

# 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 'VPN / IPSEC VPN' configuration page. In the 'ENCRYPTION POLICY - TUNNELS' section, a new tunnel named 'IPsec 01 (01)' is selected. An 'Actions' dropdown menu is open over the tunnel entry, showing options: 'Edit', 'Reset', and 'Copy to'. Below the dropdown, the 'SITE TO SITE (GATEWAY-GATEWAY)' table lists the newly created tunnel. The table has columns for 'Status', 'Name', 'Peer', 'Remote network', and 'Encryption profile'. The first row, 'Standard site-to-site tunnel', is highlighted. The bottom left sidebar lists numbered tunnels from 1 to 10.

	Status	Peer	Remote network	Encryption profile
(1) IPsec 01	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 01
(2) IPsec 02	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 02
(3) IPsec 03	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 03
(4) IPsec 04	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 04
(5) IPsec 05	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 05
(6) IPsec 06	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 06
(7) IPsec 07	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 07
(8) IPsec 08	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 08
(9) IPsec 09	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 09
(10) IPsec 10	Up	Standard site-to-site tunnel	192.168.1.10/24	IPsec 10

- 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 : Network\_in

Choix du correspondant : None

Réseau distant : Lan\_in\_B

**Créer un correspondant IKEv1**

**Créer un correspondant IKEv2**

**1**      **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**

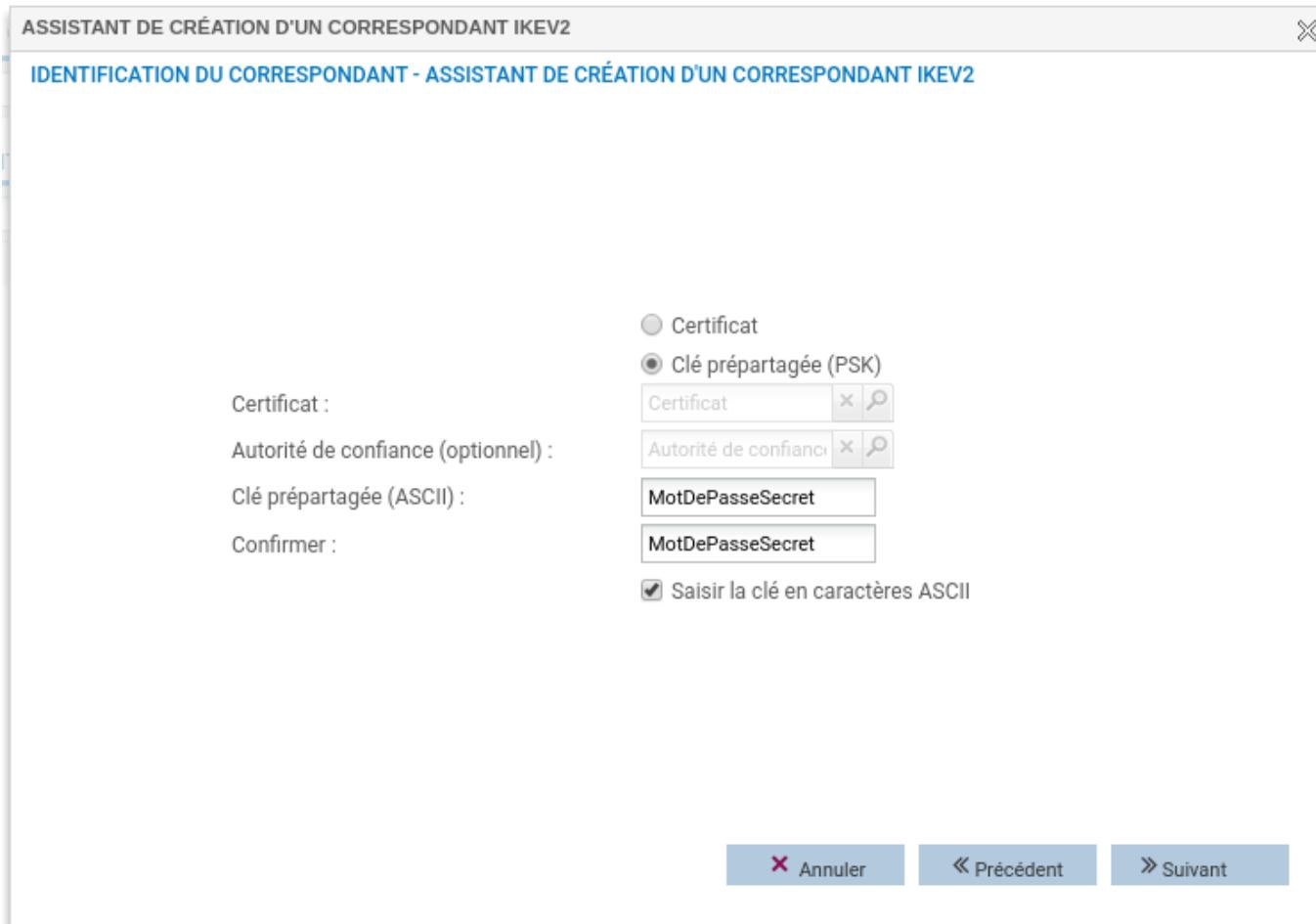
Passerelle distante : Fw\_B

Nom : Site\_Fw\_B

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)



- 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 X

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.

The screenshot shows the STORMSHIELD Network Security v4.0.1 web interface. The left sidebar is titled "CONFIGURATION" and includes sections for SYSTEME, RESEAU, OBJETS, UTILISATEURS, POLITIQUE DE SECURITE, PROTECTION APPLICATIVE, VPN, and VPN IPsec (which is selected). Below these are NOTIFICATIONS and OBJETS.

The main content area has tabs for MONITORING and CONFIGURATION, with "CONFIGURATION" selected. It displays the "VPN / VPN IPSEC" section. A sub-tab "POLITIQUE DE CHIFFREMENT - TUNNELS" is active, showing a table with one row labeled "(1) IPsec 01". The table columns are Ligne, Etat, Réseau local, Correspondant, Réseau distant, Profil de chiffrement, and Keepalive. The first row has "on" in the Etat column and "Network\_in" in the Réseau local column. An eye icon in the Etat column is highlighted with a red box.

A detailed modal window is open for "Résumé de la ligne 1 de la politique de chiffrement 1". It contains the following information:

- Version d'IKE :** 2
- Correspondants :**
  - Local : Tous (Any)
  - Distant : Machine : 192.36.253.20 (Fw\_B)
- Traffic 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 : psk
  - Type : psk
  - Local ID :
  - ID du correspondant :
  - Cle 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

At the bottom right of the modal are "Annuler" and "Enregistrer" buttons.

## Profils de chiffrement

- Le profil de chiffrement phase 1 appelé également profil IKE est configuré au niveau du correspondant.
- Le profil de chiffrement phase 2, appelé profil IPSEC est configuré au niveau du tunnel VPN.

**Profil phase 1 (IKE)**  
**Profil phase 2 (IPSEC)**

Pour les deux phases, il existe trois profils préconfigurés :

- StrongEncryption,
- GoodEncryption
- Mobile.

L'onglet **PROFILS DE CHIFFREMENT** du menu **VPN** → **VPN IPsec** permet de :

- Consulter et de modifier la configuration des profils préconfigurés,
- Définir les profils qui seront utilisés par défaut lors de l'ajout des tunnels,
- Créer de nouveaux profils phase 1 et phase 2 personnalisés.

Algorithm	Strength	Algorithm	Strength
aes	256	sha2_256	256
aes	128	sha2_256	256

**Phase 1 (IKE) profile**  
**Phase 2 (IPSec) profile**  
**Copy the selection**

#### A faire :

Configurez le tunnel VPN IPsec avec ces profils de chiffrement par défaut en configurant le SNS de l'autre extrémité du tunnel

## Fonction Keepalive

La fonction Keepalive permet de maintenir le tunnel disponible en envoyant un paquet UDP à destination du réseau distant sur le port numéro 9, avec une certaine fréquence.

Cela provoque la négociation initiale du tunnel, puis ses renégociations périodiques.

Elle permet de configurer la fréquence en secondes avec laquelle les paquets UDP sont envoyés.

## Règles du pare-feu

Lors de la création du tunnel VPN IPsec site-à-site, des règles implicites sont ajoutées automatiquement pour autoriser la réception du trafic constituant un tunnel VPN IPsec : les ports UDP/500, UDP/4500 et le protocole ESP.

Ces règles ne concernent que les flux entrants car les flux sortants sont déjà couverts par les règles flux implicites du firewall.

 SECURITY POLICY / IMPLICIT RULES

IMPLICIT FILTER RULES

Enabled	Name
<input checked="" type="checkbox"/>	Enabled Allow access to the PPTP server
<input checked="" type="checkbox"/>	Enabled Allow mutual access between the members of a firewall cluster (HA)
<input checked="" type="checkbox"/>	Enabled Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers.
<input checked="" type="checkbox"/>	Enabled Allow protected interfaces to access the firewall's DNS service (port 53).

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/activiteipsec?rev=1638739826>

Last update: **2021/12/05 22:30**

