Installation d’un VPN IPsec

Table des matières

I) Qu’est-ce que c’est un VPN IPsec ?

1) Le VPN (Virtual Private Network) permet de connecter des réseaux sur des sites distants, qui ne sont pas connectés directement entre eux. Permettant ainsi l’accès à des ressources d’un site A depuis un site B. Plusieurs protocoles sont mis à disposition pour sécuriser les échanges, dans cette documentation nous allons parler du protocole IPsec qui se divise en 2 phases, la phase de tunneling puis la phase de cryptage. A la suite de ces 2 échanges, le VPN sera opérationnel.

2) La phase de tunneling va s’effectuer via des clés privées et des clés publiques, la clé publique sera disponible par tout le monde tandis que la clé privée sera gardée par le firewall. La clé publique permettant de crypter les paquets, mais ne les décryptera pas. La clé privée à l’inverse pourra les décrypter.

3) La phase de cryptage connectera les 2 LAN afin qu’il puisse communiquer en sécurité. C’est la suite de la phase tunneling que la phase de cryptage intervient. Elle met également en relation les deux interfaces LAN pour que les deux réseaux puissent communiquer ensemble.

II) Mise en situation :

Jean, patron d’une entreprise d’imprimante à champagne voyant que son entreprise prend de l’ampleur, il décide d’ouvrir une nouvelle boutique à Gerland, car beaucoup de ses clients sont dans cette zone. Mais Jean voudrait que son serveur de fichier puisse être accessible depuis la boutique de Gerland et la boutique de Champagne. Il fait donc

appeler Koesio pour qu'elle lui propose une solution. Une des solutions les plus standards et peu couteuse est le VPN IPsec. Jean voyant que cela ne lui rajoute pas de frais matériel et seulement un peu de main d'œuvre, il accepte.

Le site de champagne est en 192.168.10.X et le site de Gerland seront en 192.168.20.X. Cependant, ce sont tous les deux des réseaux en NAT-PAT, c'est-à-dire que le firewall a une interface directement reliée à internet (WAN) qui a une adresse IP unique qui jouera un rôle de carte d'identité. Puis une interface interne (LAN) qui permettra de connecter plusieurs machines à internet qui sera reconnu sous une même adresse IP. Ce système permet de faire face à la pénurie d'adresse IP. Le firewall redirigera les paquets en modifiant l'entête du datagramme IP en fonctions de plusieurs facteurs comme le port.

Pour vous montrer ceci, on va faire un ping depuis Champagne sur le site de Gerland,

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::db35:1b6:df65:e015%3
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.10.10
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.10.254

C:\Users\guft>ping 192.168.20.254

Envoi d'une requête 'Ping'  192.168.20.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.20.254:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Ici, on peut voir que le réseau de Champagne n'est pas connecté avec le site de Gerland. Nous allons donc aller sur les paramètres firewall pour les créer.

Comme vu précédemment pour configurer un VPN IPsec, il faut faire dans une premier temps la phase de tunneling puis on fera la phase de cryptage.

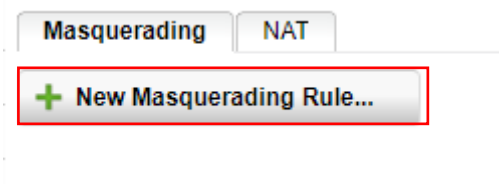
C'est, Monsieur Alain Poster qui est chargé de faire cette configuration de VPN et va vous explique comment il fait. Il va commencer par configurer le firewall de Champagne.

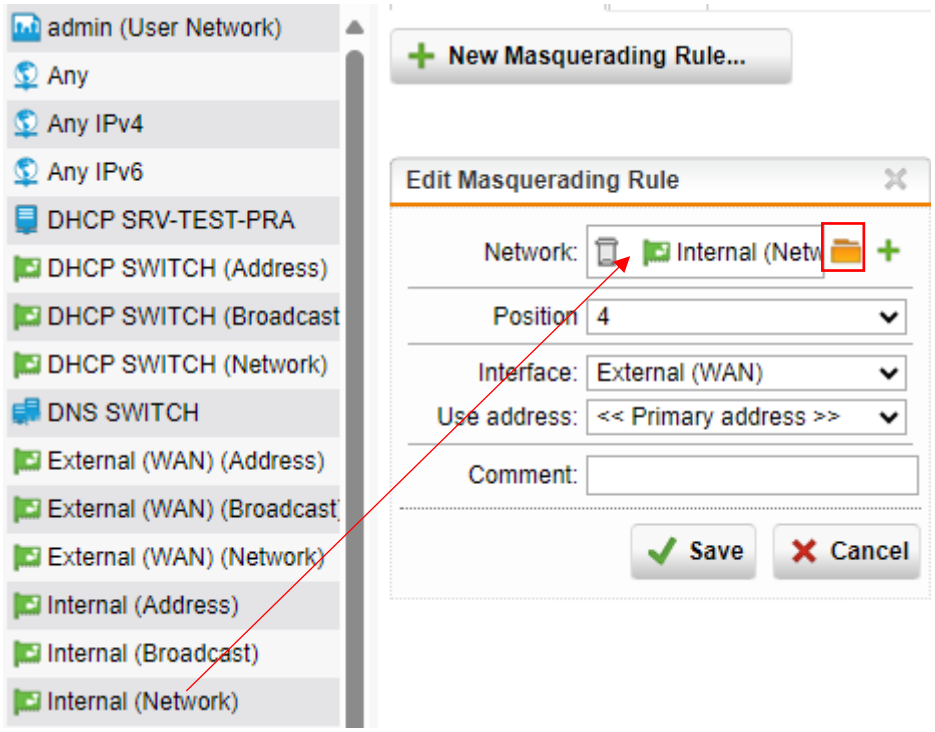
Pour faire cette phase de tunneling, les deux routeurs vous communiquer via l'IP publique fixe (WAN) des deux firewalls, Alain va vous montrer comment configurer un NAT.

III) Mise en place du NAT

Alain va donc aller dans l'onglet « Network Protection » puis aller dans « NAT », cela va permettre d'affecter le réseau privé au WAN.

Alain doit ensuite cliquer sur « new Masquering Rule » qui va ajouter un NAT sur une interface



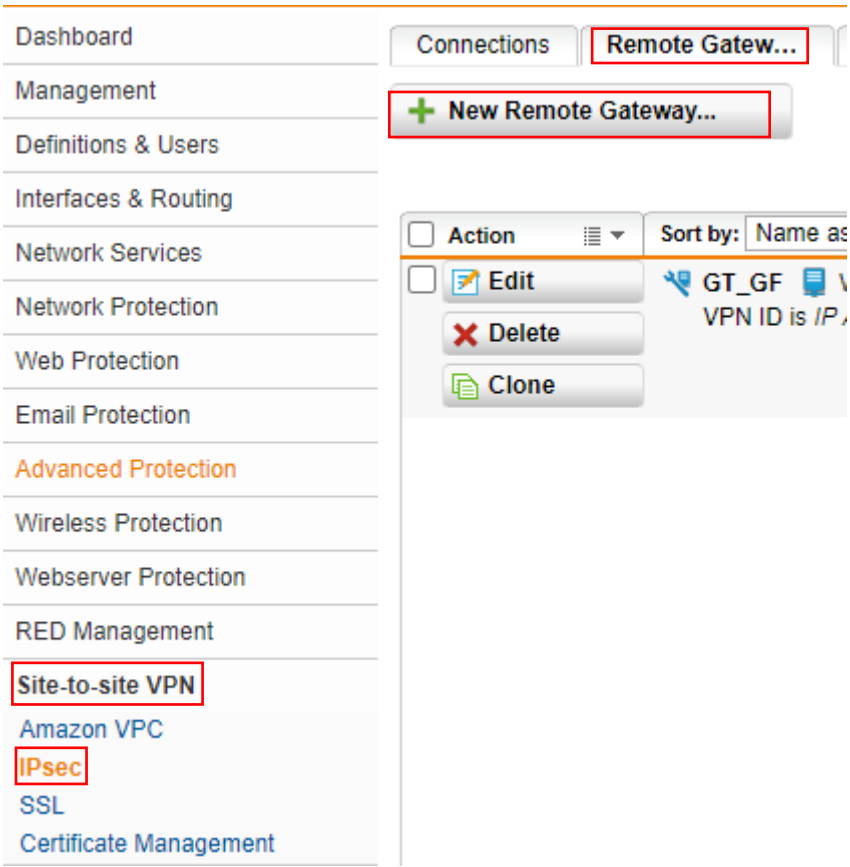


Alain va cliquer sur le petit émoticône dossier puis la liste à gauche va s'afficher, il glissera « internal (network) » dans « Network », l'interface vous mettrez celle qui est connecté directement à internet (le WAN).

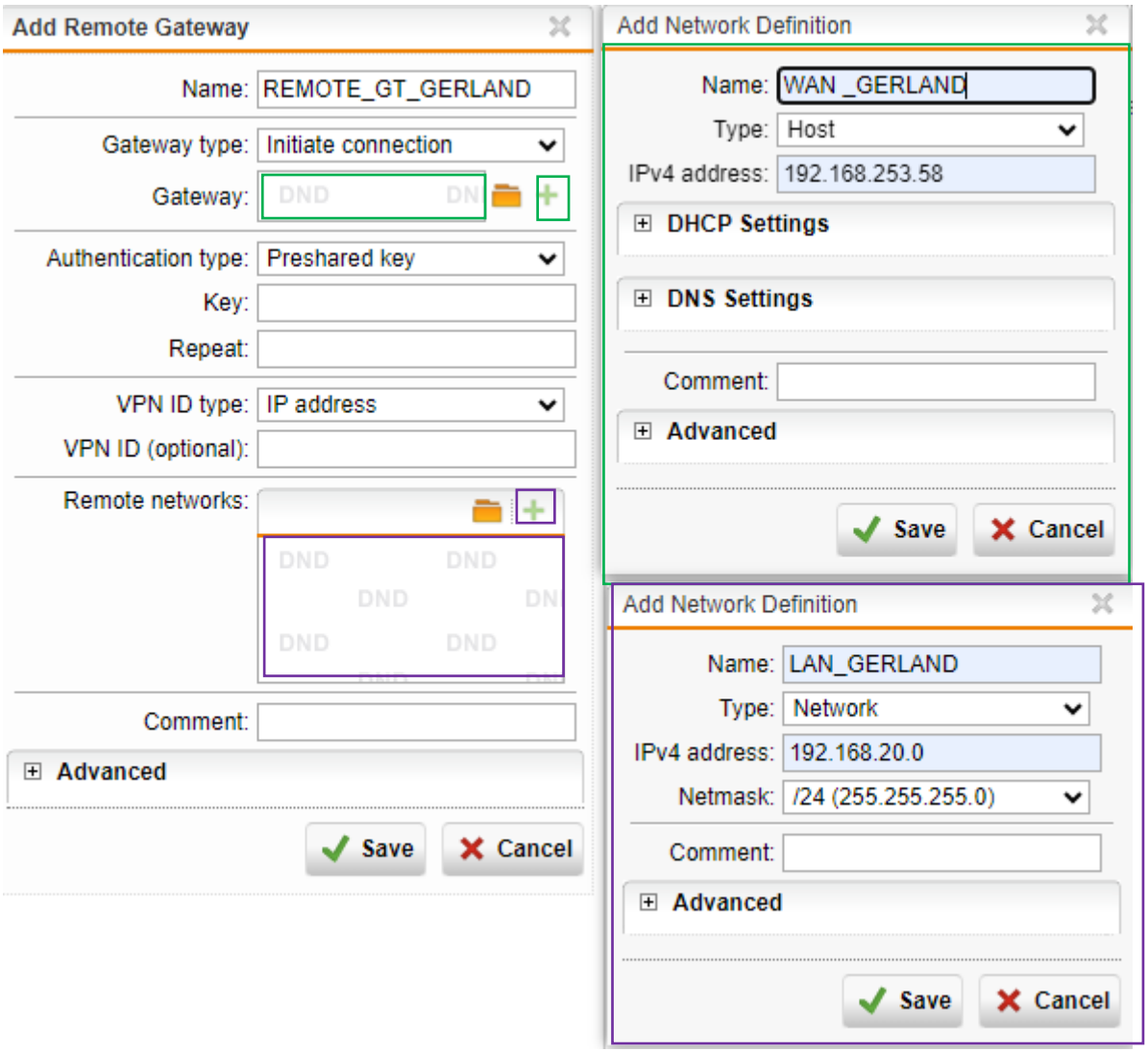
A partir de là notre NAT est opérationnel, il manque la mise en place la « remote gateway » puis de la « connection IPsec », Alain va d'abord configurer la remote gateway

IV) Mise en place d'une remote gateway

Maintenant Alain va créer une remote gateway (passerelle lointaine) pour que les deux WAN puissent communiquer.



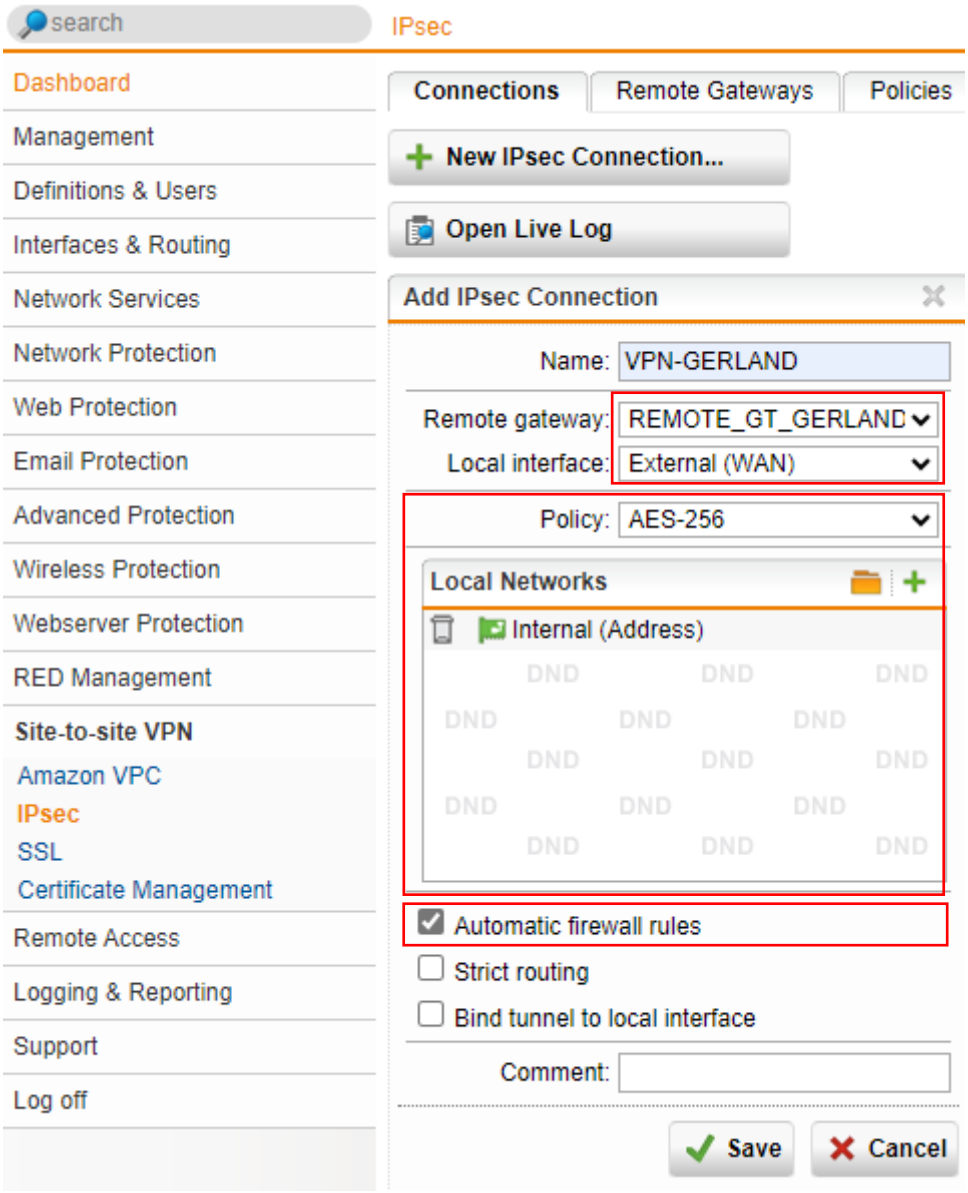
Alain va aller dans l'onglet « Site-to-site VPN », puis dans IPsec. Puis cliquer sur « remote gateway » ensuite sur « new remote gateway ».



En « Gateway type », Alain mettra « Initiate Connection » pour commencer les échanges entre les routeurs, ensuite en Gateway il faudra mettre la WAN du site distant, dans notre cas c'est celle de Gerland, en clé Alain mettra une suite de caractère qui sera identique à la remote gateway du routeur de Gerland. Et le remote network sera le LAN de Gerland.

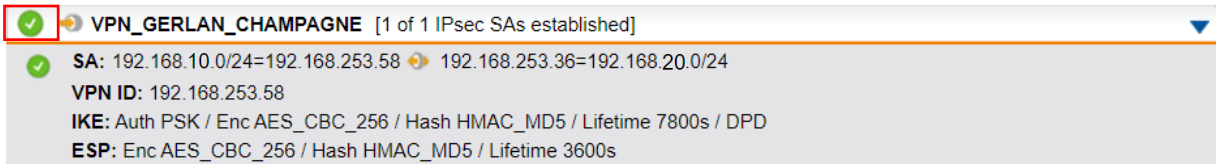
Lorsque la remote gateway est créer il ne manque plus qu'à créer la connexion qui symbolise la phase 2 du protocole IPsec.

V) Création de l' IPsec connection :



Alain va créer la connexion entre les deux routeurs le premier carré rouge représente la phase tunneling et le deuxième carré rouge représente la phase de cryptage et la connexion entre les deux LAN. Dans la remote gateway vous allez mettre la remote gateway que vous venez de créer et en local interface votre Wan, car la première connexion se fait via les WAN, puis en policy vous pouvez mettre le AES-256 qui est sécurisé. Le local network sera votre LAN que vous pouvez sélectionner de la même manière que pour le NAT. Si vous avez l'option pour créer automatiquement les règles de firewall, cocher la

Maintenant, Alain fait la même chose sur le site de champagne et vous pourrez voir alors les deux sites se connecter directement



Vous venez de faire votre premier VPN, BRAVO !