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.passapply.com/essentials.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

A. WebBlocker exception

B. WebBlocker category match

Correct Answer: A

QUESTION 2

After you enable Gateway AntiVirus, IPS, or Application control, how can you make sure the services protect your network from the latest known threats? (Select one.)

A. Enable default packet handling.

B. Configure reputation Enabled Defense.

C. Enable automatic signature updates.

D. Enable HTTPS deep inspection.

Correct Answer: C

QUESTION 3

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 4

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

C. Default route VPN uses less processing power

D. Default route VPN automatically allows dynamic NAT

Correct Answer: D

QUESTION 5

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.

Correct Answer: C

QUESTION 6

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 7

While troubleshooting a branch office VPN tunnel, you see this log message:

2014-07-23 12:29:15 iked (203.0.113.10203.0.113.20) Peer proposes phase oneencryption 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

Correct Answer: A

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.

QUESTION 8

When you examine the log messages In Traffic Monitor, you see that some network packets are denied with an unhandled packet log message. What does this log massage mean? (Select one.)

A. The packet is denied because the site is on the Blocked Sites List.

B. The packet is denied because it matched a policy.

C. The packet is denied because it matched an IPS signature.

D. The packet is denied because it does not match any firewall policies.

Correct Answer: D

QUESTION 9

The policies in a default Firebox configuration do not allow outgoing traffic from optional interfaces.

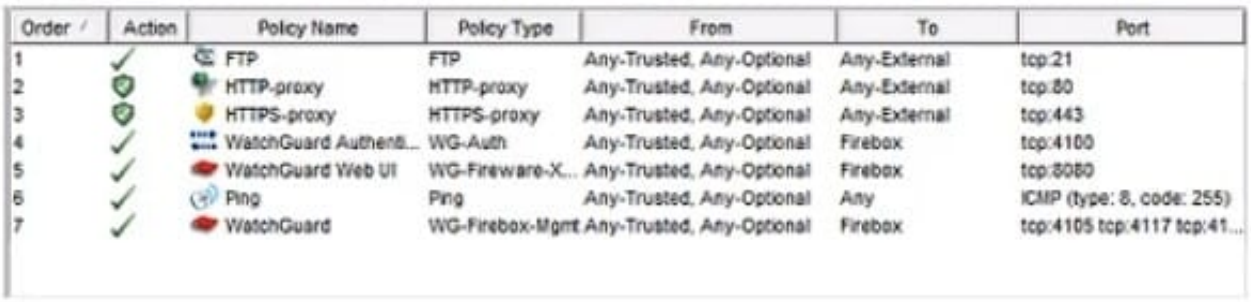
A. True

B. False

Correct Answer: B

QUESTION 10

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 Outgoing policy 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.

Correct Answer: A

QUESTION 11

Which policies can use the Intrusion Prevention Service to block network attacks? (Select one?)

A. Only HTTP and HTTPS Proxy policies

B. Only proxy policies

C. All policies

D. Only packet filter policies

E. Only inbound policies

Correct Answer: C

QUESTION 12

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 13

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

QUESTION 14

When you configure the Global Application Control action, it is automatically applied to all policies.

A. True

B. False

Correct Answer: B

QUESTION 15

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

Correct Answer: B

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