Leads4Pass

NSE4_FGT-7.0^{Q&As}

Fortinet NSE 4 - FortiOS 7.0

Pass Fortinet NSE4_FGT-7.0 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse4_fgt-7-0.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin ->sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 pclicy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```
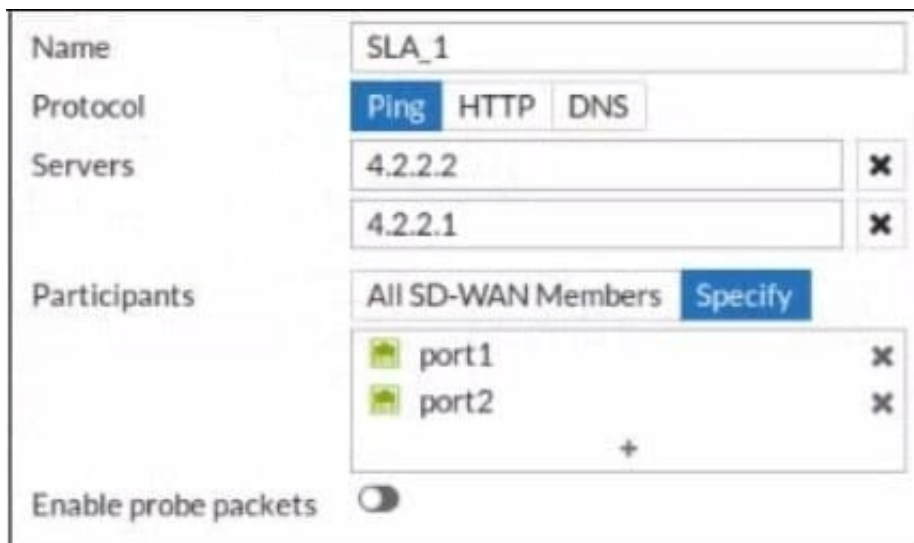
Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.

B. The session is in TCP ESTABLISHED state.

C. The session is a bidirectional UDP connection.

D. The session is a bidirectional TCP connection.

Correct Answer: C

QUESTION 2

Refer to the exhibit.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

A. The Detection Mode setting is not set to Passive.

B. Administrator didn\\'t configure a gateway for the SD-WAN members, or configured gateway is not valid.

C. The configured participants are not SD-WAN members.

D. The Enable probe packets setting is not enabled.

Correct Answer: BD

QUESTION 3

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password

B. FortiGate supports pre-shared key and signature as authentication methods.

C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.

D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Correct Answer: AB

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticatingaremote-fortigate-peer-with-a-pre-shared-key

QUESTION 4

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout

B. auth-on-demand

C. soft-timeout

D. new-session

E. Idle-timeout

Correct Answer: ADE

https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

QUESTION 5

When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.

B. Only a single virtual wire pair can be included in each policy.

C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.

D. Exactly two virtual wire pairs need to be included in each policy.

Correct Answer: A

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690

QUESTION 6

When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID

B. Universally Unique Identifier
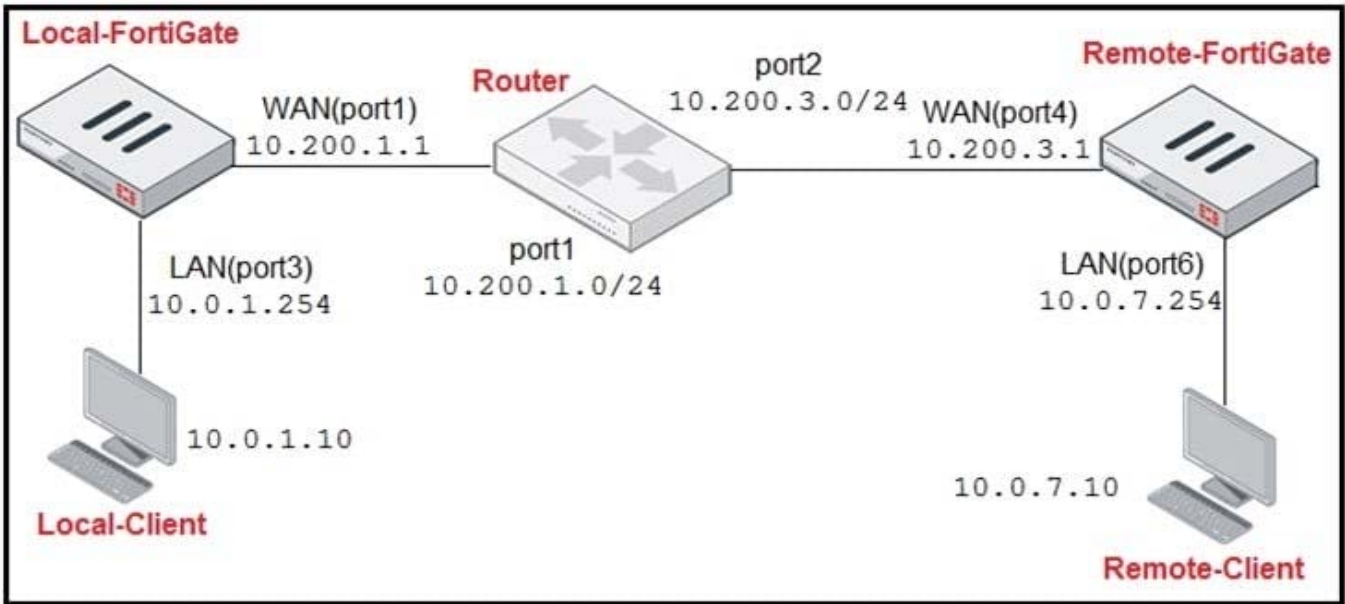
C. Policy ID

D. Sequence ID

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies

QUESTION 7

Refer to the exhibit.

Network Diagram

Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
⊟	⚪					
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

Name ⇕	External IP Range ⇕	Type ⇕	ARP Reply ⇕
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	✅ Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	✅ Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	✅ Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24.

The LAN (port3) interface has the IP address 10.0.1.254/24.

A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1).

Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.

Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP

address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.149

B. 10.200.1.1

C. 10.200.1.49

D. 10.200.1.99

Correct Answer: D

QUESTION 8

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.

B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.

D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world

devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

QUESTION 9

Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.

B. Central NAT can be enabled or disabled from the CLI only.

C. Source NAT, using central NAT, requires at least one central SNAT policy.

D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Correct Answer: AB

QUESTION 10

Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view

B. Log backups from the CLI cannot be restored to another FortiGate.

C. Log backups from the CLI can be configured to upload to FTP as a scheduled time

D. Log downloads from the GUI are stored as LZ4 compressed files.

Correct Answer: AB

QUESTION 11

Refer to the exhibit.

Edit IPS Sensor

Name	WINDOWS_SERVERS
Comments	Write a comment... 0/255
Block malicious URLs	⬤

IPS Signatures and Filters

+ Create New   **✏ Edit**   **🗑 Delete**

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	✓ Enabled	✓ Enabled
OS Windows		⊘ Block	✗ Disabled	✓ Enabled

The exhibit shows the IPS sensor configuration.

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the NTP.Spoofed.KoD.DoS signature.

B. The sensor will block all attacks aimed at Windows servers.

C. The sensor will reset all connections that match these signatures.

D. The sensor will gather a packet log for all matched traffic.

Correct Answer: AB

QUESTION 12

Examine the two static routes shown in the exhibit, then answer the following question.

+ Create New   **✏ Edit**   **☐ Clone**   **🗑 Delete**

Destination ⬍	Gateway ⬍	Interface ⬍	Priority ⬍	Distance ⬍
172.20.168.0/24	172.25.176.1	▪port1	10	20
172.20.168.0/24	172.25.178.1	▪port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.

B. FortiGate will use the port1 route as the primary candidate.

C. FortiGate will route twice as much traffic to the port2 route

D. FortiGate will only actuate the port1 route in the routing table

Correct Answer: B

"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

QUESTION 13

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.

Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention

Correct Answer: AD

QUESTION 14

Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode

B. Can act as a Layer 2 switch as well as a Layer 3 router

C. All interfaces in the software switch share the same IP address

D. It can group only physical interfaces

Correct Answer: AC

QUESTION 15

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

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

Correct Answer: B

Dumps   **Test**