

Installation des serveurs VPN & RADIUS sur Windows Serveur

Rédaction : Barkia Néhémie | Création : Logan Blachere

Prérequis :

- Un Windows serveur (Pour le VPN)
 - Un serveur RADIUS
 - Serveur VPN
 - Deux cartes réseau
- Un serveur Windows Serveur (Services autre)
 - Active directory
 - Un groupe d'utilisateurs à autoriser sur le serveur RADIUS
 - Étendue DHCP dédié aux utilisateurs distant

Installation du serveur RADIUS :

Premièrement nous allons installé le rôle "**Accès à Distance**" avec le service de rôle "**Direct Access et VPN**". Puis nous allons utiliser le gestionnaire NPS (Network Policy Server) pour configurer le serveur.

Nous allons cliquer une connexion VPN ou d'accès à distance :



Puis, nous allons sélectionner "**Connexions de réseau privé virtuel**" :



Sélectionner le type de connexions d'accès à distance ou de réseau privé virtuel (VPN)

Type de connexions :

Connexions d'accès à distance

Lorsque vous déployez des serveurs d'accès à distance sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients d'accès à distance qui se connectent via ces serveurs.

Connexions de réseau privé virtuel (VPN)

Lorsque vous déployez des serveurs VPN sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients VPN qui se connectent via ces serveurs.

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.

Précédent

Suivant

Terminer

Annuler

Puis, nous spécifions le **client RADIUS** :



Spécifier un serveur d'accès à distance ou VPN

Les clients RADIUS sont des serveurs d'accès réseau et non des ordinateurs clients. Si l'ordinateur local exécute le service Routage et accès à distance en tant que serveur VPN, il est automatiquement ajouté à la liste des clients RADIUS ci-dessous.

Si vous souhaitez ajouter des serveurs VPN en tant que clients RADIUS, cliquez sur Ajouter.

Clients RADIUS :

--

Nous allons préciser les informations détaillées du client RADIUS en spécifiant son nom, **son adresse IP, et un secret (mot de passe)** :

Nouveau client RADIUS

Paramètres

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :
test

Adresse (IP ou DNS) :
192.168.1.2 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :
Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

Secret partagé :
.....

Confirmez le secret partagé :
.....

OK Annuler

Nous pouvons désormais passer aux étapes suivantes.



Spécifier un serveur d'accès à distance ou VPN

Les clients RADIUS sont des serveurs d'accès réseau et non des ordinateurs clients. Si l'ordinateur local exécute le service Routage et accès à distance en tant que serveur VPN, il est automatiquement ajouté à la liste des clients RADIUS ci-dessous.

Si vous souhaitez ajouter des serveurs VPN en tant que clients RADIUS, cliquez sur Ajouter.

Clients RADIUS :

test

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Configuration des méthodes d'authentification :



Configurer les méthodes d'authentification

Les protocoles suivants sont pris en charge par les serveurs qui exécutent le service Routage et accès à distance de Microsoft. Si vous utilisez un autre serveur d'accès à distance, assurez-vous que les protocoles sélectionnés sont pris en charge par ce serveur.

Protocole EAP (Extensible Authentication Protocol)

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

Microsoft: PEAP (Protected EAP) ▼

Configurer...

Authentification chiffrée Microsoft version 2 (MS-CHAPv2)

Sélectionnez cette option pour autoriser vos utilisateurs à spécifier un mot de passe d'authentification.

Authentification chiffrée Microsoft (MS-CHAP)

Sélectionnez cette option uniquement si votre réseau exécute des systèmes d'exploitation qui ne prennent pas en charge MS-CHAPv2.

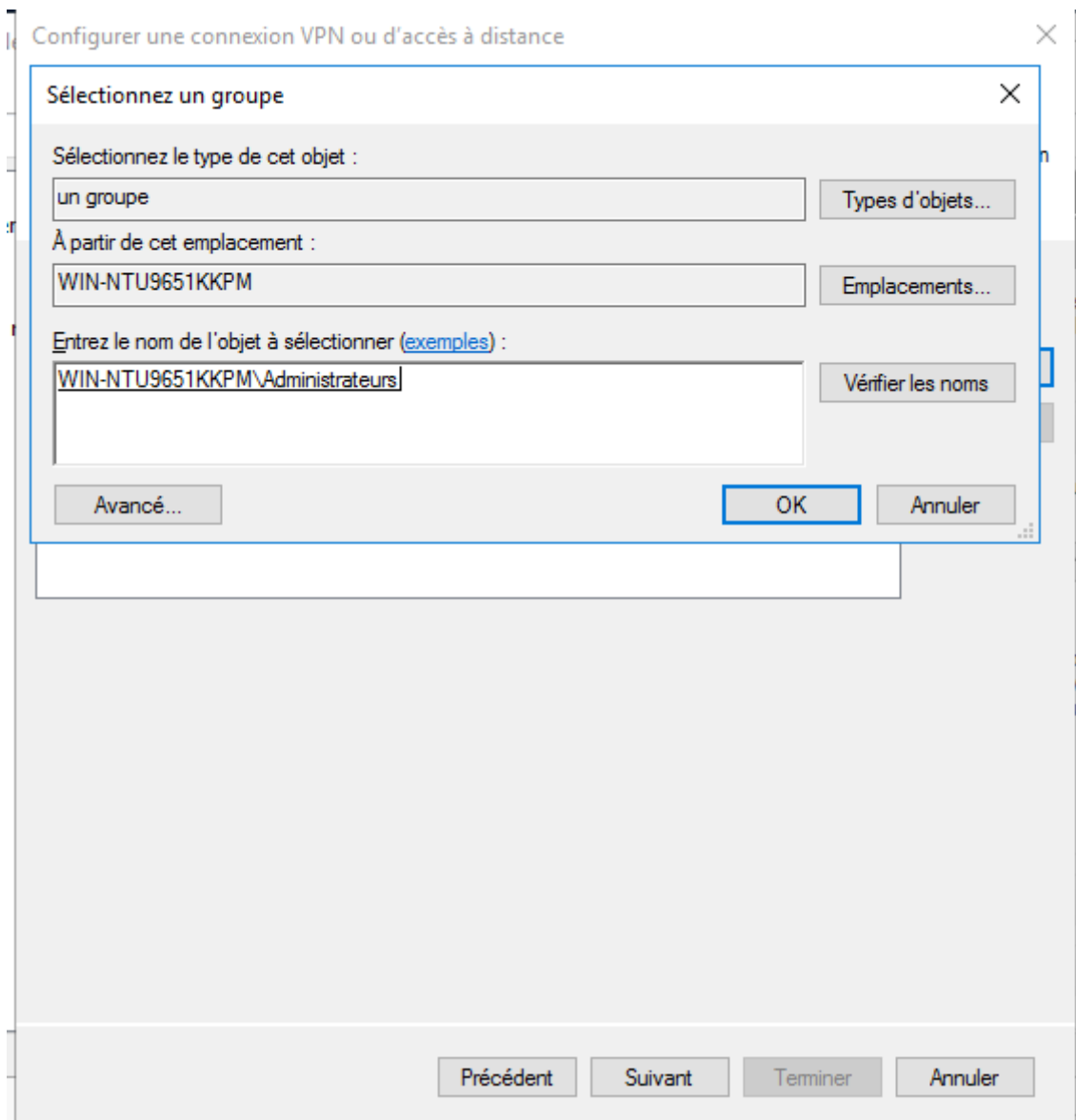
Précédent

Suivant

Terminer


Annuler

Ajout du groupe d'utilisateurs qui sera **autorisé à utiliser le VPN** :



Ici, vous pouvez définir des filtres IP (**optionnel mais important vis à vis de la cyber sécurité**) :

Configurer une connexion VPN ou d'accès à distance ×



Spécifier des filtres IP

Configurez des filtres de paquets IPv4 et IPv6 si vous souhaitez restreindre le type de trafic réseau envoyé et reçu.

Si vous utilisez le service Routage et accès à distance dans le cadre d'un serveur d'accès à distance ou VPN, vous pouvez configurer les filtres d'entrée/de sortie IPv4 et IPv6. Dans le cas contraire, cliquez sur Suivant.

Sélectionner un modèle de filtre IP existant :

Aucun ▼

IPv4

Pour contrôler les paquets IPv4 que cette interface envoie, cliquez sur Filtres d'entrée... Filtres d'entrée...

Pour contrôler les paquets IPv4 que cette interface reçoit, cliquez sur Filtres de sortie... Filtres de sortie...

IPv6

Pour contrôler les paquets IPv6 que cette interface envoie, cliquez sur Filtres d'entrée... Filtres d'entrée...

Pour contrôler les paquets IPv6 que cette interface reçoit, cliquez sur Filtres de sortie... Filtres de sortie...

PrécédentSuivantTerminerAnnuler

Nous laissons, par la suite, par défaut, la spécification des paramètres de chiffrement :



Spécifier les paramètres de chiffrement

Spécifiez les niveaux de chiffrement autorisés pour le trafic entre les clients d'accès à distance et le serveur d'accès réseau.

Si vous utilisez le service Routage et accès à distance dans le cadre d'un serveur d'accès à distance ou VPN, vous pouvez configurer le niveau de chiffrement.

Les paramètres de chiffrement sont pris en charge par les ordinateurs qui exécutent le service Routage et accès à distance Microsoft.

Si vous utilisez différents serveurs d'accès réseau pour les connexions à distance ou VPN, assurez-vous que les paramètres de chiffrement que vous sélectionnez sont pris en charge par vos serveurs.

Si la seule option sélectionnée est Aucun chiffrement, le trafic envoyé par les clients d'accès à distance au serveur d'accès réseau n'est pas sécurisé par une méthode de chiffrement. Cette configuration n'est pas recommandée.

- Chiffrement de base (MPPE 40 bits)
- Chiffrement renforcé (MPPE 56 bits)
- Chiffrement maximal (MPPE 128 bits)

Précédent

Suivant

Terminer

Annuler

Nous ne précisons pas de FQDN :



Spécifier un nom de domaine

Si vous spécifiez un nom de domaine, l'emplacement du compte d'utilisateur fourni par les utilisateurs dans les informations d'identification d'ouverture de session (par exemple un nom de domaine) est remplacé par la valeur de votre choix.

Votre fournisseur de services Internet utilise une partie du nom d'utilisateur pour identifier les demandes de connexion à router vers ce serveur. Cette partie du nom d'utilisateur représente le nom de domaine.

Si vous ne connaissez pas votre nom de domaine, contactez votre fournisseur de services Internet. Si le nom de domaine peut être ignoré, cliquez sur Suivant.

Tapez le nom de domaine, en incluant le séparateur (point ou barre oblique), que votre fournisseur de services Internet utilise pour transmettre les demandes.

Nom de domaine :

Exemple : fournisseur de services Internet.

Avant l'authentification, supprimer le nom de domaine du nom d'utilisateur

Si le nom de domaine est un identificateur ajouté au nom d'utilisateur Windows existant, il doit être supprimé pour permettre à Windows d'authentifier la demande de connexion.

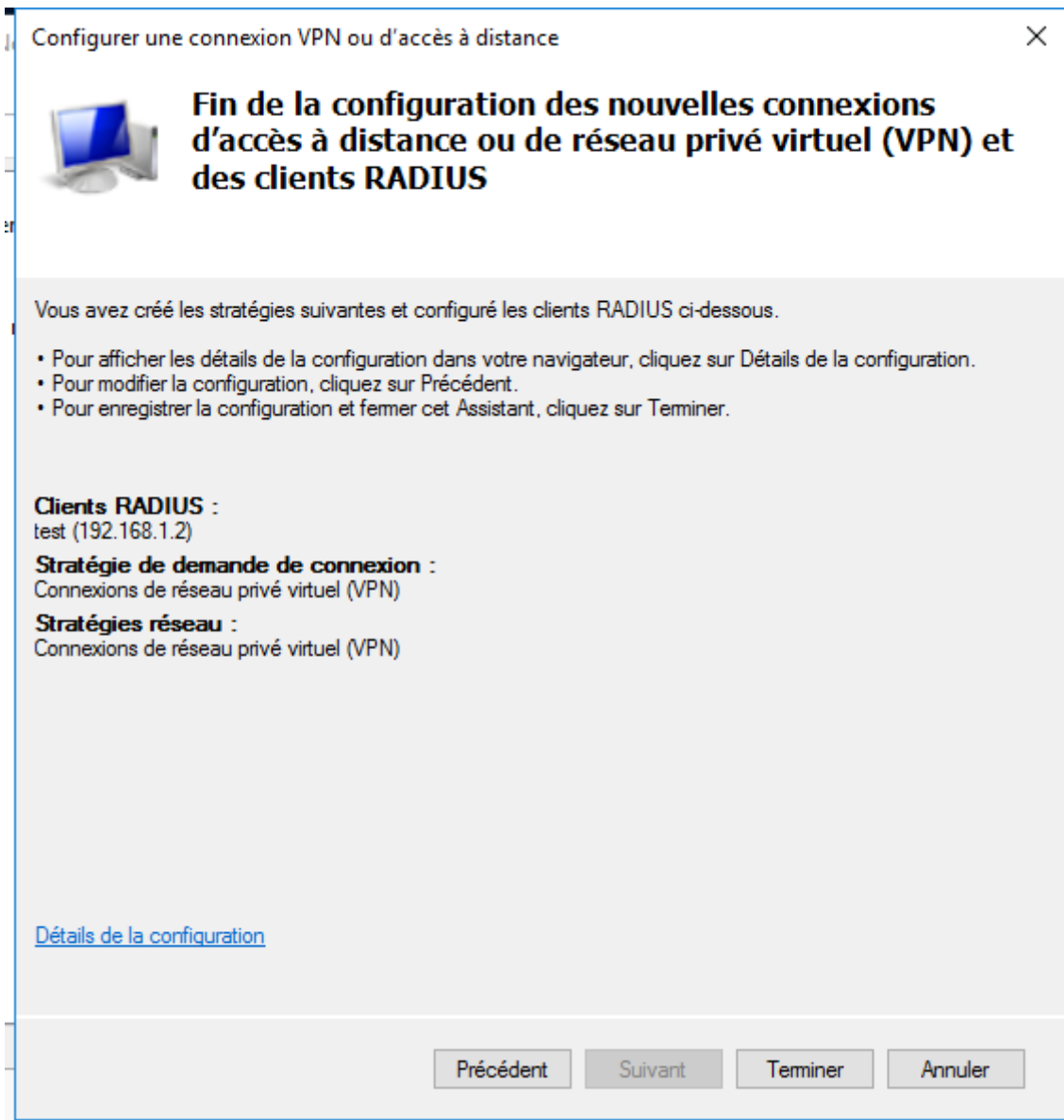
Précédent

Suivant

Terminer

Annuler

Récapitulatif :

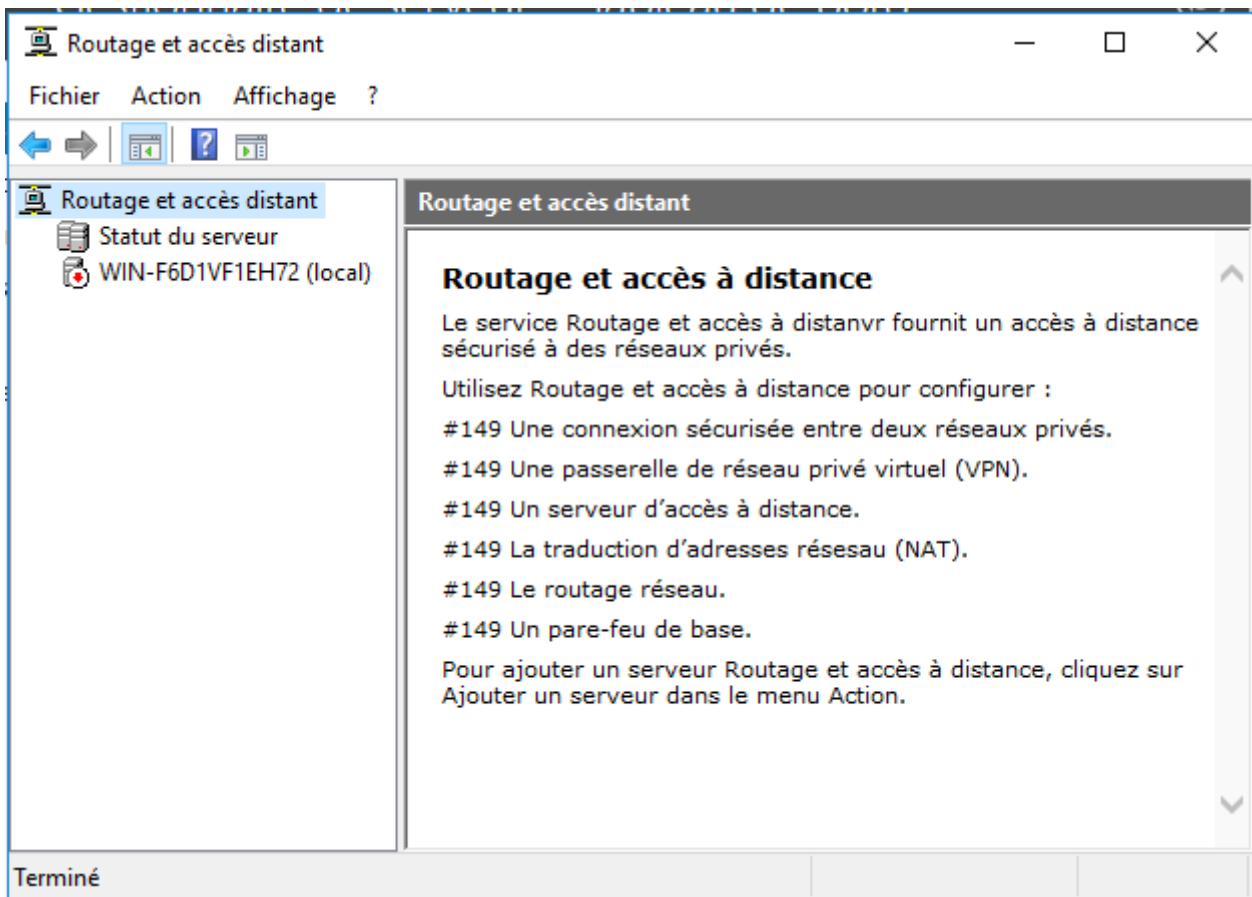


Enfin, toujours dans la console NPS, il faut faire un clic droit sur le serveur local et l'inscrire dans l'Active Directory.

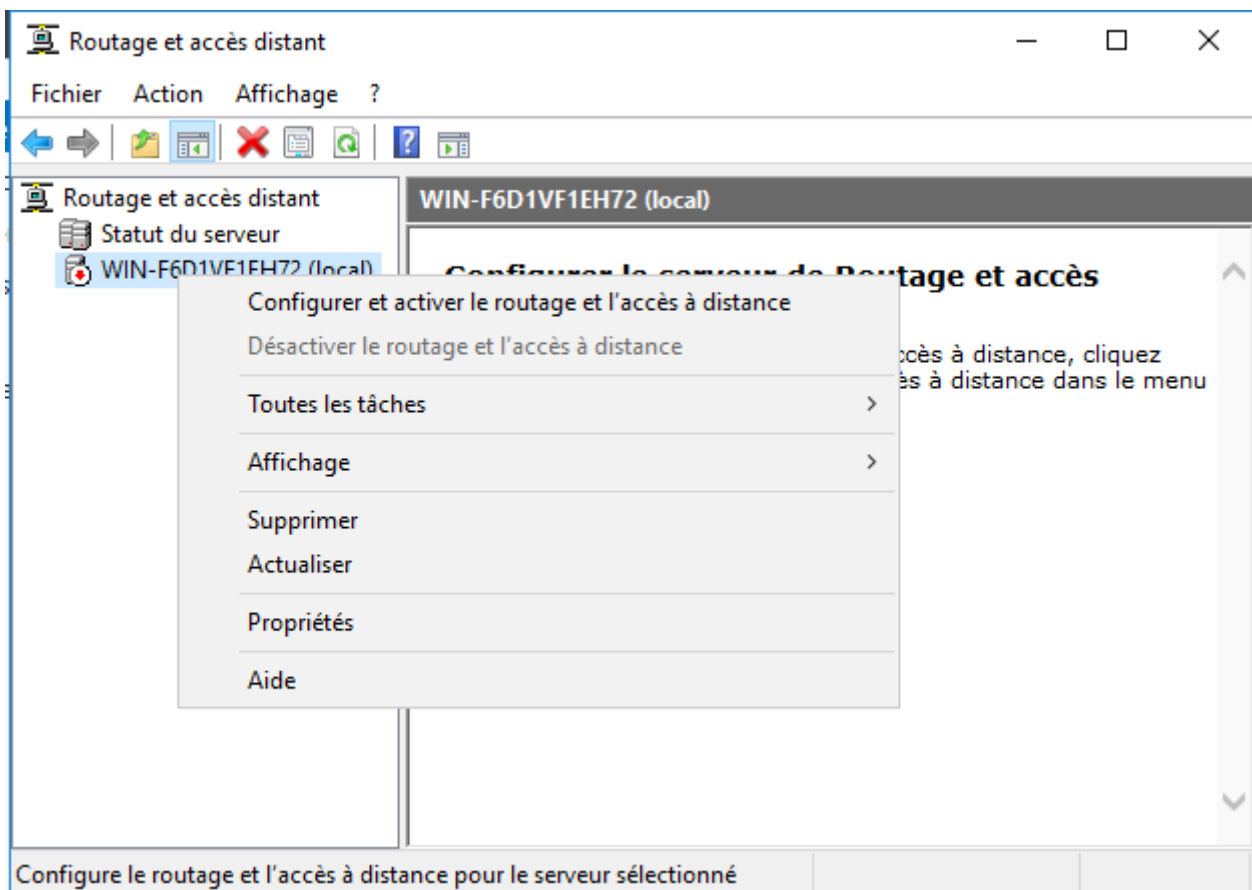
Installation du serveur VPN :

Le rôle nécessaire au bon fonctionnement de cette installation ont été installé précédemment.

Nous allons ouvrir la console de gestion "Routage et accès à distance" :



Puis, en faisant un clic droit sur le nom du serveur, nous sélectionnons "**configuration et activer le routage et l'accès à distance**" :



Nous allons configurer un accès **VPN & NAT** :

Assistant Installation d'un serveur Routage et accès distant

Configuration

Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.

- Accès à distance (connexion à distance ou VPN)
Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).
- NAT (Network address translation)
Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.
- Accès VPN (Virtual Private Network) et NAT
Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.
- Connexion sécurisée entre deux réseaux privés
Connecter ce réseau à un réseau distant tel que celui d'une succursale.
- Configuration personnalisée
Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.

< Précédent Suivant > Annuler

Sélection de la carte WAN :

Assistant Installation d'un serveur Routage et accès distant

Connexion VPN

Au moins une interface réseau doit être connectée à Internet afin de permettre aux clients VPN de se connecter à ce serveur.

Sélectionnez l'interface réseau qui connecte ce serveur à Internet.

Interfaces réseau :

Nom	Description	Adresse IP
Carte	Intel(R) Gigabit CT Deskto...	172.16.66.30
Ethernet	Intel(R) Ethernet Connecti...	192.168.1.139 (DHCP)

< Précédent Suivant > Annuler

Définition automatique de l'attribution IP :

Assistant Installation d'un serveur Routage et accès distant

Attribution d'adresses IP
Vous pouvez sélectionner la méthode d'assignation des adresses IP aux clients.

Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?

Automatiquement
Si vous utilisez un serveur DHCP pour attribuer des adresses, vérifiez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.

À partir d'une plage d'adresses spécifiée

< Précédent Suivant > Annuler

Nous sélectionnons OUI.

Assistant Installation d'un serveur Routage et accès distant

Gestion de serveurs d'accès à distance multiples
Des demandes de connexion peuvent être authentifiées localement ou transférées à un serveur RADIUS (Remote Authentication Dial-In User Service) pour être authentifiées.

Bien que le Routage et l'accès à distance permettent l'authentification de demandes de connexion, des réseaux de grande taille incluant plusieurs serveurs d'accès à distance utilisent souvent un serveur RADIUS pour centraliser l'authentification.

Si vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce serveur pour transférer les requêtes d'authentification au serveur RADIUS.

Voulez-vous configurer ce serveur pour qu'il interagisse avec un serveur RADIUS ?

Non, utiliser Routage et accès distant pour authentifier les demandes de connexion

Oui, configurer ce serveur pour travailler avec un serveur RADIUS

< Précédent Suivant > Annuler

Spécifications du serveur RADIUS :

Assistant Installation d'un serveur Routage et accès distant

Sélection des serveurs RADIUS
Vous pouvez spécifier les serveurs RADIUS que vous voulez utiliser pour l'authentification et la gestion des comptes.

Entrez les serveurs RADIUS principal et secondaire que ce serveur utilisera pour la gestion des comptes et l'authentification à distance.

Serveur RADIUS principal :

Serveur radius secondaire :

Tapez le secret partagé (mot de passe) qui est utilisé pour contacter ces serveurs RADIUS.

Secret partagé :

< Précédent **Suivant >** Annuler

Nous activons le relai DHCP :

Assistant Installation d'un serveur Routage et accès distant

Fin de l'Assistant Installation d'un serveur de routage et d'accès à distance

Vous avez terminé l'Assistant Installation d'un serveur de routage et d'accès distant.

Résumé :

Directory.

Pour fermer cet Assistant, cliquez sur Terminer.

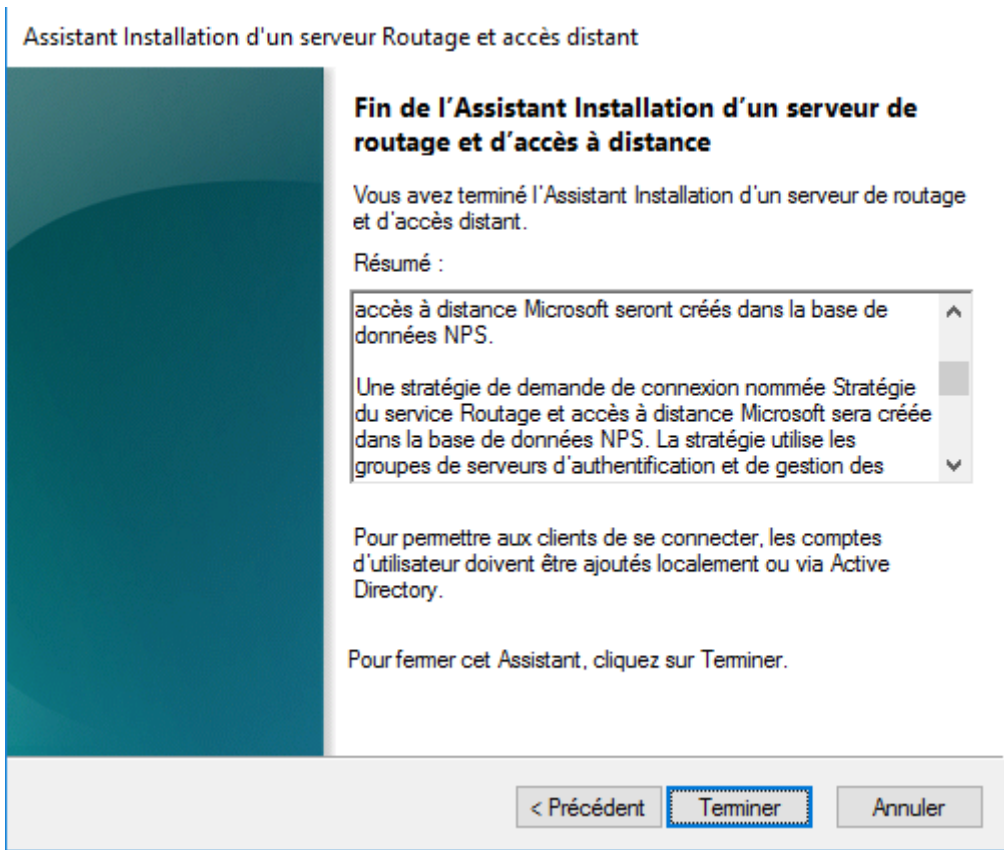
< Précédent Terminer Annuler

Routage et accès distant

Pour permettre la prise en charge du relais des messages DHCP à partir de clients d'accès à distance, vous devez configurer les propriétés de l'agent de relais DHCP avec l'adresse IP de votre serveur DHCP.

OK Aide

Enfin nous pouvons terminer l'installation :



L'installation est fonctionnelle !