
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

FortiOS 7.0

FORTINET Training Institute

Plan du module

- Fonctionnalité de haut niveau
- Décision de déploiement
- Administration basique
- Serveurs intégrés
- Maintenance de base
- Interfaces, routage et portail captif

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).

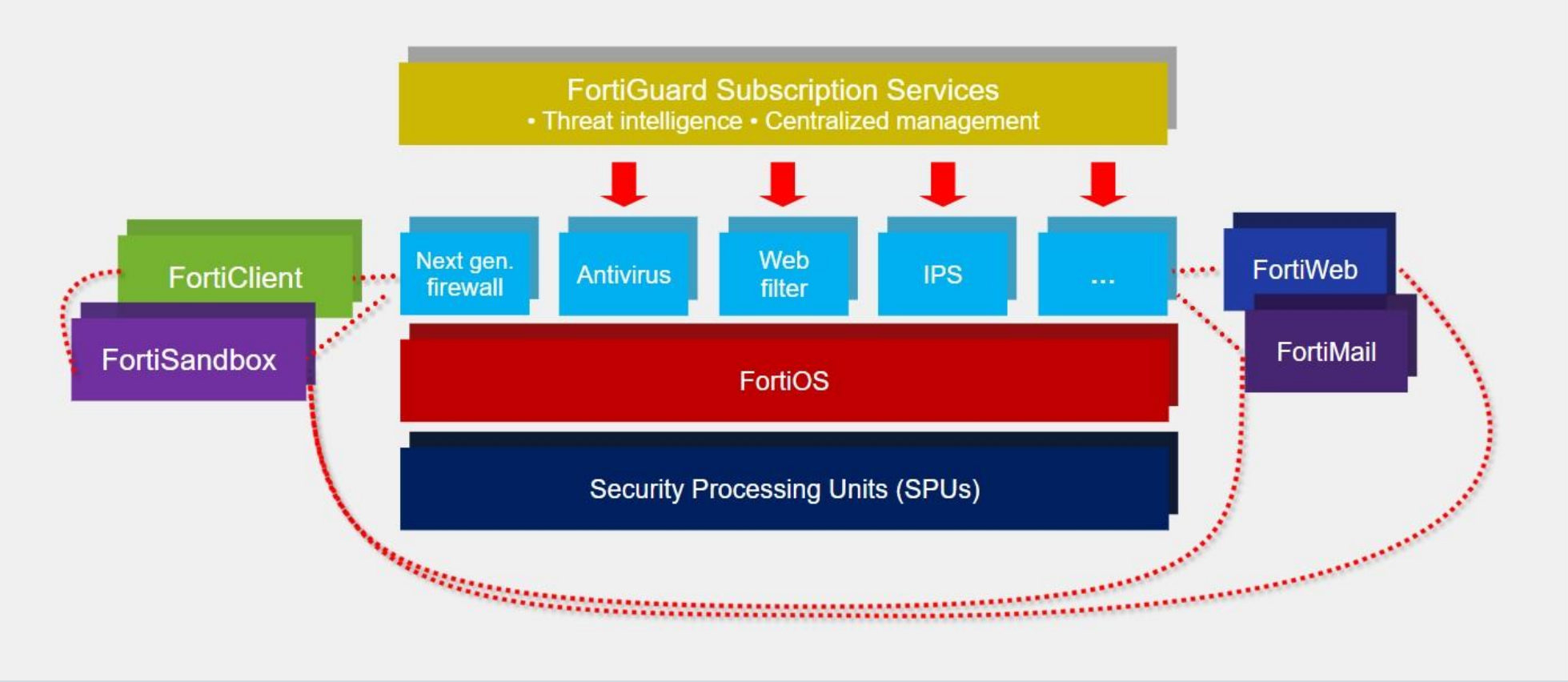
Fonctionnalités de haut niveau

Sécurité réseau | Plateforme FortiGate | Topologies Cloud | SPU (Security Processing Units)

- Firewall sont plus que les gardiens du périmètre de sécurité réseau
- Conçu aujourd'hui pour répondre aux évolution des environnement 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 différente fonction dans un réseau
  - Datacenter Firewall
  - Segmentation Firewall
  - Next-generation Firewall

Fonctionnalités de haut niveau

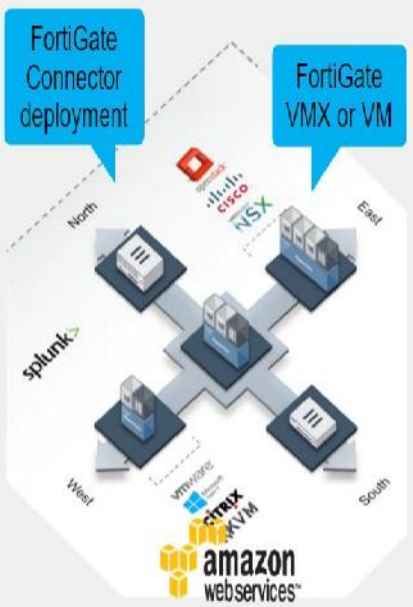
Sécurité réseau | Plateforme FortiGate | Topologies Cloud | SPU (Security Processing Units)



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;

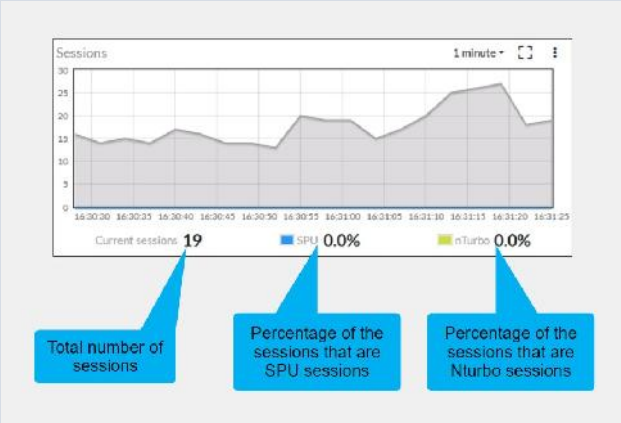


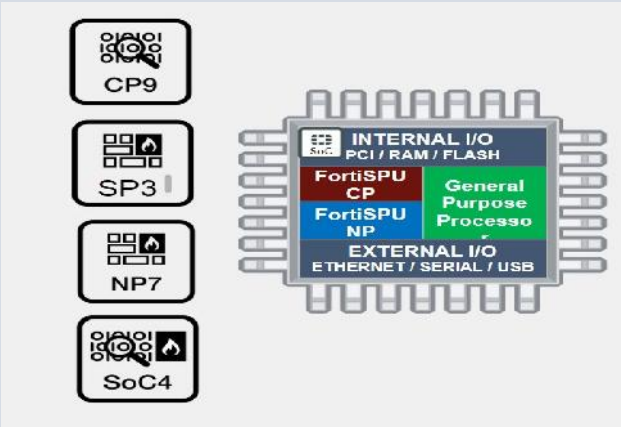
FortiGate VM Specifications	
Licenses	Max. 1 / 2 / 4 / 8 vCPU
Hypervisor	VMware, Hyper-V, KVM, Citrix Xen Server, Open Source Xen, Azure, Amazon AWS BYOL & on-demand
Memory	Max. 1/4/8/12 GB
10/100/1000 Interfaces	2-4 virtual NICs
Storage Capacity	40+ GB

Fonctionnalités de haut niveau

Sécurité réseau | Plateforme FortiGate | Topologies Cloud | SPU (Security Processing Units)

- 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





Décision de déploiement

Objectifs

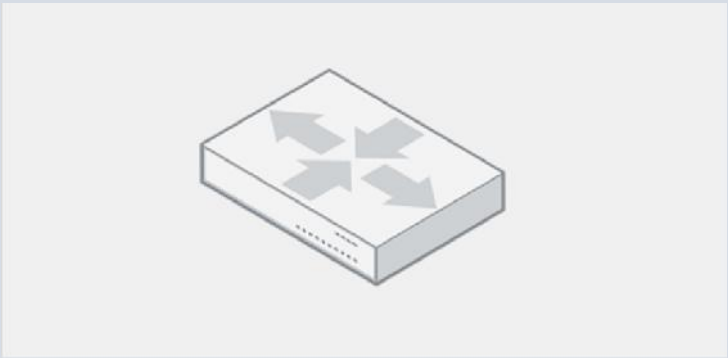
- Identifier les paramètres par défaut du pare-feu ;
- Choix d'un mode de fonctionnement ;
- Comprendre la relation entre FortiGate et FortiGuard;
- Distinguer les « lives queries » et les « packages updates »

Décision de déploiement

Mode de fonctionnement | Paramètre par défaut | Services FortiGuard

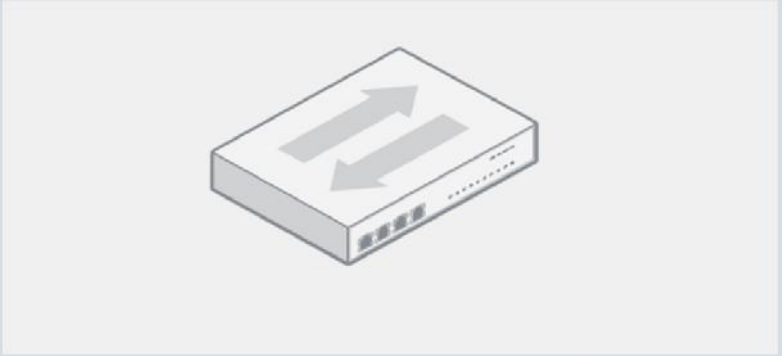
NAT

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



Transparent

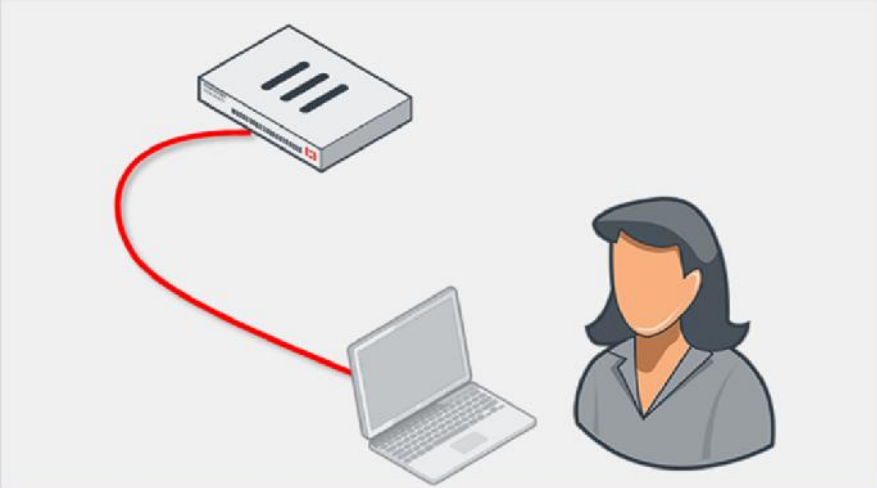
- Equipement de couche 2;
- Aucune IP sur les interfaces;
- Transfert ou bloque uniquement les paquets;
- Configurable par VDOM (Virtual Domaine).



Décision de déploiement

Mode de fonctionnement | Paramètre par défaut | Services FortiGuard

- IP par défaut: 192.168.1.99/24
  - Interface de management: modèle haut de gamme et de gamme intermédiaire;
  - Port 1 sur les modèle 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 support 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



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.

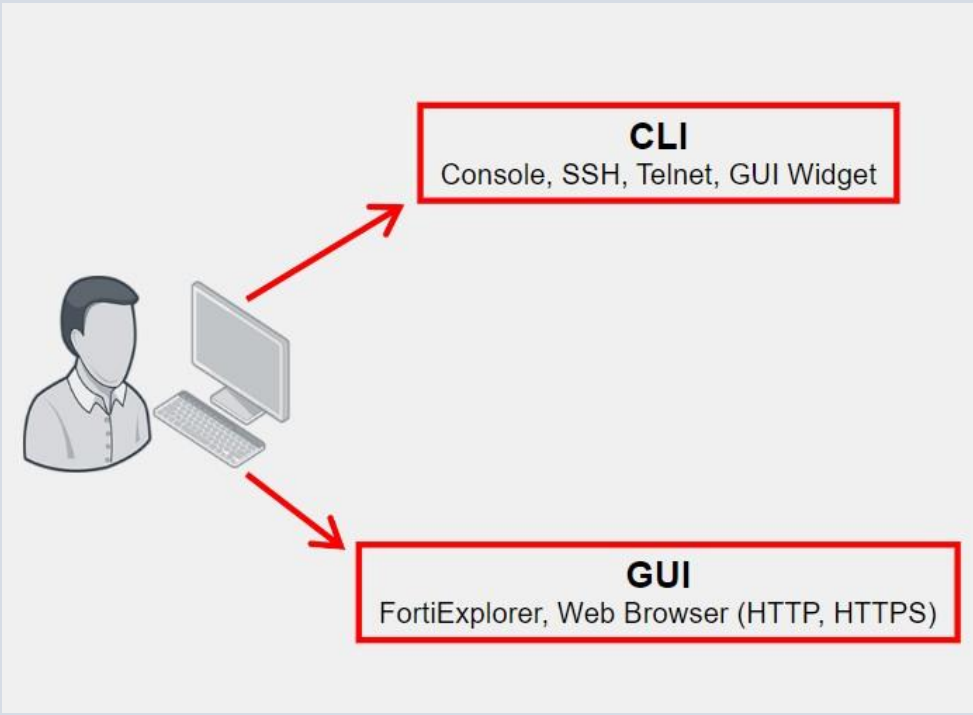
Administration de base

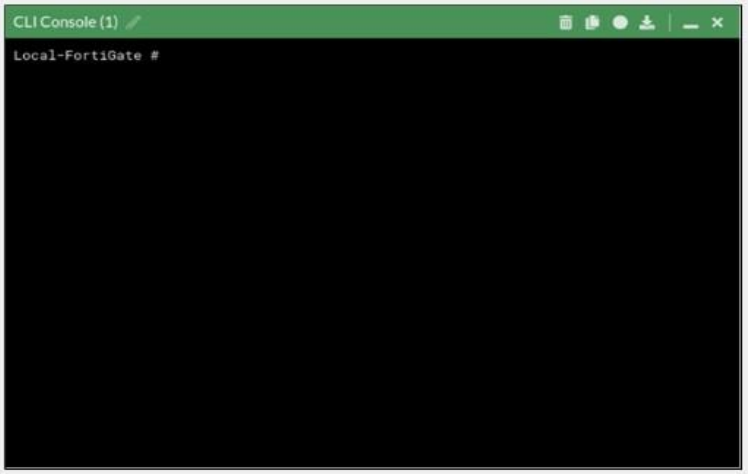
Objectifs

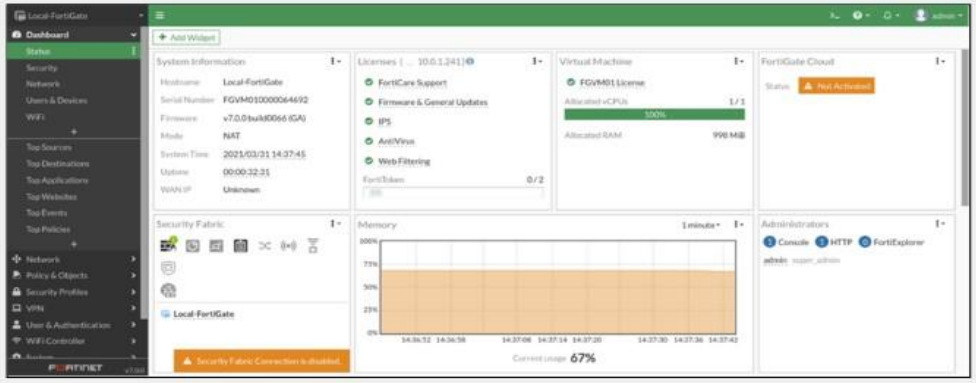
- Gérer les profils administrateurs ;
- Gérer les utilisateurs ;
- Contrôler les accès à l'interface graphique et à la CLI.

Administration de base

Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification







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) | 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;

```
FG_ANTIC_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_ANTIC_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
```

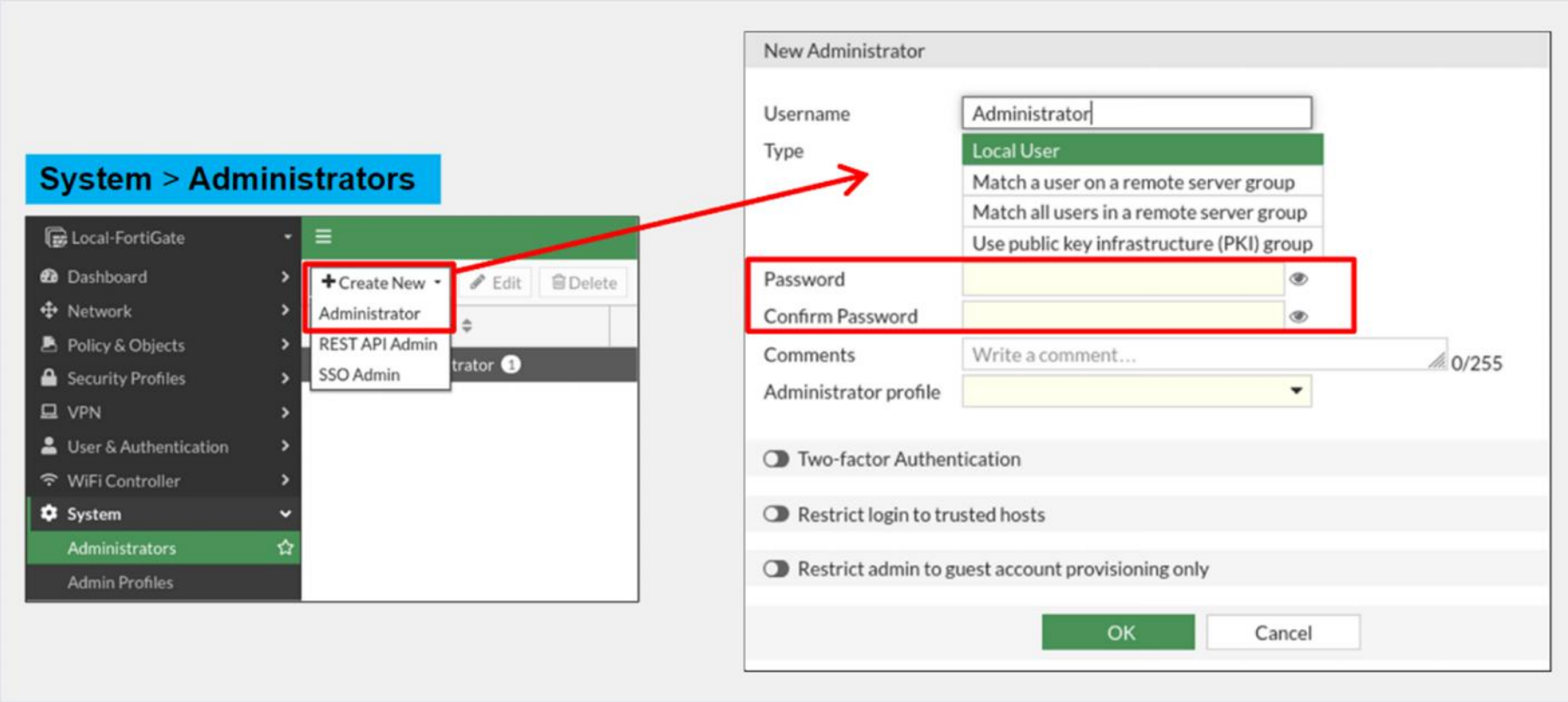
```
FG_ANTIC_HQ # show system interface port2
config system interface
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 6
    next
end
```

```
FG_ANTIC_HQ # show full-configuration system interface
config system interface
    edit "mgmt"
        set vdom "root"
        set vrf 0
        set fortilink 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

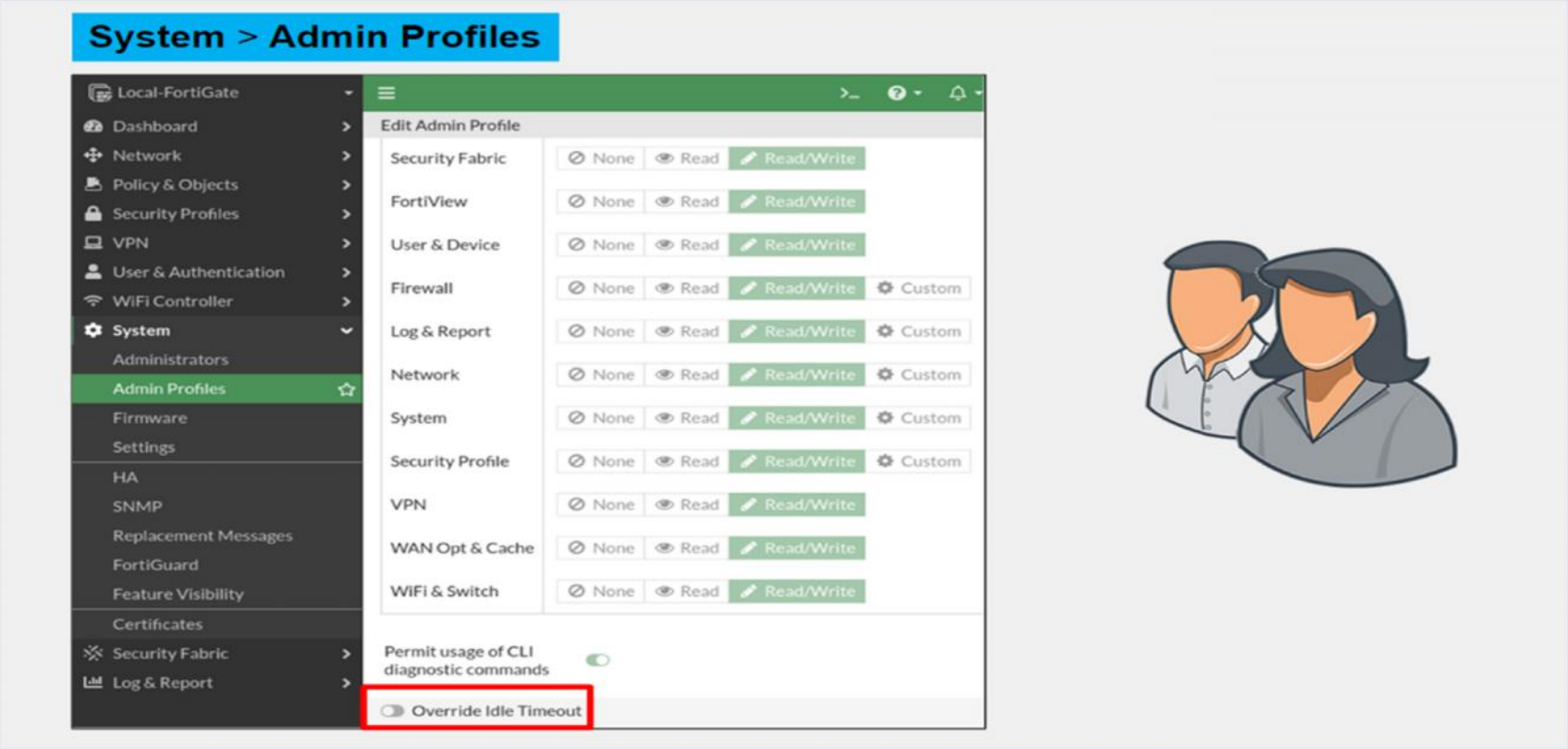
Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification

- Création d'un utilisateur (administrateur)



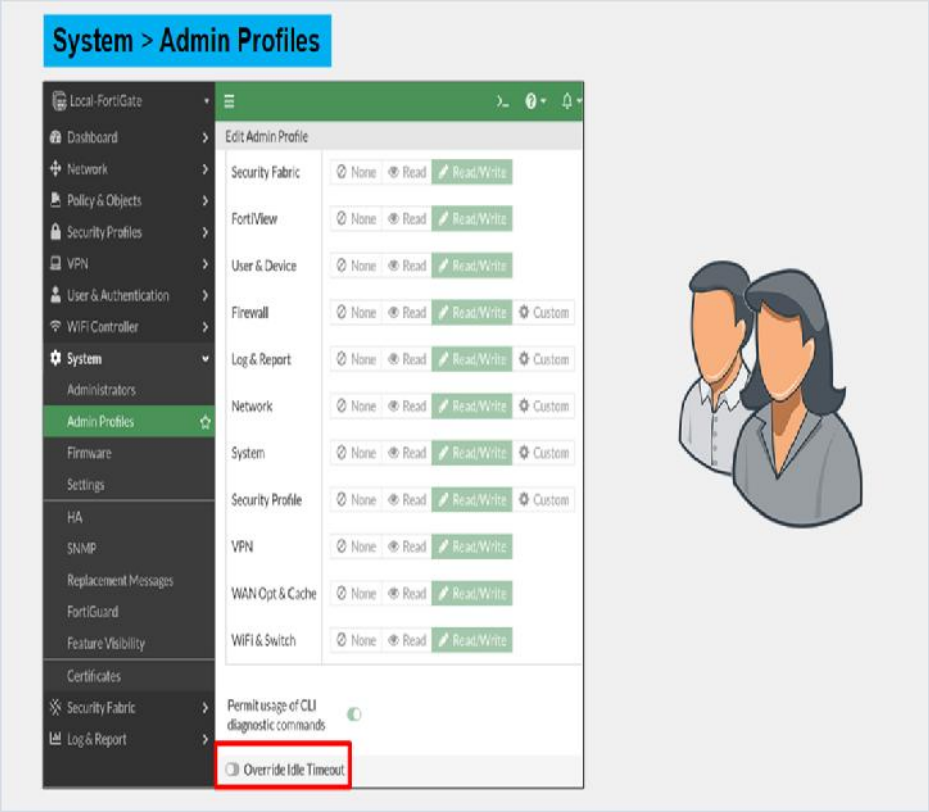
Administration de base

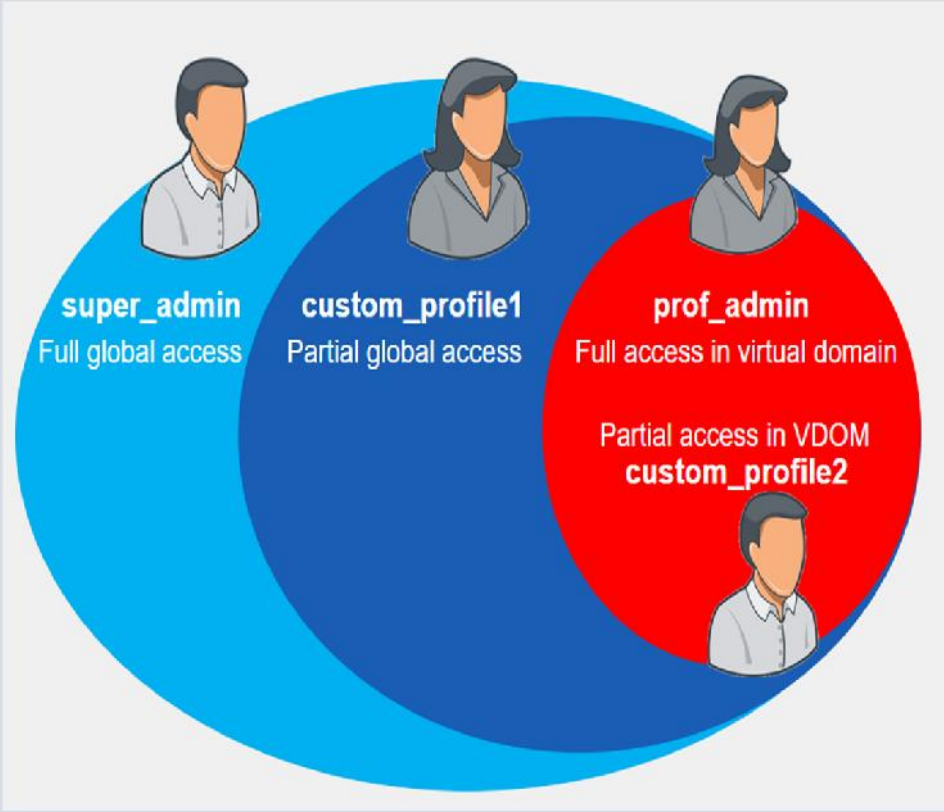
Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification



Administration de base

Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification



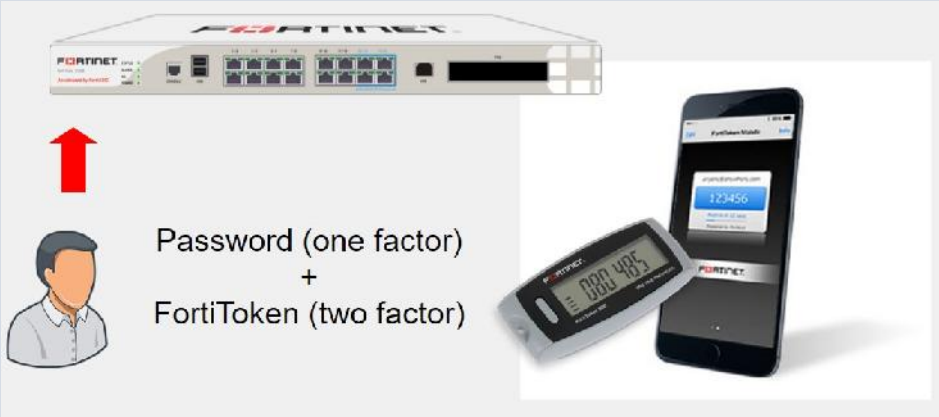


Administration de base

Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification

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

- 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 | Gestion des utilisateurs | Gestion des profils | Authentification(suite)

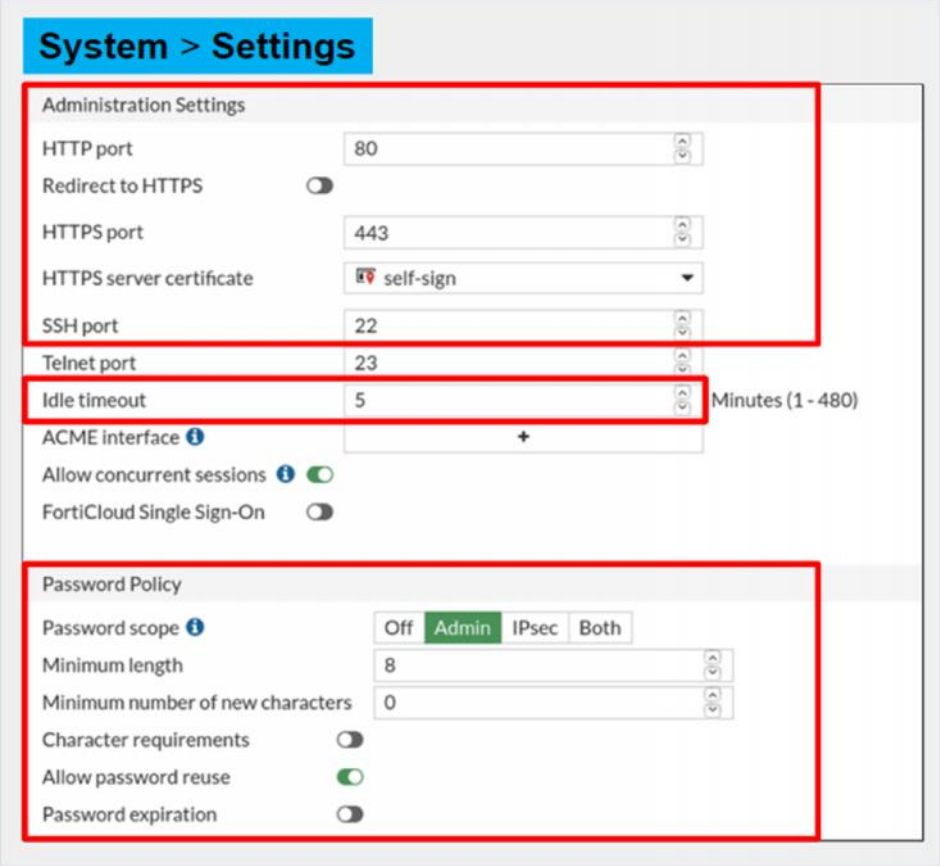
- Réinitialisation du mot de passe administrateur
  - Etape 1: Redémarrer le pare-feu (redémarrage à froid) et accéder à la console
  - Etape 2: Les paramètres suivant sont valides uniquement pendant les 60 premiers secondes après le redémarrage et via la console :
    - Login: maintien
    - Mot de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

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

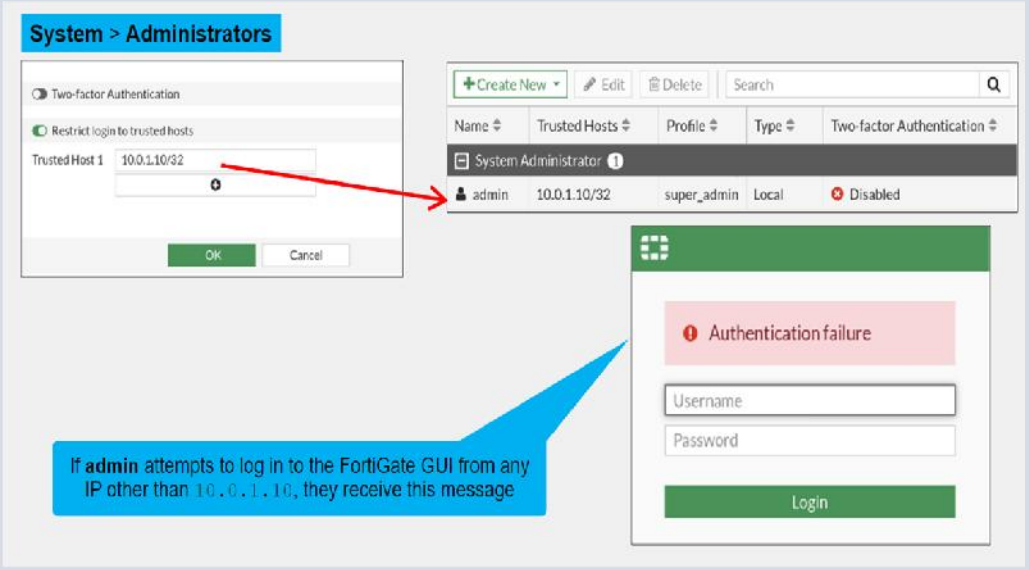
```
#config system global
set admin-maintainer
disable
end
```

Administration de base

Méthode d'administration | Gestion des utilisateurs | Gestion des profils | Authentification(suite)



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



Serveurs intégrés

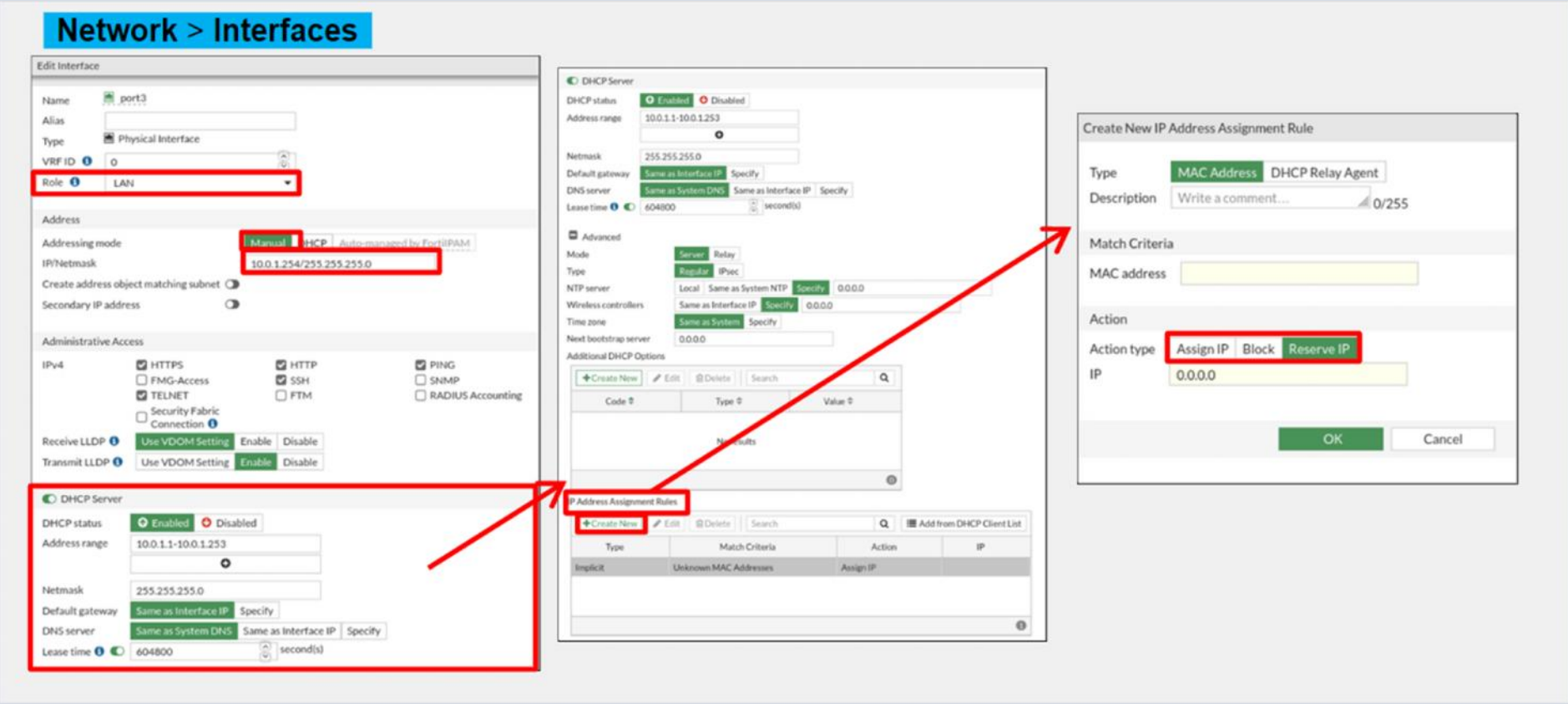
Objectifs

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

Administration de base

Serveur DHCP

Serveur DNS

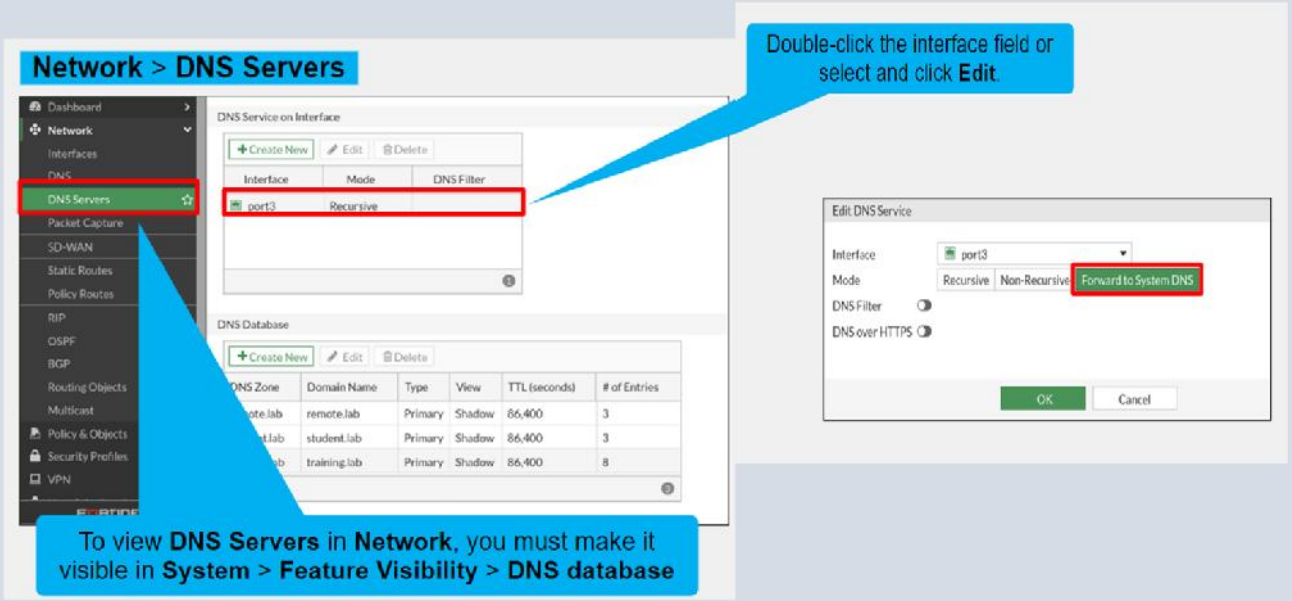


Administration de base

Serveur DHCP

- Fonctionnalité n'est pas visible par défaut, il faut ajouté la fonctionnalité DNS Database dépuis 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;
- Methodes 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

Serveur DNS



Maintenance de base

Objectifs

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

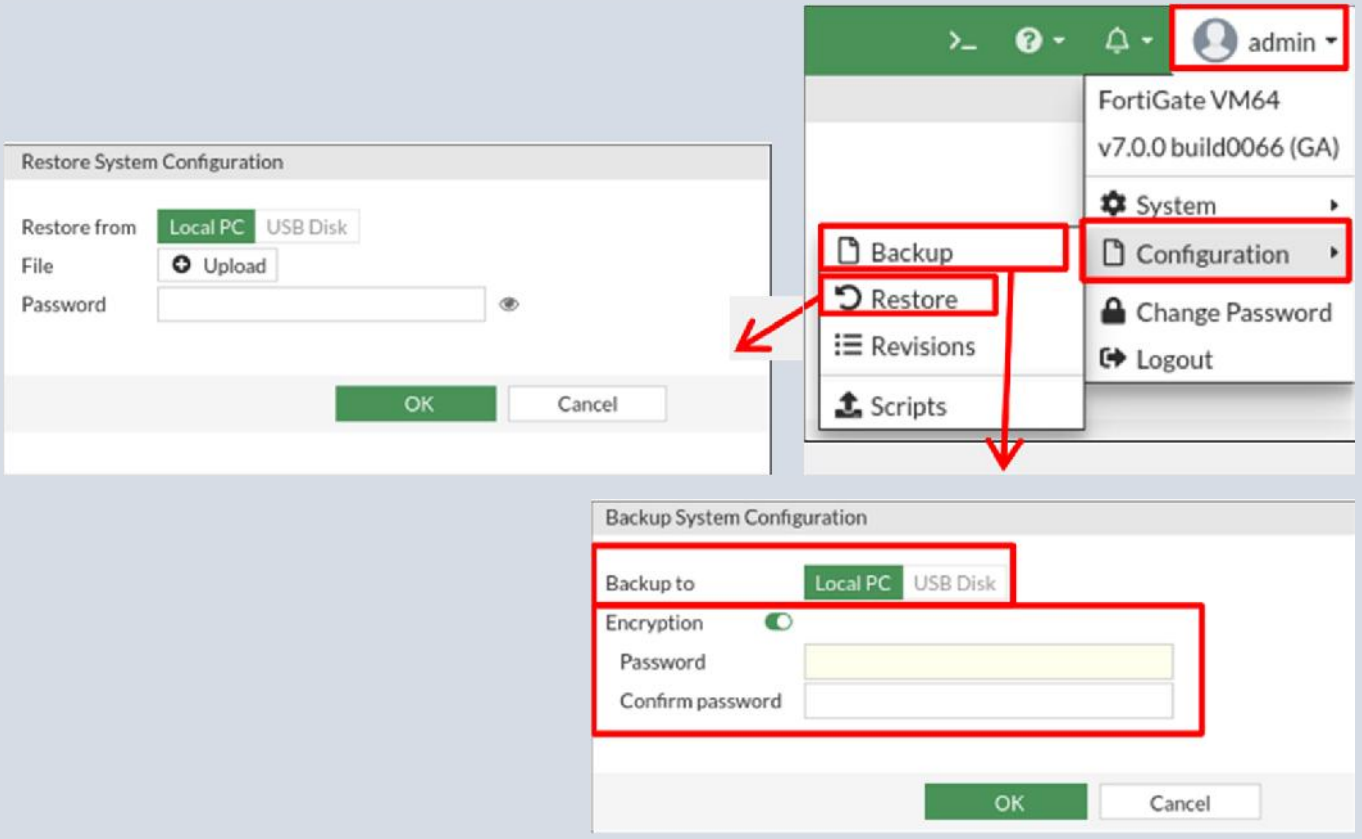
Maintenance de base

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

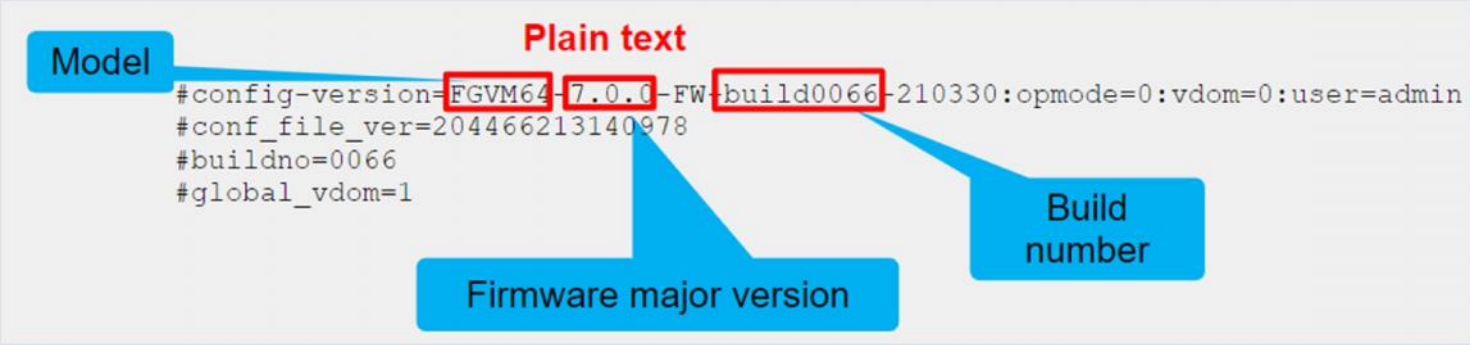
Upgrade

Downgrade

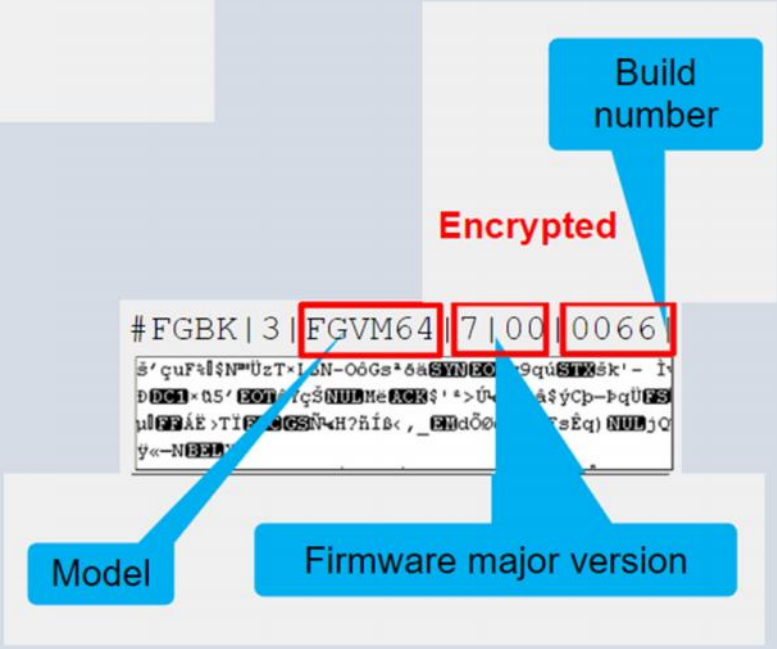


Maintenance de base

Sauvegarde/Restauration (suite) | Upgrade | Downgrade



- **Restauration**
  - Chiffré: meme équipement/modèle + build + mot de passe;
  - Non chiffré: Meme modèle



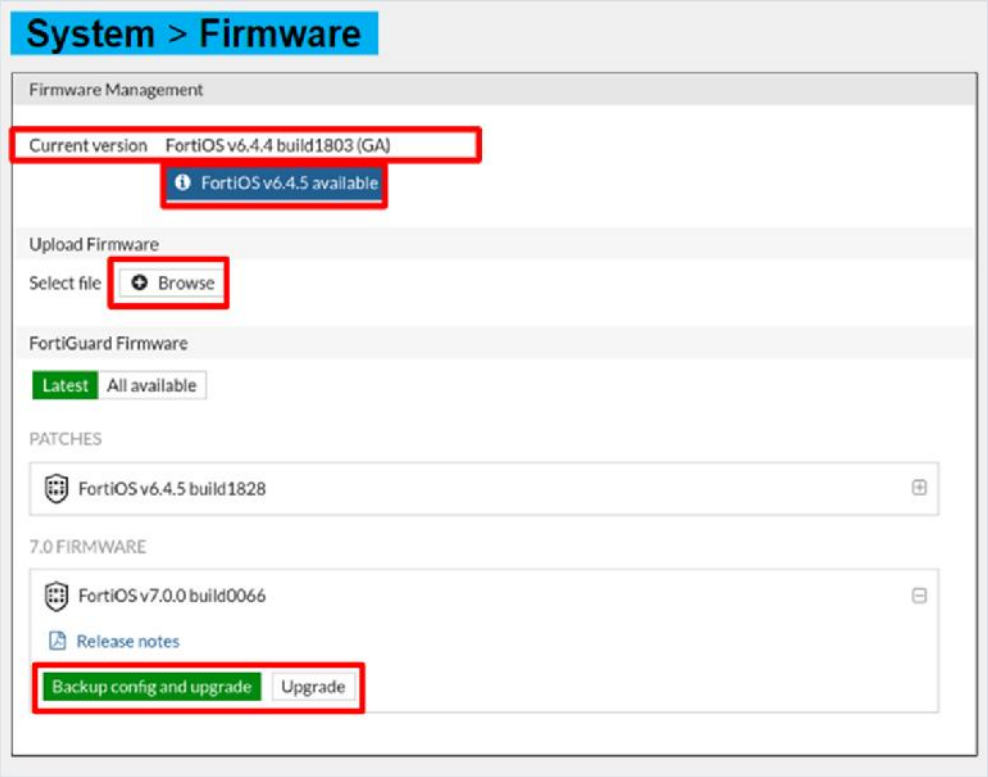
Maintenance de base

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

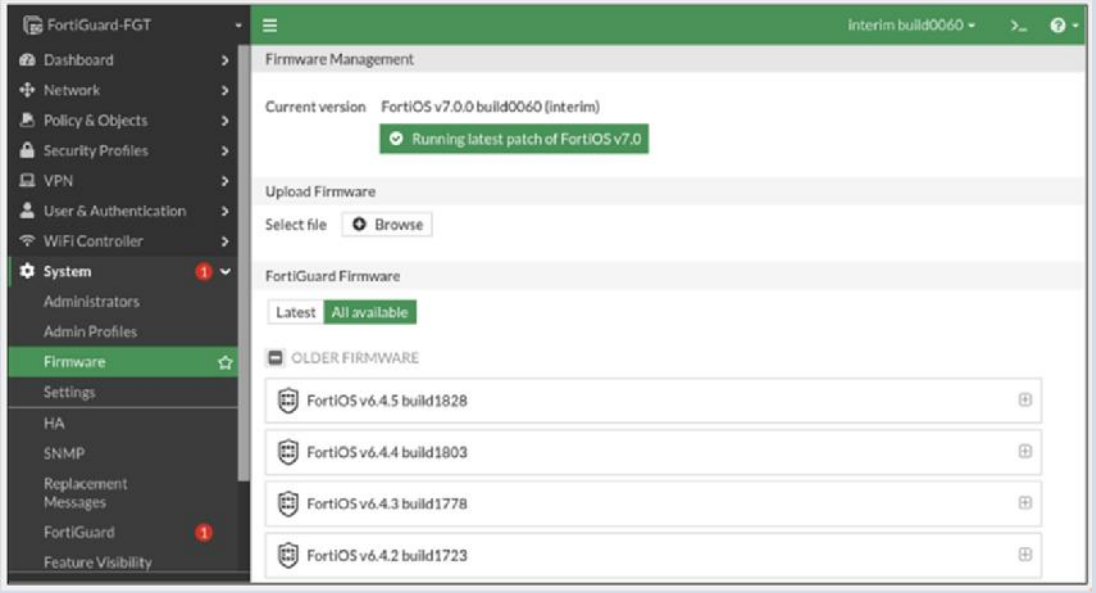
Downgrade



Maintenance de base

Sauvegarde/Restauration | Upgrade | Downgrade

- 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



Interfaces, routage et portail captif

Objectifs

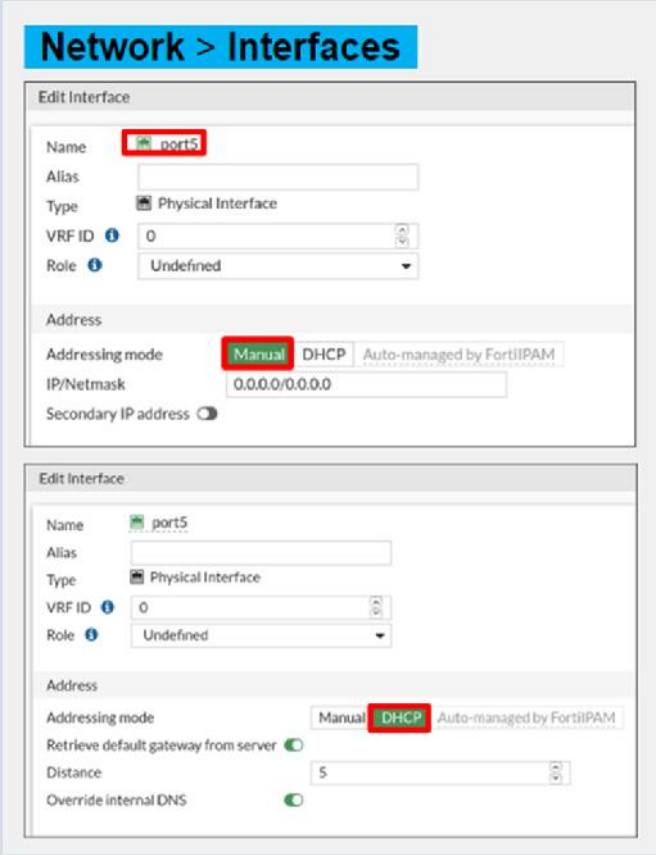
- Configurer les interfaces réseaux;
- Configurer les services associés aux interfaces;
- Configuration du routage statique et dynamique

Interfaces, routage et portail captif

Interfaces | Portail Captif | Routage

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

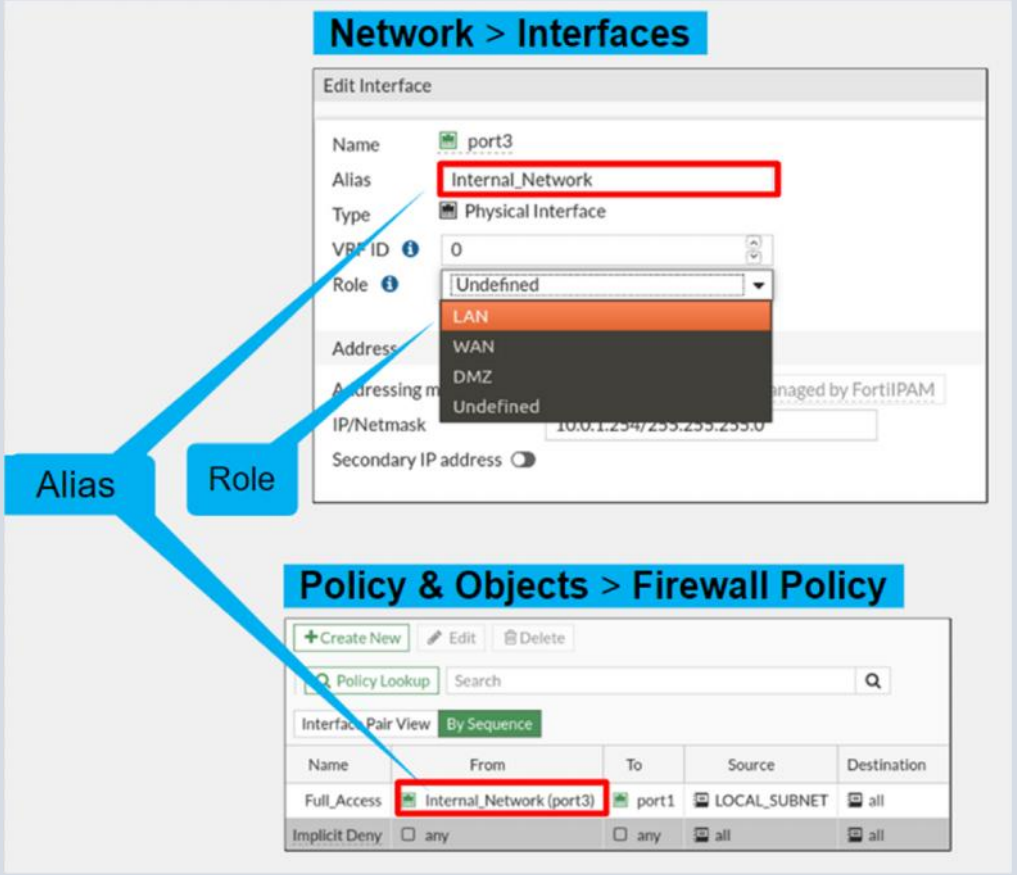
```
config system interface
  edit port <number>
   set ips-sniffer-mode enable
  end
```



Interfaces, routage et portail captif

Interfaces (suite) | Portail Captif | Routage

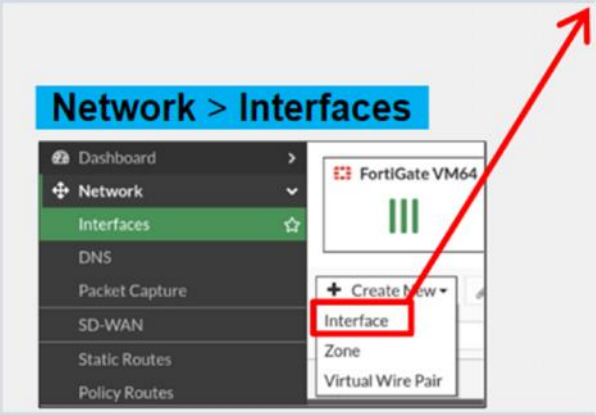
- Interfaces IP
  - Rôle
  - Définit les paramètres des interfaces ;
  - Prevention des erreurs de configuration;
  - 04 types:
    - LAN;
    - WAN;
    - DMZ;
    - Undefined (tous les paramètres)
  - Alias
    - Nom de l'interface;
    - Utilisé pour identifier les interfaces dans la liste des politiques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

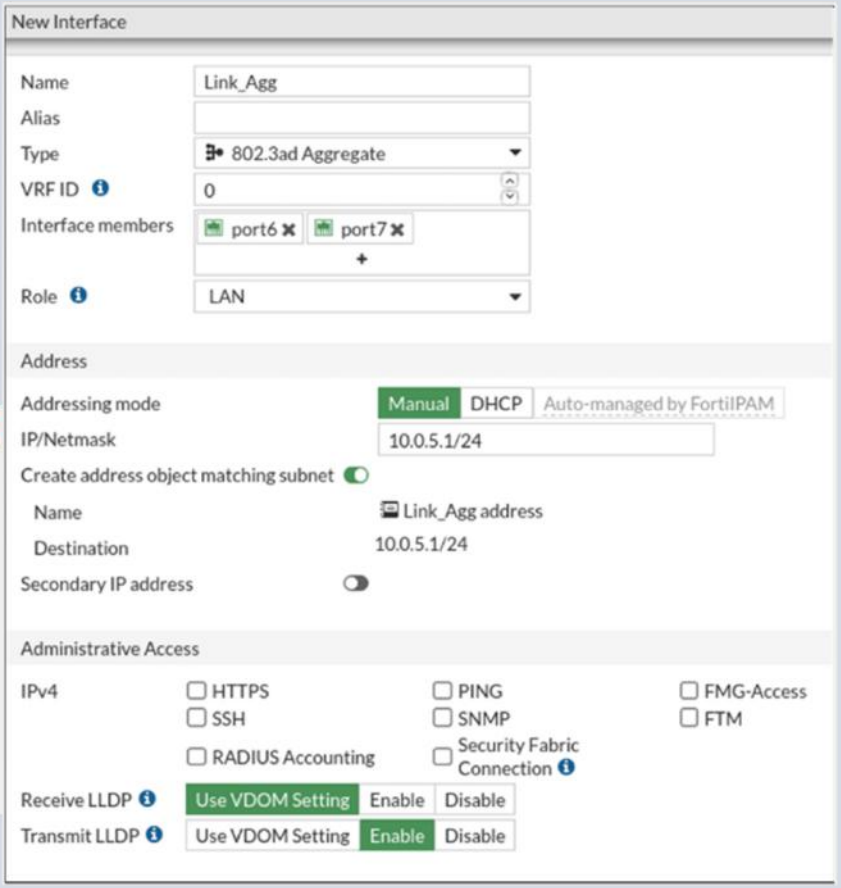


Interfaces, routage et portail captif

Interfaces (suite) Portail Captif Routage

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

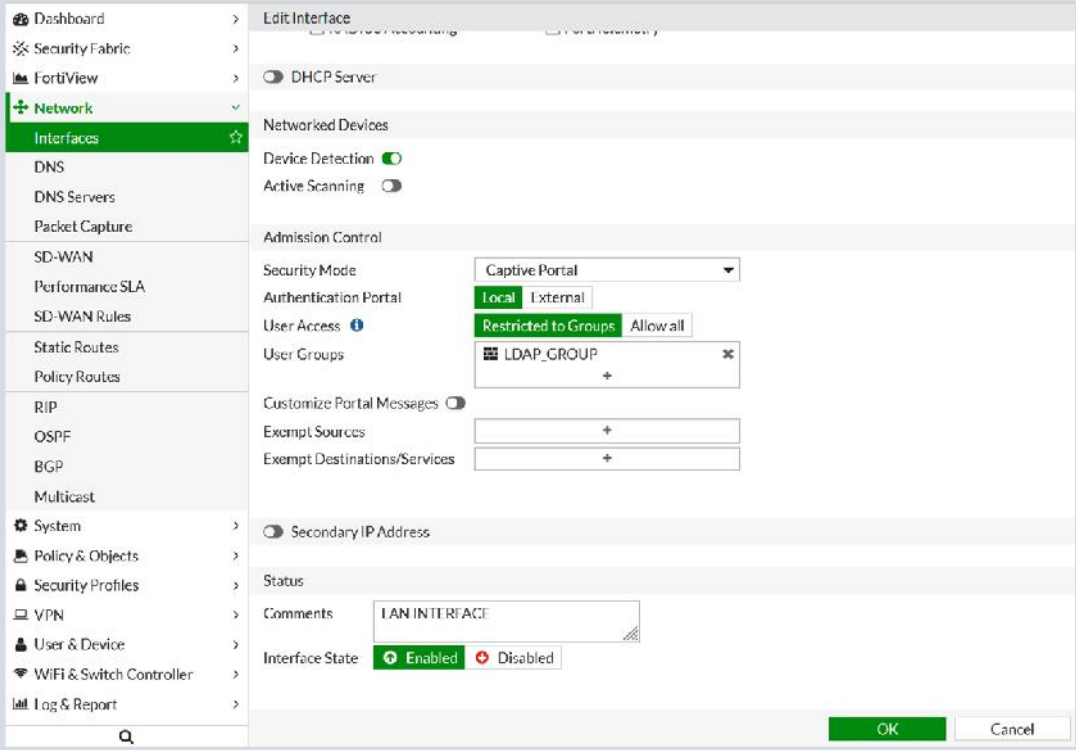




Interfaces, routage et portail captif

Interfaces | Portail Captif | Routage

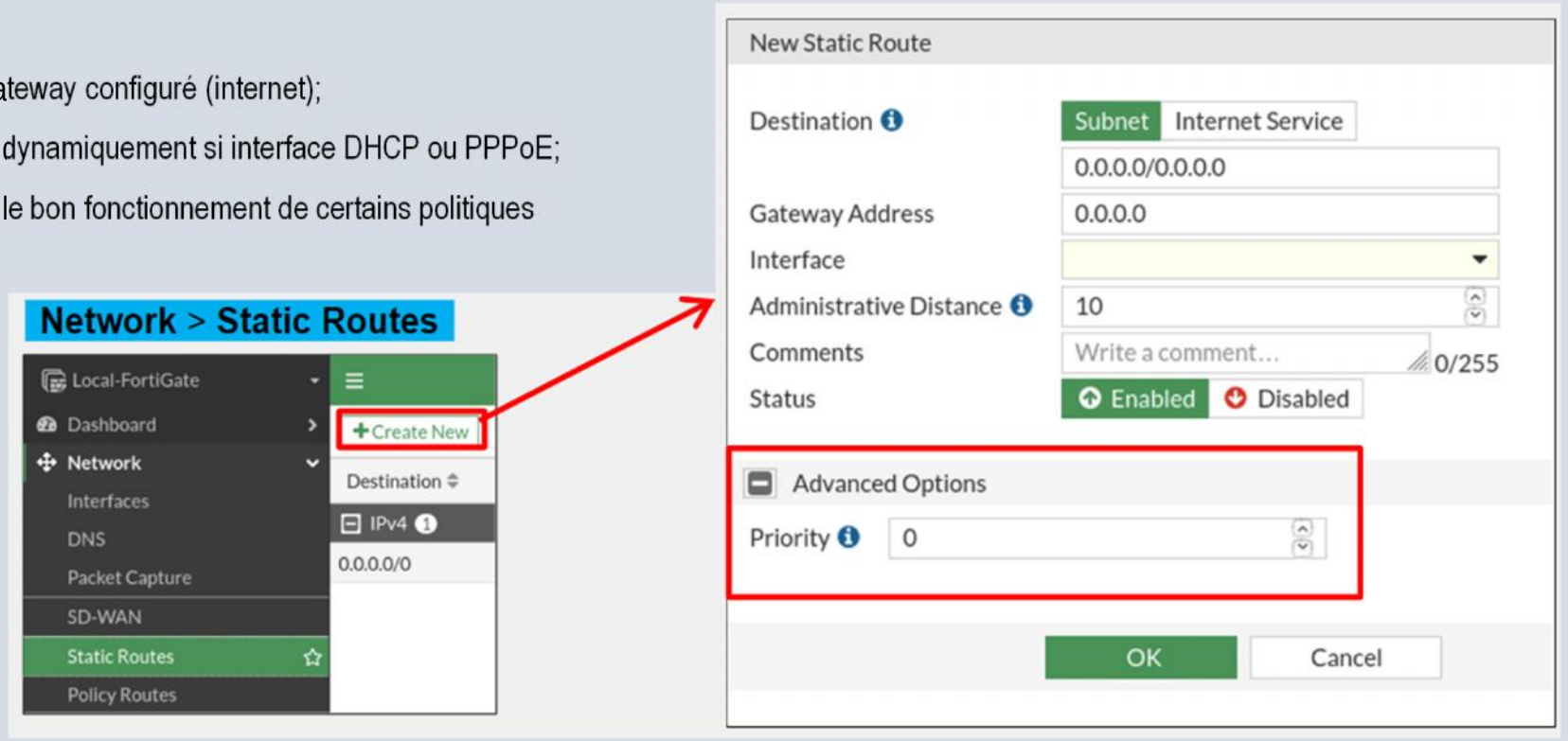
- Interfaces IP
  - Portail captif
    - Gestion et régulation de l'accès à internet aux utilisateurs finaux;
    - Configuration au niveau de l'interface LAN;
    - Intégration des sources d''authentification externe (LDAP);
    - Personnalisation de la page d'authentification.



Interfaces, routage et portail captif

Interfaces Portail Captif Routage

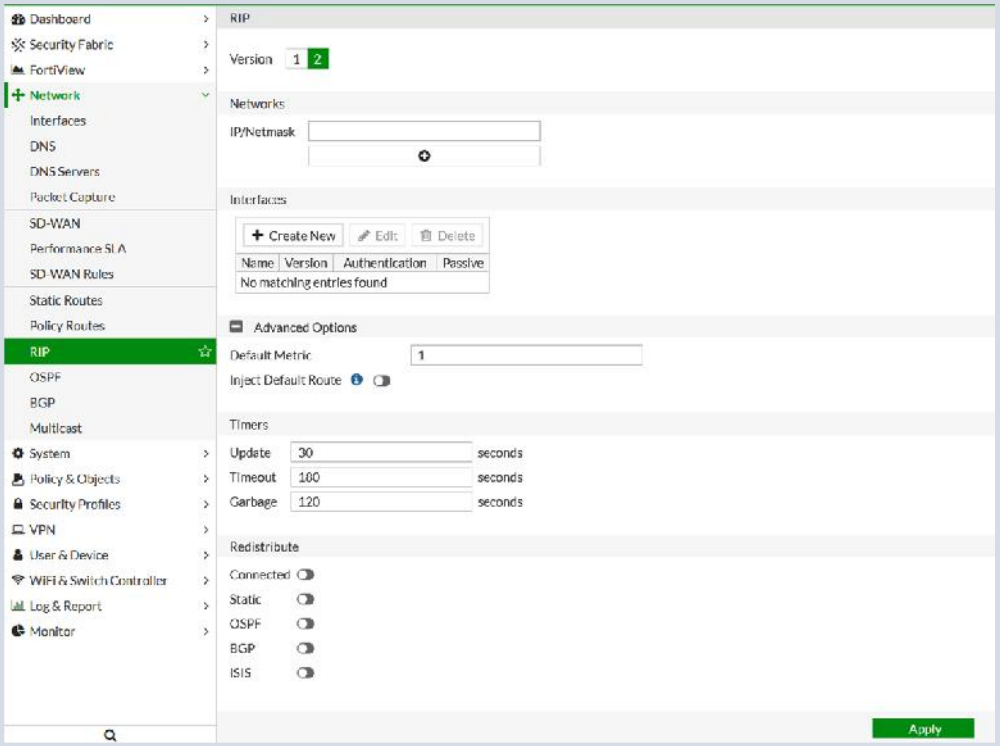
- Routage Statique
  - Au moins une Gateway configuré (internet);
  - Gateway ajouter dynamiquement si interface DHCP ou PPPoE;
  - Nécessaire pour le bon fonctionnement de certains politiques de pare-feu;

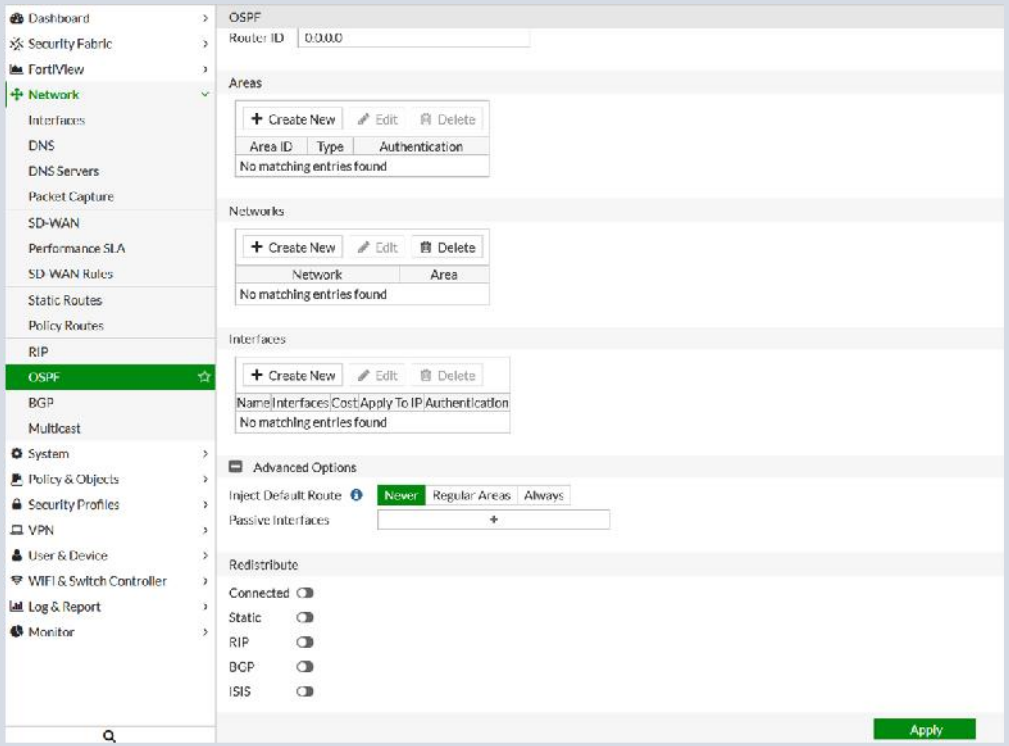


Interfaces, routage et portail captif

Interfaces | Portail Captif | Routage (suite)

- Routage Dynamique






FORTINET®

FORTINET
NSE Training Institute

FortiGate Security

FABRIC DE SECURITE

FortiOS 7.0

FORTINET Training Institute

Plan du module

- Introduction à la Fabric de sécurité Fortinet
- Déploiement d’une Fabric de sécurité
- Fonctionnalité et extension de la Fabric

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.

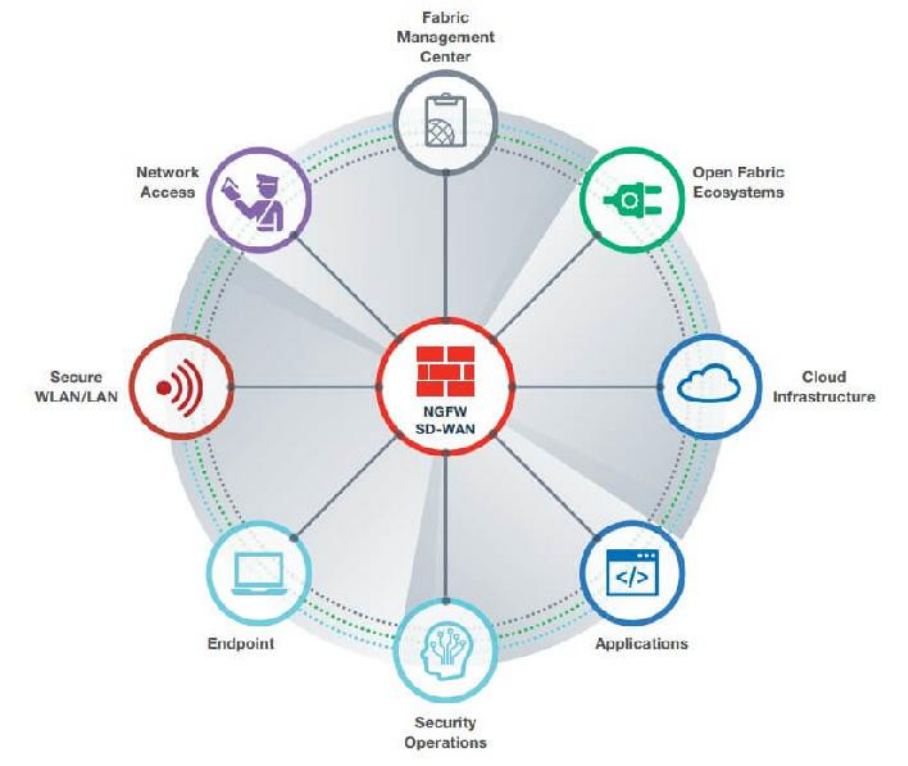
Fabric de sécurité Fortinet: Introduction

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 meilleur gestion des risques;
  - Intégrated: réduit la complexité dans la prise en charge des produit;
  - Automated: permet un échange des informations sur les menaces entre les équipements réseau en temps pour des réponses automatisées face aux ménaces
- Intégration avec les API et protocoles d'autre constructeurs disponible d'où il est considéré comme: open

Importance

Produits/Equipements de la Fabric



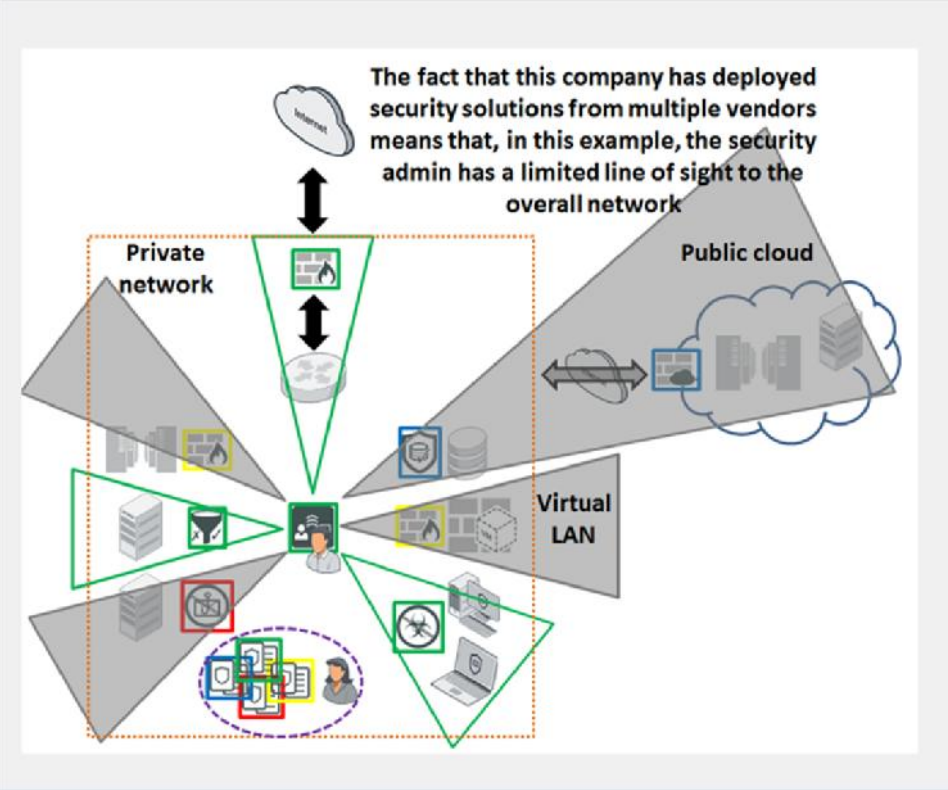
Fabric de sécurité Fortinet: Introduction

Fabric de sécurité

Importance

Produits/Equipements de la Fabric

- 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 maitrise 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 coordonnez les défenses afin de contenir et neutraliser les violations du réseau

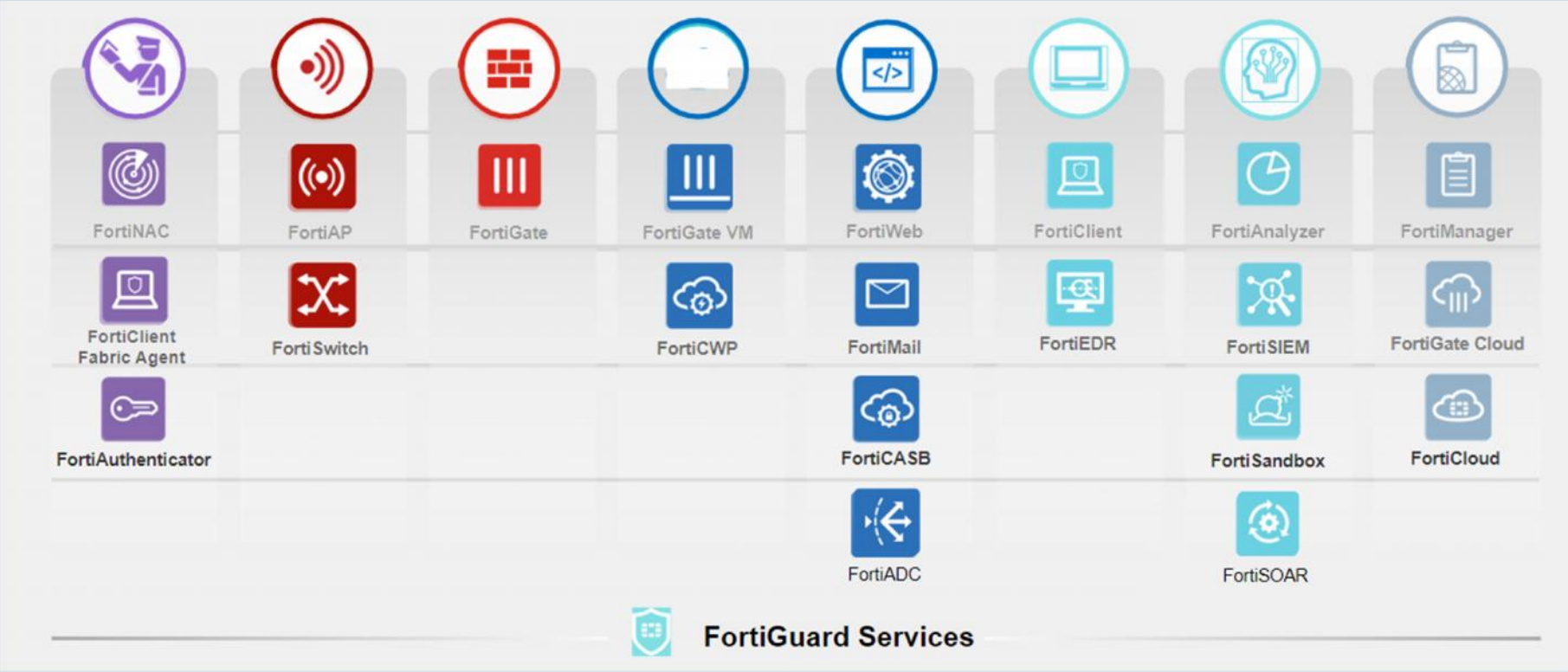


Fabric de sécurité Fortinet: Introduction

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;
  - Recommanded: 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

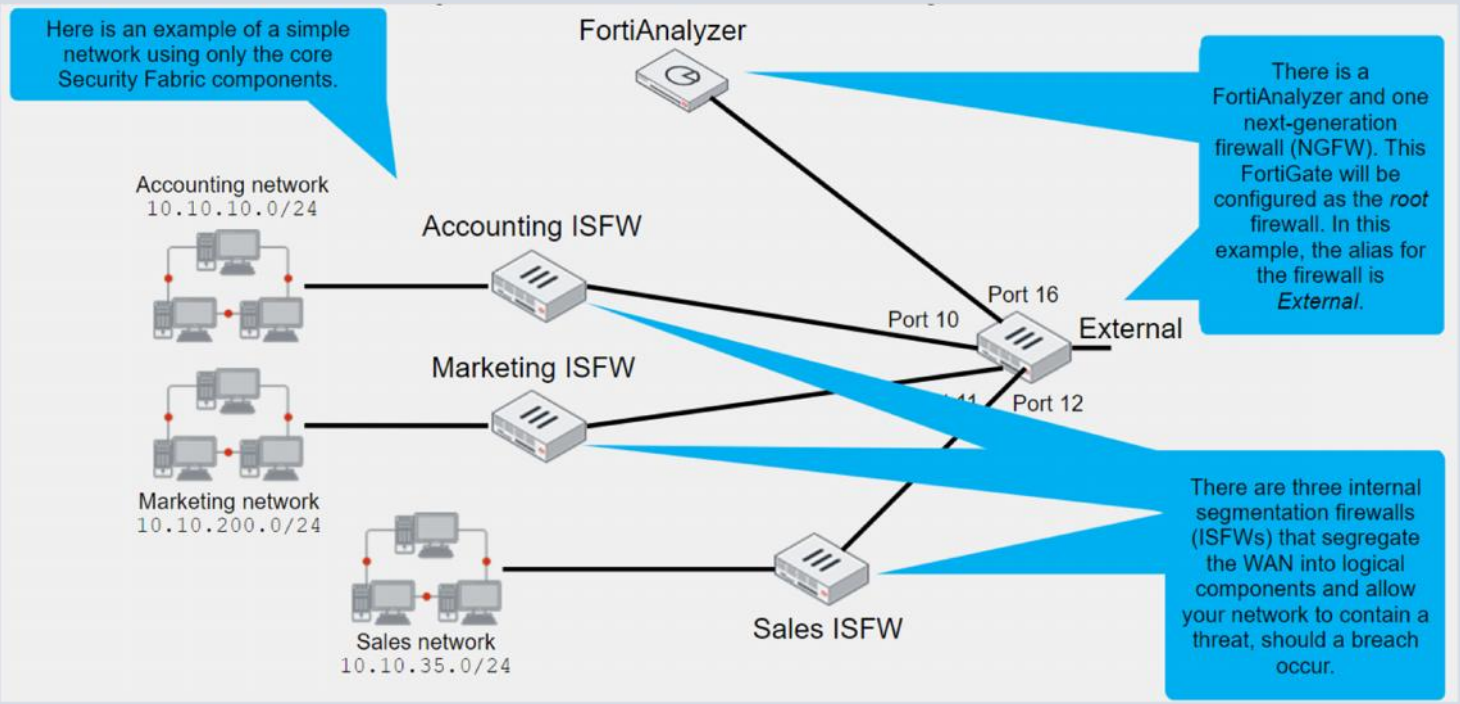
Implémentation | Configuration | VDOMS | Extension Fabric | Evaluation de la Sécurité

Equipements centraux:

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

Equipements secondaires;

- ❑ Pare-feu des différents départements (downstream);



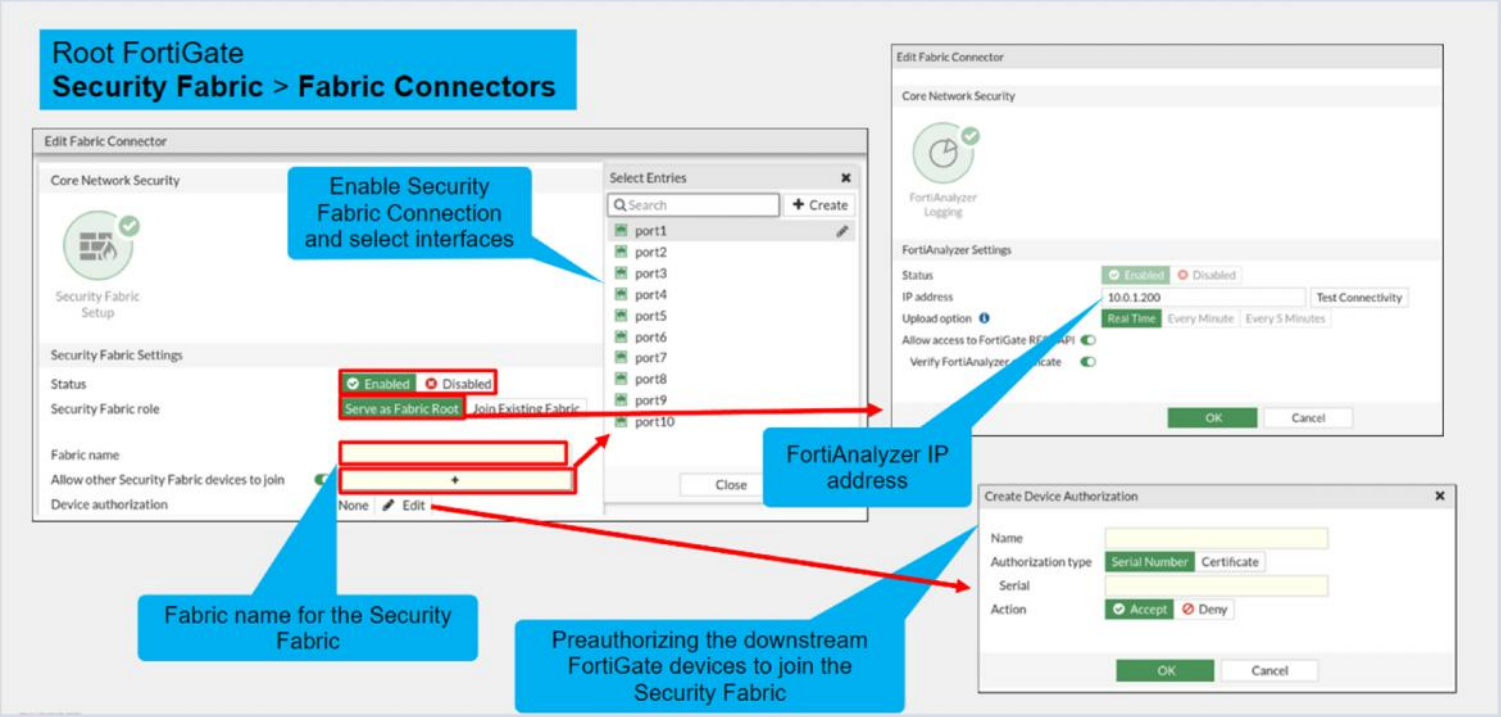
Déploiement d’une Fabric de sécurité

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 Dowstream 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;

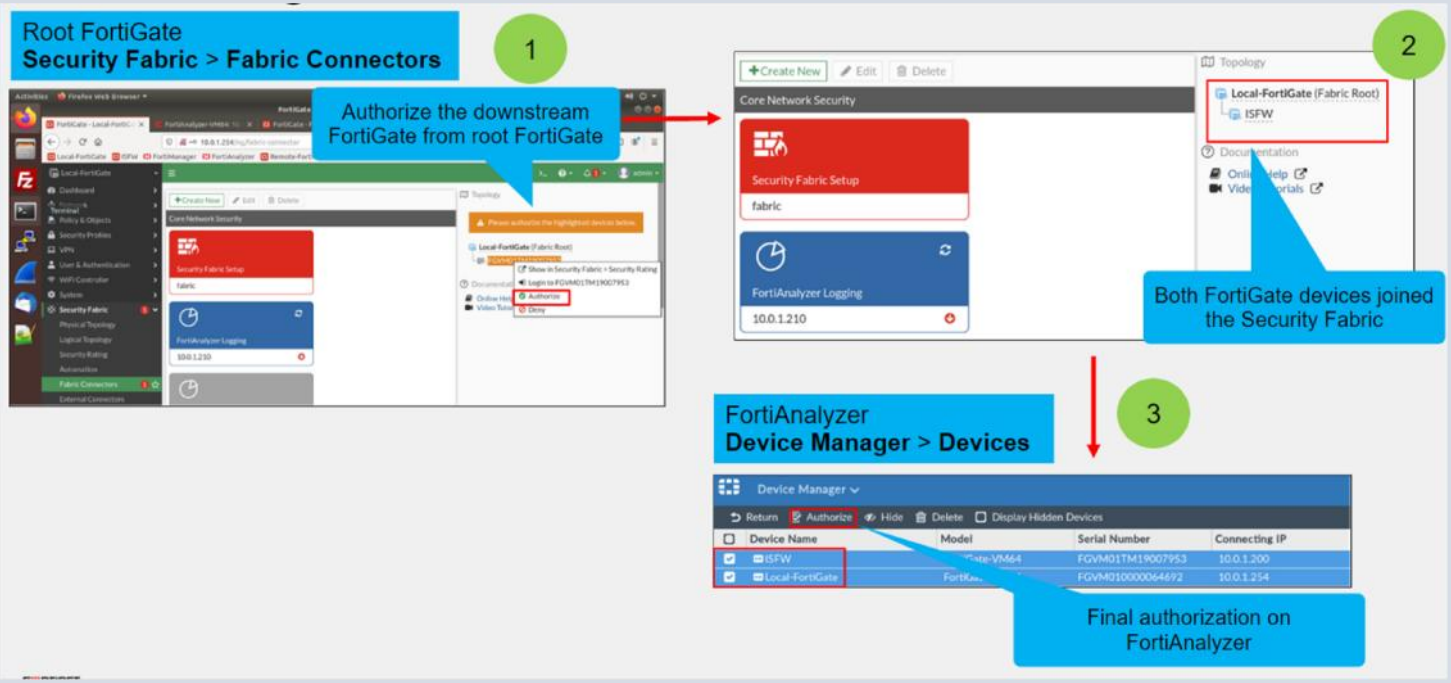
NB: Les configurations du FortiAnalyzer seront automatiquement propagées par le root sur les downstream

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.



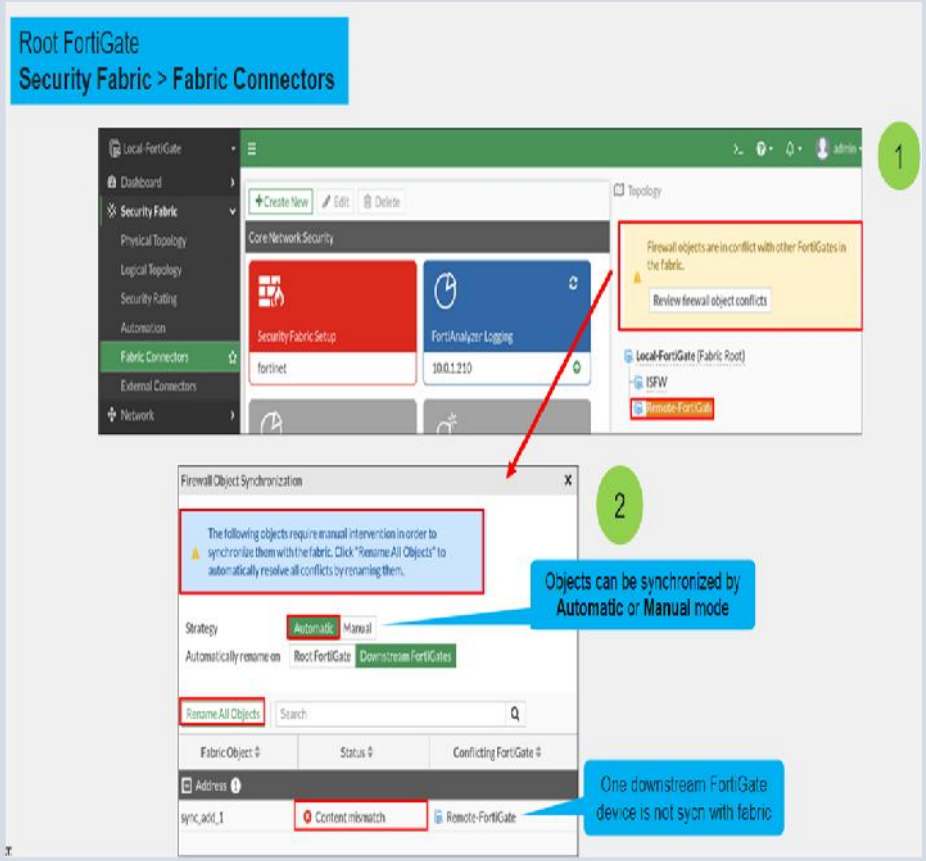
Déploiement d’une Fabric de sécurité

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 crée 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.

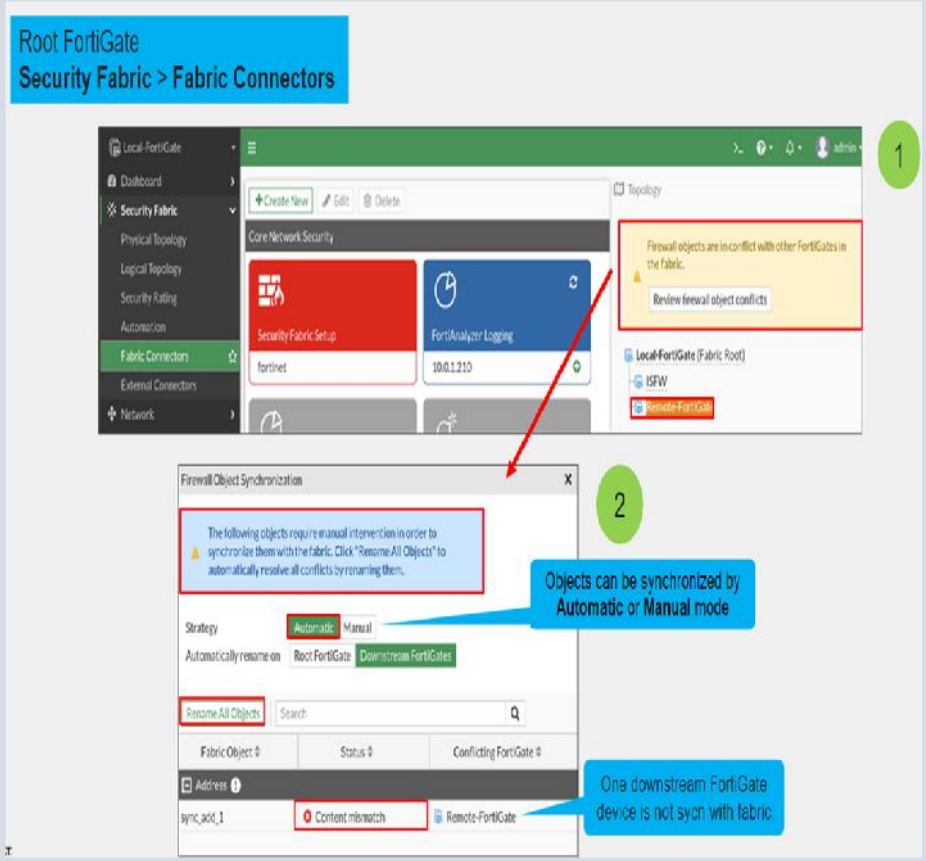
Déploiement d’une Fabric de sécurité

Implémentation | Configuration (suite) | VDOMS | Extension Fabric | Evaluation de la Sécurité



Déploiement d'une Fabric de sécurité

Implémentation | Configuration (suite) | VDOMS | Extension Fabric | Evaluation de la Sécurité



Déploiement d’une Fabric de sécurité

Implémentation | Configuration (suite) | VDOMS | Extension Fabric | Evaluation de la Sécurité

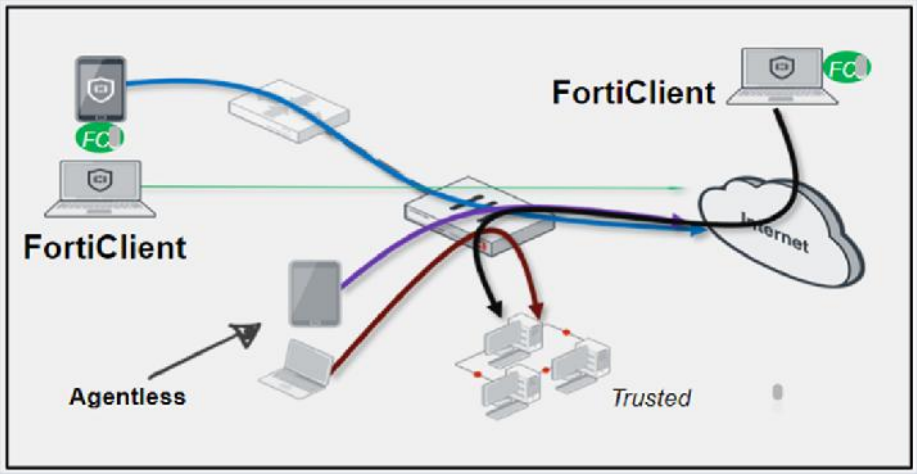
Technique d’identification des équipements dans la Fabric

Sans Agent

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

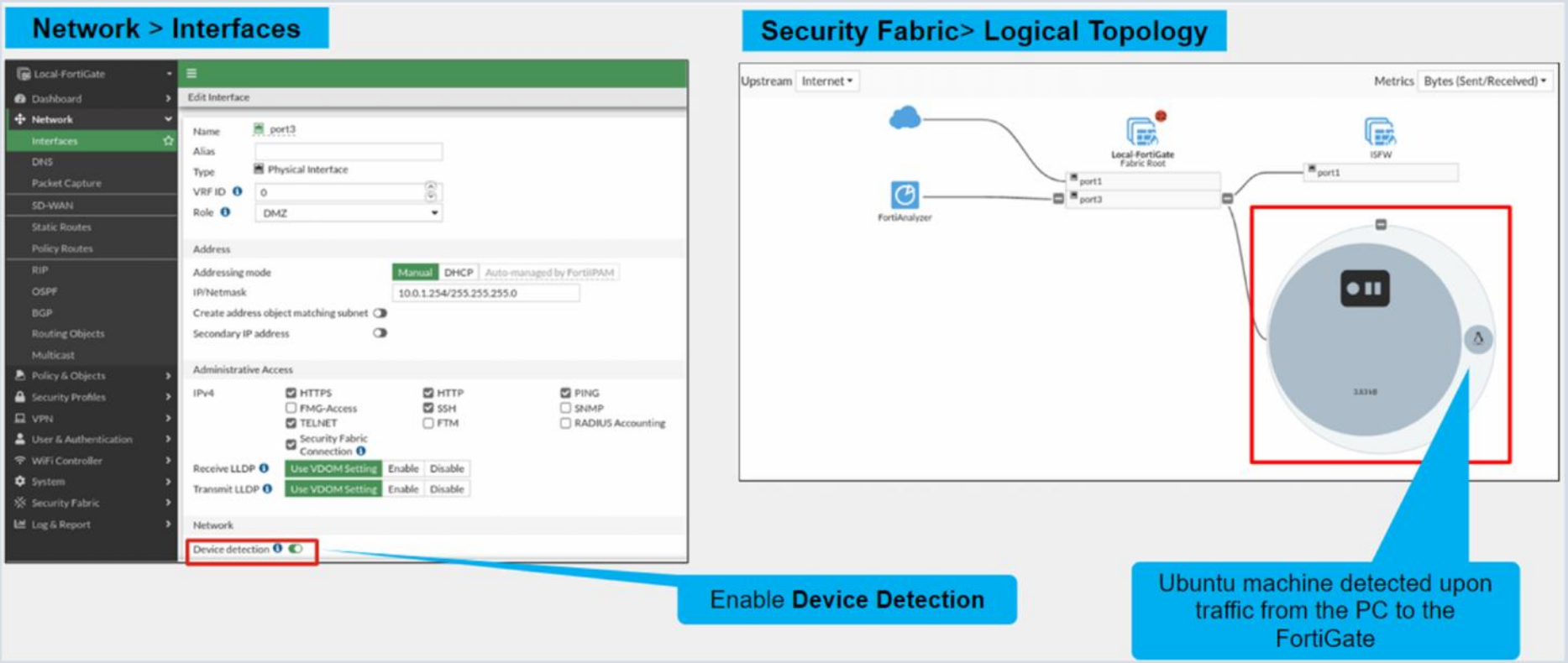
Avec Agent (FortiAgent)

- Equipement suivi par son FortiAgent User ID (unique)



Déploiement d'une Fabric de sécurité

Implémentation | Configuration (suite) | VDOMS | Extension Fabric | Evaluation de la Sécurité

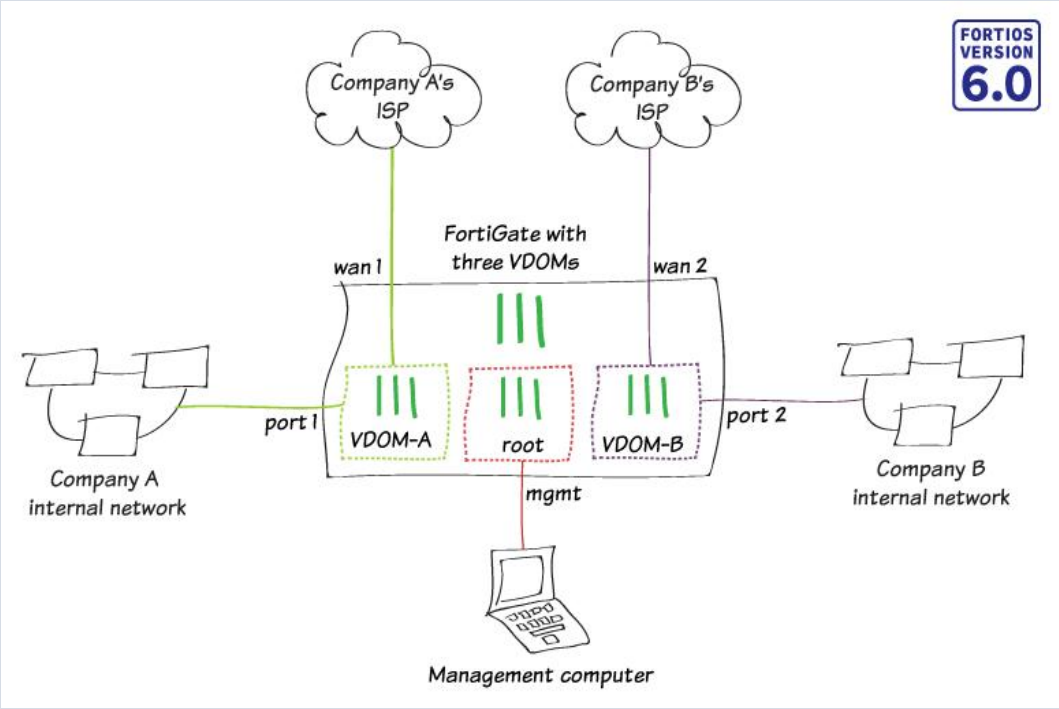


Déploiement d’une Fabric de sécurité

Implémentation Configuration VDOMS Extension Fabric Evaluation de la Sécurité

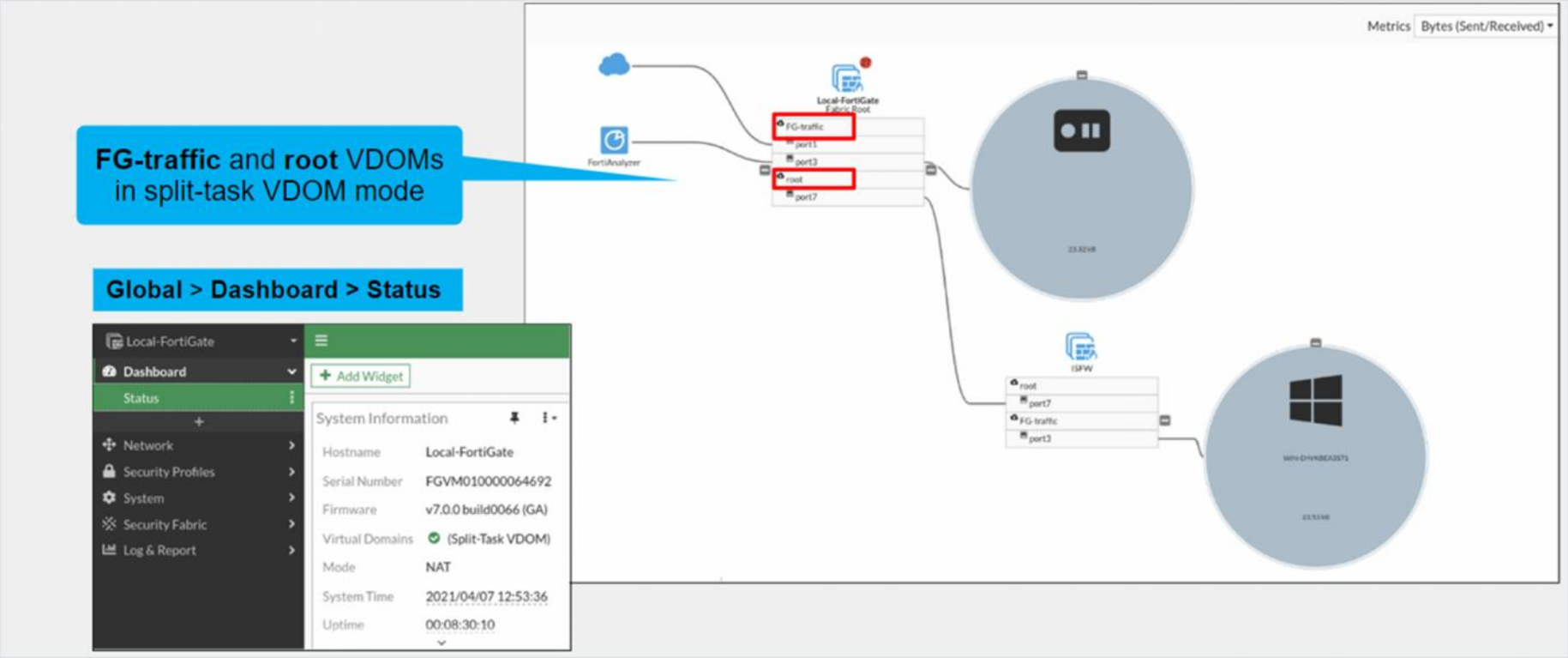
C’est quoi les VDOMs:

- 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.



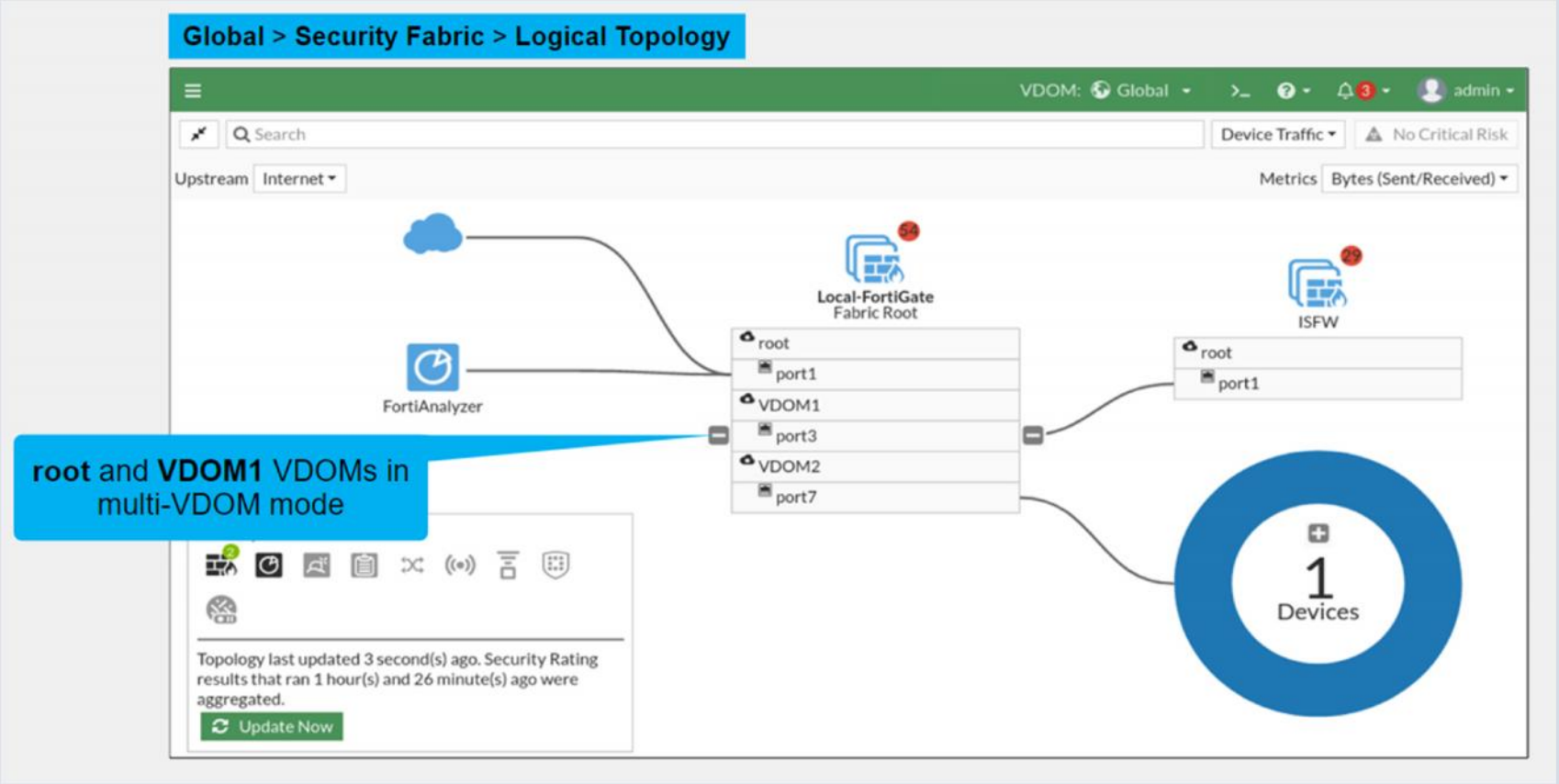
Déploiement d'une Fabric de sécurité

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

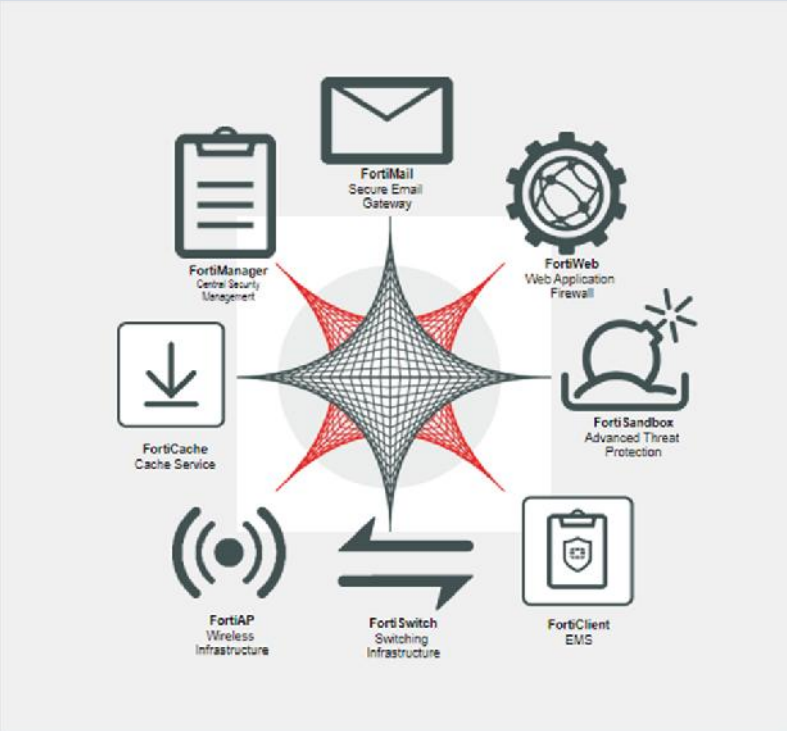
- Etendre une Fabric de sécurité;
- Comprendre les points d’automatisation et la réponse au ménaces;
- Configurer les connecteurs externes ;
- Comprendre le status des widgets de la Fabric.

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’expension de la Fabric au niveau de la couche d’accès;
- ❑ FortiMail;
- ❑ Etc.

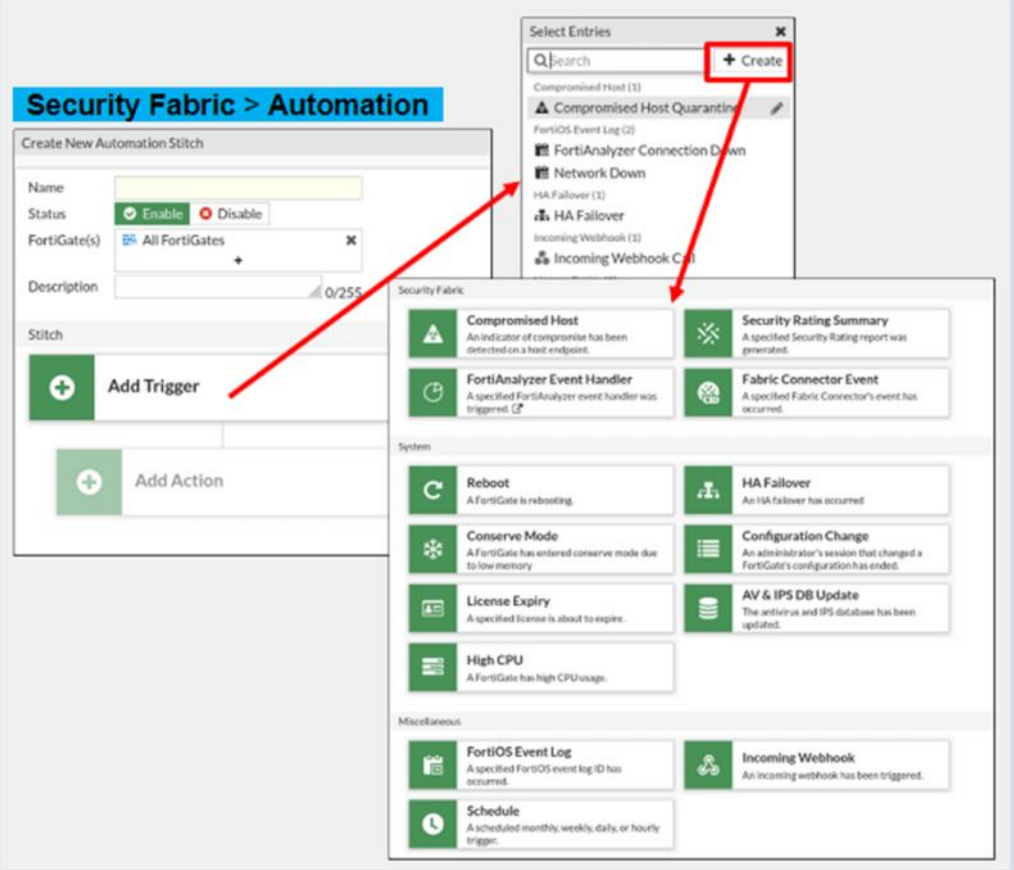


Extension d’un Fabric de sécurité

Extension | Automatisation | Connecteurs externes | Widgets

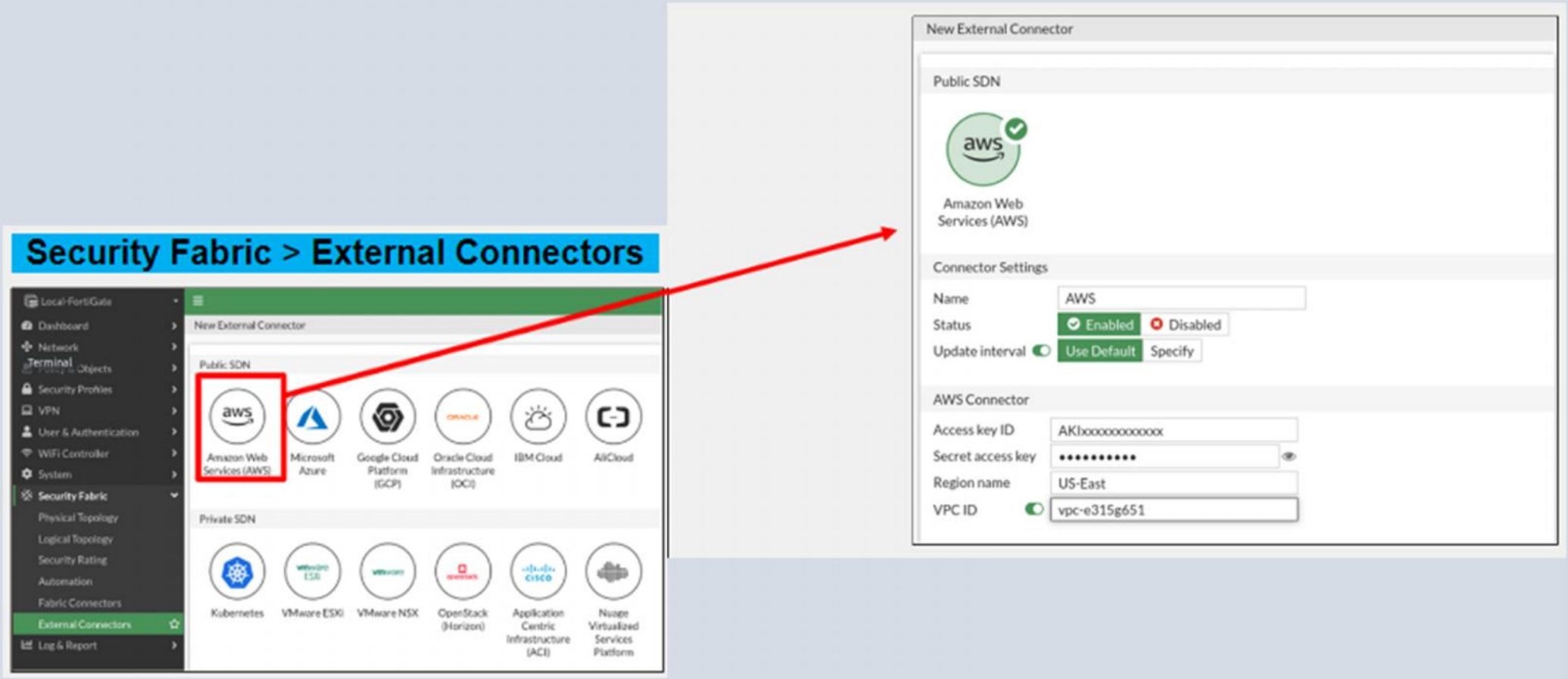
Points d’automatisation (stitches):

- ❑ Actions d’automatisation basées sur les déclencheurs (triggers);
- ❑ Stitches prédéfinies disponibles;
- ❑ Configuration du Minimum interval.



Extension d’un Fabric de sécurité

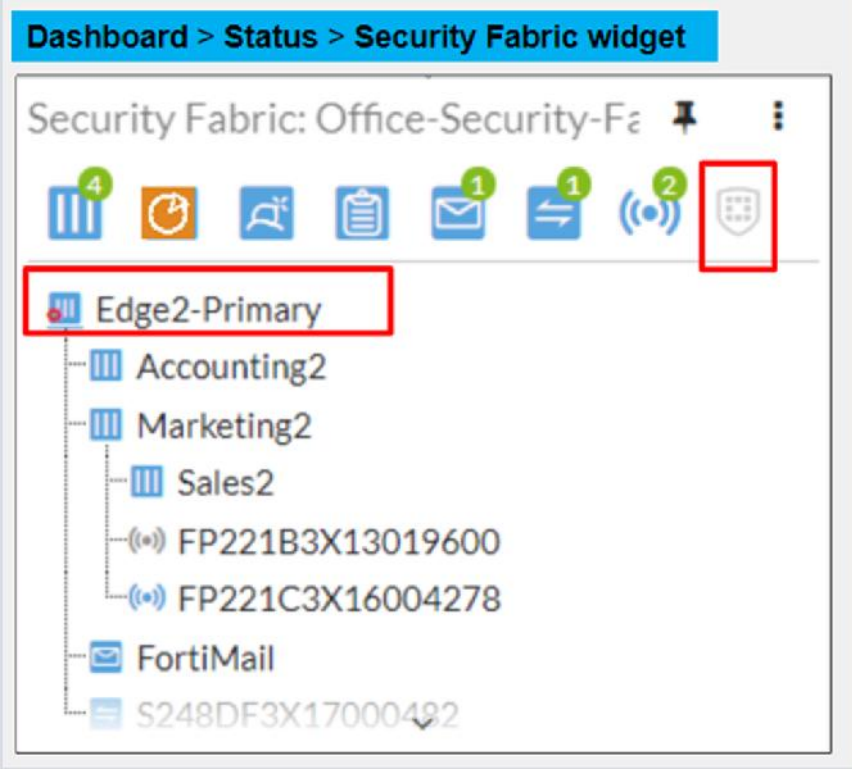
Extension | Automatisation | Connecteurs externes | Widgets



Extension d’un Fabric de sécurité

Extension Automatisation Connecteurs externes Widgets

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




FORTINET®

FORTINET
NSE Training Institute

FortiGate Security

POLITIQUES DE PARE-FEU (FIREWALL POLICIES)

FortiOS 7.0

FORTINET Training Institute

Plan du module

- Vue d’ensemble sur les politiques de pare-feu
- Configuration des politiques de pare-feu
- Gestion des politiques de pare-feu
- Bonnes pratiques et diagnostic

Politiques de pare-feu (Firewall Policies)s

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

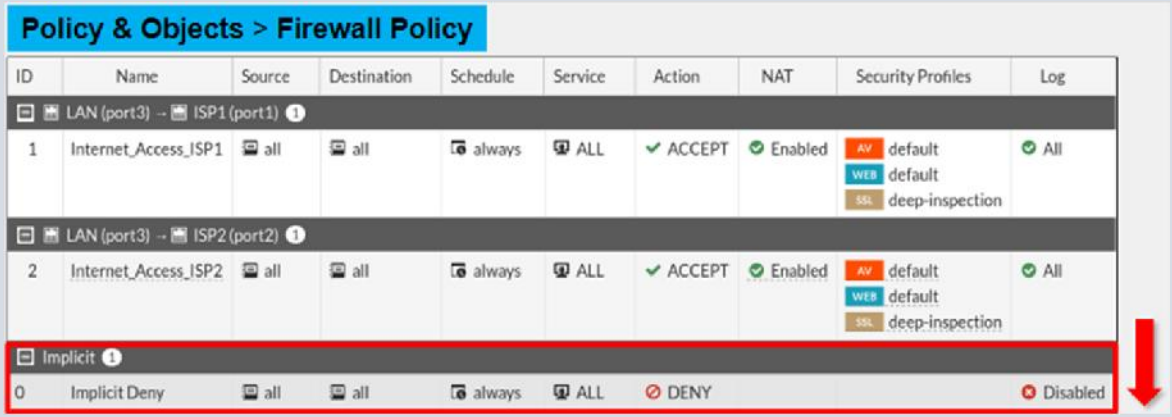
Mécanismes de correspondances de trafic

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



Politiques de pare-feu

Vue d'ensemble (suite)

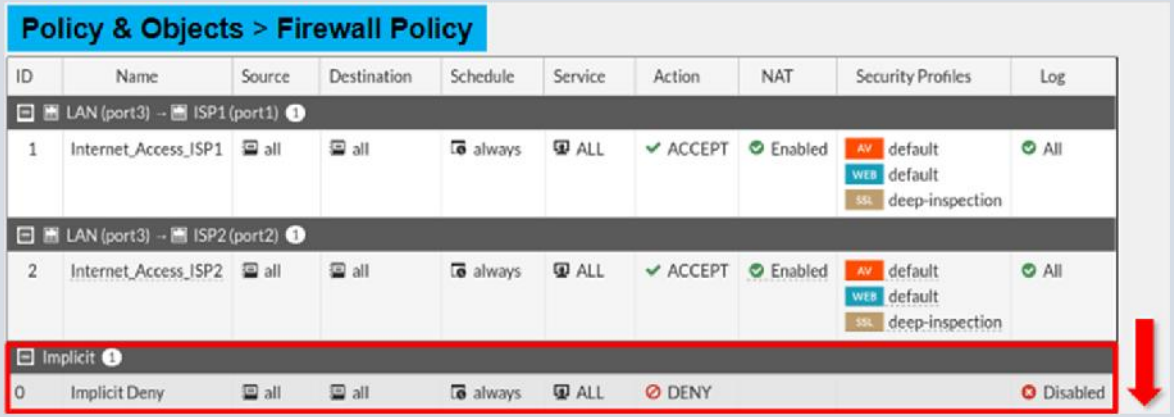
Mécanismes de correspondances de trafic

Composant d'une politique de pare-feu

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

Types:

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



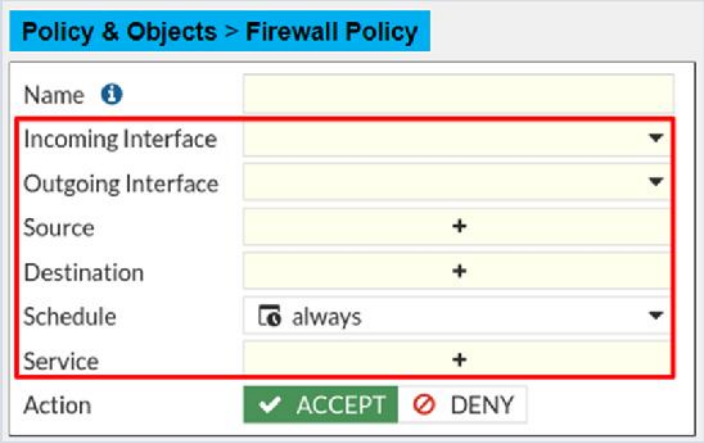
Politiques de pare-feu

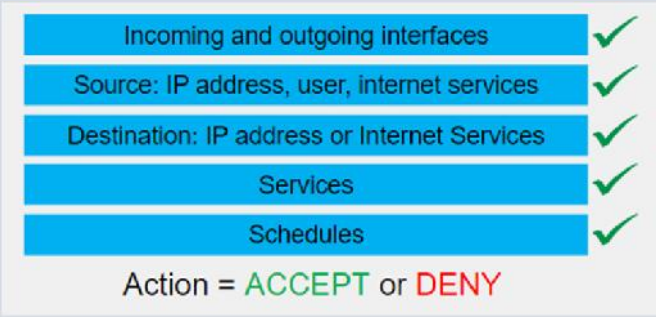
Vue d'ensemble (suite)

Mécanismes de correspondances de trafic

Correspondance de trafic

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





Configuration des politiques de pare-feu

Objectifs

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

Configuration des politiques de pare-feu

Configuration | Logging | Trafic Shapers

Correspondance de trafic

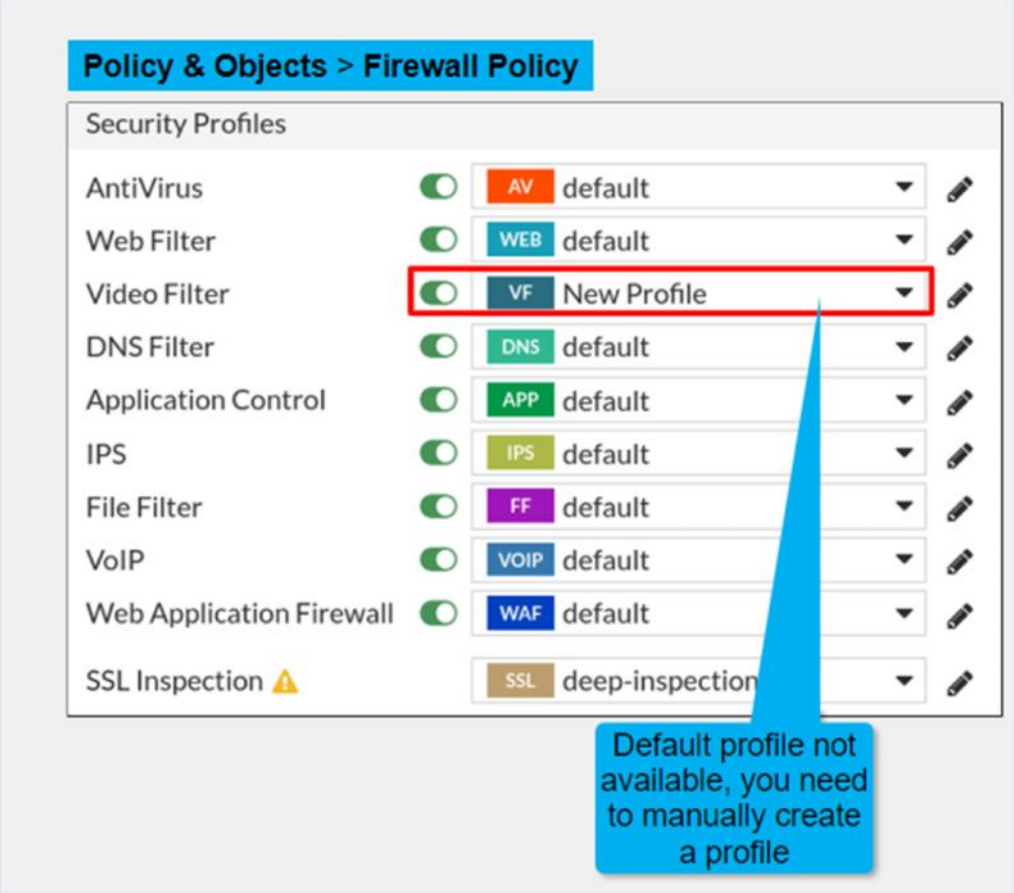
- Interface source;
- Interface de destination;
- IP Source;
- IP destination;
- Service;
- Programmation;
- Action: Accepter / Rejetter

Configuration des politiques de pare-feu

Configuration (suite) Logging Trafic Shapers

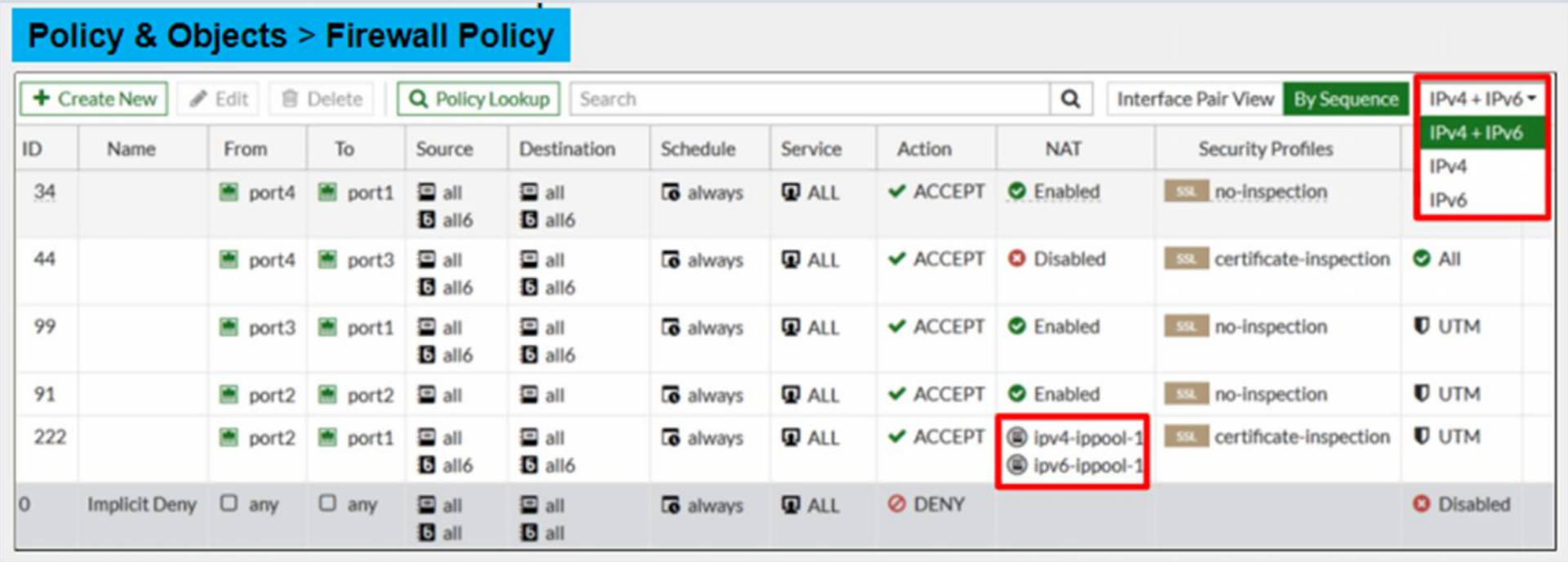
Profils de sécurité

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



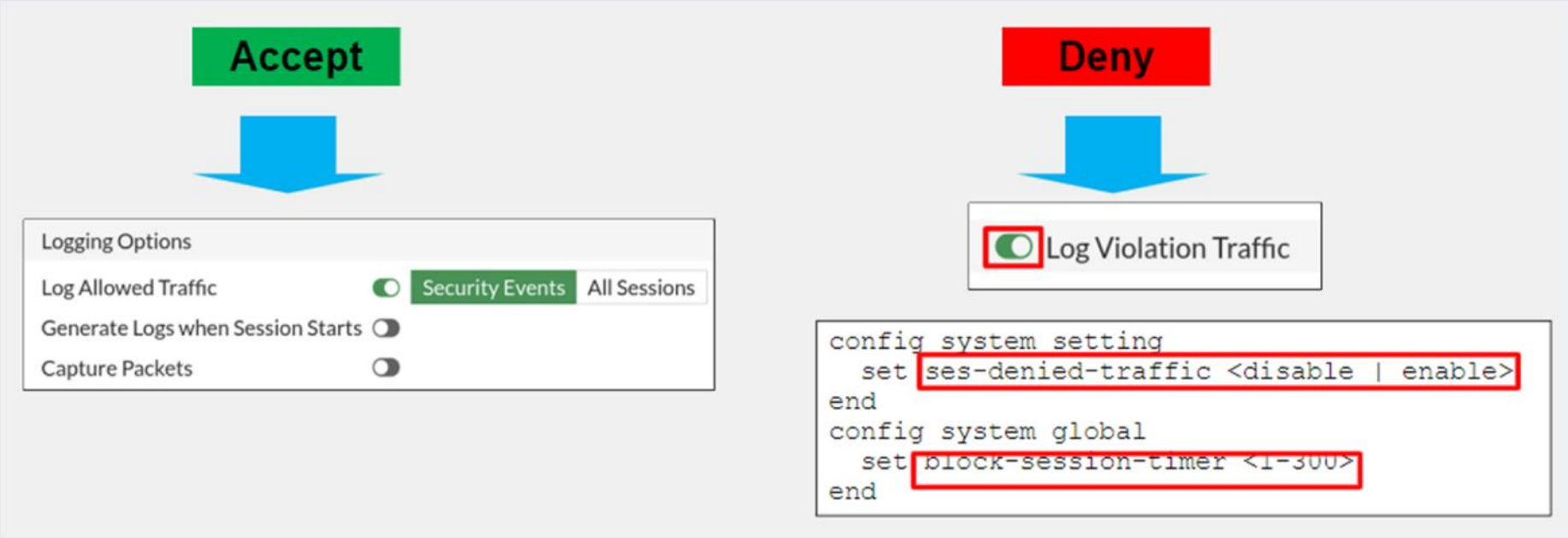
Configuration des politiques de pare-feu

Configuration (suite) Logging Trafic Shapers



Configuration des politiques de pare-feu

Configuration | Logging | Trafic Shapers



Configuration des politiques de pare-feu

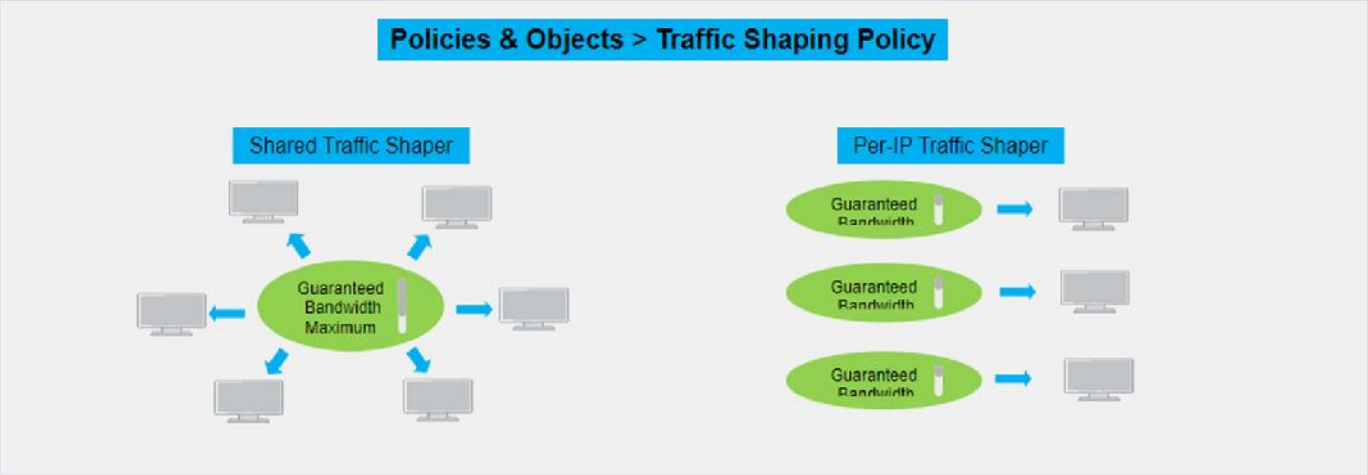
Configuration Logging Trafic Shapers

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

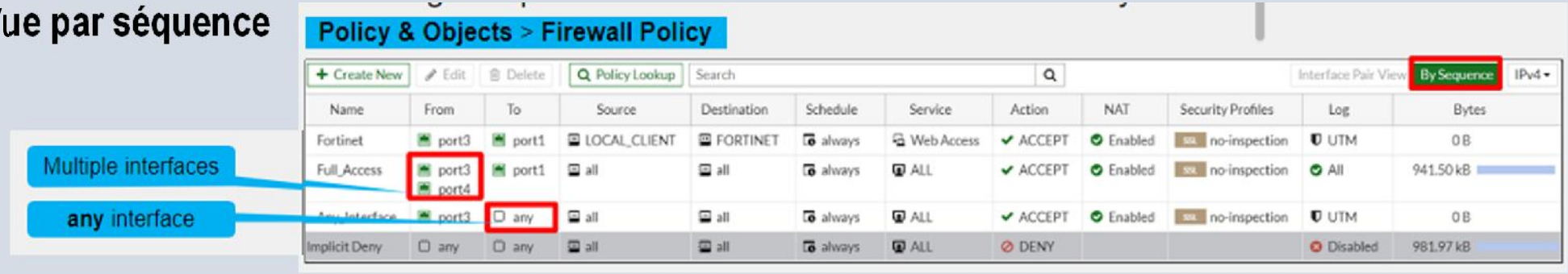
- Modifier les paramètres d'affichage des politiques ;
- Comprendre l'utilisation des IDs des politiques;
- Utilisation des objets.

Gestion des politiques

Affichage | Ids des politiques | Objets

Vue par pair

Vue par séquence

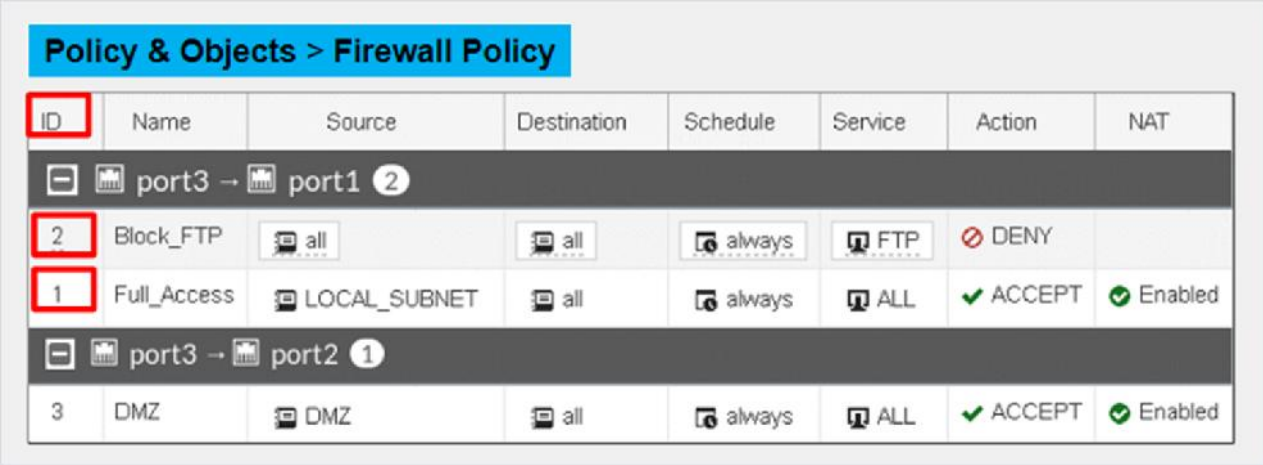


Gestion des politiques

Affichage | Ids des politiques | Objets

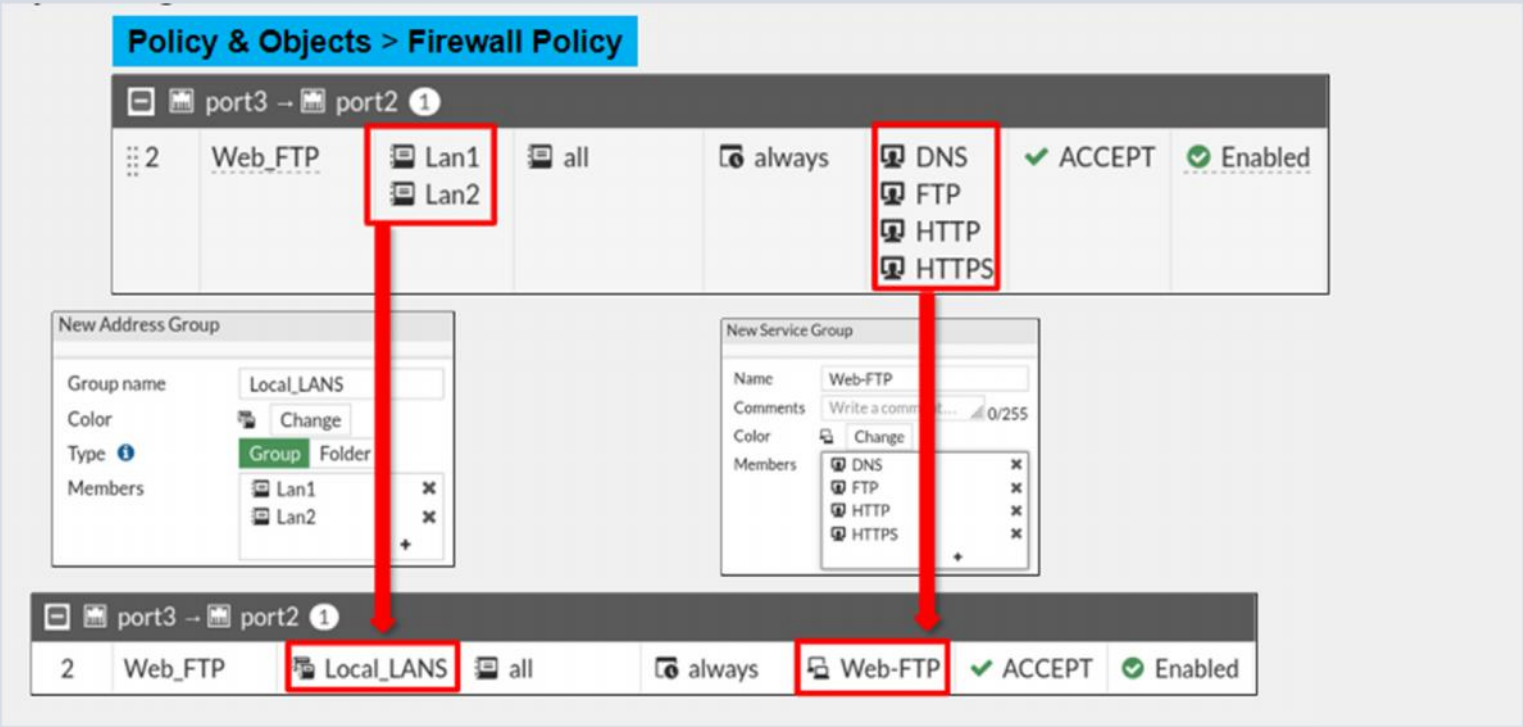
IDs des politiques

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



Gestion des politiques

Affichage Ids des politiques Objets



Quelques bonnes pratiques

Objectifs

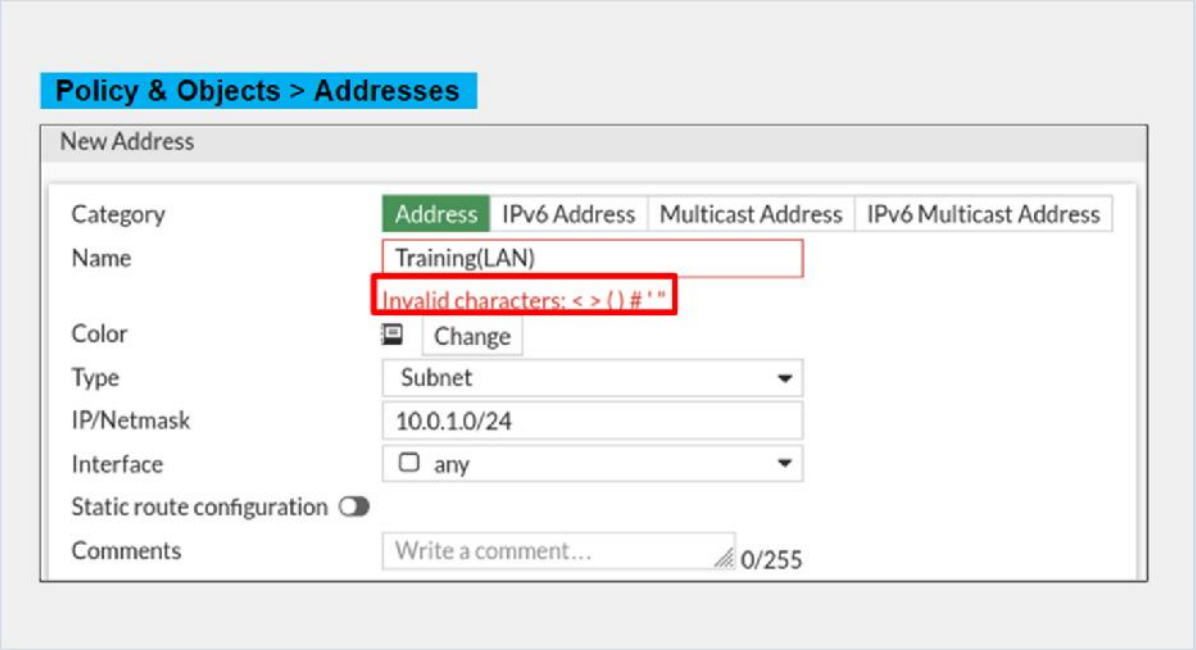
- Identifier les conventions de nommage des politiques et des objets;
- Réordonner les politiques.

Quelques bonnes pratiques

Nommage | Bonnes pratiques | Réorganisation | Recherche

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.

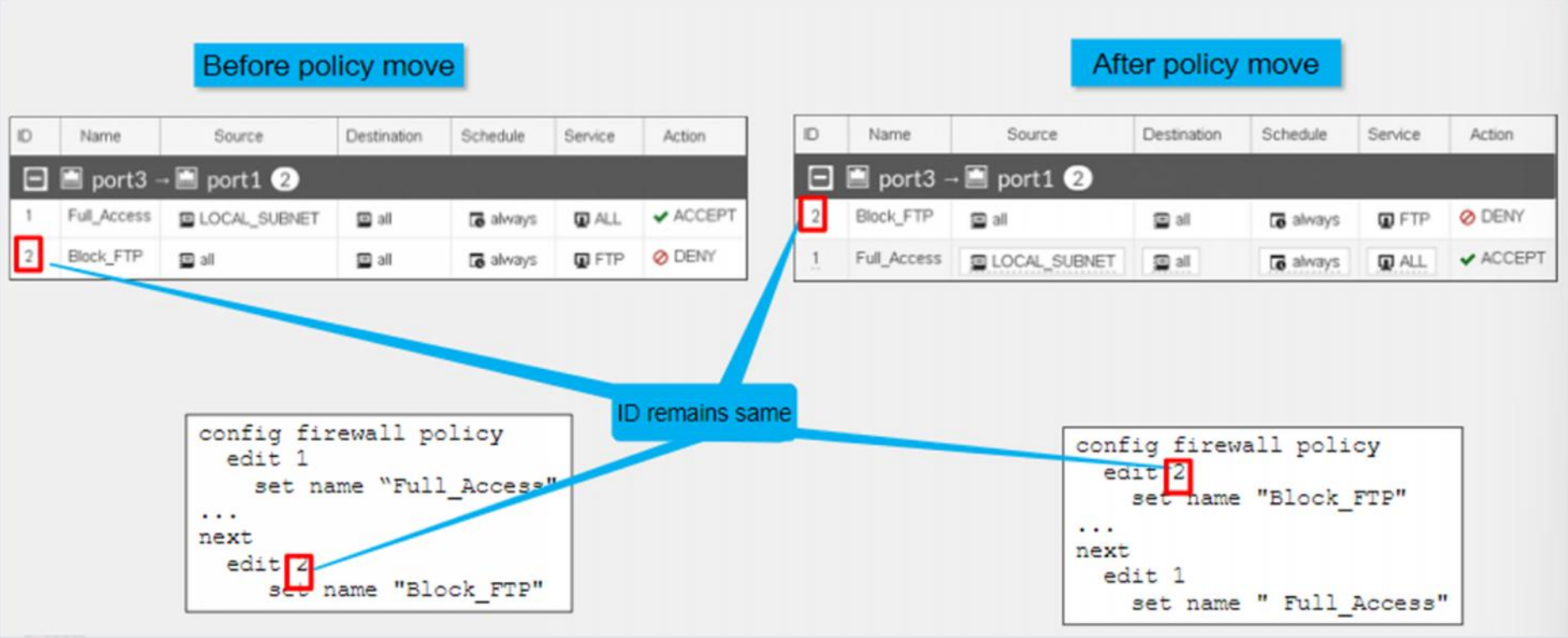


Quelques bonnes pratiques

Nommage | Bonnes pratiques | Réorganisation | Recherche

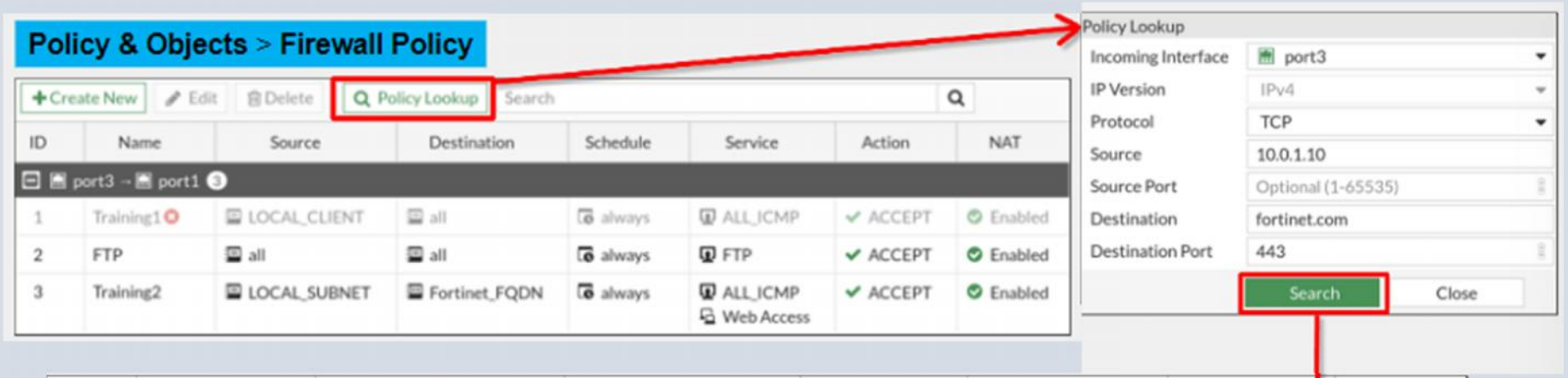
Quelques bonnes pratiques

Nommage | Bonnes pratiques | Réorganisation | Recherche



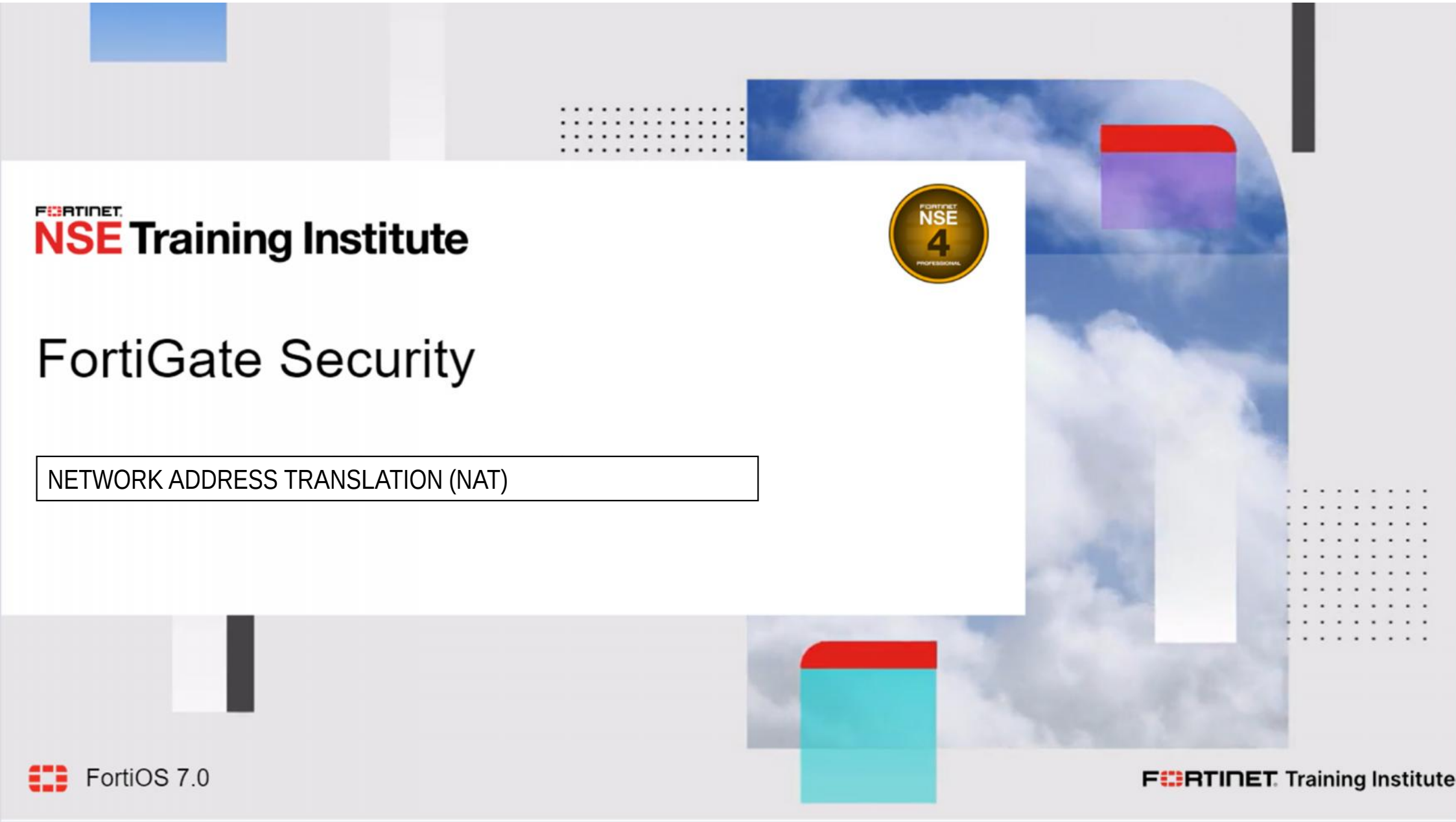
Quelques bonnes pratiques

Nommage Bonnes pratiques Réorganisation Recherche



ID	Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 3							
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


FORTINET®


FORTINET
NSE Training Institute
FortiGate Security
NETWORK ADDRESS TRANSLATION (NAT)
FortiOS 7.0
FORTINET Training Institute

Plan du module

- Introduction au NAT
- Politiques de NAT
- NAT Central
- Sessions
- Bonnes pratiques

Introduction au NAT

Objectifs

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

Introduction au NAT

NAT/PAT

Modes de configuration

NAT (Network Address Translation):

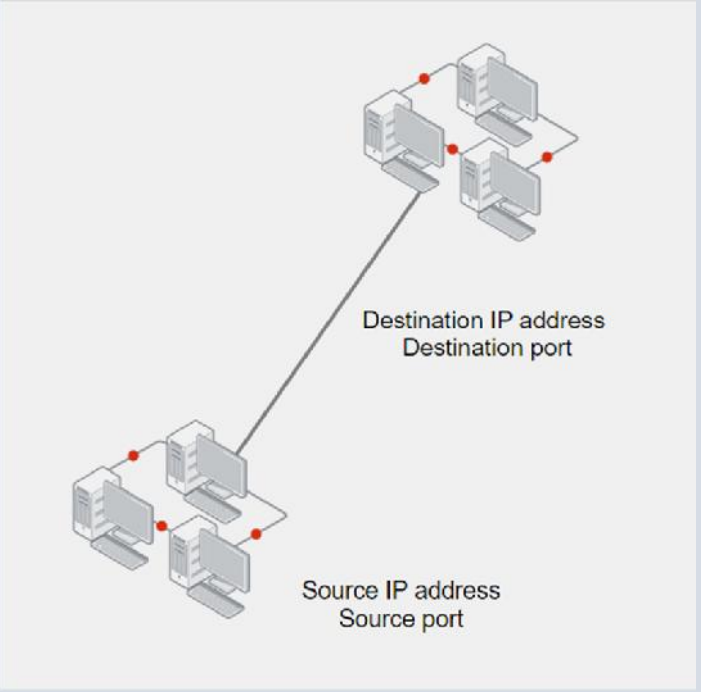
- Mécanisme permettant d'associer à une IP publique un (one to one) ou plusieurs adresse privées (one to many);
- Permet à un équipement d'agir comme agent de relai entre Internet et le réseau interne;
- NAT Source (SNAT);
- NAT Destination (DNAT).

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 utilisé une seul adresse
- Etc;



Introduction au NAT

NAT/PAT (suite)

Modes de configuration

Dans FortiOS:

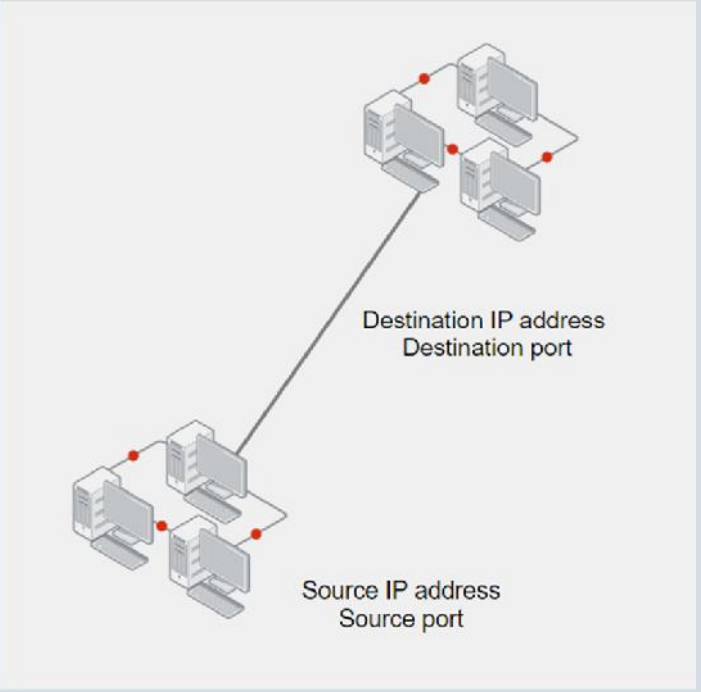
- Appliqué dans la même firewall policies;
- Connexion sortante: NAT Central (SNAT) fonction de l'implémentation;
- Connexion entrante: Virtual IP (DNAT).

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

Modes de configuration

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 dépuis le panneau de politiques de SNAT Central;
  - DNAT sont configurés dépuis le panneau DNAT et VIPs.

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.

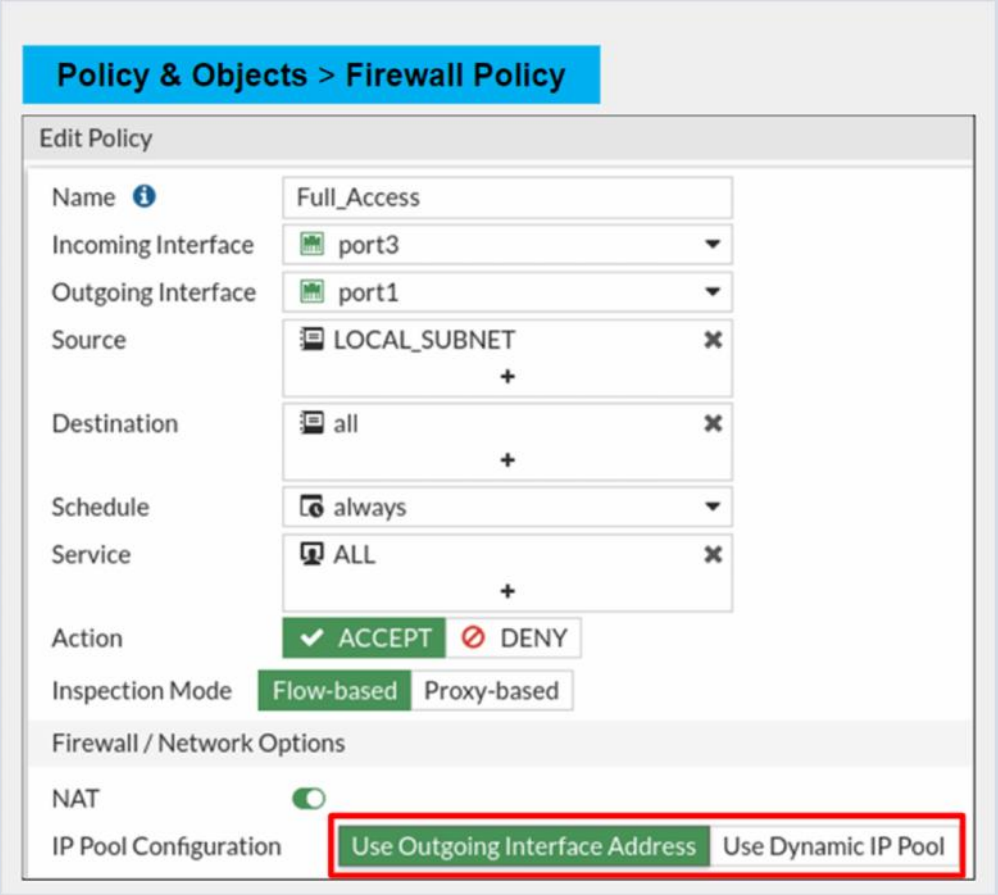
Politique de NAT

SNAT

DNAT

Configuration du SNAT:

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

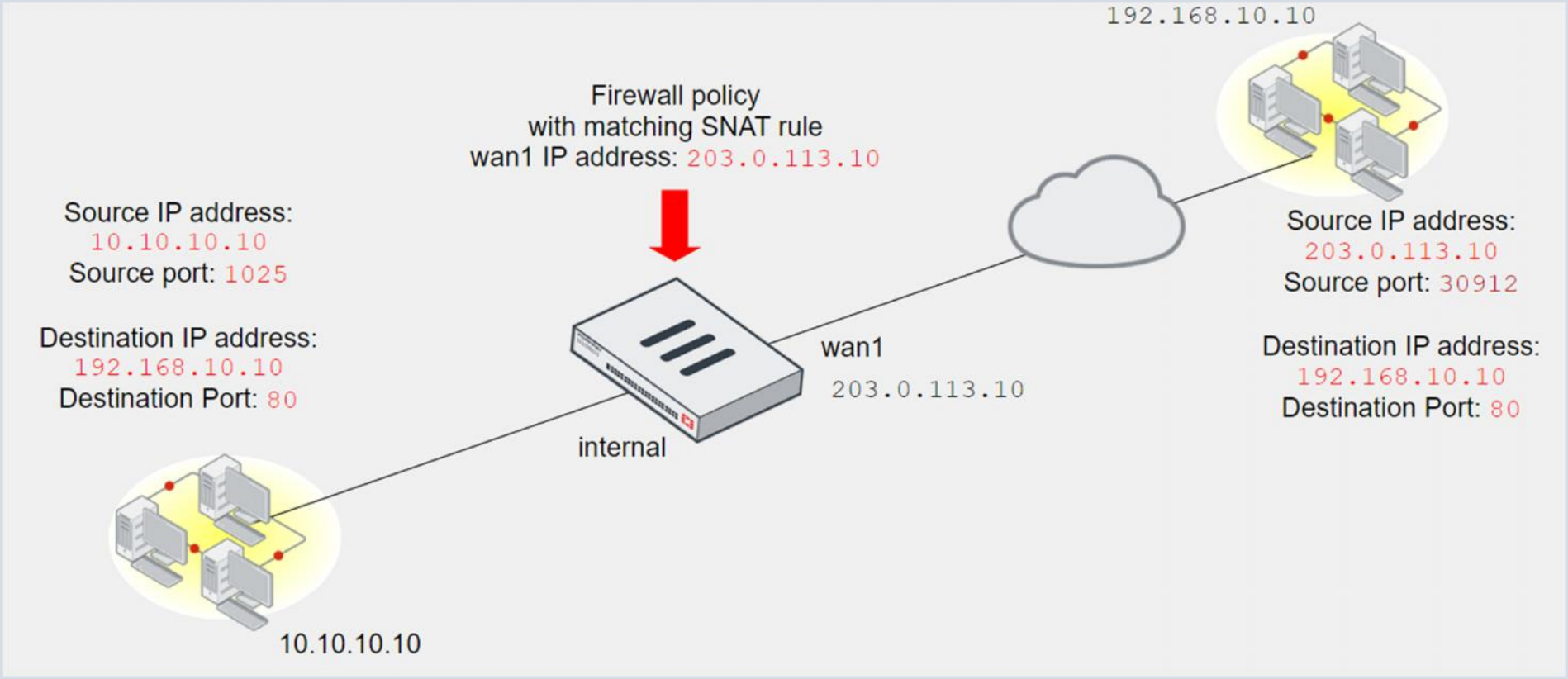


Politique de NAT

SNAT (suite)

DNAT

Utilisation de l'interface de sortie



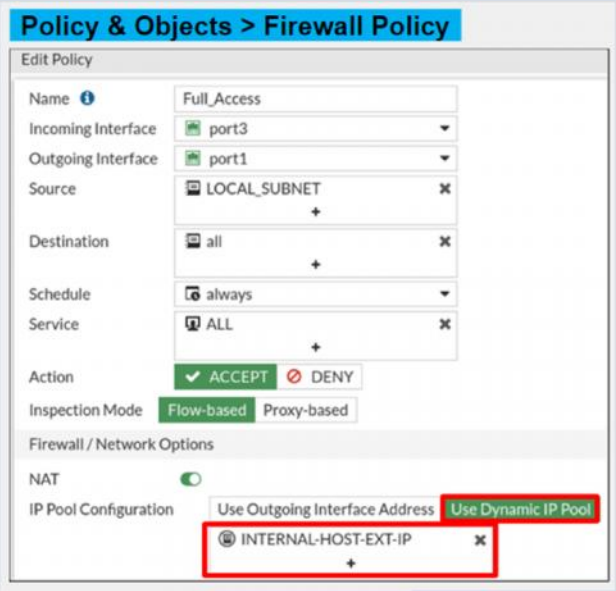
Politique de NAT

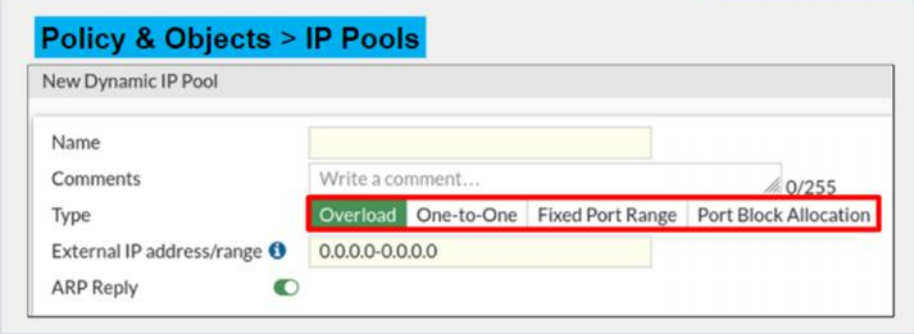
SNAT (suite)

DNAT

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.



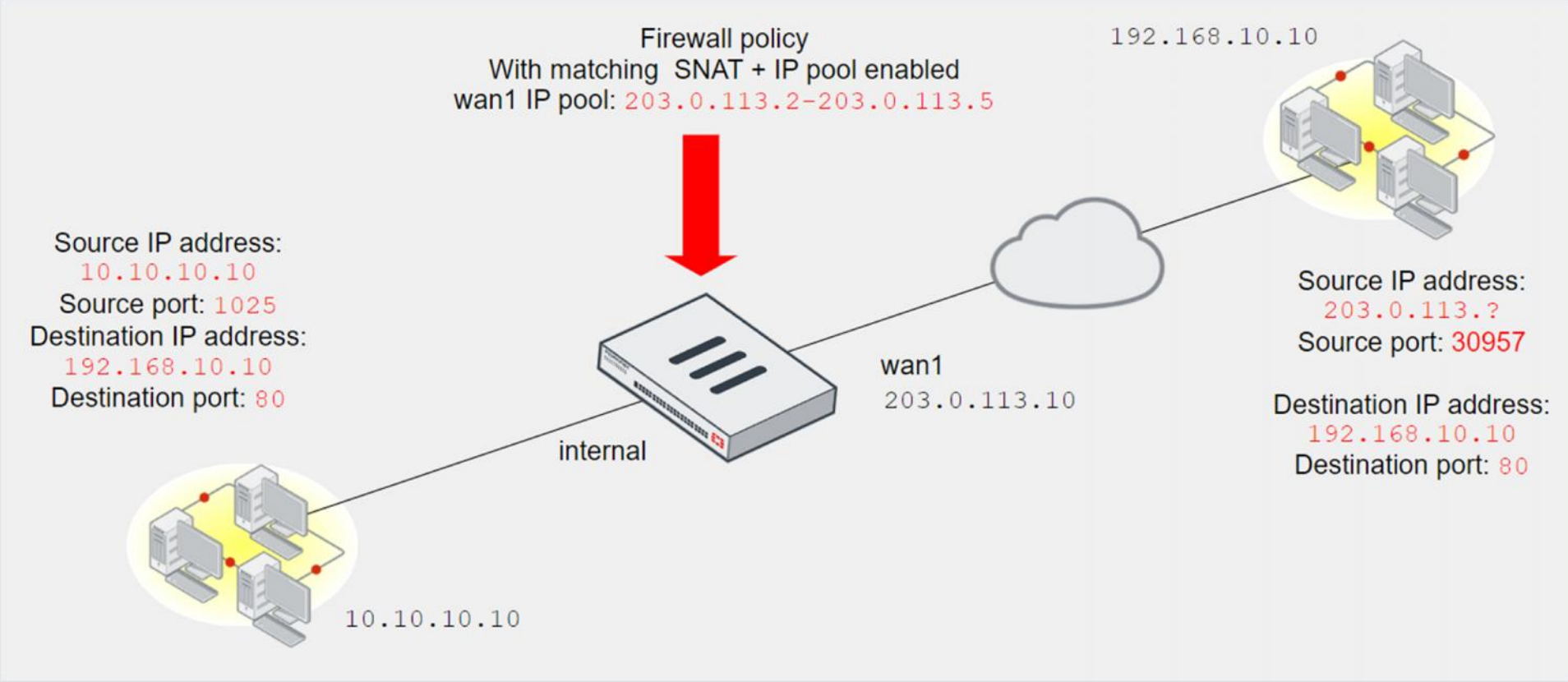


Politique de NAT

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    -
```

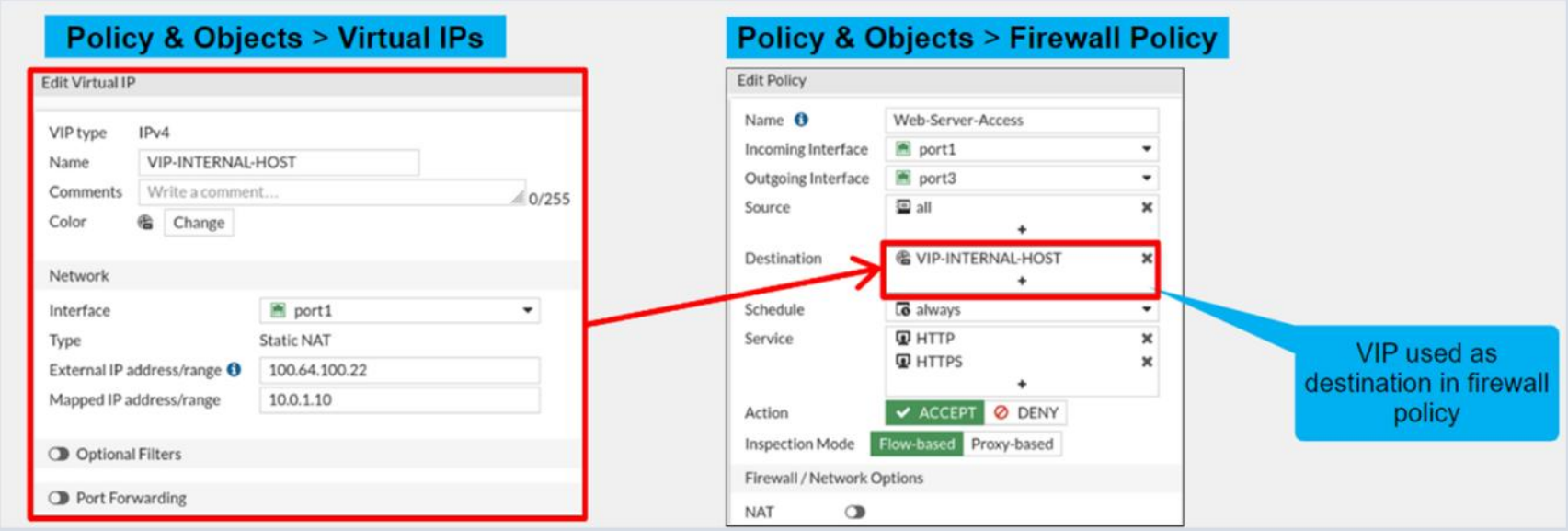
Politique de NAT

SNAT (suite)

DNAT

VIPs:

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



NAT Central

Objectifs

- Configurer le NAT Central

NAT Central

Vue d'ensemble

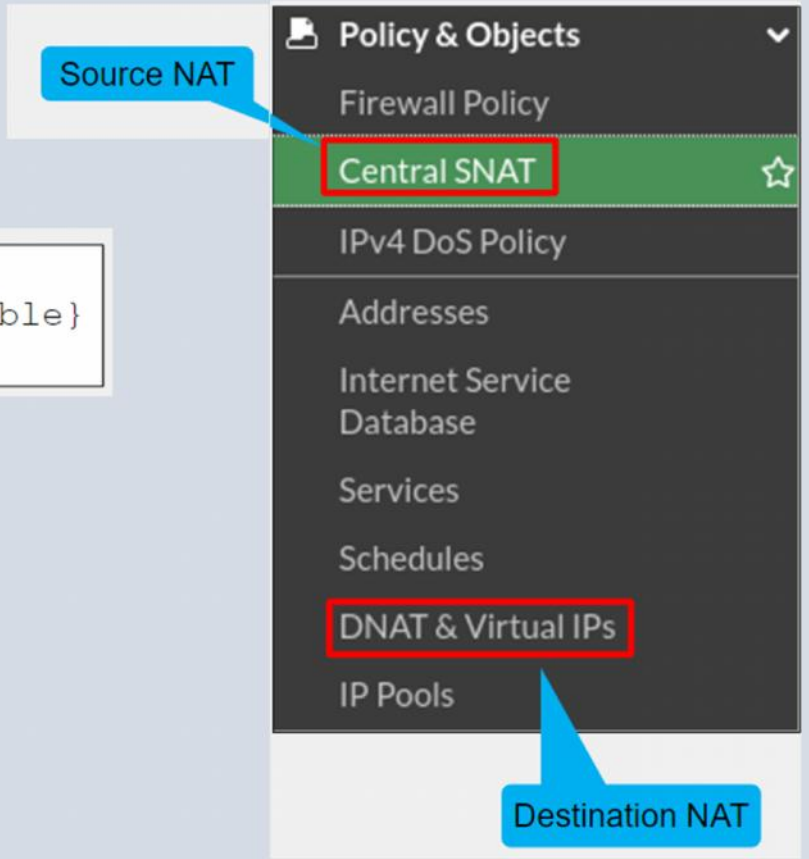
Central NAT

- Gestion des configuration de NAT de façon centralisée;
- Activation en CLI uniquement;

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

- 02 options:
  - Central NAT;
  - DNAT & Virtual IP.
- Obligatoire pour mode policy-base.

Central DNAT&VIPs



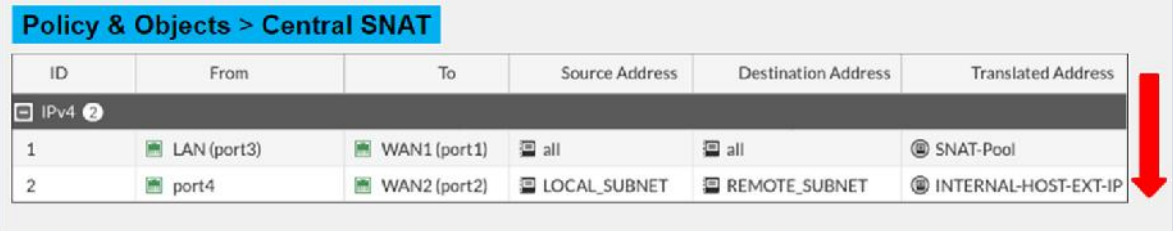
NAT Central

Vue d'ensemble (suite)

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 appliqué si aucune correspondance;
- Critère de correspondance: interface source, interface de destination, adresse source, adresse de destination, protocole, ports (source).

Central DNAT&VIPs

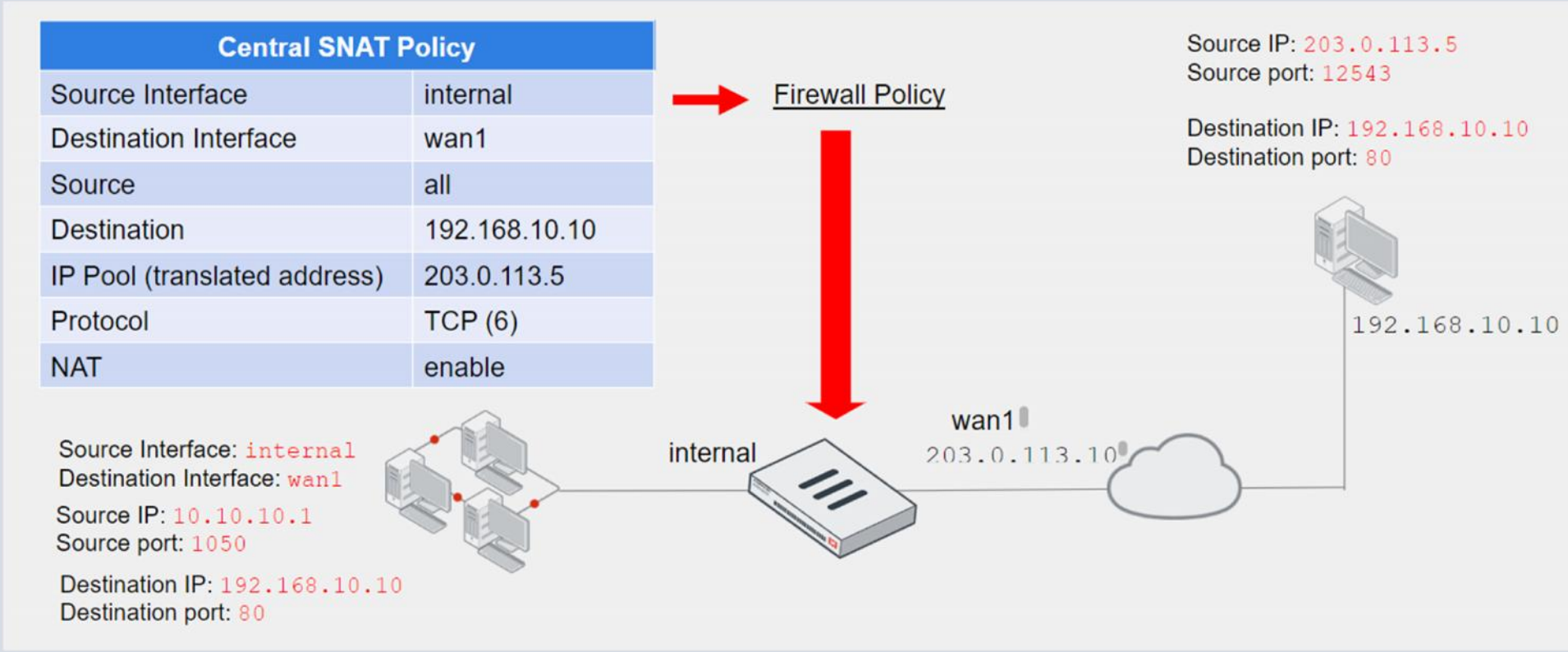


NAT Central

Vue d'ensemble (suite)

Central DNAT&VIPs

Central SNAT Policy	
Source Interface	internal
Destination Interface	wan1
Source	all
Destination	192.168.10.10
IP Pool (translated address)	203.0.113.5
Protocol	TCP (6)
NAT	enable



NAT Central

Vue d'ensemble

Central DNAT&VIPs

Central DNAT

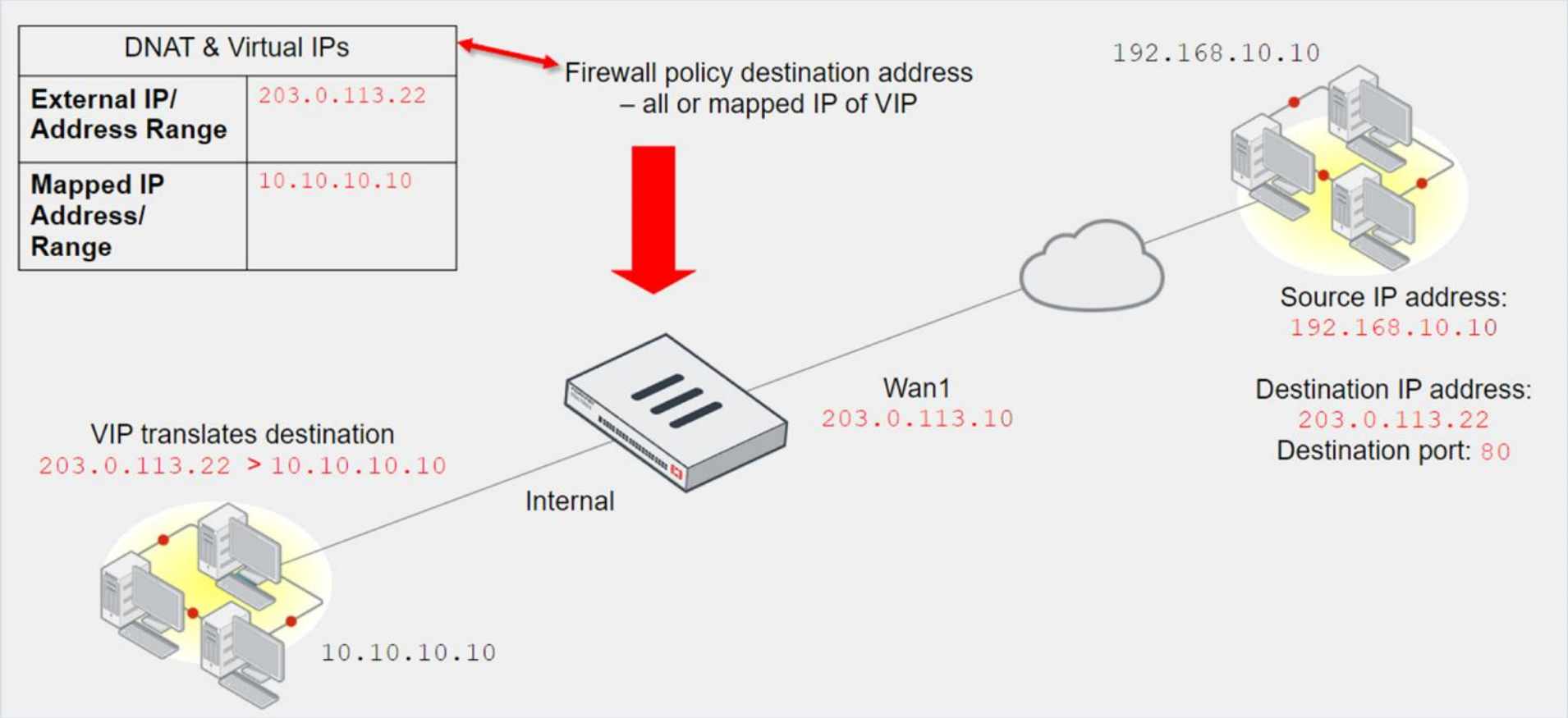
- Modifie les configurations du DNAT;
  - Définition des DNAT & Virtual IPs
- Création d'une règle au niveau du noyau;
  - VIP comme adresse de destination;
- Désactivation permet l'exclusion d'une VIP;

```
#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;

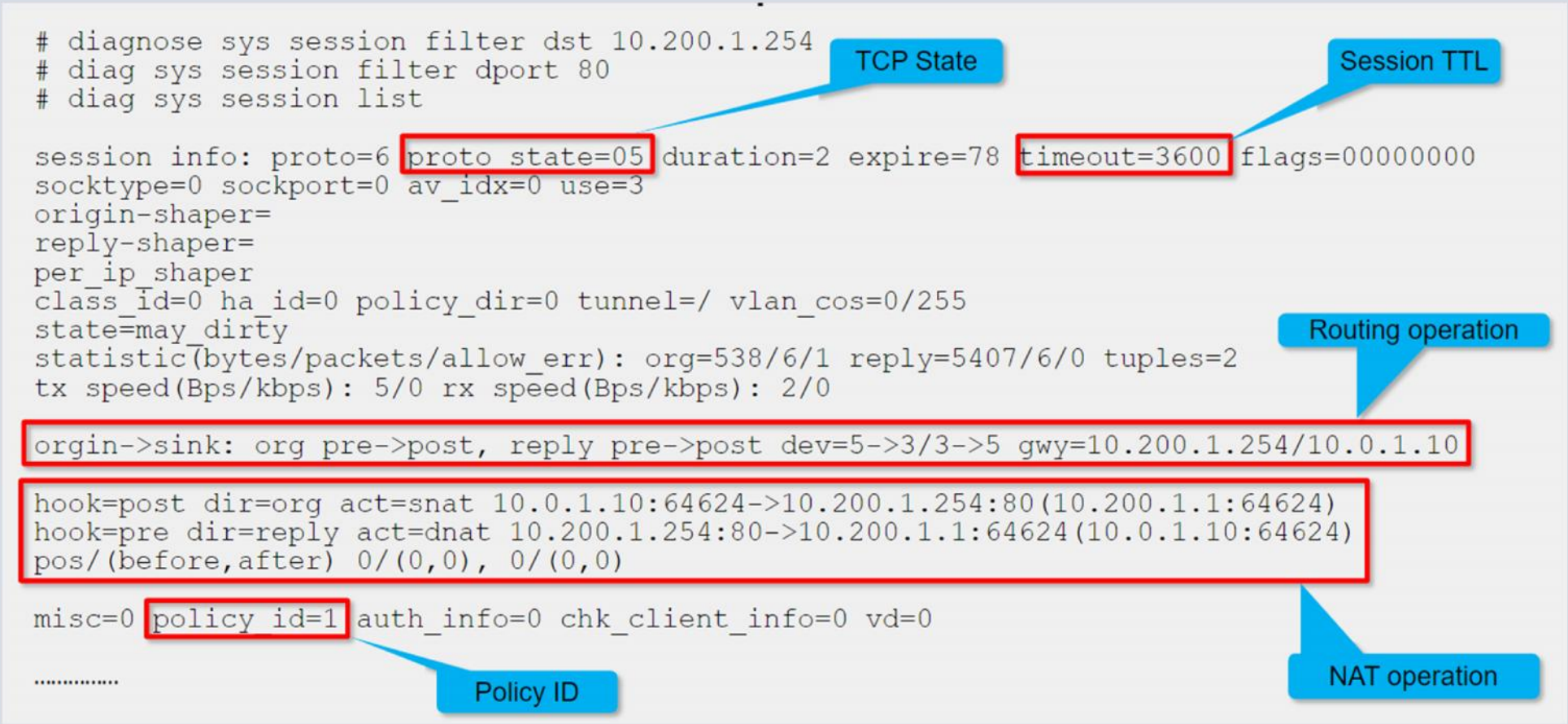
```
diagnose sys session filter ?
dport  Destination port
dst    Destination IP address
policy Policy ID
sport  Source port
src    Source IP address
```

```
diagnose sys session list
```

```
diagnose sys session clear
```

Sessions

Table de session | Session TTL | Diagnostic des sessions | Etat des protocoles



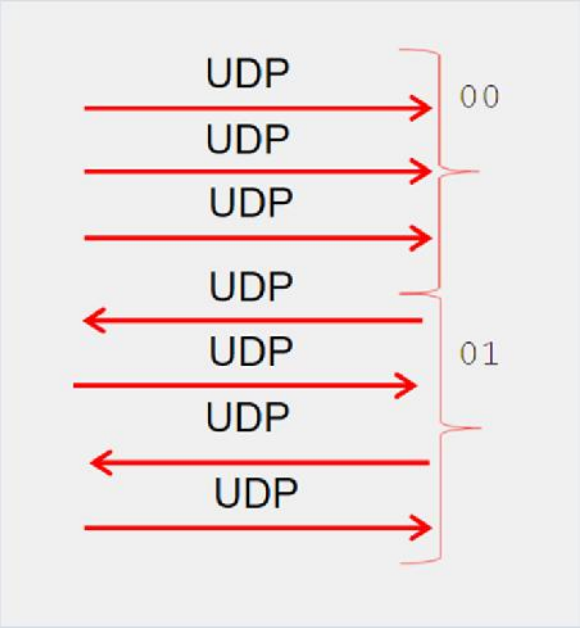

```
# diagnose sys session filter dst 10.200.1.254
# diag sys session filter dport 80
# diag sys session list

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

orgin->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

.....
```

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 commun;
- 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 effecteur 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."
```

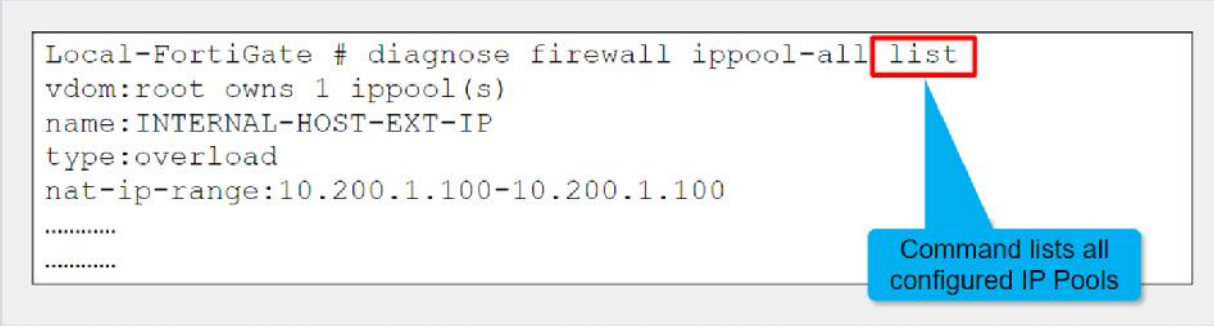
Résolution:

- 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

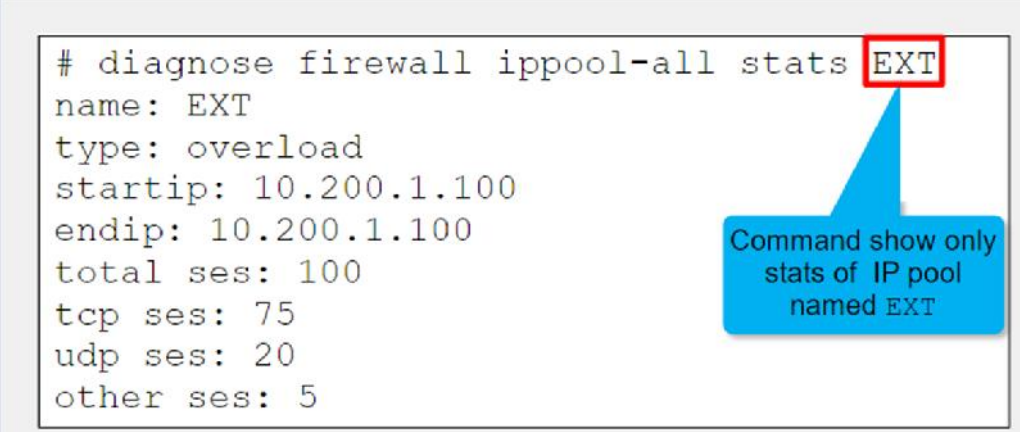
Afficher tous les pools IP (type et interval):

- diagnose firewall ippool-all list;



Afficher les stats d'un pools IP déterminé:

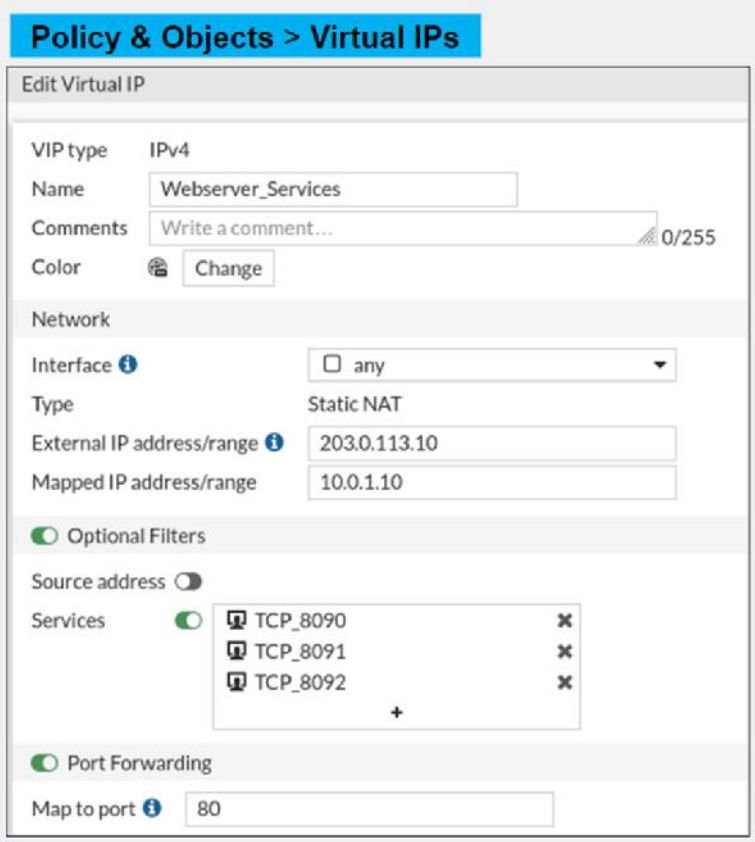
- diagnose firewall ippool-all stats <ippool>;



Quelques bonnes pratiques

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.



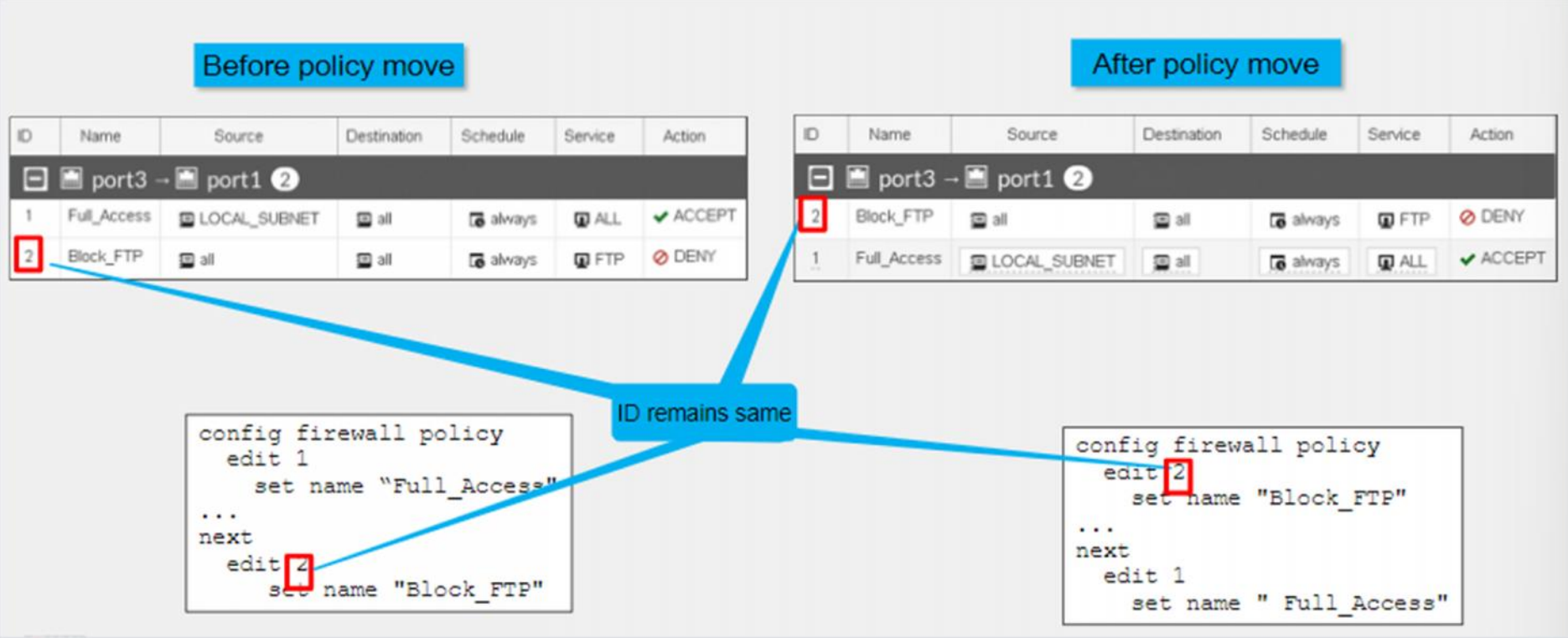
Quelques bonnes pratiques

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

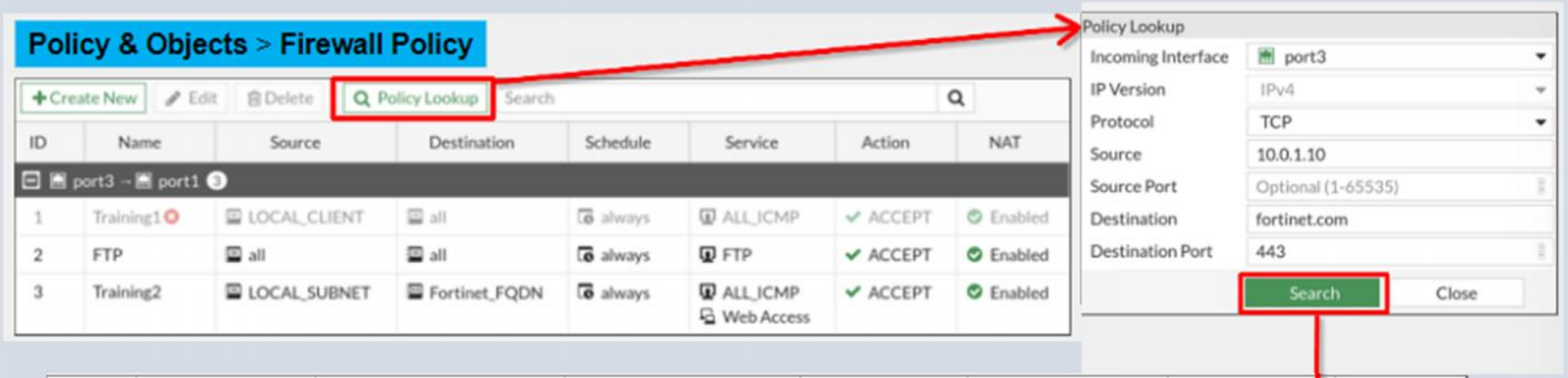
Quelques bonnes pratiques

Nommage | Bonnes pratiques | Réorganisation | Recherche



Quelques bonnes pratiques

Nommage Bonnes pratiques Réorganisation Recherche



ID	Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 3							
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


FORTINET®

FORTINET
NSE Training Institute

FortiGate Security

AUTHENTIFICATION, GESTION DES LOGS & MONITORING ET GESTION DES CERTIFICATS

FortiOS 7.0

FORTINET Training Institute

Plan du module

Authentification Firewall

Objectifs

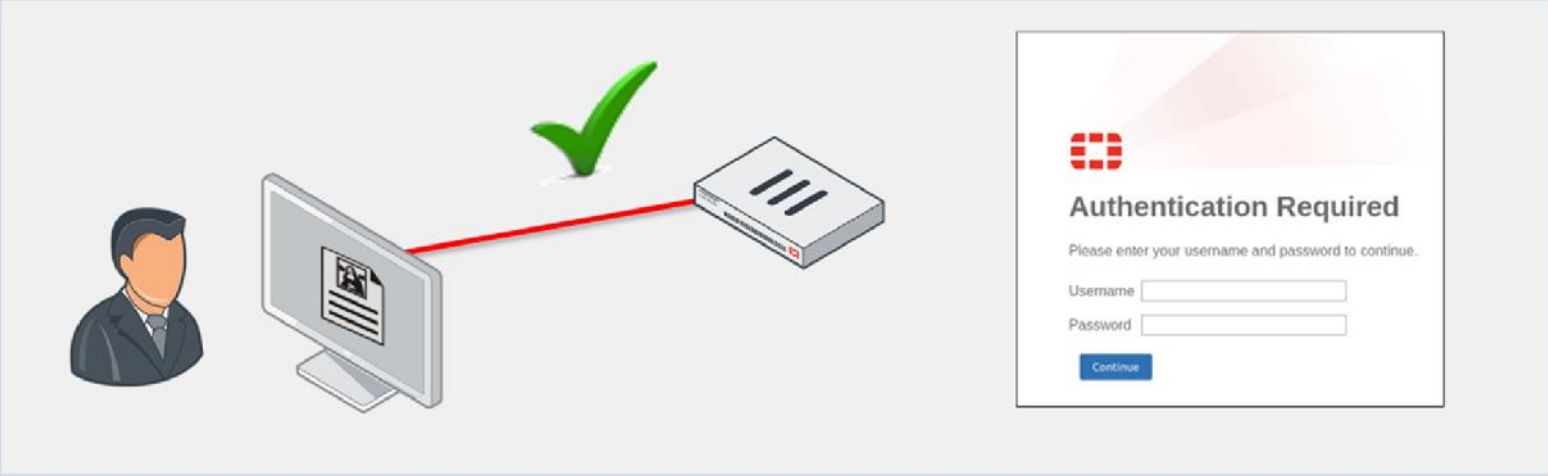
- Identifier les méthodes d’authentification pare-feu;
- Comprendre l’authentification utilisant les politiques pare-feu;
- Comprendre l’authentification via le portail captif;
- Monitoring et diagnostic.

Authentification Firewall

Authentification | Authentification avec politiques | Authentification via portail captif | Monitoring&Diagnostic

Authentification firewall?

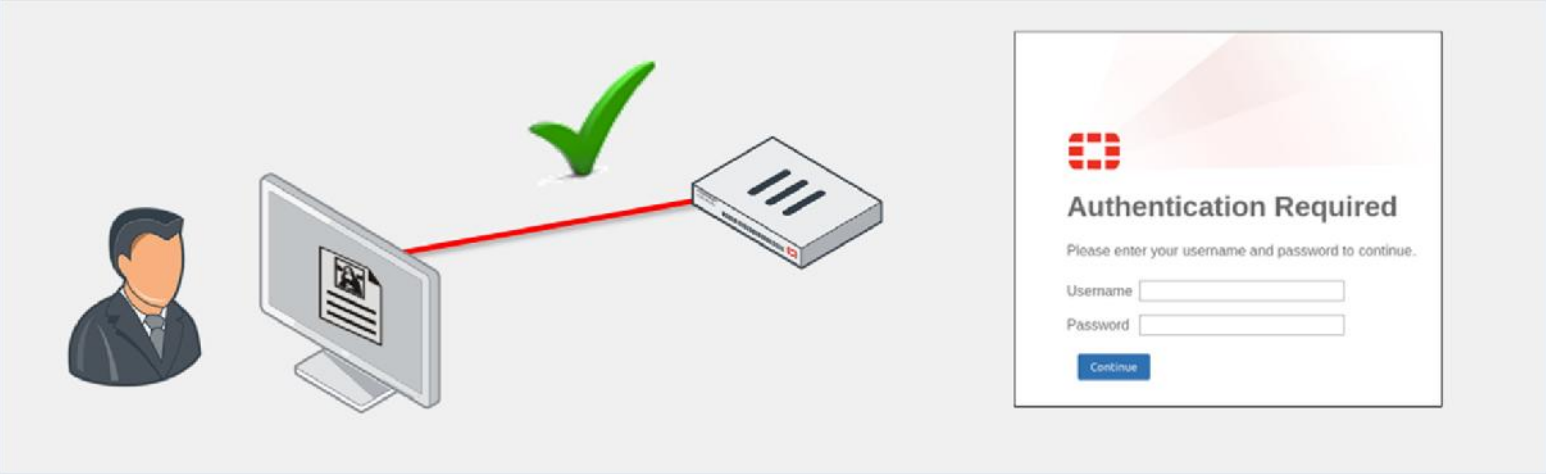
- Autorisation de l'accès par vérification de l'IP source et de l'équipement (traditionnel);
- Impossible de déterminer l'utilisateur de l'équipement;
- Authentification des utilisateurs / groupes;
- Application des politiques et profils de sécurité pour autoriser/interdire l'accès à une ressource.



Authentification Firewall

Méthode d'authentification:

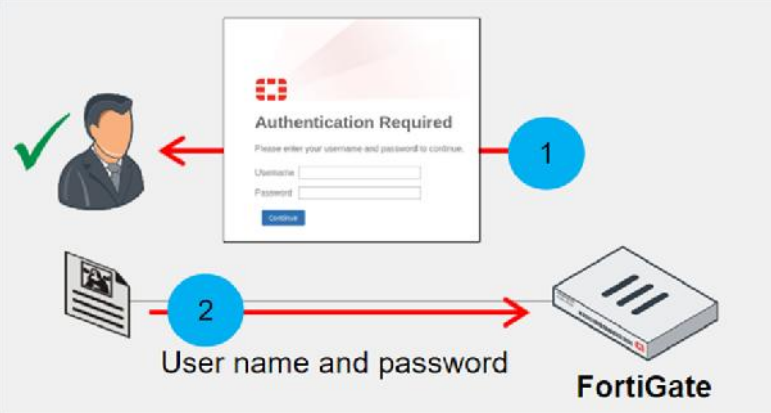
- Authentification avec les paramètres locaux: Login et mot de passe enregistrés dans la base de données interne du FortiGate;
- Authentification à distance: les credentials sont sauvegardés dans un serveur d'authentification (RADIUS, TACACS+, LDAP, etc.);
- Authentification à 02 facteurs: activer avec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

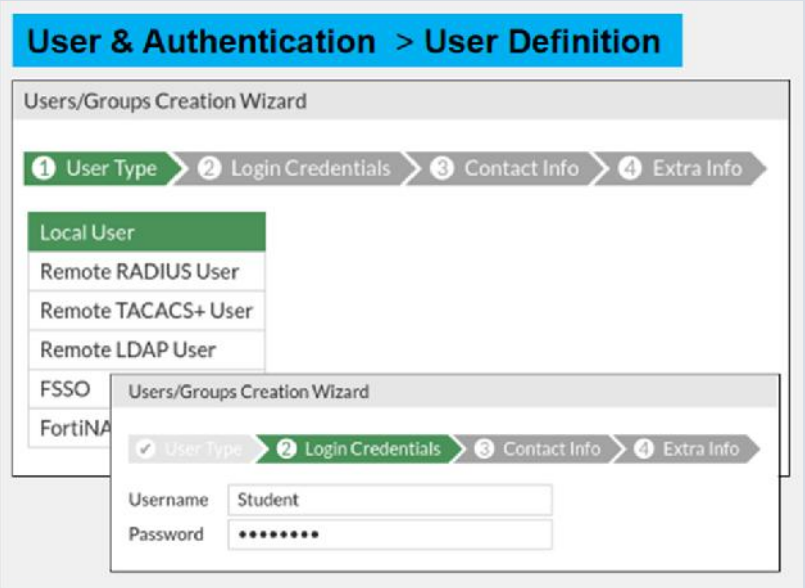


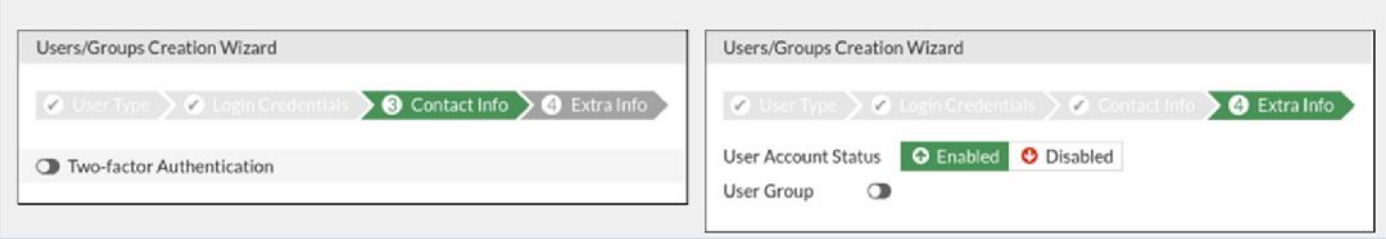
Authentification Firewall

Méthode d'authentification: Utilisation des paramètres locaux

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





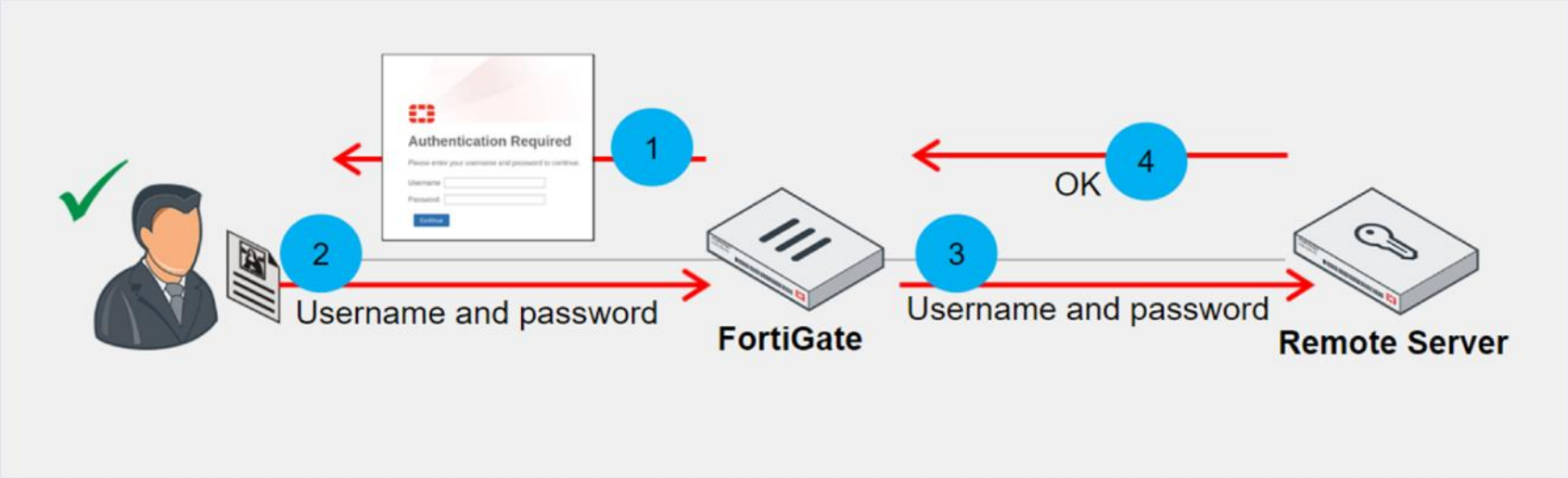


Authentification Firewall

Authentification (suite) Authentification avec politiques Authentification via portail captif Monitoring&Diagnostic

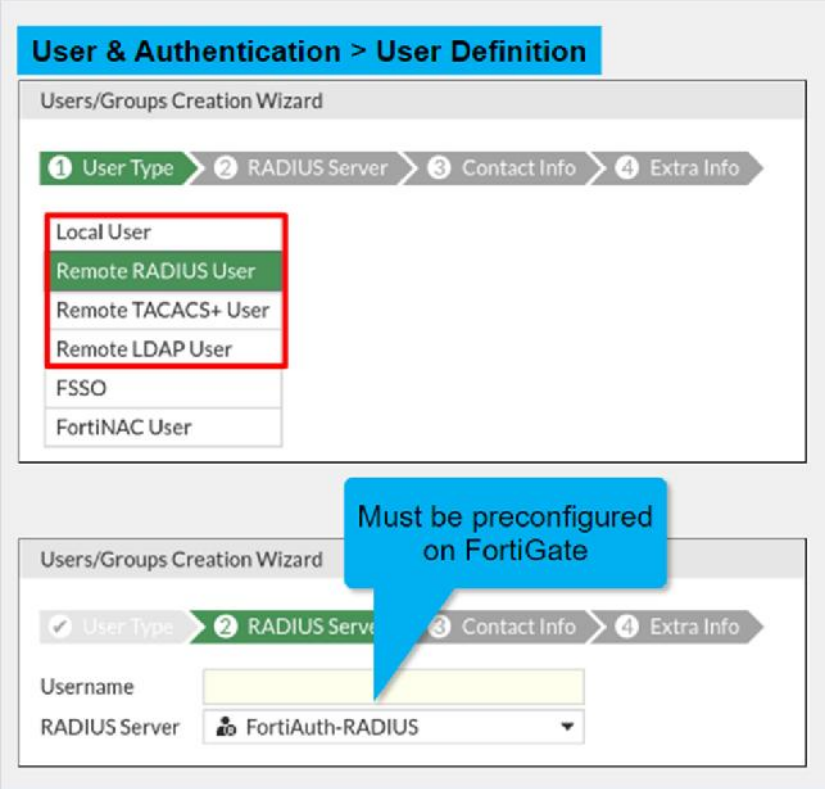
Méthode d'authentification: Authentification distante

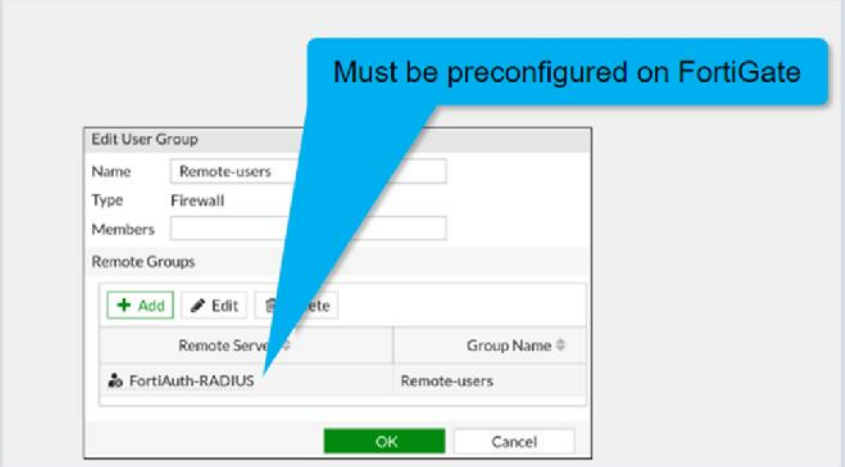
- Compte sauvegarder dans le serveur d'authentification;
- Possibilité de créer les comptes locaux en cas d'indisponibilité du serveur d'authentification.



Authentification Firewall

Méthode d'authentification: Authentification distante (suite)

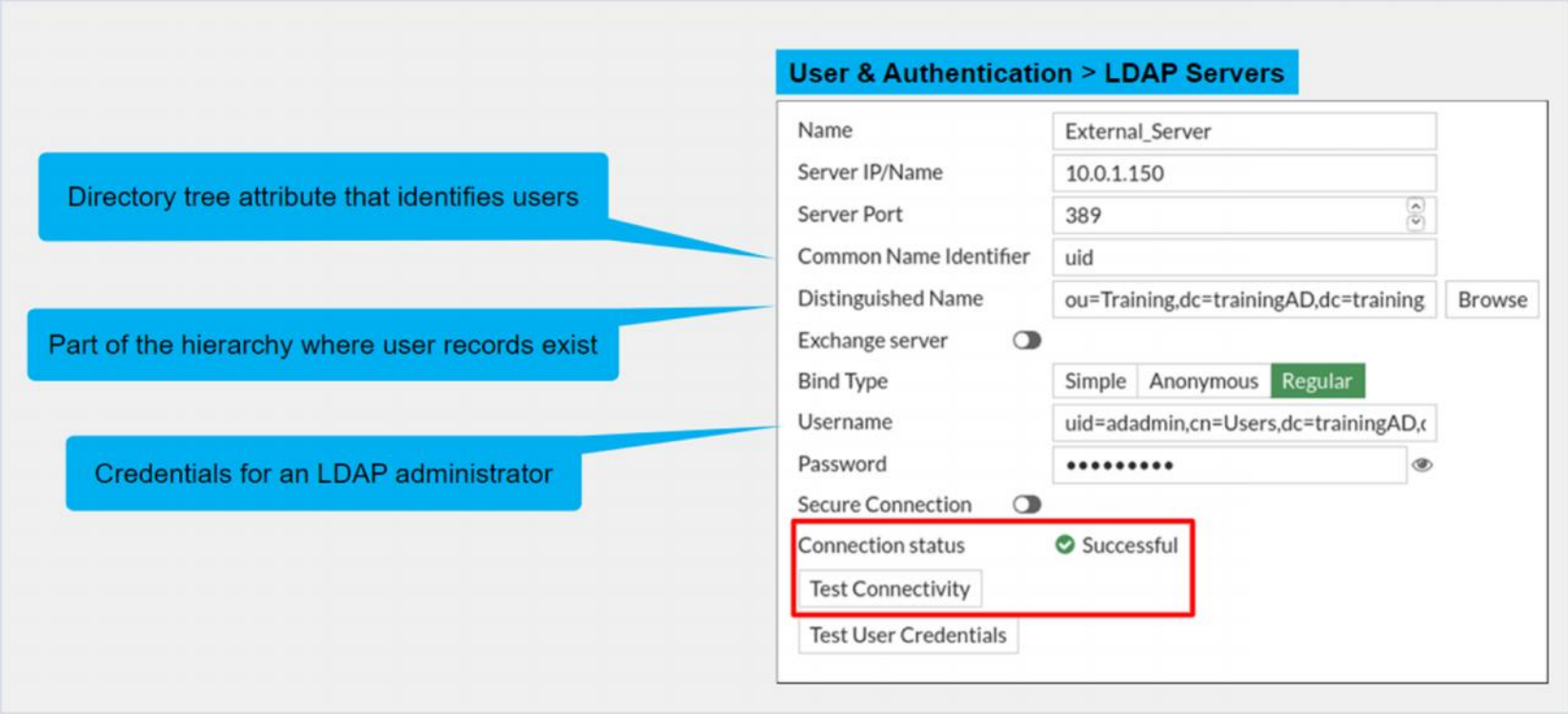




Authentification Firewall

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

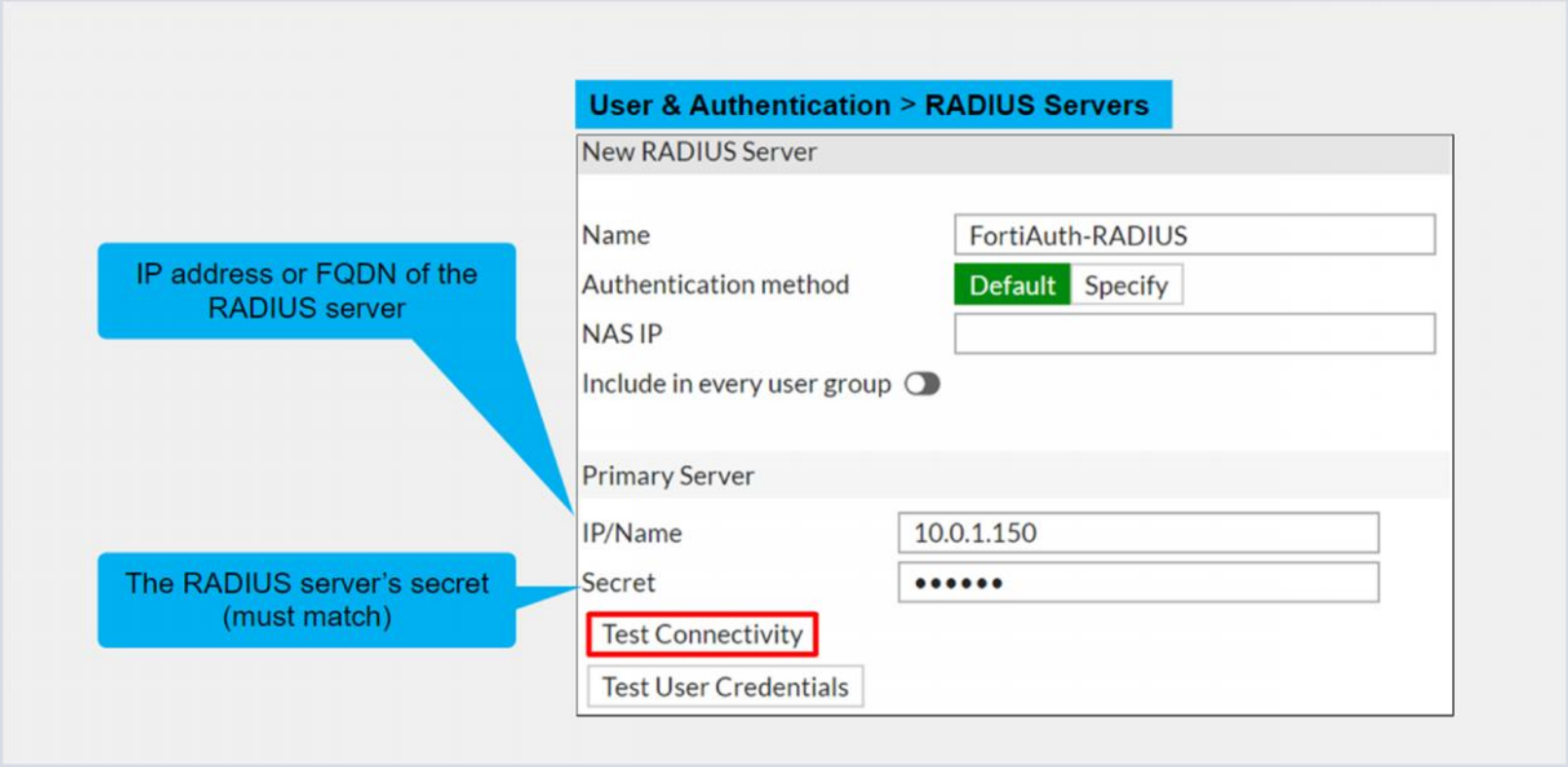
- LDAP



Authentification Firewall

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

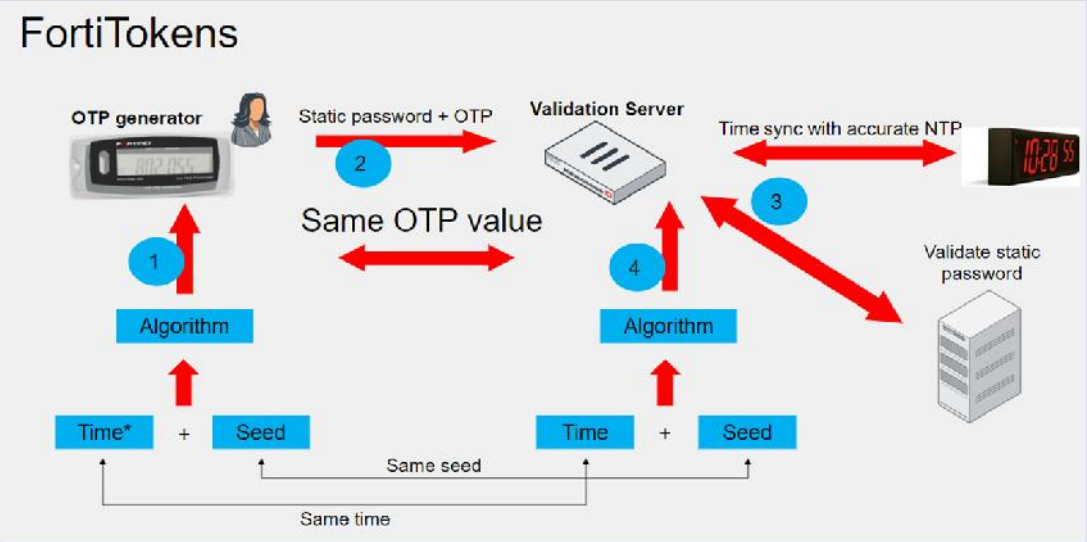
- RADIUS



Authentification Firewall

Méthode d'authentification: Authentification à 02 facteurs et OTP

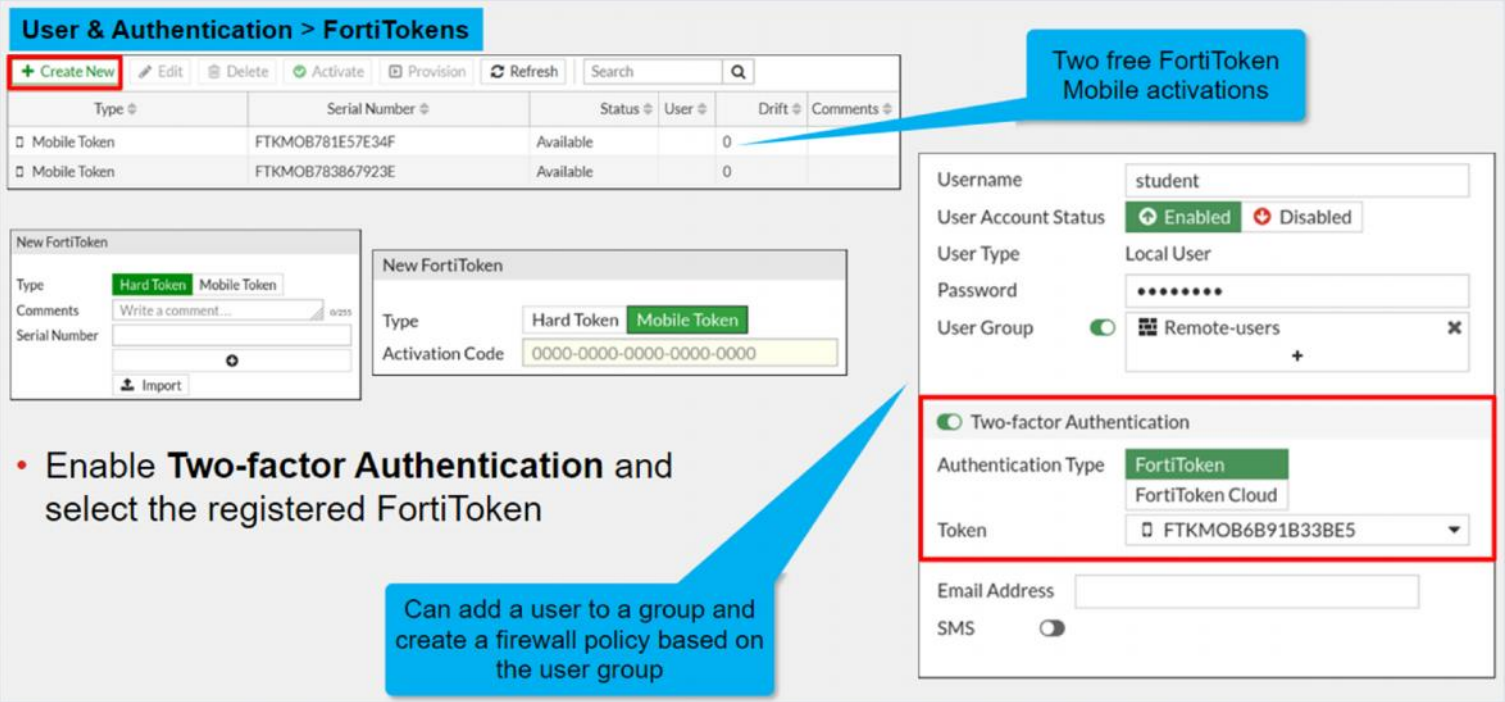
- Améliore la sécurité;
- Nécessite 02 méthodes indépendante:
  - Quelque chose que vous savez: PIN, mot de passe, etc.
  - Quelque chose que vous avez: token, certificat, etc.
- OTP (One Time Password)
  - Offre plus de sécurité;
  - Token fourni par FortiToken 200 ou FortiMobile:
    - Génération d'un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



Authentification Firewall

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

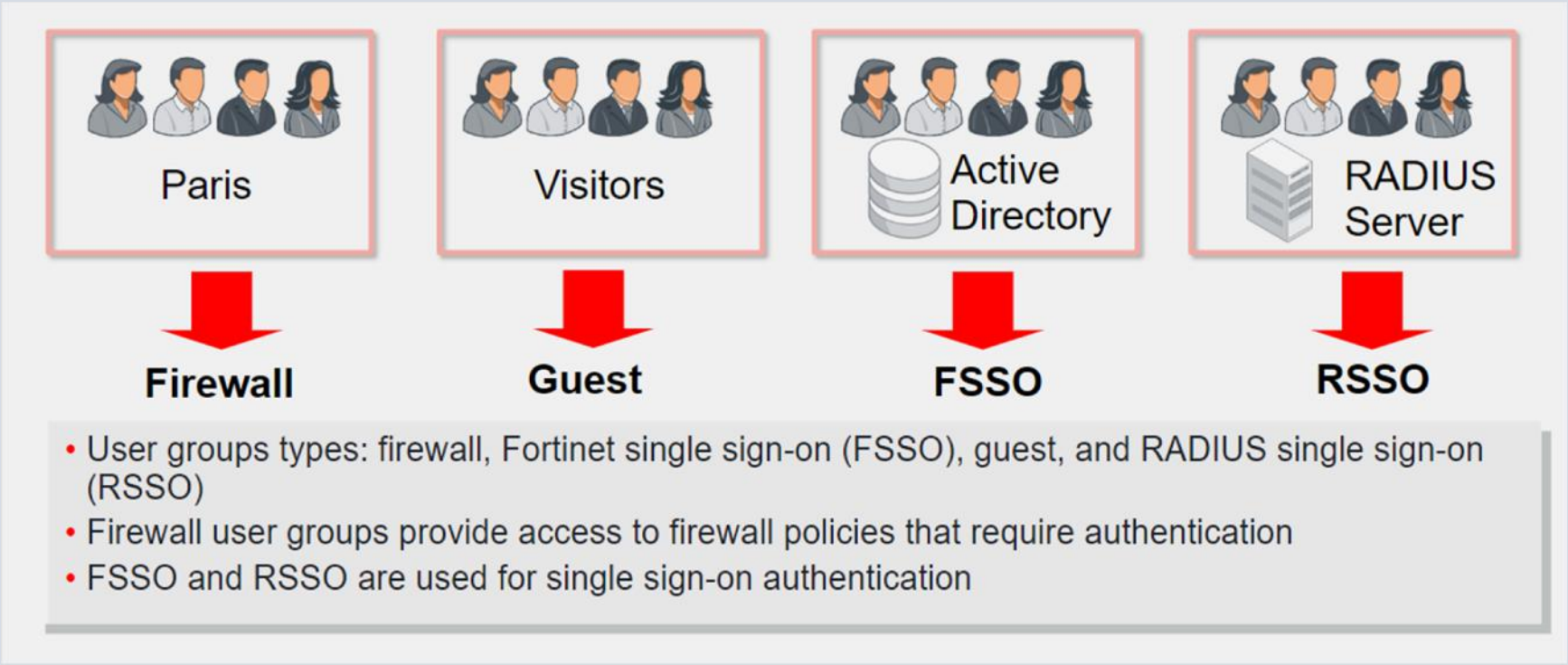
- ❑ Enregistrement des tokens au niveau du FortiGate (Hard ou Soft);
- ❑ Assignation du token à un utilisateurs.



Authentification Firewall

Authentification (suite) | Authentification avec politiques | Authentification via portail captif | Monitoring&Diagnostic

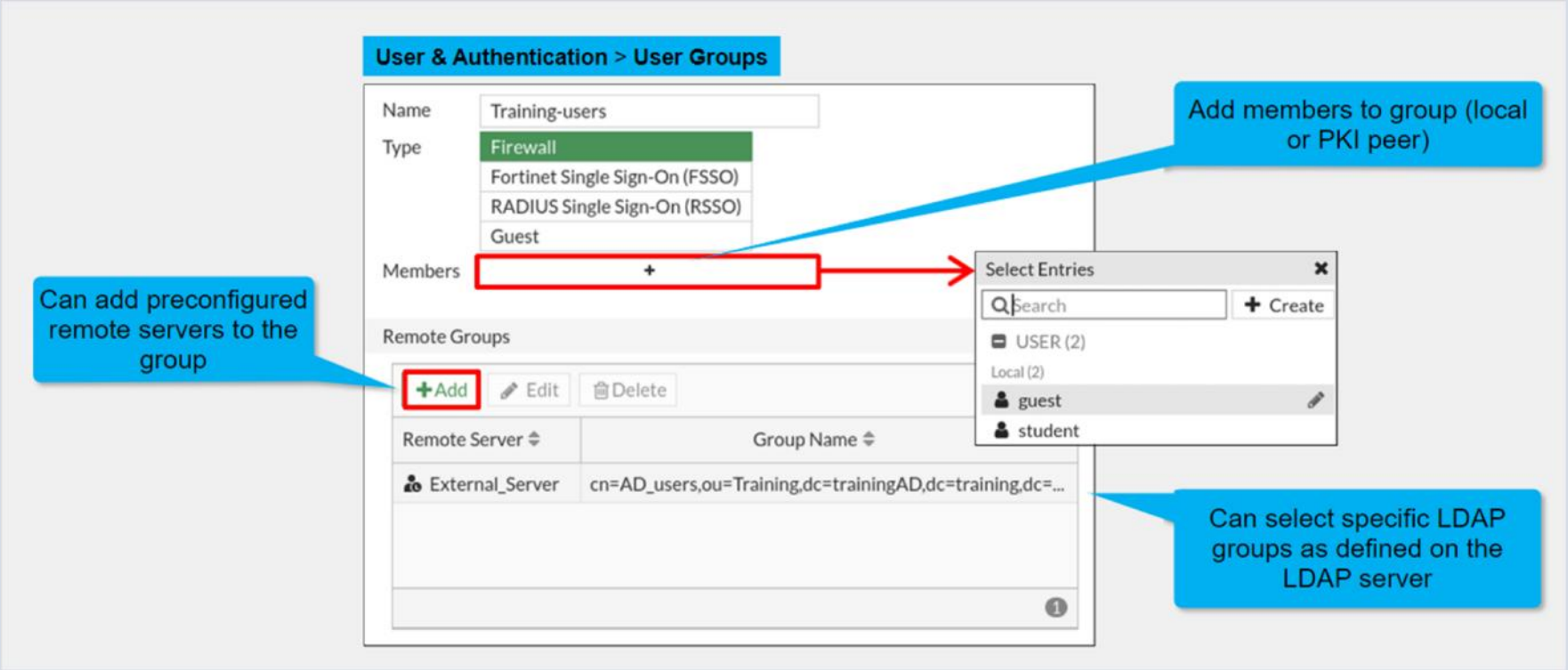
Groupes:



Authentification Firewall

Authentification (suite) | Authentification avec politiques | Authentification via portail captif | Monitoring&Diagnostic

Groupes: Configuration

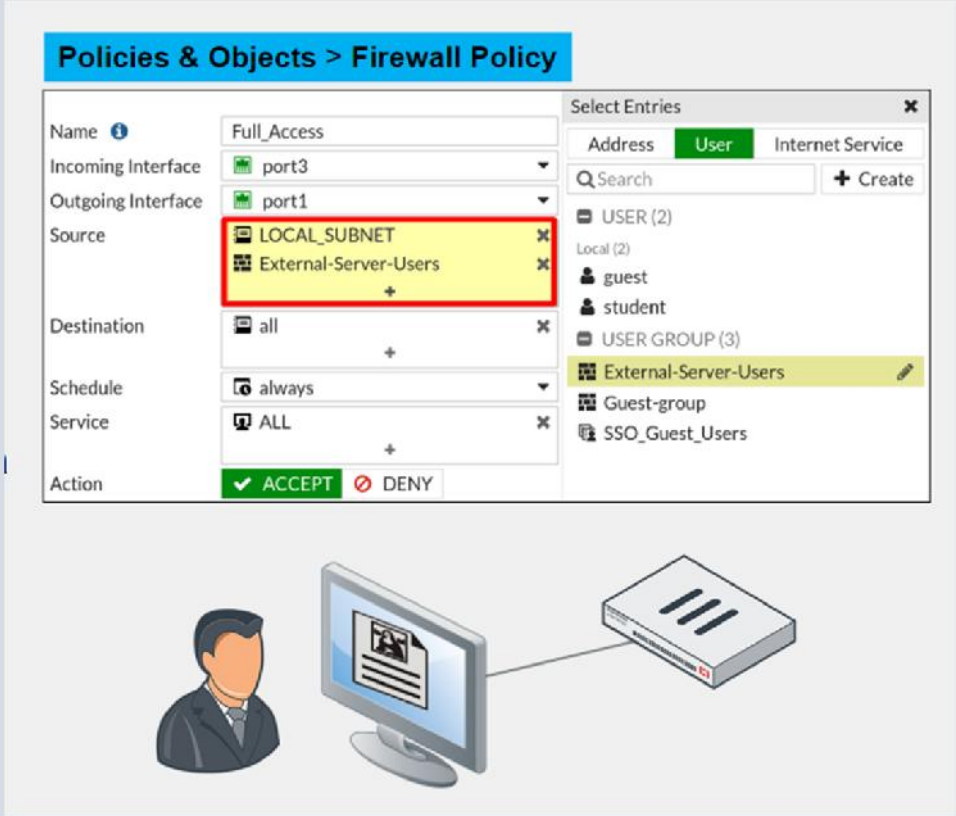


Authentification Firewall

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.

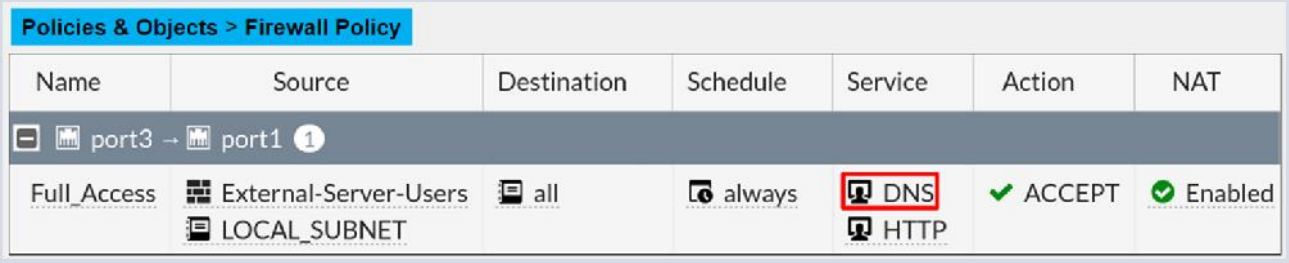


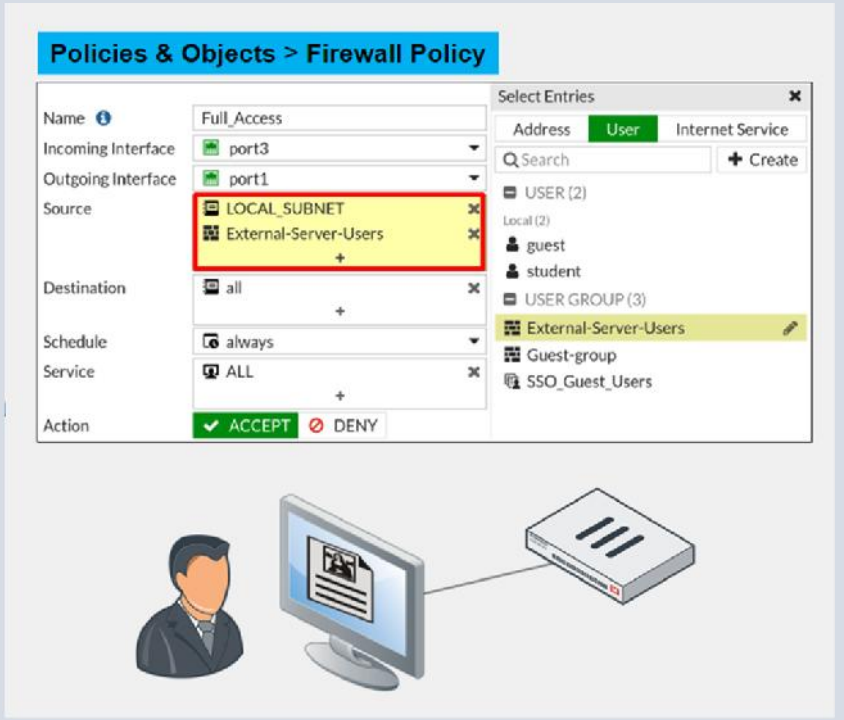
Authentification Firewall

Authentification | Authentification avec politiques (suite) | 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;
- Protocole autorisé avant l'authentification: HTTP, HTTPS, FTP et TELNET



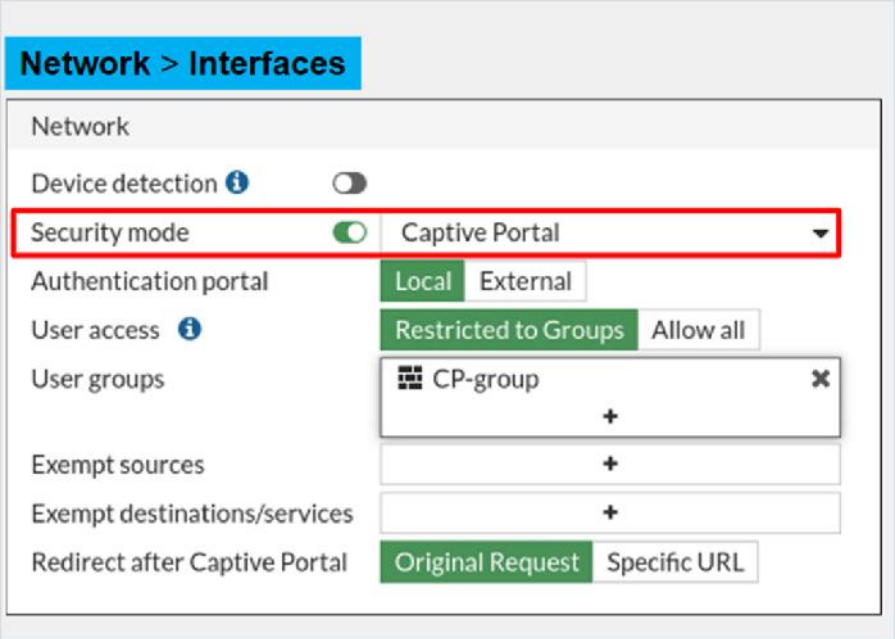


Authentification Firewall

Authentification | Authentification avec politiques | Authentification via portail captif | Monitoring&Diagnostic

Portail Captif

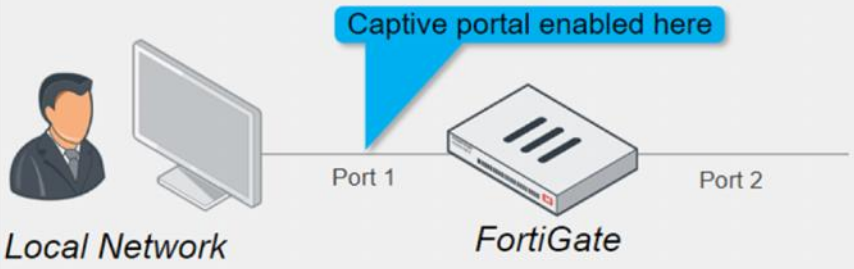
- ❑ Authentification web des utilisateurs avec login et mot de passe;
- ❑ Activation sur l'interface d'entrée du trafic;
- ❑ Méthode d'authentification active uniquement;
- ❑ Hébergement du portail captif sur le FortiGate ou sur un serveur Externe.



Authentification Firewall

Portail Captif: Configuration

- Configured on network interfaces



Network > Interfaces

Network

Device detection	
Security mode	Captive Portal
Authentication portal	Local External
User access	Restricted to Groups Allow all
User groups	CP-group
Exempt sources	
Exempt destinations/services	
Redirect after Captive Portal	Original Request Specific URL

WiFi & Switch Controller > SSIDs

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

WiFi Settings

SSID	fortinet
Client limit	
Broadcast SSID	

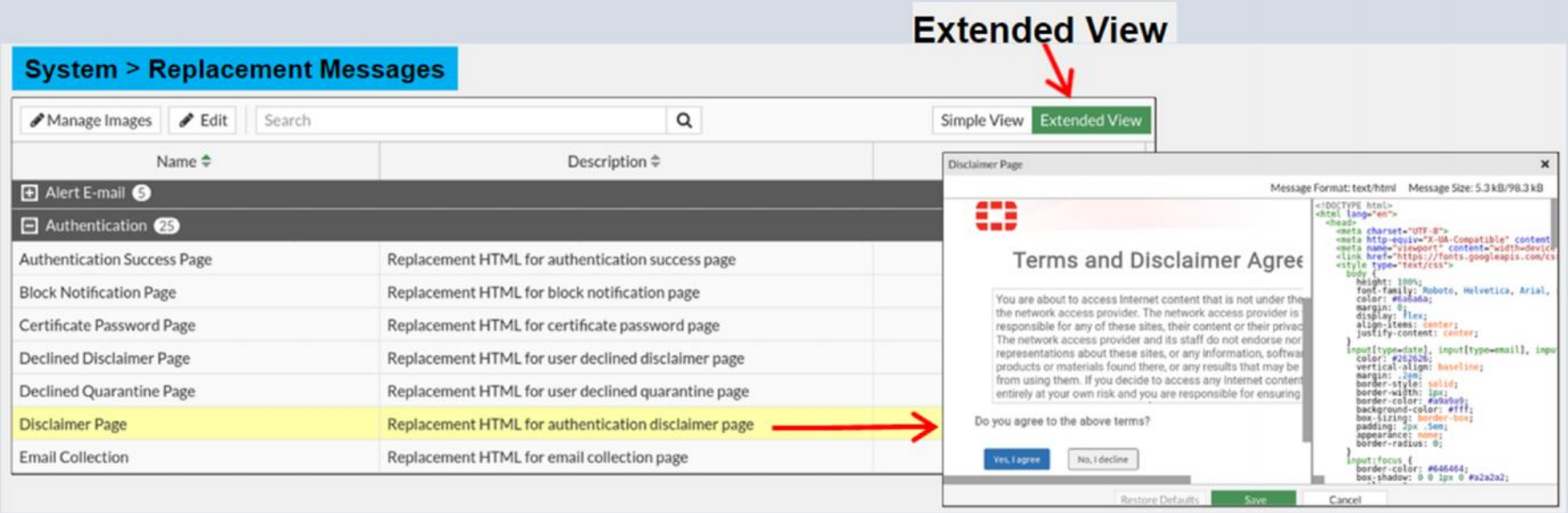
Security Mode Settings

Security mode	Captive Portal
Portal type	Disclaimer + Authentication
Authentication portal	Local External
User groups	Guest-group
Exempt sources	
Exempt destinations/services	
Redirect after Captive Portal	Original Request Specific URL

Authentification Firewall

Authentification Authentification avec politiques Authentification via portail captif (suite) Monitoring&Diagnostic

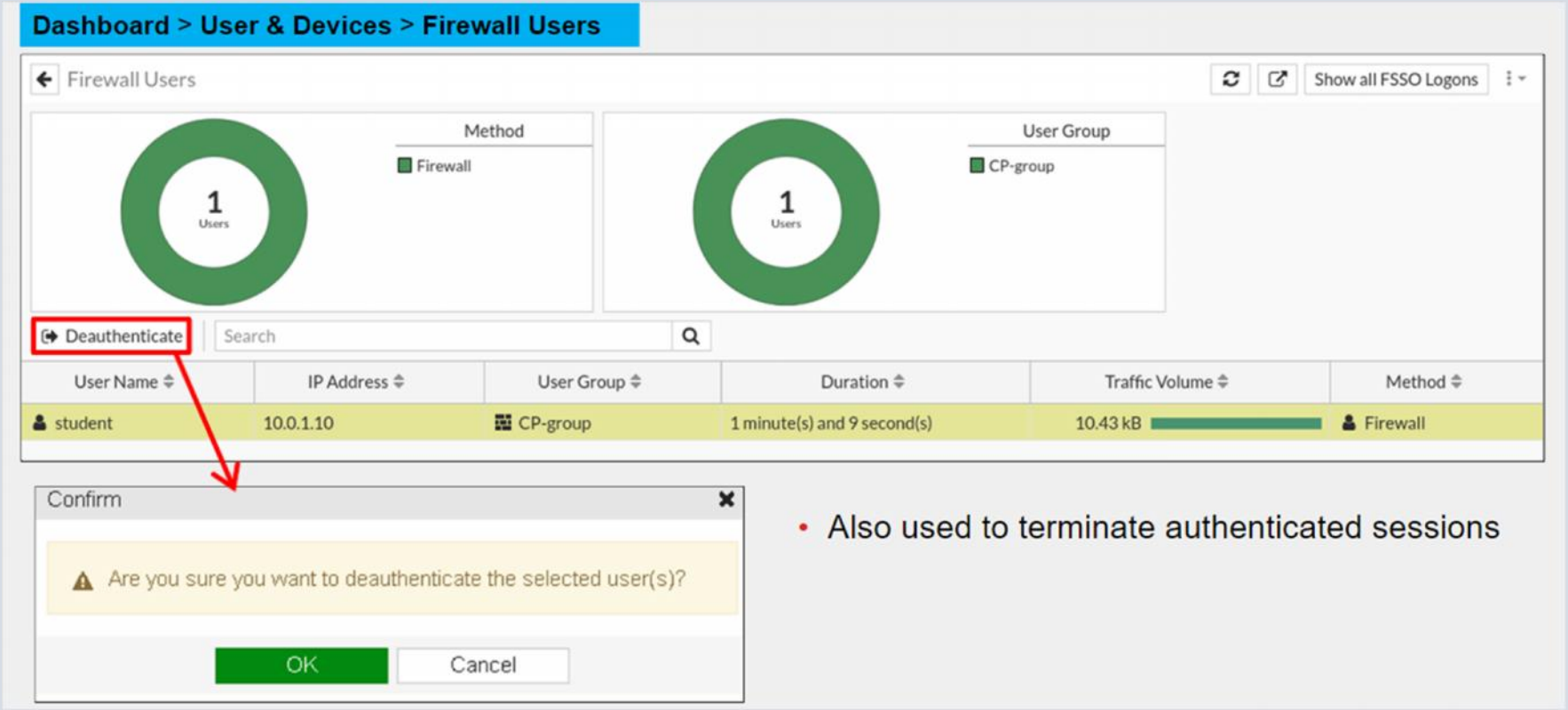
Portail Captif: Configuration des messages d'affichage



Authentification Firewall

Authentification | Authentification avec politiques | Authentification via portail captif | Monitoring&Diagnostic

Monitoring: Utilisateurs



Authentification Firewall

Authentification Authentification avec politiques Authentification via portail captif Monitoring&Diagnostic (suite)

Troubleshooting: GUI

Troubleshooting: CLI

- Diagnose firewall auth list: affiche les utilisateurs authentifié, 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;
- Daignose 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.

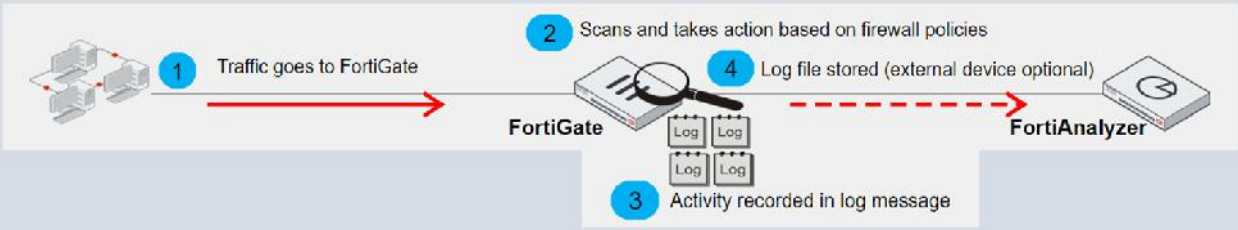
Journalisation et Supervision

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 reconnaitre 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).

Journalisation et Supervision

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

Niveau de séverité:

- 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

Message de journalisation:

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

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

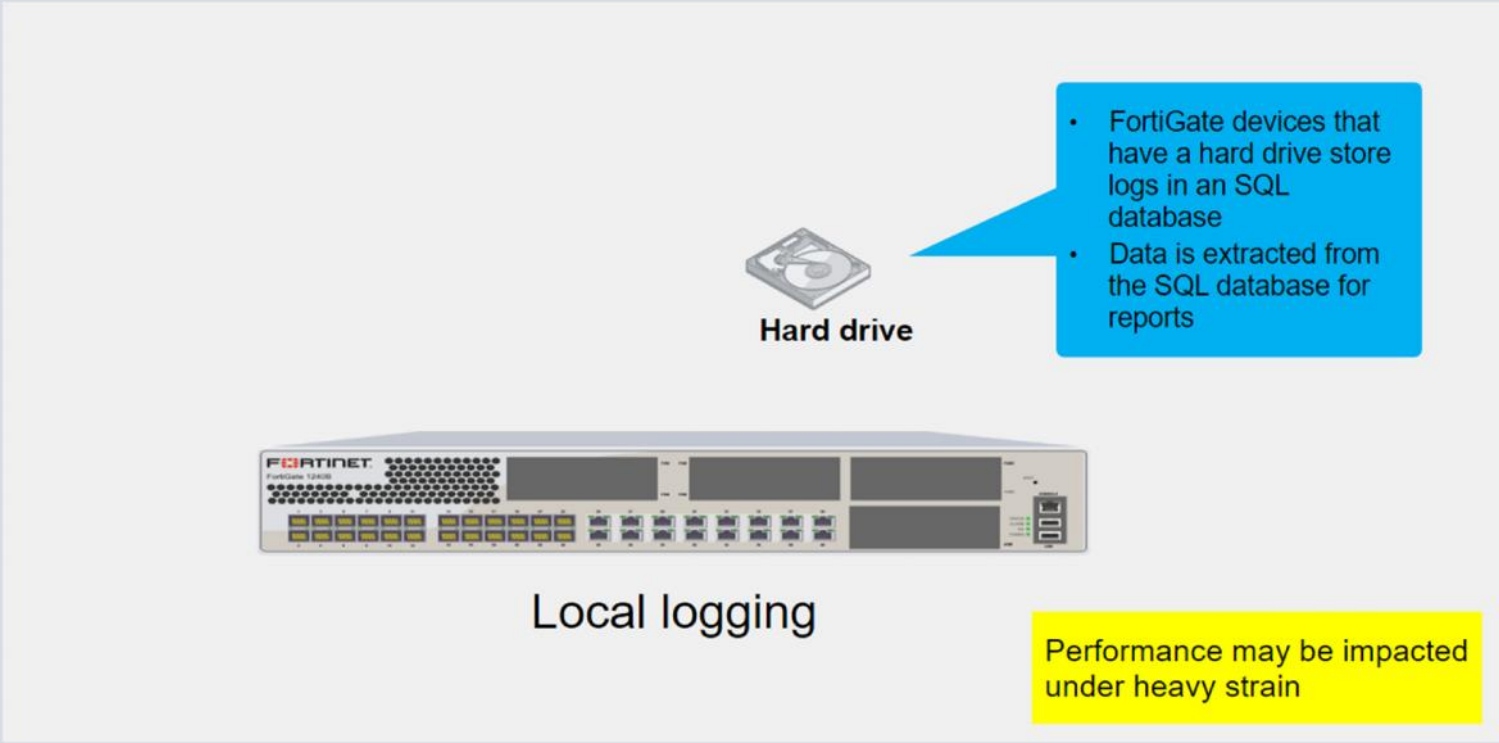
- Body: varie en fonction du type de log.

```
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=297 rcvdbyte=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 locale:

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

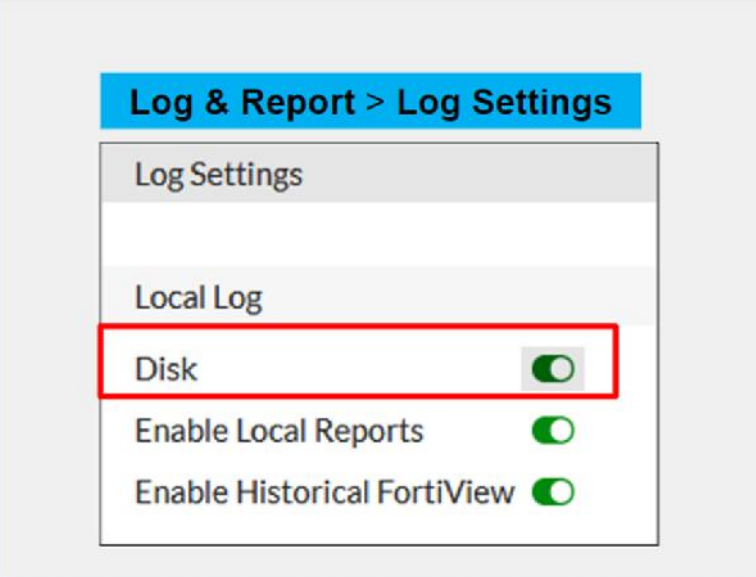


Journalisation et Supervision

Journalisation locale: Activation

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

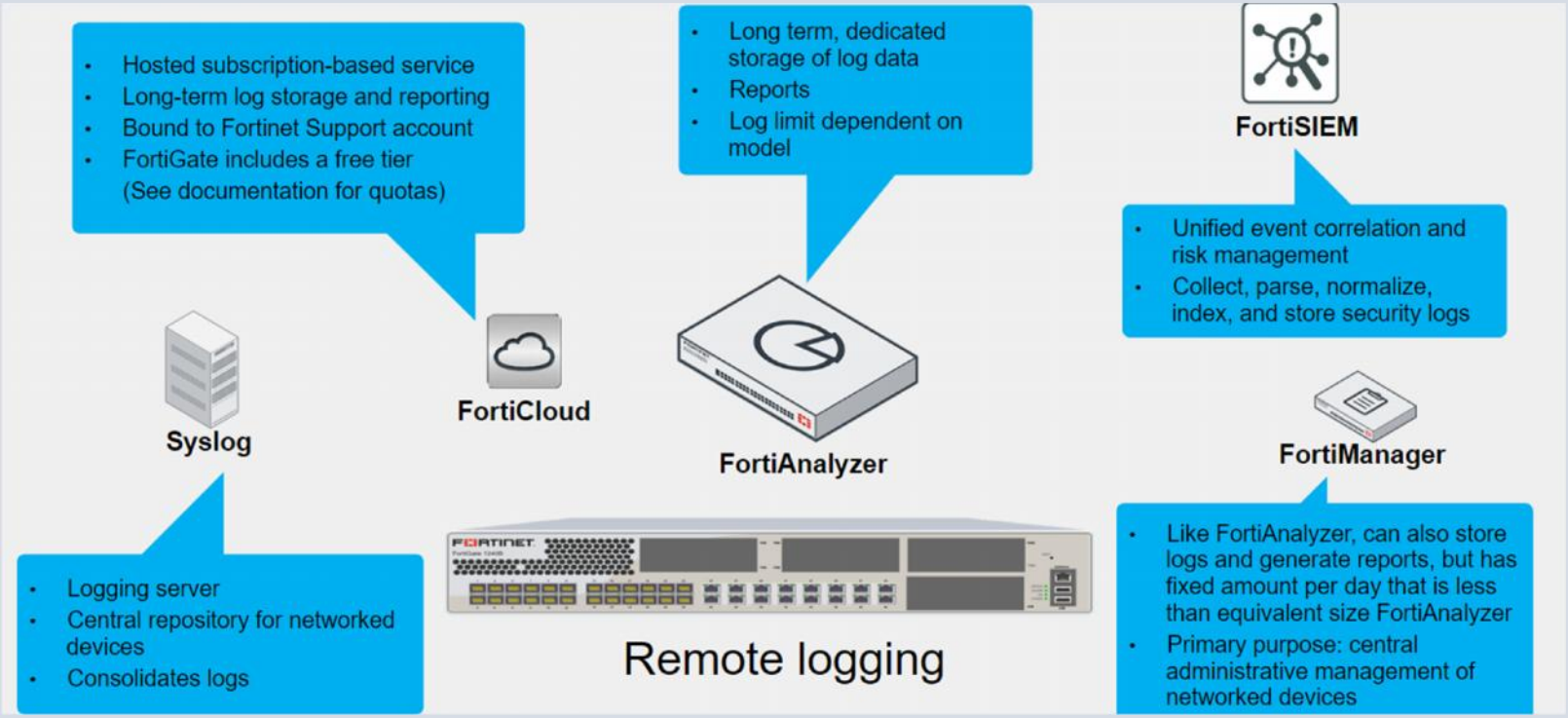
```
# config log disk setting
     set maximum-log-age <integer>
```



Journalisation et Supervision

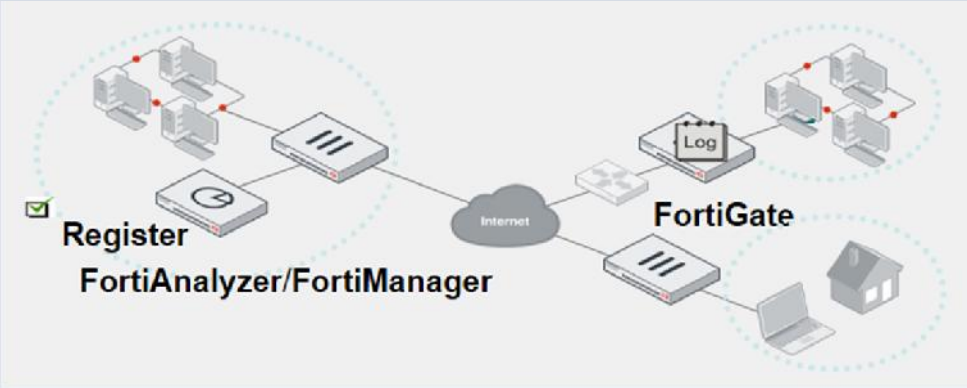
Journalisation Distante

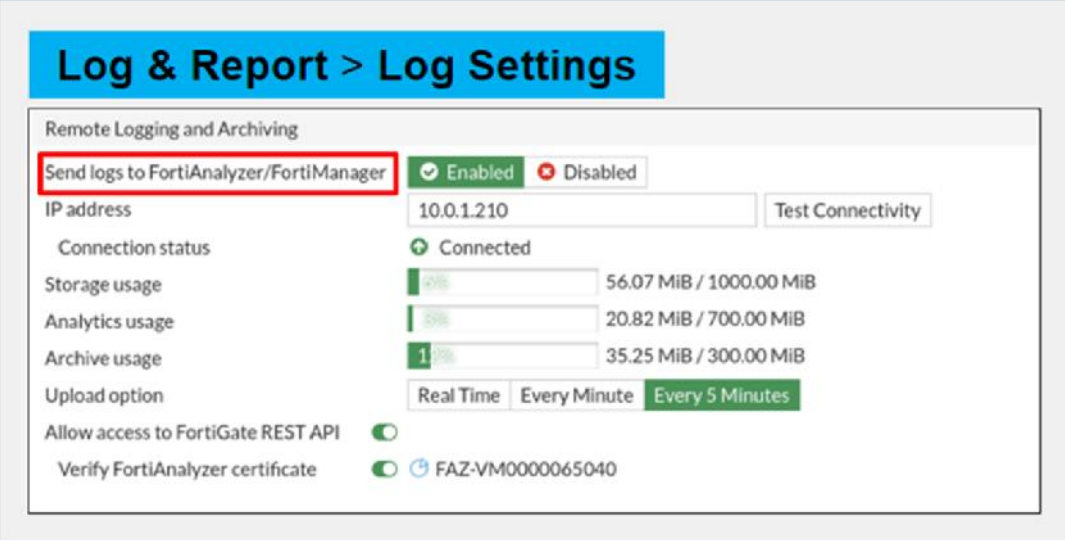
- Sauvegarde des logs sur un serveur distant.



Journalisation et Supervision

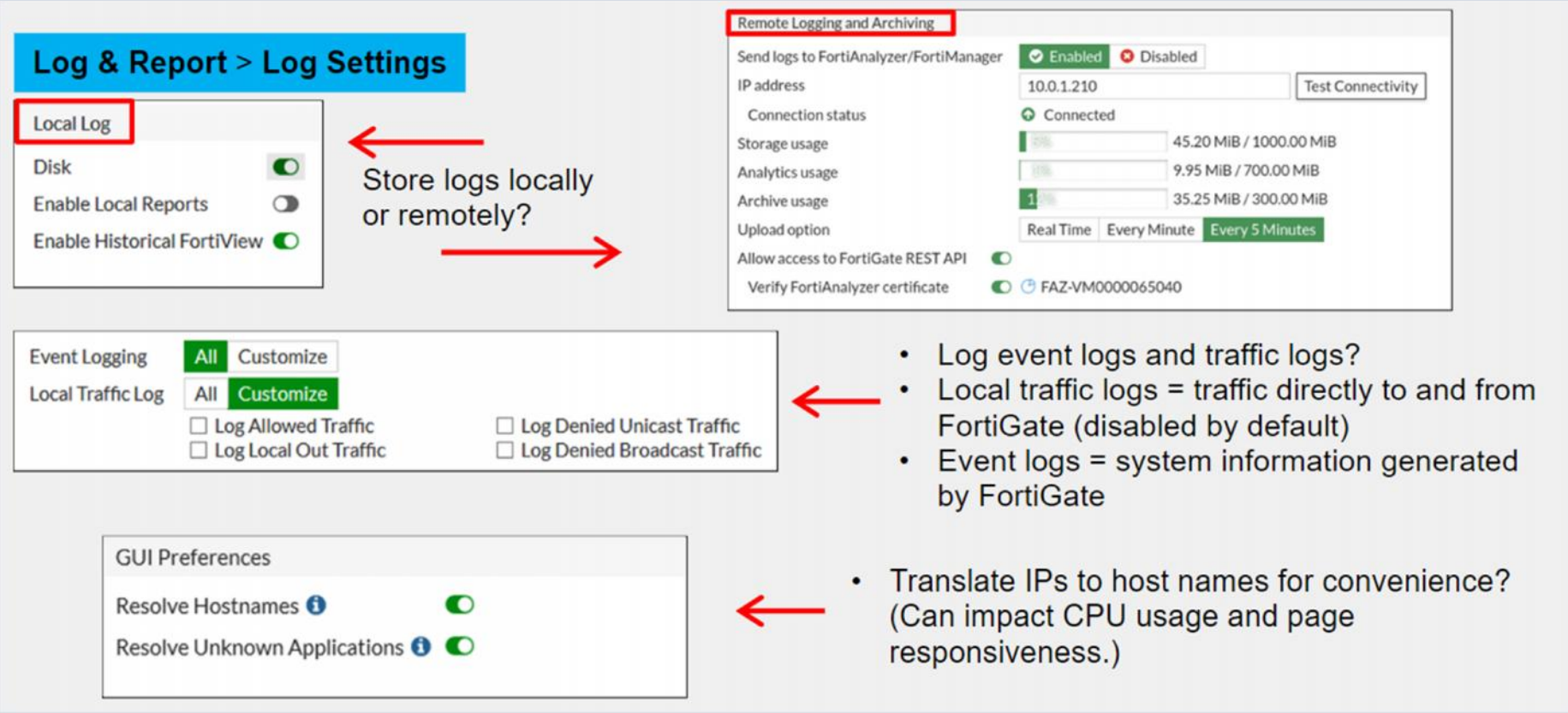
Journalisation Distante: FortiAnalyze & FortiSIEM





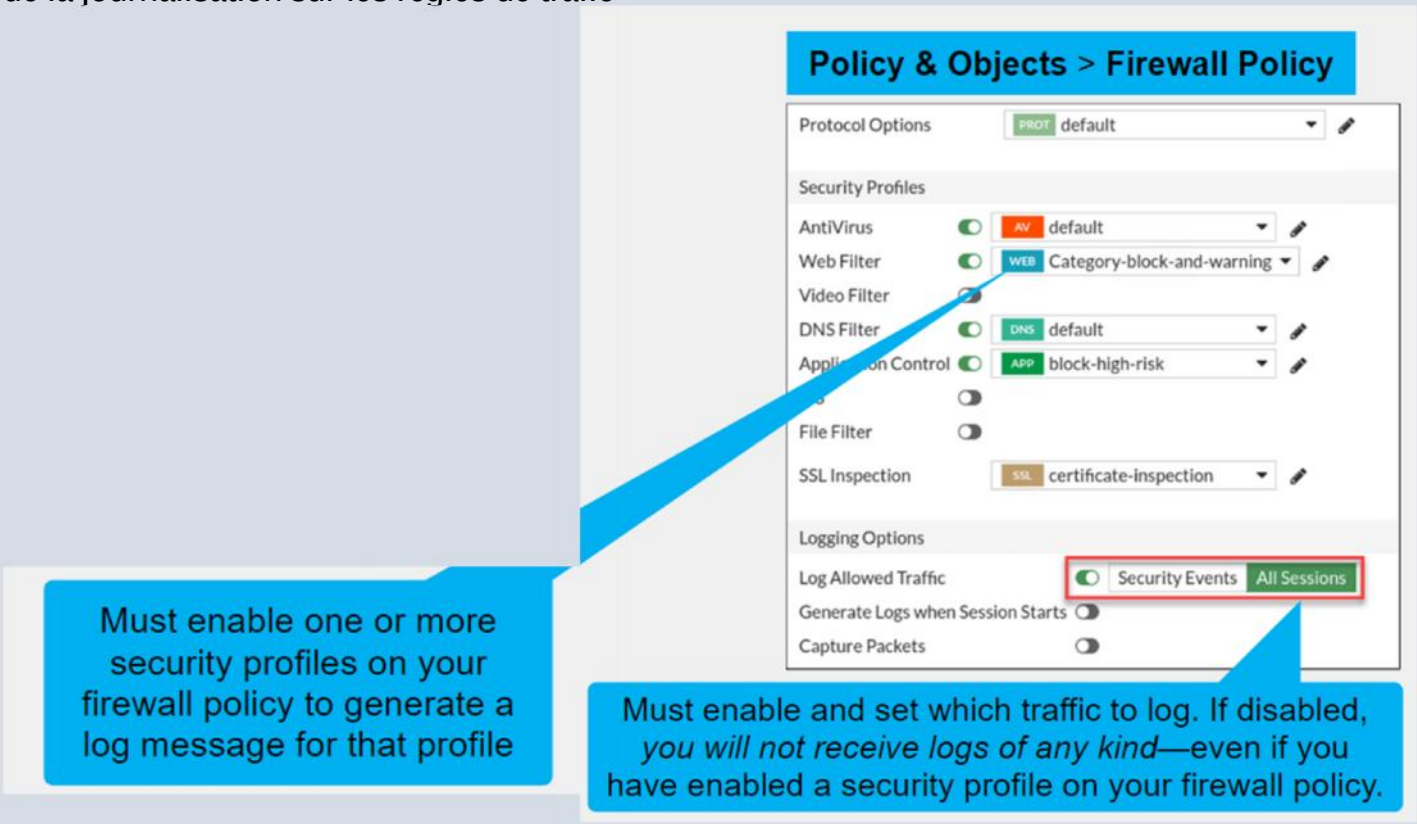
Journalisation et Supervision

Journalisation: Paramètres



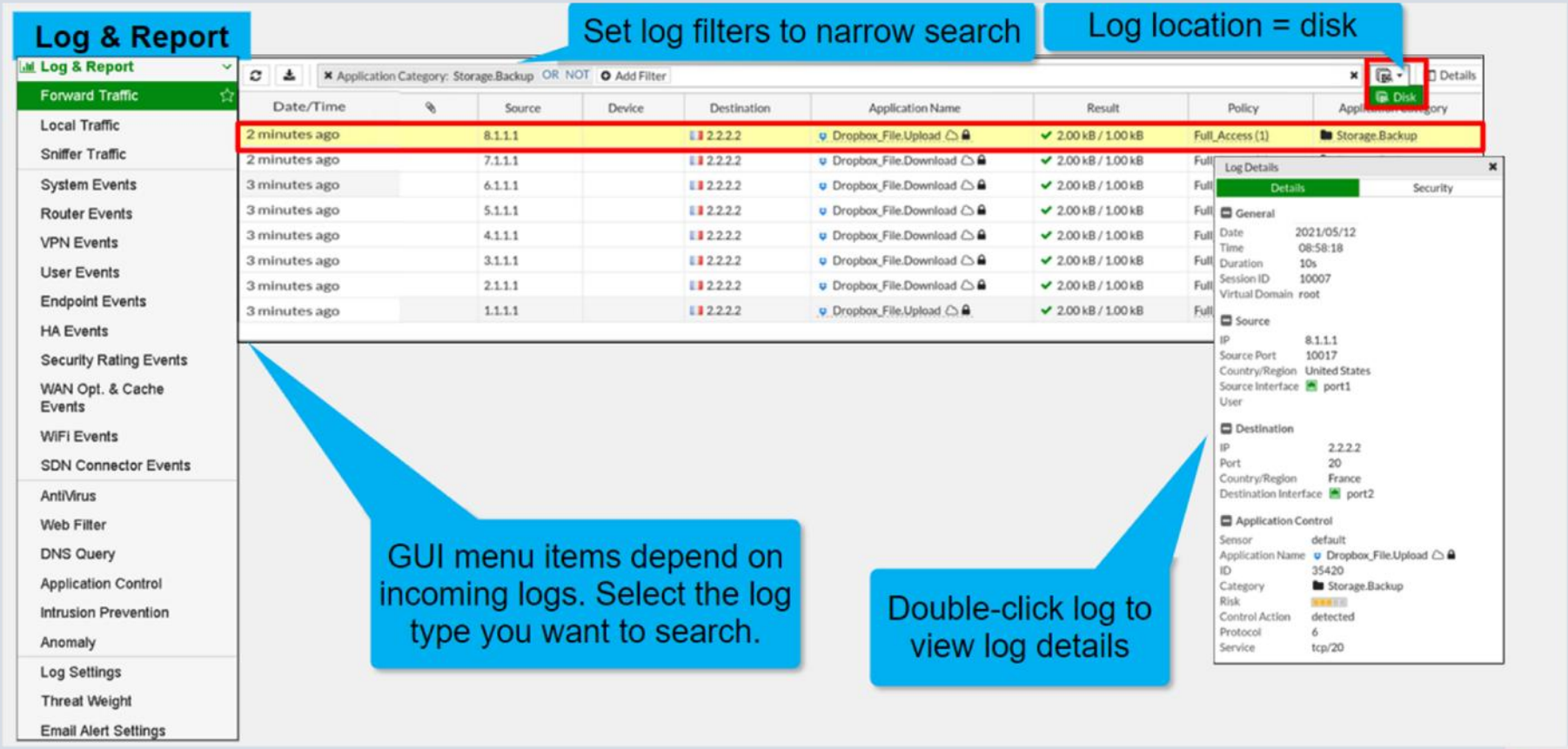
Journalisation et Supervision

Journalisation: Activation de la journalisation sur les règles de trafic



Journalisation et Supervision

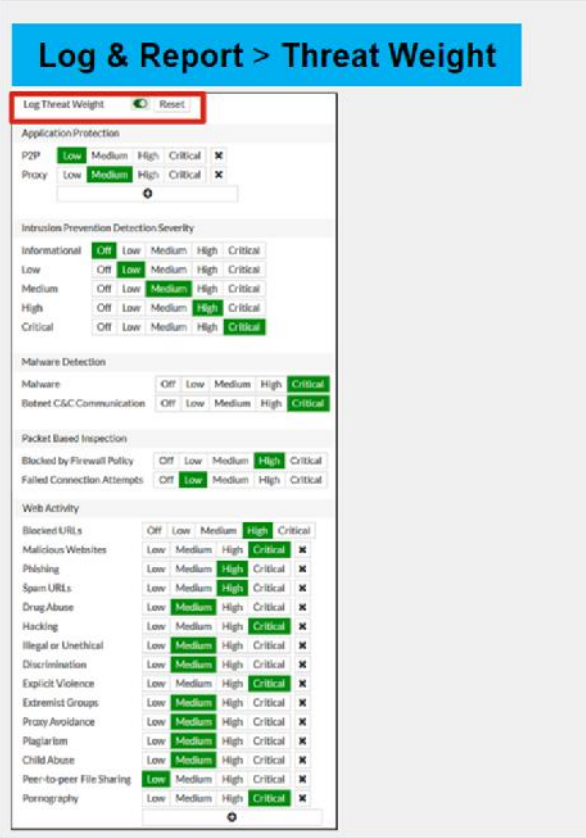
Journalisation: Consultation - GUI



Journalisation et Supervision

Journalisation: poids des menaces

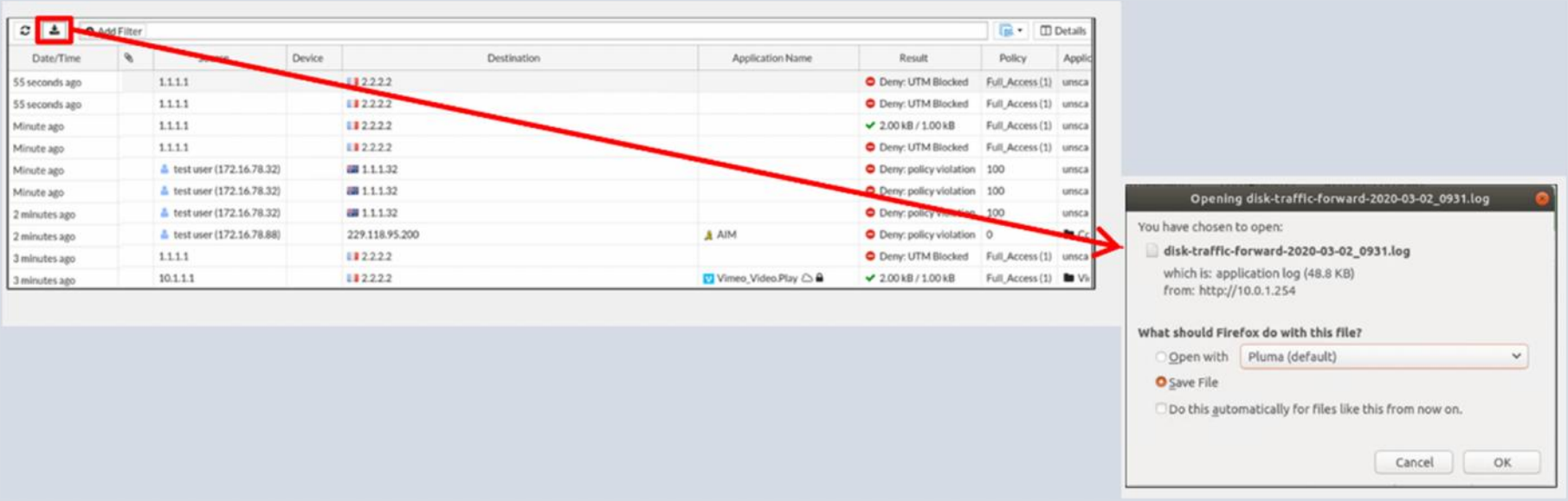
- Permet de prioriser les incidents en préconfigurant leur niveau de sévérité et de risque



Journalisation et Supervision

Journalisation | Journalisation local et distante | Paramètre de journalisation | Protection des journaux

Protection: Téléchargement



Certificats

Objectifs

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

Certificats

Certificats: utilisation

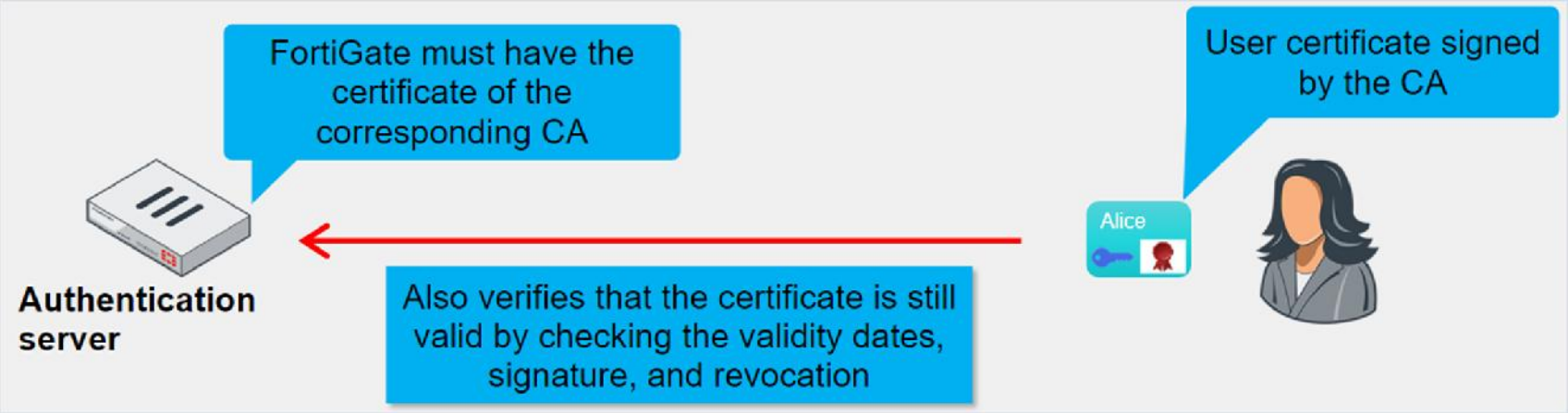
- Inspection
  - Inspection SSL;
  - S'assure de la validité d'un certificat avant l'autorisation de l'accès;
- Intimité (privacy)
  - Etablissement des connexions SSL avec les autres équipements;
- Authentification
  - Second facteurs lors de l'authentification multifacteur;
  - Authentification des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

Certificats

Authentification et sécurisation (suite) | Inspection de trafic | Gestion des certificats

Authentification: utilisateur

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

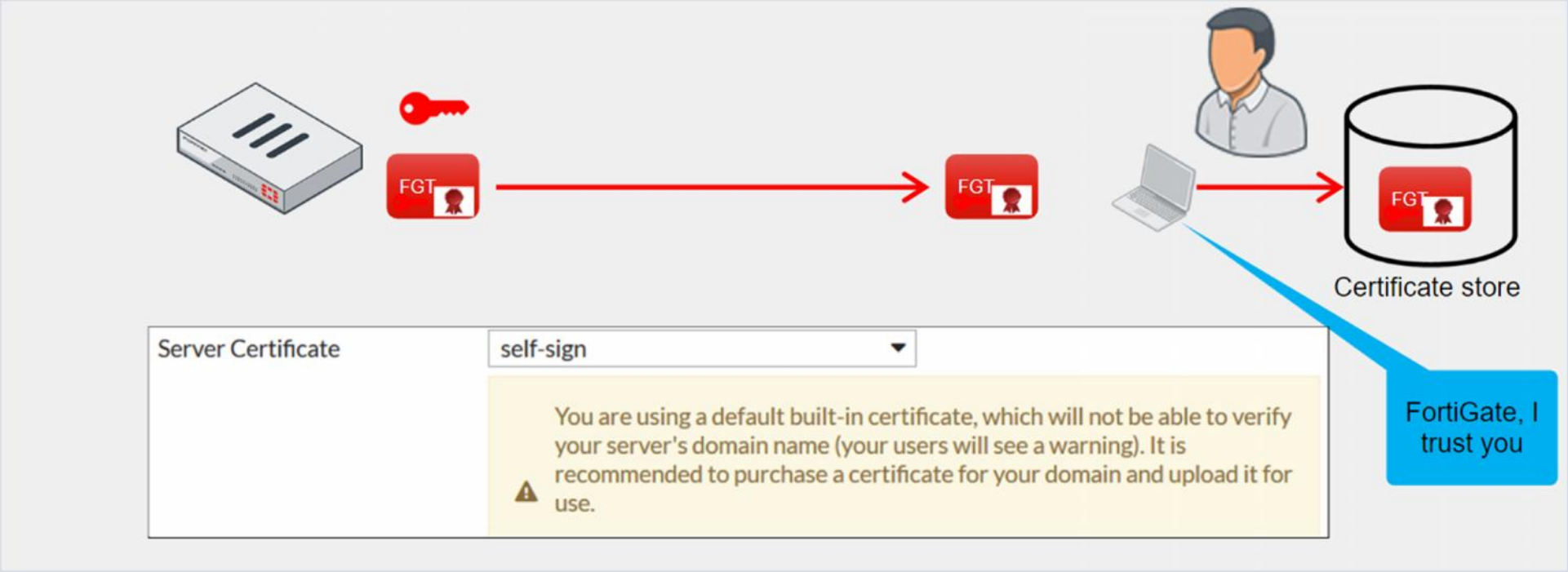


Certificats

Authentification et sécurisation (suite) | Inspection de trafic | Gestion des certificats

Authentification: utilisateur

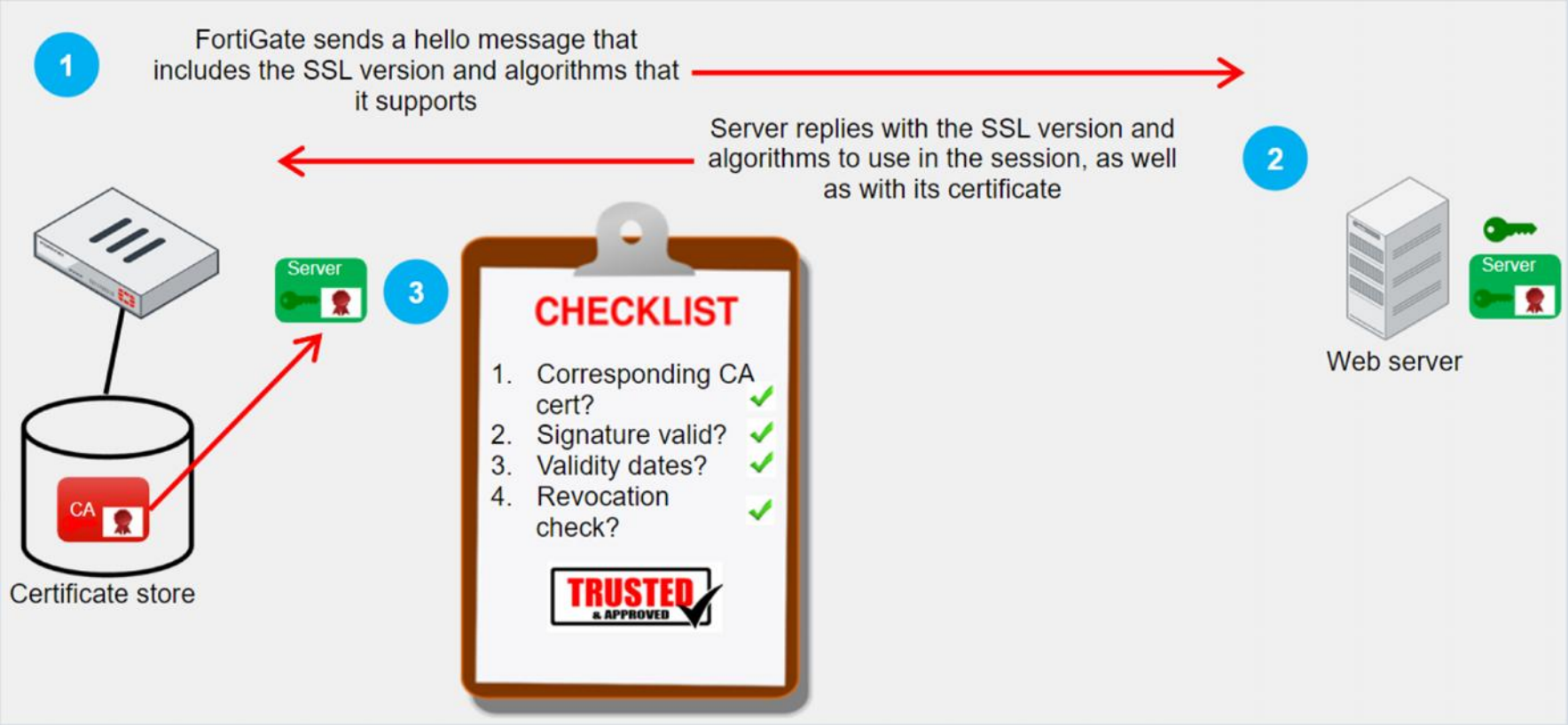
- Certificat auto signé (par défaut);
- Etablissement des sessions SSL.



Certificats

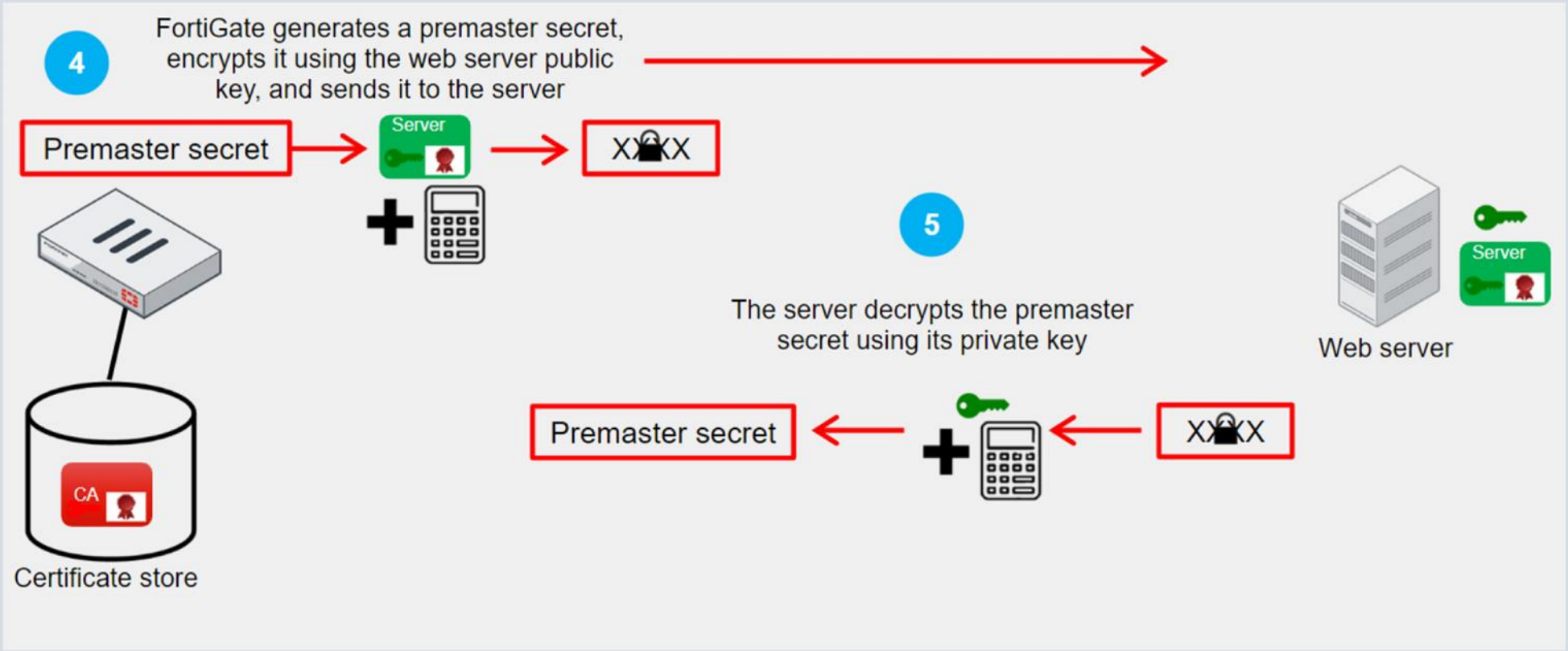
Authentification et sécurisation (suite) | Inspection de trafic | Gestion des certificats

Connection SSL.



Certificats

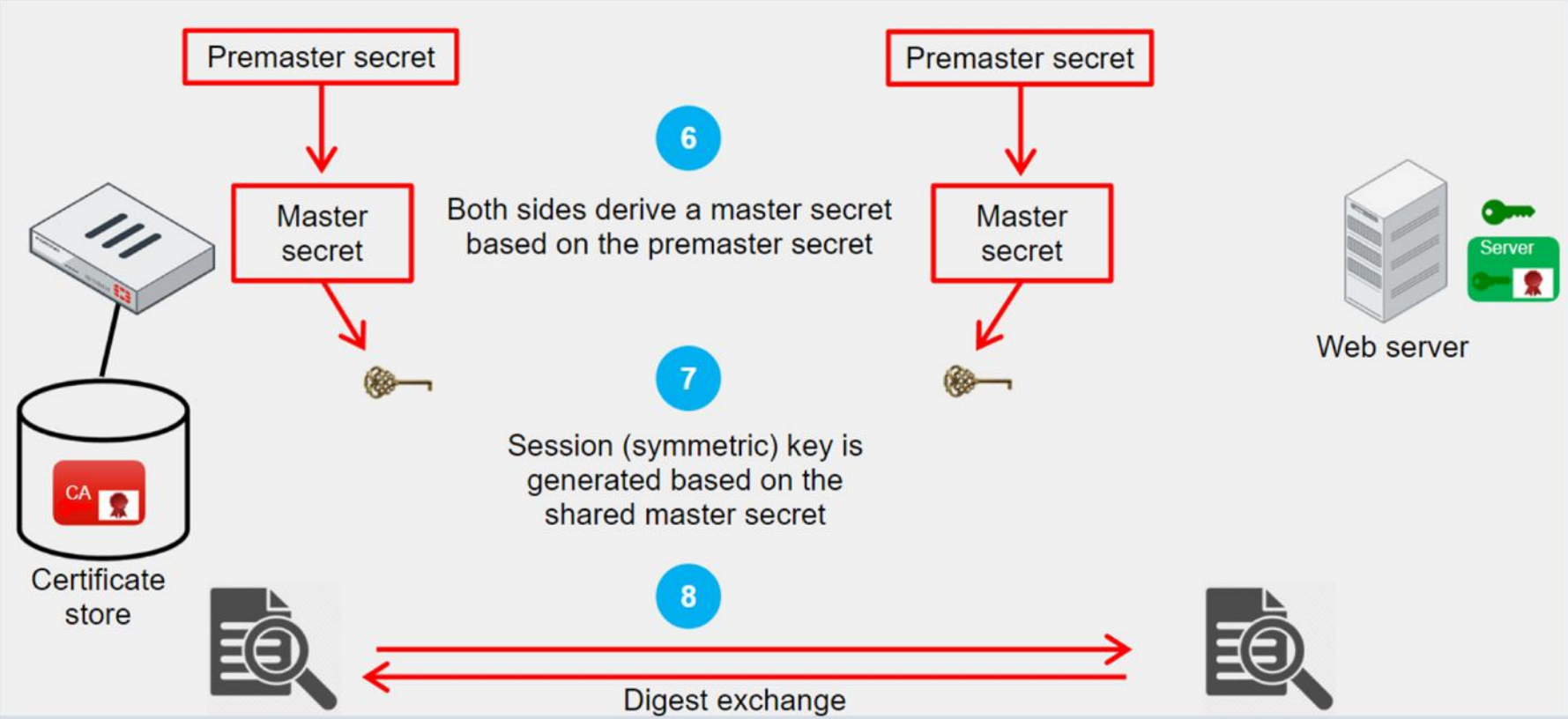
Connection SSL - 2.



Certificats

Authentification et sécurisation (suite) | Inspection de trafic | Gestion des certificats

Connection SSL - 3.

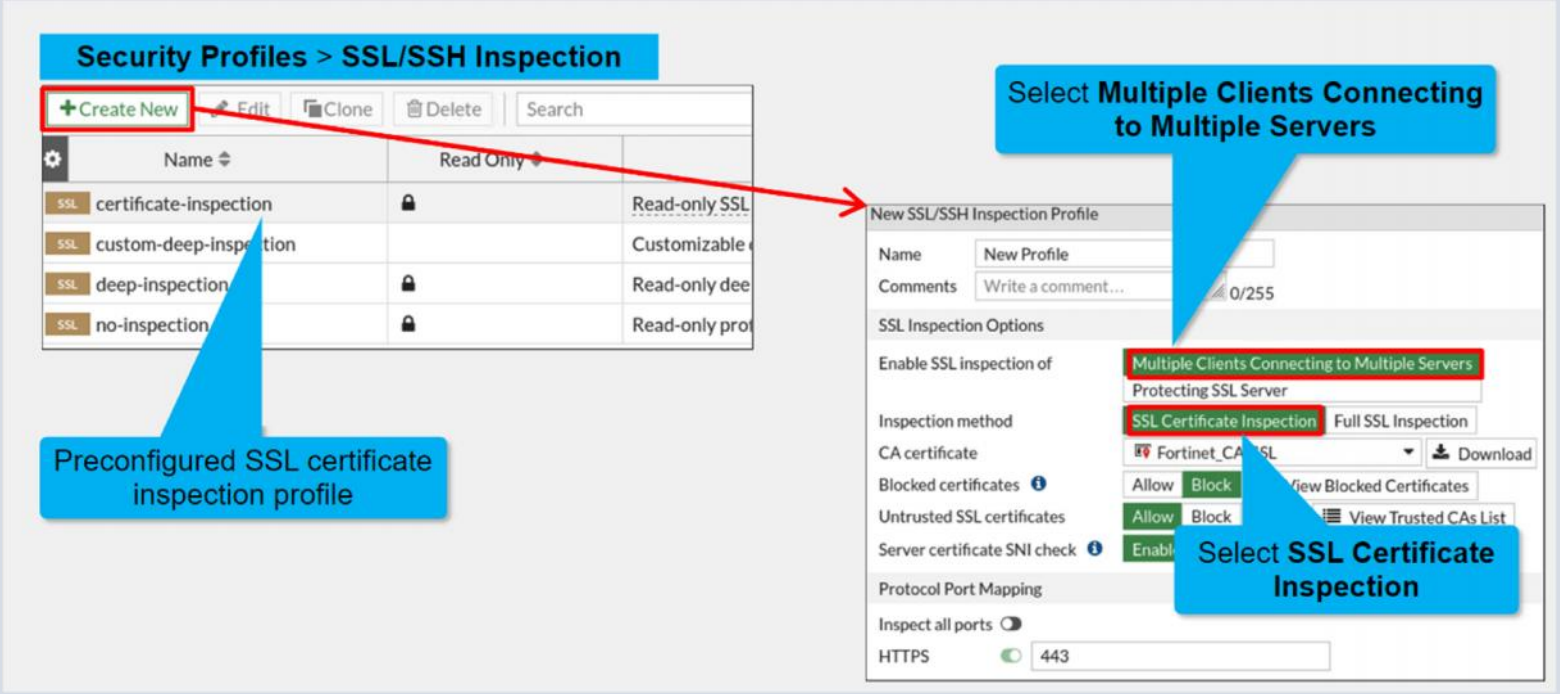


Certificats

Authentification et sécurisation | Inspection de trafic | Gestion des certificats

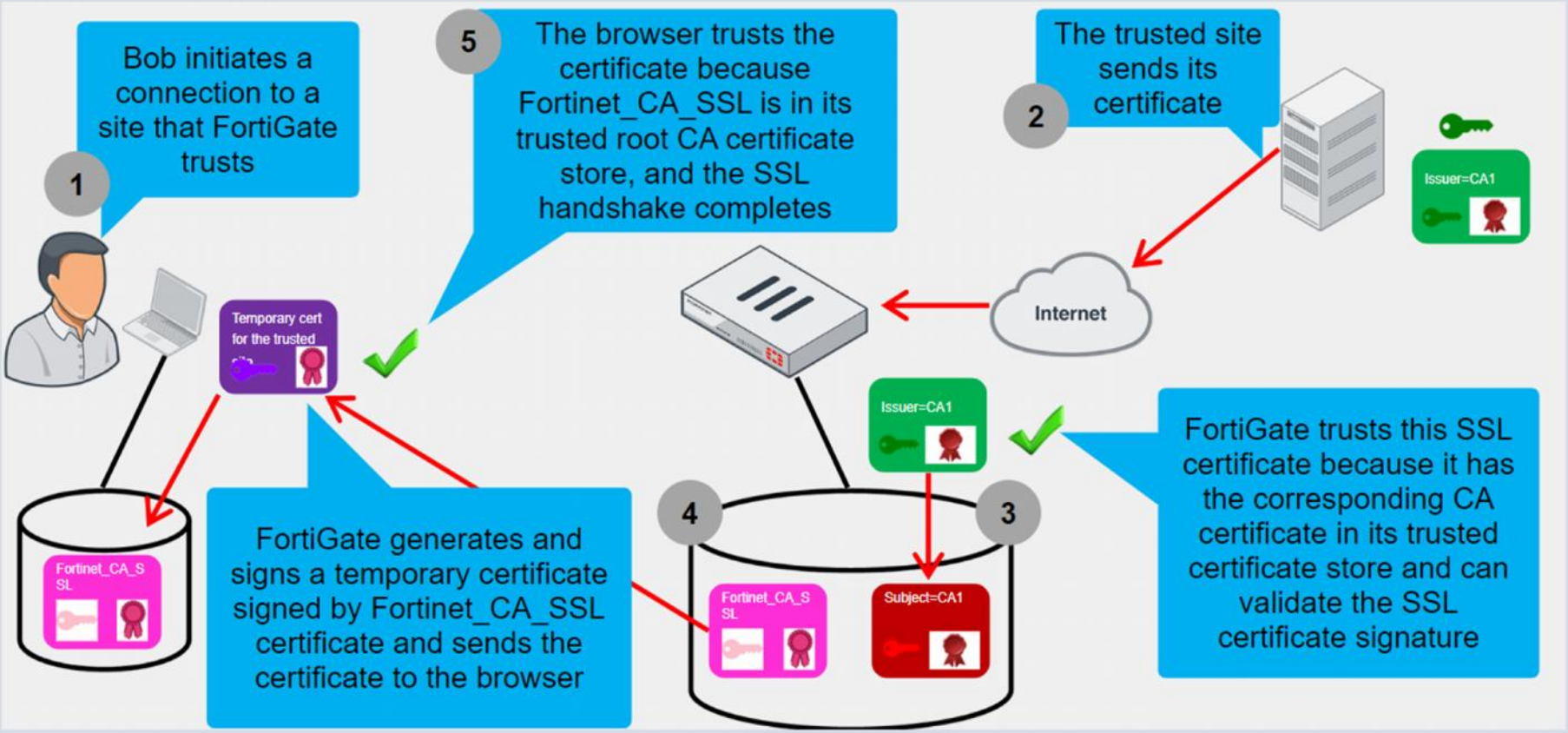
Inspection de certificat SSL

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



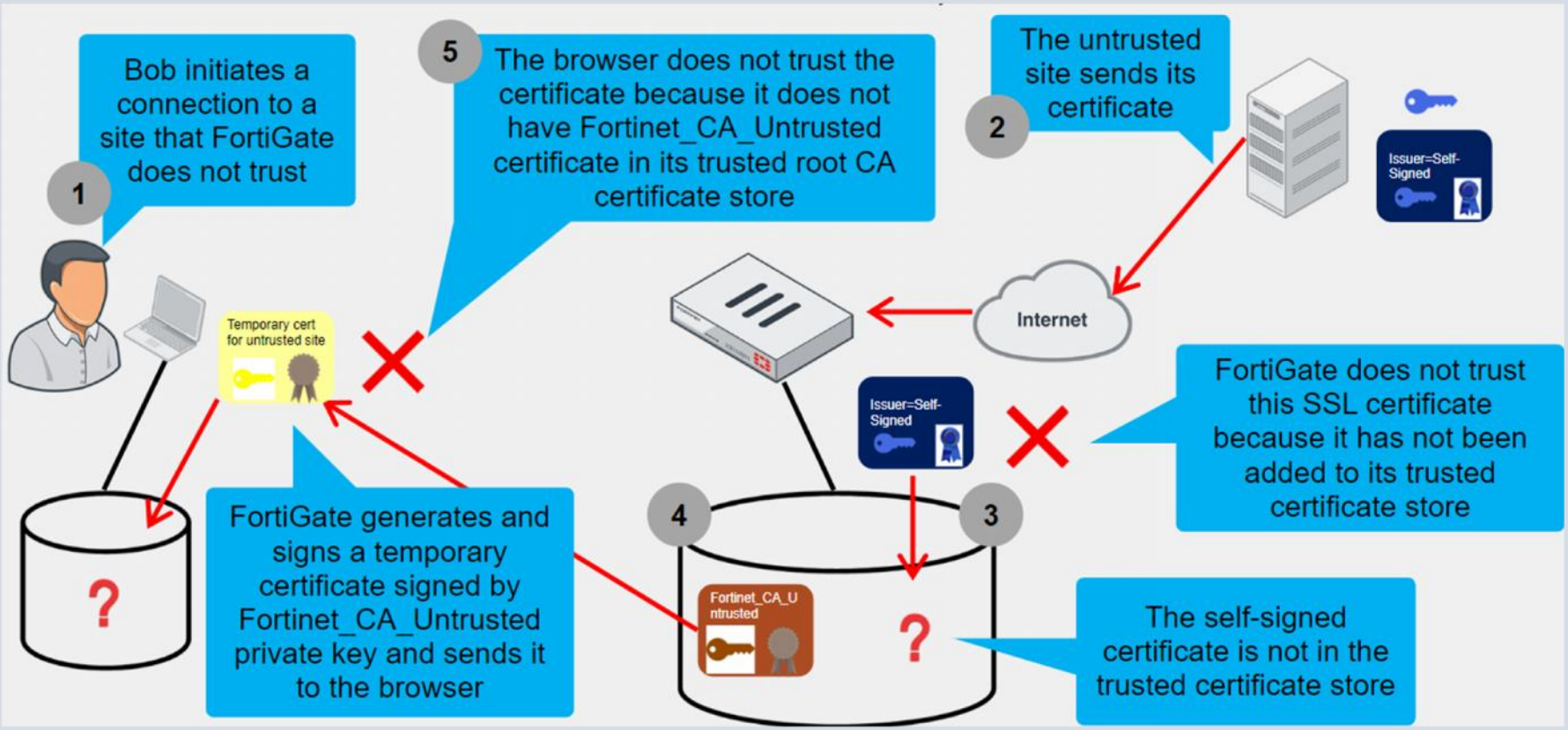
Certificats

Inspection de certificat SSL: Site de confiance



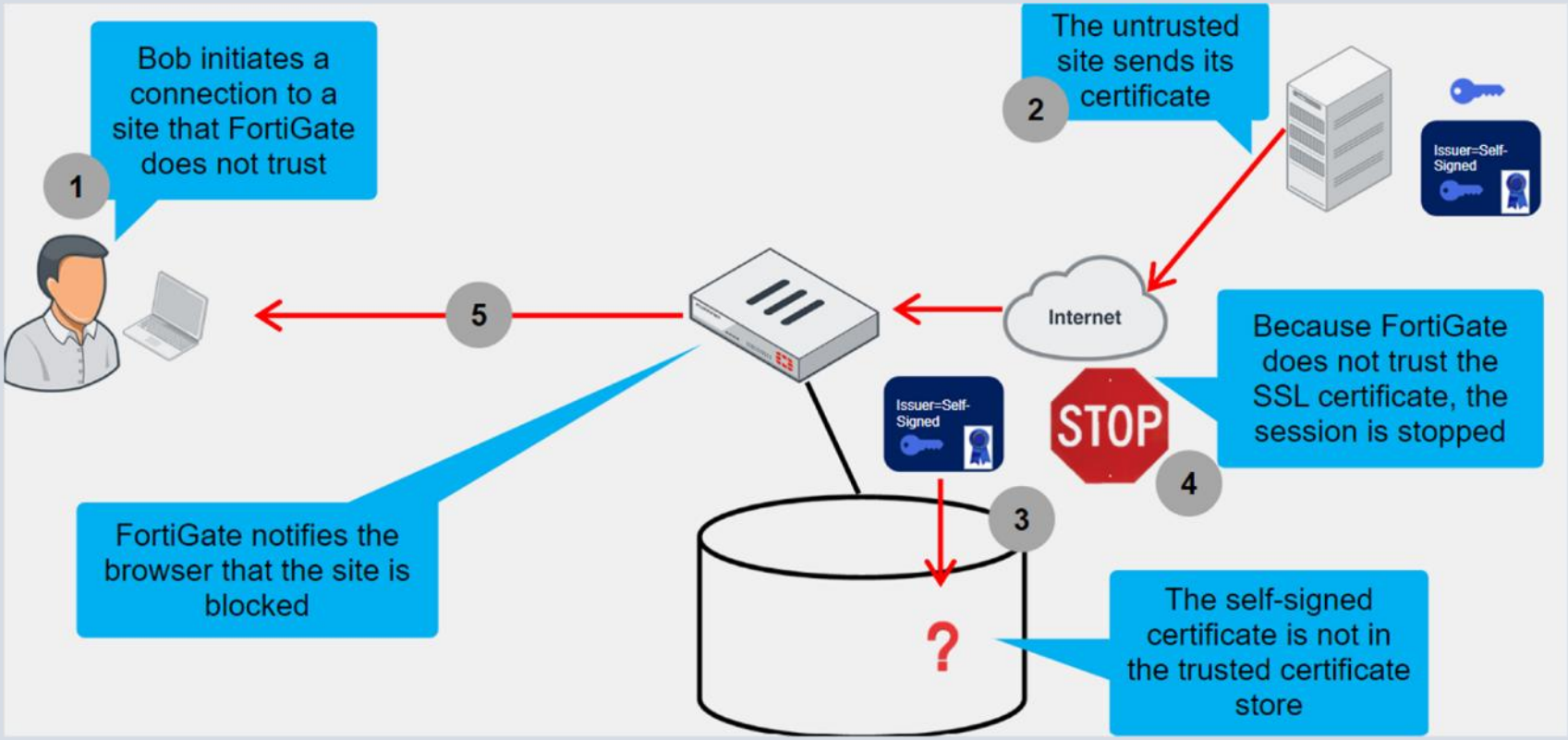
Certificats

Inspection de certificat SSL: Site de non confiance - Autorisation



Certificats

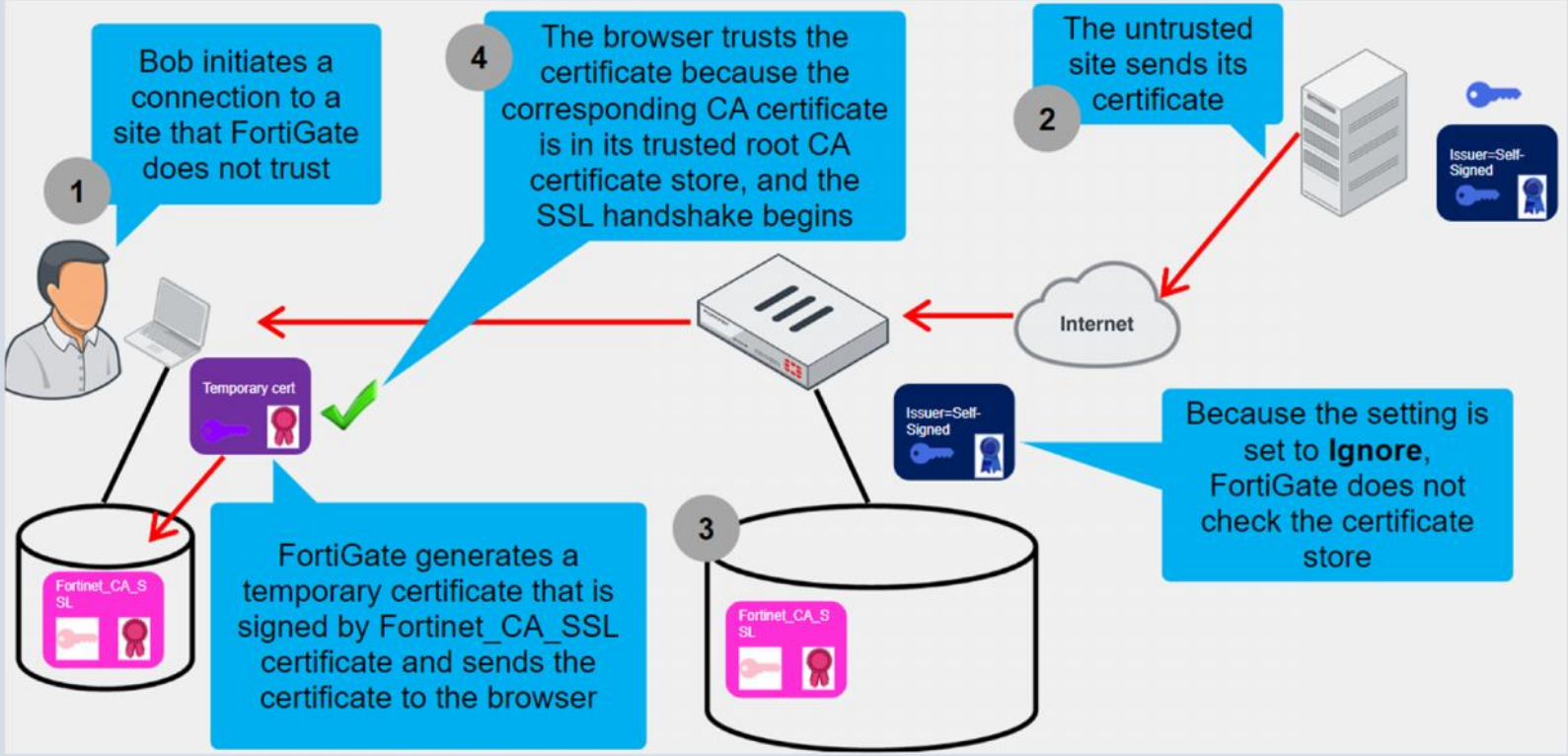
Inspection de certificat SSL: Site de non confiance - Blocage



Certificats

Authentification et sécurisation | Inspection de trafic (suite) | Gestion des certificats

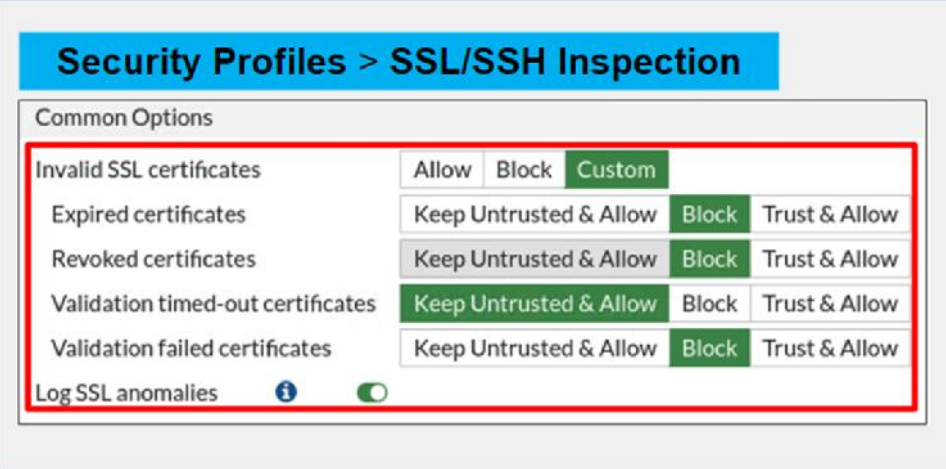
Inspection de certificat SSL: Site de non confiance - Ignorer



Certificats

Inspection de certificat SSL: Certificat invalide

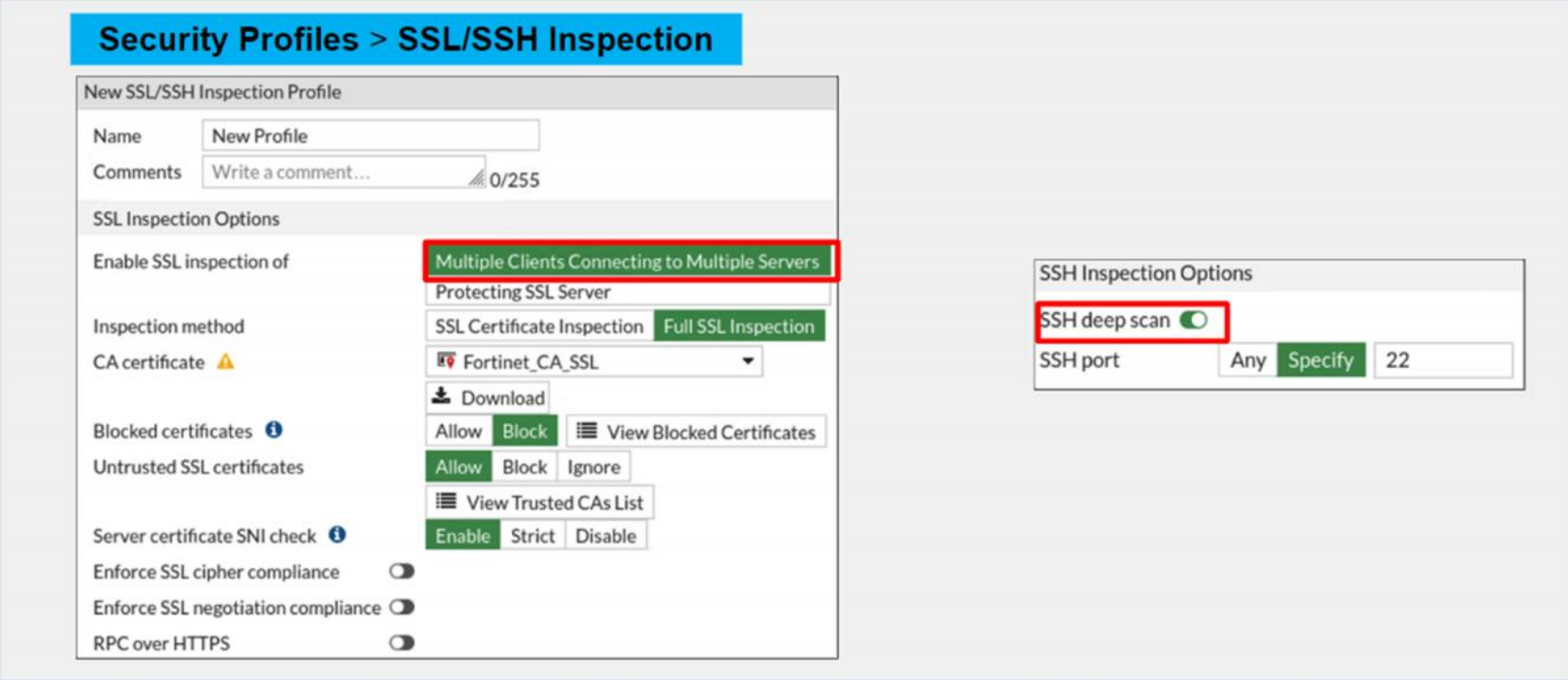
- Détection de certificat invalide:
  - Expiration;
  - Révocation;
  - Time de validation dépassé;
  - Echec de validation.
- Action configurable:
  - Keep unstruted & allow;
  - Block
  - Trust & Allow



Certificats

Inspection SSH: Configuration

- Uniquement utilisé par les profils antivirus

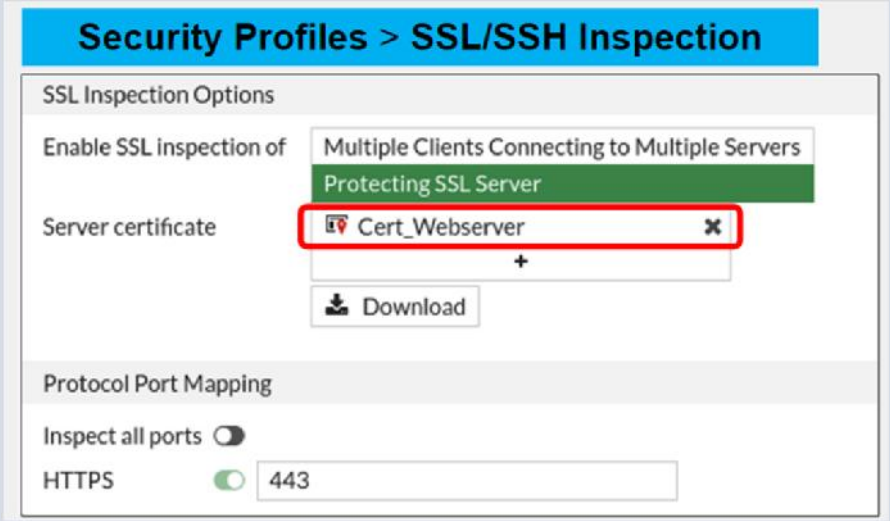


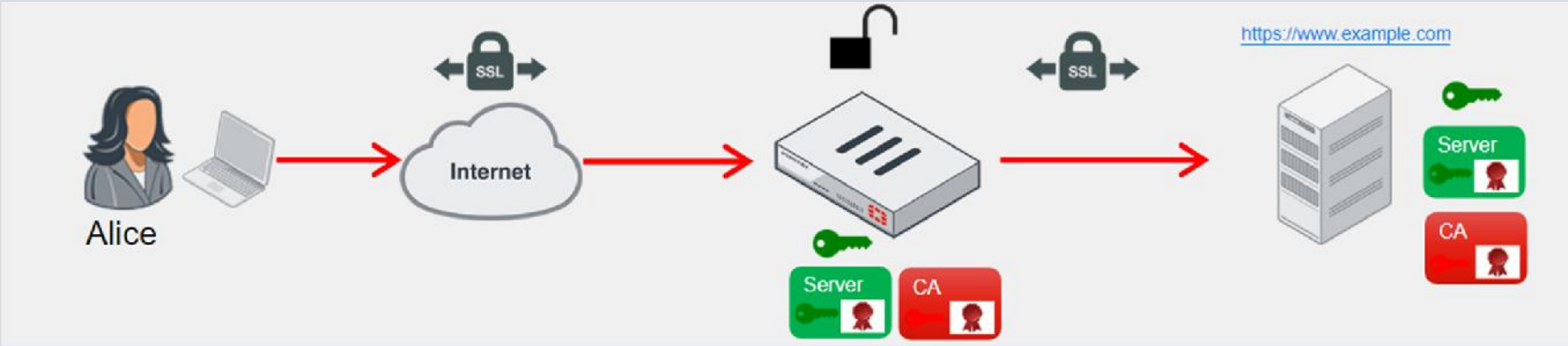
Certificats

Authentification et sécurisation | Inspection de trafic (suite) | Gestion des certificats

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 lé FortiGate

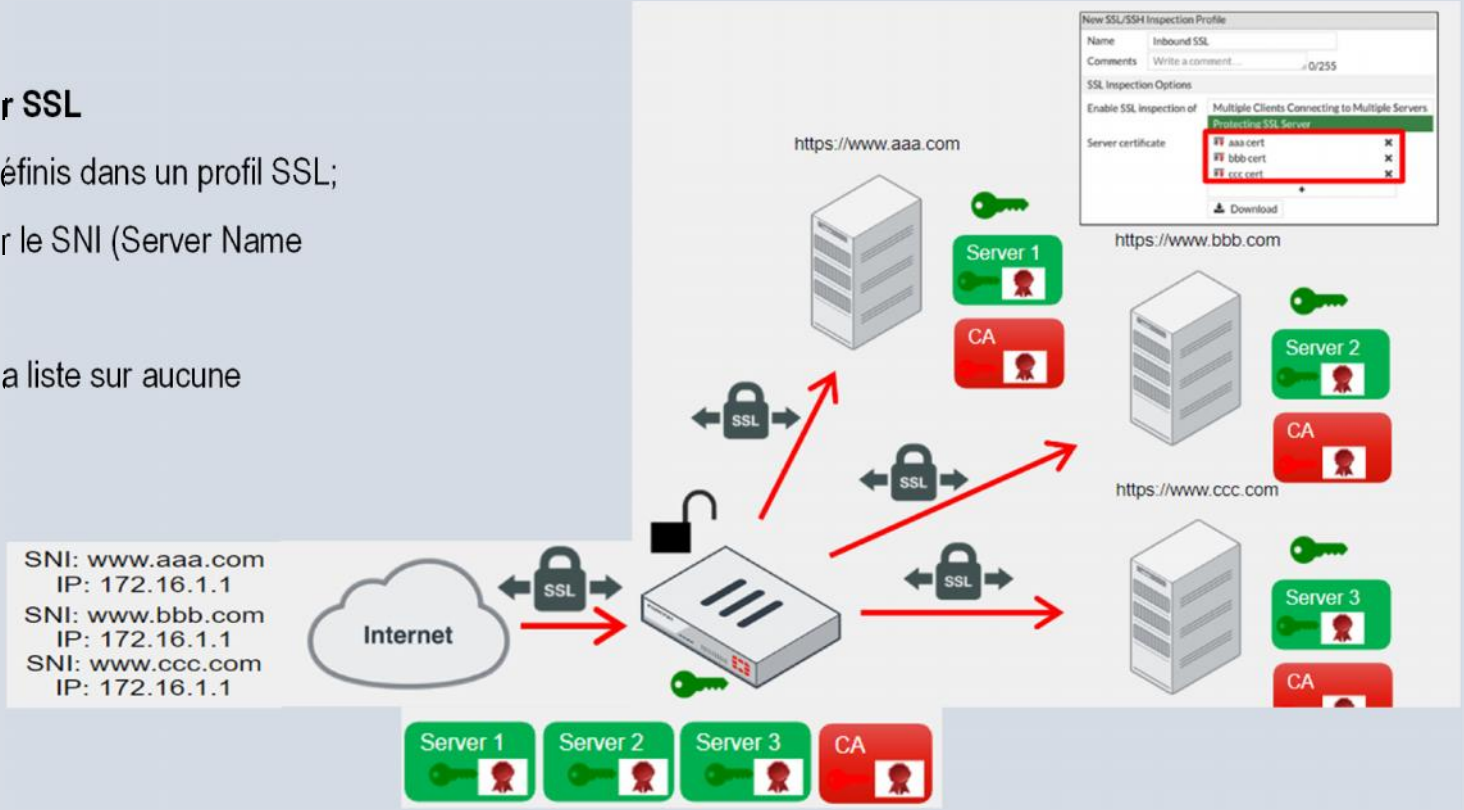




Certificats

Inspection SSL: Protection d'un serveur SSL

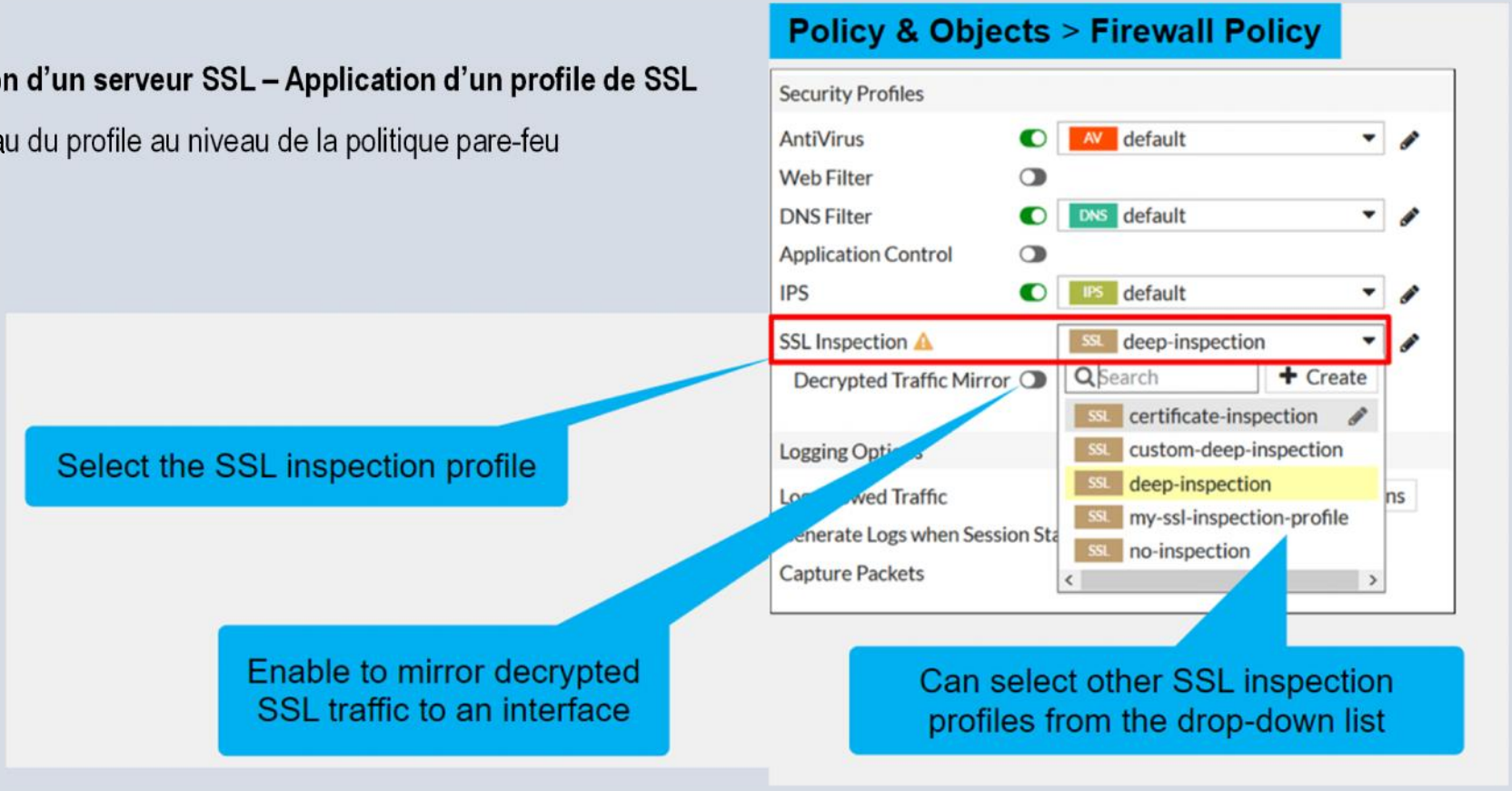
- Plusieurs certificats peuvent être définis dans un profil SSL;
  - Sélection du certificat basée sur le SNI (Server Name Indication);
  - Sélection du 1er certificat dans la liste sur aucune correspondance.



Certificats

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



Certificats

Authentification et sécurisation

Inspection de trafic (suite)

Gestion des certificats

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

Certificats

HTPS et HPKP: Limites et incidents

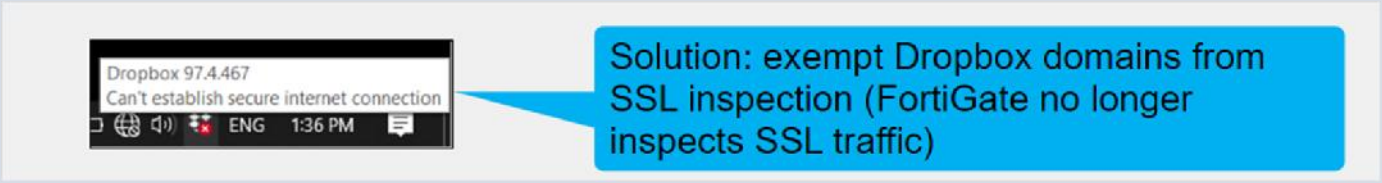
- Exclure les sites web de l'inspection SSL complet (Full Inspection
- Utiliser l'inspection de certificat SSL à la place
- Utiliser des navigateurs web qui ne supporte pas HPKP comme Chrome, Internet Explorer ou Edge
- Désactiver les paramètres de sécurités sur les navigateurs.

Certificats

Inspection SSL et Applications

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

- Dropbox

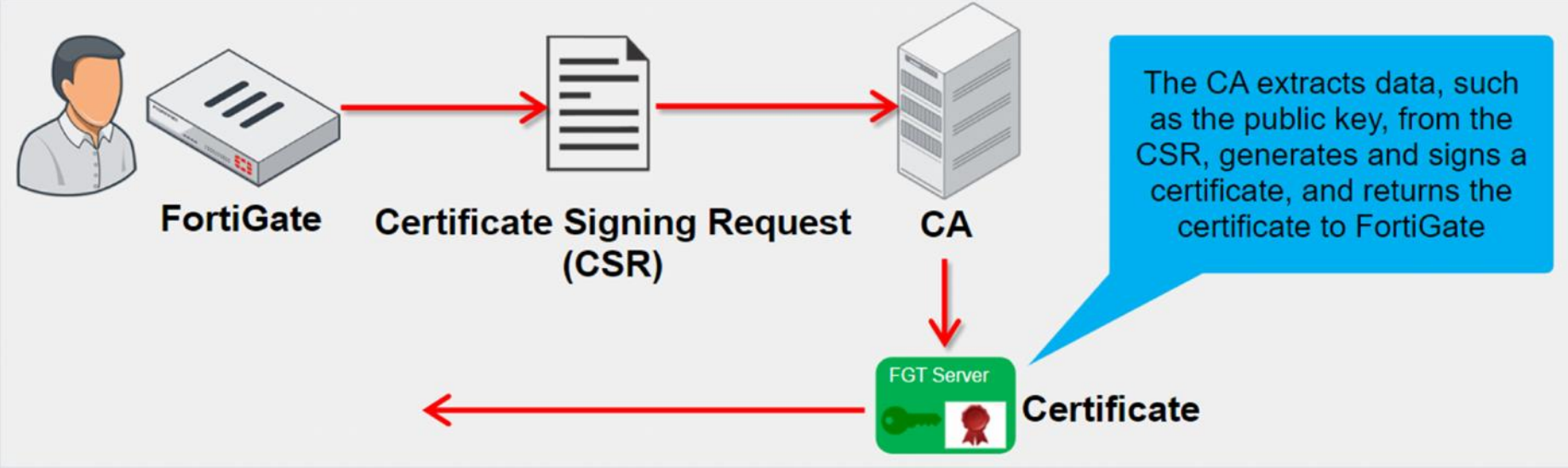


Certificats

Authentification et sécurisation | Inspection de trafic | Gestion des certificats

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

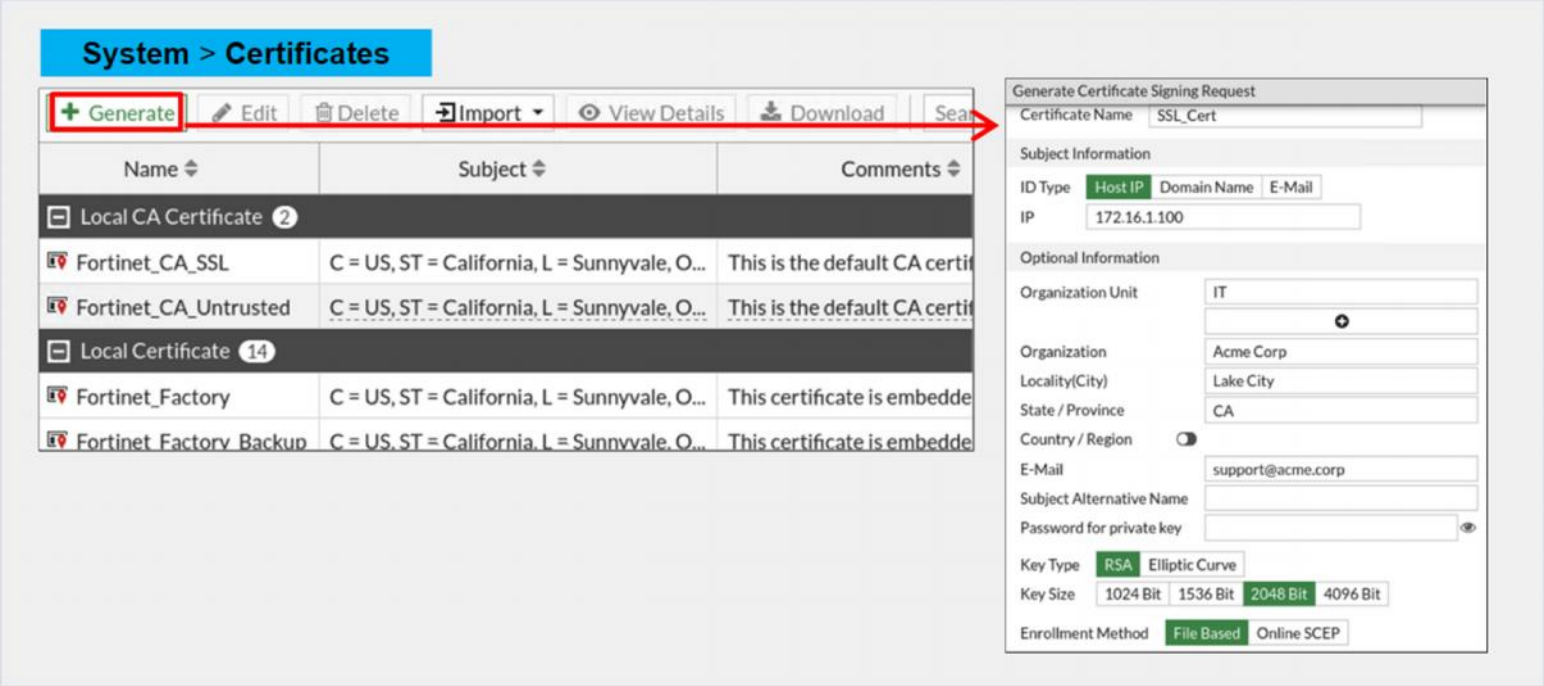
- Génération du CSR au niveau du FortiGate;
- Soumission du CSR au CA;
- Vérification du CSR par le CA;
- Création et envoie du certicat.



Certificats

Génération d'un CSR (Certificate Signing Request)

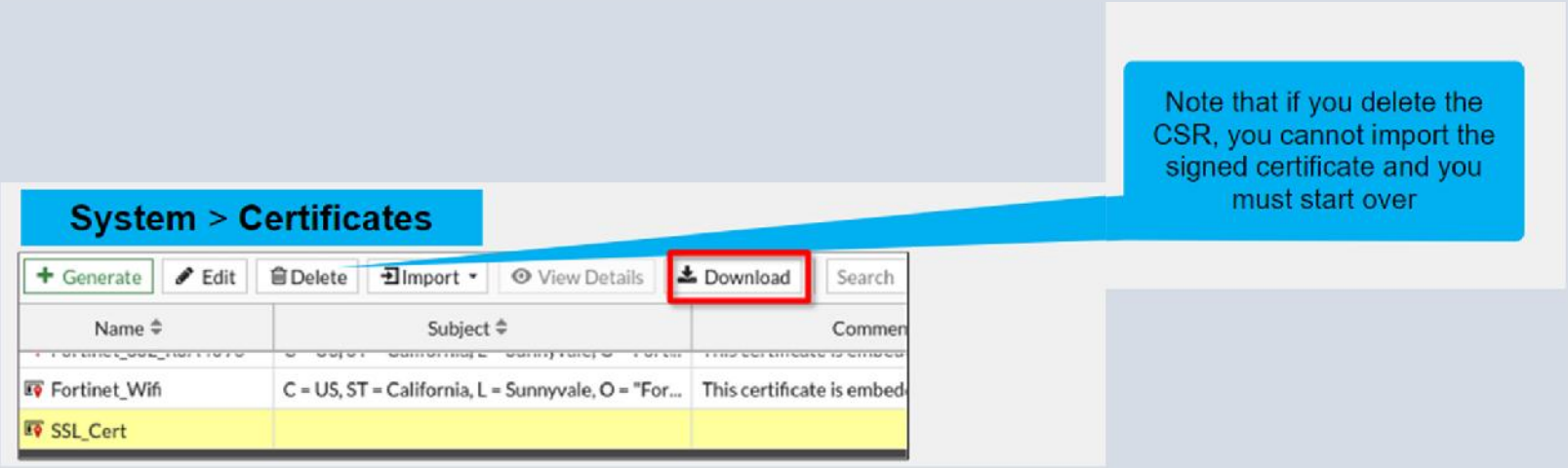
- Fichier: génération d'un fichier au format .CSR;
- SCEP (Simple Certificate Enreollement Protocol) : disponible sur FortiAuthenticator.



Certificats

Enregistrement du CSR (Certificate Signing Request)

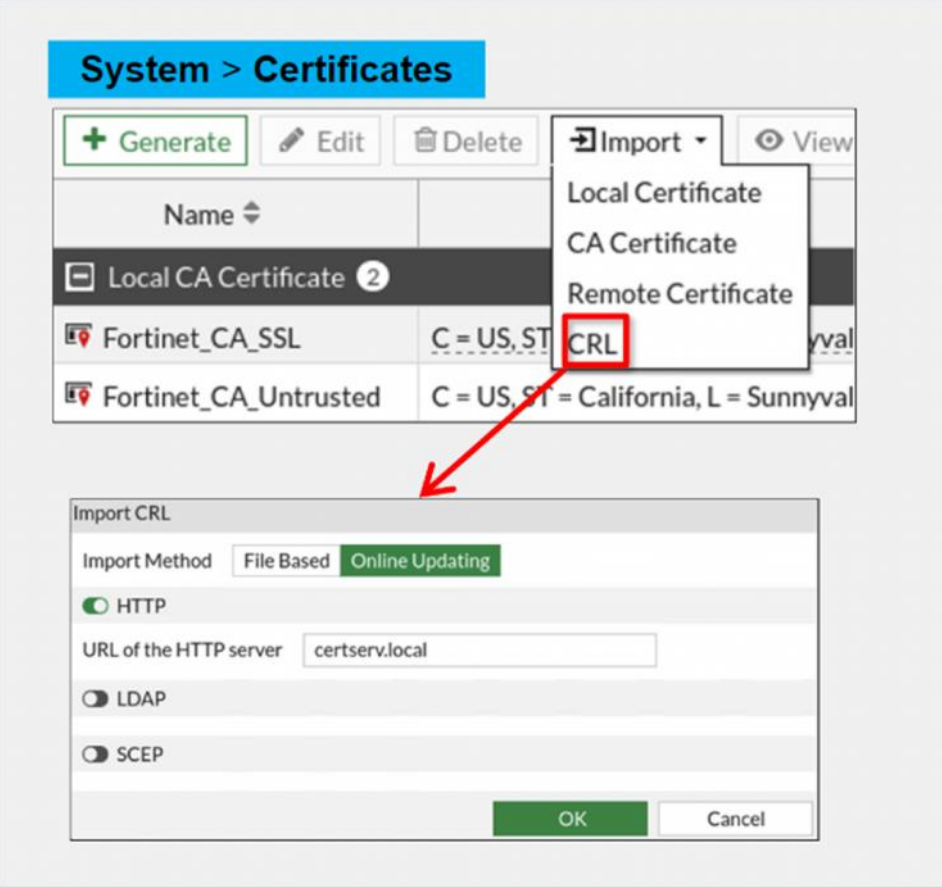
- Sélection et téléchargement du certificat dans le magasin de certificat du FortiGate;
- Soumissions au CA pour vérification.



Certificats

Importation d'une CRL (Certificat Revocation List)

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

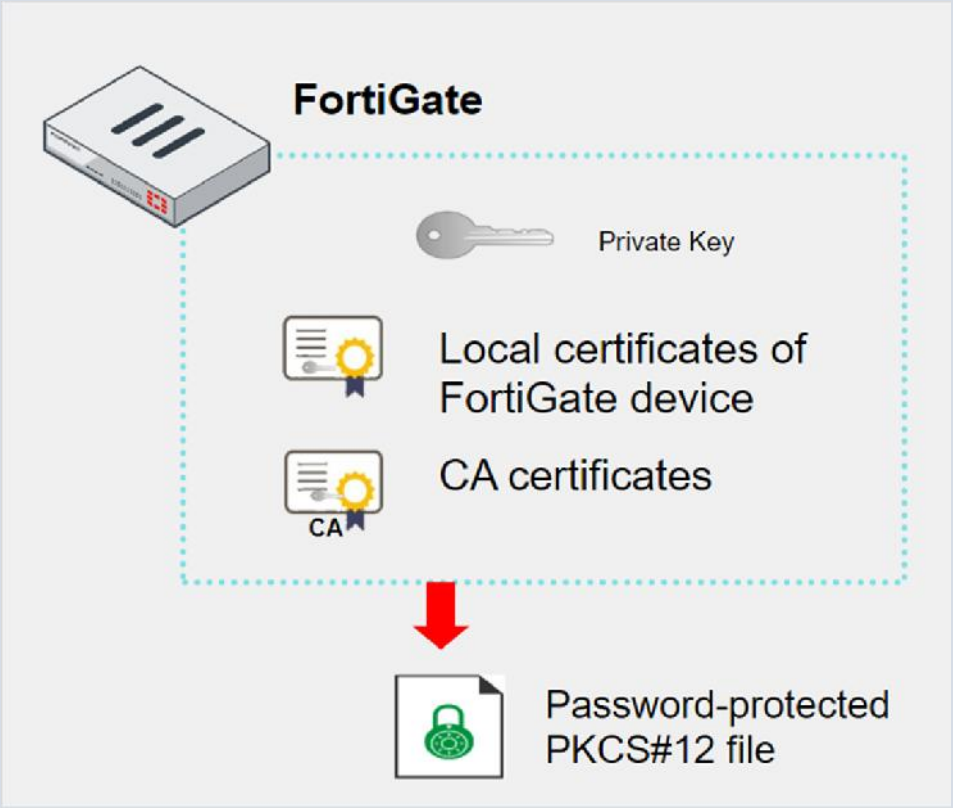


Certificats

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>.
```




FORTINET®

FORTINET
NSE Training Institute

FortiGate Security

FONCTIONNALITES UTM (UNIIFIED THREATS MANAGEMENT)

Plan du module

- Filtrage URL
- Contrôle d’application
- Antivirus
- IPS et DoS

Filtrage URL

Objectifs

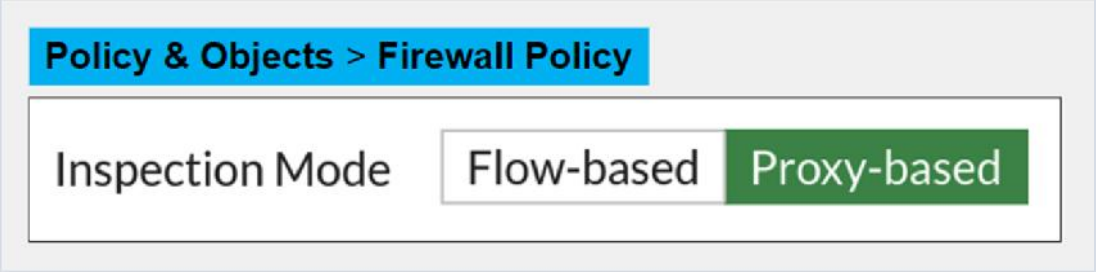
- Identifier les modes d'inspection;
- Comprendre les bases du filtrage URL;
- Configurer le filtrage vidéo;
- Configurer le filtrage DNS et de fichier;
- Bonne pratiques.

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 fflow-bases.



Filtrage URL

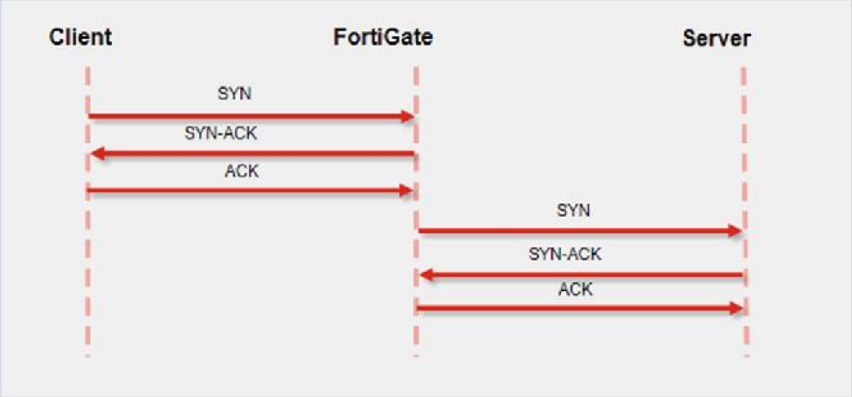
Types: Mode Flow-based

- 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

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 gourmant en ressource.



Filtrage URL

Type: Mode NGFW

- Dispose de 02 modes:
  - Mode profile-based:
    - Nécessité 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

Policy & Objects > Firewall Policy

Inspection Mode | Flow-based | Proxy-based

Customizable at the policy level

Policy & Objects > Protocol Options

Protocol Port Mapping

HTTP	Any	Specify	80
SMTP	Any	Specify	25
POP3	Any	Specify	110
IMAP	Any	Specify	143
FTP	Any	Specify	21
NNTP	Any	Specify	119
MAPI			135
DNS			53
CIFS			445

Protocol ports can be customized

Filtrage URL

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.

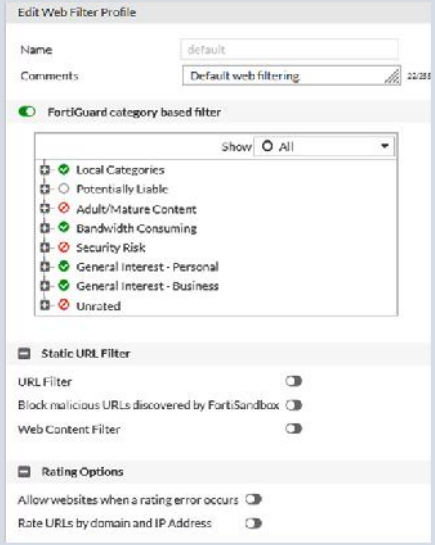
Filtrage URL

Filtrage URL: Configuration

Mode profiles based

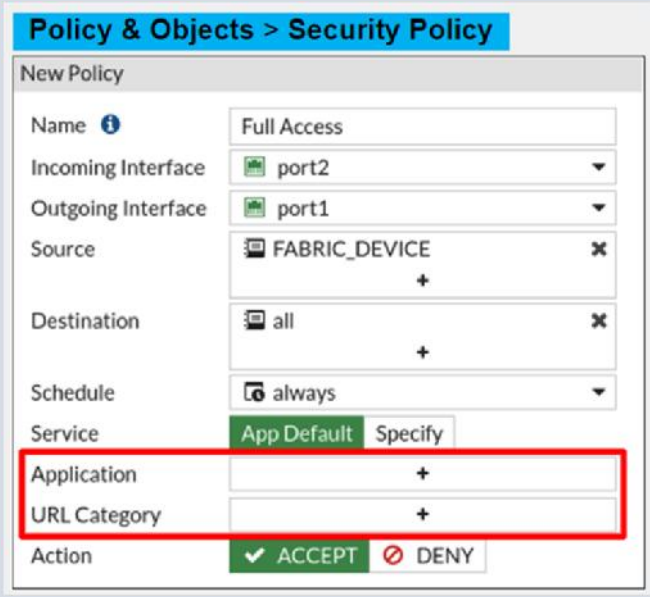
- Configuration d'un profil de sécurité web
  - Catégories préconfigurées (FortiGuard)
  - URL statique
  - Option d'évaluation
- Application du profil sur la règle de trafic

Security Profiles > Web Filter



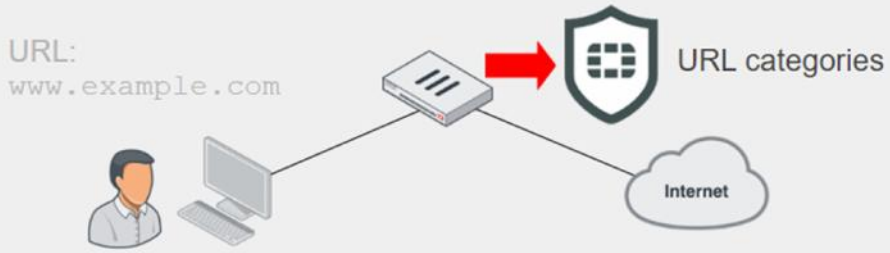
Mode policy based

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

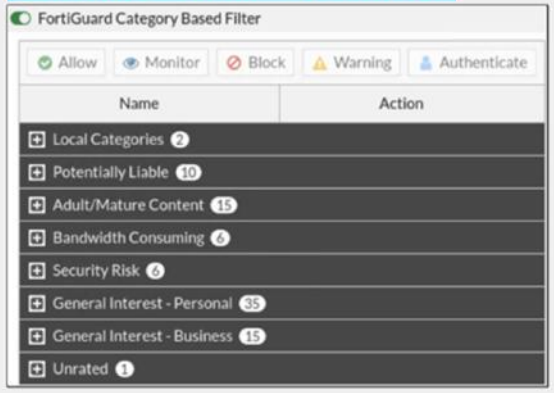


Filtrage URL

Filtrage URL: Fonctionnement



Security Profiles > Web Filter



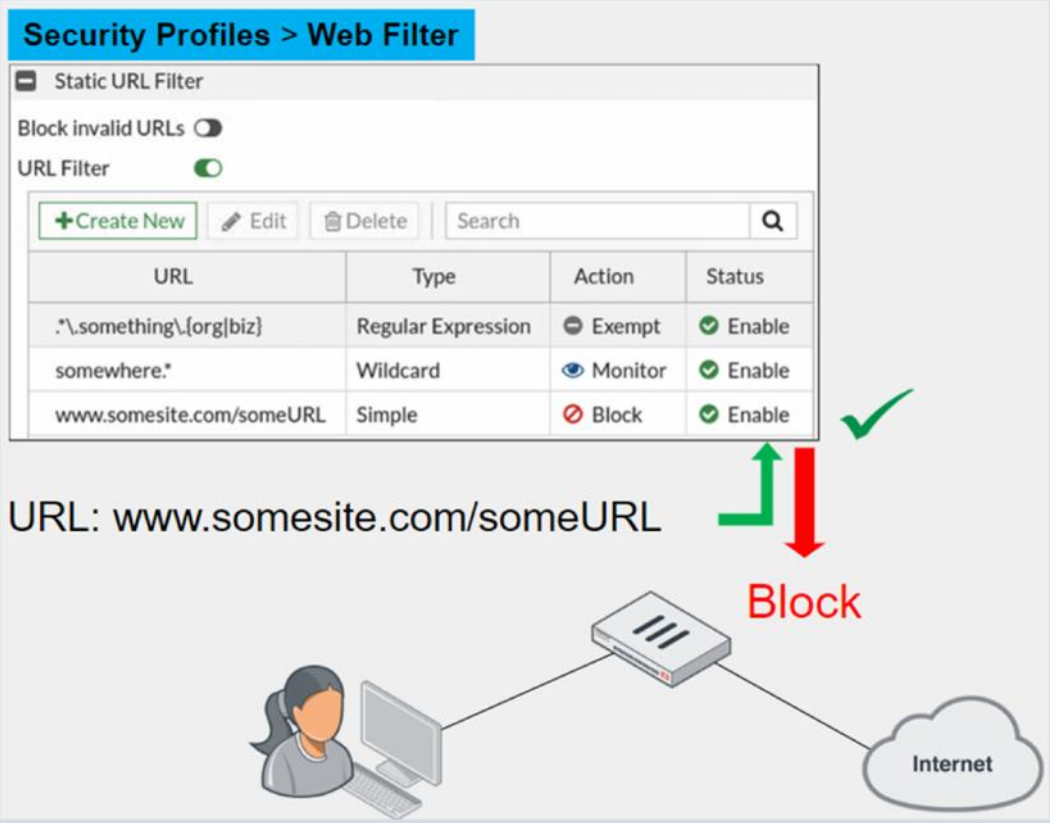
Categories action:

Proxy-Based	Flow-Based (Profile)	Flow-Based (Policy)
Allow	Allow	Accept
Block	Block	Deny
Monitor	Monitor	
Warning	Warning	
Authenticate	Authenticate	

Filtrage URL

Filtrage URL Static: Fonctionnement

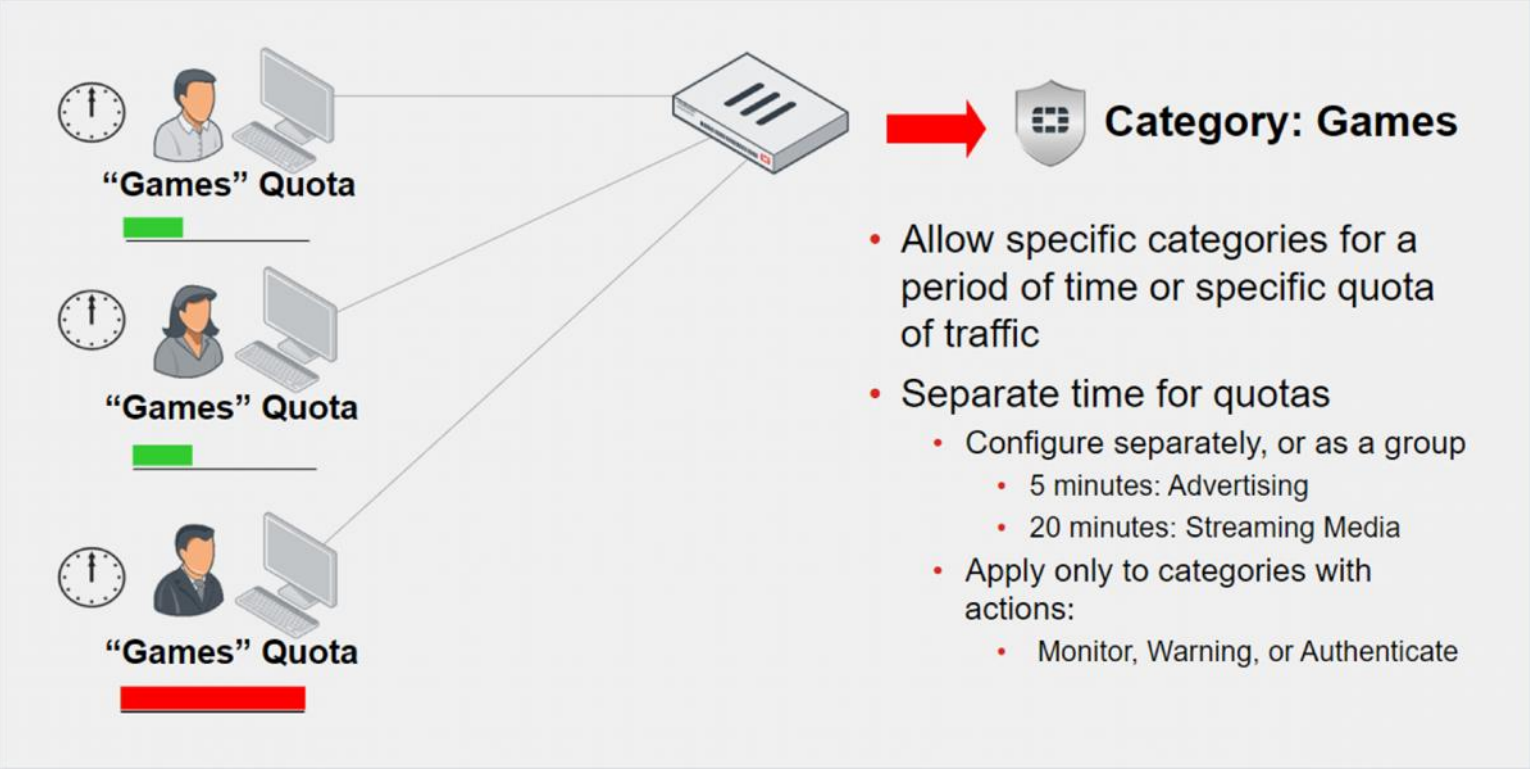
- Vérification de la liste d'URL configurée manuellement;
- 04 actions possible:
  - Allow: Accès permis;
  - Block: Accès interdit;
  - Monitor: Trafic autorisé mais journalisé;
  - Excempt: Trafic autorisé des sources de confiance uniquement.
- Type de modèle d'URL:
  - Simple: www.google.cm;
  - Wildcard: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



Filtrage URL

Filtrage URL : Profile de sécurité en mode policy-based

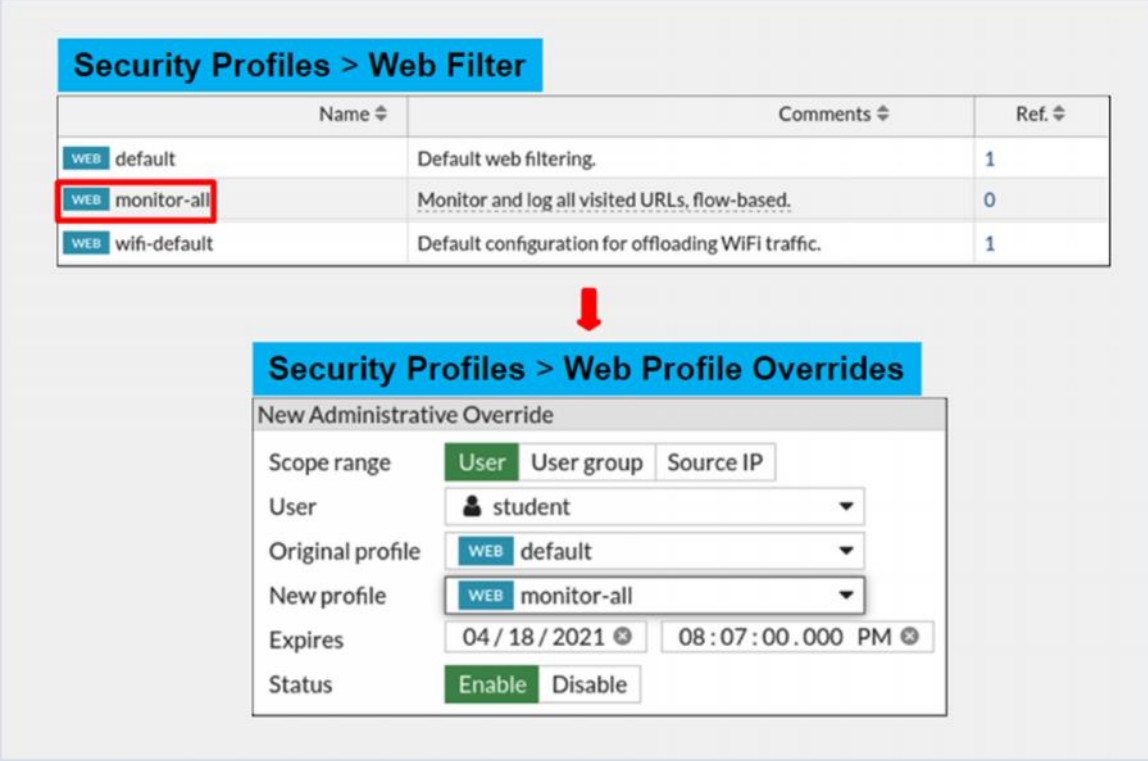
- Fonctionnalité supplémentaires: Quotas d'utilisation



Filtrage URL

Filtrage URL : Profile de sécurité en mode policy-based

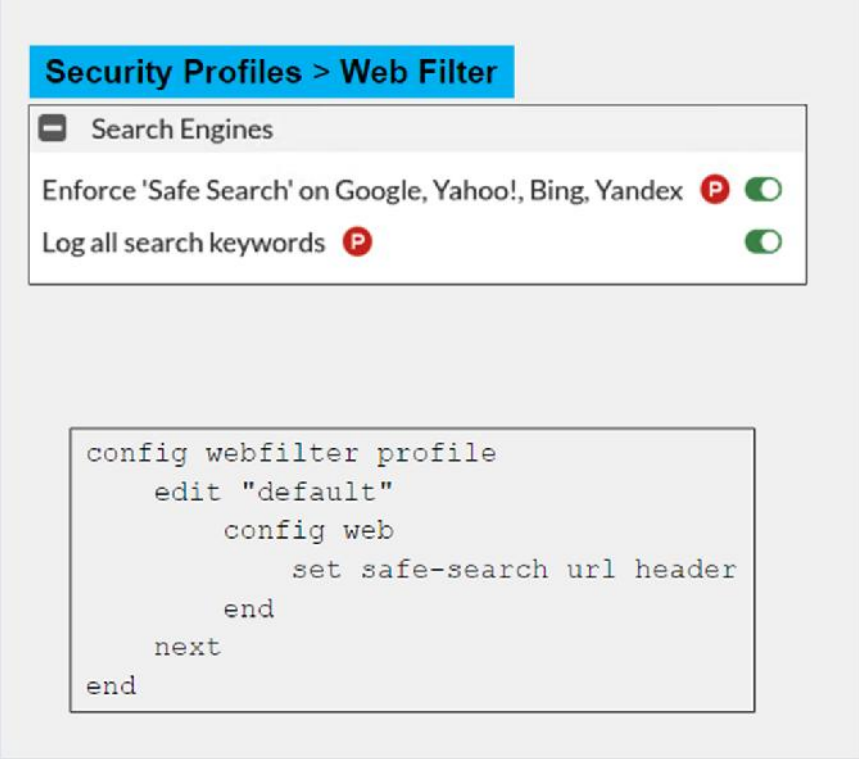
- Fonctionnalité supplémentaires: Remplacement du profil Web (Web Profile Override)
  - Permet à un utilisateur, un groupe d'utilisateur ou une IP source d'utilisé un profil web différent



Filtrage URL

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

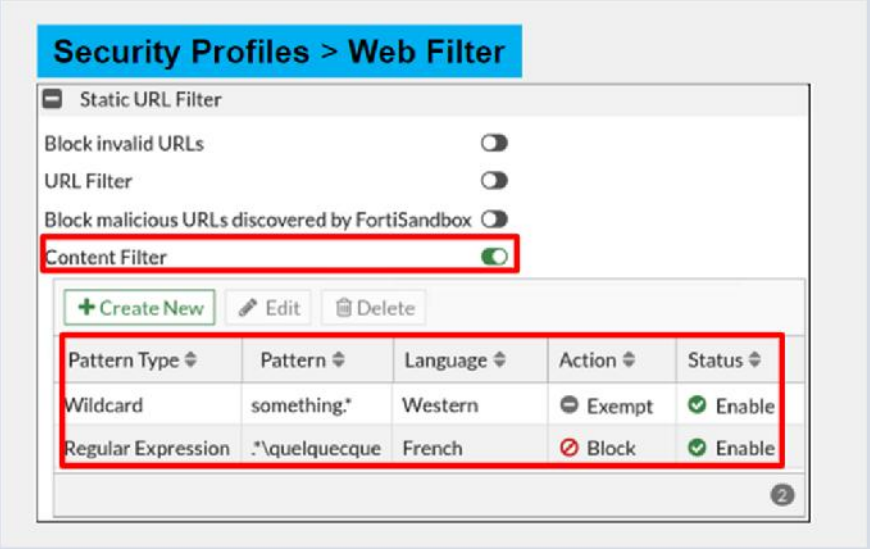



```
config webfilter profile
    edit "default"
        config web
            set safe-search url header
        end
    next
end
```

Filtrage URL

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 Excempt;
  - Nécessite l'utilisation de l'inspection SSL affrondie.



Filtrage URL

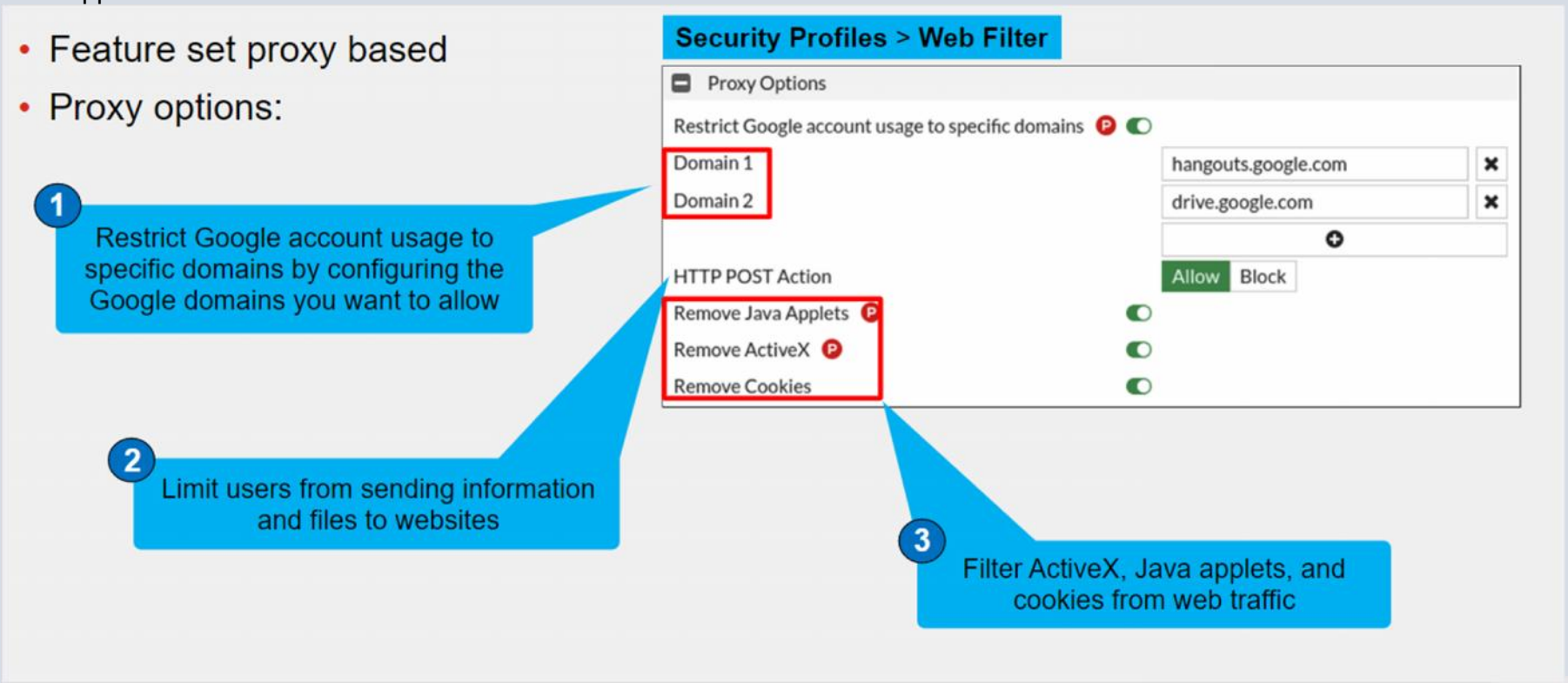
Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Paramètres avancés

Filtrage URL

Filtrage URL : Profile de sécurité en mode policy-based

- Fonctionnalité supplémentaires: Paramètres avancés



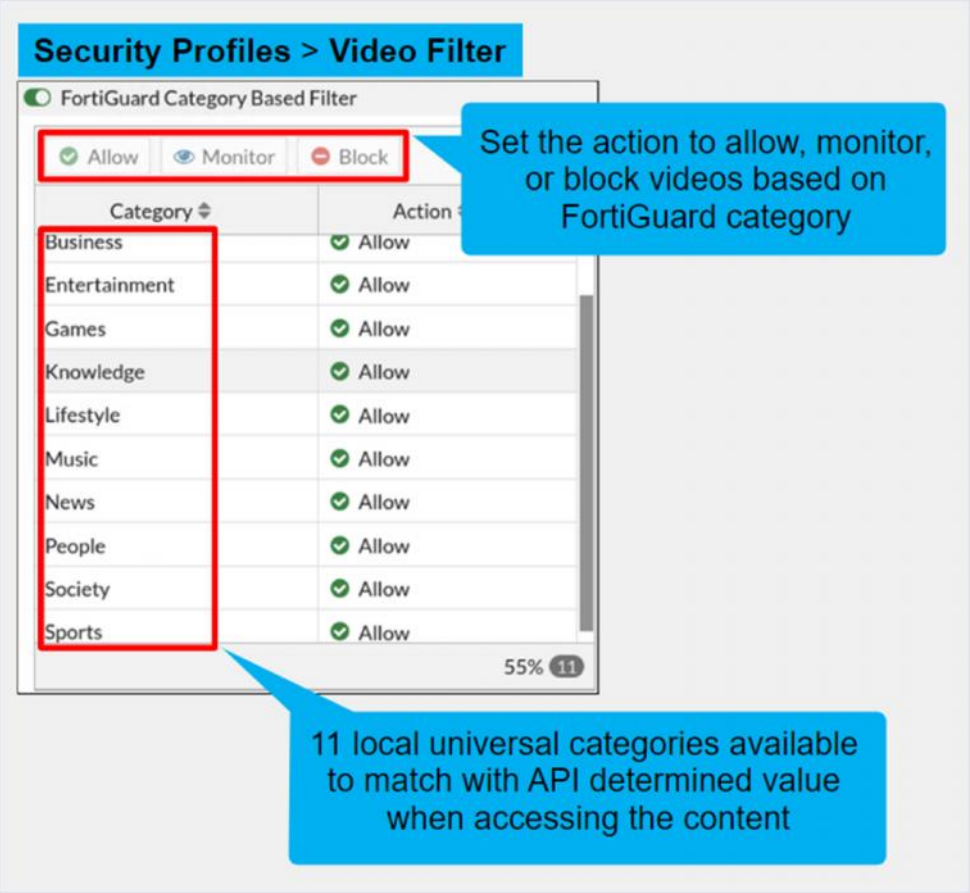
Filtrage URL

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.

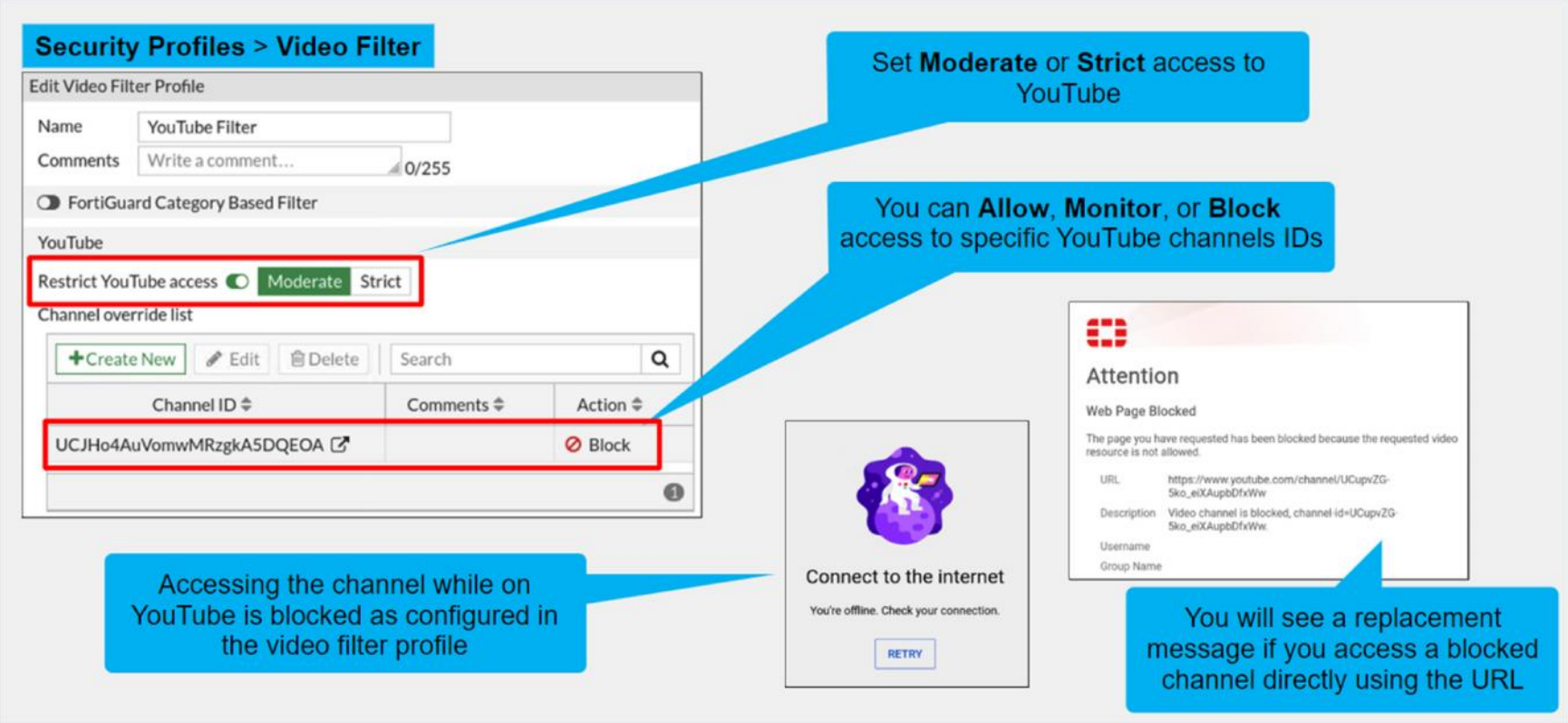
Filtrage URL

Filtrage Vidéo: Catégorie



Filtrage URL

Filtrage Vidéo: Catégorie



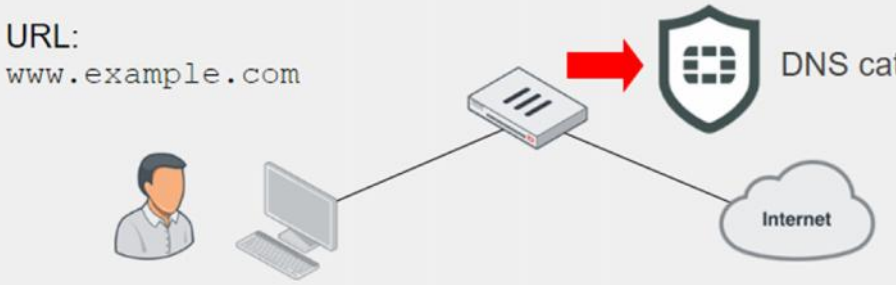
Filtrage URL

Filtrage basé sur le DNS

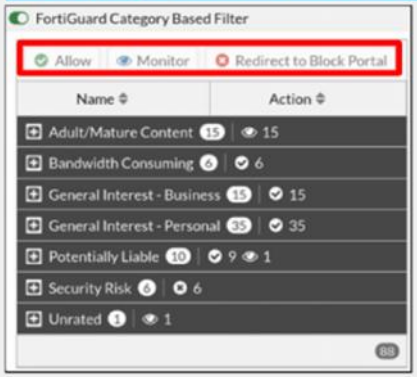
- Inspection du trafic en utilisant les filtres DNS;
- Moins précis que le filtrage basé sur HTTP
- Inspection SSL disponible
  - DNS over TLS (DoT);
  - DNS over HTTPS (DoH)
- Supporte uniquement filtrage URL statiques et les catégories FortiGuard

Filtrage URL

Filtrage basé sur le DNS: Fonctionnement



Security Profiles > DNS Filter



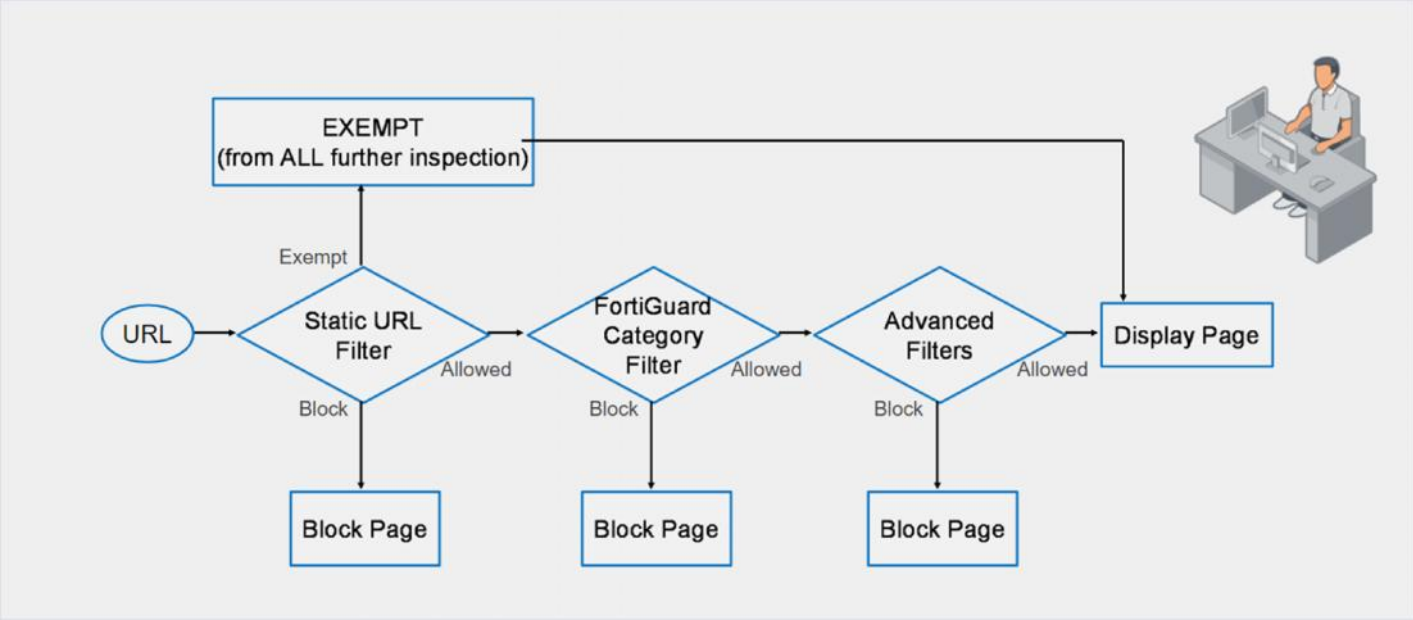
Categories action:

Proxy-Based	Flow-Based (Profile)	Flow-Based (Policy)	DNS Based
Allow	Allow	Security policy action	Allow
Block	Block		Redirect to Block Portal
Monitor	Monitor		Monitor
Warning	Warning		
Authenticate	Authenticate		

Filtrage URL

Bonnes pratiques: Ordre d'inspection HTTP

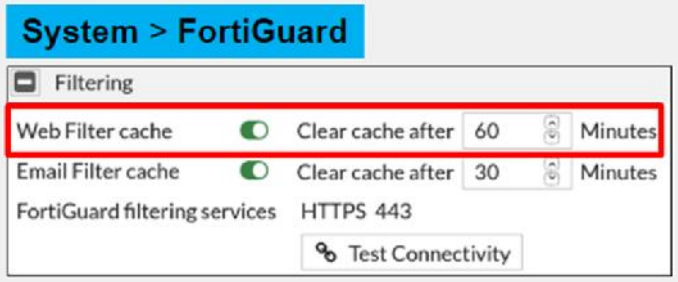
- URL Statique;
- Catégorie d'URL FortiGuard;
- Filtre avancés.



Filtrage URL

Bonnes pratiques: Cache DNS

- Améliore les performances;




```
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

Bonnes pratiques: journalisation

Log & Report > Web Filter

Add Filter | Details

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" msg="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;
- Maitriser quelques bonnes pratiques.

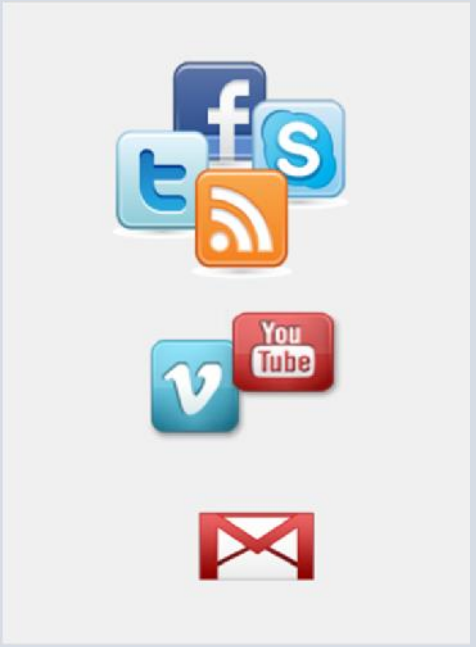
Contrôle d’application

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:

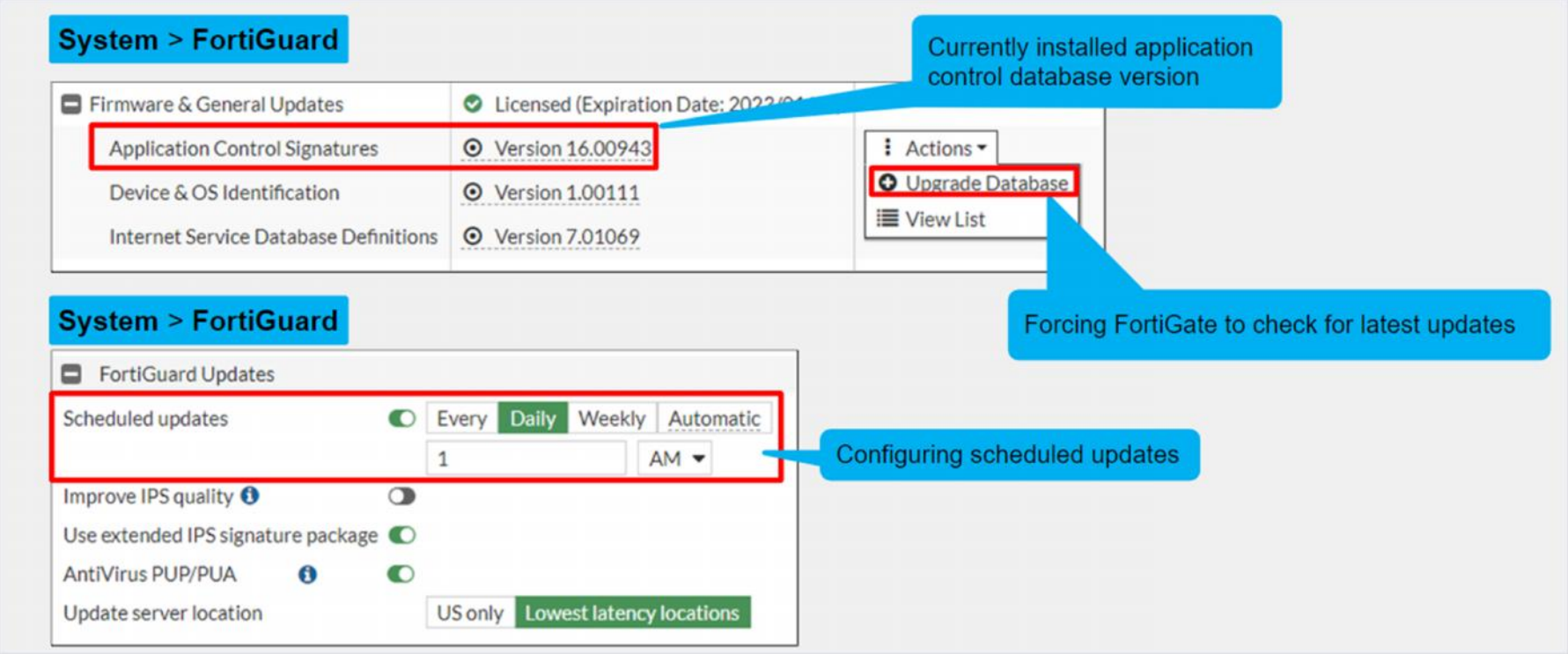
- Configurable dans les 02 modes: Flow et proxy
- Utilisation du moteur IPS;
- Utilisation du mode flow-based par défaut;
- Comparaison du trafic avec les modèles connu.



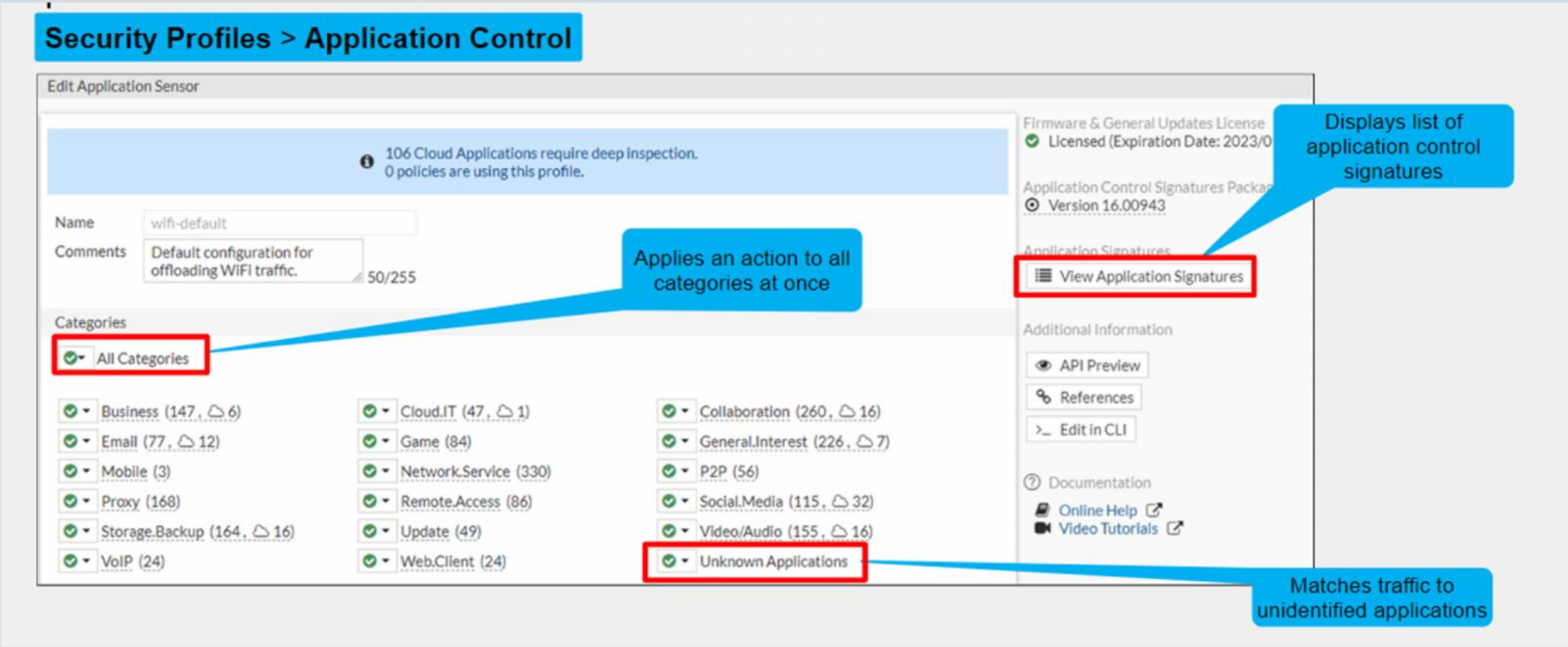
Contrôle d’application

Contrôle d’application: Signature

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

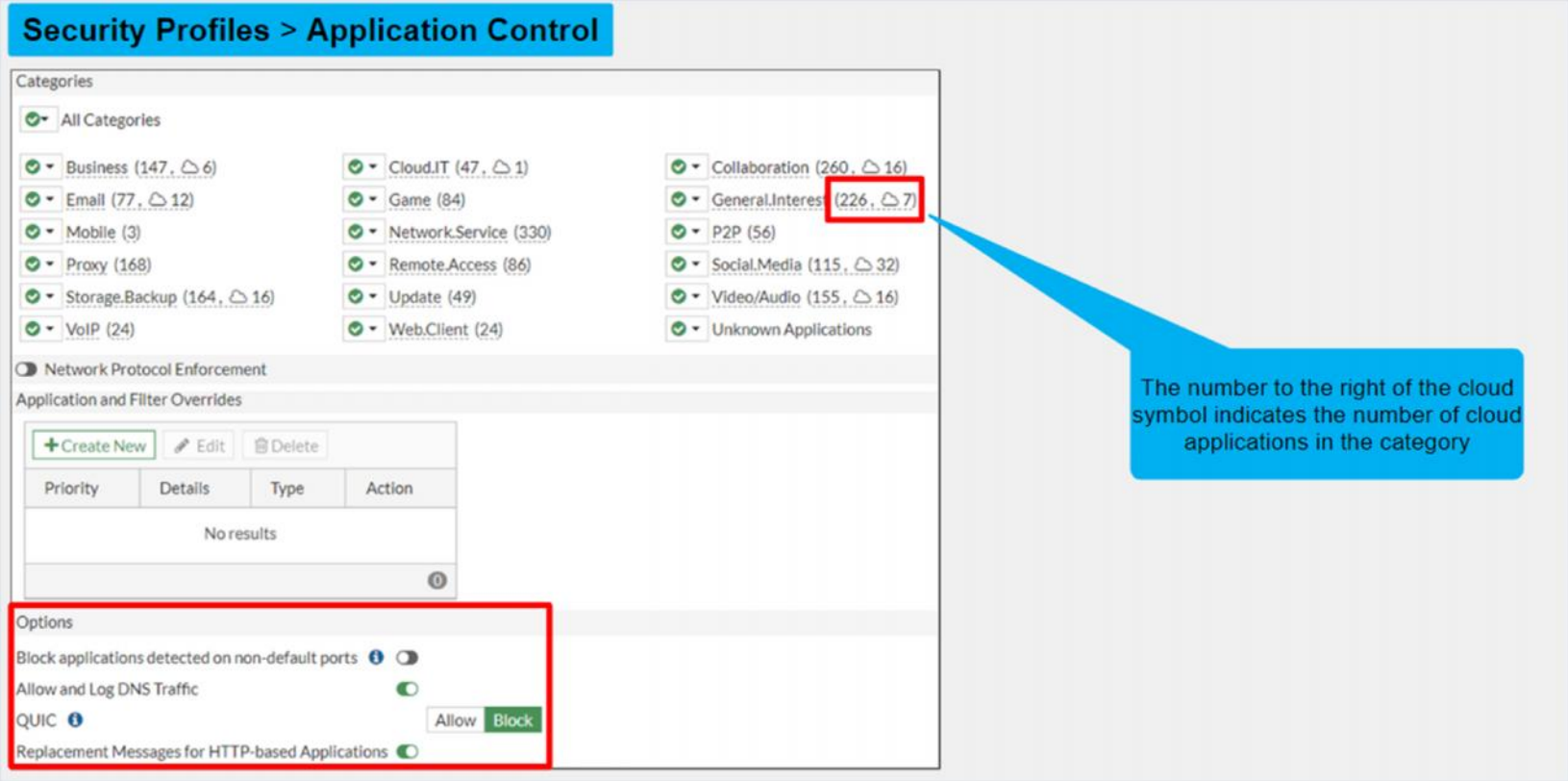


Contrôle d’application



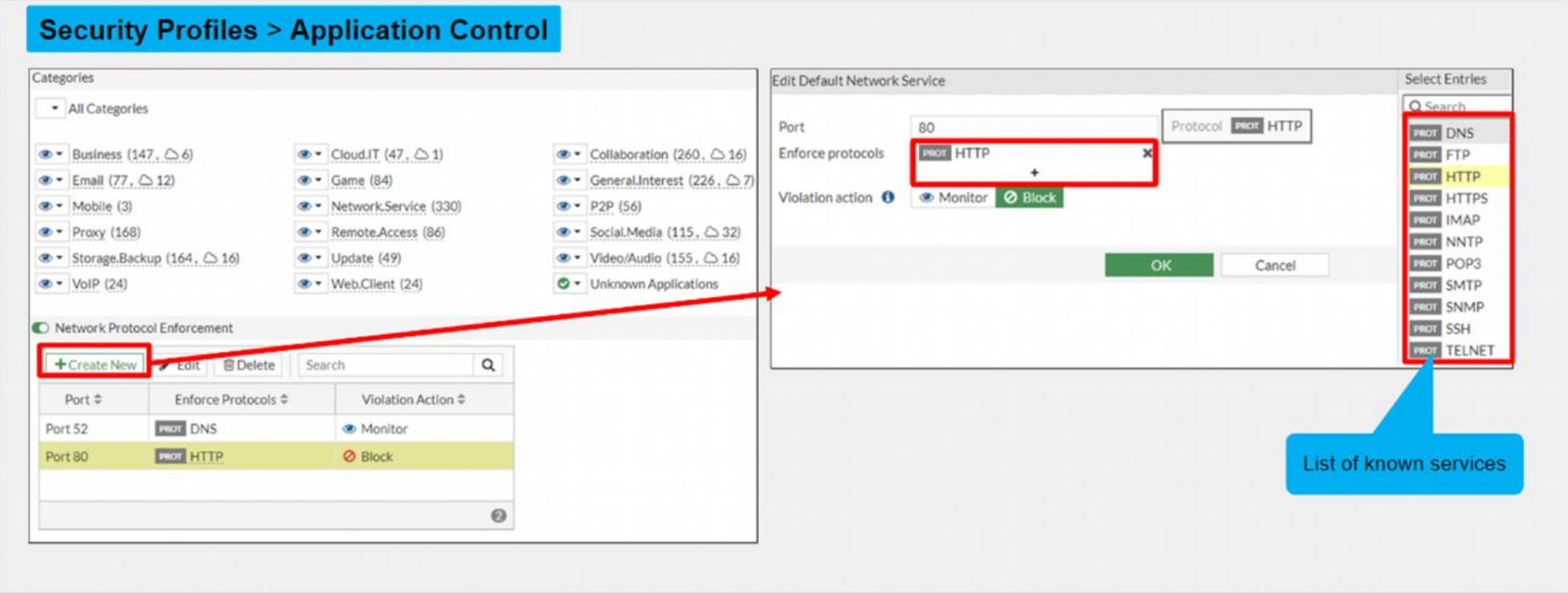
Contrôle d’application

Options avancées.



Contrôle d’application

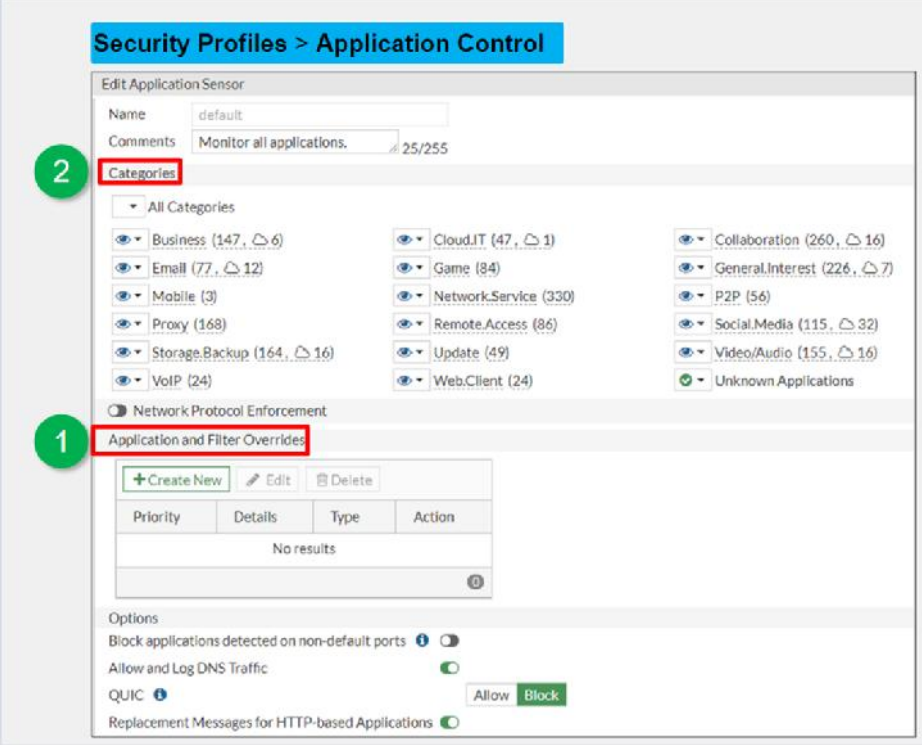
Contrôle de trafic de services sur les ports inconnus



Contrôle d’application

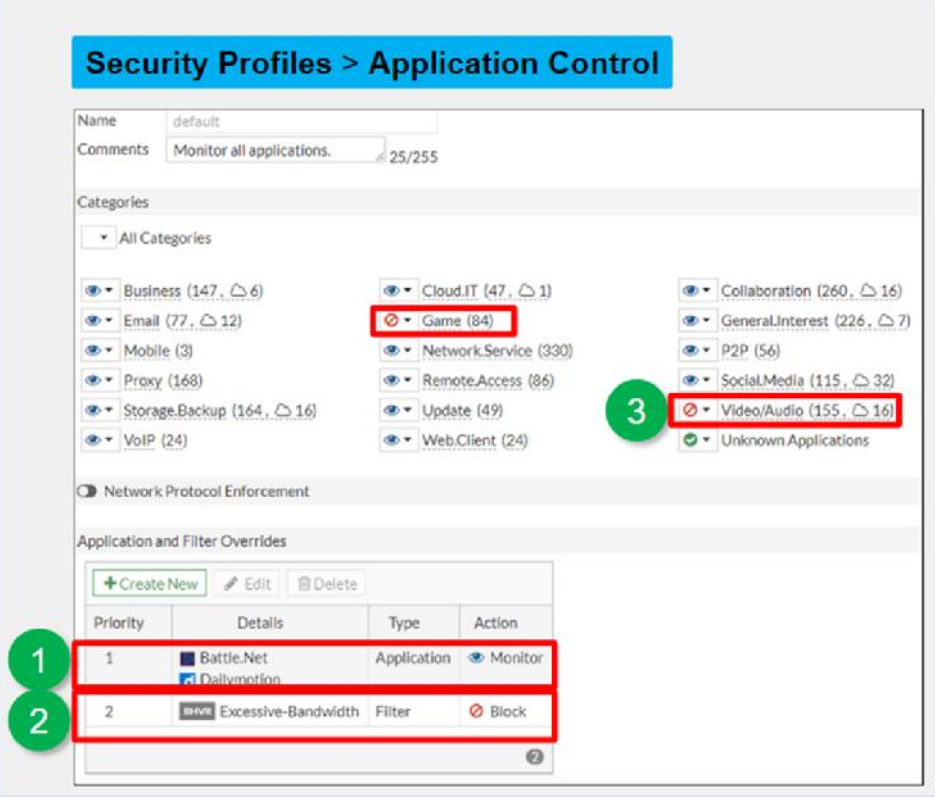
Ordre de scan

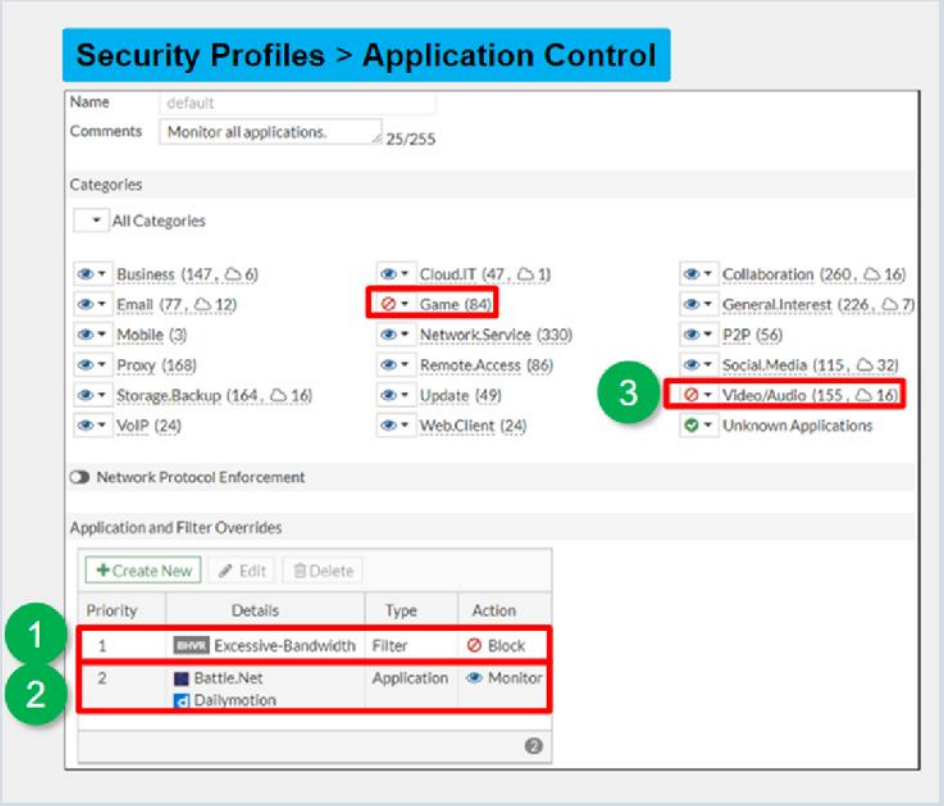
- ❑ Filtre et application statique;
- ❑ Catégories FortiGuard.



Contrôle d’application

Ordre de scan (suite)

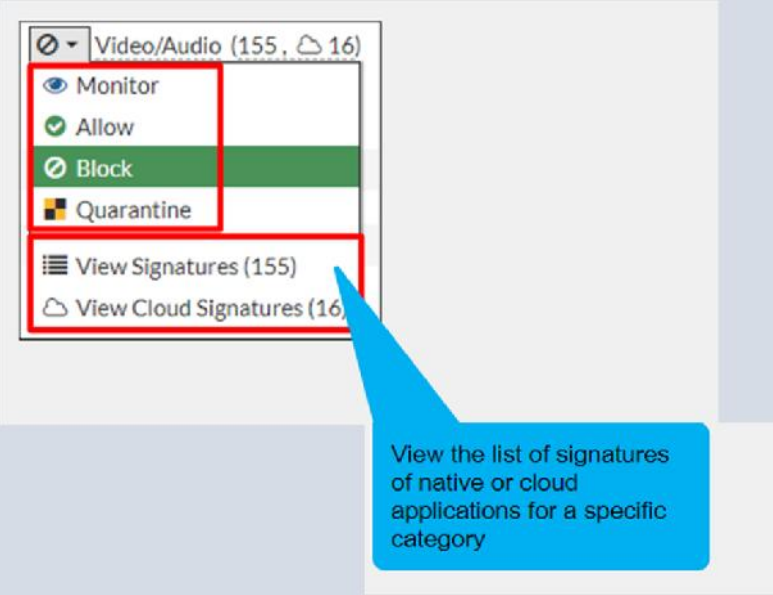




Contrôle d’application

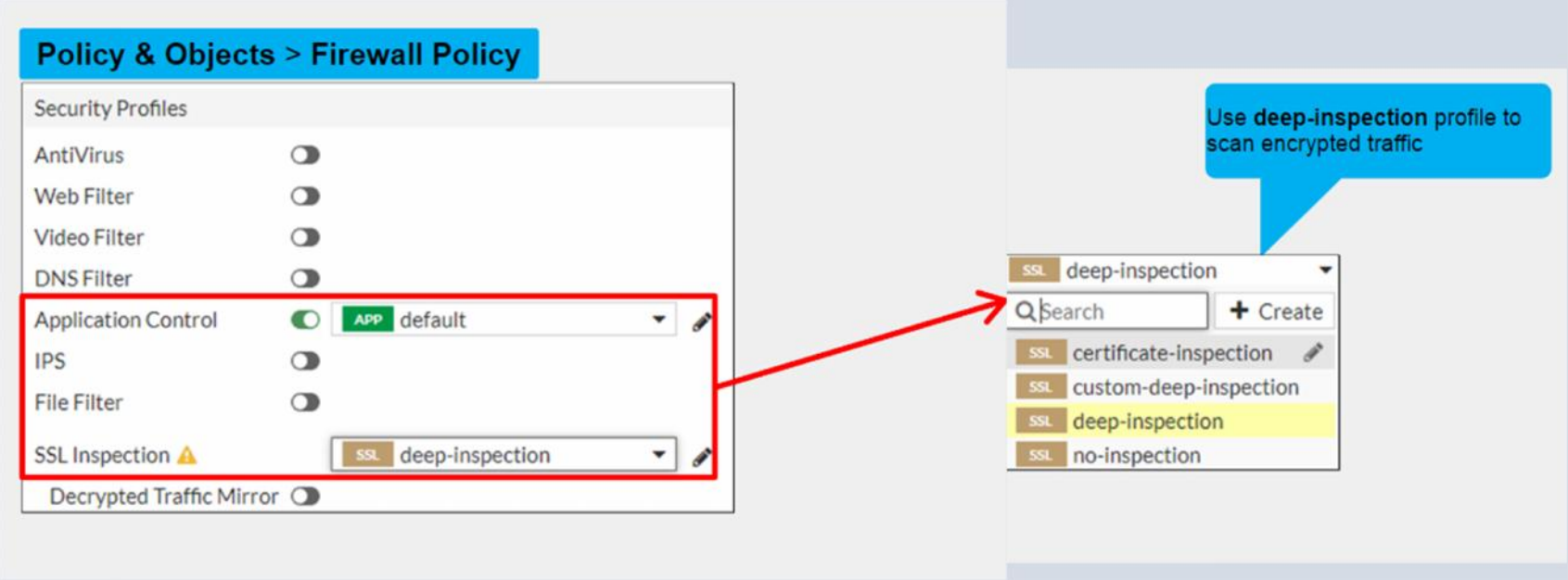
Actions:

- 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.



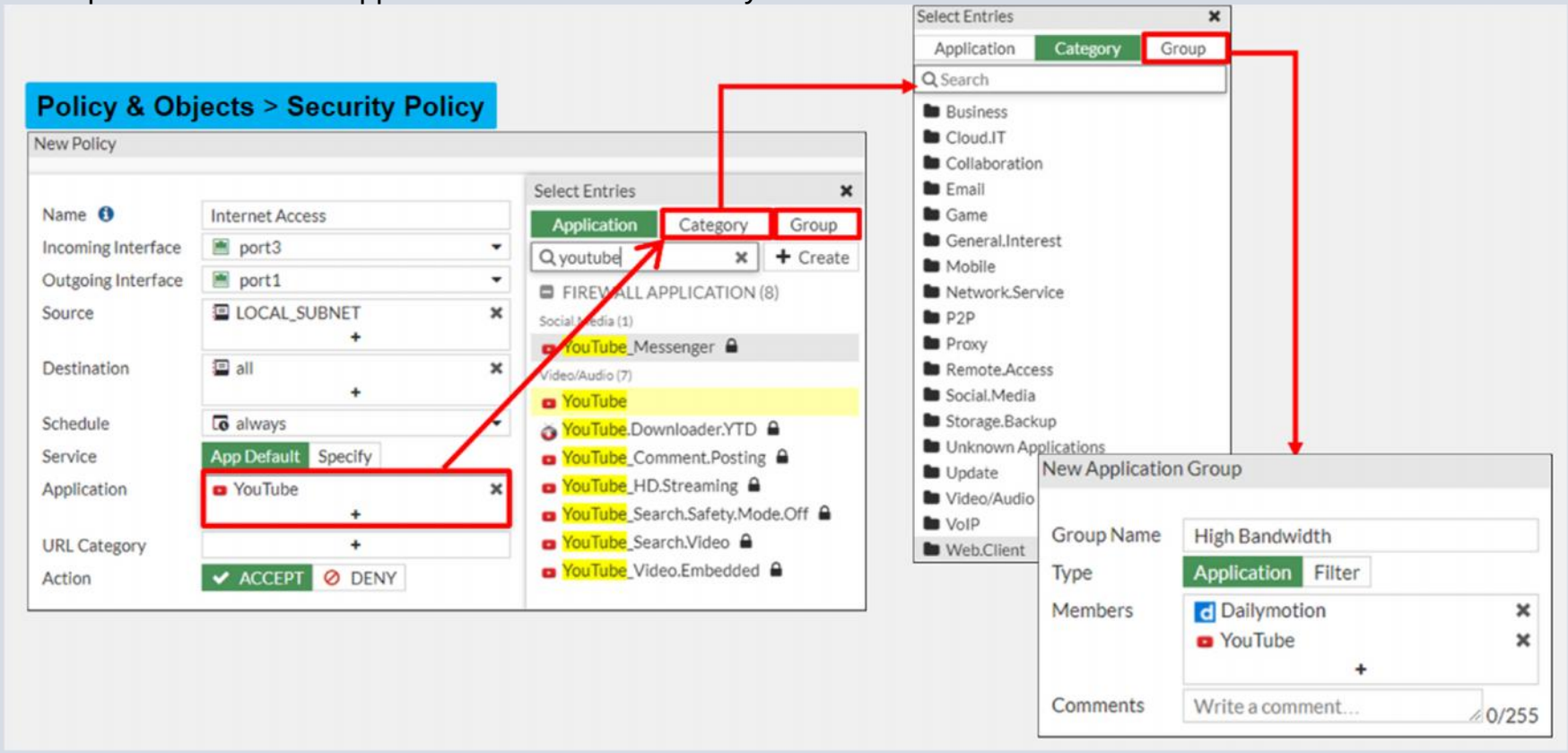
Contrôle d’application

Application d’un profil de contrôle d’application:



Contrôle d’application

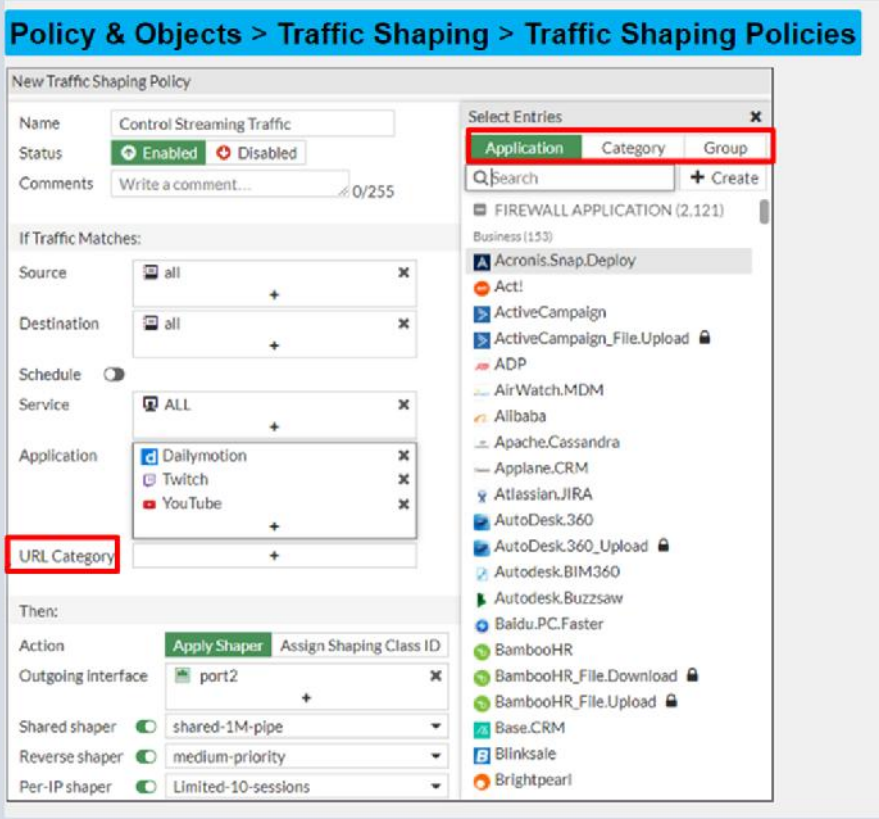
Application d’un profil de contrôle d’application: Mode NGFW-Policy Based



Contrôle d’application

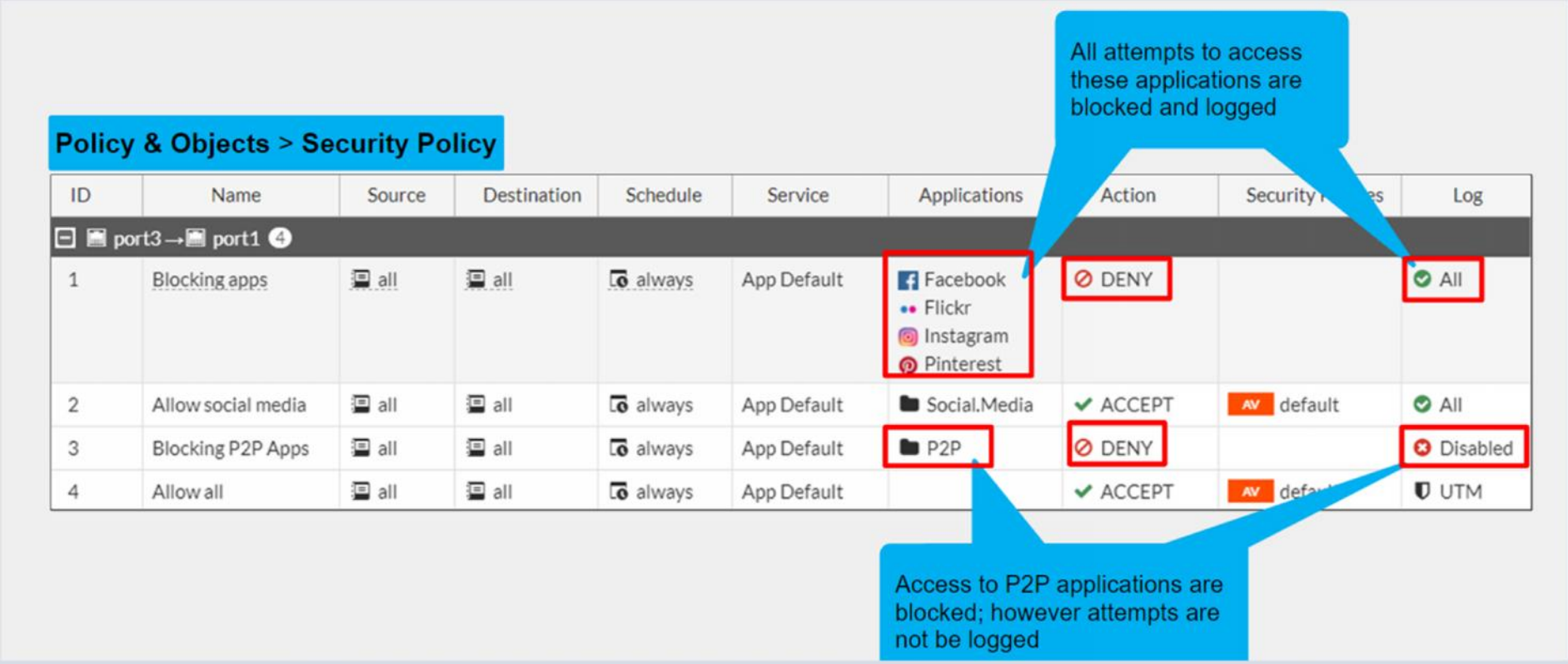
Allocation de bande passante

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



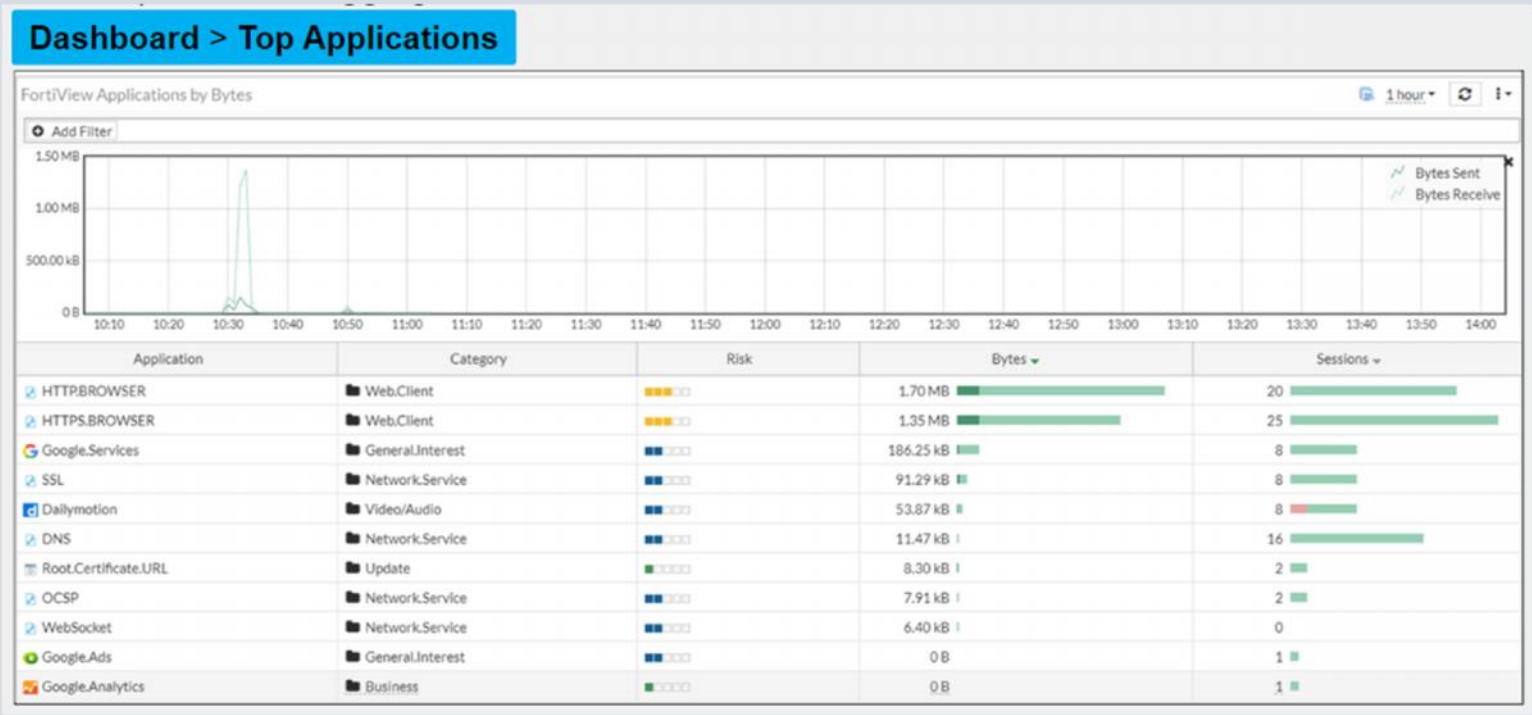
Contrôle d’application

Journalisation



Contrôle d’application

Journalisation



Contrôle d’application

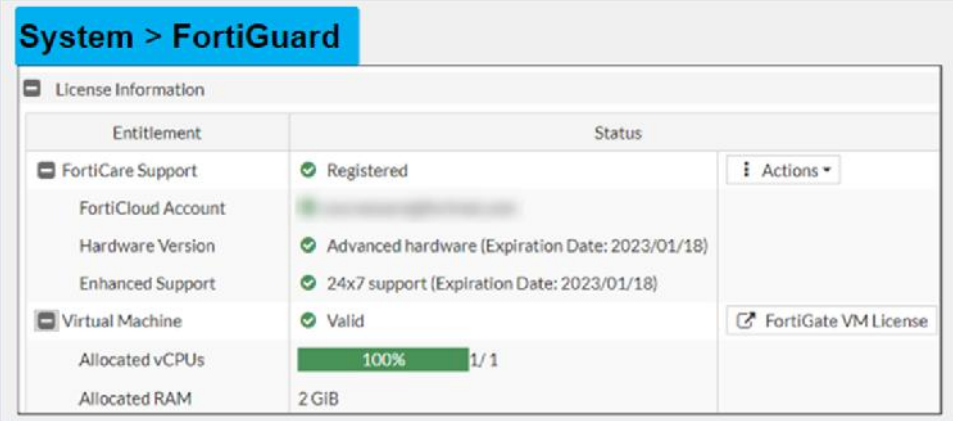
Quelques bonnes pratiques

- 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

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.



Antivirus

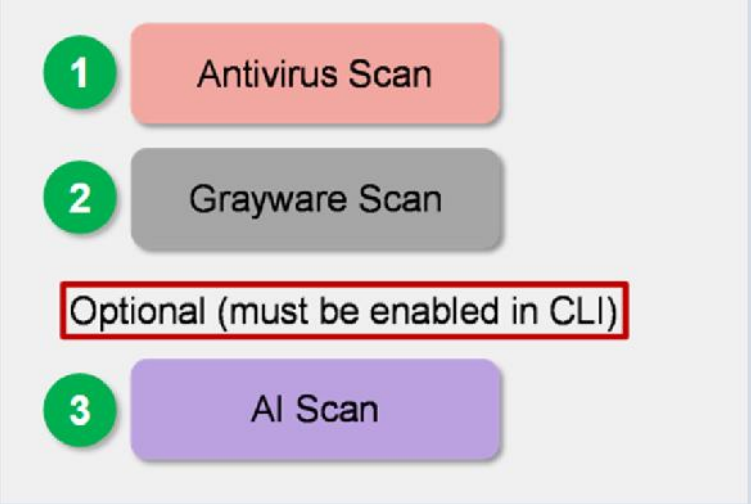
Objectifs

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

ANTIVIRUS

Fonctionnalité Antivirus

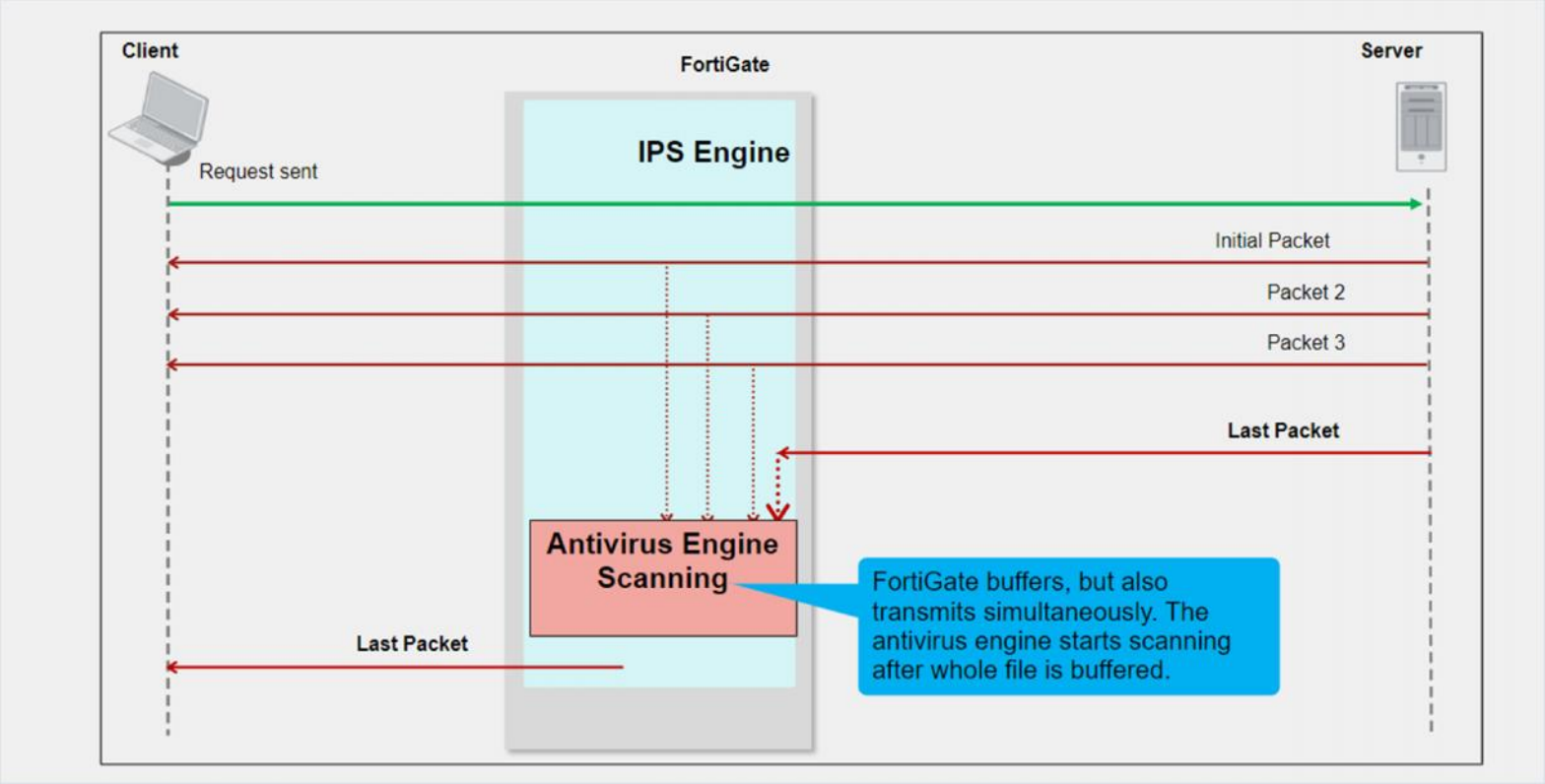
- Nécessite une licence;
- Identification/détection de virus;
- Utilisation la correspondance de modèle appelé signature;
- Signature et moteur de détection varient en fonction des fournisseurs:
  - MD5;
  - CRC;
  - Clé de chiffrements;
  - Code;
  - Etc.
- Technique de Scan:
  - Antivirus;
  - Grayware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



ANTIVIRUS

Antivirus | Modes de Scan | Configurations | Bonnes pratiques

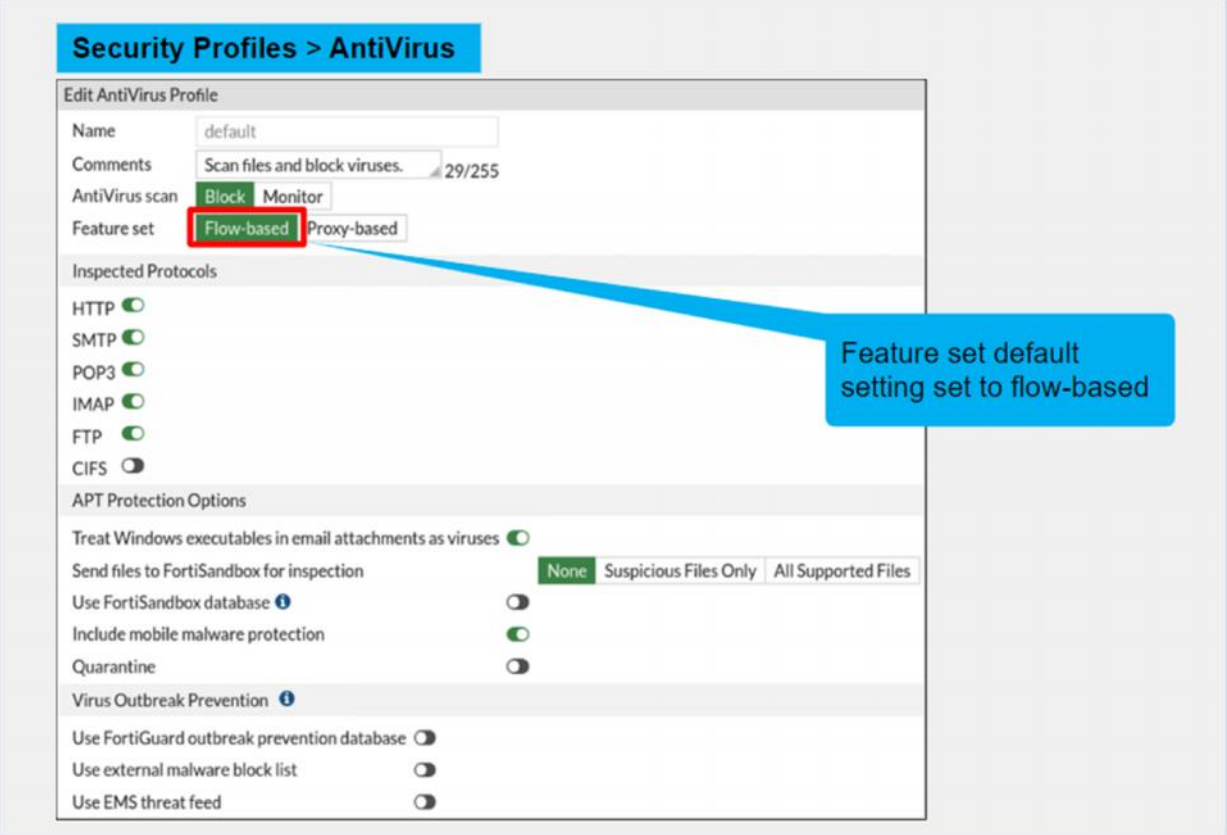
Flow-based



ANTIVIRUS

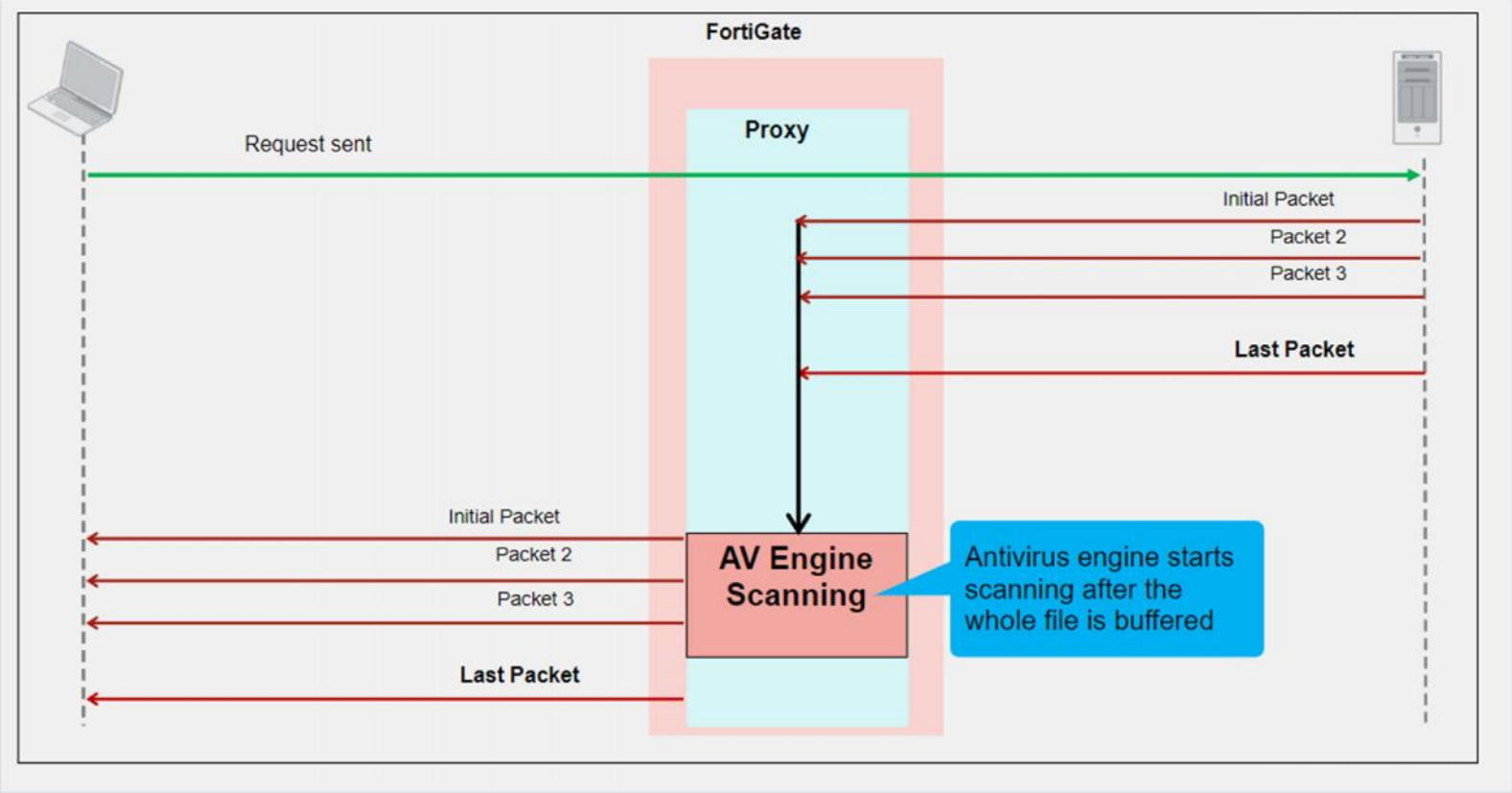
Antivirus | Modes de Scan (suite) | Configurations | Bonnes pratiques

Flow-based



ANTIVIRUS

Proxy-based



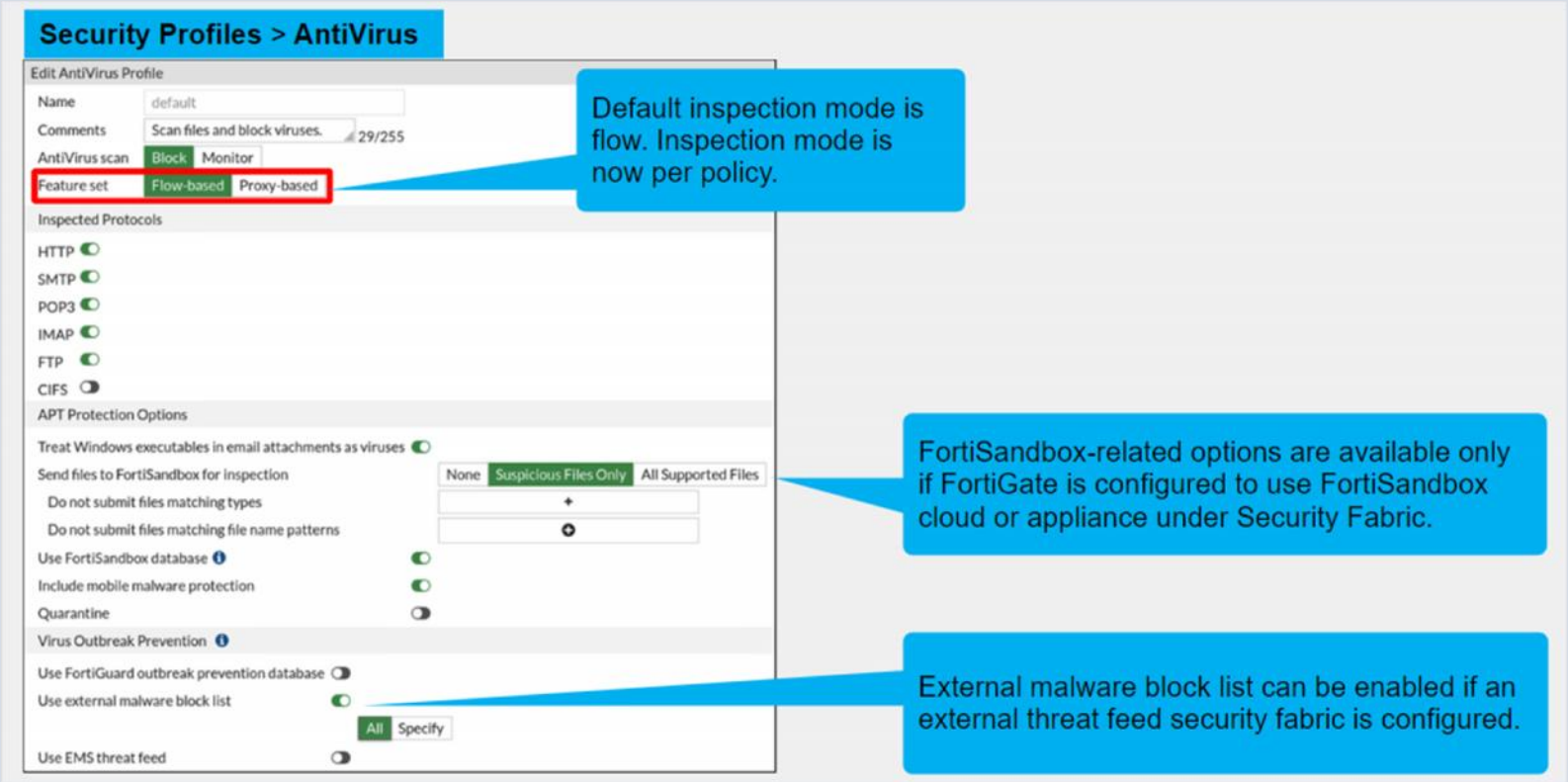
ANTIVIRUS

Proxy-based

ANTIVIRUS

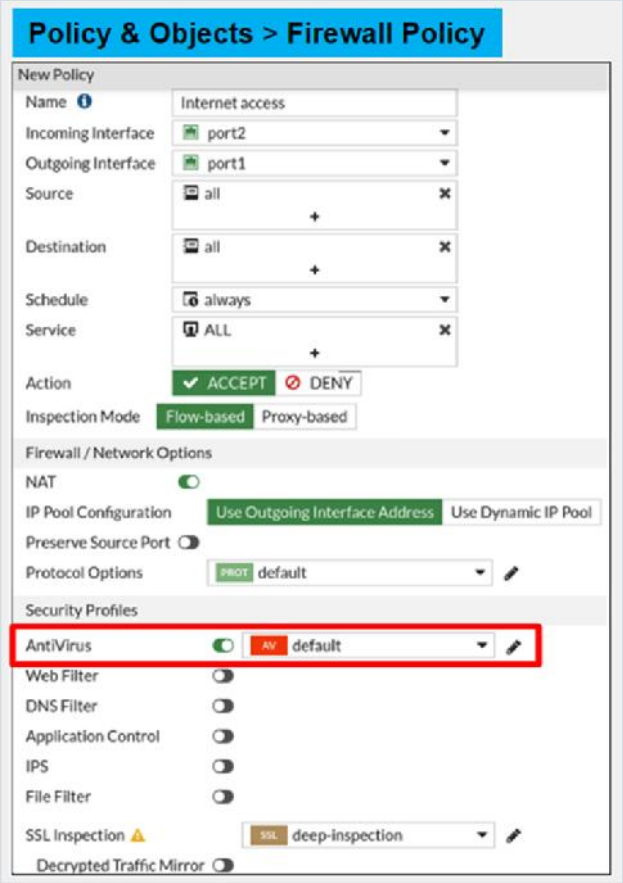
Antivirus | Modes de Scan | Configurations | Bonnes pratiques

Profils



ANTIVIRUS

Profils: Application du profil



ANTIVIRUS

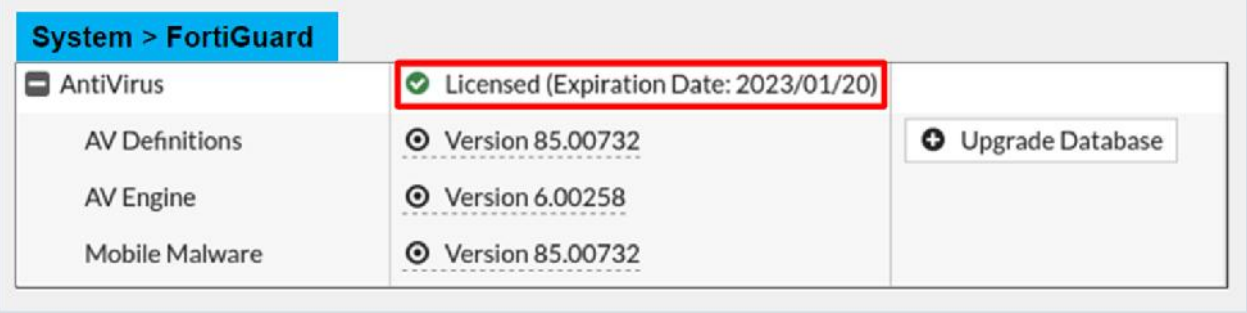
Quelques pratiques de configuration recommandées

- 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

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



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

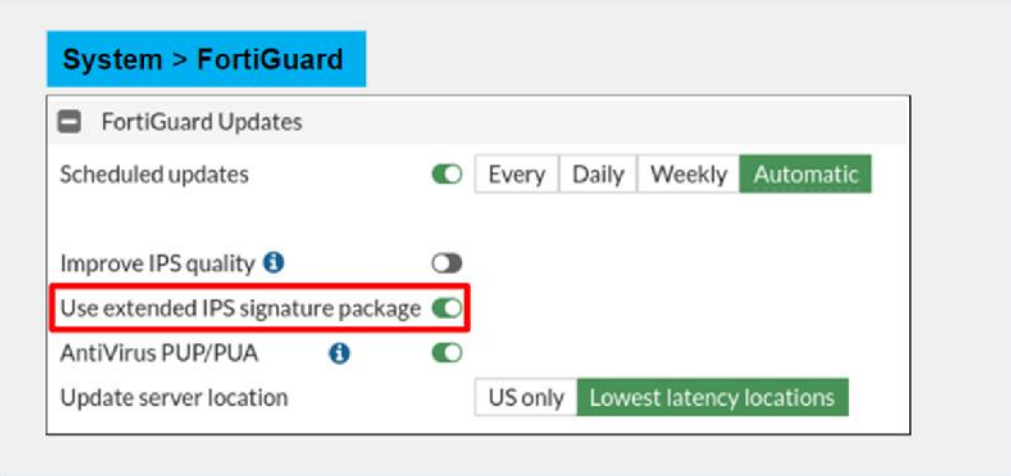
- Mode de détection et de blocage des anomalies ou des exploits;
- Composants principaux;
  - DB de signature;
  - Décodeurs de protocole;
  - Moteur IPS:;
    - Control d'application;
    - Antivirus;
    - Filtre web
    - Etc.

IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

IPS: BD de signatures

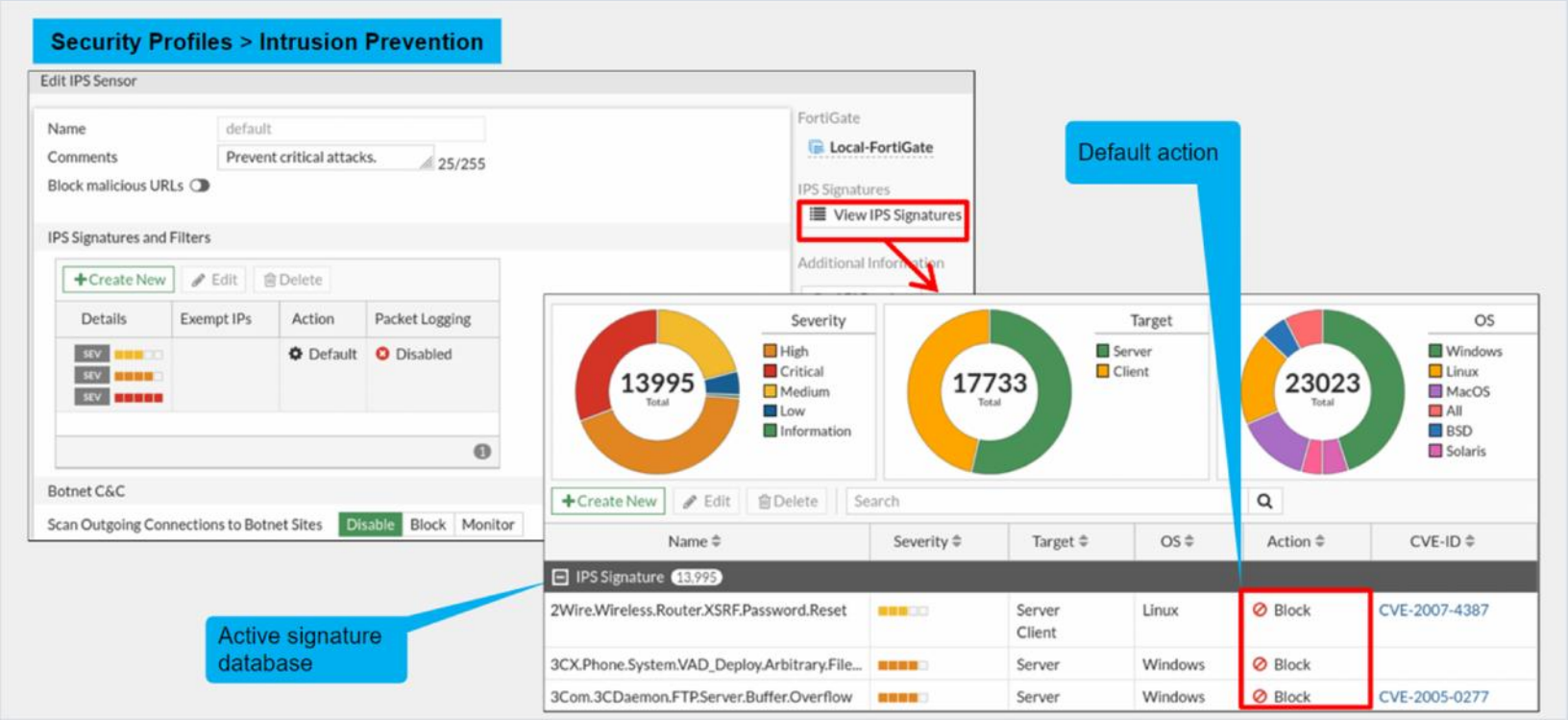
- Régulière: contient les signatures des attaques communes ;
- Etendu: contient des signatures additionnelles.



IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

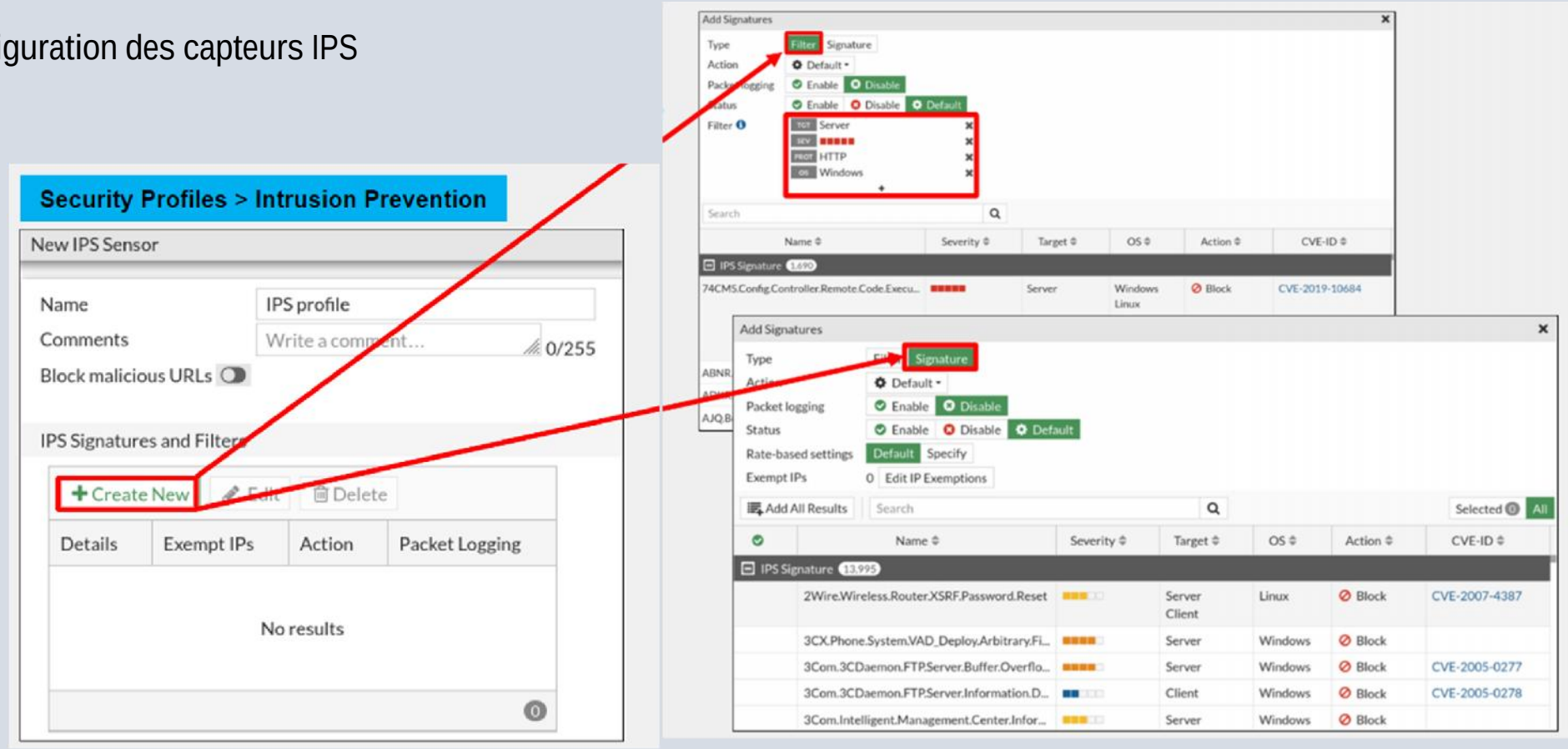
IPS: Liste de signatures



IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

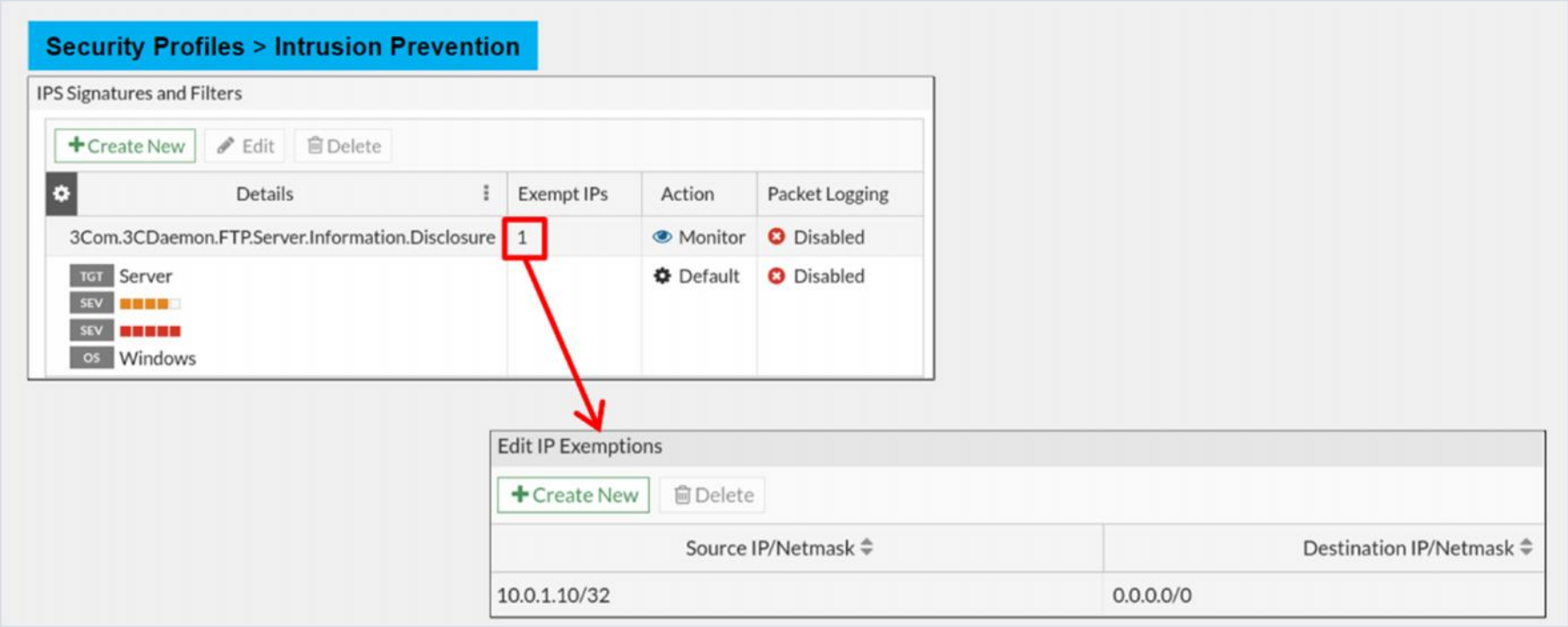
IPS: Configuration des capteurs IPS



IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

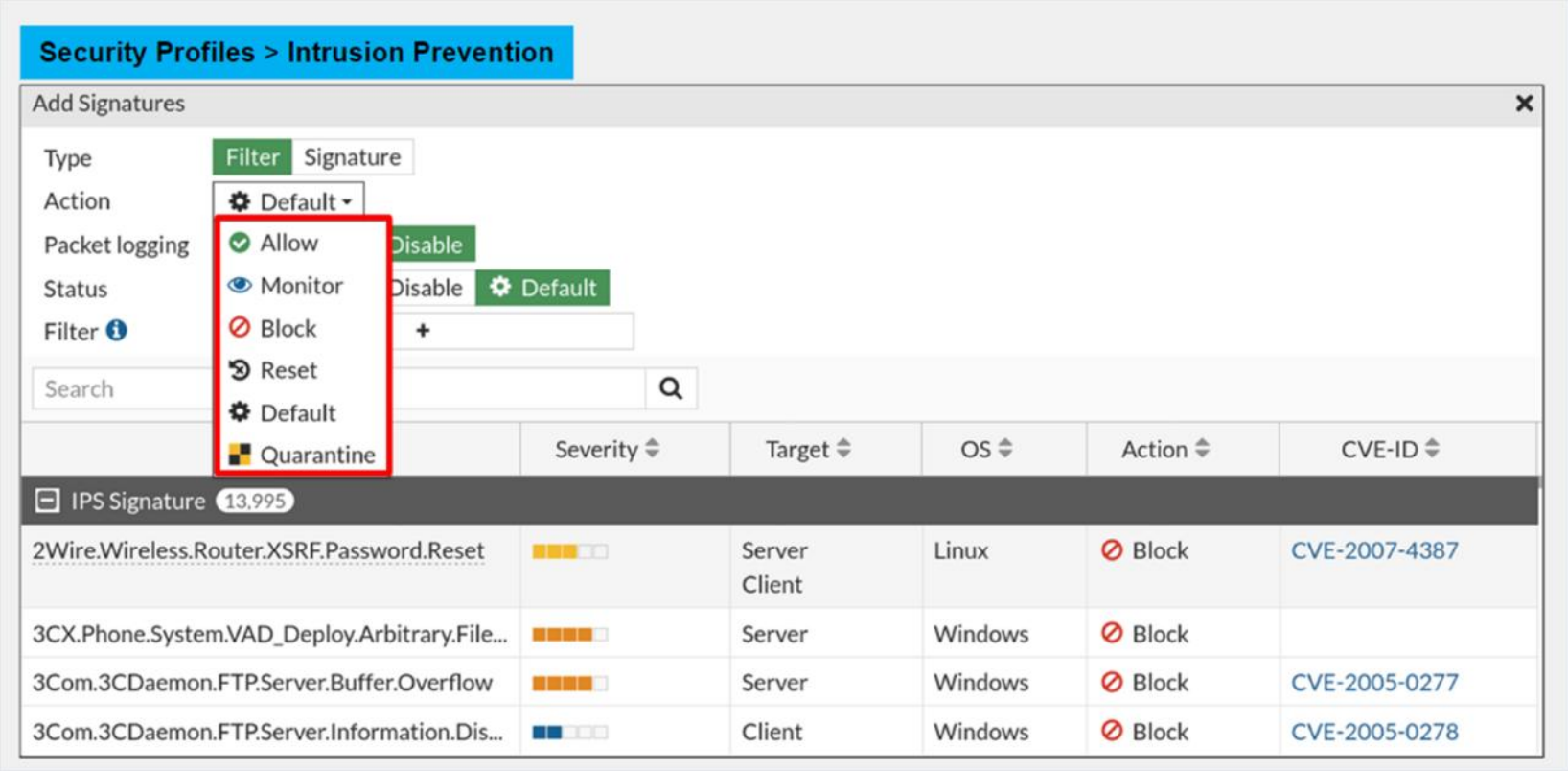
IPS: Exclusion des adresses



IPS&DOS

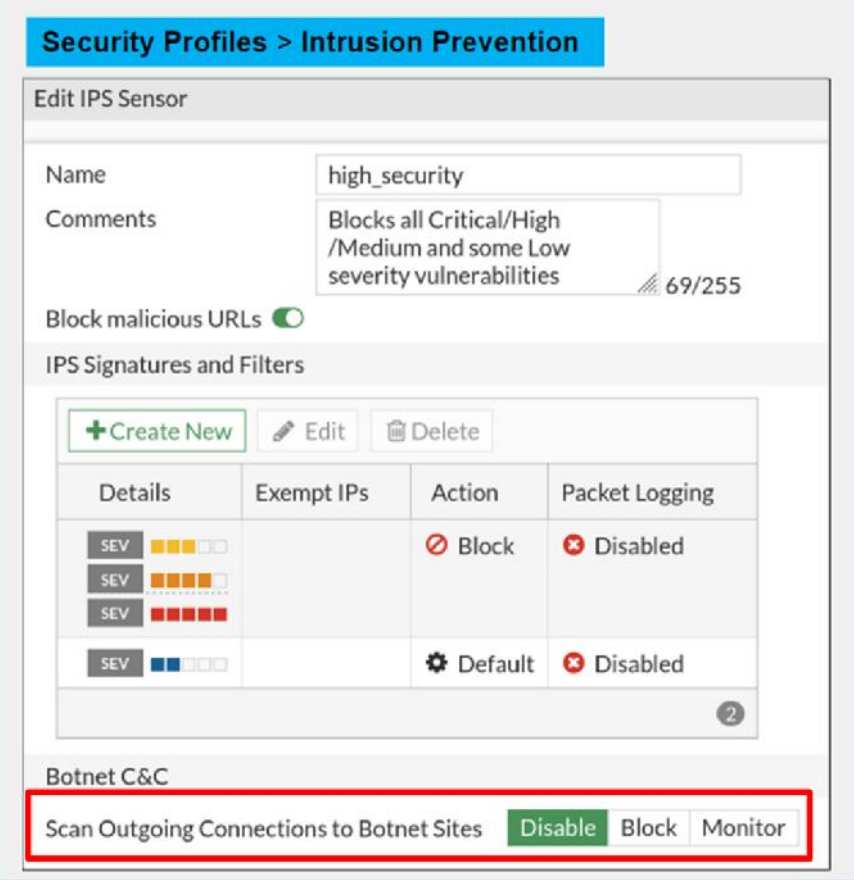
IPS (suite) DOS WAF Bonnes pratiques

IPS: Actions



IPS&DOS

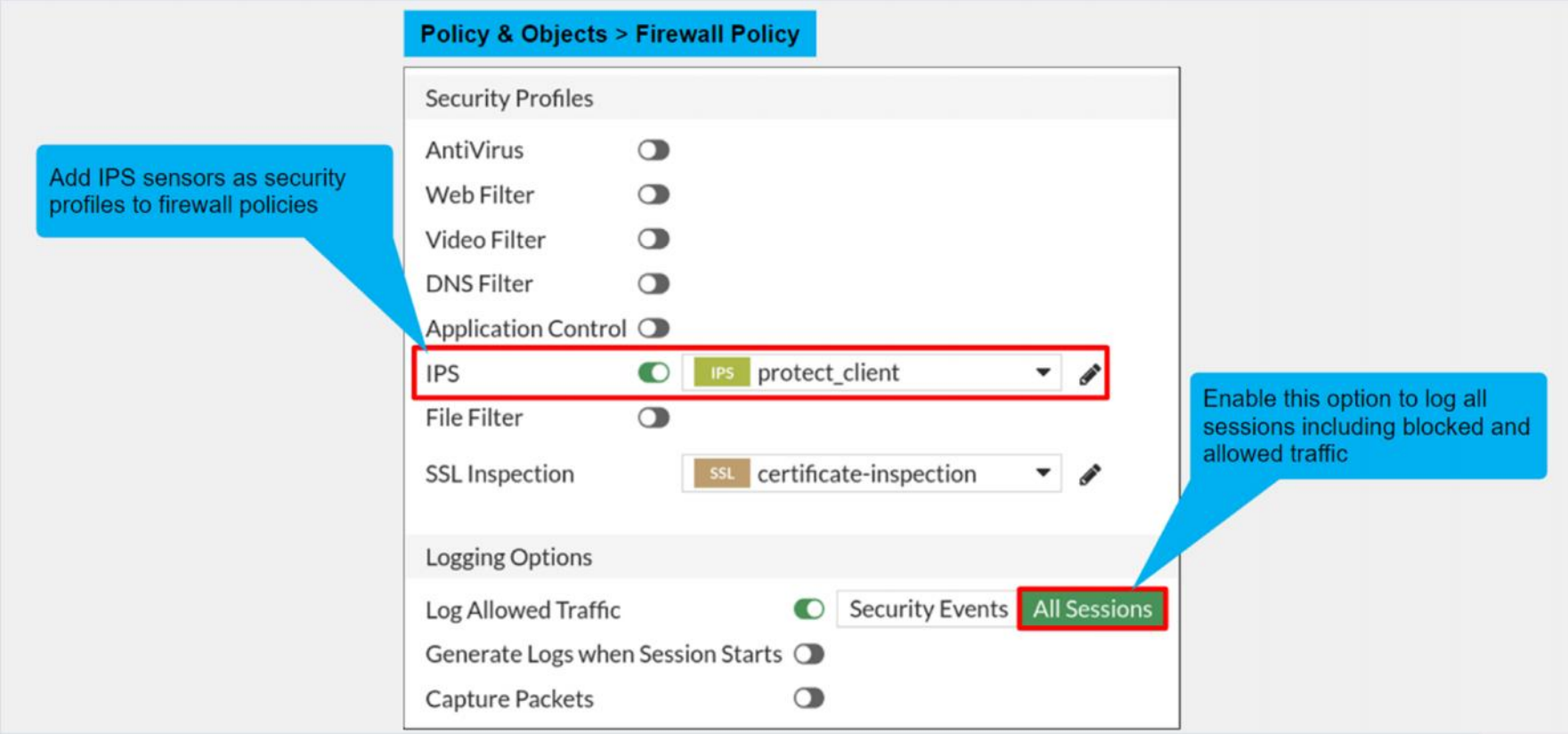
IPS: Botnet



IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

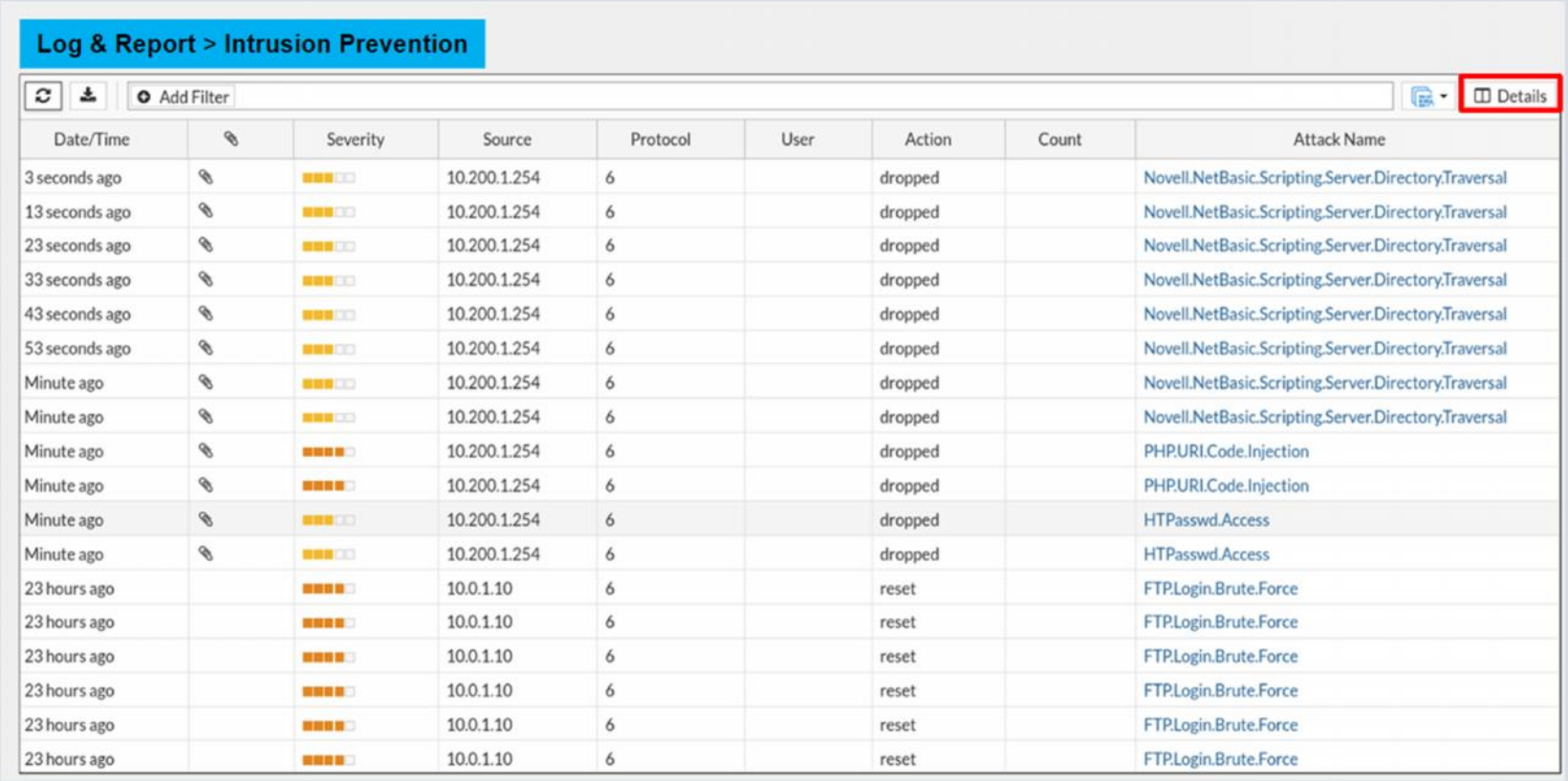
IPS: Application du profil



IPS&DOS

IPS (suite) DOS WAF Bonnes pratiques

IPS: Journaux



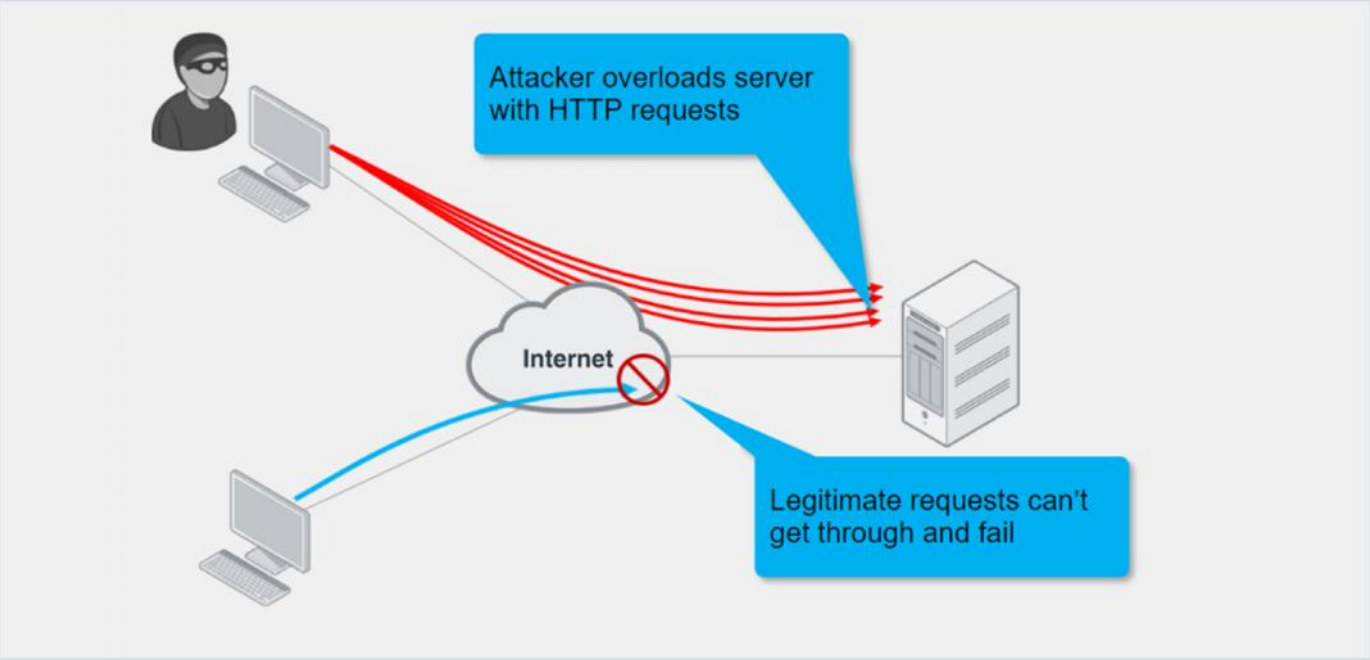
Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
3 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
13 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
23 seconds ago			10.200.1.254	6		dropped		Novell.NetBasic.Scripting.Server.Directory.Traversal
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

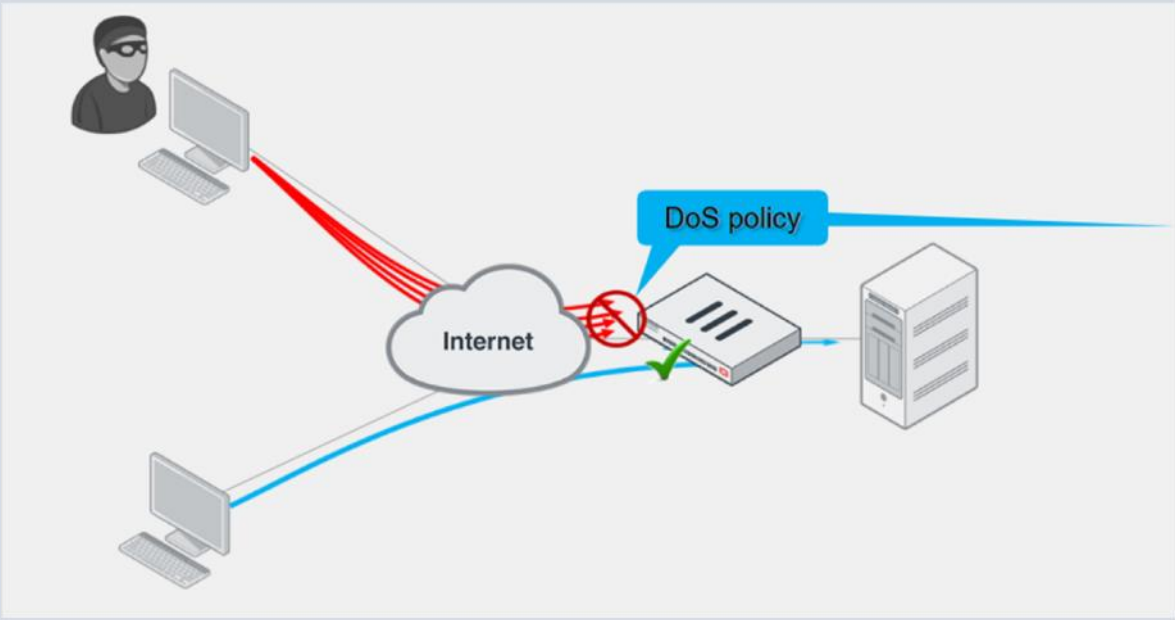
- Ralentir ou mettre hors service un système en consommant toute ses ressources dispo
- Types:
  - TCP SYN flood;
  - ICMP sweep;
  - TCP port scan;
  - DoS Distribués;
  - Etc.

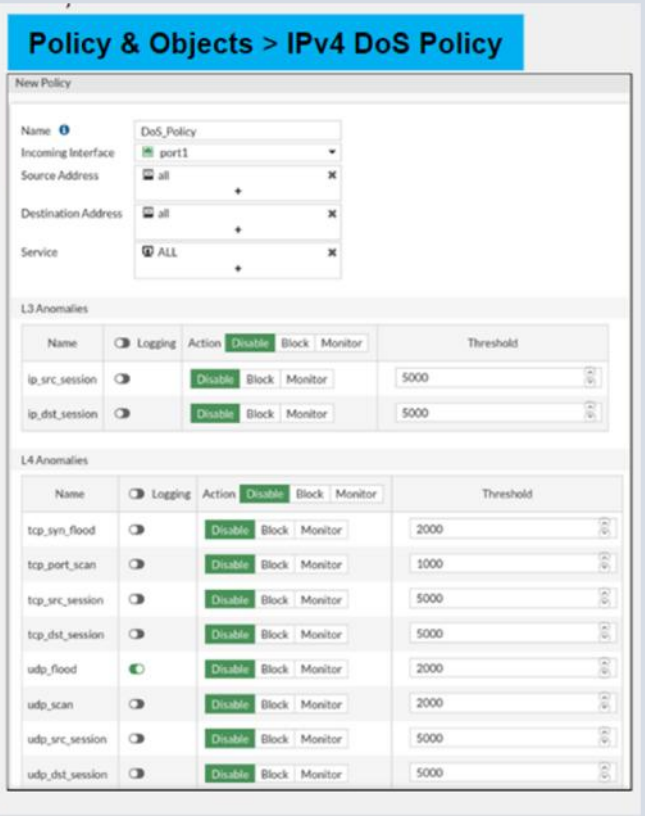


IPS&DOS

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



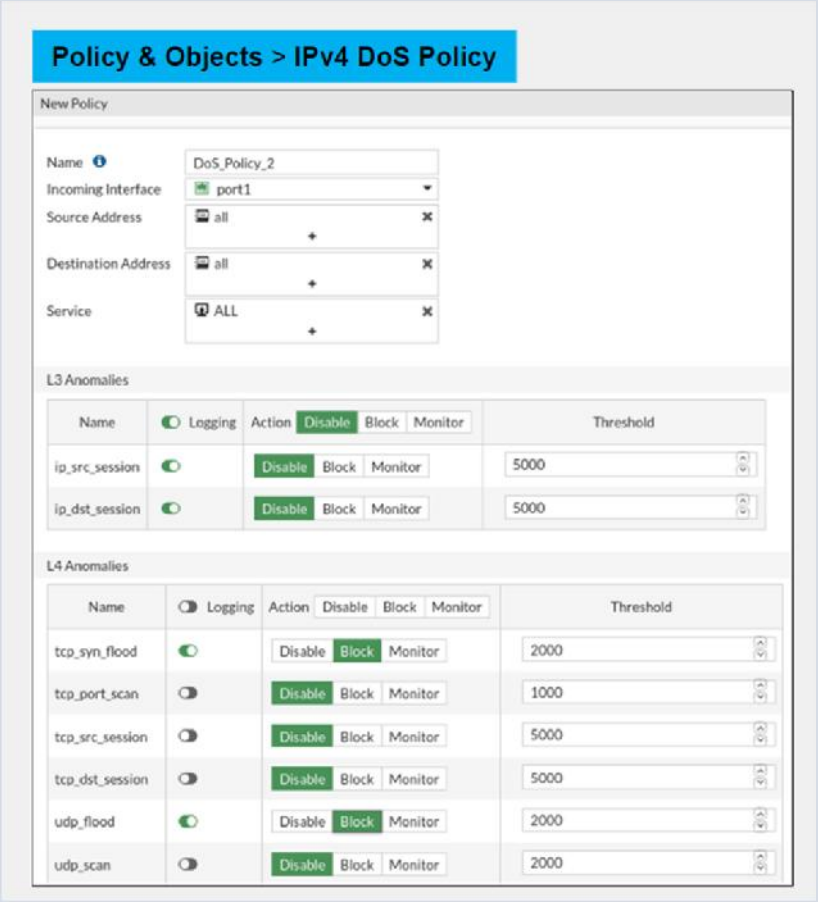


IPS&DOS

IPS DOS (suite) WAF Bonnes pratiques

DoS: Configuration des Politiques

- Flood: détection d'un volume important du meme 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.

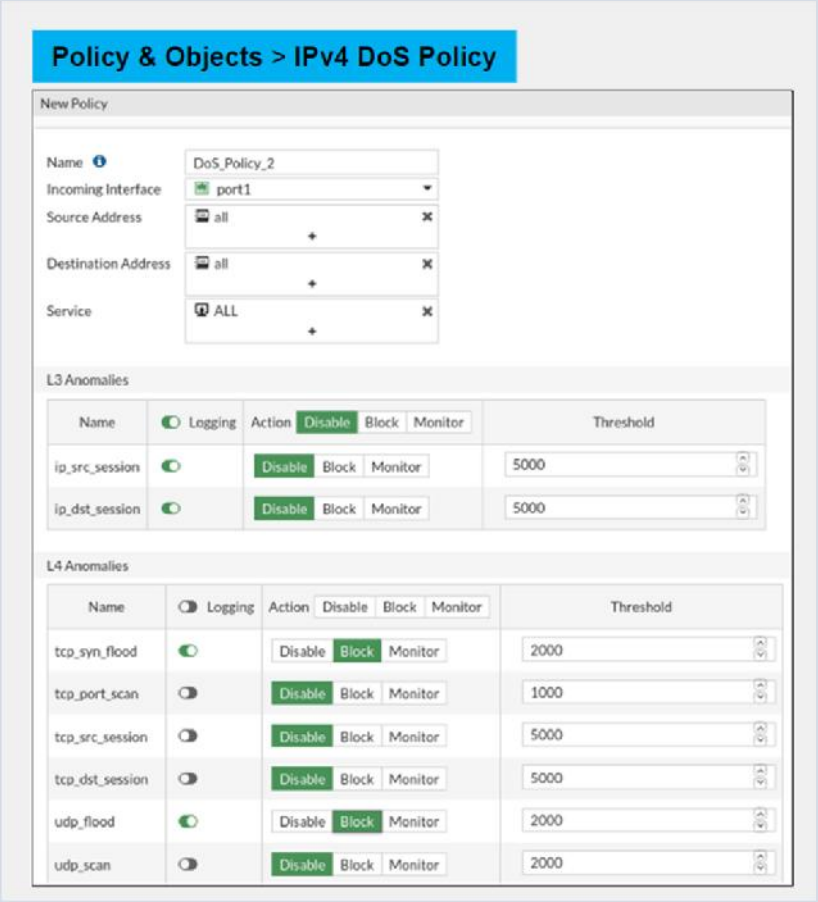


IPS&DOS

IPS DOS (suite) WAF Bonnes pratiques

DoS: Configuration des Politiques

- Flood: détection d'un volume important du meme 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.

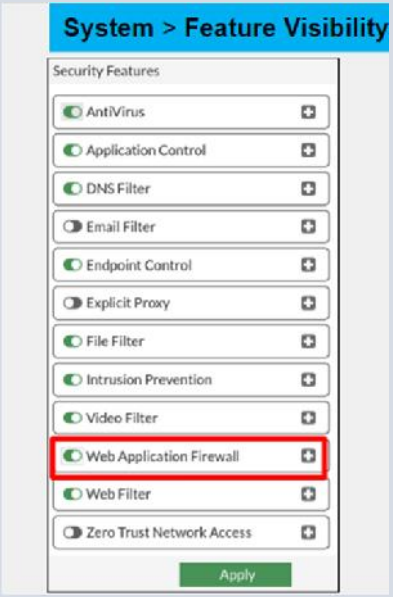


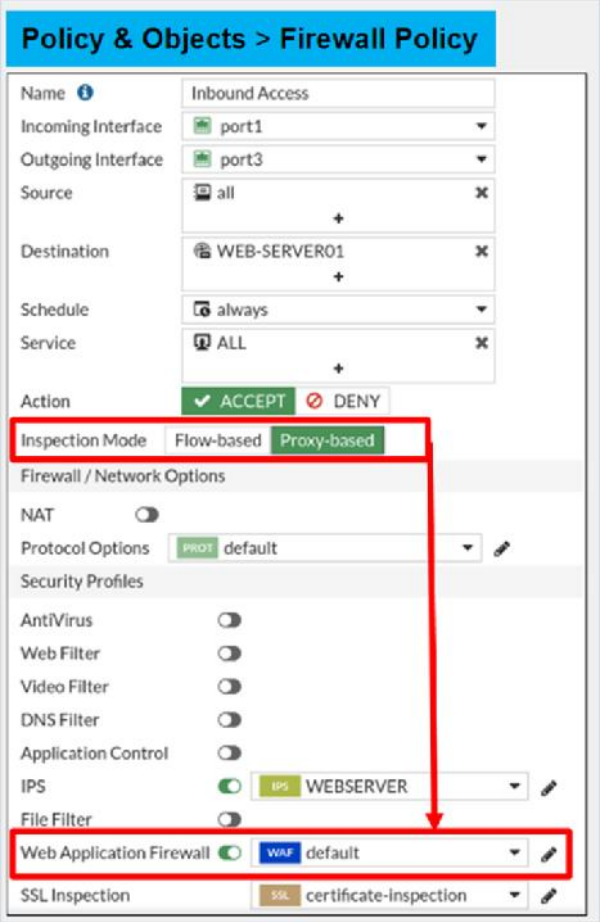
IPS&DOS

IPS DOS WAF Bonnes pratiques

Web Application Firewall (WAF)

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

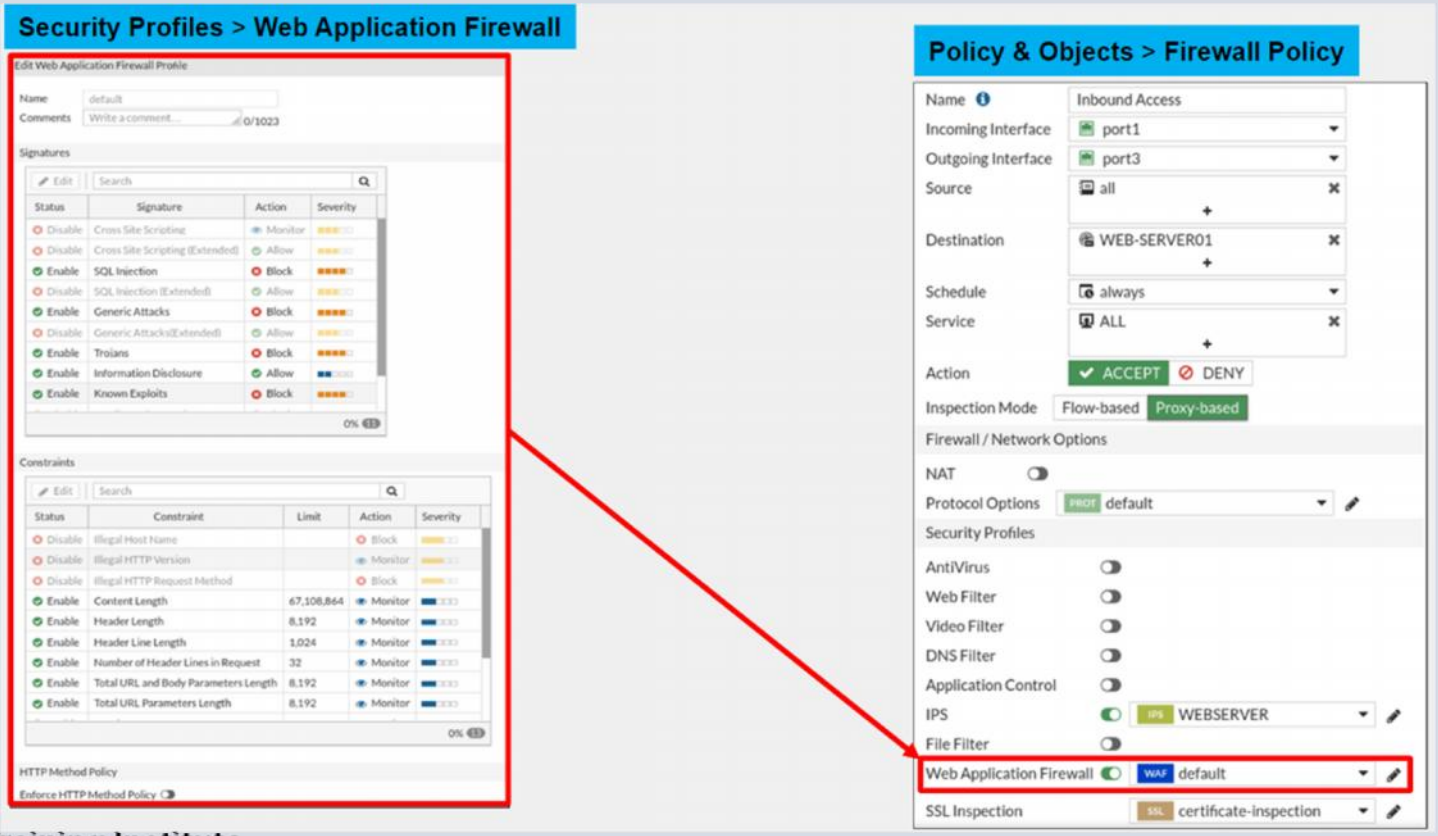




IPS&DOS

IPS DOS WAF (suite) Bonnes pratiques

WAF: Configuration



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 continuel 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 DOS WAF Bonnes pratiques (suite)

Diagnostic: FortiGuard IPS

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


```
# 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®

FORTINET
NSE Training Institute

FortiGate Security

VIRTUAL PRIVATE NETWORK (VPN)

Plan du module

- Vue d’ensemble
- Mode de déploiement
- Configuration
- Bonne pratiques

Vue d’ensemble

Objectifs

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

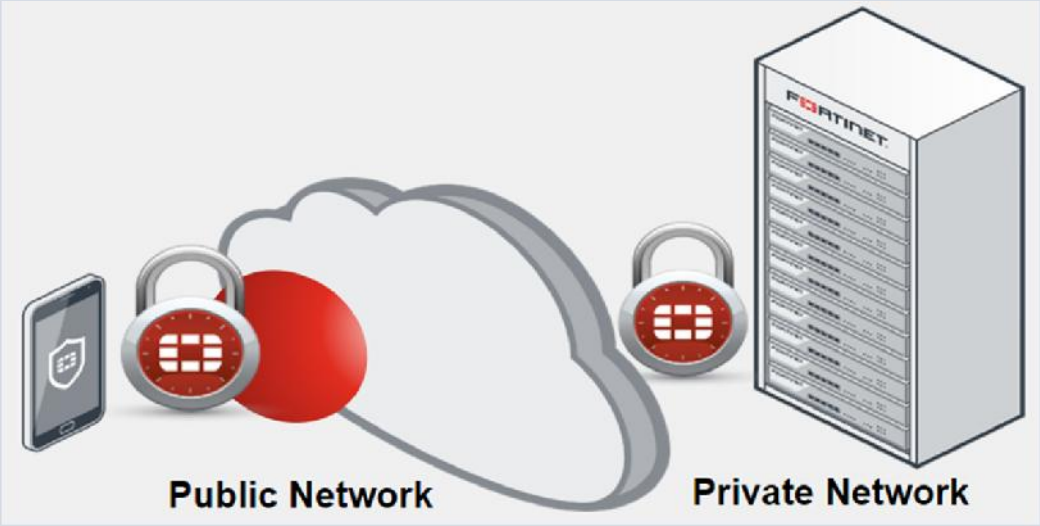
Vue d’ensemble

VPN

TYPES DE VPN

Généralités

- Extension du réseau privé à travers un réseau public (Internet);
- Sécurisation des connexion distantes au LAN ou au équipements:
  - Employés;
  - Surccursal.
- Transmission sécurisées 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:	• Requires installation
	• Flexible setup
	  • Mesh and star topologies
	  • For clients or peer gateways
	  • Performance based: IPsec encryptography is faster in FortiOS
		• Does not require installation
		• Simpler setup
		  • Only client-to-FortiGate
		  • No user-configured settings
		  • Technical support less requested
			• Does not require installation
			• Simpler setup
			  • Only client-to-FortiGate
			  • No user-configured settings
			  • Technical 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

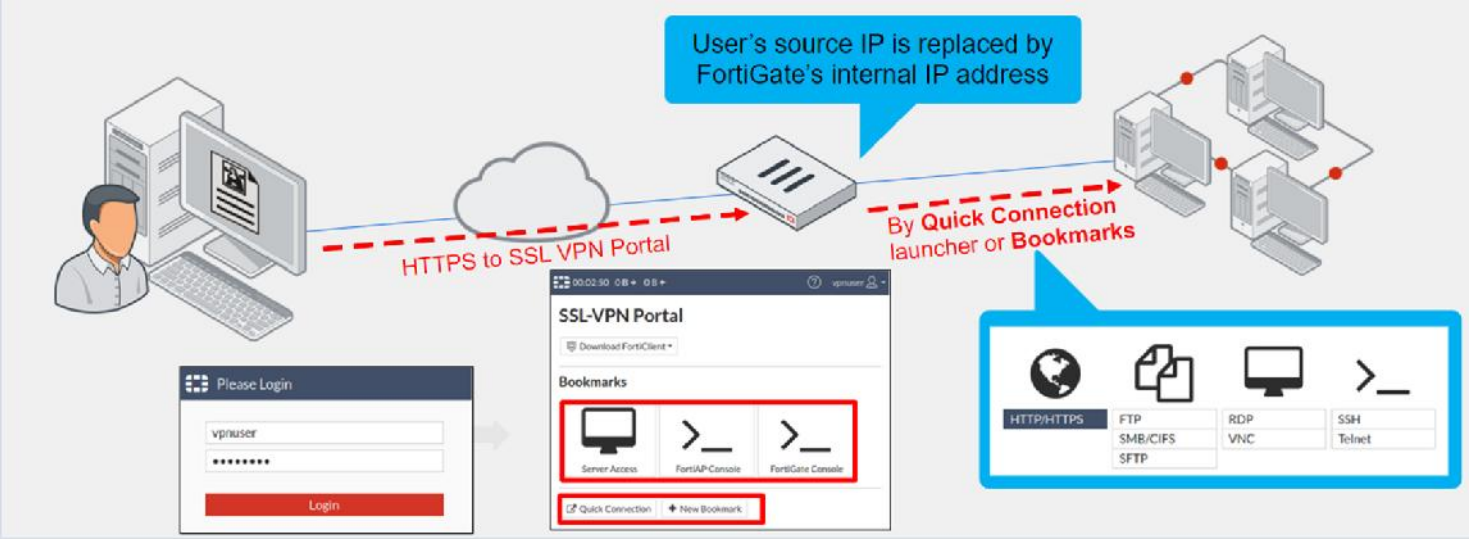
- Décrire les modes de déploiement.

Mode de déploiement

Mode

Mode: Web

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

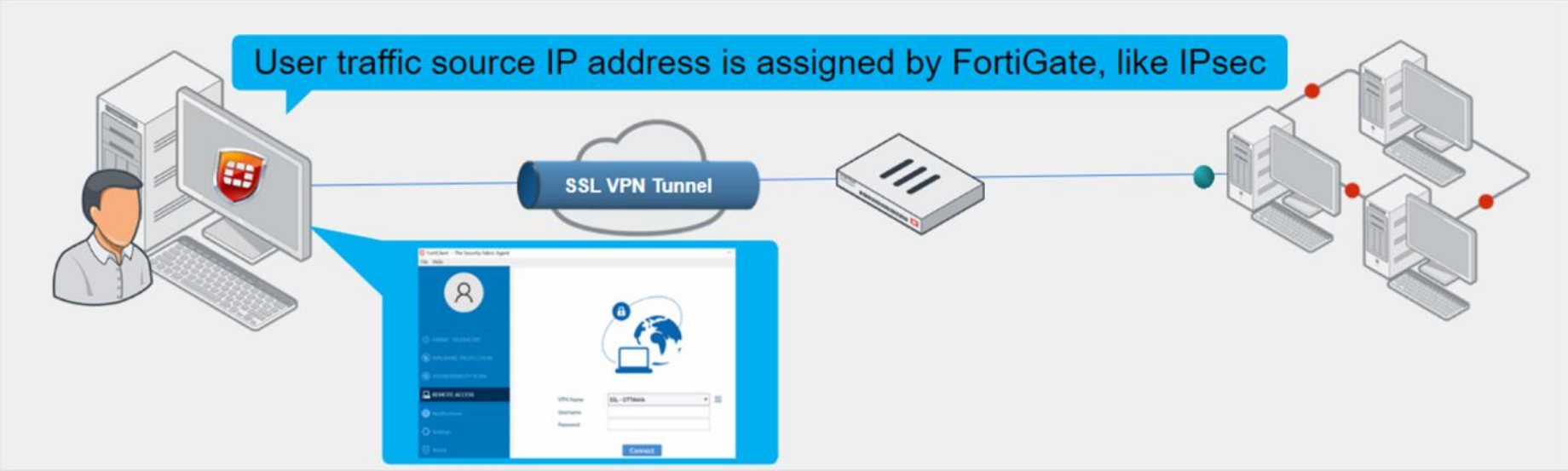


Mode de déploiement

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.

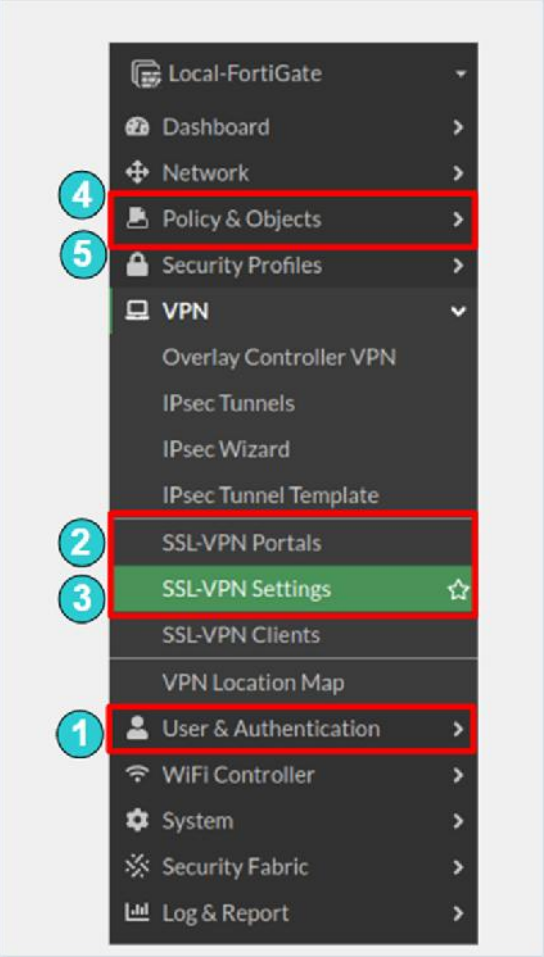
Configuration

SSL

IPSec

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.

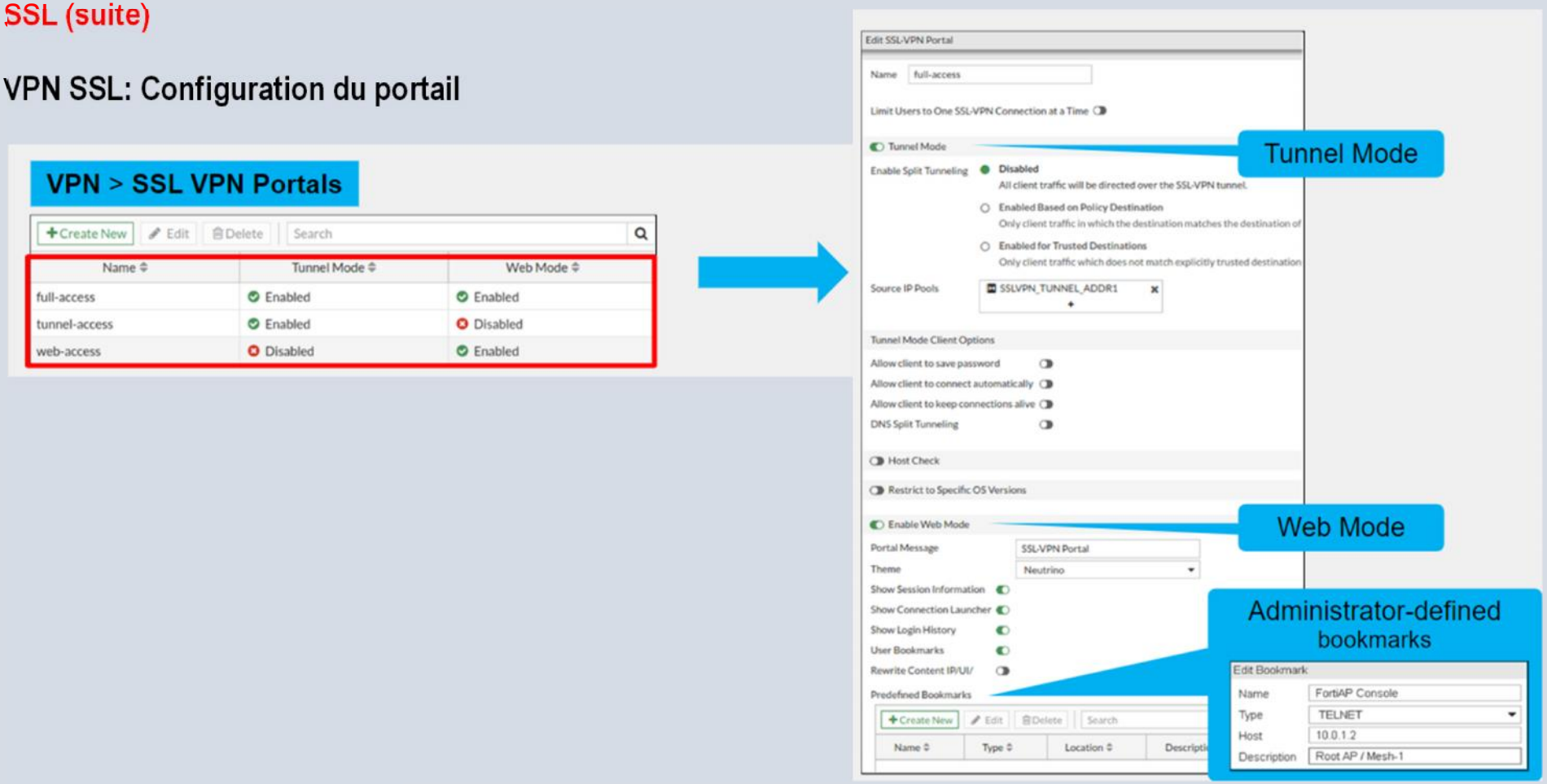


Configuration

SSL (suite)

IPSec

VPN SSL: Configuration du portail



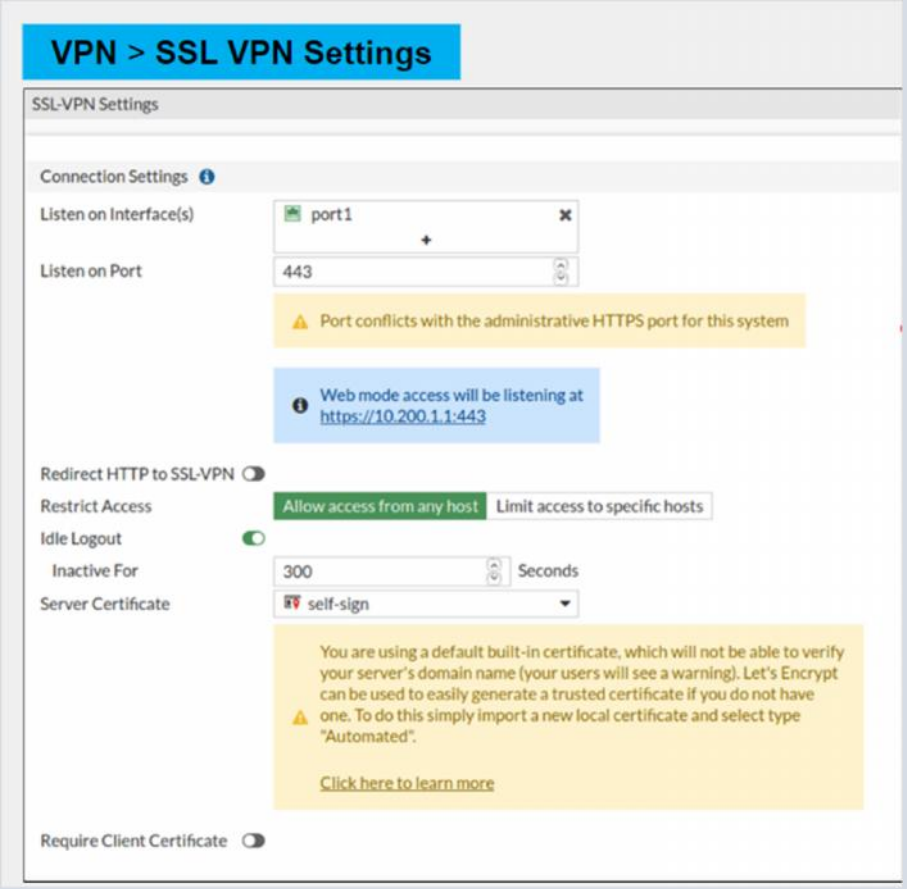
Configuration

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.

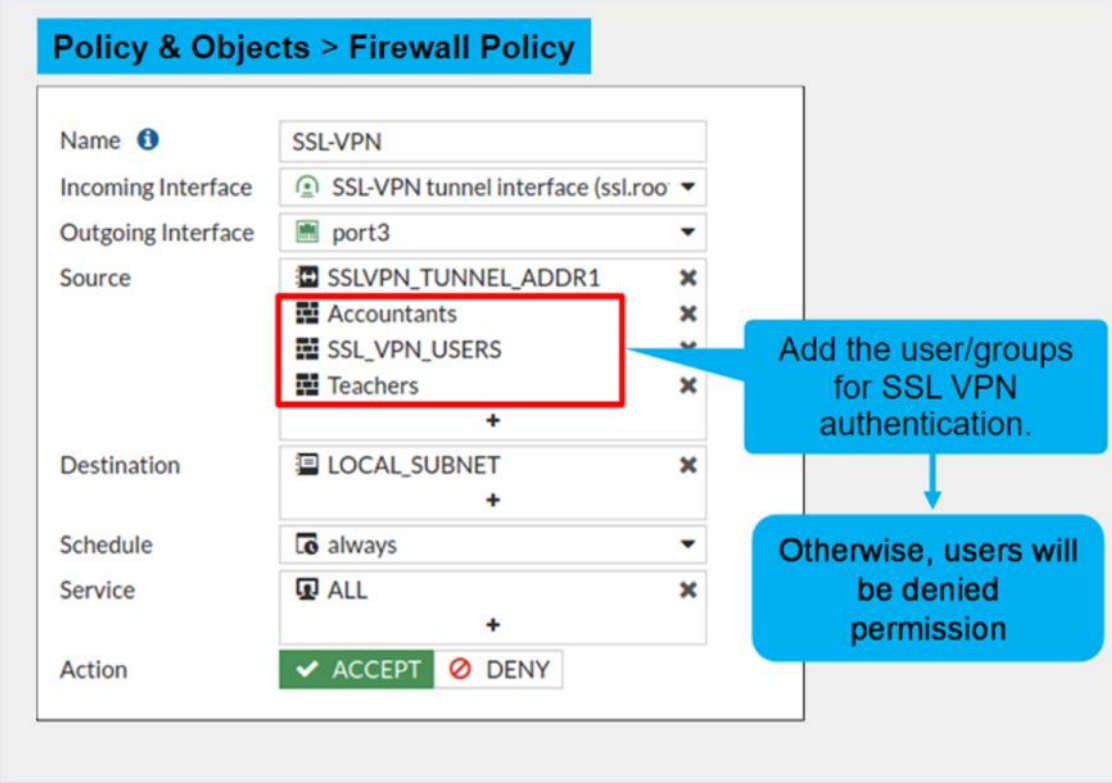


Configuration

SSL (suite)

IPSec

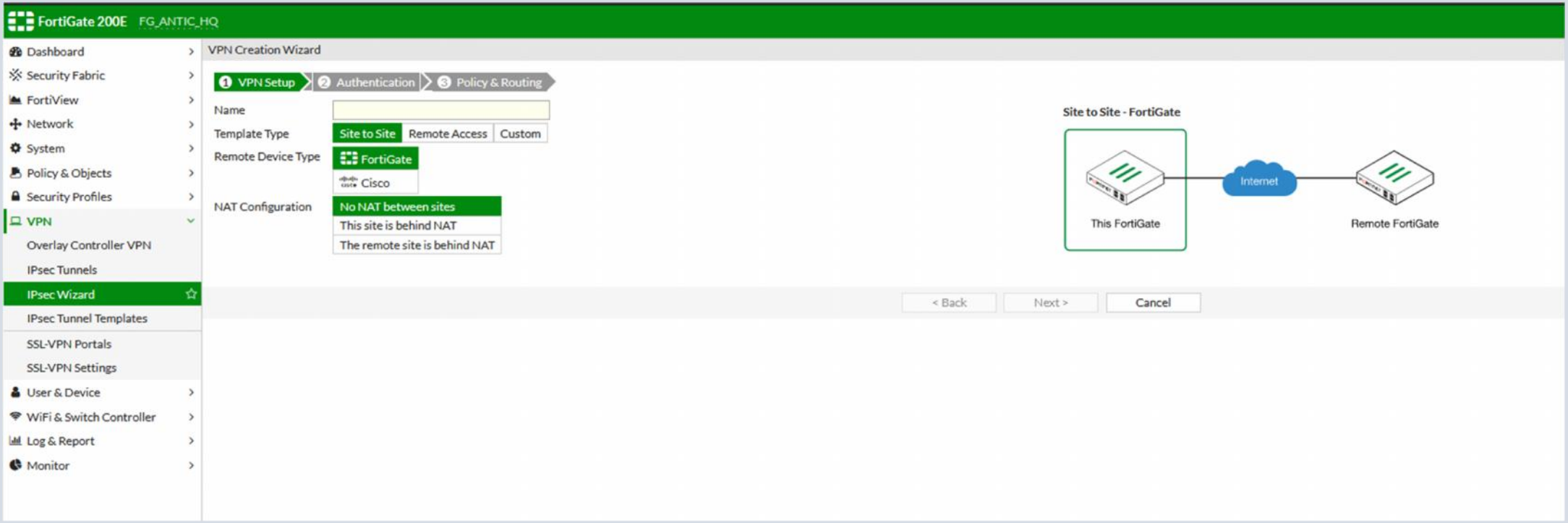
VPN SSL: Configuration des règles de trafic



Configuration

SSL IPSec

VPN IPSEC

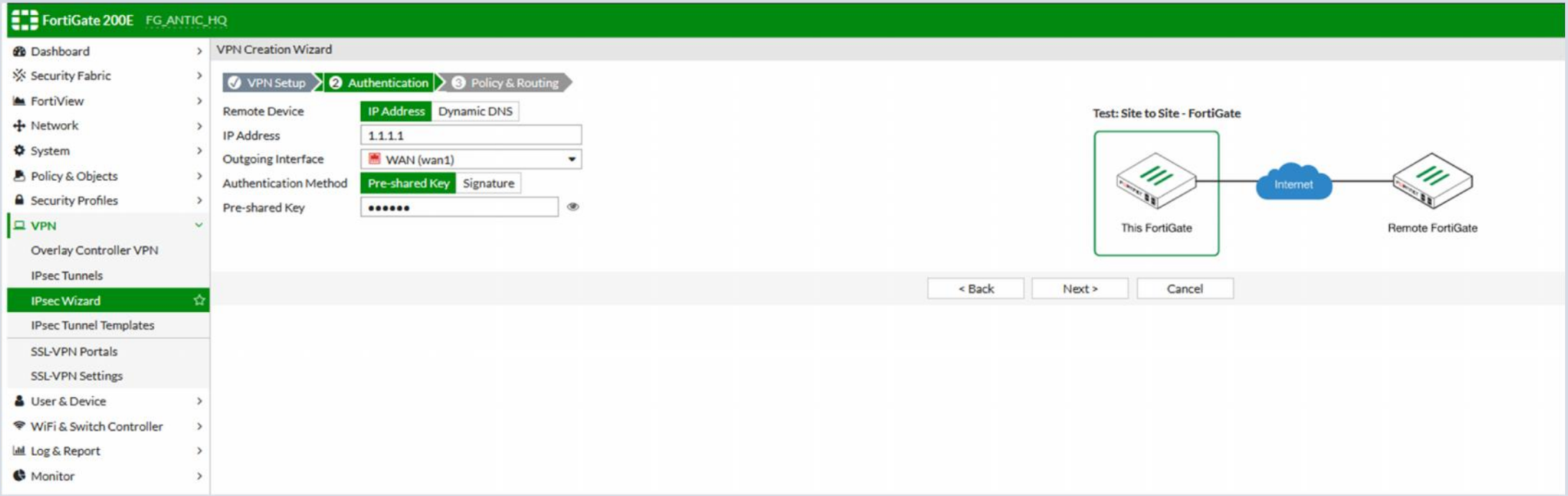


Configuration

SSL

IPSec (suite)

VPN IPSEC

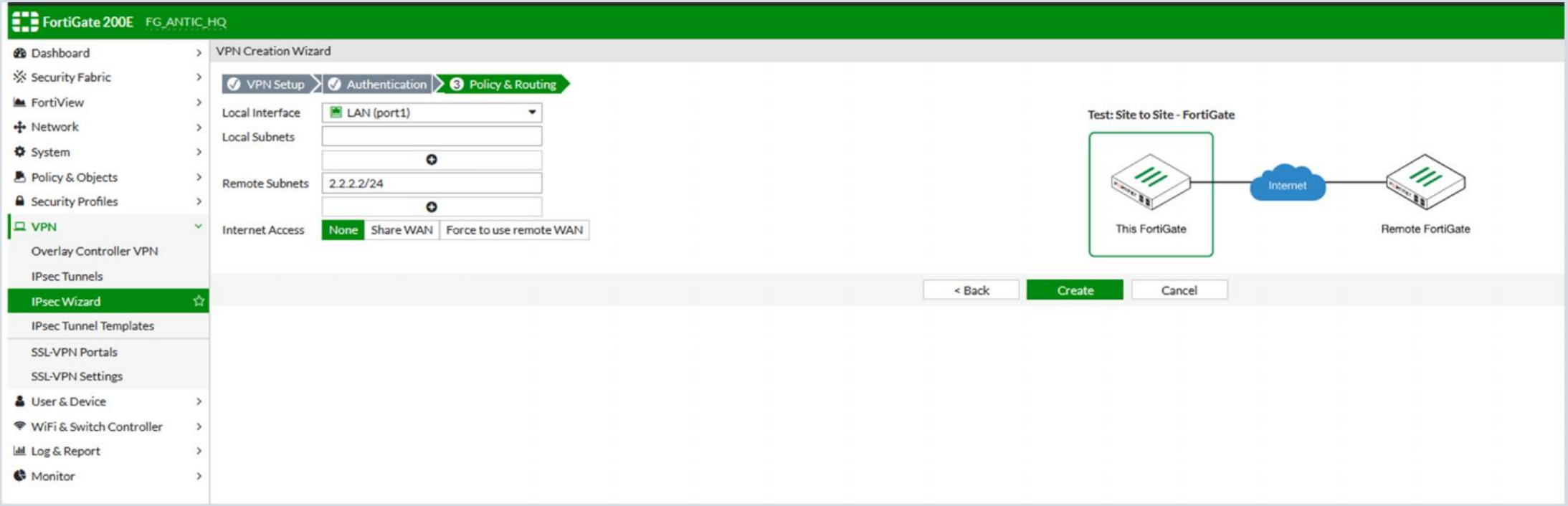


Configuration

SSL

IPSec (suite)

VPN IPSEC



Bonnes pratiques

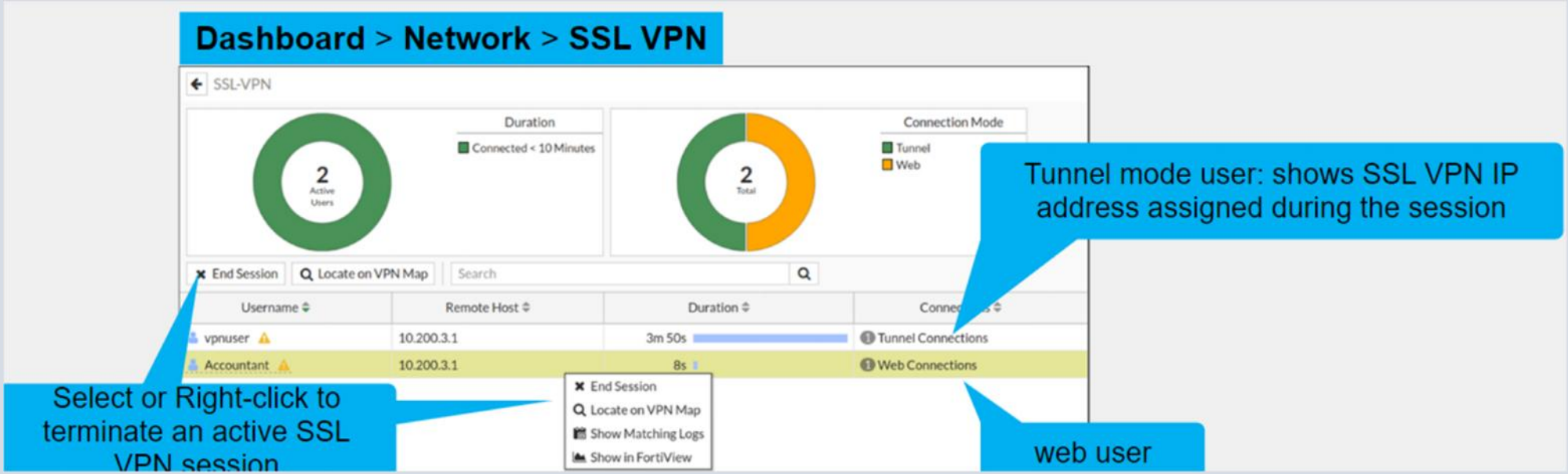
Objectifs

- Connaitre quelques bonnes pratiques.

Bonnes pratiques

Diagnostic

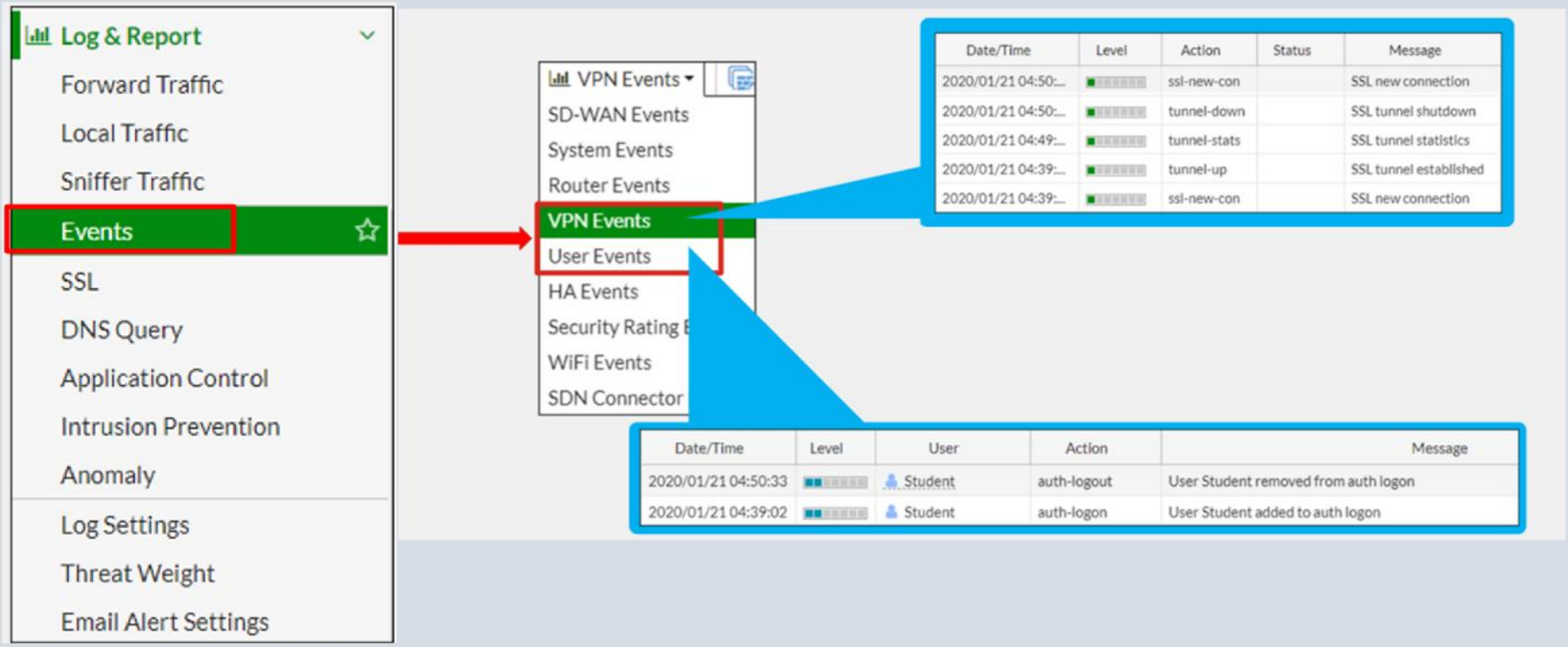
Session VPN



Bonnes pratiques

Diagnostic (suite)

Journalisation



Bonnes pratiques

Diagnostic

- 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.