Question #1 *Topic 1*

A company that acquired multiple branches across different countries needs to install new FortiGate devices on each of those branches. However, the IT staff lacks sufficient knowledge to implement the initial configuration on the FortiGate devices.
Which three approaches can the company take to successfully deploy advanced initial configurations on remote branches? (Choose three.)

A. Use metadata variables to dynamically assign values according to each FortiGate device.

B. Use provisioning templates and install configuration settings at the device layer.

C. Use the Global ADOM to deploy global object configurations to each FortiGate device.

D. Apply Jinja in the FortiManager scripts for large-scale and advanced deployments.

E. Add FortiGate devices on FortiManager as model devices, and use ZTP or LTP to connect to FortiGate devices.

Suggested Answer: *ABE*

Community vote distribution

ABE (100%)

themageofsec 1 month, 2 weeks ago

Selected Answer: ABE

A, B, E is correct

upvoted 1 times

Palfriend 1 month, 3 weeks ago

Selected Answer: ABE

anyone did the exam recently, is it stable?

upvoted 3 times

Zamile99 1 month, 1 week ago

co-ask ?

upvoted 1 times

Tweefo 2 months ago

Selected Answer: ABE

A, B, E is correct

upvoted 2 times

greeklover84 2 months, 2 weeks ago

Selected Answer: ABE

A,B, E agree. the Options C,D do not make sense.

upvoted 2 times

Question #2 *Topic 1*

An administrator is checking an enterprise network and sees a suspicious packet with the MAC address e0:23:ff:fc:00:86.
What two conclusions can the administrator draw? (Choose two.)

A. The suspicious packet is related to a cluster that has VDOMs enabled.

B. The network includes FortiGate devices configured with the FGSP protocol.

C. The suspicious packet is related to a cluster with a group-id value lower than 255.

D. The suspicious packet corresponds to port 7 on a FortiGate device.

Suggested Answer: *AD*

Community vote distribution

AD (100%)

firewalk 1 month ago

Selected Answer: AD

anyone did the exam recently, is it stable?

upvoted 1 times

Yaadd 2 months, 2 weeks ago

Selected Answer: AD

Yes, A and D are correct

upvoted 2 times

Yaghu 2 months, 3 weeks ago

Selected Answer: AD

A and D.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: AD

A: The Group ID falls within the 256–511 range, which uses the group prefix e0:23:ff:fc. The last byte of the MAC address is 86 (134 in decimal), composed of 80 (128) for the vcluster_integer and 6 for the port index, which corresponds to port7. This indicates that VDOMs are enabled.

D: Explained above but port index 6 corresponds to port7.

Source: Study Guide, pages 90–93.

upvoted 2 times

79cab4d 3 months ago

Selected Answer: AD

Study guide page 90

upvoted 3 times

Question #3 *Topic 1*

A company's guest internet policy, operating in proxy mode, blocks access to Artificial Intelligence Technology sites using FortiGuard. However, a guest user accessed a page in this category using port 8443.
Which configuration changes are required for FortiGate to analyze HTTPS traffic on nonstandard ports like 8443 when full SSL inspection is active in the guest policy?

A. Add a URL wildcard domain to the website CA certificate and use it in the SSL/SSH Inspection Profile.

B. In the Protocol Port Mapping section of the SSL/SSH Inspection Profile, enter 443, 8443 to analyze both standard (443) and non-standard (8443) HTTPS ports.

C. To analyze nonstandard ports in web filter profiles, use TLSv1.3 in the SSL/SSH Inspection Profile.

D. Administrators can block traffic on nonstandard ports by enabling the SNI check in the SSL/SSH Inspection Profile.

Suggested Answer: *B*

Community vote distribution

B (100%)

firewalk 1 month ago

Selected Answer: B

anyone did the exam recently, is it stable?

upvoted 1 times

themageofsec 1 month, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

greeklover84 2 months, 2 weeks ago

Selected Answer: B

Yes agree only B makes sense, for me at least.

upvoted 1 times

tioeudes 2 months, 2 weeks ago

Selected Answer: B

letter b is the only one that makes sense.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: B

B is correct
“Because the firewall in this example has not enabled protocol port mapping for HTTPS and port 8443, the user will bypass the firewall…”
“Protocol port mapping can be enabled... only if SSL inspection is activated… and the appropriate protocol port-mapping settings are configured.”
Source : Study Guide 166

upvoted 1 times

Yaghu 3 months ago

Selected Answer: B

Answer B appears to be the only answer pertaining to port mapping.

upvoted 1 times

Question #4 *Topic 1*

An administrator needs to install an IPS profile without triggering false positives that can impact applications and cause problems with the user's normal traffic flow.

Which action can the administrator take to prevent false positives on IPS analysis?

A. Use the IPS profile extension to select an operating system, protocol, and application for all the network internal services and users to prevent false positives.

B. Enable Scan Outgoing Connections to avoid clicking suspicious links or attachments that can deliver botnet malware and create false positives.

C. Use an IPS profile with action monitor, however, the administrator must be aware that this can compromise network integrity.

D. Install missing or expired SSL/TLS certificates on the client PC to prevent expected false positives.

Suggested Answer: *C*

Community vote distribution

C (100%)

Zamile99 1 day, 18 hours ago

Anyone ?

upvoted 1 times

firewalk 1 month ago

Selected Answer: C

anyone did the exam recently, is it stable?

upvoted 1 times

tioeudes 2 months, 2 weeks ago

Selected Answer: C

C is correct because the goal is to monitor attacks but avoid false positives. The action described in letter c is the only one that will achieve that.

upvoted 2 times

Tweefo 2 months, 3 weeks ago

Selected Answer: C

C is the correct answer

upvoted 1 times

Yaghu 3 months ago

Selected Answer: C

EFW Admin 7.4 Study Guide, p. 175

upvoted 2 times

79cab4d 3 months ago

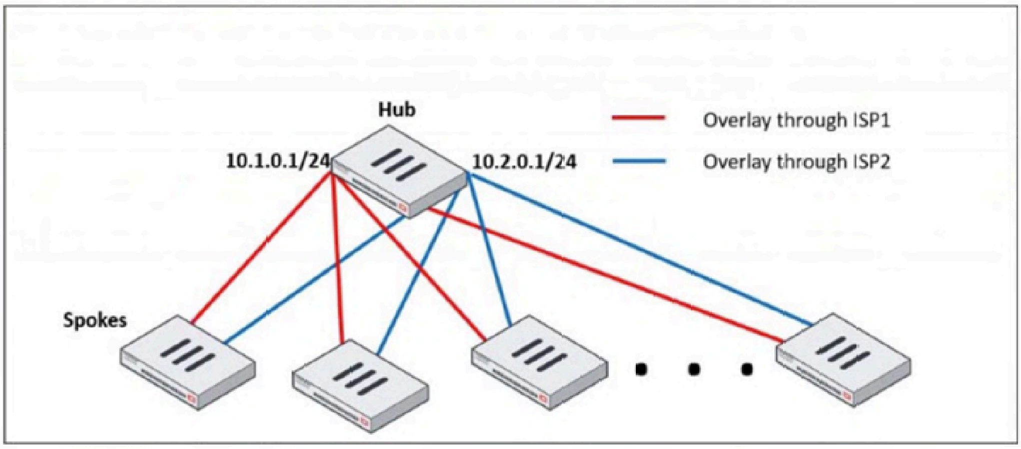
Selected Answer: C

Study guide page 176 (?)

upvoted 1 times

Question #5 Topic 1

Refer to the exhibit, which shows a hub and spokes deployment.



An administrator is deploying several spokes, including the BGP configuration for the spokes to connect to the hub.

Which two commands allow the administrator to minimize the configuration? (Choose two.)

A. neighbor-group

B. route-reflector-client

C. neighbor-range

D. ibgp-enforce-multihop

Suggested Answer: *AC*

Community vote distribution

AC (100%)

Harkell72 2 months, 1 week ago

Selected Answer: AC

A&C Page 229 in the study guide.

upvoted 2 times

tioeudes 2 months, 2 weeks ago

Selected Answer: AC

a and c makes it possible to have one cofiguration for bgp peering with many neighbors within neighbor range and have it all in the same neighbor group.

upvoted 1 times

Yaghu 2 months, 3 weeks ago

Selected Answer: AC

The question makes no mention of Spokes needing to establish connections with each other via ADVPN (route-reflector).

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: AC

A & C are correct.

B : Incorrect in this context, configured on Hub, not Spokes

D : Allow iBGP neighbors to connect over multiple hops, it's a technical connectivity setting, not a configuration simplification tool.

upvoted 3 times

Question #6 Topic 1

Why does the ISDB block layers 3 and 4 of the OSI model when applying content filtering? (Choose two.)

A. FortiGate has a predefined list of all IPs and ports for specific applications downloaded from FortiGuard.

B. The ISDB blocks the IP addresses and ports of an application predefined by FortiGuard.

C. The ISDB works in proxy mode, allowing the analysis of packets in layers 3 and 4 of the OSI model.

D. The ISDB limits access by URL and domain.

Suggested Answer: *AB*

Community vote distribution

AB (100%)

tioeudes 2 months, 2 weeks ago

Selected Answer: AB

By elimination A and B are correct, because ISDB is not related to proxy mode or works with urls.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: AB

A & B are correct.

A : ISDB is updated via FortiGuard and contains a database of IPs (3) and ports (4) for specific apps + It operates without inspecting traffic

B : The ISDB blocks the IP addresses and ports of an application predefined by Fortiguard

C : Incorrect -> ISB does not use proxy mode and does not inspect traffic, it's not a deep inspection tool

D : That's the role of the Web Filter feature

Source : Study Guide 168-170

upvoted 3 times

Yaghu 3 months ago

Selected Answer: AB

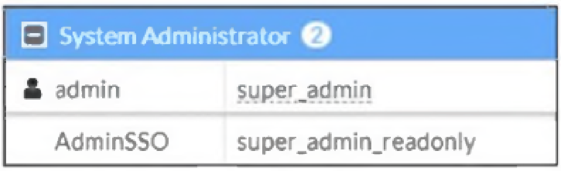
ISDB is download from FortGuard and works without inspecting traffic. EFW Admin 7.4 Study Guide, p. 169-170

upvoted 2 times

Question #7 *Topic 1*

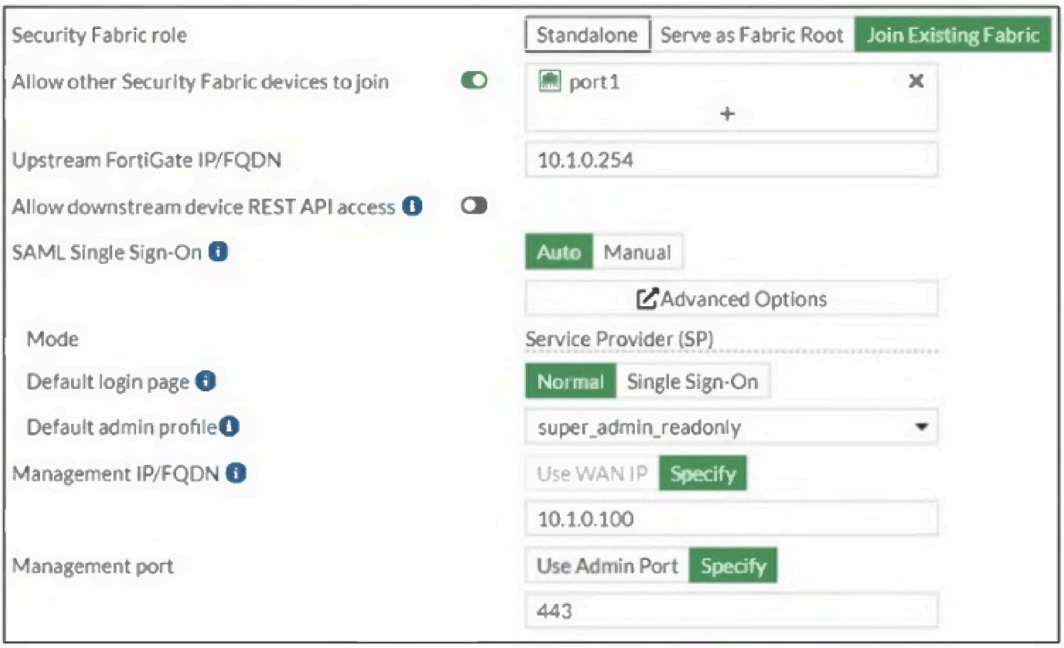
Refer to the exhibits.

Root FortiGate - System Administrator configuration



System Administrator 2	
admin	super_admin
AdminSSO	super_admin_readonly

Downstream FortiGate - Security Fabric settings



Security Fabric role: Standalone | Serve as Fabric Root | **Join Existing Fabric**

Allow other Security Fabric devices to join: ● port1 ✕ +

Upstream FortiGate IP/FQDN: 10.1.0.254

Allow downstream device REST API access ○

SAML Single Sign-On: **Auto** | Manual

Advanced Options

Mode: Service Provider (SP)

Default login page: **Normal** | Single Sign-On

Default admin profile: super_admin_readonly

Management IP/FQDN: Use WAN IP | **Specify**

10.1.0.100

Management port: Use Admin Port | **Specify**

443

The Administrators section of a root FortiGate device and the Security Fabric Settings section of a downstream FortiGate device are shown.

When prompted to sign in with Security Fabric in the downstream FortiGate device, a user enters the AdminSSO credentials.

What is the next status for the user?

A. The user is prompted to create an SSO administrator account for AdminSSO.

B. The user receives an authentication failure message.

C. The user accesses the downstream FortiGate with super_admin_readonly privileges.

D. The user accesses the downstream FortiGate with super_admin privileges.

Suggested Answer: *C*

Community vote distribution

C (100%)

tioeudes 2 months, 2 weeks ago

Selected Answer: C

Super admin readonly is both the default profile on the downstream fgt and the profile fo AdminSSO on the root. So Letter C is correct.

upvoted 2 times

Tweefo 2 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

Question #8 *Topic 1*

A user reports that their computer was infected with malware after accessing a secured HTTPS website. However, when the administrator checks the FortiGate logs, they do not see that the website was detected as insecure despite having an SSL certificate and correct profiles applied on the policy.

How can an administrator ensure that FortiGate can analyze encrypted HTTPS traffic on a website?

A. The administrator must enable reputable websites to allow only SSL/TLS websites rated by FortiGuard web filter.

B. The administrator must enable URL extraction from SNI on the SSL certificate inspection to ensure the TLS three-way handshake is correctly analyzed by FortiGate.

C. The administrator must enable DNS over TLS to protect against fake Server Name Indication (SNI) that cannot be analyzed in common DNS requests on HTTPS websites.

D. The administrator must enable full SSL inspection in the SSL/SSH Inspection Profile to decrypt packets and ensure they are analyzed as expected.

Suggested Answer: *D*

Community vote distribution

D (100%)

greeklover84 2 months, 2 weeks ago

Selected Answer: D

D. Fully Agree.

upvoted 1 times

tioeudes 2 months, 2 weeks ago

Selected Answer: D

Everything @Tweefo said!

upvoted 1 times

Yaghu 2 months, 3 weeks ago

Selected Answer: D

Enabling deep inspection (full SSL) within a policy allows the FG to decrypt all packets traveling through a policy. D is the answer.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: D

D is Correct.

A : Reputable websites setting doesn't decrypt or inspect encrypted payloads

B : SNI parsing is part of certificate inspection but does not decrypt traffic, limited to handshake and domain name info

C : Not relevant to analyzing HTTPS content or SNI-based issue

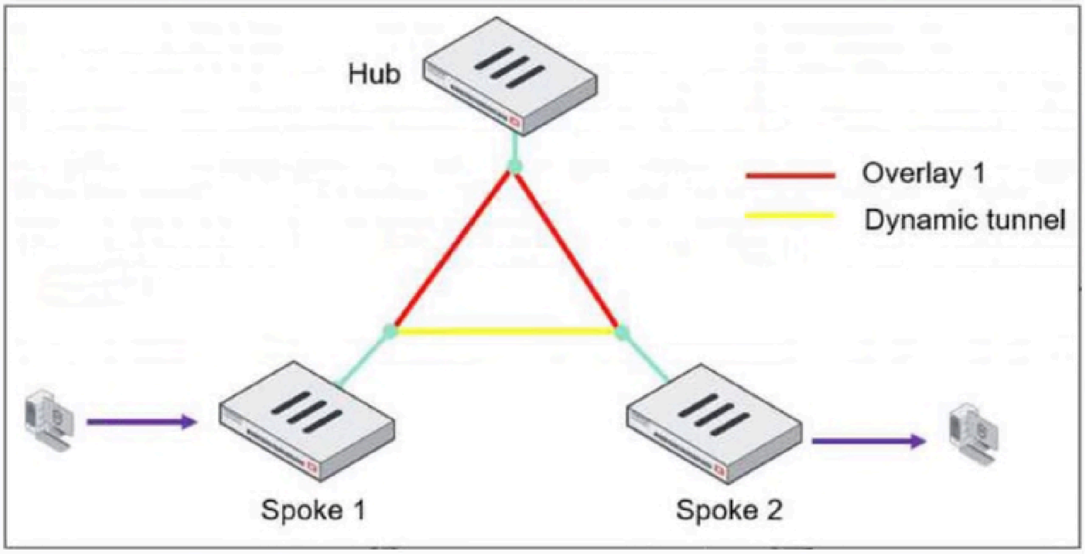
To detect malware or malicious activity inside encrypted HTTPS traffic, full SSL inspection is required

Source : Study guide P163

upvoted 2 times

Question #9 Topic 1

Refer to the exhibit, which shows an ADVPN network.



The client behind Spoke-1 generates traffic to the device located behind Spoke-2.
What is the first message that the hub sends to Spoke-1 to bring up the dynamic tunnel?

A. Shortcut query

B. Shortcut offer

C. Shortcut reply

D. Shortcut forward

Suggested Answer: *B*

Community vote distribution

B (92%) 8%

tioeudes Highly Voted 2 months, 2 weeks ago

Selected Answer: B

Offer (hub to spoke1)
Query (spoke 1 to hub)
Forward (hub to spoke 2)
Reply (spoke 2 to hub)
Forward (hub to spoke1)
Negotiation (spoke1 to spoke2)

upvoted 6 times

themageofsec Most Recent 1 month, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

Poskgraff 2 months, 1 week ago

Selected Answer: B

1 Offer
2 Query
3 Forward
4 Reply
5 Forward
6 Negotiation

upvoted 1 times

greeklover84 2 months, 2 weeks ago

Selected Answer: A

Agree A.

upvoted 1 times

⊟ **Tweefo** 2 months, 1 week ago

Wrong, B is correct.

"What is the first message that the hub sends to Spoke-1 to bring up the dynamic tunnel?"

A is the response from Spoke-1 to Hub, the first message sent by the Hub is the "shortcut offer".

upvoted 1 times

⊟ **Tweefo** 2 months, 3 weeks ago

Selected Answer: B

B is correct, look at the study guide to understand the shorcut message exchange

Source : Study guide 224

upvoted 2 times

⊟ **Yaghu** 3 months ago

Selected Answer: B

FortiOS 7.4.5 Admin Guide, p. 2259

upvoted 2 times

Question #10 *Topic 1*

What is the initial step performed by FortiGate when handling the first packets of a session?

A. Installation of the session key in the network processor (NP)

B. Data encryption and decryption

C. Security inspections such as ACL, HPE, and IP integrity header checking

D. Offloading the packets directly to the content processor (CP)

Suggested Answer: *C*

Community vote distribution

C (100%)

tioeudes 2 months, 2 weeks ago

Selected Answer: C

What Tweefo said...

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: C

C is correct, Fortigate first perfoms some security inspections such as ACL, HPE and IP integrity header ...

Source : Study Guide 287

upvoted 4 times

Yaghu 3 months ago

Selected Answer: C

EFW Admin 7.4 Study Guide, p. 18

upvoted 3 times

Question #11 *Topic 1*

An administrator applied a block-all IPS profile for client and server targets to secure the server, but the database team reported the application stopped working immediately after.

How can an administrator apply IPS in a way that ensures it does not disrupt existing applications in the network?

A. Use an IPS profile with all signatures in monitor mode and verify patterns before blocking.

B. Limit the IPS profile to server targets only to avoid blocking connections from the server to clients.

C. Select flow mode in the IPS profile to accurately analyze application patterns.

D. Set the IPS profile signature action to default to discard all possible false positives.

Suggested Answer: *A*

Community vote distribution

A (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: A

This is a good practice when deploying IPS for the first time.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: A

A is correct.

When applying IPS for the first time, especially with a block-all profiles, there's a high risk of false positives, which can block legitimate trafic.

Source : Study Guide Page 175

upvoted 4 times

Question #12 *Topic 1*

An administrator is extensively using VXLAN on FortiGate.
Which specialized acceleration hardware does FortiGate need to improve its performance?

A. NP7

B. SP5

C. CP9

D. NTurbo

Suggested Answer: *A*

Community vote distribution

A (100%)

tioeudes 2 months, 2 weeks ago

Selected Answer: A

wha they said

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: A

A is correct.
DVLAN and VXLAN offloading is only available with NP7
Source : Study guide P296

upvoted 3 times

Yaghu 3 months ago

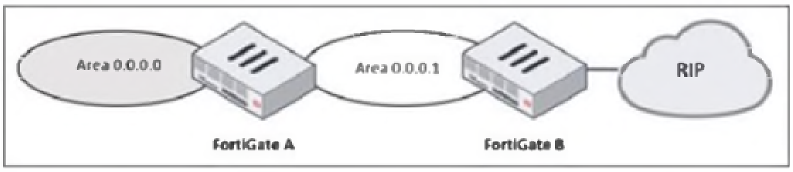
Selected Answer: A

EFW Admin Study Guide, p. 296

upvoted 2 times

Question #13 *Topic 1*

Refer to the exhibit, which shows a partial enterprise network.



An administrator would like the area 0.0.0.0 to detect the external network.

What must the administrator configure?

A. Enable RIP redistribution on FortiGate B.

B. Configure a distribute-route-map-in on FortiGate B.

C. Configure a virtual link between FortiGate A and B.

D. Set the area 0.0.0.l type to stub on FortiGate A and B.

Suggested Answer: *C*

Community vote distribution

C (100%)

datomb74 1 month, 1 week ago

Selected Answer: C

C in this case is the answer

But it does not really make sense to do it this way

upvoted 1 times

AllenSha1 1 month, 2 weeks ago

Selected Answer: C

Page 132

upvoted 1 times

Poskgraff 2 months, 1 week ago

Selected Answer: C

Cuando configura un enlace virtual en ambos enrutadores, permite que un área remota se conecte virtualmente al área de la red troncal.

Página:132

upvoted 3 times

Yaghu 2 months, 3 weeks ago

Selected Answer: C

C is the answer.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: C

C is correct

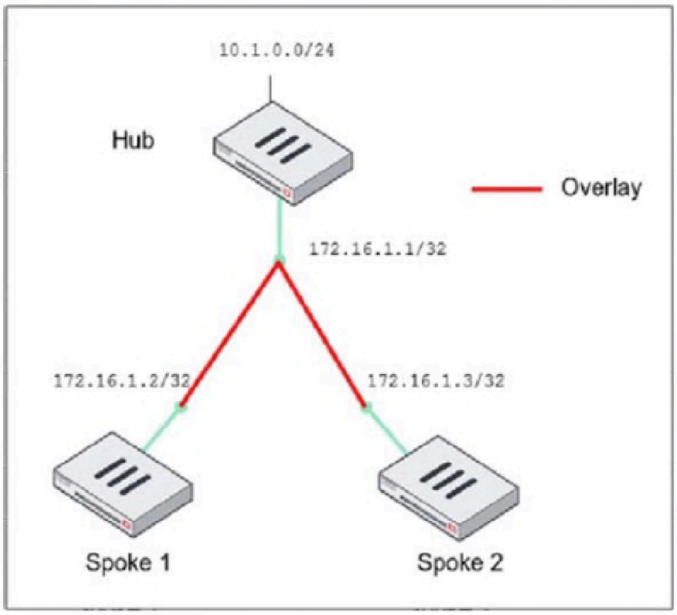
In the case an NSSA area, you can integrate it into OSPF network with a virtual link. When you configure a virtual link on both routers, you allow a remote area to virtually connect directly to the backbone area

upvoted 3 times

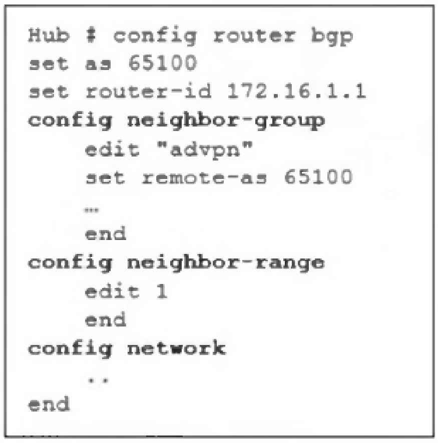
Question #14 *Topic 1*

Refer to the exhibit, which shows the ADVPN network topology and partial BGP configuration.

ADVPN network topology



Partial BGP configuration



```
Hub # config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
    edit "advpn"
    set remote-as 65100
    ...
    end
config neighbor-range
    edit 1
    end
config network
    ..
end
```

Which two parameters must an administrator configure in the config neighbor range for spokes shown in the exhibit? (Choose two.)

A. set max-neighbor-num 2

B. set neighbor-group advpn

C. set route-reflector-client enable

D. set prefix 172.16.1.0 255.255.255.0

Suggested Answer: *BD*

Community vote distribution

BD (100%)

joeytrib 1 month ago

Selected Answer: BD

B & D is correct

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: BD

B & D is correct

upvoted 1 times

Question #15 Topic 1

Which two statements about IKEv2 are true if an administrator decides to implement IKEv2 in the VPN topology? (Choose two.)

A. It includes stronger Diffie-Hellman (DH) groups, such as Elliptic Curve (ECP) groups.

B. It supports interoperability with devices using IKEv1.

C. It exchanges a minimum of two messages to establish a secure tunnel.

D. It supports the extensible authentication protocol (EAP).

Suggested Answer: *AD*

Community vote distribution

AD (100%)

⊟ **joeytrib** 1 month ago

Selected Answer: AD

A and D are correct

upvoted 1 times

⊟ **datomb74** 1 month, 1 week ago

Selected Answer: AD

A and D are correct

upvoted 1 times

⊟ **Harkell72** 2 months, 1 week ago

Selected Answer: AD

Page 193&194

upvoted 2 times

Question #16 *Topic 1*

An administrator must enable direct communication between multiple spokes in a company's network. Each spoke has more than one internet connection.

The requirement is for the spokes to connect directly without passing through the hub, and for the links to automatically switch to the best available connection.

How can this automatic detection and optimal link utilization between spokes be achieved?

A. Set up OSPF routing over static VPN tunnels between spokes.

B. Utilize ADVPN 2.0 to facilitate dynamic direct tunnels and automatic link optimization.

C. Establish static VPN tunnels between spokes with predefined backup routes.

D. Implement SD-WAN policies at the hub to manage spoke link quality.

Suggested Answer: *B*

Community vote distribution

B (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: B

ADVPN 2.0 provides these requirements. B is the answer.

upvoted 3 times

Tweefo 2 months, 3 weeks ago

Selected Answer: B

B is correct, ADVPN 2.0 enable direct spoke-to-spoke communication

Source : Study Guide P246

upvoted 4 times

Question #17 *Topic 1*

What does the command set forward-domain <domain_ID> in a transparent VDOM interface do?

A. It configures the interface to prioritize traffic based on the domain ID, enhancing quality of service for specified VLANs.

B. It isolates traffic within a specific VLAN by assigning a broadcast domain to an interface based on the VLAN ID.

C. It restricts the interface to managing traffic only from the specified VLAN, effectively segregating network traffic.

D. It assigns a unique domain ID to the interface, allowing it to operate across multiple VLANs within the same VDOM.

Suggested Answer: *B*

Community vote distribution

B (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: B

Particular verbage here, but B is the answer.

upvoted 2 times

Tweefo 2 months, 3 weeks ago

Selected Answer: B

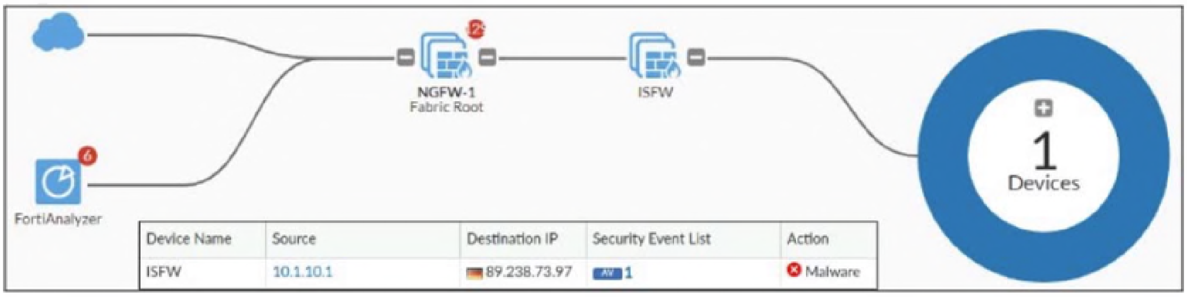
B is correct.

Source : Study Guide P76

upvoted 4 times

Question #18 *Topic 1*

Refer to the exhibit, which shows a physical topology and a traffic log.



Device Name	Source	Destination IP	Security Event List	Action
ISFW	10.1.10.1	89.238.73.97	AV 1	Malware

The administrator is checking on FortiAnalyzer traffic from the device with IP address 10.1.10.1, located behind the FortiGate ISFW device.

The firewall policy in on the ISFW device does not have UTM enabled and the administrator is surprised to see a log with the action Malware, as shown in the exhibit.

What are the two reasons FortiAnalyzer would display this log? (Choose two.)

A. Security rating is enabled in ISFW.

B. ISFW is in a Security Fabric environment.

C. ISFW is not connected to FortiAnalyzer and must go through NGFW-1.

D. The firewall policy in NGFW-1 has UTM enabled.

Suggested Answer: *BD*

Community vote distribution

BD (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: BD

Seems obvious.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: BD

B & D are correct.

B : The Security Fabric, as a whole, logs each session once. The first FortiGate that handles a session in the Security Fabric logs the session. Any upstream FortiGate... still logs UTM events, if configured.

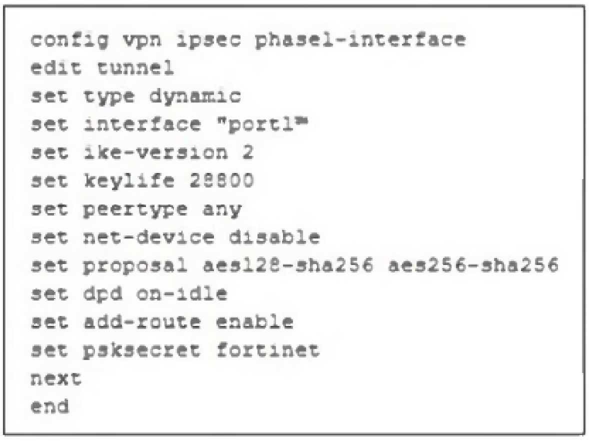
D : NGFW applies UTM and generates UTM logs

Source : Study Guide P257-259

upvoted 1 times

Question #19 Topic 1

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



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

What can you conclude from this VPN IPsec phase 1 configuration?

A. This configuration is the best for networks with regular traffic intervals, providing a balance between connectivity assurance and resource utilization.

B. Peer IDs are unencrypted and exposed, creating a security risk.

C. FortiGate will not add a route to its routing or forwarding information base when the dynamic tunnel is negotiated.

D. A separate interface is created for each dial-up tunnel, which can be slower and more resource intensive, especially in large networks.

Suggested Answer: *A*

Community vote distribution

A (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: A

The answer is A.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: A

A is correct

On-Idle mode is best for networks with regular traffic intervals, providing a balance between connectivity assurance and ressource utilization.

Source : Study Guide P195

upvoted 2 times

Question #20 *Topic 1*

A company's users on an IPsec VPN between FortiGate A and B have experienced intermittent issues since implementing VXLAN. The administrator suspects that packets exceeding the 1500-byte default MTU are causing the problems.
In which situation would adjusting the interface's maximum MTU value help resolve issues caused by protocols that add extra headers to IP packets?

A. Adjust the MTU on interfaces only if FortiGate has the FortiGuard enterprise bundle, which allows MTU modification.

B. Adjust the MTU on interfaces in all FortiGate devices that support the latest family of Fortinet SPUs: NP7, CP9 and SP5.

C. Adjust the MTU on interfaces in controlled environments where all devices along the path allow MTU interface changes.

D. Adjust the MTU on interfaces only in wired connections like PPPoE, optic fiber, and ethernet cable.

Suggested Answer: *C*

Community vote distribution

C (100%)

themageofsec 1 month, 2 weeks ago

Selected Answer: C

C is correct.
And adding Tweefo comment, Study Guide P.59.

upvoted 1 times

Yaghu 2 months, 3 weeks ago

Selected Answer: C

Knowing the network devices and how their MTU values are set allows the engineer to make the appropriate decision when adjusting those values. C is the answer.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

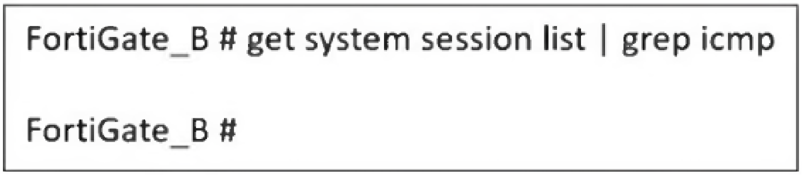
Selected Answer: C

I'd go for C.
VXLAN adds approximately 50 bytes of overhead due to encapsulation with new Ethernet, IP, UDP, and VXLAN headers. This can cause packets to exceed the standard 1500-byte MTU, leading to fragmentation or drops if not adjusted.
Source : Study Guide ~P206

upvoted 4 times

Question #21 Topic 1

Refer to the exhibit, which shows a command output.



```
FortiGate_B # get system session list | grep icmp

FortiGate_B #
```

FortiGate_A and FortiGate_B are members of an FGSP cluster in an enterprise network.

While testing the cluster using the ping command, the administrator monitors packet loss and found that the session output on FortiGate_B is as shown in the exhibit.

What could be the cause of this output on FortiGate_B?

A. The session synchronization is encrypted.

B. session-pickup-connectionless is set to disable on FortiGate_B.

C. FortiGate_B is configured in passive mode.

D. FortiGate_A and FortiGate_B have the same standalone-group-id value.

Suggested Answer: *B*

Community vote distribution

B (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: B

FGSP does not synchronize ICMP sessions by default. It must be enabled.

Study Guide p 106

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: B

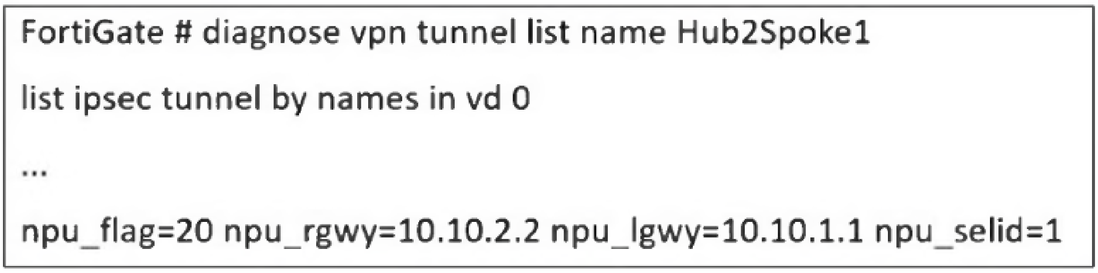
B is correct

Source : Study Guide P106

upvoted 1 times

Question #22 Topic 1

Refer to the exhibit, which shows a partial troubleshooting command output.



```
FortiGate # diagnose vpn tunnel list name Hub2Spoke1

list ipsec tunnel by names in vd 0

...

npu_flag=20 npu_rgwy=10.10.2.2 npu_lgwy=10.10.1.1 npu_selid=1
```

An administrator is extensively using IPsec on FortiGate. Many tunnels show information similar to the output shown in the exhibit.

What can the administrator conclude?

A. IPsec SAs cannot be offloaded.

B. The two IPsec SAs, inbound and outbound, are copied to the NPU.

C. Only the outbound IPsec SA is copied to the NPU.

D. Only the inbound IPsec SA is copied to the NPU.

Suggested Answer: *A*

Community vote distribution

A (100%)

Maria21 5 days, 21 hours ago

Selected Answer: A

00 = Both IPsec SAs loaded to the kernel

01 = Outbound IPsec SA copied to NPU

02 = Inbound IPsec SA copied to NPU

03 = Both outbound and inbound IPsec SA copied to NPU

20 = Unsupported cipher or HMAC, IPsec SA cannot be offloaded

upvoted 1 times

Yaghu 2 months, 3 weeks ago

Selected Answer: A

A is the answer.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: A

A is correct.

npu_flag=20 -> Unsupported cipher or HMAC, IPSec SA cannot be offloaded

Source : Study Guide P298

upvoted 2 times

Poskgraff 3 months ago

Selected Answer: A

El valor 20 en el campo npu_flag indica que la descarga de hardware no está disponible debido a un cifrado no compatible o un algoritmo HMAC.

upvoted 1 times

79cab4d 3 months ago

Selected Answer: A

Correct answer A.

npu_flag=20 means unsupported cipher or HMAC. IPsec SA cannot be offloaded.

Source: Network_Security_Support_Engineer_7.4_Study_Guide, p. 328

upvoted 1 times

Adonisthewise22 3 months ago

Selected Answer: A

npu_flag=03 Means that both ingress & egress ESP packets will be offloaded. npu_flag=20 Unsupported cipher or HMAC, IPsec SA cannot be offloaded.

upvoted 1 times

Adonisthewise22 3 months ago

npu_flag=03 Means that both ingress & egress ESP packets will be offloaded. npu_flag=20 Unsupported cipher or HMAC, IPsec SA cannot be offloaded.

upvoted 1 times

djekson 3 months ago

Selected Answer: A

npu_flag=20 means unsupported cipher or HMAC. IPsec SA cannot be offloaded. If both inbound and outbound IPsec SAs would be offloaded to NPU the flag would be npc_flag=03

upvoted 3 times

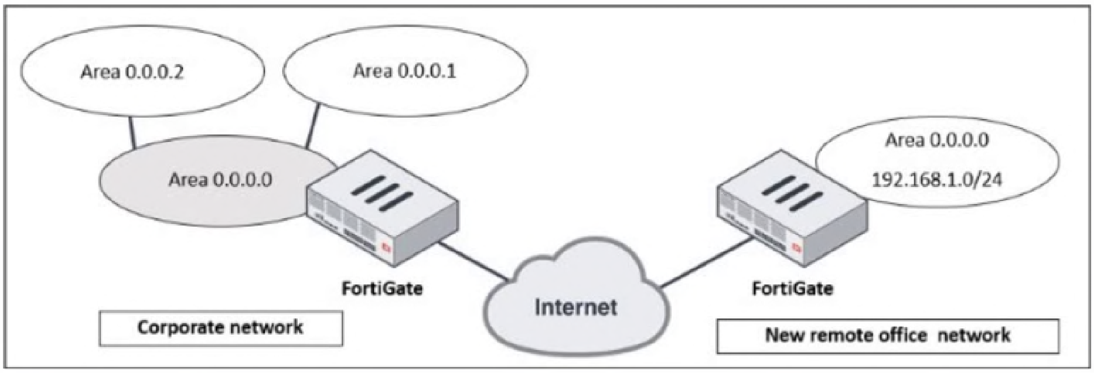
Adonisthewise22 3 months ago

npu_flag=03 Means that both ingress & egress ESP packets will be offloaded. npu_flag=20 Unsupported cipher or HMAC, IPsec SA cannot be offloaded.

upvoted 1 times

Question #23 *Topic 1*

Refer to the exhibit, which shows a corporate network and a new remote office network.



An administrator must integrate the new remote office network with the corporate enterprise network.

What must the administrator do to allow routing between the two networks?

A. The administrator must implement BGP to inject the new remote office network into the corporate FortiGate device.

B. The administrator must configure a static route to the subnet 192.168.l.0/24 on the corporate FortiGate device.

C. The administrator must configure virtual links on both FortiGate devices.

D. The administrator must implement OSPF over IPsec on both FortiGate devices.

Suggested Answer: *D*

Community vote distribution

D (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: D

D is the answer.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: D

I'd go for D, based on Study guide P131.

A : BGP is not used here

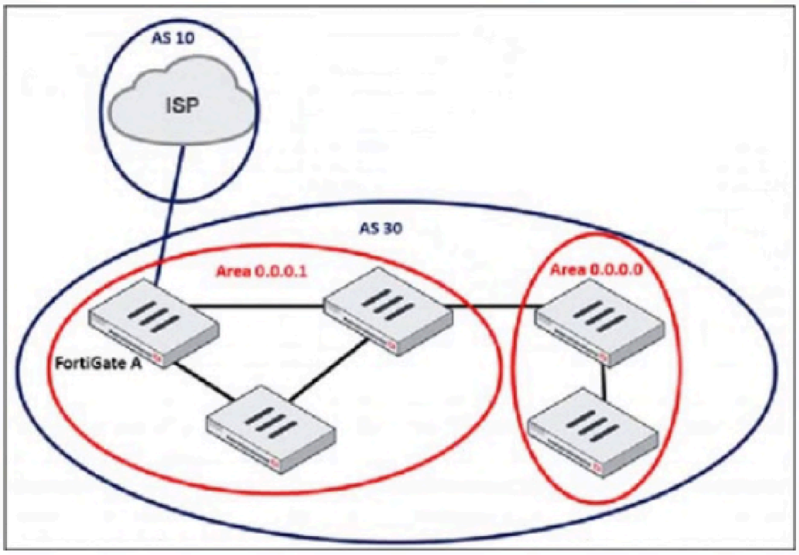
B : Could work, but not relevant in this case

C : Only used when a OSPF zone non-backbone needs to be logically connected to Area 0, not relevant in this case

upvoted 2 times

Question #24 Topic 1

Refer to the exhibit, which shows an enterprise network connected to an internet service provider.



The administrator must configure the BGP section of FortiGate A to give internet access to the enterprise network.

Which command must the administrator use to establish a connection with the internet service provider?

A. config neighbor

B. config redistribute bgp

C. config router route-map

D. config redistribute ospf

Suggested Answer: *A*

Community vote distribution

A (75%) D (25%)

sdmejia01 3 weeks, 1 day ago

Selected Answer: A

The question says which command MUST be used to establish a BGP connection with the ISP. The only correct answer in that case would be 'config neighbor'.

upvoted 1 times

40Man 1 month ago

Selected Answer: D

pg 136 of the study guide

upvoted 1 times

Yaghu 2 months, 3 weeks ago

Selected Answer: A

Config Neighbor

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: A

I'd go for A.

B : Allow to redistribute BGP routes

C : Filter or modify route

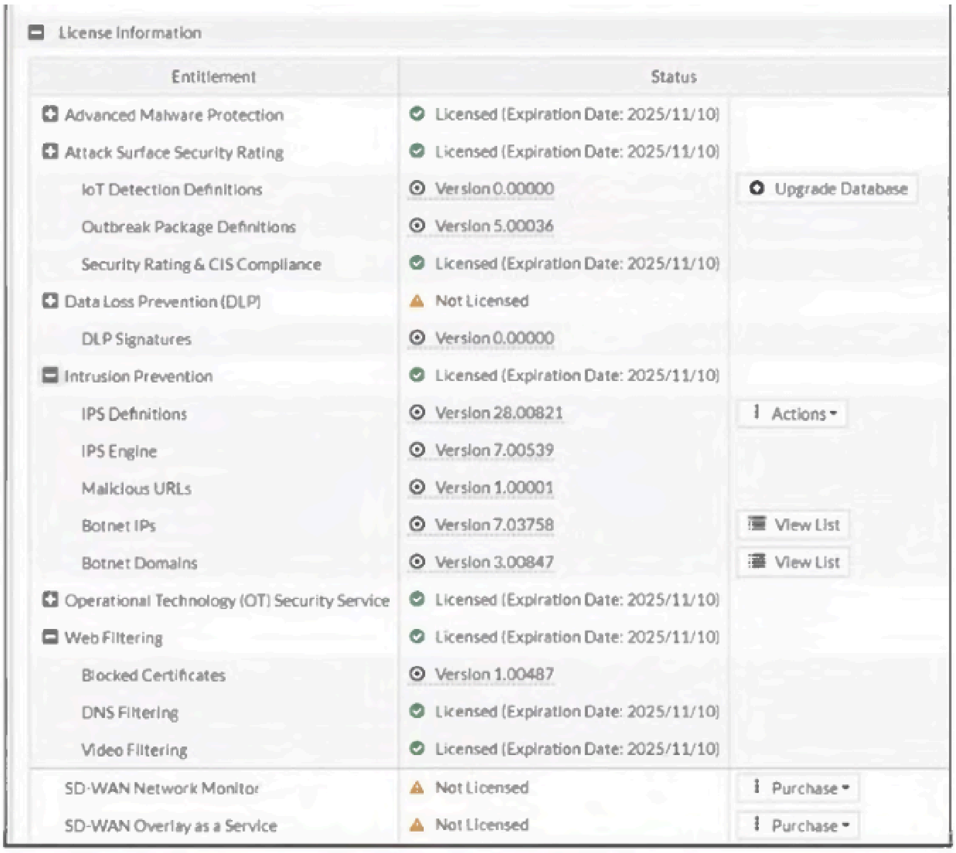
D : Redistribute OPSF routes

upvoted 1 times

Question #25 Topic 1

Refer to the exhibit, which shows the FortiGuard Distribution Network of a FortiGate device.

FortiGuard Distribution Network on FortiGate



⊟ License Information

Entitlement	Status	
⊞ Advanced Malware Protection	✓ Licensed (Expiration Date: 2025/11/10)	
⊞ Attack Surface Security Rating	✓ Licensed (Expiration Date: 2025/11/10)	
IoT Detection Definitions	⊙ Version 0.00000	Upgrade Database
Outbreak Package Definitions	⊙ Version 5.00036	
Security Rating & CIS Compliance	✓ Licensed (Expiration Date: 2025/11/10)	
⊞ Data Loss Prevention (DLP)	⚠ Not Licensed	
DLP Signatures	⊙ Version 0.00000	
⊟ Intrusion Prevention	✓ Licensed (Expiration Date: 2025/11/10)	
IPS Definitions	⊙ Version 28.00821	Actions ▾
IPS Engine	⊙ Version 7.00539	
Malicious URLs	⊙ Version 1.00001	
Botnet IPs	⊙ Version 7.03758	View List
Botnet Domains	⊙ Version 3.00847	View List
⊞ Operational Technology (OT) Security Service	✓ Licensed (Expiration Date: 2025/11/10)	
⊟ Web Filtering	✓ Licensed (Expiration Date: 2025/11/10)	
Blocked Certificates	⊙ Version 1.00487	
DNS Filtering	✓ Licensed (Expiration Date: 2025/11/10)	
Video Filtering	✓ Licensed (Expiration Date: 2025/11/10)	
SD-WAN Network Monitor	⚠ Not Licensed	Purchase ▾
SD-WAN Overlay as a Service	⚠ Not Licensed	Purchase ▾

An administrator is trying to find the web filter database signature on FortiGate to resolve issues with websites not being filtered correctly in a flow-mode web filter profile.

Why is the web filter database version not visible on the GUI, such as with IPS definitions?

A. The web filter database is stored locally, but the administrator must run over CLI diagnose autoupdate versions.

B. The web filter database is stored locally on FortiGate, but it is hidden behind the GUI. It requires enabling debug mode to make it visible.

C. The web filter database is not hosted on FortiGate: FortiGate queries FortiGuard or FortiManager for web filter ratings on demand.

D. The web filter database is only accessible after manual syncing with a valid FDS server using diagnose test update info.

Suggested Answer: *C*

Community vote distribution

C (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: C

EFW Admin 7.4 Study guide, p. 170.

upvoted 1 times

Tweefo 2 months, 3 weeks ago

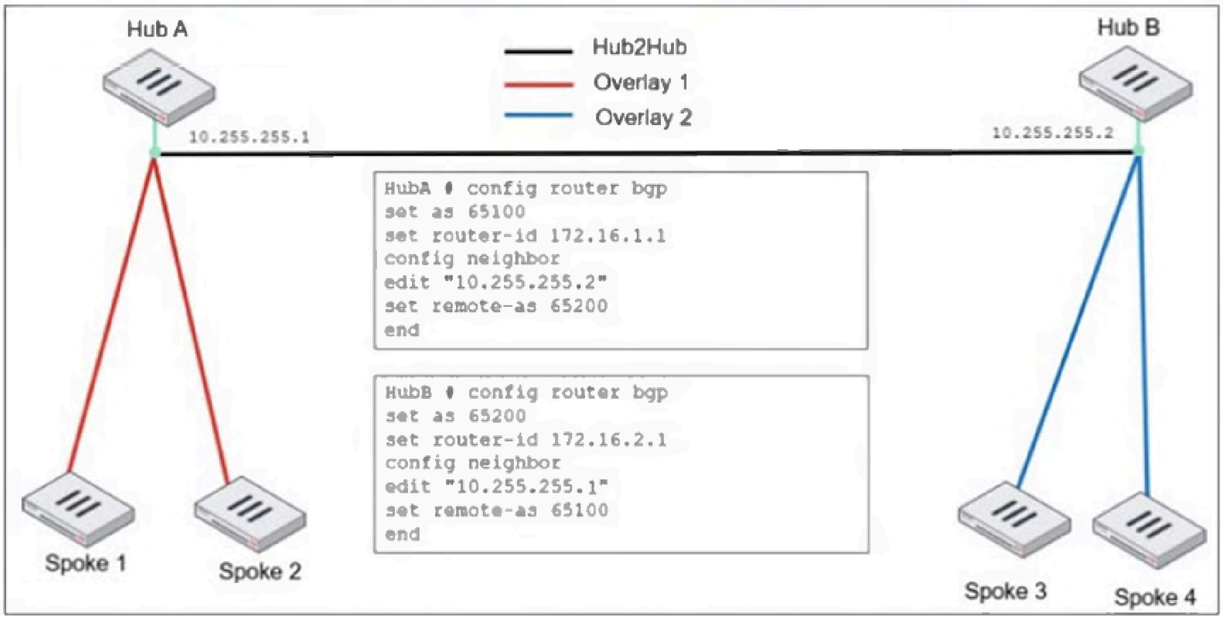
Selected Answer: C

C is correct. FortiGate does not store a full local web filtering database. When web traffic matches a policy using web filtering, FortiGate queries FortiGuard for the URL rating. The result is then cached locally on the firewall for future use.

upvoted 1 times

Question #26 *Topic 1*

Refer to the exhibit, which shows an ADVPN network



```
HubA # config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor
edit "10.255.255.2"
set remote-as 65200
end
```

```
HubB # config router bgp
set as 65200
set router-id 172.16.2.1
config neighbor
edit "10.255.255.1"
set remote-as 65100
end
```

An administrator must configure an ADVPN using IBGP and EBGP to connect overlay network 1 with 2.
What two options must the administrator configure in BGP? (Choose two.)

A. set ebgp-enforce-multrhop enable

B. set next-hop-self enable

C. set ibgp-enforce-multihop advpn

D. set attribute-unchanged next-hop

Suggested Answer: *AD*

Community vote distribution

AD (75%) AB (25%)

Maria21 5 days, 22 hours ago

Selected Answer: AB

Option A (set ebgp-enforce-multihop enable) → Ensures that EBGP neighbors can establish connections across multiple hops, which is necessary in an ADVPN overlay network where direct peer-to-peer connections may not exist.

Option B (set next-hop-self enable) → Allows the BGP hub router to advertise itself as the next-hop for IBGP routes, ensuring proper routing between spoke

upvoted 1 times

Adonisthewise22 2 months, 1 week ago

Selected Answer: AD

according Study Guide p.234

upvoted 2 times

Yaghu 3 months ago

Selected Answer: AD

EFW 7.4 Admin guide, p. 234

upvoted 2 times

Poskgraff 3 months ago

Selected Answer: AB

A. set ebgp-enforce-multihop enable

Cuando usas EBGP, los routers vecinos no están directamente conectados. En este caso, para que la sesión EBGP funcione correctamente, se debe habilitar ebgp-enforce-multihop. Esto permite establecer sesiones BGP a través de múltiples saltos.

B. set next-hop-self enable

Esta opción es útil en IBGP cuando el router recibe rutas de otro BGP peer y desea anunciarlas a sus propios peers IBGP. Al habilitar next-hop-self, el Fortigate reemplaza la dirección IP del siguiente salto (next-hop) con su propia dirección IP, asegurando que el tráfico sea enrutado correctamente.
Por otro lado:

C. set ibgp-enforce-multihop advpn no es una opción válida o reconocida para este escenario.
D. set attribute-unchanged next-hop se utiliza en casos específicos donde se requiere mantener atributos BGP sin modificar, pero no es necesario para una configuración típica de ADVPN.
upvoted 1 times

⊟ **djekson** 3 months ago

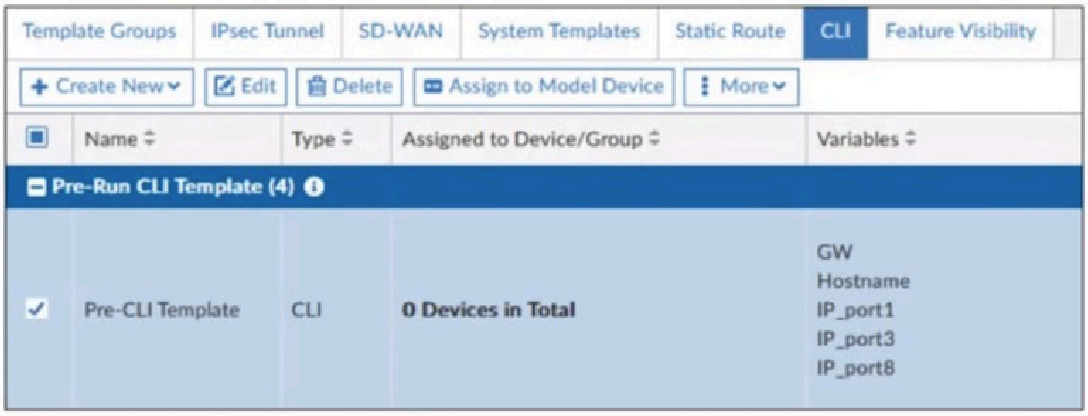
Selected Answer: AD

According to Fortinet docs this should be A and D for the Hubs connecting different overlay networks.
upvoted 2 times

Question #27 *Topic 1*

Refer to the exhibit.

A pre-run CLI template that is used in zero-touch provisioning (ZTP) and low-touch provisioning (LTP) with FortiManager is shown.



☐	Name	Type	Assigned to Device/Group	Variables
Pre-Run CLI Template (4)				
✓	Pre-CLI Template	CLI	**0 Devices in Total**	GW Hostname IP_port1 IP_port3 IP_port8

The template is not assigned even though the configuration has already been installed on FortiGate.

What is true about this scenario?

A. The administrator did not assign the template correctly when adding the model device because pre-CLI templates remain permanently assigned to the firewall

B. Pre-run CLI templates are automatically unassigned after their initial installation

C. Pre-run CLI templates for ZTP and LTP must be unassigned manually after the first installation to avoid conflicting error objects when importing a policy package

D. The administrator must use post-run CLI templates that are designed for ZTP and LTP

Suggested Answer: *B*

Community vote distribution

B (100%)

Yaghu 2 months, 3 weeks ago

Selected Answer: B

EFW Admin Study Guide, p. 43

upvoted 1 times

Tweefo 2 months, 3 weeks ago

Selected Answer: B

B is correct.

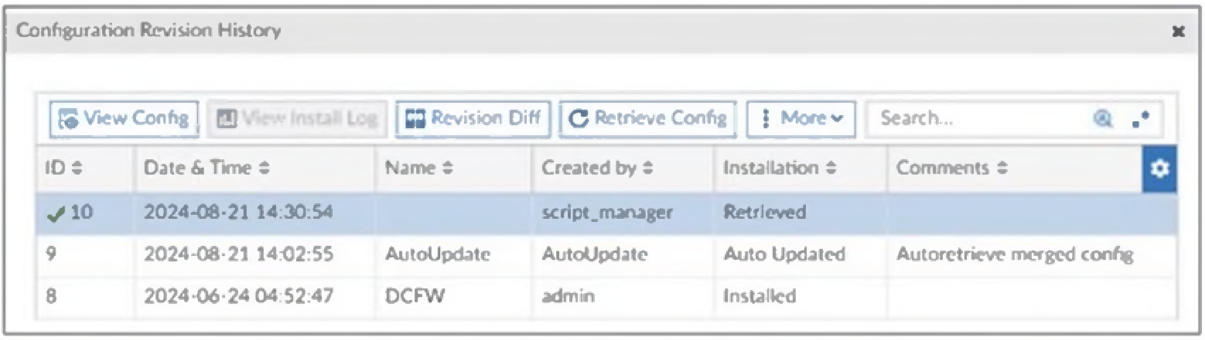
FortiManager automatically unassigns the pre-run CLI template from the FortiGate device database after the quick install process

Source : Study Guide P43

upvoted 2 times

Question #28 *Topic 1*

Refer to the exhibit, which shows a revision history window in the FortiManager device layer.



ID	Date & Time	Name	Created by	Installation	Comments
✓ 10	2024-08-21 14:30:54		script_manager	Retrieved	
9	2024-08-21 14:02:55	AutoUpdate	AutoUpdate	Auto Updated	Autoretrieve merged config
8	2024-06-24 04:52:47	DCFW	admin	Installed	

The IT team is trying to identify the administrator responsible for the most recent update in the FortiGate device database.
Which conclusion can you draw about this scenario?

A. This retrieved process was automatically triggered by a Remote FortiGate Directly (via CLI) script.

B. The user script_manager is an API user from the Fortinet Developer Network (FDN) retrieving a configuration.

C. To identify the user who created the event, check it on the Configuration and Installation widget on FortiGate within the FortiManager device layer.

D. Find the user in the FortiManager system logs and use the type=script command to find the administrator user in the user field.

Suggested Answer: *D*

Community vote distribution

A (67%) D (33%)

sacranone 1 month ago

Selected Answer: D

it is true the D: I've tried with FM

upvoted 1 times

themageofsec 1 month, 2 weeks ago

Selected Answer: A

A is correct. Check Study Guide P. 41 and 30.

B is non-sense option.

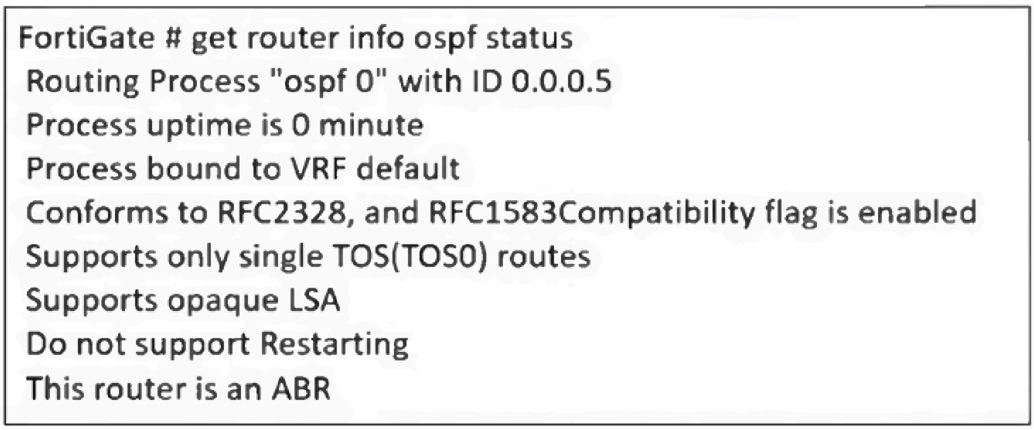
C could be, but I checked on FortiManager GUI and in "Configuration and Installation" section said about which script was ran and when and not who ran.

D also could be, but checking on FortiManager GUI I couldn't filter the Event logs with type=script, it was shown no logs; I've tried in FortiAnalyzer that received that FMG logs filtering in Text mode and I also couldn't it.

upvoted 2 times

Question #29 *Topic 1*

Refer to the exhibit, which contains the partial output of an OSPF command.



```
FortiGate # get router info ospf status
 Routing Process "ospf 0" with ID 0.0.0.5
 Process uptime is 0 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 This router is an ABR
```

An administrator is checking the OSPF status of a FortiGate device and receives the output shown in the exhibit.

What two conclusions can the administrator draw? (Choose two.)

A. The FortiGate device is a backup designated router

B. The FortiGate device is connected to multiple areas

C. The FortiGate device injects external routing information

D. The FortiGate device has OSPF ECMP enabled

Suggested Answer: *BD*

Community vote distribution

BD (100%)

⊟ **79cab4d** Highly Voted 3 months ago

Selected Answer: BD

DR/BDR status is not apparent in this output.

This router is ABR (Area Border Router), so it must be connected to several Areas,

This router is not injecting external route, as it would then be marked as ASBR, and this would be seen in provided output.

As I understand, ECMP is enabled in OSFP by default, but it uses RFC 2328 path preference rules. This router has OSPF ECMP RFC1583 Compatibility enabled.

upvoted 5 times