Vendor: Fortinet

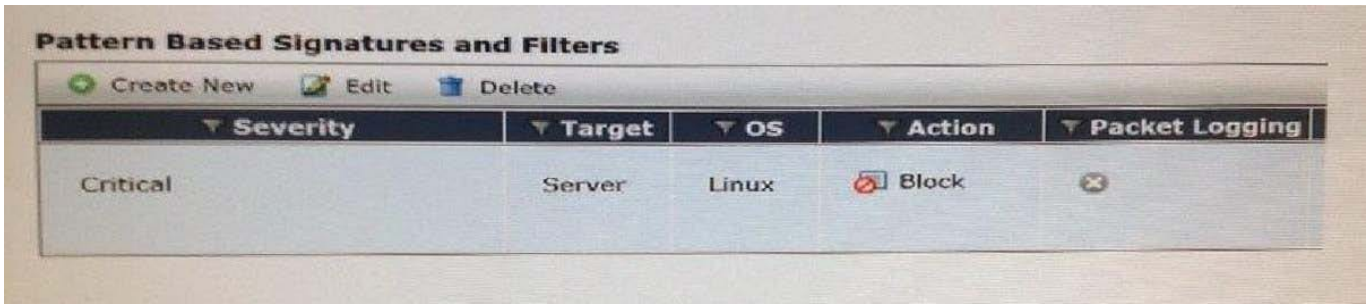
Exam Code:NSE4

Exam Name: Fortinet Network Security Expert 4 Written Exam (400)

Version: Demo

QUESTION 1

Review the IPS sensor filter configuration shown in the exhibit.



Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

A. It does not log attacks targeting Linux servers.

B. It matches all traffic to Linux servers.

C. Its action will block traffic matching these signatures.

D. It only takes affect when the sensor is applied to a policy.

Correct Answer: CD

QUESTION 2

Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

A. SSH

B. Telnet

C. NTLM

D. HTTPS

Correct Answer: AD

QUESTION 3

Regarding tunnel-mode SSL VPN, which three statements are correct? (Choose three.)

A. Split tunneling is supported.

B. It requires the installation of a VPN client.

C. It requires the use of an Internet browser.

D. It does not support traffic from third-party network applications.

E. An SSL VPN IP address is dynamically assigned to the client by the FortiGate unit.

Correct Answer: ABE

QUESTION 4

Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.

B. It can dynamically assign DNS settings to IPsec VPN clients.

C. It uses the ESP protocol.

D. It can be enabled in the phase 2 configuration.

Correct Answer: AB

QUESTION 5

Which TCP states does the global setting `tcp-half-open-timer\\' applies to? (Choose two.)

A. SYN SENT

B. SYN and SYN/ACK

C. FIN WAIT

D. TIME WAIT

Correct Answer: AD

QUESTION 6

What methods can be used to deliver the token code to a user that is configured to use two-factor authentication? (Choose three.)

A. Browser pop-up window.

B. FortiToken.

C. Email.

D. Code books.

E. SMS phone message.

Correct Answer: BCE

QUESTION 7

Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

A. It must be signed by a "trusted" CA

B. It must be listed as valid in a Certificate Revocation List (CRL)

C. The CA field must be "TRUE"

D. It must be still within its validity period

Correct Answer: AD

QUESTION 8

Examine the following spanning tree configuration on a FortiGate in transparent mode:

```
config system interface
edit
set stp-forward enable
end
```

Which statement is correct for the above configuration?

A. The FortiGate participates in spanning tree.

B. The FortiGate device forwards received spanning tree messages.

C. Ethernet layer-2 loops are likely to occur.

D. The FortiGate generates spanning tree BPDU frames.

Correct Answer: B

QUESTION 9

What types of troubleshooting can you do when uploading firmware? (Choose two.)

A. Investigate corrupted firmware

B. Investigate current runtime state

C. Investigate damaged hardware

D. Investigate configuration history

Correct Answer: AD

QUESTION 10

If you have lost your password for the "admin" account on your FortiGate, how should you reset it?

A. Log in with another administrator account that has "super_admin" profile permissions, then reset the password for the "admin" account.

B. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmware. Then you can log in with the default password.

C. Power off the FortiGate. After several seconds, restart it. Via the local console, within 30 seconds after booting has completed, log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

D. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

Correct Answer: C

QUESTION 11

What is IPsec Perfect Forwarding Secrecy (PFS)?

A. A phase-1 setting that allows the use of symmetric encryption.

B. A phase-2 setting that allows the recalculation of a new common secret key each time the session key expires.

C. A `key-agreement\\' protocol.

D. A `security-association- agreement\\' protocol.

Correct Answer: B

QUESTION 12

What log type would indicate whether a VPN is going up or down?

A. Event log

B. Security log

C. Forward log

D. Syslog

Correct Answer: A