

Projet de BTS Maison des Ligues

Présentation du projet MDL	2
Schéma réseau du laboratoire de test	2
Mission 1 : Installation du routeur-pare-feu PfSense	3
Interfaces réseau de Pfsense	3
Mission 2 - Création du domaine et d'utilisateurs	3
Ajout d'un répertoire personnels pour les utilisateurs	4
Ajout d'un utilisateur à un groupe	4
Mission 3 - GLPI	5
Installation PHP	5
Installation de Fusion Inventory	6
Connexion à l'annuaire LDAP	7
Mission 4 - Installation OpenVPN	8
Création d'une entité de certificats	8
Création d'un certificat serveur	9
Création de l'utilisateur OpenVPN	10
Création d'une autorisation d'authentification avec LDAP au SERVEUR1	10
Création du service OPENVPN sur Pfsense	12
Test de connexion	15
Modification de l'interface WAN	16
Modification du serveur DNS de Pfsense	16
Téléchargement du client OPENVPN et configuration	17
Mission 5 : Bureau à distance	18
Installation des rôles Bureau à distance	18
Installation Packet Tracer sur SERVEUR1	19
Deployment Application RemoteApp	19
Modification des paramètres d'affectations utilisateurs	20
Mission 6 : Cluster PFSense	21
Modification IP des interfaces	21
Paramétrage du cluster	22
Création de l'IP virtuelle pour l'interface LAN	23
Création de l'IP virtuelle pour l'interface DMZ	23
Configuration de la haute disponibilité	24
High Availability sur Pfsense Maître	24
High Availability sur Pfsense Esclave	25
Modification des règles de pare feu pour l'interface PFSYNC	26
Vérification du statut de la synchronisation	26

Présentation du projet MDL

Le projet MDL est une simulation de cas d'entreprise, il permet d'apprendre la mise en place d'une infrastructure d'entreprise.

Ce projet est constitué de différentes missions qui permettent d'apprendre la gestion d'un parc informatique, d'un Active directory et la mise en redondance de matériels.

Mission 1 : Installation du routeur-pare-feu PfSense

Mission 2 : Installation du serveur de domaine

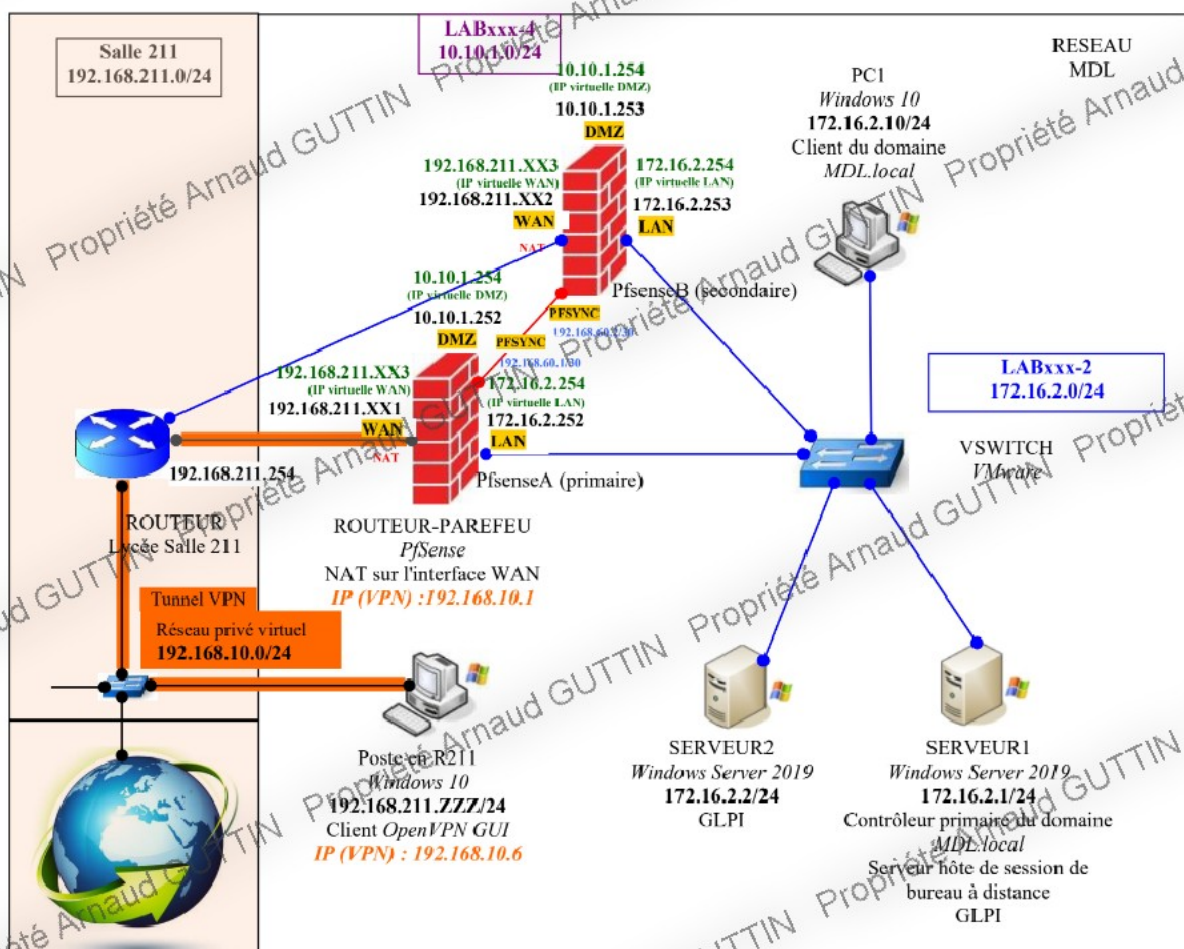
Mission 3 : Inventaire du matériel avec GLPI/FusionInventory

Mission 4 : Installation d'un VPN

Mission 5 : Installation d'un serveur hôte de session Bureau à distance

Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

Schéma réseau du laboratoire de test



Mission 1 : Installation du routeur-pare-feu PfSense

Interfaces réseau de Pfsense

Interface physique	Interface Logique	MAC@	N° Adaptateur réseau	Etiquette réseau
vmx0	WAN	00:50:56:90:ec:7d	4	Salle 211
vmx1	LAN	00:50:56:90:4c:e5	1	LAB-SISR-5-2
vmx2	OPT1 (DMZ)	00:50:56:90:20:98	2	LAB-SISR-5-4
vmx3	OPT2 (pfsync)	00:50:56:90:66:31	3	LAB-SISR-5-3

Mission 2 - Création du domaine et d'utilisateurs

Pour créer un domaine, il faudra ajouter le rôle Active Directory (ADDS).
On créera ensuite le domaine, ici MDL.local.

On ajoutera la liste des utilisateurs suivant:

Nom et prénom	Nom d'ouverture de session	Nom du dossier personnel	Mot de passe
Clément Ogier	cogier	cogier	Windows2019
Laure Dubreuil	ldubreuil	ldubreuil	Windows2019
Sylvie Pommier	spommier	spommier	Windows2019
Kevin Dalle	kdalle	kdalle	Windows2019

Pour la création d'un utilisateur on ouvre Utilisateurs et Ordinateurs Active Directory. On clique sur ajouter un utilisateur puis on rentre ses informations.

Ajout d'un répertoire personnels pour les utilisateurs

Pour attribuer un répertoire personnel à un utilisateur, il faudra se rendre dans l'onglet profil, puis mettre le chemin de partage au dossier de base, (exemple ci-dessous).

Ajout d'un utilisateur à un groupe

On ajoutera les utilisateurs aux groupes suivants:

Nom de groupe	Membres du groupe
LigueFootball	Clément Ogier Laure Dubreuil
LigueBasket	Sylvie Pommier Kevin Dalle

Pour ajouter un utilisateur à un groupe il faudra créer un groupe ou utiliser un groupe existant puis cliquer sur Ajouter des membres.

Nouvel objet - Groupe

Créer dans : MDL.local/Users

Nom du groupe :
LigueFootball

Nom de groupe (antérieur à Windows 2000) :
LigueFootball

Étendue du groupe

☒ Domaine local
☐ Globale
☐ Universelle

Type de groupe

☒ Sécurité
☐ Distribution

OK Annuler

Mission 3 - GLPI

Installation PHP

Pour mettre en place un serveur web avec PHP, il faudra installer le rôle IIS. Il faudra aussi installer PHP Manager de chez Microsoft. On mettra le répertoire PHP à la racine du disque.

On ajoutera les extensions nécessaires à GLPI, (voir exemple ci-dessous).

PHP Extensions

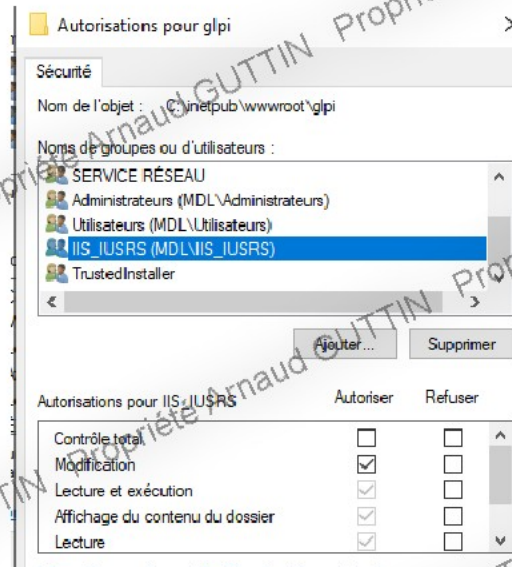
PHP extensions provide additional functionality to PHP. To configure PHP extensions settings, click on the 'Configure' button.

Filtrer : Atteindre

Name	State
Enabled	
php_curl.dll	Enabled
php_fileinfo.dll	Enabled
php_gd.dll	Enabled
php_gd2.dll	Enabled
php_gettext.dll	Enabled
php_imap.dll	Enabled
php_intl.dll	Enabled
phpldap.dll	Enabled
php_mysqli.dll	Enabled
php_openssl.dll	Enabled
php_soap.dll	Enabled
php_xmlrpc.dll	Enabled

On placera le dossier GLPI dans le répertoire C:\inetpub\wwwroot\glpi.

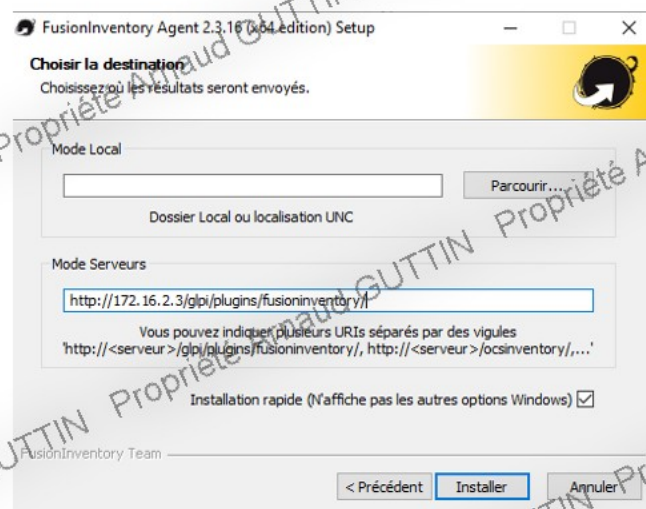
L'application GLPI a besoin d'autorisations pour fonctionner correctement, il faudra donc mettre les droits d'écriture sur le dossier dans C:\inetpub\wwwroot\glpi à l'utilisateur IIS_USERS.



Installation de Fusion Inventory

Fusion Inventory est agents permettant de transmettre les informations de statut d'une machine à un serveur (ici GLPI).

Il faudra exécuter Fusioninventory sur chaque machine, puis il faut indiquer le lien ci-dessous. Cela va indiquer à l'agent où il doit envoyer les données.



Connexion à l'annuaire LDAP

Sur l'interface web de GLPI il faudra se rendre sur l'onglet Authentification puis Annuaire LDAP. Cela va permettre de connecter GLPI à notre annuaire Active Directory.

Nouvel élément - Annuaire LDAP

Préconfiguration **Active Directory** / Valeur(s) par défaut

Nom	SERVEUR1		
Serveur par défaut	Oui	Actif	Oui
Serveur	172.16.3.2	Port (par défaut 389)	389
Filtre de connexion	(&(objectClass=user)(objectCategory=person)(userAccountControl:1.2.840.113556.1.4.803:=2)))		
BaseDN	CN=Users,DC=MDL,DC=local		
DN du compte (pour les connexions non anonymes)	CN=Administrateur,CN=Users,DC=MDL,DC=local		
Mot de passe du compte (pour les connexions non anonymes)	*****		
Champ de l'identifiant	samaccountname	Commentaires	
Champ de synchronisation			

Ajouter

Mission 4 - Installation OpenVPN

Création d'une entité de certificats

Sur Pfsense, il faudra créer une autorité de certification. Celle-ci va permettre de créer les certificats pour la connexion VPN.

Pour ce faire, il faudra aller dans System, puis Certificats et Autorité.
On remplira les informations ci-dessous.

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name CA_Acces_VPN
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ? * & % ' " \ , : ;

Method Create an internal Certificate Authority

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the OS.

Randomize Serial ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA
The length to use when generating a new RSA key.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

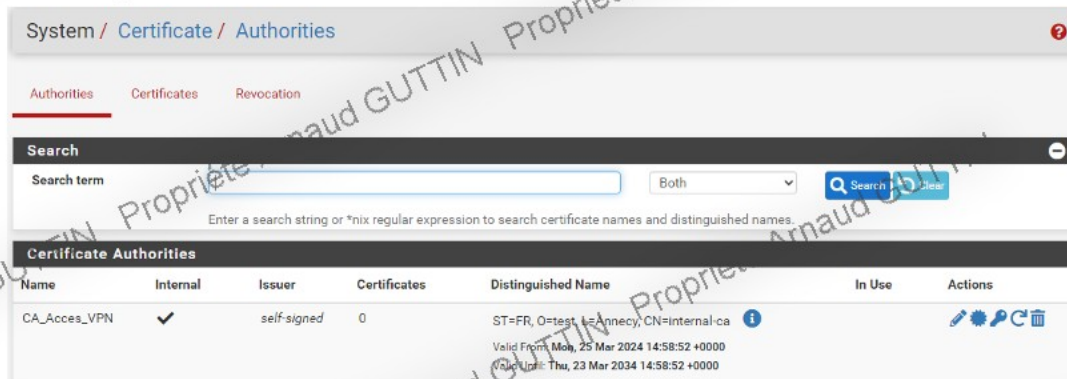
Digest Algorithm sha256
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server, may not support older algorithms and will be invalid.

Lifetime (days) 3650

Common Name CA_Acces_VPN

The following certificate authority subject components are optional and may be left blank.

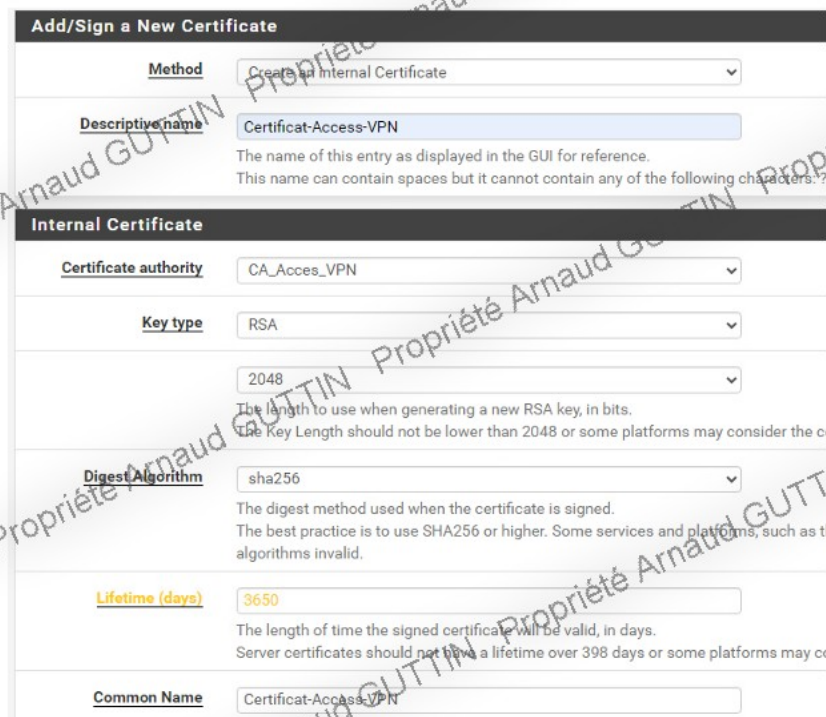
On peut voir que notre autorité de certifications est bien créée.



System / Certificate / Authorities						
Authorities Certificates Revocation						
Search						
Search term Both Search Clear						
Enter a search string or *nix regular expression to search certificate names and distinguished names.						
Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_Acces_VPN	✓	self-signed	0	ST=FR, O=test, CN=internal-ca Valid From: Mon, 25 Mar 2024 14:58:52 +0000 Valid Until: Thu, 23 Mar 2024 14:58:52 +0000		

Création d'un certificat serveur

Pour la communication VPN, il faut créer un certificat serveur. Pour ce faire, on va cliquer sur Créer un certificat et entrer les informations ci-dessous.



Add/Sign a New Certificate

Method Create an Internal Certificate

Descriptive name Certificat-Access-VPN
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?

Internal Certificate

Certificate authority CA_Acces_VPN

Key type RSA

Key length 2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the c

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as t
algorithms invalid.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may c

Common Name Certificat-Access-VPN

Certificate Attributes

Attribute Notes
The following attributes are added to certificates and requests when they are created or selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type
Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions.

Alternative Names
FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added by the signing CA and may not be changed.

Add SAN Row
+ Add SAN Row

Save

Création de l'utilisateur OpenVPN

Pour la connexion VPN, il faudra créer un utilisateur sur l'Active Directory, on appellera cet utilisateur, User_VPN_LDAP.

Création d'une autorisation d'authentification avec LDAP au SERVEUR1

Pour que les utilisateurs puissent se connecter avec leur identifiant de l'Active Directory, il faut créer une autorisation de connexion serveur avec l'annuaire LDAP. On va aller dans Gestion des utilisateurs, puis Authentification Serveurs, enfin on va entrer les informations ci-dessous.

System / User Manager / Authentication Servers / Edit

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name
Serveur AD MDI

Type
LDAP

LDAP Server Settings

Hostname or IP address
129.0.2.1
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server's SSL/TLS Certificate.

Port value
389

Transport
Standard TCP

Peer Certificate Authority
CA_Acces_VPN
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version
3

Server Timeout
25
Timeout for LDAP requests (seconds)

Search scope
Level 1 only

Base DN
DC=MDLDC-local

CN=
CN=Users DC=MDI DC-local

Base DN
DC=MDL,DC=local

Authentication containers
CN=Users,DC=MDL,DC=local [Select a container](#)

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing the full component.
Example: CN=Users,DC=example,DC=com or CN=Staff,OU=Freelancers

Extended query ☐ Enable extended query

Bind anonymous ☐ Use anonymous binds to resolve distinguished names

Bind credentials
CN=Users,DC=MDL,DC=local

Initial Template
OpenLDAP

User naming attribute
samAccountName

Group naming attribute
cn

Group member attribute
member

RFC 2307 Groups ☐ LDAP Server uses RFC 2307 style group membership.
RFC 2307 style group membership has membership listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class
posixGroup
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attribute to be able to login.
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode ☐ UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP server.

Username Alterations ☐ Do not strip away parts of the username after the @ symbol

Dans Settings, on précisera Authentication Server comme Serveur AD MDL.

System / [User Manager](#) / [Settings](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Settings

Session timeout
Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire session risk!

Authentication Server

Password Hash Algorithm
Selects which algorithm the firewall will use when creating hashes for local user passwords.
The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compatibility.

Shell Authentication ☐ Use Authentication Server for Shell Authentication
If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used.
To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first.
To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration

Auth Refresh Time
Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent authentication server requests.

[Save](#) [Save & Test](#)

Création du service OPENVPN sur Pfsense

On va ensuite créer le service OpenVPN sur le routeur Pfsense.

Pour ce faire, on va se rendre dans OpenVPN → Aller dans VPN → OpenVPN → Wizards, puis on entrera les valeurs ci-dessous.

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server:

NOTE: If unsure, leave this set to "Local User Access."

>> Next

Wizard / OpenVPN Remote Access Server Setup / LDAP Server Selection

Step 1 of 11

LDAP Server Selection

OpenVPN Remote Access Server Setup Wizard

LDAP Authentication Server List

LDAP servers:

>> Add new LDAP server >> Next

Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority:

>> Add new CA >> Next

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate

Certificat-Access-VPN

>> Add new Certificate

>> Next

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Description

Serveur VPN LDAP MDL

A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Endpoint Configuration

Protocol

UDP on IPv4 only

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Interface

WAN

The interface where OpenVPN will listen for incoming connections (typically WAN.)

Local Port

1196

Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Cryptographic Settings

TLS Authentication

☒ Enable authentication of TLS packets.

Generate TLS Key

☒ Automatically generate a shared TLS authentication key.

TLS Shared Key

Paste in a shared TLS key if one has already been generated.

Tunnel Settings

IPv4 Tunnel Network

192.168.10.0/24

This is the virtual network used for private communication between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client generated traffic through the tunnel.

IPv4 Local Network

172.16.2.0/24

This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance, which is potentially insecure.

Compression

Disable Compression [Omit Preference]

Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

Type-of-Service

☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Inter-Client Communication

☐ Allow communication between clients connected to this server.

Duplicate Connections

☐ Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.

Duplicate Connection Limit

Limit the number of concurrent connections from the same user.

Client Settings

Dynamic IP

☒ Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet - One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Advanced Client Settings

DNS Default Domain

MDL.local

Provide a default domain name to clients.

DNS Server 1

172.168.2.1

DNS server IP to provide to connecting clients.

DNS Server 2

DNS server IP to provide to connecting clients.

DNS Server 3

DNS server IP to provide to connecting clients.

DNS Server 4

DNS server IP to provide to connecting clients.

NTP Server

Network Time Protocol server to provide to connecting clients.

NTP Server 2

Network Time Protocol server to provide to connecting clients.

NetBIOS Options

☐ Enable NetBIOS over TCP/IP

If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

NetBIOS Node Type

none

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule	
☒ Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.	

Traffic from clients through VPN

OpenVPN rule	
☒ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.	

[» Next](#)

Test de connexion

Pour tester le bon fonctionnement du serveur OpenVPN, il est possible de se rendre dans Diagnostics puis Authentication, puis entrer un utilisateur de l'Active Directory.

Diagnostics / Authentication

User kdalle authenticated successfully. This user is a member of groups:

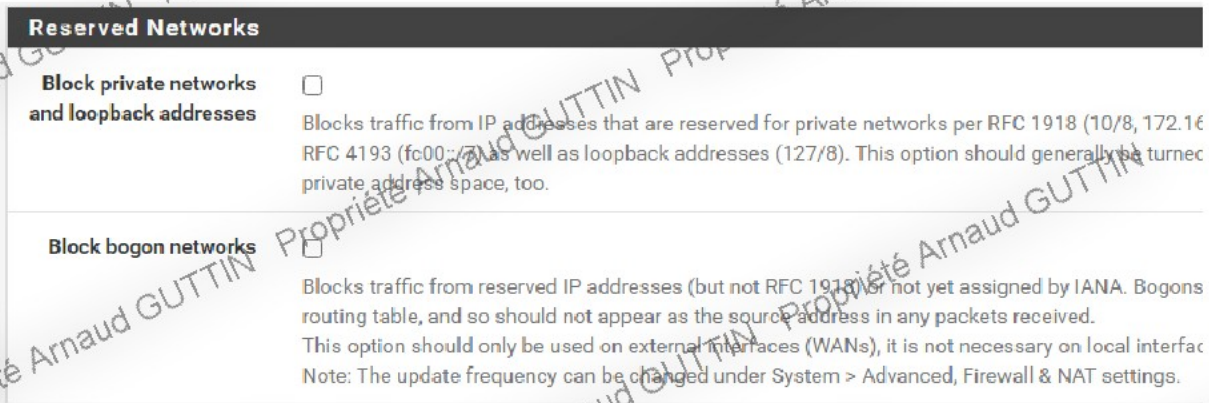
Authentication Test

Authentication Server	Serveur AD MDL Select the authentication server to test against.
Username	kdalle
Password	*****
Debug	☐ Set debug flag Sets the debug flag when performing authentication, which may trigger additional diagnostic

[Test](#)

Modification de l'interface WAN

Sur l'interface WAN, il faudra désactiver les deux cases, elles permettront de laisser la connexion entrante depuis l'extérieur.



Reserved Networks

Block private networks and loopback addresses ☐

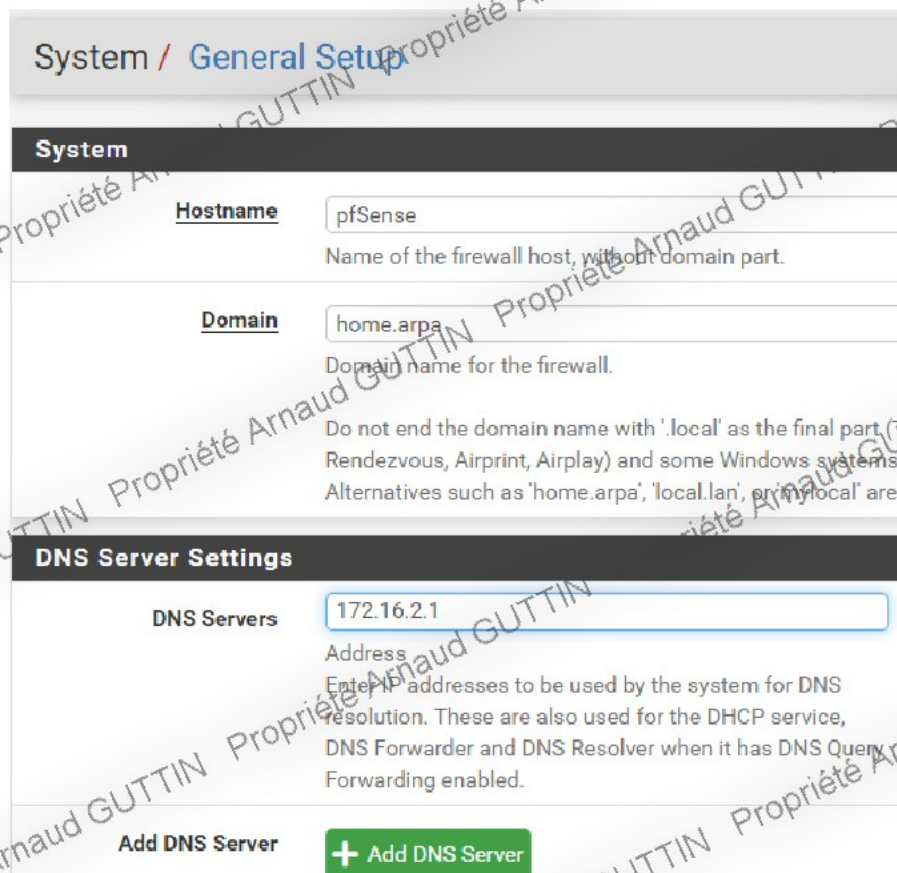
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/24) as well as loopback addresses (127/8). This option should generally be turned on for external interfaces (WANs), it is not necessary on local interfaces (LANs).

Block bogon networks ☐

Blocks traffic from reserved IP addresses (but not RFC 1918 or not yet assigned by IANA. Bogons are not in the routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces (LANs). Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Modification du serveur DNS de PfSense

Il faudra modifier le serveur DNS de PfSense et mettre l'adresse IP du Serveur1.



System / General Setup

System

Hostname pfSense
Name of the firewall host, without domain part.

Domain home.arpa
Domain name for the firewall.
Do not end the domain name with '.local' as the final part (e.g. 'home.local', 'Rendezvous', 'Airprint', 'Airplay') and some Windows systems (e.g. 'home.local') are not compatible with it. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are recommended.

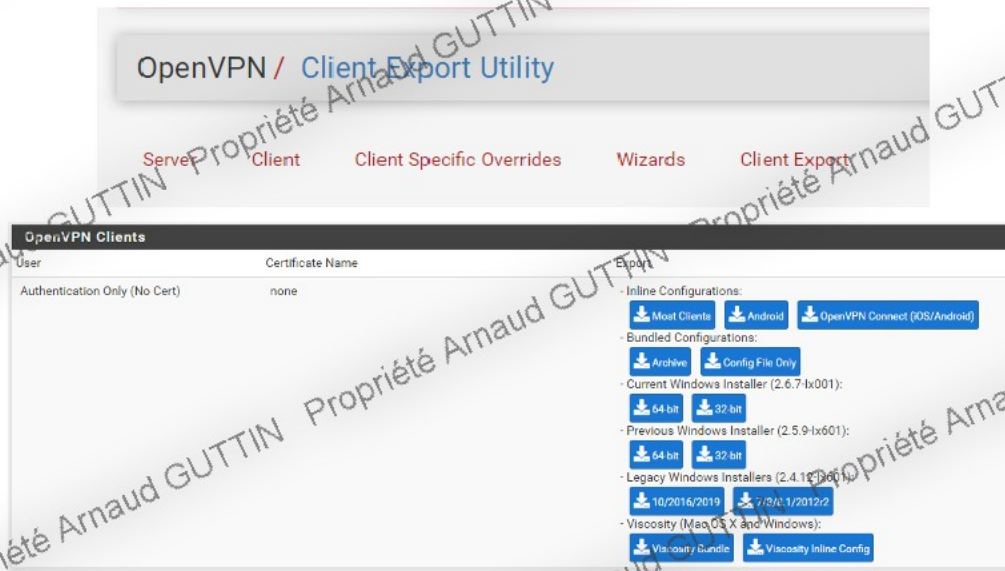
DNS Server Settings

DNS Servers 172.16.2.1
Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

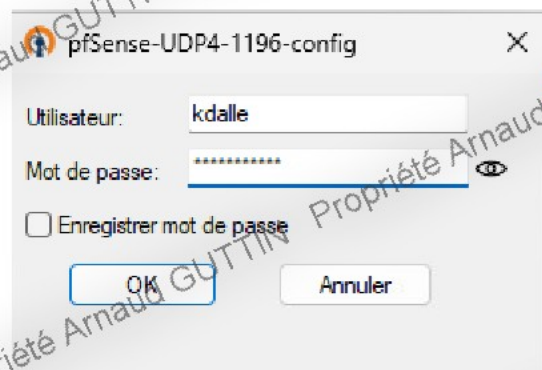
Add DNS Server + Add DNS Server

Téléchargement du client OPENVPN et configuration

Pour télécharger le client OpenVPN qu'il faudra exécuter sur les postes informatiques voulant se connecter en VPN, il faut se rendre dans OpenVPN, puis Client export. Il faudra télécharger la version correspondant à votre système d'exploitation (ici Windows Installer 64 bits).



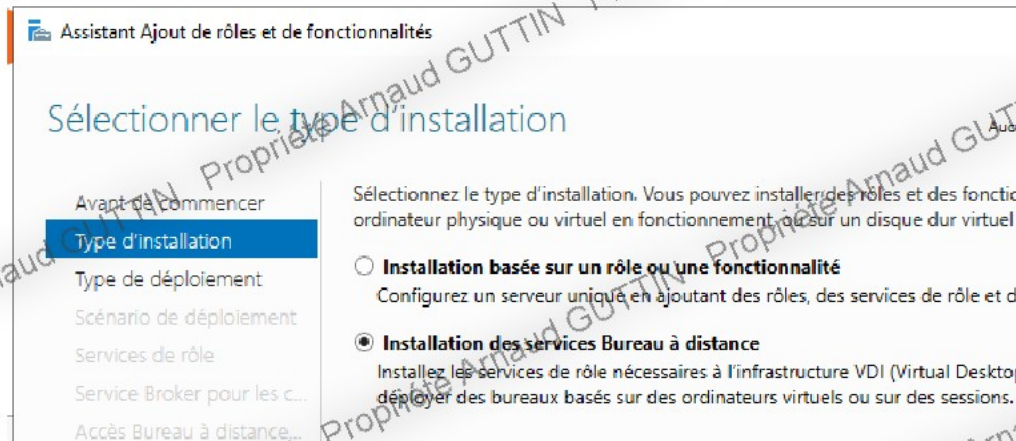
Vous pouvez ensuite tester la connexion VPN à distance.



Mission 5 : Bureau à distance

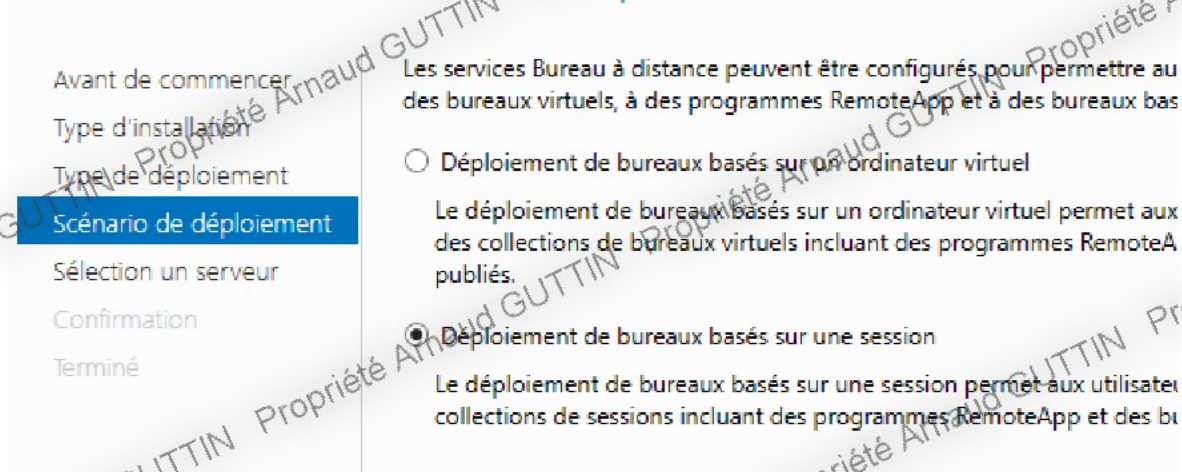
Installation des rôles Bureau à distance

Pour utiliser le service Bureau à distance, il faudra installer le rôle, dans type d'installation, il faudra cliquer sur Installation des Services Bureau à distance, (voir ci-dessous).



On choisit ensuite, Déploiement de bureaux sur une session.

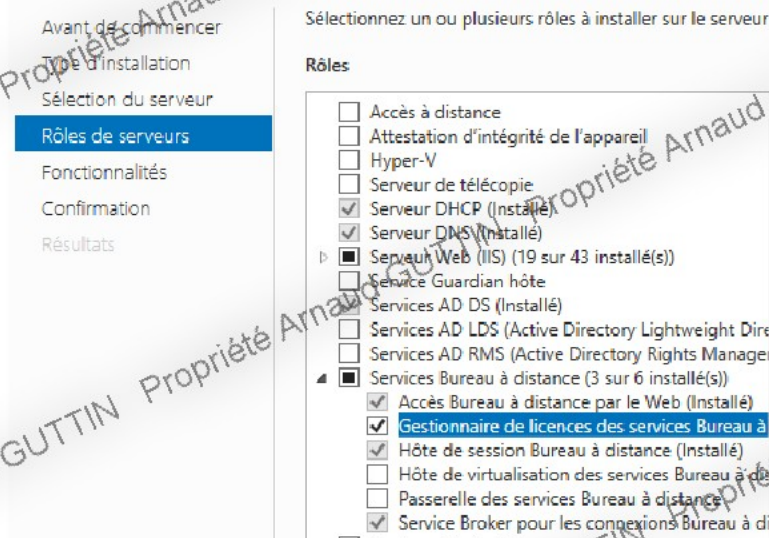
Sélectionner le scénario de déploiement



Le redémarrage se fera automatiquement.

Il faudra aussi installer le rôle Gestionnaire de licences des services bureaux à distance, (voir ci-dessous).

Sélectionner des rôles de serveurs



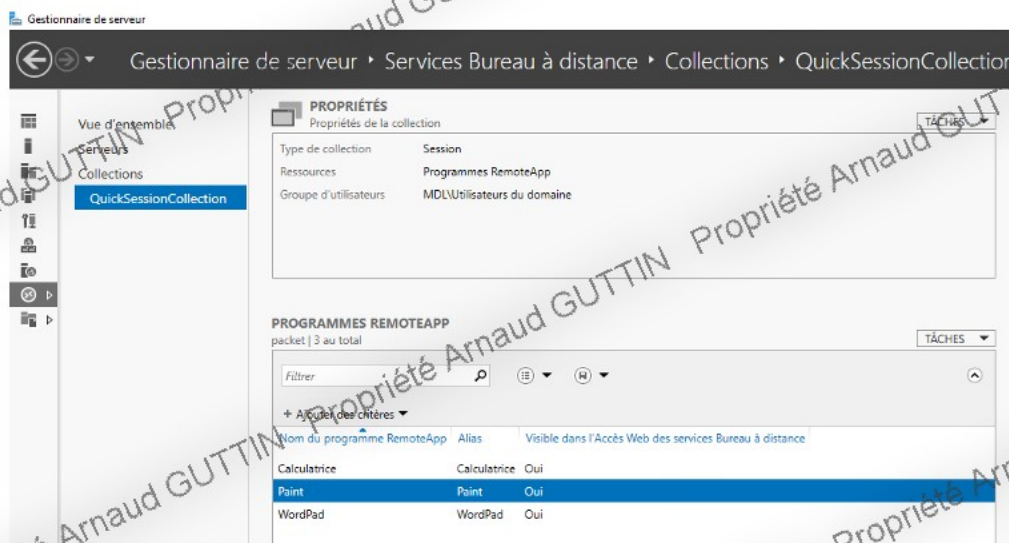
Installation Packet Tracer sur SERVEUR1

Pour installer Packet Tracer sur le Serveur1, il faudra exécuter le fichier .exe.

Deployment Application RemoteApp

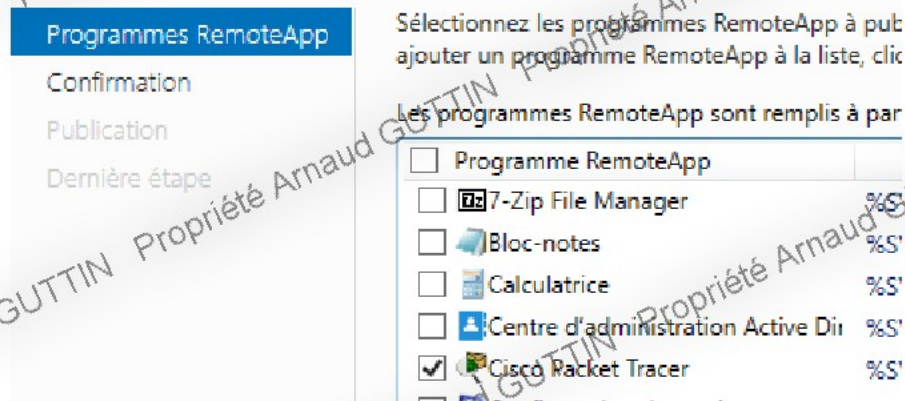
Pour déployer le logiciel Packet Tracer, il faudra se rendre sur le Gestionnaire de Serveur dans Services de bureaux à distance.

Dans Quick Session Collection vous pouvez apercevoir les outils déployés dans Bureaux à distance.



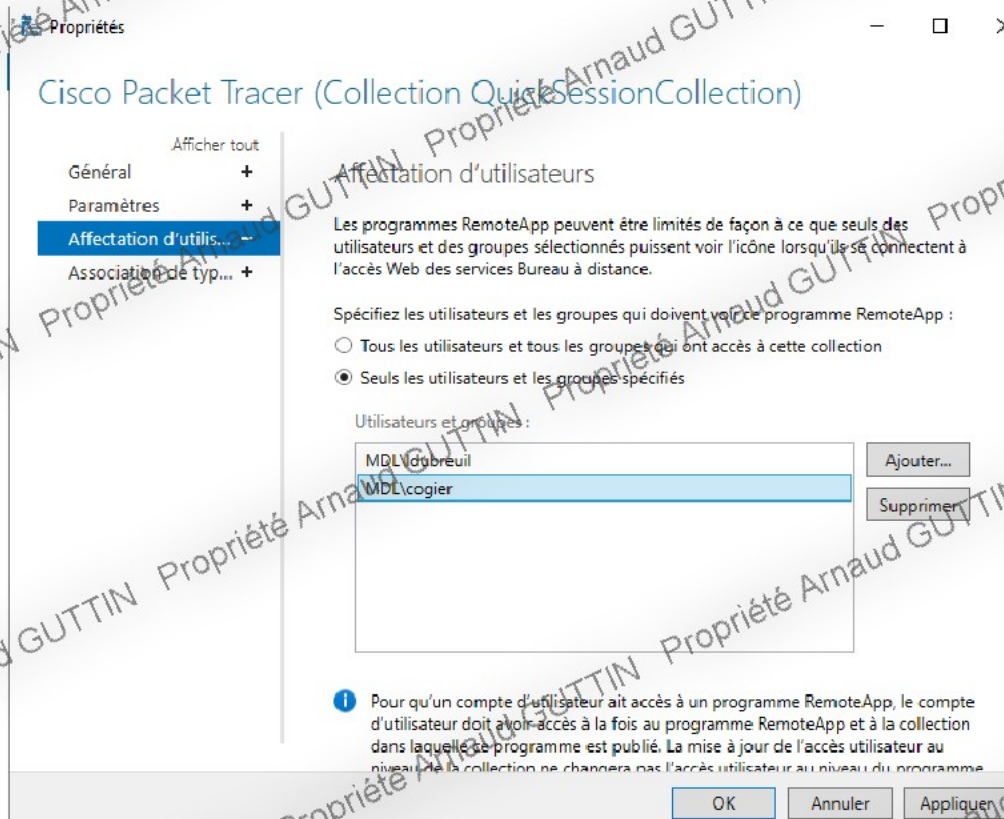
Pour publier de nouveaux logiciels tels que Packet Tracer, il faut cliquer sur le bouton Tache puis Publier des programmes RemoteApp, enfin, on sélectionne le programme souhaité.

Sélectionner les programmes RemoteApp



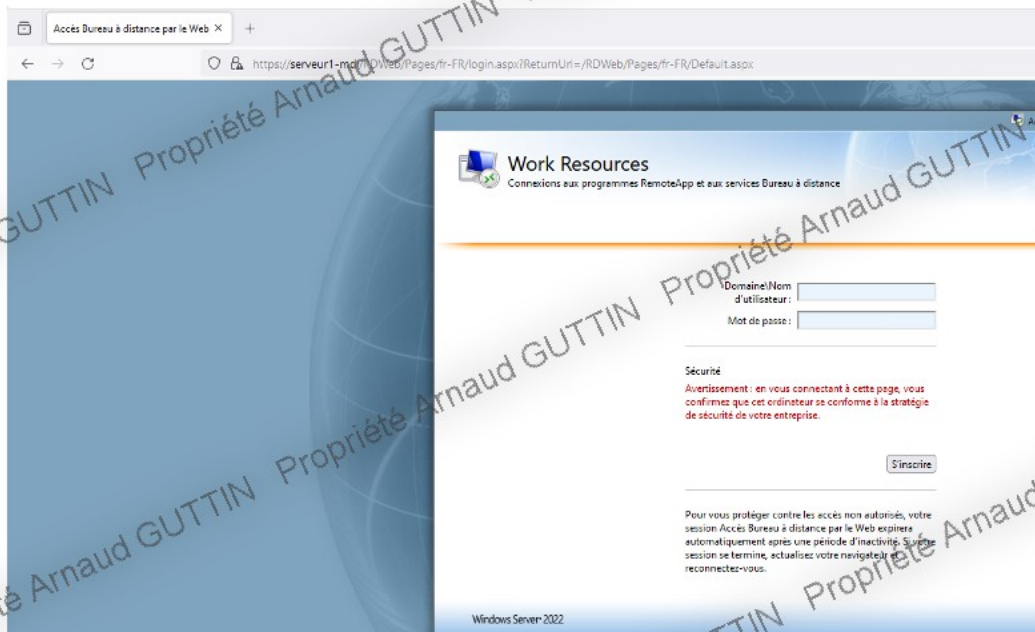
Modification des paramètres d'affectations utilisateurs

Il est possible de choisir à quels utilisateurs est affecté un déploiement.

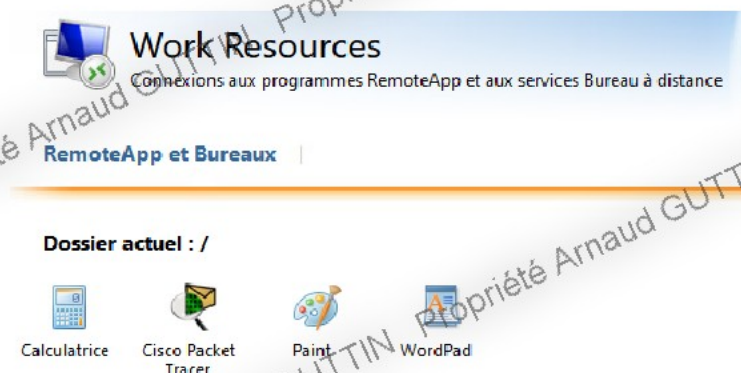


Pour vous connecter au service de bureaux à distance, il faudra se rendre sur le navigateur et entrer l'adresse, serveur1-mdl/rdweb.

Attention il y a uniquement le navigateur Firefox qui fonctionne.



Puis se connecter avec un utilisateur comme Laure Dubreuil



Mission 6 : Cluster PfSense

Le cluster de PfSense a pour objectif de mettre en redondance les routeurs/pare-feux pour prévenir d'une panne d'un des deux.

Modification IP des interfaces

Il faudra modifier les adresses IP des interfaces et se référer au IP du [schéma](#).

Les deux routeurs PfSense prendront pour adresse IP virtuelle 172.16.2.254

Sur Pfsense Esclave, pour l'interface WAN il aura l'IP 192.168.211.230.

Static IPv4 Configuration

IPv4 Address: 192.168.211.230 / 24

IPv4 Upstream gateway: WANGW - 192.168.211.254

+ Add a new gateway

Sur Pfsense Maître, pour l'interface WAN il aura l'IP 192.168.211.229.

Static IPv4 Configuration

IPv4 Address: 192.168.211.229

IPv4 Upstream gateway: WANGW - 192.168.211.254

Paramétrage du cluster

Pour paramétrer le cluster Pfsense, il faudra se rendre sur Firewall puis Virtual IPS.

Firewall ▾

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Création de l'IP virtuelle pour l'interface LAN

Il faudra ajouter la configuration ci-dessous au deux Pfsense.

Le protocole CARP, permet le transfert des informations de statut entre les routeurs.

The screenshot shows the 'Edit Virtual IP' configuration page in Pfsense. The 'Type' is set to 'CARP'. The 'Interface' is 'LAN'. The 'Address type' is 'Single address'. The 'Address(es)' field contains '172.16.1.254'. The 'Virtual IP Password' field is empty, with a 'Confirm' field next to it. The 'VHID Group' is set to '1'. The 'Advertising frequency' is set to '1' (Base) and '0' (Skew). A note at the bottom states: 'The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.'

Attention, sur le Pfsense Esclave il faudra mettre le Skew à 1, cela permet de définir la priorité (il sera donc esclave car il est à 1 et le Pfsense Maître est à 0).

A close-up of the 'Advertising frequency' section, showing the 'Skew' dropdown menu set to '1'.

Création de l'IP virtuelle pour l'interface DMZ

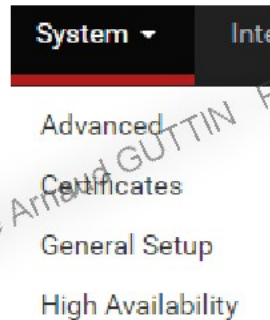
Il faudra effectuer la même pratique pour l'interface DMZ. Cependant, il faudra changer le VHID (chaque VHID permet un canal de communication différent).

The screenshot shows the 'Edit Virtual IP' configuration page in Pfsense for the DMZ interface. The 'Type' is set to 'CARP'. The 'Interface' is 'DMZ'. The 'Address type' is 'Single address'. The 'Address(es)' field contains '10.10.1.254'. The 'Virtual IP Password' field is empty, with a 'Confirm' field next to it. The 'VHID Group' is set to '2'. The 'Advertising frequency' is set to '1' (Base) and '0' (Skew). A note at the bottom states: 'The mask must be the network's subnet mask. It does not specify a CIDR range.'

Configuration de la haute disponibilité

Il faudra ensuite configurer la haute disponibilité, c'est le service qui va permettre de surveiller si le routeur voisin est toujours actif ou non. On utilisera l'interface PFSYNC des routeurs Pfsense pour la haute disponibilité.

Pour ce faire, il faut aller dans High Availability.



High Availability sur Pfsense Maître

Il faudra cocher la case Synchronize states, puis remplir les informations ci-dessous.

⚠ Non sécurisé | 172.16.2.252/system_hasync.php

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states ☒ pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, and imports them into the state table from other firewalls, and imports them into the state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Manual)

Synchronize Interface PFSYNC

If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID f6af66c5

Custom pf host identifier carried in state data to uniquely identify which host or interface. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcd). Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP 192.168.60.2

Setting this option will force pfsync to synchronize its state table to this IP address.

Select options to sync

- ☒ User manager users and groups
 - ☒ Authentication servers (e.g. LDAP, RADIUS)
 - ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
 - ☒ Firewall rules
 - ☒ Firewall schedules
 - ☒ Firewall aliases
 - ☒ NAT configuration
 - ☒ IPsec configuration
 - ☒ OpenVPN configuration (Implies CA/Cert/URL Sync)
 - ☒ DHCP Server settings
 - ☒ DHCP Relay settings
 - ☒ DHCPv6 Relay settings
 - ☒ WoL Server settings
 - ☒ Static Route configuration
 - ☒ Virtual IPs
 - ☒ Traffic Shaper configuration
 - ☒ Traffic Shaper Limiters configuration
 - ☒ DNS Forwarder and DNS Resolver configurations
 - ☒ Captive Portal
- ☒ Toggle All

High Availability sur Pfsense Esclave

Non sécurisé | 172.16.2.253/system_hasync.php

State Synchronization Settings (pfsync)

Synchronize states ☒ pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the pf interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization)

Synchronize Interface 
If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID
Custom pf host identifier carried in state data to uniquely identify which host created a firewall rule. Must be a non-zero hexadecimal string 8 characters or less (e.g. ff01, abcdef01). Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP
Setting this option will force pfsync to synchronize its state table to this IP address. The default is the interface IP.

Attention, pour le Pfsense Esclave il ne faut cocher que l'option Virtual IPS.

Modification des règles de pare feu pour l'interface PFSYNC

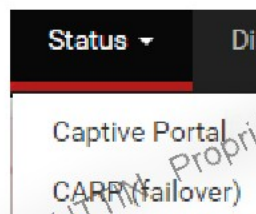
Il faudra ensuite configurer les règles pour l'interface PFSYNC.

La configuration est à réaliser sur les deux Pfsense. Il faudra créer une règle qui autorise la communication entre les deux serveurs sur PFSYNC, (ici on autorise tout le trafic mais il est possible de rendre cette règle plus sélective en utilisant les adresses IP respective des routeurs Pfsense).



Vérification du statut de la synchronisation

Pour vérifier le statut de la synchronisation entre les routeurs, il faut aller dans CARP failover.



On peut voir les deux Pfsense sur le statut de la synchronisation.

