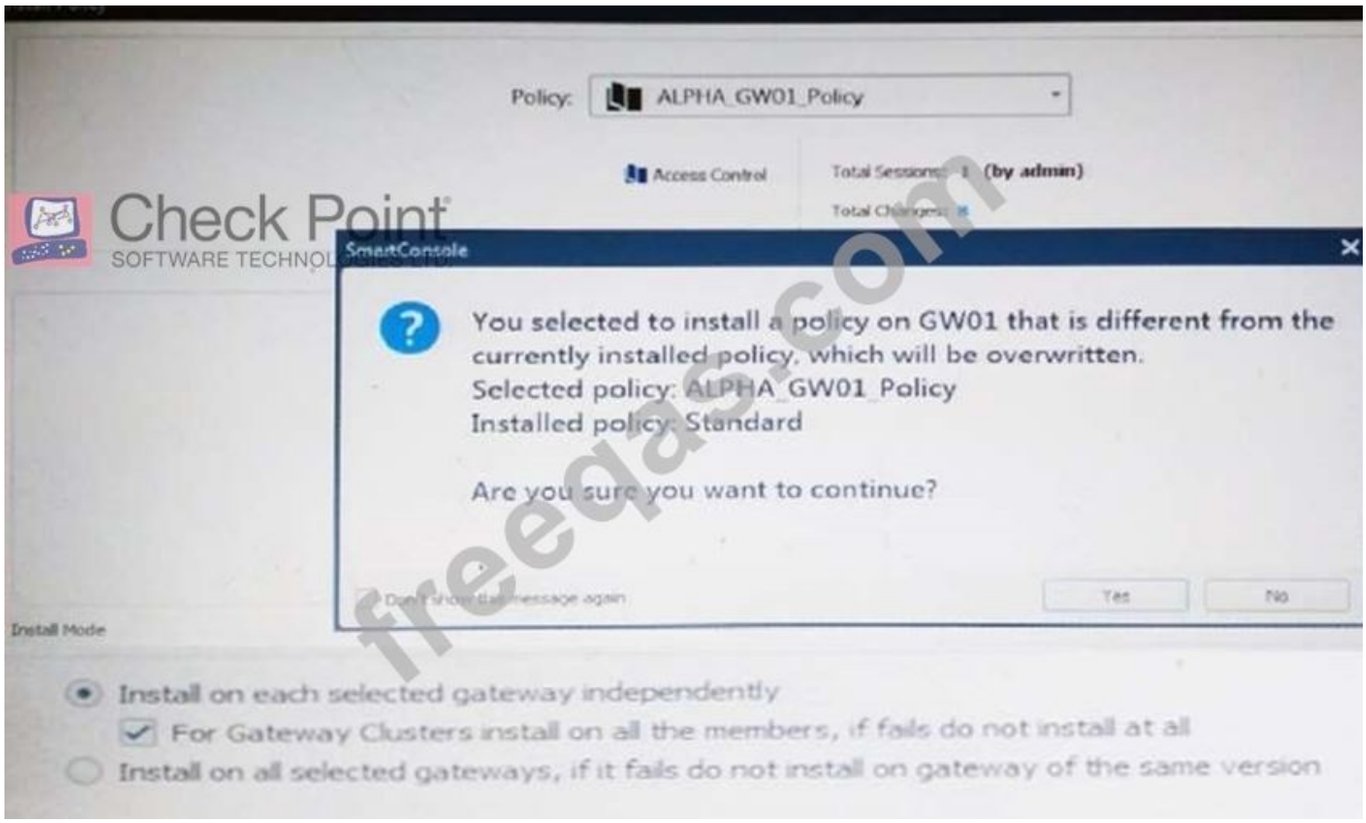
NEW QUESTION: 17

Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

A. /var/log/Cpbackup/backups/backup/backup_fw.tgs
B. /var/log/Cpbackup/backups/backup/backup_fw.tar
C. /var/log/Cpbackup/backups/backups/backup_fw.tar
D. /var/log/Cpbackup/backups/backup_fw.tgz
Answer: D (LEAVE A REPLY)
Explanation
Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration.
The configuration is saved to a .tgz file in the following directory:
Gaia OS Version
Hardware
Local Directory
R75.40 - R77.20
Check Point appliances
/var/log/CPbackup/backups/
Open Server
/var/CPbackup/backups/
R77.30
Check Point appliances
/var/log/CPbackup/backups/
Open Server

NEW QUESTION: 18
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)
Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

NEW QUESTION: 19
Why would an administrator see the message below?



A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
B. A new Policy Package created on the Gateway and transferred tothe management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.
C. A newPolicy Package created on the Management is going to be installed to the existing Gateway.
D. A new Policy Package created on the Gateway is going to be installed on the existing Management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
R80 is supported by which of the following operating systems:
A. Gaia, SecurePlatform, and Windows
B. Windows only
C. SecurePlatform only
D. Gaia only
Answer: (SHOW ANSWER)

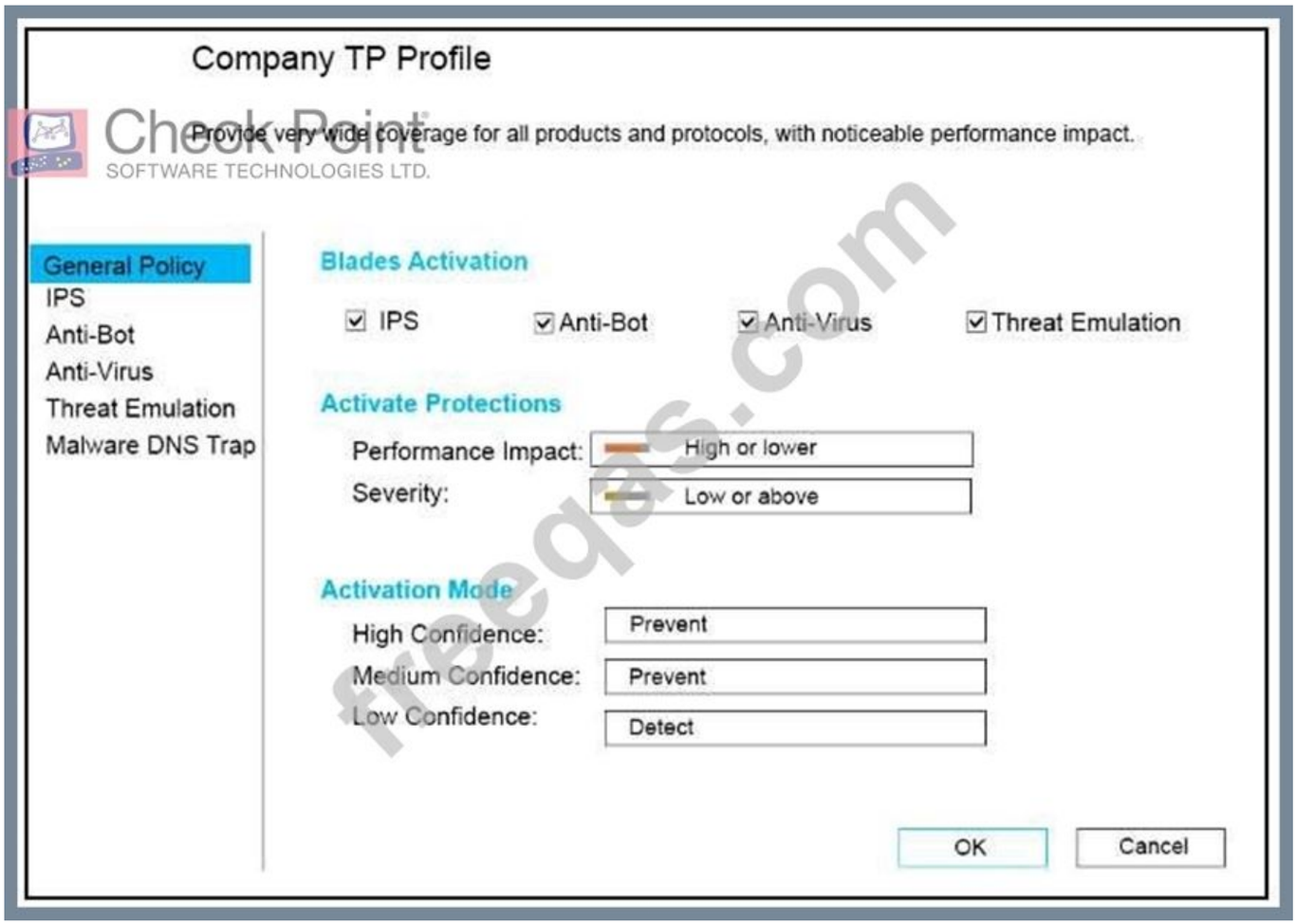
NEW QUESTION: 21
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?
A. Transfer messages between Firewall processes
B. Secure Internal Communication (SIC)

C. Pulls application monitoring status
D. Restart Daemons if they fail
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which command shows the installed licenses?
cplic print
A.
B. fwlic print
C. print cplic
D. show licenses
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
What is NOT an advantage of Stateful Inspection?
A. High Performance
B. Good Security
C. No Screening above Network layer
D. Transparency
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 24
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 the Performance Impact to Medium or lower.

B. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.

C. Set the Performance Impact to Very Low Confidence to Prevent.

D. Set High Confidence to Low and Low Confidence to Inactive.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25

What is the purpose of the Clean-up Rule?

A. To log all traffic that is not explicitly allowed or denied in the Rule Base

B. To clean up policies found inconsistent with the compliance blade reports

C. To remove all rules that could have a conflict with other rules in the database

D. To eliminate duplicate log entries in the Security Gateway

Answer: A (LEAVE A REPLY)

These are basic access control rules we recommend for all Rule Bases:

* Stealth rule that prevents direct access to the Security Gateway.

* Cleanup rule that drops all traffic that is not allowed by the earlier rules.

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

NEW QUESTION: 26
What is the purpose of Priority Delta in VRRP?
A. When a box is up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fails, Effective Priority = Priority - Priority Delta
D. When a box fails, Effective Priority = Priority - Priority Delta
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/87911.htm

NEW QUESTION: 27
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)
Explanation
Explanation:
A Security Gateway can use these procedures to translate IP addresses in your network:
* Static NAT - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.
* Hide NAT - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers, external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.
* Hide NAT with Port Translation - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules to use Port Translation.
Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/6724.htm

NEW QUESTION: 28
When configuring LDAP User Directory integration, Changes applied to a User Directory template are:
A. Reflected immediately for all users who are using template.
B. Not reflected for any users unless the local user template is changed.

C. Reflected for all users who are using that template and if the local user template is changed as well.
D. Not reflected for any users who are using that template.
Answer: A (LEAVE A REPLY)
Explanation
Explanation:
The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.
Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/94041

NEW QUESTION: 29
Choose what BEST describes users on Gaia Platform.
A. There is one default user that cannot 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 are two default users that cannot be deleted and one SmartConsole Administrator.
Answer: B (LEAVE A REPLY)
Explanation
Explanation:
These users are created by default and cannot be deleted:
* admin - Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.
* monitor - Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm

NEW QUESTION: 30
Which feature is NOT provided by all Check Point Mobile Access solutions?
A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Types of Solutions
All of Check Point's Remote Access solutions provide:
Enterprise-grade, secure connectivity to corporate resources.

- Strong user authentication.
- Granular access control.
- Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/83586.htm

NEW QUESTION: 31
There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?
A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console
Answer: C (LEAVE A REPLY)
Reference:
http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517088487_4c0acda205460a92f44c83d399826a7b&xtn=.pdf

NEW QUESTION: 32
Which method below is NOT one of the ways to communicate using the Management API's?
A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application
C. Typing API commands using Gaia's secure shell (clash)19+
D. Sending API commands over an http connection using web-services
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction

NEW QUESTION: 33
Which one of the following is the preferred licensing model? Choose the BEST answer.
A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.
B. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency on the gateway.

C. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
D. Central licensing because it ties the package license to the MAC-address of the Security Management Server's Mgmt-interface and has no dependency on the gateway.
Answer: B (LEAVE A REPLY)
Central License
A Central License is a license attached to the Security Management server IP address, rather than the gateway IP address. The benefits of a Central License are:
* Only one IP address is needed for all licenses.
* A license can be taken from one gateway and given to another.
* The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/13128.htm#o13527

NEW QUESTION: 34
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateDst

B. XlateDPort

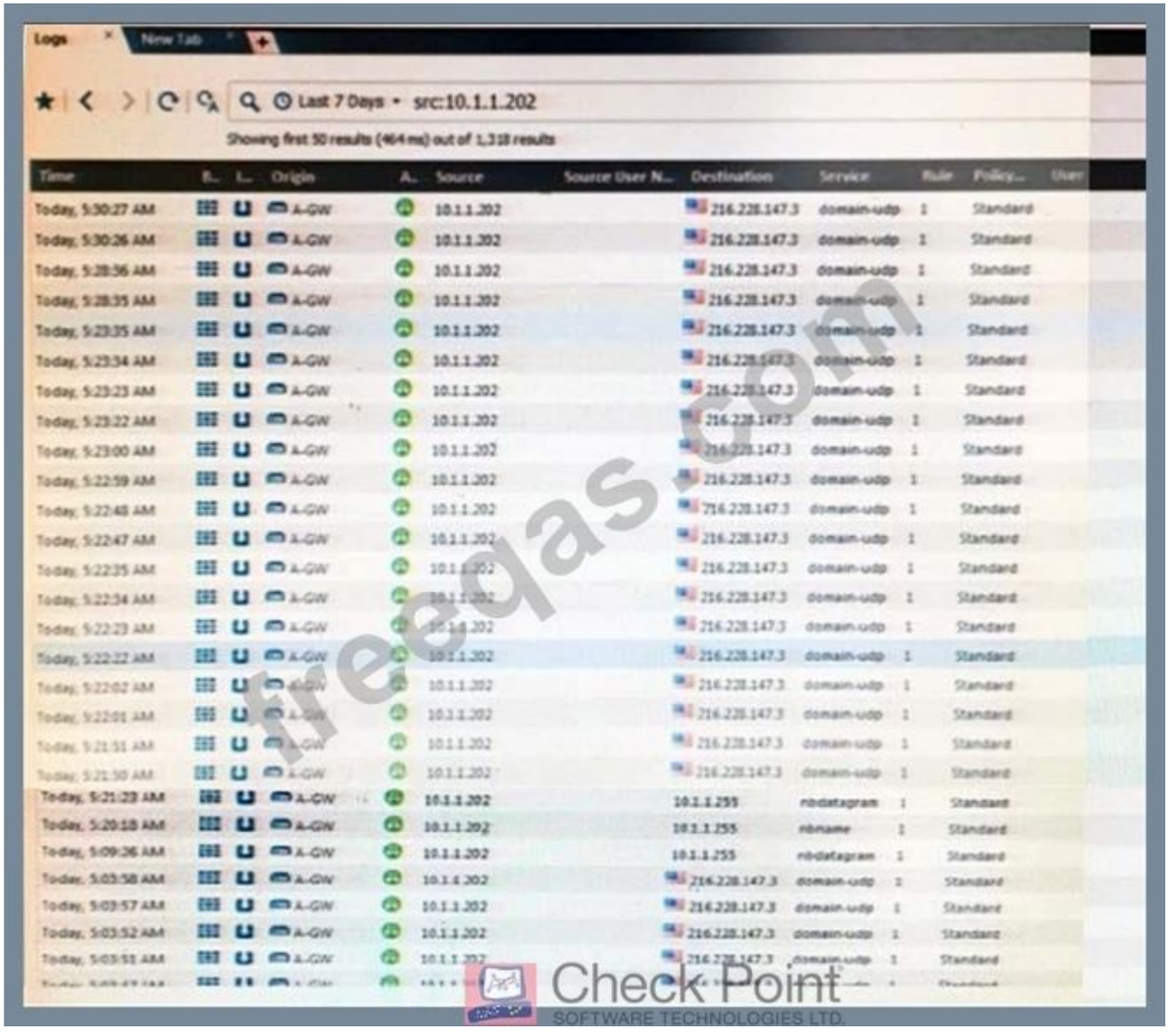
C. XlateSrc

D. XlateSPort

Answer: D (LEAVE A REPLY)

NEW QUESTION: 35

The following graphic shows:



A. View from SmartView Monitor for logs initiated from source address 10.1.1.202

B. View from SmartView Tracker for logs of destination address 10.1.1.202

C. View from SmartView Tracker for logs initiated from source address 10.1.1.202

D. View from SmartLog for logs initiated from source address 10.1.1.202

Answer: C (LEAVE A REPLY)

NEW QUESTION: 36

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

A. Install appliance TE250X on SpanPort on LAN switch in MTA mode

B. Install appliance TE250X in standalone mode and setup MTA

C. You can utilize only Check Point Cloud Services for this scenario

D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Reference: http://dl3.checkpoint.com/paid/f2/f2faf02dba06acad8cc4c57833593df6/CP_TE100X_TE250X_Appliance_GettingStartedGuide.pdf?HashKey=1517091196_a292abdde351bbdb4b3d28e82654b240&xtn=.pdf

NEW QUESTION: 37

You are going to perform a major upgrade. Which back up solution should you use to ensure your database

can be restored on that device?

A. backup

B. logswitch

C. Database Revision

D. snapshot

Answer: D (LEAVE A REPLY)

Explanation

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point

products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on another machine of the

same type is supported.

The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be saved.

NEW QUESTION: 38

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

A. RADIUS

B. Remote Access and RADIUS

C. All of the above

D. AD Query and Browser-based Authentication

Answer: D (LEAVE A REPLY)

Identity Awareness gets identities from these acquisition sources:

* AD Query

* Browser-Based Authentication

* Endpoint Identity Agent

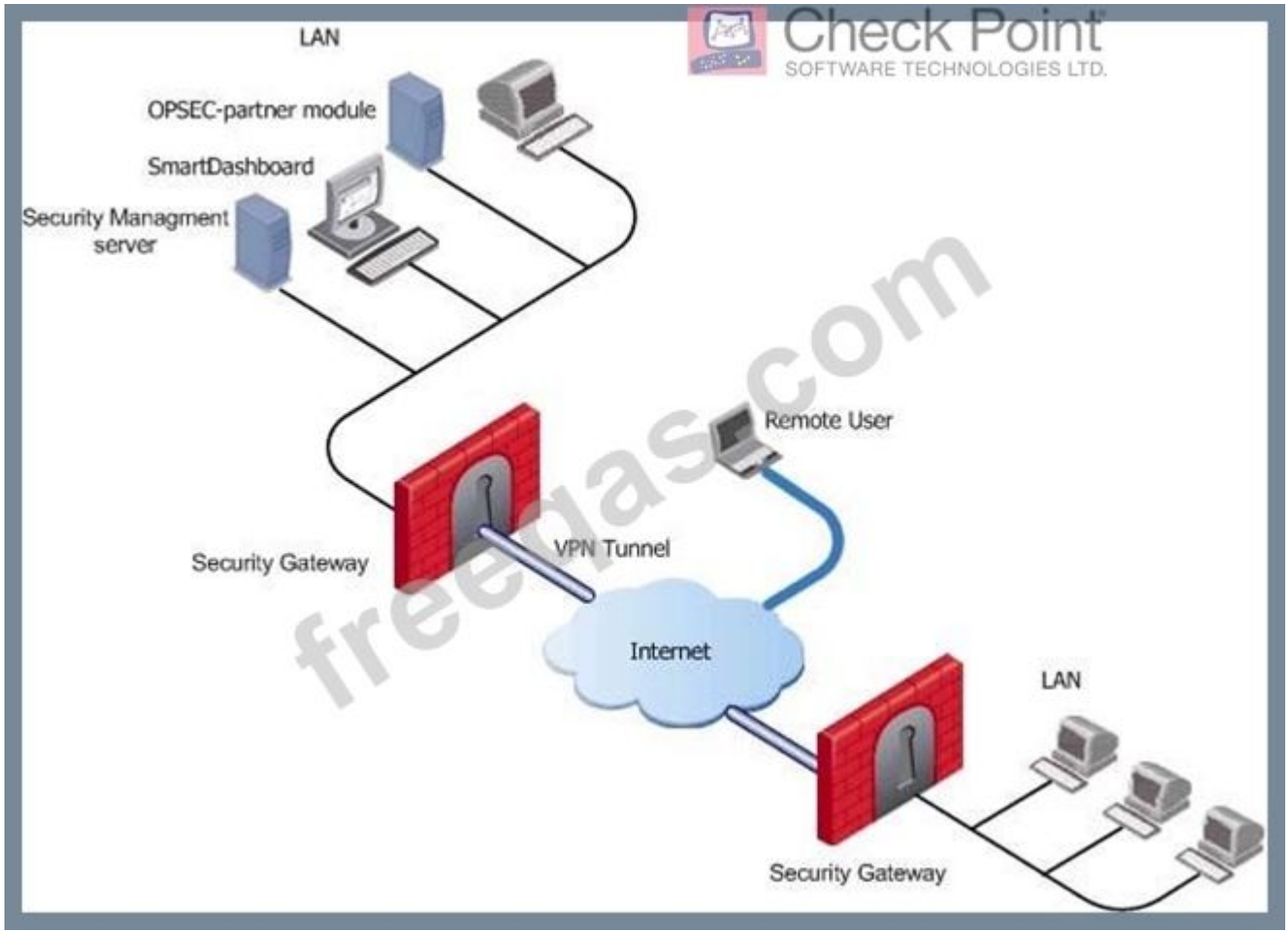
* Terminal Servers Identity Agent

* Remote Access

Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62007.htm

NEW QUESTION: 39
What are the three essential components of the Check Point Security Management Architecture?
A. SmartConsole, Security Management Server, Security Gateway
B. SmartConsole, SmartUpdate, Security Gateway
C. Security Management Server, Security Gateway, Command Line Interface
D. WebUI, SmartConsole, Security Gateway
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Deployments
Basic deployments:
- Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.
- Distributed deployment - Security Gateway and the Security Management server are installed on different machines.



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.
You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.
There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.
Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/118037

NEW QUESTION: 40
Match the following commands to their correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F2; C2>F4; C3>F1; C4>F5
C. C1>F4; C2>F6; C3>F3; C4>F5
D. C1>F2; C2>F1; C3>F6; C4>F4
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Fill in the blank; The position of an Implied rule is manipulated in the_____ window
A. Object Explorer
B. Firewall
C. NAT
D. Global Properties
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
Which options are given on features, when editing a Role on Gaia Platform?
A. Read/Write, Read Only
B. Read/Write, Read only, None
C. Read/Write, None
D. Read Only, None
Answer: B (LEAVE A REPLY)

Explanation
Roles
Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (readonly) access to other features, and no access to other features.
You can also specify which access mechanisms (WebUI or the CLI) are available to the user.
Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.
Gaia includes these predefined roles:
You cannot delete or change the predefined roles.
Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.
References:

NEW QUESTION: 43
What protocol is specifically used for clustered environments?
A. Synchronized Cluster Protocol
B. Clustered Protocol
C. Control Cluster Protocol
D. Cluster Control Protocol
Answer: (SHOW ANSWER)

NEW QUESTION: 44
You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?
A. CDP is down
B. SVR is down

C. FWM is down
D. CPSM is down
Answer: (SHOW ANSWER)
The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.). STATE is T
(Terminate = Down)
Explanation :
Symptoms
[Expert@HostName:0]# ps -aux | grep fwm
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" - command "fwm"

NEW QUESTION: 45
Review the rules. Assume domain UDP is enabled in the implied rules.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:
A. is prompted three times before connecting to the Internet successfully.
B. can connect to the Internet successfully after being authenticated.
C. can go to the Internet after Telnetting to the client authentication daemon port 259.
D. can go to the Internet, without being prompted for authentication.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
What is the purpose of Captive Portal?
A. It manages user permission in SmartConsole
B. It provides remote access to SmartConsole
C. It authenticates users, allowing them access to the Internet and corporate resources
D. It authenticates users, allowing them access to the Gaia OS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47

Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.
A. infoCP
B. infoview
C. cpinfo
D. fw cpinfo
Answer: C (LEAVE A REPLY)
CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).
The CPinfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPinfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.
When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

NEW QUESTION: 48
The most important part of a site-to-site VPN deployment is the _____ .
A. Internet
B. Remote users
C. Encrypted VPN tunnel
D. VPN gateways
Answer: C (LEAVE A REPLY)
Explanation
Site to Site VPN
The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create
a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can
maintain more than one VPN tunnel at the same time.

NEW QUESTION: 49
There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A's interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?
A. No, since "maintain current active cluster member" option on the cluster object properties is enabled by default
B. No, since "maintain current active cluster member" option is enabled by default on the Global Properties

C. Yes, since "Switch to higher priority cluster member" option on the cluster object properties is enabled by default
D. Yes, since "Switch to higher priority cluster member" option is enabled by default on the Global Properties
Answer: (SHOW ANSWER)
What Happens When a Security Gateway Recovers?
In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:
* Maintain Current Active Security Gatewaymeans that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
* Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

NEW QUESTION: 50
Administrator wishes to update IPS from SmartConsole by clicking on the option "update now" under the IPS tab. Which device requires internet access for the update to work?
A. Security Gateway
B. Device where SmartConsole is installed
C. SMS
D. SmartEvent
Answer: (SHOW ANSWER)
Updating IPS Manually
You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.
To obtain updates of all the latest protections from the IPS website:
The LAN Settings window opens.
The settings for the Internet Explorer proxy server are configured.
If you chose to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

NEW QUESTION: 51

The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

A. show configuration

B. backup

C. migrate export

D. upgrade export

Answer: B (LEAVE A REPLY)

Explanation

3. System Backup (and System Restore)

System Backup can be used to backup current system configuration. A backup creates a compressed file that contains the Check Point configuration including the networking and operating system parameters, such as routing and interface configuration etc., but unlike a snapshot, it does not include the operating system, product binaries, and hotfixes.

References:

NEW QUESTION: 52

Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

A. /var/log/Cpbackup/backups/backup/backup_fw.tgs

B. /var/log/Cpbackup/backups/backup/backup_fw.tar

C. /var/log/Cpbackup/backups/backups/backup_fw.tar

D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation: Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration.

The configuration is saved to a .tgz file in the following directory:

Gaia OS Version	Hardware	Local Directory
R75.40 - R77.20	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	/var/CPbackup/backups/
R77.30	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk91400

NEW QUESTION: 53

Which application should you use to install a contract file?

A. SmartView Monitor

B. WebUI

C. SmartUpdate

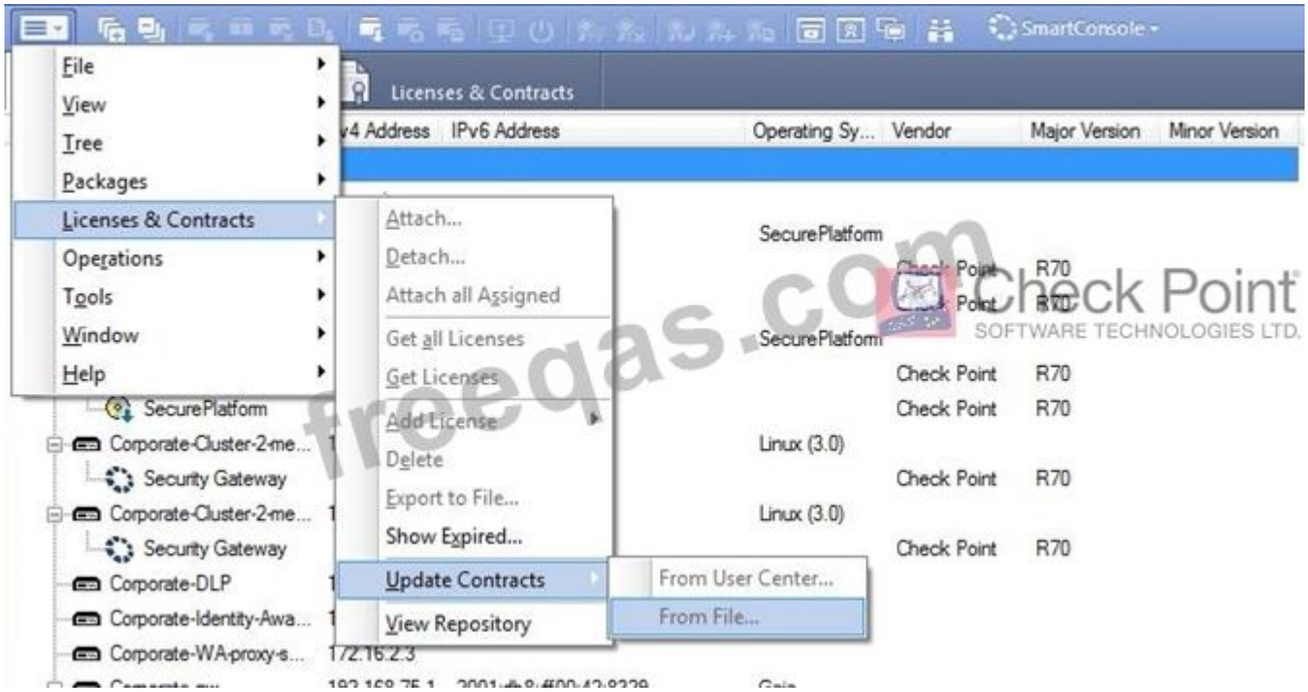
D. SmartProvisioning

Answer: C (LEAVE A REPLY)

Explanation

Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 / Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.

Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:



Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

References:

NEW QUESTION: 54

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

A. Basic - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

B. Optimized - Provides excellent protection for common network products and protocols against recent or popular attacks

C. Strict - Provides a wide coverage for all products and protocols, with impact on network performance

D. Recommended - Provides all protection for all common network products and servers, with impact on network performance

Answer: D (LEAVE A REPLY)
Explanation
References:

NEW QUESTION: 55
Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client
A. Destination
B. Identity
C. Payload
D. Location
Answer: B (LEAVE A REPLY)
Explanation
Explanation:
How RADIUS Accounting Works with Identity Awareness
RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.
Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

NEW QUESTION: 56
Which two Identity Awareness commands are used to support identity sharing?
A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
D. Policy Activation Point (PAP) and Policy Decision Point (PDP)
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/66477.htm

NEW QUESTION: 57
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?
A. Security Gateways is not part of the Domain
B. SmartConsole machine is not part of the domain
C. SMS is not part of the domain
D. Identity Awareness is not enabled on Global properties
Answer: B (LEAVE A REPLY)
Explanation/Reference:

Explanation: To enable Identity Awareness:
1. Log in to SmartDashboard.
2. From the Network Objects tree, expand the Check Point branch.
3. Double-click the Security Gateway on which to enable Identity Awareness.
4. In the Software Blades section, select Identity Awareness on the Network Security tab.
The Identity Awareness Configuration wizard opens.
5. Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers.
- Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
- Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

See Choosing Identity Sources.
Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.
6. Click Next.
The Integration With Active Directory window opens.
When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with all of the domain controllers in the organization's Active Directory.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

NEW QUESTION: 58
Your users are defined in a Windows 2008 R2 Active Directory server.
You must add LDAP users to a Client Authentication rule.
Which kind of user group do you need in the Client Authentication rule in R77?
A. A group with a genetic user
B. All Users
C. LDAP group
D. External-user group
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?
A. Create a text-file with mgmt_cli script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.

B. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command load configuration.
C. Create a text-file with DBEDIT script that creates all objects and policies. Run the file in the command line of the management server using command dbedit -f.
D. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.
Answer: A (LEAVE A REPLY)
Explanation
Did you know: mgmt_cli can accept csv files as inputs using the --batch option.
The first row should contain the argument names and the rows below it should hold the values for these parameters.
So an equivalent solution to the powershell script could look like this:
data.csv:

name	ipv4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server> This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.
References:

NEW QUESTION: 60
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or_____.
A. On all satellite gateway to satellite gateway tunnels
B. On specific tunnels for specific gateways
C. On specific tunnels in the community
D. On specific satellite gateway to central gateway tunnels
Answer: C (LEAVE A REPLY)
Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:
* Can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.

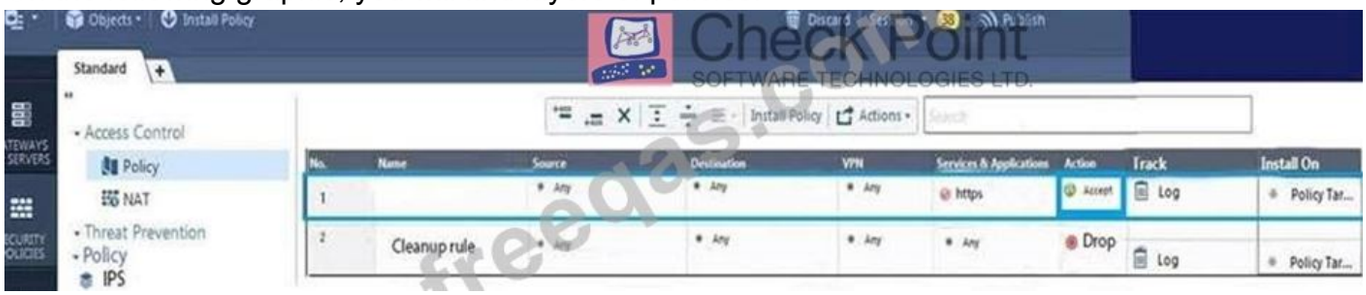
* Can be specified for a specific Security Gateway. Use this option to configure specific Security Gateways to have permanent tunnels.
* Can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific Security Gateways as permanent.
Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/14018

NEW QUESTION: 61
What Check Point tool is used to automatically update Check Point products for the Gaia OS?
A. Check Point Update Engine
B. Check Point Upgrade Service Engine
C. Check Point Upgrade Installation Service
D. Check Point INSPECT Engine
Answer: B (LEAVE A REPLY)

NEW QUESTION: 62
Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?
A. Anti-Virus
B. IPS
C. Anti-Spam
D. Anti-bot
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:
Malware attacks
▪
Dos and DDoS attacks
▪
Application and server vulnerabilities
▪
Insider threats
▪

Unwanted application traffic, including IM and P2P
▪
Reference: https://www.checkpoint.com/products/ips-software-blade/

NEW QUESTION: 63
On the following graphic, you will find layers of policies.



What is a precedence of traffic inspection for the defined polices?
A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.
B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer
C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.
D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.
Answer: (SHOW ANSWER)
To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.
For example, when you upgrade to R80 from earlier versions:
* Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.
When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.
* Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.
All layers are evaluated in parallel
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

NEW QUESTION: 64
True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

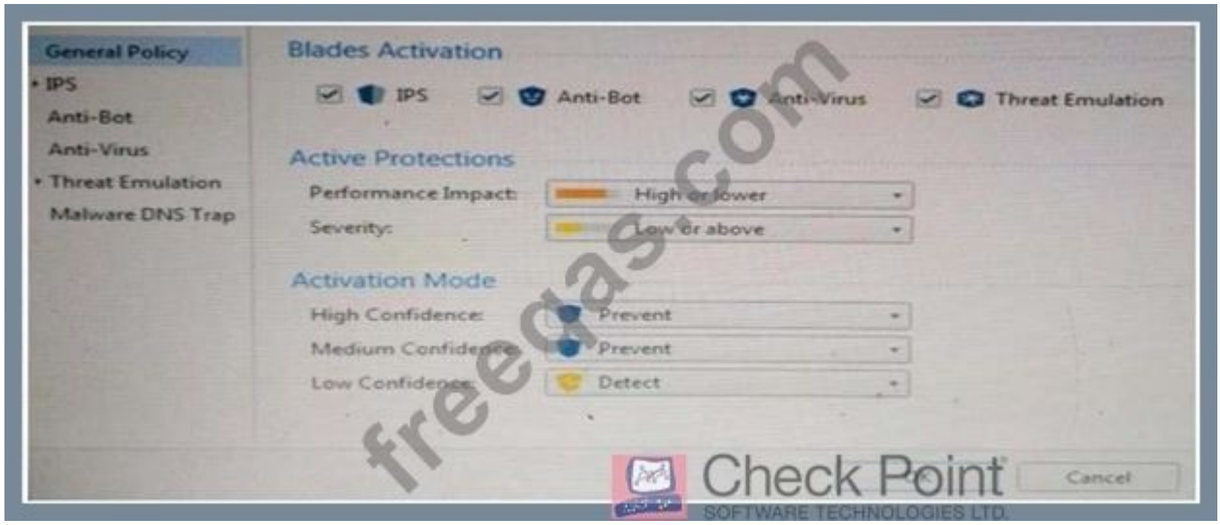
A. False, this feature has to be enabled in the Global Properties.
B. True, every administrator works in a session that is independent of the other administrators.
C. True, every administrator works on a different database that is independent of the other administrators.
D. False, only one administrator can login with write permission.
Answer: (SHOW ANSWER)
Explanation
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.
References:

NEW QUESTION: 65
Fill in the blank: A _____ is used by a VPN gateway to send traffic as if it were a physical interface.
A. VPN Tunnel Interface
B. VPN community
C. VPN router
D. VPN interface
Answer: (SHOW ANSWER)
Explanation
Route Based VPN
VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

NEW QUESTION: 66
Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?
A. Firewall
B. Identity Awareness
C. Application Control
D. URL Filtering
Answer: (SHOW ANSWER)
Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.
Reference: https://www.checkpoint.com/products/identity-awareness-software-blade/

NEW QUESTION: 67

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



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. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.

C. Set the Performance Impact to Medium or lower.

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 68

You are the administrator for Alpha Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

What does this mean?

A. The rule No.6 has been marked for deletion in another Management session.

B. The rule No.6 has been marked for deletionin your Management session.

C. The rule No.6 has been marked for editing in another Management session.

D. The rule No.6 has been marked for editing in your Management session.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 69

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

A. SmartPortal

B. SmartDashboard

C. SmartUpdate

D. SmartView Tracker

Answer: C (LEAVE A REPLY)

NEW QUESTION: 70

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

A. You achieve compartmentalization by allowing a large number of users to be distributed across several servers

B. You achieve a faster access time by placing LDAP servers containing the database at remote sites

C. You gain High Availability by replicating the same information on several servers

D. Information on a user is hidden, yet distributed across several servers

Answer: D (LEAVE A REPLY)

NEW QUESTION: 71

Which utility allows you to configure the DHCP service on GAIA from the command line?

A. ifconfig

B. dhcp_cfg

C. sysconfig

D. cpconfig

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Sysconfig Configuration Options

	end Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

Refrence: https://sc1.checkpoint.com/documents/R76/CP_R76_Splat_AdminGuide/51548.htm
NOTE:Question must be wrong because no answer is possible for GAIA system, this must be SPLAT version.
DHCP CLI configuration for GAIA reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73181.htm#o80096

NEW QUESTION: 72
Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.
A. UDP
B. TDP
C. CCP
D. HTTP
Answer: A (LEAVE A REPLY)
Parameters:

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

NEW QUESTION: 73
Which application should you use to install a contract file?
A. SmartView Monitor
B. WebUI
C. SmartUpdate

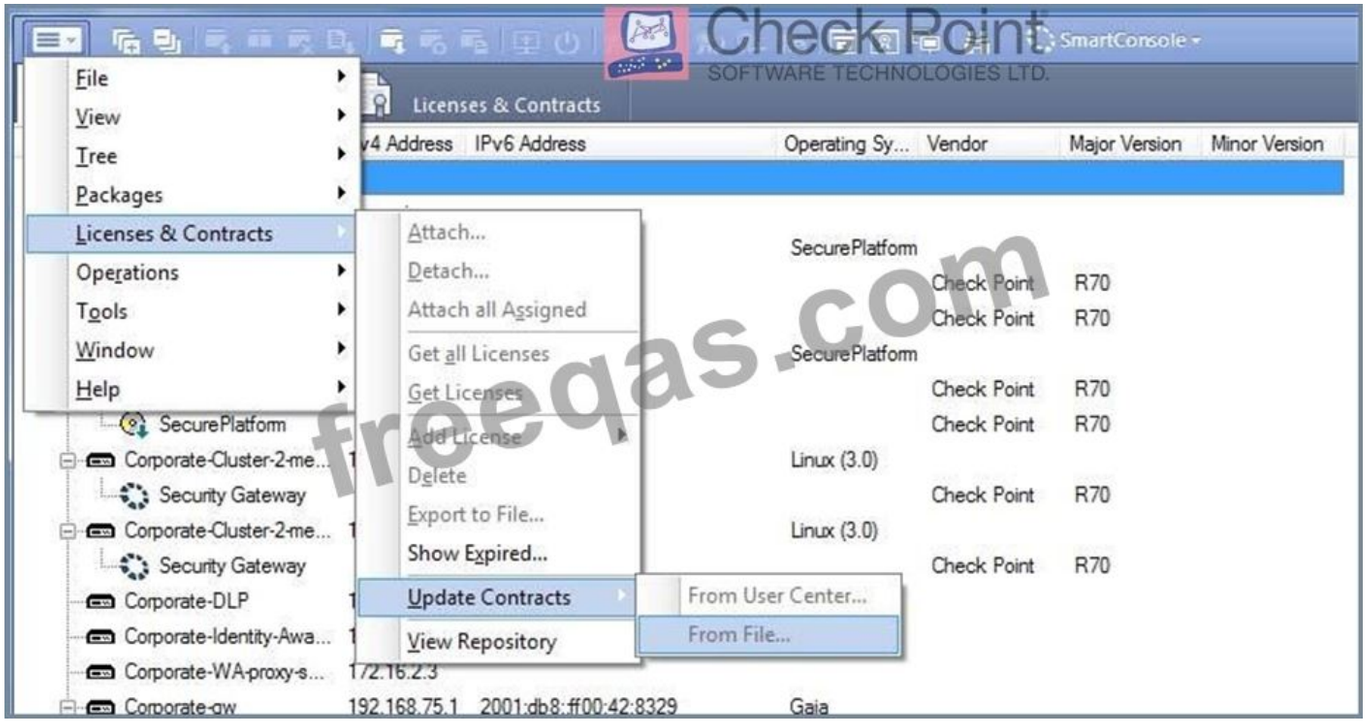
D. SmartProvisioning

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Explanation: Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 / Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.

Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:



Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089

NEW QUESTION: 74

The _____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

A. Application Control

B. Threat Emulation

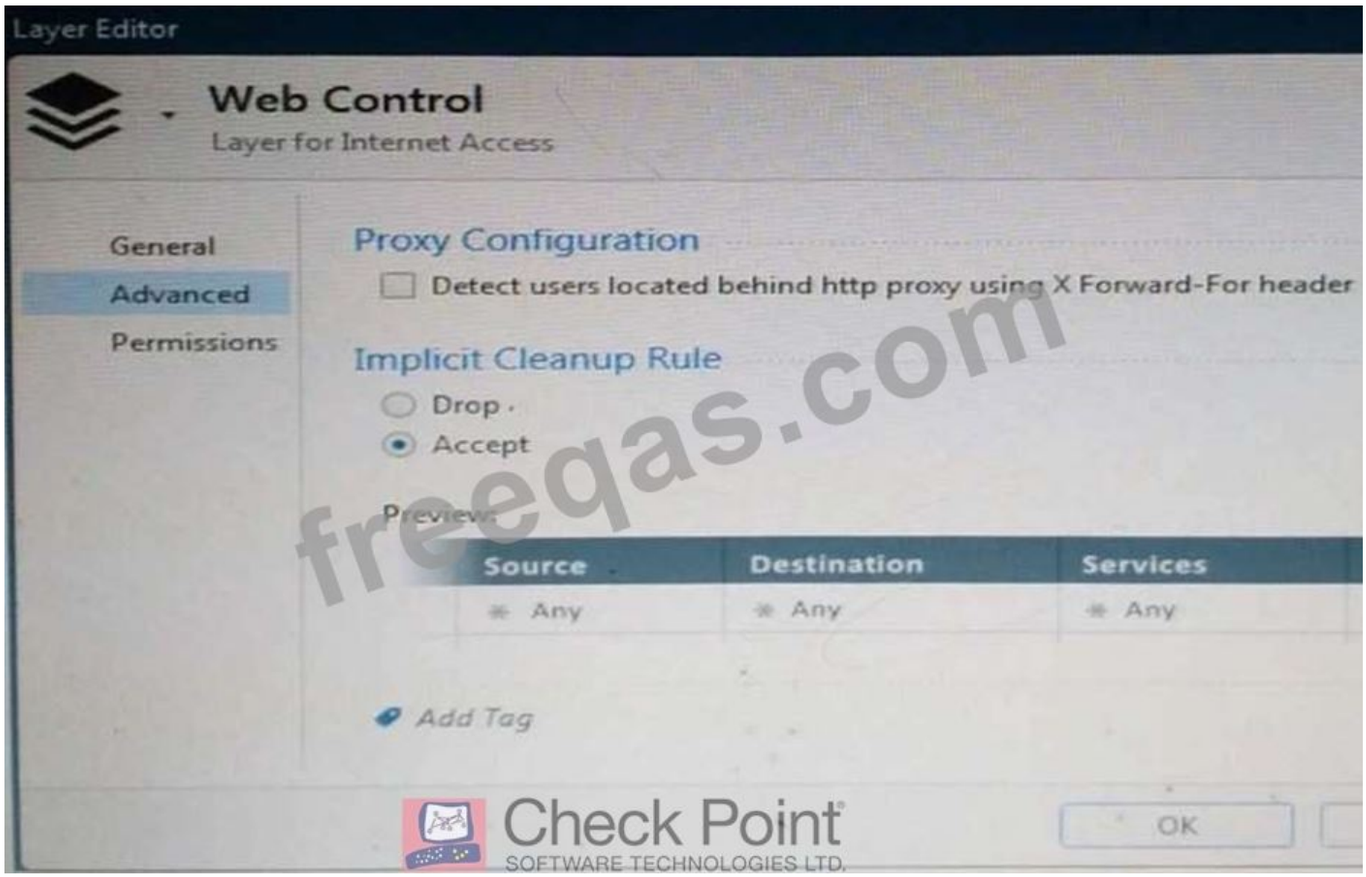
C. URL Filtering

D. Data Awareness

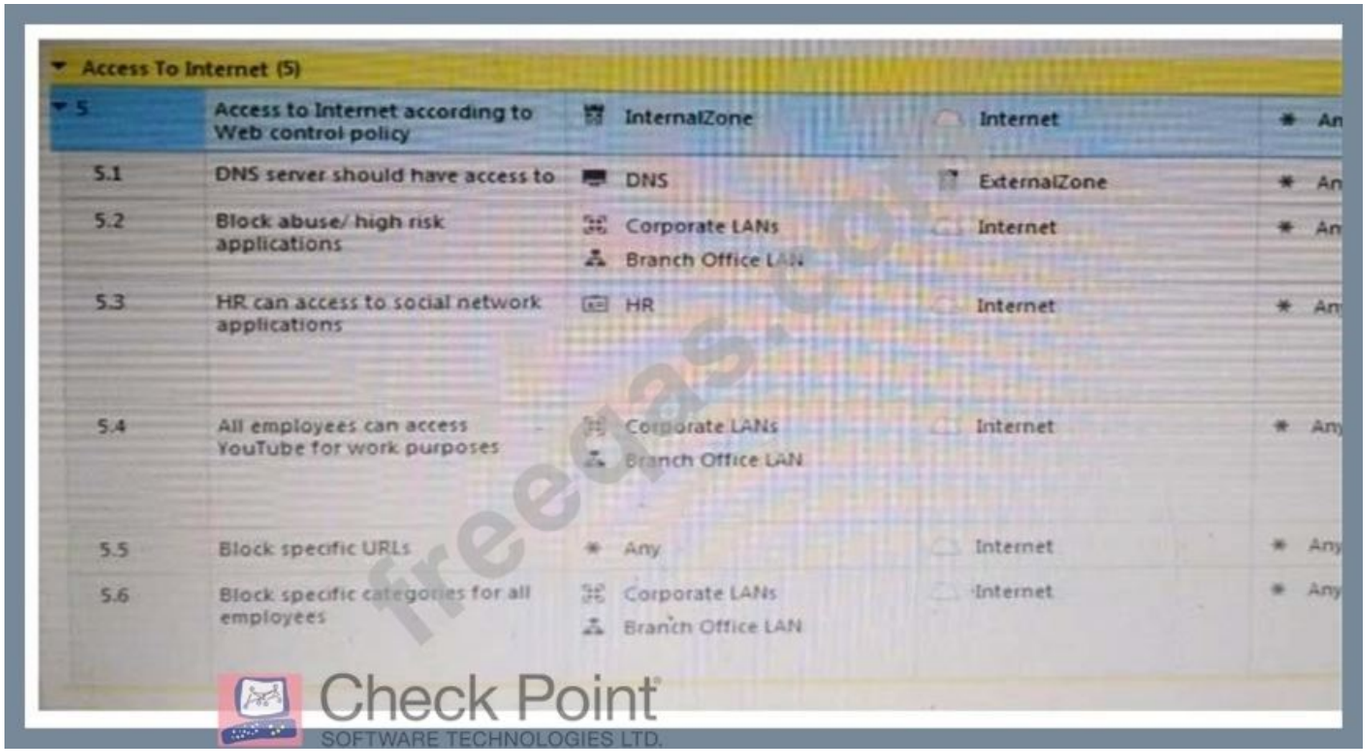
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

Web Control Layer has been set up using the settings in the following dialogue:



Consider the following policy and select the BEST answer.



A. Traffic that does not match any rule in the subpolicy is dropped.

B. All employees can access only Youtube and Vimeo.

C. Access to Youtube and Vimeo is allowed only once a day.

D. Anyone from internal network can access the internet, expect the traffic defined in drop rules 5.2, 5.5 and 5.6.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Policy Layers and Sub-Policies

R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators

- With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an "accept" action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.
- Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.
- Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

Reference: https://community.checkpoint.com/docs/DOC-1065

NEW QUESTION: 76

On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

A. 18210

B. 18184

C. 257

D. 18191

Answer: (SHOW ANSWER)

Explanation/Reference:

https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120829

NEW QUESTION: 77
In R80, Unified Policy is a combination of
A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.
Answer: D (LEAVE A REPLY)
Explanation
D is the best answer given the choices.
Unified Policy
In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:
* Firewall and VPN
* Application Control and URL Filtering
* Identity Awareness
* Data Awareness
* Mobile Access
* Security Zones

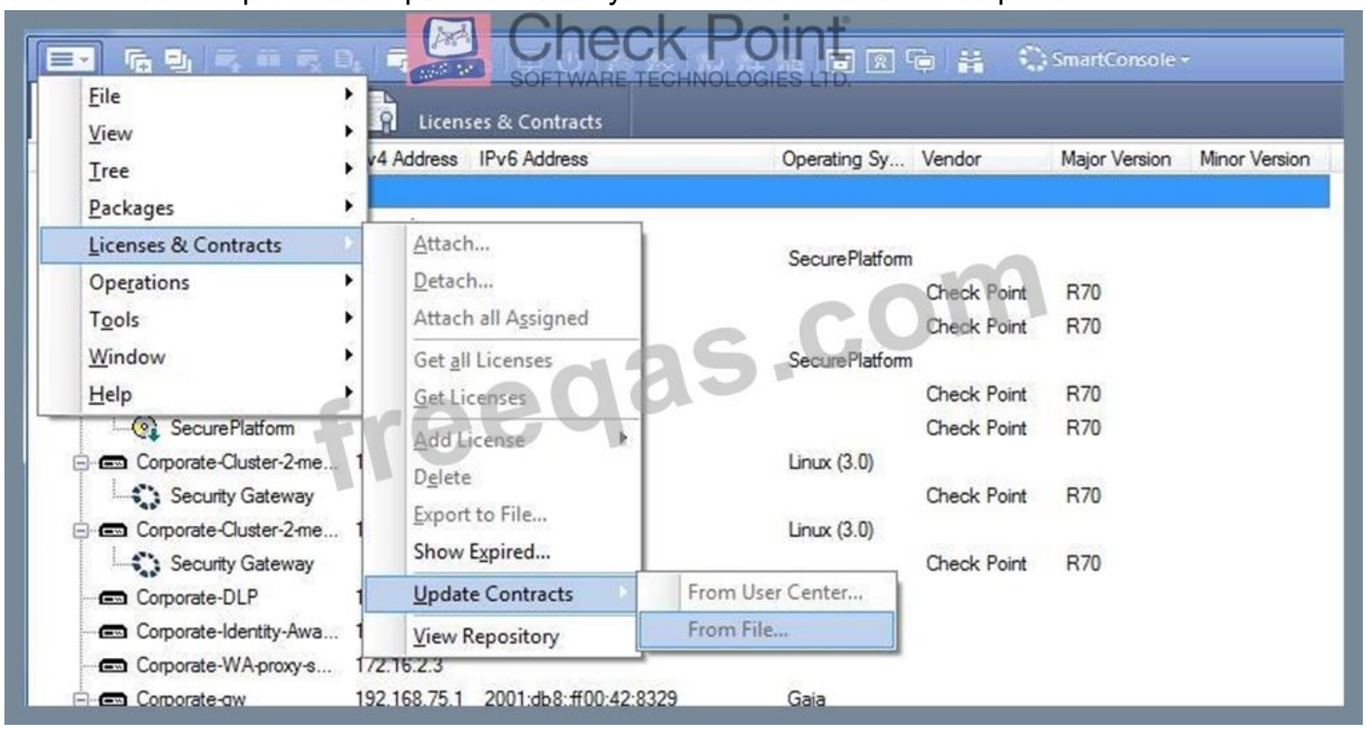
NEW QUESTION: 78
Review the rules. Assume domain UDP is enabled in the implied rules.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:
A. is prompted three times before connecting to the Internet successfully.
B. can go to the Internet, without being prompted for authentication.
C. can connect to the Internet successfully after being authenticated.
D. can go to the Internet after Telnetting to the client authentication daemon port 259.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 79
VPN gateways authenticate using _____ and _____ .
A. Passwords; tokens
B. Certificates; pre-shared secrets
C. Certificates; passwords
D. Tokens; pre-shared secrets
Answer: B (LEAVE A REPLY)
Explanation
VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

NEW QUESTION: 80
Which application should you use to install a contract file?
A. SmartView Monitor
B. WebUI
C. SmartUpdate
D. SmartProvisioning
Answer: C (LEAVE A REPLY)
Explanation
Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 / Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.
Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:

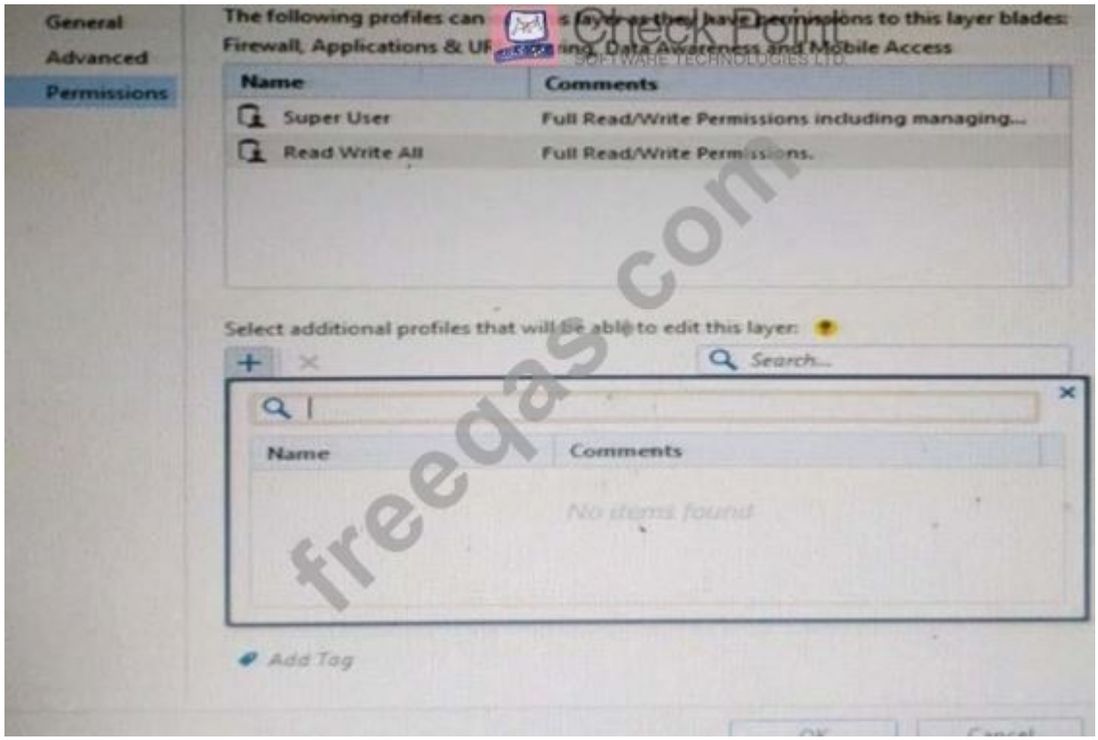


Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.
References:

NEW QUESTION: 81
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check
Point Security Gateway?
A. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance
B. You can utilize only Check Point Cloud Services for this scenario
C. Install appliance TE250X in standalone mode and setup MTA

D. Install appliance TE250X on SpanPort on LAN switch in MTA mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 82
You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything. What is the most likely cause of this problem? Select the BEST answer.



A. There are no permission profiles available and you need to create one first.
B. "Edit layers by Software Blades" is unselected in the Permission Profile
C. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.
D. All permission profiles are in use.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active
Directory users and computers?
A. UserCheck
B. Active Directory Query
C. Account Unit Query
D. User Directory Query
Answer: (SHOW ANSWER)
Explanation
AD Query extracts user and computer identity information from the Active Directory Security Event Logs.

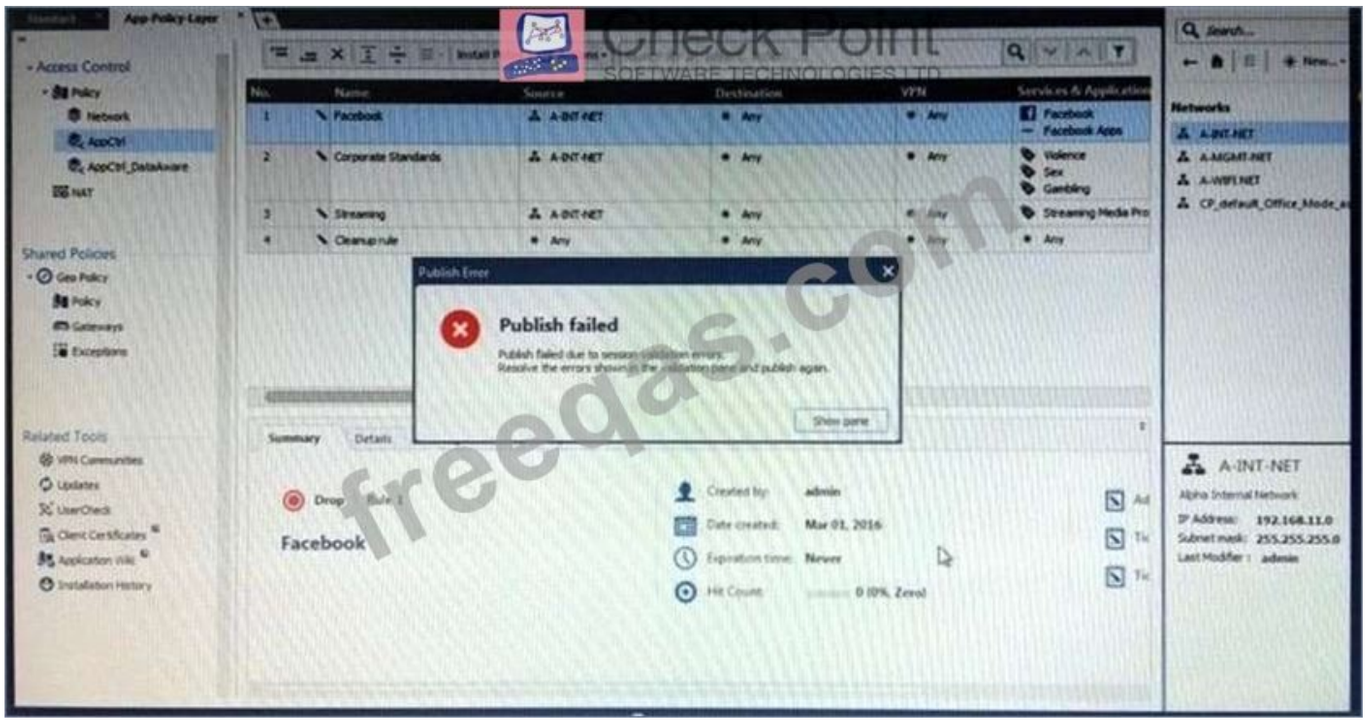
The system generates a Security Event log entry when a user or computer accesses a network resource. For
example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.
Reference :
https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION: 84
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to
00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?
A. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.
B. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field(conf:(conns: (conn:hwaddr ("00:0C:29:12:34:56")
C. As expert user, issue these commands:# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
D. As expert user, issue the command:# IP link set eth0 addr 00:0C:29:12:34:56
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use
IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to
ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates
to the Gateway before shipping it?
1. Run cpconfig on the Gateway, select Secure Internal Communication, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the Communication button in the Gateway object's General screen, enter the activation key, and click
Initialize and OK.
5. Install the Security Policy.
A. 1, 3, 2, 4, 5
B. 2, 3, 4, 1, 5
C. 2, 1, 3, 4, 5
D. 2, 3, 4, 5, 1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
In R80, Unified Policy is a combination of
A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security
Policy and Threat Prevention Policy.
D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.
Answer: (SHOW ANSWER)
Explanation
D is the best answer given the choices.
Unified Policy
In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

NEW QUESTION: 87
Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.
Where can the administrator check for more information on these errors?



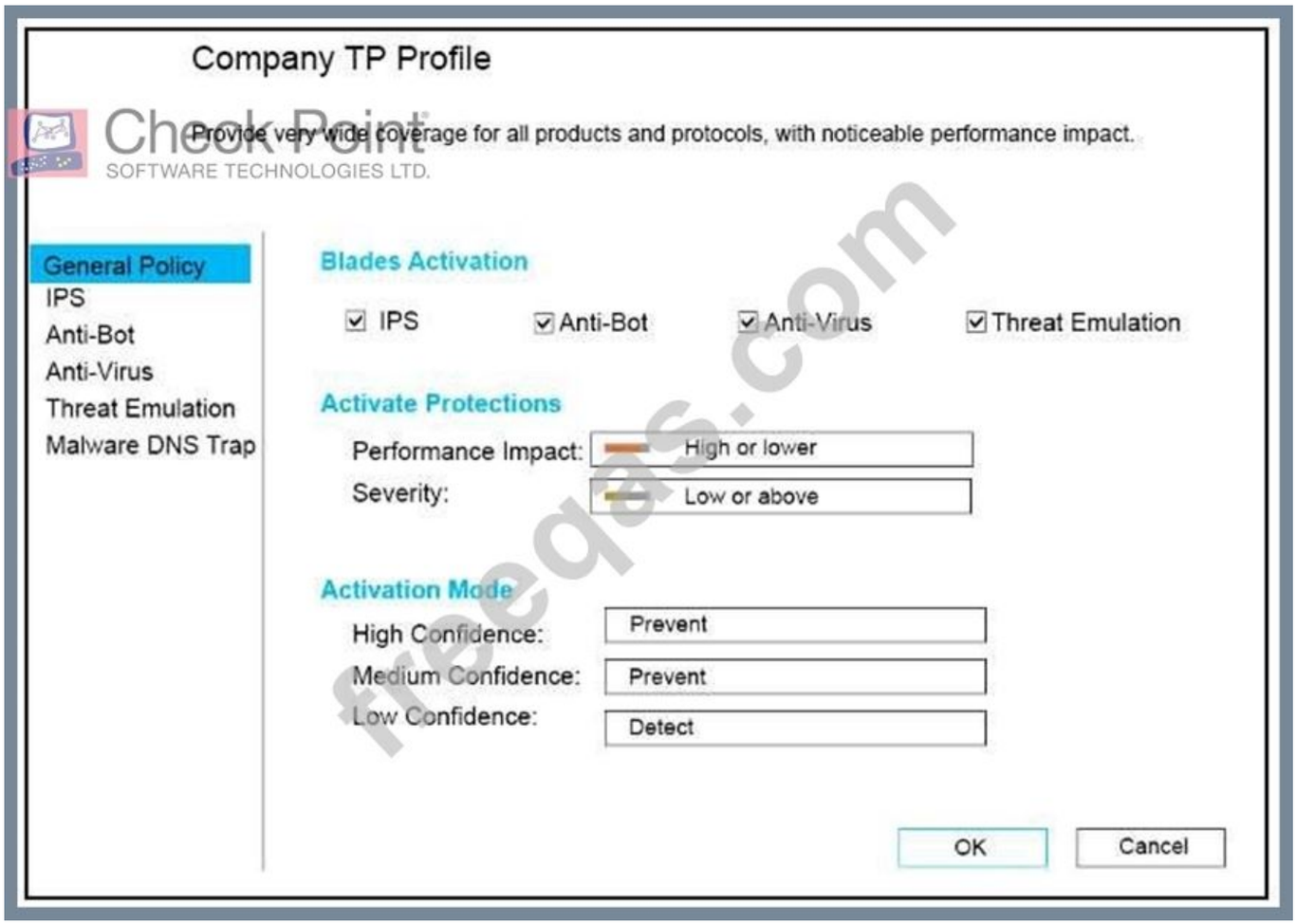
A. The Log and Monitor section in SmartConsole
B. The Validations section in SmartConsole
C. The Objects section in SmartConsole
D. The Policies section in SmartConsole
Answer: B (LEAVE A REPLY)
Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.
To publish, you must fix the errors.

NEW QUESTION: 88
Which rule is responsible for the user authentication failure?

A. Rule 3
B. Rule 5
C. Rule 6
D. Rule 4
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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)

Explanation/Reference:

NEW QUESTION: 90

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

A. Basic - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

B. Optimized - Provides excellent protection for common network products and protocols against recent or popular attacks

C. Strict - Provides a wide coverage for all products and protocols, with impact on network performance

D. Recommended - Provides all protection for all common network products and servers, with impact on network performance

Answer: D (LEAVE A REPLY)

Explanation/Reference:

https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486

NEW QUESTION: 91

You are the administrator for Alpha Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

What does this mean?

A. The rule No.6 has been marked for deletion in your Management session.

B. The rule No.6 has been marked for deletion in another Management session.

C. The rule No.6 has been marked for editing in your Management session.

D. The rule No.6 has been marked for editing in another Management session.

Answer: (SHOW ANSWER)

Explanation

NEW QUESTION: 92

Access roles allow the firewall administrator to configure network access according to:

A. a combination of computer groups and network

B. users and user groups

C. all of above

D. remote access clients

Answer: (SHOW ANSWER)

Explanation/Reference:

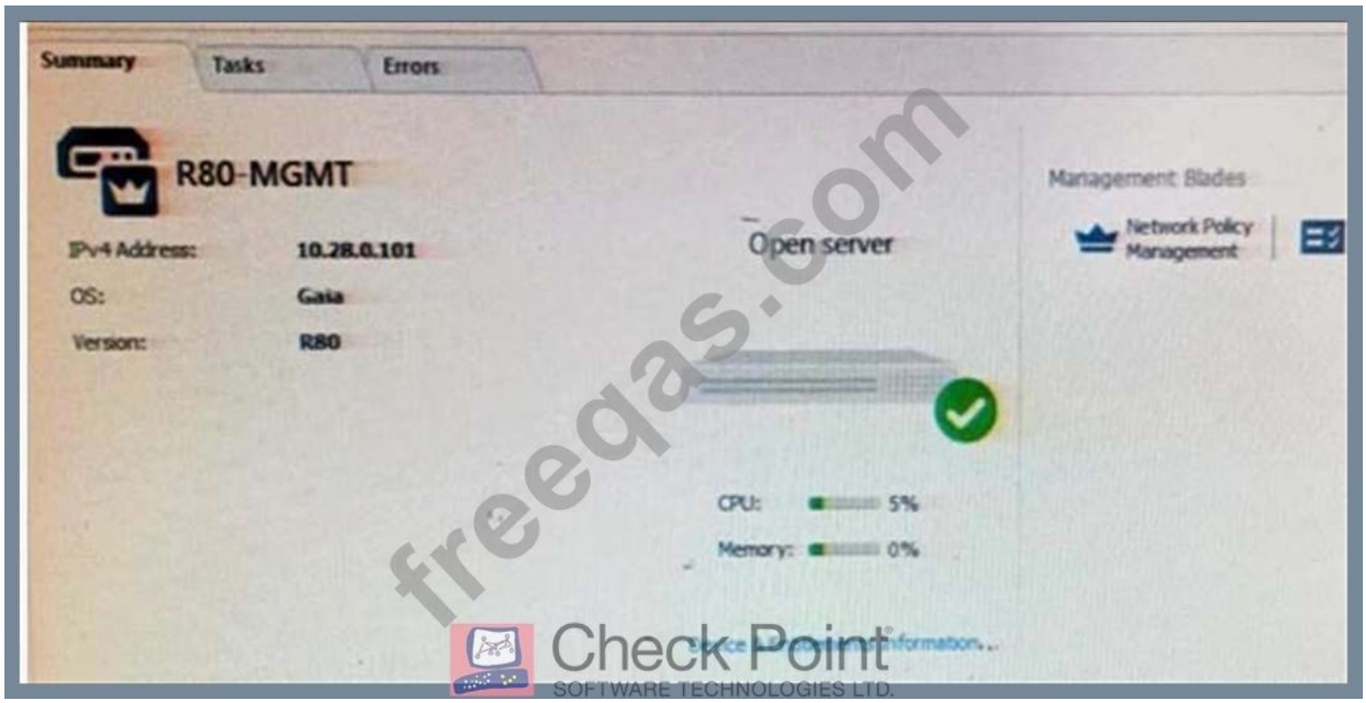
Explanation:

To create an access role:

1. Select Users and Administrators in the Objects Tree.

2. Right-click Access Roles > New Access Role.
The Access Role window opens.
3. Enter a Name and Comment (optional) for the access role.
4. In the Networks tab, select one of these:
Any network
- Specific networks - Click the plus sign and select a network.
- Your selection is shown in the Networks node in the Role Preview pane.
5. In the Users tab, select one of these:
Any user
- All identified users - Includes users identified by a supported authentication method (internal users,
- AD users or LDAP users).
Specific users - Click the plus sign.
- A window opens. You can search for Active Directory entries or select them from the list.
6. In the Machines tab, select one of these:
Any machine
- All identified machines - Includes machines identified by a supported authentication method (AD).
- Specific machines - Click the plus sign.
- You can search for AD entries or select them from the list.
7. Optional: For computers that use Full Identity Agents, from the Machines tab select Enforce IP spoofing protection.
8. Click OK.
The access role is added to the Users and Administrators tree.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92705.htm

NEW QUESTION: 93
Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What as an 'Open Server'?



A. Check Point software deployed on a non-Check Point appliance.

B. The Open Server Consortium approved Server Hardware used for the purpose of Security and Availability.

C. A check Point Management Server deployed using the Open Systems Interconnection (OSI) Server and Security deployment model.

D. A check Point Management Server software using the Open SSL.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/index.html

NEW QUESTION: 94

Which of the following is NOT a tracking option?

A. Partial log

B. Log

C. Full log

D. Network log

Answer: (SHOW ANSWER)

NEW QUESTION: 95

What is a reason for manual creation of a NAT rule?

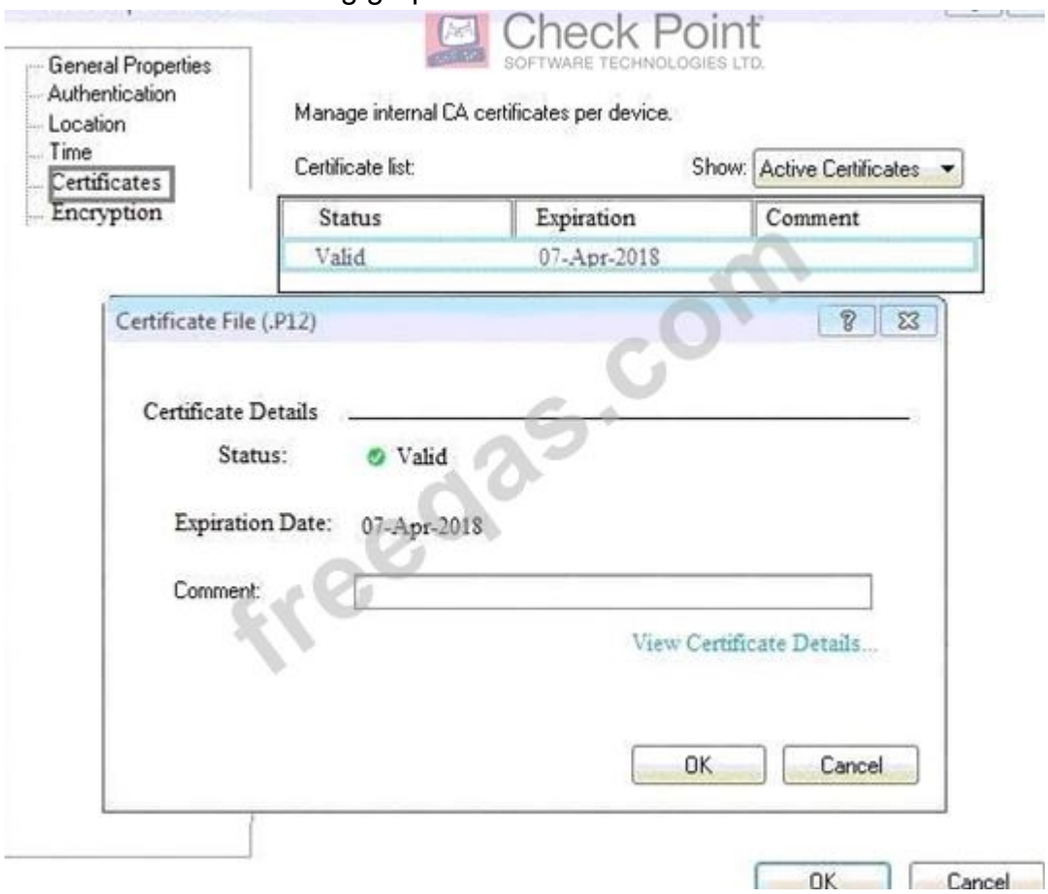
A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public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

NEW QUESTION: 96
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES
256 for IKE phase 2. Why is this a problematic setup?
A. The two algorithms do not have the same key length and so don't work together. You will get the error
... No proposal chosen...
B. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
C. All is fine and can be used as is.
D. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
Access roles allow the firewall administrator to configure network access according to:
A. a combination of computer groups and network
B. users and user groups
C. all of above
D. remote access clients
Answer: C (LEAVE A REPLY)
Explanation
To create an access role:
* Select Users and Administrators in the Objects Tree.
* Right-click Access Roles > New Access Role.
The Access Role window opens.
* Enter a Name and Comment (optional) for the access role.
* In the Networks tab, select one of these:
* Any network
* Specific networks - Click the plus sign and select a network.
Your selection is shown in the Networks node in the Role Preview pane.
* In the Users tab, select one of these:

* Any user
* All identified users - Includes users identified by a supported authentication method (internal users, AD users or LDAP users).
* Specific users - Click the plus sign.
A window opens. You can search for Active Directory entries or select them from the list.
* In the Machines tab, select one of these:
* Any machine
* All identified machines - Includes machines identified by a supported authentication method (AD).
* Specific machines - Click the plus sign.
You can search for AD entries or select them from the list.
* Optional: For computers that use Full Identity Agents, from the Machines tab select Enforce IP spoofing protection.
* Click OK.
The access role is added to the Users and Administrators tree.

NEW QUESTION: 98
You can see the following graphic:



What is presented on it?
A. VPN certificate properties of the John's gateway.
B. Properties of personal .p12 certificate file issued for user John.
C. Expired .p12 certificate properties for user John.
D. Shared secret properties of John's password.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
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)
Explanation
References:

NEW QUESTION: 100
An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through
your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG.
Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for
GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).
Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the
1-minute interval.
If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive
packet every minute.
Which of the following is the BEST explanation for this behavior?
A. The setting Log does not capture this level of detail for GRE. Set the rule tracking action to Audit since
certain types of traffic can only be tracked this way.
B. The Log Server log unification process unifies all log entries from the Security Gateway on a specific
connection into only one log entry in the SmartView Tracker. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
C. The Log Server is failing to log GRE traffic properly because it is VPN traffic. Disable all VPN configuration to the partner site to enable proper logging.
D. The log unification process is using a LUUID (Log Unification Unique Identification) that has become
corrupt. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE sessions.
This is a known issue with GRE. Use IPSEC instead of the non-standard GRE protocol for

encapsulation.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Which of the following is NOT an integral part of VPN communication within a network?
A. VPN key
B. VPN community
C. VPN trust entities
D. VPN domain
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
VPN key (to not be confused with pre-shared key that is used for authentication).
- VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.
- VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.
- VPN Community - A named collection of VPN domains, each protected by a VPN gateway.

Reference:
http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

NEW QUESTION: 102
Fill in the blank: A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.
A. Clientless remote access
B. Clientless direct access
C. Client-based remote access
D. Direct access
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation: Clientless - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80BC_Firewall/html_frameset.htm?topic=documents/R80/CP_R80BC_Firewall/92704

NEW QUESTION: 103
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address.
A. High Availability

B. Load Sharing Multicast
C. Load Sharing Pivot
D. Master/Backup
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation :
ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.
Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

NEW QUESTION: 104
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers?
A. Anti-Malware
B. IPS
C. Anti-bot
D. Anti-Spam
Answer: C (LEAVE A REPLY)
Anti-Bot
The Need for Anti-Bot
There are two emerging trends in today's threat landscape:
* A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.
* Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.
Both of these trends are driven by bot attacks.
A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.
Reference: https://sc1.checkpoint.com/documents/R77/
CP_R77_ThreatPrevention_WebAdmin/102176.htm

NEW QUESTION: 105
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https, ssh	Accept	Log	Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	Log	Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.

B. Another administrator is logged into the Management and currently editing the DNS Rule.

C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 106

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

A. An office mode address must be obtained by the client.

B. The SNX client application must be installed on the client.

C. SNX modifies the routing table to forward VPN traffic to the Security Gateway.

D. Active-X must be allowed on the client.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 107

Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161

B. Using UDP Multicast or Broadcast on port 8116

C. Quicker than Full sync

D. Transfers changes in the Kernel tables between cluster members

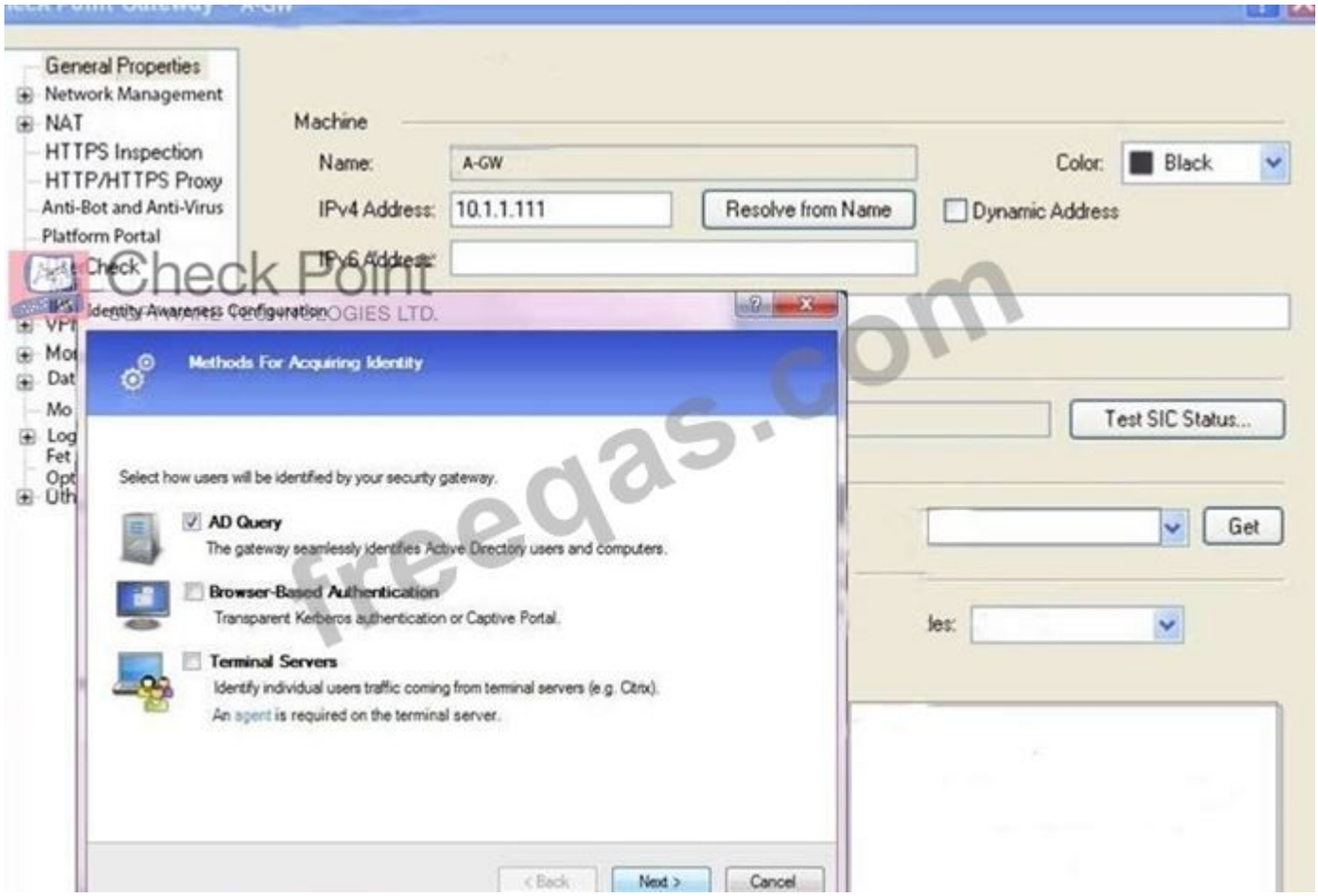
Answer: (SHOW ANSWER)

Explanation

References:

NEW QUESTION: 108

On the following picture an administrator configures Identity Awareness:



After clicking "Next" the above configuration is supported by:

A. Kerberos SSO which will be working for Active Directory integration

B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user

C. Obligatory usage of Captive Portal

D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

Answer: B (LEAVE A REPLY)

Explanation

To enable Identity Awareness:

The Identity Awareness Configuration wizard opens.

NEW QUESTION: 109

Which policy type has its own Exceptions section?

A. Thread Prevention

B. Access Control

C. Threat Emulation

D. Desktop Security

Answer: A (LEAVE A REPLY)
Explanation
The Exceptions Groups pane lets you define exception groups. When necessary, you can create exception
groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option
facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly
required exceptions. You can choose to which rules you want to add exception groups. This means they can be
added to some rules and not to others, depending on necessity.

NEW QUESTION: 110
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)
Explanation
Explanation:
The first rule is the automatic rule for the Accept All Encrypted Traffic feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.
2. Site to site VPN - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.
3. Remote access - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92709.htm

NEW QUESTION: 111
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He
can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.
A. remove database lock
B. The database feature has one command lock database override.
C. override database lock

D. The database feature has two commands: lock database override and unlock database. Both will work.

Answer: (SHOW ANSWER)

Explanation

Use the database feature to obtain the configuration lock. The database feature has two commands: The commands do the same thing: obtain the configuration lock from another administrator.

Description	Use the `lock database override` and `unlock database` commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	o `lock database override` o `unlock database`

NEW QUESTION: 112

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

A. Organization Unit

B. Country

C. Common name

D. User container

Answer: D (LEAVE A REPLY)

Distinguished Name Components

CN=common name, OU=organizational unit, O=organization, L=locality,ST=state or province, C=country name

NEW QUESTION: 113

Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

A. /var/log/Cpbackup/backups/backup/backup_fw.tgs

B. /var/log/Cpbackup/backups/backup/backup_fw.tar

C. /var/log/Cpbackup/backups/backups/backup_fw.tar

D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D (LEAVE A REPLY)

Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration.

The configuration is saved to a .tgz file in the following directory:

Gaia OS Version	Hardware	Local Directory
R75.40 - R77.20	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	/var/CPbackup/backups/
R77.30	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk91400

NEW QUESTION: 114
After the initial installation the First Time Configuration Wizard should be run.
A. First Time Configuration Wizard can be run from the Unified SmartConsole.
B. First Time Configuration Wizard can be run from the command line or from the WebUI.
C. First time Configuration Wizard can only be run from the WebUI.
D. Connection to the internet is required before running the First Time Configuration wizard.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Check Point Security Gateway and Check Point Security Management require running the First Time Configuration Wizard in order to be configured correctly. The First Time Configuration Wizard is available in Gaia Portal and also through CLI.
To invoke the First Time Configuration Wizard through CLI, run the config_system command from the Expert shell.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111119

NEW QUESTION: 115
Which policy type is used to enforce bandwidth and traffic control rules?
A. Threat Emulation
B. Access Control
C. QoS
D. Threat Prevention
Answer: C (LEAVE A REPLY)
Check Point's QoS SolutionQoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software.

NEW QUESTION: 116
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?
A. Threat Agent Solution
B. Public Cloud Services
C. Load Sharing Mode Services
D. Smart Cloud Services
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
Which Check Point software blade provides protection from zero-day and undiscovered threats?
A. Firewall
B. Threat Emulation
C. Application Control
D. Threat Extraction
Answer: D (LEAVE A REPLY)
SandBlast Threat Emulation
As part of the Next Generation Threat Extraction software bundle (NGTX), the SandBlast Threat Emulation capability prevents infections from undiscovered exploits zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network.

NEW QUESTION: 118
Which of the following is NOT an alert option?
A. SNMP
B. High alert
C. Mail
D. User defined alert
Answer: B (LEAVE A REPLY)
Explanation
In Action, select:
* none - No alert.
* log - Sends a log entry to the database.
* alert - Opens a pop-up window to your desktop.
* mail - Sends a mail alert to your Inbox.
* snmptrap - Sends an SNMP alert.
* useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert

NEW QUESTION: 119

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

_____

A. UserCheck
B. User Directory
C. User Administration
D. User Center
Answer: B (LEAVE A REPLY)
Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/118981

NEW QUESTION: 120
In Security Gateways, SIC uses _____ for encryption.
A. AES-256
B. AES-128
C. 3DES
D. DES
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
Fill in the blank: _____information is included in the "Full Log" tracking option, but is not included in the "Log" tracking option?
A. file attributes
B. application
C. destination port
D. data type
Answer: D (LEAVE A REPLY)
Tracking Options

NEW QUESTION: 122

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

A. User Directory

B. Captive Portal and Transparent Kerberos Authentication

C. Captive Portal

D. UserCheck

Answer: (SHOW ANSWER)

To enable Identity Awareness:

The Identity Awareness Configuration wizard opens.

NEW QUESTION: 123

Which of the following is NOT an identity source used for Identity Awareness?

A. Remote Access

B. UserCheck

C. AD Query

D. RADIUS

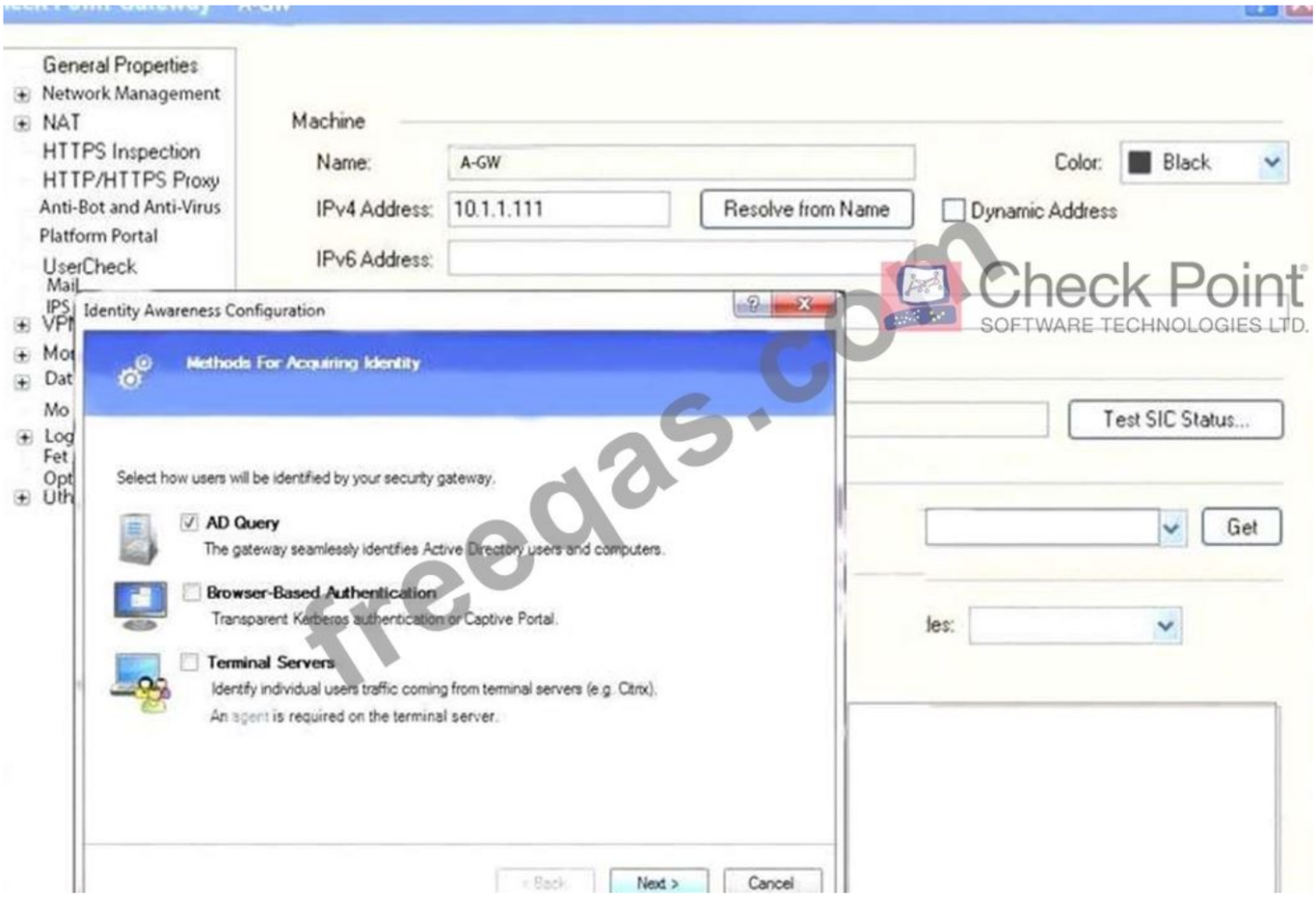
Answer: B (LEAVE A REPLY)

Explanation/Reference:

Reference: https://www.checkpoint.com/products/identity-awareness-software-blade/

NEW QUESTION: 124

On the following picture an administrator configures Identity Awareness:



After clicking "Next" the above configuration is supported by:

A. Kerberos SSO which will be working for Active Directory integration

B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user

C. Obligatory usage of Captive Portal

D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

Answer: B (LEAVE A REPLY)

Explanation

To enable Identity Awareness:

The Identity Awareness Configuration wizard opens.

NEW QUESTION: 125

Which of the following is NOT an alert option?

A. SNMP

B. High alert

C. Mail

D. User defined alert

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation: In Action, select:

none - No alert.

log - Sends a log entry to the database.
- alert - Opens a pop-up window to your desktop.
- mail - Sends a mail alert to your Inbox.
- snmptrap - Sends an SNMP alert.
- useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SmartViewMonitor_AdminGuide/101104.htm

NEW QUESTION: 126
What are the two high availability modes?
A. Load Sharing and Legacy
B. Traditional and New
C. Active and Standby
D. New and Legacy
Answer: (SHOW ANSWER)
ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION: 127
What component of R80 Management is used for indexing?
A. DBSync
B. API Server
C. fwm
D. SOLR
Answer: (SHOW ANSWER)
Explanation
References:

NEW QUESTION: 128
Which information is included in the "Full Log" tracking option, but is not included in the "Log" tracking option?
A. file attributes
B. data type information
C. application information
D. destination port
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129

Which of the following commands is used to monitor cluster members?

A. cphaprob state

B. cphaprob status

C. cphaprob

D. cluster state

Answer: A (LEAVE A REPLY)

Explanation

References:

NEW QUESTION: 130

You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:

APP	PID	S	#START	START_TIME		MON	COM
CPVIEWD	3075	E	1	[16:26:54]	5/5/2016	N	cpv
CPD	0	T	1	[17:15:57]	6/5/2016	N	cpd
FWD	21752	E	1	[17:15:31]	6/5/2016	N	fwd
CPM	0	T	1	[15:32:23]	6/5/2016	N	/op
FWM	0	T	1	[17:15:45]	6/5/2016	N	fwm
RFL	7873	E	1	[16:32:52]	5/5/2016	N	Log
SMARTVIEW	7884	E	1	[16:32:52]	5/5/2016	N	Sma
INDEXER	7954	E		[16:32:53]	5/5/2016	N	/op
SMARTLOG_	SERVER	797	E 1	[16:32:53]	5/5/2016	N	/op
SVR	8045	E	1	[16:32:54]	5/5/2016	N	SVR
DASERVICE	8054	E	1	[16:32:54]	5/5/2016	N	DAS
CPSM	0	T	0	[17:17:02]	5/5/2016	N	cps

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

A. CDP is down

B. SVR is down

C. FWM is down

D. CPSM is down

Answer: C (LEAVE A REPLY)

Explanation/Reference:

The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.). STATE is T (Terminate = Down)

Explanation :

Symptoms

SmartDashboard fails to connect to the Security Management server.

▪

1. Verify if the FWM process is running. To do this, run the command:

[Expert@HostName:0]# ps -aux | grep fwm

2. If the FWM process is not running, then try force-starting the process with the following command:

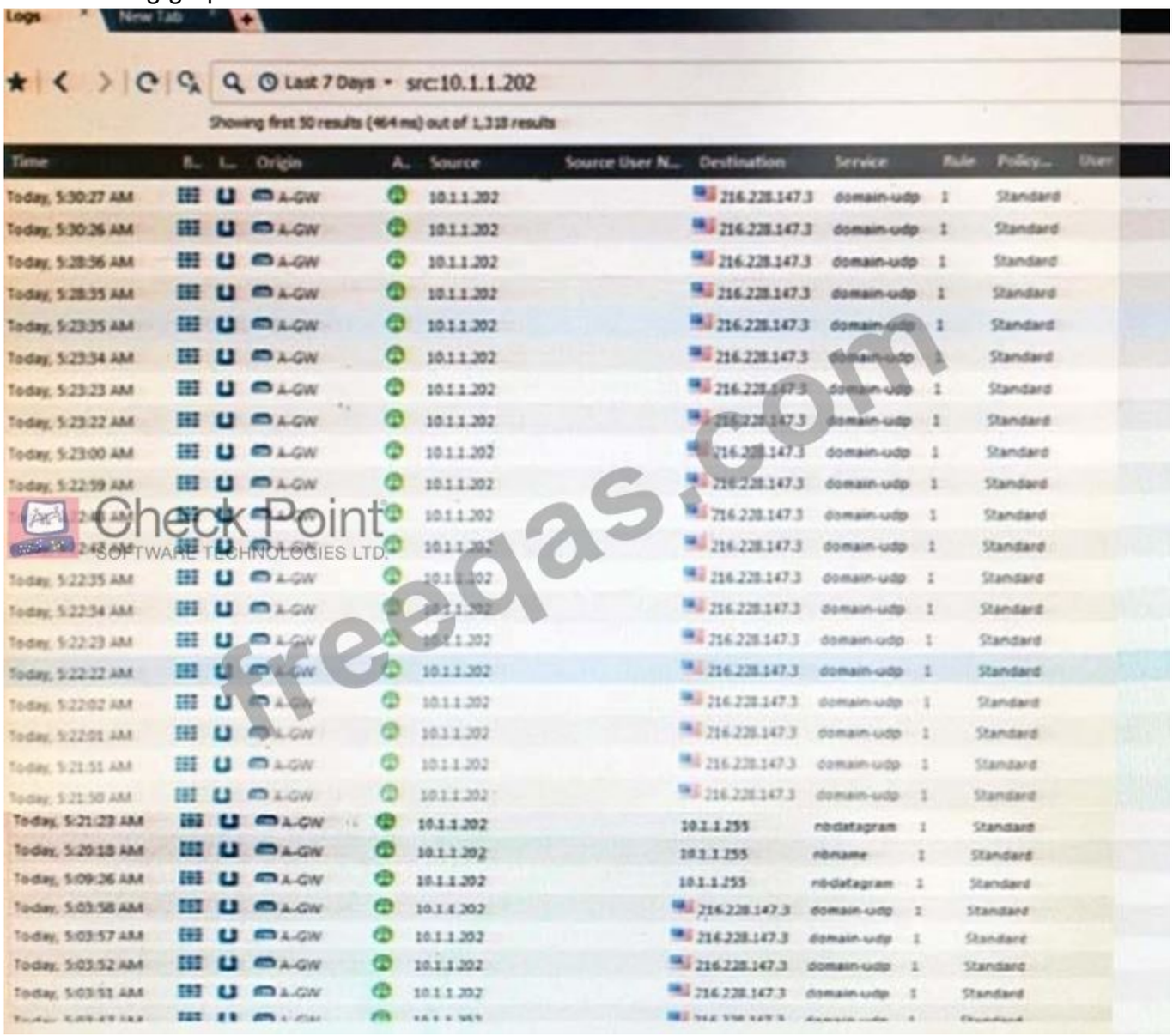
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk12120

NEW QUESTION: 131
Which tool is used to enable ClusterXL?
A. cpconfig
B. SmartConsole
C. sysconfig
D. SmartUpdate
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
The following graphic shows:

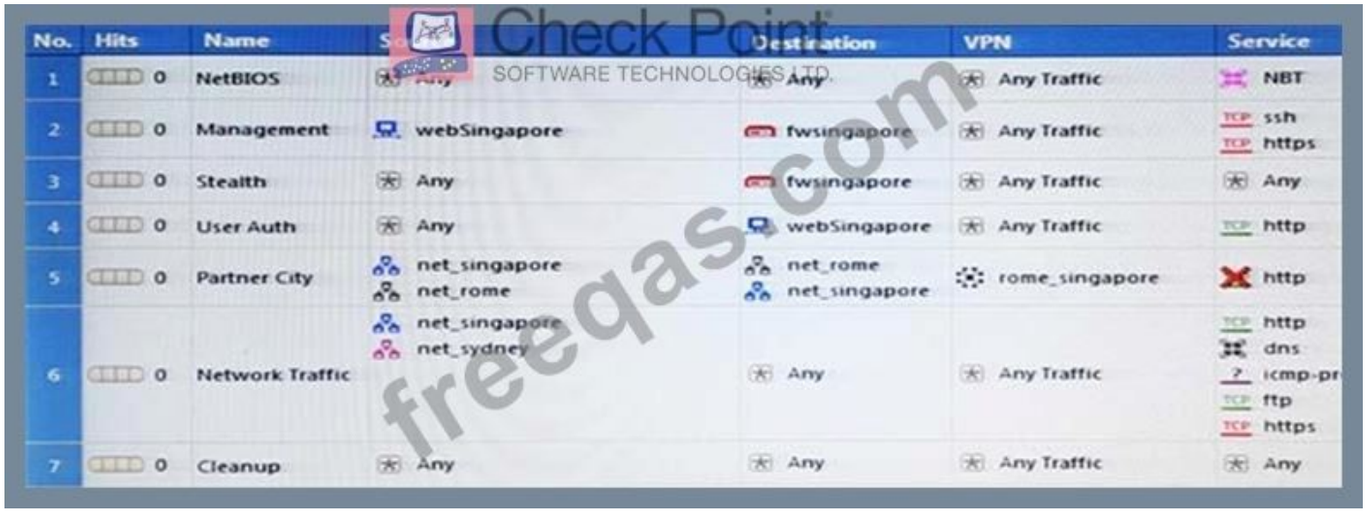


A. View from SmartView Tracker for logs initiated from source address 10.1.1.202
B. View from SmartLog for logs initiated from source address 10.1.1.202

C. View from SmartView Monitor for logs initiated from source address 10.1.1.202
D. View from SmartView Tracker for logs of destination address 10.1.1.202
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
Which deployment adds a Security Gateway to an existing environment without changing IP routing?
A. Standalone
B. Remote
C. Bridge Mode
D. Distributed
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
Which rule is responsible for the user authentication failure?



A. Rule 6
B. Rule 4
C. Rule 5
D. Rule 3
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.

What is the most likely reason?

A. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.

B. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

C. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole. Check that the correct key details are used.

D. Check Point Management software authentication details are not automatically the same as the Operating System authentication details. Check that she is using the correct details.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 136

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

A. Distributed

B. Standalone

C. Bridge Mode

D. Targeted

Answer: (SHOW ANSWER)

Explanation/Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

NEW QUESTION: 137
Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?
A. Each NIC has several traffic queues that are handled by multiple CPU cores
B. Each NIC has one traffic queue that is handled by one CPU
C. There is no traffic queue to be handled
D. Several NICs can use one traffic queue by one CPU
Answer: A (LEAVE A REPLY)

NEW QUESTION: 138
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)
Explanation
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

NEW QUESTION: 139
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?
A. UDP port 265
B. UDP port 256
C. TCP port 265
D. TCP port 256
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
Which GUI tool can be used to view and apply Check Point licenses?
A. cpconfig
B. Management Command Line
C. SmartConsole

D. SmartUpdate

Answer: D (LEAVE A REPLY)

Explanation

SmartUpdate GUI is the recommended way of managing licenses.

NEW QUESTION: 141

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select "More", and then check "Enable Identity Captive Portal"

B. On the firewall object, Legacy Authentication screen, check "Enable Identity Captive Portal"

C. In the Captive Portal screen of Global Properties, check "Enable Identity Captive Portal"

D. On the Security Management Server object, check the box "Identity Logging"

Answer: A (LEAVE A REPLY)

Explanation

NEW QUESTION: 142

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box.

What should you look for?

A. Secure Internal Communications (SIC) not configured for the object.

B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.

C. Anti-spoofing not configured on the interfaces on the Gateway object.

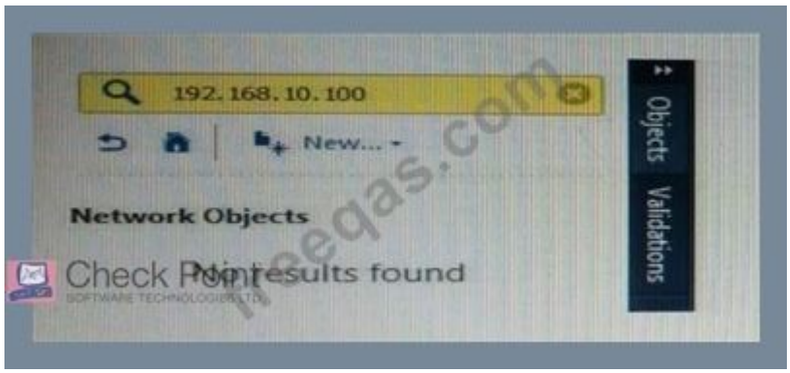
D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B (LEAVE A REPLY)

Explanation

NEW QUESTION: 143

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.



A. There is no object on the database with that IP address.
B. There is no object on the database with that name or that IP address.
C. Object does not have a NAT IP address.
D. Search detailed is missing the subnet mask.
Answer: (SHOW ANSWER)

NEW QUESTION: 144
The _____ feature allows administrators to share a policy with other policy packages.
A. Global Policies
B. Concurrent policy packages
C. Concurrent policies
D. Shared policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 145
Which of the following is NOT defined by an Access Role object?
A. Source Server
B. Source Network
C. Source User
D. Source Machine
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the
Rule Base. How do you achieve this?
A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
B. Create a Suspicious Activity Rule in Smart Monitor.
C. Select Block intruder from the Tools menu in SmartView Tracker.
D. Add a temporary rule using SmartDashboard and select hide rule.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as

_____

A. UserCheck
B. User Directory
C. User Administration
D. User Center
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/118981

NEW QUESTION: 148
Which command can you use to verify the number of active concurrent connections?
A. show all connections
B. fw ctl pst pstat
C. fw conn all
D. show connections
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
Fill in the blank: Gaia can be configured using the _____ or _____ .
A. Gaia; command line interface
B. WebUI; Gaia Interface
C. Command line interface; WebUI
D. Gaia Interface; GaiaUI
Answer: C (LEAVE A REPLY)
Configuring Gaia for the First Time
In This Section:
Running the First Time Configuration Wizard in WebUI
Running the First Time Configuration Wizard in CLI
After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112568

NEW QUESTION: 150
Joey is using the computer with IP address 192.168.20.13. He wants to access web page "www.Check Point.com", which is hosted on Web server with IP address 203.0.113.111.
How many rules on Check Point Firewall are required for this connection?
A. Two rules - first one for the HTTP traffic and second one for DNS traffic.
B. Only one rule, because Check Point firewall is using Stateful Inspection technology.
C. Only one rule, because Check Point firewall is a Packet Filtering firewall
D. Two rules - one for outgoing request and second one for incoming replay.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?
A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
B. mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json
C. mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json
D. mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.1

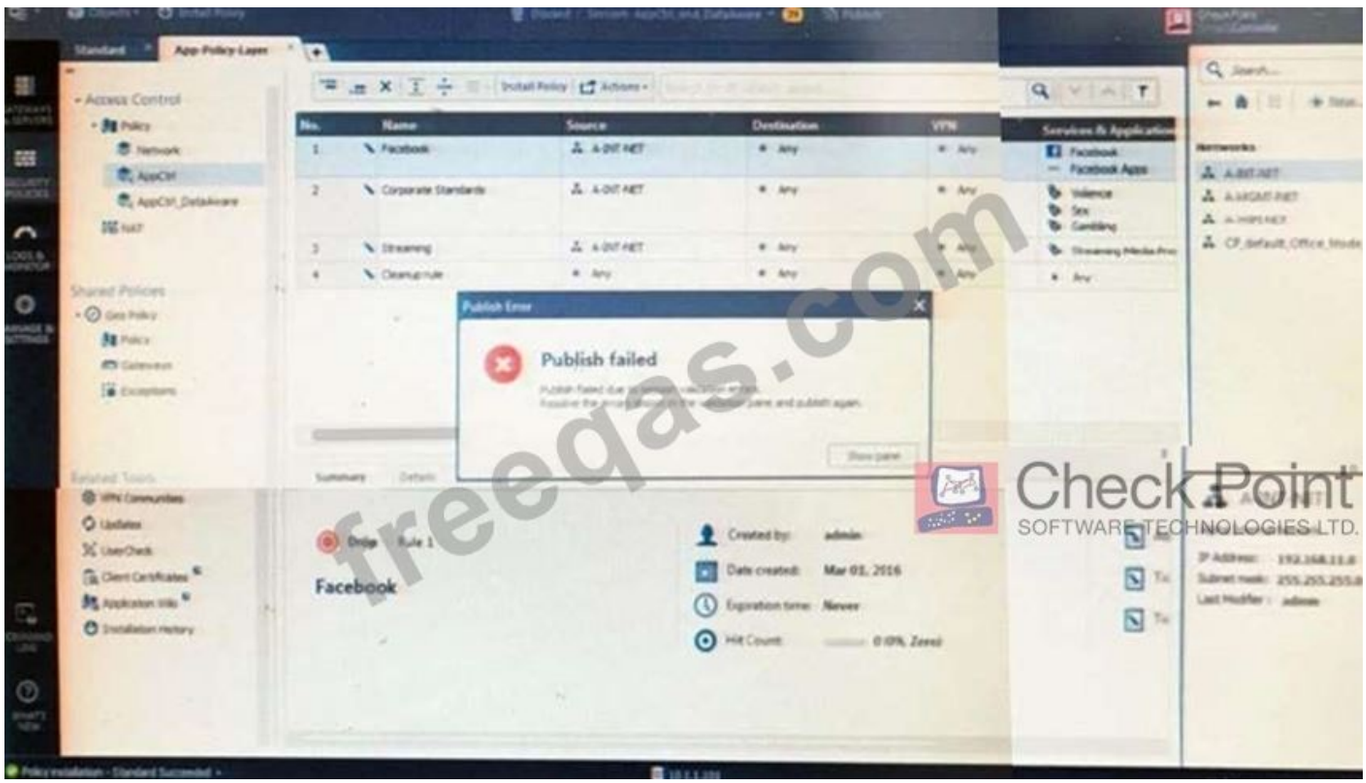
NEW QUESTION: 152
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members?
A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
C. cphaprob -a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1
Answer: (SHOW ANSWER)
Explanation/Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

NEW QUESTION: 153
Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Requested
B. Account Logon
C. Kerberos Ticket Renewed
D. Kerberos Ticket Timed Out
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.
A. True, Central Licenses can be installed with CPLIC command on a Security Gateway
B. True, CLI is the preferred method for Licensing
C. False, Central Licenses are installed via Gaia on Security Gateways
D. False, Central Licenses are handled via Security Management Server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155
Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.
Where can the administrator check for more information on these errors?



A. The Log and Monitor section in SmartConsole
B. The Validations section in SmartConsole
C. The Objects section in SmartConsole
D. The Policies section in SmartConsole
Answer: B (LEAVE A REPLY)

Validation ErrorsThe validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.
To publish, you must fix the errors.

NEW QUESTION: 156
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?
A. Create network object that restrict all applicable rules to only certain networks.
B. Create a separate Security Policy package for each remote Security Gateway.
C. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
D. Run separate SmartConsole instances to login and configure each Security Gateway directly.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
Fill in the blanks: A High Availability deployment is referred to as a _____ cluster and a Load Sharing
deployment is referred to as a _____ cluster.
A. Standby/standby; active/active
B. Active/active; standby/standby
C. Active/active; active/standby;
D. Active/standby; active/active
Answer: D (LEAVE A REPLY)
Explanation
In a High Availability cluster, only one member is active (Active/Standby operation).
ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is
increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle
network traffic (Active/Active operation).

NEW QUESTION: 158
Look at the following screenshot and select the BEST answer.

A. Internal clients can upload and download archive-files to FTP_Ext server using FTP.
B. Clients external to the Security Gateway can upload any files to the FTP_Ext-server using FTP.
C. Clients external to the Security Gateway can download archive files from FTP_Ext server using FTP.

D. Internal clients can upload and download any-files to FTP_Ext-server using FTP.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 159
Where can you trigger a failover of the cluster members?
Log in to Security Gateway CLI and run command clusterXL_admin down.
In SmartView Monitor right-click the Security Gateway member and select Cluster member stop.
Log into Security Gateway CLI and run command cphaprob down.
A. 1, 2, and 3
B. 2 and 3
C. 1 and 2
D. 1 and 3
Answer: C (LEAVE A REPLY)
Explanation
How to Initiate Failover

Method	To stop ClusterXL	To Start ClusterXL
Run: o cphaprob -d faildevice -t 0 -s ok register o cphaprob -d faildevice -s problem report and: o cphaprob -d faildevice -s ok report o cphaprob -d faildevice unregister	Effect: o Disables ClusterXL o Does not disable synchronization	Effect: o Enables ClusterXL o Does not initiate full synchronization
Recommended method: Run: o clusterXL_admin down o clusterXL_admin up	o Disables ClusterXL o Does not disable synchronization	o Enables ClusterXL o Does not initiate full synchronization
In SmartView Monitor: 1. Click the Cluster object. 2. Select one of the member gateway branches. 3. Right click the cluster member. 4. Select **Down**.	o Disables ClusterXL o Disables synchronization	o Enables ClusterXL o Does not initiate full synchronization

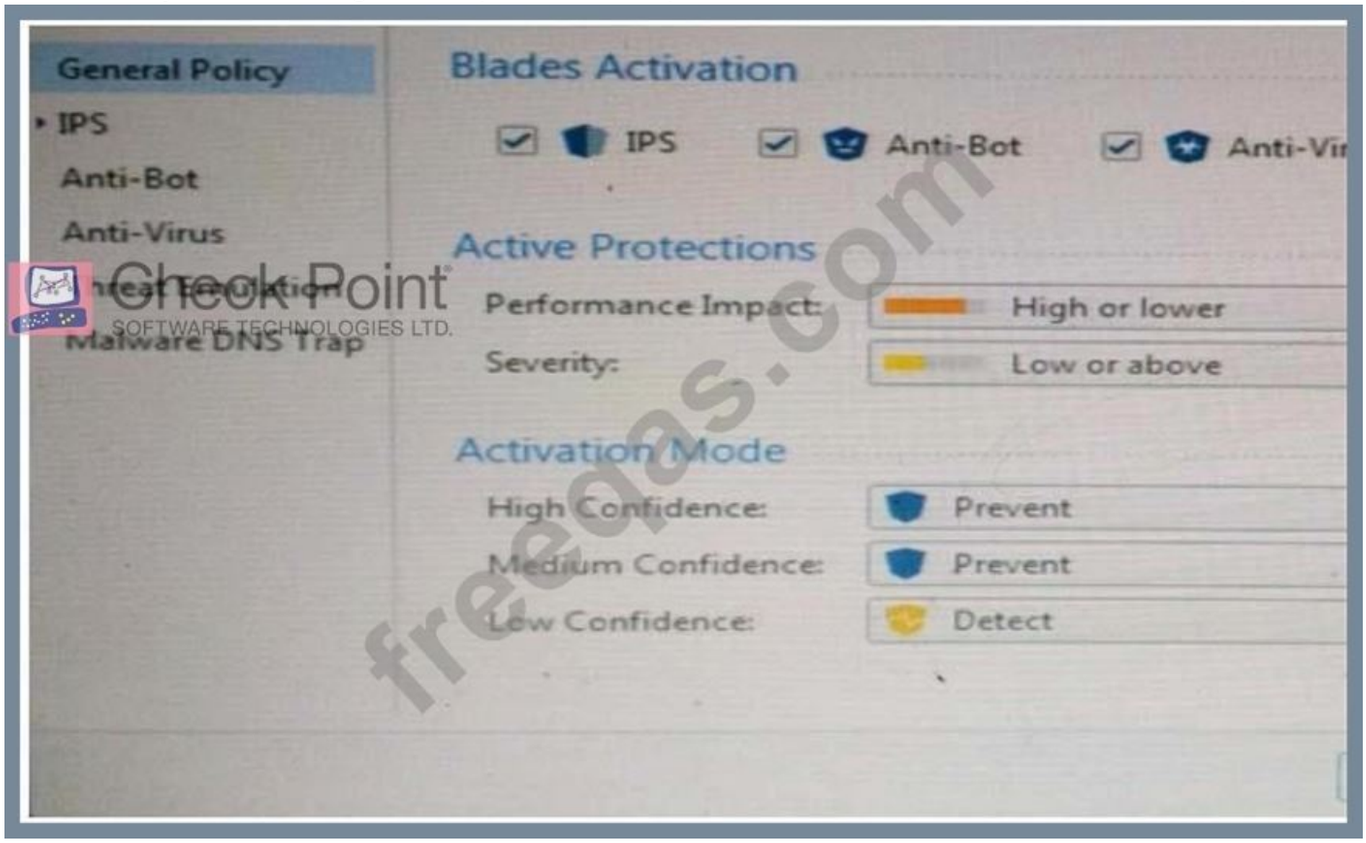
References:

NEW QUESTION: 160
Which of the following statements accurately describes the command snapshot?
A. snapshotstores only the system-configuration settings on the Gateway
B. snapshotcreates a Security Management Server full system-level backup on any OS
C. snapshotcreates a full OS-level backup, including network-interface data, Check Point production information, and configuration settings of a GAiA Security Gateway.
D. A Gateway snapshotincludes configuration settings and Check Point product information from the remote Security Management Server
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner
site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE
phase 2. Why is this a problematic setup?
A. The two algorithms do not have the same key length and so don't work together. You will get the error
... No proposal chosen...
B. All is fine and can be used as is.
C. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in
phase 2 only costs performance and does not add security due to a shorter key in phase 1.
D. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for
higher performance for setting up the tunnel.
Answer: (SHOW ANSWER)

NEW QUESTION: 162
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?
A. All options stop Check Point processes
B. backup
C. migrate export
D. snapshot
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106127

NEW QUESTION: 163
Provide very wide coverage for all products and protocols, with noticeable performance impact.



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 the Performance Impact to Medium or lower.
B. The problem is not with the Threat Prevention Profile. Consider adding more memory to the appliance.
C. Set the Performance Impact to Very Low Confidence to Prevent.
D. Set High Confidence to Low and Low Confidence to Inactive.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?
A. backup
B. Database Revision
C. snapshot
D. migrate export
Answer: (SHOW ANSWER)
2. Snapshot ManagementThe snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on anothermachine of the same type is supported.
The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be saved.

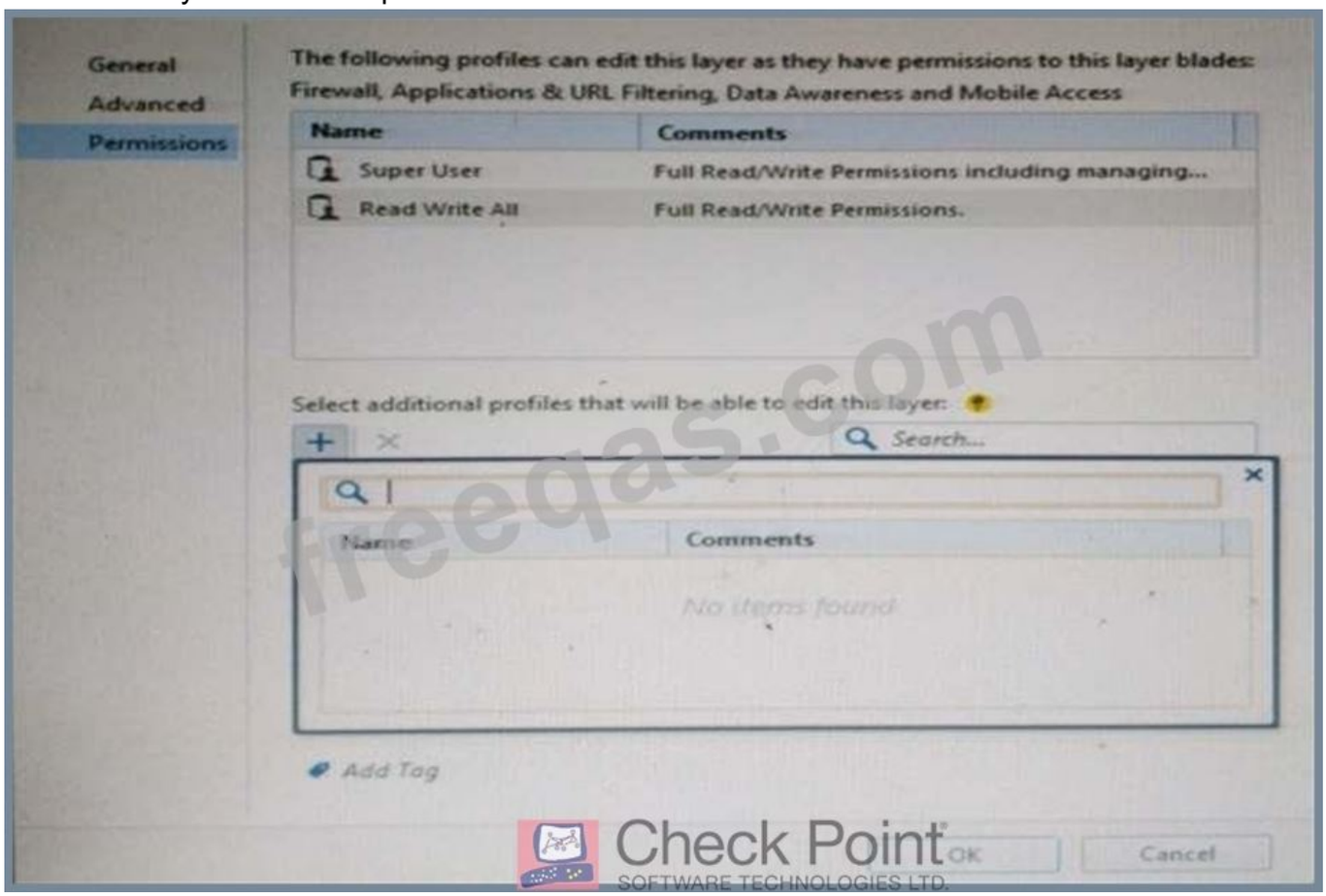
NEW QUESTION: 165
The Firewall kernel is replicated multiple times, therefore:
A. The Firewall can run different policies per core
B. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
C. The Firewall kernel only touches the packet if the connection is accelerated
D. The Firewall can run the same policy on all cores
Answer: (SHOW ANSWER)

NEW QUESTION: 166
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address.
A. Load Sharing Multicast
B. High Availability
C. Master/Backup
D. Load Sharing Pivot
Answer: (SHOW ANSWER)
Explanation :ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

NEW QUESTION: 167
How do you configure the Security Policy to provide uses access to the Captive Portal through an external
(Internet) interface?
A. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an
external interface.

B. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all
interfaces.
C. Change the gateway settings to allow Captive Portal access via an external interface.
D. No action is necessary. This access is available by default.
Answer: (SHOW ANSWER)

NEW QUESTION: 168
You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything. What is the most likely cause of this problem? Select the BEST answer.



A. "Edit layers by Software Blades" is unselected in the Permission Profile
B. There are no permission profiles available and you need to create one first.
C. All permission profiles are in use.
D. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 169
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. Security questions
B. Check Point password
C. SecurID
D. RADIUS
Answer: A (LEAVE A REPLY)
Authentication Schemes :- Check Point Password
- Operating System Password
- RADIUS
- SecurID
- TACAS
- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

NEW QUESTION: 170
A Cleanup rule:
A. logs connections that would otherwise be dropped without logging by default.
B. drops packets without logging connections that would otherwise be dropped and logged by default.
C. logs connections that would otherwise be accepted without logging by default.
D. drops packets without logging connections that would otherwise be accepted and logged by default.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

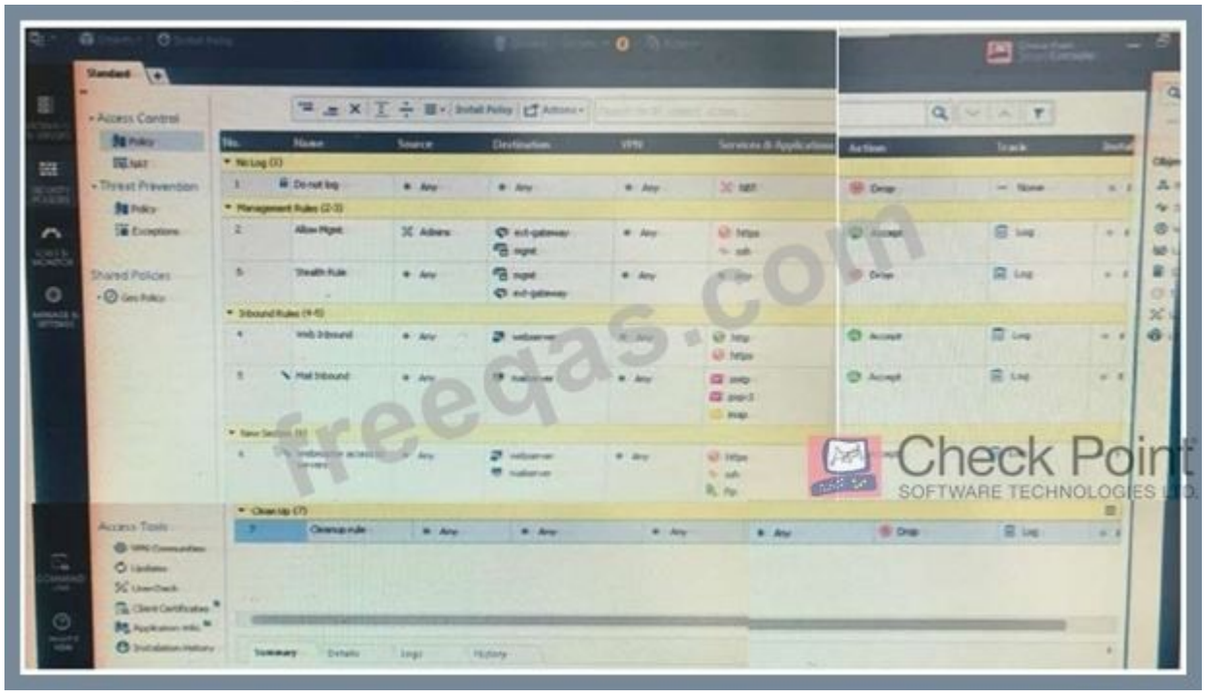
NEW QUESTION: 171
Where is the "Hit Count" feature enabled or disabled in SmartConsole?
A. On the Policy Package
B. On each Security Gateway
C. On the Policy layer
D. In Global Properties for the Security Management Server
Answer: B (LEAVE A REPLY)
Explanation
Explanation/Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

NEW QUESTION: 172
What is the Manual Client Authentication TELNET port?
A. 259
B. 900
C. 23
D. 264

Answer: A (LEAVE A REPLY)

NEW QUESTION: 173

Examine the following Rule Base.



What can we infer about the recent changes made to the Rule Base?

A. Rule 7 was created by the 'admin' administrator in the current session

B. 8 changes have been made by administrators since the last policy installation

C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator

D. Rule 1 and object webserver are locked by another administrator

Answer: D (LEAVE A REPLY)

On top of the print screen there is a number "8" which consists for the number of changes made and not saved.

Session Management Toolbar (top of SmartConsole)

NEW QUESTION: 174

You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateSPort
B. XlateDPort
C. XlateSrc
D. XlateDst
Answer: A (LEAVE A REPLY)

NEW QUESTION: 175
Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?
A. Create a text-file with mgmt_cli script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.
B. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command load configuration.
C. Create a text-file with DBEDIT script that creates all objects and policies. Run the file in the command line of the management server using command dbedit -f.
D. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.
Answer: A (LEAVE A REPLY)
Did you know: mgmt_cli can accept csv files as inputs using the --batch option.
The first row should contain the argument names and the rows below it should hold the values for these parameters.
So an equivalent solution to the powershell script could look like this:
data.csv:

name	ipv4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server> This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

NEW QUESTION: 176
The most important part of a site-to-site VPN deployment is the _____ .
A. Internet
B. Remote users
C. Encrypted VPN tunnel
D. VPN gateways
Answer: (SHOW ANSWER)
Explanation

Site to Site VPN
The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

NEW QUESTION: 177
One of major features in R80 SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?
A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.
Answer: (SHOW ANSWER)
In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions Reference: http://downloads.checkpoint.com/dc/download.htm?ID=65846

NEW QUESTION: 178
As you review this Security Policy, what changes could you make to accommodate Rule 4?

A. Remove the service HTTP from the column Service in Rule 4.
B. Modify the column VPN in Rule 2 to limit access to specific traffic.
C. Nothing at all
D. Modify the columns Source or Destination in Rule 4
Answer: (SHOW ANSWER)

NEW QUESTION: 179
Which rule is responsible for the user authentication failure?

A. Rule 4
B. Rule 5
C. Rule 6
D. Rule 3
Answer: (SHOW ANSWER)

NEW QUESTION: 180
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)
Explanation/Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120829

NEW QUESTION: 181
Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last
rules in the Rule Base.
A. Firewall drop
B. Explicit
C. Implicit accept
D. Implicit drop
E. Implied
Answer: E (LEAVE A REPLY)
Explanation
This is the order that rules are enforced:

NEW QUESTION: 182
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 local one does not install the Anti-Malware policy along with the Network policy.
B. The Global one also saves and published the session before installation.
C. The second one pre-select the installation for only the current policy and for the applicable gateways.
D. The Global one can install multiple selected policies at the same time.
Answer: (SHOW ANSWER)

NEW QUESTION: 183
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100

Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateDPort
B. XlateSPort
C. XlateSrc
D. XlateDst
Answer: B (LEAVE A REPLY)

NEW QUESTION: 184
Authentication rules are defined for _____.
A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database
Answer: A (LEAVE A REPLY)
Explanation/Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_SGW_WebAdmin/6721.htm

NEW QUESTION: 185
Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?
A. cpconfig
B. fw ctl pstat
C. cpview
D. fw ctl multik stat
Answer: C (LEAVE A REPLY)
CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and

information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101878

NEW QUESTION: 186
Which of the following is used to enforce changes made to a Rule Base?
A. Publish database
B. Activate policy
C. Save changes
D. Install policy
Answer: D (LEAVE A REPLY)
NEW QUESTION: 187
Which options are given on features, when editing a Role on Gaia Platform?
A. Read/Write, Read Only
B. Read/Write, Read only, None
C. Read/Write, None
D. Read Only, None
Answer: (SHOW ANSWER)
Roles
Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.
You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.
Gaia includes these predefined roles:
You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

NEW QUESTION: 188
Which icon indicates in the WebUI that read/write access is enabled?
A. Pencil
B. Padlock

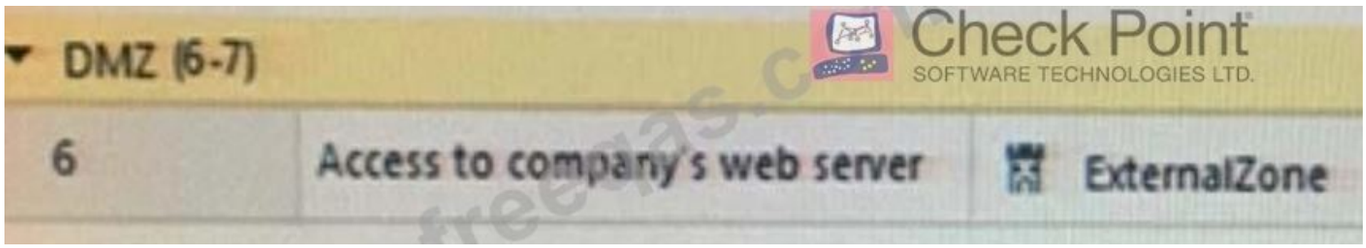
C. Book
D. Eyeglasses
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 189
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to
designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy
permits access only from Join's desktop which is assigned an IP address 10.0.0.19 via DHCP.
John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT
department gave the laptop a static IP address, but the limits him to operating it only from his desk. The
current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to
move around the organization and continue to have access to the HR Web Server.
To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server
from any machine and from any location.
John plugged in his laptop to the network on a different network segment and he is not able to connect. How
does he solve this problem?
A. The firewall admin should install the Security Policy
B. John should install the identity Awareness Agent
C. Investigate this as a network connectivity issue
D. John should lock and unlock the computer
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers?
A. Anti-Malware
B. IPS
C. Anti-bot
D. Anti-Spam
Answer: C (LEAVE A REPLY)
Explanation

Anti-Bot
The Need for Anti-Bot
There are two emerging trends in today's threat landscape:
* A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.
* Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.
Both of these trends are driven by bot attacks.
A bot is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

NEW QUESTION: 191
What does ExternalZone represent in the presented rule?



A. The Internet.
B. Interfaces that administrator has defined to be part of External Security Zone.
C. External interfaces on all security gateways.
D. External interfaces of specific gateways.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Configuring Interfaces
Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window.
To configure the interfaces:
1. From the Devices window, double-click the Security Gateway 80.
The Security Gateway window opens.
2. Select the Interfaces tab.
3. Select Use the following settings. The interface settings open.
4. Select the interface and click Edit.
The Edit window opens.
5. From the IP Assignment section, configure the IP address of the interface:
1. Select Static IP.
2. Enter the IP address and subnet mask for the interface.

6. In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartProvisioning_WebAdmin/16741.htm

NEW QUESTION: 192
Which method below is NOT one of the ways to communicate using the Management API's?
A. Typing API commands from a dialog box inside the SmartConsole GUI application
B. Typing API commands using Gaia's secure shell (clash)19+
C. Typing API commands using the "mgmt_cli" command
D. Sending API commands over an http connection using web-services
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____ .
A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation: https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486