

# “Stormshield + VPN SSL”



# STORMSHIELD

# Sommaire

<b>Sommaire.....</b>	<b>2</b>
<b>1. Qu'est-ce qu'un par-feu?.....</b>	<b>3</b>
<b>2. Procédure général.....</b>	<b>4</b>
<b>3. Qu'est-ce que.....</b>	<b>4</b>
<b>4. Procédure générale.....</b>	<b>5</b>
<b>5. Installation et configuration “NOM”.....</b>	<b>9</b>

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

*Configuration des règles NAT.*

# 3. Connection de l'AD au Pare-Feu.

**PROPRIÉTÉS**

Nom de l'objet	SRV-AD	<input type="button" value="🔍"/>
Adresse IPv4	192.168.200.1	
Adresse MAC	01:23:45:67:89:ab (Facultatif)	
Résolution	<input checked="" type="radio"/> Aucune (IP statique) <input type="radio"/> Automatique	
Commentaire	<input type="text"/>	

*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)



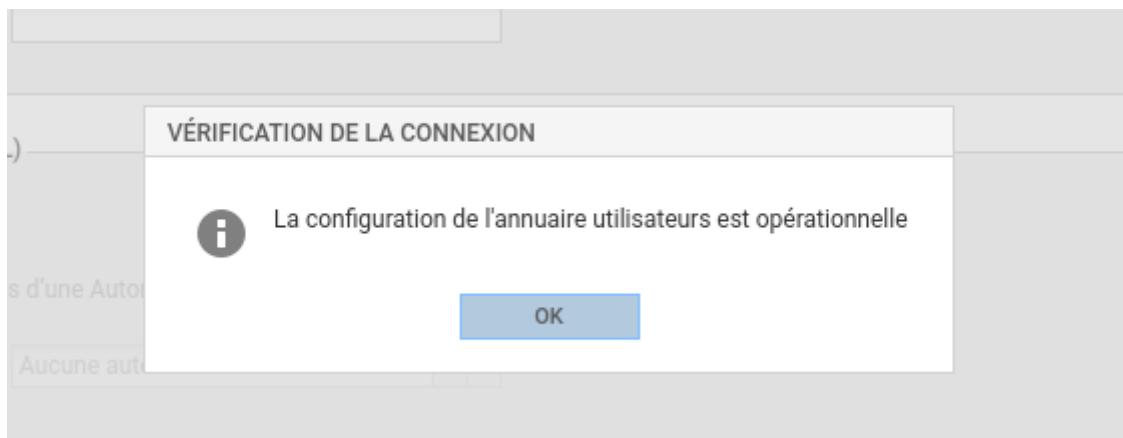
Connexion à un annuaire Microsoft Active Directory  
 Connexion à un annuaire LDAP externe  
 Connexion à un annuaire LDAP externe de type PosixAccount  
 Création d'un annuaire LDAP interne

*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.*



*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: Net\_UDPVPN

Adresses IPv4

Adresse IP de réseau: 10.0.0.0/16

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: Net\_TCPVPN

Adresses IPv4

Adresse IP de réseau: 10.1.0.0/16

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.*

The screenshot shows the EVA1 FW-CONTEXT-CUB configuration interface. The top navigation bar has tabs for MONITORING and CONFIGURATION, with CONFIGURATION selected. The main title is EVA1 FW-CONTEXT-CUB. The current page is VPN / VPN SSL. A sub-header says "ON" and "Activer le VPN SSL". Below this, there are two tabs: "PARAMÈTRES GÉNÉRAUX" (selected) and "VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)".

**PARAMÈTRES GÉNÉRAUX**

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.*

The screenshot shows the EVA1 FW-CONTEXT-CUB configuration interface. The top navigation bar has tabs for UTILISATEURS / DROITS D'ACCÈS, ACCÈS PAR DÉFAUT (selected), ACCÈS DÉTAILLÉ, and SERVEUR PPTP. The main title is UTILISATEURS / DROITS D'ACCÈS.

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

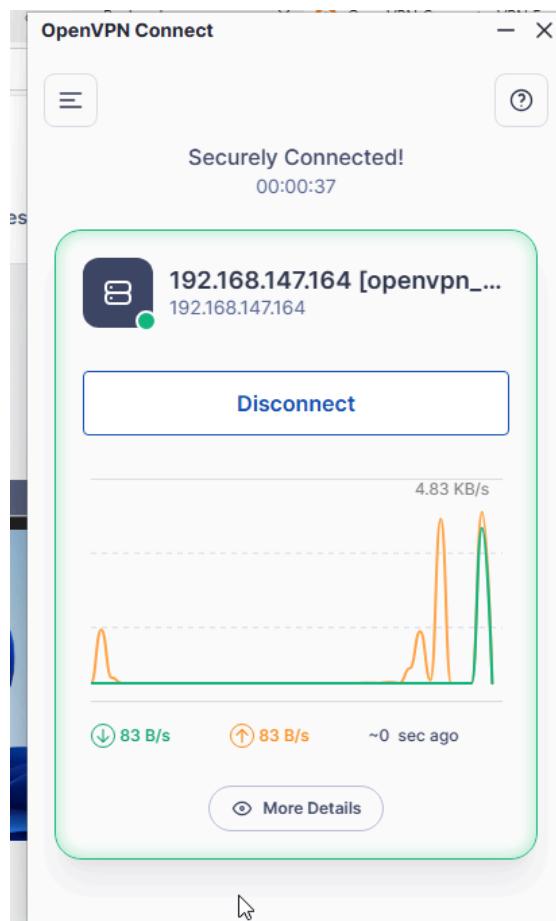
Parraining

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.*