

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.leads4pass.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

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

Correct Answer: A

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>

QUESTION 2

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

Correct Answer: I

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>

QUESTION 3

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

Correct Answer: C

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 4

Which takes precedence: WebBlocker category match or a WebBlocker exception?

- A. WebBlocker exception
- B. WebBlocker category match

Correct Answer: A

QUESTION 5

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 6

- A. DNS lookup
- B. MAC address lookup
- C. Traceroute
- D. Reputation lookup
- E. Ping
- F. TCP dump

Correct Answer: ACEF

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

QUESTION 7

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

Correct Answer: C

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>

QUESTION 8

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.

Correct Answer: CD

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

QUESTION 9

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 10

A. True

B. False

Correct Answer: A

QUESTION 11

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

Correct Answer: AD

QUESTION 12

To use the Web Setup Wizard or Quick Setup Wizard to configure your Firebox or XTM device, your computer must have an IP address on which subnet? (Select one.)

A. 10.0.10.0/24

- B. 10.0.1.0/24
- C. 172.16.10.0/24
- D. 192.168.1.0/24

Correct Answer: B

QUESTION 13

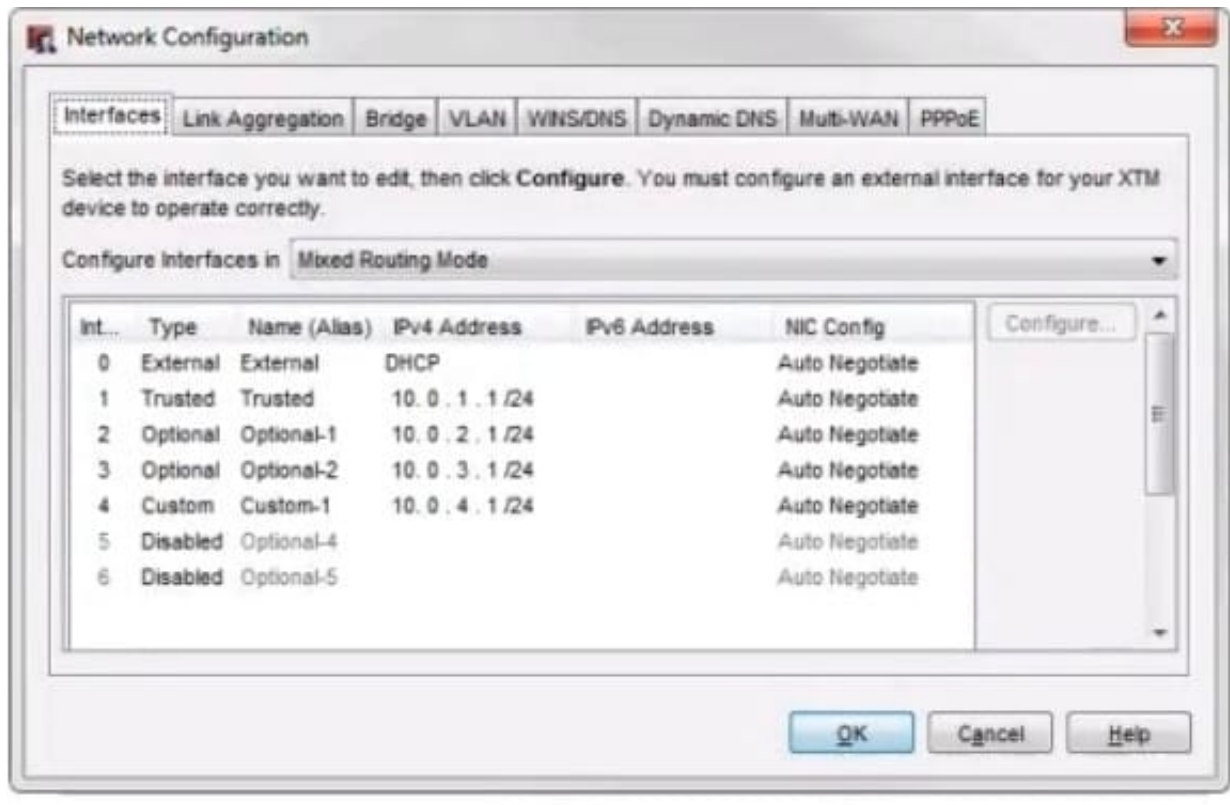
A user receives a deny message that the installation file (install.exe) is blocked by the HTTP-proxy policy and cannot be downloaded. Which HTTP proxy action rule must you modify to allow download of the installation file? (Select one.)

- 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 14

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



- A. Any-optional
- B. Any-External
- C. Optional-1
- D. Any
- E. Any-Trusted

Correct Answer: ACD

QUESTION 15

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

- A. Reputation Enabled Defense
- B. Application Control
- C. Data Loss Prevention
- D. IPS

Correct Answer: B

[Latest ESSENTIALS Dumps](#)

[ESSENTIALS VCE Dumps](#)

[ESSENTIALS Exam
Questions](#)