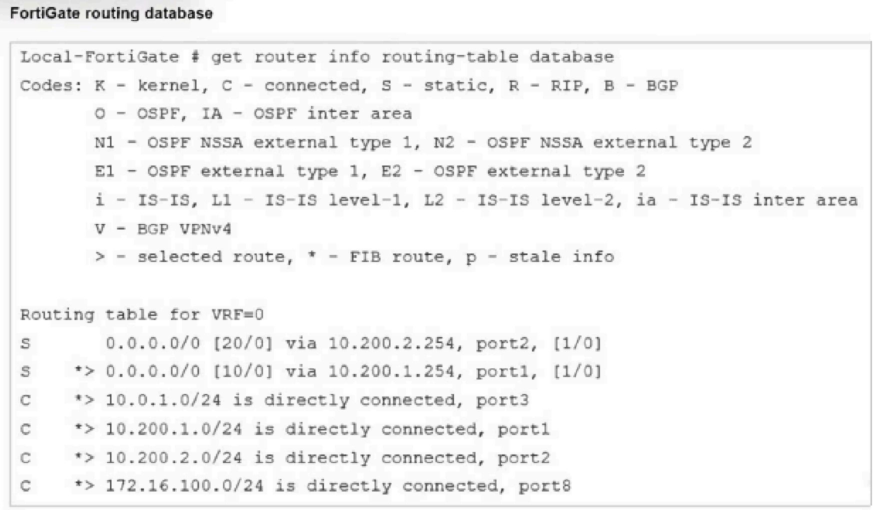
Question #1 Topic 1

Refer to the exhibit.



FortiGate routing database

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [1/0]
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
C     *> 172.16.100.0/24 is directly connected, port8
```

Which two statements are true about the routing entries in this database table? (Choose two.)

A. All of the entries in the routing database table are installed in the FortiGate routing table.

B. The port2 interface is marked as inactive.

C. Both default routes have different administrative distances.

D. The default route on port2 is marked as the standby route.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

yiyan 1 month, 3 weeks ago

Selected Answer: CD

Both are correct.

upvoted 2 times

montonearm 1 month, 3 weeks ago

Selected Answer: CD

Le due affermazioni corrette sono:

C. Both default routes have different administrative distances.
(Confermato: 10 per port1 e 20 per port2).

D. The default route on port2 is marked as the standby route.
(Confermato: La rotta su port2 è considerata standby poiché ha una distanza amministrativa maggiore rispetto a port1).

upvoted 2 times

rigonet 2 months, 3 weeks ago

Selected Answer: CD

Correct Answers:
C. Both default routes have different administrative distances.
D. The default route on port2 is marked as the standby route.

A. Incorrect: Not all routes are installed; only those marked with *.
B. Incorrect: Port2 is active but not the primary route.
C. Correct: Port1 has an administrative distance of 10, Port2 has 20.
D. Correct: Port2's route is a backup due to its higher administrative distance.

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: CD

Administrative distance are different 20/0 and 10/0

there is an ECMP route and the port2 link is UP, so is not inactive, it keeps in standby

upvoted 2 times

ablongo 3 months, 3 weeks ago

C is not true, it is false. Both entries has 1 as administrative distance. And if both are 1 they are not different!!!

A is false too.

So

Answers B&D are correct.

upvoted 1 times

> **ablongo** 3 months, 2 weeks ago
>
> Sorry, my mistake. C is correct.
>
> [20/0] means Administrative Distance while [1/0] means preference.
>
> upvoted 1 times

> **renauyd** 3 months, 2 weeks ago
>
> Administrative distance is the first number after the destination 0.0.0.0/0, which is 20 and 10.
>
> "[20/0]
>
> 20 indicates an administrative distance of 20 out of a range of 0 to 255. 0 is an additional metric associated with this route, such as in OSPF."
>
> upvoted 1 times

BartvanHees 3 months, 4 weeks ago

Selected Answer: CD

C&D are correct

upvoted 2 times

s4mu3l007 4 months, 1 week ago

C&D correct

upvoted 2 times

Popenemo123 5 months, 1 week ago

C,D correct

upvoted 2 times

mateusj11 5 months, 2 weeks ago

Selected Answer: CD

C and D

upvoted 2 times

gimy19 6 months, 2 weeks ago

C,D are correct

upvoted 3 times

terminatoritsec 6 months, 2 weeks ago

Selected Answer: CD

C and D are Correct

upvoted 3 times

Question #2 *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 host field in the HTTP header.

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

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

D. The subject field in the server certificate.

E. The serial number in the server certificate.

Suggested Answer: *BCD*

rigonet 2 months, 3 weeks ago

Selected Answer: BCD

Correct Answers:
B. The server name indication (SNI) extension in the client hello message.
C. The subject alternative name (SAN) field in the server certificate.
D. The subject field in the server certificate.

Key Points:
B: SNI identifies the hostname in the TLS handshake.
C: SAN field specifies the hostname in the certificate.
D: Subject field may also contain the hostname.
A and E: Not relevant for hostname identification.

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: BCD

SNI
Subject in the certificate
Subject alternative name in the certificate

upvoted 2 times

vuhidus 3 months, 3 weeks ago

Selected Answer: BCD

B C D are correct

upvoted 2 times

s4mu3l007 4 months, 1 week ago

BCD are correct

upvoted 2 times

hassan76 4 months, 1 week ago

FortiGate_7.4_Administrator_Study_Guide 166

upvoted 2 times

miguelmagr 5 months, 2 weeks ago

B,C,D - Related to Training Fortigate Administrator - Certificate Operations:

When using SSL certificate inspection, FortiGate is not decrypting the traffic. During the exchange of hello messages at the beginning of an SSL handshake, FortiGate parses the server name indication (SNI) from client Hello, which is an extension of the TLS protocol. The SNI tells FortiGate the hostname of the SSL server, which is validated against the DNS name before receipt of the server certificate. If there is no SNI exchanged, then FortiGate identifies the server by the value in the server by the value in the Subject field or SAN (Subject Alternative Name) field in the server certificate.

upvoted 3 times

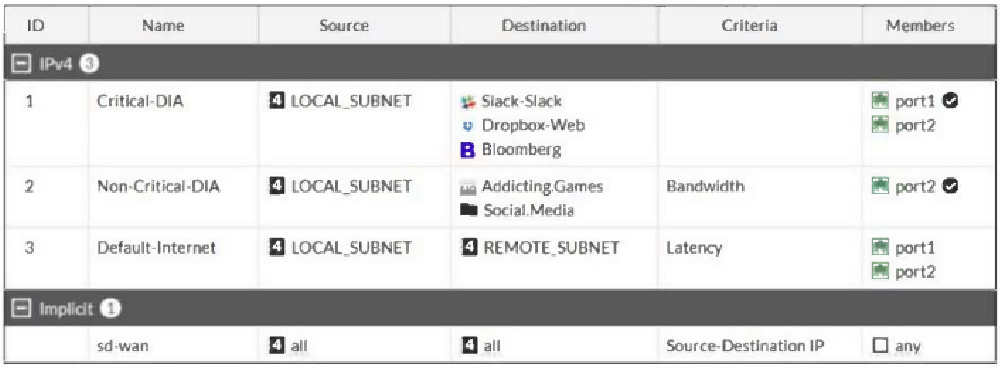
gimy19 5 months, 3 weeks ago

B,C,D are correct

upvoted 3 times

Question #3 *Topic 1*

Refer to the exhibit.



ID	Name	Source	Destination	Criteria	Members
⊟ IPv4 3					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 ✓ port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media	Bandwidth	port2 ✓
3	Default-Internet	LOCAL_SUBNET	REMOTE_SUBNET	Latency	port1 port2
⊟ Implicit 1					
	sd-wan	all	all	Source-Destination IP	□ any

Which algorithm does SD-WAN use to distribute traffic that does not match any of the SD-WAN rules?

A. All traffic from a source IP to a destination IP is sent to the same interface.

B. Traffic is sent to the link with the lowest latency.

C. Traffic is distributed based on the number of sessions through each interface.

D. All traffic from a source IP is sent to the same interface

Suggested Answer: *A*

Community vote distribution

A (100%)

rigonet 2 months, 3 weeks ago

Selected Answer: A

Correct Answer: A. All traffic from a source IP to a destination IP is sent to the same interface.

Explanation of each option:

A. Correct: Default behavior is source-destination IP-based hashing for consistency.
B. Incorrect: Latency-based routing requires a matching SD-WAN rule.
C. Incorrect: Session-based distribution is not default behavior.
D. Incorrect: Routing considers both source and destination IPs, not just source IP.

upvoted 2 times

f3eb371 3 months, 1 week ago

Selected Answer: A

A, is correct answer!

upvoted 4 times

sxcap 3 months, 1 week ago

Selected Answer: A

if no sdwan rules are matched, traffic is routed by the implicit rule, which in this case, says that traffic is routed by source - destination, it does mean that all traffic from the same source and destination IP's is routed by the same initial interface

upvoted 3 times

vuhidus 3 months, 3 weeks ago

Selected Answer: A

A answer

upvoted 2 times

OkoJun 4 months ago

A is correct because the implicit rule was set as the source and destination criteria

upvoted 3 times

262cfa1 4 months, 1 week ago

D is correct

upvoted 1 times

s4mu3l007 4 months, 1 week ago

A is correct

upvoted 3 times

herlock_sholmes_2810 5 months, 3 weeks ago

Why not D? Based that "Source-IP" is the default load balancing algorithm?

upvoted 2 times

f3eb371 3 months, 1 week ago

In the implicit rule "criteria" field, it indicates how the SDWAN treats traffic without an implicit distillation: "Source-Destination IP"

upvoted 2 times

lenriquereyes 5 months, 3 weeks ago

Selected Answer: A

https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/216765/implicit-rule

Traffic is divided equally between the interfaces. Sessions that start at the same source IP address and go to the same destination IP address use the same path.

upvoted 2 times

gimy19 6 months ago

Guys, it's easy..."is douesn't match any of the sdwan rules... will match the implicit rule and the algorithm is source-destination ip, so the answer in A

upvoted 3 times

TIGERZ44 6 months, 1 week ago

If you log into a firewall, you'll see the following options:
"Source IP" is the default setting.

Source IP:
Traffic is divided equally between members. Sessions that start at the same source address use the same route.

Sessions:
The traffic is distributed based on the number of sessions that are connected through the member.

Spillover:
The highest priority member is used until bandwidth exceeds ingress and egress thresholds. Additional traffic is sent through the next SD-WAN member.

Source-Destination IP:
Traffic is divided equally. Sessions that start at the same source IP address and go to the same destination IP address use the same route.

Volume:
The workload is distributed based on the number of packets that are going through the member.

upvoted 1 times

AlainC 1 month ago

Default setting is "Source" IP, however, on the screenshot presented, criteria is source-Destination, so Answer is A

upvoted 1 times

andres8h 6 months, 1 week ago

Selected Answer: A

A es correcto

upvoted 2 times

gimy19 6 months, 2 weeks ago

A is correct

upvoted 2 times

Question #4 *Topic 1*

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.
Which IPsec Wizard template must the administrator apply?

A. Remote Access

B. Site to Site

C. Dial up User

D. Hub-and-Spoke

Suggested Answer: *A*

Community vote distribution

A (100%)

rigonet 2 months, 3 weeks ago

Selected Answer: A

Correct Answer: A. Remote Access

Explanation of each option:

A. Remote Access (Correct): This template is designed for employees or devices accessing the network from remote locations, such as a traveling sales employee.
B. Site to Site (Incorrect): Used to connect two fixed networks, not for individual remote users.
C. Dial up User (Incorrect): Refers to legacy remote access methods, not modern IPsec VPN setups.
D. Hub-and-Spoke (Incorrect): Used to interconnect multiple branch offices to a central hub, not for individual remote users.

upvoted 1 times

krage304 3 months, 1 week ago

Selected Answer: A

Possible Template types are Site to Site, Hub-and-Spoke, Remote Access or Custom

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: A

Remote Access Wizard

upvoted 2 times

33b7b9e 3 months, 2 weeks ago

Selected Answer: C

It says IPSEC VPN for a user so it would be C - look the templates

upvoted 1 times

killer843 3 months ago

dans les wizard tu as trois type de VPN IPSEC à savoir:
-Site to Site
-Hub and Spoke
-Remote access

upvoted 1 times

s4mu3l007 4 months, 1 week ago

A is the answer

upvoted 2 times

gimy19 6 months ago

A is correct

upvoted 4 times

TIGERZ44 6 months, 1 week ago

Selected Answer: A

A is correct. When you go to VPN>IPsec Wizard and select the VPN setup, you'll see Remote Access for this type of connection

upvoted 3 times

⊟ 👤 **andres8h** 6 months, 1 week ago

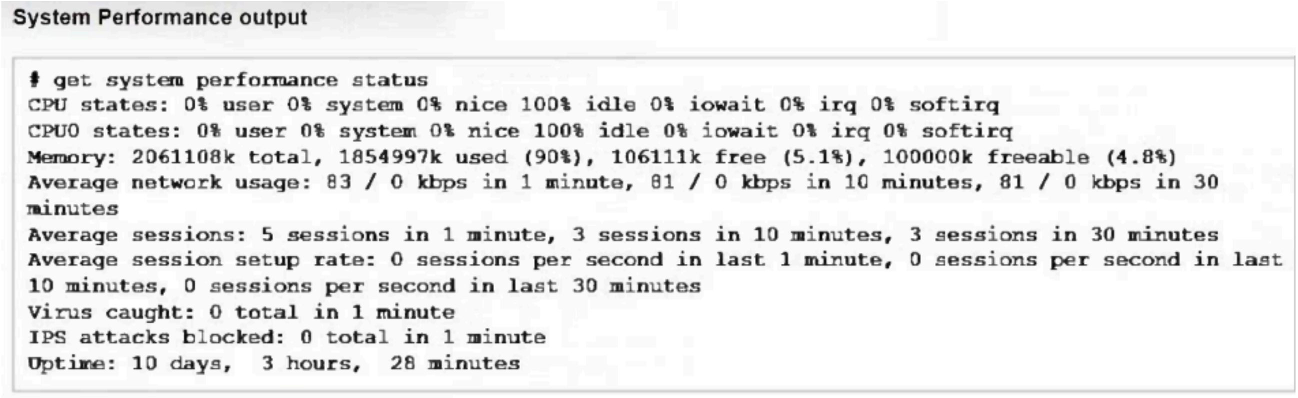
Selected Answer: A

A is correct

upvoted 3 times

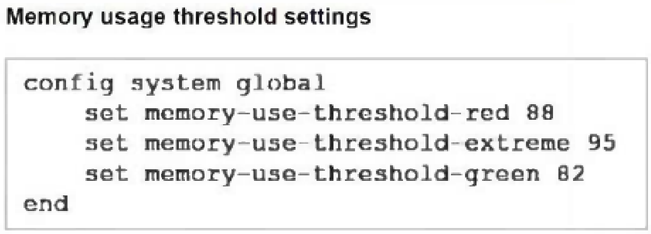
Question #5 Topic 1

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.



System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```



Memory usage threshold settings

```
config system global
     set memory-use-threshold-red 88
     set memory-use-threshold-extreme 95
     set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

A. FortiGate will start sending all files to FortiSandbox for inspection.

B. FortiGate has entered conserve mode.

C. Administrators cannot change the configuration.

D. Administrators can access FortiGate only through the console port.

Suggested Answer: *BC*

Community vote distribution

BC (100%)

bin00010111 Highly Voted 5 months, 3 weeks ago

B and C, conserve mode

upvoted 6 times

rigonet Most Recent 2 months, 3 weeks ago

Selected Answer: BC

Correct Answers:

B. FortiGate has entered conserve mode.

C. Administrators cannot change the configuration.

A: Incorrect. FortiSandbox behavior is unrelated to high memory usage.

B: Correct. Memory usage exceeded the red threshold (88%), triggering conserve mode.

C: Correct. Some configurations are restricted during conserve mode.

D: Incorrect. Console-only access happens at the extreme threshold (95%), which hasn't been reached.

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: BC

After the 88% set as "red", FortiGate sets in Conserve Mode, but you can yet access it by configured methods like Https or SSH if enabled

upvoted 3 times

212228 3 months, 3 weeks ago

Selected Answer: BC

due to conserve mode don't allow to make changes.

upvoted 3 times

⊟ **s4mu3l007** 4 months, 1 week ago

B & C correct

upvoted 2 times

⊟ **miguelmagr** 5 months, 1 week ago

Selected Answer: BC

Fortigate enter in conserve mode for that reason you cannot make changes.

upvoted 3 times

⊟ **herlock_sholmes_2810** 5 months, 2 weeks ago

Selected Answer: BC

Answer: B. and C.

It configured "set memory-use-threshold-red 88", so when memory comes up to 88% of usage and the memory consumption is 90%, so the FortiGate will enter in conserve mode.

For this reason you can't change the configuration conserve mode don't allows.

upvoted 2 times

⊟ **Knocks** 5 months, 3 weeks ago

Selected Answer: BC

B and C, conserve mode

upvoted 3 times

⊟ **gimy19** 6 months ago

Conserve mode . The answers are B and C

upvoted 3 times

⊟ **lenriquereyes** 6 months, 1 week ago

Selected Answer: BC

Fortigate Administrator Study Guide Page 459, 460

Fortigate does not accept configuration changes, because they might increase memory usage.

upvoted 3 times

⊟ **andres8h** 6 months, 1 week ago

Selected Answer: BC

Ok B and C

upvoted 3 times

⊟ **terminatoritsec** 6 months, 2 weeks ago

Selected Answer: BC

B and C are correct.

upvoted 3 times

⊟ **Qwerty379** 6 months, 2 weeks ago

Selected Answer: BC

B. FortiGate has entered conserve mode.

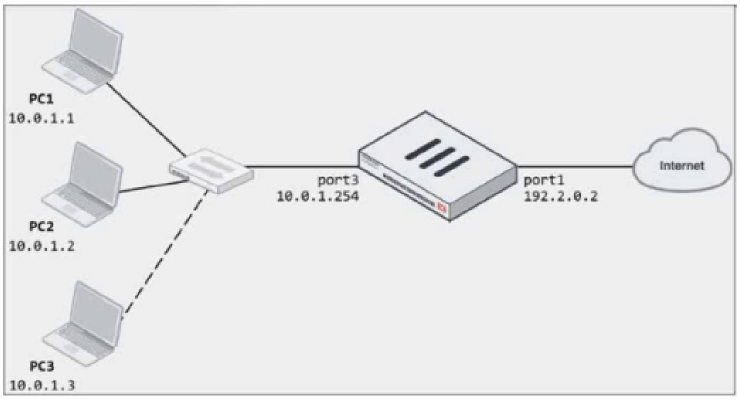
C. Administrators cannot change the configuration.

upvoted 3 times

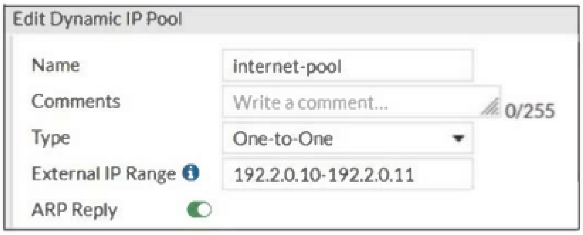
Question #6 *Topic 1*

Refer to the exhibits.

Network diagram



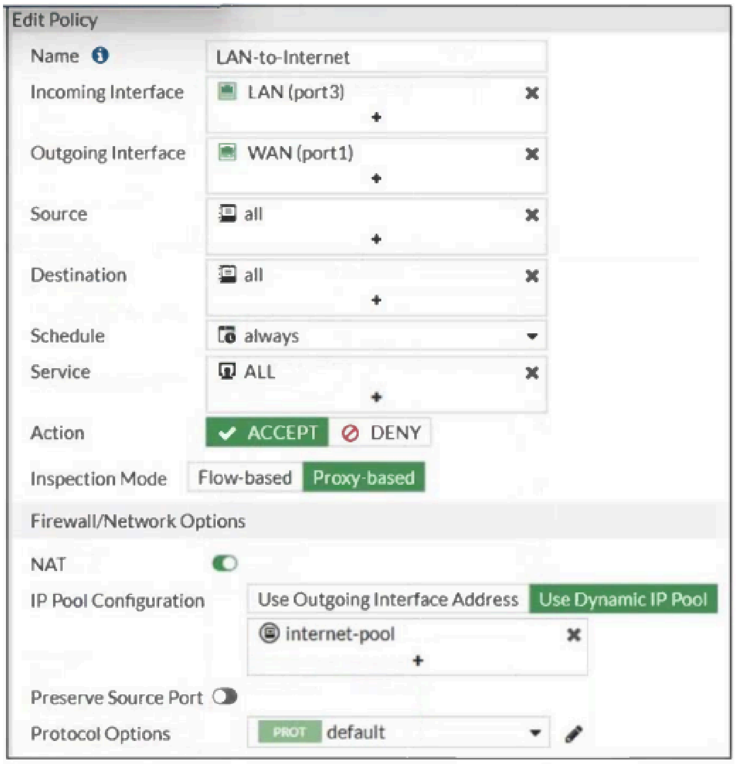
Dynamic IP pool



Edit Dynamic IP Pool

Name	internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range	192.2.0.10-192.2.0.11
ARP Reply	●

Firewall policy



Edit Policy

Name	LAN-to-Internet
Incoming Interface	LAN (port3)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic IP Pool internet-pool
Preserve Source Port	○
Protocol Options	PROT default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.

Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field.

B. In the IP pool configuration, set endip to 192.2.0.12.

C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set type to overload.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

JonathanGomes 3 days, 4 hours ago

Selected Answer: BD

Correct Answers: BD

upvoted 1 times

rigonet 2 months, 3 weeks ago

Selected Answer: BD

Correct Answers:

B. Set endip to 192.2.0.12 in the IP pool configuration.

D. Set type to overload in the IP pool configuration.

A. Incorrect: The policy already allows PC3 (source = all).

B. Correct: Expanding the IP pool gives PC3 a public IP.

C. Incorrect: A new policy won't fix the IP pool issue.

D. Correct: Overload allows multiple PCs to share the same public IP using PAT.

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: BD

Options:

Increase the IP Pool

Set the type to overload

upvoted 3 times

FHLPASSION 3 months, 2 weeks ago

B, D are correct

upvoted 3 times

s4mu3l007 4 months, 1 week ago

B & D Correct

upvoted 4 times

miguelmagr 5 months, 1 week ago

Selected Answer: BD

In the IP pool configuration, set endip to 192.2.0.12.

In the IP pool configuration, set type to overload.

upvoted 4 times

albaracin 6 months ago

Selected Answer: BD

B. In the IP pool configuration, set endip to 192.2.0.12.

D. In the IP pool configuration, set type to overload.

upvoted 4 times

gimy19 6 months ago

The answers are B and D

upvoted 4 times

TIGERZ44 6 months, 1 week ago

Selected Answer: BD

BD are correct

upvoted 3 times

andres8h 6 months, 1 week ago

Selected Answer: BD

OK B and D

upvoted 3 times

Qwerty379 6 months, 2 weeks ago

Selected Answer: BD

B. In the IP pool configuration, set endip to 192.2.0.12.

D. In the IP pool configuration, set type to overload.

upvoted 4 times

Question #7 *Topic 1*

Which method allows management access to the FortiGate CLI without network connectivity?

A. CLI console widget

B. Serial console

C. Telnet console

D. SSH console

Suggested Answer: *B*

Community vote distribution

B (100%)

rigonet 2 months, 3 weeks ago

Selected Answer: B

Correct Answer: B. Serial console

A: Requires web interface (network needed).
B: Direct physical access, no network needed.
C: Telnet needs network connectivity.
D: SSH requires network connectivity.

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: B

Serial Port with a console cable

upvoted 2 times

Magpo 3 months, 1 week ago

Selected Answer: B

B is the correct answer.

Don't be fooled by 'CLI console widget'. To even get to the console widget you would need to access the web GUI, which would require a network connection to access it with the browser.

upvoted 2 times

s4mu3l007 4 months, 1 week ago

B IS CORRECT

upvoted 2 times

3101a6a 5 months, 2 weeks ago

Selected Answer: B

Serial

upvoted 2 times

gimy19 6 months ago

Correct is B

upvoted 3 times

lenriquereyes 6 months, 1 week ago

Selected Answer: B

Serial console is correct.

upvoted 3 times

andres8h 6 months, 1 week ago

Selected Answer: B

serial console

upvoted 3 times

Qwerty379 6 months, 2 weeks ago

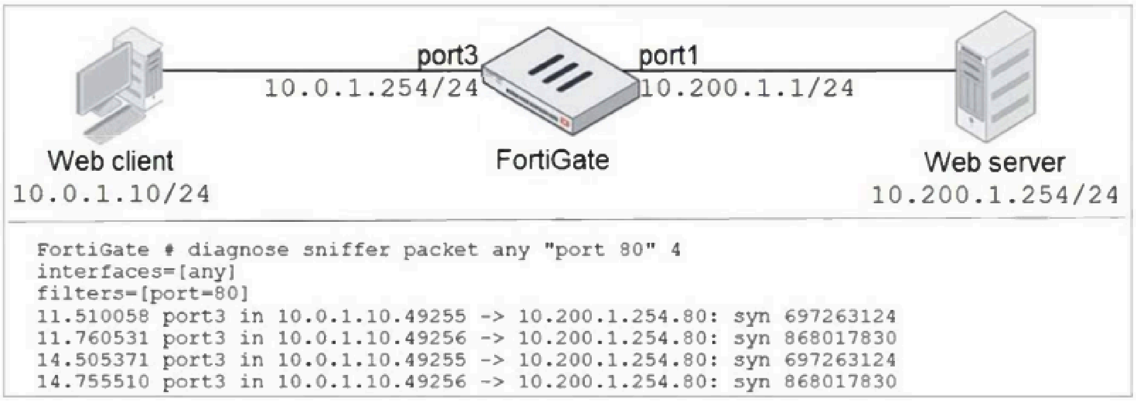
Selected Answer: B

B. Serial console

upvoted 3 times

Question #8 *Topic 1*

Refer to the exhibit.



```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port=80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit.

What should the administrator do next, to troubleshoot the problem?

A. Execute a debug flow.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer on FortiGate, this time with the filter "host 10.0.1.10".

D. Run a sniffer on the web server.

Suggested Answer: *A*

Community vote distribution

A (100%)

rigonet 2 months, 3 weeks ago

Selected Answer: A

Correct Answer: A. Execute a debug flow

A. Execute a debug flow.

Correct. Provides detailed packet routing, NAT, and policy analysis to identify the issue.

B. Capture the traffic using an external sniffer connected to port1.

Incorrect. External sniffers are unnecessary; FortiGate tools are sufficient.

C. Execute another sniffer on FortiGate with the filter "host 10.0.1.10".

Incorrect. The current sniffer already captures traffic from 10.0.1.10.

D. Run a sniffer on the web server.

Incorrect. The problem is better diagnosed from FortiGate first before moving to the server.

upvoted 3 times

sxcap 3 months, 1 week ago

Selected Answer: A

After running a sniffer, you need to run "diagnose debug flow" to inspect what is happening with the packet

upvoted 2 times

s4mu3l007 4 months, 1 week ago

A IS CORRECT

upvoted 2 times

miguelmagr 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 2 times

⊟ **youla5** 5 months, 2 weeks ago

A is correct.

upvoted 2 times

⊟ **miguelmagr** 5 months, 2 weeks ago

Execute debug flow in the web server or fortigate? If the answer is "debug flow in Fortigate" is to see if there is a firewall policy that is not matching?

upvoted 2 times

⊟ **fab1ccb** 5 months, 4 weeks ago

Selected Answer: A

A is the correct one

upvoted 2 times

⊟ **gimy19** 6 months ago

A is correct

upvoted 2 times

⊟ **andres8h** 6 months, 1 week ago

Selected Answer: A

A is correct

upvoted 2 times

⊟ **Qwerty379** 6 months, 2 weeks ago

Selected Answer: A

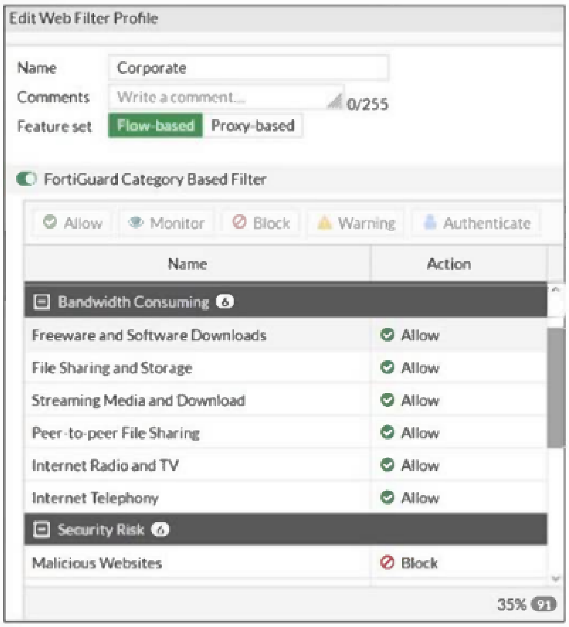
A is correct

upvoted 2 times

Question #9 Topic 1

Refer to the exhibit.

FortiGate web filter profile configuration



Edit Web Filter Profile

Name: Corporate

Comments: Write a comment... 0/255

Feature set: Flow-based Proxy-based

FortiGuard Category Based Filter

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

35% 91

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.

What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.

B. Set the Freeware and Software Downloads category Action to Warning.

C. Configure a web override rating for download.com and select Malicious Websites as the subcategory.

D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Suggested Answer: *CD*

Community vote distribution

CD (100%)

SingSingHK 2 months, 3 weeks ago

Selected Answer: CD

A - mostly does not work ... wildcard URL address object matching is very straight forward & limiting, and it simply won't match actual download site that it may redirecting user.

upvoted 2 times

rigonet 2 months, 3 weeks ago

Selected Answer: CD

Correct answer: Use C and D for a more direct and efficient solution.

A. Incorrect: A separate firewall policy for *.download.com would work but is less efficient for this specific case.

B. Incorrect: Setting the category to "Warning" does not block download.com.

C. Correct: A web rating override reclassifies download.com as "Malicious Websites," blocking it without affecting the rest of the category.

D. Correct: A static URL filter blocks download.com specifically while keeping other sites in the same category accessible.

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: CD

You can create a web rating override to change the website category to someone that is blocked in the web filter profile

You can enable the URL Filter in the Web Filter Profile and block the website

upvoted 2 times

abd_ethio 4 months, 1 week ago

CD is correct

upvoted 2 times

s4mu3l007 4 months, 1 week ago

C & D IS CORRECT

upvoted 2 times

0d6e481 5 months ago

I agree with C and D being correct answers but what about A? I think A would also do the job.

upvoted 3 times

> **262cfa1** 4 months, 1 week ago
>
> It's easier apply C & D, than A. What do you think?
>
> upvoted 2 times
>
> **evdw** 4 months, 1 week ago
>
> I agree
>
> upvoted 1 times

TIGERZ44 6 months, 1 week ago

Selected Answer: CD

CD is correct

upvoted 2 times

andres8h 6 months, 1 week ago

Selected Answer: CD

C and D are correct

upvoted 2 times

Question #10 *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 must the administrator make on FortiGate to meet the requirements? (Choose two.)

A. Enable Dead Peer Detection.

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

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

Suggested Answer: *AC*

Community vote distribution

AC (100%)

x666 2 months, 3 weeks ago

Selected Answer: AC

DPD to know when the tunnel is down + Administrative Distance to prioritize the primary tunnel.

upvoted 2 times

rigonet 2 months, 3 weeks ago

Selected Answer: AC

Conclusion:
Enable A (Dead Peer Detection) for failover detection and C (lower distance for the primary tunnel) to prioritize it.

Explanation:
A. Enable Dead Peer Detection.
Correct. Dead Peer Detection (DPD) is essential to quickly detect when a tunnel is down, enabling FortiGate to failover to the secondary tunnel.

B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
Incorrect. While helpful for maintaining tunnel stability, this setting is not directly required to detect dead tunnels or configure routing preferences.

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.
Correct. A lower distance ensures the primary tunnel is preferred for traffic. The higher distance on the secondary tunnel ensures it is used only during failover.

D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
Incorrect. This reverses the desired behavior, making the secondary tunnel primary.

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: AC

Enable Deed Pear detection complies the second requirement
Configure a lower distance on the primary static route complies the first requirement

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: AC

A & C

upvoted 2 times

s4mu3l007 4 months, 1 week ago

a & C is correct

upvoted 2 times

youla5 5 months, 2 weeks ago

correct answers

upvoted 1 times

TIGERZ44 6 months, 1 week ago

Selected Answer: AC

AC. lower administrative distance = more preferred

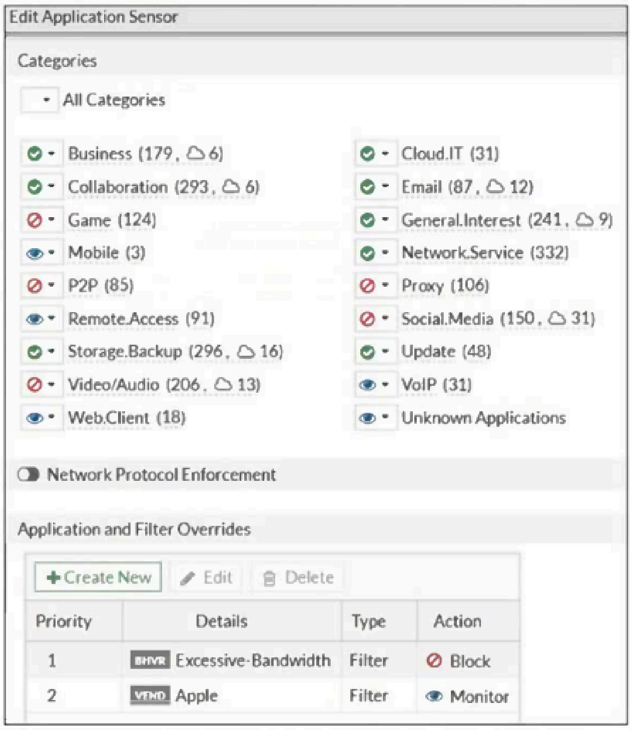
upvoted 4 times

Question #11

Topic 1

Refer to the exhibits.

Application sensor configuration



Edit Application Sensor

Categories

All Categories

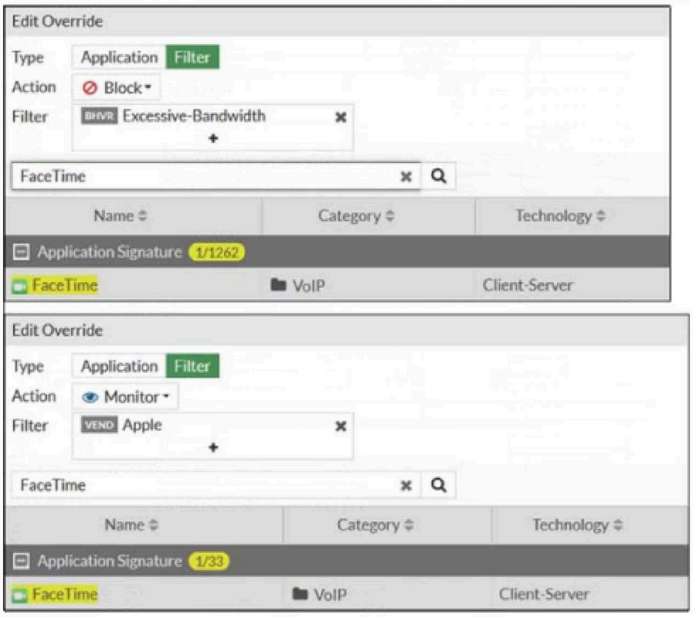
✓	Business (179, ☁ 6)	✓	Cloud.IT (31)
✓	Collaboration (293, ☁ 6)	✓	Email (87, ☁ 12)
⊘	Game (124)	✓	General.Interest (241, ☁ 9)
👁	Mobile (3)	✓	Network.Service (332)
⊘	P2P (85)	⊘	Proxy (106)
👁	Remote.Access (91)	⊘	Social.Media (150, ☁ 31)
✓	Storage.Backup (296, ☁ 16)	✓	Update (48)
⊘	Video/Audio (206, ☁ 13)	👁	VoIP (31)
👁	Web.Client (18)	👁	Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Apple	Filter	👁 Monitor

Application and Filter override configuration



Edit Override

Type: Application [✓ Filter]

Action: ⊘ Block

Filter: BHVR Excessive-Bandwidth

FaceTime

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Edit Override

Type: Application [✓ Filter]

Action: 👁 Monitor

Filter: VEND Apple

FaceTime

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details.

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

A. Apple FaceTime will be allowed, based on the Video/Audio category configuration.

B. Apple FaceTime will be allowed, based on the Apple filter configuration.

C. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

D. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.

Suggested Answer: *D*

Community vote distribution

D (80%) B (20%)

Knocks Highly Voted 5 months, 3 weeks ago

Selected Answer: D

The first rule that matches is block Excessive-Bandwidth, and FaceTime is within that filter.

upvoted 9 times

Beatledrew Highly Voted 6 months ago

D. Just because it says that there are only a few calls, the filter override is a CATEGORY of EXCESSIVE BANDWIDTH. It matches. This question comes directly from page 259 of the study guide.

upvoted 7 times

truserud Most Recent 1 month ago

Selected Answer: D

As Excessive-Bandwidth is placed above the apple Override, the Facetime-traffic wil lbe blocked, as the Excessive Bandwidth is processed first, and includes FaceTime as well. This scenario is detailed on page 259 in the FGT_7.4_Administrator study guide.

upvoted 1 times

rigonet 2 months, 3 weeks ago

Selected Answer: D

Correct Answer:

D. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.

A. Incorrect: Video/Audio category is set to "Block," so FaceTime would not be allowed.

B. Incorrect: The Apple filter set to "Monitor" does not override the higher-priority "Excessive-Bandwidth" block.

C. Incorrect: Even if Apple filter were "Allow," the "Excessive-Bandwidth" block still takes precedence.

D. Correct: FaceTime is categorized under "Excessive-Bandwidth," and this override has the highest priority, explicitly blocking it.

Conclusion: FaceTime is blocked because the "Excessive-Bandwidth" filter takes priority.

upvoted 2 times

sxcap 3 months, 1 week ago

Selected Answer: D

Based on the application control filters order, (app overrides - filter overrides - categories), when you set face time to allow, FortiGate continue to the next AC Filter, where "Excesive bandwidth" is blocked

upvoted 3 times

> **sxcap** 3 months, 1 week ago
>
> In this specific case, if you want to force the AC Profile to allow facetime, you must select "Excempt" instead of "Monitor"
>
> upvoted 1 times

rene.post 3 months, 2 weeks ago

Selected Answer: B

I think it is B because a "few calls" is mentioned.

upvoted 1 times

> **x666** 2 months, 4 weeks ago
>
> Few calls don't mean anything, it's just there to throw you off.
>
> upvoted 1 times

Charly0710 3 months, 2 weeks ago

D is correcto.

upvoted 2 times

s4mu3l007 4 months, 1 week ago

d is correct

upvoted 2 times

miguelmagr 5 months, 2 weeks ago

I guess is B 'cause FaceTime is going to be monitored If there is an excessive bandwith so FaceTime will be blocked. And also remember that said few incoming and outgoing calls would be made.

upvoted 2 times

> **miguelmagr** 5 months, 2 weeks ago
>
> It is just a tricky question. seeking on study guide the important note is the priority of the overrides rules. Ref page 259 study guide.
>
> upvoted 1 times

⊟ **wsdeffwd** 6 months ago

Selected Answer: D

Page 259

upvoted 3 times

⊟ **Billyon** 6 months ago

Selected Answer: B

With regards to the configuration above, Apple FaceTime would be allowed based on the application filter override configuration. It would only be blocked if the consumes bandwidth excessively which according to the question states that it is only a few calls originating or incoming.

upvoted 3 times

⊟ **IBB90704** 6 months, 1 week ago

Selected Answer: D

Pagina 257

Scanning Order:

After the IPS engine examines the traffic stream for a signature match, FortiGate scans packets for matches,
in this order, for the application control profile:
1. Application and filter overrides: If you have configured any application overrides or filter overrides, the
application control profile considers those first. It looks for a matching override starting at the top of the
list, like firewall policies.
2. Categories: Finally, the application control profile applies the action that you've configured for applications
in your selected categories.

upvoted 4 times

Question #12 *Topic 1*

An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. SSL VPN idle-timeout

B. SSL VPN login-timeout

C. SSL VPN dtls-hello-timeout

D. SSL VPN session-ttl

Suggested Answer: *B*

Community vote distribution

B (80%) C (20%)

⊟ **IBB90704** Highly Voted 6 months, 1 week ago

Selected Answer: B

Segun el libro pagina 287 deberia ser B y C

When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client
can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands
under config vpn ssl settings have been added to address this. The first command allows you to set
up the login timeout, replacing the previous hard timeout value. The second command allows you to set up
the maximum DTLS hello timeout for SSL VPN connections.

upvoted 8 times

⊟ **Cantero75** Highly Voted 4 months, 1 week ago

It is C, In a Fortinet SSL VPN, the "dtls-hello-timeout" setting defines the maximum time a FortiGate will wait for an initial "Hello" message from a client during the DTLS (Datagram Transport Layer Security) handshake process, essentially setting a time limit for establishing a secure connection before considering the attempt failed due to network latency or issues with the client device; this is crucial for preventing prolonged connection attempts and improving overall VPN connection stability.
The SSL VPN login-timeout in FortiGate controls the amount of time that the SSL VPN waits before disconnecting

upvoted 6 times

⊟ **Sidetone** Most Recent 1 day, 12 hours ago

Selected Answer: B

B was the correct answer in the 7.2 exam

upvoted 1 times

⊟ **davidmdlp85** 1 week, 2 days ago

Selected Answer: C

SSL VPN dtls-hello-timeout: This setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message.

SSL VPN login-timeout: This setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.

upvoted 1 times

⊟ **truserud** 1 month ago

Selected Answer: C

For high latency client connections, you can adjust the dtls-hello-timeout settings. This is detailed in the FCP FGT admin study guide on pages 287 through 289.

upvoted 1 times

⊟ **6bee64f** 1 month, 4 weeks ago

Selected Answer: C

Key word is "negotiation", that's why it is C

upvoted 1 times

⊟ **Pelau_the_Engineer** 2 months ago

Selected Answer: C

Best practices for configuring SSL VPNs require setting the DTLS timeout settings.

upvoted 1 times

wohny 2 months ago

Selected Answer: B

Another reason why B is the correct answer is: you have to manualy reconfigure the forticlient to DTLS.
To use DTLS with FortiClient: Go to File -> Settings and enable 'Preferred DTLS Tunnel'.

Source:
To use DTLS with FortiClient:
Go to File -> Settings and enable 'Preferred DTLS Tunnel'.

upvoted 1 times

alaahaider 2 months, 2 weeks ago

Selected Answer: B

allows more time for the SSL handshake to complete, which is essential in a high-latency environment to prevent the handshake from timing out prematurely

upvoted 1 times

rigonet 2 months, 2 weeks ago

Selected Answer: C

Correct answer: C. SSL VPN dtls-hello-timeout

Explanation:
Both login-timeout and dtls-hello-timeout are mentioned as important adjustments for solving SSL VPN connection issues in high-latency networks. However, dtls-hello-timeout specifically addresses the timeout for DTLS negotiation, which is crucial for UDP connections.

This is supported by the FortiGate Administrator Study Guide 7.4, on page 287, where it is stated that both parameters should be adjusted in high-latency environments, but dtls-hello-timeout is more relevant to negotiation problems.

Adjusting both is best practice, but for this scenario, dtls-hello-timeout is the most appropriate answer.

upvoted 1 times

SingSingHK 2 months, 3 weeks ago

Selected Answer: B

i know most people will pick B, while C also looks feasible option... me too, I will go for B.
>> high latency, let's say RTT is 500ms, but it still very unlikely will impact the DTLS handshake cycle that its timeout is in terms of seconds.

upvoted 1 times

Thespis 2 months, 3 weeks ago

Selected Answer: C

Both B and C are correct.

A new SSL VPN driver was added to FortiClient 5.6.0 and later to resolve SSL VPN connection issues. If the FortiOS version is compatible, upgrade to use one of these versions. Latency or poor network connectivity can cause login timeout on FortiGate. In v5.6.0 and later, use the following commands to allow a user to increase the SSL VPN login timeout setting.

```
config vpn ssl settings
set login-timeout 180 (default is 30)
set dtls-hello-timeout 60 (default is 10)
end
```

upvoted 3 times

hecjoseroag 3 months ago

Selected Answer: C

I think that the most correct answer would be C but I have the doubt because there are portals where they indicate that it is a configuration that must have both the dtls and login timed out would be perhaps B and C. I leave a part of the manual where they indicate scenario to use the DTLS

"Many factors can contribute to slow throughput.This recommendation tries to improve throughput by using the FortiOS Datagram Transport Layer Security (DTLS) tunnel option, available in FortiOS 5.4 and above. DTLS allows SSL VPN to encrypt traffic using TLS and uses UDP as the transport layer instead of TCP. This avoids retransmission problems that can occur with TCP-in-TCP."

upvoted 3 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: B

You need to give more time to complete the login, so you need to adjust the default 10sec timeout for the login.

upvoted 1 times

⊟ **1zwan** 3 months, 1 week ago

Selected Answer: C

C beause this setting determines how long the FortiGate will wait for a DTLS hello message from the client. For high-latency connections, increasing this timeout will prevent SSL VPN negotiation failures caused by delays in receiving the DTLS hello message. imo not B because this setting controls the maximum time allowed for a user to log in, but does not affect connection negotiation.

upvoted 2 times

⊟ **hkhan049** 3 months, 2 weeks ago

According to study guide page 287, B AND C are correct. The question is, if this example question is really near on the question in the real exam. Otherwise I prefer the dtls-hello-timeout, because it has a shorter default value

upvoted 2 times

⊟ **vuhidus** 3 months, 4 weeks ago

Selected Answer: B

login-timeout

https://www.examtopics.com/discussions/fortinet/view/115393-exam-nse4_fgt-72-topic-1-question-83-discussion/

upvoted 1 times

Question #13 *Topic 1*

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

A. Allow & Warning

B. Trust & Allow

C. Allow

D. Block & Warning

E. Block

Suggested Answer: *ABE*

Community vote distribution

ABE (54%) BCE (46%)

IBB90704 Highly Voted 6 months, 1 week ago

Selected Answer: BCE

Pagina 186

When a certificate fails for any of the reasons above, you can configure any of the following actions:
• Keep untrusted & Allow: FortiGate allows the website and lets the browser decide the action to take.
FortiGate takes the certificate as untrusted.
• Block: FortiGate blocks the content of the site.
• Trust & Allow: FortiGate allows the website and takes the certificate as trusted.
upvoted 12 times

andres8h Highly Voted 6 months, 1 week ago

Selected Answer: ABE

ABE is correct
fortigate 7.4 Administrator pag 186
upvoted 7 times

fa7474b 4 months, 1 week ago

I believe A is incorrect. Page 186 of the study guide does not contain the word "warning" anywhere on it.
I take "Warning" in this context to mean that Fortigate would supply a warning. That is not what happens. If you set it to "Keep untrusted and allow" then the BROWSER will generate the warning, NOT Fortigate.
upvoted 4 times

Nicae Most Recent 3 weeks, 1 day ago

Selected Answer: ABE

ABE

according to page 186 of the study guide, it states

Keep Untrusted and Allow
Block
Trust and Allow

for A: Allow and Warning would be the same as keep untrusted and Allow because the warning shows that it is untrusted but you are able to continue.

with B and E stating to either block the content or trust the website and gain access.

I Page 186 of the study guide never stated any other actions from C and D from what I can see in the options.
upvoted 1 times

Ajit9929 1 month, 1 week ago

Selected Answer: ADE

Only 3 valid actions - allow & warning, block and warning and block

upvoted 2 times

⊟ **harizmr** 1 month, 2 weeks ago

Selected Answer: ABE

ABE is correct

fortigate 7.4 Administrator pag 186

upvoted 1 times

⊟ **hecjoseroag** 3 months ago

Selected Answer: BCE

BCE

Keep Untrusted & Allow: Allow the server certificate and keep it untrusted.l Block: Block the certificate.l Trust & Allow: Allow the server certificate and re-sign it as trusted (page 1966 FortiOS Administrator Guide)

upvoted 2 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: BCE

Options available:

Trust and Allow (fortigate marks the certificate as trusted)

Keep untrusted and allow / allow (Fortigate allow the traffic and let the browser decide)

Block (Fortigate blocks the connection)

upvoted 2 times

⊟ **JRKhan** 3 months, 3 weeks ago

Selected Answer: BCE

With invalid certificates the options are Allow, Block or Custom. In custom, you can either select: Trust & Allow, Keep Untrusted and Allow, Block.

So BCE is correct.

upvoted 3 times

⊟ **s4mu3l007** 4 months, 1 week ago

BCE are correct

upvoted 2 times

⊟ **066c9f3** 4 months, 1 week ago

Selected Answer: BCE

I'd go with BCE because on FortiGate it says "Keep untrusted & Allow", "Block", "Trust & Allow".

With "Keep untrusted & Allow", Fortigate allows it and does NOT display a warning but let's the browser decide. I'd associate the Fortigate setting "Keep untrusted & allow" with "Allow" from the question (Option C). Anything else doesn't make sense. Since there's no warning displayed in any allow situation, A doesn't make sense and since Block & Warning doesn't exist, it has to be B for this. The other two (Trust & Allow, Block) are the exact same words as written in the question, so it can only be B, C, E.

upvoted 4 times

⊟ **marcovinicius4** 4 months, 1 week ago

Selected Answer: BCE

In "SSL/SSH Inspection" > Create New

I can set in "Common Options"

Invalid SSL certificates: Allow | Bloc | Custom

- Expired certificates: Keep Untrusted & Allow | Block | Trust & Allow
- Revoke certificates: Keep Untrusted & Allow | Block | Trust & Allow
- Validation time-out certificates: Keep Untrusted & Allow | Block | Trust & Allow
- Validation failed certificates: Keep Untrusted & Allow | Block | Trust & Allow

upvoted 4 times

⊟ **DBFront** 4 months, 3 weeks ago

Selected Answer: ABE

ABE

upvoted 1 times

⊟ **6f7d62a** 5 months ago

Selected Answer: BCE

In the administration guide you can confirm that there are only the options to allow or block, after enabling deep inspection, the options to trust or not trust the certificate are added.

upvoted 5 times

⊟ **0d6e481** 5 months ago

Selected Answer: BCE

There's no Warning in SSL inspection. Warning exists for Web Filter

upvoted 4 times

⊟ **miguelmagr** 5 months, 1 week ago

Selected Answer: BCE

Allow

Trust & Allow

Block

upvoted 5 times

⊟ **dumpz** 5 months, 1 week ago

Answer it's BCE on the fortinet guide there is written allow, trust & allow and block

upvoted 4 times

⊟ **Billyon** 6 months ago

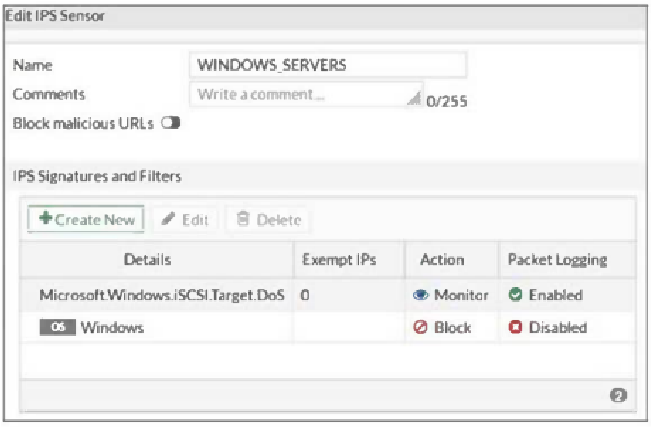
Selected Answer: ABE

The illustration on Page 186

upvoted 3 times

Question #14 Topic 1

Refer to the exhibit, which shows the IPS sensor configuration.



Edit IPS Sensor

Name: WINDOWS_SERVERS

Comments: Write a comment... 0/255

Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	Enabled
OS Windows		Block	Disabled

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will gather a packet log for all matched traffic.

B. The sensor will reset all connections that match these signatures.

C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.

D. The sensor will block all attacks aimed at Windows servers.

Suggested Answer: *CD*

Community vote distribution

CD (33%) AC (33%) AD (33%)

0d6e481 Highly Voted 5 months ago

Selected Answer: CD

How can A be a correct answer when the packet logging is enabled only for the iSCSI attack and disabled for the Windows attacks?

upvoted 11 times

rigonet Highly Voted 2 months, 3 weeks ago

Selected Answer: AC

Correct Answers: A and C

Explanation of Each Option:

A. The sensor will gather a packet log for all matched traffic.

Correct. The "Microsoft.Windows.iSCSI.Target.DoS" signature has packet logging enabled, so matched traffic will be logged.

B. The sensor will reset all connections that match these signatures.

Incorrect. The configuration does not indicate resetting connections, as the action for the "iSCSI" signature is set to "Monitor."

C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.

Correct. The action for this signature is set to "Monitor," meaning traffic matching this signature is allowed but logged.

D. The sensor will block all attacks aimed at Windows servers.

Incorrect. The signature for "iSCSI" is explicitly set to "Monitor," so it will not block this attack.

Conclusion:

The sensor will log traffic (A) for matched signatures and allow traffic (C) for the monitored "iSCSI" signature.

upvoted 5 times

JS77test Most Recent 1 week, 5 days ago

Selected Answer: AC

A. The sensor will gather a packet log for all matched traffic.

-> In other words all traffic that matches "Microsoft.Windows.iSCSI.Target.DoS" signature will match

C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.
-> Matches are only monitored but not blocked
=> Monitor: Allow traffic to continue to its destination and log the activity.

B. -> Action "Reset" exists but is not used in example

D. -> Windows Servers is only the Name of the Rule. Match criteria is set to "OS Windows", so ALL MS Windows operating systems, regardingless which role, client or server.
=> OS: Refers to the Operating System affected by the attack.

upvoted 1 times

⊟ **truserud** 3 weeks ago

Selected Answer: AC

C & D guys need to read page 243 in the study guide.
A & C are most probable the correct answers based off of that page alone:

"The rules are similar to firewall policy matching; the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters."

Sensor will gather logs for packets
Sensor will allow traffic.

Now, look at the blocked ipse sensor, it only specifies Windows, not for example target "Server". So it will not block all traffic against Windows Servers.
upvoted 1 times

⊟ **TheVaro** 3 weeks ago

Selected Answer: CD

A is incorrect because packet logging is only enabled for the "Microsoft.Windows.iSCSI.Target.DoS" signature but disabled for the general "Windows" category.
B is incorrect because "Monitor" mode does not reset connections, and while "Block" mode is enabled for Windows-related attacks, there is no explicit mention of connection resets.
upvoted 1 times

⊟ **6a61123** 3 weeks, 5 days ago

Selected Answer: C

A is incorrect because it will only log for the iSCSI DoS so if it is not iSCSI DoS, it will not be logged
B is incorrect because reset is not selected for any actions
C is correct because the iSCSI DoS is set to monitor
D is incorrect because it won't block ALL Windows attacks – it is allowing iSCSI DoS (but I think this is what they want to be the 2nd answer).
upvoted 2 times

⊟ **jrb77** 1 month, 3 weeks ago

Selected Answer: AC

How can D be correct when it states that the sensor will block all attacks at Windows servers, when it is allowing C. Explanation is needed on this one.
upvoted 1 times

⊟ **6bee64f** 1 month, 4 weeks ago

Selected Answer: CD

Packet logging is not enabled for both connection, and there are not conditions to reset connections.... CD
upvoted 1 times

⊟ **jrb77** 2 months ago

Selected Answer: AC

If you look at A, it is a true statement, because it states, The sensor will gather a packet log for all matched traffic. The ISCSI target has packet logging enabled. Even if windows OS does not have packet logging enabled, the statement for the answer is still true because it will gather a packet log for "All Matched Traffic"

For C, I believe this is correct, as you will be allowing attackers through a monitoring action.

I believe that A and C are correct.

upvoted 1 times

⊟ **wohny** 2 months ago

Selected Answer: CD

Only C is correct, but if I have to choose 2, then D is more correct than A. D is correct except for the statement from C :) A is not correct because it only logs C, if it is not met, dropped packets are not logged - D.

upvoted 2 times

⊟ **Cyber_rosh20** 2 months, 2 weeks ago

Selected Answer: AC

A because will log just the signature of iSCSI not all windows attack

upvoted 1 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: CD

A is incorrect because there is no log enabled to blocked packets

B is incorrect because iSCI packets are allowed

C is correct because iSCI packets are allowed

D is correct because all other windows server attacks will be blocked

upvoted 3 times

⊟ **Booma1234** 3 months, 1 week ago

Selected Answer: AC

A and C are the only way mes it could be when you look closely at it.

upvoted 1 times

⊟ **evdw** 3 months, 3 weeks ago

Selected Answer: AC

Correct answer is A,C

upvoted 2 times

⊟ **evdw** 3 months, 3 weeks ago

Microsoft.Windows.iSCSI.Target.DoS is allowed, so not all attacks to windows are blocked.

And when hitting the Microsoft.Windows.iSCSI.Target.DoS attack, it is getting logged

upvoted 1 times

⊟ **vuhidus** 3 months, 3 weeks ago

Selected Answer: CD

I believe it's C & D

upvoted 2 times

⊟ **Charly0710** 4 months ago

A and C.

D cannot be for the following reason: "When the IPS engine compares traffic with the signatures in each filter, order matters. The rules are similar to firewall policy matching; the engine evaluates the filters and signatures at the top of the list first, and applies the first match. The engine skips subsequent filters". Pag 243 Fortinate Administrator Study Guide

upvoted 3 times

Question #15 *Topic 1*

Which statement is a characteristic of automation stitches?

A. They can be run only on devices in the Security Fabric.

B. They can be created only on downstream devices in the fabric.

C. They can have one or more triggers.

D. They can run multiple actions at the same time.

Suggested Answer: *D*

Community vote distribution

D (67%) C (33%)

⊟ **Billyon** Highly Voted 6 months ago

Selected Answer: D

According to the illustration on page 396 of the the study guide, it says automatic stitches consist of 'a trigger' and 'one or more configurable actions'.

upvoted 13 times

⊟ **6a61123** Most Recent 3 weeks, 5 days ago

Selected Answer: D

Page 396 of study guide, it says actions can be run sequentially (one at a time) OR in parallel (at the same time)

upvoted 1 times

⊟ **rigonet** 2 months, 3 weeks ago

Selected Answer: D

The correct statement is "D", as automation stitches allow multiple actions to be executed simultaneously or in sequence.

"C" is Incorrect: Stitches support only one trigger, which initiates the configured actions.

upvoted 3 times

⊟ **hecjoseroag** 3 months ago

Selected Answer: D

The answer is D in FortiOS 7.4.5 Administration Guide page 3349

"The stitch Action execution can be set to either Sequential or Parallel. In sequential execution, actions will execute one after another with a delay (if specified). If one action fails, then the action chain stops. This is the default setting. In parallel execution, all actions will execute immediately when the stitch is triggered"

upvoted 4 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: D

You can setup automation stitches for any device in the security fabric, it consist of a trigger and one or more configurable actions.

upvoted 2 times

⊟ **evdw** 3 months, 3 weeks ago

Selected Answer: C

Correct answer is C

actions do not run simultaneously, but in sequence

upvoted 1 times

⊟ **evdw** 3 months, 3 weeks ago

Sorry D is correct, actions can run in parallel (or in sequence), but there is only one trigger

upvoted 2 times

⊟ **vuhidus** 3 months, 3 weeks ago

Selected Answer: D

Should be "D"

upvoted 1 times

⊟ **JRKhan** 3 months, 3 weeks ago

Selected Answer: D

D is correct. Stitches can be used outside of the security fabric, it is not a requirement. If used within the fabric, they can only be created on root fortigate but are applicable to all devices within the fabric. Each stitch has "a" trigger and multiple configurable actions which can either run in a sequential or parallel manner.

upvoted 2 times

bdosres 3 months, 4 weeks ago

C. They can have one or more triggers.

Explanation:

• Automation stitches on Fortinet devices allow you to automate actions based on specific events (triggers). A stitch can be configured with one or multiple triggers to respond to specific conditions, such as detecting suspicious traffic.

• A stitch can also perform actions, but not simultaneously — they execute sequentially.

• Stitches are not limited to devices within the Security Fabric, nor are they restricted to downstream devices.

Therefore, the correct option is C because the main characteristic of stitches is that they can have multiple triggers to initiate the defined actions.

upvoted 3 times

abd_ethio 4 months ago

c "Each automation stitch pairs a trigger and one or more actions"

upvoted 1 times

ThomasG7 4 months ago

Selected Answer: C

C. Correct, as automation stitches can indeed have multiple triggers, which initiate the defined actions.

D. Incorrect, as automation stitches run actions sequentially (not simultaneously).

upvoted 2 times

ThomasG7 4 months ago

Nevermind its D

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

3101a6a 4 months, 3 weeks ago

Selected Answer: D

"Administrator-defined automated workflows (called stitches) cause FortiOS to automatically respond to an event in a preprogrammed way. Because this workflow is part of the Security Fabric, you can set up automation stitches for any device in the Security Fabric. However, the Security Fabric is not required to use stitches.

Each automation stitch pairs a trigger and one or more actions. FortiOS has several predefined stitches, triggers and actions. However, you can create custom automation based on the available options."

upvoted 2 times

Ba588_ 5 months ago

Selected Answer: C

Automation stitches in Fortinet are a feature that allows you to automate responses based on specific network events. Here's why C is correct:

Triggers: Automation stitches can indeed have one or more triggers that initiate the automated action. Triggers can include security events, like IPS or antivirus alerts, or other network events.

upvoted 2 times

herlock_sholmes_2810 5 months ago

"To create an automation stitch, A TRIGGER EVENT (singular) and a response action or ACTIONS (plural) are selected."

See the documentation: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/351998

upvoted 1 times

lenriquereyes 5 months, 1 week ago

Selected Answer: D

D is correct,

upvoted 3 times

⊟ **dumpz** 5 months, 1 week ago

Fortinet guide: You can configure the Minimum internal (seconds) setting on some of the available actions to make sure they don't run more often than needed"

if there is specific a minium interval there is no possible that can start all in the same time
probably the correct Answer it's C

upvoted 2 times

⊟ **youla5** 5 months, 2 weeks ago

D is correct

upvoted 2 times

Question #16 *Topic 1*

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

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

B. Connected monitored ports > System uptime > Priority > FortiGate serial number

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

D. Connected monitored ports > HA uptime > Priority > FortiGate serial number

Suggested Answer: *D*

Community vote distribution

D (100%)

terminatoritsec Highly Voted 6 months, 2 weeks ago

Selected Answer: D

D is Correct.

Fortigate Administratror Study Guide page 414.

upvoted 5 times

TheCook Most Recent 1 month, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

hecjoseroag 3 months ago

Selected Answer: D

Override enable: Connected monitored ports - Priority - HA Uptime - SN Override disabled: Connected monitored ports - HA Uptime - Priority - SN (page 2897 FortiOS Administrator Guide)

upvoted 3 times

sxcap 3 months, 1 week ago

Selected Answer: D

Override enable: Connected monitored ports - Priority - HA Uptime - SN

Override disabled: Connected monitored ports - HA Uptime - Priority - SN

upvoted 1 times

f3eb371 4 months ago

Selected Answer: D

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disabled-default

upvoted 2 times

f3eb371 4 months ago

D is correct, patch: Failed Monitored interfaces > Age > Device Priority > Serial number

Link wthin information: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disabled-default

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct, based in documentation.

upvoted 1 times

marcovinicius4 4 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

miguelmagr 5 months, 1 week ago

Selected Answer: D

D - When override is disabled HA > Priority

When override is enabled Priority > HA

upvoted 2 times

youla5 5 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

NetworkWeaver 5 months, 2 weeks ago

D is the correct answer

When override is disabled (MUPS):

The device that has a higher number of operationally UP Monitored interfaces (M).

The device that has the highest HA Uptime. not the unit uptime (U).

The device which has the highest Priority (P)

Device which has the highest Serial Number (S).

When override is enabled (MPUS):

The device that has a higher number of operationally UP Monitored interfaces (M).

The device that has the highest Priority (P).

A device that has the highest HA Uptime. not the unit uptime (U)

The device that has the highest Serial Number (S).

upvoted 2 times

Knocks 5 months, 3 weeks ago

Selected Answer: D

1. The cluster compares the number of monitored interfaces that have a status of up. The member with the most available monitored interfaces becomes the primary.
2. The cluster compares the HA uptime of each member. The member with the highest HA uptime, by at least five minutes, becomes the primary.
3. The member with the highest priority becomes the primary.
4. The member with the highest serial number becomes the primary.

upvoted 2 times

fab1ccb 5 months, 4 weeks ago

D is the correct answer

https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-HA-Primary-unit-selection-process-when/ta-p/249745

upvoted 1 times

TIGERZ44 6 months ago

Selected Answer: D

D per study guide

upvoted 2 times

knoor 6 months, 1 week ago

D is correct

upvoted 1 times

ShrekAlmighty 6 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 2 times

andres8h 6 months, 1 week ago

Selected Answer: D

D is correct

upvoted 3 times

Question #17 Topic 1

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.

B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

D. The client FortiGate requires a manually added route to remote subnets.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

hecjoseroag 3 months ago

Selected Answer: AB

If fortigate is used as an SSL VPN client, it needs a ssl virtual tunnel interface to connect to the SSL VPN server. This is the client virtual interface that the vpn server will assign the temporary IP address to during the lifetime of an ssl connection. The SSL VPN server also needs a correct CA certificate to authenticate/trust client's certificate. (page 2527 FortiOS Administrator Guide)

upvoted 4 times

x666 1 week, 1 day ago

Page 272*

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: AB

Client FortiGate need an SSLVPN type interface
Server FortiGate need a CA to check client FortiGate certificate

upvoted 2 times

vuhidus 3 months, 3 weeks ago

Selected Answer: AB

A and B

upvoted 2 times

JRKhan 3 months, 3 weeks ago

Selected Answer: AB

If fortigate is used as an SSL VPN client, it needs a ssl virtual tunnel interface to connect to the SSL VPN server. This is the client virtual interface that the vpn server will assign the temporary IP address to during the lifetime of an ssl connection. The SSL VPN server also needs a correct CA certificate to authenticate/trust client's certificate.

upvoted 1 times

s4mu3l007 4 months, 1 week ago

B and C are correct

upvoted 1 times

s4mu3l007 4 months, 1 week ago

im sorry, is the A&B

upvoted 1 times

felixliao 4 months, 1 week ago

Selected Answer: AB

C is not mandatory, so A and B

upvoted 2 times

exmrrs 4 months, 1 week ago

Selected Answer: AB

C is not mandatory, so A and B

upvoted 2 times

⊟ **marcovinicius4** 4 months, 1 week ago

Selected Answer: BC

B and C

upvoted 1 times

⊟ **Billyon** 6 months ago

Selected Answer: AB

A and B are the correct answers

upvoted 1 times

⊟ **knoor** 6 months, 1 week ago

According to Based on FCP - FortiGate 7.4 Administrator Self-Paced course:

A and B are correct

upvoted 3 times

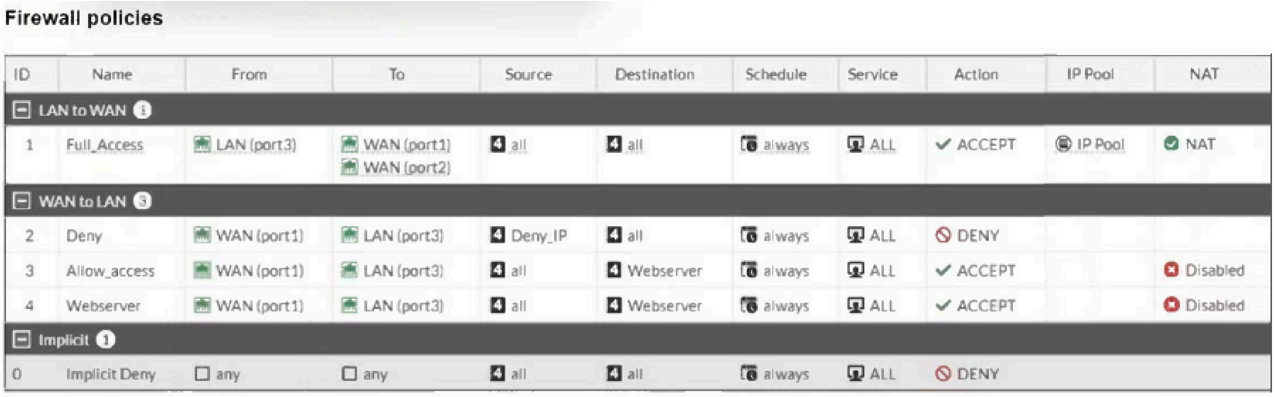
⊟ **262cfa1** 4 months ago

What page?

upvoted 1 times

Question #18 *Topic 1*

Refer to the exhibit.



Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
⊟ LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	✓ ACCEPT	IP Pool	NAT
⊟ WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	⊘ DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	✓ ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	✓ ACCEPT		Disabled
⊟ Implicit 1										
0	Implicit Deny	□ any	□ any	all	all	always	ALL	⊘ DENY		

Which statement about this firewall policy list is true?

A. The Implicit group can include more than one deny firewall policy.

B. The firewall policies are listed by ID sequence view.

C. The firewall policies are listed by ingress and egress interfaces pairing view.

D. LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.

Suggested Answer: *D*

Community vote distribution

D (75%) C (25%)

⊟ **Knocks** Highly Voted 5 months, 3 weeks ago

Selected Answer: D

I'd go with D, because the policies cannot be in interface pair view, since the policy ID 1 has multiple interfaces, so it cannot be C.

upvoted 21 times

⊟ **BloodyMery** 5 months, 3 weeks ago

you are right

upvoted 4 times

⊟ **JonathanGomes** Most Recent 4 days, 13 hours ago

Selected Answer: C

Option C - Page 43.

upvoted 1 times

⊟ **doubleA_doubleA** 2 months ago

Selected Answer: D

Answer looks to be D. Although C looks compelling, port numbers don't show up in the collapsed section in interface pairing view like it is shown here. But it does show up like this in the sequence grouping view.

upvoted 1 times

⊟ **Dineshkaarthik** 2 months, 2 weeks ago

Selected Answer: D

D as this a feature realeased on 7.4 version sequesnce grouping.

upvoted 2 times

⊟ **Bilale** 2 months, 2 weeks ago

Selected Answer: D

C. The firewall policies are listed by ingress and egress interfaces pairing view = NOK
This can be correct if we have on destination by rule
When we have 2 destination interface the view is by group sequence / sequence
Refer to NSE4 study guide | Policy List - Interface Pair view and by Sequence

upvoted 2 times

⊟ **SingSingHK** 2 months, 3 weeks ago

Selected Answer: D

if it is interface pair, the grouping info is auto & can't modify / specify by admin

upvoted 2 times

⊟ **rigonet** 2 months, 3 weeks ago

Selected Answer: C

Correct Answer:
C. The firewall policies are listed by ingress and egress interfaces pairing view.

Explanation of Each Option:
A. The Implicit group can include more than one deny firewall policy.
Incorrect. The "Implicit Deny" rule is a default, single policy applied to any unmatched traffic. It cannot include multiple policies.

B. The firewall policies are listed by ID sequence view.
Incorrect. The policies are grouped by interface pairings, not sorted by ID numbers.

C. The firewall policies are listed by ingress and egress interfaces pairing view.
Correct. The policies are grouped based on the interface pairings, such as LAN to WAN and WAN to LAN.

D. LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.
Incorrect. The view is based on interface pairings, not sequence groupings like "LAN to WAN" or "Implicit."

upvoted 1 times

⊟ **hecjoseroag** 3 months ago

Selected Answer: D

I would say it is D because when you configure more than one interface the interface per view option disappears and only leaves by sequence and in this case it is not by sequence either.

upvoted 2 times

⊟ **Johny_437** 3 months ago

Selected Answer: C

Correct answer is C. FortiGuide, page 43.

upvoted 3 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: D

I'm not sure about the group view, but for sure can NOT be C because there are 2 interfaces as destiny in the policy ID 1, when that happen, interface pair view dissapear automatically

upvoted 1 times

⊟ **FHLPASSION** 3 months, 1 week ago

Selected Answer: C

In Policy & Objects policy list pages, there are two policy views: Interface Pair View and By Sequence view. Interface Pair View displays the policies in the order that they are checked for matching traffic, grouped by the pairs of incoming and outgoing interfaces in collapsible sections. The Interface Pair View can be used when a policy is configured with multiple interfaces.

upvoted 2 times

⊟ **JRKhan** 3 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

⊟ **JRKhan** 3 months, 3 weeks ago

Selected Answer: C

C is correct. The sections appear only when you choose interface pair view. When you select sequence, it doesn't group the rules/policies into sections instead they are displayed based on the policy ID.

upvoted 2 times

⊟ **JRKhan** 3 months, 3 weeks ago

Scrap my earlier comment and selection. D seems like a more appropriate answer, since with multiple interfaces selected in the policies you cant select interface pairing view.

upvoted 2 times

⊟ **s4mu3l007** 4 months, 1 week ago

D is correct

upvoted 2 times

⊟ **marcovinicius4** 4 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

⊟ **3101a6a** 4 months, 3 weeks ago

Selected Answer: D

For each view, more than one view appeared for Rule ID 1. For only one to appear, it must be in the Grouping view list.

I recommend replicating it in the laboratory.

upvoted 1 times

⊟ **herlock_sholmes_2810** 4 months, 3 weeks ago

Selected Answer: D

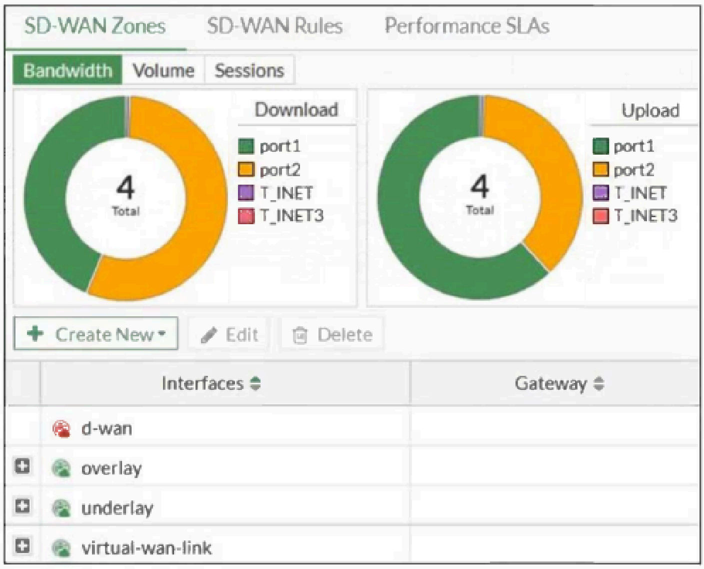
D. See this reference:

upvoted 1 times

Question #19 *Topic 1*

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



Interfaces	Gateway
d-wan	
overlay	
underlay	
virtual-wan-link	

Based on the exhibit, which statement is true?

A. The underlay zone contains port1 and port2.

B. The d-wan zone contains no member.

C. The d-wan zone cannot be deleted.

D. The virtual-wan-link zone contains no member.

Suggested Answer: *B*

TheCook 1 month, 2 weeks ago

Selected Answer: B

There is no + next to it

upvoted 2 times

hugovasconcelos 2 months, 1 week ago

Selected Answer: B

Zona sem membro fica com o símbolo vermelho.

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: B

There are no members in d-wan zone, so it doesn't have the + icon and can be deleted

upvoted 1 times

vuhidus 4 months ago

Selected Answer: B

B i think

upvoted 1 times

s4mu3l007 4 months, 1 week ago

B is correct.

upvoted 1 times

marcovinicius4 4 months, 1 week ago

Selected Answer: B

B is the correct

upvoted 1 times

youla5 5 months, 2 weeks ago

The given answer is correct.

upvoted 1 times

⊟ **fab1ccb** 5 months, 4 weeks ago

B is the correct one

upvoted 1 times

⊟ **Beatledrew** 6 months ago

B is correct. Page 351 of user guide. The D-WAN zone must have been manually created and therefore can be deleted. The default zone that CAN'T be deleted is the virtual-wan-link and is automatically created and is where 'FortiGate places any new member if you don't assign them to a user-defined zone'.

upvoted 4 times

Question #20 *Topic 1*

Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.

B. The RPF check is run on the first reply packet of any new session.

C. The RPF check is run on the first sent and reply packet of any new session.

D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Suggested Answer: *AD*

Community vote distribution

AD (89%) 11%

⊟ **wsdeffwd** Highly Voted 6 months ago

Selected Answer: AD

Page 86 "RPF check is only carried out on: The first packet in the session, not on a reply"

upvoted 10 times

⊟ **wsdeffwd** Highly Voted 6 months ago

Selected Answer: AD

Page 86

upvoted 8 times

⊟ **hecjoseroag** Most Recent 3 months ago

Selected Answer: AD

Whenever a packet arrives at one of the interfaces on a FortiGate, the FortiGate determines whether the packet was received on a legitimate interface by doing a reverse look-up using the source IP address in the packet header. This protects against IP spoofing attacks. If the FortiGate does not have a route to the source IP address through the interface on which the packet was received, the FortiGate drops the packet as per Reverse Path Forwarding (RPF) check. (page 433 FortiOS Administrator Guide)

upvoted 1 times

⊟ **sxcap** 3 months, 1 week ago

Selected Answer: AD

RPF check is done on the first sent packet

It helps to protect FortiGate against spoofing attacks

upvoted 1 times

⊟ **evdw** 3 months, 3 weeks ago

For packets in the original direction, RPF check takes place.

Packet received in the reply direction, FortiGate does not perform any RPF check.

upvoted 1 times

⊟ **JRKhan** 3 months, 3 weeks ago

Selected Answer: AD

RPF is done on the first packet of the session and not on the reply. It protects the fortigate and network from IP spoofing attacks.

upvoted 1 times

⊟ **s4mu3l007** 4 months, 1 week ago

A and D are the ans

upvoted 1 times

⊟ **felixliao** 4 months, 1 week ago

Selected Answer: AD

Study guide 7.4

upvoted 1 times

⊟ **marcovinicius4** 4 months, 1 week ago

Selected Answer: AD

A and D

upvoted 1 times

⊟ **3101a6a** 4 months, 3 weeks ago

Selected Answer: AD

Study guide 7.4 Page 86

"FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session."

upvoted 1 times

⊟ **ShrekAlmighty** 6 months, 1 week ago

Selected Answer: BD

RPF (Reverse Path Forwarding) check is not performed on the first sent packet of a new session. Instead, it is performed on the first reply packet.

upvoted 3 times

⊟ **ThomasG7** 4 months ago

I think Shrek is right.

upvoted 1 times

Question #21 *Topic 1*

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

A. Manual with load balancing

B. Lowest Cost (SLA) with load balancing

C. Best Quality with load balancing

D. Lowest Quality (SLA) with load balancing

E. Lowest Cost (SLA) without load balancing

Suggested Answer: *ABC*

Community vote distribution

ABC (50%) ABE (40%) 10%

fa7474b Highly Voted 👍 5 months ago

Selected Answer: ABE

ABE, When you select Best Quality the "Load Balancing" toggle disappears from the UI. When you select Lowest Cost (SLA) you can choose to enable or disable load balancing.

upvoted 14 times

Qwerty379 Highly Voted 👍 6 months, 1 week ago

Selected Answer: ABE

It's AB for sure, but there is no load balancing in Best quality, so, it's so tricky, I think E should be also correct. ABE.

upvoted 8 times

> **wsdeffwd** 6 months ago
>
> Page 357 - The choices are:
>
> Manual with LB, Manual w/o LB, Lowest Cost w/ LB, Lowest Cost w/o LB, Best Quality w/o LB
>
> So its ABE
>
> upvoted 4 times

2767cfc Most Recent ⊙ 1 month, 1 week ago

Selected Answer: ABE

best quality is not with load balancing

upvoted 2 times

alekgil 2 months, 1 week ago

Selected Answer: ABE

https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/708464/load-balancing-strategy

upvoted 1 times

53a24e2 2 months, 1 week ago

Selected Answer: ABC

manual

best Quality

Lowest Cost (SLA)

upvoted 1 times

DrazenSego 3 months ago

Selected Answer: ABC

https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/413288/sd-wan-rules-overview

Im currently connected to my Fortigate and can confirm that it is same as in official documentation.

So please explain how C is not answer, we can argue between B and E, but C is must

upvoted 2 times

> **x666** 2 months, 3 weeks ago
>
> I just opened a sd-wan rule and when selecting "Best quality" the toggle for "Load balancing" disappears.
>
> Also your doc is from 7.6, but the exam is 7.4 (idk if there is a difference, just saying).

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: ABE

Manual: you can choose to activate or not "load balancing"

Lowest Cost: you can choose to activate or not "load balancing"

Best Quality: "load balancing" option is not present even

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: ABE

I'm going with A B E

upvoted 1 times

Charly0710 3 months, 3 weeks ago

In the slide on page 357, it is very clear that there is no Lower Cost (SLA) option without Load Balancing. For this reason, the correct answer is ABC.

upvoted 1 times

bdosres 3 months, 4 weeks ago

The correct answers are:

A. Manual with load balancing

B. Lowest Cost (SLA) with load balancing

E. Lowest Cost (SLA) without load balancing

upvoted 1 times

Charly0710 3 months, 3 weeks ago

E is not possible. C is correct.

upvoted 1 times

s4mu3l007 4 months, 1 week ago

ABE are correct

upvoted 1 times

felixliao 4 months, 1 week ago

Selected Answer: ABC

ABC is the correct answer

upvoted 1 times

miguelmagr 5 months, 1 week ago

And is a tricky question because de option D says Lowest Quality SLA, I guess you should prefer Best Quality instead.

upvoted 1 times

miguelmagr 5 months, 1 week ago

Selected Answer: ABC

The only two which works with load balancing (Manual and Lowest Cost SLA) the other option is Best Quality

upvoted 1 times

miguelmagr 5 months, 2 weeks ago

Selected Answer: ABE

Ref: FGT 7.4 Administration study Guide in Pag357 said that Interface selection strategy: *Manual, *Best Quality, *Lowest cost (SLA)

upvoted 2 times

Beatledrew 5 months, 2 weeks ago

This is why you need hands on. If you chose Best Quality the Load Balancing switch goes away. A,B,E would seem to be the best answer if Load Balancing Strategy was what was asked. If simple, 'Interface' strategy, it would be Manual, Best Quality, or Lowest Cost SLA (ABC).

upvoted 3 times

Beatledrew 5 months, 2 weeks ago

But to follow up, based on what I just described, there IS no such thing as Best Quality with Load Balancing. So it has to be ABE

upvoted 1 times

SalamanderHoliday888 5 months, 3 weeks ago

Answer ABE, https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/342836/lowest-cost-sla-strategy

upvoted 2 times

Question #22 *Topic 1*

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Pre-shared key and certificate signature as authentication methods

B. Extended authentication (XAuth) to request the remote peer to provide a username and password

C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged

D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Suggested Answer: *AB*

Community vote distribution

AB (100%)

sxcap 3 months, 1 week ago

Selected Answer: AB

You can use PSK or certificate as authentication

Obviously if you set certificate as authentication, the client need a certificate

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: AB

A&B correct

upvoted 1 times

s4mu3l007 4 months, 1 week ago

A & B are correct

upvoted 1 times

youla5 5 months, 2 weeks ago

Selected Answer: AB

the answers are correct

upvoted 1 times

Beatledrew 6 months ago

A & B, Page 300 of Study Guide

upvoted 2 times

ShrekAlmighty 6 months, 1 week ago

Selected Answer: AB

A, B is correct.

upvoted 2 times

Question #23 *Topic 1*

Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

A. Checksums of devices are compared against each other to ensure configurations are the same.

B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.

C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster.

D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Suggested Answer: *AC*

Community vote distribution

AC (100%)

bob511 Highly Voted 6 months, 1 week ago

AC: FortiGate 7.4 Administrator Study Guide pg.421

"After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link"

upvoted 6 times

TheVaro Most Recent 3 weeks ago

Selected Answer: AC

After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link. An HA synchronization process running on each cluster device receives the configuration change and applies it to the cluster device. For example, if you create a firewall address object, the primary doesn’t resend its complete configuration—it sends only the new object.

upvoted 1 times

MZED68 1 month, 2 weeks ago

Selected Answer: AC

I made a mistake. The correct answer is AC, 100%.

upvoted 1 times

MZED68 1 month, 2 weeks ago

Selected Answer: BC

I believe that this is a tricky question. The correct answer could be A, B, and C since incremental configuration sync can happen if any of the member configurations are changed.

upvoted 1 times

MZED68 1 month, 2 weeks ago

Selected Answer: AB

The correct answer is A and B.

upvoted 1 times

hugovasconcelos 2 months, 1 week ago

Selected Answer: AB

O FortiGate usa checksums para verificar a consistência das configurações entre os membros do cluster. Se os checksums forem diferentes, isso indica que as configurações estão fora de sincronia.

Apenas o dispositivo primário pode fazer alterações na configuração. Essas alterações são então sincronizadas de forma incremental com os dispositivos secundários no cluster.

upvoted 1 times

Dineshkaarthik 2 months, 2 weeks ago

Selected Answer: AB

Incremental config sync only happens by changes on primary HA member other device's can't have any config changes when they are secondary. So the correct answer is A & B.

upvoted 1 times

SingSingHK 3 months ago

Selected Answer: CD

why D is not correct, but A is correct? as in HA mode, each unit could have difference "dedicated management interface" setting (e.g. management interface IP) ... how come the checksum must match?

upvoted 1 times

SingSingHK 2 months, 3 weeks ago

real life tried out in lab ... seems HA config didn't count in config checksum... sorry guys

upvoted 1 times

jl2307 2 months, 3 weeks ago

We know that some configurations are not synchronizable, but this does not mean that synchronization will not occur, it will occur at the level of the configurations that are synchronizable. (page 423 Fortigate 7.4 administrator guide)

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: AC

checksums must be the same

if any change occurs, incremental sync must happen to ensure checksums keep the same

upvoted 2 times

vuhidus 3 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 2 times

s4mu3l007 4 months, 1 week ago

A & C are correct

upvoted 2 times

miguelmagr 5 months, 1 week ago

Selected Answer: AC

Checksum must be equal on both fortigate.

Incremental Configuration Synchronization happens when the primary configuration is changed and changes are synchronized to the secondary.

Secondary configuration is changed and changes are synchronized to the primary.

upvoted 1 times

mhl2203 5 months, 2 weeks ago

Selected Answer: AC

A and C are correct.

upvoted 1 times

youla5 5 months, 2 weeks ago

A and C are correct.

upvoted 1 times

Beatledrew 5 months, 2 weeks ago

A&C is the correct answer.

upvoted 2 times

andres8h 6 months, 1 week ago

Selected Answer: AC

A y C son correctos

upvoted 4 times

Question #24 *Topic 1*

What are two features of the NGFW profile-based mode? (Choose two.)

A. NGFW profile-based mode can only be applied globally and not on individual VDOMs.

B. NGFW profile-based mode must require the use of central source NAT policy.

C. NGFW profile-based mode policies support both flow inspection and proxy inspection.

D. NGFW profile-based mode supports applying applications and web filtering profiles in a firewall policy.

Suggested Answer: *CD*

sxcap 3 months, 1 week ago

Selected Answer: CD

D and D are correct

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: CD

C & D

upvoted 1 times

f3eb371 4 months ago

Selected Answer: CD

c&d is the correct

upvoted 1 times

s4mu3l007 4 months, 1 week ago

C&D ans

upvoted 2 times

DBFront 4 months, 3 weeks ago

Selected Answer: CD

7.4 study guide

upvoted 3 times

youla5 5 months, 2 weeks ago

C and D are correct

upvoted 3 times

fab1ccb 5 months, 4 weeks ago

The correct answers are C and D

upvoted 3 times

Beatledrew 6 months ago

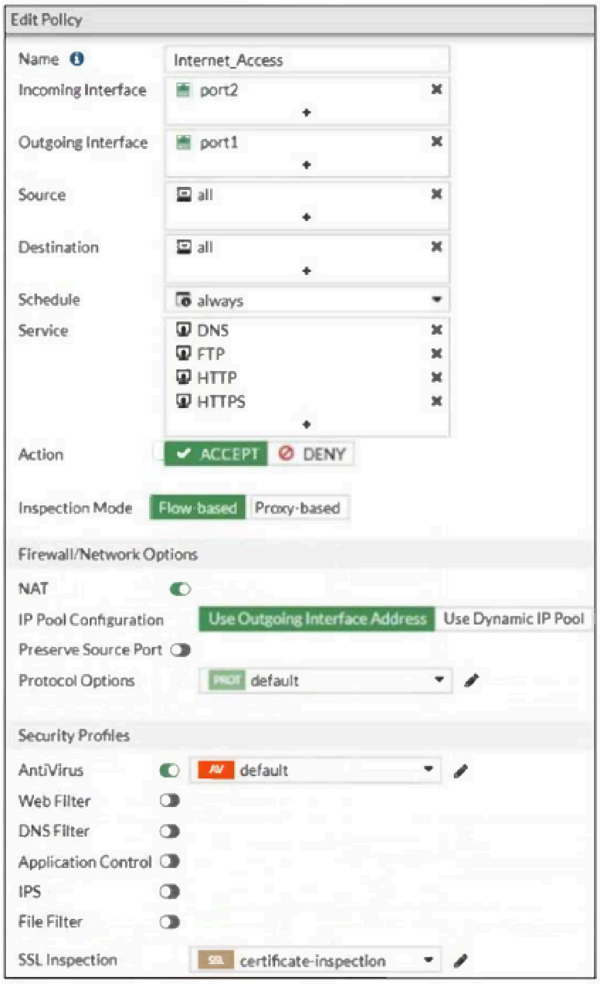
C & D, page 250 & 253

upvoted 3 times

Question #25 Topic 1

Refer to the exhibit to view the firewall policy.

Firewall policy configuration



Edit Policy

Name: Internet_Access

Incoming Interface: port2

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: DNS, FTP, HTTP, HTTPS

Action: ✓ ACCEPT | DENY

Inspection Mode: Flow-based | Proxy-based

Firewall/Network Options

NAT: ●

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Preserve Source Port: ○

Protocol Options: PROT default

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

Application Control: ○

IPS: ○

File Filter: ○

SSL Inspection: SSL certificate-inspection

Why would the firewall policy not block a well-known virus, for example eicar?

A. The action on the firewall policy is not set to deny.

B. The firewall policy is not configured in proxy-based inspection mode.

C. Web filter is not enabled on the firewall policy to complement the antivirus profile.

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

Suggested Answer: *D*

6bee64f 1 month, 4 weeks ago

Selected Answer: D

Magic word "would" makes the difference, proxy-based won't make difference, it is about doing deep inspection on the packets.

upvoted 1 times

jl2307 2 months, 3 weeks ago

Selected Answer: D

Pag. 175

For antivirus or IPS control you should use a deep-inspection profile.

upvoted 1 times

sxcap 3 months, 1 week ago

Selected Answer: D

Deep inspection is needed to ensure good function for AV

upvoted 2 times

Fs4ntos 3 months, 2 weeks ago

The answer is B

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

The firewall policy does not apply deep content inspection

upvoted 1 times

s4mu3l007 4 months, 1 week ago

The answer is D

upvoted 1 times

DBFront 4 months, 3 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 1 times

youla5 5 months, 2 weeks ago

D is the correct answer.

upvoted 2 times

Beatledrew 5 months, 4 weeks ago

D would be the most accurate response. While Flow-Based inspection mode is limited, it still can scan viruses if they are not overly complex. SSL certificate inspection only inspects the certificate of the encrypted traffic, ensuring it is valid and not self-signed or expired. It does not decrypt the actual content of the SSL/TLS traffic, meaning that any malicious content inside encrypted HTTPS traffic will pass through without being inspected. So here, we can assume the EICAR file was accessed via HTTPS.

upvoted 4 times

Question #26 *Topic 1*

Which inspection mode does FortiGate use for application profiles if it is configured as a profile-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%)

Beatledrew Highly Voted 5 months, 2 weeks ago

Page 250 of the Study Guide. More information. "You can configure application control in proxy-based and flow-based firewall policies. However, because application control uses the IPS engine, which uses flow-based inspection, the INSPECTION is always flow-based."

upvoted 7 times

sxcap Most Recent 3 months, 1 week ago

Selected Answer: D

Flow-Based is the default inspection for NGFW

upvoted 2 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

D corret

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

youla5 5 months, 1 week ago

key term is application profile. so answer is D

upvoted 1 times

fab1ccb 5 months, 4 weeks ago

Selected Answer: D

D is correct because is the default inspection applied with profile-based on NGFW.

Proxy-based is an inspection wich you can add manually to an individual policy

upvoted 1 times

7moPain 6 months ago

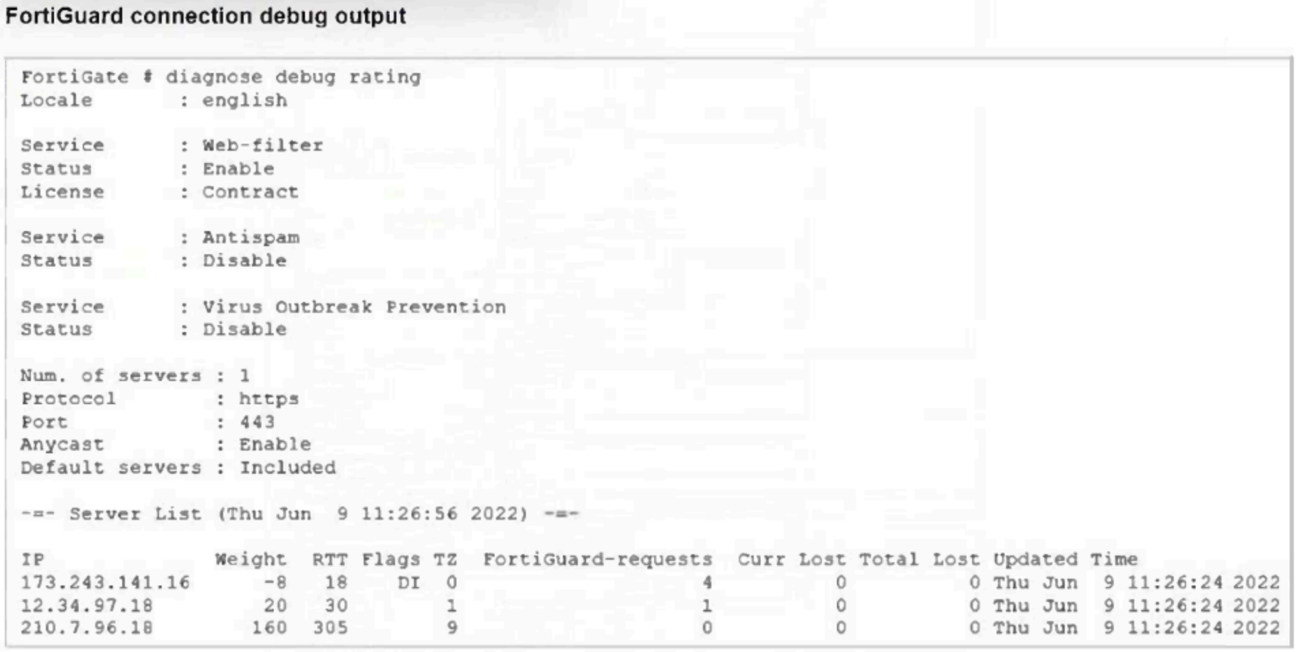
Why is B not correct? Ty

upvoted 2 times

> **Beatledrew** 5 months, 4 weeks ago
>
> In profile-based NGFW mode, FortiGate applies security profiles like Application Control at the flow level. This means the firewall inspects traffic as it passes through without fully proxying or buffering it. The firewall can detect and control applications by inspecting network traffic in real-time using signatures and heuristics. D is correct.
>
> upvoted 1 times

Question #27 Topic 1

Refer to the exhibit showing a FortiGuard connection debug output.



FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Thu Jun  9 11:26:56 2022) -=-

IP               Weight  RTT Flags TZ  FortiGuard-requests  Curr Lost Total Lost Updated Time
173.243.141.16       -8   18    DI  0                    4          0          0 Thu Jun  9 11:26:24 2022
12.34.97.18          20   30        1                    1          0          0 Thu Jun  9 11:26:24 2022
210.7.96.18         160  305        9                    0          0          0 Thu Jun  9 11:26:24 2022
```

Based on the output, which two facts does the administrator know about the FortiGuard connection? (Choose two.)

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

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

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

D. FortiGate is using default FortiGuard communication settings.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

x666 2 months, 3 weeks ago

Selected Answer: AD

FortiGate 7.4 Administrator Study Guide, Page 25 😎

upvoted 3 times

s4mu3l007 4 months ago

A&D ANSWER.

upvoted 2 times

fab1ccb 5 months, 4 weeks ago

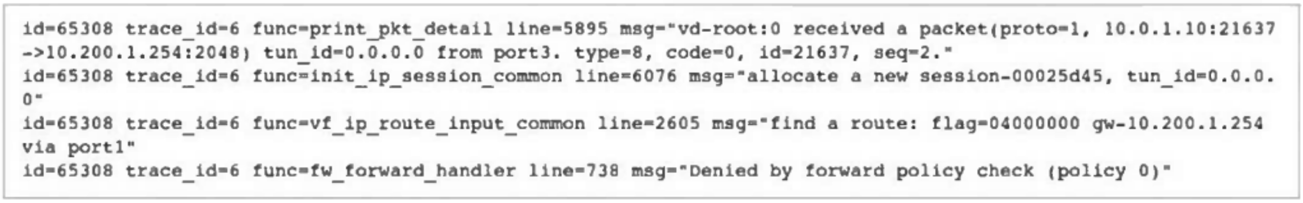
Selected Answer: AD

A and D are correct because in the output we can see num. of servers : 1, it refers to servers use to retreive contract info, and D because in the output we can see that the procolo used is HTTPS on standard port 443 and anycast is enabled

upvoted 3 times

Question #28 *Topic 1*

Refer to the exhibit.



```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 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. It failed the RPF check.

C. The next-hop IP address is unreachable.

D. It matched the default implicit firewall policy.

Suggested Answer: *D*

Community vote distribution

D (100%)

sxcap 2 months, 3 weeks ago

Selected Answer: D

Don't get confused with the word "check", the important part is (policy 0), that's the implicit policy

upvoted 1 times

Charly0710 3 months, 2 weeks ago

Selected Answer: D

D is correct. It's clear, "Denied by forward policy check (policy 0)"

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

It's D

upvoted 1 times

262cfa1 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct - traffic is denied by implicit firewall rule

upvoted 1 times

youla5 5 months, 2 weeks ago

Policy id 0 is the default drop policy. so D is correct

upvoted 1 times

Knocks 5 months, 3 weeks ago

Selected Answer: D

Denied by forward policy check means it matched a deny policy, in this case it has ID 0 so it is the implicit deny

upvoted 1 times

fab1ccb 5 months, 4 weeks ago

Selected Answer: D

D because the output shows "Denied by forward policy check (policy 0)" which is the implicit policy

upvoted 1 times

Question #29 *Topic 1*

An administrator must enable a DHCP server on one of the directly connected networks on FortiGate. However, the administrator is unable to complete the process on the GUI to enable the service on the interface.
In this scenario, what prevents the administrator from enabling DHCP service?

A. The role of the interface prevents setting a DHCP server.

B. The DHCP server setting is available only on the CLI.

C. Another interface is configured as the only DHCP server on FortiGate.

D. The FortiGate model does not support the DHCP server.

Suggested Answer: *A*

Community vote distribution

A (100%)

harizmr 1 month, 1 week ago

Selected Answer: A

cannot be placed at some interface

upvoted 1 times

sxcap 2 months, 3 weeks ago

Selected Answer: A

If the interface is set on WAN (for example), DHCP Server is not enabled

upvoted 2 times

hecjoseroag 3 months ago

Selected Answer: A

The 'DHCP server' option cannot be enabled/used on DMZ interfaces.
For the interfaces with DMZ role, DHCP server and Security mode are not available (by design).
If a DHCP server is required on that physical interface, change its role from DMZ to LAN, WAN, or Undefined.

upvoted 2 times

f3eb371 3 months ago

Selected Answer: A

The role of the interface prevents setting a DHCP server

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: A

A right one

upvoted 1 times

s4mu3l007 4 months, 1 week ago

Answer: A

upvoted 1 times

youla5 5 months, 2 weeks ago

A is correct.

upvoted 1 times

Beatledrew 5 months, 3 weeks ago

In this scenario, the issue preventing the administrator from enabling DHCP service on the FortiGate interface is most likely that the interface is configured as part of a zone or is set to use DHCP relay. Here's a breakdown of potential causes:
1. Interface in a Zone: If the interface is part of a zone, you cannot configure individual settings, such as DHCP, directly on the interface. FortiGate restricts interface-specific configurations like DHCP when the interface is assigned to a zone.
2. DHCP Relay Configured: If the interface is already configured to act as a DHCP relay (forwarding DHCP requests to an external DHCP server), FortiGate will not allow you to enable the DHCP server on that interface.
Page 8 of Study Guide

upvoted 1 times

Knocks 5 months, 3 weeks ago

Selected Answer: A

if you set the interface role to wan, it will hide useless settings on a wan link (such as DHCP server)

upvoted 4 times

fab1ccb 5 months, 4 weeks ago

Selected Answer: A

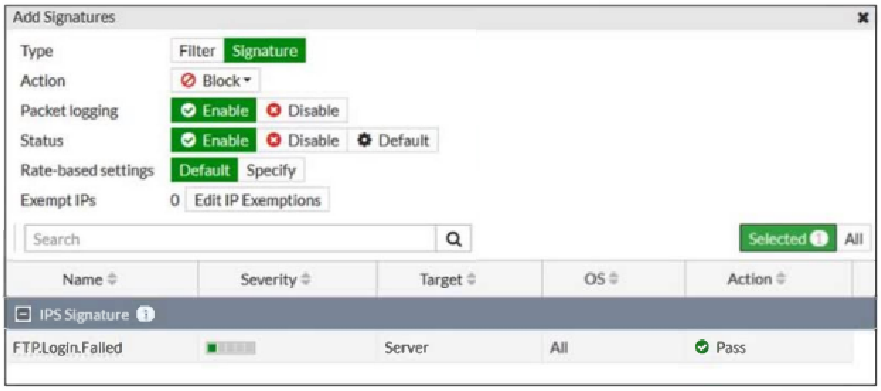
The role that prevent an interface to act like DHCP relay is assigned to DMZ interface.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-FortiGate-as-DHCP-server/ta-p/197856

upvoted 2 times

Question #30 *Topic 1*

Refer to the exhibit.



Add Signatures ✖

Type: Filter [✓ Signature]

Action: ⊘ Block ▾

Packet logging: [✓ Enable] Disable

Status: [✓ Enable] Disable Default

Rate-based settings: [✓ Default] Specify

Exempt IPs: 0 Edit IP Exemptions

Search [✓ Selected 1] All

Name	Severity	Target	OS	Action
IPS Signature				
FTP.Login.Failed	▮▯▯▯▯	Server	All	✓ Pass

Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit.

What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

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

Suggested Answer: *D*

Community vote distribution

D (100%)

truserud 3 weeks ago

Selected Answer: D

See page 245 in the Study guide.

Action set to block, is the action the IPS Filter will take for the IPS signatures added in the list. "Select Block to silently drop traffic matching any of the signatures included in the entry".

upvoted 1 times

sxcap 2 months, 3 weeks ago

Selected Answer: D

If you want to let the IPS profile to allow the login.fail, you MUST set it on "excempt" so the IPS will stop the rule order)

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

D correct

upvoted 1 times

JRKhan 3 months, 3 weeks ago

Selected Answer: D

D is correct. The action is set to Block at the top of the configuration setting. If it was set to default then the default action underneath for each signature will apply.

upvoted 3 times

s4mu3l007 4 months, 1 week ago

the ans is D

upvoted 1 times

dumpz 5 months, 1 week ago

answer it's A.. FTP.login.failed it's in action pass

upvoted 1 times

miguelmagr 5 months, 2 weeks ago

Selected Answer: D

I got confused with the IPS Signature Action "Pass". I see Rate-based setting is set to "Default". After many loging fail I guess that action is going to be logged as an action "blocked" when exceed the amount of retries. Am I wrong?

upvoted 1 times

youla5 5 months, 2 weeks ago

The answer is D.

upvoted 1 times

GopiChandMurari 5 months, 4 weeks ago

Shouldn't this be A?

upvoted 1 times

Knocks 5 months, 3 weeks ago

Nope, the action in the signature list is block (top of the screenshot). It would be A if the action was default or allow, but the action of all the signatures that will be added to this list is going to be block.

upvoted 3 times

Question #31 *Topic 1*

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

A. FortiGuard category filter and rating filter

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

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

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

Suggested Answer: *D*

Community vote distribution

D (100%)

truserud 3 weeks ago

Selected Answer: D

See page 230 in the study guide for details.

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

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

upvoted 2 times

f3eb371 4 months ago

Selected Answer: D

The correct answer is:

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

When multiple web filtering features are enabled in FortiGate, the HTTP inspection process follows a specific sequence:

Static URL Filter: This filter checks URLs against a predefined list of allowed or blocked URLs.

FortiGuard Category Filter: This checks the category of the website using the FortiGuard database.

Advanced Filters: These include features like -> "Safe Search" <-, YouTube EDU filtering, and other advanced filtering options.

This order ensures efficient and layered filtering of web traffic based on various criteria.

upvoted 2 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

youla5 5 months, 2 weeks ago

D is correct

upvoted 1 times

wsdeffwd 6 months ago

Selected Answer: D

Page 230

upvoted 1 times

Question #32 *Topic 1*

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

A. Log ID

B. Policy ID

C. Sequence ID

D. Universally Unique Identifier

Suggested Answer: *D*

Community vote distribution

D (100%)

vuhidus 3 months, 3 weeks ago

Selected Answer: D

It's D

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

lenriquereyes 5 months, 1 week ago

Selected Answer: D

Page 35

When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer.

upvoted 1 times

andres8h 6 months, 1 week ago

Selected Answer: D

FortiGate 7.4 administrator pag 35

upvoted 4 times

Question #33 *Topic 1*

An administrator configured a FortiGate to act as a collector for agentless polling mode.
What must the administrator add to the FortiGate device to retrieve AD user group information?

A. RADIUS server

B. DHCP server

C. Windows server

D. LDAP server

Suggested Answer: *D*

vuhidus 3 months, 3 weeks ago

Selected Answer: D

LDAP server

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

MHD_SDQ 4 months, 1 week ago

FortiGate_7.4_Administrator
FortiGate uses LDAP to query AD to retrieve user group information.

upvoted 1 times

herlock_sholmes_2810 4 months, 3 weeks ago

Selected Answer: D

"If FortiGate is acting as a collector for agentless polling mode, you must select Poll Active Directory Serverand configure the IP addresses and AD administrator credentials for each DC.

FortiGate uses LDAP to query AD to retrieve user group information. For this to happen, you must add the LDAP server to the Poll Active Directory Server configuration."

upvoted 2 times

herlock_sholmes_2810 4 months, 3 weeks ago

Selected Answer: D

I think that is D.

upvoted 1 times

DBFront 4 months, 3 weeks ago

Selected Answer: D

D

upvoted 1 times

GAP77 5 months, 2 weeks ago

D is correct
Pag 126 FortiGate_7.4_Administrator

upvoted 3 times

Question #34 *Topic 1*

An administrator manages a FortiGate model that supports NTurbo.
How does NTurbo enhance performance for flow-based inspection?

A. NTurbo offloads traffic to the content processor.

B. NTurbo creates two inspection sessions on the FortiGate device.

C. NTurbo buffers the whole file and then sends it to the antivirus engine.

D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

Suggested Answer: *D*

Community vote distribution

D (83%) A (17%)

andres8h Highly Voted 6 months, 1 week ago

Selected Answer: D

D is correcto, Fortigate 7.4 administrator pag 201

upvoted 9 times

hecjoseroag Most Recent 3 months ago

Selected Answer: D

NTurbo creates a special data path to redirect traffic from the ingress interface to IPS, and from IPS to the egress interface. NTurbo allows firewall operations to be offloaded along this path, and still allows IPS to behave as a stage in the processing pipeline, reducing the workload on the FortiGate CPU and improving overall throughput. Hardware Acceleration https://docs.fortinet.com/document/fortigate/7.0.1/hardware-acceleration/896174/nturbo-offloads-flow-based-processing

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: D

D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces

upvoted 1 times

s4mu3l007 4 months, 1 week ago

D is correct

upvoted 1 times

fa7474b 4 months, 1 week ago

Selected Answer: D

D, Nturbo uses NP not CP.

upvoted 1 times

Fs4ntos 4 months, 1 week ago

B is correct

For firewall sessions with flow-based security profiles, NTurbo offloads firewall and NAT sessions from the FortiGate CPU to NP7 or NP6 network processors. NTurbo distributes these sessions to different IPS engine processes spread across multiple CPU cores, ensuring a load-balanced approach for handling IPS signature/pattern matching tasks.

upvoted 1 times

3101a6a 4 months, 3 weeks ago

Selected Answer: D

"NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface."

upvoted 2 times

CharlieS8 4 months, 3 weeks ago

It should be D.

upvoted 1 times

⊟ **fa7474b** 4 months, 3 weeks ago

Selected Answer: A

I believe this is A.

The sentence in the Admin guide reads:

NTurbo creates a special data path to redirect traffic from the ingress interface to IPS, and from IPS to the egress interface.

this is NOT the same wording as is shown in D. Meanwhile you can find the EXACT same wording as A in the admin guide.

upvoted 1 times

⊟ **fa7474b** 4 months, 1 week ago

I'm wrong, it's D. Nturbo offloads to the NP processor not the CP processor.

upvoted 2 times

⊟ **mhl2203** 5 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

⊟ **herlock_sholmes_2810** 5 months, 2 weeks ago

Selected Answer: D

"NTurbo creates a special data path to redirect traffic from the ingress interface to the IPS engine, and from the IPS engine to the egress interface."

Reference: FortiGate 7.4 Administrator Study Guide, page 201 (Inspection Modes Use Cases)

upvoted 2 times

⊟ **SalamanderHoliday888** 5 months, 3 weeks ago

Selected Answer: A

For me its A, reason is that in FortiGate 7.4 administrator page 201 both statement A and D was mentioned. Difference is that in this question it only ask how does NTurbo enhance performance for flow based which is answered in the document by offlading to CP8 or CP9 processors. If the question is leaning to antivirus processing then its D. This is just my thought.

upvoted 3 times

⊟ **StefanDinev** 5 months, 3 weeks ago

D is correct

upvoted 2 times

⊟ **fab1ccb** 5 months, 3 weeks ago

Selected Answer: D

D is the correct answer

upvoted 3 times

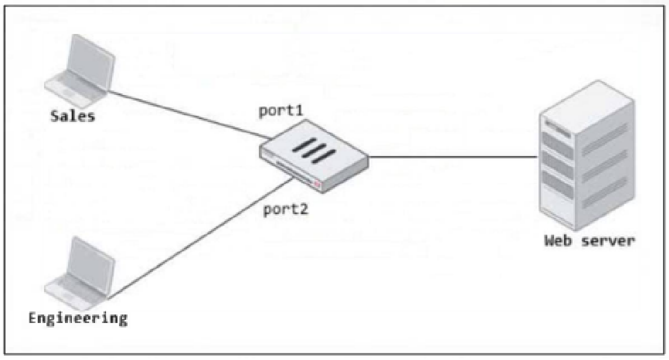
⊟ **Vdiaz** 6 months ago

D is Correct

upvoted 3 times

Question #35 Topic 1

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.
Which action must the administrator perform to consolidate the two policies into one?

A. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.

B. Create an Interface Group that includes port1 and port2 to create a single firewall policy.

C. Select port1 and port2 subnets in a single firewall policy.

D. Replace port1 and port2 with the any interface in a single firewall policy.

Suggested Answer: *A*

Community vote distribution

A (100%)

truserud 3 weeks ago

Selected Answer: A

Weird that Fortinet just forgot about using Zones with regards to this question, but yeah; enable multiple interface policies is also a way to configure this. I'd say that both A and B are valid answers though.

upvoted 1 times

sxcap 2 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: A

A correct

upvoted 1 times

Qwerty379 6 months, 1 week ago

Selected Answer: A

I feel like there should be 2 answers, like you have to enable Multiple Interface option first, and then select port1 and port2 in a single firewall policy

upvoted 4 times

andres8h 6 months, 1 week ago

Selected Answer: A

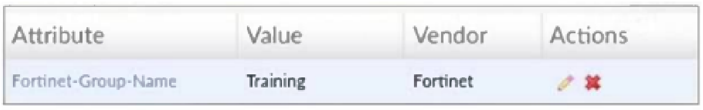
Fortigate 7.4 Adminsitrator pag 37

upvoted 4 times

Question #36

Topic 1

Refer to the exhibit, which shows a partial configuration from the remote authentication server.



Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	✎ ✖

Why does the FortiGate administrator need this configuration?

A. To authenticate only the Training user group.

B. To set up a RADIUS server Secret.

C. To authenticate and match the Training OU on the RADIUS server.

D. To authenticate Any FortiGate user groups.

Suggested Answer: *C*

Community vote distribution

A (100%)

sxcap 2 months, 3 weeks ago

Selected Answer: A

Only 1 group is defined, so only that group will authenticate

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: A

A. To authenticate only the Training user group.

upvoted 1 times

s4mu3l007 4 months, 1 week ago

ans is tha letter A

upvoted 1 times

Billyon 6 months ago

Selected Answer: A

This configuration is specifically used to authenticate users belonging to the "Training" user group, as indicated by the Fortinet-Group-Name attribute.

upvoted 2 times

TIGERZ44 6 months ago

Selected Answer: A

The Attribute is "Fortinet-GROUP-Name" so one would assume this refers to the name of a group and not an OU.

upvoted 2 times

knoor 6 months, 1 week ago

I am not sure why Training "OU" should be the answer, it looks like a LDAP attribute of group name as training so the answer should be A

upvoted 3 times

TIGERZ44 6 months ago

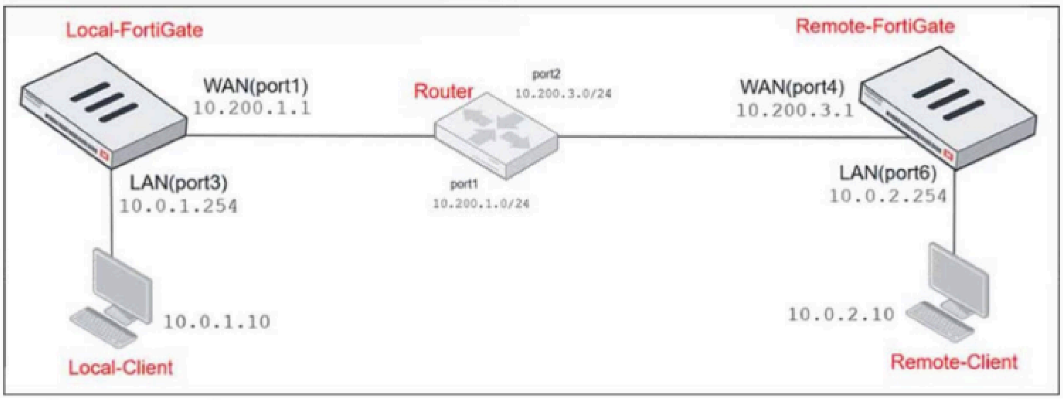
I agree. The Attribute is "Fortinet-GROUP-Name" so one would assume this refers to the name of a group and not an OU.

upvoted 2 times

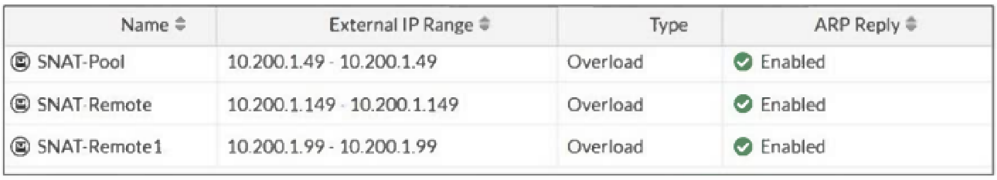
Question #37 *Topic 1*

Refer to the exhibits.

Network diagram

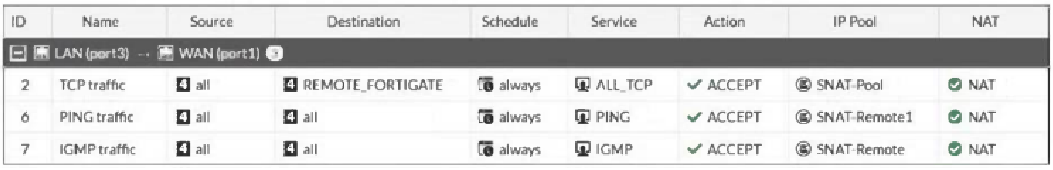


NAT IP pool configuration



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

Firewall policy



ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
⊟ LAN (port3) → WAN (port1)								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	✓ ACCEPT	SNAT-Pool	✓ NAT
6	PING traffic	all	all	always	PING	✓ ACCEPT	SNAT-Remote1	✓ NAT
7	IGMP traffic	all	all	always	IGMP	✓ ACCEPT	SNAT-Remote	✓ NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IPaddress 10.0.1.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

A. 10.200.1.1

B. 10.200.1.149

C. 10.200.1.99

D. 10.200.1.49

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **7moPain** Highly Voted 6 months ago

Selected Answer: C

C for ICMP

upvoted 5 times

⊟ **Billyon** Highly Voted 6 months ago

Selected Answer: C

C is correct, looking at the firewall policy

upvoted 5 times

⊟ **sxcap** Most Recent 2 months, 3 weeks ago

Selected Answer: C

Read well the question, is easy to fall in a trick, you would choose B if you don't read that there is a PING policy that matches the rithg answer: C

upvoted 2 times

Charly0710 3 months, 1 week ago

Selected Answer: C

It's C obviously

upvoted 2 times

vuhidus 3 months, 3 weeks ago

Selected Answer: C

It's C

upvoted 2 times

s4mu3l007 4 months, 1 week ago

C is tha ans, Considering the policy

upvoted 1 times

fab1ccb 5 months, 3 weeks ago

Selected Answer: C

C is the correct answer beacuse matched the policy ID 6 for the releated traffic

upvoted 4 times

ShrekAlmighty 6 months, 1 week ago

Id Agree that C would be correct. All_TCP doesn't include ICMP. So you would match rule ID 2, in which uses IP Poop remote 1. So answer is C.

upvoted 3 times

andres8h 6 months, 1 week ago

Selected Answer: C

C is correct

upvoted 5 times

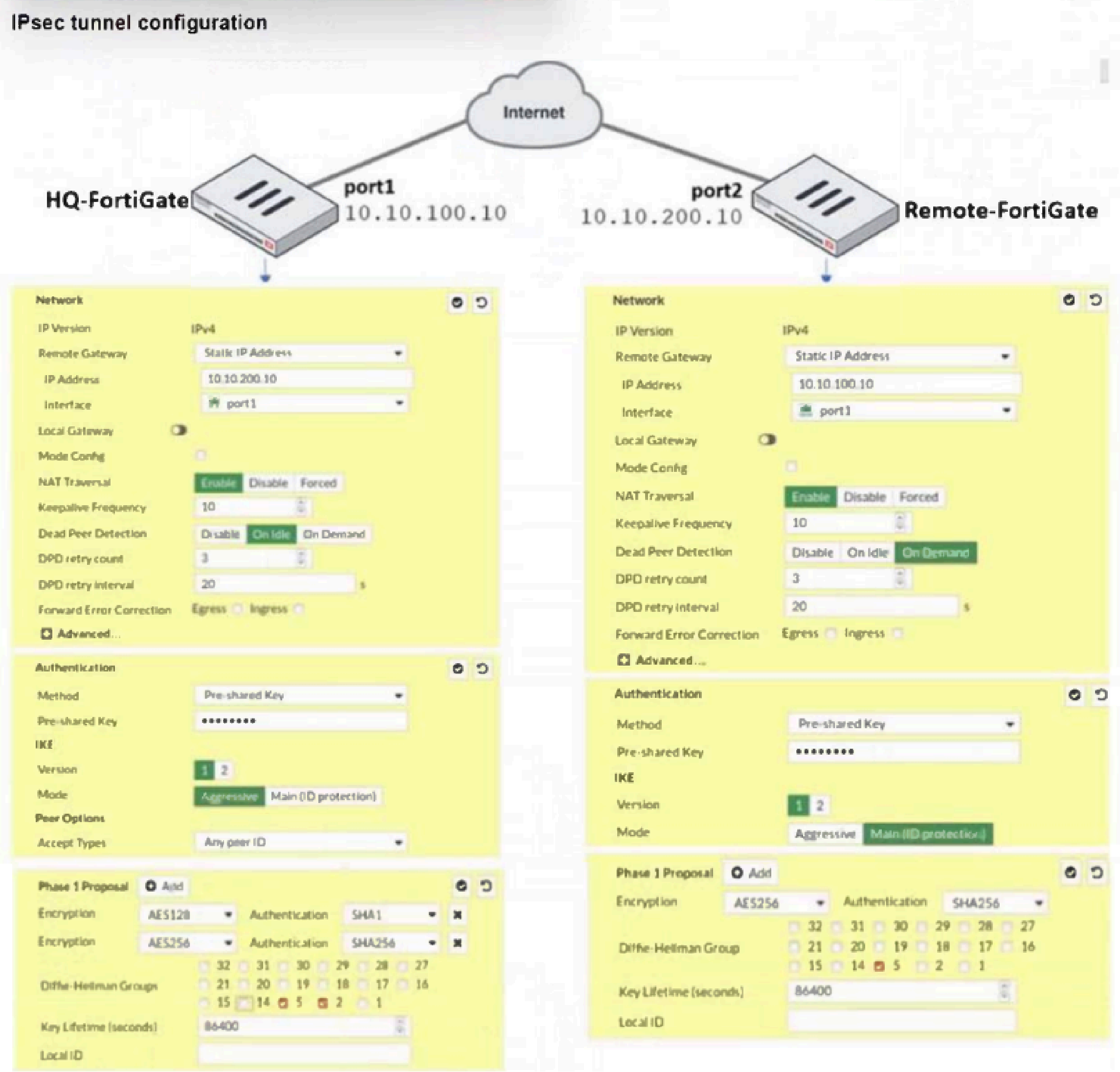
Veritas007 6 months, 2 weeks ago

Answer should be 10.200.1.99

upvoted 4 times

Question #38 Topic 1

Refer to the exhibit.



HQ-FortiGate

Network
IP Version: IPv4
Remote Gateway: Static IP Address
IP Address: 10.10.200.10
Interface: port1
Local Gateway
Mode Config □
NAT Traversal: [✓ Enable] Disable Forced
Keepalive Frequency: 10
Dead Peer Detection: Disable [✓ On Idle] On Demand
DPD retry count: 3
DPD retry interval: 20 s
Forward Error Correction: Egress □ Ingress □
Advanced...

Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version: [✓ 1] 2
Mode: [✓ Aggressive] Main (ID protection)
Peer Options
Accept Types: Any peer ID

Phase 1 Proposal Add
Encryption: AES128 Authentication: SHA1
Encryption: AES256 Authentication: SHA256
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 ☑ 2 □ 1
Key Lifetime (seconds): 86400
Local ID

Remote-FortiGate

Network
IP Version: IPv4
Remote Gateway: Static IP Address
IP Address: 10.10.100.10
Interface: port1
Local Gateway
Mode Config □
NAT Traversal: [✓ Enable] Disable Forced
Keepalive Frequency: 10
Dead Peer Detection: Disable On Idle [✓ On Demand]
DPD retry count: 3
DPD retry interval: 20 s
Forward Error Correction: Egress □ Ingress □
Advanced...

Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version: [✓ 1] 2
Mode: Aggressive [✓ Main (ID protection)]

Phase 1 Proposal Add
Encryption: AES256 Authentication: SHA256
Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 ☑ 5 □ 2 □ 1
Key Lifetime (seconds): 86400
Local ID

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

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

A. On HQ-FortiGate, disable Diffie-Helman group 2.

B. On Remote-FortiGate, set port2 as Interface.

C. On both FortiGate devices, set Dead Peer Detection to On Demand.

D. On HQ-FortiGate, set IKE mode to Main (ID protection).

Suggested Answer: *BD*

Community vote distribution

BD (100%)

ShrekAlmighty Highly Voted 6 months, 1 week ago

Selected Answer: BD

Based on the phase 1 configuration and the diagram shown in the exhibit, the administrator can make the following two configuration changes to bring phase 1 up:

B. On Remote-FortiGate, set port2 as Interface: The diagram indicates that port2 is currently not selected under 'Interface' for Remote-FortiGate. Aligning this setting with HQ-FortiGate, which has port1 set as Interface, might resolve inconsistencies.

D. On HQ-FortiGate, set IKE mode to Main (ID protection): The current setting on HQ-FortiGate is Aggressive for IKE mode, while Remote-FortiGate is set to Main mode. Matching these settings may help in establishing phase 1 of the IPsec tunnel.

upvoted 8 times

⊟ **sxcap** Most Recent 2 months, 3 weeks ago

Selected Answer: BD

B and D, because must select the same IKE method and the remote fortigate is connected to port 2 not port 1

upvoted 1 times

⊟ **Charly0710** 3 months, 2 weeks ago

Selected Answer: BD

Answer B: It is obvious that the interface must be properly configured with what is physically connected in the diagram

Answer D:

upvoted 1 times

⊟ **vuhidus** 3 months, 3 weeks ago

Selected Answer: BD

B & D

upvoted 1 times

⊟ **s4mu3l007** 4 months, 1 week ago

The answer are B and D

upvoted 1 times

Question #39

Topic 1

A network administrator has configured an SSL/SSH inspection profile defined for full SSL inspection and set with a private CA certificate. The firewall policy that allows the traffic uses this profile for SSL inspection and performs web filtering. When visiting any HTTPS websites, the browser reports certificate warning errors.

What is the reason for the certificate warning errors?

A. The SSL cipher compliance option is not enabled on the SSL inspection profile. This setting is required when the SSL inspection profile is defined with a private CA certificate.

B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

C. The browser does not recognize the certificate in use as signed by a trusted CA.

D. With full SSL inspection it is not possible to avoid certificate warning errors at the browser level.

Suggested Answer: *C*

Community vote distribution

C (100%)

wsdeffwd Highly Voted 👍 6 months ago

Selected Answer: C

Page 173

upvoted 6 times

sxcap Most Recent 6 2 months, 3 weeks ago

Selected Answer: C

C, certificate is not recognized due to used a private CA, you must install the certificate in the end user devices or use a public SSL CA

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: C

C right one

upvoted 1 times

f3eb371 3 months, 4 weeks ago

Selected Answer: C

C is this

upvoted 1 times

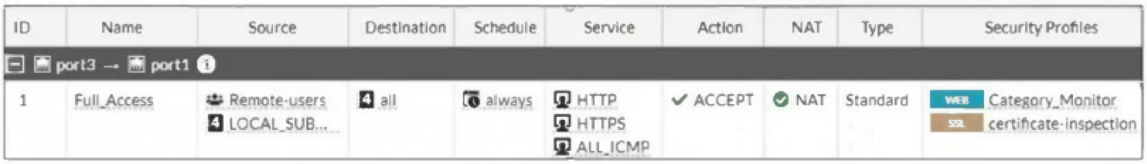
s4mu3l007 4 months ago

ans is the C

upvoted 1 times

Question #40 Topic 1

Refer to the exhibit.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	✓ ACCEPT	NAT	Standard	WEB Category_Monitor SSL certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?

A. The Service DNS is required in the firewall policy.

B. The user is using an incorrect user name.

C. The Remote-users group is not added to the Destination.

D. No matching user account exists for this user.

Suggested Answer: *A*

Community vote distribution

A (100%)

fa7474b Highly Voted 5 months ago

Selected Answer: A

Just confirmed the answer is A by replicating this config on my Fortigate. If you don't add DNS to the policy you just get a timeout and the browser cannot find the site.

Once you add DNS you get a prompt that you must log in to access the internet.

I think the confusing part of this question is that it reads as if the user is able to access the internet and is not being prompted. When in fact, they are not getting prompted AND they can't access the internet.

upvoted 9 times

bob511 Highly Voted 6 months, 1 week ago

A. page 115 in fortigate 7.4 admin guide

upvoted 5 times

sxcap Most Recent 2 months, 3 weeks ago

Selected Answer: A

DNS Service is required for authentication

upvoted 2 times

Kunot 2 months, 3 weeks ago

Selected Answer: D

what if user account is not on remote-user?

upvoted 1 times

vuhidus 3 months, 3 weeks ago

Selected Answer: A

A. The Service DNS is required in the firewall policy.

upvoted 2 times

s4mu3l007 4 months, 1 week ago

are correct, A

upvoted 2 times

herlock_sholmes_2810 5 months, 3 weeks ago

Selected Answer: A

A. The Service DNS is required in the firewall policy.

"DNS traffic can be allowed if user has not authenticated yet

Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate
DNS service must be explicity listed as a service in the policy"

Reference: FortiGate 7.4 Administration Study Guide, page 115 (Firewall Policy - Service)

upvoted 2 times

Knocks 5 months, 3 weeks ago

Selected Answer: A

It cannot be B, also because the user is never promped to login.

upvoted 2 times

miguelmagr 5 months, 2 weeks ago

If you selected B it says that you are only being advised that the username/password is incorrect and you can re-type the credentials but the login prompt would appear.

upvoted 1 times

TIGERZ44 6 months ago

Selected Answer: A

A firewall policy also checks the service in order to transport the named protocols or group of protocols. No service (with the exception of DNS) is allowed through the firewall policy before successful user authentication. DNS is usually used by HTTP so that people can use domain names for websites, instead of their IP address. DNS is allowed because it is a base protocol and will most likely be required to initially see proper authentication protocol traffic. Hostname resolution is almost always a requirement for any protocol. However, the DNS service must still be defined in the policy as allowed, in order for it to pass.

A is the correct answer

upvoted 2 times

wsdeffwd 6 months ago

Selected Answer: A

Page 115

upvoted 5 times