NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

INTÉGRATION DU NAT DANS IPSEC

Produits concernés : SNS 1.x, SNS 2.x, SNS 3.x, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-integration_du_NAT_dans_IPSEC_note_technique

Table des matières

Avant de commencer

Les firewalls SNS permettent d'effectuer des actions de translation d'adresses réseau (NAT) sur les flux entrants et sortants des tunnels VPN IPSec.

Cette fonction de NAT dans VPN IPSec peut s'avérer utile dans les situations suivantes :

- Pour interconnecter des réseaux dont les plans d'adressage se recouvrent. Pour plus d'informations, reportez-vous à la section Interconnecter des réseaux dont les plans d'adressages se recouvrent.
- Lorsque l'on ne souhaite pas révéler le plan d'adressage réel de notre LAN. Pour plus d'informations, reportez-vous à la section Masquer un plan d'adressage.

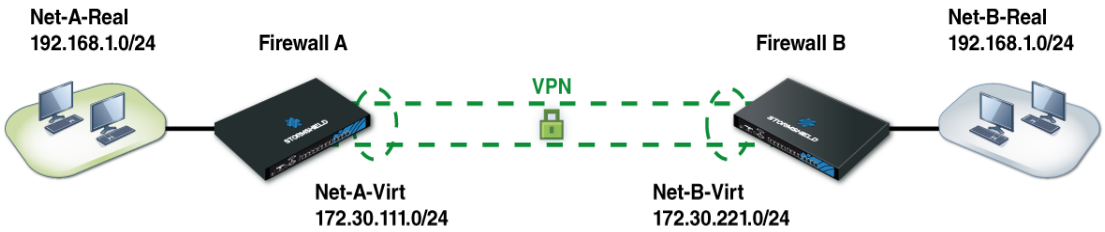
Interconnecter des réseaux dont les plans d'adressages se recouvrent

Dans le cas de réseaux dont les plans d'adressage se recouvrent, aucun des deux réseaux privés ne peut utiliser ses adresses IP réelles à travers le tunnel. En effet, les correspondants estimeraient appartenir au même réseau et tenteraient donc de se contacter directement sur ce réseau local au lieu d'emprunter le tunnel IPSec.

La stratégie sera donc ici de :

- Masquer les adresses IP réelles des hôtes du réseau A aux hôtes du réseau B et inversement.
- Faire admettre aux hôtes du réseau A que le réseau B utilise un plan d'adressage différent.
- Rétablir les destinations réelles en sortie de tunnel pour acheminer les paquets vers les adresses IP réelles des hôtes des deux réseaux.

Cela nécessite de modifier l'adresse IP source avant l'envoi des paquets dans le tunnel IPSec, et de rétablir l'adresse IP de destination réelle dans les paquets provenant du tunnel, et ce, sur les deux sites à relier.



Ici *Net-A-Real* et *Net-B-Real* sont dans le même plan d'adressage.

Nous définissons donc :

- *Net-A-Virt* pour décrire le réseau A tel que B le percevra.
- *Net-B-Virt* pour décrire le réseau B tel que A le percevra.

La politique IPSec ne connaît que les plans d'adressage IP dits "virtuels" (*-virt*). La translation des adresses source survient avant le passage dans le tunnel IPSec (avant chiffrement). La translation de l'adresse de destination survient après passage dans le tunnel (après déchiffrement du paquet provenant du tunnel).

Configurer le firewall A

Politique VPN

Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive
1	on		Net-A-Virt	Site_b	Net-B-Virt	StrongEncryption	0

Pour correspondre à la politique IPSec, il faudra provenir du réseau virtuel A *Net-A-Virt* et contacter le réseau virtuel B *Net-B-Virt*.

Veillez à ce que les réseaux virtuels et réels aient le même masque de sous-réseau.

Politique de NAT

		Status	Original traffic (before translation)				Traffic after translation				Protocol	Options
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port		
1		on	Net-A-Real	Net-B-Virt	Any	➡	Net-A-Virt		Any			NAT inside IPSec tunnel
2		on	Net-B-Virt	Net-A-Virt	Any	➡	Any		Net-A-Real			NAT inside IPSec tunnel

- La règle 1 permet de translater le réseau réel A *Net-A-Real*vers le réseau virtuel A *Net-A-Virt* avant le module IPSec (colonne **Options**).
- La règle 2 permet de rediriger les paquets à destination du réseau virtuel A *Net-A-Virt* vers le réseau réel interne A *Net-A-Real*.

Politique de filtrage

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Net-B-Virt via IPSec VPN tunnel	Net-A-Virt	Any		IPS
2		on	pass	Net-A-Real	Net-B-Virt	Any		IPS

Configurer le firewall B

Politique VPN

Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive
1	on		Net-B-Virt	Site_a	Net-A-Virt	StrongEncryption	0

Pour correspondre à la politique IPSec, il faudra provenir du réseau virtuel B *Net-B-Virt* et contacter le réseau virtuel A *Net-A-Virt*.

Politique de NAT

		Status	Original traffic (before translation)				Traffic after translation				Protocol	Options
			Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port		
1		on	Net-B-Real	Net-A-Virt	Any	➡	Net-B-Virt		Any			NAT inside IPSec tunnel
2		on	Net-A-Virt	Net-B-Virt	Any	➡	Any		Net-B-Real			NAT inside IPSec tunnel

- La règle 1 permet de translater le réseau réel B *Net-B-Real* vers le réseau virtuel B *Net-B-Virt* avant le module IPSec (colonne **Options**).
- La règle 2 permet de rediriger les paquets à destination du réseau virtuel B *Net-B-Virt* vers le réseau réel interne B *Net-B-Real*.

Veillez à ce que les réseaux virtuels et réels aient le même masque de sous-réseau.

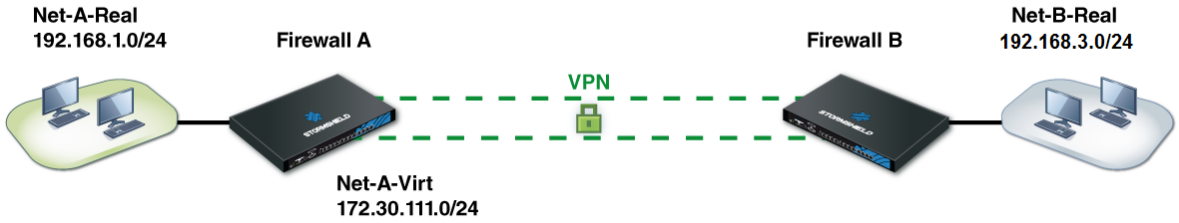
Politique de filtrage

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Net-A-Virt via IPSec VPN tunnel	Net-B-Virt	Any		IPS
2		on	pass	Net-B-Real	Net-A-Virt	Any		IPS

Masquer un plan d'adressage

Il peut arriver que le plan d'adressage interne nécessite d'être masqué, simplement pour une raison de sécurité ou par contrainte, lorsque ce plan d'adressage est utilisé sur un autre réseau, connu par le site distant avec lequel on souhaite communiquer au travers du tunnel IPSec.

La configuration est similaire au cas précédent, à la différence du fait que seul l'un des réseaux devra être masqué à l'autre.



Ici le réseau *Net-A-Real* situé derrière le firewall A apparaîtra comme *Net-A-Virt* au site B.

Configurer le firewall A

Politique VPN

Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive
1	on		Net-A-Virt	Site_b	Net-B-Real	StrongEncryption	0

Pour correspondre à la politique IPSec, il faudra provenir du réseau virtuel A *Net-A-Virt* et contacter le réseau réel B *Net-B-Real.*

Politique de NAT

		Status	Original traffic (before translation)			Traffic after translation				Protocol	Options
			Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port		
1		on	Net-A-Real	Net-B-Real	Any	Net-A-Virt		Any			NAT inside IPSec tunnel
2		on	Net-B-Real	Net-A-Virt	Any	Any		Net-A-Real			NAT inside IPSec tunnel

- La règle 1 permet de translater le réseau réel A *Net-A-Real* vers le réseau virtuel A *Net-A-Virt* avant le module IPSec (colonne **Options**).
- La règle 2 permet de rediriger les paquets à destination du réseau virtuel A *Net-A-Virt* vers le réseau réel interne A *Net-A-Real*.

Politique de filtrage

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1		on	pass	Net-B-Real via IPSec VPN tunnel	Net-A-Virt	Any		IPS
2		on	pass	Net-A-Real	Net-B-Real	Any		IPS

Configurer le firewall B

Politique VPN

Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive
1	on		Net-B-Real	Site_a	Net-A-Virt	StrongEncryption	0

Politique de filtrage

			Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1			on	pass	Net-A-Virt via IPSec VPN tunnel	Net-B-Real	Any		IPS
2			on	pass	Net-B-Real	Net-A-Virt	Any		IPS

Lors de vos tests, contactez des hôtes appartenant au réseau distant et non des interfaces internes du firewall distant.

STORMSHIELD

documentation@stormshield.eu