

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 'Encryption Policy - Tunnels' section of the SNS interface. A new tunnel named 'IPsec 01 (01)' has been 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 includes columns for Status, Identifier, Remote network, and Encryption profile. The identifier 'Standard site-to-site tunnel' is highlighted. The left sidebar lists other tunnels numbered 2 through 10.

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

- 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

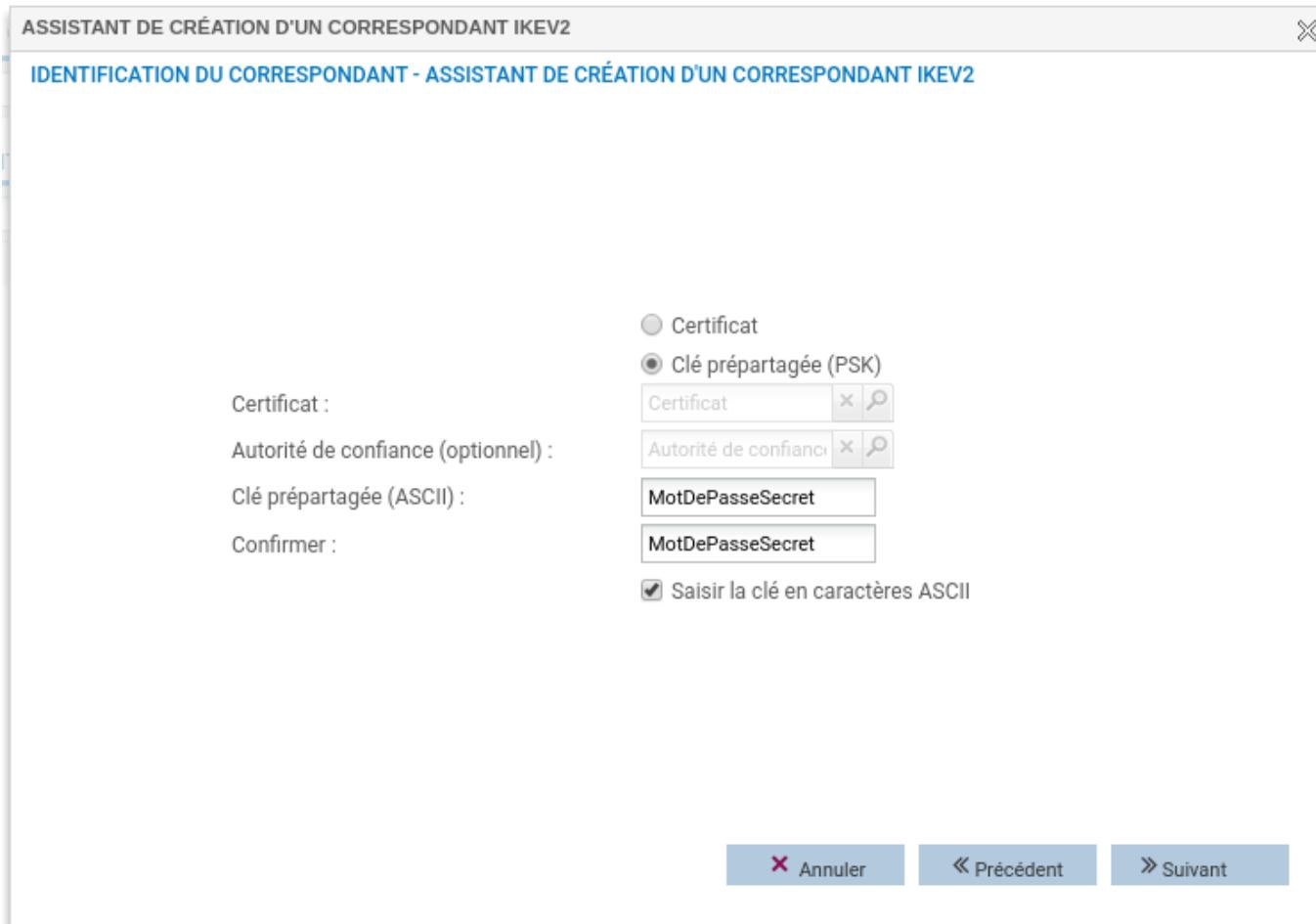
Passerelle distante : Fw_B

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). The main content area is titled 'VPN / VPN IPSEC' and shows the 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab. A table lists one policy: '(1) IPsec 01'. A detailed view of this policy is shown in a modal window. The modal window contains sections for 'Résumé de la ligne 1 de la politique de chiffrement 1', 'Paramètres d'authentification', and 'Profil de chiffrement IKE (Phase 1)'. At the bottom right of the modal is a red box around the 'Enregistrer' button.

- Cliquez sur **Enregistrer** pour créer le tunnel VPN et activer la politique.

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.

The screenshot shows two windows side-by-side. The top window is titled 'VPN / IPSEC VPN' and displays the 'PEERS' tab. It shows a list of peers under 'Remote gateways (1)' with 'Site_Fw_B' selected. The 'General' section shows 'IKE profile: StrongEncryption' highlighted with a blue arrow. The bottom window is also titled 'VPN / IPSEC VPN' and displays the 'ENCRIPTION POLICY - TUNNELS' tab. It shows a table with one row for 'IPsec 01 (01)'. The 'Encryption profile' column for this row is also highlighted with a blue arrow. Both windows have blue arrows pointing from their respective highlighted areas to the text 'Profil phase 1 (IKE)' and 'Profil phase 2 (IPSEC)' located on the right side of the screen.

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,
- Crée de nouveaux profils phase 1 et phase 2 personnalisés.

Type	Name
IKE	StrongEncryption
IKE	GoodEncryption
IKE	IKE_CUSTOM1
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IPSEC	IPSEC_CUSTOM_1

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=1638740076](https://doku.php/activiteipsec?rev=1638740076)

Last update: **2021/12/05 22:34**

