“Stormshield + VPN SSL”

STORMSHIELD

Sommaire

Sommaire.....2
1. Qu'est-ce qu'un par-feu?.....3
2. Pocédure général.....4
3. Qu'est-ce que.....4
4. Procédure générale.....5
5. Installation et configuration "NOM"..... 9

1. Qu’est-ce qu’un par-feu?

*Un pare-feu est un équipement de sécurité réseau qui **filtre et contrôle le trafic** entre plusieurs zones (LAN, DMZ, Internet).*
*Il applique des règles pour **autoriser ou bloquer** les connexions afin de protéger le réseau contre les intrusions, attaques ou accès non autorisés.*

Dans ce projet, le pare-feu Stormshield permet :

- *de séparer les réseaux internes, DMZ et WAN,*
- *de sécuriser les communications,*
- *et d’autoriser l’accès distant grâce au VPN SSL.*

2. Procédure générale.

RÉSEAU / INTERFACES

Entrer un filtre... | Éditer | Ajouter | Supprimer | Superviser | Accéder à la supervision | Vérifier l'utilisation

Interface	Port	Type	État	Adresse IPv4
WAN	1	Ethernet, 1 Gbit/s		192.168.147.136/24 (DHCP)
LAN	2	Ethernet, 1 Gbit/s		192.168.200.254/24
dmz1	3	Ethernet, 1 Gbit/s		192.168.1.254/24

Configuration des interfaces réseau du pare-feu Stormshield. Définition des zones WAN, DMZ et LAN avec leurs adresses IP respectives. Cette étape prépare la segmentation du réseau.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(1) Block all | Editer | Exporter

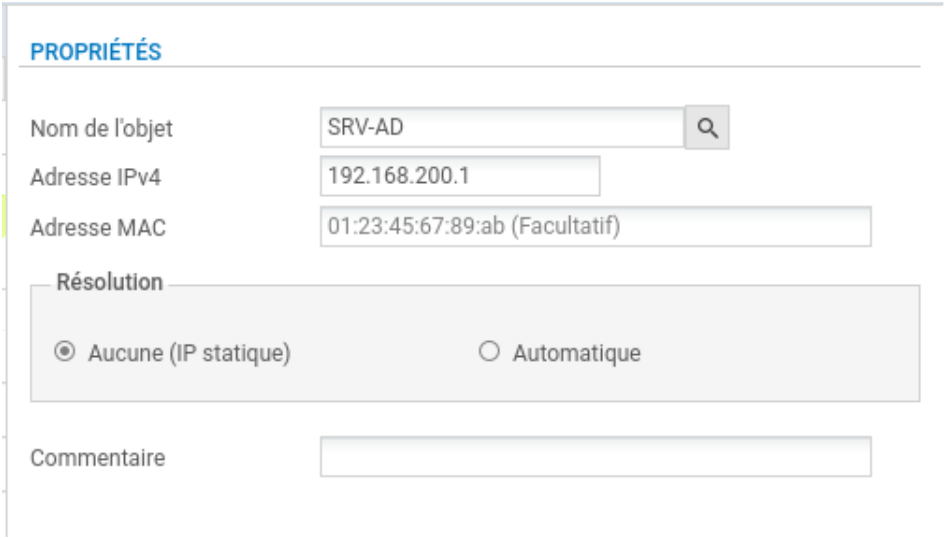
FILTRAGE | NAT

Rechercher... | Nouvelle règle | Supprimer | Couper | Copier | Coller | Chercher dans les logs | Chercher dans la supervision

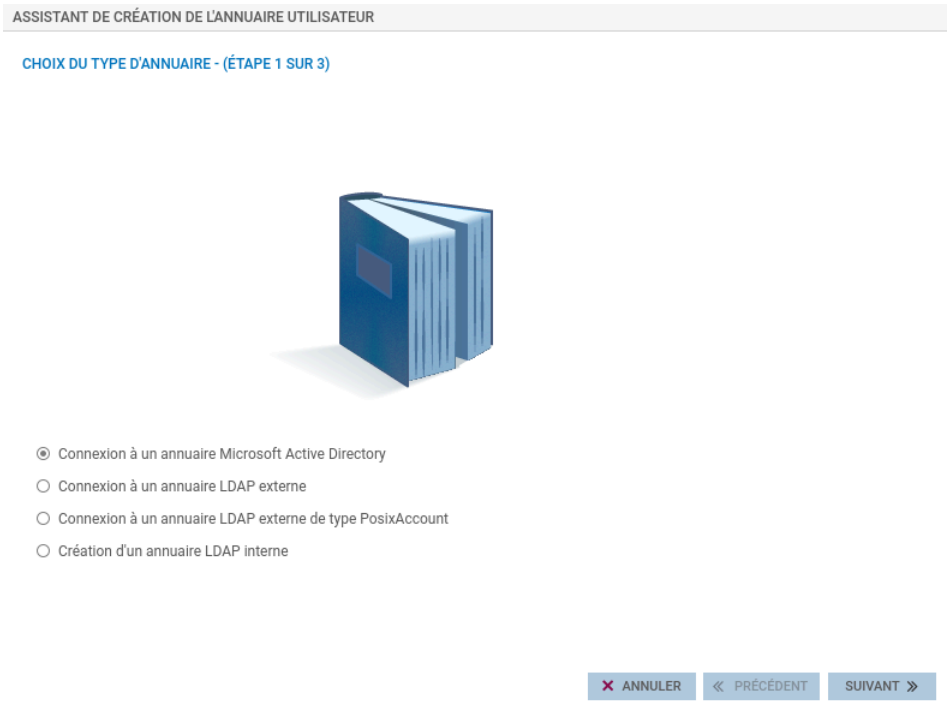
		État	Trafic original (avant translation)				Trafic après translation			
			Source	Destination	Port dest.		Source	Port src.	Destination	Port dest.
1		on	Network_internals	Internet	Any	→	Firewall_WAN	ephemeral_fw	Any	
2		on	Network_WAN	Firewall	haproxy1	→	Any		srvhaproxy1	ssh
3		on	Network_WAN	Firewall	web1	→	Any		srvweb1	ssh
4		on	Network_WAN	Firewall	haproxy2	→	Any		srvhaproxy2	ssh
5		on	Network_WAN	Firewall	web2	→	Any		srvweb2	ssh
6		on	Network_WAN	Firewall	http	→	Any		ipvirtuelle	http

Configuration des règles NAT.

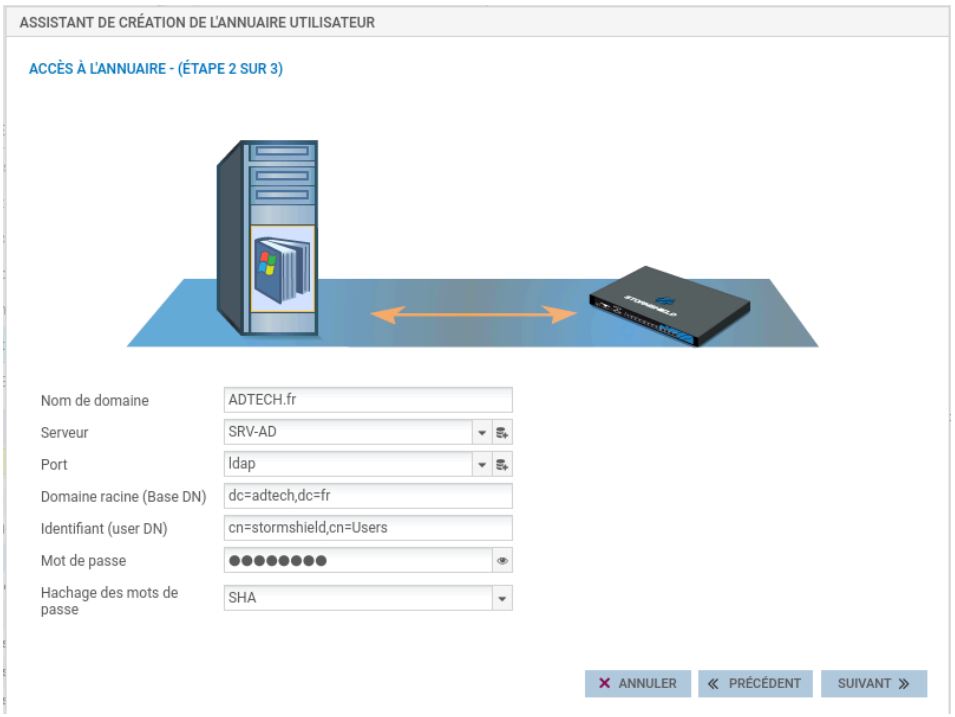
3. Connection de l’AD au Pare-Feu.



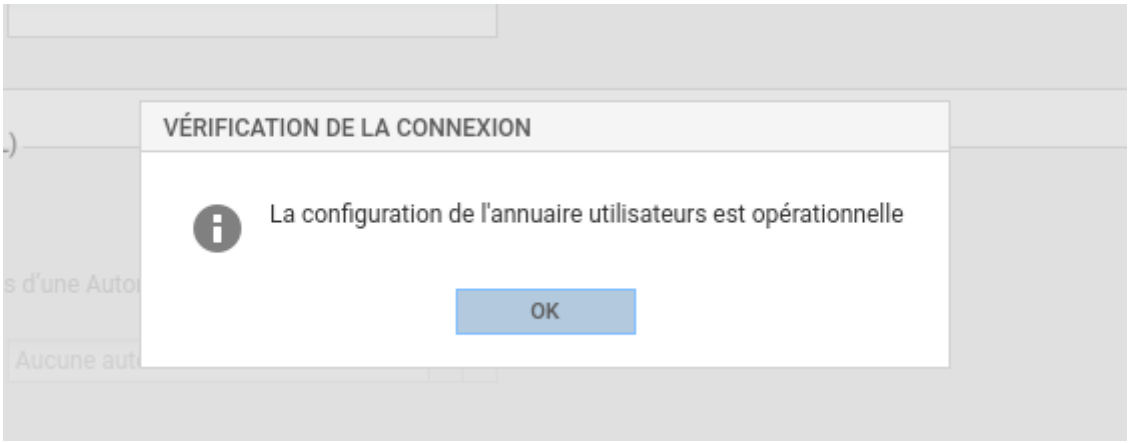
Créer un objet SRV-AD et mettre l’adresse ip du serveur AD.



Accédez au menu Configuration > Gestion des annuaires, puis cliquez sur Ajouter un annuaire. Sélectionnez ensuite l’option Connexion à un annuaire Microsoft Active Directory afin d’initier la liaison avec votre serveur AD.

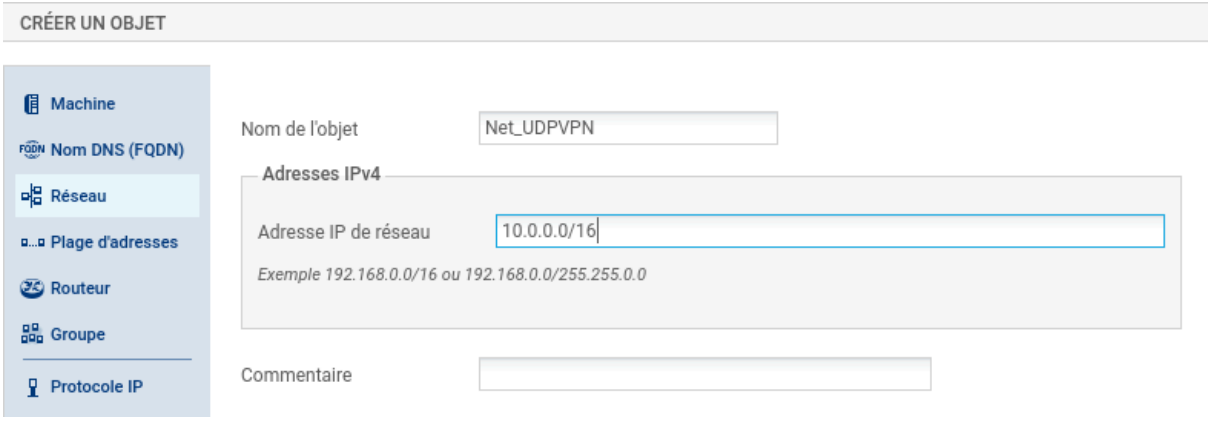


Configuration de la connexion entre le pare-feu et l'Active Directory : mise en place du domaine, de la connexion LDAP et du compte autorisé à consulter l'annuaire.

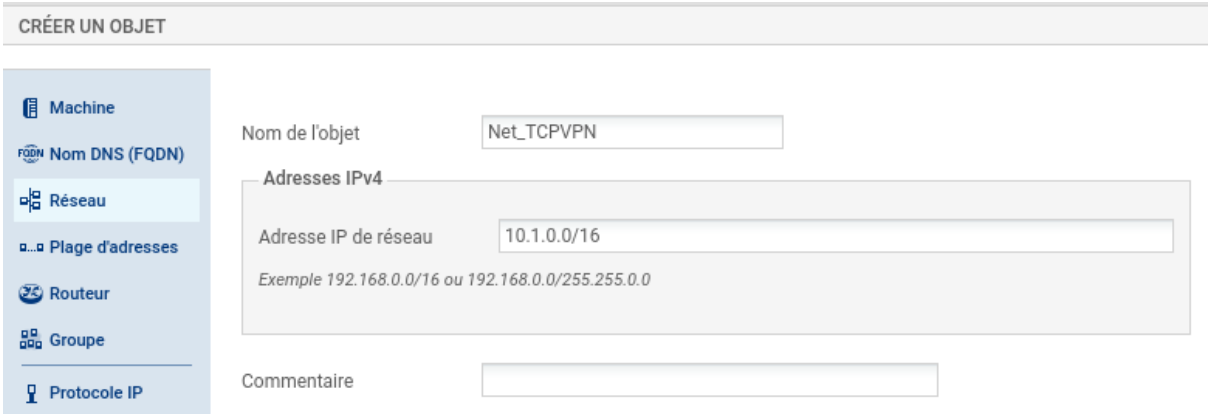


Vérification du bon fonctionnement de l'annuaire après son ajout, confirmant que la connexion est opérationnelle.

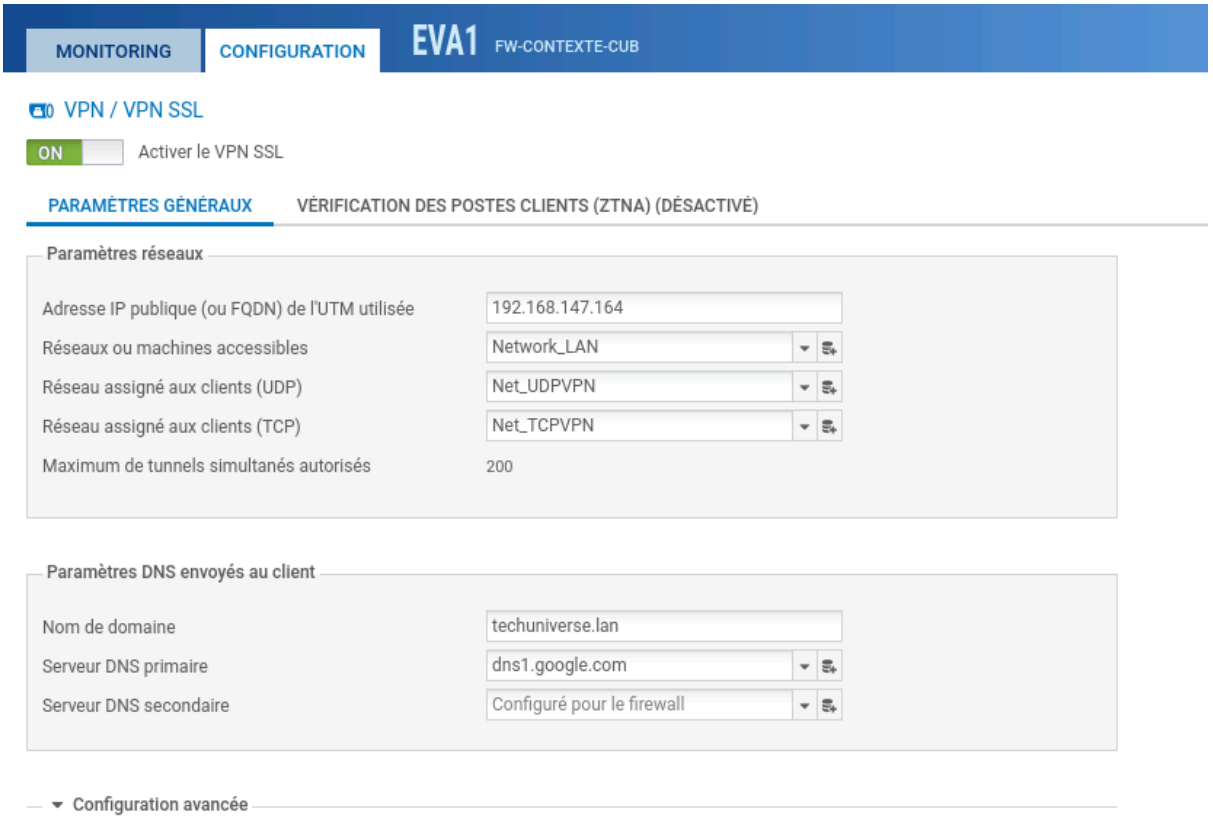
4. Configuration du VPN SSL.



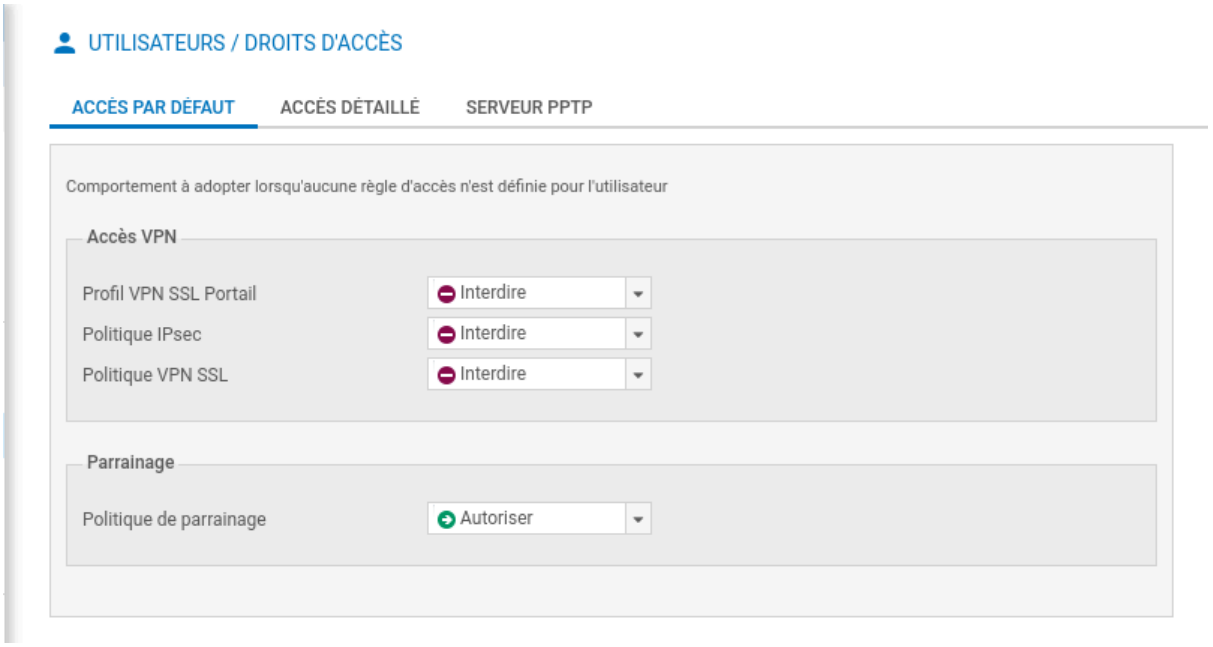
Création de l'objet réseau correspondant au sous-réseau du VPN SSL en protocole UDP. Cet objet est utilisé pour identifier et gérer le trafic VPN dans les règles de filtrage du pare-feu Stormshield.



Création de l'objet réseau correspondant au sous-réseau du VPN SSL en protocole TCP. Cet objet permet la prise en charge du trafic VPN SSL utilisant le protocole TCP.

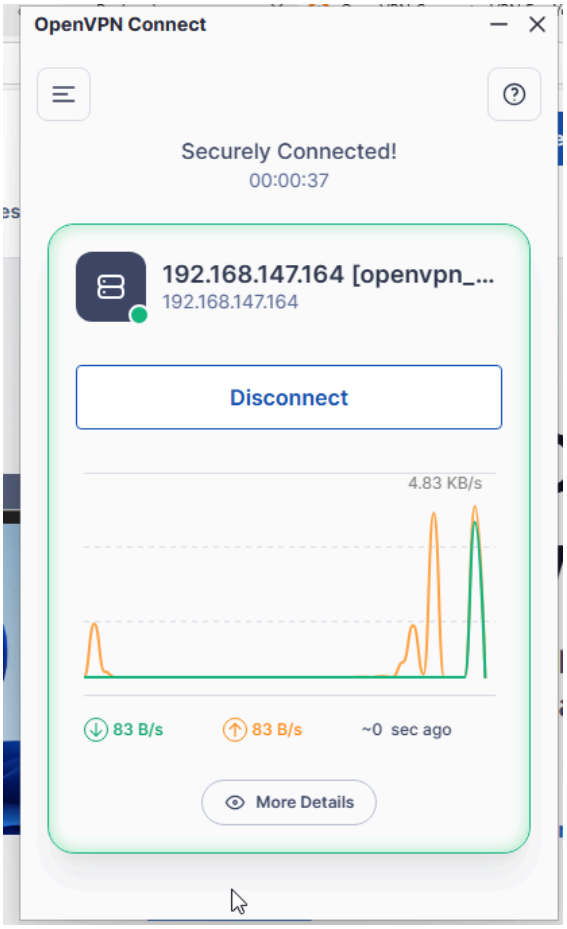


Activation et configuration du VPN SSL sur le pare-feu Stormshield.



Gestion des utilisateurs et des droits sur le pare-feu Stormshield. Cette configuration permet de définir les autorisations d'accès aux services du pare-feu et au VPN SSL selon les profils utilisateurs.

Export du fichier de configuration VPN SSL depuis le pare-feu Stormshield afin de l'importer dans l'application OpenVPN sur le poste client.



Connexion au VPN SSL établie avec succès via l'application OpenVPN, confirmant le bon fonctionnement de l'authentification et de l'accès distant au réseau interne.