Windows Server



Date de dernière modification : 06/05/24

Version : 1.2

Sommaire

page



Service VPN

Page 1 sur 55

Date : 06/05/24

2 Introduction

2.1 Présentation de Windows Server

Windows Server est un système d'exploitation développé par Microsoft pour prendre en charge la gestion au niveau de l'entreprise, le stockage des données, les applications et les communications. Malgré le fait qu'il partage une partie de son code avec les systèmes d'exploitation Windows standards, Windows Server a pour but de gérer une multitude d'appareils, de réseaux et de service via un seul serveur. En effet, si l'on compare Windows 10 à son équivalent Windows Server (WS2019), ce dernier supporte des configurations plus puissantes (allant jusqu'à 24To de RAM), peut être configuré sans interface graphique, et offre de nombreux outils et services de gestion qui ne sont pas disponibles dans les autres systèmes d'exploitation Microsoft. Enfin, la position dominante de Microsoft dans le marché des OS fait que Windows Server propose généralement une excellente compatibilité avec les différents softwares et hardwares utilisés par les entreprises.

2.2 Services Essentiels

2.2.1 Gestionnaire de Serveur

Le gestionnaire de serveur est l'interface principale de Windows Server. Ce programme sert de tableau de bord et permet de rapidement vérifier le bon fonctionnement des différents services ainsi que d'apporter des modifications aux paramètres du serveur.

2.2.2 Assistant Ajout de Rôles et de Fonctionnalités

Ce wizard permet d'installer des rôles et des fonctionnalités à Windows Server à travers une interface graphique. Il suffit de choisir le service à installer dans la liste puis de procéder à l'installation. C'est grâce à cet outil que nous pourrons installer notre service VPN durant le TP.



2.2.3 Routage et Accès Distant

Ce service permet de mettre en place et de configurer des accès distants à des réseaux privés. A travers son interface graphique, il est possible de modifier nos paramètres d'accès à distance ainsi que d'ajouter d'autres serveurs.

2.2.4 Gestion de l 'Ordinateur

Ce service rassemble de nombreux outils administratifs et permet aux utilisateurs de paramètres une multitude de services au même endroit. En effet, Gestion de l'ordinateur permet d'accéder rapidement à de nombreux outils tels que Event Viewer, Gestionnaire de Périphériques et Gestionnaire des Tâches sans avoir besoin d'ouvrir chaque service individuellement.

2.2.5 Pare-feu Windows Defender

Le pare-feu Windows Defender est le firewall par défaut de Windows Server. Il sert à filtrer les communications entre notre serveur et les autres réseaux. Son interface permet de créer, modifier et supprimer les règles de trafic entrant et sortant. Ces règles peuvent être paramétrées pour autoriser ou bloquer la connexion entre un programme ou un port spécifique et un réseau externe.

3 Qu'est-ce qu'un VPN ?

3.1 Définition VPN

Un VPN ou Virtual Private Network est un outil réseau qui permet à une machine de se connecter à un réseau distant à travers un tunnel privé. En réalité, ce tunnel est un réseau privé qui permet aux différents appareils autorisés de communiquer entre eux de façon sécurisée.

Un VPN redirige les données à travers un serveur distant, en les chiffrant au passage. En général, lorsque l'on accède à un site Web, notre FAI (fournisseur d'accès Internet) reçoit la demande et nous redirige vers notre destination. Mais lorsque l'on se connecte à un VPN, ce dernier redirige les données Internet à travers un serveur distant avant de les envoyer à notre destination.

Le VPN permet donc de masquer les données. Le chiffrement est important lorsque l'on souhaite protéger nos données et minimiser notre empreinte en ligne.



Service VPN

Page 3 sur 55

En se connectant à un VPN, l'adresse IP de notre machine est masquée. En effet, une nouvelle adresse IP appartement au serveur VPN est utilisée ce qui permet un certain niveau d'anonymité. Cela rend donc la navigation en ligne plus sécurisée et garantit une confidentialité accrue.

Ainsi, cet outil peut être utile dans de multiples cas de figure, mais généralement un VPN sert à deux choses :

- Se connecter à un réseau distant pour pouvoir accéder à ses ressources de façon relativement sécurisée
- Modifier ou dissimuler l'adresse IP d'une machine, lorsqu'elle se connecte à internet ou n'importe quel autre réseau

3.2 Service VPN Windows Server

Windows Server propose par défaut un service VPN. Ce dernier doit cependant être installé à travers l'interface Rôles et fonctionnalités avant de pouvoir être utilisé. Cet outil VPN fait parti du système d'Accès à Distance de Windows Server qui permet aux utilisateurs distants de se connecter de façon sécurisée au réseau du serveur et d'accéder aux ressources hébergées sur ce dernier. Ces fonctionnalités sont disponibles sur tous les systèmes d'exploitation Windows Server depuis WS2012.

Le VPN Remote Access de Windows Server peut être utilisé de deux façons différentes : pour mettre en place un réseau VPN site à site, ou pour mettre en place un réseau VPN client à site.

Le VPN site à site :

Un VPN site à site relie deux sites distants à travers une infrastructure réseau publique, par exemple en utilisant le réseau Internet. Si deux sites d'une même entreprise souhaitent communiquer entre eux tout en protégeant leurs échanges, ils peuvent alors faire recours à un VPN. D'un point de vue réseau, ces sites seront donc virtuellement interconnectés par un routeur géant : Internet. Dans ce cas, les échanges sont chiffrés pour empêcher que l'interception de données ne compromette la sécurité. On parle alors de tunnel VPN et deux équipements intermédiaires (un de chaque côté) appelés terminaisons VPN. Ces derniers assurent le bon fonctionnement du tunnel VPN ; il peut s'agir d'un routeur ou encore d'un firewall.





Le VPN MPLS (Multiprotocol Label Switching) est un type de réseau privé virtuel (VPN) basé sur une infrastructure MLPS. Il utilise des étiquettes pour acheminer les données sur le réseau, permettant ainsi une communication sécurisée et fiable entre les sites distants d'une entreprise ou d'une organisation. Avec le MPLS, la première fois qu'un paquet entre dans le réseau, il est affecté à une classe d'équivalence de transmission (FEC : Forwarding equivalence class) spécifique. Elle est indiquée en ajoutant une courte séquence de bits (l'étiquette) au paquet.

Chaque routeur du réseau dispose d'un tableau indiquant comment traiter les paquets d'un type de FEC spécifique. Ainsi, lorsque le paquet est entré dans le réseau, les routeurs n'ont pas besoin d'effectuer une analyse d'en-tête. Les routeurs suivants utilisent plutôt l'étiquette comme un index dans une table qui leur fournit un nouveau FEC pour ce paquet. Le VPN MPLS est également connu pour sa fiabilité, car il utilise une infrastructure hautement redondante pour acheminer les données sur le réseau. Les informations circulent par le biais de plusieurs liens de connexion, ce qui rend le réseau plus stable et moins susceptible aux interruptions.

Le VPN client à site :

Les VPN client à site ont pour but de fournir à un poste situé à l'extérieur de l'entreprise (sur un réseau partenaire ou domestique) un accès sécurisé au réseau de l'entreprise ; de cette manière le client ou l'employé peut obtenir un accès réseau aux ressources de l'entreprise au travers d'une simple connexion Internet.



Ce type de service est de plus en plus utilisé car il offre la possibilité aux employés qui sont souvent en déplacement d'accéder directement aux ressources nécessaires. Il est également utile



lorsque l'entreprise désire offrir des possibilités de télétravail à ses employés. La mise en place d'une telle solution nécessite de faire l'inventaire des exigences de sécurité car elle fournit un accès réseau à l'entreprise depuis des postes et de réseaux qui peuvent ne pas être considérés comme sécurisés.

La principale différence entre un VPN site à site et un VPN client à site est que le premier relie deux réseaux locaux distincts, tandis que le second permet à un individu de se connecter à un réseau privé virtuel à partir d'un appareil distant.

3.3 Protocoles de Tunneling VPN

Pour assurer le bon paramétrage d'une infrastructure d'accès à distance par VPN, il est essentiel de développer une certaine compréhension des protocoles de tunneling proposés. Cela nous permettra par la suite de pouvoir choisir le protocole le plus adapté à notre situation.

Windows Server offre une remarquable flexibilité en termes de configuration du service VPN en nous proposant un choix varié de protocoles de tunneling et d'authentification. Nous allons donc étudier le fonctionnement de ces protocoles pour déterminer dans quels scénarios ils peuvent être mis en place.

3.3.1 PPTP

PPTP : Point to Point Tunneling Protocol, est l'un des plus anciens protocoles de Microsoft. Il est également très rapide et simple à configurer. PPTP utilise le port TCP 1723, pour la communication qui utilise le protocole GRE (Generic Routing Encapsulation) permettant d'envelopper des paquets de données à l'intérieur de paquets de données secondaires afin d'établir une connexion réseau direct point à point.

Avantages :

- Configuration simple
- Compatible avec la plupart des systèmes d'exploitation
- Bonne vitesse de connexion

Inconvénients :

- Limite chiffrement de 128 bits (chiffrement des données n'est pas recommandé)
- Pas de garantit d'intégrité (ne vérifie pas si les données n'ont pas été modifiées en transit)
- Problèmes de performances sur les réseaux instables

3.3.2 SSTP

SSTP : Secure Socket Tunneling Protocol, est un protocole créé par Microsoft qui transporte le trafic VPN en l'encapsulant via un lien SSL (Secure Sockets Laye) à travers le port HTTPS



Service VPN

Page 6 sur 55

(HyperText Transfer Protocol Secure). Ce port TCP 443 est rarement bloqué car la plupart des navigations Web ne fonctionneraient pas sans lui. Par conséquent, non seulement SSTP passe à travers 99% des pare-feux, mais il garantit également que votre VPN est chiffré.

Avantages :

- Facile à utiliser
- Peut contourner la plupart des pare-feux 🛛 Haut niveau de sécurité
- Intégré à l'environnent Windows
- Peut supporter une large gamme d'algorithmes de chiffrement

Inconvénient :

- Détenue et maintenue à 100% par Microsoft
- Compliqué à mettre en place sur les plateformes autres que Windows

3.3.3 L2TP

L2TP : Layer 2 Tunneling Protocol, est un protocole qui ne fournit aucun chiffrement par luimême. Le VPN L2TP utilise généralement un protocole d'authentification tel que IPSec (Internet Protocol Security) pour un chiffrement fort, ce qui lui donne un avantage sur les autres protocoles. Les données transmises via le protocole L2TP/IPsec utilisent les ports UDP 500, 1701, 4500. Ces données sont généralement authentifiées deux fois, ce qui ralentit les performances mais offre le plus haut niveau de sécurité.

Avantages :

- Facile à configurer (sur les systèmes exploitation Mac et Windows)
- Haut niveau de chiffrement et de sécurité
- Double encapsulation des données, ce qui signifie une double vérification des données
- Disponible non seulement sur ordinateur de bureau mais aussi sur les systèmes d'exploitation mobile

Inconvénient :

- Performances lentes en raison de la double authentification
- Certains pare-feux peuvent bloquer les ports du protocoles L2TP

3.3.4 IKEv2

IKEv2 : Internet Key Exchange version 2, est un protocole de chiffrement de requête et de réponse développé par Cisco et Microsoft. Il établit et gère l'attribut Security Association (SA), qui est utilisé pour prendre en charge une communication sécurisée entre deux entités de réseau. Il le fait dans une suite d'authentification, généralement IPsec qui permet d'assurer un trafic sécurisé. Il permet aux périphériques VPN situés aux deux extrémités du tunnel de chiffrer et de déchiffrer les paquets à l'aide des clés pré-partagées, de protocoles d'authentification (EAP) ou de signatures numériques.

Le chiffrement et le déchiffrement utilisent l'authentification asymétrique, ce qui signifie que les deux extrémités du tunnel n'ont pas besoin de s'entendre sur une seule méthode d'authentification.

Avantages :

Service VPN

Page 7 sur 55

- Protocole hautement sécurisé
- Connexion stable et fiable
- L'un des protocoles le plus rapide

Inconvénient :

- Prend en charge un nombre limité de plateformes
- Peut être bloqué par certains pare-feux

3.4 Protocoles d'Authentification VPN

3.4.1 PAP

PAP : Password Authentification Protocole, est un protocole d'authentification point à point (PPP) qui utilise un nom d'utilisateur et un mot de passe pour authentifier les utilisateurs. Ces données d'authentification ne sont cependant pas chiffrées, ce qui fait de PAP le protocole d'authentification le moins sécurisé parmi ceux proposés par Windows Server. En effet, lorsqu'un utilisateur essaye d'établir une session PPP avec un serveur, il lui envoie son nom d'utilisateur et son mot de passe en texte brut dans un paquet de requête d'authentification. Toute personne analysant les communications entre le serveur et ses utilisateurs peut donc facilement déterminer les identifiants et mots de passe de cet utilisateur.

Avantage :

• Compatible avec la plupart des OS

Inconvénient :

• Transmet les logins et mots de passe en clair

3.4.2 CHAP

CHAP : Challenge Handshake Authentication Protocol, est un protocole d'authentification point à point (PPP) qui utilise une méthode de défi-réponse pour vérifier l'identité de ses clients. Ainsi, le pair (l'authentificateur) défie l'appelant (l'authentifié) de prouver son identité. Pour ce



faire, l'appelant doit envoyer une réponse hash en utilisant MD5. Le pair résout ensuite son propre calcul et compare sa réponse avec celle envoyée par l'appelant pour déterminer si l'authentification est réussie ou non. De plus, CHAP est capable de réauthentifier ses utilisateurs de façon périodique en renvoyant des défis à un intervalle de temps paramétrable pour encore plus de sécurité.

Avantages :

- Compatible avec la plupart des OS
- Plus sécurisé que PAP

Inconvénient :

- Seule l'identité du client est vérifiée
- Ne protège pas contre les attaques man in the middle

3.4.3 MS-CHAPv2

MS-CHAPv2 : Microsoft Challenge Handshake Authentication Protocol Version 2, est un processus d'authentification mutuelle avec mot de passe chiffré à sens unique. Cette authentification mutuelle signifie que le serveur d'authentification et le client doivent vérifier leurs identités respectives avant que la connexion soit établie. Tout comme le protocole CHAP, MS-CHAPv2 utilise le principe de défi-réponse où le pair envoie un défi et l'appelant doit envoyer une réponse hash en utilisant MD5 qui est ensuite comparée à la réponse du pair. Cependant la particularité de MS-CHAPv2 est que la réponse du pair contient elle aussi un calcul hash qui est à son tour vérifié par l'appelant avant que la connexion soit autorisée.

Avantages :

- Protocole le plus utilisé pour l'authentification VPN
- Plus sécurisé que PAP et CHAP

Inconvénient :

• Ne protège pas contre les attaques man in the middle

3.4.4 EAP

EAP : Extensible Authentication Protocol, est un système comprenant plusieurs méthodes d'authentification. Contrairement aux options étudiées précédemment, EAP est bien plus qu'un simple protocole d'authentification : c'est une infrastructure permettant au serveur d'authentification et aux utilisateurs de négocier la méthode d'authentification utilisée pour établir la connexion. Par défaut, la méthode d'authentification utilisée sera EAP-TLS (Transport Layer Security), une méthode d'authentification mutuelle qui requiert un certificat d'authentification coté client. De ce fait, EAP-TLS est l'une des méthodes d'authentification les plus sécurisées proposées par EAP.

Avantages :

- Méthode d'authentification flexible
- Plus sécurisé que PAP et CHAP

Inconvénient :



Service VPN

Page 9 sur 55

Pas aussi simple à mettre en place que PAP et CHAP 4 Mise en Place d'un Service VPN Windows Server

4.1 Présentation du TP

Afin de mieux comprendre le fonctionnement du service VPN sous Windows Server, nous allons maintenant détailler la mise en place d'un tunnel VPN entre un serveur et un client. Pour cette démonstration, nous avons décidé de mettre en place un VPN L2TP avec certificat depuis un Windows Server. Cette configuration nous permet d'étudier L2TP, un protocole couramment utilisé et relativement simple à mettre en place. De plus, cette configuration nous permet de mettre en place le protocole IPsec avec un certificat d'authentification pour sécuriser notre tunnel.

4.2 Mise en Place des Machines Virtuelles

Par souci d'efficacité, nous avons décidé de réaliser notre démonstration avec des machines virtuelles. Pour ce faire, nous allons installer Windows Server 2019 et Windows 10 version 21H2 sur VMware Workstation Pro 17.

Pour assurer le bon fonctionnement de notre VPN par la suite, nous aurons besoin que nos deux machines virtuelles soient capables d'accéder à Internet et de communiquer entre elles à travers Internet. Afin d'assurer ces fonctionnalités, nous allons donc configurer nos 2 VM en mode Bridged dans VMware.

En effet, le mode de connexion Bridged de VMware assure une connexion internet aux VM puisqu'elles se greffent virtuellement sur le même réseau que la machine physique. Le schéma ci-dessous explique cette connexion, et illustre le chemin que prendra notre VPN pour atteindre chaque machine.



New Virtual Machine Wizard

X

Ready	to Cre	ate Virt	ual Mad	chine
-------	--------	----------	---------	-------

Click Finish to create the virtual machine. Then you can install Windows Server 2019.

The virtual machine will be created with the following settings:

Name:	Windows Server 2019	^
Location:	D:\Users\victo\Documents\Virtual Machines\Windows	
Version:	Workstation 17.x	
Operating System:	Windows Server 2019	
Hard Disk:	20 GB, Split	
Memory:	2048 MB	
Network Adapter:	Bridged (Automatic)	1
Other Devices	2 CDU serves CD/DVD_USB Controller, Drinter, Sevend	1.
Ouler Devices.	2 CPO cores, CD/DVD, USB Controller, Printer, Sound	
<u>C</u> ustomize Hardwa	are	

Pour configurer nos machines virtuelles en mode Bridged, nous allons tout d'abord réaliser une installation standard en utilisant les paramètres par défaut jusqu'à arriver à la dernière page. Sur cette page nous allons cliquer sur Customize Hardware.



Х

Hardware

Device Memory Processors New CD/DVD (SATA)	Summary 2 GB 2 Using file D:\Users\victo\Des	Device status Connected Connect at power on
Network Adapter	Bridged (Automatic)	Network connection
≪ USB Controller ↓ Sound Card 금 Printer □Display	Present Auto detect Present Auto detect	Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment:
		LAN Segments Advanced

C'est ici que nous allons pouvoir configurer les paramètres réseau de nos VM. Nous allons donc cliquer sur Network Adapter puis sélectionner l'option Bridged avant de fermer la page en cliquant sur Close.

Nous pouvons ensuite terminer l'installation en cliquant sur Finish.

Il faudra répliquer cette configuration sur notre seconde machine virtuelle pour assurer le bon fonctionnement de notre VPN.

Une fois que nos deux machines sont installées et configurées en mode Bridge dans VMware, nous pouvons donc commencer la configuration du VPN sur Windows Server.



Service VPN

Page 12 sur 55

4.3 Configuration du Serveur VPN sur Windows Server

4.3.1 Adressage IP Statique

Si ce n'est déjà fait, nous vous recommandons d'assigner une adresse IPv4 statique au serveur de manière à ce qu'il soit plus facilement joignable par le client.

Gestionnaire de serveur					ŝ	- 0
🗧 🗸 Gestionnai	ire de serveur 🕨	Serveur	local • 🕲	🗗	Gérer Outils	Afficher Aic
Tableau de bord	PROPRIÉTÉS Pour WIN-177M83D	V3L8				TÂCHES 🔻
Serveur local Tous les serveurs Services de fichiers et d Þ	Nom de l'ordinateur Groupe de travail	WIN-I WORK	77M83DV3L8 IGROUP	Dernières r Windows L Dernière re	nises à jour installée Jpdate cherche de mises à	is jour :
	Pare-feu Windows Defen Gestion à distance Bureau à distance Association de cartes rése Ethernet0	der Privé : Activé Désact 2 Adress	Actif tivé <u>is IPv4 attribués par DHCP, Compatible IPv6</u>	Antivirus W Commenta Configurat Fuseau hor ID de prod	Vindows Defender ires et diagnostics ion de sécurité renfo raire uit (Product ID)	orcée d'Internet
	Version du système d'exp Informations sur le matér	loitation Micros iel VMwa	soft Windows Server 2019 Standard Evaluation re, Inc. VMware20,1	Processeur Mémoire ir Espace disc	s nstallée (RAM) que total	
	< ÉVÉNEMENTS Tous les événements 7 au	total			[> TÂCHES ▼
	Filtrer	م	(≣) ▼ (用) ▼			\odot
	Nom du serveur ID WIN-I77M83DV3L8 8198 WIN-I77M83DV3L8 7030 WIN-I77M83DV3L8 134	Gravité Erreur Erreur Avertissement	Source Microsoft-Windows-Security-SPP Microsoft-Windows-Service Control Manager Microsoft-Windows-Time-Service	Journal Application Système Système	Date et heure 04/05/2023 15:56:0 04/05/2023 15:55:5 04/05/2023 15:55:0	13 15 11

Pour ce faire, il nous suffit de nous rendre dans le gestionnaire de serveur, de cliquer à gauche sur Serveur Local, puis sur Adresse IPv4 attribuée par DHCP. (Cette page peut aussi être atteinte depuis le panneau de configuration en allant dans les options réseau.)



	eau et Internet > Connexions réseau >	ٽ ~	Rechercher dans : Co	nnexions.	p
Organiser 🔻 Désactive	r ce périphérique réseau Diagnostiquer cette connes	cion »		- 🔳	(
Ethernet0 Réseau Intel(R) 82574L Gi	gabit Net				

1 élément 1 élément sélectionné

822 📰

Ici, nous choisissons l'adaptateur réseau connecté à internet (Ethernet0 dans notre cas) et nous faisons un clic droit dessus pour ouvrir ses Propriétés.





Sur cette page, nous pouvons désactiver IPv6 en décochant la case Protocole internet version 6 car nous utiliserons uniquement IPv4 pour notre VPN.

	eters a suprace			
connexion en u	tilisant :			
Intel(R) 8	2574L Gigab	it Network Connection		
			Co	onfigurer
Cette connexior	n utilise les élé	éments suivants :		
🗹 🐺 Client (oour les résea	aux Microsoft		^
🗹 🖳 Partag	e de fichiers	et imprimantes Réseau	x Microsoft	
🗹 🐙 Planific	cateur de pac	uets QoS		
Protoc	ole Internet v	ersion 4 (TCP/IPv4)	1	
Protoc	ole de multipl	exage de carte réseau	Microsoft	
Pilote	de protocole	LLDP Microsoft		
🗆 🔔 Protoc	ole Internet v	ersion 6 (TCP/IPv6)		~
۲				>
Installer		Désinstaller	2	opriétés
Description			U	5
	P/IP (Transm	nission Control Protocol	/Internet Protocol)). Protocole
Protocole IC			unication ontro diff	fóranta

Enfin, nous pouvons sélectionner sur la ligne Protocole internet version 4 puis cliquer sur Propriétés pour passer modifier notre adresse IPv4.

ner di	
es paramètres IP peuvent être dét éseau le permet. Sinon, vous deve ppropriés à votre administrateur ré	erminés automatiquement si votre z demander les paramètres IP Íseau.
 Obtenir une adresse IP automa Utiliser l'adresse IP suivante : 	atiquement
Adresse IP :	192 . 168 .
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192 . 168 .
Obtenir les adresses des serve	urs DNS automatiquement
Utiliser l'adresse de serveur DN	NS suivante :
Serveur DNS préféré :	8.8.8.8
Serveur DNS auxiliaire :	
🗌 Valider les paramètres en quit	tant Avancé



Nous pouvons maintenant cliquer sur Utiliser l'adresse IP suivante puis renseigner l'adresse IP statique désirée avec son masque de sous-réseau et sa passerelle par défaut. Nous pouvons ensuite cliquer sur OK pour confirmer nos modifications.

4.3.2 Installation du Service VPN

Pour commencer notre installation, nous avons tout d'abord besoin d'installer le service VPN. Il est possible de l'installer en lignes de commandes avec PowerShell ou avec l'interface graphique de Rôles et Fonctionnalités. Cependant, nous utiliserons l'interface graphique pour ce TP.



Nous allons donc ouvrir le Gestionnaire de serveur et cliquer sur l'option 2 Ajouter des rôles et fonctionnalités (cette page peut aussi être atteinte en cliquant sur Gérer en haut à droite puis sur Ajouter des rôles et fonctionnalités).



	•	Gerer Outils Attricher Alde
		Supprimer des rôles et fonctionnalités
		Ajouter des serveurs
		Créer un groupe de serveurs
		Propriétés du Gestionnaire de serveur
ssistant Ajout de rôles et c	e fonctionnalités	
vant de comm	iencer	SERVEUR DE DESTINATIOI WIN-177M83DV3L
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Cet Assistant permet d'installer des rôles, des servi déterminer les rôles, services de rôle ou fonctionna de votre organisation, tels que le partage de docur Pour supprimer des rôles, des services de rôle ou d Démarrer l'Assistant de Suppression de rôles et de Avant de continuer, vérifiez que les travaux suivant • Le compte d'administrateur possède un mot de p • Les paramètres réseau, comme les adresses IP sta • Les dernières mises à jour de sécurité de Window	ces de rôle ou des fonctionnalités. Vous devez alités à installer en fonction des besoins informatiqu ments ou l'hébergement d'un site Web. des fonctionnalités : fonctionnalités ts ont été effectués : passe fort atiques, sont configurés
	Si vous devez vérifier que l'une des conditions préa exécutez les étapes, puis relancez l'Assistant. Cliquez sur Suivant pour continuer.	vs Update sont installées alables ci-dessus a été satisfaite, fermez l'Assistant,

Pour notre installation, nous allons laisser les paramètres par défaut et donc cliquer sur Suivant jusqu'à ce que nous atteignions la page Rôles de serveurs.



election net le t	ype d'installation	SERVEUR DE DESTI WIN-177M8	NATIO 33DV3
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	 Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonct ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtue Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des services de rôle et Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Deskta déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions 	ionnalités sur un el hors connexion. des fonctionnalité op Infrastructure) j s.	s. pour
	< Précédent Suivant >	Installer	nule
Assistant Ajout de rôles et de Sélectionner le s	erveur de destination	SERVEUR DE DESTI WIN-177MB) NATIC 33DV3
Assistant Ajout de rôles et de Sélectionner le s Avant de commencer	serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et	SERVEUR DE DESTI WIN-177M8 des fonctionnalité) NATIO 33DV3
Assistant Ajout de rôles et de Sélectionner le s Avant de commencer Type d'installation	Serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs	SERVEUR DE DESTI WIN-177M8 des fonctionnalité) NATIC 33DV3
Assistant Ajout de rôles et de Gélectionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	e fonctionnalités Serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs Sélectionner un disque dur virtuel 	SERVEUR DE DESTI WIN-177M8 des fonctionnalité) NATIC 33DV3
Assistant Ajout de rôles et de électionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités	Serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs Sélectionner un disque dur virtuel Pool de serveurs	SERVEUR DE DESTI WIN-177M8 des fonctionnalité) NATIC 33DV3
Assistant Ajout de rôles et de électionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation	e fonctionnalités Serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et © Sélectionner un serveur du pool de serveurs © Sélectionner un disque dur virtuel Pool de serveurs Filtre :	SERVEUR DE DESTI WIN-177M8 des fonctionnalité] NATIC 33DV3 és.
Assistant Ajout de rôles et de Gélectionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs Sélectionner un disque dur virtuel Pool de serveurs Filtre : Nom Adresse IP Système d'exploitation	SERVEUR DE DESTI WIN-177M8 des fonctionnalité] NATIC 33DV3 és.
Assistant Ajout de rôles et de Gélectionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs Sélectionner un disque dur virtuel Pool de serveurs Filtre : Nom Adresse IP Système d'exploitation WIN-177M83DV3L8 192.168. Microsoft Windows Server 20	SERVEUR DE DESTI WIN-177M8 des fonctionnalité] NATIK 33DV3
Assistant Ajout de rôles et de Gélectionner le s Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	serveur de destination Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et Sélectionner un serveur du pool de serveurs Sélectionner un disque dur virtuel Pool de serveurs Filtre : Nom Adresse IP Système d'exploitation WIN-177M83DV3L8 192.168. Nicrosoft Windows Server 20 Cette page présente les serveurs qui exécutent Windows Server 2012 ou une v ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionn serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte incomplète ne sont pas répertoriés.	SERVEUR DE DESTI WIN-177M8 des fonctionnalité des fonctionnalité 19 Standard Evalu version ultérieure e naire de serveur. Le de données est to) NATIC 33DV3 ÉS. ation et qu es ujou



álastis ses das		SERVEUR DE DESTINATI
electionnel des	roles de serveurs	WIN-177M83DV
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur séle	ectionné.
Type d'installation	Rôles	Description
Rôles de serveurs Fonctionnalités Accès à distance Services de rôle Confirmation Résultats	Accès à distance Attestation d'intégrité de l'appareil Hyper-V Serveur de télécopie Serveur DHCP Serveur DNS Serveur Web (IIS) Service Guardian hôte Services AD DS Services AD LDS (Active Directory Lightweight Dire Services AD RMS (Active Directory Rights Manager Services d'activation en volume Services d'activation en volume Services d'activation en volume Services de fédiciats Active Directory Services de fédiciation Active Directory (AD FS) Services de fichiers et de stockage (1 sur 12 installe Services de stratégie et d'accès réseau	L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réceau

Ici nous allons sélectionner la case Accès à distance puis cliquer sur Suivant.



📥 Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION WIN-177M83DV3L8

Sélectionner des fonctionnalités

Type d'installation	Fonctionnalités	Description
Sélection du serveur	Assistance à distance	Grâce à l'assistance à distance, vou
Rôles de serveurs	Base de données interne Windows BranchCache	technique) pouvez aider les
Fonctionnalités	Chiffrement de lecteur BitLocker	utilisateurs à résoudre leurs
Accès à distance	Client d'impression Internet	questions en rapport avec leur PC.
Services de rôle	Client pour NFS	Vous pouvez afficher et prendre le
	Collection des événements de configuration et de	contrôle du Bureau des utilisateurs
	Compression différentielle à distance	pour depanner et resoudre les problèmes. Les utilisateurs ont
	Data Center Bridging	également la possibilité de sollicite
	Déverrouillage réseau BitLocker	l'aide de leurs amis ou de leurs
	Direct Play	conegues de travail.
	Expérience audio-vidéo haute qualité Windows	
	Extension ISS Management OData	
	Extension WinRM IIS	
	 Fonctionnalités de .NET Framework 3.5 Fonctionnalités de .NET Framework 4.7 (2 sur 7 ins service) 	
	< >	

Nous pouvons laisser ces deux prochaines pages par défaut et cliquer Suivant jusqu'à arriver sur la page Services de rôle.



Accès à distance		SERVEUR DE DESTINATION WIN-177M83DV3L8
Avant de commencer Type d'installation	L'accès distant intègre DirectAccess, la fonctionnalité de rése d'application Web dans une même console de gestion.	au privé virtuel (VPN) et le proxy
Sélection du serveur Rôles de serveurs Fonctionnalités Accès à distance	Déployez DirectAccess pour permettre aux ordinateurs appa à un réseau d'entreprise via Internet en tant que clients Direc disponible chaque fois que les ordinateurs clients se trouven DirectAccess peuvent gérer les clients à distance, ce qui gara jour avec les mises à jour de sécurité et les exigences de con	rtenant à un domaine géré de se connecte ctAccess. La connectivité est transparente e t sur Internet. Les administrateurs ntit que les ordinateurs portables restent a formité de l'entreprise.
Services de rôle Confirmation Résultats	Déployez DirectAccess pour permettre aux ordinateurs client non pris en charge par DirectAccess ou configurés dans un g réseaux d'entreprise via une connexion VPN.	s exécutant des systèmes d'exploitation roupe de travail d'accéder à distance à de
	Déployez le proxy d'application Web pour publier certaines a votre réseau d'entreprise à destination d'appareils clients situ AD FS peuvent être utilisés pour garantir l'authentification de applications publiées. Le proxy d'application Web fournit éga vos serveurs AD FS.	applications HTTP et HTTPS spécifiques de Jés hors du réseau d'entreprise. Les service es utilisateurs avant qu'ils n'accèdent aux alement une fonctionnalité de proxy pour
	Configurez les fonctionnalités de routage RRAS à l'aide de la	console Accès à distance.
	< Précédent Suiv	ant > N Installer Annuler
ssistant Ajout de rôles et de fon	ictionnalités	- 0
electionner des s	ervices de rôle	SERVEUR DE DESTINATIO WIN-177MB3DV3
Avant de commencer	Sélectionner les services de rôle à installer pour Accès à dist	ance
IVDE CINSTALIATION	Services de rôle	Description
Sélection du serveur Rôles de serveurs Fonctionnalités	DirectAccess et VPN (accès à distance) Proxy d'application web Routage	DirectAccess donne aux utilisateur la possibilité d'être connecté en toute transparence à leur réseau d'entreprise à partir du moment o ils ont accès à Internet. Avec
Sélection du serveur Rôles de serveurs Fonctionnalités Accès à distance Services de rôle Confirmation Résultats	DirectAccess et VPN (accès à distance) Proxy d'application web Routage	DirectAccess donne aux utilisateur la possibilité d'être connecté en toute transparence à leur réseau d'entreprise à partir du moment o ils ont accès à Internet. Avec DirectAccess, il est possible de gés des ordinateurs mobiles dès que l'ordinateur est connecté à Interne permettant ainsi aux utilisateurs mobiles d'être à jour avec les stratégies de sécurité et d'intégrit
Sélection du serveur Rôles de serveurs Fonctionnalités Accès à distance Services de rôle Confirmation Résultats	Proxy d'application web Routage	DirectAccess donne aux utilisateur la possibilité d'être connecté en toute transparence à leur réseau d'entreprise à partir du moment o ils ont accès à Internet. Avec DirectAccess, il est possible de géi des ordinateurs mobiles dès que l'ordinateur est connecté à Interne permettant ainsi aux utilisateurs mobiles d'être à jour avec les stratégies de sécurité et d'intégrit système. VPN utilise la connectivit de l'Internet plus une combinaisor des technologies de tunnelling et chiffrement des données pour connecter les clients distants et les bureaux distants.
Sélection du serveur Rôles de serveurs Fonctionnalités Accès à distance Services de rôle Confirmation Résultats	Proxy d'application web Routage	DirectAccess donne aux utilisater la possibilité d'être connecté en toute transparence à leur réseau d'entreprise à partir du moment ils ont accès à Internet. Avec DirectAccess, il est possible de gr des ordinateurs mobiles dès que l'ordinateur est connecté à Interr permettant ainsi aux utilisateurs mobiles d'être à jour avec les stratégies de sécurité et d'intégri système. VPN utilise la connectiv de l'Internet plus une combinaise des technologies de tunnelling e chiffrement des données pour connecter les clients distants et le bureaux distants.

C'est ici que nous allons installer le service VPN en sélectionnant la case DirectAccess et VPN (accès à distance).



Service VPN

Page 21 sur 55

Ass	istant Ajout de roles et de fonctionnalites	×
Ajc	outer les fonctionnalités requises pour DirectAccess	
et '	VPN (accès à distance) ?	
Vou sauf égal	s ne pouvez pas installer DirectAccess et VPN (accès à distance) si les services de rôle ou les fonctionnalités suivants sont ement installés.	
	Base de données interne Windows Gestion de stratégie de groupe	^
	Outils d'administration de serveur distant	
	 Outils d'administration de rôles 	
	 Outils de gestion de l'accès à distance [Outils] Interface GUI de l'accès à distance et outils 	
	[Outils] Module d'accès à distance pour Windows Pi	
	Serveur Web (IIS)	
	Outils de gestion	
	[Outils] Console de gestion IIS	~
<	>	
-	Inclure les outils de gestion (si applicable)	

Suite à cela, une page devrait s'ouvrir nous demandant de confirmer notre installation, nous allons donc cliquer sur Ajouter des fonctionnalités.

electionner des	SETVICES de rôle Sélectionner les services de rôle à installer pour Accès à	WIN-177M83DV3L4
Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Accès à distance Services de rôle Rôle Web Server (IIS) Services de rôle Confirmation Résultats	Services de rôle DirectAccess et VPN (accès à distance) Proxy d'application web Routage	Description DirectAccess donne aux utilisateurs la possibilité d'être connecté en toute transparence à leur réseau d'entreprise à partir du moment où ils ont accès à Internet. Avec DirectAccess, il est possible de gére des ordinateurs mobiles dès que l'ordinateur est connecté à Internet, permettant ainsi aux utilisateurs mobiles d'être à jour avec les stratégies de sécurité et d'intégrité système. VPN utilise la connectivité de l'Internet plus une combinaison des technologies de tunnelling et d chiffrement des données pour connecter les clients distants et les bureaux distants.

Après cela, il nous suffit de cliquer sur Suivant jusqu'à arriver à la page Confirmation. Service VPN Page 22 sur 55



ole Web Servei	(IIS) WIN-177M83DV3L
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs	Les serveurs web sont des ordinateurs qui vous permettent de partager des informations sur Internet ou via des intranets et des extranets. Le rôle de serveur web comprend Internet Information Services (IIS) 10.0 avec des fonctionnalités améliorées de sécurité, de diagnostic et d'administration, une plateforme web unifiée qui intègre IIS 10.0, ASP.NET et WCF (Windows Communication Foundation).
Fonctionnalités Accès à distance Services de rôle	 L'installation par défaut du rôle de serveur web (IIS) inclut l'installation des services de rôle qui vou permettent de traiter du contenu statique, d'effectuer des personnalisations minimes (comme les documents par défaut et les erreurs HTTP), de surveiller et d'enregistrer l'activité du serveur, et de
Rôle Web Server (IIS)	configurer la compression du contenu statique.
Services de rôle	
Confirmation	
Résultats	
	Plus d'informations sur Web Server IIS



Windows Server



X

П

WIN-I77M83DV3L8

SERVEUR DE DESTINATION

📥 Assistant Ajout de rôles et de fonctionnalités

Sélectionner des services de rôle



Sur cette page il ne nous reste plus qu'à cliquer sur Installer pour lancer l'installation.



Service VPN

Page 25 sur 55

4.3.3 Configuration du Routage et Accès Distant

Une fois l'installation terminée, nous allons pouvoir configurer le service Routage et accès distant.

Pour ouvrir ce service, nous pouvons cliquer sur Ouvrir l'Assistant Mise en route dans la fenêtre d'installation que nous venons d'utiliser. (Cette page peut mettre un certain temps à charger).

Assistant Ajout de rôles et de	fonctionnalités	<u>800</u> 5		×
Progression de l'	installation	SERVEUR DE WIN-	DESTINAT	ION /3L8
Avant de commencer Type d'installation Sélection du serveur	Afficher la progression de l'installation	_		
Rôles de serveurs	Configuration requise. Installation réussie sur WIN-177M83DV3L8.			
Accès à distance Services de rôle Rôle Web Server (IIS) Services de rôle Confirmation Résultats	Acces a distance DirectAccess et VPN (accès à distance) Configurer le rôle Ouvrir l'Assistant Mise en route Base de données interné Windows Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils de gestion de l'accès à distance Interface GUI de l'accès à distance et outils en ligne de comm	nande		~
	Vous pouvez fermer cet Assistant sans interrompre les tâches en cours leur progression ou rouvrez cette page en cliquant sur Notifications da commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration	d'exécution. ns la barre d	Examine le	Z
	< Précédent Suivant >	Fermer	Annul	er



Gestionnaire de serveur		- 1 1			-	8	- 0	×
Gestionna Gestionna	BIENVENUE DANS GEST		LE DORD Configuration post-déploie. Configuration requise pour	TĂCH VPN	Gérer	Outils	Afficher	Aide
 Serveul local Tous les serveurs Accès à distance IIS Services de fichiers et d > 	DÉMARRAGE RAPIDE	2 3	(accès à distance) à WIN-177 Ouvrir l'Assistant Mise en ro d'un Installation de fonctionnalité Configuration requise. Insta 177M83DV3L8. Ajouter des rôles et fonctior	M83DV3L8 ute i Ilation réussie sur WIN- nnalités				
	NOUVEAUTÉS EN SAVOIR PLUS	4 5 Cor	Détails de la tâche	aux services clou	d		Masque	r
	Rôles et groupes de serve Rôles : 3 Groupes de serve	eurs urs:1 Nomb	ore total de serveurs : 1	1				
	Facilité de gestion Événements Services Performances Résultats BPA	8	Facilité de gest Événements Services Performances Résultats BPA	ion				~

(Nous pouvons aussi retrouver cet outil en cliquant sur le drapeau en haut à droite du Gestionnaire de serveur, puis sur le message Ouvrir l'Assistant Mise en route.)

	Configuration de l'acces distant	
	Assistant Prise en main	
Bier Utilis	venue dans l'accès à distance sez les options de cette page pour configurer DirectAccess et une connexion VPN	
oun		
\rightarrow	Déployer DirectAccess et VPN (recommandé)	
	Configurer DirectAccess et le réseau privé virtuel (VPN) sur le serveur et activer les ordinateurs	
	clients DirectAccess. Autoriser les ordinateurs clients distants non pris en charge pour DirectAccess à se connecter sur le réseau privé virtuel.	
\rightarrow	Déployer DirectAccess uniquement	
	Configurer DirectAccess sur le serveur et activer les ordinateurs clients DirectAccess.	
		T
\rightarrow	Déployer VPN uniquement	
	configurer VPN a l'aide de la console noutage et acces à distance. Les ordinateurs clients distants peuvent se connecter sur le réseau privé virtuel et plusieurs sites peuvent être connectés au moyen de connexions VPN de site à site. VPN peut être utilisé par les clients non pris en	
	charge pour DirectAccess.	



Page 27 sur 55

Une fenêtre de Configuration de l'accès distant devrait s'ouvrir. Dans notre cas, nous allons sélectionner Déployer VPN uniquement car nous n'aurons pas besoin de DirectAccess durant notre TP.

	🚊 Routage et accès distant			_		×	r _2	Gérer
de loc se dis	Fichier Action Affichage ? Image: Statut du serveur Image: Statut du serveur Image: Statut du serveur Image: Statut du serveur Image: Statut du serveur Image: Statut du serveur Image: Statut du serveur	Assistant Installation d'un ser	veur Routage et accès c Fin de l'Assistant routage et d'accès Vous avez terminé l'Ass routage et d'accès dista Résumé des sélections	listant Installa a dista sistant Ins ant.	ntion d'u ance tallation d	un serv 'un serve	eur de ur de	
de			Accès VPN				~ ~	
			Configurez les services et accès distant après a Pour fermer cet Assistar	sélection avoir ferm it, cliquez	nés dans é cet Assi : sur Termi	la consolo stant. iner.	e Routage	
	Fac	inements	Événeme	écédent	Termi	ner	Annuler	

Une fois l'option sélectionner, le gestionnaire Routage et accès distant devrait s'ouvrir automatiquement. Ici, nous allons configurer notre accès à distance en faisant un clic droit sur notre serveur local, puis en cliquant sur Configurer et activer le routage et l'accès à distance.



Bienvenue !
Cet Assistant vous aide à configurer votre serveur pour que vous puissiez vous connecter à d'autres réseaux et autoriser des connexions à partir de clients distants.
Cliquez sur Suivant pour continuer.
< Précédent Suivant Annuler

Dans cet Assistant d'installation nous pouvons faire Suivant sur la première page.

Assistant Installation d'un serveur Routage et accès distant

ance ou VPN) nnecter à ce serveur via une connexion d'accès à l'une connexion sécurisée à un réseau privé virtuel
nnecter à ce serveur via une connexion d'accès à l'une connexion sécurisée à un réseau privé virtuel
nnecter à Internet en utilisant une adresse IP publiqu
k) et NAT nnecter à ce serveur par Internet et les clients utilisant une seule adresse IP publique.
seaux privés istant tel que celui d'une succursale.
onctionnalités disponibles dans Routage et accès

Ensuite, sur la page configuration, nous allons sélectionner la Configuration personnalisée avant de faire Suivant.



Service VPN

Page 29 sur 55

Assistant Installation d'un serveur Routage et accès distant

électionnez l	es services q	ue vous voule	ez activer sur ce	serveur.		
🔽 Accè	VPN					
T Accè	s réseau à dis	stance				
Conn	exions <mark>à l</mark> a de	emande (utilisé	es pour le routa	ige au niv	eau d'une age	nce)
I NAT						
☐ Routa	ige réseau					
					0	

Sur la page Configuration personnalisée, nous allons sélectionner Accès VPN, puis cliquer sur Suivant.

Vous avez terminé l'Assistant Installation d'e routage et d'accès distant.	un serveur de
Résumé des sélections :	
Accès VPN	~
Configurez les services sélectionnés dans la et accès distant après avoir fermé cet Assis	a console Routage tant.
Pour fermer cet Assistant, cliquez sur Termir	ner.

Assistant Installation d'un serveur Routage et accès distant

Enfin, nous allons cliquer sur Terminer pour confirmer notre installation.



Service VPN

Page 30 sur 55

Routage et accès distant		
Démarrer le service		
Le service Routage et accès distan	t est prêt.	
	Démarrer le service	Annuler
	12	

Une fenêtre nous indiquant que le service est prêt au démarrage devrait s'ouvrir. Nous allons donc cliquer sur Démarrer le service.

Démarra	age de Gestion de l'accès à distance
Ð	Veuillez patienter pendant le démarrage du service Gestion de l'accès à distance sur .

Après un court chargement, notre service Routage et accès à distance devrait se lancer.



🚊 Routage et accès distant		_		×	r ₂
Fichier Action Affichage	?				
🗢 🔿 🖄 📰 🖾					
 Routage et accès distant Statut du serveur 	WIN-K6GK8KP0N9M (local)				
WIN-KOGKSKPUN9	Configurer et activer le routage et l'accès à distance	e es	t		lités
Ports	Désactiver le routage et l'accès à distance Activer DirectAccess	tant II	nstallation rter des		
Connexion et s	Toutes les tâches >	C)émarrer		
> <u>9</u> IPv4 > <u>9</u> IPv6	Affichage >	A	Arrêter		
<u>ن</u> الinéraires s	Supprimer Actualiser	R	leprendre ledémarrer		DL
	Propriétés	VPN p	our fourn	ir	
	Aide	-er part Acces	s en l'aide de		
<	 DirectAccess, les clients appartenant au domaine connecter de façon transparente à votre réseau o activer DirectAccess sur ce serveur, vous pouvez l'Assistant Activation de DirectAccess en sélection 	e peuve d'entrep z exécu nnant l'é	nt se prise. Pou ter pption	~	
Contient les opérations pouvant	être effectuées sur l'élément.				
•	Facilité de gestion (f) Facilité de	gestio	n		

Pour finaliser notre configuration du service, nous pouvons faire un clic droit sur notre serveur local puis cliquer sur Propriétés.







Propriété	s de : WIN	I-K6GK8	KPON91	VI (local)			?	×
Général	Sécurité	IPv4	IPv6	IKEv2	PPP	Enregia	strement	
Le fourr les clier	nisseur d'au its d'accès	uthentifica à distanc	ations va ce et les	alide les ir routeurs	formation de conne	s d'iden xion à la	tification demand	pour e.
Fourniss	seur d'auth	entificatio	ons :					
Auther	tification V	Vindows			•		onfigurer.	
Méth	nodes d'aut	thentificat	tion					
Le fourn connexi	isseur de c ons et des	comptes c sessions.	onserve	e un journ	al des der	mandes	de	
Fourniss	seur de cor	nptes :			_	1		-
Gestior	n des comp	otes Wind	ows		•		onfigurer.	
etre der authent	namé pour ifier ce sen priser la stra 1P/IKEv2	définir cel veur à l'ai atégie IPs	tte optio ide d'un iec pers	n. Les init certificat onnalisée	iateurs IK ne pourro pour les (Ev2 cor int pas s connexio	ntigurés p se connec ons	our cter.
Cie prep	banagee :	1						_
1234	6/891011							
Liaiso	n de certifi	cat SSL :						
	tiliser HTTF	Р						
Sélec Tunne	tionnez le o eling Protoc	certificat o col) doit u	que le se tiliser po	erveur SS our se lier	TP (Secu avec SSL	re Sock . (écoute	et eur Web)	
Certifi	cat: Pa	ar défaut			-	Affic	cher	
			(OK	Annu	ller	Appli	quer

Ici, nous allons nous intéresser à l'onglet Sécurité.

Pour notre TP nous avons décidé de mettre en place une clé pré-partagée pour sécuriser notre VPN.

Pour ce faire, il nous suffit de cocher la case Autoriser la stratégie IPsec personnalisée pour les connexions L2TP/IKEv2 et de taper la clé de notre choix dans le champ Clé prépartagée. (Il faudra mémoriser cette clé pour la renseigner par la suite sur le client VPN) Nous pouvons ensuite cliquer sur Appliquer.



A Pour ac	iver une stratég	in LOTD/IVEV2 p		
distanc	ons L2TP, vous d	levez redémarr	ersonnalis er Routage	ée pour des et accès à
unstante				

Une fenêtre devrait s'ouvrir pour nous demander de redémarrer le service, nous allons donc cliquer sur OK.

🦛 🤿 🛛 🚾			
🚊 Routage et acc	cès distant WIN-177M83DV3L8 (local) erveur		
> 🔂 WIN-177M	Configurer et activer le routage et l'accès à distance Désactiver le routage et l'accès à distance Activer DirectAccess	istance est t l'Assistant Installation pe. Pour apporter des électionnez un élément	1
	Toutes les tâches	Démarrer	
	Affichage >	Arrêter	
	Supprimer	Reprendre	
	Actualiser	Redémarrer	1
	Propriétés 🥑	serveur VPN pour fourni uvez tirer parti d'une	r
	Aide	a DirectAccess en ce serveur. À l'aide de	1
,	DirectAccess, les clients appartenant au connecter de façon transparente à votre activer DirectAccess sur ce serveur, vou l'Assistant Activation de DirectAccess en	domaine peuvent se réseau d'entreprise. Pour s pouvez exécuter sélectionnant l'option	

distance du serveur sélecti Redemarre le rou

Pour redémarrer le service et appliquer nos modifications, nous allons donc faire un clic droit sur notre serveur local, puis naviguer dans Toutes les tâches et cliquer sur Redémarrer.

Nous avons maintenant terminé de configurer le service Routage et accès distant.



4.3.4 Mise en Place d'Autorisations dans Gestion de l'Ordinateur

Afin d'assurer qu'un PC utilisant notre VPN soit capable de se connecter à l'un de nos utilisateurs, nous allons maintenant autoriser notre compte Administrateur local à être contrôlé à distance.



Pour ce faire, nous allons nous rendre dans le Gestionnaire de serveur, cliquer sur Outils, puis sur Gestion de l'ordinateur.



Gestion de l'ordinateur (local)	Nom Nom complet	Description	Actions
Outils système	🛃 Administrat	Compte d'utilisateur d'administra	Utilisateurs
 Planificateur de taches Observateur d'événements Obssiers partagés Utilisateurs et groupes locaux Utilisateurs et groupes locaux Oroupas Operformance Gestionnaire de périphériques Stockage Sauvegarde Windows Server Gestion des disques Services et applications 	VefaultAcco Nivité VDAGUtility	Compte utilisateur géré par le syst Compte d'utilisateur invité Compte d'utilisateur géré et utilis	Autres actions

Référence : TP-WSVPN-3123

Ici, nous allons développer le dossier Utilisateurs et groupes locaux en cliquant sur >, puis nous allons cliquer sur le sous-dossier Utilisateurs.



Windows Server

Version : 1.2

Windows Server

Gestion de l'ordinateur (local)	Nom	Nom complet	Descri	ption	Actions
 Qutils système Planificateur de tàches Observateur d'événements Obsiers partagés Utilisateurs et groupes locaux Utilisateurs Groupes Services et applications 	Administrateur DefaultAccount Invité WDAGUtilityAccou	Définir le mot de passe Toutes les tâches Supprimer Renommer Progriétés Aide		re d'utilisateur d'administra e utilisateur géré par le syst e d'utilisateur invité e d'utilisateur géré et utilis	Utilisateurs Autres actions Administrateur Autres actions

Pour notre TP, nous avons choisi de donner accès aux utilisateurs VPN à notre compte Administrateur local. Nous allons donc faire un clic droit sur Administrateur puis cliquer sur Propriétés.

	stance Profil	des services Bur	reau à distance	Appel entrant	Général	Membre de	Profil	Environnement	Sessi	ons
Général	Membre de	Profil	Environnement	Sessions 43	Contrôle à di	stance Pr	rofil des services E	lureau à distance	Appel entr	ant
Admi	nistrateur				Autorisation d Autoriser l' C Refuser l'a	'accès réseau 'accès 1				
lom complet :	l.				C Contrôler l	accès via la Straté	gie d'accès à dist	ance		
Description :	Compte d'utilis	sateur d'administr	ation		☐ Vérifier l'id	entité de l'appelant	:			1
L'utilisateur L'utilisateur Le mot de p Le compte e Le compte e	doit changer le mot de ne peut pas changer e asse n'expire jamais est désactivé est verrouillé	e passe à la proch de mot de passe	naine ouverture de se	ssion	Options de ray Pas de ray Défini par	ppel ppel l'appelant (service appeler :	de routage et d'ac	ccès à distance uniquen	nent)	
					Attribuer de	es adresses IP stati	ques			-
					Définissez les d'appel entra	s adresses IP à acti int.	iver pour cette cor	Adresses IF	⁾ statiques]
					Appliquer I	es itinéraires statiqu	Jes			_
					Définir les itin	Árairan à antivor po	ur catta connexio	n Itinárairae	statimues	1

Ici, nous allons ouvrir l'onglet Appel entrant puis cocher la case Autoriser l'accès et Appliquer.



Nous pouvons maintenant fermer cette fenêtre et passer à l'étape suivante : l'ouverture des ports.

4.3.5 Ouverture des ports L2TP

A présent, il ne nous reste plus qu'à configurer notre firewall pour laisser passer notre VPN. Pour ce faire, nous pouvons soit créer des règles dans l'interface graphique Windows Defender, soit taper la commande suivante dans PowerShell :

New-NetFirewallRule -DisplayName "VPNUDP" -Direction inbound -Profile Any -Action Allow -LocalPort 500, 1701, 4500 -Protocol UDP

Pour ajouter ces règles en interface graphique, nous pouvons ouvrir le Pare-feu Windows Defender en retournant dans le Gestionnaire de serveur, cliquer sur Outils puis sur Pare-feu Windows Defender avec fonctionnalités avancées de sécurité.





20

Pare-feu Windows Defender avec fonctions avancées de sécurité

e-feu Windows Defender av	Règles de trafic entrant					Actions
Règles de trafic entrant	1. Sm	Groupe	Profil	Activée	Action ^	Règles de trafic entrant
Règles de sécurité de conne	Gestion de l'accès à distance (DCOM-In)	Accès à distance	Tout	Oui	Autorise 2	Nouvelle règle
Analyse	🔮 Gestion de l'accès à distance (NP-In)	Accès à distance	Tout	Oui	Autoriser	V Filtrer nar profil
	Gestion de l'accès à distance (NPS-RPC-In)	Accès à distance	Tout	Oui	Autoriser	
	🔮 Gestion de l'accès à distance (RRAS-RPC	Accès à distance	Tout	Oui	Autoriser	Y Filtrer par état
	Gestion de l'accès à distance (Services-R	Accès à distance	Tout	Oui	Autoriser	Filtrer par groupe
	🔮 Gestion de l'accès à distance (WMI-In)	Accès à distance	Tout	Oui	Autoriser	Affichage
	Accès réseau COM+ (DCOM-In)	Accès réseau COM+	Tout	Non	Autoriser	
	Administration à distance COM+ (DCOM	Administration à distance C	Tout	Non	Autoriser	G Actualiser
	Agent de relais DHCPv4 [Client] (UDP-En	Agent de relais DHCP	Tout	Oui	Autoriser	Exporter la liste
	🔮 Agent de relais DHCPv6 [Serveur] (UDP-In)	Agent de relais DHCPv6	Tout	Oui	Autoriser	Aide
	Analyse de l'ordinateur virtuel (Demande	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	
	Analyse de l'ordinateur virtuel (Demande	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	
	Analyse de l'ordinateur virtuel (NB-Sessio	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	
	Analyse de l'ordinateur virtuel (RPC)	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	
	Analyse de l'ordinateur virtuel (Trafic entr	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	
	Règle entrante pour l'arrêt à distance (RP	Arrêt à distance	Tout	Non	Autoriser	
	Règle entrante pour l'arrêt à distance (TC	Arrêt à distance	Tout	Non	Autoriser	
	Découverte d'homologue de BranchCac	BranchCache - Découverte	Tout	Non	Autoriser	
	Extraction du contenu de BranchCache (BranchCache - Extraction d	Tout	Non	Autoriser	
	Serveur de cache hébergé de BranchCac	BranchCache - Serveur de c	Tout	Non	Autoriser	
	Bureau à distance - Mode utilisateur (TC	Bureau à distance	Tout	Non	Autoriser	
	Bureau à distance - Mode utilisateur (UD	Bureau à distance	Tout	Non	Autoriser	
	Bureau à distance - Contrôle à distance (Bureau à distance	Tout	Non	Autoriser	
	Bureau à distance - (TCP-WS-entrant)	Bureau à distance (WebSock	Tout	Non	Autoriser	
	Bureau à distance - (TCP-WSS-entrant)	Bureau à distance (WebSock	Tout	Non	Autoriser	
	🥨 Compte professionnel ou scolaire	Compte professionnel ou sc	Doma	Oui	Autoriser	
	Coordinateur de transactions distribuées	Coordinateur de transaction	Tout	Non	Autoriser	
	Coordinateur de transactions distribuées	Coordinateur de transaction	Tout	Non	Autoriser	
	Coordinateur de transactions distribuées	Coordinateur de transaction	Tout	Non	Autoriser Y	

Sur la partie gauche de la fenêtre nous allons cliquer sur Règles de trafic entrant puis cliquer sur Nouvelle règle.





Service VPN

Page 40 sur 55

Ici, nous allons sélectionner l'option Port puis cliquer sur Suivant.

🔗 Assistant Nouvelle règle	e de trafic entrant	×
Protocole et ports		
Spécifiez les protocoles et les p	ports auxquels s'applique cette règle.	
Étapes :		
Type de règle	Cette règle s'applique t-elle à TCP ou UDP ?	
Protocole et ports	О ТСР	
Action		
Profil		
Nom	Cette règle s'applique t-elle à tous les ports locaux ou à des ports locaux spécifiques ? Tous les ports locaux Ports locaux spécifiques : 500. 1701. 4500 Exemple : 80, 443, 5000-5010	
	< <précédent suivant=""> Annuler</précédent>	

Nous allons ensuite sélectionner UDP puis dans Ports locaux spécifiques, nous allons rentrer les ports suivants séparés de virgules : 500, 1701, 4500 et cliquer sur Suivant.

🔗 Assistant Nouvelle règ	le de trafic entrant	×
Action		
Spécifiez une action à entrepr	endre lorsqu'une connexion répond aux conditions spécifiées dans la règle.	
Étapes :		
Type de règle	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?	
Protocole et ports		
Action	Autoriser la connexion Cela comprend les connexions qui sont protégées par le protocole lPsec, ainsi que celles qui	
Profil	ne le sont pas.	
Nom	 Autoriser la connexion si elle est sécurisée Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion. Personnaliser. Bloquer la connexion 	
	< Précédent Suivant >	



w

Dans la page Action, nous allons vérifier que l'option Autoriser la connexion est sélectionnée et cliquer sur Suivant.

Assistant Nouvelle regi	le de tranc entranc	^
Profil		
Spécifiez les profils auxquels s	'applique cette règle.	
Étapes :		
Type de règle	Quand cette règle est-elle appliquée ?	
Protocole et ports		
Action	Domaine	
Profil	Lors de la connexion d'un ordinateur à son domaine d'entreprise.	
Nom	🗹 Privé	
	Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.	
	✓ Public	
	Lors de la connexion d'un ordinateur à un emplacement public.	
	< Précédent Suivant > Annuler	

Ici, nous pouvons laisser les options par défaut et cliquer sur Suivant.





Pare-feu Windows Defender av	Règles de trafic sortant					Ac	tions
Pare-feu Windows Defender av	Règles de trafic sortant Nom Agent de relais DHCPv4 [Client] (UDP-So À Agent de relais DHCPv6 [Serveur] (UDP Client de mise en cache hébergé de Bran Découverte d'homologue de BranchCac Extraction du contenu de BranchCacte (Serveur de cache hébergé de BranchCac Compte professionnel ou scolaire Coordinateur de transactions distribuées Cortana Expériences des utilisateurs connectés et Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Serveur de diffusion en continu sur un apreil (q Client de synchronisation de la gestion d Client de synchronisation de la gestion d Service d'inscription de gestion des périp Infrastructure de gestion Windows (WMI Lecteur Windows Media (UDP-Sortie) Lecteur Windows Media x86 (Trafic sorta	Groupe Agent de relais DHCP Agent de relais DHCP Agent de relais DHCPvô BranchCache - Client de mi BranchCache - Découverte BranchCache - Serveur de c Compte professionnel ou sc Cordinateur de transaction Cortana DiagTrack Expérience Windows Shell Fonctionnalité Diffuser sur u Fonctionnalité Diffuser sur u Fonctionnalité Diffuser sur u Fonctionnalité Diffuser sur u Fonctionnalité Diffuser sur u Gestion de carte à puce virt Gestion des périphériques Infrastructure de gestion Wi Lecteur Windows Media Lecteur Windows Media	Profil Tout Tout Tout Tout Tout Tout Tout Tout	Activée Oui Oui Non Non Non Oui Oui Oui Oui Oui Oui Oui Oui Oui Oui	Action Autoriser		tions sgles de trafic sortant Nouvelle règle Filtrer par profil Filtrer par groupe Affichage Actualiser Exporter la liste Aide
	mDNS (UDP-Sortie)	mDNS	Public Doma	Oui Oui	Autoriser Autoriser		
	mDNS (UDP-Sortie)	mDNS	Privé	Oui	Autoriser	~	

Enfin, nous devons donner un nom arbitraire à la règle et cliquer sur Terminer.

Développer: L'opération s'est terminée sans erreurs.

Nous pouvons maintenant cliquer sur Règles de trafic sortant puis sur Nouvelle règle.

Ici, nous allons reproduire les mêmes paramètres que pour la règle de trafic entrant (Ports ; UDP ; 500, 1701, 4500).

Il faudra cependant bien s'assurer que l'option Autoriser la connexion est sélectionnée dans la page Action.



Date : 06/05/24

Action		
Spécifiez une action à entrepre	ndre lorsqu'une connexion répond aux conditions spécifiées dans la règle.	
Étapes :		
Type de règle	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?	
Protocole et ports		
Action	Autonser la connexion Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui	
Profil	ne le sont pas.	
Nom	Cela comprend uniquement les connexions authentifiées à l'aide du protocole lPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles l'Psec du nœud Règle de sécurité de connexion. Pernonnaliser	
	< Précédent Suivant > Annuler	

Une fois nos 2 règles créées, nous avons donc fini de configurer notre VPN coté serveur. 4.4 Configuration du Client VPN sur Windows 10

4.4.1 Options VPN

Nous allons donc passer à la configuration du VPN sur notre client Windows 10. Une fois notre Windows 10 lancé, nous pouvons directement nous rendre dans les paramètres VPN pour configurer notre tunnel.

Pour ce faire, nous pouvons chercher VPN dans la barre de recherche Windows.









Il est aussi possible d'atteindre la configuration vpn en cliquant sur l'icône Notifications dans la barre de tâches puis sur l'icône VPN (vous aurez peut-être besoin de cliquer sur Développer pour voir toutes les icones)



Paramètres	- D ×
ம் Accueil	VPN
Rechercher un paramètre	+ Ajouter une connexion VPN
Réseau et Internet	
🗇 État	Options avancées
문 Ethernet	Activé
Accès à distance	Autoriser les connexions VPN en itinérance
% VPN	
™ Mode Avion	Paramètres associés
(۱۹) Point d'accès sans fil mobile	Modifier les options d'adaptateur
	Modifier les options de partage avancées
Proxy	Centre Réseau et partage
	Pare-feu Windows

Ici, il nous suffit de cliquer sur Ajouter une connexion VPN.

Enfin, nous devons remplir les informations suivantes puis cliquer sur Enregistrer :

Fournisseur VPN : Windows (intégré) Nom de la connexion : *nom arbitraire* Nom ou adresse du serveur : *adresse IPv4 du Windows Server* Type de réseau privé virtuel : L2TP/IPsec avec clé pré-partagée Clé pré-partagée : *clé pré-partagée créée sur Windows Server* Type d'informations de connexion : Nom d'utilisateur et mot de passe Nom d'utilisateur : Administrateur

Mot de passe : *mdp du compte Administrateur*



Service VPN

Page 47 sur 55

Une fois ces informations remplies, cette page devrait ressembler à cela :

Windows (intégré)		\sim			
n 987 W		_			
Nom de la connexion					
vpn					
Nom ou adresse du serveur					
192.168.					
lype de réseau privé virtuel					
L2TP/IPsec avec clé pré-partagée		\sim			
		_			
Clé pré-partagée					
•••••					
Type d'informations de connexion					
Nom d'utilisateur et mot de passe		~			
Nom d'utilisateur (facultatif)					
Administrateur	Ι				
		_			
Mot de passe (facultatif)					
••••••		0			
🗸 Mémoriser mes informations de con	nexion				



4.4.2 Connexion VPN

Pour utiliser notre VPN, nous pouvons maintenant retourner sur la page de configuration VPN, sélectionner le VPN que nous avons créé et cliquer sur Connecter.





Para	imètres		×
ல்	Accueil	VPN	
F	echercher un paramètre $ ho$	+ Ajouter une connexion VPN	
Ré	seau et Internet		
₿	État	Connecté	
臣	Ethernet	Options avancées Déconnecte	r
¶≣	Accès à distance	↓ Options avancées	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	VPN	Autoriser les connexions VPN sur des réseaux limités	
цЪ	Mode Avion	Activé	
6.5		Autoriser les connexions VPN en itinérance	
(db)	Point d'accès sans fil mobile	Activé	
⊕	Proxy		
		Paramètres associés	
		Modifier les options d'adaptateur	
		Modifier les options de partage avancées	

Après un cours chargement, le message Connecté devrait s'afficher en dessous du VPN utilisé.

Nous venons ainsi de créer un tunnel VPN permettant à nos deux machines virtuelles de communiquer de façon sécurisée à travers Internet.



## 4.5 Vérification de l'Installation

Afin de vérifier le bon fonctionnement de notre VPN nous allons maintenant utiliser plusieurs outils pour diagnostiquer notre réseau VPN.

### 4.5.1 Vérification Côté Client

Une fois que notre VPN annonce qu'il est connecté sur notre client Windows 10, nous pouvons vérifier cette connexion grâce à la commande ipconfig.



Pour ce faire, nous allons ouvrir l'invite de commandes en tapant cmd dans la barre de recherche Windows, puis en cliquant sur l'application Invite de commandes.





Une fois l'invite de commande ouvert, nous allons taper la commande ipconfig puis appuyer sur la touche Entrée pour exécuter la commande.

📾 Administrateur : Invite de commandes	<u></u>	×
C:\Windows\system32>ipconfig		^
Configuration IP de Windows		
Carte Ethernet Ethernet0 :		
Suffixe DNS propre à la connexion.       :         Adresse IPv6.       .         Adresse IPv6 temporaire       .         Adresse IPv6 de liaison locale.       :         Adresse IPv6.       .         Passerelle par défaut.       .         192.168.       .		
Carte PPP vpn :		
Suffixe DNS propre à la connexion : Adresse IPv4		
Carte Ethernet Connexion réseau Bluetooth :		
Statut du média Média déconnecté Suffixe DNS propre à la connexion :		
C:\Windows\system32>		~

Si VPN est bien connecté, les informations suivantes devraient s'afficher :

- Carte Ethernet suivi de notre adresse IP locale
- Carte PPP vpn suivi de notre adresse IP vpn

Ici, nous pouvons voir que nous avons bien ces deux adresses IP sur deux cartes réseaux différentes. Nous pouvons donc en conclure que notre VPN est bien connecté.



Service VPN

Page 52 sur 55

Windows Server

### 4.5.2 Vérification Côté Serveur

Pour finir, nous allons vérifier que notre serveur VPN est bien capable d'identifier les clients VPN auxquels il est connecté.

🧕 Routage et accès distant							o ×
Fichier Action Affichage ?							
🗢 🏟 🖄 📆 🙆 📾 🕅							
🚊 Routage et accès distant	Clients d'accès distant (1)						
📑 Statut du serveur	Nom d'utilisateur	Durée	Nombre de ports	Statu	t		
WIN-IETMBPRIBOQ (local)	WIN-IETMBPRIB0Q\Administrateur	00:00:58	1	Non	compa		
Ports	Statut			?	×		
<ul> <li>〇 Connexion et stratégies d'ac</li> <li>○ 印 Pv4</li> <li>○ 印 Pv6</li> <li>○ Général</li> <li>○ Itinéraires statiques</li> </ul>	Connexion : Administr Durée : 00:01:26 Statistiques Octets entrants Trames entrantes Compression en entrée Eneurs CRC : Délai : Alignement : Enregistrement sur le ré Adresse IP : Adresse IP : Adresse IP : Adresse IP :	8 536 116 0 0 0 seau <u>192</u> liser   R	Octets sortants Trames sortantes Compression en sortie Trames : Dépassements maté Saturation du tarr Lo 168	1 535 29 0% 0 0 0	mer		
۲ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲							

Pour ce faire, nous allons retourner dans le service Routage et accès distant.

Ici, nous allons simplement cliquer sur le dossier Clients d'accès distant (1), puis vérifier que notre client Windows 10 est bien dedans. Nous pouvons même cliquer sur notre client pour avoir plus d'informations sur le compte et l'adresse IP utilisés pour établir cette connexion.

Dans notre cas, nous pouvons voir que l'utilisateur affiché correspond bien au client VPN que nous avons configuré. Nous pouvons donc en conclure que la connexion VPN entre notre client et notre serveur est bien établie.



Service VPN

Date : 06/05/24

# **5** Sources

https://blog.avast.com/fr/windows-server-vs-windows-quelle-est-la-difference https://learn.microsoft.com/en-us/windows/win32/srvnodes/windows-server https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-vpninwindows-server-essentials https://learn.microsoft.com/fr-fr/windowsserver/remote/remote-access/get-startedinstall-ras-as-vpn?tabs=powershell https://learn.microsoft.com/fr-fr/windows-server/remote/remote-access/tutorialaovpndeploy-setup https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-onwindows-server-2019/#:~:text=A%20VPN%20or%20Virtual%20Private,connected%20over%20a%20private% 20network. https://www.expressvpn.com/what-is-vpn/protocols/pptp https://www.okta.com/identity-101/pap-security/ https://docs.oracle.com/cd/E56338 01/html/E53884/pppsvrconfig.reference-21.html https://www.tutorialspoint.com/challenge-handshake-authentication-protocol-chap https://learn.microsoft.com/fr-fr/windowsserver/networking/technologies/extensibleauthentication-protocol/network-access https://en.wikipedia.org/wiki/Extensible Authentication Protocol https://supporthost.in/how-to-setup-l2tp-vpn-on-windows-server-2019/ https://www.vpnmonami.com/vpn-pour-les-nuls/ https://www.levpn.com/fr/pptp/#:~:text=Protocole%20PPTP%20Le%20Protocole%20PPTP%20%28de%20l% E2%80%99anglais%20Point-to-Point.un%20tunnel%20GRE%20pour%20encapsuler%20des%20paguets%20PPP https://fr.wizcase.com/blog/les-protocoles-de-securite-vpn-expliques-comprendrelepptp/#:~:text=PPTP%20est%20%C3%A9conomique.-,Inconv%C3%A9nients,PPTP%20n'est%20pas%20recommand%C3%A9 http://www.ordinateur.cc/r%C3%A9seaux/R%C3%A9seau-Internet/67354.html https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/pptp https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-gre-tunneling/ https://4sysops.com/archives/how-to-setup-an-sstp-vpn-server-with-windows-server/ https://www.purevpn.fr/blog/openvpn-vs-sstp-

vpn/#:~:text=Mais%20si%20vous%20%C3%AAtes%20un,pas%20sur%20les%20appareils%20 mobiles

Windows Server

Service VPN

Page 54 sur 55



https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/l2tp https://www.bicomm.fr/livebox-

v3-redirection-de-ports-vpn-l2tp-ipsec/

https://www.vpnmonami.com/quest-ce-que-

<u>I2tp/#:~:text=L'acronyme%20L2TP%20signifie%20Layer,priv%C3%A9%20sur%20des%20r%C</u> <u>3%A9seaux%20publics</u> <u>https://rdr-it.com/serveur-vpn-windows-server-installation-</u>

configuration/4/ https://informerick.com/tutoriels-informatique/creer-vpn-server-

windows/#:~:text=En%20bref%2C%20c'est%20un,Allez%20dans%20les%20param%C3%A8tr es%20Windows https://4sysops.com/archives/how-to-setup-an-sstp-vpn-server-withwindows-server/

