Vendor: WatchGuard

Exam Code:ESSENTIALS

Exam Name: Fireware Essentials Exam

Version: Demo

QUESTION 1

Which WatchGuard tools can you use to review the log messages generated by your Firebox? (Select three).

A. Firebox System Manager > Traffic Monitor

B. Fireware XTM Web UI > Traffic Monitor

C. Firebox System Manager > Status Report

D. Dimension > Log manager

E. WatchGuard System Manager > Policy Manager

Correct Answer: ABD

A: You can use Firebox System Manager (FSM) to see log messages from your XTM device as they occur.

1.

Start Firebox System Manager.

2.

Select the Traffic Monitor tab.

Reference: http://www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html#cshid=en-US/fsm/log_msgs_traffic_mon_wsm.html

D: You can use Firebox System Manager to see log messages in real-time on the Traffic Monitor tab. You can also examine log messages with Log Manager or WatchGuard Dimension.

B: After you connect to WatchGuard WebCenter, you can review the log messages sent from your XTM devices to your WatchGuard Log Server. Log Manager enables you to see log messages from your device for any period of time you specify, if log messages were generated in the selected time frame. To see log messages for an XTM device as they are generated, in real-time, you can use Firebox System Manager Traffic Monitor.

Reference: http://www.watchguard.com/help/docs/wsm/XTM_11/en-US/index.html#en-US/logging/log_mgr_view_device_wsm.html

Incorrect:

Not C: The Status Report tab shows statistics about Firebox or XTM device traffic and performance. It does not display log messages.

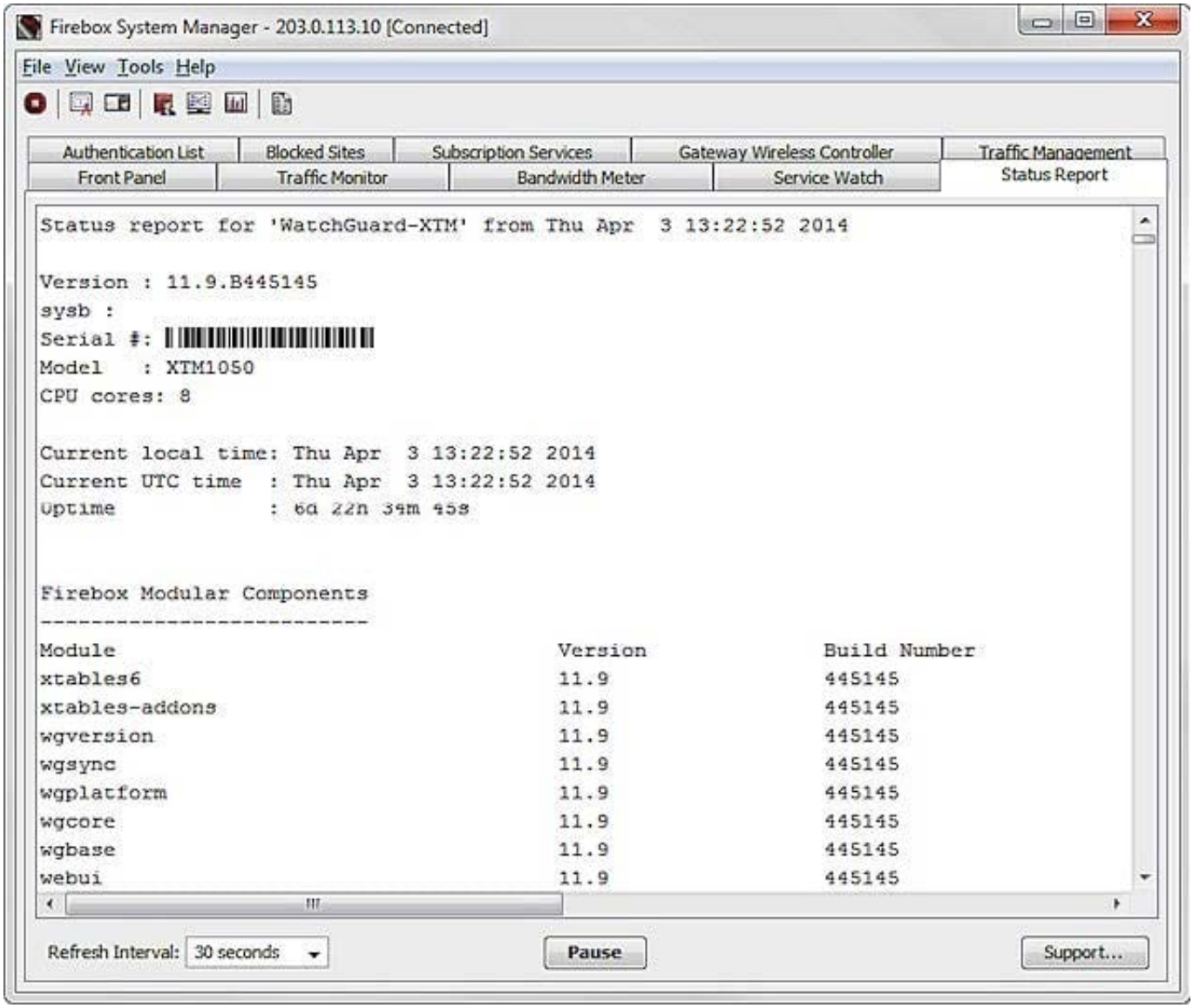
To see the Status Report:

1.

Start Firebox System Manager.

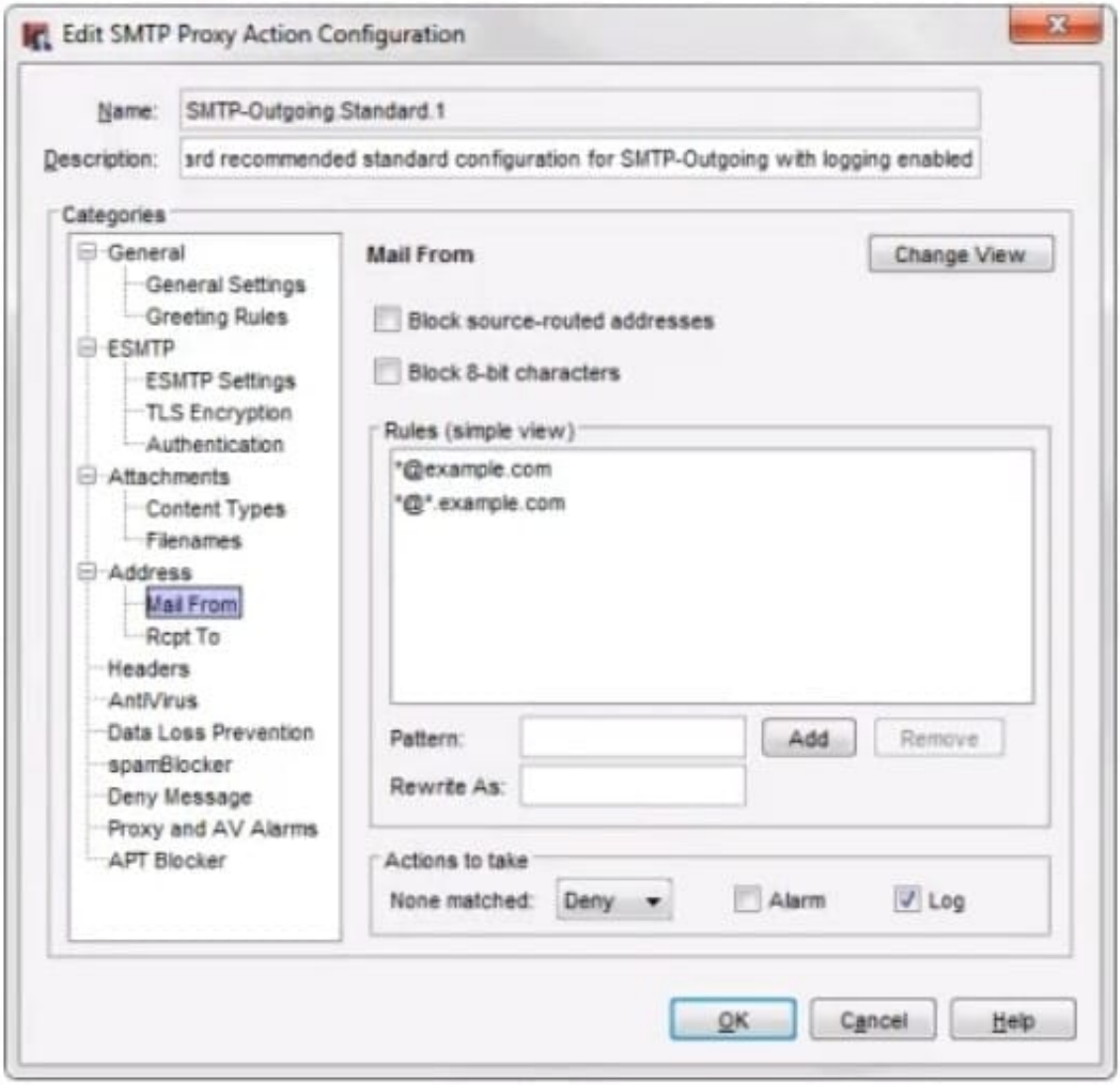
2.

Select the Status Report tab.



QUESTION 2

From the SMTP proxy action settings in this image, which of these options is configured for outgoing SMTP traffic? (Select one.)



A. Rewrite the Mail From header for the example.comdomain.

B. Deny incoming mail from the example.comdomain.

C. Prevent mail relay for the example.comdomain.

D. Deny outgoing mail from the example.comdomain.

Correct Answer: B

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

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 5

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 6

Match the monitoring tool to the correct task.

Which is not a Fireware monitoring tool? (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: B

The Fireware monitor and configuration tools are: Edge Web Manager, Firebox System Manager, HostWatch, and Ping.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 15, 34, 59, 181

QUESTION 7

Match each type of NAT with the correct description:

Changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses. (Choose one)

A. 1-to1 NAT

B. Dynamic NAT

C. NAT Loopback

Correct Answer: A

When you enable 1-to-1 NAT, the Firebox changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 74

QUESTION 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.

Correct Answer: BC

QUESTION 9

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.

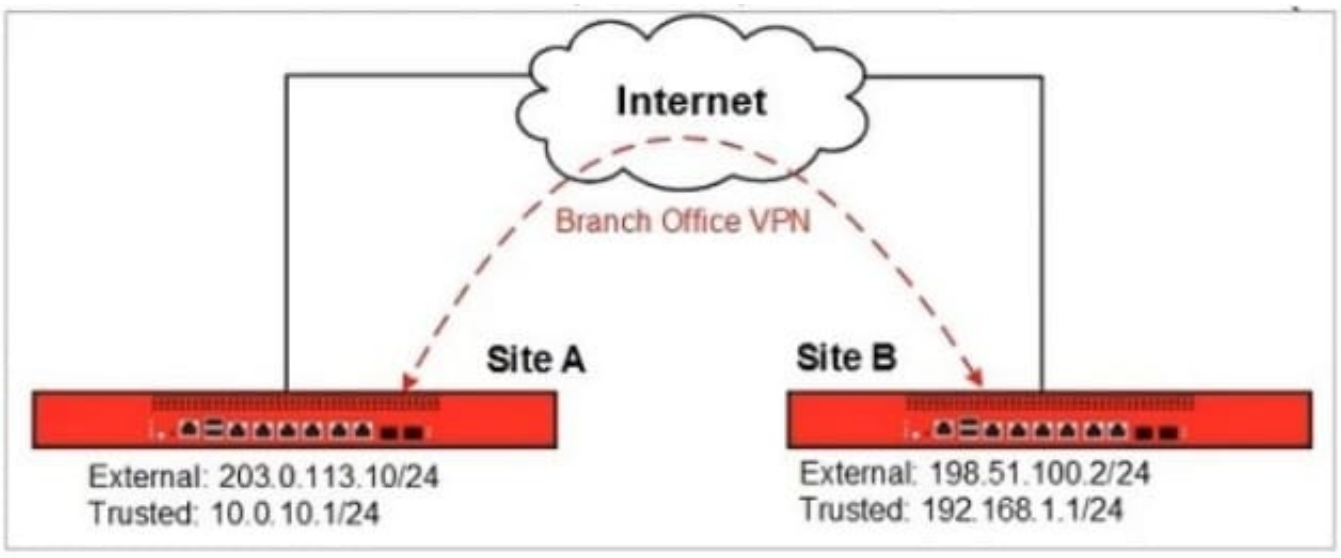
C. Enable automatic signature updates.

D. Enable HTTPS deep inspection.

Correct Answer: C

QUESTION 10

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 11

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.

Correct Answer: C

QUESTION 12

For which of these third party authentication methods must you specify a search base? (Select two.)

A. RADIUS

B. Active Directory

C. SecurID

D. LDAP

Correct Answer: BD

B: Configuring the Firebox to use Active Directory authentication is similar to the process for LDAP authentication. You must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match.

D: When you configure the Firebox to use LDAP authentication, you must set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 83-84