



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

- A. Enabled
- B. On Idle
- C. Disabled
- D. On Demand

Correct Answer: *B*

None

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

- A. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
- B. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.
- C. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
- D. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.

Correct Answer: AD

None

You have created a web filter profile named restrict_media-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down. What could be the reason?

- A. The firewall policy is in no-inspection mode instead of deep-inspection.
- B. The inspection mode in the firewall policy is not matching with web filter profile feature set.
- C. The web filter profile is already referenced in another firewall policy.
- D. The naming convention used in the web filter profile is restricting it in the firewall policy.

Correct Answer: *B*

None

Refer to the exhibit.

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
pid = 2044, engine count = 0 (+1)
0 - pid:2074:2074 cfg:1 master:0 run:1
```

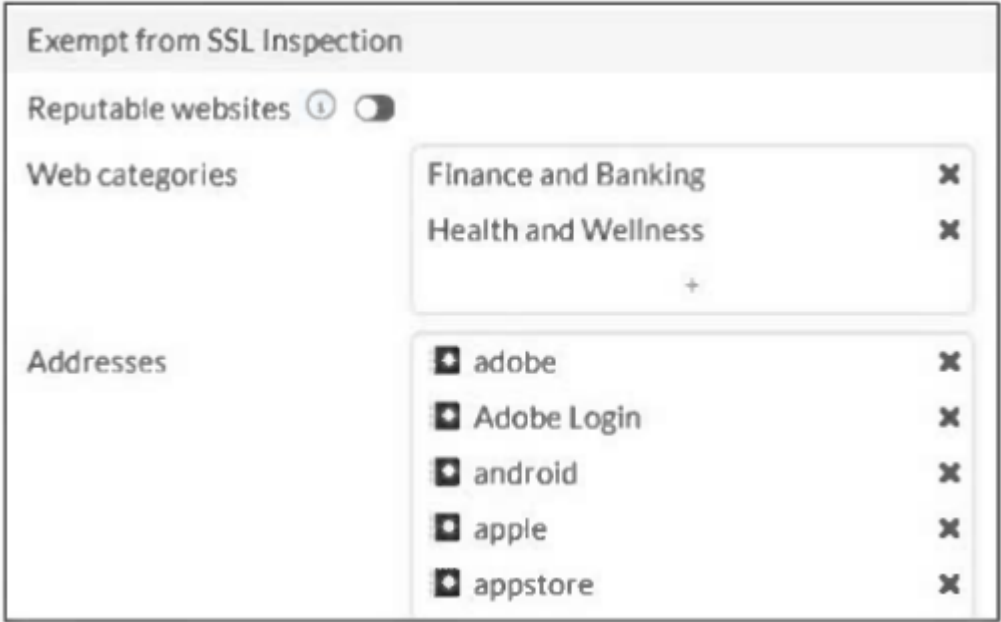
As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit. What could be the possible reason of the diagnose output shown in the exhibit?

- A. There is a no firewall policy configured with an IPS security profile.
- B. FortiGate entered into IPS fail open state.
- C. Administrator entered the command diagnose test application ipsmonitor 5.
- D. Administrator entered the command diagnose test application ipsmonitor 99.

Correct Answer: A

None

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.

Correct Answer: AD

None

Refer to the exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity.

What must the administrator configure to answer this specific request from the NOC team?

- A. Move NOC_Access to the top of the list to ensure all profile settings take effect.
- B. Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile.
- C. Ensure that all NOC_Access users are assigned the super_admin role to guarantee access
- D. Increase the admintimeout value under config system accprofile NOC_Access.

Correct Answer: D

None

Refer to the exhibit.

```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

- A. Administrators cannot change the configuration.
- B. FortiGate skips quarantine actions.
- C. Administrators must restart FortiGate to allow new session.
- D. FortiGate drops new sessions requiring inspection.

Correct Answer: *BD*

None

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

Correct Answer: A

None

An administrator wanted to configure an IPS sensor to block traffic that triggers a signature set number of times during a specific time period. How can the administrator achieve the objective?

- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS filter, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Correct Answer: C

None


A FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website. Which protocol must FortiGate allow even though the user cannot authenticate?

- A. LDAP
- B. TACASC+
- C. Kerberos
- D. DNS

Correct Answer: *D*

None

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

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	 

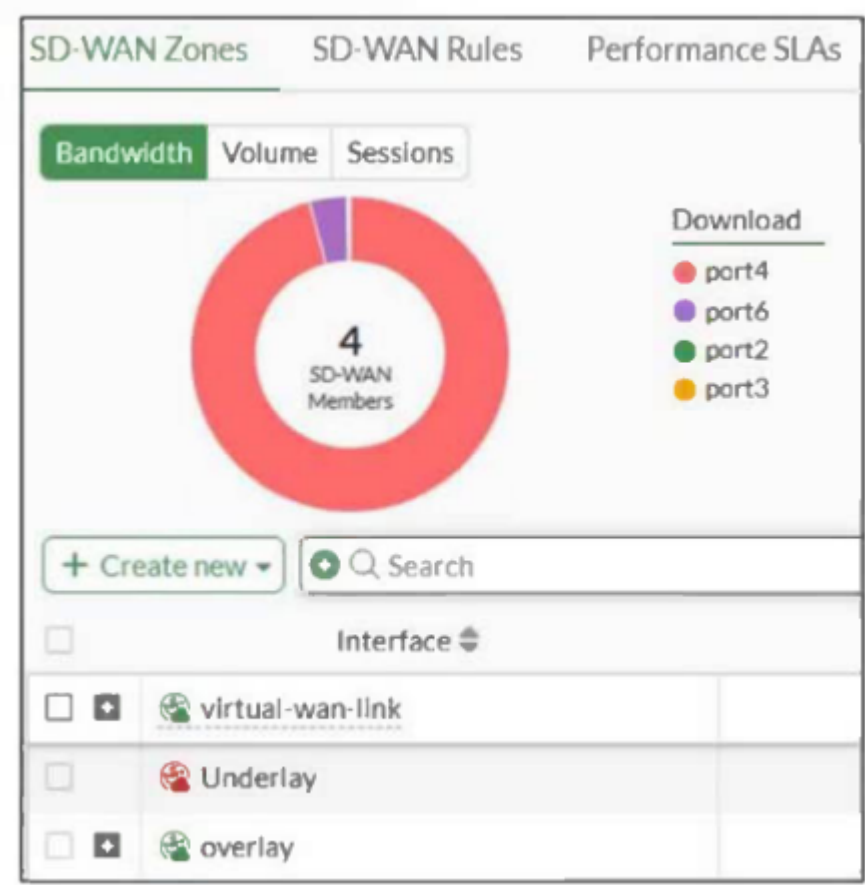
Why does the FortiGate administrator need this configuration?

- A. To set up a RADIUS server Secret.
- B. To authenticate Any FortiGate user groups.
- C. To authenticate and match the Training OU on the RADIUS server.
- D. To authenticate only the Training user group.

Correct Answer: D

None

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



Based on the exhibit, which statement is true?

- A. The Underlay zone is the zone by default.
- B. The Underlay zone contains no member.
- C. port2 and port3 are not assigned to a zone.
- D. The virtual-wan-link and overlay zones can be deleted.

Correct Answer: A

None





Which three statements explain a flow-based antivirus profile? (Choose three.)

- A. FortiGate buffers the whole file but transmits to the client at the same time.
- B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- C. If a virus is detected, the last packet is delivered to the client.
- D. Flow-based inspection optimizes performance compared to proxy-based inspection.
- E. The IPS engine handles the process as a standalone.

Correct Answer: *ABD*

None

Refer to the exhibit.

Application and Filter Overrides			
<div>+ Create New Edit Delete</div>			
Priority	Details	Type	Action
1	 ABC.Com	Application	 Allow
2	 Excessive-Bandwidth	Filter	 Block
2			

An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.

Why are there no logs generated under security logs for ABC.Com?

- A. The ABC.Com Type is set as Application instead of Filter.
- B. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
- C. The ABC.Com Action is set to Allow.
- D. The ABC.Com is hitting the category Excessive-Bandwidth.

Correct Answer: C

None

Which two statements describe characteristics of automation stitches? (Choose two.)

- A. Actions involve only devices included in the Security Fabric.
- B. An automation stitch can have multiple triggers.
- C. Multiple actions can run in parallel.
- D. Triggers can involve external connectors.

Correct Answer: *CD*

None

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They can be measured actively or passively.
- C. They are applied in a SD-WAN rule lowest cost strategy.
- D. They monitor the state of the FortiGate device.
- E. All the SLA targets can be configured.

Correct Answer: *ABE*

None

Which two statements are true about an HA cluster? (Choose two.)

- A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
- B. Link failover triggers a failover if the administrator sets the interface down on the primary device.
- C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
- D. HA incremental synchronization includes FIB entries and IPsec SAs.

Correct Answer: *BD*

None