

# Activité : configurer un VPN IPsec

## Présentation

Cette activité consiste à configurer un tunnel IPsec entre deux SNS Stormshield en utilisant :

- soit l'environnement virtuel mis en place avec VirtualBox en configurant le tunnel entre les agences A et B;
- soit l'environnement virtuel mis en place avec Proxmox en configurant le tunnel entre deux équipes .

La suite de ce document est réalisé dans l'environnement mis en place avec VirtualBox.

## Définir la politique de filtrage

Réactiver la politique de filtrage **(10) Pass All**.


## Configurer le tunnel IPsec avec une clé partagée sur le premier SNS


- Depuis l'interface d'administration du SNS de l'un des extrémités du tunnel , accédez au menu **VPN ⇒ VPN IPsec > onglet POLITIQUE DE CHIFFREMENT - TUNNELS** ;
- Dans la rubrique **SITE À SITE (GATEWAY - GATEWAY)**, cliquez sur **Ajouter ⇒ Tunnel site à site**.


The screenshot shows the Stormshield VPN configuration interface. The top navigation bar includes 'VPN / IPSEC VPN' and tabs for 'ENCRYPTION POLICY - TUNNELS', 'PEERS', 'IDENTIFICATION', and 'ENCRYPTION PROFILES'. The 'ENCRYPTION POLICY - TUNNELS' tab is selected. Below it, there are two main sections: 'SITE TO SITE (GATEWAY-GATEWAY)' and 'MOBILE - MOBILE USERS'. The 'SITE TO SITE (GATEWAY-GATEWAY)' section is active. It features a search bar, a list of IPsec policies, and a table of tunnels. The 'IPsec 01 (01)' policy is selected, and its dropdown menu is open, showing a list of policies from (1) to (10). The 'Actions' menu is also open, showing 'Edit', 'Reset', and 'Copy to' options. The 'Standard site-to-site tunnel' option is highlighted in the list.


- l'assistant de création du tunnel VPN IPsec permet de renseigner les principaux paramètres :
- les extrémités de trafic (objet réseaux local et objet réseau distant)
- l'extrémité de tunnel distante (le correspondant).

**ASSISTANT DE POLITIQUE VPN IPSEC**



Réseau local :  
 

Choix du correspondant :  
 

Réseau distant :  
 

1

Créer un correspondant IKEv1

Créer un correspondant IKEv2

2


3


Annuler Précédent Terminer

Si le correspondant n'existe pas, il faut le créer en cliquant sur le lien **Créer un correspondant IKEv2** qui sera utilisé pour la négociation du tunnel.

**ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2**

SÉLECTION DE LA PASSERELLE - ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2



Passerelle distante :  
 

Nom :

Annuler Précédent Suivant

- L'assistant de création du correspondant permet de renseigner les paramètres du correspondant :
  - la passerelle distante en renseignant l'objet machine qui porte l'adresse IP du correspondant.

- la clé partagée (PSK)

ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2

IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2

☐ Certificat

☒ Clé prépartagée (PSK)

Certificat :

Autorité de confiance (optionnel) :

Clé prépartagée (ASCII) :

Confirmer :

☒ Saisir la clé en caractères ASCII

- La dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours.
  - Cliquez sur **Terminer**, on retourne sur l'assistant de création du tunnel VPN.

## ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2



## RÉSUMÉ - ASSISTANT DE CRÉATION D'UN CORRESPONDANT IKEV2

## Paramètres du site distant :

Nom : Site\_Fw\_B

Passerelle distante : Fw\_B

## Identification du correspondant : clé prépartagée

Clé prépartagée : 4d6f7444655061737365536563726574

Annuler

« Précédent

✓ Terminer

- Sur la page de l'assistant de création du tunnel VPN, cliquez sur **Terminer**.

Le tunnel VPN IPsec est ajouté sur une ligne distincte de la politique.

[Un résumé détaillé des paramètres de configuration peut être affiché en cliquant sur le pictogramme représentant un oeil.](#)

STORMSHIELD  
Network Security v4.0.1

MONITORING CONFIGURATION EVA1 SNS\_EVA1\_V4\_A

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

OBJETS

UTILISATEURS

POLITIQUE DE SÉCURITÉ

PROTECTION APPLICATIVE

VPN

VPN IPsec

VPN SSL Portail

VPN SSL

Serveur PPTP

NOTIFICATIONS

OBJETS

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

(1) IPsec 01 Activer cette politique Editer

SITE À SITE (GATEWAY-GATEWAY) ANONYME - UTILISATEURS NOMADES

Texte recherché Ajouter Supprimer Monter Descendre Couper Copier Coller

| Ligne | Etat | Réseau local | Correspondant | Réseau distant | Profil de chiffrement | Keepalive |
|-------|------|--------------|---------------|----------------|-----------------------|-----------|
| 1     | on   | Network_in   | Site_Fw_B     | Lan_in_B       | StrongEncryption      | 0         |

Résumé de la ligne 1 de la politique de chiffrement 1

Version d'IKE : 2  
Correspondants :  
Local : Tous (Any)  
Distant : Machine : 192.36.253.20 (Fw\_B)  
Trafic chiffré :  
Local : Réseau : 192.168.1.0 / 255.255.255.0 (Network\_in)  
Distant : Réseau : 192.168.2.0 / 255.255.255.0 (Lan\_in\_B)  
Paramètres d'authentification :  
Mode :  
Type : psk  
Local ID :  
ID du correspondant :  
Clé prépartagée : 4d6f7444655061737365536563726574  
Profil de chiffrement IKE (Phase 1) :  
Diffie-Hellman : DH14 MODP Group (2048-bits)  
Durée de vie : 21600  
Propositions : sha2\_256/256,aes/256 - sha2\_256/256,aes/128  
Profil de chiffrement IPsec (Phase 2) :  
Perfect Forward Secrecy (PFS) : DH14 MODP Group (2048-bits)  
Durée de vie : 3600  
Authentification : hmac\_sha256/256  
Chiffrement : aes/256, aes/128

Annuler Enregistrer

From:  
/ - Les cours du BTS SIO

Permanent link:  
</doku.php/activiteipsec?rev=1638738710>

Last update: 2021/12/05 22:11

