DUMPSQUEEN

Fireware Essentials Exam

WatchGuard Essentials

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

Only 50 clients on the trusted network of your Firebox can connect to the Internet at the same time. What could cause this? (Select one.)

A. TheLiveSecurity feature key is expired.

B. The device feature key allows a maximum of 50 client connections.

C. The DHCP address pool on the trusted interface has only 50 IP addresses.

D. The Outgoing policy allows a maximum of 50 client connections.

ANSWER: C

QUESTION NO: 2

To enable remote devices to send log messages to Dimension through the gateway Firebox, what must you verify is included in your gateway Firebox configuration? (Select one.)

A. You can only send log messages to Dimension from a computer that is on the network behind your gateway Firebox.

B. You must change the connection settings in Dimension, not on the gateway Firebox.

C. You must add a policy to the remote device configuration file to allow traffic to a Dimension.

D. You must make sure that either the WG-Logging packet filter policy, or another policy that allows external connections to Dimension over port 4115, is included in the configuration file.

ANSWER: C

QUESTION NO: 3

Which items are included in a Firebox backup image? (Select four.)

A. Support snapshot

B. Fireware OS

C. Configuration file

D. Log file

E. Feature keys

F. Certificates

ANSWER: B C E F

Explanation:

A Firebox backup image is a saved copy of the working image from the Firebox flash disk. The backup image includes the Firebox appliance software, configuration file, licenses, and certificates. When you purchase an option for your Firebox, you add a new feature key to your configuration file.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 14, 57

QUESTION NO: 4

To prevent certificate error warnings in your browser when you use deep content inspection with the HTTPS proxy, you can export the proxy authority certificate from the Firebox and import that certificate to all client devices.

A. True

B. False

ANSWER: A

QUESTION NO: 5

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

Explanation:

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

QUESTION NO: 6

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: A C D

Explanation:

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

QUESTION NO: 7

You configured four Device Administrator user accounts for your Firebox. To see a report of witch Device Management users have made changes to the device configuration, what must you do?

(Select two.)

A. Start Firebox System Manager for the device and review the activity for the Management Users on the Authentication List tab.

B. Connect to Report Manager or Dimension and view the Audit Trail report for your device.

C. Open WatchGuard Server Center and review the configuration history for managed devices.

D. Configure your device to send audit trail log messages to your WatchGuard Log Server or Dimension Log Server.

ANSWER: B C

QUESTION NO: 8

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. Create a device group and view the reports for that group.

C. Create a report schedule that includes all the devices you want to include in the report.

D. Export report data as a single PDF file for all the devices you want to include in the report.

ANSWER: B C

QUESTION NO: 9

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

Explanation:

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

QUESTION NO: 10

You can configure the SMTP-proxy policy to restrict email messages and email content based on which of these message characteristics? (Select four.)

A. Sender Mail From address

B. Check URLs in message with WebBlocker

C. Email message size

D. Attachment file name and content type

E. Maximum email recipients

ANSWER: A C D E

Explanation:

A: Another way to protect your SMTP server is to restrict incoming traffic to only messages that use your company domain. In this example, we use the mywatchguard.com domain. You can use your own company domain.

1. From the SMTP-Incoming Categories list, select Address > Rcpt To.

2. In the Pattern text box, type *.mywatchguard.com. Click Add. This denies any email messages with a Rcpt To address that does not match the company domain.

3. Click OK to close the SMTP Proxy Action Configuration dialog box.

C: In this exercise we will reduce the maximum email size to 5 MB (5, 000 kilobytes).

1. From the SMTP Proxy Action dialog box under the Categories list, select General > General Settings.

2. Find the Limits section. In the Set the maximum email size value box, type 5000.

D: Example: He must configure the Firebox to allow Microsoft Access database files to go through the SMTP proxy. He must also configure the Firebox to deny Apple iTunes MP4 files because of a recent vulnerability announced by Apple.

1. From the SMTP-Incoming Categories list, select Attachments > Content Types.

2. In the Actions to take section, use the None Matched drop-down list to select Allow.

This allows all content types through Firebox to the SMTP server. After Successful Company is able to add in the specific content types they want to allow, they set this parameter to strip content type that does not match their list of allowed content types.

From the SMTP-Incoming Categories list, select Attachments > Filenames.

4. The filename extension for Microsoft Access databases is “.mdb”. In the list of filenames, find and select .mdb. Click Remove. Click Yes to confirm.

3. If no rules match, the Action to take option is set to allow the attachment. In this example, MS Access files are now allowed through the Firebox.

5. In the Pattern text box, type *.mp4. Click Add.

This rule configures the Firebox to deny all files with the Apple iTunes “.mp4” file extension bound for the SMTP server.

E: The Set the maximum email recipient checkbox is used to set the maximum number of email recipients to which a message can be sent in the adjacent text box that appears, type or select the number of recipients.

The XTM device counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message.

Incorrect:

Not B: Webblocker is configured through a HTTP-policy, not through an SMTP policy.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 125, 126

Reference: http://watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/proxies/smtp/proxy_smtp_gen_settings_c.html