DUMPSARENA

Fireware Essentials Exam

WatchGuard Essentials

Version Demo

Total Demo Questions: 10

Total Premium Questions: 104

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

A. Enable the AUTO-block sites that attempt to connect option in a deny policy.

B. Add the site to the Blocked Sites Exceptions list.

C. On the Firebox System Manager >Blocked Sites tab, select Add.

D. In Policy Manager, select Setup> Default Threat Protection > Blocked Sites and click Add.

ANSWER: A C D

Explanation:

Enabling the AUTO-block sites that attempt to connect option in a deny policy causes the Firebox to dynamically add a source host that attempts a prohibited connection to the temporary Blocked Sites list. This is useful for automatically limiting repeated unwanted connection attempts, and the block remains subject to the configured auto-block duration. On the Firebox System Manager >Blocked Sites tab, selecting Add is also a direct administrative method to place an address in the temporary blocked-sites list; administrators can use this view to manage currently blocked hosts. In Policy Manager, selecting Setup> Default Threat Protection > Blocked Sites and clicking Add creates a permanent blocked-site entry in the Firebox configuration. Permanent entries persist after a restart and remain in effect until an administrator removes them. Together, these actions cover both temporary runtime blocking and persistent policy-based blocking. WatchGuard documents the distinction between temporary and permanent blocked sites and the available management actions in its Blocked Sites documentation. The auto-block behavior is described in WatchGuard's Auto-block Sites documentation.

QUESTION NO: 2 - (SIMULATION)

Match each WatchGuard Subscription Service with its function:

ANSWER: Check the explanation for the answer

Explanation:

Match the services as follows:

WebBlocker — Controls and blocks web access by URL/category, such as social media, gambling, or malicious websites.
spamBlocker — Detects and blocks unsolicited/spam email messages.
Gateway AntiVirus — Scans allowed traffic and downloads for known viruses, malware, and other malicious content.
APT Blocker — Sends suspicious files to a cloud sandbox for analysis and blocks advanced/zero-day malware threats.
Application Control — Identifies applications in traffic and allows, blocks, or restricts their use.
Quarantine Server — Holds email identified as spam so users or administrators can review, release, or delete it.
Intrusion Prevention Service (IPS) — Detects and blocks network attacks, exploits, protocol attacks, and intrusion attempts.
Data Loss Prevention (DLP) — Prevents sensitive information, such as credit-card numbers or other defined data patterns, from leaving the organization.
Reputation Enabled Defense (RED) — Uses cloud reputation information to identify and block connections to websites or hosts with known bad/malicious reputations.

QUESTION NO: 3

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 Authen...	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

Explanation:

The default Outgoing policy has been removed and there is no policy to allow DNS traffic. This is the likely cause because users must resolve Internet host names to IP addresses before their browsers can connect to websites. HTTP-proxy and HTTPS-proxy policies permit web traffic after a client has an address to contact, but they do not inherently permit DNS queries. If the standard Outgoing policy was removed, its broad outbound access no longer provides a path for DNS. The configuration must therefore include an explicit DNS policy that permits clients on the trusted network to reach the organization's intended DNS resolver, typically using UDP port 53 and, where needed, TCP port 53. The resolver might be an external DNS server or an internal DNS server that performs recursive lookups on behalf of clients. Once DNS is allowed and correctly directed, users can translate website names into addresses and the existing web proxy policies can process their HTTP and HTTPS connections. WatchGuard documents DNS as a separate policy type with its own protocol and ports, and documents that policies control the traffic allowed through a Firebox: WatchGuard DNS policy documentation and WatchGuard policy overview.

QUESTION NO: 4

You can use Firebox-DB authentication with any type of Mobile VPN.

A. True

B. False

ANSWER: A

Explanation:

True is correct. Firebox-DB is the Firebox's internal authentication database, where an administrator can create and manage local user accounts and groups directly on the device. WatchGuard supports Firebox-DB as an authentication source for its Mobile VPN implementations, enabling locally defined users to authenticate without requiring an external Active Directory, LDAP, or RADIUS server. This makes Firebox-DB particularly useful for smaller deployments, temporary remote-access users, or environments where an external identity service is unavailable.

When a Mobile VPN user connects, the Firebox validates the supplied credentials against the configured authentication server. If Firebox-DB is selected, it checks the local database and can apply group-based access controls and policies to the authenticated user. The Firebox-DB documentation specifically identifies Mobile VPN connections among the supported uses for local Firebox database authentication. Administrators must still create the required users or groups and select Firebox-DB in the relevant Mobile VPN authentication configuration.

For details, see WatchGuard's About Firebox-DB Authentication documentation and its Mobile VPN overview.

QUESTION NO: 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

ANSWER: A D

Explanation:

In a default Firebox configuration, **WatchGuard** and **WatchGuard Web UI** are the predefined policies used to govern administrative connections to the Firebox itself. The WatchGuard policy permits management traffic used by WatchGuard System Manager and Policy Manager, enabling an administrator to connect with WatchGuard management tools. The WatchGuard Web UI policy permits HTTPS-based administrative access to Fireware Web UI, which is the browser interface used to configure and monitor the appliance.

These policies are device-management policies rather than ordinary transit policies: their purpose is to control services addressed to the Firebox, and administrators can edit their From criteria to restrict which trusted networks, hosts, or other sources may manage the device. Fireware's policy documentation describes these as predefined management policies and identifies the management services that Firebox policies can control. Maintaining appropriately restricted source settings for both policies is an important part of limiting administrative access to authorized users and networks.

For details, see the WatchGuard documentation on policies and the WatchGuard documentation on Firebox management access.

QUESTION NO: 6

You want the Firebox to relay DHCP requests from clients on an optional network to a DHCP server on another network. Which actions are required? (Select three.)

A. Enable DHCP relay on the interface that receives client requests.

B. Specify the IP address of the DHCP server.

C. Configure a DHCP scope for the client subnet on the DHCP server.

D. Enable dynamic NAT for the client subnet.

E. Configure the Firebox as the DHCP server for the same interface.

ANSWER: A B C

Explanation:

To relay DHCP requests, you must **enable DHCP relay on the interface where the client requests arrive**, **specify the IP address of the DHCP server**, and **configure the DHCP server with a scope for the client subnet**. The Firebox receives the client broadcast on the local interface and forwards the request as a unicast message to the configured DHCP server.

The DHCP server must have a scope that matches the subnet of the interface that receives the DHCP request. This enables the server to assign an appropriate address, subnet mask, gateway, and other DHCP options to the requesting client. DHCP relay is useful when a centralized DHCP server provides addresses for multiple routed networks. For more information, see Configure DHCP Relay.

QUESTION NO: 7

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.)

A. 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.

B. Replace the Firebox certificate with the trusted certificate from your web server.

C. Add the user accounts for your users who use the Authentication Portal to a list of trusted users on your Firebox.

D. Instruct them to disable security warning message in their preferred browsers.

ANSWER: A

Explanation:

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. This ensures that the HTTPS certificate presented by the Firebox Authentication Portal is trusted by the client. Browser warnings occur when the portal certificate cannot be validated, such as when it is self-signed and its issuing authority is not in the browser or operating system trust store, or when its name does not match the portal address users enter. A certificate issued by a public or organizationally trusted certificate authority avoids the warning when it is installed on the Firebox and issued for the correct DNS name. A self-signed certificate can also be used in a managed environment, provided its certificate or issuing authority is deployed to every client's trusted certificate store. The Firebox must use the certificate for the Authentication Portal, and users should access the portal with the hostname covered by that certificate. WatchGuard documents how to configure certificates for Firebox services and authentication-related web access in the Fireware certificate documentation. For certificate trust behavior in browsers, see the Mozilla certificate guidance.

QUESTION NO: 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.

ANSWER: B C

Explanation:

Dimension can aggregate reporting data from multiple managed Fireboxes when those devices are represented as a device group. Creating a device group and viewing reports for that group provides a single reporting scope, so Dimension combines the applicable log-message data from every member Firebox into the group-level report. This is useful for reporting on a site, department, customer, or other logical collection of Fireboxes without having to review each appliance separately.

A report schedule can also be configured to include the required devices, typically by selecting the relevant device group as the report source. When Dimension runs the scheduled report, it uses that multi-device scope and generates one report containing the aggregated data for the selected Fireboxes. This enables recurring delivery of consolidated security, traffic, and activity reporting while retaining the group as the common reporting context. Device groups therefore provide the organizational and aggregation mechanism, and report schedules provide the automated generation and distribution mechanism for the consolidated report. WatchGuard's documentation resources for Dimension and Fireware reporting are available at WatchGuard Documentation and WatchGuard Dimension Help.

QUESTION NO: 9

To use the Web Setup Wizard or Quick Setup Wizard to configure your Firebox or XTM device, your computer must have an IP address on which subnet? (Select one.)

A. 10.0.10.0/24

B. 10.0.1.0/24

C. 172.16.10.0/24

D. 192.168.1.0/24

ANSWER: B

Explanation:

The correct subnet is **10.0.1.0/24**. A new or factory-default Firebox/XTM appliance uses its trusted interface with the default IPv4 address **10.0.1.1/24**. To reach the appliance's initial management interface and launch the Web Setup Wizard or Quick Setup Wizard, the administrator's computer must therefore be connected to a trusted interface and configured with an unused address in that same Layer 3 network, such as 10.0.1.2 with subnet mask 255.255.255.0. Devices in this /24 subnet can directly communicate with the Firebox at its default trusted-interface address, allowing the browser-based setup process to begin. During the wizard, the administrator can replace the default trusted-network addressing and configure the remaining network, security, and Internet settings appropriate for the deployment. WatchGuard's installation guidance identifies 10.0.1.1 as the default Firebox trusted-interface IP address and instructs administrators to use a computer on the 10.0.1.0/24 network for initial configuration. See the WatchGuard Fireware installation documentation and the WatchGuard product documentation portal for device documentation and lifecycle resources.

QUESTION NO: 10

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.)

A. Configure a host name for update.example.com.

B. Configure an FQDN for *.example.com.

C. Add IP addresses that correspond to each software update server in the domain.

D. Create an alias for all subdomains and known IP addresses for example.com.

ANSWER: B

Explanation:

Configure an FQDN for *.example.com. This is the appropriate destination definition because the update service is distributed across multiple subdomains and uses dynamically assigned content-delivery-network addresses. A wildcard FQDN object lets the Firebox match hosts beneath the example.com domain without requiring separate policy objects for every update hostname. It also avoids relying on a static list of destination IP addresses, which is not sustainable when the provider changes CDN endpoints.

Fireware resolves FQDN objects through DNS and maintains the resolved addresses for policy matching. With a wildcard FQDN, the Firebox can apply the HTTP-proxy policy to destinations such as update.example.com, downloads.example.com, or regional service hostnames under the same domain, as they are encountered and resolved. This makes the policy more resilient to service infrastructure changes while keeping the permitted destination scope tied to the organization's domain namespace. The HTTP proxy can then inspect and enforce HTTP-proxy actions for connections that match the policy. See WatchGuard's Configure FQDN Addresses documentation and its About HTTP Proxy Policies documentation for details.