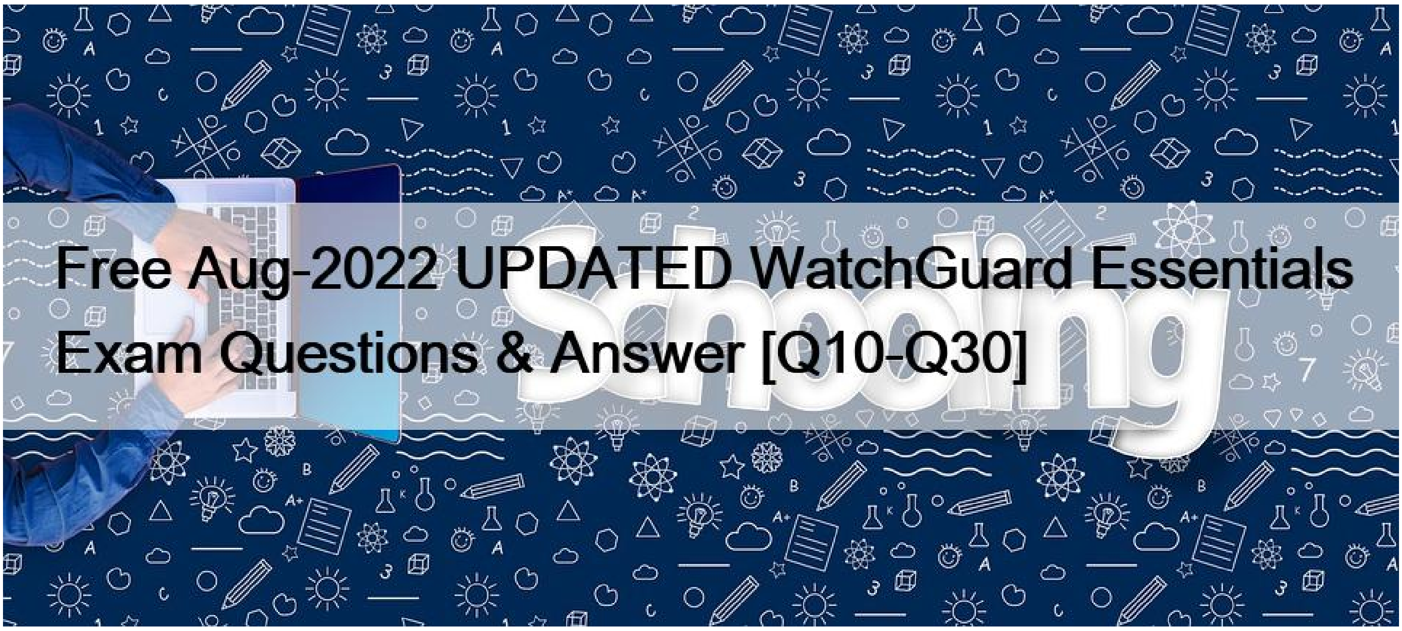
Free Aug-2022 UPDATED WatchGuard Essentials Exam Questions & Answer [Q10-Q30


Free Aug-2022 UPDATED WatchGuard Essentials Exam Questions & Answer [Q10-Q30]
Schooling

Free Aug-2022 UPDATED WatchGuard Essentials Exam Questions & Answer
Latest Success Metrics For Actual Essentials Exam Realistic Dumps

The benefit of obtaining the Essential Exam Certification

- Most of the hiring manager prefer to hire candidates who are already certified and having expertise into that domain. Company use to perform calculation because they use to spend lots of money on conducting training for the candidates who have zero knowledge about WatchGaurd Security. They use to prefer candidates who are already certified because definitely they would be having enough knowledge to start contributing to the production.- Essential exam Certification will provide you digital badge which you can add it to your CV, profile, linkedin etc. which would be bringing more recruiting Companies towards your profile.- It help you to make your career into WatchGaurd network security, Essential exam will help you to get respectful plus highly paid jobs into Market.- Essential exam certification credential will give you edge over other counterparts. Apart from knowledge from Essential Exam.

Essential exam certification will help you in providing strong understanding about Fireware Essentials, along with basic networking and new Fireware topics.

Topics of Essentials Exam

Candidates must know the exam topics before they start of preparation. Because it will really help them in hitting the core. Our **Essentials exam dumps** will include the following topics.

NEW QUESTION 10

How can you prevent connections to the Fireware Web UI from computers on optional interface Eth2?

(Select one.)
* Remove Eth2 from the Any-Optional alias.

* Remove Any-Optional from the To list of the WatchGuard Web UI policy.
* Remove Any-Optional from the From list of the WatchGuard policy.
* Remove Any-Optional from the To list of the WatchGuard policy
* Remove Any-Optional from the From list of the WatchGuard Web UI policy

NEW QUESTION 11

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.

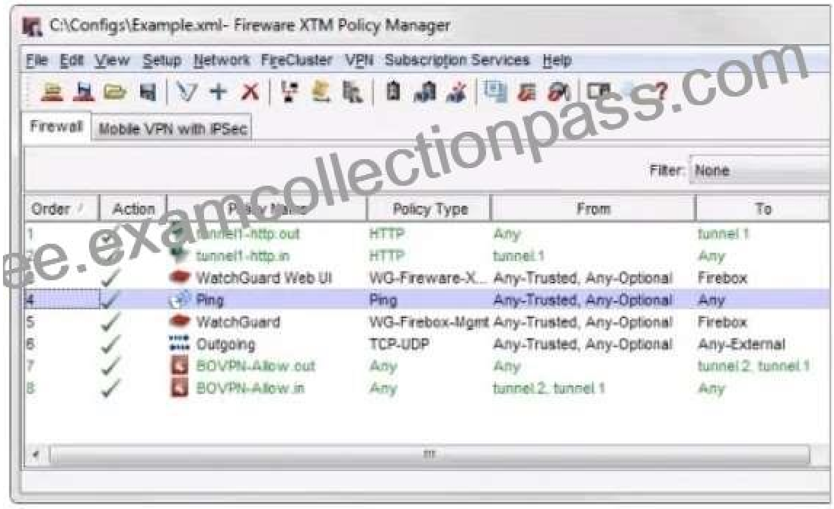
NEW QUESTION 12

Match each type of NAT with the correct description:

Conserves IP addresses and hides the internal topology of your network. (Choose one)
* 1-to1 NAT
* Dynamic NAT
* NAT Loopback

NEW QUESTION 13

With the policies configured as shown in this image, HTTP traffic can be sent and received through branch office VPN tunnel.1 and tunnel.2.


C:\Configs\Example.xml- Fireware XTM Policy Manager
File Edit View Setup Network FireCluster VPN Subscription Services Help
Firewall
Mobile VPN with IPSec
Filter: None

Order	Action	Policy Name	Policy Type	From	To
1	✓	tunnel1-http.out	HTTP	Any	tunnel.1
2	✓	tunnel1-http.in	HTTP	tunnel.1	Any
3	✓	WatchGuard Web UI	WG-Fireware-X...	Any-Trusted, Any-Optional	Firebox
4	✓	Ping	Ping	Any-Trusted, Any-Optional	Any
5	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox
6	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External
7	✓	BOVPN-Allow.out	Any	Any	tunnel.2, tunnel.1
8	✓	BOVPN-Allow.in	Any	tunnel.2, tunnel.1	Any

* True
* False

NEW QUESTION 14

Which tool can add an IP address for the Firebox to permanently block? (Select one)
* FireBox System Manager &#8211; Blocked Sites list
* Log Server
* FireWatch
* Firebox System Manager &#8211; Subscription services
* Firebox System Manager &#8211; Authentication list
* Traffic Monitor
Block a site permanently

The Successful Company networkadministrator has been driven to distraction recently by a script kiddy using addresses in the 192.136.15.0/24 network to run probes of the Successful network. In this exercise, we permanently block all connections from that network.

1.From PolicyManager, select Setup > Default Threat Protection > Blocked Sites. The Blocked Sites Configuration dialog box opens.

2.On the Blocked Sites tab, click Add.

3.The Add Site dialog box opens. 3. Use the Choose Type drop-down list to select Network IP. In the Value text box, type 192.136.15.0/ 24.

4. Click OK.

The entry appears in the Blocked Sites list. With this configuration, the Firebox blocks all packets to and from the 192.136.15.0/24 network range.

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

NEW QUESTION 15

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

NEW QUESTION 16

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.

NEW QUESTION 17

Which of these actions adds a host to the temporary or permanent blocked sites list? (Select three.)

* Enable the AUTO-block sites that attempt to connect option in a deny policy.
* Add the site to the Blocked Sites Exceptions list.
* On the Firebox System Manager >Blocked Sites tab, select Add.
* In Policy Manager, select Setup> Default Threat Protection > Blocked Sites and click Add.

NEW QUESTION 18

A user receives a deny message that the installation file (install.exe) is blocked by the HTTP-proxy policy and cannot be downloaded. Which HTTP proxy action rule must you modify to allow download of the installation file? (Select one.)
* HTTP Request > Request Methods
* HTTP Response > Body Content Types
* HTTP Response > Header Fields
* WebBlocker
* HTTP Request > Authorization

NEW QUESTION 19

Which of these actions adds a host to the temporary or permanent blocked sites list? (Select three.)
* Enable the AUTO-block sites that attempt to connect option in a deny policy.
* Add the site to the Blocked Sites Exceptions list.
* On the Firebox System Manager >Blocked Sites tab, select Add.
* In Policy Manager, select Setup> Default Threat Protection > Blocked Sites and click Add.
Explanation/Reference:

A: You can configure a deny policy to automatically block sites that originate traffic that does not comply with the policy rulese

1. From Policy Manager, double-click the PCAnywhere policy.

2. Click the Properties tab. Select the Auto-block sites that attempt to connect checkbox.

Reference: https://www.watchguard.com/training/fireware/80/defense8.htm C: The blocked sites list shows all the sites currently blocked as a result of the rules defined in Policy Manager. From this tab, you can add sites to the temporary blocked sites list, or remove temporary blocked sites.

Reference: http://www.watchguard.com/training/fireware/82/monitoa6.htm

D: You can use Policy Manager to permanently add sites to the Blocked Sites list.

1. select Setup > Default Threat Protection > Blocked Sites.

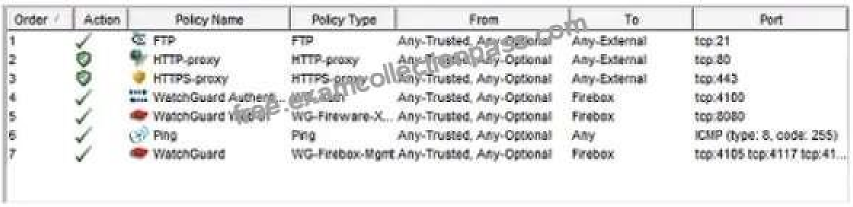
2. Click Add.

The Add Site dialog box appears.

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

NEW QUESTION 20

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 Authent...	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...

* 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.

NEW QUESTION 21

When your users connect to the Authentication Portal page to authenticate, they see a security warning message in their browses, which they must accept before they can authenticate. How can you make sure they do not see this security warning message in their browsers? (Select one.)
* Import a custom self-signed certificate or a third-party certificate to your Firebox and import the same certificate to all client computers or web browsers.
* Replace the Firebox certificate with the trusted certificate from your web server.
* Add the user accounts for your users who use the Authentication Portal to a list of trusted users on your Firebox.
* Instruct them to disable security warning message in their preferred browsers.
http://wwwwatchguard.com/help/docs/wsm/xtm_11/en-us/content/en-us/authentication/authentication_user_process_c.html

NEW QUESTION 22

Match each WatchGuard Subscription Service with its function.

Cloud based service that controls access to website based on a site&#8217;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&#8217;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

NEW QUESTION 23

From the Fireware Web UI, you can generate a report that shows your device configuration settings.
* True
* False

NEW QUESTION 24

Match each WatchGuard Subscription Service with its function.

Cloud based service that controls access to website based on a site&#8217;s previous behavior. (Choose one).
* Reputation Enable Defense RED
* Data Loss Prevention DLP
* WebBlocker
* Intrusion Prevention Server IPS
* Application Control
* QuarantineServer
Reputation Enable Device (RED) is a cloud-based reputation service that controls user&#8217;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

NEW QUESTION 25

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

NEW QUESTION 26

You can use Firebox System Manager to download a PCAP file that includes packet information about the protocols that manage traffic on your network.
* True
* False

NEW QUESTION 27

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.)
* WebBlocker
* Gateway AntiVirus
* Application Control
* Deep inspection of HTTPS content
* Data Loss Prevention

NEW QUESTION 28

Which tool can add an IP address for the Firebox to permanently block? (Select one)
* FireBox System Manager &#8211; Blocked Sites list
* Log Server
* FireWatch
* Firebox System Manager &#8211; Subscription services
* Firebox System Manager &#8211; Authentication list
* Traffic Monitor
Block a site permanently

The Successful Company networkadministrator has been driven to distraction recently by a script kiddy using addresses in the 192.136.15.0/24 network to run probes of the Successful network. In this exercise, we permanently block all connections from that network.

1.From PolicyManager, select Setup > Default Threat Protection > Blocked Sites. The Blocked Sites Configuration dialog box opens.

2.On the Blocked Sites tab, click Add.

3.The Add Site dialog box opens. 3. Use the Choose Type drop-down list to select Network IP. In the Value text box, type 192.136.15.0/ 24.

4. Click OK.

The entry appears in the Blocked Sites list. With this configuration, the Firebox blocks all packets to and from the 192.136.15.0/24 network range.

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

NEW QUESTION 29

Which tool is used to see a treemap visualization of the traffic through your Firebox? (Select one)
* FireBox SystemManager &#8211; Blocked Sites list
* Log Server
* FireWatch
* Firebox System Manager &#8211; Subscription services
* Firebox System Manager &#8211; Authentication list
* Traffic Monitor
The FireWatch page is separated into tabs of data that is presented in aTreemap 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

NEW QUESTION 30

Match each WatchGuard Subscription Service with its function.

A repository where email messages can be sent based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention. (Choose one).
* Gateway / Antivirus
* Data Loss Prevention DLP
* Spam Blocker
* Intrusion Prevention Server IPS
* Quarantine Server
Explanation/Reference:

The WatchGuard Quarantine Server provides a safe mechanism to quarantine any email messages that are suspected or known to be spam, or to contain viruses or sensitive data. The Quarantine Server is a repository for email messages that the SMTP proxy sends to quarantine based on analysis by spamBlocker, Gateway AntiVirus, or Data Loss Prevention.

Reference: https://www.watchguard.com/help/docs/webui/xtm_11/en-US/index.html#cshid=en-US/quarantineserver/quar_server_about_c.html

Updated Essentials Dumps Questions For WatchGuard Exam:
https://www.examcollectionpass.com/WatchGuard/Essentials-practice-exam-dumps.html]