

COMPTE RENDU DE STAGE

Partner Informatique

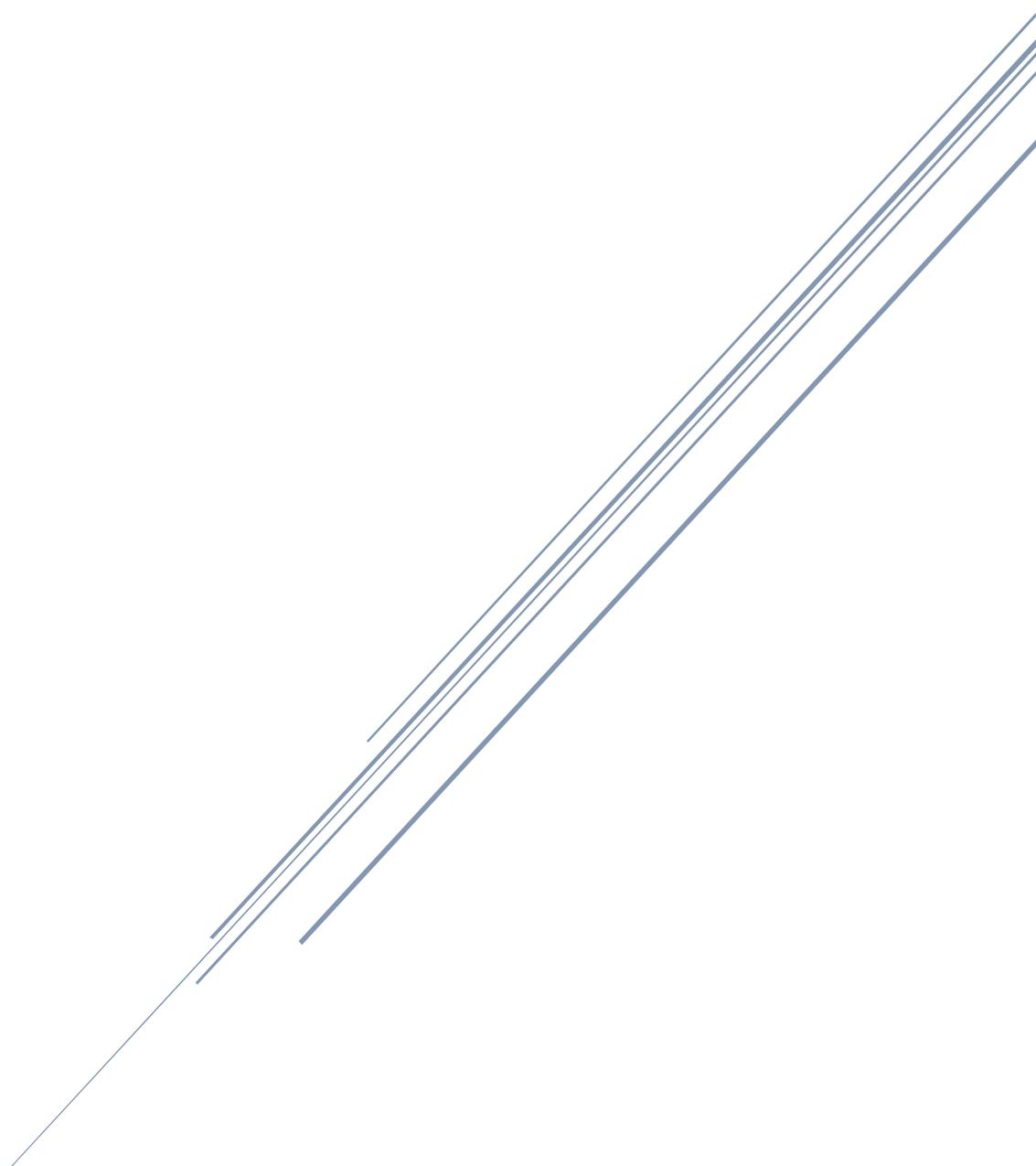


Table des matières

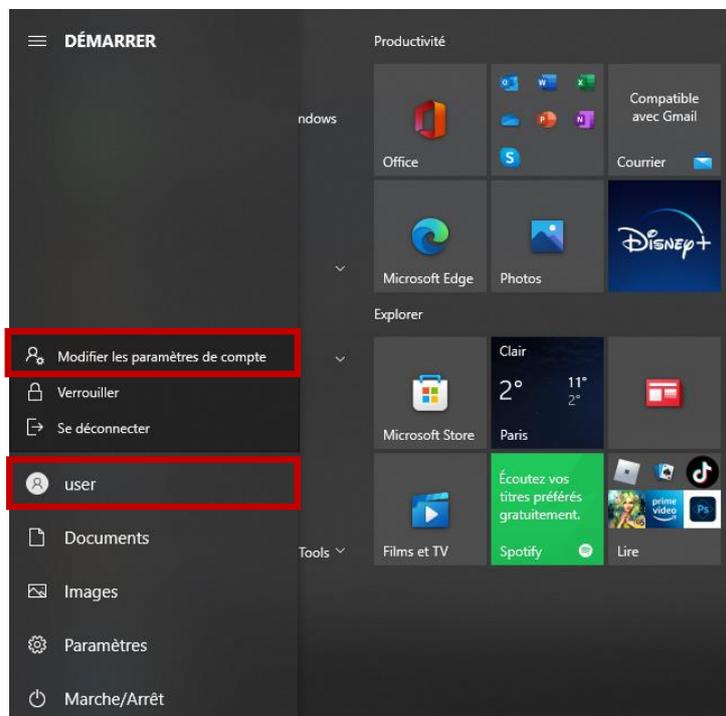
1	Procédure SFTP.....	2
1.1	Création des utilisateurs	2
2	Droits d'accès aux dossiers.....	6
2.1	Droits des Utilisateurs.....	6
3	Test de connexion via PowerShell (en SSH)	10
3.1	Test des droits des Utilisateurs	10
4	Mission Wifi : changer le ssid	12
4.1	Info	12
5	Mission Wifi : créer 2 réseaux distinct avec leur attribution propre.....	16
6	Mission Radius	25
6.1	Création des VMs	25
6.2	Ajout de la borne :.....	47
6.3	Paramétrer la borne WIFI	61

1 Procédure SFTP

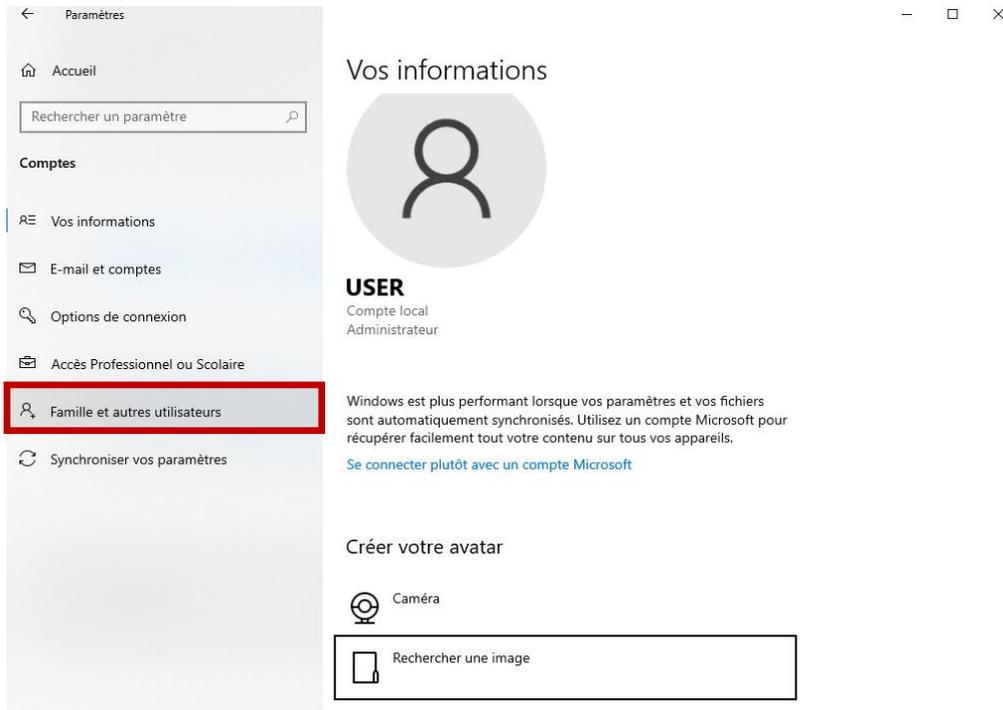
Document du 09/02/20

1.1 Création des utilisateurs

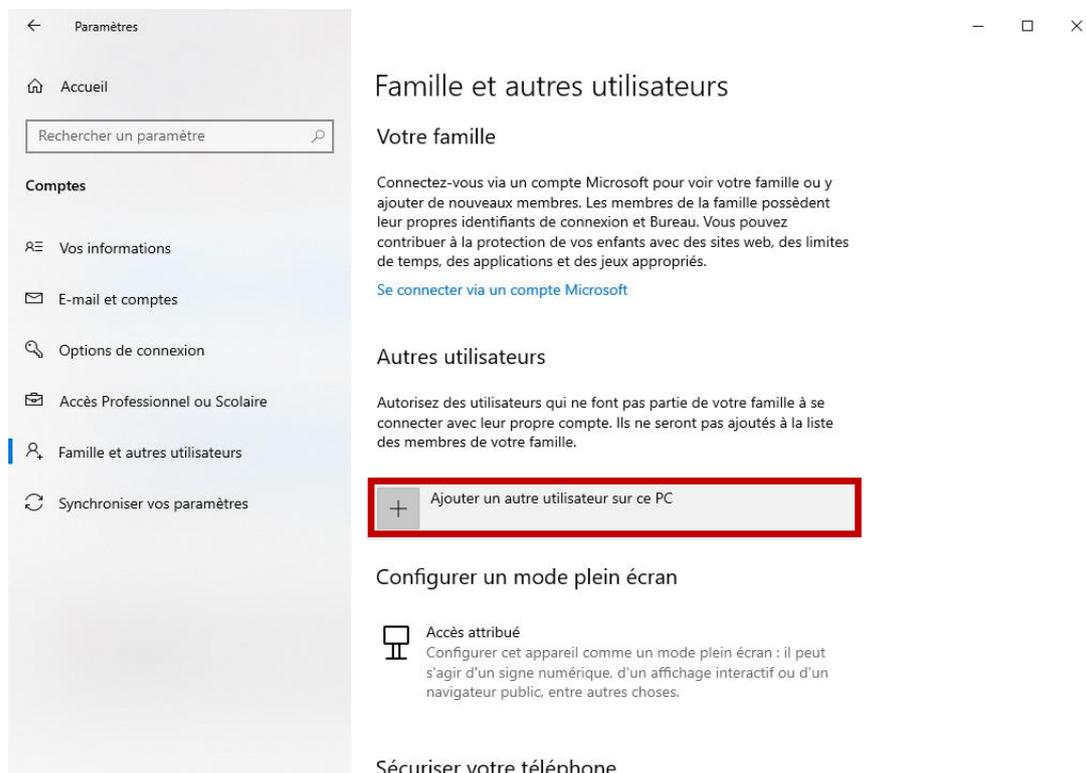
Pour effectuer une connexion SFTP, il faut créer un utilisateur. Pour ce faire, cliquer sur le bouton Windows de votre clavier puis sur l'icône de votre utilisateur. Une fois fait, sélectionner « Modifier les paramètres de compte ».



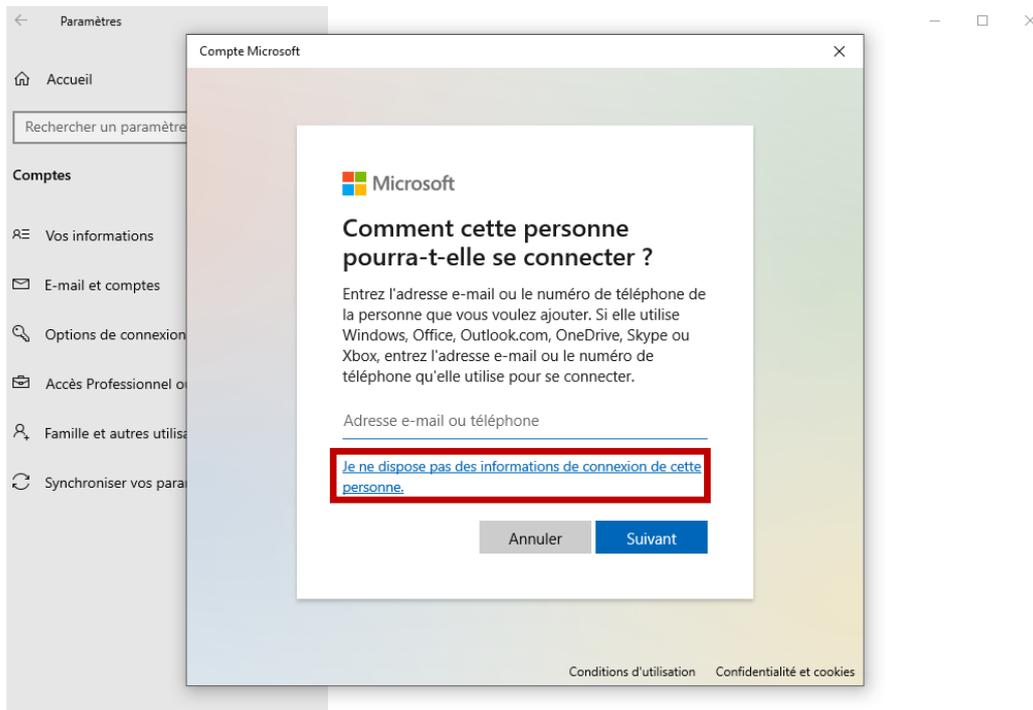
Cliquer sur « Famille et autres utilisateurs » :



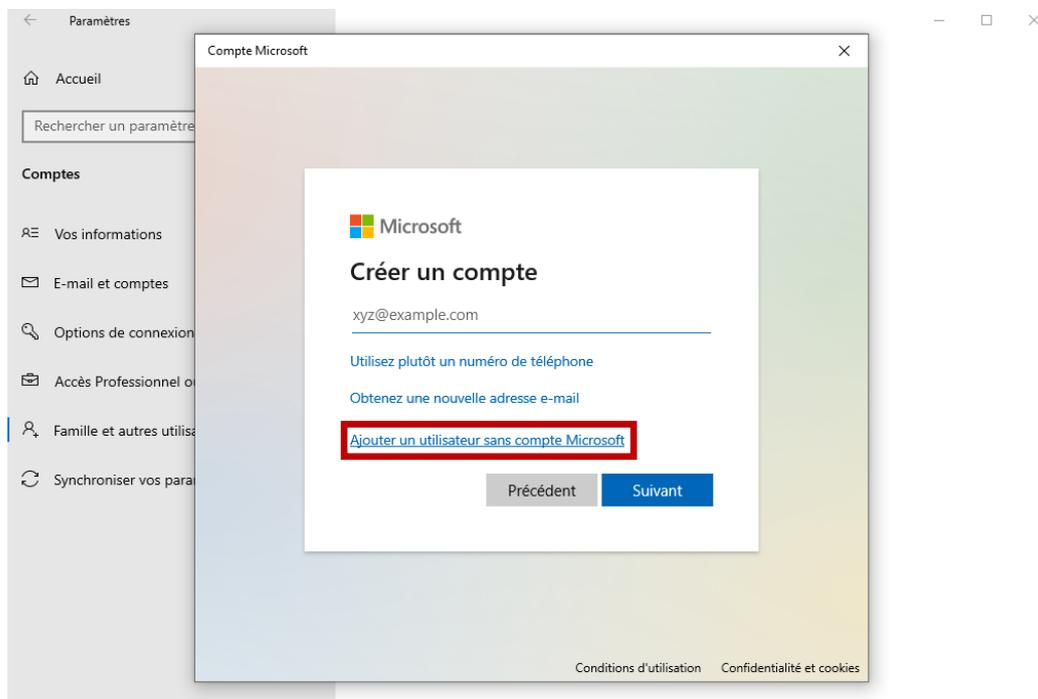
Puis « Ajouter un autre utilisateur sur ce PC » :



Ici, cliquer sur « Je ne dispose pas des informations de connexion de cette personne » :



Cliquer ensuite sur « Ajouter un utilisateur sans compte Microsoft » :



Et enfin, renseigner les informations suivantes, à noter qu'un mot de passe est obligatoire pour une connexion SFTP :

Compte Microsoft ×

Créer un utilisateur pour ce PC

Si vous souhaitez utiliser un mot de passe, choisissez une expression facile à retenir, mais difficile à deviner.

Qui sera amené à utiliser ce PC ?

Sécurisez votre mot passe.

Suivant Précédent

Nous pouvons voir que l'utilisateur a été créé :

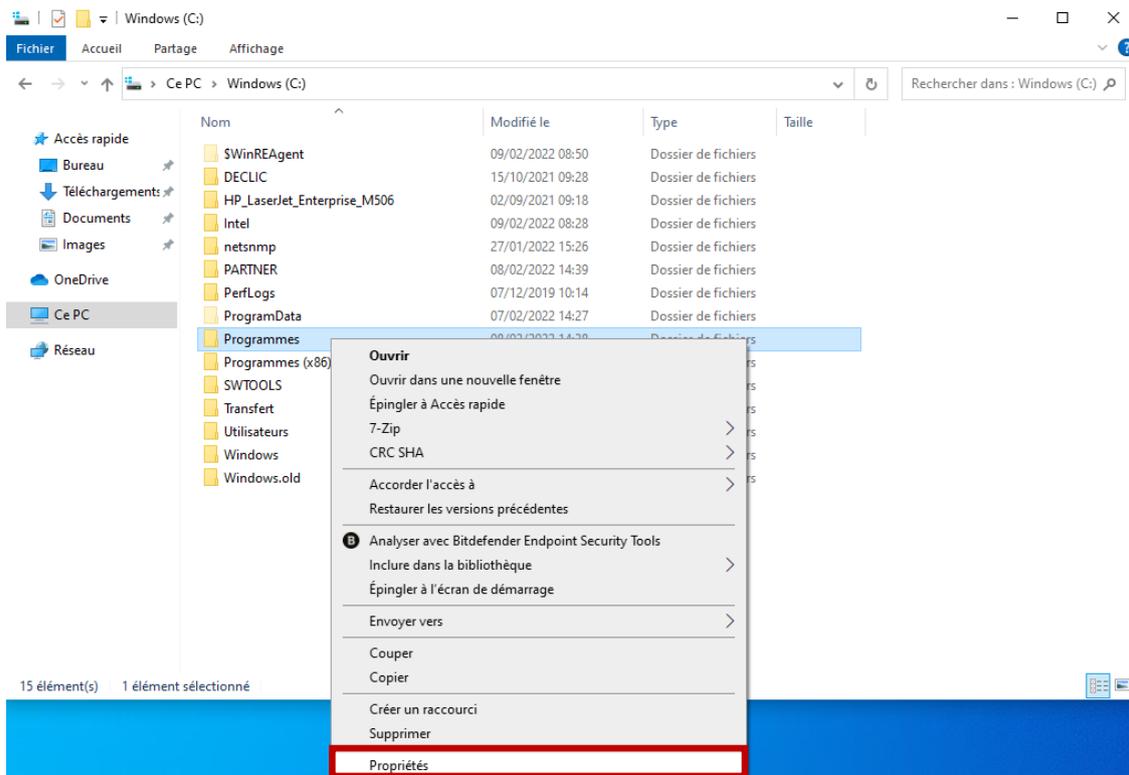
The screenshot shows the Windows Settings application. On the left is a navigation pane with 'Paramètres' at the top and 'Accueil' below. A search bar is present. Under the 'Comptes' section, 'Familie et autres utilisateurs' is selected. The main content area is titled 'Familie et autres utilisateurs' and contains sections for 'Votre famille' and 'Autres utilisateurs'. Under 'Autres utilisateurs', there is a button '+ Ajouter un autre utilisateur sur ce PC' and a list of users. One user, 'test', is listed as a 'Compte local' and is highlighted with a red rectangular box. Below this, there is a section for 'Configurer un mode plein écran' with an 'Accès attribué' icon and text.

2 Droits d'accès aux dossiers

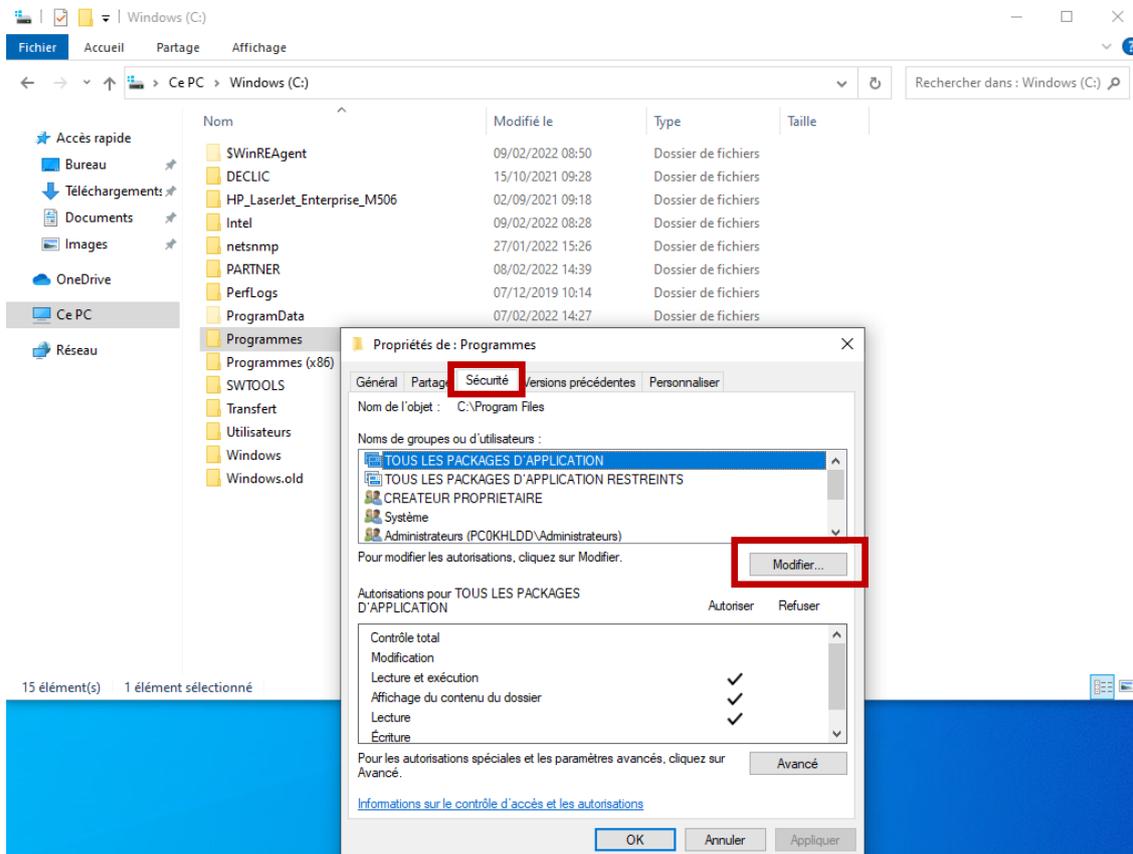
2.1 Droits des Utilisateurs

Maintenant que notre utilisateur a été créé nous pouvons maintenant modifier les droits d'accès aux différents dossiers.

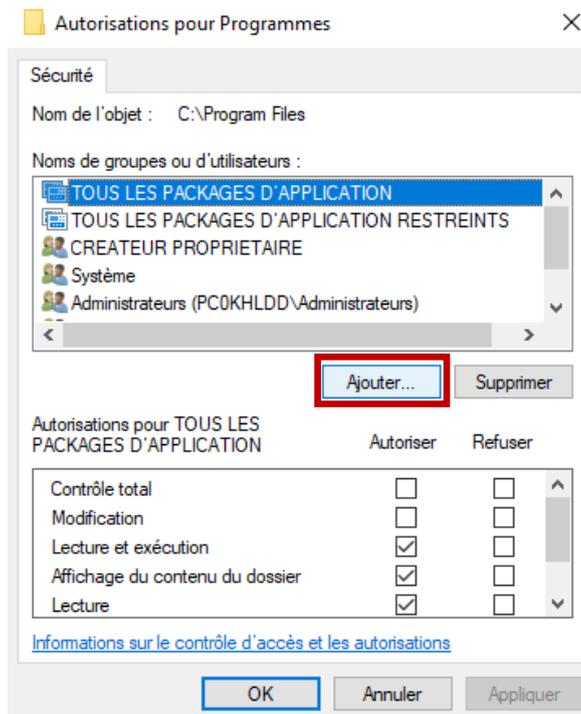
Pour ce faire, clic droit sur le dossier voulu puis « Propriétés » :



Aller dans l'onglet « Sécurité » puis cliquer sur « Modifier... » :



Cliquer sur « Ajouter... » :



Renseigner le nom de l'utilisateur et cliquer sur « Vérifier les noms » :

Sélectionnez des utilisateurs ou des groupes

Sélectionnez le type de cet objet :

des utilisateurs, des groupes ou Principaux de sécurité intégrés

Types d'objets...

À partir de cet emplacement :

PC0KHLDD

Emplacements...

Entrez les noms des objets à sélectionner (exemples) :

PC0KHLDD\test

Vérifier les noms

Avancé... OK Annuler

Ensuite, en s'assurant bien d'avoir sélectionné votre utilisateur, modifier les autorisations ci-dessous. Si l'utilisateur ne doit pas avoir d'accès au fichier cocher la case « Contrôle total » dans la colonne « Refuser » :

Autorisations pour PARTNER

Sécurité

Nom de l'objet : C:\PARTNER

Noms de groupes ou d'utilisateurs :

- Utilisateurs authentifiés
- Système
- test (PC0KHLDD\test)
- Administrateurs (PC0KHLDD\Administrateurs)
- Utilisateurs (PC0KHLDD\Utilisateurs)

Ajouter... Supprimer

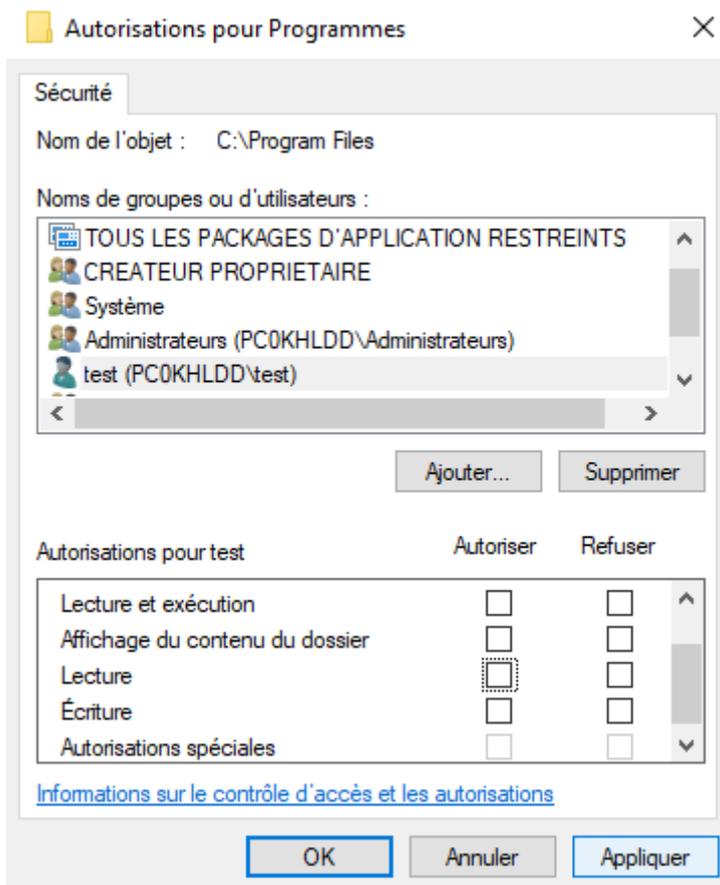
Autorisations pour test

	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Modification	<input type="checkbox"/>	<input type="checkbox"/>
Lecture et exécution	<input type="checkbox"/>	<input type="checkbox"/>
Affichage du contenu du dossier	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lecture	<input type="checkbox"/>	<input type="checkbox"/>

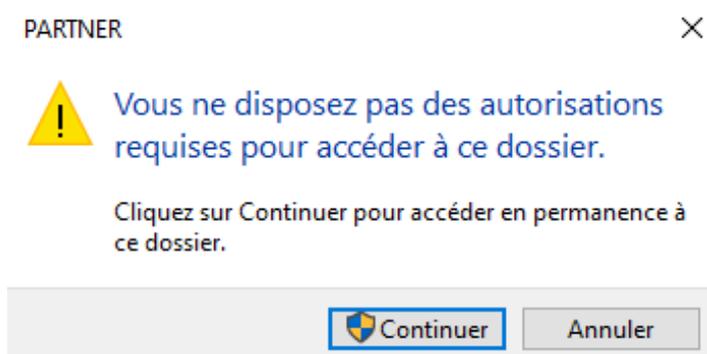
[Informations sur le contrôle d'accès et les autorisations](#)

OK Annuler Appliquer

Cependant, certains dossiers ne peuvent pas être refusé d'accès comme ici le dossier « Programmes » nécessaire à l'utilisateur ou alors les dossiers « Programmes (x86) », « Utilisateurs » et « Windows » :



Une fois connecté sur l'utilisateur test nous pouvons constater qu'il n'a plus accès au dossier :



3 Test de connexion via PowerShell (en SSH)

3.1 Test des droits des Utilisateurs

Tout d'abord, ouvrir une fenêtre PowerShell (Clic droit sur le bouton  puis sélectionner « Windows PowerShell (admin) »)

Il est possible d'utiliser 2 commandes différentes pour se connecter :

```
ssh utilisateur@ip_du_serveur  
ssh utilisateur@nom_du_serveur
```

Lors de la première connexion PowerShell va demander si vous souhaitez autoriser la communication. Répondre « yes » puis renseigner le mot de passe de l'utilisateur :

```
PS C:\Users\stage-infra> ssh test@PC0KHLDD  
The authenticity of host 'pc0khldd (fe80::a565:95d5:3f3:f13%25)' can't be established.  
ECDSA key fingerprint is SHA256:FsgvulI8FwtBkntbKAaoiIYh2gvpTADf6pu64oZTFe8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'pc0khldd,fe80::a565:95d5:3f3:f13%25' (ECDSA) to the list of known hosts.  
test@pc0khldd's password:
```

La connexion est établie sauf indications contraires :

```
Microsoft Windows [version 10.0.19044.1526]  
(c) Microsoft Corporation. Tous droits réservés.  
  
test@PC0KHLDD C:\Users\test>
```

Pour tester les accès aux dossiers, on se connecte avec l'utilisateur test puis on se place dans le répertoire C:\ avec la commande « cd C:\ ».

Pour afficher le contenu du dossier on utilise la commande « dir ».

Ensuite, on essaye d'aller dans le dossier « DECLIC » (dont l'accès a été restreint pour l'utilisateur test) On peut voir que l'accès est refusé :

```
test@PC0KHLDD C:\>dir
Le volume dans le lecteur C s'appelle Windows
Le numéro de série du volume est B40F-2835

Répertoire de C:\

15/10/2021  08:28  <DIR>          DECLIC
02/09/2021  08:18  <DIR>          HP_LaserJet_Enterprise_M506
09/02/2022  09:37  <DIR>          Intel
27/01/2022  15:26  <DIR>          netsnmp
08/02/2022  14:39  <DIR>          PARTNER
07/12/2019  10:14  <DIR>          PerfLogs
08/02/2022  14:38  <DIR>          Program Files
07/02/2022  15:59  <DIR>          Program Files (x86)
24/08/2021  08:15  <DIR>          SWTTOOLS
09/02/2022  09:51  <DIR>          Transfert
09/02/2022  09:24  <DIR>          Users
07/02/2022  15:00  <DIR>          Windows
07/02/2022  12:54  <DIR>          windows.old
             0 fichier(s)                0 octets
             13 Rép(s)  449 298 317 312 octets libres

test@PC0KHLDD C:\>Cd DECLIC
Accès refusé.
```

4 Mission Wifi : changer le ssid

4.1 Info

Adresse Ip : 192.168.1.2

Login : Admin

MDP : 1234

- Pour accéder à la console wizard renseigné l'adresse ip de votre borne (ici 192.168.1.2) et cliquer sur « Standalone Mode »



- Vous devriez arriver sur cette page de configuration

Wizard Setting

Step 1 Welcome to the Setup Wizard

Time Settings

Country Code:

Time Zone:

Enable Daylight Saving

Start Date: of at :

End Date: of at :

Offset: hours

Wizard Setting

Step 1

Change Password:

New Password:

Confirm Password:

Step 2 **Uplink Connection:**

Auto(DHCP) Static IP

IP Address:

Subnet Mask:

Gateway:

DNS Server:

Wizard Setting

Step 1

Radio

Band: 2.4GHz

Channel Width: 20MHz

Channel Selection: Auto Manual

Maximum Output Power: dBm(0~20)

Step 3

Band: 5GHz

Channel Width:

Channel Selection: Auto Manual

Maximum Output Power: dBm(0~30)

Wizard Setting

Step 1 **SSID**

Step 2

#	Status	SSID	Security Mode	Band Mode	VLAN ID
1	<input checked="" type="radio"/>	Reseau Prive	WPA2-Personal	Dual Band	1
2	<input checked="" type="radio"/>	Reseau Prive Guest	WPA2-Personal	Dual Band	10
3	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
4	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
5	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
6	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
7	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
8	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1

Step 3

Step 4

Step 5

Prev Next Cancel

Wizard Setting

Step 1 **Summary**

Step 2

Country Code: Germany

Time Zone: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna

Daylight Saving: Enable

Step 3

Management IP: Static IP

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Step 4

Gateway: 192.168.1.1

DNS Server: 192.168.1.1

Step 5

2.4G Radio: Auto

5G Radio: Auto

SSID

Prev Save Cancel

Non sécurisé | 192.168.1.2/ext-js/web-pages/index/index.html?dt=1642604767411

ZYXEL NWA1123ACv3 Welcome admin Wizard Help Forum Site Map CLI Logout nebula

DASHBOARD Widget Settings

Device Information

System Name: [NWA1123ACv3](#)

System Location: [n/a](#)

Model Name: NWA1123ACv3

Serial Number: S210Y23023849

MAC Address Range: EC:3E:B3:F4:E3:90 - EC:3E:B3:F4:E3:92

Firmware Version: [V6.10\(ARVT.9\) // 2020-10-16 11:19:40](#)

Last Firmware Upgrade Status: N/A

Last Firmware Upgrade: N/A

System Resources

CPU Usage: 6%

Memory Usage: 67%

Flash Usage: 8%

System Status

System Uptime: 2 days, 00:08:43

Current Date/Time: [2022-01-19 / 16:06:08 GMT+01:00](#)

Current Login User: admin (unlimited / 00:29:59)

Boot Status: System default configuration

Management Mode: standalone

Power Mode: Full

Interface Status Summary

Name	Status	VID	IP Addr/Netmask	IP Assign...	Action
lan	1000M/Full	1	192.168.1.2 / 255.255...	Static	n/a

AP Information

All Sensed Device:

Un-Classified AP: 0

Rogue AP: 0

Friendly AP: 0

WDS Uplink Status

MAC Address	Radio	Chan...	SSID	Security Mode	Link S...
-------------	-------	---------	------	---------------	-----------

Ethernet Neighbor

- Nous disposons d'une page de configuration de la borne wifi, nous allons la laisser en DHCP pour nous assurer d'être dans le bon réseau

ZYXEL NWA1123ACv3

Welcome admin

CONFIGURATION
IP Setting
VLAN

Network

IP Address Assignment

Get Automatically

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway: (Optional)

DNS Server IP Address: (Optional)

Use Proxy to Access NCC

Proxy Server:

Proxy Port: (1~65535)

Authentication

User Name:

Password:

- Console restreinte car Nebula est déjà installé

ZYXEL NWA1123ACv3
Welcome admin
Wizard
Help
Forum
Site Map
CLI
Logout
nebula

DASHBOARD Widget Settings

Device Information

System Name: [NWA1123ACv3](#)

System Location: [/0/0](#)

Model Name: NWA1123ACv3

Serial Number: S210Y23023849

MAC Address Range: EC:3E:B3:F4:E3:90 - EC:3E:B3:F4:E3:92

Firmware Version: [V6.10\(ABVT.9\) // 2020-10-16 11:19:40](#)

Last Firmware Upgrade Status: N/A

Last Firmware Upgrade: N/A

System Status

System Uptime: 00:24:03

Current Date/Time: [2022-01-17 / 16:21:23 GMT+01:00](#)

Current Login User: admin (unlimited / 00:29:59)

Boot Status: System default configuration

Management Mode: standalone

Power Mode: Full

System Resources

CPU Usage: 9%

Memory Usage: 61%

Flash Usage: 7%

Interface Status Summary

Name	Status	VID	IP Addr/Netmask	IP Assign...	Action
lan	1000M/Full	1	192.168.1.2 / 255.255.255.0	Static	n/a

AP Information

All Sensed Device:

Un-Classified AP: 0

Rogue AP: 0

Friendly AP: 0

WDS Uplink Status

MAC Address	Radio	Chan...	SSID	Security Mode	Link S...

ZYXEL NWA1123ACv3
Welcome admin
Wizard
Help
Forum
Site Map
CLI
Logout
nebula

CONFIGURATION

Radio

SSID

SSID List

Security List

MAC Filter List

Layer-2 Isolation List

SSID Summary

[Edit](#) [Object Reference](#)

#	Profile Name	SSID	Security Profile	QoS	MAC Filtering Pr...	Layer-2 Isolation...	VLAN ID
1	Wiz_SSID_1	Reseau Prive	Wiz_SEC_Profile_1	WMM	disable	disable	1
2	Wiz_SSID_2	Reseau Prive	Wiz_SEC_Profile_2	WMM	disable	disable	1
3	Wiz_SSID_3	Zyxel	Wiz_SEC_Profile_3	WMM	disable	disable	1
4	Wiz_SSID_4	Zyxel	Wiz_SEC_Profile_4	WMM	disable	disable	1
5	Wiz_SSID_5	Zyxel	Wiz_SEC_Profile_5	WMM	disable	disable	1
6	Wiz_SSID_6	Zyxel	Wiz_SEC_Profile_6	WMM	disable	disable	1
7	Wiz_SSID_7	Zyxel	Wiz_SEC_Profile_7	WMM	disable	disable	1
8	Wiz_SSID_8	Zyxel	Wiz_SEC_Profile_8	WMM	disable	disable	1
9	default	Zyxel-E390	default	WMM	disable	disable	1

Page 1 of 1 | Show 50 items | Displaying 1 - 9 of 9

5 Mission Wifi : créer 2 réseaux distinct avec leur attribution propre

Wizard Setting

Step 1 SSID

Step 2

Step 3

Step 4

Step 5

#	Status	SSID	Security Mode	Band Mode	VLAN ID
1	<input checked="" type="radio"/>	Reseau Prive	WPA2-Personal	Dual Band	1
2	<input checked="" type="radio"/>	Reseau Prive Guest	WPA2-Personal	Dual Band	10
3	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
4	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
5	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
6	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
7	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1
8	<input type="radio"/>	Zyxel	WPA2-Personal	Dual Band	1

Prev Next Cancel

- Mettre sur 2 vlan distinct les 2 réseaux depuis une même borne
- Pour se faire il faut utiliser un switch administrable pour créer les vlans nécessaire, dans notre cas il s'agit d'un d link dgs 1510 28
- Il faut le reset
- Et trouvez sont ip de base qui doit être 10.90.90.90 accessible depuis une interface web il faut donc se mettre sur le même réseau et changer sont ip et ensuite renseigné le nom admin et en mot de passe admin

Connexion à 192.168.1.3

Nom d'utilisateur

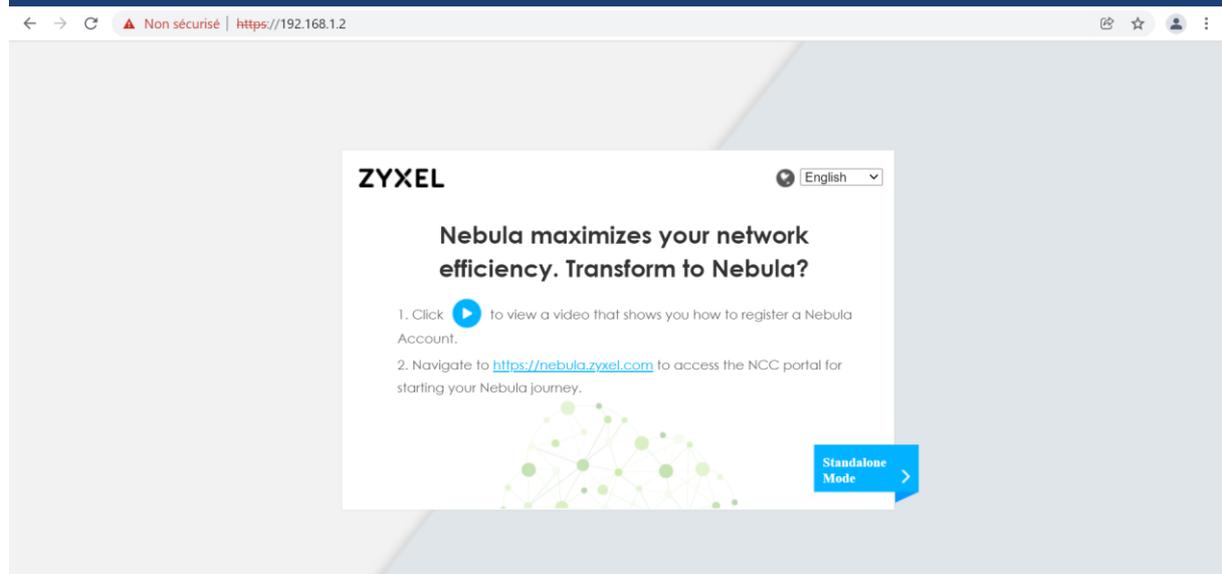
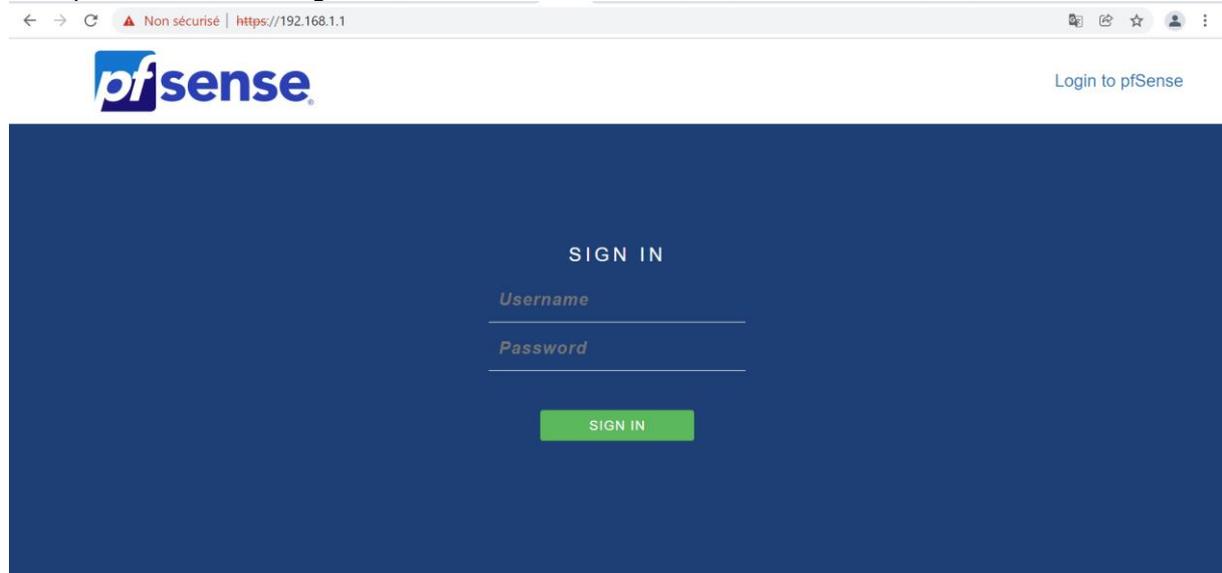
Mot de passe

Langue

Connexion Réinitialiser

Config vlan port 1
Trunk
Port 1 accueil lan pfsense
Screen
Mettre le vlan 1 étiqueté (tagged)
Same port 2
Port 2 accueil wifi

Suite à cela nous récupérons bien internet et l'accès au pfsense et à la borne wifi
Mais pour l'instant le filtrage reste le même il faut désormais administrer les 2 réseaux

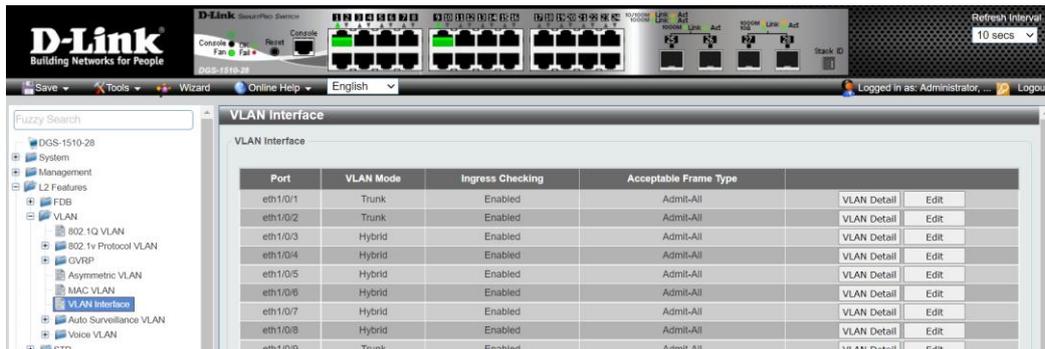


Port	Mode du réseau local virtuel	Contrôle d'entrée	Type de frame acceptable
eth1/0/1	Hybrid	Activé	Admettre tout
eth1/0/2	Hybrid	Activé	Admettre tout
eth1/0/3	Hybrid	Activé	Admettre tout
eth1/0/4	Hybrid	Activé	Admettre tout
eth1/0/5	Hybrid	Activé	Admettre tout
eth1/0/6	Hybrid	Activé	Admettre tout
eth1/0/7	Hybrid	Activé	Admettre tout
eth1/0/8	Hybrid	Activé	Admettre tout
eth1/0/9	Hybrid	Activé	Admettre tout
eth1/0/10	Hybrid	Activé	Admettre tout
eth1/0/11	Hybrid	Activé	Admettre tout
eth1/0/12	Hybrid	Activé	Admettre tout
eth1/0/13	Hybrid	Activé	Admettre tout
eth1/0/14	Hybrid	Activé	Admettre tout
eth1/0/15	Hybrid	Activé	Admettre tout
eth1/0/16	Hybrid	Activé	Admettre tout

- Sur la console des vlan on peut administrer tous les ports du switch

- On met donc le premier port en trunk pour le pfsense

Property	Value
Port	eth1/0/2
VLAN Mode	Trunk
Native VLAN	1 (tagged)
Trunk Allowed VLAN	1-4094
Dynamic Tagged VLAN	
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All



Créer le vlan 10

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface: re0 (18:d6:c7:04:e0:fd) - lan
Only VLAN capable interfaces will be shown.

VLAN Tag: 10
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority: 0
802.1Q VLAN Priority (between 0 and 7).

Description: Vlan Guest
A group description may be entered here for administrative reference (not parsed).

[Save](#)

Interface Assignments | Interface Groups | Wireless | **VLANs** | QinQs | PPPs | GREs | GIFs | Bridges | LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
re0 (lan)	10		Vlan Guest	Edit Delete

[+ Add](#)

Faites de même pour le vlan 1 (privé) vous devriez obtenir le résultat suivant

Interfaces / VLANs

Interface Assignments | Interface Groups | Wireless | **VLANs** | QinQs | PPPs | GREs | GIFs | Bridges | LAGGs

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
re0 (lan)	1		Vlan Privé	Edit Delete
re0 (lan)	10		Vlan Guest	Edit Delete

[+ Add](#)

Assigner l'interface Opt1 sur le Vlan Guest

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (00:d8:61:b8:c1:0e)
LAN	re0 (18:d6:c7:04:e0:fd) Delete
OPT1	VLAN 10 on re0 - lan (Vlan Guest) Delete

Save

Faire une règle qui laisse tout passer, pour notamment avoir internet sans soucis

Firewall / Rules / OPT1

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	4 / 260 KIB	IPv4 *	*	*	*	*	none			↓ ↻ 🗑️ 🔗 🔧 🔍

↑ Add ↓ Add Delete Save Separator

Mettre en place le dhcp sur l'interface en question

Services / DHCP Server / OPT1

LAN **OPT1**

General Options

Enable Enable DHCP server on OPT1 interface

Subnet 192.168.4.0

Subnet mask 255.255.255.0

Available range 192.168.4.1 - 192.168.4.254

Range
From To

- Après cliquer sur le save bleu

Interfaces / OPT1 (re0.10)

General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

- Faites save bleu

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
pfSenseGUIAccess	192.168.1.1	Disable Access to pfSense GUI	

Faites des alias pour chacune de vos adresses

Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
SwitchGUIAccess	192.168.1.3	Disable Access to Switch	
ZyxelGUIAccess	192.168.1.2	Disable Access to Zyxel	
pfSenseGUIAccess	192.168.1.1	Disable Access to pfSense GUI	

Il faut maintenant bloquer l'accès au réseau guest à notre serveur pfsense en créant une règles dans l'onglet floating en ajoutant les paramètres comme ci-dessous

Firewall / Rules / Floating / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Quick Apply the action immediately on match.
Set this option to apply this action to traffic that matches this rule immediately.

Interface WAN
LAN
OPT1
Choose the interface(s) for this rule.

Direction in

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source Invert match any Source Address /

[Display Advanced](#)
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match Single host or alias pfSenseGUIAccess /

Destination Port Range HTTPS (443) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description VLAN 10 - no access to pfSense GUI
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1642588039
Created	1/19/22 10:27:19 by admin@192.168.1.25 (Local Database)
Updated	1/19/22 10:27:19 by admin@192.168.1.25 (Local Database)

[Save](#)

Cliquez sur le save bleu

Faites de même pour votre ZyXEL et votre Switch vous devriez obtenir le résultat ci-dessous (à noter que ZyXEL peut être en https comme en http il faut donc bloquer les deux)

Firewall / Rules / Floating

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

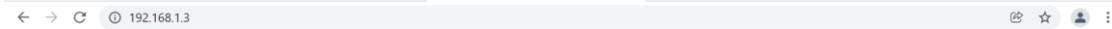
Floating WAN LAN OPT1

Rules (Drag to Change Order)

States	Interfaces	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 23 KIB	OPT1	IPv4 TCP/UDP	*	*	pfSenseGUIAccess	443 (HTTPS)	*	none		VLAN 10 - no access to pfSense GUI	
0 / 8 KIB	OPT1	IPv4 TCP/UDP	*	*	ZyxelGUIAccess	443 (HTTPS)	*	none		VLAN 10 - no access to Zyxel GUI	
0 / 4 KIB	OPT1	IPv4 TCP/UDP	*	*	ZyxelGUIAccess	80 (HTTP)	*	none		VLAN 10 - no access to Zyxel GUI	
0 / 18 KIB	OPT1	IPv4 TCP/UDP	*	*	SwitchGUIAccess	80 (HTTP)	*	none		VLAN 10 - no access to Switch GUI	

Add Add Delete Save Separator

Suite à cela lors de votre connexion au réseau guest pour les 3 adresses vous devriez avoir la page suivante :



Ce site est inaccessible

192.168.1.3 a mis trop de temps à répondre.

Voici quelques conseils :

- Vérifier la connexion
- Vérifier le proxy et le pare-feu
- Exécutez les diagnostics réseau de Windows

ERR_CONNECTION_TIMED_OUT

Actualiser

Détails

D-Link SMARTPRO SWITCH
DGS-1510-28

Enreg. Outils Assistant Aide en ligne Français

Fuzzy Search

- Mise à jour et sauvegarde du microprogramme
- Restauration et sauvegarde de la configuration
- Sauvegarde de fichier journal
- Ping
- Traceroute
- Gestion des langues
- Réinitialiser
- Redémarrer le système

du site HTTP

- Restauration de la configuration à partir du site HTTP
- Restauration de la configuration à partir du serveur TFTP
- Sauvegarde de la configuration vers le site HTTP
- Sauvegarde de la configuration vers le serveur TFTP

Sauvegarde de la configuration vers le site HTTP

Fichier source

64 chars

running-config startup-config

Sauvegarder

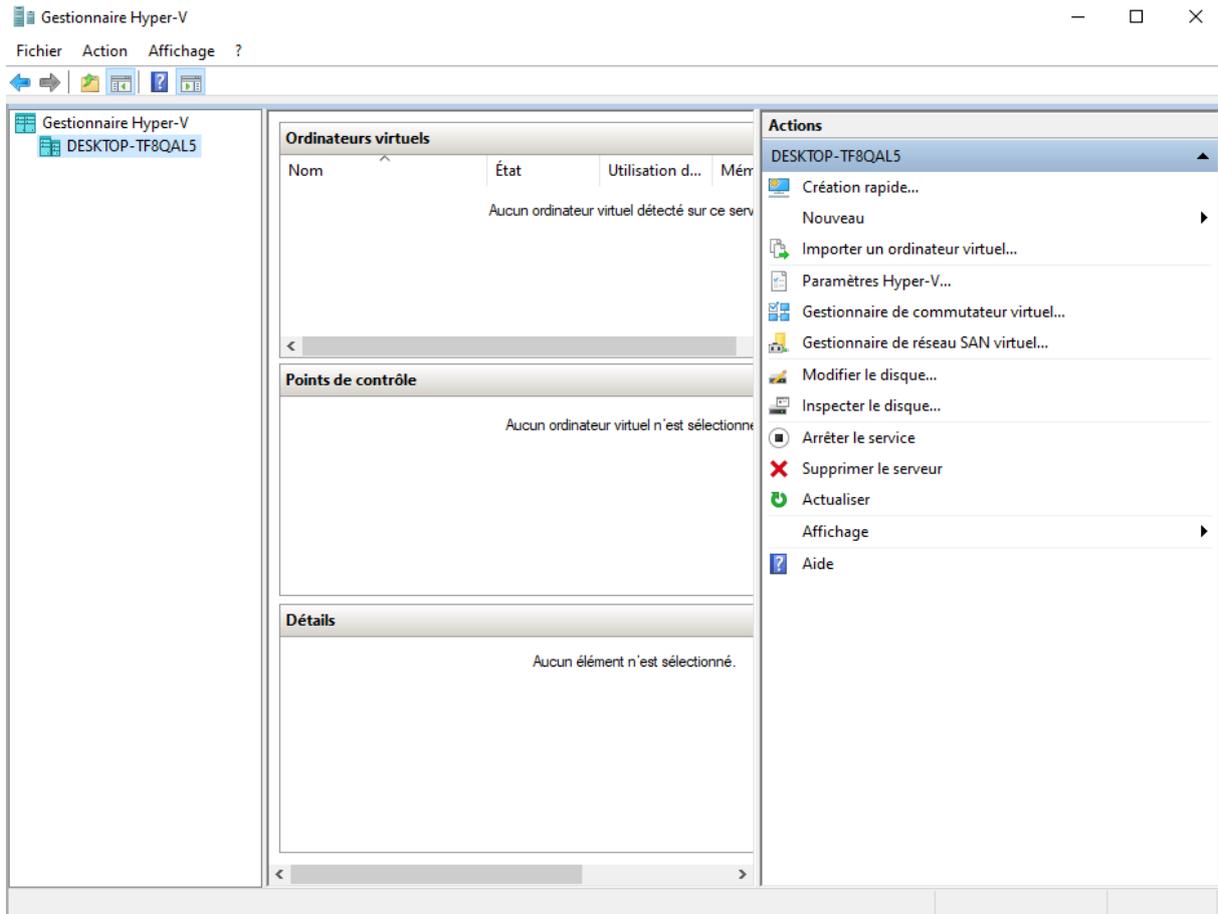
- Vous obtiendrez ensuite la running config

6 Mission Radius

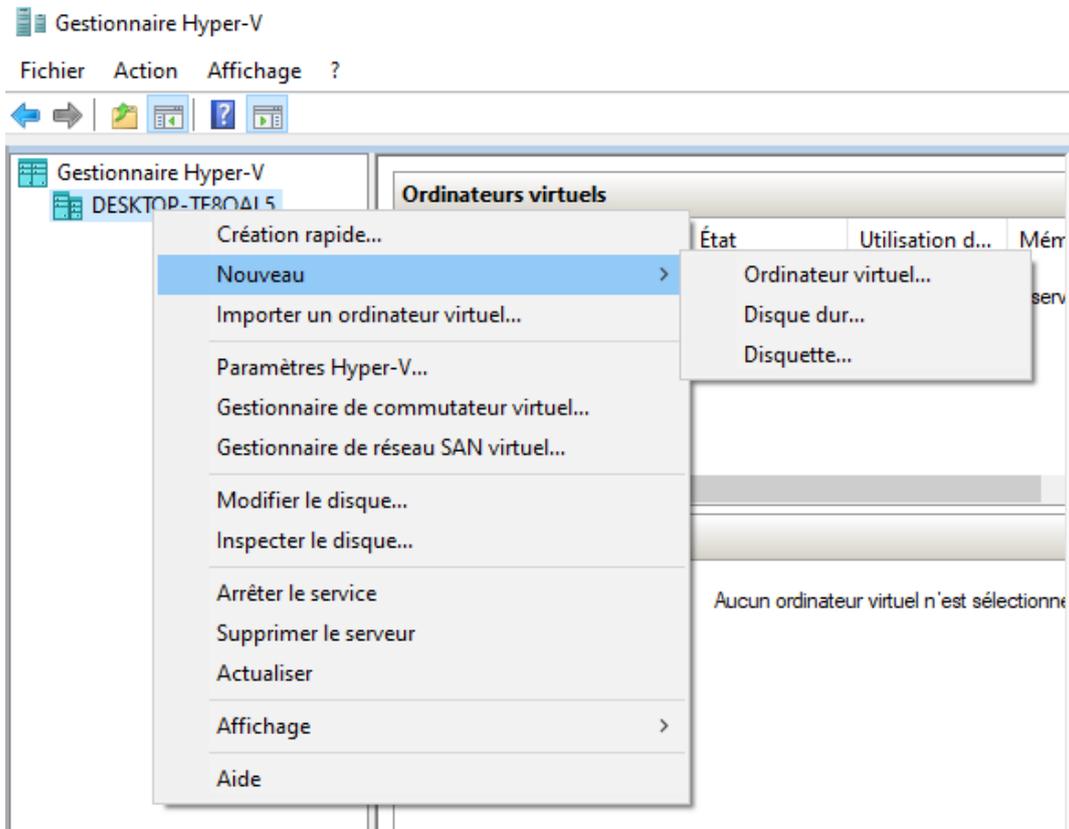
6.1 Création des VMs

Il faut hyper v, 1 serveur windows, 1 ou 2 pc test sur le domaine, 1 pfsense, 1 switch, 1 borne wifi et penser à ajouter les postes tests sur le domaine

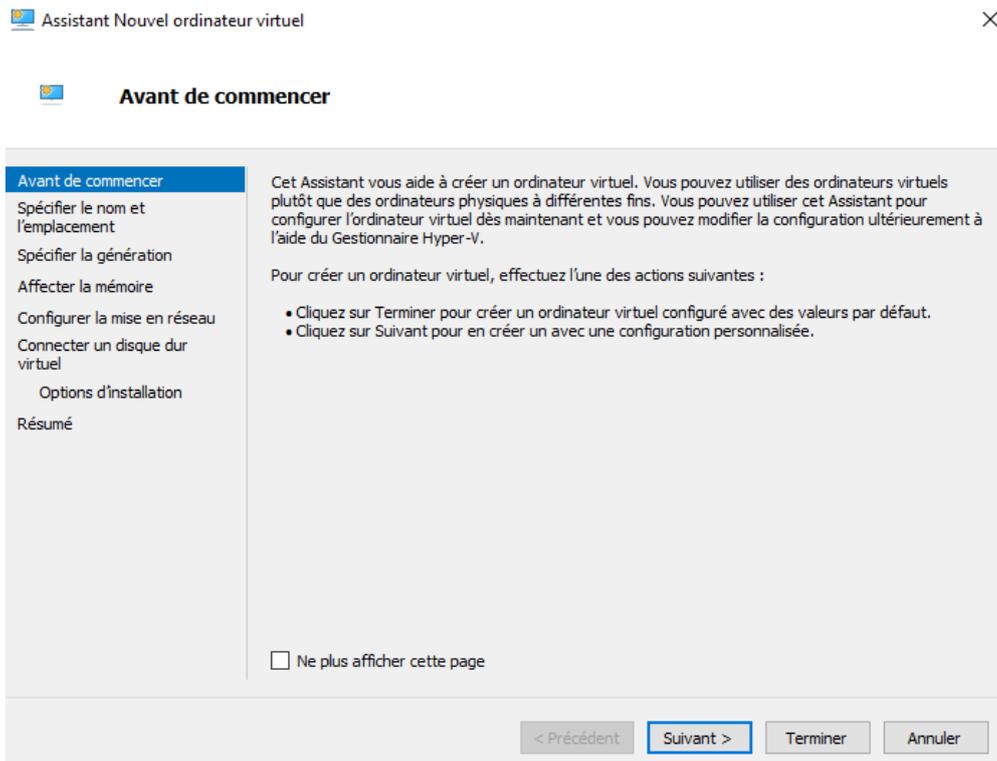
Console HyperV :



- Pour créer une nouvelle vm :



- Puis il est possible de tout modifier



Assistant Nouvel ordinateur virtuel



Spécifier le nom et l'emplacement

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Choisissez un nom et un emplacement pour cet ordinateur virtuel.

Le nom est affiché dans le Gestionnaire Hyper-V. Nous vous recommandons d'utiliser un nom qui vous permettra d'identifier facilement cet ordinateur virtuel, tel que le nom de la charge de travail ou du système d'exploitation invité.

Nom :

Vous pouvez créer un dossier ou utiliser un dossier existant pour stocker l'ordinateur virtuel. Si vous ne sélectionnez pas de dossier, l'ordinateur virtuel est stocké dans le dossier par défaut configuré pour ce serveur.

Stocker l'ordinateur virtuel à un autre emplacement

Emplacement :

Si vous envisagez de créer des points de contrôle de cet ordinateur virtuel, choisissez un emplacement avec un espace libre suffisant. Les points de contrôle incluent les données des ordinateurs virtuels et peuvent nécessiter un espace considérable.

< Précédent **Suivant >** Terminer Annuler

Assistant Nouvel ordinateur virtuel



Spécifier la génération

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Choisissez la génération de cet ordinateur virtuel.

Génération 1

Cette génération d'ordinateurs virtuels prend en charge des systèmes d'exploitation invités 32 bits et 64 bits. Elle fournit le matériel virtuel disponible dans toutes les versions précédentes d'Hyper-V.

Génération 2

Cette génération d'ordinateurs virtuels prend en charge des fonctionnalités de virtualisation plus récentes. Dotée d'un microprogramme UEFI, elle nécessite la prise en charge d'un système d'exploitation invité 64 bits.

Une fois l'ordinateur virtuel créé, vous ne pouvez plus modifier sa génération.

[En savoir plus sur la prise en charge de la génération d'ordinateurs virtuels](#)

< Précédent **Suivant >** Terminer Annuler

Assistant Nouvel ordinateur virtuel



Affecter la mémoire

Avant de commencer	<p>Spécifiez la quantité de mémoire à allouer à cet ordinateur virtuel. Vous pouvez spécifier une quantité comprise entre 32 Mo et 251658240 Mo. Pour améliorer les performances, spécifiez davantage que la quantité minimale recommandée pour le système d'exploitation.</p> <p>Mémoire de démarrage : <input type="text" value="4096"/> Mo</p> <p><input checked="" type="checkbox"/> Utiliser la mémoire dynamique pour cet ordinateur virtuel.</p> <p>i Pour déterminer la quantité de mémoire à attribuer à un ordinateur virtuel, tenez compte de la façon dont vous envisagez d'utiliser l'ordinateur virtuel et du système d'exploitation qu'il exécutera.</p>
Spécifier le nom et l'emplacement	
Spécifier la génération	
Affecter la mémoire	
Configurer la mise en réseau	
Connecter un disque dur virtuel	
Options d'installation	
Résumé	
<p>< Précédent Suivant > Terminer Annuler</p>	

Assistant Nouvel ordinateur virtuel



Configurer la mise en réseau

Avant de commencer	<p>Chaque nouvel ordinateur virtuel inclut une carte réseau. Vous pouvez configurer celle-ci de façon à utiliser un commutateur virtuel ou la laisser déconnectée.</p> <p>Connexion : <input type="text" value="Non connecté"/></p>
Spécifier le nom et l'emplacement	
Spécifier la génération	
Affecter la mémoire	
Configurer la mise en réseau	
Connecter un disque dur virtuel	
Options d'installation	
Résumé	
<p>< Précédent Suivant > Terminer Annuler</p>	

Assistant Nouvel ordinateur virtuel



Connecter un disque dur virtuel

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Un ordinateur virtuel requiert un espace de stockage pour l'installation d'un système d'exploitation. Vous pouvez spécifier le stockage dès maintenant ou le configurer ultérieurement en modifiant les propriétés de l'ordinateur virtuel.

Créer un disque dur virtuel

Utilisez cette option pour créer un disque dur virtuel de taille dynamique (VHDX).

Nom :

Emplacement :

Taille : Go (Maximum : 64 To)

Utiliser un disque dur virtuel existant

Utilisez cette option pour attacher un disque dur virtuel VHDX existant.

Emplacement :

Attacher un disque dur virtuel ultérieurement

Utilisez cette option pour ignorer cette étape et attacher un disque dur virtuel existant ultérieurement.

< Précédent

Assistant Nouvel ordinateur virtuel



Options d'installation

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Vous pouvez installer un système d'exploitation maintenant si vous avez accès au média d'installation, ou vous pouvez l'installer ultérieurement.

Installer un système d'exploitation ultérieurement

Installer un système d'exploitation à partir d'un fichier image de démarrage

Média

Fichier image (.iso) :

Installer un système d'exploitation à partir d'un serveur d'installation réseau

Votre carte réseau est déconnectée. Pour effectuer une installation réseau, revenez à la page Configurer la mise en réseau et connectez la carte réseau.

< Précédent

29

Assistant Nouvel ordinateur virtuel



Fin de l'Assistant Nouvel ordinateur virtuel

Avant de commencer

Spécifier le nom et l'emplacement

Spécifier la génération

Affecter la mémoire

Configurer la mise en réseau

Connecter un disque dur virtuel

Options d'installation

Résumé

Vous avez terminé l'Assistant Nouvel ordinateur virtuel. Vous êtes sur le point de créer l'ordinateur virtuel suivant.

Description :

Nom :	SRV-AD
Génération	Génération 2
Mémoire :	4096 Mo
Réseau :	Non connecté
Disque dur :	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\SRV-AD.vhdx (VHDX)
Système d'exploitation :	Sera installé à partir de C:\iso\Microsoft Windows 2019 serveur\SW_DVD9_1

< >

Pour créer l'ordinateur virtuel et fermer l'Assistant, cliquez sur Terminer.

< Précédent Suivant > **Terminer** Annuler

- Dans la console le serveur est ici :

Gestionnaire Hyper-V

Fichier Action Affichage ?

← → | 📁 | ? | 📄

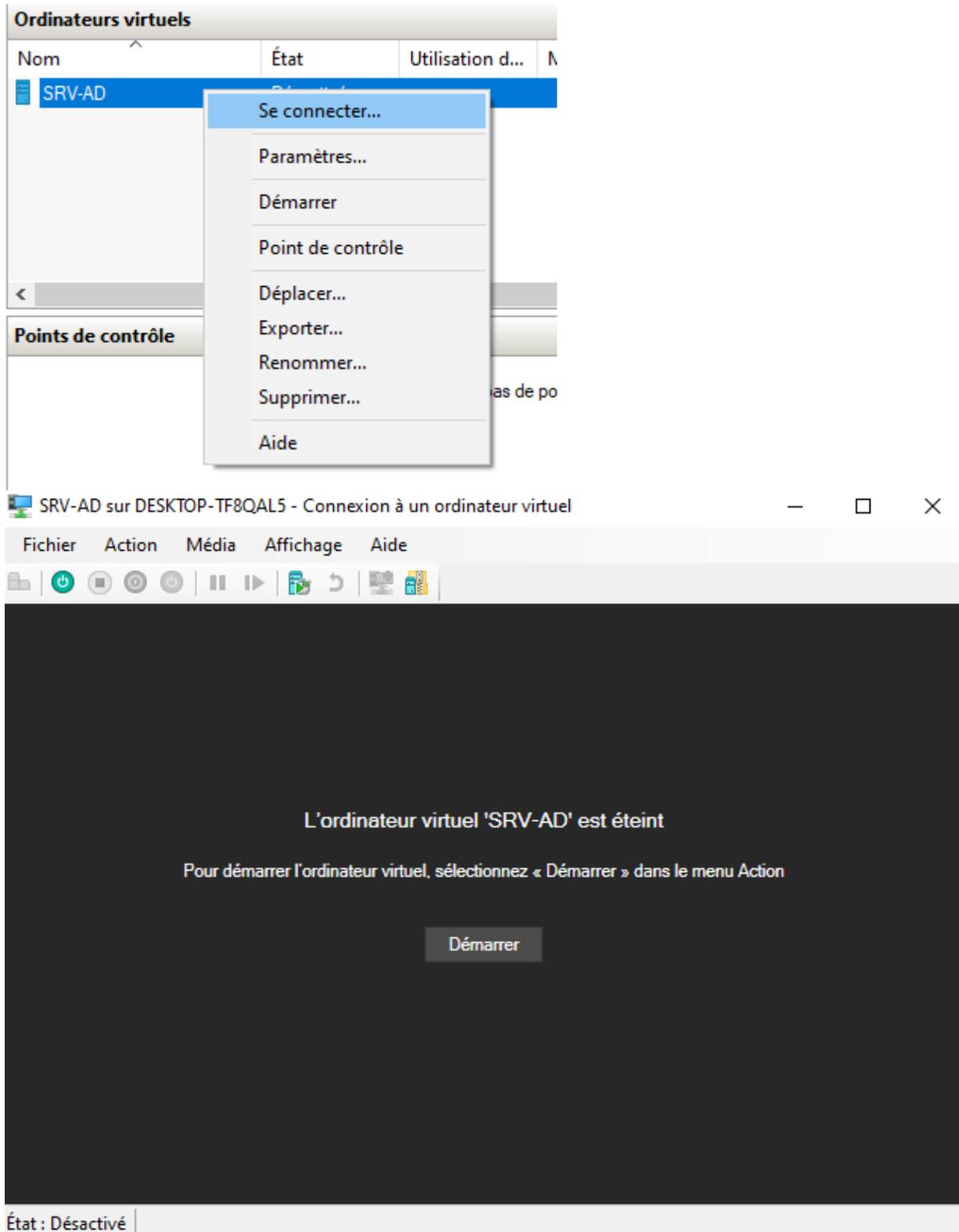
Gestionnaire Hyper-V

DESKTOP-TF8QAL5

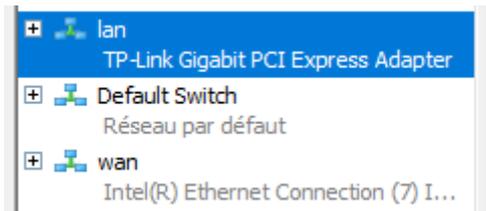
Ordinateurs virtuels				
Nom	État	Utilisation d...	Mémoire affectée	Temps d'activité
SRV-AD	Désactivé			

Points de contrôle

- Cliquez droit > se connecter :



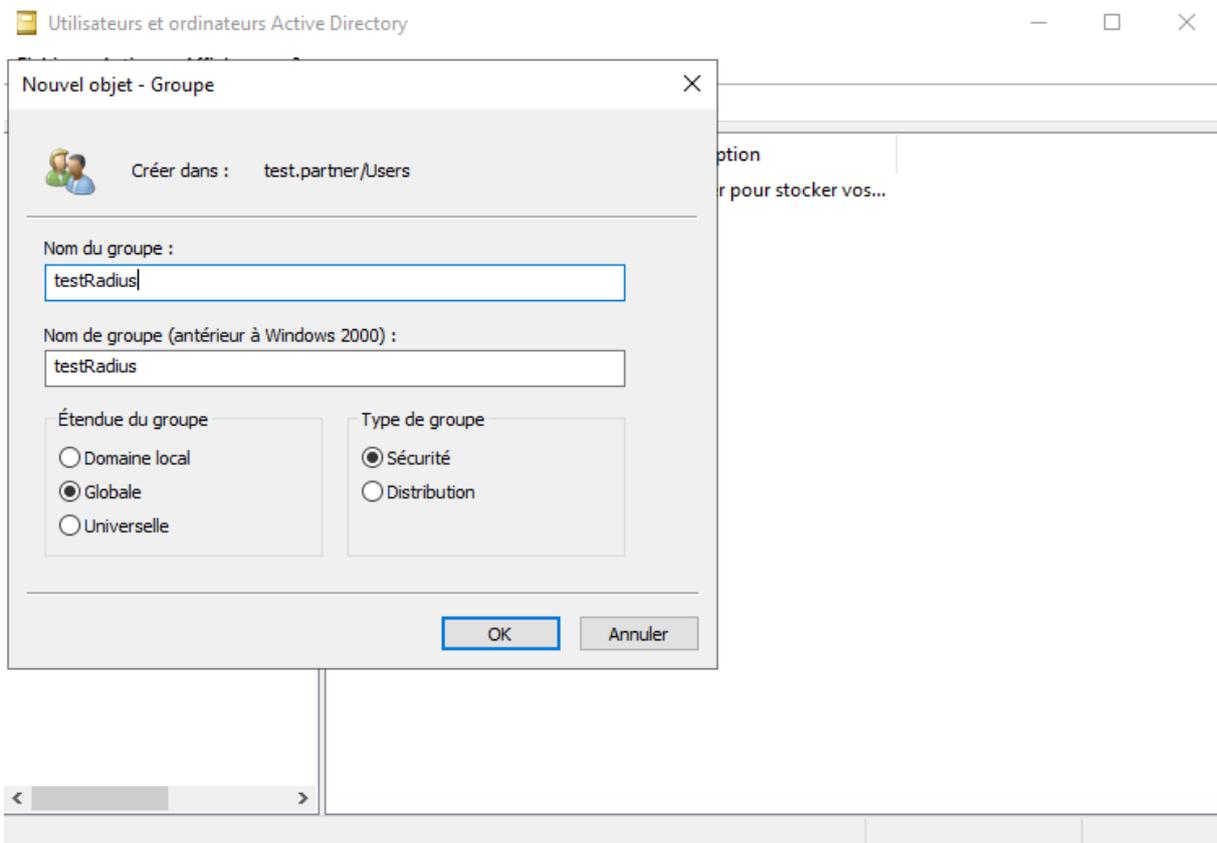
- Installer les rôles ad
- Installation d'un pfsense :
- 2 cartes réseaux virtuelles :



- Savoir leurs adresses mac pour installer un pfsense

```
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***  
WAN (wan)      -> hm1      -> v4/DHCP4: 192.168.3.11/24  
LAN (lan)      -> hm0      -> v4: 192.168.1.1/24  
OPT1 (opt1)    -> hm0.10   -> v4: 192.168.4.1/24
```

- Création d'un groupe utilisateur dans ad :



Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom	Type	Description
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...
Admins du ...	Groupe de séc...	Administrateurs désigné...
Contrôleurs ...	Groupe de séc...	Tous les contrôleurs de ...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
DnsAdmins	Groupe de séc...	Groupe des administrate...
DnsUpdateP...	Groupe de séc...	Les clients DNS qui sont ...
Éditeurs de c...	Groupe de séc...	Les membres de ce grou...
Groupe de r...	Groupe de séc...	Les mots de passe des ...
Groupe de r...	Groupe de séc...	Les mots de passe des ...
Invité	Utilisateur	Compte d'utilisateur inv...
Invités du d...	Groupe de séc...	Tous les invités du dom...
Ordinateurs ...	Groupe de séc...	Toutes les stations de tra...
Propriétaires...	Groupe de séc...	Les membres de ce grou...
Protected Us...	Groupe de séc...	Les membres de ce grou...
Serveurs RA...	Groupe de séc...	Les serveurs de ce group...
testRadius	Groupe de séc...	
Utilisateurs ...	Groupe de séc...	Tous les utilisateurs du d...

- Installation serveur radius :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
SRV-AD.test.partner

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Attestation d'intégrité de l'appareil	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input type="checkbox"/> Serveur DHCP	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Dire...	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Manage...	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de docu...	
<input type="checkbox"/> Services de certificats Active Directory	
<input type="checkbox"/> Services de déploiement Windows	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 install...	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
SRV-AD.test.partner

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation réussie sur SRV-AD.test.partner.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils de la stratégie réseau et des services d'accès

Services de stratégie et d'accès réseau

1 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

[Exporter les paramètres de configuration](#)

< Précédent Suivant > Fermer Annuler

Assistant Ajout de rôles et de fonctionnalités



Ajouter les fonctionnalités requises pour Services de stratégie et d'accès réseau ?

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ▲ Outils d'administration de serveur distant
 - ▲ Outils d'administration de rôles
 - [Outils] Outils de la stratégie réseau et des services d'accès

Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités

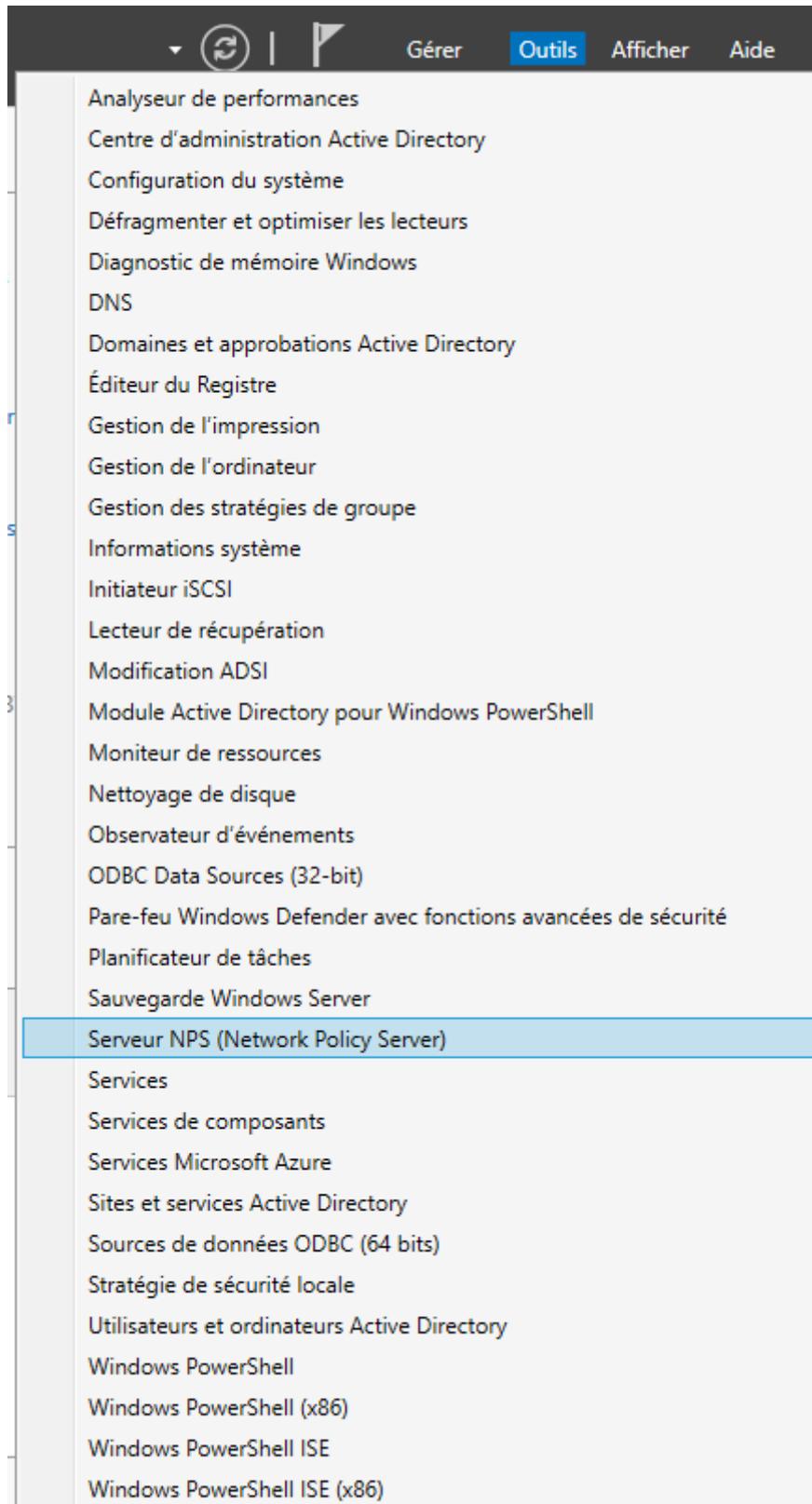
Annuler

- Ajout groupe radius dans active directory :

radius1 Utilisateur
 radius2 Utilisateur
 RadiusUser Groupe de séc...

Les utilisateurs sont dans le groupe

- Dans le menu outils > serveur NPS



- On peut choisir quel type de radius on veut :

The screenshot shows the Windows NPS (Network Policy Server) console. The window title is 'Serveur NPS (Network Policy Server)'. The menu bar includes 'Fichier', 'Action', and 'Affichage'. The left pane shows the tree view for 'NPS (Local)' with sub-items: 'Clients et serveurs RADIUS', 'Stratégies', 'Gestion', and 'Gestion des modèles'. The main pane is titled 'NPS (Local)' and contains the following content:

Mise en route

Le serveur NPS (Network Policy Server) vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'authentification et l'autorisation des demandes de connexion.

Configuration standard

Sélectionnez un scénario de configuration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.

- Serveur RADIUS pour les connexions d'accès à distance ou VPN
- Serveur RADIUS pour les connexions d'accès à distance ou VPN
- Serveur RADIUS pour les connexions câblées ou sans fil 802.1X

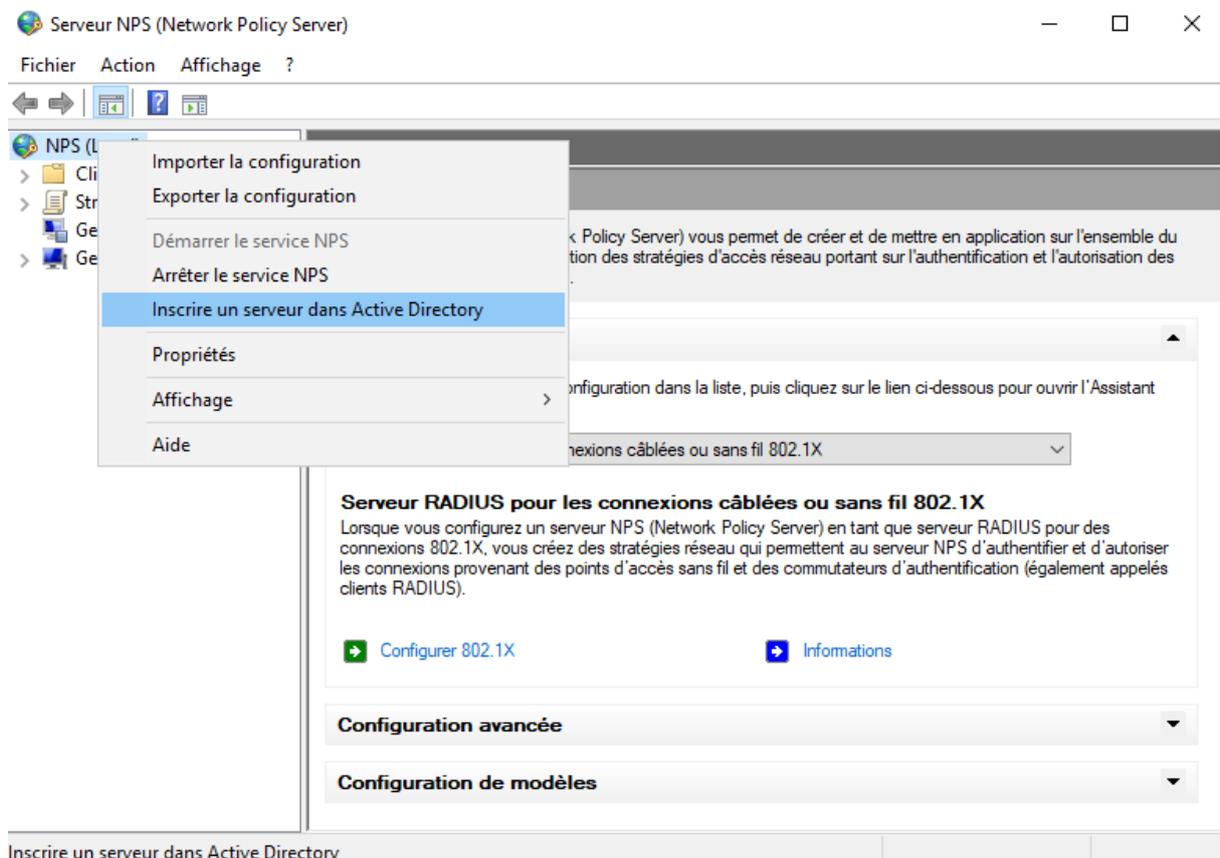
Lorsque vous configurez un serveur NPS (Network Policy Server) en tant que serveur RADIUS pour des connexions d'accès à distance ou VPN, vous créez des stratégies réseau qui permettent au serveur NPS d'authentifier et d'autoriser les connexions provenant des serveurs d'accès réseau à distance ou VPN (également appelés clients RADIUS).

[Configurer une connexion VPN ou d'accès à distance](#) [Informations](#)

Configuration avancée

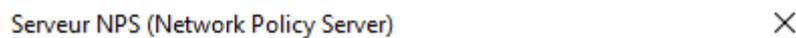
Configuration de modèles

- Clic droit > nps > inscrire un serveur dans ad :



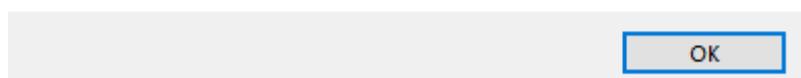
Pour permettre aux serveurs NPS (Network Policy Server) d'authentifier les utilisateurs dans Active Directory, les ordinateurs NPS doivent être autorisés à lire les propriétés de numérotation des utilisateurs du domaine.

Voulez-vous autoriser cet ordinateur à lire les propriétés de numérotation des utilisateurs du domaine test.partner ?

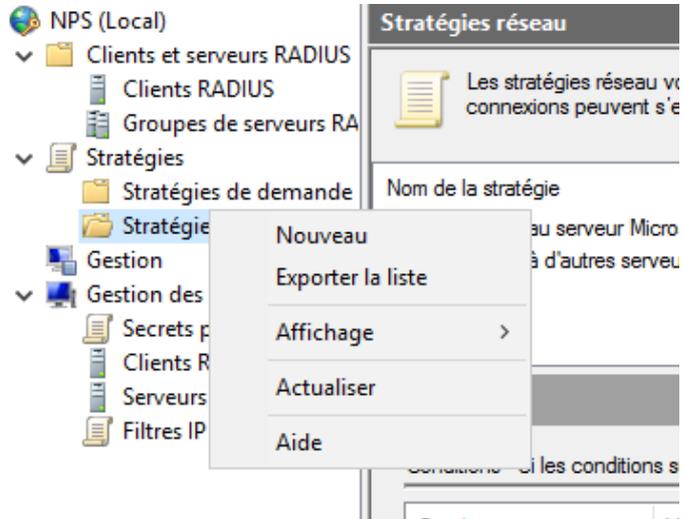


Cet ordinateur est désormais autorisé à lire les propriétés de numérotation des utilisateurs du domaine test.partner.

Pour autoriser cet ordinateur à lire les propriétés de numérotation des utilisateurs d'autres domaines, vous devez l'inscrire en tant que membre du groupe de serveurs RAS/NPS dans les domaines concernés.



- Menu :
- Clic droit sur Stratégies Réseau > nouveau



- Configuration stratégie :

Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Type de serveur d'accès réseau :

Non spécifié

Spécifique au fournisseur :

10

Précédent **Suivant** Terminer Annuler

- Ensuite, cliquer sur ajouter une condition :
- Ajouter groupes windows

Nouvelle stratégie réseau



Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition



Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

- Restrictions relatives aux jours et aux heures**
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter...

Annuler

- Cliquer sur ajouter des groupes :

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

- Restrictions relatives aux jours et aux heures**
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter des groupes...

Sélectionner un groupe

Sélectionnez le type de cet objet :

un groupe

À partir de cet emplacement :

test.local

Entrez le nom de l'objet à sélectionner (exemples) :

RadiusUserS

Types d'objets... Emplacements... Vérifier les noms

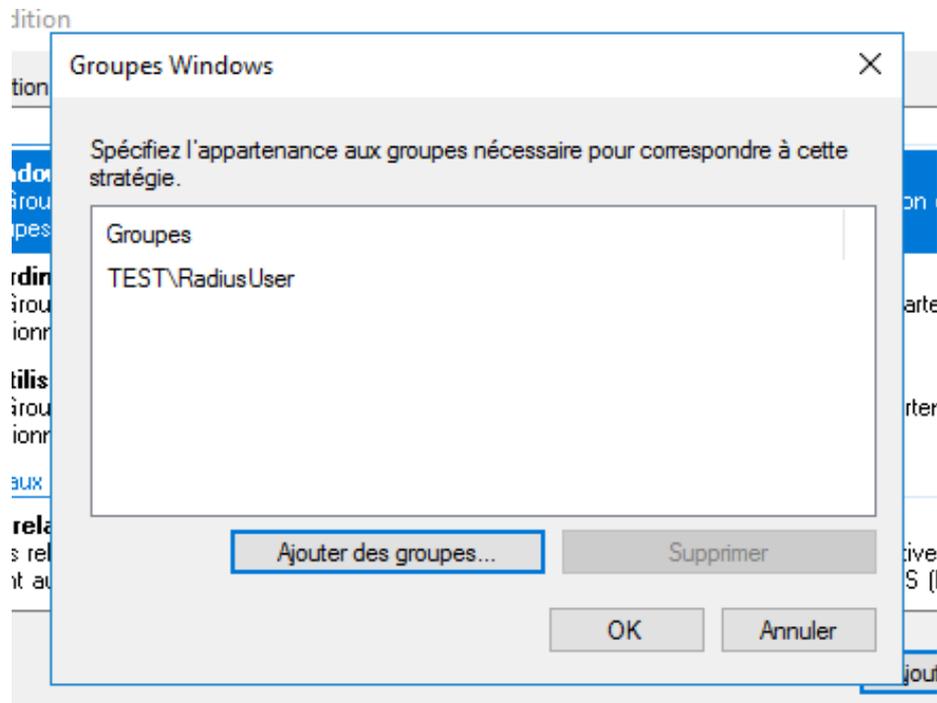
Avancé... OK Annuler

Ajouter... Annuler

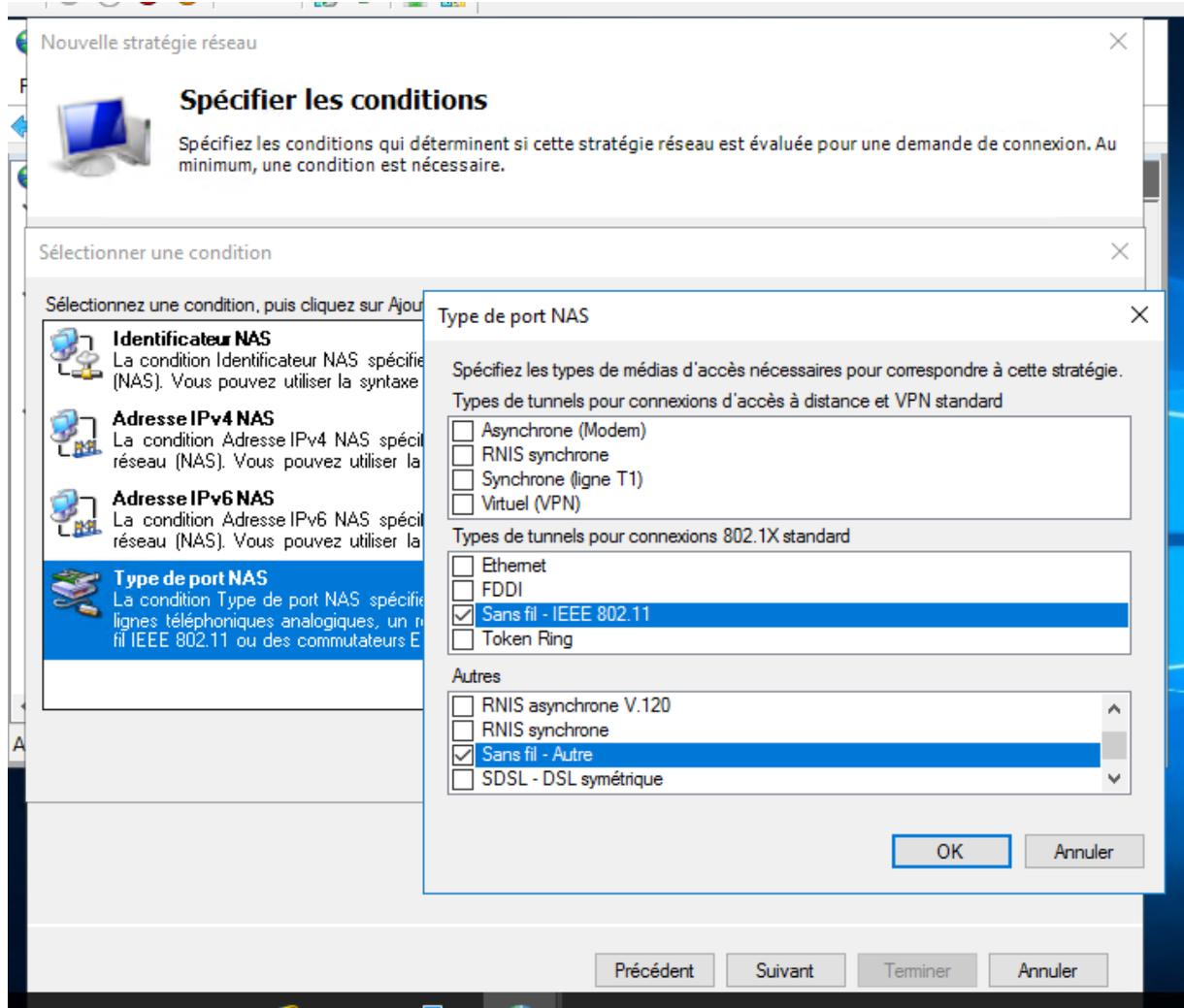
Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

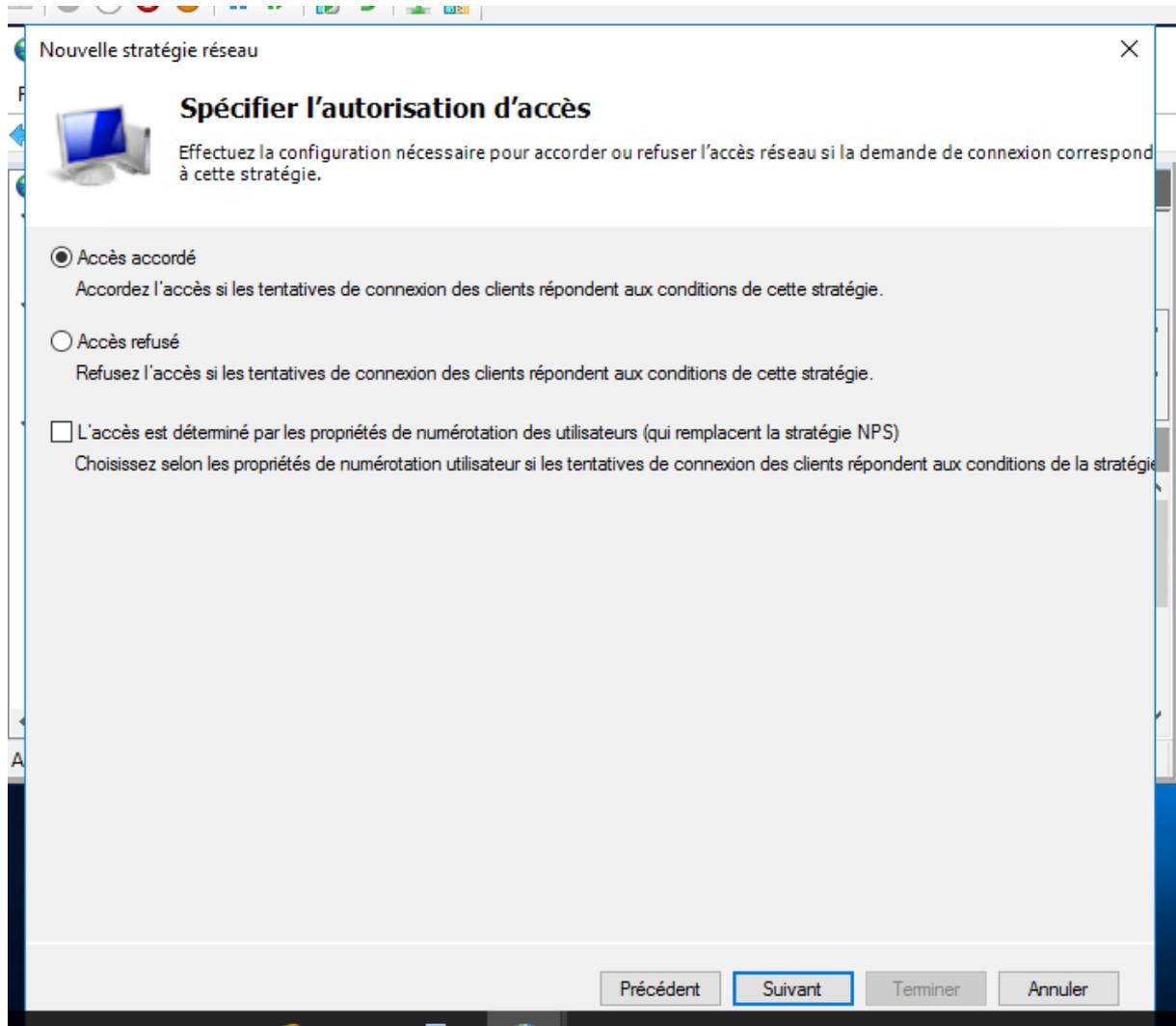
- Puis ajouter le groupe précédemment créé
- Puis



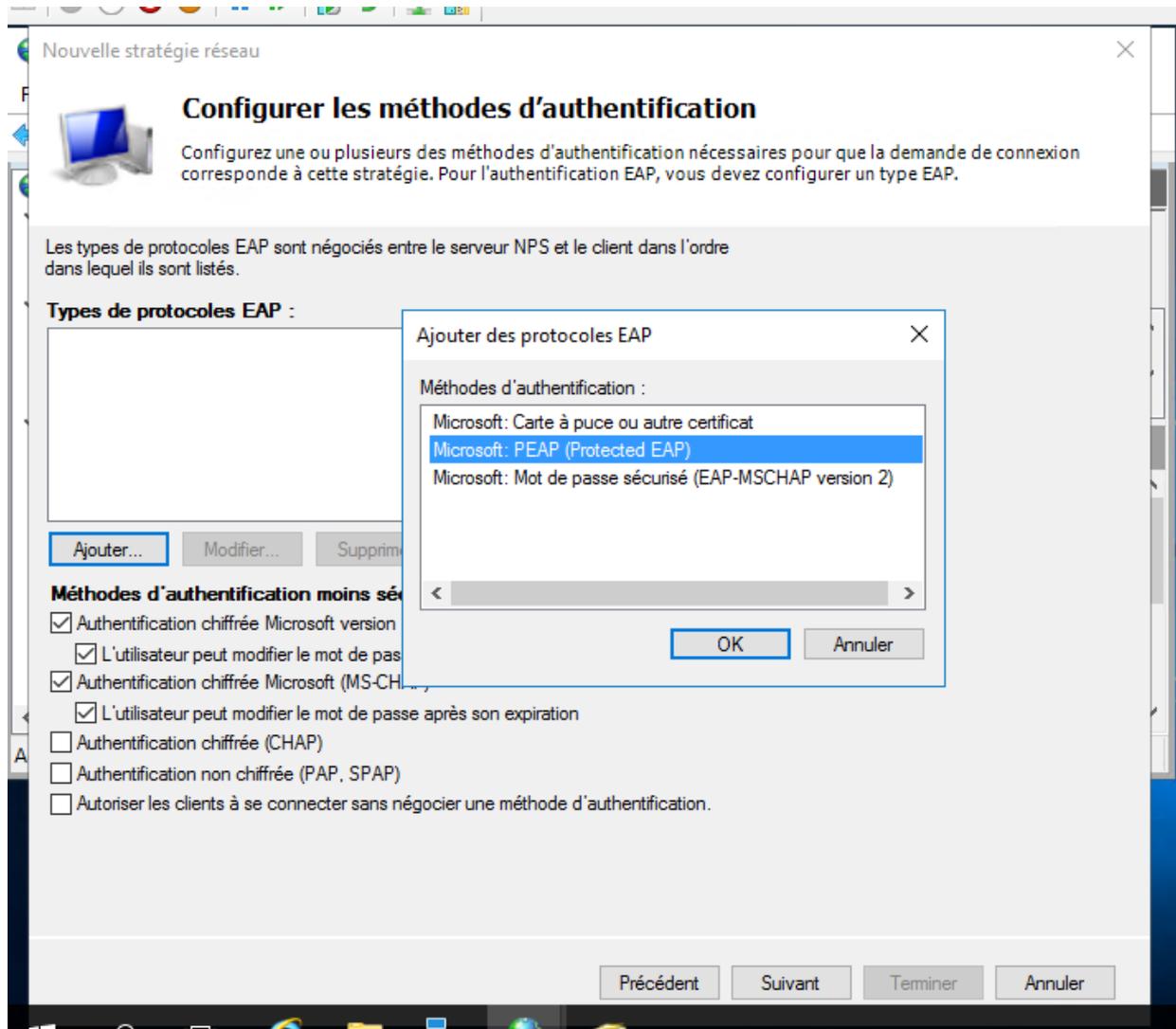
- Ensuite sélectionner type de port nas et cliquer sur ajouter puis sélectionner les deux options sans fil :



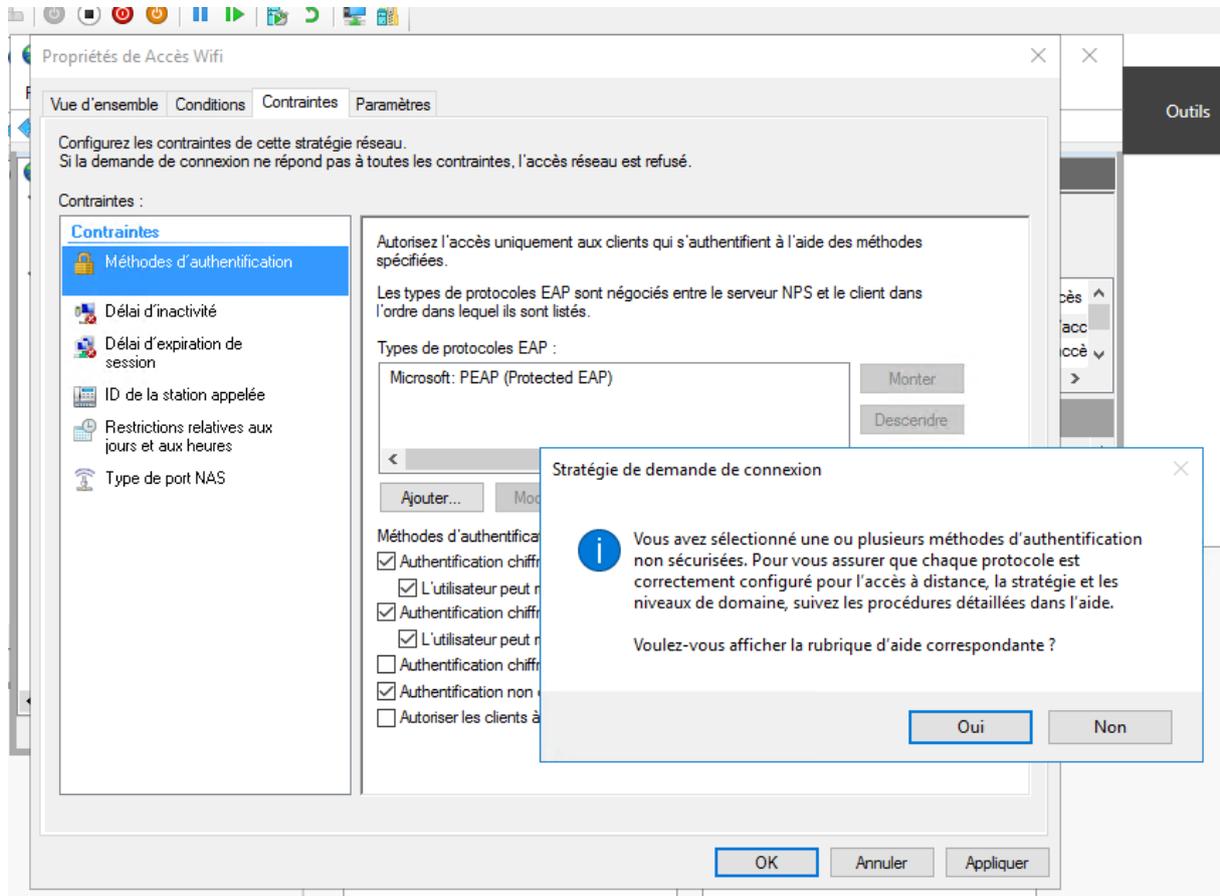
- Puis laisser coché accès accordé :



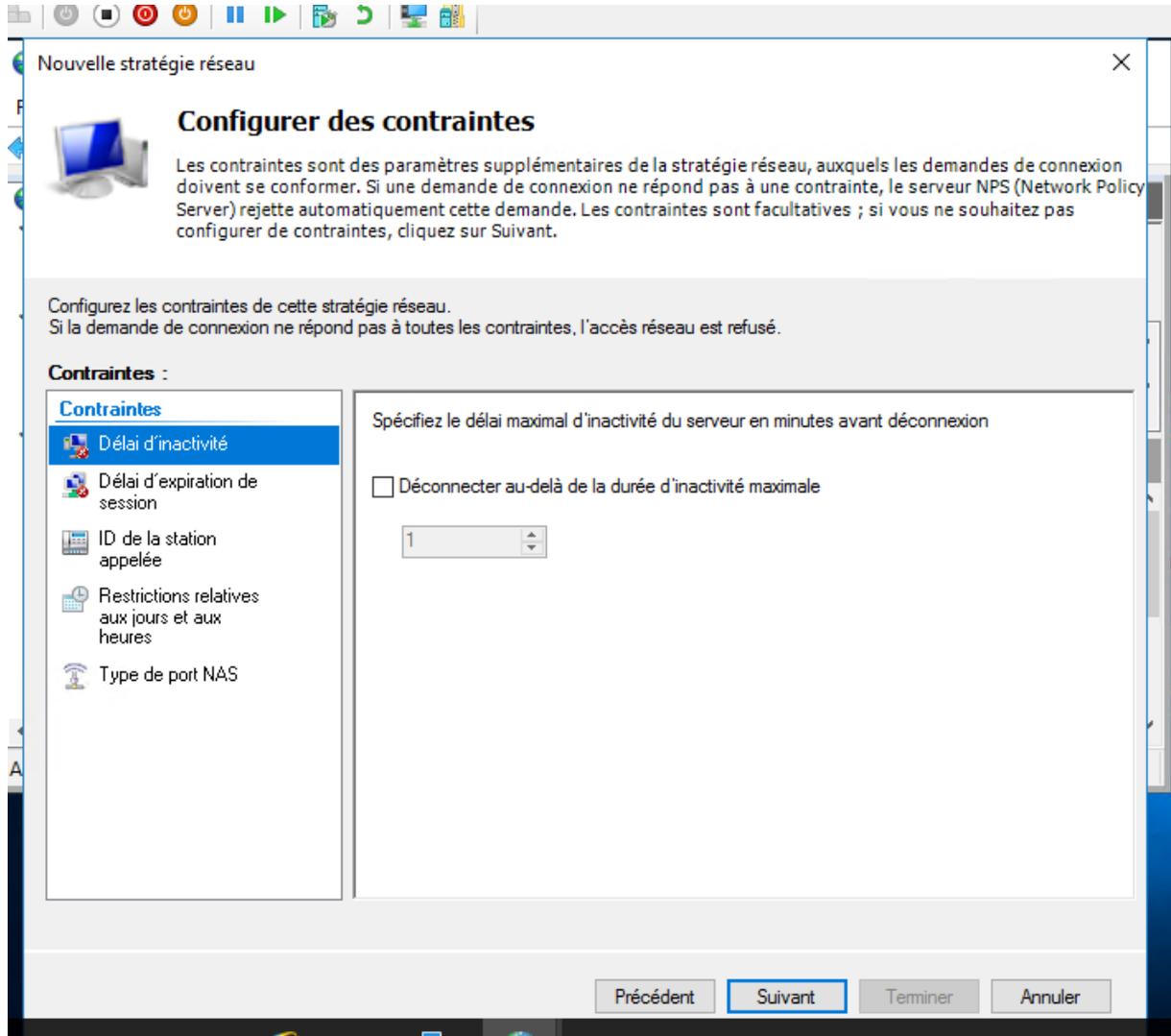
- Pour les méthodes d'authentification cliquer su rajouter puis sélectionner peap :



- Et sélectionner authentification non chiffrée :



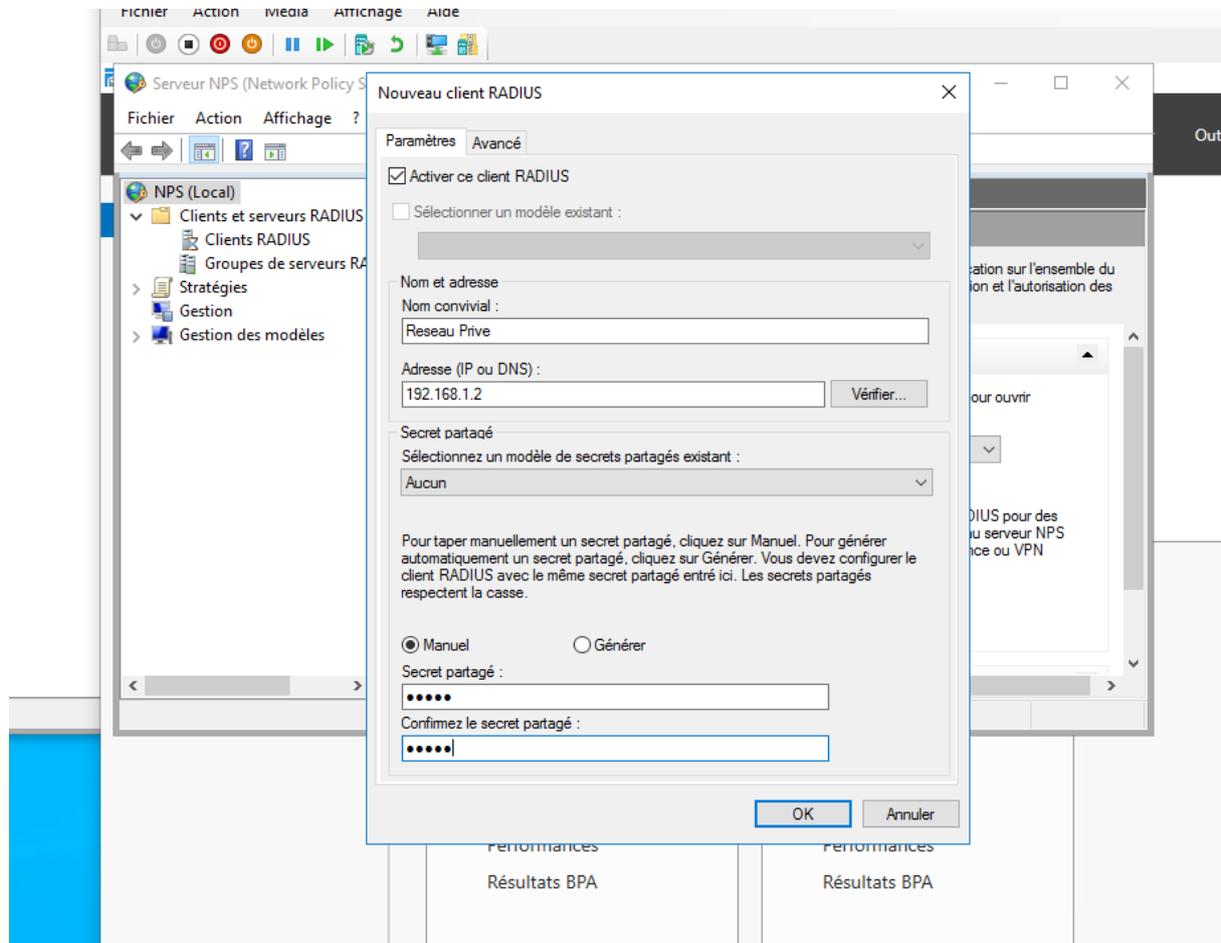
- Puis cliquer sur suivant et adapter les contraintes selon vos envies :



6.2 Ajout de la borne :

Ensuite retourner dans le menu déroulant, clic droit sur client radius :

Il faut renseigner les informations de la borne wifi : son nom, son ip et le secret partagé qu'il faudra renseigner sur la borne :



- Autorisé l'accès aux utilisateurs d'accéder au réseau

Propriétés de : radius2

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+
Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Autorisation d'accès réseau

Autoriser l'accès
 Refuser l'accès
 Contrôler l'accès via la Stratégie d'accès à distance

Vérifier l'identité de l'appelant :

Options de rappel

Pas de rappel
 Défini par l'appelant (service de routage et d'accès à distance uniquement)
 Toujours rappeler :

Attribuer des adresses IP statiques
Définissez les adresses IP à activer pour cette connexion d'appel entrant.

Appliquer les itinéraires statiques
Définir les itinéraires à activer pour cette connexion d'appel entrant.

OK Annuler Appliquer

Propriétés de : TEST3

Général Système d'exploitation Membre de Délégation
Emplacement Géré par Appel entrant

Autorisation d'accès réseau

Autoriser l'accès
 Refuser l'accès
 Contrôler l'accès via la Stratégie d'accès à distance

Vérifier l'identité de l'appelant :

Options de rappel

Pas de rappel
 Défini par l'appelant (service de routage et d'accès à distance uniquement)
 Toujours rappeler :

Attribuer des adresses IP statiques
Définissez les adresses IP à activer pour cette connexion d'appel entrant.

Appliquer les itinéraires statiques
Définir les itinéraires à activer pour cette connexion d'appel entrant.

OK Annuler Appliquer

- Faites de même pour les utilisateurs

- Ajouter service de certificats active directory

The image shows two screenshots from the Windows Server 2016 installation wizard. The top screenshot is titled "Sélectionner des rôles de serveurs" (Select server roles). It shows a list of roles with "Services de certificats Active Directory" (Active Directory Certificate Services) selected. A dialog box titled "Assistant Ajout de rôles et de fonctionnalités" (Add Roles and Features Wizard) is open, showing the selection of "Outils des services de certificats Active Directory" (Active Directory Certificate Services Tools) under "Outils d'administration de serveur distant" (Remote Server Administration Tools). The bottom screenshot is titled "Configuration des services de certificats Active Directory" (Active Directory Certificate Services Configuration). It shows the "Informations d'identification" (Identification Information) step, where the user is prompted to specify identification information for the role services. The "Informations d'identification" field contains "TEST\administrateur".

Sélectionner des rôles de serveurs

SÉLÉCTIONNER UN OU PLUSIEURS RÔLES À INSTALLER SUR LE SERVEUR SÉ

Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Expérience Windows Server Essentials
- Hyper-V
- MultiPoint Services
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS (Installé)
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS (Installé)
- Services AD LDS (Active Directory Lightweight Dire
- Services AD RMS (Active Directory Rights Manage
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de docu
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)

Assistant Ajout de rôles et de fonctionnalités

Ajouter les fonctionnalités requises pour Services de certificats Active Directory ?

Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ▲ Outils d'administration de serveur distant
 - ▲ Outils d'administration de rôles
 - ▲ Outils des services de certificats Active Directory [Outils] Outils de gestion de l'autorité de certification

Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

Configuration des services de certificats Active Directory

Informations d'identification

SÉLÉCTIONNER UN OU PLUSIEURS RÔLES À INSTALLER SUR LE SERVEUR SÉ

Spécifier les informations d'identification pour configurer les services de rôle

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :

- Utiliser l'autorité de certification autonome
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :

- Autorité de certification d'entreprise
- Service Web Stratégie d'inscription de certificats
- Service Web Inscription de certificats
- Service d'inscription de périphériques réseau

Informations d'identification : TEST\administrateur Modifier...

En savoir plus sur les rôles de serveur AD CS

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
win-srv2016.test.local

Services de rôle

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Sélectionner les services de rôle à configurer

- Autorité de certification
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne
- Service d'inscription de périphériques réseau
- Service Web Inscription de certificats
- Service Web Stratégie d'inscription de certificats

[En savoir plus sur les rôles de serveur AD CS](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
win-srv2016.test.local

Type d'installation

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

- Autorité de certification d'entreprise**
Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.
- Autorité de certification autonome**
Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

[En savoir plus sur le type d'installation](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

— □ ×

Type d'autorité de certification

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC**
- Clé privée
 - Chiffrement
 - Nom de l'AC
 - Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

- Autorité de certification racine**
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.
- Autorité de certification secondaire**
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

— □ ×

Clé privée

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée**
- Chiffrement
- Nom de l'AC
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

- Créer une clé privée**
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
- Utiliser la clé privée existante**
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.
 - Sélectionner un certificat et utiliser sa clé privée associée**
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.
 - Sélectionner une clé privée existante sur cet ordinateur**
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- Chiffrement**
- Nom de l'AC
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : RSA#Microsoft Software Key Storage Provider Longueur de la clé : 2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

- SHA256
- SHA384
- SHA512
- SHA1**

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
- Chiffrement
- Nom de l'AC**
- Période de validité
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC : WIN-SRV2016-CA

Suffixe du nom unique : DC=test,DC=local

Aperçu du nom unique : CN=WIN-SRV2016-CA,DC=test,DC=local

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

Période de validité

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
 - Chiffrement
 - Nom de l'AC
 - Période de validité**
- Base de données de certi...
- Confirmation
- Progression
- Résultats

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

Date d'expiration de l'AC : 03/02/2027 14:51:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

[En savoir plus sur la période de validité](#)

< Précédent Suivant > Configurer Annuler

Configuration des services de certificats Active Directory

Base de données de l'autorité de certification

SERVEUR DE DESTINATION
win-srv2016.test.local

- Informations d'identificati...
- Services de rôle
- Type d'installation
- Type d'AC
- Clé privée
 - Chiffrement
 - Nom de l'AC
 - Période de validité
 - Base de données de certi...**
- Confirmation
- Progression
- Résultats

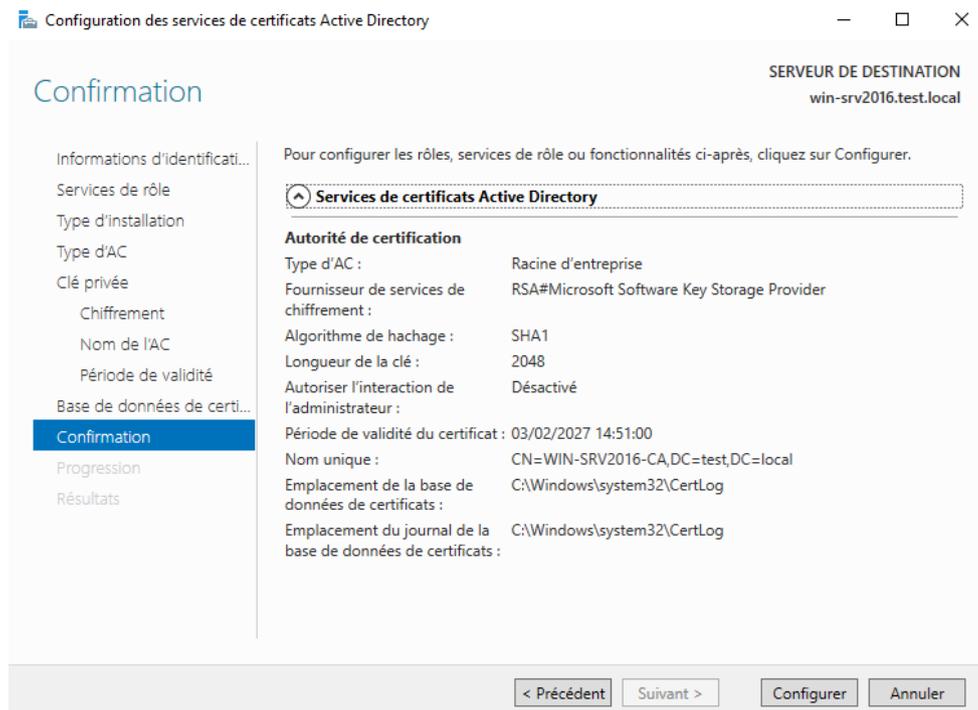
Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

Emplacement du journal de la base de données de certificats :

[En savoir plus sur la base de données de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler



- Maintenant que votre certificat est opérationnel il faut aller dans Outils > NPS et cliquer sur Configurer 802.1X



- Nous voulons configurer une connexion sans fil nous sélectionnons la 1^{ère} option

Configurer 802.1X ×



Sélectionner le type de connexions 802.1X

Type de connexions 802.1X :

Connexions sans fil sécurisées
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.

Connexions câblées (Ethernet) sécurisées
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.

Nom :
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.

- Ajouter un client avec les informations de votre réseau dans notre cas nous l'avons nommé « Reseau Prive » pointant vers l'ip de notre borne wifi

Configurer 802.1X



Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

Reseau Prive	Ajouter...
	Modifier...
	Supprimer

Précédent **Suivant** Terminer Annuler

- Ici sélectionner PEAP pour qu'il puisse sélectionner notre certificat précédemment crée (à noter que si vous possédez 2 certificats il faudra penser à cliquer sur « configurer » pour sélectionner celui souhaiter)

Configurer 802.1X

Configurer une méthode d'authentification

Sélectionnez le type de protocole EAP pour cette stratégie.

Type (basé sur la méthode d'accès et la configuration réseau) :

Microsoft: PEAP (Protected EAP) Configurer...

Précédent Suivant Terminer Annuler

- Ajouter notre groupe d'utilisateurs

Configurer 802.1X ✕



Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur *Ajouter*. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes	
TEST\RadiusUser	

[Ajouter...](#)
[Supprimer](#)

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

- Faites suivant

Configurer 802.1X



Configurer les contrôles du trafic

Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.

Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.

Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.

Configuration du contrôle du trafic

Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.

[Configurer...](#)

[Précédent](#) [Suivant](#) [Terminer](#) [Annuler](#)

Configurer 802.1X



Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS

Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.

- Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
- Pour modifier la configuration, cliquez sur Précédent.
- Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.

Stratégie de demande de connexion :
Connexions sans fil sécurisées 2

Stratégies réseau :
Connexions sans fil sécurisées 2

[Détails de la configuration](#)

Précédent

Suivant

Terminer

Annuler

- Et votre configuration sans fil est maintenant prête

6.3 Paramétrer la borne WIFI

- Une fois tout ça fait il vous faut mettre en place le radius sur la borne wifi
- Editer le ssid reseau prive

Wizard Setting

Step 1

Step 2

Step 3

Step 4

Step 5

SSID

#	Status	SSID	Security Mode	Band Mode	VLAN ID
1	<input checked="" type="checkbox"/>	Reseau Prive	WPA2-Enterprise	Dual Band	1
2	<input checked="" type="checkbox"/>	Reseau Prive Guest	WPA2-Personal	Dual Band	10
3	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1
4	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1
5	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1
6	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1
7	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1
8	<input type="checkbox"/>	Zyxel	WPA2-Personal	Dual Band	1

Prev Next Cancel

Edit SSID Profile

SSID:

Status:

VLAN ID: (1~4094)

Band Mode:

Security Type:

Personal

Enterprise

Primary RADIUS Server

RADIUS Server IP Address:

RADIUS Server Port: (1~65535)

RADIUS Server Secret:

Secondary Radius Server

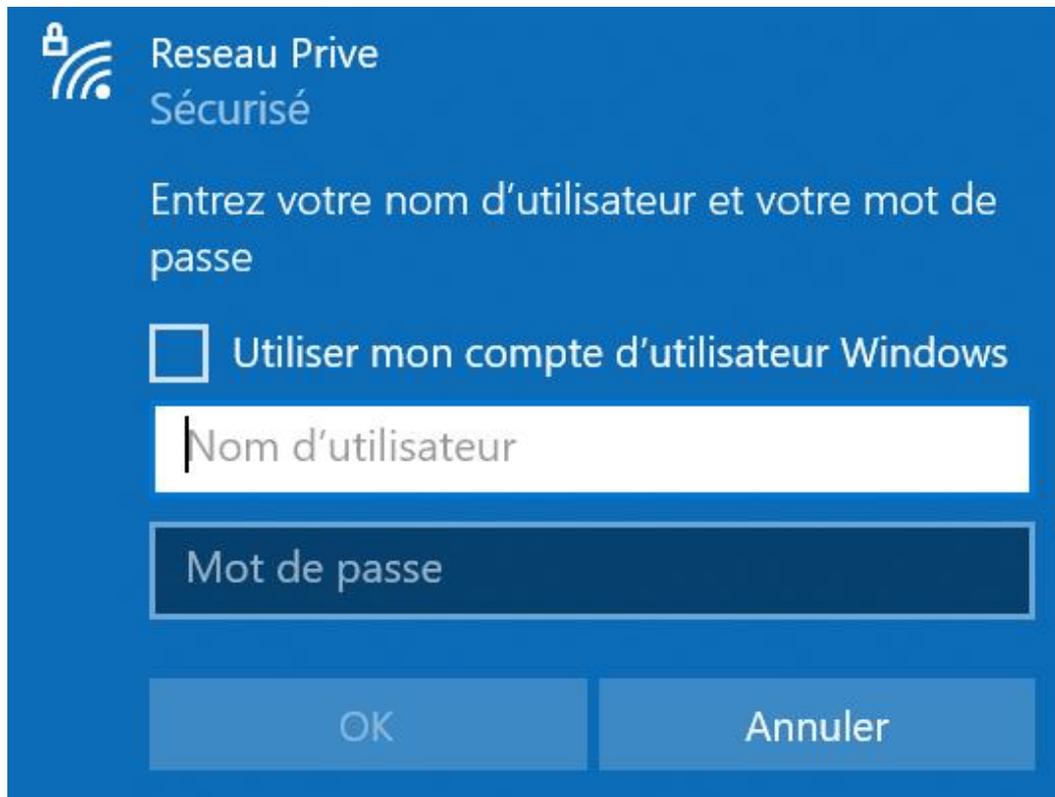
RADIUS Server IP Address:

RADIUS Server Port: (1~65535)

RADIUS Server Secret:

- Enregistrer avec l'ip de votre serveur radius, ici c'est le même que notre serveur ad, radius s'exécute par défaut sur le port 1812 ou 1645 pour l'authentification penser également à renseigner le secret radius (le mot de passe fixer lors de la création de votre client) et maintenant vous pouvez essayer une connexion wifi avec un utilisateur

- Une fois fait, vous pouvez tester l'authentification Radius simplement en renseignant l'utilisateur présent dans l'ad (ici radius1) et le tour est joué



The image shows a Windows network security dialog box with a blue background. At the top left, there is a lock icon and a Wi-Fi signal icon. The text reads "Reseau Prive" and "Sécurisé". Below this, it says "Entrez votre nom d'utilisateur et votre mot de passe". There is a checkbox labeled "Utiliser mon compte d'utilisateur Windows" which is currently unchecked. Below the checkbox are two input fields: "Nom d'utilisateur" and "Mot de passe". At the bottom, there are two buttons: "OK" and "Annuler".



