



Formation

Fortigate Security 6.2



Mohamed Anass EDDIK

Une formation
Alphorm.com



Cursus Fotigate 6.2



Une formation
Alphorm.com



Plan

Introduction

1. Configurer les stratégies
2. Configurer le NAT
3. Configurer l'authentification
4. Configurer le logging et monitoring
5. Configurer les certificats
6. Configurer le webfiltering
7. Configurer le contrôle applicatif
8. Configurer l'Antivirus
9. Configurer l'IPS et le DOS
10. Configurer le SSL VPN

Conclusion

Une formation
Alphorm
com



Public concerné

Support technique

Administrateur sécurité

Avant-vente sécurité

Préparer la Certification NSE4

Une formation
Alphorm
com



Prérequis

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



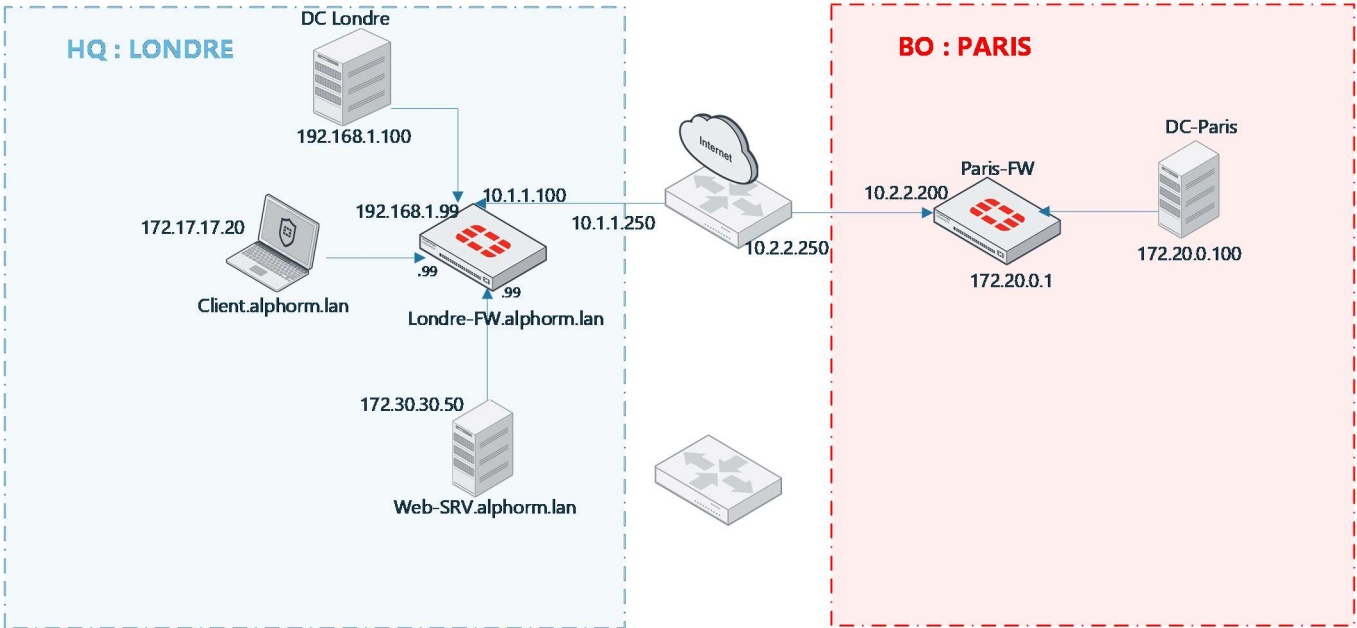
Mohamed Anass EDDIK



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
WAN-Londre	VMnet4	10.1.1.0/24
WAN-Paris	VMnet5	10.2.2.0/24
Lan-Paris	VMnet6	172.20.0.0/24





Présentation des gammes Fortigate et la security fabric



Mohamed Anass EDDIK

Une formation
Alphorm.com

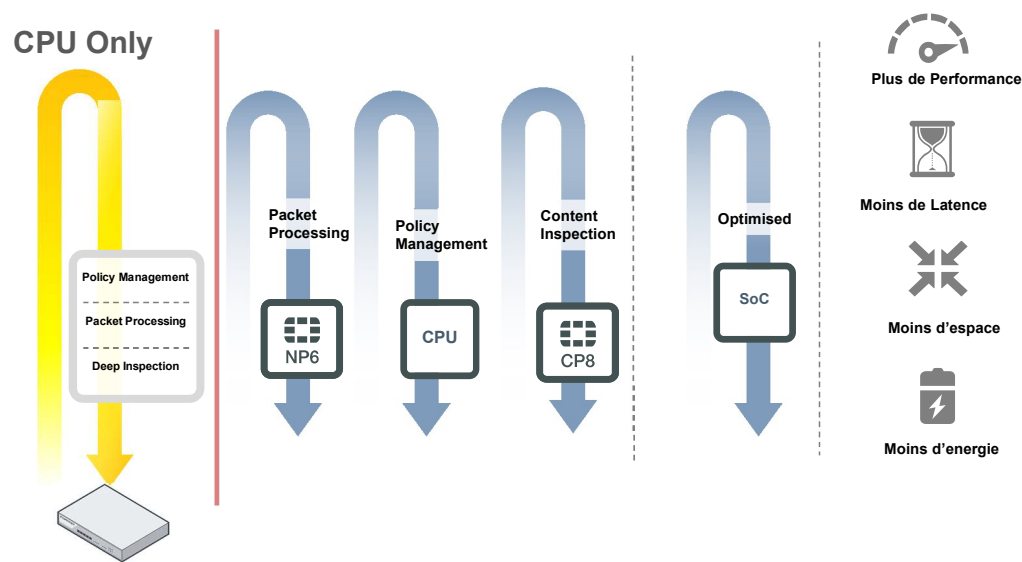


Plan

La Force de Fortigate
Les gammes Fortigate
Les fonctionnalités Fortigate
La Security Fabric

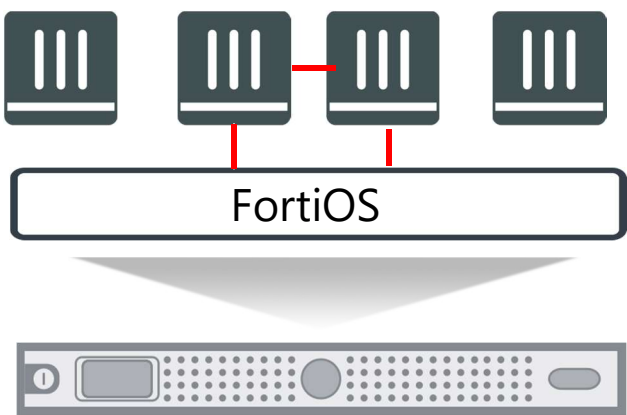
Une formation
Alphorm.com

La Force du Fortigate

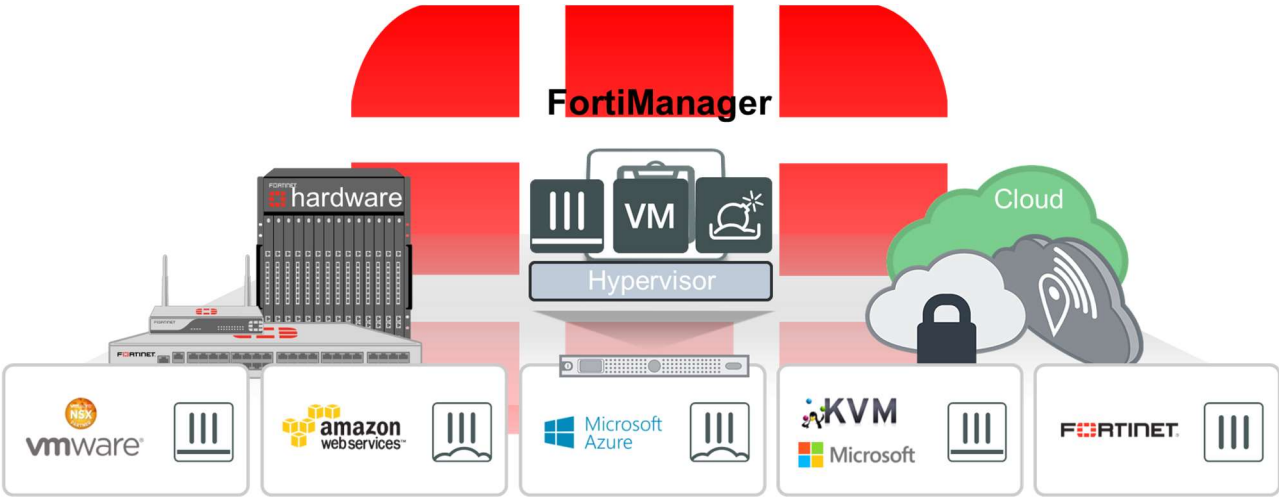


Les domaines virtuels flexibles

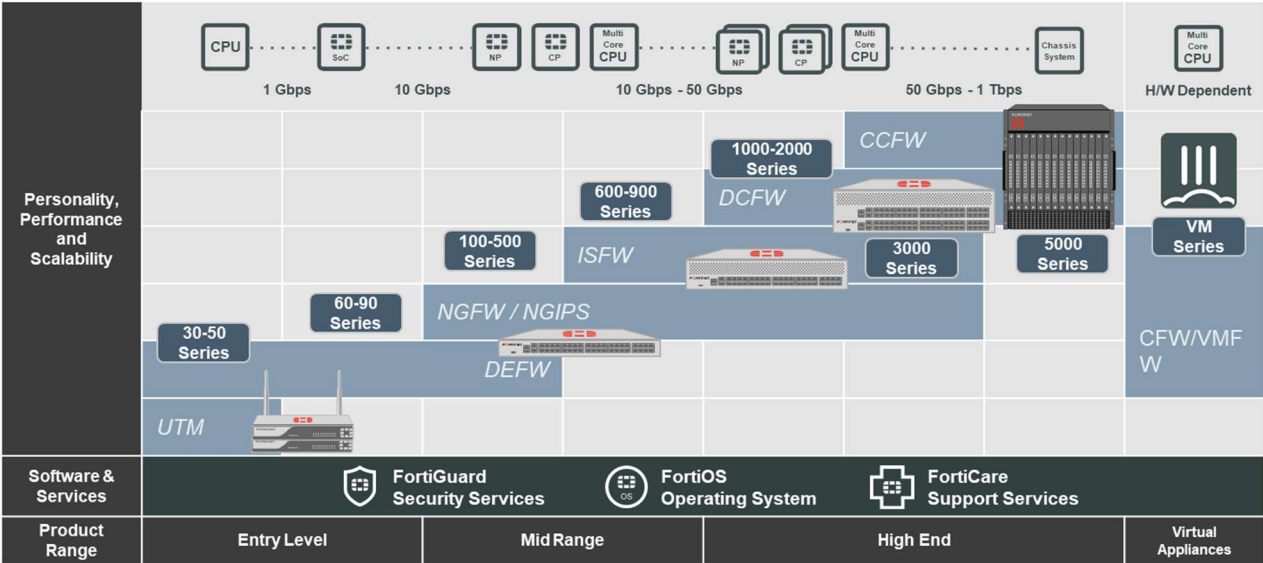
10 VDOM Inclue
Communication entre VDOMS
Multi-tenant



Les gammes Fortigate



Les gammes Fortigate



Les fonctionnalités Fortigate



Accelerated Firewall IPv4 IPv6



SSL & IPSec VPN (+ADVPN)



Dynamic Web Filtering



Anti-Virus & Anti-Botnet



Application Control & DLP



IPS & IDS



Wan Optimization
(cache, explicit proxy, wanop)



Cloud / on-premise Sandboxing



QoS & Traffic shaping



Identity & Device Awareness

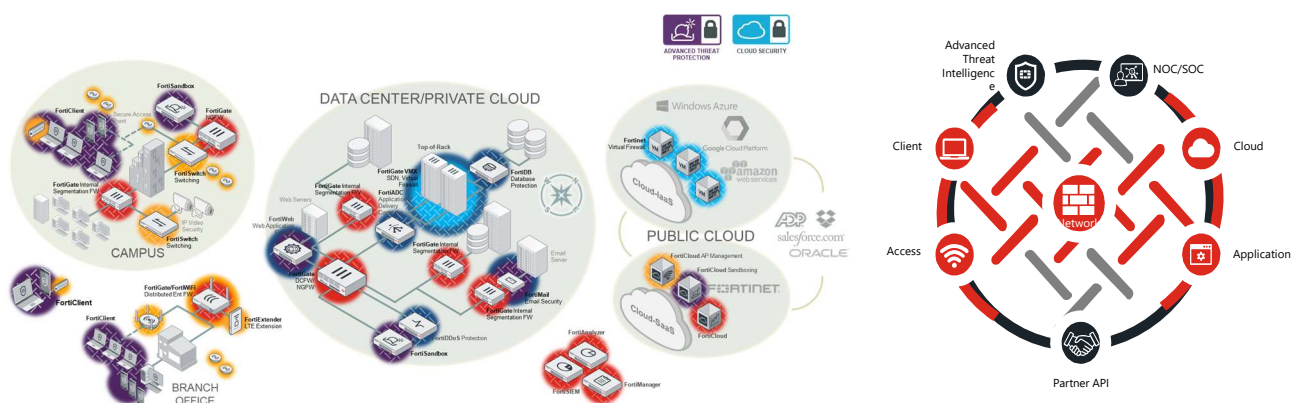


Advanced SD WAN & VXLAN



Mobile Security & Endpoint Control

Security Fabric



large

puissant

automatisé



Présentation des gammes Fortigate et la security fabric



Mohamed Anass EDDIK

Une formation
Alphorm.com

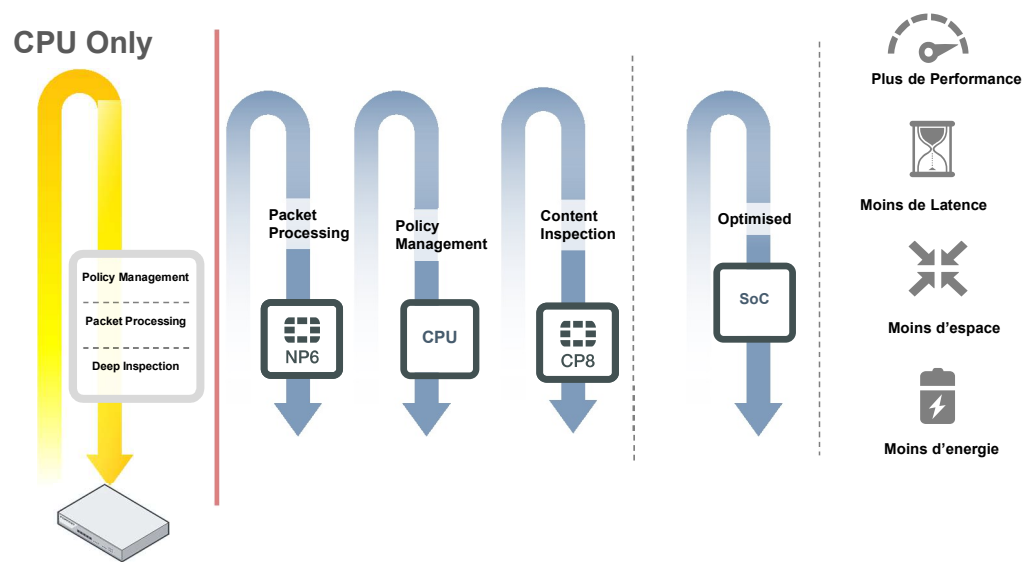


Plan

La Force de Fortigate
Les gammes Fortigate
Les fonctionnalités Fortigate
La Security Fabric

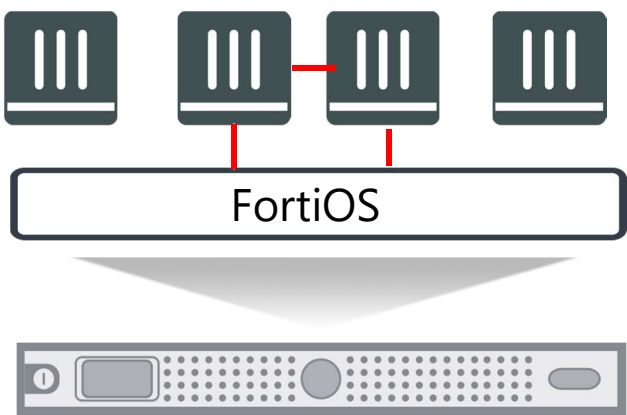
Une formation
Alphorm.com

La Force du Fortigate

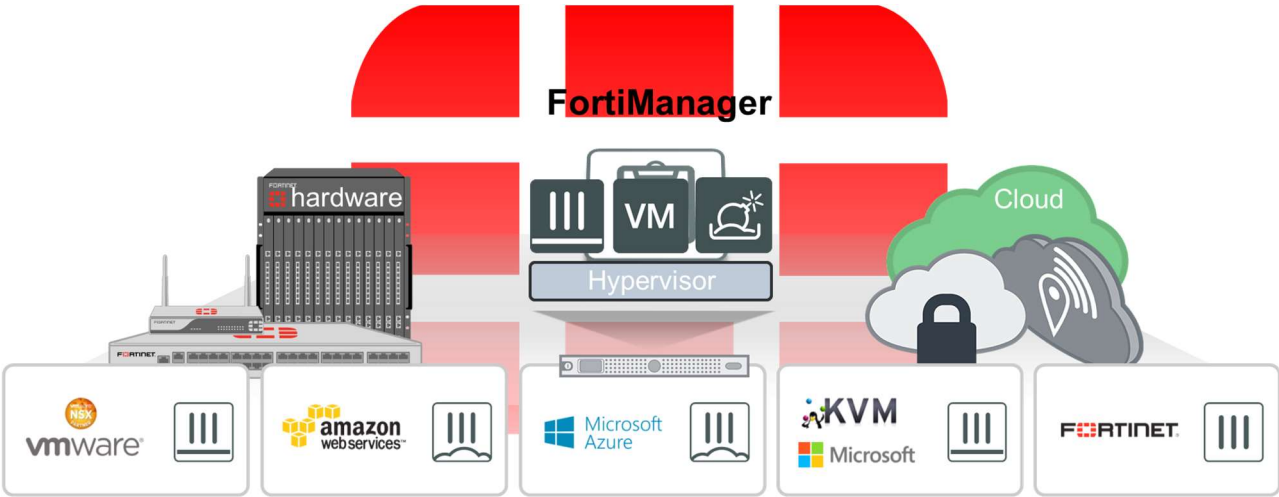


Les domaines virtuels flexibles

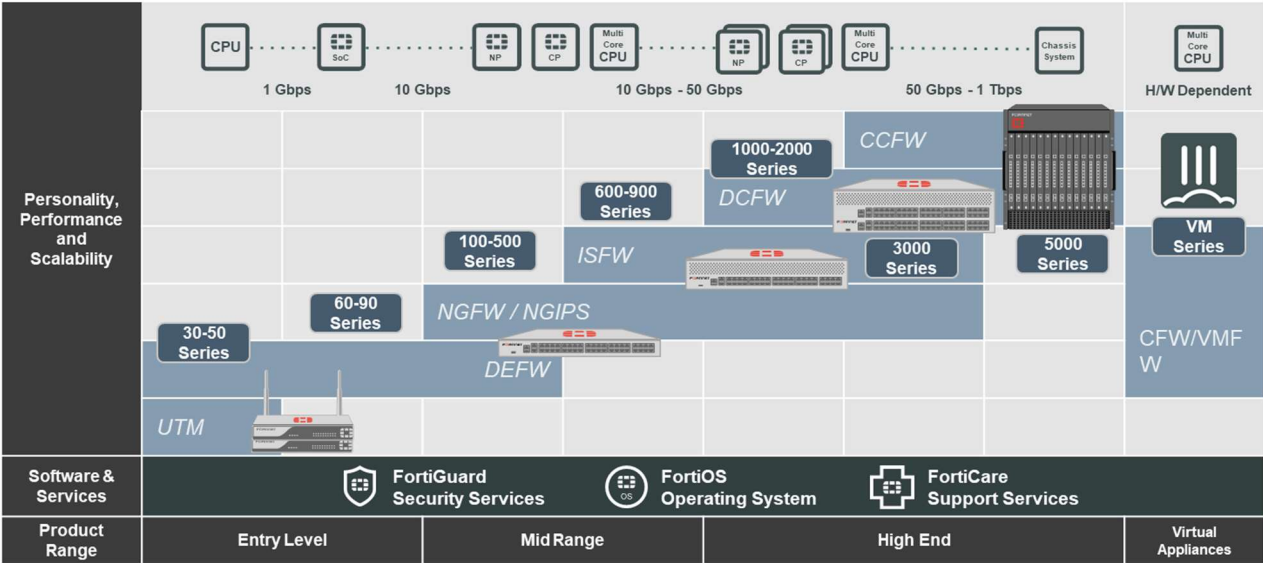
10 VDOM Inclue
Communication entre VDOMS
Multi-tenant



Les gammes Fortigate



Les gammes Fortigate



Les fonctionnalités Fortigate



Accelerated Firewall IPv4 IPv6



WAN Optimization
(cache, explicit proxy, wanop)



SSL & IPsec VPN (+ADVPN)



Cloud / on-premise Sandboxing



Dynamic Web Filtering



QoS & Traffic shaping



Anti-Virus & Anti-Botnet



Identity & Device Awareness



Application Control & DLP



Advanced SD WAN & VXLAN

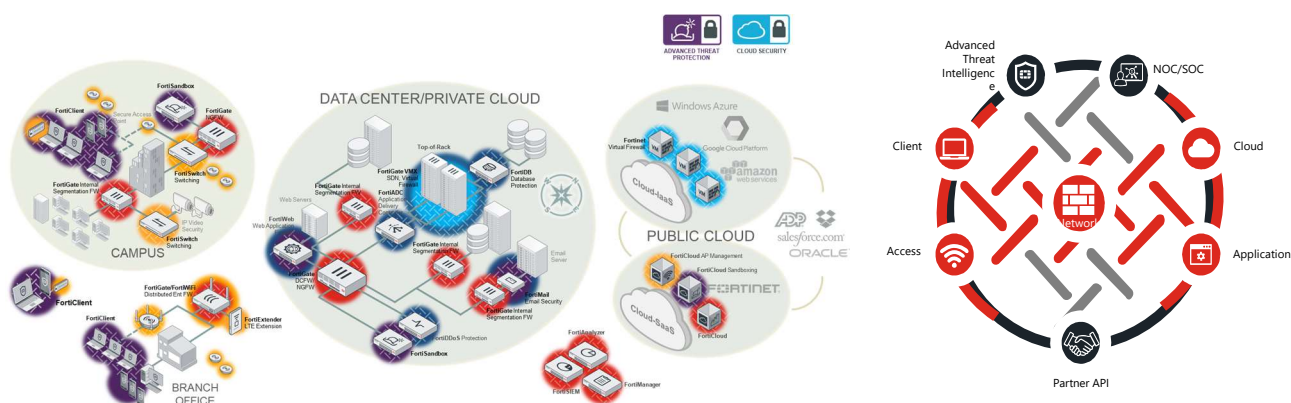


IPS & IDS



Mobile Security & Endpoint Control

Security Fabric



large

puissant

automatisé



Une formation
Alphorm
com

Comprendre les critères et actions



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Comment fonctionne une règle pare-
Feu?

Relation critères et actions

Lab



Règle du Pare-feu

Quand une session de paquet IP arrive

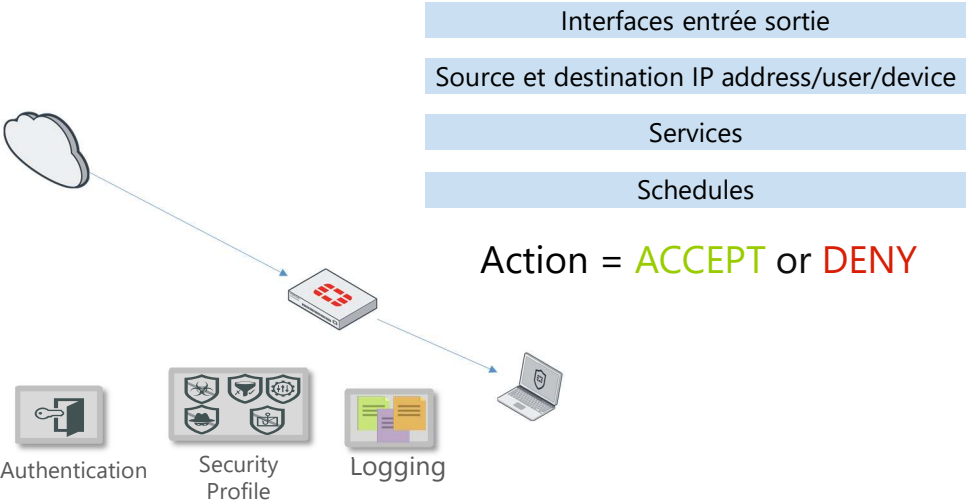
Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
port2 - port3 (1 - 2)							
1	test	REMOTE_INTERNAL	all	always	ALL	Accept	Enabled
2	Test2	all	all	always	ALL	Accept	Enabled
port3 - port1 (3 - 6)							
3	Remote	STUDENT	REMOTE_ETH1	always	ALL	Accept	Enabled
4	Web_Access	all	all	always	Web Access	Accept	Enabled
5	Full_Access	all	all	always	ALL	Accept	Enabled
6	FTP_Deny	all	all	always	FTP FTP_GET FTP_PUT	Deny	Disabled
Implicit (7 - 7)							
7	Implicit Deny	all	all	always	ALL	Deny	

Une formation
Alphorm.com

Implicit Deny



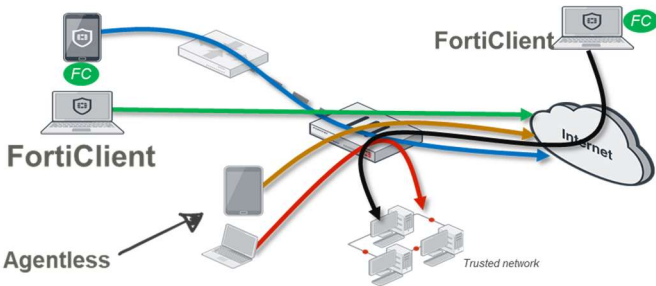
Critères et actions



Une formation
Alphorm.com

Critères et actions

Critère par Source	Critère par destination
Source adresse (IP, réseau,FQDN,Géographie,...)	Destination adresse (IP,réseau,FQDN,Géographie,...)
Source Utilisateur (Local,distant,FSSO,Certificat)	Géographiquement en se basant sur la base de données mise à jour par Fortiguard
Source machine	





Une formation
Alphorm.com

Configurer et gérer les stratégies



Mohamed Anass EDDIK

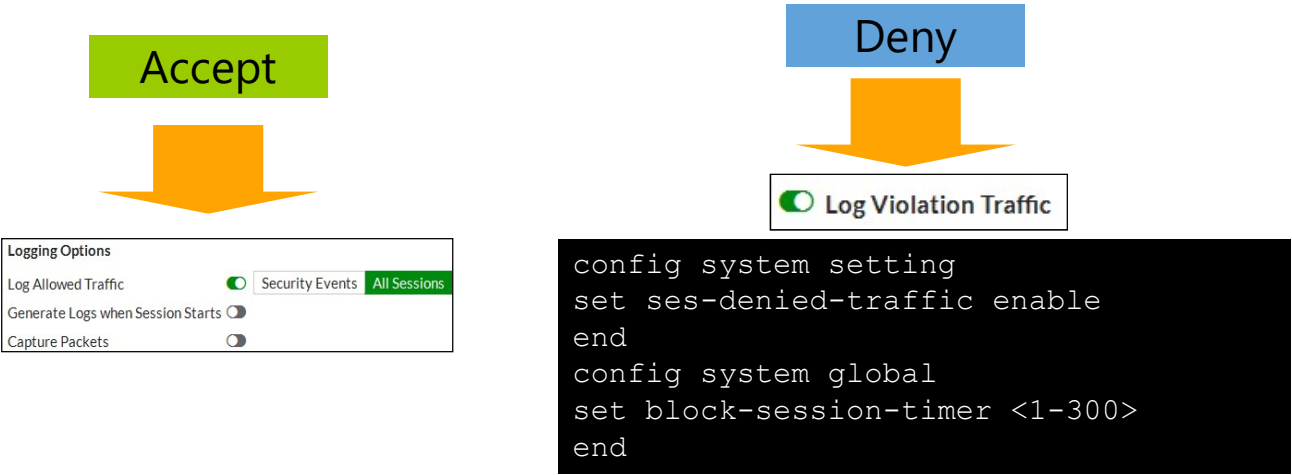


Une formation
Alphorm.com

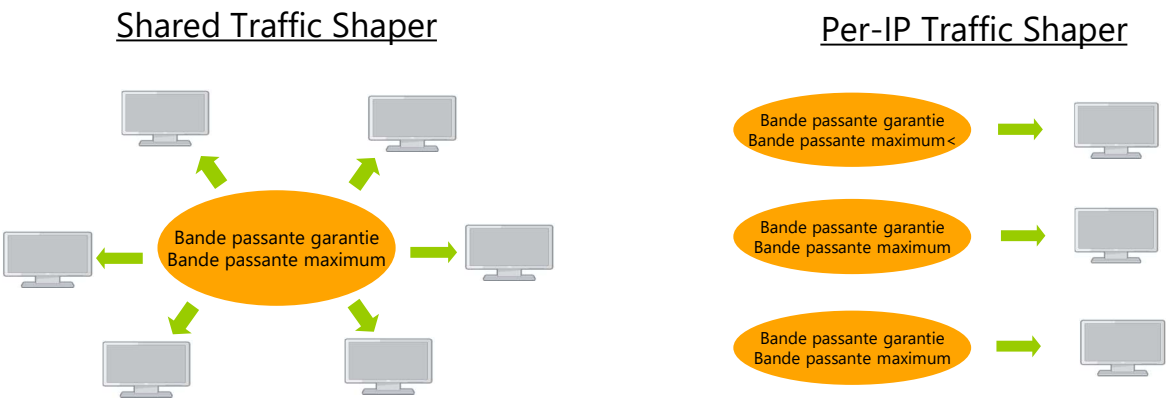
Plan

Stratégie du pare-feu
Traffic Shaper
Lab

Stratégie du pare-feu



Traffic Shapers





Une formation
Alphorm.com



Une formation
Alphorm.com

Surveiller les stratégies du Fortigate



Mohamed Anass EDDIK



Monitoring Pare-Feu

Recherche correspondant à la politique en fonction de critères d'entrée :

- Interface source
- Protocole
- Nécessite des critères d'entrée plus granulaires
- Adresse IP source
- IP / FQDN de destination

Une formation
Alphorm.com



Une formation
Alphorm.com





Configurer Firewall Policy NAT



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

NAT ET PAT
Firewall Policy SNAT
Firewall Policy DNAT
Lab

Une formation
Alphorm.com



Une formation
Alphorm.com

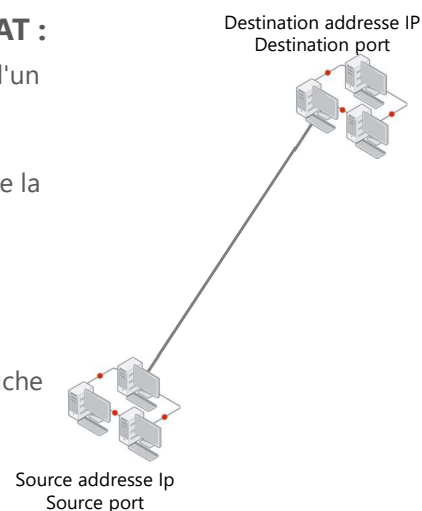
NAT ET PAT

Network Address Translation – NAT :

- Changer une adresse de couche IP d'un paquet
- Certains protocoles tels que SIP ont également des adresses au niveau de la couche applicatif, nécessitant des session helpers/ Proxies
- SNAT et DNAT

Port Address Translation-PAT :

- Changer le numéro de port de la couche IP d'un paquet



Une formation
Alphorm.com

Firewall Policy NAT ?

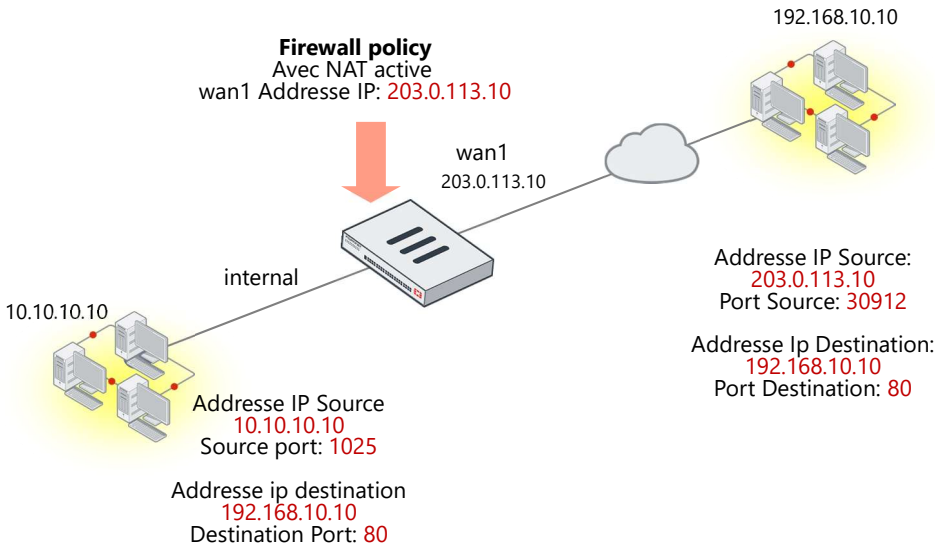
Le NAT source et le NAT de destination doivent être configurés pour chaque stratégie de pare-feu

Le NAT source-SNAT- utilise l'adresse d'interface sortante ou le pool IP configuré

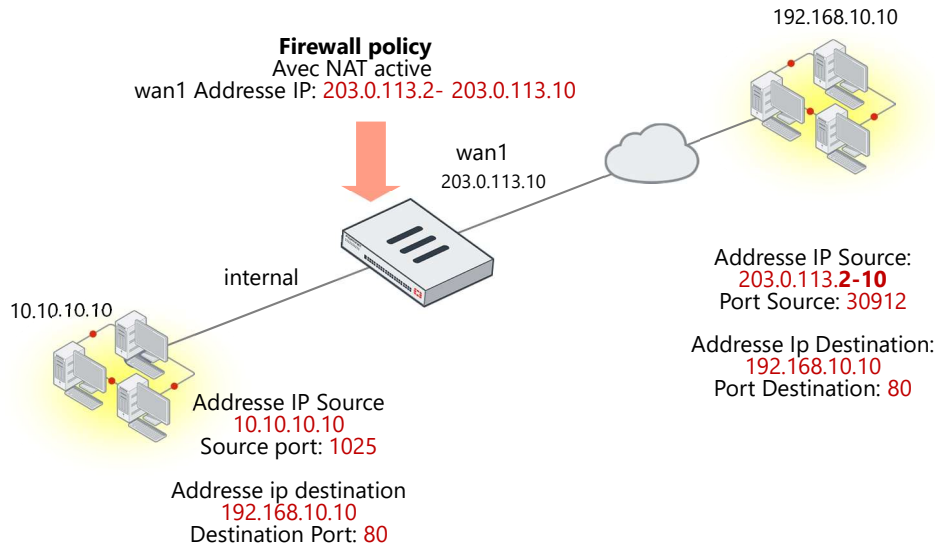
Le NAT de destination –DNAT- utilise l'adresse IP virtuelle configurée comme adresse de destination



SNAT : Many-to-One

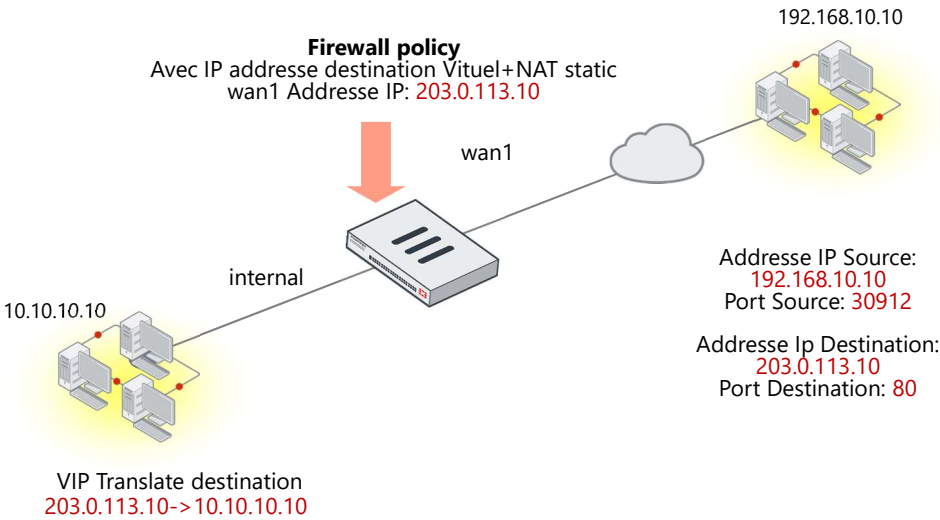


SNAT : IP POOL





DNAT : VIP





Une formation
Alphorm.com

Configurer Central NAT



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Activer Central NAT
Central SNAT
Central DNAT
Lab



Activé/désactive Central NAT

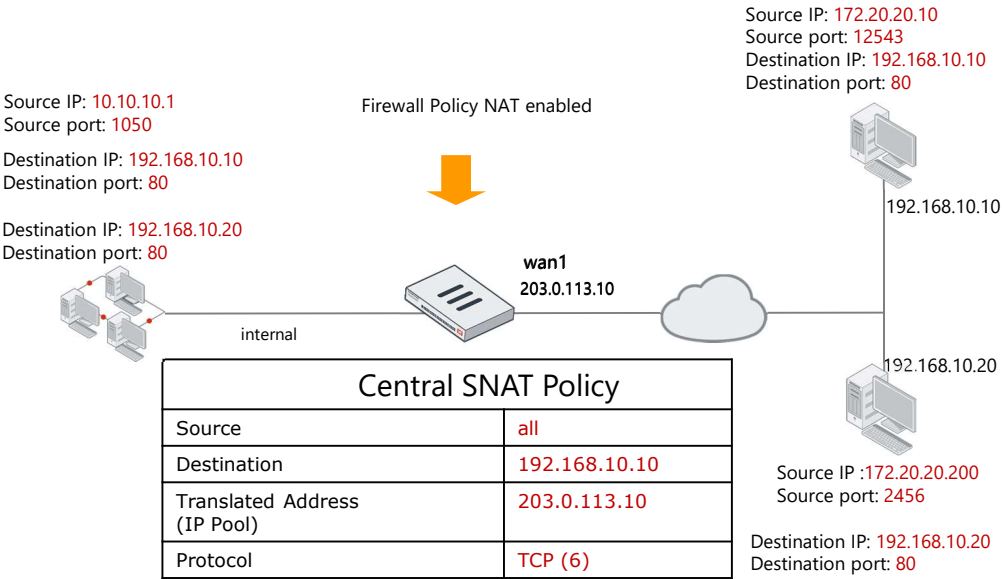
Activation en mode CLI (UNIQUEMENT) :
Il faut désactiver l'IP pool et le VIP :

```
config system settings
set central-nat {enable|disable}
end
```

Après activation 2 options sur interface graphique

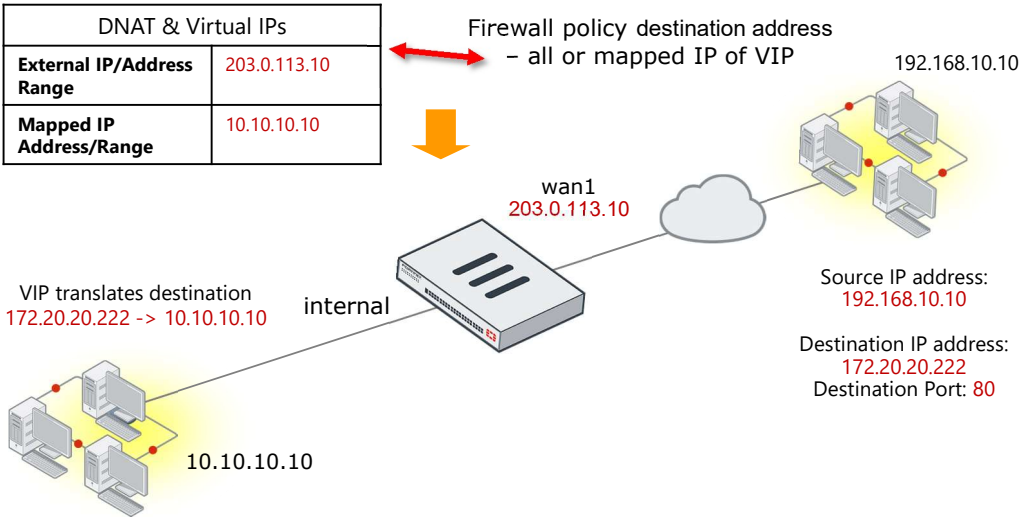


Central SNAT





Central DNAT



Une formation
Alphorm.com



Une formation
Alphorm.com



Comprendre session helpers et sessions



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Session Helpers

Sessions

Lab

Une formation
Alphorm.com



NAT64 et NAT46

NAT64 et NAT 46

Un mécanisme qui permet aux hôtes adressés par IPv6 de communiquer avec les hôtes adressés IPv4 et la réserve

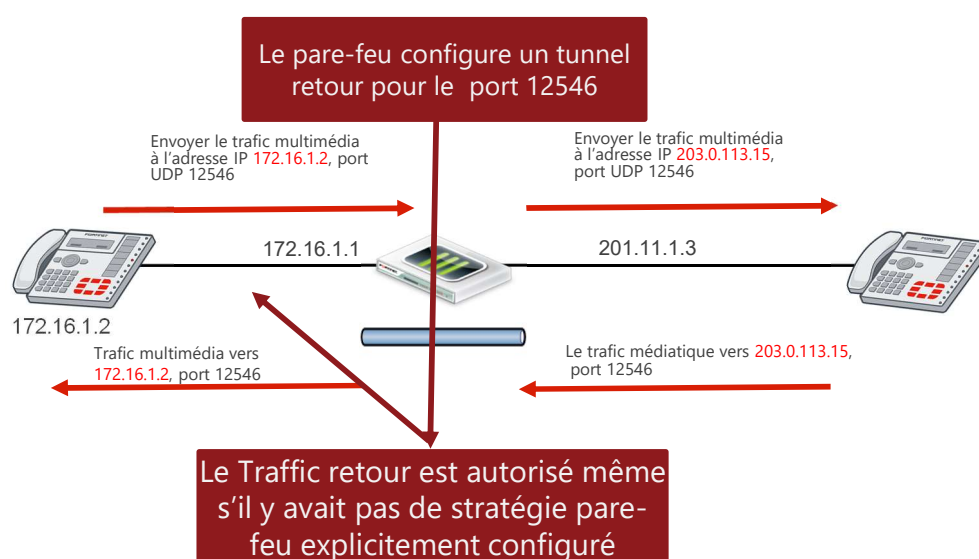
Nat66

NAT entre deux réseaux IPv6

Une formation
Alphorm.com



Session Helpers



Une formation
Alphorm.com



Table de session

La table de session stocke les informations sur les sessions comme suit :

- Adresses source et de destination, paires de numéros de port, état, délai d'attente
- Interfaces source et destination
- Actions NAT source et de destination

Quand la table de session est pleine, réduire le TTL peut beaucoup aider

Une formation
Alphorm.com



Diagnose sys session

Effacer tout filtre précédent

diagnose sys session filter clear

Définir le filtre

diagnose sys session filter ?

dport	destination port
dst	destination IP address
policy	policy id
sport	source port
src	source ip address

Répertorie toutes les entrées correspondant au filtre configuré

diagnose sys session list

Purger toutes les entrées correspondant au filtre configuré

diagnose sys session clear

Une formation
Alphorm.com



Diagnose sys session

```
# diagnose sys session filter dst 10.200.1.254
# diag sys session filter dport 80
# diag sys session list

session info: proto=6 proto_state=05 duration=2 expire=78 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_lux=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=538/6/1 reply=5407/6/0 tuples=2 speed(Bps/kbps):2596/20
orgin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwv=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64624->10.200.1.254:80(10.200.1.1:64624)
hook=pre dir=reply act=dnat 10.200.1.254:80->10.200.1.1:64624(10.0.1.10:64624)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00023a22 tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```



Etat du TCP, ICMP et UDP

Etat TCP

TCP State	Value	Expire Timer in sec (default)
NONE	0	10
ESTABLISHED	1	3600
SYN_SENT	2	120
SYN & SYN/ACK	3	60
FIN_WAIT	4	120
TIME_WAIT	5	120
CLOSE	6	10
CLOSE_WAIT	7	120
LAST_ACK	8	30
LISTEN	9	120

ETAT UDP

UDP State	Value
UDP traffic one way only	0
UDP traffic both ways	1

Etat ICMP

proto_state Toujours 00



Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir les différentes méthodes d'authentification



Mohamed Anass EDDIK



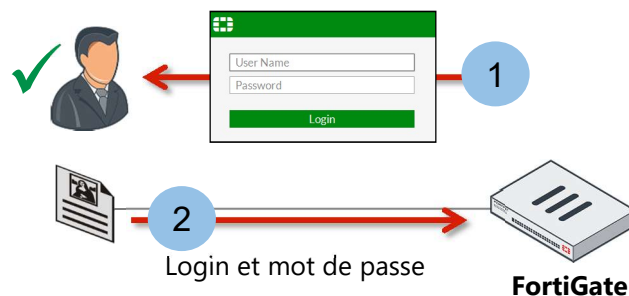
Plan

- Authentification par mot de passe local
- Authentification par mot de passe basé sur le serveur externe
- Deux facteurs d'authentification
- Méthode d'authentification active/passive

Une formation
Alphorm.com



Authentification locale



Compte utilisateur enregistré localement

Une formation
Alphorm.com

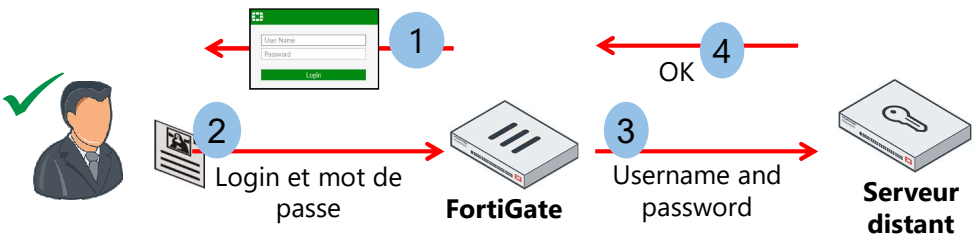


Authentification à distance

Un administrateur peut :

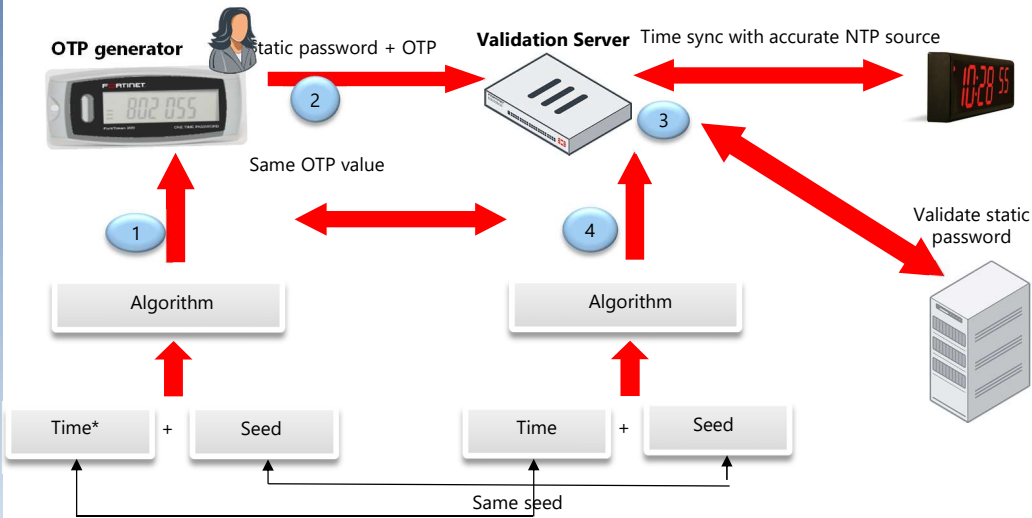
- Créez un compte pour l'utilisateur localement et spécifiez le serveur pour vérifier le mot de passe ou
- Ajouter le serveur d'authentification à un groupe d'utilisateurs
- Tous les utilisateurs de ce serveur deviennent membres du groupe.

Une formation
Alphorm.com



2 facteurs d'authentification

Une formation
Alphorm.com





Authentification active/passive

Active :

L'utilisateur reçoit une invite de connexion

Doit entrer manuellement les informations d'identification pour s'authentifier

LDAP, RADIUS, Local et TACACS +

Passive :

L'utilisateur ne reçoit pas d'invite de connexion

Les informations d'identification sont déterminées automatiquement

FSSO, RSO et NTLM

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Configurer un serveur d'authentification



Mohamed Anass EDDIK



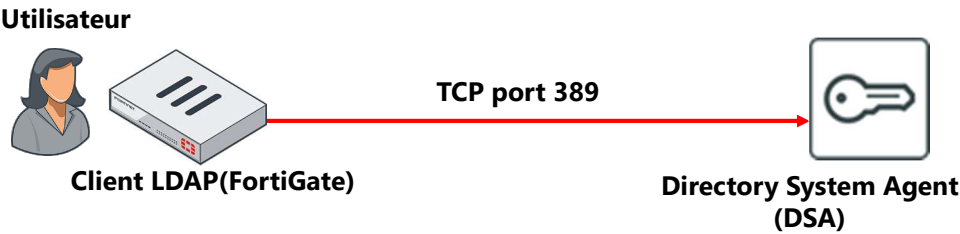
Une formation
Alphorm.com

Plan

- Comprendre le LDAP
- Tester LDAP
- Comprendre le RADIUS
- Tester RADIUS
- Lab



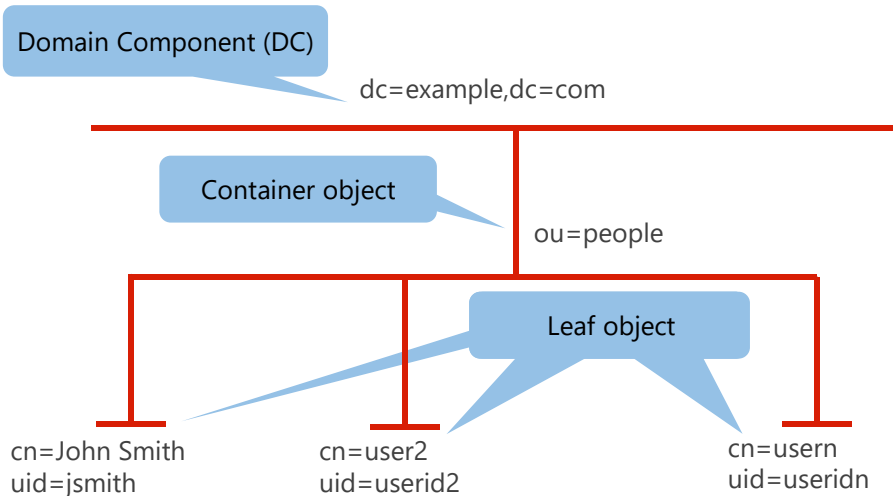
Comprendre le LDAP



Lightweight Directory Access Protocol (LDAP)



Comprendre le LDAP





Tester LDAP

```
diagnose test authserver <server_name>  
<username> <password>
```

Example :

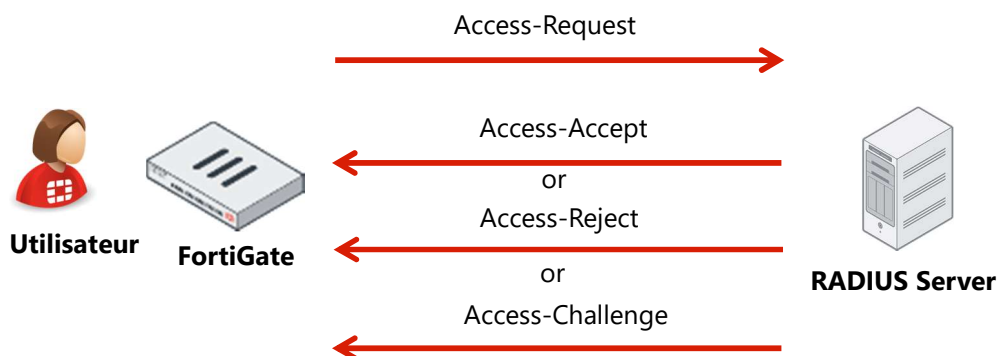
```
# diagnose test authserver ldap ADserver aduser1  
Training!  
  
authenticate 'aduser1' against 'ADserver' succeeded!  
Group membership(s) - CN=AD-  
users,OU=Training,DC=trainingAD,DC=training,DC=lab
```

Une formation
Alphorm.com



Comprendre le RADIUS

RADIUS est un protocole standard qui fournit des services AAA



Une formation
Alphorm.com



Tester RADIUS

```
diagnose test authserver radius  
<server_name> <scheme> <user> <password>
```

Example:

```
# diagnose test authserver radius FortiAuth-RADIUS  
pap student fortinet
```

```
authenticate 'aduser1' against 'pap' succeeded,  
server=primary assigned_rad_session_id=810153440  
session_timeout=0 secs!  
Group membership(s) - remote-AD-admins
```

Une formation
Alphorm.com



Une formation
Alphorm.com





Créer un portail captif sur Fortigate



Mohamed Anass EDDIK

Une formation
Alphorm.com



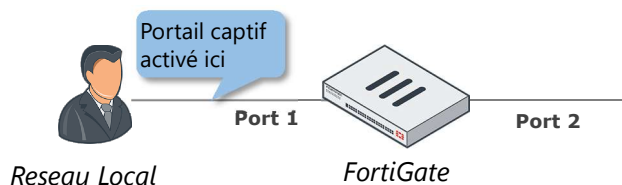
Plan

- Portail Captif
- Mentions légales de service
- Personnalisation des messages du portail
- Délai d'authentification
- Lab

Une formation
Alphorm.com



Portail Captif



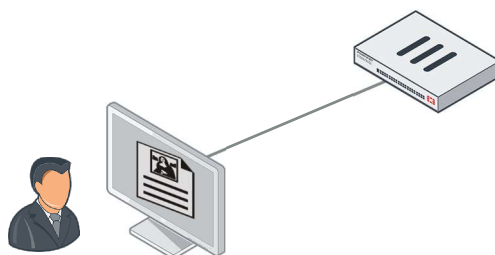
Il peut héberger le portail captif sur un FortiGate ou un serveur d'authentification externe

Une formation
Alphorm.com

Mentions légales de service

Affiche la page termes et contrat de non-responsabilité avant que l'utilisateur n'authentifie
L'utilisateur doit accepter la clause de non-responsabilité pour procéder
Une fois accepté, l'utilisateur est dirigé vers la destination d'origine

```
#config firewall policy
edit <policy_id>
set disclaimer enable
end
```





Messages du portail

System > Replacement Messages

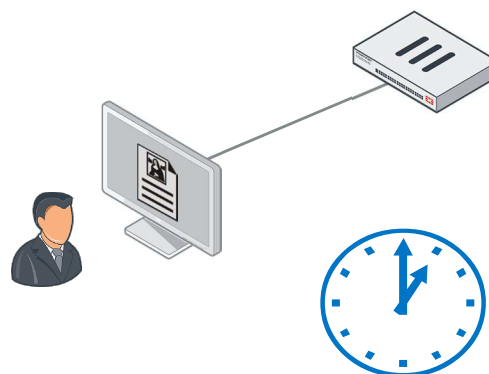
```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=
<style type="text/css">
html,body{
height:100%;
padding:0;
margin:0;
}.oc{
display:table;
width:100%;
height:100%;
}.ic{
display:table-cell;
vertical-align:middle;
height:100%;
}form{
display:block;
background:#ccc;
border:2px solid red;
padding:0 0 25px 0;
width:500px;
font-family:helvetica,sans-serif;
font-size:12px;
```

Une formation
Alphorm.com



Délai d'authentification

```
#config user setting
set auth-timeout-type [idle-timeout|hard-timeout|new-session]
end
```



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Comprendre les logs



Mohamed Anass EDDIK



Plan

Processus du logging

Type de log

Log severity

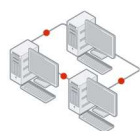
Présentation du message de journal

L'effet du logging sur les performances

Lab

Une formation
Alphorm
com

Processus du logging



L'intérêt des logs:

- surveiller les volumes de trafic réseau et Internet
- diagnostiquer les problèmes
- établir des lignes de base normales pour reconnaître les anomalies et les tendances

NTP SERVEUR est recommandé



Une formation
Alphorm.com

Type de log

Traffic	Event	Security
Forward	Endpoint Control	Application Control
Local	High Availability	Antivirus
Sniffer	System	Data Leak Prevention (DLP)
	User	Anti-Spam
	Router	Web Filter
	VPN	Intrusion Prevention System (IPS)
	WAD	Anomaly (DoS-policy)
	Wireless	WAF

Les journaux d'optimisation WAN se trouvent dans les journaux de trafic



Une formation
Alphorm.com

Log severity

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality affected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information



Log messages

Log header (similaire dans tous les journaux)

```
date=2016-06-14 time=12:05:28 logid=0316013056 type=utm  
subtype=webfilter eventtype=ftgd_blk level=warning vd=root
```

Log body (varie selon le type du journal)

```
policyid=1 sessionid=10879 user="" srcip=10.0.1.10  
srcport=60952 srcintf="port3" dstip=52.84.14.233 dstport=80  
dstintf="port1" proto=6 service="HTTP" hostname="miniclip.com"  
profile="default" action=blocked reqtype=direct  
url="/favicon.ico" sentbyte=297 rcvdbyte=0 direction=outgoing  
msg="URL belongs to a denied category in policy" method=domain  
cat=20 catdesc="Games" crscore=30 crlevel=high
```

Une formation
Alphorm.com



Logging sur les performances

Plus de journaux = plus de CPU, de mémoire et d'espace disque

En fonction de votre trafic et des paramètres de journalisation activés, vos journaux de trafic se gonflent et affectent les performances de votre pare-feu

Les journaux de trafic enregistrent chaque session :
informations supplémentaires pour le dépannage
quelques événements UTM
plus intensive du système

Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer les logs



Mohamed Anass EDDIK



Plan

Stockage des logs

Quelle configuration génère des logs

Comportement lorsque le disque local est plein

Stockage des logs FortiAnalyzer et Fortimanager

FortiAnalyzer n'est pas disponible ?

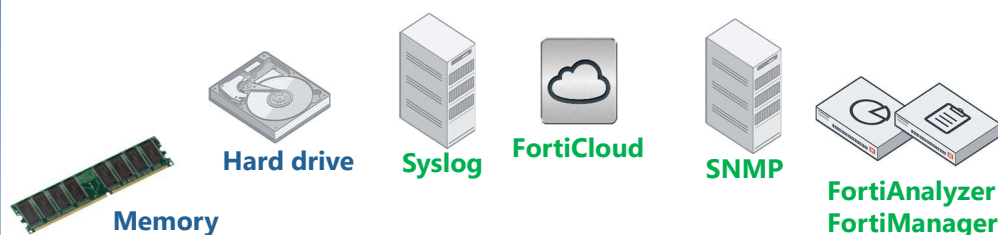
Reliable Logging et OFTPS

Lab

Une formation
Alphorm.com



Stockage des logs



Local logging

Remote logging

Une formation
Alphorm.com



Une formation
Alphorm.com

Génération des logs

Policy Log Setting	Security Profiles	Behavior
Log Allowed Traffic = disabled	Disabled	Pas de Forward Traffic ou de Security Logs
Log Allowed Traffic = disabled	Enabled	Pas de Forward Traffic ou de Security Logs
Security Events = enabled	Disabled	Pas de Forward Traffic ou de Security Logs
Security Events = enabled	Enabled	Les événements de logs de sécurité s'affichent dans le log de trafic avancé et le journal de sécurité. Un forward traffic log génère pour des paquets provoquant un événement de sécurité.
All Sessions = enabled	Disabled	Un journal de trafic à terme génère pour chaque session unique.
All Sessions = disabled	Enabled	Les événements de journal de sécurité s'affichent dans le journal de trafic avancé et le journal de sécurité. Un journal de trafic vers l'avant génère pour chaque session unique



Une formation
Alphorm.com

Le disque local est plein

Par défaut, quand le disque est plein, les anciens logs vont être écrasés

C'est configurable – il peut être changé et arrêter le logging si le disque est plein

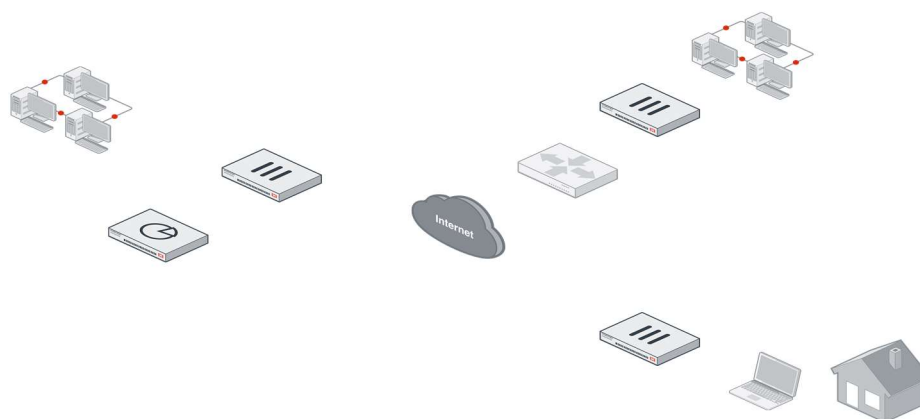
Le Fortigate affiche les warnings avant que le disque soit plein :

- Premier warning a 75%
- Deuxième warning a 90%
- Dernier warning a 95%

```
# configure log disk setting
set diskfull [overwrite | nolog]
set full-first-warning-threshold <1-98>
set full-second-warning-threshold <2-99>
set full-final-warning-threshold <3-100>
```



FortiAnalyzer et Fortimanager



Une formation
Alphorm.com



FortiAnalyzer n'est pas UP?

Le process **miglogd** de Fortigate cache les logs sur Fortigate quand FortiAnalyzer n'est pas connecté
Quand la valeur du cache est atteinte **miglogd** va arrêter de recevoir les logs

```
Local-FortiGate # diagnose test application miglogd 6
mem=0, disk=22465, alert=0, alarm=0, sys=0, faz=22488, webt=0
interface-missed=0
Queues Total in miglogds: maxium=7346 current:0
global log dev statistics:
faz 0: sent=22484, failed=0, cached=0, 123slowpath=178, relayed=0
```

Maximum cache size and current cache size

If there are bursts or link is overloaded, failed increases

```
Local-FortiGate # diagnose log kernel-stats
fgtlog: 2
fgtlog 0: total-log=3, failed-log=0 log-in-queue=0
fgtlog 1: total-log=26683, failed-log=0 log-in-queue=0
```

If queue is full, failed-log value increases

Une formation
Alphorm.com



Reliable Logging et OFTPS

Changement des logs transport de l'UDP vers le TCP

Le TCP fournit un transfert de données fiable, il garantit que les données transférées restent intactes et arrivent dans le même ordre dans lequel elles ont été envoyées

Si le logging est activé sur FortiAnalyzer au niveau de l'interface le reliable logging est auto-activé

Si vous utilisez le reliable logging, vous pouvez utiliser le SSL-secured OFTP (OFTPS)

```
# config log fortianalyzer setting
set status enable
set enc-algorithm [high-medium | high | low | disable |
set reliable enable
end
```

Reliable logging
must be enabled to
use OFTPs

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Surveiller les logs



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Filtrage Log

Confidentialité au niveau des logs

Backup logs

SNMP

Lab



Filtrage Log

On peut configurer le filtrage log pour spécifier quel log configurer, vous pouvez configurer jusqu'à 4 syslog :

```
Config log [syslogd | syslogd2 | syslogd3 | syslogd4] filter
```

- Filters include:

- Severity <level>
- Forward traffic [enable/disable]
- Local traffic [enable/disable]
- Multicast traffic [enable/disable]
- Sniffer traffic [enable/disable]
- Anomaly [enable/disable]
- VOIP [enable/disable]
- DLP archive [enable/disable]
- DNS [enable/disable]
- Filter [string]
- Filter type [include | exclude]

Une formation
Alphorm.com



Confidentialité

Il y a des loi qui oblige que le nom d'utilisateur soit confidentiel (GDPR)

```
Config log setting  
set user-anonymize enable  
end
```

```
date=2017-11-26 time=14:45:16 logid=0317013312 type=utm subtype=webfilter  
eventtype=ftgd allow level=notice vd="root" policyid=2 identidx=1  
sessionid=31232959 user="anonymous" group="ldap_users" srcip=192.168.1.24  
srcport=63355 srcintf="port2" dstip=66.171.121.44 dstport=80 dstintf="port1"  
service="http" hostname="www.fortinet.com" profiletype="Webfilter_Profile"  
profile="default" status="passthrough" reqtype="direct" url="/" sentbyte=304  
rcvdbyte=60135 msg="URL belongs to an allowed category in policy" method=domain  
class=0 cat=140 catdesc="custom1"
```

Une formation
Alphorm.com



Backup logs

Trois méthodes de sauvegarde des journaux (copie des fichiers journaux de la base de données à l'emplacement spécifié) :

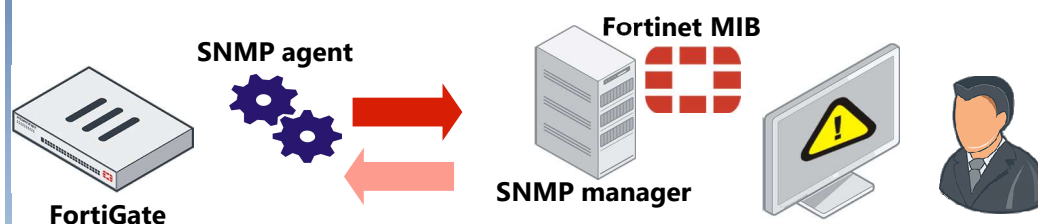
- Ftp
- Tftp
- Usb

```
# execute backup disk alllogs usb  
  
# execute backup disk log usb <log_type>
```

Une formation
Alphorm.com



SNMP



Une formation
Alphorm.com

FortiGate SNMP MIB

[Download FortiGate MIB File](#)
[Download Fortinet Core MIB File](#)



Une formation
Alphorm.com



Une formation
Alphorm.com

Créer des rapports



Mohamed Anass EDDIK



Plan

Rapport d'apprentissage

Rapport de sécurité

Lab

Une formation
Alphorm.com



Rapport d'apprentissage

Rapport d'apprentissage : rapport d'apprentissage sur l'évaluation des cybermenaces

Action = LEARN sur la politique de pare-feu

Capture des données sur tous les vecteurs de trafic et de sécurité

Recueil et consigne des données significatives à des fins de recommandation, notamment :

- Méthodologie de déploiement
- Résumé

Productivité de l'utilisateur (*Utilisation de l'application, utilisation du Web*)

Une formation
Alphorm.com



Rapport d'apprentissage

Rapport local : rapport de sécurité

Fortigate peut :

- Exécuter le rapport à la demande, quotidiennement ou hebdomadaire
- Envoyer un rapport

Compile l'activité des fonctionnalités de sécurité à partir de différents journaux liés à la sécurité

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Gérer les certificats



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Pourquoi Fortigate utilise le certificat Digital ?

Utiliser le certificat pour identifier une personne ou un équipement

Fortigate vérifie la signature digital

Authentification d'utilisateur basée sur un certificat

Authentification de serveur Web basée sur un certificat

Lab



Une formation
Alphorm.com

FG et le certificat digital

Inspection

Le fortigate émet temporairement un certificat pour une inspection full ssl
Fortigate peut inspecter les certificats pour être sûr qu'ils sont valides et qu'on peut leur faire confiance

Privacy

Fortigate utilise le certificat pour créer des connexions ssl avec d'autres équipements comme le fortiguard

Authentication

Les utilisateurs qui possèdent le certificat digital peuvent se connecter au fortigate

Les administrateurs peuvent utiliser le certificat comme un deuxième facteur d'authentification pour se connecter au fortigate

Le certificat pour une personne ou un équipement

Digital certificat ?

Une identité numérique produite et signée par une autorité de certification

Fortigate utilise le X.509v3 standard certificat

Les champs sujet et nom alternatif de sujet du certificat identifient l'appareil ou la personne associée au certificat

General Details Certification Path	
Show: <All>	
Field	Value
Version	V3
Serial number	01 86 a2
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	FortiAuthCA
Valid from	Tuesday, November 3, 2015 1...
Valid to	Wednesday, November 2, 201...
Subject	aduser1
Public key	RSA (2048 Bits)
Subject Key Identifier	07 38 4a 09 c1 a9 fd 45 79 52 ...
Authority Key Identifier	KeyID=a1 4c d6 c9 0a f4 95 9...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	31 a6 48 97 fc 66 ad a3 b5 27 ...

La confiance des certificats

Fortigate fait une panoplie de check avant de faire confiance au certificat :

Le check de la révocation

La possession d'un certificat par un CA

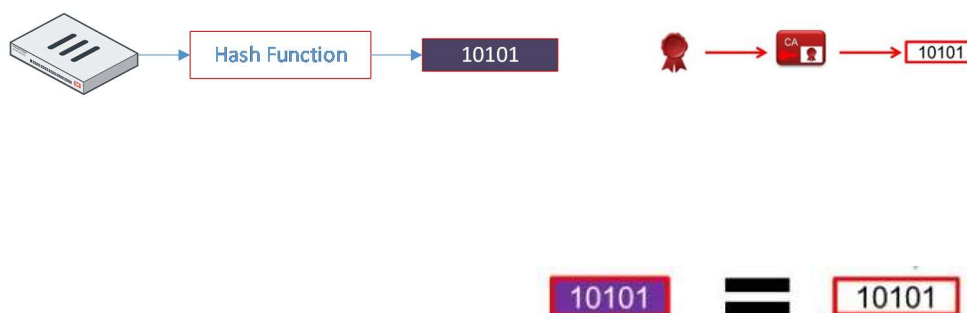
Date de validité

Validation de la signature digital

General Details Certification Path	
Show: <All>	
Field	Value
Version	V3
Serial number	01 86 a2
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	FortiAuthCA
Valid from	Tuesday, November 3, 2015 1...
Valid to	Wednesday, November 2, 201...
Subject	aduser1
Public key	RSA (2048 Bits)
Subject Key Identifier	07 38 4a 09 c1 a9 fd 45 79 52 ...
Authority Key Identifier	KeyID=a1 4c d6 c9 0a f4 95 9...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	31 a6 48 97 fc 66 ad a3 b5 27 ...



Fortigate vérifie la signature digital

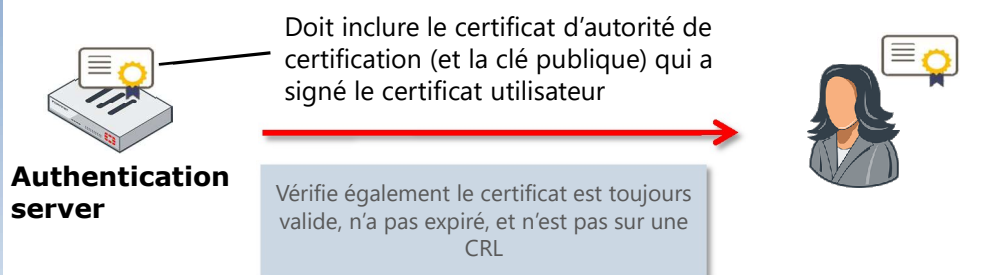




Authentification d'utilisateur

Le certificat utilisateur comprend:

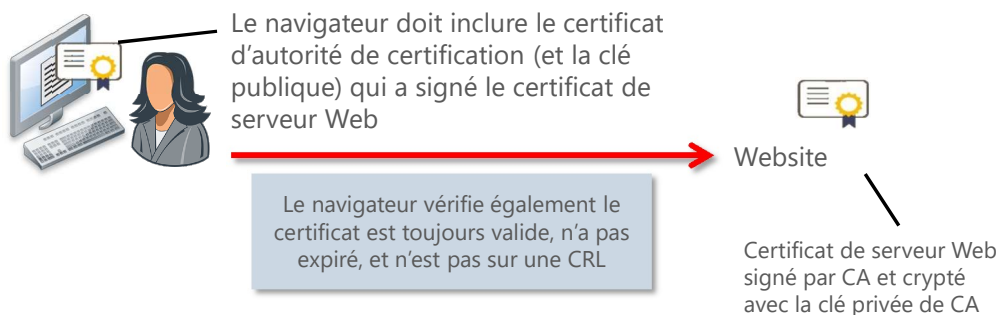
Signature de l'autorité de certification, qui est cryptée à l'aide de la clé privée de l'AC
Clé publique de l'utilisateur



Une formation
Alphorm.com



Authentification de serveur



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer l'authentification à la base du certificat



Mohamed Anass EDDIK



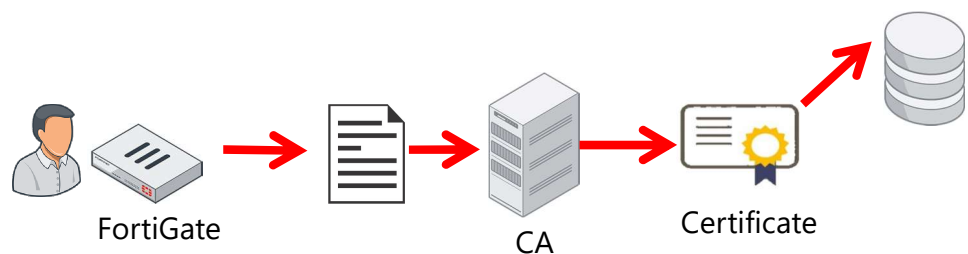
Plan

Génération du CSR pour un CA
Backup et restauration du Certificat
Configuration du certificat pour
VDOM et Global
Lab

Une formation
Alphorm.com

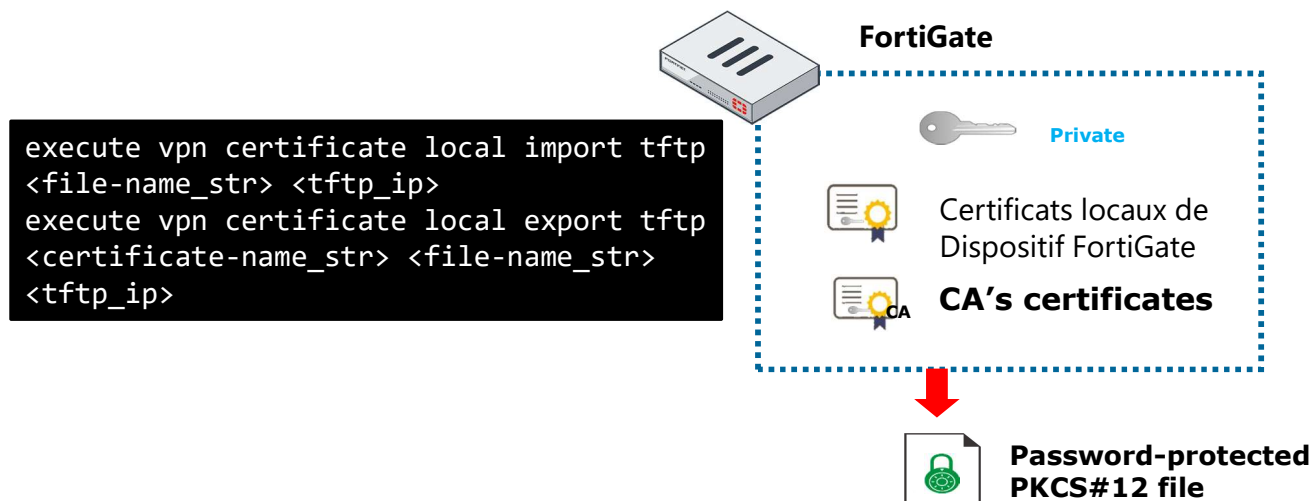


Génération du CSR pour un CA



Une formation
Alphorm.com

Backup et restauration du Certificat



Certificat pour VDOM et Global

La configuration CA et certificate local sont disponibles par VDOM

```
config certificate local  
edit Fortinet_Factory  
end  
end  
set range <global/vdom>  
set source <factory/user/fortiguard>
```



Une formation
Alphorm.com



Une formation
Alphorm.com

Utiliser le Certificat SSL



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Certificat SSL auto-signé
SSL entre Fortigate et un web serveur
Inspection SSL complète en sortie
Certificat SSL non approuvé
Inspection SSL complète et
HSTS/HPKP
Lab



Une formation
Alphorm.com

Certificats SSL auto-signés

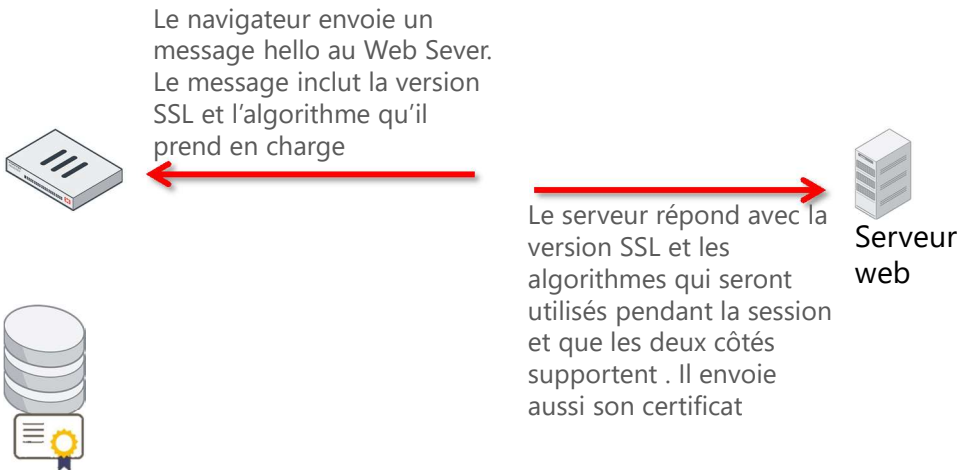


Par défaut, FortiGate utilise un certificat SSL auto-signé :
Non répertorié avec une autorité de certification approuvée, par défaut, pas de confiance



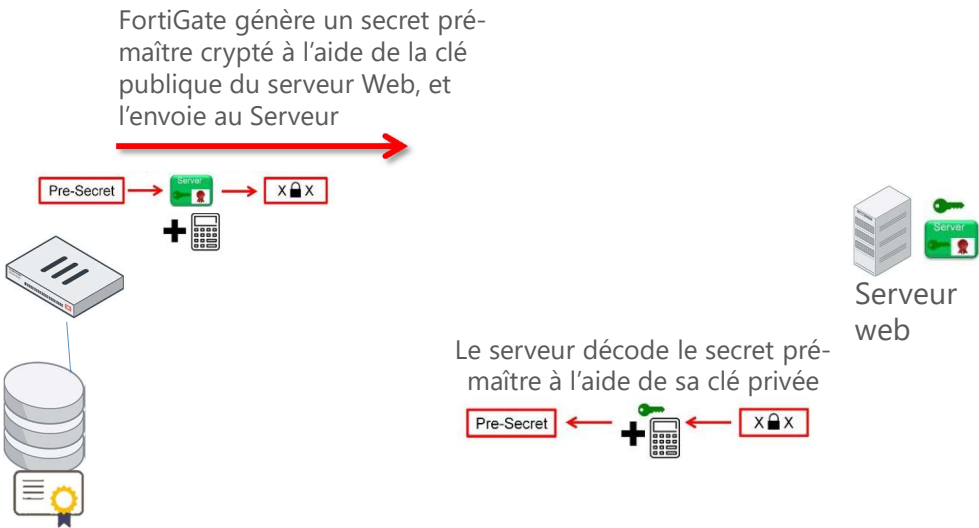
SSL Fortigate et web serveur

Partie 1



SSL Fortigate et web serveur

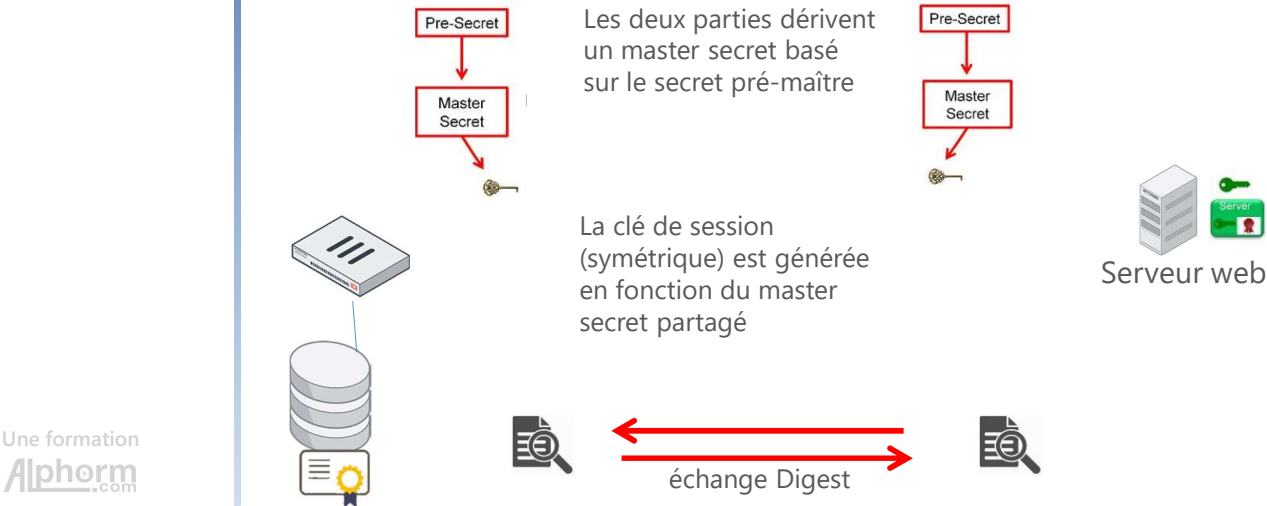
Parie 2





SSL Fortigate et web serveur

Partie 3

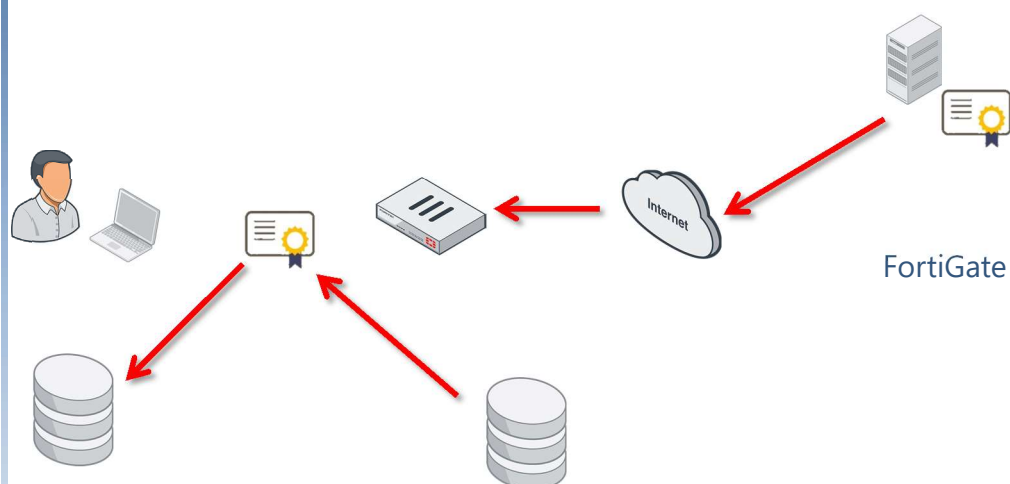


Inspection full SSL en sortie





Certificat SSL non approuvé



Une formation
Alphorm.com



Full ssl et HSTS/HPKP

Certains serveurs Web implémentent des mesures de sécurité pour atténuer les attaques MITM

HTTP STRICT TRANSPORT SECURITY (HSTS)

Un mécanisme par lequel les sites Web sont accessibles uniquement via des connexions sécurisées

http public key pinning (HPKP) : associe ou épingle une clé publique à un serveur Web spécifique



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Utiliser le web et DNS filtering



Mohamed Anass EDDIK

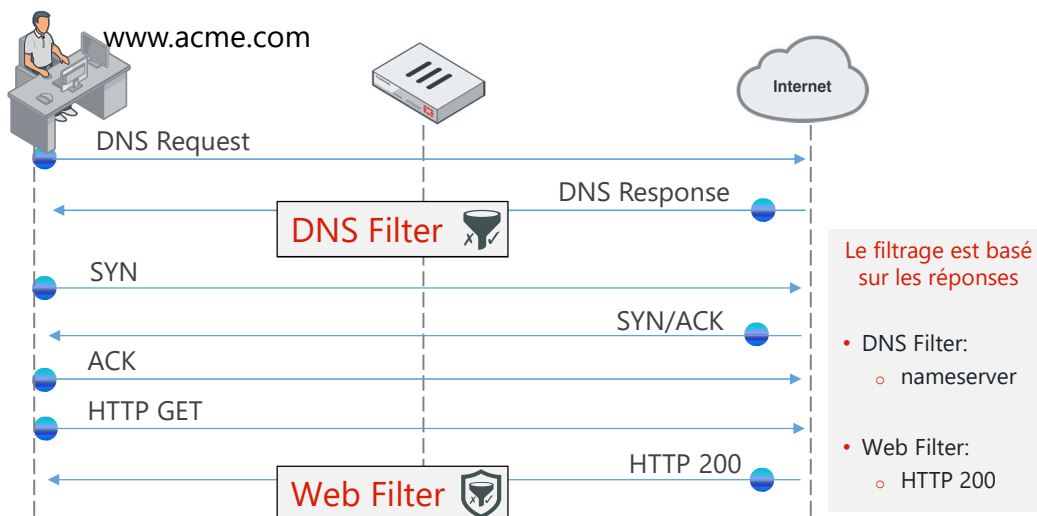


Plan

Quand le filtrage s'active ?
Types d'inspection de filtrage Web
Fonctionnement des Catégories
Filtre Web FortiGuard catégorie action :
Authentifier
URL Filtering
DNS Filtering
Lab

Une formation
Alphorm.com

Quand le filtrage s'active ?





Inspection de filtrage Web

Proxy-based

- Le trafic est mis en cache
- Prend en charge toutes les fonctionnalités possibles de filtrage de sites Web

Flow-based

- Débit plus élevé que le proxy
- Pas de mise en cache des données (en transmission)
- Ne prend pas en charge toutes les fonctionnalités de filtrage du site

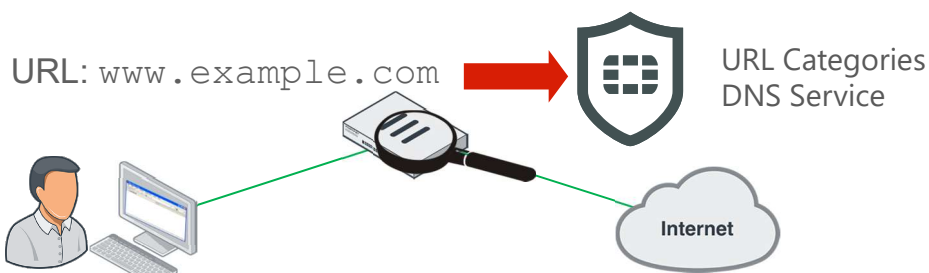
DNS-based

- Très léger (faible utilisation du CPU et de la mémoire)
- Pas aussi granulaire que le flux ou le proxy (nom d'hôte et adresse IP uniquement)
- Ne prend pas en charge la plupart des fonctionnalités de filtrage du site

Une formation
Alphorm.com



Les Catégories



Categories action:

Web Filter	DNS Filter
Allow	Allow
Block	Block
Monitor	Monitor
Warning	
Authenticate	

Une formation
Alphorm.com



Catégorie action : authentifier

Bandwidth Consuming

- File Sharing and Storage
- Freeware and Software Downloads
- Internet Radio and TV
- Internet Telephony
- Peer-to-peer File Sharing
- Streaming Media and Download**

WebFilter_Group



1. Define Users and Group

2. Set Action = Authenticate

3. Select User_Group

Web Filter Block Override

Username:

Password:

Continue

Warning Interval

5 Minute(s)

Selected User Groups

WebFilter_Users

OK Cancel

www.youtube.com



Une formation
Alphorm.com

URL Filtering

Security Profiles

- AntiVirus
- Web Filter**
- DNS Filter
- Application Control
- Cloud Access Security Inspection
- Intrusion Protection
- Data Leak Prevention

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

Create Edit Delete

URL	Type	Action	Status	Referrer
*.something\.[org biz]	Reg. Expression	Exempt	Enable	
somewhere.*	Wildcard	Monitor	Enable	
www.somesite.com/someURL	Simple	Block	Enable	✓

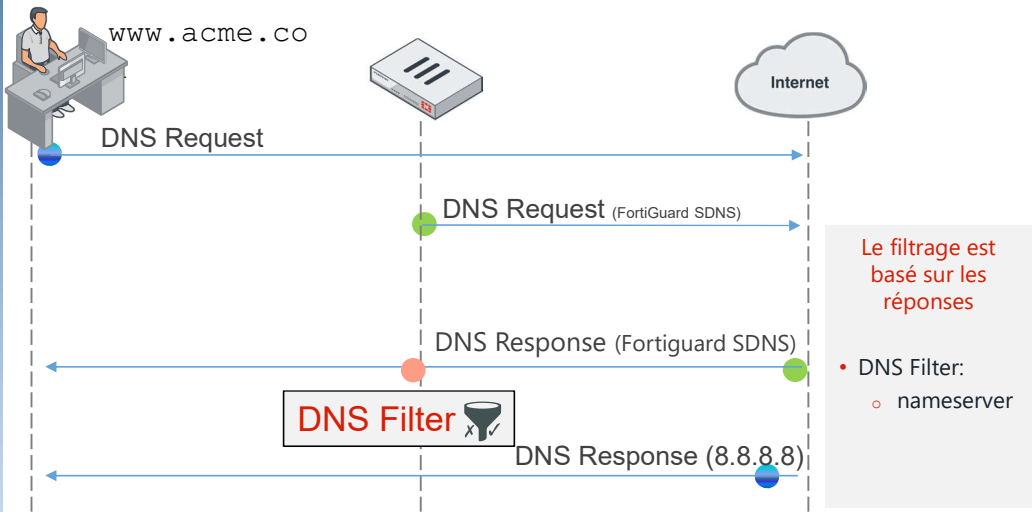
URL: `www.somesite.com/someurl`

Block

Une formation
Alphorm.com



DNS Filtering



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir les modes d'inspection



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Flow based inspection
NGFW Mode
Proxy based inspection
Lab



Flow based inspection

Mode d'inspection par défaut

Utilise la correspondance de modèle d'approche de filtre direct (DFA) à passage unique pour identifier les attaques éventuelles de menaces

Le fichier est scanné sur une base de flux en passant par FortiGate

Numérisation plus rapide

Une formation
Alphorm.com



NGFW Mode

Seulement disponible en mode flow based :

Comprend deux modes:

Basé sur le profil: nécessite l'administrateur pour créer et configurer application et le filtrage Web, puis les appliquer à la stratégie sélectionnée

Basé sur les stratégies: permet aux administrateurs d'appliquer le contrôle d'application et le filtrage Web directement à une stratégie de pare-feu, sans avoir à configurer des profils de filtrage Web

Une formation
Alphorm.com



Proxy based inspection

Inspection plus approfondie
Ajoute de la latence (le contenu complet est analysé)
Deux connexions TCP
Du client à Fortgate agissant en tant que serveur proxy
De FortiGate au serveur
La communication est terminée sur la couche 4
Plus de ressources intensives
Proviennent d'un niveau plus élevé de protection contre les menaces

Une formation
Alphorm
com



Une formation
Alphorm
com





Une formation
Alphorm.com

Diagnostiquer le WebFiltering



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

- Filtrage des moteurs de recherche
- Filtrage de contenu Web
- Ordre d'inspection HTTP
- Connexion Fortriguard
- Cache WebFilter
- Lab



Filtrage moteurs de recherche

```
config webfilter profile
edit default
config web
set safe-search url
set safe-search header
end
end
```

Accès youtube restreint
Disponible en mode
d'inspection par proxy

Requiert que Fortigate utilise une inspection SSL profonde
Non pris en charge lors de l'utilisation de l'inspection par certificat
Fortigate nécessite un accès complet à la couche d'application
Limite les sites Web ou les images aux résultats de recherche

Une formation
Alphorm.com



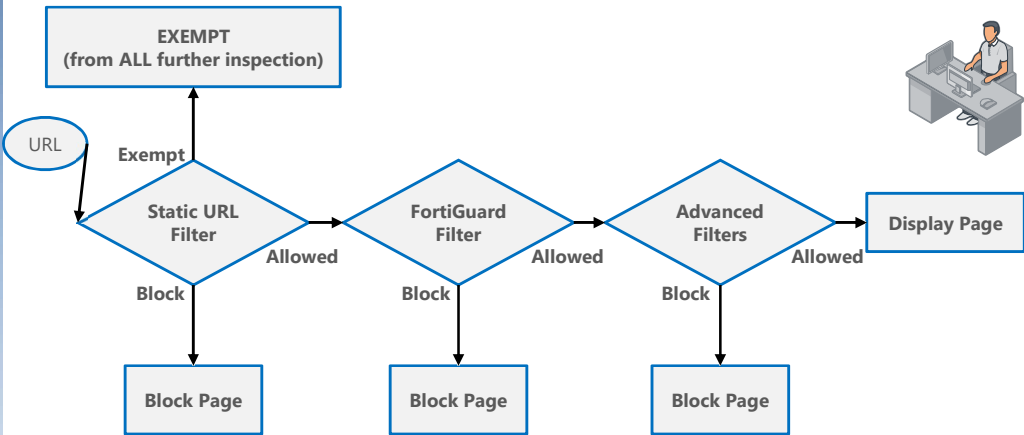
Filtrage de contenu Web

Analyser le contenu de chaque site Web accepté par
les politiques de sécurité
Faire correspondre le contenu des caractères
génériques ou des expressions régulières perl
Le nombre maximal de modèles de contenu Web
dans une liste est 5000

Une formation
Alphorm.com



Ordre d'inspection HTTP



Une formation
Alphorm.com



Connexion Fortriguard

Le filtrage de catégorie FortiGuard nécessite une connexion en direct

```
Local # diagnose debug rating
Locale      : english
License     : Contract
--- Server List (Tue Jun  7 10:41:32 2016) ---

IP           Weight  RTT  Flags  TZ    Packets  Curr Lost  Total Lost
96.45.33.65   0         72   -8     -8     868      0          114
96.45.33.64   0         72   -8     -8     868      0          114
208.91.112.196 0        106  DI     -8     859      0           80
208.91.112.198 0        118  D      -8     867      0           32
64.26.151.37  30        17   -5     -5     769      0           1
```

Une formation
Alphorm.com



Cache Web Filter

Améliore les performances en réduisant les demandes à FortiGuard
Le cache est vérifié avant d'envoyer une demande au serveur
FortiGuard
Ports UDP 53 ou 8888 pour les communications de fortiguad
Activé par défaut

```
config system fortiguad
  set webfilter-cache [ enable | disable ]
  set webfilter-cache-ttl < 300-86400 >
  set webfilter-timeout < 1-30 >
end
```

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Configurer le control applicatif



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Application Control?
Structure hiérarchique
Profil du contrôle applicatif
Lab

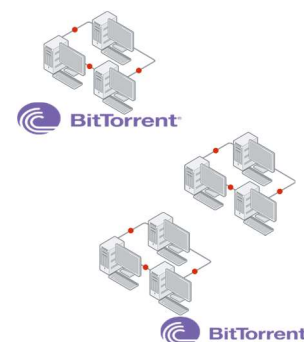


Application Contrôle?

Utilise le moteur IPS

Analyse basée sur le flux (non basée sur Proxy)

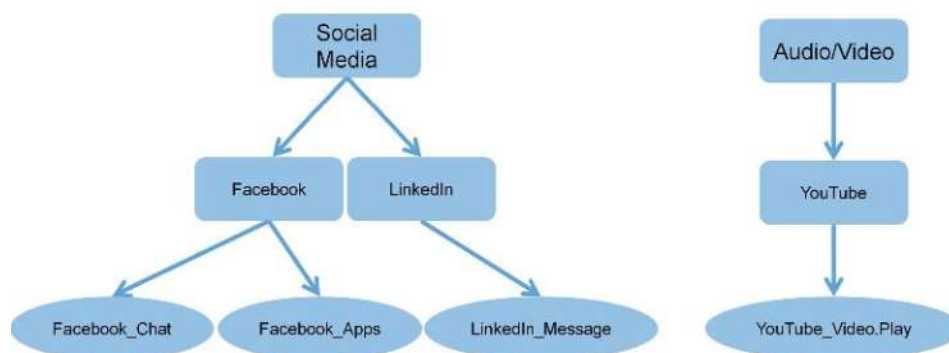
Peut détecter même si les utilisateurs tentent de contourner via un proxy externe



Une formation
Alphorm.com



Structure hiérarchique



Une formation
Alphorm.com



Profil du contrôle applicatif

Permet de filtrer le trafic en fonction de :

Catégories

Les applications similaires sont regroupées

Peut afficher les signatures de contrôle d'application pour cette catégorie

Peut configurer des actions pour des catégories prédéfinies

Remplacements d'applications

Permet de configurer l'action pour des signatures/applications spécifiques

Remplacements de filtres

Fournit un moyen plus flexible de créer une catégorisation d'application basée sur: le comportement, la popularité, le protocole, le risque et ainsi de suite

Une formation
Alphorm.com



Une formation
Alphorm.com





Diagnostiquer le contrôle applicatif



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Le traffic shaping du control applicatif
Diagnostic du control applicatif
Lab

Une formation
Alphorm.com

Le traffic shaping

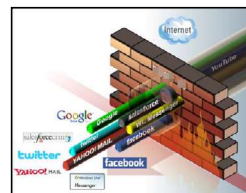
Contrôle granulaire de l'utilisation de la bande passante

Un certain trafic ne peut pas être distingué par le numéro de port/IP

Seul le trafic qui correspond à la signature est façonné

N'interférera pas avec d'autres applications sur le même port/protocole

Utile pour gérer les applications gourmandes en bande passante



Diagnostic du control applicatif

Si FortiGuard a des problèmes de mise à jour, assurez-vous que :

- FortiGate a une connexion stable à Internet
- FortiGate est capable de résoudre le DNS
- Le port TCP 443 est ouvert
- Force FortiGate pour vérifier les nouveaux updates d'application
`execute update-now`
- Vérifiez que la version de base de données de signature de contrôle d'application est à jour avec le site Web FortiGuard



Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer l'Antivirus



Mohamed Anass EDDIK



Plan

Technique d'analyse antivirus

Sandboxing

Accélération matérielle pour l'analyse
antivirus

Lab

Une formation
Alphorm
com

Technique d'analyse antivirus

Analyse antivirus

Détecte et élimine les logiciels malveillants en temps réel
(arrêter les menaces de propagation)

Prévoit la réputation du client de votre adresse IP publique

Balayage grayware

Utilise la signature graywares

Détecte et bloque les programmes non sollicités

Analyse heuristique

Recherche de virus comme le code

Compte les attributs du virus comme Fausse positive possible

Order of scan

1

Antivirus Scan

2

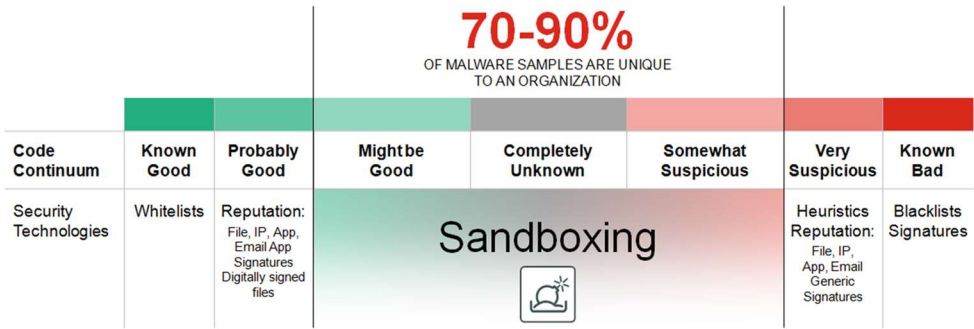
Grayware Scan

Optional (must be enabled in CLI)

3

Heuristics Scan

Sandboxing



Fortisandbox détecte les attaques Zero-Day avec une grande certitude
FortiGate télécharge des fichiers vers fortisandbox Cloud ou fortisandbox appliance
Les fichiers téléchargés sont exécutés dans un environnement isolated (VMs)
Fortisandbox examine les effets du logiciel pour détecter de nouveaux logiciels malveillants



Accélération matérielle

	Full Flow-based	Quick Flow-based	Proxy-based
Catching Rate	Highest	High	Highest
Sandbox Support	Yes	No	Yes
Advanced Heuristic	Yes	No	Yes
Memory	High	Low	High
Perceived Latency	High	Low	Highest
MAPI, NNTP Scanning	No	No	Yes
SMB Scanning	Yes	Yes	No
HTTP, FTP, IMAP, POP3, SMTP Scanning	Yes	Yes	Yes
Use FortiSandbox Database	Yes	No	Yes
Use Mobile Malware Protection Service	Yes	No	Yes



Une formation
Alphorm.com



Une formation
Alphorm.com

Découvrir les différents modes de scan



Mohamed Anass EDDIK



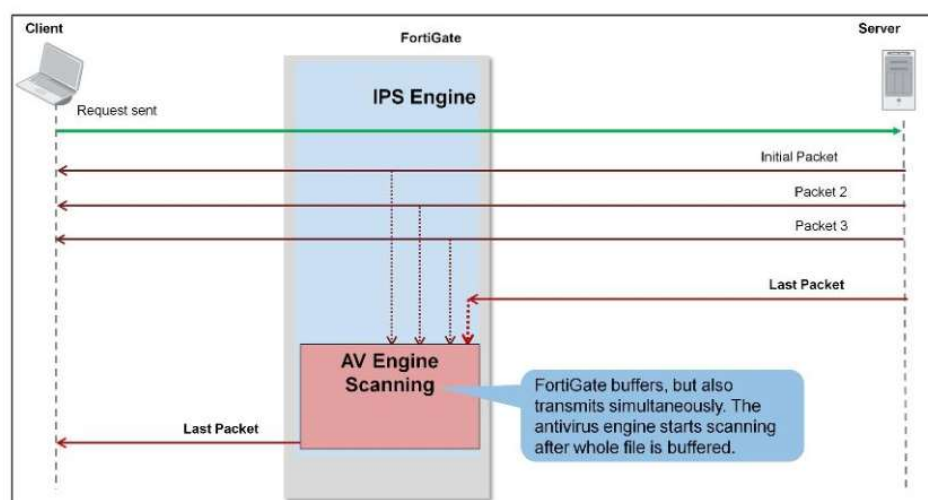
Plan

Full flow-based mode
Quick flow-based mode
Proxy-based mode
Lab

Une formation
Alphorm.com



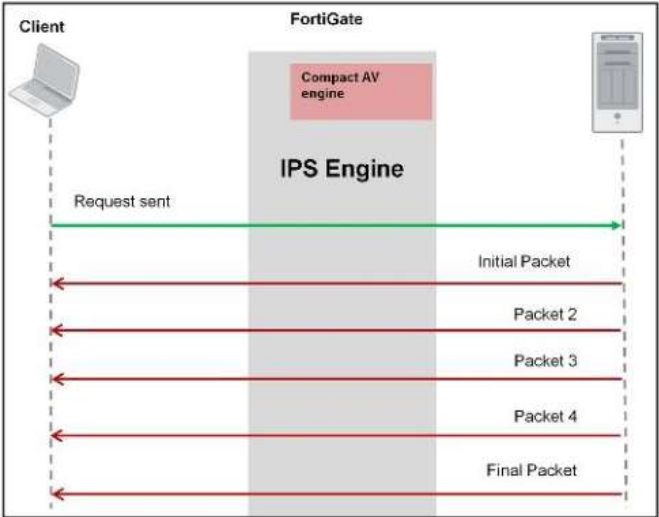
Full flow-based mode



Une formation
Alphorm.com



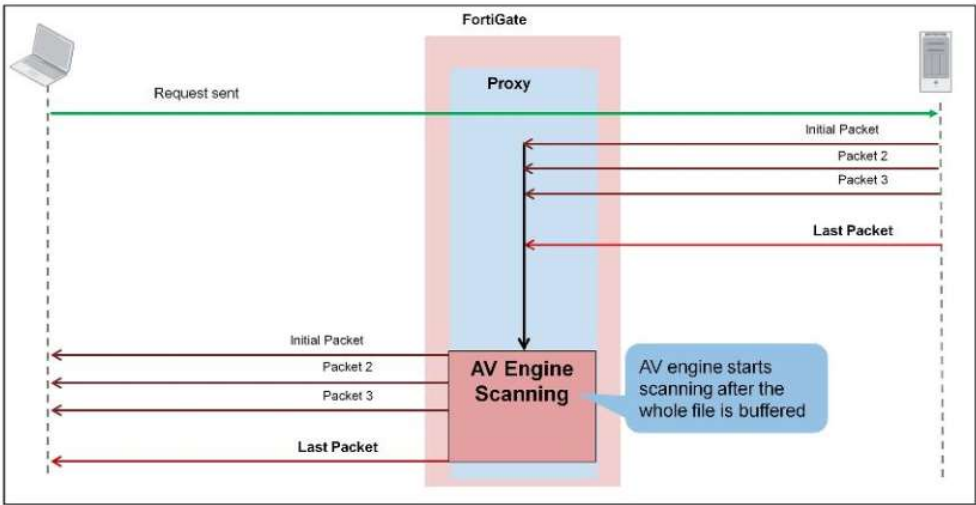
Quick flow-based mode



Une formation
Alphorm.com



Proxy-based mode



Une formation
Alphorm.com



Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer l'IPS



Mohamed Anass EDDIK



Une formation
Alphorm
com

Plan

Zero-day-attack

Fonctionnement de l'IPS

Que sont les décodeurs de protocole ?

Signature personnalisée

Configuration des capteurs IPS

Lab



Une formation
Alphorm
com

Zero-day-attack

« est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive »

Wikipédia



Une formation
Alphorm.com

Fonctionnement de l'IPS

Uniquement basé sur le flux
Exploits connus qui match la signatures
Erreurs de réseau et anomalies de protocole
Bases de données de signatures IPS
Décodeurs de protocole

Moteur IPS:

- Contrôle de l'application
- Antivirus
- Filtre Web
- Filtre de courrier électronique
- DLP



Une formation
Alphorm.com

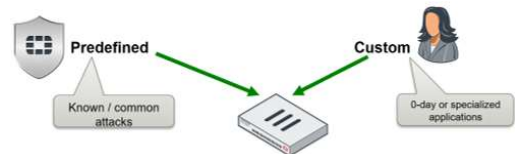
Décodeur de protocole ?



Les décodeurs PARSE les protocoles
Les signatures IPS trouvent une partie d'un protocole qui ne sont pas conformes
Sélection automatique du décodeur pour le protocole à chaque couche OSI



Signature personnalisée

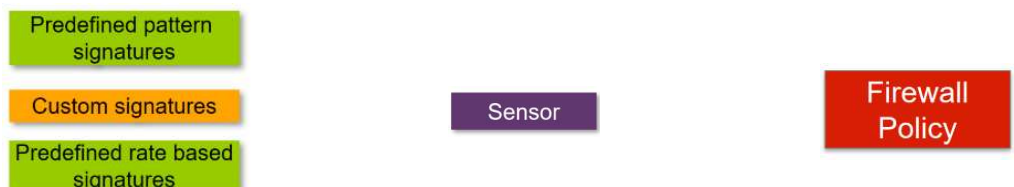


Header Keyword Value
F-SBID(--KEYWORD VALUE;)

```
F-SBID( --name "Ping.Death"; --protocol icmp; -  
-data_size >32000; )
```



Les capteurs IPS





Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer le DOS



Mohamed Anass EDDIK



Plan

Attack DOS

Types d'attack DOS

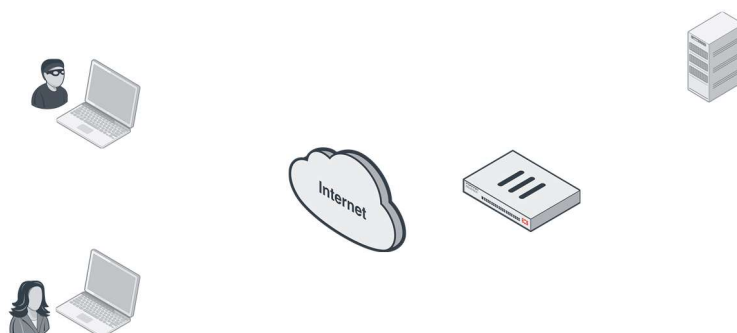
DDOS

Lab

Une formation
Alphorm.com



Attack DOS



Une formation
Alphorm.com



Une formation
Alphorm
com

Types d'attack DOS

TCP Syn Flood

Les attaquants inondent la victime avec des demandes de connexion TCP/IP incomplètes

La table de connexion de la victime devient pleine, donc les clients légitimes ne peuvent pas se connecter

ICMP sweep

Les attaquants envoient le trafic ICMP pour trouver des cibles

Les attaquants attaquent alors les hôtes qui répondent

TCP port scan

Les attaquants attaquent la victime en envoyant des demandes de connexion TCP/IP à différents ports de destination

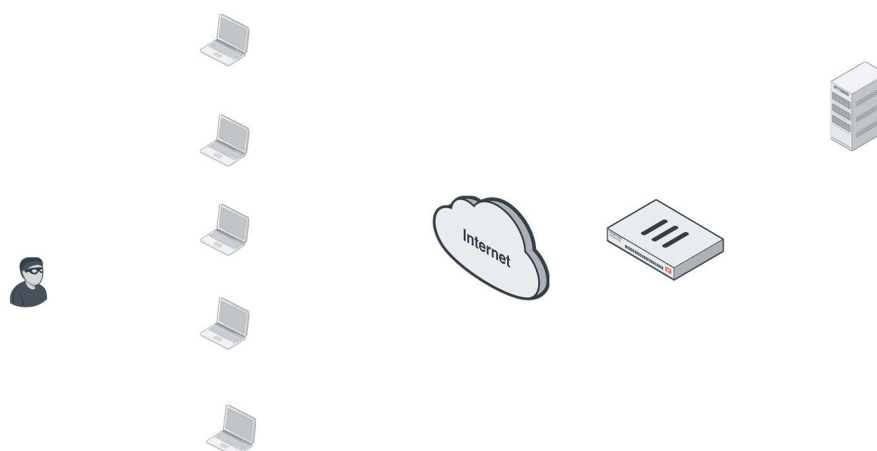
Sur la base des réponses, l'attaquant peut cartographier les services qui s'exécutent sur le système de la victime

L'attaquant cible ensuite ces ports de destination pour exploiter le système



Une formation
Alphorm
com

DDOS





Une formation
Alphorm.com



Une formation
Alphorm.com

Configurer le WAF



Mohamed Anass EDDIK



Plan

Web application Firewall (WAF)

Cross Site scripting XSS

SQL Injection

FORTIWEB

Lab

Une formation
Alphorm.com



Web application Firewall

Les sites Web sont des cibles attractives pour les pirates

Le filtrage Web FortiGuard est pour les clients, pas les serveurs

WAF est destiné à protéger les services Web

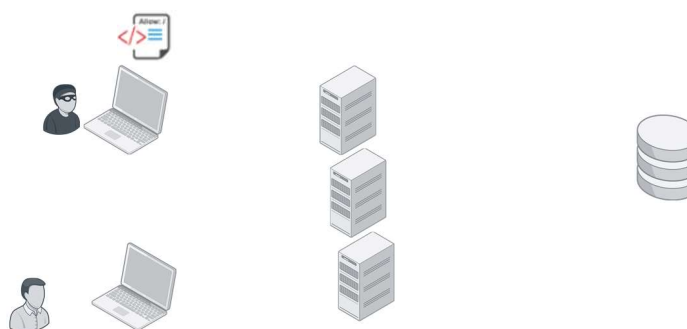
La fonctionnalité WAF est disponible

uniquement en mode d'inspection par proxy

Une formation
Alphorm.com



Cross Site scripting XSS



Une formation
Alphorm.com



SQL Injection

Les instructions SQL sont insérées dans les champs d'entrée d'une application Web

L'application Web ne rejette pas les entrées illégales

Lorsque l'application Web se connecte à la base de données pour ajouter une entrée, elle peut :

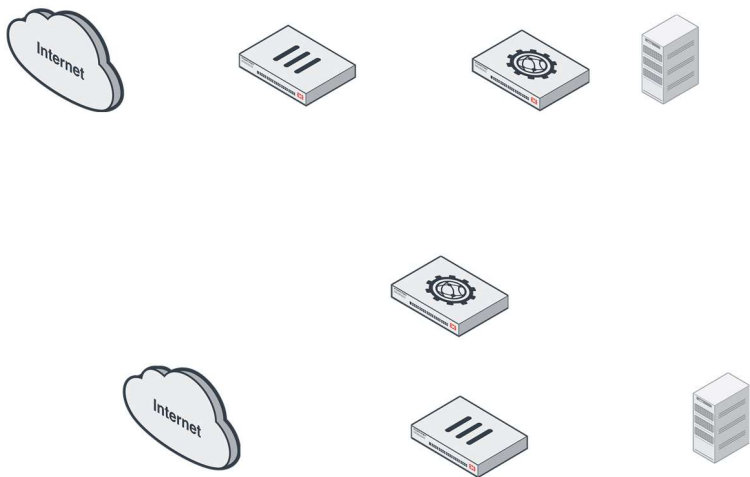
- Télécharger des données sensibles (sélectionnez * parmi les utilisateurs)
- Modifier la base de données (Insérer/supprimer/mettre à jour)

Une formation
Alphorm.com



Une formation
Alphorm.com

Fortiweb



Une formation
Alphorm.com





Une formation
Alphorm.com

Configurer le SSL VPN



Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

SSL VPN VS IPSec VPN

Mode de déploiement

Comment configurer SSL VPN

Lab



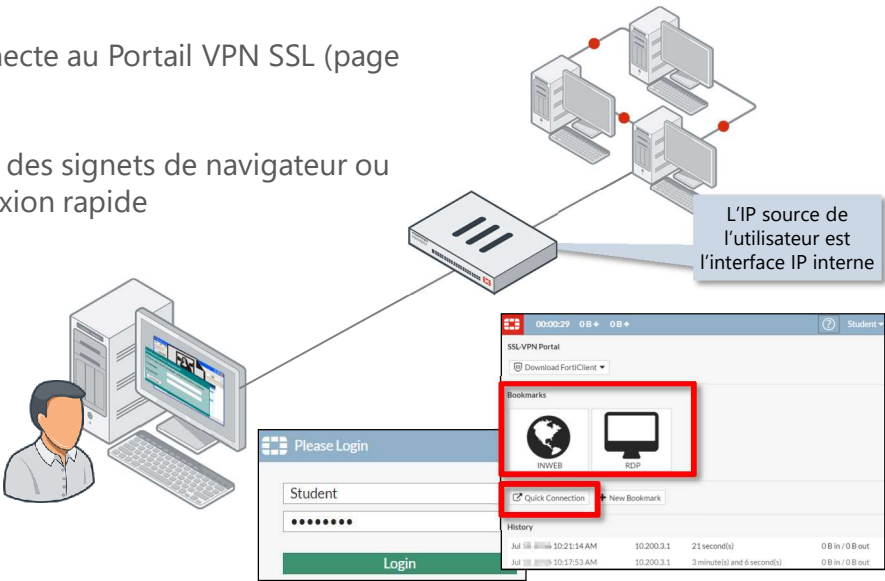
SSL VPN VS IPSec VPN

	SSL-VPN	IP-SEC
Type de tunnel	HTTPS tunnel (SSL/TLS layer)	IPsec tunnel (ESP layer)
Peut être entre	Browser/FortiClient + FortiGate	FortiClient+ FortiGate FortiGate + FortiGate FortiGate+ compatible third-party IPsec VPN gateway FortiGate + compatible third-party IPsec VPN clients
Se connecter par	HTTPS web page on FortiGate, or Use fortissl virtual adapter (FortiClient)	Site-to-site doesn't require IPsec client

Une formation
Alphorm.com

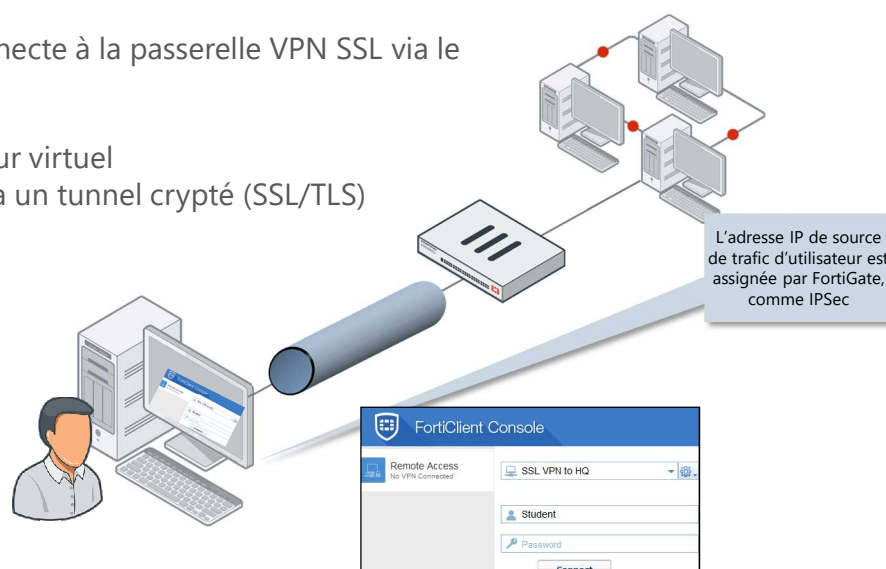
Mode Web uniquement

L'utilisateur distant se connecte au Portail VPN SSL (page Web HTTPS sur FortiGate)
Authentification
Accéder aux ressources via des signets de navigateur ou un widget d'outil de connexion rapide



Mode Tunnel

L'utilisateur distant se connecte à la passerelle VPN SSL via le client VPN SSL
authentification
Tunnel créé par l'adaptateur virtuel
Accéder aux ressources via un tunnel crypté (SSL/TLS)



Tunneling fractionné

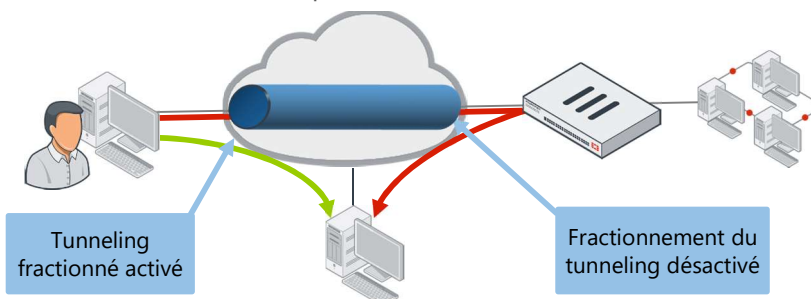
Désactivé

Tout le trafic acheminé par le tunnel VPN SSL à un FortiGate distant, puis à la destination (y compris le trafic Internet)

Activé

Seul le trafic LAN acheminé via la télécommande FortiGate

Le trafic Internet utilise la passerelle locale





Comment configurer SSL VPN

Configurer des comptes d'utilisateurs et des groupes

Configurer le portail

Configuration des paramètres du VPN SSL

Créer une stratégie de pare-feu pour accepter et déchiffrer des paquets

Généralement utilisé pour permettre l'accès au réseau interne

Facultatif : Créer une stratégie de pare-feu pour acheminer le trafic vers Internet

Utile lorsque le tunneling fractionné est désactivé pour acheminer tout le trafic du client via FortiGate vers Internet – FortiGate peut être utilisé pour appliquer des profils de sécurité

Une formation
Alphorm.com



Une formation
Alphorm.com





Une formation
Alphorm.com

Configurer Realms et bookmark



Mohamed Anass EDDIK



Une formation
Alphorm.com

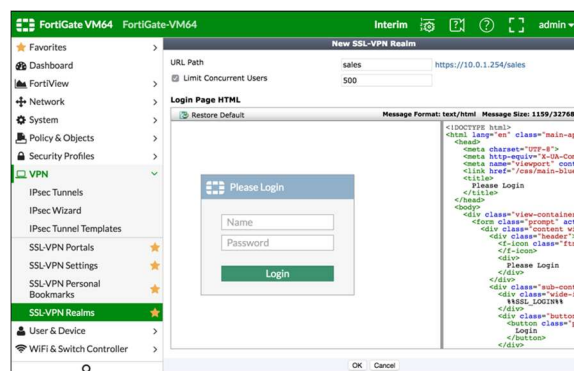
Plan

Realms
Bookmarks
Lab

Realms

Par défaut, le même portail pour tous les utilisateurs : **https://10.0.1.254/**
Peut faire des URL pour des portails spécialisés (realms) :

- **https://10.0.1.254/sales**
- **https://10.0.1.254/hr**
- **https://10.0.1.254/teachers**



Bookmarks

Pas les mêmes que les bookmarks de votre navigateur

À l'intérieur du portail Web VPN SSL

Paramètres pour les applications qui traversent le tunnel VPN

Si activé dans chaque portail, les utilisateurs peuvent créer leurs propres Bookmark

Les administrateurs peuvent:

- Via GUI, afficher/supprimer les Bookmarks des utilisateurs
- Via CLI, créer des Bookmarks d'utilisateurs

```
config vpn ssl web user-bookmark
edit <user_name>
config bookmarks
edit <bookmark_name>
set apptype {citrix | ftp | portforward | rdp | smb | ssh | telnet | vnc | web}
set description <text_string>
set sso {auto|disable}
next
end
```



Une formation
Alphorm.com



Une formation
Alphorm.com

Surveiller les logs SSL VPN



Mohamed Anass EDDIK



Plan

Meilleure sécurité VPN SSL
Accélération du matériel pour SSL-VPN
Lab

Une formation
Alphorm.com



Meilleure sécurité VPN SSL

Vérification de l'intégrité du client
Restreindre les adresses où les clients
peuvent se connecter
Exiger des certificats clients
Authentification à deux facteurs
Forticlient

Une formation
Alphorm.com

Accélération du matériel

Les appareils Fortigate avec des processeurs de contenu (CP8 ou CP9), qui déchargent des opérations spécifiques gourmandes en CPU, prennent en charge les moteurs de données en vrac SSL-VPN haute performance. L'administrateur peut désactiver le déchargement CP via des stratégies de pare-feu.

```
config firewall policy
edit 1
set auto-asic-offload [enable |disable]
end
```

Pour afficher l'état de l'accélération SSL-VPN, utilisez la commande suivante:

```
get vpn status ssl hw-acceleration-status
```

```
Acceleration hardware detected:
kxp=on cipher=on
```

```
No acceleration hardware detected
```





Une formation
Alphorm.com

Conclusion



Mohamed Anass EDDIK



Une formation
Alphorm.com

Bilan

- Configurer les stratégies
- Configurer le NAT
- Configurer l'authentification
- Configurer le logging et monitoring
- Configurer les certificats
- Configurer le webfiltering
- Configurer le contrôle applicatif
- Configurer l'Antivirus
- Configurer l'IPS et le DOS
- Configurer le SSL VPN



Prochaine formation



Une formation
Alphorm.com

A vous de jouer !

