



- Expert Verified, Online, **Free**.

Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. OSPF interface network types match.
- B. OSPF router IDs are unique.
- C. OSPF interface priority settings are unique.
- D. Authentication settings match.
- E. OSPF link costs match.

**Suggested Answer: ABD**

Community vote distribution

ABD (100%)

Alaba **Highly Voted** 1 year, 10 months ago

A, B, D are correct answers  
upvoted 8 times

Cone **Most Recent** 10 months ago

**Selected Answer: ABD**

A, B, D - basic OSPF question  
upvoted 1 times

ExamsAE 12 months ago

**Selected Answer: ABD**

A, B, D are correct answers  
upvoted 1 times

romartinedg 1 year, 1 month ago

A,B,C son correctas  
upvoted 1 times

rirax 1 year, 4 months ago

**Selected Answer: ABD**

A, B, D are correct answers  
upvoted 2 times

certifi46 1 year, 5 months ago

**Selected Answer: ABD**

A, B, D are correct answers  
upvoted 2 times

Agent1994 1 year, 5 months ago

**Selected Answer: ABD**

ABD  
Ref: Enterprise\_Firewall\_7.0\_Study\_Guide-Online page 280.  
upvoted 1 times

ducdud95 1 year, 6 months ago

A B D are correct  
upvoted 1 times

smeupics 1 year, 7 months ago

**Selected Answer: ABD**



A, B, D are correct answers  
upvoted 1 times

stalker1ua 1 year, 8 months ago

**Selected Answer: ABD**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 280

upvoted 1 times

  **Seph1** 1 year, 9 months ago

**Selected Answer: ABD**

A, B, D are correct

upvoted 1 times

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:     trans_id = KEY_IKE.
ike 0:624000:98:     encapsulation = IKE/none
ike 0:624000:98:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:       type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. In the phase 1 network configuration, set the IKE version to 2.
- B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.
- C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
- D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

**Suggested Answer: D**

*Community vote distribution*

🗨️ **Darthan** 10 months, 1 week ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ **romartinedg** 1 year, 1 month ago

D, es correcta

upvoted 1 times

🗨️ **cisco1750** 1 year, 3 months ago

Team, I tend to disagree with D as it is. The OAKLEY\_GROUP value refers to the Diffie-Hellman group, in this case, this is the mismatch, however, we don't have an answer matching this option. Please check it out here: <https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-check-if-Diffie-Hellman-DH-group-is-the/ta-p/193250>

upvoted 2 times

🗨️ **cedigger** 1 year, 3 months ago

In incoming proposals there are DH group 14 and 5. It's the same at my proposal. Because you can't change the incoming proposals D is correct.

upvoted 1 times

🗨️ **nse\_student** 1 year, 4 months ago

D is correct!

upvoted 1 times

🗨️ **rirax** 1 year, 4 months ago

**Selected Answer: D**

D, remote is AES256 SHA2-256

upvoted 1 times

🗨️ **certifi46** 1 year, 5 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ **Agent1994** 1 year, 5 months ago

**Selected Answer: D**

D, remote is offering AES256 SHA2-256

upvoted 1 times

🗨️ **ducduc95** 1 year, 6 months ago

D is correct as the SHA doesn't match

upvoted 1 times

🗨️ **smeupics** 1 year, 7 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ **Quetchup** 1 year, 7 months ago

**Selected Answer: D**

<https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852>

upvoted 1 times

🗨️ **emy74** 1 year, 7 months ago

D is correct

upvoted 1 times

🗨️ **ducduc95** 1 year, 8 months ago

**Selected Answer: D**



Answer D

upvoted 1 times

🗨️ **stalker1ua** 1 year, 8 months ago

**Selected Answer: D**

D is correct  
upvoted 1 times

  **Seph1** 1 year, 9 months ago

**Selected Answer: D**

D is correct  
upvoted 1 times

Refer to the exhibit, which shows the output of a web filtering diagnose command.

# diagnose webfilter fortiguard statistics list	# diagnose webfilter fortiguard statistics list
Rating Statistics:	Cache Statistics:
=====	=====
DNS failures : 273	Maximum memory : 0
DNS lookups : 280	Memory usage : 0
Data send failures : 0	
Data read failures : 0	Nodes : 0
Wrong package type : 0	Leaves : 0
Hash table miss : 0	Prefix nodes : 0
Unknown server : 0	Exact nodes : 0
Incorrect CRC : 0	
Proxy request failures : 0	Requests : 0
Request timeout : 1	Misses : 0
Total requests : 2409	Hits : 0
Requests to FortiGuard servers : 1182	Prefix hits : 0
Server errored responses : 0	Exact hits : 0
Relayed rating : 0	
Invalid profile : 0	No cache directives : 0
	Add after prefix : 0
Allowed : 1021	Invalid DB put : 0
Blocked : 3909	DB updates : 0
Logged : 3927	
Blocked Errors : 565	Percent full : 0%
Allowed Errors : 0	Branches : 0%
Monitors : 0	Leaves : 0%
Authenticates : 0	Prefix nodes : 0%
Warnings : 18	Exact nodes : 0%
Ovrd request timeout : 0	
Ovrd send failures : 0	Miss rate : 0%
Ovrd read failures : 0	Hit rate : 0%
Ovrd errored responses : 0	Prefix hits : 0%
...	Exact hits : 0%

Which configuration change would result in non-zero results in the cache statistics section?

- A. set server-type rating under config system central-management
- B. set webfilter-cache enable under config system fortiguard
- C. set webfilter-force-off disable under config system fortiguard
- D. set ngfw-mode policy-based under config system settings

**Suggested Answer: B**

Community vote distribution

B (100%)

**certifi46** 5 months, 2 weeks ago

**Selected Answer: B**

webcache disabled

upvoted 1 times

**Agent1994** 5 months, 4 weeks ago

**Selected Answer: B**

B

A/D: doesn't apply

C: according to the number of requests sent, the webfilter is active.

upvoted 1 times

**ducduc95** 6 months, 3 weeks ago

It is B

We can notice that the webfilter is already enable globally(disable) by looking at "Rating statistics". So it only remains to enable the cache option.

upvoted 1 times



**Iulipeoliveira** 8 months, 3 weeks ago

C - The "disable" parameter will enable web-filter globally.

upvoted 1 times

**chgook** 8 months, 3 weeks ago

All counters display zero if web filtering cache is disabled in config system fortiguard setting  
upvoted 3 times

  **stalker1ua** 8 months, 3 weeks ago



**Selected Answer: B**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 362  
upvoted 3 times

  **Seph1** 9 months ago

**Selected Answer: B**

B - NSE 7 study guide page 362  
upvoted 2 times

  **racdab** 9 months, 2 weeks ago

**Selected Answer: B**

I would say B  
upvoted 1 times



Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

### Configuration

```
config system global
    set snat-route-change disable
end
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

### Configuration

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

- A. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- B. The session would remain in the session table, and its traffic would egress from port2.
- C. The session would be deleted, and the client would need to start a new session.
- D. The session would remain in the session table, and its traffic would egress from port1.

**Suggested Answer: B**

Community vote distribution

D (97%)

 **pcbbj**  1 year, 9 months ago

**Selected Answer: D**

With snat-route-change disable, sessions using SNAT keep using the same outbound interface, as long as the old route is still active.  
upvoted 13 times

 **kocalin**  1 year, 9 months ago

**Selected Answer: D**

D is correct - Study Guide, page 146



upvoted 6 times

  **cbu\_ch** Most Recent 9 months ago

**Selected Answer: D**

Same here, D.

upvoted 1 times

  **mikerss** 10 months, 3 weeks ago

**Selected Answer: D**

D is correct.

SNAT

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-SNAT-route-change-to-update-existing-NAT/ta-p/198439>

```
config system global
```

```
set snat-route-change enable
```



```
end
```

The option 'snat-route-change' can control what action the existing SNAT session needs to take after route change.

By default, it is disabled. So after a routing change, sessions with SNAT keep using the same outbound interface, as long as the old route is still active.

When 'snat-route-change' is enabled, after a routing change, routing information is flushed from existing SNAT sessions;.

upvoted 1 times

  **adiaz\_** 11 months, 2 weeks ago


D is the correct.

upvoted 1 times

  **Ral89** 11 months, 3 weeks ago

How can we determine if snat-route-change is disabled or enabled by looking at this output ?

upvoted 1 times

  **J\_Olin** 5 months, 3 weeks ago

It says 'disable' on the second line of the Configuration screenshot

upvoted 1 times

  **Malasxd** 1 year ago

**Selected Answer: B**

In the session show the traffic using interface 2 as outbound. I don't know why, but it is.

upvoted 1 times



  **Malasxd** 1 year ago

Sorry. The interface number showed in session table is the interface index and not the interface number. I not sure if the index 2 own the port2.

We need to trust that it's not a prank and there's not a policy route matching this traffic.

I change my answer to "D"


upvoted 1 times

  **fy64** 1 year, 1 month ago

**Selected Answer: D**

snat-route-change should be enabled in order to switch routing to port 2.

upvoted 1 times

  **lucient** 1 year, 1 month ago


**Selected Answer: D**

"D" is correct.

"When you disable snat-route-change, the behavior that occurs after a routing change is different for sessions using SNAT. Sessions using SNAT continue using the same outbound interface, as long as the old route is still active."

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf - Page 146

upvoted 1 times

  **fnet007** 1 year, 2 months ago

Took the test a few weeks ago, there is a variant on this question where the snat-route-change setting is enabled. So the answer would be B in that case.

upvoted 2 times

🗨️ 👤 **javim** 1 year, 1 month ago

No, the answer would be C, the session is deleted and reestablished.

upvoted 2 times

🗨️ 👤 **cedigger** 1 year, 3 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ 👤 **Sanalthekken** 1 year, 5 months ago

**Selected Answer: D**

With snat-route-change disable, sessions using SNAT keep using the same outbound interface, as long as the old route is still active.

upvoted 1 times

🗨️ 👤 **Dayvey** 1 year, 5 months ago

**Selected Answer: D**

With snat-route-change enable will it perform the same action as non-natted traffic , aka it will flag the session as dirty and reestablish.

With snat-route-change disable it will stay on the current interface unless the interface has gone down.

upvoted 1 times

🗨️ 👤 **caleidoscopio** 1 year, 5 months ago

D is correct

upvoted 1 times

🗨️ 👤 **certifi46** 1 year, 5 months ago

**Selected Answer: D**

With snat-route-change disable, sessions using SNAT keep using the same outbound interface, as long as the old route is still active

upvoted 1 times

🗨️ 👤 **Agent1994** 1 year, 5 months ago

**Selected Answer: D**

D: snat-route-change is disabled.

Ref: Enterprise\_Firewall\_7.0\_Study\_Guide-Online 147

upvoted 1 times

🗨️ 👤 **TylerNSE** 1 year, 7 months ago

The same session is remain with the original initial traffic interface.

D - is correct

upvoted 1 times

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

### Configuration

### Session

```
config system global
    set snat-route-change disable
end
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

### Configuration

### Session

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

An administrator would like to test session failover between the two service provider connections.


What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

- A. Configure set snat-route-change enable.
- B. Change the priority of the port2 static route to 5.
- C. Change the priority of the port1 static route to 11.
- D. unset snat-route-change to return it to the default setting.

**Suggested Answer: AB**

Community vote distribution

AC (100%)

 **Comatose** Highly Voted 1 year, 9 months ago

Selected Answer: AC

It's A & C. B would just create an equal cost solution and not a failover scenario.

upvoted 11 times

 **cbu\_ch** Most Recent 9 months ago

Selected Answer: AC

A and C

upvoted 1 times

🗲️ 👤 **ronia** 10 months, 3 weeks ago

**Selected Answer: AC**

A and C

upvoted 1 times

🗲️ 👤 **Malasxd** 1 year ago

**Selected Answer: AC**

A and C

upvoted 1 times

🗲️ 👤 **cedigger** 1 year, 3 months ago

**Selected Answer: AC**

A and C

upvoted 1 times

🗲️ 👤 **pete79** 1 year, 3 months ago

vote A & C

upvoted 1 times

🗲️ 👤 **caleidoscopio** 1 year, 5 months ago

Correct answer: A C

upvoted 1 times

🗲️ 👤 **certifi46** 1 year, 5 months ago

**Selected Answer: AC**

A and C

upvoted 1 times

🗲️ 👤 **Agent1994** 1 year, 5 months ago

**Selected Answer: AC**

A, C: snat-route-changed needs to be changed to enabled (default: disabled) to make this test, and then change the priority to force traffic to go through port2.

B: nope, both ports would have the same priority.

D: default is disabled, and we need to enable it.

Ref: Enterprise\_Firewall\_7.0\_Study\_Guide-Online 147

upvoted 4 times

🗲️ 👤 **Quetchup** 1 year, 7 months ago

**Selected Answer: AC**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 148-149

upvoted 1 times

🗲️ 👤 **zanssanz** 1 year, 7 months ago

I agree with answer A and B, the question is asking for the straight solution; I read it as either or instead of step 1 step 2, I wonder which one is the correct answer. Depending on how we read it can be A and B or A and C.

upvoted 1 times

🗲️ 👤 **Beluga123** 1 year, 8 months ago

A - When 'snat-route-change' is enabled, after a routing change, routing information is flushed from existing SNAT sessions; so, the existing SNAT sessions can use the new best route

C - same distance, different priority : The routing table contains the two static routes but only the one with the lowest priority is used for routing traffic.

upvoted 1 times

🗲️ 👤 **ducduc95** 1 year, 8 months ago

**Selected Answer: AC**

vote A & C



upvoted 1 times

🗲️ 👤 **stalker1ua** 1 year, 8 months ago

**Selected Answer: AC**

vote A & C

upvoted 1 times



  **Seph1** 1 year, 9 months ago

**Selected Answer: AC**

A - to change the route when failover happens



C - to force the failover

upvoted 2 times

  **mastheooo** 1 year, 9 months ago

A & C for answer , snat-route for force existing traffic (may\_dirty flag)

upvoted 1 times

  **pcbbj** 1 year, 9 months ago

A and C

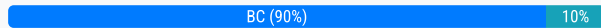
upvoted 3 times

What are two functions of automation stitches? (Choose two.)

- A. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.
- B. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.
- C. Automation stitches can be created to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.
- D. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

**Suggested Answer: BC**

Community vote distribution



**racdab** Highly Voted 1 year, 9 months ago

**Selected Answer: BC**

yes B and C are Correct  
upvoted 8 times

**nabillose** Most Recent 9 months, 1 week ago

Yes B & C are correct  
upvoted 1 times

**Tcmh** 11 months, 1 week ago

**Selected Answer: BC**

A is incorrect, within security fabric, you need to configure automation in root fortigate  
D is incorrect, parallel don't have delay option  
upvoted 1 times

**adiaz\_** 11 months, 2 weeks ago

A y B 100%  
upvoted 1 times

**romartinedg** 1 year, 1 month ago

B,C son correctas  
upvoted 3 times

**certifi46** 1 year, 5 months ago

**Selected Answer: BC**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 23, 26  
upvoted 2 times

**Quetchup** 1 year, 7 months ago

**Selected Answer: BC**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 23, 26  
upvoted 2 times

**ducdud95** 1 year, 8 months ago

**Selected Answer: BC**

yes B and C  
upvoted 1 times

**chgoonk** 1 year, 8 months ago

Sequential execution allows you to configure a delay between actions to allow for tasks to be completed before proceeding to the next action. not D  
upvoted 1 times

**daac84** 1 year, 9 months ago

page 23 "however, a security fabric is not a requirement to use stitches"  
upvoted 3 times

**Seph1** 1 year, 9 months ago



**Selected Answer: BC**

B and C are correct.

Configuration on root only.

In parallel mode, you can not use actions parameters



upvoted 3 times

  **JackeD** 1 year, 9 months ago

**Selected Answer: BC**

B and C because only the root is configured for stitches



upvoted 2 times

  **racdab** 1 year, 9 months ago

**Selected Answer: AB**

I would say A and B



upvoted 1 times

  **klapek** 1 year, 9 months ago

In security fabric stitches are configured on Root only.

B and C are correct

upvoted 5 times

  **racdab** 1 year, 9 months ago

**Selected Answer: AB**




I would say A and B

upvoted 1 times








Refer to the exhibit, which shows a partial web filter profile configuration.



**FortiGuard Category Based Filter**


Name	Action
 Bandwidth Consuming 6	
Freeware and Software Downloads	 Allow
File Sharing and Storage	 Block




**Static URL Filter**



URL Filter 

 Create New
  Edit
  Delete
 Search 

URL	Type	Action	Status
*.dropbox.com	Wildcard	 Allow	 Enable

**Content Filter** 

 Create New
  Edit
  Delete

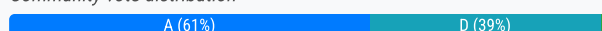
Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	 Exempt	 Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

- A. FortiGate will block the connection, based on the FortiGuard category based filter configuration.
- B. FortiGate will block the connection as an invalid URL.
- C. FortiGate will exempt the connection, based on the Web Content Filter configuration.
- D. FortiGate will allow the connection, based on the URL Filter configuration.

**Suggested Answer: A**

Community vote distribution




 **tururu1496**  1 year, 9 months ago

**Selected Answer: D**

Order of operation is:

1. URL filter
2. FortiGuard Web Filtering
3. Web content filter
4. Web script filter
5. Antivirus scanning

upvoted 44 times

 **javim** 1 year, 1 month ago

I agree!!

upvoted 1 times

🗨️ 👤 **klapek** 1 year, 9 months ago

URL filter is 'allow' not 'exempt' so it will be block on step 2: FortiGuard Category.

Correct answer is A

upvoted 26 times

🗨️ 👤 **javim** 1 year, 1 month ago

Coorect! If with "allow" action the next step is to check FortiGuard category. If the category action is "block" the connection is blocked.

Correct answer is A

upvoted 5 times

🗨️ 👤 **tururu1496** 1 year, 9 months ago

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-URL-filter-actions-explained/ta-p/206632>

upvoted 5 times

🗨️ 👤 **tururu1496** 1 year, 9 months ago

A is actually correct. My bad

upvoted 19 times

🗨️ 👤 **Rudi36** Highly Voted 1 year, 6 months ago

So, I didn't find this is the training material, however it's specified on Fortinet.com, correct answer is A.

When FortiGate performs a web filter check, it will first check the static URL filter list (if applied to the profile) and based on the action, will then perform the FortiGuard category check.

'Action' descriptions in Static URL see bellow:

- 'Block' -> destination is blocked and session dropped, no further category check is needed.

- 'Allow' -> destination is allowed from the static URL list, FortiGate proceeds with checking the category to decide further action.

- 'Exempt' -> destination is exempted from further inspection and traffic is allowed.

- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Difference-between-action-Allow-and-Exempt-in/ta-p/231334>

upvoted 8 times

🗨️ 👤 **GCISystemIntegrator** Most Recent 4 months, 3 weeks ago

Selected Answer: A

Answer - A -

- 'Allow' -> destination is allowed from the static URL list, FortiGate proceeds with checking the category to decide further action. - 'Exempt' -> destination is exempted from further inspection and traffic is allowed.

upvoted 2 times

🗨️ 👤 **cbu\_ch** 9 months ago

Selected Answer: A

Order of operation is:

1. URL filter
2. FortiGuard Web Filtering
3. Web content filter
4. Web script filter
5. Antivirus scanning

URL filter = ALLOW continues to evaluate the next steps, incl. Web Filtering.

If it is required to Allow access to a site regardless of the category, then use "Exempt".

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-URL-filter-actions-explained/ta-p/206632>

upvoted 2 times

🗨️ 👤 **FortiNoob** 9 months, 4 weeks ago

Selected Answer: A

A is indeed correct

upvoted 3 times

🗨️ 👤 **LAFNELL** 10 months ago

**Selected Answer: A**

Correct answer is 100% A. Check Study Guide p350

During web Filtering Inspection, Fortigates first check the Static Url Filter list, then the fortiguard categories, and then the content filter list. So even if the static url is allowing the site, it will be blocked and dropped by the fortiguard categories action.

upvoted 3 times

🗲️ 👤 **mikerss** 10 months, 2 weeks ago

**Selected Answer: A**

The correct answer is A. Explanation:

[https://community.fortinet.com/t5/FortiGate/Technical-Note-List-of-web-filtering-steps-and-their-order-of/ta-p/197439?](https://community.fortinet.com/t5/FortiGate/Technical-Note-List-of-web-filtering-steps-and-their-order-of/ta-p/197439?cmd=displayKC&docType=kc&externalId=11158)

[cmd=displayKC&docType=kc&externalId=11158](https://community.fortinet.com/t5/FortiGate/Technical-Note-List-of-web-filtering-steps-and-their-order-of/ta-p/197439?cmd=displayKC&docType=kc&externalId=11158)

Web filters are applied in this specific order:

- 1 URL Filter
- 2 FortiGuard Web Filter (also called Category Block)
- 3 Content Filter (Web Content Filter)
- 4 Script Filter (filters for Java applets, ActiveX controls and cookies, CLI config only)
- 5 Antivirus scanning

The URL filter list is processed in order from top to bottom. An exempt match stops all further checking including AV scanning. An allow match exits the URL filter list and checks the other web filters.

In this case, the action in the URL Filter is "allow" therefore the FortiGate checks the other web filters. In this case, the next web filter is the FortiGuard Category Based Filter, which in this case is set to block.

Therefore traffic is blocked based on the FortiGuard Category Based Filter.

upvoted 4 times

🗲️ 👤 **mordechayd** 10 months, 4 weeks ago

**Selected Answer: A**

A - action allow on local wf do not bypass fortiguard wF

upvoted 3 times

🗲️ 👤 **ricjscarvalho** 11 months, 3 weeks ago

A

the order is

- URL filter
2. FortiGuard Web Filtering
3. Web content filter
4. Web script filter
5. Antivirus scanning

But to be allowed without matching any other criteria it should be exempt and not allowed

upvoted 2 times

🗲️ 👤 **red74** 1 year ago

A: Allow

The traffic is passed to the remaining FortiGuard web filters, web content filters, web script filters, antivirus proxy operations, and DLP proxy operations. If the URL does not appear in the URL list, the traffic is permitted.

upvoted 2 times

🗲️ 👤 **PoBratsky** 1 year ago

**Selected Answer: A**

Web Filtering inspection is performed in the following order:

- 1 - URL filter
- 2 - FortiGuard Web Filter (FortiGuard Category Based Filter)
- 3 - Web Content Filter
- 4 - Advanced Filter Options

In this case: URL Filter - allow. But in the second step, the blocks by the Category Based Filter.

upvoted 3 times

🗨️ 👤 **fy64** 1 year, 1 month ago

**Selected Answer: A**

I've simulated configuration. It is being blocked because of category block. The answer is 100% A.  
upvoted 5 times

🗨️ 👤 **olimmu** 1 year, 1 month ago

**Selected Answer: A**

action allow, not exempt in URL list  
upvoted 2 times

🗨️ 👤 **KocX** 1 year, 1 month ago

**Selected Answer: A**

if it was exempt instead of allow on URL filter, it would not be blocked.  
upvoted 3 times

🗨️ 👤 **jdubyah\_** 1 year, 1 month ago

**Selected Answer: D**

I agree with tururu1496.  
upvoted 2 times

🗨️ 👤 **Rottcrown95** 1 year, 1 month ago

**Selected Answer: D**

URL filter goes First  
upvoted 2 times

🗨️ 👤 **scheuri** 1 year, 1 month ago

**Selected Answer: A**

Answer A is correct.

Reason: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Difference-between-action-Allow-and-Exempt-in/ta-p/231334>

In the URL Filter (which is checked FIRST) dropbox.com is ONLY allowed which prompts Fortigate to check further in the UTM (next is FortiGuard Web Filtering which BLOCKS file sharing).

In Order for D to be correct, the URL Filter would need to set dropbox.com on "exempt" (which leads the fortigate to stop checking and allow the traffic at once).  
upvoted 4 times

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```

Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
  inbound
    spi: 01e54b14
    enc: aes-cb 914dc5d092667ed436ea7f6efb867976
    auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
  outbound
    spi: 3dd3545f
    enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
    auth: sha1 edd8141f4956140eef703d9042621d3dbf5cd961
  NPU acceleration: encryption(outbound) decryption(inbound)

```

Based on the output, which two statements are correct? (Choose two.)

- A. The npu\_flag for this tunnel is 03.
- B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
- C. Anti-replay is enabled.
- D. The npu\_flag for this tunnel is 02.

**Suggested Answer:** AC


Community vote distribution

AC (100%)

 **johnnd** Highly Voted 1 year ago

**Selected Answer: AC**

npu\_flag=00 Both IPsec SAs loaded to the kernel  
 npu\_flag=01 Outbound IPsec SA copied to NPU  
 npu\_flag=02 Inbound IPsec SA copied to NPN  
 npu\_flag=03 Both outbound and inbound IPsec SA copied to NPU  
 npu\_flag=20 Unsupported cipher or HMAC, IPsec SA cannot be offloaded  
 upvoted 13 times

 **romartinedg** Most Recent 7 months, 3 weeks ago

A,C son correctas  
 upvoted 1 times

 **nerrabacer** 7 months, 4 weeks ago

screenshot is the correct?  
 upvoted 1 times

🗄️ 👤 **certifi46** 11 months, 3 weeks ago

**Selected Answer: AC**

npu\_flag=03 Both outbound and inbound IPsec SA copied to NPU

"set replay enable" under config vpn ipsec phase2-interface in order to enable Anti-Replay  
upvoted 3 times

🗄️ 👤 **mau\_80** 10 months, 1 week ago

Is the "set replay enable" screenshot missing?

upvoted 1 times

🗄️ 👤 **Quetchup** 1 year, 1 month ago

**Selected Answer: AC**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 444, 445, 449

upvoted 2 times

🗄️ 👤 **Beluga123** 1 year, 1 month ago

A - npu\_flag=03 Means that both ingress & egress ESP packets will be offloaded.

C - "set replay enable" under config vpn ipsec phase2-interface in order to enable Anti-Replay

upvoted 2 times

🗄️ 👤 **Seph1** 1 year, 3 months ago

A and C are correct

upvoted 2 times

Refer to the exhibit, which shows a session table entry.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=redir local may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

Which statement about FortiGate behavior relating to this session is true?

- A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate is performing security profile inspection using the CPU.
- D. FortiGate applied only IPS inspection to this session.

**Suggested Answer: B**

Community vote distribution

C (97%)

 **Seph1** Highly Voted 1 year, 8 months ago

**Selected Answer: C**

C - is correct.

url\_cat=41 - web filter is on.

NPU is 0/0 so only CPU is working

upvoted 5 times

 **mikerss** Most Recent 10 months, 2 weeks ago

**Selected Answer: C**

C is the correct answer.

This article explains that inspection is being done because proto\_state=11

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/196988?externalID=FD30042>

proto\_state: state of the session (depending on protocol)

For TCP, the first number (from left to right) is related to the server-side state and is 0 when the session is not subject to any inspection (flow or proxy). If flow or proxy inspection is done, then the first digit will be different from 0.

The second digit is the client-side state. The table above correlates the second-digit value with the different TCP session states. For example, when FortiGate receives the SYN packet, the second digit is 2. It changes to 3 when the SYCK packet is received. After the three-way handshake, the state value changes to 1.

This article explains that traffic is not offloaded to npu: <https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-Is-a-session-offloaded-Hardware-acceleration/ta-p/193373>

If traffic is not offloaded on any direction, it would appear as follows:

offload=0/0.

upvoted 1 times

🗨️ **BlackDealth** 12 months ago

C is correct

In the output from the diagnose sys session list command on a FortiGate device, the offload=0/0 information under the npu info section signifies that the session in question is not being offloaded to a Network Processing Unit (NPU), but is instead being handled by the Central Processing Unit (CPU).

Here's a breakdown of what this information means:

offload=0/0:

The two numbers represent the offload state for both directions of traffic (usually inbound and outbound).

The first number represents one direction (e.g., inbound), and the second number represents the other direction (e.g., outbound).

A value of 0 indicates that offloading to the NPU is not occurring for that direction of traffic.

Indication of CPU-based Processing:

When you see offload=0/0, it's an indication that the security profile inspection for this particular session is being processed by the CPU, rather than being offloaded to an NPU.

Offloading to an NPU would typically be represented with non-zero values in this field.

upvoted 3 times

🗨️ **PoBratsky** 1 year ago

01 - session established for non-proxy traffic.

11 - client-side session established (pc->fgt), and server-side session established (fgt->server)

upvoted 1 times

🗨️ **romartinedg** 1 year, 1 month ago

C es correcta

upvoted 1 times

🗨️ **cedigger** 1 year, 3 months ago

**Selected Answer: C**

Recording to NPU Values no offloading. So C is correct

upvoted 2 times

🗨️ **stetter2006** 1 year, 5 months ago

**Selected Answer: C**

proto\_state=11

upvoted 3 times

🗨️ **fottyfan** 1 year, 5 months ago

**Selected Answer: C**

first digit in state 11 says inspection, offload 0 means CPU is used

upvoted 3 times

🗨️ **certifi46** 1 year, 5 months ago

**Selected Answer: C**

wb enabled, proto\_state=11, offload= 0/0

upvoted 2 times

🗨️ **ducdudc95** 1 year, 6 months ago

**Selected Answer: B**

B, By looking at the NAT and GTW IPs, it is clear that the traffic is coming and going far. So no inspection as an ISP will do with a packet coming from a customer and going elsewhere

upvoted 1 times

🗨️ **ducdudc95** 1 year, 6 months ago

B, By looking at the NAT and GTW IPs, it is clear that the traffic is coming and going far. So no inspection as an ISP will do with a packet coming from a customer and going elsewhere

upvoted 1 times

🗨️ **Quetchup** 1 year, 7 months ago



**Selected Answer: C**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 91, 92

First digit of "proto\_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage  
upvoted 3 times

🗨️ 👤 **kashir** 1 year, 7 months ago

C is correct, the protocol state is 11, first digit is for server which means it is processed by proxy or flow inspection  
upvoted 2 times

🗨️ 👤 **djela45** 1 year, 8 months ago

proto\_state=11 means proxy-inspection means CPU inspects the traffic  
upvoted 1 times

🗨️ 👤 **MrMaxe** 1 year, 9 months ago

**Selected Answer: C**

I think if it was the captive portal redirection, it would need the "auth" state.  
as the redir state is there, it can't be "B".  
redir + no NPU state and offload 0/0 means the CPU did the job, so C is good.  
as there is a url\_cat, it's not only doing IPS inspection.  
upvoted 3 times

🗨️ 👤 **wisv2269** 1 year, 9 months ago

It has "local" as flag. That means "Session is attached to local fortigate ip stack" which I think is because of captive portal  
upvoted 1 times

🗨️ 👤 **tururu1496** 1 year, 9 months ago

**Selected Answer: C**

pcbbj is right  
upvoted 2 times

Refer to the exhibits, which contain the partial configurations of two VPNs on FortiGate.

```
config vpn ipsec phase1-interface
edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

```
config vpn ipsec phase1-interface
edit "user-2"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-2"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must the administrator make to fix the issue? (Choose two.)

- A. Use different pre-shared keys on both VPNs.
- B. Enable XAuth on both VPNs.
- C. Set up specific peer IDs on both VPNs.
- D. Change to aggressive mode on both VPNs.

**Suggested Answer:** BC

Community vote distribution

CD (100%)

 **kocalin** Highly Voted 1 year, 3 months ago

**Selected Answer:** CD

"In case of multiple dialup VPN with PSK, the same local GW and the same SA settings, we have to use aggress. mode and different peer IDs" - Study Guide page 421  
upvoted 12 times

 **pcbbj** Highly Voted 1 year, 3 months ago

**Selected Answer:** CD

To set peer-id, the VPN must be set in aggressive mode - <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-Peer-IDs-to-select-an-IPsec-dialup/ta-p/192292>  
upvoted 10 times

 **xxismailh0** Most Recent 5 months, 3 weeks ago

**Selected Answer:** CD

we need to set a Set up specific peer IDs on both VPNs. and Change to aggressive mode on both VPNs.

upvoted 1 times

🗲️ 👤 **marco\_a** 10 months, 2 weeks ago

**Selected Answer: CD**

c+d are corrects

upvoted 1 times

🗲️ 👤 **certifi46** 11 months, 3 weeks ago

**Selected Answer: CD**

aggressive mode + set peer-id

upvoted 2 times

🗲️ 👤 **Nope\_123** 1 year, 1 month ago

**Selected Answer: CD**

You must use aggressive mode and different peer IDs (C & D)

Page 421 of 7.0 study guide

upvoted 2 times

🗲️ 👤 **sahin** 1 year, 1 month ago

B and C is correct

Study guide page 421

upvoted 1 times

🗲️ 👤 **ducdud95** 1 year, 2 months ago

**Selected Answer: CD**

To set peer-id, the VPN must be set in aggressive mode - <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-Peer-IDs-to-select-an-IPSec-dialup/ta-p/192292>

upvoted 1 times

🗲️ 👤 **Seph1** 1 year, 2 months ago

**Selected Answer: CD**

C & D - are correct.

Set peer-id and aggressive mode

upvoted 2 times

🗲️ 👤 **tururu1496** 1 year, 3 months ago

**Selected Answer: CD**

pcbbj is correct

upvoted 3 times

Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.1.254 dev=3(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9(port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 100.64.1.254, port1
   [10/0] via 100.64.2.254, port2, [10/0]
C 10.1.0.0/24 is directly connected, port3
S 10.1.10.0/24 [10/0] via 10.1.0.1, port3
C 100.64.1.0/24 is directly connected, port1
C 100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- A. Set the priority of the static default route using port1 to 10.
- B. Set the priority of the static default route using port2 to 1.
- C. Set preserve-session-route to enable.
- D. Set snat-route-change to enable.

**Suggested Answer: B**

Community vote distribution

A (100%)

**Hesoyam** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

Correct answer is A. ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.

upvoted 12 times

**pcbbj** Highly Voted 1 year, 3 months ago

**Selected Answer: A**

By the 'get router info kernel' output, it's possible to note that route via port1 has prio=0 and route via port2 prio=10. This way, to use ECMP, both priority must have the same value - <https://community.fortinet.com/t5/FortiGate/Technical-Note-Routing-behavior-depending-on-distance-and-ta-p/198221>

upvoted 10 times

**marco\_a** Most Recent 10 months, 2 weeks ago

**Selected Answer: A**

A 100%

upvoted 1 times

**certif46** 11 months, 3 weeks ago

**Selected Answer: A**

Ecmp => same priority and ad

upvoted 2 times

**ducduc95** 1 year ago

**Selected Answer: A**

ECMP pre-requisite is "routes must have the same destination and costs. By the 'get router info kernel' output, it's possible to note that route via port1 has prio=0 and route via port2 prio=10.

upvoted 1 times

**Lerod** 1 year ago

I believe answer B is correct too in this case.

Default priority value is 1 for static routes.

Output from device:

priority Enter an integer value from <1> to <65535> (default = <1>).

upvoted 1 times

🗨️ 👤 **asa1245112345** 12 months ago

Note that defining no priority in route 1 will set a default value of 0.

<https://community.fortinet.com/t5/FortiGate/Technical-Note-Setting-priority-on-static-default-routes-to/ta-p/196645>

So the right answer is A

upvoted 2 times

🗨️ 👤 **Quetchup** 1 year, 1 month ago

**Selected Answer: A**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 131

upvoted 3 times

🗨️ 👤 **Seph1** 1 year, 2 months ago

A - is correct.

upvoted 1 times

🗨️ 👤 **tururu1496** 1 year, 3 months ago

**Selected Answer: A**

<https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/25967/equal-cost-multi-path>

upvoted 2 times

Refer to the exhibit, which shows a partial routing table.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C      10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C      10.1.0.0/24 is directly connected, port3
S      10.10.4.0/24 [10/0] via 10.1.0.100, port3
C      10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S      10.1.0.0/24 [10/0] via 10.72.3.254, port4
C      10.72.3.0/24 is directly connected, port4
S      192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, what two changes would an administrator need to make if they wanted to send traffic from a client directly connected to port3, to a server directly connected to port4? (Choose two.)


- A. Configure route leaking between VRF 12 and VRF 21.
- B. Disable auto-asic-offload as this is not supported between VRF instances.
- C. Configure RIPv2 to exchange route information between the VRF instances.
- D. Configure route leaking between port3 and port4.
- E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

**Suggested Answer: AC**

Community vote distribution

AE (89%)


11%

 **accessmsc** 8 months, 1 week ago

**Selected Answer: AC**

learn it in udemy

upvoted 2 times

 **mau\_80** 1 year, 3 months ago

**Selected Answer: AE**

A -> you need to configure route leaking

E -> net 10.1.0.0/24 overlaps, so SNAT can bypass the RPF check

upvoted 4 times

 **fortiexpertguy** 1 year, 1 month ago

Hi mau\_80, could you please provide a more detailed explanation of why there is an overlap with subnet 10.1.0.0/24? This subnet is directly connected in VRF=12 and is reachable via a static route in the VRF=21 route table. It has not been duplicated in the locally connected networks of both VRFs.

Thank you in advance.

upvoted 1 times

 **certifi46** 1 year, 5 months ago

**Selected Answer: AE**

A and E

upvoted 1 times

 **Quetchup** 1 year, 7 months ago

**Selected Answer: AE**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 148, 159

upvoted 1 times

🗨️ 👤 **Seph1** 1 year, 8 months ago

**Selected Answer: AE**

A & E seems correct:

A - is correct - you need to configure VRF route leaking

B - didn't find anything to confirm this.

C - Rip is not supported

D - route leaking configuration is not on interfaces.

E - sounds right.

upvoted 4 times

🗨️ 👤 **Nappel** 1 year, 9 months ago

C is not correct: <https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/509828/vrf-routing-support>

upvoted 1 times

🗨️ 👤 **pcbbj** 1 year, 9 months ago

**Selected Answer: AE**

RIP doesn't support VRF

upvoted 4 times

🗨️ 👤 **Hesoyam** 1 year, 9 months ago

**Selected Answer: AE**

I think the answers are A and E because RIP is not supported in VRF.

upvoted 3 times

What is the diagnose test application ipsmonitor 5 command used for?

- A. To enable IPS bypass mode
- B. To disable the IPS engine
- C. To restart all IPS engines and monitors
- D. To provide information regarding IPS sessions

**Suggested Answer: D**

Community vote distribution

A (100%)

 **pcbbj** Highly Voted 2 years, 3 months ago

**Selected Answer: A**

# diagnose test application ipsmonitor

5: Toggle bypass status

13: IPS session list

98: Stop all IPS engines

99: Restart all IPS engines and monitor

upvoted 15 times

 **Iboch46** Most Recent 7 months, 1 week ago

**Selected Answer: A**

If there are high CPU usage problems that the IPS caused, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode

fortinet-network-security-support-engineer-study-guide-for-fortios-7.2 page 269


upvoted 1 times

 **nse\_student** 1 year, 10 months ago

**Selected Answer: A**


A is 100% ok.

upvoted 2 times

 **fosi130** 1 year, 11 months ago


response is A

upvoted 1 times

 **[Removed]** 1 year, 11 months ago

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 405

upvoted 2 times

 **certifi46** 1 year, 11 months ago

**Selected Answer: A**


Study guide page 405

upvoted 2 times

 **TylerNSE** 2 years, 1 month ago

A - is correct

upvoted 1 times

 **mader** 2 years, 1 month ago

A - study guide pg 405

upvoted 1 times

 **Moprekh95** 2 years, 1 month ago

i think the correct answer is A

upvoted 1 times



🗨️ 👤 **djela45** 2 years, 2 months ago

A - definitely

upvoted 1 times

🗨️ 👤 **Seph1** 2 years, 2 months ago

Selected Answer: A

A - Bypass

upvoted 1 times

🗨️ 👤 **johnnd** 2 years, 3 months ago

Selected Answer: A

The Answer is A

upvoted 2 times

🗨️ 👤 **Alaba** 2 years, 3 months ago

The Answer is A

upvoted 4 times

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.  
What can the administrator do to fix this problem?

- A. Configure remote link monitoring to detect an issue in the forwarding path.
- B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
- C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
- D. Configure set link-failed-signal enable under config system ha on both cluster members.

**Suggested Answer: B**

Community vote distribution

D (100%)

🗳️ 👤 **LiliRose** Highly Voted 1 year, 9 months ago

**Selected Answer: D**

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.
- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

#Config system ha

set link-failed-signal enable

end

- This simulates a link failure that clears the related entries from MAC table of the switches.

upvoted 7 times

🗳️ 👤 **myrmidon3** Most Recent 3 months, 1 week ago

**Selected Answer: D**

After an HA failover, Gratuitous ARP (GARP) packets are sent by the new primary FortiGate to update the switches' MAC forwarding tables. However, some switches, especially high-end ones, might not update their MAC tables correctly, even after receiving GARPs.

To address this, you can use the command:

config system ha

set link-failed-signal enable

end

This command forces the former primary FortiGate to shut down its interfaces for one second (except heartbeat and reserved management interfaces). This simulates a link failure, causing the switches to clear their MAC table entries and correctly redirect traffic to the new primary.

upvoted 1 times

🗳️ 👤 **Tcmh** 11 months, 2 weeks ago

**Selected Answer: D**

study guide 7.2 page 98

upvoted 4 times

🗳️ 👤 **charruco** 9 months ago

does this valid to 7.2?

upvoted 1 times

🗳️ 👤 **certifi46** 1 year, 5 months ago

**Selected Answer: D**

Study guide page 206

upvoted 3 times

🗳️ 👤 **Nope\_123** 1 year, 7 months ago

**Selected Answer: D**

D is correct, see page 206 of 7.0 study guide

upvoted 2 times

🗨️ 👤 **Seph1** 1 year, 8 months ago

**Selected Answer: D**

D - is correct.

upvoted 1 times

🗨️ 👤 **JackeD** 1 year, 9 months ago

**Selected Answer: D**

D of course

upvoted 2 times

🗨️ 👤 **NoB0dY366** 1 year, 9 months ago

The answer is D

upvoted 3 times

🗨️ 👤 **johnnd** 1 year, 9 months ago

**Selected Answer: D**

link-failed-signal - Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.

upvoted 4 times

🗨️ 👤 **tururu1496** 1 year, 9 months ago

**Selected Answer: D**

D is correct. This forces ports to flap so that the switch clears CAM table

upvoted 2 times

🗨️ 👤 **Alaba** 1 year, 10 months ago

The answer is D

upvoted 4 times

Which statement about IKE and IKE NAT-T is true?

- A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.
- B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.
- C. They both use UDP as their transport protocol and the port number is configurable.
- D. They each use their own IP protocol number.

**Suggested Answer: B**

Community vote distribution

C (100%)

🗳️ 👤 **caleidoscopio** 5 months, 1 week ago

Answer: C

IKE default port (500)

IKE NAT-T default port (4500)

Both ports can be configured.

upvoted 2 times

🗳️ 👤 **certifi46** 5 months, 2 weeks ago

**Selected Answer: C**

They both use UDP as their transport protocol and the port number is configurable

upvoted 1 times

🗳️ 👤 **Quetchup** 7 months ago

**Selected Answer: C**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 414, 443

upvoted 2 times

🗳️ 👤 **Seph1** 8 months, 4 weeks ago

C - is correct

upvoted 1 times

🗳️ 👤 **pcbbj** 9 months, 3 weeks ago

**Selected Answer: C**

IKE without NAT-T runs over UDP port 500. IKE with NAT-T runs over UDP port 4500. It can be configurable - <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/33578/configurable-ike-port>

upvoted 4 times

🗳️ 👤 **johnnd** 9 months, 3 weeks ago

**Selected Answer: C**

Also agree in C

upvoted 2 times

🗳️ 👤 **Hesoyam** 9 months, 4 weeks ago

**Selected Answer: C**

The right answer is C.

upvoted 4 times

Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0 tun_id=10.200.4.1 dst_mtu=1500 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev
frag-rfc accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=2
src: 0:10.1.2.0/255.255.255.0:0
dst: 0:10.1.1.0/255.255.255.0:0
SA: ref=3 options=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42900/43200
dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which two statements are correct? (Choose two.)

- A. The remote gateway has quick mode selectors containing a destination subnet of 10.1.2.0/24.
- B. The remote gateway IP is 10.200.5.1.
- C. DPD is disabled.
- D. Anti-replay is enabled.

**Suggested Answer: AB**

Community vote distribution

AD (100%)

 **pcbbj**  1 year, 3 months ago

**Selected Answer: AD**

Since the local subnet is 10.1.2.0/24, the remote gateway has the destination subnet as 10.1.2.0.

The remote gateway IP is 10.200.4.1.

DPD is enabled (dpd-link=on)

upvoted 8 times

 **Tcmh**  5 months, 1 week ago

**Selected Answer: AD**

BC is wrong

upvoted 1 times

 **nse\_student** 10 months, 1 week ago

**Selected Answer: AD**

AD 100%

upvoted 1 times

 **fosi130** 11 months, 1 week ago

AD is the correct answer

upvoted 1 times

 **certifi46** 11 months, 3 weeks ago

**Selected Answer: AD**

Anti-replay is enabled => the replaywin=2048

10.1.2.0/24 is the local subnet so it's remote dst for the peer

upvoted 3 times

🗨️ 👤 **Bluegrass168** 1 year ago

**Selected Answer: AD**

A and D.

For D -> the replaywin=2048. So, Anti-replay is enabled.

upvoted 2 times

🗨️ 👤 **Quetchup** 1 year, 1 month ago

**Selected Answer: AD**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 427, 444

upvoted 1 times

🗨️ 👤 **mader** 1 year, 1 month ago

dpd-link=on ,so C is wrong

upvoted 1 times

🗨️ 👤 **saudiboy** 1 year, 2 months ago

**Selected Answer: AD**

Correct answer is A, D

upvoted 1 times

🗨️ 👤 **Seph1** 1 year, 2 months ago

**Selected Answer: AD**

A & D - are correct.

upvoted 2 times

🗨️ 👤 **SHASKAN** 1 year, 2 months ago

**Selected Answer: AD**

For me A & D

upvoted 1 times

🗨️ 👤 **Hesoyam** 1 year, 3 months ago

Correct answers are A and D.

upvoted 1 times

Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

- A. Only the DR receives link state information from non-DR routers.
- B. Non-DR and non-BDR routers form full adjacencies to DR only.
- C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
- D. FortiGate first checks the OSPF ID to elect a DR.

**Suggested Answer: D**

Community vote distribution

C (100%)

🗳️ **sbirare** 8 months, 3 weeks ago

**Selected Answer: C**

Study guide page 282

DR or BDR sends LSA updates and ack on 224.0.0.5

All other routers sends LSA updates and ack on 224.0.0.6

upvoted 4 times

🗳️ **nse\_student** 10 months, 1 week ago

**Selected Answer: C**

C 100%

upvoted 2 times

🗳️ **fosi130** 11 months, 1 week ago

C is correct

upvoted 1 times

🗳️ **certifi46** 11 months, 3 weeks ago

**Selected Answer: C**

Study guide page 282

upvoted 2 times

🗳️ **ciscodiscoo** 1 year ago

**Selected Answer: C**

C appears to be the best option

upvoted 1 times

🗳️ **Quetchup** 1 year, 1 month ago

**Selected Answer: C**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 282

upvoted 1 times

🗳️ **Seph1** 1 year, 2 months ago

**Selected Answer: C**

C - is only making sense.

upvoted 1 times

🗳️ **chgook** 1 year, 2 months ago

The OSPF network elects the router with the highest priority as the DR. If two or more routers are tied with the highest priority, the network elects the router with the highest OSPF ID. D is incorrect

upvoted 3 times

🗳️ **johnnd** 1 year, 3 months ago

**Selected Answer: C**


Some special IP multicast addresses are reserved for OSPF:

224.0.0.5: All OSPF routers must be able to transmit and listen to this address.

224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address.

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>



upvoted 3 times

  **tururu1496** 1 year, 3 months ago

**Selected Answer: C**

C is correct. Although B looks right, it is not correct as they also form full adjacency with BDR.

upvoted 3 times

  **klapek** 1 year, 3 months ago

**Selected Answer: C**

224.0.0.6 is for all non DR routers so correct

Fortigate first checks priority and after that it checks OSPF ID

upvoted 4 times



An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMs in FortiManager. How should the administrator accomplish this task?

- A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.
- B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.
- C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.
- D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗲️ 👤 **johnnd** Highly Voted 1 year, 3 months ago

**Selected Answer: B**

Visual representation: <https://i.imgur.com/mKLNrO4.png>  
upvoted 10 times

🗲️ 👤 **Primo\_SP** Most Recent 8 months, 2 weeks ago

**Selected Answer: B**

Correct answer B  
upvoted 2 times

🗲️ 👤 **certifi46** 11 months, 3 weeks ago

**Selected Answer: B**

need header policy  
upvoted 1 times

🗲️ 👤 **Quetchup** 1 year, 1 month ago

**Selected Answer: B**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 244  
upvoted 4 times

🗲️ 👤 **Seph1** 1 year, 2 months ago

**Selected Answer: B**

B - is correct  
upvoted 1 times

Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

- A. route-reflector enable
- B. route-reflector-server enable
- C. route-reflector-client enable
- D. route-reflector-peer enable

**Suggested Answer: A**

Community vote distribution

C (95%)

5%

🗳️ **Hesoyam** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

Correct answer is C.

upvoted 6 times

🗳️ **LoukasR** Most Recent 9 months ago

set route-reflector-client enable

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p328

upvoted 1 times

🗳️ **caleidoscopio** 11 months, 1 week ago

Correct: C

upvoted 1 times

🗳️ **certifi46** 11 months, 3 weeks ago

**Selected Answer: C**

route-reflector-client enable

upvoted 1 times

🗳️ **BoostBoris** 1 year, 1 month ago

**Selected Answer: C**

<https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/572620/config-router-bgp>

set route-reflector-client [enable|disable]

upvoted 1 times

🗳️ **Quetchup** 1 year, 1 month ago

**Selected Answer: C**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 468

upvoted 4 times

🗳️ **akukaracia** 1 year, 2 months ago

C

CLI guide has route-reflector-client only (from this list; the route-server-client exists, -client-vpn, etc.)

upvoted 1 times

🗳️ **Seph1** 1 year, 2 months ago

**Selected Answer: C**

C - is correct.

upvoted 1 times

🗳️ **djela45** 1 year, 3 months ago

**Selected Answer: C**

C is correct



upvoted 1 times

🗳️ **Nappel** 1 year, 3 months ago

**Selected Answer: C**

Correct answer is C: <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-BGP-route-reflector/ta-p/191503>

upvoted 4 times

  **jjeje** 1 year, 3 months ago

**Selected Answer: A**

Correct answer is A

upvoted 1 times

Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf neighbor
```

```
OSPF process 0:
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.0.69	1	Full/DR	00:00:32	10.126.0.69	wan1
0.0.0.117	1	Full/DROther	00:00:34	10.126.0.117	wan2
0.0.0.2	1	Full/-	00:00:38	172.16.1.2	ToRemote

What can be concluded from the debug command output?

- A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.
- B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.
- C. There are more than two OSPF routers on the wan2 network.
- D. The interface ToRemote is a broadcast OSPF network.

**Suggested Answer: B**

Community vote distribution

C (100%)

🗳️ **Nappel** Highly Voted 1 year, 9 months ago

- A: is not right, because the pri is 1
- B: is not right, because the state is Full
- D: is not right, because state "Full/-" is for point-to point OSPF networks.

The only Option left is C, but it the state "Full/DROther" only explains that there are 2 OSPF routers and not more than 2.

upvoted 14 times

🗳️ **Spyder\_Byte** Most Recent 1 year, 4 months ago

**Selected Answer: C**

Makes sense. The first two neighbors are DR/BDR and are in the same subnet, and doesn't the router the command is done on have to be adjacent to the DR/BDR? Meaning there are more than two routers on the WAN2 network.

upvoted 1 times

🗳️ **certifi46** 1 year, 5 months ago

**Selected Answer: C**

All other don't make sense

upvoted 1 times

🗳️ **Quetchup** 1 year, 7 months ago

**Selected Answer: C**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 296

upvoted 1 times

🗳️ **Seph1** 1 year, 8 months ago

**Selected Answer: C**

C - is correct

upvoted 1 times

🗳️ **LiliRose** 1 year, 9 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

🗳️ **DOSKIM** 1 year, 9 months ago

C is correct

upvoted 1 times

🗨️ 👤 **tururu1496** 1 year, 9 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗨️ 👤 **klapek** 1 year, 9 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

🗨️ 👤 **davilop992** 1 year, 9 months ago

Can you explain why it's C?

upvoted 1 times

🗨️ 👤 **klapek** 1 year, 9 months ago

To be specific - C MAY NOT be correct\*, but A, B and D are DEFINITELY NOT correct.

C is correct because state of the neighbor is DR (Drother) which means in that particular multiaccess network segment there are also DR (Designated Router) and BDR (Backup Designated Router).

\* It MAY not be correct because there can be only 2 routers: DR and DRO that has priority 0 configured. In that case there is no BDR.

upvoted 8 times

🗨️ 👤 **Lomik29** 5 months ago

If the neighbor 0.0.0.117 has Priority 1 and State DROther, it means there are at least 2 more routers in the segment that are DR and BDR, otherwise 0.0.0.117 would be either DR or BDR because it is eligible (prio!=0)

upvoted 1 times

Refer to the exhibit, which shows a FortiGate configuration.

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers 1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ''
  set fortiguard-anycast disable
  set antisipam-force-off disable
  set antisipam-cache enable
  set antisipam-cache-ttl 1800
  set antisipam-cache-mpercent 2
  set antisipam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-ip6 ::
  set proxy-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username ''
  set ddns-server-ip 0.0.0.0
  set ddns-server-port 443
end
```

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator do to fix the issue?

- A. Increase webfilter-timeout.
- B. Change protocol to TCP.
- C. Enable fortiguard-anycast.
- D. Disable webfilter-force-off.

**Suggested Answer: D**

Community vote distribution

D (100%)

  **J\_Olin** 5 months, 3 weeks ago



**Selected Answer: D**

With the webfilter-force-off flag set to 'enable' it is telling the FortiGate not to use FortiGuard web filtering. You've enabled turning it off.  
upvoted 2 times

  **[Removed]** 1 year, 5 months ago

**Selected Answer: D**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 367  
upvoted 2 times

  **certifi46** 1 year, 5 months ago

**Selected Answer: D**

set webfilter-force-off disable = WF enabled  
upvoted 1 times

🗲️ 👤 **BoostBoris** 1 year, 7 months ago

**Selected Answer: D**

set webfilter-force-off enable = Turn off the FortiGuard web filtering service.

upvoted 2 times

🗲️ 👤 **Jereban** 1 year, 7 months ago

**Selected Answer: D**

D- is correct

upvoted 2 times

🗲️ 👤 **akukaracia** 1 year, 8 months ago

D - OK

C - wrong. There are 3 methods, anycast is one of them. Read Technical Tip: FortiGuard is not reachable via Anycast default method

upvoted 1 times

🗲️ 👤 **Seph1** 1 year, 8 months ago

**Selected Answer: D**

D - is correct

upvoted 2 times

Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

- A. set av-failopen off
- B. set av-failopen pass
- C. set fail-open enable
- D. set ips fail-open disable

**Suggested Answer:** BD

Community vote distribution

AC (77%)

BC (23%)

  **johnnd** Highly Voted 1 year, 3 months ago

**Selected Answer:** AC

"change the default behavior"

Default:

IPS - disable

AV - pass

Answer:

set av-failopen off



set fail-open enable

Docs:

For IPS: <https://docs.fortinet.com/document/fortigate/7.2.3/cli-reference/409620/config-ips-global>



For AV: <https://docs.fortinet.com/document/fortigate/7.2.3/cli-reference/1620/config-system-global>

upvoted 7 times

  **klapek** 1 year, 3 months ago

correct

upvoted 1 times

  **sauls** 1 year, 3 months ago

but its 7.0, not 7.2

upvoted 1 times

  **johnnd** 1 year ago

You connect but in this case, it is the same.

upvoted 1 times

  **[Removed]** 7 months, 1 week ago

Another point: The default action of "av-failopen" is pass, BUT the default action of "av-failopen-session" is disable. Such as "av-failopen" is just configurable when "av-failopen-session" is enable, B and C are correct.

upvoted 1 times

  **[Removed]** 7 months, 1 week ago

Reading again the question "two configuration commands change the default behavior", you're right, A and C change default behavior

upvoted 1 times

  **racdab** Highly Voted 1 year, 3 months ago

**Selected Answer:** AC

config ips global

set fail-open {enable | disable}

end

When disabled (default), the IPS engine drops all new sessions that require flow-based inspection.

config system global

set av-failopen {pass | off | one-shot}



end

pass

This is the default settings.

upvoted 5 times

🗄️ 👤 **ricjscarvalho** Most Recent 5 months, 3 weeks ago

Selected Answer: AC

A and C: <https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/194558/conserv-mode>

upvoted 1 times

🗄️ 👤 **[Removed]** 7 months, 1 week ago

Selected Answer: AC

These are correct, A and C.

Details.....

upvoted 1 times

🗄️ 👤 **[Removed]** 7 months, 1 week ago

Selected Answer: BC

B,C correct

upvoted 1 times

🗄️ 👤 **caleidoscopio** 11 months, 1 week ago

Answer: A, C

upvoted 1 times

🗄️ 👤 **[Removed]** 11 months, 3 weeks ago

Selected Answer: AC

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 61/399

upvoted 1 times

🗄️ 👤 **certifi46** 11 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

🗄️ 👤 **kashir** 1 year ago

Selected Answer A,C

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserv-mode>

upvoted 1 times

🗄️ 👤 **HSilver** 1 year ago

Selected Answer: BC

B & C

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserv-mode>

upvoted 2 times

🗄️ 👤 **HSilver** 1 year ago

I WRONG, CORRECT A & C.

upvoted 2 times

🗄️ 👤 **BoostBoris** 1 year, 1 month ago

Selected Answer: AC

A because av-failopen pass is the default setting in config system global

C because fail-open disable is default in config ips global

Command set ips fail-over does not exist

upvoted 3 times

🗄️ 👤 **Seph1** 1 year, 2 months ago

Selected Answer: AC

A & C - are correct.

set fail-open for IPS

set av-failopen pass|off are correct commands, but the pass is the Default so "off" is correct.

upvoted 1 times

🗄️ 👤 **klapek** 1 year, 3 months ago

**Selected Answer: BC**



B and C are correct

Fail-open for IPS is configured as follows:

'config ips global

set fail-open enable'

upvoted 3 times

  **klapek** 1 year, 3 months ago

A and C are correct as AV default is 'pass'

upvoted 1 times

Refer to the exhibit, which shows the output of a diagnose command.

```
# diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What can you conclude from the output shown in the exhibit? (Choose two.)


- A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.
- B. This is an expected session created by the IPS engine.
- C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.
- D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

**Suggested Answer: AC**

Community vote distribution

AD (93%)

7%

 **Hesoyam** Highly Voted 1 year, 3 months ago

**Selected Answer: AD**

Correct answers are A and D.

upvoted 6 times

 **cedigger** Most Recent 9 months ago

**Selected Answer: AD**

I agree with A and D. Because B and C are wrong. But can anyone explain how I can see this is a pinhole session? I don't get it.

upvoted 1 times

 **piotrb** 9 months ago


see page 115 in the study guide.

upvoted 1 times

 **cedigger** 9 months ago

Nevermind I get it. The flag complex means the session is handled by a session helper!

upvoted 2 times

 **certifi46** 11 months, 3 weeks ago

**Selected Answer: AD**

A and D


upvoted 1 times

 **Quetchup** 1 year, 1 month ago

**Selected Answer: AD**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 110, 111, 115

upvoted 3 times

 **NZhang** 1 year, 1 month ago

A&D are correct

upvoted 1 times

🗨️ 👤 **djela45** 1 year, 2 months ago

I stand corrected: A&D are correct

upvoted 2 times

🗨️ 👤 **fcatena** 1 year, 2 months ago

A & D correct

upvoted 1 times

🗨️ 👤 **Tony87** 1 year, 2 months ago

A and C

upvoted 1 times

🗨️ 👤 **Seph1** 1 year, 2 months ago

**Selected Answer: AD**

A & D - are correct.

10.0.1.10 is a gateway and next-hop IP

upvoted 1 times

🗨️ 👤 **Bsdx** 1 year, 1 month ago

10.0.1.10 is the original source, the output shows the reply packet towards the gateway 10.200.1.1 and destined IP 10.0.1.10 (A,D are correct but your statement is wrong)

upvoted 2 times

🗨️ 👤 **djela45** 1 year, 2 months ago

**Selected Answer: AC**

A & C are correct

upvoted 1 times

🗨️ 👤 **jjeje** 1 year, 2 months ago

**Selected Answer: AD**

Answer

upvoted 1 times

🗨️ 👤 **SHASKAN** 1 year, 2 months ago

**Selected Answer: AD**

A & D seem correct

upvoted 1 times

🗨️ 👤 **harisram** 1 year, 3 months ago

A and D are correct

upvoted 1 times

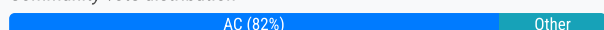
You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.

Which two settings need to be verified for these features to function? (Choose two.)

- A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.
- B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.
- C. Service access needs to be enabled on FortiManager under System Settings > Network.
- D. FortiGate needs to have include-default-servers disabled under config system central-management.

**Suggested Answer: AC**

*Community vote distribution*



🗳️ 👤 **[Removed]** 5 months, 2 weeks ago

**Selected Answer: AC**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 184/185

upvoted 3 times

🗳️ 👤 **certifi46** 5 months, 2 weeks ago

**Selected Answer: AC**

NSE 7.0 Guide page 184-185

upvoted 1 times

🗳️ 👤 **jimmyjampot** 5 months, 3 weeks ago

A and C

upvoted 1 times

🗳️ 👤 **Seph1** 8 months, 3 weeks ago

**Selected Answer: AC**

A & C - are correct.

NSE 7.0 Guide page 184-185

upvoted 2 times

🗳️ 👤 **jjeje** 9 months ago

**Selected Answer: AB**

Answer

upvoted 1 times

🗳️ 👤 **forfe** 9 months ago

A and C

upvoted 1 times

🗳️ 👤 **infodiego** 9 months, 1 week ago

A y D are corrects.

upvoted 1 times

🗳️ 👤 **racdab** 9 months, 1 week ago

D : I don't think so

enable or disable inclusion of public fortiguard servers in the override server list

upvoted 1 times

🗳️ 👤 **racdab** 9 months, 2 weeks ago

**Selected Answer: AC**

yes A and C are Correct

need to configure the service access settings for each interface under system settings> network on fortimanager

upvoted 2 times

🗨️ 👤 **klapek** 9 months, 2 weeks ago

**Selected Answer: AC**

A and C are correct

We can have default servers enabled.

upvoted 1 times

🗨️ 👤 **racdab** 9 months, 2 weeks ago

**Selected Answer: AD**

A D correct

upvoted 1 times

Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROther, Priority 1
Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Neighbor Count is 4, Adjacent neighbor count is 2
Crypt Sequence Number is 411
Hello received 106 sent 27, DD received 6 sent 3
LS-Req received 2 sent 2, LS-Upd received 7 sent 17
LS-Ack received 4 sent 3, Discarded 1
```

Which two statements about the output are true? (Choose two.)

- A. In the network connected to port 4, two OSPF routers are down.
- B. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.5.
- C. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.6.
- D. There are a total of 5 OSPF routers attached to the Port4 network segment.

**Suggested Answer: AB**

Community vote distribution

BD (73%)

CD (27%)

**Darthan** 9 months, 3 weeks ago

**Selected Answer: CD**

For me is C & D, the router isn't DR or BDR, is drother, so he use 224.0.0.6 to speak with the others  
upvoted 2 times

**santimeremans** 1 year, 2 months ago

Why is A not discussed as there is a count of 4 neighbours but only 2 of them are adjacent?  
upvoted 2 times

**ay\_dos** 1 year, 1 month ago

Adjacency is only form with the DR and BDR on the broadcast network. That is why you see in the get router info ospf neighbor output DR/FULL or BDR/FULL and DROther are 2-ways  
upvoted 2 times

**nse\_student** 1 year, 4 months ago

**Selected Answer: CD**

C & D. Updates packets are for 224.0.0.5  
upvoted 1 times

**MarkusJu** 1 year, 3 months ago

It says "hello packets" which are always 224.0.0.5 so it is B & D  
upvoted 2 times

**lulipeoliveira** 1 year, 5 months ago

C & D

C - This Firewall is not a DR or BDR to send hello packages on 224.0.0.5

D - 4 neighbors + Firewall

upvoted 2 times

**[Removed]** 1 year, 5 months ago

**Selected Answer: BD**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 282/295

upvoted 1 times

🗨️ **certifi46** 1 year, 5 months ago

**Selected Answer: BD**

4 neighbors + the router itself = 5 routers

224.0.0.5 for hello packet on broadcast networks.

upvoted 1 times

🗨️ **Seph1** 1 year, 7 months ago

**Selected Answer: BD**

B & D - are correct

B - 4 neighbors + the router itself = 5 routers

D - 224.0.0.5 for Broadcast networks.

upvoted 3 times

🗨️ **fcatena** 1 year, 8 months ago

BD correct

upvoted 1 times

🗨️ **cannoe** 1 year, 8 months ago

Why B? The output showed that this device is a DROTHER. Therefore, it would only send updates and acknowledgments to DR and BDR (224.0.0.6 - ALLDRouters)

upvoted 1 times

🗨️ **FriedExams** 1 year, 8 months ago

224.0.0.5 -HELLO packets are always sent here; also used by DR<->BDR updates

224.0.0.6 -UPDATES from all other routes (NOT HELLO PACKETS)

Do also note in P2P networks; all hello packets/and updates for all routers use 224.0.0.5

upvoted 13 times

🗨️ **SHASKAN** 1 year, 9 months ago

**Selected Answer: BD**

B and D for me not C because hello packet are sent to 225.0.0.5

upvoted 2 times

🗨️ **enasrullayev** 1 year, 9 months ago

224.0.0.6

upvoted 1 times

🗨️ **enasrullayev** 1 year, 9 months ago

**Selected Answer: CD**

Non DR and Non BDR will send updates to 225.0.0.6

upvoted 1 times

🗨️ **tururu1496** 1 year, 9 months ago

**Selected Answer: BD**

BD are correct

upvoted 1 times

🗨️ **klapek** 1 year, 9 months ago

**Selected Answer: BD**

B and D are correct

Hellos always sent to 224.0.0.5 and neighbor count = 4 what means that there is 5 routers on that segment

upvoted 3 times



Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info routing-table database

Routing table for VRF=0
S      0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command output?

- A. The port2 interface is disabled in the FortiGate configuration.
- B. The port1 default route has a lower distance than the default route using port2.
- C. The port1 default route has a higher priority value than the default route using port2.
- D. The port1 default route has a lower priority value than the default route using port2.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗲️ 👤 **mau\_80** 9 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

🗲️ 👤 **nse\_student** 10 months, 1 week ago

**Selected Answer: B**

B 100%

upvoted 1 times

🗲️ 👤 **[Removed]** 11 months, 3 weeks ago

**Selected Answer: B**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 131

upvoted 3 times

🗲️ 👤 **certifi46** 11 months, 3 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

🗲️ 👤 **TylerNSE** 1 year ago

B - is correct

upvoted 1 times

🗲️ 👤 **Seph1** 1 year, 1 month ago

**Selected Answer: B**

B - is correct

upvoted 2 times

🗲️ 👤 **SHASKAN** 1 year, 2 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

  **harisram** 1 year, 3 months ago

B is correct

upvoted 2 times

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

- A. It provides VM license validation services.
- B. It supports rating requests from non-FortiGate devices.
- C. It caches available firmware updates for unmanaged devices.
- D. It can be configured as an update server, a rating server, or both.

**Suggested Answer: D**

*Community vote distribution*

D (50%)

A (50%)

🗳️ 👤 **luismanzanero** 5 months, 3 weeks ago

**Selected Answer: D**

A y D son correctas  
upvoted 2 times

🗳️ 👤 **luismanzanero** 6 months ago

**Selected Answer: D**

A & D are correct  
upvoted 1 times

🗳️ 👤 **KocX** 7 months ago

**Selected Answer: D**

A&D are correct  
upvoted 1 times

🗳️ 👤 **Tailee** 9 months, 1 week ago

A & D are correct  
upvoted 1 times

🗳️ 👤 **mau\_80** 9 months, 1 week ago

**Selected Answer: A**

A & D are correct  
upvoted 1 times

🗳️ 👤 **nse\_student** 10 months, 1 week ago

**Selected Answer: A**

A & D are correct!  
upvoted 1 times

🗳️ 👤 **fottyfan** 11 months, 2 weeks ago

**Selected Answer: D**

A and D  
upvoted 2 times

🗳️ 👤 **[Removed]** 11 months, 3 weeks ago

**Selected Answer: A**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 184  
upvoted 2 times

🗳️ 👤 **ay\_dos** 8 months ago

2 answers required A & D  
upvoted 1 times

🗳️ 👤 **certifi46** 11 months, 3 weeks ago

A and D study guide pag. 184  
upvoted 1 times

🗳️ 👤 **AdamB3** 12 months ago

Selected Answer: D

A and D are correct  
upvoted 1 times

🗲️ 👤 **\_zero** 1 year ago

Selected Answer: D

A and D  
upvoted 1 times

🗲️ 👤 **mohamed\_ehab2009** 1 year ago

A and C  
upvoted 1 times

🗲️ 👤 **mau\_80** 10 months ago

why C? Unmanaged devices -> no firmware caching  
upvoted 1 times

🗲️ 👤 **kleonz** 1 year ago

Selected Answer: A

A and D  
upvoted 1 times

🗲️ 👤 **gautamgarg25** 1 year ago

Selected Answer: A

A,C are correct  
upvoted 1 times

🗲️ 👤 **Seph1** 1 year, 1 month ago

Selected Answer: D

A and D are correct.

\* there is no option to vote for 2 answers

upvoted 1 times

🗲️ 👤 **Bsdx** 1 year, 1 month ago

A and D, study guide pag. 184  
upvoted 1 times

🗲️ 👤 **Tony87** 1 year, 2 months ago

A and D  
upvoted 2 times

Refer to the exhibit, which contains the output of a debug command.

```
# diagnose hardware sysinfo conserve
memory conserve mode:          on
total RAM:                     3040 MB
memory used:                   2706 MB 89% of total RAM
Memory freeable:              334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:     2675 MB 88% of total RAM
memory used threshold green:   2492 MB 82% of total RAM
```

If the default settings are in place, what can be concluded about the conserve mode shown in the exhibit?

- A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.
- B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
- C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
- D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

**Suggested Answer: B**

Community vote distribution

C (84%)

Other

 **pcbbj**  1 year, 9 months ago

I'd say that there is no correct answer, as the command says that the FortiGate is running with default settings.

The correct would be:

"FortiGate is currently ALLOWING new sessions that require PROXY-based content inspection and BLOCKING sessions that require FLOW-based content inspection."


References:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Conserve-mode-changes/ta-p/198502>

<https://docs.fortinet.com/document/fortigate/6.2.12/cookbook/194558/conserve-mode>

Agree?

upvoted 7 times


 **klapek** 1 year, 9 months ago

No, I don't agree.

By default av-failopen-session is disabled and that particular option is responsible for new session behavior in proxy mode. The new sessions are blocked.


By default fail-open is disabled --> new sessions in flow-based inspection mode are blocked too.

upvoted 3 times

 **manimal666** 1 year, 9 months ago


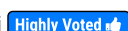
By default, set av-failopen mode is pass not disable which means pcbbj looks legit.

upvoted 2 times

 **racdab** 1 year, 9 months ago

by default fortinet blocks new session( av-failopen-session disable )

upvoted 5 times

 **k3rnelpanicpj**  1 year, 9 months ago

Based on this

<https://docs.fortinet.com/document/fortigate/6.2.12/cookbook/194558/conserv-mode>

Proxy-based have default pass (no inspection)

Flow-based have default disable (drop sessions)

None of answers are correct



upvoted 6 times

  **tuky88** Most Recent 4 months, 2 weeks ago

**Selected Answer: B**



Only extreme threshold drops sessions, red will allow but perform no inspection.

upvoted 1 times

  **Yusraaa** 10 months, 1 week ago

correct answer is C

upvoted 1 times

  **always** 10 months, 3 weeks ago

av-failopen-session kicks in not during a high memory situation (conserv mode) , but when a proxy on FortiGate runs out of available sockets to process more proxy-based inspected traffic. So, none of answers are correct!

upvoted 1 times

  **talos\_2002** 1 year, 2 months ago

When memory usage becomes extreme, all new sessions are dropped.

threshold extreme = 2887

threshold extreme = memory used + freeable

memory used + freeable = 2706 + 334 = 3034

3034 > 2887

The unit is in extreme mode, dropping all new sessions.

upvoted 3 times

  **mikerss** 1 year ago

your calculation does not make sense.

The "allowing" answers are not correct. Therefore my assumption is that it went to extreme mode at some stage, however it did not reach green state yet. Therefore the correct answer is C - block new proxy and flow sessions.

upvoted 1 times

  **mikerss** 1 year ago

Default setting are:

(1) "av-failopen-session" is disabled by default. This block all proxy mode traffic

(2) "av-failopen" is "pass" by default. However since (1) is disable it is irrelevant. For it to work (1) must be enabled

(3) "set fail-open" is disabled by default and drops all new sessions that require flow-based inspection.

Therefore by default in conserv mode all proxy/flow traffic is blocked. Hence only C is valid.

set av-failopen pass

upvoted 1 times

  **FORTIGOD** 1 year, 2 months ago

**Selected Answer: B**

Correct answer is indeed B. av-failopen-session is to address a connection pool issue, av-failopen is to address conserv mode (the topic at hand).

One condition can exist without the other and as the documentation notes, where both are occurring av-failopen is used to resolve any discrepancies (since it takes into account an entire system, not a single connection pool).

upvoted 1 times

  **mau\_80** 1 year, 3 months ago

**Selected Answer: A**

FGT is in extreme mode (89%) so why not A?

upvoted 2 times

  **mikerss** 11 months, 2 weeks ago

it is not in extreme mode. to be in extreme mode it needs to be >95%

upvoted 1 times

  **[Removed]** 1 year, 5 months ago