Fortinet

NSE4_FGT-6.2 Exam

Fortinet NSE 4 - FortiOS 6.2 Exam

Question: 1

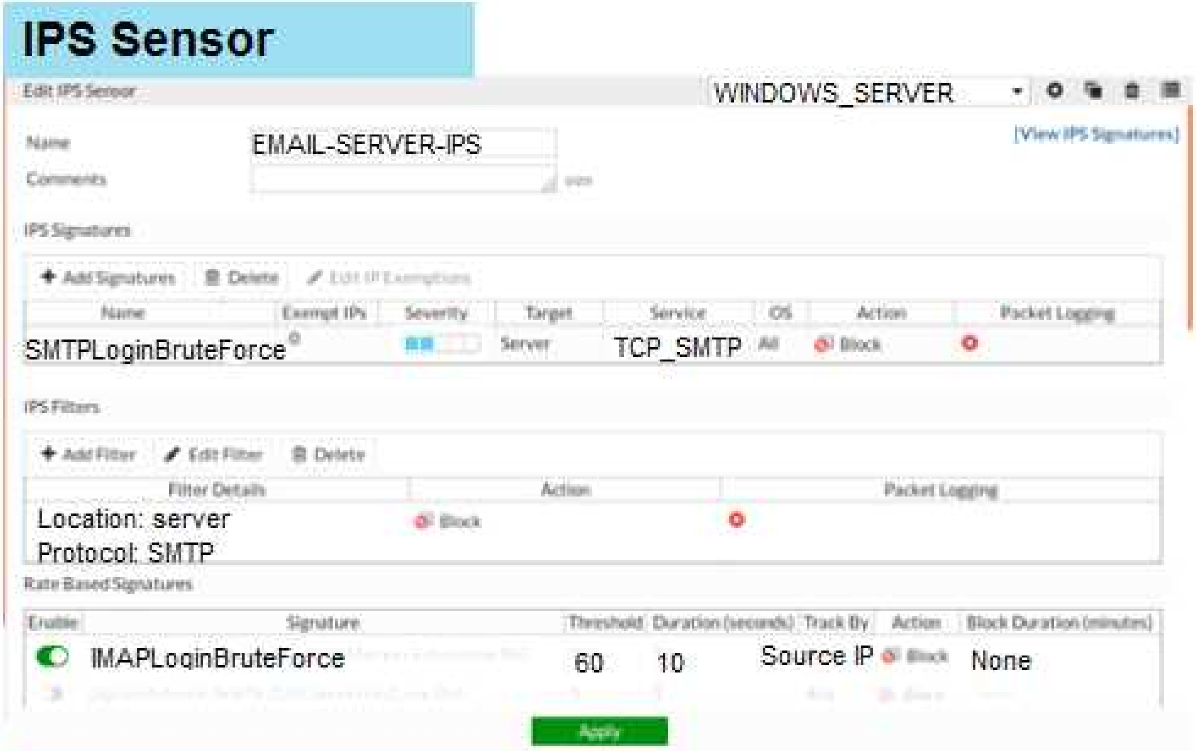
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Answer: A,C

Question: 2

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



IPS Sensor

Edit IPS Sensor

WINDOWS_SERVER

[View IPS Signatures]

Name: EMAIL-SERVER-IPS

Comments:

IPS Signatures

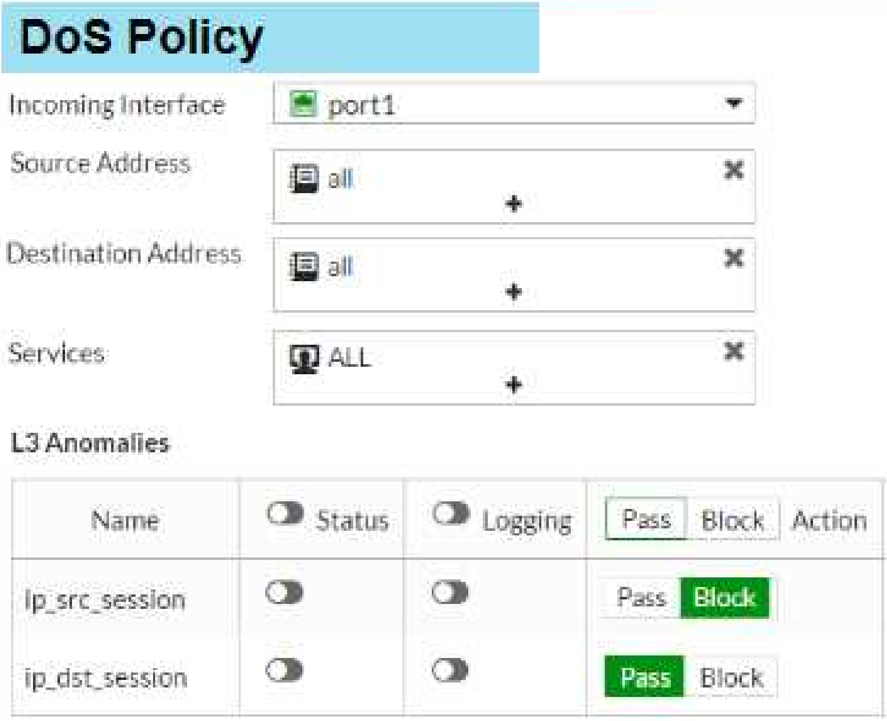
Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce			Server	TCP_SMTP	All	Block	●

IPS Filters

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	●

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
●	IMAPLoginBruteForce	60	10	Source IP	Block	None



DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

L3 Anomalies

Name	Status	Logging	Action
ip_src_session	○	○	Pass [✓ Block]
ip_dst_session	○	○	[✓ Pass] Block

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force
B. IMAP.Login.brute.Force
C. ip_src_session
D. Location: server Protocol: SMTP

Answer: B

Question: 3

An administrator wants to configure a FortiGate as a DNS server. FotiGate must use a DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS methods must you use?

A. Recursive
B. Non-recursive
C. Forward to primary and secondary DNS
D. Forward to system DNS

Answer: A

Question: 4

Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.

Answer: C

Question: 5

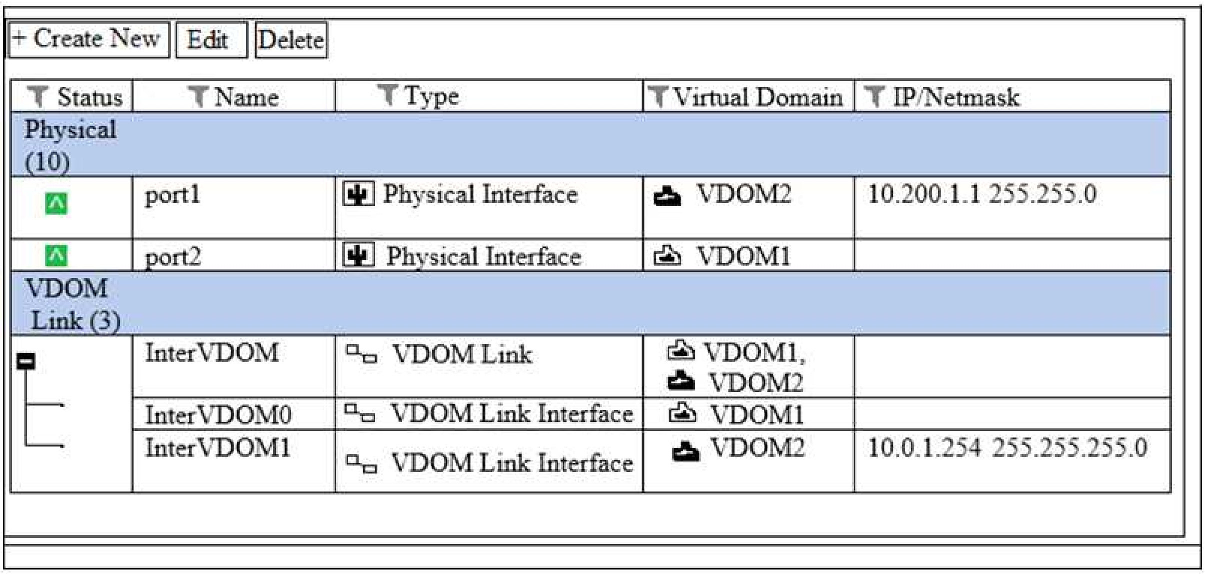
If the Services field is configured in a Virtual IP (VIP), which of the following statements is true when central NAT is used?

A. The Services field removes the requirement of creating multiple VIPs for different services.
B. The Services field is used when several VIPs need to be bundled into VIP groups.
C. The Services field does not allow source NAT and destination NAT to be combined in the same policy.
D. The Services field does not allow multiple sources of traffic, to use multiple services, to connect to a single computer.

Answer: A

Question: 6

View the exhibit.



Status	Name	Type	Virtual Domain	IP/Netmask
Physical (10)				
▲	port1	Physical Interface	VDOM2	10.200.1.1 255.255.0
▲	port2	Physical Interface	VDOM1	
VDOM Link (3)				
	InterVDOM	VDOM Link	VDOM1, VDOM2	
	InterVDOM0	VDOM Link Interface	VDOM1	
	InterVDOM1	VDOM Link Interface	VDOM2	10.0.1.254 255.255.255.0

VDOM1 is operating in transparent mode VDOM2 is operating in NAT Route mode. There is an inteface VDOM link between both VDOMs. A client workstation with the IP address 10.0.1.10/24 is connected to port2. A web server with the IP address 10.200.1.2/24 is connected to port1.

What is required in the FortiGate configuration to route and allow connections from the client workstation to the web server? (Choose two.)

A. A static or dynamic route in VDOM2 with the subnet 10.0.1.0/24 as the destination.
B. A static or dynamic route in VDOM1 with the subnet 10.200.1.0/24 as the destination.
C. One firewall policy in VDOM1 with port2 as the source interface and InterVDOM0 as the destination interface.
D. One firewall policy in VDOM2 with InterVDOM1 as the source interface and port1 as the destination interface.

Answer: C

Question: 7

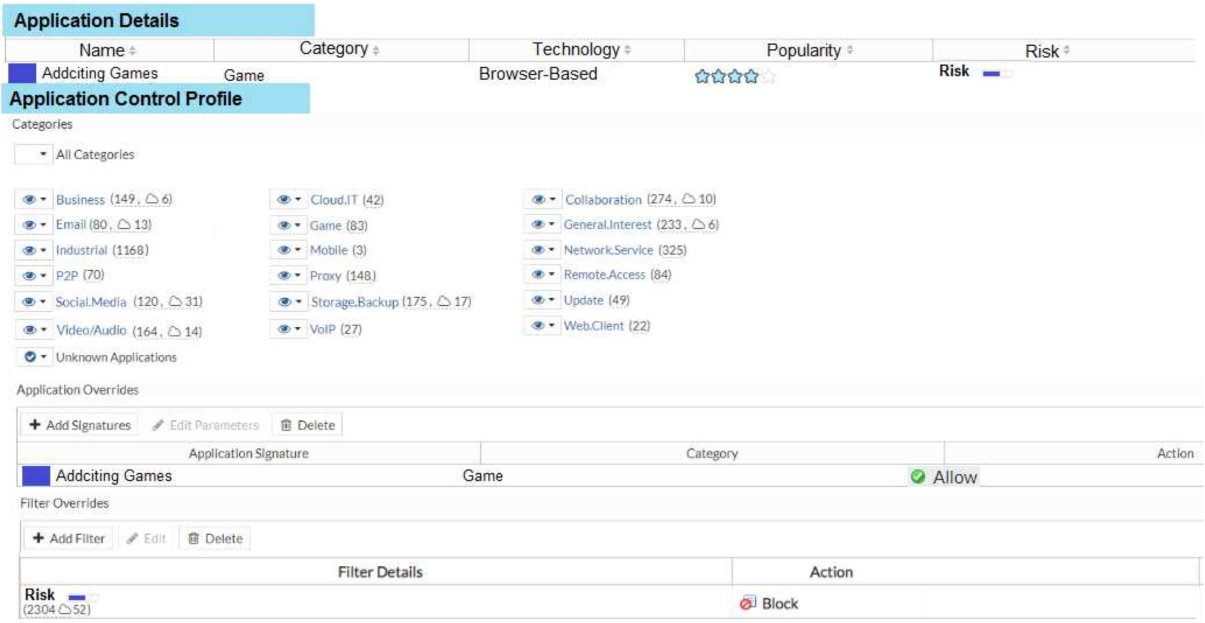
What criteria does FortiGate use to look for a matching firewall policy to process traffic? (Choose two.)

A. Services defined in the firewall policy.
B. Incoming and outgoing interfaces
C. Highest to lowest priority defined in the firewall policy.
D. Lowest to highest policy ID number.

Answer: A,B

Question: 8

View the exhibit.



Application Details

Name	Category	Technology	Popularity	Risk
Addciting Games	Game	Browser-Based	★★★★☆	Risk

Application Control Profile

Categories

All Categories

- Business (149, 6)
- Email (80, 13)
- Industrial (1168)
- P2P (70)
- Social.Media (120, 31)
- Video/Audio (164, 14)
- Unknown Applications
- Cloud.IT (42)
- Game (83)
- Mobile (3)
- Proxy (148)
- Storage.Backup (175, 17)
- VoIP (27)
- Collaboration (274, 10)
- General.Interest (233, 6)
- Network.Service (325)
- Remote.Access (84)
- Update (49)
- Web.Client (22)

Application Overrides

Application Signature	Category	Action
Addciting Games	Game	✓ Allow

Filter Overrides

Filter Details	Action
Risk (2304 52)	Block

A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addcting.Games is allowed based on the Categories configuration.

Answer: A

Question: 9

Which of the following static routes are not maintained in the routing table?

A. Named Address routes
B. Dynamic routes
C. ISDB routes
D. Policy routes

Answer: D

Question: 10

Which Statements about virtual domains (VDOMs) arc true? (Choose two.)

A. Transparent mode and NAT/Route mode VDOMs cannot be combined on the same FortiGate.
B. Each VDOM can be configured with different system hostnames.
C. Different VLAN sub-interface of the same physical interface can be assigned to different VDOMs.
D. Each VDOM has its own routing table.

Answer: C,D