Fortinet

NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

Latest Version: 6.0

Question: 1

What is the common feature shared between IPv4 and SD-WAN ECMP algorithms?

A. Both support volume algorithms.
B. Both can be enabled at the same time.
C. Both use the same physical interface load balancing settings.
D. Both control ECMP algorithms.

Answer: D

Question: 2

What is eXtended Authentication (XAuth)?

A. It is an IPsec extension that forces remote VPN users to authenticate using their credentials (username and password).
B. It is an IPsec extension that authenticates remote VPN peers using a pre-shared key.
C. It is an IPsec extension that forces remote VPN users to authenticate using their local ID.
D. It is an IPsec extension that authenticates remote VPN peers using digital certificates.

Answer: A

Question: 3

Which two statements about incoming and outgoing interfaces in firewall policies are true? (Choose two.)

A. An incoming interface is mandatory in a firewall policy, but an outgoing interface is optional.
B. A zone can be chosen as the outgoing interface.
C. Multiple interfaces can be selected as incoming and outgoing interfaces.
D. Only the any interface can be chosen as an incoming interface.

Answer: B,C

Question: 4

Which type of traffic inspection requires FortiGate to act as a CA?

A. SSL certificate inspection when protecting multiple clients connecting to multiple servers.
B. SSL traffic inspection when protecting a local SSL server.
C. SSL traffic inspection when protecting multiple clients connecting to multiple servers.
D. SSL certificate inspection when protecting a local SSL server.

Answer: C

Question: 5

Which two statements about advanced AD access mode for the FSSO collector, agent are true?
(Choose two.)

A. It supports monitoring of nested groups.
B. It is only supported if DC agents are deployed.
C. FortiGate can act as an LDAP client to configure the group filters.
D. It uses the Windows convention for naming; that is, Domain\Username.

Answer: A,C

Question: 6

Which statement about firewall policy NAT is true?

A. DNAT is not supported.
B. You must configure SNAT for each firewall policy.
C. DNAT can automatically apply to multiple firewall policies, based on DNAT rules.
D. SNAT can automatically apply to multiple firewall policies, based on SNAT policies.

Answer: B

Question: 7

Which three settings and protocols can be used to provide secure and restrictive administrative access to FortiGate?
(Choose three.)

A. SSH
B. FortiTelemetry
C. HTTPS
D. Trusted authentication

E. Trusted host

Answer: A,C,E

Question: 8

Which two statements correctly describe the differences between IPsec main mode and IPsec aggressive mode?
(Choose two.)

A. The first packet of aggressive mode contains the peer ID, while the first packet of main mode does not.
B. Main mode cannot be used for dialup VPNs, while aggressive mode can.
C. Aggressive mode supports XAuth, while main mode does not.
D. Six packets are usually exchanged during main mode, while only three packets are exchanged during aggressive mode.

Answer: A,D

Question: 9

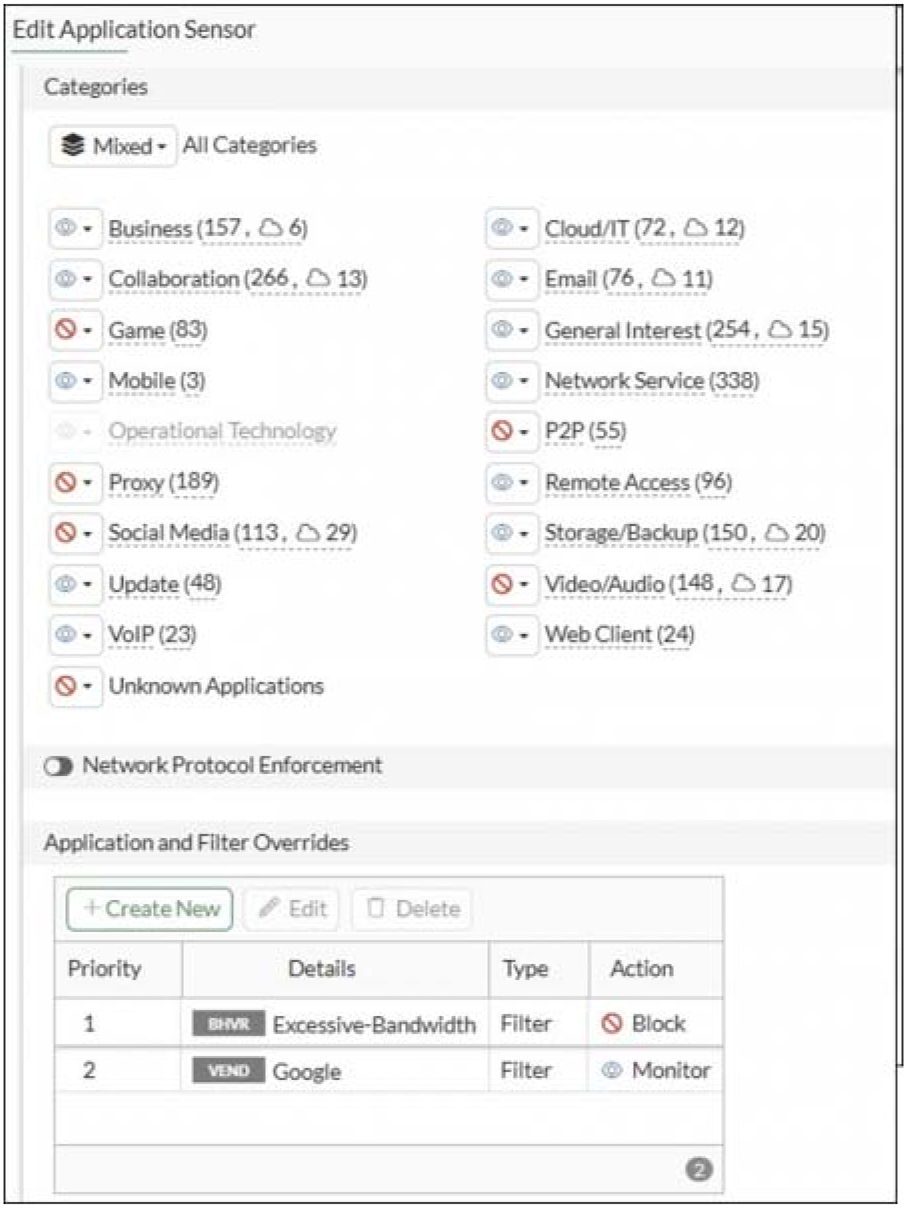
Which two IP pool types are useful for carrier-grade NAT deployments?
(Choose two.)

A. One-to-one
B. Overload
C. Fixed port range
D. Port block allocation

Answer: C,D

Question: 10

Refer to the exhibits.



Edit Application Sensor

Categories

Mixed ▾ All Categories

- ⊘ ▾ Game (83)
- 👁 ▾ Business (157, ☁ 6)
- 👁 ▾ Collaboration (266, ☁ 13)
- 👁 ▾ Mobile (3)
- 👁 ▾ Operational Technology
- ⊘ ▾ Proxy (189)
- ⊘ ▾ Social Media (113, ☁ 29)
- 👁 ▾ Update (48)
- 👁 ▾ VoIP (23)
- ⊘ ▾ Unknown Applications
- 👁 ▾ Cloud/IT (72, ☁ 12)
- 👁 ▾ Email (76, ☁ 11)
- 👁 ▾ General Interest (254, ☁ 15)
- 👁 ▾ Network Service (338)
- ⊘ ▾ P2P (55)
- 👁 ▾ Remote Access (96)
- 👁 ▾ Storage/Backup (150, ☁ 20)
- ⊘ ▾ Video/Audio (148, ☁ 17)
- 👁 ▾ Web Client (24)

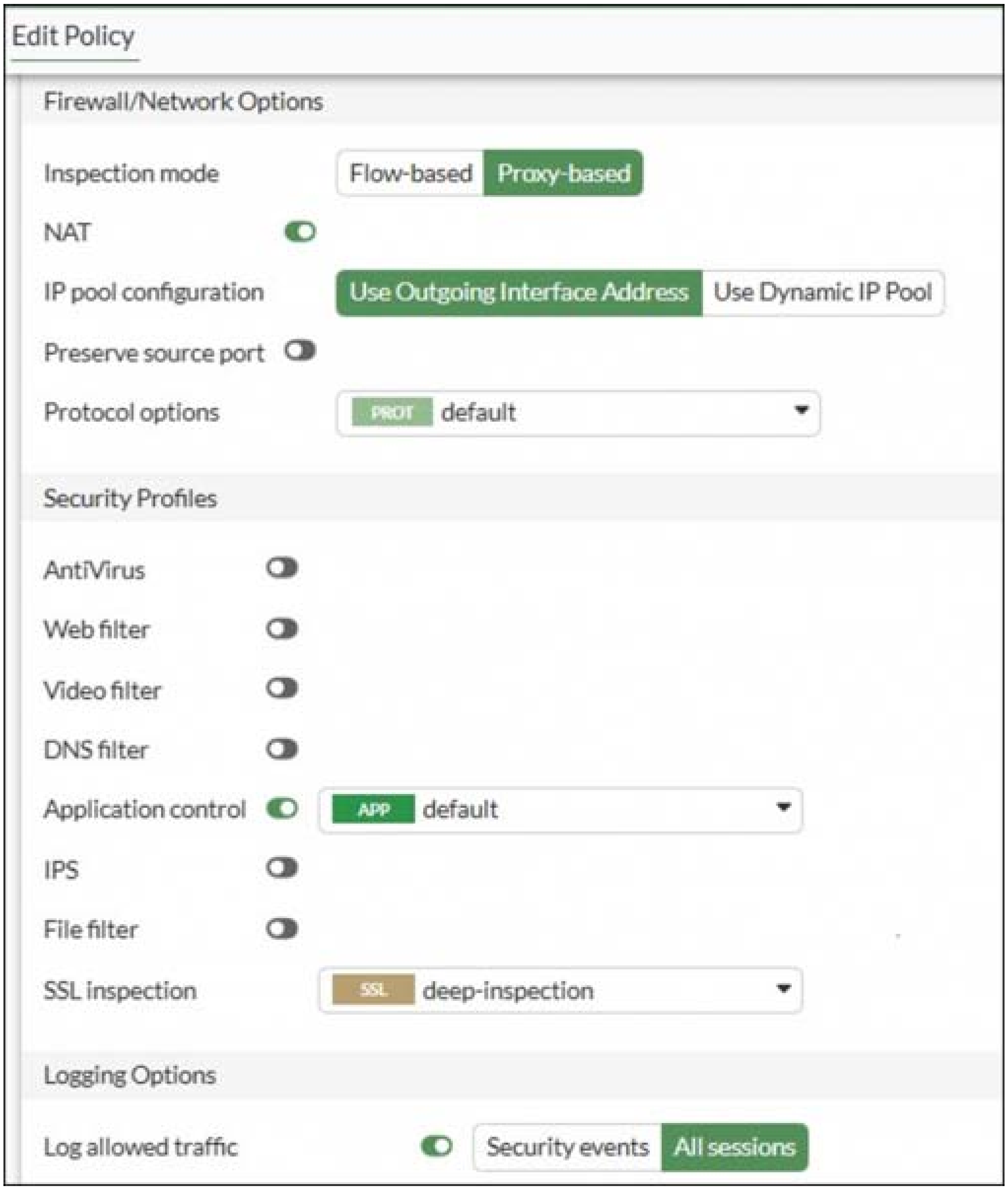
○ Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Google	Filter	👁 Monitor

2



Edit Policy

Firewall/Network Options

Inspection mode: Flow-based [✓ Proxy-based]

NAT ●

IP pool configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve source port ○

Protocol options: PROT default

Security Profiles

AntiVirus ○

Web filter ○

Video filter ○

DNS filter ○

Application control ● APP default

IPS ○

File filter ○

SSL inspection: SSL deep-inspection

Logging Options

Log allowed traffic ● Security events [✓ All sessions]

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access
What would you do to resolve this issue?

A. Move up Google in the Application and Filter Overrides section to set its priority to 1.
B. Change Inspection mode to Flow-based.
C. Set SSL inspection to certificate-inspection.
D. Add *Google*.com to the URL category in the security profile.

Answer: B