



# VPN IPSEC : CONFIGURATION HUB AND SPOKE

Produits concernés : SNS 2 et versions supérieures Date : 19 juin 2019 Référence : sns-fr-VPN\_IPSec\_Hub\_And\_Spoke\_Note\_Technique





# Table des matières

VPN IPSec : Configuration Hub and Spoke	3
Architectures présentées	3
Cas Nº 1 : trafic interne via les tunnels IPSec	. 3
Cas Nº2 : trafic total via les tunnels IPSec	. 3
Prérequis de configuration	. 5
Cas Nº1 : trafic interne via les tunnels IPSec	. 6
Paramétrer le site Hub	. 6
Créer le correspondant Site_Spoke_A.	. 6
Créer le correspondant Site_Spoke_B.	. 6
Créer les tunnels	. ?
Règles de filtrage	. 7
Regie de NAT	8 Q
Définir le correspondant IPSec	. 0 . 8
Création des tunnels	. 9
Règles de filtrage	. 9
Règle de NAT	10
Cas Nº2 : trafic total via les tunnels IPSec	11
Paramétrer le site central Hub	. 11
Définir les correspondants IPSec	. 11
Créer les tunnels	. 11
Regles de filtrage	.12
Paramétrer les sites satellites Snoke A et Snoke B	13
Définir le correspondant IPSec	13
Créer les tunnels	.13
Règles de filtrage	.13
Vérifier l'établissement des tunnels	15
Via la suite d'administration Stormshield Network	.15
Outils d'informations et de diagnostic en console	.16
Commande showSPD	. 16
Commande showSAD	. 16
Resolution d'incidents – Erreurs communes	. 17



# VPN IPSec : Configuration Hub and Spoke

### Architectures présentées

La méthode d'authentification choisie dans ce didacticiel est basée sur les certificats.

Pour le détail des opérations concernant la PKI, référez-vous au didacticiel « Mise en œuvre VPN IPSec - authentification par certificats ».

Dans la suite de ce document, le site central sera dénommé « Hub », les deux sites satellites étant représentés par « Spoke A » et « Spoke B ». Il est bien entendu que ce type d'architecture ne se limite pas à deux sites satellites.

Veuillez noter que dans la configuration présentée ici, les deux site satellites possèdent chacun un seul réseau local.

### Cas Nº 1 : trafic interne via les tunnels IPSec

Seul le trafic interne entre les trois sites (Hub, Spoke A et Spoke B) passe au travers de tunnels via le Hub. Les flux Internet sont gérés localement sur chaque site.



Cette infrastructure peut parfois être préférée à celle présentée dans le cas n°2 pour des raisons économiques notamment: un accès internet centralisé sur le site Hub peut nécessiter un très gros débit et donc s'avérer plus onéreux qu'un ensemble d'accès Internet de capacité plus réduite.

### Cas Nº2 : trafic total via les tunnels IPSec

L'ensemble du trafic passe par le site Hub au travers de tunnels. L'accès Internet est centralisé au niveau du Hub.





Cette infrastructure présente l'avantage d'une gestion centralisée de l'accès Internet et de la politique de sécurité associée.



# Prérequis de configuration

Dans ce didacticiel, les réseaux privés des 3 sites sont totalement distincts (exemple : 192.168.0.0/24, 192.168.1.0/24 et 192.168.2.0/24).

Les objets réseau nécessaires ont été créés sur chacun des sites à mettre en relation:

- l'adresse IP publique du Firewall Hub:Pub FW Hub,
- le réseau local du site Hub: Private Net Hub,
- l'adresse IP publique du Firewall Spoke A: Pub FW Spoke A,
- le réseau local du site Spoke A: Private Net Spoke A,
- l'adresse IP publique du Firewall Spoke B: Pub\_FW\_Spoke\_B,
- le réseau local du site Spoke B: Private Net Spoke B.

Vous avez mis en place votre PKI :

- Vous disposez d'une autorité de certification (CA),
- Vous avez créé les certificats des Firewalls,
- · Vous avez importé sur les Firewalls des sites Spoke leur certificat respectif,
- Vous avez ajouté la CA dans les autorités de confiance sur chacun des Firewalls à mettre en relation.



# Cas Nº1 : trafic interne via les tunnels IPSec



# Paramétrer le site Hub

### Créer le correspondant Site\_Spoke\_A.

Dans l'onglet Correspondants du menu Configuration > VPN > VPN IPSec :

- 1. Cliquez sur Ajouter.
- Choisissez Nouveau site distant.
   L'assistant vous invite à sélectionner la passerelle distante. Ici, il s'agit de l'adresse publique du Firewall du site Spoke A (objet Pub\_FW\_Spoke\_A).
- 3. Par défaut, le nom du correspondant est créé en préfixant cet objet avec « Site\_»; ce nom est personnalisable. Validez.
- 4. Choisissez la méthode Certificat.
- 5. Cliquez sur la loupe du champ Certificat.
- 6. Sélectionnez le certificat correspondant au Firewall Hub. Le champ **Autorité de confiance** est automatiquement fourni par le certificat.

	Oertificate	Select a certificate	×
	Pre-shared key (PSK)	Search	
Certificate :	Certificate × 🔎	SSL proxy default authority	
Pre-shared key (ASCII) :		✓ ① Documentation	
Confirm :		🔥 SpokeA	
		🐌 SpokeB	
		🛃 Hub	

# Créer le correspondant Site\_Spoke\_B.

De la même manière, créez le correspondant Site Spoke B en utilisant les valeurs suivantes :

- Passerelle distante : le Firewall du site Spoke B (objet Pub\_FW\_Spoke\_B),
- Certificat : le certificat du Firewall Hub.



### **Créer les tunnels**

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

- 1. Cliquez sur Ajouter.
- 2. Choisissez Tunnel site à site.
- 3. Suivez l'assistant pour définir le tunnel destiné au trafic entre sites Spoke A et Spoke B:
  - Dans le champ Réseau local, choisissez Private Net Spoke A,
  - Dans le champ Choix du correspondant, sélectionnez Site Spoke B,
  - Dans le champ Réseau distant, choisissez Private\_Net\_Spoke\_B,
  - Cliquez sur Terminer.
- 4. Procédez à l'identique pour créer les trois autres tunnels:
- Private Net Spoke B=> Site Spoke A => Private Net Spoke A,
- Private\_Net\_Hub => Site\_Spoke\_A => Private\_Net\_Spoke\_A,
- Private Net Hub => Site Spoke B=> Private Net Spoke B.

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES									
<b>A</b> (8)	🤱 (8) Hub & Spoke - Internal 🔽 🕂 Activate this policy   Edit 🗸   🛄								
	SITE-TO-S	TTE (GATEWAY-GATEWAY)	- ANONYMOUS - MOBILE	USERS					
Search	Searched text 🗴 🛨 Add - 🙁 Delete   🕇 Up 👃 Down   🚰 Cut 🚰 Copy 🕾 Insert								
Line	Stat	Local network	Peer	Remote network	Encryption profile				
1	9 .	Tunnel pour le trafic de Spoke A	A vers Spoke B						
2	🔵 on 👁	Private_Net_Spoke_A	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption				
3	в .	Tunnel pour le trafic de Spoke B	vers Spoke A						
4	🔵 on 🔍	Private_Net_Spoke_B	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption				
5	Ξ.	Tunnel pour le trafic de Hub ver	's Spoke A						
6	🔵 on 👁	Private_Net_Hub	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption				
7	Ξ.	Tunnel pour le trafic de Hub ver	s Spoke B						
8	🔵 on 👁	Private_Net_Hub	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption				

### Règles de filtrage

Définissez les règles de filtrage nécessaires au dialogue entre sites Spoke, sites Spoke et Hub ainsi qu'au trafic local vers Internet :



FILTERIN	G NAT									
Searched	text	× 🕴 + New rule -	🛛 Delete   🕇 Up 🤳 Down   🛅 I	Expand all 🔚 Collapse all 🛛	🚰 Cut 😭 Copy 🧐 Paste					
	Status 🖃	Action =	Source	Destination	Dest. port	Protocol	Security inspection			
😑 Accè	J Accès au réseau de Hub depuis Spoke A et Spoke B (trafic entrant)									
1	🔵 on	🕺 📄 pass	명 Private_Net_Spoke_A 명 Private_Net_Spoke_B via IPSec VPN tunnel	며 <mark>읍</mark> Private_Net_Hub	🐮 Any		IPS			
🖃 Accè	s aux réseaux de	Spoke A et Spoke B	depuis Hub (trafic sortant)							
2	🔵 on	🕺 📄 pass	Private_Net_Hub	Private_Net_Spoke_A	Any		PS			
😑 Accè	s de Spoke A au i	réseau de Spoke B (t	rafic traversant)							
3	🔵 on	🕺 📄 pass	며읍 Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	Any		IPS			
😑 Accè	s de Spoke B au r	éseau de Spoke A (t	rafic traversant)							
4	🔵 on	🕺 📄 pass	며읍 Private_Net_Spoke_B via IPSec VPN tunnel	며 Private_Net_Spoke_A	Any		IPS			
😑 Accè	s Internet local du	site Hub (trafic sorta	nt)							
5	🔵 on	∱ pass	역 Private_Net_Hub	💿 Internet	I http I https I dns		IPS			
😑 Admir	istration du FW									
6	🔵 on	1 pass	I Any	* Any	Mdmin_srv		IPS			

# Règle de NAT

Pour permettre l'accès à Internet des machines du réseau Private\_Net\_Hub, créez la règle de NAT suivante :

F	FLTERNG NAT										
Se	Searched text 🗙 + New rule - 🖸 Delete   🕇 Up 🦆 Down   🖺 Expand all 🗮 Collapse all   🔗 Cut 🚱 Copy 🧐 Paste										
			Original traf	Original traffic (before translation)			Traffic after translation				
		Status 🖃	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Options
1		🔵 on	며음 Private_Net_Hub	<ul> <li>Internet</li> <li>interface: out</li> </ul>	🔳 Any	•	Pub_FW_Hub	⊀ 🖞 ephemeral	🔳 Any		

# Paramétrer les sites satellites Spoke A et Spoke B

Dans une configuration de type Hub and Spoke, un site satellite ne connaît qu'un seul correspondant IPSec : le Firewall du Hub.

# Définir le correspondant IPSec

#### Site Spoke A

En suivant la méthode décrite au paragraphe **Paramétrage du site Hub > Définition des** correspondants IPSec, créez le correspondant Site FW Hub en utilisant les valeurs suivantes :

- passerelle distante : le Firewall du site Hub (objet Pub FW Hub),
- certificat : le certificat du Firewall Spoke A.

#### Site Spoke B

En suivant la méthode décrite au paragraphe **Paramétrage du site Hub > Définition des** correspondants IPSec, créez le correspondant Site FW Hub en utilisant les valeurs suivantes :

- passerelle distante : le Firewall du site Hub (objet Pub\_FW\_Hub),
- certificat : le certificat du Firewall Spoke B.



# Création des tunnels

### Site Spoke A

En suivant la méthode décrite au paragraphe **Paramétrage du site Hub > Création des tunnels**, créez les deux tunnels nécessaires :

-	SITE-TO-SITE (GATEWAY-GATEWAY)									
Searc	Searched text 🗙 🕂 Add - 🛛 Delete   🕇 Up 👃 Down   🚰 Cut 🚰 Copy 🖓 Insert									
Line	Stat Local network	Peer	Remote network	Encryption profile						
1	Image: Tunnel pour le trafic er	tre Spoke A et Hub								
2	🔵 on 🔍 Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Hub	GoodEncryption						
3	Tunnel pour le trafic er	tre Spoke A et Spoke B								
4	🔵 on 🔍 Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Spoke_B	GoodEncryption						

### Site Spoke B

En suivant la méthode décrite au paragraphe Paramétrage du site Hub > Création des tunnels, créez les deux tunnels nécessaires :

-	SITE-TO-SITE (GATEWAY-GATEWAY)									
Searched text × + Add - Z Delete   † Up ↓ Down   🚱 Cut 🔂 Copy 🗐 Insert										
Line	Stat Local network	Peer	Remote network	Encryption profile						
1	Interpretation of the second secon	oke B et Hub								
2	🔵 on 🔍 Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Hub	GoodEncryption						
3	Tunnel pour le trafic entre Sp	oke B et Spoke A								
4	🔵 on 🔍 Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Spoke_A	GoodEncryption						

# Règles de filtrage

Dans ce didacticiel, le trafic entre les réseaux privés n'est volontairement pas précisé (port destination : ANY). Pour des raisons d'optimisation de performances (économie de bande passante et de ressources machine), il est important d'affiner le filtrage sur les sites satellites (protocoles, ports... autorisés) afin d'éviter de laisser transiter des paquets inutiles dans les tunnels. Cette politique de filtrage sera également présente sur le site Hub.

### Site Spoke A

Définissez les règles de filtrage nécessaires au dialogue entre Spoke A et Spoke B, Spoke A et Hub ainsi qu'au trafic local vers Internet :

FIL	FLITERING NAT									
Sea	Searched text 🛛 🖌 New rule - 😫 Delete   🕇 Up 👃 Down   🛅 Expand all 🧮 Collapse all   🕜 Cut 🕝 Copy 🐄 Paste									
	Status 🖃	Action =	Source	Destination	Dest. port	Protocol	Security inspection			
Ξ	Accès de Spoke A aux	c réseaux de Hub et S	Spoke B (trafic sortant)							
1	🔵 on	🕺 pass	Private_Net_Spoke_A	Private_Net_Hub	* Any		IPS			
Ξ	Accès de Hub et Spok	e Bau réseau de Spo	oke A (trafic entrant)							
2	🔵 on	🕺 pass	며읍 Private_Net_Hub 며읍 Private_Net_Spoke_B via IPSec VPN tunnel	며읍 Private_Net_Spoke_A	Any		PS			
E	Accès Internet local du	i site Spoke A (trafic	sortant)							
3	🔵 on	🗴 pass	¤¦a Private_Net_Spoke_A	linternet	II http II https II dns		PS			
Ξ	Administration du Firev	vall								
4	🔵 on	🗴 pass	I Any	* Any	M Admin_srv		PS			



### Site Spoke B

Définissez les règles de filtrage nécessaires au dialogue entre Spoke B et Spoke A, Spoke B et Hub ainsi qu'au trafic local vers Internet:

FILT	TERING NAT									
Sear	Searched text 🛛 🔺 🛉 New rule - 🖸 Delete   🕇 Up 🤳 Down   🛅 Expand all 🗮 Collapse all   😭 Cut 😭 Copy 🐑 Paste									
	Status 🖃	Action =	Source	Destination	Dest. port	Protocol	Security inspection			
Ξ.	Accès de Spoke B aux	réseaux de Hub et S	Spoke A (trafic sortant)							
1	🔵 on	🕺 pass	며¦ Private_Net_Spoke_B	다음 Private_Net_Spoke_A 다양 Private_Net_Hub	* Any		PS			
Ξ.	Accès de Hub et Spoke A au réseau de Spoke B (trafic entrant)									
2	🕒 on	🕺 pass	며읍 Private_Net_Spoke_A 며읍 Private_Net_Hub via IPSec VPN tunnel	₽ <mark>8</mark> Private_Net_Spoke_B	🕷 Any		PS			
E	Accès Internet local du	a site Spoke B (trafic	sortant)							
3	🔵 on	1 pass	¤¦a Private_Net_Spoke_B	Internet	I http I https I dns		👰 IPS			
Ξ.	Administration du Firev	vall								
4	🔵 on	🕺 pass	Any	* Any	Marin_srv		IPS			

# Règle de NAT

### Site Spoke A

Pour permettre l'accès à Internet des machines du réseau Private Net Spoke A, créez la règle de NAT suivante :

FILTERIN	FLTERING NAT										
Complex	constructions N + New Mar © Relate   ♦ No.   Reveal of Construction   @ Constructions										
Searched	Searched text 🔀 🛉 New rule 🗸 🖬 Delete   T up 🖡 Down   📑 Expand all 🔚 Collapse all 🕐 Cut 🚱 Copy 😏 Paste										
		Original tra	ffic (before translation)			Traffic after translation					
	Status ≞▼	Source	Destination	Dest. port		Source	Ŧ	Src. port	Destination	Dest. port	Options
1	🔵 on	Private_Net_Spoke_A	Internet interface: out	Any	-	Pub_FW_Spoke_A		⊀ 🖞 ephemeral	Any		

### Site Spoke B

Pour permettre l'accès à Internet des machines du réseau Private Net Spoke B, créez la règle de NAT suivante :

FILTER	ING	NAT										
Search	earched text 🗙 🖡 New rule 🗸 🖸 Delete   🕇 Up 👃 Down   🛅 Expand all 🗮 Collapse all   🕐 Cut 🚱 Copy 🔄 Paste											
			Original traffic (before translation)				Traffic after translation					
	Sta	itus 🖃	Source	Destination	Ŧ	Dest. port		Source	Src. port	Destination	Dest. port	Options
1	0	on	Private_Net_Spoke_B	Internet interface: out		🕷 Any	+	Pub_FW_Spoke_B	🤸 🖞 ephemeral	Any		



# Cas Nº2 : trafic total via les tunnels IPSec



### Paramétrer le site central Hub

### Définir les correspondants IPSec

En suivant la méthode décrite au paragraphe Paramétrage du site Hub > Définition des correspondants IPSec du Cas N°1, créez les deux correspondants Site Spoke A et Site Spoke B.

Pour définir Site Spoke A, utilisez les valeurs suivantes :

- passerelle distante : le Firewall du site Spoke A (objet Pub FW Spoke A),
- certificat : le certificat du Firewall Hub.

Pour définir Site Spoke B :

- passerelle distante : le Firewall du site Spoke B (objet Pub FW Spoke B),
- certificat : le certificat du Firewall Hub.

	<ul> <li>Certificate</li> </ul>	Select a certificate ×			
	Pre-shared key (PSK)	Search × Filter: All -			
Certificate :	Certificate × P	▲ I SSL proxy default authority			
Pre-shared key (ASCII) :		▲ ( Documentation			
Confirm :		SpokeA			
		SpokeB			
		🔥 Hub			

### **Créer les tunnels**

Suivez la méthode décrite dans le paragraphe **Paramétrage du site Hub > Création des tunnels** du Cas N°1 pour définir les VPN suivants :



-	SITE-TO-S	SITE (GATEWAY-GATEWAY)	ANONYMOUS - MOBILE	USERS	
Search	ned text	🗙 🕂 Add 🗸 🙁 Delete 🔤	Up 🤳 Down   💣 Cut 😭	Copy 🔄 Insert	
Line	Stat	Local network	Peer	Remote network	Encryption profile
1	Ξ	Tunnel pour l'ensemble du trafi	c entre tous les autres réseaux	(Spoke B, Hub, Internet) et Spok	(e A
2	🔵 on 🤇	≥ <mark>all</mark>	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption
3	Ξ	Tunnel pour l'ensemble du trafi	c entre tous les autres réseaux	(Spoke A, Hub, Internet) et Spol	ke B
4	🔵 on 🤇	≥ all	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption

# Règles de filtrage

Définissez les règles de filtrage nécessaires au dialogue entre sites Spoke, sites Spoke et Hub ainsi qu'au trafic local vers Internet :

FILTER	RING NAT						
Search	ied text	× + New rule -	⊠ Delete   ¶ Up ↓ Down   🛅	Expand all 📃 Collapse all	Cut Copy 😒 Paste		
	Status 🖃	Action 🖃	Source	Destination	Dest. port	Protocol	Security inspection
😑 Ac	cès de Spoke A e	t Spoke B au réseau de	e Hub (trafic entrant)				
1	🔵 on	🏌 pass	며 유 Private_Net_Spoke_A 며 유 Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Hub	Any		PS
E Ac	cès de Hub aux ré	seaux de Spoke A et S	Spoke B (trafic sortant)				
2	🔵 on	🗴 pass	Private_Net_Hub	Private_Net_Spoke_A	🗷 Any		PS
E Ac	cès de Spoke A a	u réseau de Spoke B (f	trafic traversant)				
3	🔵 on	🕺 pass	Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	Any		PS
⊟ Ac	cès de Spoke B a	u réseau de Spoke A (f	trafic traversant)				
4	🔵 on	🕺 pass	□ ■ Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	<ul> <li>Any</li> </ul>		PS
😑 Ac	cès de Hub, Spok	e A et Spoke B à Intern	et				
5	🔵 on	🛓 pass	며 Private_Net_Spoke_A 며 Private_Net_Spoke_B 며 Private_Net_Hub	🚱 Internet	I http I https I dns		PS
😑 Ad	ministration du Fire	ewall					
6	🔵 on	1 pass	Any	Firewall_bridge	Mathematical Mathe		👰 IPS

# Règle de NAT

Pour permettre l'accès à Internet de l'ensemble des machines des réseaux privés, créez la règle de NAT suivante :

FILTER	ING NAT									
Search	ed text	🗙 🛉 New rule 🗸 🔀 Delete 🔤	🕇 Up 👃 Down   🛅 Expa	and all 🔳 Collapse all	@ C	ut 🚰 Copy 🔄 Paste				
Original traffic (before translation)							Traffic afte	er translation		
	Status 🖃	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Options
1	🔵 on	Private_Net_Hub Private_Net_Spoke_A Private_Net_Spoke_B	Internet interface: out	🕷 Any	+	🚦 Pub_FW_Hub	🔸 堂 ephemeral	Any		

Les sources ont été indiquées de manière unitaire dans cette règle, mais il est bien évident que l'emploi de groupes devient indispensable lorsque le nombre de sites satellites augmente.



# Paramétrer les sites satellites Spoke A et Spoke B

### Définir le correspondant IPSec

#### Site Spoke A

En suivant la méthode décrite au paragraphe **Paramétrage du site Hub > Définition des** correspondants IPSec du Cas N°1, créez le correspondant Site\_FW\_Hub en utilisant les valeurs suivantes :

- passerelle distante : le Firewall du site Hub (objet Pub FW Hub),
- certificat : le certificat du Firewall Spoke A.

### Site Spoke B

En suivant la méthode décrite au paragraphe **Paramétrage du site Hub > Définition des** correspondants IPSec du Cas N°1, créez le correspondant Site\_FW\_Hub en utilisant les valeurs suivantes :

- passerelle distante : le Firewall du site Hub (objet Pub\_FW\_Hub),
- certificat : le certificat du Firewall Spoke B.

### Créer les tunnels

### Site Spoke A

Suivez la méthode décrite dans le paragraphe **Paramétrage du site Hub > Création des tunnels** du Cas N°1 pour définir le VPN suivant :

-	ANONYMOUS - MOBILE USERS									
Searched text 🗙 🕂 Add - 🛚 Delete   🕇 Up 🖡 Down   🚱 Cut 🚱 Copy 🗐 Insert										
Line	e Stat Local network Peer Remote network Encryption profile									
1	Ξ	Tunnel pour l'ensemble du trafi	c entre Spoke A et les autres ré	seaux (Spoke B, Hub, Internet)						
2	🔵 on 🔍	Private_Net_Spoke_A	Site_FW_Hub	all	GoodEncryption					

#### Site Spoke B

Suivez la méthode décrite dans le paragraphe **Paramétrage du site Hub > Création des tunnels** du Cas Nº1 pour définir le VPN suivant :

-	ANONYMOUS - MOBILE USERS										
Search	Searched text 🛪 🕂 Add - 🛛 Delete   🕇 Up 👃 Down   🚰 Cut 😭 Copy 🗐 Insert										
Line	ne Stat Local network Peer Remote network Encryption profile										
1	🗉 Tunnel pou	r l'ensemble du trafic entre Spoke B	et les autres réseaux (Spoke A, Hub,	Internet)							
2	🔵 on 👁 🛛 Private_N	et_Spoke_B Site_FW_Hub	all	GoodEncryption							

# Règles de filtrage

Dans ce didacticiel, le trafic entre les réseaux privés n'est volontairement pas précisé (port destination : ANY). Pour des raisons d'optimisation de performances (économie de bande passante et de ressources machine), il est important d'affiner le filtrage sur les sites satellites (protocoles, ports... autorisés) afin d'éviter de laisser transiter des paquets inutiles dans les tunnels. Cette politique de filtrage sera également présente sur le site Hub.



### Site Spoke A

Définissez les règles de filtrage nécessaires au dialogue entre Spoke A et Spoke B, Spoke A et Hub ainsi qu'au trafic vers Internet (centralisé sur Hub) :

F	ILTERING							
S	aarched text	× New rule -	🛛 Delete   🕇 Up 👃 Down   🛅 i	Expand all 🔳 Collapse all 📔	🚰 Cut 💣 Copy 🔄 Paste			
	Status 🖃	Action 🖃	Source	Destination	Dest. port	Protocol	Security inspection	E.
§ =	Accès de Spoke A aux	réseaux de Hub et S	Spoke B (trafic sortant)					
1	🔵 on	🕺 pass	Private_Net_Spoke_A	P Private_Net_Hub Private_Net_Spoke_B	* Any		PS	
j =	Accès de Hub et Spoke	e Bau réseau de Spo	oke A (trafic entrant)					
2	🔵 on	1 pass	며읍 Private_Net_Hub 며읍 Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	Any		PS	
1	Accès à Internet du site	e Spoke A via le site	Hub (trafic sortant)					
3	🔵 on	🗴 pass	며¦은 Private_Net_Spoke_A	🚳 Internet	I http I https I dns		PS	
=	Administration du Firew	/all						
4	🔵 on	🕺 pass	💌 Any	🖹 Any	Mdmin_srv		IPS	

### Site Spoke B

Définissez les règles de filtrage nécessaires au dialogue entre Spoke B et Spoke A, Spoke B et Hub ainsi qu'au trafic vers Internet (centralisé sur Hub) :

FIL	TERING NAT						
0		V Neur ede -	💭 Delete 🗎 🌢 Ha 📕 Davua 🗌 🖼 I	Support all 🔲 Colleges all 🗌	Cut Come (P Danta		
Sea	rcned text	New rule +		Expand all 🔚 Collapse all	g cut g copy g Paste		
	Status 🖃	Action 🖃	Source	Destination	Dest. port	Protocol	Security inspection
Ξ	Accès de Spoke B aux	réseaux de Hub et S	Spoke A (trafic sortant)				
1	🔵 on	🕺 pass	Private_Net_Spoke_B	Private_Net_Spoke_A	* Any		IPS
Ξ	Accès de Hub et Spok	e A au réseau de Sp	oke B (trafic entrant)				
2	🔵 on	🕺 pass	며 Private_Net_Spoke_A 며 Private_Net_Hub via IPSec VPN tunnel	며¦을 Private_Net_Spoke_B	Any		IPS
Ξ	Accès à Internet du sit	e Spoke B via le site	Hub (trafic sortant)				
3	🔵 on	🗴 pass	며 Private_Net_Spoke_B	🚳 Internet	I http I https I dns		IPS
Ξ	Administration du Firev	vall					
4	🔵 on	🗴 pass	🕷 Any	🖹 Any	Mdmin_srv		👰 IPS



# Vérifier l'établissement des tunnels

Depuis un poste client situé sur le site Spoke A, établissez tout d'abord une connexion vers une machine du site Hub (via un Ping par exemple, si vous avez autorisé le protocole ICMP dans l'ensemble des règles de filtrage), afin de tester l'établissement du premier tunnel (Spoke A vers Hub).

# Via la suite d'administration Stormshield Network

Lancez Stormshield Network Real-Time Monitor, connectez-vous au Firewall du site Hub 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 ») :

💎 Date	💎 Niveau d'erreur	💎 Phase	Source	Destination	💎 Message	💎 Identité du distant 🔍 SPI	I entrant	SPI sortant	Vertical (entrant/sortant)	💎 Rôle
10:20:49	Information	2	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established	0x04c3	372d8 0	x09e42dc6	0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	INITIAL-CONTACT sent				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	DPD support detected				0x8b44ebe0933b4060/0x000000000000000	responder
10:04:55	Information	0			Isakmp daemon started				1	

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

i	Vue d'ensemble	C Actualiser							
	Console	Rechercher:							
	Tableau de bord	Source Source	♥ Octets		Destination	🛡 Etat	💎 Durée de vie	Authentificatio	Chiffrement
	Evénements	Pub_FW_Hub	11,06 Ko ;	5,28 Ko	, Pub_FW_Spoke_A	mature	2m 20sec	hmac-sha1	3des-cbc
8	Management de								
E	Machines								
*	Interfaces								
F	Qualité de Service								
<u>iji</u>	Utilisateurs								
$\mathbb{X}$	Quarantaine - B								
0	Tunnels VPN								

Depuis le même poste client du site Spoke A, établissez ensuite une connexion vers une machine du site Spoke B, afin de vérifier l'établissement du second tunnel (Hub vers Spoke B).

Dans le module **Traces > VPN** de Stormshield Network Real-Time Monitor, vérifiez que les phases 1 et 2 se sont correctement déroulées (messages « Phase established ») :

💎 Date	💎 Niveau d'erreur	💎 Phase	Source	Destination	💎 Message	🔻 Identité du distant	💎 SPI entrant	🛡 SPI sortant	💎 Cookie (entrant/sortant)	💎 Rôle
10:28:47	Information	2	Pub_FW_Hub	Pub_FW_Spoke_B	Phase established		0x0573b30c	0x0739c88c	0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	INITIAL-CONTACT sent				0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	Phase established				0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	DPD support detected				0x78ad430165eb1b24/0x0000000000000000	initiator
10:20:49	Information	2	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established		0x04c372d8	0x09e42dc6	0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	INITIAL-CONTACT sent				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	DPD support detected				0x8b44ebe0933b4060/0x000000000000000	responder
10:04:55	Information	0			Isakmp daemon started				1	

#### Dans le module Tunnels VPN, vous pouvez désormais visualiser les deux tunnels :

Source	♥ Octets	Destination	🛡 Etat	🛡 Durée de vie	Authentificatio	Thiffrement
Pub_FW_Hub	11,39 Ko 5,51 Ko	Pub_FW_Spoke_A	mature	8m 7sec	hmac-sha1	3des-cbc
Pub_FW_Hub	360 o 180 o	Pub_FW_Spoke_B	mature	9sec	hmac-sha1	aes-cbc



### Outils d'informations et de diagnostic en console

### Commande showSPD

La commande *showSPD* présente la politique IPSec active sur le Firewall. Son résultat est identique, que des tunnels soient établis ou non.

Dans le cas N°2 de ce didacticiel (trafic total via tunnel IPSec), cette commande passée sur le Firewall Spoke A retourne le résultat suivant :

```
>showSPD
0.0.0.0/0[any] 127.0.0.0/8[any] 255
       in none
       spid=67 seq=5 pid=62800
       refcnt=1
192.168.0.0/24[any] 192.168.0.0/24[any] 255
       in none
       spid=69 seq=4 pid=62800
       refcnt=1
0.0.0.0/0[any] 192.168.0.0/24[any] 255
       in ipsec
       esp/tunnel/ - /unique#16386
       spid=72 seq=3 pid=62800
       refcnt=1
127.0.0.0/8[any] 0.0.0.0/0[any] 255
       out none
       spid=68 seq=2 pid=62800
       refcnt=1
192.168.0.0/24[any] 192.168.0.0/24[any] 255
       out none
       spid=70 seq=1 pid=62800
       refcnt=1
192.168.0.0/24[any] 0.0.0.0/0[any] 255
       out ipsec
       esp/tunnel/ - /unique#16385
       spid=71 seq=0 pid=62800
       refcnt=1
```

On y retrouve notamment les informations suivantes :

- Le réseau local et le réseau distant : « 192.168.0.0/24 [any] 0.0.0.0/0 [any] »,
- Le sens du tunnel : « out ipsec »,
- Les adresses IP des passerelles IPSec : « esp/tunnel/adresse locale adresse distante »,
- L'ID de l'Association de Sécurité (SA) : « unique#16385 ».

### Commande showSAD

La commande *showSAD* liste les informations de sécurité des SA (Security Associations – Associations de Sécurité) établies sur une passerelle IPSec. Ces informations ne sont disponibles que lorsque des tunnels sont établis.



Dans le cas N°2 de ce didacticiel (trafic total via tunnel IPSec), cette commande passée sur le Firewall Spoke A retourne le résultat suivant :

esp mode=tunnel spi=219753044(0x0d192a54) regid=16386(0x00004002)
E: 3des-cbc 6093662d 55ec9528 818b6e7d 3f88d590 96a0d84a 80247f2c
A: hmac-sha1 e082ddd6 673a2af9 53d0b88f ea201de8 88c45da2
seq=0x00000031 replay=8 flags=0x00000000 state=mature
created: Feb 3 16:09:16 2014 current: Feb 3 16:15:44 2014
diff: 388(s) hard: 3600(s) soft: 2880(s)
last: Feb 3 16:11:58 2014 hard: 0(s) soft: 0(s)
current: 9999(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 49 hard: 0 soft: 0
<pre>sadb_seq=1 pid=29053 refcnt=1</pre>
esp mode=tunnel spi=169172253(0x0a155d1d) regid=16385(0x00004001)
E: 3des-cbc c0100685 d48e5f27 686997d8 62d09ffb ed95d1c1 89cf9566
A: hmac-sha1 0fd9d769 f63ac3a0 62869791 4cca65a1 3445527d
seq=0x00000034 replay=8 flags=0x00000000 state=mature
created: Feb 3 16:09:16 2014 current: Feb 3 16:15:44 2014
diff: 388(s) hard: 3600(s) soft: 2880(s)
last: Feb 3 16:11:58 2014 hard: 0(s) soft: 0(s)
current: 8840(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 52 hard: 0 soft: 0
<pre>sadb_seq=0 pid=29053 refcnt=2</pre>

On y retrouve notamment les informations suivantes :

- Adresse IP de la passerelle émettrice Adresse IP de la passerelle réceptrice.
- Le SPI (Security Parameter Index) : « spi=169172253 (0x0a155d1d) ». Le SPI est identifié en fonction du sens de la SA affichée. Ainsi, pour une SA décrite dans le sens IP distante – IP locale, le SPI indiqué est le SPI entrant. Il permet alors d'identifier des flux entrants,
- La méthode de chiffrement utilisée : « E : 3des-cbd »,
- La méthode d'authentification utilisée : « A: hmac-sha1 »,
- L'état du tunnel : « state=mature ». Cet état peut être mature (le tunnel est correctement établi : la SA est disponible et utilisable), larval (la SA est en cours de négociation) ou dying (la SA est arrivée au terme de sa durée de vie et sera renégociée lorsque du trafic le nécessitera).
- La date/heure d'établissement du tunnel et la date/heure courantes,
- Le nombre d'octets échangés. current : 8840 (bytes).

### Résolution d'incidents – Erreurs communes

- Si vous avez opté pour l'authentification par certificats, reportez-vous à la section

   Résolution d'incidents Erreurs communes » du didacticiel « Mise en œuvre d'un VPN
   IPSec Authentification par certificats ».
- Si vous avez opté pour l'authentification par clé prépartagée, reportez-vous à la section « Résolution d'incidents – Erreurs communes » du didacticiel « Mise en œuvre d'un VPN IPSec – Authentification par clé prépartagée ».





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.