

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 .

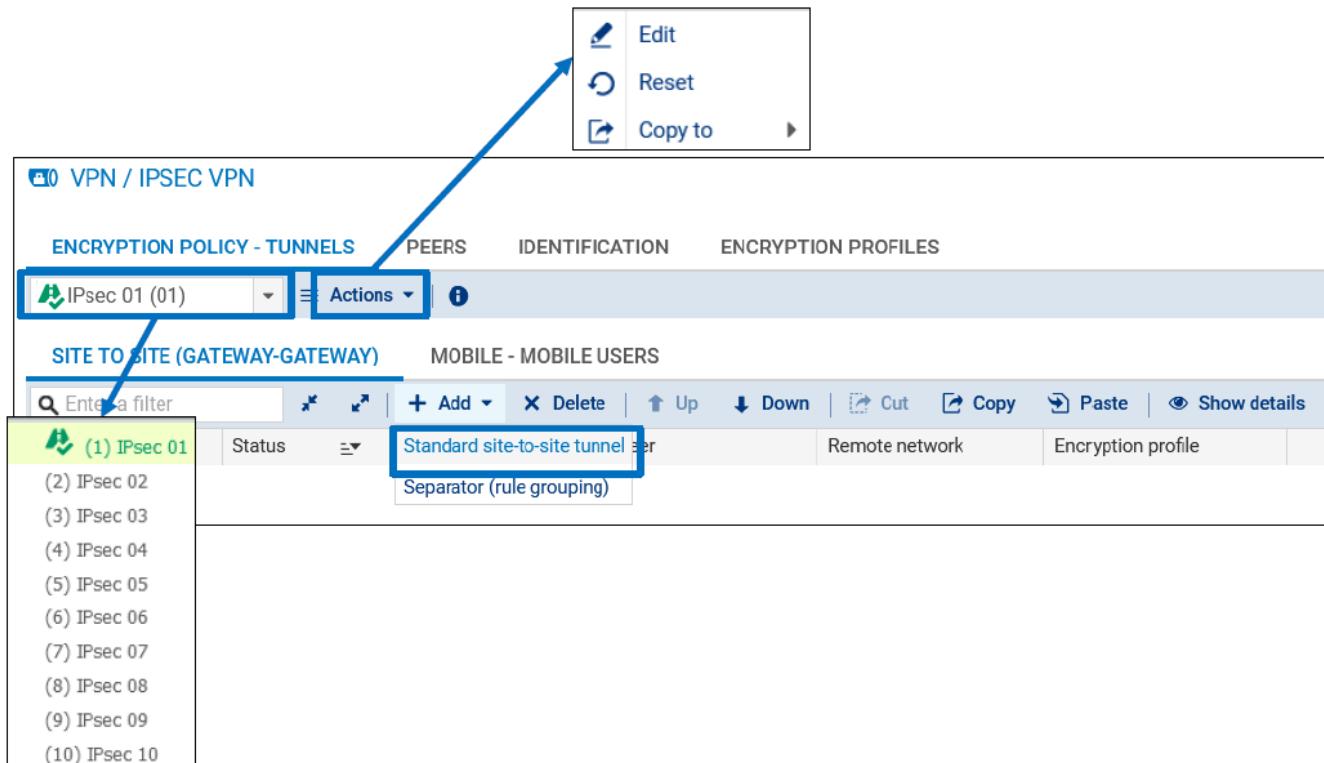
La suite de ce document est réalisé dans l'environnement mis en place avec VirtualBox.

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. The 'ENCRYPTION POLICY - TUNNELS' tab is selected. A list of tunnels is shown, with '(1) IPsec 01' highlighted. An 'Actions' dropdown menu is open over this tunnel, showing options: 'Edit', 'Reset', and 'Copy to'. Below the list, a table shows tunnel details: 'Standard site-to-site tunnel' for 'IPsec 01', 'Peer' as 'Separator (rule grouping)', and columns for 'Status', 'Remote network', and 'Encryption profile'. A sidebar on the left lists numbered tunnels from 1 to 10. A blue arrow points from the 'Actions' menu to the 'Edit' option.

- 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

1 2 3

[Créer un correspondant IKEv1](#)

[Créer un correspondant IKEv2](#)

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



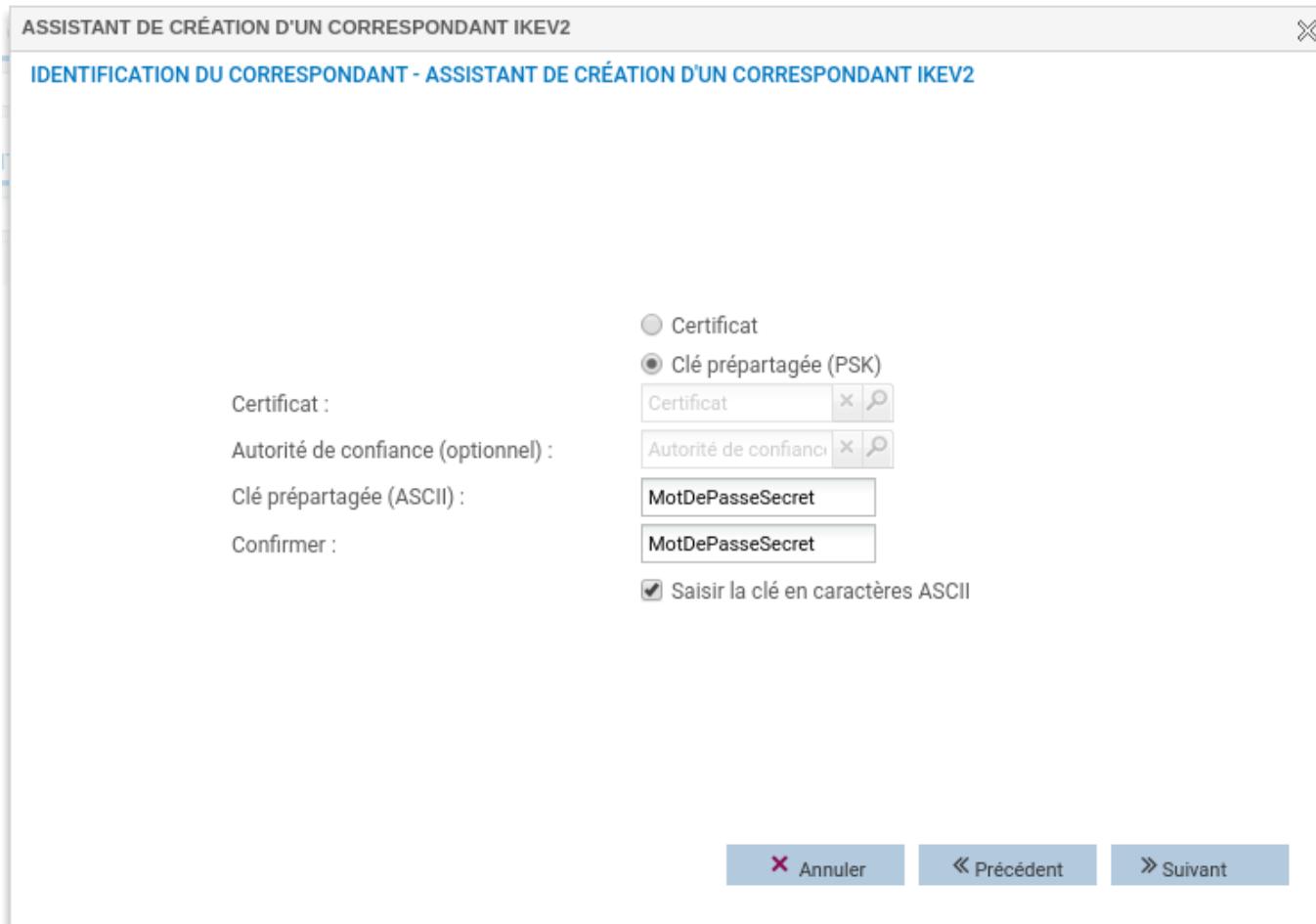
Passerelle distante : Fw_B

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.

- o la clé partagée (PSK)



- La dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours.
 - o 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

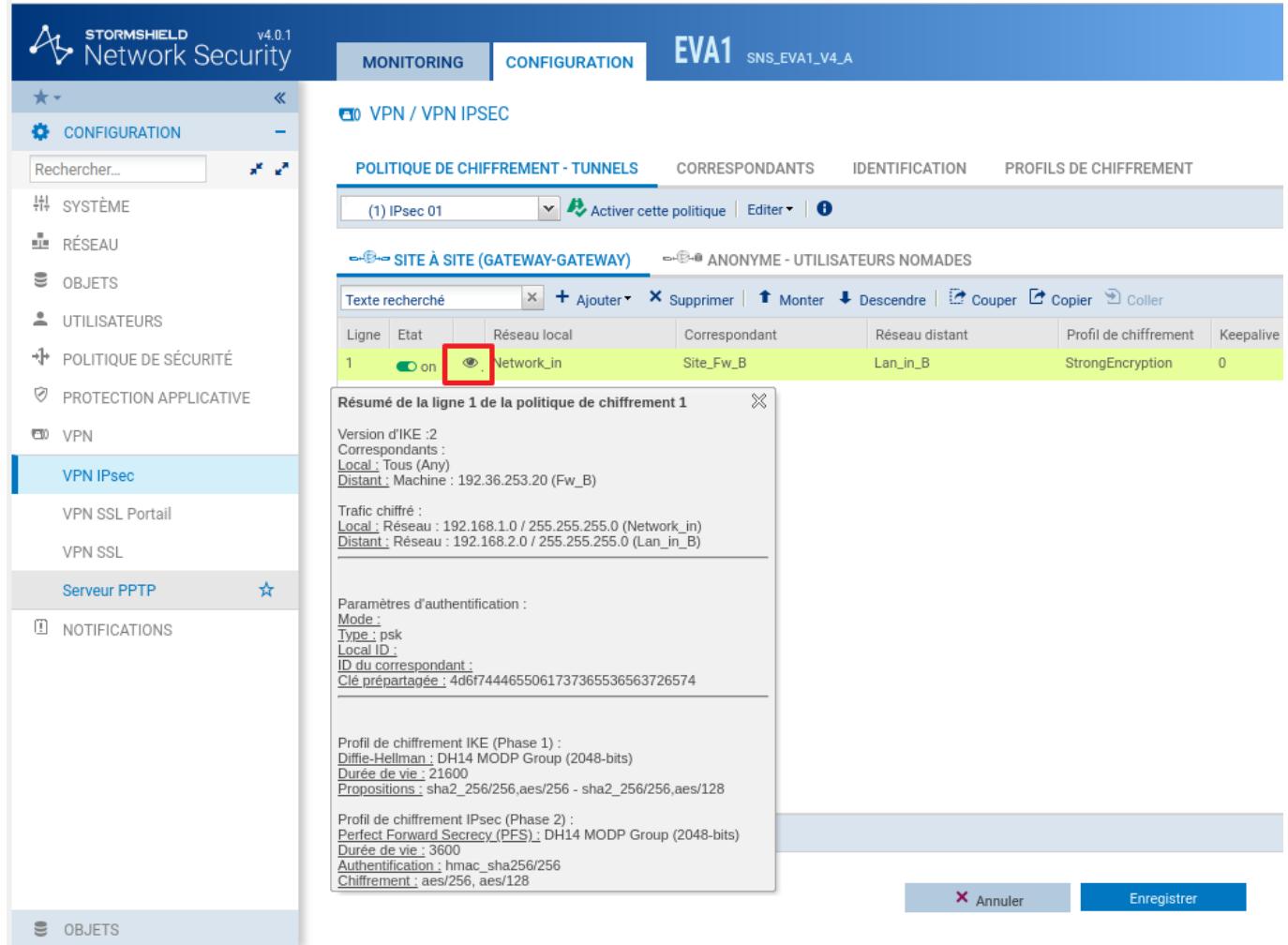
Clé prépartagée : 4d6f7444655061737365536563726574

X 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

VPN / VPN IPsec

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

(1) IPsec 01 Activer cette politique | Editer | *Info*

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)

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 :
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

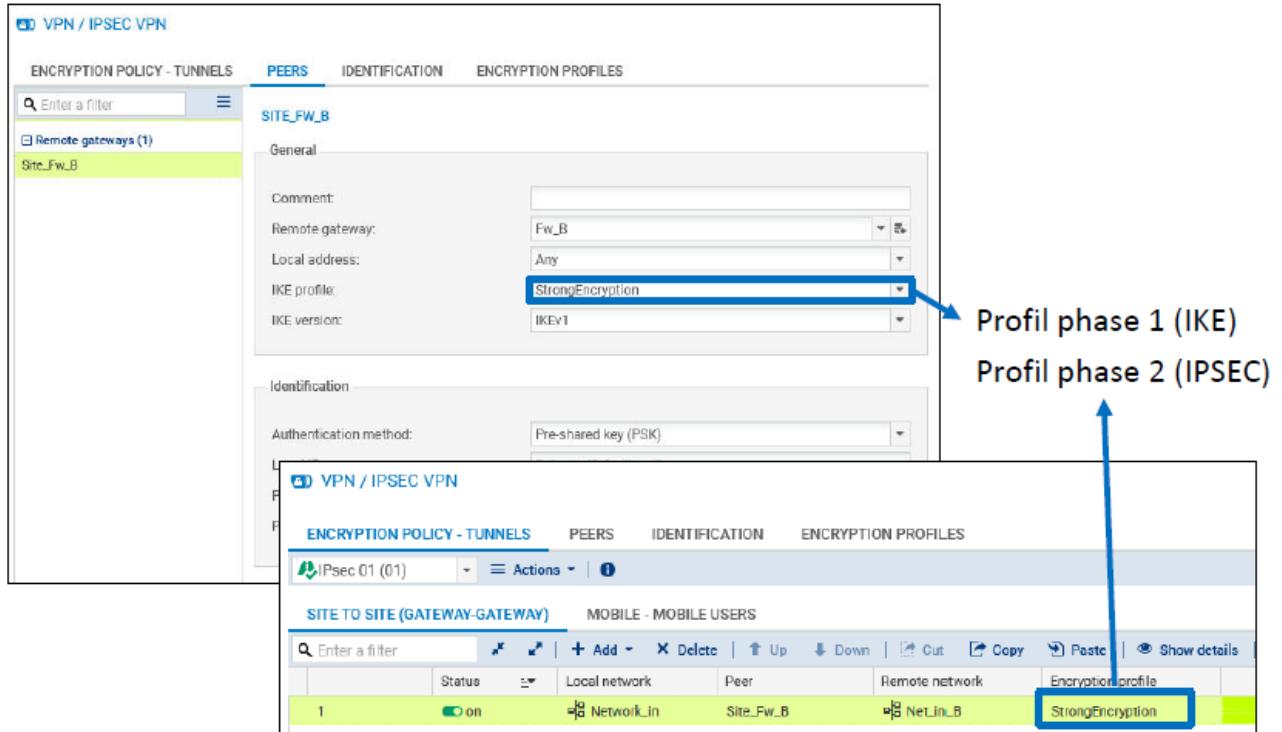
Profil de chiffrement IPsec (Phase 2) :
Perfect Forward Secrecy (PFS) : DH14 MODP Group (2048-bits)
Durée de vie : 3600
Authentification : hmac_sha256/256
Chiffrement : aes/256, aes/128

Annuler Enregistrer

- 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.



VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

Enter a filter SITE_FW_B

General

Comment :

Remote gateway : Fw_B

Local address : Any

IKE profile : StrongEncryption

IKE version : IKEv1

Identification

Authentication method : Pre-shared key (PSK)

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

IPsec 01 (01) Actions | *Info*

SITE TO SITE (GATEWAY-GATEWAY) MOBILE - MOBILE USERS

Enter a filter

| | Status | Local network | Peer | Remote network | Encryption profile |
|---|--------|---------------|-----------|----------------|--------------------|
| 1 | on | Network_in | Site_Fw_B | NetIn_B | StrongEncryption |

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

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 implicites

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). |

Règles du pare-feu explicites

Le trafic autorisé entre les usagers du tunnel doit être explicitement défini par des règles de filtrage :

- La première règle permet l'initiation de connexions à partir du réseau local Networkin et à destination du réseau distant LANINB. *
- La deuxième règle permet, quant à elle, l'initiation de connexions à partir du réseau distant LANINB à destination du réseau local Networkin. La directive via Tunnel VPN IPSec a été ajoutée à la source de cette règle pour s'assurer que le trafic du réseau distant provient bien du tunnel VPN IPSec.

NOTE : ces règles sont très permissives puisqu'elles ne spécifient pas de flux particuliers. En situation réelle, il convient de définir une politique de filtrage qui décrit strictement les flux à autoriser afin de couvrir rigoureusement les communications nécessaires entre les différentes machines des deux sites.

SECURITY POLICY / FILTER - NAT

FILTERING **NAT**

| Searching... | Status | Action | Source | Destination | Dest. port | Protocol | Security inspection |
|--------------|--|--|--|--|------------|----------|---------------------|
| 1 | <input checked="" type="checkbox"/> on | <input checked="" type="checkbox"/> pass | <input checked="" type="checkbox"/> Network_in | <input checked="" type="checkbox"/> NET_IN_B | * Any | | IPS |
| 2 | <input checked="" type="checkbox"/> on | <input checked="" type="checkbox"/> pass | <input checked="" type="checkbox"/> NET_IN_B via IPSec VPN tunnel | <input checked="" type="checkbox"/> Network_in | * Any | | IPS |

EDITING RULE NO 2

SOURCE

GENERAL **GEOLOCATION / REPUTATION** **ADVANCED PROPERTIES**

Advanced properties

Source port: Any

Via: IPSec VPN tunnel

Les logs de la négociation IKE

Le menu LOGS ⇒ VPN affiche les événements relatifs au déroulement de la négociation IKE.

Les extrémités de trafic qui ont provoqué les négociations et pour lesquelles le tunnel est disponible apparaissent explicitement sur la ligne de log concernant la négociation de phase 2.

Dans le cadre d'un diagnostic, en particulier en cas de message d'erreur ou d'avertissement, il est essentiel de relever la phase de négociation pour laquelle les messages sont rapportés.

Davantage d'informations, plus techniques, peuvent être affichées en cliquant sur la flèche qui se trouve dans l'en-tête de colonnes, puis sélectionnant les colonnes supplémentaires souhaitées.

LOG / VPN

| Dernière heure | Actualiser | Rechercher... | Recherche avancée | | |
|---|------------------------|---------------|-------------------|----------------|--------------------|
| RECHERCHE DU - 05/12/2021 21:45:14 - AU - 05/12/2021 22:45:14 | | | | | |
| Enregistré à | Message | Utilisateur | Nom de la source | Réseau local | Nom de destination |
| 22:42:08 | IPSEC SA established | | Anonymized | 192.168.1.0/24 | Fw_B |
| 22:42:08 | IKE SA established | | Anonymized | | Fw_B |
| 22:31:39 | Charon configuratio... | | | | |
| 22:31:39 | Reloading charon co... | | | | |
| 22:31:39 | Charon daemon star... | | | | |

Supervision des tunnels VPN IPsec

Le menu **Supervision** ⇒ **Tunnels VPN IPsec** permet de visualiser la politique VPN IPsec active sur le firewall.

Lorsque l'option **Masquer les tunnels établis pour afficher uniquement les politiques présentant des problèmes** est cochée, seules les politiques qui n'ont pas de tunnels négociés s'affichent.

| MONITOR / IPSEC VPN TUNNELS | | | | | | | | |
|---|--------------------|--------------------|---|---------------------|---------------------|------------|----|--|
| Configure the IPsec VPN service | | | | | | | | |
| Policies | | | | | | | | |
| Filter: | Searching... | | | | | | | |
| <input type="checkbox"/> Hide established tunnels to display only policies with issues. | | | | | | | | |
| Status | Local network name | Local gateway name | Direction ↑ | Remote gateway name | Remote network name | Lifetime | ID | |
| Policy: none | rfc5735_loopback | | ↔ in | | any | | 0 | |
| Policy: none | rfc5735_loopback | | → out | | any | | 0 | |
| <input checked="" type="checkbox"/> 1 Tunnel(s) | Network_in | Firewall_out | ↔  in | FW_B | NET_IN_B | 40d 7h 34m | 1 | |
| <input checked="" type="checkbox"/> 1 Tunnel(s) | Network_in | Firewall_out | →  out | FW_B | NET_IN_B | 40d 7h 34m | 1 | |

En dessous, la section **Tunnels** permet de superviser les tunnels disponibles.

L'âge actuel des SA et les algorithmes retenus lors des négociations apparaissent.

La colonne **État** peut afficher trois valeurs :

- **Larval*** : le tunnel est en cours de négociation, * **Mature** : la négociation des SA de phase 2 a abouti et le tunnel est opérationnel, * **Dying** : les SA de phase 2 ont atteint 80 % de leurs durées de vie.

| Tunnels | | | | | | | | |
|--|---------------------|---------------|-----------|-----------|--------|------------|-----------------|--|
| <input type="checkbox"/> Display only tunnels matching the selected policy | | | | | | | | |
| Local gateway name | Remote gateway name | Lifetime | Bytes out | Bytes in | Status | Encryption | Authenticati... | |
| Firewall_out | FW_B | 4m of 1h used | 98.18 KB | 448.57 KB | mature | aes-cbc | hmac-sha512 | |

-  Search for this value in the "All logs" view
-  Check this host
-  Show host details
-  Blacklist this object
-  Copy the selected line to the clipboard
-  Add the host to the objects base and/or add it to a group

===== Activité complémentaire 1 ===== Créez les profils de chiffrement suivants : * IKE Phase 1 : Diffie-Hellman (DH15

MODP), Durée de vie maximum (21600s), algorithme d'authentification (sha2512) et algorithme de chiffrement (AES 256bits). *
IPSEC Phase 2 : PFS (DH15 MODP), durée de vie (3600s), algorithme d'authentification (hmacsha512) et algorithme de chiffrement (AES 256bits). Appliquez vos nouveaux profils de chiffrement sur votre VPN. Puis vérifiez que tout fonctionne correctement.
===== Activité complémentaire 2 ====== Configure un tunnel VPN IPsec avec des certificats de votre autorité de certification.
===== Activité complémentaire 3 ====== Créez les profils de chiffrement suivants : Réalisez l'interconnexion de ces mêmes réseaux, mais en configurant des tunnels basés sur des VTI avec au choix du routage statique ou par politique (PBR).
Documentation Stormshield sur les

tunnels VPN IPsec par VTI

. .

From:

[/ - Les cours du BTS SIO](#)

Permanent link:

[/doku.php/activiteipsec](#)

Last update: **2021/12/05 23:26**

