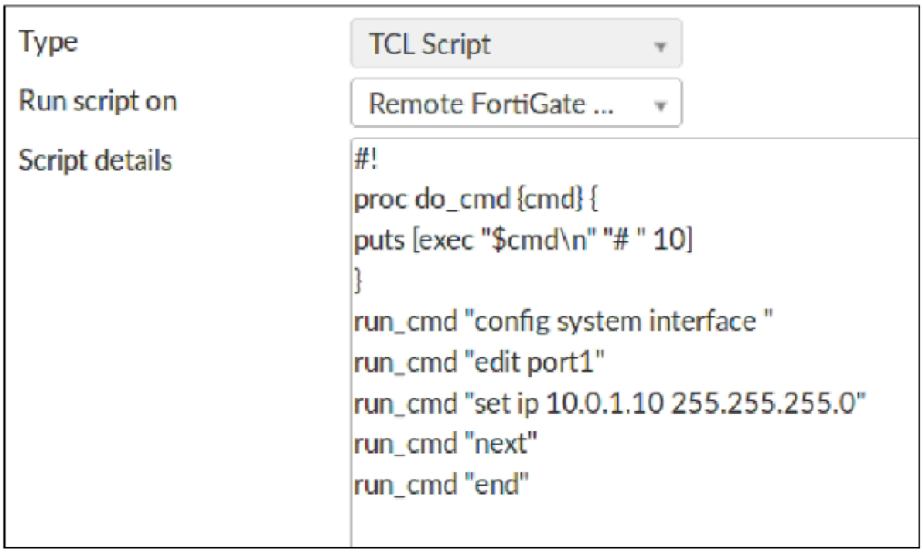
Question #1 Topic 1

Refer to the exhibit, which contains a TCL script configuration on FortiManager.



Type: TCL Script

Run script on: Remote FortiGate ...

Script details:

```
#!
proc do_cmd {cmd} {
puts [exec "$cmd\n" "# " 10]
}
run_cmd "config system interface "
run_cmd "edit port1"
run_cmd "set ip 10.0.1.10 255.255.255.0"
run_cmd "next"
run_cmd "end"
```

An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.

Why did the TCL script fail to make any changes to the managed device?

A. The TCL procedure run_cmd has not been created.

B. The TCL script must start with #include.

C. There is no corresponding #! to signify the end of the script.

D. The TCL procedure lacks the required loop statements to iterate through the changes.

Suggested Answer: *A*

Community vote distribution

A (100%)

ae0c0ec 1 month, 1 week ago

Selected Answer: A

Exam questions no longer valid. The answers from exam has been changed. Are not the same as this guide. Some questions are the same but the answers not.

upvoted 1 times

aamrcl 4 days, 23 hours ago

Ahora estan en la Version 7.4

upvoted 1 times

Palfriend 2 months, 3 weeks ago

Selected Answer: A

Not sure how to add more question here, from the exam:

Q13) you configured an address object on the root fortigate in a security fabric, the object is not synchronized with a downstream fortigate
Which two reasons could be the cause?
a) The downstream Fortigate has fabric object-unification set to local
b) The address object on the root fortigate has fabric-object set to disable
c) The root fortigate has configuration-sync set to enable
d) The downstream fortigate has configuration-sync set to local.

i believe b and D, reference : https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/880913/synchronizing-objects-across-the-security-fabric

upvoted 1 times

Palfriend 3 months ago

Selected Answer: A

Hi, anyone did the exam recently? still valid?

upvoted 2 times

Kevin_Howard 2 months, 2 weeks ago

This dump is not valid for the current test. I just took it and only like 30% of the questions are from this exam topic.

upvoted 1 times

neciwid141 4 months ago

Selected Answer: A

There was added new questions (ospf etc.) recently - last week 76q. Can someone confirm if this dump is stable now and usable for exam?

upvoted 3 times

usajn1 3 months, 4 weeks ago

yes I can confirm this questions be on my exam

upvoted 1 times

usajn1 4 months, 1 week ago

Selected Answer: A

also have new question maybe 10 be similar

upvoted 1 times

piotto777 4 months, 2 weeks ago

Selected Answer: A

90% of questions are new, reported this to admins, no update.

upvoted 2 times

Timoty15 5 months, 3 weeks ago

Selected Answer: A

Has anyone taken a dump from here in the past few days and succeeded in the exam? How many questions are new?

upvoted 2 times

jowogey808 4 months, 3 weeks ago

1 or 2 questions you can get on the real exam, most of the questions 95% are new

upvoted 4 times

boars 7 months ago

A is correct

upvoted 2 times

charruco 9 months ago

Selected Answer: A

A is correct

Study Guide 7.2 - Page 145

upvoted 2 times

truserud 9 months, 3 weeks ago

Selected Answer: A

A is correct. If you wanted the TCL script to run, you would have to change proc do_cmd to proc run_cmd, or change the procedure name to "do_cmd" from the pictured "run_cmd" in the screenshot.

More information with examples is found on page 145 in the Study Guide.

upvoted 3 times

LNR360 10 months, 1 week ago

A is correct

upvoted 2 times

rananaj 10 months, 1 week ago

Selected Answer: A

The answer is A

upvoted 4 times

Question #2 *Topic 1*

You want to improve reliability over a lossy IPSec tunnel.
Which combination of IPSec phase 1 parameters should you configure?

A. fec-ingress and fsc-egrsss

B. dpd and dpd-retryinterval

C. fragmentation and fragmentation-mtu

D. keepalive and keylive

Suggested Answer: *B*

Community vote distribution

A (100%)

myrmidon3 5 months, 2 weeks ago

Selected Answer: A

Forward Error Correction (FEC) is a method that improves reliability over lossy networks, including IPSec tunnels.
Configuring fec-ingress and fec-egress parameters ensures that data packets are error-checked and corrected at both the ingress and egress of the IPSec tunnel, reducing the impact of packet loss and improving overall reliability.

upvoted 1 times

rac_sp 1 year ago

Selected Answer: A

a is correct. The study guide mention flossy links

upvoted 2 times

ciscofgt 1 year, 2 months ago

hey guys, has anyone taken the EFW 7.2 exam recently and were all questions from this site? the ones under EWF_7.2?

upvoted 2 times

> **d567468** 7 months, 3 weeks ago
>
> Just failed. Many questions not covered here.Specially OSPF questions
>
> upvoted 4 times

charruco 1 year, 2 months ago

Selected Answer: A

A is correct
Study Guide 7.2 - Page 317

upvoted 2 times

Totoahren 1 year, 3 months ago

Selected Answer: A

Study Guide on page 317.

upvoted 4 times

Totoahren 1 year, 3 months ago

A is correct option.
Reference:
https://community.fortinet.com/t5/FortiClient/Technical-Tip-Configuring-DPD-dead-peer-detection-on-IPsec-VPN/ta-p/192616

upvoted 2 times

truserud 1 year, 3 months ago

Selected Answer: A

A is the correct option. This is briefly explained in the Study Guide on page 317.
More detailed information can be found here: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Forward-Error-Correction-for-IPsec-VPN/ta-p/191567

upvoted 3 times

Kop01 1 year, 3 months ago

Selected Answer: A

Correct option "A" p317

upvoted 4 times

5deee77 1 year, 4 months ago

Selected Answer: A

Correct option is "A"

upvoted 4 times

tachy_22 1 year, 4 months ago

The answer A is correct - Enterprise_Firewall_7.2_Study_Guide - page - 317 - "it improves reliability that can overcome adverse WAN conditions such as lossy or noisy links"

upvoted 2 times

WSCOSTA 1 year, 4 months ago

Correct option is "C"

upvoted 1 times

azeemakhtar82 1 year, 4 months ago

Correct option is "A"

upvoted 1 times

rananaj 1 year, 4 months ago

Selected Answer: A

The answer is A

upvoted 3 times

Question #3 *Topic 1*

How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

A. When run on the Device Database, changes are applied directly to the managed FortiGate device.

B. When run on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

C. When run on the All FortiGate in ADOM, changes are automatically installed without the creation of a new revision history.

D. When run on the Policy Package, ADOM database, you must use the installation wizard to apply the changes to the managed FortiGate device.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

charruco 9 months ago

Selected Answer: BD

B and D are correct

Study Guide 7.2 - Page 140 141

upvoted 3 times

FlavioBarbosa 9 months, 2 weeks ago

B e D, estão corretas, Study Guide Pag. 140, 141

upvoted 2 times

truserud 9 months, 3 weeks ago

Selected Answer: BD

B & D are correct. This is explained on page 141 in the Study Guide.

upvoted 3 times

Artbrut 10 months ago

Selected Answer: BD

B and D are correct as stated p. 141 in the study guide

upvoted 3 times

5deee77 10 months ago

Selected Answer: BD

The answer is BD page 141

upvoted 2 times

rananaj 10 months, 1 week ago

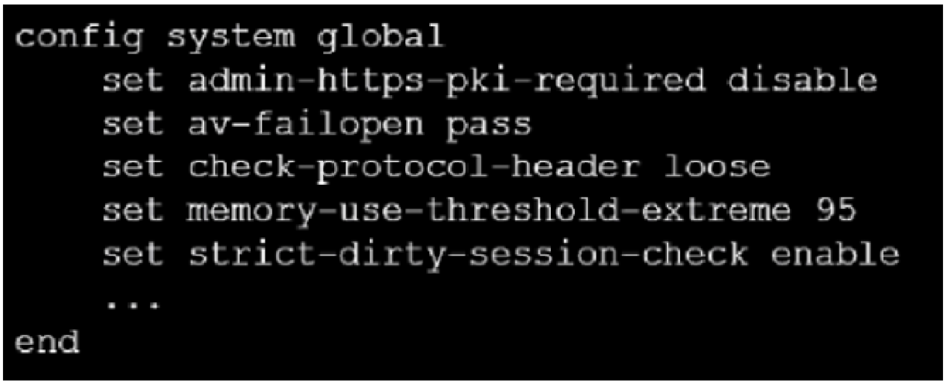
Selected Answer: BD

The answer is BD

upvoted 2 times

Question #4 *Topic 1*

Refer to the exhibit, which contains a partial configuration of the global system.



```
config system global
    set admin-https-pki-required disable
    set av-failopen pass
    set check-protocol-header loose
    set memory-use-threshold-extreme 95
    set strict-dirty-session-check enable
    ...
end
```

What can you conclude from this output?

A. Only NPs are disabled

B. Only CPs are disabled

C. NPs and CPs are enabled

D. NPs and CPs are disabled

Suggested Answer: *D*

Community vote distribution

C (95%) 5%

khalmrj Highly Voted 10 months, 3 weeks ago

anyone recently wrote the exam share experience if this is still valid?

upvoted 5 times

Welisson2 Most Recent 4 weeks, 1 day ago

Selected Answer: C

Study guide page 300

check-protocol-header strict = NPs and CPs disable

check-protocol-header loose = default = NPs and CPs enable

upvoted 1 times

bix88 3 months, 1 week ago

Selected Answer: C

This is the updated question:

A. Set strict-dirty-session-check enable command instructs the FortiGate to load all dirty session traffic to its SPU

B. set check-protocol-header loose command enables hardware acceleration on this FortiGate device

C. set av-fail open pass command instructs the FortiGate to load all traffic that uses the antivirus proxy to NP

D. Set memory-use-threshold-extreme, command instructs the FortiGate to disable hardware acceleration, if the memory extreme threshold reaches 95%.

upvoted 1 times

myrmidon3 5 months, 2 weeks ago

Selected Answer: C

the output does not explicitly reference any commands or parameters related to enabling or disabling Network Processors (NPs) or Content Processors (CPs). However, let's analyze the available settings for a conclusion:

set av-failopen pass

This indicates that antivirus scanning will allow traffic to pass even if the antivirus engine encounters an error. It does not directly affect the status of NPs or CPs.

set check-protocol-header loose

This loosens the protocol header checks for traffic. Again, this does not directly indicate the status of NPs or CPs.

set memory-use-threshold-extreme 95
This sets the memory utilization threshold at which extreme measures may be taken, but it does not indicate anything about NPs or CPs.

set strict-dirty-session-check enable
This ensures stricter checks on session consistency, but it does not influence the NP or CP settings.

Conclusion:

The configuration does not explicitly disable NPs or CPs. Therefore, the correct conclusion is:

C. NPs and CPs are enabled

upvoted 3 times

sugar12 10 months, 3 weeks ago

Selected Answer: C

Strick - disabled all NPs and CPs
loose - Enables them

Therefore C is correct

upvoted 2 times

havokdu 1 year, 1 month ago

Selected Answer: C

C is the correct answer.
check-protocol-header strict diables all NPPs and CPs. Loose doesn't disable them.

upvoted 2 times

ba68ea0 1 year, 2 months ago

Selected Answer: C

charruco is correct - scrub my comment !

upvoted 3 times

charruco 1 year, 2 months ago

Selected Answer: C

the question says: "loose"
set check-protocol-header "loose"

Enabling "strict" header checking disables all hardware acceleration (not loose config). This includes NP, SP, and CP processing.
so C is correct

upvoted 3 times

ba68ea0 1 year, 3 months ago

Answer: D "Enabling strict header checking disables all hardware acceleration. This includes NP, SP, and CP processing."
https://docs.fortinet.com/document/fortigate/7.4.3/hardware-acceleration/39956/strict-protocol-header-checking-disables-hardware-acceleration

upvoted 2 times

Totoahren 1 year, 3 months ago

Selected Answer: C

Enabling strict header checking disables all hardware acceleration. This includes NP, SP, and CP processing.

upvoted 4 times

Totoahren 1 year, 3 months ago

Answer: D
when check-protocol-header is enabled in strict or loose mode all NPs and CPs are disabled.

upvoted 2 times

charruco 1 year, 2 months ago

The documentation only mentions strict NOT loose

upvoted 1 times

ba68ea0 1 year, 3 months ago

agreed. "Enabling strict header checking disables all hardware acceleration. This includes NP, SP, and CP processing."
https://docs.fortinet.com/document/fortigate/7.4.3/hardware-acceleration/39956/strict-protocol-header-checking-disables-hardware-acceleration

upvoted 1 times

⊟ **Kop01** 1 year, 3 months ago

Selected Answer: C

Answer : C
P53 check-protocol-header strict disables all NPs and CPs.

"The option 'strict-dirty-session-check' will enable to check the session against the original policy when re-validating.
This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together.
If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session.
enable: Enable strict dirty-session check.
disable: Disable strict dirty-session check."
https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-fix-fw-strict-dirty-session-check-drop/ta-p/224031

upvoted 2 times

⊟ **Artbrut** 1 year, 4 months ago

Selected Answer: C

It's C as per https://docs.fortinet.com/document/fortigate/7.2.4/hardware-acceleration/39956

"Enabling strict header checking disables all hardware acceleration. This includes NP, SP, and CP processing."

upvoted 4 times

⊟ **5deee77** 1 year, 4 months ago

Selected Answer: C

The answer is C,

upvoted 1 times

⊟ **Flo31** 1 year, 4 months ago

Selected Answer: C

The answer is C, nothing here can prove that NP or CP is disabled

upvoted 1 times

⊟ **FlavioBarbosa** 1 year, 4 months ago

"D" e a opção correta.
Ao habilitar o "check-protocol-header loose" o FortiGate irá fazer um inspeção rigorosa no cabeçalho em L4, com isso TODA aceleração e desativada NP, SP e CP.

upvoted 2 times

⊟ **mollyk70** 1 year, 4 months ago

set check-protocol-header loose command can infer that there is an NP enabled, thus
A is wrong.
C is wrong
D is most close to answer imo

upvoted 2 times

⊟ **mollyk70** 1 year, 3 months ago

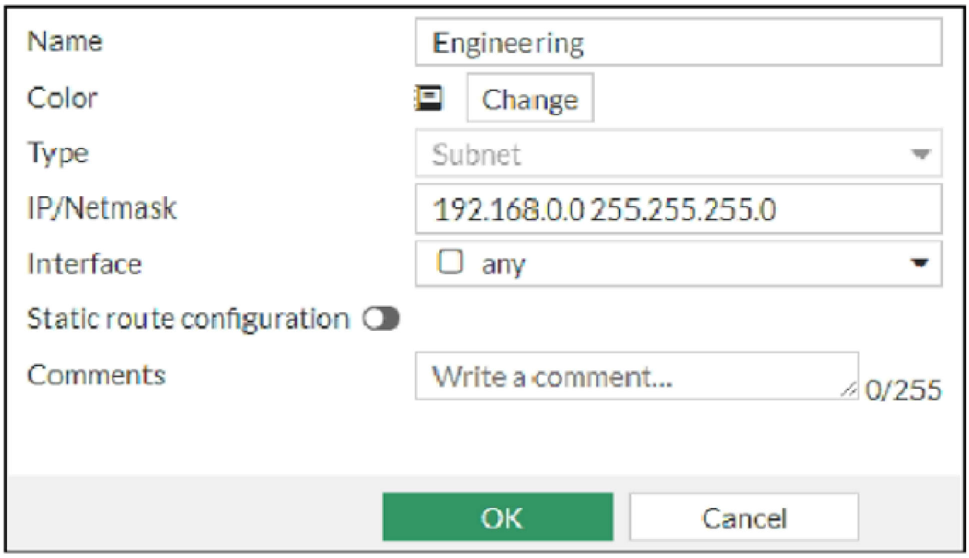
Apologies Study guide P53, set check-protocol-header loose, infers that the NP CP are NOT disabled, so D is wrong
C - Correct

upvoted 3 times

Question #5 *Topic 1*

Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.

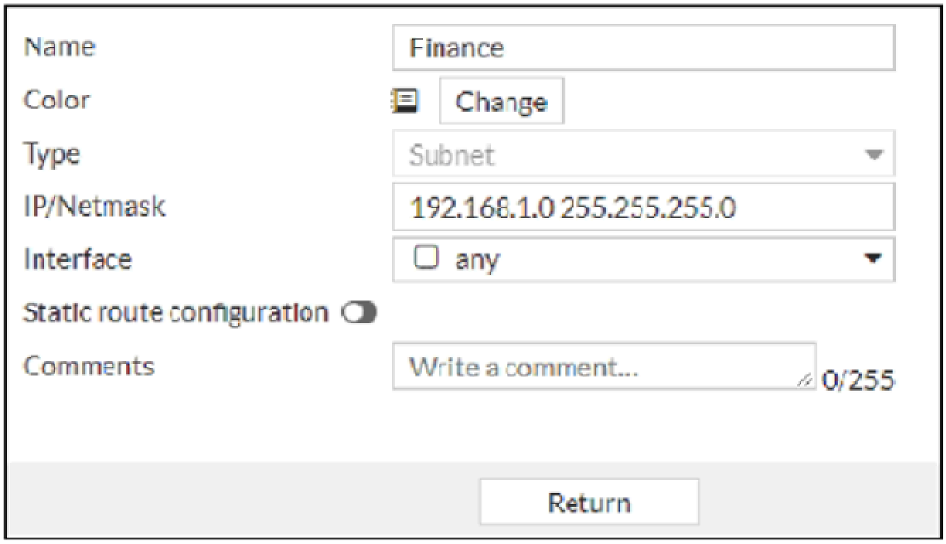
Engineering address object -



Name	Engineering
Color	Change
Type	Subnet
IP/Netmask	192.168.0.0 255.255.255.0
Interface	□ any
Static route configuration	
Comments	Write a comment... 0/255

OK Cancel

Finance address object -



Name	Finance
Color	Change
Type	Subnet
IP/Netmask	192.168.1.0 255.255.255.0
Interface	□ any
Static route configuration	
Comments	Write a comment... 0/255

Return

Why can you modify the Engineering address object, but not the Finance address object?

A. You have read-only access.

B. Another user is editing the Finance address object in workspace mode.

C. FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.

D. FortiGate is registered on FortiManager.

Suggested Answer: *B*

Community vote distribution

C (74%) B (20%) 6%

charruco Highly Voted 1 year, 2 months ago

Selected Answer: C

C is Correct

B is not correct because "Workspace mode is available only through CLI mode:

Pg. 25 in Enterprise_Firewall_7.2_Study_Guide-Online.pdf

upvoted 8 times

rac_sp 12 months ago

very true !! furthermore a warning message is shown to let the administrator know that the object is currently being configured in another workstpace transaction

upvoted 2 times

truserud Highly Voted 1 year, 2 months ago

Selected Answer: C

I made a mistake earlier and voted B as that made most sense at the time. After checking in my lab, C is the correct answer. You are indeed presented with only the "return" option on the object on a downstream device when trying to edit a Global fabric object created on the root device.

upvoted 6 times

myrmidon3 Most Recent 5 months, 2 weeks ago

Selected Answer: C

Security Fabric Configuration:

When a FortiGate is part of a Security Fabric, address objects and other configurations can be synchronized across devices.
If an address object (e.g., the Finance object) was created on the root FortiGate, it is synchronized downstream, and you cannot modify it on the downstream FortiGate. You can only modify such objects on the root FortiGate.

Engineering Address Object:

The Engineering address object is editable because it was created locally on the current FortiGate and is not synchronized from the root FortiGate.

Why the Other Options Are Incorrect:

A. You have read-only access:
If this were the case, you wouldn’t be able to modify the Engineering object either.
B. Another user is editing the Finance address object in workspace mode:
In such a scenario, the interface would indicate that the object is locked due to workspace editing.
D. FortiGate is registered on FortiManager:
While FortiManager can push configurations, the question and behavior are specific to Security Fabric synchronization, not FortiManager.

upvoted 1 times

BatherDom 8 months, 2 weeks ago

Selected Answer: B

Leer pagina 25 del libro FW 7.2

upvoted 1 times

rac_sp 1 year ago

Selected Answer: C

Fgt is joined in the security fabric

upvoted 2 times

evdw 1 year ago

Selected Answer: C

Correct answer is C

upvoted 2 times

havokdu 1 year, 1 month ago

Selected Answer: C

I created a firewall object on a root fortigate. Then, on a downstream FG the object appeared, but when I tried to edit it the OK button was missing.
Only the return button is present.
It doesn't happen like that in Workspace mode. So C is the correct option.

upvoted 3 times

GabrielVillamizar 1 year, 2 months ago

Selected Answer: B

When an administrator edits an object in workspace mode, it is locked, preventing other administrators from editing that object. A warning message is shown to let the administrator know that the object is currently being configured in another workspace transaction. Pg. 25 in Enterprise_Firewall_7.2_Study_Guide-Online.pdf

upvoted 2 times

r3n0 1 year, 3 months ago

Selected Answer: C

In workspace mode the "OK" button is present, you get an error message as soon as you click on it.

When you create a fabric object on a root device, it will synchronize to the downstream devices (if enable) and you will not be able to modify the object on any downstream devices. The "OK" button will NOT be available on downstream devices.

upvoted 4 times

Totoahren 1 year, 3 months ago

Selected Answer: B

Page 25

Enabling strict header checking disables all hardware acceleration. This includes NP, SP, and CP processing.

upvoted 1 times

Totoahren 1 year, 3 months ago

Answer B:

Answer: D

when check-protocol-header is enabled in strict or loose mode all NPs and CPs are disabled.

upvoted 1 times

Totoahren 1 year, 3 months ago

Answer: B

when check-protocol-header is enabled in strict or loose mode all NPs and CPs are disabled.

upvoted 1 times

ac89l 1 year, 3 months ago

Selected Answer: C

tested in lab

upvoted 2 times

truserud 1 year, 3 months ago

Selected Answer: B

A bit tricky from the screenshots, as if B was indeed the correct answer, a warning should be shown that the object is being edited by a different user.

A doesn't make much sense, as you wouldn't be able to make changes to either of the objects if you were in read-mode.

You can edit and configure downstream Fortigates in a Security Fabric at will. There is nothing in the screenshots signifying that this is a downstream device, or the root device.

We you can still configure objects on local devices even if they are managed by FortiManager, and as with question A; if you had logged into a Centrally managed device as read-only, you wouldn't be able to edit any of the objects.

I believe the answer is B, as that makes most sense, even though it is difficult to tell from the screenshots themselves.

upvoted 2 times

truserud 1 year, 2 months ago

Scratch that. The Answer is C. Just tested in my lab, and when creating as a global fabric object, I am not able to edit the adress object on the downstream Fortigate. If it was an object in workspace mode, you would get a warning that the object is locked in a different transistion by a different user.

upvoted 1 times

MikeSco001 1 year, 3 months ago

Selected Answer: C

Answer is C. Tested in Lab

upvoted 3 times

tenebrox 1 year, 3 months ago

Selected Answer: D

Answer is D, i test in my lab with two user, and you always can modify the address but the other user see the warning

upvoted 2 times

5deee77 1 year, 4 months ago

Selected Answer: B

The answer is B page 25

upvoted 1 times

⊟ **rananaj** 1 year, 4 months ago

Selected Answer: B

The answer is B

upvoted 1 times

Question #6 *Topic 1*

Which two statements about the neighbor-group command are true? (Choose two.)

A. It applies common settings in an OSPF area

B. You can apply it in Internal BGP (IBGP) and External BGP (EBGP)

C. You can configure it on the GUI

D. It is combined with the neighbor-range parameter

Suggested Answer: *BD*

Community vote distribution

BC (64%) BD (36%)

bestboy120 Highly Voted 11 months, 2 weeks ago

Selected Answer: BC

Its BC

D is not correct. Why? Lets see
"D. It is combined with the neighbor-range parameter"

It CAN be combined with neighbor-range, but is not required. It can work fine with the “remote-as” parameter alone (which IS required). After defining remote-as, for example, we can select route-maps for all ASes in the defined AS (remote-as)

Just run FGT (physical or VM) and check it yourself

Regarding answer C - yes you can configure it via GUI

upvoted 7 times

myrmidon3 Most Recent 5 months, 2 weeks ago

Selected Answer: BC

Option A: True. The neighbor-group command can indeed be configured using the GUI. This allows users to set up neighbor groups easily in environments where graphical interface configuration is preferred.

Option B: False. The neighbor-group command is not specific to OSPF; it is primarily a BGP construct for grouping peers. Common settings in an OSPF area would typically involve different commands or methodologies.

Option C: False. While the neighbor-group command can be used with the neighbor-range parameter, it is not a requirement. This option's wording ("It is combined") implies necessity, which is inaccurate. The neighbor-group works independently, particularly when the remote-as parameter is defined.

Option D: True. The neighbor-group command can be utilized for both IBGP and EBGP sessions, enabling the application of shared settings across both types of neighbors.

The correct options are B and C, considering the nuanced interpretations of the provided statements.

upvoted 1 times

raydel92 11 months ago

Selected Answer: BC

B and C

upvoted 1 times

Benr06 11 months, 1 week ago

Selected Answer: BC

Can be configured from gui

upvoted 1 times

havokdu 1 year, 1 month ago

Selected Answer: BC

B and C

_ neighbor-group can be configured from the GUI since FortiOS 7.2.0

_ You can use EBGP in neighbor-group

_ neighbor-range is not mandatory

upvoted 2 times

⊟ **TheUsD** 1 year, 2 months ago

I'm thinking it is B and C. While it CAN be combined, it is not required. The wording on the answer say "It IS COMBINED..." meaning it is a requirement. You can definitely, create a neighbor-range in the GUI. The wording on answer C say "YOU CAN" and not "YOU MUST".

I could be over thinking this but B C sounds more correct.

upvoted 2 times

⊟ **ac89l** 1 year, 3 months ago

but why C is not correct ?

upvoted 1 times

⊟ **Artbrut** 1 year, 4 months ago

Selected Answer: BD

Study guide p. 208/209

upvoted 3 times

⊟ **FlavioBarbosa** 1 year, 4 months ago

"B" e "D" estão corretas.

O parâmetro e utilizado com IBGP e EBGP para agrupar os Neighbors e consequentemente aplicá-lo dentro do "config neighbor-range"

upvoted 1 times

⊟ **rananaj** 1 year, 4 months ago

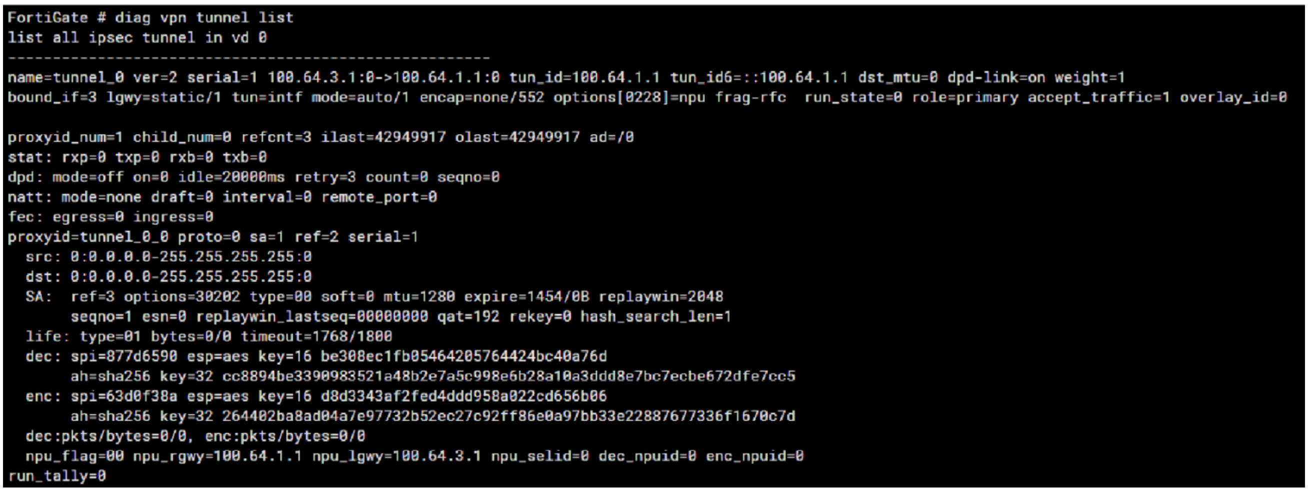
Selected Answer: BD

The answer is BD

upvoted 1 times

Question #7 Topic 1

Refer to the exhibit, which contains information about an IPsec VPN tunnel.



```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1 dst_mtu=0 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1768/1800
  dec: spi=877d6590 esp=aes key=16 be308ec1fb05464205764424bc40a76d
       ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
  enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
       ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

What two conclusions can you draw from the command output? (Choose two.)

A. Dead peer detection is set to enable

B. The IKE version is 2

C. Both IPsec SAs are loaded on the kernel

D. Forward error correction in phase 2 is set to enable

Suggested Answer: *BC*

Community vote distribution

BC (100%)

havokdu Highly Voted 7 months ago

Selected Answer: BC

ver=2 is IKEv2

dpd: mode=off (dead peer detection is disabled)

fec: egreess=0 ingress=0 (forward error correction is disabled) (also FEC is phase1 not 2)

npu_flag=00 means that both IPsec SA are loaded in the kernel
Study guide page 321

upvoted 7 times

5deee77 Highly Voted 10 months ago

Selected Answer: BC

The answer is B (ver:2) C (npu-flag=00)

upvoted 5 times

charruco Most Recent 8 months, 1 week ago

Selected Answer: BC

B and C are correct

upvoted 3 times

Totoahren 9 months, 2 weeks ago

BC Response:
ver=2 (this is ikea2)
dpd: mode=off (dead peer detection is disabled)
fec: egreess=0 ingress=0 (forward error correction is disabled)
option c is discard, I'm not sure why

upvoted 2 times

havokdu 7 months ago

npu_flag=00 means that both IPsec SA are loaded in the kernel

Study guide page 321

upvoted 1 times

rananaj 10 months, 1 week ago

Selected Answer: BC

The answer is BC

upvoted 3 times

Question #8 *Topic 1*

Which two statements about IKE version 2 fragmentation are true? (Choose two.)

A. Only some IKE version 2 packets are considered fragmentable

B. The reassembly timeout default value is 30 seconds

C. It is performed at the IP layer

D. The maximum number of IKE version 2 fragments is 128

Suggested Answer: *AD*

Community vote distribution

AC (83%) Other

havokdu Highly Voted 1 year, 1 month ago

Selected Answer: AC

A: Only some IKEv2 packets are considered fragmentable: AUTH, CREATE_CHILD_SA, and some INFORMATIONAL.

B: Reassembly timeout is 15 seconds, not 30 seconds.

C: Check the question and the Study guide. IKEv2 fragmentation does happen in the IP layer, and IKEv2 fragmentation "SUPPORT" happens at the IKE layer instead of the IP layer.

D: The maximum number of IKEv2 fragments is 64, not 128

upvoted 6 times

truserud Highly Voted 1 year, 3 months ago

Selected Answer: AC

A and C are correct. See page 300 in the Enterprise Firewall 7.2 Study Guide:

A: Only some IKEv2 packets are considered fragmentable: AUTH, CREATE_CHILD_SA, and some INFORMATIONAL.

C: Page 299 in Study Guide: If fragmentation occurs at the IP layer, during the IKEv2 connection, it is possible that payload sizes may exceed the IP MTU and packets get fragmented.

Now, on page 300, it is indeed stated that fragmentation is performed on the IKE-layer to solve the issues raised with Fragmentation on the IP-layer.

This is supported on IKEv2 with IKEv2 fragmentation support:

```
config vpn ipsec-phase1-$interface
set ike-version 2
set fragmentation enable | disable
set fragmentation-mtu $size
```

Bottom line; somewhat tricky question, at least with regards to it requesting two answers, and i definitely isn't B or D.

upvoted 5 times

networkconundrums1 Most Recent 10 months, 3 weeks ago

Maximum number of IKEv2 fragments = 64 (for reassembly)

The Answer is A and C

upvoted 1 times

mecacig953 1 year ago

only one anwer is right . A study guide page 300

upvoted 3 times

charruco 1 year, 2 months ago

Selected Answer: AC

A and C are correct

upvoted 3 times

Kop01 1 year, 3 months ago

Selected Answer: AC

Answer should be A only, but it requires 2 answers so it's AC ...

p300 :

A correct : "Only some packets are considered fragmentable."

C wrong : "With IKEv2 fragmentation support, the fragmentation occurs at the IKE layer instead of the IP layer." BUT if set fragmentation is set to disable, then answer C could be right ....

BD wrong : "The maximum number of IKEv2 fragments are 64, and the reassembly timeout is 15 seconds."

upvoted 2 times

Artbrut 1 year, 4 months ago

Selected Answer: A

only A is correct imho

A -> yes, study guide p. 300

B -> reassembly timeout 15 sec, not 30

C -> nope, fragmentation is done at IKE layer, not IP! (To not be blocked by firewalls)

D -> nope, the max number is 64 (p. 300 study guide)

upvoted 1 times

Artbrut 1 year, 4 months ago

regarding C: it could be right if ikev2 fragmentation support is not configured

upvoted 1 times

5deee77 1 year, 4 months ago

Selected Answer: AC

The answer is A (page 300) C (page 299) Enterprise_Firewall_7.2_Study_Guide

upvoted 1 times

rananaj 1 year, 4 months ago

Selected Answer: BC

The answer is BC

upvoted 1 times

rananaj 1 year, 4 months ago

The answer is AC

upvoted 1 times

Question #9 *Topic 1*

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 set link-failed-signal enable under config system ha on both cluster members

B. Configure set send-garp-on-failover enable under config system ha on both cluster members.

C. Configure remote link monitoring to detect an issue in the forwarding path.

D. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.

Suggested Answer: *B*

Community vote distribution

A (100%)

truserud Highly Voted 1 year, 3 months ago

Selected Answer: A

Page 98 in the Study Guide:
After a failover, the new primary broadcasts GARP patckets, notifying the network that each vMAC address is now reachable on a different port, however on some switch-models that might not be enough. To solve the issue that MAC-tables on switches are not updated after a failover, you should configure the following on a HA-cluster:
config system ha
set link-failed-signal enable
end

This will force the primary device to shut down all devices except mgmt and HA for one second, forcing the connected l2 devices to update their MAC-tables, as this simulates a link failure.

upvoted 5 times

ray_NSE8 Most Recent 9 months ago

Selected Answer: A

The english study guide 7.2 , page 98 explains this.

upvoted 1 times

CHUA123 10 months, 1 week ago

Selected Answer: A

The only correct answer is A

upvoted 2 times

jddc10006 11 months, 3 weeks ago

A its correct

upvoted 2 times

khalmrj 11 months, 4 weeks ago

A for sure

upvoted 2 times

rac_sp 1 year ago

Selected Answer: A

A for sure

upvoted 2 times

havokdu 1 year, 1 month ago

Selected Answer: A

The answer is A, Study_Guide 7.2, page 98

upvoted 2 times

Tommy_S 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 3 times

charruco 1 year, 2 months ago

Selected Answer: A

The answer is A, Study_Guide 7.2, page 98

upvoted 3 times

Kop01 1 year, 3 months ago

Selected Answer: A

Answer A : p98

upvoted 1 times

5deee77 1 year, 4 months ago

Selected Answer: A

The answer is A, Enterprise_Firewall_7.2_Study_Guide, page 98

upvoted 2 times

Artbrut 1 year, 4 months ago

Selected Answer: A

Should be A as per https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-HA-link-failed-signal-and/ta-p/198050

upvoted 1 times

rananaj 1 year, 4 months ago

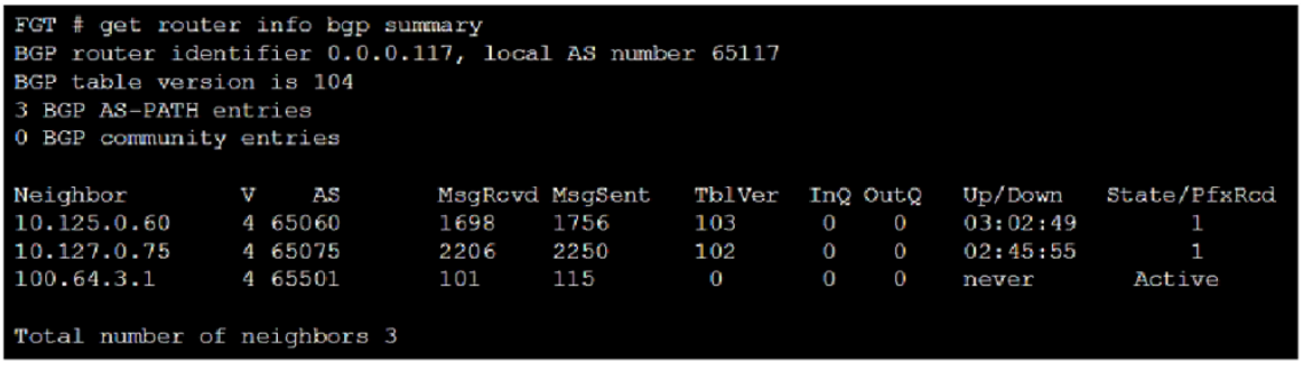
Selected Answer: A

The answer is A

upvoted 1 times

Question #10 *Topic 1*

Refer to the exhibit, which shows the output of a BGP summary.



```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS       MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down   State/PfxRcd
10.125.0.60     4 65060       1698    1756      103      0    0   03:02:49          1
10.127.0.75     4 65075       2206    2250      102      0    0   02:45:55          1
100.64.3.1      4 65501       101     115         0      0    0   never         Active

Total number of neighbors 3
```

What two conclusions can you draw from this BGP summary? (Choose two.)

A. The BGP session with peer 10.127.0.75 is established.

B. External BGP (EBGP) exchanges routing information.

C. The router 100.64.3.1 has the parameter bfd set to enable.

D. The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

Suggested Answer: *AB*

Community vote distribution

AB (89%) 11%

myrmidon3 5 months, 2 weeks ago

Selected Answer: AB

Option A: External BGP (EBGP) exchanges routing information.

True. The AS numbers for the neighbors (65060, 65075, and 65501) are different from the local AS number (65117), indicating these are EBGP sessions, as EBGP connects peers in different ASes.

Option B: The BGP session with peer 10.127.0.75 is established.

True. The State/PfxRcd column for 10.127.0.75 shows a value of 1, meaning the session is established, and it is successfully receiving one route from the peer.

Option C: The router 100.64.3.1 has the parameter bfd set to enable.

False. There is no explicit evidence in the output about the bfd parameter being enabled. This cannot be determined from the given information.

Option D: The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

False. The V column (BGP version) shows 4, which indicates the BGP protocol version used. This does not imply any specific neighbor-range configuration.

upvoted 1 times

ccie8122 8 months, 1 week ago

Selected Answer: AB

@truserd--correction: "4" in response D refers to BGP version 4, not IP version 4. BGPv4 will be used for IPv4 and IPv6. Everything else you state is correct.

upvoted 1 times

havokdu 1 year, 1 month ago

Selected Answer: AB

A and B are correct.

upvoted 1 times

Lomik29 1 year, 1 month ago

It does not matter if the ASNs are private or public. What matters is that the neighbors' ASNs are different than the local ASN which makes it EBGP

upvoted 2 times

charruco 1 year, 2 months ago

Selected Answer: AB

A and B are correct.

Page 210 in the Study Guide

upvoted 1 times

truserud 1 year, 3 months ago

Selected Answer: AB

Page 210 in the Study Guide gives a good overview of the command get router info bgp summary and it's output.

C - You can't see if BFD is enabled with get router info bgp summary. For that you would run get router info bfd neighbor. So C doesn't quite make sense as a correct answer, as the information to answer that is lacking.

D: Is just plain wrong, the "4" they are reffering to, and which you see in the output refers to IPv4 which is being used in the BGP configuration.

Thus A & B is correct.

A because the peer state is indeeed established, showing up-time and that is has received 1 prefix.

B because the peers are indeed eBGP peers and are exchanging routing-information.

upvoted 3 times

ccie8122 8 months, 1 week ago

See comment above. "4" refers to BGP not IP version.

upvoted 1 times

Artbrut 1 year, 3 months ago

Selected Answer: AB

... or they took the documentary AS number space to simulate ebgp. Somehow confusing. If this is the case, I would take A and B

upvoted 2 times

Artbrut 1 year, 3 months ago

Selected Answer: AC

Think I have to revert. B states that "external" bgp exchanges routes. Oversaw that we have here no public AS range.

0-64.495 would bei public

65.512-65.534 is private

upvoted 1 times

VeryOldITGuy 1 year, 2 months ago

Private are 64512 to 65535 and not 65512--- . Which had me searching.. Just mentionning if others wonder too

upvoted 1 times

Artbrut 1 year, 4 months ago

Selected Answer: AB

A and B

upvoted 1 times

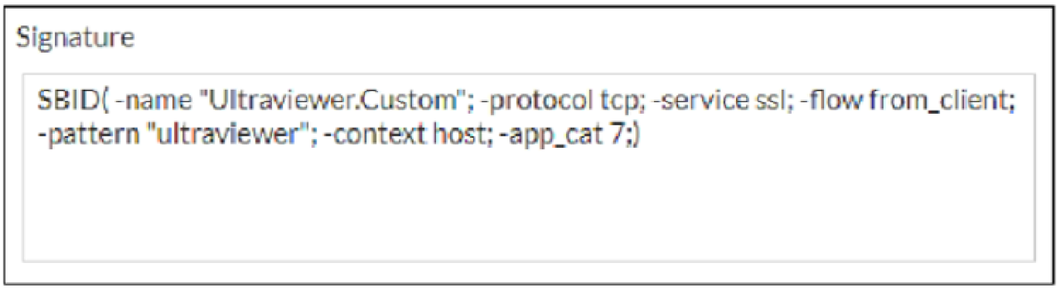
rananaj 1 year, 4 months ago

The answer is AB

upvoted 2 times

Question #11 *Topic 1*

Refer to the exhibit, which shows a custom signature.



Signature

```
SBID( -name "Ultraviewer.Custom"; -protocol tcp; -service ssl; -flow from_client;
-pattern "ultraviewer"; -context host; -app_cat 7;)
```

Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

A. Ensure that the header syntax is F-SBID.

B. Add severity.

C. Add attack_id.

D. Start options with --.

Suggested Answer: *BC*

Community vote distribution

AD (100%)

ray_NSE8 9 months ago

Selected Answer: AD

Studyguide, English, vers 7.2 page 264.

All custom signatures require a header of F-SBID.

An option starts with "--"

All custom signatures require a header of F-SBID.

An option starts with "--"

upvoted 1 times

havokdu 1 year, 1 month ago

Selected Answer: AD

All custom signatures require a header of F-SBID.

An option starts with "--", followed by the option name, and,

sometimes, a value. Some options don't require a value.

upvoted 1 times

charruco 1 year, 2 months ago

Selected Answer: AD

A and D are correct

Pages 274 to 282 Study Guide.

upvoted 1 times

jaymag2 1 year, 3 months ago

Answers are A & D - explained in pages 274 in the Study Guide.

upvoted 1 times

truserud 1 year, 3 months ago

Selected Answer: AD

Answers are A & D - explained in pages 274 to 282 in the Study Guide.

upvoted 1 times

Kop01 1 year, 3 months ago

Answer is A and D : p274

upvoted 1 times

5deee77 1 year, 4 months ago

Selected Answer: AD

A and D, study guide p. 274

upvoted 1 times

⊟ **5deee77** 1 year, 4 months ago

A and D, study guide p. 274

upvoted 1 times

⊟ **FlavioBarbosa** 1 year, 4 months ago

"A" e "D" estão corretas.

A Sintaxe do cabeçalho tem que começar com F-SBID, e as chamadas de "options" precisam começar com "--"

upvoted 1 times

⊟ **Artbrut** 1 year, 4 months ago

Selected Answer: AD

A and D, study guide p. 274

upvoted 1 times

⊟ **rananaj** 1 year, 4 months ago

Selected Answer: AD

The answer is AD

upvoted 1 times

Question #12 *Topic 1*

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

A. Automation stitches can be created to run diagnostic commands and email the results when CPU or memory usage exceeds specified thresholds.

B. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

C. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.

D. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

charruco 8 months, 1 week ago

Selected Answer: AD

A and D are correct

Pages 73 to 77 Study Guide

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: AD

Pages 73 to 77 in the Study Guide-

A - Yes, sure, you can easily create stitches to run diagnostics based on triggers like events generated on devices.

D - Administrator-defined automated workflows (called stitches) use if/then logic to cause FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up stitches for any device in the Security Fabric. However, a Security Fabric is not a requirement to use stitches. If you configure stitches in a Security Fabric, you must configure them on the root FortiGate.

upvoted 3 times

5deee77 10 months ago

Selected Answer: AD

The answer is AD

upvoted 1 times

Artbrut 10 months ago

Selected Answer: AD

A -> high CPU or memory is the trigger for the stitch

B -> nope, as action parameters can only be applied to sequential execution, not to parallel (p. 76 study guide)

C -> nope, you can apply stitches to any Fortinet device in fabric, but you should configure it on the Fortigate root (p.73)

upvoted 3 times

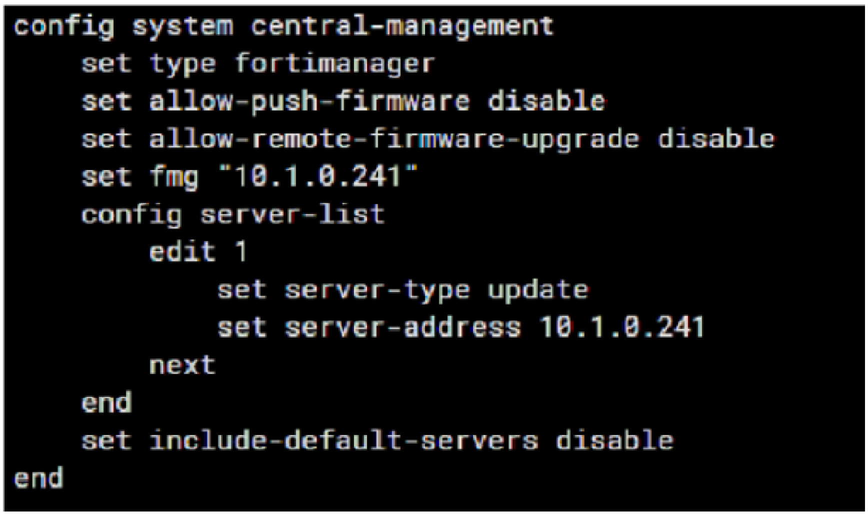
rananaj 10 months, 1 week ago

The answer is AD

upvoted 1 times

Question #13 *Topic 1*

Refer to the exhibit which shows config system central-management information.



```
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.1.0.241"
    config server-list
        edit 1
            set server-type update
            set server-address 10.1.0.241
        next
    end
    set include-default-servers disable
end
```

Which setting must you configure for the web filtering feature to function?

A. Set update-server-location to automatic

B. Add server.fortiguard.net to the Server list

C. Configure securewf.fortiguard.net on the default servers

D. Configure server-type with the rating option

Suggested Answer: *B*

Community vote distribution

D (100%)

havokdu 7 months ago

Selected Answer: D

Refer to study guide, page 223

Another correct option would be enable include-default-servers

upvoted 2 times

charruco 8 months, 1 week ago

Selected Answer: D

D is correct - Page 223 in the Study Guide.

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: D

D is correct. To configure webfilter updates where FortiManager is the FDN in the environment, you must configugue

set server-type rating

to enable webfilter, antispam and other stuff.

The "update" option is for IPS, AV and similar.

This is detailed on page 223 in the Study Guide.

upvoted 4 times

5deee77 10 months ago

Selected Answer: D

study guide, page 223

upvoted 2 times

rananaj 10 months, 1 week ago

The answer is D

upvoted 1 times

Question #14 *Topic 1*

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

A. FortiGate uses the FortiTelemetry protocol to communicate with FortiAnalyzer

B. Only the root FortiGate sends logs to FortiAnalyzer

C. Only FortiGate devices with configuration-sync set to default receive and synchronize global CMDB objects that the root FortiGate sends

D. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

Suggested Answer: *AD*

Community vote distribution

CD (100%)

charruco 8 months, 1 week ago

Selected Answer: CD

C and D are correct - Study Guide, Page 67

upvoted 2 times

ba68ea0 9 months ago

Selected Answer: CD

Answer C and d

upvoted 2 times

truserud 9 months, 3 weeks ago

Selected Answer: CD

C & D - Study Guide, Page 67 explains this.

upvoted 2 times

truserud 9 months, 3 weeks ago

Update, page 64 details information with regards to root informing FortiAnalyzer about topology information.

upvoted 2 times

Kop01 9 months, 4 weeks ago

Selected Answer: CD

Answer CD

upvoted 2 times

Artbrut 10 months ago

Selected Answer: CD

A -> nope, Fortigate uses FortiTelemetry to communicate with upstream devices, not only FortiAnalyzer

B -> nope, all devices send directly to FortiAnalyzer

C -> yes

D -> yes

pages 64 and following in study guide

upvoted 2 times

rananaj 10 months, 1 week ago

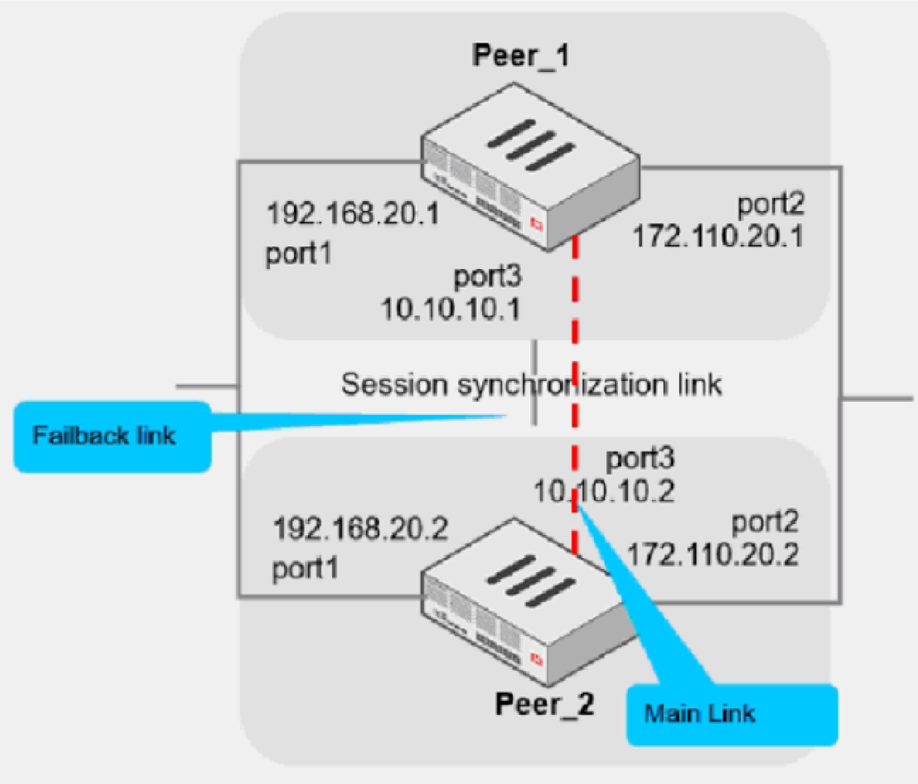
Selected Answer: CD

The answer is CD

upvoted 2 times

Question #15 Topic 1

Refer to the exhibit which shows two configured FortiGate devices and peering over
FGSP.



The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev <interface> command.
What is the primary reason to configure the main link?

A. To have only configuration synchronization in layer 3

B. To load balance both sessions and configuration synchronization between layer 2 and 3

C. To have both sessions and configuration synchronization in layer 3

D. To have both sessions and configuration synchronization in layer 2

Suggested Answer: *D*

Community vote distribution

D (81%) A (19%)

r3n0 Highly Voted 9 months, 1 week ago

Selected Answer: D

FGSP only sync sessions and it occur at L3 by default. We can move it at L2 with the set seesion-sync-dev.
Configuration sync is an independant feature and occur, by default, at L2 as is part of FGCP and use hbdev command.
Configuration sync can be configure to occur at L3 with the command unicast-peers, which is not the case here.

If we move the sessions sync at L2, the configuration is already sync at L2 both will occur at L2.

https://docs.fortinet.com/document/fortigate/7.2.7/administration-guide/84777/standalone-configuration-synchronization

upvoted 9 times

truserud Highly Voted 9 months, 3 weeks ago

Selected Answer: D

I see a lot of discussion here with regards to the correct answer being either A or D. I think D is correct based on pages 113 and 118 in the Study Guide.
Page 118 specifically states that Layer 2 is required for config sync in a FGSP standalone cluster configuration.

And that you can enable session synchronization with layer 2 with the set session-syn-dev <interface #> command. I am a bit conflicted in the choice though, so it needs some further studying to be sure.

upvoted 5 times

truserud 9 months ago

In addition to my former comment, pages 110 and 111 state the following:
Standalon configuration Synchronization is based on FGCP config sync, thus it requires layer 2 adjacency to form a cluster and sync config. This means that config sync already is using layer 2 as default.

Page 111 states that sessions are synced between peers in an FGSP topology over layer 3 by default.

Again showing that D is the correct answer.

upvoted 1 times

pepso100 Most Recent 4 months, 1 week ago

Selected Answer: B

When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize sessions in layer 2 instead of layer 3 using the session-sync-dev setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes
unavailable.

WHAT IS UNCLAR?
By def. both config and sessions are syncing via L3.
If you enalbe session-syn-dev <interface> command you CREATE DEDICATED L2 connectoins for sessions sync only!! and CONFIG sync still remain in old L3 (Heratbeat interface).

exmple:

```
config system ha
set session-sync-dev port10 port12
end
```

So if both port10 and port12 failed, session sync "return back" from L2 to original HeartBeat L3 interface.

Only B is correct answer.

upvoted 1 times

myrmidon3 5 months, 2 weeks ago

Selected Answer: D

Session synchronization (FGSP):
By default, it occurs at Layer 3.
It can be moved to Layer 2 using the set session-sync-dev command, as shown in the configuration.

Configuration synchronization (FGCP):
It is a separate feature, independent of FGSP.
By default, it operates at Layer 2 and uses the hbdev command.
It can be moved to Layer 3 using the unicast-peers command, which is not configured here.
Since the configuration in the exhibit moves session synchronization to Layer 2 using the set session-sync-dev command, and configuration synchronization remains at Layer 2 by default, both session and configuration synchronization will now occur at Layer 2.
Correct Answer: D. To have both sessions and configuration synchronization in layer 2

upvoted 1 times

havokdu 7 months ago

Selected Answer: D

Refer to study guide page 113
You can also specify the interfaces used to synchronize sessions in layer 2 INSTEAd of layer 3 using the session-sync-dev setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session
synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes
unavailable.

upvoted 2 times

charruco 8 months, 1 week ago

Selected Answer: D

D is correct

https://docs.fortinet.com/document/fortigate/7.2.7/administration-guide/84777/standalone-configuration-synchronization

upvoted 2 times

Totoahren 9 months, 2 weeks ago

Answer: D

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Suggested-Parameters-to-use-for-a-FortiGate/ta-p/230162

upvoted 1 times

for3nsic 9 months, 4 weeks ago

Selected Answer: A

p113

config sync remains at the layer 3

upvoted 2 times

Kop01 9 months, 4 weeks ago

Selected Answer: A

Answer is A:To have only configuration synchronization in layer 3

p113

When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize session in layer 2 instead of layer 3 using the "session-sync-dev" setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes unavailable.

upvoted 1 times

underground07 10 months ago

Selected Answer: D

Session synchronization

You can specify interfaces used to synchronize sessions in L2 instead of L3 using the session-sync-dev setting. For more information about using session synchronization, see Session synchronization interfaces in FGSP.

upvoted 3 times

5deee77 10 months ago

Selected Answer: D

The answer is D.

upvoted 2 times

Artbrut 10 months ago

Selected Answer: A

https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/849059/ha-heartbeat-interface

And:

https://docs.fortinet.com/document/fortiweb/7.4.0/administration-guide/435480/synchronization

"The configurations of the active (or primary) node is automatically synchronized to all the members in the HA group. Synchronization ensures that all appliances in the group remain ready to process traffic, even if you only change one of the appliances. Synchronization traffic uses TCP on port number 6010 and a reserved IP address."

session-sync-dev remains the traffic as layer 2.

The study guide always only talks about the session sync.

upvoted 1 times

grani15 10 months ago

The answer is D.

upvoted 1 times

TheUsD 10 months ago

The answer is D.

Page 113: When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize session in layer 2 instead of layer 3 using the "session-sync-dev" setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes unavailable.

upvoted 2 times

TheUsD 10 months ago

The answer is D.

Page 113: When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize session in layer 2 instead of layer 3 using the "session-sync-dev" setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes unavailable.

upvoted 3 times

33k_ 10 months, 1 week ago

Selected Answer: A

A, in a FGSP Cluster mode you can set that sessions are replicated over L2 and configuration remain in L3 with session-sync-dev:

upvoted 1 times

> **pepso100** 4 months, 1 week ago
>
> you right, but thne answer is B not A :)
>
> upvoted 1 times

> **TheUsD** 10 months ago
>
> The answer is D.
>
> Page 113: When peering over FGSP, by default, the FortiGate devices or FGCP clusters, share information over layer 3 between the interfaces that are configured with peer IP addresses. You can also specify the interfaces used to synchronize session in layer 2 instead of layer 3 using the "session-sync-dev" setting. When a session synchronization interface is configured and FGSP peers are directly connected on this interface, then session synchronization is done over layer 2, only falling back to layer 3 if the session synchronization interface becomes unavailable.
>
> upvoted 2 times

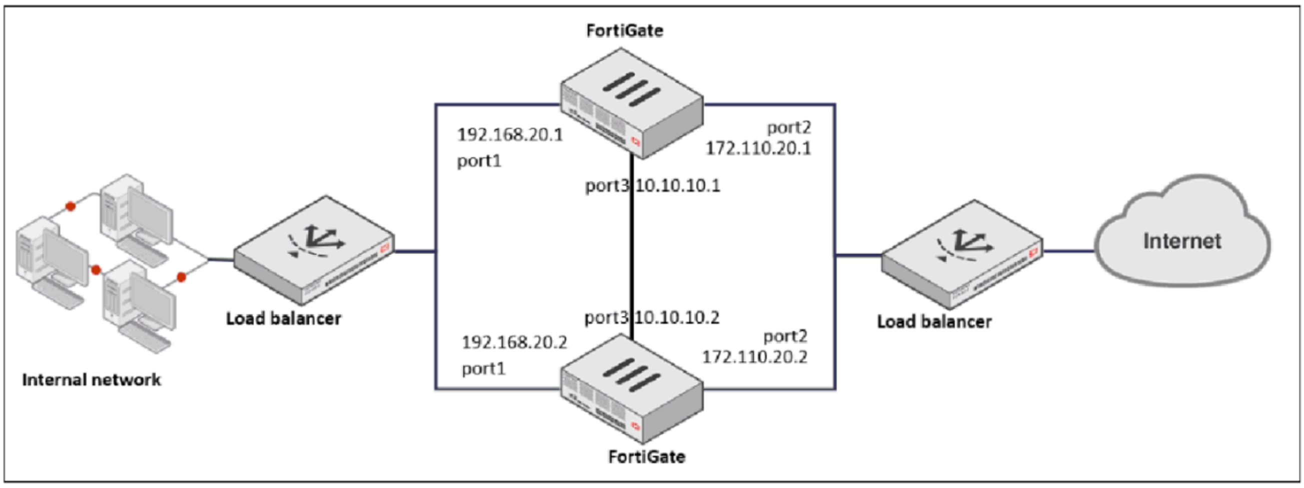
rananaj 10 months, 1 week ago

The answer is D

upvoted 3 times

Question #16 Topic 1

Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

A. FGCP in active-passive mode

B. FGCP in active-active mode

C. FGSP

D. VRRP

Suggested Answer: *C*

Community vote distribution

C (100%)

myrmidon3 5 months, 2 weeks ago

Selected Answer: C

FGSP

This is because FGSP (specifically, FGSP in this context) is designed for scenarios where external load balancers are present, and session synchronization is required between peers.

upvoted 1 times

charruco 8 months, 1 week ago

Selected Answer: C

C is correct.

FGSP is the default option when LBs are used. Study guide page 111

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: C

The Answer is C, based off the pictured topology and page 111 in the Study Guide.

upvoted 3 times

5deee77 10 months ago

Selected Answer: C

The answer is C

upvoted 1 times

Artbrut 10 months ago

Selected Answer: C

page 111 of study guide

upvoted 1 times

rananaj 10 months, 1 week ago

The answer is C

upvoted 1 times

Question #17 *Topic 1*

After enabling IPS, you receive feedback about traffic being dropped.
What could be the reason?

A. IPS is configured to monitor.

B. np-accel-node is set to enable.

C. fail-open is set to disable.

D. traffic-submit is set to disable.

Suggested Answer: *C*

Community vote distribution

C (100%)

Georgeheich 10 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

charruco 1 year, 2 months ago

Selected Answer: C

C is correct

Page 271 Study Guide.

upvoted 2 times

truserud 1 year, 3 months ago

Selected Answer: C

C is correct - explained on page 271 in the Study Guide.

upvoted 2 times

Artbrut 1 year, 4 months ago

Selected Answer: C

C, page 271

upvoted 1 times

Majkiel 1 year, 4 months ago

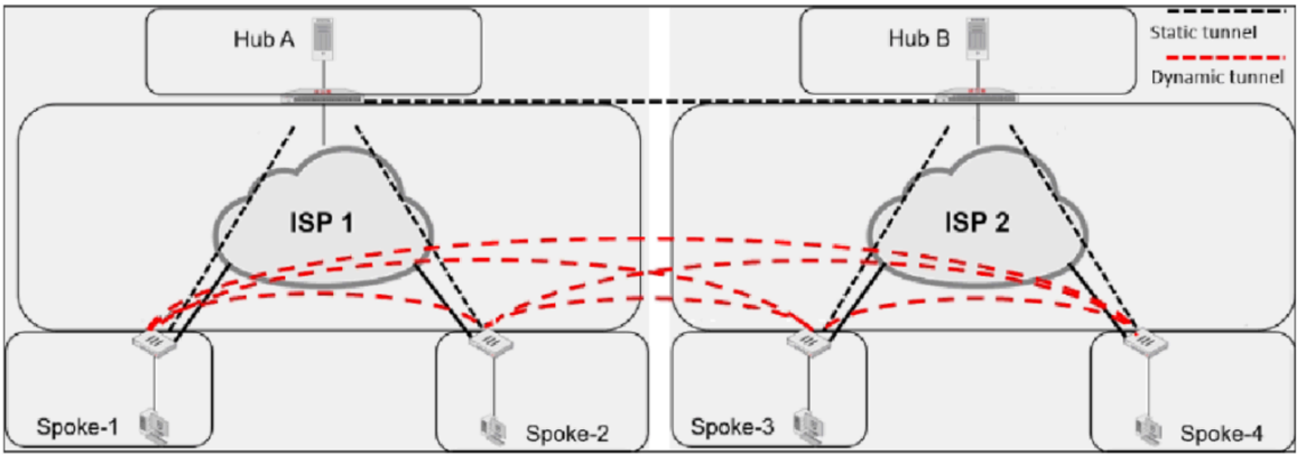
Selected Answer: C

C is the correct answer, site 271

upvoted 1 times

Question #18 Topic 1

Refer to the exhibit which shows an ADVPN network.



Which VPN phase 1 parameters must you configure on the hub for the ADVPN feature to function? (Choose two.)

A. set auto-discovery-sender enable

B. set auto-discovery-receiver enable

C. set add-route enable

D. set auto-discovery-forwarder enable

Suggested Answer: *AD*

Community vote distribution

AD (100%)

Febrian 6 months, 2 weeks ago

Selected Answer: AD

set auto-discovery-sender -> from hub to spokes

set auto-discovery-forwarder -> from hub to hub

upvoted 1 times

charruco 8 months, 1 week ago

Selected Answer: AD

A and D are correct

page 332 Study Guide

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: AD

A & D are correct, see the Study Guide from page 327 detailing ADVPN.

upvoted 2 times

5deee77 10 months ago

Selected Answer: AD

A D Study Guide d.332

upvoted 2 times

Artbrut 10 months ago

Selected Answer: AD

A and D are correct

upvoted 1 times

33k_ 10 months, 1 week ago

Selected Answer: AD

Study Guide d.332

upvoted 1 times

Question #19 *Topic 1*

Which two statements about metadata variables are true? (Choose two.)

A. The metadata format is $<metadata_variable_name>.

B. You create them on FortiGate.

C. They can be used as variables in scripts.

D. They apply only to non-firewall objects.

Suggested Answer: *AC*

Community vote distribution

AC (75%) C (25%)

myrmidon3 5 months, 2 weeks ago

Selected Answer: AC

A. The metadata format is $<metadata_variable_name>.

True. Metadata variables in Fortinet systems follow the format $<metadata_variable_name>, where the variable name is enclosed in angle brackets. This is the standard format for referencing metadata variables.

B. You create them on FortiGate.

False. Metadata variables are typically defined and managed on FortiManager or in FortiCloud, not directly on FortiGate. FortiGate uses these variables in policies or configurations pushed from FortiManager.

C. They can be used as variables in scripts.

True. Metadata variables can be utilized in scripts to dynamically reference objects or configurations, making them versatile for automation and templating.

D. They apply only to non-firewall objects.

False. Metadata variables can apply to various objects, including firewall policies and other security-related configurations, not just non-firewall objects.

upvoted 1 times

Totoahren 9 months, 1 week ago

Selected Answer: AC

https://docs.fortinet.com/document/fortimanager/7.2.0/new-features/218740/metadata-variables-are-supported-in-firewall-objects-configuration

upvoted 2 times

truserud 9 months, 3 weeks ago

Selected Answer: AC

As it is a "choose two" solution, the most correct second answer is A, even though the format isn't entirely correct. A metafield is called upon in a CLI script with $(your_metafield_name), if it's jinja2 it's called upon with {{your_metafield_name}}. C is definitely correct. The format for variables and usage is explained in page 158 in the Study Guide (jinja2 is not described though, only as a side note in comparison with TCL).

upvoted 2 times

5deee77 10 months ago

Selected Answer: C

C, page 158, A https://docs.fortinet.com/document/fortimanager/7.2.0/new-features/218740/metadata-variables-are-supported-in-firewall-objects-configuration

upvoted 2 times

Artbrut 10 months ago

Selected Answer: AC

https://docs.fortinet.com/document/fortimanager/7.2.0/new-features/218740/metadata-variables-are-supported-in-firewall-objects-configuration

upvoted 2 times

Question #20 *Topic 1*

Refer to the exhibits, which contain the network topology and BGP configuration for a hub.

Exhibit A.

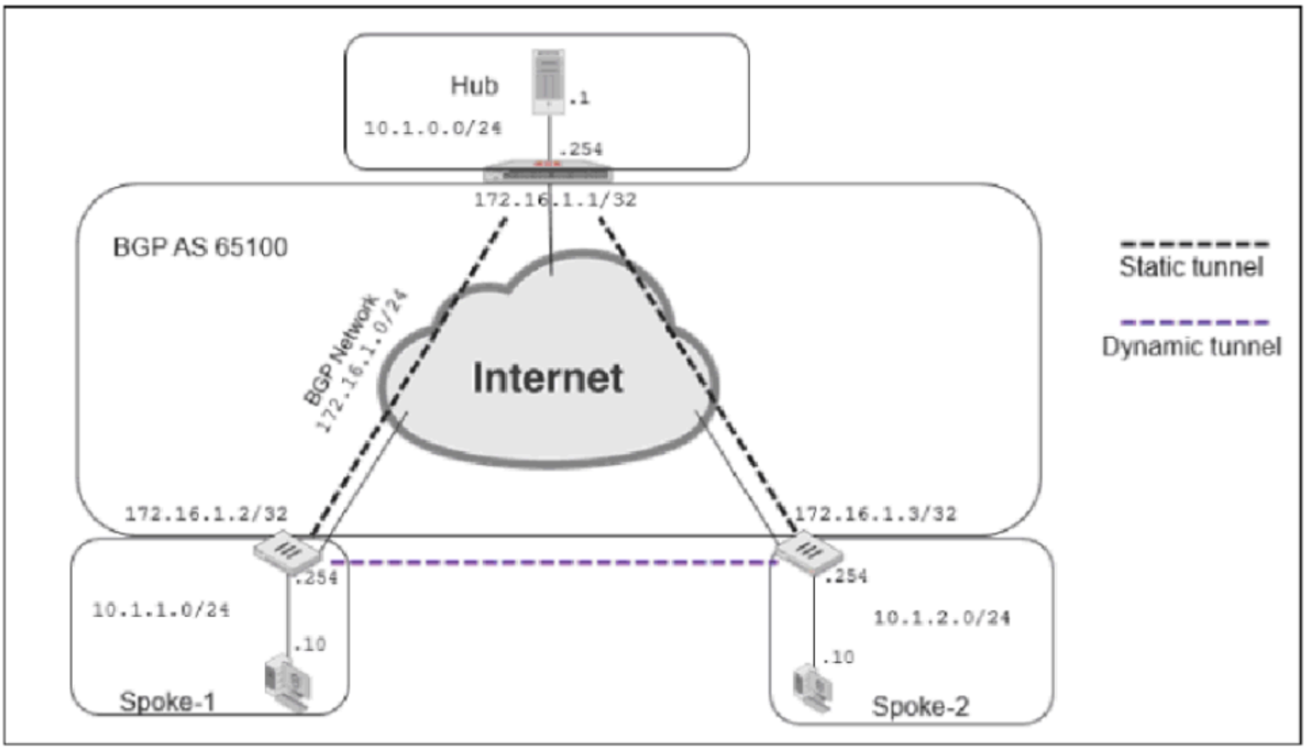
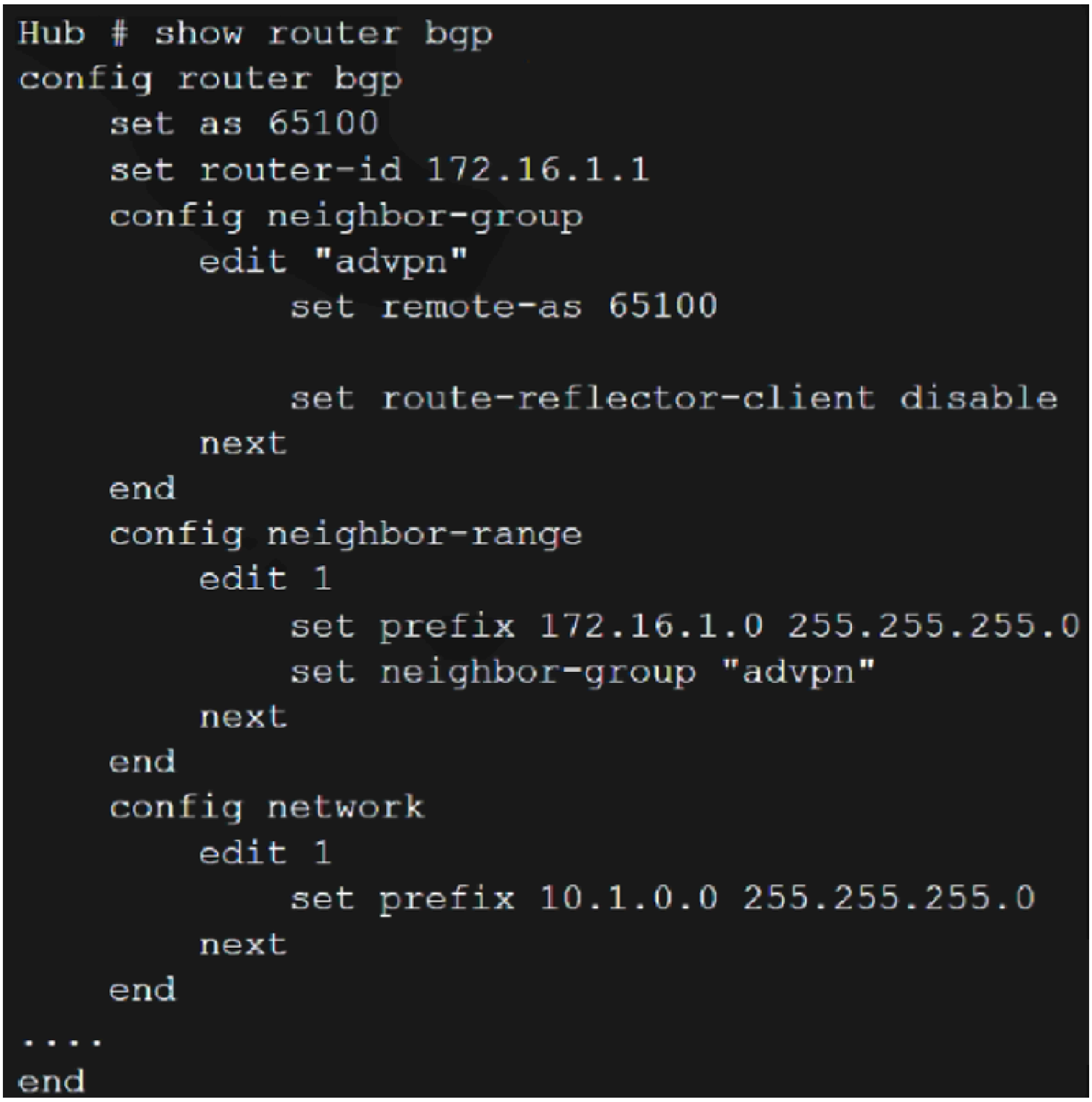


Exhibit B.



```
Hub # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.1
    config neighbor-group
        edit "advpn"
            set remote-as 65100

            set route-reflector-client disable
        next
    end
    config neighbor-range
        edit 1
            set prefix 172.16.1.0 255.255.255.0
            set neighbor-group "advpn"
        next
    end
    config network
        edit 1
            set prefix 10.1.0.0 255.255.255.0
        next
    end
....
end
```

An administrator is trying to configure ADVPN with a hub and spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub

is receiving route information from both spokes over iBGP; however the spokes are not receiving route information from each other.
What change must the administrator make to the hub BGP configuration so that the routes learned from one spoke are forwarded to the other spoke?

A. Configure the hub as a route reflector

B. Configure auto-discovery-sender on the hub

C. Add a prefix list to the hub that permits routes to be shared between the spokes

D. Enable route redistribution under config router bgp

Suggested Answer: *B*

Community vote distribution

A (90%) 10%

⊟ **ccie8122** 8 months, 1 week ago

Selected Answer: A

iBGP rules disallow advertisement of any prefix learned from any iBGP neighbor to any other iBGP neighbor. This means you must create a full mesh (i.e., all iBGP speakers must peer with ALL other iBGP speakers in the ASN). Route reflection allows you to circumvent this restriction as route reflectors will advertise all iBGP-learned routes to all of its route-reflector clients.

upvoted 1 times

⊟ **charruco** 1 year, 2 months ago

Selected Answer: A

A is correct
page 338 Study Guide.

upvoted 1 times

⊟ **truserud** 1 year, 3 months ago

Selected Answer: A

Correct answer is A, as stated on page 338 in the Study Guide.

upvoted 2 times

⊟ **Kop01** 1 year, 3 months ago

Selected Answer: A

Answer A : p338
"If you are using ibgp for advpn, you must configure the hub as a route reflector. So, routes learned from one spoke are forwarded to the other spokes."

upvoted 2 times

⊟ **5deee77** 1 year, 4 months ago

Selected Answer: A

p. 338 study guide

upvoted 1 times

⊟ **Artbrut** 1 year, 4 months ago

Selected Answer: A

p. 338 study guide.
"If you are using ibgp for advpn, you must configure the hub as a route reflector. So, routes learned from one spoke are forwarded to the other spokes."

upvoted 2 times

⊟ **Dranizz** 1 year, 4 months ago

Selected Answer: A

They are asking about route from each other not being redistributed to each other, not the ADVPN dynamic connexion. And it shows that Route Reflector is not enabled

upvoted 2 times

⊟ **Flo31** 1 year, 4 months ago

Answer A

upvoted 1 times

⊟ **33k_** 1 year, 4 months ago

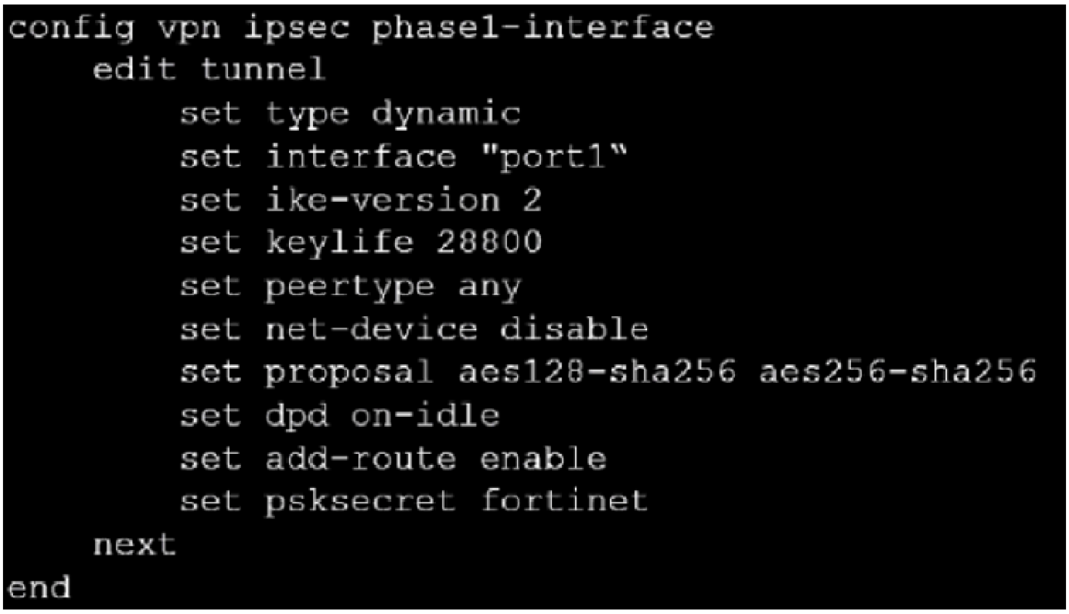
Selected Answer: B

You must enable set auto-discovery-sender if you want ADVPN. This setting indicates that when IPsec traffic transits the hub, it should send a shortcut offer to the initiator of the traffic to indicate that it couldperhaps establish a more direct connection (shortcut).

upvoted 1 times

Question #21 *Topic 1*

Refer to the exhibit, which contains a partial VPN configuration.



```
config vpn ipsec phase1-interface
    edit tunnel
        set type dynamic
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set add-route enable
        set psksecret fortinet
    next
end
```

What can you conclude from this configuration?

A. FortiGate creates separate virtual interfaces for each dial-up client

B. The VPN should use the dynamic routing protocol to exchange routing information through the tunnels

C. Dead peer detection is disabled

D. The routing table shows a single IPSec virtual interface

Suggested Answer: *A*

Community vote distribution

D (100%)

Eric0_0 1 year ago

Selected Answer: D

set net-device disable. FortiGate won't create separate virtual interface for each tunnel. Only a single interface is created.

upvoted 1 times

havokdu 1 year, 1 month ago

Selected Answer: D

If net-device is disabled, FortiGate creates a single IPsec virtual interface that is shared by all IPsec clients connecting to the same dial-up VPN.

upvoted 1 times

charruco 1 year, 2 months ago

Selected Answer: D

D is correct

Page 312 in the Study Guide.

upvoted 1 times

truserud 1 year, 3 months ago

Selected Answer: D

D is the correct answer, described on page 312 in the Study Guide.

upvoted 2 times

Kop01 1 year, 3 months ago

Selected Answer: D

Answer D : p312

If net-device id sibaled, Fortigate creates a single IPsec virtual interface that is shared by all IPsec clients connecting to the same dial-up VPN

upvoted 3 times

5deee77 1 year, 4 months ago

Selected Answer: D

D as per study guide p. 312

upvoted 1 times

Artbrut 1 year, 4 months ago

Selected Answer: D

D as per study guide p. 311

upvoted 2 times

Flo31 1 year, 4 months ago

Answer D

upvoted 1 times

33k_ 1 year, 4 months ago

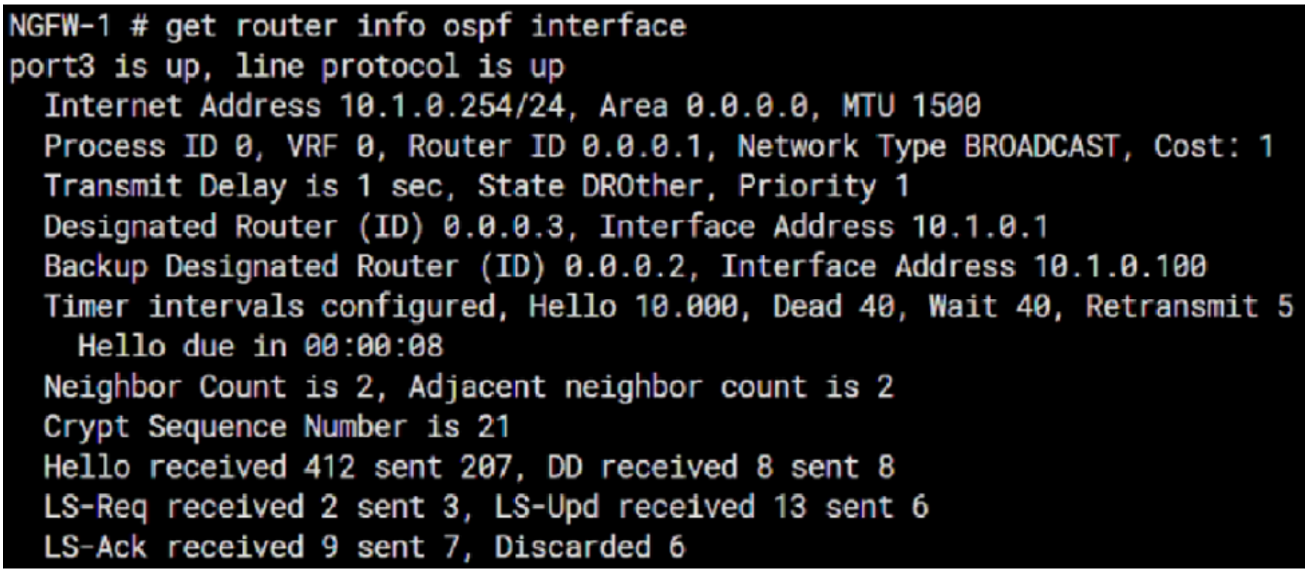
Selected Answer: D

If net-device is disabled, FortiGate creates a single IPsec virtual interface and populates the routing-table with this interface

upvoted 3 times

Question #22 *Topic 1*

Refer to the exhibit which shows information about an OSPF interface.



```
NGFW-1 # get router info ospf interface
port3 is up, line protocol is up
  Internet Address 10.1.0.254/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 0.0.0.3, Interface Address 10.1.0.1
  Backup Designated Router (ID) 0.0.0.2, Interface Address 10.1.0.100
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Crypt Sequence Number is 21
  Hello received 412 sent 207, DD received 8 sent 8
  LS-Req received 2 sent 3, LS-Upd received 13 sent 6
  LS-Ack received 9 sent 7, Discarded 6
```

What two conclusions can you draw from this command output? (Choose two.)

A. The interfaces of the OSPF routers match the MTU value that is configured as 1500.

B. NGFW-1 is the designated router.

C. The port3 network has more than one OSPF router.

D. The OSPF routers are in the area ID of 0.0.0.1.

Suggested Answer: *AC*

Community vote distribution

AC (100%)

charruco 8 months, 1 week ago

Selected Answer: AC

A and C are correct.

Page 180. Study Guide.

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: AC

A & C are correct. Get router info ospf interface is described on page 180 in the Study Guide.

upvoted 2 times

Artbrut 10 months ago

Selected Answer: AC

A -> yes

B -> nope, State is "DROther", so neither DR nor BDR

C -> yes, there is a DR and a BDR

D -> nope, the area is 0.0.0.0, 0.0.0.1 is the Router ID of NGFW-1

upvoted 4 times

Question #23 *Topic 1*

Which two statements about the BFD parameter in BGP are true? (Choose two.)

A. It detects only two-way failures.

B. The two routers must be connected to the same subnet.

C. It allows failure detection in less than one second.

D. It is supported for neighbors over multiple hops.

Suggested Answer: *CD*

Community vote distribution

CD (70%) BC (30%)

myrmidon3 5 months, 2 weeks ago

Selected Answer: CD

A. It detects only two-way failures.

False. BFD (Bidirectional Forwarding Detection) is capable of detecting failures in both directions, not limited to two-way failures.

B. The two routers must be connected to the same subnet.

False. BFD can operate over multi-hop configurations, so the routers do not need to be on the same subnet.

C. It allows failure detection in less than one second.

True. BFD is designed for rapid failure detection, often detecting failures within milliseconds, making sub-second failure detection possible.

D. It is supported for neighbors over multiple hops.

True. BFD supports multi-hop configurations, making it suitable for BGP neighbors that are not directly connected.

upvoted 1 times

charruco 8 months, 1 week ago

Selected Answer: CD

C and D are correct

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: CD

Correct answers are C & D. BFD tuning for BGP is described on page 204 in the Study Guide.
- Enable BFD for faste failure detection (in less than 1 second)
- For BFD multihop path, configure neighbor with; set ebgp-enforce-multihop enable, this is optional and needed IF you need support for multiple hops to reach your peer.
As Artbrut mentions further down, it is stated pretty clearly in the link they have provided that peers must be on the same network for BFD to properly function, HOWEVER, this is for the OSPF configuration. The source in the link they provide is this;
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/729892/bfd-for-multihop-path-for-bgp

Here it is stated that BFD only supported directly connected neighbors previously, but come 7.2.x it now supports multihop. Thus D is the correct second answer for this question.

upvoted 2 times

Kop01 9 months, 4 weeks ago

Selected Answer: CD

Answer CD : p204
"It is independent of the type of media and dtects a one-way device failure in less than a second".
"BFD was initially supported for twor routers directly connected on the same subnet. Now FortiGate can also support neighbors with BFD connected over multiple hops."

upvoted 2 times

BPPPP 10 months ago

C,D

https://docs.fortinet.com/document/fortigate/7.2.3/administration-guide/771813/bfd

BFD for Multihop paths

FortiGate BFD can support neighbors connected over multiple hops. When BFD is down, BGP sessions will be reset and will try to re-establish neighbor connection immediately. See BFD for multihop path for BGP for more information.

upvoted 2 times

5deee77 10 months ago

Selected Answer: CD

study guide page 204

upvoted 1 times

Artbrut 10 months ago

Selected Answer: CD

have to revert, as per 7.2 multiple-hop bfd is supported!

So c + d

upvoted 1 times

Artbrut 10 months ago

Selected Answer: BC

https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-BFD-implementation-and-examples/ta-p/190484

A -> nope, detects one-way device failure

B -> yes as per link

C -> yes as per link

D -> RFC5883 describes multiple-hop-bfd, but I think in context of this question it does not apply as it is under circumstances

upvoted 3 times

Question #24 *Topic 1*

You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces do not appear as available options.
What step must you take to resolve this issue?

A. Refresh the device status using the Device Manager so that FortiGate populates the IPSec interfaces.

B. Install the VPN community and gateway configuration on the FortiGate devices so that the VPN interfaces appear on the Policy Objects on FortiManager.

C. Configure the phase 1 settings in the VPN community that you didn't initially configure. FortiGate automatically generates the interfaces after you configure the required settings.

D. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

raydel92 Highly Voted 11 months ago

Selected Answer: D

When you push a config from FM to FGs nothing new appears on the Policy Objects on FortiManager. The new interfaces are created on FGs. You need to create manually vpn interface mappings under Normalized Interface option to use them on firewall policies

upvoted 8 times

Artbrut Highly Voted 1 year, 4 months ago

Selected Answer: B

It 's B as per study guide p. 304

1. Create VPN community

2. Add gateways (members) to the community

3. Install the VPN community and gateways configuration <--------

4. Add the firewall policies

5. Install the firewall policys

upvoted 5 times

charruco Most Recent 1 year, 2 months ago

Selected Answer: B

B is correct

study guide page 304

upvoted 3 times

maxwellhc 1 year, 2 months ago

Guys, I saw that everyone gets this question wrong. The correct answer is the letter D. Look at doc.fortinet.

https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/80387/interface-mapping

upvoted 3 times

dsticht 1 year, 1 month ago

I really felt like this had merit and I'm still not sure, but I dug a bit more. In this document, it talks about needing an interface for route based VPN, but not for policy based VPN. It gets VERY confusing.

https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/379233/vpn-security-policies

upvoted 1 times

truserud 1 year, 3 months ago

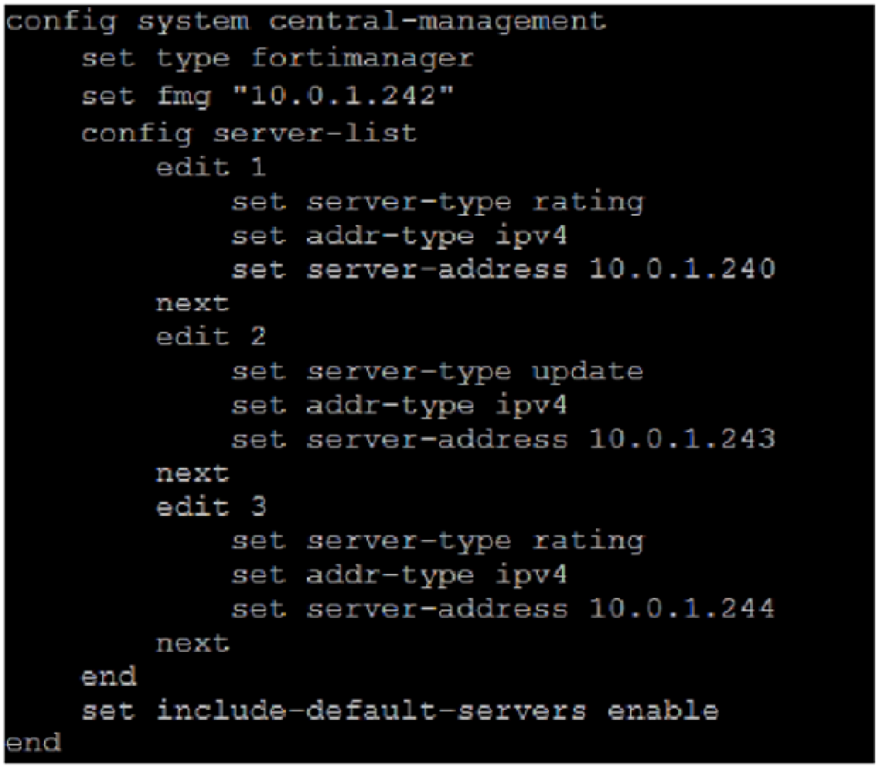
Selected Answer: B

Correct answer is B.

upvoted 4 times

Question #25 Topic 1

Refer to the exhibit, which shows a central management configuration.



```
config system central-management
    set type fortimanager
    set fmg "10.0.1.242"
    config server-list
        edit 1
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.240
        next
        edit 2
            set server-type update
            set addr-type ipv4
            set server-address 10.0.1.243
        next
        edit 3
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.244
        next
    end
    set include-default-servers enable
end
```

Which server will FortiGate choose for web filter rating requests, if 10.0.1.240 is experiencing an outage?

A. 10.0.1.244

B. 10.0.1.242

C. Public FortiGuard servers

D. 10.0.1.243

Suggested Answer: *A*

Community vote distribution

A (100%)

havokdu 7 months ago

Selected Answer: A

It will only fallback to public fortiguard servers if no additional server is configured as rating.

upvoted 1 times

charruco 8 months, 1 week ago

Selected Answer: A

A is correct.

Page 223 Study Guide

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: A

Correct answer is A. Described on page 223 in the Study Guide

upvoted 2 times

5deee77 10 months ago

Selected Answer: A

correct is A

upvoted 2 times

Artbrut 10 months ago

Selected Answer: A

Rating is for web filtering and anti spam, etc.

Update is for antivirus and IPS, etc.

So the question is about web filtering updates, and so the next server with rating is A

upvoted 2 times

Question #26 *Topic 1*

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. FortiGate first checks the OSPF ID to elect a DR.

D. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.

Suggested Answer: *B*

Community vote distribution

D (100%)

charruco 8 months, 1 week ago

Selected Answer: D

D is correct

Study Guide P. 366

upvoted 1 times

Kop01 9 months, 4 weeks ago

Selected Answer: D

Answer D.

p365 + p366 "224.0.0.6 AllDRouters : All other routers send LSA updates and acknowledgements

upvoted 3 times

5deee77 10 months ago

Selected Answer: D

The answer is D

upvoted 2 times

Artbrut 10 months ago

Selected Answer: D

https://community.cisco.com/t5/switching/dr-bdr-ospf/td-p/2010995

"On the broadcast network, all routers that are NOT a DR or BDR are called DROTHER. DROTHER will send their link state updates and LSAck to the AllDRouter address, 224.0.0.6."

upvoted 3 times

MikeSco001 10 months, 1 week ago

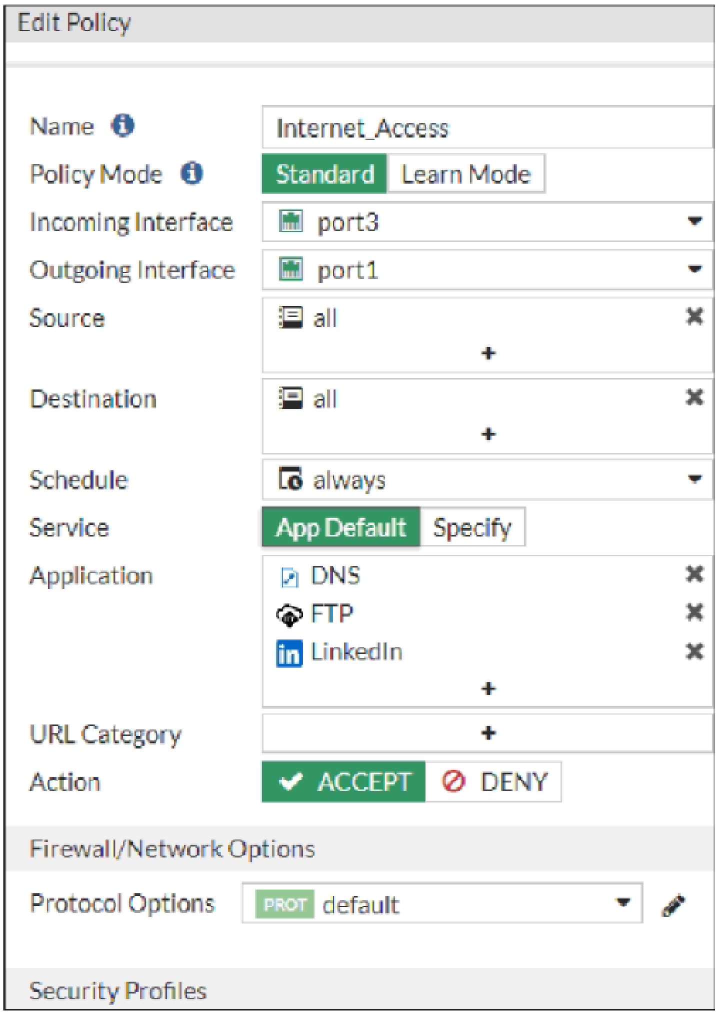
Selected Answer: D

The answer is D

upvoted 3 times

Question #27 *Topic 1*

Refer to the exhibit, which contains a partial policy configuration.



Edit Policy

Name: Internet_Access

Policy Mode: [✓ Standard] Learn Mode

Incoming Interface: port3

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: [✓ App Default] Specify

Application: DNS, FTP, LinkedIn

URL Category:

Action: [✓ ACCEPT] DENY

Firewall/Network Options

Protocol Options: PROT default

Security Profiles

Which setting must you configure to allow SSH?

A. Specify SSH in the Service field.

B. Select an application control profile corresponding to SSH in the Security Profiles section.

C. Include SSH in the Application field.

D. Configure port 22 in the Protocol Options field.

Suggested Answer: *A*

Community vote distribution

C (100%)

charruco 8 months, 1 week ago

Selected Answer: C

C is correct

Study Guide Page 250 - 252

upvoted 1 times

NathanM151 8 months, 3 weeks ago

C is the Answer

upvoted 2 times

truserud 9 months, 3 weeks ago

Selected Answer: C

Answer is C. Application Control on Fortigates configured in NGFW Policy-Based mode is described in the Study Guide on pages 250 through 252.

upvoted 3 times

⊟ **Kop01** 9 months, 4 weeks ago

Selected Answer: C

Answer C

upvoted 1 times

⊟ **Artbrut** 10 months ago

Selected Answer: C

C is correct

upvoted 2 times

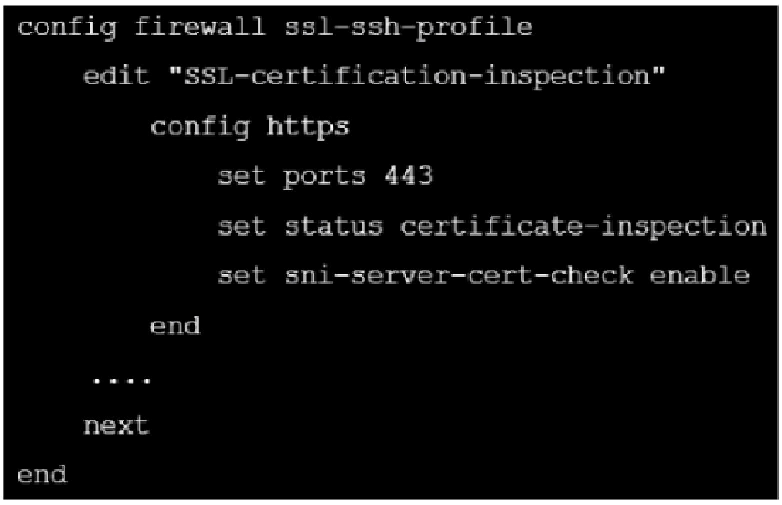
⊟ **Flo31** 10 months, 1 week ago

Answer C

upvoted 2 times

Question #28 *Topic 1*

Refer to the exhibit, which shows an SSL certification inspection configuration.



```
config firewall ssl-ssh-profile
    edit "SSL-certification-inspection"
        config https
            set ports 443
            set status certificate-inspection
            set sni-server-cert-check enable
        end
     ....
    next
end
```

Which action does FortiGate take if the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate?

A. FortiGate uses the first entry listed in the SAN field in the server certificate

B. FortiGate uses the CN information from the Subject field in the server certificate

C. FortiGate uses the SNI from the user's web browser.

D. FortiGate closes the connection because this represents an invalid SSL/TLS configuration

Suggested Answer: *D*

Community vote distribution

B (100%)

10a7494 4 months, 2 weeks ago

Selected Answer: B

enable, so answer is B.

enable: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.

strict: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.

disable: Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

From FortiOS CLI Reference :
https://docs.fortinet.com/document/fortigate/7.2.0/cli-reference/319620/config-firewall-ssl-ssh-profile

upvoted 4 times

Totoahren 6 months, 4 weeks ago

Selected Answer: D

The set sni-server-cert-check enable command ensures that FortiGate validates the Server Name Indication (SNI) in the SSL/TLS handshake. If the SNI provided by the client does not match the Common Name (CN) or any of the Subject Alternative Names (SAN) in the server's certificate, FortiGate considers the SSL/TLS configuration invalid and terminates the connection. This is a security measure to prevent potential mismatches or man-in-the-middle attacks.

upvoted 2 times

jebusruns 9 months ago

Selected Answer: B

Further inspection strict not enable would close the connection page 238 explains this. The question is phrased poorly and so are the answers. If the sni does not match then it uses the domain in the cn.

upvoted 1 times

jebusruns 9 months ago

Selected Answer: D

Questions asks what action when the sni does not match the cn nor san of a certificste. The fortigate should block it.

upvoted 2 times

charruco 1 year, 2 months ago

Selected Answer: B

B is correct

Study Guide p238

upvoted 1 times

DaLoGo 1 year, 2 months ago

D is correct. Read the question. CN does not match.

upvoted 2 times

truserud 1 year, 3 months ago

Selected Answer: B

The Correct answer i B as detailed on page 238 in the Study Guide.

upvoted 2 times

Kop01 1 year, 3 months ago

Selected Answer: B

Answer B p238

upvoted 1 times

5deee77 1 year, 4 months ago

Selected Answer: B

study guide page 238

upvoted 1 times

33k_ 1 year, 4 months ago

Selected Answer: B

If the domain in the SNI field does not match any of the domains listed in the CN and SAN fields, FortiGate uses the domain in the CN field instead of the domain in the SNI field.

upvoted 3 times

MikeSco001 1 year, 4 months ago

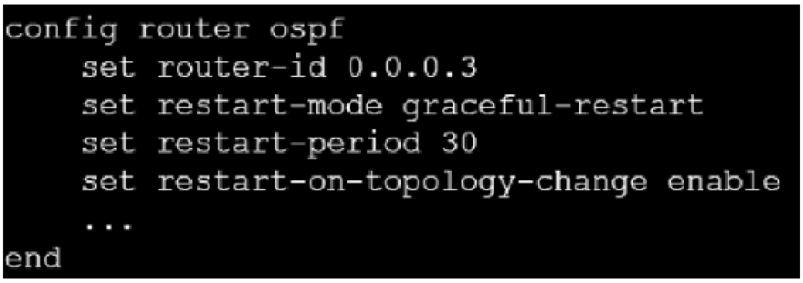
Selected Answer: B

answer is B : Enterprise_Firewall_7.2_Study_Guide-Online.pdf / p 238

upvoted 2 times

Question #29 *Topic 1*

Refer to the exhibit, which contains a partial OSPF configuration.



```
config router ospf
    set router-id 0.0.0.3
    set restart-mode graceful-restart
    set restart-period 30
    set restart-on-topology-change enable
    ...
end
```

What can you conclude from this output?

A. Neighbors maintain communication with the restarting router.

B. The restarting router sends gratuitous ARP for 30 seconds.

C. FortiGate restarts if the topology changes.

D. The router sends grace LSAs before it restarts.

Suggested Answer: *A*

Community vote distribution

D (100%)

charruco 8 months, 1 week ago

Selected Answer: D

D is correct

Study Guide p. 176

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: D

Correct answer is D, as detailed on page 176 in the Study Guide.

In an HA cluster with OSPF graceful restart mode enabled, the primary FortiGate fails over operation to the backup FortiGate. The action sets the router to send a grace LSA.

set restart-on-topology-change enable - When set to enable, the Fortigate will not exit graceful restart mode until done so manually.

upvoted 2 times

5deee77 10 months ago

Selected Answer: D

Answer is D : Enterprise_Firewall_7.2_Study_Guide p. 176

upvoted 1 times

Artbrut 10 months ago

Selected Answer: D

D is correct

upvoted 3 times

MikeSco001 10 months, 1 week ago

Selected Answer: D

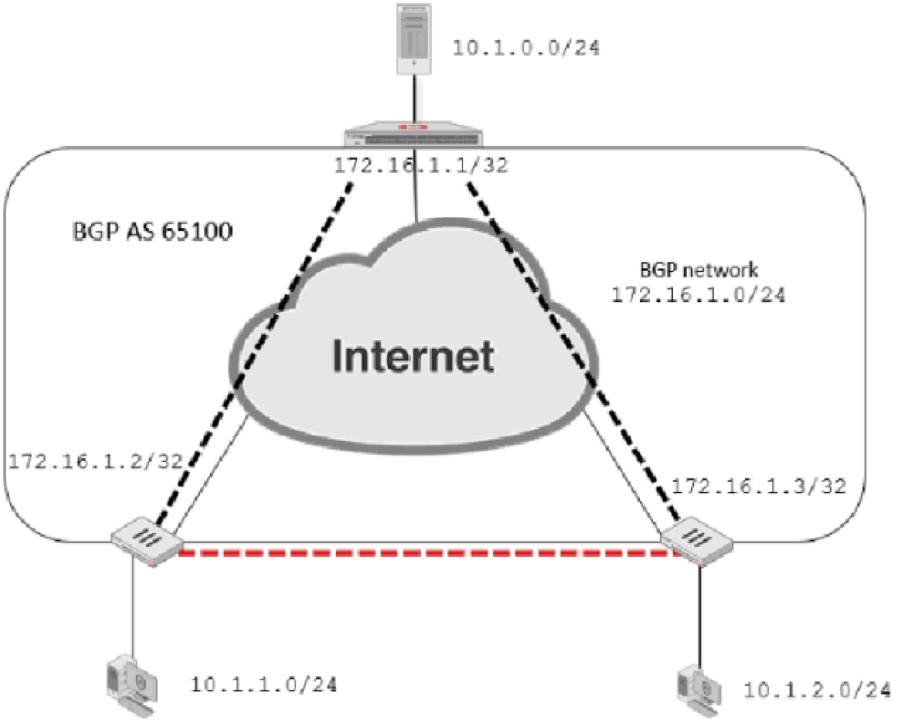
Answer is D : Enterprise_Firewall_7.2_Study_Guide p. 176

upvoted 4 times

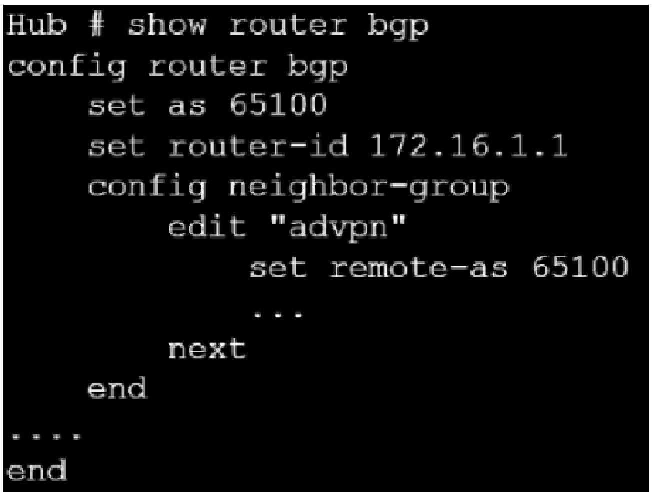
Question #30 Topic 1

Refer to the exhibit, which contains an ADVPN network diagram and a partial BGP configuration.

Network diagram -



Partial BGP configuration -



```
Hub # show router bgp
config router bgp
    set as 65100
    set router-id 172.16.1.1
    config neighbor-group
        edit "advpn"
            set remote-as 65100
            ...
        next
    end
....
end
```

Which two parameters should you configure in config neighbor-range? (Choose two.)

A. set neighbor-group advpn

B. set route-reflector-client enable

C. set prefix 10.1.0 255.255.254.0

D. set prefix 172.16.1.0 255.255.255.0

Suggested Answer: *AC*

Community vote distribution

AD (89%) 11%

ccie8122 8 months, 1 week ago

Selected Answer: AD

C is wrong because (a) to configure a network prefix to inject into the BGP table, you do this under "config network" not under "config neighbor-range" and (b) it is the wrong prefix anyway -- should be 10.1.0.0 255.255.255.0

upvoted 1 times

peterpanko 9 months, 2 weeks ago

Selected Answer: AC

in BGP it is needed to enable the networks to be advertised not interfaces like with OSPF.

upvoted 1 times

ccie8122 8 months, 1 week ago

yes, but the question does not ask what command injects LAN segment into the BGP table; it is asking what command to configure BGP neighbors that have a given range of next-hop IP addresses. Thus C is incorrect, but D is correct.

upvoted 2 times

Cyril_the_Squirl 1 year ago

In this question neighbour-group is already defined, the set route-reflector-client enable must also be defined in peer-group so that spoke to spoke networks can talk

upvoted 2 times

mecacig953 1 year ago

The question is what would you configure in the neighbour-range. AD are correct

upvoted 2 times

charruco 1 year, 2 months ago

Selected Answer: AD

A and D are correct

Study guide p. 338

upvoted 2 times

DaLoGo 1 year, 2 months ago

Study the Drawing on page 338 of the study guide. The question specifically asks for parameters in the neighbor-range. That would be Answer A and D

upvoted 1 times

truserud 1 year, 3 months ago

Selected Answer: AD

Correct answers are A & D. This is detailed on page 338 in the Study Guide.

upvoted 2 times

5deee77 1 year, 4 months ago

Selected Answer: AD

study guide 338

upvoted 1 times

Artbrut 1 year, 4 months ago

Selected Answer: AD

https://docs.fortinet.com/document/fortigate/6.4.4/cli-reference/557620/config-router-bgp

upvoted 2 times

MikeSco001 1 year, 4 months ago

Selected Answer: AD

Answer : A & D

upvoted 1 times

Question #31 *Topic 1*

You want to have faster detection for OSPF.
Which parameter should you enable on both connected FortiGate devices?

A. distribute-list-in

B. rfc1583-compatible

C. restart-on-topology-change

D. bfd

Suggested Answer: *D*

Community vote distribution

D (100%)

charruco 8 months, 1 week ago

D is correct
study guide p. 177

upvoted 1 times

truserud 9 months, 3 weeks ago

Selected Answer: D

Correct answer is D.

upvoted 2 times

5deee77 9 months, 4 weeks ago

Selected Answer: D

study guide p. 177

upvoted 2 times

Artbrut 10 months ago

Selected Answer: D

study guide p. 177

upvoted 3 times