Question #1 *Topic 1*

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

A. By default, all interfaces are part of the same broadcast domain.

B. The existing network IP schema must be changed when installing a transparent mode FortiGate in the network.

C. Static routes are required to allow traffic to the next hop.

D. FortiGate forwards frames without changing the MAC address.

Suggested Answer: *AD*
Reference:
https://kb.fortinet.com/kb/viewAttachment.do?attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

Community vote distribution

AD (100%)

g13lopez Highly Voted 2 years, 7 months ago
Hi Guys today I passed the exam NSE4_6.4 and 100% questions were here, but many answers were wrong so I advice to read the discussions because there are the real answers.
upvoted 5 times

Geraldino Most Recent 2 years, 6 months ago
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)
A. Warning
B. Exempt
C. Allow
D. Learn

I need some help here
upvoted 1 times

dudan 2 years, 5 months ago
A&C. (Fortigate_Security_7.0 page 379)
upvoted 1 times

lrosadini 2 years, 7 months ago
A FortiGate_Infrastructure_6.4 pag 166
D FortiGate_Infrastructure_6.4 pag 162
upvoted 1 times

vdmuhovskis 2 years, 8 months ago
Selected Answer: AD
A;D correct
upvoted 2 times

inculto 2 years, 10 months ago
Is correct A and D.
upvoted 4 times

deepakkalri 2 years, 11 months ago
A&D are correct
upvoted 2 times

Cunaworo 3 years ago
A&D OK
upvoted 2 times

armandolubaba 3 years, 1 month ago
A & D are correct answers

upvoted 3 times

FortiSherlock 3 years, 1 month ago

Indeed, A & D, just normal behaviour of an L2 device / Switch.

upvoted 3 times

Wachiturro 3 years, 1 month ago

Answer A&D are corrects!

FortiGate_Infrastructure_6.4 page 162

upvoted 4 times

KavinT 3 years, 2 months ago

A & D correct answer

upvoted 3 times

Question #2 *Topic 1*

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

A. Full Content inspection

B. Proxy-based inspection

C. Certificate inspection

D. Flow-based inspection

Suggested Answer: *D*

Community vote distribution

D (100%)

juvemerda Highly Voted 2 years, 5 months ago

I got this question on NSE4 7.0 exam yesterday but instead it asked me about Profile-based and it was a two answer question, with flow-based and proxy-based being the correct answer.

upvoted 8 times

Lionardo Highly Voted 3 years, 5 months ago

D is correct. FortiGate_Security_6.4 page 368

upvoted 7 times

atiles05 Most Recent 2 years ago

Selected Answer: D

Flow Based inspection mode, Correct Answer D, Page 368 Fortigate_Security_7.0(New Version!!)

---Español---

Modo de inspección basado en flujo, respuesta correcta D, página 368 Fortigate_Security_7.0 (¡nueva versión!)

upvoted 1 times

Misterio 2 years, 7 months ago

D is correct

upvoted 1 times

inculto 2 years, 10 months ago

D is correct.

upvoted 2 times

yadavarya97 3 years, 1 month ago

The default mode is flow based for the policies. NGFW mode does not change the inspection mode.

upvoted 4 times

armandolubaba 3 years, 1 month ago

D is correct

upvoted 1 times

KavinT 3 years, 2 months ago

D is correct

upvoted 1 times

MEDO162 3 years, 3 months ago

D is correct.

Flow -based inspection mode is the only applicable process available in policy-based NGFW mode.

FortiGate_Security_6.4 page 368

upvoted 3 times

testtaker59 3 years, 4 months ago

D is correct

upvoted 2 times

mahmoudlol 3 years, 4 months ago

D is correct

upvoted 2 times

jalojalo123124124124 3 years, 4 months ago

B. FortiGate_Security_6.4 page 368

upvoted 2 times

Ishan_Dis 3 years, 4 months ago

NGFW- Policy Base- Flow Base

Answer D

upvoted 2 times

Question #3 *Topic 1*

Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password.

B. FortiGate supports pre-shared key and signature as authentication methods.

C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.

D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Suggested Answer: *AB*

Reference:

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

Community vote distribution

AB (100%)

MunzerR Highly Voted 3 years, 5 months ago

A,B are correct

upvoted 10 times

Lionardo Highly Voted 3 years, 5 months ago

A & B correct. FortiGate_Infrastructure_6.4 page 224 for B and page 227 for A

upvoted 8 times

alpha520 Most Recent 2 years ago

A,B correct

upvoted 1 times

atiles05 2 years ago

Selected Answer: AB

The correct answers are: A,B

A = Fortigate_Infrastructure_7.0 page 218

B = Fortigate_Infrastructure_7.0 page 215

---Español---

Las respuestas correctas son: A,B

A = Fortigate_Infrastructure_7.0 página 218

B = Fortigate_Infrastructure_7.0 página 215

upvoted 1 times

NIGHTELF7 2 years, 9 months ago

A,B are correct.

upvoted 1 times

armandolubaba 3 years, 1 month ago

A & B are correct answers

upvoted 2 times

armandolubaba 3 years, 1 month ago

A & B are correct answer

upvoted 2 times

KavinT 3 years, 2 months ago

A & B are correct

upvoted 2 times

mahmoudlol 3 years, 4 months ago

A & B are correct

upvoted 4 times

Question #4 *Topic 1*

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

A. Heuristics scan

B. Trojan scan

C. Antivirus scan

D. Ransomware scan

Suggested Answer: *A*
Reference:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/927086/examples

Community vote distribution
A (100%)

mahmoudlol Highly Voted 3 years, 4 months ago
A is Correct
upvoted 8 times

Lionardo Highly Voted 3 years, 5 months ago
A correct. FortiGate_Security_6.4 page 470
upvoted 6 times

yasirmohy Most Recent 1 year, 6 months ago
The Trojan scan is a scanning technique on FortiGate that can only be enabled through the CLI (Command Line Interface). This scan is specifically designed to detect and remove Trojan horses, which are malicious software that appears to be harmless but actually opens a backdoor for attackers to access and control the system.
Chatgpt
upvoted 1 times

yasirmohy 1 year, 6 months ago
The statement "The Heuristics Scan is enabled by default and can be adjusted through the FortiGate's GUI or CLI" is applicable to both FortiOS 6.4 and 7.0, as the Heuristic Scan feature is a part of FortiGate's antivirus capabilities and is available in both versions. However, it's worth noting that the specific steps to adjust the sensitivity of the scan may vary slightly between the two versions.
ChatGpt answered me with confidante
upvoted 1 times

atiles05 2 years ago
Selected Answer: A
A is correct, but Heuristics scan theory is not present in the Fortigate_Security_7.0. Take note of that, this is only present in 6.4 and older versions study guides.
upvoted 1 times

An0nym0us2 2 years, 2 months ago
For FortiOS 7.0 the answer is Machine learning (AI) scan instead of Heuristics.
See FortiGate Security 7.0 page 476
upvoted 5 times

FaridKamaruddin 2 years, 1 month ago
I just took the exam and yes they replaced it with Machine learning scan
upvoted 3 times

NIGHTELF7 2 years, 9 months ago
A is correct.
upvoted 1 times

inculto 2 years, 10 months ago
A is correct
upvoted 1 times

armandolubaba 3 years, 1 month ago

A is correct

upvoted 1 times

Wachiturro 3 years, 1 month ago

Option A is correct. FortiGate_Security_6.4 page 470

upvoted 1 times

armandolubaba 3 years, 1 month ago

A is correct answer

upvoted 1 times

jalojalo123124124124 3 years, 4 months ago

A is correct. FortiGate_Security_6.4 page 468

upvoted 4 times

Xillar 3 years, 5 months ago

A is correct

upvoted 2 times

Question #5 *Topic 1*

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

A. Firewall policy

B. Policy rule

C. Security policy

D. SSL inspection and authentication policy

Suggested Answer: *AB*
Reference:
https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode

Community vote distribution
CD (100%)

Lionardo Highly Voted 3 years, 5 months ago
C & D correct. FortiGate_Security_6.4 page 369
"NGFW policy based mode, you must configure a few policies to allow traffic:
SSL inspection & Authentication, Security policy"
upvoted 29 times

mahmoudlol Highly Voted 3 years, 4 months ago
C&D
Security policies work with SSL Inspection & Authentication policies to inspect traffic. To allow traffic from a specific user or user group, both Security and SSL Inspection & Authentication policies must be configured.
https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/978598/profile-based-ngfw-vs-policy-based-ngfw
upvoted 14 times

Ibrahimadwan Most Recent 1 year, 3 months ago
C& D is correct
upvoted 1 times

atiles05 2 years ago
Selected Answer: CD
C & D are the correct answers by Fortigate_Security_7.0(New Version) page 369. If you are using Policy Based Mode, SSL Inspection & Authentication (consolidated) and Security Policy are required to allow traffic.
upvoted 2 times

CalH 2 years, 5 months ago
C & D is correct. Ref: FortiGate_Security_7.0_Study_guide Page 369
upvoted 1 times

gboy91 2 years, 5 months ago
C and D
upvoted 1 times

downlife 2 years, 6 months ago
Selected Answer: CD
C & D is correct
upvoted 1 times

malikgen 2 years, 6 months ago
Selected Answer: CD
Security policies work with SSL Inspection & Authentication policies to inspect traffic. To allow traffic from a specific user or user group, both Security and SSL Inspection & Authentication policies must be configured. A default SSL Inspection & Authentication policy with the certificate-inspection SSL Inspection profile is preconfigured. Traffic will match the SSL Inspection & Authentication policy first. If the traffic is allowed, packets are sent to the IPS engine for application, URL category, user, and user group match, and then, if enabled, UTM inspection (antivirus, IPS, DLP, and email filter) is performed.

upvoted 1 times

lrosadini 2 years, 7 months ago

C&D - FortiGate Security 6.4 Study Guide Pag 369

upvoted 1 times

AbdiAden 2 years, 7 months ago

A and B are correct. C is incorrect. Security policy has no sense. It's Security Profile.

D is incorrect. SSL inspection and authentication policy are not mandatory. They are optional.

Maybe.

upvoted 1 times

platontw 2 years, 8 months ago

Selected Answer: CD

C & D are the correct answers.

upvoted 2 times

blvackhammer 2 years, 8 months ago

Selected Answer: CD

C & D is correct

upvoted 1 times

kkched 2 years, 8 months ago

Selected Answer: CD

C&D are Corrects

upvoted 1 times

MrSaintz 2 years, 9 months ago

Selected Answer: CD

Exactly as Lionardo explained, it's in the Study Guide, very explicitly! So just an innocent question though, you hope we pay for custom view, and still apply no effort in correcting the answers, where is the value in that???

upvoted 2 times

NIGHTELF7 2 years, 9 months ago

C & D

https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/978598

upvoted 1 times

mrtim5700 2 years, 9 months ago

Agree with C&D

upvoted 1 times

stampaprints 2 years, 9 months ago

Obviously, C&D are correct 100%

upvoted 1 times

Question #6 *Topic 1*

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.
What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Suggested Answer: *C*
Reference:
https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting

Community vote distribution
C (100%)

onaicul Highly Voted 3 years, 3 months ago
C is Correct First warnig 75%, second 90% and final Warning 95%
upvoted 14 times

Lionardo Highly Voted 3 years, 5 months ago
C correct. FortiGate_Security_6.4 page 270
upvoted 6 times

atiles05 Most Recent 2 years ago
Selected Answer: C
C is correct due to:
Page 278 Fortigate Security 7.0(New Version!!), only 75% of the disk is available to store logs, this is distributed in the existing vdoms.

diagnose sys logdisk usage -- CLI command to verify this
upvoted 1 times

mob9 2 years, 1 month ago
Selected Answer: C
C is correct
Ref:
https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting
upvoted 1 times

sull3y 2 years, 2 months ago
You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.
upvoted 1 times

gboy91 2 years, 5 months ago
Selected Answer: C
Correct
upvoted 1 times

Havij 2 years, 8 months ago
C is correct. "The system reserves approximately 25% of its disk space for system usage and unexpected quota overflow."
upvoted 1 times

ambaraya 2 years, 8 months ago
C is correct
upvoted 1 times

alexilc 2 years, 10 months ago

It`s A because overwrite in 95% only warning in 75%

upvoted 3 times

forti_Ctes 2 years, 11 months ago

C are correct

upvoted 1 times

msn20 2 years, 12 months ago

C is correct

upvoted 3 times

armandolubaba 3 years, 1 month ago

C is correct

upvoted 1 times

mahmoudlol 3 years, 4 months ago

C is correct

upvoted 2 times

dbartowski 3 years, 4 months ago

C is correct

upvoted 2 times

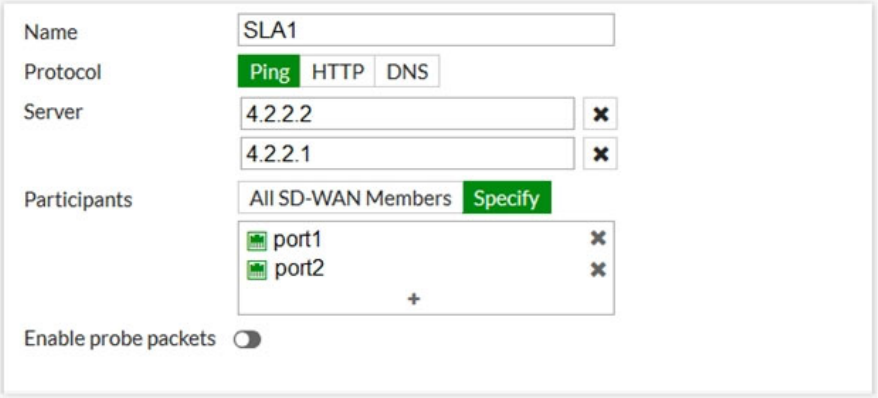
Xillar 3 years, 5 months ago

C is correct

upvoted 2 times

Question #7 *Topic 1*

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



An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic.
Why is FortiGate not generating any traffic for the performance SLA?

A. There may not be a static route to route the performance SLA traffic.

B. You need to turn on the Enable probe packets switch.

C. The Ping protocol is not supported for the public servers that are configured.

D. Participants configured are not SD-WAN members.

Suggested Answer: *B*
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-link-monitoring

Community vote distribution
B (100%)

atidd Highly Voted 3 years, 5 months ago
A is not the answer because the pings work without static route.
C is wrong
D is wrong because you can't add non SD-WAN members to SLA policy.
upvoted 11 times

onaicul Highly Voted 3 years, 3 months ago
B is correct FortiGate_Infrastructure_6.4 page 79
upvoted 7 times

atiles05 Most Recent 2 years ago
Selected Answer: B
Correct Answer is: B,
FortiGate will stop sending out probe packets when the "enabled probe packets" option is disabled. This is also called, Active Detection Mode is SLA performance. Page 81, Fortigate Infrastructure 7.0 (New Version!!)
upvoted 2 times

gboy91 2 years, 5 months ago
Selected Answer: B
correct
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: B
B é verdadeira
upvoted 1 times

lrosadini 2 years, 7 months ago
B - FortiGate_Infrastructure_6.4 page 79
probe-packets:

It’s how the FortiGate determines the target is alive. In this case the FortiGate will ping those IPs from both interfaces.

upvoted 2 times

armandolubaba 3 years, 1 month ago

B is correct answer

upvoted 2 times

yemicontrol 3 years, 1 month ago

B is the right answer.

https://docs.fortinet.com/document/fortigate/6.4.6/administration-guide/580649/link-health-monitor

upvoted 2 times

mahmoudlol 3 years, 4 months ago

B is the right answer

upvoted 2 times

Djohan23 3 years, 4 months ago

You can find the answer on Performance SLA-Link Health Monitor.

B is Correct.

upvoted 2 times

Question #8 *Topic 1*

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, which statement about VLAN IDs is true?

A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.

B. The two VLAN subinterfaces must have different VLAN IDs.

C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.

D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Suggested Answer: *B*

Community vote distribution

B (83%) A (17%)

TJBIII Highly Voted 3 years ago
Pretty positive this would be B. You cannot have the same VLAN ID on the same sub interface or there would be conflicts.
upvoted 9 times

only4u Most Recent 1 year, 2 months ago
Answer A is only correct if we use different hardware interfaces in different VDOMs.

Same VLAN ID, different VDOMs, same hardware interface - not valid.
Same VLAN ID, different VDOMs, different hardware interfaces - valid
upvoted 1 times

jarz 1 year, 3 months ago
Selected Answer: B
For this question the answer is B.
upvoted 1 times

DiscorD_RIP 1 year, 3 months ago
Answer is: A and B
Why A is right, you can see here: https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-emac-vlan-to-share-the-same-VLAN/ta-p/192843?externalID=FD43883
upvoted 1 times

iseeusee 1 year, 11 months ago
Selected Answer: B
think it as sub-interface in router..
upvoted 1 times

atiles05 2 years ago
Selected Answer: A
I'm totally sure that answer is B, but if we talk about "VDOMS" each VDOM is a different "VFR" that means, you can have in the same physical interface, multiples vlans, with the same VLAN ID, but.. in different VDOM's vlan30 -> vdom root , vlan40 -> vdom user, both interfaces on the same port1 physical interface.

If multi vdoms in multi vlans under 1 interface scheme-> A is also a Correct Answer.

Reference: Page 156, Fortigate Infrastructure 7.0 new version!
upvoted 1 times

Shieshalom 2 years, 5 months ago
Answer is B: Fortifgate_Infratructure 6.4 Pg 154
upvoted 1 times

gboy91 2 years, 5 months ago
Selected Answer: B

correct
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: B
B é verdadeira
upvoted 1 times

Elric_ 2 years, 7 months ago
Selected Answer: B
Between B and A but i think B.
upvoted 1 times

8anii 2 years, 7 months ago
I think that A is correct logically and B for sure
upvoted 1 times

lrosadini 2 years, 7 months ago
B - The same VLAN number cannot be configured twice on the same physical interface
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interface/ta-p/197640
upvoted 1 times

Expressif 2 years, 8 months ago
Why not A ?
upvoted 1 times

MetDaci 2 years, 5 months ago
Because one physical interface can belong to only one VDOM.
upvoted 6 times

lregu82 1 year, 11 months ago
I understand that it is because you can assign interfaces to different vdoms, but not to the subinterfaces, if you have a physical interface assigned to the VDOM Root for example, all the subinterfaces also belong to that vdom
upvoted 1 times

Onurcan91 2 years, 8 months ago
B without hesitation.
upvoted 1 times

forti_Ctes 2 years, 11 months ago
B are correct
upvoted 3 times

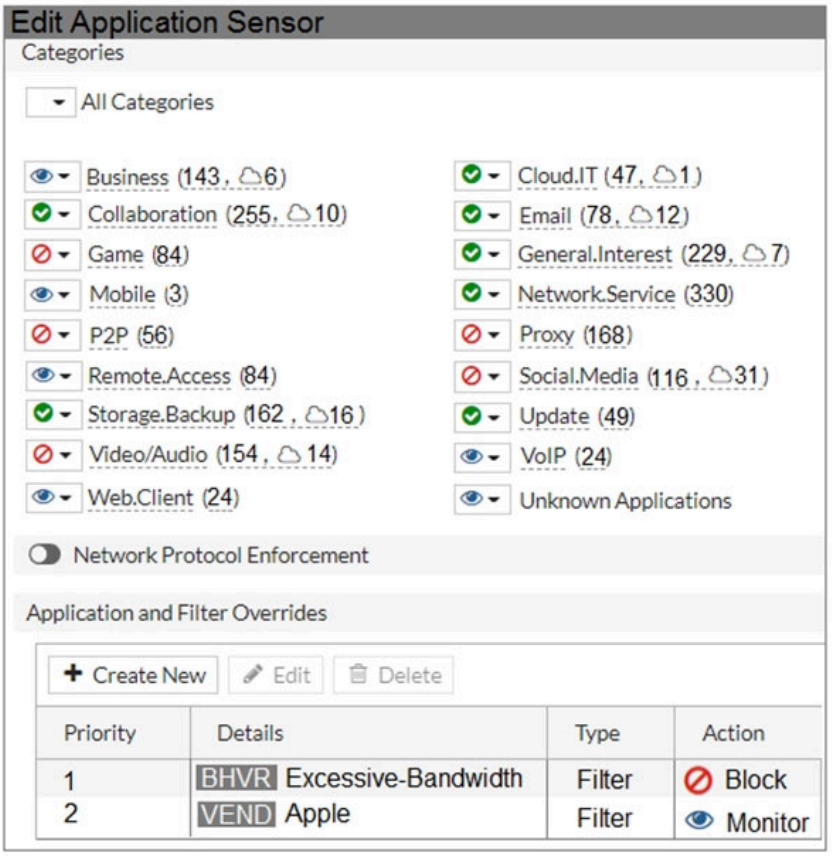
viestner 3 years ago
B. “Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID”
upvoted 4 times

ferreirajec 3 years ago
A & B are the correct I guess
upvoted 1 times

ferreirajec 3 years ago
only B
upvoted 3 times

Question #9 *Topic 1*

Refer to the exhibit to view the application control profile.



Users who use Apple FaceTime video conferences are unable to set up meetings.
In this scenario, which statement is true?

A. Apple FaceTime belongs to the custom monitored filter.

B. The category of Apple FaceTime is being monitored.

C. Apple FaceTime belongs to the custom blocked filter.

D. The category of Apple FaceTime is being blocked.

Suggested Answer: *A*

Community vote distribution

C (100%)

Lionardo Highly Voted 3 years, 5 months ago

C correct.
FaceTime categorized (filtered) under "Excessive-Bandwidth" and custom filter override set to block this.
Also we know that users can't use FaceTime
upvoted 17 times

RHK0783 3 years ago

In version 6.4, facetime falls under VoIP category. There is no application category of excessive bandwidth.
upvoted 2 times

RHK0783 3 years ago

My bad. Behavioral category is set to block by custom Filter.
C is the right answer ...
upvoted 1 times

Xillar Highly Voted 3 years, 5 months ago

I would say answer C is the correct one. This because the "Excessive-Bandwith" is under the filters section
upvoted 5 times

aslamzohaib Most Recent 1 year, 10 months ago

Selected Answer: C

c is the correct answer because video/audio is blocked

upvoted 1 times

atiles05 2 years ago

Correct C, Page 445 Fortigate Security 7.0

Fortigate will block excessive bandwidth apps like FaceTime VOIP regardless that the categories blocked.

upvoted 1 times

ibos8383 2 years, 5 months ago

it is c

upvoted 1 times

gboy91 2 years, 5 months ago

Selected Answer: C

Correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: C

C é a verdadeira

upvoted 1 times

Wachiturro 2 years, 6 months ago

FaceTime is related to: Behavior Excessive-Bandwidth

https://www.fortiguard.com/appcontrol/24426

upvoted 2 times

dbramix 2 years, 6 months ago

Selected Answer: C

it is the only answare with blocked action

upvoted 2 times

malikgen 2 years, 6 months ago

Selected Answer: C

C is the answer ..

upvoted 1 times

blahblah1234567890000 2 years, 7 months ago

Selected Answer: C

Answer is c

upvoted 1 times

jpinan11 2 years, 8 months ago

C is correct

upvoted 1 times

platontw 2 years, 8 months ago

C. Is the Correct answer.

upvoted 1 times

MrSaintz 2 years, 9 months ago

Selected Answer: C

C is correct, Excessive Bandwidth is the custom filter and override set to block, not monitor.

upvoted 2 times

mrtim5700 2 years, 9 months ago

Agree with C. FaceTime is falling under the "Excessive Bandwidth" category. The custom filters are processed top down and is hit before hitting the Vendor filter;.

upvoted 1 times

Rman0059 2 years, 9 months ago

Selected Answer: C

C is correct

upvoted 3 times

forti_Ctes 2 years, 11 months ago

C are correct

upvoted 1 times

Question #10 *Topic 1*

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

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.

B. FortiGate automatically negotiates a new security association after the existing security association expires.

C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.

D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Suggested Answer: *B*
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=12069

Community vote distribution
D (69%) B (31%)

Lionardo Highly Voted 3 years, 5 months ago
D is correct. FortiGate_Infrastructure_6.4 page 231
"Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic.
upvoted 32 times

RVE 2 years, 11 months ago
The right answer is D, this is why:
Page 230 FortiGate Infrastructure 6.4 Study Guide

Auto-negotiate. When you do this, Fortigate not only
negotiates new SAs before the current SAs expire, but it
also start using the new SAs right away. The latter prevents
traffic disruption by IPsec SA renegotiation.

On Answer B "FortiGate automatically negotiates a new security association after the existing security association expires." they claim that negotiation happens after SAs expires and not before as is written on FortiGate Infrastructure 6.4 Study Guide page 230.

Also on the same page they say:

Another benefit of enabling Auto-negotiate is that the tunnel comes
up and stays up automatically, even when there is not interesting traffic.

Which makes me think that the right answer is D.
upvoted 10 times

Thanos84 2 years, 11 months ago
https://kb.fortinet.com/kb/documentLink.do?externalID=12069
check this ;;its B
upvoted 3 times

nimvoltage 2 years, 11 months ago
D should be correct.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/156465/configuring-phase-2-parameters

They ask the effect, this ultimately takes the tunnel up.
upvoted 2 times

Seph1 3 years ago
"Another benefit", not an "effect".
Enabling Auto-negotiate will enable Auto-Keep Alive and as a benefit, the tunnel comes up and stays up.

The effect is: SA negotiation when it expires.
The answer is B.
upvoted 4 times

2021gene 3 years ago
I think its D too, because Infra 6.4 p231 also states that the equipment negotiates new SA BEFORE the current SA expires.
upvoted 2 times

Shieshalom 2 years, 5 months ago
The catch is "When the existing SA expires" The auto-negotiate negotiates for SA even before the existing SA expires. Fortigate Infrastructure page 231. The correct answer is D
upvoted 1 times

Cyril_the_Squirl Highly Voted 3 years, 5 months ago
B. Life-span of SA is often shorter than the data tranfer session, as a result multiple Phase2 SAs are negotiated. When there's zero data transfer, Phase 2 SA doesn't get negotiated and existing one expires, bringing the tunnel down. When data transfer resumes, first the peers negotiate a new SA. In short Phase 1 is to authenticate and protect Peering, Phase 2 is for data Transfer.
upvoted 13 times

redSTORM Most Recent 1 year, 4 months ago
Selected Answer: B
• B. FortiGate automatically negotiates a new security association after the existing security association expires
upvoted 1 times

Garry_G 1 year, 5 months ago
According to the referenced KB article, it would have to be B ...
upvoted 1 times

sintesinet 1 year, 12 months ago
Selected Answer: B
B is the correct answer. you are all confusing auto-keepalive with auto-negotiate
upvoted 1 times

atiles05 2 years ago
B and D are both correct, Fortigate Infrastructure page 222 7.0
upvoted 1 times

Directly_Connected 2 years ago
The Answer is B.
The key point in the question is "auto-negotiate"
Auto-negotiate: Enable the option to automatically renegotiate the tunnel when the tunnel expires.
By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established.

Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-IPSec-auto-negotiate-and-keepalive/ta-p/189536?externalID=12069
upvoted 3 times

Abdulazizas96 2 years, 4 months ago
I think C is very generic, IPsec tunnel consist of 2 phases and 2 SA. Yes it brings the tunnel up but this is happening because it is auto negotiating the 2nd SA if there's no traffic passing through the tunnel and the 2nd is expired. So I stick with B.
upvoted 1 times

ibos8383 2 years, 5 months ago
It is D
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: D
Acredito que a questão está deixando margem a dúvidas e, neste sentido, a mais correta é a D. Na B tem documentação informando que é depois de expirado o SA, já outra cita que antes de expirar o SA faz a negociação. Na D, fiz um teste usando dois FortiGate-VM sem hosts atrás (ou seja, sem tráfego), interligado através de um router. Ao desconectar a interface do router, após aproximadamente 60 segundos o túnel cai. Conectando novamente a interface o túnel não sobe (lembrem que não tem hosts atrás

dos FGT gerando tráfego). Ao habilitar Auto-negotiate, quando reconecto a interface do router o túnel sobe. Isso levar ao texto da letra D, por tanto neste cenário duvidoso me parece a mais certa.
upvoted 1 times

python_tamer 2 years, 6 months ago

Selected Answer: B

I believe the answer is B:
https://docs.fortinet.com/document/fortigate/7.0.5/administration-guide/604285/phase-2-configuration#auto
By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established. Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.

If the tunnel goes down, the auto-negotiate feature (when enabled) attempts to re-establish the tunnel. Auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.

Automatically establishing the SA can be important for a dialup peer. It ensures that the VPN tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the VPN tunnel does not exist until the dialup peer initiates traffic.
upvoted 2 times

lrosadini 2 years, 7 months ago

B - https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-the-IPSec-auto-negotiate-and-keepalive/ta-p/189536
If the tunnel goes down, the auto-negotiate feature (when enabled) attempts to re-establish the tunnel.
Auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.
upvoted 2 times

blahblah1234567890000 2 years, 7 months ago

Selected Answer: D

Answer is D
upvoted 2 times

kkched 2 years, 8 months ago

Selected Answer: D

D correct
upvoted 2 times

acaselli 2 years, 9 months ago

Selected Answer: D

D is correct
upvoted 2 times

Rman0059 2 years, 9 months ago

Selected Answer: D

D is correct
upvoted 2 times

morningstar 2 years, 10 months ago

It is B.

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

Auto-negotiate.
By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. --> This means that when the IPSEC SA expires, the phase2 remains down "UNTIL" new interesting traffic triggers the negotiation for new IPSEC SA.

But, if you enable "Auto-negotiate", as soon as the IPSEC SA expires, the "Auto-negotiate" feature will negotiate new one and start using it. So, this process will bring up the tunnel again, even if there is no interesting traffic.
upvoted 3 times

Question #11 *Topic 1*

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

A. Web filter in flow-based inspection

B. Antivirus in flow-based inspection

C. DNS filter

D. Web application firewall

E. Application control

Suggested Answer: *ACE*

Community vote distribution

ABE (100%)

Lionardo Highly Voted 3 years, 5 months ago
A, B & E is correct. FortiGate_Security_6.4 page 520
upvoted 24 times

ScottXYZ 2 years, 9 months ago
I was wondering where can I find this book Fortigate Security 6.4
upvoted 3 times

lrosadini 2 years, 7 months ago
You can buy it on Evantage website. It's the official study guide
upvoted 2 times

jonboy22 2 years, 1 month ago
You can sign up for a free Scribd account and get the 7.0 PDF for download
upvoted 2 times

Xillar Highly Voted 3 years, 5 months ago
ABE, Web Application Firewall is for ingress
upvoted 9 times

Eist Most Recent 11 months, 2 weeks ago
Application control
Anti-virus (flow-based)
Web filter (flow-based)
Email filter (flow-based)

Fortigate_Security_7.2 p.385
upvoted 1 times

hkhan049 1 year, 9 months ago
Yes, the studyguide mentions A, B, E, but DNS Filter (Answer C) seems also to be correct:

"Starting in 7.0, the IPS engine handles the DNS filter in flow mode policies and queries the FortiGuard web filter server for FortiGuard categories. "

https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow-mode
upvoted 1 times

atiles05 2 years ago
Selected Answer: ABE
Fortigate 7.0 new version, A,B,E Correct Answers page 525 Security.
upvoted 1 times

mob9 2 years, 1 month ago

In fortigate 7.0.5 its totally different
answer would be "Application control & web filter"

Other NGFW policy-based mode options
You can combine Application Control and Web Filter in the same NGFW mode policy.
The following security profiles can be used in NGFW policy-based mode:
l AntiVirus
l Web Filter
l Intrusion Prevention
l File Filter
l Email Filter
Logging can also be enabled in security policies.

FortiOS 7.0.5 Administration Guide p:679
upvoted 2 times

NicolaeEast 2 years ago
The question isn't asking about policy based though.

It asks what uses the IPS system. And that is:
Application control
Anti-virus (flow-based)
Web filter (flow-based)
Email filter (flow-based)
Data leak prevention (flow-based in one armed sniffer mode)

Fortigate 7.0 Security pg 525
upvoted 3 times

damian1111111 1 year, 11 months ago
this is incomplete too, starting in 7.0 DNS filter in Flow mode should be there too.

https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow-mode
upvoted 1 times

gboy91 2 years, 5 months ago
Selected Answer: ABE
correct
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: ABE
A, B e E são verdadeiras
upvoted 1 times

platontw 2 years, 8 months ago
A, B, E is the Correct Answer
upvoted 2 times

MrSaintz 2 years, 9 months ago
Selected Answer: ABE
A,B & E are correct
upvoted 2 times

[Removed] 2 years, 9 months ago
Selected Answer: ABE
A,B,E
FortiGate_Security_6.4_Study_Guide-Online.pdf page 520
upvoted 1 times

blabla4 2 years, 9 months ago
IPS ENGINE [APP CONTROL,AV FLOW-B,WEB FILTER FLOW-B, EMAIL FILTER FLOW-B, DLP FLOW-B] ...
ABE

upvoted 1 times

mrtim5700 2 years, 9 months ago

A,B & E. DNS filter does not rely on IPS engine.

upvoted 1 times

stampaprints 2 years, 9 months ago

A,B,E is correct

upvoted 1 times

Rman0059 2 years, 9 months ago

Selected Answer: ABE

Abe is correct answers

upvoted 1 times

[Removed] 2 years, 9 months ago

Selected Answer: ABE

Fortigate Security 7.0 Page 520

upvoted 1 times

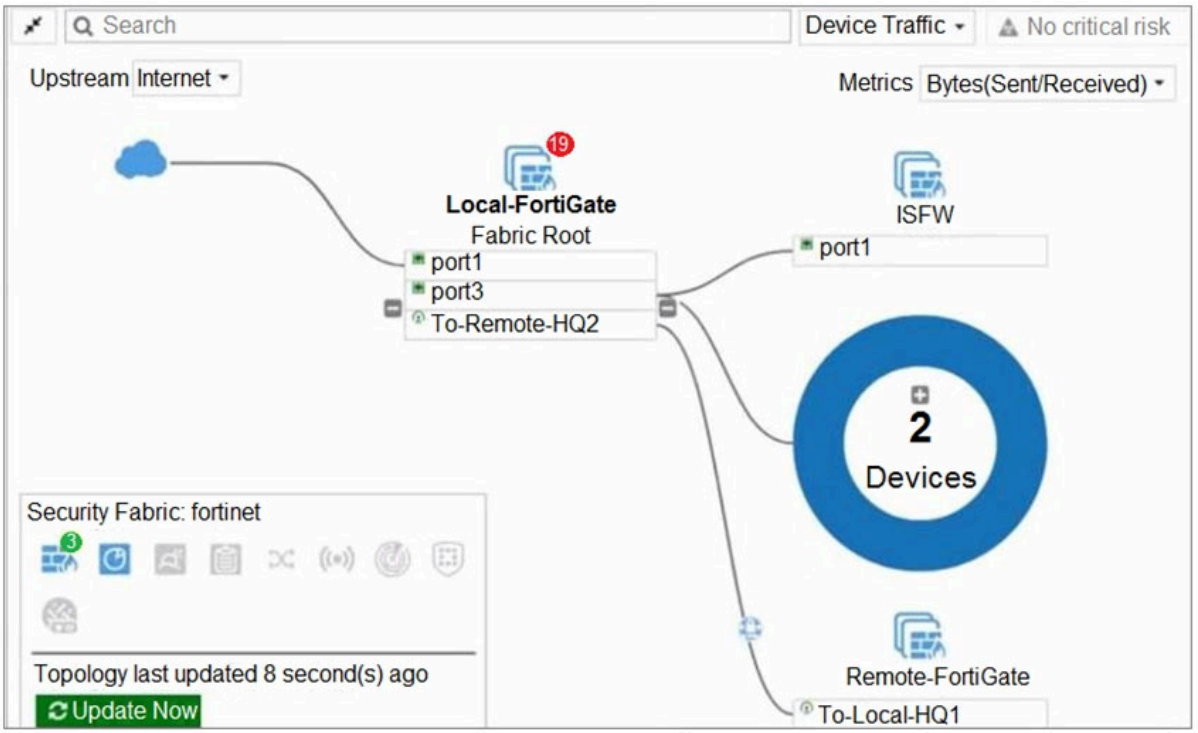
RHK0783 3 years ago

ABE are the right answers

upvoted 2 times

Question #12 *Topic 1*

Refer to the exhibit.



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

A. There are five devices that are part of the security fabric.

B. Device detection is disabled on all FortiGate devices.

C. This security fabric topology is a logical topology view.

D. There are 19 security recommendations for the security fabric.

Suggested Answer: *BC*

Community vote distribution

CD (100%)

atidd Highly Voted 3 years, 5 months ago

C and D are correct. device detection is obviously on. And that red 19 indicates security rating recommendations.

upvoted 20 times

kvn5494 Highly Voted 3 years, 4 months ago

C & D are correct, for sure 100%.

I checked on real device, Fortigate 60E, version 6.4

upvoted 11 times

Power_Shell Most Recent 2 years ago

Selected Answer: CD

I think this is

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: CD

C e D são verdadeiras, checado em laboratório

upvoted 2 times

Eduardo2022 2 years, 7 months ago

new question about Security Fabric, please help

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Shut down/reboot a downstream FortiGate device.
B. Disable FortiAnalyzer logging for a downstream FortiGate device. C. Log in to a downstream FortiSwitch device.
D. Ban or unban compromised hosts.
upvoted 6 times

blues20 2 years, 6 months ago
C and D, Page 90 of Fortigate Security 6.4
upvoted 1 times

princelionelnzi 1 year, 6 months ago
The two actions that can be performed only from the root FortiGate in a Security Fabric are:

A. Shut down/reboot a downstream FortiGate device.
D. Ban or unban compromised hosts.

Explanation:

A. Shutting down/rebooting a downstream FortiGate device can only be performed from the root FortiGate in a Security Fabric. The root FortiGate has control over all the devices in the Security Fabric, and can perform actions on them as needed.

D. Banning or unbanning compromised hosts can also only be performed from the root FortiGate in a Security Fabric. The root FortiGate is responsible for monitoring the Security Fabric and detecting compromised hosts. When a host is detected as compromised, the root FortiGate can ban it from the network to prevent further damage. Similarly, the root FortiGate can unban a previously banned host once it has been cleaned and is no longer a threat.
upvoted 1 times

MrSaintz 2 years, 9 months ago
Selected Answer: CD
C - Logical Topology, vs Phisical Topology shows interface connected to devices;
D - 19 indicates security rating recommendations
Device detection is on at least in root FG.
upvoted 3 times

Eduardo2022 2 years, 7 months ago
Exactly, logical topology show network interfaces.
upvoted 1 times

acaselli 2 years, 9 months ago
Selected Answer: CD
C&D are correct
upvoted 1 times

mrtim5700 2 years, 9 months ago
Selected Answer: CD
C & D are correct.
A is incorrect, connected devices are not part of the fabric.
B is incorrect, we have not expanded the device to see whether or not the devices are identified.
C is correct, logical view shows the interfaces
D is correct, there are 19 recommendations
upvoted 3 times

blabla4 2 years, 9 months ago
A C ... THERE ARE 3 FGT AND 2+ MORE DEVICES
TOPOLGY IS LOGICAL
upvoted 1 times

Rman0059 2 years, 9 months ago
Selected Answer: CD
CD are correct
upvoted 1 times

bhaddar 2 years, 11 months ago
C&D options are rights from the given ..

upvoted 1 times

vagedis 3 years ago

C+D is correct. This IS a logical topology view and there are 19 security recommendations.

upvoted 2 times

Akoladet 3 years ago

correct answer is C and D

upvoted 1 times

yadavarya97 3 years, 1 month ago

Only D is correct , but may be its typo . the other answer can be C if its a typo as this is a physical topology not logical

upvoted 2 times

besik 2 years, 10 months ago

This is not physical topology because only on logical topology u can see the port number.

https://docs.fortinet.com/document/fortimanager/6.2.1/administration-guide/446043/logical-topology

upvoted 1 times

armandolubaba 3 years, 1 month ago

C & D are correct answers

upvoted 1 times

mahmoudlol 3 years, 4 months ago

C & D are correct

upvoted 3 times

Djohan23 3 years, 4 months ago

C & D is the correct answer.

Logical view shown information about the interfaces that each devices.

And notification indicates about the security rating recommendations.

upvoted 3 times

Question #13 *Topic 1*

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter

B. Static URL filter, FortiGuard category filter, and advanced filters

C. Static domain filter, SSL inspection filter, and external connectors filters

D. FortiGuard category filter and rating filter

Suggested Answer: *B*

Community vote distribution

B (71%) A (29%)

Tiagopfelix Highly Voted 3 years, 5 months ago

it's B.

FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 18 times

MEDO162 Highly Voted 3 years, 3 months ago

it's B.

FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 6 times

forpsmpurpose Most Recent 9 months, 1 week ago

page 413 boys and girls

upvoted 1 times

BADEDD 2 years, 3 months ago

Selected Answer: B

it's B.

FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 1 times

gboy91 2 years, 5 months ago

Selected Answer: B

correct page 413

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: B

B é verdadeira

upvoted 1 times

downlife 2 years, 6 months ago

Selected Answer: B

It is answer B

upvoted 2 times

ticorcr 2 years, 7 months ago

FortiGate_Security_ 6.4 page 412

upvoted 1 times

blahblah1234567890000 2 years, 7 months ago

Selected Answer: B

Answer is b

upvoted 1 times

zequel 2 years, 8 months ago

Selected Answer: B

It's B. FortiGate_Security_7.0_Study_Guide-Online.pdf page 414 shows the HTTP Inspection Order (Static URL Filter -> FortiGuard Category Filter -> Advanced Filters)

upvoted 2 times

Stitch2020 2 years, 8 months ago

Selected Answer: B

It's B, as others have stated: FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 1 times

Stitch2020 2 years, 8 months ago

Selected Answer: B

It's B

upvoted 1 times

NIGHTELF7 2 years, 9 months ago

Selected Answer: A

it's B.

FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 4 times

DavidC91 2 years, 11 months ago

it's B.

FortiGate_Security_ 6.4 - Guide study page 413.

upvoted 2 times

armandolubaba 3 years, 1 month ago

B is correct

upvoted 3 times

BarCat 3 years, 4 months ago

B is the right one.

upvoted 4 times

GeorgeFortiGate 3 years, 4 months ago

B i would say

upvoted 4 times

Question #14 *Topic 1*

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

A. Log ID

B. Universally Unique Identifier

C. Policy ID

D. Sequence ID

Suggested Answer: *B*

Reference:

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

Community vote distribution

B (100%)

Tiagopfelix Highly Voted 3 years, 5 months ago

B

FortiGate Security 6.4 Study Guide page 116

upvoted 11 times

FeNadege Highly Voted 3 years, 5 months ago

B it is Correct: "Universally Unique Identifier (UUID) attributes have been added to policies to improve functionality when working with FortiManager or FortiAnalyzer units"

upvoted 11 times

BADEDD Most Recent 2 years, 3 months ago

Selected Answer: B

The B, please look the FortiGate Security 6.4 Study Guide on page 116

upvoted 1 times

maxhoman 2 years, 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

maxhoman 2 years, 4 months ago

B,

FortiGate Security 7.0 Study Guide page 125

upvoted 1 times

gboy91 2 years, 5 months ago

Selected Answer: B

correct. UUID. Study Guide FGS 6.4 page 115

upvoted 1 times

Wachiturro 2 years, 6 months ago

The B, please look the FortiGate Security 6.4 Study Guide on page 116 UUID

upvoted 1 times

DavidC91 2 years, 11 months ago

B is correct

upvoted 1 times

msn20 2 years, 12 months ago

B is correct

upvoted 1 times

armandolubaba 3 years, 1 month ago

B is correct

upvoted 2 times

yemicontrol 3 years, 1 month ago

B is the answer

Universally Unique Identifier (UUID) attributes have been added to policies to improve functionality when working with FortiManager or FortiAnalyzer units.

upvoted 1 times

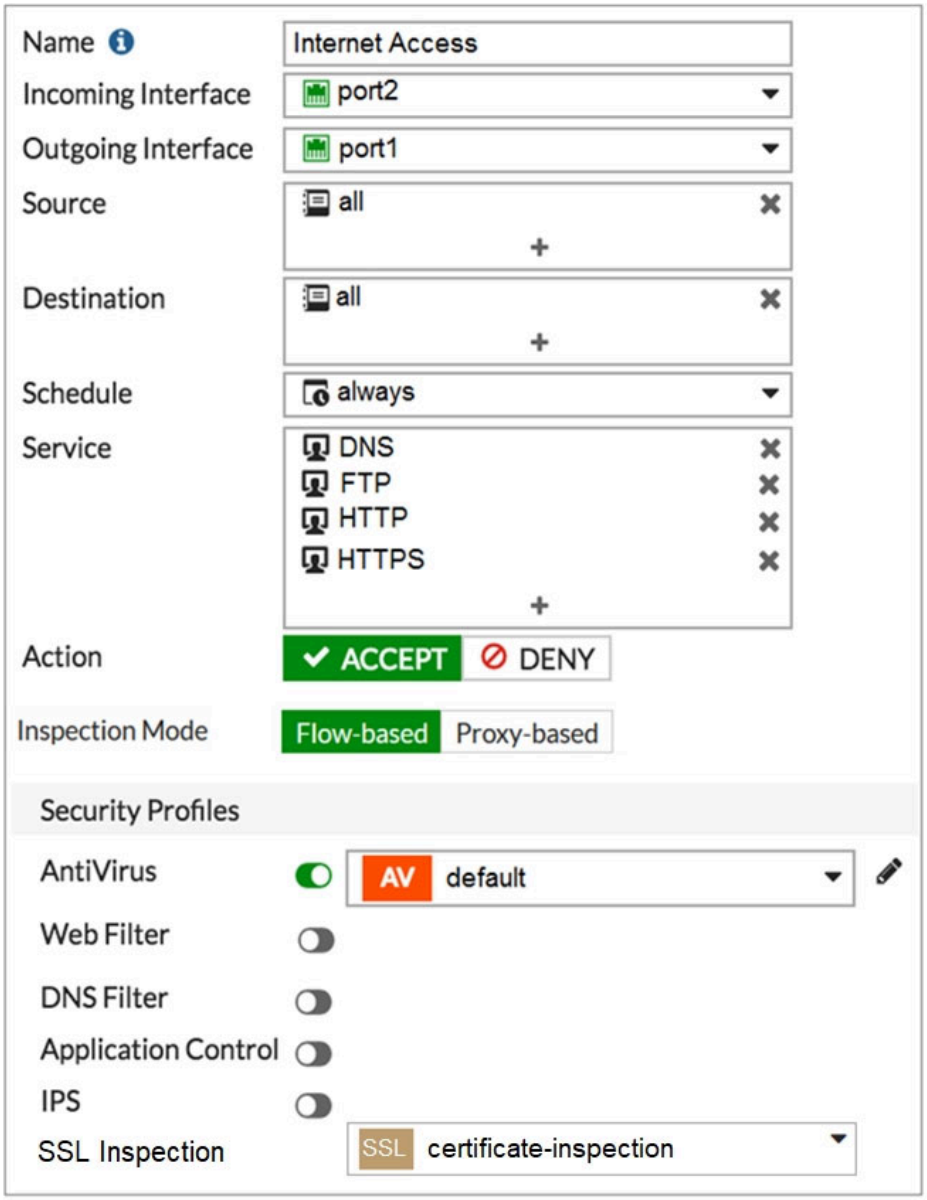
amirrr 3 years, 3 months ago

FortiGate Security 6.4 Study Guide page 116 UUID

upvoted 3 times

Question #15 *Topic 1*

Refer to the exhibit to view the firewall policy.



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

A. The firewall policy does not apply deep content inspection.

B. The firewall policy must be configured in proxy-based inspection mode.

C. The action on the firewall policy must be set to deny.

D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Suggested Answer: *D*

Community vote distribution

A (92%) 8%

vagedis Highly Voted 3 years ago

Definately A. Without deep inspection, you would never find a virus in HTTPS traffic. You will only catch a virus when it is send to you via HTTP or FTP with these settings.

upvoted 15 times

D1360_1304 Highly Voted 3 years, 1 month ago

"Ensure that deep-inspection is selected for the SSL/SSH inspection..." FortiGate_Security_6.4_Study_Guide-Online pag, 494.

upvoted 5 times

albato239 Most Recent 2 years, 2 months ago

Selected Answer: R

A es verdadera

upvoted 1 times

MetDaci 2 years, 5 months ago

Selected Answer: A

A - Certificate inspection doesn't perform a deep inspection.

upvoted 2 times

gboy91 2 years, 5 months ago

Selected Answer: A

Ans A. FortiGate_Security_6.4_Study_Guide-Online, PAGE 493

upvoted 2 times

SandroAlex 2 years, 5 months ago

Selected Answer: A

A é verdadeira

upvoted 1 times

mothersson 2 years, 7 months ago

Selected Answer: A

Study Guide Page 494

upvoted 1 times

MrSaintz 2 years, 9 months ago

Selected Answer: A

Answer A Study Guide page 494

upvoted 2 times

BIGRAOU 2 years, 9 months ago

Selected Answer: A

FortiGate_Security_6.4_Study_Guide-Online, PAGE 494

upvoted 3 times

BIGRAOU 2 years, 9 months ago

FortiGate_Security_6.4_Study_Guide-Online, PAGE 494

upvoted 2 times

blabla4 2 years, 9 months ago

A ..ANTI-V USE DEEP INSPECTION TO ENSURE FULL CONTENT INSPECTIONS PREFORMED

upvoted 1 times

psion 2 years, 9 months ago

Selected Answer: A

A you need deep inspection

upvoted 1 times

forti_Ctes 2 years, 11 months ago

A is Correct

upvoted 2 times

armandolubaba 3 years, 1 month ago

A is correct answer

upvoted 4 times

MSAU 3 years, 1 month ago

A is correct.

upvoted 3 times

Gape4 3 years, 1 month ago

A is Correct. No Doubt

upvoted 3 times

JackeD 3 years, 2 months ago

Should be answer A (Security pdf, p494

upvoted 3 times

Question #16 *Topic 1*

Refer to the exhibit, which contains a session diagnostic output.

Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.

B. The session is in TCP ESTABLISHED state.

C. The session is a bidirectional UDP connection.

D. The session is a bidirectional TCP connection.

Suggested Answer: *C*

Community vote distribution

C (100%)

Lionardo Highly Voted 3 years, 5 months ago

C is correct.

proto=17 - UDP, proto_state=1 - Bidirectional

upvoted 16 times

Tiagopfelix Highly Voted 3 years, 5 months ago

C

FortiGate Security 6.4 Study Guide page 183

upvoted 12 times

cierzo Most Recent 2 years ago

Selected Answer: C

proto=17 - UDP

proto_state=01 Udp traffic both ways.

C is correct

upvoted 1 times

maxhoman 2 years, 4 months ago

Selected Answer: C

c is correct

upvoted 1 times

Gendeebongz 2 years, 5 months ago

C correct

dns =UDP Traffic bidirectional

upvoted 1 times

gboy91 2 years, 5 months ago

Selected Answer: C

correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: C

C é verdadeira

upvoted 1 times

lrosadini 2 years, 7 months ago

C - FortiGate Security 6.4 Study Guide page 183

proto_state 0 ONE WAY

proto_state 1 BOTH WAYS

upvoted 1 times

rikicm 3 years ago

C
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042
upvoted 1 times

Cunawaro 3 years ago
B ok. guide 183 page. Although (UDP) is a message-oriented, stateless protocol, it doesn't inherently require confirmed bidirectional connections like TCP, so there is no connection state. However, FortiGate's session table does use the proto_state= field to track the unidirectional UDP as state 0, and the bidirectional UDP as state 1.When FortiGate receives the first packet, it creates the entry and sets the state to 0. If the destination replies, FortiGate updates the state flag to 1 for the remainder of the conversation.
upvoted 5 times

Cunawaro 3 years ago
sorry C its OK..Typing error
upvoted 5 times

armandolubaba 3 years, 1 month ago
C is correct answer
upvoted 2 times

yemicontrol 3 years, 1 month ago
C is the answer.
UDP (proto 17)
Note: Even though UDP is a stateless protocol, the FortiGate still keeps track of 2 different 'states'

State

Value

UDP Reply not seen

0

UDP Reply seen

1
upvoted 1 times

FortiSherlock 3 years, 1 month ago
Answer is not C, proto_state only has 2 digits for TCP traffic !

B is correct, in proto_state=01 the 0 means that the connection is only inspected one-way (1 would be two-way) and the 1 is from the TCP state machine and stands for status ESTABLISHED.
upvoted 1 times

Merl 2 years, 8 months ago
proto=17 and it is UDP!!!
upvoted 3 times

kelsie 3 years, 1 month ago
B is correct check the Knowledge check in Fortigate_security_6.4_study_guide page 184
upvoted 1 times

onaicul 3 years, 3 months ago
C is correct
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042
FortiGate Security 6.4 Study Guide page 183
upvoted 2 times

iscofate 3 years, 3 months ago
C is the answer, Protocol refers to the Assigned IP protocol number and UDP is 17 while TCP is 06. They are just simply found in the Protocol field of the IPv4 header, UDP will be presented as 11 and TCP will be presented as 06 when they are put in Hexadecimal format.

upvoted 2 times

CyberKnight 3 years ago

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

upvoted 1 times

mahmoudlol 3 years, 4 months ago

Proto = 17 (UDP)

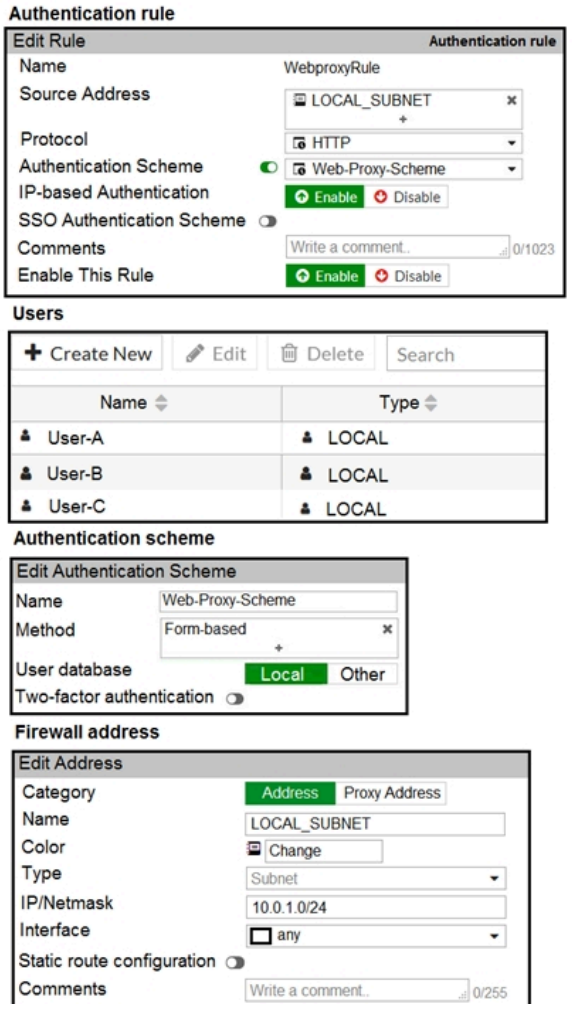
Proto_State = 1 (Bidirectional).

answer is C

upvoted 5 times

Question #17 *Topic 1*

Refer to the exhibit.



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

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

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

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

A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.

B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.

C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.

D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

E. If a Mozilla Firefox browser is used with User-C credentials, the HTTP request will be denied.

Suggested Answer: *BC*

Community vote distribution

BD (100%)

sahilk Highly Voted 3 years ago

Three exhibits are missing as below:

1. proxy custom address named "Browser CAT1" for local subnet and defined user agent "Chrome and IE"
2. proxy custom address named "Browser CAT2" for local subnet and defined user agent "Firefox"
3. proxy policy with 2 lines:

- Browser CAT2 & Local subnet & User B --> deny

- Browser CAT1 & Local subnet & User all --> accept
Beed on abowe exibits ony users from Chrome ana IE are allowed. Te correct answer should be B,D
upvoted 25 times

kkkvo 3 years ago
Thank you
upvoted 3 times

Carol254 2 years, 8 months ago
Thank you
upvoted 1 times

thissiteisgreat Highly Voted 3 years, 2 months ago
this snippet is incomplete, so not able to come up with the answer
upvoted 5 times

cessyang 3 years, 2 months ago
wasn't it B and C from before? i'll see if can find the explanations.
upvoted 3 times

Eist Most Recent 11 months, 2 weeks ago
can someone explain this question and from these answers came from?
from where did Google Chrome and Mozilla and internet explorer came from i dont get it!!!
upvoted 1 times

JuanTrabal 2 years, 1 month ago
There are Proxy addresses and 1 Web Proxy address missing in the question. What kind of bullshit is this site?
upvoted 1 times

mesql 2 years, 1 month ago
Selected Answer: BD
it is B&D
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: BD
B e D, seguindo a explicação de @sahilk das imagens inexistentes, são verdadeiras
upvoted 1 times

xYanivDx 2 years, 7 months ago
Selected Answer: BD
it is B&D
upvoted 2 times

ScottXYZ 2 years, 9 months ago
My rationale would be:
BD:
A: Is flat out WRONG as it is denied by the ID 1 (Browser-CAT-2, Local Subnet, User B, Action = Deny)
B: Is CORRECT because it is explicitly permitted by ID 2 ((Browser-CAT-1, Local Subnet, User A, Action = Permit)
E: Is wrong, there is no deny statement for User C
C&D are more tricky but I am choosing D because of the statement from 2021gene
upvoted 1 times

Seph1 3 years ago
The answer is: B & D
upvoted 1 times

2021gene 3 years ago
Yes, it looks like anything is missed. But suppossing that it is complete, I´d take B and D, take a look at FortiGate_Security_6.4 pages 357 and 345...in either case(pages) google and explorer seems to be more flexible than firefox
upvoted 5 times

Refer to the exhibit.

Exhibit A -

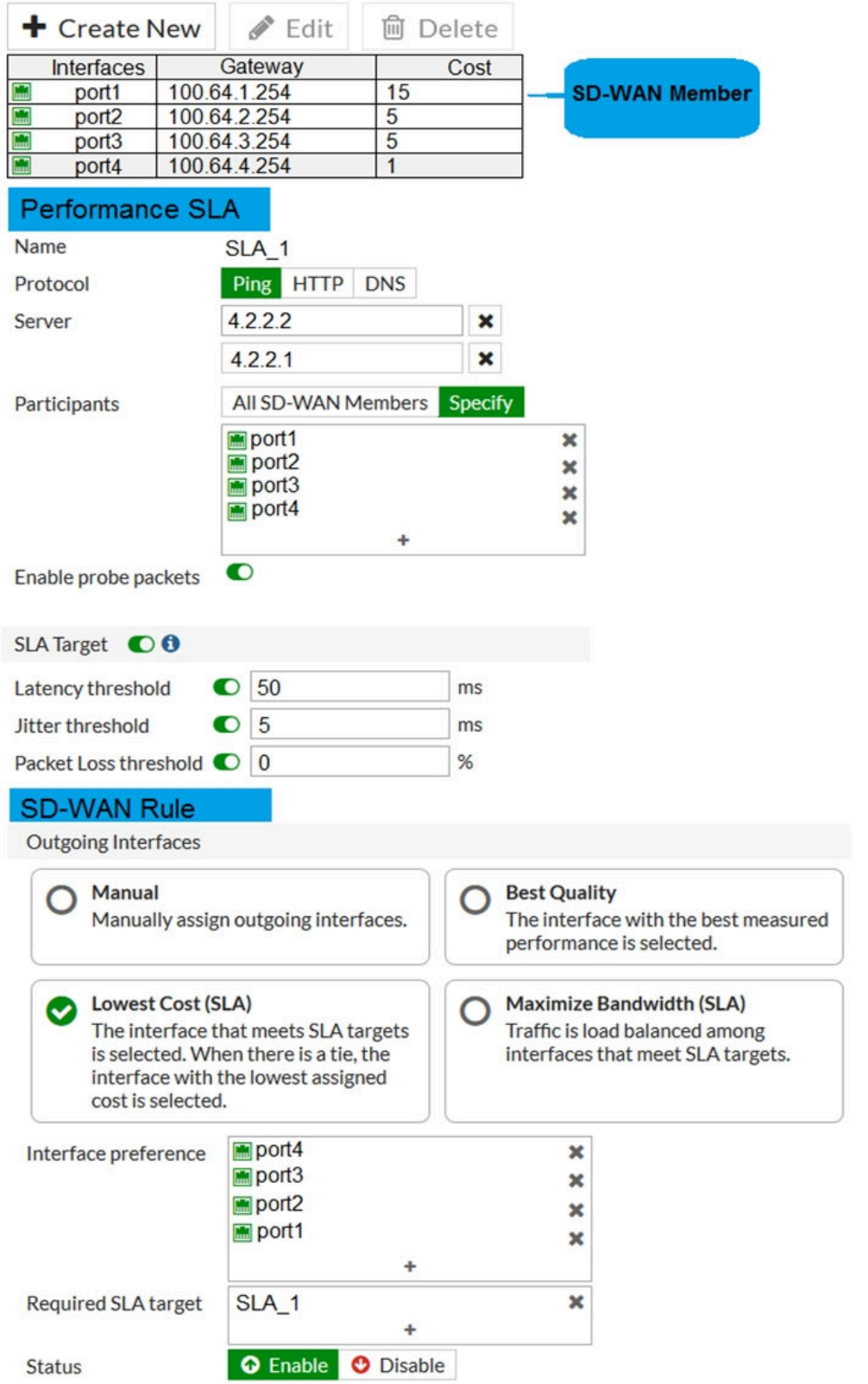


Exhibit B -

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

The exhibit shows the configuration for the SD-WAN member, Performance SLA and SD-WAN Rule, as well as the output of diagnose sys virtual-wan- link health-check.
Which interface will be selected as an outgoing interface?

A. port4

B. port2

C. port1

D. port3

Suggested Answer: *C*

Community vote distribution

D (79%) C (21%)

Ishan_Dis Highly Voted 3 years, 4 months ago
Here First SD WAN Rule check SLA Requirement. Port1,2,3 satisfied it. Then check for Lowest cost and port 2,3 has the lowest. Then check for preference and port3 is in top. So interface port3 will be selected
upvoted 29 times

Zaiderr Highly Voted 3 years, 3 months ago
The right answer is Port3
Fortigate will verify first if all interface match the SLA target -> Port 4 discarded
Then it will match with COST -> Port 3 and Port2 have equal cost.
Then it will end up choosing the most prefered one, which is the Port3
upvoted 12 times

redSTORM Most Recent 1 year, 4 months ago
Selected Answer: C
• D. port3
upvoted 1 times

redSTORM 1 year, 4 months ago
Correct answer D, missclicked C :/
upvoted 1 times

bccabrera 1 year, 11 months ago
Selected Answer: D
Lowest Cost (SLA): dinámico según coste configurado a cada interfaz y cumplimiento del SLA establecido.
Sólo se incluyen en el proceso de selección los caminos que cumplen SLA.
Entre ellos (o si ninguno cumple SLA) se elige el que tenga mejor coste, o en último caso, según orden de configuración.
upvoted 1 times

FoggiestIE 2 years, 3 months ago
Selected Answer: D
Correct is D
upvoted 2 times

juanK1982 2 years, 5 months ago
Selected Answer: D
Correct is D
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: D
D, port3, é a correta!
SD-WAN Role especifica Lowest Cost (SLA) que define a ordem de seleção: 1) SLA Target; 2) Interface Cost e; 3) Interface preference. A avaliação SLA target é top-down, logo o critério latência é atendido por todas as interfaces, seguido de jitter. O percentual de perda de pacotes da port4 ultrapassa 0%, logo ela é desconsidera restando apenas port1, port2 e port3. O menor custo é 5 que é da port2 e port3. A preferência de interface na SD-WAN rule é port3.
upvoted 1 times

ItVik 2 years, 5 months ago

I attempted the exam today and for me, this question was changed. Instead of the lowest cost, SDWAN rule was Best Quality. And Port-4 was having packet loss, Jitter on Port3 and Port-1 was best among other. So Answer was "Port-1".

Just keep in mind to read the question carefully incase question is tweeked.

upvoted 8 times

huu_nguyen 2 years, 6 months ago

Selected Answer: D

D is correct: Port 3

upvoted 1 times

MrSaintz 2 years, 8 months ago

Selected Answer: C

SLA is meet on port 1,2 and 3 and there is no tie in Lowest Cost SLA setting, port1 as the lowest SLA cost.

upvoted 2 times

lrosadini 2 years, 7 months ago

Look at Interface Preference

upvoted 1 times

MrSaintz 2 years, 9 months ago

Selected Answer: D

port 3 is correct, port 4 doesn't meet SLA so it's out, port 1 has higher cost than 2 and 3, so it's out as well, we are left with preference so port 3 has higher preference, Infrastructure Study Guide page 93.

upvoted 3 times

crimson_c 2 years, 9 months ago

FYI - On exam I got a question with these exhibits but with a small difference in chosen option second picture, and it asked "Which port is for outgoing interface based on latency?".

upvoted 1 times

blabla4 2 years, 9 months ago

PORT3

■ SD-WAN LOWEST COST RULES - BEST SLA PARAMETERS --> LOWEST COST --> TOP INTERFACE PREFERENCE

upvoted 1 times

psion 2 years, 9 months ago

Selected Answer: D

D Highest preference

upvoted 2 times

DIGGERNZ 2 years, 12 months ago

I had a similar question to this yesterday, except it was using 'Best Quality'. Also the port preference was different and. Answer was port 1. Just be sure to read the questions and make sure they are the same as what's listed here.

upvoted 2 times

vagedis 3 years ago

right answer is D: port3.

upvoted 1 times

Akoladet 3 years ago

Port 3 is the correct answer to this and there is no way it can be port 1

upvoted 1 times

Question #19 *Topic 1*

What devices form the core of the security fabric?

A. Two FortiGate devices and one FortiManager device

B. One FortiGate device and one FortiManager device

C. Two FortiGate devices and one FortiAnalyzer device

D. One FortiGate device and one FortiAnalyzer device

Suggested Answer: *C*
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components

Community vote distribution
C (71%) D (29%)

Lionardo Highly Voted 3 years, 5 months ago
C is correct. FortiGate_Security_6.4 page 63
upvoted 17 times

Kav_kk Highly Voted 3 years, 2 months ago
I got a mew question today on security fabric. Which security fabric feature causes an event trigger to monitor the network when a threat is detected?
A Security rating
B Optimization
C Automation stiches
D Fabric connectors
upvoted 6 times

Eduardo2022 2 years, 7 months ago
The answer is C. Automation stiches.
Each automation stitch pairs an event trigger and one or more actions, it allows you to monitor your network and take appropiate action when SecFabric detects a threat.
upvoted 2 times

Soulef 3 years, 2 months ago
What the answer ??
upvoted 1 times

Kav_kk 3 years, 2 months ago
It should be C
upvoted 2 times

certifi46 3 years, 2 months ago
automation stiches
upvoted 2 times

crashmurphy Most Recent 2 years, 1 month ago
Selected Answer: C
As of 7.0, the preferred answer is still C, according to FortiGate_Security_7.0 page 67.
upvoted 2 times

freeman567 2 years, 1 month ago
Selected Answer: C
FG Sec 7.0 Study Guide page 67
upvoted 1 times

moussa_rms 2 years, 1 month ago
Selected Answer: C
C is the correct answer
upvoted 1 times

PascalCert 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

PascalCert 2 years, 1 month ago

C is correct

upvoted 1 times

Ashit_patel1 2 years, 2 months ago

Selected Answer: C

C is correct Page 67 NSE 4 Fortigate Security Study Guide Chapter 2 Security Fabric

upvoted 3 times

JustAnotherKids 2 years, 2 months ago

C its written on pdf

upvoted 2 times

ArianCastle 2 years, 2 months ago

Selected Answer: D

Only 1 fortigate is needed.

upvoted 2 times

FoggiestIE 2 years, 3 months ago

Selected Answer: C

page 67 of 7.0 study guide

upvoted 1 times

xamuko 2 years, 3 months ago

Definitely D... you just need1 fgt and 1 faz..I've been setting up Sec fabric for a while.

upvoted 4 times

SandroAlex 2 years, 5 months ago

Selected Answer: C

C é a verdadeira

upvoted 1 times

xYanivDx 2 years, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

blahblah1234567890000 2 years, 7 months ago

Selected Answer: C

Answer is C

upvoted 1 times

lrosadini 2 years, 7 months ago

C - FortiGate_Security_6.4 page 63

but it works also in D configuration

upvoted 1 times

Stitch2020 2 years, 8 months ago

Selected Answer: D

One FG and one FA is all that's needed.

upvoted 3 times

Stitch2020 2 years, 8 months ago

Somehow when actually configuring it, you can enable the fabric with a single FG and FA. However the 6.4 documentation definitely says 2 FG and 1 FA... So I guess C is correct based on the documentation, not facts. Weird...

upvoted 3 times

Question #20 *Topic 1*

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

A. Source defined as Internet Services in the firewall policy.

B. Destination defined as Internet Services in the firewall policy.

C. Highest to lowest priority defined in the firewall policy.

D. Services defined in the firewall policy.

E. Lowest to highest policy ID number.

Suggested Answer: *ABD*

Reference:

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

Community vote distribution

ABD (100%)

FeNadege Highly Voted 3 years, 5 months ago

A, B, D are Correct

upvoted 13 times

Lionardo Highly Voted 3 years, 5 months ago

A, B & D is correct. FortiGate_Security_6.4 page 102

upvoted 9 times

Diego_Farani Most Recent 10 months, 2 weeks ago

Selected Answer: ABD

A, B, and D.

upvoted 1 times

NicolaeEast 2 years ago

A b and d

Fortigate 7.0 Security pg 110

upvoted 1 times

xamuko 2 years, 3 months ago

prior to 6.0 we were only able to use the ISDB as a destination

C makes sense if it wasn´t 6.4 or 7.0 .. and E niet.

A-B-D are correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: ABD

A, B e D são verdadeiras

upvoted 1 times

psion 2 years, 9 months ago

A, B, D are Correct

upvoted 1 times

Cyril_the_Squirl 3 years, 5 months ago

C & E don't make too much sense. A, B & D

upvoted 3 times

Question #21 *Topic 1*

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

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS

Suggested Answer: *CD*

Community vote distribution

CD (100%)

FeNadege Highly Voted 3 years, 5 months ago

C and D are Correct: Fortigate Hostname is not synchronized between cluster member

upvoted 12 times

NicolaeEast Most Recent 2 years ago

C and D

Fortigate Infra pg 316

Hostname and cache do not sync amongst others.

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: CD

C e D são verdadeiras

upvoted 1 times

Welisson2 2 years, 6 months ago

C, D estão OK

upvoted 1 times

lrosadini 2 years, 7 months ago

C D - FortiGate Infrastructure 6.4 Study Guide Pag 326

upvoted 2 times

Misterio 2 years, 8 months ago

C y D, Page 325, FTG Infra Study Guide

upvoted 1 times

blabla4 2 years, 9 months ago

C D

■ SETTING THAT DO NOT SYNC: (1) HA MGMT SETTINGS (2) IN BAND HA MGMT INTERFACE (3) HA OVERRIDE (4)VIRTUAL CLUSTER PRIORITY (5) HOSTNAME

(6) LICENSES (7) CACHE [FGT WF AND EMAIL FILTER, WEB CACHE] (8) PING SERVER HA PRIORITIES

upvoted 4 times

Cryptotec 2 years, 10 months ago

Selected Answer: CD

The right Answer is C&D

upvoted 3 times

Fbill 3 years ago

C and D are correct

upvoted 1 times

Cunawaro 3 years ago

c,d are OK

upvoted 1 times

davinal121 3 years, 2 months ago

C and D are correct !

upvoted 1 times

onaicul 3 years, 3 months ago

c & D are correct

upvoted 2 times

SamX 3 years, 4 months ago

c & d are correct

upvoted 2 times

davidone 3 years, 5 months ago

C and D are correct. Hostname and Licences (Foritguard) are not synchronized

upvoted 2 times

Question #22 *Topic 1*

Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service

B. Web application firewall

C. Antivirus

D. Application control

Suggested Answer: *B*

Reference:

https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/672671

Community vote distribution

B (100%)

Tiagopfelix Highly Voted 3 years, 5 months ago

B

FortiGate Security Study Guide 6.4 page 554

upvoted 11 times

Tiagopfelix 3 years, 3 months ago

page 544 is the right

upvoted 4 times

FeNadege Highly Voted 3 years, 5 months ago

B is Correct

upvoted 6 times

kevinrybar Most Recent 2 years, 2 months ago

Selected Answer: B

B .....

upvoted 1 times

juanK1982 2 years, 5 months ago

Selected Answer: B

Is B, web

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: B

B é a correta

upvoted 1 times

lrosadini 2 years, 7 months ago

B - FortiGate Security 6.4 Study Guide Pag 544

upvoted 2 times

psion 2 years, 9 months ago

Selected Answer: B

B is correct

upvoted 4 times

Cunawaro 3 years ago

B. Some FortiGate features are meant to protect clients, not servers. For example, FortiGuard web filtering blocks requests based on the category of the server's web pages. Antivirus prevents clients from accidentally downloading spyware and worms. Neither protects a server (which doesn't send requests—it receives them) from malicious scripts or SQL injections. Protecting web servers requires a different approach because they are subject to other kinds of attacks. This is where WAF applies. The WAF feature is available only in proxy inspection mode.

upvoted 6 times

siscoFe 3 years, 3 months ago

B is right, WAF is situated or facing internal servers such as Web Servers with purpose of protecting them from attacks such as XSS,SQL Inj, DOS,...

upvoted 3 times

siscoFe 3 years, 3 months ago

DOS excluded but other attacks that are caused due to OWASP Vulnerabilities and so on.

upvoted 3 times

semircan 3 years, 3 months ago

Yeap, B is correct

upvoted 4 times

SamX 3 years, 4 months ago

B is correct

upvoted 3 times

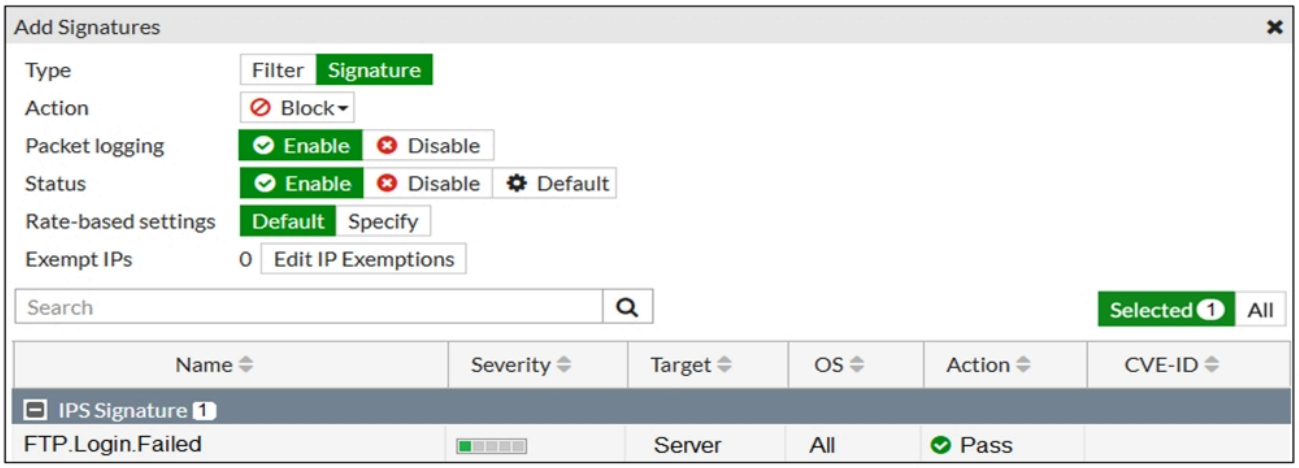
davidone 3 years, 5 months ago

B is correct.

upvoted 3 times

Question #23 *Topic 1*

Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings.
Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. Traffic matching the signature will be silently dropped and logged.

B. The signature setting uses a custom rating threshold.

C. The signature setting includes a group of other signatures.

D. Traffic matching the signature will be allowed and logged.

Suggested Answer: *D*

Community vote distribution

A (100%)

Lionardo Highly Voted 3 years, 5 months ago
A is correct. FortiGate_Security_6.4 page 525 and 529.
"pass" is only default action
upvoted 20 times

Hriibek 2 years, 9 months ago
"pass" is only default action

To explain this: the Pass action on the specific signature would only be chosen, if the Action (on the top) was set to Default. But instead its set to Block, se the action is will be to block and drop.
upvoted 5 times

Xillar Highly Voted 3 years, 5 months ago
A is the correct answer
upvoted 5 times

juanK1982 Most Recent 2 years, 5 months ago
Selected Answer: A
Is A the acción is block
upvoted 1 times

xandao 2 years, 6 months ago
A is correct. FortiGate Security 6.4 page 529. "Select the block to silently drop mathematical traffic from any of the signatures included in the entry"
upvoted 1 times

Windral 2 years, 6 months ago
Selected Answer: A
A is correct because action is "block" and not "default" on the rule
upvoted 1 times

EngelL 2 years, 7 months ago

Selected Answer: A

A is correct.

upvoted 1 times

Altimbo 2 years, 8 months ago

Selected Answer : A

upvoted 1 times

Pinchi 2 years, 8 months ago

Selected Answer: A

upvoted 1 times

aandreou020 2 years, 8 months ago

Selected Answer: A

Since the action is Blocked the answer is A

upvoted 1 times

MrSaintz 2 years, 9 months ago

Selected Answer: A

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

upvoted 1 times

ScottXYZ 2 years, 9 months ago

I vote for A, by adding this signature it will overwrite the default setting with the Block action. Silent drop means it will break the TCP session state without sending a FIN to the sender.

upvoted 2 times

picasso701 2 years, 10 months ago

Selected Answer: A

A like others stated

upvoted 1 times

forti_Ctes 2 years, 10 months ago

A is correct, test in lab

upvoted 1 times

deepakkalri 2 years, 11 months ago

D is correct as it says traffic matching with IPS signature "FTP.login" and action is passed, all others will be dropped except matching signature FTP.loginfailed.

upvoted 2 times

Hasan2021 2 years, 11 months ago

D is the correct,,

upvoted 2 times

dragonwise 3 years, 1 month ago

In option A, does anyone really know what they mean by silently dropped considering that the blocked packets will be logged?

upvoted 2 times

studentc 3 years ago

the client or server will not be notified for the dropped packet, maybe

upvoted 1 times

Zaiderr 3 years, 3 months ago

A is correct, Default signature action is ALLOW but Block will override it

upvoted 3 times

Question #24 *Topic 1*

How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.

B. FortiGate acts as an HTTP reverse proxy.

C. FortiGate acts as DNS server.

D. FortiGate acts as router.

Suggested Answer: *B*
Reference:
https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

Community vote distribution
B (100%)

Lionardo Highly Voted 3 years, 5 months ago
B is correct. FortiGate_Security_6.4 page 576
upvoted 16 times

NicolaeEast Most Recent 2 years ago
Selected Answer: B
B.

Fortigate security Pg 583
upvoted 1 times

Altimbo 2 years, 8 months ago
B is correct
upvoted 2 times

alexilc 2 years, 10 months ago
D. Fortigate acts as router its correct?
upvoted 1 times

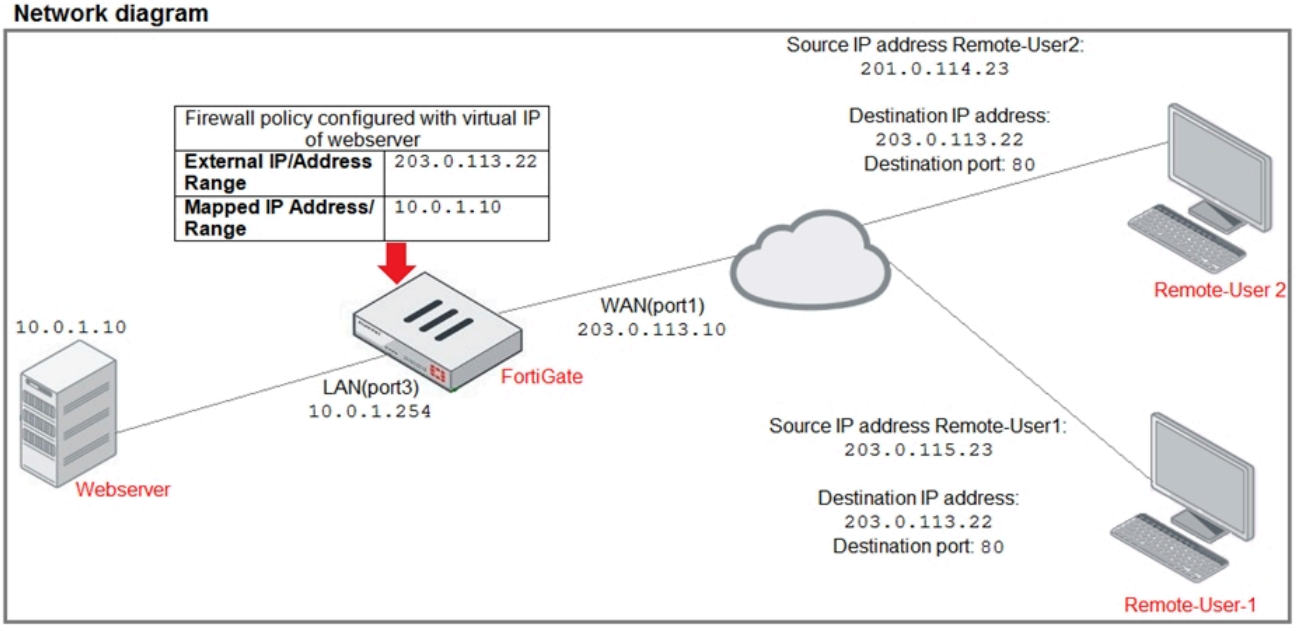
alexilc 2 years, 10 months ago
B is correct Sec 576
upvoted 2 times

SamX 3 years, 4 months ago
B is correct
upvoted 3 times

HT_TNT 3 years, 5 months ago
In web-only mode, the FortiGate unit acts as a secure HTML5 HTTPS gateway and authenticates remote users as members of a user group.
upvoted 4 times

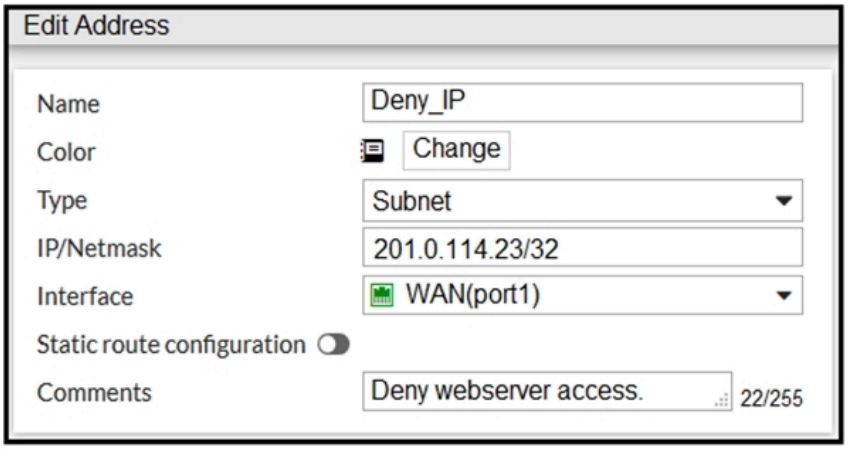
Refer to the exhibit.

Network diagram



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

Firewall address object



The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.

Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.

B. Set the Destination address as Deny_IP in the Allow-access policy.

C. Enable match-vip in the Deny policy.

D. Set the Destination address as Web_server in the Deny policy.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

Ishan_Dis Highly Voted 3 years, 4 months ago

By default does not match vip in deny policy for destination all. So 2 options wehave

1. Enable match vip in the Deny policy.
2. Add destination as webserver in deny policy

upvoted 8 times

Djohan23 Highly Voted 3 years, 4 months ago

C & D is correct answer. You can find the answer in "FortiGate Security 6.4 Self Study" page 159.

upvoted 8 times

ash8 3 years, 4 months ago

But there is written that Set the destination address as vip object look "FortiGate Security 6.4 Self Study" page 160.

upvoted 3 times

Cornelius360 Most Recent 2 years, 3 months ago

C and D is correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: CD

C e D são verdadeiras

upvoted 1 times

Alybely 2 years, 6 months ago

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta-p/189641

upvoted 1 times

lrosadini 2 years, 7 months ago

C D - FortiGate Security 6.4 Self Study. Pag 160

upvoted 1 times

damcol 2 years, 9 months ago

Should be more precise saying the VIP of the WebServer instead of the web server.

upvoted 2 times

SamX 3 years, 4 months ago

C, D are correct

upvoted 3 times

darkMmve 3 years, 4 months ago

C and D are correct

upvoted 2 times

Question #26 *Topic 1*

Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The subject field in the server certificate

B. The serial number in the server certificate

C. The server name indication (SNI) extension in the client hello message

D. The subject alternative name (SAN) field in the server certificate

E. The host field in the HTTP header

Suggested Answer: *BDE*
Reference:
https://checkthefirewall.com/blogs/fortinet/ssl-inspection

Community vote distribution
ACD (93%) 7%

Xillar Highly Voted 3 years, 5 months ago
A C and D is the correct answer.
Fortigate firtsly uses SNI, if there is no SNI it uses Subject or Subject Alternatives
upvoted 21 times

Lionardo Highly Voted 3 years, 5 months ago
A, C & D is correct. FortiGate_Security_6.4 page 328
upvoted 15 times

Sergio3000 Most Recent 1 year, 7 months ago
Selected Answer: ACD
Is correct
upvoted 1 times

JohnBB 2 years, 2 months ago
FortiGate_Security_7.0 Study Guide .pdf page 326
upvoted 1 times

TinPogi 2 years, 5 months ago
Selected Answer: ACD
FortiGate_Security_6.4 page 328
upvoted 2 times

mario156090 2 years, 7 months ago
Selected Answer: ACD
FortiGate_Security_6.4 page 328. Says clearly.
upvoted 2 times

Stitch2020 2 years, 8 months ago
Selected Answer: ACD
ACD are the right answers
upvoted 3 times

MrSaintz 2 years, 9 months ago
Selected Answer: ACD
As Lionardo claims, page 328 in study Guide
upvoted 2 times

BIGRAOU 2 years, 9 months ago
Selected Answer: ABE
FortiGate_Security_6.4_Study_Guide-Online, PAGE 315
upvoted 1 times

lrosadini 2 years, 7 months ago

on pag 315 it says how to use the certificate to identify a Persone or a Device.

This question is different.

upvoted 1 times

Hriibek 2 years, 9 months ago

Selected Answer: ACD

"...FortiGate parses server name indication (SNI) from client Hello..."

"If there is no SNI exchanged, then FortiGate identifies the server by the value in the Subject field or SAN"

Fortigate Security 6.4 Study Guide, page 328

upvoted 3 times

forti_Ctes 2 years, 11 months ago

A, C & D are correct

upvoted 1 times

Akoladet 3 years ago

The right answer is A,C and D

upvoted 1 times

Ishan_Dis 3 years, 4 months ago

A,C,D is correct one

upvoted 2 times

davidone 3 years, 5 months ago

A,C,D are correct. Fortigate uses the server name indication (SNI) to discern the hostname of the SSL server at the beginning of the SSL handshake. If there is no SNI, Forigate looks at the subject and subject alternative name fields.

upvoted 5 times

Question #27 *Topic 1*

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

A. SSH

B. HTTPS

C. FTM

D. FortiTelemetry

Suggested Answer: *AB*

Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/building-security-into-fortios

Community vote distribution

AB (100%)

FeNadege Highly Voted 3 years, 5 months ago

A and B are Correct

upvoted 13 times

Xillar Highly Voted 3 years, 5 months ago

AB is the correct answer

upvoted 6 times

Sergio3000 Most Recent 1 year, 7 months ago

Selected Answer: AB

is correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: AB

A e B são verdadeiras

upvoted 1 times

lrosadini 2 years, 7 months ago

A B - FortiGate Security 6.4 Study Guide. Pag 23

upvoted 3 times

5pik3 3 years ago

AB correct

upvoted 1 times

davinal121 3 years, 2 months ago

A and B are correct one !

upvoted 1 times

onaicul 3 years, 3 months ago

A and B are correct

upvoted 2 times

srimanta 3 years, 4 months ago

AB are correct

upvoted 3 times

SamX 3 years, 4 months ago

AB is correct

upvoted 3 times

Question #28 *Topic 1*

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale    : english

Service   : Web-Filter
Status    : Enable
License   : Contract

Num. of servers     : 1
Protocol            : https
Port                : 443
Anycast             : Enable
Default servers     : Not included
-=- Server List (Tue Feb 1 12:00:25 2020) -=-

IP                     Weight        RTT  Flags     TZ        Packets   Curr Lost  Total Lost
173.243.138.210          10           85  DI        -8         868          0         0
96.45.33.68              10          270            -8         868          0         0
173.243.138.211          10          340            -8         859          0         0
```

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

A. A local FortiManager is one of the servers FortiGate communicates with.

B. One server was contacted to retrieve the contract information.

C. There is at least one server that lost packets consecutively.

D. FortiGate is using default FortiGuard communication settings.

Suggested Answer: *BC*

Community vote distribution

BD (100%)

davidone Highly Voted 3 years, 5 months ago

It could be B and D. Those IPs starting with 173.243 are for fortiguard services, addind that uses port 443 to update.

upvoted 14 times

Lionardo Highly Voted 3 years, 5 months ago

B & D is correct. FortiGate_Security_6.4 page 415

(not sure about D)

upvoted 10 times

J_Olin Most Recent 2 years ago

Selected Answer: BD

B&D and here's why:

D is correct: In Version 6.4 FortiGuard stopped support for ports 53 and 8888, only 443 is valid now (its the whole point of this question, to differentiate between 6.2 test and 6.4 test). This is per: https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGuard-communication/ta-p/197109?externalID=FD46841

B is correct: The flags for 173.243.138.210 (a default FortiGuard Server IP) show D and I. "D" means this is a default address. "I" means it is the initial server contacted that validated the license, meaning that it didn't have to go on to another. If it had, one of the 173. servers would have a T or an F flag indicating that the connection was failing or had already failed.

This is per: https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGuard-Flags-and-Meanings/ta-p/206725

There are no private IP addresses shown, and there is no S flag, so a private FortiManager wasn't used, so A is wrong.

The Curr Lost column shows all 0s, so no packets were lost, so C is wrong.

upvoted 4 times

Vancero 2 years, 1 month ago

Selected Answer: BD

B&D correct

upvoted 2 times

Wilasky 2 years, 1 month ago

They do not correct the answers, there are many wrong, how do you want us to pay for Contribution Access?

B & D
upvoted 1 times

JustAnotherKids 2 years, 2 months ago
I think B D is correct answer. You should aware anycast is enable
upvoted 1 times

Cornelius360 2 years, 3 months ago
B and D are correct
upvoted 2 times

ibos8383 2 years, 5 months ago
Selected Answer: BD
I think it is B and D
upvoted 1 times

blahblah1234567890000 2 years, 7 months ago
Selected Answer: BD
Answer is B,D
upvoted 2 times

ScottXYZ 2 years, 9 months ago
BD

Link below shows D is correct and I agree that A and C do not make sense
https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGuard-communication/ta-p/197109?externalID=FD46841
upvoted 1 times

vdmi 2 years, 10 months ago
For A: It says "local FortiManager" and all the "Server List" IPs are public
For B: The letter "I" from the "Flags" section means "Contract server contacted"
For C: The "Curr Lost" and "Total Lost" sections have the value 0

This means that A & C are wrong, B is right and the only other option left is D.

* B & C can be verified @ FortiGate Security Study Guide - page 415 (Web Filtering - FortiGuard Connection)
upvoted 2 times

nimvoltage 2 years, 11 months ago
This has the answer
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46841
upvoted 2 times

Akoladet 3 years ago
The right answer is B and D
upvoted 1 times

2021gene 3 years ago
I understand that the correct ones are B and D, see FortiGate_Security_6.4_Study_Guide page 415(about the I flag indicating contract server contacted), and 416(HTTPS port 443 enforced by default fortiguard or manager communications)
upvoted 3 times

RHK0783 3 years ago
A & B are correct ... Default port is 8888
Also No packet drop
upvoted 1 times

RHK0783 3 years ago
My Bad, B&D are the right choices. Based on the flag definition, DI indicates that this server was contacted. 443 is also one of the default ports. NO indicator of the Fortimanager. Also, all listed IPs are public IPs that belongs to Fortiguard servers.
upvoted 2 times

alkalinegp 3 years ago

Default ports for querying Fortiguard are either udp/8888 or udp/53. If Fortigate is querying by using HTTPS tcp/443, then this indicates answer A (local FortiManager is used as Fortigurad server - https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/179018/using-fortimanager-as-a-local-fortiguard-server). So, in the end A & B answers are correct

upvoted 1 times

moneim 3 years ago

HTTPS 443 is also considered as default port for communication. If you look at a real fortigate device you will find 3 options HTTPS, UDP 8888 and udp 53

upvoted 1 times

Question #29 *Topic 1*

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.
Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning

B. File filter

C. DNS filter

D. Intrusion prevention

Suggested Answer: *AC*

Community vote distribution

AD (100%)

Lionardo Highly Voted 3 years, 5 months ago
A & D is correct. FortiGate_Security_6.4 page 445
upvoted 16 times

Djohan23 Highly Voted 3 years, 4 months ago
A & D is the correct answer. FortiGate_Security_6.4 page 368.
Security policy: If the traffic is allowed as per the consolidated policy, FortiGate will then process it based on the security policy to analyze additional criteria, such as URL categories for web filtering and application control. Also, if enabled, the security policy further inspects traffic using security profiles such as IPS and AV.
upvoted 9 times

NicolaeEast Most Recent 2 years ago
Selected Answer: AD
A and D

Fortigate security Pg 451

You can also add a file filter but for this question I think they're asking for A and D specifically.
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: AD
A e D são verdadeiras no firmware 6.4.0 no qual o guia do estudante é baseado. Entretanto nas versões mais novas de firmware da família 6.4 já é possível usar File Filter.
upvoted 1 times

Ragnar77 2 years, 6 months ago
Selected Answer: AD
Antivirus and IPS are always profile based.
upvoted 1 times

nabillose 2 years, 6 months ago
Selected Answer: AD
AD is the correct
upvoted 1 times

blahblah1234567890000 2 years, 7 months ago
Selected Answer: AD
Answer is a,d
upvoted 1 times

BIGRAOU 2 years, 9 months ago
Selected Answer: AD
A & D is correct. FortiGate_Security_6.4 page 445

upvoted 1 times

yaboi01 2 years, 9 months ago

I think this is a freebie...All of these answers are correct

upvoted 2 times

Rman0059 2 years, 9 months ago

Selected Answer: AD

AD are correct

upvoted 2 times

dragonwise 3 years ago

I have checked in on an actual firewall

A B & D

upvoted 3 times

Thanos84 2 years, 11 months ago

dude , this is a tricky one :FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.:(this is to trick you):::Which two other ****security profiles**** can you apply to the security policy?--- so A D are right no dns and file in security profile

upvoted 2 times

Enforc3r 2 years, 11 months ago

Actually there is File Filter under Security Profiles.

At least in 6.4.7 software I'm running on.

upvoted 2 times

whindkhan 2 years, 6 months ago

You're right. There are four security profiles on Policy-based: Antivirus, Web Filter, IPS and File Filter.

upvoted 1 times

MrSaintz 2 years, 9 months ago

It is true, but study guide only mentions A and D, maybe file filter was added later on, so if the question is to answer two options, what would you have?

upvoted 1 times

Cunawaro 3 years ago

A y D Are OK

upvoted 1 times

davidone 3 years, 5 months ago

A and D are correct.

upvoted 4 times

Xillar 3 years, 5 months ago

A C and D are correct answers

upvoted 2 times

Cyril_the_Squirl 3 years, 5 months ago

The question expects Only 2 options

upvoted 4 times

Question #30 *Topic 1*

Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries

B. PKI

C. Traffic shaping

D. DNS

Suggested Answer: *AB*

Community vote distribution

AD (100%)

Bong_20 Highly Voted 3 years, 4 months ago

A and D is the correct answer

upvoted 15 times

painkiller Highly Voted 3 years, 4 months ago

A and D - FortiGate_Infrastructure_6_4 page 114:

"NTP, FortiGuard updated/queries, SNMP, DNS Filtering, Log settings and other mgmt related services".

upvoted 11 times

NicolaeEast Most Recent 2 years, 1 month ago

Regardless of of question -

Fortigate Infrastructure 7.0 Book Pg. 122 says global settings for vdom's are:

Hostname

HA Settings

Fortiguard Settings

System time

Administrative Accounts

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: AD

A e D são verdadeiras

upvoted 1 times

nabillose 2 years, 6 months ago

Selected Answer: AD

A and D is the correct

upvoted 1 times

MikeWillis 2 years, 8 months ago

Selected Answer: AD

A and D are correct

upvoted 3 times

BIGRAOU 2 years, 9 months ago

Selected Answer: AD

A & D correct

upvoted 1 times

Rman0059 2 years, 9 months ago

Selected Answer: AD

AD are correct

upvoted 1 times

KemalM 2 years, 11 months ago

Answer: A & D

Fortigate Infrastructure 7.0 Study Guide P.113

upvoted 3 times

franger 3 years, 1 month ago
according to this article, A and D are the correct ones
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542
upvoted 3 times

lpalpalpa 3 years, 2 months ago
ups say traffic, AD ;)
upvoted 2 times

diegofretesc 3 years, 2 months ago
era o no el a y d?
upvoted 1 times

lpalpalpa 3 years, 2 months ago
AB. PKI is managed from root vdom and it allow certificates availabe in other vdom.
upvoted 1 times

BarCat 3 years, 4 months ago
To be strictly D is not correct since the VDOMs (but he management one) can be configured with their own DNS server.
But this is an exam not the real life so I think A & D are "correct".
upvoted 2 times

Biz90 3 years, 4 months ago
The answer is A and D
B is wrong because PKI stands for Public Key Infrastructure and is associated with VPNS
C is wrong because traffic shaping is configured on a 'Traffic Shaping Policy'
A is correct because Fortigate will use Fortiguard for these queries
D is correct as the management VDOM (very similar to Palo Alto) can use DNS for DNS queries
upvoted 6 times

BarCat 3 years, 4 months ago
Ok to A and D but remember that non mgmt VDOMs can have their own DNS servers with:
config system vdom-dns
upvoted 2 times

yopop 3 years, 5 months ago
Should be A and C, right?
upvoted 1 times

Lionardo 3 years, 5 months ago
A & B is correct. For "A" look FortiGate_Infrastructure_6.4 page 114
upvoted 3 times

freeed 3 years, 4 months ago
I think it schould be A & D because FortiGuard and DNS is mentioned in FortiGate_Infrastructure_6.4 page 114
upvoted 4 times

cabeza 3 years, 4 months ago
yes a&d https://www.skillfulist.com/fortigate/fortigate-vdoms/
upvoted 3 times

Question #31 *Topic 1*

An administrator must disable RPF check to investigate an issue.
Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

A. Enable asymmetric routing, so the RPF check will be bypassed.

B. Disable the RPF check at the FortiGate interface level for the source check.

C. Disable the RPF check at the FortiGate interface level for the reply check.

D. Enable asymmetric routing at the interface level.

Suggested Answer: *D*
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

Community vote distribution
B (92%) 8%

davidone Highly Voted 3 years, 5 months ago
"B" is the answer be careful question are very tricky. RPF methods in NSE guide says: Two ways to disable RFP. 1 Enable asymetric routing, which disables RPF checking system wide (but not at interface level is through the CLI command config system settings) 2 Disable RPF checkking at the interface level (the only way at the interface level in the CLI command). A incorrect. If you enable asymetric routing, RPF not will be bypass because is disable. B Correct. You have to disable the RPF check an the interface level, for the source. C Is incorrect is for the source D is incorrect: Asymetric routing is not enable at interface level.
upvoted 31 times

Djohan23 Highly Voted 3 years, 4 months ago
RPF checking can be disabled in tho ways. If you enable asymmetric routing, it will disable RPF checking system wide. However this reduces the security of you network greatly. Features such us ANTIVIRUS, and IPS become non-effective. So, if you need to disable RPF checking, you can do so at the interface level using the command:
config system interface
edit <interface>
set src-check [enable | disable]
end

So the correct answer is B. No more debates.
upvoted 15 times

NicolaeEast Most Recent 2 years, 1 month ago
Selected Answer: B
B

Recent 7.0 Fortigate Infrastructure Pg 39
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: B
B é a verdadeira
upvoted 1 times

JoseVillarroel 2 years, 6 months ago
Selected Answer: B
Answer is B
upvoted 3 times

Joalmici 2 years, 6 months ago
Selected Answer: D
RPF is a mechanism that protects FortiGate and the network from IP spoofing attacks.

By default, RPF is enabled on all interfaces.

Disable it by enabling asymmetric route on the specific VDOM but if the requirement is only for specific interface.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-disable-Reverse-Path-Forwarding-RPF-per/ta-p/193338
upvoted 1 times

crashmurphy 2 years, 1 month ago
This is not correct, as following 'D' would prevent A/V and IPS from working.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/58863/asymmetric-routing
upvoted 1 times

Joalmici 2 years, 6 months ago
"D" is the answer, By default, RPF is enabled on all interfaces.
Disable it by enabling asymmetric route on the specific VDOM but if the requirement is only for specific interface.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-disable-Reverse-Path-Forwarding-RPF-per/ta-p/193338
upvoted 1 times

crashmurphy 2 years, 1 month ago
This is not correct, as following 'D' would prevent A/V and IPS from working.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/58863/asymmetric-routing
upvoted 1 times

MikeSch 2 years, 8 months ago
Selected Answer: B
Otherwise AV and IPS would not work correctly
upvoted 1 times

MrSaintz 2 years, 9 months ago
Selected Answer: B
Answer is B
upvoted 1 times

jcarlosBO 2 years, 9 months ago
"D is CORRECT"
Check this: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-disable-Reverse-Path-Forwarding-RPF-per/ta-p/193338
upvoted 1 times

Ehab99 2 years, 6 months ago
The article in the link you shared says the answer is B , it tells you that if you want to disable on haul VDOM use symitric route thing "But" if need on interface only use the following command to achieve it
config system interface
edit <interface>
set src-check disable
end
this command from the link you shared recommened disabling RPF on interface.
Answer is B
upvoted 1 times

crashmurphy 2 years, 1 month ago
This is not correct, as following 'D' would prevent A/V and IPS from working.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/58863/asymmetric-routing
upvoted 1 times

BIGRAOU 2 years, 9 months ago
Selected Answer: B
FortiGate_Infrastructure_6.4_Study_Guide-Online, PAGE 39
upvoted 3 times

blabla4 2 years, 9 months ago
D
enable asymetric routing on interface level
upvoted 1 times

blabla4 2 years, 9 months ago

B
FortiGate_Infrastructure_6.4 page 39
upvoted 1 times

Rman0059 2 years, 9 months ago
Selected Answer: B
B is the correct answer
upvoted 2 times

lulipeoliveira 2 years, 12 months ago
B is correct.
Whe he say "Enable assymetric routing" on guide is not in interface level.
upvoted 2 times

Cunawaro 3 years ago
B. Period!
FG Infrast 7.0 SG page 38
You can disable RPF checking in two ways. If you enable asymmetric routing, it disables RPF checking system wide. However this reduces the security of your network. Features, such as antivirus and IPS become noneffective. So, if you need to disable RPF checking, you can do so at the interface level using the commands: set src-check [enable | disable] at system interface level.
upvoted 6 times

mouna23 3 years, 2 months ago
I think it is B because enabling the asymetric routing could not be at interace level .
config system settings
set asymroute enable
end
upvoted 1 times

onaicul 3 years, 3 months ago
B is correct. FortiGate_Infrastructure_6.4 page 39
upvoted 4 times

Question #32 *Topic 1*

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- ➪ All traffic must be routed through the primary tunnel when both tunnels are up.
- ➪ The secondary tunnel must be used only if the primary tunnel goes down.
- ➪ In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two.)

A. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

B. Enable Dead Peer Detection.

C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

Lionardo Highly Voted 3 years, 5 months ago

B & C is correct. FortiGate_Infrastructure_6.4 page 219 for "B" and 243 for "C"

upvoted 12 times

Biz90 Highly Voted 3 years, 5 months ago

Ok to answer this question is B and C.

B because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.

C remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

upvoted 5 times

NicolaeEast Most Recent 2 years ago

Selected Answer: BC

Fortigate Infrastructure pg 234

upvoted 1 times

ChuckC 2 years, 2 months ago

Selected Answer: BC

I was looking to 'Prove' these answers found FortiGate_Infrastructure_7.0 page 234 for both B and C

upvoted 2 times

SandroAlex 2 years, 5 months ago

Selected Answer: BC

B e C são verdadeiras

upvoted 1 times

Ali1982 2 years, 9 months ago

B & C Are correct

upvoted 1 times

Bluegrass168 3 years, 3 months ago

Answers are B and C.

But in the real environment, the Ipsec Tunnle keeps up even the DPD enabled ... ha ha

And the best way to resolve the issue in my opinion is to add IPSEC Tunnel to SDWAN group with Tunnel Interface IP address as health check...

upvoted 4 times

mahmoudlol 3 years, 4 months ago

B & C are correct

upvoted 1 times

Ishan_Dis 3 years, 4 months ago

DPD- Identify Dead Tunnels

Low Distance Routes will apply first

So answer is BC

upvoted 3 times

Ishan_Dis 3 years, 4 months ago

DPD- Identify Dead Tunnels

Low Distance Routes will apply first

upvoted 2 times

davidone 3 years, 5 months ago

B and C are correct.

upvoted 3 times

HT_TNT 3 years, 5 months ago

Correct is B and D. Both routes must have same AD.

upvoted 2 times

Lionardo 3 years, 5 months ago

D is incorrect, this configuration only keep alive IPsec connection. There no such requirements.

upvoted 2 times

Question #33 *Topic 1*

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

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

A. Traffic between port2 and port2-vlan1 is allowed by default.

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

C. port1 is a native VLAN.

D. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Suggested Answer: *AD*

Community vote distribution

CD (100%)

aads Highly Voted 3 years, 4 months ago

The answer must be C and D.

For A - traffic between interfaces is not allowed by default.

For B - Port1-vlan10 and port-2vlan10 are not in the same broadcast domain since the subnet is different.

upvoted 26 times

Lionardo Highly Voted 3 years, 5 months ago

B & D is correct.

FortiGate_Infrastructure_6.4 page 127 for "D" and page 154 for "B"

upvoted 6 times

murathtp 3 years, 4 months ago

fortigate ports are in different broadcast domains. so how port1 and port 2 are in same broadcast domains? ı am not sure abot the answer, but B seems incorrect to me.

upvoted 4 times

gianmarco 3 years, 4 months ago

each VLAN forms a separate broadcast domain | Pag 154

upvoted 2 times

NSE421 3 years, 4 months ago

B & D seems to me the correct answers

upvoted 1 times

MrSaintz 2 years, 9 months ago

broadcast domains are discussed in transparent-mode, no IP is assigned to the interfaces in this mode, much less considering that 10.1.10.1/24 is in the same broadcast domain as 10.0.10.1/24 B is surely incorrect.
upvoted 5 times

NicolaeEast Most Recent 2 years, 1 month ago
A. WRONG Because they are different subnets, this will not work work.
B. WRONG The interfaces can only be a part of the same broadcast domain if the Fortigate is in Transparent mode. If the Fortigate was in transpararent mode, however, the interfaces would not be assigned IP addresses.
C. CORRECT Physical interface is native VLAN.
D. CORRECT In NAT mode, which this obviously is, interfaces can be moved around. And even multi-VDOM VLAN sub-interfaces can belong in different VDOMs.
Fortigate Infrastructure 7.0 Pg 121:
Fortigate Infrastructure 7.0 Pg 134:
Fortigate Infrastructure 7.0 Pg 156
Fortigate Infrastructure 7.0 Pg 160:
upvoted 1 times

NicolaeEast 2 years ago
A wrong most of all because traffic between interfaces not allowed by default.
And D is correct for the sake of the answer... But in reality, the two vlans couldn't exist on the same vdom unless the subnets matched.
upvoted 2 times

JuanTrabal 2 years, 2 months ago
So many people here commenting and nobody knows the correct answer yet.
upvoted 2 times

MetDaci 2 years, 5 months ago
Selected Answer: CD
C&D is correct.javascript:void(0)
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: CD
C e D são verdadeiras
upvoted 1 times

AJDLM 2 years, 5 months ago
Answer B and C
A and d are wrong:
For A - traffic between interfaces is not allowed by default.
For D - "Each interface (physical or VLAN) can belong to ONLY ONE VDOM." (FortiGate Infrastructure 6.4 page 127
upvoted 1 times

AJDLM 1 year, 11 months ago
Only to confirm that B and C is correct, verified in FortiGate with 6.4.6
upvoted 1 times

MOSTAFAMETWALLY 2 years, 6 months ago
C and D.
upvoted 1 times

mario156090 2 years, 6 months ago
Selected Answer: CD
C and D.
upvoted 1 times

lrosadini 2 years, 7 months ago
C-D:
B is wrong because a brodcast domain is a datalink layer [Level2], here we are working in NAT mode
A is wrong because traffic between different interface aren't allowed
upvoted 4 times

RatheeshRavindran 2 years, 7 months ago
Selected Answer: CD

C and D is correct
upvoted 2 times

MrSaintz 2 years, 9 months ago

Selected Answer: CD

I agree with aads... "For A - traffic between interfaces is not allowed by default.
For B - Port1-vlan10 and port-2vlan10 are not in the same broadcast domain since the subnet is different."
upvoted 1 times

Stitch2020 2 years, 8 months ago

Broadcast domain is a layer 2 concept, nothing to do with subnets.
upvoted 1 times

blahblah1234567890000 2 years, 7 months ago

vlans form a separate broadcast domain though.
upvoted 1 times

ScottXYZ 2 years, 9 months ago

CD is correct
A is wrong, different interfaces are not allowed by default
B is wrong, because physical interfaces with SAME VLAN do not have to belong to the same broadcast domain. We don't know if they connect to the same switch. Also the IP subnet is different another clue
upvoted 1 times

Ali1982 2 years, 9 months ago

B & D ----Creating VLAN subinterfaces with the same VLAN ID doesn’t create an internal connection between them. For example, a VLAN ID of 300 on port1 and VLAN ID of 300 on port2 are allowed, but they aren’t connected. Their relationship is the same as between any two FortiGate network interfaces.
FortiGate interfaces can’t have overlapping IP addresses, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces, such as VLAN subinterfaces.
upvoted 1 times

damcol 2 years, 9 months ago

C and D
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interface/ta-p/197640?externalID=FD31639
upvoted 2 times

funirka 2 years, 10 months ago

D: https://kb.fortinet.com/kb/documentLink.do?externalID=FD31639 Example of VLAN setting and VDOM assignment. The same VLANs from another ports at the same VDOM.
Answer B is OK only for transparent mode, not NAT mode (IP addresses = NAT mode for this question). FG Infra 7.0 page 171
upvoted 3 times

forti_Ctes 2 years, 12 months ago

A: wrong
B: correct. same vlan ID = same broadcast domain
C: correct: Port1 = Vlan0 = Native Vlan
D: Wrong: cant have 2 vlanID interface in the same VDOM
upvoted 5 times

Question #34 *Topic 1*

Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.

B. SLA targets are optional.

C. SLA targets are required for SD-WAN rules with a Best Quality strategy.

D. SLA targets are used only when referenced by an SD-WAN rule.

Suggested Answer: *AC*

Community vote distribution

BD (100%)

Lionardo Highly Voted 3 years, 5 months ago

B & D is correct.FortiGate_Infrastructure_6.4 page 80

A incorrect - You can configure more that 2 SLA targets

C incorrect - SLA targets only required for Lower Cost (SLA) and Maximize Bandwidth (SLA)

upvoted 28 times

maxhoman Most Recent 2 years, 3 months ago

Selected Answer: BD

B&D are correct

upvoted 2 times

ibos8383 2 years, 5 months ago

Selected Answer: BD

A incorrect - You can configure more that 2 SLA targets

C incorrect - SLA targets only required for Lower Cost (SLA) and Maximize Bandwidth (SLA)

upvoted 2 times

SandroAlex 2 years, 5 months ago

Selected Answer: BD

B e D são verdadeiras

upvoted 2 times

Carol254 2 years, 8 months ago

A. port-VLAN1 is the native VLAN for the port1 physical interface.

B. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.

C. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.

D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

upvoted 1 times

Carol254 2 years, 8 months ago

I think this set of answers make more sence

upvoted 1 times

abdikissi 2 years, 7 months ago

Answer for question 33

upvoted 2 times

MrSaintz 2 years, 8 months ago

Selected Answer: BD

Agree with Lionardo, B & D are correct.

upvoted 1 times

Miguex125 2 years, 8 months ago

Answers B & D.
Not B, because is only required for lower cost (sla) and maximize BW (sla)rules.
upvoted 1 times

Miguex125 2 years, 8 months ago
Not C*
upvoted 1 times

DavidC91 2 years, 11 months ago
B & D
FortiGate_Infrastructure_6.4 page 80
upvoted 2 times

KemalM 2 years, 11 months ago
Answer B & D
Ref: Fortigate Infrastructure 7.0 Study Guide P.81
upvoted 3 times

forti_Ctes 2 years, 12 months ago
B & D Correct.
upvoted 3 times

Pierrot26 3 years ago
I think, it is B & C.
A : false, because it 's possible to add more than 2 SLA Targets
D : false, because it's possible to create a perfomance SLA without SDWAN rule
upvoted 3 times

jganuza 3 years, 2 months ago
B and D is correct!
upvoted 1 times

Ngeno 3 years, 3 months ago
Yes. B and D correct.
upvoted 3 times

Ishan_Dis 3 years, 4 months ago
B & D are correct
upvoted 1 times

aads 3 years, 4 months ago
B and D are correct
SLA targets are optional and only used when referenced by an SD-WAN policy
upvoted 1 times

jmt97 3 years, 4 months ago
B and D are correct.
When configuring Best Quality Strategy you have to select a "Measured SLA" just to analyze the result of the ping or whatever, you don't need to configure an SLA target with thresholds
upvoted 2 times

darkMmve 3 years, 4 months ago
B & D are correct. See infrastructure study guide, SD-WAN section, page 80
upvoted 3 times

Question #35 *Topic 1*

Refer to the web filter raw logs.

Based on the raw logs shown in the exhibit, which statement is correct?

A. Access to the social networking web filter category was explicitly blocked to all users.

B. The action on firewall policy ID 1 is set to warning.

C. Social networking web filter category is configured with the action set to authenticate.

D. The name of the firewall policy is all_users_web.

Suggested Answer: *B*

Community vote distribution

C (100%)

prenominal Highly Voted 3 years ago

Answer is 100% C. Tested on my Fortigate by setting Social Networking web filter category to Authenticate and applying that to a high priority policy with full SSL inspection enabled. First action listed in raw log for that IP was blocked, then authentication page popped up, entered credentials for user and then a log with action passthrough was generated.

upvoted 25 times

prenominal 3 years ago

Also, firewall policies don't have a warning action

upvoted 12 times

NicolaeEast Most Recent 2 years, 1 month ago

Selected Answer: C

a. if it were blocked it would not be allowed the second time.

b. this is not a policy.

c. CORRECT first time was incorrect password second time was correct password.

d. that is the name of the filter not the policy

Fortigate Security 7.0 PG 381

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: C

C é a verdadeira

upvoted 1 times

haymen 2 years, 8 months ago

B is correct

upvoted 1 times

Ehab99 2 years, 6 months ago

can you show me how you purt warrning as action on any firewall policy ?

upvoted 2 times

mrtim5700 2 years, 9 months ago

Selected Answer: C

The answer to this one is C.

A is incorrect. The web filter category is not explicitly blocked since it is allowed the second time around.

B is incorrect. The policy is not what is interacting, the web filter profile is. The question even refers to the "web filter logs."

D is incorrect. The name of the web filter profile is "all_users_web" not the firewall policy.

upvoted 4 times

forti_Ctes 2 years, 12 months ago

C is correct

upvoted 3 times

vagedis 3 years ago
The correct answer is A. traffic to the site in the social networking catagory is blocked for all_users_web.
upvoted 1 times

enassim 3 years ago
B is correct: When you set the Warning action, you will see firstly the blocked and if you click on the web page to continue to the site you will see another passthrough.
upvoted 1 times

RHK0783 3 years ago
There is no challenge log that shows the user was prompted for authentication.
D is incorrect as it is name of the security profile.
B is the most appropriate answer. Action-set warning is set for web category not for the firewall policy.
upvoted 1 times

2021gene 3 years ago
Have in mind that in A and C, it explicitaly talks about the action of the web filter category, not the firewall policy action. But in B it talks about the firewall policy action(if the idea was to talk about the web filter category action, then following the same logic, the sentence should be expressed more or less like A and C)
upvoted 1 times

YASL 3 years ago
correct C
upvoted 3 times

moneim 3 years ago
Also action in the firewall policy is either deny or accept. no warning action
upvoted 2 times

yadavarya97 3 years ago
B is correct as the action is set to warning.
upvoted 1 times

moneim 3 years ago
Here in the logs we have 2 different sessions, one was blocked by the firewall and the other was passed. Both hitting the same policy id. I think D is the most realistic answer
upvoted 1 times

moneim 3 years ago
I mean "C" action set to authenticate
upvoted 1 times

zqrni 3 years ago
yes, i agree. C is the correct answ.
upvoted 3 times

Question #36 *Topic 1*

Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode uses Windows convention-NetBios: Domain\Username.

B. Standard mode security profiles apply to organizational units (OU).

C. Standard mode security profiles apply to user groups.

D. Standard access mode supports nested groups.

Suggested Answer: *AB*

Community vote distribution

AC (100%)

Lionardo Highly Voted 3 years, 5 months ago

A & C is correct. FortiGate_Infrastructure_6.4 page 290

upvoted 18 times

NicolaeEast Most Recent 2 years, 1 month ago

Selected Answer: AC

Fortigate Infra 7.0 Pg 280

upvoted 1 times

evelazquez 2 years, 4 months ago

Selected Answer: AC

Correct

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: AC

A e C são verdadeiras

upvoted 2 times

Ragnar77 2 years, 6 months ago

Selected Answer: AC

C is right but answer is wrong, should be Domain\Group but thje only one possible.

upvoted 1 times

MrSaintz 2 years, 8 months ago

Selected Answer: AC

Agree with Lionardo and mrtim5700 submited answers

upvoted 2 times

mrtim5700 2 years, 9 months ago

Selected Answer: AC

B is incorrect. Standard Mode does not do OU, advanced mode does.

D is incorrect. Standard Mode cannot do nested groups.

upvoted 3 times

KemalM 2 years, 11 months ago

Answer: A & C

Fortigate Infrastructure 7.0 Study Guide P.295

upvoted 3 times

forti_Ctes 2 years, 12 months ago

A & C are correct

upvoted 2 times

Akoladet 3 years ago

The right answer is A and C while B is wrong because is for ADVANCE mode and not applicable to STANDARD

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

upvoted 2 times

franger 3 years, 1 month ago

A and C are correct:https://kb.fortinet.com/kb/documentLink.do?externalID=FD30964

upvoted 2 times

Mountfestus 3 years, 1 month ago

Can someone kindly share the download link for this; FortiGate_Infrastructure_6.4?

upvoted 1 times

bulents 3 years, 1 month ago

email me at bsahin@sahinbulent.com i will send you both of the files

upvoted 2 times

1wish 3 years, 1 month ago

https://training.fortinet.com/pluginfile.php/728897/mod_resource/content/23/FortiGate_Infrastructure_6.4_Study_Guide-Online.pdf?forcedownload=1

upvoted 2 times

youcef_f 3 years, 4 months ago

A & C are the correct.

upvoted 4 times

Ishan_Dis 3 years, 4 months ago

A & C Correct. In standard mode only sec profile can be applied for user group. Others are available in advance mode. So B is incorrect

upvoted 4 times

davidone 3 years, 5 months ago

A and C are standard modes. B and D are advanced modes.

upvoted 4 times

davidone 3 years, 5 months ago

A and C are correct.

upvoted 4 times

HT_TNT 3 years, 5 months ago

A and C are the ones!

upvoted 4 times

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A -

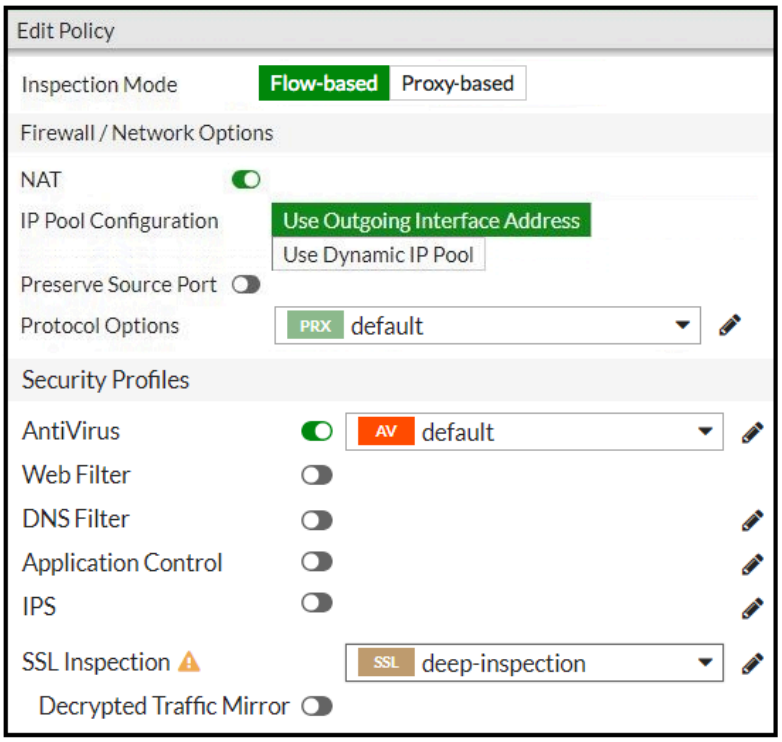
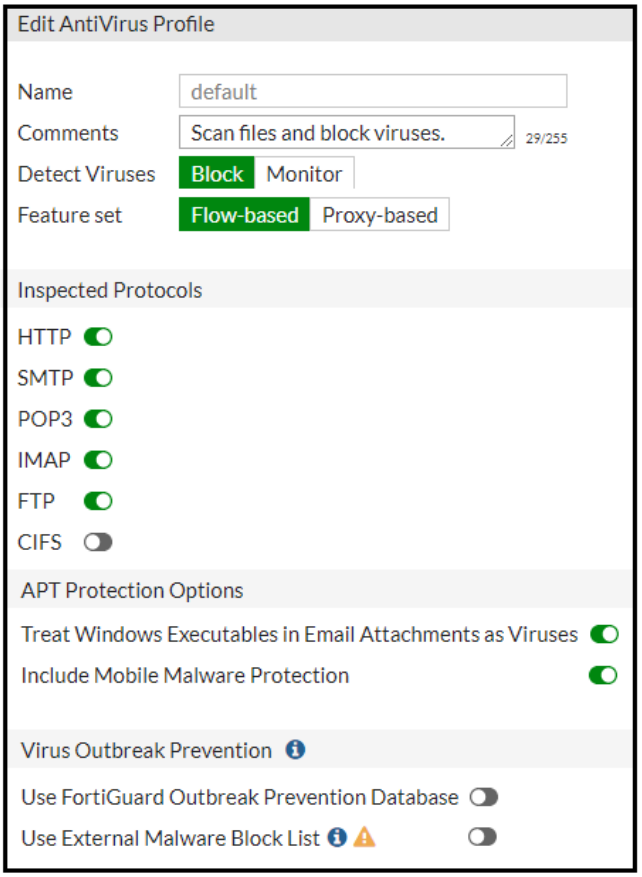


Exhibit B -



Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The volume of traffic being inspected is too high for this model of FortiGate.

B. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

C. The firewall policy performs the full content inspection on the file.

D. The flow-based inspection is used, which resets the last packet to the user.

Suggested Answer: *C*

Community vote distribution

D (100%)

Lionardo Highly Voted 3 years, 5 months ago

D is correct. FortiGate_Security_6.4 page 479

Key to rigt answer is "unable to receive a block replacement message when downloading an infected file for the first time"

upvoted 15 times

Cunawaro 3 years ago

read carefully question final part "when downloading an infected file for the first time?"

upvoted 1 times

Cunawaro 3 years ago

sorry this reply is not for u comment..

upvoted 1 times

Cunawaro Highly Voted 3 years ago

D its OK. FG-SG-6.4-P479.

• "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately

• When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

upvoted 5 times

Cunawaro 3 years ago

read carefully question final part "when downloading an infected file for the first time?"

upvoted 1 times

AMK2ENG Most Recent 8 months, 4 weeks ago

D. The flow-based inspection is used, which resets the last packet to the user

upvoted 1 times

NicolaeEast 2 years ago

Selected Answer: D

You get a block replacement after last packet is dropped, connection is reset, and identical request is made.

Fortigate security 7.0 pg 485

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: D

D é a verdadeira

upvoted 1 times

jcarlosBO 2 years, 9 months ago

Selected Answer: D

D is the correct

upvoted 3 times

mrtim5700 2 years, 9 months ago

Selected Answer: D

D is correct. In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

upvoted 2 times

Rman0059 2 years, 9 months ago

Selected Answer: D

D is correct

upvoted 2 times

yadavarya97 3 years ago

D is correct

upvoted 2 times

jmt97 3 years, 4 months ago

D is correct.

upvoted 2 times

davidone 3 years, 5 months ago

D is correct. Otherwise it should be in"proxy based" to display an instant message of blocking.

upvoted 4 times

Question #38 *Topic 1*

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dumytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

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

A. Traffic is blocked because Action is set to DENY in the firewall policy.

B. Traffic belongs to the root VDOM.

C. This is a security log.

D. Log severity is set to error on FortiGate.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

Djohan23 Highly Voted 3 years, 4 months ago

as you can see the parameter on the log view,
1. "vd=root" which means vdom is root.
2. "type=utm" which means security log event.

So, B & C is the correct answer.
upvoted 21 times

Melvin91 Most Recent 1 year, 11 months ago

Why A is wrong? Can anyone explain ?
upvoted 1 times

ariel_df 1 year, 9 months ago

Do you know why A is wrong?
upvoted 1 times

ChuckC 2 years, 2 months ago

Selected Answer: BC

FortiGate_Security_7.0_Study page 268 and 270
upvoted 2 times

juanK1982 2 years, 5 months ago

Selected Answer: BC

B & C is the correct answer
upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: BC

B e C são verdadeiras
upvoted 1 times

mario156090 2 years, 6 months ago

Selected Answer: BC

B+C is the answer.
upvoted 1 times

forti_Ctes 2 years, 12 months ago

I think B and C

upvoted 3 times

franger 3 years, 1 month ago

B and C are correct: if you pay attention to the security log web filter you can enable the UTM log but if you set the firewall policy as accepting the logs will continue to be blocked which means the answer A is not correct: https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/986892/sample-logs-by-log-type (almost in the middle you'll see web filter logs).

upvoted 2 times

FortiSherlock 3 years, 1 month ago

I was confused by this question as well. I thought A, B and C would all be obviously correct. action is blocked, vd is root and type is utm according to the log.

The tricky part is the last part of answer A, though. :-) The action in the firewall policy cannot be set to "DENY" because subtype here is "webfilter" and a webfilter does not have an action "DENY", is only has the action "BLOCK".

upvoted 3 times

2021gene 3 years ago

Perhaps Im wrong, but If you are working in policy based mode(not profile), you apply the category directly on the policy, and the only actions, are accept or deny. See FortiGate_Security_6.4_Study page 375...besides this there is part in the log where it says profile=default...that makes me think that the working mode is profile based instead of policy based, in such case I agree with you, the answer should be B, C

upvoted 2 times

wamendoza 3 years, 1 month ago

I think it's A and B

if you see the log it clearly says action = blocked and the message (msg) says "URL belongs to a denied category in a policy".

I did the practice and when I put blocked in the action in category it returns the same log.
Also, are we sure that UTM is a security log?

You can do the practice by going to web filter, blocking some category and trying to enter. Then you must execute in the CLI "execute log filter category 3 " and "execute log display" you will see the same message in the log

upvoted 1 times

Bluegrass168 3 years, 3 months ago

UTM and Root are shown on the log. So - B and C are right!

upvoted 1 times

davidone 3 years, 5 months ago

I think B and C.

upvoted 3 times

FeNadege 3 years, 5 months ago

B and C are Correct

upvoted 3 times

Question #39 *Topic 1*

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

A. FortiGate polling

B. NetAPI

C. Novell API

D. WMI

E. WinSecLog

Suggested Answer: *BDE*

Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

Community vote distribution

BDE (100%)

Lionardo Highly Voted 3 years, 5 months ago

B, D & E is correct. FortiGate_Infrastructure_6.4 page 265

upvoted 7 times

forti_Ctes Highly Voted 2 years, 12 months ago

B D & E are correct

upvoted 6 times

NicolaeEast Most Recent 2 years, 1 month ago

Selected Answer: BDE

Fortigate Infra SG 7.0 pg 255

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: BDE

B, D e E são verdadeiras

upvoted 1 times

MrSaintz 2 years, 8 months ago

Selected Answer: BDE

6.4 Infratructure Study Guide p.264

upvoted 2 times

Pierrot26 3 years ago

B, D are correct

E is correct too but not directly mentionned into https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732#:~:text=In%20polling%20mode%2C%20the%20Collector,polls%20the%20domain%20controllers%20directly.

"Extract :

2) Event log polling may run a bit slower, but will not miss events, even when the installation site has many users that require authentication.

It does not have the 10 second limit on NetAPI polling." => This is winseclog

upvoted 3 times

franger 3 years, 1 month ago

B,D and E :https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732#:~:text=In%20polling%20mode%2C%20the%20Collector,polls%20the%20domain%20controllers%20directly.

upvoted 1 times

davidone 3 years, 5 months ago

B D E are correct.

upvoted 2 times

FeNadege 3 years, 5 months ago

BDE are Correct

upvoted 2 times

Question #40 *Topic 1*

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase
2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

A. On HQ-FortiGate, enable Diffie-Hellman Group 2.

B. On HQ-FortiGate, enable Auto-negotiate.

C. On Remote-FortiGate, set Seconds to 43200.

D. On HQ-FortiGate, set Encryption to AES256.

Suggested Answer: *A*
Reference:
https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495

Community vote distribution
D (100%)

Lionardo Highly Voted 3 years, 5 months ago
D is correct. FortiGate_Infrastructure_6.4 page 230
Encryption algorithm must be the same.
upvoted 13 times

siscoFe Highly Voted 3 years, 3 months ago
D is correct, the Encryption and authentication algorithm needs to match inorder for IPSEC be successfully established
upvoted 6 times

manchrivo Most Recent 2 years, 1 month ago
D is correct
upvoted 1 times

ChuckC 2 years, 2 months ago
Selected Answer: D
Diffe-Hiellman only needs one value to match according to
https://docs.fortinet.com/document/fortigate/6.2.7/cookbook/604285/phase-2-configuration which makes A wrong
upvoted 1 times

maxhoman 2 years, 4 months ago
Selected Answer: D
D is correct
upvoted 1 times

mario156090 2 years, 6 months ago
D is the answer.
upvoted 1 times

Nirvanero94 2 years, 6 months ago
Selected Answer: D
D, es correcta, deben coincidir los 2 metodos de encripción para subir la fase 2. Comprobado
upvoted 2 times

Flo31 2 years, 8 months ago
Selected Answer: D
D is correct
upvoted 2 times

BIGRAOU 2 years, 9 months ago
Selected Answer: D

FortiGate_Infrastructure_6.4_Study_Guide-Online, PAGE 230
Phase 2 - Phase 2 proposal
upvoted 2 times

mrtim5700 2 years, 9 months ago

Selected Answer: D

This is presented as one right answer, so I will treat it as that.
D is correct, if the encryption proposals don't match, it is not going to come up.
However, if this were my set up, I'd make PFS and lifetime match as well.
upvoted 3 times

reih89 2 years, 9 months ago

Are Two correct Answer, AD
upvoted 1 times

lrosadini 2 years, 7 months ago

both have group 5
upvoted 2 times

mrigen888 3 years ago

D is correct
upvoted 4 times

Datahive 3 years, 3 months ago

D is correct
upvoted 2 times

Bluegrass168 3 years, 3 months ago

D is right. But also want to confirm one thing:
Is any one of the DH group matched will also allow to bring up the P2? assumed others matched already.
upvoted 1 times

G33 3 years, 4 months ago

D is correct
upvoted 2 times

davidone 3 years, 5 months ago

D is correct
upvoted 1 times

Xillar 3 years, 5 months ago

D is the correct answer
upvoted 3 times

Vespucci 2 years, 9 months ago

D is the correct answer
upvoted 1 times

Question #41 *Topic 1*

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source field of a firewall policy?

A. IP address

B. Once Internet Service is selected, no other object can be added

C. User or User Group

D. FQDN address

Suggested Answer: *C*
Reference:
https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

Community vote distribution
C (100%)

siscoFe Highly Voted 3 years, 3 months ago
C is correct, I have just confirmed this on a Production Fortigate FW and you can add user/User group but you cannot add Address group with ISDB object. It will simply show a red highlighted error which is read as "Addresses/groups cannot be mixed with Internet Services'
upvoted 22 times

G33 Highly Voted 3 years, 3 months ago
B is correct. If your try adding anything else you get an error
upvoted 9 times

G33 3 years, 1 month ago
C is actually the correct ans.
if src: you can add user, if dst: you cannot add any other object
upvoted 8 times

wwwwaaaa 10 months, 1 week ago
Correct, it is C, just lab tested it
upvoted 1 times

NicolaeEast Most Recent 2 years ago
Selected Answer: C
C.

You can't mix ISDB objects with regular address objects. User objects are not restricted in any way.

Fortigate Security 7.0 pg 117
upvoted 1 times

mob9 2 years, 1 month ago
Selected Answer: C
C is correct and tested (user added and user group are added to policy but ip address or network failed to add) Version 7.0.5
upvoted 3 times

SandroAlex 2 years, 5 months ago
Selected Answer: C
C é a verdadeira
upvoted 1 times

hume2022 2 years, 6 months ago
I think it's "C"

Service : This option is only available when Destination Internet Service is off.
So if you are on source you should be able to add users and groups, I didn't test but as per theory that is what is looks like.

https://docs.fortinet.com/document/fortimanager/6.2.1/administration-guide/663598/create-new-firewall-policy
upvoted 1 times

Wachiturro 2 years, 6 months ago
Addresses/groups cannot be mixed with Internet Services

For this reason the answer is the C
upvoted 1 times

aandreou020 2 years, 7 months ago
I have tested B is correct
upvoted 2 times

aandreou020 2 years, 7 months ago
Sorry C is correct . On the Source you can have Users+ Groups but not on the Destination
upvoted 2 times

lrosadini 2 years, 7 months ago
C - you can add USER if you are unig in source.
FortiGate Security 6.4 Study Guide - pag 109
upvoted 2 times

Rman0059 2 years, 9 months ago
Selected Answer: C
C is correct
upvoted 3 times

viestner 3 years ago
B. You CANNOT mix regular address objects with ISDB objects, and you CANNOT select services on a firewall policy
upvoted 1 times

viestner 3 years ago
Sorry, its C. User/group can be selected only on source, not destination.
upvoted 4 times

FortiSherlock 3 years, 1 month ago
A and D are not correct for a very simple reason: The internet service dictates them already. If you choose AWS-Web als the service, then AWS has a fixed set of IP addresses and domain names that define them. Makes no sense to say I want to block AWS on Google.com or something like this. If it is Google.com it is not AWS anymore.
C is correct and makes sense - I want to block AWS, but only for certain users in my company.
upvoted 2 times

jarz 3 years, 1 month ago
Correct answer is A. "You CANNOT mix regular address objects with ISDB objects, and you CANNOT select services on a firewall policy." Direct quote from Security 6.4 study guide page 109.
upvoted 1 times

ChuckC 2 years, 2 months ago
You quoted "You CANNOT mix regular address objects with ISDB objects,". That eliminates A
upvoted 1 times

Amrani 3 years, 2 months ago
C is the correct answer.
upvoted 1 times

jarz 3 years, 2 months ago
The correct Answer is A, you CAN add user/groups if you have added Internet Service as a Source. You CAN'T add (IP) addresses or address groups in the Source if you have Internet Service there also. I just tested this in a VM instance of a FG.
upvoted 1 times

ChuckC 2 years, 2 months ago
Aren't they asking which ones you can add
upvoted 1 times

Zaiderr 3 years, 3 months ago
C is correct, You can give it a try, HAND ON LAB

upvoted 3 times

Djohan23 3 years, 4 months ago

C is Correct. You can prove it by configuring it on FortiGate.

upvoted 2 times

Question #42 *Topic 1*

Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Suggested Answer: *BC*

Community vote distribution

CD (100%)

aads Highly Voted 3 years, 4 months ago
The key here is performing the task without affecting any of the other services.
- Not A - Changing the maximum TTL value for TELNET will affect every other policy that references the TELNET service
- Not B - Changing the session TTL on the SSLVPN policy will impact other services referenced in the policy.

Hence the answer is C and D
upvoted 40 times

Biz90 3 years, 4 months ago
aads, awesome work! I was sitting here for a good 15 minutes thinking those answers are wrong, and trying think why! I agree C and D are correct
upvoted 3 times

Ibrahimadwan Most Recent 1 year, 3 months ago
C & D is correct
upvoted 1 times

cierzo 2 years ago
Selected Answer: CD
C & D is correct
upvoted 1 times

ibos8383 2 years, 5 months ago
Selected Answer: CD
the answer is c and d
upvoted 1 times

hippo2048 2 years, 6 months ago
Selected Answer: CD
agree with aads
upvoted 2 times

mario156090 2 years, 6 months ago
C and D is the answer.
upvoted 2 times

yaboi01 2 years, 8 months ago

how do you change the TTL on a service object???
upvoted 1 times

SandroAlex 2 years, 5 months ago
In CLI, config firewall service custom
upvoted 1 times

Flo31 2 years, 8 months ago
Selected Answer: CD
C & D is correct
upvoted 1 times

forti_Ctes 2 years, 12 months ago
c & D correct
upvoted 1 times

5pik3 3 years ago
c & d. No doubt.
upvoted 1 times

mrigen888 3 years ago
c and d is correct
upvoted 1 times

salon442 3 years, 3 months ago
c and d is correct
upvoted 1 times

salon442 3 years, 3 months ago
yeah c and d is correct
upvoted 1 times

darkMmve 3 years, 4 months ago
A and B are correct. Under service objects you can do set session-TTL 0 or just increase it
upvoted 2 times

francis57 3 years, 4 months ago
A is wrong as we have "without affecting services running through FortiGate". So we need to create a new service and put it to this rule only.
upvoted 2 times

Question #43 *Topic 1*

Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage

B. Automated Response

C. Security Posture

D. Optimization

Suggested Answer: *C*
Reference:
https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-best-practices.pdf

Lionardo Highly Voted 3 years, 5 months ago
C is correct. FortiGate_Security_6.4 page 90
upvoted 13 times

Corynth Most Recent 2 years, 6 months ago
Description of the three major scorecards is seen in Security fabric > Security rating>Security posture.
Security Posture
Identify configuration weaknesses and best practice violations in your deployment.
Fabric Coverage
Identify in your overall network, where Security Fabric can enhance visibility and control.
Optimization
Optimize your fabric deployment.
upvoted 1 times

onaicul 3 years, 2 months ago
Yes C is correct - Secutiry fabric > Security rating>Security posture
FortiGate_Security_6.4 page 90
upvoted 3 times

Question #44 *Topic 1*

What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > System uptime > Priority > FortiGate Serial number

B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number

C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number

D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Suggested Answer: *B*
Reference:
http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html

Community vote distribution
B (100%)

jarz Highly Voted 3 years, 2 months ago
PUPS - Ports/Uptime/Priority/Serial
upvoted 31 times

NicolaeEast 2 years, 1 month ago
Beautiful - makes it easy
upvoted 1 times

FeNadege Highly Voted 3 years, 5 months ago
B is Correct
upvoted 9 times

johnnd Most Recent 2 years ago
Selected Answer: B
With Override disable (default) is B.
https://i.imgur.com/Q75ApJu.png
upvoted 1 times

ChuckC 2 years, 2 months ago
B is correct FortiGate_Infrastructure_7.0 page 304
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: B
B é a verdadeira
upvoted 1 times

blvackhammer 2 years, 7 months ago
B is correct. FortiGate_Infrastructure_6.4 page 314
upvoted 1 times

alexilc 2 years, 10 months ago
IT´s C, Infraestructure pag 315
Connected - Priority -HA - Serial
upvoted 1 times

MrSaintz 2 years, 8 months ago
You failed to read the question, that's what you can do with override enabled, but the question is about override disabled, B is correct.
upvoted 2 times

KemalM 2 years, 11 months ago
Answer: B
Fortigate Infrastructure 7.0 Study Guide P.319
upvoted 3 times

onaicul 3 years, 2 months ago

Yes B is correct. FortiGate_Infrastructure_6.4 page 314.

Warning: If HA override setting is enable, correct is C - > FortiGate_Infrastructure_6.4 page 315

upvoted 5 times

Ishan_Dis 3 years, 4 months ago

Answer B. FortiGate_Infrastructure_6.4 page 314

upvoted 3 times

Lionardo 3 years, 5 months ago

B is correct. FortiGate_Infrastructure_6.4 page 314

upvoted 5 times

Refer to the exhibit.

Exhibit A -

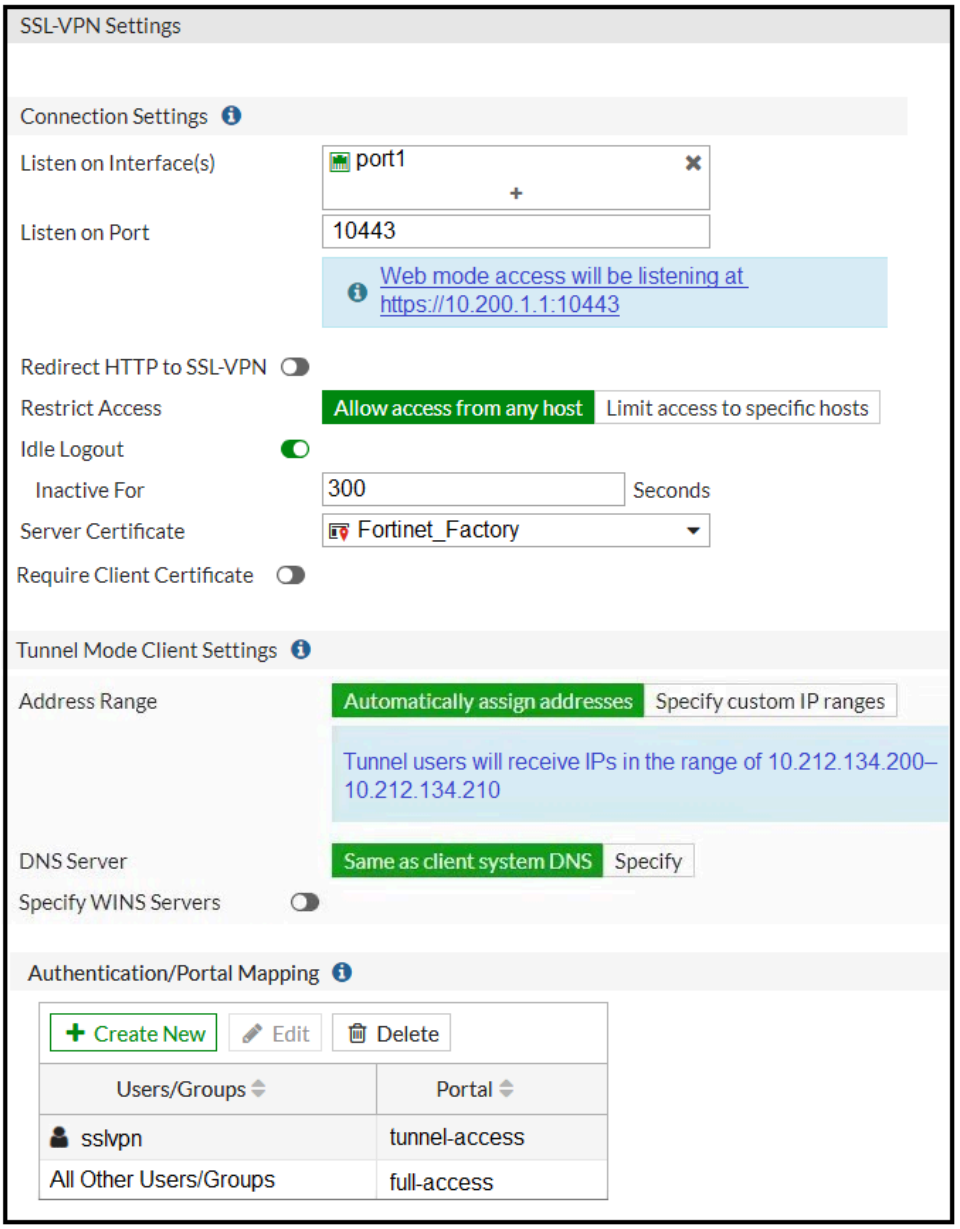


Exhibit B -

The SSL VPN connection fails when a user attempts to connect to it.
What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.

B. Change the Server IP address.

C. Change the idle-timeout.

D. Change the SSL VPN portal to the tunnel.

Suggested Answer: *A*

Reference:

https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494

Community vote distribution

A (100%)

FeNadege Highly Voted 3 years, 5 months ago

A is Correct because in exhibit, port is 10443

upvoted 18 times

Dash00 Most Recent 2 years, 4 months ago

Selected Answer: A

A - exhibit, port is 10443 and on client is 1443

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: A

A é a verdadeira

upvoted 1 times

kemi01 2 years, 6 months ago

YES, portal port is 10443 not 1443

upvoted 1 times

onaicul 3 years, 2 months ago

A is correct, port exibit is 1443 port correct is 10443.

upvoted 3 times

Ishan_Dis 3 years, 4 months ago

Check the last exibit. Port should be 10443

upvoted 4 times

Question #46 *Topic 1*

Which three statements are true regarding session-based authentication? (Choose three.)

A. HTTP sessions are treated as a single user.

B. IP sessions from the same source IP address are treated as a single user.

C. It can differentiate among multiple clients behind the same source IP address.

D. It requires more resources.

E. It is not recommended if multiple users are behind the source NAT

Suggested Answer: *ACD*

Community vote distribution

ACD (100%)

Lionardo Highly Voted 3 years, 5 months ago

A, C & D is correct. FortiGate_Infrastructure_6.4 page 387

upvoted 7 times

siscoFe Highly Voted 3 years, 3 months ago

ACD is correct, For A:Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSSO, local database etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.

upvoted 7 times

SandroAlex Most Recent 2 years, 5 months ago

Selected Answer: ACD

A, C e D são verdadeiras

upvoted 1 times

forti_Ctes 2 years, 12 months ago

A, C & D arre correct

upvoted 3 times

Ishan_Dis 3 years, 4 months ago

ACD, Infra page 33

upvoted 3 times

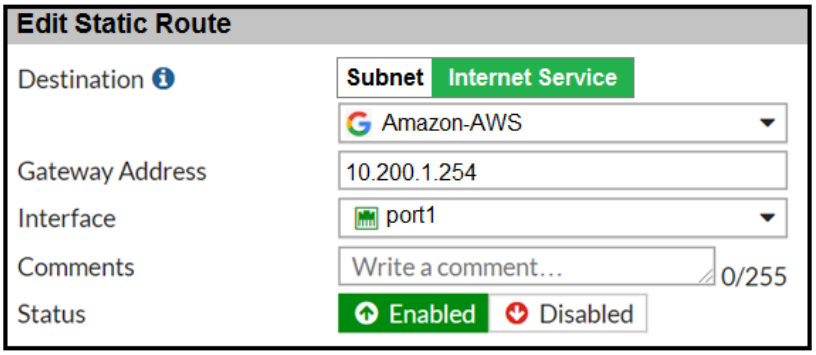
davidone 3 years, 5 months ago

A, C and D are correct. Refers to Web proxy authentication and authorization. IP based and Session based authentication.

upvoted 1 times

Question #47 *Topic 1*

Refer to the exhibit, which contains a static route configuration.



An administrator created a static route for Amazon Web Services.
What CLI command must the administrator use to view the route?

A. get router info routing-table all

B. get internet service route list

C. get router info routing-table database

D. diagnose firewall proute list

Suggested Answer: *D*
Reference:
https://www.fortinetguru.com/2019/09/troubleshooting-sd-wan-fortios-6-2/

Community vote distribution
D (71%) A (29%)

tax Highly Voted 3 years, 2 months ago
ISDB static route will not create entry directly in routing-table.
ISDB is acting as policy route. So to verify ISDB route: check https://kb.fortinet.com/kb/documentLink.do?externalID=FD44627
upvoted 9 times

KemalM Highly Voted 2 years, 11 months ago
Answer: D
Fortigate Infrastructure 7.0 Study Guide P.55
upvoted 5 times

ChuckC 2 years, 2 months ago
It's actually Page 56
upvoted 1 times

Diego_Farani Most Recent 9 months, 3 weeks ago
Selected Answer: D
ISDB static route will not create entry directly in routing-table.

Reference:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640

FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table.
As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."
upvoted 1 times

Diego_Farani 9 months, 4 weeks ago
Selected Answer: A

Please pay attention! The answer is A

diag firewall proute list --->>> list route policy info

get router info routing-table <keyword> --->>> Use this command to display the routes in the routing table.

https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/372042/router-info-routing-table

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Diagnostic-commands-to-check-the-status-of-the-SD/ta-p/194246

upvoted 1 times

Diego_Farani 10 months, 1 week ago

Selected Answer: D

A correta é a "D".
Justificativa abaixo:
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

upvoted 1 times

eldeivid8701 1 year, 10 months ago

Replique la pregunta y la A no funciona en cambio la D si entonces no hay nada que discutir

upvoted 1 times

SandroAlex 2 years, 5 months ago

Selected Answer: D

D é a verdadeira, testado no firmware 6.4.0

upvoted 1 times

jccxx 2 years, 6 months ago

This is indeed a static route, but a static route using an ISDB address, and therefore not added to the (ordinary) routing table but to the policy routing table.
Fortigate Infrastructure 6.4 page 56

upvoted 1 times

daxrob 2 years, 6 months ago

Selected Answer: D

This is not a static route. It is a policy route, therefore only the D command is able to show you the route.

upvoted 1 times

jlguillen 2 years, 6 months ago

D is correct because this is a ISDB route, not a static route. ISDB route has more preference than static route. The cli command to view the ISDB routes or Policy routes is D.

upvoted 2 times

python_tamer 2 years, 6 months ago

Selected Answer: D

Answer is D.

upvoted 1 times

Joalmici 2 years, 6 months ago

Selected Answer: A

A is Corret
https://docs.fortinet.com/document/fortigate/6.0.0/cli-reference/372042/router-info-routing-table

upvoted 1 times

Djohan23 3 years, 4 months ago

D is Correct.
You can find the answer on Routing module on "Policy Routes and ISDB Routes" section.

upvoted 4 times

Ishan_Dis 3 years, 4 months ago

diagnose firewall proute list
Answer is D

upvoted 4 times

RedTeamYoda 3 years, 4 months ago

D is correct - FortiGate_Infrastructure_6.4 pages 56

proute database

upvoted 3 times

aads 3 years, 4 months ago

The Answer is D.

ISDB routes are policy routes

upvoted 5 times

luissanchezleon 3 years, 4 months ago

is D

FortiGate_Infrastructure_6.4 pages 56

upvoted 4 times

Question #48 *Topic 1*

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

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

D. Redundant interface

Suggested Answer: *C*
Reference:
https://www.fortinetguru.com/2016/12/aggregate-interfaces/

Ishan_Dis Highly Voted 3 years, 4 months ago
Answer is C
Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces with the only noticeable effect being a reduced bandwidth.
upvoted 10 times

Inc Most Recent 2 years, 7 months ago
C Link Aggregation FortiGate_Security_6.4_Pag 37
upvoted 1 times

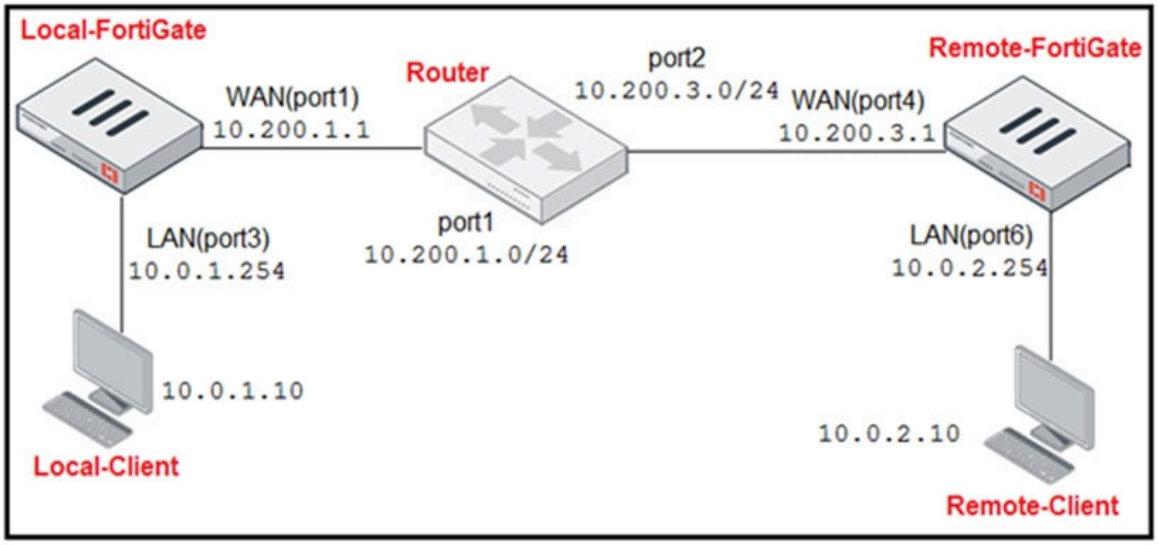
siscoFe 3 years, 3 months ago
C will be used to aggregate multiple physical/Ethernet interfaces in order to get the advantage of combined bandwidth of all member interfaces as well as a redundancy where a faulty interface won't create a failure on the whole link as the aggregate interface will stay active with the remaining working members of the link aggregation.
upvoted 1 times

Bluegrass168 3 years, 3 months ago
increase network bandwidth - LACP - Link aggregation.
The answer is C.
upvoted 1 times

FeNadege 3 years, 5 months ago
C is Correct
upvoted 3 times

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

+ Create New | Edit | Delete | Search

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

+ Create New | Edit | Clone | Delete | Search

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49-10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149-10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload	Enabled

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration.
The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1).
Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.149

B. 10.200.1.1

C. 10.200.1.49

D. 10.200.1.99

Suggested Answer: *D*

Community vote distribution

D (100%)

Lionardo Highly Voted 3 years, 5 months ago

D is correct.

Ping is ICMP protocol - protocol number = 1

=> SNAT policy ID 1 is policy that used.

=> Translated address is "SNAT-Remote1" that 10.200.1.99

upvoted 29 times

MetDaci 2 years, 5 months ago

Good explanation, thank you!

upvoted 2 times

SandroAlex Most Recent 2 years, 5 months ago

Selected Answer: D

D é a verdadeira

upvoted 1 times

ItVik 2 years, 5 months ago

This question was changed for me, Instead of SNAT. It was with NAT on outgoing traffic with IP Pool configured and Inbound with VIP configured.

The question has been asked what will be the NAT IP when traffic will go out to the internet from the machine inside the network. So choose the option of IP from IP Pool congigured. = 10.200.0.10 (i think may be i forget the IP but just check out the IP pool)

upvoted 1 times

Ragnar77 2 years, 6 months ago

Selected Answer: D

ping is ICM

upvoted 1 times

davidone 3 years, 5 months ago

D is correct.

upvoted 4 times

FeNadege 3 years, 5 months ago

D is Correct

upvoted 3 times

Question #50 *Topic 1*

An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.
What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.

B. The administrator must use a FortiAuthenticator device.

C. The administrator can use a third-party radius OTP server.

D. The administrator must use the user self-registration server.

Suggested Answer: *C*

Community vote distribution

B (100%)

Lionardo Highly Voted 3 years, 5 months ago
B is correct. FortiGate_Security_6.4 page 207
upvoted 15 times

Xillar Highly Voted 3 years, 5 months ago
B is correct due to the FortiToken, a different OTP cannot use FortiToken. So we have to choose the fortiAuthenticator
upvoted 7 times

ChuckC Most Recent 2 years, 2 months ago
Selected Answer: B
B is correct but the best explanation I found was in FortiGate_Security_7.0 page 216
upvoted 1 times

SandroAlex 2 years, 5 months ago
Selected Answer: B
B é a verdadeira
upvoted 1 times

Corynth 2 years, 6 months ago
B is correct. FortiGate_Security_7.0 page 212
upvoted 1 times

Flo31 2 years, 8 months ago
Selected Answer: B
B is correct.
upvoted 1 times

mrtim5700 2 years, 9 months ago
Selected Answer: B
B is correct. If you want to have one FortiToken assigned to multiple sites, FortiAuthenticator is required. 3rd party RADIUS is possible with things like DUO, but the key items here is FORTITOKEN.
upvoted 3 times

Rman0059 2 years, 9 months ago
Selected Answer: B
B is correct
upvoted 2 times

ayon35 3 years, 2 months ago
B is the correct answer
upvoted 2 times

Bluegrass168 3 years, 3 months ago
B - FAC can share Token to lots of Fprtigate via Radius Auth.
upvoted 4 times

Question #51 *Topic 1*

Refer to the exhibit.

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a
packet (proto=1, 10.0.1.10:1->10.200.1.254:2048) from port3. type=8, code=0,
id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a
new session-00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a
route: flag=04000000 gw-10.200.1.254 via port1"
id=20084 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward
policy check (policy 0)"
```

Why did FortiGate drop the packet?

A. It matched an explicitly configured firewall policy with the action DENY.

B. The next-hop IP address is unreachable.

C. It failed the RPF check.

D. It matched the default implicit firewall policy.

Suggested Answer: *D*

Community vote distribution

D (100%)

moneim Highly Voted 3 years ago

Answer is "D". If it was dropped by RPF, the log would've been "reverse path check fail, drop"

See KB ==> https://kb.fortinet.com/kb/documentLink.do?externalID=FD31702

upvoted 9 times

zqrni 3 years ago

agreed

upvoted 1 times

zqrni Highly Voted 3 years ago

The answer is D:

Root causes for "Denied by forward policy check"
1- There is no firewall policy matching the traffic that needs to be routed or forwarded by the FortiGate (Traffic will hit the Implicit Deny rule)
2- The traffic is matching a DENY firewall policy
3- The traffic is matching a ALLOW firewall policy, but DISCLAIMER is enabled, in this case, traffic will not be accepted unless end user will accept the HTTP disclaimer purposed by Fortigate while browser external site.
In this case we are in the first situation because at the end of the log it says policy 0.
For more details check the link:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD31702

upvoted 6 times

SandroAlex Most Recent 2 years, 5 months ago

Selected Answer: D

D é a verdadeira

upvoted 1 times

kemi01 2 years, 6 months ago

Default policy (policy 0) ,hence answer D is correct

upvoted 2 times

steef1982 3 years ago

I believe its D: Implicit Deny = “policy 0”

upvoted 5 times

yadavarya97 3 years ago

C.. failed bcoz of reverse path forwarding check

upvoted 2 times