

Config Pare-Feu



STORMSHIELD

Sommaire

Sommaire.....	2
1. Qu'est-ce qu'un Pare-Feu ?.....	3
2. Paramètre de base.....	4
3. Connecter l'AD au Pare-Feu.....	5-6
5. Configurer le VPN SSL.....	7-9
6. Connecter le client au VPN.....	10-11

1. Qu'est-ce qu'un Pare-Feu ?

Un pare-feu est un outil de sécurité informatique, matériel ou logiciel, qui surveille et filtre le trafic entrant et sortant d'un réseau ou d'un ordinateur. Il applique des règles pour autoriser ou bloquer certaines connexions, afin de prévenir les intrusions, limiter les attaques et protéger les données sensibles. En résumé, il agit comme une barrière qui laisse passer uniquement le trafic jugé sûr.

2. Paramètre de base

Interface	Port	Type	État	Adresse IPv4
WAN	1	Ethernet, 1 Gbi...	192.168.147.194/24 (DHCP)	
LAN	2	Ethernet, 1 Gbi...	192.168.200.254/24	
DMZ	3	Ethernet, 1 Gbi...	192.168.1.254/24	

Interfaces réseaux

FILTRAGE		NAT												
Rechercher...		+ Nouvelle règle		Supprimer		↑	↓	✖	✖	Couper	Copier	Coller	Chercher dans les logs	Log
		État	▼	Trafic original (avant translation)				Trafic après translation						
<input type="checkbox"/> Règle de sortie pour internet - masquage (contient 1 règles, de 1 à 1)														
1	🟢	on		Network_intern	🌐 Internet	*	Any	→	Firewall_WAN	*	Any			
<input type="checkbox"/> Règle de publication du serveur web (contient 1 règles, de 2 à 2)														
2	🔴	on		🌐 Internet	Firewall_WAN	HTTP		→	*	Any		IpVirtuelle	HTTP	
<input type="checkbox"/> Règle de connexion en SSH des serveur web et haproxy (contient 4 règles, de 3 à 6)														
3	🟢	🔴	on	🌐 Internet	Firewall_WAN	SSH-WEB1		→	*	Any		SRV-WEB1	SSH	
4	🟡	🔴	on	🌐 Internet	Firewall_WAN	SSH-WEB2		→	*	Any		SRV-WEB2	SSH	
5	🟢	🔴	on	🌐 Internet	Firewall_WAN	SSH-PROXY1		→	*	Any		SRV-HAPRC	SSH	
6	🟡	🔴	on	🌐 Internet	Firewall_WAN	SSH-PROXY2		→	*	Any		SRV-HAPRC	SSH	

Règles de NAT

3. Connecter l'AD au Pare-feu

ANNUAIRES CONFIGURÉS (5 MAXIMUM)

+ Ajouter un annuaire

Domain name

CONFIGURATION STRUCTURE

ÉDITION : SRV-AD (HOST)

Type Nom de l'objet

cloucurl-download-sns.storm

SRV-AD

agent_ad

icap

kerberos-adm

kerberos-admin_tcp

kerberos-admin_udp

netnews

radacct

radius

Nom de l'objet : SRV-AD

Adresse IPv4 : 192.168.200.1

Adresse MAC : 01:23:45:67:89:ab (Facultatif)

Résolution

Aucune (IP statique) Automatique

Commentaire

Ajouter l'objet AD au stormshield

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

✖ ANNULER << PRÉCÉDENT SUIVANT >>

Allez dans “Configuration > configuration des annuaires”, cliquez sur “Ajouter un annuaire” puis “Connexion à un annuaire Microsoft AD”



Configuration de l'accès du pare-feu à l'Active Directory : domaine, serveur LDAP et compte utilisé pour interroger l'annuaire.

Vérification si l'ajout de l'annuaire est fonctionnel

4. Configurer le VPN SSL

CRÉER UN OBJET

Machine
 Nom DNS (FQDN)
 Réseau
 Plage d'adresses
 Routeur
 Groupe
 Protocole IP
 Port
 Groupe de ports

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

CRÉER UN OBJET

Machine
 Nom DNS (FQDN)
 Réseau
 Plage d'adresses
 Routeur
 Groupe
 Protocole IP
 Port
 Groupe de ports

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

Créez les objets TCP et UDP VPN

The screenshot shows the EVA1 FW-CONTEXTE-CUB configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'CONFIGURATION' being active. The title 'EVA1 FW-CONTEXTE-CUB' is displayed. On the left, there is a vertical sidebar with various icons. The main content area is titled 'PARAMÈTRES GÉNÉRAUX' and 'VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)'. It contains sections for 'Paramètres réseaux' and 'Paramètres DNS envoyés au client'. In the 'Paramètres réseaux' section, fields include 'Adresse IP publique (ou FQDN) de l'UTM utilisée' (192.168.147.194), 'Réseaux ou machines accessibles' (Network_LAN), 'Réseau assigné aux clients (UDP)' (NET_UDPVPN), 'Réseau assigné aux clients (TCP)' (NET_TCPVPN), and 'Maximum de tunnels simultanés autorisés' (200). In the 'Paramètres DNS envoyés au client' section, fields include 'Nom de domaine' (ADTECH.fr) and 'Serveur DNS primaire' (dns1.google.com). At the bottom are 'ANNULER' and 'APPLIQUER' buttons.

Allez dans “VPN > VPN SSL”, ajoutez l’ip du pare-feu, les objets ajouté précédemment, et le nom de domaine

The screenshot shows the EVA1 FW-CONTEXTE-CUB configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'CONFIGURATION' being active. The title 'UTILISATEURS / DROITS' is displayed. On the left, there is a vertical sidebar with various icons. The main content area is titled 'ACCÈS PAR DÉFAUT', 'ACCÈS DÉTAILLÉ', and 'SERVEUR PPTP'. It contains sections for 'Accès VPN' and 'Parrainage'. In the 'Accès VPN' section, dropdown menus for 'Profil VPN SSL Portail', 'Politique IPsec', and 'Politique VPN SSL' are all set to 'Interdire'. In the 'Parrainage' section, the 'Politique de parrainage' dropdown is set to 'Autoriser'. A message box at the top right says 'La configuration du module Utilisateurs / Droits d'accès a été sauvegardée'. At the bottom are 'ANNULER' and 'APPLIQUER' buttons.

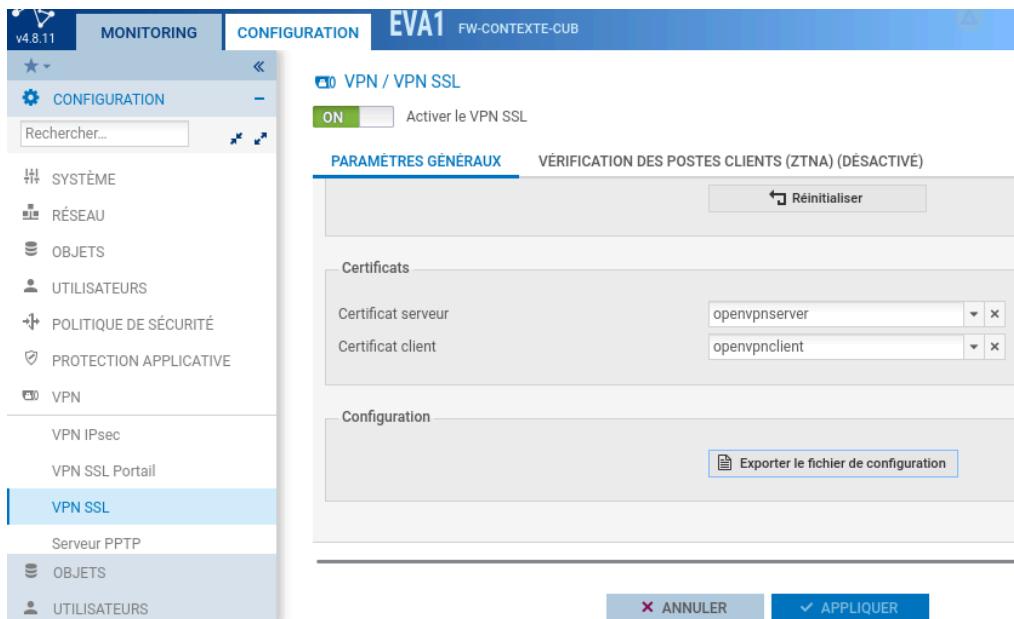
Interdire le profil “VPN SSL Portail,” “Politique IPsec et VPN SSL” Pour bloquer l'accès au VPN pour tous les utilisateurs

The screenshot shows the EVA1 FW-CONTEXTE-CUB configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'CONFIGURATION' being active. The title 'EVA1 FW-CONTEXTE-CUB' is displayed. On the left, there is a sidebar with icons for monitoring, configuration, and logs. The main content area is titled 'UTILISATEURS / DROITS D'ACCÈS'. Below this, three tabs are visible: 'ACCÈS PAR DÉFAUT', 'ACCÈS DÉTAILLÉ' (which is selected), and 'SERVEUR PPTP'. A search bar and buttons for '+ Ajouter' (Add), 'Supprimer' (Delete), 'Monter' (Move Up), and 'Descendre' (Move Down) are present. A table lists access rules:

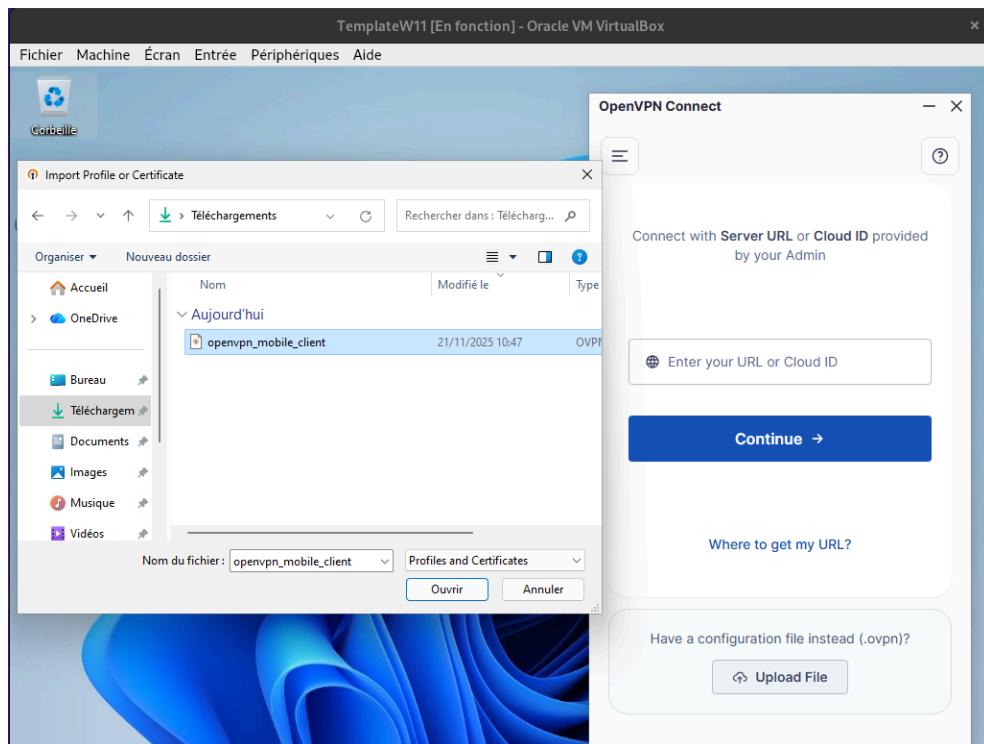
Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Dés
Activé	Télétravailleurs@adtech.fr	Interdire	Interdire	Autoriser	Interdire	

Ajoutez une règle qui autorise seulement le groupe “Télétravailleurs” au VPN SSL

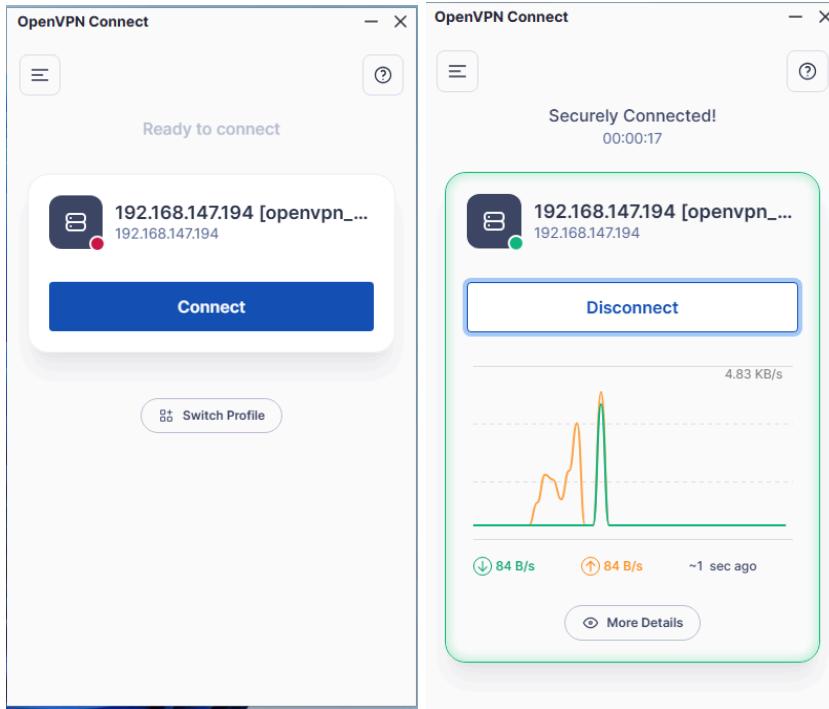
5. Connecter le client au VPN



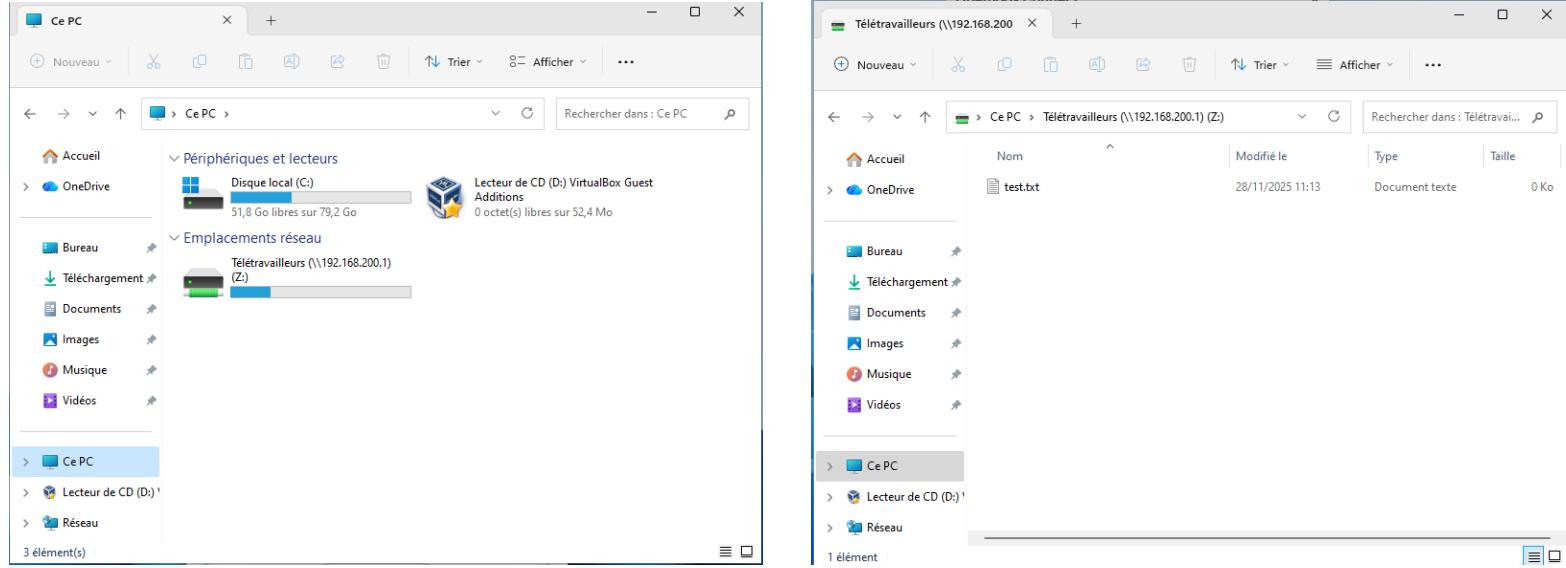
exportez le fichier de conf et l'importer sur le client



Cliquez sur "Upload File" et ouvrir le fichier de conf



Cliquez sur “Connect” et connectez vous à un utilisateurs membre du groupe “Télétravailleurs”



Vérifiez si on voit un disque d'emplacement réseau