

# RADIUS

The background of the slide features a dark blue gradient with a subtle, glowing blue wavy pattern that resembles a digital or acoustic waveform. This pattern is composed of small, light blue dots and lines, creating a sense of depth and motion.

Réalisé par

NADZI Issam

NAKAB Mohamed

OUNDA Dimitri-Gaetan

SANOGO Cheickna

Encadré par Pr. Wissam ABBASS

# PLAN

Introduction

Généralités sur Radius

Fonctionnement de Radius

Avantages et limites

Implémentation

Conclusion

# Introduction

RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau développé initialement par Livingston Enterprises en 1991. Standardisé par l'IETF (Internet Engineering Task Force) dans la RFC 2865, il est principalement utilisé pour gérer l'authentification, l'autorisation et la comptabilité (AAA : Authentication, Authorization, Accounting) des utilisateurs accédant à un réseau.



# Fonctionnalités

## Authentification

RADIUS vérifie l'identité des utilisateurs à l'aide de bases de données locales ou externes (LDAP, Active Directory, etc.)

## Autorisation

Il contrôle les droits des utilisateurs en définissant les ressources et les services accessibles

## Comptabilité

RADIUS conserve des traces des activités utilisateur, telles que les durées de session ou l'utilisation des données

# ARCHITECTURE

**Le protocole Radius est basé sur une architecture client-serveur**

## Clients Radius

Généralement un point d'accès réseau (NAS, Network Access Server) ou un équipement réseau (switch, routeur) qui relaye les demandes d'accès utilisateur au serveur RADIUS

## Serveurs Radius

Valide les informations d'identification des utilisateurs en interrogeant une base de données et renvoie une réponse (acceptation ou rejet)

# Protocole et Ports

Radius utilise le protocole UDP et les ports 1812 pour l'authentification et l'autorisation et 1813 pour la comptabilité

# Cas d'utilisation



Contrôle des connexions VPN



Gestion des accès Wi-Fi sécurisés avec 802.1X



Contrôle d'accès dans des environnements multi-sites  
grâce à une gestion centralisée

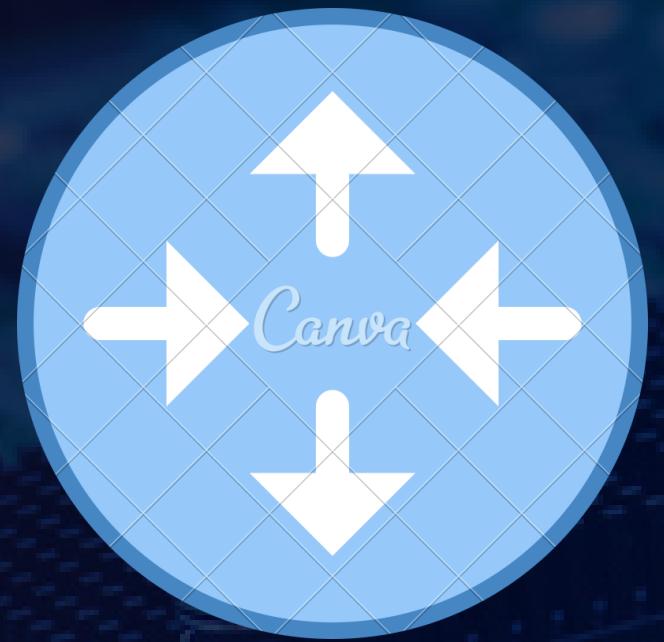
# FONCTIONNEMENT



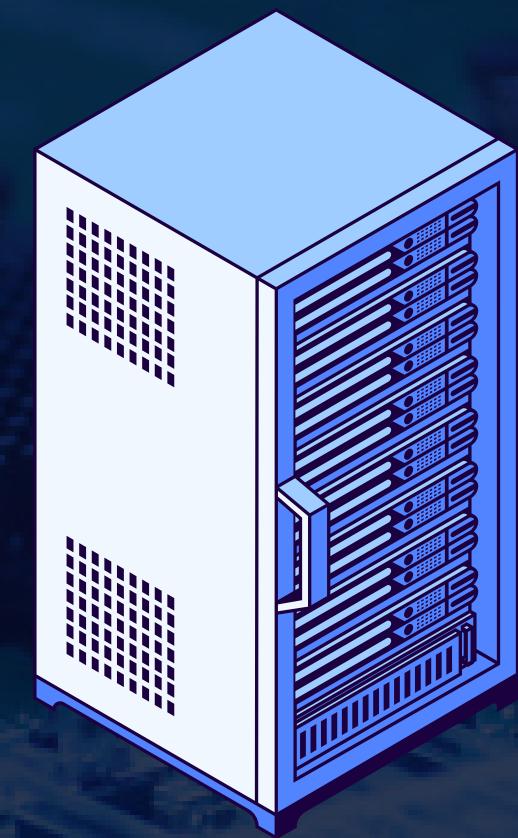
# Authentification



Utilisateur



Client-Radius

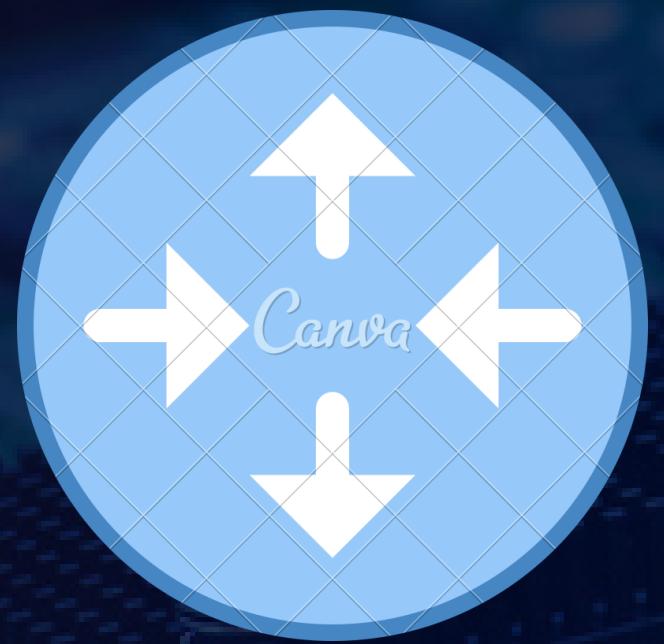


Serveur-Radius

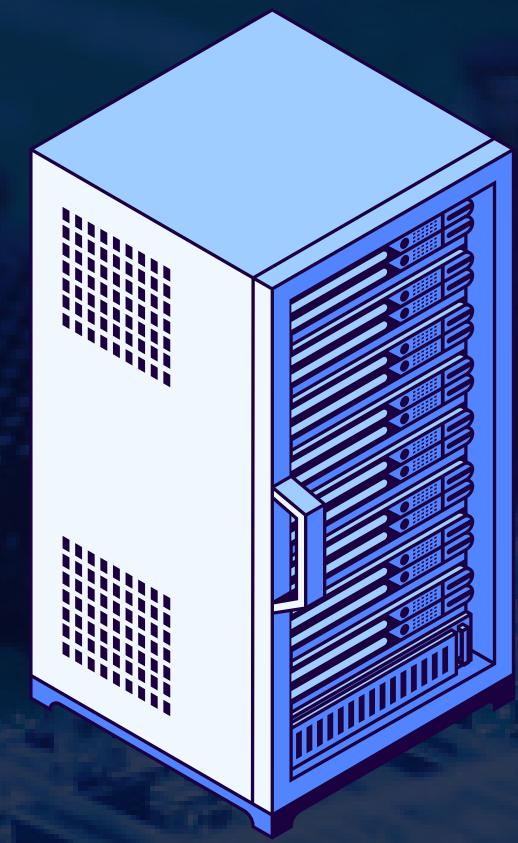
# Authentification



Utilisateur



Client-Radius

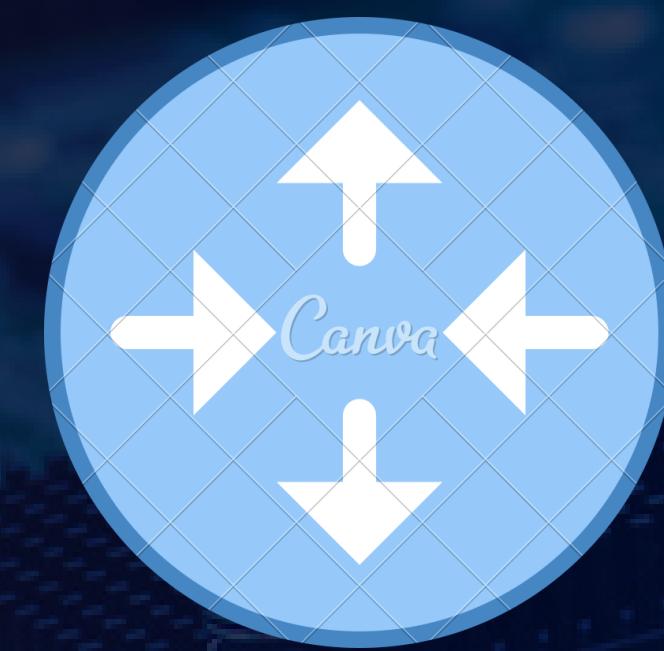


Serveur-Radius

# Authentification



Utilisateur



Client-Radius

Access-Request

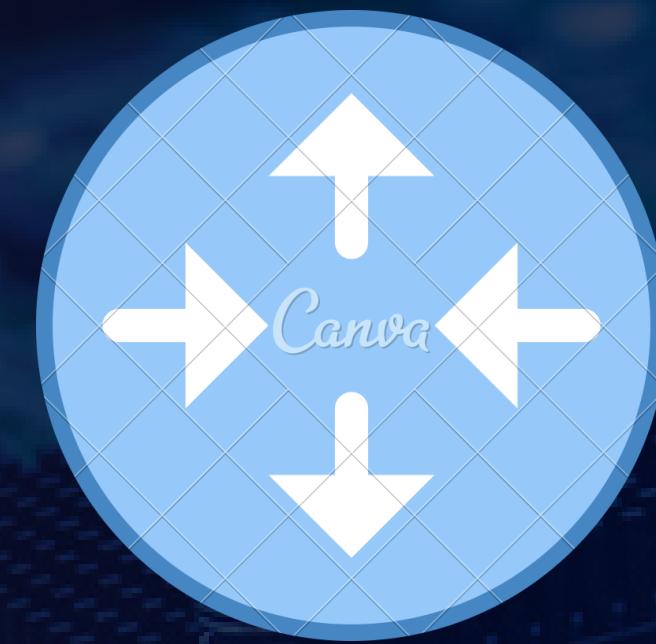


Serveur-Radius

# Authentification

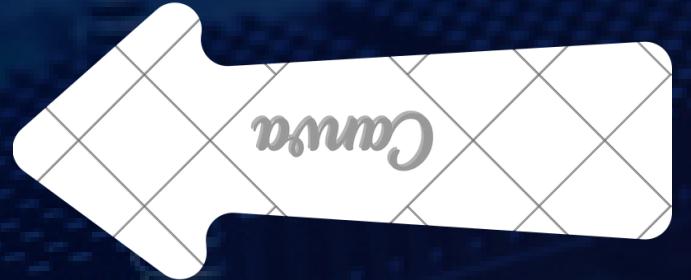


Utilisateur



Client-Radius

Access-Challenge



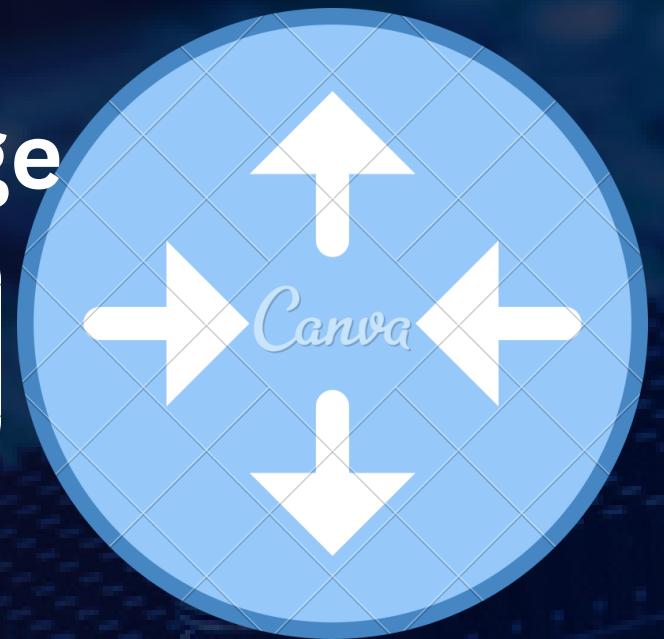
Serveur-Radius

# Authentification



Utilisateur

Access-Challenge



Client-Radius

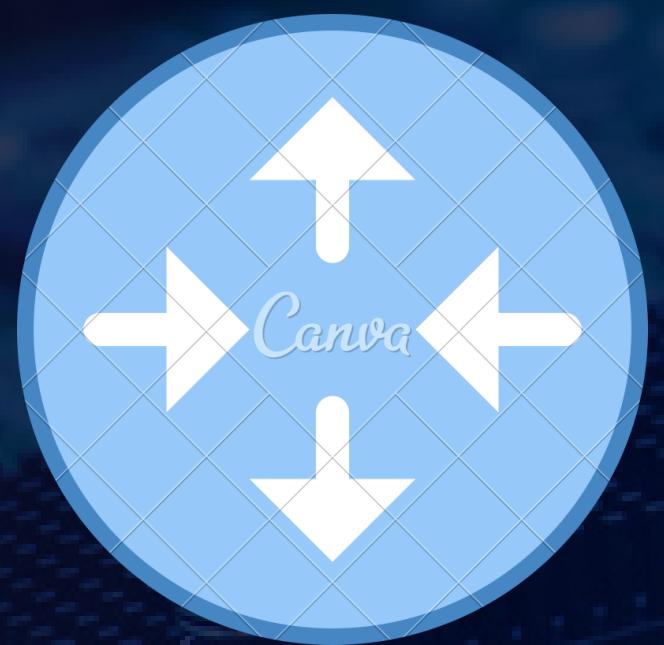


Serveur-Radius

# Authentification



Utilisateur



Client-Radius

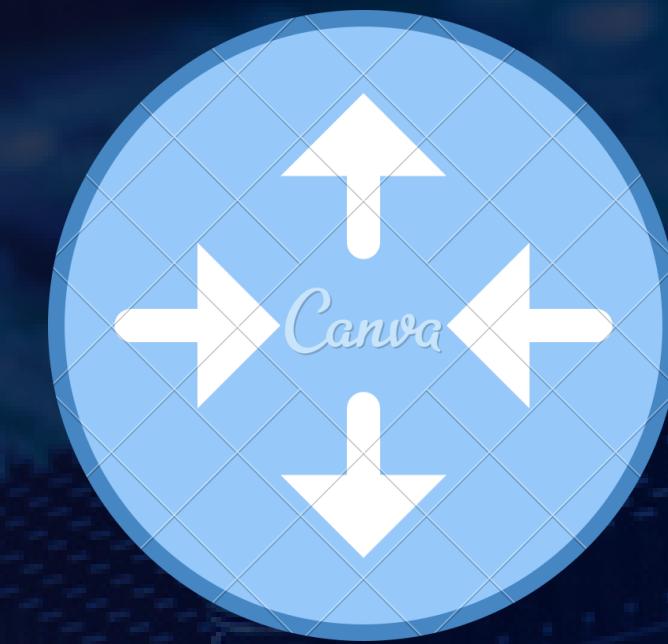


Serveur-Radius

# Authentification



Utilisateur



Client-Radius

Access-Request



Serveur-Radius

# Authentification

Protocoles de Mot de Passe :

PAP

CHAP

User-Password

CHAP-Password

# Authentification

Protocoles de Mot de Passe :

**MS-CHAP**

**MS-CHAP V2**

Par Microsoft

# Autorisation

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0 1	
+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+
Code	Identifier	Length	
+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+
	Response Authenticator		
+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+	+-+-+-+--+--+--+--+--+--+
Attributes ...			
+-+-+-+--+--+--+--+--+--			

# Autorisation

# Autorisation

1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	<b>Framed-IP-Address</b>
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	(unassigned)
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	(unassigned)
22	Framed-Route
23	Framed-IPX-Network

24	State
25	<b>Class</b>
26	Vendor-Specific
27	Session-Timeout
28	<b>Idle-Timeout</b>
29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40-59	(reserved for accounting)
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port

# Comptabilisation

Accounting  
Start



Accounting  
Stop

# Comptabilisation

Accounting  
Start



Accounting  
Stop

# Comptabilisation



# Comptabilisation

Remarque :  
L'accounting a aussi une fonction légale

# Avantages et limites



- Support des mécanismes de contrôle d'accès réseau avancés (NAC)
- Gestion dynamique des VLANs
- Compatibilité

# Avantages

- Compatibilité avec les VPNs
- Support des environnements multisites

# Avantages

# Limites

- Protocole basé sur UDP
- Absence de chiffrement natif pour toutes les données
- Manque de flexibilité pour les architectures modernes

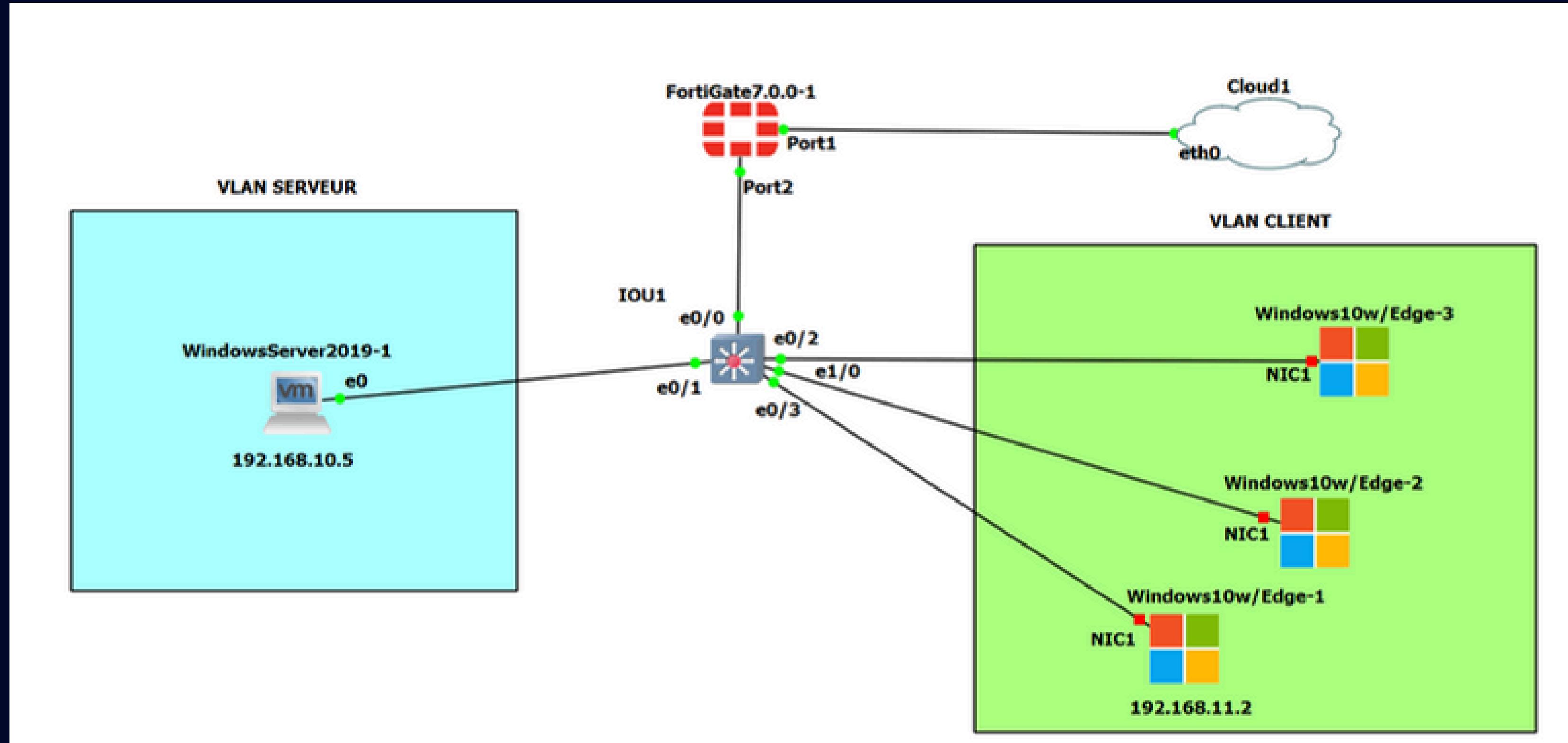
# Limites

- Maintenance coûteuse
- Conformité limitée

# Implementation

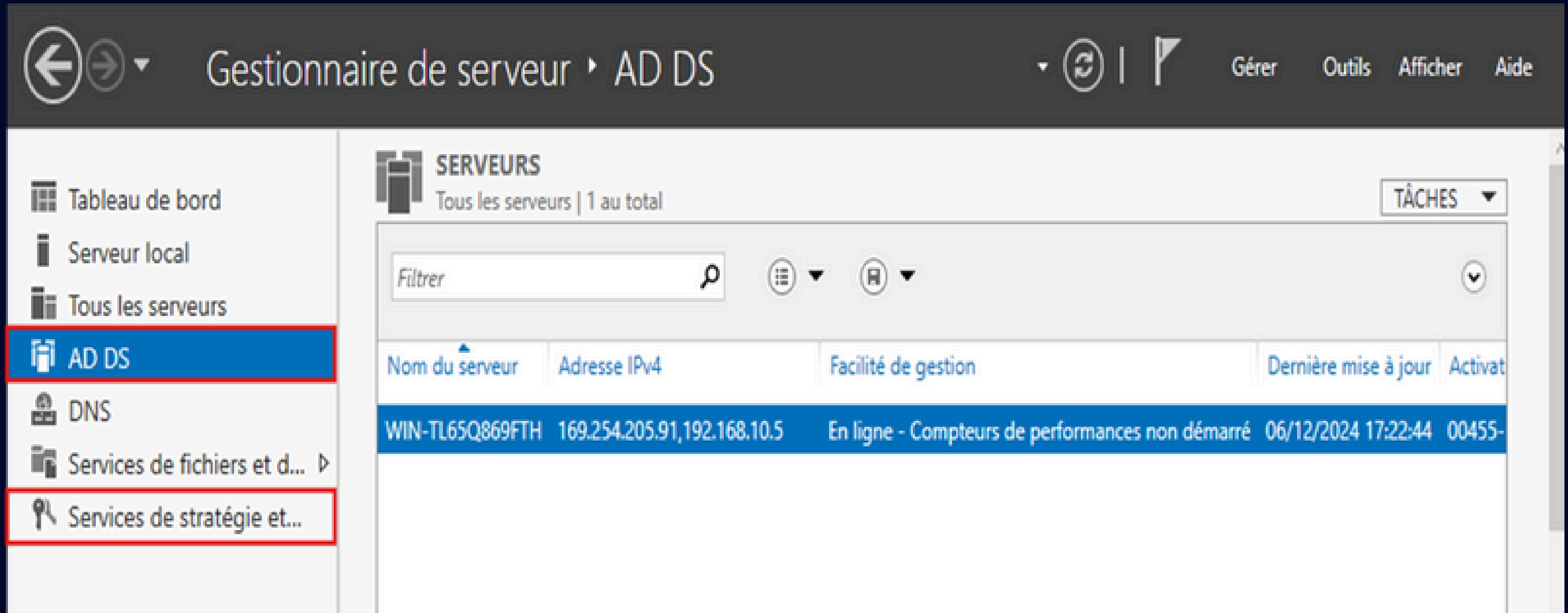


# Architecture



# ETAPES DE CONFIGURATION

## installation ADDS et NPAS (RADIUS)



The screenshot shows the Windows Server Manager interface. The left navigation pane lists several services: Tableau de bord, Serveur local, Tous les serveurs, AD DS, DNS, Services de fichiers et d..., and Services de stratégie et... The 'AD DS' and 'Services de stratégie et...' items are highlighted with red boxes. The main pane displays the 'SERVEURS' section, showing one server: WIN-TL65Q869FTH with IP 169.254.205.91, 192.168.10.5. The server is online and has performance counters not started. The 'TACHES' button is visible in the top right of the main pane.

Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activat
WIN-TL65Q869FTH	169.254.205.91, 192.168.10.5	En ligne - Compteurs de performances non démarré	06/12/2024 17:22:44	00455-

# CRÉATION DES UTILISATEURS FORTIGATE POUR CONFIGURER LE PARFEU

Nouvel objet - Utilisateur

Créer dans : anass.ma/Users

Prénom : Fortigate1

Initiales :

Nom :

Nom complet : Fortigate1

Nom d'ouverture de session de l'utilisateur : For1 @anass.ma

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : ANASS\ For1

< Précédent Suivant > Annuler

Invités du d... Groupe de séc... Tous les invité

Nouvel objet - Utilisateur

Créer dans : anass.ma/Users

Prénom : Fotrigate2

Initiales :

Nom :

Nom complet : Fotrigate2

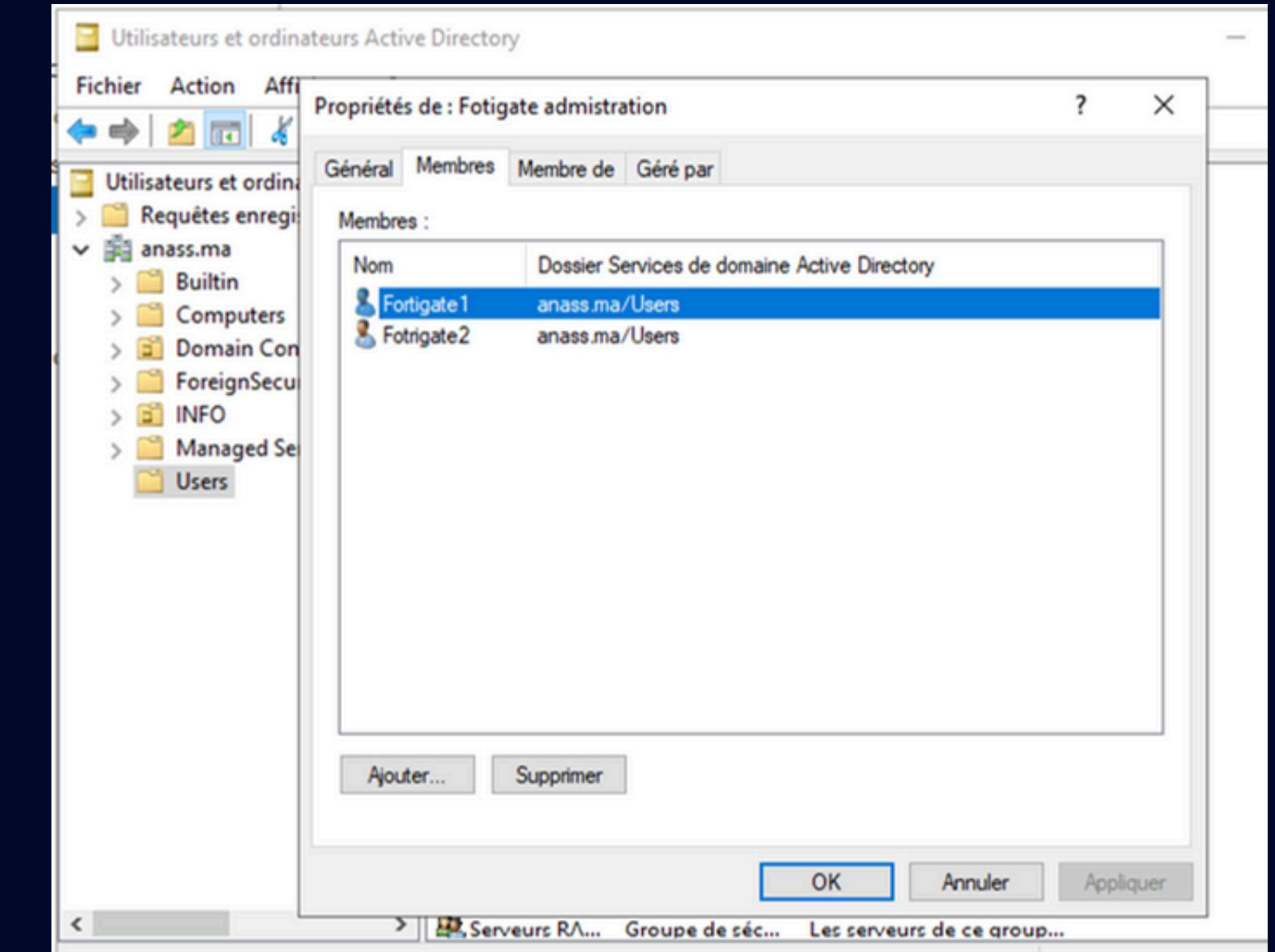
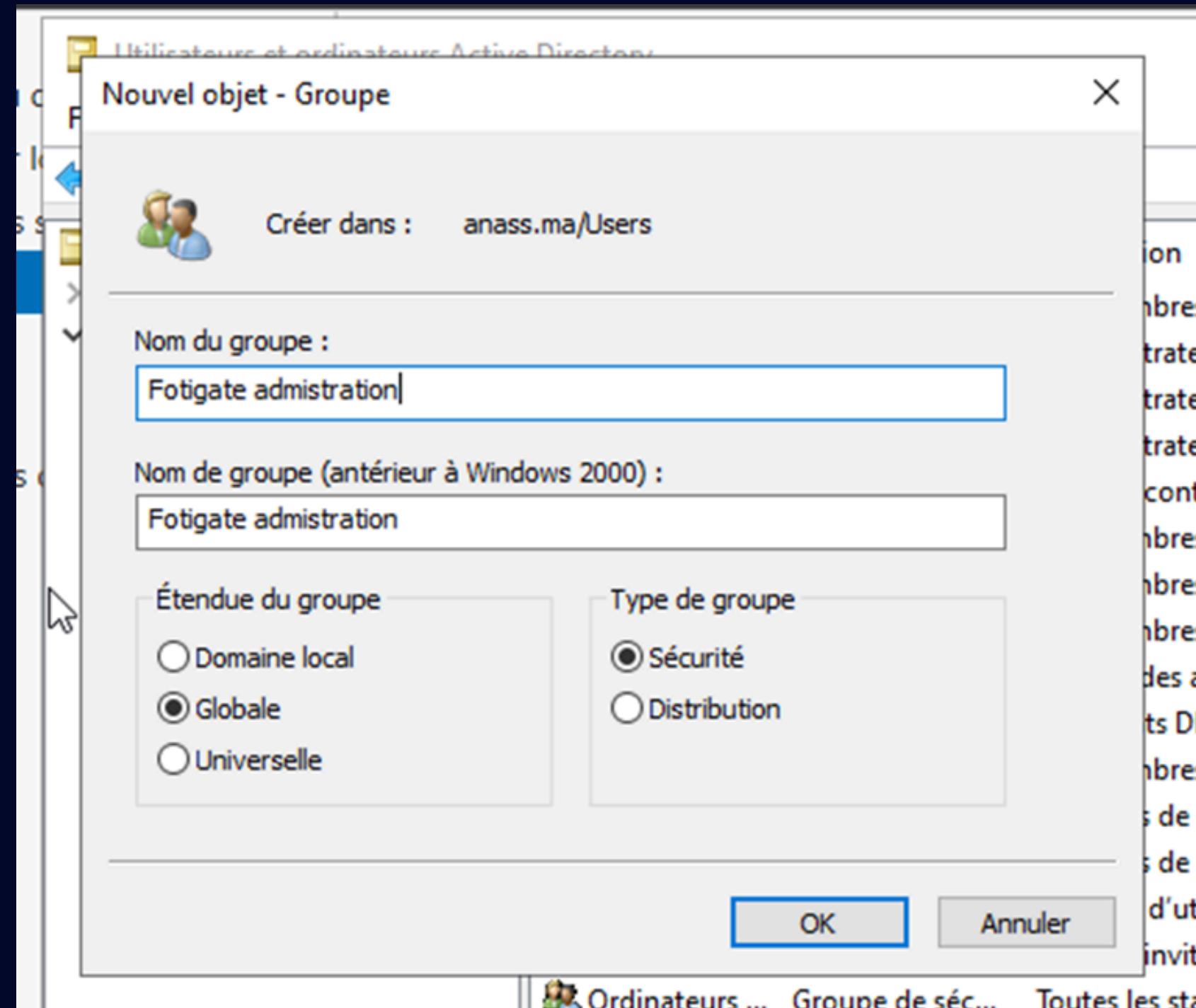
Nom d'ouverture de session de l'utilisateur : For2 @anass.ma

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : ANASS\ For2

< Précédent Suivant > Annuler

Invité Utilisateur Compte d'utilisateur

# CRÉATION DES UTILISATEURS AU SEIN DU GROUPE FORTIGATE ADMINISTRATION



# CONFIGURATION DES VLANS SUR LE SWITCH

```
IOU1#enable
IOU1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IOU1(config)#vlan 10
IOU1(config-vlan)#name VLAN10
IOU1(config-vlan)#vlan 11
IOU1(config-vlan)#name VLAN11
IOU1(config-vlan)#end
```

VLAN 10 : Vlan pour la machine serveur AD

VLAN 11 : VLAN Pour les machine clientes du domaine

# CONFIGURATION DU SWITCH : MODES TRUNK ET ACCESS

## L'interface du switch lié au fortigate

```
IOU1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IOU1(config)#int e0/2
IOU1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
IOU1(config-if)#switchport trunk encapsulation dot1q
                                ^
% Invalid input detected at '^' marker.

IOU1(config-if)#switchport trunk encapsulation dot1q
IOU1(config-if)#
*Nov 29 09:07:24.915: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
IOU1(config-if)#switchport trunk encapsulation dot1q
*Nov 29 09:07:27.921: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
IOU1(config-if)#switchport mode trunk
IOU1(config-if)#
*Nov 29 09:07:33.628: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
IOU1(config-if)#switchport mode trunk
*Nov 29 09:07:36.636: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
IOU1(config-if)#switchport trunk allowed vlan 10,11
```

## Les interfaces du switch lié aux machines clientes

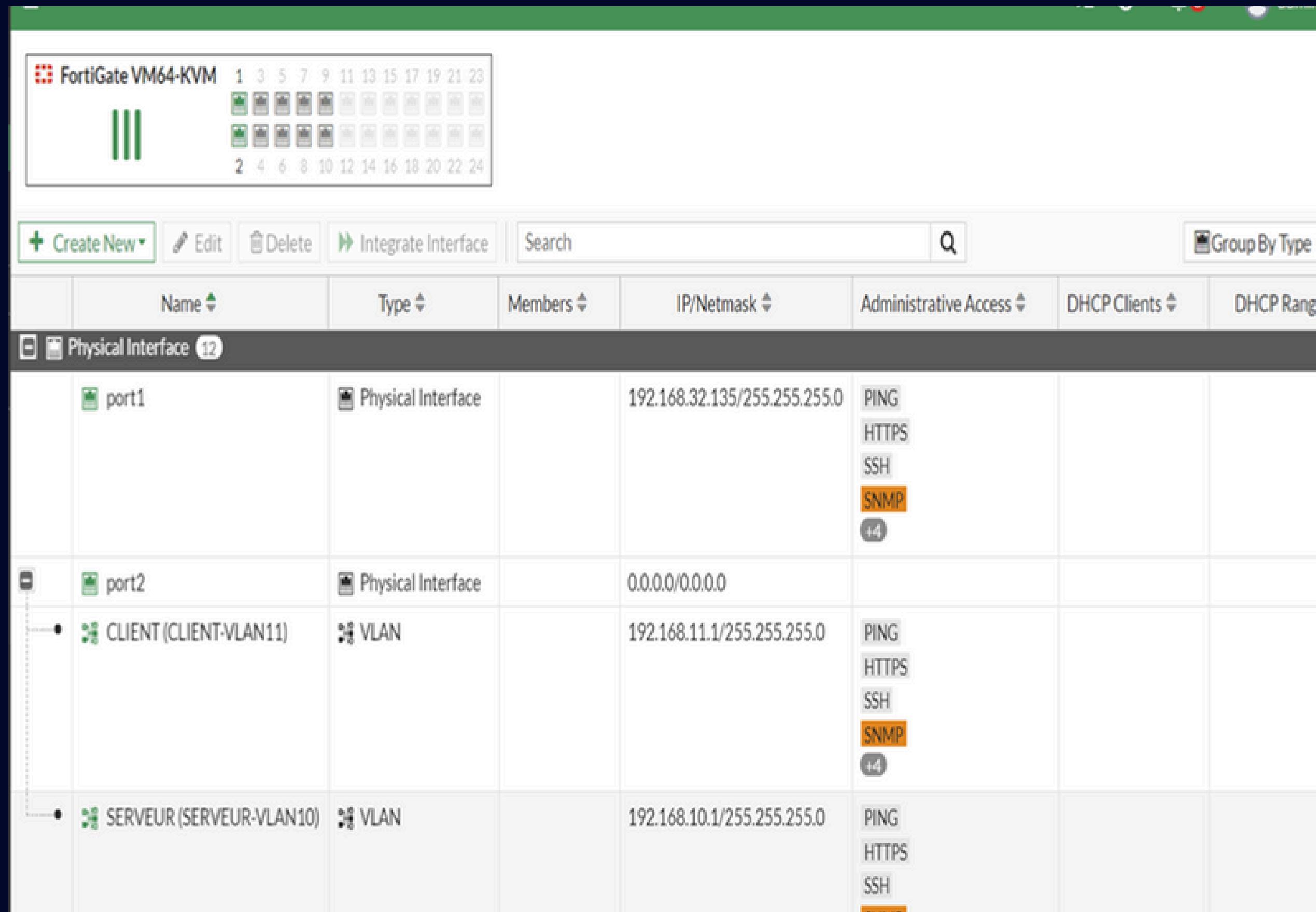
```
IOU1(config-if)#exit
IOU1(config)#int e0/0
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 10
IOU1(config-if)#exit
IOU1(config)#int e0/1
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport access vlan 11
IOU1(config-if)#no shutdown
IOU1(config-if)#exit
IOU1(config)#int e0/0
IOU1(config-if)#no shutdown
IOU1(config-if)#exit
```

# VÉRIFICATION DES VLANS CRÉÉS

```
IOU1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/3, Et1/0, Et1/1, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
10	VLAN10	active	Et0/0
11	VLAN11	active	Et0/1
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdдинet-default	act/unsup	
1005	trnet-default	act/unsup	

# CONFIGURATION DU FORTIGATE : GESTION DES VLANS



The screenshot shows the FortiGate management interface for VLAN configuration. The top navigation bar includes the device name "FortiGate VM64-KVM", a list of 24 ports (1-24), and various configuration buttons: "Create New", "Edit", "Delete", "Integrate Interface", "Search", and "Group By Type".

The main table displays VLAN configurations:

	Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
	port1	Physical Interface		192.168.32.135/255.255.255.0	PING HTTPS SSH SNMP +4		
	port2	Physical Interface		0.0.0.0/0.0.0.0			
•	CLIENT (CLIENT-VLAN11)	VLAN		192.168.11.1/255.255.255.0	PING HTTPS SSH SNMP +4		
•	SERVEUR (SERVEUR-VLAN10)	VLAN		192.168.10.1/255.255.255.0	PING HTTPS SSH SNMP		

# CONFIGURATION DU FORTIGATE : ROUTAGE INTER-VLAN ENTRE VLAN 11 ET VLAN 10

# VÉRIFICATION DE LA CONNECTIVITÉ ENTRE LES APPAREILS

PING Fortigate vers Server :

```
FortiGate-VM64-KVM # execute ping 192.168.10.5
PING 192.168.10.5 (192.168.10.5): 56 data bytes
64 bytes from 192.168.10.5: icmp_seq=0 ttl=128 time=2.9 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 192.168.10.5: icmp_seq=1 ttl=128 time=1.9 ms
64 bytes from 192.168.10.5: icmp_seq=2 ttl=128 time=2.3 ms
64 bytes from 192.168.10.5: icmp_seq=3 ttl=128 time=2.6 ms
^C
--- 192.168.10.5 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.9/2.4/2.9 ms
```

# VÉRIFICATION DE LA CONNECTIVITÉ ENTRE LES APPAREILS

PING Server vers Fortigate :

```
C:\Users\Administrateur>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.10.1 : octets=32 temps=10 ms TTL=255

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 10ms, Moyenne = 4ms
Ctrl+C
^C
C:\Users\Administrateur>
```

## PING Client vers Fortigate :

```
C:\Users\Anas>ping 192.168.11.1

Envoi d'une requête 'Ping' 192.168.11.1 avec 32 octets de données :
Réponse de 192.168.11.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.11.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.11.1 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.11.1 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 192.168.11.1:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 2ms, Maximum = 4ms, Moyenne = 2ms
```

## PING Fortigate vers Client :

```
FortiGate-VM64-KVM # execute ping 192.168.11.2
PING 192.168.11.2 (192.168.11.2): 56 data bytes
64 bytes from 192.168.11.2: icmp_seq=0 ttl=128 time=3.6 ms
64 bytes from 192.168.11.2: icmp_seq=1 ttl=128 time=2.3 ms
64 bytes from 192.168.11.2: icmp_seq=2 ttl=128 time=1.1 ms
64 bytes from 192.168.11.2: icmp_seq=3 ttl=128 time=3.1 ms
64 bytes from 192.168.11.2: icmp_seq=4 ttl=128 time=1.8 ms

--- 192.168.11.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/2.3/3.6 ms
```

## PING Client vers Server :

```
C:\Users\Anas>ping 192.168.10.5

Envoi d'une requête 'Ping' 192.168.10.5 avec 32 octets de données :
Réponse de 192.168.10.5 : octets=32 temps=5 ms TTL=127
Réponse de 192.168.10.5 : octets=32 temps=7 ms TTL=127
Réponse de 192.168.10.5 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 192.168.10.5:
  Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 5ms, Maximum = 7ms, Moyenne = 5ms
```

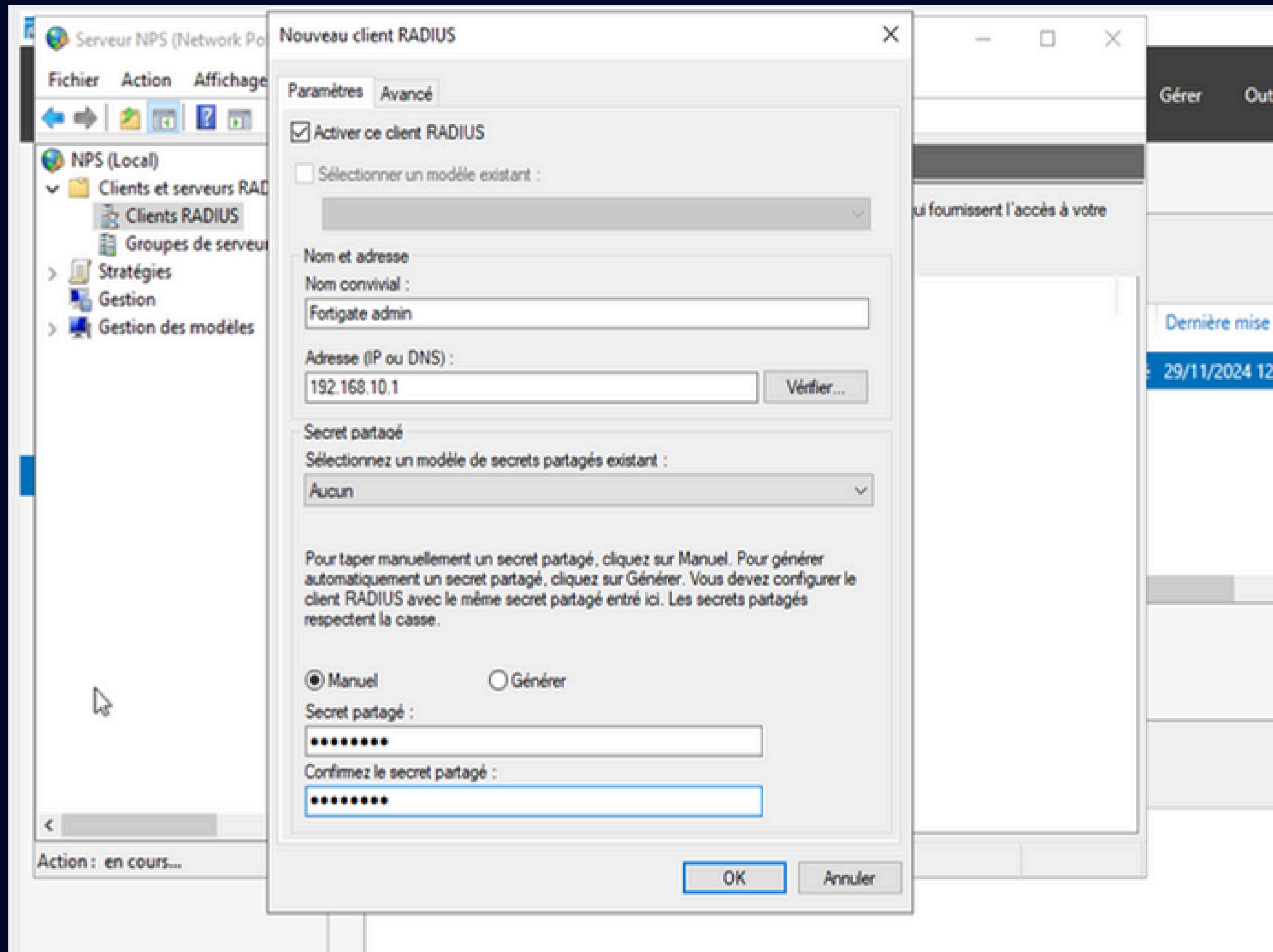
## PING SERVER VERS CLIENT :

```
C:\Users\Administrateur>ping 192.168.11.2

Envoi d'une requête 'Ping' 192.168.11.2 avec 32 octets de données :
Réponse de 192.168.11.2 : octets=32 temps=6 ms TTL=127
Réponse de 192.168.11.2 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.11.2 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 192.168.11.2:
  Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 3ms, Maximum = 6ms, Moyenne = 4ms
```

# CONFIGURATION DE RADIUS : AJOUT DU CLIENT RADIUS



# CONFIGURATION DE RADIUS : CONFIGURATION DES MÉTHODES D'AUTHENTIFICATION

Nouvelle stratégie réseau

## Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

**Types de protocoles EAP :**

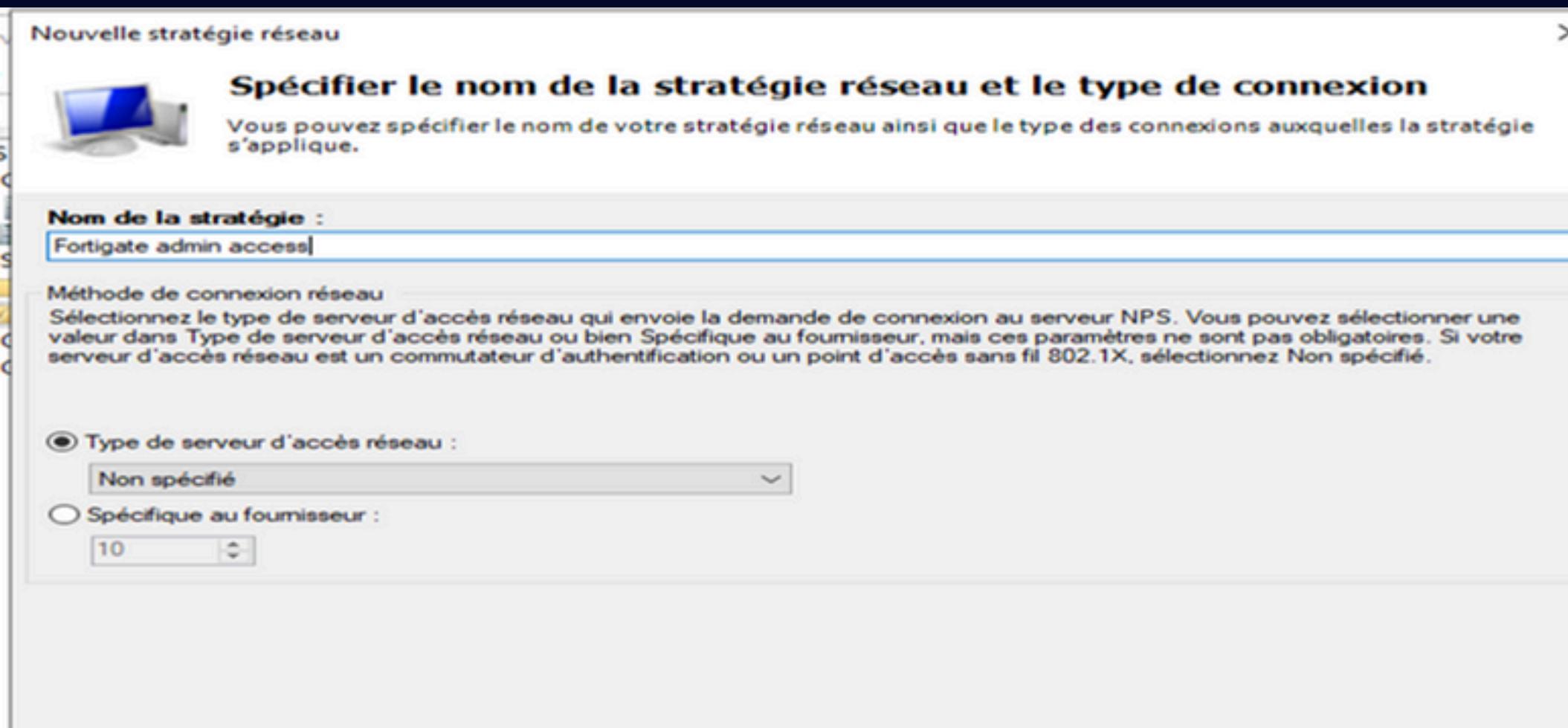
Monter      Descendre

**Méthodes d'authentification moins sécurisées :**

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
  - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
  - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

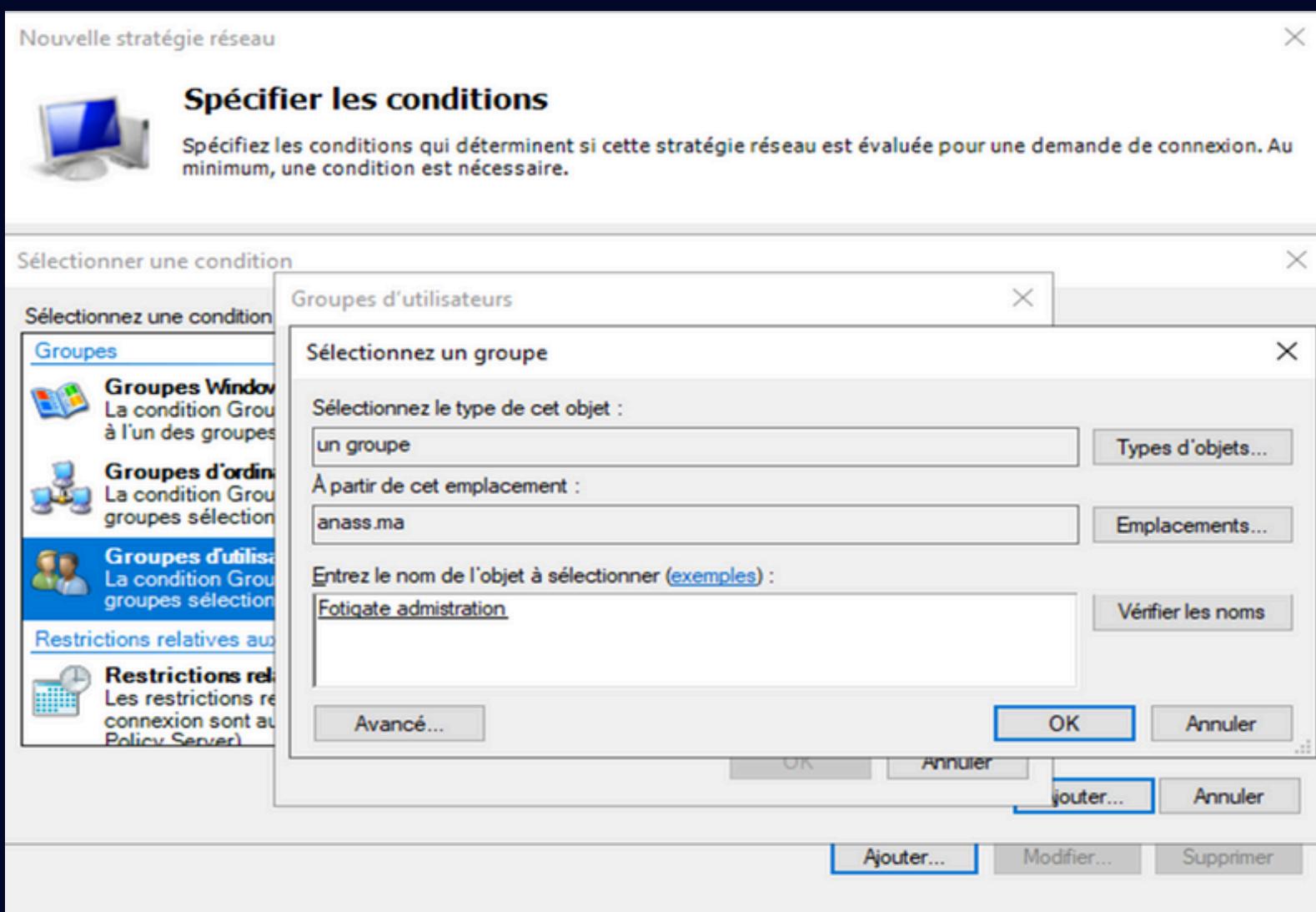
Précédent      **Suivant**      Terminer      Annuler

# POLITIQUE DU CLIENT RADIUS



Création d'une politique pour les admins fortigate

Ajout du groupe d'admins fortigate



# POLITIQUE DU CLIENT RADIUS : CONTRAINTES

Nouvelle stratégie réseau

## Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

Configurez les contraintes de cette stratégie réseau.  
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Délai d'inactivité**
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

Déconnecter au-delà de la durée d'inactivité maximale

15

Définition de 15 min d'inactivité pour se déconnecter de la session

Nouvelle stratégie réseau

## Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

Configurez les contraintes de cette stratégie réseau.  
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Délai d'inactivité**
- Délai d'expiration de session**
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

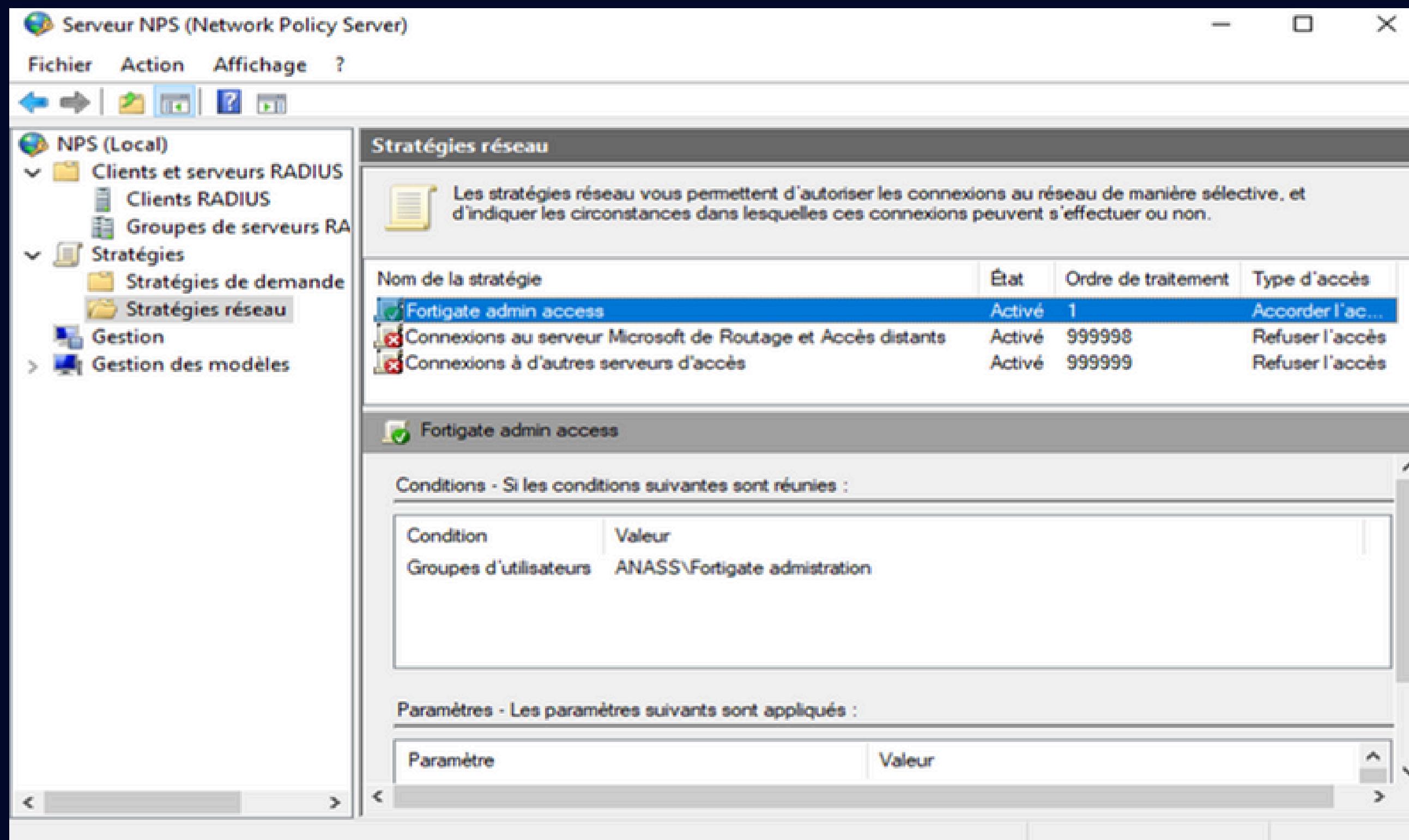
Spécifiez le délai de connexion maximal (en minutes) d'un utilisateur.

Déconnecter au-delà de la durée de session maximale suivante :

120

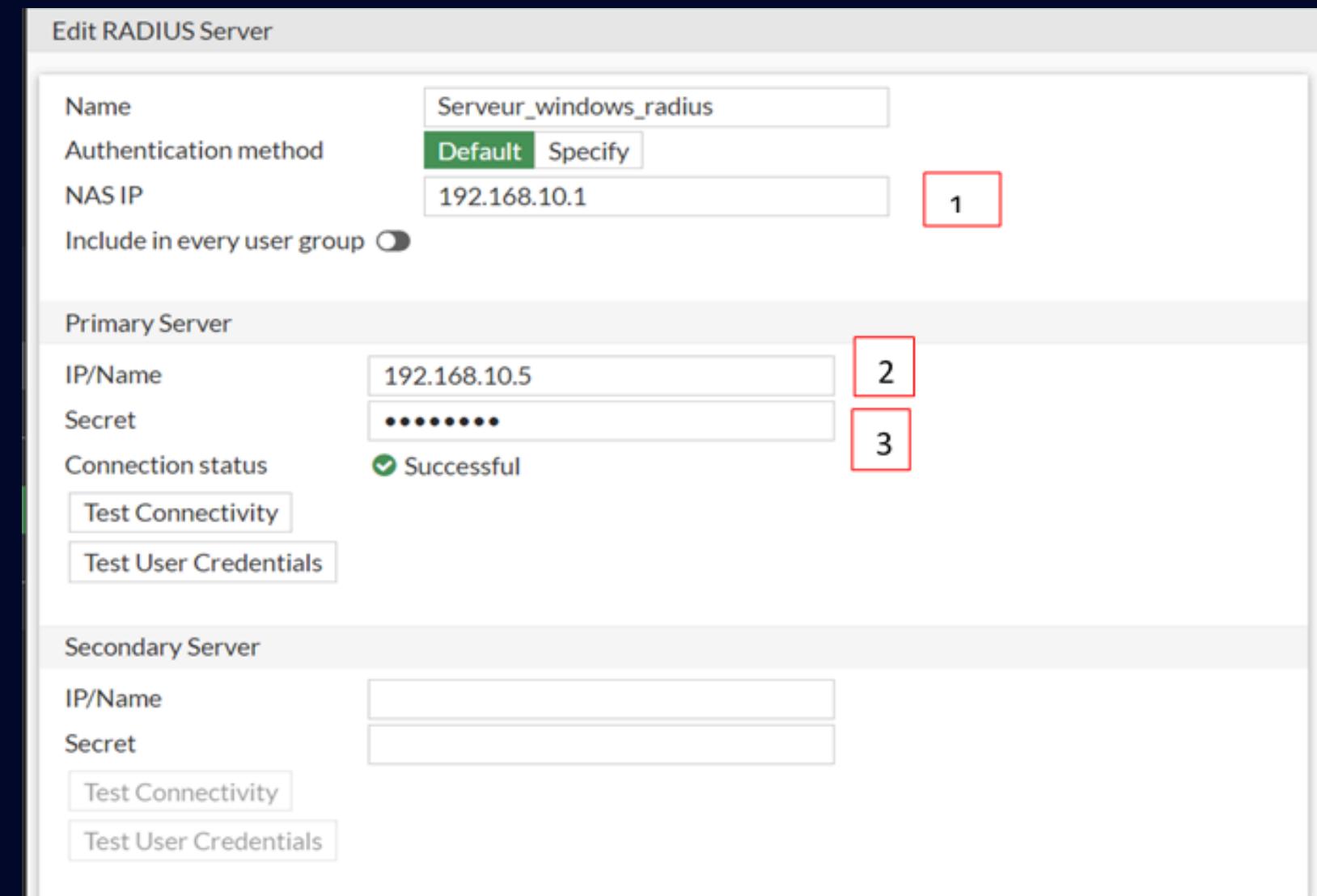
Définition de 2 heure comme temps de la session au au-delà on doit reconnecter

# POLITIQUE DU CLIENT RADIUS .



la politique a été bien créée

# CONFIGURATION DU FORTIGATE : LIAISON DU CLIENT RADIUS AVEC FORTIGATE



- 1- l'adresse IP du Fortigate utilisée pour communiquer avec le serveur RADIUS.
- 2- l'adresse IP du serveur radius principale utilisé
- 3- clé secrète partagé entre le serveur et fortigate

# VÉRIFICATION DE L'EXISTENCE DES UTILISATEURS DANS FORTIGATE

Username

Password

Connection status ✓ Successful

User credentials ✓ Successful

Server message

```
AVP: l=6 t=Framed-Protocol(7)
  Value: 1
AVP: l=6 t=Idle-Timeout(28)
  Value: 900
AVP: l=6 t=Service-Type(6)
  Value: 2
AVP: l=6 t=Session-Timeout(27)
  Value: 7200
AVP: l=46 t=Class(25)
  Value: 96 70 07 d0 00 00 01 37 00 01 02 00 c0 a8 0a 05
  00 00 00 15 12 72 72 aa 1f ac 1a 01 db 44 d9 0c dc 58
  46 00 00 00 00 00 00 04
AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
  VSA: l=36 t=MS-MPPE-Recv-Key(17)
    Value: 80 01 1c 44 ea 3a da ea ec df 9f 62 aa 64 e1 5f
    57 43 c1 07 e0 38 58 7a d8 07 e5 6d d1 2c db 23 0c 80
  i AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
    VSA: l=36 t=MS-MPPE-Send-Key(16)
    Value: 80 02 50 1f 68 f3 b3 f0 48 e3 0d 82 5f e0 42 39
    7e 49 cc 1f 45 62 37 6a b7 a2 0c 3e 3d 06 c0 1f 28 f0
```

Username

Password

Connection status ✓ Successful

User credentials ✓ Successful

Server message

```
AVP: l=6 t=Framed-Protocol(7)
  Value: 1
AVP: l=6 t=Idle-Timeout(28)
  Value: 900
AVP: l=6 t=Service-Type(6)
  Value: 2
AVP: l=6 t=Session-Timeout(27)
  Value: 7200
AVP: l=46 t=Class(25)
  Value: 96 72 07 d2 00 00 01 37 00 01 02 00 c0 a8 0a 05
  00 00 00 15 12 72 72 aa 1f ac 1a 01 db 44 d9 0c dc 58
  46 00 00 00 00 00 00 06
AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
  VSA: l=36 t=MS-MPPE-Recv-Key(17)
    Value: 80 03 b7 01 93 8a 11 ca 65 24 ea ae b6 06 66 22
    2f 86 aa 1d 76 ce cb bd 5f 61 b9 eb 6a 44 0f e1 db 45
  i AVP: l=42 t=Vendor-Specific(26) v=Microsoft(311)
    VSA: l=36 t=MS-MPPE-Send-Key(16)
    Value: 80 04 47 3e 26 20 d1 19 5d 80 a0 a5 e8 aa b0 98
    41 59 9d b8 25 41 ec 52 46 9a e9 df e6 91 d2 7a 66 55
```

# CRÉATION D'UN GROUPE D'UTILISATEURS SUR FORTIGATE

New User Group

Name	Authentification Radius
Type	Firewall
	Fortinet Single Sign-On (FSSO)
	RADIUS Single Sign-On (RSSO)
	Guest
Members	<input type="text"/> +

Remote Groups

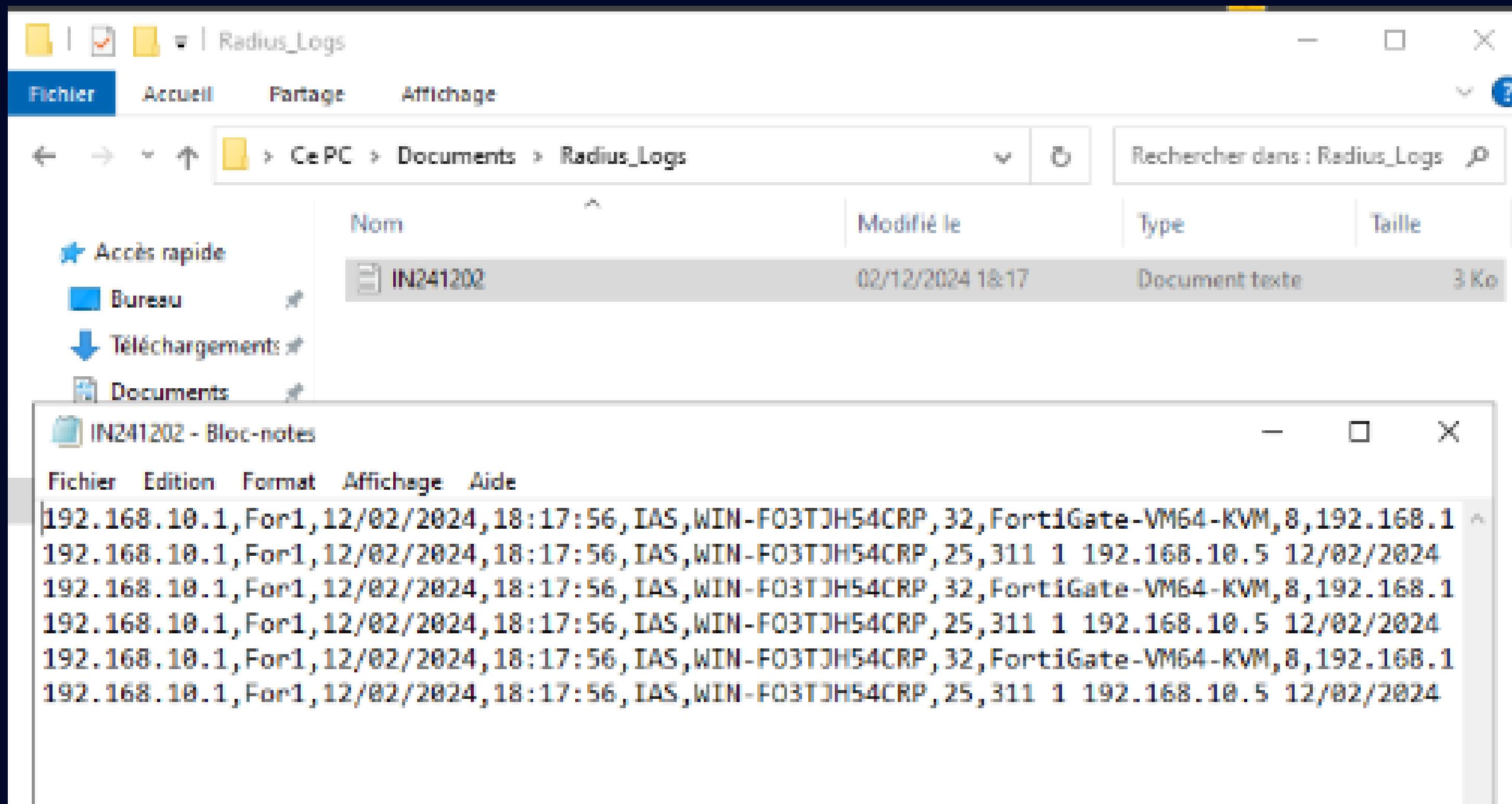
+ Add		Edit	Delete
Remote Server	Group Name		
Serveur_windows_radius			

# AJOUT DE NOUVEAUX ADMINISTRATEURS FORTIGATE

New Administrator

Username	Serveur Radius
Type	<input type="button" value="Local User"/> <input type="button" value="Match a user on a remote server group"/> <input checked="" type="button" value="Match all users in a remote server group"/> <input type="button" value="Use public key infrastructure (PKI) group"/>
Comments	Write a comment... 0/255
Administrator profile	super_admin
Remote User Group	<input type="button" value="Authentification Radius"/>
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
<input type="checkbox"/> Restrict login to trusted hosts	
<input type="checkbox"/> Restrict admin to guest account provisioning only	

# VERIFICATION DES FICHIERS LOGS DANS LE SERVEUR RADIUS



# CONCLUSION

THANK



YOU

RFC 2865 <https://datatracker.ietf.org/doc/html/rfc2865#section-4.1>

RFC 2566 <https://datatracker.ietf.org/doc/html/rfc2566>

RFC 3579 <https://www.rfc-editor.org/rfc/rfc3579#section-3.3>