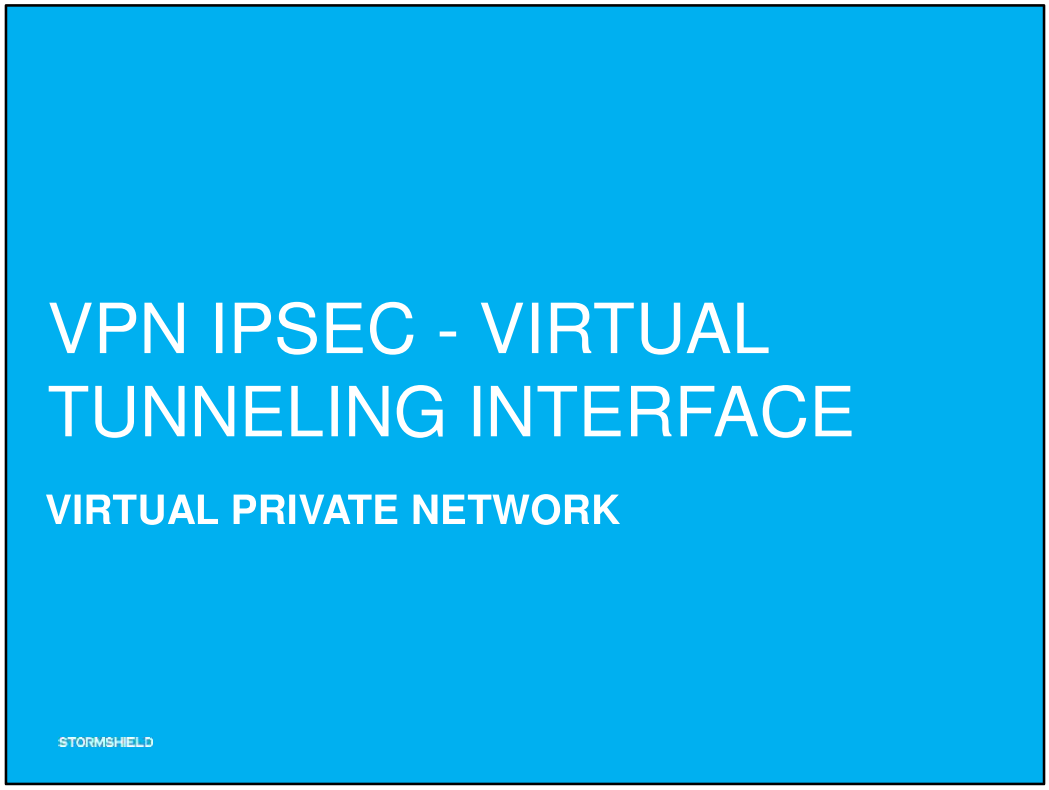
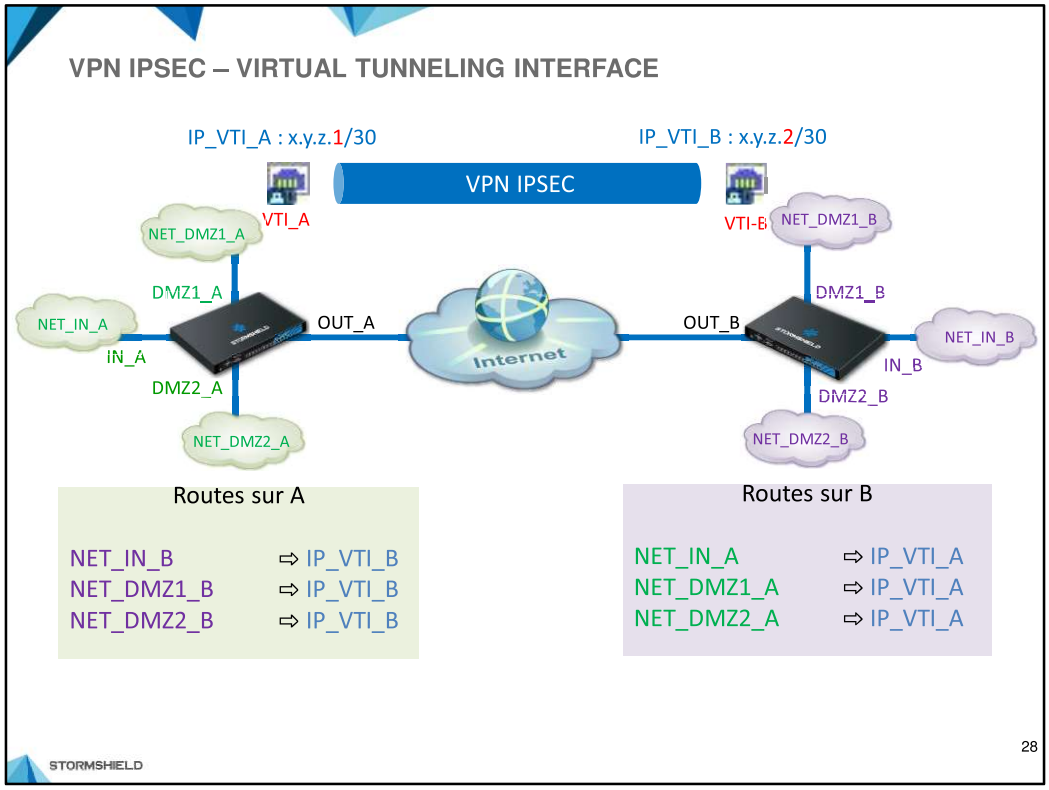


Programme du module

- ✔ Les différents réseaux privés virtuels
- ✔ VPN IPSec – Concepts et généralités
- ✔ VPN IPSec – Configuration de tunnel site-à-site
- ✔ VPN IPSec – Configuration de tunnels site-à-site multiples
- ➔ VPN IPSec – Virtual Tunneling Interface



Une autre approche est rendue possible par l'utilisation d'interfaces **VTI** dédiées à un tunnel IPSec.

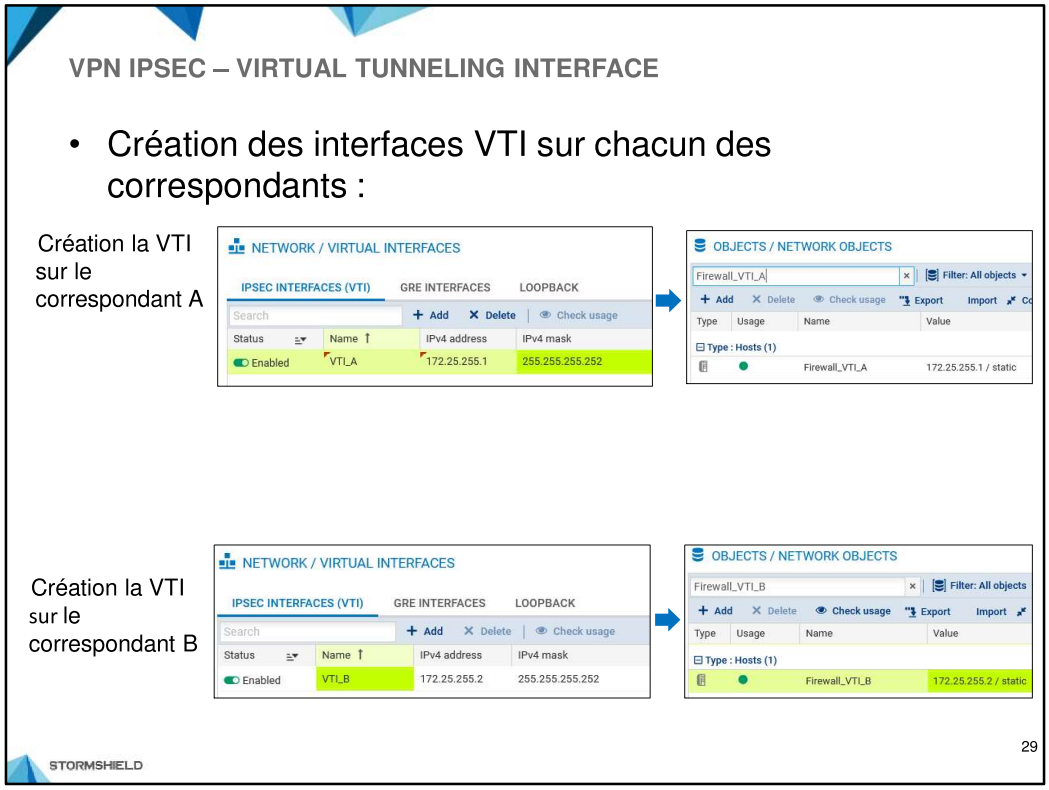
Ces **interfaces** IPSec particulières constitueront les **points de passage des flux** en entrée et en sortie de tunnel IPSec. Elles agiront comme **passerelle** l'une envers l'autre pour acheminer les flux entre les réseaux au travers du tunnel IPSec.

Les avantages de cette approche résident dans :

- L'indépendance de la politique IPSec vis-à-vis des adresses IP des usagers du tunnel et des flux à prendre en charge.
- La disponibilité immédiate du tunnel pour tout nouveau réseau ou flux.
- La souplesse et la précision dans la **sélection des flux** à envoyer dans le tunnel.
- La limitation à un seul tunnel (et donc à **une seule négociation de phase 2**) quel que soit le nombre de réseaux IP à relier entre eux.

Les diapositives suivantes détaillent les étapes qui permettent de configurer un tunnel VPN IPSec site-à-site en utilisant les interfaces VTI.

Priorité entre correspondance de politique et routage sur VTI :
Le routage sur VTI est prioritaire sur la correspondance de politique. C'est-à-dire, si une politique VPN IPSec contient deux tunnels servant à relier les mêmes réseaux, un défini par la correspondance de politique et un deuxième utilisant le routage sur VTI, les paquets seront transmis via le deuxième tunnel.



Les VTI créées sur les deux correspondants portent chacune un nom commun et une adresse IP du même plan d'adressage :

- Sur le correspondant A, la VTI est nommée « VTI_A » et son IP est 172.25.255.1/30.
- Sur le correspondant B, la VTI est nommée « VTI_B » et son IP est 172.25.255.2/30.

Pour éviter toute ambiguïté avec l'architecture existante et ses futures évolutions, il convient de choisir un plan d'adressage dédié à l'usage des VTI, dans une plage officiellement privée et suffisamment originale pour ne pas entrer en collision avec un réseau déjà existant ou le réseau distant d'une interconnexion future.

NOTE : Depuis la V3.3.0, il est possible d'utiliser un réseau en /31 qui convient mieux aux interfaces point-à-point car elles n'utilisent pas les adresses réseau et broadcast.

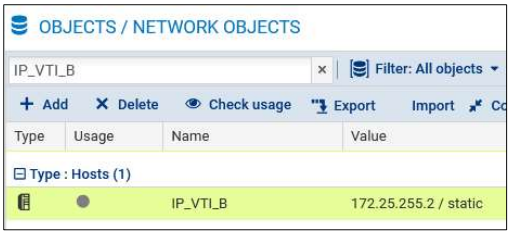
Les noms communs de ces interfaces seront automatiquement associés à un objet machine implicite, sur chacun des correspondants :

- Sur le correspondant A : Firewall_VTI_A.
- Sur le correspondant B : Firewall_VTI_B.

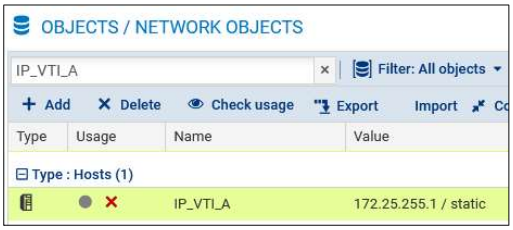
VPN IPSEC – VIRTUAL TUNNELING INTERFACE

- Création de l'objet machine qui porte l'adresse IP de l'interface VTI du correspondant distant.

Sur A, création de l'objet machine qui porte l'adresse IP de l'interface VTI_B



Sur B, création de l'objet machine qui porte l'adresse IP de l'interface VTI_A



30

STORMSHIELD

Sur chacun des firewalls, il faut également créer l'objet portant l'adresse IP de la VTI du correspondant distant.

Comme pour tous les objets, il est judicieux de définir une nomenclature rigoureuse en utilisant des noms évocateurs. Cette bonne pratique facilite l'utilisation des VTI sur des architectures VPN IPSec aux correspondants multiples.

VPN IPSEC – VIRTUAL TUNNELING INTERFACE

- Définition de la politique VPN IPSec basée sur les VTI :
  - Sur le correspondant A

  - Sur le correspondant B

31

STORMSHIELD

Les objets correspondants aux adresses IP des VTI sont définies comme extrémités de trafic du tunnel. Contrairement aux configurations IPSec basées sur la correspondance de politique, ce ne sont pas exclusivement les flux de communication entre les deux adresses IP des interfaces VTI qui sont pris en charge par IPSec, mais tout flux qui passe par ces interfaces grâce aux directives de routage.

VPN IPSEC – VIRTUAL TUNNELING INTERFACE

- Définition des routes pour les flux usagers du tunnel : routes statiques
  - Sur le correspondant A

STATIC ROUTES

Searching... + Add ✕ Delete

Status	Destination network (host, network or group object)	Interface	Address range	Gateway
on	NET_DMZ1_B	VTI_A	172.16.2.0/24	IP_VTI_B
on	NET_IN_B	VTI_A	192.168.2.0/24	IP_VTI_B

  - Sur le correspondant B

STATIC ROUTES

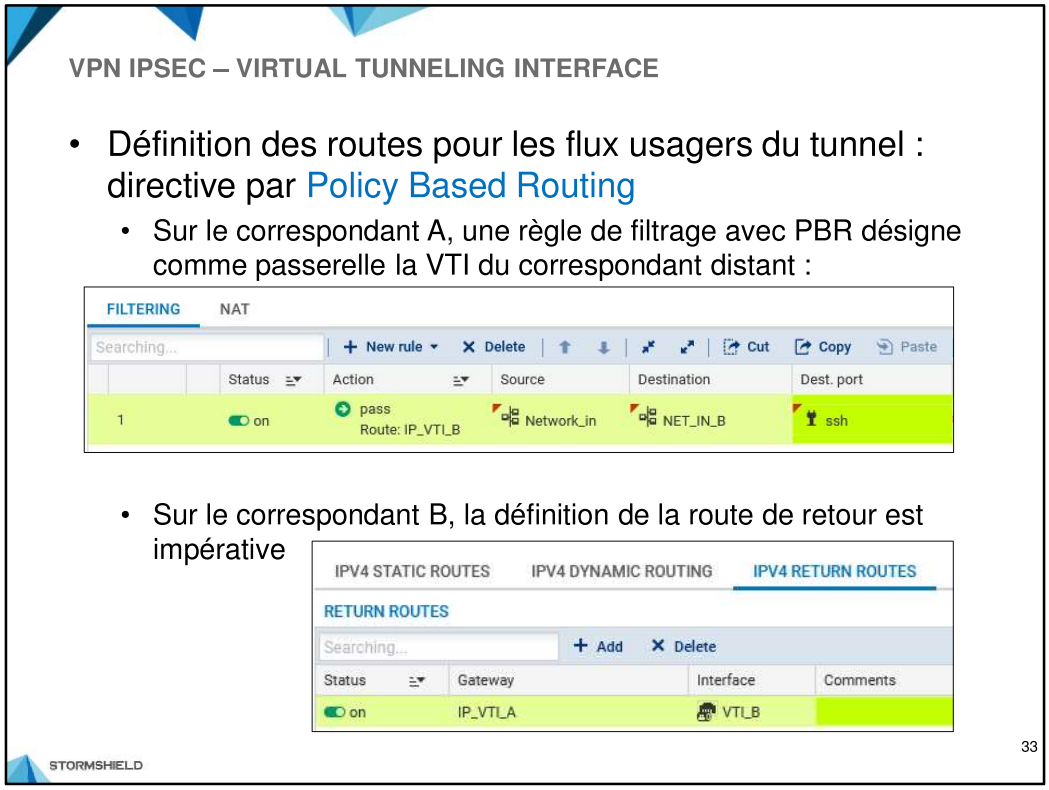
Searching... + Add ✕ Delete

Status	Destination network (host, network or group object)	Interface	Address range	Gateway
on	NET_DMZ1_A	VTI_B	172.16.1.0/24	IP_VTI_A
on	NET_IN_A	VTI_B	192.168.1.0/24	IP_VTI_A

32

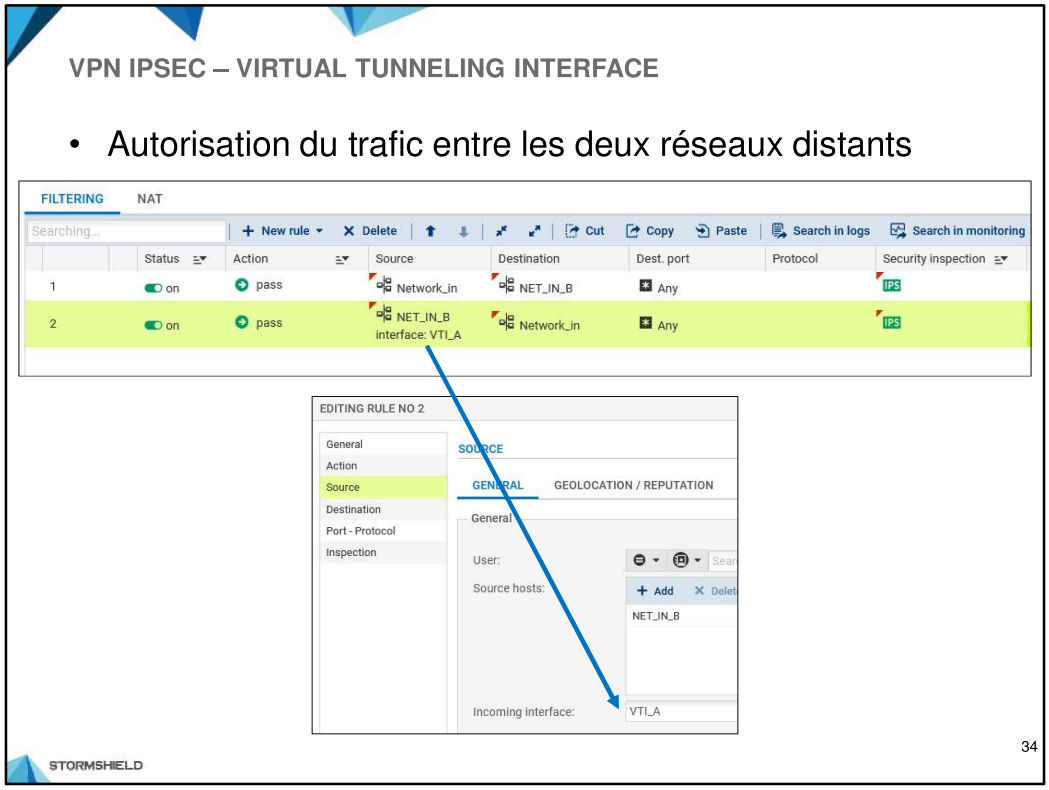
STORMSHIELD

Dans ce mode de fonctionnement, il est essentiel de veiller à ce que le routage des paquets retour coïncide avec le tunnel emprunté par les paquets aller.
Ci-dessous, les routes statiques indiquent globalement sur chaque correspondant que les réseaux distants sont joignables par le même tunnel.



L'usage de directives de routage par politique (PBR), impose également de gérer le routage des paquets retour par le même tunnel.
C'est pourquoi, il est nécessaire de définir la route retour par la VTI correspondante au tunnel par lequel les paquets aller sont arrivés.

Ces directives doivent être appliquées sur les deux correspondants si les communications dans le tunnel peuvent être initiées indifféremment par des réseaux côté A vers des réseaux côté B et inversement.



Avec les interfaces VTI, la directive **via Tunnel VPN IPSec** ne doit pas être utilisée. A sa place, il faut utiliser l'interface VTI comme interface d'entrée dans la règle autorisant le trafic entrant depuis le tunnel.