



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

Review the VPN configuration shown in the exhibit.

```
config vpn ipsec fec
  edit "fecprofile"
    config mappings
      edit 1
        set base 8
        set redundant 2
        set packet-loss-threshold 10
      next
      edit 2
        set base 9
        set redundant 3
        set bandwidth-up-threshold 450000
      next
      edit 3
        set base 5
        set redundant 3
        bandwidth-bi-threshold 5000000
      next
    end
  next
end

config vpn ipsec phase1-interface
  edit "vdl-pl "
    set fec-health-check "1"
    set fec-mapping-profile "fecprofile "
    set fec-base 10
    set fec-redundant 1
  next
end
```

What is the Forward Error Correction behavior if the SD-WAN network traffic download is 500 Mbps and has 8% of packet loss in the environment?

- A. 1 redundant packet for every 10 base packets
- B. 3 redundant packet for every 5 base packets
- C. 2 redundant packet for every 8 base packets
- D. 3 redundant packet for every 9 base packets

**Suggested Answer:** A

*Community vote distribution*

arielon **Highly Voted** 1 year, 5 months ago

**Selected Answer: A**

It's A."The FEC base and redundant values are used when the link quality has not exceeded the limits specified in the FEC profile mapping"

upvoted 8 times

ac89l 11 months, 2 weeks ago

but it did exceed

you should review this:

<https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/367620/config-vpn-ipsec-fec>

bandwidth-bi-threshold: Apply FEC parameters when available bi-bandwidth is >= threshold

So it is "greater or equal"

So if equal , then B is correct.

upvoted 2 times

Rony\_Moussa **Most Recent** 5 months, 2 weeks ago

The exam was changed, anyone has new dump ?

upvoted 3 times

BB\_norway 8 months, 1 week ago

Can someone who took the exam recently confirm if those questions are still valid as of April 2024?

upvoted 1 times

HongHCMC 9 months, 1 week ago

A is correct as 500Mbps has not exceeded 5000000 (5G) specified in the profile

upvoted 2 times

node345 10 months, 1 week ago

5000000 Kbps are 5Gbps and not 500Mbps. Correct answer is A.

upvoted 3 times

ac89l 11 months, 2 weeks ago

**Selected Answer: B**

you should review this:

<https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/367620/config-vpn-ipsec-fec>

bandwidth-bi-threshold: Apply FEC parameters when available bi-bandwidth is >= threshold

So it is "greater or equal"

So if equal , then B is correct.

upvoted 3 times

re\_john 1 year ago

B is correct.

upvoted 1 times

BozoPin 1 year, 2 months ago

**Selected Answer: A**

Exactly that, what arielon wrote

upvoted 1 times

ama6 1 year, 3 months ago

Correct is C :

The FEC configuration in the exhibit specifies that if the packet loss is greater than 10%, then the FEC mapping will be 8 base packets and 2 redundant packets. The download bandwidth of 500 Mbps is not greater than 950 Mbps, so the FEC mapping is not overridden by the bandwidth setting. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Here is the explanation of the FEC mappings in the exhibit:


Packet loss greater than 10%: 8 base packets and 2 redundant packets.

Upload bandwidth greater than 950 Mbps: 9 base packets and 3 redundant packets.

The mappings are matched from top to bottom, so the first mapping that matches the conditions will be used. In this case, the first mapping matches because the packet loss is greater than 10%. Therefore, the FEC behavior will be 2 redundant packets for every 8 base packets.

Reference: <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/169010/adaptive-forward-error-correction-7-0-2>

upvoted 1 times

 **Davidrichard** 1 year, 4 months ago

**Selected Answer: B**

B is correct

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/169010/adaptive-forward-error-correction-7-0-2>

upvoted 3 times

You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output:

```
diag npu np6 dce 1
PDQ_OSW_EHP1 :0000000000001833 [5b]
diag npu np6 dce 1
PDQ OSW EHPI :0000000000000003 [80]
diag npu np6 dce 1
PDQ OSW EHP1 :0000000000000552 [94]
```

Given the information shown in the output, which two statements are true? (Choose two.)

- A. Enabling bandwidth control between the ISF and the NP will change the output
- B. The output is showing a packet descriptor queue accumulated counter
- C. Enable HPE shaper for the NP6 will change the output
- D. Host-shortcut mode is enabled
- E. There are packet drops at the XAUI

**Suggested Answer:** B

Community vote distribution

A (100%)

🗨️ **HongHCMC** 3 months, 1 week ago

PDQ stands for packet descriptor queue so B and E is correct  
upvoted 1 times

🗨️ **node345** 4 months, 1 week ago

**Selected Answer: A**

Enabling bandwidth control can smooth burst traffic and keep the XAUI ports from getting overwhelmed and dropping sessions. Since the ISF has a larger buffer it may be able to handle more traffic.

<https://docs.fortinet.com/document/fortigate/7.4.3/hardware-acceleration/834580/enabling-bandwidth-control-between-the-isf-and-np6-xaui-ports-to-reduce-the-number-of-dropped-egress-packets>

This command displays the number of dropped packets for the selected NP6 processor.

<https://docs.fortinet.com/document/fortigate/7.4.2/hardware-acceleration/48875/diagnose-npu-np6-dce-np6-id-number-of-dropped-np6-packets>  
It is not accumulated counter.

upvoted 1 times

🗨️ **ama6** 9 months, 3 weeks ago

Corret  
B and E  
upvoted 4 times

🗨️ **Noidea** 11 months, 1 week ago

B and E  
upvoted 3 times

Which two methods are supported for importing user defined Lookup Table Data into the FortiSIEM? (Choose two.)

- A. Report
- B. FTP
- C. API
- D. SCP

**Suggested Answer:** AC

*Community vote distribution*

AC (100%)

🗉 👤 **jeabcpe** 2 months, 2 weeks ago

I don't see this question in my exam.  
upvoted 1 times

🗉 👤 **re\_john** 6 months, 1 week ago

Three options - CSV, API and Report.

Correct answers are A and C.

upvoted 2 times

🗉 👤 **ama6** 9 months, 3 weeks ago

A and C

FortiSIEM supports two methods for importing user defined Lookup Table Data:

Report: You can import lookup table data from a report. This is the most common method for importing lookup table data.

API: You can also import lookup table data using the FortiSIEM API. This is a more advanced method that allows you to import lookup table data programmatically.

upvoted 4 times

🗉 👤 **Davidrichard** 10 months ago

**Selected Answer: AC**

A and C

upvoted 3 times

🗉 👤 **Noidea** 11 months, 1 week ago

Agreed: AC

upvoted 3 times

🗉 👤 **arielon** 11 months, 2 weeks ago

**Selected Answer: AC**

[https://help.fortinet.com/fsiem/6-5-0/Online-Help/HTML5\\_Help/importing\\_lookup\\_table\\_data.htm](https://help.fortinet.com/fsiem/6-5-0/Online-Help/HTML5_Help/importing_lookup_table_data.htm)

upvoted 4 times

What is the benefit of using FortiGate NAC LAN Segments?

- A. It provides support for multiple DHCP servers within the same VLAN
- B. It provides physical isolation without changing the IP address of hosts
- C. It provides support for IGMP snooping between hosts within the same VLAN
- D. It allows for assignment of dynamic address objects matching NAC policy

**Suggested Answer: B**

Community vote distribution

B (100%)

 **musaabghanem** Highly Voted 10 months, 1 week ago

**Selected Answer: B**

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments-7-0-1>  
upvoted 9 times


 **HongHCMC** Most Recent 3 months, 1 week ago

**Selected Answer: B**

This is stated in the document.  
upvoted 1 times

 **HongHCMC** 3 months, 1 week ago

Both B and D are correct. But only one answer are selected. Confusion here  
upvoted 1 times

 **pitz** 9 months ago

**Selected Answer: B**

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/856212/nac-lan-segments-7-0-1>  
upvoted 4 times

 **ama6** 9 months, 3 weeks ago

D is correct

FortiGate NAC LAN Segments are a feature that allows users to assign different VLANs to different LAN segments without changing the IP address of hosts or bouncing the switch port. This provides physical isolation while maintaining firewall sessions and avoiding DHCP issues. One benefit of using FortiGate NAC LAN Segments is that it allows for assignment of dynamic address objects matching NAC policy.

upvoted 2 times

You are troubleshooting a FortiMail Cloud service integrated with Office 365 where outgoing emails are not reaching the recipients' mail. What are two possible reasons for this problem? (Choose two.)

- A. The FortiMail access control rule to relay from Office 365 servers FQDN is missing
- B. The FortiMail DKIM key was not set using the Auto Generation option
- C. The FortiMail access control rules to relay from Office 365 servers public IPs are missing.
- D. A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN

**Suggested Answer:** CD

Community vote distribution

CD (100%)

 **Davidrichard** Highly Voted 4 months ago

**Selected Answer:** CD

<https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/1458/configuring-outbound-settings-in-fortimail>

<https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/963264/configuring-outbound-settings-in-office-365>

upvoted 5 times


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

**Selected Answer:** CD

Additionally to the other answers, I guess the IPs are more needed than the FQDN.

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

upvoted 2 times

 **pitz** 3 months ago

**Selected Answer:** CD

there is no option to add FQDN in sender filed in access control policy.

upvoted 2 times

 **ama6** 3 months, 3 weeks ago

A and D

A: The FortiMail access control rule to relay from Office 365 servers FQDN is missing.

If the access control rule to relay from Office 365 servers FQDN is missing, then FortiMail will not be able to send emails to Office 365. This is because the access control rule specifies which IP addresses or domains are allowed to relay emails through FortiMail.

B: A Mail Flow connector from the Exchange Admin Center has not been set properly to the FortiMail Cloud FQDN.

If the Mail Flow connector from the Exchange Admin Center is not set properly to the FortiMail Cloud FQDN, then Office 365 will not be able to send emails to FortiMail. This is because the Mail Flow connector specifies which SMTP server is used to send emails to external recipients


upvoted 1 times

 **pplsh** 3 months, 3 weeks ago

**Selected Answer:** CD

Correct, should be C and D

upvoted 2 times

 **pplsh** 4 months, 2 weeks ago

Answer seen to be AD as refer to <https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/963264/configuring-outbound-settings-in-office-365>

upvoted 2 times



Refer to the exhibit.

```

config vpn ipsec phase1-interface
  edit MyVPN1
    set remote-gw 1.2.3.4
    set interface {{WAN}}
    set peertype any
    set proposal aes256-sha256
    set psksecret Fortinet!!Fortinet
  next
end
config vpn ipsec phase2-interface
  edit MyVPN1
    set phase1name MyVPN1
    set proposal aes256-sha256
    set auto-negotiate enable
  next
end

```

FortiManager is configured with the Jinja Script under CLI Templates shown in the exhibit.

Which two statements correctly describe the expected behavior when running this template? (Choose two.)

- A. The Jinja template will automatically map the interface with "WAN" role on the managed FortiGate
- B. The template will work if you change the variable format to \$(WAN).
- C. The template will work if you change the variable format to {{ WAN }}.
- D. The administrator must first manually map the interface for each device with a meta field
- E. The template will fail because this configuration can only be applied with a CLI or TCL script.


**Suggested Answer:** CD

Community vote distribution

CD (69%)

DE (23%)

8%

 **Viewable8041** Highly Voted 1 year, 4 months ago

**Selected Answer:** CD

Has to be C and D.

A is not correct, as the mapping is only done by variables and meta fields, not by Interface roles

B is not a Jinja syntax

C could be but Jinja should also understand the variable without spaces, so this is my best guess

D is correct

E is wrong

upvoted 8 times

 **kinge2** Most Recent 3 months, 3 weeks ago

**Selected Answer:** DE

DE correct

upvoted 1 times

 **kinge2** 4 months ago

**Selected Answer:** DE

DE is the better answer

upvoted 1 times

  **node345** 10 months, 1 week ago

**Selected Answer: CD**

C and D are correct.

upvoted 1 times

  **ac89l** 11 months, 2 weeks ago



**Selected Answer: DE**

I will go with DE

This script cannot be used as jinja

<https://docs.fortinet.com/document/fortimanager/7.2.0/new-features/761880/jinja2-template-sample-scripts>



upvoted 1 times

  **ama6** 1 year, 3 months ago

still going with

D and E



upvoted 1 times

  **ama6** 1 year, 4 months ago

D and E are correct

D. The administrator must first manually map the interface for each device with a meta field. The Jinja template in the exhibit is expecting a meta field called WAN to be set on the managed FortiGate. This meta field will specify which interface on the FortiGate should be assigned the "WAN" role. If the meta field is not set, then the template will fail. E. The template will fail because this configuration can only be applied with a CLI or TCL script. The Jinja template in the exhibit is trying to configure the interface role on the managed FortiGate. This type of configuration can only be applied with a CLI or TCL script. The Jinja template will fail because it is not a valid CLI or TCL script.

upvoted 2 times

  **Davidrichard** 1 year, 4 months ago

**Selected Answer: AD**

A and D seems correct

<https://docs.fortinet.com/document/fortimanager/7.2.0/new-features/761880/jinja2-template-sample-scripts>

upvoted 1 times

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work.

What should you configure?

- A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.
- B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.
- C. Configure two DNS servers and use DNS servers recommended by the two internet providers.
- D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **jeabcpe** 2 months, 2 weeks ago

I don't see this question in my exam.

upvoted 1 times

🗨️ 👤 **Viewable8041** 10 months ago

**Selected Answer: D**

Seems to be correct

upvoted 4 times

Refer to the exhibits.

Exhibit A -

```

vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82-500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1 established 1/1 time 50/50/50 ms
IPsec SA: created 1/2 established 1/2 time 0/25/50 ms
id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
direction: initiator
status: established 82236-82236s ago = 50ms
proposal: aes256-sha256
child: no
PPK: no
message-id sent/rcv: 4/1
lifetime/rekey: 86400/3863
DPD sent/rcv: 00000000/00000000
peer-id: CN = fgtdc01.example.com

```

Exhibit B -

```

fgt01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 tun_id=10.73.255.82
tun_id6=:10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options[0218]=npu create_dev fragment
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
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-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0B replaywin=2048
seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=4da0c1a4 esp=aes key=32 6495048006963561c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
ah=sha256 key=32 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2cfffca1ald572
enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c83cf
ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1

```

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set interface "wan1"
    set net-device enable
    set mode-cfg enable
    set proposal aes256-sha256
    set add-route disable
    set auto-discovery-receiver enable
    set remote-gw 10.73.255.82
  next
end
```

A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C.

Referring to the exhibits, which configuration will restore VPN connectivity?

```
A. config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
      set ike-version 1
      set authmethod signature
      set certificate "BR01FGTLOCAL"
      set peer "vpn-hub02-1_peer"
    next
end
```

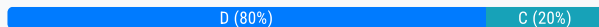
```
B. config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
      set ike-version 2
      set net-device enable
      set psksecret fortinet
    next
end
```

```
C. config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
      set ike-version 2
      set authmethod signature
      set npu-offload disable
      set certificate "BR01FGTLOCAL"
      set peer "vpn-hub02-1_peer"
    next
end
```

```
config vpn ipsec phase1-interface
  edit "vpn-hub02-1"
    set ike-version 2
    set authmethod signature
    set certificate "BR01FGTLOCAL"
    set peer "vpn-hub02-1_peer"
  next
end
```

**Suggested Answer:** D

Community vote distribution



**Noidea** Highly Voted 1 year, 5 months ago

NPU\_flag 03 both ingress and egress will be offloaded  
upvoted 6 times

**kinge2** Most Recent 4 months ago

**Selected Answer: D**

NPU off load does not restore connectivity, other than accelerating VPN, It only allow viewing of logs  
upvoted 1 times

**dspavvn** 7 months, 3 weeks ago

It is more likely to be B as the peer ID in exhibit A states CN = gftdc01.example.com with peer-id-auth: yes, so it requires this specific peer ID, and in A, C, D the peer ID is "vpn-hub02-1\_peer", which means the peer ID will be wrong.  
A cannot be because its IKEv1.  
C has disabled offloading, which does not affect the tunnel status but is not the same as the exhibit B, so cannot be correct based on that.  
D has everything correct, but using digital signature for auth, cannot verify this on any of the outputs and as the default auth-method is PSK, and they do not have a config backup, so no certificate to use if it was the case, makes D wrong too.  
B, based on the above, and the default for PSK setting for peer-id is accept all, is the only plausible option.  
upvoted 1 times

**node345** 10 months, 1 week ago

**Selected Answer: D**

npu\_flag=03. D is correct  
upvoted 1 times

**pitz** 1 year, 2 months ago

**Selected Answer: C**

The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101. To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below:

```
config vpn ipsec phase1-interface
edit "wan"
set peer-ip 192.168.1.101
set peer-id 192.168.1.101
set dhgrp 1
set auth-mode psk
set psk SECRET_PSK
next
end
```

Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel  
upvoted 1 times

🗨️ 👤 **ac89l** 11 months, 2 weeks ago  
my man, where do you see those addresses?  
upvoted 1 times

🗨️ 👤 **ama6** 1 year, 3 months ago  
Correct answer is C  
upvoted 1 times

🗨️ 👤 **pplée\_sh** 1 year, 3 months ago  
**Selected Answer: D**  
NPU\_Flag 03  
upvoted 3 times

🗨️ 👤 **Viewable8041** 1 year, 4 months ago  
**Selected Answer: D**  
As Noidea and pwatchpk  
upvoted 3 times

🗨️ 👤 **semsemccie** 1 year, 4 months ago  
**Selected Answer: C**  
Correct answer is C  
upvoted 1 times

🗨️ 👤 **pwatchpk** 1 year, 5 months ago  
D is correct  
upvoted 4 times

An HA topology is using the following configuration:

```

config system ha
  set group-id 240
  set group-name "200F"
  set mode a-p
  set hbdev "port3" 50 "port5" 100
  set hb-interval 3
  set hb-lost-threshold 2
  set hello-holddown 100
  set ha-uptime-diff-margin 300
  set override enable
  set priority 200
end

```


Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?


- A. 600ms
- B. 200ms
- C. 300ms
- D. 100ms

**Suggested Answer: A**


Community vote distribution

A (100%)


-  **Noidea** Highly Voted 1 year, 5 months ago

A: Default interval = 100ms. It can miss 2. So  $2 \times 300\text{ms} = 600\text{ms}$   
upvoted 6 times
-  **kinge2** Most Recent 4 months ago


Selected Answer: A

$100 \times 3 - 300 \times 2 = 600$   
upvoted 1 times
-  **node345** 10 months, 1 week ago


Selected Answer: A

hb-interval = 3 (3x100ms)  
hb-lost-threshold = 2  
 $2 \times 300\text{ms} = 600\text{ms}$ . A is correct  
upvoted 1 times
-  **pitz** 1 year, 2 months ago

Selected Answer: A

A is correct  
upvoted 2 times
-  **BozoPin** 1 year, 2 months ago

Selected Answer: A

Yes, he is...  
upvoted 1 times
-  **ama6** 1 year, 3 months ago



Sorry guys Noidea is correct the AW is A

upvoted 2 times

🗨️ 👤 **ama6** 1 year, 3 months ago

B is correct

in the exhibit HA heartbeat interval is 100ms and before a failover is detected is 2

$2 \times 100 = 200\text{ms}$

upvoted 1 times

🗨️ 👤 **Davidrichard** 1 year, 4 months ago

**Selected Answer: A**

<https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/489324/failover-protection>

upvoted 3 times

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

A is correct.

upvoted 2 times

Refer to the exhibit.



**Root FortiGate  
FGT\_1**



**Downstream FortiGate  
FGT\_2**



**Downstream FortiGate  
FGT\_3**

You have deployed a security fabric with three FortiGate devices as shown in the exhibit.

FGT\_2 has the following configuration:

```
config system csf
set fabric-object-unification local
end
```

FGT\_1 and FGT\_3 are configured with the default setting.

Which statement is true for the synchronization of fabric-objects?

- A. Objects from the FortiGate FGT\_2 will be synchronized to the upstream FortiGate
- B. Objects from the root FortiGate will only be synchronized to FGT\_2
- C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate
- D. Objects from the root FortiGate will only be synchronized to FGT\_3

**Suggested Answer: D**

Community vote distribution

D (88%)

13%

**Noidea** Highly Voted 11 months, 1 week ago

Local means objects will not be synchronized to and from this device (CLI Reference Guide).

So they will not be synced on FGT\_2. My guess is D is correct

upvoted 7 times

**dspavvn** Most Recent 1 month, 2 weeks ago

The root sends its global CMDB objects to FGTB-1, which has configuration-sync set to local, so FGTB-1 will not import objects sent by the root.

However, FGTB-1 will still forward these messages downstream to FGTC, which has configuration-sync set to default, so FGTC will receive and synchronize the objects sent from the root FortiGate (FGTA-1).

upvoted 1 times

**node345** 4 months, 1 week ago

**Selected Answer: D**

Exactly the same example. D is correct.

<https://docs.fortinet.com/document/fortigate/6.4.0/new-features/520820/improvements-to-synchronizing-objects-across-the-security-fabric-6-4-4>

upvoted 1 times

**ac89l** 5 months, 2 weeks ago

**Selected Answer: D**

<https://docs.fortinet.com/document/fortigate/6.4.0/new-features/520820/improvements-to-synchronizing-objects-across-the-security-fabric-6-4-4>

upvoted 2 times

**pitz** 9 months ago

**Selected Answer: C**

local: Global CMDB objects will not be synchronized to and from this device. Since FGT-3 is connected FGT-2 and root hence objects will not be synchronized to FGT-3 as well. So I am going with C.

upvoted 1 times

  **BozoPin** 9 months ago

**Selected Answer: D**

Noidea has the right idea...

upvoted 2 times

  **ama6** 9 months, 1 week ago

Still C

The fabric-object-unification setting on FGT\_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices.

Since FGT\_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be synchronized to FGT\_2.

upvoted 1 times

  **ama6** 9 months, 3 weeks ago

C is correct

<https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/880913/synchronizing-objects-across-the-security-fabric>

upvoted 1 times

  **Viewable8041** 10 months ago

**Selected Answer: D**

I am with Noidea

upvoted 2 times

Refer to the exhibit.

```
FGT_3 # show router ospf
config router ospf
  set router-id 10.10.10.3
  config area
    edit 0.0.0.0
    next
  end
  config ospf-interface
    edit "port2"
      set interface "port2"
      set network-type point-to-point
    next
  end
  config network
    edit 1
      set prefix 10.10.10.0 255.255.255.0
    next
  end
end
```

You are operation an internal network with multiple OSPF routers on the same LAN segment. FGT\_3 needs to be added to the OSPF network and has the configuration shown in the exhibit. FGT\_3 is not establishing any OSPF connection.

What needs to be changed to the configuration to make sure FGT\_3 will establish OSPF neighbors without affecting the DR/BDR election?

```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 255
      set network-type point-to-multipoint
    next
  end
end
```

A.

```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
B.      set network-type broadcast
    next
  end
end
```

```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 255
C.      set network-type broadcast
    next
  end
end
```

```
config router ospf
  config ospf-interface
    edit "port2"
      set priority 0
D.      set network-type point-to-multipoint
    next
  end
end
```

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ **Noidea** Highly Voted 1 year, 5 months ago

Correct: B

upvoted 5 times

🗳️ **ama6** Most Recent 1 year, 3 months ago

Correct: B

upvoted 1 times

🗳️ **Viewable8041** 1 year, 4 months ago

**Selected Answer: B**

A priority value of 0 means that the routing device never becomes the designated router. A value of 1 means that the routing device has the least chance of becoming a designated router.

upvoted 2 times

🗳️ **ac891** 11 months, 2 weeks ago

why not D

upvoted 2 times

  **DarkMmve** 2 months, 3 weeks ago

I'm going to say because a Ethernet lan segment is a broadcast type network. Ie, you can broadcast ARP request to find a MAC address associated to an IP

upvoted 1 times

A retail customer with a FortiADC HA cluster load balancing five webservers in L7 Full NAT mode is receiving reports of users not able to access their website during a sale event. But for clients that were able to connect, the website works fine. CPU usage on the FortiADC and the web servers is low, application and database servers are still able to handle more traffic, and the bandwidth utilization is under 30%.

Which two options can resolve this situation? (Choose two.)

- A. Change the persistence rule to LB\_PERSIS\_SSL\_SESS\_ID
- B. Add more web servers to the real server pool
- C. Disable SSL between the FortiADC and the web servers
- D. Add a connection-pool to the FortiADC virtual server

**Suggested Answer:** A

  **ama6** 3 months, 3 weeks ago

correct : A and D

upvoted 2 times

  **Noidea** 5 months ago

AD using ellimination.

upvoted 3 times

Refer to the CLI output:

```
FortiWeb Security Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-0.00177
FortiWeb Antivirus Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Regular Virus Database Version-42.00885
Extended Virus Database Version-42.00814
FortiWeb IP Reputation Service:
2022-01-03
Last Update Time: 2022-02-17 Method: Scheduled
Signature Build Number-3.00315
System files MD5SUM: 5660BD9FA1F6C86ESA31B2A139045F17
CLI files MD5SUM: 71BF206315679018536D9E19B37CBEAE
```

Given the information shown in the output, which two statements are correct? (Choose two.)

- A. Geographical IP policies are enabled and evaluated after local techniques
- B. Attackers can be blocked before they target the servers behind the FortiWeb
- C. The IP Reputation feature has been manually updated
- D. An IP address that was previously used by an attacker will always be blocked
- E. Reputation from blacklisted IP addresses from DHCP or PPPoE pools can be restored

**Suggested Answer:** BE

Community vote distribution

BE (100%)

 **jr01239a** 4 months, 1 week ago

B and E. <https://docs.fortinet.com/document/fortiweb/7.4.2/administration-guide/608374/ip-reputation-blocklisting-source-ips-with-poor-reputation>

Fortinet compiles a reputation for each public IP address. Clients will have poor reputations if they have been participating in attacks, willingly or otherwise. Because blacklisting innocent clients is equally undesirable, Fortinet also restores the reputations of clients that improve their behavior. This is crucial when an infected computer is cleaned, or in DHCP or PPPoE pools where an innocent client receives an IP address that was previously leased by an attacker.

upvoted 1 times

 **re\_john** 4 months, 2 weeks ago

B and D

upvoted 1 times

 **BozoPin** 9 months ago

**Selected Answer:** BE

Rest makes no sense

upvoted 2 times

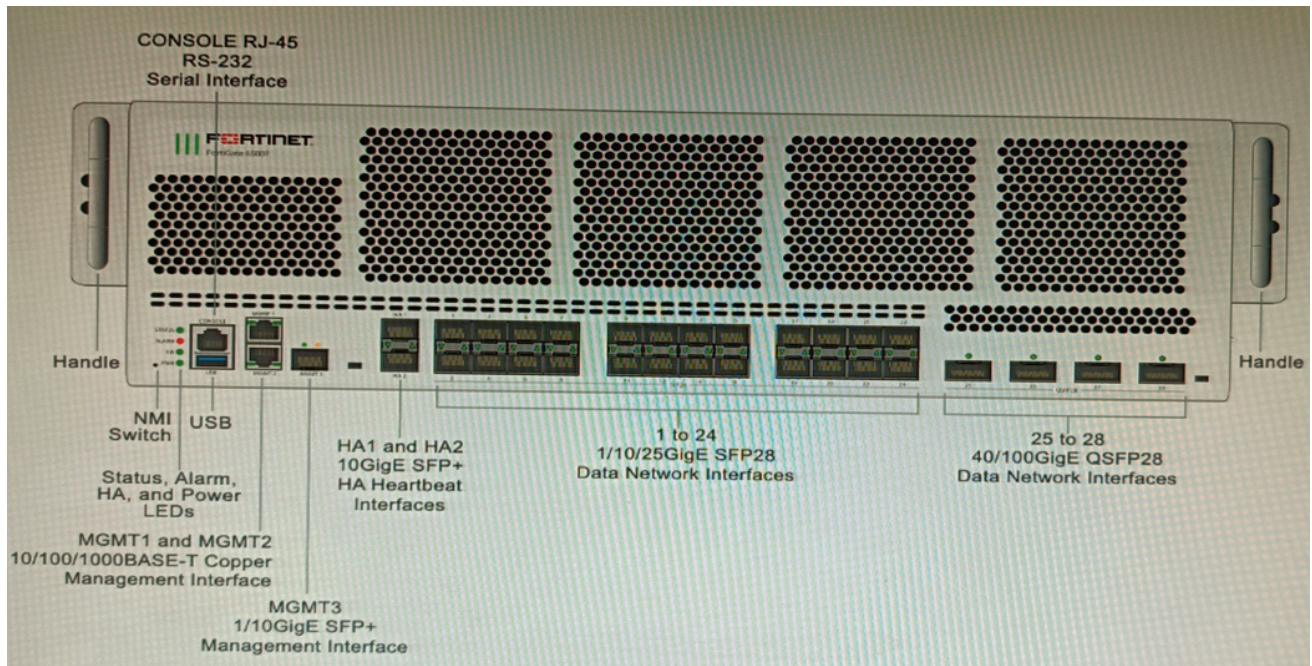
 **ama6** 9 months, 1 week ago

B and E



upvoted 2 times

Refer to the exhibit.



You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port.

You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.

How should the initial connection be made?

- A. Connect the switch on any interface between ports 21 to 24
- B. Connect the switch on any interface between ports 25 to 28
- C. Connect the switch on any interface between ports 1 to 4
- D. Connect the switch on any interface between ports 5 to 8

**Suggested Answer: B**

Community vote distribution

B (100%)

**Noidea** Highly Voted 1 year, 5 months ago

6000F has 6 interface groups:

1 to 4 - 5 to 8 - 9 to 12 - 13 to 16 - 17 to 20 - 21 to 24.

This means the only way to be sure the initial connection does not affect the rest is 25-28. B

upvoted 6 times

**kinge2** Most Recent 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

**node345** 10 months, 1 week ago

Selected Answer: B

The port25 to port28 interfaces are not part of an interface group. You can set the speed of each of these interfaces independently of the other three.

B is correct.

upvoted 1 times

**re\_j0hn** 1 year ago

B. <https://docs.fortinet.com/document/fortigate-6000/7.0.12/fortigate-6000-handbook/633498/interface-groups-and-changing-data-interface-speeds>

upvoted 1 times

  **Viewable8041** 1 year, 4 months ago

**Selected Answer: B**

see explanation from Noidea

upvoted 1 times

  **semsemccie** 1 year, 4 months ago

B is correct answer

upvoted 2 times

You are designing a setup where the FortiGate device is connected to two upstream ISPs using BGP. Part of the requirement is that you must be able to refresh the route advertisements manually without disconnecting the BGP neighborships. Which feature must you enable on the BGP neighbors to accomplish this goal?

- A. Graceful-restart
- B. Deterministic-med
- C. Synchronization
- D. Soft-reconfiguration

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ **FortigateEXP** 6 months ago

**Selected Answer: D**

The soft reconfigure is correct by elimination (FGTs all support BGP Refresh, so question is not worded correctly - to refresh routes in advertisements, there is no need to do manually anything, after the change is committed to config FGT will send BGP Refresh message to the peers to notify them of it. The same is true for Cisco and Juniper routers. The question should ask "when routing policy was changed" - then yes, reconfiguraiton is the way to notify BGP peers that BGP policy was changed.

Anyway:

Graceful restart - tells BGP neighbors to keep the routes advertised by peer even when peer GOES DOWN, i.e. it contradicts with the question condition that BGP session should not go down.

Synchronization - unrelated at all, refers to the ancient rule that routes advertised/learned via BGP HAVE to be first learned via IGP (like OSPF/IS-IS/etc) to prevent loops in iBGP topology. No one uses it anymore, everyone either disables synchronization or it is disabled (as in FGTs) by default.

Deterministic MED - is about route preference between EBGp peers, unrelated at all to the question.

upvoted 2 times

🗨️ **pitz** 9 months ago

**Selected Answer: D**

D Seems correct.

When the BGP routing policy is changed (such as by changing the attributes or adding filters), it is necessary to reset the BGP session before the new policy takes effect.

A soft reset is recommended to refresh the BGP routing table without disturbing existing BGP peering sessions.

To do this, first enable soft-reconfiguration:

```
# config router bgp
```

```
# config neighbor
```

```
edit 10.0.0.1
```

```
set soft-reconfiguration enable
```

```
end
```

end

Use the following command to perform a soft reset:

upvoted 1 times

🗨️ **ama6** 9 months, 3 weeks ago

sorry D is correct set soft-reconfiguration

upvoted 1 times

🗨️ **ama6** 9 months, 3 weeks ago

correct is A

upvoted 1 times

🗨️ **Davidrichard** 10 months ago

**Selected Answer: D**

D Seems correct

upvoted 2 times

🗨️ **Noidea** 11 months ago

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-BGP-soft-reset-to-refresh-BGP-routing-table/ta-p/190141>

upvoted 2 times

Refer to the exhibit, which shows a Branch1 configuration and routing table.

```
Branch1 # show system sdwan
config system sdwan
  set status enable
  set load-balance-mode source-dest-ip-based
config zone
  edit "internet"
  next
  edit "overlay"
  next
end
config members
  edit 1
    set interface "wan1"
    set zone "internet"
  next
  edit 2
    set interface "wan2"
    set zone "internet"
  next
  edit 3
    set interface "vpn1-net"
    set zone "overlay"
  next
  edit 4
    set interface "vpn2-mpls"
    set zone "overlay"
  next
end
  config service
  end
end

#####

Branch1 # get: router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type
2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default

Routing table for VRF=0
S*    0.0.0.0/0 [1/0] via 10.198.1.1, wan1, [1/0]
      [1/0] via 10.198.2.1, wan2, [1/0]
      [1/0] via vpn1-net tunnel 10.198.5.2, [1/0]
      [1/0] via vpn1-mpls tunnel 10.198.6.2, [1/0]
C     10.1.1.0/24 is directly connected, port3
...
```

In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available. In this scenario, which configuration change will meet this requirement?

- A. Change the load-balance-mode to source-ip-based.
- B. Create a new static route with the internet sdwan-zone only.
- C. Configure the cost in each overlay member to 10.
- D. Configure the priority in each overlay member to 10.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **JackieTYF** 2 months, 2 weeks ago

**Selected Answer:** D

D is correct, use higher value priority value so the route less preferred.

upvoted 1 times

🗨️ 👤 **re\_john** 10 months, 2 weeks ago

Answer is D. Priority preference is the lowest value is preferred for the routing table.

upvoted 1 times

🗨️ 👤 **Davidrichard** 1 year, 4 months ago

**Selected Answer:** D

<https://docs.fortinet.com/document/fortigate/6.4.0/sd-wan-deployment-for-mssps/775385/defining-interface-members>

upvoted 2 times

Refer to the exhibits.

GUI Access -

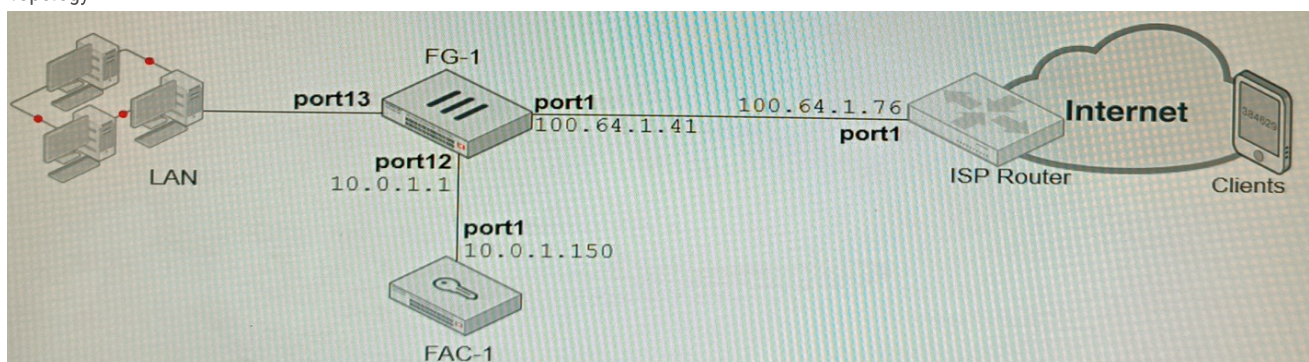
GUI Access	
Site title:	FortiAuthenticator
GUI idle timeout:	480 minutes (1-480 mins)
Maximum HTTP header length:	4 (4-16 KB)
HTTPS Certificate:	Default-Server-Certificate   CN=Default-Server-Certificate-7D895AD8
<input type="radio"/> HTTP Strict Transport Security (HSTS) Expiry	180 (0-730 days)
Certificate authority type:	Local CA <input type="radio"/> Trusted CA <input checked="" type="radio"/>
CA certificate that issued the server certificate:	Fortinet_CA1_Root   emailAddress=support@fortinet.com
<input checked="" type="radio"/> Allow all hosts/domain names	
Public IP/FQDN for FortiToken Mobile:	100.64.1.76

Configuration -

```
FG-1 # show system ftm-push
config system ftm-push
    set server-cert "self-sign"
    set server "10.0.1.150"
    set status enable
end
```

```
FG-1# show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set ip 100.64.1.41 255.255.255.0
        set allowaccess ping
        set type physical
        set alias "WAN"
        set role wan
        set snmp-index 1
    next
end
```

Topology -





An administrator has configured a FortiGate and FortiAuthenticator for two-factor authentication with FortiToken push notifications for their SSL VPN login. Upon initial review of the setup, the administrator has discovered that the customers can manually type in their two-factor code and authenticate but push notifications.

Based on the information given in the exhibits, what must be done to fix this?

- A. On FG-1 port1, the ftm access protocol must be enabled.
- B. FAC-1 must have an internet routable IP address for push notifications.
- C. On FG-1 CLI, the ftm-push server setting must point to 100.64.1.41.
- D. On FAC-1, the FortiToken public IP setting must point to 100.64.1.41.

**Suggested Answer: D**

Community vote distribution



**kinge2** 4 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

**re\_john** 1 year ago

A. <https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiToken-mobile-push-notification/ta-p/195578>

upvoted 1 times

**re\_john** 10 months, 2 weeks ago

Change my answer to D.

<https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on-FortiAuthenticator-operation/ta-p/190810>

upvoted 1 times

**FortigateEXP** 1 year ago

**Selected Answer: D**

This one is tricky because answers present configurations relevant to Fortitokens with Push notifications when FTKs are registered to the FORTIGATE itself, not the FAC. This relates to answers A and C - so if FTKs were configured on the FGT itself, then A and C would have to be fixed, and then question would ask for 2 answers, not one.

But here FTKs are created/registered on the FORTIAUTHENTICATOR and such set up works everywhere, even when the perimeter firewall before FAC is NOT Fortigate, but Checkpoint/Juniper/Cisco ASA. So A & C are excluded as not impacting tokens located on the FAC.

So the D is correct, because this configure IP should always be PUBLIC one that clients on the Internet can reach from their homes/hotels/etc. This is the IP FAC sends to the Forticlient telling him "Connect to this IP and port". Therefore it should be fixed to IP on the perimeter (here FGT) firewall.

upvoted 2 times

**BozoPin** 1 year, 2 months ago

**Selected Answer: A**

FTM allow access must be enabled, so A is correct

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiToken-mobile-push-notification/ta-p/195578>

Requirements for FTM push to work properly

"

1) The FTM service must be allowed on the FTM response receiving interface

```
# config system interface
```

```
edit <name>
```

```
set allowaccess ftm
```

```
next
```

```
end
```

```
"
```

Nethertheless C is correct, too ;) I am confused:

On same doc:

"

Note:

server-ip : The server IP address is the FortiGate's public IP or public IP address of device which is upstream and forwarding the push notification responses towards FortiGate. (This command is not supported from 6.4.10 onwards).

server : This can be public IP or Domain name(which resolved to FortiGate's Public IP).This option is not available on 6.4.9 and below

"



upvoted 2 times

  **pitz** 1 year, 2 months ago

**Selected Answer: B**

100.64.1.41 is private ip and hence token push will not work as all fortitoken send request to public ip only.

upvoted 1 times

  **ama6** 1 year, 3 months ago

B is correct

upvoted 2 times

  **Viewable8041** 1 year, 4 months ago



**Selected Answer: D**

<https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on-FortiAuthenticator-operation/ta-p/190810>

The 'Public IP/FQDN for FortiToken Mobile' needs to be set to a reachable ip for FortiToken APP access. Assuming there is NAT involved it needs to be changed to FG-1 port1 ip.

ISP Router port1 IP is definitely wrong in any case.

upvoted 2 times

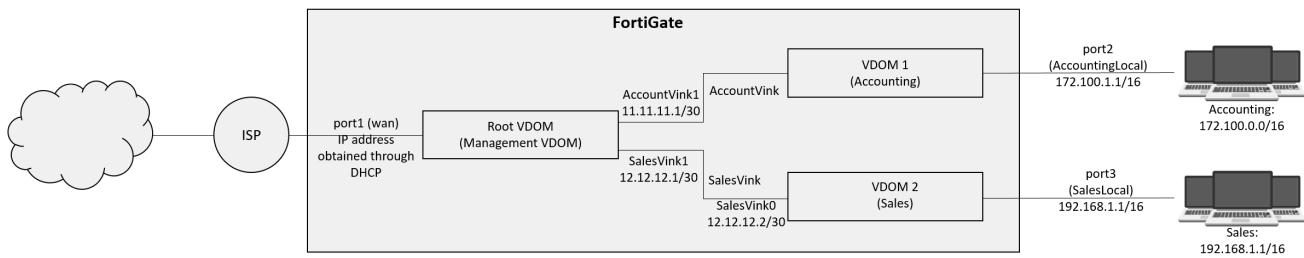
  **WBP43** 1 year, 4 months ago

<https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-FortiToken-Push-on-FortiAuthenticator-operation/ta-p/190810>

Correct answer is C

upvoted 1 times

Refer to the exhibit.



A customer has deployed a FortiGate 300E with virtual domains (VDOMs) enabled in the multi-VDOM mode. There are three VDOMs: Root is for management and internet access, while VDOM 1 and VDOM 2 are used for segregating internal traffic. AccountVlnk and SalesVlnk are standard VDOM links in Ethernet mode.

Given the exhibit, which two statements below about VDOM behavior are correct? (Choose two.)

- A. You can apply OSPF routing on the VDOM link in either PPP or Ethernet mode
- B. Traffic on AccountVlnk and SalesVlnk will not be accelerated
- C. The VDOM links are in Ethernet mode because they have IP addressed assigned on both sides
- D. Root VDOM is an Admin type VDOM, while VDOM 1 and VDOM 2 are Traffic type VDOMs
- E. OSPF routing can be configured between VDOM 1 and Root VDOM without any configuration changes to AccountVlnk

**Suggested Answer: A**

Community vote distribution

A (80%)

B (20%)

**kinge2** 4 months ago

**Selected Answer: B**

AB correct

upvoted 1 times

**fa82432** 6 months, 2 weeks ago

A and B seem right.

A - It does not matter and OSPF can be configured without any changes.

B - Offload is available NPU-VDOM link only.

upvoted 1 times

**BozoPin** 1 year, 2 months ago

**Selected Answer: A**

I guess its A and B:

B is quite obvious:

<https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/335646/inter-vdom-routing>:

"VDOM link does not support traffic offload. If you want to use traffic offload, use NPU-VDOM-LINK."

Type Ethernet is only needed for IPv6:

<https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/335646/inter-vdom-routing>

"For example, when running OSPF in IPv6, a link-local address is required in order to communicate with OSPF neighbors. For a VDOM link to obtain a link-local address its type must be set to ethernet"

C is wrong because you can set IPs on PPP. You do not need to.

D is wrong because Root VDOM is routing, so no Admin VDOM

E is wrong because I need a IP in AccountLink though this is in Ethernet Mode

So imho its A and B

upvoted 4 times

🗨️ **ama6** 1 year, 3 months ago

Guy if you read the question you will see that it says standard vdom link i think they would have mentioned something about accelerated so B is not correct

AccountVlnk and SalesVlnk are standard VDOM links in Ethernet mode.

upvoted 1 times

🗨️ **ITStudies** 1 year, 3 months ago

IP is missing in this picture only, the dump i have is having IP on it 11.11.11.2/30

And this dump is missing around 50 questions, i got failed with this dump. The one i have now is having more than 100 questions

upvoted 2 times

🗨️ **bastuman** 1 year, 3 months ago

Where did you get that dump?

upvoted 2 times

🗨️ **ama6** 1 year, 3 months ago

going for A and D

upvoted 1 times

🗨️ **Viewable8041** 1 year, 4 months ago

So for me A and B is correct. an

A because OSPF ipv4 can be run with PPP and Ethernet.

Not E because of the missing IP within VDOM 1 on the Vlnk

upvoted 1 times

🗨️ **Davidrichard** 1 year, 4 months ago

Should be two answers, B and E

<https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/335646/inter-vdom-routing>

<https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/335646/inter-vdom-routing-configuration-example-internet-access>

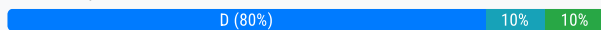
upvoted 2 times

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

- A. Native ESXi Networking with E1000
- B. Virtual Function (VF) PCI Passthrough
- C. Native ESXi Networking with VMXNET3
- D. Physical Function (PF) PCI Passthrough

**Suggested Answer: D**

Community vote distribution



**ac891** 5 months, 2 weeks ago

**Selected Answer: D**

PF provides the ability for PCI Passthrough, but requires an entire Network Interface Card (NIC) for a VM. It can usually achieve greater performance than a Virtual Function (VF) based SR-IOV. PF is also expensive. While VF allows one NIC to be shared among multiple guests VMs, PF is allocated to one port on a VM.

<https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/632344/pf-and-vf-sr-iov-driver-and-virtual-spu-support>  
upvoted 1 times

**cciesam** 6 months, 3 weeks ago

**Selected Answer: B**

VFs are actual PCIe hardware resources and only a limited number of VFs are available for each PF.

<https://docs.fortinet.com/document/fortigate-private-cloud/6.4.0/vmware-esxi-administration-guide/553137/sr-iov>  
upvoted 1 times

**pitz** 9 months ago

**Selected Answer: C**

agree with Ama6  
upvoted 1 times

**ama6** 9 months, 1 week ago

For performance considerations in a virtualized environment like ESXi, the recommended adapter type for NICs on a FortiGate VM would be:

C. Native ESXi Networking with VMXNET3

The VMXNET3 adapter type is optimized for performance and is well-suited for virtualized environments. It typically outperforms other adapter types like the E1000 or E1000e. VMXNET3 takes advantage of VMware's paravirtualization technology and offers features such as hardware offload and enhanced driver support, which can result in improved network performance and lower CPU utilization compared to other adapter types.

While Virtual Function (VF) and Physical Function (PF) PCI Passthrough are options that can provide direct hardware access for specific use cases, they are more complex to set up and may not be necessary unless you have very specific requirements that demand direct access to physical NICs. For general performance and ease of use in a virtualized environment, VMXNET3 is the recommended choice.  
upvoted 1 times

**ama6** 9 months, 2 weeks ago

GUY this should be  
C

VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without

requiring additional hardware or software components. References: <https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/installing-fortigate-vm-on-vmware-esxi> <https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation-for-vmware-esxi/19662/networking>

upvoted 1 times

🗨️ 👤 **pplée\_sh** 10 months ago

**Selected Answer: D**

Answer is D if cost is not a factor

upvoted 3 times

🗨️ 👤 **Viewable8041** 10 months ago

**Selected Answer: D**

<https://docs.fortinet.com/document/fortigate-private-cloud/6.4.0/vmware-esxi-administration-guide/553137/sr-iov>

upvoted 4 times

You are deploying a FortiExtender (FEX) on a FortiGate-60F. The FEX will be managed by the FortiGate. You anticipate high utilization. The requirement is to minimize the overhead on the device for WAN traffic.

Which action achieves the requirement in this scenario?

- A. Add a switch between the FortiGate and FEX.
- B. Enable CAPWAP connectivity between the FortiGate and the FortiExtender
- C. Change connectivity between the FortiGate and the FortiExtender to use VLAN Mode
- D. Add a VLAN under the FEX-WAN interface on the FortiGate

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Davidrichard** 4 months ago

**Selected Answer: C**

C is correct

<http://docs.fortinet.com/document/fortiextender/7.0.3/admin-guide-fgt-managed/394272/vlan-mode>

<http://docs.fortinet.com/document/fortiextender/7.0.3/admin-guide-fgt-managed/618684/vlan-mode-and-performance>  
upvoted 3 times

Refer to the exhibits.

Exhibit A -

FORTIAP 431F	
<b>Hardware</b>	
<b>Hardware Type</b>	Indoor AP
<b>Number of Radios</b>	3 + 1 BLE
<b>Number of Antennas</b>	5 Internal + 1 BLE Internal
<b>Antenna Type and Peak Gain</b>	PIFA: 4 dBi for 2.4 GHz, 5 dBi for 5 GHz
<b>Maximum Data Rate</b>	Radio 1: up to 1147 Mbps Radio 2: up to 2402 Mbps Radio 3: scan only
<b>Bluetooth Low Energy Radio</b>	Bluetooth scanning and iBeacon advertisement @ 6 dBm max TX power
<b>Interfaces</b>	1 x 100/1000/2500 Base-T RJ45, 1 x 10/100/1000 Base-T RJ45, 1x Type A USB, 1x RS-232 RJ45 Serial Port
<b>Power over Ethernet (PoE)</b>	<ul style="list-style-type: none"> <li>• 802.3at PoE default</li> <li>• 1 port powered by 802.3at or 2 ports powered by 802.3af - Full System functionality + USB support</li> <li>• 1 port is connected to 802.3af - No USB support, Operate in 2x2 mode with reduced power R1/R2 17dBm(Tx power)</li> </ul>
<b>Maximum Tx Power (Conducted)</b>	Radio 1: 2.4 GHz 24 dBm / 251 mW (4 chains combined)* Radio 2: 5 GHz 23 dBm / 200 mW (4 chains combined)* Radio 3: NA
<b>Environment</b>	
<b>Power Supply</b>	SP-FAP400-PA-XX or GPI-130
<b>Power Consumption (Max)</b>	24.5 W
<b>Directives</b>	Low Voltage Directive • RoHS
<b>UL2043 Plenum Material</b>	No
<b>Mean Time Between Failures</b>	>10 Years
<b>Surge Protection Built In</b>	Yes
<b>Hit-less PoE Failover</b>	Yes

Exhibit B -

	FORTISWITCH 224E-POE	FORTISWITCH 124E-FPOE	FORTISWITCH 248E-FPOE
<b>Hardware Specifications</b>			
<b>Total Network Interfaces</b>	24x GE RJ45 ports and 4x GE SFP ports	24x GE RJ45 and 4x GE SFP	48x GE RJ45 ports and 4x GE SFP ports
<b>Dedicated Management 10/100 Port</b>	1	0	1
<b>RJ-45 Serial Console Port</b>	1	1	1
<b>Form Factor</b>	1 RU Rack Mount	1 RU Rack Mount	1 RU Rack Mount
<b>Power over Ethernet (PoE) Ports</b>	12 (802.3af/802.3at)	24 (802.3af/at)	48 (802.3af/802.3at)
<b>PoE Power Budget</b>	180 W	370 W	740 W
<b>Mean Time Between Failures</b>	> 10 years	> 10 years	> 10 years
<b>Retail Price</b>	\$1,000	\$1,250	\$1,500

A customer wants to deploy 12 FortiAP 431F devices on high density conference center, but they do not currently have any PoE switches to connect them to. They want to be able to run them at full power while having network redundancy.

From the FortiSwitch models and sample retail prices shown in the exhibit, which build of materials would have the lowest cost, while fulfilling the customer's requirements?

- 1x FortiSwitch 248E-FPOE
- 2x FortiSwitch 224E-POE
- 2x FortiSwitch 248E-FPOE
- 2x FortiSwitch 124E-FPOE

**Suggested Answer: D**

Community vote distribution



D (100%)



**Selected Answer: D**

D is correct

upvoted 1 times

  **gabriel** 11 months, 1 week ago



B is correct, since you can power the FAP with 2x802.3af (15w) ports at full power. If you connect one port to each switch from each AP you get redundancy and full power with 180w for 12 ports with the cheaper 224E poe. The cost is in the input diagram and it says 224E poe is cheaper than 124F FPOE

upvoted 3 times

  **re\_john** 1 year ago

B. Split the APs to two FortiSwitch 224E-POE and this also provides network redundancy at cheaper cost.

upvoted 1 times

  **ama6** 1 year, 3 months ago

D is correct

the access point will require about 24.5 W of power and the 124E-FPOE has a Capacity of about 370 meaning  $25 \times 12 = 300$  so you left with about 70 W on the switch meaning you can still add two more access point on that switch.



upvoted 2 times

  **Davidrichard** 1 year, 4 months ago

**Selected Answer: D**

224E power budget is 180 W and requirement of 12 AP is around 250 watts

upvoted 3 times

  **pplée\_sh** 1 year, 4 months ago

**Selected Answer: D**

124E is cheaper compare to 224E

upvoted 3 times

Refer to the exhibits.

Exhibit A -

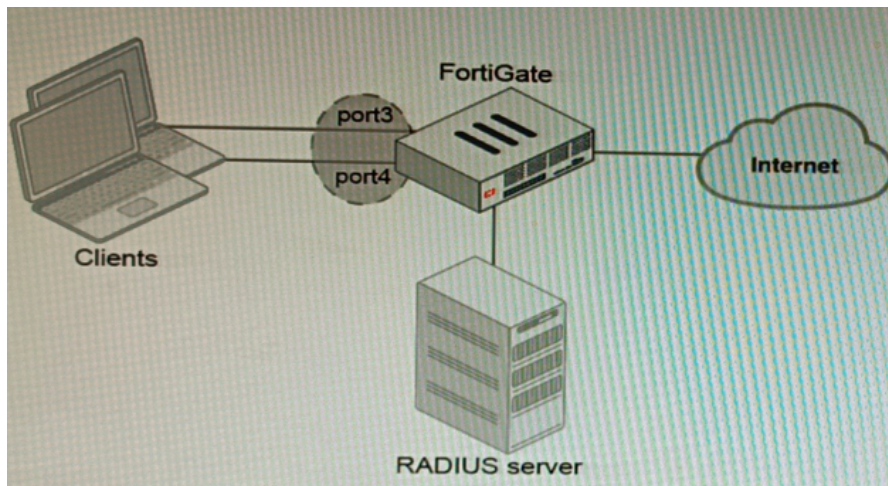


Exhibit B -

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
```

```
-----
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
-----
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E. Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)


- A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication
- B. Devices connected directly to ports 3 and 4 can perform 802.1X authentication
- C. Ports 3 and 4 can be part of different switch interfaces

D. Client devices must have 802.1X authentication enabled

**Suggested Answer:** *BD*

*Community vote distribution*




 **kinge2** 4 months ago

**Selected Answer:** *BD*

BD correct

upvoted 1 times

 **Davidrichard** 1 year, 4 months ago

B and D

<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/959502/support-802-1x-on-virtual-switch-for-certain-np6-platforms>

upvoted 3 times

You want to use the MTA adapter feature on FortiSandbox in an HA-Cluster.  
Which statement about this solution is true?

- A. The configuration of the MTA Adapter Local Interface is different than on port1
- B. The MTA adapter is only available in the primary node
- C. The MTA adapter mode is only detection mode
- D. The configuration is different than on a standalone device

**Suggested Answer:** B

*Community vote distribution*

B (100%)

🗨️ 👤 **ac891** 5 months, 2 weeks ago

**Selected Answer: B**

<https://docs.fortinet.com/document/fortisandbox/4.4.3/administration-guide/877925/mta-adapter>  
upvoted 2 times

🗨️ 👤 **pitz** 9 months ago

**Selected Answer: B**

Using MTA in HA-Cluster  
In HA-Cluster, the MTA adapter is only available in the primary node.  
upvoted 2 times

🗨️ 👤 **ama6** 9 months, 3 weeks ago

Correct is B  
upvoted 1 times

🗨️ 👤 **Davidrichard** 10 months ago

**Selected Answer: B**

<https://docs.fortinet.com/document/fortisandbox/4.2.4/administration-guide/877925/mta-adapter>  
upvoted 2 times

🗨️ 👤 **arielon** 11 months, 1 week ago

**Selected Answer: B**

Es B. In HA-Cluster, the MTA adapter is only available in the primary node.  
Configuration is the same as on a standalone device. When the primary node receives MTA jobs, depending on workload and VM association, it distributes the jobs to itself or worker nodes.  
upvoted 4 times

Refer to the exhibit showing the history logs from a FortiMail device.

History									
System Event Mail Event AntiVirus AntiSpam Encryption Log Search Task									
List View Search Export									
Records per page 100 Go to line									
#	Classifier	Disposition	From	Header From	To	Subject	Directi...	Policy ID	Domain
1	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	bob@companya.com	Order Confirmation #130282	in	0:1:1:companya.com	companya.com
2	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	alice@companya.com	Order Confirmation #130282	in	0:1:1:companya.com	companya.com
3	Not Spam	Accept	localhost@remotedomain	postmaster@acme.com	administrator@companya.com	Order Confirmation #130282	in	0:1:1:companya.com	companya.com

Which FortiMail email security feature can an administrator enable to treat these emails as spam?

- A. DKIM validation in a session profile
- B. Sender domain validation in a session profile
- C. Impersonation analysis in an antispam profile
- D. Soft fail SPF validation in an antispam profile

**Suggested Answer: C**

Community vote distribution

C (100%)

 **Davidrichard** 4 months ago

**Selected Answer: C**

<https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/221814/protecting-against-email-impersonation-in-fortimail>  
upvoted 4 times

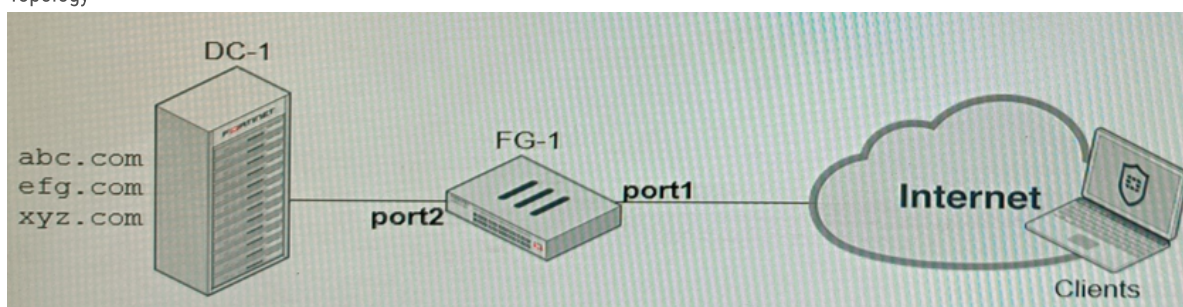
Refer to the exhibits, which show a firewall policy configuration and a network topology.

Configuration -

```
config firewall policy
  edit 1
    set name "DC-1-Traffic-In"
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "DC-1-VIP-GRP"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set ssl-ssh-profile "DC1-Certs"
    set av-profile "servers"
    set webfilter-profile "servers"
    set logtraffic all
  next
end

config firewall ssl-ssh-profile
  edit "DC1-Certs"
    config https
      set ports 443
      set status deep-inspection
    end
    ...omitted output...
    set server-cert-mode replace
    set server-cert "abc" "efg"
    set supported-alpn http2
  next
end
```

Topology -



An administrator has configured an inbound SSL inspection profile on a FortiGate device (FG-1) that is protecting a data center hosting multiple web pages.

Given the scenario shown in the exhibits, which certificate will FortiGate use to handle requests to xyz.com?

- A. FortiGate will fall-back to the default Fortinet\_CA\_SSL certificate
- B. FortiGate will reject the connection since no certificate is defined
- C. FortiGate will use the Fortinet\_CA\_Untrusted certificate for the untrusted connection
- D. FortiGate will use the first certificate in the server-cert list—the abc.com certificate

**Suggested Answer: D**

*Community vote distribution*

D (100%)

ama6 3 months, 1 week ago

D is correct

upvoted 2 times

Davidrichard 3 months, 3 weeks ago

**Selected Answer: D**

D is correct

upvoted 4 times

Viewable8041 4 months ago

**Selected Answer: D**

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/850344/define-multiple-certificates-in-an-ssl-profile-in-replace-mode>

If there is no matched server certificate in the list, then the first server certificate in the list is used as a replacement.

upvoted 4 times

Refer to the exhibits.

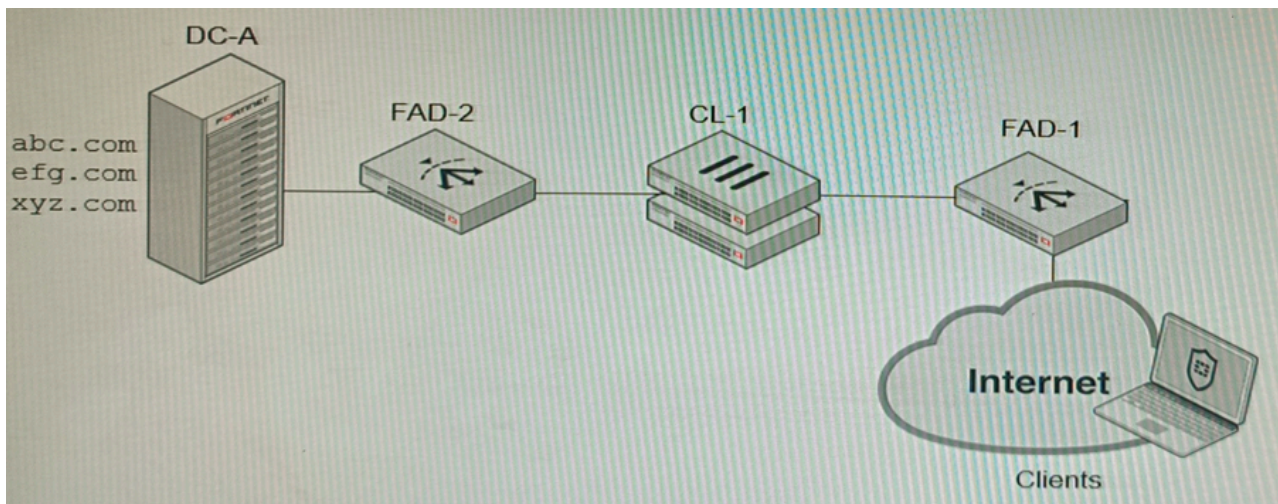
Configuration -

```
config firewall profile-protocol-options
  edit "SSL-Offload"
    set comment "For FAD decrypted traffic"
    config http
      set ports 80
      unset options
      unset post-lang
    end
    config ftp
      set ports 21
      set options splice
    end
    config imap
      set ports 143
      set options fragmail
    end
    ...output omitted...
  next
end

config application list
  edit SSL-Of f load-App-Detect11
    set comment "App detect in decrypted traffic"
    config entries
      edit 1
        set action pass
      next
    end
  next
end
```

Topology -





A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1, perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

```

config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end

```

A.

```

config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set options splice
        end
    next
end

```

B.

```

config firewall ssl-server
    edit FAD-1
        set ip <FAD-1 IP address>
        set ssl-mode full
    next
end

```

C.

D.

```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
end
```

E.

**Suggested Answer:** AD

Community vote distribution

AD (100%)

🗳️ 👤 **JJISHE** 3 months, 3 weeks ago

**Selected Answer:** AD

A - (<https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/162551/handling-ssl-offloaded-traffic-from-an-external-decryption-device>)

D - (<https://community.fortinet.com/t5/FortiGate/Technical-Tip-SSL-based-application-detection-over-decrypted/ta-p/196027>)  
upvoted 2 times

🗳️ 👤 **pitz** 9 months ago

**Selected Answer:** AD

A and D, There is no option of https in cli. only http.  
upvoted 2 times

🗳️ 👤 **ama6** 9 months, 1 week ago

correct is B and D

To enable application detection on plain-text traffic that has been decrypted by FortiADC, the administrator must perform two configuration tasks on CL-1:

Enable SSL offloading in the firewall policy and select the SSL-Offload protocol options profile.

Enable application control in the firewall policy and select the SSL-Offload-App-Detect application list.

upvoted 1 times

🗳️ 👤 **Viewable8041** 10 months ago

**Selected Answer:** AD

ssl-offloaded yes

SSL decryption and encryption performed by an external device.

force-inclusion-ssl-di-sigs enable

Enable forced inclusion of signatures which normally require SSL deep inspection.

upvoted 3 times

🗳️ 👤 **semsemccie** 10 months, 1 week ago

Answer is A and D

upvoted 3 times

You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network. After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.

Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

- A. No change in design is needed as even small FortiGate devices have a large memory capacity
- B. Acquire a FortiGate model with more capacity, considering the next 5 years growth
- C. Implement network-id, neighbor-group and increase the advertisement-interval
- D. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

**Suggested Answer:** D

Community vote distribution

D (67%)

C (33%)

🗨️ 👤 **kinge2** 3 months, 3 weeks ago

Selected Answer: C

Neighbor group and route reflectors is the answer to reduce BGP sessions  
upvoted 1 times

🗨️ 👤 **WBP43** 1 year, 3 months ago

Selected Answer: C

Route reflector is the only option to decrease BGP sessions number.  
upvoted 1 times

🗨️ 👤 **Viewable8041** 1 year, 4 months ago

Selected Answer: D

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/810981/sd-wan-segmentation-over-a-single-overlay>  
upvoted 4 times

You must analyze an event that happened at 20:37 UTC.

```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" logid="0000000022"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91.12 srcport=51542
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1" fstintfrole="wan"
srcuuid="2b4ee3fc-0124-51ed-7898-eae1b990blec" dstuuid="2b4ee3fc-0124-51ed-7898-eae1b990blec"
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=17 action="accept"
policyid=13 policytype="policy" poluuid="766bb040-0124-51ed-ca3a-eacce4ed289f" policyname="LAN to
Internet" service="DNS" trandisp="snat" transip=10.100.64.101 transport=51542 appid16195 app="DNS"
appcat="Network.Service" apprisk="elevated" applist="default" duration=180 setbyte=45 rcvbyte=120
sentpkt=1 rcvdpkt=1 srchwvndor="Fortinet" devtype="Router" srcfamily="FortyGate" osname="FortyOS"
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

One log relevant to the event is extracted from FortiGate logs:

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled.

The FortiGate is at GMT-10:00 -

The FortiAnalyzer is at GMT-08:00

Your browser local time zone is at GMT-03:00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

- A. 20:37:08
- B. 10:37:08
- C. 17:37:08
- D. 12:37:08

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **JackieTYF** 2 months, 2 weeks ago

**Selected Answer: D**

D is correct follow FAZ local time.

upvoted 1 times

🗳️ 👤 **dspavvn** 7 months, 1 week ago

**Selected Answer: D**

- GUI 'Date/time' column is calculated based on itime.

- itime is generated by FAZ when it receives a log (with SQL enabled) i.e. FAZ local time.

So the filter will be based on itime which is the local time on the FAZ (GMT-8) so UTC 20:37 makes the time GMT 20:37, so that minus 8 makes it 12:37.

upvoted 2 times

🗳️ 👤 **JJISHE** 9 months, 3 weeks ago

**Selected Answer: D**

I suppose D. The question says that something happened at 20:37, but u have extracted a related log from fortigate (time 10:37:08). FGT is GMT-10 and FAZ is GMT-8 (so +2). When a FAZ receive a log it register the hour of the device as dtime and maintain itime as the time it received the log. FAZ use itime as a reference for Time in GUI (<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-Understanding-FortiAnalyzer-time-related-fields/ta-p/197569>)

So if u want to search the related log u must use 12:37:08.

This IMPO

upvoted 2 times

🗳️ 👤 **ac89l** 11 months, 2 weeks ago

Can anyone please confirm this answer?

I could not find any related document on this ..


upvoted 1 times

🗳️ 👤 **ac89l** 11 months, 2 weeks ago

i would go for D. but not sure

i think FAZ will display the log as its local time, and not as the FGT time.



upvoted 1 times

  **re\_john** 11 months ago

Uses the FAZ time which is UTC-8.

Answer is D. 12:37:08.

upvoted 2 times

  **ama6** 1 year, 3 months ago

C: C. 17:37:08

upvoted 1 times

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems on Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main data center. They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy, and performance as a priority. Which two design options are true based on these requirements? (Choose two.)

- A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.
- B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.
- C. Branch FortiGate devices must be configured as VPN clients for the branches' internal network to be able to access Oracle services without using public IPs.
- D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge.

**Suggested Answer:** BC

Community vote distribution

BC (100%)

🗨️ **JackieTYF** 2 months, 2 weeks ago

**Selected Answer: BC**

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-encryption>  
upvoted 1 times

🗨️ **Pat1361** 5 months, 3 weeks ago

Azure does not encrypt by default so B is correct.  
upvoted 1 times

🗨️ **node345** 9 months, 3 weeks ago

**Selected Answer: BC**

ExpressRoute supports a couple of encryption technologies to ensure confidentiality and integrity of the data traversing between your network and Microsoft's network. By default traffic over an ExpressRoute connection isn't encrypted.  
upvoted 2 times

🗨️ **ama6** 1 year, 3 months ago

B is wrong Whenever Azure customer traffic moves between datacenters, Microsoft applies a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (MACsec). This encryption is implemented to secure the traffic outside physical boundaries  
upvoted 2 times

🗨️ **ama6** 1 year, 3 months ago

A and C  
Whenever Azure customer traffic moves between datacenters, Microsoft applies a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (MACsec). This encryption is implemented to secure the traffic outside physical boundaries  
upvoted 2 times

🗨️ **Viewable8041** 1 year, 4 months ago

**Selected Answer: BC**

Azure Expressroute is not encrypted.  
upvoted 2 times

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).

GUI Access -

High Availability Settings

Enable HA

Role:

Cluster member

Standalone Primary

Load Balancer

Password:

Load Balancers:

Name	IP Address	Delete
+ Add Secondary Load Balancer		

OK Cancel

Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

- A. FAC2 can only process requests when FAC1 fails.
- B. FAC2 can have its HA interface on a different network than FAC1
- C. The FortiToken license will need to be installed on the FAC2
- D. FSSO sessions from FAC1 will be synchronized to FAC2

**Suggested Answer: B**

Community vote distribution

B (86%)

14%

**re\_john** 4 months, 3 weeks ago

**Selected Answer: B**

Answer is B.

A is wrong because the setup is not Active/Passive HA.

C is wrong because FortiToken is synced.

D is wrong because FSSO session is not synced.

upvoted 2 times

**pitz** 9 months ago

**Selected Answer: B**

Other features, such as FSSO cannot be synchronized between devices.

<https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/122076/high-availability>

upvoted 2 times

**ama6** 9 months, 3 weeks ago

B is correct

FortiAuthenticator VMs used in a HA cluster each require a license. Each license is tied to a specific IP address. In an HA cluster, all interface IP addresses are the same on the units, except for the HA interface.

Request each license backed on either the unique IP address of the unit's HA interface or the IP address of a non-HA interface which is the same on both units.

<https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/122076/high-availability#Standalone>

upvoted 1 times

**Viewable8041** 10 months ago

**Selected Answer: B**

As semsemccie described:

configured as active-active (Standalone Primary for FAC1) so interfaces can be in different network

B is correct



upvoted 2 times

  **semsemccie** 10 months, 1 week ago

configured as active-active so interfaces can be in different network

B is correct



upvoted 2 times

  **pplée\_sh** 10 months, 2 weeks ago

**Selected Answer: D**

B is wrong, Select a network interface to use for communication between the cluster members. This interface must not already have a IP address assigned and it cannot be used for authentication services. Both units must use the same interface for HA communication.

upvoted 1 times

  **PaloPalacios** 9 months, 4 weeks ago

D is wrong - Other features, such as FSSO cannot be synchronized between devices.

<https://docs.fortinet.com/document/fortiauthenticator/6.5.3/administration-guide/122076/high-availability>

upvoted 1 times



Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

- A. The FortiGuard VOS can be used only with proxy-base policy inspections.
- B. If third-party AV database returns a match the scanned file is deemed to be malicious.
- C. The antivirus database queries FortiGuard with the hash of a scanned file
- D. The AV engine scan must be enabled to use the FortiGuard VOS feature
- E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database

**Suggested Answer:** CE

Community vote distribution

CE (80%)

CD (20%)

🗨️ 👤 **Pat1361** 5 months, 2 weeks ago

**Selected Answer: CD**

quoting from docs.Fortinet "The hash signatures are obtained from external sources such as VirusTotal, Symantec, Kaspersky, and other third-party websites and services." so E is incorrect.

C 100% correct

E is correct because you enable VoS under the antivirus profile so AV engine must be enabled.

upvoted 1 times

🗨️ 👤 **ac89I** 11 months, 2 weeks ago

**Selected Answer: CE**

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/889364/fortiguard-outbreak-prevention>

-Enabling the AV engine scan is not required to use this feature.

-The hash signatures are obtained from FortiGuard's Global Threat Intelligence database

upvoted 2 times

🗨️ 👤 **ac89I** 11 months, 2 weeks ago

A wrong: FortiGuard VOS can be used in both proxy-based and flow-based policy inspections across all supported protocols.

B is suspicious and tricky: As If FortiGuard returns a match, the scanned file is deemed to be malicious, not if the "third-party AV database" returns a match, while on the other hand, the third-party malware hash signatures curated by FortiGuard.

C 100% correct: The antivirus database queries FortiGuard with the hash of a scanned file

D wrong: Enabling the AV engine scan is not required to use this feature.

E 100% correct: The hash signatures are obtained from FortiGuard's Global Threat Intelligence database

And all according to this:

<https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/889364/fortiguard-outbreak-prevention>

upvoted 3 times

🗨️ 👤 **Golux** 1 year ago

CD

The hashes are obtained from third party database

upvoted 2 times

🗨️ 👤 **Viewable8041** 1 year, 4 months ago

**Selected Answer: CE**

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/889364/fortiguard-outbreak-prevention>

First paragraph

upvoted 2 times

A remote worker requests access to an SSH server inside the network. You deployed a ZTNA Rule to their FortiClient. You need to follow the security requirements to inspect this traffic.

Which two statements are true regarding the requirements? (Choose two.)

- A. FortiGate can perform SSH access proxy host-key validation.
- B. You need to configure a FortiClient SSL-VPN tunnel to inspect the SSH traffic.
- C. SSH traffic is tunneled between the client and the access proxy over HTTPS.
- D. Traffic is discarded as ZTNA does not support SSH connection rules.

**Suggested Answer:** AC

Community vote distribution

AC (100%)

🗨️ **node345** 4 months ago

**Selected Answer:** AC

C is tricky but still correct because it says "tunneled" and not encrypted. The SSH traffic is tunneled over TCP443, but not encrypted.  
upvoted 1 times

🗨️ **Viewable8041** 10 months ago

**Selected Answer:** AC

Correct

<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/29927/ztna-ssh-access-proxy-example>

upvoted 1 times

🗨️ **ac891** 5 months, 2 weeks ago

Are you sure about C

because in the same link it says:

When Encryption is disabled, the connection between the client and FortiGate access proxy is not encapsulated in HTTPS after the client and FortiGate connection is established. This allows for less overhead, because SSH is already a secure connection.

Does this eliminate C ?

upvoted 1 times