

📍 Avenue V. Maistriau 8a
B-7000 Mons
📞 +32 (0)65 33 81 54
✉️ scitech-mons@heh.be

WWW.HEH.BE

UE : Networks : Connected and secure

- AA : Cybersécurité 2
Denis Mandoux

Bachelier en Informatique
Orientation réseaux et télécommunications

Table des matières

1. Authentication	(slide 2)	1
2. Antivirus	(slide 37)	19
3. Filtrage Web.....	(slide 125)	63
4. Contrôle d'application.....	(slide 167)	84
5. Dialup VPN - ADVPN.....	(slide 199)	100
6. TLS.....	(slide 238)	119
7. Configuration d'un VPN SSL/TLS.....	(slide 290)	145
8. Intrusion Prevention System	(slide 337)	169
9. Haute disponibilité	(slide 387)	193
10. Single Sign On	(slide 437)	218
11. ZTNA	(slide 475)	237
12. SD-WAN	(slide 522)	261
13. Bibliographie.....		281

UE : Networks : Connected and secure

- AA : Cybersécurité 2

Denis Mandoux

Bachelier en Informatique
Orientation réseaux et télécommunications

Chapitre 1

Authentification

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Décrire l'authentification au niveau des règles de pare-feu.
 - Identifier les différentes méthodes d'authentification de pare-feu disponibles sur un périphérique FortiGate.
 - Configurer des règles de FW pour authentifier les utilisateurs.
 - Par mot de passe local.
 - Par mot de passe sur serveur distant.
 - Par authentification à deux facteurs.
 - Configurer un portail captif.

Firewall authentication

- Authentification par le pare-feu
 - Contrôle de l'IP source et du périphérique
 - Pour décider si un accès est autorisé, un pare-feu peut se baser sur l'IP source et le périphérique (Device Identification).
 - Ce contrôle peut être insuffisant car le pare-feu ne peut pas déterminer quel utilisateur se trouve derrière l'appareil auquel il donne accès.
 - Authentification des utilisateurs
 - Pour certains accès, il est nécessaire de pouvoir authentifier les utilisateurs.
 - Seulement après avoir authentifié l'utilisateur, l'UTM appliquera les règles de pare-feu et les profils de sécurité.



Méthode d'authentification

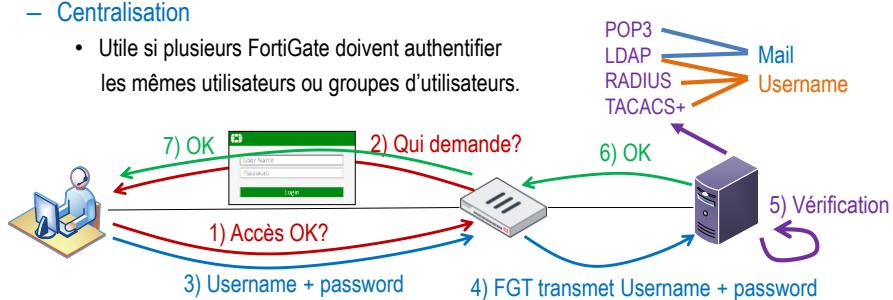
- Local password authentication
 - Authentification par mot de passe local
 - Le nom d'utilisateur et le mot de passe sont stockés localement sur le FortiGate.
 - A utiliser s'il n'y a qu'un ou deux FortiGates.
 - L'authentification à deux facteurs est possible.
 - Création d'un utilisateur local
 - User & Device > User Definition (voir cours précédent).
 - Une fois créé, l'utilisateur peut être utilisé dans une règle de pare-feu.



• • • 5

Méthode d'authentification

- Server-based Password Authentication
 - Principe
 - Le FortiGate stocke peu voire pas du tout d'informations utilisateur en local.
 - Les identifiants sont transmis à un serveur pour vérification.
 - Centralisation
 - Utile si plusieurs FortiGate doivent authentifier les mêmes utilisateurs ou groupes d'utilisateurs.



• • • 6

Méthode d'authentification

- Server-based Password Authentication : method 1
 - Créer un compte utilisateur de type « Remote » et spécifier le serveur qui contiendra/vérifiera les identifiants

User & Device > RADIUS Servers

Définir le ou les serveurs d'authentification

User & Device > User Definition

Créer le compte utilisateur
L'authentification
POP3 est uniquement
disponible via la CLI

Choix du serveur à contacter pour l'authentification
Doit avoir été préconfiguré sur le FortiGate

WALLONIE-BRUXELLES
ENSEIGNEMENT

● ● ● 7

User & Device > User Group

Add Group Match

Choix du serveur à contacter
Doit avoir été préconfiguré sur le FortiGate (diapo. précédente)

– Ajouter le groupe d'utilisateur à une règle de pare-feu

WALLONIE-BRUXELLES
ENSEIGNEMENT

● ● ● 8

Méthode d'authentification

- Two-Factor Authentication and One-Time Passwords (OTP)
 - Mots de passe à usage unique
 - Plus sûrs que les mots de passe statiques
 - Ils ne sont valides que pour une courte période de temps.
 - Une fois utilisé l'OTP ne peut plus être utilisé, donc même s'il est intercepté, il est inutile.
 - Un OTP peut être utilisé comme deuxième facteur d'authentification
 - Time-based OTP
 - FortiGate peut délivrer des OTP via des jetons (token)
 - FortiToken (jeton matériel), FortiToken Mobile (jeton logiciel via smartphone).
 - Par défaut, un FortiToken génèrent un nouveau mot de passe toutes les 60 secondes.
 - FortiToken mobile push : juste accepter le jeton suffit sans devoir entrer le code envoyé (uniquement sur le même téléphone portable que celui enregistré).
 - FortiGate peut aussi délivrer des OTP via SMS ou par e-mail
 - En cas d'envoi par courriel ou SMS, le compte utilisateur doit contenir les informations de contact de l'utilisateur
 - Serveur NTP recommandé !

User Type > Login Credentials > Contact Info > Extra Info

Email Address: student@fortinet.lab

SMS:

9

Méthode d'authentification

- Assigner un FortiToken à un utilisateur
 1. Configurer le token (User & Authentication > FortiTokens)
 - Ajout, suppression, modification d'un Token

Type	Serial Number	Status	User	Drift
Mobile Token	FTKMOB49AF7C8B6D	Available		
Mobile Token	FTKMOB4975658F0A	Available		
 - Un code d'activation est requis pour les jetons logiciels (à acheter).
 - Il est possible d'importer les n° de série des FortiToken depuis un fichier .txt

HEH.be
Sciences
et technologies

Méthode d'authentification

- Assigner un FortiToken à un utilisateur (suite)
 - Activer l'authentification à deux facteurs
 - Selectionner le FortiToken qui sera associé à l'utilisateur.

The screenshot shows the 'Edit User' window. On the left, there's a navigation bar with 'User & Device' and 'User Definition'. The main area has fields for 'User Name' (guest), 'User Account Status' (Enabled), 'User Type' (Local User), 'Password' (redacted), 'Email Address' (redacted), 'SMS' (checkbox), and 'Two-factor Authentication' (checkbox, highlighted with a red box). Below these are 'Token' and 'User Group' sections. A dropdown menu is open under 'Token', showing two options: 'FTKMOB5C94FE73B4' and 'FTKMOB5CC0DB3E44', with the first one selected. Red arrows point from the text 'Activation' to the 'Two-factor Authentication' checkbox and from 'Choix d'un FortiToken préalablement enregistré' to the dropdown menu.

HEH.be
Sciences
et technologies

Méthode d'authentification

- Authentification active et authentification passive
 - Authentification active
 - Invite de connexion
 - Les utilisateurs doivent saisir manuellement leurs identifiants de connexion avant d'obtenir un accès.
 - L'authentification active peut être utilisée avec :
 - L'authentification par mot de passe local.
 - L'authentification basée sur un serveur d'authentification (POP3, LDAP, RADIUS, TACACS+).
 - L'authentification à deux facteurs.

This section is identical to the one above, showing the 'Edit User' interface with the 'Two-factor Authentication' checkbox highlighted and the 'Token' dropdown menu showing two options: 'FTKMOB5C94FE73B4' and 'FTKMOB5CC0DB3E44', with the first one selected.

Méthode d'authentification

- Authentification active et authentification passive (suite)
 - Authentification passive
 - Le processus d'authentification est transparent pour l'utilisateur
 - L'utilisateur ne devra pas entrer ses identifiants de connexion, ils sont déterminés automatiquement par le pare-feu.
 - Le FortiGate peut obtenir les identifiants selon plusieurs méthodes
 - FSSO, RSSO et NTLM → Voir chapitre FSSO.
 - Authentification active et passive à la fois
 - Si les deux sont utilisées, l'authentification active est utilisée comme backup en cas d'échec de l'authentification passive.

Remote Authentication Servers

- Configuration de l'authentification avec serveur LDAP

Le Common name est cn pour la plupart des serveurs LDAP.

Le DN doit pointer vers le bon niveau dans Active Directory.

Compte utilisateur que FortiGate utilise pour interroger le serveur LDAP

Sécurisation de la connexion avec SSL il faut préciser le certificat de la CA qui vérifiera le certificat du serveur.

User & Authentication > LDAP Servers

Name	ADserver
Server IP/Name	10.0.1.10
Server Port	636
Common Name Identifier	cn
Distinguished Name	ningAD,dc=training,dc=lab
Bind Type	Simple Anonymous Regular
User DN	cn=ADadmin,cn=users,dc=
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Protocol	LDAPS STARTTLS
Certificate	No Certificate
<input type="button" value="Test"/> Teste la connexion au serveur LDAP. Ne teste pas l'auth. des utilisateurs.	

Remote Authentication Servers

- Configuration de l'authentification avec serveur LDAP (suite)

Simple : à utiliser si tous les enregistrements de l'utilisateur sont sous le même nom de domaine.

Anonymous : à utiliser lorsque les recherches anonymes sont acceptées par le LDAP.

Regular : à utiliser si serveur LDAP nécessite une authentification pour effectuer des recherches.

Remote Authentication Servers

- Tester l'authentification d'un utilisateur

- La commande `test authserver`

- Permet de vérifier si les informations d'identification d'un utilisateur permettent de l'authentifier correctement.

- Syntaxe

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

- Exemple

```
# diagnose test authserver ldap ADserver aduser1 mypassword

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

Remote Authentication Servers

- Configuration de l'authentification avec serveur RADIUS
 - Remote Authentication and Dial-in User Service
 - Protocole client-serveur qui fournit des fonctions centralisées d'authentification, d'autorisation et de comptabilisation.
 - RFC 2865 (RADIUS) et RFC 2866 (Accounting)
 - Utilise le protocole UDP pour les échanges entre client et serveur.
 - Ports UDP : 1812 ou 1645 (authentification) et 1813 ou 1646 (tracabilité).
 - Configuration du serveur
 - Le serveur RADIUS doit être configuré pour accepter le FortiGate comme client.



• • • 17

Remote Authentication Servers

- Configuration de l'authentification avec serveur RADIUS
 - Configuration du FortiGate pour utiliser un serveur RADIUS

IP du FortiGate à utiliser dans le cas où plusieurs interfaces sont utilisées.

User & Device > RADIUS Servers

New RADIUS Server

Name	FortiAuth-RADIUS
Authentication method	Default Specify
NAS IP	
Include in every user group	<input checked="" type="checkbox"/>
Primary Server	
IP/Name	10.0.1.150
Secret	*****
Test Connectivity	
Test User Credentials	

Ajoute le serveur Radius, à chaque groupe d'utilisateurs créé sur le FortiGate. Utile si tous les utilisateurs s'authentifient avec ce serveur.

Protocole d'authentification pris en charge par le serveur RADIUS

PAP
MS-CHAP-v2
MS-CHAP
CHAP
PAP

• • • 18

Remote Authentication Servers

- Tester l'authentification d'un utilisateur

- La commande `test authserver`

- Permet de vérifier si les informations d'identification d'un utilisateur permettent de l'authentifier correctement.

- Syntaxe

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

- Exemple

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

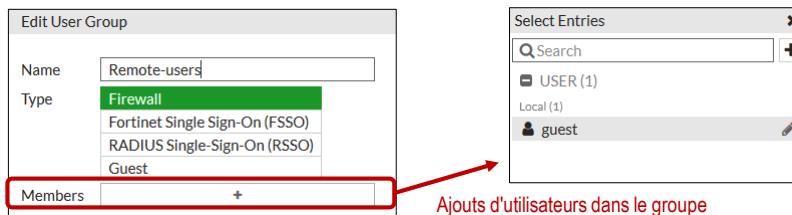
authenticate 'aduser1' against 'pap' succeeded, server=primary
assigned_rad_session_id=810153440 session_timeout=0 secs!
Group membership(s) - remote-AD-admins
```

User Groups

- Types de groupes d'utilisateurs

- Firewall user group

- Ils sont utilisés localement au niveau d'une règle de pare-feu afin d'autoriser des accès uniquement à certains groupes d'utilisateurs.
- Configuration : User & Device > User Groups > Create New



Ajouts d'utilisateurs dans le groupe

HEH.be
Sciences
et technologies

User Groups

- Types de groupes d'utilisateurs (suite)
 - 2. Guest user group
 - Ces groupes sont généralement utilisés pour les accès invités dans les réseaux sans fil.

Plusieurs comptes d'invités peuvent être créés en une fois à l'aide d'identifiants et de mots de passe générés de façon aléatoire.

WALLONIE-BRUXELLES
ENSEIGNEMENT

• • • 21

HEH.be
Sciences
et technologies

User Groups

- 2. Guest user group (suite)
 - Ce type de compte contient le compte entier, pas seulement le mot de passe.
 - Les comptes invités expirent après une période de temps pré-déterminée.

WALLONIE-BRUXELLES
ENSEIGNEMENT

• • • 22

User Groups

- Types de groupes d'utilisateurs
 - 3. Fortinet Single Sign-On (FSSO) user group
 - Utilisé pour l'authentification unique et passive (voir chapitre FSSO).
 - 4. RADIUS Single Sign-On (RSSO) user group
 - Utilisé pour l'authentification unique et passive (voir chapitre FSSO).

User Groups

- Règle de pare-feu et authentification
 - Principe
 - Authentifier avant d'accepter le trafic utilisateur
 - Ajouter des utilisateurs ou groupes d'utilisateurs dans le champ source d'une règle de pare-feu permet d'authentifier l'utilisateur avant d'accepter le trafic.
 - Normalement, aucun service n'est autorisé par la règle de pare-feu avant l'authentification réussie des utilisateurs.



- Comptes locaux
- Comptes externes (remote server)
- Utilisateurs PKI (certificate)
- Utilisateurs SSO

User Groups

- Règle de pare-feu et authentification (suite)
 - Exceptions
 - La règle de pare-feu doit parfois autoriser certains protocoles avant l'authentification active (HTTP/HTTPS/FTP/Telnet)
 - Le protocole permettant d'afficher la boîte de dialogue d'authentification utilisée dans l'authentification active.
 - » Ce n'est pas le cas avec l'authentification passive.
 - Le protocole DNS peut être autorisé même si l'utilisateur ne s'est pas encore authentifié.
 - » En effet, la résolution du nom d'hôte est souvent requise par le protocole de couche application qui est utilisé pour l'authentification.
 - Pour cela, la règle de pare-feu doit spécifier les protocoles autorisés.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Full_Access	LOCAL_SUBNET	all	always	DNS HTTP	ACCEPT	Enabled

User Groups

- Règle de pare-feu et authentification (suite)
 - Combinaison de règles avec et sans authentification
 - ⚠️ • Activer l'authentification dans une règle de pare-feu ne garantit pas que l'utilisateur devra s'authentifier

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled
2		LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled

- Dans l'exemple ci-dessus, le trafic d'un utilisateur de HR-group ne « matche » pas avec la règle 1 car l'utilisateur n'est pas encore authentifié.
- Par contre son trafic « matche » avec la règle 2 car son IP est bien comprise dans l'objet LOCAL_SUBNET.

User Groups

- Règle de pare-feu et authentification (suite)
 - Comment garantir l'authentification des utilisateurs
 1. Activer l'authentification dans chaque règle de pare-feu qui pourrait correspondre au trafic.
 2. Appliquer l'option d'authentification à la demande (CLI uniquement).


```
# config user setting
(setting) # set auth-on-demand <always|implicit>
```

 - **Implicit** : option par défaut, elle ne déclenchera pas l'authentification de l'utilisateur s'il existe une autre règle sans authentification qui autorise le trafic.
 - **Always** : garanti que l'utilisateur devra s'authentifier pour les règles dont l'authentification active est activée.
 3. Activer un portail captif sur l'interface d'entrée du trafic.
 - Dans ce cas, tous les utilisateurs qui envoient du trafic par cette interface devront s'authentifier.

Authentification via un portail captif

- Portail captif
 - Permet une authentification des utilisateurs via une page Web
 - Le portail captif est utilisé pour que tous les utilisateurs qui se connectent au réseau doivent s'authentifier via une authentification active.
 - Le portail captif peut être hébergé sur le FortiGate ou un serveur d'authentification externe.
 - Le portail captif est activé au niveau d'une interface
 - WiFi (SSID) → OK
 - Interfaces VLAN → OK
 - Interfaces en mode DHCP → pas OK

Network > Interfaces

Admission Control	
Security Mode	Captive Portal
Authentication Portal	<input checked="" type="radio"/> Local <input type="radio"/> External
User Access	<input type="checkbox"/> Restricted to Groups <input checked="" type="checkbox"/> Allow all
Customize Portal Messages	
Exempt Sources	+
Exempt Destinations/Services	+

Authentification via un portail captif

- Configuration d'un portail captif

- Il est possible d'exempter certains utilisateurs ou certains périphériques de l'authentification car certains appareils ne sont pas capables de s'authentifier (imprimante). **Tous les groupes listés dans les règles de pare-feu pourront s'authentifier et accéder aux ressources**

Seuls les groupes listés dans « User Groups » pourront s'authentifier et accéder aux ressources

Liste des appareils qui ne devront pas fournir d'authentification

Network > Interfaces

Admission Control	Captive Portal
Security Mode	Local External
Authentication Portal	
User Access	Restricted to Groups Allow all
User Groups	+ +
Customize Portal Messages	
Exempt Sources	+ +
Exempt Destinations/Services	+ +

Authentification via un portail captif

- Configuration d'un portail captif (suite)

- Il est possible de configurer l'exemption en CLI.

1. Par le biais d'une liste d'exemption de sécurité

```
#config user security-exempt-list
  edit <list_name>
    config rule
      edit <name>
        set srcaddr|dstaddr|service
      next
    end
```

2. Par le biais de la politique de pare-feu

Tout le trafic correspondant à la règle <policy ID> est exempté de l'obligation de s'authentifier par le biais d'un portail captif.

```
{ #config firewall policy
  edit <policy_id>
    set captive-portal-exempt enable
  end }
```

Authentification via un portail captif

- Configuration d'un portail captif (suite)

- Disclaimer

- Il est possible d'afficher une page reprenant les conditions d'utilisation.
 - Tous les utilisateurs devront accepter ces conditions pour poursuivre.
 - Pas d'exemption possible.

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



Authentification via un portail captif

- Configuration d'un portail captif (suite)

- Personnaliser les messages

Seule l'option « Extended View » affiche l'ensemble des messages configurable

System > Replacement Messages

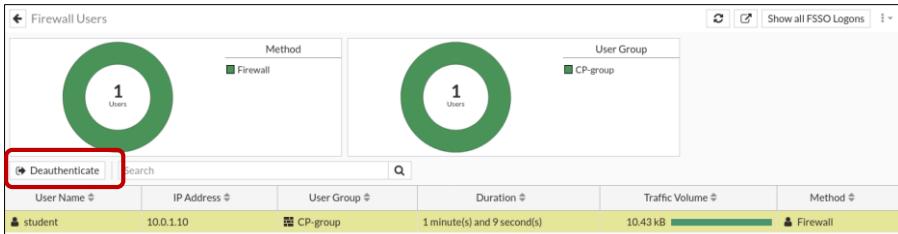
Manage Images		Search	Simple View	Extended View
Name	Description			
Administrator (2)				
Post-login Disclaimer Message	Replacement message for post-login disclaimer			
Pre-login Disclaimer Message	Replacement message for pre-login disclaimer			
Alert Email (5)				
alertmail-block				
alertmail-crit-event				
alertmail-disk-full				
alertmail-nids-event				
alertmail-virus				
Authentication (24)				

Authentification via un portail captif

- Authentication Timeout
 - Minuteur d'expiration de l'authentification
 - Il spécifie combien de temps un utilisateur peut rester inactif avant de devoir s'authentifier à nouveau (5 min. par défaut).
 - Réduit les risques qu'une personne réutilise l'IP d'un utilisateur authentifié.
 - Limite l'utilisation des ressources.
 - Le FortiGate ne doit pas garder indéfiniment en mémoire les informations de connexions.
 - Options
 - Idle
 - Si le FortiGate ne reçoit pas de paquets du périphérique hôte dans le délai configuré, l'utilisateur est déconnecté.
 - Hard
 - L'authentification expire à la fin du minuteur, quel que soit le comportement de l'utilisateur.
 - New session
 - L'authentification expire si aucune nouvelle session n'est créée pendant la durée du minuteur, même si du trafic est généré.

Monitoreder les utilisateurs authentifiés

- Surveiller les utilisateurs authentifiés
 - Monitor > Firewall User Monitor
 - Affiche l'utilisateur, le groupe d'utilisateurs, la durée, l'adresse IP, le volume de trafic et la méthode d'authentification.
 - Permet de désauthentifier un (ou plusieurs) utilisateurs.



Dépannage

- Commandes de dépannage

- Afficher les utilisateurs authentifiés, les groupes associés et leur adresse IP.

```
diagnose firewall auth list
```

- Effacer tous les utilisateurs autorisés de la liste actuelle.

```
diagnose firewall auth clear
```

- Tester la clé pré-partagée entre FortiGate et le serveur RADIUS.

```
diagnose test authserver radius-direct <ip> <port> <secret>
```

- Débogage de l'authentification active.

```
diagnose debug enable  
diagnose debug app fnbamd -1
```

Dépannage

- Surveiller les utilisateurs authentifiés

- Règle de pare-feu

- La colonne « bytes » permet de vérifier si une règle voit passer du trafic.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
0	port3 --> port1									
1	Full_Access	LOCAL_SURNET	all	always	ALL	✓ ACCEPT	Enabled	upg_deep-inspection	UTM	3.47 MB
0	implicit									

Chapitre 2

Antivirus

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Décrire les techniques antivirales du FortiGate.
 - Expliquer les différences entre le scan en mode proxy et le scan en mode flow.
 - Configurer un profil antivirus et l'appliquer dans une règle de pare-feu.
 - Configurer l'UTM pour scanner du trafic chiffré.
 - Mettre à jour l'antivirus d'un FortiGate.

Techniques antivirales

- **Analyse antivirus**

- Objectifs de l'analyse antivirus en périphérie

- DéTECTer et éLIMINer les logiciels malveillants en temps réel avant qu'ils n'entrent dans le réseau.
- Empêcher les menaces de se propager.
- Préserver la réputation des IP publiques de l'entreprise.

- **Analyse grayware**

- DÉTECTe les programmes non sollicités

- Ils ne sont pas vraiment dangereux mais ont des effets secondaires indésirables (perte de productivité, ...) et sont donc classés comme logiciels malveillants.

- **Machine learning scan (AI scan)**

- Analyses basées sur des probabilités, elles augmentent donc la possibilité de faux positifs, mais peuvent détecter des attaques de type "zero-day".

Techniques antivirales

- **Analyse par signature**

- Signature virale

- A l'origine :

- Une signature est une suite continue de bits présente dans les malwares ou les fichiers infectés mais pas dans les fichiers non infectés.

- Actuellement :

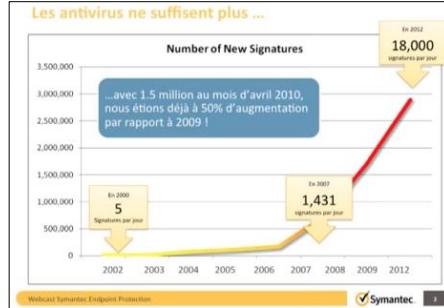
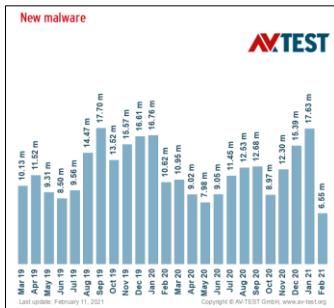
- Différentes technologies sont utilisées pour alimenter les bases de données antivirus, mais on continue d'utiliser le terme signature.
- Une signature peut être une partie de code, un hash d'un fichier malveillant, une combinaisons d'attributs, des valeurs binaires à certains endroits, etc.

- Principe de l'analyse par signature

- Différentes technologies sont utilisées pour créer des signatures antivirus.
- Les signatures sont téléchargées dans des bases de données sur le matériel.
- Les antivirus scannent les fichiers à la recherche d'une correspondance dans leur base de données de signatures.

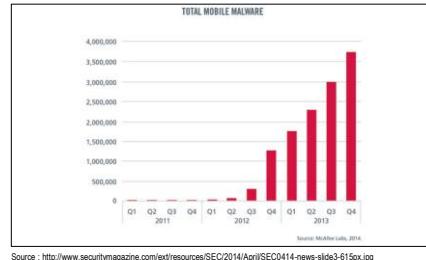
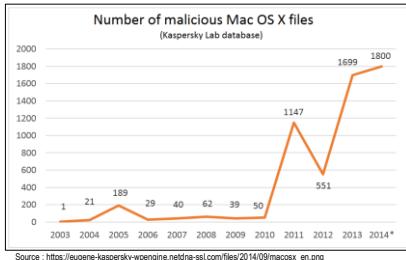
Techniques antivirales

- Le cybercrime est une industrie
 - Chaque jour, l'Institut AV-TEST enregistre plus de 350 000 nouveaux programmes malveillants (malware) et applications potentiellement indésirables (PUA)..



Techniques antivirales

- Pas seulement sous Windows



Techniques antivirales

- Avantages de l'analyse par signature
 - Le scan est très rapide
 - Pas de faux positifs
- Limites de l'analyse par signature
 - Il y a trop de signatures à devoir créer
 - Il y a tellement de variantes de malware qui sont créées chaque jour qu'il est impossible de maintenir les bases de données de signatures à jour.
 - Ne peut bloquer que les malwares connus (dont il existe une signature)
 - Le taux de détection peut donc être assez faible lors du premier mois du malware.
 - Nécessité de télécharger en continu une liste actualisée des signatures de virus connus.
 - Sensible à certains mécanismes d'obfuscation

Techniques antivirales

- Limites de l'analyse par signatures (suite)
 - Les pirates dissimulent leurs malwares en utilisant des techniques d'obfuscation telles que :
 - de la compression,
 - du polymorphisme,
 - du packer,
 - du chiffrement,
 - du dead code,
 - ...

En 2018, 93,6 % des logiciels malveillants observés étaient polymorphes.
[\(2020 Webroot Threat Report\)](#)



Techniques antivirales

- Antivirus multi-scanner ou multi-moteur

Online Multi-Engine Antivirus Scanners

- VirusTotal
- Metascan Online
- VirSCAN
- Jotti
- NoVirusThanks
- Chk4me
- Serenity Scanner
- ...

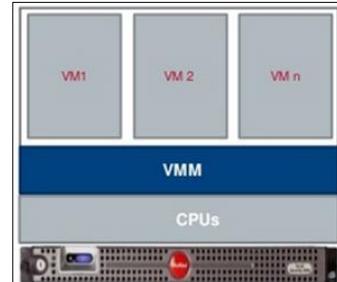
Antivirus	Result	Update
Avgitum	-	20130220
AhnLab-V3	Trojan.Win32.Jorik	20130220
AntiVyr	TR/Hijacker.Gen	20130221
Antiy-AVL	-	20130220
Avast	Win32.Malware-gen	20130221
AVG	Worm.Generic2.CMVO	20130221

Techniques antivirales

- Machine learning (AI) scan (anciennement scan Heuristique)
 - Principe
 - Recherche de codes se comportant comme des virus
 - Par exemple, une application qui cherche à modifier des entrées de la base de registre.
 - Attention, cela peut aussi être un comportement normal : par ex. installation d'un driver.
 - Totalise l'ensemble des comportements similaires à ceux d'un virus
 - Si ce total dépasse un seuil, l'application est suspecte.
 - Rend possible la détection de virus non connus (zero-day).
 - FortiGate scanne uniquement les fichiers exécutables Microsoft Windows
 - Inconvénients
 - Risque de faux positifs
 - Par défaut, les fichiers suspects ne sont pas bloqués (pour éviter les faux positifs).
 - Consomme plus de ressources que le scan par signatures
 - Sensible à certains mécanismes d'obfuscation

Techniques antivirales

- Analyse du comportement via une sandbox
 - Environnement d'exécution virtuel sécurisé
 - Permet d'exécuter les fichiers afin d'analyser leurs comportements et révéler les menaces inconnues (pour lesquelles il n'existe pas de signature).
 - Détection des attaques zero-day avec un haut niveau de certitude.
 - Détection et neutralisation
 - En cas de détection, génération possible de signatures et transmission aux autres équipements de sécurité.
 - Reporting
 - Un rapport détaillé sur la menace est fourni après l'analyse.



• • • 47

Techniques antivirales

- Analyse du comportement via une sandbox (suite)
 - Analyse avec une sandbox locale
 - Plus rapide mais nécessite l'achat et la maintenance du boîtier.
 - Analyse avec une sandbox dans le cloud
 - Plus lent, mais pas besoin de faire la maintenance.
 - Attention à la taille maximale des fichiers uploadé.
 - Deux types : FortiGate cloud ou FortiSandbox cloud



• • • 48

Techniques antivirales

- Analyse du comportement via une sandbox (suite)
 - Exemples de techniques d'évasion
 - Interaction humaine
 - Le code malicieux nécessite une action humaine pour s'exécuter (un clic de souris, du scrolling, ...).
 - Détection de sandbox
 - Le malware essaie de détecter s'il se trouve dans une sandbox.
 - S'il y arrive, la partie malicieuse reste en sommeil.
 - Fragmentation des données
 - Les paquets malicieux sont fragmentés en paquets plus petits.
 - Ces petits paquets contenant chacun une partie du malware ne sont pas envoyés directement l'un après l'autre mais en attendant un certains laps de temps.
 - Utilisation de packer ou crypter
 - Programme dont le but va être de compresser et chiffrer, par exemple des exécutables, pour cacher un objet malveillant.
 - Utile pour les pirates mais aussi pour le pentesting.
 - ...

Techniques antivirales

- Exemples de techniques d'évasion (suite)
 - Exemple d'un Crypter
 - Permet de chiffrer les malware pour tenter de les rendre plus difficilement détectables.
 - Permet de compiler du code source à la volée pour modifier les signatures.
 - Permet d'insérer des fonctions de détection de sandbox ou de VM.
 - ...



Techniques antivirales

- **Limites de l'analyse par sandbox**

- La configuration offrant la meilleure protection nécessite probablement trop de temps d'analyse.
- Nombre limité de VM → Limite le nombre de fichiers analysés simultanément.
- Les pirates utilisent des techniques d'évasion/obfuscation.
- Plus lent que les autres types d'analyse.



Un malware peut passer inaperçu dans une sandbox

Techniques antivirales

- **FortiGuard Protection Services**

- **Virus Outbreak Prevention**

- **Virus n'ayant pas encore de signature**

- Il faut un certain temps pour créer et distribuer une signature de virus, ce qui peut laisser le temps à un nouveau virus de se répandre.

- **Principe**

- Virus Outbreak Prevention permet de filtrer des virus n'ayant pas encore de signature en se basant sur des hashs.
- Une requête est envoyées en temps réel à Fortiguard pour obtenir une évaluation basée sur les hashs du fichier.

- **Nécessite une license Zero-Hour Virus Outbreak (ZHVO)**



Techniques antivirales

- FortiGuard Protection Services (suite)
 - Malware block list
 - Liste de malwares complémentaire à la DB FortiGate
 - Il est possible d'enrichir la base de données antivirus en liant à FortiGate une liste externe de hash à bloquer.
 - La liste est hébergée sur un serveur web
 - Disponible via l'URL HTTP(S) définie dans la "Security Fabric malware hash list".
 - Elle se présente sous la forme d'un fichier texte contenant une liste de hachages MD5, SHA1 et SHA256.
 - Connecteur Security Fabric
 - La liste de blocage peut être définie comme un connecteur Security Fabric et configurée pour extraire la liste de façon dynamique.
 - La fréquence de rafraîchissement peut être configurée.



• • • 53

Techniques antivirales

- FortiGuard Protection Services (suite)
 - Content Disarm and Reconstruction (CDR)
 - Principe
 - Certains malwares ne sont présents que dans une partie d'un fichier.
 - » Les documents Microsoft Office sont structurés comme des fichiers ZIP, contenant des dossiers avec un certain nombre de fichiers différents.
 - CDR enlève les contenus de fichiers jugés malicieux, exploitables ou non sûrs mais envoie le reste du document à l'utilisateur.
 - FortiGate envoie le fichier original (complet) à une sandbox pour inspection.
 - Le client reçoit la version propre du document qui contient une page de couverture renvoyant vers le document original via la sandbox.
 - Contenus et protocoles supportés
 - Fichiers PDF, fichiers Microsoft Office.
 - Téléchargement Web HTTP, l'envoi d'e-mails SMTP, la réception d'e-mails IMAP et



• • • 54

Techniques antivirales

- Machine learning

- Domaine de l'intelligence artificielle

- Il permet aux ordinateurs d'effectuer des tâches pour lesquelles ils ne sont pas explicitement programmés.
 - Ils réalisent ces tâches en apprenant à partir de données d'apprentissage.



Techniques antivirales

- Machine learning et cybersécurité

- De plus en plus intégrés dans les solutions de sécurité

- Notamment sur les solutions de protection des postes clients.

- Les fichiers sont décomposés en petites parties

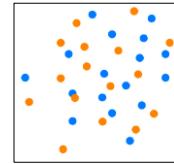
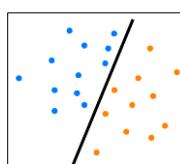
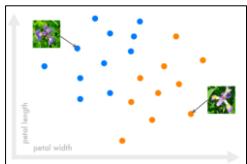
- Un peu comme si l'on regardait l'ADN du fichier.
→ permet de détecter des "traces" de malwares, même des malwares dont la signature n'est pas connue.

- Pas infaillible → faut garder les autres techniques.

Techniques antivirales

- **Limites du Machine learning**

- Il est nécessaire que les résultats que l'on souhaite prédire soient différentiables.



- Les algorithmes sont incapables d'extrapoler les données de manière fiable

- Il est donc nécessaire de faire des prédictions uniquement sur le même domaine de données que celui utilisé pour l'apprentissage.

- Pour les classifications, il est important d'avoir suffisamment d'éléments de chaque classe.

Protection anti-malware

- **Protection contre les malwares**

- Mécanismes d'évasion, nombreux nouveaux malwares, ...

- Nécessité d'analyser en continu (pas juste à un moment).

- Nécessité d'avoir un plan B si un malware passe quand même.

- Sécurité rétrospective



- Analyse rétrospective

- Il faut pouvoir réévaluer ce fichier plus tard afin de vérifier s'il est toujours sain.

- Analyse forensique

- Analyse d'un système informatique après incident.

- **Il est avantageux de pouvoir disposer de points de contrôle à différents endroits du réseau (défense en profondeur)**

- NGFW.

- Web security appliance.

- Email security appliance.

- Endpoints protection.

- Private cloud virtual appliance.

- ...

AGIR :

- AVANT

- PENDANT

- APRES

HEH.be Sciences et technologies

Protection anti-malware

- Protection contre les malwares
 - Exemple d'importance d'une protection rétrospective et d'une bonne visibilité.

Dans cet exemple, les systèmes de sécurité n'ont pas vu qu'il s'agissait d'un malware lorsqu'il est entré dans le réseau.

Source : Cisco System Inc., Allez au-delà du contrôle et de la visibilité sur les applications. Choisissez un next-generation firewall axé sur les menaces, Webinar du 29 Septembre 2016

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

• • • 59

HEH.be Sciences et technologies

Antivirus FortiGate

- Scan Antivirus
 - Moteur antivirus et base de données de signatures
 - Chaque antivirus est constitué
 - D'un moteur de détection.
 - D'une base de données de signatures de virus.
 - Chaque éditeur utilise ses propres moteurs de détection et ses signatures.
 - Le nom d'un virus est composé de deux parties
 - <vector>/<pattern> : W32/Kryptik.EMT!tr
 - <vector> : Toujours le même pour le même virus
 - » W32 pour Windows 32 bits,
 - » W64 pour Windows 64 bits
 - » JS pour JavaScript
 - » ...
 - <pattern> : Varie selon le vendeur de solution A-V.

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

• • • 60

Antivirus FortiGate

- Scan Antivirus (suite)
 - Liste des Virus
 - <https://fortiguard.com/updates/antivirus>

Updated: Apr 10th, 2020 - 16:50
+ Added (19)

Updated: Apr 10th, 2020 - 17:49
+ Added (38)

Updated: Apr 10th, 2020 - 19:23
+ Added (12)

Updated: Apr 10th, 2020 - 20:58
+ Added (41)

Name	Status	Update
Adware/Ewind!Android		Sig Added
Android/Agent.BDS!tr.spy		Sig Added
W32/Agent.OFI!tr		Sig Added
W32/Agent.TJAX!tr.pws		Sig Added
W32/Alien.IMFJKXJ!tr		Sig Added
W32/CUOZ!tr		Sig Added
W32/ICUQ7 MW!tr		Sig Added

Antivirus FortiGate

- Scan Antivirus (suite)

At a glance:

ID	8203943
Released	Apr 10, 2020
Description	Apr 10, 2020
Updated	Apr 10, 2020

Detection Availability

FortiGate	
Active	<input type="radio"/>
Extended	<input checked="" type="radio"/>
Extreme	<input type="radio"/>
Mobile	<input type="radio"/>

Virus

W32/Agent.OFI!tr

Analysis

W32/Agent.OFI!tr is classified as a trojan.

A trojan is a type of malware that performs activities without the user's knowledge. These activities commonly include establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes.

The Fortinet Antivirus Analyst Team is constantly updating our descriptions. Please check the FortiGuard Encyclopedia regularly for updates.

Antivirus FortiGate

- Scan Antivirus (suite)
 - Le scan analyse les fichiers à la recherche de virus
 - Déetecte et bloque les malwares en temps réel
 - Le moteur A-V vérifie la correspondance avec la signature d'un virus connu.
 - Empêche la propagation des menaces au sein du réseau
 - Important si l'on ne peut pas contrôler l'A-V de tous les postes du réseau (BYOD).
 - Important car on ne peut pas installer d'A-V sur tous périphériques du réseau (imprimantes, matériel médical, ...).
 - Preserve la réputation de l'IP publique de l'entreprise
 - Empêche la distribution des malwares depuis l'IP de l'entreprise.
 - Méthode rapide et simple pour détecter des malwares
 - Mais impossible de disposer d'une liste exhaustive et à jour de virus.

Antivirus FortiGate

- Scan antigrayware
 - Grayware
 - Applications ou fichiers qui ne sont pas considérés comme des virus mais qui peuvent avoir des effets indésirables (par exemple les adwares).
 - Ils ne sont pas franchement malveillants, mais ils ne sont pas non plus inoffensifs.
 - Peuvent faire perdre du temps, de la productivité ou consommer des ressources.
 - Grayware Scan
 - Les graywares sont détectables de la même manière que les virus.
 - Souvent ils sont détectés avec une simple signature.
 - Sur FortiGate, la protection contre les graywares est activée par défaut

# config antivirus setting (settings) # set grayware {enable disable} (settings) # end	FGT60D4Q16067135 (settings) # get default-db : extended grayware : enable
---	---

Antivirus FortiGate

- AI Scan

- Activer le scan heuristique (CLI uniquement)

```
config antivirus settings
    set machine-learning-detection {enable| monitor | disable}
end
```

- Options

- Pass

- Active le scan heuristique et la journalisation.
- Laisse passer les fichiers suspicieux.

- Block

- Active le scan heuristique et la journalisation.
- Ne laisse pas passer les fichiers suspicieux.

- Disable

- Désactive le scan heuristique.

Conseil :

Commencer par utiliser l'option **pass** afin d'analyser les logs et pouvoir mieux déterminer les éléments à bloquer.

Ordre des scans

1. Scan antivirus
2. Scan antigrayware
3. Scan heuristique



65

Antivirus FortiGate

- Sandbox

- Quels fichiers envoyer à une sandbox ?

- Soit tous les types de fichiers supportés, soit laisser FortiGate (FortiGuard) choisir quels fichiers envoyer en fonction du climat de menace actuel.
- Exemptions possibles.

Security Profile > AntiVirus

Send files to FortiSandbox for inspection	<input checked="" type="radio"/> Post Transfer
Scan strategy	<input checked="" type="radio"/> Post Transfer
File types	<input checked="" type="radio"/> Suspicious Files Only
Do not submit files matching types	<input type="radio"/>
Do not submit files matching file name patterns	<input type="radio"/>
Use FortiSandbox database	<input checked="" type="radio"/>

Autorise FortiGate à utiliser la DB
FortiSandbox en complément à sa propre DB.

Security Fabric > Fabric Connectors

The screenshot shows two fabric connectors:

- FortiSandbox:** Status: Enabled, Type: On-Premises, Server: 10.0.1.201, Notifier email: admin@fortinet.com
- Core Network Security:** Status: Enabled, Type: FortiGate Cloud, Region: Global



66

HEH.be Sciences et technologies

Antivirus FortiGate

– Quels fichiers envoyer à une sandbox ? (suite)

Inline: activable uniquement en CLI et en mode d'inspection proxy

Le fichier continuera d'être transmis au client sans attendre le résultat de l'analyse de la sandbox.

```
config system fortisandbox
    set inline-scan {enable | disable}
end
```

• • • 67

HEH.be Sciences et technologies

Antivirus FortiGate

- Mise à jour de la base de données de signatures antivirales
 - Prérequis
 - Nécessite une souscription à FortiGuard antivirus.
 - Nécessite d'avoir activé le scan antivirus dans au moins une règle de pare-feu.
 - Vérifier si l'antivirus est à jour

System > FortiGuard	
AntiVirus	Licensed (Expires on 2017-03-17) <input type="button" value="Upload Package"/>
AV Definitions	Version 35.00254
AV Engine	Version 5.00234

```
config antivirus settings
    set default-db {normal | extended | extreme}
End

diagnose autoupdate status
diagnose autoupdate versions
```

- Choisir une base de données (CLI only)
 - Normal** : Inclut les signatures d'attaques récentes courantes.
 - Extended** : Inclut plus de signatures de virus, actifs ou non.
 - Extreme** : Inclut une DB de virus étendues ainsi que les anciens virus dormants. Disponible sur la plupart des FortiGate mais pas tous les modèles.

• • • 68

HEH.be
Sciences
et technologies

Antivirus FortiGate

- Mise à jour de la base de données de signatures antivirales (suite)
 - Méthodes de mise à jour
 - Push** : permet d'accepter les nouvelles mises à jour dès qu'elles sont publiées par Fortiguard.
 - Schedule** : permet de configurer des mises à jour régulières .
 - Manual** : nécessite de télécharger les paquetages et les charger manuellement dans le FortiGate.

Replacement Messages

FortiGuard

External Security Devices

Advanced

Feature Select

Certificates

AntiVirus & IPS Updates

Accept push updates

Scheduled Updates

Improve IPS quality

Use extended IPS signature package

Daily ▾ 1 AM ▾

Update AV & IPS Definitions

WALLONIE-BRUXELLES ENSEIGNEMENT

DU Professeur

• • • 69

HEH.be
Sciences
et technologies

Modes d'inspection

- Flow-based inspection mode
 - Mode flux (Pas de proxy)
 - Les paquets sont mis en cache et transmis immédiatement
 - Consomme plus de CPU que le mode proxy-based.
 - Avantageux de disposer de puces FortiAsic.
 - Supporte moins de fonctions de sécurité (pas SSH, pas MAPI).
 - A l'exception du dernier paquet, les paquets ne sont pas retardés
 - Il est nécessaire d'extraire la charge utile pour découvrir si elle est virale.
 - Les clients perçoivent moins de latence qu'avec le mode proxy-based.

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name	default
Comments	Scan files and block viruses. 29/255
AntiVirus scan	<input checked="" type="radio"/> Block <input type="radio"/> Monitor
Feature set	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based

WALLONIE-BRUXELLES ENSEIGNEMENT

DU Professeur

• • • 70

Modes d'inspection

- Flow-based inspection mode (Cont.)
 2. Une copie des paquets est conservée en mémoire tampon
 - Le moteur antivirus scanne le fichier
 - Uniquement lorsque le dernier paquet est bufférisé.
 - Ce dernier paquet n'est pas transmis, on attend le résultat du scan.
 - Fichiers de grande taille
 - Les fichiers de taille supérieure à celle de la mémoire tampon ne sont pas scannés.
 - Full scan
 - Le scan utilise l'entièreté de la base de données antivirale configurée (Normal, extended ou extreme → Extended par défaut)
 3. Si le fichier est sain :
 - Le dernier paquet est transmis à la fin du scan.

Modes d'inspection

- Flow-based inspection mode (Cont.)
 4. Si le fichier est suspect
 - Le dernier paquet des fichiers suspects n'est pas transmis
 - La connexion est alors réinitialisée.
 - Si le virus est détecté alors que des paquets ont déjà été envoyés au client :
 - Le client ne reçoit pas de message signalant le blocage du fichier.
 - L'UTM place en cache l'URL du fichier.
 - » Si le client tente de télécharger le fichier, un message de blocage est envoyé.
 - Si le virus est détecté au début du flux
 - Un message de blocage est envoyé dès la première tentative de téléchargement.

Modes d'inspection

- **Proxy-based inspection mode**

1. Le proxy du protocole concerné intercepte la connexion et bufferise le fichier
 - Transparent pour l'utilisateur.
 - Aucune partie du fichier n'est transmise à l'utilisateur.
2. Le moteur antivirus examine le fichier entièrement bufférisé
 - **Scanne le fichier jusqu'à**
 - La taille maximum définie.
 - La taille de la mémoire tampon.
 - **Un grand fichier ne peut pas être scanné**
 - Nécessité d'avoir aussi un A-V sur le poste client.
 - Possibilité de laisser passer ou bloquer les fichiers > à la taille de la mémoire tampon.
 - **Full scan**
 - Le scan utilise l'entièreté de la base de données antivirale configurée (Normal, extended ou extreme).

Les virus sont souvent détectés dans les deux premiers Mo du fichier.

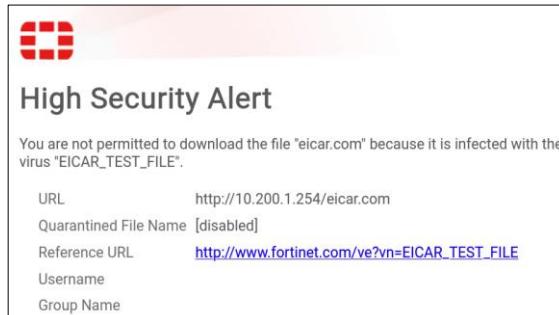
Modes d'inspection

- **Proxy-based inspection mode (suite)**

3. Si les fichiers sont sains
 - Les paquets sont transmis uniquement à la fin du scan.
 - Une latence perceptible par les utilisateurs est possible.
 - Suivant les performances de l'UTM et la quantité de trafic à traiter.
 - Si tous les paquets ne sont pas reçus suffisamment rapidement, le client pourrait mettre fin à la connexion.
 - Il est possible de configurer le proxy pour délivrer lentement les paquets afin de lui permettre de compléter son buffer et scanner le fichier.
4. Les fichiers suspects sont soumis à l'action pass ou block
 - Si l'action est block, aucun paquet n'a été transmis aux clients.
 - Les clients sont toujours informés du blocage du fichier via un message.

Modes d'inspection

- Page de blocage
 - Exemple



Modes d'inspection

- Comparaison des modes d'inspection

Edit AntiVirus Profile

Comments	Write a comment...
AntiVirus scan	<input checked="" type="radio"/> Block <input type="radio"/> Monitor
Feature set	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Inspected Protocols	
HTTP	<input checked="" type="radio"/>
SMTP	<input checked="" type="radio"/>
POP3	<input checked="" type="radio"/>
IMAP	<input checked="" type="radio"/>
FTP	<input checked="" type="radio"/>
CIFS	<input checked="" type="radio"/>
APT Protection Options	
Treat Windows executables	<input checked="" type="radio"/>

Edit AntiVirus Profile

Name	AV-Monitor
Comments	Write a comment...
AntiVirus scan	<input checked="" type="radio"/> Block <input type="radio"/> Monitor
Feature set	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Inspected Protocols	
HTTP	<input checked="" type="radio"/>
SMTP	<input checked="" type="radio"/>
POP3	<input checked="" type="radio"/>
IMAP	<input checked="" type="radio"/>
FTP	<input checked="" type="radio"/>
CIFS	<input checked="" type="radio"/>
MAPI	<input checked="" type="radio"/>
SSH	<input checked="" type="radio"/>
APT Protection Options	
Content Disarm and Reconstruction	<input checked="" type="radio"/>

Configuration de l'antivirus

- Security Profiles > AntiVirus

Activé par défaut

Contain des signatures pour les logiciels malveillants ciblant les smartphones.

Les fichiers malicieux peuvent être bloqués, Monitorés ou mis en quarantaine.

FortiClient Enterprise Management Server : solution de gestion centralisée de plusieurs points d'extrémité (ordinateurs).

77

Configuration de l'antivirus

- Configuration des options de protocole

→ Les options de protocole sont utilisées par les antivirus mais aussi par d'autres profils de Sécurité (filtrage Web, DLP, ...)

Permet l'analyse antivirus des e-mails Microsoft Exchange Server qui utilisent le protocole RPC sur HTTP.

Configuration du mappage de ports (plusieurs ports possibles).

Policy & Objects > Protocol Options

Protocol	Port	Action	Port
HTTP	Any	Specify	80
SMTP	Any	Specify	25
POP3	Any	Specify	110
IMAP	Any	Specify	143
FTP	Any	Specify	21
NNTP	Any	Specify	119
MAPI			135
DNS			53

78

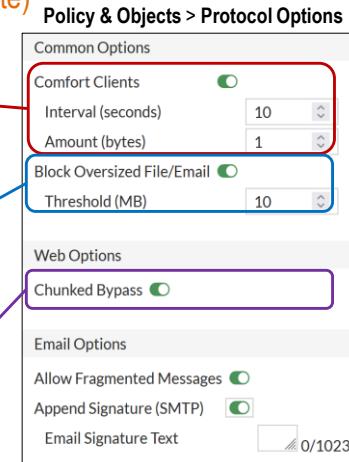
Configuration de l'antivirus

- Configuration des options de protocole (suite)

Envoie petit à petit le fichier au client pendant qu'il est scanné. Évite que les clients impatients annulent le téléchargement en ne le voyant pas démarrer.
Disponible pour HTTP(S) et FTP(S).

Bloque les fichiers de taille > seuil/buffer
Permet de fixer à partir de quelle taille les fichiers ne seront pas scannés mais directement bloqués.

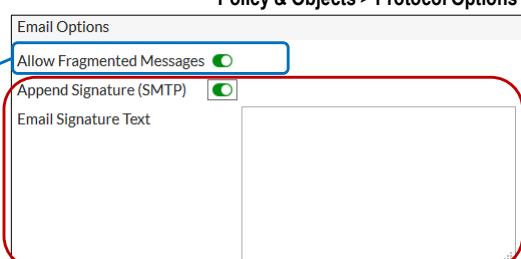
Certains serveurs temps réel peuvent envoyer des données à un applet en utilisant des messages HTTP. Le proxy AV ne détectera jamais la fin du flux TCP et pourrait donc bloquer le flux.



Configuration de l'antivirus

- Configuration des options de protocole (suite)

Autorise les fichiers fragmentés.
Anciennement utilisé par les messageries pour fragmenter les mails volumineux et transmettre les fragments en parallèle sur des lignes bas débit.



Permet de s'assurer que les emails sortants contiennent tous les termes souhaités par l'entreprise (par exemple des clauses de non responsabilité).
Cette signature annexe est ajoutée après la signature personnelle de l'utilisateur.

Configuration de l'antivirus

- Gestion des grands fichiers

- Rappel :

- Par défaut, les fichiers plus grand que le buffer ne sont pas scannés.
 - Par défaut, pas de log des fichiers "trop" grands.
 - Par défaut, pas de blocage des fichiers "trop" grands.

- Option **Oversize-limit**

- Permet d'ajuster la taille du buffer (10Mo par défaut)

- Un buffer plus petit permet de réduire la latence et utilise moins de RAM.
 - Un buffer plus grand améliore la sécurité en permettant de scanner de plus gros fichiers.

```
config firewall profile-protocol-options
edit <profile_name>
  config <protocol_name>
    set oversize-limit [1-<model_limit>]
    oversize-limit      Enter an integer value from <1> to <183>
  end
```

Configuration de l'antivirus

- Gestion des grands fichiers

- Les options **Oversize** et **Oversize-log**

- L'option **oversize** bloque les fichiers plus grands que le buffer.
 - L'option **oversize-log**
 - Quand elle est activée, FortiGate consigne si des fichiers grande taille ont été bloqués ou autorisés à passer.
 - Permet de savoir si le FortiGate voit passer beaucoup de grands fichiers afin de déterminer s'il est intéressant de les bloquer ou non.

```
config firewall profile-protocol-options
edit <profile_name>
  set oversize-log {enable|disable}          → Configuration globale.
  config <protocol_name>
    set oversize-limit [1-<model_limit>]
    set options oversize
```

Configuration par protocole

Configuration de l'antivirus

- Gestion des grands fichiers (suite)
 - Seuil par défaut de 10Mo
 - Avec le seuil par défaut de 10 Mo, seulement 0,01% des virus passent.

	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB
exploit	99.83%	99.95%	99.97%	99.97%	99.98%	99.98%	99.99%	100%	100%	100%
mass-mailer	99.62%	99.87%	100%	100%	100%	100%	100%	100%	100%	100%
phish	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
spyware	95.08%	97.97%	98.88%	99.47%	99.76%	99.83%	99.89%	99.91%	99.94%	99.95%
trojan	97.52%	99.24%	99.62%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.98%
virus	98.27%	99.37%	99.63%	99.80%	99.88%	99.93%	99.95%	99.97%	99.98%	99.99%
worm	99.02%	99.65%	99.74%	99.86%	99.89%	99.92%	99.94%	99.94%	99.95%	99.96%

Source : Fortinet Inc.

Configuration de l'antivirus

- Gestion des fichiers compressés
 - Compression et scan antivirus
 - Si un fichier est compressé, sa signature est différente.
 - Il est donc nécessaire de décompresser le fichier avant le scan.
 - Décompression des fichiers
 - Il faut utiliser le bon algorithme de décompression.
 - Certains formats de compression peuvent être trouvés en analysant les en-têtes.
 - Fichiers compressés protégés par mot de passe
 - L'UTM ne pourra pas décompresser ni scanner le fichier !
 - Compressions imbriquées (nested archive)
 - Si un fichier a été compressé plusieurs fois, l'UTM décompressera tous les niveaux de compression.
 - Jusqu'à 12 niveaux par défaut.
 - Modifiable jusqu'à 100 niveaux (attention à la consommation de RAM).

Configuration de l'antivirus

- Gestion des fichiers compressés (suite)
 - Taille limite
 - La taille limite des fichiers compressés est différente de celle des autres fichiers.

Configuration par protocole

```
config firewall profile-protocol-options
edit <profile_name>
  config <protocol_name>
    set uncompressed-oversize-limit [1-<model_limit>]
    set uncompressed-nest-limit [1-200]
  end
end
```

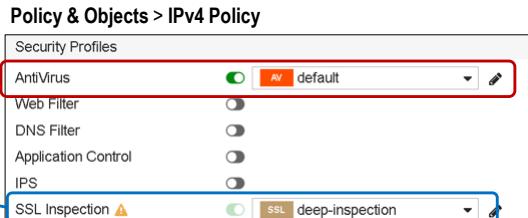
Fixe la taille maximale des fichiers décompressés qui seront soumis au scan antivirus

Fixe le nombre de compressions imbriquées maximales que l'UTM pourra décompresser

Configuration de l'antivirus

- Activer l'antivirus
 - Règles de Pare-feu
 - Pour que le profil de sécurité antivirus défini soit actif, il faudra l'appliquer à une règle de sécurité.

Activer l'inspection SSL/SSH et sélectionner "deep-inspection" afin de pouvoir contrôler le trafic chiffré



HEH.be
Sciences
et technologies

Configuration de l'antivirus

- Eicar test file
 - Fichier qui a une signature correspondant à un virus mais qui ne contient pas de charge active.

HEH.be
Sciences
et technologies

« Conserve mode »

- Conserve mode
 - Quantité de mémoire limitée
 - Si la mémoire vient à manquer, FortiOS ne peut plus s'acquitter de ses tâches et pourrait agir de manière inattendue.
 - Pour éviter cette incertitude, FortiOS entre en « conserve mode ».
 - Seuils
 - Seuil « red » (par ex. 88% de mémoire utilisée)
 - FortiOS entre en « conserve mode » lorsqu'il atteint le seuil rouge:
 - » Il génère des messages de journal (log).
 - » Il génère des trap SNMP.
 - » Il affiche une bannière qui apparaît sur l'interface graphique.
 - Seuil extrême (Par ex. 95% de mémoire utilisée)
 - Le « conserve mode » se poursuit, de plus les nouvelles sessions sont abandonnées.
 - Seuil « green » (Par ex. 82 % de mémoire utilisée)
 - Le conserve mode se poursuit jusqu'à ce que l'utilisation de la mémoire soit réduite au seuil « green ».

« Conserve mode »

- Fonctionnement de l'antivirus en « conserve mode »
 - Off
 - Tout trafic devant être inspecté par le proxy antivirus est bloqué.
 - Les nouvelles sessions ne sont pas autorisées, mais les sessions en cours continuent d'être traitées normalement, à moins qu'elles ne demandent plus de mémoire.
 - A utiliser lorsque la sécurité est plus importante qu'une perte d'accès momentanée.
 - Pass
 - Permet au trafic de continuer vers sa destination mais aucune analyse antivirus n'est effectuée.
 - Les profils de sécurité n'utilisant pas le proxy antivirus sont effectués normalement.
 - One-shot
 - Similaire au paramètre « pass » mais l'antivirus reste dans ce mode même après avoir quitté le « conserve mode ».
 - Il reprend l'utilisation du proxy AV uniquement lorsque le paramètre av-failopen est modifié ou lorsque le FortiGate est redémarré.

« Conserve mode »

- Configuration du « Conserve mode »
 - Configuration des seuils
 - Fortinet recommande de ne pas les modifier

```
config system global
  set memory-use-threshold-extreme 95
  set memory-use-threshold-red 88
  set memory-use-threshold-green 82
end
```

- Vérification des seuils

```
FGVM # diagnose hardware sysinfo conserve
memory conserve mode: off
total RAM: 994 MB
memory used: 448 MB 45% of total RAM
memory used threshold extreme: 944 MB 95% of total RAM
memory used threshold red: 874 MB 88% of total RAM
memory used threshold green: 815 MB 82% of total RAM
```

« Conserve mode »

- Configuration du « Conserve mode » (suite)

- Configuration du paramètre « av-failopen »

```
config system global
    set av-failopen {pass | off | one-shot}
end
```

- Vérifier si le FortiGate est en « conserve mode »

- conservemode: 0 → Le FortiGate n'est pas en "conserve mode"
 - conservemode: 1 → Le FortiGate est entré en "conserve mode"

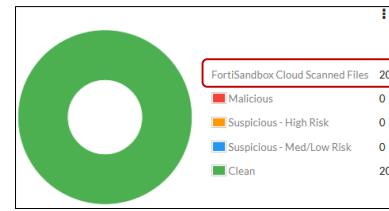
```
# diag hardware sysinfo shm
SHM counter: 67
SHM allocated: 1556480
SHM total: 101220352
conservemode: 0
```

Configuration de l'antivirus

- Advanced Threat Protection Statistics

- Fournit des statistiques en temps réel relatives aux analyses antivirus

Dashboard Widget



Configuration de l'antivirus

- Activez la journalisation (règle de pare-feu)

Log & Report > Security Events

#	Date/Time	Source	File Name	Virus/Botnet	User	Details	Action	Submitted to FortiSandbox
21	07-24-10:59	HTTP	10.0.1.10	8-0-General-Info.html		host:2132.11.198.62	analytics	true
22	07-24-12:07	HTTP	10.0.1.10	Projects.html		host:2132.11.198.62	analytics	false
23	07-24-12:26	HTTP	10.0.1.10	elcar.com	EICAR TEST FILE	host:2132.11.198.62	blocked	false
24	07-24-12:26	HTTP	10.0.1.10	elcar.com	EICAR TEST FILE	host:2132.11.198.62	blocked	false
25	07-21-09:16	HTTP	10.0.1.10	8-0-Download.html		host:2132.11.198.62	monitored	
26	07-21-09:16	HTTP	10.0.1.10	search		host:208.9.11.114.28	monitored	
27	07-21-09:11	HTTP	10.0.1.10	8-6-Intended-use.html		host:213.2.11.198.62	monitored	
28	07-21-09:11	HTTP	10.0.1.10	vendor.min.js		host:208.9.11.114.28	monitored	
29	07-21-09:11	HTTP	10.0.1.10	easySlider.1.7.js		host:213.2.11.198.62	monitored	
30	07-21-09:11	HTTP	10.0.1.10	jquery2.js		host:213.2.11.198.62	monitored	

Log Details	
Application	Protocol 6
Service	HTTP
Data	File Name: elcar.com
Action	Action: blocked
Policy	Policy: 1
Level	critical
Threat Level	critical
Threat Score	50
AntiVirus	
Profile Name	default
Virus/Botnet	EICAR_TEST_FILE
Virus ID	2172
Reference	http://www.fortinet.com/virus/
Detection Type	Virus
Direction	Incoming
Quarantine Skip	File was not-quarantined.
FortiSandbox Checksum	275a021bbf6489e544d7389
Submitted to FortiSandbox	false
Message	File is infected.
Other	File was not-quarantined. http://www.fortinet.com/virus/

Log & Report > Forward Traffic

#	Date/Time	Source	Description	Application Name	Security Events	Result	Policy	Log Details
1	07-21-09:10	10.0.1.10	HTTP/208.9.11.114.28/www.elcar.guard.com	Fortinet Web	✓ 2.0KB / 7.25KB	1 Full-Access		
2	07-21-09:10	10.0.1.10	HTTP/208.9.11.114.28/www.elcar.guard.com	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
3	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
4	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
5	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/?	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
6	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
7	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
8	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
9	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
10	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
11	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
12	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
13	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
14	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
15	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
16	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
17	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
18	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
19	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
20	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
21	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
22	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
23	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
24	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
25	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
26	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
27	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
28	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
29	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		
30	07-21-09:10	10.0.1.10	HTTP/213.2.11.198.62/www.elcar.org/208.9.11.114.28	Fortinet Web	✓ 0.0KB / 9.37 KB	1 Full-Access		

93

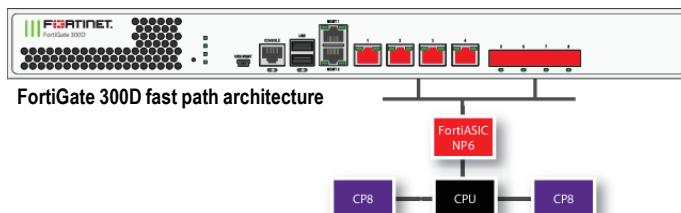
Accélération matérielle

- Hardware acceleration

– Certains modèles FortiGate possèdent des puces spécialisées

- Ces puces peuvent décharger le processeur des tâches d'inspection pour améliorer les performances
- Les modèles FortiGate avec NTurbo (NP4 ou NP6).
- Les modèles FortiGate avec SoC3.

– Accélération matérielle uniquement disponible en mode flow-based

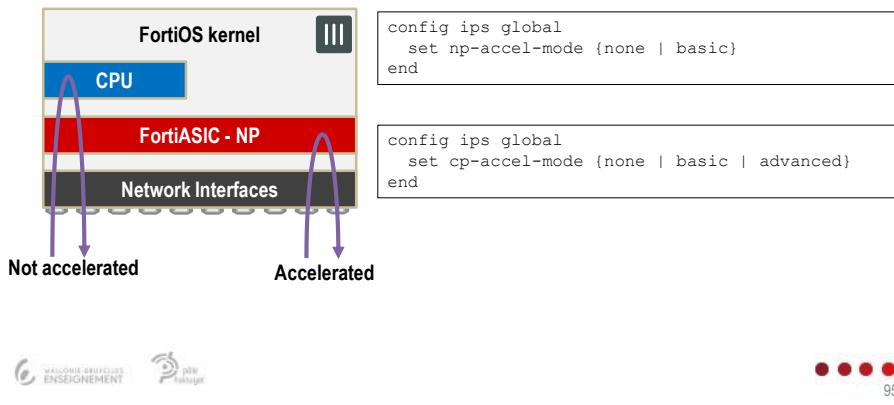


94

Accélération matérielle

- Hardware acceleration

- Ce qui peut être accéléré et la manière dont l'accélération s'effectue dépend du type de puce utilisée (NP, CP, SP)



Configuration de l'antivirus

- Recommandations

- Activer le scan antivirus
 - En bordure de réseau, pour tout le trafic Internet, avec SSL deep-inspection.
 - Sur tous les FW d'un cluster HA.
- Configurez les mises à jour automatique Fortiguard (push updates)
 - Si l'UTM le supporte, activer la base de données de virus étendue.
- Journalisez les événements de sécurité
 - Activez la journalisation des fichiers trop grands pour être scannés.
 - Examinez périodiquement les journaux antivirus.
- Activez l'option "Treat Windows Executables in Email Attachments as Viruses"

Recommandations

- Recommandations (suite)

- N'augmentez pas la taille maximale des fichiers à scanner, sauf si cela est nécessaire
 - Généralement pas nécessaire car les virus sont souvent des petits fichiers.
 - Cela consommerait plus de mémoire.
- Utilisez l'accélération matérielle
 - Uniquement en mode flow-based.
 - En mode proxy, le trafic ne peut pas être accéléré.
- Ne vous limitez pas à l'antivirus du FortiGate
 - Utilisez un antivirus sur toutes les stations de travail.
 - Utilisez une sandbox.

Dépannage

- Résolution de problème

- Le service FortiGuard update est-il accessible ?
 - Vérifiez votre connexion à l'internet.
 - Vérifiez que le FortiGate est capable de résolutions DNS (update.fortiguard.net).
 - Vérifiez que le port TCP 443 est ouvert.
- La licence FortiGuard est-elle toujours valide?

System > FortiGuard

License Information		Status
Contract		
FortiCare Support	Registered - denis.mandoux@heh.be	<input type="button" value="Launch Portal"/>
Hardware Version	Return to factory - expired on 2018/12/03	
Firmware	Web/online - expired on 2018/12/03	
Enhanced Support	8x5 support - expired on 2018/12/03	
Application Control Signatures	Version 6.00741	<input type="button" value="Upgrade Database"/>
AntiVirus	Expired - expired on 2018/12/03	<input type="button" value="Upgrade Database"/>
AV Definitions	Version 75.00039	
AV Engine	Version 5.00361	

Dépannage

- Résolution de problème

- La version de la base de données antivirus est-elle à jour?

- Consultez le site web FortiGuard
<https://fortiguard.com/updates/antivirus>

Updated: Apr 20th, 2020 - 01:42
+ Added (24)
🕒 Modified (77)
Latest Versions
76.834

- Démarrer un mise à jour manuelle.

```
# execute update-av
```

- Le scan antivirus ne détecte pas les virus

- Vérifiez la configuration

- Vérifiez que le profil antivirus est appliqué sur au moins une règle de pare-feu.
- Vérifiez que le bon profil antivirus est sélectionné.
- Vérifiez que les options de protocole sont correctes (par exemple l'inspection SSH/SSL).
- Vérifiez que la configuration antivirus s'applique bien à toutes les connexions redondantes.

Dépannage

- Résolution de problème

- Utiliser les commandes de dépannage

```
# get system performance status
    → Affiche les statistiques sur les virus pour la dernière minute écoulée.

# diagnose antivirus database-info
    → Affiche les informations actuelles de la base de données antivirus

# diagnose autoupdate versions
    → Affiche les versions actuelles du moteur antivirus et des signatures

# diagnose antivirus test "get scantime"
    → Affiche la durée d'analyse des fichiers infectés

# diagnose debug enable
    → active le débogage.

# diagnose debug application update -1
    → Affiche des informations détaillées de débogage relatives aux mises à jour
```

Test des AV et NGFW

- Test des solutions antivirus
 - Différents organismes réalisent des tests
 - ICSA labs.
 - NSS labs.
 - AV-comparatives.
 - Virusbulletin
 - ...

Technology Program	Vendor	Product Testing Reports	Certification	Product Version	Date	Certification Type	Operating Systems
Firewalls	A10 Networks	A10 Networks Thunder Series	Network Firewalls	current	04/17/2019	Corporate	Proprietary
Firewalls	Allied Telesis, Inc.	AR4050S	Network Firewalls	current	08/08/2018	Corporate	Proprietary
Firewalls	Microsoft Corporation	Azure Firewall	Network Firewalls	current	02/18/2020	Corporate	Proprietary
<Items omisés>							
Firewalls	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	Network Firewalls	current	09/05/2019	Corporate	Proprietary
		GaiaShield Next Generation Firewall	Network	current	07/24/2019	Corporate	Proprietary
		Certified Individually					

Avril 2020



juin 2020



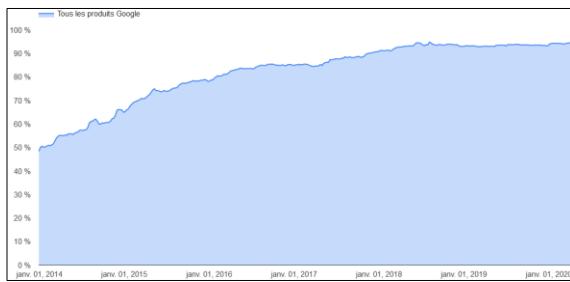
101

Inspection SSL/SSH

- Traffic chiffré
 - De plus en plus d'applications exploitent la technologie de chiffrement SSL/TLS
 - Les pirates peuvent masquer leurs malwares dans des communications chiffrées.

Google Transparency Report

Plus de 90 % des pages de Google Chrome aux États-Unis ont été chargées avec du chiffrement (HTTPS)



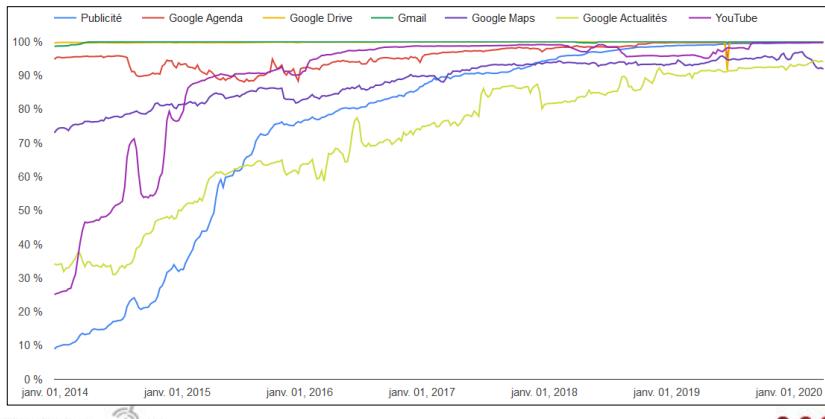
Source : <https://transparencyreport.google.com/https/overview>



102

- Trafic chiffré (suite)

- Evolution du trafic chiffré pour les produits Google



- Trafic chiffré (suite)

- Il n'est pas possible de lire son contenu

- Dès lors impossible de filtrer ou vérifier la présence de virus.

- Pour contrôler le trafic, il faut déchiffrer

- Les NGFW disposent de fonctionnalités de déchiffrement du trafic SSL/TLS et SSH.
 - Une fois déchiffré, il est possible d'appliquer de l'analyse antivirus, le filtrage Web ou encore le filtrage des e-mails.

- Deux méthodes d'inspection

- SSL Certificate Inspection

- Méthode plus rapide (moins de latences, moins de ressources) mais moins sécurisée.
 - Ne vérifie que la validité des certificats.

- Full SSL Inspection (Deep inspection)

- Offre une meilleure protection que le mode SSL Certificate Inspection
 - Introduit plus de latence et consomme plus de ressources.
 - Permet de déchiffrer le trafic SSL/SSH pour appliquer des profils de sécurité.

SSL Certificate Inspection

- **SSL Certificate Inspection**

- Utilisée pour vérifier l'identité des serveurs Web
 - L'UTM vérifie la validité du certificat pour le trafic chiffré
 - Les fichiers restent chiffrés et ne sont pas scannés.
 - Si le certificat est valide, le trafic est accepté, même s'il contient des virus.
- Utilisée pour permettre le filtrage Web
 - Le filtrage Web est la seule fonctionnalité de sécurité qui peut être appliquée en mode SSL Certificate Inspection.
 - Permet de vérifier que le protocole HTTPS n'est pas utilisé pour accéder à des sites normalement bloqués par le filtrage Web.

SSL Certificate Inspection

- **SSL Certificate Inspection Configuration**

A utiliser pour configurer un profil personnalisé pour un serveur précis avec un certificat spécifique.

A utiliser lorsque les destinataires ne sont pas connus.

Par défaut le profil est non modifiable → choisir « custom »

Indique quel certificat le FortiGate doit utiliser.

Edit SSL Inspection Profile	
Name	<input type="text"/>
Comments	<input type="text"/> 37/255
SSL Inspection Options	
Enable SSL Inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server
Inspection Method	SSL Certificate Inspection Full SSL Inspection
CA Certificate	Fortinet_CA_SSL <input type="button" value="Download Certificate"/>
Untrusted SSL Certificates	Allow Block <input type="button" value="View Trusted CAs List"/>

Security Profiles > SSL/SSH Inspection

custom-deep-inspection
certificate-inspection
custom-deep-inspection
deep-inspection

SSL Certificate Inspection

Edit SSL Inspection Profile

Name	custom-deep-inspection	custom-deep-inspection
Comments	Customizable deep inspection profile.	37/255
SSL Inspection Options		
Enable SSL Inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server	
Inspection Method	SSL Certificate Inspection	Full SSL Inspection
CA Certificate	Fortinet_CA_SSL	<input type="button" value="Download Certificate"/>
Untrusted SSL Certificates	Allow	Block
Protocol Port Mapping		
Inspect All Ports	<input checked="" type="checkbox"/>	443
HTTPS	<input checked="" type="checkbox"/>	
Common Options		
Allow Invalid SSL Certificates	<input checked="" type="checkbox"/>	
Log SSL anomalies	<input checked="" type="checkbox"/>	

Inspecte tous les ports ou uniquement le port par défaut pour HTTPS

Journalise si des certificats sont expirés ou « untrusted ».

• • • 107

Full SSL Inspection

- "Full SSL Inspection"

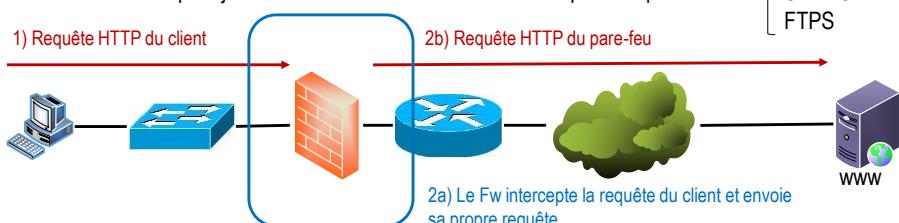
- Principe

1. Le client contacte le serveur Web

2. Le FortiGate agit en proxy :

- a) Il intercepte la requête du client.
- b) Il envoie sa propre requête vers le serveur Web.

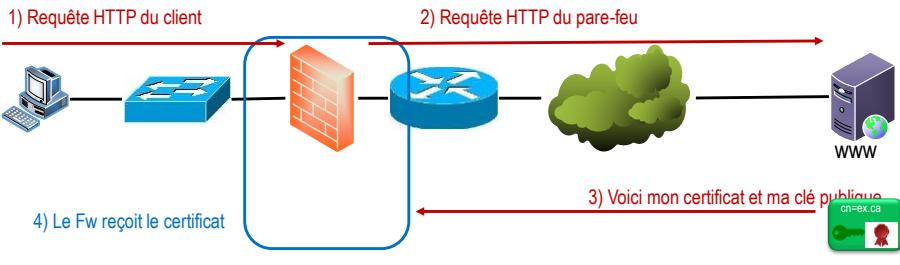
L'UTM peut jouer le rôle de la terminaison SSL/TLS pour les protocoles



Full SSL Inspection

– Principe (suite)

3. Le serveur Web répond en envoyant son certificat contenant sa clé publique.
4. Le FW reçoit le certificat suite à sa requête.



Full SSL Inspection

- Vérification du certificat du serveur par le FW :
 - Vérification s'il y a eu révocation du certificat
 - Télécharger les listes de révocation de certificats (CRL) sur le FortiGate ou configurer le FortiGate pour utiliser OCSP.
 - Les certificats sont identifiés par un numéro de série sur la CRL.
 - Possession du certificat de l'AC
 - FortiGate utilise la valeur « Issuer » pour déterminer s'il possède le certificat CA correspondant dans son magasin.
 - Dates de validité
 - Vérification de la signature numérique

cn=ex.ca	
Field	Value
Version	v3
Serial number	7e 9b 8a 8d 00 00 00 00 6b
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	fortinet-us-FGT-NPS-CA, forti...
Valid from	Tuesday, September 06, 2016...
Valid to	Wednesday, September 06, 2...
Subject	*****@*****.Training, Ottawa...
Public key	RSA (1024 Bits)
Certificate Template Name	EFS
Enhanced Key Usage	Encrypting File System (1.3.6....)
Key Usage	Key Encipherment (20)
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	11 d7 43 b3 be 04 4a f9 7d a0...
Authority Key Identifier	KeyID=f3 92 ec cb 4d cf e8 d4...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=d...
Thumbprint algorithm	sha1
Thumbprint	0b ba 6a 93 8d 77 0c 93 bb fb ...

Full SSL Inspection

– Principe (suite)

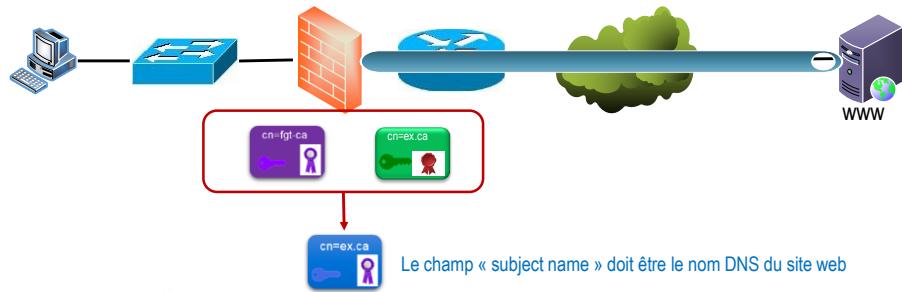
5. Le FW utilise le certifikat pour établir un tunnel chiffré avec le serveur



Full SSL Inspection

– Principe (suite)

6. Le FW génère un nouveau certifikat au nom du serveur
 - Pour cela, le FW doit disposer d'un certifikat permettant d'émettre des certifikats
 - » CA=True
 - » keyUsage=keyCertSign

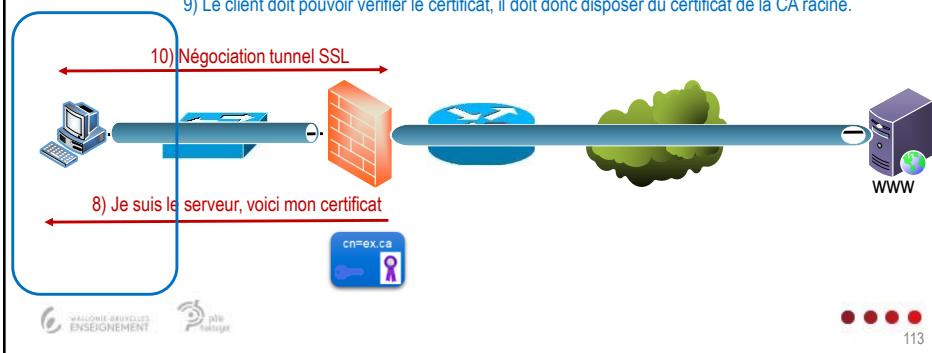


Full SSL Inspection

– Principe (suite)

7. Le FW utilise ce nouveau certificat afin de se faire passer pour le serveur et établir un tunnel chiffré avec le client.
8. Le client vérifie la validité du certificat.
9. Négociation pour établir un tunnel chiffré.

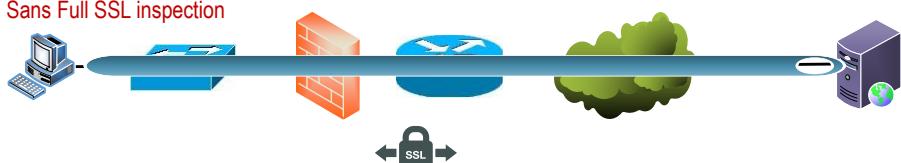
9) Le client doit pouvoir vérifier le certificat, il doit donc disposer du certificat de la CA racine.



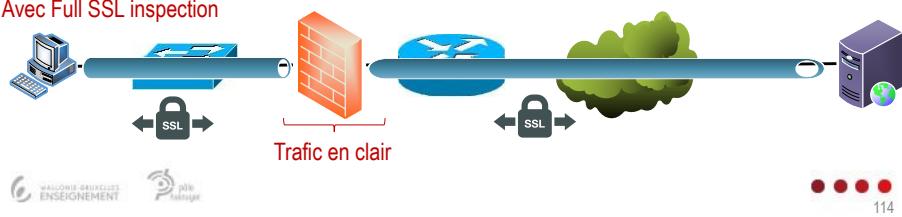
Full SSL Inspection

– Principe (suite)

Sans Full SSL inspection



Avec Full SSL inspection



Full SSL Inspection

- CA interne

- Émission de certificats

- Le FortiGate doit disposer d'un certificat permettant d'émettre des certificats
 - Chaque fois qu'un utilisateur interne se connecte à un serveur SSL externe, le FortiGate doit générer une clé privée et un certificat SSL (Il agit comme une CA).
 - La paire de clés et le certificat sont générés instantanément (pas de latence).
 - Un tel certificat doit avoir (selon la RFC 5280) :
 - CA=True
 - Key Usage=KeyCertSign

- Deux possibilités

- **Fortinet_CA_SSL**
 - Certificat local utilisé par défaut pour l'inspection SSL (auto-signé).
 - **Internal CA**
 - Autorité de certification interne au FortiGate lui permettant d'agir comme une CA subordonnée capable de délivrer des certificats.
 - Le certificat de l'autorité de certification racine doit être importé sur les machines clientes.

Full SSL Inspection

- "Untrusted and invalid certificates"

- Certificats non fiables, non approuvé (untrusted)

- Les certificats SSL auto-signés ne sont pas considérés comme de confiance.
 - Ils génèrent un avertissement dans le navigateur.
 - Indiquant que le navigateur ne peut pas vérifier l'identité du site Web.
 - Actions : Untrusted SSL Certificates Allow Block Ignore View Trusted CAs List

Allow : L'utilisateur reçoit un avertissement mais peut se rendre sur le site en ajoutant une exception au navigateur.

Block : Connexion au serveur bloquée, pas d'exception possible.

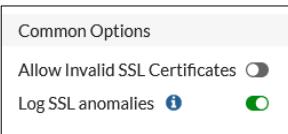
Ignore : FortiGate utilise toujours un certificat de confiance (Fortinet_CA_SSL) pour remplacer celui du serveur.

```
config firewall ssl-ssh-profile
  edit "SSL-Profile"
    config https
      set port 443
      set untrusted-server-cert ignore
    end
  end
```

HEH.be
Sciences
et technologies

Full SSL Inspection

- "Untrusted and invalid certificates" (Cont.)
 - FortiGate effectue les contrôles suivants sur les certificats :
 - Contrôle de la date de validité.
 - Contrôle de la signature du certificat.
 - Contrôle de la liste de révocation (CRL).
 - Certificats invalides (Invalid)
 - Par défaut, les certificats invalides (les certificats expirés, ...) génèrent un avertissement dans le navigateur.
 - Il est possible d'autoriser les certificats invalides.



Common Options

Allow Invalid SSL Certificates

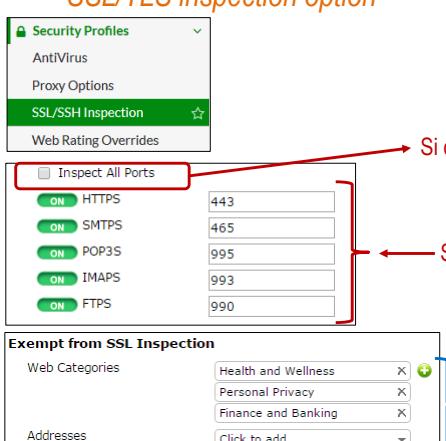
Log SSL anomalies

WALLONIE-BRUXELLES ENSEIGNEMENT  117

HEH.be
Sciences
et technologies

Full SSL Inspection

- SSL/TLS inspection option



Security Profiles

AntiVirus

Proxy Options

SSL/TLS Inspection 

Web Rating Overrides

Inspect All Ports

ON	HTTPS	443
ON	SMTPS	465
ON	POP3S	995
ON	IMAPS	993
ON	FTPS	990

Exempt from SSL Inspection

Web Categories

Health and Wellness 

Personal Privacy 

Finance and Banking 

Addresses

Click to add...

Si coché, inspecte tous les ports

Sinon, inspecte uniquement les ports spécifiés

Permet de définir des sites Web, des catégories ou encore des adresses exemptées de l'inspection. Obligation légale, HPKP, ...

WALLONIE-BRUXELLES ENSEIGNEMENT  118

Full SSL Inspection

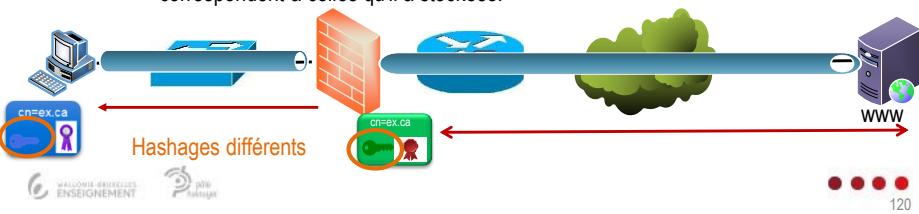
- Éviter les messages d'avertissement de certificat
 - a) Utiliser un certificat émis par une CA dont le certificat racine est présent dans la liste des autorités de certification racine de confiance du navigateur.
 - b) Si le certificat SSL est émis par une autorité de certification privée, installez le certificat dans la liste des autorités de certification racine de confiance.

FortiGate > System > Certificates

The screenshot shows the FortiGate configuration interface under 'System > Certificates'. It lists several certificates, including 'FGT' and 'Fortinet_CA_Signed' which is highlighted. A red box highlights the 'Download' button for the selected certificate. To the right, a modal window titled 'Gestionnaire de certificats' (Certificate Manager) is displayed, showing a list of registered root certificates. The 'Autorités' tab is selected, and a red box highlights the 'Ajouter...' (Add...) button. The bottom right corner of the slide shows a navigation bar with three dots and the number 119.

Full SSL Inspection

- HTTP Public Key Pinning
 - HPKP
 - Fonctionnalité de sécurité destinée à éviter les attaques MITM avec des certificats contrefaçons. Serveur Web et navigateur doivent être compatibles HPKP.
 - Technique TOFU, Trust on First Use
 - HPKP est une technique qui s'appuie sur la confiance au premier accès.
 - La première fois qu'un utilisateur visite un site, il va mettre en cache un certain temps les hachages d'une ou plusieurs clés publiques associées au site Web.
 - Lors des autres visites, le navigateur s'assurera que les clés publiques correspondent à celles qu'il a stockées.

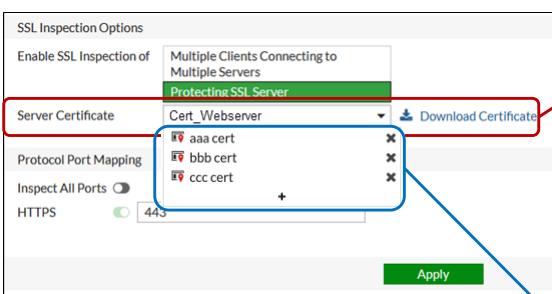


Full SSL Inspection

- Les options disponibles pour contourner le HPKP sont limitées
 - Exempter l'inspection SSL pour ces sites.
 - Utiliser l'inspection des certificats SSL à la place.
 - Utiliser un navigateur qui ne supporte pas HPKP
 - Internet Explorer, Edge et Chrome ne supporte pas HPKP.

Full SSL Inspection

- Protecting SSL Server
 - Utilisé pour protéger un ou plusieurs serveur(s) spécifique(s).



Le certificat, la clé privée et la chaîne de certificats du serveur doivent être installés dans le FortiGate

Depuis FortiOS 7, il est possible de définir plusieurs certificats dans un même profil pour protéger plusieurs serveurs.

HEH.be Sciences et technologies

Full SSL Inspection

- Protecting SSL Server (cont.)
 - Principe

Trafic en clair

Le FW agit comme un client auprès du serveur

Lorsque le client tente d'accéder au serveur, le FW se fait passer pour le serveur Web auprès du client

Import

• • • 123

HEH.be Sciences et technologies

Full SSL Inspection

- Profil de sécurité
 - SSL/SSH inspection est un profil de sécurité à assigner à une règle de pare-feu.

Protocol Options PRX default

Security Profiles

AntiVirus AV default

Web Filter

DNS Filter DNS default

Application Control APP default

IPS

SSL Inspection SSL deep-inspection

Choix du profil

• • • 124

Chapitre 3

Filtrage Web

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Choisir un mode de filtrage Web approprié.
 - Créer et appliquer des profils de filtrage Web et de filtrage DNS.
 - Créer des filtres URL statiques.

Web Filtering

- Intérêts du filtrage Web
 - Préserver les ressources
 - Éviter une mauvaise utilisation de la bande passante.
 - Préserver la productivité des employés.
 - Réduire l'exposition aux menaces Web.
 - Empêcher l'accès aux sites connus pour être infectés.
 - Empêcher la perte ou l'exposition d'informations confidentielles.
 - Empêcher la violation du droit d'auteur.
 - Protéger contre certains contenus
 - Empêcher (les enfants) de regarder des contenus inappropriés (Écoles).

Web Filtering

- Modes d'inspection
 - Depuis FortiOS 6.2, le mode d'inspection est personnalisable au niveau de la règle de pare-feu.

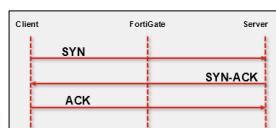
Policy & Objects > IPv4 Policy (Edit Policy)

Inspection Mode Flow-based Proxy-based

```
config firewall policy
edit <policy_id>
  set utm-inspection-mode [proxy | flow]
end
```

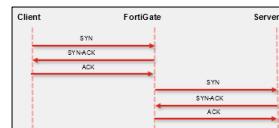
Flow-based inspection

- Mode d'inspection par défaut.
- Moins de latence (scan plus rapide).
- Consomme moins de ressources.
- Moins d'options de filtrage.
- NGFW mode disponible.



Proxy-based inspection

- Intercepte le trafic (proxy transparent, deux connexions TCP).
- Plus de latence.
- Consomme plus de ressources.
- Plus d'options de filtrage, meilleure sécurité.



Web Filtering

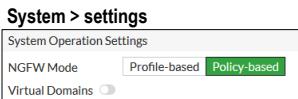
- Modes NGFW

- NGFW Profile-based

- Créer un profil de sécurité puis appliquer ce profil à une règle de pare-feu.
- Peut-être utilisé dans les modes d'inspection flow et proxy.

- NGFW Policy-based

- Uniquement disponible avec le mode d'inspection flow-based.
- Le contrôle d'application et le filtrage web peuvent être appliqués directement dans la règle de pare-feu. Il n'est pas nécessaire de configurer un profil de sécurité.
- SSL/SSH inspection doit être configuré.



129

Web Filtering

- Deux modes NGFW

- Profile-based Web Filter

- Configurer un profil de sécurité Web filter.
- Appliquer le profil à une règle de pare-feu

- Policy-based Web Filter

- Appliquer le filtrage par catégorie directement dans une règle de pare-feu
- Profil d'inspection SSL/SSH est requis

- Policy & Objects > Security Policy

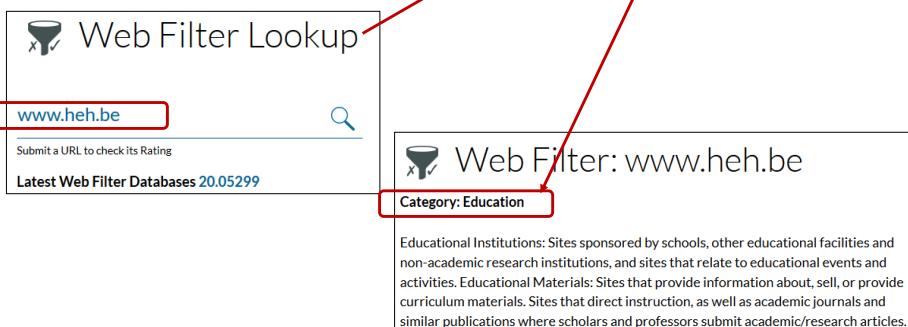
130

FortiGuard Category Filter

- Filtres de catégorie FortiGuard
 - Catégories
 - Permet de regrouper des URL afin d'éviter de devoir filtrer individuellement les sites Web.
 - L'action (pass ou block) est basée sur la catégorie et non sur l'URL elle-même.
 - Catégories FortiGuard
 - Nécessite un contrat actif.
 - Période de grâce de 7 jours.
 - Si le contrat expire, le FortiGate ne pourra pas évaluer les sites Web.
 - Contenus des catégories FortiGuard
 - Déterminés par des humains et par des robots d'exploration du Web.
 - Ils examinent différents aspects des sites Web et établissent une note.
 - Nécessite une licence

FortiGuard Category Filter

- Filtres de catégorie FortiGuard
 - Web Filter lookup
 - <https://fortiguard.com/webfilter>



The screenshot shows the FortiGuard Web Filter Lookup interface. On the left, there is a search bar with the URL "www.heh.be" and a magnifying glass icon. Below the search bar, it says "Submit a URL to check its Rating" and "Latest Web Filter Databases 20.05299". On the right, the results are displayed in a box with the heading "Web Filter: www.heh.be". Inside this box, the word "Category: Education" is highlighted with a red box and an arrow pointing from the left side of the slide. Below this, a detailed description of the "Education" category is provided:

Educational Institutions: Sites sponsored by schools, other educational facilities and non-academic research institutions, and sites that relate to educational events and activities. Educational Materials: Sites that provide information about, sell, or provide curriculum materials. Sites that direct instruction, as well as academic journals and similar publications where scholars and professors submit academic/research articles.

HEH.be
Sciences
et technologies

FortiGuard Category Filter

- Filtres de catégorie FortiGuard
 - Web Filter Categories
 - Permet de trouver des pages de test afin de vérifier le filtrage opéré par le fortigate

Bandwidth Consuming	
Category	Description
File Sharing and Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.

<https://fortiguard.com/wftest/24.html>

FortiGuard Web Filtering Test Page

This is a test page that will be rated by FortiGuard Web Filtering as:

File Sharing and Storage

Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.
Examples: instagram.com, imgur.com, flickr.com, dropbox.com

133

HEH.be
Sciences
et technologies

FortiGuard Category Filter

- Filtres de catégorie FortiGuard
 - FortiManager
 - Peut servir de serveur FortiGuard local.
 - Nécessite de télécharger les bases de données dans FortiManager.
 - Nécessite de configurer le FortiGate pour que les catégories soient validées via FortiManager et pas FortiGuard.

134

FortiGuard Category Filter

- Principe des filtres de catégorie FortiGuard

- Principe du filtrage Web

1. Le FortiGate interroge le réseau de distribution FortiGuard (ou un FortiManager), afin de déterminer la catégorie de la page Web demandée.
2. Le Fortigate effectue l'action configurée pour cette catégorie.

- Actions

- Les actions à effectuer peuvent être configurées par catégories et par sous-catégories.

Proxy-based :

Flow-based (Profile-based) :

Flow-based (Policy-based) : Action définie dans la règle de pare-feu (accept/deny)

FortiGuard Category Filter

- Principe des filtres de catégorie FortiGuard (suite)

- Action "Warning"

- Informe les utilisateurs que le site Web demandé n'est pas autorisé
 - L'utilisateur a la possibilité de tout de même se rendre sur le site ou de revenir sur le site précédent.
 - Disponible uniquement avec
 - Mode proxy
 - Mode flow avec "profile-based"
 - Intervalle d'avertissement
 - Permet de présenter la page d'avertissement uniquement pendant certaines périodes.
 - La page peut être personnalisée.



FortiGuard Category Filter

- Principe des filtres de catégorie FortiGuard (suite)
 - Action "Authenticate"
 - Bloque les sites Web demandés, sauf si l'utilisateur s'authentifie.
 - Intervalle de temps d'autorisation
 - Les utilisateurs ne doivent pas s'authentifier à nouveau s'ils accèdent à d'autres sites Web de la même catégorie.
 - Intervalle de temps personnalisable.

FortiGuard Category Filter

- Configuration de l'action "Authenticate"

The screenshot shows the configuration interface for a FortiGuard category-based filter. At the top, there are several action buttons: Allow (green), Monitor (blue eye), Block (red circle), Warning (yellow triangle), and Authenticate (blue user icon). The 'Authenticate' button is highlighted with a blue border. Below this, a table lists categories and their actions:

Name	Action
Local Categories (2)	
custom1	Allow
custom2	Allow

A yellow box highlights the 'custom2' row. A red arrow points from the text 'Choisir l'action "Authenticate"' to the 'Authenticate' button. Another red arrow points from the text 'Choix des groupes d'utilisateurs' to the 'Selected User Groups' field in the 'Edit Filter' dialog at the bottom. The 'Edit Filter' dialog shows a 'Warning Interval' of 0 hour(s), 5 minute(s), 0 second(s), and a 'Selected User Groups' field containing '+'. A red box highlights the 'Warning Interval' input.

Les utilisateurs ne doivent pas s'authentifier à nouveau s'ils accèdent à d'autres sites Web de la même catégorie dans cet intervalle de temps.

FortiGuard Category Filter

- Principe des Filtres de catégorie FortiGuard (suite)

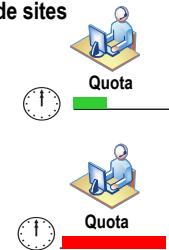
- Quotas de temps

- Permettent de limiter le temps passé sur certaines catégories de sites

- Uniquement disponible
 - » pour le filtrage web en mode proxy.
 - » avec les actions Monitor, Warning, et Authenticate

- Plusieurs quotas (minuteurs) peuvent être configurés

- Chaque quota peut être lié à une ou plusieurs catégories.
 - Les quotas peuvent être assignés
 - » Pour chaque IP source.
 - » Ou pour chaque utilisateur si l'authentification est activée.



User	Web Filter Profile	Used Quota
10.0.1.10	default	5 Minutes 34 Seconds

FortiGuard Category Filter

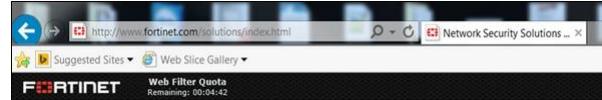
- Fortinet Bar

- No direct feedback

- La fonctionnalité Fortiguard Quota ne fournit aucune information aux utilisateurs.
 - Les utilisateurs ne sont donc pas informés en temps réel du quota de temps restant avant blocage du site.

- Applet Java

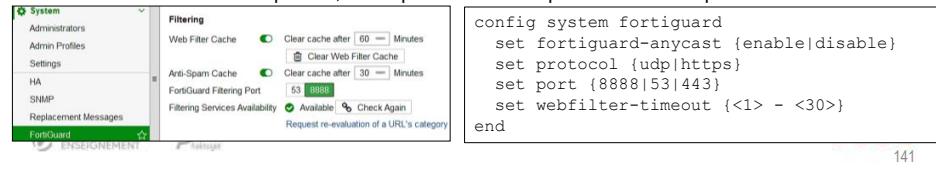
- La barre Fortinet injecte une applet Java
 - Cette applet communique avec le FortiGate, récupère des informations et les affiche.
 - Notamment, la Fortinet Bar affiche un compte à rebours pour les quotas FortiGuard.



HEH.be Sciences et technologies

FortiGuard Category Filter

- **Web Filter Cache**
 - Fonction cache
 - FortiGate peut conserver en mémoire les réponses aux évaluations de sites Web.
 - Si en cache, FortiGate ne renvoie pas de demande d'évaluation à FortiGuard.
 - Evaluation plus rapide.
 - TTL par défaut = 60 minutes.
 - Par défaut, FortiGate communique en HTTPS sur le port 443
 - Désactiver le paramètre « fortiguard-anycast » permet d'utiliser un autre port (HTTPS port 53 ou port 8888, UDP port 443, port 53, ou port 8888).
 - Attention au port 53, les requêtes seront bloquées en cas d'inspection.



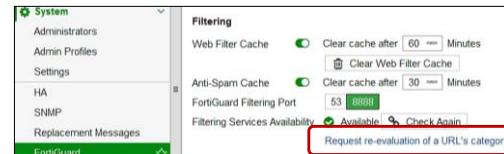
```
config system fortiguard
  set fortiguard-anycast {enable|disable}
  set protocol {udp|https}
  set port {8888|53|443}
  set webfilter-timeout {<1> - <30>}
end
```

141

HEH.be Sciences et technologies

FortiGuard Category Filter

- **FortiGuard Rating Submissions**
 - Classement correct des sites?
 - Il est possible que des erreurs soit présentent dans les classements (robots...)
 - Vous pouvez ne pas être d'accord avec la notation donnée par FortiGuard.
 - Modifier l'évaluation d'un site?
 - Vous pouvez contacter l'équipe de FortiGuard
 - Pour demander à modifier l'évaluation d'un site.
 - Pour faire évaluer un site qui ne figure pas déjà dans la base de données.



142

HEH.be Sciences et technologies

FortiGuard Category Filter

- Web Rating Override
 - Permet de modifier la catégorie d'un site sans passer par FortiGuard
 - Ne s'applique qu'aux noms d'hôte
 - Aucun caractère générique ou URL n'est autorisé.
 - Ne fonctionne plus si la licence FortiGuard expire

Il est possible d'ajouter ses propres catégories

URL	Override Category	Original Category	Status
fortinet.com	Business	undefined	Enabled
somewebsite.org	Phishing	undefined	Enabled

OK Pas OK
heh.be www.heh.be/index.html
www.heh.be www.heh.*

Edit Web Rating Overrides

URL: www.something.com

Override to:

Category: Bandwidth Consuming

Sub-Category: Peer-to-peer File Sharing

OK Cancel

143

HEH.be Sciences et technologies

FortiGuard Category Filter

- Web Profile Overrides
 - Changer le profil de filtrage Web
 - Permet d'adapter les règles d'inspection du trafic
 - Selon les utilisateurs, les groupes d'utilisateurs ou les adresses IP.
 - Uniquement disponible pour l'inspection en mode proxy.
 - Pour l'utiliser, une authentification est nécessaire
 - Une fois activée, la page de blocage de FortiGuard affiche un lien que les utilisateurs peuvent sélectionner pour activer le remplacement.

New Administrative Override

Scope Range: User

User: Student

Original Profile: default

New Profile: monitor-all

Expires: 0 Days, 0 Hours, 15 Minutes

(Expires: 4/27/2016, 10:16:00 AM)

OK Cancel

Security Profiles

AntVirus

Web Filter

default

block-security-risks

default

flow-monitor-all

monitor-all

web-filter-flow

Le nouveau profil est appliqué à l'utilisateur pendant un certain laps de temps

144

HEH.be Sciences et technologies

Inspection HTTPS

- **Filtrage HTTPS?**
 - Le filtrage Web s'applique uniquement au protocole HTTP
 - Le trafic HTTPS est encapsulé dans un tunnel SSL crypté.
 - Utilise le port 443.
 - Pour scanner le trafic HTTPS il faut utiliser l'inspection SSL/SSH
 - Un profil de sécurité SSL/SSH inspection doit donc être appliqué à la règle de pare-feu correspondante.

SSL Inspection Options

Enable SSL Inspection of **Multiple Clients Connecting to Multiple Servers**

Inspection Method **SSL Certificate Inspection** **Full SSL Inspection**

CA Certificate **Fortinet_CA_SSLProxy** **Download Certificate**

Server Certificate **Fortinet_SSL** **Download Certificate**

Untrusted SSL Certificates **Allow** **Block** **View Trusted CAs List**

RPC over HTTPS **Off**

Analysé réduit (éléments non chiffrés, SNI, Certificate CA)

Agit en proxy
Permet de scanner l'entièreté du contenu

• • • 145

HEH.be Sciences et technologies

Web filter configuration

- **Configuration du filtrage Web**
 - Supporte le mode proxy ou le mode flow

FortiGate VM64 FGVM010000051907 Interim admin

Dashboard FortiView Network System Policy & Objects Security Profiles AntiVirus Web Filter DNS Filter Application Control Cloud Access Security Inspection Intrusion Protection Data Leak Prevention FortiClient Profiles Proxy Options

Edit Web Filter Profile default

Name default

Comments Default web filtering. 22/255

Log all URLs FortiGuard category based filter

Allow users to override blocked categories

Search Engines Static URL Filter Rating Options Proxy Options

Apply

Proxy-based options

- Category-based
- Search engines
- Static URL
- Rating option
- Proxy option

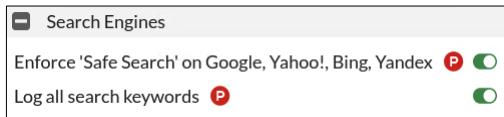
Flow-based options

- Category-based
- Static URL
- Rating Options

• • • 146

Web filter configuration

- Search Engines filtering (proxy-based only)
 - Safe search
 - Un code est ajouté à l'URL pour imposer l'utilisation de safe search
 - Par exemple, pour une recherche Google, la chaîne "&safe=active" est ajoutée à l'URL.
 - Fortigate prends en charge le safe search pour Google, Yahoo, Bing et Yandex.
 - Permet d'utiliser safe search même si la fonction n'est pas configurée dans le browser.
 - Deep SSL inspection est requis
 - Ne fonctionne pas avec « certificate inspection ».



URL filtering configuration

- Web Content Filter
 - Deep SSL inspection est requis
 - ↑ Filtrage sur base de phrases ou de mots contenus dans les pages Web.
- | Pattern Type | Pattern | Language | Action | Status |
|-----------------|------------------|----------|---|--------|
| Wildcard | something.* | Western | <input checked="" type="radio"/> Exempt | Enable |
| Reg. Expression | \"quelquechose\" | French | <input checked="" type="radio"/> Block | Enable |
- Les mots à rechercher sont associés à une valeur numérique.
- Si la somme des valeurs est supérieure à un seuil défini dans le profil du filtre Web, l'action est réalisée :
- Exempt
 - Block

URL filtering configuration

- Static URL Filter

URL	Type	Action	Status	Referrer
.(something org biz) somewhere.	Reg. Expression	<input checked="" type="radio"/> Exempt	Enable	
www.somesite.com/someURL	Simple	<input checked="" type="radio"/> Monitor	Enable	

Filtrage au niveau URL.

Si une correspondance est trouvée, l'action configurée est effectuée.

- Allow
- Exempt
- Block
- Monitor

URL filtering configuration

- Rating Options

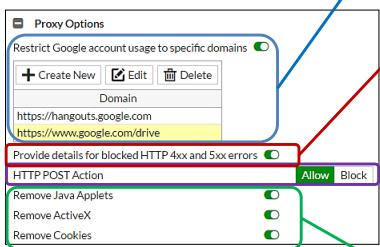
Si une erreur d'évaluation se produit, les utilisateurs auront un accès complet non filtré à tous les sites Web.

Compare les évaluations par URL et par adresse IP du site.

L'action de l'évaluation la plus élevée est appliquée.

URL filtering configuration

- Proxy options



Permet de bloquer l'accès à certains comptes et services Google.

Le Fortigate affiche ses propres pages d'erreurs de type 4xx et 5xx.

L'option Allow empêche un timeout du serveur lors du scan ou lorsque d'autres processus de filtrage sont exécutés pour le trafic sortant.

Permet de filtrer les scripts ActiveX, les applets Java ou les cookies.

Attention, les sites concernés pourraient ne plus fonctionner correctement.

Filtrage Vidéo

- Permet de contrôler l'accès au contenu YouTube (> FortiOS 7)

- Contrôle l'accès aux vidéos YouTube

- Pour autoriser, surveiller ou bloquer
 - en fonction de la catégorie,
 - Des chaînes YouTube spécifiques via leurs identifiants (Channel ID).

- Disponible depuis FortiOS 7

- Nécessite d'activer l'inspection SSL/SSH complète.
 - Nécessite une licence FortiGuard spécifique.
 - Nécessite le mode d'inspection proxy.
 - Nécessite une clé API YouTube (plusieurs API possibles).
 - L'API permet de faire correspondre les paramètres identifiés lorsque les utilisateurs accèdent au contenu YouTube aux catégories du FortiGate.

HEH.be Sciences et technologies

Filtrage Vidéo

- Filtrage vidéo par catégorie
 - Catégories de filtrage vidéo FortiGuard
 - Une catégorie FortiGuard combine plusieurs catégories des fournisseurs de contenus vidéo en une seule catégorie.
 - Par exemple, la catégorie vidéo FortiGuard « Entertainment » comprend diverses catégories YouTube telles que divertissement, comédie ou encore film.
 - Les catégories s'appliquent aux contenus hébergés par YouTube, Vimeo et Dailymotion.

Empêche la vidéo et génère un log

11 catégories locales au FortiGate

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

• • • 153

HEH.be Sciences et technologies

Filtrage Vidéo

- Filtrage vidéo par niveau et par chaîne

Les utilisateurs ne reçoivent que le contenu qui est filtré selon le filtre « Moderate » ou « Strict » appliqué par Google.

Autoriser, surveiller ou bloquer l'accès à une chaîne YouTube selon son ID.

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

• • • 154

HEH.be
Sciences
et technologies

Web filter configuration

- Log
 - Log & Report > Security Events

Date/Time	User	Source	Action	URL	Category
20 minutes ago	10.0.1.10		passthrough	https://www.bing.com/	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	https://www.bing.com/	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	http://www.bing.com/rp/hqv4EMgsH4xwi6kpApki-DF...	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	http://www.bing.com/rp/hqx6FcD0hjfrON5oLgx2RM...	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	http://www.bing.com/rp/mlKxxkf6UTEZv7k-d_D59PC...	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	http://www.bing.com/rp/08hWncb4hLQzpDIAvQdqLl...	Malicious Websites
20 minutes ago	10.0.1.10		passthrough	http://www.bing.com/rp/bLUVERLX4vU6bjspboNMw...	Malicious Websites

• • • 155

HEH.be
Sciences
et technologies

DNS Filtering

- DNS-Based Web Filtering
 - Filtrage des requêtes DNS
 - Avant une requête HTTP GET, les machines clientes utilisent des requêtes DNS pour connaître l'IP du serveur à joindre.
 - Cette option filtre la requête DNS plutôt que la requête HTTP GET.
 - Caractéristiques
 - Impacte tous les protocoles qui dépendent du DNS, pas seulement le trafic HTTP.
 - Ne permet pas de filtrer aussi précisément que le filtrage HTTP.
 - Prend en charge le filtrage d'URL et les catégories FortiGuard uniquement.
 - Possible de filtrer les requêtes DNS chiffrées (> FortiOS 7)
 - DNS over TLS (DoT).
 - DNS over HTTPS (DoH).
 - Le filtrage DNS s'effectue sur les réponses.

• • • 156

DNS Filtering

- Principe du filtrage DNS

- Etapes du filtrage DNS

1. Lorsqu'il reçoit une requête DNS d'un client, FortiGate génère une requête DNS vers le service SDNS FortiGuard.
2. FortiGuard renvoient une adresse IP et une évaluation qui inclut la catégorie FortiGuard de la page Web demandée.
3. Le Fortigate effectue l'action configurée pour cette catégorie.

- Actions

- Les actions à effectuer peuvent être configurées par catégories et sous-catégories.

- DNS-based actions :



DNS Filter Configuration

- DNS Filter Profile

- Uniquement disponible en mode proxy-based inspection

Activer/désactiver le filtrage par catégorie

Bloque les requêtes DNS vers les serveurs de commande et contrôle des botnets connus.
Nécessite une licence FortiGuard Web Filtering

Edit DNS Filter Profile

Name	default
Comments	Default dnsfiltering.
Block DNS requests to known botnet C&C	<input checked="" type="checkbox"/>
Enforce 'Safe search' on Google, Bing, YouTube	<input type="checkbox"/>

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter**

FortiGuard category based filter

Show: All

- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming**
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

Static Domain Filter

Domain Filter:

DNS Filter Configuration

• DNS Filter Profile (suite)

Autorise les requêtes DNS s'il n'est pas possible d'obtenir une évaluation (FortiGuard non accessible). Sans cela, toutes les requêtes seront bloquées.

The screenshot shows the 'Options' tab of the DNS Filter profile configuration. It includes settings for allowing DNS requests when a rating error occurs (disabled), logging all DNS queries and responses (disabled), redirecting blocked DNS requests (enabled), and redirecting portal IP (set to 'Use FortiGuard Default' with IP 208.91.112.55). A blue arrow points from the 'Redirect blocked DNS requests' section to a callout box titled 'Web Page Blocked!' containing the message: 'You have tried to access a web page which belongs to a category that is blocked.' The bottom right corner shows a navigation bar with three dots and the number 159.

DNS Filter Configuration

• DNS Filter Profile (suite) Filtrage selon le nom du domaine.

The screenshot shows the 'Static Domain Filter' table. It lists three entries: 'Domain' (http://something.com/), 'Type' (Simple), 'Action' (Block), and 'Status' (Enable). Below this, there is a detailed view of a row with columns for 'Domain' ('.\somesites\$'), 'Type' (Reg. Expression), 'Action' (Monitor), and 'Status' (Enable). A red arrow points from the 'Domain' column of the main table to this detailed view. Another red arrow points from the 'Action' column of the detailed view to a callout box explaining the actions: 'Allow', 'Monitor', and 'Redirect to Block Portal'. A purple arrow points from the 'Action' column of the detailed view to another callout box stating: 'Affiche une page de blocage'. The bottom right corner shows a navigation bar with three dots and the number 160.

Motif simple : correspondances exactes.
 Regex : autorise l'utilisation des expressions régulières.
 Wildcard : autorise l'utilisation de caractères génériques et de correspondances partielles

DNS Filtering

- Principe du filtrage DNS

- Etapes du filtrage DNS

1. Lorsqu'il reçoit une requête DNS d'un client, FortiGate génère une requête DNS vers le service SDNS FortiGuard.
2. FortiGuard renvoient une adresse IP et une évaluation qui inclut la catégorie FortiGuard de la page Web demandée.
3. Le Fortigate effectue l'action configurée pour cette catégorie.

- Actions

- Les actions à effectuer peuvent être configurées par catégories et sous-catégories.
 - Allow
 - Monitor
 - Redirect to Block Portal.

DNS Filter Configuration



- DNS Filter Profile

- Uniquement disponible en mode proxy-based inspection

Activer/désactiver le filtrage par catégorie

Bloque les requêtes DNS vers les serveurs de commande et contrôle des botnets connus.
Nécessite une licence IPS et Web Filtering

DNS Filter Configuration

• DNS Filter Profile (suite)

Activer/désactiver le filtrage statique

Permet de traduire une adresse IP résolue par DNS en une autre adresse IP de votre choix..

WALLONIE-BRUXELLES
ENSEIGNEMENT

Pro
Prise

163

DNS Filter Configuration

• DNS Filter Profile (suite) Filtrage selon le nom du domaine.

Motif simple : correspondances exactes.
Regex : autorise l'utilisation des expressions régulières.
Wildcard : autorise l'utilisation de caractères génériques et de correspondances partielles

Si une correspondance est trouvée, l'action configurée est effectuée.

- Allow
- Monitor
- Block

Affiche une page de blocage

WALLONIE-BRUXELLES
ENSEIGNEMENT

Pro
Prise

164

DNS Filter Configuration

• DNS Filter Profile (suite)

Autorise les requêtes DNS s'il n'est pas possible d'obtenir une évaluation (FortiGuard non accessible). Sans cela, toutes les requêtes seront bloquées.

The screenshot shows the 'Options' section of the DNS Filter Configuration. It includes the following settings:

- Allow DNS requests when a rating error occurs:** A checkbox is checked.
- Log all DNS queries and responses:** A checkbox is checked.
- Redirect blocked DNS requests:** A checkbox is checked.
- Redirect Portal IP:** A dropdown menu offers two choices: "Use FortiGuard Default" (selected) and "Specify", with the IP address "208.91.112.55" listed.

An annotation points to the "Use FortiGuard Default" option with the text: "Rediriger les requêtes bloquées vers un portail "Use FortiGuard Default" est recommandé."

To the right, a message box displays: "Web Page Blocked! You have tried to access a web page which belongs to a category that is blocked."

Logos for Wallonie-Bruxelles Enseignement and Pôle Formation are at the bottom left, and a navigation bar with three dots and the number 165 is at the bottom right.

Ordre du filtrage

• Ordre d'inspection

1. Filtrage statique d'URL.
2. Filtrage par catégorie.
3. Filtrages avancés (safe search, Active X, ...)

• Vérifier la connexion avec les serveurs FortiGuard

```
FortiGate-VM64 # diagnose debug rating
Locale      : english
Service     : Web-filter
Status      : Enable
License     : Contract

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

--- Server List (Wed Apr 21 13:59:43 2021) ---
IP          Weight RTT Flags TZ FortiGuard-requests Curr Lost Total Lost Updated Time
173.243.140.16    -72 101 DI      0                      36      0      0      Wed Apr 21
                                                               13:58:13 2021
```

Annotations highlight the 'Status : Enable' line in the configuration and the 'Updated Time' column in the server list table.

Page number 166 is at the bottom right.

Chapitre 4

Contrôle d'application

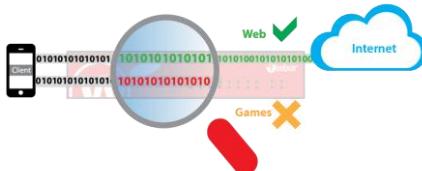
Application control

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Configurer et appliquer les profils de contrôle applicatif.
 - Configurer le traffic shaping.
 - Analyser les journaux relatifs aux événements du contrôle d'application.

Contrôle d'application

- Capable de détecter et agir sur le trafic applicatif
 - Déetecter
 - Par exemple les jeux ou les applications utilisant beaucoup de bande passante.
 - Prend en charge de nombreuses applications et catégories.
 - Si une application n'est pas prise en charge, il est possible de demander à FortiGuard de la prendre en charge.
 - Le scan de protocoles sécurisés est possible via le profil d'inspection SSL/SSH.
 - Agir
 - Monitorer, laisser passer, bloquer ou appliquer du contrôle de flux (trafic shaping)



Contrôle d'application

- Avantages du contrôle d'application
 - Apporter une meilleure visibilité et un contrôle fin des applications.
 - Quel que soit le port ou le protocole utilisé.
 - Réduire les risques liés au Bring-Your-Own-Device (BYOD).
 - Ne maîtrisant pas les applications installées sur les équipements BYOD, les administrateurs doivent pouvoir réaliser un contrôle d'application afin de réguler ce qu'un utilisateur peut faire sur le réseau.
 - Limiter l'exposition notamment créée par les applications de médias sociaux
 - Certaines fonctionnalités peuvent être intéressante pour l'entreprise, tout bloquer pourrait causer une perte de productivité.
 - Réduire les surfaces d'attaque
 - En bloquant certaines applications ou fonctionnalités des applications, certaines attaques sont rendues impossibles.
 - Récupérer la bande passante
 - En contrôlant la BP allouées aux applications de streaming ou encore de partage (P2P).
 - En garantissant une bande passante suffisante pour les applications stratégiques.

Contrôle d'application

- Principe du contrôle d'application FortiGate
 - Utilise le moteur IPS pour analyser le trafic
 - Peut être utilisé dans des règles de pare-feu en mode flow-based ou proxy-based.
 - Cependant, le scan est toujours de type flow-based.
 - Comme il utilise le moteur IPS, il devrait consommer plus ou moins la même chose que la fonction IPS.
 - Pas de risque de tomber à court de connexions proxy.
 - Le moteur IPS recherche des motifs (pattern) connus dans tout le flux d'octets
 - Permet de détecter les applications même si elles utilisent des protocoles et des ports non standards.
 - Permet d'identifier les applications même si l'utilisateur passe par un proxy externe.
 - Il faut que l'application utilise des motifs (pattern) spécifiques (reconnaissables).

Contrôle d'application

- Mise à jour des signatures
 - La mise à jour des signatures est importante
 - Lorsque le comportement des applications sont modifiées notamment lorsque les développeurs y ajoutent des fonctionnalités.
 - Lorsque de nouveaux protocoles / applications sont utilisés.
 - La mise à jour nécessite un abonnement Fortiguard

System > FortiGuard

<input checked="" type="checkbox"/> Firmware & General Updates	<input checked="" type="checkbox"/> Licensed (Expiration Date: 2023/01/18)	<input type="button" value="Actions ▾"/>
Application Control Signatures	<input checked="" type="radio"/> Version 16.00943	<input type="button" value="Upgrade Database"/>
Device & OS Identification	<input type="radio"/> Version 1.00111	<input type="button" value="View List"/>
Internet Service Database Definitions	<input type="radio"/> Version 7.01069	

Contrôle d'application

- Recherche d'une application

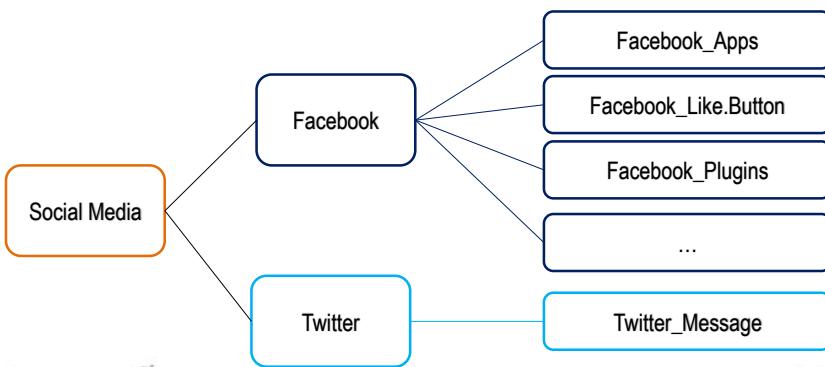
- Sur <https://fortiguard.com>, Fortinet garde une encyclopédie des applications supportées.

The screenshot shows a web browser displaying the FortiGuard Labs website at <https://www.fortiguard.com>. A red arrow points from the search bar to the search results. The search term 'bitTorrent' is entered in the search bar. The results show a single entry for 'BitTorrent' under the 'Application' category. A detailed description of BitTorrent as a popular P2P file-sharing protocol is provided. The page includes navigation links like 'Outbreak Alerts', 'Learn', and 'Services'.

Contrôle d'application

- Signatures (suite)

- Les signatures sont organisées de manière hiérarchique
 - Les signatures parentes prevalent sur les signatures enfants.



HEH.be Sciences et technologies

Contrôle d'application

- Signatures
 - Afficher les signatures du contrôle d'applications

Security Profiles

- AntiVirus
- Web Filter
- DNS Filter
- Application Control

Edit Application Sensor

Name: default
Comments: Monitor all applications. 25/255

[View Application Signatures]

Catégories

- All Categories
- Business (185)
- Cloud.IT (31)
- Collaboration (299)
- Email (99)
- Game (124)
- General.Interest (250)

Les applications sont regroupées en catégories

• • • 175

HEH.be Sciences et technologies

Contrôle d'application

Classement par nom, catégorie, technologie, popularité ou risque

- Signatures (suite)

Name	Category	Technology	Popularity	Risk
1luxun	Video/Audio	Client-Server	★★★★★	Low
lund1.Mail	Email	Browser-Based	★★★★☆	Medium
2ch	Social.Media	Browser-Based	★★★★★	Medium
2ch.Post	Social.Media	Browser-Based	★★★★★	Medium
2Safe	Storage.Backup	Browser-Based	★★☆☆☆	Medium
2Safe_File.Download	Storage.Backup	Browser-Based	★★☆☆☆	Medium
2Safe_File.Upload	Storage.Backup	Browser-Based	★★☆☆☆	Medium

2Safe

Severity: medium Reference: 36322

This indicates an attempt to access 2Safe.

Cloud service 2Safe gives everyone an opportunity to save their data to the Internet and provide access to them from a variety of devices and platforms

Affected Products: 2Safe

Impact: Network bandwidth consumption

Recommended Actions: If required, this signature's action can be set to "Block" to block this application.

Contrôle précis des applications

Pour chaque signature, FortiGuard évalue le niveau de risque. Le niveau calculé est propre à Fortinet et n'est pas lié au CVSS (Common Vulnerability Scoring System)

• • • 176

- Common Vulnerability Scoring System

- Quels risques sont liés à une vulnérabilité?

- De nombreux éditeurs de solutions de sécurité utilisent leurs propres méthodes propriétaires pour attribuer des notes à l'impact des vulnérabilités.
 - Il n'est pas facile pour une entreprise d'évaluer l'importance des vulnérabilités afin de les prioriser et remédier à celles qui posent les plus grands risques.

- Système de notation des vulnérabilités

- CVSS permet de classer les vulnérabilités et fournir un score représentant la gravité globale et le risque que présente une vulnérabilité.
 - CVSS est une initiative publique conçue pour aider les analystes à noter les vulnérabilités et pour aider les organisations à utiliser les scores.

- FIRST

- Le CVSS est actuellement géré par le Forum of Incident Response and Security Teams (FIRST).

- Niveau de risque

Niveau de risque	Icone	Description	Exemples
Critical		Applications utilisées pour dissimuler des activités, utilisant des techniques d'évasion.	Tor, Spyboss.
High		Applications pouvant causer des fuites d'informations ou susceptibles d'introduire des malwares.	P2P, torrent, remote desktop
Medium		Applications qui peuvent être mal utilisées.	Gmail, VoIP, ...
Elevated		Applications pouvant mener à une perte de productivité.	Facebook, Youtube, jeux
Low		Applications métier ou inoffensives.	Mises à jour OS

- Profils du contrôle d'application
 - NGFW profile-based
 - Pour utiliser les profils, l'option NGFW doit être réglée sur le mode «profile-based».
 - Rappel : Le scan des paquets est toujours flow-based.
 - Les applications sont filtrées sur base de 3 filtres :
 1. Application overrides
 2. Filter overrides
 3. Categories
 - Une fois configuré, le profil doit être appliqué à une règle de pare-feu

- Profils du contrôle d'application (suite)
 - Categories
 - Une catégorie est un regroupement d'applications
 - Par exemple, toutes les applications P2P ou toutes les applications de médias sociaux.

Security Profiles > Application Control

The screenshot shows the 'Edit Application Sensor' interface under the 'Categories' tab. A green box highlights the 'Monitor' category, which includes options: Allow, Block, Quarantine, and View Signatures (185). A red box highlights the 'Unknown Applications' category. A callout points to the 'Monitor' category with the text: 'Affiche les actions à appliquer pour cette catégorie'. Another callout points to the 'Unknown Applications' category with the text: 'Le nuage indique le nombre d'applications Cloud de cette catégorie'.

Correspond au trafic qui n'a pu être associé à aucune signature de contrôle d'application

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)

- Application overrides

- Offre de la flexibilité en permettant de configurer des actions pour des signatures d'applications spécifiques (individuelles).

- Filter overrides

- Permet de définir ses propres catégories de filtrage dans le cas où celles proposées ne conviennent pas.

Application and Filter Overrides

Priority	Details	Type	Action
1	Battle.Net Dailymotion	Application	<input checked="" type="radio"/> Allow
2	Excessive-Bandwidth	Filter	<input type="radio"/> Block

No results

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	<input type="radio"/> Block
2	Battle.Net Dailymotion	Application	<input checked="" type="radio"/> Allow

Attention à l'ordre

WALLONIE-BRUXELLES
ENSEIGNEMENT

DU
Présage

• • • 181

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)

- Ordre du filtrage d'application

1. Le moteur IPS identifie l'application.
2. Application overrides (si configuré) et Filter overrides (si configuré).
 - ATTENTION : l'ordre (*application* en premier ou *filter* en premier) dépend de la configuration réalisée.
3. Categories.

- Actions

- **Allow** : le trafic est accepté et ne génère pas de log.
- **Monitor** : le trafic peut passer et il y a génération d'un log (utile pour découvrir le trafic d'un réseau).
- **Block** : abandonne le trafic et journalise. Un message de blocage est envoyé s'il s'agit d'une application HTTP.
- **Quarantine** : bloque le trafic de l'IP source jusqu'à l'expiration du temps de quarantaine et journalise.

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)
 - Deep inspection (SSL/SSH) est requis pour scanner le trafic chiffré avec SSL

106 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: default
Comments: Monitor all applications. 25/255

Categories: All Categories

Network Protocol Enforcement

183

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)
 - Protocol enforcement
 - Permet d'empêcher l'utilisation de protocoles connus sur d'autres ports que ceux normalement prévus.

Security Profiles > Application Control

+ Create New Edit Delete Search

Port	Enforce Protocols
Port 80	PROT HTTP
Port 53	PROT DNS

New Default Network Service

Port: 80
Enforce protocols: PROT HTTP
Violation action: Monitor Block

Select Entries

PROT DNS
PROT FTP
PROT HTTP
PROT HTTPS
PROT IMAP
PROT NNTP
PROT POP3
PROT SMTP
PROT SNMP
PROT SSH
PROT TELNET

OK Cancel

184

HEH.be Sciences et technologies

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)
 - Options

Bloquer les applications n'utilisant pas le port par défaut (HTTP 80, SSL 443, ...)

Attention à la consommation de ressources si trop de logs

Options

Block applications detected on non-default ports

Allow and Log DNS Traffic

QUIC Allow Block

Replacement Messages for HTTP-based Applications

Active l'envoie d'une page HTTP expliquant la raison d'un blocage.

Protocol de transport basé sur UDP, disposant d'un chiffrement équivalent à TLS, mais plus rapide.
Utilisé par Chrome et les serveurs Google.
QUIC n'est pas scanné par le pare-feu.

Allow QUIC
Recherche d'en-tête QUIC et journalise en tant que message QUIC.

Block QUIC
Force Google Chrome à utiliser TLS et journalise QUIC comme étant bloqué.

185

HEH.be Sciences et technologies

Configuration du contrôle d'application

- Profils du contrôle d'application (suite)
 - Appliquer le profil à une règle de pare-feu

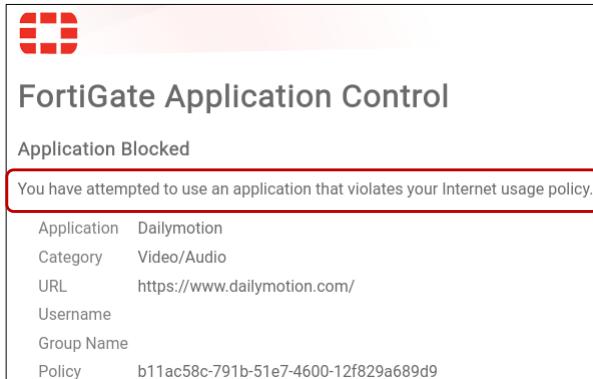
Policy & Objects > Firewall Policy →

Name: WAN-IBE	Incoming Interface: WAN_Uplink (port36)
Outgoing Interface: P22	Source: all
Destination: FortiMail IBE	Schedule: always
Service: ALL	Action: ACCEPT
Inspection Mode: Flow-based	
Firewall / Network Options	
NAT: OFF	
Protocol Options: PROT default	
Security Profiles	
AntVirus: OFF	
Web Filter: OFF	
DNS Filter: OFF	
Application Control: APP default	
IPS: OFF	
File Filter: OFF	
SSL Inspection: deep-inspection	

Ne pas oublier de choisir le profil « deep inspection », sans quoi le trafic chiffré avec SSL ne sera pas inspecté

186

- **Page de blocage**
 - Permet d'afficher les raisons du blocage à l'utilisateur



- **NGFW Policy-based mode**
 - **Flow-based inspection + NGFW Policy-based mode**
 - Le contrôle d'application se configure directement au niveau de la règle de pare-feu (pas de profil d'inspection possible).
 - Uniquement possible en mode « flow-based ».
 - **SSL/SSH inspection**
 - Toutes les règles du pare-feu en mode NGFW Policy-based doivent utiliser le même profil d'inspection SSL/SSH.
 - **Central SNAT**
 - Le mode NGFW Policy-based nécessite l'utilisation du Central SNAT.

Configuration du contrôle d'application

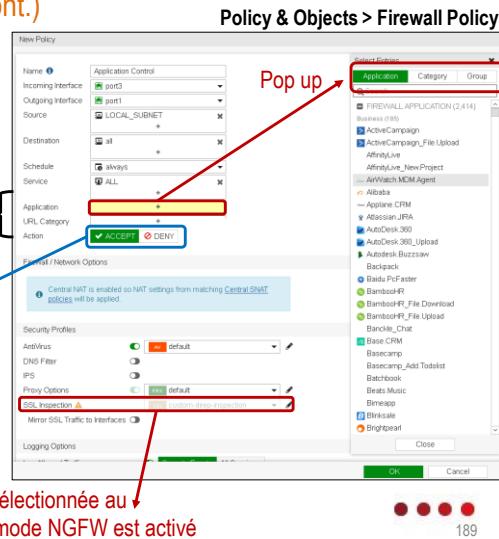
- NGFW Policy-based mode (Cont.)
 - Configuration

Le contrôle d'application et le filtrage Web peuvent être configurés au niveau de la règle de FW

Si URL category, seules les applications de la catégorie browser-based technology peuvent être utilisées par le contrôle d'applications

Les seules actions possibles sont celles de la règle de FW

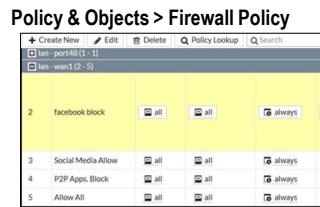
On peut uniquement ajouter ces profils de sécurité :



Configuration du contrôle d'application

- NGFW Policy-based mode (Cont.)
 - Exemple

Ces applications de médias sociaux sont bloquées par la règle N°1



10.30 MB

7.79 MB

0 B

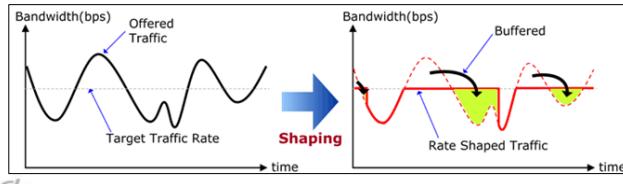
124.76 GB

Trafic journalisé ou non

Les autres applications de médias sociaux sont autorisées par la règle N°2

Application Control Traffic Shaping

- Régulation du trafic (Traffic shaping)
 - Régulation de la bande passante utilisée par les applications
 - Permet de définir une bande passante maximale utilisable par les applications
 - Uniquement le trafic qui correspond à une signature d'application.
 - N'interfère pas avec d'autres applications qui utilisent le même port/protocole.
 - File d'attente
 - Les paquets excédentaires sont maintenus dans une file d'attente.
 - Cette régulation nécessite de la mémoire pour stocker tous les paquets retardés.
 - Les paquets retardés sont transmis graduellement dans le temps
 - Uniquement lorsque de la BP pour l'application concernée est à nouveau disponible.



Configuration du contrôle d'application

- Configuration de la régulation du trafic
 - Policy & Objects > Traffic Shaping Policy

Il est nécessaire qu'une règle du pare-feu autorise le trafic à réguler.

La règle de pare-feu ne doit pas nécessairement correspondre exactement à la règle de régulation de flux (all ↔ 10.10.0.x/24).

- Le traffic shaping peut s'appliquer à
- une catégorie d'applications,
 - une application spécifique,
 - un groupe personnalisé d'applications (> FortiOS 6.2)

Configuration du contrôle d'application

- Types de traffic shaping

- Shared shaper

- Fixe une limite à la bande passante en upload, tous les utilisateurs se partagent cette bande passante.

- Reverse shaper

- Idem shared shaper mais pour le téléchargement/streaming.

- Per-IP Shaper

- Applique la mise en forme du trafic à toutes les adresses IP source listée dans la politique de sécurité. Chaque IP se verra allouer la même bande passante maximale.

The screenshot shows two configuration panels side-by-side:

- Left Panel (Action Rule):**
 - Action: Apply Shaper | Assign Shaping Class ID
 - Outgoing interface: port2 (highlighted with a red box)
 - Shared shaper: shared-1M-pipe
 - Reverse shaper: medium-priority
 - Per-IP shaper: limited-10-sessions
- Right Panel (Traffic Shaping Class ID):**
 - Action: Apply Shaper | Assign Shaping Class ID
 - Outgoing interface: + (highlighted with a red box)
 - Traffic shaping class ID: This field is required. (highlighted with a red box)
 - Search: Search + Create (highlighted with a red box)
 - No entries

Bottom right corner: 193

Configuration du contrôle d'application

- Classes de trafic

- Depuis FortiOS 6.2.2, vous pouvez configurer des classes de trafic avec un nom

The screenshot shows three windows illustrating the creation and selection of a traffic shaping class:

- Left Window (New Traffic Shaping Class ID):**
 - ID: 2
 - Name: High priority voice
 - Buttons: OK, Cancel
- Middle Window (Select Traffic Shaping Class ID):**
 - Default: (radio button selected)
 - Traffic shaping class ID: High priority voice (2) (highlighted with a red box)
 - Buttons: OK, Cancel
- Right Window (Action Rule):**
 - Action: Apply Shaper | Assign Shaping Class ID
 - Outgoing interface: + (highlighted with a red box)
 - Traffic shaping class ID: This field is required. (highlighted with a red box)
 - Search: Search + Create (highlighted with a red box)
 - No entries

Bottom right corner: 194

Journalisation

- Journalisation du contrôle d'application
 - Afficher les journaux
 - Log & Report > Application Control.
 - La journalisation doit être activée dans la règle de pare-feu.
 - Exemple d'un client essayant d'accéder à BitTorrent

Log & Report > Security Events

Summary Details

Top Category	Action	Count
WebClient	Pass	601
NetworkService	Pass	279
Video/Audio	Pass	71
Video/Audio	Block	3

A [Application Control] →

Clic pour afficher les détails (voir diapo. suivante)

#	Date/Time	Source	Destination	Application	Action
37	12:15:53	10.0.1.10	4.2.2.2	DNS	pass
38	12:15:52	10.0.1.10	4.2.2.2	DNS	pass
39	12:15:52	10.0.1.10	172.217.3.78	YouTube	pass
40	12:15:52	10.0.1.10	172.217.3.67	Google.Accounts	pass
41	12:15:51	10.0.1.10	172.217.3.78	YouTube	pass
42	12:15:51	10.0.1.10	172.217.3.78	YouTube	pass
43	12:15:46	10.0.1.10	172.217.3.78	HTTPS.BROWSER_Firefox	pass
44	12:15:46	10.0.1.10	69.28.188.36	BitTorrent	pass
45	12:15:46	10.0.1.10	98.143.146.7	HTTPS.BROWSER_Firefox	pass
46	12:15:21	10.0.1.10	69.28.188.36	BitTorrent	pass
47	12:15:20	10.0.1.10	69.28.188.36	BitTorrent	pass
48	12:14:27	10.0.1.10	205.178.187.13	HTTPS.BROWSER	pass
49	12:13:44	10.0.1.10	69.171.239.11	DNS	pass

195

HEH.be Sciences et technologies

Journalisation

- Journalisation du contrôle d'application
 - Exemple de détail d'un log

Horodatage

Adresses Port Interface URL

Catégorie N° de la règle

196

Journalisation

- **Dashboard**

- Les événements du contrôle d'applications sont visibles dans le widget « Top Applications » du dashboard
 - Nécessite un disque dur.
 - Les modèles sans disque dur peuvent utiliser FortiView via la journalisation avec FortiCloud.

Dashboard > Top Applications

Application	Category	Risk	Bytes	Sessions	Bandwidth
SSL	Network.Service	Low	12.29 MB	33	1.11 Mbps
YouTube_HD_Streaming	Video.Audio	Medium	3.94 MB	1	2.47 kbps
YouTube_Video.Access	Video.Audio	Medium	2.32 MB	1	13.48 kbps
HTTPBROWSER_Firefox	Web.Client	Medium	2.15 MB	7	3.64 kbps
Vimeo_Video.Play	Video.Audio	Medium	1.95 MB	2	872.04 kbps
YouTube_Video.Play	Video.Audio	Medium	1.07 MB	3	1.92 Mbps
Vimeo	Video.Audio	Medium	173.30 kB	5	46.79 kbps
LinkedIn	Social.Media	Medium	75.13 kB	6	37.69 kbps
Dailymotion	Video.Audio	Medium	70.19 kB	1	13.13 kbps
GoogleServices	General.Interest	Medium	33.66 kB	2	3.67 kbps
Vimeo_Video.Access	Video.Audio	Medium	19.31 kB	1	1.18 kbps
OCSP	Network.Service	Medium	7.30 kB	4	1.66 kbps
NTP	Network.Service	Medium	152 B	1	16 bps

197

Quand utiliser le contrôle applicatif?

- **Conseils**

- **Evitez de consommer des ressources inutilement**
 - Appliquez le contrôle d'application uniquement au trafic qui le nécessite
 - Ne pas appliquer le contrôle d'applications au trafic interne-interne si vous connaissez exactement les applications installées sur les serveurs et les clients du réseau.
- **Balancez de charge**
 - Appliquez les mêmes inspections sur tous les périphériques redondants.
- **Inspection SSL/SSH**
 - Choisissez « Deep SSL/SSH inspection » plutôt que la simple vérification des certificats.
- **Loguez**
 - Pour voir les logs depuis un FortiGate qui n'a pas de disque interne, utilisez FortiCloud.
- **Si elle est disponible, utilisez l'accélération matérielle**

Chapitre 5

Dialup VPN - ADVPN

Auto Discovery Virtual Private Network

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Schématiser les différentes topologies VPN
 - Expliquer les avantages et inconvénients des différentes topologies VPN.
 - Choisir une topologie VPN appropriée en fonction de contraintes.
 - Déployer un VPN dialup entre deux FortiGates.
 - Déployer un VPN dialup entre un FortiGate et un FortiClient.
 - Configurer des VPN redondants entre deux FortiGates.
 - Dépanner des problèmes de base liés aux VPN.

- Rappel IPsec

- Suite de protocoles utilisés pour sécuriser des communications IP

- Objectifs : authentification, chiffrement, intégrité, anti-rejet

- Internet Key Exchange (IKE, UDP port 500).
- Échanges Diffie-Hellman (DH group).
- Encapsulation Security Payload (ESP).
- keyed-hash message authentication code

- NAT Traversal

- Permet d'utiliser des VPN en présence de NAT et PAT.
- ESP est encapsulé dans UDP port 4500.

- VPN

- Route-based (tunnel L2TP, tunnel GRE, routage).
- Policy-based (FortiGate en mode transparent).

- Types de pairs distants

- Static IP Address

- Utilisé lorsque l'adresse IP du pair distant est connue et ne changera pas.
- Le FortiGate peut être l'initiateur du tunnel VPN ou le répondeur.

- Dynamic DNS

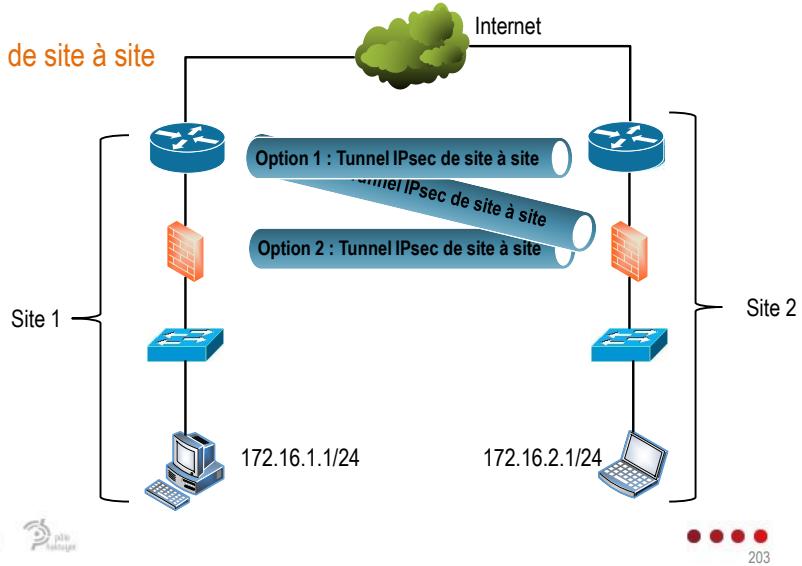
- Le pair distant a une IP dynamique, mais son domaine DNS est statique.
- Un DNS dynamique est utilisé pour résoudre l'IP la rendant ainsi prévisible.
- Le FortiGate peut être l'initiateur du tunnel VPN ou le répondeur.

- Dialup

- Utilisé lorsque l'adresse IP du pair est dynamique et qu'il n'est pas possible de la retrouver.
- Le FortiGate peut uniquement être répondeur
 - Il ne peut pas initier la communication car il ne saurait pas vers quelle IP diriger sa requête.

Topologies VPN

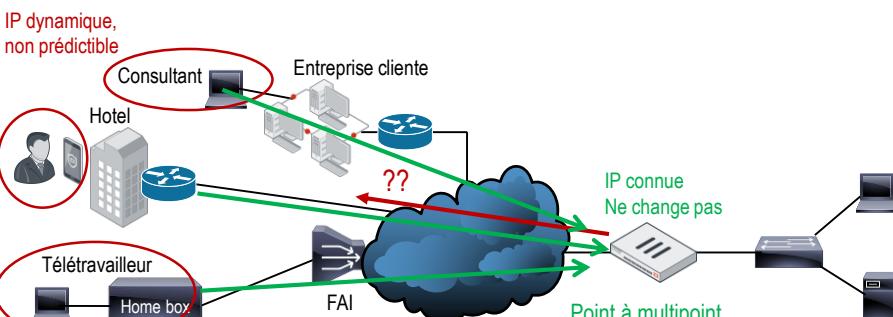
1. VPN de site à site



Topologies VPN

2. Dialup VPN

- Utilisé lorsque l'on ne sait pas avec quelle IP le pair distant se connectera
 - C'est notamment le cas des travailleurs mobiles (télétravailleurs, en déplacement, ...)
 - Point-à-multipoint : une configuration dialup VPN peut être utilisée pour plusieurs tunnels IPsec d'utilisateurs distants.



Topologies VPN

3. Hub and spoke

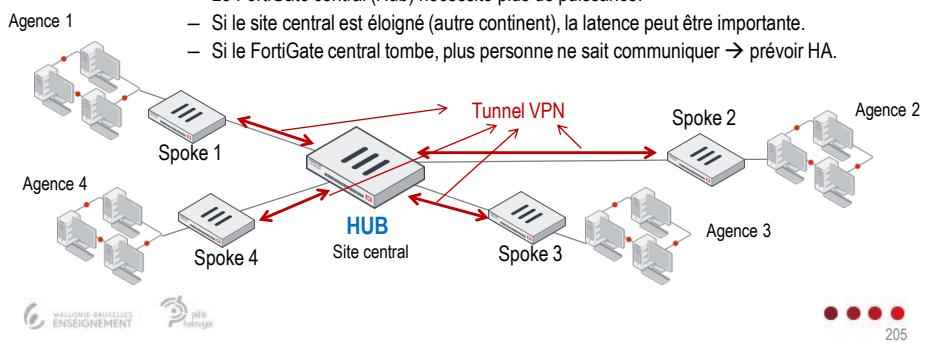
- Tous les clients se connectent via un équipement central appelé hub

- Avantages**

- La configuration VPN et les règles de pare-feu sont facilement gérées.
- Consommation minimales de ressources dans chaque agence : un seul tunnel suffit.

- Inconvénients**

- Le FortiGate central (Hub) nécessite plus de puissance.
- Si le site central est éloigné (autre continent), la latence peut être importante.
- Si le FortiGate central tombe, plus personne ne sait communiquer → prévoir HA.



Topologies VPN

4. Full meshed

- Maillage complet**

- Tous les FortiGates sont reliés les uns aux autres.

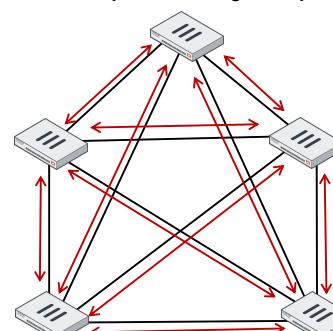
- Avantages**

- Moins de latence.
- Excellent tolérance aux pannes.
- Le site central nécessite moins de BP.

- Inconvénients**

- Consommation de ressources**
 - Chaque FortiGate nécessite autant de tunnels qu'il n'y a de FortiGates distants.
- Topologie la plus complexe**
 - Notamment au niveau du routage.
- Plus cher**
 - Nécessite du matériel plus puissant.

Exemple de maillage complet



Chaque double flèche représente un tunnel VPN

Topologies VPN

5. Partial meshed

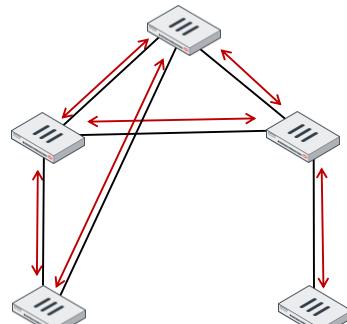
– Maillage partiel

- Chaque FortiGate (site, agence) n'a pas nécessairement besoin de communiquer avec tous les autres.

– Caractéristiques

- Nécessite moins de ressources qu'un maillage complet.
- Conserve une bonne latence par rapport à une topologie hub and spoke.
- La configuration reste plus complexe par rapport à une topologie hub and spoke.

Exemple de maillage partiel



Chaque double flèche représente un tunnel VPN

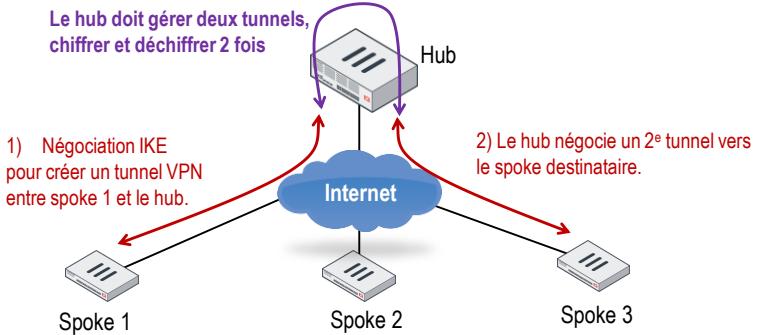
Comparatif

Hub-and-Spoke	Partial Mesh	Full Mesh
Configuration plus facile	Configuration moyenne	Configuration plus complexe
Peu de tunnels	Nombre moyen de tunnels	Plus de tunnels
Nécessite plus de BP aux Hubs	BP moyenne aux hubs	Moins de BP
Pas de tolérance de panne (SPOF)	Tolérance de panne partielle	Tolérance de panne pour chaque site
Spokes : peu de ressources Hubs : beaucoup de ressources	Consommation moyenne de ressources	Nécessite plus de ressources système
Evolutif	Un peu évolutif	Difficilement évolutif
Pas de communications directes entre sites	Communications directes entre certains sites	Communications directes entre tous les sites

Auto Discovery VPN (ADVPN)

- Sans ADVPN

- Communication VPN entre spoke 1 et spoke 3.

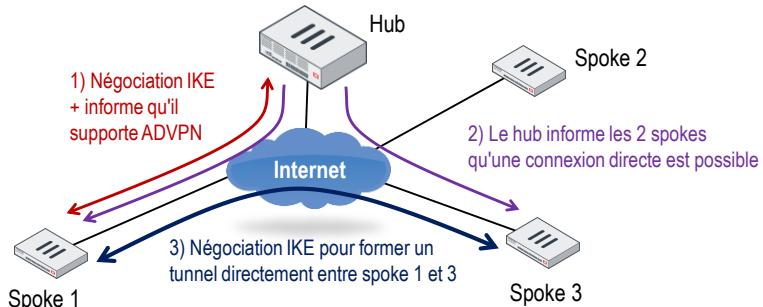


Auto Discovery VPN (ADVPN)

- Avec ADVPN

- Négociation dynamique de VPN

- ADVPN est un protocole permettant de négocier dynamiquement et à la demande des tunnel VPN directs entre les sites secondaires (spokes).



Auto Discovery VPN (ADVPN)

- **ADVPN**

- **Avantages**

- **Utile dans une topologie Hub-and-spoke ou partial meshed :**

- Offre les avantages d'une topologie à maillage complet.
 - Offre les facilités de configuration et d'évolutivité d'un déploiement hub and spoke ou partial meshed.

- **Routage dynamique nécessaire**

- ADVPN nécessite l'utilisation d'un protocole de routage pour que les spokes puissent apprendre les routes vers d'autres spokes sans devoir être préconfigurés.

- **FortiOS**

- Actuellement Auto-discovery VPN est uniquement supporté par IKEv1.
 - Les spokes doivent avoir une IP routable à partir de n'importe quel autre spoke.
 - Les périphériques derrière NAT sont supportés depuis la version 6 pour autant que les ports UDP 500 et 4500 soient ouverts.
 - ADVPN est similaire mais non compatible avec DMVPN (Cisco).

Auto Discovery VPN (ADVPN)

- **Étapes de configuration ADVPN**

1. **Ajouter aux FortiGates les configurations VPN**

- De manière à construire une topologie hub and spoke ou partial meshed.
 - Voir chapitre VPN IPsec.

2. **Activer ADVPN**

- *auto-discovery-receiver* sur les VPN des spokes
 - *auto-discovery-sender* sur les VPN du hub qui vont vers les spokes.
 - *auto-discovery-forwarded* sur les VPN du hub qui vont vers d'autres hub.

3. **Configurer le routage**

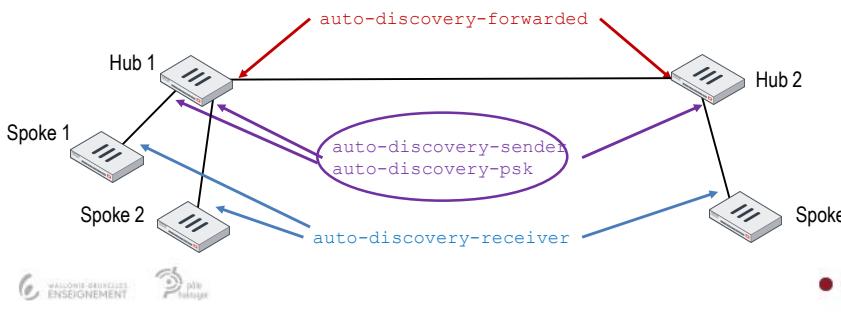
- Un routage dynamique est nécessaire afin que les spokes puissent apprendre les routes vers d'autres spokes après que les VPN dynamiques aient été négociés.
 - Voir chapitre sur le routage.

Auto Discovery VPN (ADVPN)

- Exemple de configuration ADVPN

Configurer IPsec phase 1 :

- A configurer sur les hubs vers les spokes : **auto-discovery-sender**
auto-discovery-psk
- A configurer sur les hubs reliés à d'autres hubs : **auto-discovery-forwarded**
- A configurer sur les spokes : **auto-discovery-receiver**



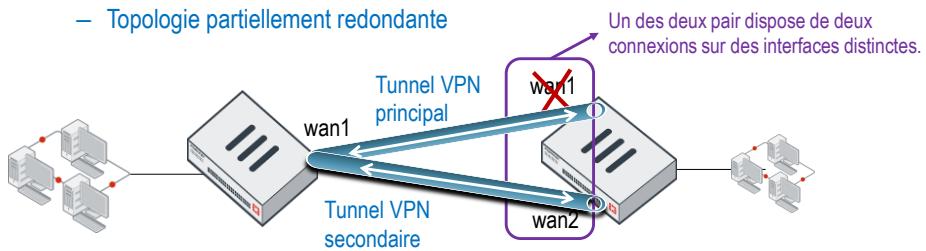
VPN redondants

- Tolérance aux pannes

- Résilience

- Selon la topologie, si un hub tombe en panne, tous les VPN pourraient tomber.
 - Pour améliorer la tolérance aux pannes, il est possible de configurer plusieurs VPN entre deux passerelles VPN.
 - Uniquement pris en charge par les VPN route-based.

- Topologie partiellement redondante



Si le tunnel VPN principal échoue, FortiGate redirige le trafic à travers le VPN de secours

VPN redondants

– Topologie totalement redondante

- Les deux pairs terminent leurs VPN sur des ports physiques différents.



- Les deux pairs terminent leurs VPN sur des ports physiques différents et passent par des FAI différents.



VPN redondants

• Étapes de configuration de VPN redondants

1. Créer une IKE phase 1 en mode route-based pour chaque tunnel VPN
 - Activer l'option Dead peer detection à chaque extrémité du tunnel (nécessaire).
2. Créer au moins une IKE phase 2 pour chaque phase 1
3. Ajouter au moins une route pour chaque VPN (route-based)
 - Routes statiques et/ou dynamiques.
 - Utiliser la distance administrative, la priorité ou la métrique pour sélectionner les routes principales par rapport aux routes de sauvegarde.
4. Configurez les règles de pare-feu pour chaque interface tunnel
 - Autoriser le trafic à la fois pour le VPN principal et le VPN de sauvegarde.

VPN redondants

- Configuration de VPN redondants avec SD-WAN

Network > SD-WAN

SD-WAN
Name SD-WAN
Type SD-WAN Interface
Status Enable Disable
SD-WAN Interface Members

Interface	Gateway	Cost	Status
	Search		
	+ VPN		
port1			
port2			
port3			
port4			
port5			
port6			
port7			
port8			
port9			
port10			

SD-WAN Usage
 Bandwidth
 Upstream D

Apply

Create IPsec VPN for SD-WAN members

Authentication
Name: Branch_Office
Remote Device: IP Address: Dynamic DNS: 10.200.3.1
Outgoing Interface: port1, port2

Authentication Method: Pre-shared Key, Signature
Pre-shared Key: *****
VPN tunnel will be created for each selected interface.

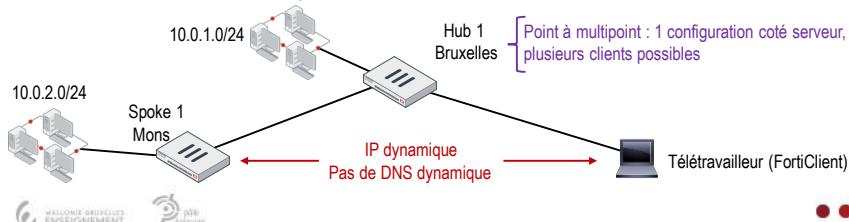
Branch_Office: Site to Site - FortiGate

< Back Create 217

Les VPN liés à ces deux interfaces sont membres du SD-WAN

Dialup VPN

- Configuration d'un VPN d'accès à distance (Remote access)
 - Les étapes sont identiques à celles pour un VPN de site à site
 - Configurer IKE phase 1 et IKE phase 2.
 - Configurer les règles de pare-feu.
 - Configurer le routage.
 - Les paramètres de configuration sont différents sur les deux pairs
 - Contrairement à un VPN de site à site où les pairs ont des configurations miroirs.
 - Seul le côté "client" peut initier le tunnel VPN



Dialup VPN

• Configuration IKE phase 1 côté serveur

Choix de l'option « Dialup » pour le pair distant

Si plusieurs dialup VPN sont requis :
 - Le mode « Aggressive » doit être sélectionné.
 - « Peer ID » doit être configuré.

Permet de renforcer la sécurité (Optionnel):
 - Demande un couple username/password en plus de la Pre Shared Key.

XAUTH
Type : Auto Server
User Group : Choose

Autorisé tous les groupes d'utilisateurs authentifiés par la règle de pare-feu autorisant le trafic VPN

Dialup VPN

• Configuration IKE phase 2 côté serveur

Extension IPsec appelée "IKE Mode Configuration"

Par défaut, les VPN FortiClient l'utilisent pour récupérer leurs paramètres IP pour le VPN.

- Configuration IKE phase 2 coté serveur (suite)
 - IKE Phase 2 Quick mode selectors (Coté serveur)
 - Local address: le sous-réseau coté serveur VPN.
 - Remote address: 0.0.0.0/0 (permet de correspondre à n'importe quelle adresse client).
- Configuration du routage (coté serveur)
 - Pour les VPN en mode route, une route statique vers le sous-réseau du client est automatiquement ajoutée après l'établissement du VPN.

Phase 2 Selectors			
Name	Local Address	Remote Address	
ToRemote	10.0.1.0/255.255.255.0	0.0.0.0/0.0.0.0	

Type	Network	Gateway IP	Interfaces	Distance
Static	0.0.0.0	10.200.1.254		10
Connected	10.0.1.0/24	0.0.0.0		0
Static	10.0.2.0/24	10.200.3.1		15
Connected	10.200.10.24	0.0.0.0		0
Connected	10.200.2.0/24	0.0.0.0		0

- Configuration du routage (coté serveur)
 - Si `add-route` est activé (choix par défaut) et le pair distant est de type “Dialup User”
 - Inutile de configurer une route statique.
 - A la fin de IKE phase 2 FortiGate ajoute **automatiquement** une route statique ayant comme destination le réseau local présenté par le pair distant.
 - Si `add-route` est désactivé
 - Un protocole de routage dynamique doit être utilisé et se charge de la mise à jour des routes.

```
config vpn ipsec phase1-interface
  edit "Dialup"
    set add-route enable | disable
  next
end
```

Destination	Subnet	Named Address	Internet Service
	10.0.2.0/24		
Device			
Administrative Distance	10		0/255
Comments			
Status	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
<input type="checkbox"/> Advanced Options			

Dialup VPN

- Configuration des règles de pare-feu
 - Deux règles à configurer sur chaque équipement (1 par sens).
 - Utiliser l'interface virtuelle IPsec (ToRemote dans l'exemple).

The image shows two side-by-side policy configuration windows from a FortiGate interface:

- New Policy (Traffic to Remote):**
 - Name: Traffic to Remote
 - Incoming Interface: port3
 - Outgoing Interface: ToRemote
 - Source: LOCAL_SUBNET
 - Destination: REMOTE_SUBNET
 - Schedule: always
 - Action: ✓ ACCEPT (selected)
 - Inspection Mode: Flow-based
- New Policy (Traffic from Remote):**
 - Name: Traffic from Remote
 - Incoming Interface: ToRemote
 - Outgoing Interface: port3
 - Source: REMOTE_SUBNET
 - Destination: LOCAL_SUBNET
 - Schedule: always
 - Action: ✓ ACCEPT (selected)
 - Inspection Mode: Flow-based

Dialup VPN

- Configuration d'un Dialup VPN coté serveur avec le wizard
 - Assistant de configuration facilitant la configuration de VPN.
 - Pratique si tous les clients sont des FortClients.

Le Wizard va notamment utiliser :

- Le mode route-based.
- Xauth.
- IKE Mode Configuration.

The image shows the FortiGate VPN Setup wizard interface across three tabs:

- VPN Setup:** Shows 'DialUp' as the Site-to-Site connection type.
- Authentication:** Shows 'FortiClient VPN for OS X, Windows, and Android' selected. It includes fields for 'Incoming Interface' (port1), 'Authentication Method' (Signature), 'Pre-shared Key' (*****), and 'User Group' (Training).
- Policy & Routing:** Shows 'port3' as the Local Interface, 'LOCAL_SUBNET' as the Local Address, and '10.200.200.1-10.200.200.10' as the Client Address Range.
- Client Options:** Shows 'Save Password' checked, 'Auto Connect' unchecked, and 'Always Up (Keep Alive)' unchecked.

A red exclamation mark icon with the text 'Vérifier la compatibilité des versions FortiClient et FortiOS' is overlaid on the first tab.

Dialup VPN

- Configuration IKE phase 1 côté client (client FortiGate)

The screenshot shows the FortiGate configuration interface for IKE Phase 1. It includes sections for Network (Remote Gateway: Static IP Address, Interface: port1), Authentication (Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Aggressive), and XAUTH (Type: Client, User Name: VPNUser). Annotations explain the 'Local ID' field (Site 1) and the 'XAUTH' section.

Annotations:

- Remote Gateway: Static IP Address, Interface: port1 → Définir si le serveur utilise une adresse IP statique ou dynamique DNS.
- IKE Version: 1, Mode: Aggressive → Mode « Aggressive » et « local ID » si de multiples dialup VPN sont utilisés.
L'ID local doit correspondre au « Peer ID » défini sur le serveur et identifiant ce client.
- XAUTH → Xauth en mode client

Bottom right corner: 225

Dialup VPNs

- Configuration IKE phase 2 côté client (client FortiGate) (suite)

- IKE phase 2 Quick mode selectors (côté client)

- Local address : le sous-réseau du client VPN.
 - Remote address : le sous-réseau du serveur.

Phase 2 Selectors		
Name	Local Address	Remote Address
ToLocal	10.0.2.0/255.255.255.0	10.0.1.0/255.255.255.0

- Configuration du routage (côté client)

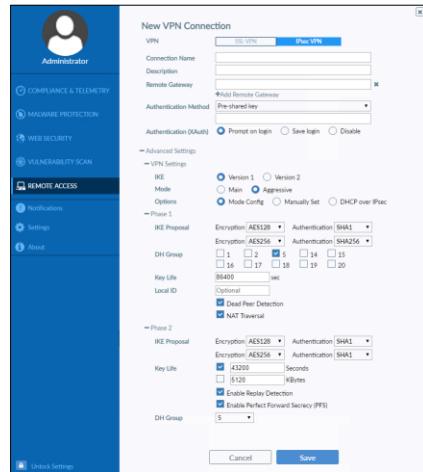
- Une route statique vers le réseau du serveur doit être ajoutée manuellement.

Edit Static Route		
Destination	Subnet	Named Address / Internet Service
Interface	ToLocal	10.0.1.0/255.255.255.0
Administrative Distance	10	
Comments	Write a comment... 0/55	
Status	Enabled	Disabled

Dialup VPNs

- Configuration IKE phase 1 côté client (client FortiClient)

Remote Access tab > Configure VPN > IPsec VPN



227

Accélération matérielle

- Accélération matérielle

- Possible selon le modèle de pare-feu

- Certains modèles permettent le déchargement des opérations de chiffrement et déchiffrement IPsec.

- Si elle est disponible, l'accélération matérielle est activée par défaut

- Pour désactiver l'accélération matérielle :

```
config vpn ipsec phase1-interface
  edit <VPN-interface>
    set npu-offload enable | disable
  end
```

• • • 228

Accélération matérielle

- Vérifier le déchargement dans le cas d'un VPN IPsec

```
# diagnose vpn tunnel list
list all ipsec tunnel in vd 3
-----
name=p1-vdom1 ver=1 serial=5
11.11.11.1:0->11.11.11.2:0
lgwy=static
tun=tunnel mode=auto bound_if=47
proxyid_num=1 child_num=0 refcnt=8
ilast=2 olast=2
stat: rxp=3076 txp=1667
rxb=4299623276 txb=66323
.....
ah=md5 key=16
6214155f76b63a93345dcc9ec02d6415
dec:pkts/bytes=3073/4299621477,
enc:pkts/bytes=1667/66375
npu_flag=03 npu_rgwy=11.11.11.2
npu_lgwy=11.11.11.1 npu_selid=4
```

- npu_flag* indique le déchargement du VPN :
- npu_flag=00* - Pas d'accélération matérielle
 - npu_flag=01* - Chiffrement uniquement
 - npu_flag=02* - Déchiffrement uniquement
 - npu_flag=03* – Chiffrement et déchiffrement

IPsec Log

- Journaliser les événements VPN

Log & Report > Log settings

Event Logging	All	Customize
<input checked="" type="checkbox"/> System activity event	<input type="checkbox"/>	<input checked="" type="checkbox"/> VPN activity event
<input checked="" type="checkbox"/> User activity event	<input type="checkbox"/>	<input checked="" type="checkbox"/> Router activity event
<input checked="" type="checkbox"/> WiFi activity event	<input type="checkbox"/>	<input checked="" type="checkbox"/> Explicit web proxy event
<input checked="" type="checkbox"/> Endpoint event	<input type="checkbox"/>	<input checked="" type="checkbox"/> HA event
<input checked="" type="checkbox"/> Compliance Check Event	<input type="checkbox"/>	<input checked="" type="checkbox"/> Security audit event

Log & Report > VPN Events

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
42	05:12:04	██████	negotiate	failure	progress IPsec phase 2	To Remote

Log Details

- General
 - Date: 01/18/2018
 - Time: 05:12:04
 - Virtual Domain: root
- Log Description: Progress IPsec phase 2
- Source
 - Local IP: 10.200.1.1
 - User: fortinet
 - Group: N/A
 - XAUTH User: N/A
 - XAUTH Group: N/A
- Action
 - Action: negotiate
 - Status: failure
 - Result: ERROR

Une erreur est survenue pendant la négociation de la phase 2

HEH.be Sciences et technologies

IPsec Log

- Journaliser les événements VPN

Log & Report > VPN Events

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
5	06:16:46		tunnel-up		IPSec connection status change	FClient 0

Log Details

General

Date: 01/18/2018
Time: 06:16:46
Duration: 0s
Virtual Domain: root

Log Description: IPSec connection status changed

Source

Local IP: 10.200.1.1
User: N/A
Group: N/A
XAUTH User: student
XAUTH Group: training

L'utilisateur est connecté via un Forticlient

L'utilisateur est connecté

231

HEH.be Sciences et technologies

IPsec Log

- Journaliser les événements VPN

Log & Report > VPN Events

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
2	06:29:41		negotiate	failure	negotiate IPSec phase 1	FClient

Log Details

General

Date: 01/18/2018
Time: 06:29:41
Virtual Domain: root

Log Description: Negotiate IPSec phase 1

Source

Local IP: 10.200.1.1
User: N/A
Group: N/A
XAUTH User: student
XAUTH Group: N/A

Action

Action: negotiate
Status: failure
Result: XAUTH authentication

L'authentification de l'utilisateur a échoué

232

HEH.be
Sciences
et technologies

IPsec VPN Monitor

- Moniteur de tunnel IPsec
 - Permet d'afficher les informations sur les tunnels actifs.

Utilisateurs authentifiés

Adresse IP du client VPN distant

Clic droit offre la possibilité de déconnecter le tunnel

Monitor > IPsec Monitor

Name	XAUTH User	Type	Remote Gateway	Incoming Data	Outgoing Data
FClient_0	student	Dialup - FortiClient (Windows, Mac OS, Android)	10.200.3.1	14.34 kB	3.96 kB

Resel Statistics Bring Up Bring Down Phase 2 Selector: FClient Locate on VPN Map All Phase 2 Selectors

HEH.be
Sciences
et technologies

Dépannage

- Dépannage
 - Interopérabilité
 - Certaines marques de périphériques ne supportent pas :
 - Le quick mode selectors configuré à 0.0.0.0/0
 - Et/ou qui utilisent des sous-réseaux de tailles différentes.
 - Par conséquent, ces appareils nécessitent un SA différent (et une phase 2 différente) pour chaque paire de sous-réseaux locaux et distants protégés.
 - Solution
 - Soit configurer une phase 2 différente pour chaque paire de sous-réseaux locaux et distants
 - Soit définir une seule phase 2 et activer le sélecteur dynamique IKEv1

```
config vpn ipsec [ phase1 | phase1-interface ]
    edit <vpn_name>
        set mesh-selector-type subnet
```

- Le tunnel ne se forme pas

- Vérifier les configurations

- La plupart des problèmes de connexion sont dus à des erreurs de configuration.
 - Vérifier que les paramètres sont cohérents au niveau des deux extrémités.

- IKE real time debug

- Activer le débogage temps réel sur chaque extrémité du tunnel.
 - Permet de voir les détails de négociation des phases 1 et 2.

Filtrer les messages de débogage

```
diagnose vpn ike log-filter dst-addr4 <remote peer IP>
diagnose debug application ike -1
diagnose debug enable
```

- Stopper le débogage

```
diagnose debug reset
diagnose debug disable
```

Activer le débogage

- Exemple de debug (phase 1)

Réception du 1^{er} paquet, la phase 1 utilise le mode « Main »

```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2...
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
Nom de la phase 1
ike 0: Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
...
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

Le peer distant a été trouvé et une phase 1 correspond

Réussite de l'authentification et établissement de la IKE SA (Phase 1)

- Exemple de *debug* (phase 2)

Proposition d'un « quick mode selector » par le pair distant.

```

ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0.0.0.0-255.255.255.255:0,
me:0:0.0.0.0-255.255.255.255:0
...
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:500, len=356
ike 0: comes 172.20.187.114:500->172.20.186.222:500, ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
...
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap

```

Le quick mode selector négocié.

La SA IPsec a été correctement négociée et le tunnel est up.

Chapitre 6

Transport Layer Security

TLS

- **Objectifs**

- Comprendre et expliquer le fonctionnement de SSL/TLS.
- Comprendre et expliquer les différents niveaux de validations des certificats numériques.
- Pouvoir vérifier la sécurité d'un site et d'un navigateur en ce qui concerne les accès en HTTPS.

- **VPN d'accès à distance**

- **Communications sécurisées entre les télétravailleurs et l'entreprise**

- Le VPN peut assurer la confidentialité, l'intégrité, l'authentification et l'anti-rejeu.
- Les droits d'accès peuvent être adaptés selon les utilisateurs
 - Employés, sous-traitants, partenaires, ...

- **Déploiement d'un VPN d'accès à distance**

- **Via le protocole SSL (VPN SSL)**

- Permet la connectivité à partir de périphérique BYOD.
- Peu, voir pas de maintenance logicielle.
- Portails Web personnalisés pour les utilisateurs à l'ouverture d'une session.

- **Via le protocole IPsec (VPN IPsec)**

- D'un point de vue sécurité (Puissance du chiffrement et de l'authentification), IPsec est meilleur que SSL.
- Le VPN IPsec prend en charge un plus grand nombre d'applications que le VPN SSL.

- SSL et TLS

- Secure Socket Layer

- Développé initialement par Netscape pour protéger les échanges sur Internet.
 - A l'époque, norme imparfaite et non normalisée.

- Transport Layer Security

- L'IETF a poursuivi le développement de SSL

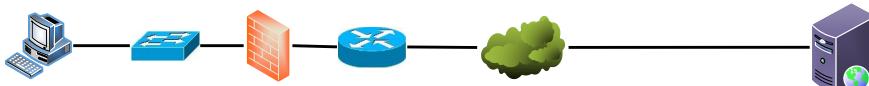
- En rebaptisant TLS pour des questions de droits.
 - Fonctionne en mode client-serveur.
 - Norme actuelle = TLS 1.2

- TLS est un ensemble de protocoles de sécurisation des échanges

- Il permet d'authentifier le serveur et le client.
 - Il permet de chiffrer les données.
 - Il permet de vérifier l'intégrité des données.
 - Il permet d'empêcher le rejet.

On emploie souvent SSL bien que ce soit TLS qui est maintenant utilisé.

TLS est complètement transparent pour les utilisateurs



Client Hello

- 1) Requête https du client (versions TLS, algorithmes supportés, ... + nombre aléatoire)

Keys	Cipher	Hash
RSA, DH-RSA	AES, 3DES	HMAC-SHA2, AEAD

Server Hello

- 2) Utilise tels algorithmes + nombre aléatoire.

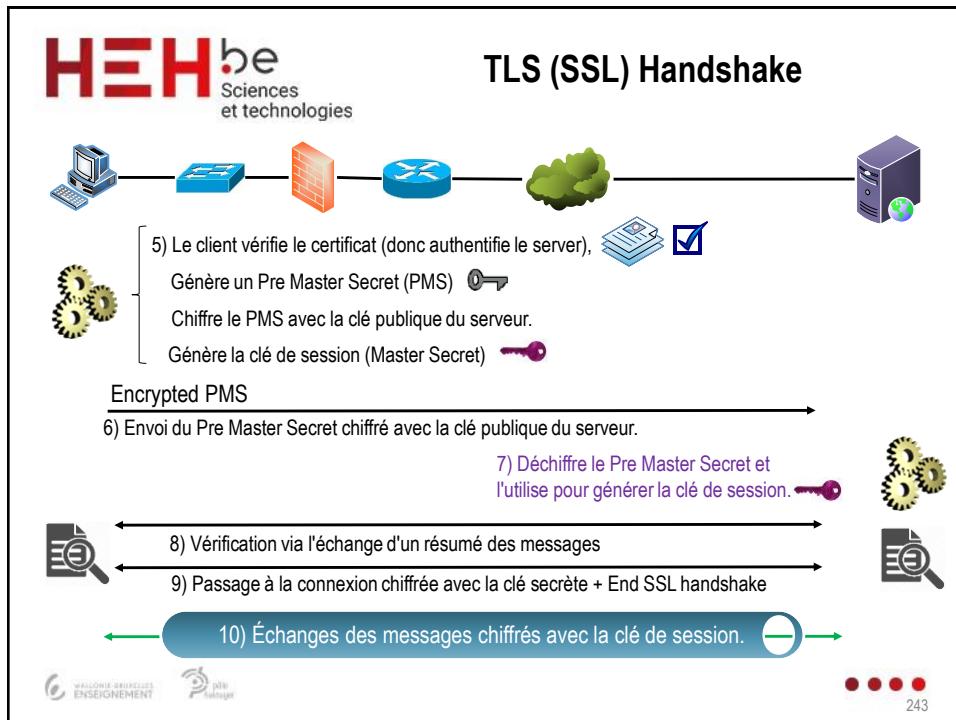


Server Hello Done

- 3) Le serveur envoie son certificat

Demand Client Certificate

- 4) Optionnel : demande le certificat du client et l'authentifie.



HEH.be Sciences et technologies

SSL/TLS

- TLS est transparent pour l'utilisateur
 - Comment savoir si l'on se connecte à un site sécurisé?

Cadenas
HTTPS

Vérifier la sécurité de la connexion d'un site

Pour savoir si un site peut être consulté en toute sécurité, vous pouvez vous reporter aux informations de sécurité relatives au site en question. Un message d'avertissement s'affiche dans Chrome s'il s'avère impossible de consulter le site de manière sécurisée ou de manière confidentielle.

1. Ouvrez une page dans Chrome sur votre ordinateur.
2. Pour vérifier la sécurité d'un site, consultez l'état de sécurité à gauche de l'adresse Web :
 - 🔒 Sécurisé
 - ⓘ Informations ou Non sécurisé
 - ⚡ Non sécurisé ou Dangereux
3. Pour afficher les détails et les autorisations du site, cliquez sur l'icône. En haut du panneau se trouve un récapitulatif sur le niveau de sécurité de la connexion selon Chrome.

Wallonie-Bruxelles Enseignement Pôle Formation

244

HEH.be
Sciences
et technologies

SSL/TLS

- Reconnaitre un site sécurisé avec TLS

Indique aussi la société ou l'individu qui possède le nom de domaine → certificat EV.

www.zdnet.fr Connexion non sécurisée
Permissions
Vous n'avez pas accordé de permission particulière à ce site.

www.abondance.com/a
Walla! Vérifié par : Let's Encrypt https://

Belfius Bank (BE) https://www.belfius.be/common/nl/fv
Belfius Bank Connexion sécurisée
Votre connexion à ce site est sécurisée.
Son détenteur est :
Belfius Bank
Bruxelles
Bruxelles, BE
Vérifié par : DigiCert Inc

WALLONIE-BRUXELLES
ENSEIGNEMENT

245

Niveaux de validations des certificats

Let's Encrypt (LE)

- Autorité de certification (depuis 2015)
 - Plus de 10 millions de certificats ont été délivrés après seulement un an.
- Peut fournir des certificats gratuits X.509
 - Pour la sécurisation des sites Internet avec TLS.
- Tout est automatisé
 - Création, validation, signature, installation et renouvellement des certificats,

Niveaux de validations des certificats

- Domain Validated (DV)
- Organization Validated (OV)
- Extended Validation (EV)

WALLONIE-BRUXELLES
ENSEIGNEMENT

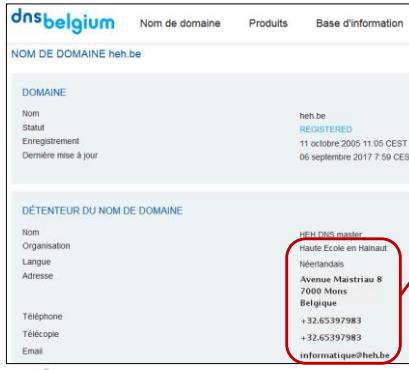
246

Niveaux de validations des certificats

- WHOIS

- Service de recherche

- Permet d'obtenir des informations sur une adresse IP ou un nom de domaine.



The screenshot shows the dnsbelgium interface with the domain 'heh.be' entered. It displays two sections: 'DOMAINE' and 'DÉTENTEUR DU NOM DE DOMAINE'. The 'DOMAINE' section shows the name 'heh.be', status 'REGISTERED', registration date '11 octobre 2005 11:05 CEST', and last update '06 septembre 2017 7:59 CEST'. The 'DÉTENTEUR DU NOM DE DOMAINE' section shows contact details for 'HEH DNS master' at 'Haute Ecole en Hainaut-Wallonie, Avenue Maistriau 8, 7000 Mons, Belgique' with phone numbers '+32 65 397 983' and '+32 65 397 983' and email 'informatique@heh.be'. A red box highlights this contact information, and a red arrow points from it to the text below.

Ces informations sont purement déclaratives
Elles ne sont pas vérifiées par les registraires.



247

Niveaux de validations des certificats

- Domain Validated (DV SSL)

- Avantages

- Certificat bon marché et délivré rapidement (automatisé).

- Inconvénients

- La CA vérifie uniquement que le propriétaire du nom de domaine est le demandeur du certificat

- Vérification généralement par envoi d'un e-mail à l'adresse trouvée dans le WHOIS.
 - Ne garanti pas l'identité du propriétaire du site Web ni même l'existence de l'organisation/entreprise.

- Une attaque par phishing est possible. Un pirate peut :

- Faire enregistrer www.belfius.be (un L au lieu du i).
 - Fournir de fausses informations au WHOIS (adresse gmail, numéro de téléphone VoIP, ...).
 - Créer un faux site ressemblant à celui de la banque.

→ le pirate aura un faux site similaire au site de Belfius, avec une URL très similaire et un certificat valide.

Blogs,
Sites Web perso,
Sites Web d'entreprise (*)

248

Niveaux de validations des certificats

- Domain Validated (DV)
 - Vérification du type de certificat

Niveaux de validations des certificats

- Organization Validated (OV SSL)
 - Ils garantissent la légitimité de l'organisation
 - Ils "activent" le protocole https, ainsi que le cadenas sur les navigateurs.
 - L'identité de l'entreprise est affichée sur les navigateurs, prouvant que le site est légitime.
- Extended Validation (EV SSL)
 - Appelé aussi High-Assurance Certificate
 - Ils "activent" le protocole https, le cadenas et la barre d'adresse verte.
 - Haut niveau de vérification
 - Vérification du droit exclusif d'utilisation du nom de domaine.
 - Vérification de l'accord de l'organisation pour l'émission du certificat.
 - Vérification de l'existence légale, physique et opérationnelle de l'organisation.
 - Vérification de l'exactitude des informations transmises (adresse, n° de téléphone), etc.

HEH.be
Sciences
et technologies

Les certificats

- Afficher les certificats

Belfius Banque - Belfius

Belfius Bank (BE) https://www.belfius.be/retail/fr/index.aspx

Belfius Bank Connexion sécurisée

Permissions

Vous n'avez pas accordé de permission particulière à ce site.

Belfius Bank

Connexion sécurisée

Votre connexion à ce site est sécurisée.
Son détenteur est :

Belfius Bank
Bruxelles
Bruxelles, BE

Vérifié par : DigiCert Inc

Plus d'informations

WALLONIE-BRUXELLES
ENSEIGNEMENT

DU
PROJET

251

HEH.be
Sciences
et technologies

Les certificats

Elliptic Curve Diffie-Hellman Ephemeral Clés éphémères Diffie-Hellman basées sur les courbes elliptiques

Informations sur la page - https://www.belfius.be/common/nl/fw/language....

Général Médias Permissions Sécurité

Identité du site web

Site web : www.belfius.be
Propriétaire : Belfius Bank
Vérifiée par : DigiCert Inc

Identité du site web

Site web : www.heh.be
Propriétaire : Ce site web ne fournit pas d'informations sur son propriétaire
Vérifiée par : TERENA

Afficher le certificat

Vie privée et historique

Ai-je déjà visité ce site web auparavant ? Oui, 3 fois
Ce site web collecte-t-il des informations (cookies) sur mon ordinateur ? Oui Voir les cookies
Ai-je un mot de passe enregistré pour ce site web ? Non Voir les mots de passe enregistrés

Détails techniques

Connexion chiffrée (clé 1 S_ECDHE_RSA_WITH_AES_256_GCM SHA384, 256 bits, TLS 1.2)

AES_256_GCM
AES en mode GCM

Galois/Counter Mode est un algorithme de chaînage

WALLONIE-BRUXELLES
ENSEIGNEMENT

DU
PROJET

252

Les certificats

- **Algorithme de chainage**

- **Algorithmes symétriques**

- Ils utilisent toujours la même clé et chiffrent des petits blocs de données : il y a risque de chiffrer plusieurs fois les mêmes blocs.
- En chiffrant toujours avec la même clé, il y a plus de risques qu'un pirate arrive à retrouver les clés (voir méthodes de cryptanalyse).

- **Algorithme de chainage.**

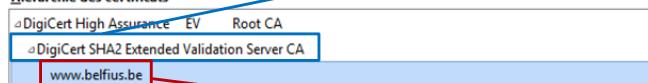
- Ces algorithmes permettent de s'assurer que des chiffrements distincts sont produits même lorsque le même texte est chiffré plusieurs fois avec la même clé.
- Exemples d'algorithmes
 - **CBC** : Cipher Block Chaining
 - **GCM** : Galois/Counter Mode
 - **EBC** : Electronic Codebook

Les certificats

Détails du certificat : « www.belfius.be »

[Général](#) [Détails](#)

Hierarchie des certificats



Le certificat de Belfius a été signé par DigiCert SHA2.

Ce serveur a le droit de parler pour www.belfius.be

Champs du certificat

- www.belfius.be
- Certificat
 - Version
 - Numéro de série
 - Algorithme de signature des certificats
 - Émetteur
 - Validité
 - Pas avant

On peut voir les attributs du certificat : N° de série, validité, ...

Valeur du champ

HEH.be
Sciences
et technologies

Les certificats

- Attributs du certificat

Champs du certificat

- Numéro de série
- Algorithme de signature des certificats
- Emetteur
- Validité
 - Pas avant
 - Pas après
- Sujet
- Info clé publique du sujet

Valeur du champ

PKCS #1 SHA-256 avec chiffrement RSA

Champs du certificat

- Numéro de série
- Algorithme de signature des certificats
- Emetteur
- Validité
 - Pas avant
 - Pas après**
- Sujet
- Info clé publique du sujet

Valeur du champ

11 juin 2018 à 14:00:00
(11 juin 2018 à 12:00:00 GMT)

Public-Key Cryptography Standards

Spécifications permettant d'accélérer le déploiement de la cryptographie à clé publique en définissant des norme de stockage et d'échange de certificats.

WALLONIE-BRUXELLES
ENSEIGNEMENT

DIGIPESTAGE

• • • 255

HEH.be
Sciences
et technologies

Les certificats

- Attributs du certificat

Champs du certificat

- Numéro de série
- Algorithme de signature des certificats
- Emetteur
- Validité
 - Pas avant
 - Pas après
- Sujet
- Info clé publique du sujet

Valeur du champ

CN = DigiCert SHA2 Extended Validation Server CA
OU = www.digicert.com
O = DigiCert Inc
C = US

Le certificat a été émis par l'autorité de certification
DigiCert SHA2 Extended Validation Server

WALLONIE-BRUXELLES
ENSEIGNEMENT

DIGIPESTAGE

• • • 256

Les certificats

- Attributs du certificat

Champs du certificat

Sujet
Info clé publique du sujet
Algorithme clé publique du sujet
Clé publique du sujet
Extentions
Identificateur de la clé d'autorité de certification
Clé d'identification du sujet du certificat
Nom alternatif du sujet du certificat

Valeur du champ

```
Module (2048 bits) :
d3 f7 06 54 d3 02 38 44 aa df d7 63 78 39 9f 8b
a1 25 41 dd 3b 26 bd 6c 22 fb 5a df f8 46 54 55
b4 d0 ff fa c0 76 48 73 5e 2d 93 6e 9e 8a 80 68
11 e3 0a 53 7a 09 34 c7 56 53 ec 15 17 9b 33 f3
5f c7 6d 1c f1 0e 64 33 64 90 17 10 df 17 1b 73
5d 6f f8 2d 2f 09 8e 74 fe e2 75 16 39 b7 aa 54
ad 7c ef 07 11 94 ad 5d 4e 4d a1 40 d5 09 20 eb
b5 98 28 7f 89 ad fe 0a 5a 90 4b 5d 07 83 a6 39
```

Le certificat contient la clé publique du serveur www.belfius.be

Les certificats

- Attributs du certificat

Champs du certificat

Utilisation de la clé étendue
Points de distribution de listes de certificats révoqués (LCR)
Politiques du certificat
Accès aux informations de l'autorité
Contraintes de base du certificat
Identificateur d'objet (13 6 1 4 1 11129 2 4 2)
Algorithme de signature des certificats
Valeur de signature du certificat

Valeur du champ

```
Taille : 256 octets / 2048 bits
43 99 81 37 62 0a a9 5b f1 2a d4 db 6d 3f 97 07
57 ae 9d c6 a1 98 84 37 ef 29 c7 74 63 04 57 11
73 c1 4b 51 33 74 17 ee 32 3d a6 17 7a 89 93 05
02 79 73 05 2a 14 4c 3b 75 44 3b 9c 1c e5 b5 d1
46 4a 3d ce d2 ef 7e 00 1d ae 51 36 5e 03 ce 76
73 d5 84 9a 00 b5 40 35 78 1f 0a 75 37 b5 98 66
15 93 57 61 37 9a 21 96 06 83 2e fb ac 77 4d d4
7f 2e e4 35 5a 57 13 93 bc fc 05 f8 a6 18 3e 39
```

Les informations du certificat (dont la clé publique de Belfius) ont été chiffrées par la clé privée de DigiCert SHA2 Extended Validation Server

Les certificats

- Attributs du certificat

Champs du certificat

- Validité
 - Pas avant
 - Pas après
- Sujet
 - Info clé publique du sujet
 - Algorithmie clé publique du sujet
 - Clé publique du sujet
- Extensions

Valeur du champ

CN = www.belfius.be

O = Belfius Bank
L = Bruxelles
ST = Bruxelles
C = BE

Identificateur d'objet (2 5 4 17) = 1000
Identificateur d'objet (2 5 4 9) = Boulevard Pachéco 44
Identificateur d'objet (2 5 4 5) = 0403.201.185

Indique le nom du serveur (CN : Common Name).

Informations sur l'Organisation à qui appartient le certificat.

259

Les certificats

- Chaine de certificats

DigiCert SHA2 a lui-même un certificat qui est joint au certificat de Belfius.

Détails du certificat : « www.belfius.be »

Général **Détails**

Hierarchie des certificats

- DigiCert High Assurance EV Root CA
- DigiCert SHA2 Extended Validation Server CA
- www.belfius.be

Champs du certificat

- Validité
 - Pas avant
 - Pas après
- Sujet
 - Info clé publique du sujet
 - Algorithmie clé publique du sujet
 - Clé publique du sujet
- Extensions

Valeur du champ

22 octobre 2028 à 14:00:00
(22 octobre 2028 à 12:00:00 GMT)

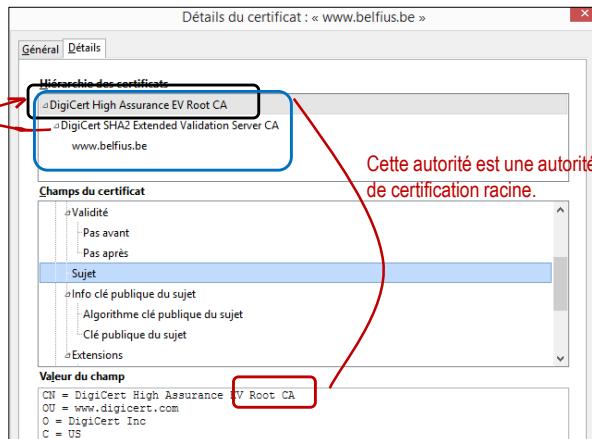
260

Les certificats

- Chaine de certificats

Le certificat DigiCert SHA2 est lui-même signé par une autre autorité de certification :
DigiCert High Assurance EV Root CA

C'est la chaîne de certificats classique :
 - Le certificat de l'autorité racine,
 - Le certificat de l'autorité d'enregistrement,
 - Le certificat client



Les certificats

- Pourquoi une chaîne de certificats ?

- Le navigateur doit pouvoir vérifier le certificat que le serveur lui envoie
 - Le certificat du serveur contient la signature de la CA (signé avec la clé privée de la CA).
 - Si le client parvient à déchiffrer la signature du certificat avec la clé publique de la CA, le certificat est authentique.
- Certains certificats sont intégrés aux navigateurs Il faut donc faire confiance à l'éditeur du navigateur !
 - La clé publique de la CA se trouve dans un de ces certificats intégrés
 - Pour que le navigateur puisse authentifier le certificat du serveur, il doit avoir le certificat de la CA contenant la clé publique de la CA.
 - Tous les certificats de toutes les CA et RA ne sont pas intégrés aux navigateurs.
 - » Les certificats des CA racines pourraient suffire.
- Au niveau mondial
 - Si une CA veut vendre des certificats au niveau mondial, ceux-ci vont se retrouver sur des milliers de machines à travers le monde.

Les certificats

- Pourquoi une chaîne de certificat ? (suite)

- Et si une CA racine perd sa clé privée?

- Si une CA racine perd ou se fait voler sa clé privée, il faut aller sur tous les navigateurs du monde pour modifier le certificat !
 - Pour cette raison, la clé privée de la CA racine est utilisée une seule fois puis placée en sécurité.

- Autorité intermédiaire

- Avant de mettre « au coffre » :

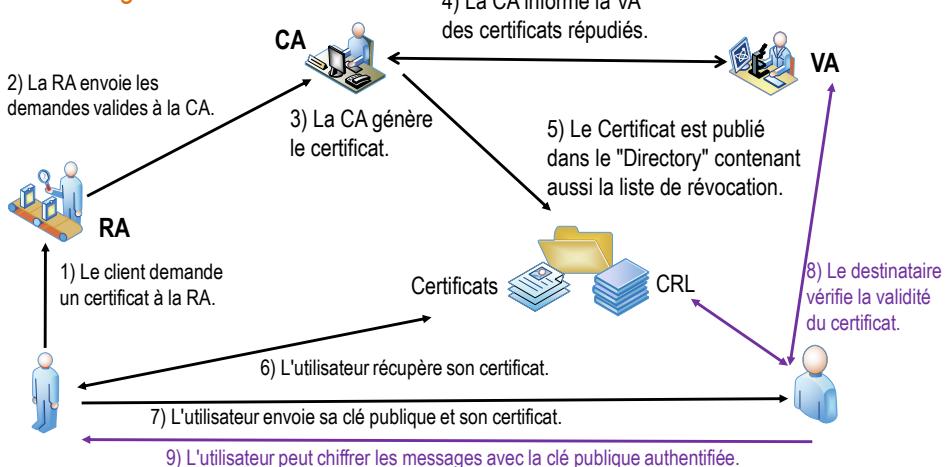
- On utilise la clé privée de l'autorité racine pour signer la paire de clés d'une autorité intermédiaire : l'autorité d'enregistrement.

- Si les clés de la RA sont compromises :

- On répudie le certificat de la RA.
 - On ressort la clé privée de la CA root de son coffre et on signe une nouvelle RA.
 - On n'a pas d'aller modifier tous les navigateurs car on garde la même CA root en qui on a toujours confiance.

Certificat

- Organisation d'une PKI



Une PKI est un ensemble de technologies, de procédures et de logiciels conçus pour gérer de manière sécurisée le cycle de vie des certificats numériques.

HEH.be
Sciences
et technologies

Les certificats

- Afficher les certificats connus du navigateur (Firefox)

Fichier Édition Affichage Historique Marque-pages Outils ?

Avancé

Général Données collectées Réseau Mises à jour Certificats

Requêtes

Lorsqu'un serveur demande votre certificat personnel :

en sélectionner un automatiquement
 vous demander à chaque fois

Interroger le répondeur OCSP pour confirmer la validité de vos certificats

Afficher les certificats Périphériques de sécurité

WALLONIE-BRUXELLES ENSEIGNEMENT DÉPARTEMENT DE L'ÉDUCATION ET DU PATRIMOINE 265

HEH.be
Sciences
et technologies

Les certificats

- Afficher les certificats connus du navigateur (Firefox)

Gestionnaire de certificats

Vos certificats Personnes Serveurs Autorités Autres

Nos navigateurs intègrent de nombreux certificats provenant de diverses autorités de certification.

Vous possédez des certificats enregistrés identifiant ces autorités de certification :

Nom du certificat	Périphérique de sécurité
Certigna Services CA	Sécurité personnelle
DigiCert Inc	Builtin Object Token
DigiCert Assured ID Root CA	Builtin Object Token
DigiCert Global Root CA	Builtin Object Token
DigiCert High Assurance EV Root CA	Builtin Object Token
DigiCert Assured ID Root G2	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token
DigiCert Global Root G2	Builtin Object Token
DigiCert Global Root G3	Builtin Object Token
DigiCert Trusted Root G4	Builtin Object Token

Voir... Modifier la confiance... Importer... Exporter... Supprimer ou ne plus faire confiance...

Le certificat de la RA n'est pas connu du navigateur? Celui de la CA root oui!

WALLONIE-BRUXELLES ENSEIGNEMENT DÉPARTEMENT DE L'ÉDUCATION ET DU PATRIMOINE 266

Les certificats

- Usage des certificats

– Exemple n°1 : le certificat du serveur www.belfius.be

The screenshot shows a list of certificate fields. The 'Usage of the certificate key' field is highlighted with a blue selection bar. Below it, under 'Value of the field', there is a list of three items: 'Critique', 'Signature', and 'Chiffrement de la clé'. The 'Chiffrement de la clé' item is also highlighted with a red box.

Un des champ renseigne à quoi peut servir le certificat.

La clé publique du certificat peut être utilisée pour signer et chiffrer.

Critique

Le certificat doit être utilisé uniquement pour le ou les objectifs indiqués.

Le contraire constituerait une violation de la politique de la CA.

Les certificats

- Usage des certificats

– Exemple n°2 : le certificat de la RA

The screenshot shows a list of certificate fields. The 'Usage of the certificate key' field is highlighted with a blue selection bar. Below it, under 'Value of the field', there is a list of four items: 'Critique', 'Signature', 'Signature de certificat', and 'Signature LCR'. The 'Signature de certificat' item is also highlighted with a red box.

La clé de la RA peut aussi servir à signer des certificats ou des CRL.

Les certificats

- Certification Practice Statement (CPS)
 - La politique de certification (CPS) est un document reprenant l'ensemble des règles que suit l'autorité d'enregistrement pour ses prestations.

Champs du certificat

Utilisation de la clé étendue
Points de distribution de listes de certificats révoqués (LCR)
Politiques du certificat
Accès aux informations de l'autorité
Contraintes de base du certificat
Identificateur d'objet (1 3 6 1 4 1 11129 2 4 2)
Algorithme de signature des certificats
Valeur de signature du certificat

Valeur du champ

Non critique
2.16.840.1.114412.2.1:
Pointeur de déclaration de pratique de certification:
<https://www.digicert.com/CPS>

La PCS est renseignée dans le certificat.

Les certificats

- OCSP

Champs du certificat

Utilisation de la clé étendue
Points de distribution de listes de certificats révoqués (LCR)
Politiques du certificat
Accès aux informations de l'autorité
Contraintes de base du certificat
Identificateur d'objet (1 3 6 1 4 1 11129 2 4 2)
Algorithme de signature des certificats
Valeur de signature du certificat

Valeur du champ

Non critique
OCSP: URI: <http://ocsp.digicert.com>
Emetteurs CA: URI: <http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt>

URL permettant de valider le certificat via OCSP

Les certificats

- Répondeur OCSP

- Problème

- La validation des certificats est généralement faite par les clients PKI
 - Le client va vérifier dans le "Directory" la liste actualisée des certificats révoqués.
 - Les clients ne gèrent pas toujours cette validation correctement
 - Par exemple, la mise à jour des informations des CRL n'est pas automatisée.
 - Les navigateurs ne disposent donc pas toujours d'une liste correcte des certificats révoqués.

- Online Certificate Status Protocol

- Protocole utilisé pour vérifier la validité d'un certificat numérique X.509
 - OCSP permet de centraliser les CRL au sein d'une PKI.
 - Le client communique alors avec qu'avec une seule entité.
 - Standard IETF (RFC 6960)

- Répondeur OCSP

- Comme les serveurs OCSP répondent aux requêtes clients, ils sont appelés répondeurs OCSP.

Les certificats

- OCSP Stapling

- Inconvénients d'OCSP

- Cela ajoute de la latence aux connexions HTTPS
 - Il faut une connexion supplémentaire vers l'autorité de validation afin de vérifier le certificat.
 - Cela peut bloquer l'accès au site si le répondeur OCSP ne répond pas.
 - Peut être considéré comme une fuite d'informations
 - Vous indiquez au répondeur OCSP les sites que vous visitez, ce qui peut être dommageable en termes de respect de la vie privée.

- L'agrafage OCSP

- Principe

- Le serveur HTTPS va lui-même fournir une réponse OCSP, directement lors de la négociation TLS (handshake).
 - » Il va agrafe cette réponse OCSP aux informations échangées lors de la phase de handshake TLS.
 - » Ce n'est donc plus au client d'effectuer le contrôle de validité.
 - La réponse OCSP agrafée par le serveur est fiable car elle est horodatée (donc non périmee) et signée par la CA.

- Le navigateur doit être compatible OCSP stapling

Quelques outils

- Qualys SSL Labs

- Documentations et outils

- Nombreux conseils pour gérer la sécurité de son site Web.
 - Des outils permettent de vérifier son site Web ainsi que son navigateur.

- Exemple de vérification d'un navigateur

Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2, which is recommended protocol version at the moment.

Logjam Vulnerability

Your user agent is not vulnerable.
For more information about the Logjam attack, please go to [weakdh.org](#).
To test manually, click [here](#). Your user agent is not vulnerable if it fails to connect to the site.

FREAK Vulnerability

POODLE Vulnerability

• • • 273

Quelques outils

- Qualys SSL Labs (suite)

- Exemple de vérification d'un navigateur (suite)

Protocol Features

Protocols	No
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	No
SSL 3	No
SSL 2	No

• • • 274

137

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple de vérification d'un navigateur (suite)

Cipher Suites (in order of preference)	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc0a) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc08) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Forward Secrecy	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) Forward Secrecy	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) Forward Secrecy	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112

(1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh.

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple de vérification d'un navigateur (suite)

Protocol Details	
Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA256/ECDSA, SHA384/ECDSA, SHA512/ECDSA, RSA_PSS_SHA256, RSA_PSS_SHA384, RSA_PSS_SHA512, SHA256/RSA, SHA384/RSA, SHA512/RSA, SHA1/ECDSA, SHA1/RSA
Named Groups	x25519, secp256r1, secp384r1, secp521r1
Next Protocol Negotiation	No
Application Layer Protocol Negotiation	Yes h2 http/1.1
SSL 2 handshake compatibility	No

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple de vérification d'un navigateur (suite)

Mixed Content Handling



Mixed Content Tests

Images

	Passive	Yes
Images	Active	No
CSS	Active	No
Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

CSS

Scripts

XMLHttpRequest

WebSockets

Frames

(1) These tests might cause a mixed content warning in your browser. That's expected.

(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Related Functionality

Upgrade Insecure Requests request header ([more info](#))

Yes



277

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple de vérification d'un site Web ne supportant pas HTTPS
 - Résultat du test effectué en aout 2017

SSL Report:

Assessed on: Thu, 10 Aug 2017 08:02:28 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Assessment failed: Unable to connect to the server

Known Problems

There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- No secure protocols supported - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- no more data allowed for version 1 certificate - the certificate is invalid, it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- Failed to obtain certificate and Internal Error - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- NetScaler issues - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- Unexpected failure - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers behind the same IP address. In such cases we can't provide accurate results, which is why we fail.



278

HEH.be
Sciences
et technologies

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple moins sécurisé
 - Résultat du test effectué en octobre 2018

SSL Report:
Assessed on: Tue, 23 Oct 2018 07:56:11 UTC | [Hide](#) | [Clear cache](#)

Scan Another »

WALLONIE-BRUXELLES
ENSEIGNEMENT

PRO
Présage

• • • 279

HEH.be
Sciences
et technologies

Quelques outils

- Qualys SSL Labs (suite)
 - Exemple moins sécurisé
 - Résultat du test effectué en février 2023

SSL Report:
Assessed on: Fri, 17 Feb 2023 08:57:24 UTC | [Hide](#) | [Clear cache](#)

Scan Another

WALLONIE-BRUXELLES
ENSEIGNEMENT

PRO
Présage

• • • 280

Quelques outils

- Qualys SSL Labs (suite)

Cipher Suites

Cipher Suite	Protocol	Key Exchange	Hash	AES	SHA	SSL/TLS
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	TLS	RSA	SIMPLE	128	128	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS	TLS	DHE RSA	SIMPLE	128	128	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	TLS	RSA	CAMELLIA	128	128	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 2048 bits FS	TLS	DHE RSA	CAMELLIA	128	128	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0x0113) ECDH secp571r1 (eq. 15360 bits RSA) FS	TLS	ECDHE RSA	SIMPLE	128	128	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	TLS	RSA	SIMPLE	128	256	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS	TLS	DHE RSA	SIMPLE	128	256	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9d) WEAK	TLS	RSA	GCM	128	256	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	TLS	DHE RSA	GCM	128	256	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc027) ECDH secp571r1 (eq. 15360 bits RSA) FS	TLS	ECDHE RSA	GCM	128	256	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp771r1 (eq. 15360 bits RSA) FS	TLS	ECDHE RSA	GCM	128	256	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	TLS	RSA	SIMPLE	256	256	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS	TLS	DHE RSA	SIMPLE	256	256	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x44) WEAK	TLS	RSA	CAMELLIA	256	256	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x58) DH 2048 bits FS	TLS	DHE RSA	CAMELLIA	256	256	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp571r1 (eq. 15360 bits RSA) FS	TLS	ECDHE RSA	SIMPLE	256	256	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0xd3) WEAK	TLS	RSA	SIMPLE	256	256	256

Quelques outils

- Qualys SSL Labs (suite)

- Exemple de vérification d'un site Web

- L'outil permet de vérifier la négociation du certificat, la négociation du protocole, l'échange de clé et la force du chiffrement.

SSL Report: www.heh.be (193.190.65.24)

Assessed on: Thu, 10 Aug 2017 08:08:32 UTC | [Hide](#) | [Clear cache](#) | [Scan Another](#)

Summary

Overall Rating: **A**

Certificate: 100

Protocol Support: 100

Key Exchange: 100

Cipher Strength: 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web (suite)

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1	
Subject	mail.heh.be Fingerprint SHA256: 42:05:ed:4e:4d:1d:b3:a3:d7:1f:3a:3b:2e:a1:0b:01:n0:0f:98:1d:4a:3d:32:47:7a:0
Common names	mail.heh.be
Alternative names	mail.heh.be admin.heh.be autodiscover.heh.be autodiscover.heh.be intranet.heh.be ext.ranet.heh.be hub.heh.be mail.heh.be phpmyadmin.heh.be phpmyadmin.heh.be student.heh.be student.heh.be webmail.heh.be webmail.heh.be www.heh.be www.heh.be
Serial Number	5cd258007612cfa6520036797fe634
Valid from	Tue, 17 Mar 2015 00:00 UTC
Valid until	Fri, 16 Mar 2016 23:59:59 UTC (expires in 7 months and 7 days)
Key	RSA 2048 bits (65537)
Weak key (Debian)	No
Issuer	TERENA-SSL CA 2 Alt: http://ca1.terena.org/TERENA-SSLCA2.cer
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://ca1.terena.org/TERENA-SSLCA2.crl OCSP: http://ocsp.terena.org
Revocation status	Good (not revoked)
DNS CAA	No (none info)
Trusted	Yes

• • • 283

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web (suite)

Configuration

Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web

Cipher Suites	
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x22)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
# TLS 1.1 (suites in server-preferred order)	
# TLS 1.0 (suites in server-preferred order)	

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web (suite)

Handshake Simulation	
Android 2.3.7 No Ssl 2 RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 4.0 RSA 2048 (SHA256)	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.1.1 RSA 2048 (SHA256)	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.2.2 RSA 2048 (SHA256)	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.3 RSA 2048 (SHA256)	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 4.4.2 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 5.0.0 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 6.0 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Android 7.0 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Baidu Jan 2015 RSA 2048 (SHA256)	TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
BlogReview Jan 2015 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Chrome 49 /XP SP3 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Chrome 57 /Win 7 R RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 31.3.0 ESR /Win 7 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 47 /Win 7 R RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 49 /XP SP3 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Firefox 53 /Win 7 R RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
Googlebot Feb 2015 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS
IE 8 /XP No F1 No Ssl 2 Server closed connection	
IE 7 /Windows 7 RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp521r1 FS

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web (suite)

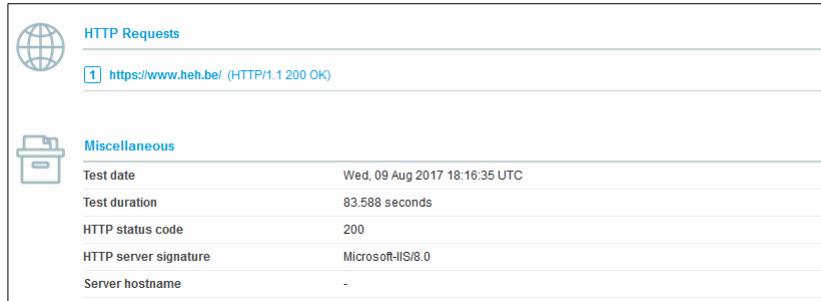
OpenSSL CCS vuln. (CVE-2014-0224)	Unknown (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE

Quelques outils

- HTTP Strict Transport Security (HSTS)
 - HSTS doit être activé sur le site Web
 - Permet à un serveur web de signifier au navigateur web compatible, qu'il doit obligatoirement être contacté en HTTPS.
 - Strict
 - Si la sécurité de la connexion n'est pas garantie (certificat auto-signé), l'utilisateur ne peut accéder au site.
 - Liste de pré-préchargement pour les pages HTTPS
 - Chaque première visite d'un site est vulnérable aux attaques (SSL stripping).
 - HSTS ne fonctionne que si un site Internet a été consulté au moins une fois dans le passé via une connexion HTTPS non manipulée.
 - Les navigateurs populaires utilisent aujourd'hui des listes basées sur un service de pré-chargement pour HSTS.
 - <https://hstspreload.org/>

Quelques outils

- Qualys SSL Labs
 - Exemple de vérification d'un site Web (suite)



HTTP Requests

1 [https://www.heh.be/ \(HTTP/1.1 200 OK\)](https://www.heh.be/)

Miscellaneous

Test date	Wed, 09 Aug 2017 18:16:35 UTC
Test duration	83.588 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/8.0
Server hostname	-

Chapitre 7

Configuration d'un VPN SSL/TLS

- **VPN SSL**
 - Utilisé notamment pour sécuriser les transactions Web.
 - Basé sur un tunnel HTTPS.
 - Utilisé pour accéder à des ressources internes
 - Les clients doivent s'authentifier sur une page Web : le portail VPN-SSL.
- **VPN IPsec**
 - Pour n'importe quelle application client-serveur.
 - Plutôt utilisé pour les VPN de site à site.
 - Compatible avec d'autres matériel que FortiGate.

	VPN SSL	VPN IPsec
Applications	<ul style="list-style-type: none"> • Applications Web, partage de fichiers, email. 	<ul style="list-style-type: none"> • Toutes les applications basées sur IP.
Type de tunnel	<ul style="list-style-type: none"> • Tunnel HTTPS (SSL/TLS) 	<ul style="list-style-type: none"> • Tunnel IPsec (ESP)
Sécurité	<ul style="list-style-type: none"> • Plus faible que IPsec. • Authentification unidirectionnelle possible. • Sécurise une application à la fois. 	<ul style="list-style-type: none"> • Meilleur que SSL/TLS. • Authentification bidirectionnelle avec secret partagé ou certificat. • Le tunnel IPsec sécurise toutes les communications entre les deux périphériques.
Identification Authentification	<ul style="list-style-type: none"> • Via une page web sur le Fortigate • Via un Forticlient (adaptateur virtuel Fortissl). 	<ul style="list-style-type: none"> • Via un Forticlient. • Les VPN de site à site ne nécessitent pas de Forticlient.

Comparaison VPN IPsec – VPN SSL

	VPN SSL	VPN IPsec
Interopérabilité	<ul style="list-style-type: none"> Peut être spécifique au fournisseur. 	<ul style="list-style-type: none"> Standard interopérable avec plusieurs fournisseurs.
Implémentation	<ul style="list-style-type: none"> Configuration plus simple (aucune installation) Uniquement d'un client SSL vers un serveur SSL (Fortigate). Aucun paramétrage requis par l'utilisateur. 	<ul style="list-style-type: none"> Plus flexible. <ul style="list-style-type: none"> Topologies en étoile et maillée possibles. Vers client ou autre passerelle VPN.
Connexions	<ul style="list-style-type: none"> Forticlient ↔ Fortigate. Navigateur Web ↔ Fortigate FortiGate ↔ FortiGate (depuis FortiOS 7.0) 	<ul style="list-style-type: none"> FortiClient ↔ FortiGate FortiGate ↔ FortiGate FortiGate ↔ Passerelle VPN IPsec tiers FortiGate ↔ Logiciel Client VPN IPsec tiers
Utilisation	<ul style="list-style-type: none"> Télétravailleurs, Utilisateurs mobile (Internet cafés, bibliothèques, ...) 	<ul style="list-style-type: none"> Site à site, site à agence. Data center.

Modes d'accès au VPN SSL

1. Mode tunnel

- Nécessite l'utilisation d'un client VPN (FortiClient ou FortiSSL)
 - Un adaptateur réseau virtuel nommé "fortissl" est créé sur le poste client.
 - L'UTM assigne dynamiquement une adresse IP routable à l'adaptateur virtuel.
- Deux modes de connexion
 - Soit via connexion au portail VPN-SSL
 - Sur la page du portail, on aura alors la possibilité d'activer le tunnel VPN.
 - Soit directement depuis le FortiClient sans passer par le portail
- Accès direct aux ressources
 - En mode tunnel
 - L'utilisateur sera "directement connecté" (pas de proxy) au réseau où se trouvent les ressources de l'entreprise.
 - L'utilisateur aura donc potentiellement accès à toutes les ressources de ce réseau comme s'il était lui-même physiquement connecté à ce réseau.
 - N'importe quelle application IP peut transmettre des données via le tunnel

Modes d'accès au VPN SSL

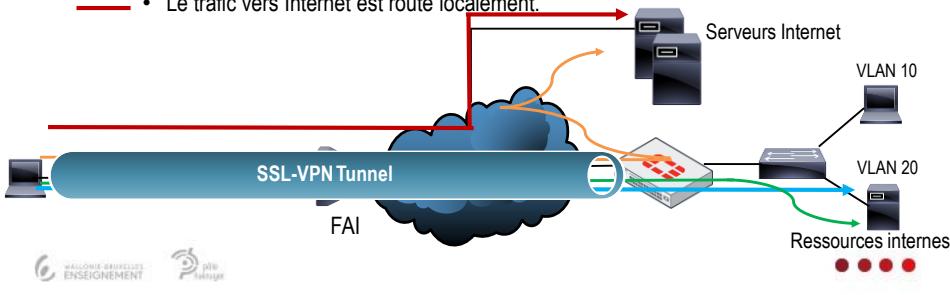
- Mode tunnel : Split tunneling

- Désactivé

- Tout le trafic du client est routé via le tunnel VPN SSL, y compris le trafic Internet.
 - Le FortiGate devient la passerelle par défaut des hôtes.

- Activé

- Le trafic du client destiné au réseau privé est routé via le tunnel VPN-SSL.
 - Le trafic vers Internet est routé localement.



Modes d'accès au VPN SSL

- Mode tunnel : FortiGate en tant que client VPN SSL

- Possible depuis FortiOS 7

- Un FortiGate peut être configuré comme un client VPN SSL, en utilisant une interface de type SSL-VPN Tunnel.
 - Permet aux appareils connectés au FortiGate client d'accéder aux ressources situées derrière le FortiGate serveur via un tunnel VPN SSL.

- Avantages

- Tunnel entre deux FGT → Autorise des topologies Hub and spoke en VPN SSL.
 - Utile lorsqu'un tunnel IPsec ne peut être établi
 - Le protocole ESP est bloqué.
 - Les ports UDP 500 ou 4500 sont bloqués.
 - Problèmes de fragmentation IKE.

- Inconvénient

- Nécessite l'installation d'un certificat sur le FortiGate serveur.

Modes d'accès au VPN SSL

2. Mode Web-only

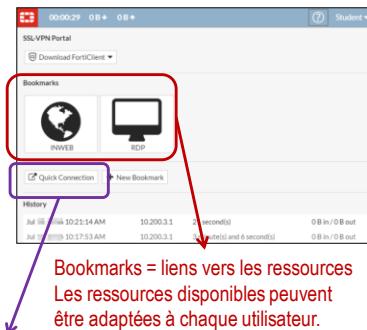
- L'utilisateur distant doit se connecter au portail VPN-SSL du FortiGate

- Une fois authentifié et connecté l'utilisateur a accès uniquement aux ressources disponibles via le portail.

- Soit via des bookmarks (liens).
- Soit via des widgets.

- Le portail va donner accès aux ressources en mode reverse proxy

- Pas un accès direct aux ressources.
- Supporte un nombre limité de protocoles
 - HTTP(S), FTP, SMB/CIFS, SSH,VNC, ping, RDP, citrix, Port Forward.
- Nécessite un navigateur Web et que la page du portail reste ouverte.



Le "Quick connection widget" permet d'entrer l'URL ou l'IP du serveur à joindre.

Configuration VPN SSL

• Étapes de configuration (FortiGate en serveur VPN SSL)

- Configurer les comptes utilisateur et les groupes

- Il faudra s'authentifier pour accéder au VPN.

- Configurer le portail-VPN (SSL VPN Portals)

- Nécessaire en mode Web-only.

- Configurer les paramètres de connexion au VPN (SSL VPN settings)

- Quel timeout, quelle authentification est requise, ...

- Créer une règle de pare-feu pour autoriser l'accès aux ressources

- Pour accepter et déchiffrer les paquets de l'interface VPN.

- Généralement pour permettre l'accès au réseau interne.

- (Optionnel) Créer une règle de pare-feu pour router le trafic vers Internet

- Lorsque le split tunneling est désactivé, une règle de pare-feu doit autoriser le trafic du client vers Internet en passant par l'UTM.

- L'UTM peut être utilisé pour appliquer des profils de sécurité.

Configurer les comptes utilisateur et les groupes

- **Authentification pour l'accès au VPN**
 - Authentifications supportées par le VPN SSL
 - Compte local.
 - Compte distant (LDAP, RADIUS, ...).
 - Authentification à un ou deux facteur (FortiToken + Login/mot de passe)
 - **Authentification FSSO non supportée**
 - L'authentification distante Fortinet Single Sign-On (FSSO) ne peut pas être utilisée pour l'authentification VPN.
 - **Rappel**
 - **Conflit par défaut : administration du FW et portail utilisent le port 443**
 - Uniquement si les deux utilisent le même port sur la même interface
 - En cas de conflit, seul le login au portail VPN SSL apparaîtra.

Configurer les comptes utilisateur et les groupes



1. Création d'un utilisateur local

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Local User
 Remote RADIUS User

✓ User Type > ✓ Login Credentials > 3 Contact Info > 4 Extra Info

User Name: _____
 Password: _____

✓ User Type > ✓ Login Credentials > ✓ Contact Info > 4 Extra Info

Email Address: _____
 SMS

✓ User Type > ✓ Login Credentials > ✓ Contact Info > 4 Extra Info

Enable
 Two-factor Authentication
 User Group: Click to add...

Paramétriser les comptes utilisateurs et les groupes.

- **Création d'un groupe d'utilisateurs**
 - Create new → donner un nom au groupe.
 - On assigne l'utilisateur voulu comme membre de ce groupe.



On définit si le groupe est local ou distant.

Configurer un portail Web

2. Configuration du portail

- Deux rubriques
 - Rubrique **SSL-VPN Portals**
 - Permet de configurer les portails.
 - Rubrique **SSL-VPN Settings**
 - Permet de configurer les paramètres du VPN SSL.
- Portails par défaut
 - Plusieurs portails sont déjà créés par défaut.



Name	Tunnel Mode	Web Mode
full-access	✓	✓
tunnel-access	✓	✗
web-access	✗	✓

Configurer un portail Web

- SSL-VPN Portals

- Portail

- Un portail est une page Web contenant des outils et des liens vers des ressources.
 - Les utilisateurs peuvent accéder aux ressources en utilisant ces outils et ces liens.

- Configuration d'un portail

- Un portail peut être paramétré pour

- Définir ce que l'utilisateur distant voit comme ressources disponibles.
 - Être lié à un utilisateur ou à un groupe d'utilisateurs spécifique afin qu'il n'ait accès qu'aux ressources requises.
 - Définir le mode d'accès : mode Web-only, mode tunnel ou les deux.
 - Fournir l'historique de connexion.
 - ...

- L'administrateur et l'utilisateur ont tous les deux la possibilité de personnaliser le portail VPN SSL



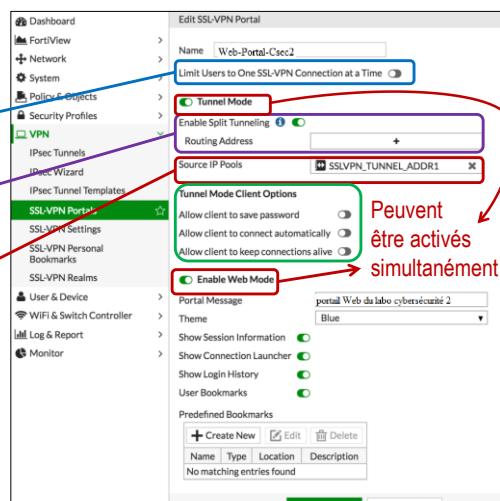
Configurer un portail Web

- SSL-VPN Portals

Empêche un utilisateur de se connecter depuis un autre PC avec les mêmes informations d'identification.

Si activé, il faut définir les réseaux qui seront accessibles via le VPN.

En mode tunnel, il faut renseigner les IP qui seront assignées aux adaptateurs virtuels sur les PC clients.



Configurer un portail Web

- SSL-VPN Portals

Permet l'autocomplétion du mot de passe lors de la prochaine connexion au VPN.

Lorsque FortiClient démarre, il tente automatiquement de se connecter au tunnel VPN.

FortiClient doit essayer de se reconnecter lorsqu'il détecte que la connexion VPN est interrompue de manière inattendue (càd pas déconnectée manuellement par l'utilisateur).

Tunnel Mode Client Options

- Allow client to save password
- Allow client to connect automatically
- Allow client to keep connections alive

Options qui peuvent être affichées sur le portail et que l'utilisateur pourra choisir d'utiliser.

Configurer un portail Web

- Configurer un portail Web

Affiche le nom de connexion de l'utilisateur, la durée de connexion de l'utilisateur et les statistiques de trafic entrant et sortant.

Affiche le widget Connection Launcher dans le portail Web.

<input checked="" type="radio"/> Enable Web Mode	portail Web du labo cybersécurité 2											
Portal Message	Blue											
Theme												
Show Session Information	<input checked="" type="checkbox"/>											
Show Connection Launcher	<input checked="" type="checkbox"/>											
Show Login History	<input checked="" type="checkbox"/>											
User Bookmarks	<input checked="" type="checkbox"/>											
Predefined Bookmarks	<table border="1"> <tr> <td>+ Create New</td> <td>Edit</td> <td>Delete</td> </tr> <tr> <td>Name</td> <td>Type</td> <td>Location</td> <td>Description</td> </tr> <tr> <td colspan="4">No matching entries found</td> </tr> </table>	+ Create New	Edit	Delete	Name	Type	Location	Description	No matching entries found			
+ Create New	Edit	Delete										
Name	Type	Location	Description									
No matching entries found												

Active la possibilité pour les utilisateurs de pouvoir créer leurs propres bookmarks.

Permet à l'administrateur de créer des bookmarks.

Configurer un portail Web

- Realms and bookmarks

- Configuration par défaut

- Par défaut, tous les utilisateurs verront le même portail : les mêmes signets, le même thème, ...

- Afficher les rubriques de configuration

- Les rubriques pour configurer d'autres signets et domaines sont masquées par défaut.

Permet de configurer des domaines VPN SSL afin d'apporter plus de flexibilité.

Permet à l'administrateur de surveiller et supprimer des bookmarks créés par les utilisateurs

Configurer un portail Web

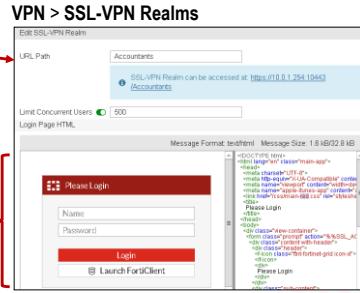
- Realms

- Les domaines sont des pages de connexion personnalisées

- Généralement pour des groupes d'utilisateurs mais possible aussi pour un utilisateur unique.

- Donnent accès à différents portails en fonction de l'URL saisie par l'utilisateur

- Par exemple, vous pouvez créer des portails différents selon les départements
 - <https://10.0.1.254:/marketing>
 - <https://10.0.1.254:/accountants>
 - <https://10.0.1.254:/administratif>



HEH.be
Sciences
et technologies

Configurer un portail Web

- **Bookmarks**
 - Ce sont des liens vers des ressources réseau
 - Ils sont affichés dans le portail.
 - Une fois connecté sur le portail, l'utilisateur n'a plus qu'à cliquer sur le lien pour lancer l'application souhaitée.
 - **Predefined Bookmarks**
 - Permet à l'administrateur de créer des signets pour les utilisateurs.

VPN > SSL-VPN Portals

Wallonie-Bruxelles
ENSEIGNEMENT

310

HEH.be
Sciences
et technologies

Configurer un portail Web

- **Bookmarks (suite)**
 - Une fois le signet créé par l'administrateur
 - Il est affiché dans la page de configuration.

→ Il est visible sur le portail.

Wallonie-Bruxelles
ENSEIGNEMENT

311

Configurer un portail Web

- Bookmarks (suite)

- User Bookmarks

- Donner la possibilité aux utilisateurs de pouvoir créer leurs propres book
 - L'option User Bookmarks doit être activée dans VPN > SSL-VPN Portals.

Nécessite une certaine connaissance informatique de la part de l'utilisateur.

The screenshot shows the HEH.be SSL-VPN Portal interface. On the left, there's a sidebar with icons for 'Wallonie-Bruxelles Enseignement' and 'DÉ Pro'. The main area has a 'My Bookmarks' section with 'Add' and 'Edit' buttons. A red arrow points from this section to a detailed 'My bookmarks' dialog box. This dialog box shows a form for adding a bookmark with fields for 'Name', 'Type' (set to 'HTTP/HTTPS'), 'Location', 'Description', and 'SSO'. It also lists existing protocols: FTP, RDP, SMB/CIFS, TELNET, VNC, RDP Native, and Port Forward. Buttons for 'OK' and 'Cancel' are at the bottom. To the right of the dialog, a large red bracket groups it with another red bracket enclosing the 'User Bookmarks' checkbox in the top right corner of the main portal header. Below the dialog, a text box states: 'L'utilisateur doit savoir quel protocole choisir en fonction de la ressource à atteindre.' (The user must know which protocol to choose based on the resource to be reached.)

– Suppression de bookmarks indésirables
Permet à l'administrateur de surveiller et supprimer des Bookmarks indésirables créés par les utilisateurs.

A red box highlights the 'SSL-VPN Personal Bookmarks' link in the sidebar menu. The bottom right corner shows a navigation bar with three dots and the number '312'.

Configurer un portail Web

- Exemple de portail

The screenshot shows the HEH.be SSL-VPN Portal interface. At the top, there's a 'Student' dropdown and a 'Download FortiClient' button with a dropdown menu for iOS, Android, Windows, and Mac. The main area has sections for 'Bookmarks' (Windows icon) and 'Your Bookmarks' (Internal server icon). A red box highlights the 'Quick Connection' button in the 'Your Bookmarks' section. Another red arrow points from this button to a 'Quick Connection' dialog box. This dialog box has tabs for 'HTTP/HTTPS', 'FTP', 'SMB/CIFS', 'RDP', 'VNC', 'Citrix', 'SSH', 'Telnet', 'Port Forward', and 'Ping'. It includes fields for 'URL', 'Launch', and 'Cancel'. Below the dialog, a 'History' table shows connection logs for two dates: Jul 11, 2016 10:41:23 AM and Jul 11, 2016 10:35:05 AM. The bottom right corner shows a navigation bar with three dots and the number '313'.

HEH.be
Sciences
et technologies

Configurer un portail Web

- Exemple de portail

Session Information

Time Logged In: test (0 hour(s), 0 minute(s), 0 second(s))
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Login History

Time	Time Logged In	Inbound/Outbound Traffic
23/1/2016 23:19:05	8 Seconds	0 B / 0 B

Connection tool

Type: HTTP/HTTPS Host: Go

FortiClient Download

My Bookmarks

Add Edit

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

314

HEH.be
Sciences
et technologies

Configurer un portail Web

- Exemple de portail
 - Si le mode tunnel a été activé, on retrouve une rubrique "Tunnel Mode" sur le portail.

Session Information

Time Logged In: test (0 hour(s), 0 minute(s), 0 second(s))
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes

Tunnel Mode

Login History

Time	Time Logged In	Inbound/Outbound Traffic
26/1/2016 20:53:07	38 Seconds	0 B / 0 B

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

315

HEH.be Sciences et technologies

Configurer les paramètres de connexion

3. SSL-VPN Settings

Interface(s) qui fournit un portail de connexion VPN SSL.

Modifier le port de gestion pour éviter les conflit avec le portail.

Le portail SSL VPN présente un certificat numérique pour prouver son identité aux utilisateurs qui se connectent.

Le FortiGate peut authentifier le client en lui imposant de fournir son certificat.

SSL-VPN Portals
SSL-VPN Settings

Connection Settings

- Listen on Interface(s): any
- Listen on Port: 443
- Restrict Access: Allow access from any host
- Idle Logout: Inactive For: 300 Seconds
- Server Certificate: certificate-fortidemo
- Require Client Certificate: off

Par défaut, le certificat présenté est auto-signé.

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
[Click here to learn more](#)

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

HEH.be Sciences et technologies

Configurer les paramètres de connexion

- Connection Settings
 - Restrict Access
 - Permet de restreindre l'accès à certains hôtes spécifiques
 - Tous les utilisateurs n'ont pas nécessairement besoin de se connecter en VPN SSL.
 - On peut refuser l'accès pour des raisons de sécurité (par ex. sur base géographique).
 - Ces hôtes doivent avoir été définis dans Policy & Objects

SSL-VPN Settings

Connection Settings

- Listen on Interface(s): any
- Listen on Port: 4430
- Restrict Access: Allow access from any host
- Hosts: all (highlighted)
- Idle Logout: Inactive For: 300 Seconds
- Server Certificate: certificate-fortidemo
- Require Client Certificate: off

Limit access to specific hosts

Liste des hôtes autorisés. Vide par défaut.

Select Entries

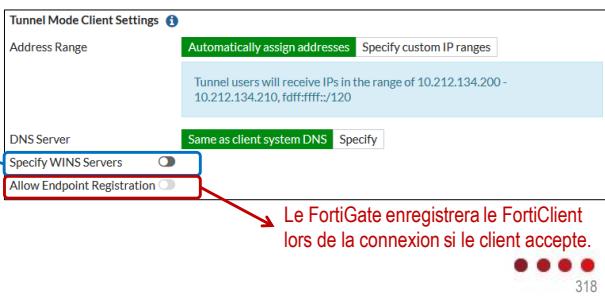
- ADDRESS (31)
 - *.live.com
 - Adobe Login
 - Gotomeeting
 - SSLVPN_TUNNEL_ADDR1
 - Windows update 2
 - adobe
 - all
 - android
 - apple
 - appstore

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

Configurer les paramètres de connexion

- Tunnel mode client settings
 - Address Range
 - Défini quelles adresses seront données aux clients qui vont se connecter.
 - L'étendue d'IP va définir le nombre d'utilisateurs qui pourront se connecter simultanément.
 - DNS Server
 - Adresse du serveur DNS qui sera donné au client lorsque le mode tunnel est activé.
 - Généralement utilisé si le split tunneling est désactivé.

Permet de définir l'adresse d'un serveur WINS à fournir aux clients.



Configurer les paramètres de connexion

- Authentication/Portal Mapping
 - Création de règles
 - Elles permettent d'associer un portail et/ou un domaine à des utilisateurs/groupes.
 - Seuls les utilisateurs/groupes spécifiés auront accès à ce portail.
 - All Other Users/Groups
 - Règle par défaut qui s'applique au domaine racine.
 - Permet de définir un portail qui ne contient que de l'information (pas d'accès à des ressources) à destination des utilisateurs qui ne sont pas associé à un portail.
 - La règle ne peut pas être supprimée.

The screenshot shows the 'Authentication/Portal Mapping' configuration page. It includes sections for 'Create New', 'Edit', and 'Delete'. The 'Users/Groups' column lists 'Accountants' and 'Teachers', while the 'Realm' and 'Portal' columns show '/Accountants' and '/Teachers' respectively, both mapped to 'full-access' and 'tunnel-access' respectively. A red box highlights the 'All Other Users/Groups' row, which is mapped to 'Global-portal'. A red arrow points from the 'All Other Users/Groups' row to the text 'La règle ne peut pas être supprimée.'. There are three red dots at the bottom right.

HEH.be
Sciences
et technologies

Configurer les paramètres de connexion

- Fin de la configuration
 - Message WARNING 1
 - Certificat autosigné
 - Avec un certificat autosigné, l'utilisateur qui essaiera de se connecter sur le portail VPN SSL avec un navigateur Web va recevoir un avertissement.
 - Message d'avertissement
 - Si l'on n'utilise pas de certificat numérique signé par une autorité de certification (CA) connue, le FortiGate s'en rend compte et demande une confirmation.

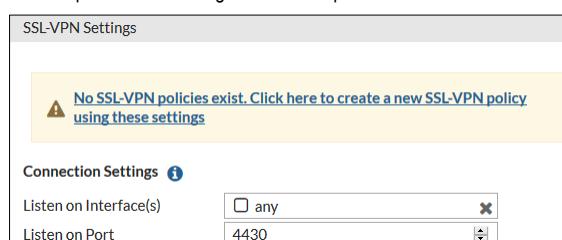
WALLONIE-BRUXELLES
ENSEIGNEMENT

Pro
Présage

320

HEH.be
Sciences
et technologies

Configurer les paramètres de connexion

- Fin de la configuration (suite)
 - Message WARNING 2
 - Configuration incomplète
 - Le FortiGate nous signale que la configuration n'est pas finie.
 - Il reste à paramétriser une règle de sécurité pour l'accès aux ressources.

WALLONIE-BRUXELLES
ENSEIGNEMENT

Pro
Présage

321

Créer les règles de pare-feu

4. Autoriser l'accès aux ressources internes

Généralement, on utilise le VPN SSL pour les utilisateurs nomades, donc à l'extérieur de l'entreprise. Les paquets vont dès lors arriver (incoming) via l'interface externe. Le trafic VPN SSL utilise une interface virtuelle nommée "ssl.<vdom_name>"

L'interface de sortie correspond à une interface interne : c'est en interne que se trouvent les ressources auxquelles on veut donner l'accès. Ici, *Internal* est un alias.

Les utilisateurs nomades pourraient se connecter de n'importe où, donc avec n'importe quelle adresse. Dans cet exemple, on autorise n'importe quelle IP : all. Les utilisateurs/groupes autorisés doivent être ajoutés.

Le NAT est à désactiver puisque l'on configure un VPN afin d'avoir un accès "local" aux ressources.

Edit Policy

Name: SSLVPN

Incoming Interface: SSL-VPN tunnel interface (ssl.root)

Outgoing Interface: Internal

Source: all, Training_One, Training_Two

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options

NAT: OFF

Créer les règles de pare-feu

5. Autoriser l'accès à Internet

- Une autre règle est nécessaire pour permettre l'accès à Internet lorsque le split tunneling est désactivé.

Le trafic VPN SSL arrive sur l'interface virtuelle.

Interface connectée à Internet

On ne connaît pas toutes les adresses sur Internet → All

Edit Policy

Name: Internet_policy

Incoming Interface: SSL-VPN tunnel interface (ssl.root)

Outgoing Interface: port1

Source: all, Training_One, Training_Two

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options

NAT: ON

Créer des règles de sécurité

- Configurer les profils de sécurité
 - Le cas échéant, configurer et activer les fonctions de sécurité de l'UTM

Security Profiles

OFF / AntiVirus	default
OFF / Web Filter	default
OFF / Application Control	default
OFF / IPS	default
OFF / SSL/SSH Inspection	certificate-inspection

Traffic Shaping

OFF / Shared Shaper	guarantee-100kbps
OFF / Reverse Shaper	guarantee-100kbps
OFF / Per-IP Shaper	Click to set...

Configurer les paramètres de connexion

- FortiGate en tant que client SSL-VPN
 - Importer le certificat pour l'authentification.
 - Créer une interface de type tunnel (Network > Interface > Create new).
 - Configurer les paramètres client VPN SSL (VPN > SSL-VPN client).
 - Créer la règle de pare-feu.

FortiGate distant configuré en serveur VPN-SSL

Utilisateur local et certificat local (identifie ce client auprès du serveur)

La route statique ajoutée vers le réseau distant aura cette distance et cette priorité

Edit SSL-VPN Client

Name	SSLClienttoHQ
Interface	sslclient_port
Server	10.200.1.1
Port	10443
Username	clientfortigate
Pre-shared Key	*****
Client Certificate	pk1
Peer	10.200.1.1
Administrative Distance	10
Priority	0
Status	Enabled
Comments	0/255

OK Cancel

Accélération matérielle

- **Hardware Acceleration for SSL-VPN**
 - Activer ou désactiver l'accélération matérielle
 - Par défaut, le trafic SSL-VPN est déchargé vers des processeurs CP8 ou CP9.
 - Uniquement sur les modèles disposant de processeurs CP8 ou CP9.

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

- Afficher le status de l'accélération matérielle

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

Acceleration hardware detected:
kxp=on cipher=on

No acceleration hardware
detected

Renforcer la sécurité des accès au VPN

- **Client Integrity Checking (mode tunnel uniquement)**
 - Le FortiGate vérifie l'intégrité du client
 - Déetecte, sur la machine cliente, les applications de sécurité reconnues par le centre de sécurité Windows (A-V et FW).
 - Donc uniquement compatible avec les clients Microsoft Windows.
 - Vérification de l'état des applications
 - » Actif/inactif, numéro de version, signatures à jour.
 - Custom Host Check
 - La vérification de l'état d'autres applications est possible via l'identificateur global unique (GUID) dans le registre de configuration de Windows.
 - **Caractéristiques**
 - Le Client Integrity Check a lieu juste après la phase d'authentification.
 - Si la vérification échoue, la connexion VPN est refusée.
 - La vérification peut être activée séparément pour chaque portail.
 - Compatible avec le mode Web et le mode tunnel.

- Client Integrity Checking (cont.)
 - Inconvénient
 - Peu générer une charge de travail supplémentaire aux administrateurs
 - Tous les logiciels des PC clients doivent être à jour.
 - Nécessite une bonne connaissance du fonctionnement des OS Windows
 - Les mises à jour logicielles peuvent entraîner une modification des valeurs de la clé de registre empêchant les utilisateurs de se connecter au VPN.
 - Client Integrity Checking configuration
 - L'activation et la configuration se font uniquement en CLI.

```
#config vpn ssl web portal
  edit <portal_name>
    set host-check {none | av | fw | av-fw | custom}
    set host-check-interval <seconds>
  end
```

- Client Integrity Checking configuration
 - On entre dans le menu correspondant au portail web VPN SSL

```
Connected
FGVM040000052157 # config vpn ssl web portal
FGVM040000052157 (portal) # edit
name  Portal name.
full-access
tunnel-access
web-access
FGVM040000052157 (portal) # edit web-access
FGVM040000052157 (web-access) #
```

- On peut alors choisir ce que l'on souhaite que le FortiGate vérifie

<pre>FGVM040000052157 (web-access) # set host-check none none av av fw fw av-fw av-fw custom custom</pre>	<pre>FGVM040000052157 (web-access) # set host-check av FGVM040000052157 (web-access) # end</pre>
---	--

- Client Integrity Checking

- Afficher la liste des logiciels de sécurité compatibles

```
FGT# config vpn ssl web host-check-software
show
edit "FortiClient-AV-Vista-Win7"
    set guid "005610A0-2206-700L-3FB9-7E98B93F91F9"
next
edit "FortiClient-FW-Vista-Win7"
    set type fw
    set guid "006D9983-6839-71D6-14E6-D7AD47ECD682"
next
edit "AVG-Internet-Security-AV"
    set guid "1/DDDU97-3err-435r-9E1B-52D74245D6BF"
next
edit "AVG-Internet-Security-FW"
    set type fw
    set guid "8DECF618-9569-4340-B3BA-D78D28969B66"
next
edit "Kaspersky-AV"
    set guid "2C4D4BC6-0793-4956-A9F9-E252435469C0"
--More-- ■
```

- Autres options de sécurité

- Require Client Certificate

- Obligation pour les clients de fournir un certificat.

- Imposer Forticlient

- Impose aux utilisateurs d'installer Forticlient pour continuer.
- Les utilisateurs ont la possibilité, via de portail, de télécharger le logiciel Forticlient
 - Ils peuvent ainsi l'installer avant de poursuivre le processus d'authentification et de connexion au VPN SSL.

- Imposer l'authentification à deux facteurs

Connection Settings ⓘ

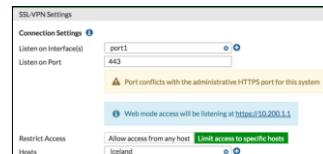
Require Client Certificate

Renforcer la sécurité des accès au VPN

- Autres options de sécurité

- Autoriser uniquement certaines adresses IP
 - Voir l'option "Restrict Access" dans la rubrique "Connection Settings".

```
config vpn ssl setting
  set source-address <name1>, <name2>, ...
end
```



- Refuser certaines adresses IP (CLI only)

```
config vpn ssl setting
  set source-address-negate [enable|disable]
  set source-address6-negate [enable|disable]
end
```

Renforcer la sécurité des accès au VPN

- Minuteurs SSL-VPN

- Problèmes de déconnexion

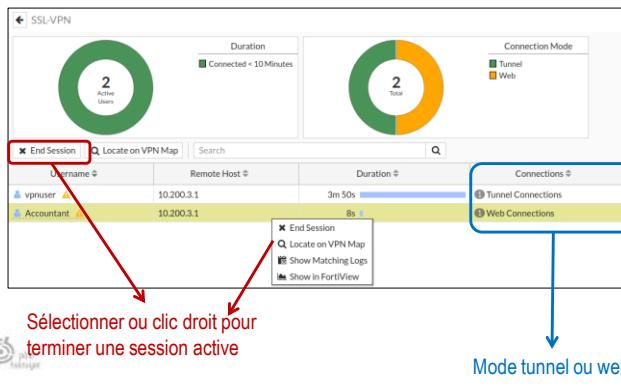
- Si la latence est importante sur le réseau, FortiGate peut déconnecter le client
 - Le minuteur pourrait expirer avant que l'utilisateur ne puisse terminer les processus de négociation (Temps de résolution DNS, temps pour entrer un token, ...).

```
config vpn ssl settings
set login-timeout <10-180> → Remplace "hard timeout"
set dtls-hello-timeout <10-60> → Datagram Transport Layer Security
set http-request-header-timeout <1-60> Le VPN SSL utilise UDP au lieu de TCP
Set http-request-body-timeout <1-60> Peut permettre d'améliorer le débit
end
```

Permet d'atténuer les attaques DoS causées par des requêtes HTTP partielles

Montrer les sessions VPN SSL

- Dashboard > Network > SSL VPN
 - Permet de vérifier quel utilisateur d'un VPN SSL est connecté ainsi que l'état du tunnel.
 - Les logs sont affichés dans Log & Report > System Events.



Montrer les sessions VPN SSL

- Déconnexion VPN
 - La session d'authentification de la règle de pare-feu est associée à la session du tunnel VPN SSL
 - Lorsqu'un VPN SSL est déconnecté toutes les sessions associées dans la table de sessions sont supprimées.
 - Peu importe que la déconnexion ait lieu par l'utilisateur ou via le paramètre d'inactivité du VPN SSL (Idle timeout).
 - Cela empêche la réutilisation des sessions VPN SSL authentifiées.

VPN > SSL-VPN Settings

Redirect HTTP to SSL-VPN	<input checked="" type="checkbox"/>
Restrict Access	<input type="radio"/> Allow access from any host <input type="radio"/> Limit access
Idle Logout	<input checked="" type="radio"/>
Inactive For	300 Seconds
Server Certificate	Fortinet_Factory

```
config vpn ssl settings
  set idle-timeout <0-259200>
end
```

HEH.be
Sciences
et technologies

Montrer les sessions VPN SSL

- SSL-VPN logs
 - Permet de vérifier quel utilisateur d'un VPN SSL est connecté

#	Date/Time	Level	Action	Status	Message
1	05:33:20	[redacted]	ssl-new-con		SSL new connection
2	05:33:19	[redacted]	tunnel-down		SSL tunnel shutdown
3	05:33:19	[redacted]	tunnel-down		SSL tunnel shutdown
4	05:28:27	[redacted]	tunnel-up		SSL tunnel established
5	05:28:27	[redacted]	ssl-new-con		SSL new connection

Affiche les demandes de connexion et si le VPN est ouvert ou fermé

#	Date/Time	Level	User	Action	Message	Group
1	05:33:19	[redacted]	student	authentication	User student succeeded in logout	SSL_VPN_USERS

Affiche les informations relatives à l'authentification des utilisateurs

#	Date/Time	Level	User	Action	Message
1	05:33:19	[redacted]	student	authentication	User student succeeded in logout

Affiche les connexions établies ou fermées via FortiClient

#	Date/Time	Level	User	Action	Message
1	05:33:19	[redacted]	student	close	Close a FortiClient Connection.
2	05:28:27	[redacted]	student	add	Add a FortiClient Connection.

• • • 336

HEH.be
Sciences
et technologies

Chapitre 8

Intrusion Prevention System

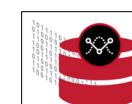
• • • 337

Objectifs

- **A l'issue de ce chapitre, l'apprenant doit être capable de**
 - Protéger un réseau contre les attaques connues en utilisant les signatures IPS.
 - Protéger un réseau contre des "anomalies" telles que du trafic inhabituel ou des paquets mal formés.
 - Protéger un réseau contre des attaques DoS.
 - Protéger les services Web à l'aide de profils WAF (Web Application Firewall).
 - Configurer un FortiGate pour inspecter le trafic réseau hors ligne (IDS).

Introduction

- **IDS : Intrusion Detection System**
 - Analyse l'activité d'un réseau (NIDS) ou d'un hôte (HIPS)
 - Pour y détecter des exploits
 - Attaques connues (Il existe des signatures).
 - Pour y détecter des anomalies
 - Erreurs de protocoles, trafic anormal (DoS, ...), attaque zero-day.
 - De manière passive
 - Aucune action directe sur le trafic, l'IDS est offline.
 - Collecte des informations
 - Par exemple via l'enregistrement de tout le trafic ou uniquement du trafic concernant une attaque.
 - Le HIDS est donc indispensable dans une optique de traçabilité d'attaque
 - Alerte les administrateurs
 - L'IDS n'agit pas sur le trafic
 - Le trafic malicieux peut pénétrer dans le réseau.
 - L'administrateur doit réagir à postériori.
 - L'IDS peut cependant faire appel à un FW pour que celui-ci bloque le trafic



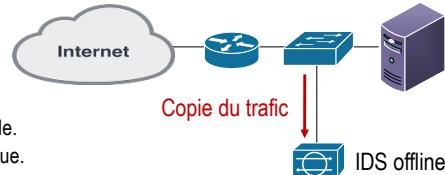
Introduction

- **IDS : Intrusion Detection System**

- **Avantages des IDS (si offline)**

- **Pas d'impact sur le réseau**

- Ni en cas de panne d'une sonde.
 - Ni en cas de surcharge d'une sonde.
 - N'introduit pas de latence ni de gigue.



- **Inconvénients des IDS**

- **Ne peut pas être totalement automatisé**

- La configuration et l'administration des IDS nécessitent beaucoup de temps et de connaissances (analyse des logs).

- **Nécessite du personnel compétent**

- L'exploitation des remontées d'alertes nécessite des connaissances pointues.
 - Quelle mesure prendre ? Comment distinguer un faux-positif d'un véritable incident de sécurité ? Etc.

- **Vulnérable à certaines techniques d'évasion**

Introduction

- **IPS : Intrusion Prevention System**

- **Si un IDS peut détecter une intrusion, alors pourquoi ne pas la bloquer?**

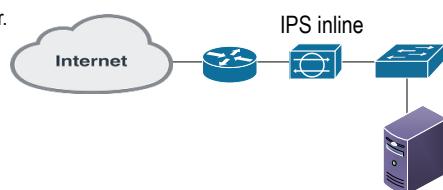
- **Techniquement, un IPS est un IDS qui ajoute des fonctionnalités de blocage**

- Aucun paquet ne peut pénétrer dans le réseau sans avoir été analysé par l'IPS.
 - *Inline mode* :

- » L'IPS doit être sur le chemin du trafic.

- **L'IPS est actif, il peut agir sur le trafic**

- Empêcher les paquets de passer.
 - Interrompre une connexion.
 - Ralentir une connexion.
 - Bloquer les sources.
 - ...



Introduction

- **IPS : Intrusion Prevention System**
 - **Avantages des IPS**
 - Contrairement à un IDS, les attaques sont bloquées immédiatement.
 - Permet de bloquer d'autres types d'attaques que l'antivirus.
 - Permet de créer des règles pour protéger les systèmes vulnérables, le temps que des correctifs de sécurité soient distribués.
 - **Inconvénients des IPS**
 - **Possibilité de nombreux faux-positifs**
 - Un faux-positif est un paquet ou message injustement considéré comme nuisible.
 - De nombreux paquets sains peuvent ainsi être bloqués.
 - **Possibilité d'impacts négatifs sur le réseau**
 - Paralyser le réseau si l'IPS ne fonctionne plus.
 - Introduire de la latence et de la gigue sur le réseau si l'IPS est mal dimensionné.
 - Bloquer du trafic légitime à cause des faux-positifs.

Introduction

- **Stream normalization**
 - **Normalisation de flux**
 - Ensemble de techniques utilisées pour réduire ou éliminer des tentatives d'évasion ou d'insertion
 - Les IPS doivent être *inline* pour pouvoir utiliser la normalisation de flux.
 - **Exemples**
 - TCP normalization
 - » Mauvais checksum.
 - » Mauvaises longueurs de Payload.
 - » Drapeaux TCP suspects (NULL, SYN/FIN, ...).
 - IP Normalization
 - » Vérification de la fragmentation (un paquet dépasse le MTU).
 - » Vérification ICMP (Echo-reply sans echo-request préalable, ...).
 - ...

- **IPS FortiGate**
 - Peut détecter des attaques connues
 - Un trafic ou un fichier correspond à une signature
 - Les signatures sont régulièrement mises à jour par le service Fortiguard.
 - Peut détecter des anomalies
 - DéTECTé par l'analyse comportementale
 - Signatures IPS basées sur des taux.
 - Règles spécifique contre du DoS.
 - Inspection du protocole.
 - Exemples :
 - Quantité de trafic anormalement élevé (DoS/flood) par rapport à la ligne de base.
 - Utilisation anormale du protocole (drapeau SYN et RST en même temps).

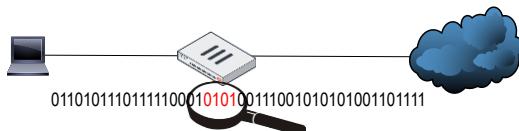
1. IPS engine

- Le moteur IPS intervient dans de nombreuses fonctionnalités sur le FortiGate
 - Contrôle des applications.
 - Protection antivirus (flow based).
 - Filtrage Web (flow based).
 - Filtrage des e-mails (flow based).
 - Data Leak Prevention (flow based).

Le moteur IPS n'est pas exclusivement utilisé pour la fonction IPS.

2. Protocol decoders

- Décodeurs de protocoles (ou analyseur de protocoles)
 - 1. L'IPS analyse le paquet et détecte le protocole utilisé.
 - 2. Il utilise automatiquement le décodeur correspondant pour analyser chaque paquet selon les spécifications du protocole.
 - 3. Il détecte les paquets/commandes mal formés ou qui ne respectent pas les spécifications du protocole.
 - Par exemple trop d'en-têtes HTTP ou une tentative de buffer overflow.



3. Bases de données de signatures

- Regular signatures database
 - Base de données réduite reprenant des signatures d'attaques classiques
 - Inclue par défaut dans chaque version du firmware FortiGate.
 - Provoquent rarement de faux positifs.
 - L'action par défaut est le blocage (Default action = Block)
- Extended signature database
 - La base de données de signatures étendue contient des signatures supplémentaires
 - Disponible uniquement pour les FortiGate ayant suffisamment d'espace disque ou de RAM.
 - Ces signatures peuvent plus facilement générer des faux positifs.
 - Plutôt utilisée pour les réseaux nécessitant une plus haute sécurité

HEH.be Sciences et technologies

IPS Package

- Mises à jour
 - Les mises à jour permettent d'inclure automatiquement de nouvelles signatures
 - Nécessite un abonnement au service Fortiguard IPS.
 - Les décodeurs sont également mis à jour
 - Assez rare, par exemple en cas de modification des RFC ou des spécifications d'un protocole.
 - Le moteur IPS est lui-aussi mis à jour
- Choisir la base de données de signatures
 - System > FortiGuard



WALLONIE-BRUXELLES
ENSEIGNEMENT

DU
PROFESSIONNEL

348

HEH.be Sciences et technologies

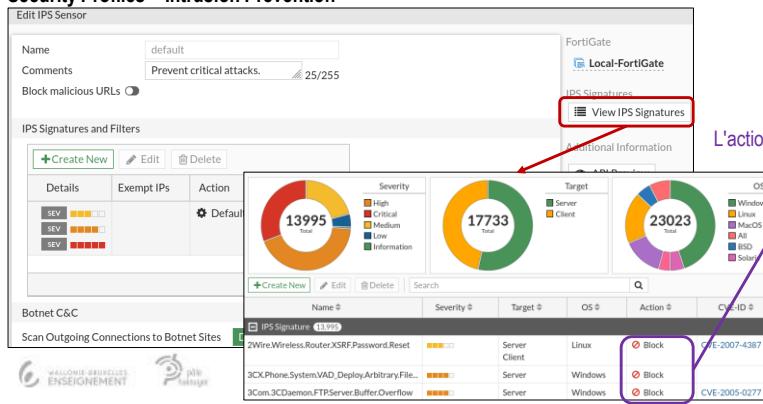
IPS Package

- Listes des signatures IPS

L'action par défaut est généralement correcte mais peut être modifiée ou la signature supprimée :

- Si une application "maison" déclenche une signature IPS.
- Si un correctif de sécurité bloque un exploit, il n'est plus utile de continuer à rechercher cet exploit.

Security Profiles > Intrusion Prevention



WALLONIE-BRUXELLES
ENSEIGNEMENT

DU
PROFESSIONNEL

L'action peut être modifiée

349

HEH.be
Sciences
et technologies

Ressources Fortiguard

- Encyclopédie FortiGuard
 - Disponible sur le site Web Fortiguard
 - Contient des renseignements utiles comme les systèmes touchés et les mesures correctives recommandées.

The screenshot shows a detailed view of a vulnerability entry in the FortiGuard Encyclopedia. The entry is for "Vulnerability: WordPress.Shortcode.Tags.XSS". It includes sections for Info (Last Updated: March 1, 2016, Severity: High, Impact: System Compromise - Remote attackers can execute arbitrary script code on vulnerable systems, Coverage: IPS (Regular DB), VCM, Update History: 2016-03-02, Version: 8.804, Detail: Released), Description (explains the XSS vulnerability), Affected Products (WordPress versions 4.3 and earlier), and Recommended Actions (apply the most recent upgrade or patch from the vendor). To the right, there are links to the FortiGuard Encyclopedia, Live Threat Monitor, and Free Tools like FortiClient and Online Virus Scan. The bottom right corner shows a navigation bar with three dots and the number 350.

HEH.be
Sciences
et technologies

Custom IPS Signatures

- Signatures personnalisées
 - Il est possible de créer ses propres signatures

Syntaxe :

F-SBID (--KEYWORD VALUE ; --KEYWORD VALUE ;)

Mots-clés spécifiques au protocole.
Défini dans quelle partie du paquet rechercher une correspondance

En-tête

Toutes les signatures personnalisées commencent par F-SBID

Valeur pour laquelle il y aura une correspondance.

Opérateurs utilisables
=, !=, >=, <=, &, |, ^, in

Chaque paire mot-clé/valeur se termine par un point-virgule et un espace

The diagram illustrates the syntax for custom IPS signatures. It shows the structure: F-SBID (--KEYWORD VALUE ; --KEYWORD VALUE ;). Annotations explain: "En-tête" points to the first part before the first parenthesis; "Toutes les signatures personnalisées commencent par F-SBID" points to the start of the structure; "Mots-clés spécifiques au protocole. Défini dans quelle partie du paquet rechercher une correspondance" points to the first KEYWORD; "Valeur pour laquelle il y aura une correspondance." points to the first VALUE; and "Opérateurs utilisables =, !=, >=, <=, &, |, ^, in" is enclosed in a green box. Red arrows point from the text annotations to their corresponding parts in the syntax string. The bottom right corner shows a navigation bar with three dots and the number 351.

- **Les sondes IPS**

- **Les signatures IPS**

- Elles contiennent des paramètres (valeurs, mots clés)
 - Ces paramètres peuvent être comparés au contenu des paquets reçus à la recherche d'une correspondance.

- **Les filtres IPS**

- Ils regroupent un ensemble de signatures
 - Permettent de fournir différents niveaux de protection selon les signatures incluses.
 - Ils peuvent être personnalisés
 - Plus un filtre sera précis, moins il consommera de ressources pour analyser le trafic.

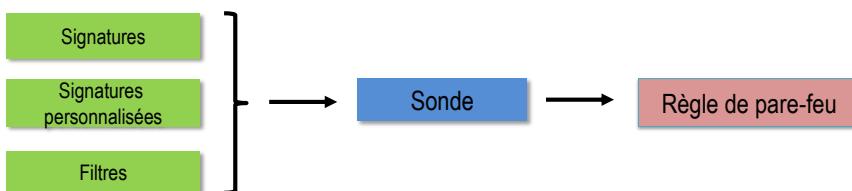
- **Les sondes IPS**

- Elles regroupent des filtres et/ou des signatures individuelles.
 - Elles sont chargées d'analyser le trafic réseau :
 - Par rapport aux signatures et filtres paramétrés.
 - Pour y détecter des tentatives d'intrusion, des paquets mal formés ou des attaques DoS.

- **Les sondes IPS (suite)**

- **Remarque**

- Si la signature qui correspond au trafic se trouve à la fois dans la liste des signatures IPS et dans la liste des filtres IPS, FortiGate applique l'action spécifiée dans la liste des signatures.



- **Les options de filtres**

- **Le minuteur « hold time »**

- Permet de définir la durée pendant laquelle les signatures sont maintenues avec l'action « Monitor » après une mise à jour de signature FortiGuard IPS.
 - L'action par défaut des nouvelles signatures est activée à l'expiration du minuteur, afin d'éviter les faux positifs.
 - Configurable entre 0 jour et 0 heure (par défaut) et 7 jours.

```
# config system ips
  set signature-hold-time 3d12h
  set override-signature-hold-by-id enable
end
```

- **Fichiers journaux**

- Les logs renseignent si le minuteur est actif.

```
date=2021-04-06 time=00:00:57 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="vd1" eventtime=1278399657778481842 tz="-0700"
severity="info" srcip=10.1.100.22 srccountry="Reserved" dstip=172.16.200.55
srcintf="port13" srcintfrole="undefined" dstintf="port14" dstintfrole="undefined"
sessionid=3620 action="detected" proto=6 service="HTTP" policyid=1
attack="Eicar.Virus.Test.File" srcport=52170 dstport=80 hostname="172.16.200.55"
url="/virus/eicar" direction="incoming" attackid=29844 profile="test"
ref="http://www.fortinet.com/ids/VID29844" incidentserialno=25165825 msg="file_transfer:
Eicar.Virus.Test.File, (signature is on hold)"
```

354

- **Les options de filtres**

- **CVE (Common Vulnerabilities and Exposures)**

- CVE est une liste publique des informations relatives aux vulnérabilités de sécurité informatique.
 - Fournit un descriptif succinct de chaque vulnérabilité.
 - Fournit un ensemble de liens pour plus d'informations.
 - Il est maintenu par l'organisme à but non lucratif MITRE.
 - <https://www.cve.mitre.org>
 - Aident les professionnels
 - A coordonner leurs efforts visant à hiérarchiser et résoudre les vulnérabilités.

- **Format : CVE-AAAA-NNNN**

- AAAA = l'année de publication.
 - NNNN = un numéro d'identification unique.

- Les options de filtres (suite)

- Exemple de CVE

- La vulnérabilité qui a permis une attaque massive par le ransomware WannaCry.
 - A l'origine de l'arrêt des lignes de production de Renault. Plus 200.000 ordinateurs ont été impactés dans environ 100 pays.

CVE-ID

CVE-2017-0144 [Learn more at National Vulnerability Database \(NVD\)](#)

CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The SMB1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:96704
- URL:<http://www.securityfocus.com/bid/96704>
- CONFIRM:<https://cert-portal.siemens.com/productcert/cert/odt/ssa-701903.pdf>
- CONFIRM:<https://cert-portal.siemens.com/productcert/cert/odt/ssa-966341.pdf>
- CONFIRM:<https://portals.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144>
- EXPLOIT-DB:41891
- URL:<https://www.exploit-db.com/exploits/41891/>
- EXPLOIT-DB:41987
- URL:<https://www.exploit-db.com/exploits/41987/>
- EXPLOIT-DB:42030

• • • 356

- Les options de filtres (suite)

- L'option « CVE Pattern »

- Permet de filtrer les signatures IPS sur la base des ID CVE ou sur un ensemble de CVE (CVE wildcard).
 - Facilite l'utilisation des CVE : toutes les signatures marquées avec ce CVE sont automatiquement incluses.

- Exemple

```
# config ips sensor
edit "cve"
set comment "cve"
config entries
edit 1
set cve "cve-2010-0177"
set status enable
set log-packet enable
set action block
next
end
```

• • • 357

HEH.be Sciences et technologies

IPS sensors

- Ajouter des signatures à une sonde IPS
Sélectionner les signatures individuellement

Security Profiles > Intrusion Prevention > Create new

Add Signatures

Type: Default Action: Enable Status: Enable

Rate-based settings: Threshold: 0 Duration (seconds): 60 Track By: Any Source IP Destination IP Exempt IPs: 0 Edit IP Exemptions

Créer un filtre

Paramètres appliqués aux signatures listées ci-dessous.

Une fois ajoutée, il est possible de modifier l'action associée à une signature.

Selected All

Packet Logging

358

HEH.be Sciences et technologies

IPS sensors

- Les règles sont lues dans l'ordre
 - Si possible, placer les règles les plus utilisées en premier.
 - Ne pas utiliser de trop gros filtres ni trop de filtres (consommation de ressources).

Security Profiles > Intrusion Prevention

New IPS Sensor

Name: Server IPS Profile Comments: Write a comment... 0/255

Block malicious URLs:

IPS Signatures and Filters

Create New		Edit	Delete	Exempt IPs	Action	Packet Logging
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	0	<input checked="" type="radio"/> Monitor	<input type="radio"/> Disabled	<input checked="" type="radio"/> Default	<input type="radio"/> Disabled	
TGT Server						
SEV ■■■■■						
SEV ■■■■■						
OS Windows						

Possible d'exempter certaines adresses source ou destination (analyse faux positifs)

Edit IP Exemptions

Create New Delete

Source IP/Netmask: 10.0.1.10/32 Destination IP/Netmask: 0.0.0.0/0

359

Rate Based Signatures

- Les signatures basées sur les taux/seuils
 - Blocage du trafic en fonction d'un seuil
 - Ces signatures permettent de bloquer le trafic concerné lorsqu'un des seuils est dépassé pendant la période de temps configurée.
 - Cela permet d'économiser les ressources du système et peut décourager une attaque répétée.
 - Elles ne devraient s'appliquer qu'aux protocoles que vous utilisez réellement
 - Inutile de rechercher à inspecter des protocoles non utilisés dans le réseau.

Security Profiles > Intrusion Prevention

Rate Based Signatures						
Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
<input checked="" type="checkbox"/>	Digium Asterisk File Descriptor DoS	20	1	Any	<input checked="" type="radio"/> Block	None
<input checked="" type="checkbox"/>	Digium Asterisk IAX2 Call Number DoS	275	1	Any	<input checked="" type="radio"/> Block	None
<input checked="" type="checkbox"/>	DenNuke Padding Oracle Attack	1000	5	Any	<input checked="" type="radio"/> Block	None
<input checked="" type="checkbox"/>	FTP Login Brute Force	200	10	Source IP	<input checked="" type="radio"/> Block	None
<input checked="" type="checkbox"/>	FreeBSD TCP Reassembly DoS	10	2	Destination IP	<input checked="" type="radio"/> Monitor	None
<input checked="" type="checkbox"/>	IMAP Login Brute Force	60	10	Any	<input checked="" type="radio"/> Block	None
<input checked="" type="checkbox"/>	MS Active Directory LDAP Packet Handling DoS	100	1	Any	<input checked="" type="radio"/> Block	None

• • • 360

Botnet Protection

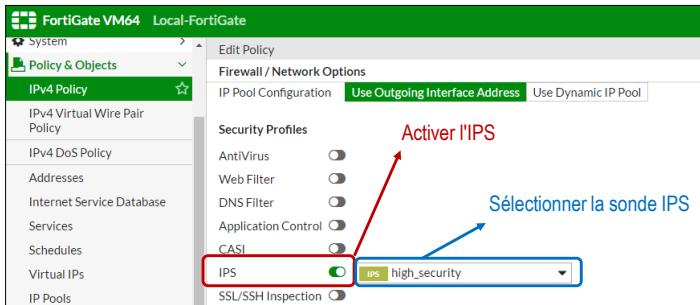
- Activer la protection contre les botnets
 - Fait partie de la licence IPS depuis FortiOS 6.2

The screenshot shows the 'Edit IPS Sensor' configuration page. It includes sections for 'IPS Signatures' (with a table showing no matching entries found), 'IPS Filters' (with a table showing a filter for 'Severity: yellow, orange, red' set to 'Default' action and 'Packet Logging'), and 'Botnet C&C' (with a button to 'Scan Outgoing Connections to Botnet Sites'). Below these are 'Rate Based Signatures' and a table listing several signatures with their respective thresholds, durations, and actions. A green 'Apply' button is at the bottom right of the table.

• • • 361

IPS sensor

- Activer un profil d'inspection IPS
 - Activer le profil de sécurité IPS et sélectionner la sonde à associer à la règle de pare-feu.



Denial of Service (DoS)

- DoS, DDoS
 - Déni de service, Déni de service distribué
 - Une attaque DoS vise à consommer toutes les ressources
 - La RAM, le CPU, le nombre de connexions, etc.
 - Dans le but de ralentir ou empêcher le fonctionnement d'un système
 - Trop de requêtes vont saturer la cible.
 - Via des requêtes valides ou non valides
 - Bloquer une attaque DoS
 - Appliquer une règle DoS
 - Celle-ci exécute une action lorsqu'un seuil est dépassé.
 - » Trop de connexions à moitié ouvertes, trop de trafic provenant de la même source, ...
 - Utiliser plusieurs sondes permet de détecter différentes anomalies.
 - FortiGate Inline
 - La règle DoS doit s'appliquer sur un FortiGate placé entre les attaquants et les ressources à protéger

Denial of Service (DoS)

- Configuration des règles de protection DoS

- La protection DoS peut être appliquée à quatre protocoles

- TCP, UDP, ICMP et SCTP.
- Plusieurs règles sont prédéfinies.

Plusieurs règles DoS peuvent être appliquées à une interface physique ou logique.

Edit DoS Policy						
Incoming Interface	port1	pour ce address	all	Destination Address	all	
	+ X		+ X		+ X	
Services	ALL					
L3 Anomalies						
Name	Status	Logging	Pass	Block	Action	Threshold
ip_src_session	○	○	Pass	Block		5000
ip_dst_session	○	○	Pass	Block		5000
L4 Anomalies						
Name	Status	Logging	Pass	Block	Action	Threshold
tcp_syn_flood	○	○	Pass	Block		2000
tcp_port_scan	○	○	Pass	Block		1000
tcp_src_session	○	○	Pass	Block		5000
tcp_dst_session	○	○	Pass	Block		5000
udp_flood	○	○	Pass	Block		2000



364

Denial of Service (DoS)

- Configuration des règles de protection DoS (suite)

- Quatre types différents de détection d'anomalies peuvent être appliqués à chaque protocole supporté

- **Flood sensor**
 - Déetecte un volume élevé de trafic d'un protocole particulier (e.g. TCP SYN flood).
- **Sweep/scan**
 - Déetecte les tentatives de scan de ports (ou de réseau :ICMP sweep) ou de recherche de cibles (*probing attempts*).
- **Source (SRC)**
 - Déetecte de gros volumes de trafic provenant d'une seule adresse IP.
- **Destination (DST)**
 - Déetecte de gros volumes de trafic destinés à une seule adresse IP.

Denial of Service (DoS)

- Configuration des règles de protection DoS
 - Conseil
 - Consulter la Network Baseline pour déterminer les seuils à appliquer.
 - Si vous ne disposez pas de références précises
 - Pour la première implémentation :
 - » Ne pas bloquez le trafic.
 - » Journalisez le trafic.
 - Analysez les journaux pour déterminer les niveaux normaux et les pics pour chaque protocole.
 - Réglez les seuils de façon à ce que les pics habituels ne soient pas bloqués.

Seuils trop élevés → risque d'épuisement des ressources avant que la règle ne déclenche.

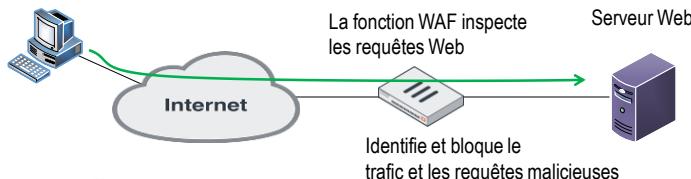
Seuils trop bas → risque d'abandon du trafic normal.

Name	Status	Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass Block	2000

Web Application Firewall

- WAF
 - Web Application Firewall
 - Web filter = pour protéger des postes clients.
 - WAF = Utilisé pour protéger des services Web.
 - Disponible uniquement en mode proxy
 - Analyse en profondeur du trafic HTTP(S).

Client Web envoie
une requête



- **WAF signatures**

- **Les signatures WAF**

- L'UTM effectue une action prédéfinie sur le trafic qui correspond à une signature.
- Base étendue de signatures
 - Peut être nécessaire dans les environnements très sécurisés mais génère plus de faux-positifs.

- **Offre une protection contre une série d'attaques contre les serveurs Web**

- Cross-site scripting (XSS).
- SQL injection.
- Exploits web connus.
- Injection de commandes OS.
- Robots/spiders/scripts malicieux.
- Chevaux de Troie.
- Divulgation d'informations à propos du serveur (Server information disclosure).
- Fuites de données concernant des cartes de crédit.
- ...

- **Cross Site Scripting (XSS)**

- **Possible en cas de faille dans un site Web**

- **Par exemple une variable mal protégée (formulaire)**

- Il est alors possible d'injecter du code dans ces variables.
- Potentiellement, le code peut être écrit dans n'importe quel langage supporté par le navigateur Web (Javascript, Java, Flash, ...)

- **La vulnérabilité affecte le client, pas le serveur.**

- Peut permettre de transmettre des données privées, comme des cookies d'authentification ou d'autres informations de session.

- **XSS permanent ou non**

- **Souvent, les sites Web enregistrent les variables dans des bases de données**

- Dans ce cas, c'est le code malicieux qui sera enregistré, il sera exécuté à chaque lecture de la variable.

Exemples d'attaques ciblant les applications Web

- **SQL Injection**

- Possible en cas de faille dans un site Web

- De nouveau, la faille peut provenir de variables mal protégées qui ne rejettent pas les valeurs non autorisées .
- L'attaquant peut alors placer une requête SQL à la place de la variable. consiste à modifier une requête SQL en injectant des morceaux de code, par exemple via le biais d'un formulaire.

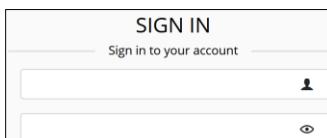
- Pour protéger le site Web

- Il faut coder le site en utilisant des requêtes préparées.
- Si le site a été mal sécurisé, il faut utiliser un WAF.

Exemples d'attaques ciblant les applications Web

- Exemple

- Connexion à un espace membre



```
<?php
// On récupère les variables envoyées par le formulaire
$login = $_POST['login'];
$password = $_POST['password'];

// On envoie une requête de vérification à la DB
$req = $bdd->query("SELECT * FROM utilisateurs WHERE
login='".$login"' AND password='".$password"');

?>
```

Exemples d'attaques ciblant les applications Web

- Si les entrées ne sont pas filtrées, l'attaquant pourrait répondre à l'invite de connexion tel que :

SIGN IN

Sign in to your account

```
<?php
$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='admin'"); -- AND password='';

// Qui sera interprété de la façon suivante
$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='admin'");
?>
```

```
<?php
$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='admin' AND password='pwd' OR
'1=1' ");-

// Qui sera interprété de la façon suivante
$req = $bdd->query("SELECT * FROM utilisateurs WHERE login='admin'");
?>
```

ENSEIGNEMENT P. - 372

372

Web Application Firewall

- **WAF Protocol Constraints**
 - Permet de contrôler le protocole HTTP
 - Le nombre d'en-têtes, la taille du contenu, la version HTTP, ...
 - Permet d'éviter certaines attaques
 - **Trop nombreux en-têtes ou de trop gros contenus**
 - Vérifie les en-têtes qui pourraient saturer la mémoire du serveur Web.
 - **Illegal host name**
 - Vérifie que les noms d'hôtes ne contiennent pas de caractères interdits.
 - **Illegal HTTP Version**
 - Les versions valides sont HTTP/0.9, HTTP/1.0, HTTP/1.1.
 - ...

HEH.be Sciences et technologies

Web Application Firewall

- FortiGate implémente un WAF
 - Disponible uniquement en mode proxy

System > Feature Visibility

Security Profiles > Web Application Firewall

Policy & Objects > IPv4 Policy

The screenshot shows the FortiGate management interface. On the left, there are navigation menus for 'System > Feature Visibility' and 'Security Profiles > Web Application Firewall'. The main area displays the 'Policy & Objects > IPv4 Policy' configuration. A policy named 'Full_Access' is selected, with settings for incoming and outgoing interfaces, source and destination, schedule, service, and action (ACCEPT). Below this, the 'Inspection Mode' is set to 'Proxy-based'. To the right, the 'Edit Policy' dialog is open, showing detailed configuration for signatures and constraints. The 'Security Profiles' section includes options for Antivirus, Web Filter (set to 'Web'), DNS Filter, Application Control, and IPS. The 'IPS' section has 'Web Application Firewall' and 'SSL Inspection' enabled. At the bottom right, there are three red dots and the number '374'.

HEH.be Sciences et technologies

FortiWeb

- FortiWeb (NSE6)
 - Offre de meilleures performances que la fonction WAF d'un FortiGate
 - Équipement dédié à la protection Web.
 - Protection plus complète que le WAF d'un FortiGate
 - Meilleure connaissance du protocole HTTP.
 - Peut effectuer des analyses de vulnérabilités.
 - Peut réaliser des tests de pénétration.
 - Contrôleur de mise à disposition d'applications
 - Peut réécrire des paquets HTTP et acheminer le trafic en fonction du contenu HTTP.
 - « Application Delivery Controller » (ADC) basique.
 - Leur fonction est d'améliorer les performances, la sécurité et la résilience des applications Web.
 - Répartition de charge serveur, traffic shaping, cache, accélération SSL, ...

The screenshot shows the FortiWeb management interface. It features a header with the HEH.be logo and the word 'FortiWeb'. Below the header, there is a list of bullet points detailing the features and performance advantages of FortiWeb compared to FortiGate's WAF. At the bottom right, there are three red dots and the number '375'.

HEH.be Sciences et technologies

FortiWeb

- Architecture
 - **Inline FortiWeb**
 - Le FortiWeb est placé entre le FortiGate et le serveur Web à protéger.
 - **Offline FortiWeb**
 - Le FortiGate doit être configuré pour transférer le trafic vers le FortiWeb.
 - Le FortiWeb peut être externe.

WALLONIE-BRUXELLES
ENSEIGNEMENT

376

HEH.be Sciences et technologies

FortiWeb

- Configuration pour rediriger le trafic vers un FortiWeb offline

WALLONIE-BRUXELLES
ENSEIGNEMENT

377

One-arm-sniffer IPS

- One-arm-sniffer IPS
 - One-arm topology
 - Le FortiGate doit être connecté à un port en mirroring (SPAN).
 - Il inspecte donc une copie des paquets, pas les paquets originaux.
 - Utilisation
 - Permet de placer un FortiGate en offline pour faire du sniffing
 - On parle de mode sniffer parce que le FortiGate ne peut pas bloquer le trafic.
 - Permet la journalisation des actions que le FortiGate aurait appliquées aux paquets.
 - Actuellement utilisé pour des phases de test ou d'évaluation
 - Utilisé au début de l'introduction des IPS qui étaient trop lents et introduisaient trop de latence.

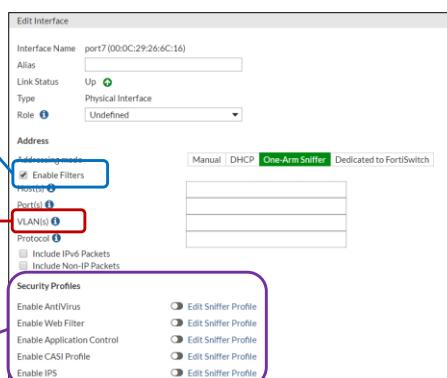
One-arm-sniffer IPS

- One-arm-sniffer Configuration
 - Uniquement activable sur des interfaces physiques

Permet de préciser que type de trafic doit être inspecté

Par défaut, seul le trafic non tagué (VLAN Natif) est inspecté

Liste des profils de sécurité supportés



- Conseils d'implémentation
 - Analyser les besoins
 - Toutes les règles de pare-feu ne nécessitent pas une inspection IPS
 - Commencez par les services les plus critiques pour l'entreprise.
 - Commencez par montrer avant de bloquer.
 - Évitez d'activer l'IPS sur les politiques internes ↔ internes.
 - Évaluer les menaces applicables
 - Créer des sondes IPS spécifiquement pour les ressources à protéger
 - Inutile de scanner les signatures MacOS si votre parc est en Windows.
 - Inutile de garder des signatures si une menace n'existe plus (correctif)
 - Surveillance et ajustement régulier
 - Surveiller régulièrement les journaux pour détecter les modèles de trafic anormaux.
 - Ajuster les profils IPS en fonction des observations.

- Conseils d'implémentation (suite)
 - Trafic chiffré
 - N'oubliez pas le profil d'inspection SSL/SSH (deep inspection), sans lui il est impossible d'inspecter le trafic chiffré.
 - Règles DoS
 - Il n'est pas possible d'appliquer un profil d'inspection SSL pour les règles DoS.
 - Ces règles n'inspectent pas la charge utile des paquets mais les types de session et le volume qui leur est associé.

Implémentation IPS

- Conseils d'implémentation (suite)

- Accélération matérielle

- Les modèles FortiGate qui prennent en charge la fonction « Nturbo » peuvent décharger le traitement IPS sur les processeurs NP6, NP7 ou SoC4.
 - Si la commande `np-accel-mode` est disponible sous config system global, le modèle FortiGate prend en charge NTurbo.

```
# config ips global
# set np-accel-mode [ basic | none ]
# set cp-accel-mode [ basic | advanced | none ]
# end
```

Logging

- Afficher les logs de l'IPS

- Log & Report > Security Events

Date/Time	%	Severity	Source	Protocol	User	Action
2 seconds ago	██████	6	10.200.1.254	6		dropped
2 seconds ago	██████	6	10.200.1.254	6		detected
2 seconds ago	██████	6	10.200.1.254	6		detected
2 seconds ago	██████	6	10.200.1.254	6		detected
12 seconds ago	██████	6	10.200.1.254	6		dropped
22 seconds ago	██████	6	10.200.1.254	6		dropped
32 seconds ago	██████	6	10.200.1.254	6		dropped
42 seconds ago	██████	6	10.200.1.254	6		dropped
53 seconds ago	██████	6	10.200.1.254	6		dropped
Minute ago	██████	6	10.200.1.254	6		dropped

Log Details

General

- Absolute Date/Time: 2022/04/21 22:44:13
- Time: 22:44:13
- Session ID: 10137
- Virtual Domain: root
- Agent: Mozilla/5.0 (Nitro/2.1.5) (Evasion:None) (Test:004131)

Source

- IP: 10.200.1.254
- Source Port: 48810
- Country/Region: Reserved
- Source Interface: port1
- User:

- Dépannage IPS

- Vérifier les mises à jour : System > FortiGuard

- Mâj envoyée à update.fortiguard.net sur TCP 443

<input checked="" type="checkbox"/> Intrusion Prevention	Licensed (Expiration Date: 2023/01/18)	<input type="button" value="Actions"/>
IPS Definitions	Version 18.00052	<input type="button" value="View List"/>
IPS Engine	Version 7.00018	<input type="button" value="View List"/>
Malicious URLs	Version 2.00970	<input type="button" value="View List"/>
Botnet IPs	Version 7.01436	<input type="button" value="View List"/>
Botnet Domains	Version 2.00721	<input type="button" value="View List"/>

- Forcer une mise à jour manuelle

```
# diagnose debug application update -1
# diagnose debug enable
# execute update-now
```

- Dépannage IPS (suite)

- Utilisation élevée du processeur

- L'option 5 laisse le moteur IPS fonctionner, mais il n'inspecte pas le trafic.
 - Si l'utilisation du processeur diminue, cela indique généralement que le volume de trafic inspecté est trop élevé pour ce modèle de FortiGate.

```
# diagnose test application ipsmonitor <Integer>

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPS A statistics
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

- **Dépannage IPS (suite)**

- Mode « Fail-open »

- Si l'IPS manque de mémoire pour traiter les nouveaux paquets, il passe en mode fail-open.

```
date=2021-04-21 time=09:07:59 logid=0100022700 type=event
subtype=system level=critical vd="root" logdesc="IPS session scan
paused" action="drop" msg="IPS session scan, enter fail open mode"
```

- Comportement

- Si le paramètre fail-open est activé : certains nouveaux paquets (en fonction de la charge du système) passeront sans être inspectés.
 - Si le paramètre fail-open est désactivé : tous les nouveaux paquets sont abandonnés

```
config ips global
  set fail-open <enable|disable>
```

- Essayez de déterminer la cause et réalisez les ajustements nécessaires

- Le volume de trafic a-t-il augmenté récemment ?
 - Le mode fail-open se déclenche-t-il à des heures précises de la journée ?

Chapitre 9

Haute disponibilité

Objectifs

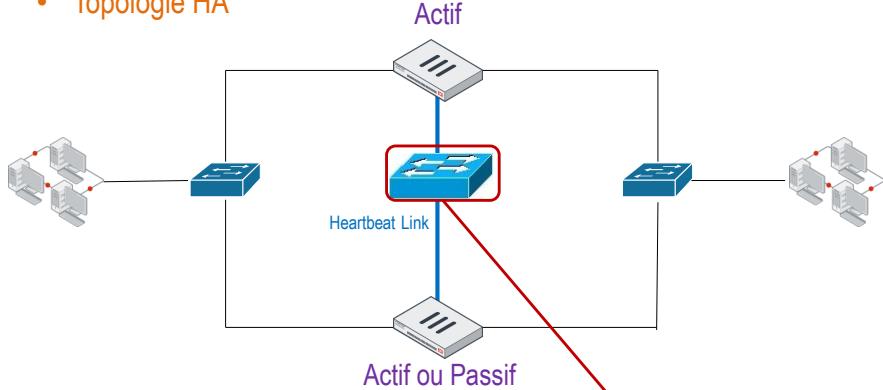
- **A l'issue de ce chapitre, l'apprenant doit être capable de**
 - Choisir le bon mode de fonctionnement haute disponibilité (HA).
 - Implémenter et configurer une solution HA.
 - Configurer la synchronisation de session pour un basculement en douceur.
 - Utiliser le clustering virtuel pour une haute disponibilité par VDOM.
 - Mettre à niveau le firmware d'un cluster HA.
 - Vérifier le fonctionnement d'un cluster HA.

High Availability (HA)

- **Principe de la HA**
 - **Haute disponibilité**
 - La HA relie et synchronise deux ou plusieurs appareils.
 - Un des appareils doit être actif, les autres peuvent être actif ou passif.
 - **FortiGate actif**
 - Le FortiGate qui traite le trafic.
 - Il synchronise sa configuration avec les autres appareils.
 - **FortiGate passif**
 - FortiGate qui ne traite pas le trafic.
 - Il synchronise sa configuration sur celle d'un FortiGate primaire pour être prêt à traiter le trafic dans le cas où le primaire a un problème.
 - **Heartbeat link**
 - Liens (UTP RJ45) reliant tous les appareils participant à la HA.
 - Utilisé pour détecter les appareils qui ne répondent plus.

Topologie

- Topologie HA



Modes de haute disponibilité

- Mode actif-passif

- FortiGate primaire

- Diffuse des paquets Hello pour la découverte et la surveillance.
 - Le FortiGate qui agit en tant qu'appareil primaire synchronise sa configuration avec les autres appareils.
 - Seul le primaire traite le trafic, il est actif.
 - Si le primaire est redémarré ou éteint, il devient un FortiGate secondaire et attend que le trafic soit redirigé vers le nouveau primaire avant de s'éteindre.

- FortiGate secondaire

- Diffuse des paquets Hello pour la découverte et la surveillance.
 - Il synchronise sa configuration sur celle d'un FortiGate primaire.
 - Il peut y avoir plusieurs secondaires.
 - Il surveille l'état du primaire (paquet Hello reçu du primaire?).
 - Si le primaire ne « répond » plus, un secondaire reprend le rôle de primaire et traite le trafic.
 - On parle alors de *HA failover* (basculement).

Modes de haute disponibilité

- Mode actif-actif

- FortiGate primaire

- Il synchronise sa configuration avec les autres appareils.
 - Le primaire traite le trafic, il est actif.
 - Le primaire a la charge d'équilibrer le trafic entre tous les dispositifs du cluster HA.

- FortiGate secondaire

- Tous les FortiGate secondaires traitent le trafic, ils sont aussi actifs.
 - Ils surveillent l'état du primaire.
 - Si le primaire a un problème, un des secondaires reprend le rôle de primaire.
 - On parle alors de *HA failover* (basculement).

FortiGate Clustering Protocol (FGCP)

- FGCP

- FGCP fonctionne uniquement sur les liens Heartbeat et est utilisé pour :

- Découvrir des FortiGates qui appartiennent au même groupe HA.
 - Élire le primaire.
 - Synchroniser les configurations et d'autres données.
 - Déetecter la défaillance d'un FortiGate.

- EtherType et ports utilisés

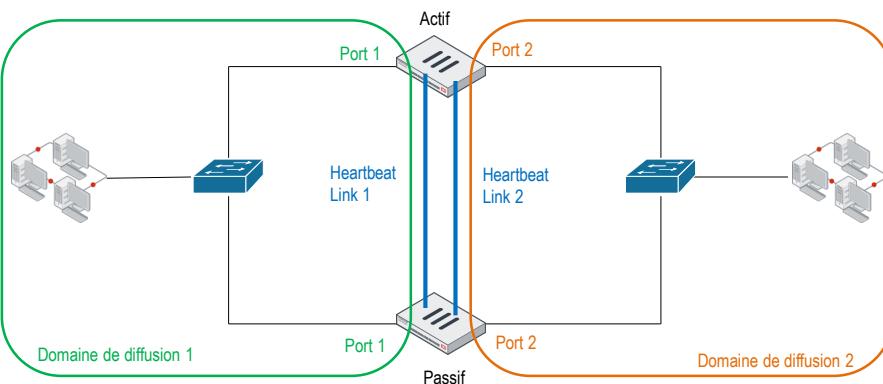
- Découverte des membres via diffusion sur les liens heartbeat (En mode NAT, le champ type Ethernet = 0x8890. En mode transparent, EtherType = 0x8891)
 - Si le cluster fonctionne en mode actif-actif, le premier paquet d'une session distribué au secondaire est encapsulé dans des trames Ethernet de type 8891
 - Pour la synchronisation des données, la gestion locale de la CLI et la journalisation, les membres échangent des Ethernet trames de type 8893.
 - Selon le type de données à synchroniser, le port TCP 703 ou le port UDP 703, est utilisé pour la synchronisation des données.
 - Le primaire relaie les journaux et les courriels d'alerte des secondaires sur le port TCP 700.

Topologie

- **Conditions requise pour la HA**

1. De deux à quatre FortiGates avec les mêmes :
 - Firmware.
 - Modèle pour le matériel et même licence pour les VM.
 - Licenses FortiGuard, FortiCloud, and FortiClient.
 - Capacité du disque dur et partitions.
 - Mode de fonctionnement (transparent ou NAT).
2. Au moins une liaison entre les appareils FortiGate
 - Pour la communication HA (Heartbeat traffic).
 - Pour la redondance, jusqu'à huit interfaces Heartbeat peuvent être utilisées.
 - Si un lien échoue, HA utilisera le suivant, selon la priorité et la position dans la liste des interfaces Heartbeat.
3. Mêmes interfaces connectées aux mêmes domaines de diffusion
 - Les mêmes interfaces sur chaque appareil FortiGate doivent être connectées au même commutateur ou segment de réseau local (voir diapositive suivante).

Topologie



- **Remarques**

- **Adressage dynamique**

- Depuis FortiOS 5.2, la HA supporte les interfaces dont les adresses IP sont assignées dynamiquement (DHCP ou PPPoE).
- Pour éviter des problèmes d'attribution d'adresses, il est recommandé de
 1. Configurer le cluster avec des IP statiques.
 2. Configurer l'adressage dynamique des interfaces uniquement lorsque le cluster HA est formé.

- **Licences différentes**

- Si les membres du cluster n'ont pas les mêmes licences, le cluster s'aligne sur la "licence la plus faible".
- Par exemple, si un des FortiGates n'a pas de licence Antivirus, l'ensemble du cluster fonctionnera sans licence antivirus.

- **Processus d'élection du FortiGate primaire**

- a) **Avec le paramètre "HA override" désactivé**

1. Le cluster compare le nombre d'interfaces monitorées dont le statut est up.
 - Le FortiGate avec le plus grand nombre d'interfaces monitorées disponibles devient le primaire.
2. Le cluster compare les temps de fonctionnement du système (system uptime).
 - Si le temps de fonctionnement du système d'un appareil est supérieur de cinq minutes au temps de fonctionnement du système des autres FortiGates, il devient le primaire.
3. Le FortiGate avec la priorité la plus élevée devient le primaire.
4. Le FortiGate dont le numéro de série est le plus élevé devient le primaire.

- **Modifier le primaire si "HA override" est désactivé**

- Il est possible de forcer manuellement le basculement (HA failover) en réinitialisant le temps de fonctionnement.

```
# diagnose sys ha reset-upptime
```

Le processus de sélection s'arrête au premier critère permettant d'élire le primaire.

Élection du FortiGate primaire

- Processus d'élection du FortiGate primaire (suite)

- b) Avec le paramètre "HA override" activé

- La priorité est prise en compte avant le temps de fonctionnement du système.
 - Permet de configurer la priorité pour favoriser l'élection d'un FortiGate.
 - Conséquence sur le basculement HA
 - Le basculement se produit lorsque le primaire tombe en panne (cas normal).
 - Se produit aussi lorsque l'ancien primaire redevient disponible (à cause de sa priorité).

- Ordre des critères de sélection

1. Nombre d'interfaces monitrées dont le statut est up.
2. Priorité la plus élevée.
3. System uptime.
4. Numéro de série le plus élevé.

Le processus de sélection s'arrête au premier critère permettant d'élire le primaire

- Modifier le primaire si "HA override" est activé

- Il est possible de forcer manuellement le basculement (HA failover) en modifiant la priorité d'un FortiGate.

Élection du FortiGate primaire

- Remarques

- Synchronisation

- Les paramètres "override" et "priority" ne sont pas synchronisés au sein du cluster, ils doivent être ajustés manuellement sur chaque FortiGate.

- Afficher les temps de fonctionnement des membres du cluster HA

Renseigne la différence de uptime en 1/10eme de seconde.

Ce FGT a un uptime de 781,4 secondes plus grand que l'autre.

```
# diagnose sys ha dump-by vcluster
...
FGVMxxxx92:...uptime/reset_cnt = 7814 / 0
FGVMxxxx36:...uptime/reset_cnt = 0 / 1
```

La valeur 0 indique le FortiGate avec le plus faible uptime

Indique le nombre de fois que l'uptime a été réinitialisé

Fonctionnement HA

- Rôles du primaire

- Découvrir et surveiller les membres du cluster
 - Échanges de paquets "heartbeat hello" avec tous les secondaires.
 - Permet de découvrir des FortiGates ou vérifier que les FortiGates sont toujours présents dans le cluster HA.
- Synchronisation
 - Le primaire synchronise sa table de routage et une partie de sa configuration avec tous les secondaires.
 - Le primaire peut être configuré pour synchroniser certaines informations de sessions de trafic pour un basculement en douceur. (voir plus loin)
- En mode actif-actif
 - Le primaire répartit le trafic entre tous les périphériques du cluster.

Fonctionnement HA

- Rôles des secondaires

- Surveillance du primaire
 - Surveille les ports et les paquets hello du primaire pour déceler des signes de défaillance.
 - Si un problème est détecté avec le primaire, les secondaires élisent un nouveau primaire et surveillent ce nouveau primaire.
- Traitement du trafic distribué par le primaire
 - En mode actif-actif uniquement.

Fonctionnement HA

- **Adresses IP des interfaces "Heartbeat"**
 - Le cluster assigne automatiquement des IP virtuelles aux interfaces Heartbeat
 - Les adresses sont distribuées en fonction du N° de série de chaque FortiGate
 - 169.254.0.1 : pour le numéro de série le plus élevé.
 - 169.254.0.2 : pour le deuxième numéro de série le plus élevé.
 - 169.254.0.3 : pour le troisième numéro de série le plus élevé
 - Etc.
 - Ces IP sont utilisées pour distinguer les membres du cluster et synchroniser les données
 - Modification de l'adresse IP virtuelle Heartbeat
 - Les FortiGates conservent leurs adresses IP virtuelles Heartbeat
 - Peu importe leur rôle (primaire ou secondaire).
 - Peu importe s'il y a basculement (primaire vers secondaire ou secondaire vers primaire).
 - Les FortiGates changent d'adresses IP virtuelles Heartbeat
 - Uniquement lorsqu'un FortiGate quitte ou rejoint le cluster.
 - Le cluster renégocie alors l'attribution de l'adresse IP Heartbeat en tenant compte du numéro de série de tout nouveau périphérique.

Fonctionnement HA

- **Les ports "Heartbeat"**
 - Le trafic heartbeat est important pour le bon fonctionnement du cluster
 - Il est nécessaire de disposer d'une BP suffisante
 - Permet de garantir que les configurations du cluster sont dans un état synchronisé à tout moment.
 - Si un switch est présent entre deux FortiGates
 - Il doit être dédié et isolé du reste du réseau.
 - Ainsi, FGCP n'est pas concurrencé par d'autres trafics pour l'utilisation de la BP.
 - **Interfaces physiques routées requises**
 - La communication Heartbeat est activée sur les interfaces physiques routées
 - Pas sur les sous-interfaces VLAN, les interfaces VPN IPsec, les interfaces redondantes, les interfaces agrégées 802.3ad ou les ports "switchés" du FortiGate.

Fonctionnement HA

- **Les ports monitorés**

- Un cluster HA peut être configuré pour surveiller l'état des liens de certaines interfaces
 - Les ports surveillés sont généralement des interfaces réseaux traitant un trafic hautement prioritaire.
 - Les interfaces physique, VLAN et les LAG peuvent être monitorées.
 - » Rappel LAG = Link Aggregation Group (= Etherchannel)

- **Basculement nécessaire ?**

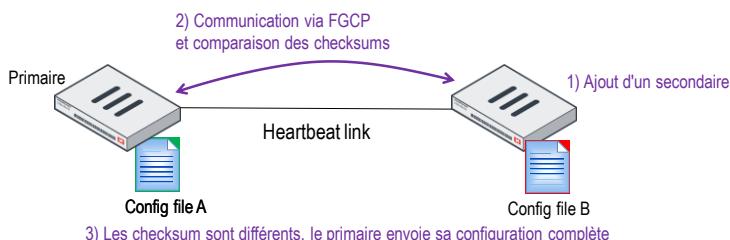
- **Éviter de configurer la surveillance pour toutes les interfaces**

- Vous ne devez configurer la surveillance d'interface que pour les ports dont la défaillance doit déclencher un basculement de périphérique.
- Notamment, ne surveillez pas les interfaces heartbeat.

Synchronisation des configurations

- **Synchronisation complète**

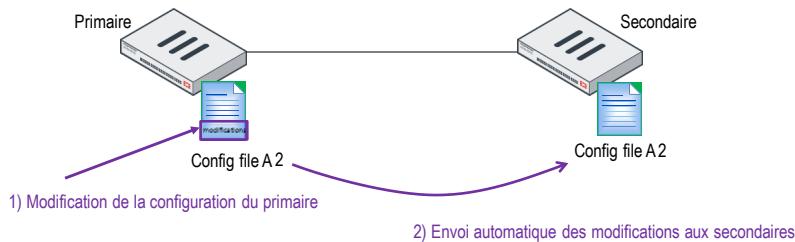
- 1) Un secondaire est ajouté au cluster.
- 2) Le primaire compare la somme de contrôle de sa configuration avec celle du secondaire.
- 3) Si elles sont différentes, le primaire envoie sa configuration au secondaire.



Synchronisation des configurations

- **Synchronisation incrémentale**

- Est utilisée lorsque la synchronisation initiale (complète) est terminée.
- Le primaire enverra tout changement de configuration à tous les secondaires.
 - Seules les modifications sont envoyées.



Synchronisation des configurations

- **Caractéristiques de la synchronisation incrémentale**

- **Quelles informations sont synchronisées ?**

- Les configurations mais aussi d'autres données telles que la table de routage, les baux DHCP, les SA IPsec, les tables ARP, ...
- Les sessions peuvent être synchronisées (désactivé par défaut).

- **Vérifications périodiques**

- **Par défaut, le primaire vérifie toutes les 60 secondes que tous les périphériques sont synchronisés**
 - Si l'un des secondaires n'est pas synchronisé, le checksum des secondaires est vérifié toutes les 15 secondes.
 - Si le checksum ne correspond pas pour cinq contrôles consécutifs, une re-synchronisation complète est effectuée.

Synchronisation des sessions

- Session Synchronization

- La synchronisation des sessions permet un basculement en douceur
 - Les informations de sessions étant synchronisées, les sessions peuvent rester ouvertes.
 - Le nouveau primaire peut prendre le relais là où les sessions en étaient arrivées.
 - Le trafic peut être interrompu pendant un court instant lors du basculement
 - Cependant, les applications n'ont pas besoin de reconnecter les sessions à nouveau.
- Uniquement possible pour certains types de trafic
 - Les sessions TCP et IPsec VPN qui ne sont pas traitées par une inspection en mode proxy
 - Exception : les sessions SIP peuvent être synchronisées même en mode proxy.
 - La commande set session-pickup permet d'activer la synchronisation des sessions TCP

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

Synchronisation des sessions

- Session Synchronization (suite)

- Il est possible d'activer la synchronisation des sessions UDP et ICMP
 - Bien que les deux protocoles soient sans session
 - Des entrées sont créées dans la table de session FortiGate pour chaque flux de trafic UDP et ICMP.
 - Généralement pas nécessaire
 - La plupart des applications réseau basées sur UDP ou ICMP sont capables de garder la communication même lorsque leurs informations de session sont perdues.

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

- **Éléments non synchronisés**

- Tous les paramètres de configuration ne sont pas synchronisés, c'est notamment de cas :
 - Des paramètres de l'interface de gestion du HA.
 - Du paramètre "HA override".
 - De la priorité HA du FortiGate.
 - De la priorité du cluster virtuel.
 - Du nom d'hôte.
 - Des licences.
 - Les licences FortiToken (numéros de series) sont synchronisées.
 - Des caches (Filtrage Web, Email, ...).
 - Des priorités HA du "ping server" (permettant la détection de passerelles en panne).

- **Causes de basculement et de journalisation**

- **Dead member (Membre mort)**
 - Le basculement est déclenché lorsque le FortiGate primaire cesse d'envoyer du trafic heartbeat.
- **Failed link (Liaison défaillante)**
 - Le basculement est déclenché lorsque l'état d'une interface surveillée sur le FortiGate primaire tombe en panne.
 - Seules les interfaces physique, redondante et LAG peuvent être surveillées.
- **Failed remote link (Lien distant défaillant)**
 - Le FortiGate utilise la fonction de surveillance de l'état des liens (LHM) pour surveiller l'état d'une ou de plusieurs interfaces.
 - Le FortiGate primaire est considéré comme défaillant si la pénalité cumulée de toutes les interfaces défaillantes atteint le seuil fixé.

Surveiller une interface :

```
config system ha
  set monitor <interface1> <interface2> ...
end
```

Failover

- Configuration du basculement

- Memory-based (Basé sur l'utilisation de la mémoire)

- Un seuil d'utilisation de la mémoire peut être configuré. Lorsque ce seuil est dépassé pendant le laps de temps défini, il y a basculement.

- Failed SSD (SSD défaillant)

- Le basculement est déclenché lorsque le FortiOS détecte une défaillance dans un SSD.
- Uniquement disponible pour les appareils équipés de disques SSD.

- Admin-triggered (déclenché par l'administrateur)

- Le basculement est déclenché manuellement par l'administrateur.

- Remarque

- Lorsqu'un basculement se produit, un fichier journal est généré.
- Le Fortigate peut également générer un trap SNMP et un email d'alerte.

Activer le memory-based failover :



```
config system ha
  set ssd-failover enable
end
```

• • • 412

Failover

- Causes de basculement et de journalisation

- Device failover (dead member)

- Ce type de basculement est toujours actif.

```
config system ha
  set hb-interval <1 - 20>
    set hb-interval-in-milliseconds 100ms | 10ms
    set hb-lost-threshold <1 - 60>
  end
```

Nombre d'échecs de réception de paquets « Hello » avant que l'appareil ne soit considéré comme mort

Temps entre deux envois (nombre entier fois 100ms) ou intervalle fixé à 10 ou 100ms



• • • 413

Failover

- Causes de basculement et de journalisation

- Remote link failover (Failed link)

- Configurer le Link Health Monitor (voir chapitre sur le routage)

```
config system link-monitor
    edit "port1-ha"
        set srcintf "port1"
        set server "4.2.2.1" "4.2.2.2"
        set ha-priority 10
```

Pénalité à affecter si le lien est défaillant

- Configurer les paramètres HA relatifs à la défaillance de lien

```
config system ha
    set pingserver-monitor-interface port1
    set pingserver-failover-threshold 5
    set pingserver-secondary-force-reset enable
    set pingserver-flip-timeout 30
end
```

Active le remote link failover sur port1

Seuil de pénalité déclenchant un basculement

Pas d'élection de nouveau primaire avant le flip-timeout (30 min.)
Impose l'élection d'un nouveau primaire à l'expiration du flip-timeout.



414

Failover

- Causes de basculement et de journalisation

- Memory-based failover (Utilisation élevée de la mémoire)

- Un seuil d'utilisation de la mémoire peut être configuré. Lorsque ce seuil est dépassé pendant le laps de temps défini, il y a basculement.

```
config system ha
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 30
    set memory-failover-sample-rate 2
    set memory-failover-flip-timeout 20
end
```

Basculement lorsque l'utilisation de la mémoire dépasse 70% pendant 30 secondes

Vérification du pourcentage de mémoire utilisée toutes les 2 secondes



415

- **Adresses MAC virtuelles et basculement**
 - Pour transférer le trafic, la HA utilise des adresses MAC virtuelles
 - **Assignation automatique d'une adresse MAC virtuelle**
 - Lorsqu'un primaire rejoint un cluster HA, une adresse MAC virtuelle est assignée à chacune de ses interfaces (hormis les interfaces heartbeat).
 - **Le primaire informe tous les secondaires de l'adresse MAC virtuelle assignée**
 - Via les liens heartbeat.
 - **En cas de basculement**
 - **L'adresse MAC virtuelle du FortiGate actif ne change pas**
 - Lors du basculement, le secondaire qui devient le nouveau primaire adopte les mêmes adresses MAC virtuelles que l'ancien primaire pour les interfaces équivalentes.
 - **Le nouveau primaire informe tous les secondaires**
 - Après le basculement, le nouveau primaire informe, via des paquets gratuits ARP, que chaque adresse MAC virtuelle est désormais accessible via un autre chemin.

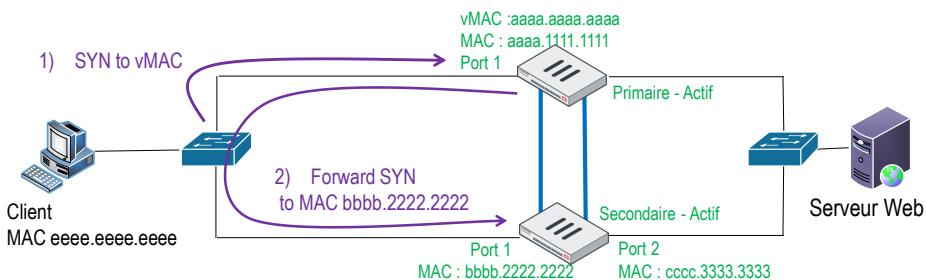
- **Panne d'un secondaire**
 - **Dans un cluster actif-passif**
 - Le primaire met à jour la liste les FortiGates secondaires disponibles.
 - Le primaire surveille le secondaire défaillant en attendant qu'il soit de nouveau opérationnel.
 - **Dans un cluster actif-actif**
 - **Tous les secondaires gèrent aussi le trafic**
 - Le primaire suit et assigne des sessions à chaque secondaire.
 - **En cas de défaillance d'un secondaire**
 - Le primaire doit également réassigner les sessions du FortiGate défaillant à un autre FortiGate secondaire.
 - Le primaire surveille le secondaire défaillant en attendant qu'il soit de nouveau opérationnel.

Active-Active Load Balancing

- Répartition de la charge en mode actif – actif
 - Le client envoie un paquet SYN au FortiGate primaire
 - Il utilise l'adresse MAC virtuelle de l'interface interne comme destination.
 - Le primaire décide si la session sera traitée par un secondaire
 - Si oui, il transmet le paquet SYN au secondaire qui effectuera les inspections.
 - Le primaire utilise l'adresse MAC physique du FortiGate secondaire comme adresse de destination.
 - Par défaut, seules les sessions en mode proxy sont envoyées à un secondaire.
 - L'option `load-balance-all` permet de distribuer n'importe quelle session.
 - Le secondaire traite la session
 - Le secondaire répond avec un SYN/ACK au client.
 - Le secondaire démarre la connexion avec le serveur (auquel le client souhaite se connecter) en lui envoyant directement un paquet SYN.

Active-Active Load Balancing

- Répartition de la charge en mode actif – actif (suite)
 - 1) Le client envoie un paquet SYN au FortiGate primaire
 - Dest MAC aaaa.aaaa.aaaa, src MAC eeee.eeee.eeee, TCP SYN dport 80
 - 2) Le primaire décide si la session sera traitée par un secondaire
 - Si oui, il transmet le paquet SYN au secondaire qui effectuera les inspections.
 - Dest MAC bbbb.2222.2222, src MAC aaaa.1111.1111, TCP SYN dport 80



Active-Active Load Balancing

- Répartition de la charge en mode actif – actif (suite)

- 3) Le secondaire traite la session

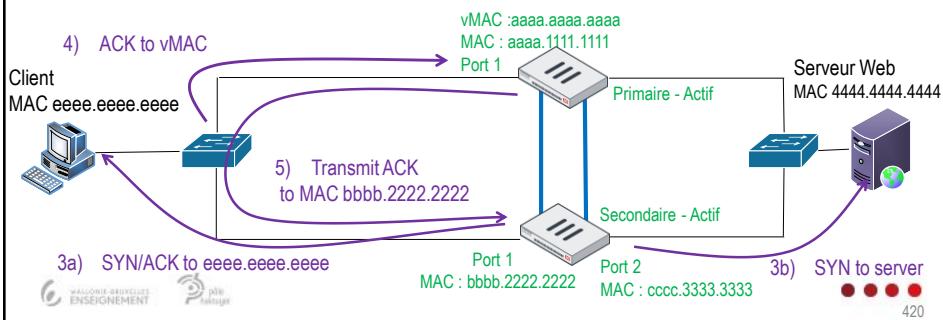
- a. Le secondaire répond avec un SYN/ACK au client.
 - Dest MAC eeee.eeee.eeee, src MAC bbbb.2222.2222, TCP ACK sport 80.
- b. Le secondaire démarre la connexion avec le serveur
 - Dest 4444.4444.4444, src cccc.3333.3333, TCP SYN dport 80.

- 4) Le client envoie un paquet ACK au FortiGate primaire

- Dest aaaa.aaaa.aaaa, src eeee.eeee.eeee, TCP ACK dport 80.

- 5) Le primaire transmet l'ACK au secondaire

- Dest bbbb.2222.2222, src aaaa.1111.1111, TCP ACK dport 80.



HEH.be Sciences et technologies

Active-Active Load Balancing

- Répartition de la charge en mode actif – actif (suite)

- 6) Le serveur répond au primaire par un SYN/ACK

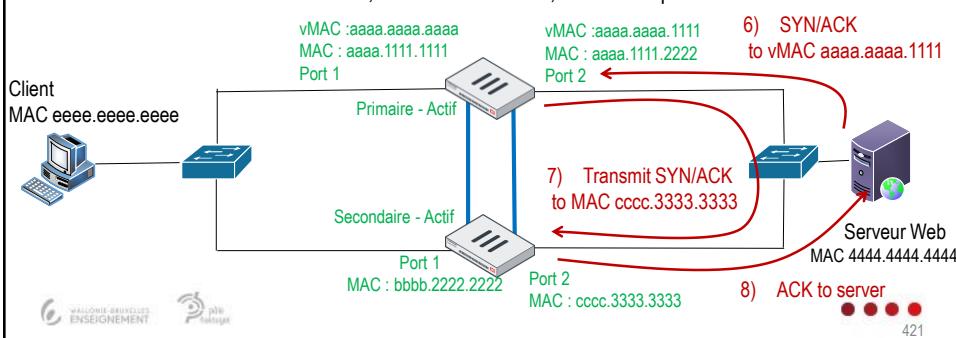
- a. Dest MAC aaaa.aaaa.1111, src MAC 4444.4444.4444, TCP SYN ACK sport 80

- 7) Le primaire transmet le SYN/ACK au secondaire

- Dest cccc.3333.3333, src aaaa.1111.2222, TCP ACK sport 80.

- 8) Le secondaire accueille réception du SYN/ACK au serveur

- Dest 4444.4444.4444, src cccc.3333.3333, TCP ACK sport 80.



Virtual clustering

- **Balanceur de charge en mode actif-actif**
 - Les sessions suivantes ne sont pas pris en charge par le balanceur de charge
 - ICMP, multicast, broadcast, SIP ALG, IM, P2P, IPsec VPN, SSL VPN, HTTP multiplexing, SSL offloading, WAN optimization, explicit web proxy, WCCP
 - Les sessions HTTPS ne sont pas équilibrées en charge si elles font l'objet d'une inspection en mode proxy.
 - La charge des sessions HTTPS est équilibrée uniquement lorsque `load-balance-all` est activé et le mode d'inspection est en mode flux ou lorsque le mode d'inspection est proxy et le trafic HTTPS n'est pas inspecté.

Virtual clustering

- **Méthodes de balanceur de charge en mode actif-actif**
 - **none**
 - Pas de balanceur de charge, le primaire prend en charge toutes les sessions
 - **leastconnection**
 - Le primaire distribue les sessions au secondaire en ayant le moins.
 - **Round-robin**
 - Le primaire distribue les sessions à tour de rôle.
 - **Weight-round-robin**
 - Le primaire distribue les sessions en fonction du poids de chaque membre du cluster.
 - **Random**
 - Le primaire distribue les sessions aléatoirement
 - **Iphub**
 - Les sessions ayant le même couple source/destination sont traitées par le même membre.
 - **Iport**
 - Les sessions sont distribuées en fonction des adresses et ports source/destination. Plus le trafic est varié, plus le trafic sera distribué parmi les membres.

Virtual clustering

- Méthodes de balancement de charge en mode actif-actif (suite)
 - Configuration de la Méthodes de balancement de charge en mode actif-actif

```
config system ha
  set schedule none | hub | leastconnection | round-robin | weight-
round-robin | random | ip | ipport
end
```

- Configuration du poids (si round-robin)

- A faire sur le primaire (pour chaque membre du cluster HA va se synchroniser)

```
config system ha
  set weight <id> <weight>
end
```

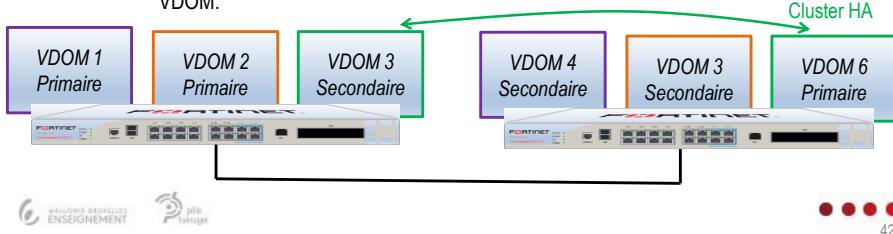
- Vous pouvez obtenir l'ID (index) du membre avec la commande `get system ha status`

```
# get system ha status
...
Primary: FGVM010000064692, HA operating index = 0
Secondary: FGVM010000065036, HA operating index = 1
```

424

Virtual clustering

- Virtual clustering
 - Multiples VDOM
 - Lorsque plusieurs VDOM sont utilisés, il est possible de configurer des clusters virtuels.
 - Répartition de charge
 - Chaque FortiGate peut agir à la fois comme primaire pour un VDOM d'un cluster et comme secondaire pour un autre VDOM d'un autre cluster.
 - De cette manière, la charge de trafic est répartie entre les FortiGate des clusters.
 - Limitation
 - Le clustering virtuel est réalisable uniquement entre deux FortiGate ayant plusieurs VDOM.



425

Full mesh HA

- Full mesh HA

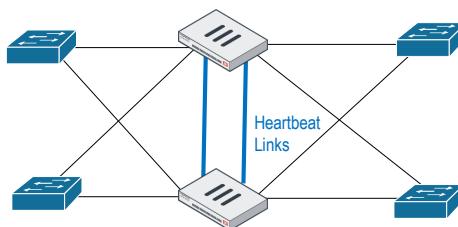
- Haute disponibilité avec maillage complet

- Topologie plus robuste

- Offre une tolérance aux pannes au niveau des commutateurs, des FortiGates et des interfaces des FortiGates (Pas de Single point of failure).

Redondance :

- Des fortigates
- Des switches
- Des interfaces
- Des liens



- Limitation

- Uniquement disponible sur le matériel haut de gamme.

Mise à jour d'un cluster

- Firmware updates

- Redémarrage nécessaire

- Comme pour une mise à jour classique, chaque FortiGate devra redémarrer.
 - Seul le primaire doit être mis à jour.

- Uninterruptable upgrade

- Le paramètre "Uninterruptable upgrade" est activé par défaut
 - Cela implique que le cluster mettra d'abord à niveau les FortiGates secondaires.
 - S'il est désactivé, tous les FortiGates se mettront à jour en même temps.
 - » L'opération est plus rapide, mais le trafic sera interrompu momentanément.

- Élection d'un nouveau primaire

- Une fois que tous les FortiGates secondaires mis à jour, un nouveau primaire est élu et le firmware de l'ancien primaire est mis à niveau.

- Cluster en mode actif - actif

- L'équilibrage de la charge de trafic est temporairement désactivé pendant que tous les périphériques mettent à jour leur firmware.

Mise à jour d'un cluster

- Se connecter à un membre du cluster

- Via l'adresse IP virtuelle du cluster HA
 - Dans ce cas, vous vous connectez toujours au FortiGate primaire.
- Via une interface réseau (In-band HA management interface)
 - Permet d'utiliser n'importe quelle interface

```
config system interface
  edit "port1"
    set management-ip 10.0.10.1 255.0.0.0
    set allowaccess ping https ssh snmp
```

- Configurer une interface réservée pour l'administration HA (Out-of-band)

- Consiste à utiliser une interface dédiée à l'administration du cluster (pas d'autres trafic via cette interface).

```
config system ha
  set ha-mgmt-status enable
  config ha-mgmt-interfaces
    edit 1
      set interface "port10"
      set gateway 192.168.100.254
```

428

Dépannage et monitoring

- Vérifier le statut du cluster HA en GUI

Clic droit sur le menu permet d'ajouter d'autres colonnes

System > HA

FortiGate VM64		FortiGate VM4	
Local-FortiGate (Primary)		Remote-FortiGate (Secondary)	
Status	Priority	Hostname	Serial No.
Synchronized	200	Local-FortiGate	FGVM01000064692
Synchronized	100	Remote-FortiGate	FGVM01000065036

Role dans le cluster HA

Role	Uptime	Sessions	Throughput
Primary	3d 23h	11	22.00 kbps
Secondary	0s	5	17.00 kbps

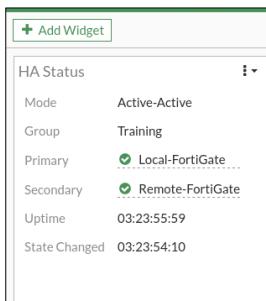
Refresh
Edit
Remove device from HA cluster

Affichage de tous les Fortigates dans le cluster

Clic droit permet de déconnecter du cluster

Dépannage et monitoring

- Vérifier le statut du cluster HA en GUI (suite)
 - Un widget peut être ajouté dans le dashboard pour connaître l'état du cluster



Dépannage et monitoring

- Vérifier le statut du cluster HA en CLI
 - Permet d'obtenir plus d'informations qu'en GUI

```
# diagnose system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P → Mode A-P (Actif-Passif)
Group: 210
Debug: 0
Cluster Uptime: 2 days 21:28:23
Cluster state change time: 2022-04-20 18:28:23 → Dans cet exemple, SN1 remplace le N° de série
Primary selected using:
  <2022/04/20 18:28:23> vcluster-1: SN1 is selected as the primary because its uptime
  is larger than peer member SN2.
  <2022/04/20 16:13:49> vcluster-1: SN2 is selected as the primary because its uptime
  is larger than peer member SN1.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
  SN1(updated 4 seconds ago): in-sync
  SN2(updated 4 seconds ago): in-sync

System Usage stats:
  SN1(updated 4 seconds ago):
    sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=57%
  SN2(updated 4 seconds ago):
    sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=56%
<suite diapositive suivante>
```

Dépannage et monitoring

Statut des interfaces heartbeat (HBDEV),
monitorées (MONDEV) et surveillées (PINGSRV)

```
# suite de la commande "diagnose system ha status"
HBDEV stats:
    SN1(updated 4 seconds ago):
        port9: physical/10000full, up, rx-bytes/packets/dropped/errors=154684218/384596/0/0,
        tx=352015560/498020/0
    SN2(updated 4 seconds ago):
        port9: physical/10000full, up, rx-bytes/packets/dropped/errors=386075683/578563/0/0,
        tx=269160874/516602/0
MONDEV stats:
    SN1(updated 4 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0,
        tx=13209070/157763/0/0
    SN2(updated 4 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0,
        tx=6345393/37126/0/0
PINGSRV stats:
    SN1(updated 4 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=238546316/964449/0/0,
        tx=13209070/157763/0/0
    pingsrv: state=up(since 2022/04/20 16:13:50), server=10.9.15.40, ha_prio=5
    SN2(updated 4 seconds ago):
        port1: physical/10000full, up, rx-bytes/packets/dropped/errors=214804265/993451/0/0,
        tx=6345393/37126/0/0
    pingsrv: state=N/A(since 2022/04/20 16:13:54), server=10.9.15.40, ha_prio=5

Primary      : Local-FortiGate , SN1, HA cluster index = 0
Secondary     : Remote-FortiGate, SN2, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: SN1, HA operating index = 0
Secondary: SN2, HA operating index = 1
```

Rôle des membres, noms d'hôte,
numéro de série, et ID.

Dépannage et monitoring

- Vérifier l'état de la synchronisation de la configuration
 - Si le primaire et le secondaire présentent les mêmes checksum, ils sont synchronisés.

```
# diagnose sys ha checksum cluster
=====
===== FGVM010000112065 =====
is_manage_master()=1, is_root_master()=1
debugzone
global: 7b 05 62 17 8f cd 76 29 57 da 32 8e
root: 97 91 80 67 9d 97 e3 a1 dd 0d ca
all: e1 ad dd fb ff f6 e5 55 2c ed 3b

checksum
global: 7b 05 62 17 8f cd 76 29 57 da 32 8e
root: 97 91 80 67 9d 97 e3 a1 dd 0d ca
all: e1 ad dd fb ff f6 e5 55 2c ed 3b
```

```
# diagnose sys ha checksum cluster
=====
===== FGVM010000065036 =====
is_manage_master()=0, is_root_master()=0
debugzone
global: 7b 05 62 17 8f cd 76 29 57 da 32 8e
root: 97 91 80 67 9d 97 e3 a1 dd 0d ca
all: e1 ad dd fb ff f6 e5 55 2c ed 3b

checksum
global: 7b 05 62 17 8f cd 76 29 57 da 32 8e
root: 97 91 80 67 9d 97 e3 a1 dd 0d ca
all: e1 ad dd fb ff f6 e5 55 2c ed 3b
```

- Si les checksum ne correspondent pas, essayez de les faire recalculer :

```
# diagnose sys ha checksum recalculate
```

Dépannage et monitoring

- Se connecter à un secondaire
 - La CLI d'un membre permet de se connecter à un autre membre

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

- Le point d'interrogation permet de lister les numéros d'index de chaque FortiGate.

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

- Afficher ou recalculer les checksum

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

Dépannage et monitoring

- Vérifier l'état de la synchronisation de la configuration

Checksum de la configuration globale

```
# diagnose sys ha checksum cluster
=====
FGVM010000030273 =====

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 9f
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 9f
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
or
```

Checksum de la configuration du VDOM racine

Checksum de la configuration globale + toutes les sommes de contrôle des VDOM

Reserved HA Management Interface

- **Interfaces de management d'un cluster HA**

- Réserver une interface dédiée pour la gestion du cluster

- Il est possible de réserver une interface physique de gestion différente pour chaque appareil.
 - Permet de se connecter en CLI et GUI directement à chaque FortiGate du cluster sans devoir se connecter via le primaire.
 - Permet que chaque appareil envoie ses logs et son trafic SNMP indépendamment.
 - La configuration de cette interface de gestion n'est pas synchronisée.
 - Fonction disponible en mode NAT et en mode transparent.

- Interface de gestion "In-band"

- Permet de se connecter directement à chaque FortiGate du cluster sans devoir se connecter via le primaire et sans devoir réserver une interface de gestion.

```
config system interface
  edit <port name>
    set management-ip <IP address and subnet mask>
```

Chapitre 10

Single Sign On

SSO

Objectifs

- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Définir la notion de *Fortinet Single Sign On* (FSSO)
 - Expliquer les différentes méthodes FSSO.
 - Configurer un FortiGate pour FSSO.
 - Dépanner des problèmes liés au FSSO.

SSO

- Single Sign-On (SSO)
 - Authentification unique
 - Après avoir été identifiés une première fois, les utilisateurs peuvent accéder à diverses ressources du réseau :
 - Sans avoir à saisir à nouveau leurs identifiants.
 - Indépendamment de la plate-forme, de la technologie ou du domaine.
 - La première authentification se fait auprès d'un serveur d'authentification
 - Annuaires
 - Active Directory ou NTLM pour les réseaux Microsoft.
 - eDirectory pour les réseaux Novell.
 - Serveur AAA
 - Serveur RADIUS.
 - FortiAuthenticator est un serveur AAA qui comprend un serveur RADIUS, un serveur LDAP et peut remplacer l'agent de collecte FSSO sur un réseau Windows AD.

- **Fortinet Single Sign-On agents**
 - Agent logiciel Fortinet utilisé pour faire du SSO
 - Logiciel à installer sur certains serveurs de la topologie.
 - Permet à un FortiGate de récupérer les identifiants des utilisateurs de manière passive.
 - Sans leur demander directement leurs identifiants via un prompt.
 - **Quel agent faut-il installer et où?**
 - Le mode de déploiement du SSO et (le ou) les agents à installer et dépendent du type de serveur d'authentification.
- **Mode de déploiement du SSO avec Novell eDirectory**
 - **eDirectory agent mode**
 - Fonctionne sensiblement comme l'agent collecteur sur un DC Windows AD.

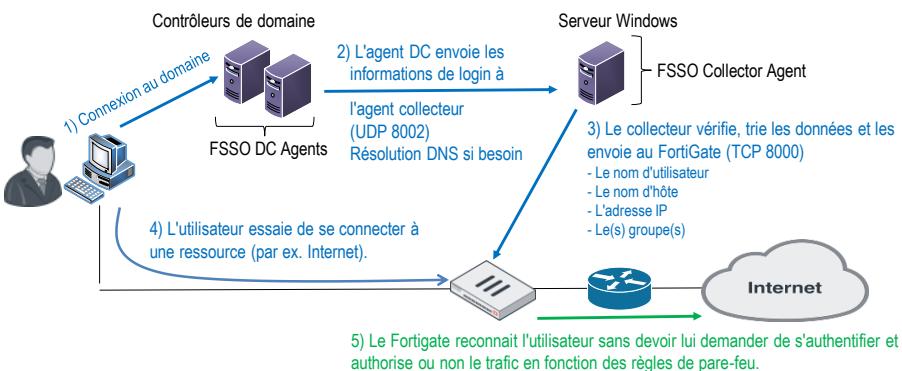
- **Les modes de déploiement du SSO avec Windows AD**
 1. **Domain Controller agent mode**
 - Nécessite un agent (*DC agent*) sur chaque contrôleur du domaine ainsi qu'au moins un agent collecteur.
 - Nécessite un redémarrage après l'installation des agents.
 2. **Polling mode**
 - Ce mode permet le SSO lorsqu'il n'est pas possible d'installer un agent sur les DC.
 - Ce mode génère plus de trafic.
 - Deux options :
 - **Soit avec un agent collecteur** (Collector agent) installé sur un serveur du domaine.
 - **Soit sans agent** (agentless).
 3. **Terminal Server agent mode**
 - Utilise un agent collecteur (TS agent) ou un Fortiauthenticator.
 - Utilisé exclusivement pour les environnements Citrix et Terminal Services.

FSSO avec Active Directory

- Domain Controller agent mode
 - DC agent
 - Nécessite un agent (DC agent) installé sur chaque contrôleur du domaine
 - Sous forme de dll dans Windows\system32\dcagent.dll
 - Un redémarrage est nécessaire après l'installation de l'agent.
 - L'agent DC surveille les connexion des utilisateurs sur le DC
 - L'agent DC envoie les informations de connexion à l'agent collecteur.
 - Effectue les résolutions DNS pour connaître les IP des utilisateurs.
 - Collector agent
 - Nécessite au moins un agent collecteur sur un serveur Windows membre du domaine.
 - L'agent collecteur est chargé de :
 - Vérifier les groupes d'utilisateurs.
 - Vérifier les stations de travail (workstation check).
 - » Refait les résolutions DNS au cas où des IP auraient changé.
 - Envoyer les informations de connexion mises à jour vers les FortiGates.

FSSO avec Windows AD

- Principe du "DC Agent Mode"
 - Le mode agent DC est le mode le plus évolutif



- **Collector Agent-based Polling Mode**
 - **Collector agent**
 - **Nécessite au moins un agent collecteur**
 - Sur un serveur Windows membre du domaine.
 - **Aucun agent DC n'est requis**
 - Pas besoin de redémarrer les DC.
 - Pas besoin de maintenir à jour les agents DC.
 - **Polling**
 - **L'agent collecteur questionne chaque DC régulièrement sur les événements de connexion**
 - Génère du trafic (parfois inutile si aucun utilisateur ne se connecte)
 - Par défaut via SMB (TCP 445)
 - Sinon via TCP 135, TCP 139, and UDP 137
 - **Trois méthodes de polling**
 - WMI, WinSecLog, NetAPI

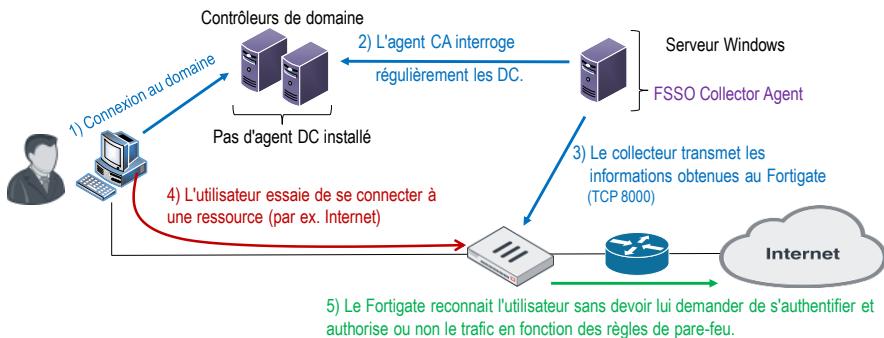
- **Event log polling using WMI**
 - **Windows Management Instrumentation (WMI)**
 - **WMI est une API Windows**
 - Permet d'obtenir des informations système d'un serveur Windows.
 - L'agent collecteur joue le rôle de client WMI et envoie des requêtes au DC qui agit en tant que Serveur WMI.
 - **Caractéristiques**
 - **Ne renvoie que les événements de connexion demandés**
 - Le collecteur ne doit pas rechercher les événements de connexion parmi tous les logs.
 - Le journal des événements (Event Log) doit être activé.
 - **Utilisation de BP optimisée entre l'agent collecteur et le DC**

- Event log polling (WinSecLog)
 - Le collecteur interroge le journal des événements des DC
 - Le journal des événements (Event Log) doit donc être activé.
 - Caractéristiques
 - Méthode plus lente
 - Car il faut aller lire des journaux d'événements plutôt que des tables en RAM.
 - Aucun événement de connexion n'est manqué, même en cas de forte charge.
 - Car les logs ne sont généralement pas supprimés (rapidement).
 - Latence possible
 - Attention dans les grands réseaux ou en cas de lenteurs des systèmes.
 - Nécessite des liens réseau rapides.
 - Méthode requise pour les clients Mac OS qui se connectent à l'AD

- NetAPI polling
 - Le collecteur interroge la fonction `NetSessionEnum`
 - Le collecteur récupère les informations de sessions établies sur un serveur DC via des requêtes envoyées à la fonction Windows `NetSessionEnum`.
 - Caractéristiques
 - Méthode la plus rapide.
 - Interroge la table des sessions en RAM
 - Les sessions peuvent être rapidement créées et purgées de la RAM, avant que l'agent n'ait la possibilité d'interroger et de notifier les pare-feux.
 - Il est donc possible de rater certaines ouvertures de sessions utilisateur en cas de forte charge du serveur AD ou du réseau.

FSSO avec Windows AD

- Principe du "Collector Agent-based Polling Mode"
 - Le collecteur doit régulièrement envoyer des requêtes au DC
 - Pour connaître les événements de connexion (login events).



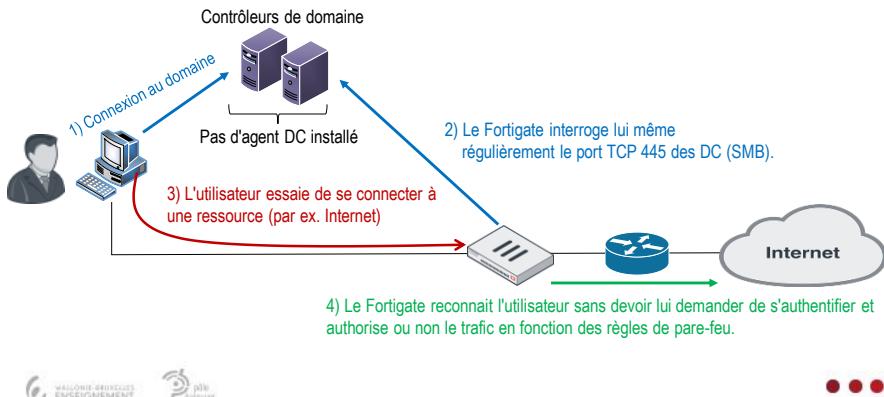
FSSO avec Windows AD

- Agentless polling mode
 - Le Fortigate envoie lui-même les requêtes au DC
 - Aucun agent n'est utilisé.
 - Le Fortigate interroge directement les logs des DC (WinSecLog) via SMB.
 - Caractéristiques
 - Event log doit être activé
 - Le Fortigate interroge le journal des événements du DC, celui-ci doit donc être activé.
 - Consomme les ressources du pare-feu
 - Le Fortigate nécessite des ressources système (CPU, RAM) plus importantes car il collecte et traite toutes les données lui-même.
 - Certaines fonctionnalités ne sont pas disponibles
 - Notamment la vérification des stations de travail (workstation check).

FSSO avec Windows AD

- Principe du "Agentless Polling Mode"

- N'utilise aucun agent
 - Le Fortigate contacte lui-même les DC pour collecter les informations.



FSSO avec Windows AD

- Remarques (Quelle que soit la méthode)

- Serveur DNS

- Event log fourni le nom d'hôte mais pas l'IP
 - Les événements de connexion permettent d'obtenir le nom d'utilisateur et le nom de la station de travail mais pas l'adresse IP.
- Il est nécessaire de disposer de son propre serveur DNS
 - Car si l'adresse IP d'un poste de travail change, les enregistrements DNS doivent être mis à jour immédiatement.

- Connectivité avec les postes de travail

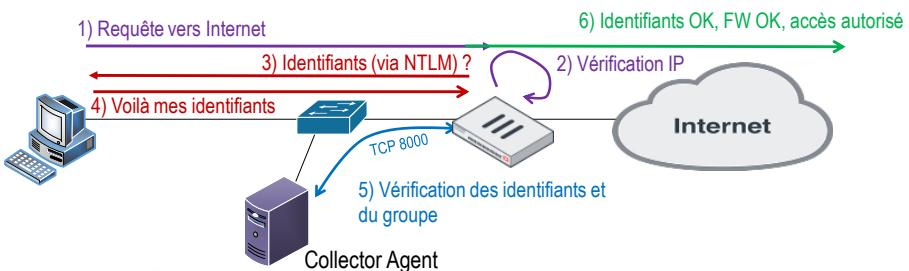
- La déconnexion d'un utilisateur ne génère pas d'entrée dans le journal des événements
 - Chaque poste de travail utilisateur doit donc être régulièrement interrogé pour voir s'ils sont toujours là.
- Les agents collecteurs doivent donc pouvoir contacter les postes de travail
 - Les ports TCP 139 et 445 doivent être ouverts entre les agents collecteurs/FortiGate et tous les hôtes.
 - "Remote registry service" doit s'exécuter sur chaque poste de travail.

Web-Initiated FSSO

- Authentication FSSO via NTLM
 - NT Lan Manager (NTLM)
 - Suite de protocoles de sécurité propriétaire de Microsoft
 - FortiGate utilise NTLM pour authentifier les utilisateurs via le navigateur web du client.
 - Le navigateur Web doit donc supporter l'authentification NTLM.
 - Solution non transparente pour les utilisateurs
 - Les utilisateurs devront entrer leurs identifiants (Exception de IE).
 - Utilisations
 - Dans des configurations de domaine simple, NTLM n'exige pas d'agents DC
 - Solution souvent utilisée en backup du FSSO DC agent mode.
 - » Si le collecteur ne peut pas retrouver des utilisateurs connectés à un AD (par exemple lors d'un problème de communication entre un DC et un collecteur).
 - » FortiGate lance alors la négociation NTLM avec le navigateur du client pour les utilisateurs FSSO non actifs.
 - La solution peut être utile dans des configurations de domaine complexes
 - En présence de multiples domaines elle ne nécessite qu'un seul agent collecteur global.

Web-Initiated FSSO

- Principe de l'authentification via NTLM
 1. L'utilisateur tente d'accéder à Internet avec son navigateur.
 2. Vérification si l'adresse IP figure dans la liste des utilisateurs actifs du FSSO.
 3. Si non, FortiGate utilise NTLM pour demander les identifiants de l'utilisateur.
 4. Le navigateur de l'utilisateur envoie les identifiants au FortiGate.
 5. FortiGate vérifie les identifiants et l'appartenance à un groupe via un agent collecteur.
 6. Si l'identification est correcte, l'accès est accordé en fonction de l'appartenance à un groupe.



HEH.be Sciences et technologies

Web-Initiated FSSO

- Authentication NTLM transparente
 - Certains navigateurs peuvent être configuré pour envoyer automatiquement les informations d'authentification lorsqu'ils reçoivent une requête NTLM.

Internet Explorer : Outils > Options Internet.

Paramètres de sécurité - Zone Internet

Demande le nom d'utilisateur et le mot de passe

OK Annuler

454

HEH.be Sciences et technologies

Configuration FSSO

- Agentless polling mode

Security Fabric > Fabric Connectors > Create new

FortiGate VM64

Dashboard

Security Fabric

Physical Topology

Logical Topology

Security Rating

Automation

Settings

Fabric Connectors

FortiView

Compléter l'adresse IP et les identifiants "administrateur" du DC

New Fabric Connector

SSO/Identity

Poll Active Directory Server

RADIUS Single Sign-On Agent

Fortinet Single Sign-On Agent

Server IP/Name: [redacted]

User: [redacted]

Password: [redacted]

LDAP Server: [redacted]

Enable Polling:

OK Cancel

455

HEH.be Sciences et technologies

Configuration FSSO

- Collector agent polling mode and DC agent mode

Security Fabric > Fabric Connectors > create new

Le collecteur doit être configuré en mode "advanced"

SSO/Identity

SSO/Identity

Nom du serveur AD
IP/nom du serveur où l'agent est installé
Eventuellement un mot de passe

Primary FSSO Agent

Name: []

Primary FSSO Agent

Server IP/Name: []

Password: []

User Group Source: Collector Agent Local

Users/Groups: 0

Apply & Refresh OK

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

456

HEH.be Sciences et technologies

Configuration FSSO

- Installation des agents FSSO
 - A télécharger sur <https://support.fortinet.com>
 - Les versions des agent DC et collector doivent correspondre.

Home Asset Assistance Download Feedback

Firmware Images

Select Product: FortiGate

Release Notes Download

v5.00 Directory

v6.00 Directory

Name:

Image File Path: / FortiGate/v5.00/ 5.4/ 5.4.1/

Up to higher level directory

Name: FSSO

Agent DC pour Windows

Agent collector pour Windows

Agent collector pour Novell

Agent collector pour Citrix

Firmware Version: v5.4.1.build5447 (GA) [Update]
A new firmware version is available (5.4.8) [View Release Notes]

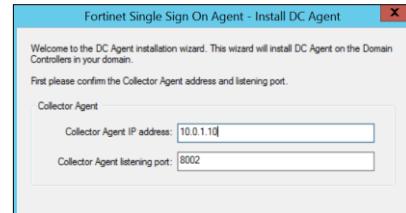
WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

457

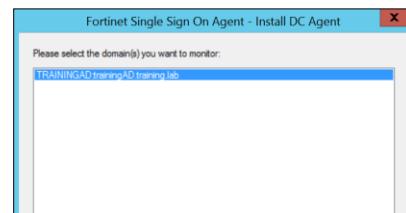
Configuration FSSO

- Installation des agents "DC"

1. Entrer l'IP/port de l'agent collecteur.



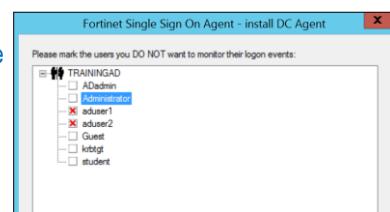
2. Sélectionner le domaine à surveiller



Configuration FSSO

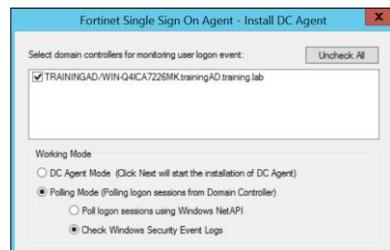
- Installation des agents "DC"

3. (Optionnel) Sélectionner les utilisateurs à ne pas surveiller.



4. Sélectionner les DC sur lesquels installer l'agent. Au moins un DC doit être sélectionné.

Le mode polling n'installera pas d'agent DC.
Redémarrer le serveur.



HEH.be Sciences et technologies

Configuration FSSO

- Installation des agents "collector"
 1. Exécuter en tant qu'admin.
 2. Compléter le nom d'utilisateur
 - DomainName\UserName
 3. Sélectionner quels événements le collecteur doit surveiller
 - "User logon events"
 - "NTLM authentication"
 4. Sélectionner la méthode d'accès
 - Standard / advanced

WALLONIE-BRUXELLES
ENSEIGNEMENT

Fortinet Single Sign On Agent

User name must be in form DomainName\UserName. If you want to use local user account, please enter \UserName.

User Name: Administrator

Password: *****

Install Options

Fortinet Single Sign On Agent could be set up to monitor user logon events and/or serving NTLM authentication requests from Fortigates. Select the proper options below.

Monitor User logon events and send the information to FortiGate.

Serve NTLM authentication requests coming from FortiGate.

Please select the access method of Windows Directory

Standard (e.g domain\user)
Select this option for easy setup, works for most situations

Advanced (e.g. CN=user,OU=Sales,DC=domain,DC=com)
Select this option if you setup LDAP access to Windows AD to retrieve user/group information from FortiGate

Back Next Cancel

460

HEH.be Sciences et technologies

Configuration FSSO

- Configuration des agents collecteur

Activer le monitoring des événements de connexion des utilisateurs

Activer ou désactiver l'authentification NTLM

Ports d'écoute par défaut du Fortigate et de l'agent DC

Configuration des logs (voir plus loin)

Activer l'authentification entre FortiGate et l'agent collecteur

Configuration des minuteurs

Fortinet Single Sign On Agent Configuration

Collector Agent Status: RUNNING

Common Tasks

Listening ports

FortiGate: 8000 DC Agent: 8002

Logging

Log level: Warning Log file size limit(MB): 10 View Log

Logon events in separate logs View Logon Events

Authentication

Require authenticated connection from FortiGate Password: *****

Timers

Workstation verify interval (minutes): 5

Dead entry timeout interval (minutes): 480

IP address change verify interval (seconds): 60

Cache user group lookup result Cache expire in (minutes): 60 Clear Group Cache

Advanced Settings Save&Close Apply Default Help

WALLONIE-BRUXELLES
ENSEIGNEMENT

Fortinet Single Sign On Agent

User name must be in form DomainName\UserName. If you want to use local user account, please enter \UserName.

User Name: Administrator

Password: *****

Install Options

Fortinet Single Sign On Agent could be set up to monitor user logon events and/or serving NTLM authentication requests from Fortigates. Select the proper options below.

Monitor User logon events and send the information to FortiGate.

Serve NTLM authentication requests coming from FortiGate.

Please select the access method of Windows Directory

Standard (e.g domain\user)
Select this option for easy setup, works for most situations

Advanced (e.g. CN=user,OU=Sales,DC=domain,DC=com)
Select this option if you setup LDAP access to Windows AD to retrieve user/group information from FortiGate

Back Next Cancel

461

Configuration FSSO

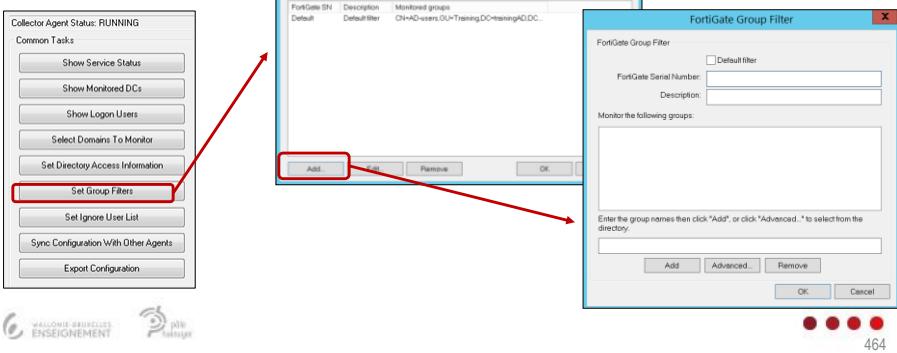
- Configuration des minuteurs (collecteur)
 - Workstation verify interval
 - Intervalle de temps entre deux vérifications (si un utilisateur est toujours connecté).
 - Par défaut : 5 minutes.
 - Désactivation : régler la valeur sur 0.
 - Le statut de l'utilisateur devient "not verified" si le collecteur ne peut pas se connecter au poste de travail pour faire la vérification
 - IP address change verify interval
 - Vérifie les IP et met à jour le FortiGate lorsque les adresses IP des utilisateurs changent (Environnement DHCP).
 - Le serveur DNS doit mettre à jour rapidement les modifications d'IP en cas de modification d'IP.
 - Par défaut = 60 secondes.

Configuration FSSO

- Configuration des minuteurs (collecteur) (suite)
 - Dead entry timeout
 - Si le statut est *not verified*, ce timer démarre.
 - Utilisé pour purger les informations de connexion non vérifiée.
 - Pour un Fortigate, toutes les entrées sont valides (vérifiée ou non).
 - Par défaut : 480 minutes (8h).
 - Désactivation : régler la valeur sur 0 → Le statut est toujours *log on*.
 - Cache users group
 - L'agent collecteur met en cache l'appartenance à un groupe d'utilisateurs pendant une période de temps définie.
 - Pendant cette période, il n'est pas mis à jour, même si l'utilisateur change de groupe dans l'AD.

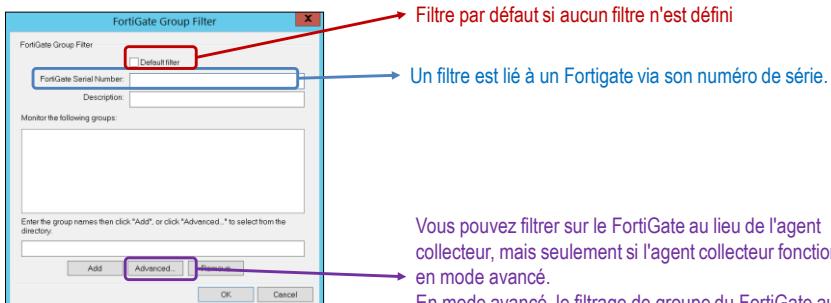
Configuration FSSO

- Configuration des filtres de groupe (collecteur)
 - Permet de définir quelles informations de connexion sont envoyées à quel FW
 - Surveiller trop d'informations (grande structure AD) est inefficace et consomme des ressources.



Configuration FSSO

- Configuration des filtres de groupe (collecteur) (suite)



Vous pouvez filtrer sur le FortiGate au lieu de l'agent collecteur, mais seulement si l'agent collecteur fonctionne en mode avancé.
En mode avancé, le filtrage de groupe du FortiGate aura la priorité sur le filtre défini sur l'agent collecteur

HEH.be
Sciences
et technologies

Configuration FSSO

- Ignored User List
 - Les événements de connexion qui correspondent aux entrées de cette liste ne sont pas enregistrés par l'agent collecteur.
 - Par exemple, il est intéressant d'y ajouter les comptes des services réseau.

Ajout manuel d'un nom

Ajout d'un nom ou d'une OU via une liste

Collector Agent Status: RUNNING
Common Tasks
Show Service Status
Show Monitored DCs
Show Logon Users
Select Domains To Monitor
Set Directory Access Information
Set Ignore List
Sync Configuration With Other Agents
Export Configuration

WALLONIE-BRUXELLES
ENSEIGNEMENT

Pré
Présage

466

HEH.be
Sciences
et technologies

Configuration FSSO

- AD Group Support
 - Tous les types de groupes ne sont pas pris en charge, les groupes supportés pour le filtrage sont :
 - Les groupes de sécurité (Security groups).
 - Les groupes universels (Universal groups).
 - Les groupes à l'intérieur des unités d'organisation (OU).
 - Les groupes locaux ou universels qui contiennent des groupes universels de domaines enfants (uniquement avec le catalogue global).
- Utilisateurs ne faisant pas partie d'un groupe d'utilisateurs FSSO
 - Authentification passive uniquement
 - Tous les utilisateurs qui n'appartiennent à aucun groupe FSSO sont automatiquement inclus dans le groupe d'invités SSO_guest_user (créé par défaut).
 - Authentifications active et passive activées
 - Les utilisateurs qui n'appartiennent à aucun groupe FSSO seront invités à entrer leurs identifiants.

WALLONIE-BRUXELLES
ENSEIGNEMENT

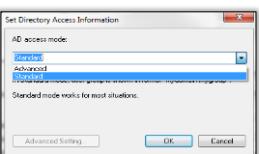
Pré
Présage

467

HEH.be Sciences et technologies

Configuration FSSO

- AD Access Mode Configuration**
 - Permet de définir comment l'agent collecteur accède et recueille l'information sur les utilisateurs et les groupes d'utilisateurs.



Mode d'accès standard

- Utilise la convention Windows-NetBIOS : `Domain\username`
- Les profils de sécurité peuvent être appliqués uniquement à des groupes d'utilisateurs.
- Les groupes imbriqués ne sont pas supportés.
- Filtres de groupe uniquement sur l'agent collecteur.

Mode d'accès avancé

- Utilise la convention LDAP : `CN=User, OU=Name, DC=Domain`
- Les profils de sécurité peuvent être appliqués aux utilisateurs ou aux groupes (imbriqués).
- Supporte les filtres de groupe sur le Fortigate ou sur l'agent collecteur.

• • • 468

HEH.be Sciences et technologies

Dépannage

- Journalisation des événements FSSO**
 - Les logs liés au FSSO sont générés à partir des événements d'authentification.

User	Action	Message
ADUSER1	authentication	User ADUSER1 succeeded in logout
ADUSER1	FSSO-logoff	FSSO-logoff event from TrainingDomain: user ADUSER1 logged off 10.0.1.10
ADUSER1	FSSO-logon	FSSO-logon event from TrainingDomain: user ADUSER1 logged on 10.0.1.10

Log & Report > System Events > User Event

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication successful
43017	Notification	NTLM authentication failed

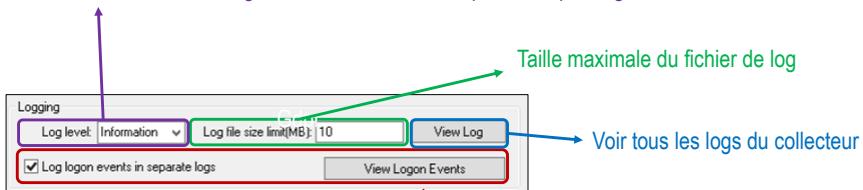
• • • 469

Dépannage

- Configuration des logs au niveau du collecteur

Niveau de log

Le niveau information est généralement celui utilisé pour le dépannage.



Si "Log logon events in separate logs" est coché,
"View logon events" permet de voir uniquement les logs liés aux événements de connexion.

Dépannage

- Affichage des utilisateurs "FSSO" connectés

```
# diagnose debug authd fssso 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: GROUP3AD/USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logons listed: 2, filtered: 0
----end of FSSO logons ---
```

A green arrow points from the IP address '192.168.1.1' to the text 'Adresse IP et nom de l'utilisateur'. A blue arrow points from the 'User' field 'STUDENT' to the text 'Groupe de l'utilisateur'. A red box highlights the 'User' field 'STUDENT' and the 'Groups' field 'GROUP3AD/USERS'. A purple arrow points from the 'Workstation' field 'WIN-INTERNAL' to the text 'Nom du poste de travail de l'utilisateur'. A red arrow points from the 'MemberOf' field 'Training' to the text 'Groupe créé sur le Fortigate auquel on a mappé le groupe de l'AD'.

Dashboard > Users & Devices > Firewall Users

User Name	User Group	Duration	IP Address	Traffic Volume	Method
ADUSER1	Training	3 minutes 51 seconds	10.0.1.10	8.65 MB	Fortinet Single-Sign-On
ADUSER1	Training			0 B	Fortinet Single-Sign-On

A red box highlights the 'Refresh' button. A red arrow points from the 'User Group' field 'Training' to the text 'Groupe créé sur le Fortigate auquel on a mappé le groupe de l'AD'. A red box highlights the 'User Group' field 'Training' and the 'Members' field 'TRAININGAD/AD-USERS'. A red box highlights the 'Group Type' field 'Fortinet Single-Sign-On (FSSO)'.

HEH.be Sciences et technologies

Dépannage

- Affichage des utilisateurs "FSSO" connectés

```
# diagnose debug authd fssso 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: GROUP3AD/USERS
Workstation: WIN-INTERNAL MemberOf: Training

Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
```

Adresse IP et nom de l'utilisateur

Groupe de l'utilisateur

Nom du poste de travail de l'utilisateur

Groupe créé sur le Fortigate auquel on a mappé le groupe de l'AD

Dashboard > Users & Devices > Firewall Users

Show all FSSO Logons

execute fssso refresh

User Group	Members	Group Type
Training	TRAININGAD/AD-USERS	Fortinet Single Sign-On (FSSO)

472

HEH.be Sciences et technologies

Dépannage

- Vérifier la connectivité entre agents collecteurs et FortiGate

```
# diagnose debug enable
# diagnose debug authd fssso server-status
```

Server Name	Connection Status	Version
TrainingDomain	connected	FSSO 5.0.0.0275

WALLONIE-BRUXELLES ENSEIGNEMENT

FortiGate

473

- Vérifier l'état du « polling » fait par le Fortigate (agentless mode)

```
# diagnose debug fssso-polling detail
```

Fréquence de polling

```
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
```

Statistiques

```
# diagnose sniffer packet any 'host ip address and tcp port 445'
```

```
# diagnose debug application fssod -1
```

Activer le débogage en temps réel en mode sans agent.
fssod = le démon du mode polling

Permet de sniffer le trafic de polling du Fortigate (en mode sans agent).

Chapitre 11

ZTNA

Zero Trust Network Access

Introduction ZTNA

- **Objectifs**

- Comprendre le principe du Zero Trust
- Comprendre les avantages de l'utilisation de Zero Trust Network Access (ZTNA)
- Comprendre les principes fondamentaux de ZTNA
- Comprendre comment établir l'identité d'un dispositif et la confiance
- Comprendre l'authentification basée sur un certificat SSL
- Configurer l'accès ZTNA sur FortiOS
- Décrire les types de configuration ZTNA

Introduction ZTNA

- **Zero trust (ZT), Zero Trust Architecture (ZTA), Zero Trust Access (ZTA)**

- **Le modèle zéro confiance**

- Modèle stratégique de cybersécurité qui part du principe qu'il n'existe aucune zone de confiance : il faut toujours vérifier.
 - Aucun utilisateur ni terminal n'est considéré comme étant de confiance (trusted) tant que son identification et son accréditation n'ont pas été minutieusement vérifiées.
- **Zero Trust est basé sur un ensemble de technologies existantes telles que**
 - le contrôle d'accès,
 - l'authentification (multifacteur - MFA),
 - la segmentation,
 - la vérification continue des utilisateurs et des appareils,
 - la surveillance du réseau,
 - le principe du moindre privilège,
 - ...
- **Aucune confiance implicite et aucun privilège n'est accordé par défaut**
 - Même si l'utilisateur se connecte depuis l'intérieur de l'entreprise avec un PC de l'entreprise.

Introduction ZTNA

- **Zero trust (suite)**

- **Aucune transaction n'est autorisée sans confiance**

- Aucun utilisateur ni terminal n'est autorisé à accéder à une ressource (fichier, application, ...) tant qu'il n'est pas considéré comme étant de confiance.
 - Peu importe sa localisation (réseau interne de l'entreprise, télétravail, ...) et celle de la ressource (LAN, DMZ, cloud, ...)
 - Peu importe s'il a déjà eu un accès auparavant.

- **La confiance est obtenue après vérification d'un ensemble de paramètres**

- Les paramètres peuvent être basés sur l'identité (authentification de l'utilisateur et/ou du terminal) et le contexte (posture check : présence d'un antivirus, localisation, ...).

- **L'accès accordé après vérification est limité (Least privilege)**

- L'accès peut être donné à une seule ressource et pendant un temps limité.

- **La confiance n'est pas conservée**

- Des vérifications sont effectuées continuellement, et pas seulement une fois.
 - L'accès peut être révoqué en cours de session si l'état de sécurité change.

Introduction ZTNA

- **Le NIST définit 7 principes sur lesquels repose une architecture ZTA**

1. **Données, services et équipements sont des ressources**

- L'accès et les actions sur une ressource doivent être systématiquement contrôlés et supervisés.

2. **Toutes les communications devraient être sécurisées**

- Les communications doivent être sécurisées (certificat, chiffrement), indépendamment de l'emplacement des ressources.

3. **Chaque tentative d'accès à une ressource devrait être vérifiée et évaluée**

- Il faut définir des habilitations et contrôler les accès sur base de ces habilitations.
 - RBAC : Role-Based Access Control.
 - Les utilisateurs doivent être authentifiés et disposer uniquement des droits nécessaires à leurs fonctions, ni plus ni moins (principe du moindre privilège).

Introduction ZTNA

4. L'accès à une ressource devrait être soumis à une politique d'accès dynamique
 - **Dynamique**
 - Le niveau de sécurité nécessaire pour accéder à chaque ressource doit pouvoir s'adapter en fonction du contexte dans lequel se trouve l'utilisateur.
 - **Le contexte peut être fonction de :**
 - L'identité du client, du service ou de la ressource demandée.
 - L'état du client demandant l'accès (versions installées, certificat, indices de compromission, ...)
 - Les attributs comportementaux (première fois que la connexion est demandée depuis un pays étranger, ...)
 - Les attributs d'environnement (localisation réseau, date de la requête, ...)

Introduction ZTNA

5. Un système de surveillance de l'intégrité et du niveau de sécurité en temps réel devrait être implémenté
 - Idéalement, l'intégralité des composants du réseau doit être surveillée afin de détecter rapidement tout comportement suspect ou anormal.
 - **CDM**
 - Continuous Diagnostics and Mitigation. Un système de diagnostic et d'atténuation des risques en continu doit être mis en place pour surveiller l'état des appareils et des applications et appliquer les correctifs nécessaires.
 - **SOC**
 - Le Security Operations Center est une équipe de professionnels de la sécurité informatique qui surveille l'ensemble de l'infrastructure informatique d'une entreprise, 24h/24 et 7j/7, afin de détecter les événements de cybersécurité en temps réel et y faire face aussi rapidement et efficacement que possible.
 - **SIEM**
 - Le Security Information Event Management collecte les données des journaux d'événements à partir de sources diverses, identifie les activités qui s'écartent de la norme grâce à une analyse en temps réel et applique les mesures appropriées.

Introduction ZTNA

6. Les mécanismes d'authentification et d'autorisation devraient être dynamiques et strictement appliqués avant qu'un accès soit autorisé
 - L'entreprise devrait disposer d'un système de gestion des identités, des habilitations et des accès et d'un système de gestion des actifs.
 - ICAM : Identity, Credential, and Access Management.
 - IAM : Identity and Access Management.
 - L'entreprise devrait mettre en place une surveillance continue avec réauthentification et réautorisation éventuelles tout au long des transactions.
7. L'entreprise devrait assurer une supervision constante de la sécurité
 - L'entreprise doit collecter le maximum d'informations possibles sur le niveau de sécurité des actifs, l'infrastructure réseau et les communications en cours.
 - La traçabilité et l'exploitation continue des informations collectées doivent servir à l'amélioration constante de la sécurité du SI.

Introduction ZTNA

- **ZTNA : Zero Trust Network Access**
 - **ZTNA est une fonctionnalité de Zero Trust Access (ZTA) qui se concentre sur le contrôle d'accès aux applications**
 - ZTNA de Fortinet n'accorde l'accès **par session** à une application qu'après vérification de différents paramètres.
 - Périphérique, utilisateur, contexte.
 - Le contrôle s'effectue à chaque nouvelle session.
 - Car entre cette session et la précédente, le PC s'est peut-être fait infecter ou voler.
 - **Le processus de contrôle s'effectue indépendamment de l'emplacement du client et de la ressource.**
 - Indépendamment dans le sens où des contrôles sont effectués peu importe la localisation, mais ces contrôles peuvent être différents selon l'environnement.
 - Par exemple, un accès peut nécessiter une authentification 2FA depuis l'extérieur mais pas depuis l'intérieur de l'entreprise.

Introduction ZTNA

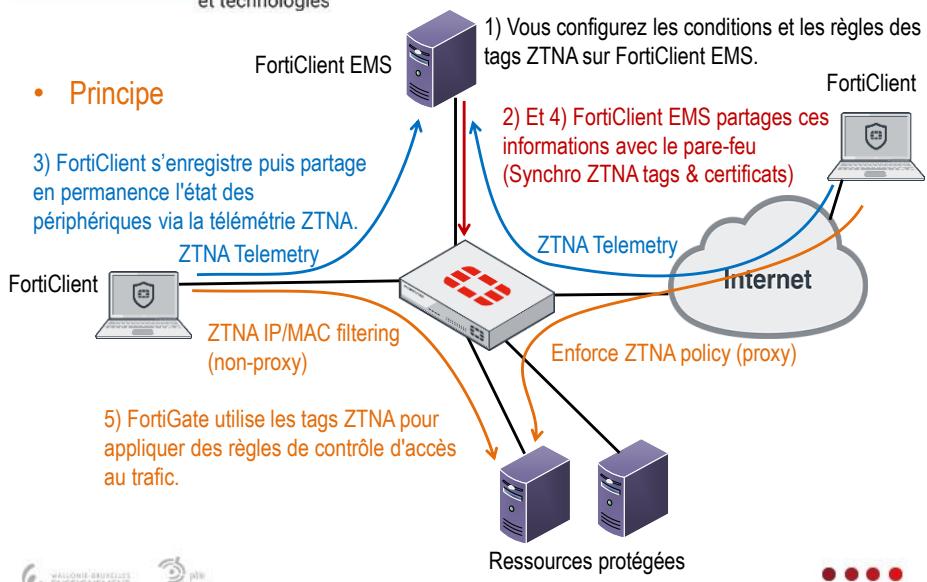
- ZTNA : Zero Trust Network Access (suite)

- Fortinet ZTNA contrôle les accès en :

- Vérifiant l'identité des périphériques client (Via des certificats).
 - Authentifiant l'identité de l'utilisateur (MFA supporté).
 - Vérifiant l'autorisation de l'utilisateur (Habilitations, RBAC).
 - Vérifiant la posture en fonction du contexte.
 - Réalisant des contrôles basés sur des attributs et contextes définis dans des tags zéro confiance (Zero-trust tags).
 - Par exemple, ZTNA peut vérifier : la localisation, présence d'un antivirus, d'un certificat, d'une connexion à FortiClient EMS, la présence d'un fichier spécifique, d'un OS spécifique, d'une connexion à un domaine AD, etc.

Introduction ZTNA

- Principe



Introduction ZTNA

- **Deux modes ZTNA**

1. **ZTNA access proxy (Le proxy d'accès ZTNA)**

- Utilisé pour permettre aux utilisateurs d'accéder aux ressources par le biais d'un proxy en SSL.
 - Un proxy HTTP pour les applications Web.
 - Un TFAP (TCP Forwarding Access Proxy) pour les autres applications supportées (SSH, RDP, ...).
- Simplifie l'accès à distance en éliminant l'utilisation d'un dial-up VPN.
- Des règles ZTNA et le balisage (ZTNA tag) offrent un contrôle supplémentaire des utilisateurs et des périphériques clients.

Introduction ZTNA

2. **ZTNA IP/MAC filtering (ZTNA secure access)**

- Ce contrôle d'accès est typiquement utilisé lorsque les terminaux sont physiquement situés dans le réseau de l'entreprise.
- Utilise les règles et les tags ZTNA pour mettre en œuvre un accès zéro confiance basé sur les rôles.
 - Ce contrôle d'accès combine les adresses IP/MAC (règles de pare-feu) avec des tags ZTNA pour l'identification et le contrôle de la posture de sécurité.
 - Ce mode ne nécessite pas l'utilisation du proxy d'accès

Les équipements et leurs rôles

- **FortiClient**

- Solution de sécurité pour les périphériques clients
 - FortiClient permet à chaque appareil - local ou distant, fixe ou mobile - de s'intégrer à FortiClient EMS.
 - Plusieurs plates-formes supportées :
 - Windows, Mac OS, Linux, iOS, les appareils mobiles Android et Chromebook.
 - FortiClient peut être utilisé soit avec FortiClient EMS uniquement, soit dans la Security Fabric.

ZTNA Edition
✓ Zero Trust Agent
✓ Central Management via EMS
✓ Central Logging & Reporting
✓ Dynamic Security Fabric Connector
✓ Vulnerability Agent & Remediation
✓ SSL VPN with MFA
✓ IPSEC VPN with MFA
✓ FortiGuard Web & Video Filtering
✓ ZTNA Application Access control

EPP/APT Edition
All the Features of ZTNA Edition plus:
✓ SSL Inspection
✓ Inline AV & Anti-Malware
✓ Intrusion Prevention (IPS)
✓ FortiGuard Web & Video Filtering
✓ DNS Security
✓ USB Device Control



488

Les équipements et leurs rôles

- **FortiClient (suite)**

- Fournit des informations au FortiClient EMS lorsqu'il s'y enregistre :
 - Informations sur le client (réseau, système d'exploitation, version, etc.).
 - Informations sur l'utilisateur connecté.
 - Informations sur l'état de la sécurité (dans ou en dehors de la Security Fabric, antivirus à jour et activé, vulnérabilités détectées, etc.).
- Demande et obtient un certificat de périphérique client
 - Demande et obtient un certificat de périphérique client auprès de l'autorité de certification EMS ZTNA lors de sa première tentative de connexion.
 - Vous ne pouvez pas utiliser les fonctionnalités de FortiClient tant que celui-ci n'est pas connecté à FortiClient EMS et qu'il n'a pas de licence.
 - Le client utilisera ce certificat pour s'identifier auprès d'un FortiGate.
- Est configuré via le profil de sécurité que l'administrateur a configuré dans FortiClient EMS.

Les équipements et leurs rôles

- **FortiClient EMS**

- Solution de gestion centralisée de FortiClients

- Permet de configurer de manière centralisée des profils de sécurité avec lesquels les FortiClients seront approvisionnés.
 - Vous pouvez y créer, modifier et supprimer des règles d'étiquetage zéro confiance.
- Permet l'administration des connexions des terminaux FortiClient
 - Acceptation, déconnexion et blocage des terminaux.
- Il apporte une visibilité sur l'ensemble des FortiClients du réseau
 - L'état, le système (versions obsolètes?), les règles, les exceptions, la sécurité,...
- Il comprend des fonctions d'automatisation pour la gestion des périphériques et le dépannage.
- Dans une architecture ZTNA, vous ne pouvez modifier les configurations d'un FortiClient qu'à partir du FortiClient EMS.

Les équipements et leurs rôles

- **FortiClient EMS (suite)**

- Émet et signe le certificat du FortiClient

- Avec l'UID du FortiClient, le numéro de série du certificat et le numéro de série de l'EMS.
- FortiClient EMS synchronise ensuite le certificat Client avec le FortiGate.
- FortiClient EMS partage son certificat EMS ZTNA CA avec le FortiGate.
 - Afin que les FortiGates puissent l'utiliser pour authentifier les certificats clients.

Les équipements et leurs rôles

- FortiClient EMS (suite)

- Utilise des règles Zero Trust pour étiqueter les clients (tag) en fonction des informations dont il dispose sur chaque client.
 1. EMS envoie des règles zéro confiance aux périphériques client.
 2. Le FortiClient vérifie les clients à l'aide des règles zéro confiance fournies et envoie les résultats à EMS.
 3. EMS regroupe dynamiquement les clients à l'aide du tag configuré pour chaque règle.
 4. EMS synchronise les balises ZTNA avec les FortiGates.
- Met à jour les informations relatives aux clients lorsque celles-ci changent
 - Synchronise ces mises à jour avec les FortiGates.

EMS > Zero-trust Tags > zero-trust Tagging Monitor

Endpoint with Tag					Refresh
Remote-Endpoints (1)					
Endpoint	User	OS	IP	Tagged on	
Remote-Client	Administrator	Microsoft Windows Ser...	10.0.2.20	2021-08-25 02:43:06	

• • • 492

Introduction ZTNA

- Les équipements et leur rôle (suite)

- FortiGate

- Maintient une connexion continue avec FortiClient EMS

- Afin de synchroniser les informations sur les clients (l'UID du FortiClient, le SN du certificat client, le SN du FortiClient EMS, les détails du réseau (adresses IP et MAC), etc.)

- Vérification des sessions actives ZTNA

- Changements de posture des terminaux clients

- Ils déclenchent la revérification des sessions actives.

- Si le terminal n'est plus conforme aux règles ZTNA, la session est interrompue.

- Les tags ZTNA sont mis à jour par le FortiClient EMS

- FortiGate surveille ces mises à jour. En cas de changement, les sessions ZTNA actives doivent à nouveau correspondre à la politique ZTNA.

- Changements des règles ZTNA

- Les modifications apportées aux règles ZTNA déclenchent également une nouvelle vérification de l'appareil client par rapport à la politique.

Les équipements et leurs rôles

- ZTNA avec ou sans client (client and clientless ZTNA)

- Client-initiated, endpoint-initiated

- Le modèle ZTNA initié par le client utilise un agent sur les clients (Par exemple, FortiClient).
 - Avantages
 - Fonctionne que vous accédez à des ressources dans le cloud ou sur site.
 - Offre une meilleure visibilité et un meilleur contrôle des appareils.

- Service-initiated, clientless

- Le modèle ZTNA initié par le service ou "sans client" utilise une architecture de reverse proxy.
 - Pas d'agent sur les clients mais un plug-in de navigateur pour créer un tunnel sécurisé et effectuer l'évaluation de l'appareil et la vérification de la posture.
 - Il ne prend généralement en charge que les applications basées sur HTTP/HTTPS.
 - Plutôt que de résider localement, le logiciel doit être téléchargé à chaque connexion, ce qui ralentit et dégrade l'expérience de l'utilisateur.
 - N'offre pas le même niveau de contrôle ou de visibilité qu'un agent
 - Or un élément important de ZTNA consiste justement à évaluer la posture de l'appareil et son état de vulnérabilité.

Configuration ZTNA

- Zero-Trust tagging rules

- Configuration des règles de balisage Zéro confiance sur FortiClient EMS

Zero-trust Tags > Zero-trust Tagging Rules > + Add

Name	Tag	Enabled	Comments
Corporate Linux Endpoints	Corporate Linux	Enabled	
Finance	Finance	Enabled	
TAG_ANTIVIRUS_ON	TAG_ANTIVIRUS_ON	Enabled	
Windows_Customer_Service	Windows_Customer_Service	Enabled	
Windows_Marketing	Windows_Marketing	Enabled	

Configuration ZTNA

- Zero-Trust tagging rules (suite)
 - Configuration des règles de balisage zéro confiance sur FortiClient EMS

Zero-trust Tags > Zero-trust Tagging Rules

The screenshot shows the 'Zero-trust Tagging Rules' configuration interface. It includes fields for 'Name' (HQ-safe), 'Tag Endpoint As' (HQ-safeRange), and 'Enabled' status. A 'Comments' field is also present. The 'Rules' section displays two configured rules for Windows devices. The 'Rule Logic' dropdown at the bottom indicates a logical OR condition between the two rules.

- Choisissez un tag existant ou entrer un nouveau tag.
EMS utilise ce tag pour regrouper dynamiquement les clients qui satisfont à la règle.
 - Cliquez sur Add Rule pour créer la règle (voir diapositive suivante).
 - Affichage des règles créées
Par défaut, un terminal doit satisfaire à toutes les règles configurées.
« Rule Logic » permet de modifier ce comportement par défaut.
- 496

Configuration ZTNA

- Zero-Trust tagging rules (suite)

The screenshot shows the 'Add New Rule' dialog. It includes a note about compatibility with FortiClients 6.2.1 and below. The 'OS' dropdown is set to 'Windows'. The 'Rule Type' dropdown is set to 'AD Group'. The 'AD Group' dropdown shows the option 'NOT Domain Computers'. There are also 'Save' and 'Cancel' buttons.

Le choix de l'OS détermine les types de règles disponibles.
Le type de règle choisi détermine les options possibles

AD Group
AD Group
AntiVirus Software
Certificate
EMS Management
File
Logged in Domain
Registry Key
Running Process
OS Version
Sandbox Detection
User Identity
Vulnerable Devices
Windows Security

HEH.be Sciences et technologies

Configuration ZTNA

- Zero Trust tag monitor
 - Menu de l'EMS affichant toutes les règles zero trust.

WALLONIE-BRUXELLES
ENSEIGNEMENT

Pré
Présage

498

HEH.be Sciences et technologies

Configuration ZTNA

- Gestion des certificats sur le FortiClient EMS
 - Default_ZTNARootCA
 - FortiClient EMS dispose d'un certificat racine par défaut.
 - La CA ZTNA utilise ce certificat racine pour signer les CSR des terminaux FortiClient.
 - Vous pouvez révoquer tous les certificats ou le certificat individuel d'un FortiClient.

Le bouton d'actualisation permet de révoquer et mettre à jour l'autorité de certification racine.

Cela oblige à mettre à jour les FortiGate et FortiClient en générant de nouveaux certificats pour chaque client.

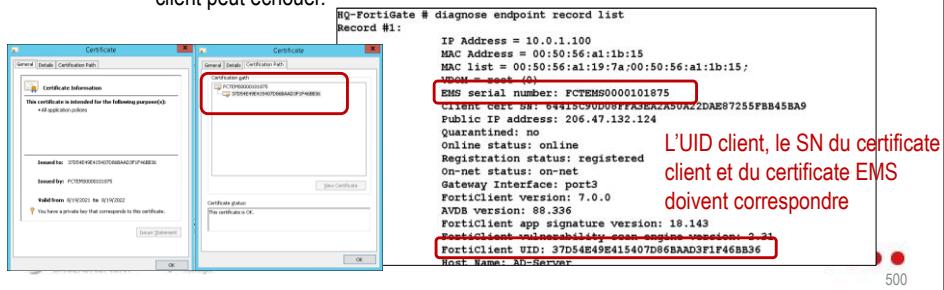
WALLONIE-BRUXELLES
ENSEIGNEMENT

Pré
Présage

499

Configuration ZTNA

- Gestion des certificats sur le FortiClient EMS (suite)
 - Certificats
 - Sous Windows, les certificats sont installés directement dans le magasin de certificats.
 - Sur d'autres systèmes d'exploitation, consultez la documentation du fournisseur.
 - FortiGate
 - Les informations du certificat dans le magasin du client doivent correspondre aux informations du FortiClient EMS et du FortiGate sinon l'authentification du certificat client peut échouer.



Configuration ZTNA

- Authentification par certificat
 - Obtention du certificat client
 - Lorsqu'il s'enregistre auprès du FortiClient EMS, le FortiClient soumet automatiquement une demande CSR.
 - Le FortiClient EMS signe et renvoie le certificat client.
 - Ce certificat est stocké dans le magasin de certificats du système d'exploitation pour les connexions ultérieures.
 - Les informations sur les terminaux sont synchronisées avec FortiGate et FortiClient EMS.
 - Actuellement, ZTNA prend en charge les navigateurs Microsoft Edge et Google Chrome.
 - Révocation du certificat client
 - Lorsqu'un client se déconnecte ou est désenregistré de FortiClient EMS, son certificat est supprimé du magasin de certificats et révoqué sur FortiClient EMS.

Configuration ZTNA

- **Authentification par certificat (suite)**
 - Par défaut, l'authentification du certificat client est activée sur le proxy d'accès
 - Lorsque le FortiGate reçoit la requête HTTPS, le processus WAD demande au client de s'identifier à l'aide de son certificat.
 - Si le client répond avec le bon certificat, l'UID du client et le SN du certificat peuvent être extraits :
 - Si l'UID du client et le SN du certificat correspondent à l'enregistrement du FortiGate, le client est autorisé à poursuivre le traitement de la règle de proxy ZTNA.
 - Si l'UID du client et le certificat SN ne correspondent pas à l'enregistrement du FortiGate, le client est empêché de poursuivre le traitement de la règle de proxy ZTNA.
 - Si le client annule et répond avec un certificat client vide,
 - Le client est autorisé à poursuivre si l'option *empty-cert-action* est configurée sur *accept*. Sinon, FortiGate bloque le client et l'empêche de poursuivre.

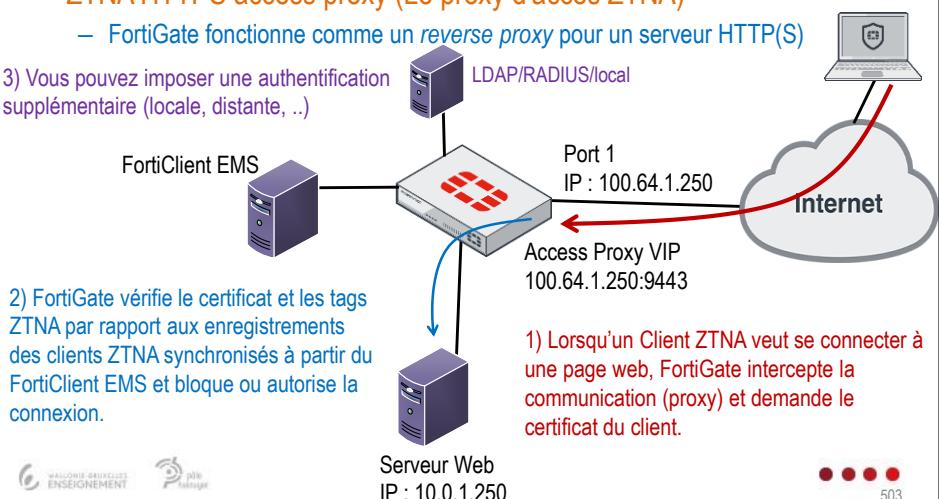
```
config firewall access-proxy
  edit <name>
    set client-cert enable
    set empty-cert-action block
```

...
502

Configuration ZTNA

- **ZTNA HTTPS access proxy (Le proxy d'accès ZTNA)**
 - FortiGate fonctionne comme un *reverse proxy* pour un serveur HTTP(S)

3) Vous pouvez imposer une authentification supplémentaire (locale, distante, ..)

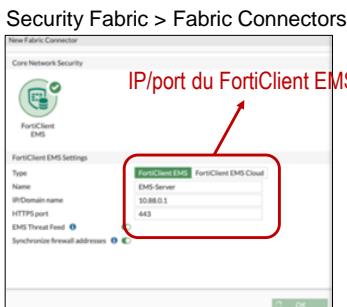


Configuration ZTNA

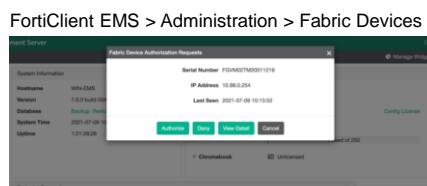
- Configuration ZTNA HTTPS access proxy
 - Configuration à réaliser sur le FortiGate
 - Connecteur Security Fabric FortiClient EMS
 - Le FortiGate maintient une connexion continue avec le serveur EMS pour synchroniser les informations sur les terminaux et les balises ZTNA.
 - Serveur ZTNA
 - Il définit l'adresse VIP du proxy d'accès et les serveurs réels auxquels les clients peuvent se connecter.
 - Règles ZTNA
 - Permet de définir des tags ou des groupes de tags ZTNA pour appliquer l'accès basé sur le rôle.
 - Vous pouvez également configurer des profils de sécurité pour protéger ce trafic.
 - [Optionnel] Authentification
 - ZTNA prend en charge les méthodes HTTP et SAML.

Configuration ZTNA

- Configuration ZTNA HTTPS access proxy (suite)
 - Configurer la connexion entre FortiGate et FortiClient EMS
 - FortiGate utilise un connecteur Fabric pour se connecter au FortiClient EMS.



- Le FortiGate doit être autorisé sur le FortiClient EMS.



HEH.be Sciences et technologies

Configuration ZTNA

- Configuration ZTNA HTTPS Access Proxy (suite)
 - Configurer un serveur ZTNA (proxy d'accès)
 - Définir l'adresse VIP du proxy d'accès et le serveur réel auquel les clients peuvent se connecter.

Policy & Objects > ZTNA > ZTNA Servers

Access proxy VIP (les clients envoient leurs requêtes vers cette adresse).

Définition des correspondances (mappages) entre des hôtes virtuels et les serveurs réels.

Voir diapositive suivante

506

HEH.be Sciences et technologies

Configuration ZTNA

- Configuration ZTNA HTTPS Access Proxy (suite)

Adresse et port réel du serveur Web

Service	HTTPS
Virtual Host	Any Host Specify
Match by	Substring Wildcard
Host	www.example2.com
Use certificate	Fortinet_CA_SSL
Match path by	Substring Wildcard Regular Expression
Path	/map1

Servers		
+ Create New	Edit	Delete
IP	Port	Status
10.0.1.250	443	Active

507

HEH.be Sciences et technologies

Configuration ZTNA

- Configuration ZTNA HTTPS Access Proxy (suite)
 - Configurer les règles ZTNA
 - Permet de définir des balises et/ou des groupes de balises ZTNA afin d'appliquer le contrôle d'accès (basé sur le rôle).

Règle ZTNA autorisant les clients à accéder au serveur si ZTNA tag est satisfait

Vous pouvez aussi configurer des profils de sécurité pour protéger ce trafic.

Exemple de règle ZTNA refusant l'accès si un malware a été détecté sur le client

HEH.be Sciences et technologies

Configuration ZTNA

- Configuration ZTNA HTTPS Access Proxy (suite)
 - Configurer l'authentification

Les membres du groupe ZTNAaccess_group devront s'authentifier.

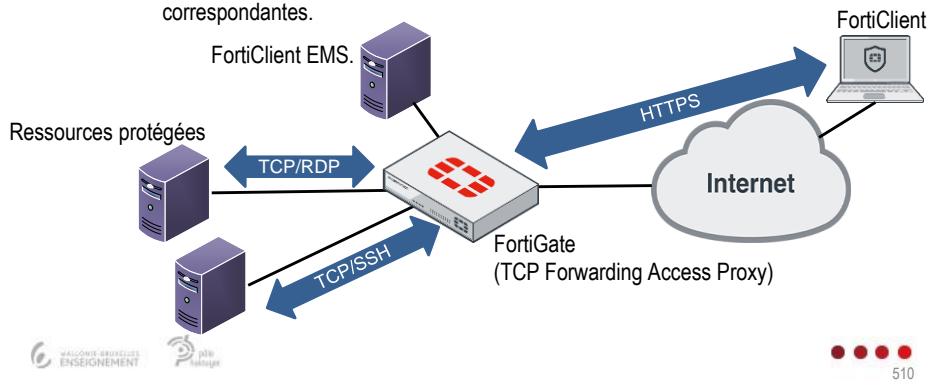
Authentification supportées : LDAP, RADIUS, Local

Configuration ZTNA

- ZTNA TCP Forwarding Access Proxy (TFAP)

- RDP, SSH, SMB

- ZTNA prend en charge les applications basées sur HTTP/HTTPS.
 - TFAP permet de transmettre le trafic RDP, SSH, SMB vers les ressources correspondantes.



Configuration ZTNA

- Configuration

- Choisir TCP forwarding, sinon les étapes sont les mêmes que pour l'access proxy (serveur, règles, authentification)

The screenshot shows the FortiGate configuration interface. In the top navigation bar, 'Policy & Objects > ZTNA > ZTNA Rules' is selected. The main pane displays a list of rules with a 'Create New' button highlighted. A detailed view of a rule is shown in a modal window:

- Edit ZTNA Server** (Type: IPv4)
 - Name: Web
 - Comments:
- Network**
 - External Interface: wan1
 - External IP: 192.168.160.198
 - External port: 8443
- Services and Servers**
 - Default certificate: Fortinet_Factory
 - Service/server mapping
- Edit Service/Server Mapping** (Type: IPv4, Service: HTTP, HTTPS, TCP Forwarding)
 - Virtual Host: Any Host
 - Servers: Web_Server (Port: 443)

Configuration ZTNA

- **ZTNA SSH Access Proxy**

- Même rôle que TFAP mais spécifiquement prévu pour le trafic SSH
 - Permet d'appliquer les contrôles ZTNA au trafic SSH.
 - Permet l'application de l'inspection approfondie du trafic SSH (SSL/SSH inspection).
 - Permet la validation de la clé d'hôte SSH du serveur (facultatif).
 - Permet l'utilisation d'une authentification utilisateur à usage unique
 - Pour ne pas devoir s'authentifier au proxy d'accès SSH ZTNA et puis au serveur SSH.

Configuration ZTNA

- **ZTNA IP/MAC-Based Access Control**

- Utilisé pour accéder à un serveur Web interne lorsque les terminaux sont physiquement situés sur le réseau de l'entreprise (On-net).

Policy & Objects > Firewall Policy

Name	Block-Malicious
Incoming Interface	port3
Outgoing Interface	port1
Source	all
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT DENY
Log Violation Traffic	
Comments	Write a comment... / 0/1023
Enable this policy	

- Ce mode ne nécessite pas l'utilisation d'un proxy d'accès.
- Permet d'utiliser les balises ZTNA pour le contrôle d'accès au niveau des règles de FW.

Select Entries

ZTNA TAG (51)
FCTEMS - IP (10)
ZTNA IP all_registered_clients
ZTNA IP EDR-Classification
ZTNA IP Endpoint_Compliance
ZTNA IP Important
ZTNA IP Infected
ZTNA IP noav
ZTNA IP noc

ZTNA vs IPsec vs SSL

- Comparaison ZTNA vs VPN

- Granularité

- Un VPN donne généralement un plus large accès aux ressources
 - Par exemple, l'accès à un réseau entier.
 - Le ZTNA traite chaque utilisateur et appareil individuellement
 - Seules les ressources auxquelles l'utilisateur et l'appareil sont autorisés à accéder sont mises véritablement à disposition.

- Visibilité

- Le VPN n'a pas conscience du trafic et de son utilisation
 - Cela rend plus difficile la visibilité de l'activité des utilisateurs et de l'utilisation des applications.
 - ZTNA est micro-segmenté
 - Il peut offrir une visibilité accrue sur l'activité des applications.
 - Cette possibilité facilite grandement la surveillance de l'état des applications, la planification des capacités, la gestion et l'audit des licences.

Introduction ZTNA

- Comparaison ZTNA vs VPN (suite)

- Sécurité

- Une architecture Zero Trust réduit considérablement la surface d'attaque
 - Car les ports et les applications sont invisibles à moins d'être authentifiés et autorisés.
 - Car il impose une vérification permanente des utilisateurs et des appareils.
 - Car il fournit un accès minimal (Least privilege) aux utilisateurs et aux appareils en fonction de leur rôle dans l'entreprise.
 - Car il n'y a pas de risque de laisser un VPN accidentellement ouvert.
 - Une architecture Zero Trust entrave considérablement les possibilités de déplacement latéral d'un pirate sur le réseau (micro-segmentation).
 - État de sécurité de l'appareil :
 - Un VPN d'accès à distance n'a aucune connaissance de l'état de fonctionnement d'un périphérique client.
 - ZTNA intègre la conformité et l'état de sécurité des appareils dans les politiques d'accès.
 - » Cette approche réduit considérablement le risque de vol ou de fuite de données.

- Comparaison ZTNA vs VPN (suite)

- Expérience utilisateur

- Les clients VPN d'accès à distance sont connus pour offrir une expérience utilisateur médiocre
 - Ajout de latence, problèmes en matière de connectivité, à quel VPN se connecter, ...
 - Avec ZTNA, l'utilisateur n'a plus besoin de savoir à quel VPN se connecter ni où se trouvent les ressources.
 - L'utilisateur clique simplement sur l'application pour obtenir une connexion sécurisée, que l'application soit sur site, dans un cloud public ou un cloud privé.
 - ZTNA établit automatiquement des connexions sécurisées à la demande, la plupart des utilisateurs ne remarqueront même pas la présence de la solution ZTNA.

- Mise en conformité

- Avec ZTNA, chaque demande d'accès est évaluée et peut être enregistrée
 - Il est donc plus facile de constituer la documentation relative à la conformité.
 - Les audits sont simplifiés, car il existe une chaîne de preuves visibles pour toutes les demandes d'accès.

- Comparaison ZTNA vs VPN (suite)

- Flexibilité et agilité

- Les VPN n'offrent pas la même granularité que les solutions ZTNA.
 - L'installation et la configuration d'un logiciel client VPN sur les terminaux de tous les utilisateurs et la configuration de multiples tunnels VPN peuvent s'avérer complexes : nœuds multiples, règles d'accès au pare-feu, gestion des adresses IP, des flux de trafic et du routage.
 - ZTNA est plus agile dans des environnements qui changent rapidement, avec des utilisateurs, des applications et des appareils qui vont et viennent.
 - Il est beaucoup plus facile d'ajouter ou de supprimer des règles de sécurité et les autorisations des utilisateurs en fonction de leurs besoins immédiats.
 - Déploiement ZTNA
 - ZTNA ne nécessite pas d'être déployé en une fois dans l'ensemble de l'infrastructure mais peut être déployé pour des groupes d'utilisateurs ou des applications spécifiques.
 - ZTNA utilise les méthodes d'authentification existantes et les méthodes d'accès aux applications natives, ce qui se traduit par une expérience utilisateur transparente.

ZTNA vs IPsec vs SSL

	VPN IPsec	VPN SSL	ZTNA
Type de tunnel	Tunnel	Tunnel	Par session
Configuré entre :	<ul style="list-style-type: none"> Forticlient-Fortigate. Browser-Fortigate FortiGate-GW VPN tiers FortiGate-client VPN tiers 	<ul style="list-style-type: none"> Forticlient-Fortigate. Browser-Fortigate FortiGate-GW VPN tiers FortiGate-client VPN tiers 	<ul style="list-style-type: none"> Browser-Fortigate Forticlient-Fortigate (TCP Forwarding Access)
Connexion via	Client IPsec	Page web sur le Fortigate FortiClient FortiGate (client SSL)	Noms d'hôte HTTPS ou IP/Port FortiClient (TCP forwarding access)
Interopérabilité	<ul style="list-style-type: none"> Standard interopérable avec plusieurs fournisseurs. 	<ul style="list-style-type: none"> Peut être spécifique au fournisseur. 	<ul style="list-style-type: none"> Peut être spécifique au fournisseur.
Utilisation courante	<ul style="list-style-type: none"> Site à site, site à agence. Data center. 	<ul style="list-style-type: none"> Télétravailleurs, Utilisateurs mobile (Internet cafés, bibliothèques, ...) Flexible ; Mode tunnel ou par session 	<ul style="list-style-type: none"> Télétravailleurs Utilisateurs locaux Uniquement par session

ZTNA vs IPsec vs SSL

	VPN IPsec	VPN SSL	ZTNA
Implémentation	<ul style="list-style-type: none"> Plus flexible. Topologies en étoile et maillée possibles. Vers client ou autre passerelle VPN. Chiffrement plus rapide car réalisé par la passerelle BPN. 	<ul style="list-style-type: none"> Configuration plus simple que IPsec Ne nécessite pas d'installation (Web only) Uniquement d'un client SSL vers un serveur SSL Aucun paramétrage requis par l'utilisateur. 	<ul style="list-style-type: none"> Configuration plus simple que IPsec Ne nécessite pas d'installation Seulement de client à FortiGate Aucun paramétrage requis par l'utilisateur. Support technique est moins sollicité
Surface d'attaque	<ul style="list-style-type: none"> Protection traditionnelle du périmètre : Protection contre les menaces externes uniquement Ne couvre pas les menaces à l'intérieur du réseau 	<ul style="list-style-type: none"> Protection traditionnelle du périmètre : Protection contre les menaces externes uniquement Ne couvre pas les menaces à l'intérieur du réseau 	<ul style="list-style-type: none"> Philosophie Zero Trust Personne à l'intérieur ou à l'extérieur du réseau ne doit être digne de confiance sans vérifications. Basée sur l'authentification systématique de l'identité.

ZTNA vs IPsec vs SSL

- **Limites du ZTNA**

- **BYOD**

- Le Zero Trust dans un lieu de travail qui s'appuie fortement sur le BYOD peut nécessiter beaucoup de travail, surtout en amont.

- **Nombre élevé d'applications**

- Un grand nombre d'applications devant être surveillées et sécurisées selon les normes Zero Trust peut rendre difficile la mise en œuvre de l'architecture ZTA.

- **Dépendance aux fournisseurs**

- La mise en œuvre du ZTNA peut entraîner une dépendance accrue vis-à-vis des fournisseurs de solutions de sécurité spécifiques.
- Cela peut limiter la flexibilité et la portabilité des infrastructures, et peut également entraîner des problèmes de compatibilité avec d'autres systèmes ou solutions.

ZTNA vs IPsec vs SSL

- **Limites du ZTNA**

- **Latence**

- Le ZTNA peut potentiellement entraîner une augmentation de la latence et une réduction des performances réseau.
- Cela est dû aux exigences de chiffrement et de déchiffrement des données, ainsi qu'à la nécessité de vérifier l'authentification de chaque utilisateur avant d'autoriser l'accès aux ressources.

- **Coût :**

- L'adoption du ZTNA peut entraîner des coûts supplémentaires, notamment pour l'achat et la configuration de solutions logicielles ou matérielles spécifiques. De plus, la gestion et la maintenance continues de l'infrastructure ZTNA peuvent nécessiter des ressources supplémentaires.

Chapitre 12

SD-WAN

Software-Defined WAN

Objectifs

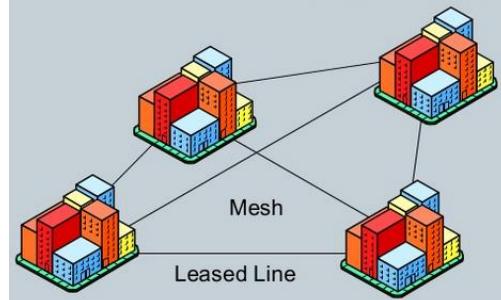
- A l'issue de ce chapitre, l'apprenant doit être capable de
 - Identifier les cas d'utilisation du SD-WAN.
 - Déterminer les exigences de mise en œuvre du SD-WAN.
 - Configurer un lien virtuel SD-WAN et l'équilibrage de charge.
 - Configurer des routes statiques et des stratégies de pare-feu pour le SD-WAN.
 - Configurer un SLA de performance SD-WAN.
 - Identifier comment les mesures FortiGate lient la qualité.
 - Identifier les critères d'appariement des règles SD-WAN.
 - Configurer la sélection dynamique des liens en fonction de la qualité des liens.

SD-WAN

- Solutions WAN (suite)

- PPP (Lignes louées)

- Utilisé pour fournir des communications point à point sur des lignes louées.
 - Circuit préétabli et permanent.
 - Bande passante fixe.
 - Très cher.



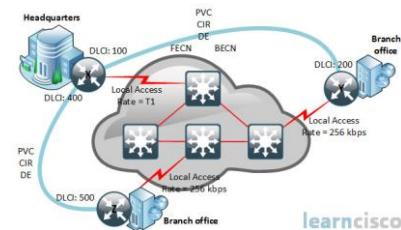
524

SD-WAN

- Solutions WAN (suite)

- Frame Relay

- Ressources partagées
 - Plusieurs circuits virtuels sont établis via les mêmes interfaces/lignes.
 - Moins chère que les lignes louées
 - Néanmoins, la solution reste chère.
 - Moins bonnes performances que les lignes louées car le partage des lignes peut provoquer de la congestion.



learnCisco

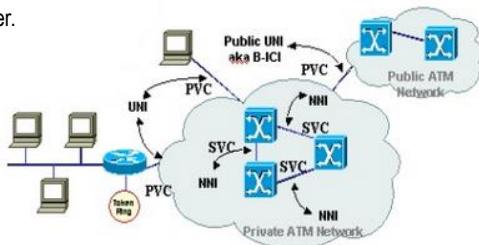
525

SD-WAN

- Solutions WAN (suite)

- ATM

- Partage des ressources (comme pour Frame Relay).
 - Commutation de cellules de petite taille (53 octets).
 - A permis d'augmenter les vitesses disponibles.
 - Plus compliqué à déployer et à gérer.
 - Reste cher.

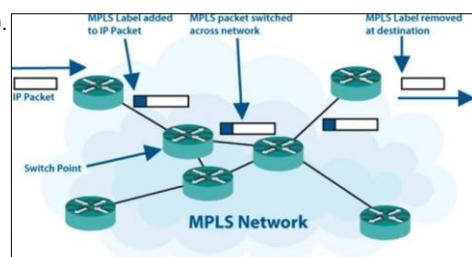


SD-WAN

- Solutions WAN (suite)

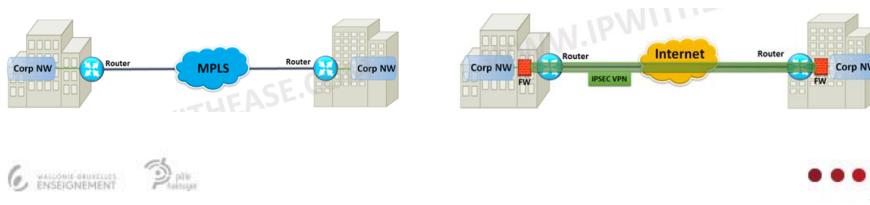
- MPLS (Multiprotocol Label Switching)

- Très bien pour interconnecter des sites (central – agences/filiales)
 - Performances fiables, QoS peut être garantie → Voix/vidéo OK.
 - Assure un cloisonnement et une sécurité des flux informatiques internes à l'entreprise.
 - Communication directe de site à site possible (Full/partial meshed).
 - Nombreux supports utilisables (DSL, câble, sans fil, fibre, ...).
 - Reste cher, surtout si nombreux sites à interconnecter.



SD-WAN

- Solutions WAN (suite)
 - VPN IP
 - Très bien pour interconnecter des sites (central – agences/filiales)
 - Communication directe de site à site possible (Full meshed).
 - Supporte de nombreux supports (E1, DSL, câble, sans fil, fibre optique).
 - Best effort : Aucune garantie sur la qualité de service, vitesses variables.
 - Beaucoup moins cher que MPLS.
 - Sécurité faible (ligne Internet publique), nécessité d'une infrastructure de sécurité (Firewall, VPN, ...).



SD-WAN

- Les challenges d'un réseau WAN
 - Internet s'est développé vers le cloud
 - Des entreprises n'utilisent plus certaines applications en local (SaaS)
 - Office 365, skype for business, ...
 - Des entreprises hébergent leurs propres services dans le cloud (IaaS)
 - Via AWS, Azure, ...
 - On veut accéder à ses applications de partout et à n'importe quel moment
 - Internet devient incontournable.
 - Les applications et les infrastructures peuvent être situées n'importe où.
 - Les modèles de trafic ont changés et changent régulièrement, il faut pouvoir s'adapter rapidement.
 - Cela rend plus difficile de garantir de bonnes performances pour les utilisateurs.

- **Les challenges d'un réseau WAN (suite)**
 - Certains services sont toujours en interne
 - **Par exemple un LAN et un Data Center sur site**
 - Dans une infrastructure traditionnelle, chaque périphérique a son propre control plane (QoS, Routage) et son propre data plane.
 - **Dans une infrastructure distribuées (Site central + filiales/agences)**
 - Dans les agences, on n'a généralement pas les moyens d'utiliser toutes les solutions de sécurité que l'on a mises en place dans le site central.
 - Du coup on relie la filiale au site central via une ligne MPLS couteuse.

→ Pas de système centralisé d'approvisionnement.

- **Les challenges d'un réseau WAN (suite)**
 - **Routage**
 - Peut nécessiter plusieurs accès WAN
 - Une ligne VPN IP vers Internet.
 - Une ligne louée ou MPLS pour les données/business critique vers Internet.
 - Une ligne 3G/4G en backup vers Internet.
 - Des lignes MPLS pour relier les agences et site central.
 - Le trafic est priorisé sur base des n° de port, donc des protocoles et pas en fonction des applications.

→ Pas d'équilibrage de charge en fonction de l'application.
 - **Qualité de service**
 - La QoS se base sur DSCP qui ne tient pas compte de la qualité de la ligne.

→ Pas de basculement dynamique en fonction de la qualité de la ligne.

HEH.be Sciences et technologies

SD-WAN

- Solution MPLS

MPLS

Tout le trafic de la filiale passe par le MPLS vers le cloud du fournisseur.

Site central

Cloud privé du FAI

Internet

Cloud public

VPN IP

Backup 3G/4G

Ligne louées ou MPLS (Applications critiques)

Filiale

ORACLE Microsoft Azure vmware

a Office 365

• • • 532

HEH.be Sciences et technologies

SD-WAN

- Solution MPLS + VPN IP

MPLS

On garde le MPLS pour les applications critiques.

Site central

Cloud privé du FAI

Internet

Cloud public

Backup MPLS

VPN IP

Backup 3G/4G

Ligne louées ou MPLS (Applications critiques)

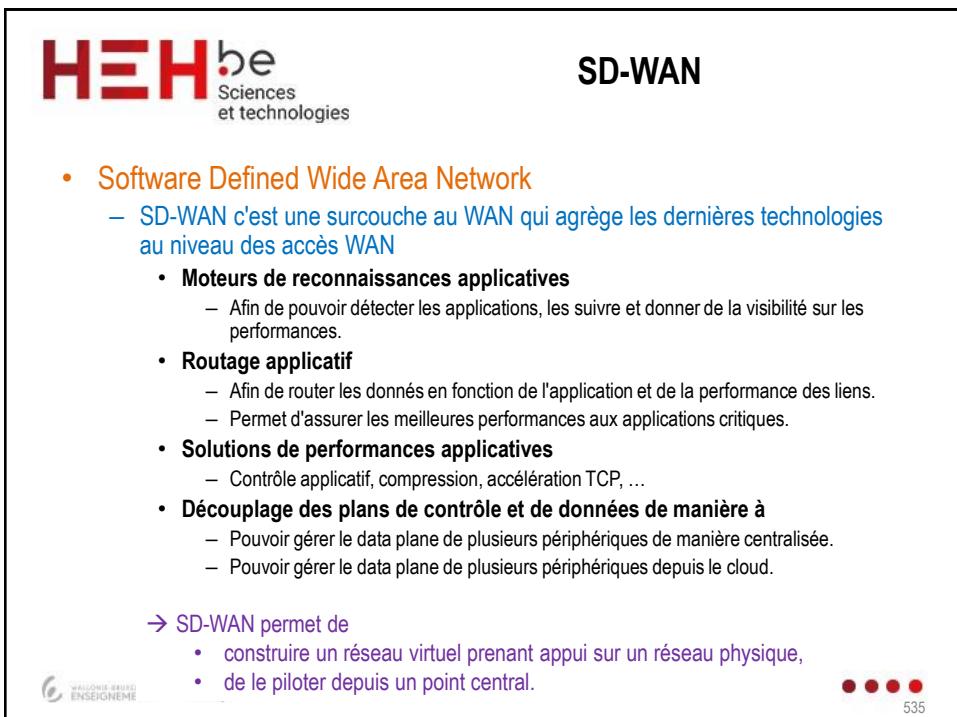
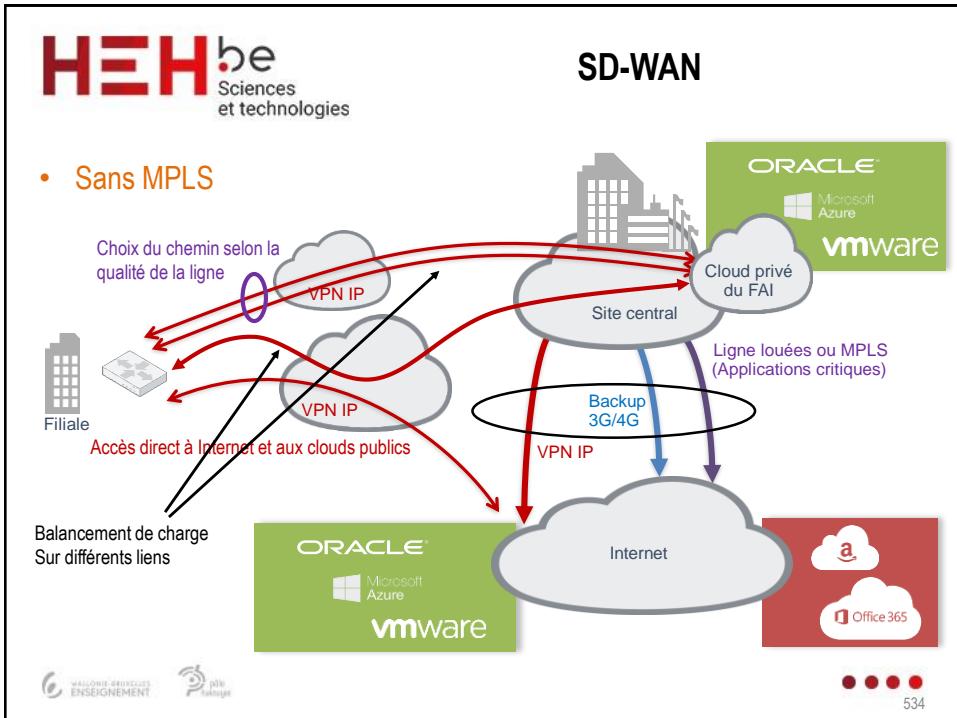
Filiale

ORACLE Microsoft Azure vmware

a Office 365

Accès direct à Internet et aux clouds publics

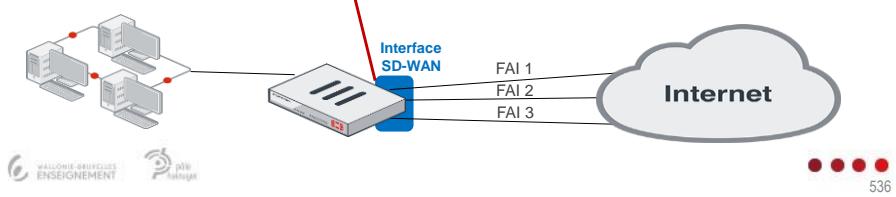
• • • 533



SD-WAN

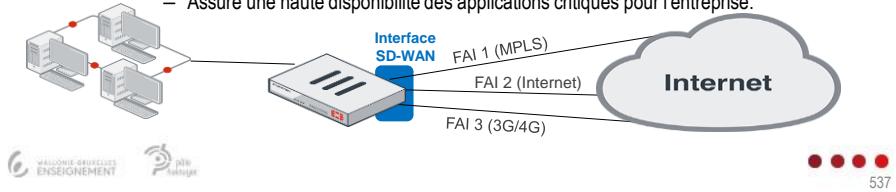
- Interface SD-WAN
 - Interface virtuelle
 - Constituée d'un groupe d'interfaces membres
 - Les interfaces membres peuvent être connectées à différents types de liens (Généralement connectées à plusieurs FAI).
 - Prise en charge des interfaces physique, agrégées, VLAN et IPsec.
 - Ces interfaces sont vues comme une seule interface logique appelée interface SD-WAN
 - Une règle implicite est générée automatiquement pour équilibrer le trafic.

Il n'est pas nécessaire que les interfaces soient celles étiquetées WAN.



SD-WAN

- Interface SD-WAN (suite)
 - Caractéristiques d'une interface SD-WAN
 - Permet une utilisation efficace du WAN
 - Différents algorithmes permettent d'équilibrer la charge en fonction de la BP, du nombre de sessions, de l'application, ...
 - Simplifie la configuration
 - Permet de configurer un ensemble unique de routes et de règles de pare-feu qui seront appliquées à tous les FAI.
 - Prend en charge la mesure de la qualité des liens
 - Sélection dynamique des liens basée sur la qualité des liens.
 - Assure une haute disponibilité des applications critiques pour l'entreprise.



SD-WAN

- Configuration

Une seule interface SD-WAN par VDOM

Spécifier au moins deux interfaces membres et leurs passerelles
 → Ces interfaces ne doivent pas être référencées par un autre élément de configuration (routes ou règle de FW).

Les interfaces membres sont regroupées en une seule interface virtuelle nommée sd-wan

ID	Name	Source	Destination	Criteria	Members
Implicit	sd-wan	all	all	Source IP	any

Network > SD-WAN

Possible d'ajouter une autre interface membre à une date ultérieure.

SD-WAN

- Configuration de la méthode d'équilibrage de charge

- Load-balance mode

- Le mode "load-balance" remplace le mode "v4-ecmp" lorsque le SD-WAN est activé.

- Source IP (default)

- Les sessions d'une même adresse IP source utilisent la même interface.

- Source-destination IP

- Les sessions avec la même paire IP source/destination utilisent la même interface.

- Spillover (Usage)

- La même route est utilisée jusqu'à ce qu'un seuil de volume de trafic (en kbps) soit atteint. Tout trafic au-delà de ce seuil est envoyé sur une autre interface.
- oad-balance-mode utilise les seuils de débordement définis dans la configuration du membre SD-WAN, v4-ecmp-mode les seuils de débordement définis dans les paramètres de l'interface.

```
config system virtual-wan-link
  set load-balance-mode <load balance mode>
end
```

- Configuration de la méthode d'équilibrage de charge (suite)

4. Weight

- Le trafic est distribué en fonction du poids de l'interface.
- « Load-balance-mode » utilise le poids défini dans la configuration du membre SD-WAN, v4-ecmp-mode le poids défini dans la route statique.
 - Le poids est un nombre entier.

5. Volume (Bandwidth)

- Le mode “load-balance” remplace le mode “v4-ecmp” lorsque le SD-WAN est activé.
- Dans ce mode, les sessions peuvent être distribuées de manière à répartir le volume de trafic en fonction du poids de l'interface.

```
config system virtual-wan-link
  set load-balance-mode <load balance mode>
end
```

- Zones SD-WAN

- Plus petit regroupement d'interfaces membre du SD-WAN

- Plusieurs interfaces membre du SD-WAN peuvent être regroupées en groupes logiques plus petits (appelés zones SD-WAN).
 - Permet un contrôle plus granulaire du trafic inspecté et autorisé dans les règles de pare-feu.
 - Les interfaces membres individuelles du SD-WAN ne peuvent pas être utilisées dans une règle de FW..

- Caractéristiques

- Une même interface membre du SD-WAN ne peut pas être partagée entre plusieurs zones.
 - Par défaut, FortiGate crée la zone « virtual-wan-link ».
 - Les zones SD-WAN sont incluses dans la vue topologique de la Security Fabric.

HEH.be Sciences et technologies

SD-WAN

- Configuration de Zones SD-WAN

The screenshot shows a web-based management interface for SD-WAN zones. At the top, there's a header with the HEH.be logo and a 'SD-WAN' section. Below the header, there's a table with columns for 'SD-WAN Member' and 'SD-WAN Zone'. A red box highlights the 'Create New' button at the top left of the table. A red arrow points from this button to a modal window titled 'New SD-WAN Zone' which is displayed below. This modal has fields for 'Name' (set to 'IPSS') and 'Interface members' (listing 'port1' and 'port2').

HEH.be Sciences et technologies

SD-WAN

- Configuration des règles de FW
- Configurer uniquement les règles avec l'interface SD-WAN
 - Inutile de configurer des règles de pare-feu pour chaque interfaces membres.

The screenshot shows a 'Policy & Objects > IPv4 Policy' configuration screen. It displays a 'New Policy' dialog with various settings. A red box highlights the 'Outgoing Interface' dropdown menu, which is currently set to 'sd-wan'. Other visible settings include 'Name' (Full_Access), 'Incoming Interface' (port3), 'Source' (LOCAL_SUBNET), 'Destination' (all), 'Schedule' (always), 'Service' (ALL), and 'Action' (ACCEPT). There are also 'DENY' and 'LEARN' options available.

SD-WAN

- Configuration du routage

- Configuration d'une route par défaut utilisant l'interface SD-WAN

- Même si une seule route est configurée via l'interface SD-WAN, FortiGate installe des routes individuelles pour les interfaces membres dans la table de routage.

La configuration d'une route par défaut utilisant l'interface SD-WAN ne nécessite pas d'adresse de passerelle.

Network > Static Routes

Edit Static Route

Destination	Submit Named Address Internet Service 0.0.0.0/0.0.0.0
Interface	SD-WAN
Administrative Distance	1
Comments	6096
Status	Enabled

```
# 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
```

● ● ● 544

SD-WAN

- Performance SLA : LHM

- Link Health Monitor (Link health check)

- Permet de détecter l'arrêt ou la dégradation d'un routeur le long du trajet.
- Vérifie le statut de chaque membre de l'interface SD-WAN.

+ Network
SD-WAN
SD-WAN Rules
Performance SLA

Network > Performance SLA

Edit Performance SLA

Name	DC_PBX_SLA
Protocol	ping HTTP
Server	4.2.2.2 4.2.2.1
Participants	port1 port2
Enable Probe Packets	<input checked="" type="radio"/>

5 choix en CLI :

- Ping
- HTTP
- TCP echo
- UDP echo
- TWAMP (Two-Way Active Measurement Protocol)

Définir 2 serveurs permet d'éviter que le serveur ne soit en faute, et non le lien.
IP ou FQDN.

HEH.be Sciences et technologies

SD-WAN

- Performance SLA : Link Quality Measurement
 - Mesure également la qualité de la liaison de chaque interface membre
 - Latence, de la gigue et du pourcentage de perte de paquets.

Les flèches vertes indiquent seulement que le serveur répond
Chiffres en rouge si les performances SLA ne sont pas atteintes

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

546

HEH.be Sciences et technologies

SD-WAN

- Performance SLA : SLA Targets
 - SLA Targets
 - Un lien membre SD-WAN affecté à un performance SLA doit satisfaire au SLA Targets afin d'être sélectionné parmi les autres liens participants.

Network > Performance SLA

SLA Targets

Target 1	<input type="checkbox"/> Replace with Recommended Values Latency threshold: 200 ms Jitter threshold: 50 ms Packet Loss threshold: 5 %
<input type="button" value="Add Target"/>	

Valeurs prédéfinies selon le service (voir diapositive suivante).

Un lien du SD-WAN affecté à ce SLA doit atteindre ce niveau de performance afin d'être sélectionné parmi les autres liens participants.

Vous pouvez spécifier plusieurs SLA Targets dans un "Performance SLA" (rarement utile).

Network

- SD-WAN
- SD-WAN Rules
- Performance SLA

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

547

HEH.be Sciences et technologies

SD-WAN

- Performance SLA : SLA Targets (Cont.)

Network > Performance SLA

SLA Targets

Target 1

Replace with Recommended Values

Latency threshold: 200 ms

Jitter threshold: 50 ms

Packet Loss threshold: 5 %

Add Target

Link Status

Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

Update static route

Select Entries

Performance Criteria

Internet Service

General

General-Cloud

General-Web

Office365

SAP

Skype

VoIP-Video

Other

Select Entries

Performance Criteria

Internet Service

General-Cloud (9)

- Adobe Adobe Cloud
- Alibaba Alibaba Cloud
- Amazon AWS
- Aruba Web
- CrownStrike CrowdStrike Cloud
- Google Google Cloud
- Lifesize Lifesize Cloud
- Microsoft Azure
- Zscaler Zscaler Cloud
- General-Web (160)
- Act-on Web
- Adobe Web
- ADP Web
- AdRoll Web

WALLONIE-BRUXELLES ENSEIGNEMENT

Développeur

www.heh.be

19-09-23

548

HEH.be Sciences et technologies

SD-WAN

- Performance SLA : SLA Targets (Cont.)

SLA Targets

Target 1

Replace with Recommended Values

Latency threshold: 200 ms

Jitter threshold: 50 ms

Packet Loss threshold: 5 %

Add Target

Link Status

Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

Update static route

+ Network

- SD-WAN
- SD-WAN Rules
- Performance SLA

Définir la fréquence à laquelle le système vérifie le statut de la liaison (et donc l'éventuel basculement).

Empêchent le "flapping". (Basculement incessant du trafic entre les liens).

Désactive automatiquement les routes statiques pour les interfaces inactives et restaure les routes lors de la restauration des interfaces.

! Les valeurs d'une SLA target ne sont utilisées que lorsqu'elles sont référencées par une règle SD-WAN.

WALLONIE-BRUXELLES ENSEIGNEMENT

Développeur

549

HEH.be Sciences et technologies

SD-WAN Rules

- SD-WAN Rules
 - Définissent quel trafic doit être acheminé à travers quelle interface membre

Network > SD-WAN Rules

Critères de correspondance

- Adresse IP source
- Adresse IP de destination
- Numéro du port de destination
- Les objets ISDB
- Application
- Utilisateurs ou groupes d'utilisateurs
- Type de service (ToS)

Critères de qualité

- Latence
- Gigue
- Pourcentage de perte de paquets

550

HEH.be Sciences et technologies

SD-WAN rules

- SD-WAN Rules (Cont.)

Network > SD-WAN Rules

Liste de règles

- de haut en bas,
- première correspondance.

Internet Service Database

Application Control Database

551

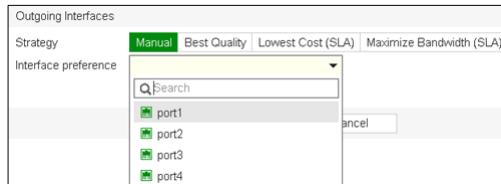
SD-WAN rules

- SD-WAN Rules (Cont.)

- Stratégie de sélection d'une interface de sortie

1. Manual

- Si le trafic correspond aux critères de correspondance, l'interface renseignée est utilisées.
- Ne tient pas compte des éventuelles configurations de SLA targets.



SD-WAN rules

- SD-WAN Rules (Cont.)

- Stratégie de sélection d'une interface de sortie

2. Best Quality

- Se base sur la performance du réseau (health check) mais pas sur les SLA targets.
- La première interface listée est utilisée jusqu'à ce que les critères de qualité de cette interface ne soient plus valides, puis l'interface suivante.

Outgoing Interfaces

Strategy: Best Quality

Measured SLA: DC_PBX_SLA

Quality criteria: Latency

Link Quality = (a*latency)+(b*jitter)+(c*packet loss)+(d/bandwidth)

Choix basé sur la BP.
Utile en fonction du type d'application basée
plutôt sur l'upload ou le download.

Custom permet de se baser sur un ensemble de critères

SD-WAN rules

- SD-WAN Rules (Cont.)
 - Stratégie de sélection d'une interface de sortie

3. Lowest Cost (SLA)

The screenshot shows three windows related to SD-WAN configuration:

- Edit Performance SLA**: Shows a list of participants (port1, port2, port3, port4) and their associated protocols (4.2.2.2, 4.2.2.1). A red box highlights the "DC_PBX_SLA" entry.
- Select Entries**: A modal window showing two entries: "DC_PBX_SLA#1" and "DC_PBX_SLA#2". A red arrow points from this window to the "Priority Rule" window.
- Priority Rule**: Shows a configuration for "Softphone_PBX". It includes a "Source address" of "LOCAL_SUBNET", a "Protocol number" of "TCP / UDP / All", and an "Outgoing Interfaces" section where "Lowest Cost (SLA)" is selected. A red box highlights this selection. The "Required SLA target" field contains "DC_PBX_SLA#1".

Annotations in red text:

- "Se base sur un SLA targets."
- "Plusieurs SLA targets ont été configurés."
- "Un seul SLA targets peut être sélectionné."

SD-WAN rules

3. Lowest Cost (SLA) (suite)

Principe :

- 1) Vérifier si les SLA sont satisfais.
- 2) Vérifier le coût des interfaces
 - Élimine les coûts plus élevés.
- 3) Vérifier la priorité des interfaces
 - Élimine les priorités plus faibles.

Configurable

The screenshot shows two parts of the SD-WAN configuration:

- Network > SD-WAN**: A table titled "SD-WAN Interface Members" showing interface details. The "Cost" field for "port1" is circled in orange and has a value of 5. The "Status" field has buttons for "Enable" and "Disable".
- Cost Prioritization Table**: A table with columns "Interface", "SLA", "Coût", and "Priorité". The data is as follows:

Interface	SLA	Coût	Priorité
Interface1	Ok	5	4
Interface2	Ok	5	3
Interface3	Ok	10	2
Interface4	Non ok	2	1

 The "Coût" column values are circled in orange: 5, 5, 10, and 2. The "Priorité" column values are circled in brown: 4, 3, 2, and 1. The "Non ok" entry for Interface4 is crossed out with a red X.

SD-WAN rules

- SD-WAN Rules (Cont.)

4. Rules-Maximize Bandwidth (SLA)

Principe :

- 1) Vérifier si les SLA sont satisfait.
- 2) Vérifier combien de critères SLA sont satisfait
 - Le trafic est réparti sur les membres qui satisfont le plus de critères SLA.

Interface	SLA	Coût	Priorité
Interface1	Ok	5	4
Interface2	Ok	5	3
Interface3	Ok	10	2
Interface4	Non ok	2	1

SD-WAN rules

- SD-WAN Rules (Cont.)

– Application des règles

- Même principe que pour les règles d'un pare-feu
 - Lecture séquentielle.
 - La première correspondance est appliquée.
- Les règles SD-WAN sont traitées comme des policy-based routes
 - Elles sont prioritaires par rapport aux routes de la table de routage.

Network > SD-WAN Rules

SD-WAN Rules					
Create New Edit Delete Search					
ID	Name	Source	Destination	Criteria	Members
1	Facebook	all	Facebook		port1
2	YouTube	LOCAL_SUBNET	YouTube	Latency	port1 port2
3	MS-Office-360	all	Microsoft Office 365	SLA	port1 port2
	Implicit	sd-wan	all	alt	Source-Destination IP: any

Règle implicite : équilibre la charge sur toutes les interfaces membre

HEH.be
Sciences
et technologies

SD-WAN Monitor

- SD-WAN Usage Monitor
 - Permet de voir la répartition du trafic entre les interfaces membres

The screenshot shows the 'Network > SD-WAN' interface with tabs for 'Bandwidth', 'Volume' (highlighted in red), and 'Sessions'. Two pie charts are displayed: 'Upstream' and 'Downstream'. Arrows point from the labels to specific parts of the charts.

Port	Percentage
port1	74%
port2	26%

Port	Percentage
port1	69%
port2	31%

Quantité de BP utilisée par chaque interface (Blue arrow)

Volume de trafic envoyé et reçu par interface (Red arrow)

Nombre de session par interface (Purple arrow)

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

558

HEH.be
Sciences
et technologies

SD-WAN Monitor

- SD-WAN Link Status Monitoring
 - Le changement d'état d'un interface génère un log

Network > Performance SLA

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Netflix	http://www.netflix.com/	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: 0.00 % port2: 0.00 %	port1: 41.35 ms port2: 32.70 ms	port1: 306.34 ms port2: 61.04 ms	5	5
AWSService	www.amazon.com	port1: 0.00 % port2: 0.00 %	port1: 14.80 ms port2: 14.90 ms	port1: 16.55 ms port2: 16.57 ms	5	5

Log & Report > System Events

#	Date/Time	Level	User	Message
1	14:02:37	INFO		The member(1) link is available. Start forwarding traffic.
2	14:02:36	INFO		Static route is added. Route: (10.200.1.1->4.2.2.1 ping-up)
3	14:02:01	INFO		The member(1) link is unreachable. Stop forwarding traffic.
4	14:02:01	INFO		Static route is removed. Route: (10.200.1.1->4.2.2.1 ping-down)
5	14:01:01	INFO		The member(1) link is available. Start forwarding traffic.
6	14:01:01	INFO		Static route is added. Route: (10.200.1.1->4.2.2.1 ping-up)

WALLONIE-BRUXELLES ENSEIGNEMENT Pôle Formation

559

- Vérifier le routage du traffic SD-WAN

– Les logs permettent de vérifier par quelle interface membre le trafic est envoyé

Log & Report > Forward Traffic

#	Date/Time	Source	Destination	Application Name	Security Events	Result	Policy	Destination Interface
1	13:19:15	10.0.1.10	54.241.244.69 (sthebrighttag.com)	Amazon-AWS		✓ 1.76 kB / 7.30 kB	1(Full_Access)	☒ port2
2	13:19:15	10.0.1.10	54.241.244.69 (sthebrighttag.com)	Amazon-AWS		✓ 664 B / 3.98 kB	1(Full_Access)	☒ port2
3	13:19:15	10.0.1.10	54.241.244.69 (sthebrighttag.com)	Amazon-AWS		✓ 664 B / 3.98 kB	1(Full_Access)	☒ port2
4	13:19:15	10.0.1.10	54.241.244.69 (sthebrighttag.com)	Amazon-AWS		✓ 664 B / 3.98 kB	1(Full_Access)	☒ port2
5	13:19:15	10.0.1.10	74.50.51.79 (ethnlo)	HTTPS		✓ 1.07 kB / 9.25 kB	1(Full_Access)	☒ port2
6	13:19:15	10.0.1.10	23.36.68.28 (codexnfixtext.com)	Netflix-Web		✓ 172 B / 92 B	1(Full_Access)	☒ port1

– Le sniffer intégré permet aussi de vérifier par quelle interface le trafic est envoyé

```
# diagnose sniffer packet any 'tcp[13]&2==2 and port 443' 4
5.455914 port1 out 192.168.1.254.59785 -> 192.168.1.11.443: syn 457459
5.455930 port2 out 192.168.1.11.443 -> 192.168.1.254.59785: syn 163440 ack 457460
5.455979 port2 out 192.168.1.32.49573 -> 192.168.1.25.443 : syn 927943
5.456043 port1 out 192.168.1.21.54711 -> 192.168.1.114.443: syn 930863
```

Bibliographie

Ouvrages

O. SANTOS, J. STUPPI, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.

Sources électroniques

ANSSI, *Recommandations de sécurité relatives à TLS*,
https://www.ssi.gouv.fr/uploads/2016/09/guide_tls_v1.1.pdf, 2016.

ANSSI, *Note technique. Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, https://www.ssi.gouv.fr/uploads/2012/09/NT_IPsec.pdf, 2015.

BOUSABER C., IKE v2, <https://www.randco.fr/blog/2013/ike-v2/>, 2013.

ETUTORIALS.ORG, *RSA Encrypted Nonces Overview*,
<http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+II+Virtual+Private+Networks+VPNs/Chapter+11+Cisco+IOS+IPSec+Certificate+Authority+Support/RSA+Encrypted+Nonces+Overview/>,

FRIEDL S., *An Illustrated Guide to IPsec*, <http://www.unixwiz.net/techtips/iguide-ipsec.html>, 2005.

FORTINET, INC., *FortiOS-AdministrationGuide Version 7.2.0*,
<https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/954635/getting-started>; 2022.

FORTINET NSE TRAINING INSTITUTE, *NSE4 -FortiGate Security and Infrastructure (FortiOS 7.0)*, <https://www.fortinet.com/training/security-academy-program>, 2022.

MILLER L., *Zero trust access for dummies*,
<https://www.fortinet.com/content/dam/fortinet/assets/ebook/zero-trust-access-for-dummies.pdf>, 2022