WatchGuard.Essentials.v2023-05-01.q73

Exam Code:	Essentials
Exam Name:	Fireware Essentials Exam
Certification Provider:	WatchGuard
Free Question Number:	73
Version:	v2023-05-01
# of views:	1881
# of Questions views:	730
https://www.exam-tests.com/Essentials-exam/WatchGuard.Essentials.v2023-05-01.q73.html	

NEW QUESTION: 1
What settings must you device configuration file include for Gateway AntiVirus to protect users on your network? (Select two.)
A. Decrease the scan limits
B. Configure Gateway AntiVirus settings for a proxy action.
C. Install the Gateway AntiVirus server on your network.
D. Disable automatic signature updates.
E. Configure a policy to use a proxy action that has AntiVirus settings configured.
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 2
When you configure the Global Application Control action, it is automatically applied to all policies.
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
Match each WatchGuard Subscription Service with its function.
Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware. (Choose one).
A. Reputation Enable Defense RED
B. Gateway / Antivirus
C. DataLoss Prevention DLP
D. Spam Blocker
E. WebBlocker
F. Intrusion Prevention Server IPS

G. Application Control
H. Quarantine Server
I. APT Blocker
Answer: I (LEAVE A REPLY)
APT Blocker is intended to stop malware and zero-day threats that are trying to invade anorganization's network.
APT Blocker uses a next-gen sandbox to get detailed views into the execution of a malware program. After first running through other security services, files are fingerprinted and checked against an existing database - first on theappliance and then in the cloud. If the file has never been seen before, it is analyzed using the system emulator, which monitors the execution of all instructions. It can spot the evasion techniques that other sandboxes miss.
Reference:http://www.watchguard.com/wgrd-products/security-modules/apt-blocker

NEW QUESTION: 4
Which tool can add an IP address for the Firebox to permanently block? (Select one)
A. FireBox System Manager - Blocked Sites list
B. Log Server
C. FireWatch
D. Firebox System Manager - Subscription services
E. Firebox System Manager - Authentication list
F. Traffic Monitor
Answer: E (LEAVE A REPLY)
Block a site permanently
The Successful Company networkadministrator has been driven to distraction recently by a script kiddy using addresses in the 192.136.15.0/24 network to run probes of the Successful network. In this exercise, we permanently block all connections from that network.
1.From PolicyManager, select Setup > Default Threat Protection > Blocked Sites. The Blocked Sites Configuration dialog box opens.
2.On the Blocked Sites tab, click Add.
3.The Add Site dialog box opens. 3. Use the Choose Type drop-down list to select Network IP. In the Value text box, type 192.136.15.0/ 24.
4. Click OK.
The entry appears in the Blocked Sites list. With this configuration, the Firebox blocks all packets to and from the 192.136.15.0/24 network range.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

NEW QUESTION: 5
You need to create an HTTP-proxy policy to a specific domain for software updates (example.com). The update site has multiple subdomains and dynamic IP addresses on a content

delivery network. Which of these options is the best way to define the destination in your HTTP-proxy policy? (Select one.)
A. Configure an FQDN for *.example.com.
B. Add IP addresses that correspond to each software update server in the domain.
C. Configure a host name for update.example.com.
D. Create an alias for all subdomains and known IP addresses for example.com.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
If you disable the Outgoing policy, which policies must you add to allow trusted users to connect to commonly used websites? (Select three.)
A. HTTP port 80
B. NAT policy
C. FTP port 21
D. HTTPS port 443
E. DNS port 53
Answer: A,D,E (LEAVE A REPLY)
Explanation/Reference:
TCP-UDP packet filter
If you decide to remove the Outgoing policy, you must add a policy for any type of traffic you want to allow through the Firebox. If you remove the Outgoing policy and then decide you want to allow all TCP and UDP connections through the Firebox again, you must add the TCP-UDP packet filter to provide the same function. This is because the Outgoing policy does not appear in the list of standard policies available from Policy Manager.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 97

NEW QUESTION: 7
Which takes precedence: WebBlocker category match or a WebBlocker exception?
A. WebBlocker category match
B. WebBlocker exception
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
You can use Firebox-DB authentication with any type of Mobile VPN.
A. True
B. False
Answer: (SHOW ANSWER)
http://www.watchguard.com/help/docs/fireware/11/en-US/Content/en-US/mvpn/general/mobile_vpn_types_c.html

NEW QUESTION: 9

Which tool is used to see a treemap visualization of the traffic through your Firebox? (Select one)

A. FireBox SystemManager - Blocked Sites list

B. Log Server

C. FireWatch

D. Firebox System Manager - Subscription services

E. Firebox System Manager - Authentication list

F. Traffic Monitor

Answer: (SHOW ANSWER)

The FireWatch page is separated into tabs of data that is presented in aTreemap Visualization. The treemap is a widget that proportionally sizes blocks in the display to represent the data for that tab. The largest blocks on the tab represent the largest data users. The data is sorted by the tab you select and the type you select from the drop-down list at the top right of the page.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

NEW QUESTION: 10

You can use Firebox System Manager to download a PCAP file that includes packet information about the protocols that manage traffic on your network.

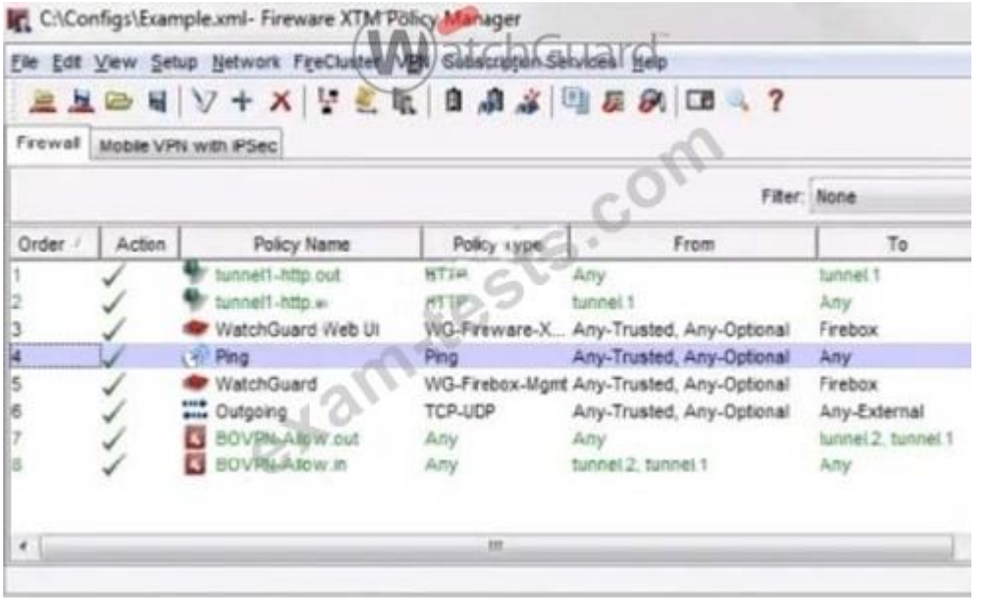
A. False

B. True

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

With the policies configured as shown in this image, HTTP traffic can be sent and received through branch office VPN tunnel.1 and tunnel.2.



A. True

B. False

Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
Match the monitoring tool to the correct task.
Which is not a Fireware monitoring tool? (Select one)
A. FireBox System Manager - Blocked Sites list
B. Log Server
C. FireWatch
D. Firebox System Manager - Subscription services
E. Firebox System Manager - Authentication list
F. Traffic Monitor
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The Fireware monitor and configuration tools are: Edge Web Manager, Firebox System Manager, HostWatch, and Ping.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

NEW QUESTION: 13
Match each WatchGuard Subscription Service with its function.
Controls access to website based on content categories. . (Choose one).
A. Reputation Enable Defense RED
B. Gateway / Antivirus
C. WebBlocker
D. Intrusion Prevention Server IPS
E. Application Control
F. Explanation:
WebBlocker controls access to the good and bad places that are reachable on the web,preventing users from gaining access to sites that have evil intentions.
If you configure WebBlocker to use the Websense cloud for WebBlocker lookups, WebBlocker uses the Websense content categories. A web site is added to a category when the content of the web site meets the criteria for the content category.
Reference:http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html
QUESTIONNO: 74
Match each type of NAT with the correct description:
Allows a user on the trusted or optional network to connect to a public server that is on the same physical Firebox interface by its public IP address or domain name. (Choose one)
A. 1-to1 NAT
B. Dynamic NAT
C. NAT Loopback
Answer: C (LEAVE A REPLY)

NAT loopback allows a user on the trusted or optional networks to get access to a public server that is on the same physical Firebox or XTM device interface by its public IP address or domain name.
Reference:http://www.watchguard.com/help/docs/wsm/11/en-US/index_Left.html#CSHID=en-US%2Fnat%2Fnat_loopback_c.html|StartTopic=Content%2FenUS%2Fnat%2Fnat_loopback_c.html

NEW QUESTION: 14
Match the monitoring tool to the correct task.
Which tool can learn the status of your IPS signature database? (Select one)
A. FireBox System Manager - Blocked Sites list
B. Log Server
C. FireWatch
D. Firebox System Manager - Subscription services
E. Firebox System Manager - Authentication list
F. Traffic Monitor
Answer: D (LEAVE A REPLY)
Explanation/Reference:
To look up information about an IPS signature:
1. Open Firebox System Manager.
2. Select the Subscription Services tab.
3. In the Intrusion Prevention section, click Show.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

NEW QUESTION: 15
Which WatchGuard Subscription Service must be enabled in a proxy policy before you can use APT Blocker? (Select one.)
A. IPS
B. RED
C. Gateway Antivirus
D. Application Control
E. WebBlocker
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of these options must you configure in an HTTPS-proxy policy to detect credit card numbers in HTTP traffic that is encrypted with SSL? (Select two.)
A. Data Loss Prevention
B. Gateway AntiVirus
C. Application Control
D. Deep inspection of HTTPS content

E. WebBlocker
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
An email newsletter about sales from an external company is sometimes blocked by spamBlocker. What option could you choose to make sure the newsletter is delivered to your users? (Select one.)
A. Set the spamBlocker action to quarantine the email for later retrieval.
B. Add a spamBlocker subject tag for bulk email messages.
C. Set the spamBlocker virus outbreak detection action to allow emails from the newsletter source.
D. Add a spamBlocker exception based on the From field of the newsletter email.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 18
What is the best method to downgrade the version of Fireware OS on your Firebox without losing all device configuration settings? (Select one.)
A. Change the OS compatibility setting in Policy Manager to downgrade the device. Then use Policy Manager to save the configuration to the device.
B. Use the downgrade feature on Policy Manager to select a previous of Fireware OS.
C. Use the Upgrade OS feature in Fireware Web UI to install the sysa_dl file for an order version of Fireware OS.
D. Restore a saved backup image that was created for the device before the last Fireware OS upgrade.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
With the policies configured as shown in this image, HTTP traffic can be sent and received through branch office VPN tunnel.1 and tunnel.2.

A. True

B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 20

Match the monitoring tool to the correct task.

Which tool can ping the source of a denied packet? (Select one)

A. FireBox System Manager - Blocked Sites list

B. Log Server

C. FireWatch

D. FireboxSystem Manager - Subscription services

E. Firebox System Manager - Authentication list

F. Traffic Monitor

Answer: F (LEAVE A REPLY)

For a quick look at the log messages generated by the Firebox, use Traffic Monitor. With Traffic Monitor, you can apply color to differenttypes of messages, and ping or traceroute to the IP addresses of computers included in the log messages.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

NEW QUESTION: 21

Which of these services would you use to allow the use of P2P programs for a specific department in your organization? (Select one.)

A. Application Control

B. Reputation Enabled Defense

C. Data Loss Prevention

D. IPS

Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
You can configure the SMTP-proxy policy to restrict email messages and email content based on which of these message characteristics? (Select four.)
A. Email message size
B. Maximum email recipients
C. Check URLs in message with WebBlocker
D. Sender Mail From address
E. Attachment file name and content type
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 23
How can you include log messages from more than one Firebox in a single report generated by Dimension? (Select two.)
A. Create a report schedule that includes all the devices you want to include in the report.
B. Export report data as a single PDF file for all the devices you want to include in the report.
C. You cannot see report data in Dimension for more than one device.
D. Create a device group and view the reports for that group.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 24
The policies in a default Firebox configuration do not allow outgoing traffic from optional interfaces.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
You have a privately addressed email server behind your Firebox. If you want to make sure that all traffic from this server to the Internet appears to come from the public IP address 203.0.113.25, regardless of policies, which from of NAT would you use? (Select one.)
A. In the SMTP policy that handles traffic from the email server, select the option to apply dynamic NAT to all traffic in the policy and set the source IP address203.0.113.25.
B. Create a static NAT action for traffic to the email server, and set the source IP address to 203.0.113.25.
C. Create a global dynamic NAT rule for traffic from the email server and set the source IP address to
203.0.113.25.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
While troubleshooting a branch office VPN tunnel, you see this log message:
2 014-07-23 12:29:15 iked (203.0.113.10<->203.0.113.20) Peer proposes phase one encryption 3DES, expecting AES
What settings could you modify in the local device configuration to resolve this issue? (Select one.)
A. BOVPN Gateway settings
B. BOVPN-Allow policies
C. BOVPN Tunnel settings
D. BOVPN Tunnel Route settings
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The WatchGuard BOVPN settings error in this example states phase one encryption. Only the BOVPN Gateway settings can specify phase one settings. BOVPN Tunnel settings specify phase 2 settings.

NEW QUESTION: 27
Match each WatchGuard Subscription Service with its function.
Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware. (Choose one).
A. Reputation Enable Defense RED
B. Gateway / Antivirus
C. Data Loss Prevention DLP
D. Spam Blocker
E. WebBlocker
F. Intrusion Prevention Server IPS
G. Application Control
H. Quarantine Server
I. APT Blocker
Answer: I (LEAVE A REPLY)
Explanation/Reference:
APT Blocker is intended to stop malware and zero-day threats that are trying to invade an organization's network.
APT Blocker uses a next-gen sandbox to get detailed views into the execution of a malware program. After first running through other security services, files are fingerprinted and checked against an existing database - first on the appliance and then in the cloud. If the file has never been seen before, it is analyzed using the system emulator, which monitors the execution of all instructions. It can spot the evasion techniques that other sandboxes miss.
Reference: http://www.watchguard.com/wgrd-products/security-modules/apt-blocker

NEW QUESTION: 28

Which takes precedence: WebBlocker category match or a WebBlocker exception?
A. WebBlocker category match
B. WebBlocker exception
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Your company denies downloads of executable files from all websites. What can you do to allow users on the network to download executable files from the company's remote website? (Select one.)
A. Configure HTTP Request > URL Paths to allow the company's remote website.
B. Create a WebBlocker exception to allow access to the company's remote website.
C. Create an IPS exception.
D. Create a Blocked Sites exception.
E. Add an HTTP proxy exception for the company's remote website.
Answer: E (LEAVE A REPLY)

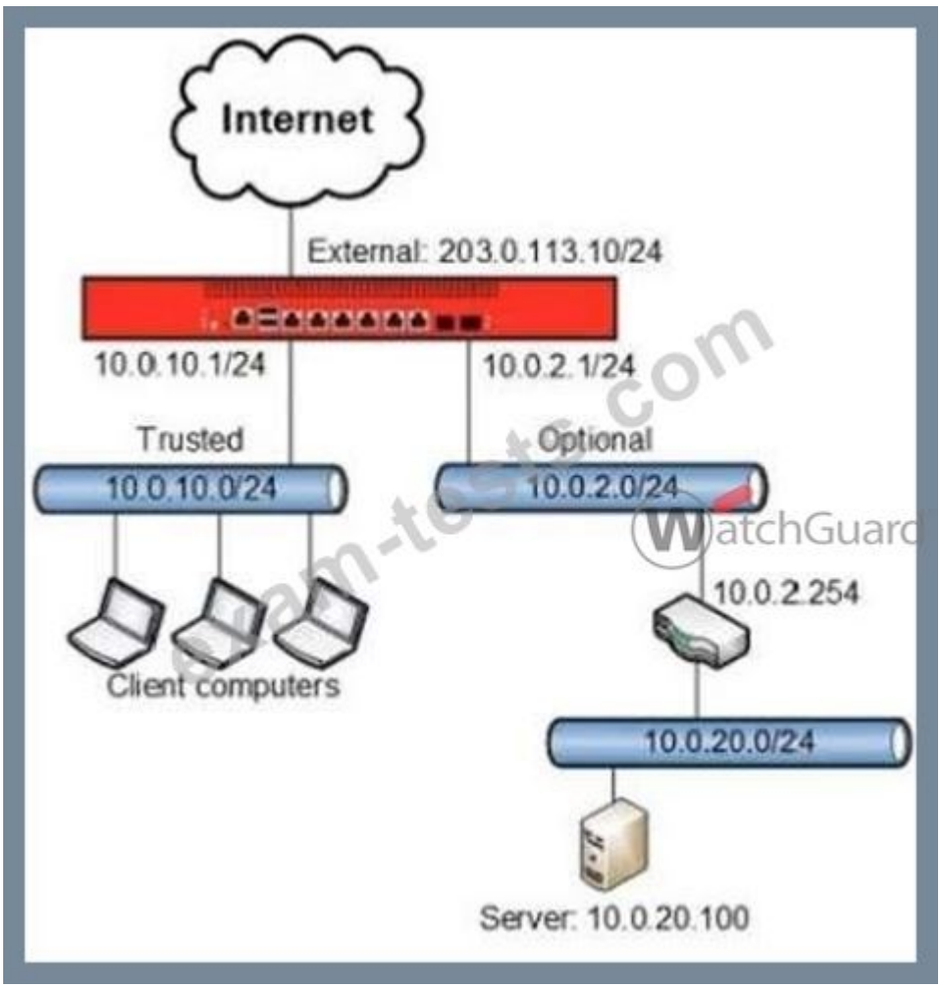
NEW QUESTION: 30
You can configure your Firebox to automatically redirect users to the Authentication Portal page.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
For which of these third party authentication methods must you specify a search base? (Select two.)
A. RADIUS
B. Active Directory
C. SecurID
D. LDAP
Answer: B,D (LEAVE A REPLY)
Explanation/Reference:
B: Configuring the Firebox to use Active Directory authentication is similar to the process for LDAP authentication. You must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.
D: When you configure the Firebox to use LDAP authentication, you must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 83-84

NEW QUESTION: 32
Which WatchGuard Subscription Service must be enabled in a proxy policy before you can use APT Blocker? (Select one.)
A. WebBlocker
B. Application Control
C. RED
D. Gateway Antivirus
E. IPS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
When your device is in a default state, to which interface do you connect your management computer so you can use the Quick Setup Wizard or Web Setup Wizard to configure the device? (Select one.)
A. Interface 0
B. Console interface
C. Any interface
D. Interface 1
Answer: D (LEAVE A REPLY)
Explanation/Reference:
To start the Web Setup Wizard, connect your computer to interface number 1 of your XTM device with an Ethernet cable. This is the trusted interface.
Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#en-US/installation/ qsw_web_about_c.html

NEW QUESTION: 34
Clients on the trusted network need to connect to a server behind a router on the optional network. Based on this image, what static route must be added to the Firebox for traffic from clients on the trusted network to reach a server at 10.0.20.100? (Select one.)

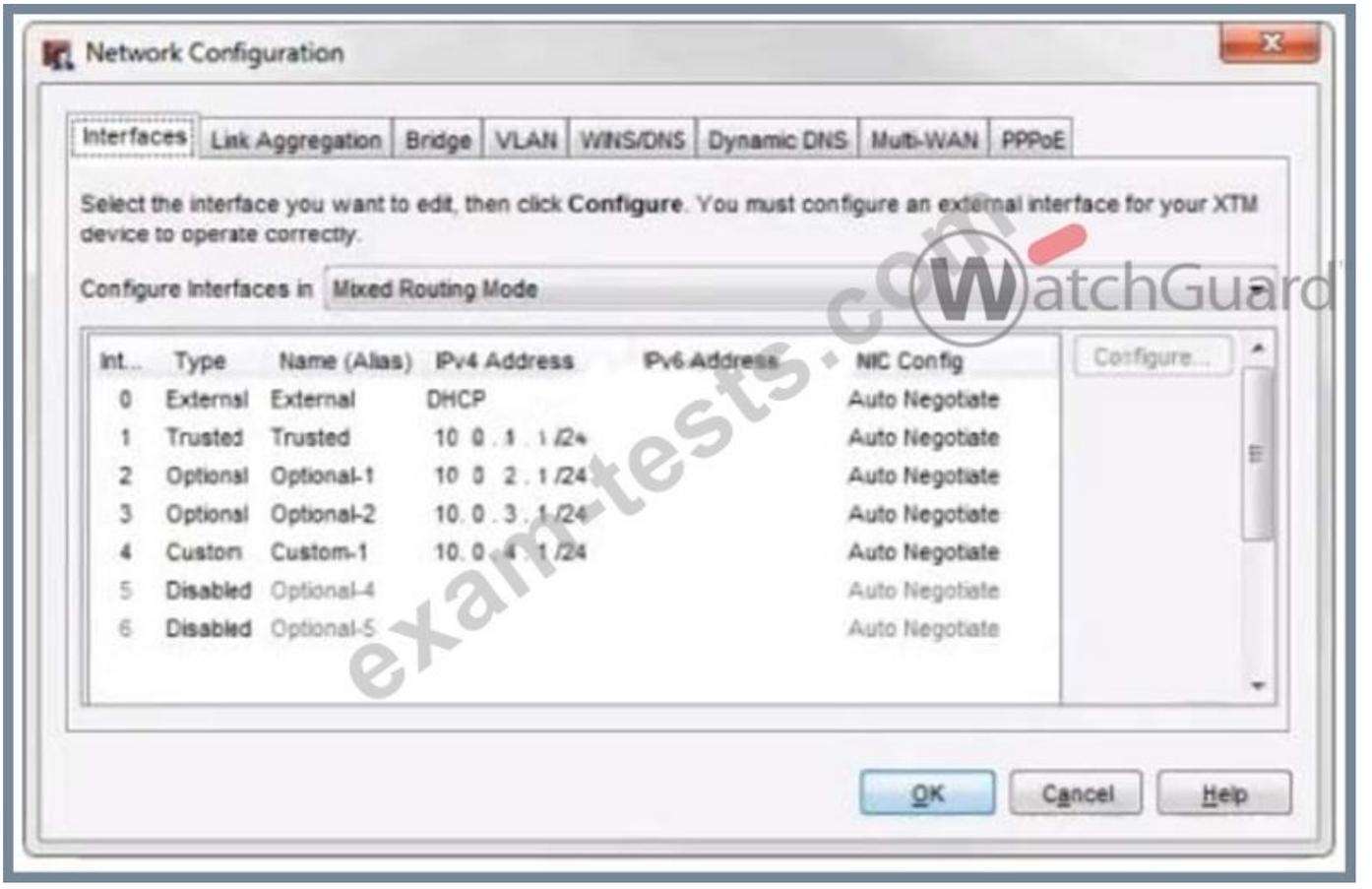


A. Route to 10.0.20.0/24, Gateway 10.0.2.1
B. Route to 10.0.20.0/24, Gateway 10.0.2.254
C. Route to 10.0.20.0, Gateway 10.0.2.254
D. Route to 10.0.10.0/24, Gateway 10.0.10.1
Answer: B (LEAVE A REPLY)
Explanation/Reference:
We must add a trusted static route to the 10.0.20.0/24 network through the 10.0.2.254 gateway.

NEW QUESTION: 35
After you enable spamBlocker, your users experience no reduction in the amount of spam they receive.
What could explain this? (Select three.)
A. Connections cannot be resolved to the spamBlocker servers because DNS is not configured on the Firebox.
B. The spamBlocker action for Confirmed Spam is set to Allow.
C. The Maximum File Size to Scan option is set too high.
D. A spamBlocker exception is configured to allow traffic from sender *.
E. spamBlocker Virus Outbreak Detection is not enabled.
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:

A: Spamblocker requires DNS to be configured on your XTM device
B: If you use spamBlocker with the POP3 proxy, you have only two actions to choose from: Add Subject Tag and Allow. Allow lets spam email messages go through the Firebox without a tag.
D: The Firebox might sometimes identify a message as spam when it is not spam. If you know the address of the sender, you can configure the Firebox with an exception that tells it not to examine messages from that source address or domain.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 138

NEW QUESTION: 36
In the network configuration in this image, which aliases is Eth2 a member of? (Select three.)



A. Optional-1
B. Any-Trusted
C. Any
D. Any-External
E. Any-optional
Answer: (SHOW ANSWER)

NEW QUESTION: 37
When your users connect to the Authentication Portal page to authenticate, they see a security warning message in their browses, which they must accept before they can authenticate. How can you make sure they do not see this security warning message in their browsers? (Select one.)

A. Import a custom self-signed certificate or a third-party certificate to your Firebox and import the same certificate to all client computers or web browsers.
B. Replace the Firebox certificate with the trusted certificate from your web server.
C. Add the user accounts for your users who use the Authentication Portal to a list of trusted users on your Firebox.
D. Instruct them to disable security warning message in their preferred browsers.
Answer: (SHOW ANSWER)
http://wwwwatchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/authentication/authentication_user_process_c.html

NEW QUESTION: 38
When you configure the Global Application Control action, it is automatically applied to all policies.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
After you enable spamBlocker, your users experience no reduction in the amount of spam they receive. What could explain this? (Select three.)
A. Connections cannot be resolved to the spamBlocker servers because DNS is not configured on the Firebox.
B. The spamBlocker action for Confirmed Spam is set to Allow.
C. A spamBlocker exception is configured to allow traffic from sender *.
D. The Maximum File Size to Scan option is set too high.
E. spamBlocker Virus Outbreak Detection is not enabled.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which diagnostic tasks can you run from the Traffic Monitor tab of Firebox System Manager? (Select four.)
A. DNS lookup
B. MAC address lookup
C. Traceroute
D. Reputation lookup
E. Ping
F. TCP dump
Answer: (SHOW ANSWER)
Explanation/Reference:
From Firebox System Manager, you can run diagnostic tasks to review information in all the log messages from your Firebox or XTM device. This can help you debug problems on your network.

1. On the Traffic Monitor tab, right-click a message and select Diagnostic Tasks.
Or, select Tools > Diagnostic Tasks.
2. From the Task drop-down list, select the task to run.
Ping IPv4
Ping IPv6
traceroute
DNS Lookup
TCP Dump
Reference: http://watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/fsm/log_message_learn_more_wsm.html

NEW QUESTION: 41
Which of these actions adds a host to the temporary or permanent blocked sites list? (Select three.)
A. Enable the AUTO-block sites that attempt to connect option in a deny policy.
B. Add the site to the Blocked Sites Exceptions list.
C. On the Firebox System Manager >Blocked Sites tab, select Add.
D. In Policy Manager, select Setup> Default Threat Protection > Blocked Sites and click Add.
Answer: (SHOW ANSWER)
Explanation/Reference:
A: You can configure a deny policy to automatically block sites that originate traffic that does not comply with the policy rulese
1. From Policy Manager, double-click the PCAnywhere policy.
2. Click the Properties tab. Select the Auto-block sites that attempt to connect checkbox.
Reference: https://www.watchguard.com/training/fireware/80/defense8.htm C: The blocked sites list shows all the sites currently blocked as a result of the rules defined in Policy Manager.
From this tab, you can add sites to the temporary blocked sites list, or remove temporary blocked sites.
Reference: http://www.watchguard.com/training/fireware/82/monitoa6.htm
D: You can use Policy Manager to permanently add sites to the Blocked Sites list.
1. select Setup > Default Threat Protection > Blocked Sites.
2. Click Add.
The Add Site dialog box appears.
Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#cshid=en-US/intrusionprevention/blocked_sites_permanent_c.html

NEW QUESTION: 42
HOTSPOT
Match each type of NAT with the correct description:

Conserves IP addresses and hides the internal topology of your network

Choose One
Choose One
1-to1 NAT
Dynamic NAT
NAT loopback

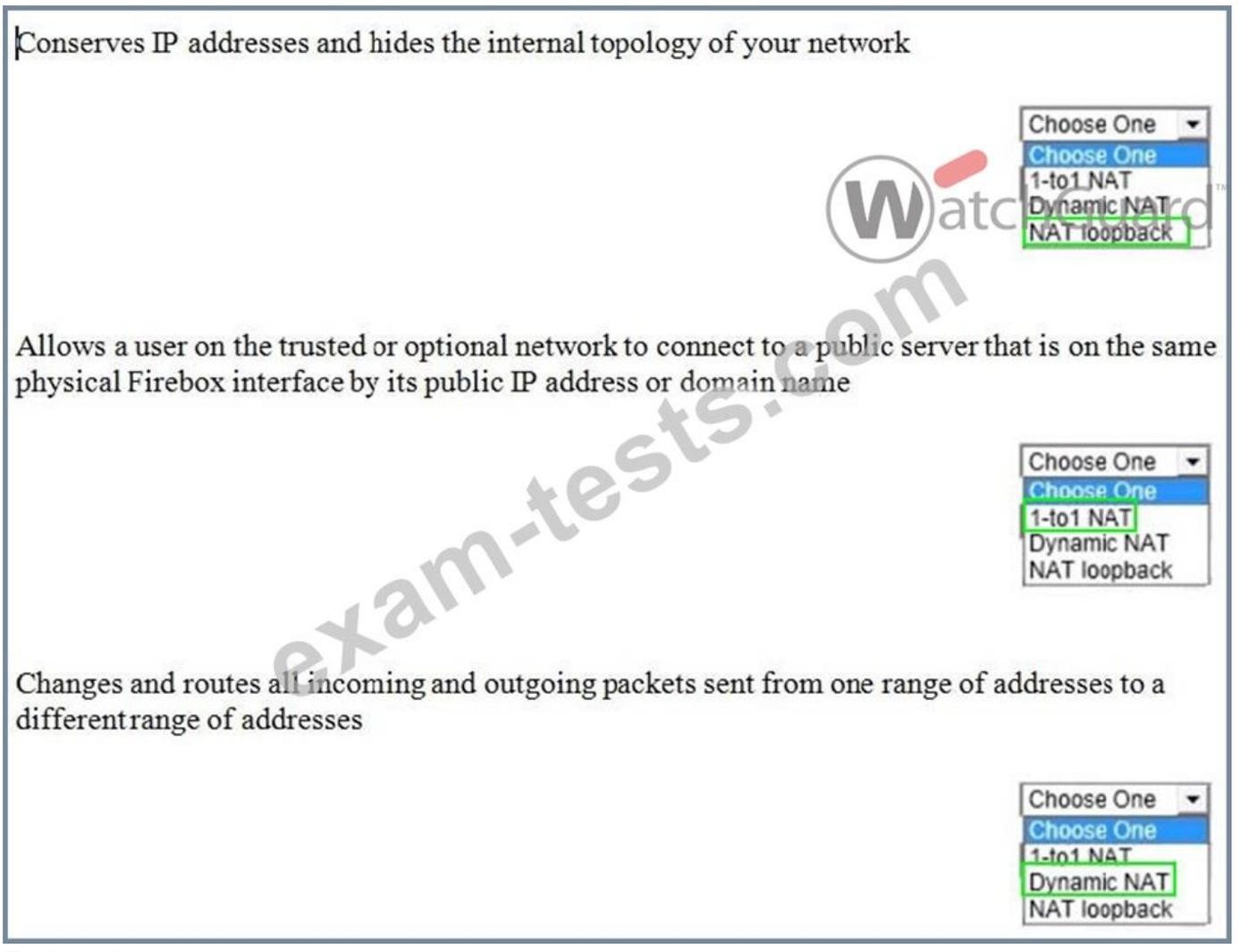
Allows a user on the trusted or optional network to connect to a public server that is on the same physical Firebox interface by its public IP address or domain name

Choose One
Choose One
1-to1 NAT
Dynamic NAT
NAT loopback

Changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses

Choose One
Choose One
1-to1 NAT
Dynamic NAT
NAT loopback

Answer:

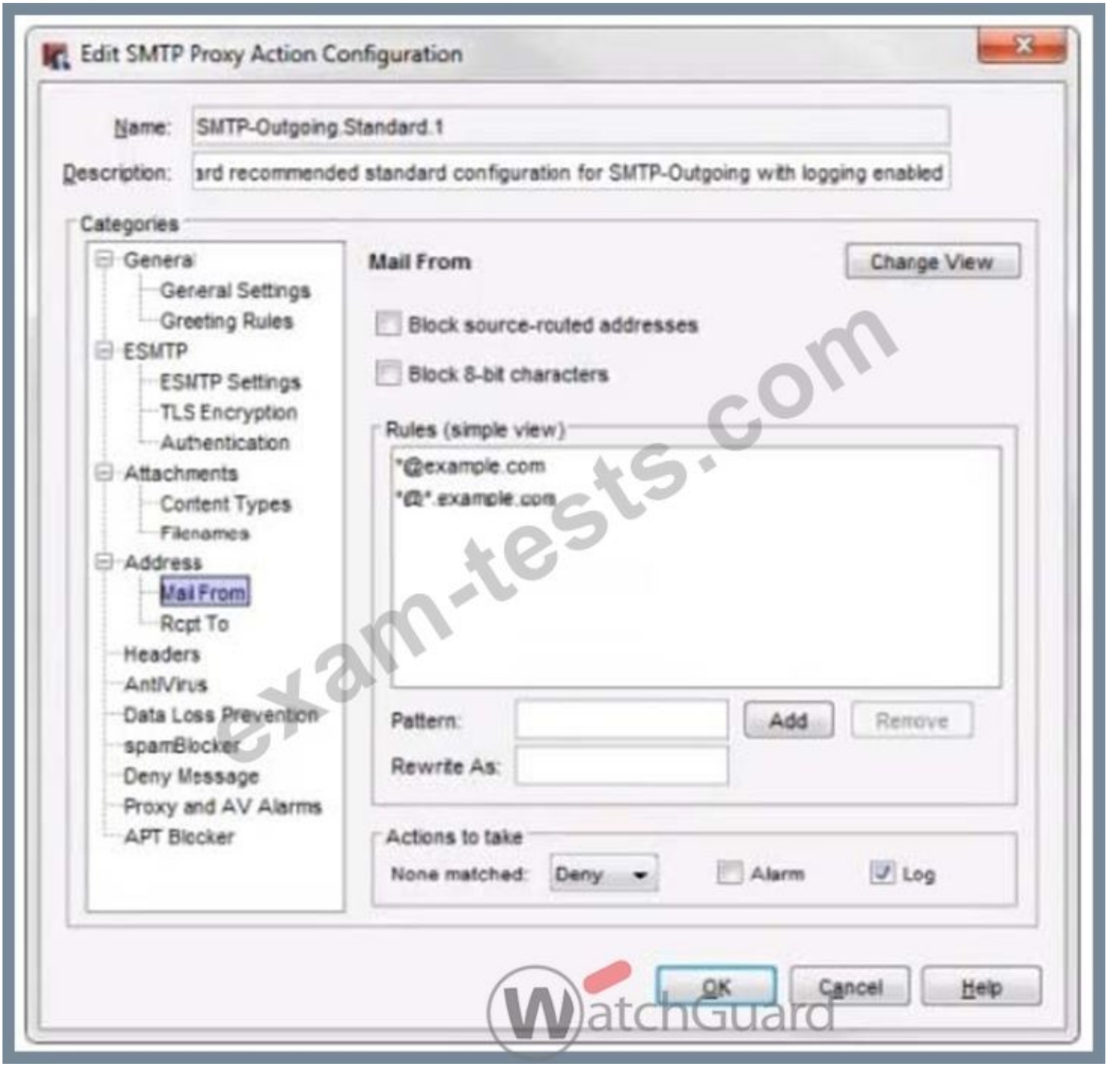


Explanation:
NAT Loopback 1-to 1 NAT
Dynamic NAT

NEW QUESTION: 43
What settings must you device configuration file include for Gateway AntiVirus to protect users on your network? (Select two.)
A. Configure a policy to use a proxy action that has AntiVirus settings configured.
B. Install the Gateway AntiVirus server on your network.
C. Configure Gateway AntiVirus settings for a proxy action.
D. Disable automatic signature updates.
E. Decrease the scan limits
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:
When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page download or upload post (HTTP proxy), or uploaded or downloaded file (FTP proxy). When Gateway AntiVirus is enabled, it scans

each file up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Reference: http://watchguard.com/help/docs/webui/xtm_11/en-us/content/en-us/services/gateway_av/ av_actions_config_c.html

NEW QUESTION: 44
From the SMTP proxy action settings in this image, which of these options is configured for outgoing SMTP traffic? (Select one.)



A. Prevent mail relay for theexample.comdomain.
B. Deny incoming mail from theexample.comdomain.
C. Deny outgoing mail from theexample.comdomain.
D. Rewrite theMail Fromheader for theexample.comdomain.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
When your device is in a default state, to which interface do you connect your management computer so you can use the Quick Setup Wizard or Web Setup Wizard to configure the device? (Select one.)
A. Interface 0
B. Console interface
C. Any interface
D. Interface 1
Answer: (SHOW ANSWER)
To start the Web Setup Wizard, connect your computer to interface number 1 of your XTMdevice with an Ethernet cable. This is the trusted interface.
Reference:http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#en-US/installation/qsw_web_about_c.html

NEW QUESTION: 46
Which diagnostic tasks can you run from the Traffic Monitor tab of Firebox System Manager? (Select four.)
A. DNSlookup
B. MAC address lookup
C. Traceroute
D. Reputation lookup
E. Ping
F. TCP dump
Answer: A,C,E,F (LEAVE A REPLY)
From Firebox System Manager, you can run diagnostic tasks to review information in all the log messages from your Firebox or XTM device. This can help you debug problems on your network.
1.On the Traffic Monitor tab, right-click a message and select Diagnostic Tasks. Or, select Tools > Diagnostic Tasks.
2.From the Task drop-down list, select the task to run. Ping IPv4 Ping IPv6 traceroute DNS Lookup TCP Dump
Reference:http://watchguard.com/help/docs/wsm/xtm_11/en-us/content/enus/fsm/log_message_learn_more_wsm.html

NEW QUESTION: 47
Match each type of NAT with the correct description:
Changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses. (Choose one)
A. 1-to1 NAT
B. Dynamic NAT
C. NAT Loopback
Answer: A (LEAVE A REPLY)
Explanation/Reference:
When you enable 1-to-1 NAT, the Firebox changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 74

NEW QUESTION: 48
If your Firebox has a single public IP address, and you want to forward inbound traffic to internal hosts based on the destination port, which type of NAT should you use? (Select one.)
A. Dynamic NAT
B. Static NAT
C. 1-to-1 NAT
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
Match each WatchGuard Subscription Service with its function.
Uses rules, pattern matching, and sender reputation to block unwanted email messages. (Choose one).
A. Reputation Enable Defense RED
B. Gateway / Antivirus
C. Spam Blocker
D. Intrusion Prevention Server IPS
E. APT Blocker
Answer: (SHOW ANSWER)
Explanation/Reference:
SpamBlocker provides a spam scanning engine that works in concert with WatchGuard's cloud-based technology to prevent spam from gaining access to the email servers (and clients).
Reference: http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html

NEW QUESTION: 50

Which of these options must you configure in an HTTPS-proxy policy to detect credit card numbers in HTTP traffic that is encrypted with SSL? (Select two.)

A. Deep inspection of HTTPS content

B. WebBlocker

C. Gateway AntiVirus

D. Data Loss Prevention

E. Application Control

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 51

Which of these options are private IPv4 addresses you can assign to a trusted interface, as described in RFC 1918, Address Allocation for Private Internets? (Select three.)

A. 198.51.100.1/24

B. 192.0.2.1/24

C. 192.168.50.1/24

D. 10.50.1.1/16

E. 172.16.0.1/16

Answer: (SHOW ANSWER)

NEW QUESTION: 52

HOTSPOT

Match the monitoring tool to the correct task:

Not a Fireware monitoring tool

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

See a treemap visualization of the traffic through your Firebox

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

Add an IP address for the Firebox to permanently block

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

Ping the source of a denied packet

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

Learn the status of your IPS signature database

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

View a list of users connected to the Firebox

Choose One
Choose One
Firebox System Manager - Blocked Sites List
Log Server
FireWatch
Firebox System Manager - Subscription Services
Firebox System Manager - Authentication List
Traffic Monitor

Answer:

Not a Fireware monitoring tool

See a treemap visualization of the traffic through your Firebox

Add an IP address for the Firebox to permanently block

Ping the source of a denied packet

Learn the status of your IPS signature database

View a list of users connected to the Firebox

Explanation:

Firewatch Traffic Monitor Firebox system Manager - Authentication List Log Server Firbox System Manager - Blocked State List Firebox System Manager - Subscription Services

NEW QUESTION: 53
Which policies can use the Intrusion Prevention Service to block network attacks? (Select one?)
A. Only packet filter policies
B. Only HTTP and HTTPS Proxy policies
C. Only proxy policies
D. Only inbound policies
E. All policies
Answer: E (LEAVE A REPLY)

NEW QUESTION: 54
An email newsletter about sales from an external company is sometimes blocked by spamBlocker. What option could you choose to make sure the newsletter is delivered to your users? (Select one.)
A. Add a spamBlocker subject tag for bulk email messages.
B. Add a spamBlocker exception based on the From field of the newsletter email.
C. Set the spamBlocker virus outbreak detection action to allow emails from the newsletter source.
D. Set the spamBlocker action to quarantine the email for later retrieval.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
Match the monitoring tool to the correct task.
Which is not a Fireware monitoring tool? (Select one)
A. FireBox System Manager - Blocked Sites list
B. Log Server
C. FireWatch
D. Firebox System Manager - Subscription services
E. Firebox System Manager - Authentication list
F. Traffic Monitor
Answer: B (LEAVE A REPLY)
The Fireware monitor and configuration tools are: Edge Web Manager, Firebox System Manager, HostWatch, and Ping.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59,

NEW QUESTION: 56
Users on the trusted network cannot browse Internet websites. Based on the configuration shown in this image, what could be the problem with this policy configuration? (Select one.)

Order	Action	Policy Name	Policy Type	From	To	Port
1	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
2	✓	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:80
3	✓	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Optional	Any-External	tcp:443
4	✓	WatchGuard Authenti...	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
5	✓	WatchGuard Web UI	WG-Fireware-X...	Any-Trusted, Any-Optional	Firebox	tcp:8080
6	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	ICMP (type: 8, code: 255)
7	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:41...

A. The default Outgoingpolicy has been removed and there is no policy to allow DNS traffic.
B. The HTTP-proxy policy has higher precedence than the HTTPS-proxy policy.
C. The HTTP-proxy policy is configured for the wrong port.
D. The HTTP-proxy allows Any-Trusted and Any-Optional to Any-External.
Answer: (SHOW ANSWER)
http://www.watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/policies/policy_outgoing_about_c.html
http://www.watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/proxies/http/http_proxy_about_chtml

NEW QUESTION: 57
The IP address for the trusted interface on your Firebox is 10.0.40.1/24, but you want to change the IP address for this interface. How can you avoid a network outage for clients on the trusted network when you change the interface IP address to 10.0.50.1/24? (Select one.)
A. Add IP addresses on the 10.0.40.0/24 subnet to the DHCP Server IP address pool for this interface.
B. Add 10.0.40.1/24 as a secondary IP address for the interface.
C. Add a route to 10.0.40.0/24 with the gateway 10.0.50.1.
D. Create a 1-to-1 NAT rule for traffic from the 10.0.40.0/24 subnet to addresses on the 10.0.50.0/24 subnet.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Match each type of NAT with the correct description:
Allows a user on the trusted or optional network to connect to a public server that is on the same physical Firebox interface by its public IP address or domain name. (Choose one)
A. 1-to1 NAT
B. Dynamic NAT
C. NAT Loopback
Answer: (SHOW ANSWER)
Explanation/Reference:
NAT loopback allows a user on the trusted or optional networks to get access to a public server that is on the same physical Firebox or XTM device interface by its public IP address or domain name.

Reference: http://www.watchguard.com/help/docs/wsm/11/en-US/index_Left.html#CSHID=en-US%2Fnat%2Fnat_loopback_c.html|StartTopic=Content%2Fen-US%2Fnat%2Fnat_loopback_c.html

NEW QUESTION: 59
If your Firebox has a single public IP address, and you want to forward inbound traffic to internal hosts based on the destination port, which type of NAT should you use? (Select one.)
A. Dynamic NAT
B. 1-to-1 NAT
C. Static NAT
Answer: (SHOW ANSWER)

NEW QUESTION: 60
In the default Firebox configuration file, which policies control management access to the device? (Select two.)
A. Outgoing
B. WatchGuard Web UI
C. Ping
D. WatchGuard
E. FTP
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 61
Match each WatchGuard Subscription Service with its function.
Uses signatures to provide real-time protection against network attacks. (Choose one).
A. Reputation Enable Defense RED
B. Data Loss Prevention DLP
C. Intrusion Prevention Server IPS
D. Application Control
E. APT Blocker
Answer: C (LEAVE A REPLY)
Intrusion PreventionService (IPS) -- As with the other IPS offers, the IPS module is intended to detect and in real time mitigate intrusions coming into a network. This includes a large signaturedata base that monitors for spyware, SQL injections, cross-site scripting (XSS),and buffer overflows.
Reference:http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html

NEW QUESTION: 62
The policies in a default Firebox configuration do not allow outgoing traffic from optional interfaces.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
In the default Firebox configuration file, which policies control management access to the device? (Select two.)
A. Ping
B. Outgoing
C. WatchGuard
D. FTP
E. WatchGuard Web UI
Answer: (SHOW ANSWER)

NEW QUESTION: 64
How can you include log messages from more than one Firebox in a single report generated by Dimension? (Select two.)
A. You cannot see report data in Dimension for more than one device.
B. Export report data as a single PDF file for all the devices you want to include in the report.
C. Create a report schedule that includes all the devices you want to include in the report.
D. Create a device group and view the reports for that group.
Answer: C,D (LEAVE A REPLY)

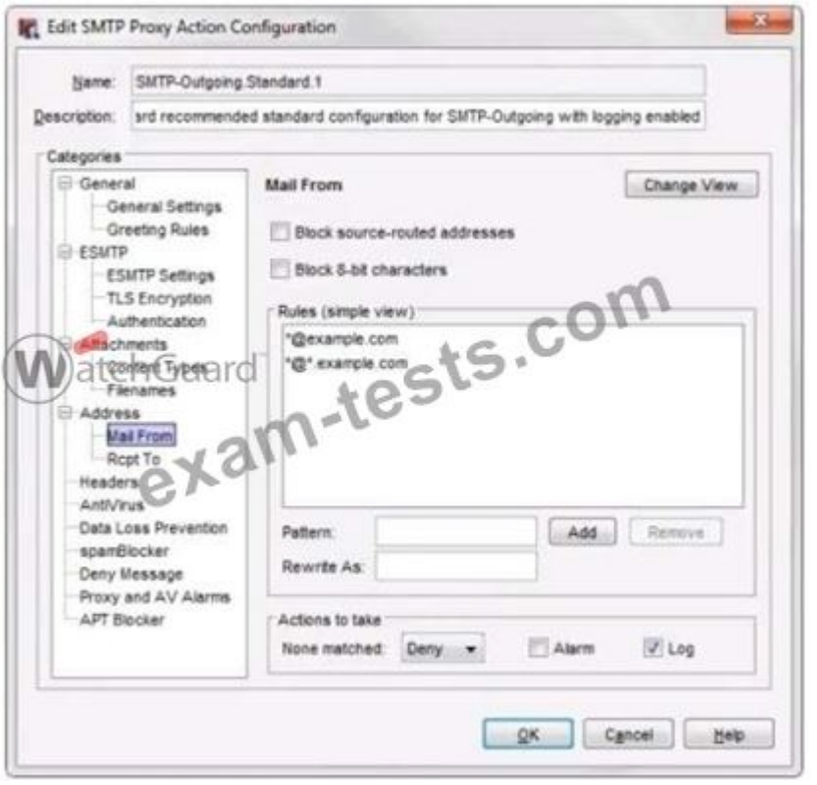
NEW QUESTION: 65
How is a proxy policy different from a packet filter policy? (Select two.)
A. Only a proxy policy examines information in the IP header.
B. Only a proxy policy uses the IP source, destination, and port to control network traffic.
C. Only a proxy policy can prevent specific threats without blocking the entire connection.
D. Only a proxy works at the application, network, and transport layers to examine all connection data.
Answer: C,D (LEAVE A REPLY)
Explanation/Reference:

C: Proxies can prevent potential threats from reaching your network without blocking the entire connection.
D: A proxy operates at the application layer, as well as the network and transport layers of a TCP/IP packet, while a packet filter operates only at the network and transport protocol layers.
Incorrect:
Not A: A packet filter examines each packet's IP header to control the network traffic into and out of your network.
Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 95

NEW QUESTION: 66
Match each WatchGuard Subscription Service with its function.
Cloud based service that controls access to website based on a site's previous behavior. (Choose one).
A. Reputation Enable Defense RED
B. Data Loss Prevention DLP
C. WebBlocker
D. Intrusion Prevention Server IPS
E. Application Control
F. Quarantine Server
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reputation Enable Device (RED) is a cloud-based reputation service that controls user's ability to get main access to web malicious sites. Works in concert with the WebBlocker module.
Reference: http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html

NEW QUESTION: 67
Match each WatchGuard Subscription Service with its function.
Scans files to detect malicious software infections. (Choose one).
A. Reputation Enable Defense RED
B. Gateway / Antivirus
C. Data Loss Prevention DLP
D. Spam Blocker
E. Quarantine Server
Answer: B (LEAVE A REPLY)
Gateway Antivirus provides a virus scanner that uses both an extensive signature database (updated through subscription) and a heuristic analysis engine.
Reference:http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html

NEW QUESTION: 68
From the SMTP proxy action settings in this image, which of these options is configured for outgoing SMTP traffic? (Select one.)



A. Prevent mail relay for the example.comdomain.
B. Rewrite the Mail From header for the example.comdomain.
C. Deny outgoing mail from the example.comdomain.
D. Deny incoming mail from the example.comdomain.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Your company denies downloads of executable files from all websites. What can you do to allow users on the network to download executable files from the company's remote website? (Select one.)
A. Create an IPS exception.
B. Create a WebBlocker exception to allow access to the company's remote website.
C. Create a Blocked Sites exception.
D. Add an HTTP proxy exception for the company's remote website.
E. Configure HTTP Request > URL Paths to allow the company's remote website.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
A user receives a deny message that the installation file (install.exe) is blocked by the HTTP-proxy policy and cannot be downloaded. Which HTTP proxy action rule must you modify to allow download of the installation file? (Select one.)
A. HTTP Request > Authorization
B. HTTP Request > Request Methods
C. WebBlocker

D. HTTP Response > Header Fields
E. HTTP Response > Body Content Types
Answer: E (LEAVE A REPLY)

NEW QUESTION: 71
If you disable the Outgoing policy, which policies must you add to allow trusted users to connect to commonly used websites? (Select three.)
A. DNS port 53
B. HTTPS port 443
C. NAT policy
D. FTP port 21
E. HTTP port 80
Answer: B,D,E (LEAVE A REPLY)

NEW QUESTION: 72
HOTSPOT
Match each WatchGuard Subscription Service with its function:

Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware

Manages use of applications on your network

A repository where email messages can be sent based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention

Cloud based service that controls access to website based on a site's previous behavior

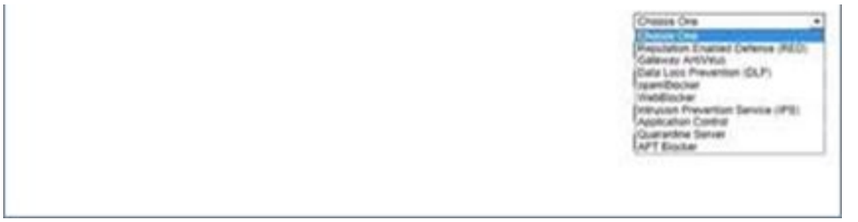
Scans files to detect malicious software infections

Prevents accidental or unauthorized transmission of confidential information outside your network

Uses signatures to provide real-time protection against network attacks

Uses rules, pattern matching, and sender reputation to block unwanted email messages

Controls access to website based on content categories


Choose One
Choose One
Reputation Enabled Defense (RED)
Gateway AntiVirus
Data Loss Prevention (DLP)
SpamBlocker
WebBlocker
Intrusion Prevention Service (IPS)
Application Control
Quarantine Server
APT Blocker

Answer:

Uses full-system emulation analysis to identify characteristics and behavior of zero-day malware

Manages use of applications on your network

A repository where email messages can be sent based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention

Cloud based service that controls access to website based on a site's previous behavior

Scans files to detect malicious software infections

Prevents accidental or unauthorized transmission of confidential information outside your network

Uses signatures to provide real-time protection against network attacks

Uses rules, pattern matching, and sender reputation to block unwanted email messages

Controls access to website based on content categories

Explanation:

WebBlocker

Spam Blocker Gateway / Antivirus APT Blocker Application Control Quarantee Server Intrusion Prevention Server IPS Data Loss Prvention DLP Reputation Enable Defense RED

NEW QUESTION: 73
In the default Firebox configuration file, which policies control management access to the device? (Select two.)
A. WatchGuard
B. FTP
C. Ping
D. WatchGuard Web UI
E. Outgoing
Answer: A,D (LEAVE A REPLY)
Ping is generated by default as the explanation states but Ping does not manage the device. The policies that manage the device are WatchGuard & WatchGuard Web UI