ESSENTIALS^Q&As

Fireware Essentials Exam

Pass WatchGuard ESSENTIALS Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/essentials.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by WatchGuard Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: BCEF

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 2

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. WebBlocker

B. Gateway AntiVirus

C. Application Control

D. Deep inspection of HTTPS content

E. Data Loss Prevention

Correct Answer: DE

QUESTION 3

What is the best method to downgrade the version of Fireware OS on your Firebox without losing all device configuration settings? (Select one.)

A. Restore a saved backup image that was created for the device before the last Fireware OS upgrade.

B. Use the Upgrade OS feature in Fireware Web UI to install the sysa_dl file for an order version of Fireware OS.

C. Change the OS compatibility setting in Policy Manager to downgrade the device. Then use Policy Manager to save the configuration to the device.

D. Use the downgrade feature on Policy Manager to select a previous of Fireware OS.

Correct Answer: A

QUESTION 4

Which WatchGuard Subscription Service must be enabled in a proxy policy before you can use APT Blocker? (Select one.)

A. RED

B. Application Control

C. Gateway Antivirus

D. WebBlocker

E. IPS

Correct Answer: C

QUESTION 5

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 > Request Methods

B. HTTP Response > Body Content Types

C. HTTP Response > Header Fields

D. WebBlocker

E. HTTP Request > Authorization

Correct Answer: B

QUESTION 6

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

Correct Answer: D

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

QUESTION 7

A local branch office VPN tunnel route is configured as shown in this image. On the remote peer device, what must be configured as the remote network address for this tunnel route? (Select one.)
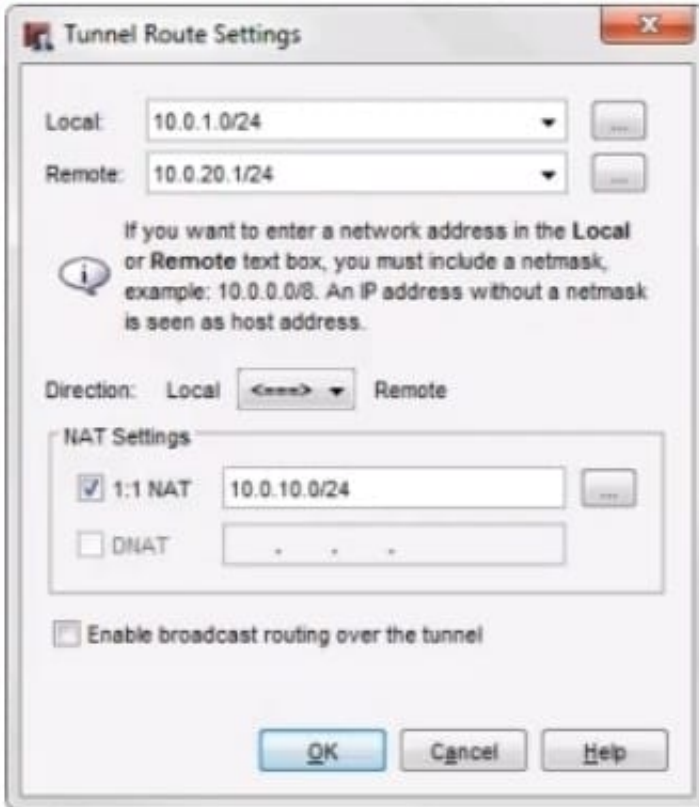
![Pass2Lead logo](https://Pass2Lead.com)
A. 10.0.1.0/24

B. 10.0.10.0/24

C. 10.0.20.0/24

Correct Answer: B

QUESTION 8

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.

Correct Answer: ABD

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

QUESTION 9

Match each type of NAT with the correct description:

Conserves IP addresses and hides the internal topology of your network. (Choose one)

A. 1-to1 NAT

B. Dynamic NAT

C. NAT Loopback

Correct Answer: B

Dynamic NAT is also known as IP masquerading. With dynamic NAT many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network.

Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#en-US/nat/ nat_dynamic_use_c.html%3FTocPath%3DNetwork%2520Address%2520Translation%2520(NAT)% 7CAbout%2520Dynamic%2520NAT%7C_____0

QUESTION 10

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

Correct Answer: ADE

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

QUESTION 11

Match each WatchGuard Subscription Service with its function.

Prevents accidental or unauthorized transmission of confidential information outside your network. (Choose one).

A. Reputation Enable Defense RED

B. Gateway / Antivirus

C. Data Loss Prevention DLP

D. Intrusion Prevention Server IPS

E. APT Blocker

Correct Answer: C

Data Loss Prevention (DLP) watches for accidental and intentional breaches of private/sensitive data through an organizational policy. Provides a library of over 200 rules to protect organization data and has the ability to parse over 30 different file formats including Microsoft Office formats and PDFs.

Reference: http://www.tomsitpro.com/articles/network-security-solutions-guide, 2-866-6.html

QUESTION 12

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.

Correct Answer: BC

QUESTION 13

In a Mobile VPN configuration, why would you choose default route VPN over split tunnel VPN? (Select one.)

A. Default route VPN allows your Firebox to examine all remote user traffic

B. Default route VPN uses less bandwidth

![Pass2Lead](https://Pass2Lead.com)
C. Default route VPN uses less processing power

D. Default route VPN automatically allows dynamic NAT

Correct Answer: D

QUESTION 14

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. Static NAT

B. 1-to-1 NAT

C. Dynamic NAT

Correct Answer: B

QUESTION 15

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

Correct Answer: C

The FireWatch page is separated into tabs of data that is presented in a Treemap 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