ESSENTIALS$^{Q\&As}$

Fireware Essentials Exam

Pass WatchGuard ESSENTIALS Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/essentials.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by WatchGuard Official Exam Center

QUESTION 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.

Correct Answer: ACD

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

QUESTION 2

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

A. True

B. False

Correct Answer: A

QUESTION 3

If your Firebox has a single public IP address, and you want to forward inbound traffic to internal hosts based on the destination port, which type of NAT should you use? (Select one.)

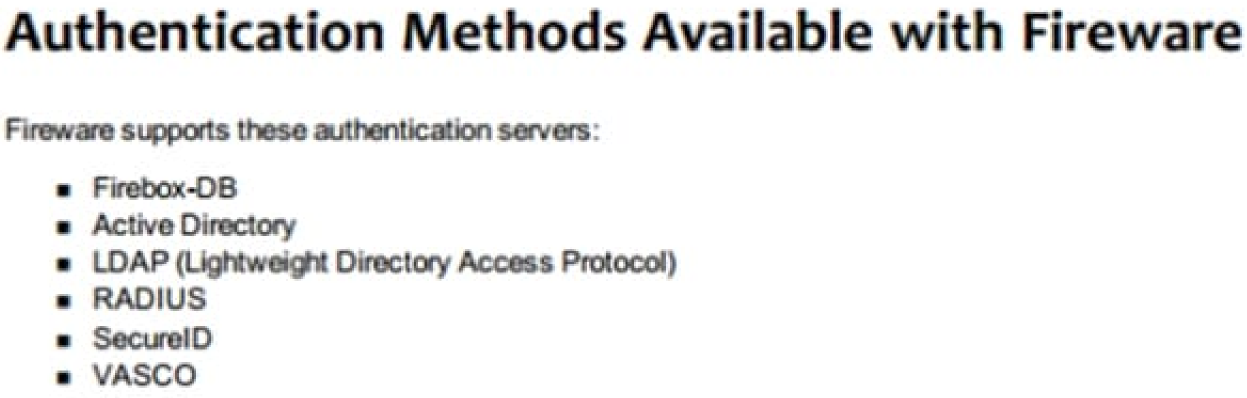
A. Static NAT

B. 1-to-1 NAT

C. Dynamic NAT

Correct Answer: B

QUESTION 4



Authentication Methods Available with Fireware

Fireware supports these authentication servers:

- Firebox-DB
- Active Directory
- LDAP (Lightweight Directory Access Protocol)
- RADIUS
- SecureID
- VASCO

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.

Correct Answer: A

QUESTION 5

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

Correct Answer: I

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