[Q40-Q64 Tested Material Used To Essentials Test Engine Exam Questions in here [Nov-2023

Tested Material Used To Essentials Test Engine Exam Questions in here [Nov-2023]
Penetration testers simulate Essentials exam PDF NO.40 If you disable the Outgoing policy, which policies must you add to allow trusted users to connect to commonly used websites? (Select three.)
* HTTP port 80
* NAT policy
* FTP port 21
* HTTPS port 443
* DNS port 53
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 TCPand 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

NO.41 The policies in a default Firebox configuration do not allow outgoing traffic from optional interfaces.
* True
* False

NO.42 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.)
* Static NAT
* 1-to-1 NAT
* Dynamic NAT

https://www.watchguard.com/training/fireware/10/fireware10_basics.pdf

See page 76: Static NAT allows inbound connections on specific ports to one or more public servers from a single external IP address. The Firebox changes the destination IP address of the packets and forwards them based on the original destination port number.

NO.43 You can configure your Firebox to send log messages to how many WatchGuard Log Servers at the same time? (Select one.)
* One
* Two
* As many as you have configured on your network.

NO.44 You configured four Device Administrator user accounts for your Firebox. To see a report of witch Device Management users have made changes to the device configuration, what must you do? (Select two.)
* Start Firebox System Manager for the device and review the activity for the Management Users on the Authentication List tab.
* Connect to Report Manager or Dimension and view the Audit Trail report for your device.
* Open WatchGuard Server Center and review the configuration history for managed devices.
* Configure your device to send audit trail log messages to your WatchGuard Log Server or Dimension Log Server.

NO.45 Which policies can use the Intrusion Prevention Service to block network attacks? (Select one?)
* Only HTTP and HTTPS Proxy policies
* Only proxy policies
* All policies
* Only packet filter policies
* Only inbound policies

NO.46 Which of these options are private IPv4 addresses you can assign to a trusted interface, as described in RFC 1918, Address Allocation for Private Internets? (Select three.)
* 192.168.50.1/24
* 10.50.1.1/16
* 198.51.100.1/24
* 172.16.0.1/16
* 192.0.2.1/24

NO.47 You configured four Device Administrator user accounts for your Firebox. To see a report of witch Device Management users have made changes to the device configuration, what must you do? (Select two.)
* Start Firebox System Manager for the device and review the activity for the Management Users on the Authentication List tab.
* Connect to Report Manager or Dimension and view the Audit Trail report for your device.
* Open WatchGuard Server Center and review the configuration history for managed devices.
* Configure your device to send audit trail log messages to your WatchGuard Log Server or Dimension Log Server.

NO.48 You need to create an HTTP-proxy policy to a specific domain for software updates (example.com). The update site has

multiple subdomains and dynamic IP addresses on a content delivery network. Which of these options is the best way to define the destination in your HTTP-proxy policy? (Select one.)
* Configure a host name for update.example.com.
* Configure an FQDN for *.example.com.
* Add IP addresses that correspond to each software update server in the domain.
* Create an alias for all subdomains and known IP addresses for example.com.

NO.49 Which of these threats can the Firebox prevent with the default packet handling settings? (Select four.)
* Access to inappropriate websites
* Denial of service attacks
* Flood attacks
* Malware in downloaded files
* Port scans
* Viruses in email messages
* IP spoofing

Explanation/Reference:

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

NO.50 After you enable spamBlocker, your users experience no reduction in the amount of spam they receive. What could explain this? (Select three.)
* Connections cannot be resolved to the spamBlocker servers because DNS is not configured on the Firebox.
* The spamBlocker action for Confirmed Spam is set to Allow.
* The Maximum File Size to Scan option is set too high.
* A spamBlocker exception is configured to allow traffic from sender *.
* spamBlocker Virus Outbreak Detection is not enabled.

NO.51 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).
* Reputation Enable Defense RED
* Data Loss Prevention DLP
* WebBlocker
* Intrusion Prevention Server IPS
* Application Control

* Quarantine Server
Explanation/Reference:

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

NO.52 Which of these options are private IPv4 addresses you can assign to a trusted interface, as described in RFC

1918, Address Allocation for Private Internets? (Select three.)
* 192.168.50.1/24
* 10.50.1.1/16
* 198.51.100.1/24
* 172.16.0.1/16
* 192.0.2.1/24
Explanation/Reference:

NO.53 Your company denies downloads of executable files from all websites. What can you do to allow users on the network to download executable files from the company’s remote website? (Select one.)
* Add an HTTP proxy exception for the company’s remote website.
* Create a WebBlocker exception to allow access to the company’s remote website.
* Create an IPS exception.
* Create a Blocked Sites exception.
* Configure HTTP Request > URL Paths to allow the company’s remote website.

NO.54 What is one reason that users could see a certificate warning in their web browsers when they connect to Fireware XTM Web UI? (Select one.)
* The Firebox or XTM device uses the default self-signed certificate.
* The authentication server does not respond after three minutes.
* The user has been previously added to the Blocked Sites list.
* The user or group is not present in the Firebox User database.

NO.55 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.)
* You can only send log messages to Dimension from a computer that is on the network behind your gateway Firebox.
* You must change the connection settings in Dimension, not on the gateway Firebox.
* You must add a policy to the remote device configuration file to allow traffic to a Dimension.
* 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.

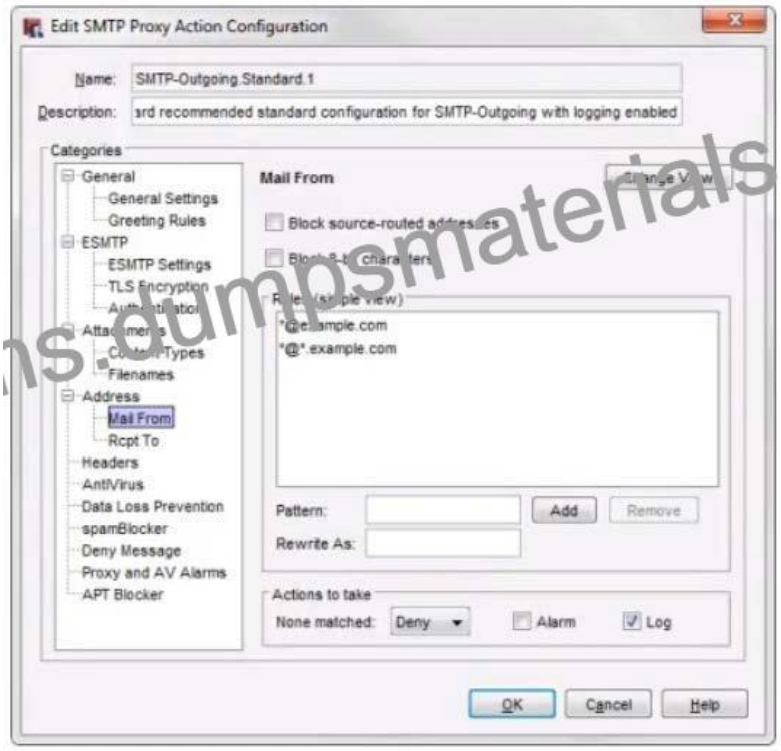
NO.56 An email newsletter about sales from an external company is sometimes blocked by spamBlocker. What option could you choose to make sure the newsletter is delivered to your users? (Select one.)
* Add a spamBlocker exception based on the From field of the newsletter email.
* Set the spamBlocker action to quarantine the email for later retrieval.
* Add a spamBlocker subject tag for bulk email messages.
* Set the spamBlocker virus outbreak detection action to allow emails from the newsletter source.

NO.57 Users on the trusted network cannot browse Internet websites.

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 Authent...	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
5	✓	WatchGuard Web ...	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...

Based on the configuration shown in this image, what could be the problem with this policy configuration? (Select one.)
* The default Outgoing policy has been removed and there is no policy to allow DNS traffic.
* The HTTP-proxy policy has higher precedence than the HTTPS-proxy policy.
* The HTTP-proxy policy is configured for the wrong port.
* The HTTP-proxy allows Any-Trusted and Any-Optional to Any-External.

NO.58 From the SMTP proxy action settings in this image, which of these options is configured for outgoing SMTP traffic? (Select one.)



* Rewrite the Mail From header for the example.comdomain.
* Deny incoming mail from the example.comdomain.
* Prevent mail relay for the example.comdomain.
* Deny outgoing mail from the example.comdomain.

NO.59 Match each WatchGuard Subscription Service with its function.

Uses rules, pattern matching, and sender reputation to block unwanted email messages. (Choose one).
* Reputation Enable Defense RED
* Gateway / Antivirus

* Spam Blocker
* Intrusion Prevention Server IPS
* APT Blocker

Explanation/Reference:

SpamBlocker provides a spam scanning engine that works in concert with WatchGuard’s cloud-based technology to prevent spam from gaining access to the email servers (and clients).

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

NO.60 Which items are included in a Firebox backup image? (Select four.)

* Support snapshot
* Fireware OS
* Configuration file
* Log file
* Feature keys
* Certificates

NO.61 Match the monitoring tool to the correct task.

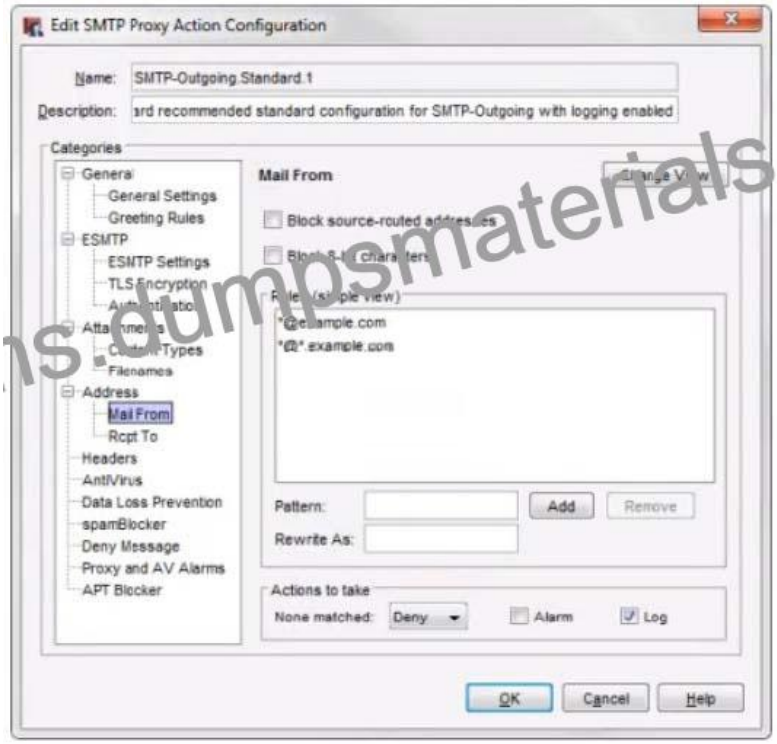
Which tool can learn the status of your IPS signature database? (Select one)

* FireBox System Manager – Blocked Sites list
* Log Server
* FireWatch
* Firebox System Manager – Subscription services
* Firebox System Manager – Authentication list
* Traffic Monitor

To look up information about an IPS signature:

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

NO.62 From the SMTP proxy action settings in this image, which of these options is configured for outgoing SMTP traffic? (Select one.)



* Rewrite the Mail From header for the example.com domain.
* Deny incoming mail from the example.com domain.
* Prevent mail relay for the example.com domain.
* Deny outgoing mail from the example.com domain.

NO.63 In the default Firebox configuration file, which policies control management access to the device? (Select two.)
* WatchGuard
* FTP
* Ping
* WatchGuard Web UI
* Outgoing

When you configure the Firebox with the Quick Setup Wizard, the wizard adds four basic policies: TCP/UDP outgoing, FTP packet filter, ping, and WatchGuard.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, page 15

NO.64 When you configure the Global Application Control action, it is automatically applied to all policies.
* True
* False

WatchGuard Essentials (Fireware Essentials) Certification Exam is a vendor-neutral certification program that is recognized by organizations around the world. Fireware Essentials Exam certification program is designed to help candidates demonstrate their expertise in the field of network security and increase their career opportunities. Fireware Essentials Exam certification program focuses on providing candidates with a thorough understanding of the WatchGuard Fireware Essentials platform, which is essential for network security professionals who want to work with WatchGuard products.

WatchGuard Essentials (Fireware Essentials) Certification Exam is a certification program designed to help IT professionals demonstrate their knowledge and skills in managing WatchGuard Firebox devices. The program is designed to be challenging and comprehensive, ensuring that those who pass the exam have a deep understanding of WatchGuard Firebox devices. It is an ideal certification program for those who want to enhance their career prospects in the field of network security.

Authentic Best resources for Essentials Online Practice Exam: https://www.dumpsmaterials.com/Essentials-real-torrent.html]