Historique des versions :

Révision	Date	Objet
1.0.1	02/12/2024	Création du document
1.0.2	02/12/2024	Corrections et mise en forme du document

Auteurs et Intervenants :

Initiales	Nom	Fonction	Organisation - Rôle
YK	Youssouf KEITA	Apprenti	BTS-SIO IIA LAVAL

Identification du document :

Document applicable	**à compter du 02 Décembre 2024**		
Identification du document			
Direction:	IIA Saint-Berthevin / BTS 2eme année		
Objet:	Installation serveur NPS sous Windows serveur 2022		
Domaine:	Architecture technique		
Nature:	Procédure d'installation		
N° d'ordre:	0001	Version:	1.0.1
Durée installation	Environ 2 heures.		
Nb pages:	44		
Nom fichier:	Procedure_Installation_SRV-NPS_V-1.odt		
Format document:	ODT réalisé avec Libre Office		

Table des matières :

I. Objectif du document :

Fournir un guide clair et structuré pour installer, configurer et sécuriser un serveur NPS (Network Policy Server), assurant l'authentification et l'autorisation des connexions réseau tout en facilitant son utilisation, sa maintenance et son transfert de compétences à d'autres administrateurs.

II. Caractéristique générale :

Expression des besoins :

Mettre en place une solution interne pour gérer et sécuriser l'accès au réseau via des politiques centralisées d'authentification et d'autorisation. Cela inclut la prise en charge des utilisateurs distants et locaux, la compatibilité avec les services existants (Active Directory, DNS, etc.), et la protection contre les accès non autorisés.

1- Authentification et autorisation centralisées :

Configurer un serveur NPS pour gérer les demandes d'accès réseau à partir de clients RADIUS, comme les points d'accès Wi-Fi, les VPN, ou les commutateurs Ethernet.

2- Sécurisation des connexions :

Protéger les échanges grâce à des méthodes d'authentification robustes (EAP, PEAP) et en chiffrant les communications entre le serveur NPS et les clients réseau.

3- Personnalisation et gestion des politiques :

Définir des règles spécifiques basées sur les groupes d'utilisateurs Active Directory, l'emplacement des clients, ou les heures d'accès, tout en surveillant les connexions réseau pour détecter les abus ou les anomalies.

III. Pré-requis :

- Un serveur Windows Server 2022 intégré à un domaine Active Directory.
- Accès administrateur pour gérer les rôles et fonctionnalités.
- Configuration réseau fonctionnelle avec DNS et IP statiques.

IV. À qui s'adresse ce document ?

Compte tenu de sa nature technique, cette documentation est destinée aux techniciens informatiques ayant de solides compétences en systèmes et réseaux, ainsi qu'une compréhension approfondie des environnements Microsoft Windows Serveur. Les connaissances en gestion des rôles réseau (RADIUS, VPN) et des services Active Directory sont également essentielles.

V. Que ce qu'un serveur NPS sous Windows Server 2022 ?

Un NPS (Network Policy Server) sous Windows Serveur 2022 est le rôle serveur Microsoft qui permet de centraliser l'authentification, l'autorisation, et la gestion des comptes (AAA : Authentication, Authorization, Accounting) pour les connexions réseau. Il agit comme un serveur RADIUS, fournissant un point unique de contrôle pour appliquer des politiques d'accès réseau.

Fonctionnement :

IV. Installation des rôles et les fonctionnalités NPS via via Windows server 22:

1. Configuration réseau :

Nom de serveur :	SRV-NPS
Vlan :	0526
Nom de domaine :	Dom.test.fr (samba)

Adresse IP :	172.17.2.2
Masque :	255.255.255.0
Passerelle :	172.17.2.254
DNS :	10.223.255.2

2.Installation des rôles :

Pour installer un serveur NPS (Network Policy Server) à l'aide du Gestionnaire de serveur :

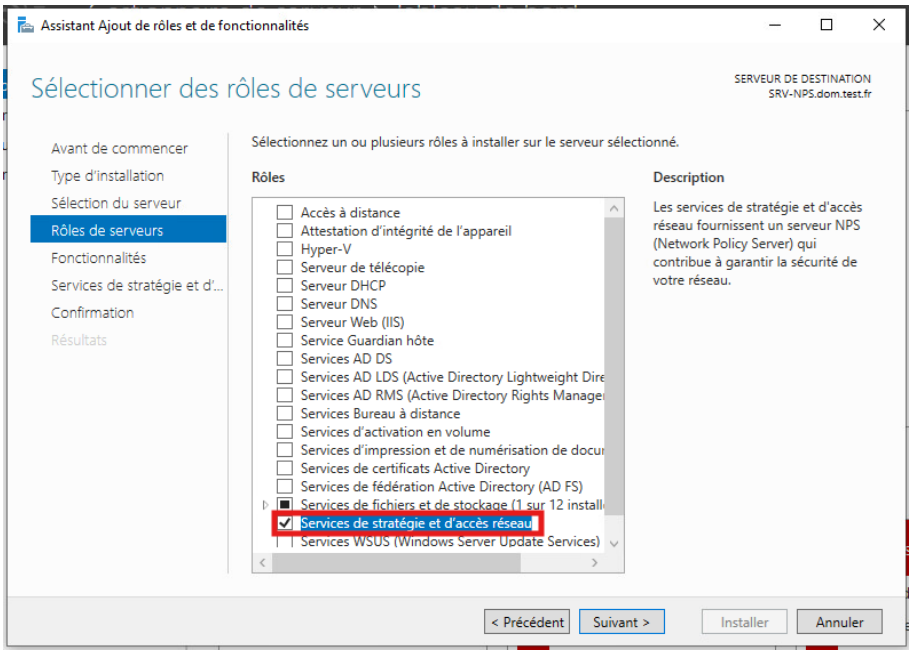
- Sur le serveur NPS, dans le Gestionnaire de serveur, cliquez sur Gérer, puis sur Ajouter des rôles et des fonctionnalités. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.

- Dans Avant de commencer, cliquez sur Suivant.

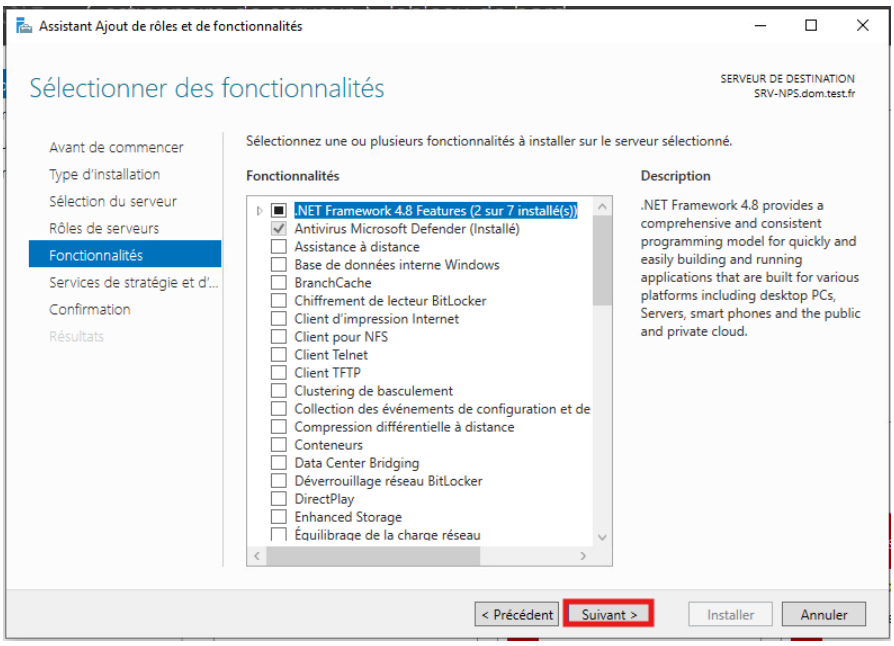
- Dans Sélectionner le type d'installation, vérifiez que Installation basée sur un rôle ou une fonctionnalité est sélectionné, puis cliquez sur Suivant.

- Dans Sélectionner le serveur de destination, vérifiez que Sélectionner un serveur du pool de serveurs est sélectionné. Dans Pool de serveurs, vérifiez que l'ordinateur local est sélectionné. Cliquez sur Suivant.

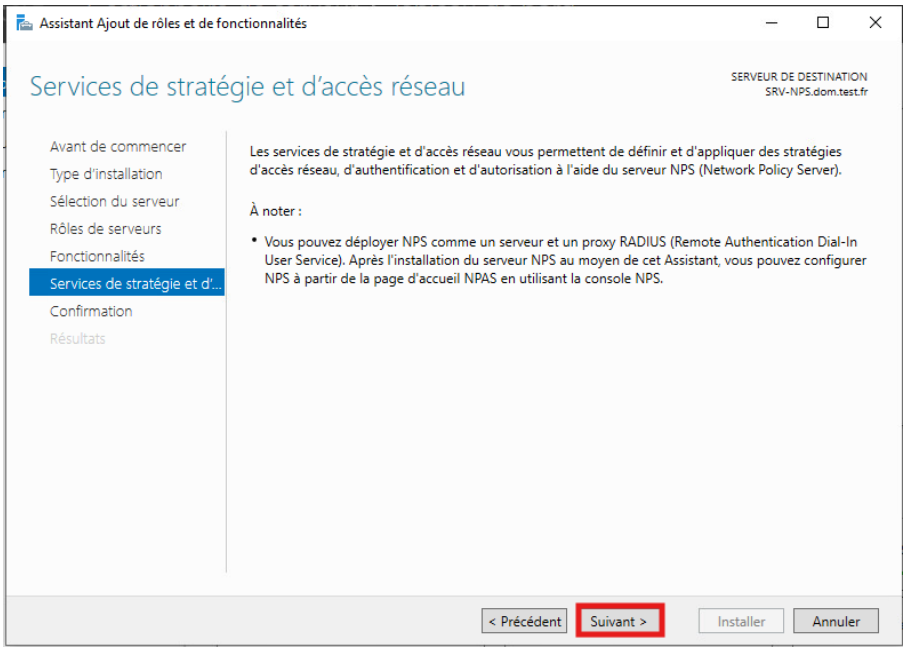
- Dans Sélectionner des rôles de serveurs, dans Rôles, sélectionnez Services de stratégie et d'accès réseau. Une boîte de dialogue s'ouvre pour demander s'il faut ajouter les fonctionnalités requises pour les services de stratégie et d'accès réseau. Cliquez sur Ajouter les fonctionnalités, puis sur Suivant.



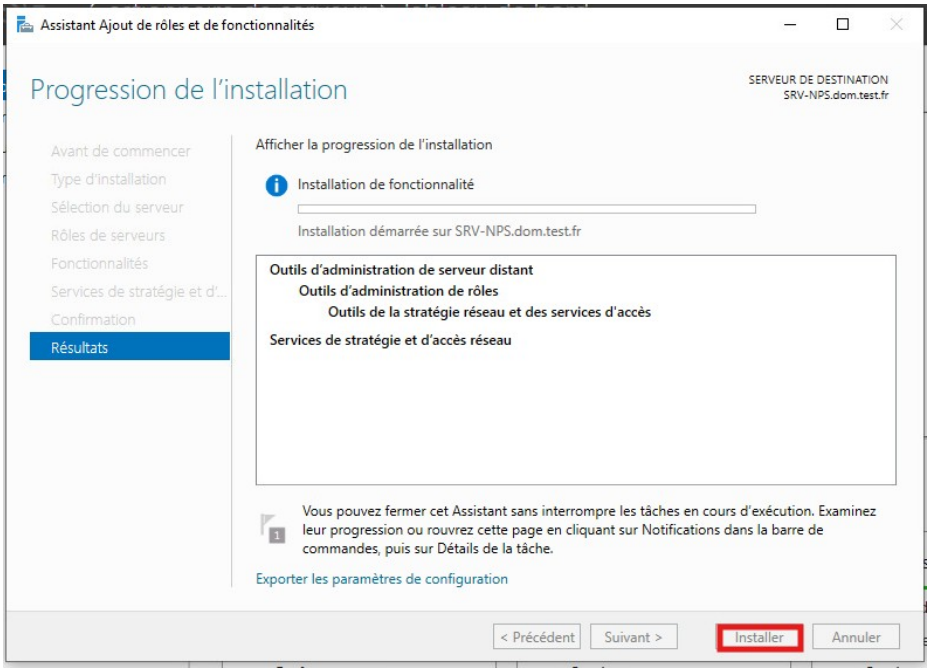
- Dans la page fonctionnalités, cliquez sur Suivant.



- À l'étape « **Services de stratégie et d'accès réseau** », faites « **Suivant** ».



- À l'étape « **Cofirmation »**, faites « **Suivant** ».



- Après l'installation, vous pouvez cliquer sur Fermer .
- Ajouter le serveur NPS au domaine Active Directory.

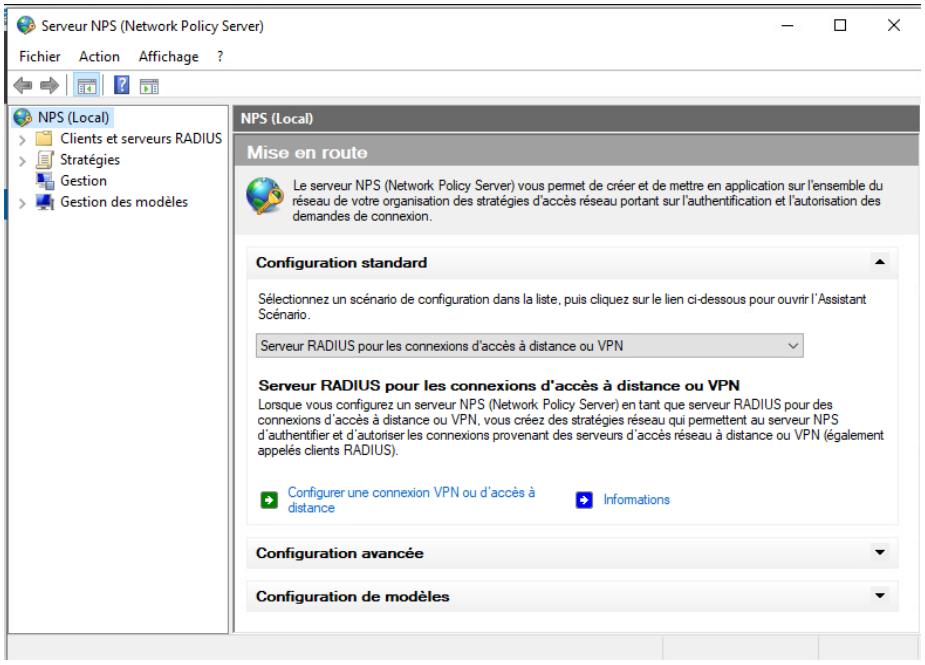
V. Configuration des clients RADIUS :

1. Déclarer les switchs et points d'accès comme clients RADIUS :

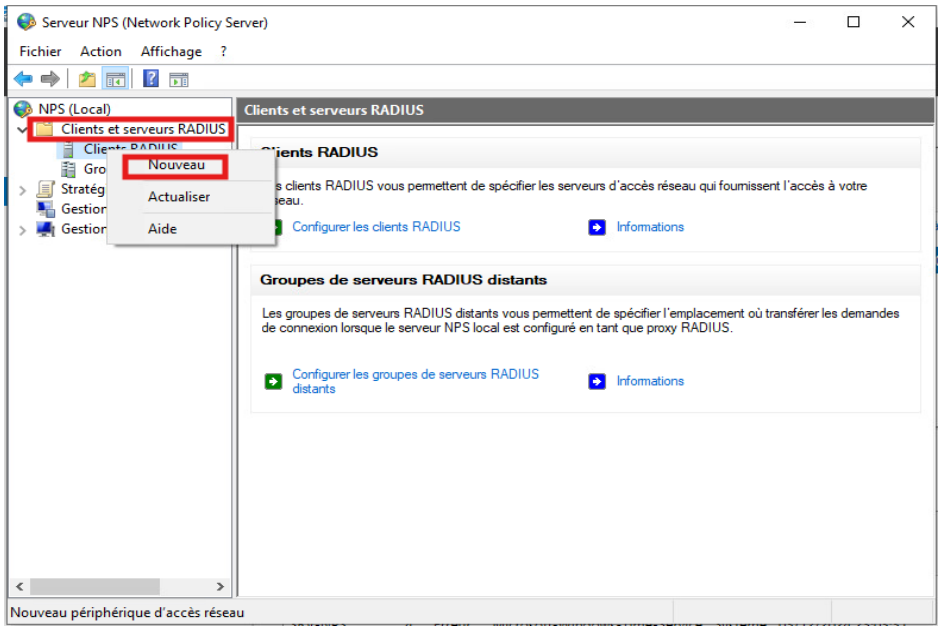
Ouvrez la console NPS :
Pour ce faire :

- Cliquez sur le menu « **Démarrer** », taper dans la barre de recherche « **NPS** », puis cliquer dessus pour l'ouvrir.

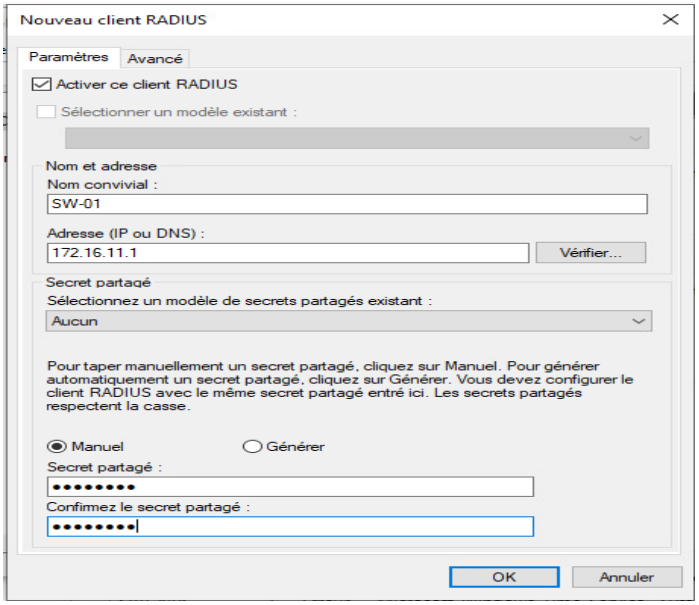
- Ensuite la page configuration du serveur **NPS** s'ouvre.



- Développer le dossier **Clients et serveurs RADIUS**, faites un clic droit sur « **Clients RADIUS** », puis faites « **Nouveau** ».

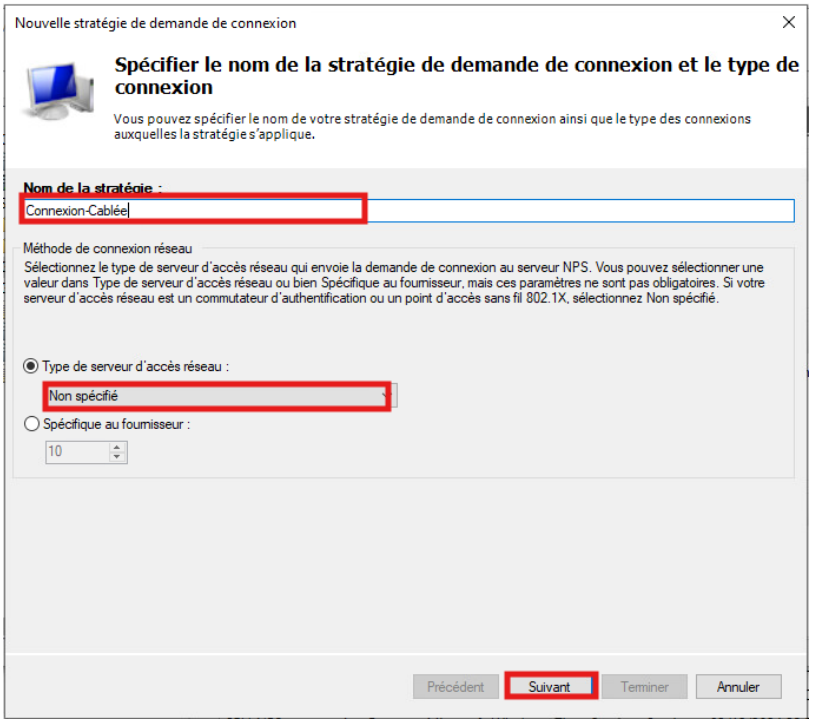


- Dans notre cas, le commutateur est un Cisco compatible 802.1x. Les éléments à renseigner sont : le nom "C**onvivial**" du client-RADIUS (SW-01) , son adresse IP (172.16.11.1 et "**secret partagé**" entre le serveur RADIUS et le **client RADIUS**, ici la chaîne "**Not...**"



2. Déclaration d'une stratégie de demande de connexion :

- On déclare une stratégie de demande de connexion pour Ethernet. Il s'agit de la connexion physique au média.
- Ici, on choisit un nom de stratégie. On laisse le type de serveur par défaut "**Non spécifié**" (nous utilisons un commutateur en tant que client Radius).
- Puis faites "**Suivant**".

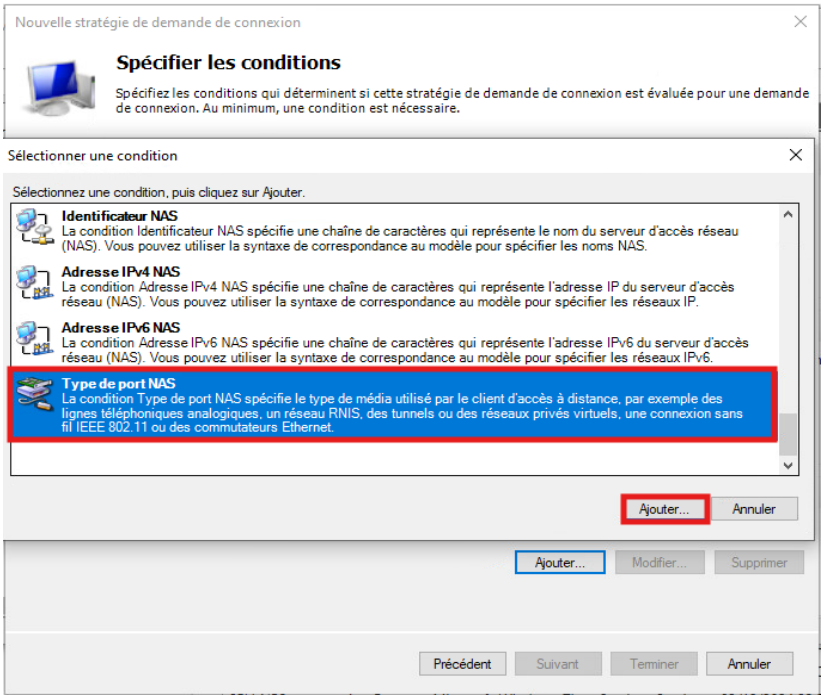


- Dans la page « **Spécifier une condition** », faites "Ajouter" ensuite on choisit d'indiquer un « **Type de port NAS** » (type de media concerné)

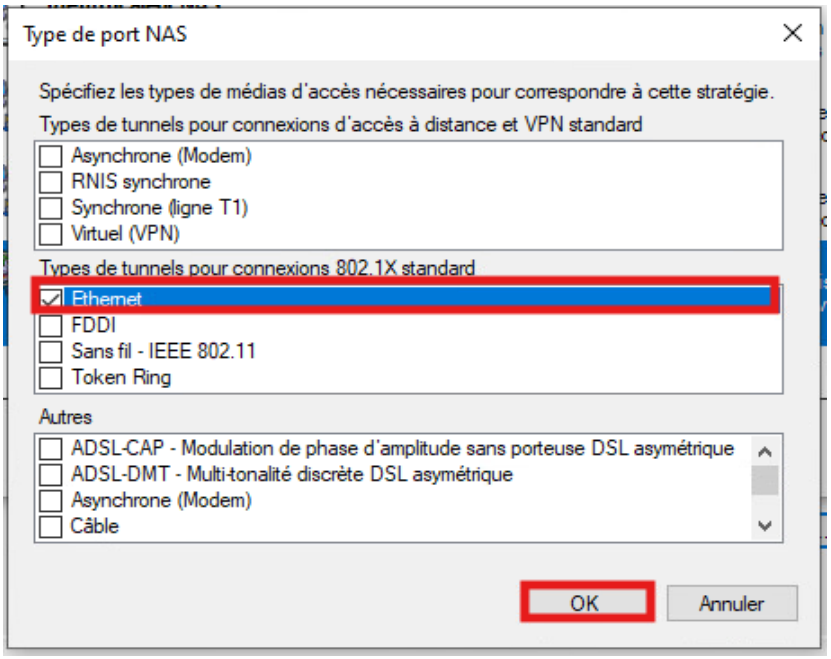
Info : NAS est ici l'acronyme "Network Access Server" et désigne le client RADIUS.

Ne pas confondre avec Network Authentication Server, qui désigne le serveur

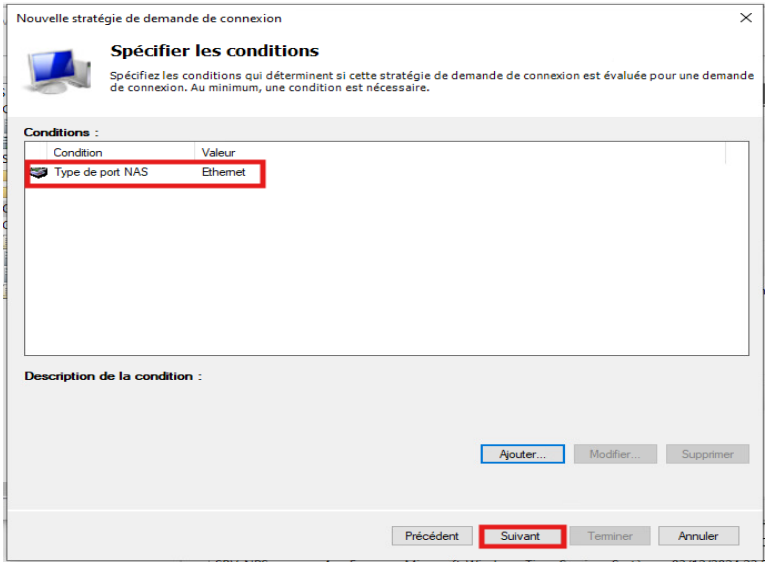
Radius lui-même.



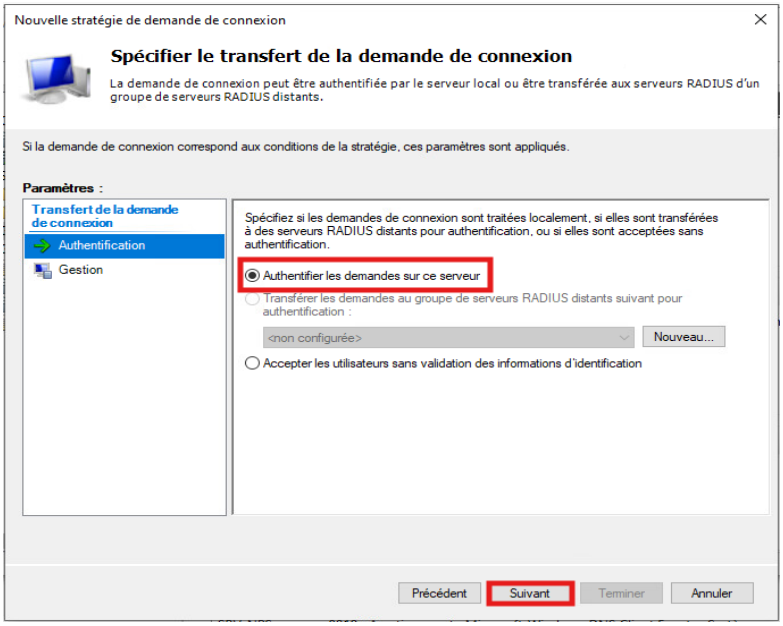
- Dans la page "**Type de port NAS**" on coche "**Ethernet**" puis "**OK**"



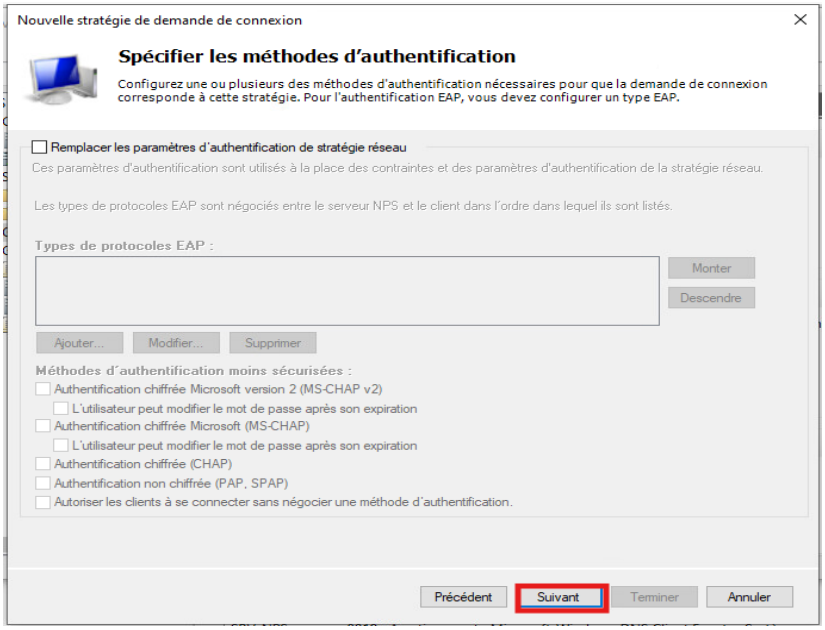
Récapitulatif :



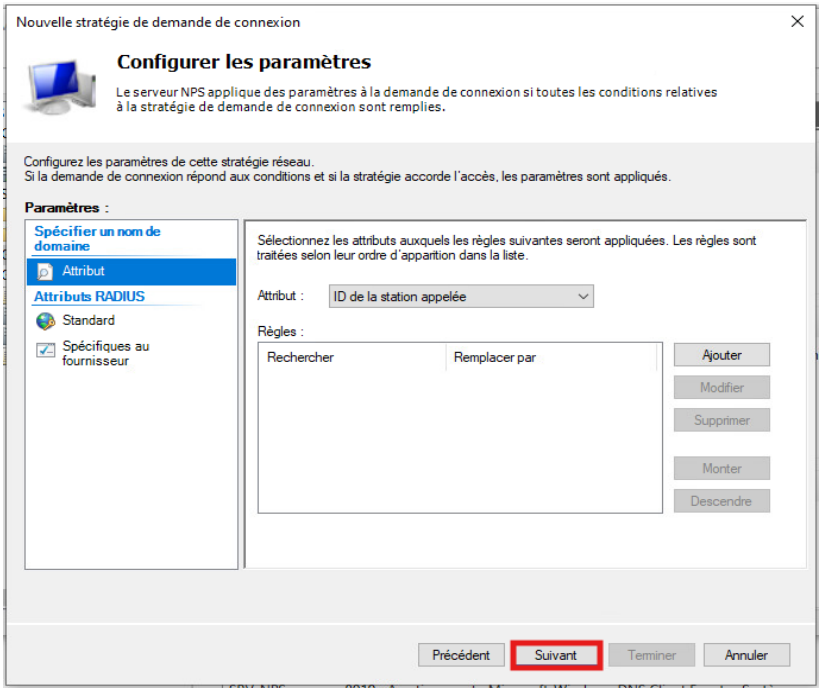
- Dans la page « **Spécifier le transfert de la demande de connexion** », laisser l'option par défaut « **Authentifier les demandes sur ce serveur** », (Les demandes seront traitées sur ce serveur et non sur un autre. Ce qui veut dire que ce NPS pourrait jouer un rôle de "PROXY NPS" s'il relayait les demandes à un autre serveur).



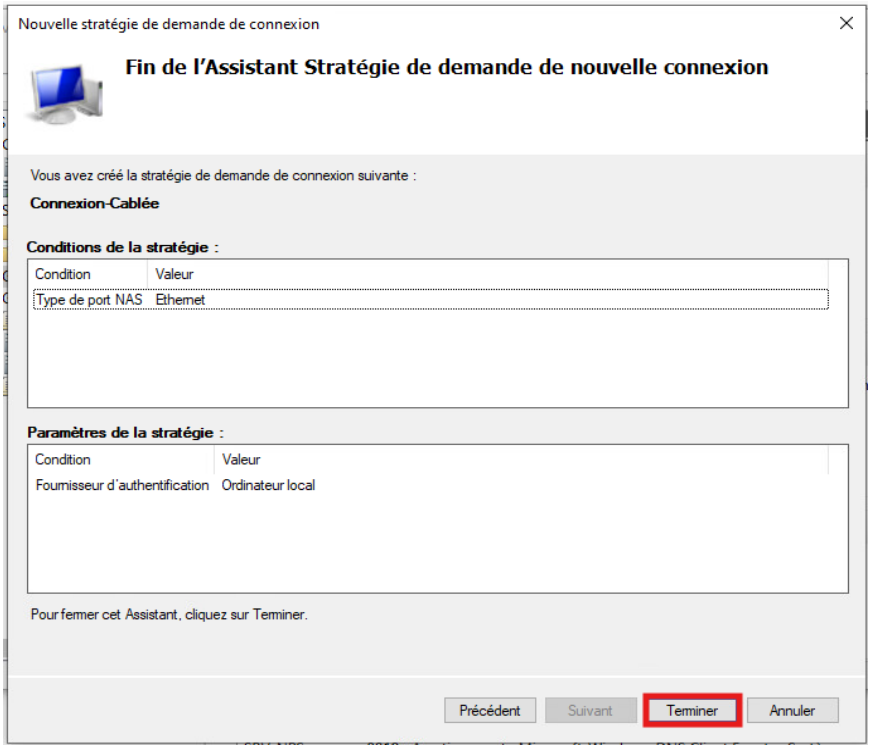
- À l'étape suivant, faites « **Suivant** » .



- Dans la page « **Configurer les paramètres** », faites « **Suivant** ».



- Dans la page « **Fin de l'Assistant stratégie de demande de nouvelle connexion** », faites « **Terminer** »



3. Déclaration d'une stratégie d'accès réseau pour le VLAN 2 (groupe "GP-Direction") :

La configuration repose sur une stratégie de demande de connexion unique, permettant de centraliser les critères d'accès au réseau. Chaque VLAN sera associé à une stratégie réseau distincte, garantissant un placement dynamique selon le groupe d'utilisateurs Active Directory :

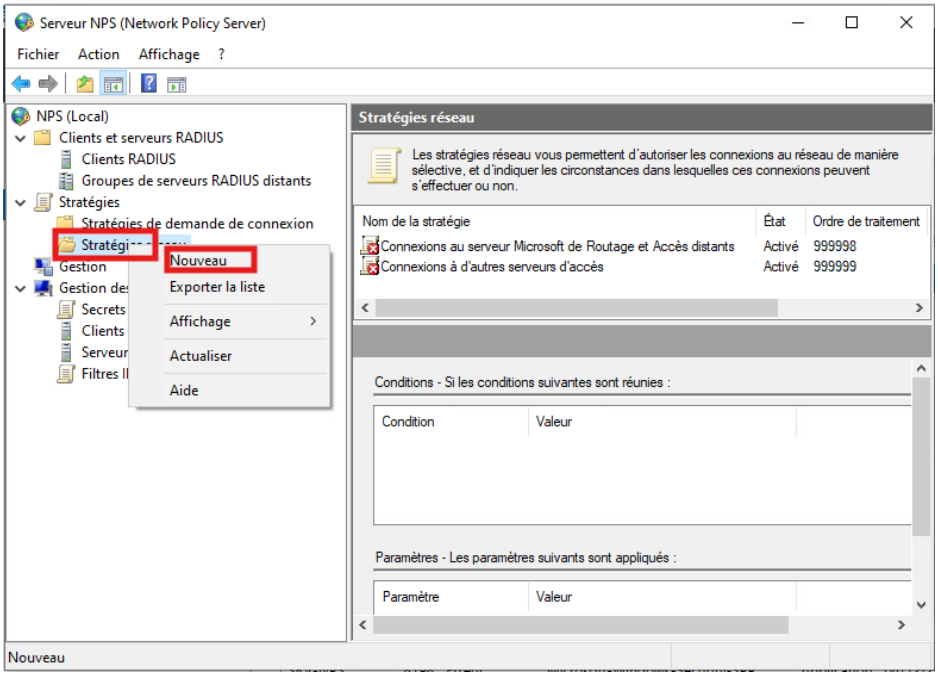
- Les membres du groupe **GP-Direction** seront assignés via une stratégie réseau dédiée au VLAN 2 (172.16.12.X/24).
- Une seconde stratégie réseau placera les membres du groupe **GP-RH** dans le VLAN 3 (172.16.13.X/24).
- De même, les membres du groupe **GP-Production** auront leur propre stratégie réseau pour accéder au VLAN 4 (172.16.14.X/24).

- Enfin, les utilisateurs non authentifiés ou ne correspondant à aucun groupe prédéfini seront automatiquement affectés au VLAN 254 (172.16.254.X/24) grâce à une stratégie réseau dédiée.

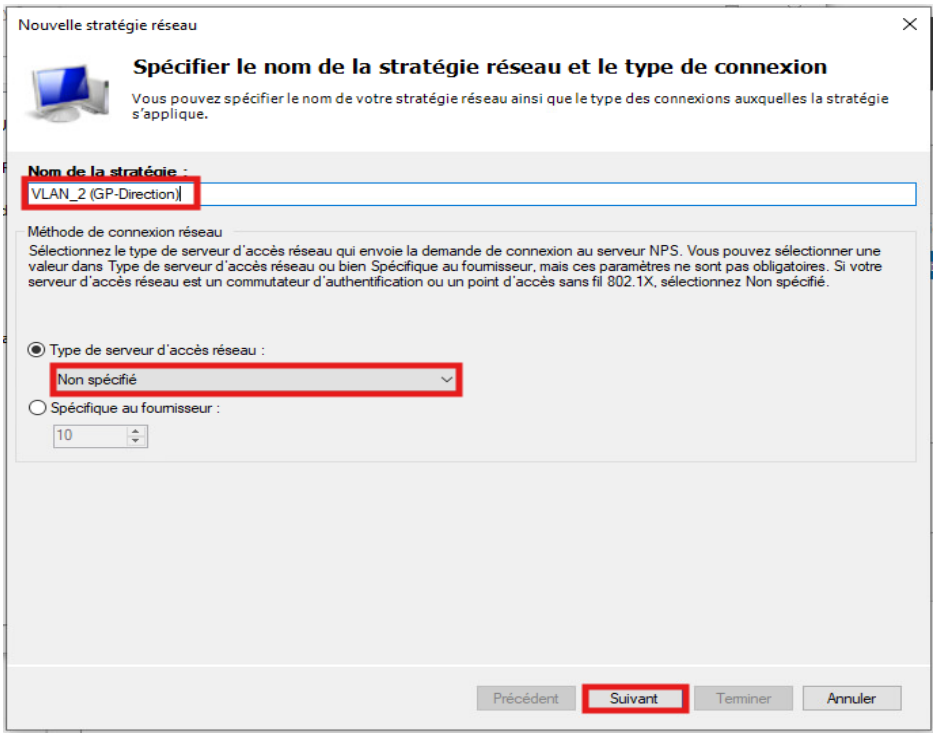
Cette architecture permet une gestion centralisée via une seule stratégie de demande de connexion, tout en offrant une flexibilité granulaire pour l'attribution des VLANs selon les besoins organisationnels.

Pour se faire :

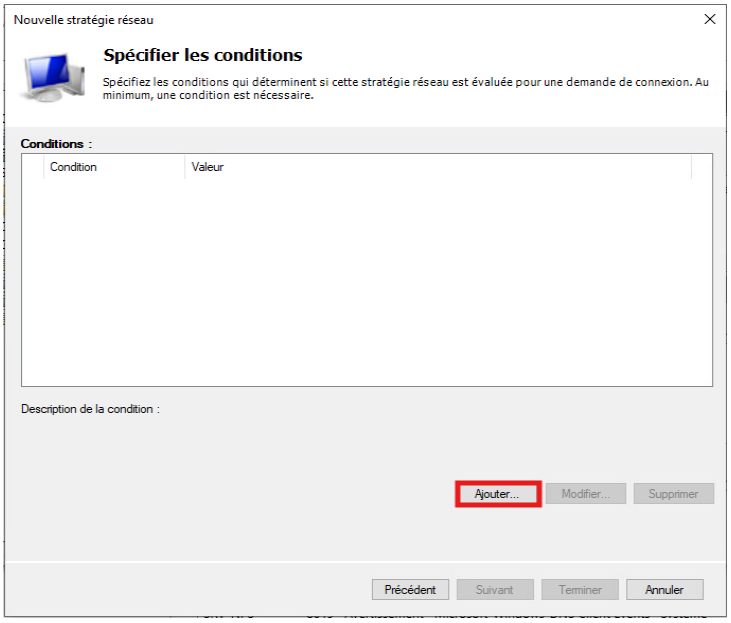
- Faites un clic droit sur « **Stratégie Réseau** », puis **Nouveau**



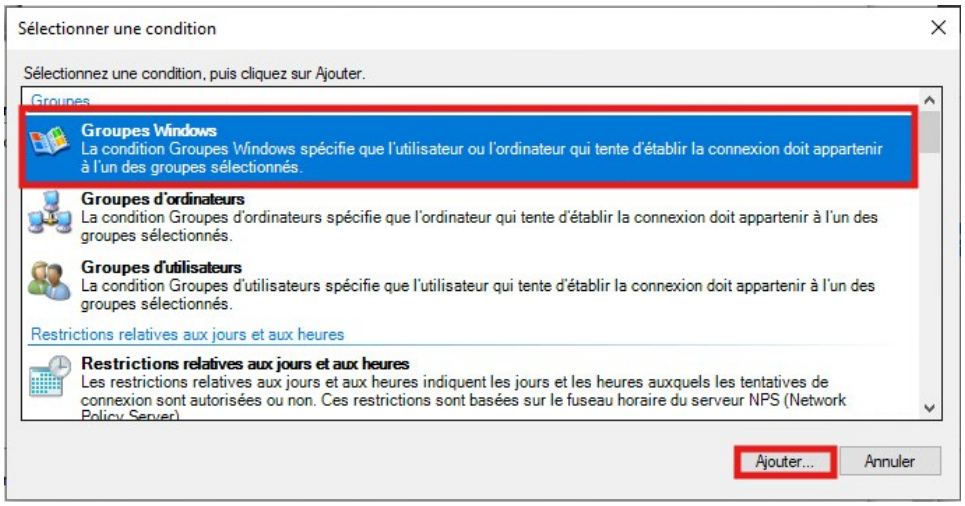
- Une page « **Nouvelle stratégie réseau** » s'affiche à l'écran, taper le nom de votre stratégie et dans l'option « **Type de serveur d'accès réseau** », laisser celle proposé par défaut « **Non spécifie** » pour une authentification via un commutateur 802.1x.



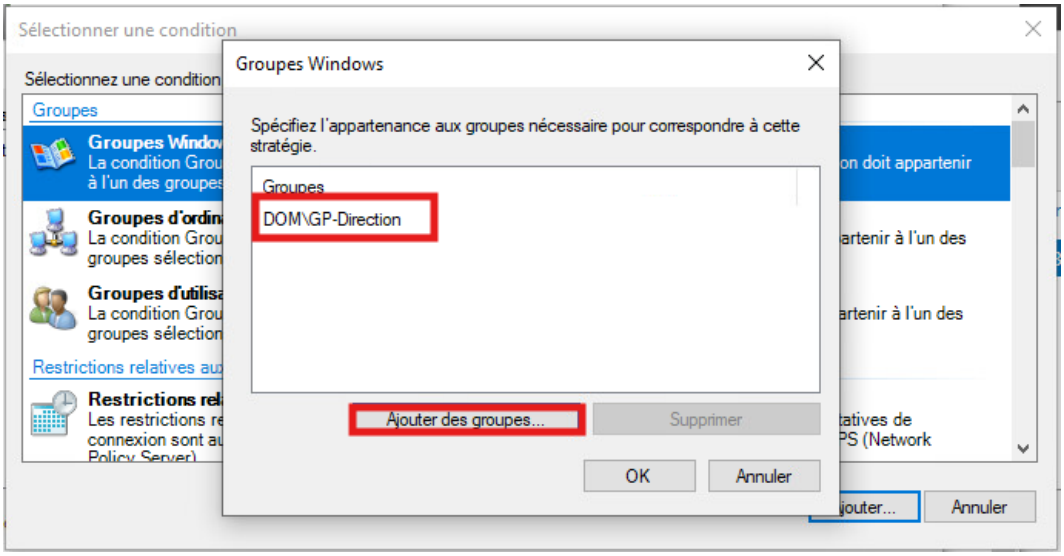
- À l'étape « **Spécifier les conditions** », faites « **Ajouter** » .



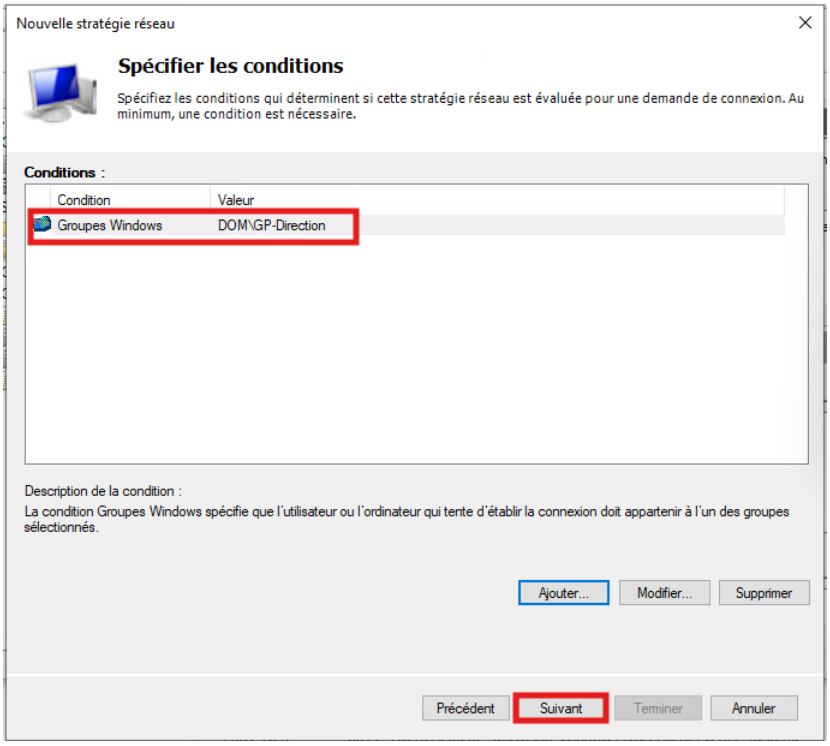
- Ensuite la page « **Sélectionner une condition** » s'affiche, sélectionner « **Groupe Windows** », puis faites « **Ajouter** ».



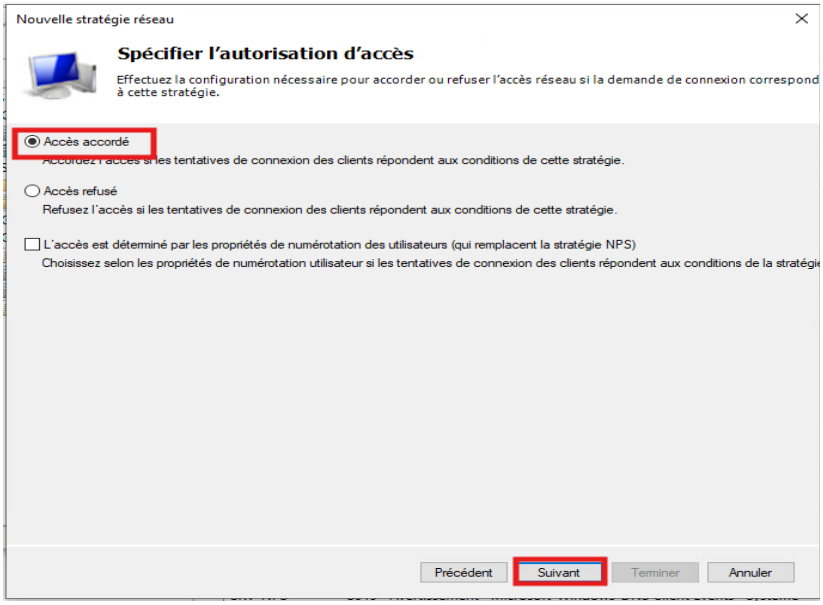
- Ensuite la page **Groupes Windows** s'affiche à l'écran, faites « **Ajouter des groupes** » puis chercher votre groupe et faites « OK » pour ajouter.



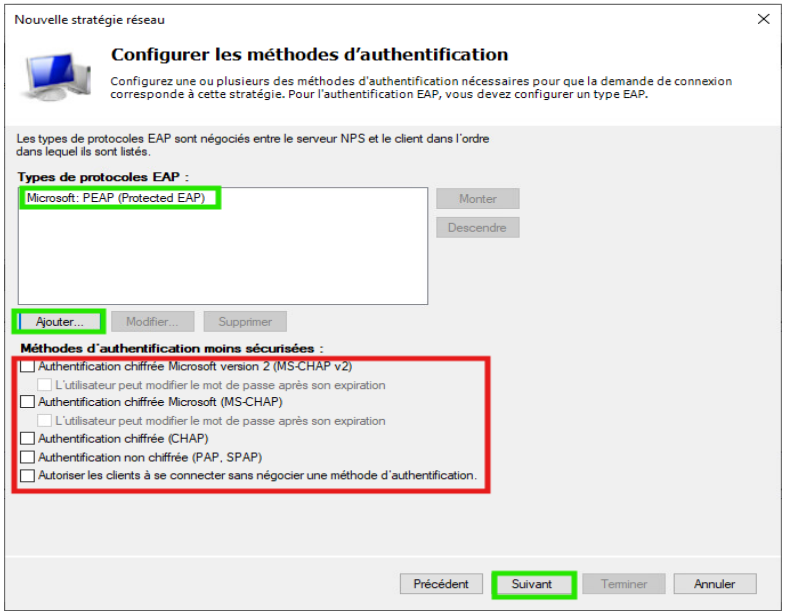
- Récapitulatif du choix des groupes Windows, faites « **Suivant** ».



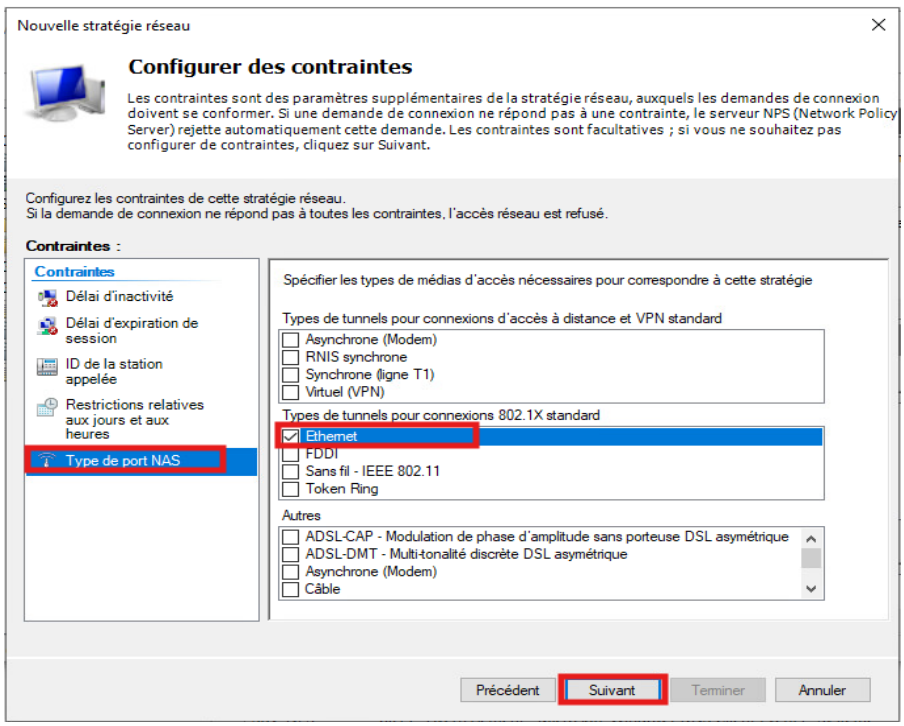
- À l'étape « **Spécifier l'autorisation d'accès** », ils est possible d'autoriser ou refuser l'accès.



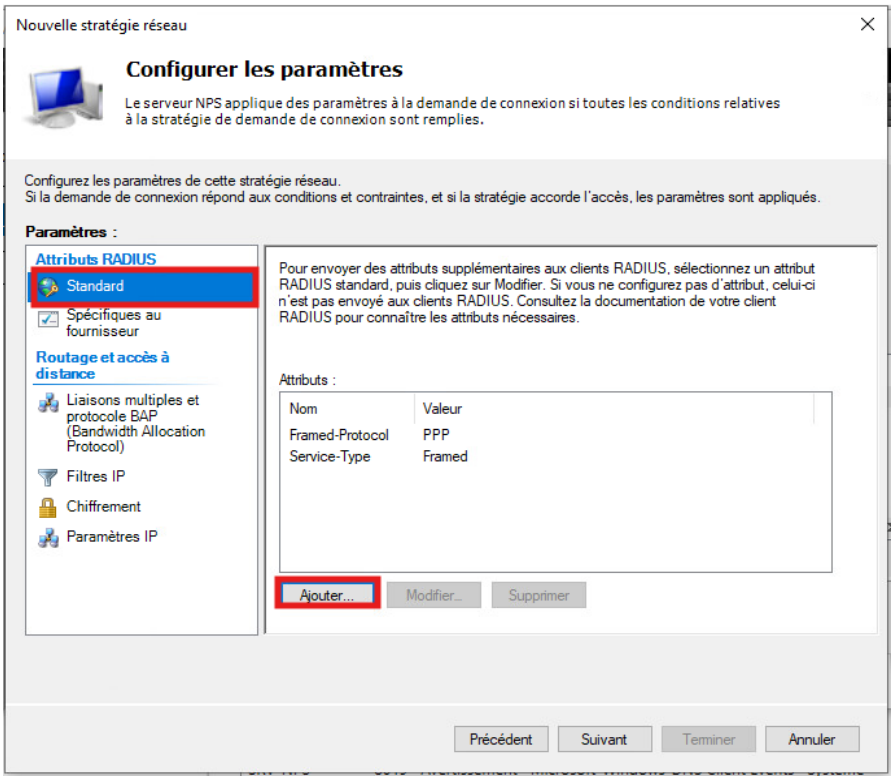
- Ensuite on décoche les authentification par défaut et on ajoute les types de protocoles accepté, faites « **Ajouter** », puis « **OK** », ici « **Micosoft : PEAP (protected EAP** ».



- Dans la page « **Configurer des contraintes** », on sélectionne « **Types de ports NAS** » et dans l'option type de tunnels pour connexion 802.1X … on coche la case « **Ethernet** ».

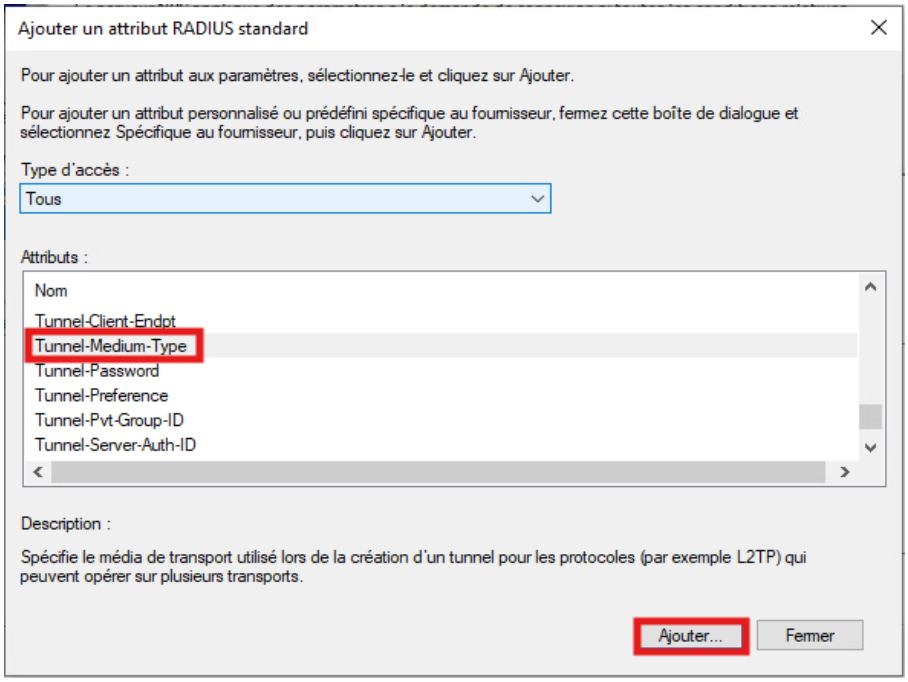


- Dans la page « **Configurer les paramètres** », dans la section « **Attributs RADIUS** », faites « **Ajouter** » pour ajouter des attributs de contrôle de trafic (**Tunnel-Medium-Type, Tunnel-Pvt-Group-ID et Tunnel-Type**).

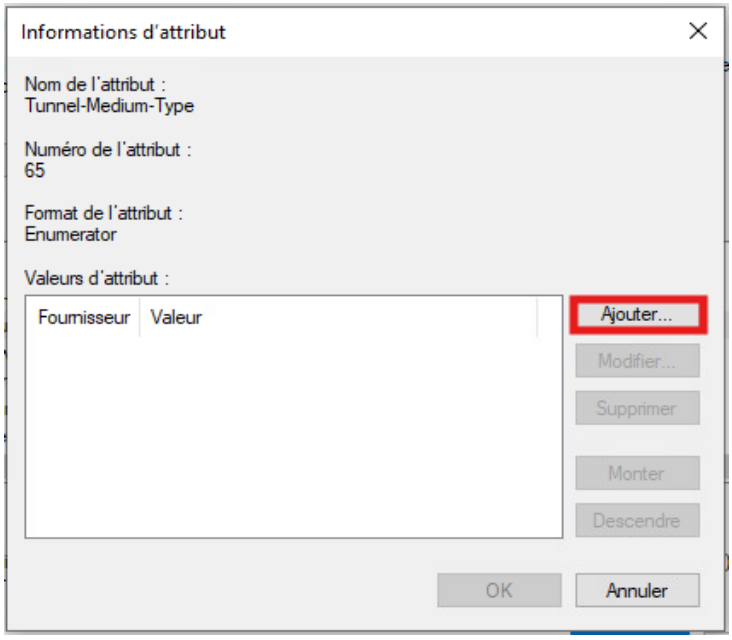


a) Ajout de l'attribut « Tunnel-Medium-Type » :

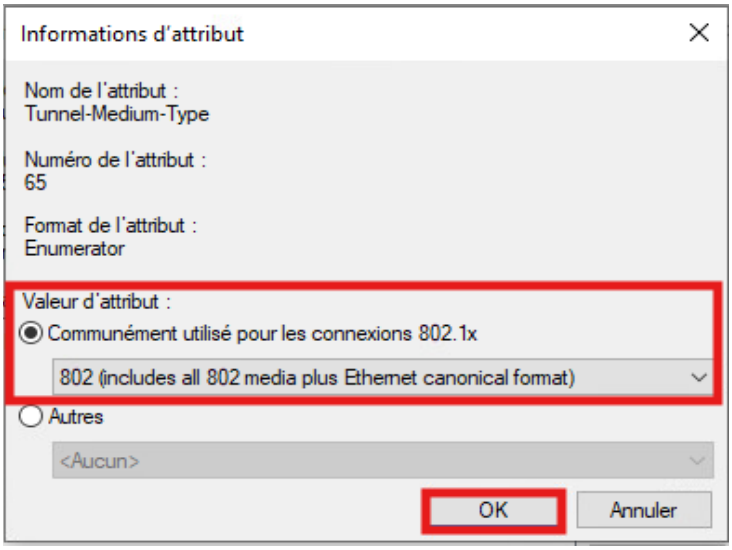
- Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».



- La page d'information d'attribut s'affiche à l'écran, faites « **Ajouter** ».

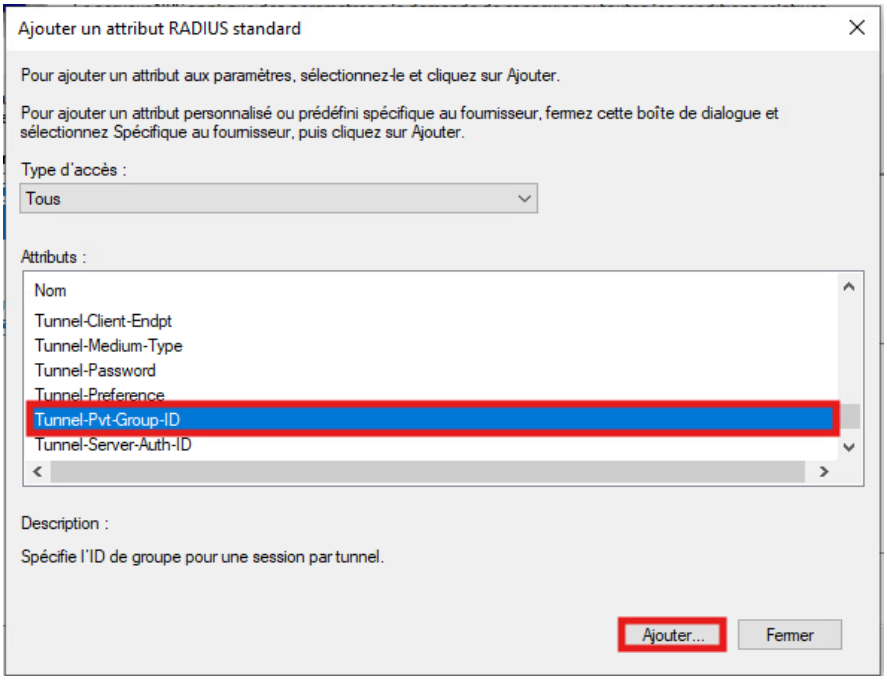


- Ensuite la deuxième page d'information d'attribut s'affiche à l'écran, laissez l'option « **Valeur d'attribut** » coché par défaut et faites « **OK** ».

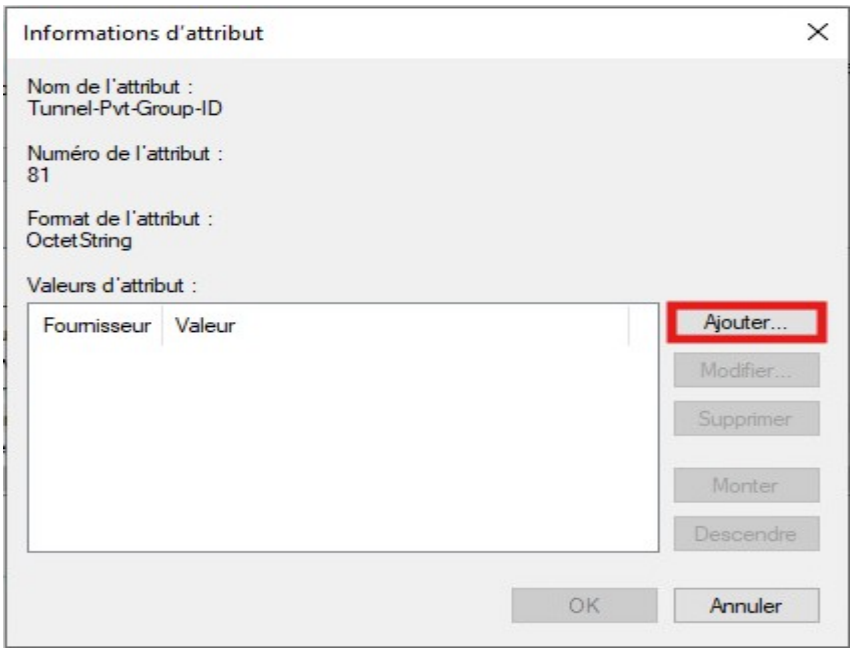


b) Ajout de l'attribut « Tunnel-Pvt-Group-ID » :

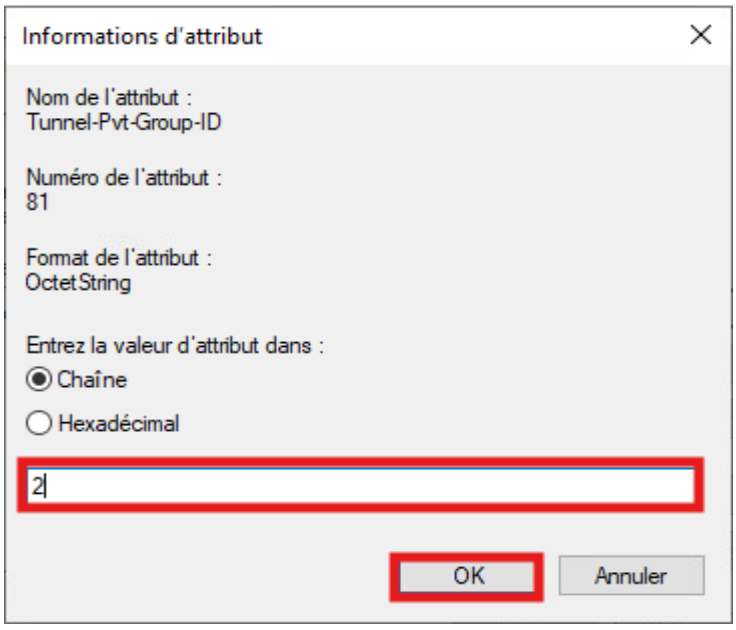
- Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».



- La page d'information d'attribut s'affiche à l'écran, faites « **Ajouter** ».

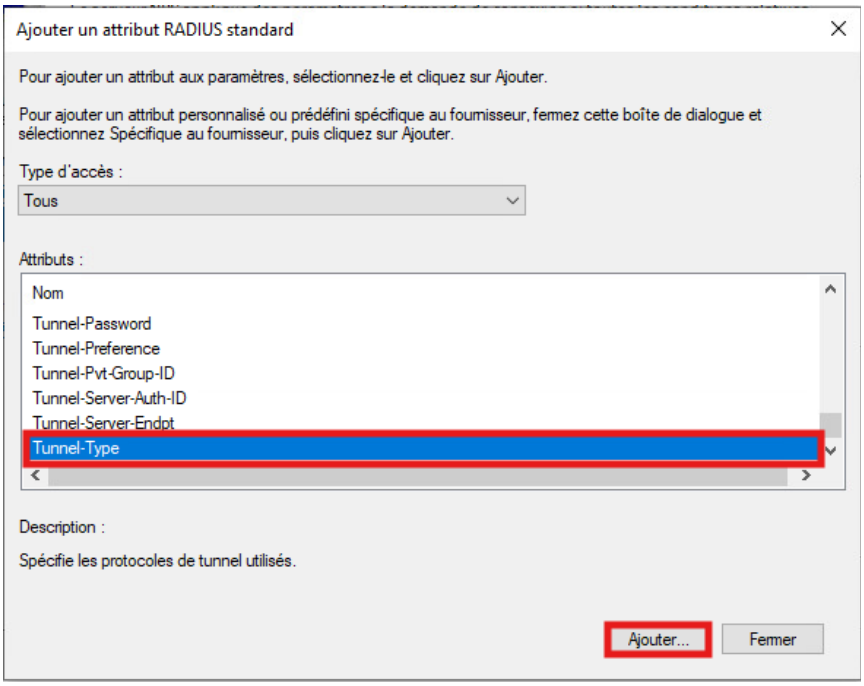


- Ensuite la deuxième page d'informations d'attribut s'affiche à l'écran, laissez l'option « **Chaîne** » coché par défaut et taper ID de VLAN concerné dans la case ici (VLAN 2), puis faites « **OK** ».

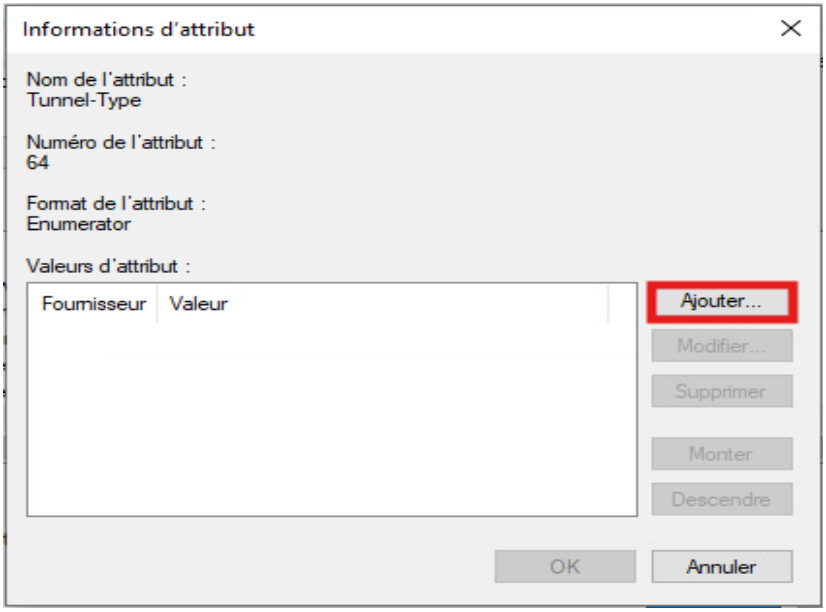


c) Ajout de l'attribut « Tunnel-Type » :

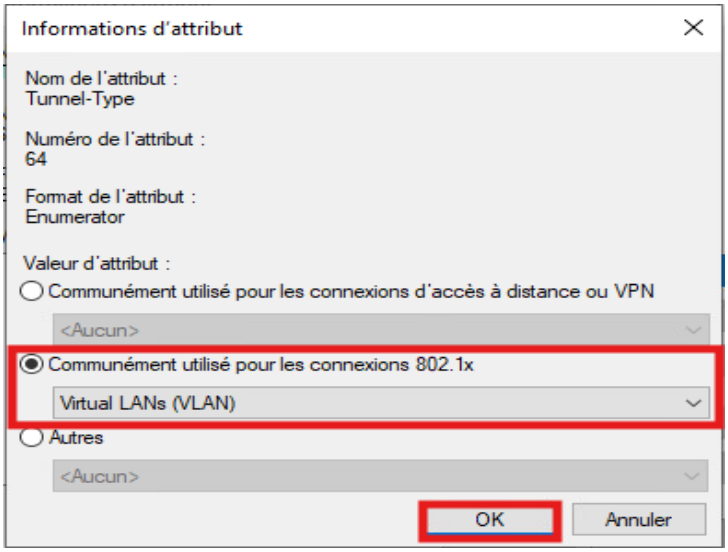
- Dans Ajouter un attribut **RADIUS** standard, dans Attributs, faites défiler vers le bas jusqu'aux attributs et faites « **Ajouter** ».



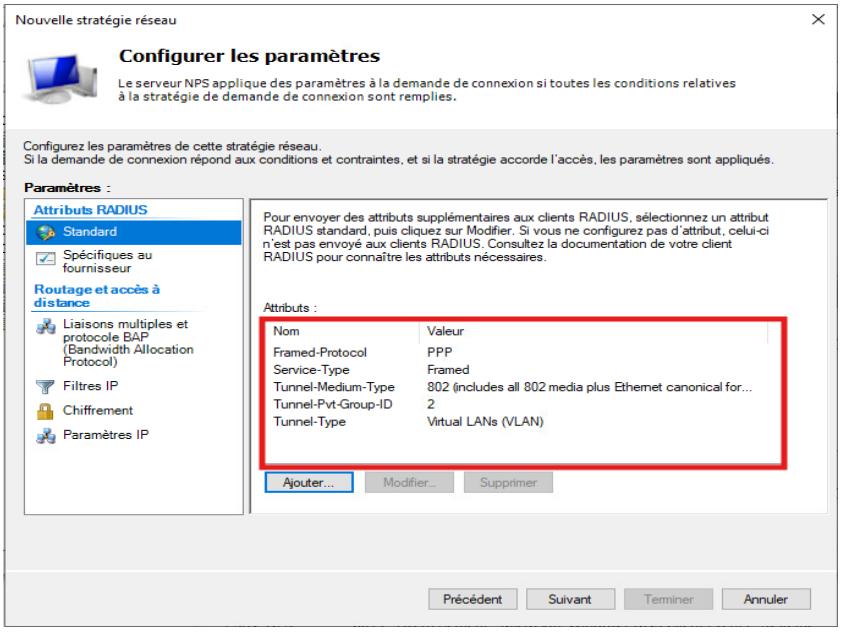
- La page d'information d'attribut s'affiche à l'écran, faites « **Ajouter** ».



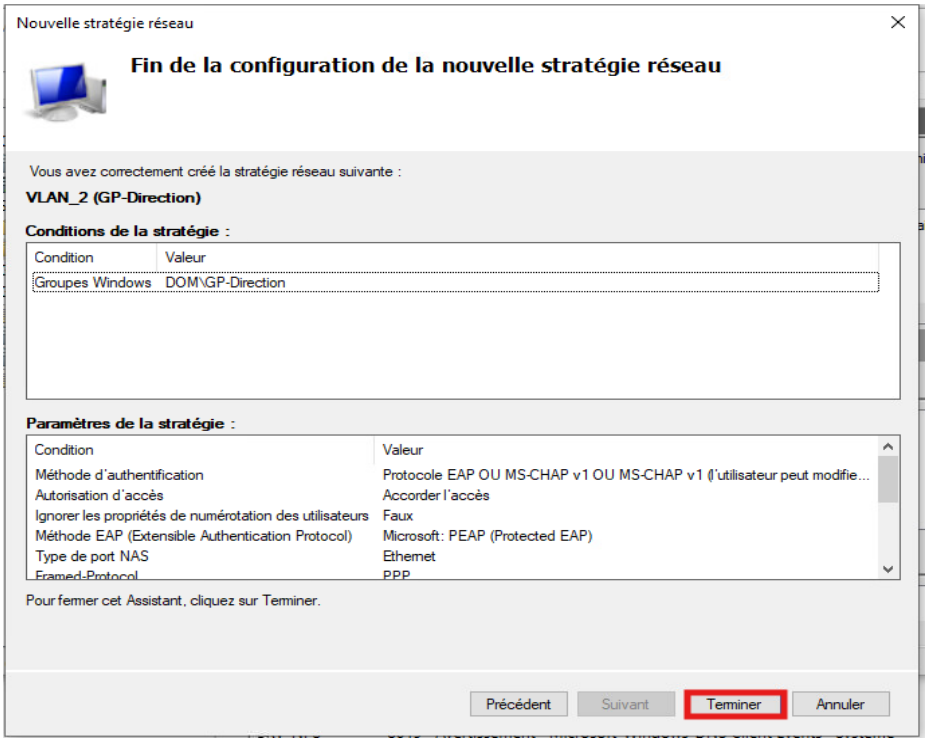
- Ensuite la deuxième page d'informations d'attribut s'affiche à l'écran, coché l'option « **Communément utilisé pour les connexions 802,1X** », puis faites « **OK** ».



- Voici le récapitulatif des attributs « **Ajouter** », faites « Suivant ».



- Le résumé de notre configuration, faites **« Terminer ».**

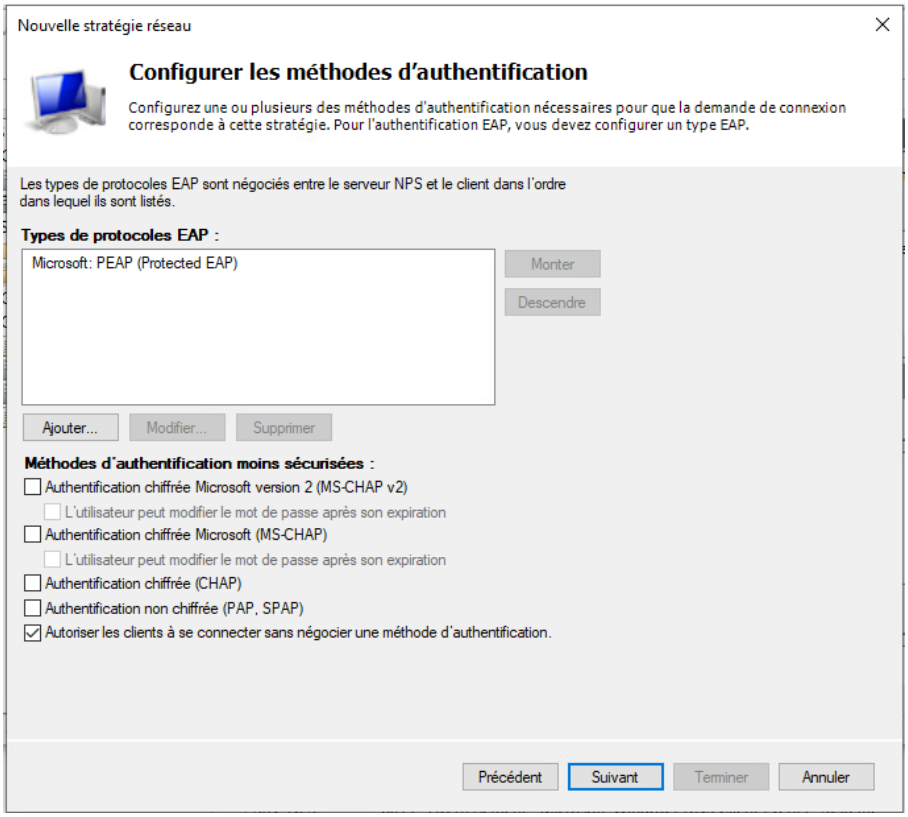


NB : Dans ce cas, étant donné que nous avons trois VLAN, il est nécessaire de définir une stratégie réseau distincte pour chacun d'eux. Ainsi, la même procédure devra être appliquée aux VLAN 3 et 4.

4. Stratégie réseau pour les utilisateurs non authentifier (VLAN 254):

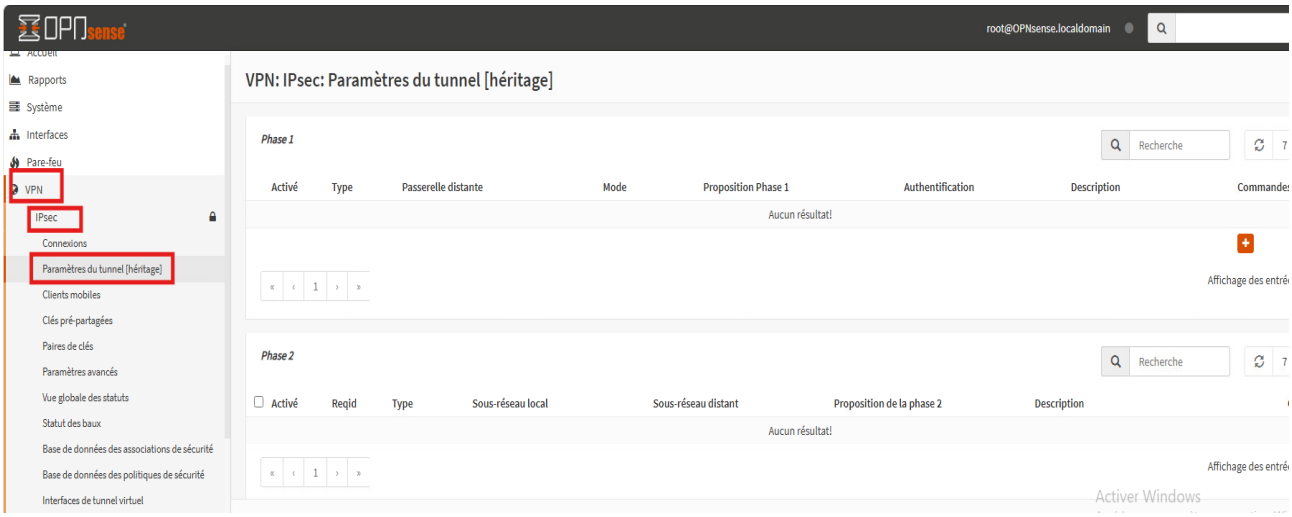
Pour se faire :

- Faites un clic droit sur « **Stratégie Réseau** », puis **Nouveau,**
- Une page « Nouvelle stratégie réseau » s'affiche à l'écran, taper le nom de votre stratégie et dans l'option « Type de serveur d'accès réseau », laisser celle proposé par défaut « Non spécifie » pour une authentification via un commutateur 802.1x.

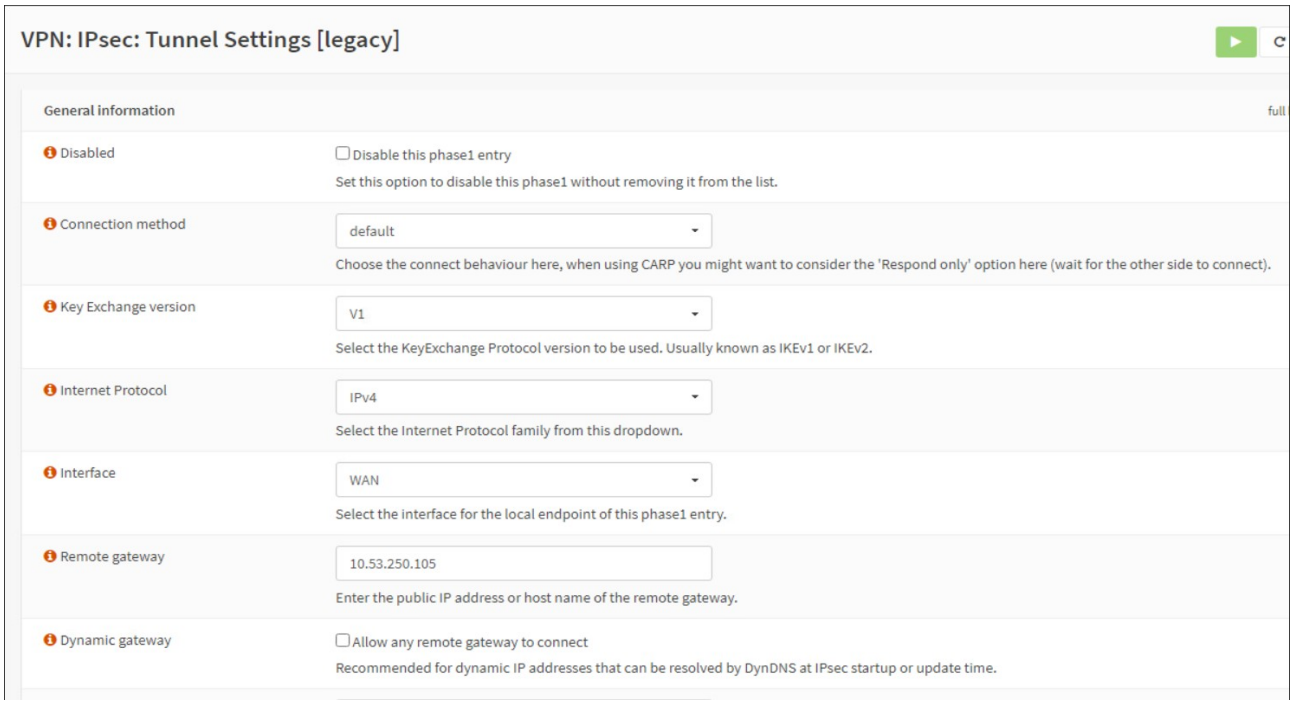


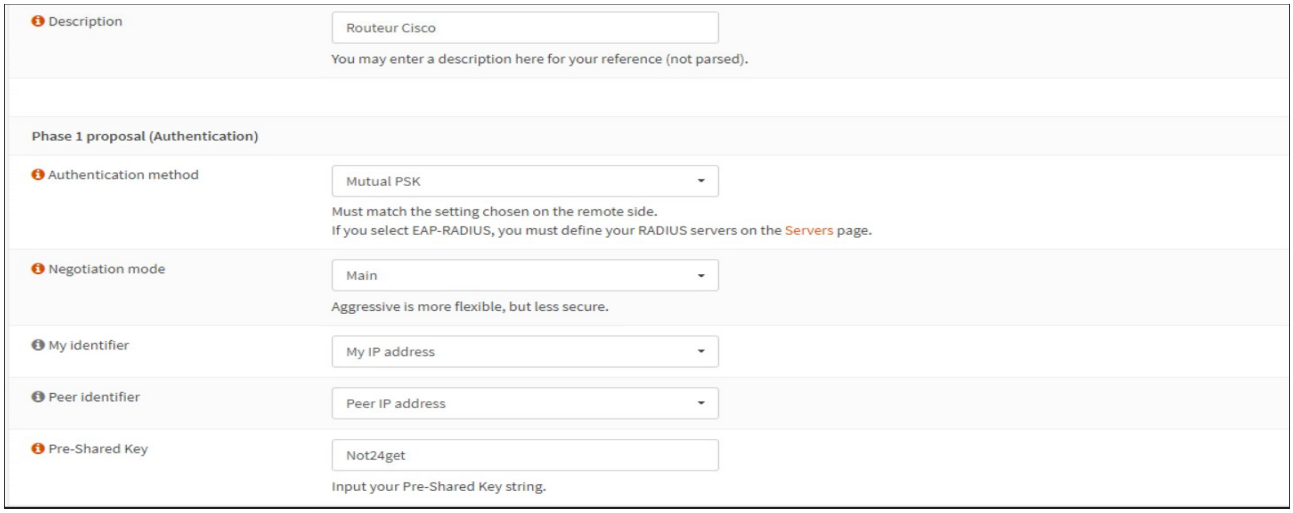
4. Configuration VPN Ipsec sur OPNSense :

- Se connecter à OPNSense,
- Allez dans OpenVPN, puis IPSEC, et cliquer sur paramètre du tunnel (héritage)

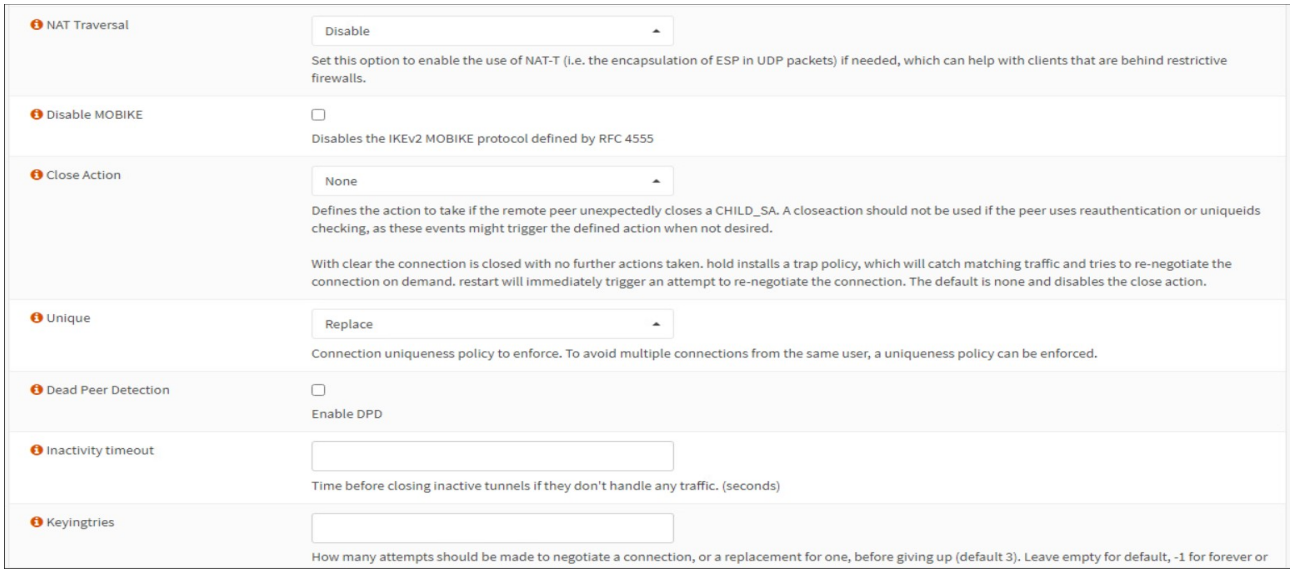


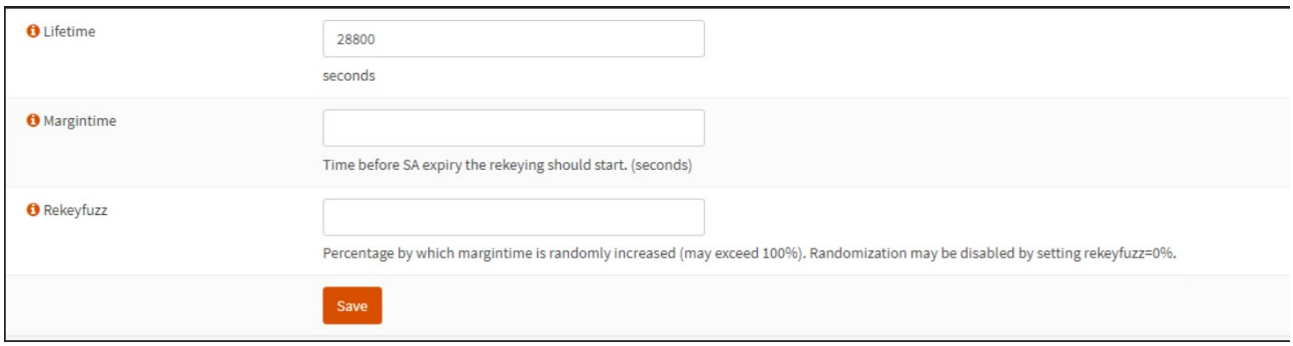
Contenue du règle ipsec :



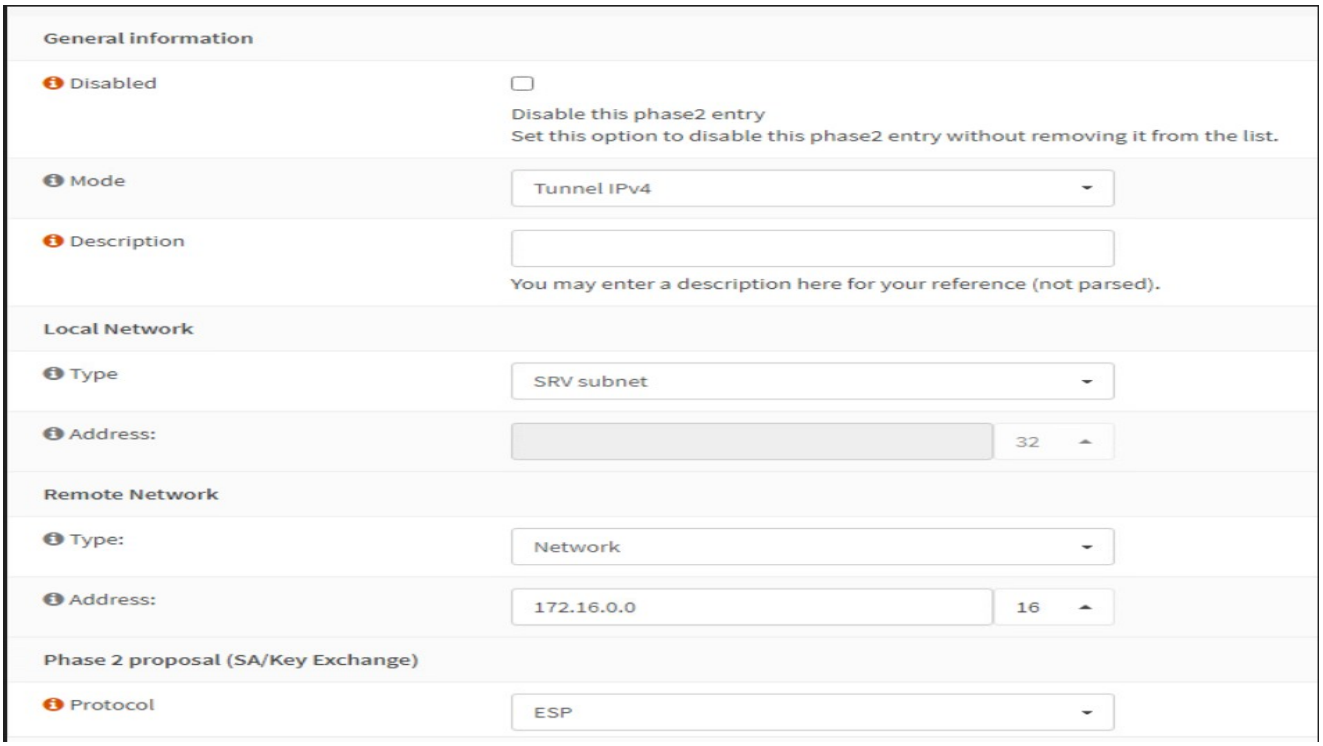

Description
Routeur Cisco
You may enter a description here for your reference (not parsed).
Phase 1 proposal (Authentication)
Authentication method
Mutual PSK
Must match the setting chosen on the remote side.
If you select EAP-RADIUS, you must define your RADIUS servers on the Servers page.
Negotiation mode
Main
Aggressive is more flexible, but less secure.
My identifier
My IP address
Peer identifier
Peer IP address
Pre-Shared Key
Not24get
Input your Pre-Shared Key string.

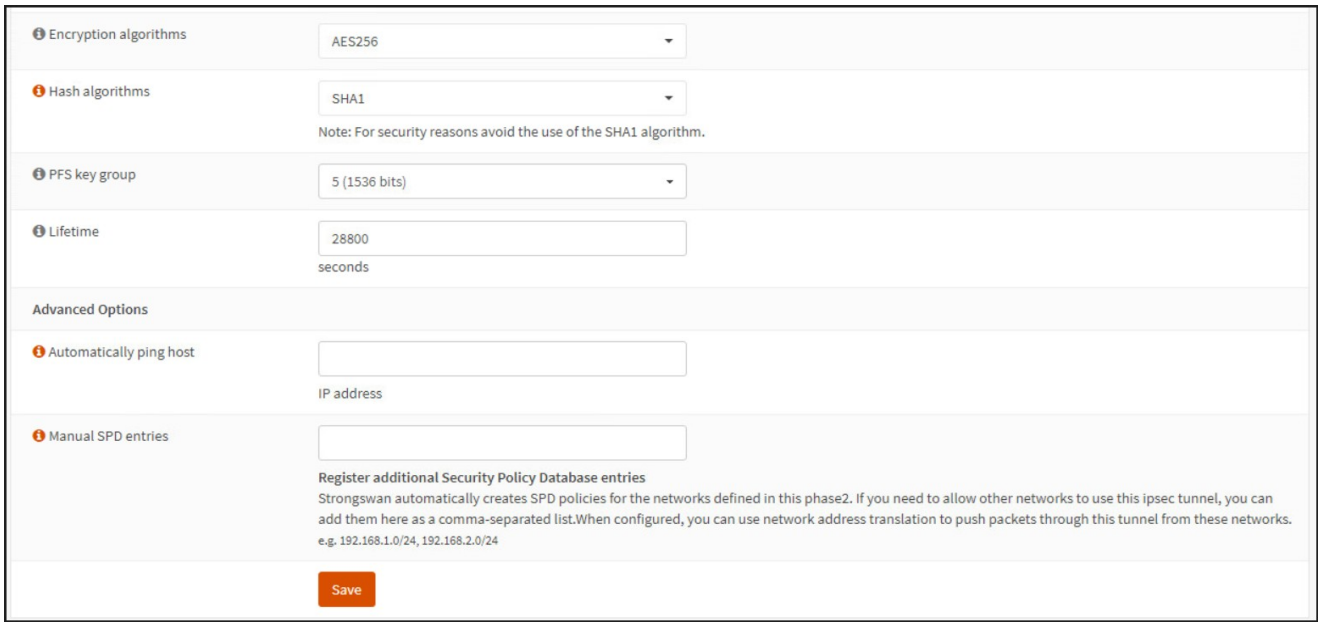

Phase 1 proposal (Algorithms)
Encryption algorithm
AES
256
Note: For security reasons avoid the use of DES,3DES,CAST and BLOWFISH protocols.
Hash algorithm
SHA1
Note: For security reasons avoid the use of MD5 and SHA1 algorithms.
DH key group
5 (1536 bits)
Must match the setting chosen on the remote side.
Advanced Options
Install policy
Decides whether IPsec policies are installed in the kernel by the charon daemon for a given connection. When using route-based mode (VTI) this needs to be disabled.
Disable Rekey
Whether a connection should be renegotiated when it is about to expire.
Disable Reauth
Whether rekeying of an IKE_SA should also reauthenticate the peer. In IKEv1, reauthentication is always done.
Tunnel Isolation
This option will create a tunnel for each phase 2 entry for IKEv2 interoperability with e.g. FortiGate devices.
SHA256 96 Bit Truncation





- Ensuite faites ajouter un second page supplémentaire et remplir les contenues :


General information
Disabled
Disable this phase2 entry
Set this option to disable this phase2 entry without removing it from the list.
Mode
Tunnel IPv4
Description
You may enter a description here for your reference (not parsed).
Local Network
Type
SRV subnet
Address:
32
Remote Network
Type:
Network
Address:
172.16.0.0
16
Phase 2 proposal (SA/Key Exchange)
Protocol
ESP


Encryption algorithms
AES256
Hash algorithms
SHA1
Note: For security reasons avoid the use of the SHA1 algorithm.
PFS key group
5 (1536 bits)
Lifetime
28800
seconds
Advanced Options
Automatically ping host
IP address
Manual SPD entries
Register additional Security Policy Database entries
Strongswan automatically creates SPD policies for the networks defined in this phase2. If you need to allow other networks to use this ipsec tunnel, you can add them here as a comma-separated list.When configured, you can use network address translation to push packets through this tunnel from these networks.
e.g. 192.168.1.0/24, 192.168.2.0/24
Save

4. Configuration du basique de switch :

Config 802.1x avec AD DHCP NPS sur switch catalyst avec attribution de vlan (PEAP-MSCHAPv2)

```
## Config basique switch
```

```
enable
conf t
vlan 2
name GP-Direction
vlan 3
name GP-RH
vlan 4
name GP-Production
vlan 5
name GP-WIFI-BYOD
vlan 254
name GP-Public
interface vlan 1
ip address 172.16.11.1 255.255.255.0
no shutdown
exit
!Desactiver le serveur web integre
no ip http server
no ip http secure-server
!Desactiver le recherche de nom dns
no ip domain-lookup
```

```
ip default-gateway 172.16.11.253
hostname yzotalocalswitch
ip domain-name lan.iia-laval.info
crypto key generate rsa general-keys modulus 2048
ip ssh time-out 30
ip ssh authentication-retries 4
ip ssh version 2
service password-encryption
username admin privilege 15 secret 0 Not24get
enable secret 0 Not24get
line console 0
password Not24get
login
exit
line vty 0 15
transport input ssh
login local
exit
banner login !
##################################################################################
Attention toute tentative d'acces sera enregistre et vous encourez des poursuites penales si vous tentez d'y acceder...
##################################################################################
!
interface gigabitEthernet 0/1
switchport mode trunk
```

```
switchport trunk allowed vlan all
switchport trunk native vlan 1
description LOCAL-TRUSTED
exit
interface fastEthernet 0/12
switchport mode access
switchport access vlan 2
spanning-tree portfast
description VLANLOCAL-DIRECTION
exit
interface fastEthernet 0/13
switchport mode access
switchport access vlan 3
spanning-tree portfast
description VLANLOCAL-RH
exit
interface fastEthernet 0/14
switchport mode access
switchport access vlan 4
spanning-tree portfast
description VLANLOCAL-PROD
exit
interface fastEthernet 0/15
switchport mode access
switchport access vlan 5
spanning-tree portfast
```

description VLANLOCAL-WIFIBYOD

exit

interface fastEthernet 0/16

switchport mode access

switchport access vlan 254

spanning-tree portfast

description VLANLOCAL-PUBLIC

exit

! Activer le protocole AAA sur le switch :

Config 802.1x switch

```

!Enables AAA

aaa new-model

!aaa authentication dot1x {default} method1

!Creates an 802.1x authentication method list.

!To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.

!For method1 , enter the group radius keywords to use the list of all RADIUS servers for authentication.

aaa authentication dot1x default group radius

!Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default group radius command.

aaa authorization network default group radius
```

```
!Enable 802.1x accounting using the list of all RADIUS servers.
aaa accounting dot1x default start-stop group radius

!Globally enables 802.1X port-based authentication on a switch
dot1x system-auth-control

!config radius server for aaa
radius-server host 10.196.72.1 auth-port 1812 acct-port 1813 timeout 10 key Not24get



interface range FastEthernet0/1-22
switchport mode access
! Set the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.
dot1x pae authenticator
!Enable 802.1x authentication on the port.
authentication port-control auto

!Les étape facultatifs (pour les bonne pratique)
!Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated.
!authentication host-mode multi-host  (cette commande n'avais fonctionné)
!Permettre l'authentification avec le wake-on-lan en authentificant que ce qui vient de l'interface
authentication control-direction in
!Configure the violation mode : Removes the current session and authenticates with the new host.
```

```
authentication violation replace

!Set the number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. (default 60)

authentication timer inactivity 10

!Enable periodic reauthentication of the client, which is disabled by default.

authentication periodic

! Set reauthentication attempt for the client (set to one hour by default).

authentication timer reauthenticate 1800

!Vlan guest si pas d'auth

authentication event no-response action authorize vlan 254

!Vlan guest si authentification échoue

authentication event fail action authorize vlan 254

!Vlan guest si pas de serveur radius

authentication event server dead action authorize vlan 254

spanning-tree portfast
```

4. Configuration du basique de Routeur :

```
# Config basique routeur

```cisco

enable

conf t

hostname yzlocalrouter

enable secret 0 Not24get

service password-encryption

line console 0
```
```

```
password Not24get
login
exit
ip domain-name lan.iia-laval.info
aaa new-model
username admin privilege 15 secret 0 Not24get
line vty 0 15
transport input ssh
exit
crypto key generate rsa general-keys modulus 2048
ip ssh time-out 30
ip ssh authentication-retries 4
ip ssh version 2
banner login !
################################################################################
Attention toute tentative d'acces sera enregistre et vous encourez des poursuites penales si vous tentez d'y acceder...
################################################################################
!
interface GigabitEthernet0/1
ip address 172.16.11.253 255.255.255.0
description LOCAL-MGMT
no shutdown
exit

interface GigabitEthernet0/1.2
```

```
encapsulation dot1Q 2
ip address 172.16.12.253 255.255.255.0
ip helper-address 172.17.2.254
description LOCAL-direction
no shutdown
exit
interface GigabitEthernet0/1.3
encapsulation dot1Q 3
ip address 172.16.13.253 255.255.255.0
ip helper-address 172.17.2.254
description LOCAL-rh
no shutdown
exit
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 172.16.14.253 255.255.255.0
ip helper-address 172.17.2.254
description LOCAL-production
no shutdown
exit
interface GigabitEthernet0/1.5
encapsulation dot1Q 5
ip address 172.16.15.253 255.255.255.0
ip helper-address 172.17.2.254
description LOCAL-WIFI-BYOD
no shutdown
```

```
exit
interface GigabitEthernet0/1.254
encapsulation dot1Q 254
ip address 172.16.254.253 255.255.255.0
ip helper-address 10.192.1.11
description LOCAL-public
no shutdown
exit


================================================================================
================================================================================
```

Config VPN routeur

```cisco
!Utiliser IP OPNsense
crypto isakmp key Not24get address 10.192.0.200 no-xauth
crypto ipsec security-association lifetime seconds 28800

crypto isakmp policy 5
 encryption aes 256
 hash sha
 authentication pre-share
 group 5
 lifetime 28800
 exit
crypto ipsec transform-set VPN-OPNSENSE esp-aes 256 esp-sha-hmac
 mode tunnel
```

```
 exit
!Access list pour les reseaux locaux
access-list 100 permit ip 172.16.0.0 0.0.255.255 172.17.1.0 0.0.255.255
!Access list pour le routeur VPN
access-list 100 permit ip 10.53.250.114 0.0.0.0 172.17.0.0 0.0.255.255
crypto map OPNSENSE-MAP 2 ipsec-isakmp
! Utiliser IP OPNsense
 set peer 10.192.0.200
 set security-association lifetime seconds 28800
 set transform-set VPN-OPNSENSE
 set pfs group5
 match address 100
exit
crypto isakmp invalid-spi-recovery
int GigabitEthernet0/1
crypto map OPNSENSE-MAP
!Commandes debug
show crypto map
show crypto session
!Si ça marche pas la commande crypto
show license
conf t
license boot module c2900 technology-package securityk9
exit
wr
show license
```

```
reload

! Ensuite commencer la configuration

!https://getlabsdone.com/how-to-configure-ipsec-vpn-between-pfsense-and-cisco-router/

!https://forum.opnsense.org/index.php?topic=3645.0



!(Suite à souci de configuration de service DHCP, d'ou la création de services des pools DHCP sur le routeur en annulant le relai DHCP configurer précedement.)

 !attention la première étape consiste à annuler les configuration  relai dhcp déjà faite pour le service dhcp depuis OpnNebula cet étape nest pas adapter à tout les cas)

configure terminal

interface gigabitEthernet 0/0.2

no ip helper-address

interface gigabitEthernet 0/0.3

no ip helper-address

interface gigabitEthernet 0/0.4

no ip helper-address

interface gigabitEthernet 0/0.5

no ip helper-address

exit

!Cette étape permet d'exclure certains adresse IP pour le service DHCP

ip dhcp excluded-address 172.16.12.253

ip dhcp excluded-address 172.16.13.253

ip dhcp excluded-address 172.16.14.253

ip dhcp excluded-address 172.16.15.253

ip dhcp excluded-address 172.16.254.253
```

```
!Début de configuration des pools d'adressage IP
ip dhcp pool vlan2-Direction
network 172.16.12.0 255.255.255.0
default-router 172.16.12.253
dns-server 172.17.2.1
exit

ip dhcp pool vlan3-RH
network 172.16.13.0 255.255.255.0
default-router 172.16.13.253
dns-server 172.17.2.1
exit
ip dhcp pool vlan4-Prod
network 172.16.14.0 255.255.255.0
default-router 172.16.14.253
dns-server 172.17.2.1
exit
ip dhcp pool vlan254-Public
network 172.16.254.0 255.255.255.0
default-router 172.16.254.253
dns-server 1.1.1.1
exit
exit
write
```

Faire le test de ping vers le plateforme OpenNebula :

Info : Attentions pour que cela fonctionne il faut d'abord activer le protocole ICMP dans le pare-feu de serveur Radius et le PC.