NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

VPN IPSEC : AUTHENTIFICATION PAR CLÉ PRÉPARTAGÉE

Produits concernés : SNS 2.x, SNS 3.x, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-VPN_IPSec_Authentification_Cle_Pre_Partagee_Note_Technique

Table des matières

VPN IPSec : Authentification par clé prépartagée

Vous souhaitez mettre en relation de manière sécurisée deux sites de votre entreprise reliés via Internet. Pour cela, vous devez créer un VPN IPSec site à site (également appelé « gateway to gateway »).

La méthode d'authentification présentée dans ce didacticiel est basée sur l'utilisation d'une clé prépartagée (une authentification par certificats aurait également pu être mise en œuvre).

Ce document décrit la configuration VPN à réaliser, afin d'autoriser un poste client du site distant à accéder en HTTP à un serveur intranet du site principal au travers de ce tunnel.

Mise en œuvre

L'objectif de cette section est de décrire le paramétrage nécessaire sur les différents Firewalls participant au VPN IPSec.

Configurer le site principal

Sur le site principal, il est nécessaire de :

- Créer les objets réseau des sites à connecter,
- Créer le tunnel IPSec,
- Mettre en place les règles de filtrage autorisant les flux entre sites.

Créer les objets réseau

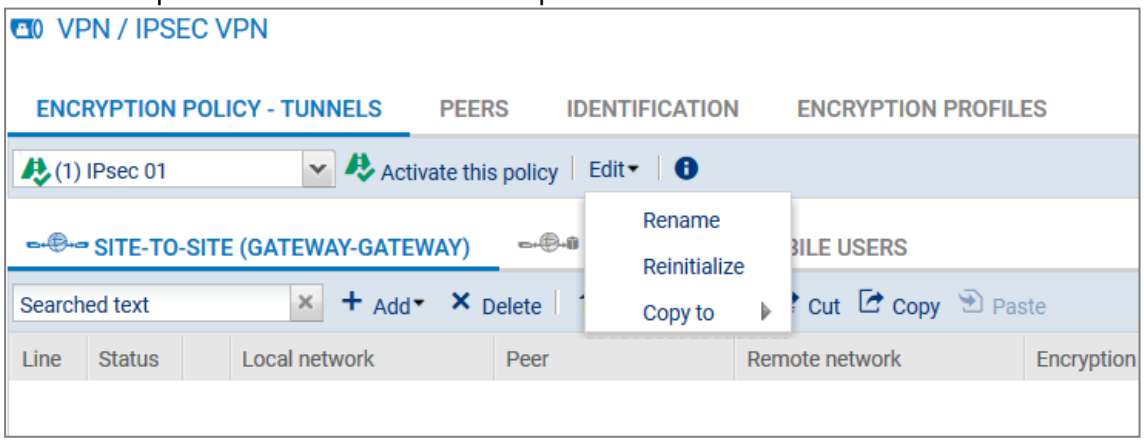
La création de cette connexion VPN IPSEC site à site nécessite à minima cinq objets réseau :

- le réseau local du site principal :Private_Net_Main_Site,
- l'adresse publique du Firewall principal : Pub_Main_FW,
- le réseau local du site distant :Private_Net_Remote_Site,
- l'adresse publique du Firewall distant : Pub_Remote_FW,
- le serveur intranet à joindre sur le site principal :Intranet_Server.

Ces objets peuvent être définis via le menu : **Configuration > Objets > Objets réseau**.

Créer le tunnel IPSec

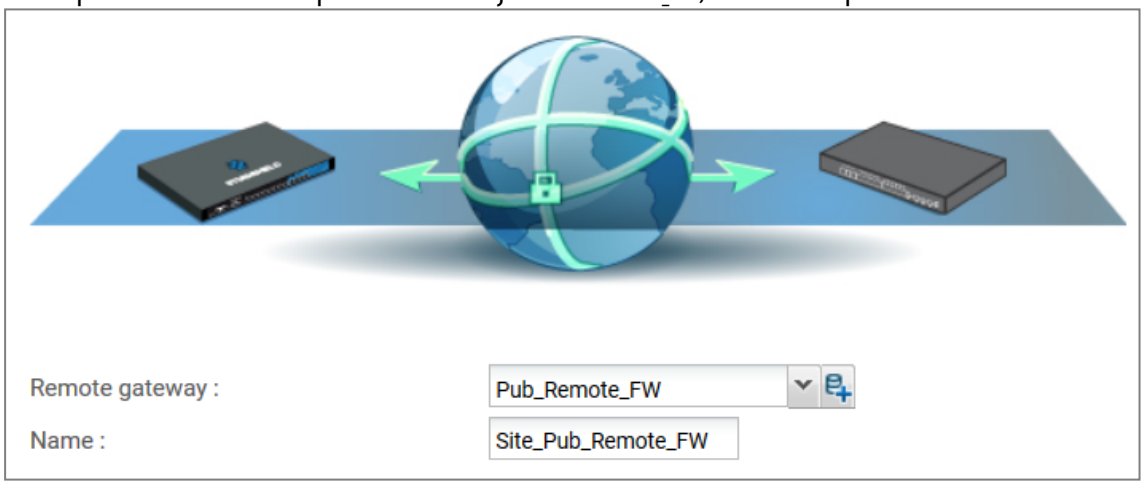
1. Cliquez sur **Configuration** > **VPN** > **VPN IPSec**.
2. Choisissez la politique de chiffrement que vous souhaitez configurer.
   Vous avez la possibilité de la renommer en cliquant sur le bouton **Éditer**.



3. Cliquez sur **Ajouter** > **Tunnel site à site.**
   Un assistant de création se lance automatiquement.
4. Dans le champ **Réseau local**, sélectionnez votre objet Private_Net_Main_Site.

5. Dans le champ **Réseau distant**, sélectionnez l'objet Private_Net_Remote_Site.

6. Choisissez un correspondant.
Si celui-ci n'existe pas encore, comme dans cet exemple, vous pouvez le créer en cliquant sur l'hyperlien **Créer un correspondant** (cette étape correspond aux paramètres pouvant être définis directement dans l'onglet *Correspondant* du menu **Configuration** > **VPN** > **VPN IPSec**),
7. L'assistant vous invite à sélectionner la passerelle distante: dans le cas présent, il s'agit de l'adresse publique du Firewall distant (objet Pub_Remote_FW). Par défaut, le nom du correspondant est créé en préfixant cet objet avec « Site_ » ; ce nom est personnalisable :

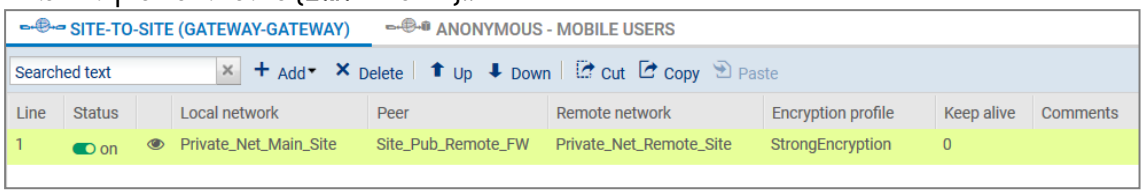


8. Sélectionnez la méthode d'authentification : **Clé pré-partagée (PSK)**.
9. Dans les champs **Clé pré-partagée (ASCII)** et **Confirmer**, saisissez un mot de passe complexe qui sera échangé entre les deux sites afin d'établir le tunnel IPSec, puis validez.

> **NOTE**
>
> Pour définir une clé pré-partagée suffisamment sécurisée, il est conseillé de suivre quelques règles de bonne conduite:
>
> - Respectez une longueur minimale de 8 caractères,
> - Utilisez des majuscules, minuscules, chiffres et caractères spéciaux,
> - Ne basez pas votre clé sur un mot du dictionnaire.
>
> **Exemple** : 7f4V8!>Xdu.

10. L'assistant vous propose un résumé du correspondant que vous venez de créer.
11. Cliquez sur **Terminer** pour fermer cette fenêtre.

12. Cliquez à nouveau sur **Terminer** pour fermer l'assistant.
    La définition du Tunnel IPSec est terminée sur le site principal et le tunnel est automatiquement activé (**État** à « on »).:



13. Cliquez sur **Activer cette politique**.

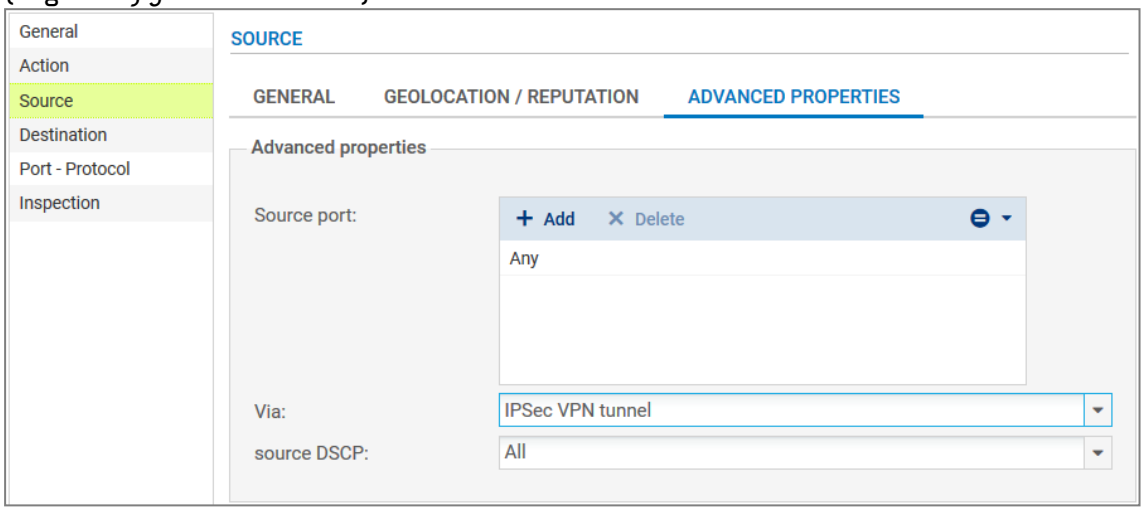
Créer les règles de filtrage

Le tunnel VPN est destiné à mettre en relation de manière sécurisée les deux sites distants, mais il n'a pas pour vocation de filtrer les flux entre ces deux entités. Des règles de filtrage doivent donc être mises en place afin de :

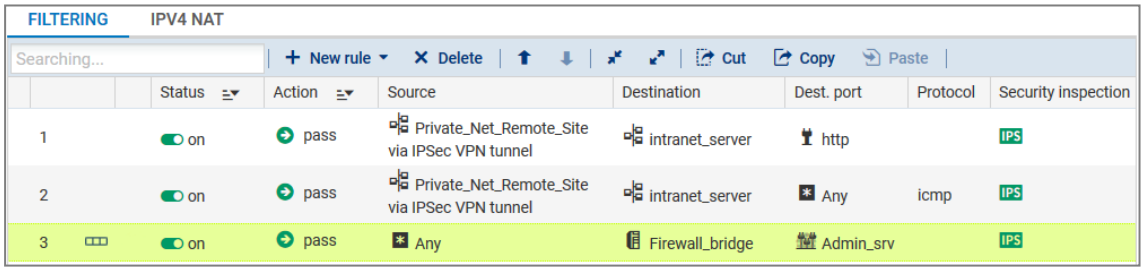
- n'autoriser que les flux nécessaires entre des machines sources et destinations identifiées,
- optimiser les performances (ressources machines, bande passante de l'accès Internet) en évitant que des paquets inutiles ne déclenchent l'établissement d'un tunnel.

1. Dans le menu **Configuration > Politique de Sécurité > Filtrage et NAT**, sélectionnez votre politique de filtrage.

2. Dans l'onglet **Filtrage**, cliquez sur le menu **Nouvelle règle > Règle standard**.
Pour une sécurité accrue, il est possible de créer une règle plus restrictive sur le Firewall hébergeant le serveur intranet en précisant l'origine des paquets. Pour cela, lors de la sélection de la source du trafic, indiquez la valeur « Tunnel VPN IPSec » dans le champ **Via** (onglet *Configuration avancée*) :



Dans le cas présenté, un poste client situé sur le réseau local du **site distant** doit pouvoir se connecter en HTTP au serveur intranet situé sur le réseau local du **site principal** (règle N°1). Vous pouvez également y ajouter temporairement, par exemple, le protocole ICMP afin de tester plus facilement l'établissement du tunnel (règle N°2). La règle de filtrage prend la forme suivante :



NOTE

Les fonctionnalités avancées des Firewalls (utilisation de proxies, profils d'inspection de sécurité…) peuvent bien évidemment être mises en œuvre dans ces règles de filtrage.

Configurer le site distant

L'objectif de cette section est de reproduire sur le site distant, une configuration symétrique à celle réalisée sur le Firewall principal.

Créer les objets réseau

Les objets sont identiques à ceux définis sur le Firewall principal. Reportez-vous à la section **Configuration du site principal**, partie Création des objets réseau.

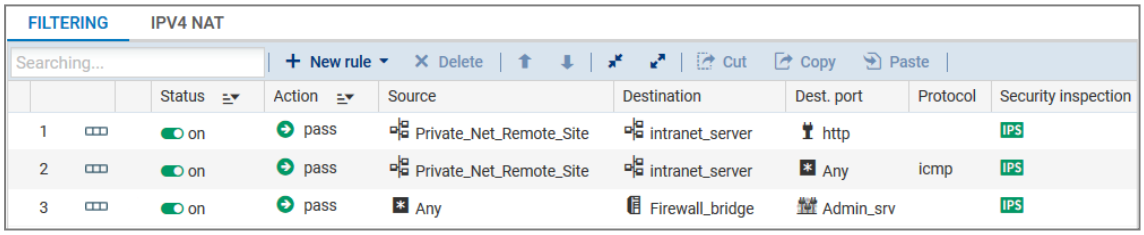
Créer le tunnel IPSec

Reportez-vous à la section **Configuration du site principal**, partie Création du tunnel IPSec. Pour le site distant, les champs à renseigner dans l'assistant prennent les valeurs suivantes :

- **Réseau local :** Private_Net_Remote_Site,
- **Réseau distant :** Private_Net_Main_Site,
- **Passerelle distante :** Pub_Main_FW,
- **Clé pré-partagée :** le même mot de passe que celui renseigné sur le Firewall principal.

Créer les règles de filtrage

1. Dans le menu **Configuration > Politique de Sécurité > Filtrage et NAT**, sélectionnez votre politique de filtrage.
2. Dans l'onglet **Filtrage**, cliquez sur le menu **Nouvelle règle > Règle standard**.
   Dans le cas présenté, un poste client situé sur le réseau local du **site distant** doit pouvoir se connecter en HTTP au serveur intranet situé sur le réseau local du **site principal** (règle N°1).
   Vous pouvez également y ajouter temporairement, par exemple, le protocole ICMP afin de tester plus facilement l'établissement du tunnel (règle N°2). La règle de filtrage prend la forme suivante :



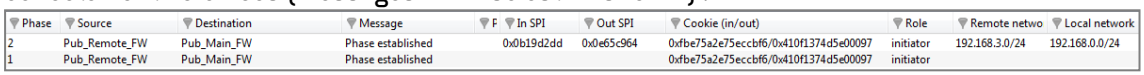
Vérifier l'établissement du tunnel

Depuis un poste client situé sur le site distant, saisissez l'URL de votre site intranet dans un navigateur web. Par exemple : *http://nom_site_intranet*.

Si vous avez autorisé le protocole ICMP dans les règles de filtrage, vous pouvez également faire un PING depuis le poste vers le serveur intranet.

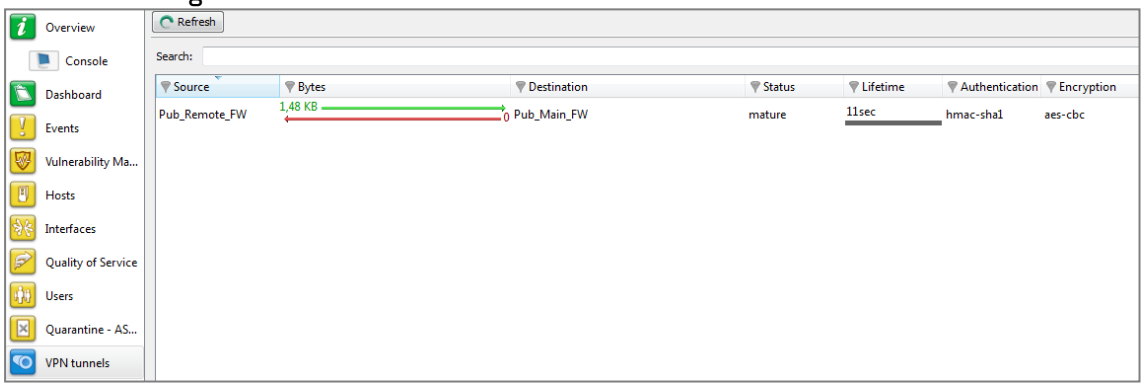
Vérifier dans Stormshield Network Real-Time Monitor

Lancez Stormshield Network Real-Time Monitor, connectez-vous au Firewall du site principal par le biais du logiciel et cliquez sur le module **Traces > VPN**. Vérifiez que les phases 1 et 2 se sont correctement déroulées (messages « Phase established ») :



Phase	Source	Destination	Message	F	In SPI	Out SPI	Cookie (in/out)	Role	Remote netwo	Local network
2	Pub_Remote_FW	Pub_Main_FW	Phase established		0x0b19d2dd	0x0e65c964	0xfbe75a2e75eccbf6/0x410f1374d5e00097	initiator	192.168.3.0/24	192.168.0.0/24
1	Pub_Remote_FW	Pub_Main_FW	Phase established				0xfbe75a2e75eccbf6/0x410f1374d5e00097	initiator		

Dans le module **Tunnels VPN,** vous pouvez également visualiser le tunnel ainsi que la quantité de données échangées :



Si ce n'est pas le cas, vous pouvez consulter la section Résolution d'incidents – Erreurs communes.

Résoudre les incidents – Erreurs communes

Dans la suite de cette section, le Firewall du site distant est appelé « initiator », car il est à l'origine de l'établissement du tunnel pour l'exemple choisi. Le Firewall du site principal est quant à lui nommé « responder ».

Symptôme : Le tunnel entre les équipements est bien établi mais aucun trafic ne semble l'emprunter.

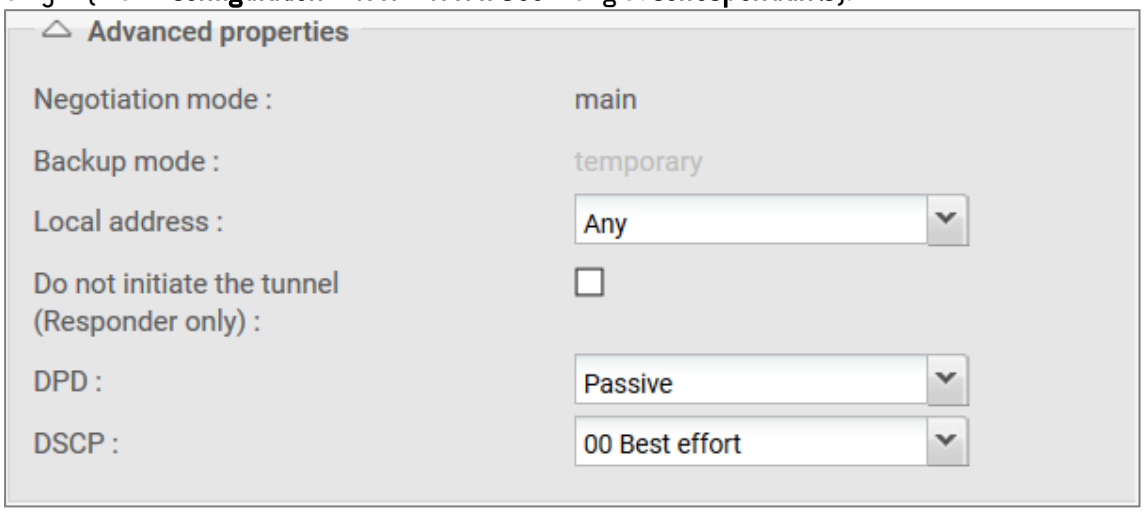
Solution : Vérifiez vos règles de filtrage sur le « responder ». Vérifiez également le routage entre les hôtes (poste client, serveur intranet) et leur passerelle respective (routage statique ou passerelle par défaut).

Symptôme : Le tunnel ne s'établit pas.

- Aucun message n'apparaît dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « initiator ».

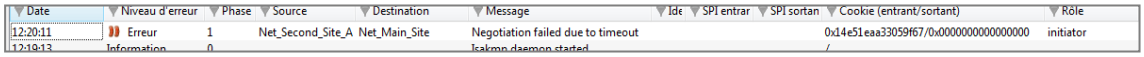
- Aucun message n'apparaît dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « responder ».

Solution : Vérifiez le routage entre les hôtes (poste client, serveur intranet) et leur passerelle respective (routage statique ou passerelle par défaut). Vérifiez vos règles de filtrage sur l'« initiator ». Vérifiez également que le tunnel de l' « initiator » n'est pas en mode « responder only » (menu **Configuration** > **VPN** > **VPN IPSec** > onglet **Correspondants**).



Symptôme : Le tunnel ne s'établit pas.

- Un message « Negotiation failed due to timeout » en phase 1 est présent dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « initiator ».

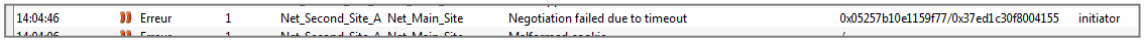


- Aucun message n'est présent dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « responder ».

Solution : La passerelle IPSec distante (« responder ») ne répond pas aux requêtes. Vérifiez que la politique VPN IPSec est activée sur le Firewall « responder ». Vérifiez que les objets correspondant aux extrémités de tunnel soient renseignés avec les bonnes adresses IP (généralement des adresses IP publiques).

Symptôme : Le tunnel ne s'établit pas.

- Un message « Negotiation failed due to timeout » en phase 1 est présent dans le module **Traces > VPN** de Stormshield Network Real-Time Monitor sur le Firewall « initiator ».

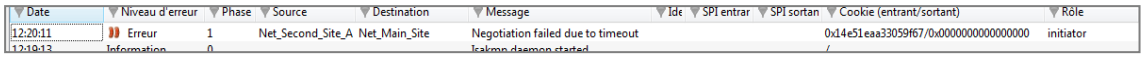


- Un message « Negotiation failed » en phase 1 est présent dans le module **Traces > VPN** de Stormshield Network Real-Time Monitor sur le Firewall « responder ».

Solution : Les équipements tentent de négocier mais ne parviennent pas à s'entendre sur une politique d'authentification. Vérifiez que la clé pré-partagée est bien identique sur les deux Firewalls.

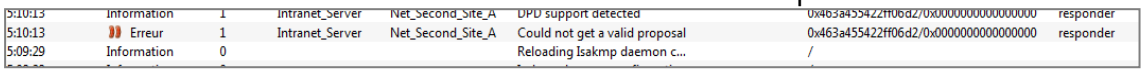
Symptôme : Le tunnel ne s'établit pas.

- Un message « Negotiation failed due to timeout » en phase 1 est présent dans le module **Traces > VPN** de Stormshield Network Real-Time Monitor sur le Firewall « initiator ».



Date	Niveau d'erreur	Phase	Source	Destination	Message	Ide	SPI entrar	SPI sortan	Cookie (entrant/sortant)	Rôle
12:20:11	Erreur	1	Net_Second_Site_A	Net_Main_Site	Negotiation failed due to timeout				0x14e51eaa33059f67/0x0000000000000000	initiator
12:19:13	Information	0			Isakmp daemon started				/	

- Un message « Could not get a valid proposal » en phase 1 est présent dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « responder ».

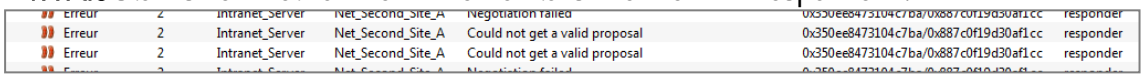


5:10:13	Information	1	Intranet_Server	Net_Second_Site_A	DPD support detected	0x463a45542Zff06d2/0x0000000000000000	responder
5:10:13	Erreur	1	Intranet_Server	Net_Second_Site_A	Could not get a valid proposal	0x463a455422ff06d2/0x0000000000000000	responder
5:09:29	Information	0			Reloading Isakmp daemon c...	/	

Solution : Les équipements tentent de négocier mais ne parviennent pas à s'entendre sur une politique de chiffrement en phase 1 (IKE). Vérifiez que le profil de chiffrement est bien identique sur les deux Firewalls (groupe Diffie-Hellman, durée de vie maximum...).

Symptôme : Le tunnel ne s'établit pas.

- Un message « Could not get a valid proposal » en phase 2 est présent dans le module **Traces > VPN de** Stormshield Network Real-Time Monitor sur le Firewall « responder ».



Erreur	2	Intranet_Server	Net_Second_Site_A	Negotiation failed	0x350ee8473104c7ba/0x887c0f19d30af1cc	responder
Erreur	2	Intranet_Server	Net_Second_Site_A	Could not get a valid proposal	0x350ee8473104c7ba/0x887c0f19d30af1cc	responder
Erreur	2	Intranet_Server	Net_Second_Site_A	Could not get a valid proposal	0x350ee8473104c7ba/0x887c0f19d30af1cc	responder

Solution : Les équipements tentent de négocier mais ne parviennent pas à s'entendre sur une politique de chiffrement en phase 2 (IPSEC). Vérifiez que le profil de chiffrement est bien identique sur les deux Firewalls (propositions d'authentification, de chiffrement…).

documentation@stormshield.eu