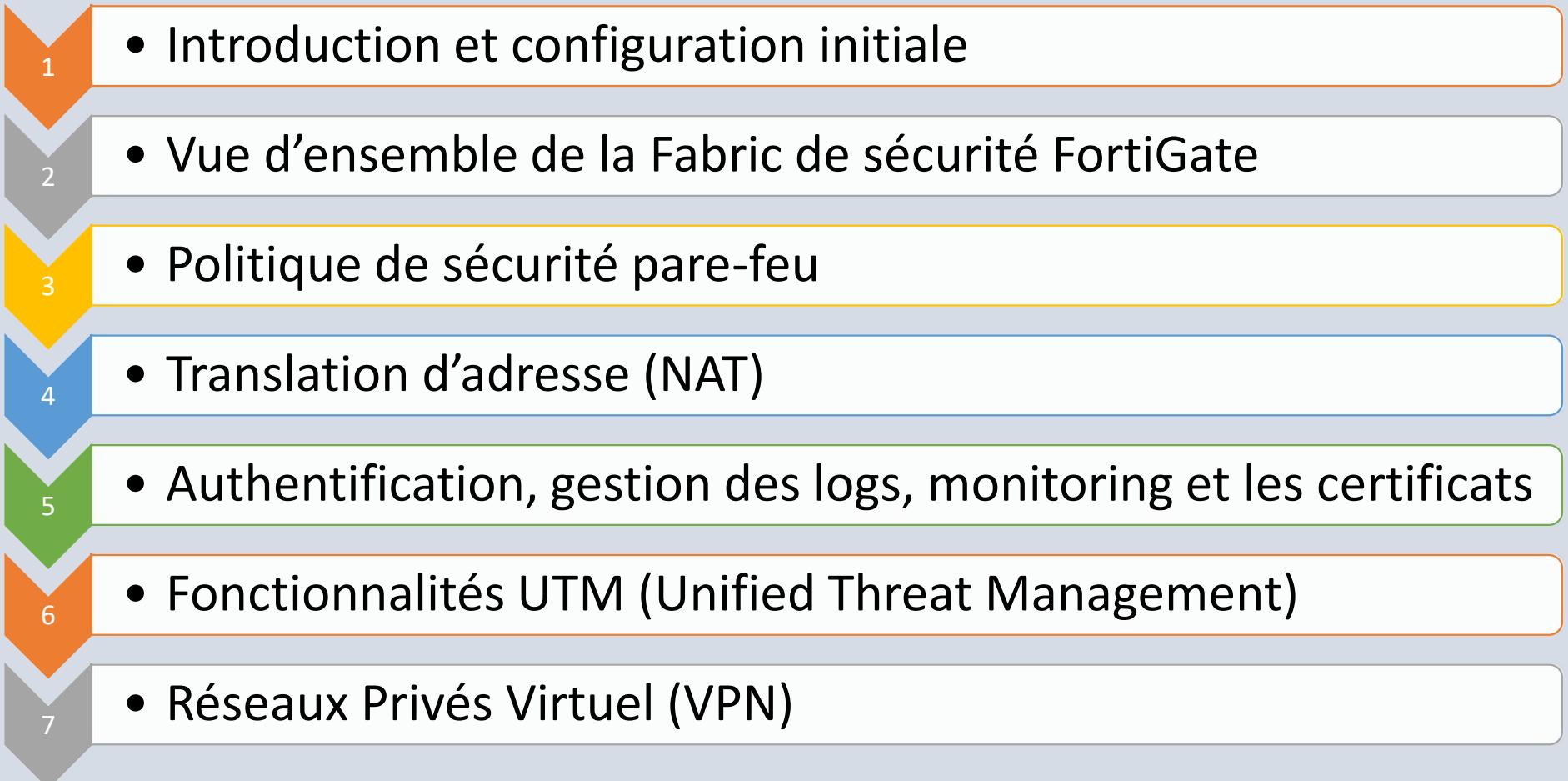


FORTINET®

Plan de la formation

- 
- 1 • Introduction et configuration initiale
 - 2 • Vue d'ensemble de la Fabric de sécurité FortiGate
 - 3 • Politique de sécurité pare-feu
 - 4 • Translation d'adresse (NAT)
 - 5 • Authentification, gestion des logs, monitoring et les certificats
 - 6 • Fonctionnalités UTM (Unified Threat Management)
 - 7 • Réseaux Privés Virtuel (VPN)

Introduction Générale

Description

- Prise en main d'un pare-feu FortiGate;
- FortiOS 7.0

Cible

- Administrateur réseaux;
- Responsable sécurité.

Prérequis

- Protocoles Réseaux;
- Firewalling.

Introduction Générale

Objectifs

- Choix du mode de déploiement
- Navigation GUI/CLI
- Caractéristiques Fabric
- Configuration NAT
- Utilisation des politiques de pare-feu
- Fonction de chiffrement et certificats
- Inspection de trafic
- Utilisation et configuration des profils de sécurité
- VPN
- Collecte et interprétation des logs

FORTINET
NSE Training Institute

FortiGate Security

INTRODUCTION ET CONFIGURATION INITIALE



Plan du module



Fonctionnalités de haut niveaux

Objectifs

- Identifier les caractéristiques de conception de la plateforme FortiGate ;
- Identifier les fonctionnalités du FortiGate dans les réseaux virtualisés et dans le cloud ;
- Comprendre les SPU FortiGate (Security Processing Unit).

Fonctionnalités de haut niveau

Sécurité réseau

- ❑ Firewall sont plus que les gardiens du périmètre de sécurité réseau
- ❑ Conçu aujourd'hui pour répondre aux évolutions des environnements réseau à la fois multi équipements et multifacette
 - ❑ Equipements internes et mobiles des employés ;
 - ❑ Equipements de partenaires ;
 - ❑ Cloud public ou privé ;
 - ❑ Equipements IoT ;
 - ❑ Equipements BYOD
- ❑ Firewall peuvent effectuer différentes fonctions dans un réseau
 - ❑ Datacenter Firewall
 - ❑ Segmentation Firewall
 - ❑ Next-generation Firewall

Plateforme FortiGate

Topologies Cloud

SPU (Security Processing Units)

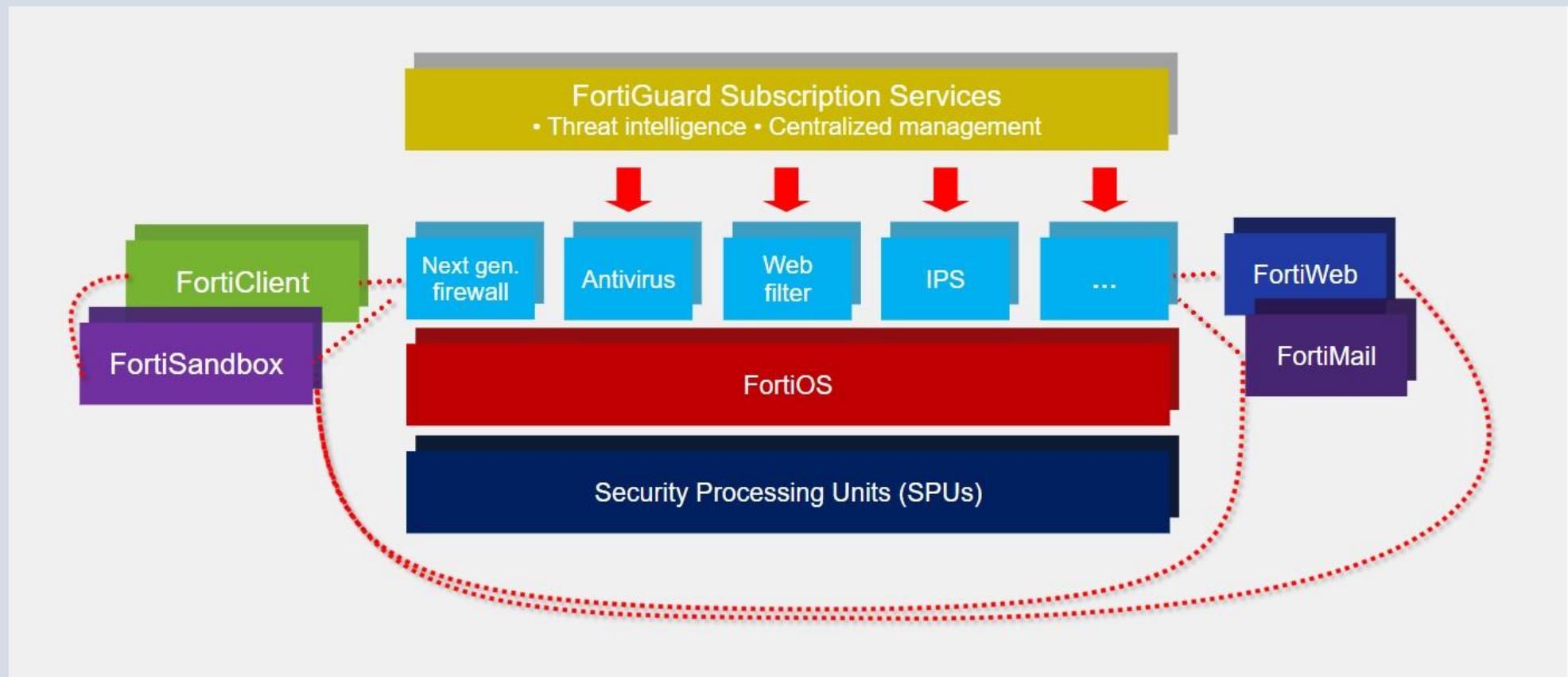
Fonctionnalités de haut niveau

Sécurité réseau

Plateforme FortiGate

Topologies Cloud

SPU (Security Processing Units)



Fonctionnalités de haut niveau

Sécurité réseau

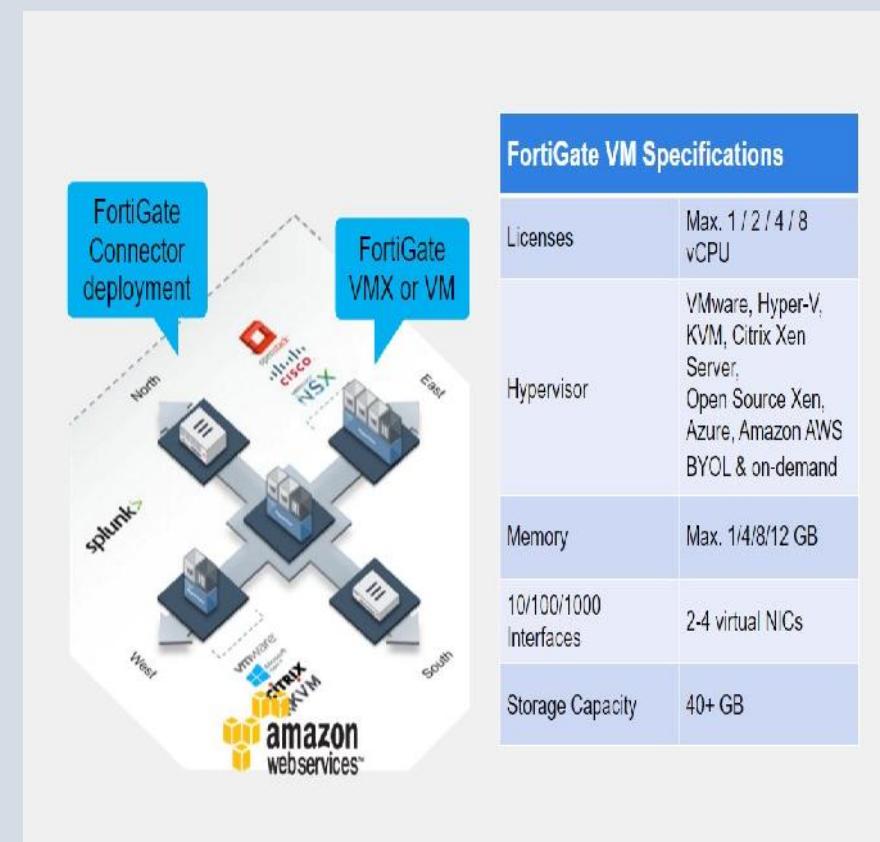
Plateforme FortiGate

Topologies Cloud

SPU (Security Processing Units)

- Déploiement dans un réseau virtualisé:

- **FortiGate VM**: Déployé comme VM dans un hyperviseur;
- **FortiGate VMX**: Déployé au sein du réseau virtuel d'un hyperviseur ;
- **FortiGate Connector for Cisco ACI**: Permet le déploiement physique ou virtuel des VM FortiGate pour les trafic nord-sud;



Fonctionnalités de haut niveau

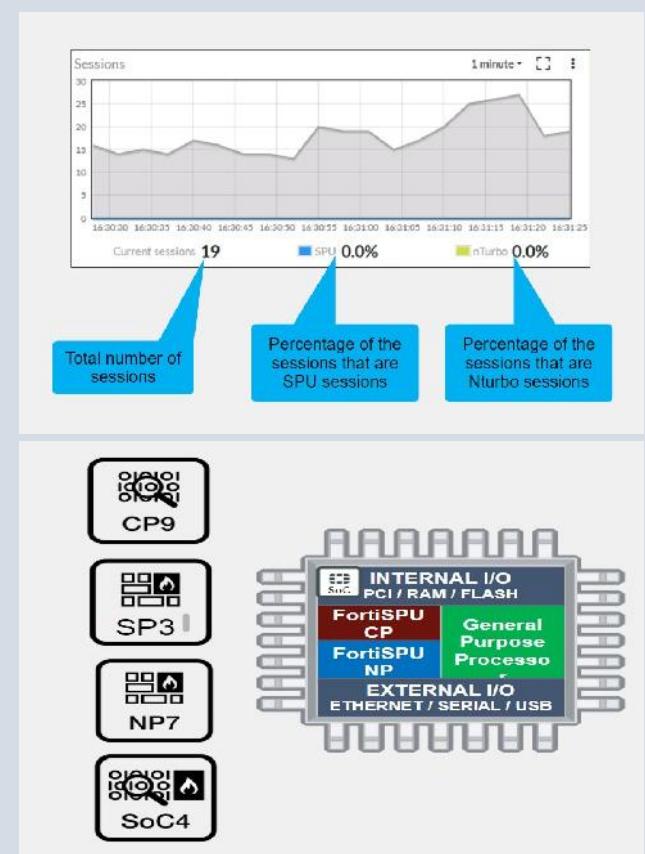
Sécurité réseau

- Security Processing Units (SPUs):
 - Décharger le CPU principal du traitement des processus gourmant en ressources
 - 03 types: CP (Content Processor), SP (Security Processor) et NP (Network Processor);
 - CP (Content Processor): gère les processus liés au chiffrement et déchiffrement SSL, antivirus, etc
 - SP (Security Processor): augment les performances du système en accelerant les IPS et sont directement attachés aux interfaces
 - NP (Network Processor): gère le traitement des paquets et est directement attaché aux interfaces
 - SoC (System on a Chip Processor): optimise les performances aux niveau des entrées

Plateforme FortiGate

Topologies Cloud

SPU (Security Processing Units)



Décision de déploiement

Objectifs

- Identifier les paramètres par défaut du pare-feu ;
- Choix d'un mode de fonctionnement ;
- Comprendre la relation entre FortiGate et FortiGuard;
- Distinguer les « lives queries » et les « packages updates »

Décision de déploiement

Mode de fonctionnement

NAT

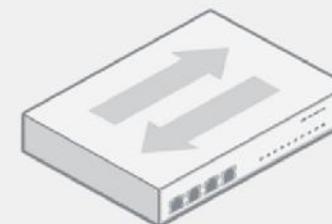
- Equipement de couche 3;
- Interfaces peuvent avoir les IPs;
- Paquets sont routés par IP;
- Configurable par VDOM (Virtual Domaine);
- Mode de fonctionnement par défaut.



Paramètre par défaut

Transparent

- Equipement de couche 2;
- Aucune IP sur les interfaces;
- Transfert ou bloque uniquement les paquets;
- Configurable par VDOM (Virtual Domaine).



Services FortiGuard

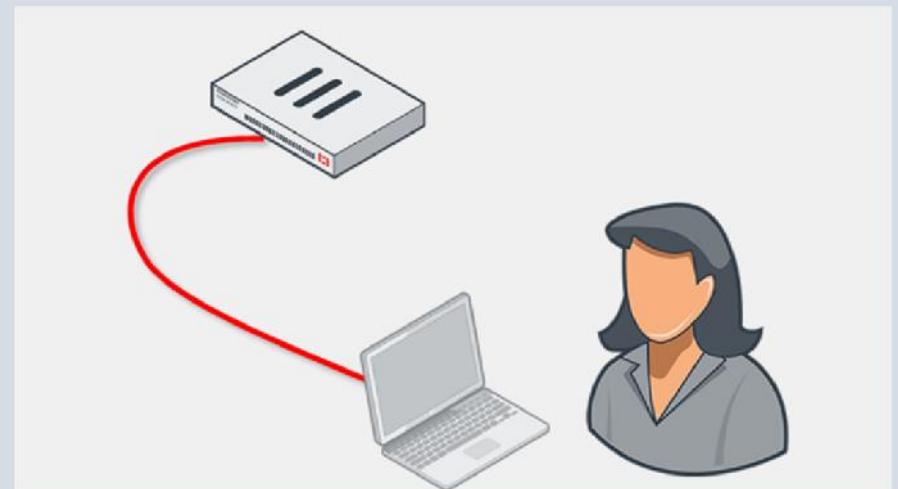
Décision de déploiement

Mode de fonctionnement

- IP par défaut: 192.168.1.99/24
 - Interface de management: modèle haut de gamme et de gamme intermédiaire;
 - Port 1 sur les modèles d'entrée de gamme.
- Protocole activé: PING, HTTPS et SSH;
- Serveur DHCP intégré activé sur le Port 1 (sur les modèles d'entrée de gamme qui supportent les serveurs DHCP);
- Paramètre de connexion par défaut:
 - Utilisateur: admin
 - Mot de passe: Blank
- Accès à la CLI
 - Via le port console;
 - Via un émulateur: PuTTY ou Tera Term

Paramètre par défaut

Services FortiGuard



Décision de déploiement

Mode de fonctionnement

Paramètre par défaut

Services FortiGuard

- Fournit une base de donnée intelligente de menace au FortiGate:
 - Nécessite une connexion internet et un contrat (licence);
 - Fourni par FDN (FortiGuard Distribution Network).
- Queries
 - Requêtes faites en temps réel par le pare-feu au FDN lors du scan d'un spam ou du filtrage d'un site;
 - UDP ou HTTPs utilisé pour le transport;
 - Requête au lieu du téléchargement
- Paquets
 - Antivirus / IPS;
 - TCP utilisé pour le téléchargement.



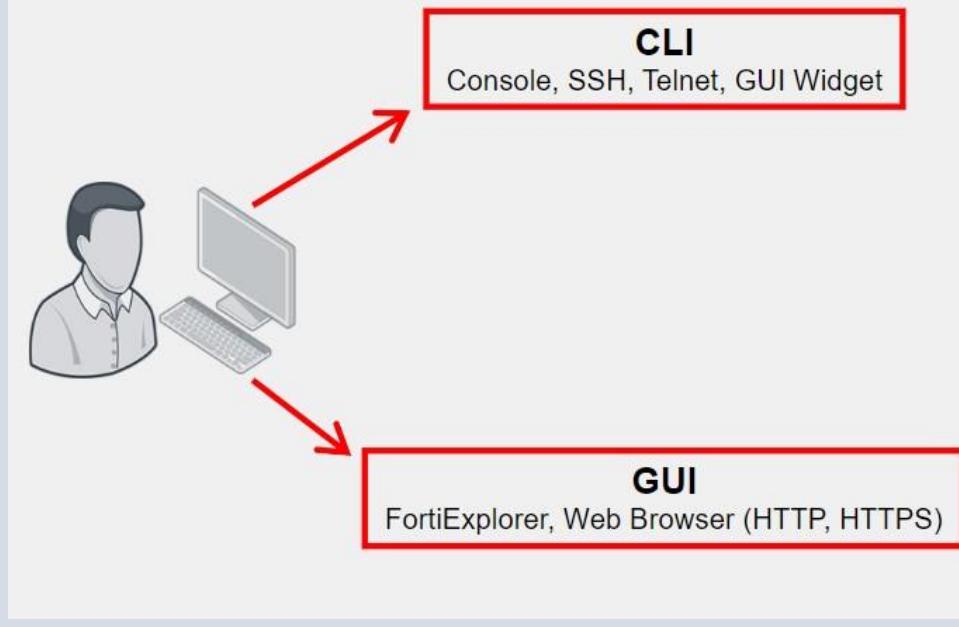
Administration de base

Objectifs

- Gérer les profils administrateurs ;
- Gérer les utilisateurs ;
- Contrôler les accès à l'interface graphique et à la CLI.

Administration de base

Méthode d'administration



Gestion des utilisateurs

Gestion des profils

Authentification

The slide displays three screenshots of the FortiGate management interface. The top screenshot shows the 'CLI Console' window with a black screen and a green header bar. The middle screenshot shows the 'Dashboard' in the 'GUI' (Graphical User Interface), featuring various system status metrics like CPU usage, memory, and network traffic. The bottom screenshot shows the 'Authentication' screen, which includes fields for 'Username' and 'Password' and a 'Log In' button.

Administration de base

Méthode d'administration (suite)

Gestion des utilisateurs

Gestion des profils

Authentification

- Quelques commandes CLI de base:
 - get system status: Affiche le status courant du FortiGate;
 - show full-configuration system interface <port>: Affiche la liste des attributs et les valeurs pour une interface donnée;

Administration de base

Méthode d'administration (suite)

- ❑ Quelques commandes CLI de base:
 - ❑ get system status: Affiche le status courant du FortiGate;
 - ❑ show full-configuration system interface <port>: Affiche la liste des attributs et les valeurs pour une interface donnée;

```
FG_ANТИC_HQ # get system status
Version: FortiGate-200E v6.0.4.build0231,190107 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FG200ETK19907084
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Botnet DB: 1.00000(2012-05-28 22:51)
BIOS version: 05000006
System Part-Number: P19082-03
Log hard disk: Not available
Hostname: FG_ANТИC_HQ
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0231
Release Version Information: GA
FortiOS x86-64: Yes
System time: Thu Oct 27 17:27:29 2022
```

Gestion des utilisateurs

Gestion des profils

Authentification

```
FG_ANТИC_HQ # show system interface port2
config system interface
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 6
    next
end
```

```
FG_ANТИC_HQ # show full-configuration system interface
config system interface
    edit "mgmt"
        set vdom "root"
        set vrf 0
        set fortiflink disable
        set priority 0
        set dhcp-relay-service disable
        set ip 178.18.190.221 255.255.254.0
        set allowaccess ping https ssh http fgfm
        set fail-detect disable
        set pptp-client disable
        set arpforward enable
        set broadcast-forward disable
        set bfd global
        set l2forward disable
        set icmp-send-redirect enable
        set icmp-accept-redirect enable
        set vlanforward disable
        set stpforward disable
        set ips-sniffer-mode disable
        set ident-accept disable
        set ipmac disable
        set subst disable
        set substitute-dst-mac 00:00:00:00:00:00
        set status up
        set netbios-forward disable
        set wins-ip 0.0.0.0
        set type physical
        set dedicated-to management
        set netflow-sampler disable
```

Administration de base

Méthode d'administration

Gestion des utilisateurs

Gestion des profils

Authentification

- Création d'un utilisateur (administrateur)

The screenshot shows the FortiGate Management Interface. On the left, the navigation bar is visible with sections like Local-FortiGate, Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Administrators (selected), and Admin Profiles. The main panel shows the 'System > Administrators' page. A red box highlights the '+ Create New' button in the top right corner of the list area. Below it, a red arrow points from the 'Create New' button to the 'New Administrator' dialog box on the right. The 'New Administrator' dialog has the following fields:

- Username: Administrator
- Type: Local User (selected, highlighted in green)
- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group
- Password: (empty field)
- Confirm Password: (empty field)
- Comments: Write a comment... (0/255)
- Administrator profile: (dropdown menu)
- checkboxes for Two-factor Authentication, Restrict login to trusted hosts, and Restrict admin to guest account provisioning only

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Administration de base

Méthode d'administration

Gestion des utilisateurs

Gestion des profils

Authentification

System > Admin Profiles

The screenshot shows the 'Edit Admin Profile' page under 'System > Admin Profiles'. On the left is a sidebar with navigation links like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System (Administrators, Admin Profiles selected), Firmware, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Security Fabric, and Log & Report. The main area displays a table of permissions for 12 categories: Security Fabric, FortiView, User & Device, Firewall, Log & Report, Network, System, Security Profile, VPN, WAN Opt & Cache, and WiFi & Switch. Each category has three permission levels: None (disabled), Read (light green), and Read/Write (dark green). A 'Custom' button is available for Firewall, Log & Report, Network, System, Security Profile, and WiFi & Switch. At the bottom, there are two checkboxes: 'Permit usage of CLI diagnostic commands' (unchecked) and 'Override Idle Timeout' (checked, highlighted with a red border).



Administration de base

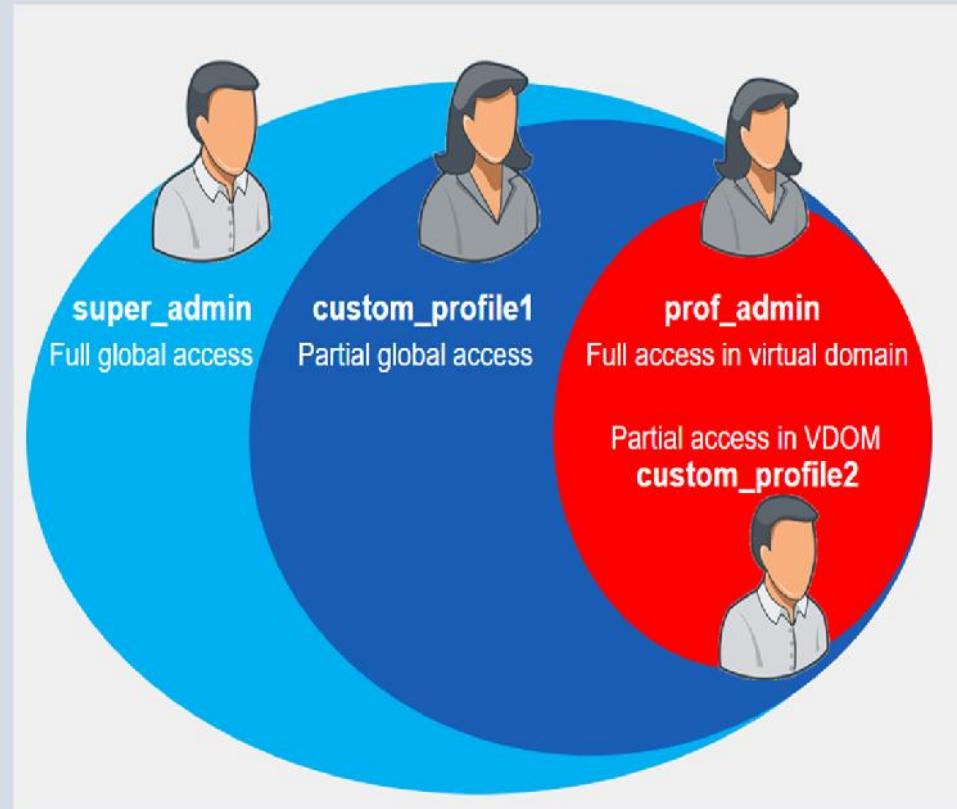
Méthode d'administration

The screenshot shows the 'System > Admin Profiles' section of the FortiGate management interface. On the left is a navigation tree with categories like Local-FortiGate, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Administrators, Admin Profiles (selected), Firmware, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Security Fabric, and Log & Report. The 'Admin Profiles' section is expanded, showing a list of profiles: Security Fabric, FortiView, User & Device, Firewall, Log & Report, Network, System, Security Profile, VPN, WAN Opt & Cache, and WiFi & Switch. Each profile has a dropdown menu with options: None, Read, Read/Write, or Custom. The 'Read/Write' option is selected for most profiles. At the bottom of the list, there are two additional items: 'Permit usage of CLI diagnostic commands' and 'Override Idle Timeout'. The 'Override Idle Timeout' item is highlighted with a red box.

Gestion des utilisateurs



Gestion des profils



Authentification

Administration de base

Méthode d'administration

- Authentification à double facteur
 - Facteur 1 : mot de passe ou certificat;
 - Facteur 2 : Token (synchroniser avec FortiGate).

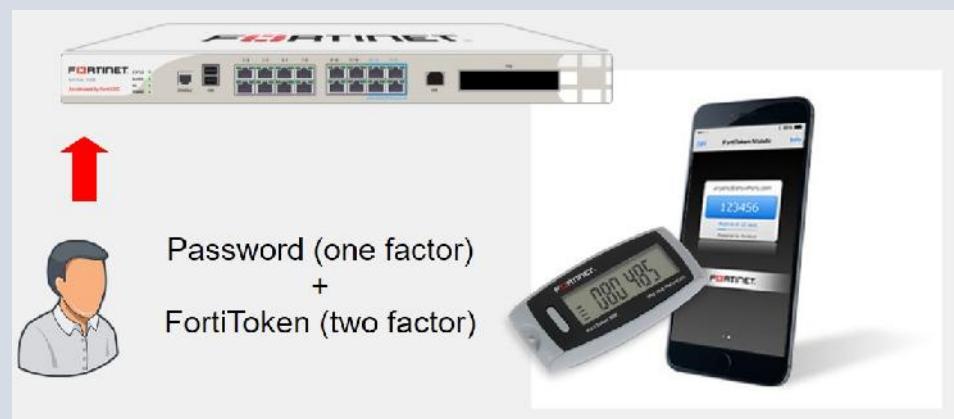
Gestion des utilisateurs

Gestion des profils

Authentification

- Authentification distante

- Configuration du serveur d'authentification;
- Création du compte d'administration et assignation des droits via un profils



Administration de base

Méthode d'administration

- ❑ Réinitialisation du mot de passe administrateur
 - ❑ Etape 1: Redémarrer le pare-feu (redémarrage à froid) et accéder à la console
 - ❑ Etape 2: Les paramètres suivant sont valides uniquement pendant les 60 premiers secondes après le redémarrage et via la console :
 - ❑ Login: maintien
 - ❑ Mot de passe: bcpb<numero de série> (numéro de série doit être en lettre majuscule bcpbFGT101ETKxxxxxx)
 - ❑ Etape 3: Commade sur la 1^{ère} image puis redémarrer
- ❑ Destiné aux FortiGate et certaines autre solution comme FortiMail;
- ❑ Ne fonctionne pas sur les VM;

Gestion des utilisateurs

Gestion des profils

Authentification(suite)

```
#config system admin  
edit admin  
set password <psswrd>  
end
```

```
#config system global  
set admin-maintainer  
disable  
end
```

Administration de base

Méthode d'administration

The screenshot shows the 'System > Settings' page. It includes sections for 'Administration Settings' and 'Password Policy'. The 'Administration Settings' section contains fields for HTTP port (80), Redirect to HTTPS (disabled), HTTPS port (443), HTTPS server certificate (self-sign), SSH port (22), Telnet port (23), and Idle timeout (5 minutes). The 'Password Policy' section includes fields for Password scope (Admin selected), Minimum length (8), Minimum number of new characters (0), Character requirements (disabled), Allow password reuse (disabled), and Password expiration (disabled).

Gestion des utilisateurs

Gestion des profils

Authentification(suite)

- Accès aux pare-feu depuis les sources les confiances;
- Port et Mot de passe.

The screenshot shows the 'System > Administrators' page. It displays a configuration dialog for 'Restrict login to trusted hosts' with 'Trusted Host 1' set to 10.0.1.0/32. To the right is a table of administrators, showing 'admin' with 'super_admin' profile, 'Local' type, and 'Disabled' status. A red arrow points from the configuration dialog to the table. Below the table is a message: 'If admin attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message'. On the far right is a screenshot of a login interface with a red error message: 'Authentication failure'.

Serveurs intégrés

Objectifs

- Activer le DHCP sur le FortiGate ;
- Activer le DNS sur le FortiGate ;

Administration de base

Serveur DHCP

The screenshot shows the FortiOS 7.0 interface for network administration. It includes three main windows:

- Network > Interfaces**: Shows the configuration for a physical interface named "port3". The "Role" dropdown is set to "LAN". The "Address" section shows "Address mode" as "Manual" and "IP/Netmask" as "10.0.1.254/255.255.255.0". The "Administrative Access" section lists various protocols (HTTPS, HTTP, PING, SSH, TELNET, etc.) and LLDP settings.
- DHCP Server**: Displays basic DHCP server settings: "DHCP status" is "Enabled", "Address range" is "10.0.1.1-10.0.1.253", "Netmask" is "255.255.255.0", and "Lease time" is "604800 seconds". It also shows advanced options like "Mode" (Regular), "NTP server", "Wireless controllers", "Time zone", and "Next bootstrap server".
- Create New IP Address Assignment Rule**: A dialog box for creating a new rule. It has fields for "Type" (set to "MAC Address"), "Description" ("Write a comment... 0/255"), "Match Criteria" (with a "MAC address" field), "Action" (with "Action type" set to "Assign IP" and "IP" set to "0.0.0"), and "OK" and "Cancel" buttons.

Red arrows highlight the flow of configuration: one arrow points from the "port3" interface configuration to the "DHCP Server" settings, and another arrow points from the "DHCP Server" settings to the "Create New IP Address Assignment Rule" dialog.

Serveur DNS

Administration de base

Serveur DHCP

- ❑ Fonctionnalité n'est pas visible par défaut, il faut ajouté la fonctionnalité DNS Database depuis le panneau de visibilité des fonctionnalité;
- ❑ Résout les requêtes DNS du réseau interne;
 - ❑ Activé par interface;
- ❑ Base de données DNS partagée par toute les interfaces du FortiGate;
- ❑ Méthodes de résolution:
 - ❑ Forward: Relaie les requêtes au prochain server
 - ❑ Non-Recursive: Utilise la base de donnée DNS pour essayé de résoudre uniquement les requêtes;
 - ❑ Recursive: Utilise d'abord la base de donnée interne et relaie au prochain serveur si la résolution ne s'est pas faite.
 - ❑ Configuration GUI ou CLI

The screenshot shows the FortiGate management interface under the 'Network > DNS Servers' section. On the left, a sidebar lists various network-related configurations. The 'DNS Servers' option is highlighted with a red box. The main pane displays two tables: 'DNS Service on Interface' and 'DNS Database'. The 'DNS Service on Interface' table has a single entry for 'port3' set to 'Recursive'. The 'DNS Database' table lists three DNS zones: 'note.lab', 'remote.lab', and 'student.lab', each with a primary and shadow entry. A large blue callout points from the 'DNS Servers' section towards the 'Edit' button in a modal dialog titled 'Edit DNS Service'. This dialog allows changing the 'Interface' (set to 'port3'), 'Mode' (set to 'Recursive'), and 'DNS Filter' (disabled). A red box highlights the 'Forward to System DNS' checkbox, which is checked. Another blue callout at the bottom left explains that to view DNS Servers, it must be made visible in 'System > Feature Visibility > DNS database'.

To view **DNS Servers** in **Network**, you must make it visible in **System > Feature Visibility > DNS database**

Double-click the interface field or select and click **Edit**.

Serveur DNS

Maintenance de base

Objectifs

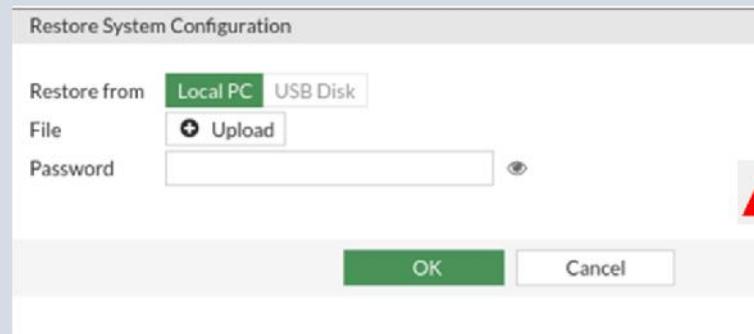
- Sauvegarde et restauration des fichiers de configurations ;
- Identifier la version du Firmware
- Upgrader et downgrader le Firmware

Maintenance de base

Sauvegarde/Restauration

- Configuration peut être enregistré sur un équipement externe; Chiffré ou non
- Peut être restaurer automatiquement
 - Déconnexion requis
 - Non disponible sur tout les modèles;
- Restauration se fait par chargement d'un fichier de configuration précédent;
- Redémarrage requis

Upgrade



Downgrade

admin

FortiGate VM64
v7.0.0 build0066 (GA)

System

Configuration

Change Password

Logout

Backup

Restore

Revisions

Scripts

Backup System Configuration

Backup to Local PC USB Disk

Encryption

Password

Confirm password

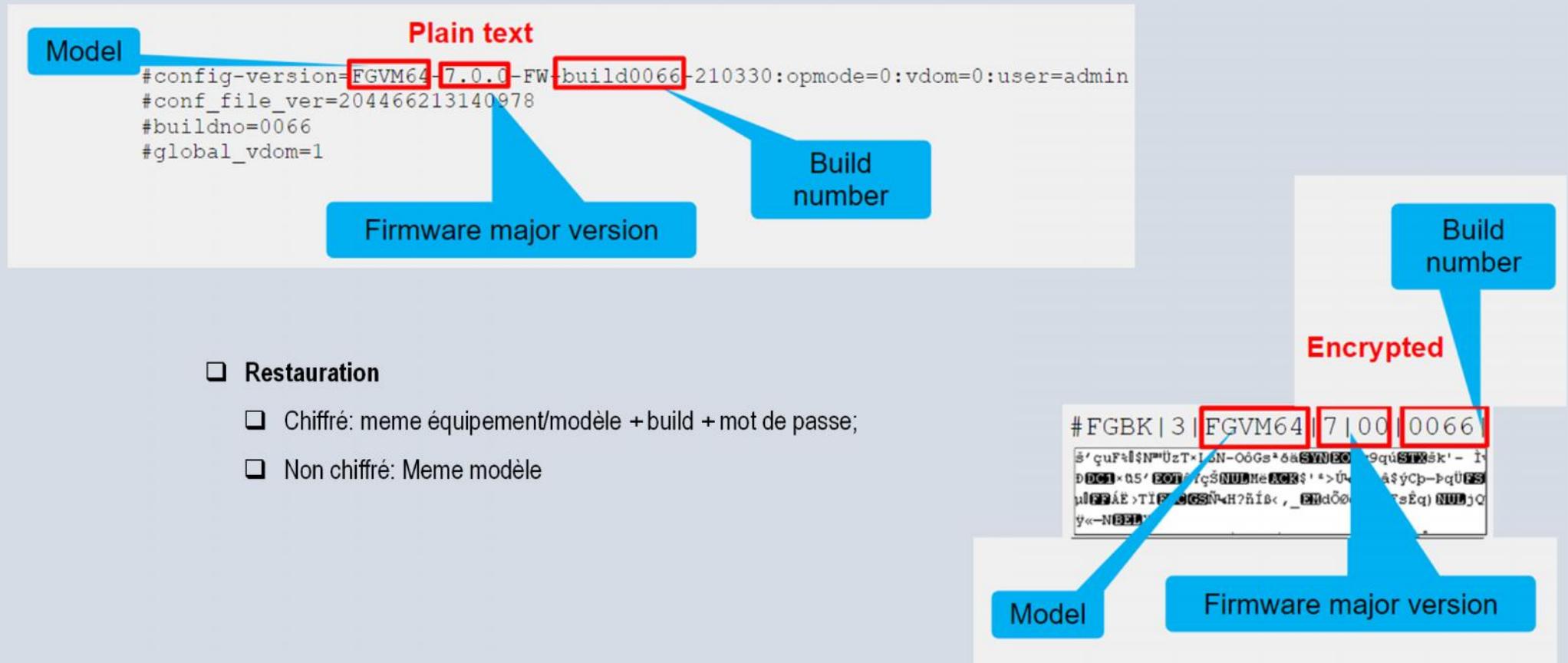
OK Cancel

Maintenance de base

Sauvegarde/Restauration (suite)

Upgrade

Downgrade



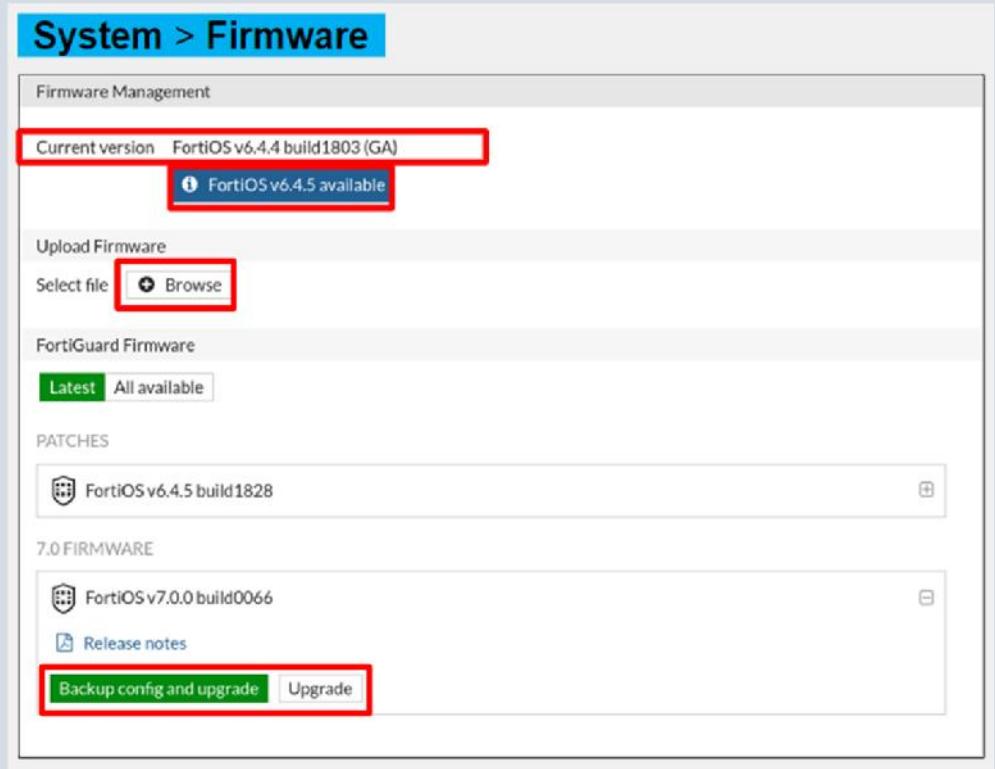
Maintenance de base

Sauvegarde/Restauration

- Vérification de la version du Firmware
 - GUI: System>Firmware;
 - CLI: get system status
- Notification lorsqu'un Firmware disponible;
- Mise à partir d'un fichier;
- Vérification préalable des informations de mise à jour avant l'Upgrade puis:
 - Sauvegarder la configuration;
 - Télécharger une copie de l'actuel Firmware pour prévenir les échecs;
 - Lire attentivement concernant la mise à niveau;
 - Effectuer la mise à niveau.

Upgrade

Downgrade

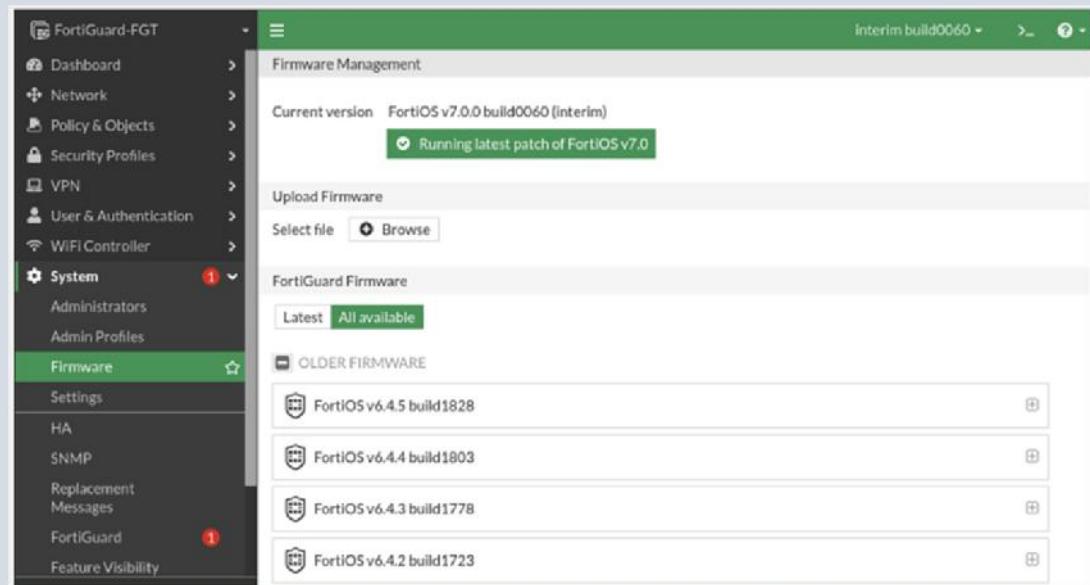


Maintenance de base

Sauvegarde/Restauration

- ❑ Downgrade le Firmware
 - ❑ Avoir une sauvegarde de fichier de configuration avant la mise à niveau;
 - ❑ Télécharger une copie de l'actuel Firmware pour prévenir les échecs;
 - ❑ Avoir un accès physique à la console en cas de rollback;
 - ❑ Télécharger le Firmware;
 - ❑ Si nécessaire, chargé le fichier de configuration qui correspond avec la version actuel du Firmware

Upgrade



Downgrade

Interfaces, routage et portail captif

Objectifs

- Configurer les interfaces réseaux;
- Configurer les services associés aux interfaces;
- Configuration du routage statique et dynamique

Interfaces, routage et portail captif

Interfaces

- Interfaces IP
 - Mode NAT;
 - Adresse IP: statique ou dynamique (DHCP, PPPoE);
 - Peuvent être auto gérés par FortiPAM;
 - Solution de gestion des adresses IP;
 - Solution payante;
 - Destiné au Fabric.
- One-Arm Sniffer
 - N'est pas un mode d'allocation d'adresse IP;
 - Utilisé pour le scan de trafic;
 - Disponible en CLI uniquement

Portail Captif

Network > Interfaces

Network > Interfaces

Edit Interface

Name: port5
Alias:
Type: Physical Interface
VRF ID: 0
Role: Undefined

Address

Addressing mode: Manual DHCP Auto-managed by FortiPAM
IP/Netmask: 0.0.0.0/0.0.0.0
Secondary IP address:

Edit Interface

Name: port5
Alias:
Type: Physical Interface
VRF ID: 0
Role: Undefined

Address

Addressing mode: Manual DHCP Auto-managed by FortiPAM
Retrieve default gateway from server:
Distance: 5
Override internal DNS:

Routage

Interfaces, routage et portail captif

Interfaces (suite)

- ❑ Interfaces IP
 - ❑ Rôle
 - ❑ Définit les paramètres des interfaces ;
 - ❑ Prévention des erreurs de configuration;
 - ❑ 04 types:
 - ❑ LAN;
 - ❑ WAN;
 - ❑ DMZ;
 - ❑ Undefined (tous les paramètres)
- ❑ Alias
 - ❑ Nom de l'interface;
 - ❑ Utilisé pour identifier les interfaces dans la liste des politiques pare-feu;

Portail Captif

Routage

The diagram illustrates the relationship between interface configuration and firewall policy. On the left, a central node labeled 'Alias' has two arrows pointing to it from the 'Alias' and 'Role' fields in the 'Edit Interface' dialog. Another arrow points from the 'Role' field to the 'Policy & Objects > Firewall Policy' screen below.

Network > Interfaces

Edit Interface	
Name	port3
Alias	Internal_Network
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	LAN
Addressing m	WAN
IP/Netmask	DMZ
Secondary IP address	Undefined
	10.0.1.254/255.255.255.0

Policy & Objects > Firewall Policy

+ Create New Edit Delete Policy Lookup Search Q				
Interface Pair View By Sequence				
Name	From	To	Source	Destination
Full_Access	Internal_Network (port3)	port1	LOCAL_SUBNET	all
Implicit Deny	any	any	all	all

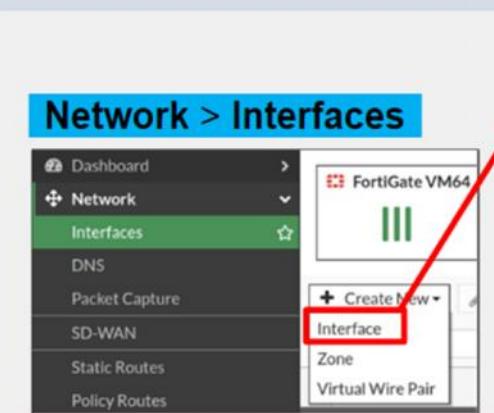
Interfaces, routage et portail captif

Interfaces (suite)

- ❑ Interfaces IP
 - ❑ Agrégation de lien
 - ❑ Combinaison de plusieurs lien physique en un lien logique ;
 - ❑ Augmentation de la bande passante;
 - ❑ Redondance et Haute disponibilité.

Portail Captif

Routage



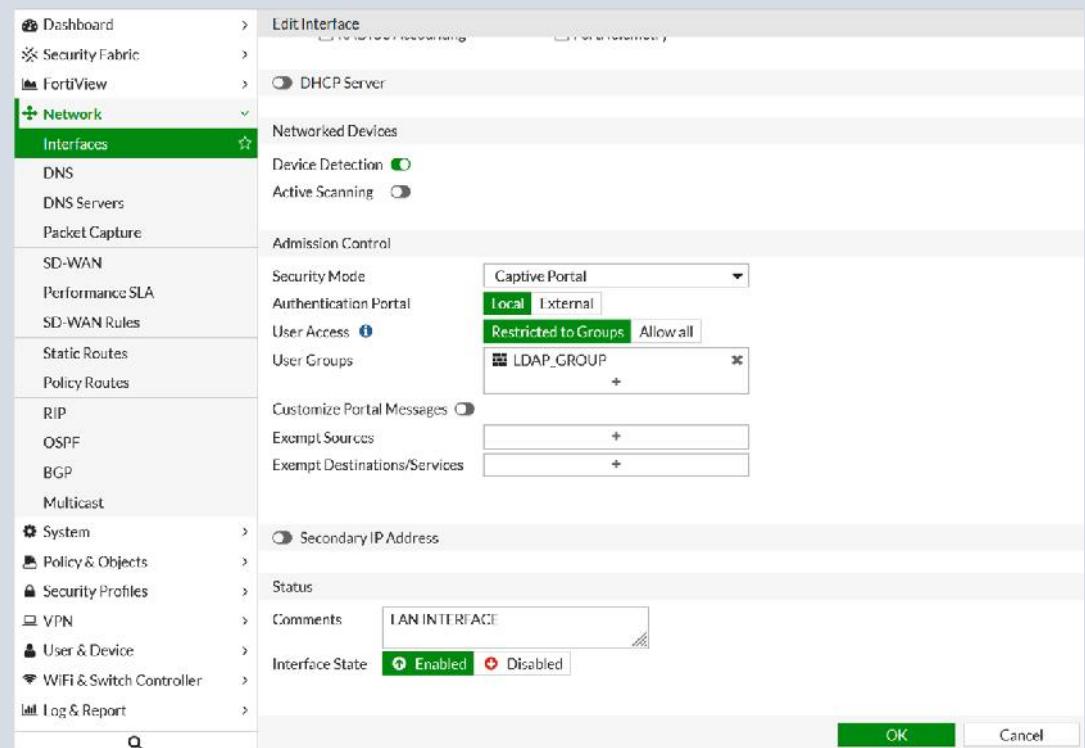
The screenshot shows the 'New Interface' configuration window. The 'Name' field is set to 'Link_Agg'. The 'Type' dropdown is set to '802.3ad Aggregate'. The 'VRF ID' dropdown is set to '0'. The 'Interface members' section contains 'port6' and 'port7'. The 'Role' dropdown is set to 'LAN'. In the 'Address' section, the 'Addressing mode' dropdown has 'Manual' selected. The 'IP/Netmask' field is set to '10.0.5.1/24'. The 'Create address object matching subnet' checkbox is checked. The 'Name' field under 'Address' is set to 'Link_Agg address'. The 'Destination' field is set to '10.0.5.1/24'. The 'Secondary IP address' checkbox is unchecked. In the 'Administrative Access' section, there are checkboxes for 'HTTPS', 'SSH', 'RADIUS Accounting', 'PING', 'SNMP', 'Security Fabric Connection', 'FMG-Access', and 'FTP'. Under 'Receive LLDP', the 'Use VDOM Setting' button is green and 'Enable' is selected. Under 'Transmit LLDP', the 'Use VDOM Setting' button is green and 'Enable' is selected.

Interfaces, routage et portail captif

Interfaces

- Interfaces IP
- Portail captif
 - Gestion et régulation de l'accès à internet aux utilisateurs finaux;
 - Configuration au niveau de l'interface LAN;
 - Intégration des sources d'authentification externe (LDAP);
 - Personnalisation de la page d'authentification.

Portail Captif



Routage

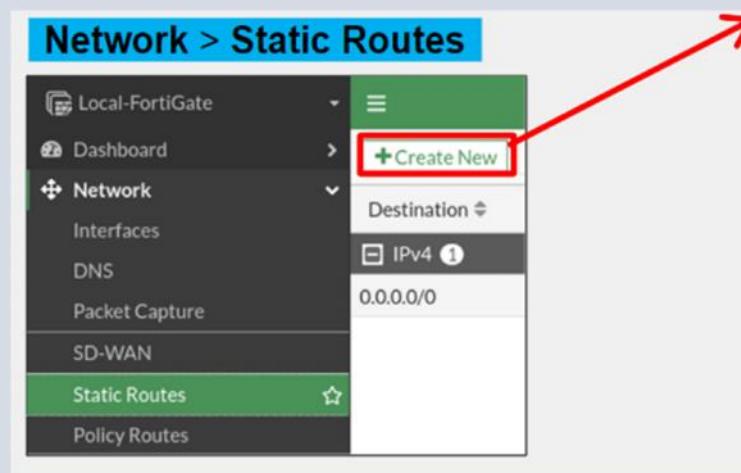
Interfaces, routage et portail captif

Interfaces

Portail Captif

Routage

- Routage Statique
 - Au moins une Gateway configuré (internet);
 - Gateway ajouter dynamiquement si interface DHCP ou PPPoE;
 - Nécessaire pour le bon fonctionnement de certains politiques de pare-feu;



New Static Route

Destination <small>i</small>	Subnet Internet Service 0.0.0.0/0.0.0.0
Gateway Address	0.0.0.0
Interface	(dropdown menu)
Administrative Distance <small>i</small>	10
Comments	Write a comment... 0/255
Status	<input checked="" type="button"/> Enabled <input type="button"/> Disabled
Advanced Options	
Priority <small>i</small>	0

OK Cancel

Interfaces, routage et portail captif

Interfaces

☐ Routage Dynamique

The screenshot shows the FortiView interface under the Network tab. The left sidebar includes options like Dashboard, Security Fabric, FortiView, Network (selected), Interfaces, DNS, DNS Servers, and Packet Capture. Under Network, the sub-menu shows SD-WAN, Performance SLA, SD-WAN Rules, Static Routes, Policy Routes, RIP (selected), OSPF, BGP, and Multicast. The main pane displays the RIP configuration. It shows the current version as 1.2. There is a 'Networks' section with an IP/Netmask input field. Below it is an 'Interfaces' section with a table for creating new interfaces. The table has columns for Name, Version, Authentication, and Passive. A note says 'No matching entries found'. Under 'Advanced Options', there is a 'Default Metric' input field set to 1, and a 'Inject Default Route' toggle switch which is turned off. The 'Timers' section includes 'Update' (30 seconds), 'Timeout' (100 seconds), and 'Garbage' (120 seconds). The 'Redistribute' section lists Connected (off), Static (off), OSPF (off), BGP (off), and ISIS (off). At the bottom right is a green 'Apply' button.

Portail Captif

Routage (suite)

The screenshot shows the FortiView interface under the Network tab. The left sidebar includes options like Dashboard, Security Fabric, FortiView, Network (selected), Interfaces, DNS, DNS Servers, and Packet Capture. Under Network, the sub-menu shows SD-WAN, Performance SLA, SD-WAN Rules, Static Routes, Policy Routes, RIP, OSPF (selected), BGP, and Multicast. The main pane displays the OSPF configuration. It shows the Router ID as 0.0.0.0. There is a 'Areas' section with a table for creating new areas. The table has columns for Area ID, Type, and Authentication. A note says 'No matching entries found'. Below it is a 'Networks' section with a table for creating new networks. The table has columns for Network and Area. A note says 'No matching entries found'. The 'Interfaces' section is identical to the one in the RIP configuration screenshot. Under 'Advanced Options', there is a 'Inject Default Route' toggle switch which is turned off, and three radio buttons: 'Never' (selected), 'Regular Areas', and 'Always'. The 'Passive Interfaces' section has a '+' button. The 'Redistribute' section lists Connected (off), Static (off), RIP (off), BGP (off), and ISIS (off). At the bottom right is a green 'Apply' button.

FORTINET®

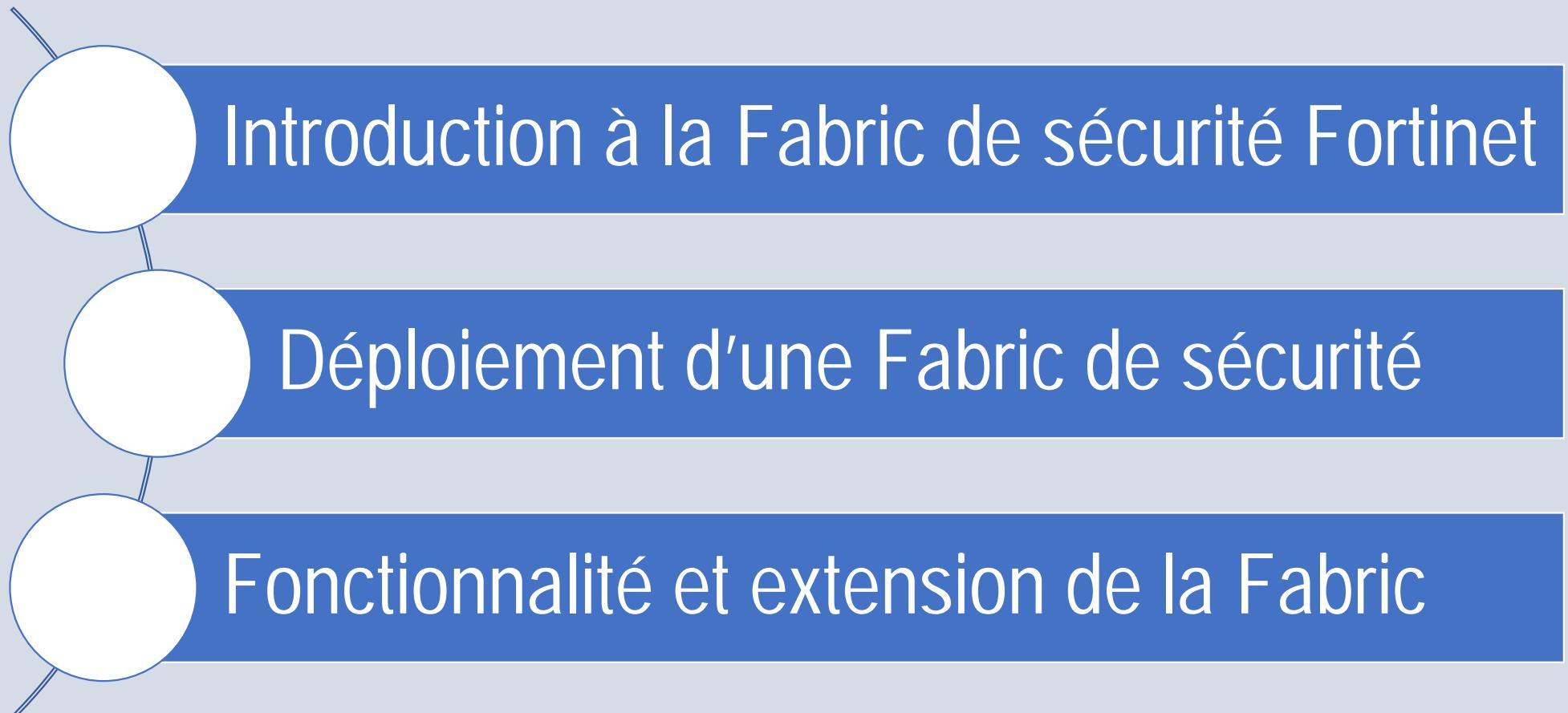


FortiGate Security

FABRIC DE SECURITE



Plan du module



Introduction à la Fabric de sécurité Fortinet

Objectifs

- Définir une Fabric de sécurité Fortinet ;
- Identifier l'importance de la Fabric de sécurité ;
- Identifier les équipement Fortinet pouvant faire parti d'une Fabric de sécurité.

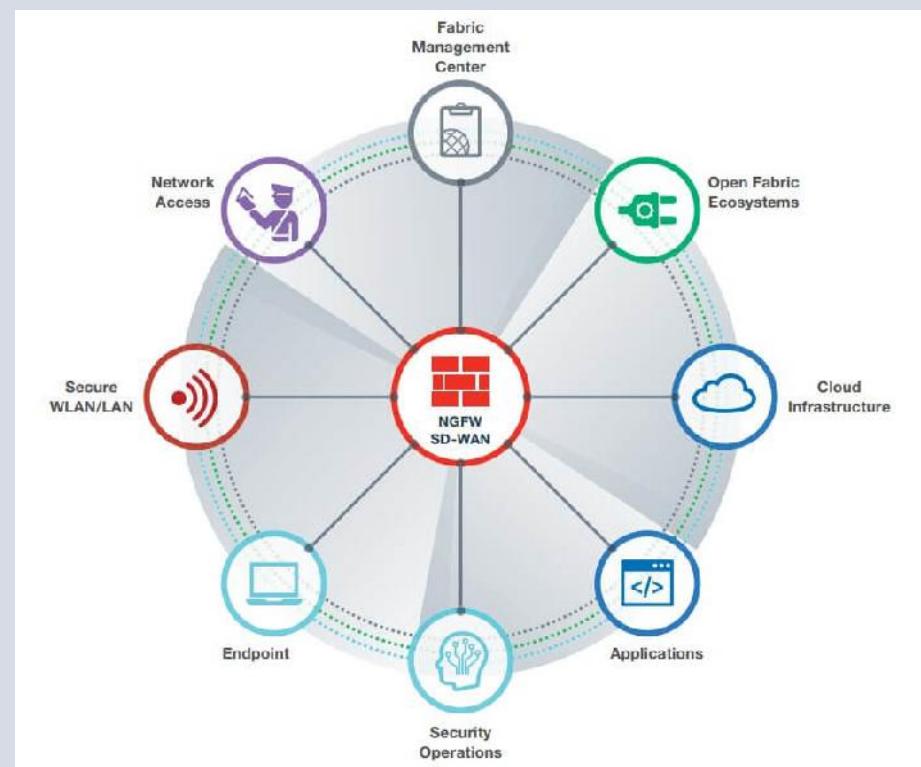
Fabric de sécurité Fortinet: Introduction

Fabric de sécurité

- Fabric de sécurité Fortinet
 - Solution de sécurité entreprise ;
 - Vue d'ensemble globale de l'environnement de défense réseau (des endpoints physiques au VM dans le cloud);
 - Gestion centralisée et automatisée des mécanismes de défense ;
- Caractéristiques :
 - Broad: entière visibilité de la surface d'attaque pour une meilleure gestion des risques;
 - Intégrated: réduit la complexité dans la prise en charge des produits;
 - Automated: permet un échange des informations sur les menaces entre les équipements réseau en temps pour des réponses automatisées face aux menaces
- Intégration avec les API et protocoles d'autre constructeurs disponible d'où il est considéré comme: open

Importance

Produits/Equipements de la Fabric



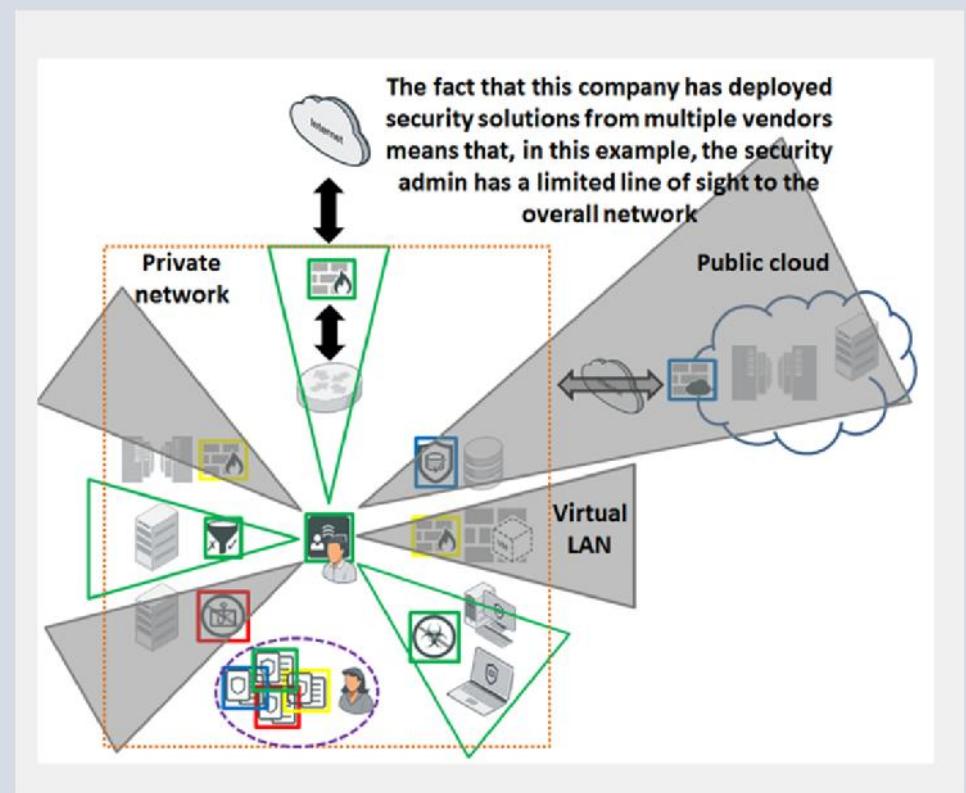
Fabric de sécurité Fortinet: Introduction

Fabric de sécurité

- Pourquoi une Fabric de sécurité?: Causes
 - Evolution des technologies réseaux et augmentation des risques d'attaque ;
 - Intégration des solutions de sécurité de différents constructeurs afin d'adresser les problèmes de sécurité;
 - Manque de visibilité sur la défense globale du réseau.
- Conséquences :
 - Augmentation du risque d'infiltrations et d'attaques;
 - Expansion de la surface d'attaques;
 - Non maîtrise du périmètre de sécurité.
- Solutions
 - Construire une approche globale de gestion de la sécurité, qui offrirait vue dégagée sur tous les points d'infiltration potentiels et aiderait à coordonner les défenses afin de contenir et neutraliser les violations du réseau

Importance

Produits/Equipements de la Fabric

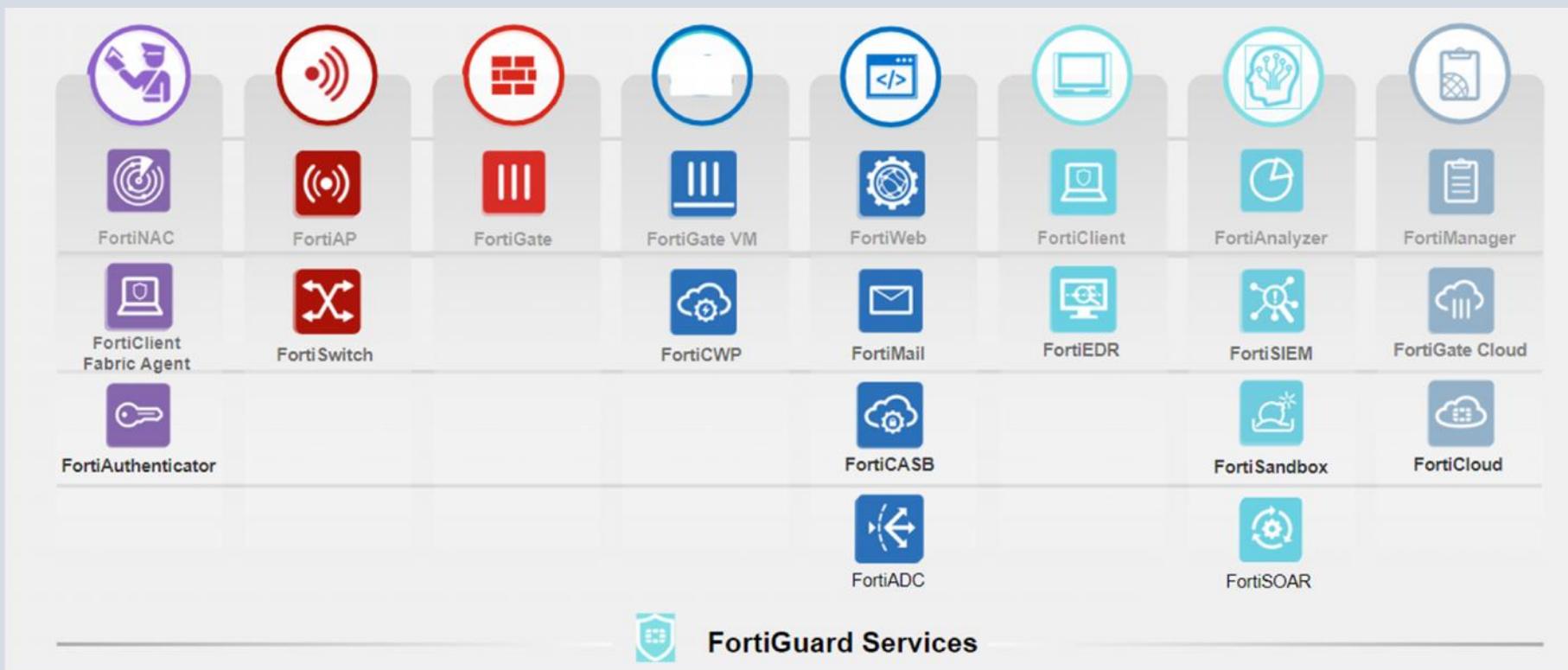


Fabric de sécurité Fortinet: Introduction

Fabric de sécurité

Importance

Produits/Equipements de la Fabric



Fabric de sécurité Fortinet: Introduction

Fabric de sécurité

Importance

Produits/Equipements de la Fabric (suite)

- ❑ Equipements qui composent la Fabric de sécurité
 - ❑ Core: FortiGate (au moins 2) et FortiAnalyze;
 - ❑ Recommended: pour plus de visibilité Fortinet recommande: FortiManager, FortiAP, FortiClient, FortiSandbox, FortiMail, FortiWeb, FortiAI et FortiSwitch;
 - ❑ Extended: ajout d'autre solution de sécurité réseau avec les API pour l'extension.



Déploiement d'une Fabric de sécurité

Objectifs

- Comment implémenter une Fabric de sécurité ;
- Configuration du Fabric de sécurité sur le FortiGate ;
- Vue d'ensemble sur les Virtuals Domaine (VDOM);
- Comment étendre une Fabric de sécurité.

Déploiement d'une Fabric de sécurité

Implémentation

Configuration

VDOMS

Extension Fabric

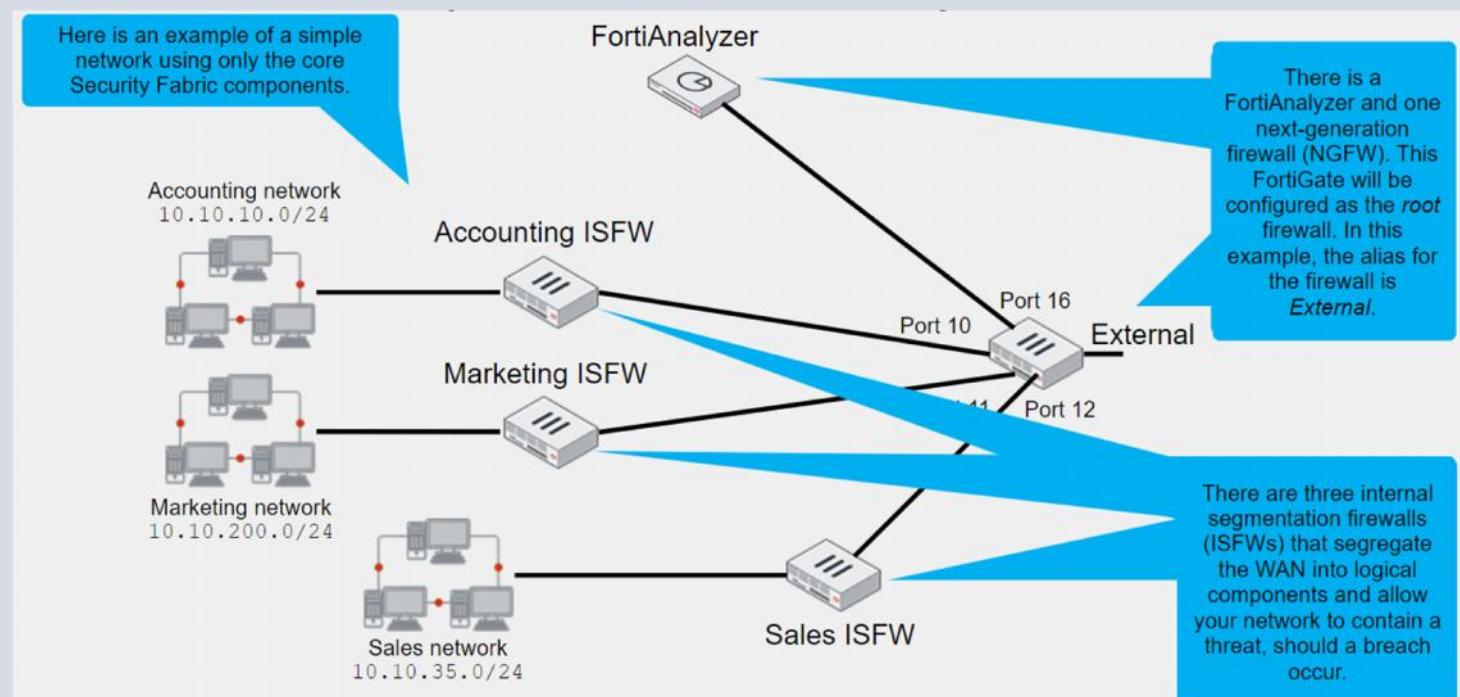
Evaluation de la Sécurité

Equipements centraux:

- FortiGate (External): Pare-feu principal (root);
- FortiAnalyzer

Equipements secondaires:

- Pare-feu des différents départements (downstream);



Déploiement d'une Fabric de sécurité

Implémentation

Configuration

VDOMS

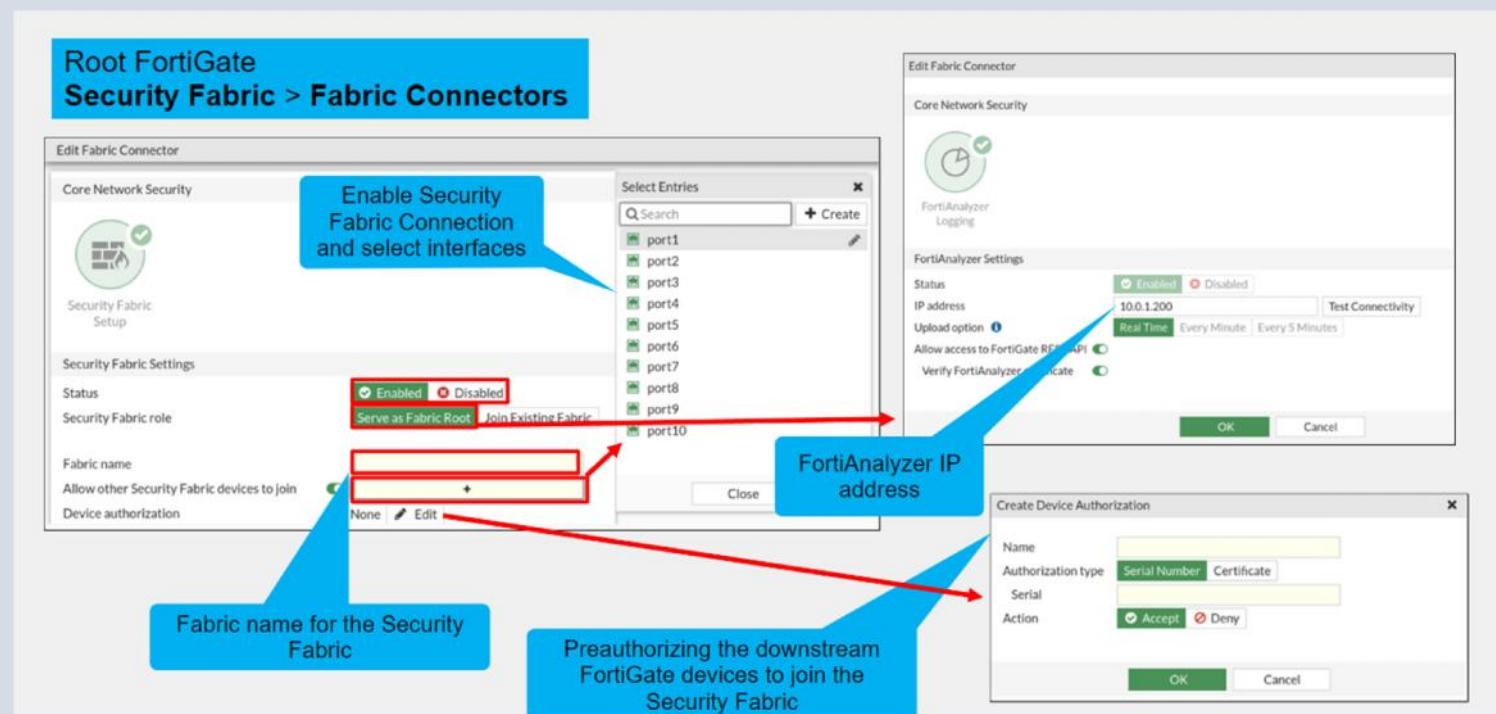
Extension Fabric

Evaluation de la Sécurité

Configuration du Root pare-feu:

- Activer la connexion sur l'interface qui communique avec le downstream;
- Configurer l'IP du FortiAnalyzer;
- Configurer le nom de la Fabric au niveau du root;
- Configurer la préautorisation de connexion du downstream au root (facultatif)

NB: Les configurations du FortiAnalyzer seront automatiquement propagées sur les downstream



Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

Extension Fabric

Evaluation de la Sécurité

Configuration du Downstream pare-feu:

- ❑ Activer la connexion et la détection d'équipement sur l'interface qui communique avec les downstream;
- ❑ Sélectionner join existing Fabric dans le menu Fabric connectors puis ajouter l'IP du root pare-feu;

NB: Les configurations du FortiAnalyzer seront automatiquement propagées par le root sur les downstream

The screenshot displays three panels of the FortiGate management interface:

- Downstream FortiGate Security Fabric > Fabric Connectors**: Shows the "Edit Fabric Connector" screen. It includes sections for Core Network Security (with a gear icon), Security Fabric Setup (with a forticon icon), and Security Fabric Settings. Under Security Fabric Settings, there is a "Status" section with "Enabled" checked and "Disabled" as an option. Below it is a "Join Existing Fabric" button. A callout bubble points to this button with the text "Select Join Existing Fabric". Another callout bubble points to the "Status" section with the text "Add Root FortiGate IP address".
- Downstream FortiGate Network > Interfaces**: Shows the "Administrative Access" section for IPv4. It lists various protocols: HTTPS (checked), HTTP (unchecked), SSH (checked), FTM (unchecked), RADIUS Accounting (unchecked), TELNET (unchecked), and SNMP (unchecked). A callout bubble points to the "SNMP" checkbox with the text "Enable Security Fabric Connection on downstream FortiGate".
- Enable Security Fabric Connection on downstream FortiGate**: Shows the "Edit Fabric Connector" screen for a FortiAnalyzer. It includes sections for Core Network Security (with a forticon icon) and FortiAnalyzer Settings. In the FortiAnalyzer Settings section, there is a note: "Settings will be retrieved from the root FortiGate in the Security Fabric." A callout bubble points to this note with the text "Root FortiGate pushes its FortiAnalyzer configuration to all downstream FortiGate devices".

Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

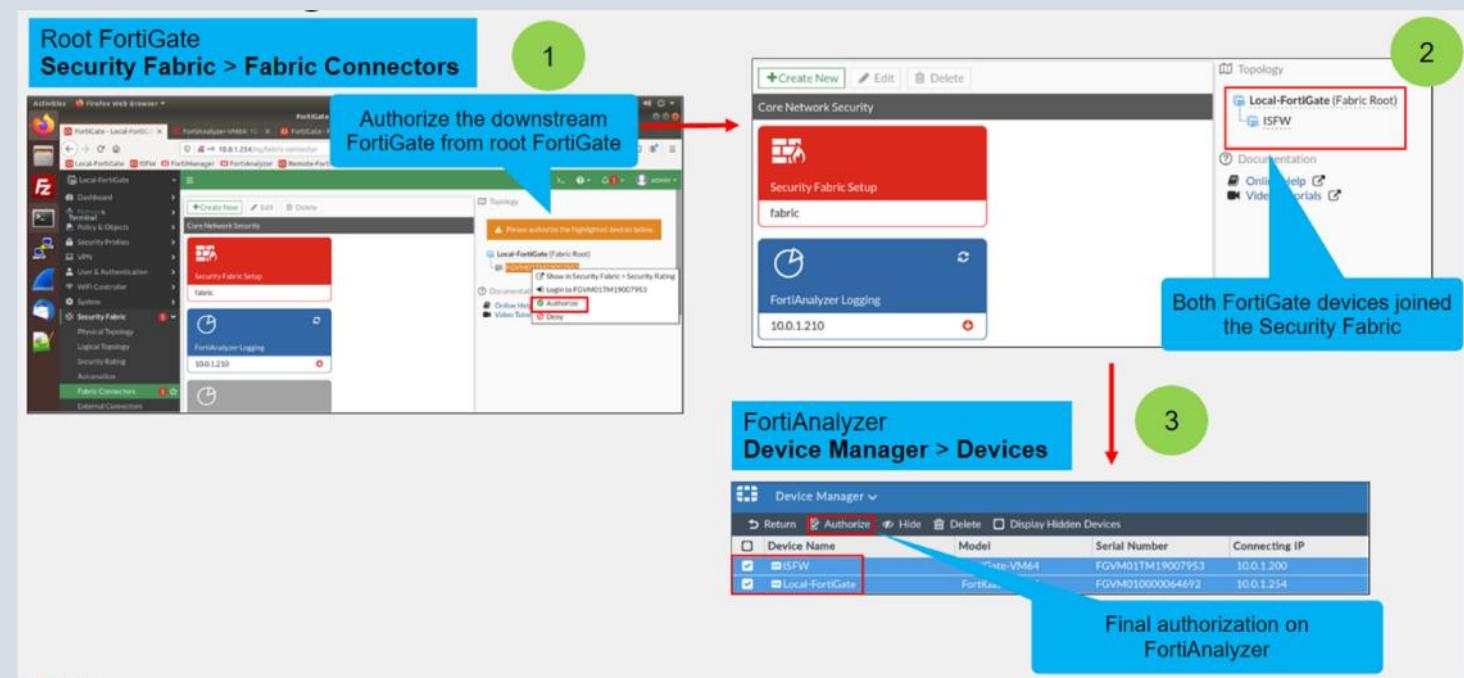
VDOMS

Extension Fabric

Evaluation de la Sécurité

Autorisation du downstream sur les équipements Centraux:

- ❑ Sur le root pare-feu: dans le menu Fabric Connectors
- ❑ Sur le FortiAnalyzer: dans le menu Device manager.



Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

Extension Fabric

Evaluation de la Sécurité

Mécanismes de détection

- ❑ Synchronisation:
 - ❑ Adresses, services, etc;
 - ❑ Faite sur le upstream;
 - ❑ Activer par défaut.

- ❑ Commande de synchronisation: Downstream pare-feu
 - ❑ Set configuration-sync local;
 - ❑ Utilisé au niveau des downstream;
 - ❑ Ne synchronise aucun object au niveau du root;
 - ❑ Objet synchronisé au niveau des downstream.

- ❑ Synchronisation des objets: Activation et désactivation
 - ❑ Objet créé sur les root;
 - ❑ Désactivé par défaut;

- ❑ Commande de synchronisation: Root pare-feu
 - ❑ set fabric-object-unification;
 - ❑ Utilisé uniquement sur le root pare-feu;
 - ❑ Valeur par défaut: default.

Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

Extension Fabric

Evaluation de la Sécurité

Root FortiGate
Security Fabric > Fabric Connectors

The screenshot shows the FortiGate Management Interface under the 'Fabric Connectors' section. A red arrow points from the main interface to the 'Firewall Object Synchronization' dialog. The dialog displays a message: "The following objects require manual intervention in order to synchronize them with the fabric. Click 'Rename All Objects' to automatically resolve all conflicts by renaming them." It also shows a 'Strategy' section with 'Automatic' selected and 'Downstream FortiGates' chosen. Below this is a table with one entry: sync.add_1_Remote-FortiGate, Status: Resolved, Conflicting FortiGate: Remote-FortiGate. A blue callout box highlights the 'Automatic or Manual mode' selection.

Root FortiGate
Security Fabric > Fabric Connectors

This screenshot shows the 'Firewall Object Synchronization' dialog and the 'Topology' view. The dialog has a message: "The following objects require manual intervention in order to synchronize them with the fabric. Click 'Rename All Objects' to automatically resolve all conflicts by renaming them." It includes a 'Strategy' section with 'Automatic' and 'Manual' options, and a table showing synchronization status. The 'Topology' view shows a hierarchy: Local-FortiGate (Fabric Root) -> ISFW -> Remote-FortiGate. A blue callout box highlights the 'One downstream FortiGate device is not syn with fabric' message.

Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

Extension Fabric

Evaluation de la Sécurité

Root FortiGate
Security Fabric > Fabric Connectors

The screenshot shows the FortiGate Management interface under the Security Fabric section. A red arrow points from the main dashboard area to a sub-modal window titled "Firewall Object Synchronization". Inside this window, a blue callout box states: "Objects can be synchronized by Automatic or Manual mode". Another blue callout box at the bottom right indicates: "One downstream FortiGate device is not synch with fabric".

Root FortiGate
Security Fabric > Fabric Connectors

This screenshot shows the "Firewall Object Synchronization" dialog box. It displays a message: "The following objects require manual intervention in order to synchronize them with the fabric. Click 'Rename All Objects' to automatically resolve all conflicts by renaming them." Below this, there are tabs for "Automatic" and "Manual" modes, with "Automatic" selected. A table lists synchronization status for various objects, including one entry for "sync_add_1" which is marked as "Content mismatch" and "Resolved".

Root FortiGate
Security Fabric > Fabric Connectors

This screenshot shows the "Topology" section of the interface. It displays a hierarchical tree structure with nodes like "Local-FortiGate (Fabric Root)", "ISFW", and "Remote-FortiGate". To the right of the topology, there are links for "Documentation", "Online Help", and "Video Tutorials".

Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

Extension Fabric

Evaluation de la Sécurité

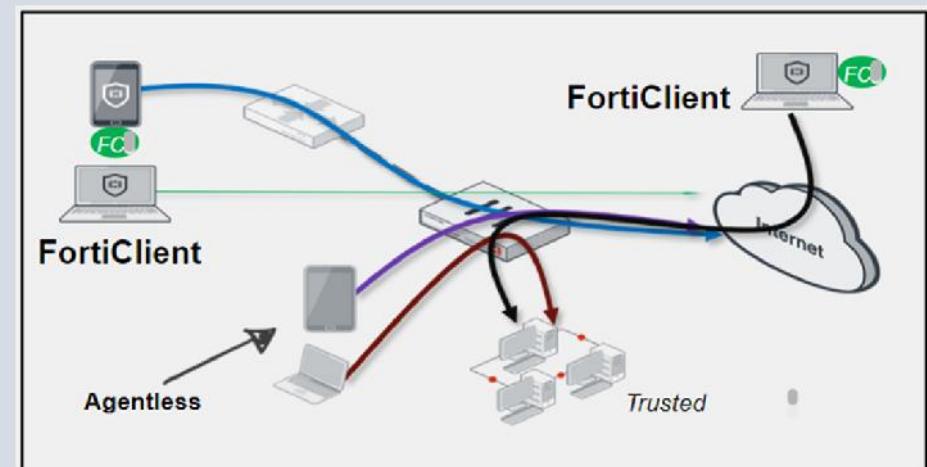
Technique d'identification des équipements dans la Fabric

Sans Agent

- Utile pour avoir une vue d'ensemble de la topologie;
- Nécessite une connexion directe au FortiGate;
- Méthode de détection:
 - Agent HTTP;
 - DHCP;
 - MAC;
 - LLDP;
 - Etc

Avec Agent (FortiAgent)

- Équipement suivi par son FortiAgent User ID (unique)



Déploiement d'une Fabric de sécurité

Implémentation

Configuration (suite)

VDOMS

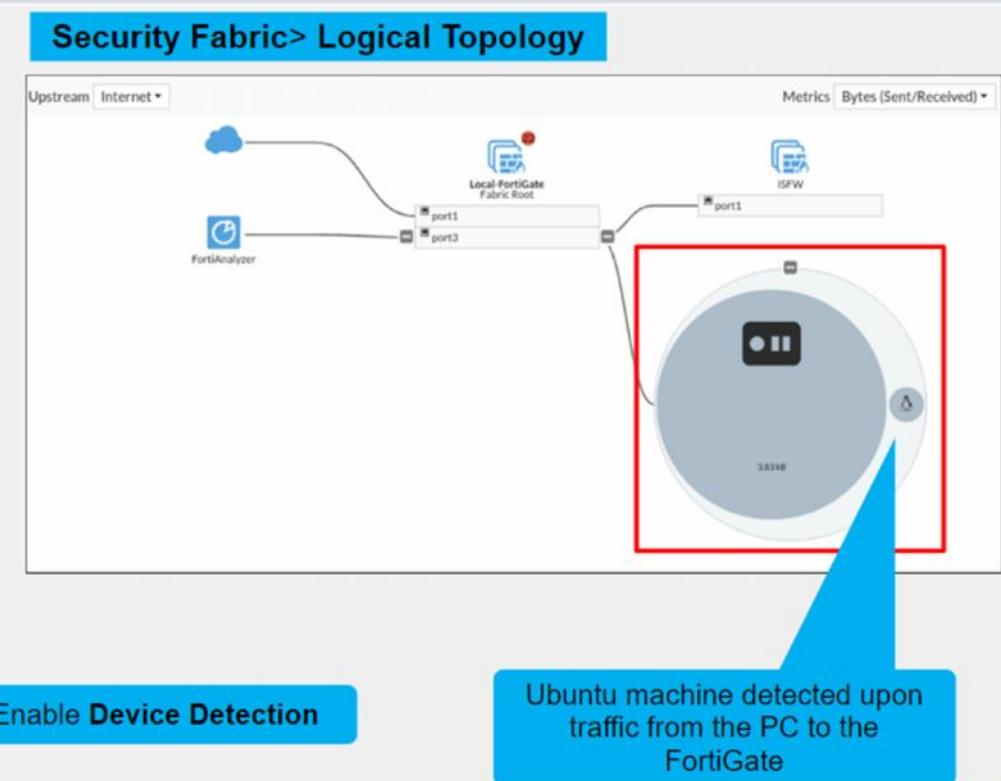
Extension Fabric

Evaluation de la Sécurité

Network > Interfaces

The screenshot shows the 'Edit Interface' configuration for 'port3'. The interface is a Physical Interface assigned to VRF ID 0 and the DMZ role. It has an IP address of 10.0.1.254/255.255.255.0. Under 'Administrative Access', 'Device detection' is enabled (indicated by a red box).

Name: port3
Alias:
Type: Physical Interface
VRF ID: 0
Role: DMZ
Address:
Addressing mode: Manual
IP/Netmask: 10.0.1.254/255.255.255.0
Create address object matching subnet: Off
Secondary IP address: Off
Administrative Access:
IPv4: HTTPS, TELNET, Security Fabric Connection, HTTP, SSH, PING, FMG-Access, FTM, SNMP, RADIUS Accounting
Receive LLDP: Use VDOM Setting, Enable
Transmit LLDP: Use VDOM Setting, Enable
Network:
Device detection:



Déploiement d'une Fabric de sécurité

Implémentation

Configuration

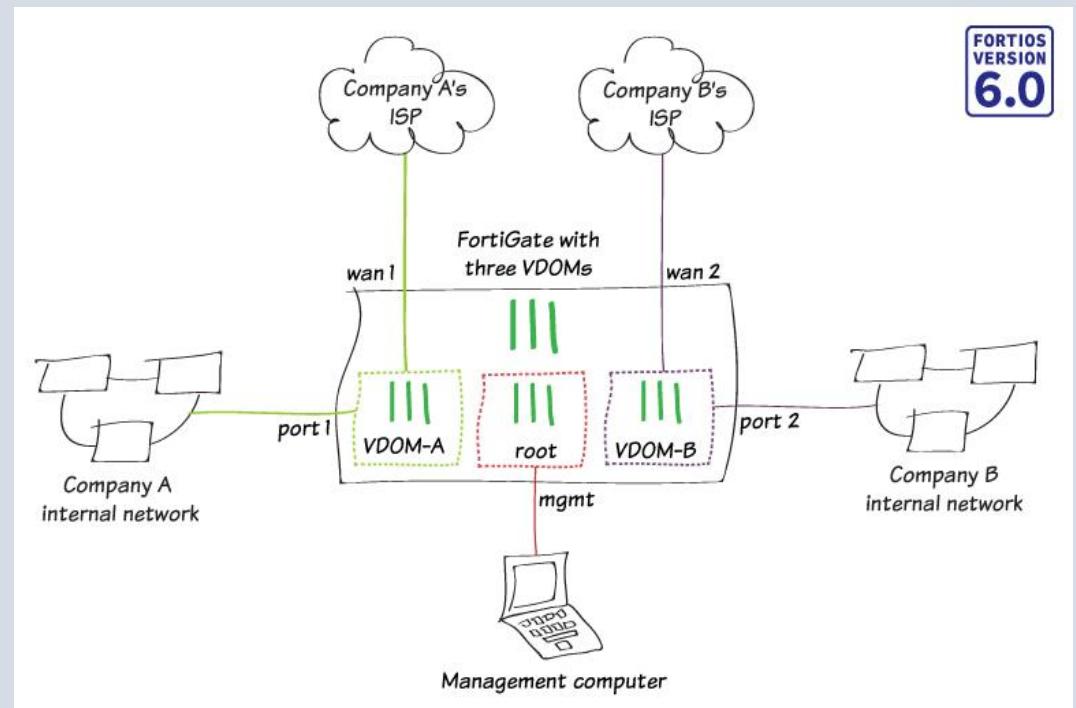
VDOMS

Extension Fabric

Evaluation de la Sécurité

C'est quoi les VDOMs:

- ❑ Technologie utilisé pour diviser le FortiGate en 02 ou plusieurs unité indépendante;
- ❑ Fonctionnalité indépendante: politique pare-feu, NAT, routage et VPN;
- ❑ 02 types de VDOMs:
 - ❑ Split-VDOM: divise l'équipement 02 VDOM uniquement
 - ❑ Root: gestion du trafic;
 - ❑ FG-traffic: gestion de trafic.
 - ❑ Multi-VDOM: possibilité de créer plusieurs VDOMs sur l'équipement fonctionnant chacun comme des pare-feu indépendant.



Déploiement d'une Fabric de sécurité

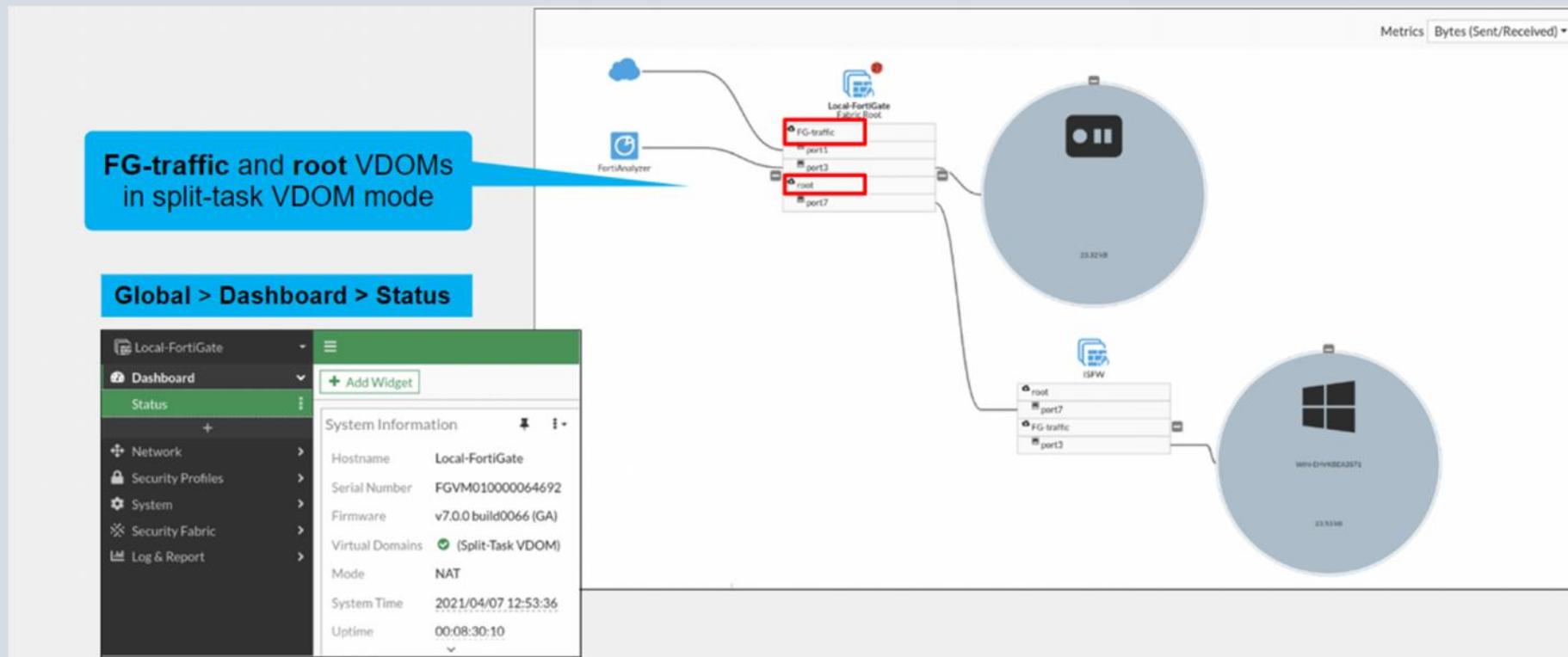
Implémentation

Configuration

VDOMS (suite)

Extension Fabric

Evaluation de la Sécurité



Déploiement d'une Fabric de sécurité

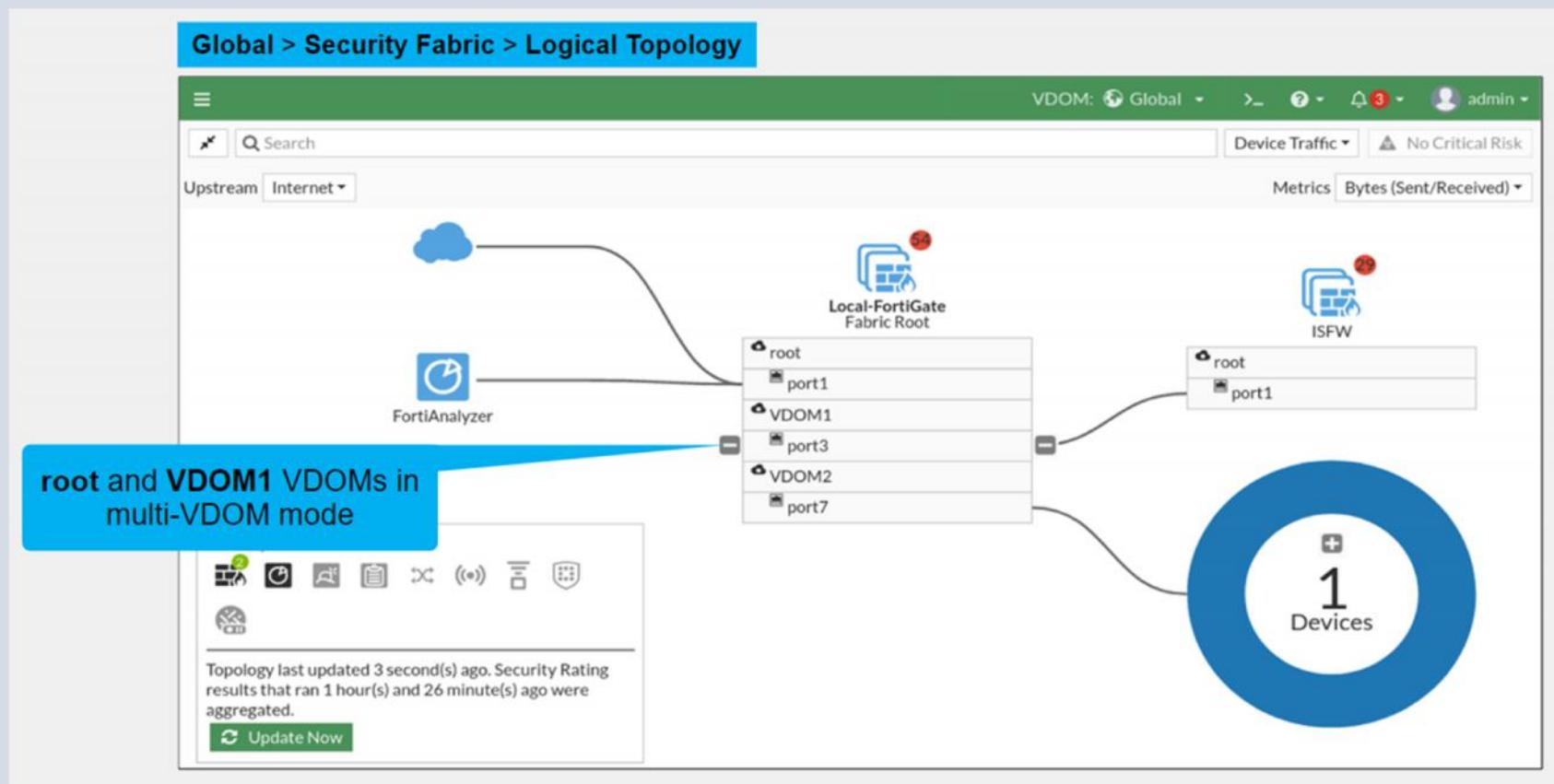
Implémentation

Configuration

VDOMS (suite)

Extension Fabric

Evaluation de la Sécurité



Service d'évaluation

Objectifs

- Etendre une Fabric de sécurité;
- Comprendre les points d'automatisation et la réponse au ménaces;
- Configurer les connecteurs externes ;
- Comprendre le status des widgets de la Fabric.

Extension d'un Fabric de sécurité

Extension

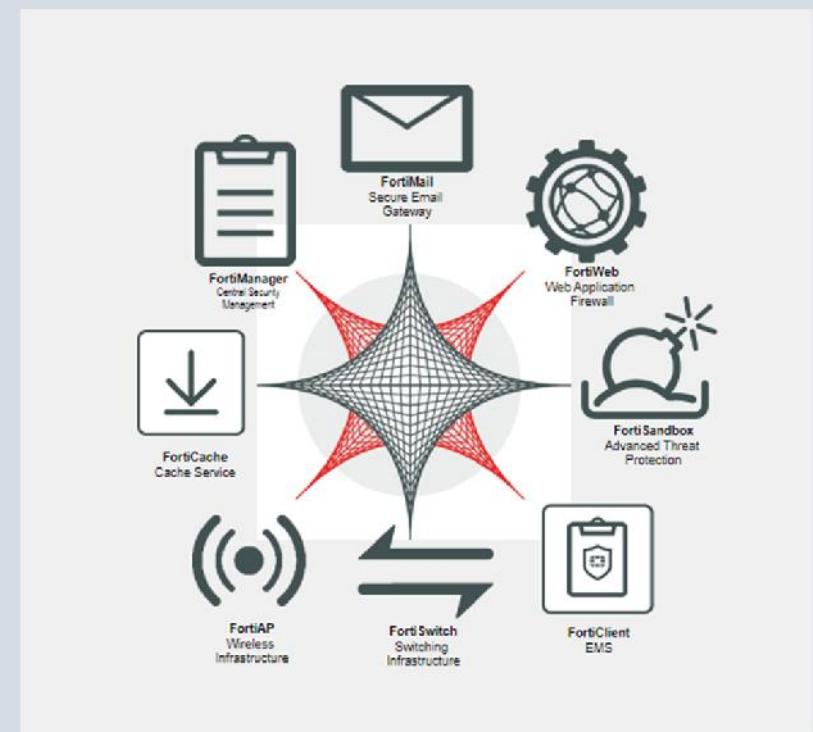
Automatisation

Connecteurs externes

Widgets

Intégration des solutions recommandées:

- FortiManager: Pour la gestion centralisée de tous les équipements de la Fabric;
- FortiSwitch et FortiAP: Pour l'expansion de la Fabric au niveau de la couche d'accès;
- FortiMail;
- Etc.



Extension d'un Fabric de sécurité

Extension

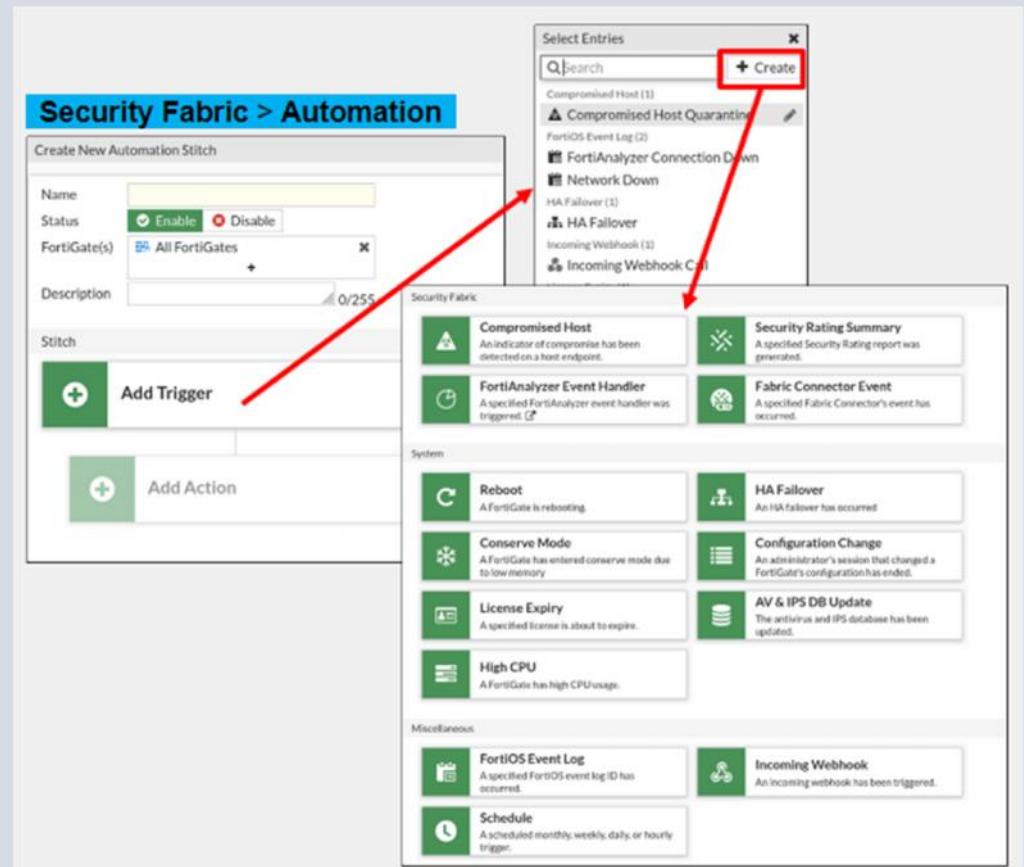
Automatisation

Connecteurs externes

Widgets

Points d'automatisation (stitches):

- Actions d'automatisation basées sur les déclencheurs (triggers);
- Stitches prédefinies disponibles;
- Configuration du Minimum interval.



Extension d'un Fabric de sécurité

Extension

Automatisation

Connecteurs externes

Widgets

The screenshot shows the Fortinet Security Fabric interface under the 'External Connectors' section. A red arrow points from the 'Amazon Web Services (AWS)' icon in the 'Public SDN' section of the main interface to the detailed configuration window on the right.

Security Fabric > External Connectors

New External Connector

Public SDN

- Amazon Web Services (AWS) (selected)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)
- IBM Cloud
- AllCloud

Private SDN

- Kubernetes
- VMware ESXi
- VMware NSX
- OpenStack (Horizon)
- Application Centric Infrastructure (ACI)
- Nuage Virtualized Services Platform

Connector Settings

Name: AWS
Status: Enabled (checked)
Update interval: Use Default

AWS Connector

Access key ID: AKIxxxxxxxxxxxxxx
Secret access key: [REDACTED]
Region name: US-East
VPC ID: vpc-e315g651

Extension d'un Fabric de sécurité

Extension

Automatisation

Connecteurs externes

Widgets

- ❑ Bleu: Equipements connectés au réseau;
- ❑ Orange: Equipements non autorisés connectés au réseau;
- ❑ Rouge: Equipements qui ne sont pas détectés dans le réseau mais sont recommandés pour la Fabric.

The screenshot shows a dashboard titled "Dashboard > Status > Security Fabric widget". The main title is "Security Fabric: Office-Security-Fa". Below the title, there are several icons representing different network components, some with green numbers indicating their status. A red box highlights the "Edge2-Primary" entry in the list below, which is also highlighted with a red box. The list includes the following items:

- Edge2-Primary
- Accounting2
- Marketing2
- Sales2
- FP221B3X13019600
- FP221C3X16004278
- FortiMail
- S248DF3X17000492

FORTINET®



NSE Training Institute

FortiGate Security

POLITIQUES DE PARE-FEU (FIREWALL POLICIES)



Plan du module



Politiques de pare-feu (Firewall Policies)

Objectifs

- Identifier les composants des politiques de pare-feu;
- Identifier comment les pare-feu FortiGate match le trafic au politiques de pare-feu.

Politiques de pare-feu

Vue d'ensemble

Une politique de sécurité définit:

- ❑ les mécanismes de régulations de trafic entre les interfaces ou les groupes d'interface (zone) ;
- ❑ Le processus de correspondance de trafic;

Correspondance de trafic:

- ❑ Vérification se fait du haut vers le bas;
- ❑ Application de la 1ere règle correspondante;
- ❑ Paquet ignoré si aucune correspondance faite parmi les règles: Implicit deny

Mécanismes de correspondances de trafic

Policy & Objects > Firewall Policy										
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	
1	Internet_Access_ISP1	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All	
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All	
0	Implicit	all	all	always	ALL	DENY	Disabled			

Politiques de pare-feu

Vue d'ensemble (suite)

Composant d'une politique de pare-feu

- Interface/Zone
- IP, utilisateurs et services;
- Règles NAT;
- Profil de Sécurité;
- Services;
- Etc.

Types:

- Politique IPv4 /IPv6;
- Cable virtuel;
- Trafic shaping;
- Dos IPv4 / IPv6
- Etc.

Mécanismes de correspondances de trafic

Policy & Objects > Firewall Policy										
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	
1	Internet_Access_ISP1	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All	
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All	
0	Implicit	all	all	always	ALL	DENY	Disabled			

Politiques de pare-feu

Vue d'ensemble (suite)

Mécanismes de correspondances de trafic

Correspondance de trafic

- Interface source;
- Interface de destination;
- IP Source;
- IP destination;
- Service;
- Programmation;
- Action: Accepter / Rejeter

Policy & Objects > Firewall Policy

Name	<input type="text"/>
Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="text"/> +
Destination	<input type="text"/> +
Schedule	<input checked="" type="radio"/> always
Service	<input type="text"/> +
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY

Incoming and outgoing interfaces	✓
Source: IP address, user, internet services	✓
Destination: IP address or Internet Services	✓
Services	✓
Schedules	✓
Action = ACCEPT or DENY	

Configuration des politiques de pare-feu

Objectifs

- Configurer un politique de pare-feu;
- Configuration du logging.

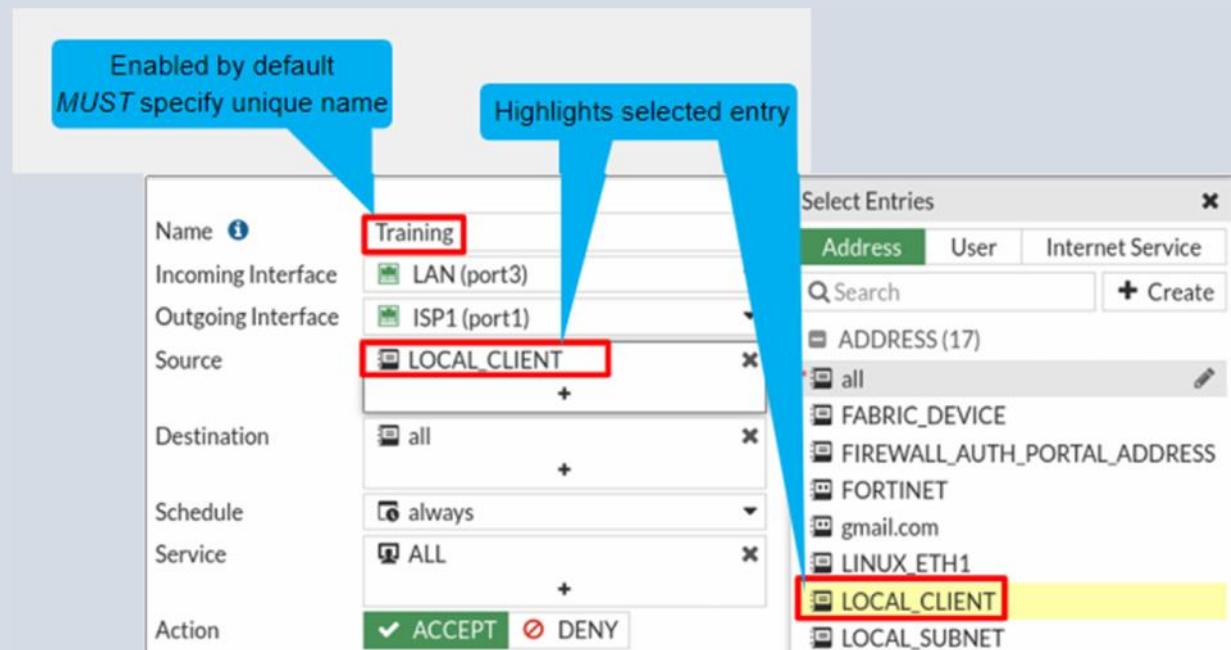
Configuration des politiques de pare-feu

Configuration

Correspondance de trafic

- Interface source;
- Interface de destination;
- IP Source;
- IP destination;
- Service;
- Programmation;
- Action: Accepter / Rejeter

Logging



Trafic Shapers

Configuration des politiques de pare-feu

Configuration (suite)

Profils de sécurité

- Configuré au niveau de la politique de pare-feu;
- Régule l'accès à certaines applications et URL;
- Etc;

Logging

Trafic Shapers

Policy & Objects > Firewall Policy

Security Profiles	
AntiVirus	<input checked="" type="checkbox"/> AV default
Web Filter	<input checked="" type="checkbox"/> WEB default
Video Filter	<input checked="" type="checkbox"/> VF New Profile
DNS Filter	<input checked="" type="checkbox"/> DNS default
Application Control	<input checked="" type="checkbox"/> APP default
IPS	<input checked="" type="checkbox"/> IPS default
File Filter	<input checked="" type="checkbox"/> FF default
VoIP	<input checked="" type="checkbox"/> VOIP default
Web Application Firewall	<input checked="" type="checkbox"/> WAF default
SSL Inspection ⚠	<input checked="" type="checkbox"/> SSL deep-inspection

A red box highlights the "VF New Profile" row. A blue callout bubble points to it with the text: "Default profile not available, you need to manually create a profile".

Configuration des politiques de pare-feu

Configuration (suite)

Logging

Trafic Shapers

Policy & Objects > Firewall Policy

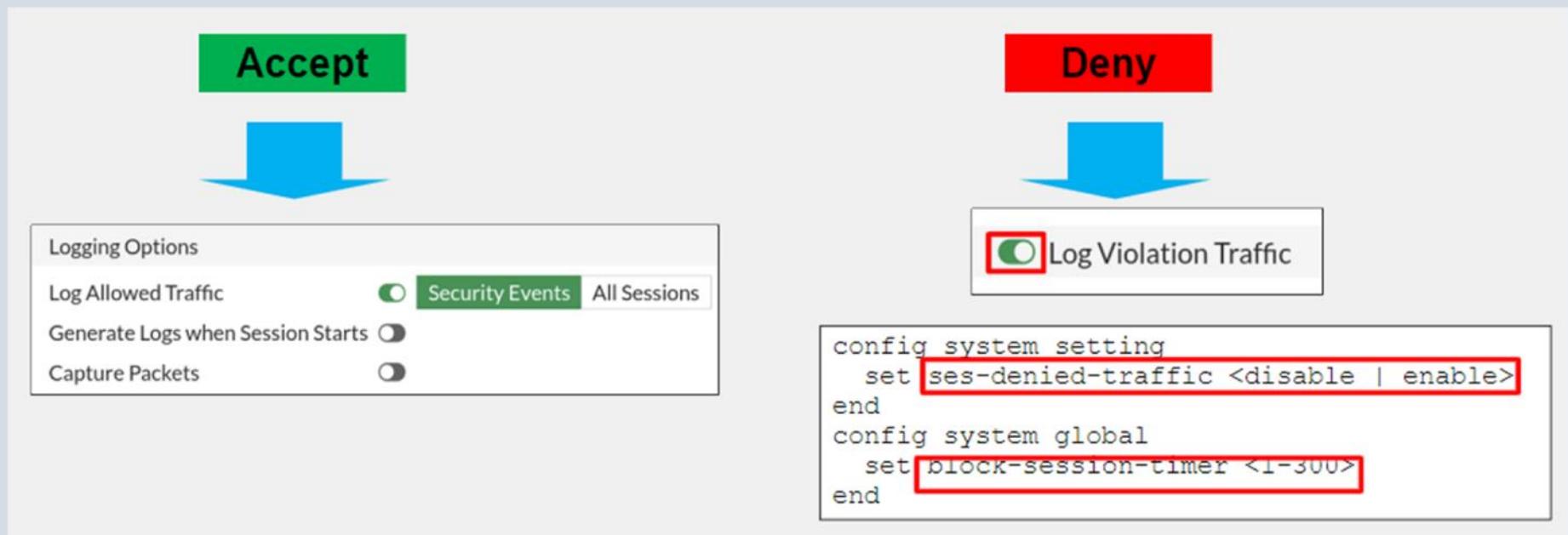
Firewall Policy											IPv4 + IPv6
ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	IPv4 + IPv6
34		port4	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	IPv4 IPv6
44		port4	port3	all	all	always	ALL	ACCEPT	Disabled	certificate-inspection	All
99		port3	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM
91		port2	port2	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM
222		port2	port1	all	all	always	ALL	ACCEPT	ipv4-ippool-1 ipv6-ippool-1	certificate-inspection	UTM
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	all	all	always	ALL	DENY			Disabled

Configuration des politiques de pare-feu

Configuration

Logging

Traffic Shapers



Configuration des politiques de pare-feu

Configuration

Logging

Trafic Shapers

Role:

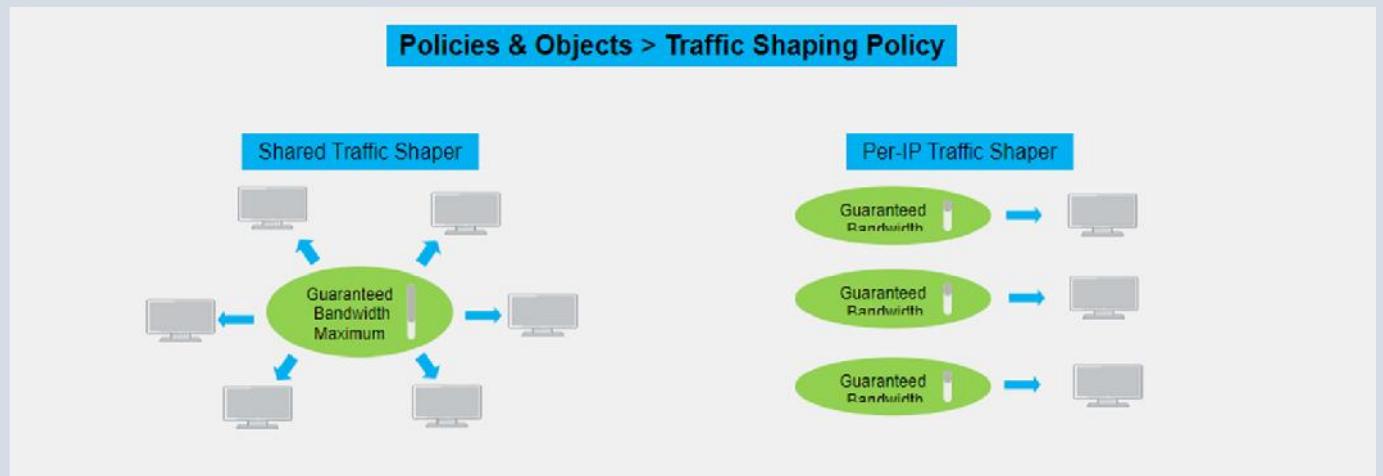
- Limitation de l'utilisation de la BP;

Types:

- Partagé (shared);
- Par IP;

Politiques:

- Partagé: gestion globale;
- Par IP: gestion par IP;
- Control d'application: gestion par application.



Gestion des politiques de pare-feu

Objectifs

- Modifier les paramètres d'affichage des politiques ;
- Comprendre l'utilisation des IDs des politiques;
- Utilisation des objets.

Gestion des politiques

Affichage

Ids des politiques

Objets

Vue par paire

Interface policy pairs

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
port3 → port1	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection	UTM
Full_Access	all	all	always	All	ACCEPT	Enabled	no-inspection	All
port3 → port2								912.05 kB

Vue par séquence

Multiple interfaces

any interface

Name	From	To	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
Fortinet	port3	port1	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection	UTM
Full_Access	port3	port1	all	all	always	All	ACCEPT	Enabled	no-inspection	All
New Interface	port3	any	all	all	always	All	ACCEPT	Enabled	no-inspection	UTM
Implicit Deny	any	any	all	all	always	All	DENY		Disabled	981.97 kB

Gestion des politiques

Affichage

Ids des politiques

Objets

IDs des politiques

- Identifiant;
- Assigné par le système;
- Ne change pas;
- Non visible par défaut sur le

GUI

ID	Name	Source	Destination	Schedule	Service	Action	NAT
2	port3 → port1 ②						
2	Block_FTP	all	all	always	FTP	DENY	
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled
3	port3 → port2 ①						
3	DMZ	DMZ	all	always	ALL	ACCEPT	Enabled

Gestion des politiques

Affichage

Ids des politiques

Objets

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. At the top, a policy is listed with source 'port3' to 'port2'. The source address is 'Web_FTP' (with 'Lan1' and 'Lan2' selected) and the destination service is 'Web-FTP' (with 'DNS', 'FTP', 'HTTP', and 'HTTPS' selected). Both the source and destination groups are highlighted with red boxes. Below the policy list, two configuration windows are shown: 'New Address Group' containing 'Local_LANS' with members 'Lan1' and 'Lan2'; and 'New Service Group' containing 'Web-FTP' with members 'DNS', 'FTP', 'HTTP', and 'HTTPS'. Red arrows point from the highlighted objects in the policy list down to their respective definitions in the configuration windows.

port3 → port2	Web_FTP	Lan1, Lan2	all	always	DNS, FTP, HTTP, HTTPS	ACCEPT	Enabled
---------------	---------	------------	-----	--------	-----------------------	--------	---------

New Address Group	Local_LANS	Group	Members: Lan1, Lan2
-------------------	------------	-------	---------------------

New Service Group	Web-FTP	Comments: Write a comment... 0/255	Members: DNS, FTP, HTTP, HTTPS
-------------------	---------	------------------------------------	--------------------------------

port3 → port2	2	Web_FTP	Local_LANS	all	always	Web-FTP	ACCEPT	Enabled
---------------	---	---------	------------	-----	--------	---------	--------	---------

Quelques bonnes pratiques

Objectifs

- Identifier les conventions de nommage des politiques et des objets;
- Réordonner les politiques.

Quelques bonnes pratiques

Nommage

Règles et restriction:

- 35 caractères max;
- Type de caractères supportés:
 - Chiffres: 0 à 9;
 - Lettres: A à Z (majuscule et minuscule);
 - Caractères spéciaux: -, _
 - Espace.\$
- Autres caractères spéciaux supportés (mot de passe, commentaire, message, etc.)
 - <>, (), #, etc.

Bonnes pratiques

Réorganisation

Recherche

Policy & Objects > Addresses

New Address

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address <input type="radio"/> IPv6 Multicast Address
Name	<input type="text" value="Training(LAN)"/>
Color	<input type="button" value="Change"/>
Type	<input type="button" value="Subnet"/>
IP/Netmask	<input type="text" value="10.0.1.0/24"/>
Interface	<input type="button" value="any"/>
Static route configuration	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Invalid characters: < > () # ' "

Quelques bonnes pratiques

Nommage

Test des politiques avant la production.

Bonnes pratiques

Faire attention lors de la manipulations des politiques et des objets.

Réorganisation

Création des politiques le plus affinés possible.

Recherche

Analyser et activer les paramètres appropriés sur les politiques.

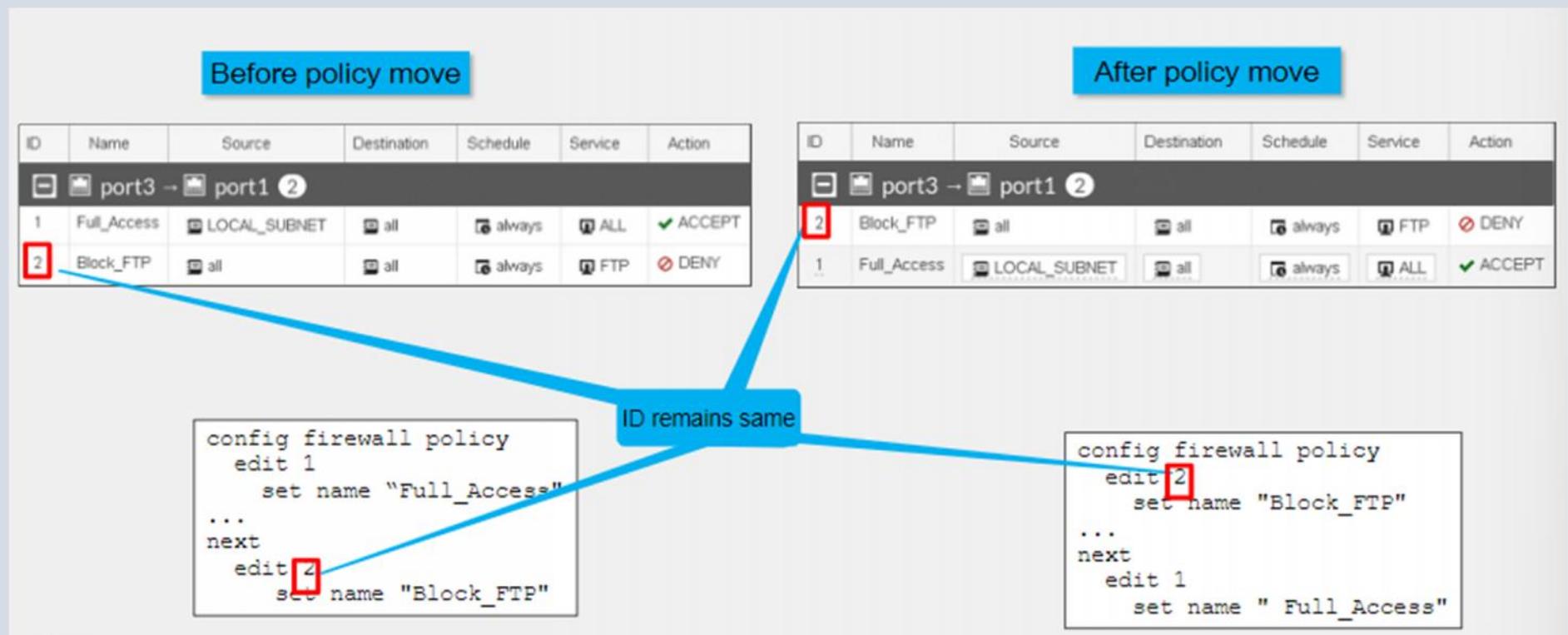
Quelques bonnes pratiques

Nommage

Bonnes pratiques

Réorganisation

Recherche



Quelques bonnes pratiques

Nommage

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. A red arrow points from the 'Policy Lookup' button in the top navigation bar to a search dialog box. The search dialog box contains the following fields:

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	fortinet.com
Destination Port	443

A red button labeled 'Search' is highlighted. Below the search dialog is a table showing firewall policies. The third policy row (Training2) has its entire row highlighted in orange. A red arrow points from the bottom right of the orange-highlighted row to the 'Enabled' column of the third policy row.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	all	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	ALL_ICMP Web Access	ACCEPT	Enabled

Bonnes pratiques

Réorganisation

Recherche

FORTINET®

FORTINET
NSE Training Institute

FortiGate Security

NETWORK ADDRESS TRANSLATION (NAT)



Plan du module



Introduction au NAT

Objectifs

- Comprendre le NAT et le PAT;
- Identifier les différents modes de configuration de NAT disponible.

Introduction au NAT

NAT/PAT

NAT (Network Address Translation):

- Mécanisme permettant d'associer à une IP publique un (one to one) ou plusieurs adresses privées (one to many);
- Permet à un équipement d'agir comme agent de relai entre Internet et le réseau interne;
- NAT Source (SNAT);
- NAT Destination (DNAT).

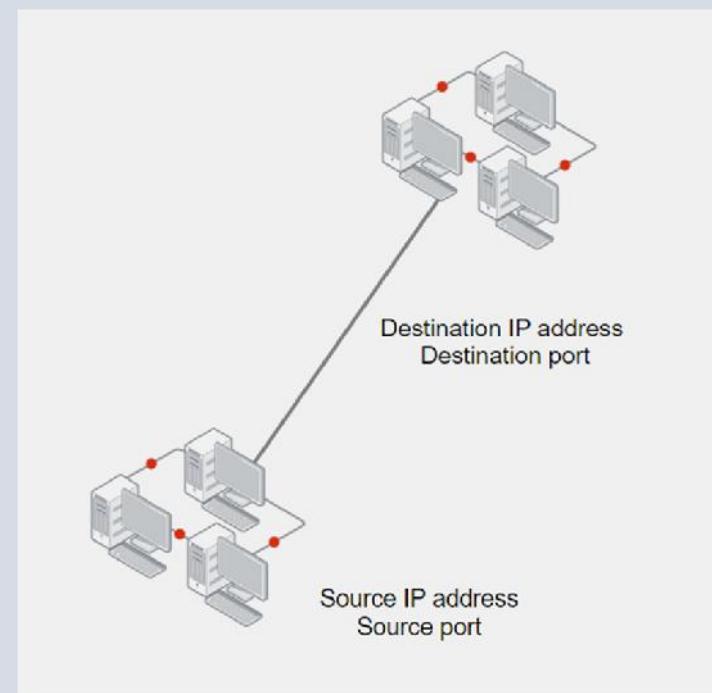
PAT (Port Address Translation)

- Association de plusieurs adresses IPv4 à une seul adresse en utilisant différents ports source;

Rôle:

- Améliorer la sécurité: adresses derrière le NAT sont cachées;
- Amplification d'adresse: plusieurs équipements peuvent utiliser une seul adresse
- Etc;

Modes de configuration



Introduction au NAT

NAT/PAT (suite)

Modes de configuration

Dans FortiOS:

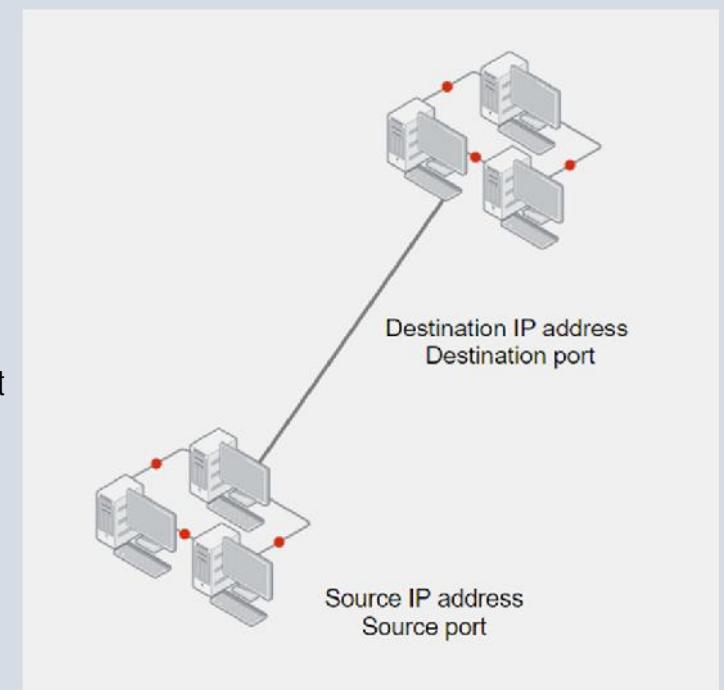
- ❑ Appliqué dans la même firewall policies;
- ❑ Connexion sortante: NAT Central (SNAT) fonction de l'implémentation;
- ❑ Connexion entrante: Virtual IP (DNAT).

NAT 64 et NAT 46

- ❑ Mécanisme permettant aux hôtes avec les adresses IPv6 de communiquer avec les hôtes ayant les adresses IPv4 et vice versa.

NAT 66:

- ❑ Mécanisme de translation d'adresse entre les réseaux IPv6.



Introduction au NAT

NAT/PAT

02 modes de configuration:

- SNAT: NAT source;
- DNAT: NAT de Destination;

Méthodes de configuration:

- Politique NAT
 - SNAT et DNAT configurés pour chaque politique pare-feu;
 - SNAT utilise les adresses ou les pools d'adresses sur les interfaces de sortie;
 - DNAT utilise les VIP (Virtual IP) comme adresse de destination.
- NAT Central
 - SNAT et DNAT configuré par VDOMs;
 - Appliqué à plusieurs politiques pare-feu en fonction des règles SNAT et DNAT configuré;
 - SNAT sont des règles configurées depuis le panneau de politiques de SNAT Central;
 - DNAT sont configurés depuis le panneau DNAT et VIPs.

Modes de configuration

Politiques de NAT

Objectifs

- Configurer une politique NAT pour effectuer le SNAT et le DNAT (VIP);
- Appliquer le SNAT avec un pool d'adresse IP;
- Configurer le DNAT avec les VIPs ou un serveur virtuel.

Politique de NAT

SNAT

DNAT

Configuration du SNAT:

- Adresse de l'interface de sortie;
- Pool d'adresse IP.

Policy & Objects > Firewall Policy

Edit Policy

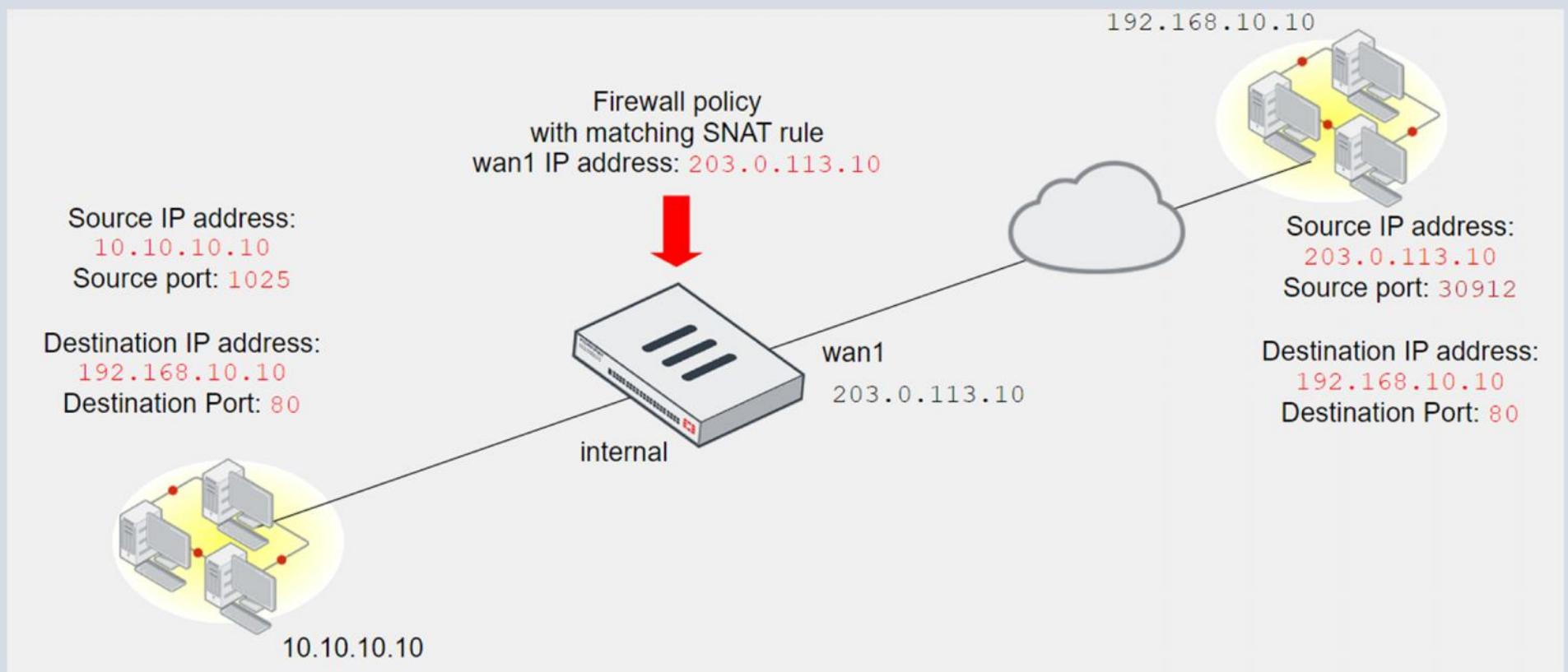
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input checked="" type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="radio"/>
IP Pool Configuration	<input checked="" type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Dynamic IP Pool

Politique de NAT

SNAT (suite)

DNAT

Utilisation de l'interface de sortie

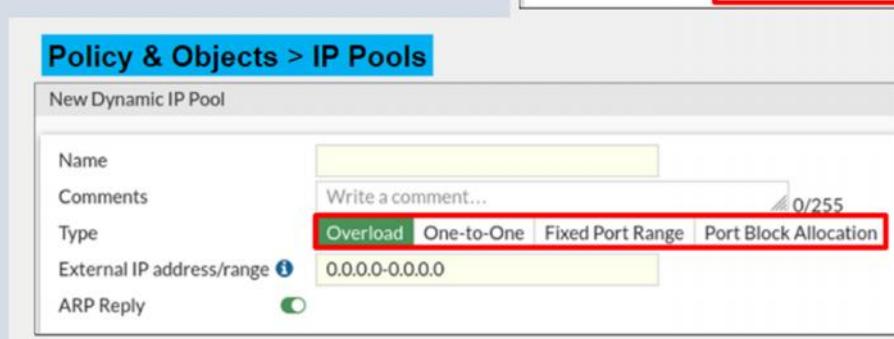
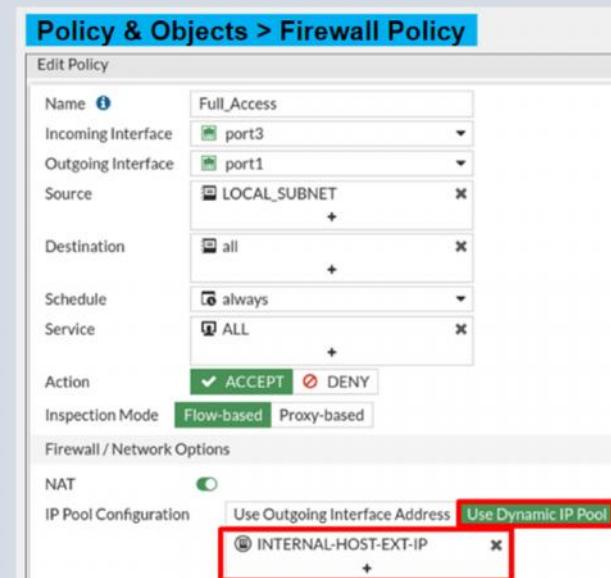


Politique de NAT

SNAT (suite)

Pools d'IP:

- ❑ Adresse ou ensemble d'adresse utilisée comme source comme lors d'une session;
- ❑ Configuré dans la même plage que l'adresse IP de l'interface de sortie;
- ❑ 04 types:
 - ❑ Overload (PAT) – par défaut;
 - ❑ One to One;
 - ❑ Fixed port range;
 - ❑ Port block allocation.

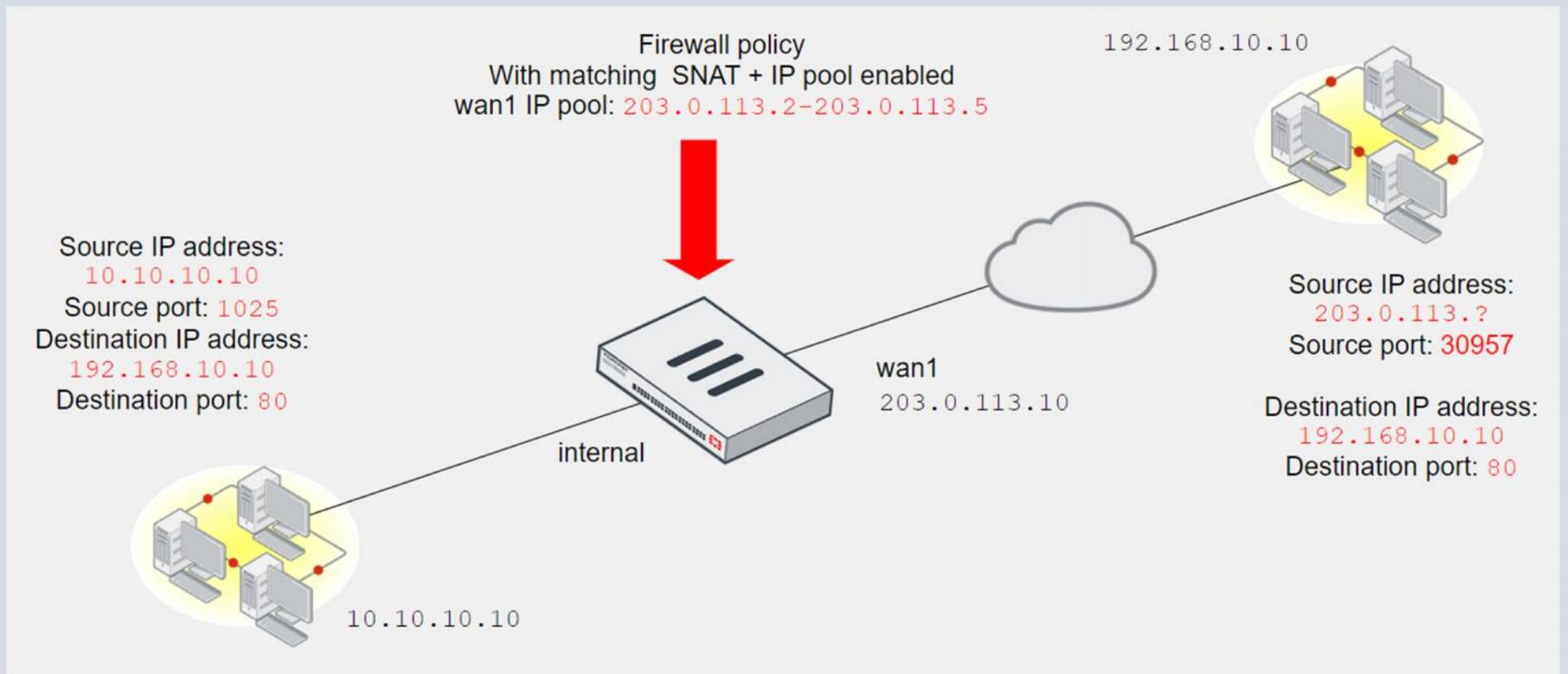


Politique de NAT

SNAT (suite)

DNAT

Pools d'IP: Overload



Politique de NAT

SNAT (suite)

DNAT

Pools d'IP: One to One

- IP interne est associé à une IP public;
- FCFS;
- Association n'est pas fixe;
- Connexion refusé si aucune adresse disponible;
- PAT non nécessaire.

STUDENT # get system session list				
PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION
DESTINATION-NAT				
tcp	3598	10.0.1.10:2706	10.200.1.6:2706	10.200.1.254:80
tcp	3598	10.0.1.10:2704	10.200.1.6:2704	10.200.1.254:80
tcp	3596	10.0.1.10:2702	10.200.1.6:2702	10.200.1.254:80
tcp	3599	10.0.1.10:2700	10.200.1.6:2700	10.200.1.254:443
tcp	3599	10.0.1.10:2698	10.200.1.6:2698	10.200.1.254:80
tcp	3598	10.0.1.10:2696	10.200.1.6:2696	10.200.1.254:443
udp	174	10.0.1.10:2694	-	10.0.1.254:53
udp	173	10.0.1.10:2690	-	10.0.1.254:53

Politique de NAT

SNAT (suite)

DNAT

Pools d'IP: Fixed Port Range

- Définition de la plage d'IP interne et externe.

STUDENT	#	get system session list				
PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT	
tcp	3574	10.0.1.11:60843	10.200.1.8:60843	216.23.154.83:80	-	
tcp	3570	10.0.1.11:60809	10.200.1.8:60809	216.23.154.81:80	-	
tcp	3590	10.0.1.11:60819	10.200.1.8:60819	216.23.154.74:80	-	
tcp	3599	10.0.1.11:60817	10.200.1.8:60817	216.23.154.74:80	-	
tcp	3586	10.0.1.11:60815	10.200.1.8:60815	216.23.154.81:80	-	
tcp	3564	10.0.1.11:60807	10.200.1.8:60807	216.23.154.74:80	-	
tcp	9	10.0.1.10:7112	10.200.1.7:7112	10.200.1.254:80	-	
tcp	7	10.0.1.10:7110	10.200.1.7:7110	10.200.1.254:80	-	
tcp	5	10.0.1.10:7108	10.200.1.7:7108	10.200.1.254:80	-	
tcp	3	10.0.1.10:7106	10.200.1.7:7106	10.200.1.254:80	-	
tcp	1	10.0.1.10:7104	10.200.1.7:7104	10.200.1.254:80	-	

Politique de NAT

SNAT (suite)

DNAT

VIPs:

- Objet du DNAT;
- Type par défaut: NAT Static;
- Autre fonctionnalité disponible en CLI: load-balance ou server-load-balance

The screenshot displays two windows from the FortiOS 'Policy & Objects' section.

Policy & Objects > Virtual IPs: This window shows the configuration for a Virtual IP named 'VIP-INTERNAL-HOST'. The 'Name' field is set to 'VIP-INTERNAL-HOST'. The 'Type' is 'Static NAT', with the external IP address set to '100.64.100.22' and the mapped IP address set to '10.0.1.10'. The 'Interface' is 'port1'. A red box highlights this entire configuration window.

Policy & Objects > Firewall Policy: This window shows the configuration for a policy named 'Web-Server-Access'. The 'Destination' field is set to 'VIP-INTERNAL-HOST'. A red box highlights this destination entry. A blue arrow points from the highlighted 'VIP-INTERNAL-HOST' in the first window to the same entry in the second window. A callout bubble on the right side of the second window states: 'VIP used as destination in firewall policy'.

NAT Central

Objectifs

- Configurer le NAT Central

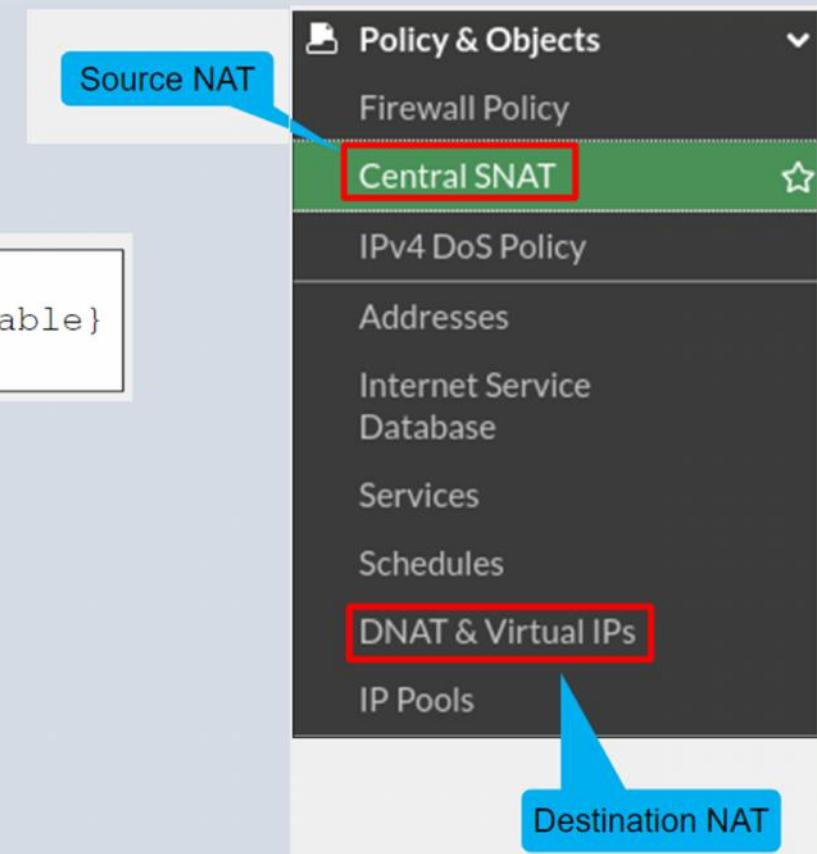
NAT Central

Vue d'ensemble

Central NAT

- Gestion des configuration de NAT de façon centralisée;
- Activation en CLI uniquement;
- 02 options:
 - Central NAT;
 - DNAT & Virtual IP.
- Obligatoire pour mode policy-base.

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



NAT Central

Vue d'ensemble (suite)

Central DNAT&VIPs

Central NAT

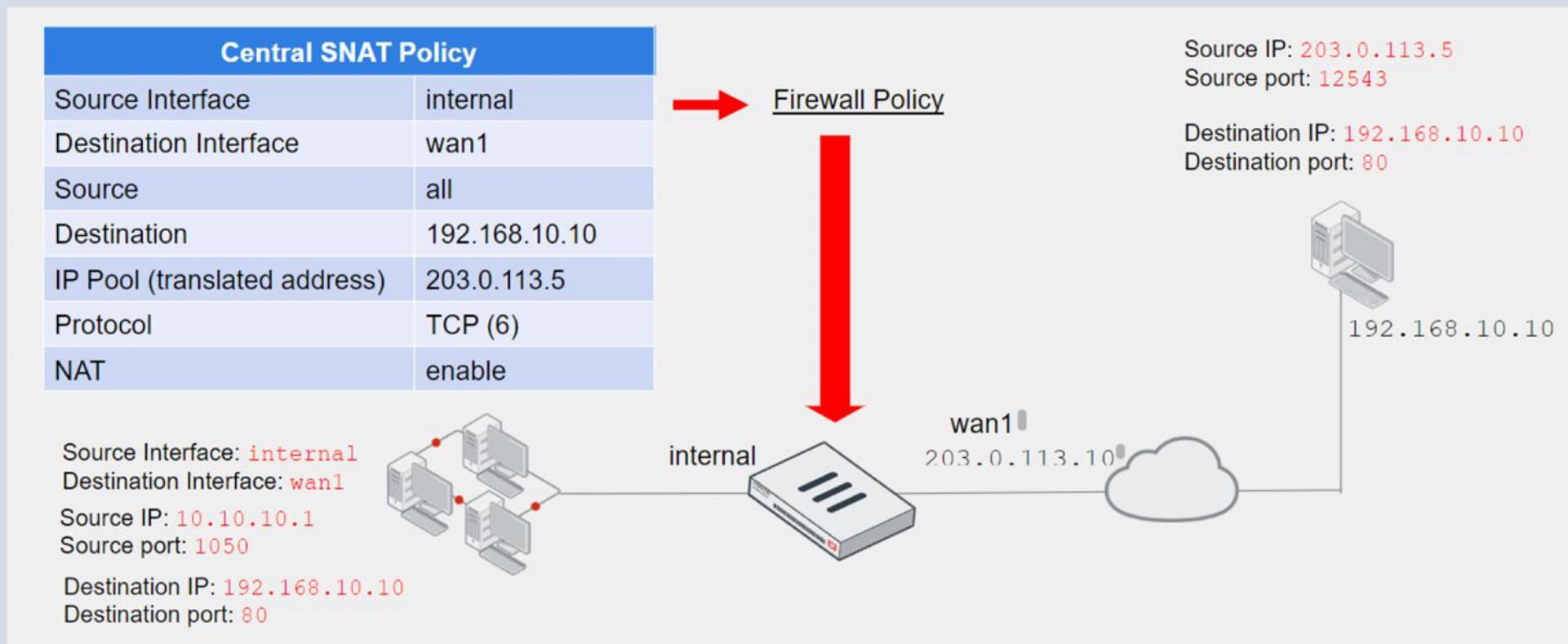
- ❑ Modifie les configurations du SNAT;
- ❑ Définition les pools d'IPs ou utilisation des de l'interface de sortie;
- ❑ Configuration de la politique central;
- ❑ Traitement des politiques du haut en bas;
- ❑ Politique sélectionner en fonction du trafic correspondant au trafic
- ❑ Aucune règle n'est appliquée si aucune correspondance;
- ❑ Critère de correspondance: interface source, interface de destination, adresse source, adresse de destination, protocole, ports (source).

Policy & Objects > Central SNAT						
ID	From	To	Source Address	Destination Address	Translated Address	
IPv4 ②						
1	LAN (port3)	WAN1 (port1)	all	all	SNAT-Pool	
2	port4	WAN2 (port2)	LOCAL_SUBNET	REMOTE_SUBNET	INTERNAL-HOST-EXT-IP	

NAT Central

Vue d'ensemble (suite)

Central DNAT&VIPs



NAT Central

Vue d'ensemble

Central DNAT&VIPs

Central DNAT

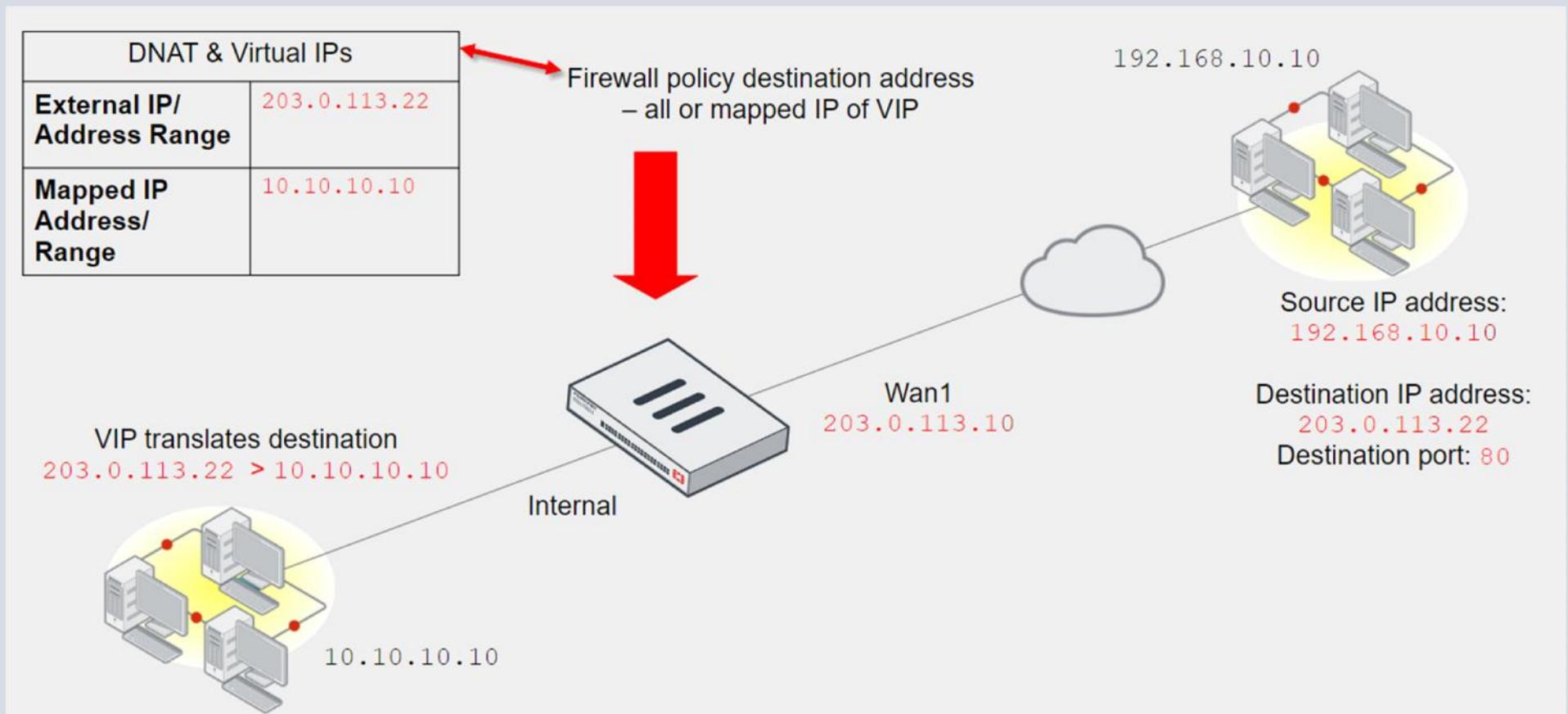
- ❑ Modifie les configurations du DNAT:
 - ❑ Définition des DNAT & Virtual IPs
- ❑ Création d'une règle au niveau du noyau;
- ❑ VIP comme adresse de destination;
- ❑ Désactivation permet l'exclusion d'une VIP;

```
#config firewall vip
    edit "name of the VIP"
        set status disable
    next
end
```

NAT Central

Vue d'ensemble

Central DNAT&VIPs (suite)



Sessions

Objectifs

- Comprendre les tables de sessions;
- Comprendre les sessions TTL;
- Analyser les résultats de la commande 'session diagnose';
- Comprendre les états des protocoles TCP, UDP et ICMP.

Sessions

Table de session

Session TTL

Diagnostic des sessions

Etat des protocoles

Quelques commandes:

- Diagnose sys sessions: ;
- Timers sont configurés dans les paramètres globaux.

TCP default TTL

```
config system session-ttl  
set default 3600  
end
```

Specific state timers

```
config system global  
set tcp-halfclose-timer 120  
set tcp-halfopen-timer 10  
set tcp-timewait-timer 1  
set udp-idle-timer 180  
end
```

Sessions

Table de session

Session TTL

Diagnostic des sessions

Etat des protocoles

Diagnose sys sessions :

- ❑ Fourni les options pour filtrer, effacer et lister les sessions;

```
• diagnose sys session filter ?  
• dport Destination port  
• dst      Destination IP address  
• policy   Policy ID  
• sport    Source port  
• src      Source IP address
```

- diagnose sys session list

- diagnose sys session clear

Sessions

Table de session

Session TTL

Diagnostic des sessions

Etat des protocoles

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

session info: proto=6 proto state=05 duration=2 expire=78 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper
class_Id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=538/6/1 reply=5407/6/0 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 2/0

origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64624->10.200.1.254:80(10.200.1.1:64624)
hook=pre dir=reply act=dnat 10.200.1.254:80->10.200.1.1:64624(10.0.1.10:64624)
pos/ (before,after) 0/(0,0), 0/(0,0)

misc=0 policy id=1 auth_info=0 chk_client_info=0 vd=0
.....
```

TCP State

Session TTL

Routing operation

NAT operation

Policy ID

Sessions

Table de session

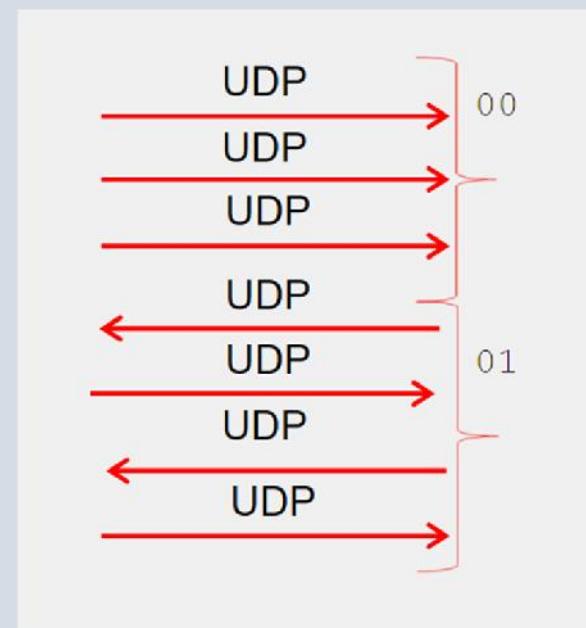
Session TTL

Diagnostic des sessions

Etat des protocoles (suite)

Etat UDP :

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



Quelques bonnes pratiques

Objectifs

- Identifier les incidents communs;
- Monitorer les sessions avec les commandes de diagnostic;
- Utiliser les filtres VIPs pour le NAT central;
- Utiliser les bonnes pratiques de mise en œuvre du NAT.

Quelques bonnes pratiques

Incidents

Monitoring des Sessions NAT

Filtres VIPs

Bonnes pratiques

NAT port exhaustion (épuisement de port) :

- Allocation de port impossible pour effectuer le NAT;
- Augmentation du compteur clash au visible au niveau des logs qui sont accessible via la commande: diagnose system session stat
- Informe l'administrateur via message log (si activé);

```
Message meets Alert condition date=2011-02-01 time=19:52:01 devname=master  
device_id="" log_id=0100020007 type=event subtype=system pri=critical vd=root  
service=kernel status=failure msg="NAT port is exhausted."
```

Résolution:

- Création d'un pool d'IP avec une ou plusieurs IP externe qui lui sont liés;
- Réduire le nombre de sessions nécessitant le NAT;

Quelques bonnes pratiques

Incidents

Monitoring des Sessions NAT

Filtres VIPs

Bonnes pratiques

Afficher tous les pools IP (type et interval):

- diagnose firewall ippool-all list;

```
Local-FortiGate # diagnose firewall ippool-all list  
vdom:root owns 1 ippool(s)  
name:INTERNAL-HOST-EXT-IP  
type:overload  
nat-ip-range:10.200.1.100-10.200.1.100  
.....  
.....
```

Command lists all configured IP Pools

Afficher les stats d'un pools IP déterminé:

- diagnose firewall ippool-all stats <ippool>;

```
# diagnose firewall ippool-all stats EXT  
name: EXT  
type: overload  
startip: 10.200.1.100  
endip: 10.200.1.100  
total ses: 100  
tcp ses: 75  
udp ses: 20  
other ses: 5
```

Command show only stats of IP pool named EXT

Quelques bonnes pratiques

Incidents

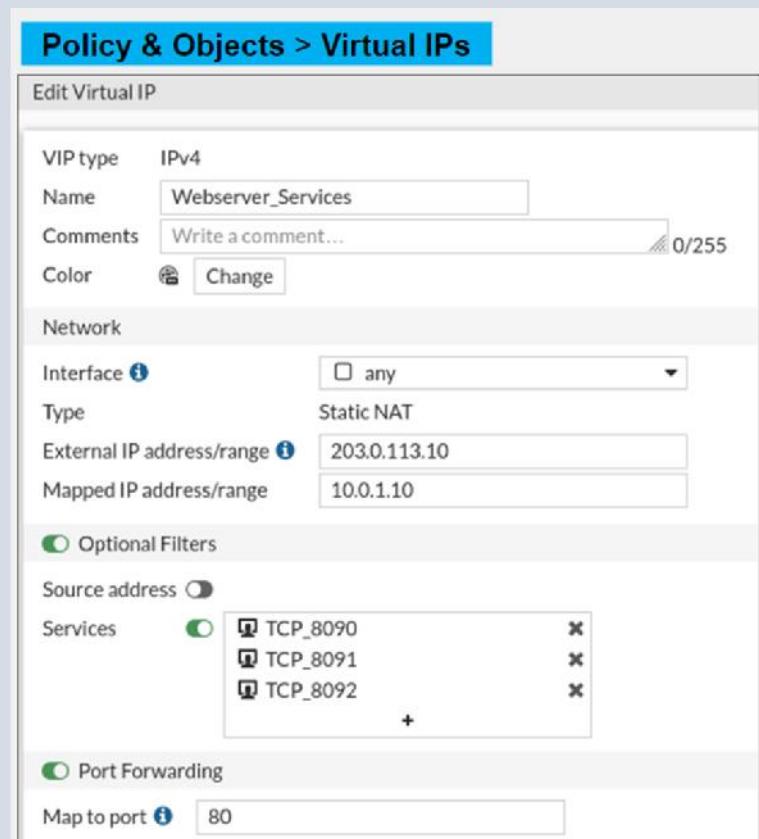
Monitoring des Sessions NAT

Filtre optionnel VIP:

- Permet de définir un ensemble de services sur un mappage de numéro de port unique
- Permet la mise en œuvre des scenarios où plusieurs sources de trafic externe utilise plusieurs services pour se connecter à un unique serveur interne;
- Evite la création de plusieurs VIP dans un groupe de VIP.

Filtres VIPs

Bonnes pratiques



Quelques bonnes pratiques

Incidents

Monitoring des Sessions NAT

Filtres VIPs

Bonnes pratiques

Quelques bonnes pratiques de configuration du NAT.

Eviter les mauvaises configurations des pools d'IP

Ne configurez pas NAT pour le trafic entrant à moins qu'il ne soit requis par une application

Planifier une fenêtre de maintenance pour passer d'un mode NAT à un autre

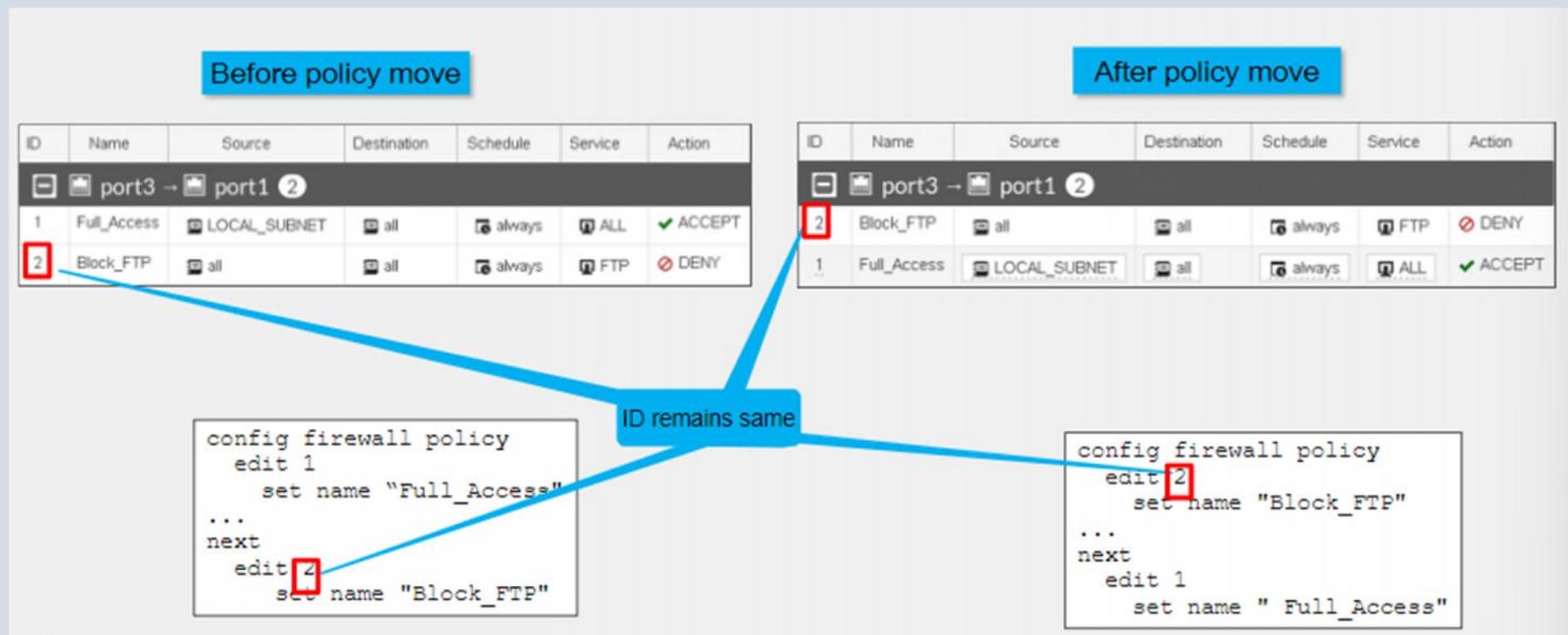
Quelques bonnes pratiques

Nommage

Bonnes pratiques

Réorganisation

Recherche



Quelques bonnes pratiques

Nommage

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. A red arrow points from the 'Policy Lookup' button in the top navigation bar to a search dialog window titled 'Policy Lookup'. The search dialog contains the following fields:

Incoming Interface	port3
IP Version	IPv4
Protocol	TCP
Source	10.0.1.10
Source Port	Optional (1-65535)
Destination	fortinet.com
Destination Port	443

A red box highlights the 'Search' button in the dialog, and another red arrow points from the dialog back to the main policy list below.

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	all	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	ALL_ICMP WebAccess	ACCEPT	Enabled

Bonnes pratiques

Réorganisation

Recherche

The screenshot shows the same 'Policy & Objects > Firewall Policy' interface. The third row has been modified: the 'Name' field now contains 'Training1' with a red 'X' icon, and the 'Action' field for the 'WebAccess' service has been changed to 'REJECT'. A red arrow points from the 'ACCEPT' button in the original screenshot to the 'REJECT' button in this one.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	all	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	ALL_ICMP WebAccess	REJECT	Enabled

FORTINET®



NSE Training Institute

FortiGate Security

AUTHENTICATION, GESTION DES LOGS & MONITORING ET GESTION DES CERTIFICATS



Plan du module



Authentification Firewall

Objectifs

- Identifier les méthodes d'authentification pare-feu;
- Comprendre l'authentification utilisant les politiques pare-feu;
- Comprendre l'authentification via le portail captif;
- Monitoring et diagnostic.

Authentification Firewall

Authentification

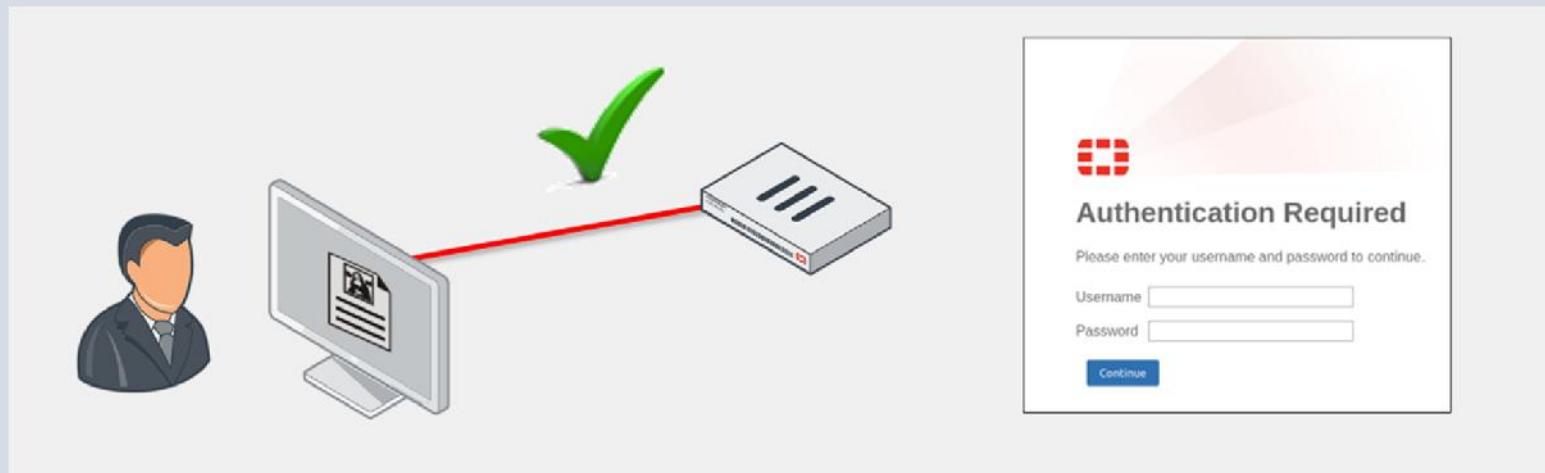
Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Authentification firewall?

- Autorisation de l'accès par vérification de l'IP source et de l'équipement (traditionnel);
- Impossible de déterminer l'utilisateur de l'équipement;
- Authentification des utilisateurs / groupes;
- Application des politiques et profils de sécurité pour autoriser/interdire l'accès à une ressource.



Authentification Firewall

Authentification (suite)

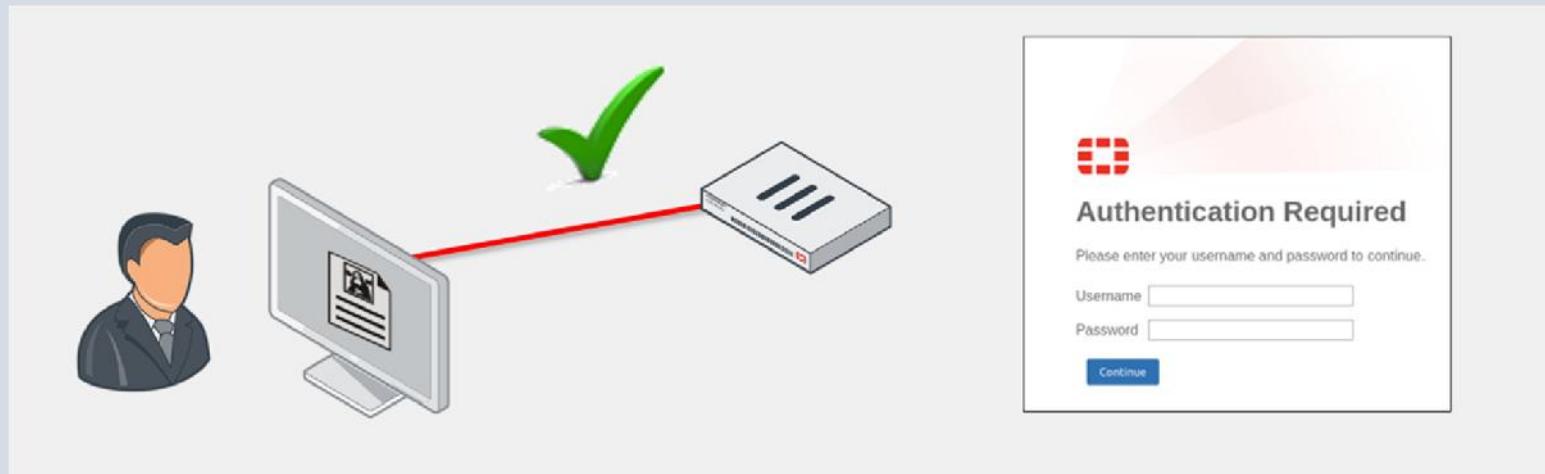
Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Méthode d'authentification:

- Authentification avec les paramètres locaux: Login et mot de passe enregistrés dans la base de données interne du FortiGate;
- Authentification à distance: les credentials sont sauvegardés dans un serveur d'authentification (RADIUS, TACACS+, LDAP, etc.);
- Authentification à 02 facteurs: activer avec l'une des méthodes précédente et nécessite une autre facteur.



Authentification Firewall

Authentification (suite)

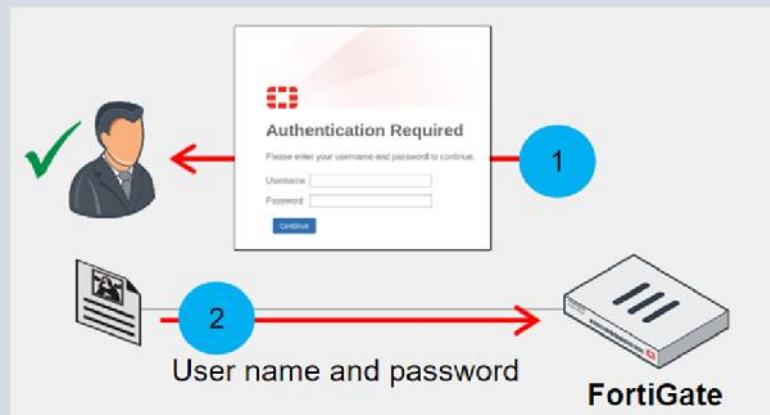
Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Méthode d'authentification: Utilisation des paramètres locaux

- Création d'un utilisateur local;
- Ajout de l'utilisateur à un groupe.



User & Authentication > User Definition

Users/Groups Creation Wizard

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

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

FortiNA

Users/Groups Creation Wizard

User Type: Local User

Username: Student

Password: *****

Users/Groups Creation Wizard

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

Two-factor Authentication

Users/Groups Creation Wizard

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

User Account Status: Enabled

User Group:

Authentification Firewall

Authentification (suite)

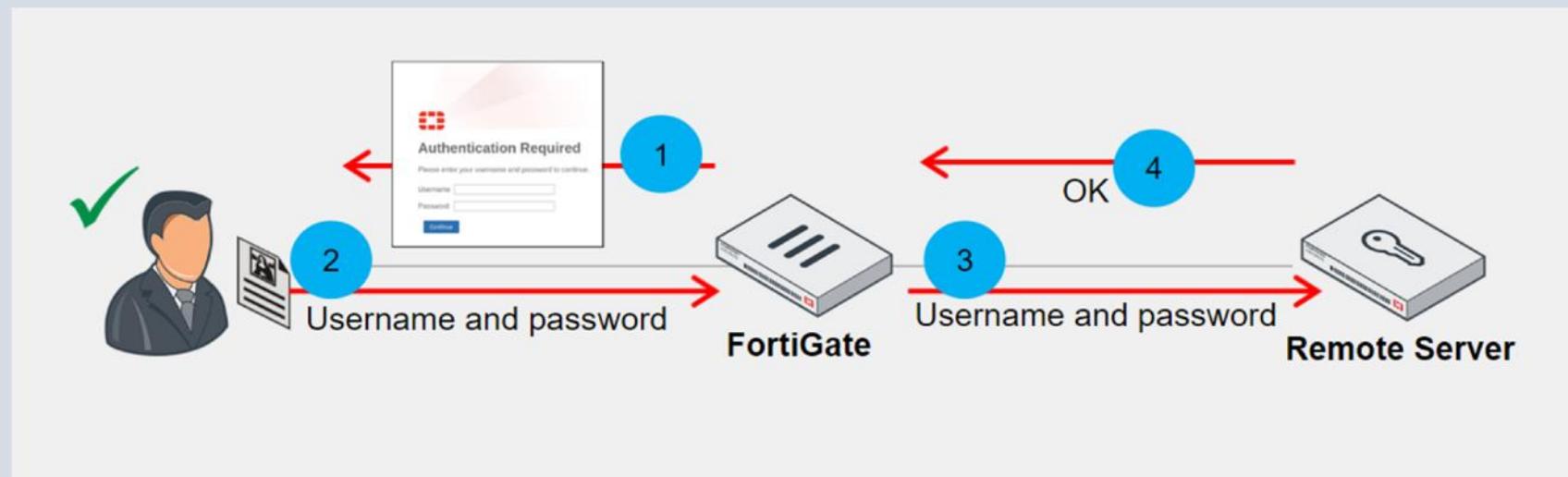
Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Méthode d'authentification: Authentification distante

- Compte sauvegarder dans le serveur d'authentification;
- Possibilité de créer les comptes locaux en cas d'indisponibilité du serveur d'authentification.



Authentification Firewall

Authentification (suite)

Authentification avec politiques

Méthode d'authentification: Authentification distante (suite)

Authentification via portal captif

Monitoring&Diagnostic

User & Authentication > User Definition

Users/Groups Creation Wizard

① User Type > ② RADIUS Server > ③ Contact Info > ④ Extra Info

Local User
Remote RADIUS User
Remote TACACS+ User
Remote LDAP User
FSSO
FortiNAC User

Must be preconfigured on FortiGate

Users/Groups Creation Wizard

① User Type > ② RADIUS Server > ③ Contact Info > ④ Extra Info

Username:
RADIUS Server:

Must be preconfigured on FortiGate

Edit User Group

Name: Remote-users
Type: Firewall
Members:
Remote Groups:

Remote Service	Group Name
FortiAuth-RADIUS	Remote-users

OK Cancel

Authentification Firewall

Authentification (suite)

Authentification avec politiques

Authentification via portal captif

Monitoring&Diagnostic

Méthode d'authentification: Authentification distante – Serveur d'authentification (suite)

□ LDAP

Directory tree attribute that identifies users

Part of the hierarchy where user records exist

Credentials for an LDAP administrator

User & Authentication > LDAP Servers	
Name	External_Server
Server IP/Name	10.0.1.150
Server Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training
Exchange server	<input checked="" type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	uid=adadmin,cn=Users,dc=trainingAD,c
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Connection status	Successful
Test Connectivity	
Test User Credentials	

Authentification Firewall

Authentification (suite)

Authentification avec politiques

Authentification via portal captif

Monitoring&Diagnostic

Méthode d'authentification: Authentification distante – Serveur d'authentification (suite)

RADIUS

User & Authentication > RADIUS Servers

New RADIUS Server

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

IP address or FQDN of the RADIUS server

The RADIUS server's secret (must match)

Authentification Firewall

Authentification (suite)

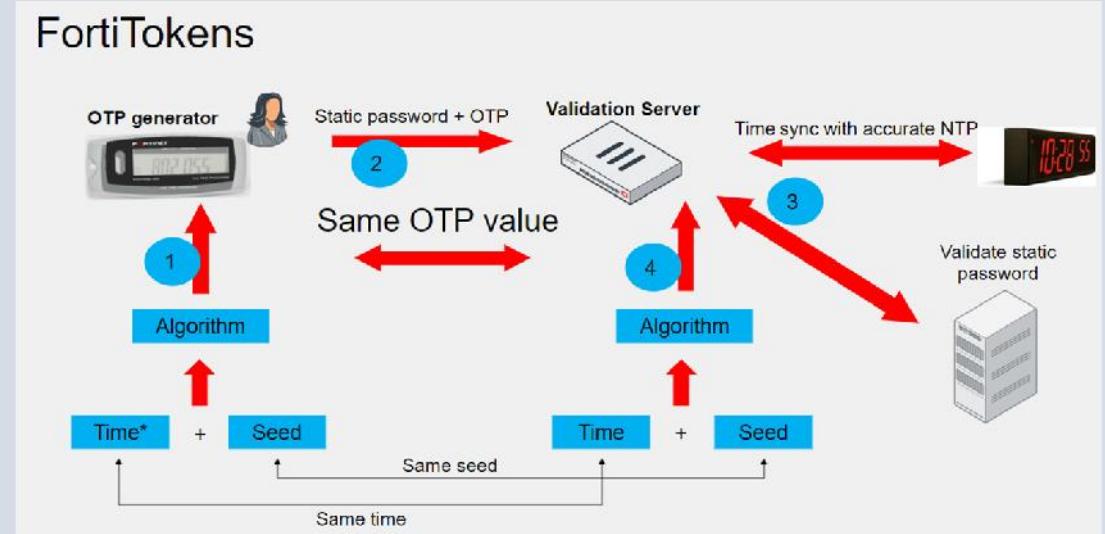
Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Méthode d'authentification: Authentification à 02 facteurs et OTP

- Améliore la sécurité;
- Nécessite 02 méthodes indépendante:
 - Quelque chose que vous savez: PIN, mot de passe, etc.
 - Quelque chose que vous avez: token, certificat, etc.
- OTP (One Time Password)
 - Offre plus de sécurité;
 - Token fourni par FortiToken 200 ou FortiMobile:
 - Génération d'un code de 6 caractères
 - Envoie par email ou par sms (configuration au niveau du compte);
- Serveur NTP recommandé.



Authentification Firewall

Authentification (suite)

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Méthode d'authentification: Authentification à 02 facteurs et OTP (suite)

- Enregistrement des tokens au niveau du FortiGate (Hard ou Soft);
- Assignation du token à un utilisateurs.

The screenshot shows the FortiOS User & Authentication interface. On the left, there's a table titled "User & Authentication > FortiTokens" with two entries: "Mobile Token" FTKMOB781E57E34F and "Mobile Token" FTKMOB783867923E, both marked as "Available". A red box highlights the "Create New" button. Two blue callout boxes point to the "Mobile Token" entries: one pointing to the first entry with the text "Two free FortiToken Mobile activations", and another pointing to the second entry with the text "Can add a user to a group and create a firewall policy based on the user group". On the right, there's a "New FortiToken" dialog and a "New FortiToken" dialog. The "New FortiToken" dialog has "Mobile Token" selected. The "New FortiToken" dialog has "Activation Code" 0000-0000-0000-0000 selected. On the far right, there's a "User" creation dialog for a user named "student". It includes fields for Username (student), User Account Status (Enabled), User Type (Local User), Password (*****), User Group (Remote-users), and "Two-factor Authentication" (selected). The "Authentication Type" dropdown is set to "FortiToken" and the "Token" dropdown is set to "FTKMOB6B91B33BE5". A red box highlights the "Authentication Type" and "Token" fields.

Authentification Firewall

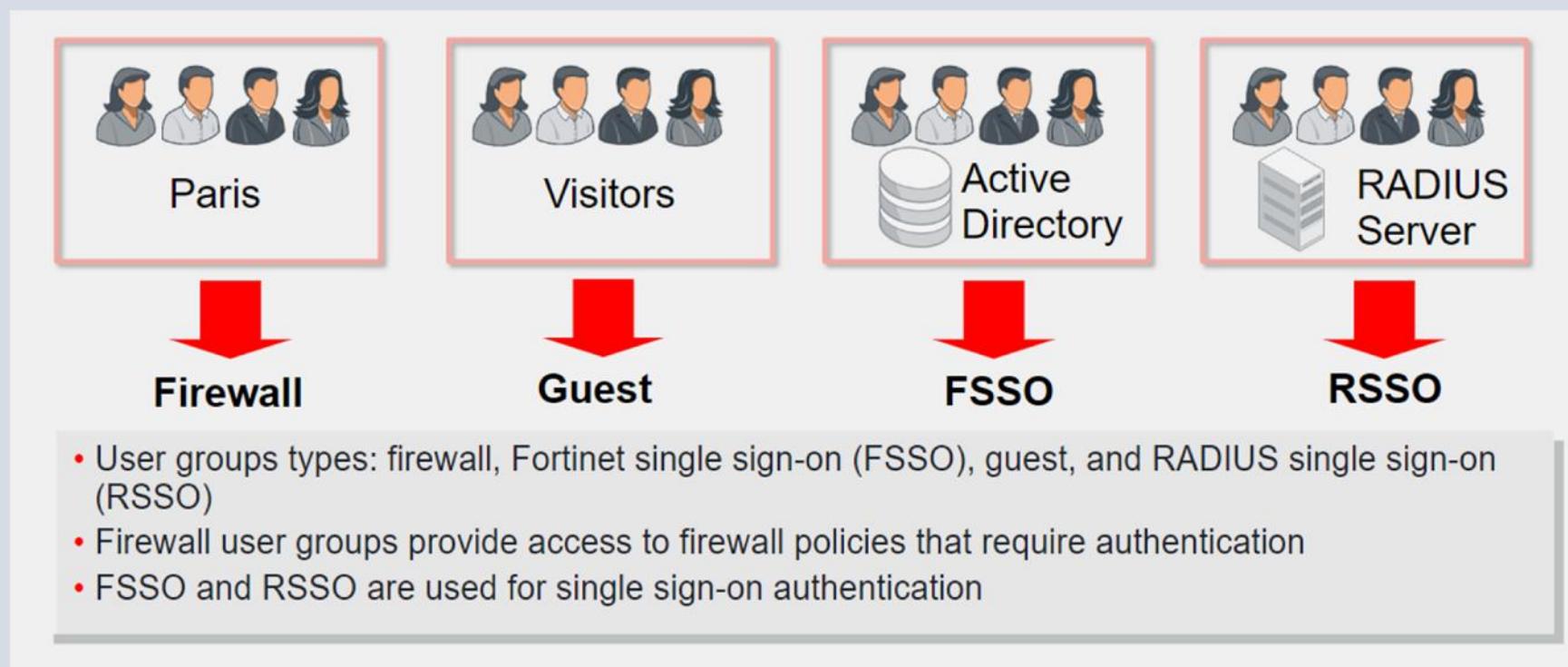
Authentification (suite)

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Groupes:



Authentification Firewall

Authentification (suite)

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Groupes: Configuration

The screenshot shows the 'User & Authentication > User Groups' page. A new group named 'Training-users' is being created. The 'Type' dropdown is set to 'Firewall'. The 'Members' section contains a red box around the '+ Add' button, with a callout 'Can add preconfigured remote servers to the group' pointing to it. The 'Remote Groups' section has a red box around the '+ Add' button, with a callout 'Can select specific LDAP groups as defined on the LDAP server' pointing to it. A modal window titled 'Select Entries' lists 'USER (2)' and 'Local (2)' entries, with 'guest' selected.

User & Authentication > User Groups

Name: Training-users

Type: Firewall

Members: + Add

Remote Groups: + Add

Select Entries:

- USER (2)
- Local (2)
- guest
- student

Authentification Firewall

Authentification

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Politiques Pare-feu

- Utilisation des objets utilisateurs ou groupe comme paramètre au niveau de l'identification de la source de trafic;
- Autorisation d'accès aux membres du groupes ayant fourni les bons paramètres d'authentification.

Policies & Objects > Firewall Policy

Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET External-Server-Users
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY

Select Entries

Address User Internet Service

Search + Create

USER (2)

Local (2)

guest student

USER GROUP (3)

External-Server-Users

Guest-group SSO_Guest_Users



Authentification Firewall

Authentification

Authentification avec politiques (suite)

Politiques Pare-feu

- ❑ Utilisation des objets utilisateurs ou groupe comme paramètre au niveau de l'identification de la source de trafic;
- ❑ Autorisation d'accès aux membres du groupes ayant fourni les bons paramètres d'authentification;
- ❑ Protocole autorisé avant l'authentification: HTTP, HTTPS, FTP et TELNET

Policies & Objects > Firewall Policy

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1						
Full_Access	External-Server-Users LOCAL_SUBNET	all	always	DNS HTTP	✓ ACCEPT	✓ Enabled

Authentification via portail captif

Monitoring&Diagnostic

Policies & Objects > Firewall Policy

Full_Access

port3 → port1 1

Source: LOCAL_SUBNET, External-Server-Users

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT

Select Entries: User (2) Local (2) guest student USER GROUP (3) External-Server-Users Guest-group SSO_Guest_Users



Authentification Firewall

Authentification

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Portail Captif

- Authentification web des utilisateurs avec login et mot de passe;
- Activation sur l'interface d'entrée du trafic;
- Méthode d'authentification active uniquement;
- Hébergement du portail captif sur le FortiGate ou sur un serveur Externe.

The screenshot shows the 'Network > Interfaces' configuration screen. Under the 'Security mode' section, the dropdown menu is set to 'Captive Portal'. A red box highlights this selection. Below it, under 'User access', the 'Restricted to Groups' tab is selected, and a group named 'CP-group' is listed. Other tabs like 'Local' and 'External' are also visible. The 'User groups' section lists 'CP-group'. The 'Exempt sources' and 'Exempt destinations/services' sections are empty. At the bottom, there are options for 'Original Request' and 'Specific URL'.

Authentification Firewall

Authentification

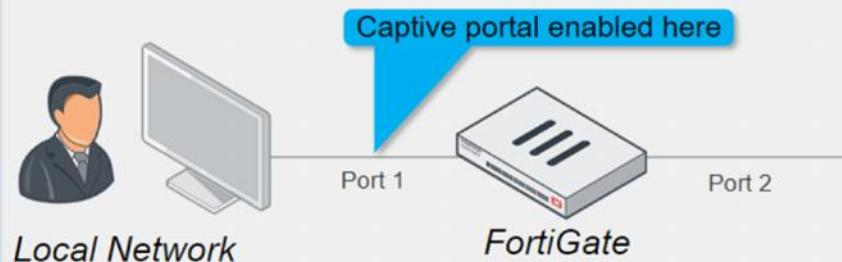
Authentification avec politiques

Authentification via portal captif (suite)

Monitoring&Diagnostic

Portail Captif: Configuration

- Configured on network interfaces



The screenshot shows the 'Network > Interfaces' configuration page. Under the 'Network' section, the 'Security mode' dropdown is set to 'Captive Portal', which is highlighted with a red box. Other settings include 'Device detection' (on), 'Authentication portal' (Local selected), 'User access' (Restricted to Groups selected), and 'User groups' (CP-group selected). The 'Exempt sources' and 'Exempt destinations/services' sections are empty. The 'Redirect after Captive Portal' section has 'Original Request' selected.

WiFi & Switch Controller > SSIDs

Name	SSID	Traffic Mode	Security
SSID 1	WIFI-fortinet (WIFI)	Tunnel	Captive Portal

WiFi Settings

SSID: fortinet
Client limit: off
Broadcast SSID: on

Security Mode Settings

Security mode: Captive Portal (highlighted with a red box)
Portal type: Disclaimer + Authentication
Authentication portal: Local selected
User groups: Guest-group selected
Exempt sources: empty
Exempt destinations/services: empty
Redirect after Captive Portal: Original Request selected

Authentification Firewall

Authentification

Authentification avec politiques

Authentification via portail captif (suite)

Monitoring&Diagnostic

Portail Captif: Configuration des messages d'affichage

Extended View

The screenshot shows the 'System > Replacement Messages' page. The 'Extended View' tab is selected. In the table, the 'Disclaimer Page' row is highlighted with a yellow background. A red arrow points from this row to a preview window on the right. Another red arrow points from the 'Extended View' tab to the same preview window. The preview window displays the 'Terms and Disclaimer Agree' page with its HTML code.

Name	Description
Alert E-mail	Replacement HTML for authentication success page
Authentication	Replacement HTML for block notification page
Authentication Success Page	Replacement HTML for certificate password page
Block Notification Page	Replacement HTML for declined disclaimer page
Certificate Password Page	Replacement HTML for user declined quarantine page
Declined Disclaimer Page	Replacement HTML for user declined disclaimer page
Declined Quarantine Page	Replacement HTML for email collection page
Disclaimer Page	Replacement HTML for authentication disclaimer page
Email Collection	Replacement HTML for authentication success page

Terms and Disclaimer Agree

You are about to access Internet content that is not under the network access provider. The network access provider is responsible for any of these sites, their content or their privacy. The network access provider and its staff do not endorse nor representations about these sites, or any information, software products or materials found there, or any results that may be from using them. If you decide to access any Internet content entirely at your own risk and you are responsible for ensuring

Do you agree to the above terms?

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">
<style type="text/css">
body {
    font-family: Roboto, Helvetica, Arial, sans-serif;
    color: #333333;
    margin: 0;
    display: flex;
    align-items: center;
    justify-content: center;
}
input[type="button"], input[type="email"], input[type="checkbox"] {
    vertical-align: baseline;
    margin: 0 2px;
    border-style: solid;
    border-width: 1px;
    border-color: #4CAF50;
    background-color: #4CAF50;
    box-sizing: border-box;
    padding: 2px 5em;
    color: white;
    border-radius: 0;
}
input:focus {
    border-color: #4CAF50;
    box-shadow: 0 0 1px #a2a2a2;
}
```

Authentification Firewall

Authentification

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic

Monitoring: Utilisateurs

The screenshot shows the 'Dashboard > User & Devices > Firewall Users' page. It displays two circular dashboards: one for 'Method' (Firewall) showing 1 user, and another for 'User Group' (CP-group) showing 1 user. Below these are search and filter fields, followed by a table of active sessions. A row for a user named 'student' is highlighted in yellow, showing details: IP Address 10.0.1.10, User Group CP-group, Duration 1 minute(s) and 9 second(s), Traffic Volume 10.43 kB, and Method Firewall. A red box highlights the 'Deauthenticate' button in the table header. A red arrow points from this button to a 'Confirm' dialog box at the bottom left, which asks 'Are you sure you want to deauthenticate the selected user(s)?' with 'OK' and 'Cancel' buttons.

- Also used to terminate authenticated sessions

Authentification Firewall

Authentification

Authentification avec politiques

Authentification via portail captif

Monitoring&Diagnostic (suite)

Troubleshooting: GUI

The screenshot shows a table titled "Policy & Objects > Firewall Policy". The table has columns: ID, Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. There is one row visible:

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Full_Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled	upg_deep-inspection	UTM	3.47 MB

A red box highlights the "Bytes" column for the first row.

Troubleshooting: CLI

- Diagnose firewall auth list: affiche les utilisateurs authentifiés, les IPs et leurs groupes;
- Diagnose firewall auth clear: Efface la liste actuelle d'utilisateurs connectés;
- Diagnose debug application fnbamd -1: utilisé pour diagnostiquer les authentifications actives;
- Diagnose test authserver radius-direct <ip> <port> >secret>: Test la clé prépartagé entre FortiGate et le serveur RADIUS;
- Diagnose test authserver ldap <server_name> <username> <password>: Test l'authentification LDAP pour un compte spécifique.

Journalisation et Supervision

Objectifs

- Comprendre les journaux;
- Configurer les journaux locaux et distants;
- Identifier les paramètres de journaux;
- Protéger les données de journaux.

Journalisation et Supervision

Journalisation

Journalisation local et distante

Log (journaux):

- Stocke l'historique des évènements survenus sur un équipement;
- Stockage local ou distant (FortiAnalyzer)

Rôle:

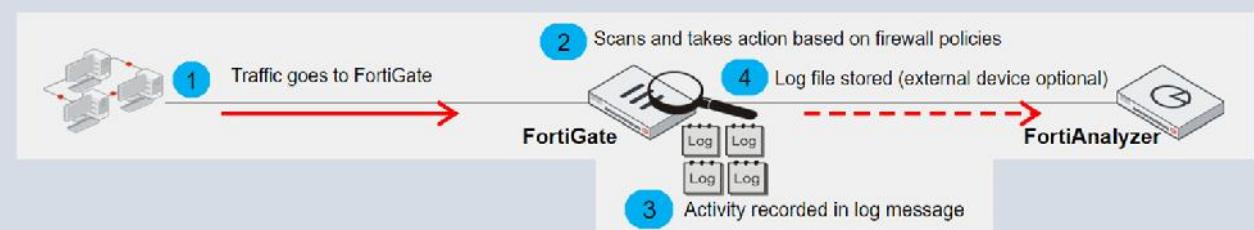
- Supervision des activités réseaux et le volume du trafic internet;
- Diagnostiquer les problèmes;
- Etablir les bases pour reconnaître les anomalies.
- Etc.

Flux de travail

- Trafic passe via le FortiGate;
- FortiGate scan le trafic et applique les actions basées sur les règles de trafic;
- Activités sont enregistrés dans les fichiers logs;
- Log (journaux) sont stockés sur équipements capable de stocker les logs (local/distant).

Paramètre de journalisation

Protection des journaux



Journalisation et Supervision

Journalisation (suite)

Journalisation local et distante

Paramètre de journalisation

Protection des journaux

Types de journaux:

- Log de trafic: enregistre les informations sur le flux de trafic tel que les requêtes et réponses HTTP/HTTPS.
- Log de transfert de trafic: contient les informations sur les trafic acceptés ou refusés;
- Log de trafic local: contient les informations sur le trafic en provenant ou en direction du management;
- Log sniffer: contient les informations relatives au trafic traité par les interfaces one-arm-sniffer.
- Log des évènements: enregistre les évènements systèmes.
 - Log des évènements système: contient les informations relatives aux opérations telles que update ou les accès GUI;
 - Log des utilisateurs: contient les informations sur les évènements de connection et de déconnexion avec les authentification utilisant les règles de trafic;
 - Log de routeur, VPN: contient les informations relatives à ces fonctionnalités
- Log de sécurité: enregistre les informations relatives aux évènements de sécurité.
 - Tentative d'attaques ou intrusion virale;
 - Profils de sécurité
 - Etc.

Journalisation et Supervision

Journalisation (suite)

Journalisation local et distante

Paramètre de journalisation

Protection des journaux

Niveau de sévérité:

- 0 = importance élevée;
- 6 = importance faible.

Rarely used, unless actively investigating an issue with Fortinet Support

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

Journalisation et Supervision

Journalisation (suite)

Journalisation local et distante

Paramètre de journalisation

Protection des journaux

Message de journalisation:

- En-tête: constitué du type/sous-type (nom du fichier) et du niveau de严重性.

```
date=2021-03-14 time=12:05:28 logid=0316013056 type=utm subtype=webfilter  
eventtype=ftgd_blk level=warning vd=root
```

- Body: varie en fonction du type de log.

```
policyid=1 sessionid=10879 user="" srcip=10.0.1.10 srcport=60952 srcintf="port3"  
dstip=52.84.14.233 dstport=80 dstintf="port1" proto=6 service="HTTP"  
hostname="miniclip.com" profile="default" action=blocked reqtype=direct url="/favicon.ico"  
sentbyte=29 / rcvbyte=0 direction=outgoing  
msg="URL belongs to a denied category in policy" method=domain cat=20 catdesc="Games"  
crscore=30 crlevel=high
```

Journalisation et Supervision

Journalisation

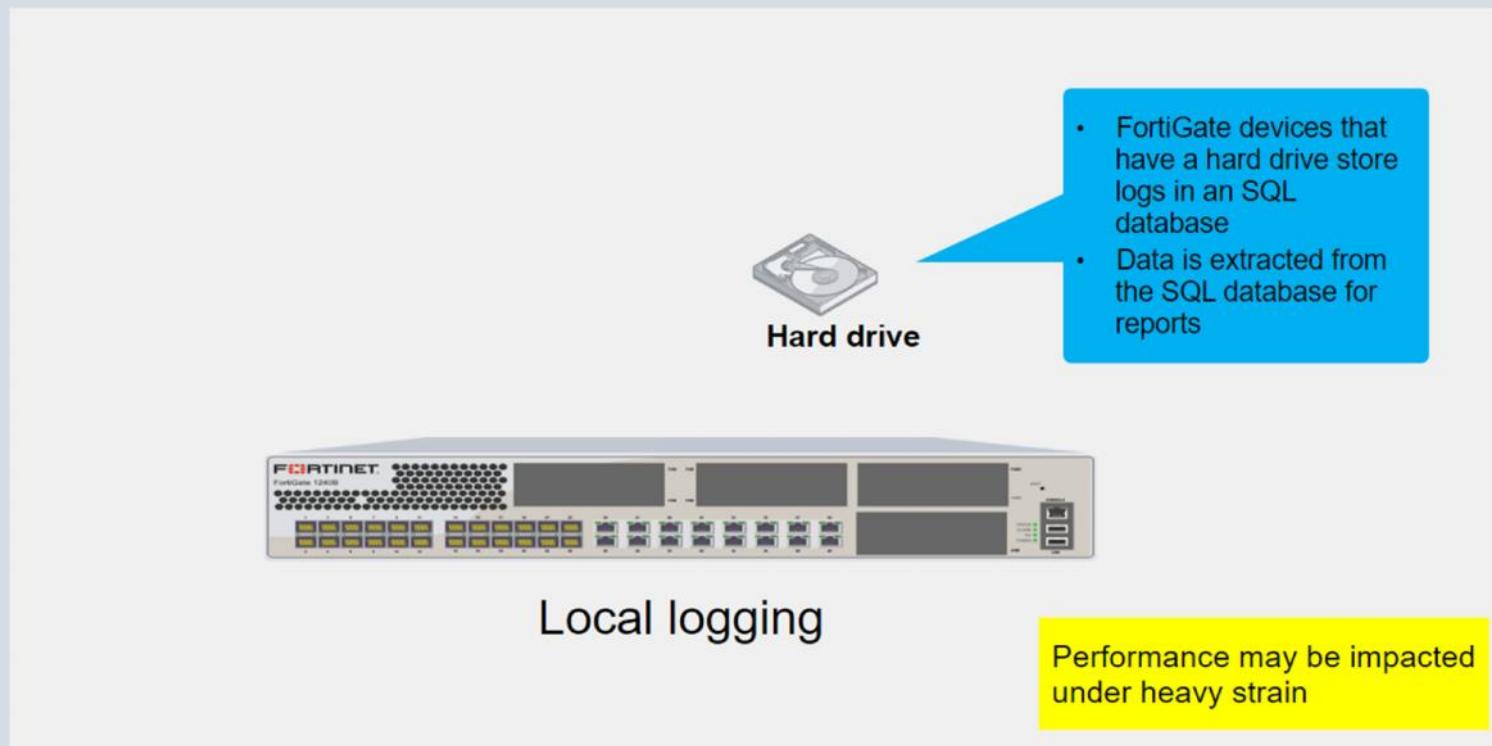
Journalisation local et distante

Journalisation locale:

- Sauvegarde local des fichier de journalisation;
- Baisse de performance en cas d'utilisation intensive.

Paramètre de journalisation

Protection des journaux



Journalisation et Supervision

Journalisation

Journalisation local et distante (suite)

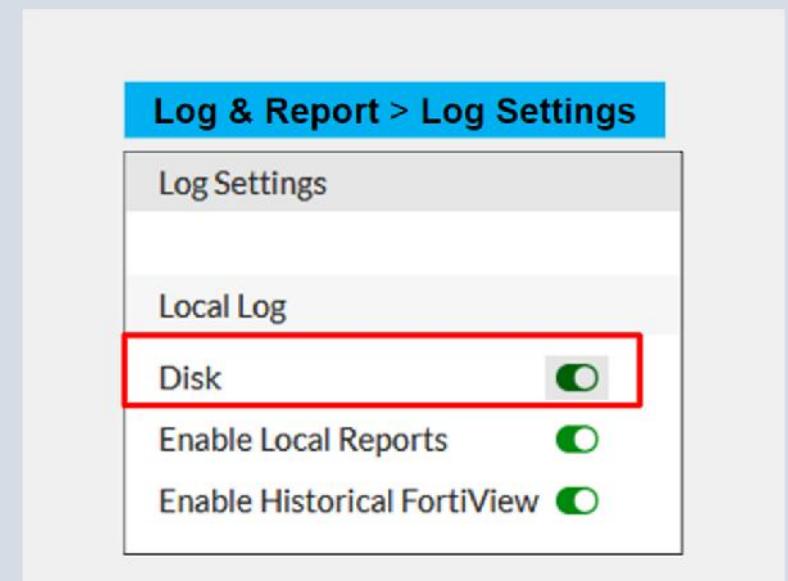
Paramètre de journalisation

Protection des journaux

Journalisation locale: Activation

- Activation de la sauvegarde sur le disque;
- Suppression des anciens logs après 07 jours par défaut.

```
# config log disk setting  
    set maximum-log-age <integer>
```



Journalisation et Supervision

Journalisation

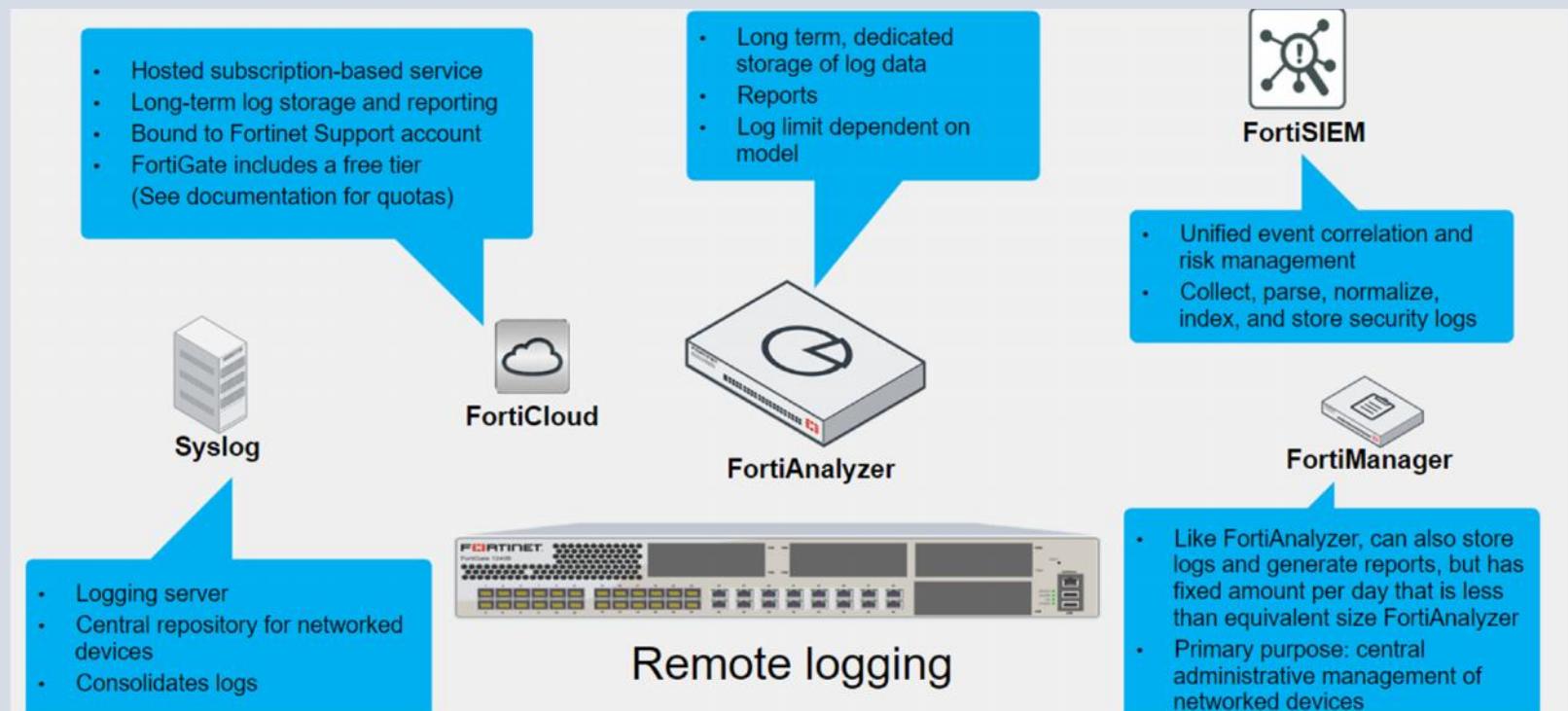
Journalisation local et distante (suite)

Paramètre de journalisation

Protection des journaux

Journalisation Distante

- Sauvegarde des logs sur un serveur distant.



Journalisation et Supervision

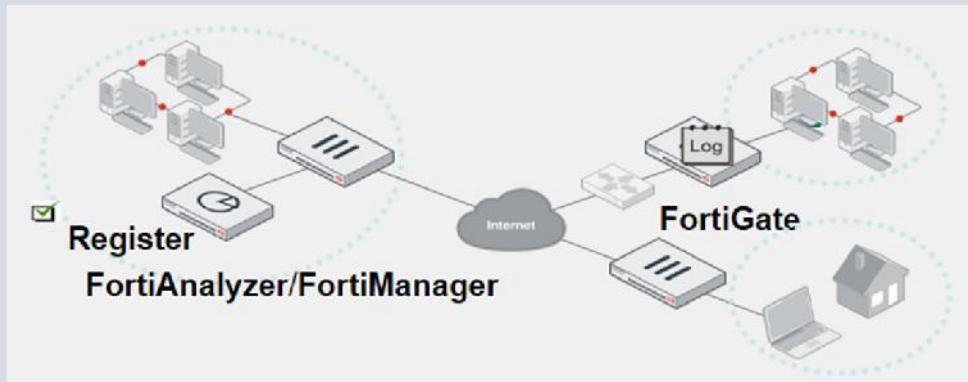
Journalisation

Journalisation local et distante (suite)

Journalisation Distante: FortiAnalyze & FortiSIEM

Paramètre de journalisation

Protection des journaux



Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager Enabled Disabled

IP address: 10.0.1.210

Connection status: Connected

Storage usage: 56.07 MiB / 1000.00 MiB

Analytics usage: 20.82 MiB / 700.00 MiB

Archive usage: 35.25 MiB / 300.00 MiB

Upload option: Real Time | Every Minute | **Every 5 Minutes**

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate FAZ-VM0000065040

This screenshot shows the 'Log & Report > Log Settings' interface. It displays various log-related metrics and configuration options. The 'Send logs to FortiAnalyzer/FortiManager' section is highlighted with a red border. Other sections include IP address, connection status, storage usage, analytics usage, archive usage, upload options (set to 'Every 5 Minutes'), and security settings for the REST API and certificate verification.

Journalisation et Supervision

Journalisation

Journalisation local et distante

Journalisation: Paramètres

The screenshot shows the FortiGate Log & Report interface with the following sections:

- Local Log:** Enabled (green switch). Options: Disk (Enabled), Enable Local Reports (Enabled), Enable Historical FortiView (Enabled).
- Event Logging:** All (selected). Options: Local Traffic Log (All selected), Log Allowed Traffic (unchecked), Log Local Out Traffic (unchecked), Log Denied Unicast Traffic (unchecked), Log Denied Broadcast Traffic (unchecked).
- GUI Preferences:** Resolve Hostnames (Enabled), Resolve Unknown Applications (Enabled).
- Remote Logging and Archiving:** Enabled (green switch). IP address: 10.0.1.210. Connection status: Connected. Storage usage: 45.20 MiB / 1000.00 MiB. Analytics usage: 9.95 MiB / 700.00 MiB. Archive usage: 35.25 MiB / 300.00 MiB. Upload option: Real Time, Every Minute, Every 5 Minutes. Allow access to FortiGate REST API (Enabled). Verify FortiAnalyzer certificate (FAZ-VM0000065040) (Enabled).

Annotations with red arrows point from the Local Log section to the Remote Logging and Archiving section, and from the GUI Preferences section to the Remote Logging and Archiving section. A central text box asks "Store logs locally or remotely?" with arrows pointing towards both sections.

- Log event logs and traffic logs?
- Local traffic logs = traffic directly to and from FortiGate (disabled by default)
- Event logs = system information generated by FortiGate

- Translate IPs to host names for convenience? (Can impact CPU usage and page responsiveness.)

Journalisation et Supervision

Journalisation

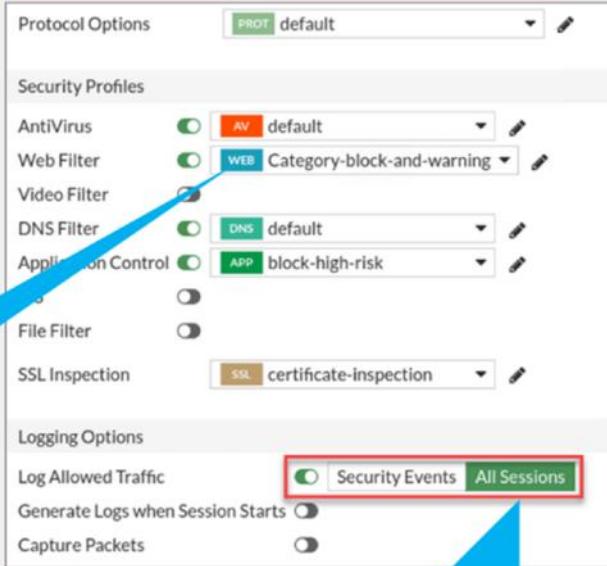
Journalisation local et distante

Paramètre de journalisation(suite)

Protection des journaux

Journalisation: Activation de la journalisation sur les règles de trafic

Policy & Objects > Firewall Policy



Must enable one or more security profiles on your firewall policy to generate a log message for that profile

Must enable and set which traffic to log. If disabled, you will not receive logs of any kind—even if you have enabled a security profile on your firewall policy.

Journalisation et Supervision

Journalisation

Journalisation local et distante

Paramètre de journalisation(suite)

Protection des journaux

Journalisation: Consultation - GUI

The screenshot shows the Fortinet Log & Report interface. On the left, a sidebar lists various log categories like Forward Traffic, Local Traffic, Sniffer Traffic, etc. The main area displays a table of logs with columns for Date/Time, Source, Destination, Application Name, Result, Policy, and Application Category. A specific row for a 'Dropbox_File.Upload' event is selected. A blue callout box points to this row with the text: "GUI menu items depend on incoming logs. Select the log type you want to search." To the right of the table, a large blue callout box contains the text "Set log filters to narrow search" and "Log location = disk". A red box highlights the "Disk" button in the top right corner of the log table header. A detailed log view is shown on the right, with tabs for Details and Security. The Details tab shows fields like IP, Port, Country/Region, and Application Control settings. The Security tab shows risk levels and control actions. Another blue callout box on the right says "Double-click log to view log details".

Journalisation et Supervision

Journalisation

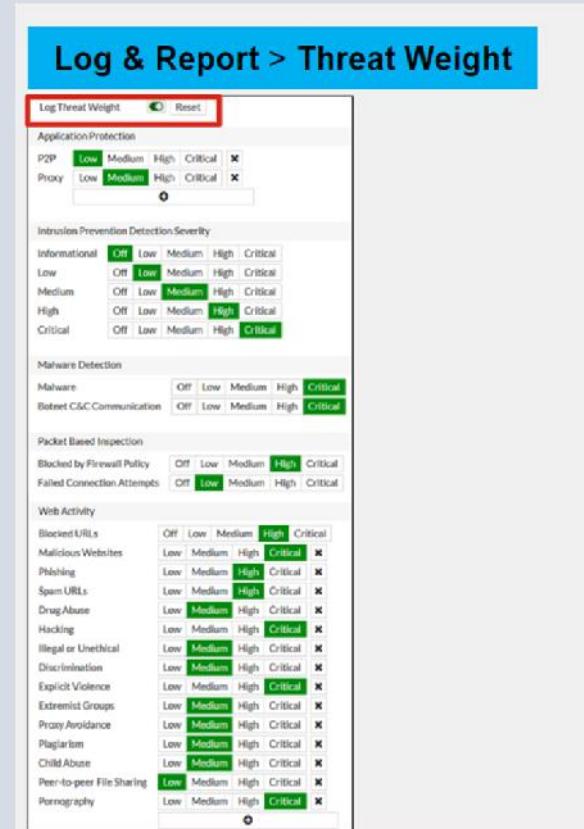
Journalisation local et distante

Paramètre de journalisation(suite)

Protection des journaux

Journalisation: poids des menaces

- ❑ Permet de prioriser les incidents en préconfigurant leur niveau de sévérité et de risque



Journalisation et Supervision

Journalisation

Journalisation local et distante

Paramètre de journalisation

Protection des journaux

Protection: Téléchargement

The screenshot shows a network monitoring interface with two main windows. The left window displays a table of traffic logs with columns for Date/Time, Source, Device, Destination, Application Name, Result, Policy, and Applic. A red arrow points from the 'Add Filter' button at the top left of this window towards the right window. The right window is a 'Opening disk-traffic-forward-2020-03-02_0931.log' dialog box from Firefox. It shows the log file path, its size (48.8 KB), and the source (HTTP://10.0.1.254). It also contains options for what Firefox should do with the file: 'Open with Pluma (default)', 'Save File', and 'Do this automatically for files like this from now on.' Buttons for 'Cancel' and 'OK' are at the bottom.

Date/Time	Source	Device	Destination	Application Name	Result	Policy	Applic
55 seconds ago	1.1.1.1		2.2.2.2		Deny: UTM Blocked	Full_Access(1)	unsc
55 seconds ago	1.1.1.1		2.2.2.2		Deny: UTM Blocked	Full_Access(1)	unsc
Minute ago	1.1.1.1		2.2.2.2		✓ 2.00 kB / 1.00 kB	Full_Access(1)	unsc
Minute ago	1.1.1.1		2.2.2.2		Deny: UTM Blocked	Full_Access(1)	unsc
Minute ago	test user (172.16.78.32)		1.1.1.32		Deny: policy violation	100	unsc
Minute ago	test user (172.16.78.32)		1.1.1.32		Deny: policy violation	100	unsc
2 minutes ago	test user (172.16.78.32)		1.1.1.32		Deny: policy violation	100	unsc
2 minutes ago	test user (172.16.78.88)		229.118.95.200		Deny: policy violation	0	unsc
3 minutes ago	1.1.1.1		2.2.2.2		Deny: UTM Blocked	Full_Access(1)	unsc
3 minutes ago	10.1.1.1		2.2.2.2		✓ 2.00 kB / 1.00 kB	Full_Access(1)	Vi

Certificats

Objectifs

- Authentifier et sécuriser les données avec les certificats;
- Inspecter le trafic chiffré;
- Gérer les certificats digitaux.

Certificats

Authentification et sécurisation

Inspection de trafic

Gestion des certificats

Certificats: utilisation

- Inspection
 - Inspection SSL;
 - S'assure de la validité d'un certificat avant l'autorisation de l'accès;
- Intimité (privacy)
 - Etablissement des connexions SSL avec les autres équipements;
- Authentification
 - Second facteurs lors de l'authentification multifacteur;
 - Authentification des équipements lors des sessions VPN.

Certificats

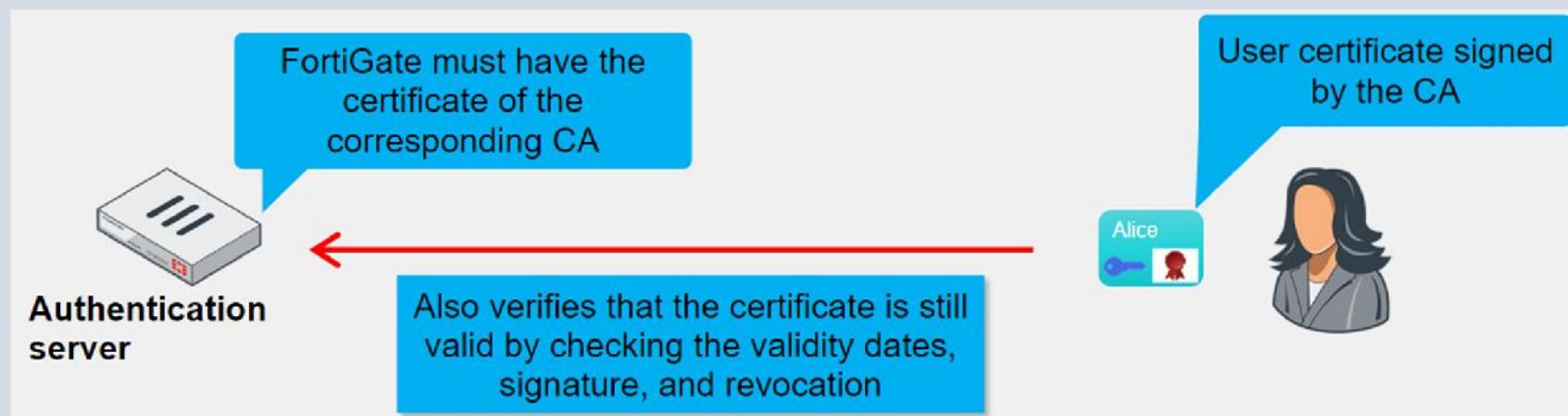
Authentification et sécurisation (suite)

Authentification: utilisateur

- Certificat utilisateurs
 - Signature digitale;
 - Clé publique de l'utilisateur.
- CA (autorité de certification)
- Configuré sur le serveur d'authentification.

Inspection de trafic

Gestion des certificats



Certificats

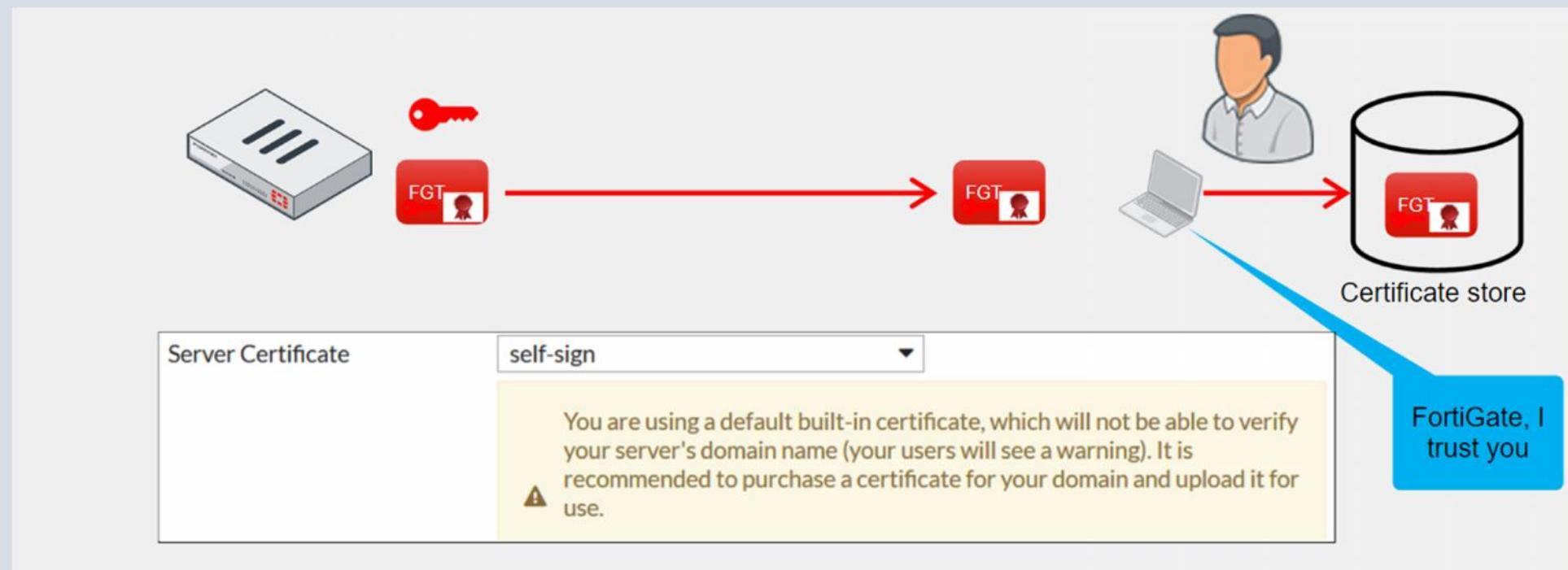
Authentification et sécurisation (suite)

Authentification: utilisateur

- Certificat auto signé (par défaut);
- Etablissement des sessions SSL.

Inspection de trafic

Gestion des certificats



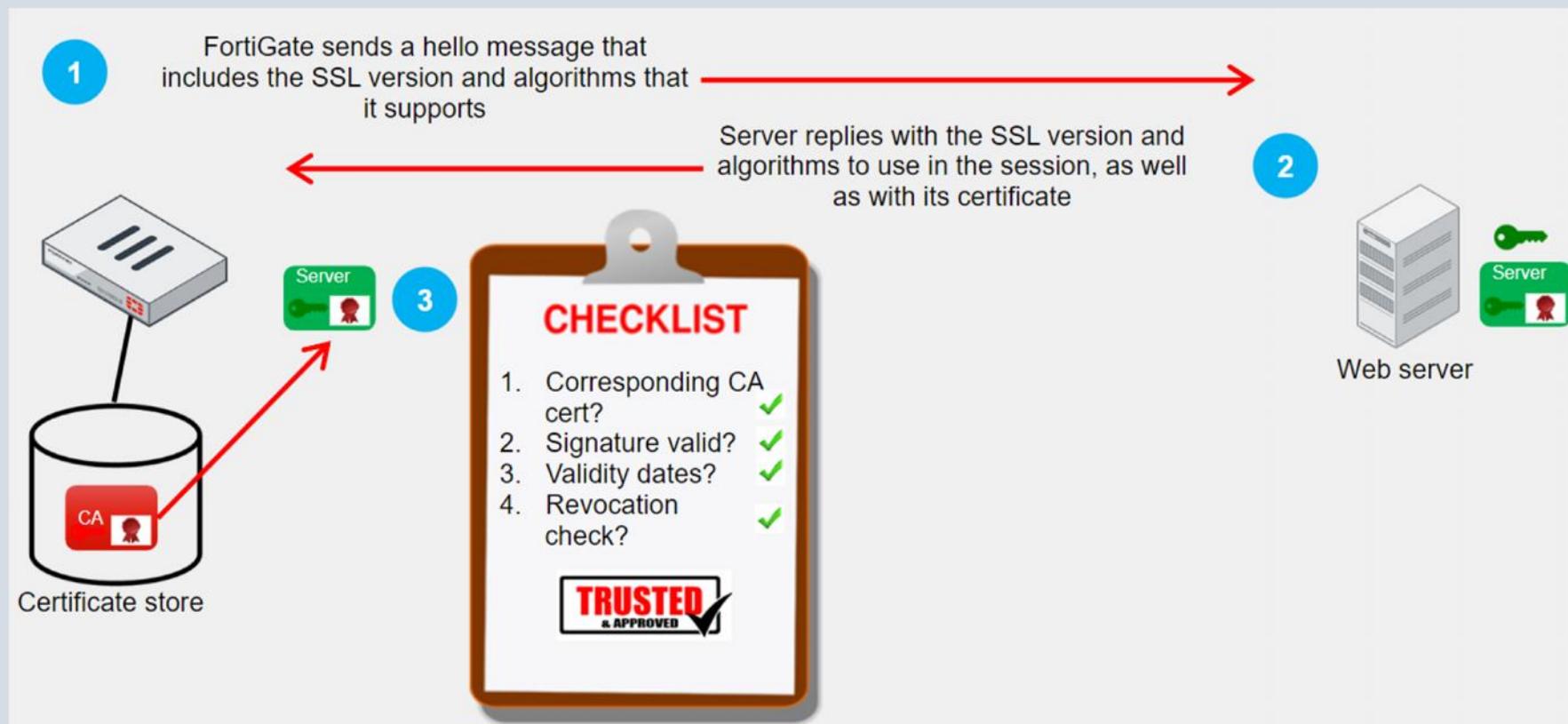
Certificats

Authentification et sécurisation (suite)

Connection SSL.

Inspection de trafic

Gestion des certificats



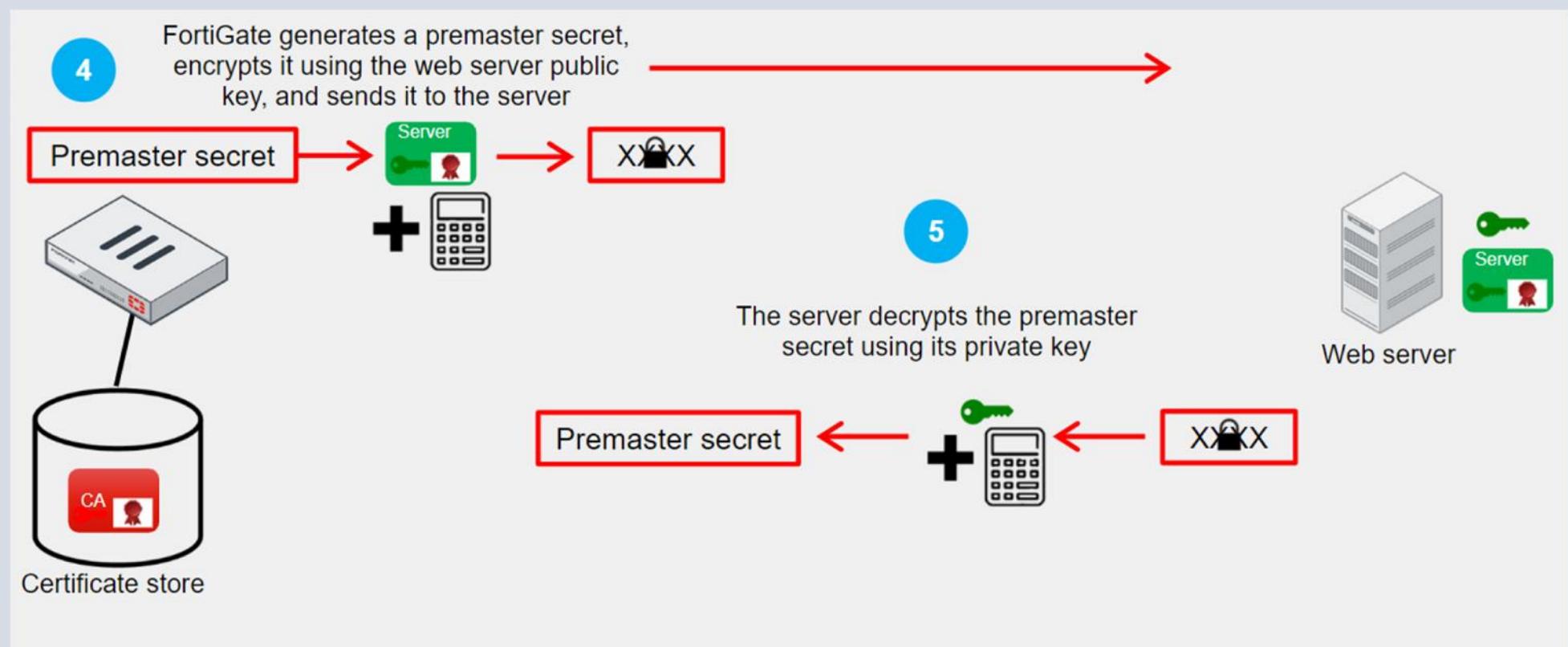
Certificats

Authentification et sécurisation (suite)

Inspection de trafic

Gestion des certificats

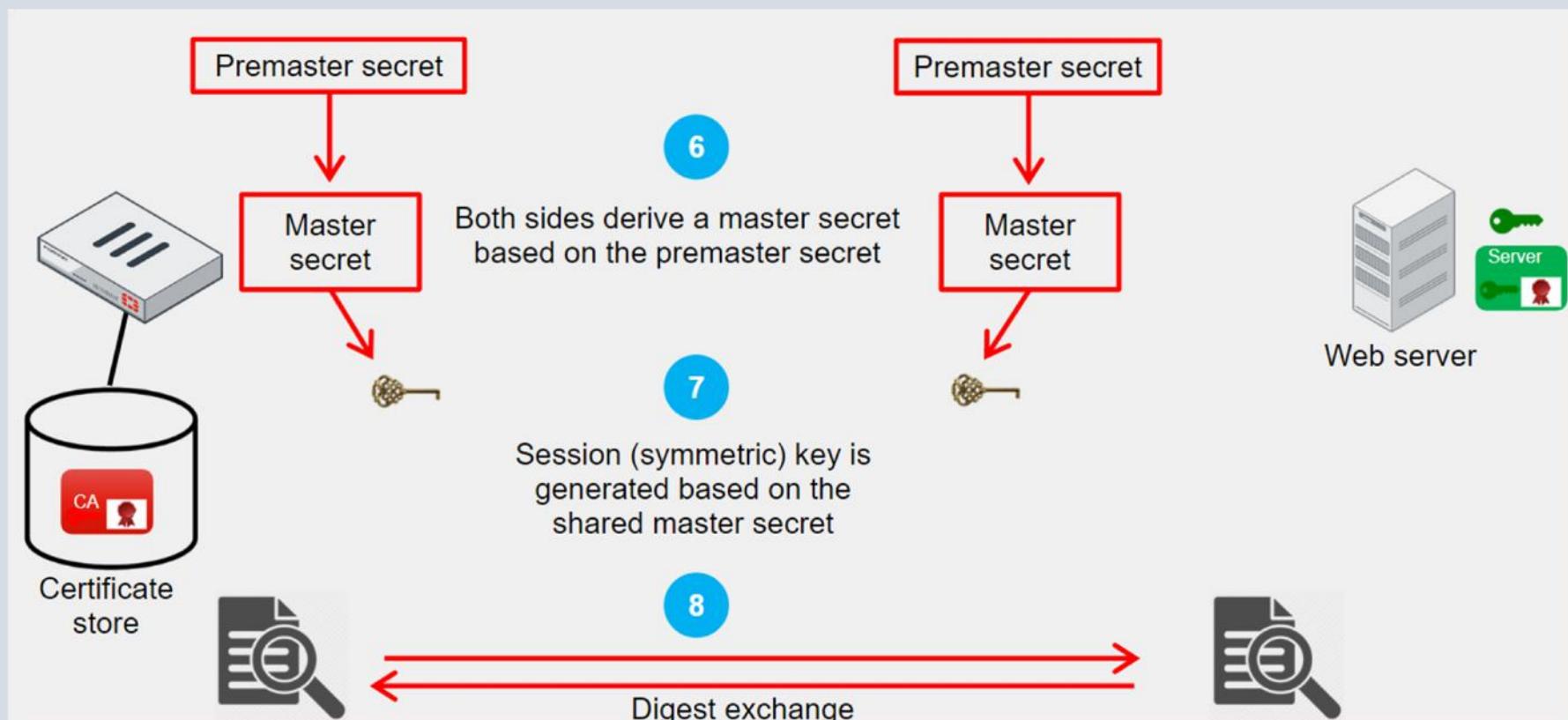
Connection SSL - 2.



Certificats

Authentification et sécurisation (suite)

Connection SSL - 3.



Certificats

Authentification et sécurisation

Inspection de certificat SSL

- Uniquement utilisé sur le filtrage URL;
- Ne permet pas l'inspection des données chiffrées.

Inspection de trafic

Gestion des certificats

The screenshot shows two windows related to SSL/SSH inspection profiles:

- Left Window: Security Profiles > SSL/SSH Inspection**
 - Header: Security Profiles > SSL/SSH Inspection
 - Buttons: +Create New, Edit, Clone, Delete, Search
 - Table:

Name	Read Only	Action
SSL certificate-inspection	🔒	Read-only SSL
SSL custom-deep-inspection	🔒	Customizable
SSL deep-inspection	🔒	Read-only dee
SSL no-inspection	🔒	Read-only prof
 - A red box highlights the "+Create New" button.
 - A blue callout box points to the table with the text "Preconfigured SSL certificate inspection profile".- Right Window: Select Multiple Clients Connecting to Multiple Servers**
 - Header: Select Multiple Clients Connecting to Multiple Servers
 - Form:

New SSL/SSH Inspection Profile
Name: New Profile
Comments: Write a comment... 0/255
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_CAs_SSL
Blocked certificates: Allow Block View Blocked Certificates
Untrusted SSL certificates: Allow Block View Trusted CAs List
Server certificate SNI check: Enabled
Protocol Port Mapping
Inspect all ports: HTTPS 443
 - A red box highlights the "SSL Certificate Inspection" option under "Inspection method".
 - A blue callout box points to the "SSL Certificate Inspection" option with the text "Select SSL Certificate Inspection".

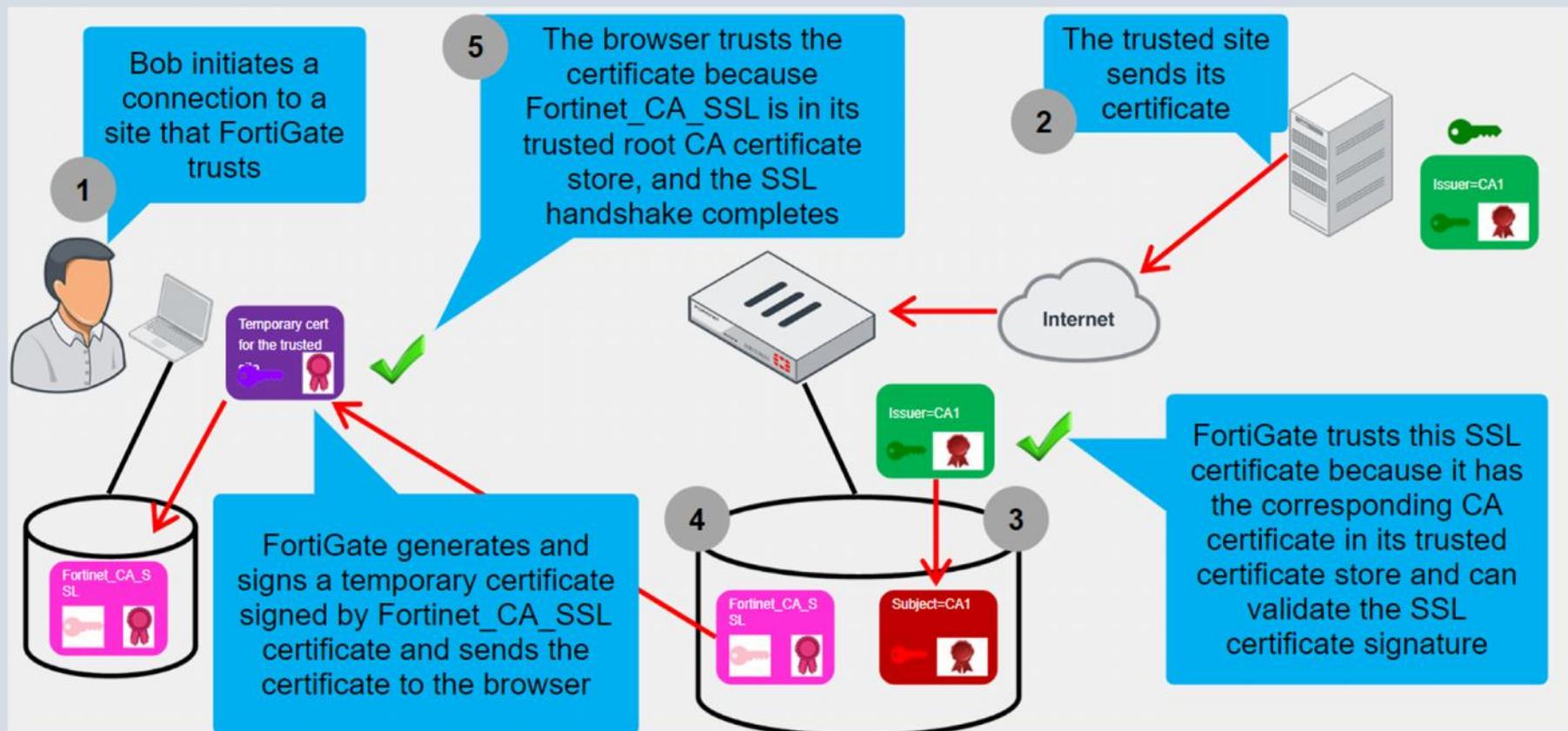
Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection de certificat SSL: Site de confiance



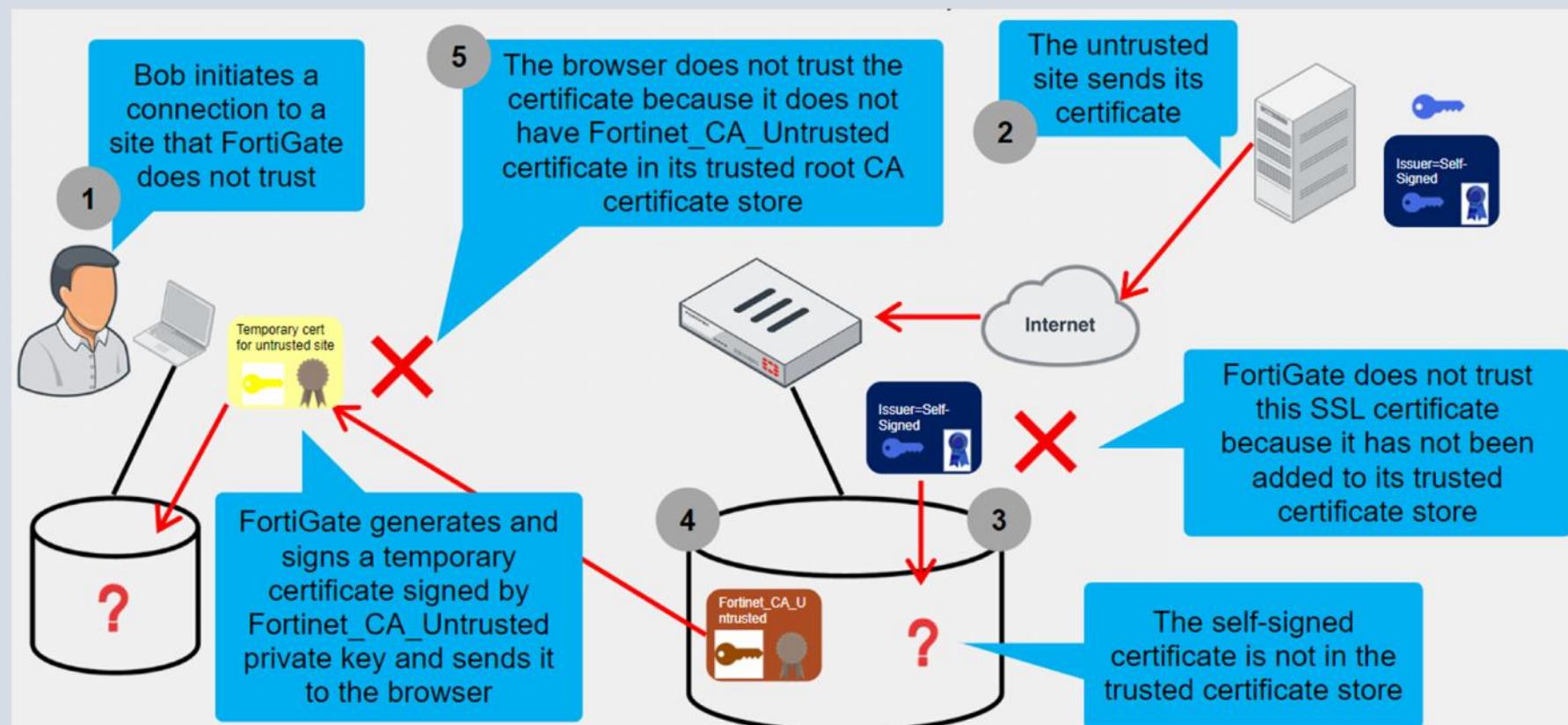
Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection de certificat SSL: Site de non confiance - Autorisation



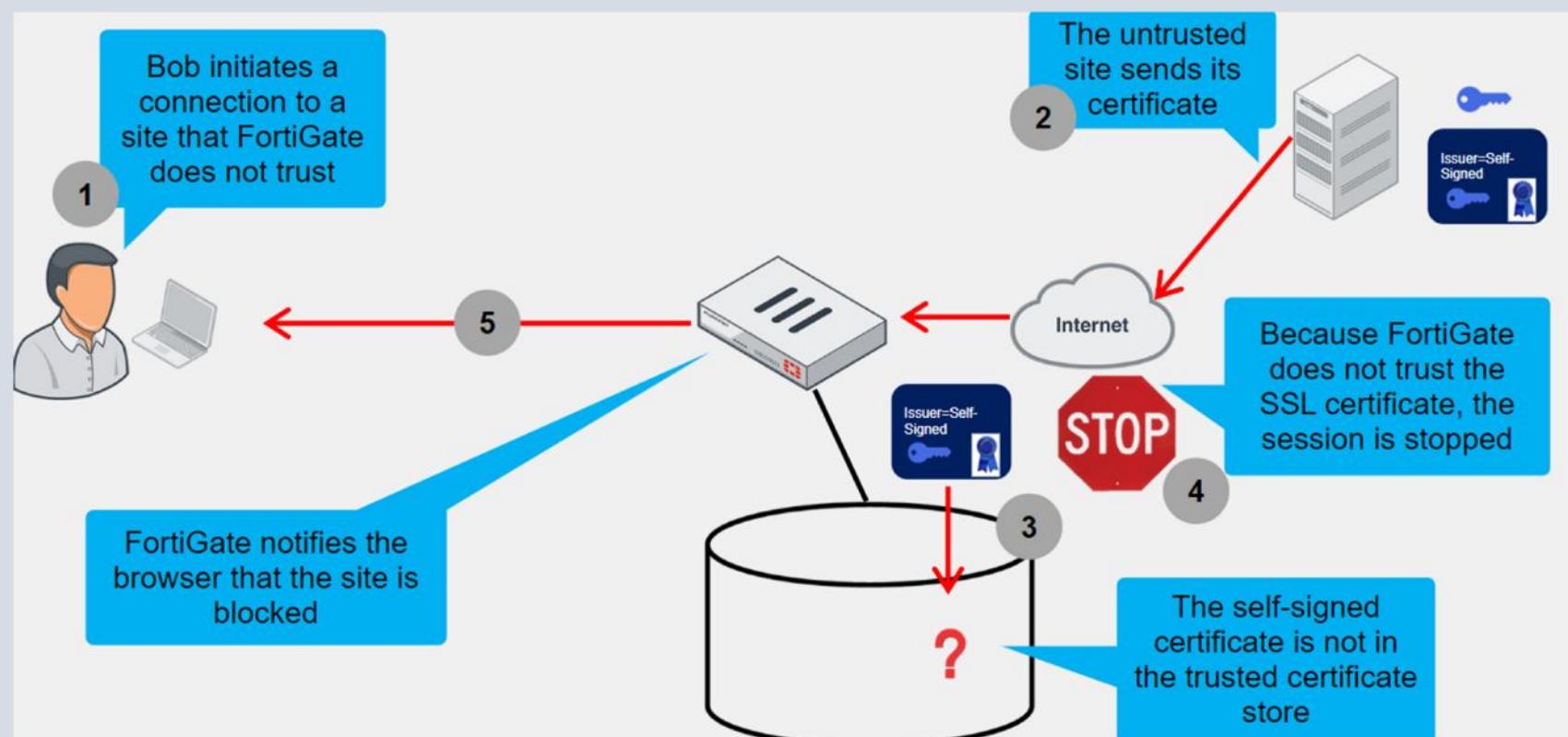
Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection de certificat SSL: Site de non confiance - Blocage



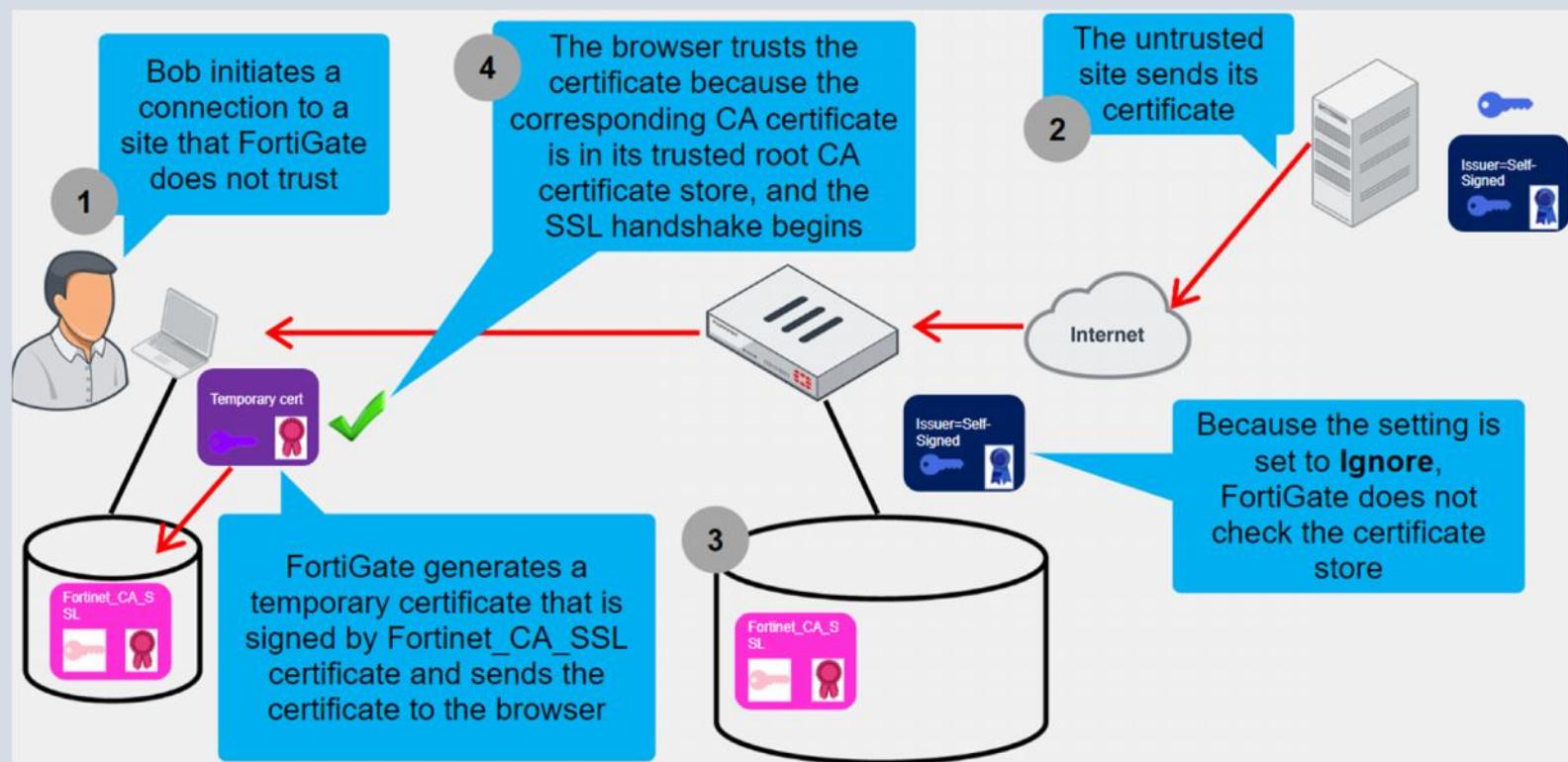
Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection de certificat SSL: Site de non confiance - Ignorer



Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection de certificat SSL: Certificat invalide

- Détection de certificat invalide:
 - Expiration;
 - Révocation;
 - Temps de validation dépassé;
 - Echec de validation.
- Action configurable:
 - Keep untrusted & allow;
 - Block
 - Trust & Allow

Security Profiles > SSL/SSH Inspection

Common Options			
Invalid SSL certificates	Allow	Block	Custom
Expired certificates	Keep Untrusted & Allow	Block	Trust & Allow
Revoked certificates	Keep Untrusted & Allow	Block	Trust & Allow
Validation timed-out certificates	Keep Untrusted & Allow	Block	Trust & Allow
Validation failed certificates	Keep Untrusted & Allow	Block	Trust & Allow

Log SSL anomalies  

Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

Inspection SSH: Configuration

- Uniquement utilisé par les profils antivirus

The screenshot shows the 'Security Profiles > SSL/SSH Inspection' interface. On the left, under 'SSL Inspection Options', the 'Enable SSL inspection of' dropdown is set to 'Multiple Clients Connecting to Multiple Servers', which is highlighted with a red box. Below it, the 'Inspection method' dropdown is set to 'Full SSL Inspection'. Under 'CA certificate', there is a warning icon and a dropdown menu showing 'Fortinet_CA_SSL'. There are also sections for 'Blocked certificates', 'Untrusted SSL certificates', 'Server certificate SNI check', and several compliance checkboxes for SSL cipher, negotiation, and RPC over HTTPS.

On the right, under 'SSH Inspection Options', the 'SSH deep scan' checkbox is checked (highlighted with a red box), and the 'SSH port' dropdown is set to 'Specify' with the value '22'.

Certificats

Authentification et sécurisation

Inspection SSL: Protection d'un serveur SSL

- ❑ Configuration d'un profil SSL;
- ❑ Définition d'un certificat pour le serveur SSL
- ❑ Le serveur de certificat, la clé privée et le certificat intermédiaire doivent être installés sur le FortiGate

Inspection de trafic (suite)

Security Profiles > SSL/SSH Inspection

SSL Inspection Options

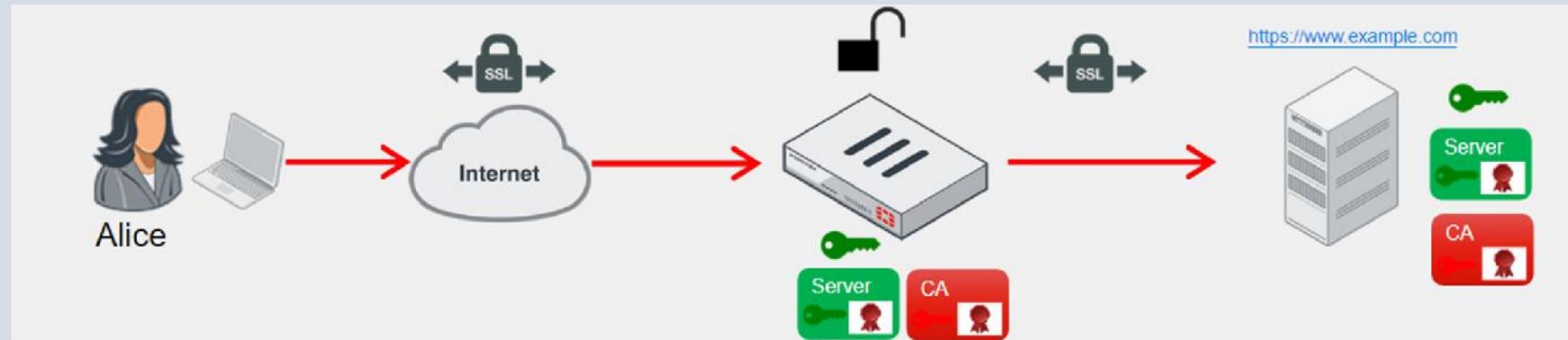
Enable SSL Inspection of Multiple Clients Connecting to Multiple Servers
 Protecting SSL Server

Server certificate Cert_Webserver

Protocol Port Mapping

Inspect all ports

HTTPS 443



Certificats

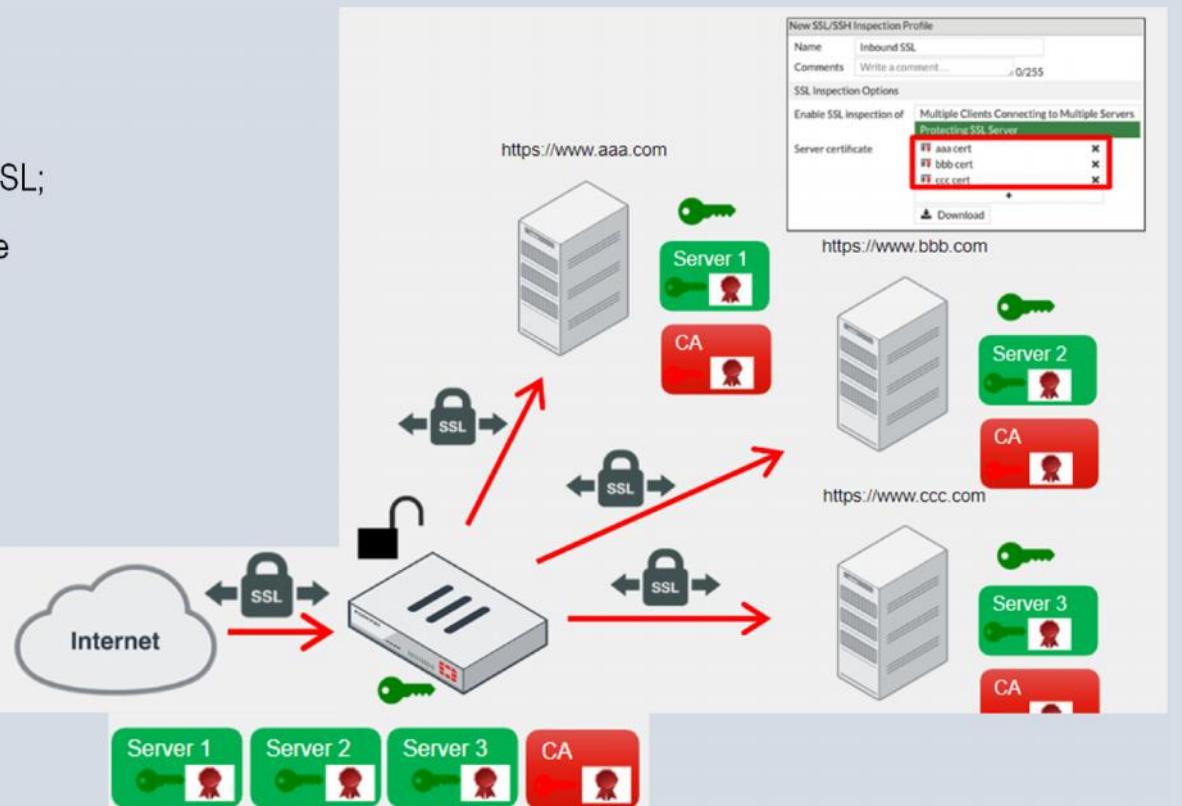
Authentification et sécurisation

Inspection SSL: Protection d'un serveur SSL

- Plusieurs certificats peuvent être définis dans un profil SSL;
- Sélection du certificat basée sur le SNI (Server Name Indication);
- Sélection du 1^{er} certificat dans la liste sur aucune correspondance.

SNI: www.aaa.com
IP: 172.16.1.1
SNI: www.bbb.com
IP: 172.16.1.1
SNI: www.ccc.com
IP: 172.16.1.1

Inspection de trafic (suite)



Gestion des certificats

Certificats

Authentification et sécurisation

Inspection SSL: Protection d'un serveur SSL – Application d'un profile de SSL

- Application au niveau du profile au niveau de la politique pare-feu

Inspection de trafic (suite)

Gestion des certificats

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Security Profiles' section, the 'SSL Inspection' dropdown is highlighted with a red box and contains the value 'SSL deep-inspection'. A callout bubble points to this dropdown with the text 'Select the SSL inspection profile'. Below the dropdown, there is a 'Decrypted Traffic Mirror' toggle switch, which is currently off. Another callout bubble points to this switch with the text 'Enable to mirror decrypted SSL traffic to an interface'. To the right of the dropdown, a list of available SSL inspection profiles is shown in a dropdown menu, with 'SSL deep-inspection' highlighted in yellow. A third callout bubble points to this list with the text 'Can select other SSL inspection profiles from the drop-down list'. The list includes: certificate-inspection, custom-deep-inspection, deep-inspection (highlighted), my-ssl-inspection-profile, and no-inspection.

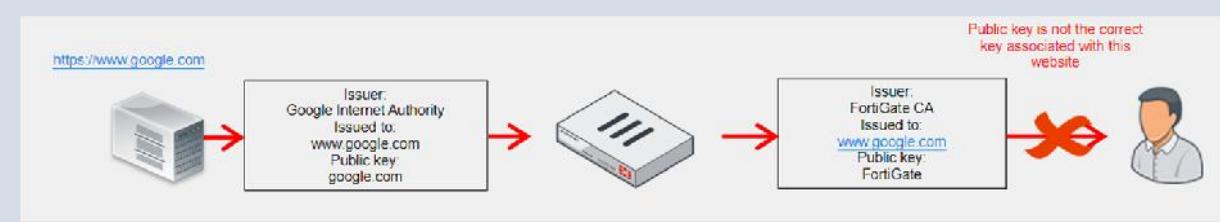
Certificats

Authentification et sécurisation

Inspection SSL: HTPS et HPKP

- Mesure de sécurité utilisée pour mitiger les attaques MITM (Man In The Middle);
- HSTS (HTTP Strict Transport Security)
 - Mécanisme permettant aux sites web de se déclarer accessible uniquement par connexion sécurisée
- HPKP (HTTP Public Key Pinning)
 - Imposé par le serveur web;
 - Association d'une ou de plusieurs clés publiques au site web pour une période.
- HSTS et HPKP destinés à travailler ensemble

Inspection de trafic (suite)



Gestion des certificats

Certificats

Authentification et sécurisation

HTTPS et HPKP: Limites et incidents

Inspection de trafic (suite)

Gestion des certificats

Exclure les sites web de l'inspection SSL complet (Full Inspection)

Utiliser l'inspection de certificat SSL à la place

Utiliser des navigateurs web qui ne supporte pas HPKP comme Chrome, Internet Explorer ou Edge

Désactiver les paramètres de sécurité sur les navigateurs.

Certificats

Authentification et sécurisation

Inspection SSL et Applications

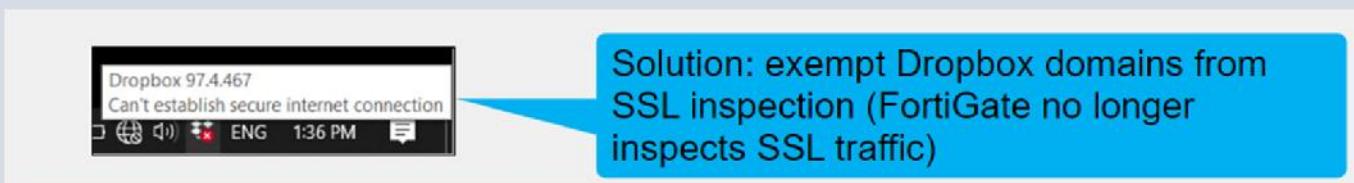
- L'inspection SSL touche les applications;
- Solution à l'incident dépend de l'application;
- Microsoft Outlook



Inspection de trafic (suite)

Gestion des certificats

- Dropbox



Certificats

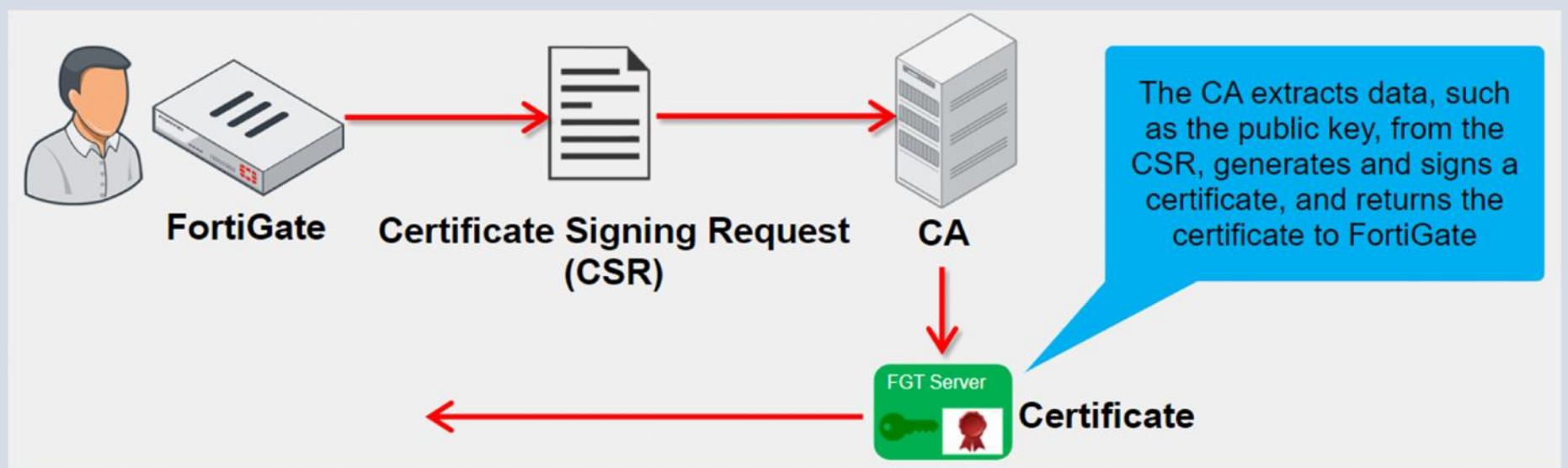
Authentification et sécurisation

Inspection de trafic

Gestion des certificats

Génération d'un CSR (Certificate Signing Request): Procédure

- Génération du CSR au niveau du FortiGate;
- Soumission du CSR au CA;
- Vérification du CSR par le CA;
- Création et envoi du certificat.



Certificats

Authentification et sécurisation

Génération d'un CSR (Certificate Signing Request)

- ❑ Fichier: génération d'un fichier au format .CSR;
- ❑ SCEP (Simple Certificate Enrollment Protocol) : disponible sur FortiAuthenticator.

Inspection de trafic

Gestion des certificats (suite)

The screenshot shows the FortiAuthenticator web interface under the 'System > Certificates' section. On the left, there is a list of certificates categorized into 'Local CA Certificate' (2 items) and 'Local Certificate' (14 items). The 'Generate' button in the top navigation bar is highlighted with a red box and a red arrow points from it to a detailed configuration dialog box on the right. The configuration dialog is titled 'Generate Certificate Signing Request' and contains the following fields:

- Certificate Name:** SSL_Cert
- Subject Information:** ID Type: Host IP, IP: 172.16.1.100
- Optional Information:**
 - Organization Unit: IT
 - Organization: Acme Corp
 - Locality(City): Lake City
 - State / Province: CA
 - Country / Region: US
 - E-Mail: support@acme.corp
 - Subject Alternative Name: (empty)
 - Password for private key: (empty)
- Key Type:** RSA
- Key Size:** 1024 Bit, 1536 Bit, 2048 Bit, 4096 Bit
- Enrollment Method:** File Based, Online SCEP

Certificats

Authentification et sécurisation

Inspection de trafic

Gestion des certificats (suite)

Enregistrement du CSR (Certificate Signing Request)

- Sélection et téléchargement du certificat dans le magasin de certificat du FortiGate;
- Soumissions au CA pour vérification.

The screenshot shows the 'System > Certificates' interface. At the top, there are buttons for 'Generate', 'Edit', 'Delete', 'Import', 'View Details', and 'Download'. The 'Download' button is highlighted with a red box. Below the buttons is a table with columns 'Name', 'Subject', and 'Comment'. Two certificates are listed: 'Fortinet_Wif' and 'SSL_Cert'. A blue tooltip box points to the 'Download' button with the text: 'Note that if you delete the CSR, you cannot import the signed certificate and you must start over'.

Name	Subject	Comment
Fortinet_Wif	C = US, ST = California, L = Sunnyvale, O = "For...	This certificate is embed...
SSL_Cert		

Certificats

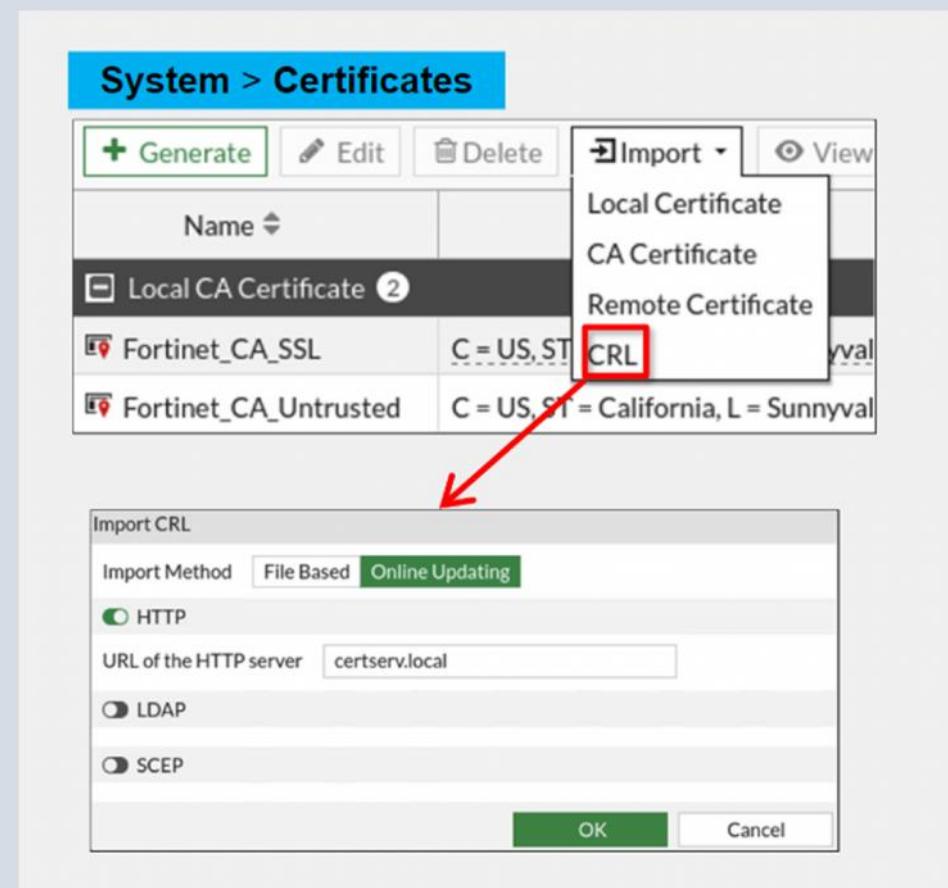
Authentification et sécurisation

Importation d'une CRL (Certificat Revocation List)

- Méthode d'importation: HTTP; LDAP, SCRP, Fichier
- Mise à jour automatique avant l'expiration de la liste.

Inspection de trafic

Gestion des certificats (suite)



Certificats

Authentification et sécurisation

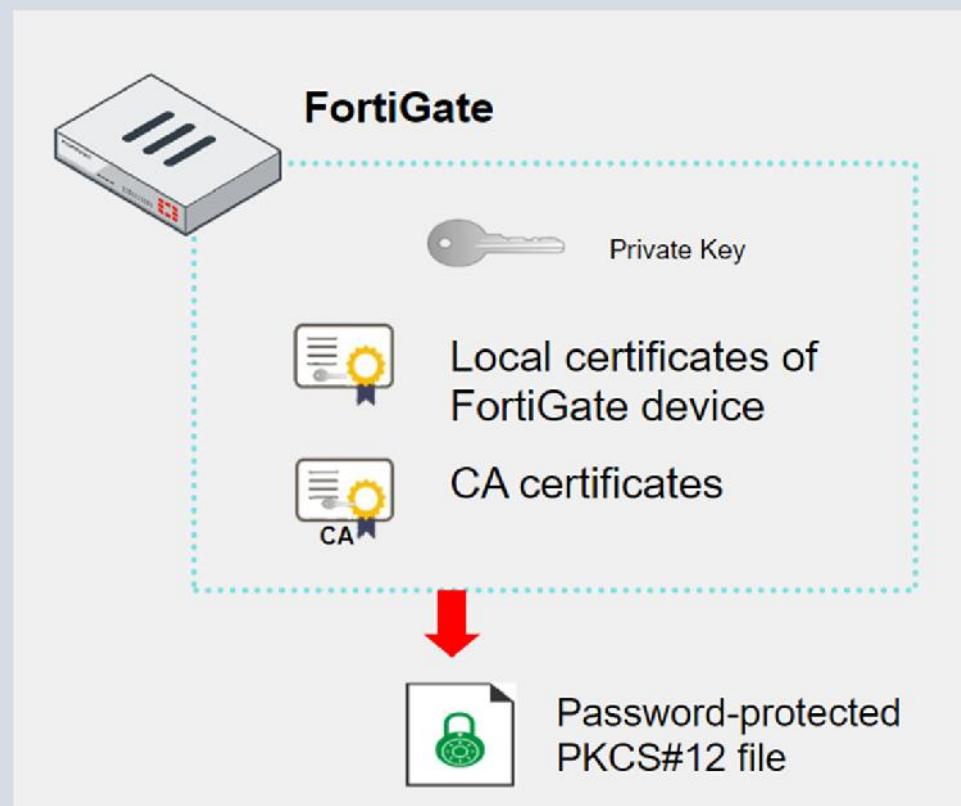
Sauvegarde et restauration des certificats

- ❑ Sauvegarde des clés et certificat via CLI;
- ❑ Clés et certificats sauvegardés dans le fichiers PKCS#12;
- ❑ Backup des configurations contiennent également les clés et les certificats.

```
execute vpn certificate local
import tftp <file-name_str>
<tftp_ip>.
execute vpn certificate local
export tftp <certificate-name_str>
<file-name_str> <tftp_ip>.
```

Inspection de trafic

Gestion des certificats (suite)



FORTINET®



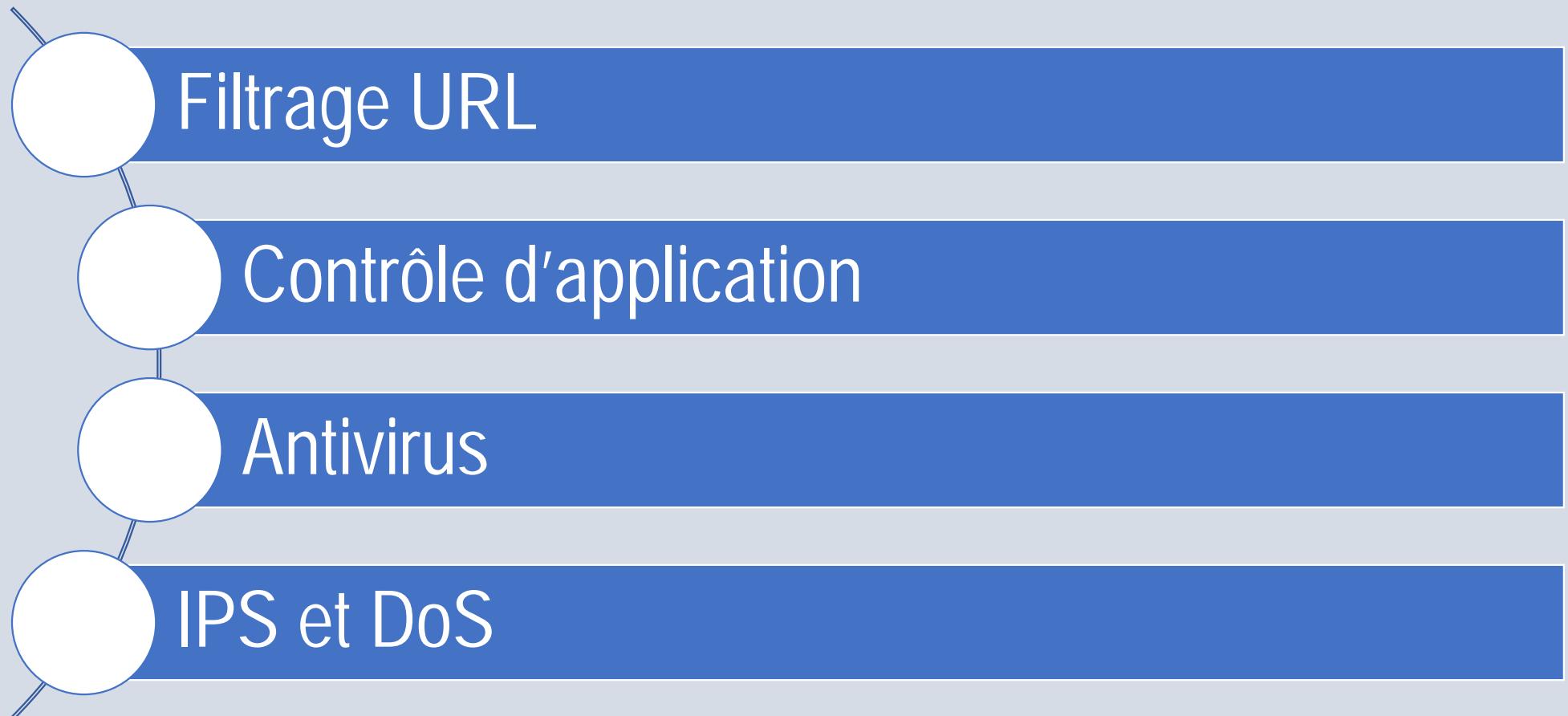
NSE Training Institute

FortiGate Security

FONCTIONNALITES UTM (UNIFIED THREATS MANAGEMENT)



Plan du module



Filtrage URL

Objectifs

- Identifier les modes d'inspection;
- Comprendre les bases du filtrage URL;
- Configurer le filtrage vidéo;
- Configurer le filtrage DNS et de fichier;
- Bonne pratiques.

Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Généralités: Mode d'inspection

- Application au niveau des paramètres de règles de trafic;
- 02 Types:
 - Flow-based
 - Mode par défaut;
 - Supporter uniquement sur les règles de trafic de type flow-based
 - Proxy-based
 - Permet à la fois les 02 modes d'inspection sur les profils de sécurité
 - Plus approfondie et couvre plus de protocoles que le type flow-based.

The screenshot shows a portion of the FortiOS interface under the heading "Policy & Objects > Firewall Policy". A sub-menu bar at the top includes "Inspection Mode". Below it, two buttons are displayed: "Flow-based" (which is highlighted in green) and "Proxy-based".

Filtrage URL

Mode d'inspection (suite)

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Types: Mode Flow-based

- Mode d'inspection par défaut;
- Identification et blocage des menaces de sécurité en temps réel;
- Avantages:
 - Temps de réponse relativement court;
 - Probabilité d'erreur du au temps mort faible.
- Inconvénients:
 - Nombre de fonctionnalité de sécurité disponible réduit par rapport au mode proxy-based;
 - Actions disponibles en foncton de la catégorisation des sites wen réduites.

Filtrage URL

Mode d'inspection (suite)

Base du Filtrage URL

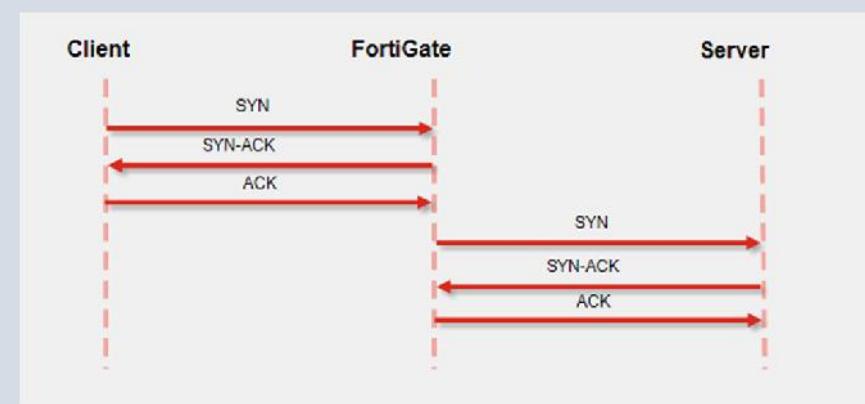
Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Type: Mode Proxy-based

- Inspection approfondie;
- Augmentation de la latence en raison du scan complet de contenu;
- Fourniture d'un niveau élevé de protection contre les menaces;
- Etablissement de 02 connexion TCP:
 - Client au FortiGate: Serveur proxy;
 - FortiGate au Serveur.
- Plus gourmand en ressource.



Filtrage URL

Mode d'inspection (suite)

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Type: Mode NGFW

- Dispose de 02 modes:
 - Mode profile-based:
 - Nécessite la création préalable des profils pour le control d'application et le filtrage des URL;
 - Application des profils sur les règles de trafic;
 - Applicable aux 02 modes d'inspection.
 - Mode policy-based:
 - Application des profils directement sur la politique;
 - Ne nécessite les profils de control d'application et filtrage URL;
 - Applicable uniquement sur le mode d'inspection flow- base;
 - Active la fonctionnalité NAT central?

Filtrage URL

Mode d'inspection (suite)

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Policy & Objects > Firewall Policy

Inspection Mode Flow-based Proxy-based

Customizable at the policy level

Protocol & Objects > Protocol Options

Protocol Port Mapping

HTTP	<input checked="" type="checkbox"/>	Any	Specify	80
SMTP	<input checked="" type="checkbox"/>	Any	Specify	25
POP3	<input checked="" type="checkbox"/>	Any	Specify	110
IMAP	<input checked="" type="checkbox"/>	Any	Specify	143
FTP	<input checked="" type="checkbox"/>	Any	Specify	21
NNTP	<input checked="" type="checkbox"/>	Any	Specify	119
MAPI	<input checked="" type="checkbox"/>			135
DNS	<input checked="" type="checkbox"/>			53
CIFS	<input checked="" type="checkbox"/>			445

Protocol ports can be customized

The screenshot shows the FortiGate management interface. In the top navigation bar, 'Policy & Objects > Firewall Policy' is selected. Below it, there's a section for 'Inspection Mode' with three options: 'Flow-based' (selected), 'Proxy-based', and 'Flow+Proxy'. A callout bubble points to the 'Proxy-based' option with the text 'Customizable at the policy level'. Another callout bubble points to the 'Specify' button in the 'Protocol Port Mapping' table with the text 'Protocol ports can be customized'. The 'Protocol Options' table lists various protocols with their current port settings.

Filtrage URL

Mode d'inspection

Base du Filtrage URL

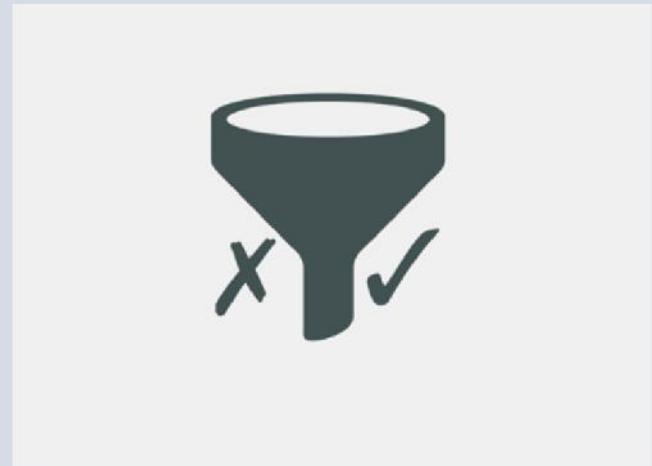
Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL: Pourquoi?

- Mitiger les effets négatif des contenus web inappropriés;
- Préserver la productivité des employés;
- Prévenir les congestions réseaux;
- Prévenir la perte de donnée et l'exposition des informations confidentiels;
- Diminuer l'exposition aux menaces web;
- Etc.



Filtrage URL

Mode d'inspection

Base du Filtrage URL (suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

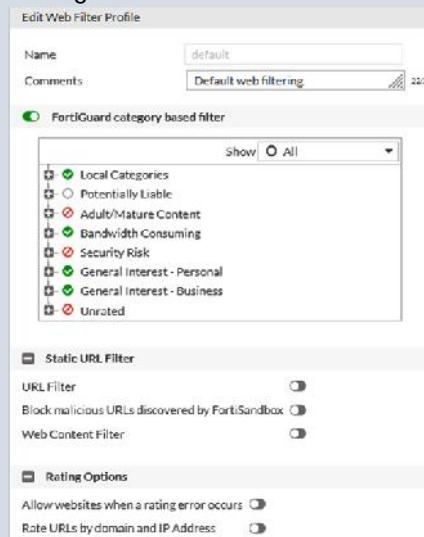
Bonne Pratiques

Filtrage URL: Configuration

Mode profiles based

- Configuration d'un profil de sécurité web
 - Catégories préconfigurées (FortiGuard)
 - URL statique
 - Option d'évaluation
- Application du profil sur la règle de trafic

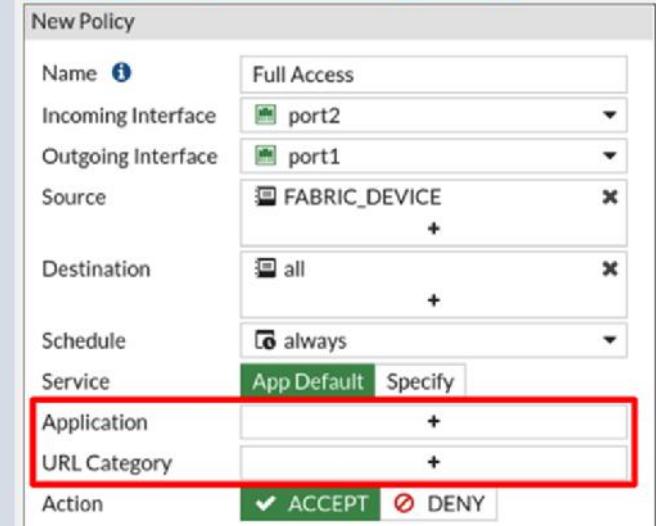
Security Profiles > Web Filter



Mode policy based

- Application des catégories d'URL et options de contrôle d'application directement sur la règle de trafic

Policy & Objects > Security Policy



Filtrage URL

Mode d'inspection

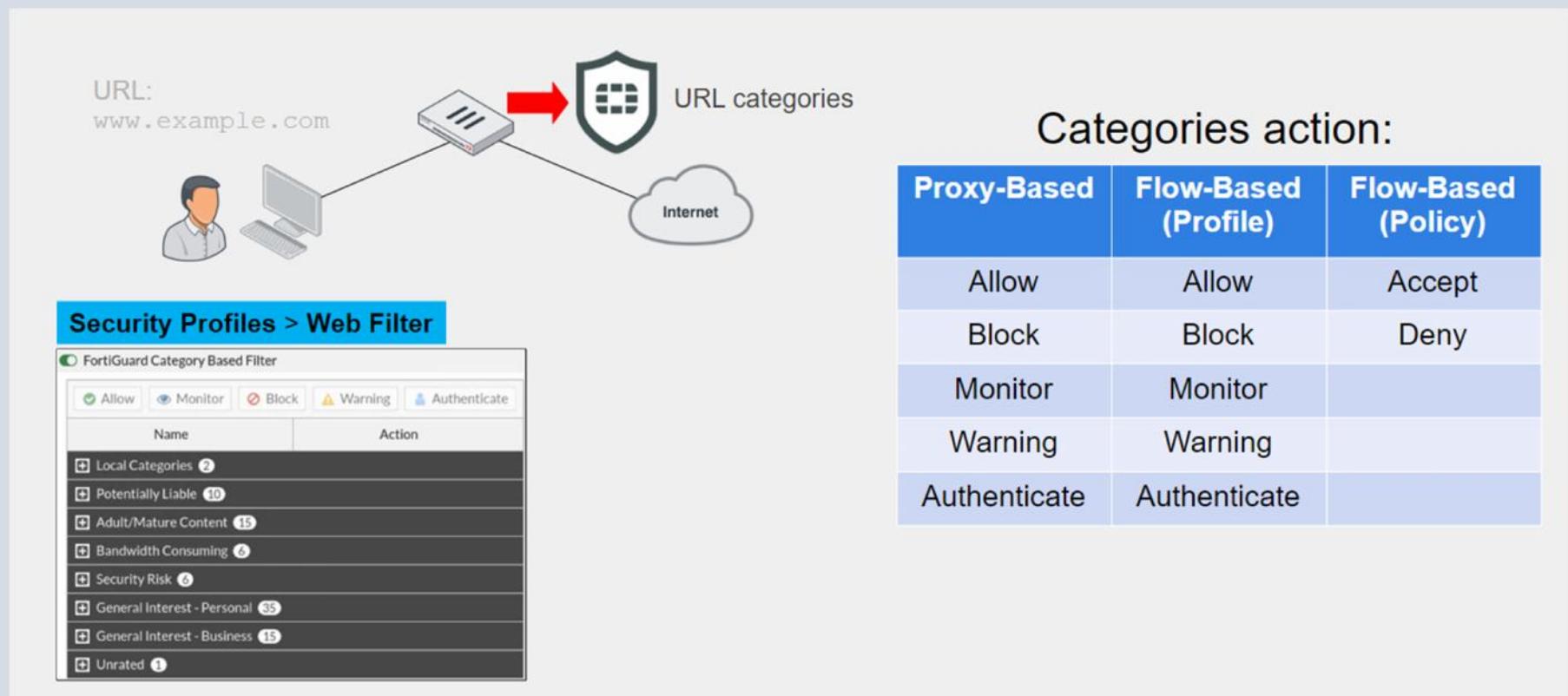
Base du Filtrage URL (suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL: Fonctionnement



Filtrage URL

Mode d'inspection

Base du Filtrage URL (suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL Static: Fonctionnement

- Vérification de la liste d'URL configurée manuellement;
- 04 actions possible:
 - Allow: Accès permis;
 - Block: Accès interdit;
 - Monitor: Trafic autorisé mais journalisé;
 - Exempt: Trafic autorisé des sources de confiance uniquement.
- Type de modèle d'URL:
 - Simple: www.google.cm;
 - Wildcard: *.google.*:
 - Expression Régulière: .*\.\.google\.\{org|biz\}

Security Profiles > Web Filter

URL	Type	Action	Status
.*\.something\.\{org biz\}	Regular Expression	Exempt	Enable
somewhere.*	Wildcard	Monitor	Enable
www.somesite.com/someURL	Simple	Block	Enable

URL: www.somesite.com/someURL

Block

Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

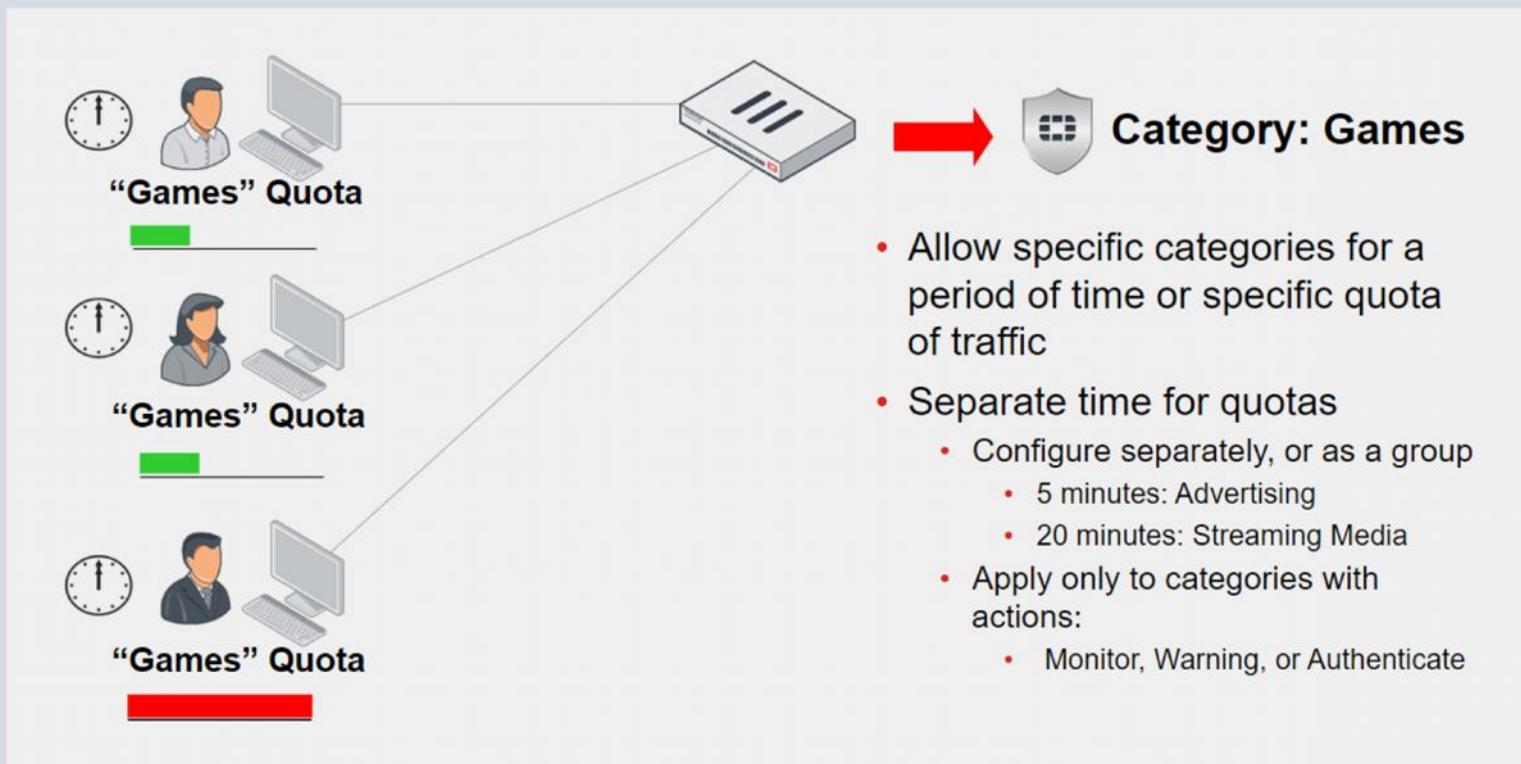
Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Quotas d'utilisation



Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Remplacement du profil Web (Web Profile Override)
- Permet à un utilisateur, un groupe d'utilisateur ou une IP source d'utilisé un profil web différent

The screenshot shows two FortiOS configuration screens. The top screen is titled "Security Profiles > Web Filter" and lists three profiles: "default" (Comments: Default web filtering, Ref: 1), "monitor-all" (Comments: Monitor and log all visited URLs, flow-based, Ref: 0), and "wifi-default" (Comments: Default configuration for offloading WiFi traffic, Ref: 1). The "monitor-all" profile is highlighted with a red border. A red arrow points from this screen down to the second screen. The second screen is titled "Security Profiles > Web Profile Overrides" and shows a "New Administrative Override" dialog. The dialog fields are: Scope range (User selected), User (student selected), Original profile (default selected), New profile (monitor-all selected), Expires (04/18/2021 at 08:07:00.000 PM), and Status (Enable selected).

Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Filtrage des moteurs de recherche
- Force l'utilisation d'un navigateur particulier;
- Nécessite l'utilisation de l'inspection SSL approfondie;
- Supporter par Google, Yahoo, Bing et Yandex

The screenshot shows the 'Security Profiles > Web Filter' configuration page. It includes a section for 'Search Engines' with the rule 'Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex' (status: P, On) and another for 'Log all search keywords' (status: P, On). Below this is a code block showing the CLI configuration:

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

Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Filtrage de contenu web
- Contrôler l'accès à des sites contenus certains mots;
- Contrôle effectué via: Mots, phrases, etc.;
- Pondération des modèles afin de déterminer l'action appropriée;
- Action: Block ou Exempt;
- Nécessite l'utilisation de l'inspection SSL affrondie.

The screenshot shows the 'Security Profiles > Web Filter' configuration page. At the top, there are four toggle switches for 'Static URL Filter' (disabled), 'Block invalid URLs' (disabled), 'URL Filter' (disabled), and 'Block malicious URLs discovered by FortiSandbox' (disabled). Below these is a 'Content Filter' toggle switch, which is enabled and highlighted with a red border. Underneath is a table with two rows of filter rules:

Pattern Type	Pattern	Language	Action	Status
Wildcard	something.*	Western	Exempt	Enable
Regular Expression	.*quelqueque	French	Block	Enable

Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

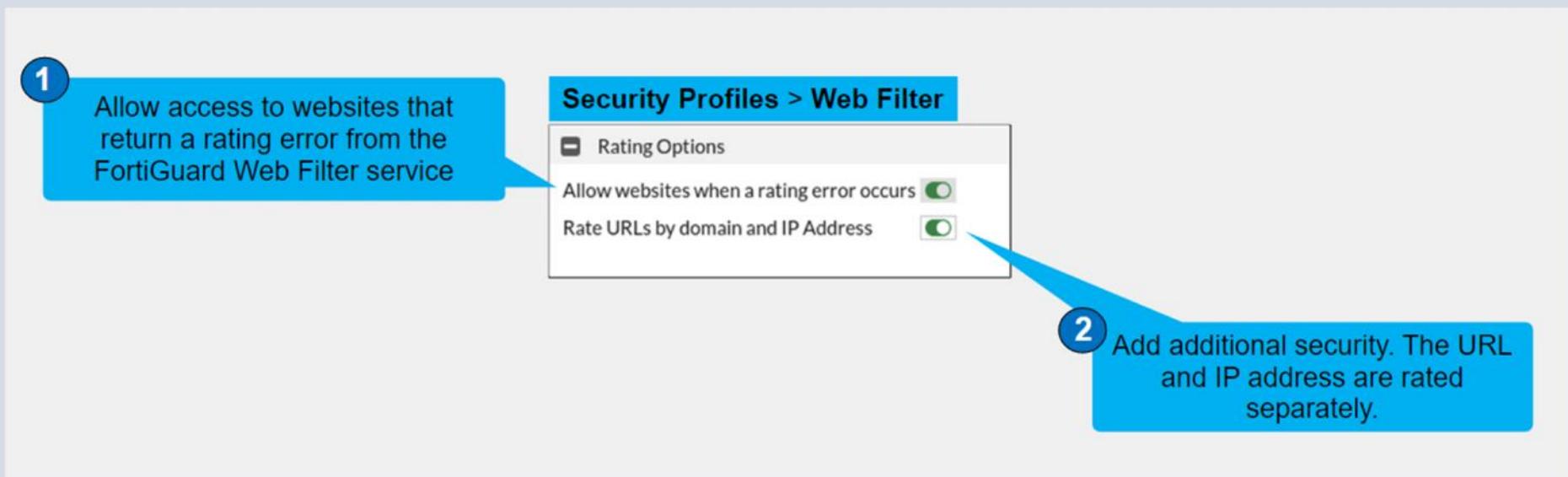
Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

- ❑ Fonctionnalité supplémentaires: Paramètres avancés



Filtrage URL

Mode d'inspection

Base du Filtrage URL(suite)

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage URL : Profile de sécurité en mode policy-based

Fonctionnalité supplémentaires: Paramètres avancés

- Feature set proxy based
- Proxy options:

1

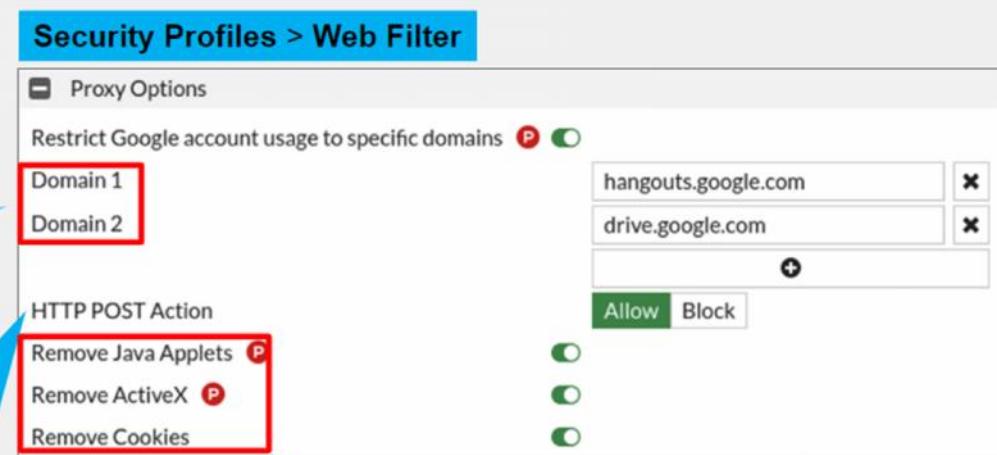
Restrict Google account usage to specific domains by configuring the Google domains you want to allow

2

Limit users from sending information and files to websites

3

Filter ActiveX, Java applets, and cookies from web traffic



Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage Vidéo

- Contrôle de l'accès à YouTube
 - Contrôle basé sur les catégories, les chaines ou les vidéos;
 - Nécessite une licence;
 - Mode d'inspection prox-based uniquement;
 - Nécessite l'inspection SSL approfondie;
 - Nécessite les clés d4API YouTube;
 - 02 méthodes de filtrage:
 - Catégories FortiGuard;
 - ID des chaines.



Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo (suite)

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage Vidéo: Catégorie

Security Profiles > Video Filter

FortiGuard Category Based Filter

Category	Action
Business	Allow
Entertainment	Allow
Games	Allow
Knowledge	Allow
Lifestyle	Allow
Music	Allow
News	Allow
People	Allow
Society	Allow
Sports	Allow

Set the action to allow, monitor, or block videos based on FortiGuard category

11 local universal categories available to match with API determined value when accessing the content

55% (11)

Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo (suite)

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage Vidéo: Catégorie

The screenshot shows the 'Edit Video Filter Profile' screen for a profile named 'YouTube Filter'. It includes fields for 'Name' (YouTube Filter), 'Comments' (Write a comment... 0/255), and a radio button for 'FortiGuard Category Based Filter'. Under the 'YouTube' section, there's a 'Restrict YouTube access' dropdown with options 'Moderate' and 'Strict', where 'Moderate' is selected. A 'Channel override list' table is present, with one row highlighted in red containing 'UCJHo4AuVormwMRzgkA5DQEOA' in the Channel ID column and 'Block' in the Action column. A blue callout points to this row with the text: 'Accessing the channel while on YouTube is blocked as configured in the video filter profile'.

Set Moderate or Strict access to YouTube

You can Allow, Monitor, or Block access to specific YouTube channels IDs

Attention

Web Page Blocked

The page you have requested has been blocked because the requested video resource is not allowed.

URL: https://www.youtube.com/channel/UCUpvZG-Sko_eXAuspbDfxWw
Description: Video channel is blocked, channel id=UCUpvZG-Sko_eXAuspbDfxWw.
Username:
Group Name:

Connect to the internet
You're offline. Check your connection.
RETRY

You will see a replacement message if you access a blocked channel directly using the URL

Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Filtrage basé sur le DNS

- Inspection du trafic en utilisant les filtres DNS;
- Moins précis que le filtrage basé sur HTTP
- Inspection SSL disponible
 - DNS over TLS (DoT);
 - DNS over HTTPS (DoH)
- Supporte uniquement filtrage URL statiques et les catégories FortiGuard

Filtrage URL

Mode d'inspection

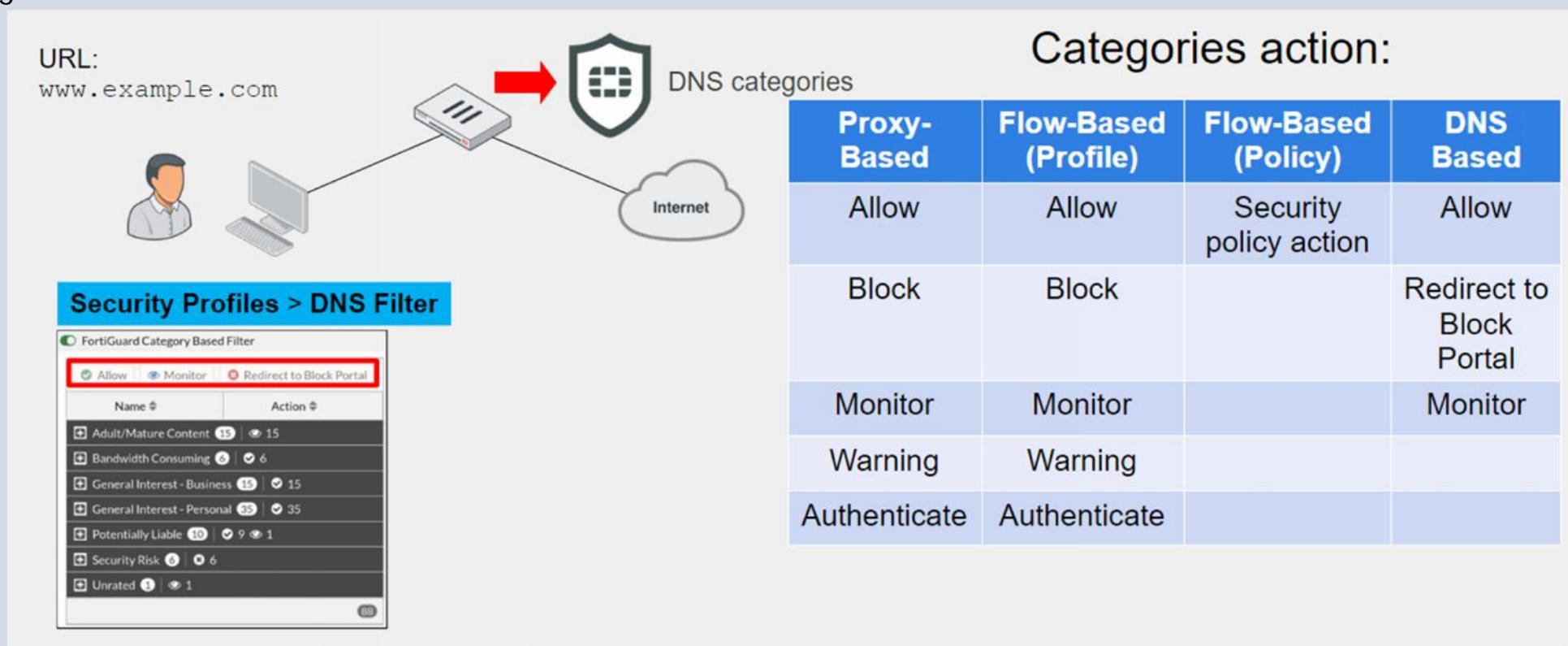
Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS (suite)

Bonne Pratiques

Filtrage basé sur le DNS: Fonctionnement



Filtrage URL

Mode d'inspection

Base du Filtrage URL

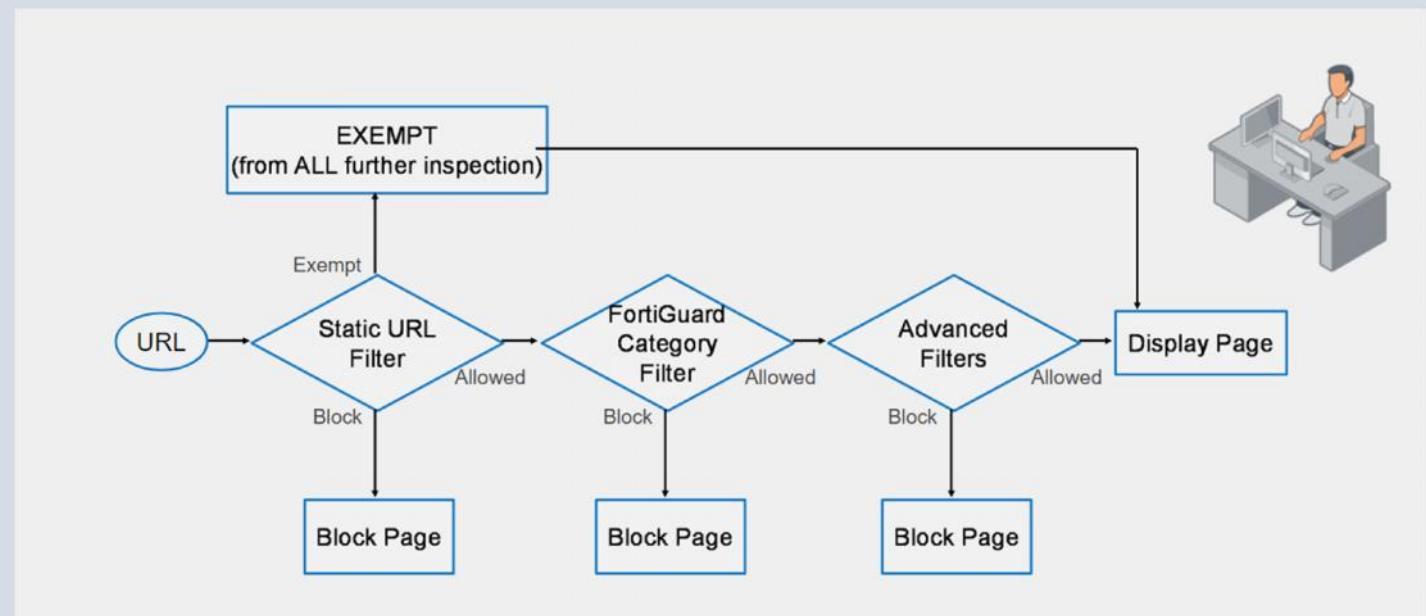
Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques

Bonnes pratiques: Ordre d'inspection HTTP

- URL Statique;
- Catégorie d'URL FortiGuard;
- Filtre avancés.



Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques (suite)

Bonnes pratiques: Cache DNS

- Améliore les performances;

System > FortiGuard

Filtering	
Web Filter cache	<input checked="" type="checkbox"/> Clear cache after 60 Minutes
Email Filter cache	<input checked="" type="checkbox"/> Clear cache after 30 Minutes
FortiGuard filtering services	HTTPS 443
Test Connectivity	

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

Filtrage URL

Mode d'inspection

Base du Filtrage URL

Filtrage Vidéo

Filtrage de Fichier et DNS

Bonne Pratiques (suite)

Bonnes pratiques: journalisation

Log & Report > Web Filter						
Date/Time	User	Source	Action	URL	Category Description	Sent / Rece
Minute ago		10.0.1.10	passthrough	https://bat.bing.com/	Search Engines and Portals	517 B/0
Minute ago		10.0.1.10	passthrough	https://site.fortinet.com/	Information Technology	517 B/0
Minute ago		10.0.1.10	passthrough	https://site.fortinet.com/	Information Technology	517 B/0

```
date=2021-04-22 time=09:32:04 eventtime=1619109124643229175 tz="-0700"
logid="0317013312" type="utm" subtype="webfilter" eventtype="ftgd_allow"
level="notice" vd="root" policyid=1 sessionid=9505 srcip=10.0.1.10 srcport=57734
srcintf="port3" srcintfrole="undefined" dstip=96.45.36.159 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="site.fortinet.com" profile="monitor-all" action="passthrough"
reqtype="direct" url="https://site.fortinet.com/" sentbyte=517 rcvdbyte=0
direction="outgoing" msq="URL belongs to an allowed category in policy"
method="domain" cat=52 catdesc="Information Technology"
```

Contrôle d'applications

Objectifs

- Comprendre les bases du contrôle d'application;
- Configurer le contrôle d'application;
- Superviser et journaliser les évènements;
- Maîtriser quelques bonnes pratiques.

Contrôle d'application

Contrôle d'application

Contrôle d'application

- Contrôler le trafic des applications;
- Détecte et agit au niveau du trafic réseau des application:
 - FaceBook, Skype, Gmail, etc
 - Supporte les applications P2P et Proxy;
 - Scan des protocoles sécurisés mais nécessite l'activation de l'inspection SSL/SSH

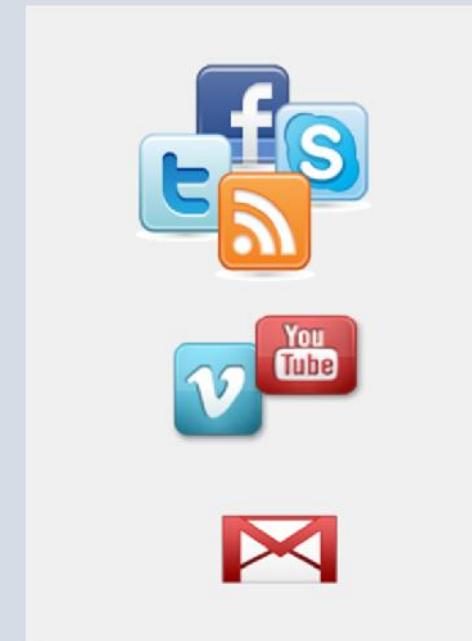
Fonctionnement:

- Configurable dans les 02 modes: Flow et proxy
- Utilisation du moteur IPS;
- Utilisation du mode flow-based par défaut;
- Comparaison du trafic avec les modèles connu.

Configuration

Journalisation&Supervision

Bonnes pratiques



Contrôle d'application

Contrôle d'application (suite)

Contrôle d'application: Signature

- Nécessite une licence;
- Elément de base pour l'identification des applications.

Configuration

Journalisation&Supervision

Bonnes pratiques

The screenshot shows two panels of the FortiGuard configuration interface. The top panel, titled 'System > FortiGuard', displays the 'Currently installed application control database version' as Version 16.00943. The bottom panel, also titled 'System > FortiGuard', shows the 'Scheduled updates' section where 'Daily' is selected. A large blue arrow points from the 'Upgrade Database' button in the top panel to the 'Scheduled updates' section in the bottom panel, indicating the process of forcing a database update.

System > FortiGuard

Firmware & General Updates	Licensed (Expiration Date: 2022/01/01)
Application Control Signatures	Version 16.00943
Device & OS Identification	Version 1.00111
Internet Service Database Definitions	Version 7.01069

Actions: Upgrade Database, View List

System > FortiGuard

FortiGuard Updates	
Scheduled updates	Every Daily Weekly Automatic
1	AM
Improve IPS quality	Off
Use extended IPS signature package	On
AntiVirus PUP/PUA	On
Update server location	US only Lowest latency locations

Currently installed application control database version

Actions: Upgrade Database, View List

Forcing FortiGate to check for latest updates

Configuring scheduled updates

Contrôle d'application

Contrôle d'application

Configuration

Journalisation&Supervision

Bonnes pratiques

Security Profiles > Application Control

Edit Application Sensor

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

Name: wifi-default
Comments: Default configuration for offloading WiFi traffic. 50/255

Categories:

- All Categories (selected)
- Business (147, ▲ 6)
- Email (77, ▲ 12)
- Mobile (3)
- Proxy (168)
- Storage.Backup (164, ▲ 16)
- VoIP (24)
- Cloud.IT (47, ▲ 1)
- Game (84)
- Network.Service (330)
- Remote.Access (86)
- Update (49)
- Web.Client (24)
- Collaboration (260, ▲ 16)
- General.Interest (226, ▲ 7)
- P2P (56)
- Social.Media (115, ▲ 32)
- Video/Audio (155, ▲ 16)
- Unknown Applications

Applies an action to all categories at once

Firmware & General Updates License
Licensed (Expiration Date: 2023/01/01)

Application Control Signatures Packaged
Version 16.00943

Application Signatures
[View Application Signatures](#)

Additional Information

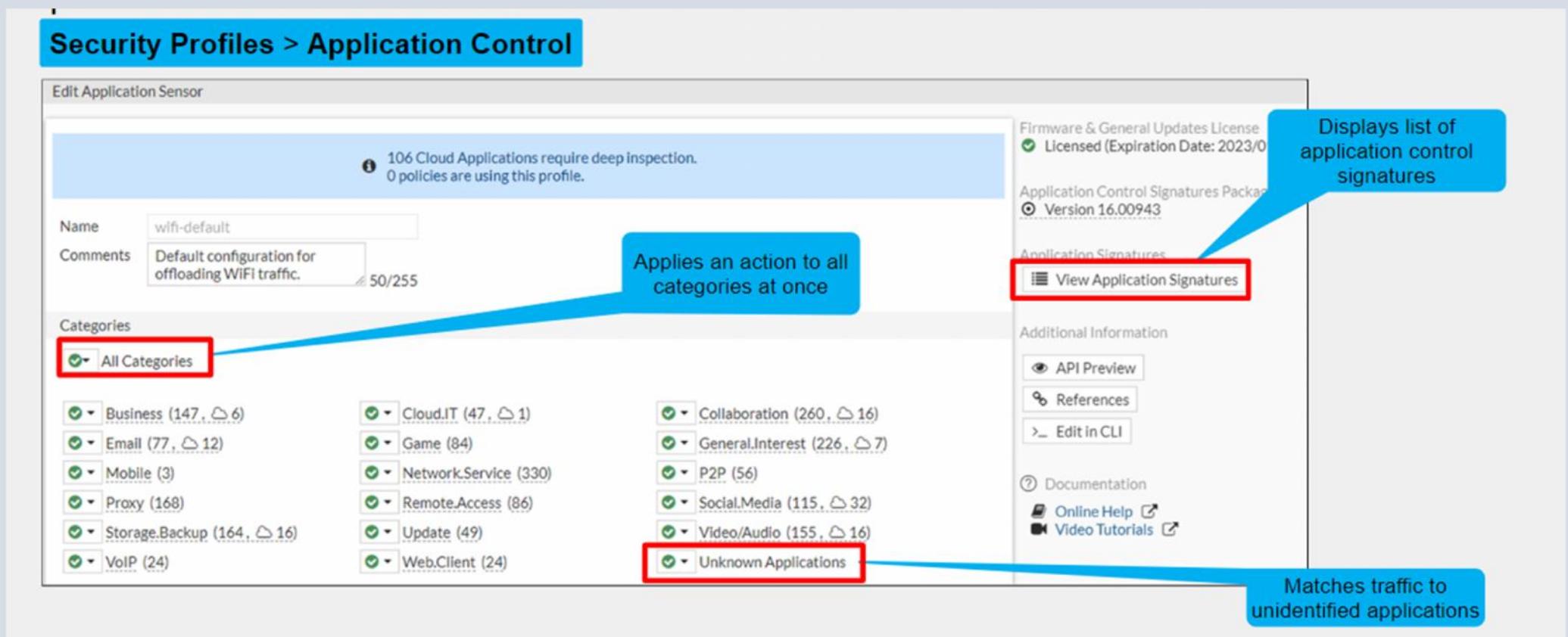
- API Preview
- References
- Edit in CLI

Documentation

- Online Help
- Video Tutorials

Displays list of application control signatures

Matches traffic to unidentified applications



Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Options avancées.

Security Profiles > Application Control

Categories

- All Categories
- Business (147, ▲ 6)
- Email (77, ▲ 12)
- Mobile (3)
- Proxy (168)
- Storage/Backup (164, ▲ 16)
- VoIP (24)
- Cloud.IT (47, ▲ 1)
- Game (84)
- Network.Service (330)
- Remote.Access (86)
- Update (49)
- Web.Client (24)
- Collaboration (260, ▲ 16)
- General.Interest (226, ▲ 7) (226, ▲ 7)
- P2P (56)
- Social.Media (115, ▲ 32)
- Video/Audio (155, ▲ 16)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority				Details	Type	Action
No results						

Options

- Block applications detected on non-default ports
- Allow and Log DNS Traffic
- QUIC Allow Block
- Replacement Messages for HTTP-based Applications

The number to the right of the cloud symbol indicates the number of cloud applications in the category

Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Contrôle de trafic de services sur les ports inconnus

The screenshot shows the 'Security Profiles > Application Control' interface. On the left, there's a tree view of categories like Business, Email, Mobile, etc., and a table for 'Network Protocol Enforcement' with rows for Port 52 (DNS, Monitor) and Port 80 (HTTP, Block). A red arrow points from the 'Create New' button in this table to the 'Edit Default Network Service' dialog on the right. This dialog shows port 80 with enforced protocols PROT DNS and PROT HTTP, and a violation action of Block. A red box highlights the 'PROT HTTP' entry in the 'Enforce protocols' dropdown. A blue callout bubble labeled 'List of known services' points to a sidebar on the right containing a list of services with their corresponding PROTOs: DNS (PROT DNS), FTP (PROT FTP), HTTP (PROT HTTP highlighted in yellow), HTTPS (PROT HTTPS), IMAP (PROT IMAP), NNTP (PROT NNTP), POP3 (PROT POP3), SMTP (PROT SMTP), SNMP (PROT SNMP), SSH (PROT SSH), and TELNET (PROT TELNET).

Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Ordre de scan

- Filtre et application statique;
- Catégories FortiGuard.

The screenshot shows the 'Edit Application Sensor' configuration page. At the top, there are fields for 'Name' (set to 'default') and 'Comments' (set to 'Monitor all applications.'). Below these are two main sections:

- Categories**: This section lists various application categories with their counts:
 - All Categories
 - Business (147, ▲ 6)
 - Email (77, ▲ 12)
 - Mobile (3)
 - Proxy (168)
 - Storage.Backup (164, ▲ 16)
 - VoIP (24)
 - Cloud.IT (47, ▲ 1)
 - Game (84)
 - Network.Service (330)
 - Remote.Access (86)
 - Update (49)
 - Web.Client (24)
 - Collaboration (260, ▲ 16)
 - General.Interest (226, ▲ 7)
 - P2P (56)
 - Social.Media (115, ▲ 32)
 - Video/Audio (155, ▲ 16)
 - Unknown Applications (checked)
- Application and Filter Overrides**: This section includes a table with columns: Priority, Details, Type, and Action. It displays the message "No results". Below the table are several options:
 - Block applications detected on non-default ports (checkbox)
 - Allow and Log DNS Traffic (checkbox)
 - QUIC (checkbox)
 - Replacement Messages for HTTP-based Applications (checkbox, set to Allow)

Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Ordre de scan (suite)

Security Profiles > Application Control

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

Categories:

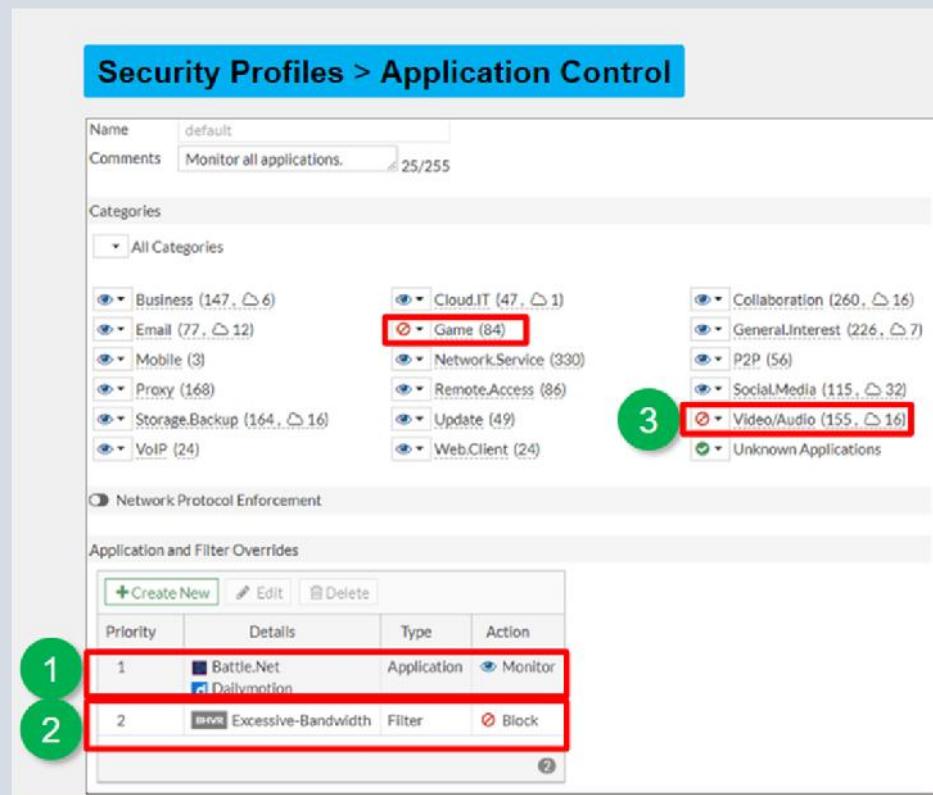
- All Categories
 - Business (147, △ 6)
 - Email (77, △ 12)
 - Mobile (3)
 - Proxy (168)
 - Storage.Backup (164, △ 16)
 - VoIP (24)
 - Cloud.IT (47, △ 1)
 - Game (84) (3)
 - Network.Service (330)
 - Remote.Access (86)
 - Update (49)
 - Web.Client (24)
 - Collaboration (260, △ 16)
 - General.Interest (226, △ 7)
 - P2P (56)
 - Social.Media (115, △ 32)
 - Video.Audio (155, △ 16)
 - Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides:

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

1 2 3



Security Profiles > Application Control

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

Categories:

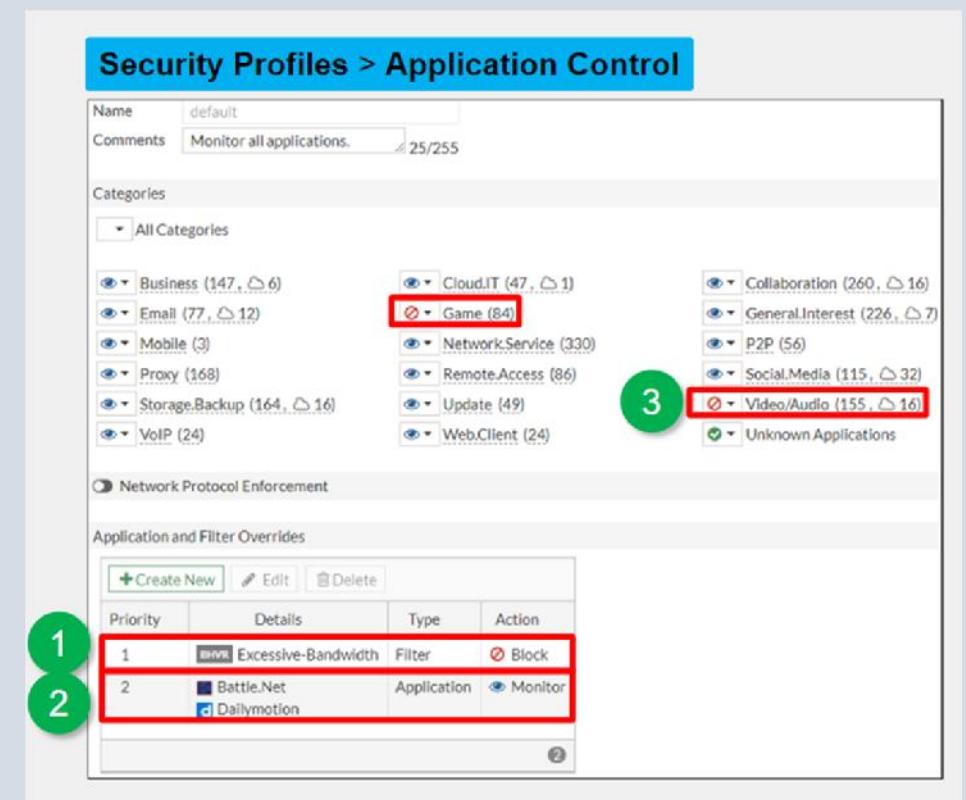
- All Categories
 - Business (147, △ 6)
 - Email (77, △ 12)
 - Mobile (3)
 - Proxy (168)
 - Storage.Backup (164, △ 16)
 - VoIP (24)
 - Cloud.IT (47, △ 1)
 - Game (84) (3)
 - Network.Service (330)
 - Remote.Access (86)
 - Update (49)
 - Web.Client (24)
 - Collaboration (260, △ 16)
 - General.Interest (226, △ 7)
 - P2P (56)
 - Social.Media (115, △ 32)
 - Video.Audio (155, △ 16)
 - Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides:

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

1 2 3



Contrôle d'application

Contrôle d'application

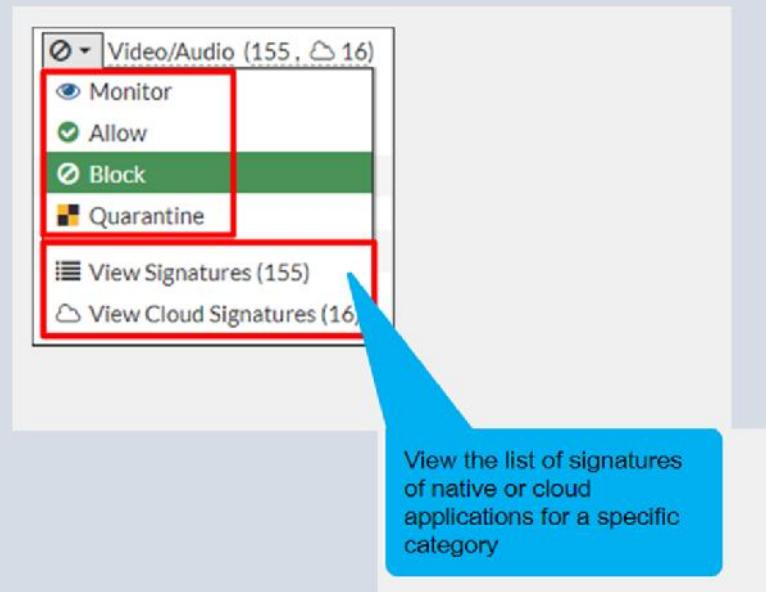
Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Actions:

- Allow: Autorise le trafic d'une application et ne journalise pas;
- Monitor: Autorise le trafic et journalise;
- Block: Ignore le trafic et journalise;
- Quarantine: Bloque le trafic et journalise.



Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Application d'un profil de contrôle d'application:

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. On the left, under 'Security Profiles', the 'Application Control' section is highlighted with a red box. It shows 'default' selected from a dropdown menu. Below it, 'SSL Inspection' is also highlighted with a red box, showing 'ssl deep-inspection' selected from another dropdown. A red arrow points from the 'SSL Inspection' dropdown to a detailed view of the 'ssl deep-inspection' profile on the right. A blue speech bubble above the profile says: 'Use deep-inspection profile to scan encrypted traffic'. The detailed view shows the 'ssl deep-inspection' profile selected (highlighted in yellow), along with other profiles: 'certificate-inspection', 'custom-deep-inspection', 'no-inspection', and 'deep-inspection'.

Profile Type	Profile Name
SSL	deep-inspection
SSL	certificate-inspection
SSL	custom-deep-inspection
SSL	deep-inspection
SSL	no-inspection

Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Application d'un profil de contrôle d'application: Mode NGFW-Policy Based

Policy & Objects > Security Policy

New Policy

Name: Internet Access
Incoming Interface: port3
Outgoing Interface: port1
Source: LOCAL_SUBNET
Destination: all
Schedule: always
Service: App Default
Application: YouTube
URL Category:
Action: ✓ ACCEPT / DENY

Select Entries

Application Category Group

Search

FIREWALL APPLICATION (8)
Social Media (1)
YouTube_Messenger
YouTube
YouTube_Downloader.YTD
YouTube_Comment.Posting
YouTube_HD.Streaming
YouTube_Search.Safety.Mode.Off
YouTube_Search.Video
YouTube_Video.Embedded

Business
Cloud.IT
Collaboration
Email
Game
General.Interest
Mobile
Network.Service
P2P
Proxy
Remote.Access
Social.Media
Storage.Backup
Unknown Applications
Update
Video/Audio
VoIP
Web.Client

New Application Group

Group Name: High Bandwidth
Type: Application
Members: Dailymotion, YouTube
Comments: Write a comment... 0/255

Contrôle d'application

Contrôle d'application

Configuration (suite)

Journalisation&Supervision

Bonnes pratiques

Allocation de bande passante

- Application;
- Catégorie d'application;
- Groupe d'application.

Policy & Objects > Traffic Shaping > Traffic Shaping Policies

New Traffic Shaping Policy

Name: Control Streaming Traffic
Status: Enabled
Comments: Write a comment... 0/255

If Traffic Matches:

Source: all
Destination: all
Schedule: ALL
Service: ALL
Application: Dailymotion, Twitch, YouTube
URL Category: (highlighted with a red box)

Then:

Action: Apply Shaper, Assign Shaping Class ID
Outgoing Interface: port2
Shared shaper: shared-1M-pipe
Reverse shaper: medium-priority
Per-IP shaper: Limited-10-sessions

Select Entries:

Application	Category	Group
FIREWALL APPLICATION (2,121)		
Business (153)		
Acronis.Snap.Deploy	Act!	
ActiveCampaign		
ActiveCampaign_File.Upload	ADP	
AirWatch.MDM		
Alibaba		
Apache.Cassandra		
Applane.CRM		
Atlassian.JIRA		
AutoDesk.360		
AutoDesk.360_Uplod		
Autodesk.BIM360		
Autodesk.Buzzsaw		
Baidu.PC.Faster		
BambooHR		
BambooHR_File.Download		
BambooHR_File.Upload		
Base.CRM		
Blinksale		
Brightpearl		

Contrôle d'application

Contrôle d'application

Configuration

Journalisation&Supervision

Bonnes pratiques

Journalisation

ID	Name	Source	Destination	Schedule	Service	Applications	Action	Security Rules	Log
port3 → port1 4									
1	Blocking apps	all	all	always	App Default	Facebook Flickr Instagram Pinterest	DENY		All
2	Allow social media	all	all	always	App Default	Social.Media	ACCEPT	default	All
3	Blocking P2P Apps	all	all	always	App Default	P2P	DENY		Disabled
4	Allow all	all	all	always	App Default		ACCEPT	default	UTM

All attempts to access these applications are blocked and logged

Access to P2P applications are blocked; however attempts are not be logged

Contrôle d'application

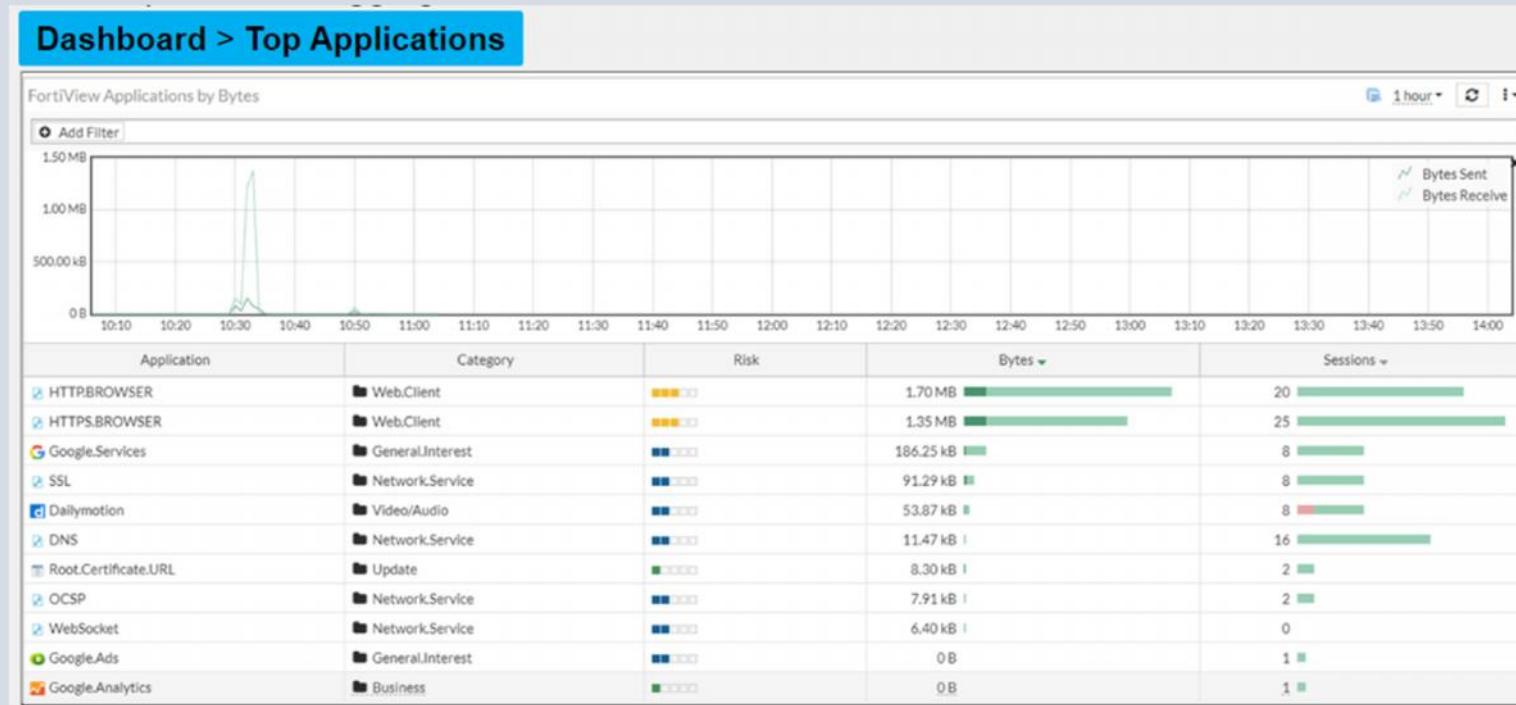
Contrôle d'application

Configuration

Journalisation&Supervision (suite)

Bonnes pratiques

Journalisation



Contrôle d'application

Contrôle d'application

Configuration

Journalisation&Supervision

Bonnes pratiques

Quelques bonnes pratiques

- ❑ Appliquer les profils de contrôle d'application uniquement sur les trafics nécessaires;
- ❑ Si nécessaire, appliquer le même profil d'application sur les connexion internet redondante;
- ❑ Sélectionner le mode d'inspection Deep-inspection au lieu de Certificat-based comme méthode d'inspection SSL/SSH;
- ❑ Utiliser un compte FortiCloud pour sauvegarder et consulter les évènements FortiView;

Contrôle d'application

Contrôle d'application

Configuration

Journalisation&Supervision

Bonnes pratiques

Troubleshooting

❑ Problème de mise à jour:

- ❑ Vérification de l'état de la connexion;
- ❑ Vérification de la résolution;
- ❑ Vérification du port 443;
- ❑ Forcer la vérification de la mise à jour: execute update-now

❑ Vérification de la BD de signature.

System > FortiGuard		
License Information		Status
Entitlement	Status	
FortiCare Support	Registered	<input type="button" value="Actions"/>
FortiCloud Account	Advanced hardware (Expiration Date: 2023/01/18)	
Hardware Version	24x7 support (Expiration Date: 2023/01/18)	
Enhanced Support	Valid	
Virtual Machine	100% 1 / 1	<input type="button" value="FortiGate VM License"/>
Allocated vCPUs	2 GiB	
Allocated RAM		

Antivirus

Objectifs

- Comprendre les bases de la fonctionnalité;
- Identifier les modes de scans;
- Configurer la fonctionnalité antivirus;
- Bonnes pratiques

ANTIVIRUS

Antivirus

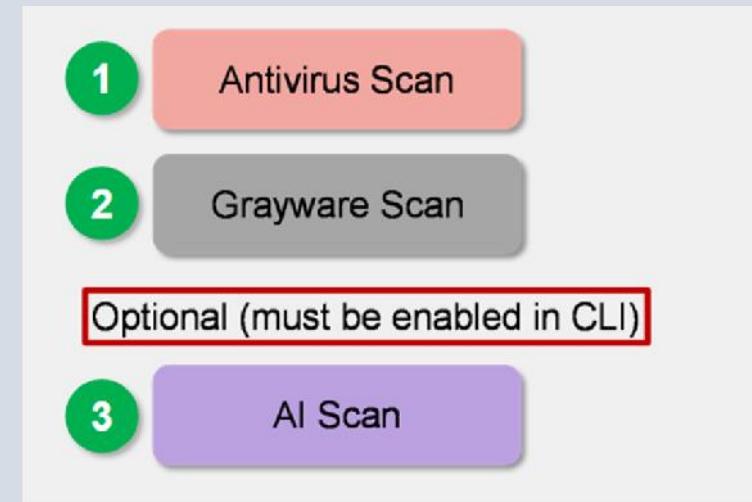
Fonctionnalité Antivirus

- Nécessite une licence;
- Identification/détection de virus;
- Utilisation la correspondance de modèle appelé signature;
- Signature et moteur de détection varient en fonction des fournisseurs:
 - MD5;
 - CRC;
 - Clé de chiffrements;
 - Code;
 - Etc.
- Technique de Scan:
 - Antivirus;
 - Grayware
 - IA

Modes de Scan

Configurations

Bonnes pratiques



ANTIVIRUS

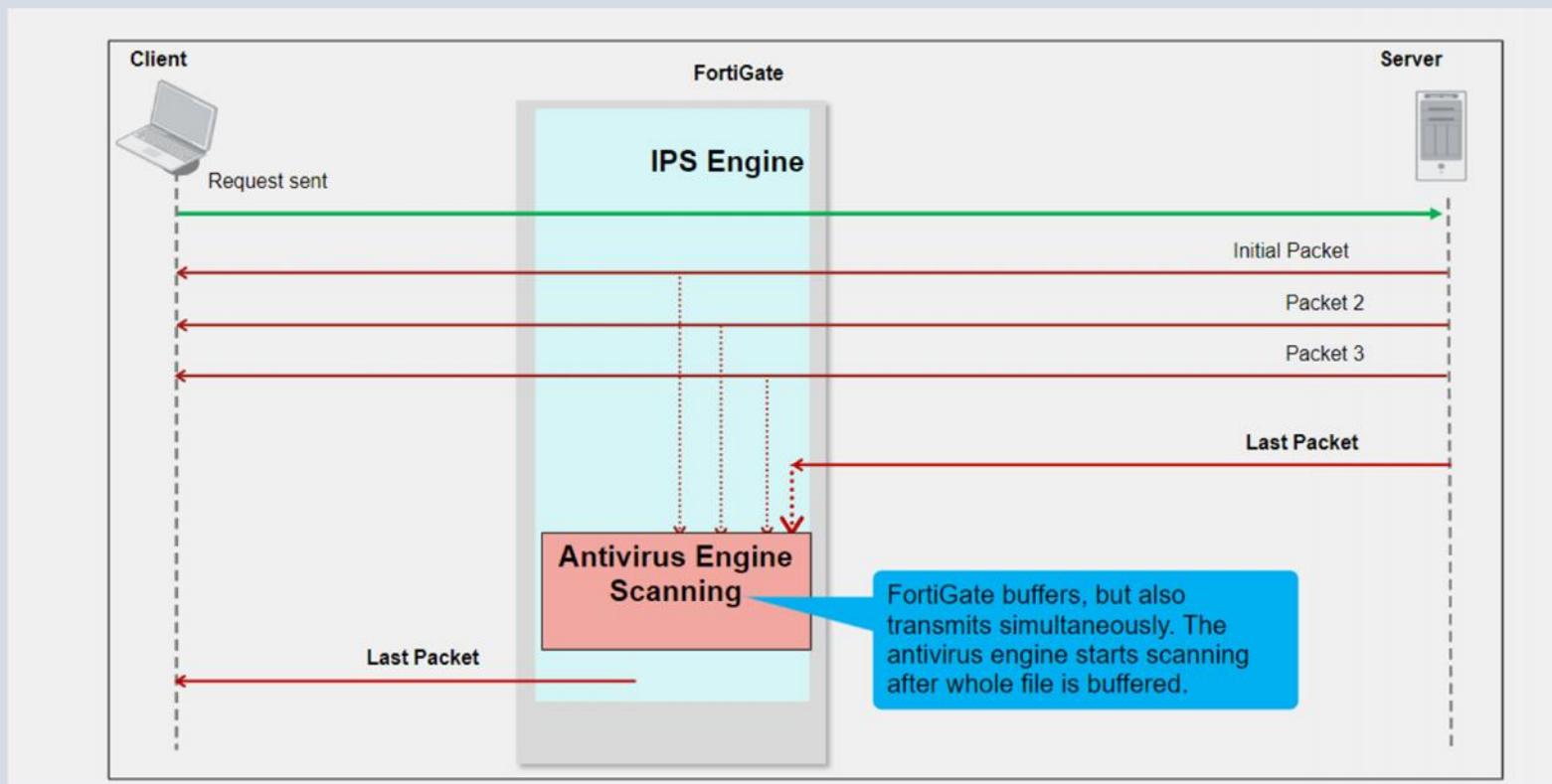
Antivirus

Modes de Scan

Configurations

Bonnes pratiques

Flow-based



ANTIVIRUS

Antivirus

Modes de Scan (suite)

Configurations

Bonnes pratiques

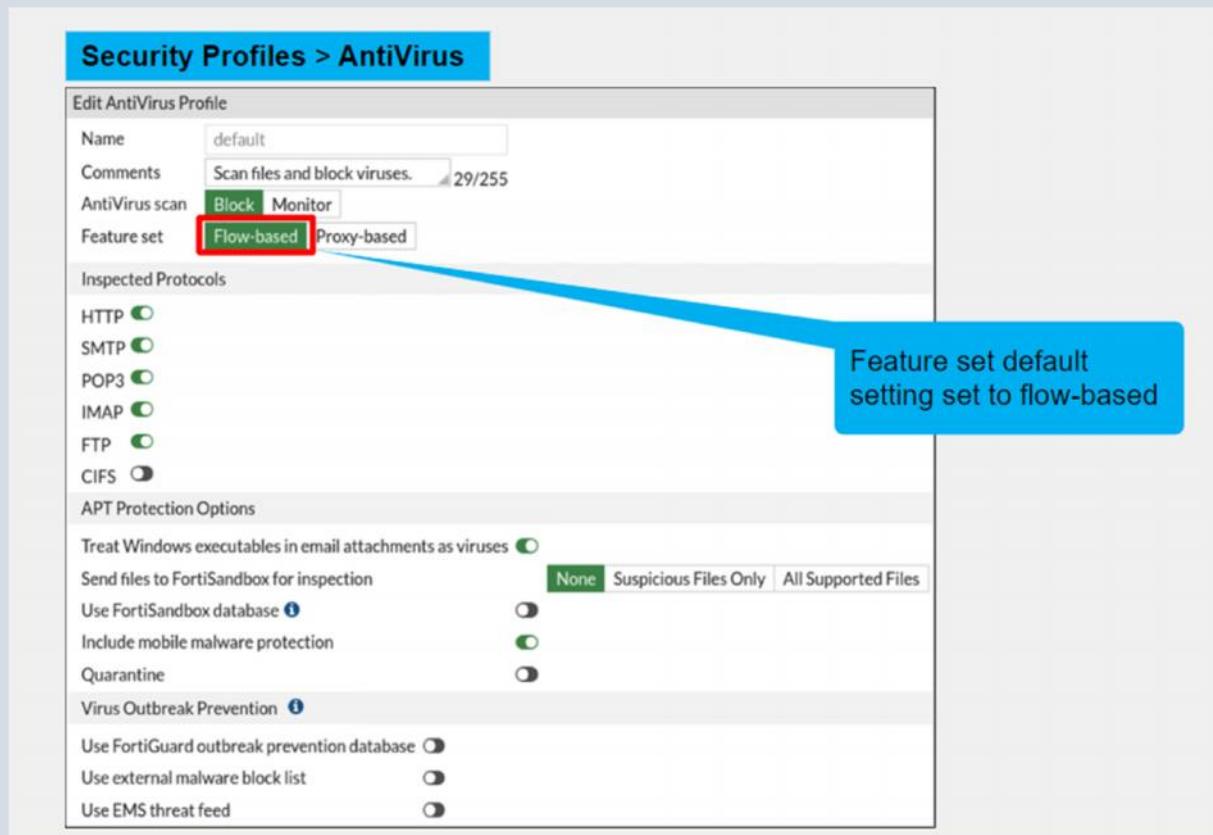
Flow-based

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default
Comments: Scan files and block viruses. 29/255
AntiVirus scan: Block Monitor
Feature set: Flow-based (highlighted with a red box) Proxy-based
Inspected Protocols:
HTTP (radio button selected)
SMTP (radio button selected)
POP3 (radio button selected)
IMAP (radio button selected)
FTP (radio button selected)
CIFS (radio button unselected)
APT Protection Options:
Treat Windows executables in email attachments as viruses (radio button selected)
Send files to FortiSandbox for inspection: None Suspicious Files Only All Supported Files
Use FortiSandbox database (radio button unselected)
Include mobile malware protection (radio button selected)
Quarantine (radio button unselected)
Virus Outbreak Prevention (radio button unselected)
Use FortiGuard outbreak prevention database (radio button unselected)
Use external malware block list (radio button unselected)
Use EMS threat feed (radio button unselected)

Feature set default setting set to flow-based



ANTIVIRUS

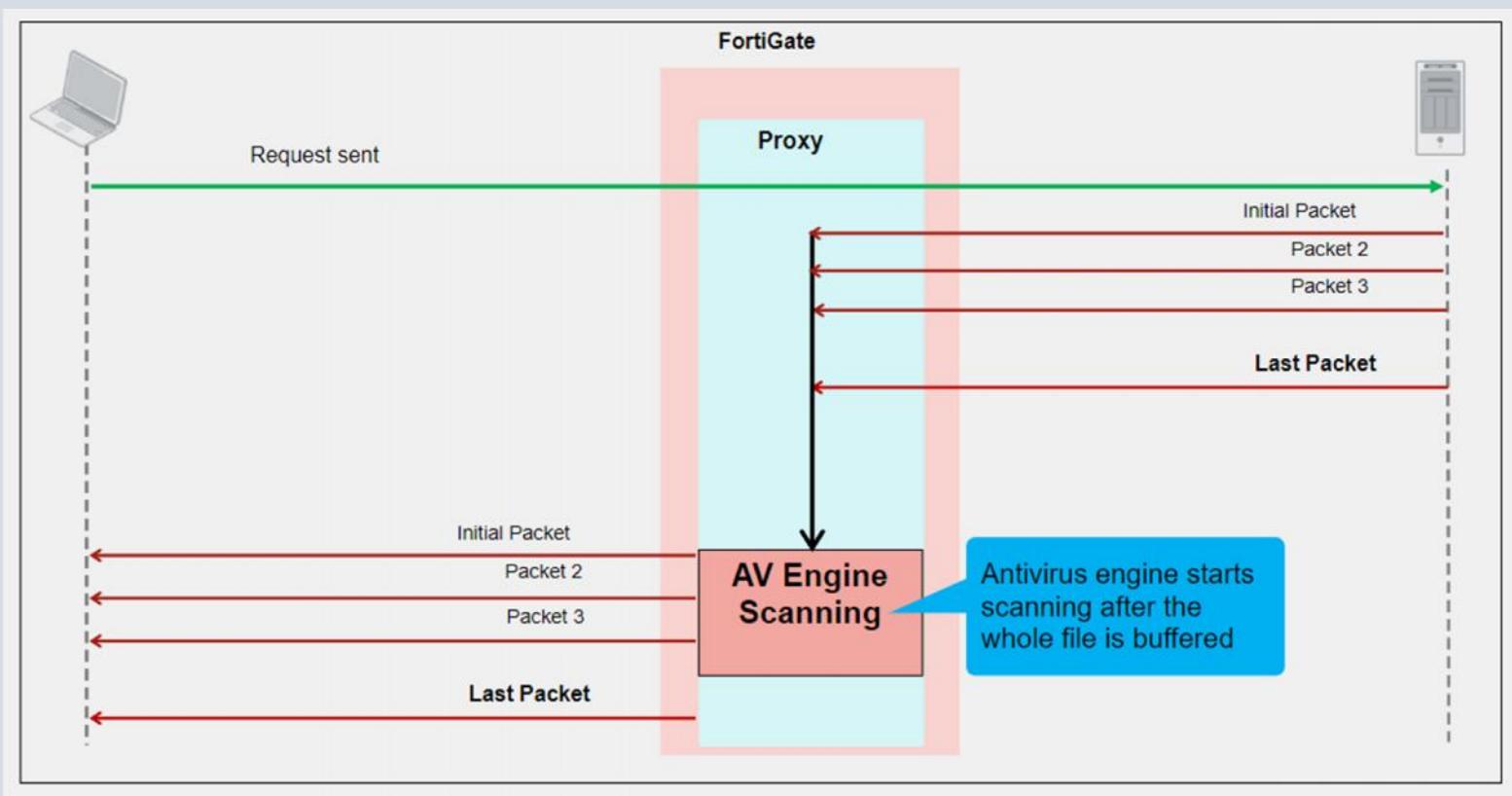
Antivirus

Modes de Scan (suite)

Configurations

Bonnes pratiques

Proxy-based



ANTIVIRUS

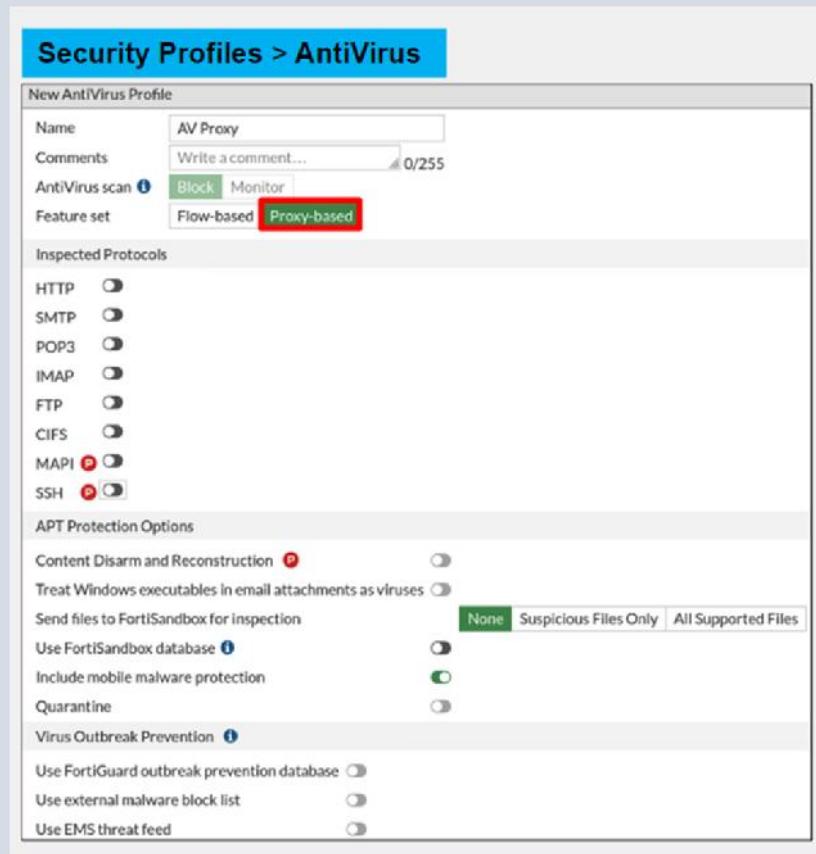
Antivirus

Proxy-based

Modes de Scan (suite)

Configurations

Bonnes pratiques



ANTIVIRUS

Antivirus

Profils

Modes de Scan

Configurations

Bonnes pratiques

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: Block, Monitor

Feature set: Flow-based, Proxy-based

Inspected Protocols:

- HTTP (checked)
- SMTP (checked)
- POP3 (checked)
- IMAP (checked)
- FTP (checked)
- CIFS (unchecked)

APT Protection Options:

- Treat Windows executables in email attachments as viruses (checked)
- Send files to FortiSandbox for inspection (checked)
- Do not submit files matching types (unchecked)
- Do not submit files matching file name patterns (unchecked)
- Use FortiSandbox database (checked)
- Include mobile malware protection (checked)
- Quarantine (unchecked)

Virus Outbreak Prevention:

- Use FortiGuard outbreak prevention database (checked)
- Use external malware block list (checked)
- Use EMS threat feed (unchecked)

Default inspection mode is flow. Inspection mode is now per policy.

FortiSandbox-related options are available only if FortiGate is configured to use FortiSandbox cloud or appliance under Security Fabric.

External malware block list can be enabled if an external threat feed security fabric is configured.

ANTIVIRUS

Antivirus

Profils: Application du profil

Modes de Scan

Configurations (suite)

Bonnes pratiques

Policy & Objects > Firewall Policy

New Policy

Name	Internet access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROT default

Security Profiles

AntiVirus	<input type="checkbox"/> AV default <input type="button" value="edit"/>
Web Filter	<input type="checkbox"/>
DNS Filter	<input type="checkbox"/>
Application Control	<input type="checkbox"/>
IPS	<input type="checkbox"/>
File Filter	<input type="checkbox"/>

SSL Inspection: SSL deep-inspection

Decrypted Traffic Mirror:

ANTIVIRUS

Antivirus

Modes de Scan

Configurations

Bonnes pratiques

Quelques pratiques de configuration recommandées

- ❑ Effectuer les scans antivirus sur tout le trafic internet;
- ❑ Utiliser le mode d'inspection deep-inspection au lieu de certificat-based pour s'assurer d'un meilleur scan;
- ❑ Ne pas augmenter la taille max de fichier à scanner sauf si nécessaire.

ANTIVIRUS

Antivirus

Modes de Scan

Configurations

Bonnes pratiques

Troubleshooting

Problème de mise à jour:

- Vérification de l'état de la connexion;
- Vérification de la résolution;
- Vérification du port 443;
- Forcer la vérification de la mise à jour: execute update-av

Vérification de la licence

System > FortiGuard

AntiVirus	Licensed (Expiration Date: 2023/01/20)
AV Definitions	Version 85.00732
AV Engine	Version 6.00258
Mobile Malware	Version 85.00732

IPS&DOS

Objectifs

- Configurer les IPS;
- Configurer les DoS;
- Configurer les WAF (Web Firewall Application);
- Bonnes pratiques.

IPS&DOS

IPS

DOS

WAF

Bonnes pratiques

IPS

- Mode de détection et de blocage des anomalies ou des exploits;
- Composants principaux:
 - DB de signature;
 - Décodeurs de protocole;
 - Moteur IPS::
 - Control d'application;
 - Antivirus;
 - Filtre web
 - Etc.



IPS&DOS

IPS (suite)

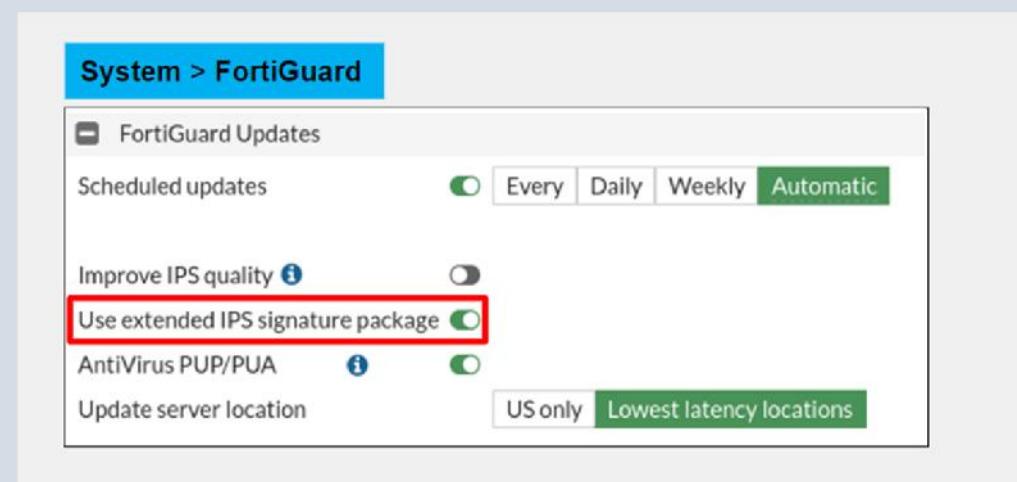
DOS

WAF

Bonnes pratiques

IPS: BD de signatures

- ❑ Régulière: contient les signatures des attaques communes ;
- ❑ Etendu: contient des signatures additionnelles.



IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Liste de signatures

Security Profiles > Intrusion Prevention

Edit IPS Sensor

Name: default
Comments: Prevent critical attacks. 25/255
Block malicious URLs:

IPS Signatures and Filters

+ Create New | Edit | Delete

Details	Exempt IPs	Action	Packet Logging
SEV: ■■■■■		<input checked="" type="radio"/> Default	<input type="radio"/> Disabled
SEV: ■■■■■			
SEV: ■■■■■			

Botnet C&C
Scan Outgoing Connections to Botnet Sites:

IPS Signatures

View IPS Signatures

Default action

Additional Information

Severity: 13995 Total (High: 0%, Critical: 0%, Medium: 100%, Low: 0%, Information: 0%)

Target: 17733 Total (Server: 50%, Client: 50%)

OS: 23023 Total (Windows: 50%, Linux: 25%, MacOS: 10%, All: 5%, BSD: 5%, Solaris: 5%)

Active signature database

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature (13,995)					
2Wire.Wireless.Router.XSRF.Password.Reset	■■■■■	Server Client	Linux	<input checked="" type="checkbox"/> Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.File...	■■■■■	Server	Windows	<input checked="" type="checkbox"/> Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■■	Server	Windows	<input checked="" type="checkbox"/> Block	CVE-2005-0277

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Configuration des capteurs IPS

Security Profiles > Intrusion Prevention

New IPS Sensor

Name: IPS profile

Comments: Write a comment... 0/255

Block malicious URLs:

IPS Signatures and Filters:

+ Create New

Details	Exempt IPs	Action	Packet Logging
No results			

0

Add Signatures

Type: Signature **Filter**

Action: Default Enable Disable

Packet logging: Enable Disable

Status: Enable Disable Default

Filter: **+**

Name	Severity	Target	OS	Action	CVE-ID
74CM5.Config.Controller.Remote.Code.Execu...	██████	Server	Windows	<input type="checkbox"/> Block	CVE-2019-10684

Add Signatures

Type: Signature **Filter**

Action: Default Enable Disable

Packet logging: Enable Disable

Status: Enable Disable Default

Rate-based settings: **Specify**

Exempt IPs: **Edit IP Exemptions**

Add All Results **Search** **Selected** **All**

Name	Severity	Target	OS	Action	CVE-ID
2Wire.Wireless.Router.XSRF.Password.Reset	██████	Server Client	Linux	<input type="checkbox"/> Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.FL...	██████	Server	Windows	<input type="checkbox"/> Block	
3Com.3CDaemon.FTPServer.Buffer.Overflow...	██████	Server	Windows	<input type="checkbox"/> Block	CVE-2005-0277
3Com.3CDaemon.FTPServer.Information.D...	██████	Client	Windows	<input type="checkbox"/> Block	CVE-2005-0278
3Com.Intelligent.Management.Center.Infor...	██████	Server	Windows	<input type="checkbox"/> Block	

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Exclusion des adresses

The screenshot shows two windows from the FortiOS interface:

Security Profiles > Intrusion Prevention

IPS Signatures and Filters

	Details	Exempt IPs	Action	Packet Logging
3Com.3CDaemon.FTP.Server.Information.Disclosure	1		<input checked="" type="radio"/> Monitor <input type="radio"/> Default	<input checked="" type="checkbox"/> Disabled <input type="checkbox"/> Disabled
TGT	Server			
SEV	■■■■■			
SEV	■■■■■			
OS	Windows			

A red box highlights the number '1' in the 'Exempt IPs' column, and a red arrow points down to the 'Edit IP Exemptions' window.

Edit IP Exemptions

Source IP/Netmask	Destination IP/Netmask
10.0.1.10/32	0.0.0.0/0

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Actions

Security Profiles > Intrusion Prevention						
Add Signatures						
Type	Filter	Signature	Action	Packet logging	Status	Filter <small>i</small>
	<input checked="" type="radio"/> Default		<input checked="" type="radio"/> Allow	Disable	<input checked="" type="radio"/> Monitor	<input checked="" type="radio"/> Default
			<input type="radio"/> Block	Disable	<input type="radio"/> Reset	<input type="radio"/> Default
			<input type="radio"/> Quarantine	+ <input type="text"/>	<input type="button" value="Search"/>	<input type="button" value=""/>
			Severity <small>▼</small>	Target <small>▼</small>	OS <small>▼</small>	Action <small>▼</small>
IPS Signature <small>13,995</small>						CVE-ID <small>▼</small>
2Wire.Wireless.Router.XSRF.Password.Reset			Server Client	Linux	<input type="radio"/> Block	CVE-2007-4387
3CX.Phone.System.VAD_Deploy.Arbitrary.File...			Server	Windows	<input type="radio"/> Block	
3Com.3CDaemon.FTP.Server.Buffer.Overflow			Server	Windows	<input type="radio"/> Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Dis...			Client	Windows	<input type="radio"/> Block	CVE-2005-0278

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Botnet

Security Profiles > Intrusion Prevention

Edit IPS Sensor

Name: high_security

Comments: Blocks all Critical/High /Medium and some Low severity vulnerabilities 69/255

Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
SEV: ■■■■□		<input checked="" type="radio"/> Block	<input checked="" type="radio"/> Disabled
SEV: ■■■■■□			
SEV: ■■■■■■			
SEV: ■■■■■■		<input checked="" type="radio"/> Default	<input checked="" type="radio"/> Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites Disable Block Monitor

The screenshot shows the 'Edit IPS Sensor' configuration for a profile named 'high_security'. It includes a comments section stating 'Blocks all Critical/High /Medium and some Low severity vulnerabilities' with a character count of 69/255. A 'Block malicious URLs' checkbox is checked. The 'IPS Signatures and Filters' section contains a table with four rows for different severity levels (SEV). The first row (yellow) has 'Block' checked and 'Disabled' selected. The second (orange), third (red), and fourth (blue) rows have 'Default' checked and 'Disabled' selected. A red box highlights the 'Scan Outgoing Connections to Botnet Sites' button at the bottom.

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Application du profil

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. In the 'Security Profiles' section, the 'IPS' profile is selected and highlighted with a red box. A tooltip says: 'Add IPS sensors as security profiles to firewall policies'. Below it, the 'SSL Inspection' profile is shown. In the 'Logging Options' section, the 'All Sessions' checkbox is selected and highlighted with a red box. A tooltip says: 'Enable this option to log all sessions including blocked and allowed traffic'.

Policy & Objects > Firewall Policy

Security Profiles

- AntiVirus
- Web Filter
- Video Filter
- DNS Filter
- Application Control
- IPS IPS protect_client ▼ ✎**
- File Filter
- SSL Inspection SSL certificate-inspection ▼ ✎

Logging Options

- Log Allowed Traffic Security Events All Sessions
- Generate Logs when Session Starts
- Capture Packets

IPS&DOS

IPS (suite)

DOS

WAF

Bonnes pratiques

IPS: Journaux

Log & Report > Intrusion Prevention								
Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
3 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
13 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
23 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
33 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
43 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
53 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
Minute ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
Minute ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
Minute ago			10.200.1.254	6		dropped		PHP.URI.Code.Injection
Minute ago			10.200.1.254	6		dropped		PHP.URI.Code.Injection
Minute ago			10.200.1.254	6		dropped		HTPasswd.Access
Minute ago			10.200.1.254	6		dropped		HTPasswd.Access
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force
23 hours ago			10.0.1.10	6		reset		FTP.Login.Brute.Force

IPS&DOS

IPS

DOS

WAF

Bonnes pratiques

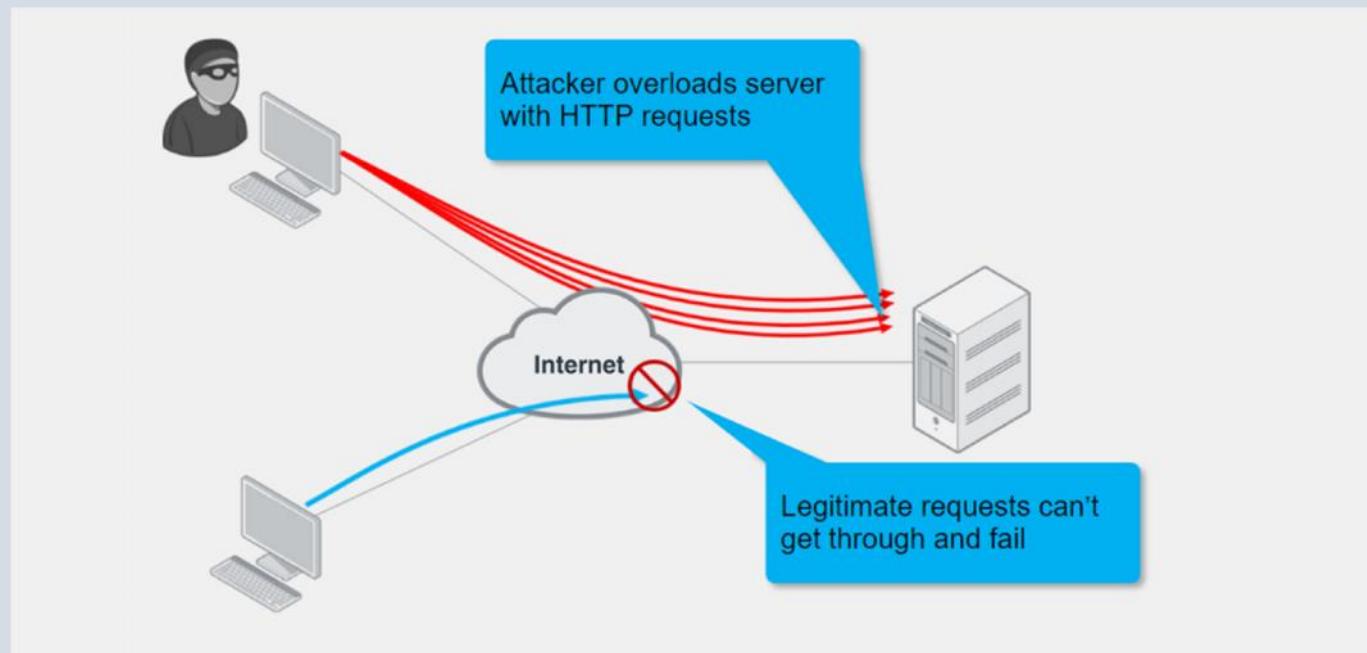
DoS

- Ralentir ou mettre hors service un système en consommant toute ses ressources

dispo

- Types:

- TCP SYN flood;
- ICMP sweep;
- TCP port scan;
- DoS Distribués;
- Etc.



IPS&DOS

IPS

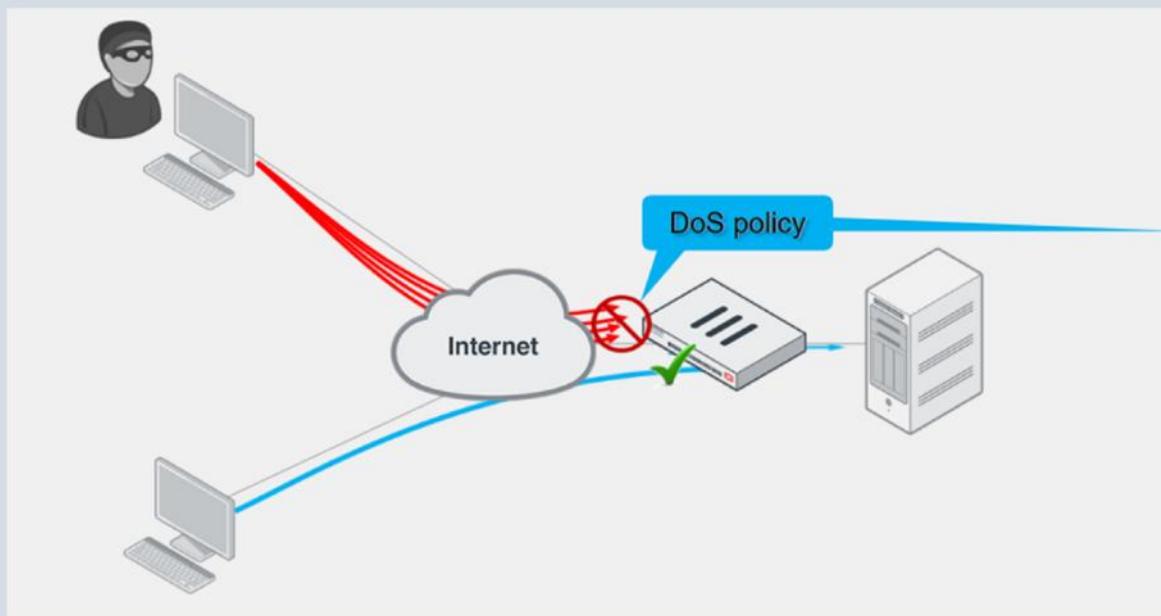
DOS (suite)

WAF

Bonnes pratiques

DoS: Politiques

- Appliquer au début du processus de traitement du paquet;
- Peuvent être appliquer sur les interfaces physiques ou logiques
- Plusieurs capteurs peuvent détecter différents anomalies



Policy & Objects > IPv4 DoS Policy

Name	Logging	Action	Disable	Block	Monitor	Threshold
ip_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
ip_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000

L3 Anomalies

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
tcp_port_scan	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		1000
tcp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
tcp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
udp_scan	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
udp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
udp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000

L4 Anomalies

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
tcp_port_scan	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		1000
tcp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
tcp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
udp_scan	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		2000
udp_src_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000
udp_dst_session	<input type="checkbox"/>	<input checked="" type="button" value="Disable"/>	<input type="button" value="Block"/>	<input type="button" value="Monitor"/>		5000

IPS&DOS

IPS

DOS (suite)

DoS: Configuration des Politiques

- ❑ Flood: détection d'un volume important du même type de trafic;
- ❑ Sweep/scan: détection des tentatives de sondes;
- ❑ Source(SRC): détection d'un volume important de trafic en provenance d'une IP spécifiques;
- ❑ Destination (DST): détection d'un volume de trafic important en destination d'une IP spécifiques.

WAF

Bonnes pratiques

The screenshot shows the 'Policy & Objects > IPv4 DoS Policy' configuration screen. It includes sections for 'New Policy' and two tabs for 'L3 Anomalies' and 'L4 Anomalies'.
New Policy:

Name	DoS_Policy_2
Incoming Interface	port1
Source Address	all
Destination Address	all
Service	ALL

L3 Anomalies:

Name	Logging	Action	Disable	Block	Monitor	Threshold
ip_src_session	On	Disable	Block	Monitor		5000
ip_dst_session	On	Disable	Block	Monitor		5000

L4 Anomalies:

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	On	Disable	Block	Monitor		2000
tcp_port_scan	Off	Disable	Block	Monitor		1000
tcp_src_session	Off	Disable	Block	Monitor		5000
tcp_dst_session	Off	Disable	Block	Monitor		5000
udp_flood	On	Disable	Block	Monitor		2000
udp_scan	Off	Disable	Block	Monitor		2000

IPS&DOS

IPS

DOS (suite)

DoS: Configuration des Politiques

- ❑ Flood: détection d'un volume important du même type de trafic;
- ❑ Sweep/scan: détection des tentatives de sondes;
- ❑ Source(SRC): détection d'un volume important de trafic en provenance d'une IP spécifiques;
- ❑ Destination (DST): détection d'un volume de trafic important en destination d'une IP spécifiques.

WAF

Bonnes pratiques

The screenshot shows the 'Policy & Objects > IPv4 DoS Policy' configuration screen. It includes sections for 'New Policy' and two tabs for 'L3 Anomalies' and 'L4 Anomalies'.
New Policy:

Name	DoS_Policy_2
Incoming Interface	port1
Source Address	all
Destination Address	all
Service	ALL

L3 Anomalies:

Name	Logging	Action	Disable	Block	Monitor	Threshold
ip_src_session	ON	Disable	Block	Monitor		5000
ip_dst_session	ON	Disable	Block	Monitor		5000

L4 Anomalies:

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	ON	Disable	Block	Monitor		2000
tcp_port_scan	OFF	Disable	Block	Monitor		1000
tcp_src_session	OFF	Disable	Block	Monitor		5000
tcp_dst_session	OFF	Disable	Block	Monitor		5000
udp_flood	ON	Disable	Block	Monitor		2000
udp_scan	OFF	Disable	Block	Monitor		2000

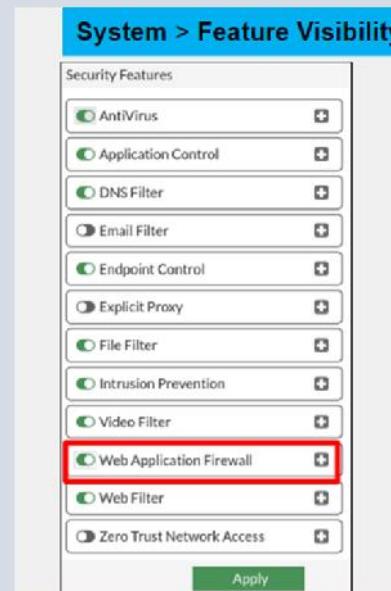
IPS&DOS

IPS

Web Application Firewall (WAF)

- Protection des web services (site web);
- Fonctionnalité par défaut désactivée;
- Disponible uniquement en mode d'inspection proxy

DOS



WAF

The screenshot shows the 'Policy & Objects > Firewall Policy' configuration page. It includes fields for Name (Inbound Access), Incoming Interface (port1), Outgoing Interface (port3), Source (all), Destination (WEB-SERVER01), Schedule (always), Service (ALL), Action (ACCEPT), Inspection Mode (set to 'Proxy-based'), NAT, Protocol Options (PROT default), Security Profiles, and various filter and inspection options. A red box highlights the 'Inspection Mode' field. Another red box highlights the 'Web Application Firewall' section at the bottom, which is set to 'WAF default'. At the bottom right, there is a red arrow pointing from the 'Proxy-based' box in the main configuration to the 'WAF default' box in the detailed settings.

Bonnes pratiques

IPS&DOS

IPS

DOS

WAF (suite)

Bonnes pratiques

WAF: Configuration

The diagram illustrates the configuration flow for a Web Application Firewall (WAF) profile and its application in a firewall policy.

Security Profiles > Web Application Firewall

This section shows the configuration of a WAF profile named "default". It includes:

- Signatures:** A table listing various attack signatures with their status (Enable/Disable), signature name, action (Monitor, Allow, Block), and severity. Examples include Cross Site Scripting, SQL Injection, and Trojans.
- Constraints:** A table listing request constraints with their status (Enable/Disable), constraint name, limit, action (Block, Monitor), and severity. Examples include Content Length, Header Length, and Total URL and Body Parameters Length.
- HTTP Method Policy:** A section for defining HTTP method policies.

Policy & Objects > Firewall Policy

This section shows the configuration of a firewall policy named "Inbound Access". It includes:

- Source:** All
- Destination:** WEB-SERVER01
- Schedule:** always
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based
- Firewall / Network Options:** NAT (disabled), Protocol Options (PROT default), Security Profiles (selected).
- IPS:** IPS WEB SERVER (selected)
- Web Application Firewall:** WAF default (selected)
- SSL Inspection:** certificate-inspection

IPS&DOS

IPS

DOS

WAF

Bonnes pratiques

Bonne pratiques: Implémentation

- Analyse des exigences
- Application des IPS sur des politiques nécessaires;
- Eviter d'appliquer les IP sur les règles de trafic de type internal-to-internal.
- Création des capteurs spécifiquement pour les ressources à protéger;
- Maintien continual des IPS
- Revue des logs;
- Personnalisation des IPS sur la base des observations.
- Utilisation du l'inspection SSL approfondie pour bénéficier pleinement des IPS;

IPS&DOS

IPS

Diagnostic: FortiGuard IPS

- Vérification du port 443;
- Vérification du status en GUI;
- Vérification du status en CLI.

DOS

WAF

Bonnes pratiques (suite)

System > FortiGuard

Intrusion Prevention	IPS Definitions	Actions
<input checked="" type="checkbox"/> Version 18.00052	<input checked="" type="radio"/> Version 7.00018	<input type="button" value="View List"/>
<input checked="" type="checkbox"/> Version 7.00018	<input checked="" type="radio"/> Version 2.00970	<input type="button" value="View List"/>
<input checked="" type="checkbox"/> Version 2.00970	<input checked="" type="radio"/> Version 7.01436	<input type="button" value="View List"/>
<input checked="" type="checkbox"/> Version 7.01436	<input checked="" type="radio"/> Version 2.00721	<input type="button" value="View List"/>
<input checked="" type="checkbox"/> Version 2.00721		

```
# diagnose debug application update -1
# diagnose debug enable
# execute update-now
```

After enabling real-time debugging, force a manual update of all FortiGuard packages

IPS&DOS

IPS

DOS

WAF

Bonnes pratiques (suite)

Diagnostic: Forte utilisation du CPU

```
# 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
```

Shuts down IPS engine completely

IPS engine remains active, but does not inspect traffic

FORTINET®

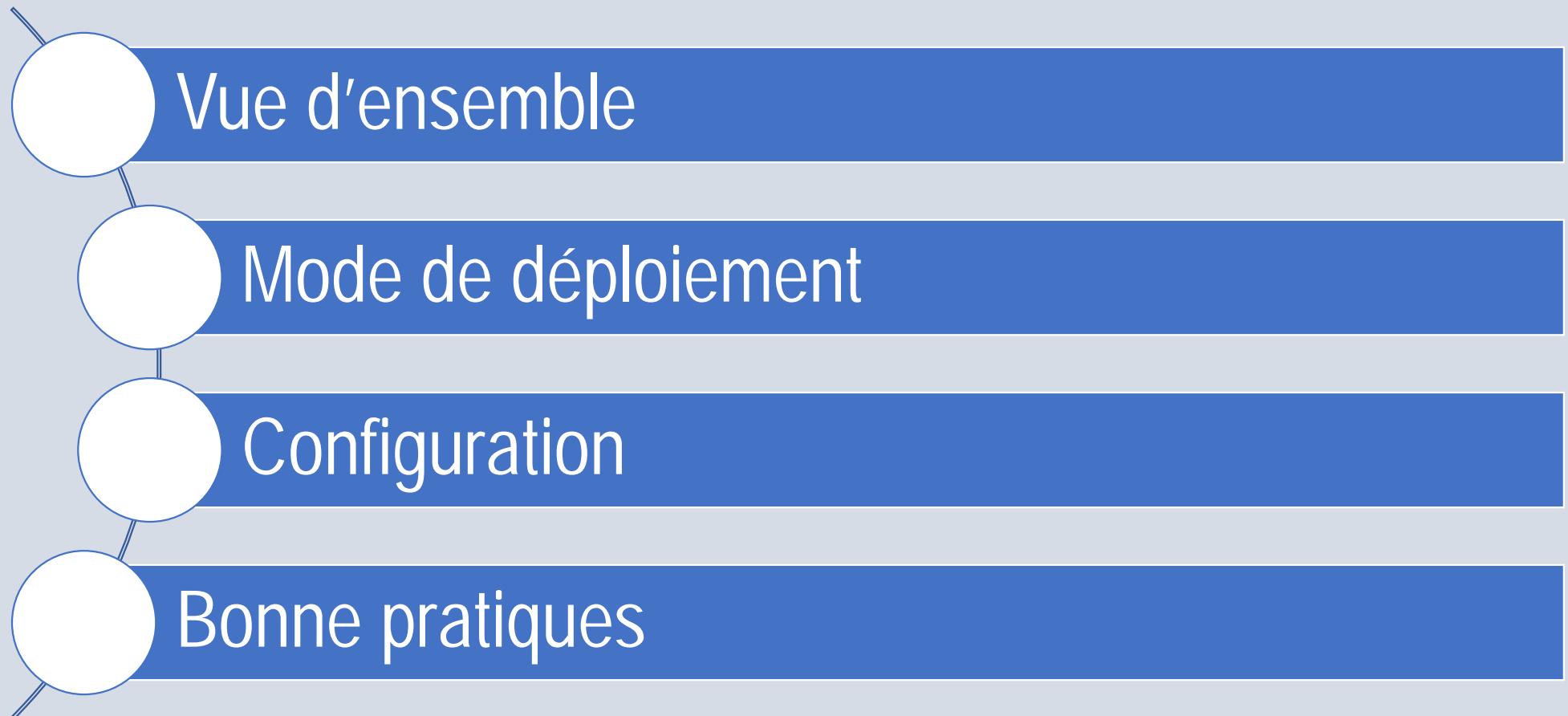


FortiGate Security

VIRTUAL PRIVATE NETWORK (VPN)



Plan du module



Vue d'ensemble

Objectifs

- Définir VPN;
- Décrire les différents type de VPN; SSL, IPSec et ZTNA.

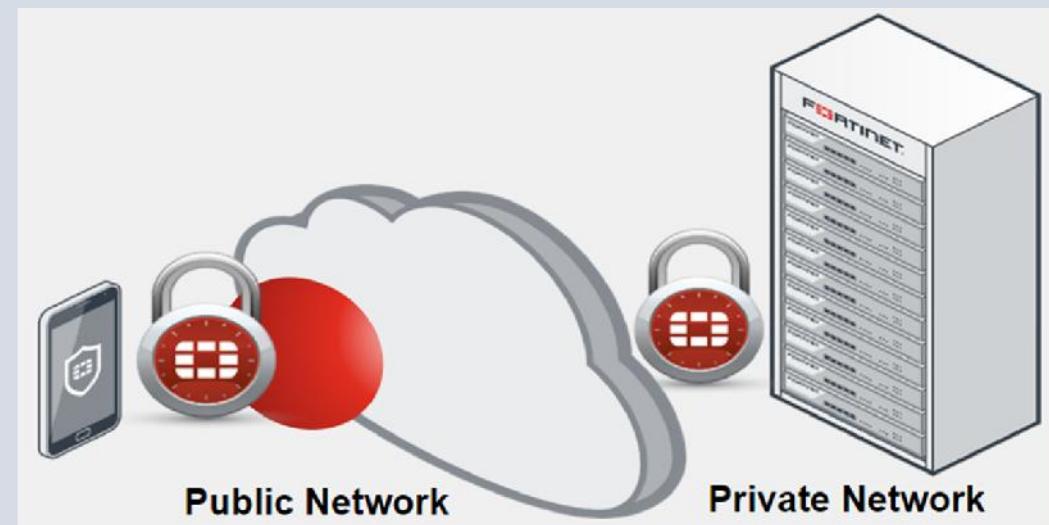
Vue d'ensemble

VPN

TYPES DE VPN

Généralités

- ❑ Extension du réseau privé à travers un réseau public (Internet);
- ❑ Sécurisation des connexions distantes au LAN ou aux équipements:
 - ❑ Employés;
 - ❑ Succursales.
- ❑ Transmission sécurisée des données privées via Internet:
 - ❑ Chiffré;
 - ❑ Utilisateurs authentifiés uniquement.



Vue d'ensemble

VPN

TYPES DE VPN

Types

	IPsec VPN	SSL VPN	ZTNA
Tunnel type:	IPsec tunnel only	Session-based OR tunnel	Session-based only
Configured between:	FortiClient and FortiGate FortiGate and FortiGate FortiGate and compatible third-party IPsec VPN gateway FortiGate and compatible third-party IPsec VPN clients	Browser and FortiGate FortiClient and FortiGate FortiGate (SSL Client) and FortiGate (SSL Server)	Browser and FortiGate FortiClient and FortiGate (TCP forwarding access)
Log in through:	IPsec client	HTTPS web page on FortiGate FortiClient FortiGate (SSL Client)	HTTPS hostname or IP and port number FortiClient (TCP forwarding access)

Vue d'ensemble

VPN

TYPES DE VPN (suite)

Types

	IPsec VPN	SSL VPN	ZTNA
Category:	Industry standard	Vendor specific	Vendor specific
Configuration:	<ul style="list-style-type: none">Requires installationFlexible setup<ul style="list-style-type: none">Mesh and star topologiesFor clients or peer gatewaysPerformance based: IPsec cryptography is faster in FortiOS	<ul style="list-style-type: none">Does not require installationSimpler setup<ul style="list-style-type: none">Only client-to-FortiGateNo user-configured settingsTechnical support less requested	<ul style="list-style-type: none">Does not require installationSimpler setup<ul style="list-style-type: none">Only client-to-FortiGateNo user-configured settingsTechnical support less requested
Better for:	Office-to-office traffic Data centers	Provides flexibility tunnel-mode or session-based access	Session-based access only

Mode de déploiement

Objectifs

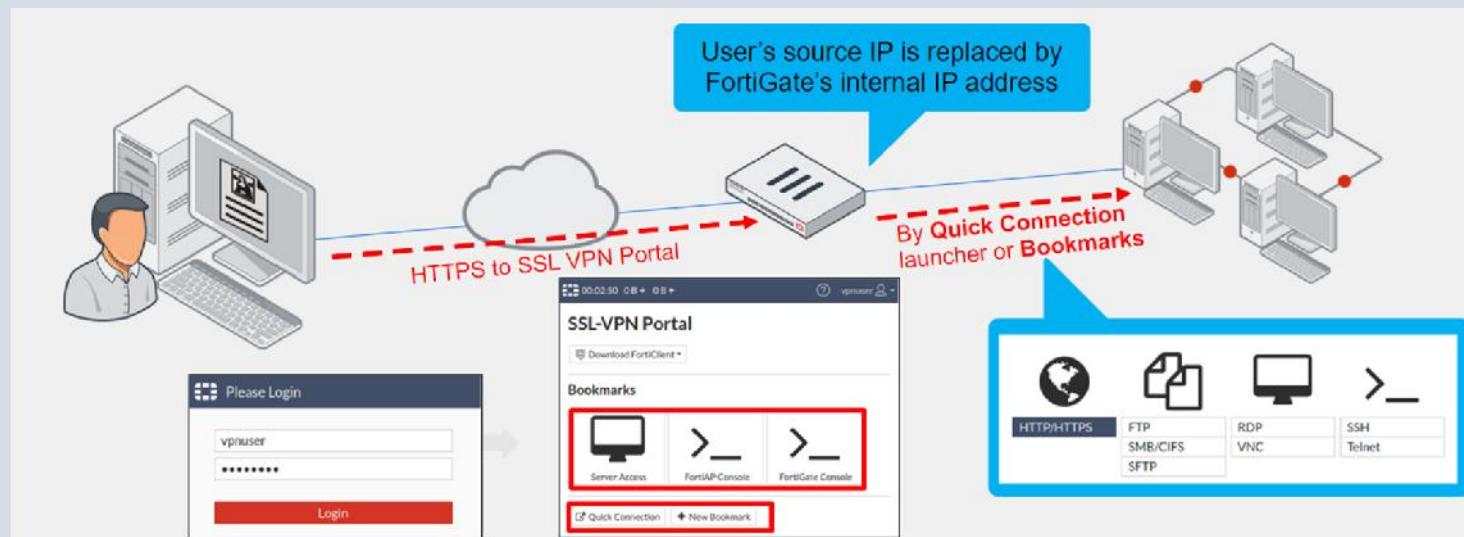
- Décrire les modes de déploiement.

Mode de déploiement

Mode

Mode: Web

- Connexion à un portail SSL
 - Affiche le statut du VPN (ssl);
 - VPN reste actif uniquement lorsque le portail ssl est ouvert

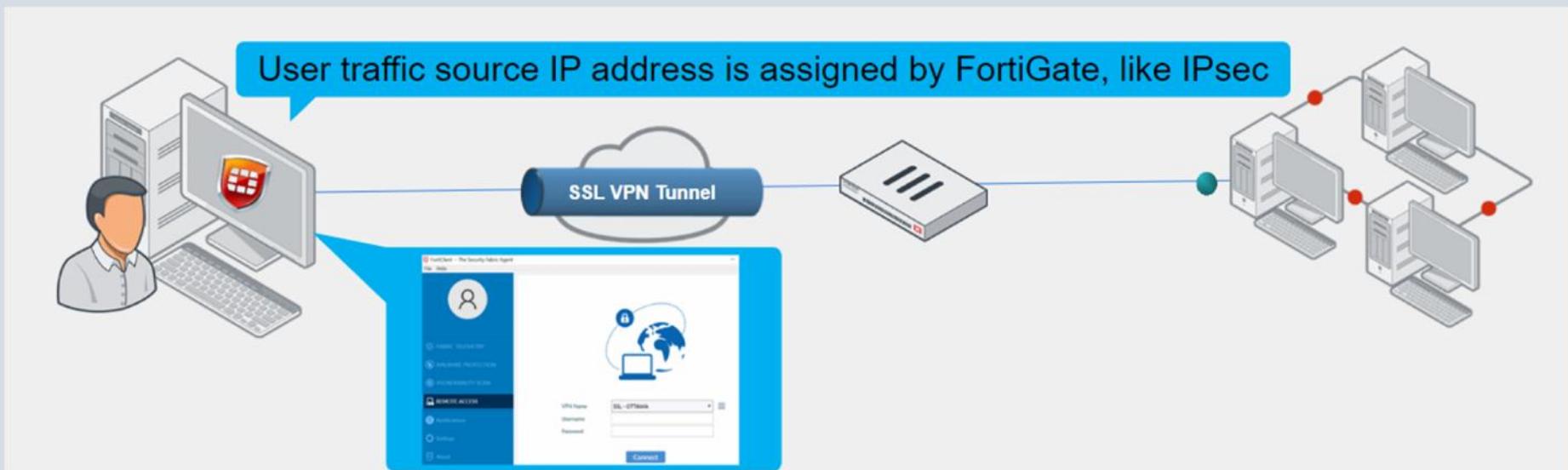


Mode de déploiement

Mode (suite)

Mode: Tunnel

- ❑ Etablissement d'un tunnel pour les échanges
- ❑ Trafic encapsulé dans du SSL/TLS



Configuration

Objectifs

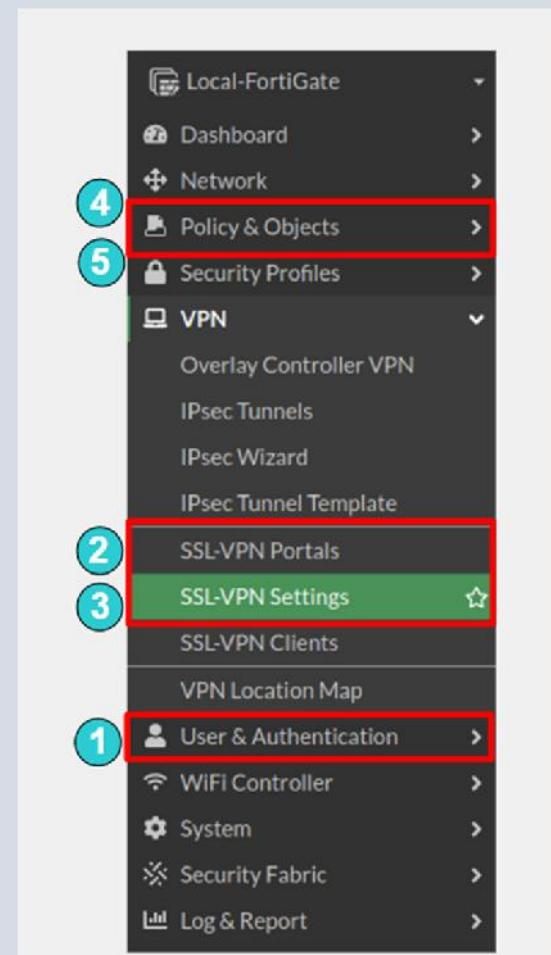
- Configurer un VPN SSL;
- Configurer un VPN IPSEC.

Configuration

SSL

VPN SSL: Utilisateur (client)

- ❑ Création des comptes ou groupes d'utilisateurs pour les utilisateurs distants;
- ❑ Configuration du portail SSL;
- ❑ Configuration des paramètres SSL VPN;
- ❑ Création des profils de sécurité (optionnel);
- ❑ Création des règles de trafic.



IPSec

Configuration

SSL (suite)

IPSec

VPN SSL: Configuration du portail

VPN > SSL VPN Portals

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

Edit SSL-VPN Portal

Name: full-access

Tunnel Mode

Source IP Pools: SSLVPN_TUNNEL_ADDR1

Web Mode

Administrator-defined bookmarks

Bookmark: FortiAP Console (Type: TELNET, Host: 10.0.1.2, Description: Root AP / Mesh-1)

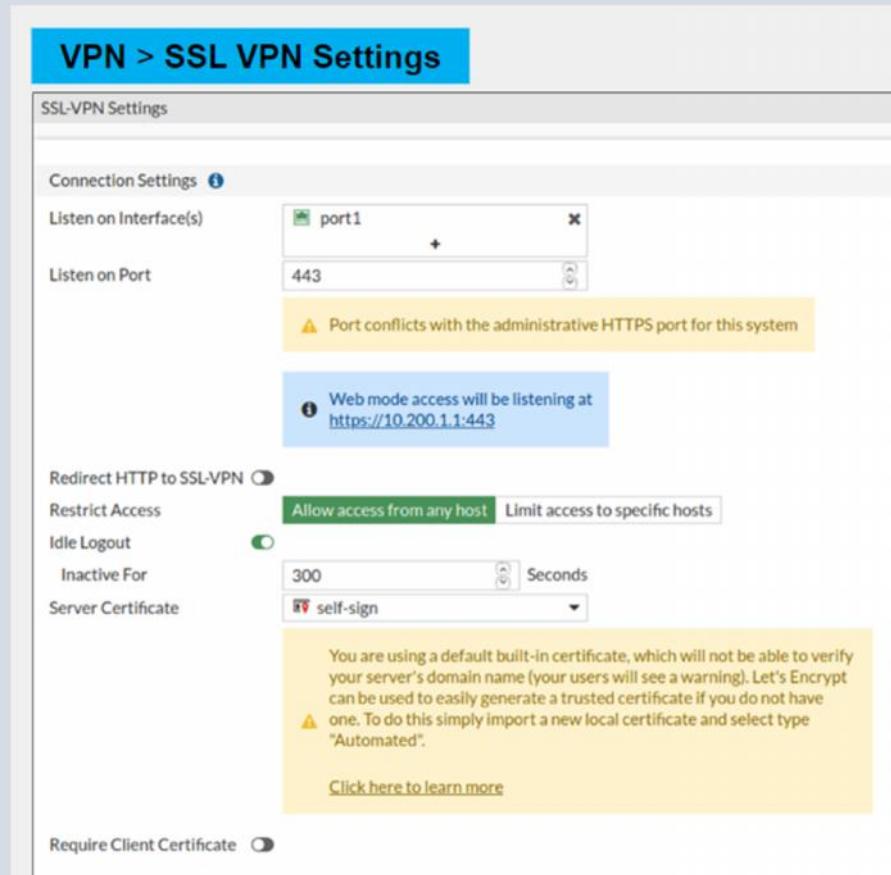
Configuration

SSL (suite)

IPSec

VPN SSL: Configuration des paramètres VPN SSL

- Recommander d'utiliser une interface différente pour le GUI et le portail SSL;
- Restriction de l'accès aux hôtes connus;
- Certificat
 - Utilisation des certificats émis par un CA public ou installation des certificats auto-signés sur tous les clients afin d'éviter les avertissements de sécurité.



Configuration

SSL (suite)

IPSec

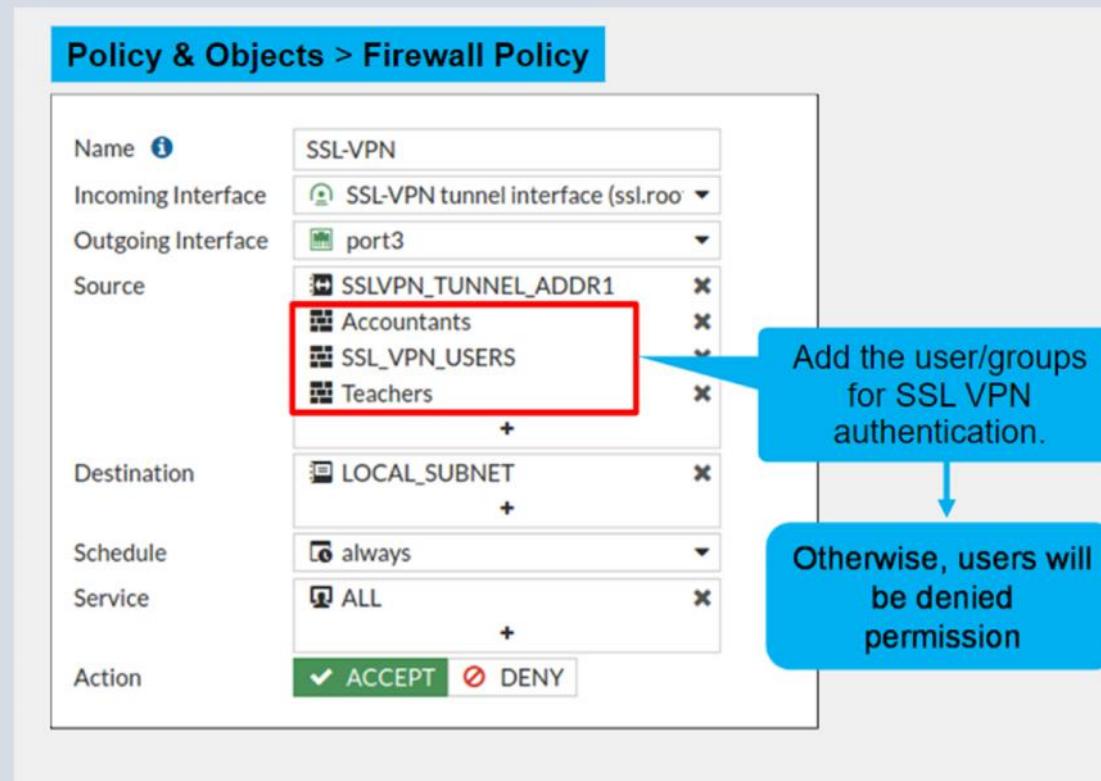
VPN SSL: Configuration des règles de trafic

Policy & Objects > Firewall Policy

Name	SSL-VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.roo...)
Outgoing Interface	port3
Source	SSLVPN_TUNNEL_ADDR1 Accounts SSL_VPN_USERS Teachers
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	✓ ACCEPT ✘ DENY

Add the user/groups for SSL VPN authentication.

Otherwise, users will be denied permission



Configuration

SSL

IPSec

VPN IPSEC

FortiGate 200E FG_ANTC_HQ

VPN Creation Wizard

① VPN Setup > ② Authentication > ③ Policy & Routing

Name: []

Template Type: Site to Site (selected), Remote Access, Custom

Remote Device Type: FortiGate, Cisco

NAT Configuration: No NAT between sites (selected), This site is behind NAT, The remote site is behind NAT

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

< Back | Next > | Cancel

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

- Overlay Controller VPN
- IPsec Tunnels
- IPsec Wizard (selected)
- IPsec Tunnel Templates
- SSL-VPN Portals
- SSL-VPN Settings
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

Configuration

SSL

IPSec (suite)

VPN IPSEC

FortiGate 200E FG_ANTC_HQ

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Remote Device IP Address Dynamic DNS

IP Address 1.1.1.1

Outgoing Interface WAN (wan1)

Authentication Method Pre-shared Key Signature

Pre-shared Key *****

Test: Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

< Back Next > Cancel

The screenshot shows the FortiGate 200E management interface. On the left, the navigation menu is open, showing 'IPsec Wizard' selected under 'VPN'. The main content area displays the 'VPN Creation Wizard' with the second step, 'Authentication', active. It requires configuration for a 'Remote Device' with an 'IP Address' of 1.1.1.1 and an 'Outgoing Interface' of 'WAN (wan1)'. The 'Authentication Method' is set to 'Pre-shared Key' with the key value '*****'. To the right, a network diagram titled 'Test: Site to Site - FortiGate' shows two FortiGate units connected through the 'Internet'. Below the diagram are buttons for '< Back', 'Next >', and 'Cancel'.

Configuration

SSL

IPSec (suite)

VPN IPSEC

FortiGate 200E FG_ANTC_HQ

VPN Creation Wizard

VPN Setup > Authentication > Policy & Routing

Local Interface: LAN (port1)

Local Subnets:

Remote Subnets: 2.2.2.2/24

Internet Access: None Share WAN Force to use remote WAN

Test: Site to Site - FortiGate

This FortiGate

Remote FortiGate

< Back Create Cancel

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Templates

SSL-VPN Portals

SSL-VPN Settings

User & Device

WiFi & Switch Controller

Log & Report

Monitor

Bonnes pratiques

Objectifs

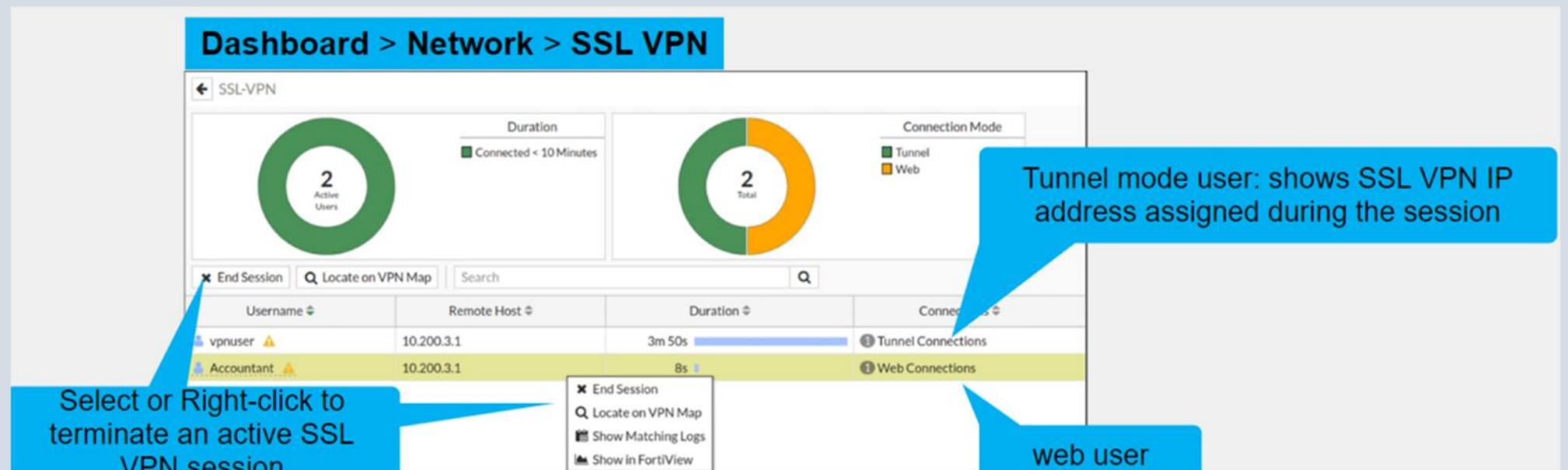
- Connaitre quelques bonnes pratiques.

Bonnes pratiques

Diagnostic

Session VPN

Bonnes pratiques



Bonnes pratiques

Diagnostic (suite)

Bonnes pratiques

Journalisation

The screenshot shows the FortiOS Log & Report interface. On the left, a sidebar lists various monitoring categories: Forward Traffic, Local Traffic, Sniffer Traffic, Events (which is selected and highlighted in green), SSL, DNS Query, Application Control, Intrusion Prevention, Anomaly, Log Settings, Threat Weight, and Email Alert Settings. A red arrow points from the 'Events' button in the sidebar to the 'VPN Events' section in the main content area. The main content area displays two tables of event logs. The top table, titled 'VPN Events', shows logs for a connection attempt and its subsequent status changes. The bottom table, titled 'User Events', shows logins and logouts for a user named 'Student'. Both tables have columns for Date/Time, Level, Action, Status, and Message.

Date/Time	Level	Action	Status	Message
2020/01/21 04:50:...	[green bar]	ssl-new-con		SSL new connection
2020/01/21 04:50:...	[green bar]	tunnel-down		SSL tunnel shutdown
2020/01/21 04:49:...	[green bar]	tunnel-stats		SSL tunnel statistics
2020/01/21 04:39:...	[green bar]	tunnel-up		SSL tunnel established
2020/01/21 04:39:...	[green bar]	ssl-new-con		SSL new connection

Date/Time	Level	User	Action	Message
2020/01/21 04:50:33	[blue bar]	Student	auth-logout	User Student removed from auth logon
2020/01/21 04:39:02	[blue bar]	Student	auth-logon	User Student added to auth logon

Bonnes pratiques

Diagnostic

Bonnes pratiques

- Activation des cookies;
- Respect de la structure de l'URL: `https://<FortiGateIP>:<Port>`;
- Vérification du numéro de port de connexion;
- Vérification de la configuration des règles de trafic;
- Sensibilisation des utilisateurs.