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

QUESTION 1

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

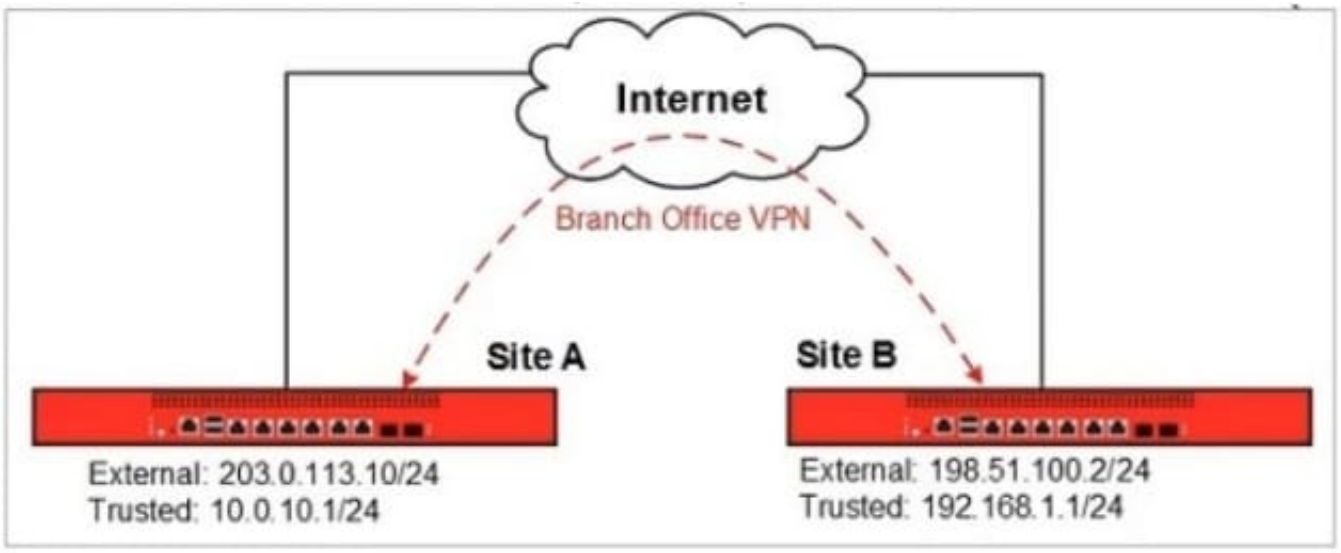
Correct Answer: C

Intrusion Prevention Service (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 signature data 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

QUESTION 2

In this diagram, which branch office VPN tunnel route must you add on the Site A Firebox to allow traffic between devices on the trusted network at Site A and the trusted network at site B? (Select one.)



A. Local: 192.168.1.0/24 Remote: 10.0.10.0/24

B. Local: 203.0.113.10/24 Remote: 198.151.100.2/24

C. Local: 10.0.10.1/24 Remote: 192.168.1.1/24

D. Local: 10.0.10.0/24 Remote: 192.168.1.0/24

Correct Answer: C

The local, Site A, network is 10.0.10.1/24 while the remote, Site B, network is 192.168.1.1/24.

QUESTION 3

Which of these threats can the Firebox prevent with the default packet handling settings? (Select four.)

A. Access to inappropriate websites

B. Denial of service attacks

C. Flood attacks

D. Malware in downloaded files

E. Port scans

F. Viruses in email messages

G. IP spoofing

Correct Answer: BCEG

B: The default configuration of the XTM device is to block DDoS attacks.

C: In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all of its resources to send reply commands. The XTM device can protect against these types of flood attacks: IPSec, IKE, ICMP. SYN, and UDP.

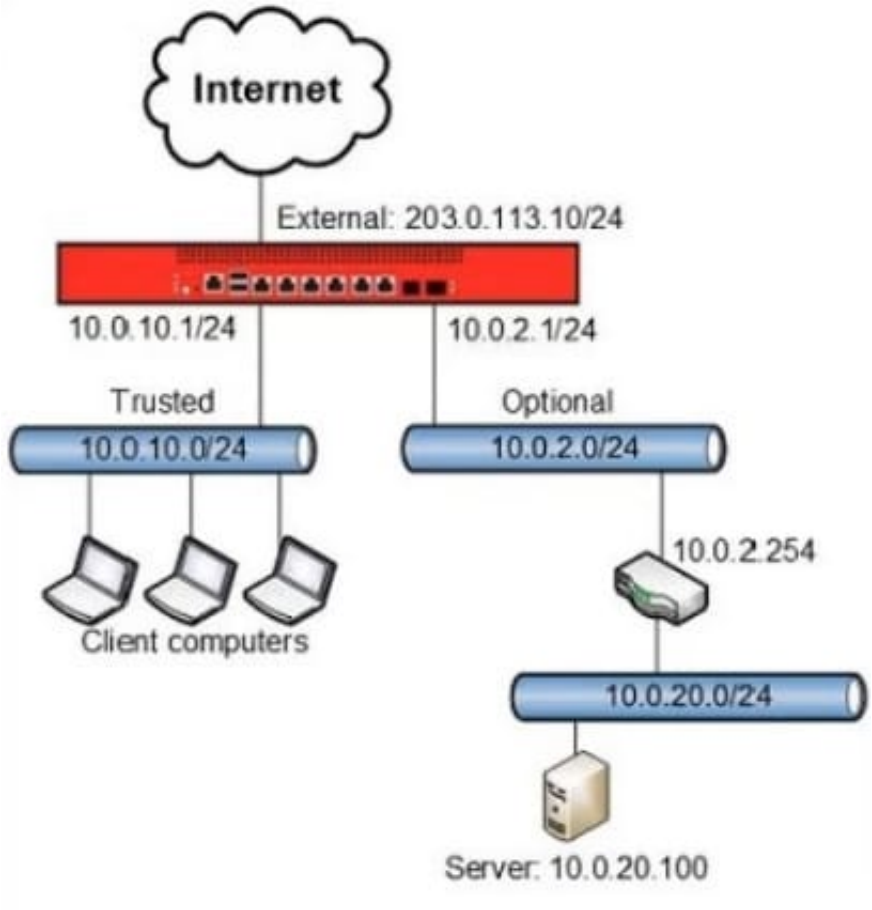
E: When the Block Port Space Probes (port scans) and Block Address Space Probes check boxes are selected, all incoming traffic on all interfaces is examined by the XTM device.

CG: Default packet handling can reject a packet that could be a security risk, including packets that could be part of a spoofing attack or SYN flood attack

Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#en-US/intrusionprevention/default_pkt_handling_opt_about_c.html%3FTocPath%3DDefault%2520Threat%2520Protection%7CAbout%2520Default%2520Packet%2520Handling%2520Options%7C_____0

QUESTION 4

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

Correct Answer: B

We must add a trusted static route to the 10.0.20.0/24 network through the 10.0.2.254 gateway.

QUESTION 5

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