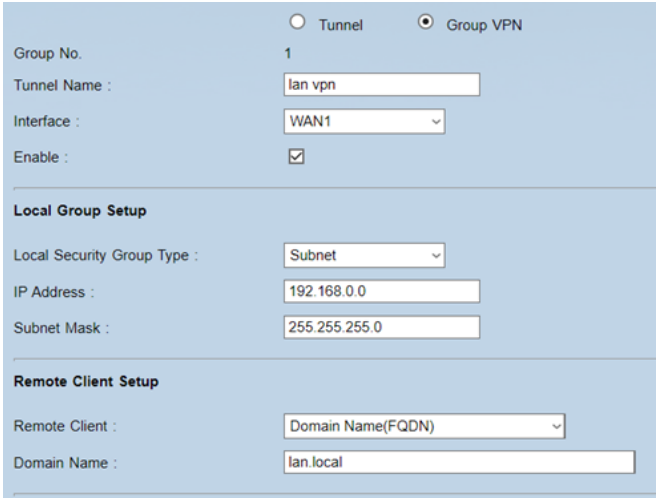
VPN IPsec - Client-to-Site

- Configuration Serveur
  - Configuration générale

« Tunnel name » : Nom du tunnel
« Interface » : Interface d’écoute du tunnel

Local Group Setup
« Local security groupe type » : Subnet
« IP Address » : Adresse du réseau local
« Subnet Mask » : Masque du réseau local

Remote client Setup
« Remote client » : Domain Name(FQDN)
« Domain Name » : Domaine DNS sur lesquels les clients distants seront



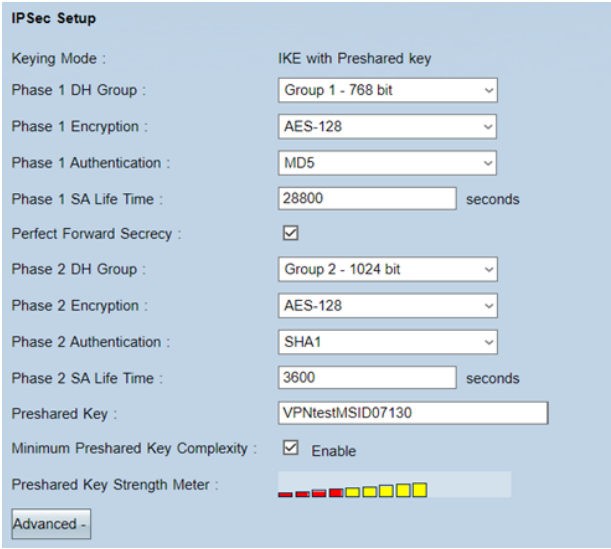
  - Configuration phase 1 et 2

Phase 1 :
Group : Group 1 – 768 bit
Encryption : AES-128
Authentification : MD5
Sa Life Time : 28800

Phase 2 :
Group : Group 2 – 1024 bit
Encryption : AES-128
Authentification : SHA1

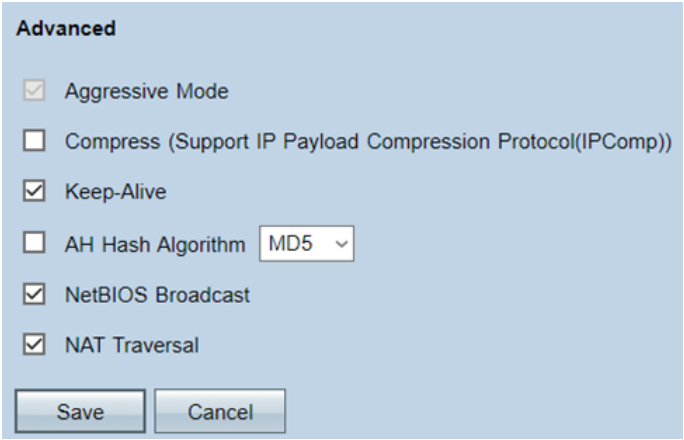
Sa Life Time : 3600

Preshared Key : « Mot de passe » complexe à renseigner



- Advanced

Cocher :
« Aggressive Mode »
« Keep-Alive »
« NetBIOS Brodcast »
« NAT Traversal »



- ## Configuration Client

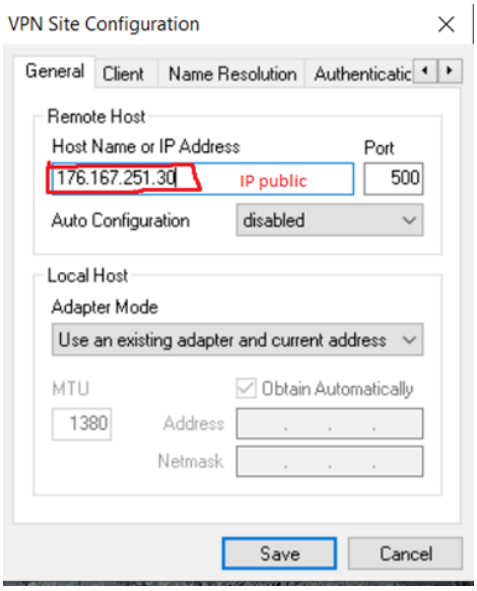
Télécharger le logiciel Shrew soft VPN client for Windows

https://www.shrew.net/download/vpn

- Configuration Générale

Remote host :
« Host name or IP address » : IP WAN du réseau distant
« Port » : 500
« Auto configuration » : Disable

Local Host :
« Adaptateur mode » : Use an existing adapter and current address



- Configuration des ports et paramètre réseau « Client »

Firewall Options :
« NAT Traversal » : Enable
« NAT Traversal Port » : 4500
« IKE Fragmentation» : Disable

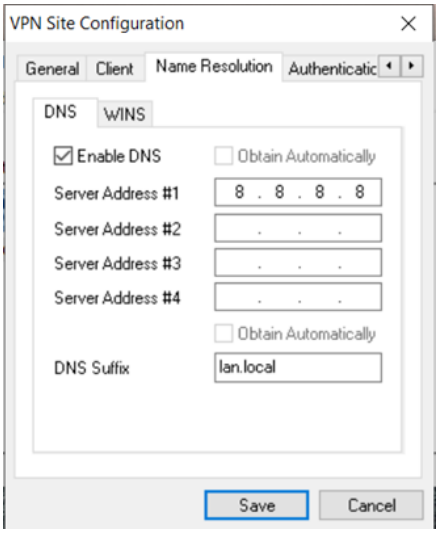
Other options:
Cocher :
« Enable dead peer detection »
« Enable ISAKMP Failure Notification »

- Configuration DNS

Cocher Enable DNS
Servers Address #1 : 8.8.8.8

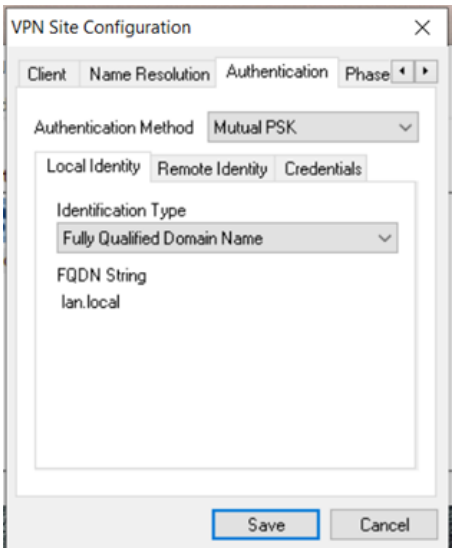
DNS Suffix : Nom du domaine renseigner sur le routeur

Onglet WINS, décocher la case.



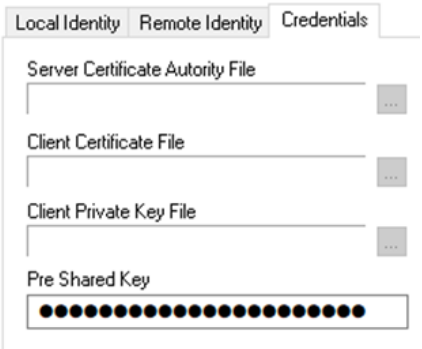
- Configuration de l’authentification

Authentication Method : Mutual PSK
Onglet « Local identity »
« Identification type » : Fully Qualified Domain Name.
« FQDN String » : Nom du domaine renseigner sur le routeur



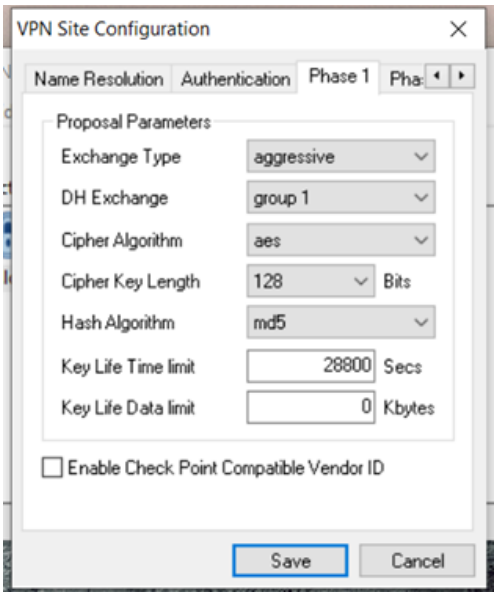
Onglet « Credentials »

Pre Shared Key Entrer la clé partager configurer sur le serveur.



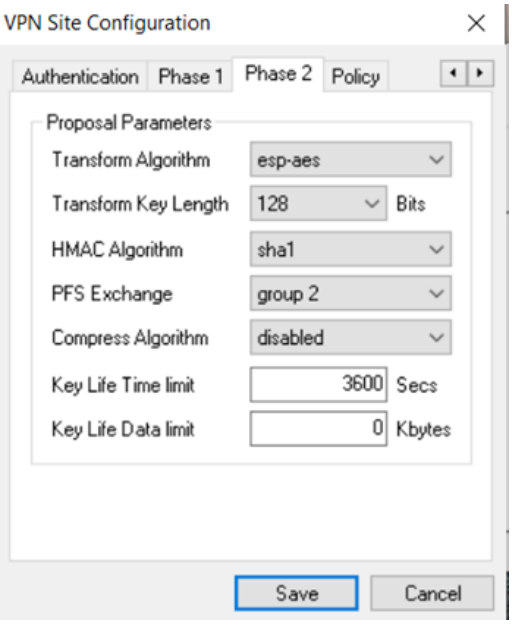
- Configuration de la phase 1

Exchange Type : Aggressive
DH Exchange : Group 1
Cipher Algorithm : AES
Cipher Key Length : 128
Hash Algorithm : MD5
Key Life Time Limit : 28800



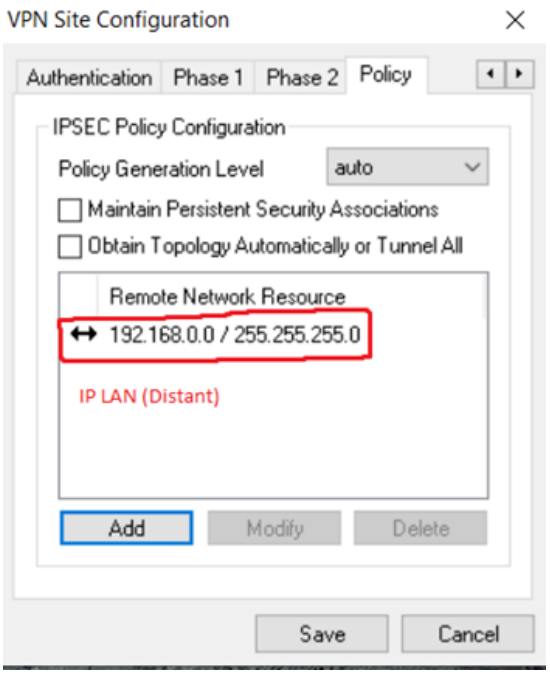
- Configuration de la phase 2

Transform Algorithm : ESP-AES
Transform Key Length : 128
HMAC Algorithm : SHA1
PFS Exchange : Groupe 2
Compress Algorithm : Disable
Key Life Time Limit : 3600



- Configuration du réseau distant

« Policy Generation Level » -> Auto
Décocher « Obtain topology Automatically or tunnel All »
« Add » Ajouter l’adresse du réseau local distant avec son masque



Revision #4
Created 11 May 2023 15:38:56 by Corentin Roche
Updated 30 April 2024 08:22:20 by Corentin Roche