

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/



NEW QUESTION 1

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. FTM
- B. SSH
- C. HTTPS
- D. FortiTelemetry

Answer: BC

NEW QUESTION 2

Refer to the exhibit.

```
# diagnose test application ipsmonitor

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command shown in the exhibit.

If option 5 is used with the IPS diagnostic command and the outcome is a decrease in the CPU usage, what is the correct conclusion?

- A. The IPS engine is unable to prevent an intrusion attack.
- B. The IPS engine is inspecting a high volume of traffic.
- C. The IPS engine will continue to run in a normal state.
- D. The IPS engine is blocking all traffic.

Answer: B

NEW QUESTION 3

Which three methods are used by the collector agent for AD polling? (Choose three.)

- A. FortiGate polling
- B. NetAPI
- C. Novell API
- D. WMI
- E. WinSecLog

Answer: BDE

NEW QUESTION 4

Which two attributes are required on a certificate so it can be used as a CA certificate on SSL inspection? (Choose two.)

- A. The keyUsage extension must be set to keyCertSign.
- B. The CA extension must be set to TRUE.
- C. The issuer must be a public CA.
- D. The common name on the subject field must use a wildcard name.

Answer: AB

NEW QUESTION 5

Which three statements explain a flow-based antivirus profile? (Choose three.)

- A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- B. If a virus is detected, the last packet is delivered to the client.
- C. The IPS engine handles the process as a standalone.
- D. FortiGate buffers the whole file but transmits to the client at the same time.
- E. Flow-based inspection optimizes performance compared to proxy-based inspection.

Answer: ADE

NEW QUESTION 6

What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

- A. FortiGate uses fewer resources.
- B. FortiGate performs a more exhaustive inspection on traffic.
- C. FortiGate adds less latency to traffic.
- D. FortiGate allocates two sessions per connection.

Answer: AC

NEW QUESTION 7

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

- A. The debug flow is for ICMP traffic.
- B. The default route is required to receive a reply.
- C. A new traffic session was created.
- D. A firewall policy allowed the connection.

Answer: AC

NEW 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, what are two requirements for the VLAN ID? (Choose two.)

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

Answer: CD

NEW QUESTION 9

Refer to the exhibit.



```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 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=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
origin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id= 00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN_SENT state.
- B. The session is in FIN_ACK state.
- C. The session is in FTN_WAIT state.
- D. The session is in ESTABLISHED state.

Answer: A

Explanation:

Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 10

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Answer: CD

NEW QUESTION 10

Refer to the exhibits.

The exhibits show the firewall policies and the objects used in the firewall policies.

The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A

Exhibit B

Address Object

| Name | Details |
|-----------------|--------------|
| IP Range/Subnet | |
| LOCAL_CLIENT | 10.0.1.10/32 |
| all | 0.0.0.0 |
| FQDN | |
| facebook.com | facebook.com |

Internet Service Object

| Name | Direction | Number of Entries |
|------------------------------|-------------|-------------------|
| Predefined Internet Services | | |
| Facebook-Web | Destination | 26.578 |
| IP | Port | Protocol |
| 1.9.91.17 - 1.9.91.18 | 80 | TCP |
| | 443 | |
| | 8443 | |
| 1.9.91.17 - 1.9.91.18 | 443 | UDP |
| 1.9.91.30 | 443 | UDP |

Firewall Policies

| ID | From | To | Source | Destination | Schedule | Service | Action | NAT |
|----|-------|-------|--------------|--------------|----------|----------------------|----------|---------|
| 3 | port3 | port1 | LOCAL_CLIENT | facebook.com | always | ULL_UDP | ✓ ACCEPT | Enabled |
| 1 | port1 | port3 | facebook.com | LOCAL_CLIENT | always | ULL_UDP | ✓ ACCEPT | Enabled |
| 4 | port4 | port1 | LOCAL_CLIENT | all | always | HTTP DNS HTTPS | ✓ ACCEPT | Enabled |
| 5 | port3 | port1 | LOCAL_CLIENT | Facebook-Web | always | Internet Service | ✓ ACCEPT | Enabled |
| 2 | port3 | port1 | all | all | always | ALL | ✓ ACCEPT | Enabled |

Exhibit A

Exhibit B

Policy Lookup

Incoming Interface: port3

IP Version: IPv4

Protocol: TCP

Source: 10.0.1.10

Source Port: Optional (1-65535)

Destination: facebook.com

Destination Port: 443

Search Close

Which policy will be highlighted, based on the input criteria?

- A. Policy with ID 4.
- B. Policy with ID 5.
- C. Policies with ID 2 and 3.
- D. Policy with ID 4.

Answer: A

NEW QUESTION 13

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

- A. The IP version of the sources and destinations in a firewall policy must be different.
- B. The Incoming Interface
- C. Outgoing Interface
- D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
- E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
- F. The IP version of the sources and destinations in a policy must match.
- G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 14

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.

Answer: ABD

Explanation:

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- Incoming Interface
- Outgoing Interface
- Source: IP address, user, internet services
- Destination: IP address or internet services
- Service: IP protocol and port number
- Schedule: Applies during configured times

NEW QUESTION 17

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface. Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

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

Answer: B

Explanation:

FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf > page 147

"Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID"

NEW QUESTION 22

Which two statements explain antivirus scanning modes? (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.

Answer: BC

Explanation:

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.

NEW QUESTION 23

FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be

configured using a specific syntax.

Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

- A. www.example.com:443
- B. www.example.com
- C. example.com
- D. www.example.com/index.html

Answer: BC

Explanation:

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names - no URLs or wildcard characters are allowed.

OK: google.com or www.google.com

NO OK: www.google.com/index.html or google.* FortiGate_Security_6.4 page 384

When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names-- "no URLs or wildcard characters are allowed".

NEW QUESTION 27

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

Answer: AC

NEW QUESTION 31

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
rpd_b_link_id= 00000000 rpd_b_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.

Answer: C

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 35

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.

Exhibit A Exhibit B

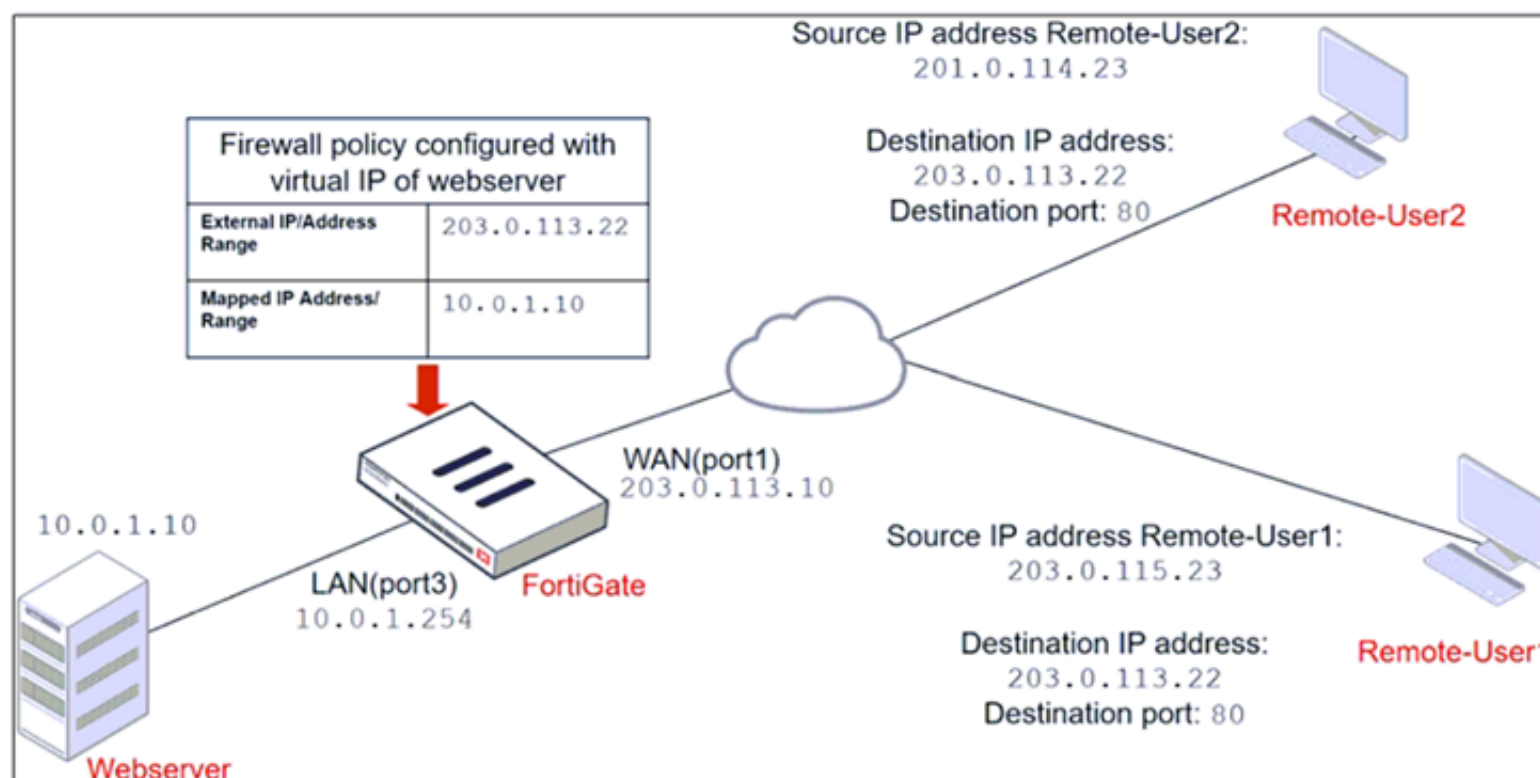


Exhibit A Exhibit B

Edit Address

| | |
|----------------------------|--------------------------------|
| Name | Deny_IP |
| Color | Change |
| Type | Subnet |
| IP/Netmask | 201.0.114.23/32 |
| Interface | WAN (port1) |
| Static route configuration | <input type="checkbox"/> |
| Comments | Deny web server access. 23/255 |

Firewall address object

Firewall policies

| ID | Name | Source | Destination | Schedule | Service | Action |
|-----------------------------|--------------|---------|-------------|----------|---------|--------|
| WAN (port1) → LAN (port3) 2 | | | | | | |
| 4 | Deny | Deny_IP | all | always | ALL | DENY |
| 3 | Allow_access | all | Webserver | always | ALL | ACCEPT |

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web_server in the Deny policy.

Answer: CD

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta>

NEW QUESTION 40

Refer to the exhibit.

Name: SLA1

Protocol: ☒ Ping ☐ HTTP ☐ DNS

Server: 4.2.2.2 4.2.2.1

Participants: All SD-WAN Members

☒ port1 ☒ port2

Enable probe packets ☐

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.

Answer: BD

NEW QUESTION 44

Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

- A. The IPS engine was inspecting high volume of traffic.
- B. The IPS engine was unable to prevent an intrusion attack .
- C. The IPS engine was blocking all traffic.
- D. The IPS engine will continue to run in a normal state.

Answer: A

NEW QUESTION 49

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821>

NEW QUESTION 53

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

- A. It limits the scope of application control to the browser-based technology category only.
- B. It limits the scope of application control to scan application traffic based on application category only.
- C. It limits the scope of application control to scan application traffic using parent signatures only
- D. It limits the scope of application control to scan application traffic on DNS protocol only.

Answer: B

NEW QUESTION 58

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

Name: Allow_Twitter
Comments: Write a comment... 0/255
Feature set: **Flow-based** Proxy-based
☒ FortiGuard Category Based Filter

☒ Allow
☒ Monitor
☒ Block
☒ Warning
☒ Authenticate

| Name | Action |
|-------------------------|---|
| Medicine | <input checked="" type="checkbox"/> Allow |
| News and Media | <input checked="" type="checkbox"/> Allow |
| Social Networking | <input checked="" type="checkbox"/> Block |
| Political Organizations | <input checked="" type="checkbox"/> Allow |
| Reference | <input checked="" type="checkbox"/> Allow |
| Global Religion | <input checked="" type="checkbox"/> Allow |
| Shopping | <input checked="" type="checkbox"/> Allow |
| Society and Lifestyles | <input checked="" type="checkbox"/> Allow |
| Sports | <input checked="" type="checkbox"/> Allow |

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New
Edit
Delete
Search

| URL | Type | Action | Status |
|-------------|----------|---|--|
| twitter.com | Wildcard | <input checked="" type="checkbox"/> Allow | <input checked="" type="checkbox"/> Enable |

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- On the Static URL Filter configuration, set Type to Simple
- On the Static URL Filter configuration, set Action to Exempt.
- On the Static URL Filter configuration, set Action to Monitor.

Answer: C

NEW QUESTION 59

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A CRL
- A person
- A subordinate CA
- A root CA

Answer: D

NEW QUESTION 61

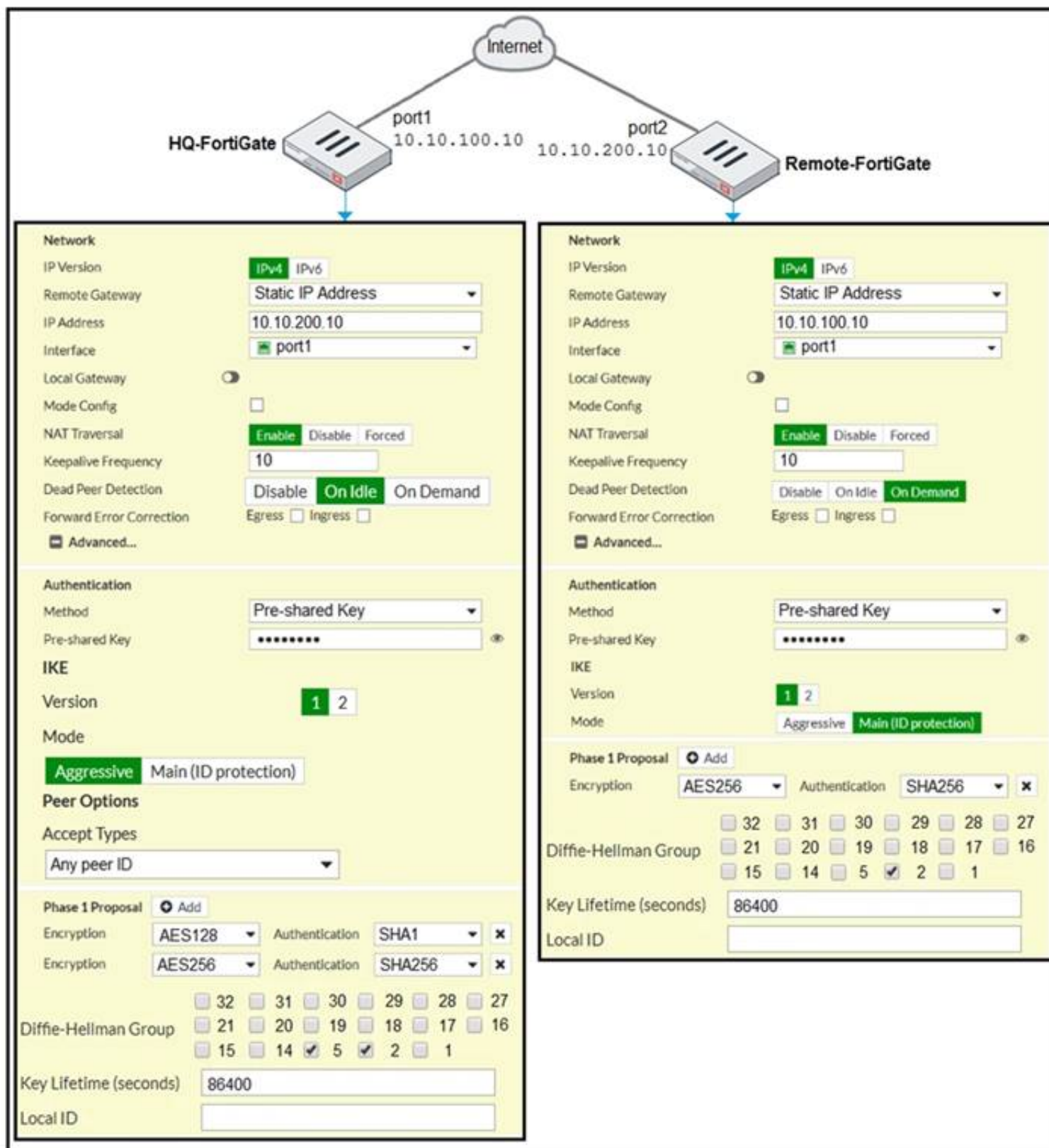
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

- VLAN interface
- Software Switch interface
- Aggregate interface
- Redundant interface

Answer: C

NEW QUESTION 64

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.



Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

NEW QUESTION 69

Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

- A. Source IP
- B. Spillover
- C. Volume
- D. Session

Answer: CD

Explanation:

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

NEW QUESTION 73

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT-7.2 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-7.2/

Money Back Guarantee

NSE4_FGT-7.2 Practice Exam Features:

- * NSE4_FGT-7.2 Questions and Answers Updated Frequently
- * NSE4_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year