CheckPoint.156-210.v2025-07-12.q115

Exam Code:	156-210
Exam Name:	Check Point CCSA NG
Certification Provider:	CheckPoint
Free Question Number:	115
Version:	v2025-07-12
# of views:	106
# of Questions views:	1150
https://www.freepdfdumps.com/CheckPoint.156-210.v2025-07-12.q115.html	

NEW QUESTION: 1
You are following the procedure to setup user authentication for TELNET to prompt for a distinct destination. This allows the firewall to simulate a TELNET Proxy. After you defined the user on the Firewall and use VPN-1/FireWall-1 Authentication, you would:
A. Stop the Firewall.
B. Restart the Firewall.
C. Start the Policy Editor and go to Manage service, and edit TELNET service.
D. Ensure that the Authentication method is enabled in the firewall object.
E. Ensure that there are no existing rules already allowing TELNET.
Answer: D (LEAVE A REPLY)
Explanation: Remember, we have to enable the desired authentication method in both, the user and the firewall object, in this case we use firewall 1 authentication.
Incorrect Answers
A:we don't need to stop the firewall to achieve this kind of functionally, actually we are loosing all of it.
B:its not necessary to make a restart, we could make this configuration in a dynamic way.
C:We don't need to modify the service definition, remember that user authentication has its own telnet proxy.
E:you can have existing rules, you just need to make sure that they are below of the one that makes telnet authentication for your users.

NEW QUESTION: 2
What are the two components of SecureUpdate? (Select two.)
A. Central License
B. Installation Service
C. Installation Manager
D. License Manager

E. Local Manager
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 3
As a firewall administrator, you are required to create VPN-1/Firewall-1 users for authentication. When you create a user for user authentication, the data is stored in the?
A. Inspect Engine.
B. Rule base.
C. Users database
D. Rulebase fws file
E. Inspect module.
Answer: C (LEAVE A REPLY)
Explanation: When you create users in VPN/Firewall 1 you are storing them in a component, called the User Database. Note that the user database reside in the management station and si pushed / installed to the firewall modules when a policy is installed. See page 219 of Syngress Book "Checkpoint NG - Next Generation Security Administration".
Incorrect Answers
A:This is not the place where users are stored, this is the place where the traffic is matched to the rules inside the policies.
B:The rulebase contains the criteria for the security policy that is scanned through the inspect engine, it doesn't store the users.
D:The users aren't here, they are in the User Database, see the explanation above.
E:An inspect module is a piece of inspect code used by the inspect engine to extend the capabilities of the firewall in native form, it doesn't store the users.

NEW QUESTION: 4
Client Authentication rules should be placed above the Stealth rule, so users can authenticate to the firewall.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation: you should always place any client authentication rule above the stealth rule, the stealth rule will prevent any connection to the firewall for security purposes, the client authentication needs to make a telnet connection on port 259 TCP or an HTTP connection in port 900 TCP. So, you should always place your client authentication rules above the stealth rule or you will have your traffic dropped.
Incorrect Answers
B:The statement at the question is true, we need the stealth rule below the client authentication rule, if we don't do it this way, our authentication request will be logged or dropped depending on our Stealth rule.

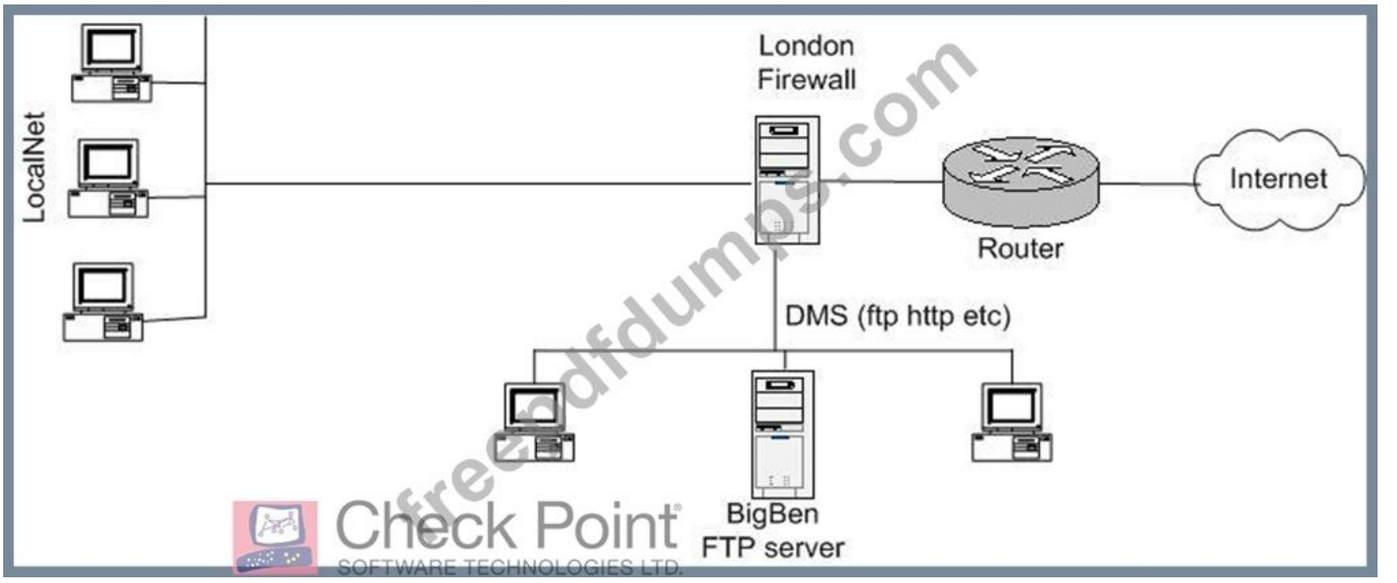
NEW QUESTION: 5
CORRECT TEXT
At Certpaper, auditors are Check Point Security Administrators with a customized permissions profile. Auditors must have the ability to review information from SmartView Tracker, SmartView Status, and SmartView Monitoring, but they may not make changes to the information. Auditors are not permitted to view security Policies or the objects database.
Which of the following settings grants auditors the MOST appropriate set of permissions, based on the corporate environment, described above for Certpaper?
Answer:
Pending

NEW QUESTION: 6
How do recover communications between your management module and
enforcement module if you lock yourself out via a rule policy that is configured incorrectly?
A. Cp delete all all.
B. Cp pause all all.
C. Cp stop all all.
D. Cp unload all all.
E. Cp push all all.
Answer: D (LEAVE A REPLY)
Explanation: you can use the command "cp unload all all" to discard any policy installed in the gateway module, with this, you can reset the communication and correct the rulebase in your policy so you don't lock out the communication between the firewall and the management module.
Incorrect AnswersA:this is not a valid command to resolve this communication problem, you have to unload the current installed policy.
B:this is not a valid option.
C:This will stop the checkpoint applications running, this answer is wrong because we need to unload a policy, and also, we need our applications running to make this.
E:This will start checkpoint applications, this answer is wrong because we need to unload a policy that is corrupting communication, we don't need to start services.

NEW QUESTION: 7
What complements are necessary for VPN-1/FireWall-1 NG to scan e-mail, passing through the firewall, for macro viruses?
A. UFP and OPSEC-certified scanning product.
B. CVP and OPSEC-certified virus scanning product.
C. UFP and CVP.
D. UFP, CVP and OPSEC-certified content filter.
E. None of the above, VPN-1/FireWall-1 NG scans for macro viruses by default.
Answer: B (LEAVE A REPLY)

Explanation: since we want to scan e-mail and check for viruses, all we need is a product that check for certain virus fingerprints, this products is the OPSEC certified Application and we link it with the firewall module with CVP (Content Vectoring Protocol). The most common in enterprise environments is to have asecond server with a crossover cable to the firewall running this virus checking application, this is also a best practice.
Incorrect Answers
A:UFP (URI Filtering Protocol) is not used for Virus scanning, it is usually for Content Management with applications like WebSense to restrict access to some URI's (URL's).
C:We don't need both of them, we can provide the functionality only with CVP.
D:We don't need UFP for this.
E:This is not a functionality provided by default you need to use an OPSEC application connected by Content Vectoring Protocol.

NEW QUESTION: 8
The security administrator for the following configuration only allows members of the localnet managers group access files in BigBen (the FTP Server)



Select below the rule that allows local managers to access the FTP server from any location.
No
SOURCE
DESTINATION
SERVICE
ACTION
1
LocalManagers@Any
BigBen
ftp
User Auth
2
LocalManagers@Net_London

BigBen
ftp
Client Auth
3
LocalManagers@Any
BigBen
ftp
Session Auth
4
LocalManagers@Net_Tokyo
BigBen
ftp
User Auth
A. Rule 1.
B. Rule 2.
C. Rule 3.
D. Rule 4.
E. None of these rules allow access.
Answer: A (LEAVE A REPLY)
Explanation: Rule 1 is the appropriate rule in here because since we want the managers to access from any location we have the "@any" at the end of the source with an user authentication action that is the most appropriate authentication method because the local managers group wants to make FTP connections and User authentication provides advanced proxy services for FTP. It also supports HTTP, Telnet and Rlogin.
Incorrect Answers
B:Rule 2 is incorrect because we want the managers to access from anywhere.
C:Rule 3 is incorrect because Session authentication does not provide the advanced capabilities of User authentication in the case of the FTP service D:Rule 4 is incorrect because we want the managers to access from anywhere.
E:This is incorrect because answer A provide the desired results.

NEW QUESTION: 9
Which of the following ports would TELNET service use for communications?
A. 25
B. 23
C. 30
D. 29
E. 21
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10

CORRECT TEXT
You have locked yourself out, with a rule or an incorrectly configured Security Policy. What would you do to recover communication between your SmartCenter Server and Enforcement Module?
Answer:
Pending

NEW QUESTION: 11
If users authenticated successfully, they have matched the User and Authentication rule restriction of the user group to which they belong.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation: if a user belong to several groups and the user authenticates successfully it means that he have matched his user & authentication restrictions and also the ones of the groups he belongs to. This is the way checkpoint authentication works, you have to pass your personal authentication restrictions, and the ones in your groups to authenticate successfully.
Incorrect Answers
B:This answer is wrong because you have to get a match in your user & group authentication restrictions to get a successful authentication. You must get a match in all of them.

NEW QUESTION: 12
Your customer has created a rule so that every time a user wants to go to Internet, that user must be authenticated. The customer requires an authentication scheme that provides transparency for the user and granular control for the administrator.
User must also be able to log in from any location. Based on this information, which authentication schemes meets the customer's needs?
A. Session
B. User
C. Client
D. Dual
E. Reverse
Answer: (SHOW ANSWER)
Explanation: As it says in the question, the administrator wants granular control and that requires authentication in a user basis, he also wants logging from any place, so the best option is to use "User Authentication" because we can have a centralized user database that will provide successfully provide the mobility requirements exposed in the question.
Incorrect Answers
A:Session authentication does not provide the mobility requirements because the user will have to install the session authentication agent on every PC and that's not a transparent experience for him.

C:Client authentication does not provide a transparent experience to the user because he / she have to make a manual logon to the firewall with Telnet or HTTP.
D:This is not one of the 3 authentication methods supported by the NG suite.
E:This is not one of the 3 authentication methods supported by the NG suite.

NEW QUESTION: 13
What configuration is said to be used if the Policy Editor and the Management Server are deployed on separate machines?
A. None of the above
B. Client/Client
C. Server/Server
D. Firewall
E. Client/Server
Answer: E (LEAVE A REPLY)

NEW QUESTION: 14
CORRECT TEXT
Which of the following are core functions of Application Intelligence? (Choose two)
Answer:
Pending

NEW QUESTION: 15
You are working with multiple firewalls that have extensive Rule Bases. To simplify administration task, which of the following should you choose to do?
A. Create Network range objects that restrict all applicable rules to only certain networks.
B. Run separate GUI clients for external and internal firewalls.
C. Eliminate all possible contradictory rules such as stealth and clean-up rules.
D. Save a different Rule Base for each remote firewall.
E. None of the above.
Answer: (SHOW ANSWER)
Explanation: this is one of the best practices recommended by Checkpoint engineers, if you have a large number of entries in your rulebase for multiple remote firewalls you can have one rulebase for each remote one, so you can simplify your administration for each of them.
Incorrect Answers
A:This is not recommended because you could have hosts in one network sending packets through multiple firewalls modules, so you don't need to manipulate Network Range objects.
B:Checkpoint is trying to make their products as consolidated as possible, they are trying to put all the components in the same console, as is the case of the Policy Editor that includes "Object Tree", "Visual Policy Editor" and "Security Policy Editor", in the same console.
C:this is not an option because this rules are often necessary to comply with business requirements, they are best practices too.

E:is incorrect because Answer D is the only valid choice.

NEW QUESTION: 16
CORRECT TEXT
Which of the following statements is TRUE of transparent authentication in NG with Application Intelligence? (Choose three)
Answer:
Pending

NEW QUESTION: 17
When you select the alert radio button on the topology tab of the interface properties window:
A. The action specified in the Action element of the Rule Base is taken.
B. The action specified in the Anti-Spoofing Alert field in the Global properties window is taken.
C. The action specified in the Pop up Alter Command in the Global properties window is taken.
D. Both A and B.
E. Both B and C.
Answer: E (LEAVE A REPLY)
Explanation: when you select the alert button in the properties of the interface at the topology tab, you achieve to main things: the action specified at the anti-spoof alert in the global properties is executed and theaction of the alert pop up command at the Global Properties gets executed too. The configuration of these action is made from the policy editor at the Global Configuration of the Checkpoint infrastructure.
Incorrect Answers
A:This is wrong, the action taken is in the Anti-Spoofing Alert field in the Global properties window is taken, not at the action field of the rule base.
B:This is only part of the answer.
C:This is only part of the answer
D:This in wrong because it includes answer A that is incorrect.

NEW QUESTION: 18
Which is the correct rule in the following Rule Base?
No

SOURCE
DESTINATION
SERVICE
ACTION
TRACK
1
AllUsers@Chicago
Any
Any
Session Auth
Log
2
AllUsers@Chicago
Chicago
Any
Session Auth
Log
3
AllUsers@Any
Any
Any
Session Auth
Log
4
AllUsers@Chicago
Any
Any
User Auth
Log
A. Rule 2
B. Rule 1
C. Rule 3
D. Rule 4
E. None of the rules allow access.
Answer: B (LEAVE A REPLY)
Explanation: Rule 1 is the entry to apply to our rulebase, in this rule we are including all the users defined at Chicago, giving access to any service at any destination always that the session could be authenticated. This rule is the only one that covers the needs of the questions in a 100%.
Incorrect Answers

A:Rule 2 is incorrect since you cannot have the users at the same source to the same destination, in this fashion, the traffic is local and it doesn't need to pass though the gateway. That is not agood practice.
D:Putting "ANY" on the service entry is not correct because user authentication only works with HTTP, Telnet, FTP and RLogin, not with "ANY" service.

NEW QUESTION: 19
Choose the BEST response to finish this statement.
A Firewall:
A. Prevents unauthorized to or from a secured network.
B. Prevents unauthorized to or from a unsecured network.
C. Prevents authorized access to or from an Intranet.
D. Prevents authorized access to or from an Internet.
E. Prevents macro viruses from infecting the network.
Answer: A (LEAVE A REPLY)
Explanation: this is the most correct answer because we use firewalls in networks where we need security, so we secure our network from unauthorized, and with this we can control who can get in or get out of it.
Incorrect Answers
B:We don't need firewalls in a unsecured network, we need them in networks that require security.
C:We should not need to prevent authorized access, if it authorized, the traffic should go through.
D:We should not need to prevent authorized access, if it authorized, the traffic should go through.
E:A firewall is not a virus scanning engine, we have anti-virus for that matter, Firewalls are a form of packet analyzers that says if traffics go through, is redirected or is discarded at one of its interfaces, it doesn't look for virus patterns.

NEW QUESTION: 20
Which of the following characteristics BEST describes the behaviour of Check Point NG with Application Intelligence?
A. Traffic not expressly permitted is prohibited.
B. TELNET, HTTP; and SMTP are allowed by default.
C. Secure connections are authorized by default. Unsecured connectdions are not.
D. Traffic is filtered using controlled ports.
E. All traffic is expressly permitted by explicit rules.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
Why would an administrator want to negate a selected object in the Rule Base?
A. To connect to any destination using tcp/ip service.
B. To include all objects or users and exclude a specific object or user

C. To nest a specific object or user
D. To include a specific object or user
E. To connect to any destination using ftp service.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
CORRECT TEXT
One of the functions of the SmartDefense console is to:
Answer:
Pending

NEW QUESTION: 23
What component of CheckPoint NG allows you to export Logs to an external program such as Access or Excel.
A. ELA
B. LEA
C. Logs cannot be exported to external programs.
D. ULLLS
Answer: B (LEAVE A REPLY)
Explanation: You can use LEA (Log export API), first Microsoft have to create an interface so it can access the information in the logs. See Appendix D.3 of the CCSA NG Courseware - Management I.
Incorrect Answers
A:ELA is used to send information inside the checkpoint logs (import data).
C:This is possible through LEA.
D:This is not related to our question matters.

NEW QUESTION: 24
What Implicit Rules are allowed by default in the Global Properties?
Answer:
Explanation: by the default "Accept Firewall control connections" is allowed, it opens port 256 for firewall communications. Also CPRID connections are accepted, this port is used for Secure Update.
Incorrect Answers
A:By default RIP is not allowed, how have to change the global configuration to change this.
C:By default DNS over port 53 UDP is not allowed, how have to change the global configuration to change this.
D:By default ICMP messages are not allowed, how have to change the global configuration to change this.

NEW QUESTION: 25

Which NG with Application Intelligence feature allows a Security Administrator to granularly control acceptable FTP commands?
A. SmartDefense, FTP Security Server settings
B. Rule Base Service field
C. Check Point Gateway object, Security Server settings
D. FTP Security Server object settings
E. Global Properties, Security Server settings.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
Choose the two responses that BEST describe a VPN-1/Firewall-1 Rule Base.
A Rule Base is:
A. A collection of corporate guidelines used to structure the network Security Policies for users operating behind the firewall.
B. A collection of system settings that make up implicit rules defining network security.
C. A repository of DLL files, each provides a specific security function.
D. A set of explicitly and implicitly defined rules used to define network security.
E. The process by which secure communications are established between different VPN-1/Firewall-1 Modules, operating within an enterprise security environment.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 27
CORRECT TEXT
Which authentication method could be used for SIP services? (Choose two)
Answer:
Pending

NEW QUESTION: 28
Which command utility allows verification of the Security Policy installed on a firewall module?
A. Fw ct1 pstat.
B. Fw printlic.
C. Fw stat.
D. Fw ver.
E. Fw pol.
Answer: C (LEAVE A REPLY)
Explanation: you can issue the command "fw stat" at the enforcement modules to get a print out of the installed policy with the date and time of installation, the name of the policy and the name of the host fromwhich it was installed. See Page 114 of the Syngress Book - Checkpoint NG "Next Generation Security Administration".
Incorrect Answers
A:This command is used to get internal status information of Firewall 1.

B:This command is not related to policy verification.
D:This command returns the currently installed version of Firewall 1.
E:This is not a valid command.

NEW QUESTION: 29
You are the Security Administrator with one SmartCenter Server managing one Enforcement Moduel. SmartView Status displayes a computer icon with an "I" in the Status column. What does this mean?
A. The Enforcement Module is installed and responding to status checks, but the status is problematic.
B. Secure Internal Communications (SIC) has not been established between the SmartCenter Server and the Enforcement Module.
C. You have entered the wrong password at SmartView Status login.
D. The VPN-1/Firewall-1 Enforcement Module has been compromised and is no longer controlled by this SmartCenter Sever.
E. The SmartCenter Server cannot contact a gateway.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
Installation time for creating network objects will decrease if you list machine names and IP addresses in the hosts files.
A. True
B. False
Answer: (SHOW ANSWER)
Explanation: the installation time for network objects will always be lower if you populate your "hosts" file because the lookup process for the name resolution process will be much lower, since the Hosts file is always checked first upon going to resolve the name-to-IP mappings with a DNS server.
Incorrect AnswersB:When you populate the hosts file, you can speed up the creation of network objects, this is because all the name resolution take place locally.

NEW QUESTION: 31
CORRECT TEXT
Which type of rule should be placed above the Stealth Rule?
Answer:
Pending

NEW QUESTION: 32
CORRECT TEXT
As a Security Administrator, you want to force users to authenticate. You have selected Client Authentication for the type of authentication. Users will be using a Web browser to authenticate. Which of the following TCP ports will authenticate users?
Answer:
Pending

NEW QUESTION: 33
With SecureUpdate you are able to: (Select all that apply)
Answer:
Explanation: Secure update is a tool for the easy management of both, the version and licensing for both Checkpoint and OPSEC products, In the GUI you have two main panels, one for the products and one for the licenses. It provides information on the version of OPSEC and Checkpoint products installed, it allows the central management of licenses for checkpoint products and also allows remote update capabilities for OPSEC and Checkpoint products.
Incorrect Answers
A:This is not currently possible, you cannot change license from central to local, however you can do the opposite, you can change a license from local to central. See "Checkpoint licensing FAQ" in the Checkpoint web site.
E:With Secure Update you can update existing Checkpoint and OPSEC software, but you cannot perform new installations remotely from it.

NEW QUESTION: 34
Which of the following are tasks performed by a VPN-1/FireWall-1 SmartCenter Server? Choose three.
A. Compiles the Rule Base into an enforceable Security Policy.
B. Replicates state tables for high availability.
C. Manages the User Database.
D. Examines all communications according to the Enterprise Security Policy.
E. Stores VPN-1/FirWall-1 logs.
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 35
You can edit VPE objects before they are actualized (translated from virtual network objects to real).

A. True
B. False.
Answer: B (LEAVE A REPLY)
Explanation: as stated by checkpoint engineers in the checkpoint web site, the objects corresponding to the Visual Policy Editor cannot be edited until they are actualized, and that actualization takes place when the topology calculations get to a consistent state, this makes the Visual Policy editor gets to a convergent state and let you edit the VPE's.
Incorrect Answers
A:You can't edit VPO objects until the VPO gets to a consistent state through the topology calculations.

NEW QUESTION: 36
How would you remedy a conflict between Anti-Spoofing and NAT?
A. By removing die translated, external I? address to the invalid Addresses on the internal interface
B. Do nothing
C. By adding the translated, external IP address to the Valid Addresses on the external interface
D. By adding the translated external IP address to the Valid Addresses on the internal interface
E. Reinstall NAT rules
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
Currently, the Accounting Department is FTP-ing a file in the bank. Which Log Viewer Module would show you the activity occurring at the present time?
A. Security Log.
B. Active Connections Log.
C. Accounting Log-
D. Administrative Log.
E. None of the above.
Answer: B (LEAVE A REPLY)
Explanation: The "active Connection" is one of the 3 available modes inside the Log Viewer, it allows you to see in real time what is the status of certain connections that are passing though the firewall, FTP connections are supported.
Incorrect Answers
A:This does not provide real time capabilities, its not even a Log viewer mode.
C:The only component that provide real time information inside the Log Viewer is the Active Connection Log. No other provide real time capabilities.
D:The only component that provide real time information inside the Log Viewer is the Active Connection Log. No other provide real time capabilities.
E:is wrong because answer B is the right choice.

NEW QUESTION: 38
CORRECT TEXT
The SANS Dshield.org Storm center integrates with SmartDefense, by: (Choose two)
Answer:
Pending

NEW QUESTION: 39
Consider the following network:
No
Original Packet
Translated Packet
Source
Destination
Service
Source
Destination
Service
The administrator wants to take all the local and DMZ hosts behind the gateway except the HTTP server 192.9.200.9. The http server will be providing public services and must be accessible from Internet. Select the best NAT solution below that meets these requirements.
A. Use automatic NAT that creates a static NAT to the HTTP server.
B. To hide the private addresses set the address translation for Private Net.
C. To hide the private address set the address translation for 192.9.200.0.
D. Use automatic NAT rule creation to hide NAT Local net and private Net.
E. Both A and D.
Answer: E (LEAVE A REPLY)
Explanation: Since we want the HTTP server to be accessible from the Internet, you have to use Static NAT, and since you need to hide the other hosts in the DMZ and in the private network, you can use Dynamic NAT to achieve the desired results.
Incorrect AnswersA:This is only part of the correct answer, is not complete.
B:We have the hosts at the private net, What about the other hosts in the DMZ?.
C:This is just the network containing the hosts in the DMZ, what about the hosts at the internal net?
D:This is only part of the correct answer, is not complete.

NEW QUESTION: 40
Which is not a step in Session Authentication?
Answer:
Explanation: In session authentication the session agent doesn't try to authenticate the user if the validation checking is already done.

Here is the complete process:First, the user connects directly to the destination server, then the inspection module intercepts the connection and the inspection module connects to the session agent on the client PC, then the session agent prompts the user for authentication data and returns it to the inspection engine in the firewall, at the end, if the authentication is successful, the gateway allows the connection to pass through to the target server.
Incorrect Answers
E:This is not part of the session authentication process.

NEW QUESTION: 41
What are the advantages of Central Licensing? (Select all that apply.)
A. Multiple IP address are needed for all licenses
B. A license can be removed from one Module and installed on another Module
C. The licenses remain valid when changing the IP address of a Module
D. The licenses are revoked when changing the IP address of a Module
E. Only one IP address is needed for all licenses
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Hybrid Authentication allows VPN-1/Firewall-1 NG to authenticate SecuRemote/SecureClient, using which of the following?
A. RADIUS
B. 3DES
C. TACACS
D. Any authentication method supported by VPN-1/Firewall-1.
E. Both A and C.
Answer: D (LEAVE A REPLY)
Explanation: "Hybrid Authentication for IKE" is just that, it allows you to use existing authentication servers supported by VPN1/FW1 as shared secrets for IKE. This is supported since FW 1 4.1 SP1 and SecuRemote 4153. See Page 382 of "Essential Checkpoint Firewall 1" from Dameon Welch.
Incorrect AnswersA:This is not the most complete answer, the most complete is answer "D".
B:This is not a kind of authentication server, its an encryption algorithm.
C:This is not the most complete answer, the most complete is answer "D".
E:This is not the most complete answer, the most complete is answer "D".

NEW QUESTION: 43
Tess was initiating a client authentication session by beginning an HTTP session on port 259 with the gateway named London. What do you think might be wrong with the address Tess specified in the browser?

A. The user should use Session Authentication method to successfully connect to the destination server.
B. The user should bypass the firewall at port 259 to connect successfully.
C. The user was using the wrong port. She needs to use port 900 to connect successfully.
D. The user should bypass the firewall at port 900 to connect successfully.
E. The user should be able to connect, since she was using the right port.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
When you disable a rule the rule is NOT disabled until you verify your Security Policy.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: once you disable a rule, it becomes ineffective in your policy, you don't have to verify the policy to make the disabling effective, once you want to push the policy to the enforcement modules again the disabled rule is not enforced. To disable a rule just right click the rule number and select "Disable".
Incorrect Answers
A:You don't have to verify your policy to make a disabling action take effect over your policy, this is not necessary. See page 215 from the Syngress Book "Checkpoint NG - Next Generation Security Administration).

NEW QUESTION: 45
You are a firewall administrator with one Management Server managing 3 different Enforcement Modules. One of the Enforcement Modules does NOT show up in the dialog box when attempting to install a Security Policy. Which of the following is the most likely cause?
A. No master file was created.
B. License for multiple firewalls has expired.
C. The firewall has NOT been rebooted.
D. The firewall was NOT listed in the Install On column of the rule.
E. The firewall is listed as "Managed by another Management Module (external)" in the Workstation Properties dialog box.
Answer: E (LEAVE A REPLY)
Explanation: when you have firewall objects defined in the policy editor you can select between 2 options in the general tab of the object at the "Object Management" setting. The options are "Managed by another management server (External)" or "Managed by this management server (Internal)". If you select our first option (External) we will not be able to install any policy on this firewall, because our management server does not figure as the master for the object.
Incorrect AnswersA:Our need cant be addressed by a Master file. You can have a review to the Checkpoint documentation with the functions of the Masters file.
B:This is not a licenses problem, the management station cannot see the firewall as an option.

C:We don't need to reboot the firewall to allow it to receive policy updates.
D:This is not a possible cause.

NEW QUESTION: 46
CORRECT TEXT
Which of the following BEST describes the function of Dynamic Network Address Translation (Dynamic NAT)?
Dynamic NAT:
Answer:
Pending

NEW QUESTION: 47
Why must Client Authentication rule be placed above Stealth rule in the Rule Base?
A. In order that they can have access to the Policy Editor
B. In order that they can have access to the Management Server
C. In order that they can have access to the local Management Server
D. In order that they can have access to the OS
E. In order that they can have access to the local firewall
Answer: E (LEAVE A REPLY)

NEW QUESTION: 48
Why is Application Layer particularly vulnerable to attacks? Choose three
A. The Application Layer does not perform unauthorized operations.
B. Malicious Java, ActiveX, and VB Scripts can exploit host system simply by browsing.
C. Defending against attacks at the Application Layer is more difficult, than at lower layers of the OSI model.
D. The application Layer supports many protocols.
E. The application Layer performs access-control and legitimate-use checks.
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 49

What NAT type translates valid IP addresses to invalid IP addresses for connections initiated by external clients?

A. Static Destination NAT

B. None of the above

C. Hide Mode

D. Static NAT

E. Static Source NAT

Answer: A (LEAVE A REPLY)

NEW QUESTION: 50

CORRECT TEXT

VPN-1/FireWall-1 supports User Authentication for which of the following services?

Select the response below that contains the MOST complete list of supported services.

Answer:

Pending

NEW QUESTION: 51

CORRECT TEXT

Which authentication method could be used for H.323 services? (Choose two)

Answer:

Pending

NEW QUESTION: 52

If the security policy editor or system status GUI is open, you can open the log viewer GUI from the window menu.

A. True

B. False

Answer: A (LEAVE A REPLY)

Explanation: when you are at the policy editor or the system status, you can click on the windows menu and go to the log viewer or other GUIs. When you call the GUIs this way you don't have to re-authenticate, you use your current security credentials.

Incorrect Answers

B:This answer is incorrect because you can call the log viewer through the Windows menu in the policy editor or the system status.

NEW QUESTION: 53

What is true of the Enforcement Module? (Select all that apply)

Answer:

Explanation: We normally use a multihomed machine to have internal, external and DMZ interfaces. It's also installed in a enforcement point, because it will analyze the network traffic to comply with the enterprise security policy. Additionally, it can provide authentication through the

supported schemes (Client, Session, User) and also some content security at the application level like stripping off Java code from HTTP connections.
Incorrect Answers
B:Logging is maintained at the management module.

NEW QUESTION: 54
What command uninstalls the currently loaded Inspection Code from selected targets?
A. cp load
B. cp uninstall
C. cp unload
D. cp putkey
E. cp install
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
Which of the following statements about Client Authentication is FALSE?
A. In contrast to User Authentication that allows access per user. Client Authentication allows access per IP address.
B. Authentication is by user name and password, but it is the host machine (client) that is granted access.
C. Client Authentication enables Security Administrators to grant access privileges to a specific IP address, after successful authentication.
D. Client Authentication is more secure than User Authentication, because it allows multiple users and connections from an authorized IP address or host.
E. Client Authentication is not restricted to a limited set of protocols.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 56
You are Security Administrator preparing to deploy a new hot-fix to ten Enforcement Modules at five geographically separated locations. What is the BEST method to implement this hot-fix?
A. Use SmartView installer to deploy the hot-fix to each Enforcement Module.
B. Use SmartInstaller to install the packages to each of the Enforcement Models remotely.
C. Send a CDROM with the hot-fix to each location, and have local personnel install it.
D. Use SmartUpdate to install the packages to each of the Enforcement Models remotely.
E. Send a Certified Security Engineer to each site to perform the update.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Your customer has created a rule so that every time a user wants to go to the Internet, that user must be authenticated. Firewall load is a concern for the customer. Which authentication method does not result in any additional connections to the firewall?

A. Session
B. User
C. Client
D. Connection
E. None of the above.
Answer: A (LEAVE A REPLY)
Explanation: Session authentication does not result in any additional connection to the firewall, you can use one connection and use it for the rest of the session for any service, also remember that session authentication is controlled by the Session authentication agent. See the online product documentation for more info.
Incorrect Answers
B:User authentication needs additional connection because it manages a proxy for each service.
C:Client authentication also requires additional connection because you have to connect to the firewall with HTTP or Telnet and enable the service for your use through the gateway.
D:This is not a valid authentication method.
E:This answer is wrong because answer A is correct, session authentication doesn't need additional connections to the firewall.

NEW QUESTION: 58
The VPN-1/Firewall-1 NG User Interface consists of which of the following elements?
Answer:
Explanation: as stated in the Checkpoint Official Website, the User interface of the NG suite is composed of 3 components:
The Security Policy Editor (Where you create the rulebase entries).
The Visual Policy Editor (That let you see a graphical view of you Checkpoint Deployment).
The Object Tree (Where you can find the created objects of your Checkpoint implementation).
Incorrect Answers
B:Those are components of the infrastructure, not from the user interface.
C:The inspection module is not a part of the user interface, it's the part of code installed on the firewall that makes the actual inspection.
D:The security server is not part of the interface, and there is not such a thing like System GUI.
E:Those are components of the infrastructure, not of the Interface.

NEW QUESTION: 59
Anna is a security administrator setting up User Authentication for the first time. She has correctly configured her Authentication rule, but authentication still does not work. What is the Check Point recommended way to troubleshoot this issue?
A. Verify the properties of the user attempting authentication and the authentication method selected in the Authentication Properties of your firewall object.
B. Verify the firewall settings of your firewall object, and the properties for the user attempting encryption and authentication.

C. Verify the properties for the user attempting authentication and make sure that the file Stealth Authentication method is selected in the Authentication properties of both the peer gateway object and your firewall object.
D. Verify both Client and User Authentication, and the authentication method selected in the Authentication properties of your Firewall object.
E. Re-import Schema from the VPN-1/FireWall-1 NG installation CD.
Answer: (SHOW ANSWER)
Explanation: this is the best practice, you have to check both, the properties of the user, to see that the correct authentication has been selected & the settings are correct and also the authentication properties of the firewall object to see if that authentication method is enabled.
Incorrect Answers
B:we are not talking about encryption, only authentication, the question does not talk about a user performing encryption of traffic through any rule.
C:this is wrong because this option is not mandatory to achieve a successful authentication process.
D:You don't have to check client authentication, the question clearly talks only about user authentication.
E:this is not an available option for this issue.

NEW QUESTION: 60
What Blocking Scope options are available when using Block Intruder? Choose three.
A. Block access from this Source.
B. Block source and destination
C. Block all traffic
D. Block only this connection
E. Block access to this Destination.
Answer: (SHOW ANSWER)

NEW QUESTION: 61
If the security policy is enforced by more than two firewalls how many rule bases would you need?
A. Only one rule base.
B. One rule base each for each number of network objects there
C. Two rule bases.
D. Three rule bases.
E. No rule base is needed to implement your security policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
CORRECT TEXT
Which of the following statements is TRUE concerning how NG with Application Intelligence handles the authentication of users?
Answer:
Pending

NEW QUESTION: 63
CORRECT TEXT
Which of the following is NOT included in SVN Foundation?
Answer:
Pending

NEW QUESTION: 64
CORRECT TEXT
You are the Security Administrator with one SmartCenter Server managing one Enforcement Module. SmartView Status displays a computer icon with an "?" in the Status column.
What does this mean?
Answer:
Pending

NEW QUESTION: 65
You are a Security Administrator preparing to implement an address translation solution for Certpaper.com.
The solution you choose must meet the following requirements:
Which address translation solution BEST meets your requirements?
A. The requirements cannot be met with any address translation solution.
B. Hide NAT
C. IP Pool Nat
D. Static NAT
E. Dynamic NAT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
The only way to unblock BLOCKED connections by deleting all the blocking rules from the Rule base.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: you don't have blocking rules inside your rulebase, all your blocking actions are made from "Block intruder" dialog box" at the active connection monitor in the log viewer. To unlock connection youcould unload the firewall module (fwstop command) or remove it manual, this is done without modifying the existing rulebase in policy editor. See page 108 from book "Essential Checkpoint Firewall 1".
Incorrect Answers
A:You don't have to modify the current rulebase from the policy editor. You take you unblocking action unloading the firewall or unblocking the connections manually. See explanation above for more information.

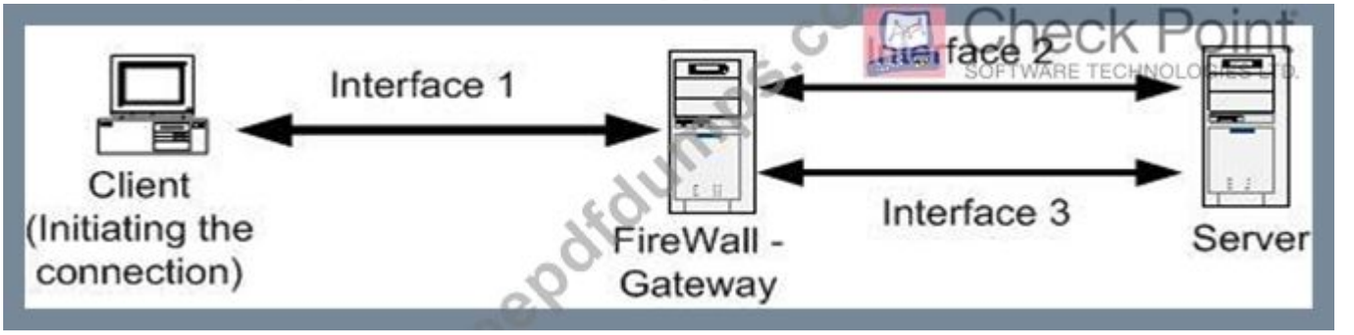
NEW QUESTION: 67
The following rule base tells you any automatically created NAT rules have simply hidden but have not been deleted from the Rule Base.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: its difficult to explain without the exhibit, but the answer is B, the statement exposed in the question is not true, its false. The NAT rules are not simply hidden.
Incorrect AnswersA:This answer is wrong because the NAT rules aren't simply hidden, is hard to explain without the exhibit.

NEW QUESTION: 68
What function does the Active mode of SmartView Tracker perform?
A. It displays current active connections traversing Enforcement Modules.
B. It displays only current connections between VPN-1/FireWall-1 modules.
C. It displays the active Security Policy.
D. It displays active Security Administrators currently logged into a SmartCenter Server.
E. It displays the current log file, as it is stored on a SmartCenter Server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
Assume there has been no change made to default policy properties. To allow a telnet connection into your network, you must create two rules.
One to allow the initial Telnet connection in.
One to allow the destination machine to send information back to the client.

A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: by default, in the case of Telnet (Port TCP 23) you only need one rule allowing the traffic from the inside or from the outside of the firewall, any reply to that Telnet connection request will be allowed by the firewall because of the connection tracker database located at the gateway. This behavior can be configured to work in a different fashion depending on the implementation requirements.
Incorrect Answers
A:You don't need 2 rules for a Telnet request and a Telnet reply because if the connection is allowed with the first rule through the gateway, the reply is expected in connection tracker database inside the gateway.

NEW QUESTION: 70
A connection initiated by the client in the figure below will be hidden behind the IP address of the interface through which the connection was routed on the server side if the gateway (behind either interface 2 or interface 3). Specifying 0.0.0.0 as the address is convenient because of network address translation (NAT) is performed dynamically. And if the IP addresses of the gateway are changed, it is not necessary to reconfigure the NAT parameters.
Which of the following is true about the following figure?



A. A connection initiated by the client will be hidden behind the IP address of the exit interface.
B. A connection initiated by the server will be hidden behind the IP address of the exit interface.
C. A connection initiated by the server will be hidden by the IP address of the client.
D. Source addresses of outbound packets from the client will be translated to 0.0.0.0.
E. Source addresses of outbound packets from the server will be translated to 0.0.0.0.
Answer: A (LEAVE A REPLY)
Explanation: making this actions, you will make the packets hide behind the exit interface, this is because of the address specified. Refer to Checkpoint Online Documentation to see how the whole process work.
Incorrect Answers
B:The connection needs to be iniciated by the client, not the server.
C:You can't hide the IP address of the server with the client one.
D:You can't translate a source address to 0.0.0.0.
E:You can't translate outbound packets in the server to a 0.0.0.0. address.

NEW QUESTION: 71
Which of the following statements BEST describes Dynamic Network Address Translation (Hide NAT)?
A. Translates private external IP addresses to public IP addresses.
B. Translates public internal IP addresses to private IP addresses.
C. Allow you to hide an entire network behind one IP address.
D. Allow you to hide an entire network behind random IP addresses.
E. Allows you to hide an entire network behind public IP addresses.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72

A. Data
B. Transport

C. Physical
D. Application
E. Network
Answer: E (LEAVE A REPLY)
Explanation: VPN1/FW1 resides on the top of layer 2 (DataLink) and below Network layer of the OSI model. In this place, the firewall engine can get all the packets before they get to the TCP/IP stack of the operating system, incrementing performance and improving security.
Incorrect Answers
A:VPN1/FW1 resides below the Network layer (3) of the OSI model.
B:VPN1/FW1 resides below the Network layer (3) of the OSI model.
C:VPN1/FW1 resides below the Network layer (3) of the OSI model.
D:VPN1/FW1 resides below the Network layer (3) of the OSI model.

NEW QUESTION: 73
When you make a rule, the rule is not enforces as part of your Security Policy.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: by default, any rule that you add to your rulebase for certain policy is enforced automatically once you push the updated policy to the enforcement modules from the management station. See "Basics of Security policy Administration" at the Checkpoint Official Courseware for CCSA.
Incorrect Answers
A:When you create a rule it is enforced as part of the security policy. See the explanation above for details.

NEW QUESTION: 74
If you configure the Minutes interval for a firewall in the User Authentication session timeout box, as shown below on the Authentication Tab of the Workstations properties window, users of one time password must re-authenticate for each request during this time period.
A. True
B. False
Answer: B (LEAVE A REPLY)
Explanation: this is the opposite, the time specified in the session time-out box will tell the firewall how much time the users with one time passwords can make request without re authenticating to the firewall.
Incorrect Answers
A:The session time-out specifies how much time should it pass until the firewall ask for re-authentication to the users of one time passwords during their requests.

NEW QUESTION: 75

CORRECT TEXT
When are Anti-Spoofing Rules enforced during packet inspection?
Answer:
Pending

NEW QUESTION: 76
The implicit-drop rule follows the principle "that which is not expressly permitted is _____"
A. Dropped
B. Moved
C. Rejected
D. Prohibited
E. Allowed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
Howa re Storm Center Block Lists activated? Choose the correction order.
A. 2, 1, 3
B. 1, 2, 3
C. 3, 2, 1
D. 3, 1, 2
E. 2, 3, 1
Answer: (SHOW ANSWER)

NEW QUESTION: 78
CORRECT TEXT
Which of the following statements are TRUE of VPN-1/FireWall-1 groups? (Choose two)
Answer:
Pending

NEW QUESTION: 79

Static Source NAT translates public internal source IP addresses to private external source IP addresses.

A. True

B. False.

Answer: B (LEAVE A REPLY)

Explanation: this statement is false because Static NAT translates "Private" Internal Source IP addresses to "Public" External Source IP addresses and not "Public" internal source IP addresses to "Private" external source IP addresses. Remember that our internal hosts don't have public addresses.

Incorrect Answers

A:Remember that we have Private Internal source IP's behind the gateway and Public external source IP's connected to the external network. (Example: Internet).

NEW QUESTION: 80

Changes made to the Security Policy do not take effect on the Enforcement Module until the administrator performs which of the following actions?

A. Saves the policy.

B. Verifies the policy.

C. Install the policy.

D. Stops firewall services on the Enforcement Module.

E. Stops firewall services on the Management module.

Answer: C (LEAVE A REPLY)

Explanation: If you make changes to your configuration / rulebase and you want them to be applied to your Firewall modules you have to install the updated policy (that contains the modified rulebase) from the Install Policy button at the Policy Editor. When you are installing the policy, the Management Server translates the configuration to Inspect code and then pushes it to the applicable firewalls at their Inspection engine.

Incorrect Answers

A:To make policy changes effective in the firewall modules you have to install it, when you save it, you are only storing the new definition, but not pushing it to the gateway modules for enforcement.

B:When you verify a policy you are only checking the syntax, the rule order and the objects, you are not enforcing the definition on the gateway modules.

D:The changes made to a policy are not enforced through the start or stop of the Firewall service in any of the components of the infrastructure.

E:The changes made to a policy are not enforced through the start or stop of the Firewall service in any of the components of the infrastructure.

NEW QUESTION: 81

CORRECT TEXT

Which of the following objects are allowed in the Source components of the Rule Base? (Choose two)

Answer:

Pending

NEW QUESTION: 82

In the Install On column of a rule, when you select a specific firewall object as the only configuration object, that rule is enforced on all firewalls with in the network, with related configurations.

A. True

B. False.

Answer: B (LEAVE A REPLY)

Explanation: when you select only one firewall object in the "install on field" of a rule, that rule is enforced only on that firewall object. In case there are other firewalls referred in the whole policy, they will have the complete policy installed (with all the rules in the rulebase), but they will not enforce the rules that are not relevant to them. See page 175 of Syngress Book "Checkpoint NG - Next Generation Security Administration".

Incorrect Answers

A:When you select only one firewall object on the "install on" field of a rule, that rule is enforced only in that firewall after the policy installation.

NEW QUESTION: 83

CORRECT TEXT

Which of the following is NOT a step in the Session Authentication process?

Answer:

Pending

NEW QUESTION: 84

You are attempting to implement Client Authentication for FTP. You have the accept firewall control connection option unchecked in the Policies and Properties dialog box.

In the following Rule base, which rule would prevent a user from performing Client Authentication?

No

SOURCE

DESTINATION

SERVICE

ACTION

1

Any

fw.chicago.com

Any

drop
2
AllUsers@Sales.net
Any
ftp
Client Encrypt
3
Any
localNet
http
telnet
Accept
4
Any
Any
Any
drop
A. Rule 1
B. Rule 2
C. Rule 3
D. Rule 4
Answer: A (LEAVE A REPLY)
Explanation: The client authentication will not be performed because rule 1 states that every packet that is destined to fw.chicago.com will be dropped (without creating a log entry) for any kind of traffic, the firewall will not accept any connection to it, therefore the authentication request will be dropped either at port 259 for Telnet or port 900 with HTTP.
Incorrect Answers
B:This rule provide the authentication.
C:This rule is not related to FTP.
D:This is the clean-up rule, perfectly correct at the end of the rule base.

NEW QUESTION: 85
CORRECT TEXT
With VPN-1/FireWall-1 central licensing, a license is linked to which of the following?
Answer:
Pending

NEW QUESTION: 86
When configuring Static NAT, you cannot map the routable IP address to the external IP address of the Firewall if attempted, the security policy installation fails with the following error "rule X conflicts with rule Y".

A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation: when you map a routable address with an external one, you will get the message "rule x conflicts with rule y" this is because of the behavior of the Checkpoint firewall suite in relation with the limitations of Static NAT, this behavior will make your policy verification and installation fail.
Incorrect Answers
B:As stated in the explanation above, you can't make this configuration because your policy verification will fail, and you will get the error message, this error makes this answer wrong.

NEW QUESTION: 87
What variable is used to extend the interval of the Timeout in a NAT to prevent a hidden UDP connection from losing its port?
Answer:
Explanation: if you want to prevent an UDP mapping from loosing its port you have the "Fwx_udp_time-out", you just need to extend the value, its in seconds, check the product online help .
Incorrect Answers
A:this is not a valid variable to achieve this objective.
B:this is not a valid variable to achieve this objective.
C:this is not a valid variable to achieve this objective.
E:this is not a valid variable to achieve this objective.

NEW QUESTION: 88
The system display status displays a firewall with "!". What does this mean?
A. The firewall is defined as external
B. The module is problematic
C. The firewall is unprotected, no security policy is loaded
D. Nothing is wrong
E. The firewall has been turned off
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
Selection and Explanation of UDP Packet Delivery Conditions?
A. A request.
B. A response to a request.
C. Source routed.
D. Allowed by the Rule Base.
E. Both B and D.
Answer: E (LEAVE A REPLY)

Explanation: when an UDP packets enters to the Inspect engine inside the firewall, the database that contains the pending connections is reviewed and the packet is delivered if its a reply to a request, we know this because there is an entry expecting the reply in the pending connections database, this is the first case. The second case that allows the deliver of the UDP packet is if it is allowed by the rulebase, for example, a rule that allows DNS Query traffic through port 53 UDP.
Incorrect Answers
A:A request cannot pass the firewall unless there is a rulebase permitting that service.
B:This is only part of the correct answer. This is only 1 of the 2 cases.
C:Source routed request are not allowed unless there is a rule permitting it.
D:This is only part of the correct answer. This is only 1 of the 2 cases.

NEW QUESTION: 90
For which of the following objectd types can Network Address Translation be configured?
A. Networks, OSE Devices logical servers.
B. Domains, host nodes, network.
C. Domains, networks, users
D. Host nodes, networks, address ranges
E. Host nodes, networks, OSE devices
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
CORRECT TEXT
Which of the following statements is specifically TRUE of user groups?
Answer:
Pending

NEW QUESTION: 92
User Authentication can be used to authenticate which services? (Select all that apply.)
Explanation: With Session Authentication you can authenticate 4 services: HTTP, FTP, Telnet and RLogin. See Page 282 of Syngress Book "Check Point NG - Next Generation Security Administration".
Incorrect Answers

B:HTTPS is not supported by user authentication. See Page 282 of Syngress Book "Check Point NG - Next Generation Security Administration".
QUESTION200
To block an active connection with Block Intruder, select the connection you want to block, and then select Block Intruder from the Select mune. The following default options are available from the Block Intruder window (Select all that apply.)
Answer:
B, C, EExplanation:the block intruder windows has 3 options available to block intruder connections, they are "Block only this source", "Block access to this source" and "Block access to this destination". See Page 376 of Syngress Book "Check Point NG - Next Generation Security Administration".
Incorrect AnswersA:This is not a valid option.
D:This is not a valid option.

NEW QUESTION: 93
New users are created from templates. What is the name of the standard template from which you would create a new user?
A. New
B. User
C. Group
D. Standard User.
E. Default
Answer: E (LEAVE A REPLY)
Explanation: this is the correct answer, when you create a new user its create by default from the "default" template. See checkpoint NG online documentation.
Incorrect AnswersA:This is not the name of the default template. See checkpoint NG online documentation.
B:This is not the name of the default template. See checkpoint NG online documentation.
C:This is not the name of the default template. See checkpoint NG online documentation.
D:This is not the name of the default template. See checkpoint NG online documentation.

NEW QUESTION: 94
Your customer has created a rule so that every user wants to go to Internet, that user must be authenticated. Which is the best method of authentication for users who must use specific computers for Internet access?
A. Session
B. User
C. Client
D. Connection
E. None of the above.
Answer: C (LEAVE A REPLY)

Explanation: Client authentication includes verification of the IP address of the client.
Access can be restricted to only specific client IP addresses.
Incorrect Answers
A:With Session authentication you can use any computer to connect if you have the session authentication agent installed in the PC.
B:User authentication allows you to connect from any PC, it doesn't have Ip checking capabilities to restrict the users to certain hosts.
D:This isn't one of the 3 authentication methods of the Checkpoint NG Suite.
E:This answer is wrong because client authentication provide the functionality required.

NEW QUESTION: 95
CORRECT TEXT
When the Client Authentication method requires Manual Sign On, users must connect to which of the following ports?
Answer:
Pending

NEW QUESTION: 96
CORRECT TEXT
Which of the following is NOT configured under Application Intelligence in SmartDefense?
Answer:
Pending

NEW QUESTION: 97
Fully Automatic Client authentication provides authentication for all protocols, whether supported by these protocols or not.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation: when we are using client authentication with all the setting for fully automatic authentication, you can authenticate all the protocols, it doesn't matters if the protocol supports authentication. See the Client Authentication features in the Secure knowledge base of Checkpoint for more information.
Incorrect AnswersB:You can authenticate all the protocol whatever or not they support authentication, remember, this is client authentication.

NEW QUESTION: 98
How is the Block Intruder request used?
A. It blocks access from a Source, or to a Destination, for a specified amount of time, or indefinitely.
B. It is used in the Log mode of SmartView Tracker to kill active connections.

C. It is activated in SmartDashboard through the Security Policy.
D. It is used in place of the HTTP Security Server.
E. SmartDefense automatically uses this capability.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
What two services or protocols can Client Authentication uses to initiate connection to the firewall? (Select two.)
A. HTTP and TCP
B. TELNET and RPC
C. HTTP and UDP
D. TELNET and HTTP
E. HTTP and HTTPS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 100
VPN-1/Firewall-1 NG differs from Packet filtering and Application Layer Gateways, because?
A. VPN-1/Firewall-1 NG provides only minimal logging and altering mechanism.
B. VPN-1/Firewal-1 NG uses Stateful inspection which allows packet to be examined at the top of the layers of the OSI model.
C. VPN-1/Firewall-1 NG has access to a limited part of the packet header only.
D. VPN-1/Firewall-1NG requires a connection from a client to a firewall and firewall to a server.
E. VPN-1/Firewall-1 NG has access to packets passing through key locations in a network.
Answer: B (LEAVE A REPLY)
Explanation: this is the main difference between the listed firewall technologies, the statefull inspection, because with it, we can see the packet before it goes to the Layer 3 of the OSI model (Network Layer = O.S TCP/IP Protocol Stack), this technology has the most access to the TCP/IP packet including the top layers.
Incorrect Answers
A:This is configurable and is not a difference between the listed firewall technologies.
C:VPN1/Firewall 1 has full access to the packet headers.
D:This is not a difference.
E:All firewall technologies has access to the network, you define what are your key locations inside it, then, you put the firewall to make that "key locations" pass the traffic through it.

NEW QUESTION: 101
In a distributed management environment, the firewall administrator has removed the default check from Accept VPN-1/Firewall-1 control connections under the Security Policy tab of the properties setup dialogue box. In order for the management module and the Firewall to communicate, you must create a rule to allow the Management Module to communicate to the firewall on which port?

A. 80
B. 256
C. 259
D. 900
E. 23
Answer: B (LEAVE A REPLY)
Explanation: the port 256 is used by the management station to push the policies to the enforcement modules, therefore it provides communication between the firewall and the management module. See the official CCSA courseware. Appendix C.4.
Incorrect Answers
A:The communication does not take place through the standard HTTP port.
C:This port is used for client authentication through Telnet.
D:This port is used for client authentication trough HTTP.
E:This is the default port for Telnet.

NEW QUESTION: 102
Within the Secure Internal Communications (SIC) framework the Management Server and Modules are identified by their SIC name. What is this commonly known as?
Answer:
Explanation: The management server and the modules are identified by their SIC name, also known as Distinguished Name (DN). See Page 1.22 of the official CCSA NG Courseware - Management 1.
Incorrect Answers
A:The Checkpoint products are not recognized internally by SIC with their IP address, their are recognized with a DN (Distinguished Name).
B:The Checkpoint products are not recognized internally by SIC with their Hosts name, their are recognized with a DN (Distinguished Name).
C:The Checkpoint products are not recognized internally by SIC with a custom name defined by the administrator, their are recognized with a DN (Distinguished Name).
E:The Checkpoint products are not recognized internally by SIC with the name of the machine, their are recognized with a DN (Distinguished Name).

NEW QUESTION: 103
SmartUpdate CANNOT be used to:
A. Uninstall Check Point and OPSEC software remotely, from a centralized location.
B. Remotely install NG with Application Intelligence for the first time, on a new machine.
C. Update installed Check Point and OPSEC software remotely, from a centralized location.
D. Manage licenses centrally.
E. Track installed versions of Check Point and OPSEC products.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
In order to install a new Security Policy on a remote firewall, what command must be issued on the remote firewall?
A. Fw unload all all.
B. Fw load new.
C. Cp clear policy.
D. None of the above, the command cp policy remove is issued from the manager.
E. None of the above, the new policy will automatically overwrite the existing policy.
Answer: E (LEAVE A REPLY)
Explanation: To install a new policy in a enforcement module you don't have to issue anything on it, you just need to select the install option in the policy editor and the management station will push the new policy as inspect code overwriting the actual policy being enforced at the remote firewall module.
Incorrect Answers
A:You don't need to unload the current policy to make a new one effective, is not necessary.
B:The policy is pushed from the management station in a transparent fashion on installation, you don't need to issue any additional command at the remote module.
C:You don't need to issue any command.
D:You doesn't need to use any "cp" command, the overwriting is automatic.

NEW QUESTION: 105
Which type of authentication will require users to TELNET to port 259 or connect via HTTP at port 900 to be authenticated for a service?
A. IP authentication
B. Client authentication
C. None
D. User authentication
E. Session authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 106
How does VPN-1/Firewall-1 NG implement Transparent authentication?
A. Unknown user receive error messages indicating that the firewalled gateway does not know the user names on the gateway.
B. VPN-1/Firewall-1 NG prompts for user names even through the authentication data may not be recognized by the firewall's user database.
C. VPN-1/Firewall-1 NG allows connections, but hides the firewall from authenticated users.
D. Unknown users error messages indicating that the host does not know the users names on the server.
E. VPN-1/Firewall-1 NG does not allow connections from users who do not know the name of the firewall.

Answer: C (LEAVE A REPLY)
Explanation: the concept of transparent authentication for Checkpoint Systems relies in making the Firewall authenticate the connections from the user, but make the user experience transparent, in other words, they don't know that the firewall is authenticating their connections.
Incorrect Answers
A:This is not the essence of transparent authentication, we will not get error messages, we will just not go through with our requests.
B:This authentication fashion does not prompt for user input, remember, this is "transparent" authentication.
D:This is not the way transparent authentication works, you can check the transparent authentication behavior at the Knowledge base of Checkpoint.
E:The user doesn't need to know the name of the firewall, it is usually configured by the administrator, the user doesn't need to know.

NEW QUESTION: 107
You Enterprise Security Policy is made up of what? (Select all that apply) Explanation: a security policy is the group of explicit and implicit rules created in the policy editor and pushed to the enforcement modules. The explicit rules are created by the administrator through manual definition and implicit rules are created automatically with the setting of the Global Properties in Policy Editor.
Answer:
Incorrect Answers
C:There is nothing else in a enterprise security policy.
D:There is nothing else in a enterprise security policy.

NEW QUESTION: 108
For most installations, the Clean-Up rule should be the last rule in Rule Base.
A. True
B. False
Answer: A (LEAVE A REPLY)
Explanation: this is an absolute truth for Checkpoint firewall implementations, since the cleanup rule drops all the traffic without making any logging, it should always be the last entry in the

rulebase because any packets that gets through or to the firewall is dropped at the inspection engine before getting to the Network layer at the OSI model.
Incorrect AnswersB:This is one of the basics, the clean up rule should always be the last rule in the rulebase of the installed policy.

NEW QUESTION: 109
You are a Security Administrator preparing to implement Hide NAT. You must justify your decision. Which of the following statements justifies implementing a Hide NAT solution? Choose two.
A. Your organization does not allow internal hosts to access Internet resources
B. Internally, your organization uses an RFC 1918-compliant addressing scheme.
C. You have more internal hosts than public IP addresses
D. Internally, you have more public IP addresses than hosts.
E. Your organization requires internal hosts, with RFC 1918-compliant addresses to be assessable from the Internet.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 110
In Windows NT to force log entries other than the default directory.
A. Modify the registry.
B. You must use thecpconfigcommand.
C. Change thefwlogenvironment variable.
D. Change the directory in log viewer.
E. Use the fw log switch command.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
What NAT mode is necessary if you want to start an HTTP session on a Reserved or Illegal IP address?
A. Static Source
B. Dynamic Source
C. Static Destination
D. None of the above
E. Dynamic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following user actions would you insert as an INTERNAL
Authentication scheme?
A. The user enters the security dynamics passcode.
B. The user prompted for a response from the RADIUS server.

C. The user prompted for a response from the AXENT server.
D. The user prompted for a response from the TACACS server.
E. The user enters an operating system account password.
Answer: E (LEAVE A REPLY)
Explanation: this is the only correct answer, since we are talking about "Internal" authentication scheme, the only valid answer is the Operating System authentication because the authentication occurs locally to the user.
Incorrect Answers
A:When we talk about dynamic passwords we often talk about an external security server changing the access password in a continuos basis, the user usually see the current password with the help of a hardware Token, an example is RSA.
B:Radius is an external security server, the authentication is checked remotely.
C:AXENT is an external security server, the authentication is checked remotely.
D:TACACS is an external security server, the authentication is checked remotely.

NEW QUESTION: 113
The _____ maintains the VPN-1/Firewall-1 NG database. The database includes network object definitions, user definitions, security policy, and the log files.
A. None of the above
B. Client Module
C. Management Server
D. Firewall Module
E. Server Module
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
Why would you want to verify a Security Policy before installation?
A. To install Security Policy cleanly.
B. To check up the enforcement-point firewall for errors.
C. To identify conflicting rules in your Security Policy.
D. To compress the Rule Base for faster installation
E. There us no benefit verifying a Security Policy before installing it.
Answer: C (LEAVE A REPLY)
Explanation: one of the uses of the "Verify Policy" command is that it can check if two or more rules conflict with another one. For example if you have a cleanup rule as the first in the rule base it will deny access of the traffic to any other criteria below.
Incorrect Answers
A:This is not the primary purpose of the policy verification, the main purpose of the verification is to achieve functionality and correct syntax and conflicting rules.
B:When you verify a policy you are making it at the management server, not at the enforcement modules.

D:In policy verification there is not a compression procedure.
E:This is obviously wrong, it is always good to verify your policies, is one of the best practices recommended by Checkpoint engineers, see Checkpoint Policy deployment help at their web site.

NEW QUESTION: 115
The rules that you define in the Rule Base are known as _____ rules.
A. Implicit
B. Properties setup
C. Explicit
D. Cleanup
E. Stealth
Answer: C (LEAVE A REPLY)