# Examens : Optimisation de l'Administration FortiGate 7.6

Avoir un **bon contrôle** de la configuration et de l'administration de **FortiGate 7.6** est crucial pour assurer la sécurité de votre réseau. Pour plus d'informations, vous pouvez consulter ce lien. Voici quelques étapes et conseils pour vous aider à mieux comprendre ce système.

## Qu'est-ce que FortiGate 7.6 ?

**FortiGate 7.6** est une solution de pare-feu de *nouvelle génération* qui offre de nombreuses fonctionnalités pour **protéger** votre réseau. En comprenant son architecture, vous pouvez le configurer de manière plus efficace.

## Pourquoi choisir FortiGate pour votre réseau ?

Le pare-feu **FortiGate** est reconnu pour sa capacité à **empêcher les menaces externes** et à garantir une **connexion sécurisée**. Une bonne administration de FortiGate permet de renforcer cette sécurité.

## Configuration de FortiGate

La configuration initiale de FortiGate peut sembler complexe, mais elle repose sur des **principes simples**. Commencez par définir vos *politiques de sécurité* et vos *règles d'accès*.

## Les éléments essentiels de la sécurité réseau FortiGate

Pour que votre sécurité réseau soit efficace, il est important de comprendre les éléments clés tels que :

- *VPN*
- *IDS/IPS*
- *Filtrage web*

Chaque composant joue un rôle important dans la **protection de votre infrastructure**. Pour une préparation approfondie, vous pouvez lire plus à propos des certifications sur cette

plateforme.

## Gestion de FortiGate

La gestion de FortiGate implique la **surveillance constante** et l'ajustement des configurations. Utilisez des outils de reporting pour **analyser les performances** et **détecter les anomalies**.

## Astuce : Utiliser des mises à jour régulières

Assurez-vous de garder votre **logiciel FortiGate** à jour. Les mises à jour incluent souvent des **correctifs de sécurité** qui peuvent **protéger votre réseau** contre de nouvelles menaces.

## Formation et certification

Pour approfondir vos **connaissances**, envisagez de suivre des formations sur l'administration de FortiGate. Cela peut non seulement vous aider dans votre travail actuel, mais aussi ouvrir des portes à de **nouvelles opportunités**.

## Conclusion

Optimiser l'administration de FortiGate 7.6 est un **atout précieux** pour quiconque s'occupe de la sécurité réseau. En suivant ces conseils, vous serez en mesure de configurer votre réseau de manière plus **sûre** et **efficace**.

# Fortinet

## FCP_FGT_AD-7.6 Exam

### FCP - FortiGate 7.6 Administrator

Thank you for Downloading FCP_FGT_AD-7.6 exam PDF Demo

You can Buy Latest FCP_FGT_AD-7.6 Full Version Download

https://www.certkillers.net/Exam/FCP_FGT_AD-7.6

# Version: 4.0

## Question: 1

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

**Answer: A**

Explanation:

The "On Idle" DPD mode configures FortiGate to send DPD probes only when no inbound traffic is detected, meeting the requirement to send probes only when the tunnel is idle.

## Question: 2

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.

**Answer: A, D**

Explanation:

When SD-WAN is disabled, FortiGate supports volume-based ECMP mode via the v4-ecmp-mode parameter.
When SD-WAN is enabled, the load balancing algorithm is controlled by the load-balance-mode parameter within the SD-WAN configuration.

## Question: 3

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.

**Answer: B**

Explanation:

Web filter profiles with category usage quotas require the firewall policy to be in proxy-based (deep) inspection mode; if the inspection mode does not match this requirement, the profile will not appear in the drop-down list.

## Question: 4

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.

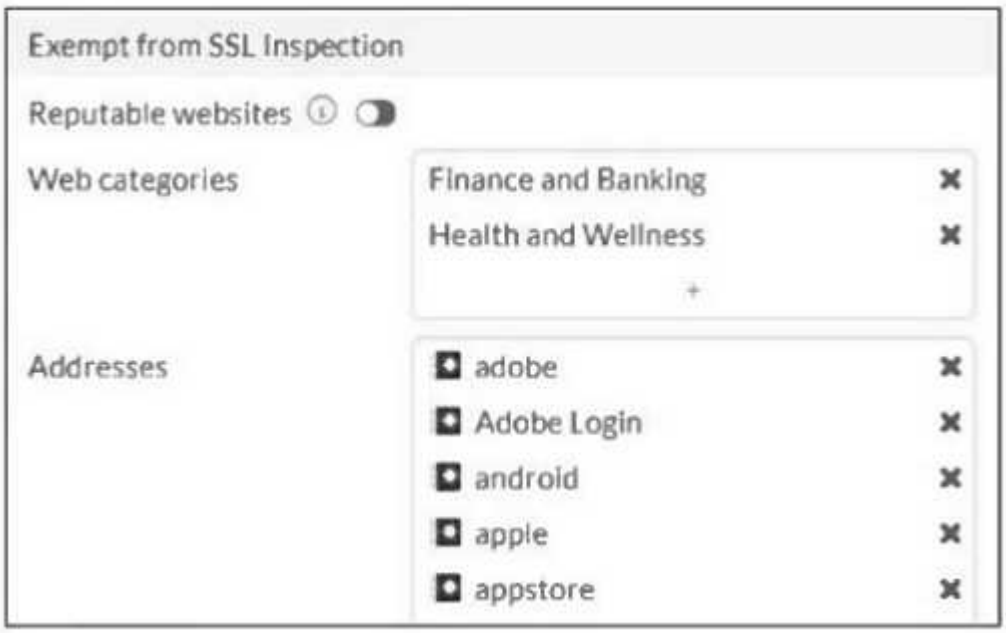
**Answer: A**

Explanation:

The output shows the IPS engine count as 0, indicating no active IPS engines are running. This typically means no firewall policy is referencing the IPS security profile, so the IPS profile is not being applied or triggered.

## Question: 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:

FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection.
Legal regulations require exemption of certain categories to protect user privacy and sensitive information, so these web categories are excluded from SSL inspection.

**Thank You for trying FCP_FGT_AD-7.6 PDF Demo**

To Buy New FCP_FGT_AD-7.6 Full Version Download visit link below

**https://www.certkillers.net/Exam/FCP_FGT_AD-7.6**

# Start Your FCP_FGT_AD-7.6 Preparation

*[Limited Time Offer]* Use Coupon "CKNET" for Further discount on your purchase. Test your FCP_FGT_AD-7.6 preparation with actual exam questions.