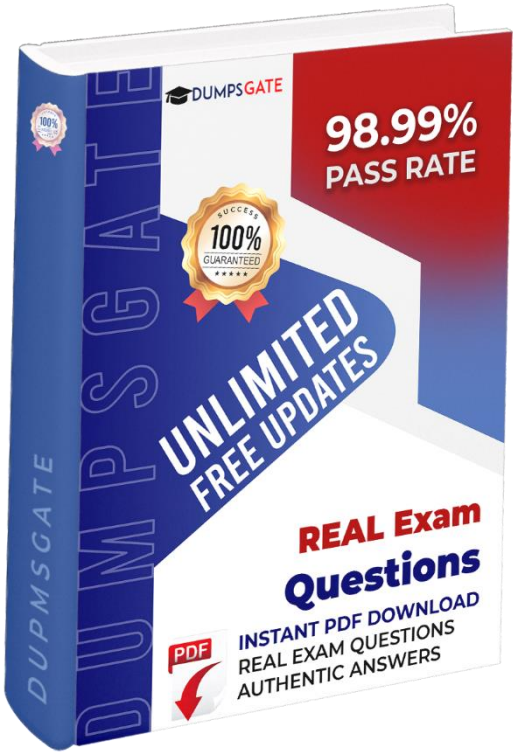


Exam	**NSE4_FGT-6.4**
Title	**Fortinet NSE 4 - FortiOS 6.4 Exam**
Version	**3.0**
Product Type	**119 Q&A with explanations**

https://dumpsgate.com/dumps/nse4_fgt-6-4/

Exam A

QUESTION 1
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode FortiGate in the network.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

QUESTION 2
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/100552/using-xauth-authentication

QUESTION 4
Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan
B. Trojan scan
C. Antivirus scan
D. Ransomware scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/927086/examples

QUESTION 5
Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

A. Firewall policy
B. Policy rule
C. Security policy
D. SSL inspection and authentication policy

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode

QUESTION 6
You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.
B. No new log is recorded until you manually clear logs from the local disk.
C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.
D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting

QUESTION 7
Refer to the exhibit, which contains a Performance SLA configuration.

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.

Why is FortiGate not generating any traffic for the performance SLA?

A. There may not be a static route to route the performance SLA traffic.
B. You need to turn on the **Enable probe packets** switch.
C. The Ping protocol is not supported for the public servers that are configured.
D. Participants configured are not SD-WAN members.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-link-monitoring

QUESTION 8
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

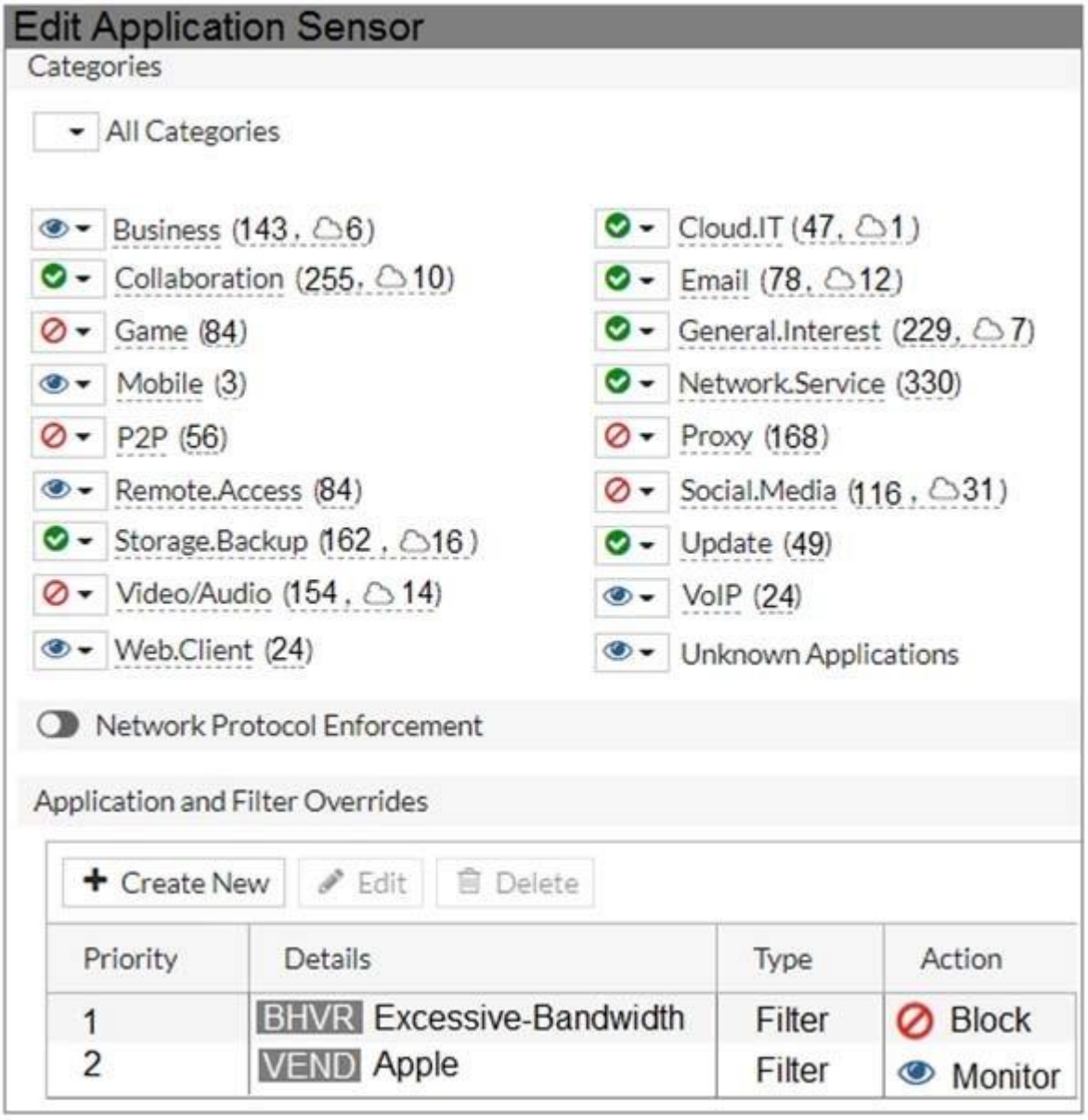
In this scenario, which statement about VLAN IDs is true?

A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
B. The two VLAN subinterfaces must have different VLAN IDs.
C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Refer to the exhibit to view the application control profile.



Users who use Apple FaceTime video conferences are unable to set up meetings.

In this scenario, which statement is true?

A. Apple FaceTime belongs to the custom monitored filter.
B. The category of Apple FaceTime is being monitored.
C. Apple FaceTime belongs to the custom blocked filter.
D. The category of Apple FaceTime is being blocked.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

https://dumpsgate.com/dumps/nse4_fgt-6-4/

QUESTION 10
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
B. FortiGate automatically negotiates a new security association after the existing security association expires.
C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=12069

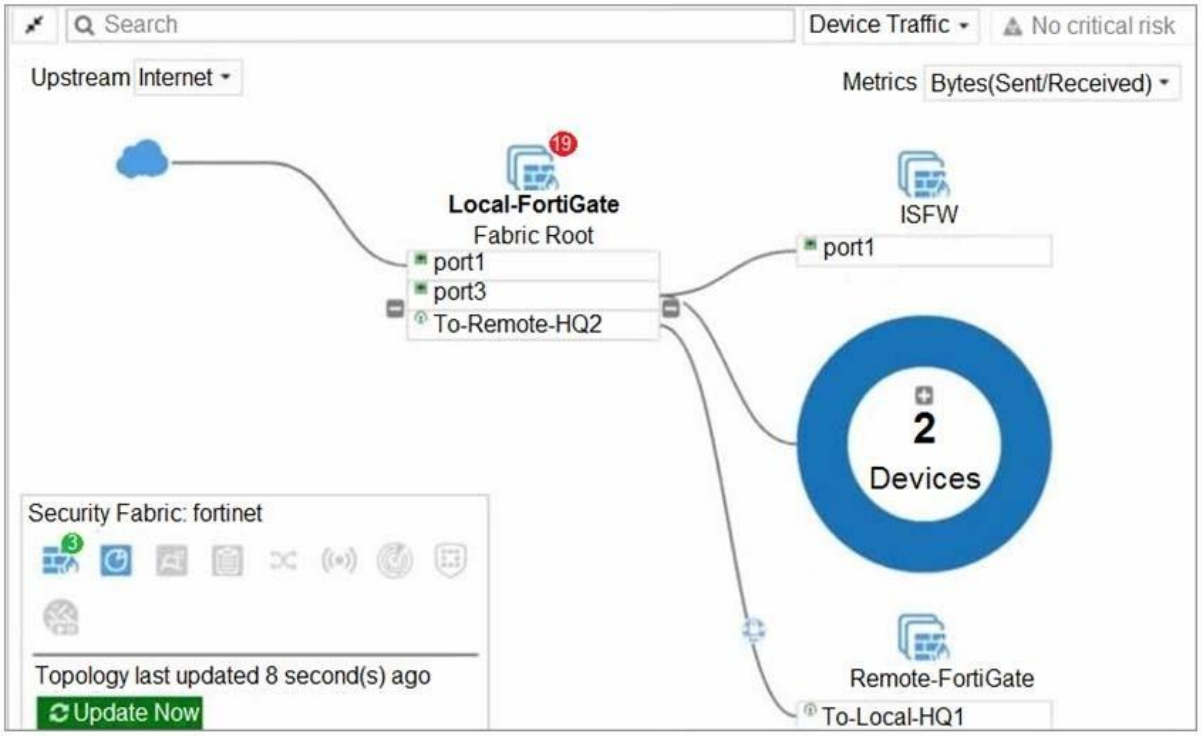
QUESTION 11
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection
B. Antivirus in flow-based inspection
C. DNS filter
D. Web application firewall
E. Application control

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.

What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter
B. Static URL filter, FortiGuard category filter, and advanced filters
C. Static domain filter, SSL inspection filter, and external connectors filters
D. FortiGuard category filter and rating filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

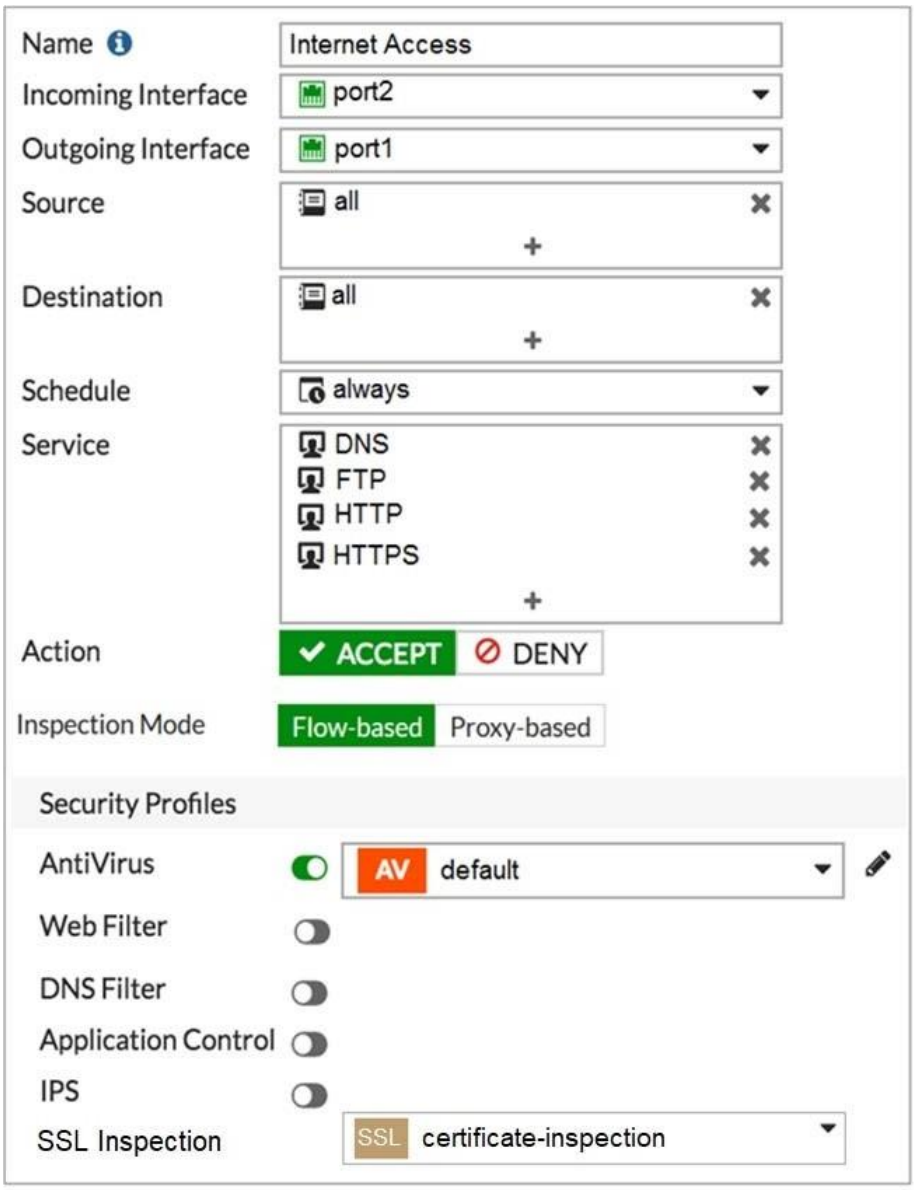
QUESTION 14
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID
B. Universally Unique Identifier
C. Policy ID
D. Sequence ID

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 15
Refer to the exhibit to view the firewall policy.



Which statement is correct if well-known viruses are not being blocked?

A. The firewall policy does not apply deep content inspection.
B. The firewall policy must be configured in proxy-based inspection mode.
C. The action on the firewall policy must be set to deny.
D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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 policy_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?

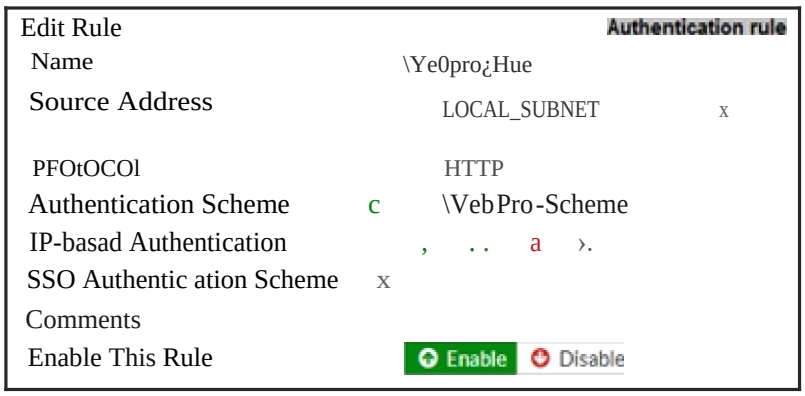
A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Correct Answer: C
Section: (none)
Explanation

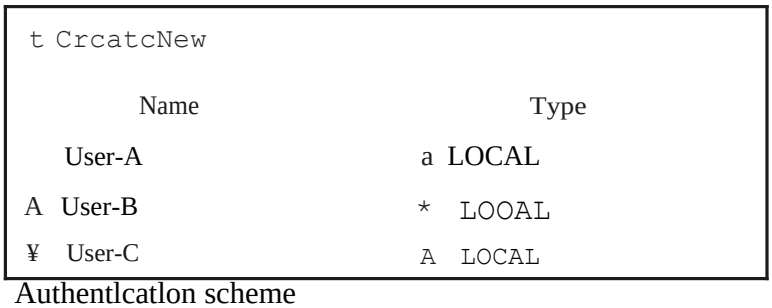
Explanation/Reference:

QUESTION 17
Refer to the exhibit.

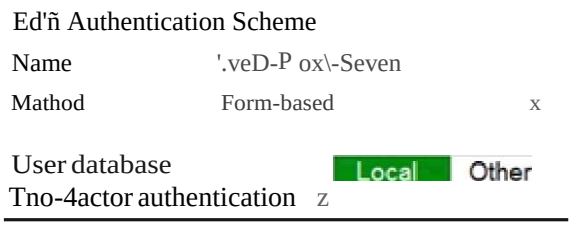
Authentication rule



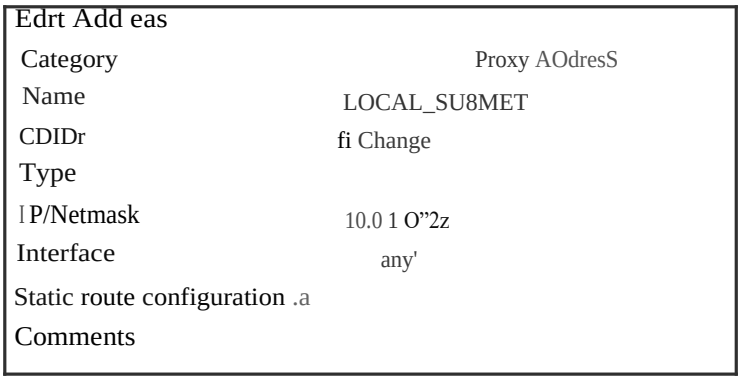
Users



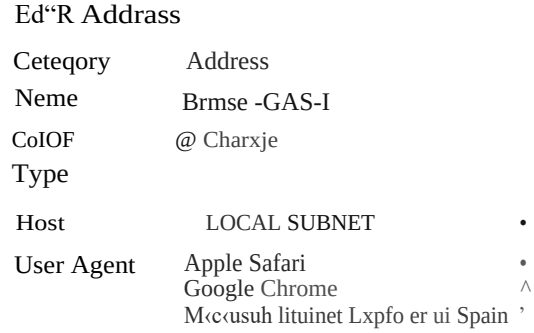
Authentlcatlon scheme



Firewall address



Proxy address



Comments

Proxy address

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies.

The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database. Users will be prompted for authentication.

How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP `10.0.1.10` to the destination `http://www.fortinet.com`? (Choose two.)

A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.
E. If a Mozilla Firefox browser is used with User-C credentials, the HTTP request will be denied.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Refer to the exhibit.

Exhibit A

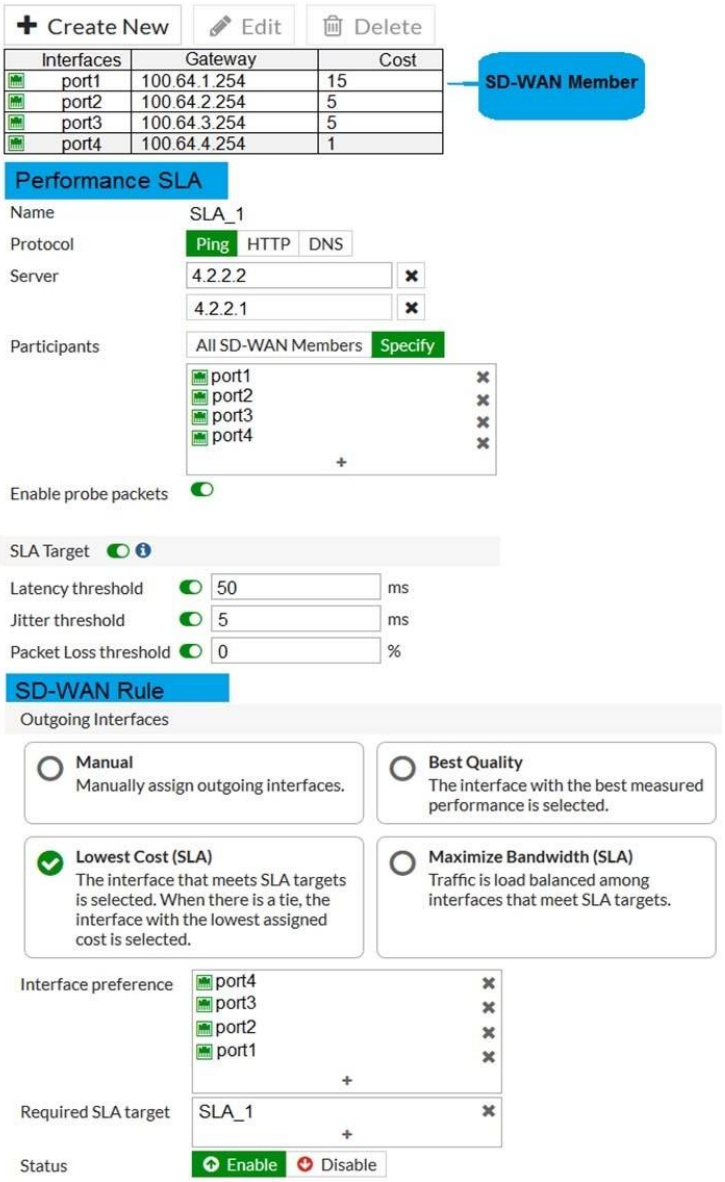


Exhibit B

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(SLA_1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(34.349), jitter(3.887) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.000%) latency(31.476), jitter(3.254) sla_map=0x1
Seq(4 port4): state(alive), packet-loss(2.130%) latency(46.229), jitter(4.287) sla_map=0x1
```

The exhibit shows the configuration for the SD-WAN member, Performance SLA and SD-WAN Rule, as well as the output of `diagnose sys virtual-wan-link health-check`.

Which interface will be selected as an outgoing interface?

A. port4
B. port2
C. port1

D. port3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
What devices form the core of the security fabric?

A. Two FortiGate devices and one FortiManager device
B. One FortiGate device and one FortiManager device
C. Two FortiGate devices and one FortiAnalyzer device
D. One FortiGate device and one FortiAnalyzer device

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components

QUESTION 20
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435