Projet de Réseau Virtuel Paris-Perpignan

M. KHALILI (BTS SIO 2 SISR)

Professeur chargé de l'AP : Mme.GHOUA















Table des matières

1/Installation et configuration de base d'OPNsense	3
1.1/Création de la machine Virtuelle :	3
1.2/Installation d'OPNSense :	1
1.3/Configuration des interfaces :	7
1.4/Test :	3
2/Installation et configuration de l'AD. 12	L
2.1/Configuration Nécessaire	L
2.2/Installation de Windows Server 2022 12	2
2.4/Configuration IP de l'AD :)
2.3/Crée un domaine AD DS)
2.5/Configuration de l'AD :)
3 /Configuration d'un Serveur Web sur VM Linux	5
3.1/Mise en place de la machine virtuelle :	5
3.2/Installation de MobaXtream :	7
3.3/Installation d'Apache :	3
3.4/Activation du HTTPS :)
3.5/Retrait de la carte réseau bridge :42	L
4/Installation et Configuration de l'OpenVPN sur Paris	2
4.1/Mise en œuvre OpenVPN – SSL/TLS – Rappel 43	3
4.2/Génération de l'autorité de certification (CA) 44	1
4.3/Génération du certificat du serveur45	5
4.4/Créer un utilisateur VPN et son certificat utilisateur associé	7
4.5/Création du serveur OpenVPN 49)
4.6/Création de règles de pare-feu54	1
4.7/Exporter la configuration du client OpenVPN56	5
4.8/Configuration du NAT	3
4.9/Outbound (NAT))
4.10/Connexion au tunnel sécurisé sur le client coté perpignan62	L
4.11/Règles pour bloquer un site	5
5/Merci pour votre lecture !	7





1/Installation et configuration de base d'OPNsense

1.1/Création de la machine Virtuelle :

Pour installer OPNsense il faut récupérer l'iso depuis le site officiel :

https://opnsense.org/download/

Il faut sélectionner DVD comme ci-dessous :







Il faut faire une VM en host-only avec l'ISO téléchargé comme ci-dessous (il y a de nombreux tutos sur internet pour faire une VM). Il faut minimum 2 Go de RAM à la VM pour assurer un bon fonctionnement :

C OPNSENSE	
Power on this virtual mac Edit virtual machine settir	hine ngs
▼Devices	
📟 Memory	2 GB
Processors	2
🖂 Hard Disk (SCSI)	20 GB
💿 CD/DVD (IDE)	Using file M:\Wind
🗣 Network Adapter	Custom (VMnet1)
🚭 USB Controller	Present
 Sound Card 	Auto detect
Display	Auto detect

1.2/Installation d'OPNSense :

On peut la démarrer et la laisser charger.

Une fois arrivé sur la connexion, on rentre :

Login : installer

Password : opnsense

Attention, pour l'instant le clavier est en Qwerty







Ensuite, il faut choisir le « keymap », la disposition clavier : il faut descendre et sélectionner « french » et ensuite sélectionner « Continux witth fr.kbd keymap ».



Sélectionner « Install (ZFS) ».



Choisir « stripe – No Redundancy » car nous voulons aucune redondance.

stripe	Stripe - No Redundancy
Mirror	Mirror - n-Way Mirroring
raid10	RAID 1+0 - n x 2-Way Mirrors
raidz1	RAID-21 - Single Redundant RAID
raidz2	RAID-Z2 - Double Redundant RAID
raidz3	RAID-23 - Triple Redundant RAID

Choisir le disque en cliquant sur espace puis entrer.





Valider la destruction du disque. Dans notre cas, il est formaté, mais s'il y a des données dessus, il faut vérifier avant.

Last Chances the current daØ	Are you contents	<mark>sure</mark> you of the fo	want to bllowing	<mark>destroy</mark> disks:
	< YES >	< NO) >	

L'installation se lance.

Cloning current system Verifying resulting files Preparing target system	ISS [<mark>100%]</mark>] [Completed] [In Progress]
98%	

Une fois fini, il demande si on veut modifier le mot de passe root, nous allons le faire pour avoir plus de sécurité, appuyez sur entrée.

Final Configuration Setup of your OPNsense system is nearly complete.
Root Password Change root password Complete Install Exit and reboot

Entrer votre nouveau mot de passe 2 fois.

Set P Please select a system managemen	assword password for the t account (root):
< 0K >	<cancel></cancel>

Enfin, sélectionnez « complete install ».

La machine va redémarrer.





1.3/Configuration des interfaces :

Il faut se connecter en root et le mot de passe qu'on vient de modifier.

Pour « enter an option » appuyez sur 1.

Aux questions « Do you want to configure LAGGs now » et « Do you want to configure VLANs now » appuyez sur « n » pour non.

Pour « Enter the WAN interface ... » appuyer sur entrée car nous ne l'utiliserons pas.

Pour « Enter the LAN interface ... » saisir « em0 ».

Pour « Enter the Optional interface ... », appuyez sur entrée car nous ne l'utiliserons pas.

Puis appuyez sur « y » pour valider.

```
Enter the WAN interface name or 'a' for auto-detection:

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(or nothing if finished): em0

Enter the Optional interface 1 name or 'a' for auto-detection

(or nothing if finished):

The interfaces will be assigned as follows:

LAN -> em0

Do you want to proceed? [y/N]: y
```

Maintenant on va attribuée l'adresse IP.

Pour « Enter an option » appuyez sur 2.

Enter an option: 2

« Configure IPv4 adress LAN interface via DHCP ? » saisir « n » car il faut configurer l'interface en statique.

Saisissez l'adresse IP de l'interface. Cette adresse IP sera la passerelle du LAN.

Saisissez le masque en CIDR.

```
Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.200.1
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```





Pour la Gateway appuyer sur entrée pour cause que la passerelle sera elle-même.



« Configure IPv6 adress LAN interface via DHCP ? » saisir « n » car nous ne voulons pas configurer l'IPv6.

Appuyez sur entrée pour sauter la configuration de l'IPV6.

« Do you want configure DHCP server on LAN ? » saisir « n » car nous ne voulons pas configurer de serveur DHCP.

« Do you want to change the web GUI protocol from HTTPS to HTTP ? » saisir « n » car nous ne voulons pas configurer le protocole HTTPS.

« Do you want to genere a new self-signed web GUI certificate ? » saisir « n » car nous ne voulons pas générer de certificat.

« Restore web GUI access default ? » appuyer sur entrée.

Il nous donne l'url pour configurer depuis l'interface web

```
https://192.168.200.1
```

1.4/Test :

Pour essayer, nous allons utiliser un client dans le même VMNET que notre serveur OPNSense.

Il faut changer la configuration IP du client pour quelle correspond à celle de notre serveur, la passerelle sera l'adresse IP de l'OPNSense.

• Utiliser l'adresse IP suivante :	
Adresse IP :	192.168.200.2
Masque de sous-réseau :	255.255.255.0
Passerelle par défaut :	192.168.200.1
Obterni les auresses des serve	eurs DNS automatiquement
Obterni les auresses des servi	eurs DNS automatiquement
Otterni les adresses des serveur Di Otterni les adresse de serveur Di Convour DNC préféré :	eurs DNS automatiquement NS suivante :
 Obterin les auresses des servi Otterin les auresses de serveur DI Serveur DNS préféré : 	eurs DNS automatiquement NS suivante :
 Obterin les auresses des serve Outliser l'adresse de serveur DI Serveur DNS préféré : Serveur DNS auxiliaire : 	eurs DNS automatiquement NS suivante :
OUterninies auresses des serveur DI Serveur DNS préféré : Serveur DNS auxiliaire :	eurs DNS automatiquement NS suivante :

Dans le navigateur, il faut saisir l'adresse IP attribuée à l'OPNSense.

Continuer même si le certificat de sécurité n'est pas approuvé par le système d'exploitation.

Se connecter :





Login : root

Password : le mot de passe créé précédemment.

Nous arrivons sur le Wizard.

Starting initial configuration!



Cliquez « Recharger » pour appliquer les changements.

Nous voilà sur le tableau de bord, nous avons terminé la configuration du serveur OPNSense. Il faut maintenant configurer les différents services.







NOTE : Il faudra recommencer l'installation pour le serveur du coté Perpignan en rajoutant une carte réseau pour l'accès à internet et faire attention lors de l'assignement des interfaces de ne pas inversé les cartes réseau (mettre la carte réseau du WAN pour l'interface LAN ou l'inverse) il faut bien les identifier par leurs adresses MAC.





2/Installation et configuration de l'AD.

2.1/Configuration Nécessaire

Pour la bonne réalisation de cette installation, il faudra disposer d'une configuration minimum à respecter :

- Processeur : 1.4 GHz 64-bit
 - Compatible avec le jeu d'instructions x64
 - Prend en charge NX et DEP
 - Prend en charge CMPXCHG16b, LAHF/SAHF et PrefetchW
 - Prend en charge la traduction d'adresse de deuxième niveau (EPT ou NPT)
- RAM : 512 Mo
 - ECC conseillé
- Disque : 32 Go





2.2/Installation de Windows Server 2022

Pour récupérer l'ISO de Windows Server, il suffit de se rendre sur le site de Microsoft :

https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2022

Veuillez sélectionner votre téléchargement de Windows Server 2022

Anglais (États-Unis)	Téléchargemen t ISO Édition 64 bits	Téléchargement VHD Édition 64 bits	Essayer sur Azure En savoir plus	Créer une machine virtuelle dans Azure En savoir plus >
Chinois (simplifié)	Téléchargemen t ISO Édition 64 bits →			
Français	Téléchargemen t ISO Édition 64 bits →			
Allemand	Téléchargemen t ISO Édition 64 bits →			
Italien	Téléchargemen t ISO Édition 64 bits			
Japonais	Téléchargemen t ISO Édition 64 bits			





Une fois l'ISO téléchargé, l'inclure dans VMware dans la VM créée préamblement :







Démarrer la Machine Virtuel :

Sélectionnez la langue désirée, et cliquez sur suivant :

		📒 Micro	soft	
	Langue à installe	er : Français (France)		•
Eorma	at horaire et monétai	re: Français (France)		•
Clavier	r ou méthode d'entré	e: Français		•
Entre	z la langue et les pré	férences de votre choi	et cliquez sur Suivant pour	continuer.
Microsoft Corp	oration. Tous droits nisen	vés.		Suivar

On clique sur Installer maintenant

Configuration do systeme o	expectation necrosors server	1010
	Hicrosoft	
	Installer maintenant	
Béparer l'ordinateur		
	roits niservis	





Saisissez la clef de produit (ou choisissez de la saisir plus tard) :



Choix du type d'installation :

Attention le choix peut varier suivant la clef de produit saisie, ici nous allons choisir la version Windows Server 2022 Standard (expérience du bureau) :







Acceptez le contrat de licence :



Sélectionnez ensuite le type d'installation, personnellement je ne vous recommande jamais de faire une mise à jour pour un serveur en production :

uel type d'installation voulez-vou	us effectuer ?
Mise à jour : Installer le système d'ex lichiers, les paramètres et les applicat vec cette option, les fichiers, paramètres et l'exploitation. Cette option est disponible u ystème d'exploitation est déjà en cours d'ex	ploitation Microsoft Server et conserver les bions. applications sont déplacés vers le nouveau système niquement lersqu'une version prise en charge du décution sur l'ordinateur.
Personnalisé : installer uniquement le (avancé) Wec cette option, les fichiers, les paramètre houveau système d'exploitation. Pour modif i l'aide du disque d'installation. Nous vous r continuer.	e système d'exploitation Microsoft Server s et les applications ne sont pas déplacés vers le fier les partitions et les lecteurs, démarrez l'ordinateu recommandons de sauvegarder vos fichiers avant de





Sélectionnez le disque et la partition sur lesquels vous souhaitez installer le système (minimum 32 Go) puis cliquez sur Suivant :

Nom		Taille totale	Espace libre	Туре
Lecteur 0 Espa	ce non alloué	127.0 Go	127.0 Go	
🚱 Actualiser 🚱 Charger un pilote	Supprimer	Eormater	* Nouve	au

Si vous ne voyez pas de disque dans la liste, il est possible que la carte contrôleur de votre disque (SCSI, RAID, ...) nécessite un pilote spécial, dans ce cas, cliquez sur "Charger un pilote".

l'installation commence :







Le serveur va redémarrer... plusieurs fois.

onnecter automatique	ment à cet ordinateur.		
om d'utilitateur	Administrations		
lot de passe	1		
ntrez de nouveau le lot de passe			

Vous pouvez ouvrir la session en saisissant le mot de passe, taper précédemment :



Vous arrivez sur le bureau :







Maintenant que vous avez ouvert votre session, vous pouvez découvrir le Gestionnaire de Serveur :



Passons, maintenant à la partie la plus intéressante la configuration (;

2.4/Configuration IP de l'AD :

Premièrement, on va commencer à configurer notre carte réseau, en allant dans Panneau de configuration -> Réseau et Internet -> Centre Réseau et partage puis cliquer sur « Ethernet 0 » :

Propriétés de : Protocole Internet versi	on 4 (TCP/IPv4) X					
Général						
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.						
Obtenir une adresse IP automatiq	uement					
• Utiliser l'adresse IP suivante :						
Adresse IP :	192 . 168 . 212 . 254					
Masque de sous-réseau :	255.255.255.0					
Passerelle par défaut :	192.168.212.1					
Obtenir les adresses des serveurs	DNS automatiquement					
• Utiliser l'adresse de serveur DNS s	uivante :					
Serveur DNS préféré :	127.0.0.1					
Serveur DNS auxiliaire :	192.168.212.1					
Valider les paramètres en quittant Avancé						
	OK Annuler					





Information : Ces Informations doivent correspondre à votre schéma réseau.

Dans mon cas « 192.168.212.1 » est ma passerelle (Lan-Perpi) OPNsense.

2.3/Crée un domaine AD DS

Aller dans le Gestionnaire de serveur :



Puis :

📥 Assistant Ajout de rôles et de	a Assistant Ajout de rôles et de fonctionnalités			×
Avant de comme	encer	SERVEUR DE AD-PER	DESTINATIO PI.MK212.lo	DN cal
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Cet Assistant permet d'installer des rôles, des services de rôle ou des fonction déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction de votre organisation, tels que le partage de documents ou l'hébergement de Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant de Suppression de rôles et de fonctionnalités Avant de continuer, vérifiez que les travaux suivants ont été effectués : • Le compte d'administrateur possède un mot de passe fort • Les paramètres réseau, comme les adresses IP statiques, sont configurés • Les dernières mises à jour de sécurité de Windows Update sont installées Si vous devez vérifier que l'une des conditions préalables ci-dessus a été sati exécutez les étapes, puis relancez l'Assistant. Cliquez sur Suivant pour continuer.	nnalités. Vous n des besoins i l'un site Web.	devez informatic	jues
	< Précédent Suivant >	Installer	Annule	er

Cliquer sur « Suivant »



BTSSIC



Continuer sur suivant à sélection du serveur.

Puis :

Sélectionner Services AD DS et Ajouter des fonctionnalités :







Facultatif : On peut ajouter également le « DNS » et le « DHCP » pour donner au client une configuration dynamique.

Il faudra sélectionner alors :

Services DHCP et DNS.

électionner de	s rôles de serveurs	SERVEUR DE DESTINATION AD-PERM ANZ 12 Jord
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.	
Type d'installation	Rôles	Description
Stection du serveur Roles de serveurs Fonctionnaliés Confirmation Résultats	Acc64 distance distanc	Les enrices de donaine Asixo Directory (AD DS) atxicent des informations à propos des objets en réserva et reduction es informations directorisation provinces pour donner aux utilisateurs du réseau un accès aux services AD DS utilisent les contrôleurs de donaine gour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
-		< Précédent Suivant > Installer Annule
Q Tapez ici pou	effectuer une recherche	~ 뒫 da

assistant Ajout de rôles et de fonctionnalités	- 🛛 🗙
Sélectionner des fonctionnalités	SERVER OF DESTINATION AD-REPLACE
Avant de commencer Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.	
Type d'installation Fonctionnalités	Description
View Filmments Fordcomains Selection du serveur Mit Transverk 4.8 Features (2 sur 7 installé(ji)) Roles de serveurs Anstance à Batinera (0 Conformation Basiliante et l'enternet de lecteur Billocker Conformation Basiliante et l'enternet de lecteur Billocker Chendromation Centernet de lecteur Billocker Ciellettiner (1) Centernet de lecteur Billocker Ciellettiner (2) Centernet de lecteur Billocker Ciellettiner (2) Centernet de lecteur Billocker Ciellettiner (2) Centernet de lecteur Billocker Cielletting de basculement Collecting de basculement Collection de verdiversité differentélé à distance Deterfingr Data Center Tripiques de l'estau Billocker Deterfingr Deterfingr Estantion IS Management OData Epidencia addivisité Nition Esternion Vision Esternion Vision Esterinion Vision <t< td=""><td>Provides services and environments for running native user-mode Linux shells and tools on Windows.</td></t<>	Provides services and environments for running native user-mode Linux shells and tools on Windows.
Media Foundation Media Gueucing Moniteur de port LPR	
	< Précédent Suivant > Installer Annuler
# 🔎 Tapez ici pour effectuer une recherche 🛛 🛱 🜔 📕 🔚	~ 및 4 <mark>, 1623</mark> ↓



Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les Avant de commencer ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de Type d'installation gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs. Sélection du serveur Rôles de serveurs À noter : Fonctionnalités · Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine. AD DS Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS Confirmation n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur. Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site. En savoir plus sur Azure Active Directory Configurer Office 365 avec Azure Active Directory Connect < Précédent Suivant > Installer Annuler Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Avant de commencer Installer. Type d'installation Redémarrer automatiquement le serveur de destination, si nécessaire Sélection du serveur Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur Rôles de serveurs cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces Fonctionnalités fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher. AD DS Gestion de stratégie de groupe Confirmation Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS Module Active Directory pour Windows PowerShell Outils AD DS Centre d'administration Active Directory

Composants logiciels enfichables et outils en ligne de commande AD DS Services AD DS Exporter les paramètres de configuration Spécifier un autre chemin d'accès source

< Précédent Suivant >



Annuler

Installer



	• @ 🍢	Gérer	Outils	Afficher	Aide
Configuration post-déploie Configuration requise pour : PERPI Promouvoir ce serveur en co	Services AD DS à AD-				
Détails de la tâche					

Étant donné qu'il s'agit d'un domaine inconnu au sein d'une forêt nouvellement créée, sélectionnez l'option « Ajouter une nouvelle forêt » et saisissez le nom de domaine souhaité. Il est important de noter que l'utilisation d'un nom de domaine tel que « mk-212.local » le rendra non routable, ce qui peut entraîner des complications avec des services spécifiques.

🛓 Assistant Configuration des serv	rices de domaine Active Directory		- 🗆 X
Configuration de déploiement			SERVEUR CIBLE AD-PERPI.MK212.local
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner l'opération de dépl Ajouter un contrôleur de dor Ajouter un nouveau domaine Ajouter une nouvelle forêt Spécifiez les informations de dou Nom de domaine racine :	oiement maine à un domaine existant e à une forêt existante maine pour cette opération mk-212.local	Choisissiez votre nom de domaine xxx.local
	En savoir plus sur les configurati	ons de déploiement	
		< Précédent Suivant >	Installer Annuler





Choisissiez votre propre mot de passe.

Assistant Configuration des serv	vices de domaine Active Directory		-		\times
Options du contro	ôleur de domaine		AD-PEF	SERVEUR (RPI.MK212.	CIBLE local
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner le niveau fonctionnel de la Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine : Spécifier les fonctionnalités de contrôle Serveur DNS (Domain Name System Catalogue global (GC) Contrôleur de domaine en lecture s Taper le mot de passe du mode de rest Mot de passe : Confirmer le mot de passe :	a nouvelle forêt et du domaine racin Windows Server 2016 Windows Server 2016 eur de domaine n) eule (RODC) auration des services d'annuaire (DS 	e v		
	En savoir plus sur les options pour le co	ontrôleur de domaine			
	< Pr	écédent Suivant > In	staller	Annul	er

Comme il s'agit d'un nouveau serveur DNS pour une nouvelle zone, ne vous inquiétez pas pour ce message, vous pouvez poursuivre.





📥 Assistant Configuration des serv	rices de domaine Active Directory —		×
Options DNS	AD-PEF	SERVEUR RPI.MK212	CIBLE 2.local
Il est impossible de créer u Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	ne délégation pour ce serveur DNS car la zone parente faisant autorité est intro Affich Spécifier les options de délégation DNS Créer une délégation DNS	er plus	×
	< Précédent Suivant > Installer	Annu	ler

Cliquer sur « Suivant »

Assistant Configuration des serv	- 🗆 ×		
Options suppléme	SERVEUR CIBLE AD-PERPI.MK212.local		
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur	Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si néces Le nom de domaine NetBIOS : MK-212	saire.	
Installation Résultats			
	En savoir plus sur d'autres options		
	< Précédent Suivant >	Installer Annuler	





Assistant Configuration des serv	ices de domaine Active Directory		_		×
Chemins d'accès			SE AD-PERP	RVEUR (I.MK212.	CIBLE local
Configuration de déploie Options du contrôleur de	Spécifier l'emplacement de la base de	données AD DS, des fichiers journ	aux et de SYS	VOL	_
Options DNS	Dossier de la base de données :	C:\Windows\NTDS			
Options supplémentaires	Dossier des fichiers journaux :	C:\Windows\NTDS			
Chemins d'accès	Dossier SYSVOL :	C:\Windows\SYSVOL			
Examiner les options Vérification de la configur Installation Résultats					
	En savoir plus sur les chemins d'accès /	Active Directory			
	< P1	récédent Suivant >	Installer	Annul	er

Vérifiez les options et continuez.

📥 Assistant Configuration des servi	ces de domaine Active Directory	_		×
Examiner les optic	ons	SE AD-PERF	RVEUR 91.MK212	CIBLE 2.local
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez vos sélections : Configurez ce serveur en tant que premier contrôleur de domaine Active I nouvelle forêt. Le nouveau nom de domaine est « mk-212.local ». C'est aussi le nom de la Nom NetBIOS du domaine : MK-212 Niveau fonctionnel de la forêt : Windows Server 2016 Niveau fonctionnel du domaine : Windows Server 2016 Options supplémentaires : Catalogue global : Oui Serveur DNS : Oui	Directory d'i	une orêt.	×
	automatiser des installations supplémentaires En savoir plus sur les options d'installation	Affic	her le so	cript
	< Précédent Suivant >	staller	Annu	ller





Finissez en cliquant sur installer pour démarrer la création de votre domaine et la configuration du DC.



Votre serveur va redémarrer, une fois redémarrer vous verrez que votre ad est bien rentrer dans le domaine :







2.5/Configuration de l'AD :

Nous allons maintenant créer les utilisateurs pour notre AD.

Allez dans « Utilisateurs et ordinateurs Active Directory »

🚡 Gestionnaire de serveur					– a ×
Gestionn	aire de serveur • Tableau	de bord			
Tableau de bord Serveur local Tous les serveurs AD DS DP	DÉMARRAGE DÉMARRAGE	gurer ce serveur local			Centre d'administration Active Directory Configuration du système Défegnemente et optimiser les lecteurs DHCP Diagnostic de mémoire Windows DNS
a DNS	2 Ajc 3 Ajc 000VFAUTES 4 Crt 5 Co EN SAVOIR PLUS Reles et groupes de serveurs Roles (4) (croopes de serveurs 1) Nom	uter des rôles et des fonctionnalit uter d'autres serveurs à gérer ier un groupe de serveurs nnecter ce serveur aux services cl bre total de serveurs : 1	loud		Domaines et approbations Active Directory Editeur out Aregistre Gestion de l'ordinateur Gestion des stratégies de groupe Informations système Instateur IGS3 Letteur de réceptration Module Active Directory pour Windows PowerShell Moniteur de ressources Nettoyage de disque Observateur d'evinements
	AD DS 1 • Facilité de gestion Événements Services Performances Résultats BPA	Image: The second sec	DNS 1	Services de fichiers et 1 de stockage Facilité de gestion Événements Services Performances Résultats BPA	DOBC Data Sources (22-bit) Par-Fice Mindows Defendence avec fenctions avancées de sécurité Parlicitateur de táches Services de composants Services de composants Services de donniers ODBC (64-bit) Stantigie de sicurals locate Ubilisateurs et ortinateurs Active Directory Windows PowerShell (v88)

Nous devons crée une nouvelle Unité Organisation (UO)

	Utilisateurs et o	ordinateurs Active	Directory				_	Х
Fic	hier Action	Affichage ?						
•	🔿 🖄 🖬	📋 📑 🖸 🖬	👌 🔽 🖬 🙎	🐮 📷 🔻 🖻 🤇	8			
	Utilisateurs et o Requêtes er Builtii Com Doma Foreiç Mana Users	rdinateurs Active pregistrées Délégation de Rechercher Changer de d Changer de c Augmenter le Maîtres d'opé	Nom Builtin contrôle omaine ontrôleur de doma niveau fonctionne rations	Type builtinDomain ine I du domaine	Desc	cription ult container for up ult container for do ult container for sec ult container for ma ult container for up		
		Nouveau			>	Ordinateur		
		Toutes les tâc	hes		>	Contact		
		Affichage			>	Groupe		
		Actualiser Exporter la lis	te			InetOrgPerson msDS-ShadowPrincipalContain msImaging-PSPs	er	
		Propriétés				Alias de file d'attente MSMQ		
		Aide				Unité d'organisation		
< Cufe		>				Imprimante ਯੋ Utilisateur Dossier partagé		





Ajouter votre nom d'organisation.

	Utilisateurs et erdinateurs Active Directory		7		\times
F	Nouvel objet - Unité d'organisation	×			
	Créer dans : mk-212.local/		on		
Ĵ	Non :				
		1	container for up		
	<u>Р</u>	J	container for do		
	Protéger le conteneur contre une suppression accidentelle		container for ma		
			container for up		
	OK Annuler	Aide			
			-		
<	>				
_					

Crée maintenant, un nouvel utilisateur :

Fichier Action Affichage ?				
Utilisateurs et ordinateurs Active Utilisateurs et ordinateurs Active Requètes enregistrées Builtin Builtin Computers G Domain Controllers ForeignSecurityPrincipal:	Nom Type	Descriptio Aucun élément à on de contrôle	on afficher	dans cet aperçu.
Users MK-VPN	Déplace Recherc	r her		
	Toutes le	u es tâches	>	Contact
	Actualis	er	>	Groupe InetOrgPerson
	Réorgan Aligner Propriét	,- iser les icônes les icônes és	>	msDS-ShadowPrincipalContainer msImaging-PSPs Alias de file d'attente MSMQ Unité d'organisation
	Aide			Imprimante Utilisateur
< >				Decrier partagé





Remplissez les informations de votre nouvel utilisateur.

Itilicatours of ordin	actours Active Directory	
ouvel objet - Utilis	ateur	>
🤏 Créer dan	ns : mk-212.local/MK-VPN	
Prénom :	Initiales :	
Nom :		
Nom complet :		
Nom d'ouverture de	e session de l'utilisateur :	
	@mk-212.local ~	
Nom d'ouverture de	e session de l'utilisateur (antérieur à Windows 2000) :	
MK-212\		
MK-212\		
MK-212\		

Puis-ajouter le mot de passe qui peut-être changer par l'utilisateur à l'ouverture de sa session (Si option coché).

Nouvel objet - Utilisateur		×			
Créer dans : mk-212.local/MK-VPN					
Mot de passe :	•••••				
Confirmer le mot de passe :	•••••				
L'utilisateur doit changer le mo	t de passe à la prochaine ouverture de session				
L'utilisateur ne peut pas chang	ger de mot de passe				
🔽 Le mot de passe n'expire jama	is				
Le compte est désactivé					
	< Précédent Suivant > Annuler				





Une fois terminé, aller sur le poste client et changer l'adresse IP, si vous n'avez pas mis de DHCP sur votre AD sinon dans l'invité de commande taper « ipconfig /release puis ipconfig /renew »

arte Ethernet Ethernet1 :
Suffixe DNS propre à la connexion : MK212.local Description Intel(R) 82574L Gigabit Network Connection #2
Adresse physique
DHCP activé Oui
Configuration automatique activée : Oui
Adresse IPv6 de liaison locale : fe80::c2c1:9c15:cce4:5b4d%31(préféré)
Adresse IPv4
Masque de sous-réseau
Bail obtenu jeudi 3 octobre 2024 17:42:28
Bail expirant vendredi 11 octobre 2024 17:42:28
Passerelle par défaut fe80::20c:29ff:fece:8942%31
192.168.212.1
Serveur DHCP
IAID DHCPv6
DUID de client DHCPv6
Serveurs DNS
NetBIOS sur Tcpip Activé

Pour rentrer dans le client dans l'AD, il faut aller dans les paramètres puis Système -> A propos de – Renommer ce PC (Avancé) :

Propriétés système				×
Paramètres système avance Nom de l'ordin	cés Protection d nateur	u système	Utilisation Matériel	à distance
Windows utilise ordinateur sur	e les informations su e réseau.	iivantes pou	r identifier vo	otre
Description de l'ordinateur :	:			
Nom complet de l'ordinateur : Groupe de travail : Pour utiliser un Assistant e domaine ou un groupe de sur le réseau. Pour renommer cet ordina domaine ou de groupe de	Par exemple : "L'o "L'ordinateur d'Ant DESKTOP-CLRH4 WORKGROUP et vous joindre à un travail, cliquez sur teur ou changer de travail, cliquez sur	rdinateur du ioine''. 47A Identité Modifier.	entité sur le Modifier	réseau
	ОК	Ann	uler	Appliquer





Entrer votre nom de domaine ----.local

Propriétés système	×
Modification du nom ou du domaine de l'ordinateur $ imes$	on à distance
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.	el r votre
Nom de l'ordinateur :	
DESKTOP-CLRH47A	μ
Nom complet de l'ordinateur : DESKTOP-CLRH47A Autres	
Membre d'un	le réseau
Domaine :	
	fier
◯ Groupe de travail :	
WORKGROUP	
OK Annuler	J
OK Annuler	Appliquer





Entrer vos données de connexion :

211		A hinhos de	:			
ier un paramèt	rre 🔎	Votre ordinateur protégé.	est surveillé	et		
	Propriétés système		×			
	Modification du nom ou du	domaine de l'ordinateur $~~ imes~~ imes~$	on à distance			
age	Vous pouvez modifier le nom et ordinateur. Ces modifications pe ressources réseau.	l'appartenance de cet euvent influer sur l'accès aux	el I	Sécurité Windows Modification du nom ou	u du domaine de	
tte	Nom de l'ordinateur :		ES	l'ordinateur		
tâche	Nom complet de l'ordinateur : DESKTOP-CLRH47A		60 00	Entrez le nom et le mot de passe le domaine.	d'un compte autorisé à joindre	
ction sur ce P(Manhar d'un	Autres	DE 22 le réseau	Nom d'utilisateur		
iences partag	Domaine : mk-212.local		///////////////////////////////////////	Mot de passe		
oosants systèr	O Groupe de travail : WORKGROUP		tier o	ОК	Annuler	
2-papiers		OK Annuler	ir			
u à distance						
ionnalités fac						
pos de		OK Annuler	Appliquer			

Vous devrez obtenir ça après avoir valider, cliquer sur OK puis cliquer sur « redémarrer maintenant » :









Cliquer sur paramètre puis information du compte et vous voilà dans le domaine :







3 /Configuration d'un Serveur Web sur VM Linux

3.1/Mise en place de la machine virtuelle :

Pour faire le serveur web, j'ai choisi d'utiliser une VM Linux sans interface graphique pour minimiser les consommations de ressources. Cette VM aura deux cartes réseaux : une en Host-only et une en Bridge, qui vont nous servir à la configuration en SSH, que nous retirerons à la fin de la configuration.

	3	
Power on this virtual machine set	achine tings	
 Devices 		
📟 Memory	2 GB	
Processors	2	
🖂 Hard Disk (SCSI)	20 GB	
💿 CD/DVD (SATA)	Using file M:\VM\I	
Network Adapter	Custom (VMnet1)	
PNetwork Adapter 2	Bridged (Automatic)	
🚭 USB Controller	Present	
🗇 Sound Card	Auto detect	
🖵 Display	Auto detect	

Voici un tuto pour installer Linux sans interface graphique :

https://goopensource.fr/debian-installation-sans-interface-graphique/

Une fois la VM créée, on peut la démarrer et se connecter avec l'utilisateur. Il est conseillé de vérifier l'adresse IP de l'interface Bridge en utilisant la commande :

ip a
<pre>permitted dy applicable law. Last login: Sun Sep 23 15:22:46 CEST 2024 on tty1 chR0vmlinuxcmdclean:~% ip a 1: lo: (JODPBACK, UP, DMRE, UP> mtu 65536 gdisc noqueue state UNKNOWN group default glen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00 inet 127.00.1/8 scope host noperfixed. valid.ht forever preferred.ht forever inet6 s:U/128 scope host noperfixeroute valid.ht forever preferred.ht forever 2: ens33: </pre> (BR0ADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 gdisc fq_codel state UP group default glen 1000 link/ether 00:0:02:3180:453ad brd ff:ff:ff:ff:ff: altname enp251 inet6 fe80::20c:29ff:fe88:45ad/64 scope link valid.ht forever preferred.ht forever 3: ens37: (BR0ADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 gdisc fq_codel state UP group default glen 1000 link/ether 00:0:0:29:88:45:ad brd ff:ff:ff:ff:ff: altname enp251 inet 5: 480:00CAST, MULTICAST, UP, DNEN LUP> mtu 1500 gdisc fq_codel state UP group default glen 1000 link/ether 00:0:0:29:88:45:b7 brd ff:ff:ff:ff:ff:ff: altname enp255 ine 192.168.0.23724 brd 192.168.0.255 scope global dynamic ens37 valid.ht galosse preferred.lft 43188sec inet6 2a0::200:17:4490:200:29:ff:ef8:45aD/64 scope global dynamic mngtmpaddr valid.ht 6806:sec preferred.lft 66386:sec inet6 2a0::200:29:ff:ef8:45aD/64 scope global dynamic mngtmpaddr valid.ht 8386sec preferred.lft 66386sec inet6 2a0::200:29:ff:ef8:45aD/64 scope link
valid_lft forever preferred_lft forever chk@vmlinuxcmdclean:"\$

Si vous n'avez pas d'adresse IP, il faut rajouter la carte réseau dans le fichier "/etc/network/interfaces".

nano /etc/network/interfaces







Nous allons modifier l'adresse ip du host-only (ens33).



La gateway est l'adresse IP de l'interface LAN du firewall.

Il faut sauvegarder avec Ctrl+x.

Recharger la configuration et vérifier:



3.2/Installation de MobaXtream :

Pour activer l'accès root via SSH, commencer par installer le serveur SSH:

sudo apt-get update

sudo apt-get install openssh-server

Ensuite, éditez le fichier de configuration SSH pour permettre la connexion root. Ouvrez le fichier "/etc/ssh/sshd_config" avec un éditeur de texte :

sudo nano /etc/ssh/sshd_config





Modifier la ligne "PermitRootLogin" en : PermitRootLogin yes

Ensuite, redémarrez le service SSH pour appliquer les modifications:

sudo systemctl restart ssh

Une fois ici, vous pouvez vous connecter en root à la VM depuis le PC physique grâce au logiciel MobaXterm.

Vous pouvez facilement installer MobaXtrem sur Windows grâce à ce lien : <u>https://mobaxterm.mobatek.net/download.html</u>



3.3/Installation d'Apache :

Installez Apache avec la commande suivante :

sudo apt-get install apache2

Accédez au répertoire où se trouvent les fichiers du site :

cd /var/www/hml

Supprimez la page par défaut :

sudo rm index.html

Cliquez sur « Follow terminal Folder » en bas à gauche et faites glisser-déposer les pages de votre site.



Redémarrer le serveur web :

systemctl restart apache2





Si on tape l'adresse IP du serveur web dans un navigateur depuis un client dans le même vmnet (vmnet 1) avec la bonne configuration IP, on tombe sur le site web.

C A Non sécur	isé 192.168.200.11			A ⁸ ☆	Φ	£'#	۵	~	
BTS <mark>SIO</mark>	ACADÉMIE DE MONTPELLIER Valori Falori Franceio	Projet Réseau Virtuel							
L'en échang est de c	treprise MC-212, qui gère des activités jes fluides et sécurisés entre ces deux l céré un tunnel sécurisé via un VPN (V de Perpignan de travailler ensemble co	Contexte du Projet réparties sur plusieurs sites, possède deux bareaux principaux exu; il est essentiel de mettre en place une solution efficace po rual Private Neteorch; en utilisant la technologie OpenVPN sur mme si d'est étaient dans le méme bureau, avec un accès secu	: un à Paris et un à Perpignan. ur relier les réseaux internes d OPNsense. Cela permettra aux isé aux fichiers et aux applicati	Pour garant es deux site équipes de ons interne	tir des es. L'idé e Paris e es.	e et			
		Schématisation des Réseaux							
	and and a second s		MAR (1990) Semana B M 200 U/H						
	Las an		can Maria						

3.4/Activation du HTTPS :

Activer le module SSL d'Apache :

a2enmod ssl

Activer le site « default-ssl » d'Apache :

a2ensite default-ssl

A2ensite default-ssl

Recharger apache2 :

systemctl reload apache2

Installer openssl :

apt-get update

apt-get install openssl

Générer un certificat :

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key

Cela permetrra d'obtenir un certificat valable 1 ans.

Il faut rentrer les informations pour le certificat comme par exemple :





You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.
Country Name (2 letter code) [AU]:FR State or Province Name (full name) [Some-State]: Locality Name (eg, city) []:Perpignan Organization Name (eg, company) [Internet Widgits Pty Ltd]:MC-212.fr Organizational Unit Name (eg, section) []:IT Common Name (e.g. server FQDN or YOUR name) []:CHK Email Address []:contact@mlc.fr root@vmlinuxcmdclean:~#

Il faut modifier les droits sur la clé :

chmod440 /etc/apache2/server.crt

Indiquer à Apache2 où se trouve le certificat :

nano /etc/apache2/sites-available/default-ssl

A self-signed (snakeoil) certificate can be created by installing # the ssl-cert package. See # /usr/share/doc/apache2/README.Debian.gz for more info. # If both key and certificate are stored in the same file, only the # SSLCertificateFile directive is needed. SSLCertificateFile /etc/apache2/server.crt SSLCertificateKeyFile /etc/apache2/server.key

Enregistrer et quitter.

Active le module SSL :

a2enmod ssl	
Activer le site HTTPS :	
a2ensite default-ssl	

Redémarrer apache2 :

systemctl reload apache2

Le https est activé.







3.5/Retrait de la carte réseau bridge :

Il est possible de retirer la carte réseau qui est en bridge.

Enlever les lignes de configuration avec:



Redémarrer le service networking :

systemctl restart networking

1. Verification :

Nous avons toujours accès au serveur web depuis le VMnet 1.

Présentation du Projet R	éseau Villix 🕂 🕂								-
- C 🛛 8 Non sécurisé #	ttps://192.168.200.11			A٩	☆	¢	£≡	æ	~G
TS <mark>SIO</mark>	ACADÉMIE DE MONTPELLIER Liberté Tgattas Fatteratit	Projet Rése	au Virtuel Détails						
L'entreprise échanges fluid est de créer ui de Perp	MC-212, qui gère des activités i des et sécurisés entre ces deux li n tunnel sécurisé via un VPN (Vir oignan de travailler ensemble cor	Contexte d réparties sur plusieurs sites, possèd eux, il est essentiel de mettre en pla tual Private Network) en utilisant la mme si elles étaient dans le même	lu Projet e deux bureaux principaux : un à Paris et un à f icce une solution efficace pour relier les réseaux technologie OpenVPN sur OPNsense. Cela pe pureau, avec un accès sécurisé aux fichiers et a	Perpignan. Pou x internes des c ermettra aux éq aux applications	r garant leux site uipes de interne	ir des s. L'idée Paris e s.	e st		
		Schématisation	des Réseaux						
	91910/00 1009 1009	Ar (1600) 382 382 382 382 382 382 382 382 382 388 212 212	1979 1982 1993 1993 1993 1993 1993 1993 1993 199						
	LAN-PERM	Cient Direz	Server Web 19214612011/24						

La configuration du serveur web est terminée.



4/Installation et Configuration de l'OpenVPN sur Paris.

i Information : Sous OpnSense, on peut mettre en place plusieurs types de VPN

- **Peer to peer (SSL/TLS)** : pour monter un VPN site-à-site en utilisant une authentification par certificat.
- **Peer to peer (Shared Key)** : pour monter un VPN site-à-site en utilisant une authentification par clé partagée.
- **Remote Access (SSL/TLS)** : pour monter un accès distant pour clients nomades en utilisant une authentification par certificat.
- **Remote Access (User Auth)** : pour monter un accès distant pour clients nomades en utilisant une authentification par login/password.
- **Remote Access (SSL/TLS + User Auth)** : pour monter un accès distant pour clients nomades en utilisation une authentification par certificat et par login/password.

Dans notre Atelier Professionnel, nous allons utiliser « Remote Access (SSL/TLS + User Auth) »





4.1/Mise en œuvre OpenVPN – SSL/TLS – Rappel



Le module VPN permet de créer un client, un serveur ou les deux. Lors de l'activation du service VPN, une carte OPT virtuelle est générée, facilitant la transmission des paquets vers le VPN distant.

Il est également possible d'établir différents types de serveurs sur un système PfSense, à condition d'utiliser des réseaux ou des tunnels distincts.

OpenVPN fonctionne sur un modèle client-serveur. Lors de la liaison de deux sites, l'un fonctionne comme client tandis que l'autre sert de serveur, permettant ainsi la connexion de plusieurs sites distants à un emplacement central.

Le serveur conserve à la fois le certificat de l'autorité et son propre certificat ainsi que la clé privée correspondante.

À partir du serveur, nous générons également les fichiers essentiels requis pour les clients, notamment un certificat client, une clé et le fichier client OpenVPN, qui varie en fonction de la plateforme du client (Android, Windows ou Mac).





4.2/Génération de l'autorité de certification (CA)

Pour commencer, nous allons générer notre autorité de certification (CA) pour valider l'identité du serveur OpenVPN et authentifier les certificats utilisateur :

🖵 Lobby		
Reporting		
System		
Access		섵
Configu	ration	3
Firmwar	re	
Gateway	/S	1
High Ava	ailability	0
Routes		Ŧ
Settings		00
Trust		٠
Authori	ities	
Certific	ates	
Revoca	tion	
Wizard		1
Log Files	5	۲
Diagnos	tics	D
A Interfaces		
5 Firewall		
VPN		
Services		
🖌 Power		
🗘 Help		

Puis Cliquez sur le signe + . La page de configuration **des autorités** s'affiche.

System: Trust	: Authorities				
Name	Internal	Issuer	Certificates	Distinguished Name	
Edit Certificat	e				×
				full help	Q
Method	Create	an internal Certificate Aut	hority -		Saisissez un nom pour votre CA dans l
Description	OpenV	PN-Paris	•		champ Nom descriptif.
Key					Définissez le type de clé et sa longueu
Key type	RSA-40	96	•		sur RSA
Digest Algorithm	SHA512	2	•		Définissez l'algorithme de digestion sur SHA-
Issuer	self-sig	ned	• •		Laissez par défaut
Lifetime (days)	365		4		
General					Définissez la durée de vie sur 365 jo
Country Code	France		• •		Vous pouvez définir des
State or Province	ê Île-de-	France	•		valeurs aléatoires pour le
City					champs Code du
				Cancel Sav	e pays , État ou province ,
					le , Organisation et Adre
					a la sus att

Liberté Égalité Fraternité

ACADÉMIE DE MONTPELLIER BTSSIO

Cliquez sur Enregistrer en bas de la page.

Vous êtes ramené à la page principale **des autorités** et nous pouvons voir que notre autorité de certification nouvellement créée est affichée.

System: Trust: Authori	ties							
Certificates								
				C) Search	C	7•	
Description	Issuer	Name	Usages	Valid from	Valid to	Comr	nands	
SSL VPN CA	self-signed	/C=FR/ST=Île-de-France/L=Paris/O=MKVPN/OU=SYSVPN/emailAd	3	Sep 18, 2024 7:43	2 PM Sep 18, 2025 7:42 PM	0	۰ /	
OPENVPN-Paris	self-signed	/C=FR/ST=Île-de-France/L=Paris/O=mkvpb/emailAddress=mk@	3	Sep 26, 2024 7:4	1 PM Sep 26, 2025 7:41 PM	0	6	
« (1) »					s	+ howing:	🗎 L to 2 of	2 entries

4.3/Génération du certificat du serveur

Dans les menus latéraux, sélectionnez **Certificats** (nous sommes déjà dans la section **Système > Confiance** de l'interface utilisateur). La page principale **Certificats** s'affiche.

₹0₽∩ <mark>sense</mark> ` <	:
🖵 Lobby	
Reporting	
🗃 System	
Access	<u>85</u>
Configuration	5
Firmware	
Gateways	1
High Availability	c
Routes	÷
Settings	¢;
Snapshots	8
Trust	٠
Authorities	
Certificates	
Revocation	
Wizard	P
Log Files	۲
Diagnostics	(C)

Cliquez sur le signe + . La page de configuration **des certificats** s'affiche.





Edit Certificate		×
() Method	Create an internal Certificate	•
Description	OpenVpn-SERV-Paris	
∨ Key		
🚯 Туре	Server Certificate	Définissez le type sur Certificat de
Private key location	Save on this firewall	_ serveur
6 Key type	RSA-4096	•
Digest Algorithm	SHA512	Dans le menu déroulant Autorité de
 Issuer 	SSL VPN CA	 certification, selectionnez l'autorité de certification que nous venons de créer. Dans mon cas il s'agit de SSLVPN CA qui
Difetime (days)	365	(OpenVpn-Paris comme vu précedement), cela dépend de votre
✓ General		nom de certificat.
Ountry Code	France	▲
		Cancel Save

Replisser la suite, comme nous l'avons fait précédemment.





4.4/Créer un utilisateur VPN et son certificat utilisateur associé

Nous allons maintenant créer un utilisateur pour accéder à notre serveur OpenVPN.

Dans les menus latéraux, sélectionnez **Système > Accès > Utilisateurs** . La page principale **Utilisateurs** s'affiche :

EDPO sense	<
🖵 Lobby	
keporting	
🛢 System	
Access	<u>88</u>
Users	
Groups	
Servers	
Tester	
Configuration	5
Firmware	
Gateways	1
High Availability	c
Routes	ŧ
Settings	o;
Snapshots	
Trust	
Wizard	1
Log Files	۲
Diagnostics	(Ĉ)
🛔 Interfaces	
✤ Firewall	

Cliquez sur le signe + . La page **de configuration des utilisateurs** s'affiche.

System: Access: Users					
Username	Full name			Groups	•
🚢 root	System Administrator			admins	1
	System Administrator	Disabled User	Normal User		



System: Access: Users	
	full help 🖸
Defined by	USER
• Disabled	0
() Username	Mahmoud.K
Password	
	(confirmation)
	Generate a scrambled password to prevent local database logins for this user.
0 Full name	
🔁 E-Mail	MK@Mc212.ma
Comment	

OPNsense (c) 2014-2024 Deciso B.V.

0 Language	Default		
0 Login shell	/usr/sbin/nologin 👻		
6 Expiration date			
Group Memberships	Not Member Of		Member Of
			admins
			N'oublier pas de cocher cette case
Certificate	Click to create a user certificate.		pour pouvoir crée
€ OTP seed	Generate new secret (160 bit)		le certificat de votre utilisateur
Authorized kevs			votre atmoateur.

Vous arrivez sur cette page

Edit Certificate				×
() Method	Create an internal Certificate			
Description				
~ Key				
🛈 Туре	Client Certificate 🔹	-	Définisse	ez le type sur
Private key location	Save on this firewall		Certifica	t client.
G Key type	RSA-4096 -			
Digest Algorithm	SHA512 -			
() Issuer	SSL VPN CA			
1 Lifetime (days)	365			
 General 				
O Country Code	France			
				Cancel Save





Une fois rempli toutes les informations et vérifier qu'elles sont bien correctes cliquer sur enregistrer

Vous revenez à la page de configuration **de l'utilisateur** et nous pouvons voir que notre certificat client nouvellement créé a été ajouté au profil utilisateur. Cliquez à nouveau sur **Enregistrer**

User Certificates	Name	CA	Valid From	Valid To	
	OPEN-VPN-PARIS1	SSL VPN CA	Sat, 05 Oct 2024 11:57:06 +0000	Sun, 05 Oct 2025 11:57:06 +0000	• •
	+				
API keys					

Les modifications sont enregistrées et vous devriez voir Les modifications ont été appliquées avec succès en haut de la page.

4.5/Création du serveur OpenVPN

Nous avons maintenant tout ce dont nous avons besoin pour créer le serveur OpenVPN.

Dans les menus latéraux, sélectionnez VPN > OpenVPN > Serveurs . La page principale des serveurs OpenVPN s'affiche.

	E OPN <mark>sense'</mark> <	
	Lobby	
	Reporting	
	System	
*	Interfaces	
6)	Firewall	
Ø	VPN	
	IPsec	
	OpenVPN	
	Instances	
	Servers [legacy]	
	Clients [legacy]	
	Client Specific Overrides	
	Client Export	
	Connection Status	
	Log File	0
	WireGuard	-
	OpenConnect	-
•	Services	
¥	Power	
٥	Help	





Cliquez sur le signe + pour ajouter un nouveau serveur OpenVPN. La page principale de configuration du serveur OpenVPN s'affiche.

VPN: OpenVPN: Servers Protocol / Port Tunnel Network Description

VPN: OpenVPN: Servers [legacy]

General information		full help 🕥
6 Disabled	0	
Description		
Server Mode	Remote Access (SSL/TLS + User Auth)	
Backend for authentication	Local Database 👻	
Enforce local group	(none) -	
Protocol	TCP	
Device Mode	tun 👻	
0 Interface	any	
1 Local port	1194	
)PNsense (c) 2014-2024 Deciso B.V.		

Cryptographic Settings

TLS Authentication	Enabled - Authentication only
TLS Shared Key	# # 2048 bit OpenVPN static key # BEGIN OpenVPN Static key V1 02416399767339567994c02ffb0bada9 2a7cefd62094055323eefe493af33d3 600ba3cbdd1dffd8a2c9373577ab52f4 Paste your shared key here.
Peer Certificate Authority	OPENVPN_SERVER
Peer Certificate Revocation List	No Certificate Revocation Lists (CRLs) defined. Create one under System: Certificates.
Server Certificate	CA SERVR (OPENVPN_SERVER) *In Use
• Encryption algorithm (deprecated)	AES-256-GCM (256 bit key, 128 bit block, TLS client/se +
🔁 Auth Digest Algorithm	SHA512 (512-bit)





1 Certificate Depth	One (Client+Server)
6 Strict User/CN Matching	
Tunnel Settings	
1 IPv4 Tunnel Network	10.168.254.0/24
1 IPv6 Tunnel Network	
Redirect Gateway	
1 IPv4 Local Network	192.168.200.0/24
1 IPv6 Local Network	
1 IPv4 Remote Network	
1 IPv6 Remote Network	
Concurrent connections	

Compression	No Preference
Type-of-Service	
1 Inter-client communication	0
Duplicate Connections	0
Client Settings	
Oynamic IP	
Topology	





Informations générales

- 1. Indiquez un nom pour votre serveur OpenVPN dans le champ Description .
- 2. Définissez le mode serveur sur Accès à distance (SSL/TLS + authentification utilisateur) .
- 3. Définissez le backend pour l'authentification sur la base de données locale .
- 4. Définissez le protocole sur TCP4 (TCP en mode IPv4).
- 5. Réglez le mode de l'appareil sur tun .
- 6. Réglez l' interface sur WAN (afin que nous puissions nous connecter depuis l'extérieur).
- 7. Définissez le **port local** sur le port que vous souhaitez utiliser. Je le laisserai à **1194**, le port par défaut pour OpenVPN.

Paramètres cryptographiques

- 1. Dans le menu déroulant Authentification TLS , sélectionnez Activé Authentification et chiffrement .
- 2. Cochez la case Générer automatiquement une clé d'authentification TLS partagée .
- 3. Définissez l' **autorité de certification homologue** sur l'autorité de certification que nous avons créée précédemment.
- 4. Dans le menu déroulant **Certificat de serveur , sélectionnez le certificat de serveur que nous avons créé précédemment.**
- 5. Dans le menu déroulant Algorithme de chiffrement , sélectionnez AES-256-GCM .
- 6. Définissez l'algorithme Auth Digest sur SHA512 (512 bits).
- 7. Définissez la profondeur du certificat sur un (client + serveur) .
- 8. Cochez la case Correspondance stricte utilisateur/CN

Paramètres du tunnel

- 1. Saisissez un sous-réseau qui n'est pas utilisé sur votre système dans le champ **Réseau de** tunnel IPv4.
- 2. Cochez la case Rediriger la passerelle .
- 3. Sélectionnez Activé Algorithme de stub (–compress stub) dans le menu déroulant Compression .
- 4. Cochez la case communication inter-clients

Paramètres du client

- 1. Cochez la case IP dynamique .
- 2. Cochez la case Topologie .
- 3. Cliquez sur Enregistrer en bas de la page.





Vous êtes ramené à la page principale des serveurs OpenVPN et nous pouvons voir notre serveur nouvellement créé affiché dans la liste.

VPN: C	penVPN: Servers [legacy]			
	Protocol / Port	Tunnel Network	Description	•
•	TCP / 1194	10.168.254.0/24		

Vérification de la configuration du serveur OpenVPN

 Vérifions les journaux OpenVPN pour nous assurer que notre serveur est correctement configuré. Dans les menus latéraux, accédez à VPN > OpenVPN > Journaux système . La page Journaux OpenVPN s'affiche.

Vous devriez voir **la séquence d'initialisation terminée** dans les journaux si tout est correctement configuré.

₩ OPN <mark>sense</mark> <										root@OPNsei	nse.localo	domain 🛛 🌒	Q			
🖵 Lobby																
📥 Reporting		VPN: OpenVPN: L	og File													
System																
🛦 Interfaces						Q	Search		Debug		÷	Last day		- C	20 -	1
Sirewall														~		
VPN		Date	Severity	Process	Line											
IPsec	•	2024-10-05T12:16:19	Notice	openvpn_server1	Initialization Sequence Completed											>
OpenVPN	a	2024-10-05T12:16:19	Notice	openvpn_server1	TCPv6_SERVER link remote: [AF_UNS	SPEC]										>
Instances		2024-10-05T12:16:19	Notice	openvpn_server1	TCPv6_SERVER link local (bound): [A	F_INET6][undef]:1194									>
Servers [legacy]		2024-10-05T12:16:19	Notice	openvpn_server1	Listening for incoming TCP connection	on on [AF_	INET6][undef]:1194	1								>
Clients [legacy]		2024-10-05T12:16:19	Notice	openvpn_server1	setsockopt(IPV6_V6ONLY=0)											*
Client Export		2024-10-05T12:16:19	Warning	openvpn_server1	Could not determine IPv4/IPv6 proto	col. Using	AF_INET6									>
Connection Status		2024-10-05T12:16:19	Notice	openvpn_server1	/usr/local/etc/inc/plugins.inc.d/open	nvpn/ovpn	-linkup ovpns1 1500	0 0 10.1	168.254.1 2	55.255.255.0 init	t					>
Log File		2024-10-05T12:16:19	Notice	openvpn_server1	/sbin/ifconfig ovpns1 10.168.254.1/2-	4 mtu 150) up									>
WireGuard	a	2024-10-05T12:16:19	Notice	openvpn_server1	TUN/TAP device /dev/tun1 opened											>
OpenConnect	a	2024-10-05T12:16:19	Notice	openvpn_server1	TUN/TAP device ovpns1 exists previo	usly, keep	at program end									>
Services		2024-10-05T12:16:19	Warning	openvpn_server1	NOTE: the currentscript-security se	etting may	allow this configura	ation to	o call user-o	lefined scripts						*
🖋 Power		2024-10-05T12:16:19	Notice	openvpn_server1	DCO version: FreeBSD 14.1-RELEASE	-p4 stable/	24.7-n267825-d0d1	18dbba	ba SMP							•
Help																
		OPNsense (c) 2014-2024 Deciso BA	λ.													





4.6/Création de règles de pare-feu

Maintenant que nous avons configuré notre serveur OpenVPN, nous devons créer une règle de pare-feu pour autoriser le trafic vers et depuis notre serveur.

Règle OpenVPN

Dans les menus latéraux, sélectionnez Pare-feu > Règles > OpenVPN . La page Règles de l'interface OpenVPN s'affiche

ZOPO <mark>sense'</mark> <	
🖵 Lobby	
陆 Reporting	
📑 System	
🛔 Interfaces	
🚯 Firewall	
Aliases	
Automation	•
Categories	۲
Groups	4
NAT	≓
Rules	~
Floating	
LAN	
Loopback	
OpenVPN	
Opt1	
WAN	
Shaper	T
Settings	¢\$
Log Files	۲
Diagnostics	(
· · · · · ·	

Cliquez sur le signe + pour créer une nouvelle règle. La page Configuration de la règle de parefeu s'affiche.

Firew	all: Rules: O	penVPN								Select category		•	۲	Inspect
No Op	enVPN rules are curr	ently defined.	All incoming con	nnections on this inter	rface will be bloo	ked until you add a p	ass rule. Exceptions f	or automatic	ally generated ru	les may apply.				
2	Protocol	Source	Port	Destination	Port	Gateway	Schedule	ф	Description	0		•	0 6	8 0
2									Automaticall	y generated rules		0 🚯		
▶ pa ▶ pa	ss ss (disabled)	1	k block k block (disal	bled)	rejectreject	disabled)	loglog (di	abled)	÷	in out	9 7	first match last match		
m m /	Active/Inactive Schee	dule (click to vi	ew/edit)											
Alia:	s (click to view/edit)													
OpenVP explicitl	PN rules are evaluate ly passed is blocked l	d on a first-mat by default.	ch basis by defa	ult (i.e. the action of t	the first rule to m	atch a packet will be	executed). This mean	s that if you	use block rules, y	ou will have to pay atten	tion to the r	ule order. Everything	hat is i	not





irewall:	Rules:	OpenVPN	

Edit Firewall rule		full help
8 Action	Pass •	
8 Disabled	□ Disable this rule	
0 Quick	Apply the action immediately on match.	
() Interface	OpenVPN -	
Direction	in ·	
TCP/IP Version	IPv4 *	
Protocol	TCP/UDP -	
O Source / Invert	\Box Use this option to invert the sense of the match.	
Source	any •	
Source	Advanced	
O Destination / Invert	□ Use this option to invert the sense of the match.	
VPNsense (c) 2014-2024 Deciso B.V.		

O Destination port range	from:	to:
	OpenVPN +	OpenVPN -
O Log	□ Log packets that are handled by this rule	
Octegory		
Description	OpenVPN wizard	
No XMLRPC Sync	0	
Schedule	none *	
Gateway	default -	
Advanced features	Show/Hide	
Rule Information		
Created	9/26/24 16:49:11 (root@192.168.212.254)	
	Save Cancel	
Disease (a) 2014 2024 Desire P.V		





4.7/Exporter la configuration du client OpenVPN

Nous avons créé notre CA et nos certificats, notre serveur OpenVPN et nos règles de pare-feu. Il ne nous reste plus qu'à exporter notre configuration utilisateur et à nous connecter à notre serveur.

Dans les menus latéraux, accédez à VPN > OpenVPN > Exportation du client . La page Exportation du client s'affiche.







- Sélectionnez le serveur OpenVPN que nous avons créé dans le menu déroulant **Serveur d'accès à distance.**
- Définissez le type d'exportation sur Fichier uniquement.
- Saisissez votre adresse IP WAN publique dans le champ Nom d'hôte. Si vous utilisez <u>un DNS</u> <u>dynamique</u> pour accéder à l'interface WAN d'OPNsense, vous pouvez saisir votre nom d'hôte DNS dynamique dans ce champ et vous connecter en utilisant ce nom d'hôte comme adresse de serveur.
- Saisissez le port que vous avez sélectionné lors de la création du serveur dans le champ **Port**.
- Cliquez sur le bouton Télécharger à côté du nom d'utilisateur OpenVPN.

			full help 🛈
Remote Access Server	server TCP:1194 •		
Export type	File Only 👻		
() Hostname	192.168.210.254		
0 Port	1194		
🚯 Use random local port			
6 Validate server subject			
Windows Certificate System Store	0		
Oisable password save	0		
O Custom config			
Accounts / certificates			
Certificate		Linked user	
(none) Exclude certificate from export		۵	
CA SERVR		۵	
Mahmoud.K		Mahmoud.K 🛆	

OPNsense (c) 2014-2024 Deciso B.V.





4.8/Configuration du NAT

La traduction d'adresses réseau (NAT) est utilisée pour traduire des adresses IP privées en adresses IP publiques. OpnSense propose plusieurs options NAT, notamment le transfert de port, le NAT 1:1 et le NAT sortant. Vous pouvez configurer NAT en accédant à Pare-feu > NAT.

Sur l'OPNsense de Perpignan et de Paris, il faudra ajouter une règle NAT (Network Address Translation) :

2 D 🖸 Port Forward	I NAT Firewall OP	× +				- 0 ×
← C 🛛 😣 Non sée	curisé https ://1	92.168.212.1/firewall_nat_edit.php			at A 🖒	0 🕼 🐨 🗞 🏈
EDP D sense	<			1	root@OPNsense.localdomain	
Reporting		Firewalls NAT: Dort Fo	muand			
System		Filewall, NAL FOIL FO	iwaid			
Interfaces		Edit Redirect entry				full help 🕥
Firewall						
Aliases		Disabled	Disable this rule		L'interface pai	lequel se fera la
Automation	•	No RDR (NOT)			translation d'a	dresse (NAT) dans
Categories		Interface			notre cas WAI	J
Groups			WAN	· ·		
Port Forward	-	TCP/IP Version	IPv4	•		
One-to-One					——— Ipv4 ou IPV	6 ou IPV4+IPv6
Outbound		Protocol	TCP	· ·		
NPTv6		Source				DIE TCF, ODF OU
Rules	~		Advanced		TPC/UDP	
Shaper	т	 Destination / Invert 				
Settings	¢;	Destination				
Log Files	۲		Single host or Network			- Destination dans
Diagnostics	۵			32		notre cas la
VPN		Operation 10 Destination port range	from:		to:	notic cus la
Services		OPNsense (c) 2014-2024 Deciso B.V.				Wan Paris





4.9/Outbound (NAT)

Allez dabns Firewall -> NAT -> Outbound.

	Lobby	
	Reporting	
=	System	
	Interfaces	
6)	Firewall	
	Aliases	
	Automation	٥
	Categories	۲
	Groups	
	NAT	≓
	Port Forward	
	One-to-One	
	Outbound	
	NPTv6	
	Rules	~
	Shaper	T
	Settings	Q °
	Log Files	۲
	Diagnostics	
0	VPN	
٥	Services	
۶	Power	
٥	Help	

Par défaut il existe ces règles, il faudra ajouter une nouvelle.





Tout d'abord

Firewall: NAT: Outbound Mode Automatic outbound NAT rule generation (no manual rules can be used) Hybrid outbound NAT rule generation (automatically generated rules are applied after manual rules) ۲ Manual outbound NAT rule generation (no automatic rules are being generated) Disable outbound NAT rule generation (outbound NAT is disabled) Save Automatic rules Source Networks Source Networks, Opt1 networks, 127.0.0.0/6, 10.168.254.022 Electionne Hybrid outbound nat VES NAT Address NAT Port Static Port Description Interface Source Networks ► LAN Auto created rule for ISAKMP LAN Auto created rule WAN • YES WAN • NO WAN Loopback networks, Opt1 networks, 127.0.0.0/8, 10.168.254.0/24 500 . . Auto created rule for ISAKMP . . . WAN Loopback networks, Opt1 networks, 127.0.0.0/8, 10.168.254.0/24 Auto created rule

Mada													
O	Automatic ou (no manual ru	Automatic outbound NAT rule generation (no manual rules can be used)					d outbound NAT rule natically generated r	generation ules are applied after m	anual rules)				
0	Manual outbo (no automatie	und NAT rule gen rules are being g	eration generated)			O Disabl (outbo	e outbound NAT rule ound NAT is disabled)	generation					
Save													
Manual	rules										Select category		
0	Interface	Source	Source Port	Destination	Destination P	ort	NAT Address	NAT Port	Static Port	Desci	iption	+ + * • •	
	WAN	any	•	•	•		Interface address	*	NO			< / B B	
Ena	bled rule												
Disa	bled rule												
Automa	tic rules												
	Interface	Source Networ	ks			Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	
►	LAN	Loopback netw	vorks, Opt1 networks,	127.0.0.0/8, 10.168.254.0/	24	•		500	LAN	*	YES	Auto created rule for ISAKMP	
•	LAN	Loopback netw	vorks, Opt1 networks,	127.0.0.0/8, 10.168.254.0/	24	•		*	LAN	*	NO	Auto created rule	
•	WAN	Loopback netw	orks, Opt1 networks,	127.0.0.0/8, 10.168.254.0/	24	•	•	500	WAN	•	YES	Auto created rule for ISAKMP	
	 a) 2014 2024 Partie 	- P.V											

Configurer selon vos réseaux.





4.10/Connexion au tunnel sécurisé sur le client coté perpignan.

Installer OpenVPN sur internet (<u>https://openvpn.net/community-downloads/</u>)

Lancer et importer la configuration.

OpenVPN Co	nnect		- >
≡	Get cor	nnected	P
	URL	UPLOAD FIL	E
Drag a You ca	and drop to u n import only	/PN pload *.OVPN prof one profile at a ti	file me.
On't	have '.ovpn' file?		ď
	BRO	WSE	





Connecter-vous avec vos identifiants.







Et vous voilà connecter !

OpenVPN C	onnect		- ×
≡	Profile	es	Ð
CONNE	CTED		
	OpenVPN Profile 192.168.210.254 [openvpn_Mahm	e noud_K]	
CONNE	CTION STATS		_
7.3KB/s			_
OB/S BYTES IN 576 B/S	↓	120 BYT	ES OUT B/S
DURATIO 00:00:0	N PAC 6 3 s	CKET RECEIVED ec ago)
YOU Mahmou	ıd.K		•

YOU Mahmoud.K YOUR PRIVATE IP 10.168.254.3 SERVER 192.168.210.254 SERVER PUBLIC IP 192.168.210.254 PORT VPN PROTOCOL TCP



On va voir, si on accéder bien à notre site distant :

Dans mon cas l'adresse sera : <u>https://192.168.200.11</u>







On peut réaliser égalament un tracert pour voir le chemin emprunter :

CMD -> tracert @IP







4.11/Règles pour bloquer un site

Il vous suffit tout d'abord d'aller dans Aliases dans FireWall -> Aliases puis Crée un nouveau Aliases

ి 🗖 📲 Maroc.ma	I	× 1 Nouvel of	onglet X 🗓	Aliases Firewall OPNsense.local × +					- 0
← C 🛛 😣 Non se	écurisé https:/	/192.168.212.1/ui/f	irewall/alias					88 A ⁿ 🖒 🖽 🕉	• @ % ···
	• <					root@C	PNsense.localdom	ain 💿 🔍	
Lobby Reporting		Firewall: A	liases					0% (2	3/1000000)
System		Aliases Ge	eoIP settings						
) Firewall	_				Q Search	Filter type	•	Categories 🔹 💭	7
Allases	•	Enabled	Name	Туре	Description	Content	Loaded#	Last updated	Commands
Categories		0 8	chatgpt	Host(s)		www.chatgpt.com	4	2024-09-30 13:21:34	/ 0 8
Groups	ф	0 8	chatgptip	Host(s)		www.chatgpt.com 172.	5 4	2024-09-30 13:22:33	/ 0 0
NAT	=		bogons	External (advanced)	bogon networks (internal)		10		
Rules	×	0 0	bogonsv6	External (advanced)	bogon networks IPv6 (int				
Shaper	т	0 8	virusprot	External (advanced)	overload table for rate li		0		
Settings	O ^o		sshlockout	External (advanced)	abuse lockout table (inte		0		
Log Files	۲		wan_network	Internal (automatic)	wan net		1		
Diagnostics	â								1
VPN									0 0
Services								Showing 1	to 7 of 10 entries
Power		1	2 > *					choning a	to r or to church
D Help									
		Apply							
								Activer Windows	
		OPNsense (c) 2014-2	024 Deciso B.V.						r activer Windows.
ttps://192.168.212.1/ui/firewall/	/alias#Firewall_NAT								

Par quel type, souhaitez-vous bloquer :

Pour ma part pour ChatGpt, ça sera Host(s)

Edit Alias		×
		full help 🛈
1 Enabled	✓	
() Name	LE NOM DE VOTRE SITE	
О Туре	Host(s) 🔹	
O Categories	Host(s)	
() Content	Port(s) URL (IPs)	
1 Statistics	URL Table (IPs)	
Description	GeoIP Network group	
	MAC address BGP ASN Dynamic IPv6 Host	Cancel Save
	OpenVPN group Internal (automatic) External (advanced)	



Edit Alias	×
	full help 🖸
1 Enabled	
O Name	LE NOM DE VOTRE SITE
🛈 Туре	Host(s) -
Categories	
1 Content	©IP/CIDR DU SITE A BLOQUER × URL DU SITE × © Clear All ⁽²⁾ Copy ■ Paste
1 Statistics	
Description	
	Cancel Save

Maintenant ajouter une règle sur le réseau ou vous voulez le bloquer :

ి 🗖 👹 Maroc.ma	I	X 🖍 Nouvel onglet	× 🗉 u	N Rules Firew	all OPNse	nse × +												-	0
	sécurisé https	k//192.168.212.1/firewall_rule	s.php?if=lan									86	Aø.		¢D	£^≣	ŵ		
	<								roo	it@OPNs	ense.localdomain		۹						
Lobby		Circura III: Dedacar									1								
Reporting		Firewall: Rules:	LAN								Select category	(Inspect	
🕯 System																			
Interfaces		0	Protocol	Source	Port	Destination	Port	Gateway	Schedule	ф	Description @					•		8 0	
Firewall											Automatically ¿	generate	d rules			020			
Aliases		□ × → * 0	IPv4+6 TCP/UDP			chatgpt 🔳	53 (DNS)		,							+ /	0	۵	
Automation	٥	□ × → + 0	IPv4+6 TCP/UDP	•		chatgptip 🧮										+ /	0	۵	
Categories	۲	□ ► → † 0	IPv4 *					•								+ /	0		
Groups	#	□ ► → + 0	IPv6 *													+ /	0		
NAT	=	pass	× block			O reject		0 lo	2		→ in			4	first ma	tch			
Rules	~	pass (disabled)	× block	(disabled)		O reject (dis	abled)	O lo	g (disabled)		← out			4	last mat	tch			
Floating		M Active/Inactive Sc	hedule (click to view/edit)																
LAN		III Alias (click to view/ed	it)																
Loopback		LAN rules are evaluated o	in a first-match basis by di	fault (i.e. the a	ction of th	e first rule to match	a packet will be	executed). This r	neans that if you i	use block	rules, you will have	e to pay	attenti	on to the	rule ord	ler. Ever	ything	that is	
OPI1		not explicitly passed is of	ocked by defaults																
WAR .	-																		
Snaper	~																		
Jea files	0,																		
Dischartin																			
unagriusaics	G																		
VPN																			
a pervices												Act		Vinde					
Power													dez au	x parar					
D Help		OPNsense (c) 2014-2024 Deciso	B.V.																

Chatgpt est désormais bloquer.

🙎 🗖 🔿 ehatgot.com 💦 🗙 🚺 Maroc.ma) 🛛 x (=1 192.168.200.11 🛛 x (+			-	0)
← X ③ https://chatgpt.com	A* 🔂 🖬) 🕸 🕀	-	4
				0
***				-
Désolé, impossible d'accéder à cette page.				
chatgpt.com a mis trop de temps pour répondre				
Essayez :				
Vérification de la connexion				
Ventication du proxy et du paré-feu				
ant convertion (see) on				
Diagnostiquer le problème Actualiser				
	AntipactAlederate			





5/Merci pour votre lecture !





