Question #1 *Topic 1*

Examine the FortiGate configuration:

```
config user settings
     set auth-on-demand implicitly
end
```

What will happen to unauthenticated users when an active authentication policy is followed by a fall through policy without authentication?

A. The user must log in again to authenticate.

B. The user will be denied access to resources without authentication.

C. The user will not be prompted for authentication.

D. User authentication happens at an interface level.

Suggested Answer: *A*
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46875

SebaAr22 Highly Voted 4 years, 3 months ago
C is correct, read KB
upvoted 9 times

pollyy Highly Voted 4 years, 2 months ago
Correct - C - https://docs.fortinet.com/document/fortigate/6.2.0/new-features/238665/authentication-policy-extensions
upvoted 6 times

MEDO162 Most Recent 3 years, 11 months ago
If there is a fall-through policy in place, unauthenticated users will no be prompted for authentication.
C is correct
upvoted 1 times

KobeBryant0212 4 years ago
A should be the correct answer
upvoted 1 times

nilkanthy 4 years ago
C is correct
upvoted 1 times

Angel123 4 years, 2 months ago
Correct - C - FortiGate_security_6.2_Study_Guide 233
upvoted 2 times

Ho_Al 4 years, 3 months ago
I don´t know what this means
Implicitly (default) - Implicitly trigger firewall authentication on demand.
upvoted 1 times

Question #2 *Topic 1*

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

A. FG-traffic VDOM

B. Root VDOM

C. Customer VDOM

D. Global VDOM

Suggested Answer: *B*
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/new-features/287377/split-task-vdom-support

MEDO162 3 years, 11 months ago

If you enable split-task VDOM mode on the upstream FGT device, it can allow downstream FGT devices to join the Security Fabric in the root and FG-Traffic VDOMs.
If split-task VDOM mode is enabled on the downstream FortiGate, it can only connect to the upstream FortiGate through the downstream FortiGate interface on the root VDOM.
B is correct.

upvoted 2 times

AOC 4 years ago

correcto

upvoted 1 times

pollyy 4 years, 2 months ago

Correct - B - NSE4_FGT-6.2-Infrastructure_Manual, p. 112

upvoted 2 times

Question #3 *Topic 1*

In an HA cluster operating in active-active mode, which path is taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

A. Client > secondary FortiGate > primary FortiGate > web server

B. Client > primary FortiGate > secondary FortiGate > primary FortiGate > web server

C. Client > primary FortiGate > secondary FortiGate > web server

D. Client > secondary FortiGate > web server

Suggested Answer: *C*

DmitriyS 4 years ago

Correct -C - Infrastructure_Manual-6.2, p.335

upvoted 1 times

AOC 4 years ago

Correcto es la C

upvoted 2 times

amihai 4 years, 2 months ago

Correct - C

upvoted 3 times

pollyy 4 years, 2 months ago

Sorry, Correct is C

upvoted 3 times

pollyy 4 years, 2 months ago

Correct - B - Infrastructure_Manual-6.2, p.316

upvoted 2 times

Question #4 *Topic 1*

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, antivirus buffers the whole file for scanning, before sending it to the client.

B. In full scan flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.

C. In proxy-based inspection mode, files bigger than the buffer size are scanned.

D. In quick scan mode, you can configure antivirus profiles to use any of the available antivirus signature databases.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

wwwwaaaa 1 year, 5 months ago

Selected Answer: AB

otherwise answers are not correct in general

upvoted 1 times

AOC 4 years ago

a y b, correcto

upvoted 1 times

pollyy 4 years, 2 months ago

Correct - A,B - Security_Manual-6.2, p.478, p.484

upvoted 3 times

Question #5 *Topic 1*

The FSSO collector agent set to advanced access mode for the Windows Active Directory uses which convention?

A. LDAP

B. Windows

C. RSSO

D. NTLM

Suggested Answer: *A*

AOC 4 years ago

A, pagina 236 del infraestructure

upvoted 1 times

bwman 4 years, 1 month ago

A is coorect :

- Advanced: The FSSO Collector Agent obtains user group information using LDAP.

https://kb.fortinet.com/kb/documentLink.do?externalID=FD36607

upvoted 1 times

Question #6 *Topic 1*

Which two statements about virtual domains (VDOMs) are true? (Choose two.)

A. Transparent mode and NAT mode VDOMs cannot be combined on the same FortiGate.

B. Each VDOM can be configured with different system hostnames.

C. Different VLAN subinterfaces of the same physical interface can be assigned to different VDOMs.

D. Each VDOM has its own routing table.

Suggested Answer: *CD*

AOC 4 years ago

c y d correcto

upvoted 2 times

jorgeoscar90 4 years, 2 months ago

B and D. Two VDOMs cannot share the same interface or VLAN

upvoted 3 times

> **Angel123** 4 years, 2 months ago
>
> "Note that in multi-VDOM environment, the physical interface and its VLAN sub-interface can be in separate VDOMs."
>
> Infrastructure_Manual-6.2, p.156
>
> upvoted 7 times

pollyy 4 years, 2 months ago

C & D are correct - https://kb.fortinet.com/kb/documentLink.do?externalID=FD31639

upvoted 3 times

pollyy 4 years, 2 months ago

C & D are correct - Infrastructure_Manual-6.2, p.107, p.125

upvoted 4 times

Question #7 *Topic 1*

What three FortiGate components are tested during the hardware test? (Choose three.)

A. CPU

B. Administrative access

C. HA heartbeat

D. Hard disk

E. Network interfaces

Suggested Answer: *ADE*

pollyy 4 years, 2 months ago

A,D,E are correct - Infrastructure_Manual-6.2, p. 406

upvoted 4 times

Question #8 *Topic 1*

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not.
Which configuration option is the most effective way to support this request?

A. Implement web filter authentication for the specified website.

B. Implement a web filter category override for the specified website.

C. Implement DNS filter for the specified website.

D. Implement web filter quotas for the specified website.

Suggested Answer: *B*

Angel123 Highly Voted 4 years, 2 months ago

A is correct answer.
Since both A and B are working options, answer B needs one more Web filter profile - the one that will allow access to the category in which resides website's domain name.
In both cases a custom category is needed and a rating override, which will assign the website to that category.
The question is "Which configuration option is the most effective way to support this request" in that case this is answer A

upvoted 9 times

pollyy Highly Voted 4 years, 2 months ago

For me A sounds correct, not B

upvoted 6 times

jaz600 4 years, 2 months ago

I concur

upvoted 1 times

kirades Most Recent 2 years, 1 month ago

A and B are correct, in 7.0 there's two answer for this question.

upvoted 2 times

Jrr 4 years, 2 months ago

For me it is ok the B, since the authentication is to a category not to a specific url.

upvoted 1 times

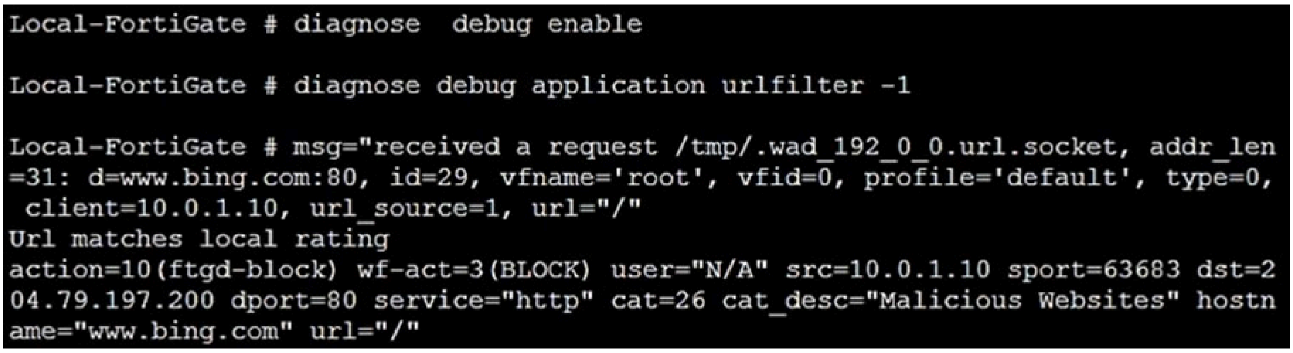
pollyy 4 years, 2 months ago

Refer to the Security_Manual-6.2, p.380

upvoted 6 times

Question #9 *Topic 1*

Examine the exhibit, which shows the output of a web filtering real time debug.



```
Local-FortiGate # diagnose  debug enable

Local-FortiGate # diagnose debug application urlfilter -1

Local-FortiGate # msg="received a request /tmp/.wad_192_0_0.url.socket, addr_len
=31: d=www.bing.com:80, id=29, vfname='root', vfid=0, profile='default', type=0,
 client=10.0.1.10, url_source=1, url="/"
Url matches local rating
action=10(ftgd-block) wf-act=3(BLOCK) user="N/A" src=10.0.1.10 sport=63683 dst=2
04.79.197.200 dport=80 service="http" cat=26 cat_desc="Malicious Websites" hostn
ame="www.bing.com" url="/"
```

Why is the site www.bing.com being blocked?

A. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.

B. The user has not authenticated with the FortiGate yet.

C. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.

D. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

Suggested Answer: *D*

AOC 4 years ago

Correcto, es la d

upvoted 1 times

Sachitha28 4 years ago

D is correct

upvoted 1 times

gordonF 4 years, 1 month ago

agree with pollyyy

upvoted 1 times

pollyy 4 years, 2 months ago

It seems that D is correct based on debug "URL matches a local rating" and https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122974/web-rating-override

upvoted 4 times

Question #10 *Topic 1*

When using WPAD DNS method, which FQDN format do browsers use to query the DNS server?

A. srv_proxy.<local-domain>/wpad.dat

B. srv_tcp.wpad.<local-domain>

C. wpad.<local-domain>

D. proxy.<local-domain>.wpad

Suggested Answer: *C*

pollyy Highly Voted 4 years, 2 months ago

C is correct according to the Infrastructure_Manual, p. 343

upvoted 5 times

MSAU Most Recent 3 years, 8 months ago

C and the page is Infrastructure - 363.

upvoted 1 times

AOC 4 years ago

C es la correcta.

upvoted 2 times

Sachitha28 4 years ago

C is the answer

upvoted 2 times

Question #11 *Topic 1*

Consider a new IPsec deployment with the following criteria:

✑ All satellite offices must connect to the two HQ sites.

✑ The satellite offices do not need to communicate directly with other satellite offices.

✑ Backup VPN is not required.

✑ The design should minimize the number of tunnels being configured.

Which topology should you use to satisfy all of the requirements?

A. Partial mesh

B. Redundant

C. Full mesh

D. Hub-and-spoke

Suggested Answer: *D*

MunzerR Highly Voted 4 years ago

Answer is D,,,

if the Backup is required in this case,,,,will be Partial mesh

upvoted 7 times

MSAU Most Recent 3 years, 8 months ago

A. - Partial mesh

upvoted 1 times

AOC 4 years ago

La respuesta correcta es la D porque deben conectarse con 2 HQ

upvoted 2 times

mau_80 4 years ago

Partial Mesh is the corect answer

upvoted 1 times

Question #12 *Topic 1*

What criteria does FortiGate use to look for a matching firewall policy to process traffic? (Choose two.)

A. Services defined in the firewall policy.

B. Incoming and outgoing interfaces

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

D. Lowest to highest policy ID number.

Suggested Answer: *AB*

AOC 4 years ago

AyB Correcto. De acuerdo con gordonF

upvoted 3 times

gordonF 4 years, 1 month ago

Incoming Interface
Outgoing Interface
Source: IP address, user
Destination: IP address or Internet Services
Service: IP protocol and port number
Schedule: applies during configured times

upvoted 1 times

Cyril_the_Squirl 3 years, 12 months ago

The order is in fact like so:

Incoming Interface
Source: IP address, user
Outgoing Interface
Destination: IP address or Internet Services
Service: IP protocol and port number
Schedule: applies during configured times

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

A & B are correct

upvoted 1 times

siscoFe 3 years, 10 months ago

There is a difference between how the GUI displays the Policy config parameters order and how the packet is processed when traversing. A and B are correct answers since they are required during the policy configuration.

upvoted 1 times

gordonF 4 years, 1 month ago

Confirm A and B.
fortigate security pg 99 and 100

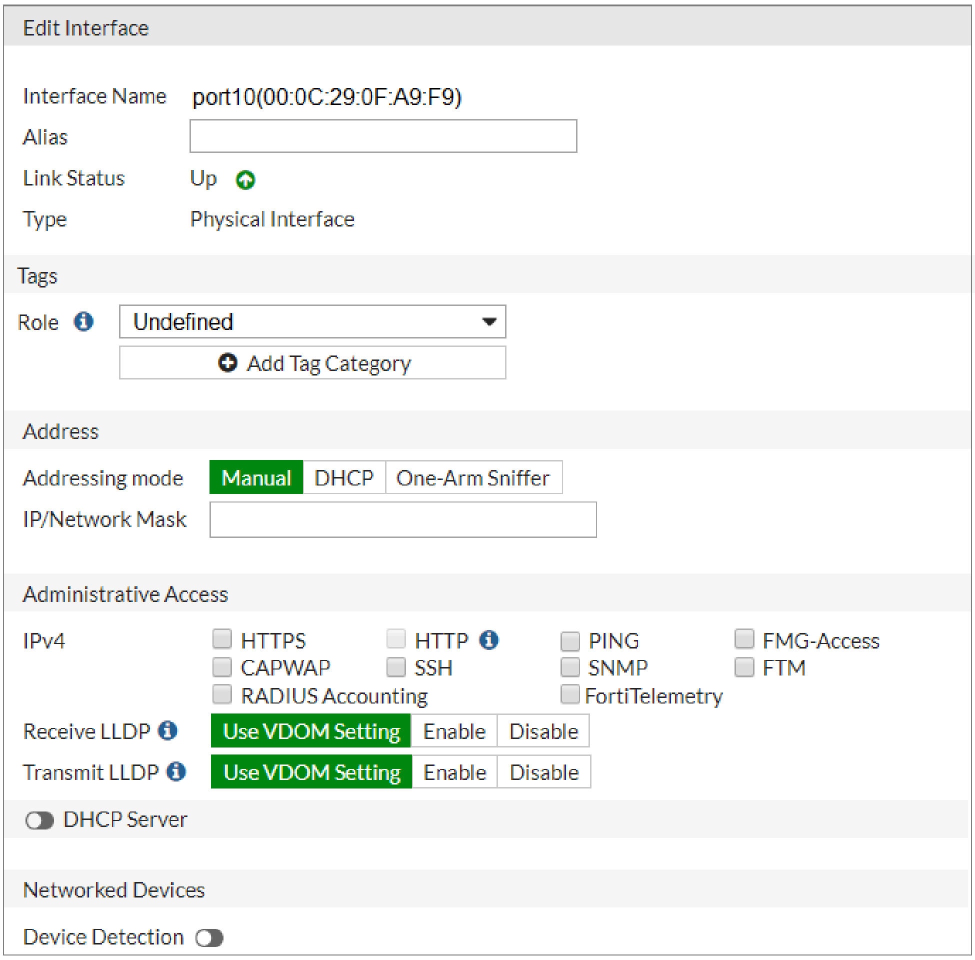
upvoted 1 times

Question #13 *Topic 1*

Refer to the exhibit.

You are configuring the root FortiGate to implement the Security Fabric. You are configuring port10 to communicate with a downstream FortiGate.

The exhibit shows the default Edit Interface.



Edit Interface

Interface Name port10(00:0C:29:0F:A9:F9)

Alias

Link Status Up

Type Physical Interface

Tags

Role Undefined

Add Tag Category

Address

Addressing mode [✓ Manual] DHCP One-Arm Sniffer

IP/Network Mask

Administrative Access

IPv4 □ HTTPS □ HTTP □ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ FTM □ RADIUS Accounting □ FortiTelemetry

Receive LLDP [✓ Use VDOM Setting] Enable Disable

Transmit LLDP [✓ Use VDOM Setting] Enable Disable

DHCP Server

Networked Devices

Device Detection

When configuring the root FortiGate to communicate with a downstream FortiGate, which two settings must you configure? (Choose two.)

A. Enable Device Detection

B. Administrative Access: FortiTelemetry.

C. IP/Network Mask.

D. Role: Security Fabric.

Suggested Answer: *BC*

Katorcio Highly Voted 4 years, 2 months ago

Hi,

i think B & C are correct. If the question is right, they ask about what you have to configure just on the ROOT FORTIGATE.

In Security_Manual-6.2, p.69 is written about DEVICE DETECTION about the downstream FortiGate, not about the root FortiGate.

upvoted 5 times

JOY099 Most Recent 3 years, 10 months ago

A & B is the correct answer

upvoted 1 times

AOC 4 years ago

Correcto AyB

upvoted 2 times

Ping2Jo 4 years ago

B & C is correct. The question is about ROOT Fortigate and FortiTelemetry & IP address are the must in order to communicate to downstream FortiGate.
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/788897/fortigate
upvoted 2 times

Typhoeus 4 years, 1 month ago
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/788897/fortigate
Device request
A device can request to join the Security Fabric from another FortiGate, but it must have the IP address of the root FortiGate. The administrator of the root FortiGate must also authorize the device before it can join the Security Fabric.

The root FortiGate must have FortiTelemetry enabled on the interface that the device connects to.

To enable FortiTelemetry on an interface:
Go to Network > Interfaces.
Edit the interface that the device that you authorizing to join the Security Fabric is connected to.
Under Administrative Access, enable FortiTelemetry.
Under Networked Devices, turn on Device Detection.
upvoted 1 times

gordonF 4 years, 1 month ago
Agree A and B: pg 260 fg security
upvoted 1 times

pollyy 4 years, 2 months ago
Sorry A & B are correct - the screenshot is from the network interface configuration not from the Security Fabric Settings, Security_Manual-6.2, p.68 - 69
upvoted 2 times

yemicontrol 4 years, 2 months ago
I AGREE WITH YOU A & B CORRECT
upvoted 2 times

jorgeoscar90 4 years, 2 months ago
B and C. Without IP/Mask the fortigate can't talk on the network.
upvoted 2 times

pollyy 4 years, 2 months ago
Correct B & C - Security_Manual-6.2, p.68
upvoted 2 times

fg488493 4 years, 2 months ago
Hi Sir
I think A&B
I see Security_Manual-6.2, p.68 and there tell me" you must enable FortiTelemetry, Connect to upstream Fortigate, and Device Detection on the interfaces facing downstream Fortigate device."
upvoted 3 times

jaz600 4 years, 2 months ago
Device detection for detecting endpoints not Forti devices.
upvoted 1 times

Question #14 *Topic 1*

Which two statements about NTLM authentication are correct? (Choose two.)

A. It requires DC agents on every domain controller when used in multidomain environments.

B. It is useful when users log in to DCs that are not monitored by a collector agent.

C. It requires NTLM-enabled web browsers.

D. It takes over as the primary authentication method when configured alongside FSSO.

Suggested Answer: *BC*

Reference:

https://www.fortinetguru.com/2016/07/configuring-authenticated-access/12/

pollyy Highly Voted 4 years, 2 months ago

B & C - correct - Infrastructure_Manual-6.2, p. 252

upvoted 5 times

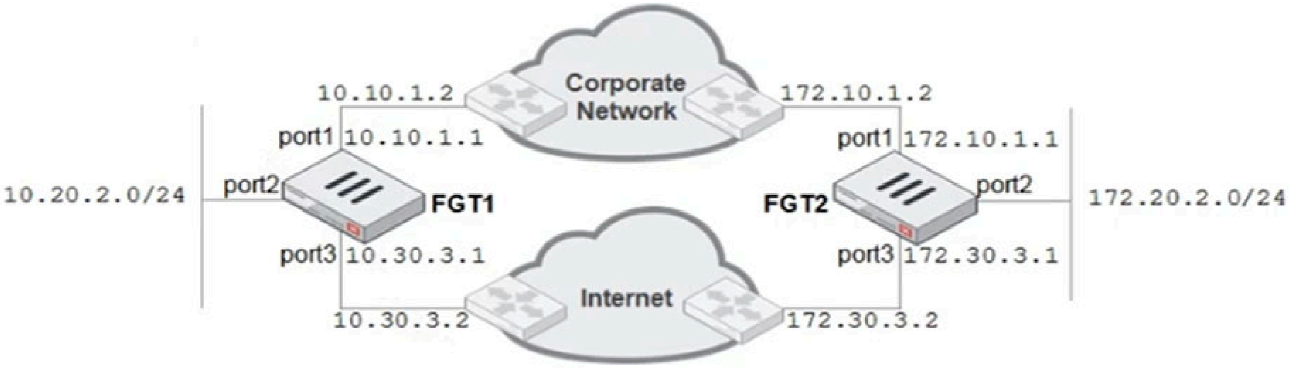
AOC Most Recent 4 years ago

ByC correcto. De acuerdo con pollyy

upvoted 1 times

Question #15 *Topic 1*

Refer to the exhibit.



A firewall administrator must configure equal cost multipath (ECMP) routing on FGT1 to ensure both port1 and port3 links are used, at the same time, for all traffic destined for 172.20.2.0/24.

Given the network diagram shown in the exhibit, which two static routes will satisfy this requirement on FGT1? (Choose two.)

A. 172.20.2.0/24 [1/0] via 10.10.1.2, port1 [0/0]

B. 172.20.2.0/24 [25/0] via 10.30.3.2, port3 [5/0]

C. 172.20.2.0/24 [25/0] via 10.10.1.2, port1 [5/0]

D. 172.20.2.0/24 [1/150] via 10.30.3.2, port3 [10/0]

Suggested Answer: *BC*

AOC 4 years ago

Correcto, b y c .

upvoted 1 times

pollyy 4 years, 2 months ago

and priority of 5

upvoted 1 times

pollyy 4 years, 2 months ago

B & C - correct - equal distance of 25

upvoted 4 times

Question #16 *Topic 1*

On a FortiGate with a hard disk, how frequently can you upload logs to FortiAnalyzer or FortiManager? (Choose two.)

A. On-demand

B. Hourly

C. Every 5 minutes

D. In real time

Suggested Answer: *CD*

AOC 4 years ago

Correcto, c y d.

upvoted 1 times

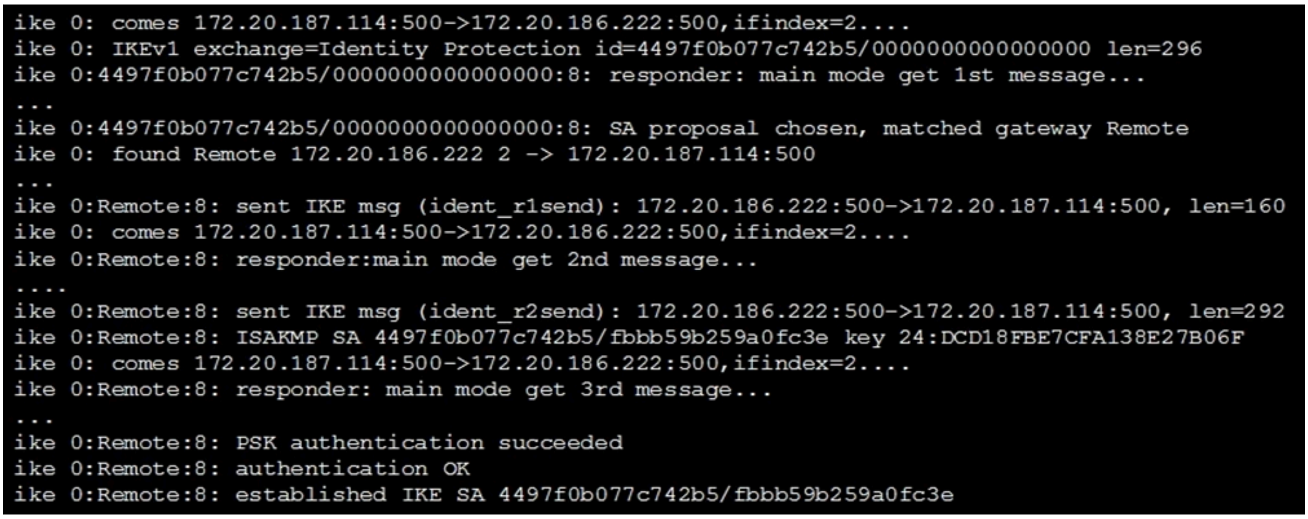
pollyy 4 years, 2 months ago

Correct is C & D - Security_Manual, p. 275

upvoted 3 times

Question #17 Topic 1

Refer to the exhibit.



```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

Given the partial output of an IKE real-time debug shown in the exhibit, which statement about the output is true?

A. The VPN is configured to use pre-shared key authentication.

B. Extended authentication (XAuth) was successful.

C. Remote is the host name of the remote IPsec peer.

D. Phase 1 went down.

Suggested Answer: *A*

pollyy Highly Voted 4 years, 2 months ago

Correct is A - PSK authentication succeeded

upvoted 6 times

ali_red Most Recent 3 years, 12 months ago

A for sure

upvoted 2 times

AOC 4 years ago

Correcto, A.

upvoted 1 times

Question #18 *Topic 1*

An administrator needs to create an SSL-VPN connection for accessing an internal server using the bookmark, Port Forward.
Which step must the administrator take to successfully achieve this configuration?

A. Configure an SSL VPN realm for clients to use the Port Forward bookmark.

B. Configure the client application to forward IP traffic through FortiClient.

C. Configure the virtual IP address to be assigned to the SSL VPN users.

D. Configure the client application to forward IP traffic to a Java applet proxy.

Suggested Answer: *D*

⊟ **MSAU** 3 years, 8 months ago

It should be A

upvoted 1 times

⊟ **AOC** 4 years ago

Correcto, es la d

upvoted 1 times

⊟ **pollyy** 4 years, 2 months ago

D is correct - Security_Manual, p. 590

upvoted 2 times

Question #19 *Topic 1*

Which two static routes are not maintained in the routing table? (Choose two.)

A. Dynamic routes

B. Policy routes

C. Named Address routes

D. ISDB routes

Suggested Answer: *CD*

Reference:

https://help.fortinet.com/fadc/4-8-0/olh/Content/FortiADC/handbook/routing_static.htm

⊟ **variaj8** Highly Voted 👍 4 years, 3 months ago

The correct answer is B & D, I created a Named Address Route in my firewall and apears in the routing table.

upvoted 7 times

⊟ **AOC** Most Recent ⏱ 4 years ago

Correcto b y d.

upvoted 1 times

⊟ **pollyy** 4 years, 2 months ago

B & D are corrects - Infrastructure_Manual-6.2, p. 14

upvoted 4 times

⊟ **SebaAr22** 4 years, 3 months ago

B & D are corrects

upvoted 4 times

⊟ **NETeng01** 4 years, 3 months ago

B D for me also

upvoted 4 times

Question #20 *Topic 1*

An administrator wants to configure a FortiGate as a DNS server. FotiGate must use a DNS database first, and then relay all irresolvable queries to an external
DNS server. Which DNS method must you use?

A. Recursive

B. Non-recursive

C. Forward to primary and secondary DNS

D. Forward to system DNS

Suggested Answer: *A*

AOC 4 years ago

Correcto, a.

upvoted 1 times

pollyy 4 years, 2 months ago

A is correct

upvoted 3 times

Question #21 *Topic 1*

Which two FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Creating an SD-WAN route for individual member interfaces

B. Creating an SD-WAN rule to route traffic based on link latency

C. Creating a static route with a named address object

D. Creating a static route with an Internet services object

Suggested Answer: *BD*

⊟ **pollyy** Highly Voted 👍 4 years, 2 months ago

B & D - correct - Infrastructure_Manual-6.2, p.94

upvoted 8 times

⊟ **tochno** Most Recent ⏱ 4 years ago

B & D are correct. SD-WAN rules are treated as policy routes.

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/793167/configuring-sd-wan-rules

upvoted 3 times

⊟ **rhylos** 4 years, 1 month ago

A & D correct. infrastructure_Manual-6.2, p.15

upvoted 1 times

⊟ **pollyy** 4 years, 2 months ago

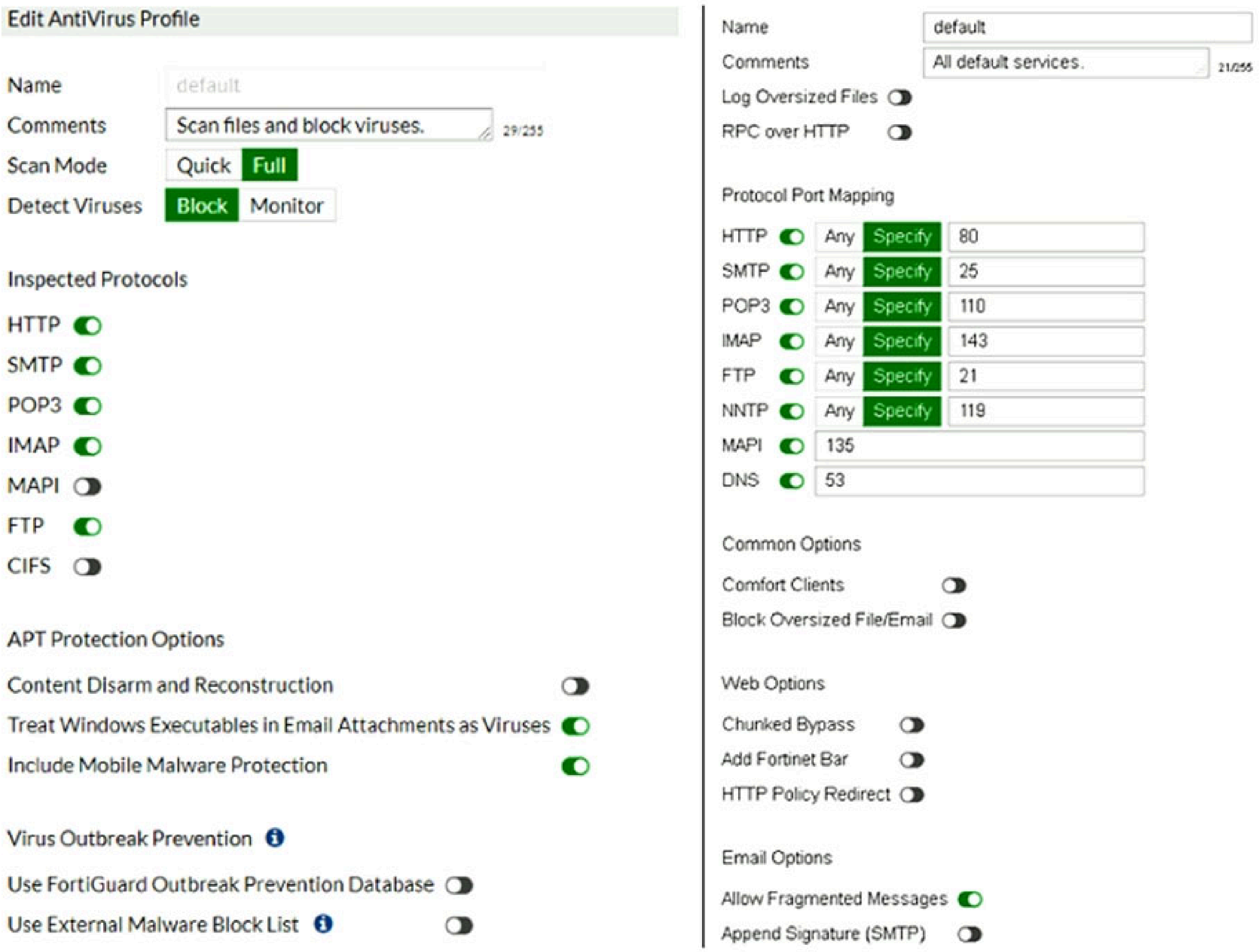
Infrastructure_Manual-6.2, p.15

upvoted 2 times

Question #22 Topic 1

Refer to the exhibits.

AV profile



Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
Scan Mode	Quick [✓ Full]
Detect Viruses	[✓ Block] Monitor

Inspected Protocols

- HTTP ●
- SMTP ●
- POP3 ●
- IMAP ●
- MAPI ○
- FTP ●
- CIFS ○

APT Protection Options

- Content Disarm and Reconstruction ○
- Treat Windows Executables in Email Attachments as Viruses ●
- Include Mobile Malware Protection ●

Virus Outbreak Prevention

- Use FortiGuard Outbreak Prevention Database ○
- Use External Malware Block List ○

Name	default
Comments	All default services. 21/255
Log Oversized Files	○
RPC over HTTP	○

Protocol Port Mapping

HTTP	●	Any [✓ Specify]	80
SMTP	●	Any [✓ Specify]	25
POP3	●	Any [✓ Specify]	110
IMAP	●	Any [✓ Specify]	143
FTP	●	Any [✓ Specify]	21
NNTP	●	Any [✓ Specify]	119
MAPI	●		135
DNS	●		53

Common Options

- Comfort Clients ○
- Block Oversized File/Email ○

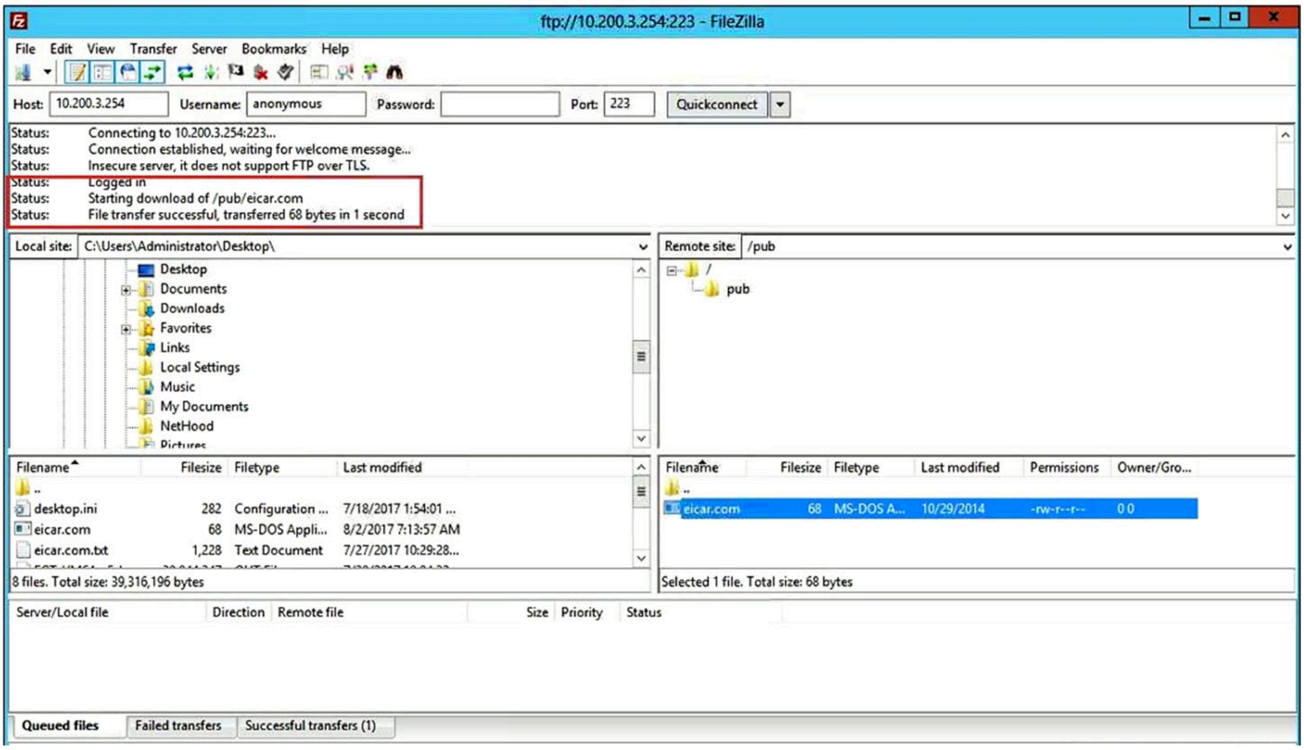
Web Options

- Chunked Bypass ○
- Add Fortinet Bar ○
- HTTP Policy Redirect ○

Email Options

- Allow Fragmented Messages ●
- Append Signature (SMTP) ○

File transfer output



ftp://10.200.3.254:223 - FileZilla

Host: 10.200.3.254 Username: anonymous Password: Port: 223 Quickconnect

```
Status:    Connecting to 10.200.3.254:223...
Status:    Connection established, waiting for welcome message...
Status:    Insecure server, it does not support FTP over TLS.
Status:    Logged in
Status:    Starting download of /pub/eicar.com
Status:    File transfer successful, transferred 68 bytes in 1 second
```

Local site: C:\Users\Administrator\Desktop\

Remote site: /pub

Filename	Filesize	Filetype	Last modified
..			
desktop.ini	282	Configuration ...	7/18/2017 1:54:01 ...
eicar.com	68	MS-DOS Appli...	8/2/2017 7:13:57 AM
eicar.com.txt	1,228	Text Document	7/27/2017 10:29:28...

8 files. Total size: 39,316,196 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
eicar.com	68	MS-DOS A...	10/29/2014	-rw-r--r--	0 0

Selected 1 file. Total size: 68 bytes

Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers (1)

Given the antivirus profile and file transfer output shown in the exhibits, why is FortiGate not blocking the eicar.com file over FTP download?

A. Because the proxy options profile needs to scan FTP traffic on a non-standard port

B. Because the FortiSandbox signature database is required to successfully scan FTP traffic

C. Because deep-inspection must be enabled for FortiGate to fully scan FTP traffic

D. Because FortiGate needs to be operating in flow-based inspection mode in order to scan FTP traffic

Suggested Answer: *A*

⊟ **pollyy** Highly Voted 👍 4 years, 2 months ago

A is correct - ftp is working on port 223

upvoted 10 times

⊟ **Pierrot26** Most Recent 🕒 3 years, 6 months ago

I think, it's C. There is a warning in log, cannot .... FTP over TLS.

upvoted 1 times

⊟ **AOC** 4 years ago

Correcto, a

upvoted 1 times

⊟ **Robin999** 4 years ago

i dont know whats correct but standard port for FTP is 21.
Like its used in the exhibit. has anyone good explaination?

upvoted 1 times

⊟ **fihocoy633** 3 years, 9 months ago

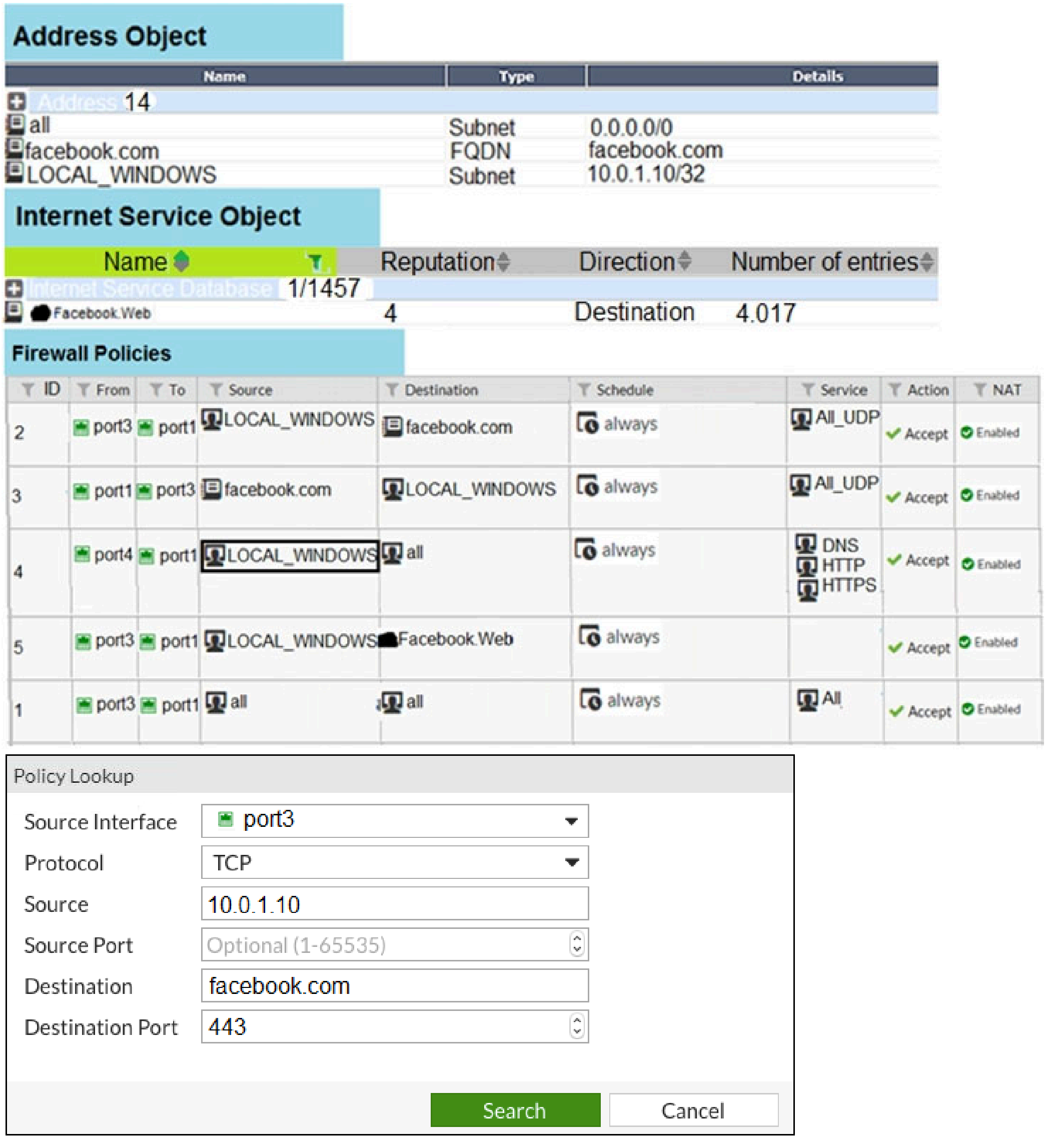
If you look at the Filezilla screenshot, the person is using ftp on port 223 (non-standard port)

upvoted 2 times

Question #23

Topic 1

Refer to the exhibit.



Address Object

Name	Type	Details
Address 14		
all	Subnet	0.0.0.0/0
facebook.com	FQDN	facebook.com
LOCAL_WINDOWS	Subnet	10.0.1.10/32

Internet Service Object

Name	Reputation	Direction	Number of entries
Internet Service Database 1/1457			
Facebook.Web	4	Destination	4.017

Firewall Policies

ID	From	To	Source	Destination	Schedule	Service	Action	NAT
2	port3	port1	LOCAL_WINDOWS	facebook.com	always	All_UDP	✓ Accept	Enabled
3	port1	port3	facebook.com	LOCAL_WINDOWS	always	All_UDP	✓ Accept	Enabled
4	port4	port1	LOCAL_WINDOWS	all	always	DNS HTTP HTTPS	✓ Accept	Enabled
5	port3	port1	LOCAL_WINDOWS	Facebook.Web	always		✓ Accept	Enabled
1	port3	port1	all	all	always	All	✓ Accept	Enabled

Policy Lookup

Source Interface	port3
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	facebook.com
Destination Port	443

The exhibits show the firewall policies and the objects used in the firewall policies. The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Based on the input criteria, which of the following will be highlighted?

A. The policy with ID 1

B. The policy with ID 5

C. The policies with ID 2 and 3

D. The policy with ID 4

Suggested Answer: *B*

pollyy Highly Voted 4 years, 2 months ago

B is correct - policy id:5::port3->port1, LOCAL_WINDOWS, Facebook,443

upvoted 9 times

serancris 4 years ago

B is correct Facebook.web is a internet service

upvoted 2 times

Murilodsant Most Recent 4 years, 1 month ago

A is correct because ISDB name is Facebook-web and not Facebook.web

upvoted 1 times

⊟ **amihai** 4 years, 2 months ago

A is correct - Because in B the destination is Facebook.web and not Facebook.com

upvoted 1 times

⊟ **jorgeoscar90** 4 years, 2 months ago

A only match udp service and not tcp 443.

upvoted 1 times

⊟ **petrus28** 4 years, 2 months ago

A. The policy with ID 1 (ID 1 matches ALL services). Where does it say it only match UDP service? I am also in doubt because like amihai said, on B says that the destination is Facebook.web and not Facebook.com

upvoted 2 times

⊟ **petrus28** 4 years, 2 months ago

Nevermind, just realized now that facebook.web is a Internet Service Object, what include facebook.com...

B is correct.

upvoted 4 times

⊟ **Ping2Jo** 4 years ago

The policy with ID 5 doesn't contain a service port.

upvoted 1 times

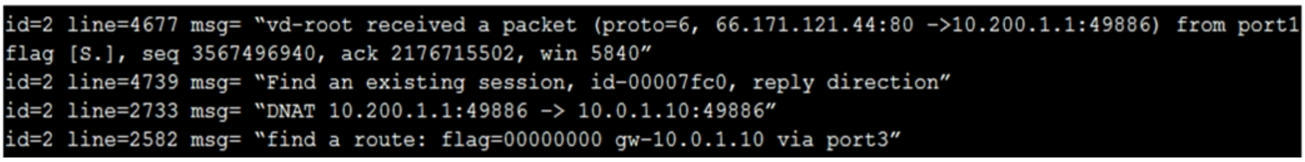
⊟ **Xunsi** 4 years ago

Tthe facebook.web contains service ports(80,443)

upvoted 1 times

Question #24 Topic 1

Refer to the exhibit.



```
id=2 line=4677 msg= “vd-root received a packet (proto=6, 66.171.121.44:80 ->10.200.1.1:49886) from port1
flag [S.], seq 3567496940, ack 2176715502, win 5840”
id=2 line=4739 msg= “Find an existing session, id-00007fc0, reply direction”
id=2 line=2733 msg= “DNAT 10.200.1.1:49886 -> 10.0.1.10:49886”
id=2 line=2582 msg= “find a route: flag=00000000 gw-10.0.1.10 via port3”
```

The exhibit shows the output from a debug flow.

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

A. The packet was allowed by the firewall policy with the ID 00007fc0.

B. The source IP address of the packet was translated to 10.0.1.10.

C. FortiGate received a TCP SYCK packet.

D. FortiGate routed the packet through port3.

Suggested Answer: *CD*

pollyy Highly Voted 4 years, 2 months ago

C & D - correct

upvoted 7 times

Melvin91 Most Recent 2 years, 6 months ago

Why B is no correct?

upvoted 1 times

jarz 3 years, 9 months ago

The source was also translated to 10.0.1.10

upvoted 1 times

AOC 4 years ago

Correcto, cyd.

upvoted 1 times

Question #25 *Topic 1*

What is required to create an inter-VDOM link between two VDOMs?

A. At least one of the VDOMs must operate in NAT mode.

B. Both VDOMs must operate in NAT mode.

C. The inspection mode of at least one VDOM must be NGFW policy-based.

D. The inspection mode of both VDOMs must match.

Suggested Answer: *A*

Angel123 Highly Voted 👍 4 years, 2 months ago

Correct answer is A according to FortiGate_Infrastructure_6.2_Study_Guide p.134

upvoted 6 times

gordonF 4 years, 1 month ago

According to which part on that page?

upvoted 1 times

eduard655 4 years ago

Note that similar to using inter-VLAN routing, Layer 3 must be involved–you cannot create an inter-VDOM link between Layer 2 transparent mode VDOMs. At least one of the VDOMs must be operating in NAT mode.

This, among other benefits, prevents potential Layer 2 loops.

upvoted 1 times

Question #26 *Topic 1*

What FortiGate configuration is required to actively prompt users for credentials?

A. You must enable one or more protocols that support active authentication on a firewall policy.

B. You must position the firewall policy for active authentication before a firewall policy for passive authentication

C. You must assign users to a group for active authentication

D. You must enable the Authentication setting on the firewall policy

Suggested Answer: *A*

AOC 4 years ago

Correcto, a

upvoted 1 times

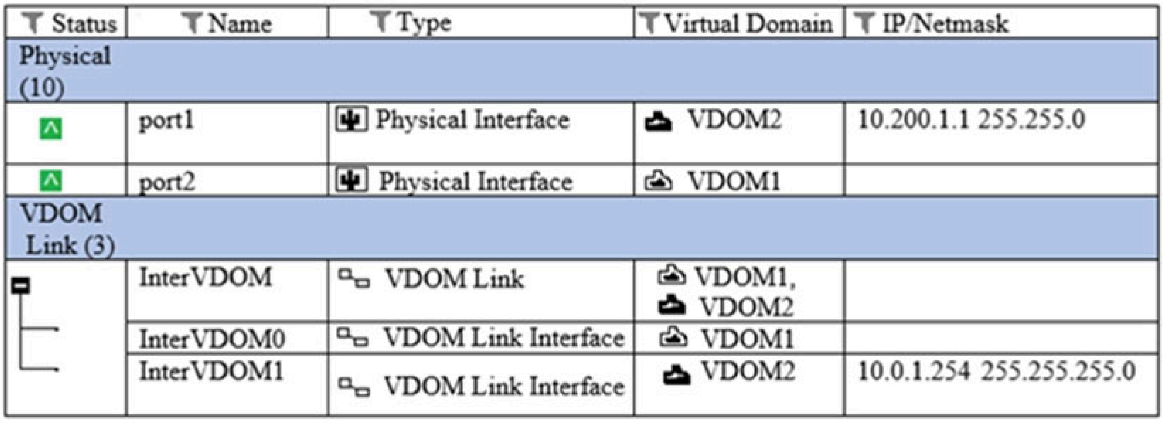
pollyy 4 years, 2 months ago

A is correct - Security_Manual-6.2, p.231

upvoted 2 times

Question #27 Topic 1

Refer to the exhibit.



Status	Name	Type	Virtual Domain	IP/Netmask
Physical (10)				
🟩	port1	Physical Interface	VDOM2	10.200.1.1 255.255.255.0
🟩	port2	Physical Interface	VDOM1	
VDOM Link (3)				
⊟	InterVDOM	VDOM Link	VDOM1, VDOM2	
	InterVDOM0	VDOM Link Interface	VDOM1	
	InterVDOM1	VDOM Link Interface	VDOM2	10.0.1.254 255.255.255.0

The exhibit shows network configurations. VDOM1 is operating in transparent mode. VDOM2 is operating in NAT mode. There is an inter-VDOM link between both VDOMs. A client workstation with the IP address 10.0.1.10/24 is connected to port2. A web server with the IP address 10.200.1.2/24 is connected to port1.

Which two options must be included in the FortiGate configuration to route and allow connections from the client workstation to the web server? (Choose two.)

A. A static or dynamic route in VDOM2 with the subnet 10.0.1.0/24 as the destination.

B. A static or dynamic route in VDOM1 with the subnet 10.200.1.0/24 as the destination.

C. One firewall policy in VDOM1 with port2 as the source interface and InterVDOM0 as the destination interface.

D. One firewall policy in VDOM2 with InterVDOM1 as the source interface and port1 as the destination interface.

Suggested Answer: *CD*

AOC 4 years ago

Correcto c y d

upvoted 1 times

pollyy 4 years, 2 months ago

C & D are correct;

A is not correct because dynamic routing is not possible between the Transparent and NAT VDOMs

upvoted 3 times

Question #28 *Topic 1*

NGFW mode allows policy-based configuration for most inspection rules.
Which security profile configuration does not change when you enable policy-based inspection?

A. Application control

B. Web filtering

C. Web proxy

D. Antivirus

Suggested Answer: *D*

⊟ **pollyy** Highly Voted 👍 4 years, 2 months ago

D is correct - Security_Manual-6.2, p.366

upvoted 10 times

⊟ **compucastle** Highly Voted 👍 4 years, 2 months ago

D is correct , “Antivirus configuration is always profile-based, regardless of the NGFW mode selection”

upvoted 7 times

⊟ **AOC** Most Recent ⏲ 4 years ago

Correcto D.

upvoted 2 times

⊟ **vwboy** 4 years, 2 months ago

why do you say C

upvoted 1 times

⊟ **SebaAr22** 4 years, 3 months ago

C is correct

upvoted 1 times

Question #29 Topic 1

Which two statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be uploaded manually to each FortiGate.

B. Uninterruptable upgrade is enabled by default.

C. Traffic load balancing is temporarily disabled while the firmware is upgraded.

D. Only secondary FortiGate devices are rebooted.

Suggested Answer: *BC*

Reference:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_operatingFirmUpgd.htm

AOC 4 years ago

Correcto, byc

upvoted 1 times

pollyy 4 years, 2 months ago

B & C are correct - Infrastructure_Manual-6.2, p.327

upvoted 4 times

Question #30 *Topic 1*

Which statement about the firewall policy authentication timeout is true?

A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.

B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.

C. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.

D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Suggested Answer: *A*

pollyy 4 years, 2 months ago

A sound as a correct answer - Secuity_Manual-6-2, p. 243.

B is wrong - no temporary firewall policy is removed

upvoted 4 times

Question #31 *Topic 1*

Which two statements correctly describe how FortiGate performs route lookup, when searching for a suitable gateway? (Choose two.)

A. Lookup is done on the first packet from the session originator

B. Lookup is done on the last packet sent from the responder

C. Lookup is done on every packet, regardless of direction

D. Lookup is done on the first reply packet from the responder

Suggested Answer: *AD*

pollyy Highly Voted 4 years, 2 months ago

A & D are correct - NSE7-Enretprise_FW-6.2, p. 132

upvoted 5 times

herlock_sholmes_2810 Most Recent 3 months, 3 weeks ago

Selected Answer: AD

A. and D.

For each session, FortiGate performs two route lookups:

• For the first packet sent by the originator

• For the first reply packet coming from the responder

upvoted 1 times

NetStef 4 years, 1 month ago

Correct is A,D

FortiGate_Infrastructure 6.2 Study Guide page 10

upvoted 4 times

rcharger00 4 years, 3 months ago

Correct answer A, D

For any session, FortiGate performs a routing table lookup twice:

1) For the first packet sent by the originator

2) For the first reply packet coming from the responder

upvoted 4 times

Question #32 *Topic 1*

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

A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

B. The two VLAN sub interfaces must have different VLAN IDs.

C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.

D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Suggested Answer: *B*

AOC 4 years ago

Correcto la b

upvoted 1 times

pollyy 4 years, 2 months ago

B is correct, D is not correct - no information that FortiG is in multi-VDOM mode

upvoted 3 times

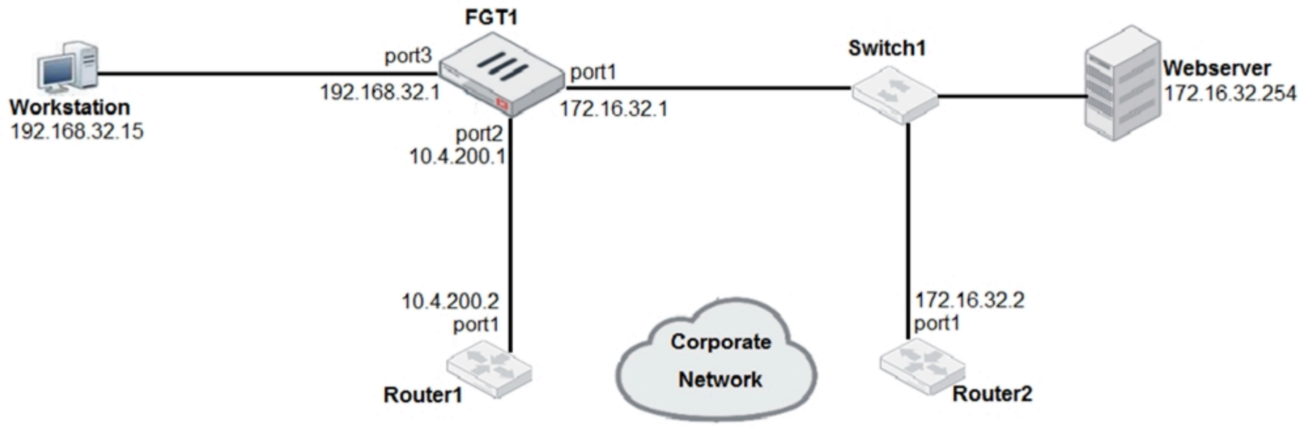
siscoFe 3 years, 10 months ago

B is the answer in the solution or was it D before. I think B is correct too.

upvoted 1 times

Question #33 *Topic 1*

Refer to the exhibit.



Given the network diagram shown in the exhibit, which route is the best candidate route for FGT1 to route traffic from the workstation to the webserver?

A. 172.16.32.0/24 is directly connected, port1

B. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]

C. 10.4.200.0/30 is directly connected, port2

D. 0.0.0.0/0 [20/0] via 10.4.200.2, port2

Suggested Answer: *A*

pollyy Highly Voted 4 years, 2 months ago

A is correct

upvoted 6 times

ali_red Most Recent 3 years, 12 months ago

A for sure

upvoted 1 times

AOC 4 years ago

Correcto, a

upvoted 1 times

Question #34 *Topic 1*

Which two statements about central NAT are true? (Choose two.)

A. SNAT using central NAT does not require a central SNAT policy.

B. Central NAT can be enabled or disabled from the CLI only.

C. IP pool references must be removed from existing firewall policies, before enabling central NAT.

D. DNAT using central NAT requires a VIP object as the destination address in a firewall policy.

Suggested Answer: *BC*

MEDO162 3 years, 11 months ago

B and C are correct.

FortiGate_Security_6.4 P.164

upvoted 1 times

AOC 4 years ago

byc correcto

upvoted 1 times

bwman 4 years, 1 month ago

B is correct -> security guide 6.4 p163
C is correct
D is incorrect : As soon as a VIP or DNAT rule is created, no need for IPV4 policy. It is implicitely allowed. We can block trafic by adding IPV4 policy

upvoted 1 times

NetStef 4 years, 1 month ago

B & C Corect

upvoted 1 times

gordonF 4 years, 2 months ago

B is wrong
If NGFW mode is policy-based, then it is assumed that central-nat (specifically SNAT) is enabled implicitly.

From GUI:
Got to System -> Settings, under 'Inspection Mode' select 'Flow-based and under 'NGFW Mode' select 'Profil-based'.

From CLI.

```
# Config sys setting
set central-nat disable
end
```

https://kb.fortinet.com/kb/documentLink.do?externalID=FD49932

upvoted 1 times

petrus28 4 years, 2 months ago

Security_manual-6.2, p.164

upvoted 1 times

pollyy 4 years, 2 months ago

D is not correct - Security_manual-6.2, p. 167

upvoted 2 times

pollyy 4 years, 2 months ago

B & C are correct - Security_manual-6.2, p.164

upvoted 3 times

Jay1982 4 years, 3 months ago

B is wrong, Central NAT can be enabled from CLI/GUI

upvoted 1 times

Jay1982 4 years, 3 months ago

When central NAT is enabled in CLI, Policy & Objects displays the Central SNAT section in GUI so B is right.

upvoted 2 times

petrus28 4 years, 2 months ago

Security_manual-6.2, p.164

upvoted 1 times

Question #35 *Topic 1*

Which condition must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The private key of the CA certificate that is signed the browser certificate must be installed on the browser.

B. The CA certificate that signed the web server certificate must be installed on the browser.

C. The public key of the web server certificate must be installed on the web browser.

D. The web-server certificate must be installed on the browser.

Suggested Answer: *B*

pollyy Highly Voted 4 years, 2 months ago

B is correct

upvoted 6 times

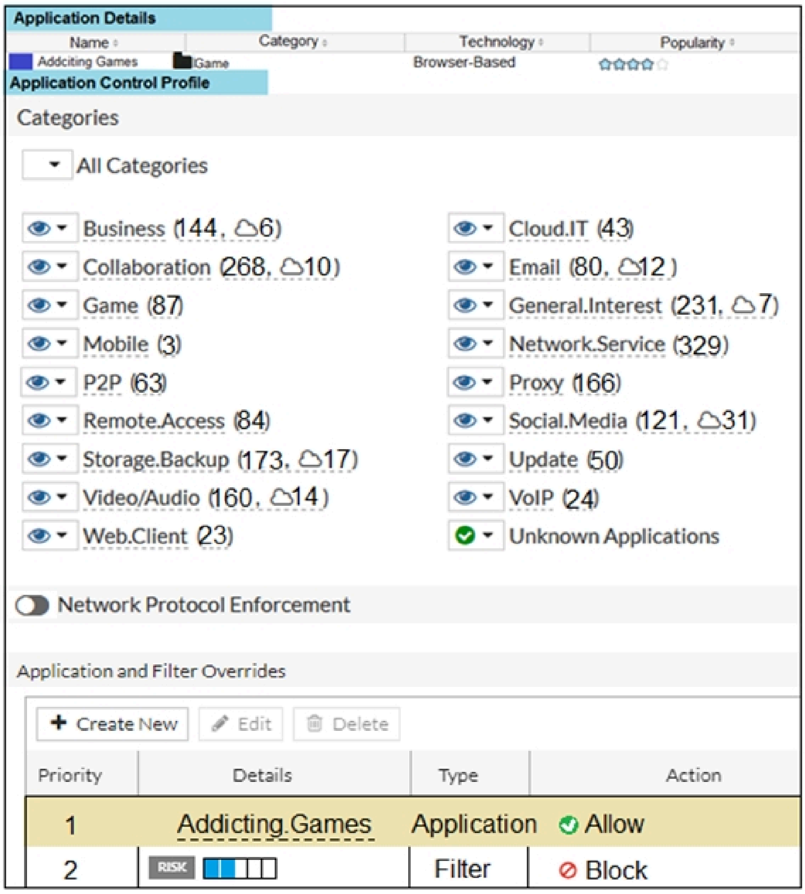
AOC Most Recent 4 years ago

es la b

upvoted 1 times

Question #36 *Topic 1*

Refer to the exhibit.



Application Details

Name	Category	Technology	Popularity
Addciting Games	Game	Browser-Based	★★★★☆

Application Control Profile

Categories

▾ All Categories

👁 ▾ Business (144, ☁6)
👁 ▾ Collaboration (268, ☁10)
👁 ▾ Game (87)
👁 ▾ Mobile (3)
👁 ▾ P2P (63)
👁 ▾ Remote.Access (84)
👁 ▾ Storage.Backup (173, ☁17)
👁 ▾ Video/Audio (160, ☁14)
👁 ▾ Web.Client (23)
👁 ▾ Cloud.IT (43)
👁 ▾ Email (80, ☁12)
👁 ▾ General.Interest (231, ☁7)
👁 ▾ Network.Service (329)
👁 ▾ Proxy (166)
👁 ▾ Social.Media (121, ☁31)
👁 ▾ Update (50)
👁 ▾ VoIP (24)
✓ ▾ Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Addicting.Games	Application	✓ Allow
2	RISK ▮▮□□	Filter	⊘ Block

A user located behind the FortiGate device is trying to go to http://www.addictinggames.com (Addicting.Games). The exhibit shows the application detains and application control profile.

Based on this configuration, which statement is true?

A. Addicting.Games will be blocked, based on the Filter Overrides configuration.

B. Addicting.Games will be allowed only if the Filter Overrides action is set to Learn.

C. Addicting.Games will be allowed, based on the Categories configuration.

D. Addicting.Games will be allowed, based on the Application Overrides configuration.

Suggested Answer: *D*

pollyy Highly Voted 4 years, 2 months ago

D is Correct

upvoted 6 times

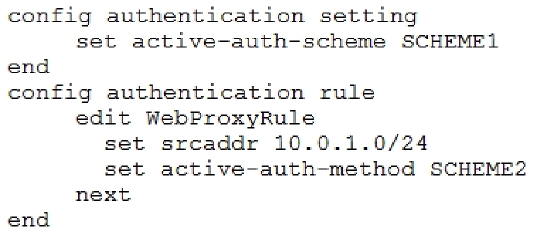
AOC Most Recent 4 years ago

correcto es la d

upvoted 1 times

Question #37 Topic 1

Refer to the exhibit.



```
config authentication setting
      set active-auth-scheme SCHEME1
end
config authentication rule
      edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
      next
end
```

The exhibit shows a FortiGate configuration.

How does FortiGate handle web proxy traffic coming from the IP address 10.2.1.200, that requires authorization?

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic

C. It authenticates the traffic using the authentication scheme SCHEME2.

D. It authenticates the traffic using the authentication scheme SCHEME1.

Suggested Answer: *D*

Community vote distribution

D (100%)

nerdypitt 1 year, 2 months ago

- FGT Security 7.2 p310

- The application control profile scans for matches in this order:

○ Application and filter overrides: If you have configured any applications 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.

○ Categories: Finally, the application control profiles applies the action that you've configured for applications in your selected categories.

upvoted 1 times

Diego_Farani 1 year, 5 months ago

Selected Answer: D

The answer is D.

upvoted 1 times

AOC 4 years ago

d es correcto

upvoted 1 times

pollyy 4 years, 2 months ago

D is correct

upvoted 4 times

Question #38 *Topic 1*

Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not support perfect forward secrecy.

B. AH provides strong data integrity but weak encryption.

C. AH provides data integrity but no encryption.

D. AH does not provide any data integrity or encryption.

Suggested Answer: *C*

AOC 4 years ago

correcto la c

upvoted 1 times

pollyy 4 years, 2 months ago

C - correct

upvoted 4 times

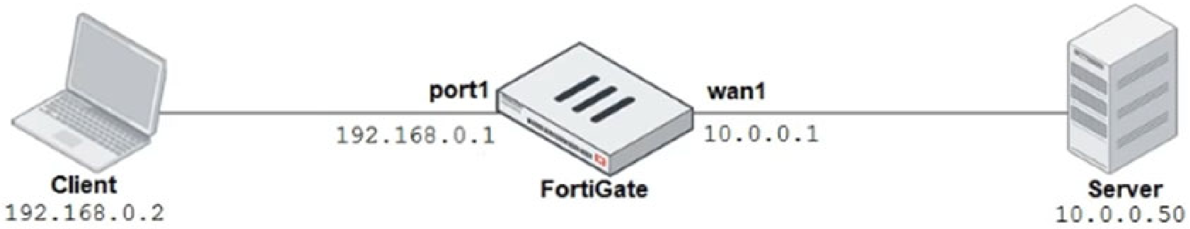
anti1983 4 years, 2 months ago

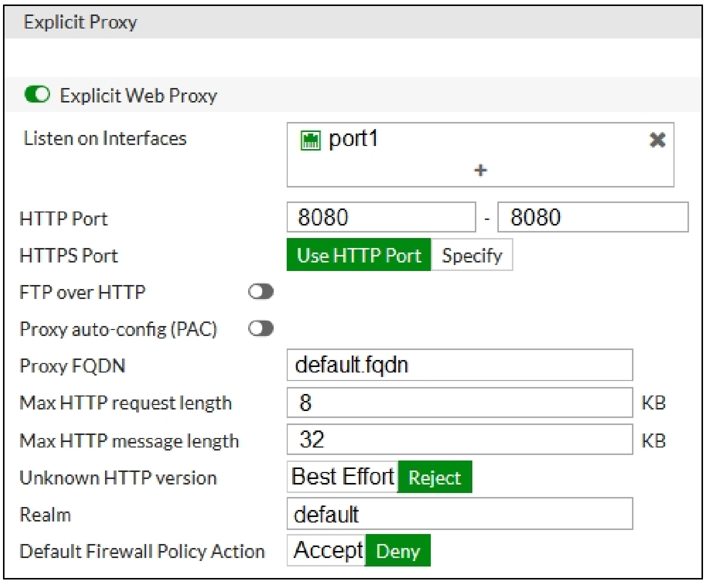
C, Fortigate Security P. 628

upvoted 4 times

Question #39 Topic 1

Refer to the exhibits.





Explicit Proxy

● Explicit Web Proxy

Listen on Interfaces	port1 ✖ +
HTTP Port	8080 - 8080
HTTPS Port	[✓ Use HTTP Port] Specify
FTP over HTTP	○
Proxy auto-config (PAC)	○
Proxy FQDN	default.fqdn
Max HTTP request length	8 KB
Max HTTP message length	32 KB
Unknown HTTP version	Best Effort [✓ Reject]
Realm	default
Default Firewall Policy Action	Accept [✓ Deny]

The exhibits show a network diagram and the explicit web proxy configuration.

In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

A. "˜host 192.168.0.2 and port 8080'

B. "˜host 10.0.0.50 and port 80'

C. "˜host 192.168.0.1 and port 80'

D. "˜host 10.0.0.50 and port 8080'

Suggested Answer: *A*

Community vote distribution

A (100%)

pollyy Highly Voted 4 years, 2 months ago

A is correct

upvoted 6 times

mob9 Most Recent 2 years, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

AOC 4 years ago

Correcto la a

upvoted 1 times

Question #40 Topic 1

How do you format the FortiGate flash disk?

A. Execute the CLI command execute formatlogdisk.

B. Select the format boot device option from the BIOS menu.

C. Load the hardware test (HQIP) image.

D. Load a debug FortiOS image.

Suggested Answer: *B*

Community vote distribution

B (100%)

pollyy Highly Voted 4 years, 2 months ago

B is correct for Flash Memory according to Infrastructure_manual-6.2, p.403

upvoted 7 times

Ibrahimadwan Most Recent 1 year, 11 months ago

Selected Answer: B

B is correct

upvoted 1 times

AOC 4 years ago

b es correcto

upvoted 2 times

anti1983 4 years, 2 months ago

Never heard of "Flash Disk", if it refers to Flash Memory the answer is B.

Fortigate Infrastructure P. 403

upvoted 4 times

scuadro 4 years, 3 months ago

Option B is correct, https://kb.fortinet.com/kb/documentLink.do?externalID=FD46582

upvoted 4 times

SebaAr22 4 years, 3 months ago

A is correct for log flash disk and B is correct for boot flash disk, this cuestion is wrong

upvoted 2 times

SebaAr22 4 years, 3 months ago

mmmmmmmmmmm

upvoted 1 times

Question #41 *Topic 1*

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. The Services field prevents SNAT and DNAT from being combined in the same policy.

B. The Services field is used when you need to bundle several VIPs into VIP groups.

C. The Services field removes the requirement to create multiple VIPs for different services.

D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **einstein85** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

⊟ **AOC** 3 years, 12 months ago

c, security p 164

upvoted 2 times

⊟ **pollyy** 4 years, 2 months ago

C is correct

upvoted 3 times

Question #42 *Topic 1*

Which three types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Server information disclosure attacks

B. Traffic to botnet servers

C. Credit card data leaks

D. Traffic to inappropriate web sites

E. SQL injection attacks

Suggested Answer: *ACE*
Reference:
https://help.fortinet.com/fweb/570/Content/FortiWeb/fortiweb-admin/web_protection.htm

Ping2Jo 4 years ago
A, B, & E are correct
https://www.fortinet.com/products/web-application-firewall/fortiweb#services
upvoted 1 times

> **Ping2Jo** 4 years ago
> Please ignore my comment. According to below reference the correct answer should be A, C, E.
> https://help.fortinet.com/fweb/570/Content/FortiWeb/fortiweb-admin/web_protection.htm
> upvoted 3 times

scuadro 4 years, 2 months ago
it is right. https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/491256/protecting-a-server-running-web-applications
upvoted 4 times

Question #43 *Topic 1*

Why does FortiGate keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To generate logs

B. To remove the NAT operation

C. To finish any inspection operations

D. To allow for out-of-order packets that could arrive after the FICK packets

Suggested Answer: *D*

AOC 3 years, 12 months ago

d, security p182

upvoted 1 times

pollyy 4 years, 2 months ago

D is correct

upvoted 4 times

Question #44 *Topic 1*

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
if (shExpMatch (url, “*.fortinet.com/*”)) {
return “DIRECT”;}
if (isInNet (host, “172.25.120.0”, “255.255.255.0”)) {
return “PROXY altproxy.corp.com: 8060”;) }
return “PROXY proxy.corp.com:8090”;
}
```

Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from FortiGate.

B. Any web request sent to the 172.25.120.0/24 subnet is allowed to bypass the proxy.

C. All requests not sent to fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.

D. Any web request sent to fortinet.com is allowed to bypass the proxy.

Suggested Answer: *AD*

AOC 3 years, 12 months ago

a y d es correcto

upvoted 1 times

brunojlm88 4 years ago

AD is correct. The command direct bypass the proxy and it is a standard for pac files. And browsers can download de pac file from any server/fortigate.

upvoted 2 times

pollyy 4 years, 2 months ago

FGT_Infrastructure-6.2, p.341

upvoted 2 times

pollyy 4 years, 2 months ago

B & C is not correct hence A & D are correct :-)

upvoted 1 times

Question #45

Topic 1

Which two statements correctly describe auto discovery VPN (ADVPN)? (Choose two.)

A. IPSec tunnels are negotiated dynamically between spokes.

B. ADVPN is supported only with IKEv2.

C. It recommends the use of dynamic routing protocols, so that spokes can learn the routes to other spokes.

D. Every spoke requires a static tunnel to be configured to other spokes, so that phase 1 and phase 2 proposals are defined in advance.

Suggested Answer: *AC*

amalmose 3 years, 8 months ago

A and C are correct

Fortigate_ Infrastructure_209

upvoted 1 times

AOC 3 years, 12 months ago

infra p 203, a y c

upvoted 1 times

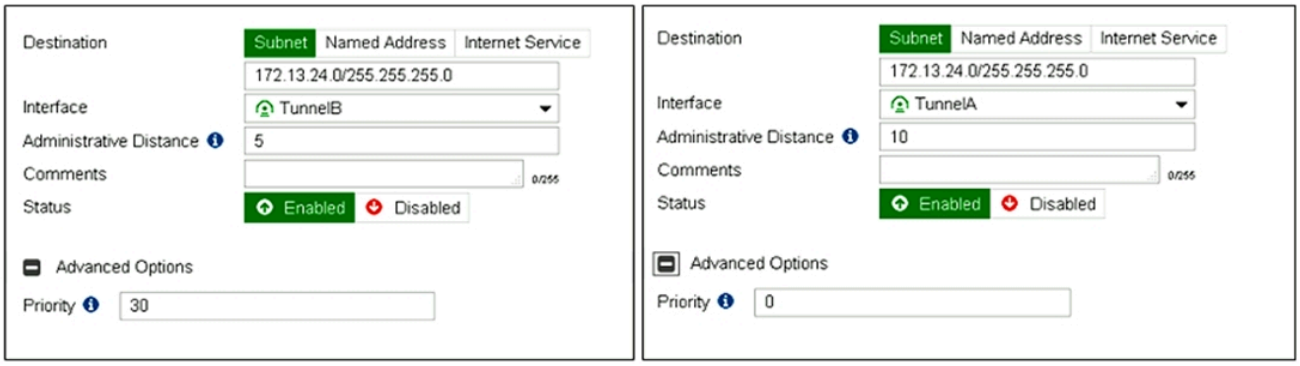
pollyy 4 years, 2 months ago

A & C are correct - Enterprise_FW_Manual-6.2, p. 457-458

upvoted 2 times

Question #46 *Topic 1*

Refer to the exhibit.



Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: TunnelB
Administrative Distance: 5
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 30

Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: TunnelA
Administrative Distance: 10
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 0

Given to the static routes shown in the exhibit, which statements are correct? (Choose two.)

A. This is a redundant IPsec setup.

B. This setup requires at least two firewall policies with the action set to IPsec.

C. Dead peer detection must be disabled to support this type of IPsec setup.

D. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

Suggested Answer: *AD*

pollyy Highly Voted 4 years, 2 months ago

A & D are correct - https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundancy

upvoted 5 times

AOC Most Recent 3 years, 12 months ago

correcto a y d

upvoted 1 times

Question #47 *Topic 1*

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager

B. Root FortiGate

C. FortiAnalyzer

D. Downstream FortiGate

Suggested Answer: *B*

Community vote distribution

C (100%)

rinsable Highly Voted 4 years, 3 months ago

The answer is C. All devices must be authorized on the root Fortigate, and then after this step all must be authorized on the FortiAnalyzer.

upvoted 6 times

jaz600 4 years, 2 months ago

You are right C

upvoted 2 times

herlock_sholmes_2810 Most Recent 2 months, 2 weeks ago

Selected Answer: B

"The third step (AND LAST) in implementing the Security Fabric is to authorize the downstream FortiGate devices on the root FortiGate."

Reference: FortiGate Administrator 7.4 - Study Guide, page 389

When you authorize the downstream devices, you automatically authorize them in FortiAnalyzer.

upvoted 1 times

Kunot 4 months, 2 weeks ago

Selected Answer: B

need to authorize on device first (from GUI) before authorize on fortimanager, so the answer is B

upvoted 2 times

einstein85 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

AOC 3 years, 12 months ago

Correcto es la c

upvoted 2 times

brunojlm88 4 years ago

C is correct. "Final Step" is authorize Fortigate on Fortianalyzer. Authorize downstream Fortigates on Root Fortigate is required too but is the third step not the final one. Study Guide 6.4 chapter Security Fabric look for authorizing devices.

upvoted 4 times

bwman 4 years, 1 month ago

C is correct, fortigate study guide 6.4 p69

upvoted 2 times

pollyy 4 years, 2 months ago

C is correct - Security_Manual-6.2, p.70

upvoted 4 times

Question #48 *Topic 1*

If the Issuer and Subject values are the same in a digital certificate, to which type of entity was the certificate issued?

A. A subordinate CA

B. A root CA

C. A user

D. A CRL

Suggested Answer: *B*

⊟ **ali_red** 3 years, 12 months ago

B for sure

upvoted 1 times

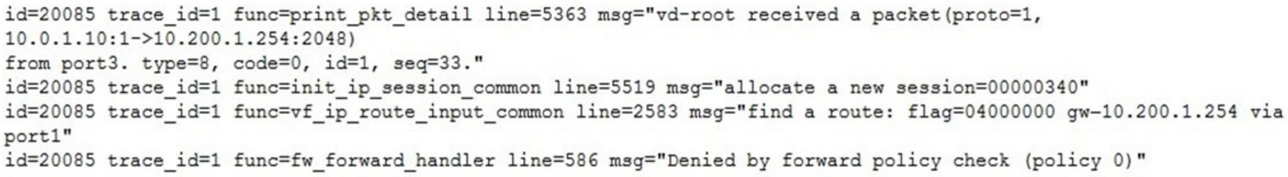
⊟ **pollyy** 4 years, 2 months ago

B is correct

upvoted 4 times

Question #49 *Topic 1*

Examine the output from a debug flow:



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

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.

B. It failed the RPF check.

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

D. It matched the default implicit firewall policy.

Suggested Answer: *D*

AOC 3 years, 12 months ago

correcto la d

upvoted 1 times

pollyy 4 years, 2 months ago

implicit firewall rule == (policy id 0)

upvoted 4 times

pollyy 4 years, 2 months ago

D is correct - traffic is denied by implicit firewall rule

upvoted 3 times

Question #50 *Topic 1*

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes.

B. Denied users are blocked for 30 minutes.

C. A session for denied traffic is created.

D. The number of logs generated by denied traffic is reduced.

Suggested Answer: *CD*

Reference:

https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328

Community vote distribution

CD (50%) BC (50%)

⊟ **Ronaldvb** 2 years, 1 month ago

Selected Answer: CD

Duration 30 is in seconds, not minutes.

upvoted 1 times

⊟ **myname_1** 2 years, 10 months ago

Selected Answer: BC

It's B and C, it's even in the KB pollyy linked....

upvoted 1 times

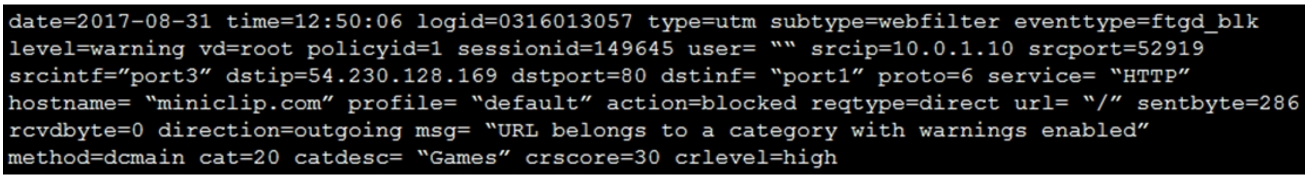
⊟ **pollyy** 4 years, 2 months ago

C & D - correct - https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328

upvoted 4 times

Question #51 *Topic 1*

Refer to the exhibit.



```
date=2017-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk
level=warning vd=root policyid=1 sessionid=149645 user= “” srcip=10.0.1.10 srcport=52919
srcintf=”port3” dstip=54.230.128.169 dstport=80 dstinf= “port1” proto=6 service= “HTTP”
hostname= “miniclip.com” profile= “default” action=blocked reqtype=direct url= “/” sentbyte=286
rcvdbyte=0 direction=outgoing msg= “URL belongs to a category with warnings enabled”
method=dcmain cat=20 catdesc= “Games” crscore=30 crlevel=high
```

The exhibit shows a web filtering log.

Which statement about the log message is true?

A. The web site miniclip.com matches a static URL filter whose action is set to Warning.

B. The usage quota for the IP address 10.0.1.10 has expired.

C. The action for the category Games is set to block.

D. The name of the applied web filter profile is default.

Suggested Answer: *D*

petrus28 4 years, 2 months ago

D. is correct - profile= "default"

upvoted 2 times

Question #52 *Topic 1*

Which two statements about firewall policy NAT using the outgoing interface IP address with fixed port disabled are true? (Choose two.)

A. The source IP is translated to the outgoing interface IP.

B. This is known as many-to-one NAT.

C. Port address translation is not used.

D. Connections are tracked using source port and source MAC address.

Suggested Answer: *AB*

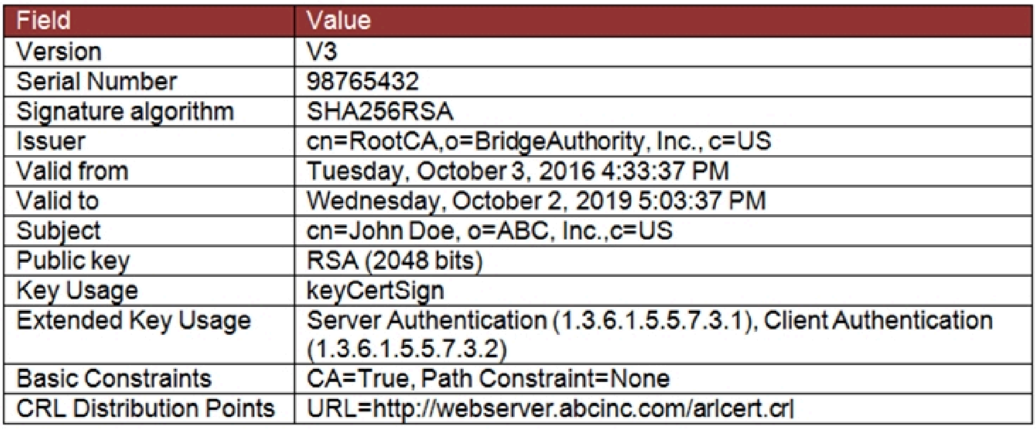
⊟ **pollyy** 4 years, 2 months ago

A & B are correct - Security_Manual-6.2, p.152

upvoted 3 times

Question #53 Topic 1

Refer to the exhibit.



Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc., c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc.,c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

A. A user

B. A root CA

C. A bridge CA

D. A subordinate

Suggested Answer: *A*

Community vote distribution

C (100%)

pollyy Highly Voted 4 years, 2 months ago

A is correct

upvoted 5 times

painkiller Highly Voted 4 years, 1 month ago

cn=Joe Doe

upvoted 5 times

icehot Most Recent 2 years, 2 months ago

Selected Answer: C

I belive that Cross certificates(bridge CA), because Basic constraints saying CA=True. It's not Root CA, because Field Issuer and Subject is different. It's not user certificate, because CA=True. And It's not subordinate, because Issuer and Subject different company.

My answer is C

upvoted 1 times

BeeC 3 years, 11 months ago

Issued to, not issued from. The Subject tells you who it's issued to. In this case, a user. Answer is A: A user.

upvoted 3 times

Cyril_the_Squirl 3 years, 12 months ago

1. Whenever you see the "Ca=True", you should know that the certificate you're looking at belongs to a CA.

2. KeyUsage=keycertsign: What is the intended use of this certificate, answer=keycertsign...in my opinion this is self-explanatory, it is used to sign digital certificates...

This is another reason it's a CA....NOT a person.

B is Correct.

upvoted 2 times

BarCat 3 years, 11 months ago

From my understanding CA:true means it is a CA. Not a root CA but a CA.

Path none means there is no other CA below it so I think it is a clearly a SUBORDINATED one.

upvoted 3 times

Question #54 *Topic 1*

Which two actions are valid for a FortiGuard category-based filter, in a web filter profile, for a firewall policy in proxy-based inspection mode? (Choose two.)

A. Learn

B. Exempt

C. Allow

D. Warning

Suggested Answer: *BC*

Community vote distribution

CD (100%)

variaj8 Highly Voted 4 years, 3 months ago

The correct answers are C&D

upvoted 5 times

einstein85 Most Recent 2 years ago

Selected Answer: CD

https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/675558/fortiguard-filter

upvoted 1 times

bhuiyan 3 years, 12 months ago

C & D is correct

upvoted 1 times

KobeBryant0212 4 years ago

Answers C&D is correct, Allow and Warning

upvoted 1 times

bwman 4 years, 2 months ago

C&D : "the actions available depend on the mode of inspection:

proxy : allow bloc monitor warning and authenticate

upvoted 3 times

anti1983 4 years, 2 months ago

C, D

Fortigate Secutiry P. 378

upvoted 4 times

Jay1982 4 years, 3 months ago

C&D

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/675558/fortiguard-filter

upvoted 3 times

Question #55 *Topic 1*

Which two options are purposes of NAT traversal in IPsec? (Choose two.)

A. To force a new DH exchange with each phase 2 rekey

B. To detect intermediary NAT devices in the tunnel path

C. To encapsulate ESP packets in UDP packets using port 4500

D. To dynamically change phase 1 negotiation mode to aggressive mode

Suggested Answer: *BC*

ali_red 3 years, 12 months ago

BC for sure

upvoted 2 times

pollyy 4 years, 2 months ago

B & C - correct - Security_Manual-6.2, p.641

upvoted 4 times

Question #56 Topic 1

An administrator has configured a route-based IPsec VPN between two FortiGate devices.
Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.

B. This VPN cannot be used as part of a hub-and-spoke topology.

C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

D. The IPsec firewall policies must be placed at the top of the list.

Suggested Answer: *C*

pollyy 4 years, 2 months ago

C is correct - Security-6.2, p.210

upvoted 3 times

Angel123 4 years, 2 months ago

C is correct - Infrastructure-6.2, p.210

upvoted 3 times

Question #57 *Topic 1*

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

A. It limits the scope of application control to scan traffic based on the browser-based technology category only.

B. It limits the scope of application control to scan application traffic based on application category only.

C. It limits the scope of application control to scan application traffic using parent signatures only

D. It limits the scope of application control to scan application traffic on DNS protocol only.

Suggested Answer: *B*

KobeBryant0212 4 years ago

A should be the correct answer

upvoted 1 times

anti1983 4 years, 2 months ago

A Correct

Fortigate Security P.443

upvoted 1 times

compucastle 4 years, 2 months ago

A is correct

https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode

upvoted 3 times

SebaAr22 4 years, 3 months ago

A is correct

upvoted 2 times

variaj8 4 years, 3 months ago

The answer is A

upvoted 3 times

Question #58 *Topic 1*

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address.
For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.1.0/24

B. 192.168.0.0/8

C. 192.168.2.0/24

D. 192.168.3.0/24

Suggested Answer: *C*

⊟ **pollyy** Highly Voted 👍 4 years, 2 months ago

C. 192.168.2.0/24 is correct

upvoted 5 times

⊟ **rhylos** Most Recent 🕘 4 years, 1 month ago

Why Not A? Shouldn't the config on both sides mirror each other? FGT_Security_6.2 pg 643

upvoted 1 times

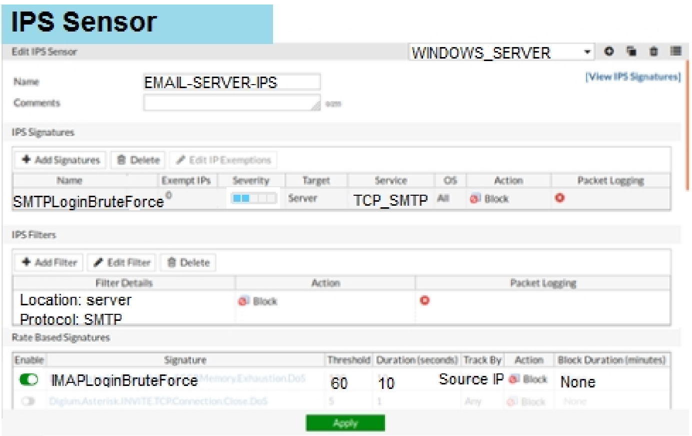
⊟ **brunojlm88** 4 years ago

Local B side is 192.168.2.0/24. 192.168.1.0/24 will be the remote side.

upvoted 2 times

Question #59 *Topic 1*

Refer to the exhibits.



IPS Sensor

Edit IPS Sensor — WINDOWS_SERVER

Name: EMAIL-SERVER-IPS

Comments: 0/255

[View IPS Signatures]

IPS Signatures

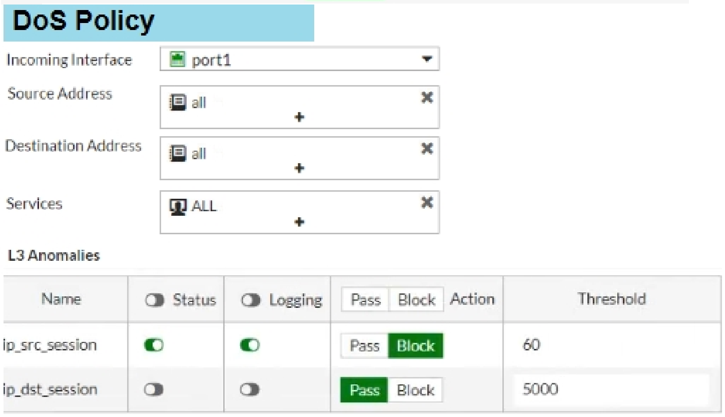
Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce	0		Server	TCP_SMTP	All	Block	●

IPS Filters

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	●

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
●	IMAPLoginBruteForce	60	10	Source IP	Block	None
○	Digium.Asterisk.INVITE.TCPConnection.Close.DoS	5	1	Any	Block	None



DoS Policy

Incoming Interface: port1

Source Address: all

Destination Address: all

Services: ALL

L3 Anomalies

Name	Status	Logging	Pass Block Action	Threshold
ip_src_session	●	●	Block	60
ip_dst_session	○	○	Pass	5000

The exhibits show the IPS sensor and DoS policy configuration.

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. ip_src_session

B. IMAP.Login.Brute.Force

C. Location: server Protocol:SMTP

D. SMTP.Login.Brute.Force

Suggested Answer: *A*

hkhan049 Highly Voted 4 years, 3 months ago

I think A is right, because the DoS Policy will be processed before any other policy.

https://docs.fortinet.com/document/fortigate/6.2.0/parallel-path-processing-life-of-a-packet/86811/packet-flow-ingress-and-egress-fortigates-without-network-processor-offloading

upvoted 13 times

ccsa_ccse Highly Voted 4 years, 1 month ago

The correct answer is A.

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack.

upvoted 6 times

SebaAr22 Most Recent 4 years, 3 months ago

A - ip_src_session is the first

upvoted 3 times

Destaire 4 years, 3 months ago

Right answer is B

upvoted 2 times

Destaire 4 years, 3 months ago

The answer is B

upvoted 1 times