NOTE TECHNIQUE
STORMSHIELD NETWORK SECURITY

VPN IPSEC : INTERFACES VIRTUELLES IPSEC - CONFIGURATION DE TUNNELS ANONYMES

Produits concernés : SNS 4.3, SNS 4.8 et SNS 5.0

Dernière mise à jour du document : 4 novembre 2025

Référence : sns-fr-VPN_IPsec_tunnels_anonymes_VTI_Note_Technique

Table des matières

Historique des modifications

Date	Description
4 novembre 2025	Nouveau document

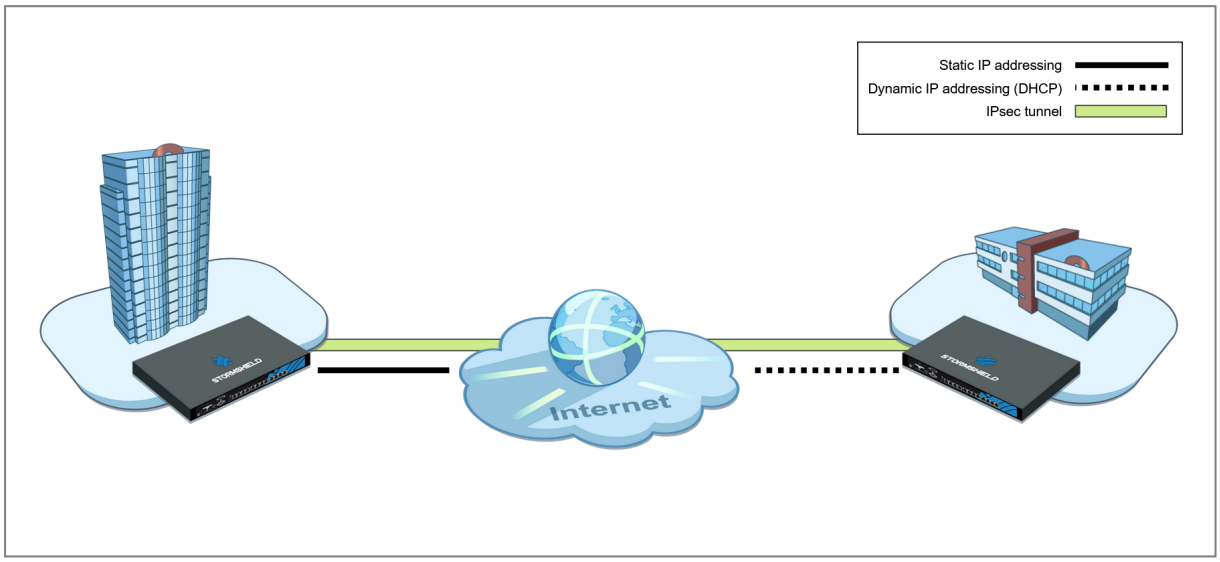
Avant de commencer

Les firewalls SNS permettent de mettre en oeuvre des tunnels IPsec basés sur le routage. Ce ne sont plus les informations définies dans la Security Policy Database (SPD) mais les instructions de routage (routage statique, dynamique ou routage défini par le filtrage) qui déterminent si les paquets doivent transiter par ces tunnels IPsec.

Cette note technique présente le cas d'usage d'une architecture présentant un site central (Hub) et un site satellite (Spoke) mettant en œuvre des interfaces virtuelles IPsec et comment établir un tunnel IPsec basé sur le routage avec un correspondant dynamique (ou anonyme). Ce correspondant peut être par exemple une unité mobile telle qu'un service d'urgence ou un prestataire événementiel qui aurait accès à internet de manière nomade.

Architecture présentée

Le cas d'usage principal de cette architecture présente une topologie en étoile avec un site central (Hub) et un site satellite (Spoke). Ce type d'architecture ne se limite pas à un seul site satellite.



Chaque site dispose d'un accès à internet :

- Le site central (Hub) dispose d'un accès à internet avec un adressage IP statique.
- Le site satellite (Spoke) dispose d'un accès à internet avec un adressage IP dynamique.

La contrainte de cette architecture réside dans l'adressage dynamique du site Spoke et donc en la nécessité d'établir des tunnels IPsec routés avec un correspondant anonyme.

Prérequis

Cette section présente les prérequis nécessaires pour configurer chacun des firewalls de l'architecture présentée.

Les adresses IP 198.51.100.0/24 et 203.0.113.0/24 utilisées dans cette note technique pour représenter les adresses IP publiques des firewalls sont réservées pour la documentation conformément à la RFC 5737.

Conditions et limitations

Ce cas d'usage est supporté selon les conditions et limitations suivantes :

- Vous utilisez une des versions de firmware SNS 4.3, SNS 4.8 ou SNS 5
- Vous utilisez le protocole IKEv2,
- Vous utilisez le protocole DHCP.

Configuration du réseau et de la PKI

Vous avez configuré au préalable votre réseau et optionnellement votre PKI afin que les différents sites puissent communiquer via leurs interfaces physiques.

Configuration du réseau

Configuration réseau du Hub :

- Interface WAN : 198.51.100.1/24,
- Interface LAN : 192.168.1.1/24,
- Route par défaut : GW_default (198.51.100.254).

Configuration réseau du Spoke :

- Interface WAN : 203.0.113.59/24 (DHCP),
- Interface LAN : 192.168.2.1/24,
- Route par défaut : Firewall_WAN_router.

Configuration de la PKI (optionnel)

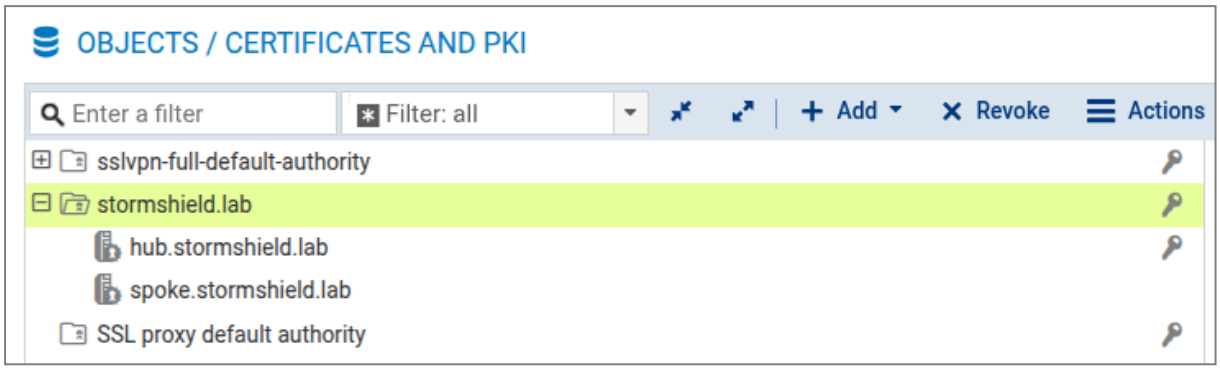
Vous pouvez choisir de configurer l'authentification des correspondants IPsec par certificat ou par clé pré-partagée (PSK).

Nous vous recommandons l'authentification par certificat.

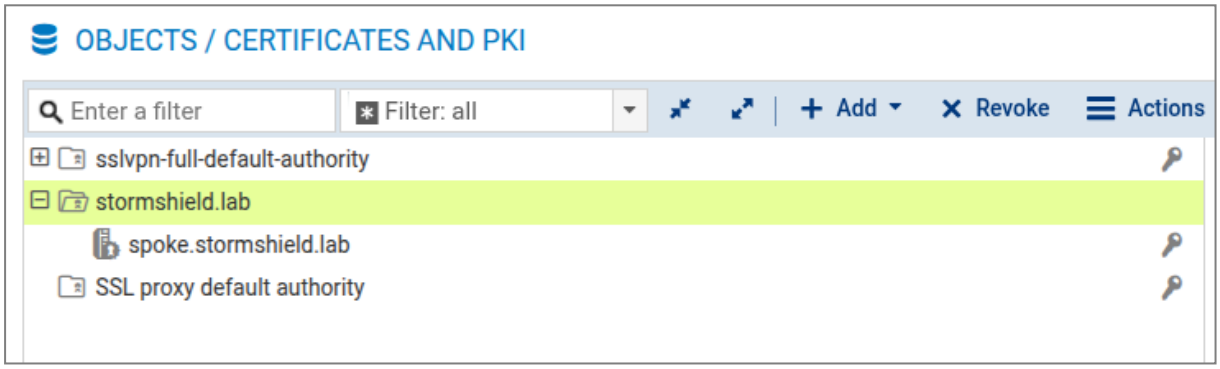
Dans ce cas, vous devez avoir mis en place votre PKI :

- Vous avez créé l'autorité de certification (CA) et les certificats des firewalls sur le Hub,
- Vous avez exporté le certificat de la CA et l'identité du Spoke (certificat et clé privée) puis vous les avez importés dans la PKI du Spoke,
- Vous avez ajouté la CA dans les autorités de confiance sur chacun des firewalls à mettre en relation.

Configuration de la PKI du Hub



Configuration de la PKI du Spoke



NOTE
Pour des raisons de sécurité, nous vous recommandons de supprimer la clé privée générée sur le Hub dès lors que l'identité (*spoke.stormshield.lab* dans l'exemple) a été exportée et importée dans la PKI du Spoke.

Paramétrer le site central (Hub)

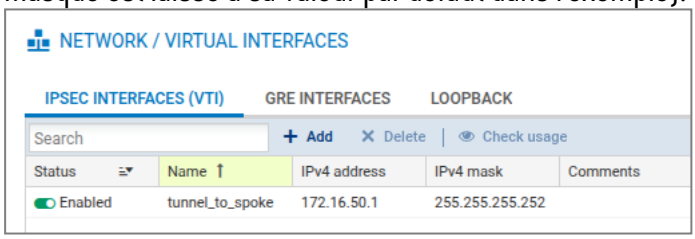
Les tunnels dans lesquels transitent les flux sont définis par des interfaces virtuelles IPsec.

Vous devez donc créer une interface virtuelle IPsec locale permettant de définir les extrémités locale et distante du tunnel. Dans l'exemple, cette interface est nommée **tunnel_to_spoke**. Les extrémités de tunnel sont définies par des objets réseau (**VTI_local_spoke** et **VTI_remote_spoke** dans l'exemple).

Créer l'interface virtuelle IPsec locale

Vous devez créer l'interface virtuelle IPsec permettant de définir le tunnel.

1. Rendez-vous dans **Configuration** > **Réseau** > **Interfaces virtuelles** et sélectionnez l'onglet **Interfaces IPsec (VTI)**.
2. Cliquez sur **Ajouter**.
3. Renseignez les champs suivants :
   - **Nom** : **tunnel_to_spoke** dans l'exemple,
   - **Adresse IP** : **172.16.50.1** dans l'exemple,
   - **Masque réseau** : la valeur par défaut est un masque de type 255.255.255.252 (le masque est laissé à sa valeur par défaut dans l'exemple).

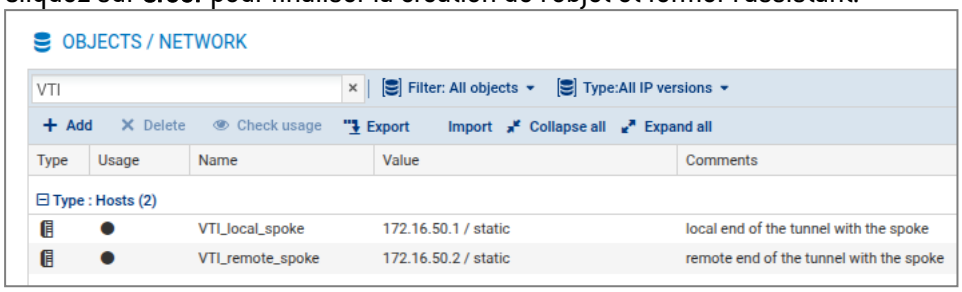


Créer les extrémités locale et distante du tunnel

Les interfaces virtuelles du Spoke sont définies à l'aide d'objets réseau. Elles sont utilisées comme passerelles au sein des objets routeur du Hub et servent à la définition des tunnels IPsec. Vous devez définir les objets réseau qui correspondent aux extrémités locale et distante du tunnel avec le Spoke.

1. Rendez-vous dans **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter** et sélectionnez **Machine** dans le bandeau de gauche.
3. Configurez l'objet réseau correspondant à l'extrémité locale du tunnel en renseignant les champs suivants :
   - **Nom de l'objet** : **VTI_local_spoke** dans l'exemple,
   - **Adresse IPv4** : **172.16.50.1** dans l'exemple,
   - **Adresse MAC** : vous pouvez indiquer une adresse MAC,
   - **Commentaire** : vous pouvez saisir un commentaire libre.
4. Cliquez sur **Créer et dupliquer** pour finaliser la création de l'objet et créer le suivant.
5. Configurez l'objet réseau correspondant à l'extrémité distante du tunnel avec les valeurs indiquées ci-dessous.
   - **Nom de l'objet** : **VTI_remote_spoke** dans l'exemple,
   - **Adresse IPv4** : **172.16.50.2** dans l'exemple.

6. Cliquez sur **Créer** pour finaliser la création de l'objet et fermer l'assistant.



Configurer le routage

Le routage du Hub doit être configuré afin de permettre aux flux d'atteindre leur destination. Pour cela, vous devez créer un objet réseau correspondant au réseau local du Spoke et définir le routage.

Créer un objet réseau

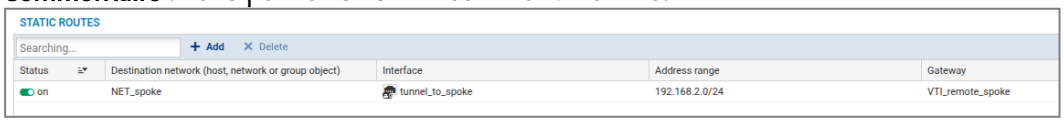
Vous devez créer un objet réseau correspondant au réseau local du Spoke.

1. Rendez-vous dans **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter** et sélectionnez **Réseau** dans le bandeau de gauche.
3. Renseignez les champs suivants :
   - **Nom de l'objet** : **NET_spoke** dans l'exemple,
   - **Adresse IP de réseau** : **192.168.2.0/24** dans l'exemple,
   - **Commentaire** : vous pouvez ajouter un commentaire libre.
4. Cliquez sur **Créer** pour finaliser la création de l'objet et fermer l'assistant.

Définir le routage

Vous devez définir le routage des flux vers le réseau local du Spoke.

1. Rendez-vous dans **Configuration** > **Réseau** > **Routage** et sélectionnez l'onglet **Routes statiques IPv4**.
2. Cliquez sur **Ajouter**.
3. Renseignez les champs suivants :
   - **Réseau de destination** : **NET_spoke** dans l'exemple,
   - **Plan d'adressage** : **192.168.2.0/24** dans l'exemple,
   - **Passerelle** : **VTI_remote_spoke** dans l'exemple,
   - **Commentaire** : vous pouvez saisir un commentaire libre.



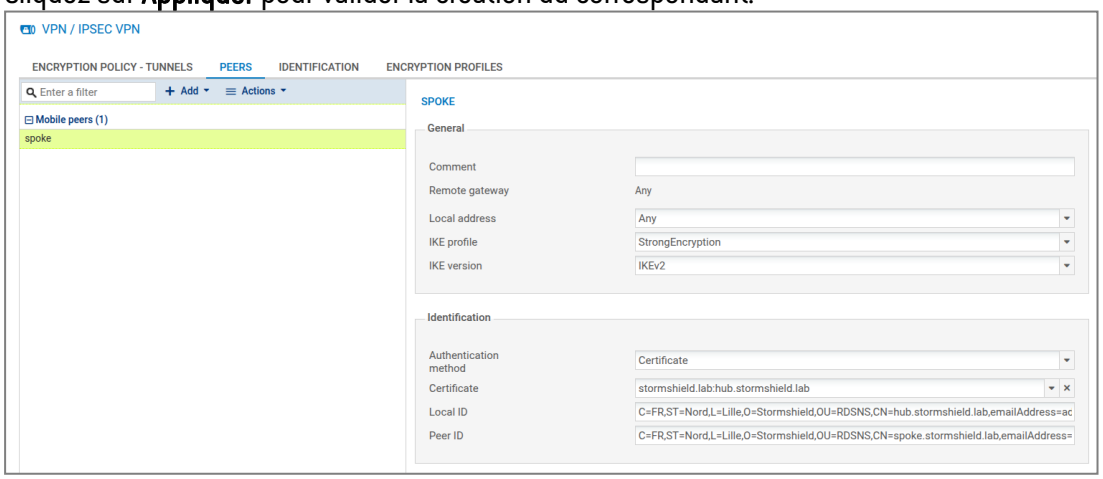
Créer le correspondant IPsec dynamique (ou anonyme)

Afin que le Hub soit en mesure d'identifier précisément le Spoke, vous devez créer le correspondant *spoke*. Vous pouvez le créer soit en utilisant la méthode d'authentification par

certificat (recommandé), soit en suivant la méthode d'authentification par clé pré-partagée (PSK).

Créer le correspondant avec la méthode d'authentification par certificat (recommandé)

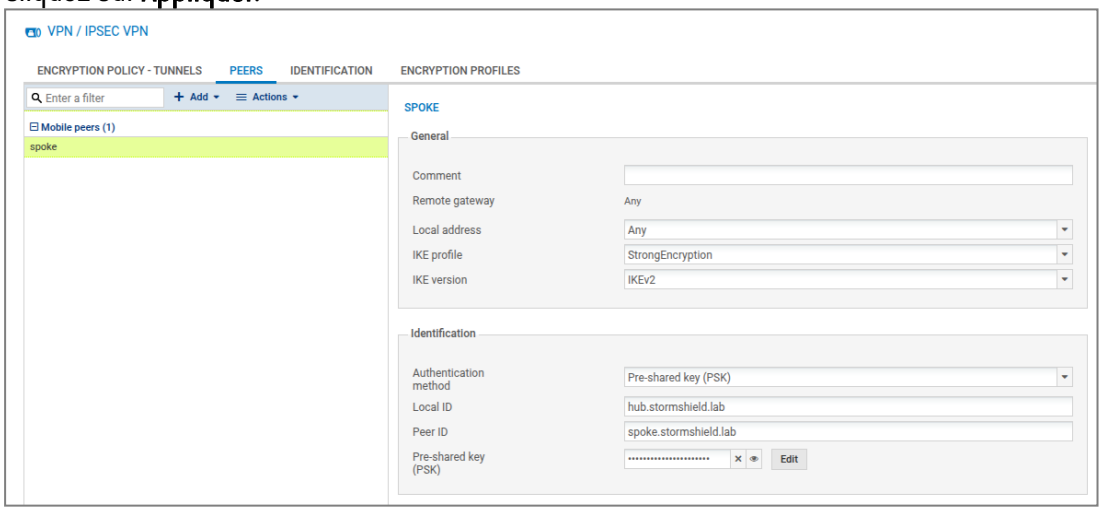
1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter**.
3. Choisissez **Nouveau correspondant mobile**. Un assistant s'affiche, vous invitant à sélectionner la passerelle distante.
4. Choisissez **Any**.
5. Renseignez le nom du correspondant. Par défaut, son nom est préfixé en "mobile_", ce nom est personnalisable (**spoke** dans l'exemple). Validez.
6. Sélectionnez la version **IKEv2** comme version IKE et cliquez sur **Suivant**.
7. Sélectionnez le type d'authentification par **Certificat**.
8. Dans le menu déroulant **Certificat**, sélectionnez le certificat qui sera présenté par le Hub pour établir le tunnel avec son correspondant mobile et cliquez sur **Suivant**.
9. Dans la fenêtre qui s'ouvre et résume les paramètres du correspondant, vérifiez les informations puis cliquez sur **Terminer**.
10. Dans la zone **Identification**, renseignez les champs suivants :
    - **Local ID** (optionnel) : il s'agit de l'identifiant local précisé lors de la création du correspondant. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **ID du correspondant** sur le Spoke.
    - **ID du correspondant** (optionnel) : il s'agit de l'identifiant attribué au correspondant. Il est recommandé de le spécifier afin d'identifier formellement le correspondant mobile et d'y associer la bonne politique IPsec lors de la négociation du tunnel. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **Local ID** sur le Spoke.
11. Cliquez sur **Appliquer** pour valider la création du correspondant.



Créer le correspondant avec la méthode d'authentification par clé pré-partagée (PSK)

1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter**.
3. Choisissez **Nouveau correspondant mobile**. Un assistant s'affiche, vous invitant à sélectionner la passerelle distante.
4. Choisissez **Any**.

5. Par défaut le nom du correspondant est créé en préfixant cet objet avec "mobile_", ce nom est personnalisable (**spoke** dans l'exemple). Validez.
6. Sélectionnez la méthode d'authentification par **Clé pré-partagée (PSK)**.
7. Dans la zone **Identification**, renseignez les champs suivants :
   - **Local ID** (optionnel) : il s'agit de l'identifiant local précisé lors de la création du correspondant. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **ID du correspondant** sur le Spoke.
   - **ID du correspondant** (optionnel) : il s'agit de l'identifiant attribué au correspondant. Il est recommandé de le spécifier afin d'identifier formellement le correspondant et d'y associer la bonne politique IPsec lors de la négociation du tunnel. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **Local ID** sur le Spoke.
   - **Clé pré-partagée** : cliquez sur le bouton **Éditer** et saisissez dans les champs **Clé pré-partagée** et **Confirmer** une clé complexe qui sera échangée entre le Hub et le Spoke afin d'établir le tunnel IPsec.
     Pour définir une clé pré-partagée suffisamment sécurisée :
     - Respectez une longueur minimale de 15 caractères,
     - Utilisez des majuscules, minuscules, chiffres et caractères spéciaux,
     - Ne basez pas votre clé sur un mot du dictionnaire.
8. Cliquez sur **Appliquer**.

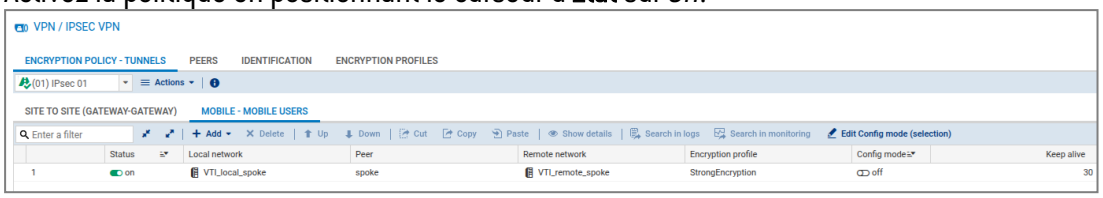


Configurer la politique VPN IPsec

Vous devez définir les règles de la politique de chiffrement qui s'appliquera aux flux.

1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - tunnels** > onglet **Mobile - Utilisateurs nomades**.
2. Cliquez sur **Ajouter** puis sélectionnez **Nouvelle politique mobile simple**.
3. Sélectionnez **spoke** comme **Choix du correspondant**.
4. Pour le champ **Réseau local**, sélectionnez l'objet **VTI_local_spoke**.
5. Pour le champ **Réseau distant**, sélectionnez l'objet **VTI_remote_spoke**.

6. Activez la politique en positionnant le curseur d'**État** sur *On*.



Vous avez terminé la configuration du Hub et pouvez poursuivre la procédure par la configuration du Spoke.

Paramétrer le site satellite (Spoke)

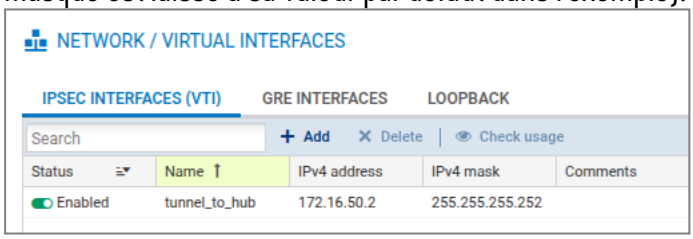
Les tunnels dans lesquels transitent les flux sont définis par des interfaces virtuelles IPsec.

Vous devez donc créer une interface virtuelle IPsec locale permettant de définir les extrémités locale et distante du tunnel. Dans l'exemple, cette interface est nommée **tunnel_to_hub**. Les extrémités de tunnel sont définies par des objets réseau (**VTI_local_hub** et **VTI_remote_hub** dans l'exemple).

Créer l'interface virtuelle IPsec locale

Vous devez créer l'interface virtuelle IPsec permettant de définir le tunnel.

1. Rendez-vous dans **Configuration** > **Réseau** > **Interfaces virtuelles** et sélectionnez l'onglet **Interfaces IPsec (VTI)**.
2. Cliquez sur **Ajouter**.
3. Renseignez les champs suivants :
   - **Nom** : **tunnel_to_hub** dans l'exemple,
   - **Adresse IP** : **172.16.50.2** dans l'exemple,
   - **Masque réseau** : la valeur par défaut est un masque de type 255.255.255.252 (le masque est laissé à sa valeur par défaut dans l'exemple).

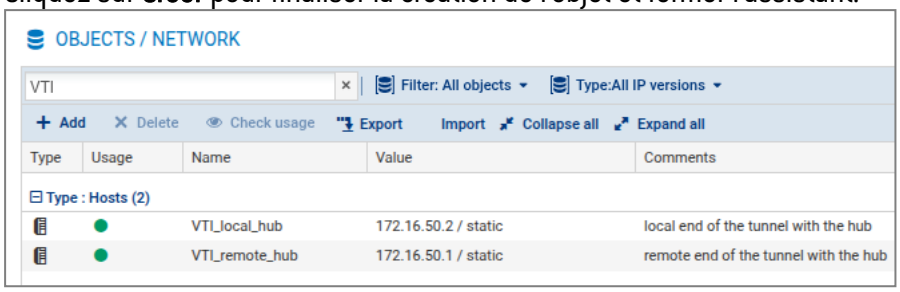


Créer les extrémités locale et distante du tunnel

Les interfaces virtuelles du Hub sont définies à l'aide d'objets réseau. Elles sont utilisées comme passerelles au sein des objets routeur du Spoke et servent à la définition des tunnels IPsec. Vous devez définir les objets réseau qui correspondent aux extrémités locale et distante du tunnel avec le Hub.

1. Rendez-vous dans **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter** et sélectionnez **Machine** dans le bandeau de gauche.
3. Configurez l'objet réseau correspondant à l'extrémité locale du tunnel en renseignant les champs suivants :
   - **Nom de l'objet** : **VTI_local_hub** dans l'exemple,
   - **Adresse IPv4** : **172.16.50.2** dans l'exemple,
   - **Adresse MAC** : vous pouvez indiquer une adresse MAC,
   - **Commentaire** : vous pouvez saisir un commentaire libre.
4. Cliquez sur **Créer et dupliquer** pour finaliser la création de l'objet et créer le suivant.
5. Configurez l'objet réseau correspondant à l'extrémité distante du tunnel avec les valeurs indiquées ci-dessous.
   - **Nom de l'objet** : **VTI_remote_hub** dans l'exemple,
   - **Adresse IPv4** : **172.16.50.1** dans l'exemple.

6. Cliquez sur **Créer** pour finaliser la création de l'objet et fermer l'assistant.



Configurer le routage

Le routage du Spoke doit être configuré afin de permettre aux flux d'atteindre leur destination. Pour cela, vous devez créer un objet réseau correspondant au réseau local du Hub et définir le routage.

Créer un objet réseau

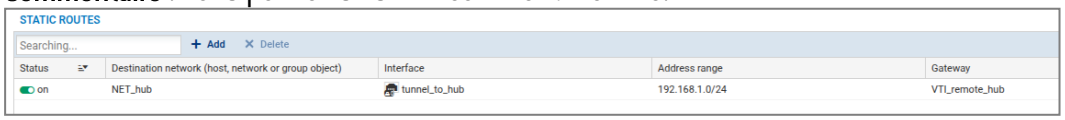
Vous devez créer un objet réseau correspondant au réseau local du Hub.

1. Rendez-vous dans **Configuration** > **Objets** > **Réseau**.
2. Cliquez sur **Ajouter** et sélectionnez **Réseau** dans le bandeau de gauche.
3. Renseignez les champs suivants :
   - **Nom de l'objet** : **NET_hub** dans l'exemple,
   - **Adresse IP de réseau** : **192.168.1.0/24** dans l'exemple,
   - **Commentaire** : vous pouvez ajouter un commentaire libre.
4. Cliquez sur **Créer** pour finaliser la création de l'objet et fermer l'assistant.

Définir le routage

Vous devez définir le routage des flux vers le réseau local du Hub.

1. Rendez-vous dans **Configuration** > **Réseau** > **Routage** et sélectionnez l'onglet **Routes statiques IPv4**.
2. Cliquez sur **Ajouter**.
3. Renseignez les champs suivants :
   - **Réseau de destination** : **NET_hub** dans l'exemple,
   - **Plan d'adressage** : **192.168.1.0/24** dans l'exemple,
   - **Passerelle** : **VTI_remote_hub** dans l'exemple,
   - **Commentaire** : vous pouvez saisir un commentaire libre.



Créer le correspondant IPsec

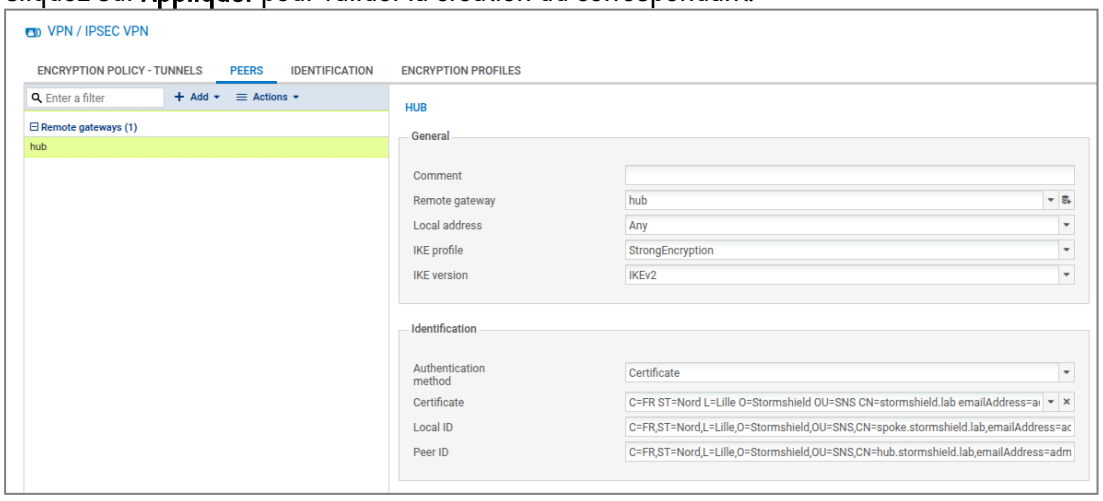
Afin que le Spoke soit en mesure d'identifier précisément le Hub, vous devez créer le correspondant *hub*. Vous pouvez le créer soit en utilisant la méthode d'authentification par

certificat (recommandé), soit en suivant la méthode d'authentification par clé pré-partagée (PSK).

> **NOTE**
> L'adresse locale utilisée doit être "any" afin que le service IKE s'adapte en cas de rechargement de la configuration réseau (modification du routage, renouvellement du bail DHCP, etc.).

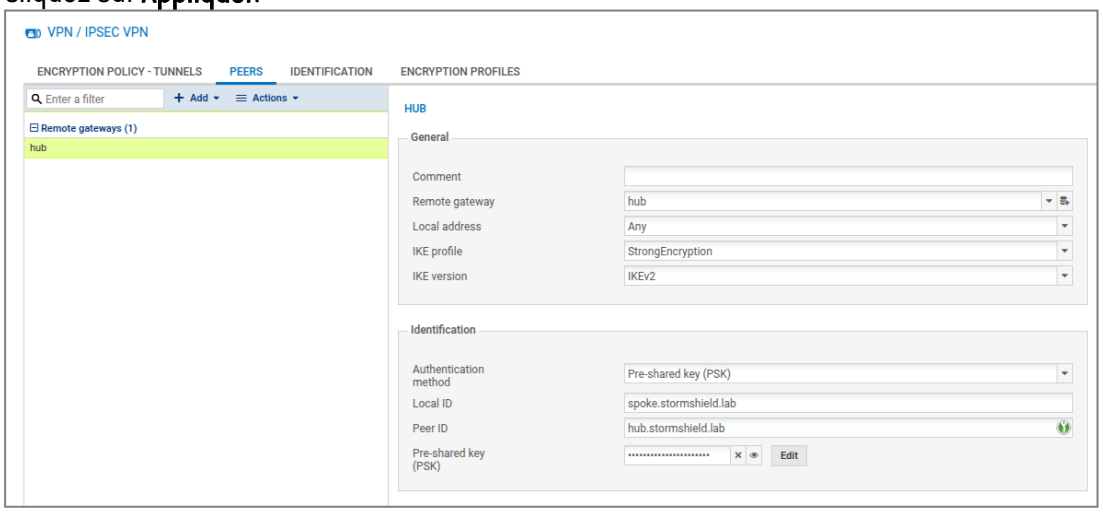
Créer le correspondant avec la méthode d'authentification par certificat (recommandé)

1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter**.
3. Choisissez **Nouvelle passerelle distante**. Un assistant s'affiche vous invitant à sélectionner la passerelle distante.
4. Choisissez **hub**.
5. Renseignez le nom du correspondant. Par défaut, son nom est préfixé en "Site_", ce nom est personnalisable (**hub** dans l'exemple). Validez.
6. Sélectionnez la version **IKEv2** comme version IKE et cliquez sur **Suivant**.
7. Sélectionnez la méthode d'authentification par **Certificat**.
8. Dans le menu déroulant **Certificat**, sélectionnez le certificat qui sera présenté par le Spoke pour établir le tunnel avec son correspondant et cliquez sur **Suivant**.
9. Dans la fenêtre qui s'ouvre et résume les paramètres du correspondant, vérifiez les informations puis cliquez sur **Terminer**.
10. Dans la zone **Identification**, renseignez les champs suivants :
    - **Local ID** (optionnel) : il s'agit de l'identifiant local précisé lors de la création du correspondant. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **ID du correspondant** sur le Hub.
    - **ID du correspondant** (optionnel) : il s'agit de l'identifiant attribué au correspondant. Il est recommandé de le spécifier afin d'identifier formellement le correspondant mobile et d'y associer la bonne politique IPsec lors de la négociation du tunnel. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **Local ID** sur le Hub.
11. Cliquez sur **Appliquer** pour valider la création du correspondant.



Créer le correspondant avec la méthode d'authentification par clé pré-partagée (PSK)

1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Correspondants**.
2. Cliquez sur **Ajouter**.
3. Choisissez **Nouvelle passerelle distante**. Un assistant s'affiche vous invitant à sélectionner la passerelle distante.
4. Choisissez l'objet **hub**.
5. Par défaut le nom du correspondant est créé en préfixant cet objet avec "Site_", ce nom est personnalisable (**hub** dans l'exemple). Validez.
6. Sélectionnez **IKEv2** comme version IKE et cliquez sur **Suivant**.
7. Sélectionnez la méthode d'authentification par **Clé pré-partagée (PSK)**.
8. Dans la zone **Identification**, renseignez les champs suivants :
   - **Local ID** (optionnel) : il s'agit de l'identifiant local précisé lors de la création du correspondant. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **ID du correspondant** sur le Hub.
   - **ID du correspondant** (optionnel) : il s'agit de l'identifiant attribué au correspondant. Il est recommandé de le spécifier afin d'identifier formellement le correspondant et d'y associer la bonne politique IPsec lors de la négocation du tunnel. Si vous renseignez ce champ, vous devez indiquer la même valeur dans le champ **Local ID** sur le Hub.
   - **Clé pré-partagée** : cliquez sur le bouton **Éditer** et saisissez dans les champs **Clé pré-partagée** et **Confirmer** une clé complexe qui sera échangée entre le Hub et le Spoke afin d'établir le tunnel IPsec.
     Pour définir une clé pré-partagée suffisamment sécurisée :
     - Respectez une longueur minimale de 15 caractères,
     - Utilisez des majuscules, minuscules, chiffres et caractères spéciaux,
     - Ne basez pas votre clé sur un mot du dictionnaire.
9. Cliquez sur **Appliquer**.

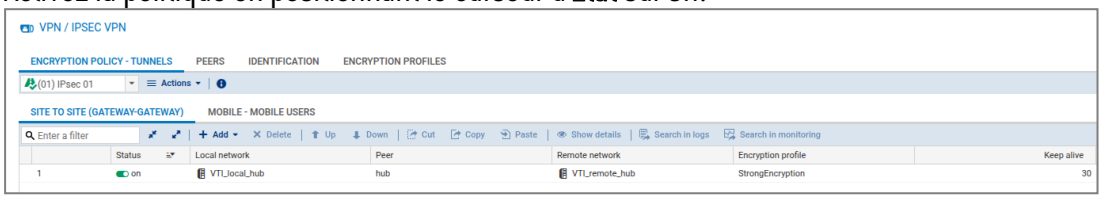


Configurer la politique IPsec

Vous devez définir les règles de la politique de chiffrement qui s'appliquera aux flux.

1. Rendez-vous dans **Configuration** > **VPN** > **VPN IPsec** > onglet **Politique de chiffrement - tunnels** > onglet **Site à site**.

2. Cliquez sur **Ajouter** puis sélectionnez **Tunnel site à site simple**.
3. Sélectionnez **hub** comme **Choix du correspondant**.
4. Pour le champ **Réseau local**, sélectionnez l'objet **VTI_local_hub**.
5. Pour le champ **Réseau distant**, sélectionnez l'objet **VTI_remote_hub**.
6. Activez la politique en positionnant le curseur d'**État** sur *On*.



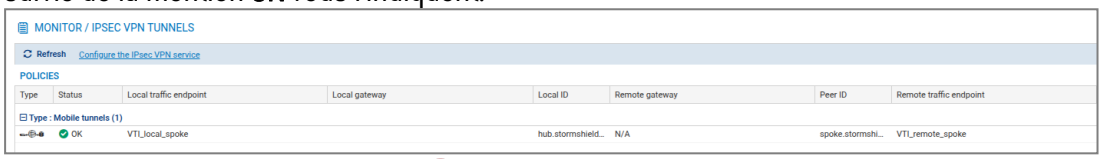
Vous avez terminé la configuration du Spoke et pouvez poursuivre la procédure en vérifiant l'établissement des tunnels.

Vérifier l'établissement des tunnels

Vous pouvez vérifier l'établissement des tunnels depuis l'interface web d'administration du firewall.

Vérifier l'établissement du tunnel sur le Hub

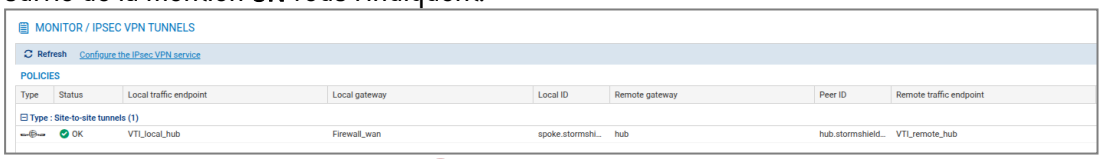
1. Rendez-vous dans **Monitoring** > **Supervision** > **Tunnels VPN IPsec**.
2. Dans la colonne **État**, vérifiez l'état du tunnel : si le tunnel est correctement établi, l'icône suivie de la mention **OK** vous l'indiquent.



Si un problème est survenu, l'icône suivie de la mention **Aucun tunnel** vous l'indiquent. Vous pouvez passer la souris sur cet état afin d'obtenir des informations concernant le problème rencontré.

Vérifier l'établissement du tunnel sur le Spoke

1. Rendez-vous dans **Monitoring** > **Supervision** > **Tunnels VPN IPsec**.
2. Dans la colonne **État**, vérifiez l'état du tunnel : si le tunnel est correctement établi, l'icône suivie de la mention **OK** vous l'indiquent.



Si un problème est survenu, l'icône suivie de la mention **Aucun tunnel** vous l'indiquent. Vous pouvez passer la souris sur cet état afin d'obtenir des informations concernant le problème rencontré.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu