



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	. 3
Mise en œuvre	. 4
Configurer le site principal	. 4
Créer les objets réseau	. 4
Créer le tunnel IPSec	. 4
Créer les règles de filtrage	6
Configurer le site distant	. 7
Créer les objets réseau	. 7
Créer le tunnel IPSec	. 8
Créer les règles de filtrage	8
Vérifier l'établissement du tunnel	. 9
Vérifier dans Stormshield Network Real-Time Monitor	9
Résoudre les incidents – Erreurs communes	9



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.
- Choisissez la politique de chiffrement que vous souhaitez configurer. Vous avez la possibilité de la renommer en cliquant sur le bouton Éditer.

	PN / IPSEC \	/PN							
ENC	RYPTION POL	ICY - TUNNELS	PEER	RS I	DENTIFICATION	1	ENCRYPTION PR	ROFILI	ES
A (1)	IPsec 01	💌 🥀 Act	ivate this	s policy	Edit - 🛛 🕄				
6 +®+c	SITE-TO-SIT	E (GATEWAY-GATE	WAY)	⊳+⊕+0	Rename	e	SILE USERS		
Search	ed text	× + Add	• × c	Delete	Copy to	•	Cut 🖸 Copy	Pas	te
Line	Status	Local network		Peer		Rem	ote network		Encryption

- 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.

Local network :	Peer selection :	Remote network :
Private_Net_Main_Si 🗡 🛼	Select a peer	Private_Net_Remote. 🚩 🗳
	Create an IKEv1 peer	< >
	Create an IKEv2 peer	

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 :

Remote gateway :	Pub_Remote_FW
Name :	Site_Pub_Remote_FW

- 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 »).:

D+®+ C	SITE-TO-SITE (GATEWAY-GATEWAY)									
Search	Searched text 🛛 🔺 + Add - 🗙 Delete 🕴 🕇 Up 🖡 Down 🗌 🚰 Cut 🕝 Copy 🕙 Paste									
Line	ine Status Local network Peer Remote network Encry					Encryption profile	Keep alive	Comments		
1	🜑 on	on Private_Net_Main_Site		Site_Pub_Remote_FW Private_Net_Remote_Site		StrongEncryption	0			

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.



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*) :

General	SOURCE			
Action				
Source	GENERAL GEOLOCATIO	N / REPUTATION ADVANCED PROPERTIES		
Destination	Advanced properties			
Port - Protocol				
Inspection	Source port:	+ Add X Delete	θ.	
			•	
		Any		
	Via:	IPSec VPN tunnel		-
	source DSCP:	All		-

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 :

FILTERING	IPV4 NAT						
Searching		+ New rule	▪ X Delete ↑ ↓	🗶 🖓 🔁 Cut - [🔁 Copy 🛛 🐑 Pa	iste	
	Status ≞▼	Action 🚉	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	P Private_Net_Remote_Site via IPSec VPN tunnel	₽ <mark>₽</mark> intranet_server	Ï http		IPS
2	on	pass	P Private_Net_Remote_Site via IPSec VPN tunnel	₽ <mark>₽</mark> intranet_server	* Any	icmp	IPS
3 🚥	🜑 on	📀 pass	* Any	E Firewall_bridge	🟙 Admin_srv		IPS

🕦 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 :

FI	LTERING	3 I	PV4 NAT						
Searching				+ New rule	▪ X Delete ↑ ↓ →	🐔 🛃 🔂 Cut - 🛛	🕈 Copy 🛛 🕥 Pa	iste	
			Status 🚉	Action =	Source	Destination	Dest. port	Protocol	Security inspection
1	1 🚥	2	on	pass	Private_Net_Remote_Site	₽ intranet_server	🖞 http		IPS
2	2 🚥		💶 on	🕤 pass	Private_Net_Remote_Site	₽ <mark>₽</mark> intranet_server	* Any	icmp	IPS
:	3 🖽	-	💽 on	pass	* Any	Firewall_bridge	🟙 Admin_srv		IPS



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	V Source	Pestination	💎 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 :

1	Overview	C Refresh						
	Console	Search:						
	Dashboard	Source	🛡 Bytes	Destination	💎 Status	🛡 Lifetime	Authentication	Encryption
<u>.</u>	Events	Pub_Remote_FW	1,48 KBC) Pub_Main_FW	mature	11sec	hmac-sha1	aes-cbc
1	Vulnerability Ma							
Ľ	Hosts							
* *	Interfaces							
6	Quality of Service							
ι ή ΰ	Users							
	Quarantine - AS							
1	VPN tunnels							

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**).

△ Advanced properties		
Negotiation mode :	main	
Backup mode :	temporary	
Local address :	Any	~
Do not initiate the tunnel (Responder only) :		
DPD :	Passive	*
DSCP :	00 Best effort	¥

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 ».
 Voire Viveau d'erreur V Phase V Source V Destination V Message V ldc V SPI entrar V SPI sortan V Cookie (entrant/sortant) V Role
 12:20:11 Information 0
- 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 ».

 14.04.46
 10 Erreur
 1 Net_Second_Site_A Net_Main_Site
 Negotiation failed due to timeout
 0x05257b10e1159177/0x37ed1c30f8004155
 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 ».

Date	💎 Niveau d'erreur	💎 Phase	Source	Destination	♥ Message	▼Ide ▼SPI entrar ▼S ▼Cookie (entrant/sortant)	💎 Rôle	🔻 Réseau distant
4:28	3 Erreur	1	Intranet_Server	Net_Second_Site_A	Negotiation failed	0x05257b10e1159f77/0x37ed1c30f8004155	responder	
M-28	11 Freeur	1	Intranet Server	Net Second Site A	Negotiation failed	0v05257k10a1150f77/0v27ad1-20f800/1155	recoonder	

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 ».

V Date	Viveau d'erreur	Phase	Source	Destination	▼ Message	₹ Id€	SPI entrar	SPI sortan	Cookie (entrant/sortant)	V Rôle
12:20:11	33 Erreur	1	Net_Second_Site_A	Net_Main_Site	Negotiation failed due to timeout				0x14e51eaa33059f67/0x000000000000000	initiator
12-10-13	Information	0			Icakmo daemon started				1	

• 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	0x463a455422tt06d2/0x000000000000000	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 ».

1	JJ Erreur	4	intranet_Server	Net_Second_Site_A	ivegotiation failed	0X5500ee8475104C7ba/0X887C0T19050aT1CC	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
1	99 F	2	Internet Course	Mat Canad City A	Manadiation failed	0.250-0472104-71-00.007-000-00-01-0	

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

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2019. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.