[Q23-Q37 The Network-Security-Essentials PDF Dumps Greatest for the WatchGuard Exam Study Guide!

The Network-Security-Essentials PDF Dumps Greatest for the WatchGuard Exam Study Guide! Read Online Network-Security-Essentials Test Practice Test Questions Exam Dumps QUESTION 23

If a Firebox has two trusted interfaces enabled, the default policies allow HTTPS connections between computers on different trusted networks.
* True
* False
By default, Firebox policies do not allow HTTPS connections between devices on separate trusted networks without specific policy configuration. Firebox&#8217;s default security posture is to restrict inter-network traffic unless explicitly permitted, enhancing network segmentation and security within trusted zones.

QUESTION 24

If policies are automatically ordered, which of these policies has the highest precedence? (Select one.)
* HTTPS policy &#8211; From: Any-Trusted, Any-Optional To: Any-External
* HTTPS policy &#8211; From: Trusted To: Any-External
* Outgoing policy &#8211; From: Any-Trusted, Any-Optional To: Any-External
* HTTPS policy &#8211; From: User1@Firebox-DB To: Any-External

When policies are automatically ordered, policies with more specific user-based criteria have higher precedence over general policies. In this scenario, an HTTPS policy for a specific user (e.g.,User1@Firebox- DB) would take precedence over policies that apply to broader groups or networks, such asAny-Trustedor Any-Optional. This ordering ensures that individual user rules are evaluated first before generic policies, providing finer access control.

QUESTION 25

You can add your Firebox to WatchGuard Cloud but continue to manage it locally. When you do this, what additional features does WatchGuard Cloud provide for your locally-managed Firebox? (Select two.)
* Automatic Firebox firmware updates
* Ability to schedule Firebox firmware updates
* Real-time network traffic data
* Unified event correlation and analysis
* Live status and access to reports
When adding a Firebox to WatchGuard Cloud while maintaining local management:

* Option B: WatchGuard Cloud allows the scheduling of Firebox firmware updates, which provides flexibility in managing update timing without disrupting operations.

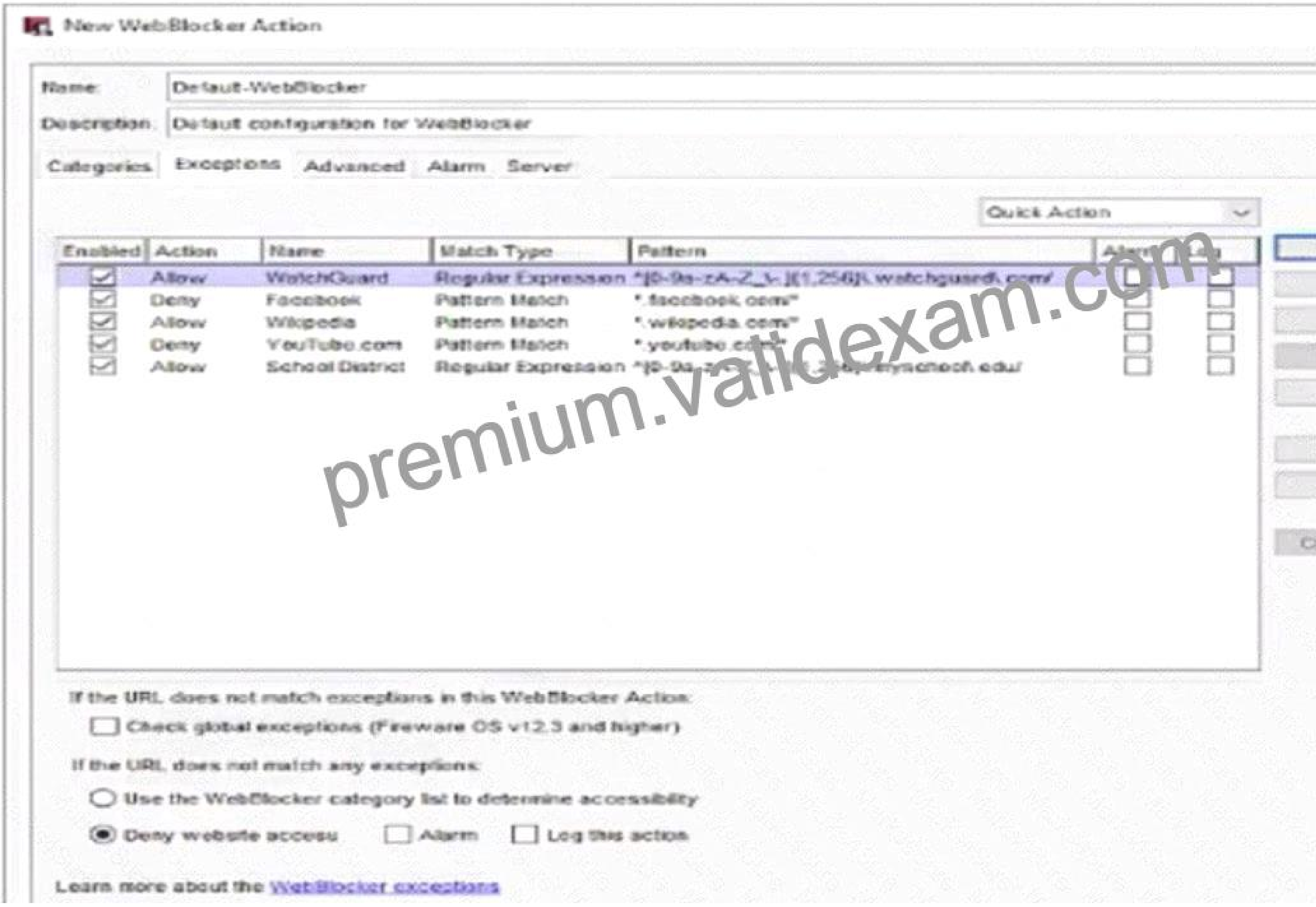
* Option E: It provides live status updates and reporting access, giving insights into device health and performance metrics for informed management decisions.

* Option A(Automatic firmware updates) is typically managed manually in a locally managed configuration.

* Option C(Real-time network traffic data) andOption D(Unified event correlation andanalysis) are advanced features that require full cloud management rather than hybrid (local/cloud) setup.

QUESTION 26

Which of these sites are denied by the WebBlocker action shown in this image? (Select three.)



New WebBlocker Action

Name: Default-WebBlocker

Description: Default configuration for WebBlocker

Enabled	Action	Name	Match Type	Pattern	Alarm	Log
☑	Allow	WatchGuard	Regular Expression	^[0-9a-zA-Z_\-.]{1,256}\.watchguard\.com/	□	□
☑	Deny	Facebook	Pattern Match	*.facebook.com/*	□	□
☑	Allow	Wikipedia	Pattern Match	*.wikipedia.com/*	□	□
☑	Deny	YouTube.com	Pattern Match	*.youtube.com/*	□	□
☑	Allow	School District	Regular Expression	^[0-9a-zA-Z_\-.]{1,256}\.myschool\.edu/	□	□

If the URL does not match exceptions in this WebBlocker Action:

□ Check global exceptions (Fireware OS v12.3 and higher)

If the URL does not match any exceptions:

○ Use the WebBlocker category list to determine accessibility

● Deny website access □ Alarm □ Log this action

Learn more about the WebBlocker exceptions

* www.wikipedia.com/firewall
* www.youtube.com
* www.google.com
* schedule.myschool.edu
* www.watchguard.com/wgrd-blog
* login.facebook.com

The WebBlocker action in the image contains bothAllowandDenyrules based on specific patterns:

* www.youtube.com- This is explicitly denied by the WebBlocker configuration for the pattern youtube.

com*.

* login.facebook.com- This would also be denied because it matches the pattern facebook.com*.

* www.google.com- There is no specificAllowrule for google.com or any associated subdomain, and since WebBlocker defaults toDenywhen a URL does not match any exceptions, www.google.com would be denied as well.

The other options:

* A.www.wikipedia.com/firewall- Allowed due to the wikipedia.com* pattern.

* D. schedule.myschool.edu- Allowed due to the regular expression matching *.myschool.edu.

* E.www.watchguard.com/wgrd-blog- Allowed by the regular expression for watchguard.com.

QUESTION 27

In a Mobile VPN configuration, why would you choose default-route (full tunnel) VPN instead of split tunnel VPN? (Select one.)
* Default-route VPN uses less bandwidth.
* Default-route VPN enables your Firebox to examine all remote user traffic.
* Default-route VPN uses less processing power.
* Default-route VPN automatically allows dynamic NAT.
* Default-route VPN is the only option you can use to apply security services to connections routed to your internal servers.

In a Mobile VPN setup, adefault-route (full tunnel)VPN routes all of a remote user&#8217;s internet traffic through the VPN tunnel to the Firebox. This configuration allows the Firebox to inspect and apply security policies to all traffic, including traffic that is not destined for internal network resources. In contrast, asplit tunnel VPN would route only traffic meant for the internal network through the VPN, while internet-bound traffic would bypass the Firebox, potentially exposing it to threats and limiting the Firebox&#8217;s ability to inspect all traffic.

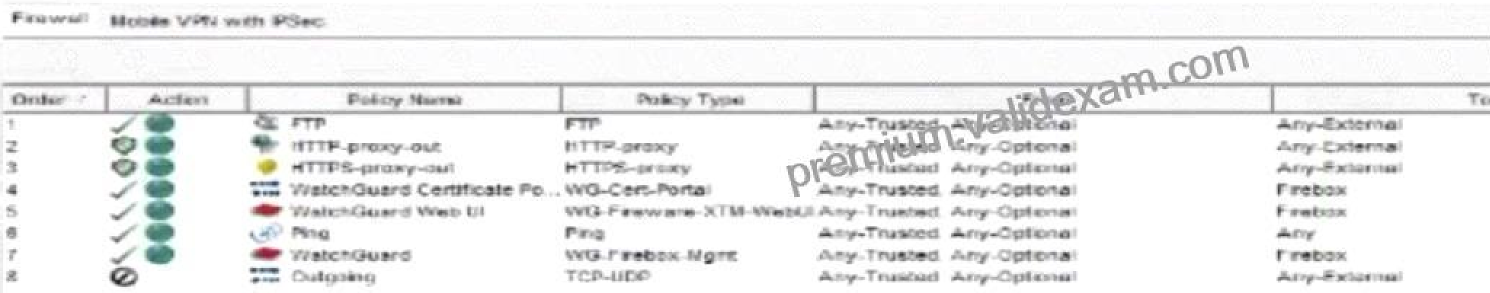
QUESTION 28

You have just configured Mobile VPN with IKEv2 for your customer. By default, authenticated Mobile VPN users are allowed to send traffic to all Firebox networks through the VPN.
* True
* False

In the default configuration ofMobile VPN with IKEv2, authenticated VPN users are only allowed access to specified networks or resources as defined by the VPN policy. They do not automatically have access to all Firebox networks through the VPN. To enable access to specific networks, administrators need to configure access routes explicitly within the Mobile VPN settings.

QUESTION 29

Based on the configuration shown in this image, clients on the network can successfully connect tohttps://www.watchguard.com.



Firewall Mobile VPN with IPSec

Order	Action	Policy Name	Policy Type	From	To
1	✓ ●	FTP	FTP	Any-Trusted Any-Optional	Any-External
2	●	HTTP-proxy-out	HTTP-proxy	Any-Trusted Any-Optional	Any-External
3	●	HTTPS-proxy-out	HTTPS-proxy	Any-Trusted Any-Optional	Any-External
4	✓ ●	WatchGuard Certificate Po...	WG-Cert-Portal	Any-Trusted Any-Optional	Firebox
5	✓ ●	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted Any-Optional	Firebox
6	✓ ●	Ping	Ping	Any-Trusted Any-Optional	Any
7	✓ ●	WatchGuard	WG-Firebox-Mgmt	Any-Trusted Any-Optional	Firebox
8	⊘	Outgoing	TCP-UDP	Any-Trusted Any-Optional	Any-External

* True
* False

Based on the configuration shown in the image, the HTTPS-proxy-out policy allows traffic fromAny-Trusted andAny-Optionalnetworks toAny-Externaldestination on port443(which is the standard port for HTTPS).

This rule effectively permits outbound HTTPS connections from clients within the trusted network to external HTTPS websites, such as https://www.watchguard.com.

Since the policy type isHTTPS-proxy, it can inspect and manage HTTPS traffic according to configured policies, but it does not block the connection itself. Therefore, users on the network should be able to successfully connect to external HTTPS sites.

QUESTION 30

The Firebox can scan the contents of encrypted zip files with Gateway AntiVirus when HTTPS content inspection is enabled.
* True
* False
The Firebox cannot scan the contents of encrypted zip files even if HTTPS content inspection is enabled.

HTTPS content inspection allows the Firebox to inspect encrypted HTTPS traffic by decrypting it. However, the content within encrypted zip files remains inaccessible to Gateway AntiVirus scanning because the encryption key for the zip file is not available to the Firebox. This limitation is consistent with standard network security practices, where encrypted files need to be decrypted with a known key before content scanning can occur.

QUESTION 31

Which of these is a network IP address? (Select one.)
* 1G2 153 10 O 1
* 1Q2 158.10 0-24
* 172 16 100 1/12
* 10 0.1 255 8
* 10 10 10 255/24
In this question, we need to identify the correctly formatted network IP address. IPv4 addresses are represented in a dotted decimal format, typically in the form of x.x.x.x/n, where x represents decimal values from 0 to 255, and /n is the CIDR notation indicating the subnet mask. Among the options:

* Option E (10 10 10 255/24)fits the IPv4 standard and CIDR notation.

* The other options contain invalid characters or formats (letters like &#8220;G&#8221; or &#8220;Q&#8221; or unusual symbols like

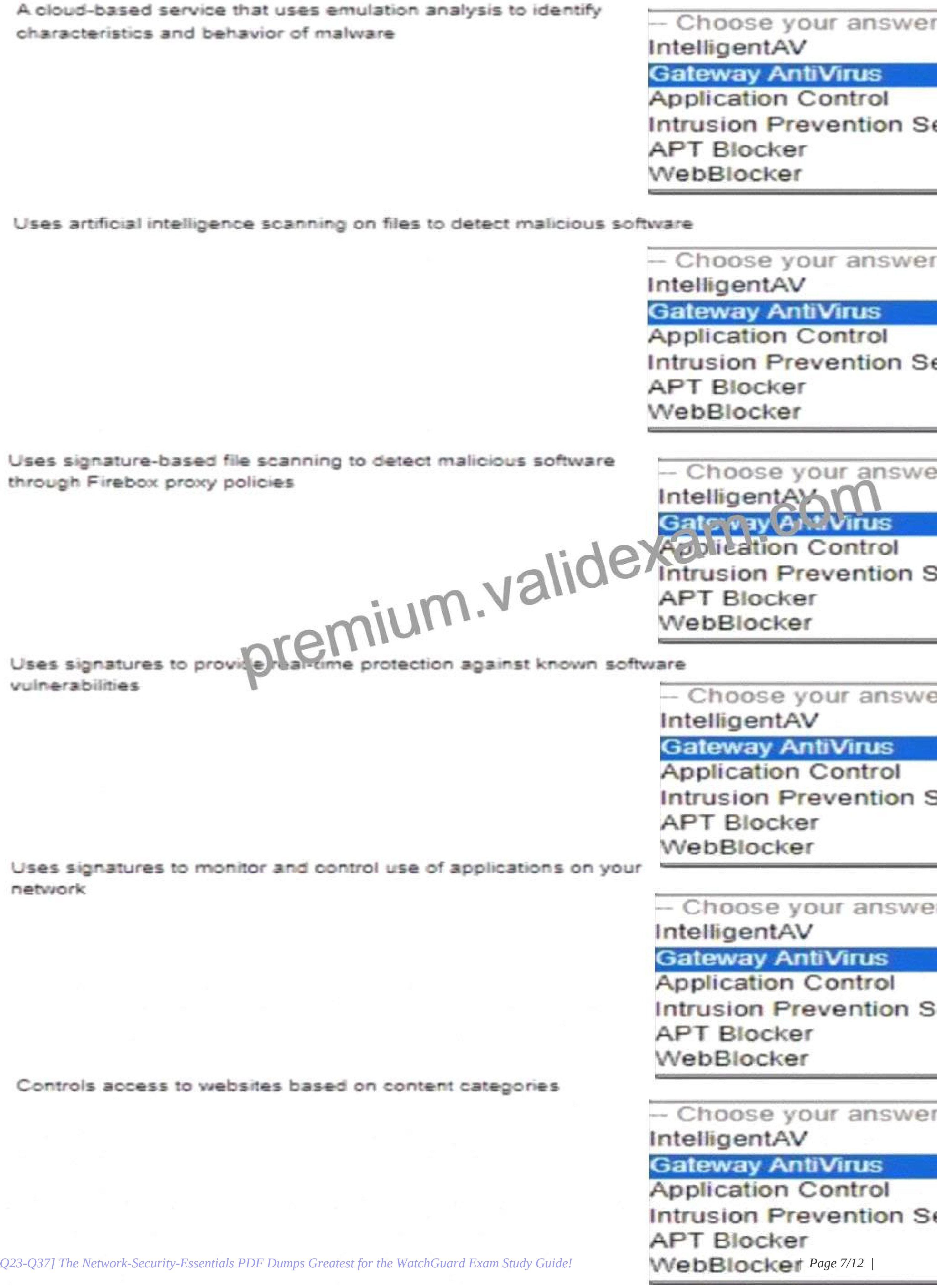
&#8220;O&#8221; or &#8220;-&#8220;) and do not conform to IP addressing standards.

QUESTION 32

What type of NAT enables clients on a private network to connect to servers on the Internet? (Select one.)
* Static NAT
* Dynamic NAT
* NAT loopback
* Hairpin NAT
Dynamic NAT enables clients on a private network to connect to servers on the Internet. By translating private IP addresses to a public IP address (or pool of addresses), Dynamic NAT allows multiple devices within a private network to access external resources on the Internet. This form of NAT is essential in conserving IP addresses and maintaining privacy for internal network topologies.

QUESTION 33

Match each WatchGuard Subscription Service with its function.



A cloud-based service that uses emulation analysis to identify characteristics and behavior of malware

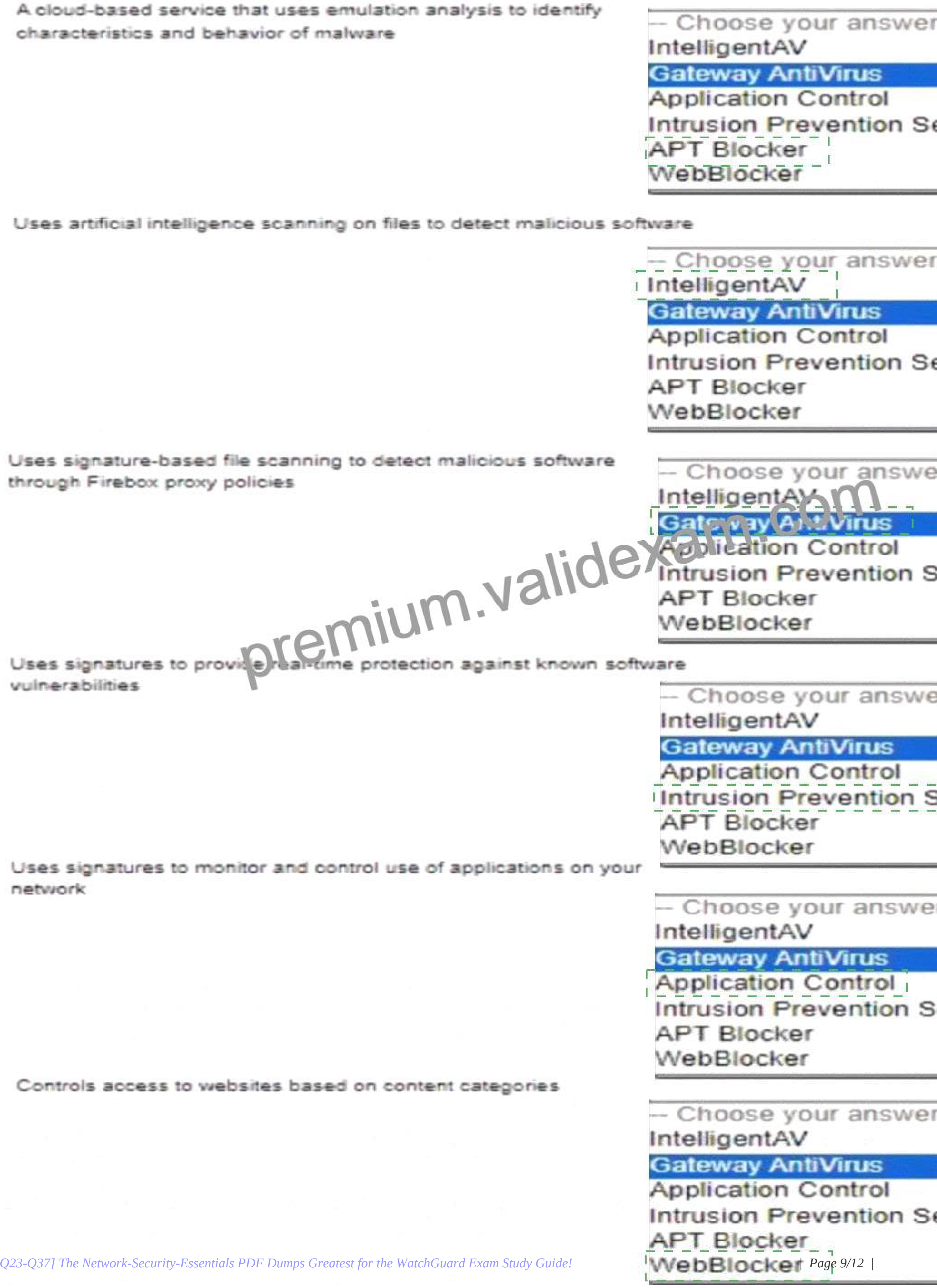
Uses artificial intelligence scanning on files to detect malicious software

Uses signature-based file scanning to detect malicious software through Firebox proxy policies

Uses signatures to provide real-time protection against known software vulnerabilities

Uses signatures to monitor and control use of applications on your network

Controls access to websites based on content categories



A cloud-based service that uses emulation analysis to identify characteristics and behavior of malware

- -- Choose your answer
- IntelligentAV
- Gateway AntiVirus
- Application Control
- Intrusion Prevention Se
- [✓ APT Blocker]
- WebBlocker

Uses artificial intelligence scanning on files to detect malicious software

- -- Choose your answer
- [✓ IntelligentAV]
- Gateway AntiVirus
- Application Control
- Intrusion Prevention Se
- APT Blocker
- WebBlocker

Uses signature-based file scanning to detect malicious software through Firebox proxy policies

- -- Choose your answe
- IntelligentAV
- [✓ Gateway AntiVirus]
- Application Control
- Intrusion Prevention S
- APT Blocker
- WebBlocker

Uses signatures to provide real-time protection against known software vulnerabilities

- -- Choose your answe
- IntelligentAV
- Gateway AntiVirus
- Application Control
- [✓ Intrusion Prevention S]
- APT Blocker
- WebBlocker

Uses signatures to monitor and control use of applications on your network

- -- Choose your answe
- IntelligentAV
- Gateway AntiVirus
- [✓ Application Control]
- Intrusion Prevention S
- APT Blocker
- WebBlocker

Controls access to websites based on content categories

- -- Choose your answer
- IntelligentAV
- Gateway AntiVirus
- Application Control
- Intrusion Prevention Se
- APT Blocker
- [✓ WebBlocker]

Explanation:

Here is the correct match for each WatchGuard Subscription Service and its function:

* A cloud-based service that uses emulation analysis to identify characteristics and behavior of malware : APT Blocker

* Uses artificial intelligence scanning on files to detect malicious software : IntelligentAV

* Uses signature-based file scanning to detect malicious software through Firebox proxy policies : Gateway AntiVirus

* Uses signatures to provide real-time protection against known software vulnerabilities : Intrusion Prevention Service

* Uses signatures to monitor and control use of applications on your network : Application Control

* Controls access to websites based on content categories : WebBlocker APT Blockeris a cloud-based, advanced threat detection service that performs behavioral analysis in a sandbox environment to identify sophisticated malware.

It focuses on identifying advanced persistent threats (APT) by observing their behavior in a controlled setting.

IntelligentAVleverages artificial intelligence to perform deep scanning and analysis of files to detect malware using predictive modeling techniques. This provides proactive protection by identifying previously unknown threats.

Gateway AntiVirusrelies on a signature-based detection mechanism to identify malware in real-time. It is used within Firebox&#8217;s proxy policies to scan file transfers, ensuring files containing known malware are blocked.

Intrusion Prevention Service (IPS)scans network traffic against a database of known vulnerabilities to detect and prevent exploitation attempts in real time. It protects against network-based attacks targeting known vulnerabilities.

Application Controlhelps in monitoring, managing, and enforcing the use of applications across the network using a signature-based approach. It provides visibility and control over applications to enhance productivity and security.

WebBlockeris a content filtering service that restricts access to websites based on their content categories. It helps enforce web usage policies and block access to inappropriate or harmful content.

QUESTION 34

What steps must you take to send log messages from a Firebox to WatchGuard Cloud? (Select two.)
* Enable WatchGuard Cloud in the Firebox configuration
* Add the FQDN of your WatchGuard Cloud account as a Log Server on the Firebox
* Define an Authentication Key that all your Fireboxes use to communicate with WatchGuard Cloud
* Configure Dimension to synchronize log messages with WatchGuard Cloud
* Use the WatchGuard Cloud Add Device wizard to add the Firebox to WatchGuard Cloud
* Enable WatchGuard Cloud in Firebox Configuration: To send log messages to WatchGuard Cloud, you need to activate WatchGuard Cloud integration within the Firebox&#8217;s configuration settings. This action prepares the device to communicate with WatchGuard Cloud and transfer log data.

* Use the WatchGuard Cloud Add Device Wizard: The Add Device wizard in WatchGuard Cloud is used to register and connect the Firebox to WatchGuard Cloud. This wizard guides administrators through the setup and ensures that the device is correctly

configured to send logs and other data to the cloud.

These steps are required to establish connectivity and ensure that log messages are sent to WatchGuard Cloud.

Other options, such as adding an FQDN or configuring Dimension synchronization, are not necessary for this task.

QUESTION 35

You have five public IP addresses available from your ISP. When you create a Static NAT action, you want to specify one of the public IP addresses for inbound traffic but do not see it in the IP address drop-down list.

How can you change the Firebox configuration to see additional public IP addresses in the Static NAT action?

(Select one.)
* Add secondary IP addresses to the external interface
* Configure 1-to-1 NAT for your entire subnet
* Add the public IP addresses to the From field of the policy that uses the Static NAT action
* Enable the Set Source IP option in the policy
* Add the IP addresses to the Dynamic NAT configuration

To use additional public IP addresses in a Static NAT action, you need to add them as secondary IP addresses to the external interface on the Firebox. By adding these IPs as secondary addresses, they become selectable options in the Static NAT configuration, allowing inbound traffic to be routed based on specific public IPs allocated by the ISP.

QUESTION 36

Your users have no network connectivity on their computers in the 10.0.40.0/24 network. You investigate and discover the DHCP address pool for this network is exhausted, but there are no available IP addresses in the network to assign. Which of these options can you use to expand the IP address space of this network? (Select two.)
* Change the IP address of the 10.0.40.1/24 network to 10.0.40.123/24
* Enable a wireless SSID for the 10.0.40.1/24 network
* Add 10.0.50.1/24 to the 10.0.40.1/24 network as a secondary network
* Create a Dynamic NAT rule for traffic from the 10.0.40.1/24 network going to the 10.0.50.1/24 network
* Bridge the 10.0.40.1/24 network across additional interfaces

* Adding a Secondary Network (10.0.50.1/24): By adding a secondary subnet (such as10.0.50.1/24) to the existing 10.0.40.1/24 network, you expand the IP address space, effectively increasing the number of available IP addresses for DHCP allocation.

* Bridging Across Additional Interfaces: Bridging the 10.0.40.1/24 network across multiple interfaces can also increase the available address pool by creating a larger logical network. This approach helps manage IP space across a broader range of devices without subnet fragmentation.

These methods provide scalable solutions to expand IP address availability within constrained network spaces.

QUESTION 37

Before packets are examined by Default Threat Protection, they are processed by firewall policies in top- down order.
* True
* False

In Firebox configuration, packets are processed by firewall policies in atop-down orderbefore they reach Default Threat Protection. This ordering ensures that the firewall policies defined higher in the policy list take precedence. Packets are evaluated against each rule sequentially from top to bottom until a matching policy is found, which then determines the action taken (allow, deny, or inspect further). Only after this process will any unfiltered traffic be subject to Default Threat Protection for additional security checks.

Network-Security-Essentials Certification All-in-One Exam Guide Jan-2025:
https://www.validexam.com/Network-Security-Essentials-latest-dumps.html]