PROMEO FORMATION – BTS SIO SISR

Projet Personnel Encadré 2 - Netelia

Sécurisation d'une architecture réseau multisite grâce à des Firewalls Stormshield.

Brice GAZEAUX
2024-2026

Sommaire

⚠ Ce document est à but d'information et de démonstration, les configurations présentées ne suivent pas les recommandations de sécurité, et ne représentent pas l'intégralité des configurations réelles pour éviter les dupliquas d'informations. ⚠

1) Présentation du Projet

a) Généralités et Objectif

Dans le cadre du PPE-2 du BTS SIO SISR, ce projet vise à réaliser la simulation d'une architecture réseau multisite à l'aide de firewall Stormshield. L'objectif est de concevoir la structure des différents sites, et de configurer les firewalls pour répondre aux besoins de communication et de sécurité inter-sites d'une entreprise.

Ce PPE vise à mettre en pratique des compétences acquises au cours du BTS, développer une autonomie de travail et réaliser, par une approche minimaliste, une architecture réseau sécurisée grâce à l'utilisation de firewalls Stormshield.

b) Contextualisation

L'entreprise Netelia souhaite relier trois de ses sites dans les Hauts-de-France, respectivement à Clermont, Beauvais et Amiens. Après avoir missionné plusieurs équipes pour traiter les aspects légaux, financiers et organisationnels, un pôle informatique voit le jour avec pour objectif de relier les différents sites tout en garantissant la sécurité des réseaux internes.

Pour cela une toute première maquette est créée, avec deux firewalls situés aux sites de Beauvais et Amiens.
La zone primaire d'Amiens supportera le LAN local ainsi que les serveurs internes de l'entreprise. De l'autre, le site de Beauvais disposera également de son propre LAN, et accueillera en plus une DMZ, ainsi qu'une liaison secondaire vers Clermont, un site tertiaire nécessitant des accès, mais de manière plus limitée.

c) Contraintes

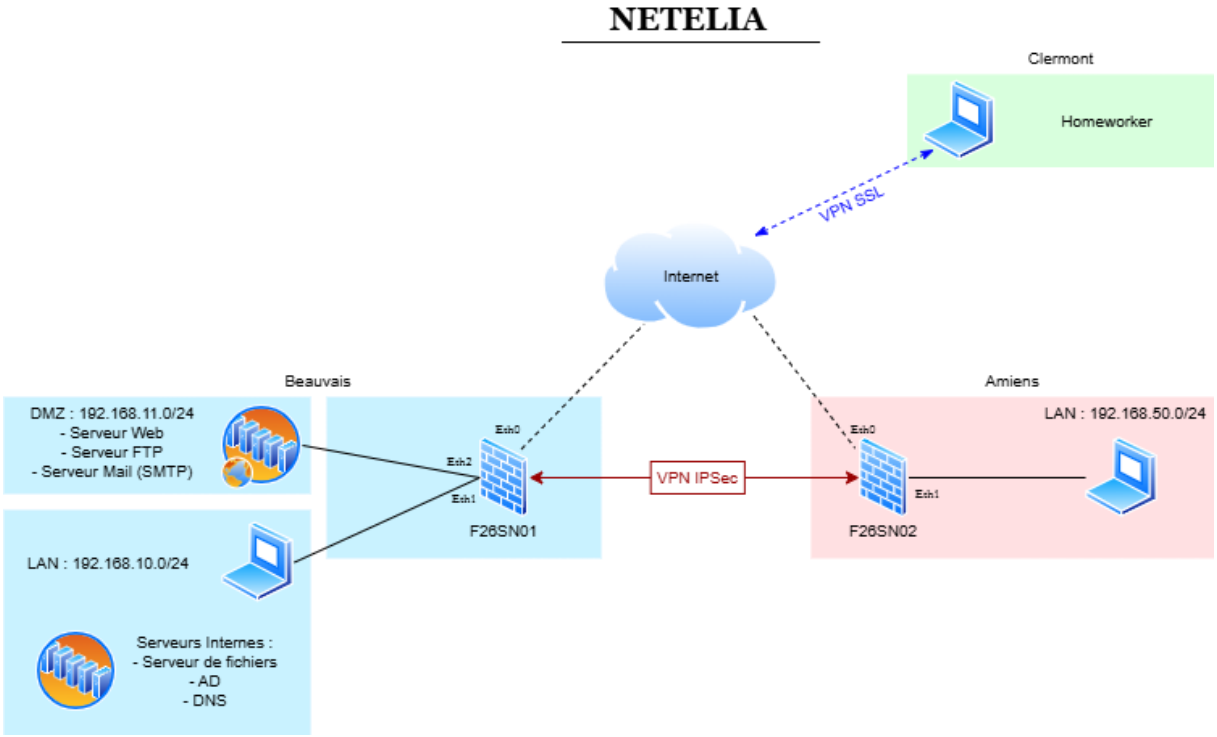
La distance entre les sites très éloignés de Beauvais et Amiens sera supporté par une liaison VPN dédiée. D'autres contraintes de la maquette concernent la mise en place d'une architecture réseau simple comprenant deux firewalls Stormshield, trois réseaux LAN, une DMZ, des serveurs internes isolés, ainsi qu'un tunnel VPN permettant d'assurer une communication sécurisée entre les différents sites.

2) Schématisation de la Situation

a) Besoins

- Plan d'adressage IP
- Deux firewall Stormshield
- Serveurs DMZ : FTP, SMTP / Serveurs Internes : Fichiers, AD, DNS
- Appareils finaux
- NAT, Filtrage, DHCP, VPN

b) Architecture réseau



3) Mise en œuvre de l'infrastructure

a) Informations et organisation générale

Tableau d'adressage :

Équipement	Port	Adresse IP	Masque de Sous Réseau	Description
F26SN01	Eth0	172.18.204.104	/24	Internet
	Eth1	192.168.10.1	/24	LAN Beauvais
	Eth2	192.168.11.1	/24	DMZ
	X	192.168.100.1	/24	VPN SSL TCP
	X	192.168.101.1	/24	VPN SSL UDP
F26SN02	Eth0	172.18.204.204	/24	Internet
	Eth1	192.168.50.1	/24	LAN Amiens
N201P0 ?	Ethernet	192.168.11.10	/24	Hyperviseur
V26DB01	Bridge	192.168.11.11	/24	Web
V26DB02	Bridge	192.168.11.12	/24	FTP
V26DB03	Bridge	192.168.11.13	/24	Mail (SMTP)
N205P04	Ethernet	192.168.10.10	/24	Hyperviseur
V26WN01	Bridge	192.168.10.11	/24	Fichiers
V26WN02	Bridge	192.168.10.12	/24	AD, DNS
N201P0?	Ethernet	DHCP	DHCP	PC
N201P0?	Ethernet	DHCP	DHCP	PC
N201P0?	Ethernet	DHCP	DHCP	PC

b) Mise en place de la DMZ

Hyperviseur : VMWare sur Windows 11 (N201P0?)
VMs - Debian 13 :
- root : P@ssw0rd
- user : P@ssw0rd
- VMnet10 Bridge Intel® Ethernet

VM	Adresse IP	Package Tool	Utilisation
V26DB01	192.168.11.11	Apache2	Serveur Web HTTP / TCP:80
V26DB02	192.168.11.12	vsftpd	Serveur FTP FTP / TCP:21

V26DB03	192.168.11.13	postfix	Serveur Mail SMTP / 25

Vérifications :

- Serveur Web : Moteur de recherche → 192.168.11.11 → Ouverture page web
- Serveur FTP : ftp 192.168.11.12 → Message accès ftp
- Serveur Mail : Activer telnet dans « optionalfeatures » → telnet 192.168.11.13 25 → Message accès postfix

c) Mise en place des serveurs internes

Hyperviseur : VMWare sur Windows 11 (N205P04)

VMs – Windows Serveur 2019 :
- Adminsitrateur : P@ssw0rd ou rien
- AdminPPE : P@ssw0rd
- UserPPE : P@ssw0rd
- VMnet 10 Intel® Ethernet

VM	Adresse IP	Rôles et fonctionnalités	Utilisation
V26WN01	192.168.10.11	Service de fichier > Serveur de fichier	Partage de fichiers
V26WN02	192.168.10.12	AD DS, DNS	Accès Domaine Résolution DNS

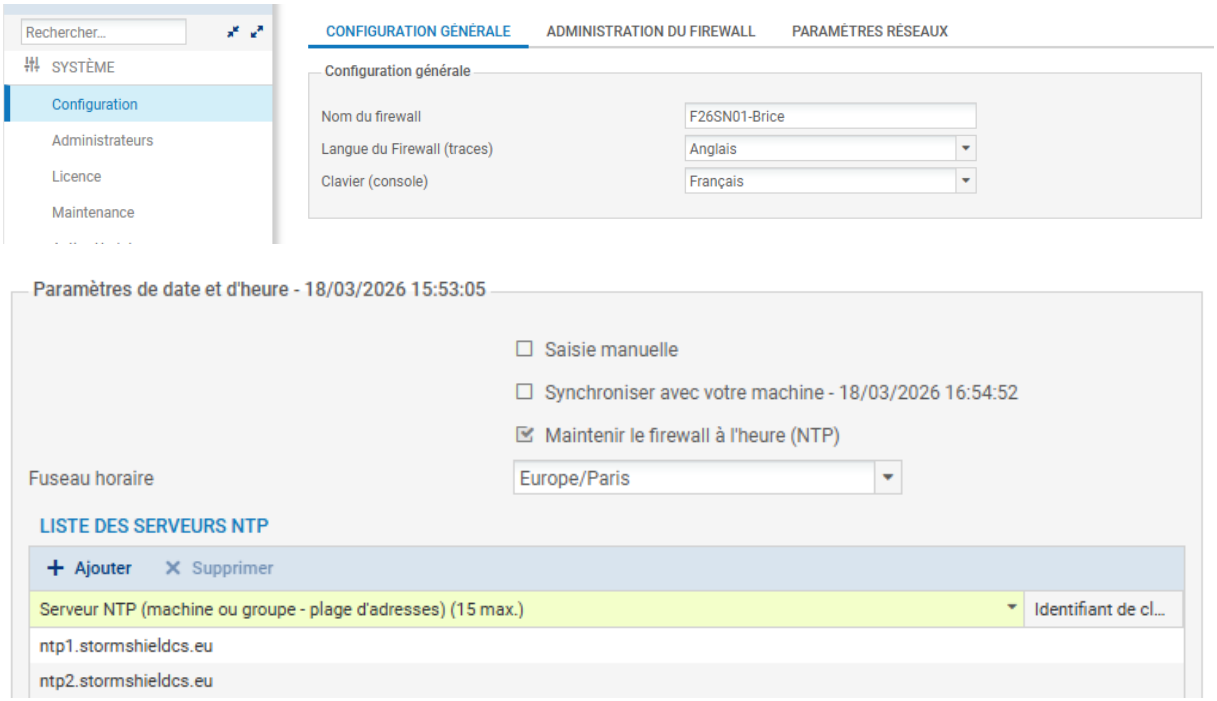
Vérifications :

- Active Directory : Joindre un poste au domaine depuis le site d'Amiens
- DNS : Résolution DNS de 192.168.11.11 en web.ppe2.local

4) Configuration pare-feu Stormshield

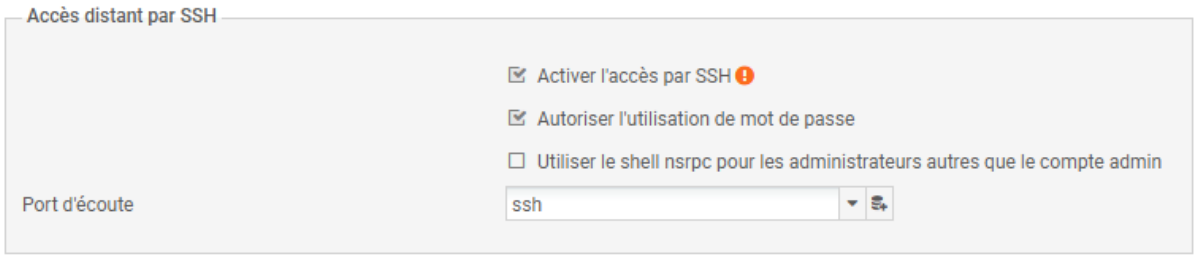
a) Configuration minimale de fonctionnement

Changement du nom du Firewall, de la langue du clavier et synchronisation NTP :
`Configuration > Système > Configuration > Configuration Générale`



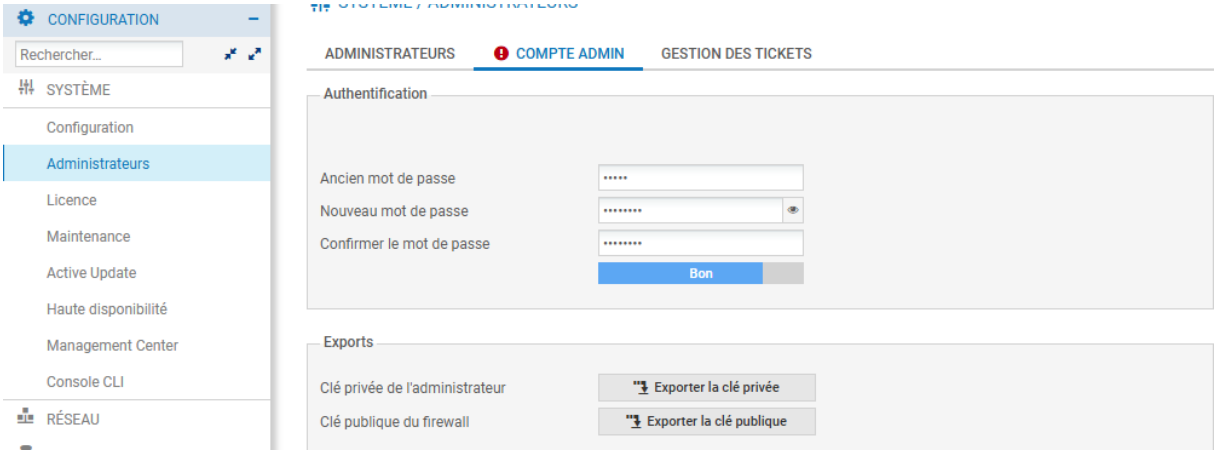
Activation SSH :

`Configuration > Système > Configuration > Configuration Générale`



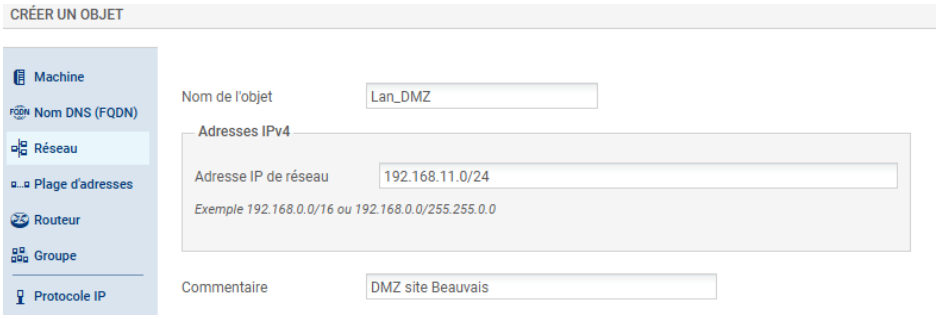
Mise en place mot de passe sur le compte admin :

`Configuration > Système > Administrateurs > Compte Admin`



Création des objets (exemple avec le Lan de la DMZ) :

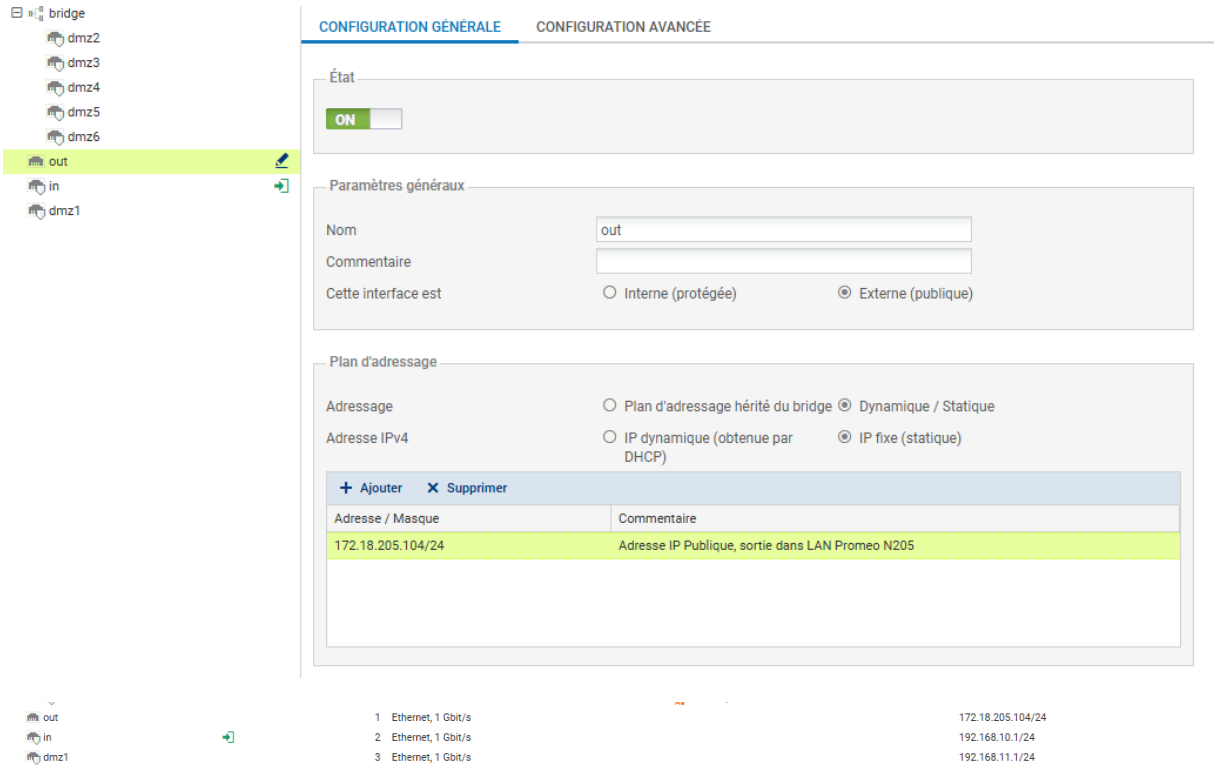
`Configuration > Objets > Réseau > +Ajouter`



b) Configuration Réseau

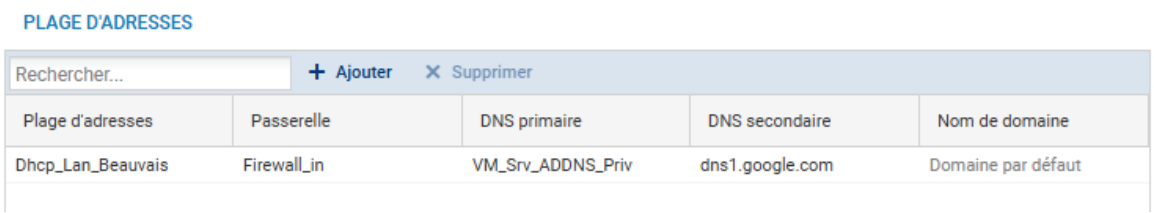
Configuration des interfaces physiques (exemple avec l'interface out) :

`Configuration > Réseau > Interfaces`

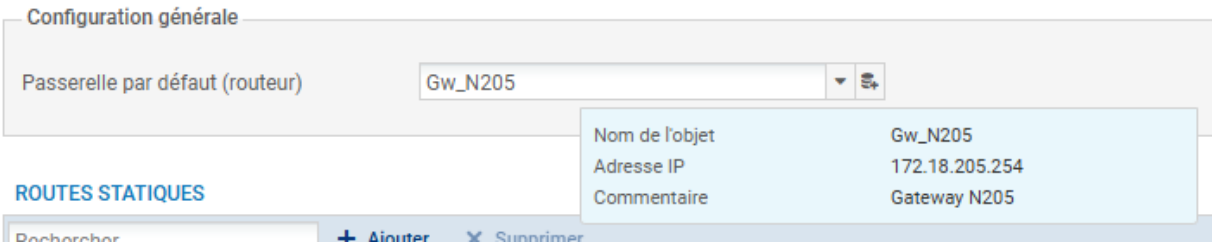


DHCP sur le site de Beauvais :

`Configuration > Réseau > DHCP`



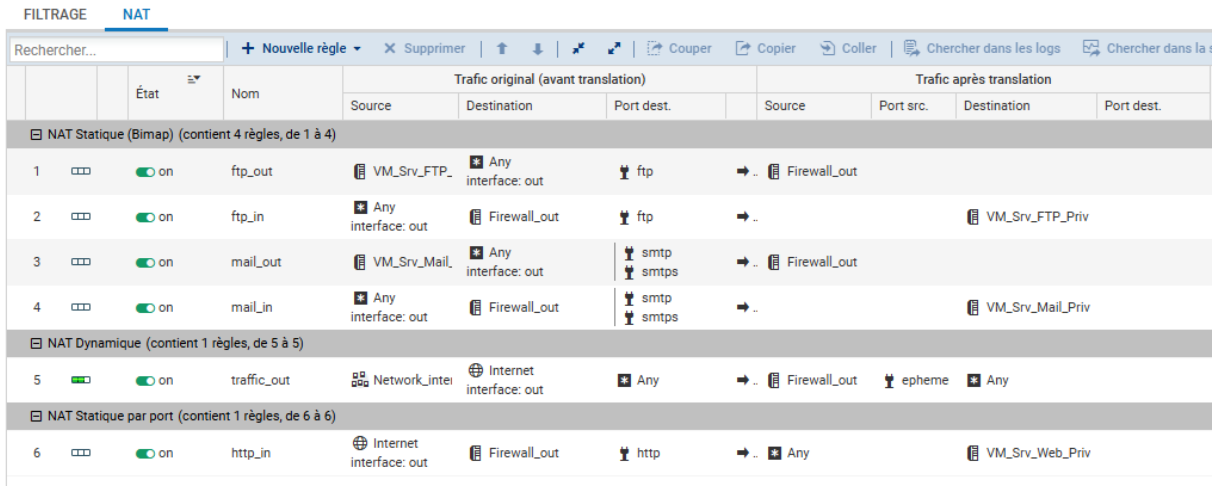
Passerelle par défaut :
`Configuration > Réseau > Routage`



c) Traduction d'adresses (NAT)

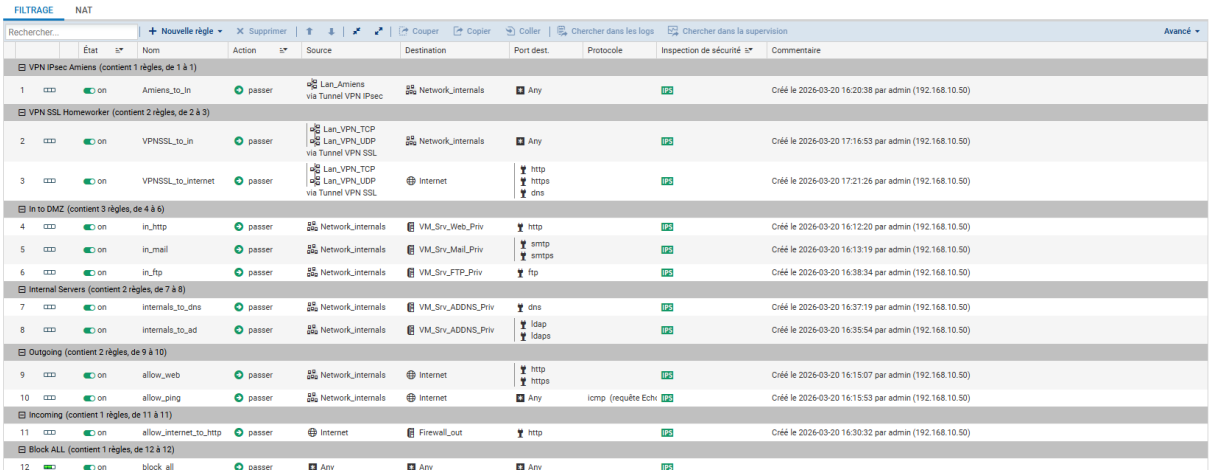
Création de NAT Statique Bimap (ftp, mail) et par port (http) pour les serveurs présents en DMZ.

NAT sur F26SN01 :
`Configuration > Politique de sécurité > Filtrage et NAT > NAT`



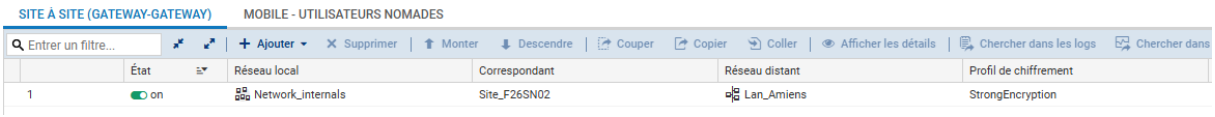
d) Règles de Filtrage

Entièreté des règles de filtrages mises en place sur le F26SN01 (y compris VPN).



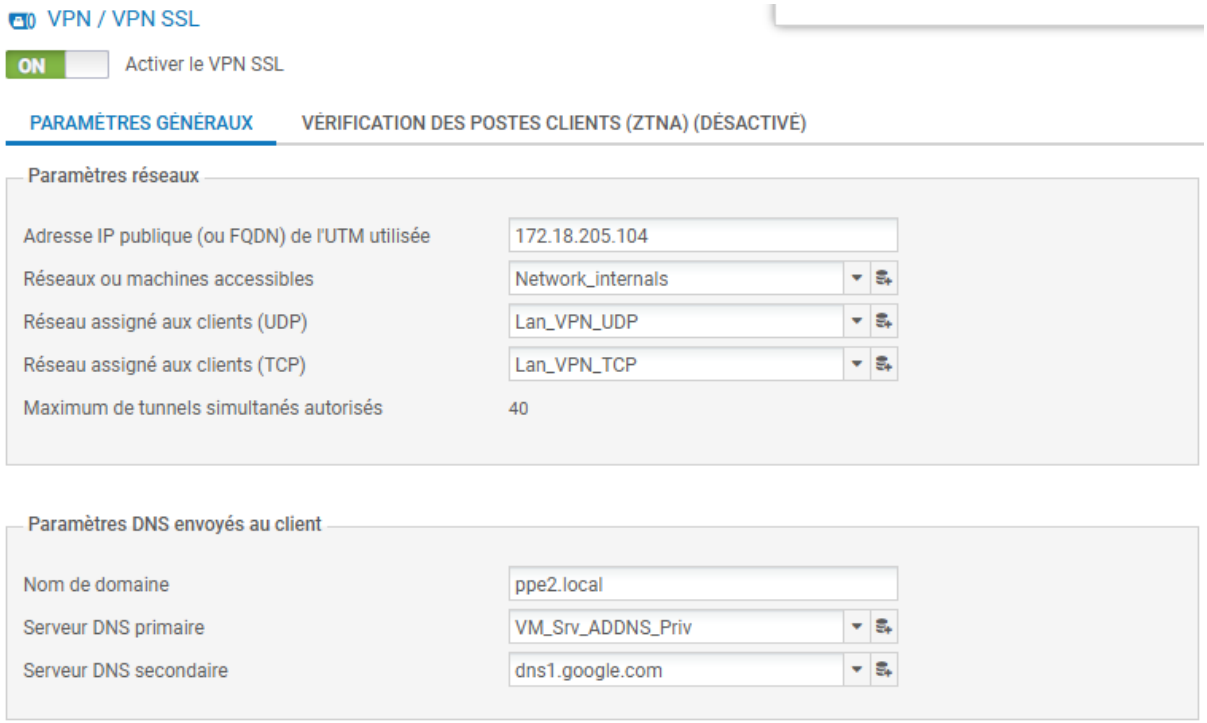
e) VPN

VPN site à site simple IPsec :
Configuration > VPN > VPN IPsec > Site à Site

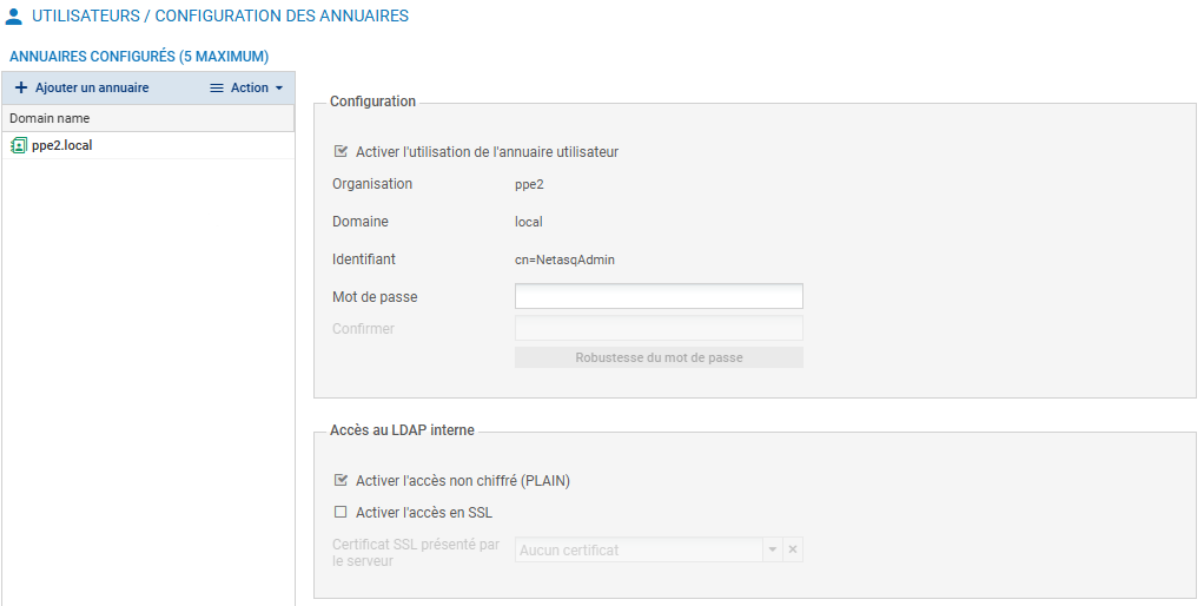


Ajout d'une règle dans le filtrage :

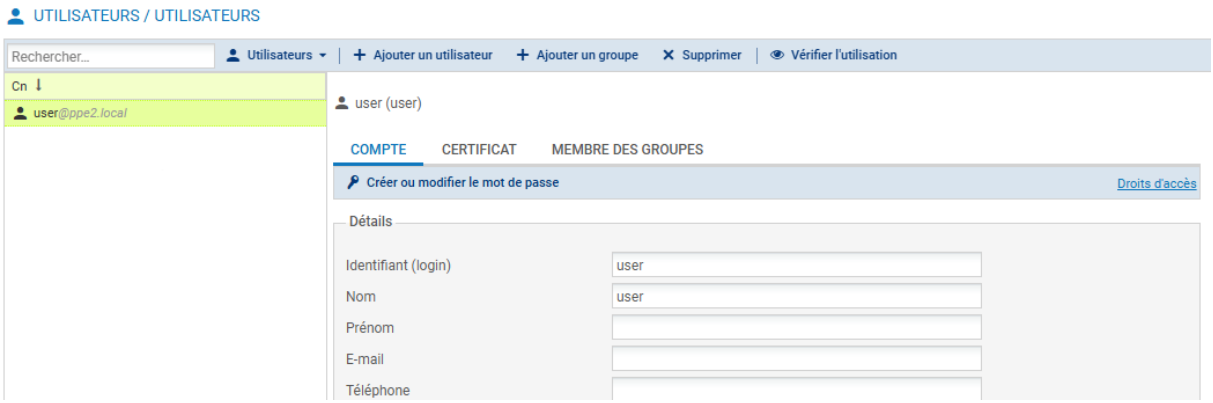
VPN SSL :
Configuration > VPN > VPN SSL



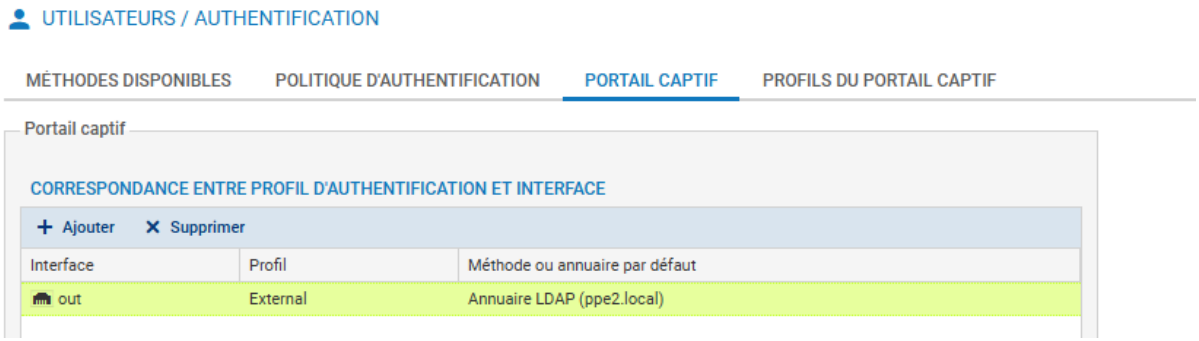
Créer un annuaire interne :
Configuration > Utilisateurs > Configuration des annuaires



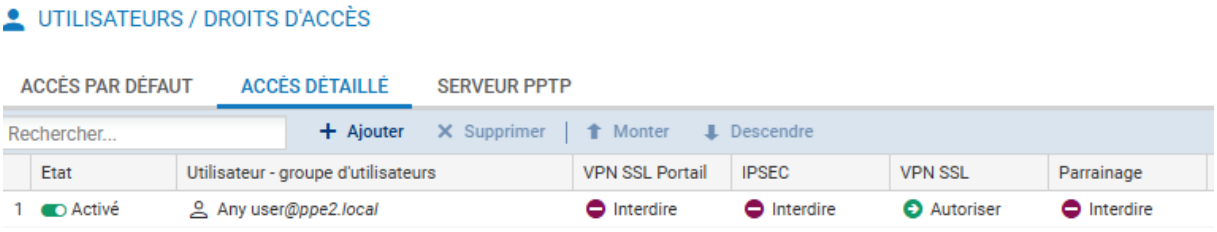
Créer un utilisateur :
Configuration > Utilisateurs > Utilisateurs



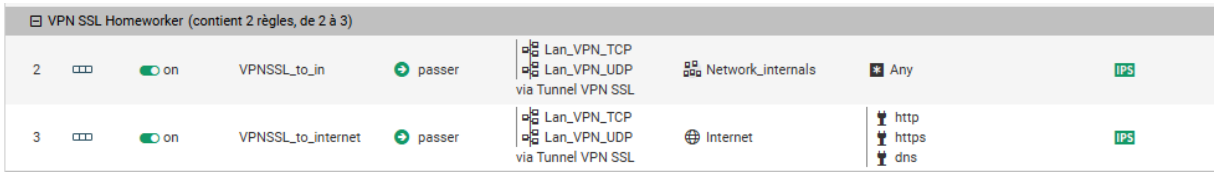
Profil External sur le port out :
Configuration > Utilisateurs > Authentification > Portail Captif



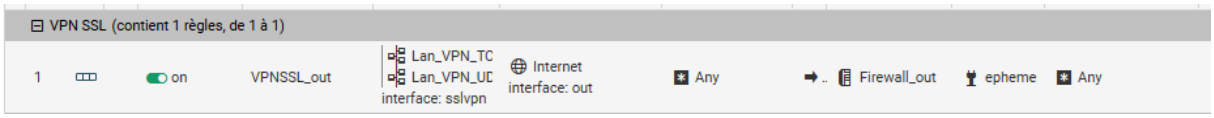
Autoriser l'accès à tout le monde :
Configuration > Utilisateurs > Droits d'accès > Accès détaillé



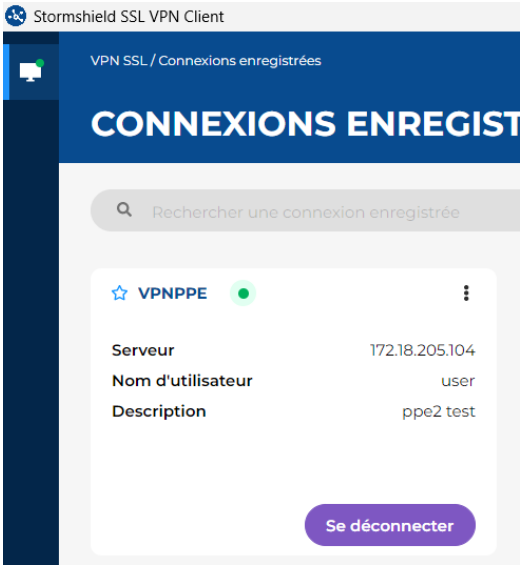
Règles de filtrage :

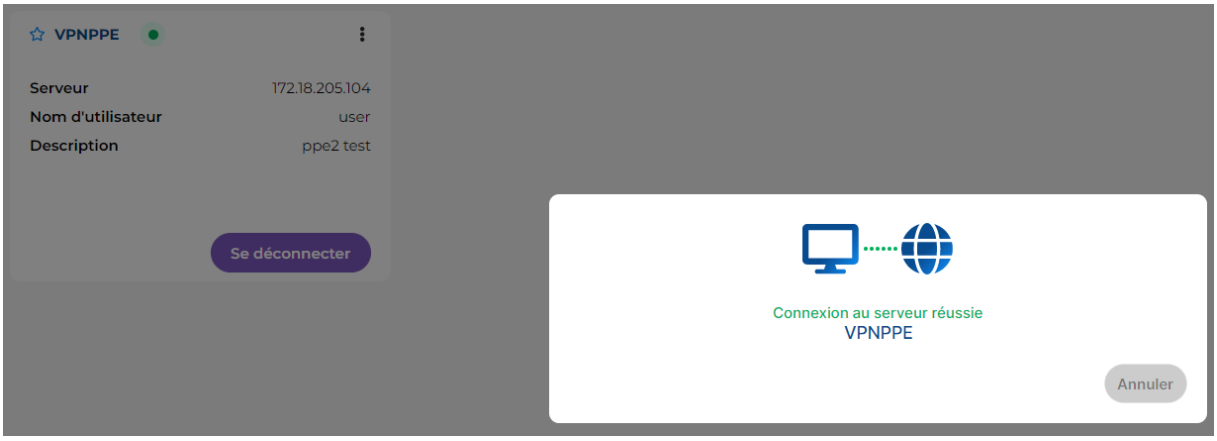


Règles NAT :



Utilisation de l'application « Stormshield SSL VPN Client » :





5) Tests et Validations

ICMP (Ping) :

✓ - Des LAN Beauvais, Amiens, VPN et DMZ vers Internet

✓ - Des LAN Beauvais, Amiens, VPN et DMZ entre eux

Serveurs :

✓ - Serveurs de la DMZ (Web, FTP et Mail) accessibles par tous

✓ - Serveurs internes (AD, DNS) depuis les réseaux internes

DHCP :

✓ - Des pare-feu pour les LAN de Beauvais, Amiens et VPN

NAT :

✓ - Redirection de l'interface out du pare-feu vers les serveurs en DMZ

✓ - NAT des réseaux internes en sortie vers internet

VPN :

✓ - IPSec entre les deux sites

✓ - SSL pour le Homeworker