

STORMSHIELD



VPN IPSEC : AUTHENTIFICATION PAR CERTIFICATS

Produits concernés : SNS 3.x, SNS 4.x Dernière mise à jour du document : 9 décembre 2019 Référence : sns-fr-VPN_IPSec_Authentification_Certificats_Note_Technique





Table des matières

Avant de commencer	
Mise en œuvre	4
Configurer le site principal	
Créer les objets réseau	4
Créer l'infrastructure PKI	4
Créer les tunnels IPsec	7
Mettre en place les règles de filtrage	
Configurer les sites distants A et B	
Créer les objets réseau	
Importer les éléments d'authentification	
Créer les tunnels IPsec	11
Mettre en place les règles de filtrage	12
Vérifier l'établissement du tunnel	
Vérification dans Stormshield Network Realtime Monitor	13
Résolution d'incidents – Erreurs communes	
Pour aller plus loin	





Avant de commencer

Vous souhaitez mettre en relation de manière sécurisée différents sites de votre entreprise reliés via Internet.

Pour cela, vous devez créer une configuration VPN IPsec Site à Site en étoile. La méthode d'authentification présentée dans ce didacticiel repose sur la vérification de certificats (l'authentification par clé prépartagée aurait également pu être mise en œuvre).

Ce document décrit la configuration à réaliser, afin d'autoriser les postes clients de deux sites distants à accéder en HTTP à un serveur intranet du site principal au travers d'un tunnel VPN. Il est bien entendu que ce type d'architecture ne se limite pas à trois sites.

L'autorité de certification sera hébergée par l'une des trois passerelles lPsec en jeu: le firewall du site principal.







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 de l'ensemble des sites à connecter,
- Créer l'infrastructure PKI,
- Créer les tunnels IPsec,
- Mettre en place les règles de filtrage autorisant les flux entre sites.

Créer les objets réseau

La création d'une connexion VPN IPSEC entre ces trois entités nécessite à minima sept 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 A: Private Net Site A,
- l'adresse publique du Firewall du site distant A: Pub_FW_Site_A,
- le réseau local du site distant B: Private Net Site B,
- l'adresse publique du Firewall du site distant B: Pub_FW_Site_B,
- le serveur intranet à joindre sur le site principal: Intranet server.

Ces objets doivent être définis sur chacun des Firewalls à mettre en relation, via le menu : **Configuration** > **Objets** > **Objets réseau**.

Créer l'infrastructure PKI

Autorité de Certification (CA)

- 1. Cliquez sur Ajouter > Ajouter une autorité racine :
- 2. Renseignez les différents champs obligatoires de l'assistant de création :
 - CN : le nom de votre autorité de certification,
 - Identifiant : le nom entré dans le champ CN est proposé par défaut,
 - Organisation (0). Exemple : le nom de votre entreprise,
 - Unité d'organisation (OU). Exemple : le nom du service utilisateur de la CA,
 - État ou province (ST),
 - Pays (C).





Γ

CREATE	ROOT	AUTHORITY	
the state of the s			

CN:	documentation.stormshiek
Identifier:	documentation.stormshiek
Autority attributes	
Organization:	stormshield.eu
Organizational unit:	documentation
City (L):	VdA
State (ST):	North
Country:	France 💌
	★ CANCEL ≪ PREVIOUS → NEXT

- 3. Complétez ensuite les champs :
 - Mot de passe (nécessaire lors de la création de certificats),
 - E-mail (optionnel),
 - Taille de clé (2048 octets par défaut),
 - Validité (365 jours par défaut).
- 4. Il vous est possible de définir les URI des points de distribution des CRL (Listes de Révocation de Certificats).

Listes de Révocation de Certificats (CRL)

- 1. Sélectionnez votre CA
- 2. Cliquez sur Actions > Créer CRL.
- 3. L'assistant vous demande le mot de passe de l'autorité de certification. Saisissez-le et cliquez sur **Créer CRL** pour valider.
- 4. Téléchargez ensuite la CRL (fichier au format PEM) afin de l'importer ultérieurement sur les Firewalls distants.







SOBJECTS / CERTIFIC	ATES AND PKI						
Q Enter a filter	∗ Filter: all	- x ^k − x ⁿ	+ Add -	× Revoke	=	Actions 🔹 📔 🛱 Do	wnload
🗄 🗈 sslvpn-full-default-autho	rity		PEVOCATIO		۲	Create CRL	
documentation.stormsh	DETAILS	REVOCATION		×	Remove CRL	-	
		Validity			×	Remove private key	-
	Issued:				Set as default	GMT	
					r	LDAP publication	
		Expires:			N	lov 25 08:47:56 2029	GMT

Certificat du Firewall principal

Dans le menu Configuration > Objets > Certificats et PKI :

- 1. Cliquez sur Ajouter > Identité serveur.
- Renseignez le champ Nom de domaine qualifié avec le nom FQDN du Firewall principal. Le champ Identifiant propose par défaut ce même nom.
- 3. Indiquez la durée de Validité et la Taille de clé.
- 4. Cliquez sur la loupe du champ **Autorité de Certification** et sélectionnez votre CA pour signer ce certificat.
- Renseignez ensuite le mot de passe de l'autorité de certification. Les attributs du certificat sont importés automatiquement; il vous est néanmoins possible de les modifier.
- 6. L'assistant présente un résumé du certificat : cliquez sur Terminer pour le fermer.

Certificat des Firewalls distants

Procédez à la création des certificats serveurs des Firewalls distants en suivant la méthode précédemment décrite.

Exporter les données de sécurité des sites distants

- 1. Sélectionnez le certificat d'un des deux Firewalls distants.
- 2. Cliquez sur Téléchargement > Certificat et choisissez le fichier souhaité.
- 3. Après avoir saisi un mot de passe pour le protéger, téléchargez le certificat en cliquant sur l'hyperlien proposé.
- 4. Stockez-le sur votre poste d'administration.
- 5. Procédez de la même manière pour exporter le certificat du deuxième Firewall distant.

S OBJECTS / CERTIFICATES AND PKI												
Q Enter a filter Filter: all	$\mathbf{x} = \mathbf{x}_{\mathbf{x}} = \mathbf{x}_{\mathbf{x}}$	+ Add - X Rev	oke 🗮 Actions 🕶	C,	Download 🔻 👁							
	DETAILS	REVOCATION (CR	as PEM file	•	Certificate							
□ I documentation.stormshield.eu	DETAILO	REVOCATION (ON	as DER file	٩	Identity							
SpokeA	Validity				CRL							
D SpokeB	Issued:	Nov 28 09:07:13 2019 GMT										
BFW-Site-A.documentation.stormshield.eu	Expires:	s: Nov 27 09:07:13 2020 GMT										





Créer les tunnels IPsec

Ajouter la CA dans les autorités de confiance

Dans le menu Configuration > VPN > VPN IPsec > onglet Identification :

- 1. Dans le bloc Autorités de Certification Acceptées, cliquez sur Ajouter.
- 2. Sélectionnez votre CA.
- 3. Sauvegardez.

Créer les correspondants lPsec

Dans le menu Configuration > VPN > VPN IPsec :

- 1. Sélectionnez l'onglet Correspondants.
- 2. Cliquez sur Ajouter.
- 3. Cliquez sur **Nouveau Site distant IKEv1** ou **Nouveau Site distant IKEv2** selon la version du protocole IKE utilisée.
- L'assistant vous invite à sélectionner la passerelle distante. Ici, il s'agit de l'adresse publique du premier Firewall distant (objet Pub_FW_Site_A).
 Par défaut, le nom du correspondant est créé en préfixant cet objet avec « Site_ »; ce nom est personnalisable.

Remote gateway :	Pub_FW_Site_A
Name :	Site_Pub_FW_Site_A

- 5. Validez.
- 6. Cochez la case Certificat.
- 7. Cliquez sur la loupe du champ Certificat.
- Sélectionnez celui correspondant au Firewall principal.
 Le champ Autorité de confiance est automatiquement fourni par le certificat.
- 9. L'assistant vous propose un résumé du correspondant que vous venez de créer. Cliquez sur **Terminer** pour fermer cette fenêtre.
- 10. Cliquez à nouveau sur Terminer pour fermer l'assistant.
- 11. Répétez l'ensemble de ces opérations pour la création du correspondant lPsec du site distant B.

Sélectionner la politique de chiffrement et ajouter les tunnels VPN

Dans le menu Configuration > VPN > VPN IPsec > onglet Politique de chiffrement – Tunnels :



- 1. Choisissez la politique de chiffrement que vous souhaitez configurer.
- 2. Vous avez la possibilité de la renommer en cliquant sur le bouton Éditer.
- 3. Cliquez ensuite sur Ajouter afin de définir les tunnels IPsec.
- Choisissez le modèle Configuration en étoile.
 Un assistant de création se lance automatiquement.
- 5. Dans le champ Réseau local, sélectionnez votre objet Private_Net_Main_Site,
- 6. Dans le tableau Sites Distants, cliquer sur Ajouter pour sélectionner le premier correspondant en lui associant son réseau (Site Pub_FW_Site A et Private Net Site A). Les correspondants peuvent être directement créés au sein de cet assistant en cliquant sur >> puis Créer un correspondant.
- Répétez les opérations 3 à 6 pour le second correspondant (Site_Pub_FW_Site_B et Private_ Net_Site_B),



🕕 IMPORTANT

Veillez à ne pas cocher la case **Considérer l'(es) interface(s) IPsec comme interne(s) (s'applique à tous les tunnels)**. Cette option empêcherait l'établissement des tunnels entre les sites distants et le site principal (elle ne peut être utilisée que dans le cadre d'une configuration de type Hub & Spoke). Si vous avez coché cette case par erreur, rendez-vous dans la fenêtre **Configuration avancée** du module **Profils d'inspection** (menu **Protection applicative**) et décochez la case **Considérer l'(es) interface(s) IPsec comme interne(s) (s'applique à tous les tunnels - les réseaux distants devront être explicitement légitimés)**.

- Validez en cliquant sur Terminer. La définition des tunnels IPsec est terminée sur le site principal et les tunnels sont automatiquement activés (État à « on »).
- 9. Vous pouvez désormais cliquer sur Activer cette politique.







ENC	RYPTION	POLIC	Y - TUNNELS	PEER	S IDENTIFICATIO	N ENCRYPTI	ON PROFILI	ES				
🔔 (1)	(1) IPsec 01 ▲ Activate this policy Edit • • ▲ Activate this policy											
₽+® +c	SITE-TO-SITE (GATEWAY-GATEWAY)											
Search	Searched text × HAdd × Delete 1 Up I Down 2 Cut C Copy Paste											
Line	Status	L	ocal network		Peer	Remote network		Encryption profile	Ke	ep alive		
1 ×	Star co	onfigurat	tion: start									
2	💽 on	()	Private_Net_Main_S	Site	Site_Pub_FW_Site_A	Private_Net_Site_	A	StrongEncryption	0			
3	💽 on	()	Private_Net_Main_S	Site	Site_Pub_FW_Site_B	Private_Net_Site_	В	StrongEncryption	0			
4 ×	Star co	onfigurat	tion: end									

Mettre en place 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 autorisés entre ces deux entités. C'est la raison pour laquelle des règles de filtrages doivent être mises en place afin de n'autoriser que les flux nécessaires entre des machines sources et destinations identifiées.

Dans le menu Configuration > Politique de Sécurité > Filtrage et NAT:

- 1. Sélectionnez votre politique de filtrage.
- 2. Dans l'onglet Filtrage, cliquez sur le menu Nouvelle règle > Règle standard.
- 3. Renseignez les champs Action, Source, Destination et Port destination.

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	ON / REPUTATION ADVANCED PROPERTIES		
Destination	Advanced properties			
Port - Protocol				
Inspection	Source port:	+ Add × Delete	θ.	
		Any		
	Via:	IPSec VPN tunnel		-
	source DSCP:	All		-

Dans le cas présenté, les postes clients des sites distants doivent 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).

Sur le site principal, les règles de filtrage prendront la forme suivante :







FILTE	RING	IPV4 NAT								
Searchi	ing		+ New rule	▪ X Delete ↑	🌲 🛛 🖈 🖉 🖓 Cut	🗁 Copy 🛛 🐑 Pi	aste 🖳	Search in logs 🛛 🗠	Search in monito	ring \equiv •
		Status 🚉	Action 🖃	Source	Destination	Dest. port	Protocol	Security inspection	<u>=</u> *	Comments
1		on	pass	P Private_Net_Site_A P Private_Net_Site_B via IPSec VPN tunnel	며 Intranet_Server	1 http		IPS		Created on
2		on	pass	P Private_Net_Site_A P Private_Net_Site_B via IPSec VPN tunnel	□ <mark>월</mark> Intranet_Server	* Any	icmp	IPS		Created on
3		🜑 on	🕤 pass	🛎 Any	Firewall_bridge	🕍 Admin_srv		IPS		Created on

1 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 les sites distants A et B

Sur chaque site distant, il est nécessaire de :

- Créer les objets réseau du site local et du site principal,
- Importer la CRL et le certificat destiné au firewall local,
- Créer les tunnels IPsec,
- Mettre en place les règles de filtrage.

Créer les objets réseau

Définissez les cinq objets réseau nécessaires via le menu : **Configuration** > **Objets** > **Objets réseau**.

Sur le site distant A :

- 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 A: Private Net Site A,
- L'adresse publique du Firewall du site distant A: Pub FW Site A,
- Le serveur intranet à joindre sur le site principal: Intranet server.

Sur le site distant B :

- 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 B: Private Net Site B,
- L'adresse publique du Firewall du site distant B: Pub_FW_Site_B,
- Le serveur intranet à joindre sur le site principal:Intranet_server.

Importer les éléments d'authentification

Importer le certificat sur chaque Firewall distant

- 1. Cliquer sur Ajouter > Importer un fichier.
- 2. Sélectionnez le certificat correspondant au Firewall et renseignez son mot de passe.







IMPORT FILE	
File to import:	C:\FW-Site-A.documentation.stormshiel
File format:	P12
	O DER
	O PEM
File password:	
What to import:	All
	O Certificate(s)
	O Private key(s)
	O CRL
	O CA
	Overwrite existing content
	X CANCEL VIMPORT

Importer la CRL

Dans le menu Configuration > Objets > Certificats et PKI :

- 1. Cliquer sur Ajouter > Importer un fichier.
- 2. Sélectionner le fichier de la CRL exportée précédemment et renseignez son mot de passe.

Créer les tunnels IPsec

Ajouter la CA dans les autorités de confiance

Reportez-vous à la section Configuration du site principal, partie Ajouter la CA dans les autorités de confiance.

Créer le correspondant lPsec

Sur chaque site distant, définissez le correspondant lPsec du site principal.

Pour ce faire, reportez-vous à la section **Configuration du site principal**, partie **Créer les correspondants IPsec**.

Les objets à sélectionner sont les suivants :

Sur le site distant A :

- Réseau local : Private_Net_Site_A,
- Champ Correspondant : Pub_Main_FW,
- Champ Réseaux distants : Private_Net_Main_Site.

Sur le site distant B :

- Réseau local :Private_Net_Site_B,
- Champ Correspondant : Pub_Main_FW,
- Champ Réseaux distants : Private_Net_Main_Site.





Choisir la politique de chiffrement et ajout du tunnel VPN

Dans le menu Configuration > VPN > VPN IPsec > onglet Politique de chiffrement – Tunnels :

- 1. Choisissez la politique de chiffrement que vous souhaitez configurer.
- 2. Vous avez la possibilité de la renommer en cliquant sur le bouton Éditer.
- 3. Cliquez sur Ajouter afin de définir le tunnel IPsec.
- 4. Choisissez le modèle **Tunnel site à site**.
- 5. Renseignez les champs de l'assistant de création avec les valeurs adaptées à chacun des sites distants.

Sur le site distant A :

- Réseau local : Private_Net_Site_A,
- Réseau distant : Private Net Main Site,
- Passerelle distante : Pub Main FW,
- Certificat : le certificat créé pour le Firewall distant du site A.

Sur le site distant B :

- Réseau local : Private_Net_Site_B,
- Réseau distant : Private_Net_Main_Site,
- Passerelle distante : Pub_Main_FW,
- Certificat : le certificat créé pour le Firewall distant du site B.

Mettre en place les règles de filtrage

Dans le menu Configuration > Politique de Sécurité > Filtrage et NAT :

- 1. Sélectionnez votre politique de filtrage.
- 2. Dans l'onglet Filtrage, cliquez sur le menu Nouvelle règle > Règle standard.
- 3. Renseignez les champs Action, Source, Destination et Port destination.

Dans le cas présenté, les postes clients des sites distants doivent 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).

Les règles de filtrage prendront la forme suivante :

Sur le site distant A :

FILTER	RING	IPV4 NAT								
Searchi	ng		+ New rule	▪ X Delete ↑ ↓	💉 🖉 🔄 Cut	🔁 Copy 🛛 👻 Pa	iste 🖳	Search in logs 🛛 🖓 S	earch in monito	ring \equiv -
		Status 🚉	Action 🚉	Source	Destination	Dest. port	Protocol	Security inspection	<u>=</u> *	Comments
1		on	🕤 pass	Private_Net_Site_A	📲 Intranet_Server	İ http		IPS		Created on
2		on	📀 pass	Private_Net_Site_A	₽ <mark>₽</mark> Intranet_Server	* Any	icmp	IPS		Created on
3		🜑 on	🕑 pass	🗶 Any	Firewall_bridge	🟙 Admin_srv		IPS		Created on

Sur le site distant B :

FILTERI	NG	IPV4 NAT									
Searching]		+ New rule	▪ X Delete ↑	$1 \mid \mathbf{s}$	🛀 🖉 🔄 Cut	🗁 Copy 🛛 🐑 F	Paste 🖳	Search in logs	Search in monito	oring \equiv -
		Status 🚉	Action 🚉	Source		Destination	Dest. port	Protocol	Security inspec	tion 🚉	Comments
1		on	🕤 pass	Private_Net_Site_B		□ Intranet_Server	🕇 http		IPS		Created on
2		💽 on	🕤 pass	Parivate_Net_Site_B		Intranet_Server	* Any	icmp	IPS		Created on
3	æ	🜑 on	📀 pass	▲ Any		Firewall_bridge	🟙 Admin_srv		IPS		Created on





sns-fr-VPN_IPSec_Authentification_Certificats_Note_Technique - 09/12/2019



Vérifier l'établissement du tunnel

Depuis un poste client situé sur chacun des sites distants, 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.

Vérification dans Stormshield Network Realtime Monitor

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

Frror level	💎 Phase	V Source	Destination	🛡 Message	₹ P	💎 In SPI	🛡 Out SPI	🛡 Cookie (in/out)	💎 Role
Information	2	Pub_Main_FW	Pub_FW_Site_A	Phase established		0x0b177225	0x0327a8f0	0x07ba826eae24b615/0x227a3bd376801377	responder
Information	1	Pub_Main_FW	Pub_FW_Site_A	INITIAL-CONTACT received				0x07ba826eae24b615/0x227a3bd376801377	responder
Information	1	Pub_Main_FW	Pub_FW_Site_A	Phase established				0x07ba826eae24b615/0x227a3bd376801377	responder

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

i	Overview	C Refresh					Firewall :	10.3.30.252 Pw-
	Dashboard	Search:						
7	Events	Source Source	Bytes	Destination	Visit Status	🛡 Lifetime	Authentication	Encryption
V	Vulnerability Ma	Pub_Main_FW	200,64 KB 57,18 KB	Pub_FW_Site_A	mature	2m 41sec -	hmac-sha1	aes-cbc
8	Hosts							
\$ \$	Interfaces							
R	Quality of Service							
i ĝij	Users							
×	Quarantine - AS							
0	VPN tunnels							

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

Résolution d'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. 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 Realtime Monitor sur l'IPS-Firewall « initiator ».
- Aucun message n'apparaît dans le module Traces > VPN de Stormshield Network Realtime Monitor sur l'IPS-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 » (onglet *Correspondants* du menu **Configuration** > **VPN** > **VPN IPsec**).

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 ».

Error	1	Pub_FW_Site_A	Pub_Main_FW	Negotiation failed due to timeout	0x931bbf24cbe49312/0x000000000000000	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.

Symptôme: Le tunnel ne s'établit pas.

 Les messages « Negociation failed » et « Certificate with serial XXX from issuer YYY: unable to get local issuer certificate » (en phase 1) sont présents dans le module Traces > VPN de Stormshield Network Real-Time Monitor sur le Firewall « responder »:

Erreur 1 Private_Net_Mail_Private_Net_S... Negotiation failed
 Orba28b2f6beb1ad51/0xc020addb0900dda responder
 Erreur 1 Certificate with serial 89A77294 from issuer /C=FR/ST= CN=... /

Solution: le Firewall « responder » ne peut vérifier la validité du certificat du Firewall « initiator ». Vérifiez que vous avez bien défini la CA comme autorité de confiance sur le « responder » (onglet Identification du menu **Configuration** > **VPN** > **VPN IPsec**).

Symptôme: Le tunnel ne s'établit pas.

Page 14/17





• Les messages « Negociation failed » et « Certificate with serial XXX from issuer YYY: unable to get local issuer certificate » (en phase 1) sont présents dans le module **Traces** > **VPN** de Stormshield Network Real-Time Monitor sur le Firewall « initiator »:

▼Niveau c ▼F ▼Source ▼Destination ▼Message		Ÿ	I 🛡 S 🛡 S 🛡 Cookie (entrant/sortant)	💎 Rôle
Erreur 1 Certificate with serial 89A77293 from	uer /C=FR/ST=	′CN=	/	
Erreur 1 Net_Second_Site_A Net_Main_Site Negotiation failed			0x72715ffb63449fb9/0xd813a1bc50d8b1f4	initiator

Solution: le Firewall « initiator » ne peut vérifier la validité du certificat du Firewall « responder ». Vérifiez que vous avez bien défini la CA comme autorité de confiance sur l' « initiator » (onglet *Identification* du menu **Configuration** > **VPN** > **VPN IPsec**).









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









documentation@stormshield.eu

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

Copyright © Stormshield 2022. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.



