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 .

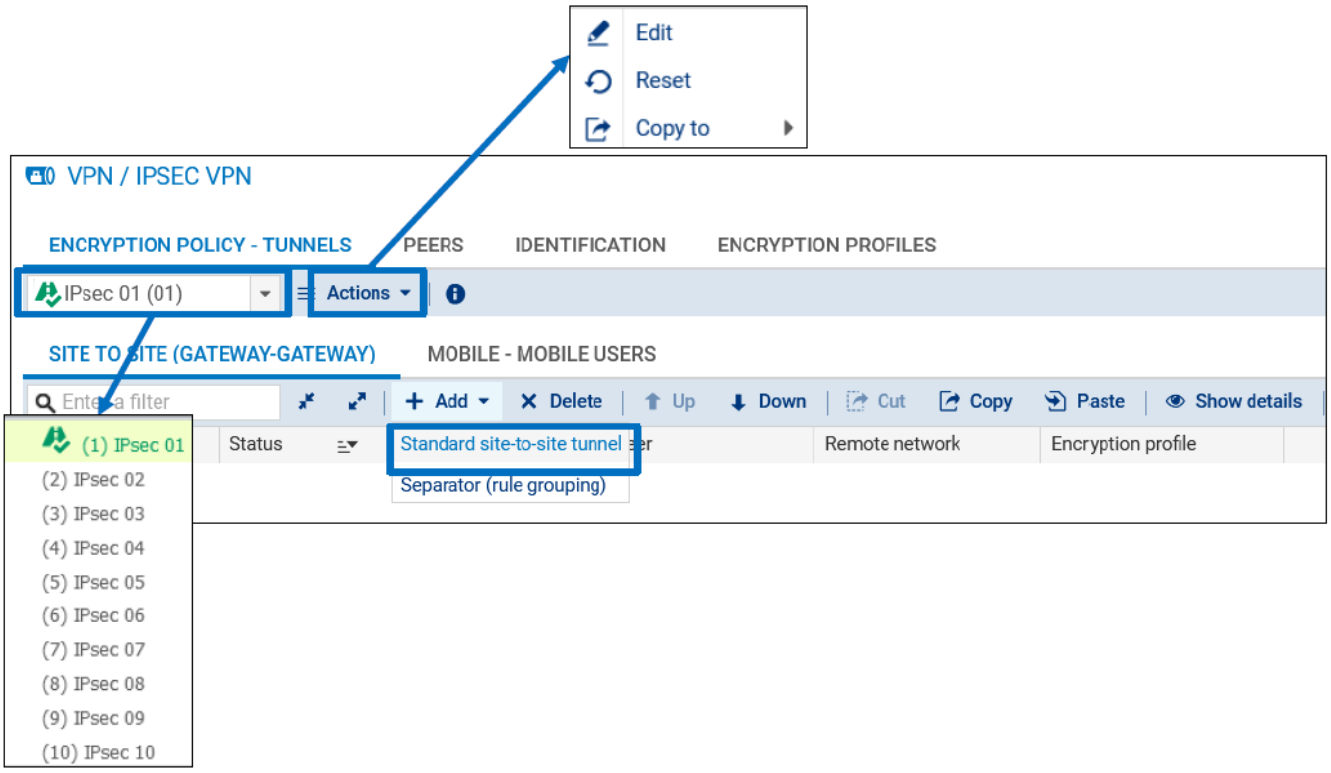
La suite de ce document est réalisé dans l'environnement mis en place avec VirtualBox.

Définir la politique de filtrage

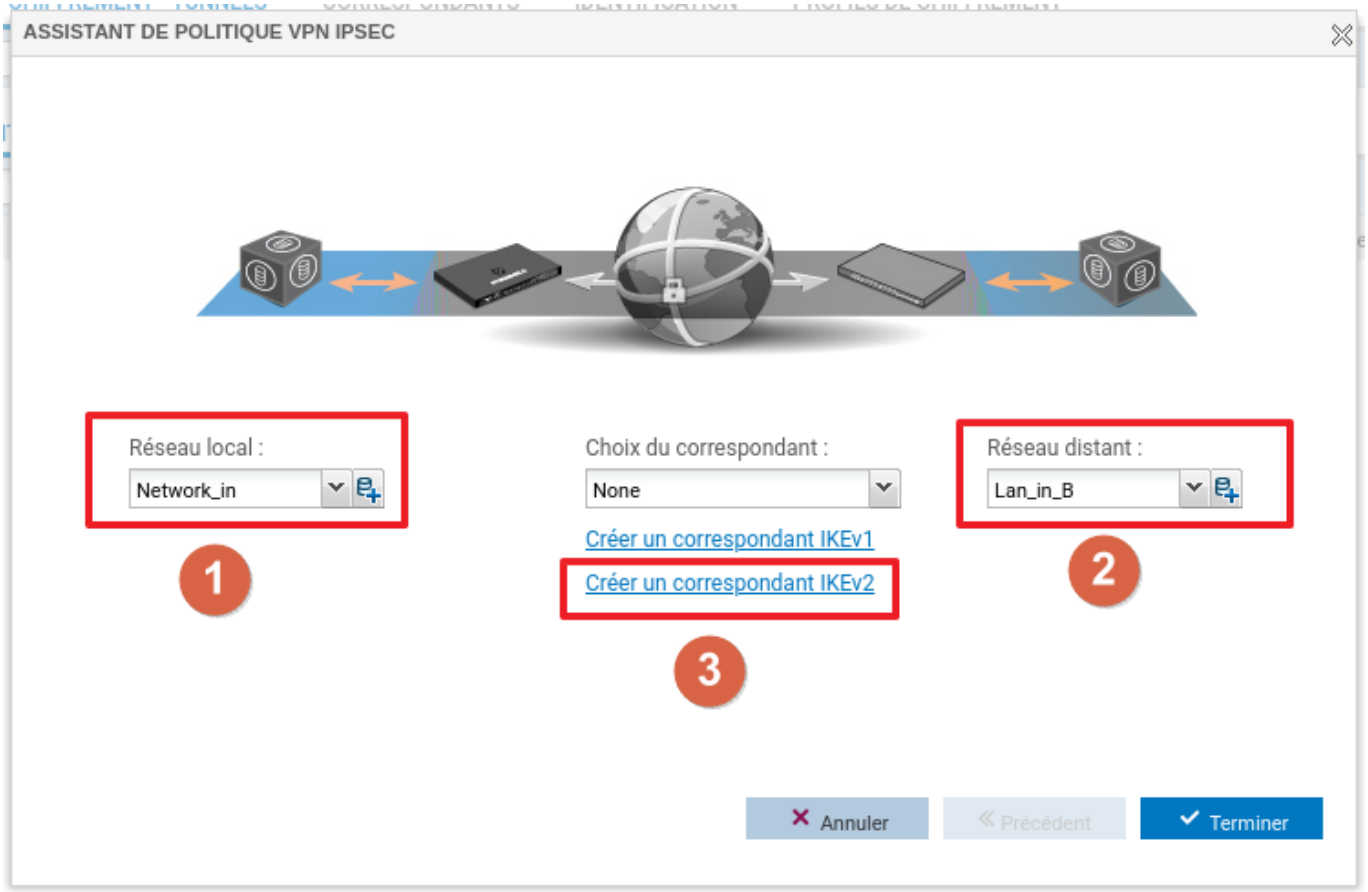
Réactiver la politique de filtrage **(10) Pass All**.

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

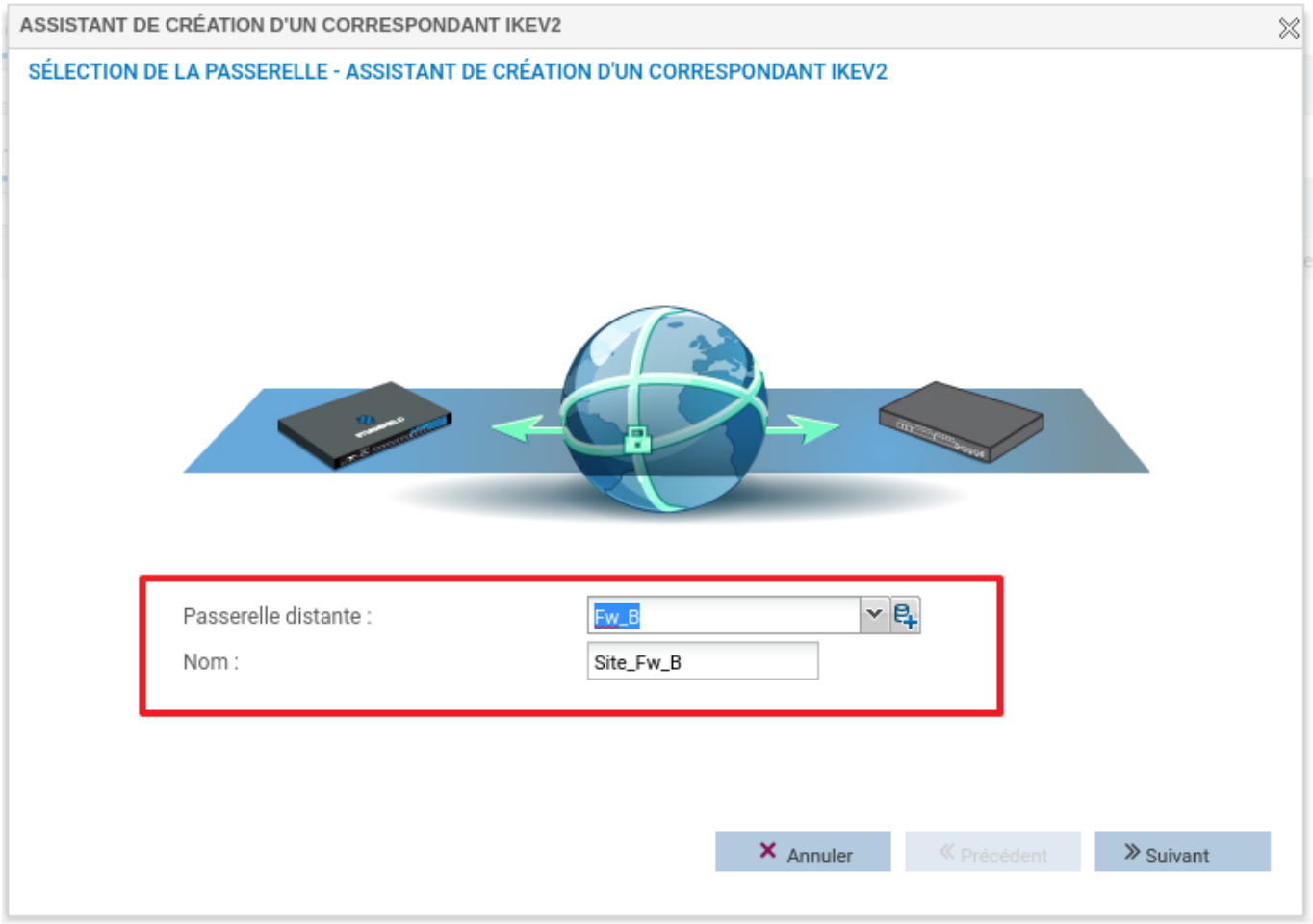
- Depuis l'interface d'administration du SNS de l'un des extrémités du tunnel , accédez au menu **VPN ⇒ VPN IPsec > onglet POLITIQUE DE CHIFFREMENT – TUNNELS** ;
- Dans la rubrique **SITE À SITE (GATEWAY – GATEWAY)**, cliquez sur **Ajouter ⇒ Tunnel site à site**.



- 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).

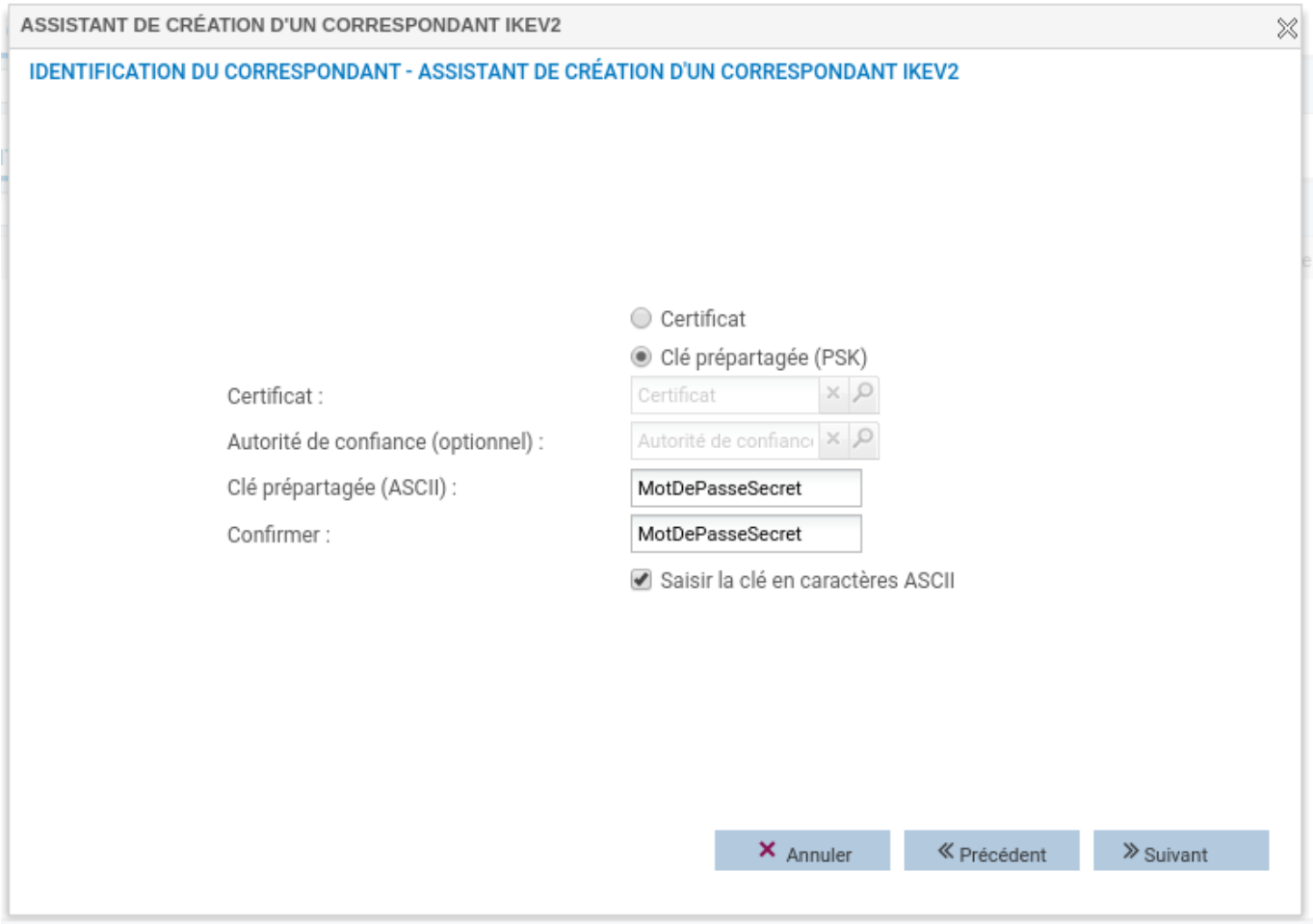


Si le correspondant n'existe pas, il faut le créer en cliquant sur le lien **Créer un correspondant IKEv2** qui sera utilisé pour la négociation du tunnel.

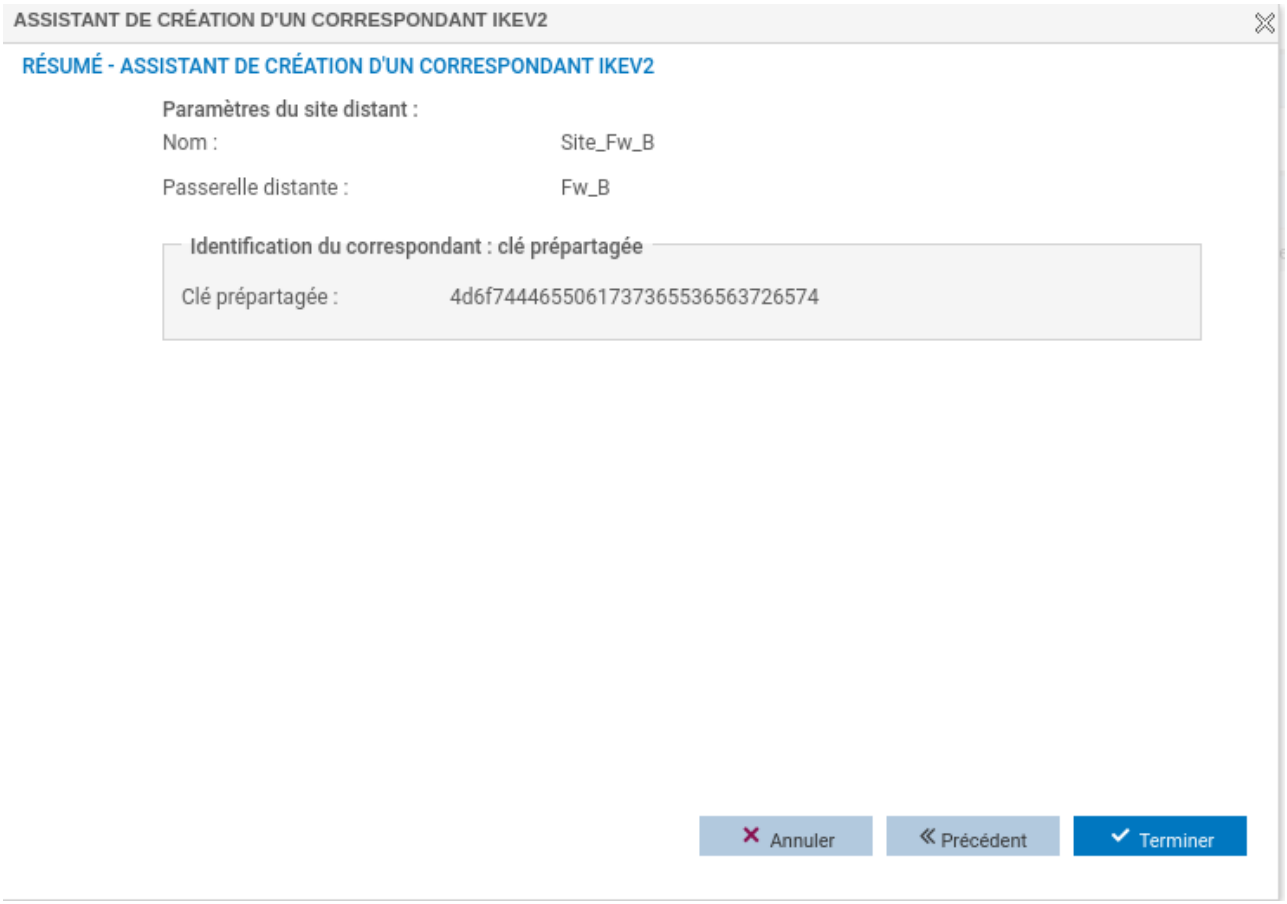


- L'assistant de création du correspondant permet de renseigner les paramètres du correspondant :
  - la passerelle distante en renseignant l'objet machine qui porte l'adresse IP du correspondant.

- la clé partagée (PSK)



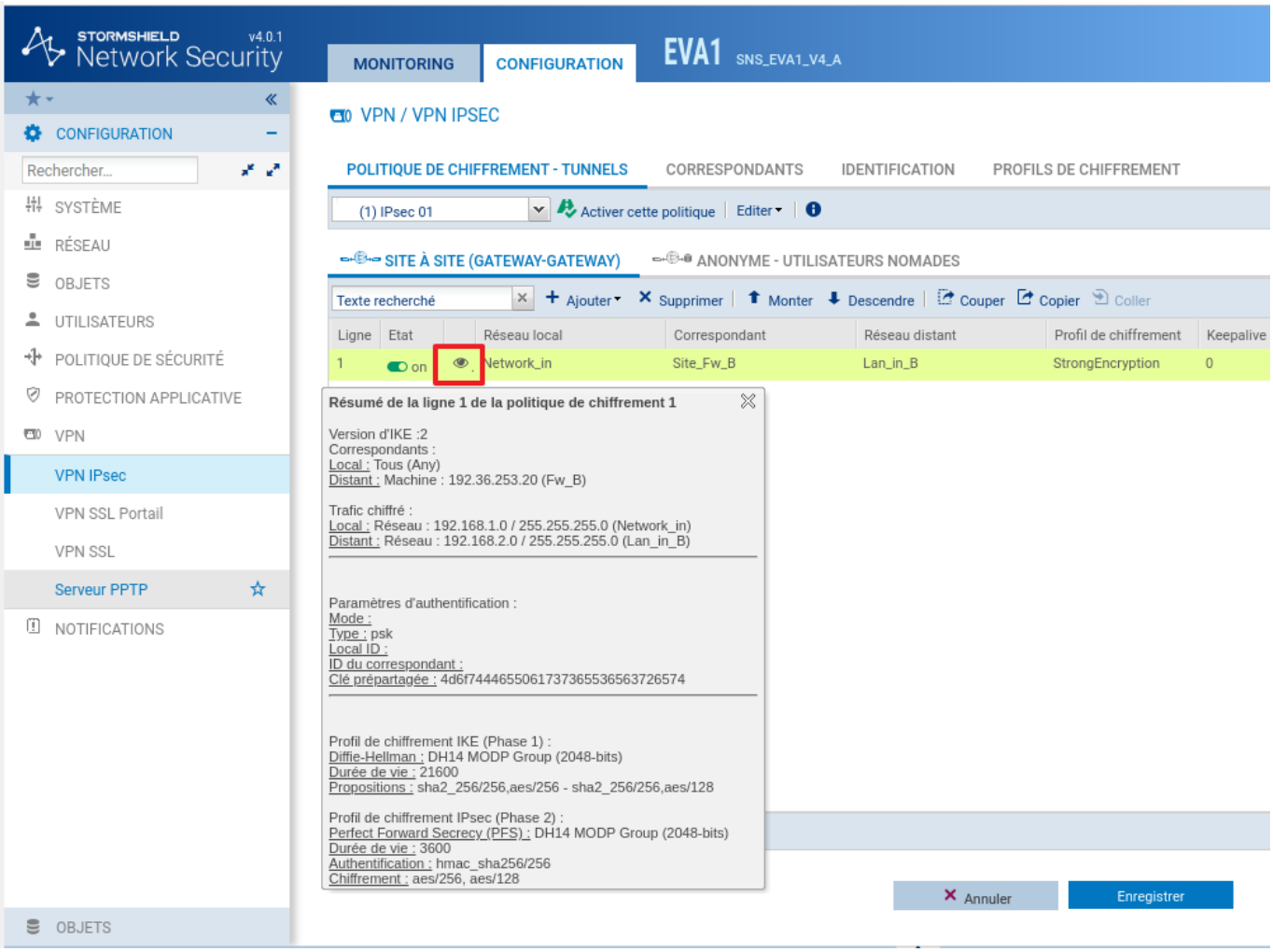
- La dernière étape liste les paramètres renseignés et permet éventuellement d'ajouter une passerelle de secours.
  - Cliquez sur **Terminer**, on retourne sur l'assistant de création du tunnel VPN.



- 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.

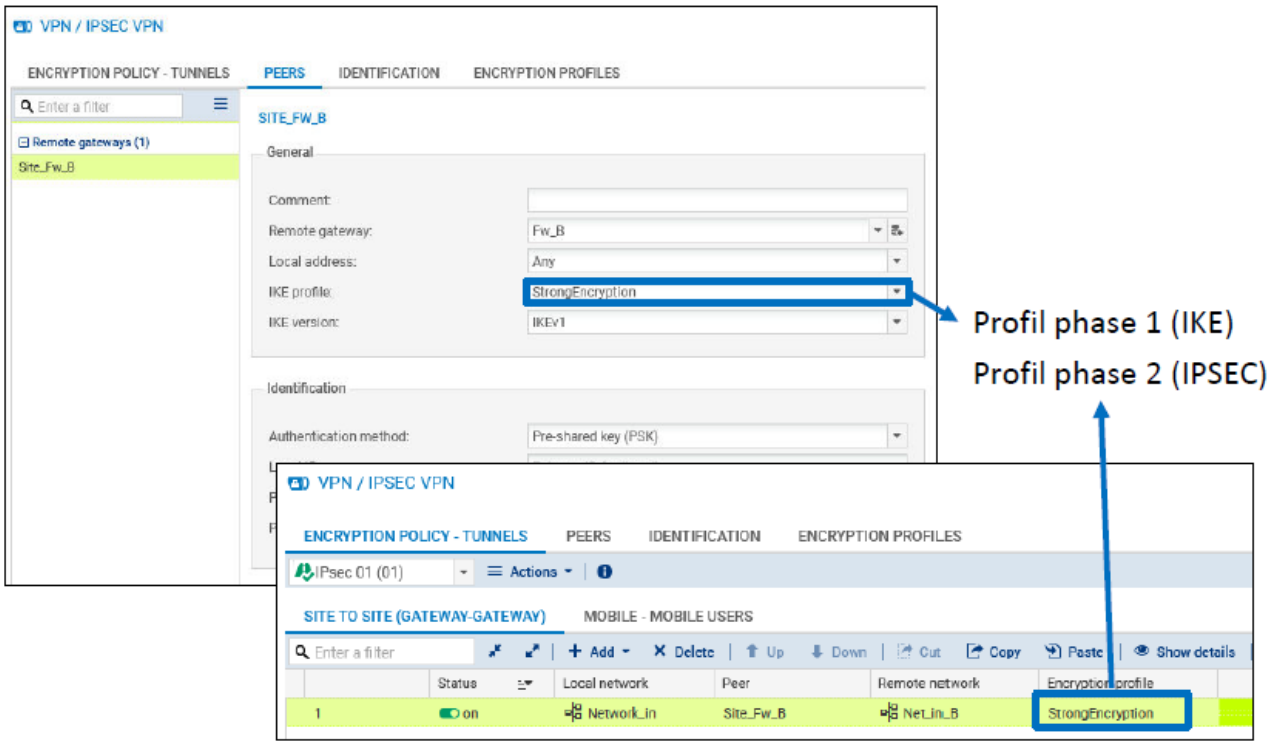
Un résumé détaillé des paramètres de configuration peut être affiché en cliquant sur le pictogramme représentant un oeil.



- 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.

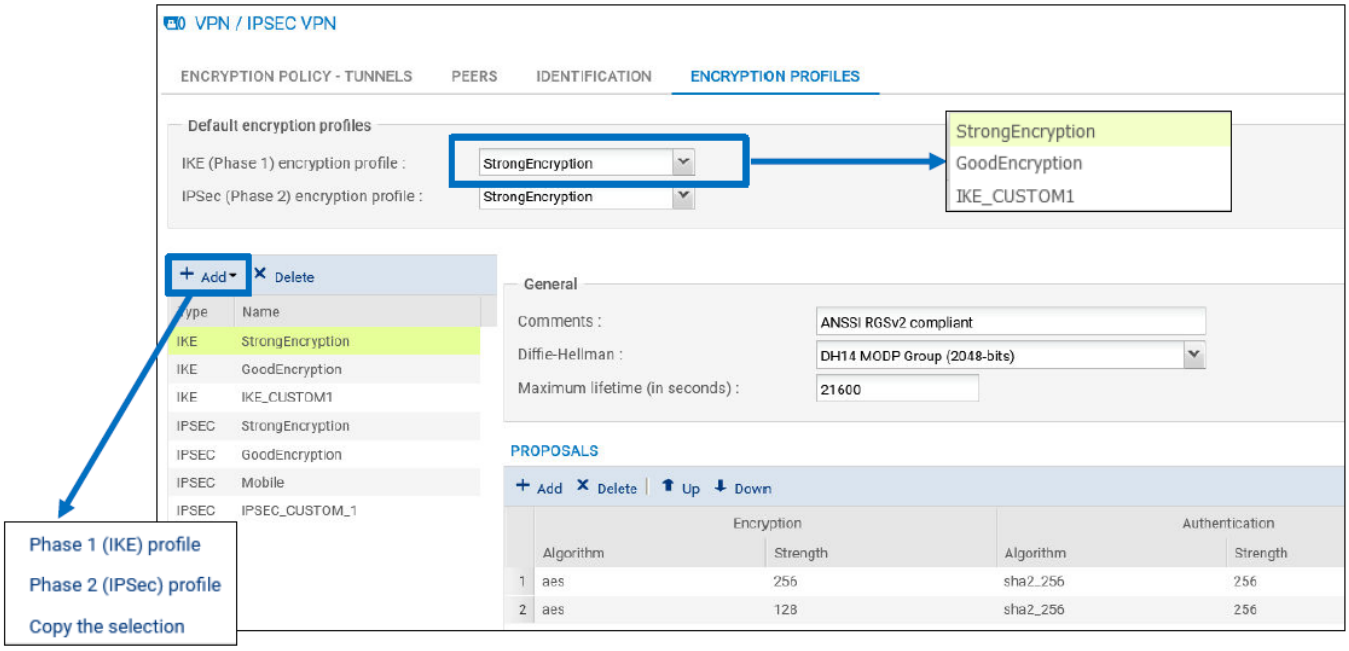


Pour les deux phases, il existe trois profils préconfigurés :

- 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.



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.

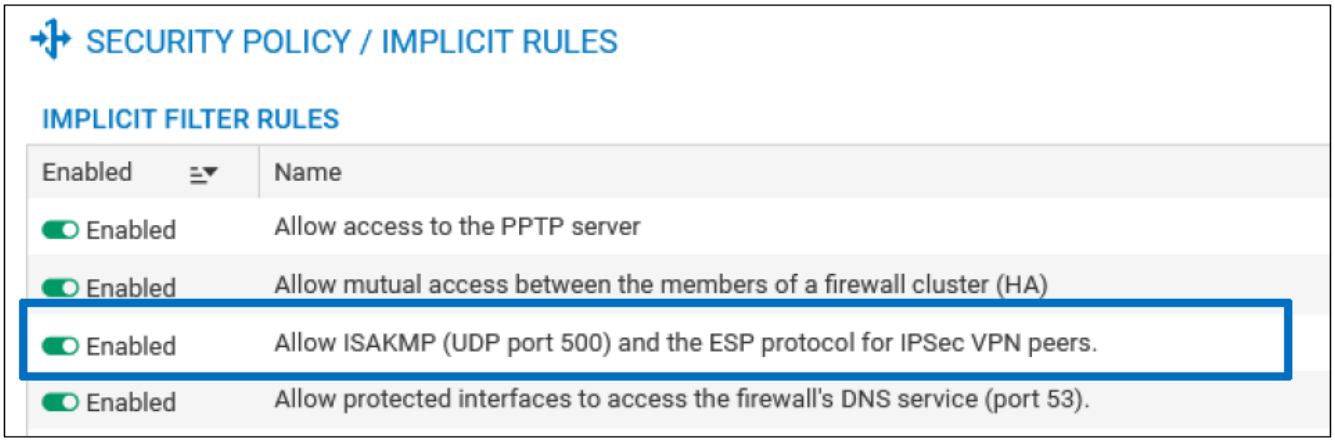
Cela provoque la négociation initiale du tunnel, puis ses renégociations périodiques.

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.

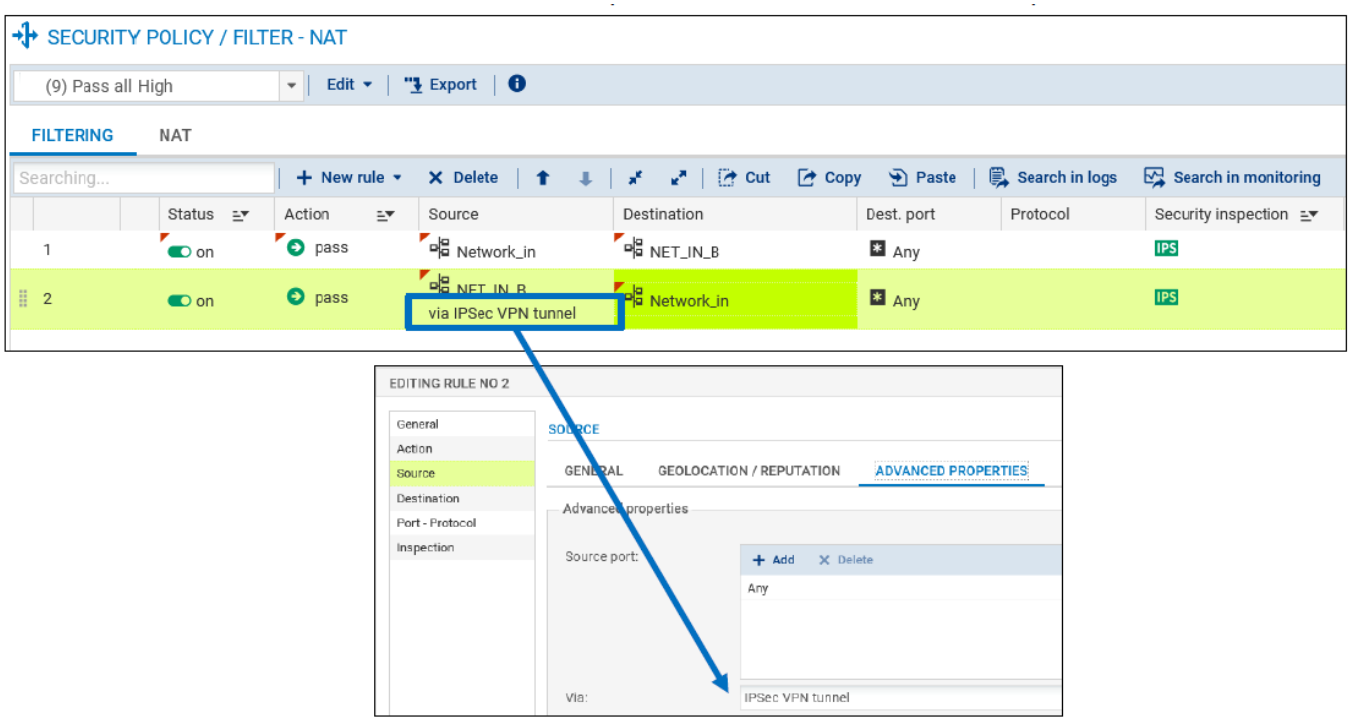


Règles du pare-feu explicites

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 Network*in 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 Network*in. 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.



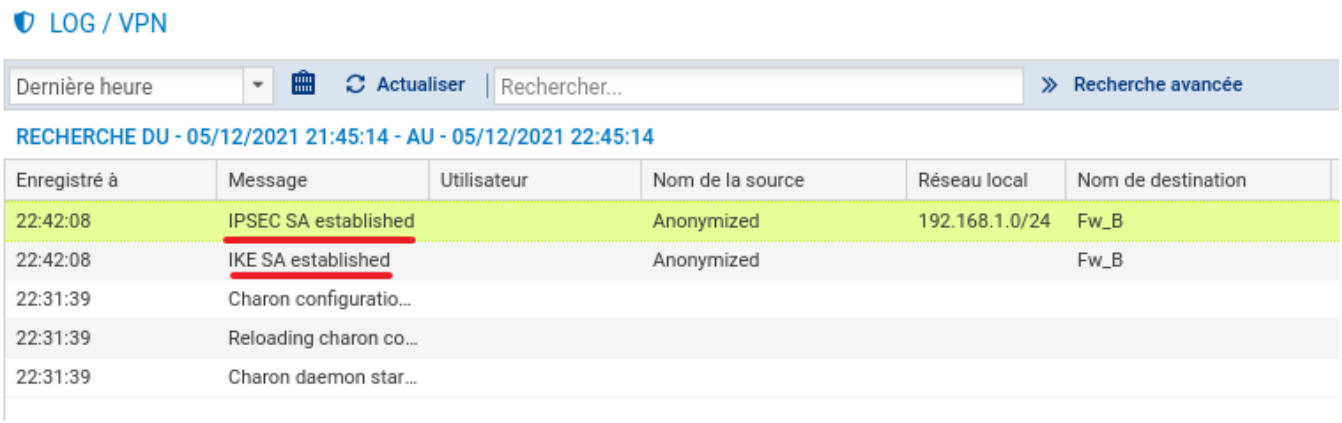
Les logs de la négociation IKE

Le menu LOGS ⇒ VPN affiche les évènements 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.



Supervision des tunnels VPN IPsec

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

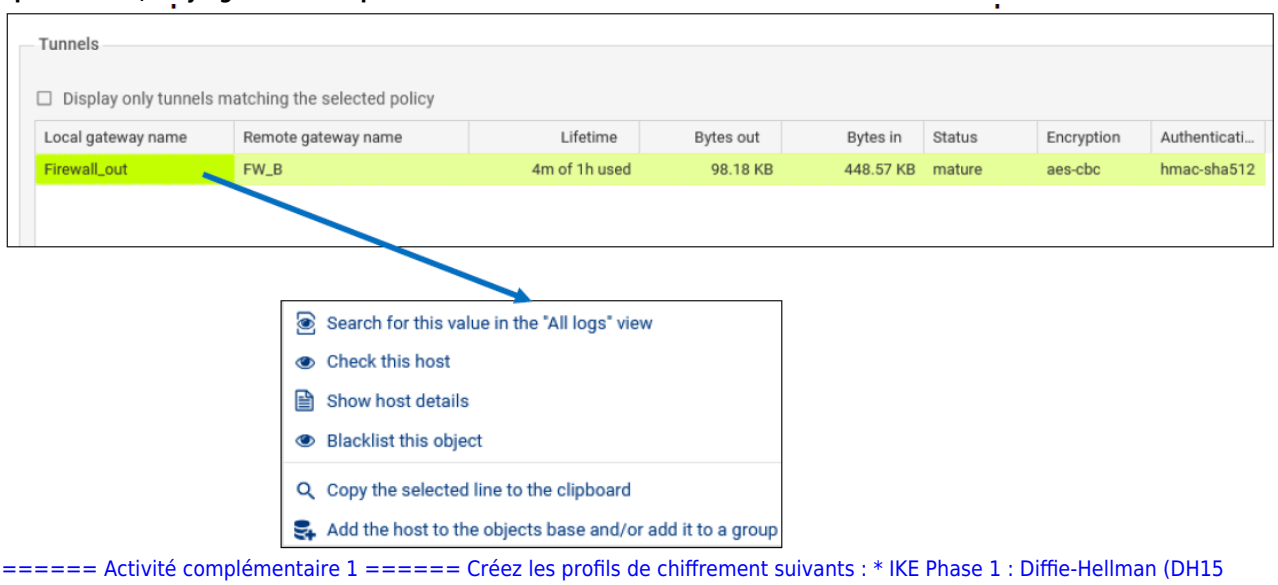
Lorsque l'option **Masquer les tunnels établis pour afficher uniquement les politiques présentant des problèmes** est cochée, seules les politiques qui n'ont pas de tunnels négociés s'affichent.

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.**



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

MODP), Durée de vie maximum (21600s), algorithme d'authentification (sha2*512) et algorithme de chiffrement (AES 256bits). * IPSEC Phase 2 : PFS (DH15 MODP), durée de vie (3600s), algorithme d'authemtificatiom (hmac*sha512) et algorithme de chiffrement (AES 256bits). Appliquez vos nouveaux profils de chiffrement sur votre VPN. Puis vérifiez que tout fonctionne correctement. ====== Activité complémentaire 2 ====== 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

. :