

“Stormshield + VPN SSL”



STORMSHIELD

Sommaire

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

1. Qu'est-ce qu'un pare-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

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. Connexion de l'AD au Pare-Feu.

PROPRIÉTÉS

Nom de l'objet

Adresse IPv4

Adresse MAC

Résolution

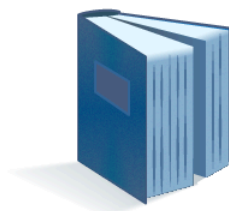
Aucune (IP statique) Automatique

Commentaire

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

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

CHOIX DU TYPE D'ANNUAIRE - (ÉTAPE 1 SUR 3)




- Connexion à un annuaire Microsoft Active Directory
- Connexion à un annuaire LDAP externe
- Connexion à un annuaire LDAP externe de type PosixAccount
- Création d'un annuaire LDAP interne

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.

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Nom de domaine: ADTECH.fr

Serveur: SRV-AD

Port: ldap

Domaine racine (Base DN): dc=adtech,dc=fr

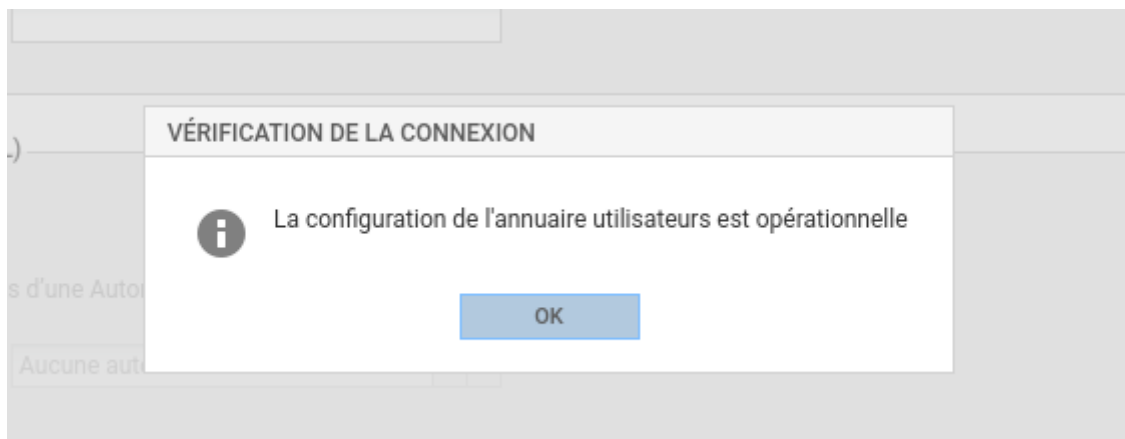
Identifiant (user DN): cn=stormshield,cn=Users

Mot de passe: [masqué]

Hachage des mots de passe: SHA

ANNULER PRÉCÉDENT SUIVANT

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.

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet

Adresses IPv4

Adresse IP de réseau

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire

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.

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet

Adresses IPv4

Adresse IP de réseau

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire

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.

VPN / VPN SSL

ON Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée	192.168.147.164
Réseaux ou machines accessibles	Network_LAN
Réseau assigné aux clients (UDP)	Net_UDPVPN
Réseau assigné aux clients (TCP)	Net_TCPVPN
Maximum de tunnels simultanés autorisés	200

Paramètres DNS envoyés au client

Nom de domaine	techuniverse.lan
Serveur DNS primaire	dns1.google.com
Serveur DNS secondaire	Configuré pour le firewall

Configuration avancée

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

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT ACCÈS DÉTAILLÉ SERVEUR PPTP

Comportement à adopter lorsqu'aucune règle d'accès n'est définie pour l'utilisateur

Accès VPN

Profil VPN SSL Portail	Interdire
Politique IPsec	Interdire
Politique VPN SSL	Interdire

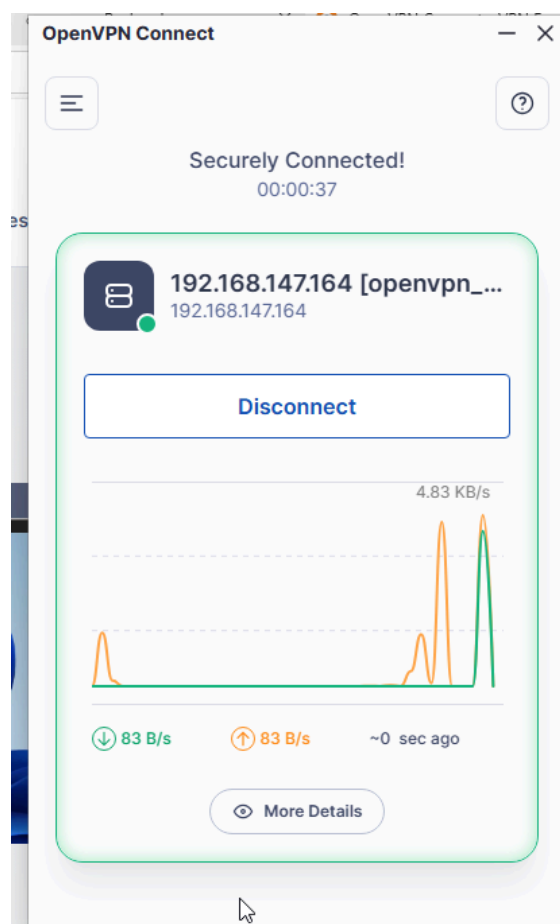
Parrainage

Politique de parrainage	Autoriser
-------------------------	-----------

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.