

# [Cisco] 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

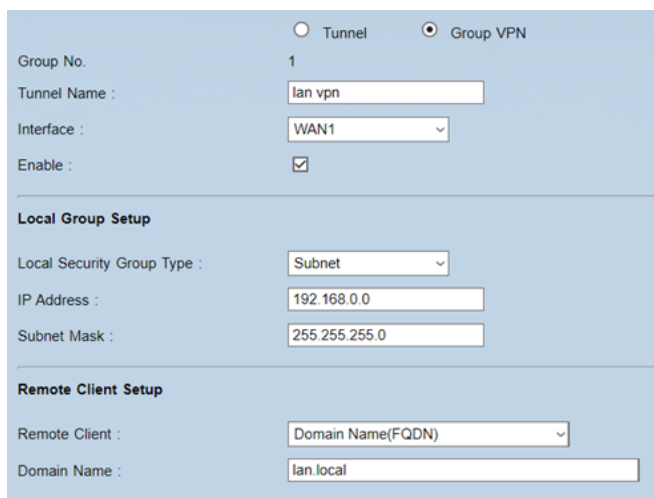
« IP Address » : Adresse du réseau local

« Subnet Mask » : Masque du réseau local

## Remote client Setup

« Remote client » : Domain Name(FQDN)

« Domain Name » : Domaine DNS sur lesquels les clients distants seront



The screenshot shows a configuration interface for a Cisco VPN. It is divided into three main sections:

- Tunnel Configuration:** Includes radio buttons for "Tunnel" (unselected) and "Group VPN" (selected). Below are fields for "Group No." (1), "Tunnel Name" (lan vpn), "Interface" (WAN1), and an "Enable" checkbox (checked).
- Local Group Setup:** Includes a dropdown for "Local Security Group Type" (Subnet), and input fields for "IP Address" (192.168.0.0) and "Subnet Mask" (255.255.255.0).
- Remote Client Setup:** Includes a dropdown for "Remote Client" (Domain Name(FQDN)) and an input field for "Domain Name" (lan.local).

- Configuration phase 1 et 2

## Phase 1 :

Group : Group 1 - 768 bit

Encryption : AES-128

Authentification : MD5

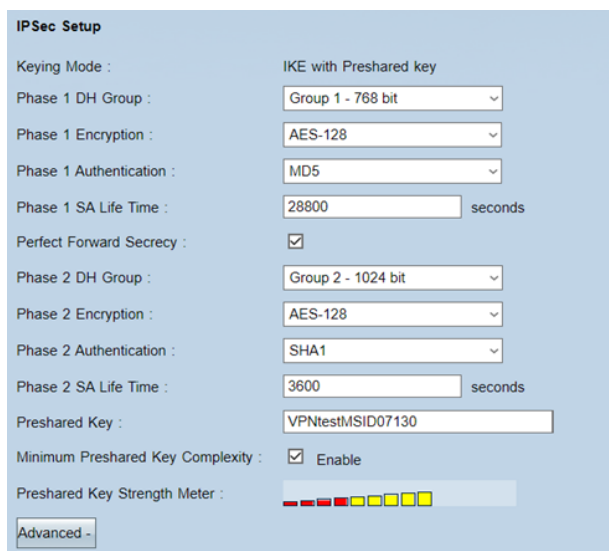
Sa Life Time : 28800

## Phase 2 :

Group : Group 2 - 1024 bit

Encryption : AES-128  
Authentication : SHA1  
Sa Life Time : 3600

Preshared Key : « Mot de passe » complexe à renseigner

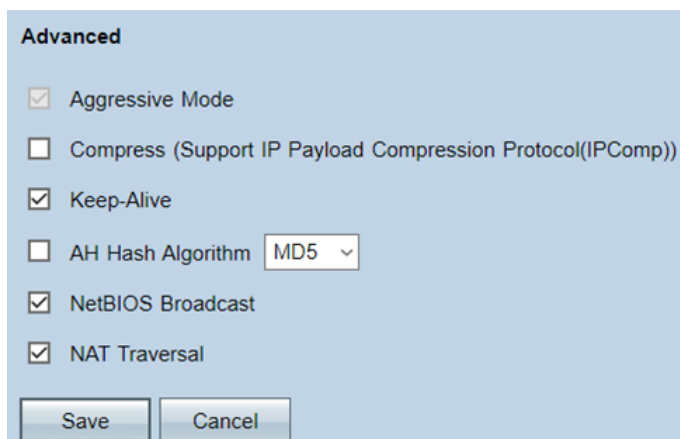


The image shows the 'IPSec Setup' configuration window. It is divided into two phases. Phase 1 is configured with 'IKE with Preshared key' as the Keying Mode, 'Group 1 - 768 bit' as the DH Group, 'AES-128' as the Encryption, 'MD5' as the Authentication, and '28800' seconds as the SA Life Time. Phase 2 is configured with 'Group 2 - 1024 bit' as the DH Group, 'AES-128' as the Encryption, 'SHA1' as the Authentication, and '3600' seconds as the SA Life Time. The Preshared Key is set to 'VPNtestMSID07130'. The 'Perfect Forward Secrecy' checkbox is checked. The 'Minimum Preshared Key Complexity' checkbox is also checked and labeled 'Enable'. Below this is a 'Preshared Key Strength Meter' with a progress bar showing approximately 80% completion. An 'Advanced -' button is located at the bottom left of the window.

o Advanced

Cocher :

- « Aggressive Mode »
- « Keep-Alive »
- « NetBIOS Broadcast »
- « NAT Traversal »



The image shows the 'Advanced' configuration window. It contains several checkboxes: 'Aggressive Mode' (checked), 'Compress (Support IP Payload Compression Protocol(IPComp))' (unchecked), 'Keep-Alive' (checked), 'AH Hash Algorithm' (unchecked, with a dropdown menu set to 'MD5'), 'NetBIOS Broadcast' (checked), and 'NAT Traversal' (checked). At the bottom of the window are 'Save' and 'Cancel' buttons.

## • Configuration Client

Télécharger le logiciel Shrew soft VPN client for Windows

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

- Configuration Générale

Remote host :

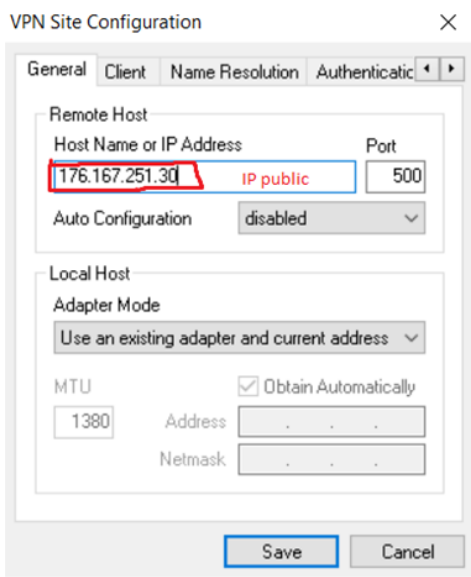
« Host name or IP address » : IP WAN du réseau distant

« Port » : 500

« Auto configuration » : Disable

Local Host :

« Adapter mode » : Use an existing adapter and current address



- Configuration des ports et paramètre réseau « Client »

Firewall Options :

« NAT Traversal » : Enable

« NAT Traversal Port » : 4500

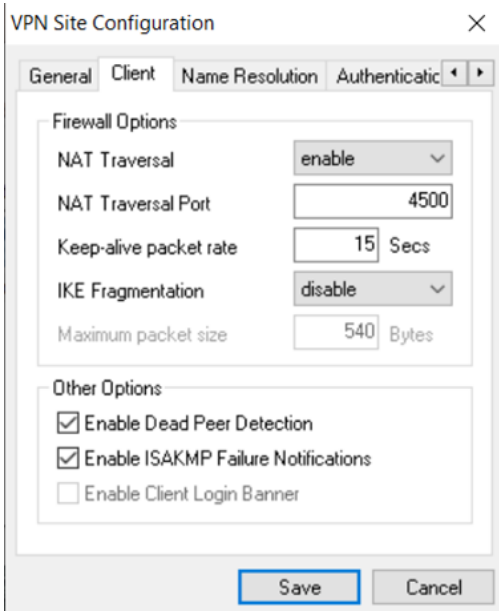
« IKE Fragmentation » : Disable

Other options:

Cocher :

« Enable dead peer detection »

« Enable ISAKMP Failure Notification »



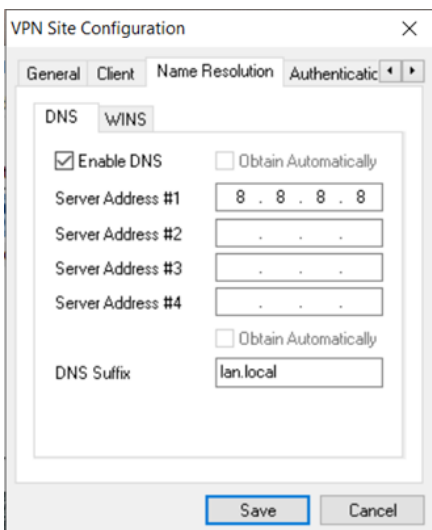
- Configuration DNS

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 »

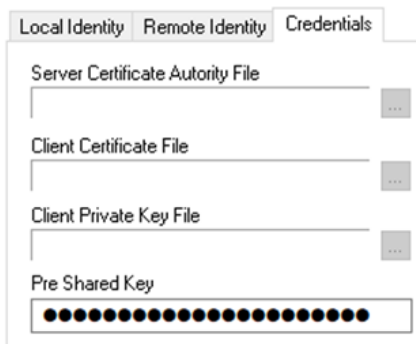
« Identification type » : Fully Qualified Domain Name.

« 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

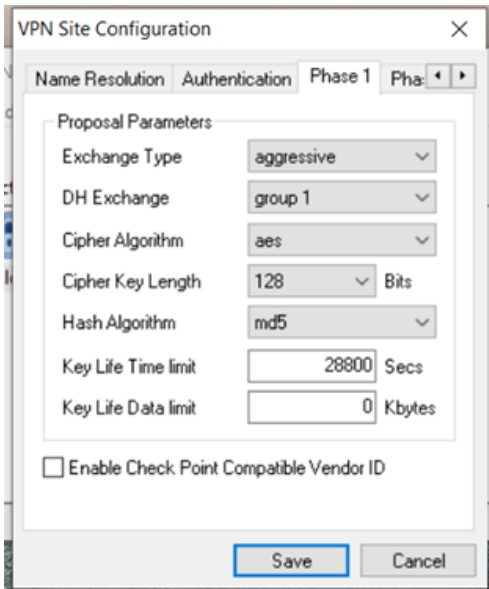
DH Exchange : Group 1

Cipher Algorithm : AES

Cipher Key Length : 128

Hash Algorithm : MD5

Key Life Time Limit : 28800



- Configuration de la phase 2

Transform Algorithm : ESP-AES

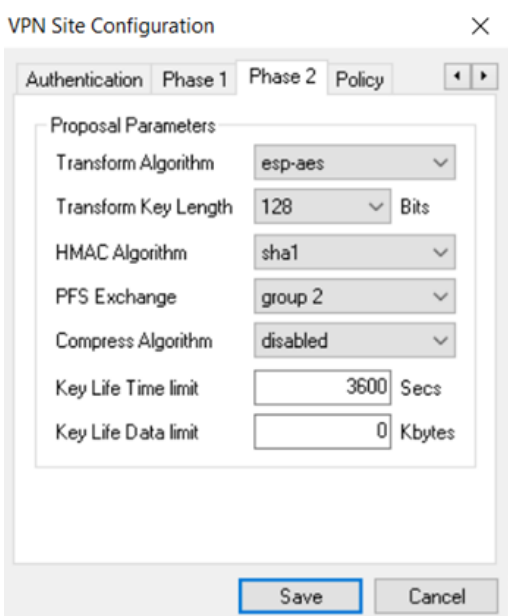
Transform Key Length : 128

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

Authentication Phase 1 Phase 2 Policy

IPSEC Policy Configuration

Policy Generation Level: auto

Maintain Persistent Security Associations

Obtain Topology Automatically or Tunnel All

Remote Network Resource

↔ 192.168.0.0 / 255.255.255.0

IP LAN (Distant)

Add Modify Delete

Save Cancel

Revision #5

Created 2023-05-11 15:38:56 UTC by Corentin Roche

Updated 2026-04-20 13:51:32 UTC by Corentin Roche