DUMPSBOSS.

FCPFortiGate 7.6 Administrator

Fortinet FCP_FGT_AD-7.6

Version Demo

Total Demo Questions: 10

Total Premium Questions: 128

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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

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

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

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

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

ANSWER: A

Explanation:

With HA override turned on, FortiGate follows a pretty specific “who becomes primary?” checklist. First, it looks at how many monitored interfaces are actually up and connected. The unit with more healthy monitored links wins, because that usually means it’s in a better position to forward traffic reliably.

If there’s still a tie, FortiGate then checks the configured HA device priority. Higher priority is meant to let you intentionally prefer one box as the primary when everything else is equal.

When priorities match too, the next tiebreaker is HA uptime (how long the unit has been up as part of the cluster), and if they’re still identical, it finally falls back to the FortiGate serial number as the last deterministic way to pick a winner.

Reference: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/907502/ha-cluster-elections

QUESTION NO: 2

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

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

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

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

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

ANSWER: B D

Explanation:

FortiGate supports the common IKEv1 authentication methods you’d expect in real deployments: you can authenticate peers using either a pre-shared key (PSK) or digital certificates (certificate signature). PSK is simple and quick to set up, while certificates are usually preferred in larger environments because they scale better and give you stronger identity checking.

On top of that, FortiGate also supports XAuth in IKEv1. XAuth is basically an extra login step where the remote user/peer must also provide a username and password after the IKE phase 1 authentication. It's not about "fewer packets" or being faster—it's about adding user-level authentication to the tunnel setup.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/363127/ipsec-vpn-overview and https://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION NO: 3

Refer to the exhibit, which shows a routing table.

Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Connected
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only.

What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

A. The new static route must have the distance set to 9.

B. The existing static route through port3 must have the distance set to 11.

C. The new static route must have the priority set to 3.

D. The new static route must have the metric set to 1.

ANSWER: A B

Explanation:

On FortiGate, if there are multiple routes to the same destination prefix (like 172.20.1.0/24), the firewall picks the "best" one based on route selection rules. For static routes, the most important tie-breaker you can easily control is the administrative distance: lower distance wins.

So to force traffic to use port2, you can either make the new static route via port2 more preferred (give it a lower distance than the competing route), or make the existing route via port3 less preferred (raise its distance). That's why setting the new route's distance to 9 works (assuming the competing one is 10), and alternatively changing the port3 route's distance to 11 would also make the port2 route win.

Priority and metric aren't the deciding factors here in the way these options suggest. "Priority" is mainly relevant for policy routes, and "metric" is typically used within dynamic routing protocols or as an internal value, not the primary selector over administrative distance for competing static routes.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/ and https://docs.fortinet.com/document/fortigate/7.6.0/cli-reference

QUESTION NO: 4

An administrator notices that some users are unable to establish SSL VPN connections, while others can connect without any issues.

What should the administrator check first?

A. Ensure that the affected users are using the correct port number.

B. Ensure that user traffic is hitting the firewall policy.

C. Ensure that forced tunneling is enabled to reroute all traffic through the SSL VPN

D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface

ANSWER: A

Explanation:

If only *some* users can't connect while others are fine, the SSL VPN service itself is probably up and listening. That usually points to a client-side mismatch or a per-user setting rather than a global FortiGate problem. The quickest first check is whether the affected users are trying to connect to the right SSL VPN port (for example, 443 vs 10443). A wrong port will fail the connection before authentication and before any firewall policy comes into play.

Firewall policies and split/forced tunneling matter after the tunnel is established, so they're not the first place to look for a basic "can't connect" symptom. Also, enabling HTTPS on the SSL VPN tunnel interface isn't what controls SSL VPN listening; SSL VPN uses its own configured listen interface and port.

For background on SSL VPN port/listener behavior, see Fortinet docs: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide

QUESTION NO: 5

Refer to the exhibit.

The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit.

For which two reasons are these web categories exempted? (Choose two.)

A. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport

Security.

B. These websites are in an allowlist of reputable domain names maintained by FortiGuard.

C. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.

D. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

ANSWER: A D

Explanation:

Some categories are skipped because deep inspection works by having FortiGate generate a substitute (temporary) certificate. That breaks sites that enforce certificate pinning or strict TLS behaviors—most commonly seen with HSTS-style “don’t accept anything unexpected” setups—so users can get blocked or see constant certificate errors. To avoid those support headaches and broken logins, FortiGate exempts those types of sites by default.

The other big reason is privacy and compliance. Categories like health, finance, and other sensitive services can fall under legal or regulatory rules, and many organizations choose (or are required) not to intercept and decrypt that traffic. So FortiGate’s default profiles exclude them to reduce the risk of capturing private data while still allowing you to override the list if your policy allows it.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/122794/deep-inspection and https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

QUESTION NO: 6

FortiGate is integrated with FortiAnalyzer and FortiManager.

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

A. Sequence ID

B. Log ID

C. Policy ID

D. Universally Unique Identifier

ANSWER: D

Explanation:

When you connect FortiGate to FortiManager or FortiAnalyzer, FortiGate adds a UUID (Universally Unique Identifier) to each firewall policy. The key idea is that policy IDs can change over time (for example, if you reorder policies, insert new ones, or import policies), but the UUID stays the same. That “stable identity” is what makes centralized management and log correlation work smoothly.

In practice, FortiAnalyzer can use the UUID to reliably tie log entries back to the exact policy that matched the traffic, even if the policy’s position or numeric policy ID changes later. FortiManager also benefits because it can track and synchronize the same policy consistently across revisions and installs.

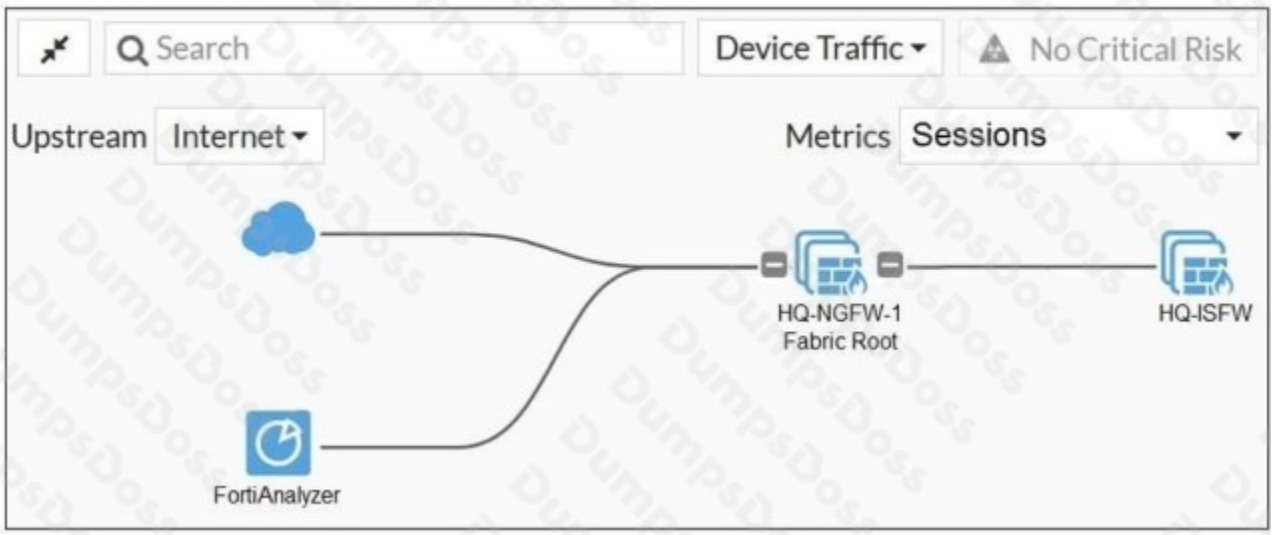
That’s why options like “Policy ID” or “Sequence ID” aren’t the best answer here—they’re not guaranteed to remain consistent. The UUID is specifically designed for this kind of cross-system tracking and is the attribute Fortinet relies on for better integration.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide and https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide

QUESTION NO: 7

Refer to the exhibits.

Security Fabric physical topology view



New address object on HQ-NGFW-1

Security Fabric configuration on HQ-NGFW-1

```
HQ-NGFW-1 # show full-configuration system csf
config system csf
     set status enable
     set uid "10e202dad887c02ac8bafa024228d86d"
     set upstream ' '
     set source-ip 0.0.0.0
     set upstream-interface-select-method auto
     set upstream-port 8013
     set-group-name "Fortinet"
     set group-password ENC M8h5eGm9sVzi555Pp5y
YEaCjk/95p0MHllmMjY3dkVA
     set accept-auth-by-cert enable
     set log-unification enable
     set authorization-request-type serial
     set fabric-workers 2
     set downstream-access disable
     set configuration-sync default
     set fabric-object-unification local
     set saml-configuration-sync default
```

Security Fabric configuration on HQ-ISFW

```
HQ-NGFW-1 # show full-configuration system csf
config system csf
    set status enable
    set uid "dd0263000fa8209fc0d99a40faf9c818"
    set upstream "10.0.11.254"
    set source-ip 0.0.0.0
    set upstream-interface-select-method auto
    set upstream-port 8013
    set-group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync local
    set file-mgmt enable
    set file-quota 0
    set file-quota-warning 90
end
```

An administrator creates a new address object on the root FortiGate (HQ-NGFW-1) in the Security Fabric. After synchronization, this object is not available on the downstream FortiGate (HQ-ISFW).

What must the administrator do to synchronize the address object?

A. Change the csf setting on HQ-ISFW (downstream) to set configuration-sync local.

B. Change the csf setting on HQ-ISFW (downstream) to set saml-configuration-sync default.

C. Change the csf setting on HQ-NGFW-1 (root) to set fabric-object-unification default.

D. Change the csf setting on both devices to set downstream-access enable.

ANSWER: C

Explanation:

This happens when the root FortiGate is set to keep “fabric objects” local instead of sharing them across the Security Fabric. In other words, you can create the address object on the root, but FortiGate won’t push it down to downstream devices because object unification is not set to the normal shared behavior.

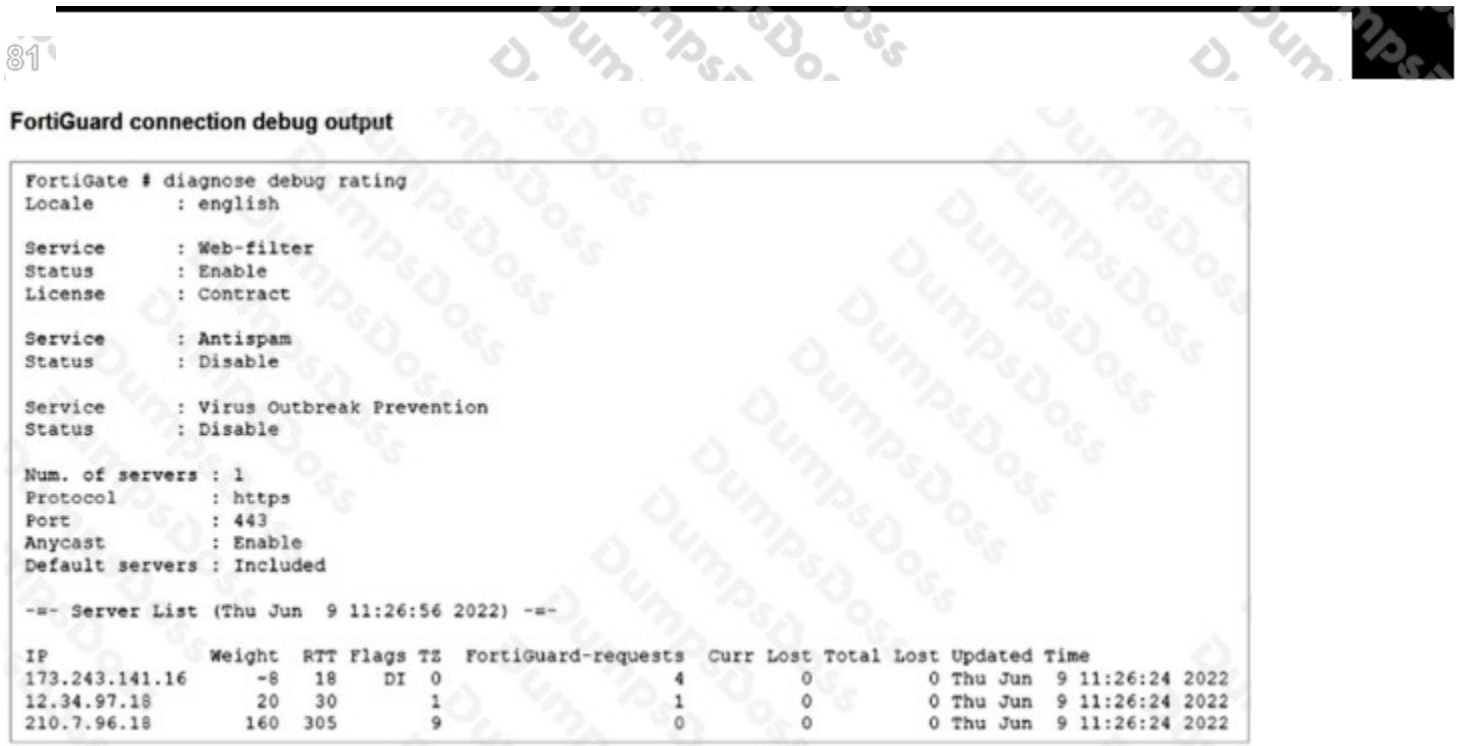
To fix it, you change the CSF (Security Fabric) setting on the root device (HQ-NGFW-1) to use the default fabric object unification mode. Once it’s set back to *default*, newly created objects like addresses (and other shared objects) can be synchronized to downstream FortiGates such as HQ-ISFW.

The other options don't really address object propagation. Things like SAML sync are unrelated, and changing downstream-only settings won't help if the root is explicitly configured not to unify/share objects.

Reference: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/50915/security-fabric

QUESTION NO: 8

Refer to the exhibit showing a FortiGuard connection debug output.



FortiGuard connection debug output

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

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

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

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

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

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

B. FortiGate is using default FortiGuard communication settings.

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

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

ANSWER: A B

Explanation:

From the debug, you can see the service listed (for example, Web-filter) with the license shown as *Contract* and the line indicating *Num. of servers: 1*. That tells you FortiGate successfully contacted a single FortiGuard server to pull contract/licensing information for that service.

The output also shows *Default servers: Included*. That's FortiGate's way of saying it's using the built-in FortiGuard server list (the normal, public FortiGuard infrastructure), not a custom override like a private server list or a local proxy/service point.

The other choices don't match what this snippet proves. Packet loss would require seeing loss counters or consecutive failures, and nothing here confirms that. And FortiManager is not a FortiGuard server—FortiGate can be managed by FortiManager, but FortiGuard rating/contract checks go to FortiGuard servers, not FortiManager.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/561790/fortiguard https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/779786/troubleshooting-fortiguard-services

QUESTION NO: 9

FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

A. Policy ID

B. Log ID

C. Universally Unique Identifier

D. Sequence ID

ANSWER: C

Explanation:

The key attribute here is the policy UUID (Universally Unique Identifier). FortiGate assigns a UUID to each firewall policy, and that UUID is what FortiAnalyzer and FortiManager use to consistently recognize the same policy over time.

This matters because things like the policy ID, order/sequence, or even edits to the policy can change as you rearrange rules or import configurations. If FortiAnalyzer/FortiManager relied only on the policy ID or sequence, logs and policy references could get confusing or mismatched after changes. The UUID stays stable, so logs keep pointing to the right policy and management features work more reliably.

So, to improve integration and make sure logging and policy tracking stay accurate across FortiGate, FortiAnalyzer, and FortiManager, the UUID is the attribute that really makes it work smoothly.

References: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide and https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide

QUESTION NO: 10

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.

B. Heartbeat IP addresses are used to distinguish between cluster members.

C. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.

D. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.

ANSWER: B D

Explanation:

In a FortiGate HA cluster, the heartbeat links aren't just "cables between boxes"—they need a simple way for each unit to recognize who's who. That's why heartbeat IP addresses exist: each cluster member gets a unique heartbeat IP so the devices can identify each other and exchange HA control traffic reliably.

These heartbeat IPs are also not something you typically set by hand. FortiGate assigns them automatically, and they can be re-assigned when the cluster membership changes. So if a unit joins the cluster or one drops out, the heartbeat IP addressing can shift to keep the heartbeat communication consistent across the remaining members.

You can read more about how FortiGate HA works (including heartbeat behavior and HA communication) in the Fortinet docs here: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/ and specifically HA concepts here: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/365339/high-availability.