

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 X Supprimer ↑ ↓ ↕ ↗ Couper Copier Coller Chercher dans les logs											
	État	Trafic original (avant translation)				Trafic après translation							
		Source	Destination	Port dest.		Source	Port src.	Destination	Port dest.				
Regle de sortie pour internet - masquage (contient 1 règles, de 1 à 1)													
1	on	Network_intern	Internet	Any	⇒	Firewall_WAN		Any					
Règle de publication du serveur web (contient 1 règles, de 2 à 2)													
2	on	Internet	Firewall_WAN	http	⇒	Any		IpVirtuelle	http				
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

OBJETS

ad

ANNUAIRES CONFIGURÉS (5 MAXIMUM)

+ Ajouter un annuaire

Action

CONFIGURATION

STRUC

ÉDITION : SRV-AD (HOST)

Nom de l'objet: SRV-AD

Adresse IPv4: 192.168.200.1

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

Résolution

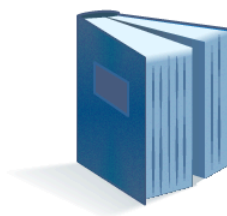
☒ Aucune (IP statique) ☐ Automatique

Commentaire

Ajouter l'objet AD au stormshield

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

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



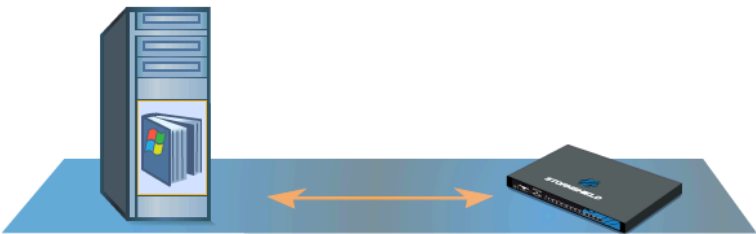
- ☒ Connexion à un annuaire Microsoft Active Directory
- ☐ Connexion à un annuaire LDAP externe
- ☐ Connexion à un annuaire LDAP externe de type PosixAccount
- ☐ Création d'un annuaire LDAP interne

✖ ANNULER « PRÉCÉDENT SUIVANT »

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

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: [masked]

Hachage des mots de passe: SHA

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

+ Ajouter un annuaire Action ▾

Domain name

ADTECH.fr

CONFIGURATION STRUCTURE

Annuaire distant

Activer l'utilisation de l'annuaire utilisateur

Serveur: SRV-AD

Port: ldap

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

Identifiant: cn=stormshield,cn=Users

Mot de passe: [masked]

VÉRIFICATION DE LA CONNEXION

i La configuration de l'annuaire utilisateurs est opérationnelle

OK

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

MONITORING **CONFIGURATION** **EVA1** FW-CONTEXTE-CUB

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	192.168.147.194
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	ADTECH.fr
Serveur DNS primaire	dns1.google.com

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

MONITORING **CONFIGURATION** **UTILISATEURS / DROITS**

La configuration du module Utilisateurs / Droits d'accès a été sauvegardée

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
-------------------------	-----------

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

 v4.8.11
 MONITORING
CONFIGURATION
EVA1 FW-CONTEXTE-CUB
 ad
ÉC
LO

>>
 ★

⚙️

 🏠

 📊

 👤

👤 UTILISATEURS / DROITS D'ACCÈS

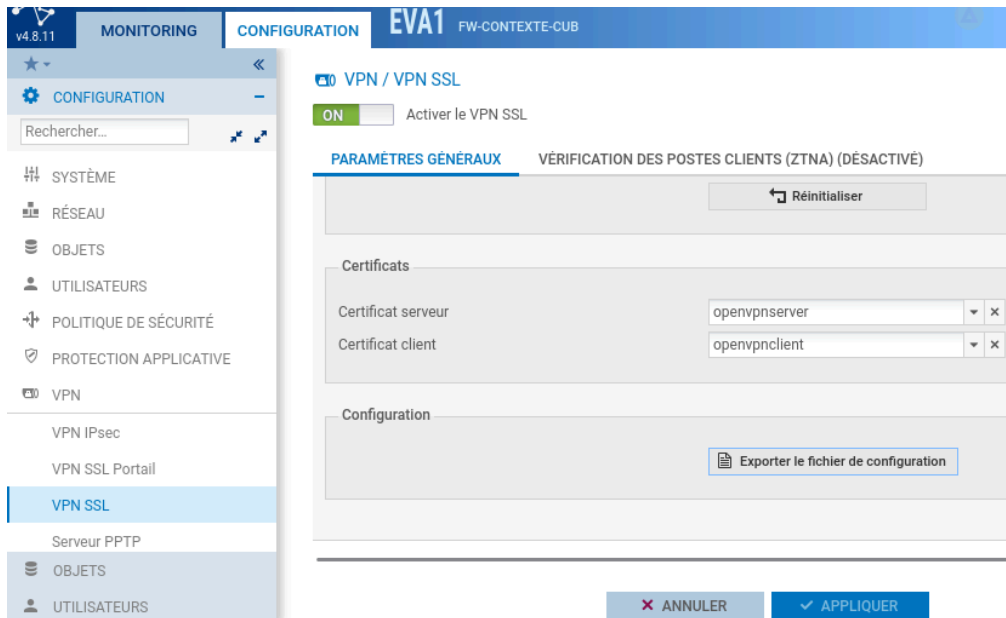
ACCÈS PAR DÉFAUT
 ACCÈS DÉTAILLÉ
 SERVEUR PPTP

Rechercher...
 + Ajouter
✕ Supprimer
↑ Monter
↓ Descendre

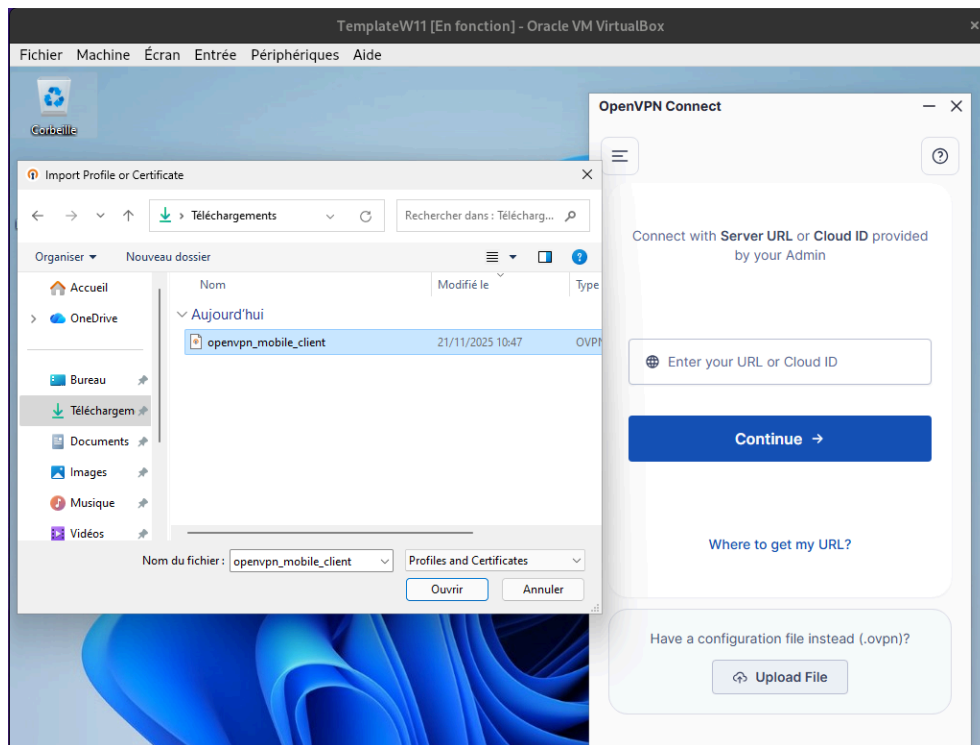
	Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Des
1	🟢 Activé	👤 Télétravailleurs@adtech.fr	🚫 Interdire	🚫 Interdire	🟢 Autoriser	🚫 Interdire	

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

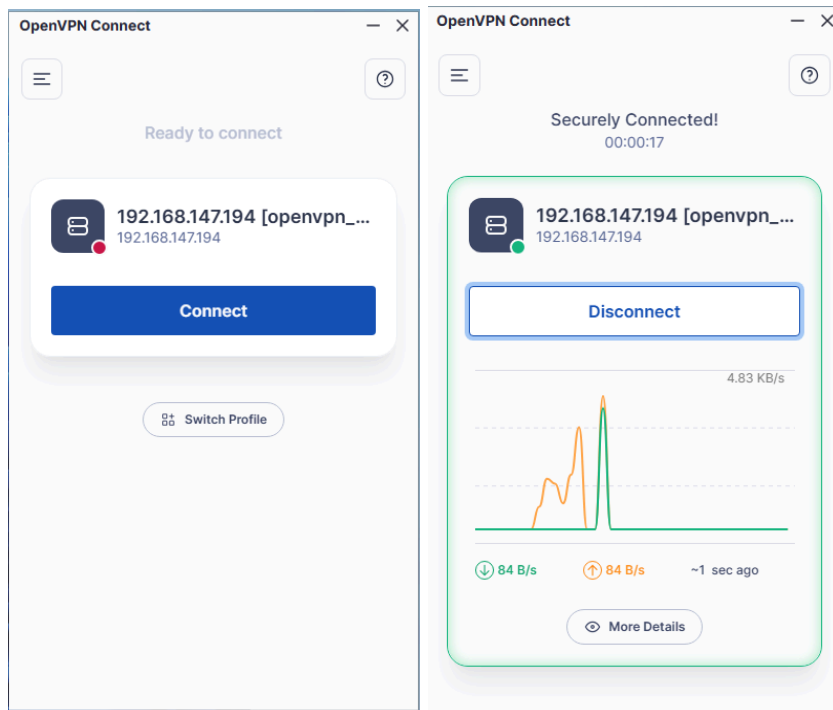
5. Connecter le client au VPN



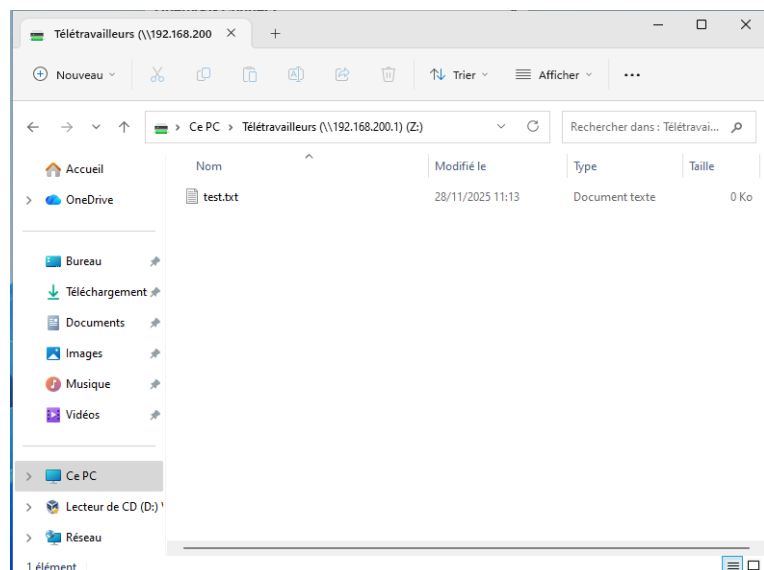
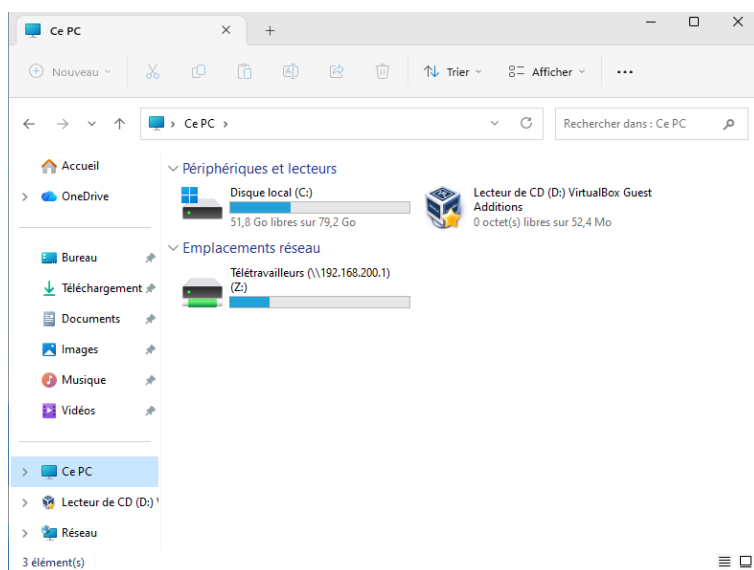
exportez le fichier de conf et l'importer sur le client



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