DUMPSARENA

Fireware Essentials Exam

WatchGuard Essentials

Version Demo

Total Demo Questions: 10

Total Premium Questions: 75

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

ANSWER: C

Explanation:

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 NO: 2

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

ANSWER: B D

Explanation:

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

QUESTION NO: 3

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.

ANSWER: B C

QUESTION NO: 4

You can configure the SMTP-proxy policy to restrict email messages and email content based on which of these message characteristics? (Select four.)

A. Sender Mail From address

B. Check URLs in message with WebBlocker

C. Email message size

D. Attachment file name and content type

E. Maximum email recipients

ANSWER: A C D E

Explanation:

A: Another way to protect your SMTP server is to restrict incoming traffic to only messages that use your company domain. In this example, we use the mywatchguard.com domain. You can use your own company domain.

1. From the SMTP-Incoming Categories list, select Address > Rcpt To.

2. In the Pattern text box, type *.mywatchguard.com. Click Add. This denies any email messages with a Rcpt To address that does not match the company domain.

3. Click OK to close the SMTP Proxy Action Configuration dialog box.

C: In this exercise we will reduce the maximum email size to 5 MB (5, 000 kilobytes).

1. From the SMTP Proxy Action dialog box under the Categories list, select General > General Settings.

2. Find the Limits section. In the Set the maximum email size value box, type 5000.

D: Example: He must configure the Firebox to allow Microsoft Access database files to go through the SMTP proxy. He must also configure the Firebox to deny Apple iTunes MP4 files because of a recent vulnerability announced by Apple.

1. From the SMTP-Incoming Categories list, select Attachments > Content Types.

2. In the Actions to take section, use the None Matched drop-down list to select Allow.

This allows all content types through Firebox to the SMTP server. After Successful Company is able to add in the specific content types they want to allow, they set this parameter to strip content type that does not match their list of allowed content types.

From the SMTP-Incoming Categories list, select Attachments > Filenames.

4. The filename extension for Microsoft Access databases is ".mdb". In the list of filenames, find and select .mdb. Click Remove. Click Yes to confirm.

3. If no rules match, the Action to take option is set to allow the attachment. In this example, MS Access files are now allowed through the Firebox.

5. In the Pattern text box, type *.mp4. Click Add.

This rule configures the Firebox to deny all files with the Apple iTunes ".mp4" file extension bound for the SMTP server.

E: The Set the maximum email recipient checkbox is used to set the maximum number of email recipients to which a message can be sent in the adjacent text box that appears, type or select the number of recipients.

The XTM device counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message.

Incorrect:

Not B: Webblocker is configured through a HTTP-policy, not through an SMTP policy.

Reference: Fireware Basics, Courseware: WatchGuard System Manager 10, pages 125, 126

Reference: http://watchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/proxies/smtp/proxy_smtp_gen_settings_c.html

QUESTION NO: 5

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

ANSWER: D

Explanation:

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 NO: 6

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.

ANSWER: A

QUESTION NO: 7

Which diagnostic tasks can you run from the Traffic Monitor tab of Firebox System Manager? (Select four.)

A. DNS lookup

B. MAC address lookup

C. Traceroute

D. Reputation lookup

E. Ping

F. TCP dump

ANSWER: A C E F

Explanation:

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 NO: 8

Which authentication servers can you use with your Firebox? (Select four.)

A. Active Directory

B. RADIUS

C. LDAP

D. Linux Authentication

E. Kerberos

F. TACACS+

G. Firebox databases

ANSWER: A B C G

Explanation:

QUESTION NO: 9

From the Firebox System Manager >Authentication List tab, you can view all of the authenticated users connected to your Firebox and disconnect any of them.

A. True

B. False

ANSWER: A

QUESTION NO: 10

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

ANSWER: I

Explanation:

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