

Fortinet

Exam NSE4

Fortinet Network Security Expert 4

Verson: Demo

[Total Questions: 10]

Question No : 1

Which methods can FortiGate use to send a One Time Password (OTP) to Two-Factor Authentication users? (Choose three.)

- A. Hardware FortiToken
- B. Web Portal
- C. Email
- D. USB Token
- E. Software FortiToken (FortiToken mobile)

Answer: A,C,E

Question No : 2

How can DLP file filters be configured to detect Office 2010 files?

- A. File Type. Microsoft Office(msoffice)
- B. File Type. Archive(zip)
- C. File Type. Unknown Filetype(unknown)
- D. File Name. "*.ppt", "*.doc", "*.xls"
- E. File Name. "*.pptx", "*.docx", "*.xlsx"

Answer: B,E

Question No : 3

Which best describe the mechanism of a TCP SYN flood?

- A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
- B. The attacker sends a packet designed to "sync" with the FortiGate.
- C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
- D. The attacker starts many connections, but never acknowledges to fully form them.

Answer: D

Question No : 4

Which network protocols are supported for administrative access to a FortiGate unit?
(Choose three.)

- A. SMTP
- B. WINS
- C. HTTP
- D. Telnet
- E. SSH

Answer: C,D,E

Question No : 5

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE.
Exhibit A shows the command output of diagnose sys session stat for the STUDENT device. Exhibit B shows the command output of diagnose sys session stat for the REMOTE device.

Exhibit A:

```
STUDENT # diagnose sys session stat
misc info:      session_count=166 setup_rate=68 exp_count=0 clash=0
                memory_tension_drop=0 ephemeral=0/57344 removeable=0 ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
    8 in ESTABLISHED state
    3 in SYN_SENT state
    1 in FIN_WAIT state
   139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
    syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
REMOTE # diagnose sys session stat
misc info:      session_count=11 setup_rate=0 exp_count=0 clash=4
memory_tension_drop=0 ephemeral=0/57344 removeable=0 ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
      2 in ESTABLISHED state
      1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
      syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

- A. STUDENT is likely to be the master device.
- B. Session-pickup is likely to be enabled.
- C. The cluster mode is active-passive.
- D. There is not enough information to determine the cluster mode.

Answer: A,D

Question No : 6

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent.
- B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.
- C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate in this manner because each

domain controller agent requires a dedicated collector agent.

Answer: A,C

Question No : 7

Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

- A. Antivirus (flow based)
- B. Web filtering (PROXY BASED)
- C. Intrusion Protection
- D. Application Control
- E. Endpoint control

Answer: A,B,D

Question No : 8

Which best describes the authentication timeout?

- A. How long FortiGate waits for the user to enter his or her credentials.
- B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
- C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
- D. How long a user-authenticated session can exist without having to authenticate again.

Answer: C

Question No : 9

What is the FortiGate password recovery process?

- A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.
- B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.

C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.

D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

Answer: B

Question No : 10

Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

A. Antivirus

B. VPN

C. IPS

D. Web Filtering

Answer: D