



Formation Fortigate Infrastructure 6.2



Mohamed Anass EDDIK

Une formation
Alphorm.com



Cursus Fotigate 6.2



Une formation
Alphorm.com



Une formation
Alphorm
com

Plan

Introduction

1. Configurer IPsec VPN
2. Configurer le DLP
3. Configurer Routage
4. Configurer SD-WAN
5. Configurer les domaines virtuels
6. Configurer le Switching
7. Configurer le VPN site-to-site IPsec
8. Configurer le Fortinet SSO
9. Configurer la HA
10. Configurer le Proxy Web
11. Effectuer les diagnostics

Conclusion



Une formation
Alphorm
com

Public concerné

Support technique

Administrateur sécurité

Avant-vente sécurité

Préparer la Certification NSE4



Prérequis

Passer la formation Fortigate Security
Connaissances en sécurité
Connaissances en TCP/IP
ou bien



Une formation
Alphorm
com

A vous de jouer !





Une formation
Alphorm.com

Présentation du Lab de la formation



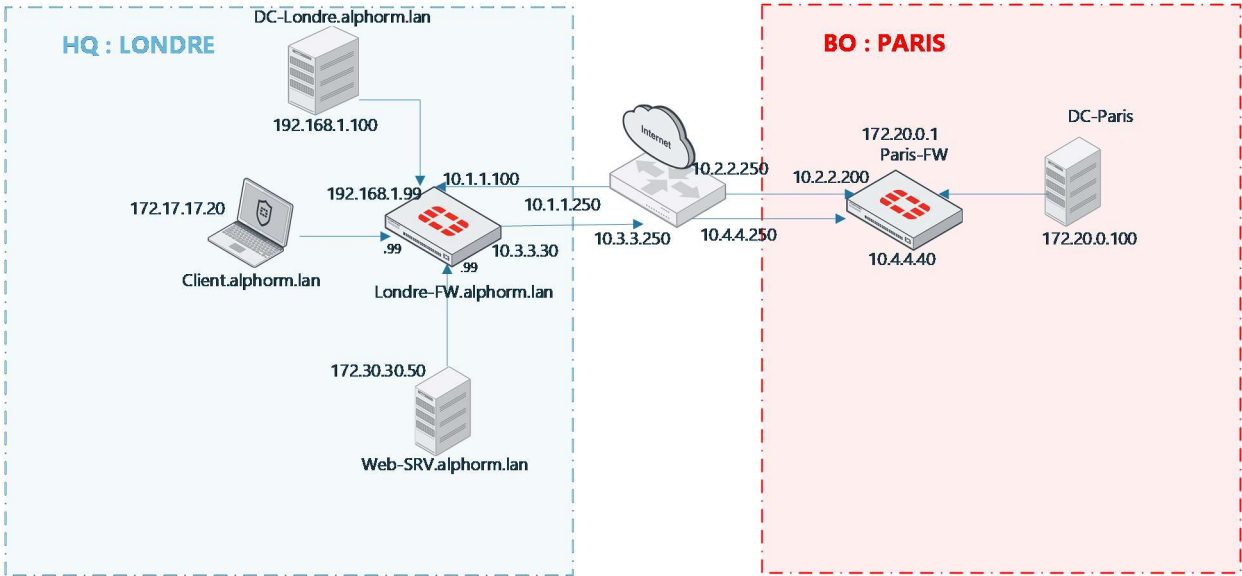
Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Schéma du Lab
Environnement du Lab
Connectique VMnet



Environnement du Lab

HQ:LONDRE

Nom machine	IP	Rôle
DC-londre.alphorm.lan	192.168.1.100	DC + Autorité de certification
Web-srv.alphorm.lan	172.30.30.50	Serveur web
Client.alphorm.lan	172.17.17.20	Client final
Londre-FW.alphorm.lan	192.168.1.99	Fortigate FW + passerelle par défaut + plusieurs interfaces DMZ

BO:Paris

Nom machine	IP	Rôle
DC-Paris	172.20.0.100	DC + Autorité de certification + Webmail + Client final
Paris-FW	172.20.0.1	Fortigate XG FW + passerelle par défaut



Connectique VMnet

Nom	VMnet	Réseau
Lan-Londre	VMnet1	192.168.1.0/24
User	VMnet2	172.17.17.0/24
DMZ-Srv	VMnet3	172.30.30.50/24
WAN-Londre	VMnet4	10.1.1.0/24
WAN-Paris	VMnet5	10.2.2.0/24
WAN2-Londre	VMnet7	10.3.3.0/24
Wan2-Paris	VMnet8	10.4.4.0/24
Lan-Paris	VMnet6	172.20.0.0/24

Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Comprendre Policy-Based et Route-based



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Encapsulation

IKE Phase 1

NAT-T

IKE Phase 2

Policy-based et Route-based

Lab



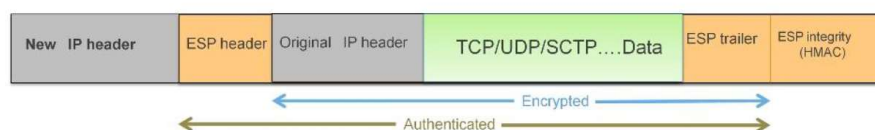
Une formation
Alphorm.com

Encapsulation

No VPN



Tunnel Mode

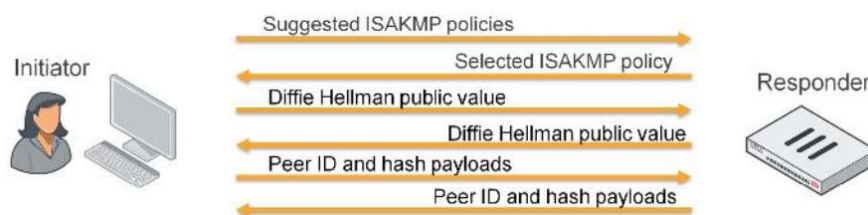


Transport Mode



Une formation
Alphorm.com

IKE Phase 1



- Authentifier les pairs
- Négocier une SA bidirectionnelle
- Echange DH pour clés secrètes

Le premier paquet n'a pas l'ID d'homologue, ainsi le répondeur ne peut pas l'utiliser pour identifier l'initiateur



Une formation
Alphorm.com

NAT-T

ESP ne peut pas prendre en charge NAT car il n'a pas de numéros de port

Si **NAT Traversal** est défini sur **Enable**, il détecte si les périphériques NAT existent sur le chemin d'accès.

Si oui, ESP est encapsulé sur UDP 4500, il est conseillé si initiateur ou répondeur est derrière NAT.

Si **NAT Traversal** est défini sur forcé :

ESP est toujours encapsulé sur UDP, même lorsqu'il n'y a pas de périphériques NAT sur le chemin



Une formation
Alphorm.com

IKE Phase 2

Négocie deux SAs unidirectionnels pour ESP (protégé par phase1 IKE SA)

Lorsque SA est sur le sujet d'expirer, il renégocie .

Chaque phase 1 peut avoir plusieurs phases 2

Si plusieurs phases 2 existent, FortiGate dirige le trafic pour corriger la phase 2



Policy-based et Route-based

Feature	Policy-based	Route-based
FortiGate operation mode	NAT and transparent	Only NAT
L2TP-over-IPsec	Yes	Yes
GRE-over-IPsec	No	Yes
Routing Protocols	No	Yes
Number of policies per VPN	One policy controls both traffic directions	2 policies usually – one for each direction





Une formation
Alphorm.com

Configurer IPsec VPN



Mohamed Anass EDDIK



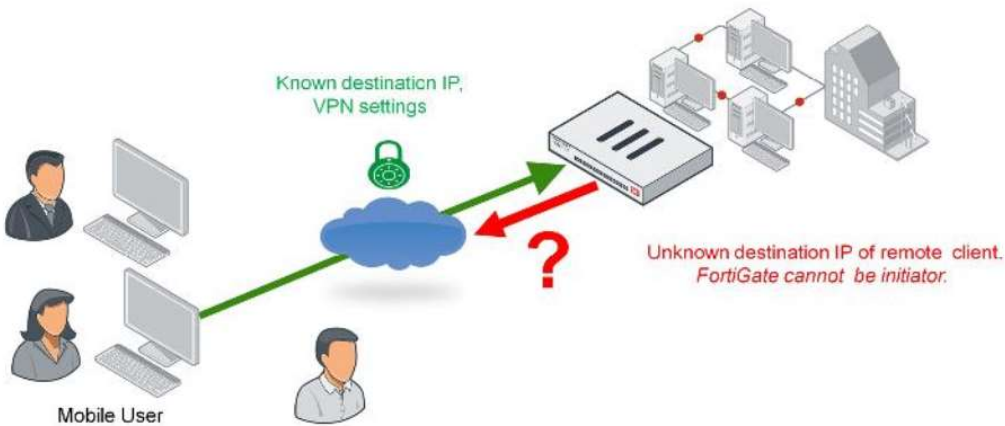
Une formation
Alphorm.com

Plan

DialUp VPN Lab



DialUp VPN



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Surveiller l'IPsec VPN



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Bonnes pratiques
Lab



Une formation
Alphorm.com

Bonnes pratiques

Dans les circonstances où plusieurs tunnels VPN à distance commutés existent, assurez-vous que le tunnel a un PEER ID appliqué

Assurez-vous de la compatibilité entre la version **FortiClient** et la version **FortiClient OS**

Si votre dispositif **FortiGate** est derrière un périphérique NAT, comme un routeur, configurez le transfert de port pour les ports UDP 500 et 4500

Assurez-vous que l'accélération matérielle est activée pour les meilleures performances d'IPsec



Une formation
Alphorm.com





Une formation
Alphorm.com

Comprendre DLP



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Fonctionnement DLP
Modèles de nom de fichier
Types de fichiers
Lab

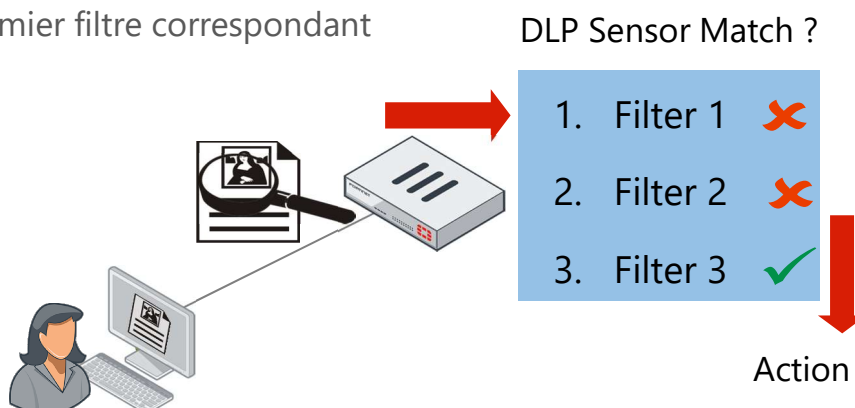
Fonctionnement DLP

Les délégués du moteur DLP numérisent vers les processus appropriés (IPS, proxy)

Les filtres définissent le ou les motifs à rechercher dans le paquet/fichier

Le capteur contient des filtres – Liste des critères de correspondance

FortiGate applique le premier filtre correspondant



Modèles de nom de fichier

Modèles spécifiés par :

Nom de fichier complet ou partiel

Extension de fichier complète ou partielle

Une combinaison de nom et d'extension



nicepainting.jpg



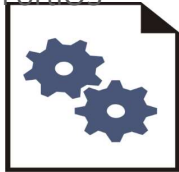
mona.jpg	✗
painting.jpg	✗
nicepainting.png	✗
nicepainting.jpg	✓
*.jpg	✓
nice*.jpg	✓



Types de fichiers

Basé sur le contenu binaire, quel que soit le nom de fichier/extension
Fonctions même si l'utilisateur tente de contourner DLP en
changeant le nom/l'extension de fichier

Types de fichiers pris en charge codés en dur dans le micro-logiciel
FortiOS



File Type Match?

JPEG image	✗
BMP image	✗
CAB archive	✗
ZIP archive	✗
Executable	✓





Une formation
Alphorm.com

Configurer le DLP



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

DLP Fingerprinting
Configuration du capteur DLP pour
Fingerprinting
Archivage DLP
Lab

DLP Fingerprinting

FortiGate scans partagent la recherche de noms de fichiers correspondant au modèle

Fait des empreintes digitales pour les fichiers correspondants

FortiGate effectue une somme de contrôle pour chaque segment du fichier

Stocke les totaux de contrôle des segments, pas le fichier – fonctionne avec des fichiers volumineux

Si la plupart des morceaux correspondent, DLP identifie positivement le fichier

Peut fonctionner même si le fichier est modifié un peu

La taille de bloc par défaut est 2800 octets

```
#config dlp settings
#set chunk-size [100-100000]
#end
```

Modification de la taille du bloc vide toute la base de données



Capteur pour Fingerprinting

La fonction d'empreinte digitale est activée de CLI (seulement) pour chaque filtre dans le capteur DLP

Si configuré dans CLI devient visible dans l'interface graphique, les actions du capteur DLP s'appliquent à toutes les empreintes digitales avec son niveau de sensibilité

```
config dlp sensor
edit <name>
config filter
edit <filter ID>
set proto http get
set filter-by fingerprint
set ip-sensitivity "Critical"
next
end
```

Activé dans le CLI
pour le filtre DLP

Archivage DLP

Archivage Sommaire

Logs correspondant au trafic (URL, email header To/From...)

Protocoles pris en charge (SMTP, POP3, IMAP, MAPI, HTTP (GET et POST seulement), FTP, NNTP)

Activé via la CLI :

```
config dlp sensor
edit <profile_name>
set summary-proto <protocol_list>
end
```

Full Archiving

Log and archive email messages, attachments, webpages

Peut être utile pour l'investigations à court terme

Activé en CLI :

```
config dlp sensor
edit <profile_name>
set full-archive-proto <protocol_list>
end
```





Une formation
Alphorm
com

Paramétrer le Routage sur Fortigate



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Routage statique

Routage Dynamique

PBR

Routage services internet



Une formation
Alphorm.com

Routage statique

Le routage est la façon dont un paquet est envoyé le long d'un chemin-de point à point sur le réseau-de la source à la destination

Si la destination est sur un sous-réseau qui n'est pas directement connecté au routeur, le paquet est relayé à un autre routeur qui est plus proche

Les entrées de la table de routage peuvent être configurées manuellement, dynamiquement ou les deux



Une formation
Alphorm.com

Routage Dynamique

Les chemins sont automatiquement découverts

FortiGate communique avec les voisins pour trouver les meilleurs itinéraires

Les chemins sont basés sur l'adresse IP de destination du paquet

Le routage devient auto-organisateur

FortiGate support : RIP, OSPF, BGP, IS-IS



Une formation
Alphorm.com

Policy-Based Routes

Correspondance plus granulaire que les itinéraires statiques :

- Protocole

- Adresse source

- Port source

- Ports de destination

- Types de bits de service (ToS)

Avoir la priorité sur la table de routage

Maintenu dans une table de routage distincte

Action : FortiGate envoie en utilisant l'interface sortante spécifiée pour la passerelle spécifiée. Arrête le routage des stratégies et utilise la table de routage à la place



Une formation
Alphorm.com

Routage services internet

Acheminer des services Internet bien connus grâce à des interfaces WAN spécifiques

Il cherche automatiquement les nouvelles adresses IP d'un site web et il configure la table de routage static pour vous

Les itinéraires de base de données de service Internet sont en fait des itinéraires de stratégie et prévalent sur tous les autres itinéraires de la table de routage



Une formation
Alphorm
com



Une formation
Alphorm
com

Découvrir l'ECMP et le RFP



Mohamed Anass EDDIK



Plan

ECMP (Equal Cost Multipath) Routing
RPF (Reverse path Forwarding)
LAB

Une formation
Alphorm.com



ECMP

Si les multiples statiques, OSPF, ou BGP ont les mêmes attributs, ils sont tous actifs et FortiGate distribue le trafic à travers chacun d'eux

Pour être pris en compte pour ECMP, les itinéraires doivent avoir les mêmes valeurs pour les attributs suivants : Sous-réseau de destination, distance du système métrique priorité

```
FGT # get router info routing-table all
...output omitted...
S*    0.0.0.0/0 [10/0] via 10.0.1.254, wan1
S     10.0.4.0/24 [10/0] via 10.0.3.254, port1, [5/0]
      [10/0] via 10.200.3.254, port2, [5/0]
C     10.200.3.0/24 is directly connected, port2
C     10.0.1.0/24 is directly connected, wan1
C     10.0.3.0/24 is directly connected, port1
```

Une formation
Alphorm.com



Une formation
Alphorm.com

Méthodes ECMP

Source IP (default) : Les sessions de la même adresse IP source utilisent la même route

Source-destination IP : Les sessions avec la même source et la même paire IP de destination utilisent la même route

Weighted : Les sessions sont distribuées en fonction du poids de l'interface

Usage (Spillover) : Un itinéraire est utilisé jusqu'à ce que le seuil de volume soit atteint, puis utiliser l'itinéraire suivant est utilisé

```
config system settings
    set v4-ecmp-mode [source-ip-based | weight-based | usage-based |
    source-dest-ip-based]
end
```



Une formation
Alphorm.com

Policy-Based Routes

Correspondance plus granulaire que les itinéraires statiques:

- Protocole
- Adresse source
- Port source
- Ports de destination
- Types de bits de service (ToS)

Avoir la priorité sur la table de routage

Maintenu dans une table de routage distincte

Actions:

FortiGate transfère, en utilisant l'interface sortante spécifiée, pour la passerelle spécifiée

Arrête le routage des stratégies et utilise la table de routage à la place



Policy-Based Routes

Source IP (default) : Les sessions de la même adresse IP source utilisent la même route

Source-destination IP : Les sessions avec la même source et la même paire IP de destination utilisent la même route

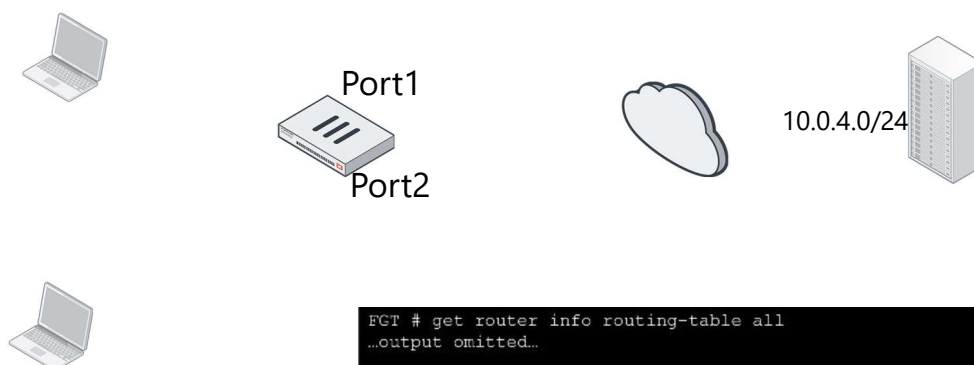
Weighted : Les sessions sont distribuées en fonction du poids de l'interface

Usage (Spillover) : Un itinéraire est utilisé jusqu'à ce que le seuil de volume soit atteint, puis utiliser l'itinéraire suivant est utilisé

Une formation
Alphorm.com



Exemple



```
FGT # get router info routing-table all
...output omitted...

S*   0.0.0.0/0 [10/0] via 10.0.1.254, wan1
S    10.0.4.0/24 [10/0] via 10.0.3.254, port1, [5/0]
      [10/0] via 10.200.3.254, port2, [5/0]
C    10.200.3.0/24 is directly connected, port2
C    10.0.1.0/24 is directly connected, wan1
C    10.0.3.0/24 is directly connected, port1
```

Une formation
Alphorm.com



RFP

Protège contre les attaques de usurpation IP
L'adresse IP source est vérifiée par rapport à la table de routage pour le chemin inverse
Le RPF n'est effectué que sur:

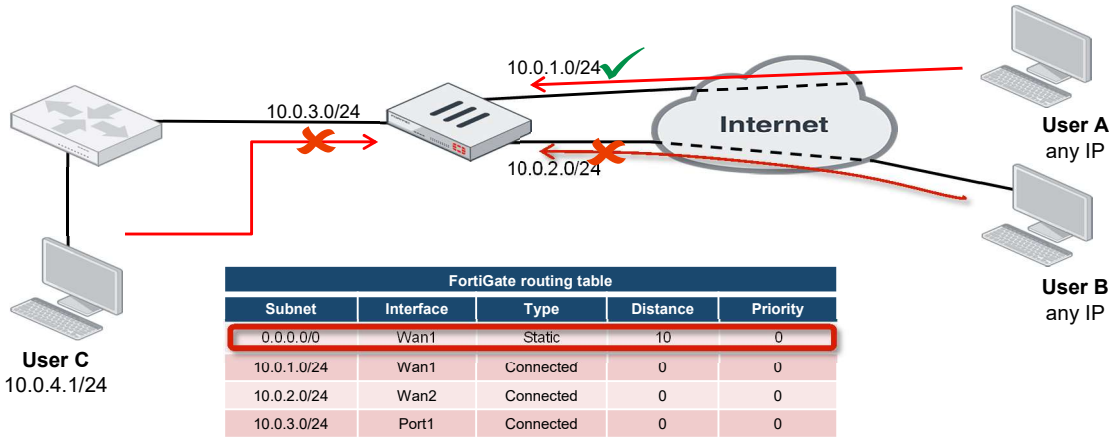
- Le premier paquet dans la session, pas sur la réponse
- Le paquet suivant dans la direction d'origine après un changement d'itinéraire, pas sur la réponse

Deux modes:
Loose
Strict

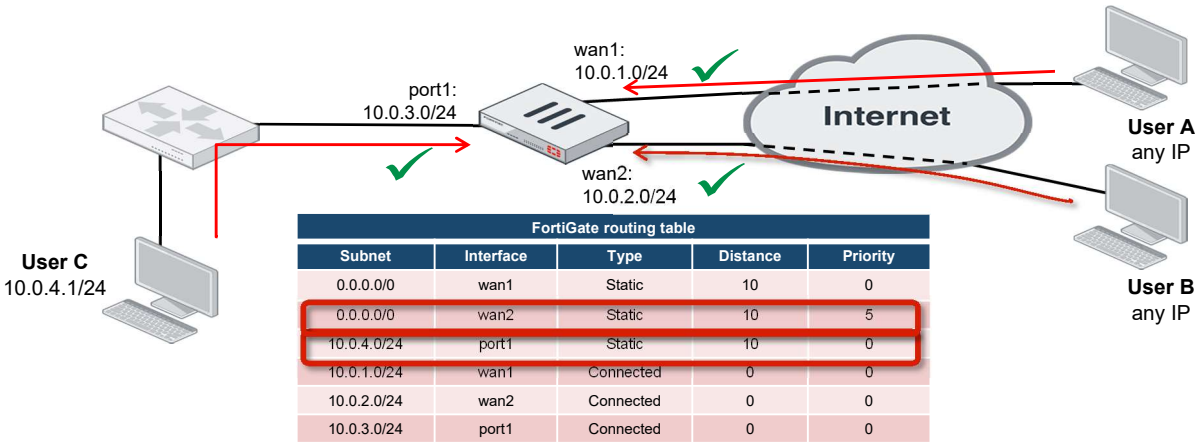


Une formation
Alphorm.com

Exemple



Solution





Une formation
Alphorm.com

Surveiller et analyser le routage



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Health Monitor
Routage actif et Routage inactif
Policy Routes et ISDB Routes
Capture des paquets
LAB



Une formation
Alphorm.com

Health Monitor

Mécanisme pour détecter quand un routeur le long du chemin est injoignable : Sonde périodiquement un serveur au-delà de la passerelle

Si FortiGate ne reçoit pas de réponses dans le seuil de basculement, tous les itinéraires statiques à l'aide de la passerelle sont supprimés de la table de routage

Si les itinéraires de secours sont disponibles, FortiGate s'activent et les utilise à la place

```
# config system link-monitor
# edit <name>
# set srcintf <interface>
# set server <server ip>
# set gateway-ip <gateway ip>
# set protocol [ ping | tcp-echo | udp-echo | twamp | http ]
# set update-static-route [ enable | disable ]
# next
# end
```



Une formation
Alphorm.com

Routage actif et inactif

- get router info routing-table database

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

0 - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

> - selected route, * - FIB route, p - stale info

```
S 0.0.0.0/0 [20/0] via 10.200.2.254, port2
S *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
C *> 10.0.1.0/24 is directly connected, port3
C *> 10.200.1.0/24 is directly connected, port1
C *> 10.200.2.0/24 is directly connected, port2
C *> 192.168.2.0/24 is directly connected, port8
```

Route inactive

Routes actives



Policy Routes et ISDB Routes

```
# diagnose firewall proute list
list route policy info(vf=root):

id=1 flags=0x0 tos=0x00 tos_mask=0x00 protocol=6 sport=1:65535 iif=9
dport=443 oif=11 gwy=100.64.1.254
destination(1): 0.0.0.0-255.255.255.255
source wildcard(1): 10.0.1.10/255.255.255.255

id=4261412866 static_route=2 flags=0x0 tos=0x00 tos_mask=0x00 protocol=0
sport=0:0 iif=0 dport=1-65535 oif=11 gwy=100.64.1.254
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Apple-App.Store(196723)
```

Une formation
Alphorm.com



Capture des paquets

Peut être utilisée pour vérifier si un paquet arrive à la FortiGate, et quelle interface est utilisée pour le Router

```
#diagnose sniffer packet <interface>
'<filter>' [verbosity]
```

<interface> peut être any

<filter> suit le format **tcpdump**

<level> indique la quantité d'informations à capturer

Une formation
Alphorm.com



Capture des paquets

Level	IP headers	IP payload	Ethernet headers	Interface names
1	√			
2	√	√		
3	√	√	√	
4	√			√
5	√	√		√
6	√	√	√	√

Les niveaux les plus courants sont :

4 : pour vérifier comment le trafic est acheminé ou si FortiGate abandonne des paquets

3, 6 : pour exporter la sortie vers un fichier de capture de paquets (PCAP) (à l'aide d'un script perl) qui peut être ouvert avec un analyseur de paquets





Une formation
Alphorm
com

Comprendre le SD-WAN



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

SD-WAN ?

Cas d'usage de SD-WAN

Méthodes de load balancing

SD-WAN dans la table de routage

LAB



Une formation
Alphorm.com

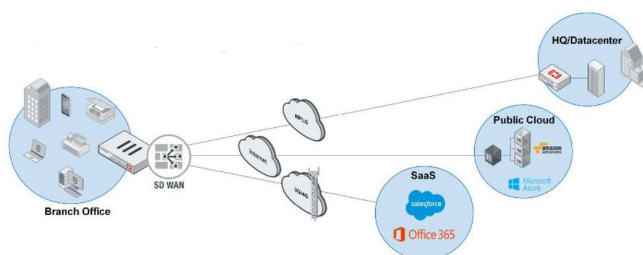
SD-WAN ?

Interface virtuelle composée d'un groupe d'interfaces membres
pouvant être connectées à différents types de liaisons
Permet une utilisation WAN efficace avec divers algorithmes
d'équilibrage de charge

Prend en charge la mesure de qualité de liaison

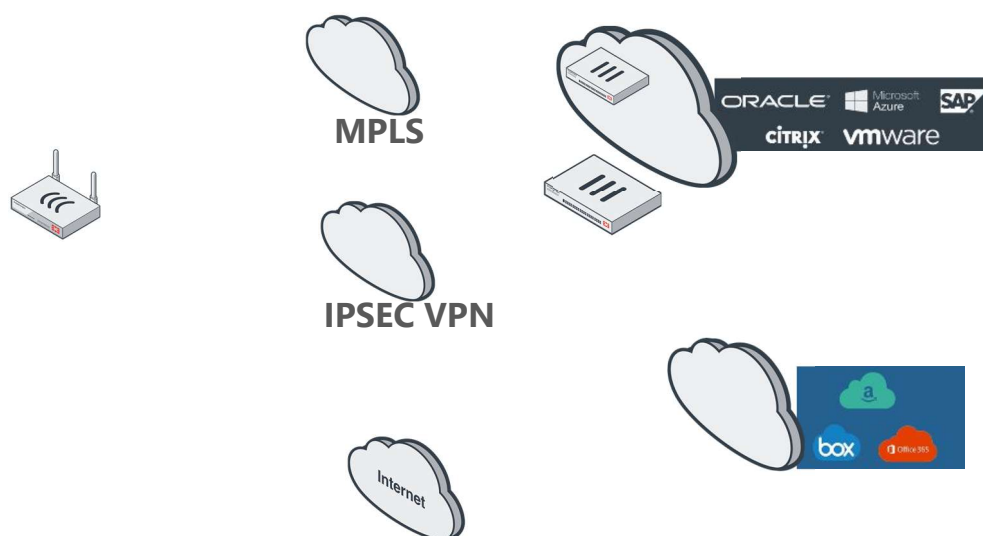
Sélection de liens dynamiques en fonction de la qualité des liens

Assure une disponibilité élevée des applications critiques pour les
entreprises



Une formation
Alphorm.com

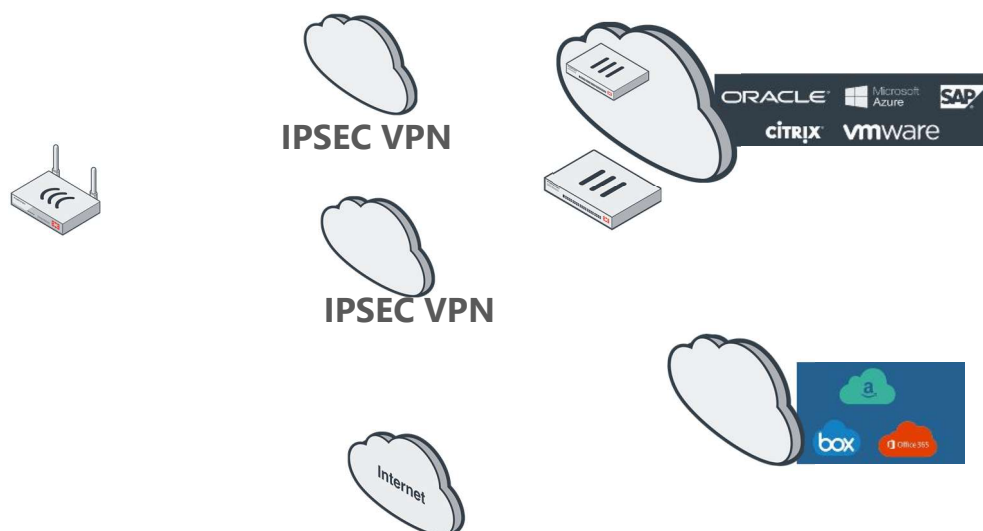
Cas d'usage de SD-WAN





Une formation
Alphorm.com

Cas d'usage de SD-WAN



Une formation
Alphorm.com

Méthodes de load balancing

Source IP (default)

Les sessions de la même adresse IP source utilisent la même interface

Source-destination IP

Les sessions avec la même source et la même paire IP de destination utilisent la même interface

Spillover

Utilisez l'interface jusqu'à ce que le seuil soit atteint; Ensuite, utilisez la prochaine interface.

Sessions

Le nombre de sessions distribuées est déterminé par les pondérations d'interface

Volume

Les sessions sont distribuées de tel sorte que le volume de trafic soit distribué par les pondérations d'interface.



La table de routage

```
# get router info routing-table all
...omitted output...
S*      0.0.0.0/0 [1/0] via 10.200.2.254, port2
          [1/0] via 10.200.1.254, port1
C       10.200.2.0/24 is directly connected, port2
C       10.200.1.0/24 is directly connected, port1
```





Une formation
Alphorm.com

Découvrir SD-WAN règles et performance



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Performance SLA-LINK
Mesures de qualité de liaison
Configuration CLI
Règles de la SD-WAN
LAB



Une formation
Alphorm.com

Performance SLA-LINK

La vérification d'État est renommée SLA de performance

Vous pouvez utiliser deux serveurs pour tester la qualité d'un lien

Vous pouvez spécifier les membres SD-WAN que ce SLA applique à l'interface

Le moniteur de santé de lien est un moyen pour détecter quand un routeur le long du chemin est arrêté ou dégradé



Une formation
Alphorm.com

Mesures de qualité de liaison

Le SLA de performance mesure la qualité des liens connectés à l'interface membre participant à un contrat SLA de performance

Trois critères différents sont utilisés pour cette mesure : **latence**, **gigue** et **perte de paquets**

Les critères affichés sont basés sur les réponses du serveur que le SLA de performance utilisé

Configuration CLI

```
# config system virtual-wan-link
# set status enable
# config health-check
# edit <name>
# set protocol [ ping | tcp-echo | udp-echo | http | twamp ]
# set threshold-warning-packetloss <percentage>
# set threshold-alert-packetloss <percentage>
# set threshold-warning-latency <ms>
# set threshold-alert-latency <ms>
# set threshold-warning-jitter <ms>
# set threshold-alert-jitter <ms>
# config sla
# edit <id>
# set link-cost-factor [latency | jitter | packet-loss]
# set latency-threshold <integer> (0 - 10000000, default = 5)
# set jitter-threshold <integer> (0 - 10000000, default = 5)
# set packetloss-threshold <integer> (0 - 100, default = 0)
# next
```



Règles de la SD-WAN

Acheminez le trafic à travers les interfaces membres avec la meilleure qualité de lien :

Qualité de liaison mesurée en fonction de la latence, de la gigue ou du pourcentage de perte de paquets

Les règles peuvent correspondre au trafic en fonction de :

Adresse IP source, adresse IP de destination ou, numéro de PortObjet de l'adresse de base de données des services Internet (ISDB) Les utilisateurs ou groupes d'utilisateurs Type de service (ToS)



Une formation
Alphorm
com



Une formation
Alphorm
com

Analyser le SD-WAN



Mohamed Anass EDDIK



Plan

Surveiller la SD-WAN
Surveiller l'état des liens SD-WAN
LAB

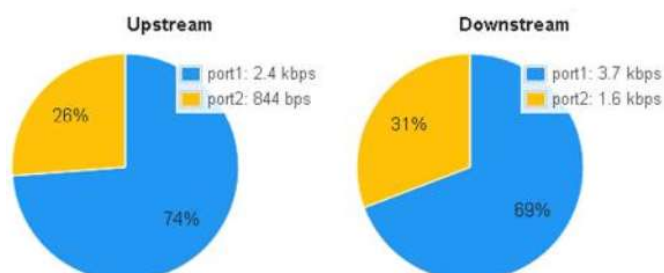
Une formation
Alphorm.com



Surveiller la SD-WAN

Surveiller l'utilisation en temps réel de la SD-WAN
Afficher la distribution du trafic SD-WAN par bande
passante ou volume

Une formation
Alphorm.com





SD-WAN link status monitor

La surveillance de la qualité des liaisons des interfaces des membres du SD-WAN est une bonne pratique

Tout problème prolongé avec perte de paquets et latence doit être étudié afin de s'assurer que le trafic réseau ne présente pas de panne ou de dégradation des performances

Netflix	http://www.netflix.com/	port1 port2	port1: 0.00 % port2: 0.00 %	port1: 41.35 ms port2: 32.70 ms	port1: 306.34 ms port2: 61.04 ms	5	5
Skype	http://www.skype.com/	port1 port2	port1: 0.00 % port2: 0.00 %	port1: 41.35 ms port2: 32.70 ms	port1: 306.34 ms port2: 61.04 ms	5	5





Une formation
Alphorm
com

Comprendre les différents concepts du VDOM



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

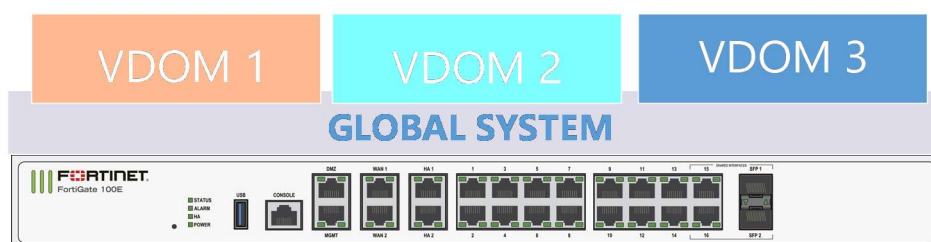
Les différents concepts des VDOMS
Administration VDOM



Une formation
Alphorm.com

VDOM

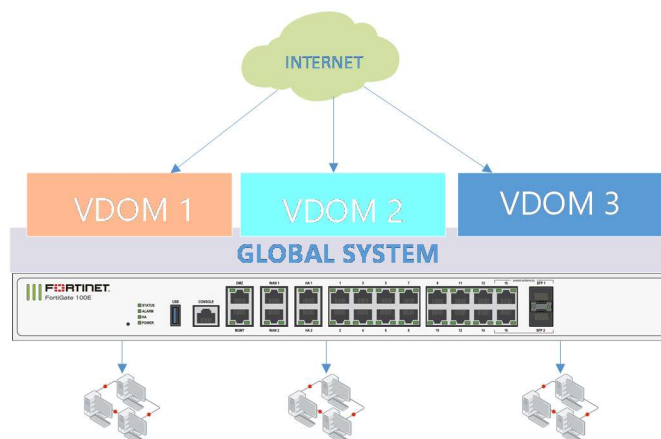
Les VDOM divisent un FortiGate physique en plusieurs périphériques virtuels
Les paquets sont configurés pour le même VDOM
Par défaut, FortiGate prend en charge jusqu'à 10 VDOM



Une formation
Alphorm.com

VDOM indépendant

Plusieurs VDOM sont complètement séparés
Il n'y a pas de communication entre les VDOM
Chaque VDOM a son propre interface physique à Internet

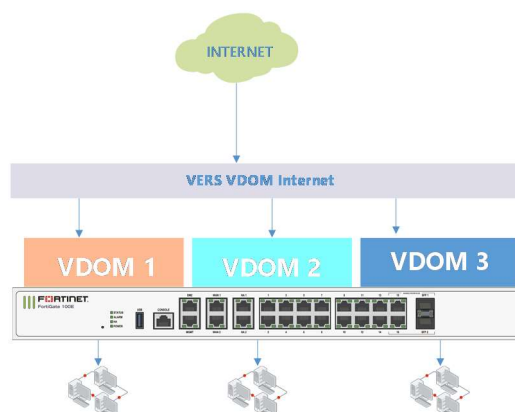




Une formation
Alphorm.com

Routage via un seul VDOM

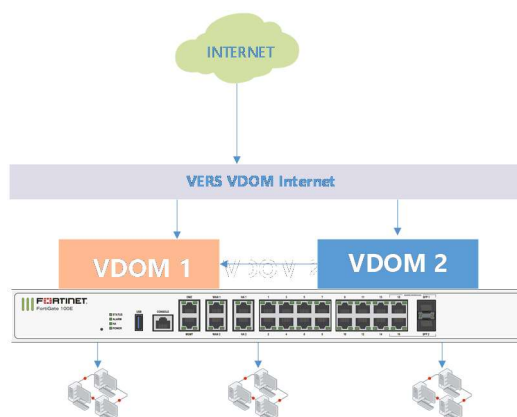
Le trafic destiné à l'Internet sera toujours acheminé par le VDOM désigné
Seul le «vers VDOM Internet» est physiquement connecté à Internet



Une formation
Alphorm.com

VDOM maillé

Les VDOM se connectent à d'autres réseaux virtuels via des liens inter-virtuels
Seul le trafic Internet doit passer par le «vers VDOM Internet»

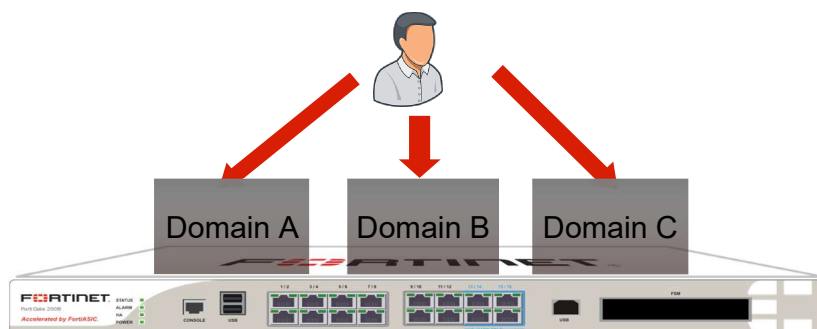




Une formation
Alphorm.com

Administration VDOM

Juste le compte admin ou bien un compte avec les droits de **super_admin** ont le droit de voir tous les VDOMs et les configurer

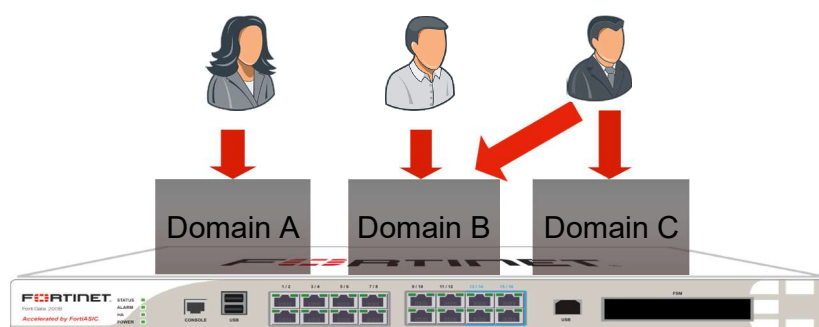


Une formation
Alphorm.com

Administration VDOM

Les autres administrateurs peuvent accéder uniquement à leurs VDOM attribués

Ils ne peuvent pas accéder au global settings





Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer les VDOMS



Mohamed Anass EDDIK



Plan

Activation et création de VDOM Paramètres VDOM

Une formation
Alphorm.com



Activation et création

Pour activer les VDOMs

```
#config system global
    set vdom-admin enable
end
```

Après activation des VDOMs.

Le seul VDOM par défaut c'est le Root

Pour créer un VDOM

```
#config vdom
Edit <vdom>
    config system settings
        set opmode [nat | transparent]
    end
```

Une formation
Alphorm.com



Une formation
Alphorm.com

Paramètres VDOM

Affectent toutes les VDOM configurées :

- Hostname
- Paramètres HA
- Paramètres FortiGuard
- Heure système
- Comptes administratifs



Une formation
Alphorm.com

Paramètres VDOM

Configuré séparément, dans chaque VDOM:

- Mode de fonctionnement (transparent, NAT/route)
- Mode d'inspection (basé sur le flux, basé sur Proxy)
- Itinéraires et interfaces réseau
- Stratégies de pare-feu
- Profils de sécurité





Paramètres VDOM

Réglage des paramètres globaux :

```
#config global
(global) #
```

Accès par paramètres VDOM:

```
#config vdom
(vdom) # edit <vdom-name>
(vdom-name) #
```

Exécution de commandes globales et par VDOM à partir de n'importe quel contexte:

```
#sudo [global | vdom-name] [diagnose | execute | show | get]
```

Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm
com

Paramétrer l'inter-VDOM



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Liens inter-VDOM

Accélération du lien inter-VDOM



Liens inter-VDOM

Peut connecter différent VDOM

Le soutien varie selon les modes de fonctionnement des VDOM

NAT à NAT

NAT à transparent/transparent à NAT

Transparent-transparent (pas de couche 3; boucles potentielles de la couche 2)



Une formation
Alphorm.com



Accélération du lien

Les appareils FortiGate avec les processeurs NP4 ou NP6 incluent des liens inter-VDOM qui peuvent être utilisés pour accélérer le trafic de liaisons inter-VDOM

Pour un appareil FortiGate sans processeurs NP4 ou NP6, il existe deux liaisons inter-VDOM accélérées, chacune avec deux interfaces :

Npu0_vlink

Npu1_vlink

Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir les VLANs et le mode transparent



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

VLANs

VLAN Tags

Mode de fonctionnement NAT

Mode de fonctionnement transparent

Fortigate avec un domaine de transfert

Fortigate avec multiple domaines de transfert

LAB



Une formation
Alphorm.com

VLANs

Les VLANs partagent logiquement votre réseau physique de couche 2 en segments plus petits
Les VLANs tags sont ajoutées aux trames pour identifier leurs segments réseaux





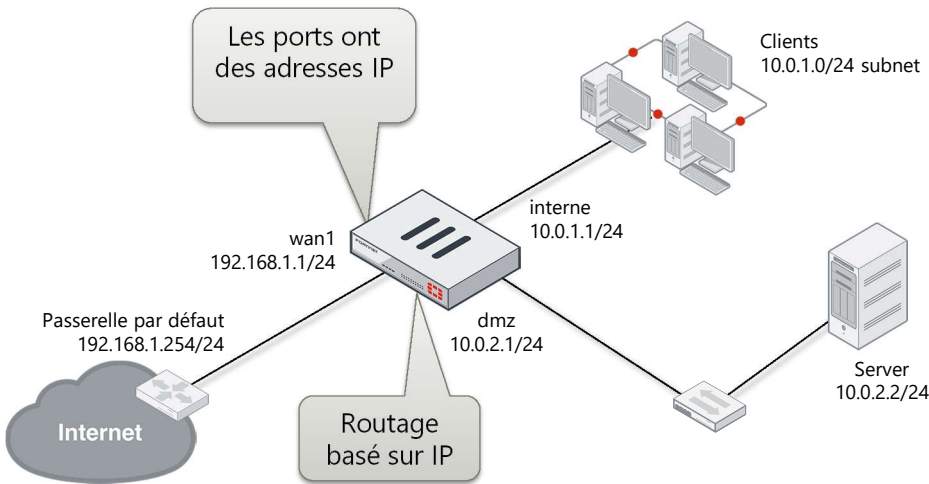
VLAN Tags

Les VLANs tags ajoutent une extension de 4 octets à une trame Ethernet
Les appareils de la couche 2 peuvent ajouter ou supprimer des tags
Les appareils de la couche 3 peuvent réécrire les tags avant le routage

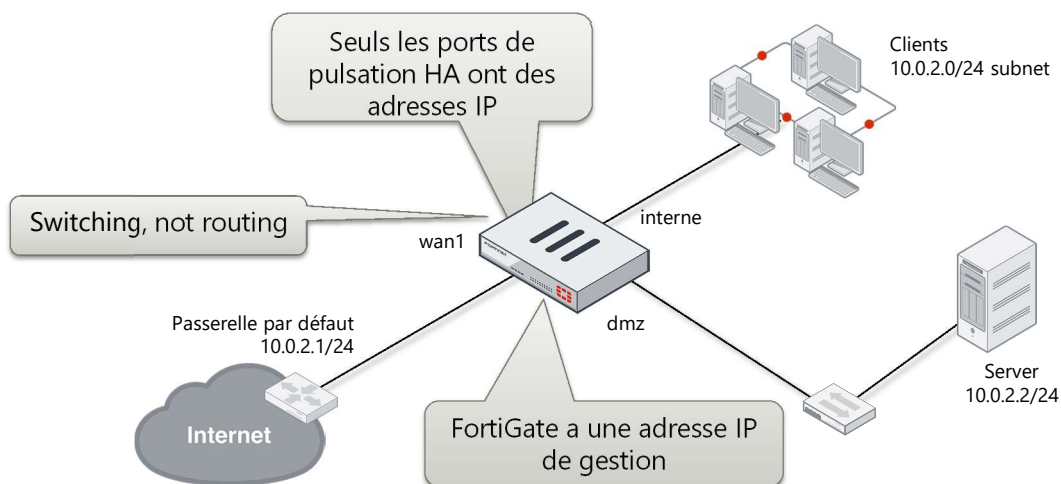


Une formation
Alphorm.com

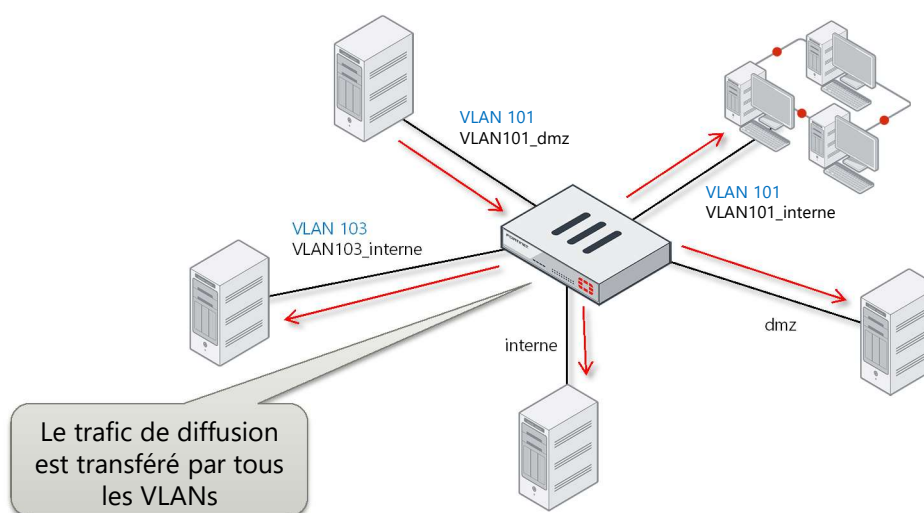
Mode de fonctionnement NAT



Mode de fonctionnement transparent

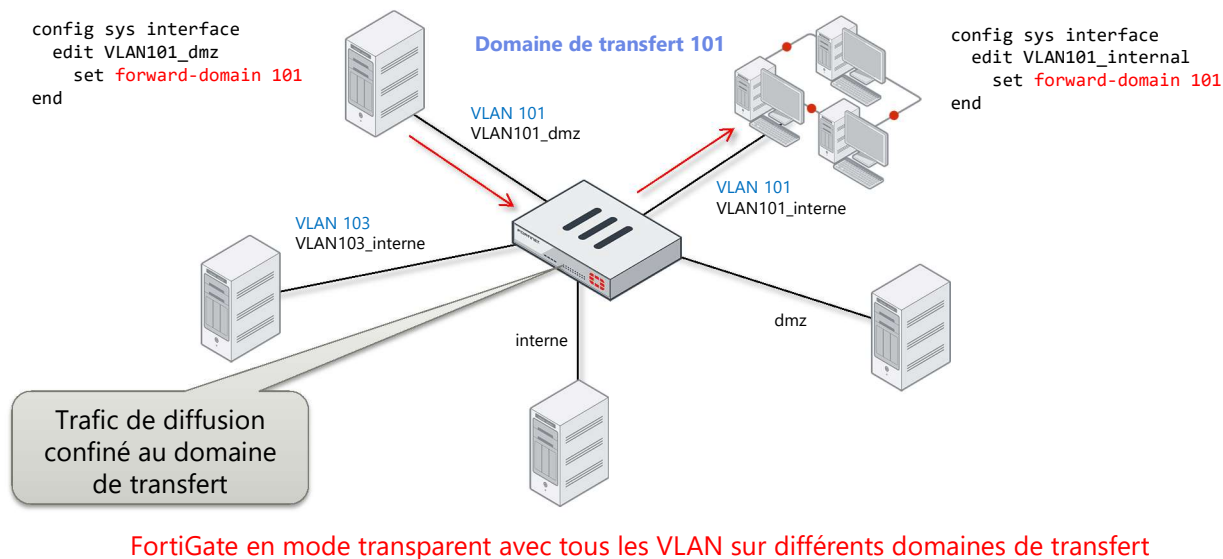


Un domaine de transfert



FortiGate en mode transparent avec tous les VLANs sur le même domaine de transfert

Multiple domaines de transfert





Une formation
Alphorm.com

Configurer le Virtual WirePairing



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Virtual Wire Pair

Virtual Wire Pairing et le mode transparent

Virtual Wire-Pairing et le mode NAT
LAB

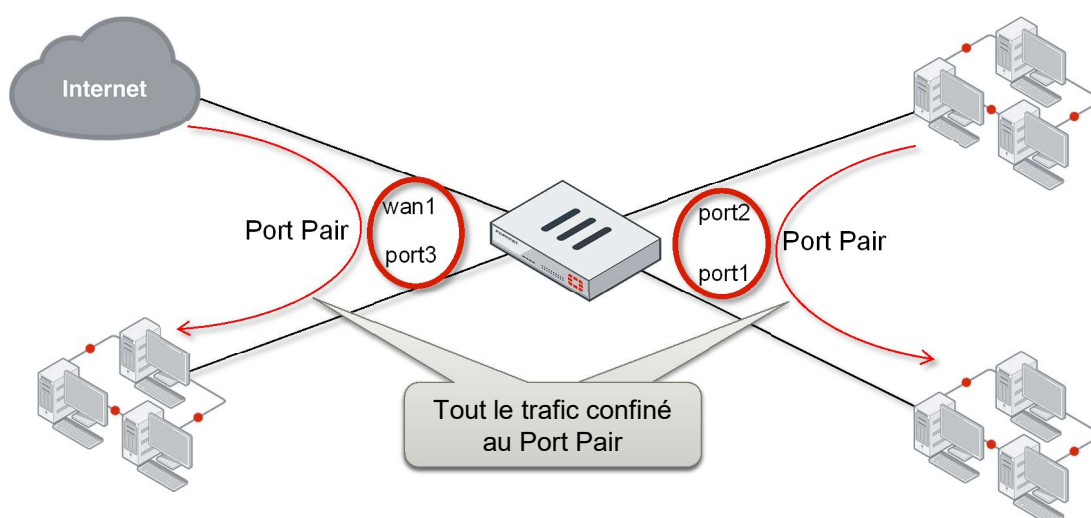


Virtual Wire Pair

Relie logiquement deux interfaces physiques
Habituellement une interface interne et une externe
Le trafic est capturé entre ces interfaces
Le trafic entrant vers une interface est toujours
expédié par l'autre interface
Aucun autre trafic ne peut entrer ou laisser une paire
de ports

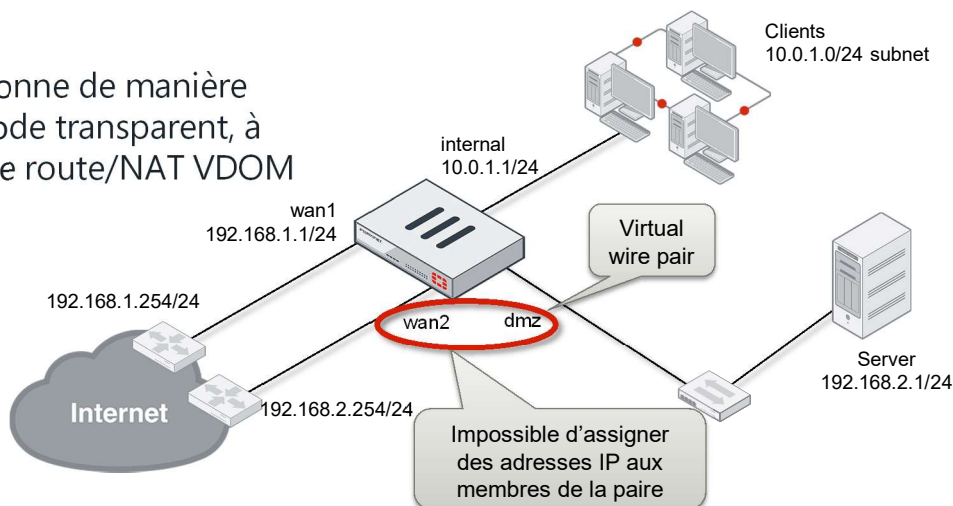
Une formation
Alphorm.com

Le mode transparent



Virtual wire Pairing et le mode NAT

La paire fonctionne de manière
similaire au mode transparent, à
l'intérieur d'une route/NAT VDOM



Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm
com

Paramétrer le commutateur logiciel et le Spanning Three



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Commutateur logiciel
Spanning Three
LAB



Commutateur Logiciel

Regroupe plusieurs interfaces dans une seule interface de commutation virtuelle

Uniquement pris en charge en mode NAT VDOM

Agit comme un commutateur de la couche matérielle 2

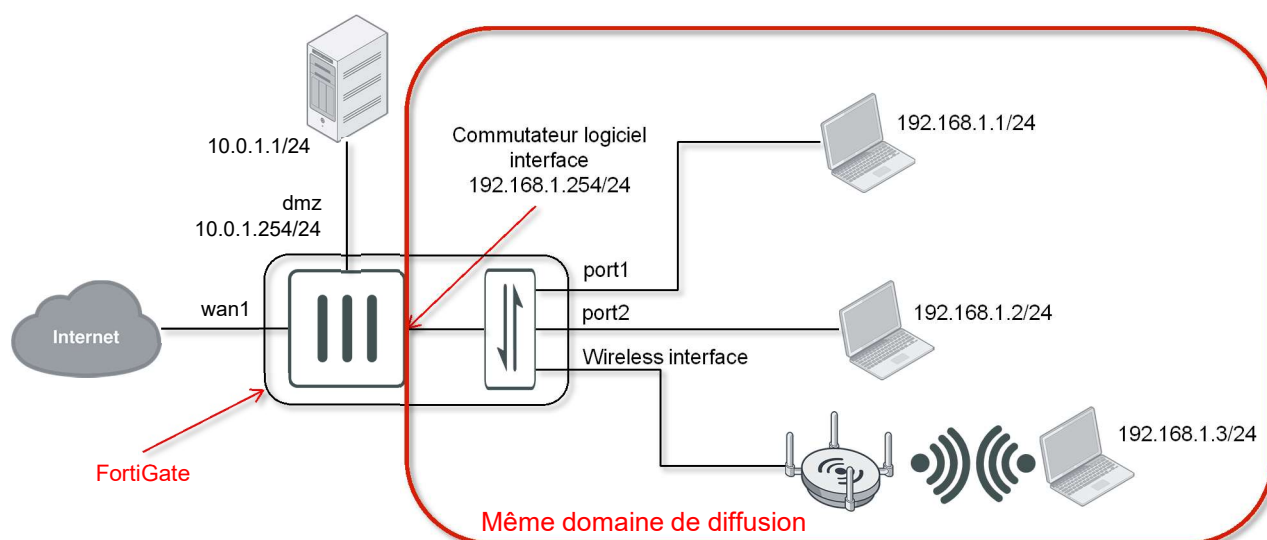
Les interfaces :

Partagent la même adresse IP

Appartiennent au même domaine de diffusion

Une formation
Alphorm.com

Commutateur Logiciel





Une formation
Alphorm.com

Spanning Three

Les commutateurs STP apprennent les uns sur les autres et élisent la racine en échangeant des unités de données de protocole de pont (BPDU)

FortiGate peut transférer, bloquer (par défaut) ou participer
Crée automatiquement une topologie efficace et sans boucle pour les liens redondants

Structure arborescente couvrant tous les commutateurs

Si une branche devient inaccessible, les commutateurs participants reconfigureraient la topologie de lien pour permettre à une branche différente



Une formation
Alphorm.com

Configuration STP

Pour configurer FortiGate pour participer à STP :

```
config system stp
    set config-revision <revision number>
    set forward-delay <seconds>
    set hello-time <seconds>
    set max-age <seconds>
    set region-name <region>
    set status [enable | disable]
    set switch-priority <priority>
end
```

Uniquement pris en charge sur les modèles avec interfaces de commutation



STP Forwarding

Configurez chaque interface en bloc (par défaut) ou en STP Forwarding :

```
config system interface
  edit <interface name>
    set stpforward [enable | disable]
  end
```

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm
com

Comprendre la topologie



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

IKE and IPSec review

Site-to-site

Hub-and-Spoke

Maillage complet et partiel

Auto Discover VPN(ADVPN)

LAB



IKE and IPSEC review

Suite de protocoles pour sécuriser les communications IP

Authentifie et/ou crypte les paquets :

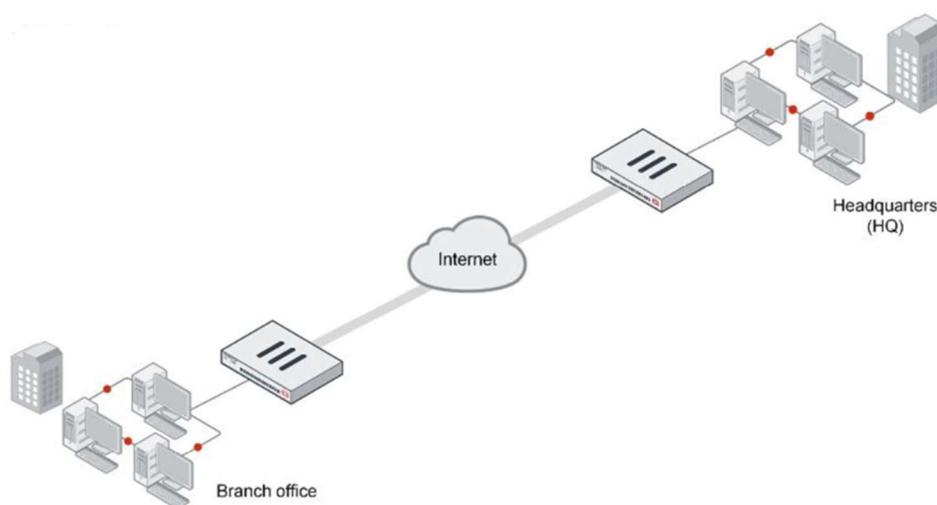
- Échange de clés Internet (IKE)
- Charge utile de sécurité d'encapsulation (ESP)
- Fournit à la fois l'intégrité des données et le cryptage
- En-tête d'authentification (AH)
- Fournit uniquement l'intégrité des données
- Non utilisé par FortiGate

Pour le Traversal NAT, l'ESP est encapsulé par UDP

Une formation
Alphorm.com

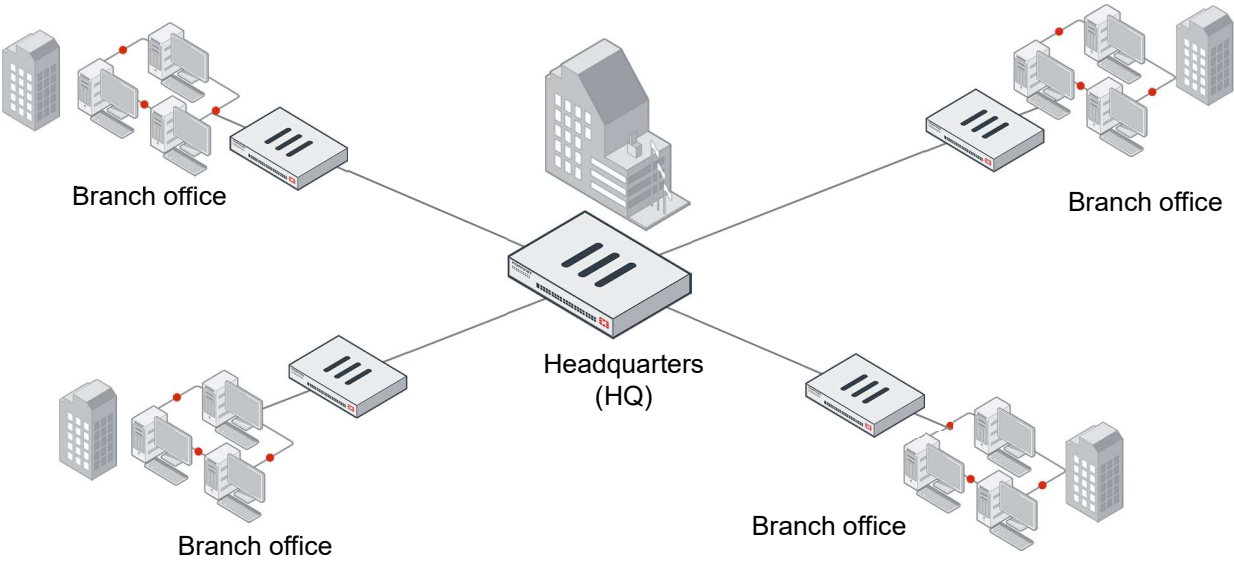


Site-to-site

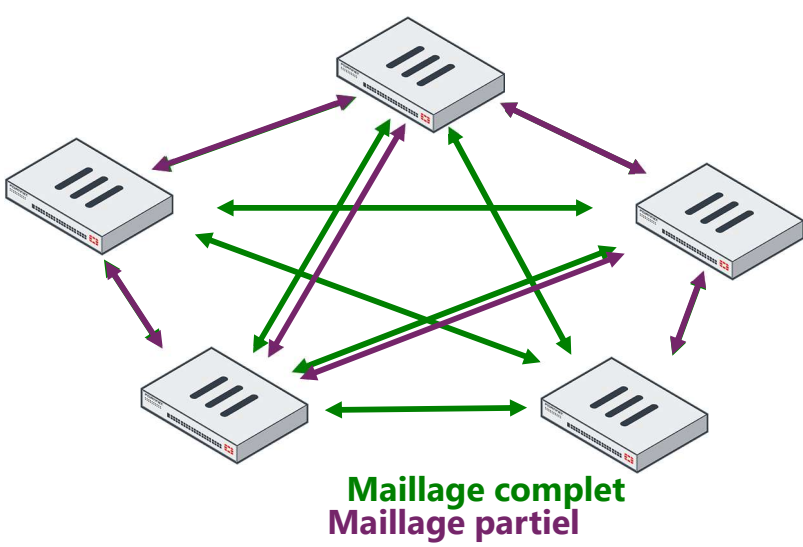


Une formation
Alphorm.com

Hub-and-Spoke



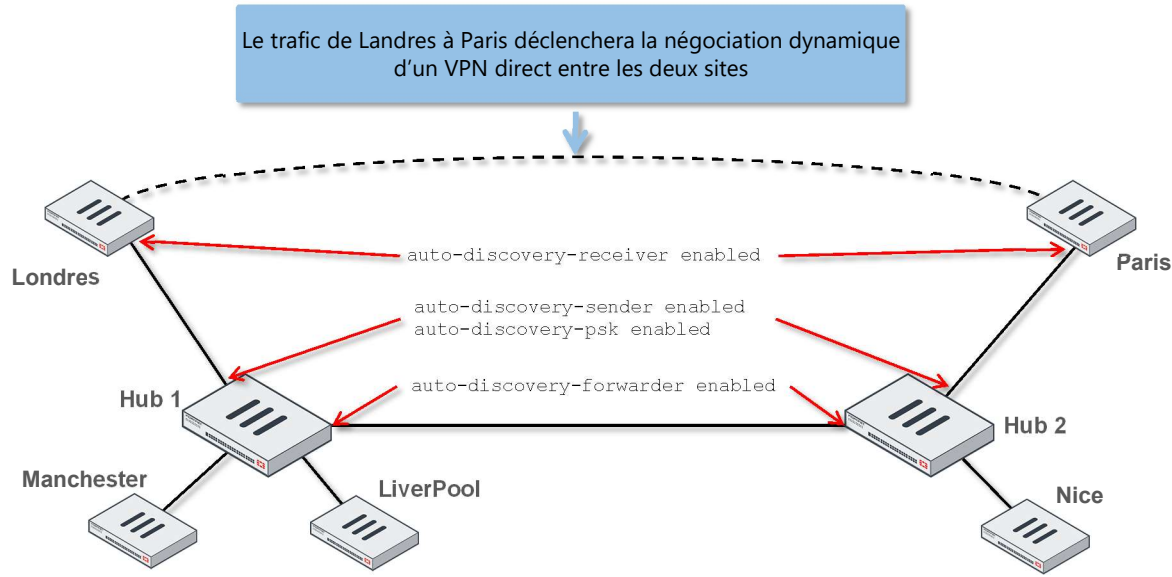
Maillage complet et partiel



Comparaison des topologies

Hub-and-Spoke	Maillage partiel	Maillage complet
Configuration facile	Configur modérée	Configuration complexe
Quelques tunnels	Tunnels moyens	De nombreux tunnels
Bande passante centrale élevée	Bande passante moyenne dans les sites hub	Faible bande passante
Pas tolérant aux pannes	Une certaine tolérance de panne	Tolérant aux pannes
Faible configuration requise (moyenne); Haut pour le centre	Exigences moyennes du système	Exigences système élevées
Extensible	Peu évolutif	Difficile à redimensionner
Pas de communication directe entre les rayons	Communication directe entre certains sites	Communication directe entre tous les sites

ADVPN





Une formation
Alphorm
com



Une formation
Alphorm
com

Déployer du site-to-site VPN IPSec



Mohamed Anass EDDIK



Plan

Policy Based VS Route Based
VPN redondant
LAB

Une formation
Alphorm.com

Policy Based VS Route Based

Feature	Policy-based	Route-based
FortiGate operation mode	NAT and transparent	Only NAT
L2TP-over-IPsec	Yes	Yes
GRE-over-IPsec	No	Yes
Routing protocols	No	Yes
Number of policies per VPN	One policy controls both traffic directions	Two policies (usually)—one for each direction

Routed-based (interface-based)

Le trafic doit être acheminé vers l'interface de réseau virtuel IPsec
Généralement, deux stratégies de pare-feu avec l'ACTION définie sur ACCEPT sont requises (une par direction)

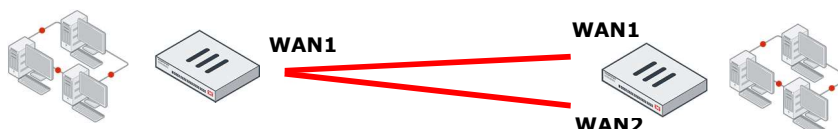
Policy-based (tunnel-based)

Une stratégie de pare-feu avec l'ACTION définie sur IPsec est requise

VPN redondant

Uniquement entièrement pris en charge par les VPN basés sur les itinéraires
Si le tunnel VPN principal échoue, FortiGate réachemine le trafic via le VPN de sauvegarde

Partiellement redondant : un pair a deux connexions



Entièrement redondant : les deux pairs ont deux connexions

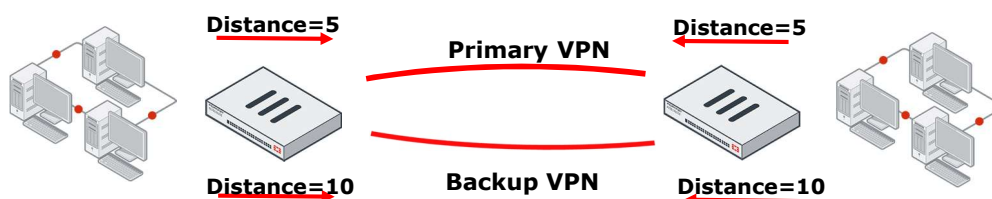


VPN redondant

Ajouter une configuration de phase 1 pour chaque tunnel. La détection des pairs morts (DPD) doit être activée aux deux extrémités

Ajouter au moins une définition de phase 2 pour chaque phase 1

Ajouter un itinéraire statique pour chaque chemin. Utiliser la distance ou la priorité pour sélectionner le principal sur les itinéraires de sauvegarde. Vous pouvez également utiliser le routage dynamique ou les stratégies de pare-feu pour chaque interface IPSec





Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer le FSSO avec l'AD



Mohamed Anass EDDIK



Plan

Flux en mode agent DC

Flux du mode d'interrogation basé sur
l'agent collecteur

Flux de mode d'interrogation sans agent

Comparaison des modes

LAB

Une formation
Alphorm.com

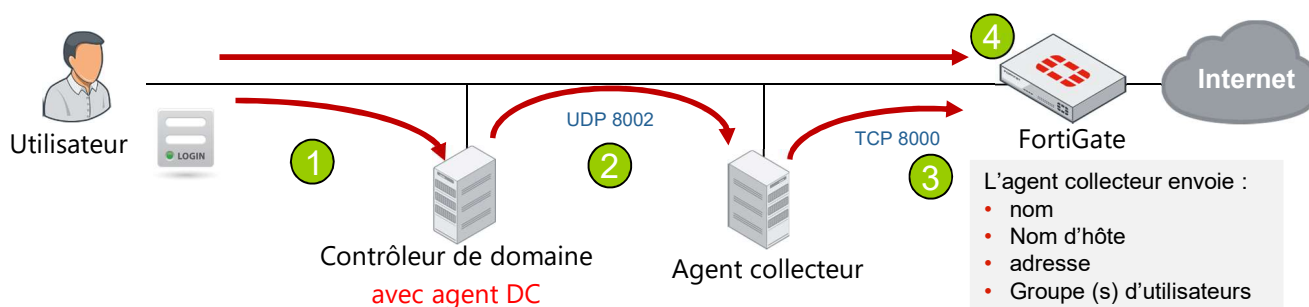
Flux en mode agent DC

L'utilisateur s'authentifie contre Windows DC

L'agent DC voit l'événement de connexion et le transmet à l'agent collecteur

L'agent de collecte reçoit l'événement des agents de DC, et le transmet à FortiGate

FortiGate connaît l'utilisateur, en fonction de son adresse IP. L'utilisateur n'a pas besoin de s'authentifier



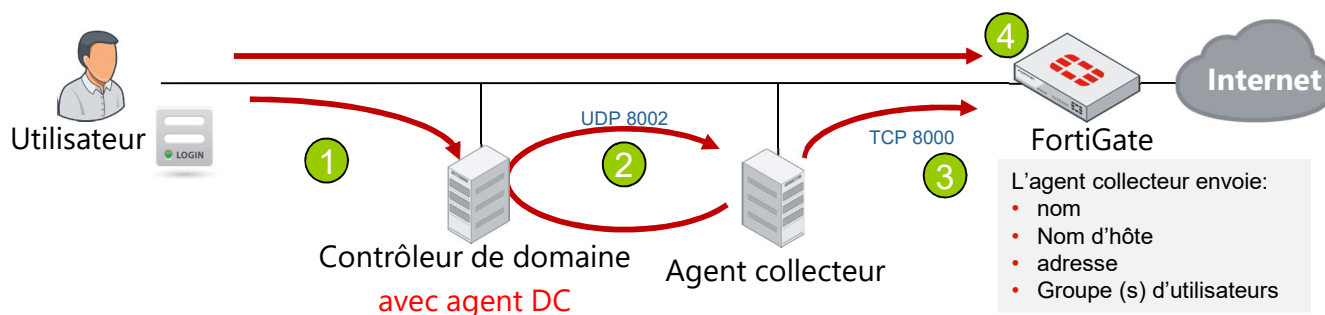
Mode d'interrogation basé sur l'agent collecteur

L'utilisateur s'authentifie avec le contrôleur de domaine (DC)

Les agents collecteurs interrogent fréquemment les contrôleurs de session pour obtenir des événements de connexion utilisateur

L'agent collecteur transfère les ouvertures de session à FortiGate

L'utilisateur n'a pas besoin de s'authentifier



Options du mode d'interrogation

NetAPI

Interroge la fonction NetSessionEnum sur Windows toutes les 9 secondes ou moins *

Table de session d'authentification dans la RAM

Récupérer les sessions de connexion y compris les événements de connexion de DC

Plus rapide, mais...

Si le DC a une charge système lourde, il peut manquer quelques événements de connexion

WinSecLog

Interroge tous les événements de sécurité sur DC toutes les 10 secs ou plus*

Latence du journal si le réseau est de grande taille ou que le système est lent

Nécessite des liaisons réseau rapides

Plus lent, mais...

Voit tous les événements de connexion

Analyse uniquement les eventIDs connus par l'agent collecteur

WMI

Le DC renvoie tous les événements de connexion demandés - 3 secs *

Lit les journaux d'événements sélectionnés

Améliore l'utilisation de la bande passante WinSec

Réduit la charge réseau entre l'agent collecteur et le DC

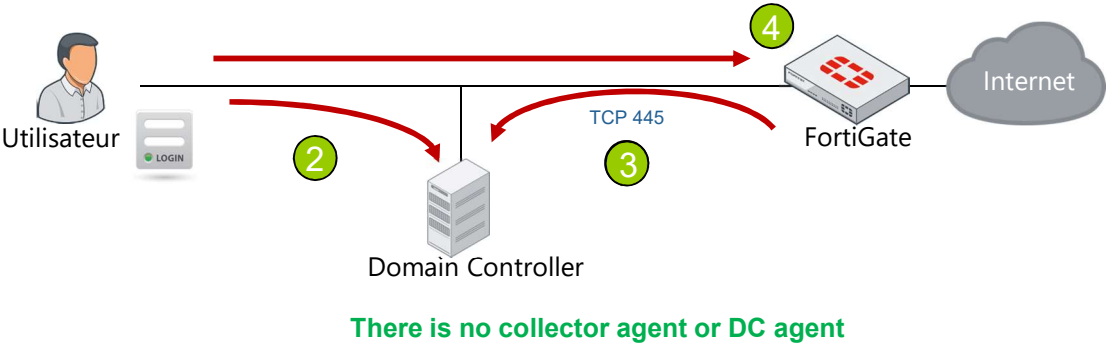
Mode d'interrogation sans agent

FortiGate interroge fréquemment les contrôleurs de session pour obtenir des événements de connexion utilisateur

L'utilisateur s'authentifie avec le contrôleur de domaine

FortiGate découvrira l'événement de connexion dans le prochain sondage

L'utilisateur n'a pas besoin de s'authentifier



Comparaison des modes

	Mode agent DC	Mode interrogation
Installation	Complexe — plusieurs installations (une par DC). Redémarrage requis	Simple — Pas ou une installation. Pas de redémarrage requis
Agent DC	Requis	Non requis
Ressources	Actions avec des agents DC	Dispose de ressources propres
Evolutivité	Forte	Faible
Redondance	Oui	Non
Niveau de confiance	Capture toutes les ouvertures	Peut manquer une connexion (NetAPI), ou avoir un délai (WinSecLog)



Une formation
Alphorm
com



Une formation
Alphorm
com

Découvrir l'authentification NTLM



Mohamed Anass EDDIK

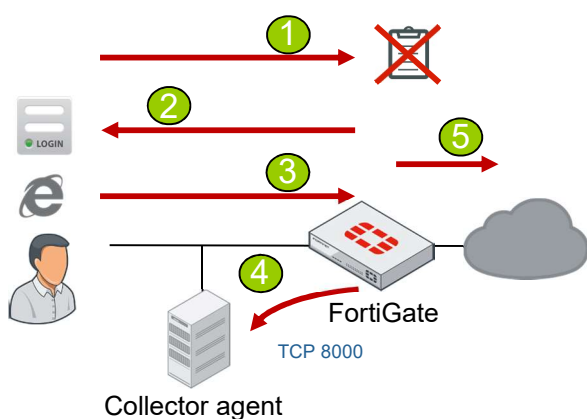


Plan

Domaine simple
Domaine multiple
LAB

Une formation
Alphorm.com

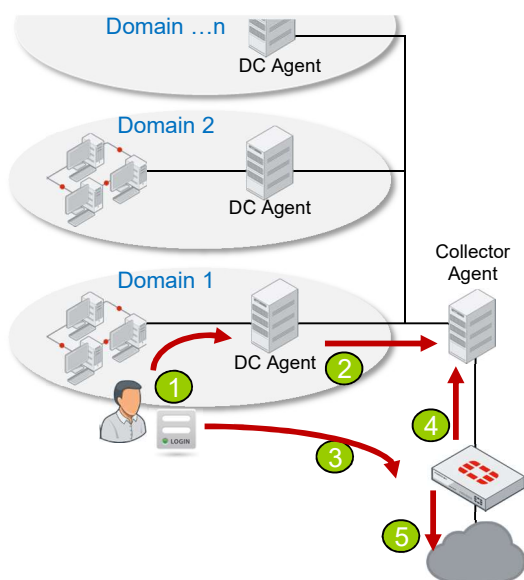
Domaine simple



1. L'utilisateur tente d'accéder à Internet avec le navigateur
 - Son adresse IP n'est pas dans la liste active des utilisateurs FSSO
2. FortiGate demande des informations d'identification
 - domaine/nom d'utilisateur et mot de passe

Le navigateur de l'utilisateur envoie des informations à FortiGate
3. FortiGate vérifie les informations d'identification et l'appartenance au groupe avec l'agent collecteur
4. Accès accordé en fonction de l'appartenance au groupe

Domaine multiple



➤ NTLM requiert une relation d'approbation entre les domaines :

- Si les domaines sont dans une forêt AD, vous avez seulement besoin d'un agent de contrôleur de domaine global.
- Si les domaines ne sont pas dans une forêt AD, vous devez installer un agent DC sur chaque domaine (à DC)

➤ Flux d'authentification NTLM à plusieurs domaines :

- Les utilisateurs se connectent à leur DC local
- Les agents DC envoient les événements de connexion des utilisateurs à l'agent collecteur
- Les utilisateurs tentent d'accéder à Internet
- FortiGate vérifie l'agent collecteur pour les informations de connexion.
- Accès accordé à Internet





Une formation
Alphorm.com

Paramétrer le FSSO



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Collect Agent Timers
Mode d'accès AD
Support du groupe AD
Troubleshooting
LAB



Une formation
Alphorm.com

Collect Agent Timers

Workstation verify interval

Vérifier si un utilisateur est toujours connecté

Par défaut – 5 minutes

Désactiver – définissez la valeur sur 0

Dead entry timeout

Appliquer lorsque l'État n'est pas vérifié uniquement

Utilisé pour purger les informations de connexion

Par défaut – 480 minutes (8h)

Désactiver – définissez la valeur sur 0

Statut rester connecté pour toujours



Une formation
Alphorm.com

Collect Agent Timers

IP address change

Important sur les environnements DHCP ou dynamiques

Par défaut – 60 seconds

Cache users group

L'agent Collector mémorise l'appartenance au groupe d'utilisateurs



Une formation
Alphorm
com

Mode d'accès AD

Standard Access Mode

Windows convention: `Domain\username`

Profile UTM appliqué uniquement aux groupes d'utilisateurs

`Nested group n'est pas supporté`

`Group filters at collector agent`

Advanced Access Mode

LDAP convention user names: `CN=User,OU=Name,DC=Domain`

Profile UTM pour les utilisateurs et les groupes

`nested et inhiere groups sont supportés`

Configuration:

`FortiGate en tant que client LDAP ou filtre de groupe sur l'agent collecteur`



Une formation
Alphorm
com

Support du groupe AD

Type de groupe pris en charge

Groupes de sécurité

Groupes universels

Groupes à l'intérieur des unités organisationnelles (UO)

Groupe local/universel qui contient des groupes universels de domaines enfants (uniquement avec GC)

Si l'utilisateur ne fait pas partie d'un groupe FSSO

Pour FSSO passif, l'utilisateur fait partie de `SSO_guest_user`

Pour passive et active, l'utilisateur est invité à se connecter

Troubleshooting

The screenshot shows the output of the command `# diagnose debug authd fsso list`. The output lists two FSSO logons. Annotations with red boxes and lines point to specific fields:

- Adresse IP**: Points to the IP address `192.168.1.1` in the first logon entry.
- Nom du poste de travail**: Points to the workstation name `WIN-INTERNAL` in the first logon entry.
- utilisateur**: Points to the username `ANNAH2` in the first logon entry.
- groupe**: Points to the group `TRAININGAD/USERS` in the first logon entry.
- Groupe créé sur FortiGate**: Points to the group `TRAININGAD/USERS` in the second logon entry.

```
# diagnose debug authd fsso list
----FSSO logons----
IP: 192.168.1.1 User: ANNAH2 Groups: TRAININGAD/USERS
Workstation: WIN-INTERNAL MemberOf: Training
IP: 10.0.1.10 User: STUDENT Groups: TRAININGAD/USERS
Workstation: WIN-INTERNAL MemberOf: Training
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
```

Troubleshooting

The screenshot shows the output of two commands. Annotations with red boxes and lines point to specific parts of the output:

- Statut des sondages par FortiGate à DC**: Points to the command `# diagnose debug fsso-polling detail`.
- Utilisateurs actifs de FSSO**: Points to the command `# diagnose debug fsso-polling refresh-user`.
- Sniff polls**: Points to the port number `445` in the command `# diagnose sniffer packet any 'host ip address and tcp port 445'`.

```
# diagnose debug fsso-polling detail
AD Server Status:
ID=1, name(10.0.1.10),ip=10.0.1.10,source(security),users(0)
port=auto username=administrator
read log offset=251636, latest login timestamp: Wed Feb 4 09:47:31 2015
polling frequency: every 10 second(s) success(246), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
most recent connection status: connected

# diagnose debug fsso-polling refresh-user
refresh completes. All login users are obsolete. Please re-login to make them
available.

# diagnose sniffer packet any 'host ip address and tcp port 445'
# diagnose debug application fssod -1
```



Une formation
Alphorm
com



Une formation
Alphorm
com

Découvrir les modes d'opérations du HA



Mohamed Anass EDDIK



Plan

Mode actif-passif

Mode actif-actif

Fortigate Clustering Protocol (FGCP)

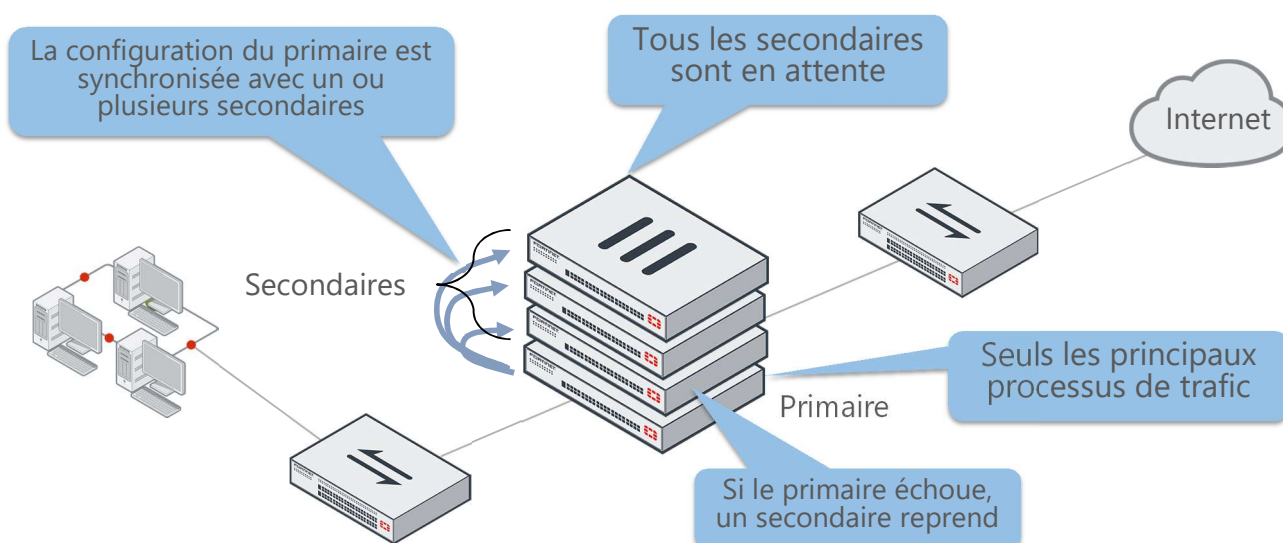
Élection principale FortiGate : remplacement désactivé

Élection principale FortiGate : remplacement activé

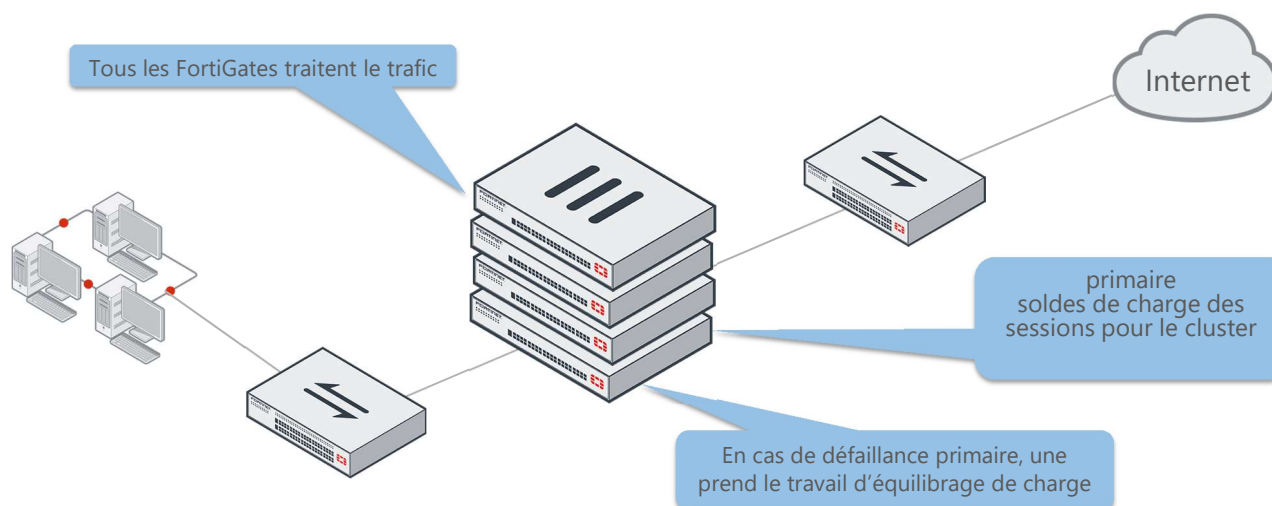
LAB

Une formation
Alphorm.com

Mode actif-passif



Mode actif-actif



Clustering Protocol(FGCP)

Le cluster utilise le protocole de clustering FortiGate (FGCP) pour :

- Découvrir d'autres FortiGates appartenant au même groupe HA
- Élire le principal
- Synchroniser la configuration et d'autres données
- Détecter quand un FortiGate échoue

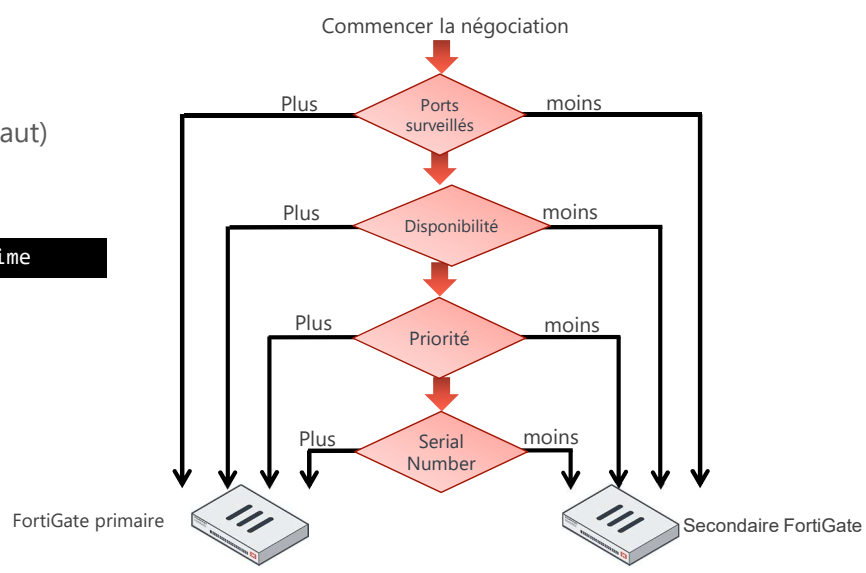
Runs only over the heartbeat links

- Utilise le port TCP 703 avec différentes valeurs de type Ethernet
 - 0x8890 – mode NAT
 - 0x8891 – mode transparent
- Uses TCP port 23 with Ethernet type 0x8893 for configuration synchronization

Remplacement désactivé

Ignorer désactivé (par défaut)
Forcer un basculement

```
diagnose sys ha reset-uptime
```

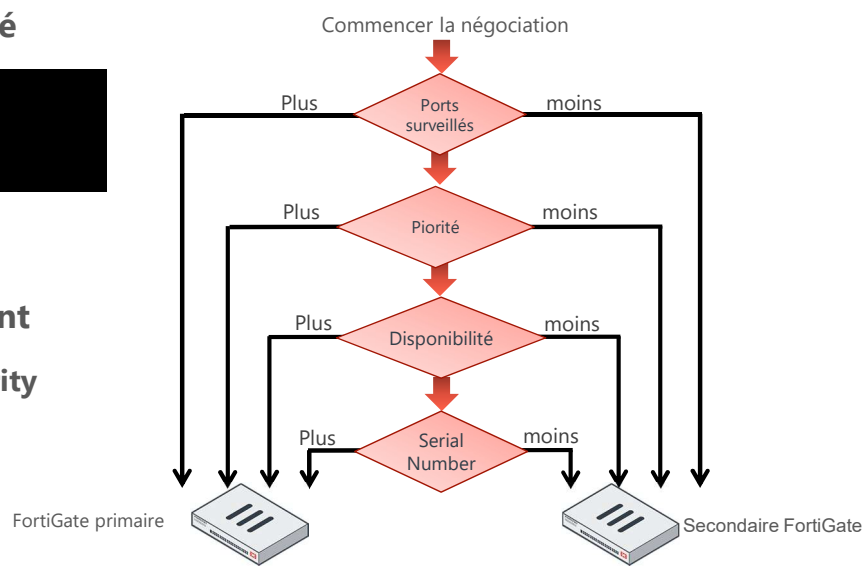


Remplacement activé

Remplacement activé

```
config system ha  
set override enable  
end
```

Forcer un basculement
Change the HA priority





Une formation
Alphorm
com



Une formation
Alphorm
com

Mettre en œuvre la synchronisation du cluster du HA



Mohamed Anass EDDIK



Plan

Tâches FortiGate primaires et secondaires
Synchronisation complète de la config HA
Synchronisation config incrémentielle HA
Qu'est-ce qui n'est pas synchronisé?
Synchronisation de session
LAB

Une formation
Alphorm.com

Les tâches Fortigate

Tâches primaires

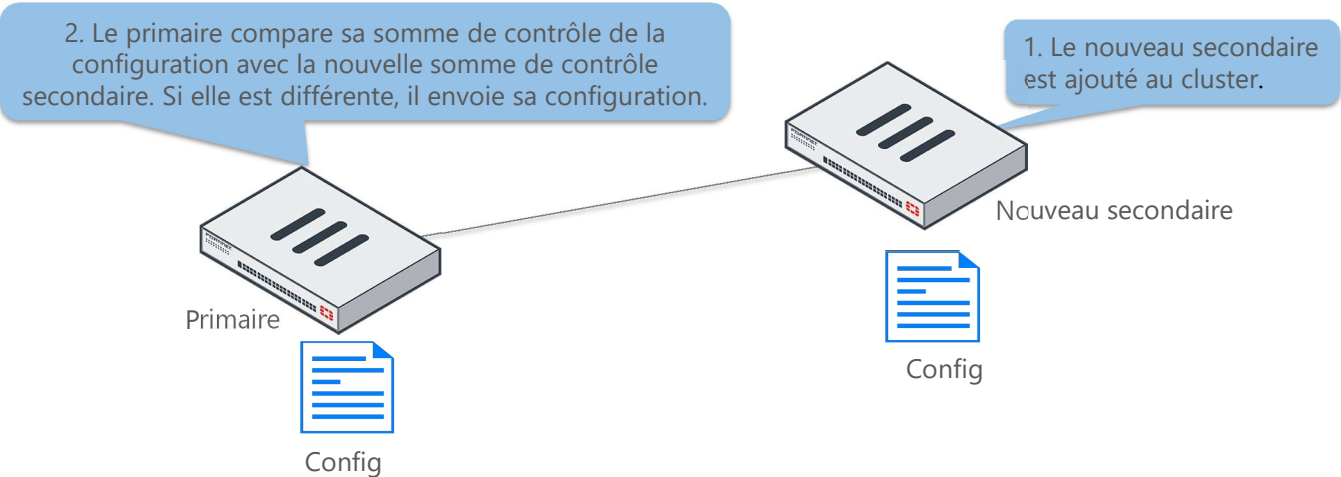
Échange Heartbeat Hello paquets avec tous les secondaires
Synchronise sa table de routage et une partie de sa configuration à tous les secondaires
Peut synchroniser les informations de certaines sessions de trafic pour un basculement transparent
Distribue le trafic entre tous les périphériques du cluster (En mode actif-actif uniquement)

Tâches secondaires

Surveille le principal pour les signes de défaillance à l'aide de la surveillance Hello ou port
Si un problème est détecté avec le primaire, les secondaires élisent un nouveau
Traite le trafic distribué par le principal (En mode actif-actif uniquement)

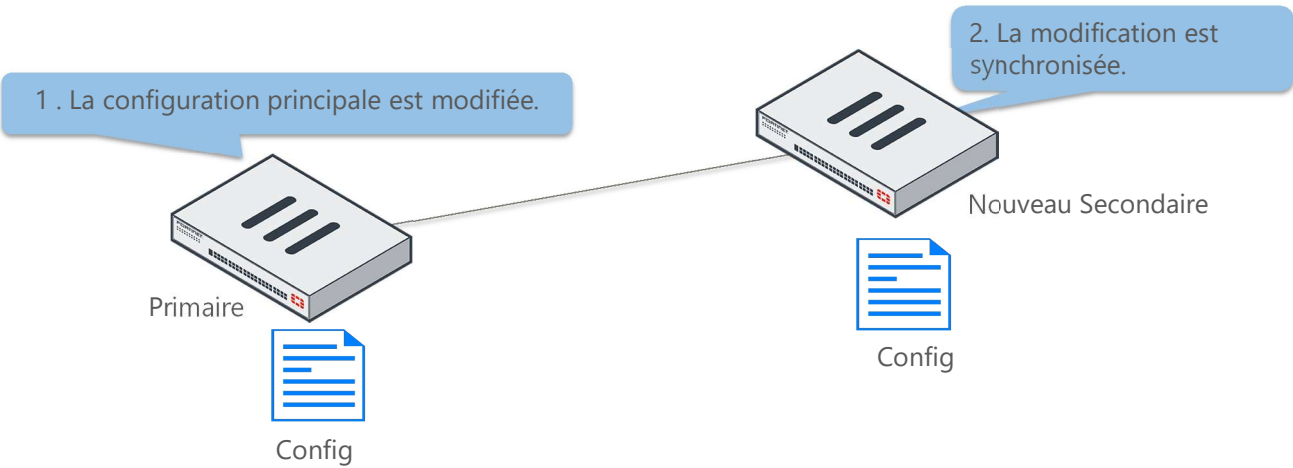
Synchronisation la config HA

Synchronisation complète



Synchronisation la config HA

Synchronisation incrémentielle





Une formation
Alphorm.com

Ce qui n'est pas synchronisé?

Paramètres de configuration qui ne sont pas synchronisés entre les membres du cluster :

- Paramètres de l'interface de gestion HA
- Route par défaut HA pour l'interface de gestion réservée
- Dépassement de la HA
- Priorité de l'appareil HA
- Priorité de cluster virtuel HA
- FortiGate nom d'hôte
- Priorités du serveur ping HA

Le FortiGate principal synchronise tous les autres paramètres de configuration et autres détails de configuration liés à HA settings



Une formation
Alphorm.com

Synchronisation de session

Table de session synchronisée pour la plupart des sessions VPN TCP et IPsec

Seules les sessions qui ne sont pas gérées par un proxy UTM peuvent être synchronisées

```
config system ha
    set session-pickup enable
end
```

Les sessions UDP et ICMP peuvent également être synchronisées

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
end
```

La multidiffusion et la session VPN SSL ne sont pas synchronisées



Une formation
Alphorm
com



Une formation
Alphorm
com

Comprendre la charge du travail du HA et le failover



Mohamed Anass EDDIK



Plan

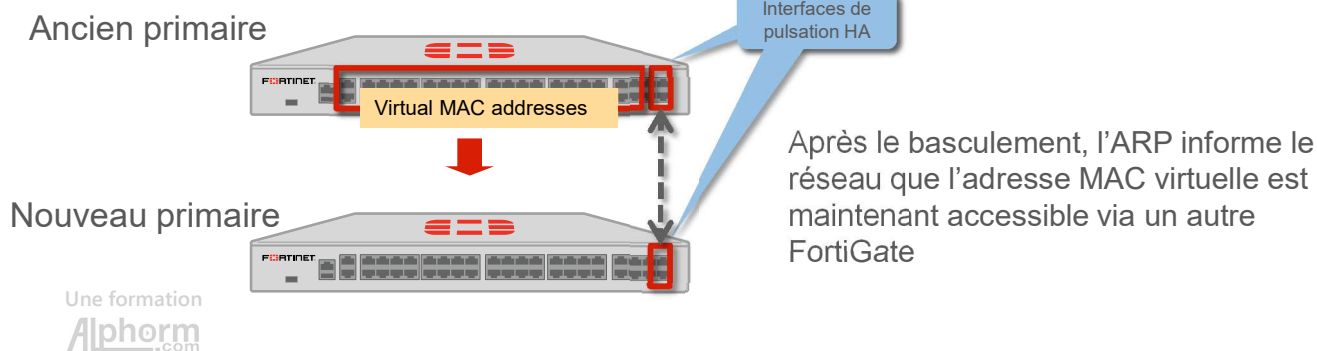
- Adresses MAC virtuelles et failover
- Types de basculement
- Charge de travail
- Active-Active Traffic Flow
- Virtual Clustering
- Full Mesh HA
- LAB

Une formation
Alphorm.com

Adresses MAC virtuelles et le basculement

Sur le primaire, chaque interface – à l'exception des interfaces de pulsation HA – reçoit une adresse MAC virtuelle

Lors du basculement, le primaire nouvellement élu adopte les mêmes adresses MAC virtuelles que l'ancien





Une formation
Alphorm
com

Types de basculement

Device Failover

Si le primaire cesse d'envoyer des paquets de pulsation, un autre FortiGate prend automatiquement sa place

Link failover

Le cluster peut surveiller certaines interfaces pour déterminer s'ils sont opérationnels et connectés

Si une interface surveillée sur le primaire échoue, le cluster élit un nouveau

Session failover

Quand le ramassage de session est activé, le nouveau primaire élu reprend le session actif évitant le besoin de redémarrer la session active



Une formation
Alphorm
com

Charge de travail

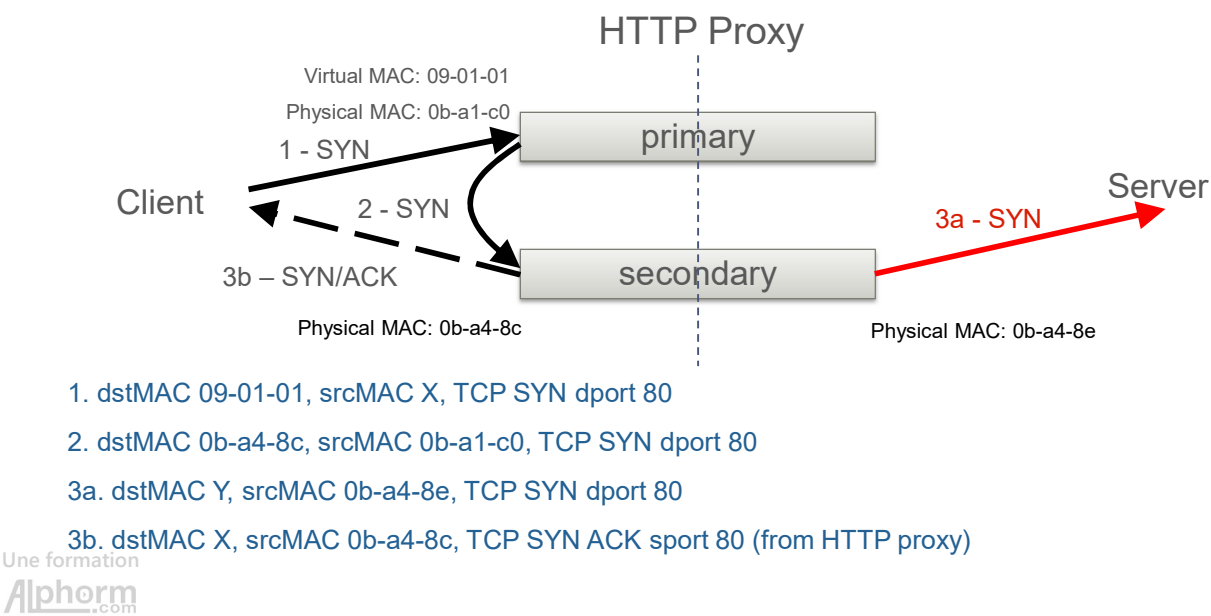
Active-Passive

Le primaire reçoit et traite tout le trafic
Les secondaires attendent passivement

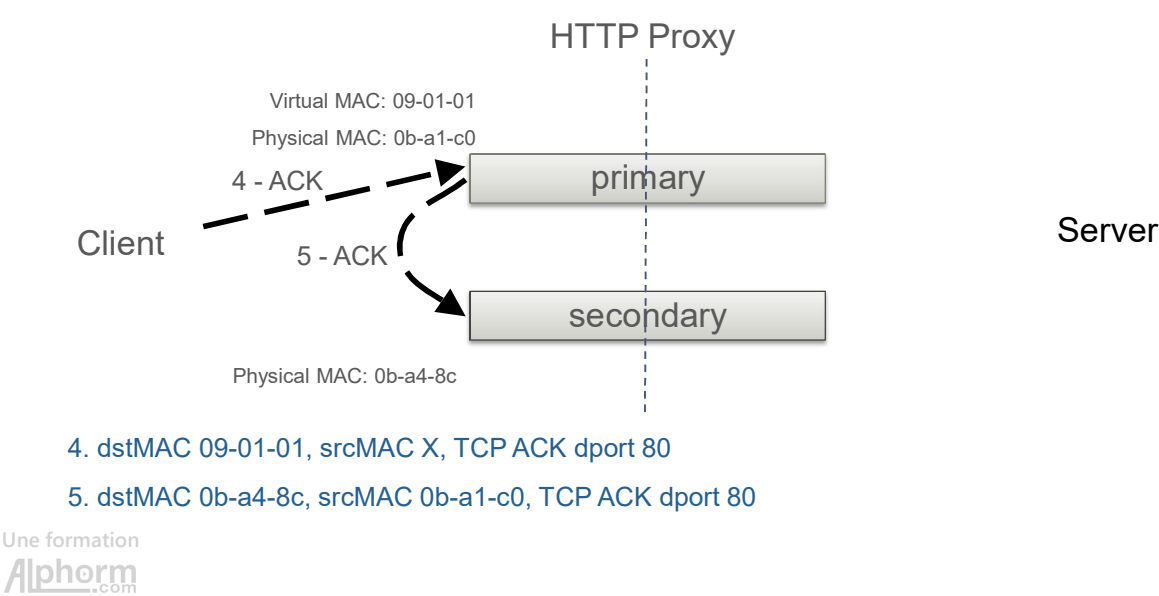
Active-Active

Le primaire reçoit tout le trafic et le redirige vers les secondaires

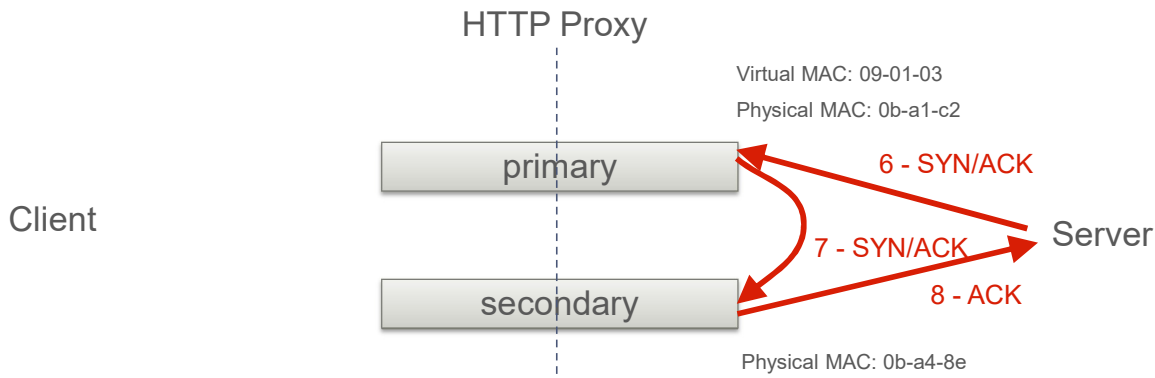
Active-Active Traffic Flow



Active-Active Traffic Flow



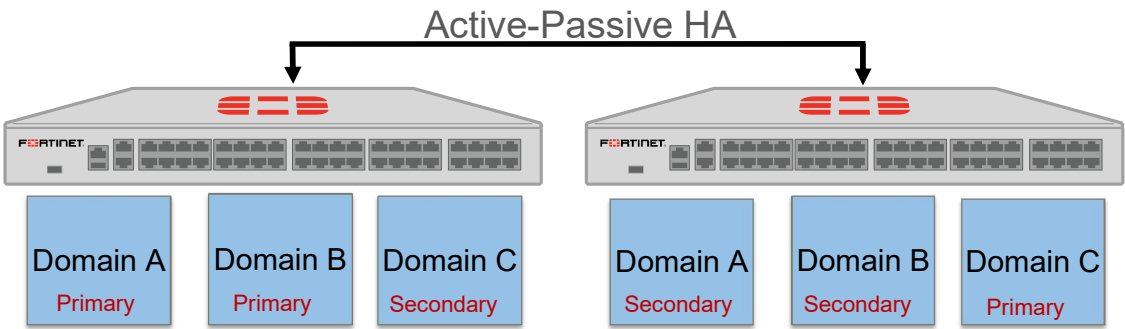
Active-Active Traffic Flow



- 6. dstMAC 09-01-03, srcMAC Y, TCP SYN ACK sport 80
- 7. dstMAC 0b-a4-8e, srcMAC 0b-a1-c2, TCP SYN ACK sport 80
- 8. dstMAC Y, srcMAC 0b-a4-8e, TCP ACK dport 80

Virtual Clustering

Extension de FGCP pour FortiGate avec plusieurs VDOM
Le cluster HA ne doit comporter que deux appareils FortiGate
Permet à un FortiGate d’être le principal pour certains VDOM et le secondaire pour les autres VDOM

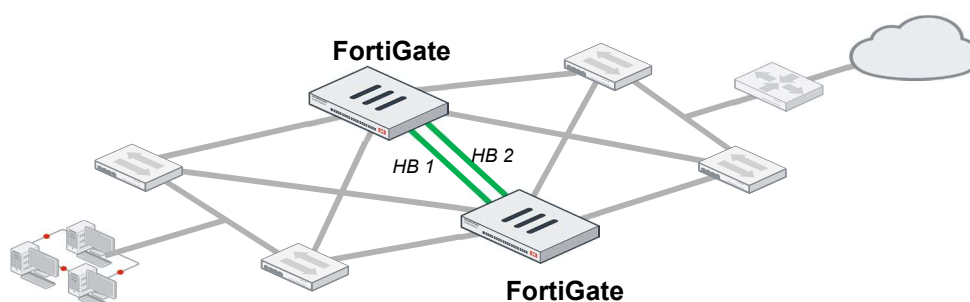


Full Mesh HA

Réduit le nombre de points de défaillance uniques

Disponible sur certains modèles FortiGate

Utilise des interfaces agrégées et redondantes pour des connexions robustes entre tous les composants réseau



Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Surveiller et analyser le HA



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

- Mise à jour du Firmware
- Vérification de l'état du HA
- Passage au secondaire
- Vérification de la synchronisation de la Configuration
- LAB



Mise à jour du Firmware

La mise à niveau non interruptible est activée par défaut

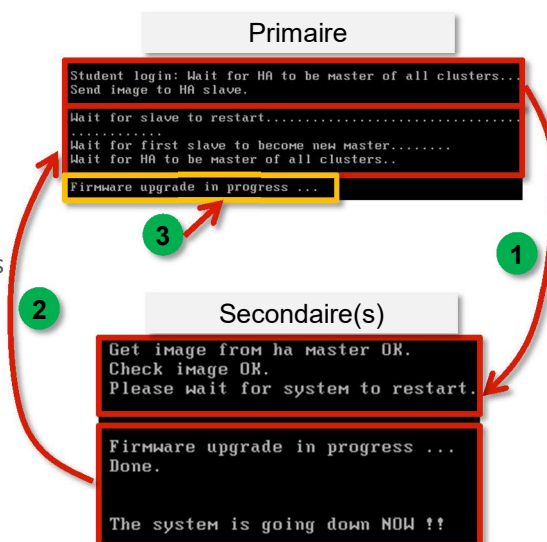
Si le cluster fonctionne en mode actif-actif, l'équilibrage de la charge du trafic est désactivé

Le cluster met à niveau le Firmware sur tous les secondaires d'abord

Un nouveau primaire est élu

Le cluster met à niveau le micrologiciel dans l'ancien primaire

Si le cluster fonctionne en mode actif-actif, l'équilibrage de la charge du trafic est retourné



Une formation
Alphorm.com

Vérification de l'état du HA

diagnose sys ha status

```
HA information
Statistics
  traffic.local = s:0 p:14211 b:5343415
  traffic.total = s:951 p:14211 b:5343415
  activity.fdb = c:0 q:0
Model=5, Mode=1 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0, load_balance=0, schedule=3, ldr_undp=0,
upgrade_mode=0.
```

Informations sur les HA
primaires et secondaires

```
[Debug_Zone HA information]
HA group member information: is_manage_master=1.
FGVM010000030273: Master, serialno_prio=0, usr_priority=200, hostname=Student
FGVM010000030272: Slave, serialno_prio=1, usr_priority=100, hostname=Remote
```

```
[Kernel HA information]
vcluster 1, state=work, master_ip=169.254.0.1, master_id=0:
FGVM010000030273: Master, ha_prio/o_ha_prio=0/0
FGVM010000030272: Slave, ha_prio/o_ha_prio=1/1
```

169.254.0.1 IP de l'interface Heartbeat:
assigné au numéro de série le plus élevé



Une formation
Alphorm.com

Passage au secondaire

En utilisant le CLI du primaire, vous pouvez vous connecter à n'importe quelle CLI secondaire :

```
# execute ha manage <HA_device_index>
```

Pour répertorier les numéros d'index de chaque FortiGate, utilisez le point d'interrogation :

```
# execute ha manage ?  
  <id>    please input peer box index.  
  <1>     Subsidiary unit FGVM0100000xxxxx
```



Une formation
Alphorm.com

Vérification de la synchro

Exécutez la commande suivante dans le ou les membres du cluster :

```
# diagnose sys ha checksum  
cluster      Show HA cluster checksum  
show         Show HA checksum of logged  
              in FortiGate  
recalculate  Re-calculate HA checksum
```

Tous les pairs doivent avoir les mêmes séquences de numéros de contrôle



Exemple de Checksum du cluster

```
Student # diagnose sys ha checksum cluster

===== FGVMO10000030273 =====

is_manage_master()=1, is_root_master()=1
debugzone
global: a4 f7 cf 90 21 b2 c7 51 72 ca 13 dc 6f 1c b1 99
root: 7c 52 f6 c7 28 d4 e7 34 7d fa 86 48 42 c1 17 7d
all: 59 4c e3 6b c6 1d b1 c7 e3 42 97 cf 05 13 0c 42

checksum
global: a4 f7 cf 90 21 b2 c7 51 72 ca 13 dc 6f 1c b1 99
root: 7c 52 f6 c7 28 d4 e7 34 7d fa 86 48 42 c1 17 7d
all: 59 4c e3 6b c6 1d b1 c7 e3 42 97 cf 05 13 0c 42

===== FGVMO10000030272 =====

is_manage_master()=0, is_root_master()=0
debugzone
global: a4 f7 cf 90 21 b2 c7 51 72 ca 13 dc 6f 1c b1 99
root: 7c 52 f6 c7 28 d4 e7 34 7d fa 86 48 42 c1 17 7d
all: 59 4c e3 6b c6 1d b1 c7 e3 42 97 cf 05 13 0c 42

checksum
global: a4 f7 cf 90 21 b2 c7 51 72 ca 13 dc 6f 1c b1 99
root: 7c 52 f6 c7 28 d4 e7 34 7d fa 86 48 42 c1 17 7d
all: 59 4c e3 6b c6 1d b1 c7 e3 42 97 cf 05 13 0c 42
```





Une formation
Alphorm.com

Comprendre les concepts du proxy web



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

- Proxy implicite (transparent)
- Proxy explicite
- Pac File
- Méthode WPAD (DHCP)
- Méthode WDAP(DNS)
- LAB



Une formation
Alphorm.com

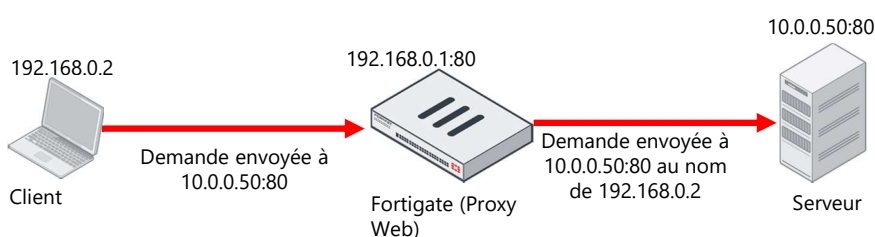
Proxy implicite (transparent)

Le client envoie la demande au port IP + de serveur, pas au proxy

Le proxy implicite intercepte les demandes

Aucune modification de la configuration du client requise pour implémenter un proxy Web

Les demandes envoyées à l'adresse IP du serveur, et non le proxy



Une formation
Alphorm.com

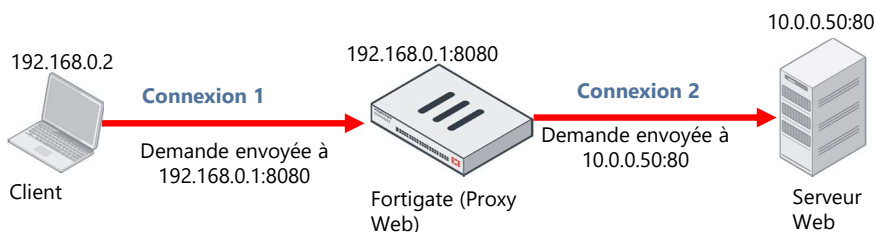
Proxy explicite

Les clients doivent être configurés pour utiliser un proxy Web explicite

Le client envoie les demandes à l'adresse IP et au port du proxy Web. Il n'envoie rien directement au site Web

Le proxy Web écoute sur son (adresse IP, numéro de port) et intercepte ainsi les les paquets envoyés par le client

Le proxy Web envoie les paquets reçus vers le serveur Web en utilisant son adresse IP





Pac File

Définit la façon dont les navigateurs choisissent un proxy
Prend en charge plus d'un proxy
Spécifie le trafic qui sera envoyé à quel proxy
Configurez chaque navigateur avec l'URL du fichier PAC

```
function FindProxyForURL(url, host) {  
  if (shExpMatch(url, "*.example.com/*")) {  
    return "DIRECT";  
  }  
  if (shExpMatch(url, "*.example.com:*/*")) {  
    return "DIRECT";  
  }  
  if (isInNet(host, "10.0.0.0", "255.255.255.0")) {  
    return "PROXY fastproxy.example.com:8080";  
  }  
  return "PROXY proxy.example.com:8080";  
}
```

Les connexions à n'importe quel sous-domaine example.com n'utilisent aucun proxy

Sinon, tout autre trafic utilise proxy.example.com:8080

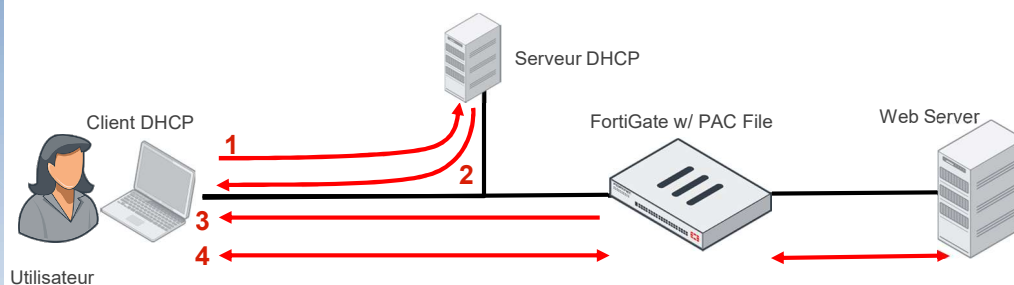
Connexions à 10.0.0.0/24 utilisation fastproxy.example.com:8080

Une formation
Alphorm.com



Méthode WPAD (DHCP)

Navigateur interroge le serveur DHCP
Le serveur DHCP répond avec l'URL du fichier PAC
Navigateur télécharge le fichier PAC
Le navigateur accède au Web via le proxy



Une formation
Alphorm.com



Méthode WDPAP(DNS)

Le navigateur interroge le serveur DNS pour le nom de domaine complet suivant:wpad.<local-domain>

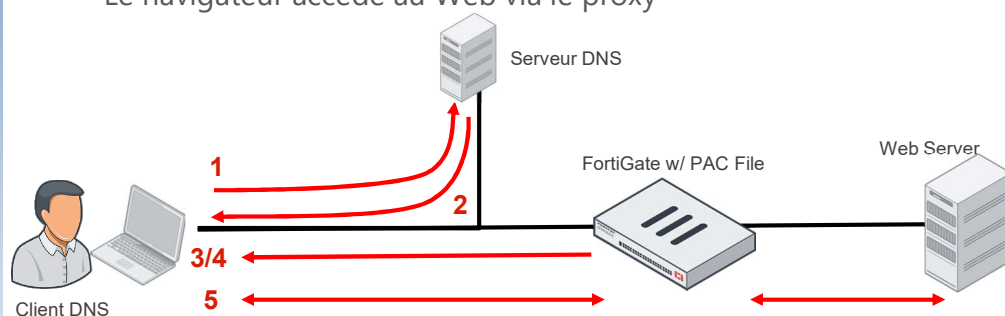
Le serveur DNS répond avec l'adresse IP où le fichier PAC

Le navigateur construit l'URL en utilisant l'adresse IP, le port 80 et le nom de fichier PAC WPAD. dat: http://<pac-server>:80/wpad.dat

Navigateur télécharge le fichier PAC

Le navigateur accède au Web via le proxy

Une formation
Alphorm
com



Une formation
Alphorm
com





Une formation
Alphorm.com

Configurer le proxy web



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Configurer le proxy Web
Web cache
Activer le cache Web
LAB



Une formation
Alphorm.com

Configurer le proxy Web

Explicite web proxy configuration :

- Activer le proxy Web explicite
- Indiquer les interfaces internes que le proxy Web explicite va être en écoute
- Créer des stratégies de proxy explicites pour autoriser et inspecter le trafic
- Configurer les navigateurs de chaque client pour se connecter via le proxy

Transparent Web proxy configuration

- Créer des stratégies régulières pour faire correspondre le trafic, en appliquant un proxy avec le paramètre de redirection de proxy HTTP activé
- Créer des politiques de proxy pour autoriser ou inspecter le trafic



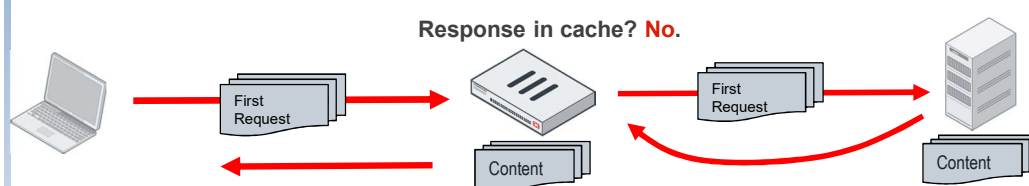
Une formation
Alphorm.com

Web cache

Pour la première demande, la réponse n'est pas encore en cache.

Proxy:

- Obtient le contenu du serveur
- Stocke en mémoire si le contenu n'est pas dynamique
- Réponse en avant au client





Web cache

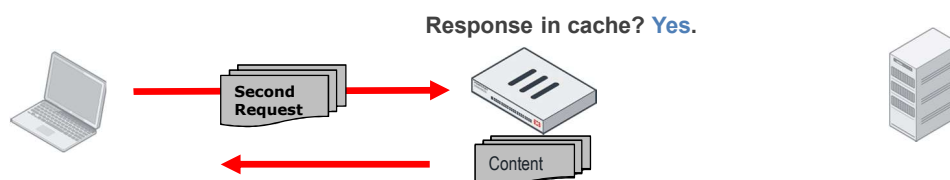
Pour les demandes ultérieures, la réponse est généralement déjà dans le cache

Proxy transfère une copie du cache au client

Ne télécharge pas le contenu du serveur à nouveau

Le contenu dynamique est une exception, donc proxy le traite comme première demande à chaque fois

Une formation
Alphorm.com



Activer le cache Web

```
config firewall proxy-policy
  edit <proxy_policy_number>
    set webcache enable
  next
end
```

Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Maitriser l'authentification et l'autorisation du proxy web



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Authentification par proxy Web
Schémas d'authentification et règles
Authentification basée sur IP et basée sur
une session
Authentification basée sur une session
LAB



Une formation
Alphorm.com

Authentification par proxy Web

Le proxy Web sépare l'authentification de l'utilisateur de l'autorisation utilisateur

Les schémas d'authentification et les règles sont utilisés pour identifier les utilisateurs

L'autorisation est ensuite appliquée dans les stratégies de proxy

Un schéma définit la méthode d'inscription et l'utilisateur d'authen à utiliser

Les règles d'authentification définissent le schéma à utiliser pour l'authentification active et passive (SSO), selon l'adresse IP et le protocole de l'utilisateur (HTTP, FTP ou SOCKS)



Schémas et règles

Schémas d'authentification

```
config authentication scheme
edit <scheme-name>
set method [basic|digest|ntlm|form|negotiate|fsso|rsso]
set user-database [local|<ldap-server>|<radius-server>|<fsso-name>|<rsso-name>|<tacacs+-server>]
set require-tfa [enable|disable]
set fsso-guest [enable|disable]
end
```

Règle d'authentification

```
config authentication rule
edit <rule-name>
set protocol [http|ftp|socks]
set status [enable|disable]
set srcaddr <addr-name or addrgrp-name>
set ip-based [enable|disable]
set sso-auth-method <scheme-name>
set active-auth-method <scheme-name>
next
end
```

Une formation
Alphorm.com



Authentification explicite

Basée sur IP

Les sessions IP à partir de la même adresse IP source sont traitées comme un seul utilisateur

Déconseillé si plusieurs utilisateurs sont derrière la source NAT
Partage d'accès Internet, Citrix, serveurs Terminal Server, etc

Basée sur la session

Les sessions HTTP sont traitées comme un seul utilisateur

Peut différencier plusieurs clients derrière la même adresse IP source

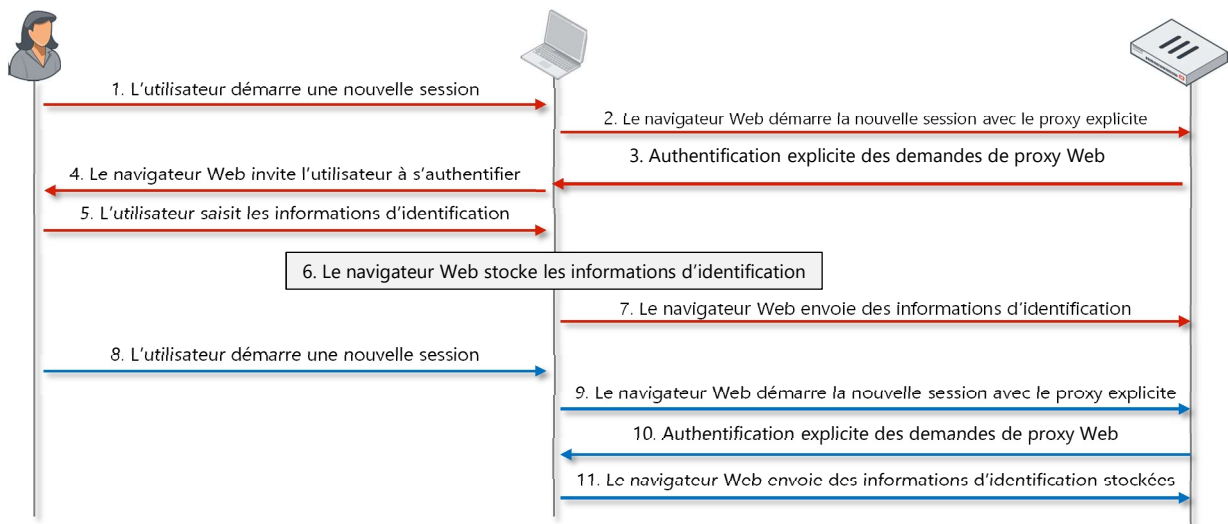
Après l'authentification, le navigateur stocke les informations utilisateur dans un cookie de session

Chaque requête suivante contient le cookie de session

Nécessite plus de ressources

Une formation
Alphorm.com

Authentification basée sur une session





Une formation
Alphorm
com

Réaliser un diagnostic Général



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Informations système
Informations sur la couche physique
Table ARP
Dépannage de la couche réseau
LAB



Une formation
Alphorm.com

Informations système

```
# get system status

Version: FortiGate-VM64 v5.4.0,build1011,151221 (GA)
Virus-DB: 31.00050(2015-12-09 08:12)
Extended DB: 31.00050(2015-12-09 08:12)
IPS-DB: 6.00746(2015-12-08 01:57)
Serial-Number: FGVM010000051317
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
License Status: Valid
VM Resources: 1 CPU/1 allowed, 994 MB RAM/2048 MB allowed
Log hard disk: Available
Hostname: Student
Operation Mode: NAT
Current virtual domain: root
Virtual domains status: 1 in NAT mode, 0 in TP mode
Current HA mode: standalone
Branch point: 1011
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Feb 3 18:18:29 2016
```



Une formation
Alphorm.com

La couche physique

```
# get hardware nic <port>

# Name: port1
# Driver: vmxnet3
# Version: 1.1.29.0-k-NAPI
# Hwaddr: 00:0c:29:04:60:1b
# Permanent Hwaddr:00:0c:29:04:60:1b
# State: up
# Link: up
# Mtu: 1500
# Supported: 1000full 10000full
# ...
# Auto: disabled
# Rx packets: 11827
# Rx bytes: 16243808
# Rx dropped: 0
# Rx errors: 0
# ...
# Tx packets: 7175
# Tx bytes: 761511
# Tx dropped: 0
# Tx errors: 0
# Multicasts: 34
# Collisions: 0
```



Table ARP

```
# diagnose ip arp list

index=2 ifname=port1 192.168.1.99 state=00000001 use=174 confirm=916499 update=174
ref=17
index=2 ifname=port1 192.168.1.116 ac:72:89:56:aa:31 state=00000002 use=0 confirm=7
update=12141 ref=2
index=2 ifname=port1 224.0.1.140 01:00:5e:00:01:8c state=00000040 use=911087
confirm=917087 update=911087 ref=1
```



Dépannage réseau

```
# execute ping-options
data-size      Integer value to specify datagram size in bytes.
df-bit         Set DF bit in IP header <yes | no>.
interval       Integer value to specify seconds between two pings.
repeat-count   Integer value to specify how many times to repeat PING.
source         Auto | <source interface IP>.
timeout        Integer value to specify timeout in seconds.
tos            IP type-of-service option.
ttl            Integer value to specify time-to-live.

# execute ping {<ipv4_address> | <host_fqdn>}

# execute traceroute {<ipv4_address> | <host_fqdn>}
```



Une formation
Alphorm.com



Une formation
Alphorm.com

Analyser le debug-low , CPU et la mémoire



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Debug flow

Utilisation de la CPU et de la mémoire

Résolution des problèmes de CPU et de mémoire

Utilisation des processus de cotation

Forked Processes et Mémoire partagée

Mode de conservation de la mémoire système

LAB



Une formation
Alphorm.com

Debug flow

Montre le traitement des paquets par le CPU étape par étape

Si un paquet est abandonné, il indique la raison

Effectuer via CLI à plusieurs étapes :

Activer la sortie de la console: `diagnose debug flow show console enable`

Spécifiez le filtre: `diagnose debug flow filter <filter>`

Activer la sortie de débogage: `diagnose debug enable`

Démarrez la trace: `diagnose debug flow trace start [number_of_packets]`

Arrêter la trace: `diagnose debug flow trace stop`

Debug flow

```
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, 10-00007fc0,  
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"
```

Adresses IP, numéros de port et
interface entrante

Utilisation d'une session existante

NAT de destination

un itinéraire correspondant. Affiche
l'adresse IP et l'interface sortante du
prochain saut



CPU, RAM et réseau

```
# get system performance status  
CPU states: 4% user 13% system 0% nice 83% idle  
CPU0 states: 3% user 13% system 0% nice 84% idle  
CPU1 states: 5% user 13% system 0% nice 82% idle  
CPU2 states: 2% user 13% system 0% nice 85% idle  
CPU3 states: 6% user 13% system 0% nice 81% idle  
Memory states: 19% used  
Average network usage: 12740 kbps in 1 minute,  
3573 kbps in 10 minutes, 1077 kbps in 30  
minutes  
Average sessions: 118 sessions in 1 minute, 11  
sessions in 10 minutes, 40 sessions in 30  
minutes  
Average session setup rate: 11 sessions per second  
in last 1 minute, 0 sessions per second in last  
10 minutes, 1 sessions per second in last 30  
minutes  
Virus caught: 3 total in 1 minute  
IPS attacks blocked: 64 total in 1 minute  
Uptime: 60 days, 9 hours, 58 minutes
```

Utilisation
du CPU

Utilisation
de la RAM

Utilisation
du réseau



Résolution des problèmes

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
1U, 4N, 0S, 95I, 0WA, 0HI, 0SI, 0ST; 994T, 421F
  pyfcgid      248      S      2.9      3.8
  newcli       251      R      0.1      1.0
merged_daemons 185      S      0.1      0.7
  miglogd      177      S      0.0      6.8
  pyfcgid      249      S      0.0      3.0
  pyfcgid      246      S      0.0      2.8
  reportd      197      S      0.0      2.7
  cmdbsvr      113      S      0.0      2.4
```

Utilisation de la mémoire (%)

Nom du processus ID du processus État du processus Utilisation du CPU (%)

Une formation
Alphorm.com

Trier par CPU: Shift + P ; Trier par RAM: Shift + M

Utilisation des processus de cotation

```
# diagnose sys top
Run Time: 11 days, 3 hours and 29
minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST;
994T, 429F
  thttp      48      S      0.0      4.4
  httpsd     74      S      0.0      0.5
  httpsd     76      S      0.0      0.4
  cmdbsvr    23      S      0.0      3.4
  httpsd    18618     S      0.0      2.9
```

Forked processes sont répertoriés individuellement

```
# diagnose sys top-summary
CPU [|||||] ] 38.4%
Mem [|||||||] ] 54.0% 1009M/1841M
Processes: 20 (running=1 sleeping=86)

PID  RSS  ^CPU% MEM%  FDS  TIME+  NAME
* 72   32M  34.2  1.7   11  00:03.39 httpclid [x5]
95   11M   1.9  0.6   20  53:07.83 cw_wtpd
40   23M   0.0  1.3   24  03:02.60 httpsd [x2]
1173 27M   0.0  1.5   10  00:02.82 pyfcgid [x4]
37    9M   0.0  0.5    9  00:00.23 uploadd
```

Mémoire totale utilisée par tous les forked processes, y compris la mémoire partagée

Forked processes sont répertoriés ensemble

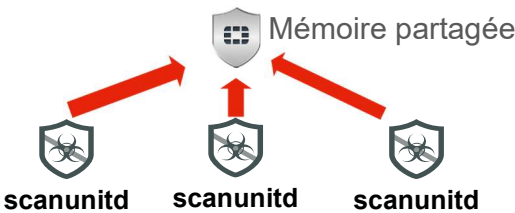
Nombre de fois où le processus a forked



Une formation
Alphorm.com

Forked Processes et Mémoire partagée

Les processus peuvent frayer ("fork") plusieurs copies
Exemple : l'analyse antivirus de chaque stratégie est distincte, bien qu'ils utilisent les mêmes signatures chargées dans la mémoire vive
La mémoire partagée est affectée globalement au système (pas un ID de processus)



Une formation
Alphorm.com

Mode de conservation

FortiOS se protège lorsque l'utilisation de la mémoire est élevée. Ainsi, il évite d'utiliser tant de mémoire que le FortiGate ne pourra pas réagir
FortiOS offre trois seuils configurables :

Threshold	Definition	Default (% of total RAM)
Green	Threshold at which FortiGate exits conserve mode	82%
Red	Threshold at which FortiGate enters conserve mode	88%
Extreme	Threshold at which new sessions are dropped	95%

```
# config system global
memory-use-threshold-green <percentage>
memory-use-threshold-red <percentage>
memory-use-threshold-extreme <percentage>
end
```



Une formation
Alphorm
com



Une formation
Alphorm
com

Gérer le Firmware et le Hardware



Mohamed Anass EDDIK



Plan

BIOS

Installation du Firmware à partir de la console

Transfert du Firmware du BIOS

Test du matériel

Crash logs

LAB

Une formation
Alphorm.com



Accès au BIOS

```
FGT60D (18:34-05.06.2014)
Ver:04000005
Serial number:FG60DXXXXXXXXX
RAM activation
Total RAM: 512MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Enabling Interrupts...Done.
Boot up, boot device capacity: 122MB.
Press any key to display configuration
menu.....

Reading boot image 1375833 bytes.
Initializing firewall...
System is started.
```

Version du BIOS. Les options dans le menu du BIOS dépendent de la version

Appuyez sur n'importe quelle touche à cette invite pour entrer dans le menu BIOS

Une formation
Alphorm.com



Une formation
Alphorm.com

Firmware installation

Assurez-vous qu'une application de serveur TFTP est installée sur votre PC

Configurez le répertoire du serveur TFTP et copiez le Firmware FortiGate [image. Out]

Connectez votre carte réseau PC à l'interface d'installation de FortiGate TFTP

Sélectionnez obtenir l'image du micrologiciel dans le menu du BIOS



Une formation
Alphorm.com

Transfert du Firmware

Please connect TFTP server to Ethernet port "3".

Enter TFTP server address [192.168.1.168]: 192.168.1.110

Enter local address [192.168.1.188]:

Enter firmware image file name [image.out]

MAC:00090FC371BE

#####

Total 23299683 bytes data downloaded.

Verifying the integrity of the firmware image

Total 40000kB unzipped.

Save as Default firmware/Backup firmware/Run image without

saving:[D/B/R]?d

Programming the boot device now.

.....

Reading boot image 1375833 bytes.

Initializing firewall...

System is started.

Formatting shared data partition ... done!

AVERTISSEMENT: le transfert d'une image du Firmware supprime la configuration et installe la configuration usine par

défaut



Une formation
Alphorm.com

Test du matériel

Conçu pour les tests de fabrication et les utilisateurs finaux pour vérifier les principaux composants matériels : CPU, FLASH, RAM, Disque dur, interfaces réseaux, interface USB, ...

Dans certains modèles de la série E et de la série D, le test matériel peut être exécuté directement à partir de FortiOS

Il est possible d'exécuter un seul test ou plusieurs

Pour les autres modèles, une image HQIP spéciale doit être chargée à l'aide d'un serveur TFTP et exécutée à partir du menu du BIOS. La procédure est détaillée sur le lien suivant : <https://support.fortinet.com/Download/HQIPImages.aspx>



Une formation
Alphorm.com

Test du matériel

```
# diagnose hardware test suite all
#
# - Please connect ethernet cables:
# [WAN - Any of PORT1...PORT4]
# To skip this test, please press 'N'.
# Do you want to continue? (y/n) (default is n) N
#
# Following tests will request you to check the colours of the
# system LEDs.
# To skip this test, please press 'N'.
# Do you want to continue? (y/n) (default is n) N
#
# Following tests will request you to check the colours of the
# NIC LEDs.
# - Please connect ethernet cables:
# [WAN - Any of PORT1...PORT4]
# To skip this test, please press 'N'.
# Do you want to continue? (y/n) (default is n) N
#
# Test Begin at UTC Time Tue Aug 25 21:08:53 2015.
```



Une formation
Alphorm
com

Crash logs

Inspecter les journaux de crash à des fins de débogage
Chaque fois qu'un processus se referme, il est enregistré
comme killed. Certains sont normaux (ex. fermeture de
scanunit pour mettre à jour les définitions)

Les événements de mode de conservation sont également
enregistrés

```
# diagnose debug crashlog read
36: 2015-11-25 17:20:02 the killed daemon is /bin/quard: status=0xf
37: 2015-11-25 17:20:02 the killed daemon is /bin/thmd: status=0x0
38: 2015-11-25 17:20:02 the killed daemon is /bin/snmpd: status=0x0
39: 2015-11-25 17:20:02 the killed daemon is /bin/proxyd: status=0x0
40: 2015-11-25 17:20:02 the killed daemon is /bin/fgfmd: status=0x0
41: 2015-11-25 17:20:02 the killed daemon is /bin/reportd: status=0x0
```



Une formation
Alphorm
com

Crash logs Conserve Mode

The Crash log enregistre également les événements de
mode de conservation

Entrée :

```
12: 2017-05-12 14:10:16 logdesc="Kernel enters conserve mode"
Service=kernel conserve=on free="127962
13: 2017-05-12 14:10:16 pages" red=128000 pages" msg="Kernel enters
conserve mode"
```

Sortie :

```
14: 2017-05-12 14:19:55 logdesc="Kernel leaves conserve mode"
Service=kernel conserve=exit
15: 2017-05-12 14:19:55 free="192987 pages" green=192000 pages"
msg="Kernel leaves conserve mode"
```



Une formation
Alphorm.com



Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Bilan

Configurer IPsec VPN
Configurer le DLP
Configurer Routage
Configurer SD-WAN
Configurer les domaines virtuels
Configurer le Switching
Configurer le VPN site-to-site IPsec
Configurer le Fortinet SSO
Configurer la HA
Configurer le Proxy Web
Effectuer les diagnostics

Une formation
Alphorm
com



Cursus Fortigate



Une formation
Alphorm
com

A vous de jouer !

