DUMPSARENA

Network Security Essentials for Locally-Managed Fireboxes

WatchGuard Network-Security-Essentials

Version Demo

Total Demo Questions: 4

Total Premium Questions: 47

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Fundamentals	4
Topic 2, Firebox Configuration	3
Topic 3, Network Configuration	6
Topic 4, Firewall Policies	6
Topic 5, Network Address Translation	4
Topic 6, Security Services	6
Topic 7, VPNs	5
Topic 8, Network Monitoring	13
Total	47

QUESTION NO: 1

An administrator investigates a policy issue on a locally-managed Firebox and needs to determine both the policy decision recorded by the Firebox and whether packets are actually leaving a specified interface. Which two tools provide this information? (Select two.)

A. Traffic Monitor

B. TCP Dump Diagnostic Task

C. Policy Manager

D. FireWatch

E. Feature Key Synchronization

ANSWER: A B

Explanation:

Traffic Monitor displays Firebox log messages, including policy allow and deny decisions and security-service events. **TCP Dump** captures packets on selected Firebox interfaces and can show whether the expected traffic enters or leaves an interface. Together, these tools help distinguish a policy-processing issue from a routing, NAT, or host-response issue. Policy Manager is used to configure policies, but it does not provide packet capture or real-time traffic-log analysis. FireWatch is useful for connection visibility, but it is not a replacement for packet-level capture.

QUESTION NO: 2

When you configure a Branch Office VPN tunnel to a third-party device, AES-GCM encryption is recommended for:

A. Better performance and throughput when supported by both VPN endpoints

B. Troubleshooting purposes

C. Better uptime because of additional keep-alive options

D. Routing over a BOVPN

E. Connections to third-party firewalls only

ANSWER: A

Explanation:

Better performance and throughput when supported by both VPN endpoints is correct because AES-GCM is an authenticated-encryption algorithm designed to provide confidentiality and integrity efficiently in a single cryptographic operation. In an IPsec Branch Office VPN tunnel, this can reduce processing overhead compared to configurations that use a separate encryption algorithm and integrity/authentication algorithm. The result can be higher throughput and more efficient use of the Firebox and peer device resources, which is particularly valuable for site-to-site traffic.

For a tunnel to a third-party device, both peers must support AES-GCM and must be configured with compatible IKE and IPsec proposal settings. WatchGuard documentation specifically recommends AES-GCM for improved BOVPN performance when it is available on both ends of the tunnel. The exact usable proposal also depends on the Fireware version and the capabilities/configuration of the third-party VPN gateway. AES-GCM selection is therefore a performance and cryptographic-efficiency decision, while interoperability still requires matched settings between the Firebox and the remote endpoint.

See WatchGuard's About Manual BOVPN Tunnels and Configure a Manual BOVPN Tunnel.

QUESTION NO: 3

A company allows users on a trusted network to download software updates from Internet web servers. The administrator wants Gateway AntiVirus to examine files transferred with unencrypted HTTP before they reach the users. Which policy type should the administrator use?

A. An HTTP-proxy policy with Gateway AntiVirus enabled

B. An HTTP packet filter policy with Dynamic NAT enabled

C. An Outgoing packet filter policy with Application Control enabled

D. An FTP-proxy policy with Gateway AntiVirus enabled

ANSWER: A

Explanation:

An **HTTP-proxy policy** is correct because an HTTP proxy can inspect HTTP requests and responses at the application layer and apply security services such as Gateway AntiVirus to supported downloaded content. A TCP-UDP packet filter can allow or deny traffic by protocol and port, but it does not provide the same HTTP content-inspection context required for Gateway AntiVirus scanning of web downloads.

QUESTION NO: 4 - (SIMULATION)

Match the "network server to the protocol and port it uses."

ANSWER: See the explanation for the answer

Explanation:

Match each network server/protocol to its standard transport protocol and port:

DHCP — `UDP/67, UDP/68`
SMTP — `TCP/25`
DNS — `UDP/53`
HTTPS — `TCP/443`
HTTP — `TCP/80`

DHCP uses UDP 67 for the server and UDP 68 for clients. DNS normally uses UDP 53 for name queries. SMTP uses TCP 25, while web traffic uses TCP 80 for HTTP and TCP 443 for HTTPS.