TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

INTEGRATING NAT INTO IPSEC

Product concerned: SNS 1.x, SNS 2.x, SNS 3.x, SNS 4.x

Document last updated: December 9, 2019

Reference: sns-en-integrating_NAT_into_IPSEC_technical_note

Table of contents

Getting Started

SNS firewalls allow Network Address Translation (NAT) to be applied on incoming and outgoing traffic in IPsec VPN tunnels.

The NAT feature in IPsec VPN may come in useful in several situations:

- Interconnecting networks with overlapping address ranges. For more information, please refer to the section **Interconnecting networks with overlapping address ranges**.
- When you wish to hide the real address range of your LAN. For more information, please refer to the section **Hiding an address range**.

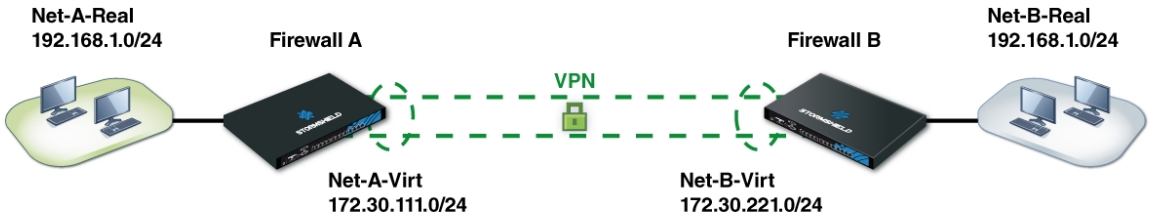
Interconnecting networks with overlapping address ranges

In this case, neither of the private networks can use their real IP addresses through the tunnel as the peers would assume that they belong to the same network and would therefore attempt to contact each other directly on this local network instead of going through the IPsec tunnel.

The strategy to adopt would therefore be to:

- Hide the real IP addresses of the hosts on Network A from the hosts on Network B and vice versa,
- Indicate to the hosts on Network A that Network B uses a different address range,
- Restore the real destinations when leaving the tunnel in order to transport packets to the real IP addresses of the hosts on both networks.

This would require modifying the source IP address before sending the packets through the IPsec tunnel, and restoring the real destination IP address in the packets coming from the tunnel on both of the sites to be linked.



In this example, *Net-A-Real* and *Net-B-Real* are in the same address range.

We have defined as follows:

- *Net-A-Virt* to represent Network A as Network B will see it,
- *Net-B-Virt* to represent Network B as Network A will see it.

The IPsec policy will only know the "virtual" IP address ranges (*-virt*), as source addresses would have been translated before going into the IPsec tunnel (before encryption) and destination addresses would be translated after having gone through the tunnel (after decryption of the packet that came from the tunnel).

Configuring firewall A

VPN policy

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

To correspond to the IPsec policy, traffic has to come from the virtual network A *Net-A-Virt* and contact the virtual network B *Net-B-Virt*.

Ensure that the virtual and real networks have the same sub-network mask.

NAT policy

		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

- Rule 1 allows translating traffic from real network A *Net-A-Real* to virtual network A *Net-A-Virt* before the IPsec module (**Options** column).
- Rule 2 allows redirecting packets going to virtual network A *Net-A-Virt* to internal real network A *Net-A-Real*.

Filter policy

		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

Configuring firewall B

VPN policy

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

To correspond to the IPsec policy, traffic has to come from the virtual network B *Net-B-Virt* and contact the virtual network A *Net-A-Virt*.

NAT policy

		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

- Rule 1 allows translating traffic from real network B *Net-B-Real* to virtual network B *Net-B-Virt* before the IPsec module (**Options** column).
- Rule 2 allows redirecting packets going to virtual network B *Net-B-Virt* to internal real network B *Net-B-Real*.

Ensure that virtual and real networks have the same sub-network mask.

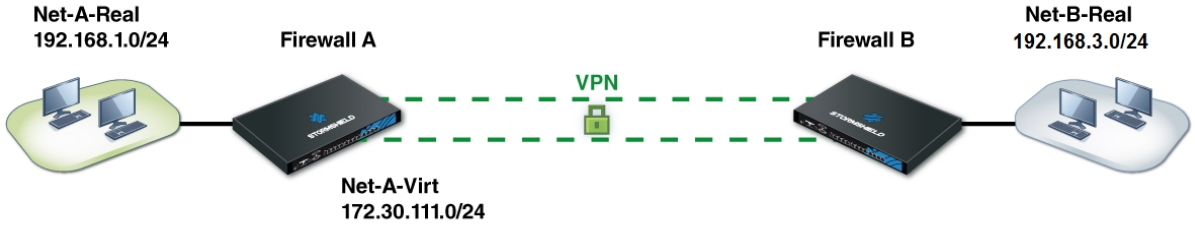
Filter policy

		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

Hiding an address range

An internal address range may sometimes need to be masked, simply for security reasons or out of necessity when this address range is used on another network known by the remote site and with which you would like to communicate through the IPsec tunnel.

The configuration is similar to the one in the previous example, except for the fact that only one of the networks needs to be masked from the other.



In this example, *Net-A-Real* located behind Firewall A will appear as *Net-A-Virt* to site B.

Configuring firewall A

VPN policy

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

To correspond to the IPsec policy, traffic has to come from the virtual network A *Net-A-Virt* and contact the real network B *Net-B-Real*.

NAT policy

		Original traffic (before translation)				Traffic after translation				
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port	Options
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

- Rule 1 allows translating traffic from real network A *Net-A-Real* to virtual network A *Net-A-Virt* before the IPsec module (**Options** column).
- Rule 2 allows redirecting packets going to virtual network A *Net-A-Virt* to internal real network A *Net-A-Real*.

Filter policy

		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

Configuring firewall B

VPN policy

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

Filter policy

			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

During tests, contact hosts belonging to the remote network instead of the internal interfaces of the remote firewall.

Further reading

Stormshield Knowledge Base

Additional information and responses to questions you may have about the NAT into IPsec are available in the Stormshield knowledge base (authentication required).

STORMSHIELD

documentation@stormshield.eu