PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : MOREAU

Prénom : Matt

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), MOREAU , Matt , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Bouguenais
Date 26/03/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : MOREAU Matt	**N° candidat : 02542583108**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 28/05/2026

Organisation support de la réalisation professionnelle

Entreprise fictive **Oasis** et prestataire **NTxSystem**

Intitulé de la réalisation professionnelle

Mise en place de pare-feu OPNsense

Période de réalisation : 2024 - 2026 *Lieu :* CFA Fab'Academy Bouguenais (UIMM)

Modalité : ☐ *Seul(e)* ☒ *En équipe*

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau
☒ Installer, tester et déployer une solution d'infrastructure réseau
☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Mise en place d'une solution de pare-feu OPNsense afin de répondre aux exigences de sécurité réseau. La solution doit permettre d'assurer le routage de l'infrastructure, le filtrage réseau, le NAT ainsi que la mise en place de connexions VPN site à site.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Différentes ressources ont été utilisées pour la mise en place de la solution de pare-feu, tout d'abord pour les ressources documentaires, la ressource principale utilisée a été la documentation officielle de OPNsense ainsi que différentes pages expliquant les différentes notions. Pour les ressources matérielles, un Serveur HP en tant qu'hyperviseur a été utilisé, pour les ressources logicielles, ESXI VMware et OPNsense ont été utilisés.

Modalités d'accès aux productions[3] et à leur documentation[4]

L'ensemble des documents liés à l'infrastructure est disponible sur le partage réseau accessible depuis le réseau BTS SIO. Cet emplacement est dédié au stockage des informations relatives à la section. Il contient notamment des documentations sur l'environnement virtuel déployé, l'ensemble de la configuration de l'infrastructure mise en place, les différentes solutions étudiées, le plan d'adressage ainsi que les différents schémas réalisés de l'infrastructure.

L'ensemble des mots de passe de l'infrastructure sont conservés dans notre gestionnaire de mot de passe Bitwarden.

Partage Réseau Documentation NTxSystem : \\partage.btssio.nte\fichiers\BAIES-PEDA\NTXSYSTEM

Identifiant Bitwarden : ntxsystem@proton.me
Mot de passe Bitwarden : NTxbitwarden44.
Lien Bitwarden : https://vault.bitwarden.com

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

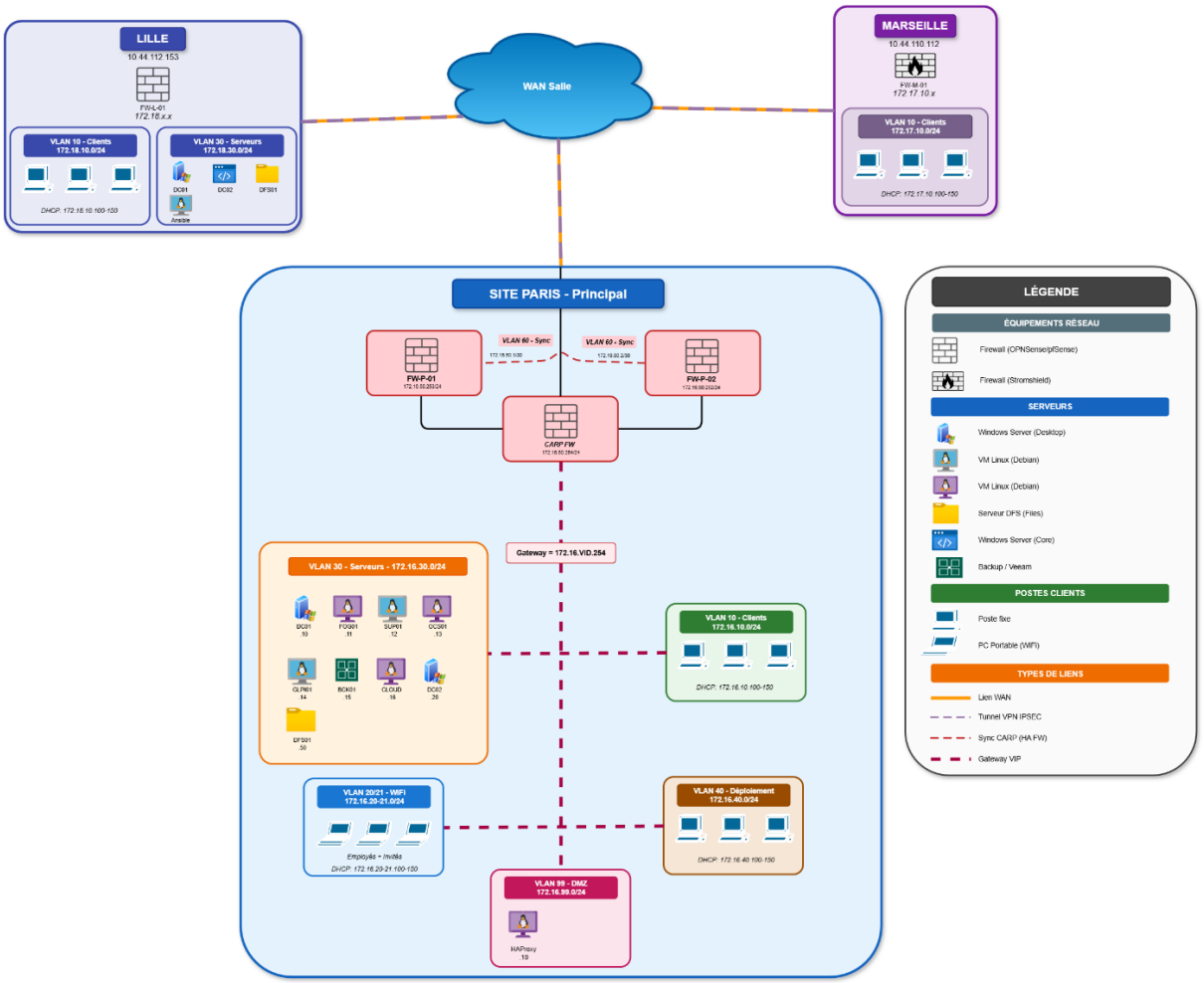
A travers cette réalisation professionnelle portant sur la mise en place d'un pare-feu permettant de segmenter le LAN et le WAN de façon sécurisée, différents outils ont été montés au sein de l'infrastructure, tout l'environnement est virtualisé sur deux serveurs HP utilisant VMware ESXi et il y a différentes machines virtuelles dédiées à différents services.

Cette infrastructure a été construite sur trois sites. Le premier correspondant au site commun au groupe NTxSystem, le site de Paris, le second correspondant au site de Marseille, sur lequel il est possible de retrouver des clients et le dernier correspondant à mon site personnel, se trouvant sur les Proxmox de la salle BTS SIO, le site de Lille.

L'objectif principal de cette réalisation était de mettre en place une solution permettant de segmenter le LAN et le WAN de manière sécurisée. Pour répondre à ce besoin, j'ai utilisé l'outil OPNsense afin de disposer d'une machine permettant de relier les différents réseaux de manière sécurisée via des règles de pare-feu. Cette solution s'appuie sur FreeBSD.

Grâce à cette solution, il est possible de segmenter les différents réseaux de manière sécurisée avec une redondance entre les deux pare-feux, ainsi que de faire communiquer les différents sites grâce aux tunnels VPN.

Ci-dessous les schémas logique et physique ainsi que le plan d'adressage de l'infrastructure.


LILLE
10.44.112.153
FW-L-01
172.16.x.x
VLAN 10 - Clients
172.16.10.0/24
VLAN 30 - Serveurs
172.16.30.0/24
DHCP: 172.16.10.100-150
WAN Salle
MARSEILLE
10.44.110.112
FW-M-01
172.17.10.x
VLAN 10 - Clients
172.17.10.0/24
DHCP: 172.17.10.100-150
SITE PARIS - Principal
VLAN 60 - Sync
VLAN 60 - Sync
FW-P-01
FW-P-02
CARP FW
Gateway = 172.16.VID.254
VLAN 30 - Serveurs - 172.16.30.0/24
VLAN 10 - Clients
172.16.10.0/24
DHCP: 172.16.10.100-150
VLAN 20/21 - WIFI
172.16.20-21.0/24
Employés + Invités
DHCP: 172.16.20-21.100-150
VLAN 40 - Déploiement
172.16.40.0/24
DHCP: 172.16.40.100-150
VLAN 99 - DMZ
172.16.99.0/24
HAProxy
LÉGENDE
ÉQUIPEMENTS RÉSEAU
Firewall (OPNSense/pfSense)
Firewall (Stormshield)
SERVEURS
Windows Server (Desktop)
VM Linux (Debian)
VM Linux (Debian)
Serveur DFS (Files)
Windows Server (Core)
Backup / Veeam
POSTES CLIENTS
Poste fixe
PC Portable (WIFI)
TYPES DE LIENS
Lien WAN
Tunnel VPN IPSEC
Sync CARP (HA FW)
Gateway VIP
LÉGENDE
Liaison Infrastructure

Plage IP de base :	Description :
10.44.150.0/24	Plage IP du WAN

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

Proxmox Matt (Lille)

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-L-DC01	172.18.30.10	255.255.255.0	172.18.30.0	172.18.30.254	DC1 Lille
SRV-L-DC02	172.18.30.20	255.255.255.0	172.18.30.0	172.18.30.254	DC2 Core Lille
SRV-L-ANS01	172.18.30.15	255.255.255.0	172.18.30.0	172.18.30.254	Ansible Lille
SRV-L-NETBOX01	172.18.30.30	255.255.255.0	172.18.30.0	172.18.30.254	Netbox Infrastructure
FW-L-01	172.18.10.254	255.255.255.0	172.18.10.0	172.18.10.254	IP FW-L-01 LAN Lille
FW-L-02	172.18.10.252	255.255.255.0	172.18.10.0	172.18.10.254	IP FW-L-02 LAN Lille
CARP Firewall Lille	172.18.10.254	255.255.255.0	172.18.10.0	172.18.10.254	Passerelle du VLAN 10
FW-L-01	172.18.30.254	255.255.255.0	172.18.30.0	172.18.30.254	IP FW-L-01 SRV Lille
FW-L-02	172.18.30.252	255.255.255.0	172.18.30.0	172.18.30.254	IP FW-L-02 SRV Lille
CARP Firewall Lille	172.18.30.254	255.255.255.0	172.18.30.0	172.18.30.254	Passerelle du VLAN 30
FW-L-01	172.18.60.1	255.255.255.252	172.18.60.0	-	IP FW-L-01 SYNC_OPN
FW-L-02	172.18.60.2	255.255.255.252	172.18.60.0	-	IP FW-L-02 SYNC_OPN
FW-L-01	172.18.99.254	255.255.255.0	172.18.99.0	172.18.99.254	IP FW-L-01 DMZ Lille
FW-L-02	172.18.99.252	255.255.255.0	172.18.99.0	172.18.99.254	IP FW-L-02 DMZ Lille
CARP Firewall Lille	172.18.99.254	255.255.255.0	172.18.99.0	172.18.99.254	Passerelle du VLAN 99
FW-L-01	10.44.115.50	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Lille
FW-L-02	10.44.112.100	255.255.255.0	10.44.112.0	10.44.112.254	IP FW-L-02 WAN
CARP Firewall Lille	10.44.112.153	255.255.255.0	10.44.112.0	10.44.112.254	CARP WAN

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	SS	172.18.10.254	172.18.30.10	172.18.30.20	Plage DHCP Client Lille

Pour plus de détails, les deux schémas montrant l'ensemble de l'infrastructure ainsi que le plan d'adressage peuvent être trouvés en Annexe n°1 pour le schéma logique, en annexe n°2 pour le schéma physique et en annexe n°3 pour le plan d'adressage.

BTS Services informatiques aux organisations SESSION 2026
ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE
En référence à l'annexe II.E – « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[5]	**Fab'Academy, 9 Rue de l'Halbrane, 44340 Bouguenais**	**SISR**

1. Environnement commun aux deux options
1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	**Active Directory Windows**	
Un SGBD	**MySQL / MariaDB**	
Un accès sécurisé à internet	**Firewall OPNsense, Stormshield**	
Un environnement de travail collaboratif	**DFS/DFSR (Partage de fichiers), Nextcloud**	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	**GLPI (Debian), Windows Server 2022**	

[5] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Veeam B&R	
Des ressources dont l'accès est sécurisé et soumis à habilitation	DFS/DFS/R (Partage de fichier), Nextcloud	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Tablette / PC Portable via connexion Wifi	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Wazuh, Stormshield	
Chiffrement	TLS, IPsec, SSH, PKI	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentation VLANs via Switch	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Partage Réseau avec droits d'accès via DFS/R suivant méthode AGDLP	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible, GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH, RDP, HTTPS	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Centreon	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Firewall OPNsense, HaProxy, VPN	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	**Veeam B&R, Haute disponibilité OPNsense**	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**RAID 1, redondance switch et Firewall OPNsense**	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	**DFS/R , DHCP, DNS, Firewall OPNsense**	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	**VPN IPsec**	
Une solution permettant le déploiement des solutions techniques d'accès	**FOG, Ansible**	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Ansible, Batch GPO**	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Stormshield IPS, Wazuh**	

Projet : Mise en place de Firewall OPNsense

a) Contexte

Dans le cadre de ma formation BTS SIO, j'ai eu l'opportunité d'intervenir sur un projet de mise en place d'infrastructure réseau et sécurité pour l'entreprise Oasis.

Ce projet consiste à accompagner Oasis dans la conception et le déploiement de son infrastructure informatique pour sa nouvelle agence, tout en assurant une communication sécurisée avec les autres sites. Pour répondre à ces besoins, j'ai été amené à mettre en place une solution de pare-feu OPNsense, permettant de sécuriser les échanges entre les différents sites et de garantir la protection du réseau interne.

b) Présentation de l'entreprise Oasis

L'entreprise Oasis est une société parisienne spécialisée dans la conception de voyages sur mesure pour une clientèle exigeante, à la recherche d'expériences uniques, loin des circuits touristiques classiques.

Créé en 2017, elle s'est rapidement imposée comme un acteur innovant dans le secteur du tourisme personnalisé, grâce à une approche centrée sur l'écoute client, la connaissance culturelle approfondie des destinations, et un réseau de partenaires locaux dans plus de 30 pays.

Après plusieurs années de forte croissance, Oasis a décidé d'ouvrir une nouvelle agence à Marseille, pour mieux couvrir le sud de la France et répondre à une demande croissante dans cette zone. L'agence parisienne reste le siège social et le cœur de la stratégie de conception et de relation client haut de gamme.

En 2024, Oasis a atteint un chiffre d'affaires de 2,3 millions d'euros, et ambitionne désormais de renforcer sa structure numérique afin d'améliorer la coordination entre les sites, la sécurité des données clients, et la fluidité de l'expérience interne.

C'est dans ce contexte de croissance que NTxSystem a été sollicitée pour concevoir et déployer une infrastructure informatique adaptée aux besoins d'Oasis que ce soit pour l'agence parisienne, le siège social où pour l'agence de Marseille.

c) Présentation de l'entreprise NTxSystem

NTxSystem est une entreprise prestataire spécialisée dans les solutions informatiques pour les professionnels. Dans le cadre de l'expansion d'Oasis, NTxSystem a été chargé de concevoir et déployer l'ensemble de l'infrastructure réseau des agences Paris et Marseille.

Les enjeux de ce projet sont multiples : centralisation des services, virtualisation des ressources, gestion des utilisateurs, sécurisation des communications inter-sites et mise en place d'un environnement stable et évolutif.

Pour répondre aux différentes exigences d'Oasis, l'ensemble de l'infrastructure est déployé dans un environnement virtualisé VMware ESXi.

d) Cahier des charges

L'entreprise Oasis a chargé NTxSystem de concevoir et de tester une infrastructure système et réseau virtualisée, capable de répondre aux besoins opérationnels et organisationnels de l'entité.

Les attentes techniques de la direction portent sur la centralisation des services, la virtualisation des ressources, la gestion des utilisateurs, la communication inter-sites, et la mise en place d'un environnement stable, évolutif et sécurisé, le tout dans un environnement de test isolé avant déploiement réel.

Dans ce cadre, j'ai eu la charge de mettre en place le pare-feu OPNsense, afin d'assurer la séparation du LAN et du WAN, d'appliquer des règles de sécurité adaptées aux besoins d'Oasis, et de garantir une infrastructure réseau cohérente et sécurisée.

e) Analyse du besoin

Avant de réaliser le projet, nous avions fait une veille sur les différentes solutions que l'on avait à notre disposition par rapport à notre infrastructure.

Pour cela, nous avons réalisé une analyse du besoin, dans cette étude, nous avons comparé trois solutions, PFsense, OPNsense et Stormshield en fonction de différents critères :

- Est-ce que les solutions sont toujours maintenu à jour ?
- Quelle est la difficulté de mise en place pour chaque solution ?
- Y'a-t-il de la documentation sur chaque solution ?

Ces différents critères nous permettent de juger quel est la solution la plus adapté par rapport à notre besoin général.

f) Etude de solutions

Dans un premier temps, pour le premier critère par rapport à la maintenance de la solution, nous avons pu regarder si chaque solution était toujours maintenue à jour à partir des sites officiels ou de GitHub.

Ensuite, pour le second critère, nous avons pu évaluer la difficulté de la mise en place pour chaque solution en fonction des documentations et en testant chaque solution.

Enfin pour le troisième critère, nous avons pu évaluer la documentation de chaque solution en regardant si celle-ci était maintenue à jour et si elle répondait à tous nos besoins.

Grâce à ces différents points, nous avons pu réaliser l'étude de solutions ci-dessous.

Les solutions	Solution 1	Solution 2	Solution 3
Intitulé	Pfsense	OPNsense	Stormshield
Faisabilité technique *(Oui / Non, en précisant pourquoi)*	Pfsense est une solution fiable, celle-ci à 21 ans d'expérience, sa dernière mise à jour date de cette année mais les mises à jour vont être arrêté prochainement, l'outil va devenir obsolète.	OPNsense est une solution qui est basé sur Pfsense qui est fiable, sa dernière mise à jour date de cette année, les mises à jour vont être continué contrairement à Pfsense.	Stormshield est une solution française et commerciale spécialisée dans la cybersécurité, ses mises à jour sont régulières et assurées sur le long terme, elle est certifiée par l'ANSSI ce qui en fait une solution fiable.
Besoins RH *(Internes et/ou Externes)*	Interne	Interne	Interne
Besoin Matériel et Immatériel	Serveur Physique (hyperviseur), ISO Pfsense	Serveur Physique (hyperviSseur), ISO OPNsense	Firewall Stormshield Physique
Coût total estimé	0	0	0
Temps Jours / Hommes	1,5	1,5	3
Durée de réalisation estimée	4h30	5h	6h
Points forts **Points faibles**	• PF: Expérience sur la solution, Documentation facilement accessible, code fermé, moins destiné au développement • Pf: Support payant, interface fonctionnelle mais datée, moins de fonctionnalité, des mises à jour moins récurrente	• PF: Interface moderne, solution qui est encore en développement, plus de mise à jour récurrente et de fonctionnalités • Pf: Support payant, interface qui est peut être complexe au départ, moins d'expérience	• PF: Matériel Physique, meilleure performance et plus de fonctionnalités • Pf: Interface vieillissante (matériel à disposition vieillissant), plus de mises à jour, interface plus complexe, support payant

Nous pouvons voir sur ce tableau que les besoins matériels restent globalement les mêmes sauf pour Stormshield qui a besoin d'un appareil physique dédié. Ensuite, PFsense et OPNsense sont deux solutions semblables mais il y a des changements au niveau des mises à jour et de la modernité de l'interface.

Grâce à ces différentes comparaisons et à la veille réalisée sur les documentations de chaque solution, nous avons conclu que la solution OPNsense correspondait le plus à nos besoins car celle-ci est gratuite, non gourmande en ressources, plutôt facile à mettre en place, elle a une interface moderne et est maintenue à jour.

g) Planification

Le projet pour la mise en place de la solution OPNsense a été séparé en diverses étapes, ces étapes sont détaillées dans les différentes parties.

1) Discussion de la problématique

Cette partie correspond à l'étude de la mission donnée par Oasis afin de comprendre comment séparer le WAN et le LAN de façon sécurisée.

2) Réalisation de l'étude de solutions

Dans cette partie, j'ai pu étudier les différents besoins sur cette séparation LAN / WAN afin de voir quelles étaient les solutions à ma disposition pour répondre au cahier des charges.

3) Réalisation du GANTT

Pour cette étape, j'ai pu lister les différentes tâches pour la mise en place d'un pare-feu et j'ai pu formuler cela sous forme d'un GANTT afin d'avoir une prévision sur les différentes tâches.

4) Installation de la machine virtuelle

L'installation correspond à la création de la machine virtuelle, l'ajout des différentes ressources pour celle-ci et la première configuration afin de pouvoir accéder à l'interface de OPNsense.

5) Configuration des interfaces

La configuration des interfaces correspond à l'ajout des différentes cartes réseaux dans l'interface OPNsense ainsi que la configuration des adresses IP.

6) Ajout des différents alias

L'ajout des différents alias correspond à l'ajout de nom par rapport aux adresses IP configurées et l'ajout de groupe de ports afin de segmenter les règles pour chaque service.

7) Mise en place de règles

La mise en place de règles correspond à la sécurisation pour le passage des paquets entre les différents VLANs ainsi que le WAN.

8) Configuration des accès à internet

La configuration des accès à internet correspond à la mise en place de route afin d'accéder à internet depuis le LAN.

9) Mise en place du LDAP

La mise en place du LDAP correspond à la configuration pour se connecter sur le pare-feu à partir de certains utilisateurs de l'Active Directory.

10) Configuration Haute Disponibilité (CARP)

La configuration de la Haute Disponibilité correspond à la mise en place de la redondance de pare-feu.

11) Configuration de l'IPsec

L'ajout de la fonctionnalité IPsec permet de créer des tunnels VPN entre différents sites pour qu'ils puissent communiquer

12) Test accès à internet

Ce premier test correspond au fait de tester l'accès à internet depuis les différents VLANs sur le LAN.

13) Test différents services

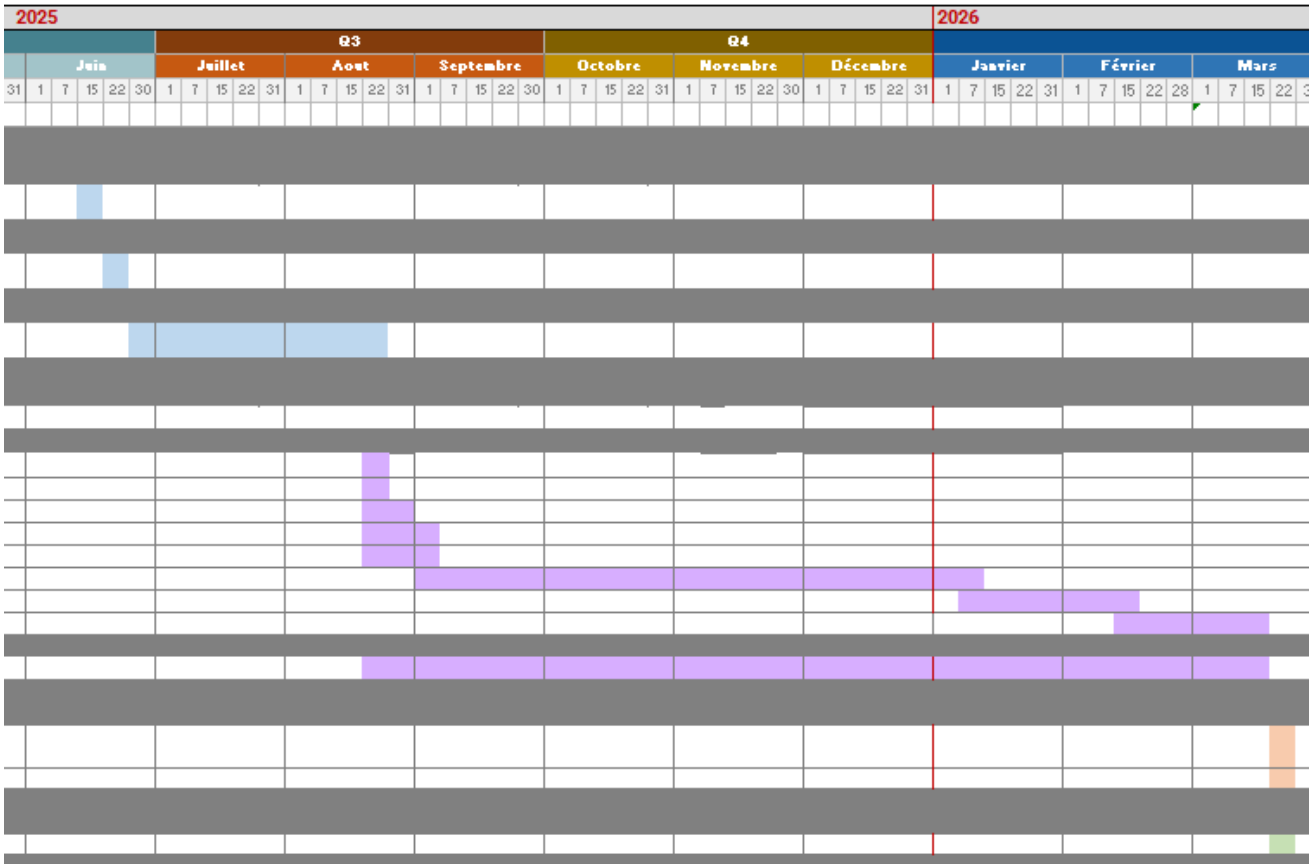
Ce second test correspond au fait de tester si les différents services sont fonctionnels avec les règles de pare-feu mises en place.

14) Clôture du projet

Pour terminer, la clôture du projet correspond à la fin du projet, cela nous permet de vérifier que le projet a bien répondu au cahier des charges.

Ci-dessous, nous pouvons voir les tâches du diagramme de Gantt ainsi que le diagramme correspondant. Celui-ci permet de voir et de comprendre l'ensemble des tâches du projet. Nous pouvons également voir à qui elles sont attribuées et le temps de réalisation de ces différentes tâches.

LOT	INTITULE DE LA PHASE	INTERVENANT(S)	TEMPS J/H	DATE DE DÉBUT	DEADLINE	DATE DE FIN RÉELLE	COMMENTAIRE(S)	STATUT	TÂCHES TERMINÉES (EN %)
Phase 1 : Initialisation			**3h30**	**12-juin-25**	**25-août-25**	**25-août-25**		**Terminé**	**100 %**
	Phase 1 : Initialisation								
	Discussion de la problématique	NTxSystem	1h	12-juin-25	20-juin-25	20-juin-25		Terminé	100 %
	Phase 2 : Faisabilité								
	Réalisation de l'étude de solutions	Matt MOREAU	1h30	20-juin-25	27-juin-25	27-juin-25		Terminé	100 %
	Phase 3 : Etude et Cadrage								
	Réalisation du GANTT	Matt MOREAU	1h	30-juin-25	25-août-25	25-août-25		Terminé	100 %
Phase 2 : Réalisation, Déploiement & Recette			**7h30**	**25-août-2025**	**20-mars-2026**	**19-mars-2026**			
	Phase 4 : Matériel								
	-	-	-	-	-	-		Terminé	100 %
	Phas 5 : Installation et Configuration solution								
	Installation Machine Virtuelle	Matt MOREAU	30min	25-août-2025	29-août-2025	25-août-2025		Terminé	100 %
	Configuration des interfaces	Matt MOREAU	30min	25-août-2025	29-août-2025	25-août-2025		Terminé	100 %
	Ajout d'alias & Alias de Ports	Matt MOREAU	30min	25-août-2025	28-août-2025	28-août-2025		Terminé	100 %
	Mise en place de règles	Matt MOREAU	1h30	25-août-2025	5-sept.-2025	4-sept.-2025		Terminé	100 %
	Configuration accès à internet	Matt MOREAU	15min	25-août-2025	5-sept.-2025	4-sept.-2025		Terminé	100 %
	Mise en place LDAP	Matt MOREAU	45min	5-sept.-2025	9-janv.-2026	8-janv.-2026		Terminé	100 %
	Configuration Haute Disponibilité (CARP)	Matt MOREAU	2h	9-janv.-2026	20-févr.-2026	20-févr.-2026		Terminé	100 %
	Configuration IPsec	Matt MOREAU	1h30	20-févr.-2026	20-mars-2026	19-mars-2026		Terminé	100 %
	Phase 6 : Documentation								
	Réalisation documentation complète de la solution	Matt MOREAU	4h	25-août-2025	20-mars-2026	20-mars-2025		Terminé	100 %
Phase 3 : Exploitation			**40min**	**16-mars-2026**	**20-mars-2026**	**20-mars-2026**			
	Phase 7 : Test de la solution								
	Test accès à internet	Matt MOREAU	10min	16-mars-2026	16-mars-2026	20-mars-2026		Terminé	100 %
	Test différents services par rapport règles pare-feu	Matt MOREAU	30min	16-mars-2026	20-mars-2026	20-mars-2026		Terminé	100 %
Phase 4 : Clôture du Projet			**10min**	**20-mars-26**	**20-mars-26**	**20-mars-26**			
	Phase 8 : Clôture du Projet								
	Clôture du Projet	Matt MOREAU	10min	20-mars-2026	20-mars-2026	20-mars-2026		Terminé	100 %



h) Définitions et abréviations

Pare-feu (Firewall) : Un pare-feu est un outil de sécurité réseau qui permet de filtrer et de contrôler le trafic entrant et sortant d'un réseau. Il agit comme une barrière entre un réseau interne et l'extérieur, en autorisant ou en bloquant les communications en fonction de règles définies au préalable.

NAT : Le NAT (Network Address Translation) est une technique qui permet de traduire des adresses IP. Il est utilisé pour permettre de communiquer avec des machines disposant d'adresses IP privées depuis une adresse IP publique.

Route par défaut : La route par défaut est une route qui permet de diriger tout le trafic qui ne correspond à aucune autre route vers une passerelle spécifique.

LDAP : Le LDAP (Lightweight Directory Access Protocol) est un protocole qui permet d'accéder à un annuaire d'entreprise. Il est utilisé pour centraliser l'authentification des utilisateurs en se basant sur un Active Directory.

CARP : Le CARP (Common Address Redundancy Protocol) est un protocole qui permet de mettre en place de la haute disponibilité entre plusieurs pare-feux. Il fonctionne sur un principe de master et de backup, c'est-à-dire qu'un pare-feu principal prend en charge l'ensemble du trafic et si celui-ci ne fonctionne plus, le pare-feu de backup prend alors automatiquement le relais afin d'assurer la continuité du service.

IP Virtuelle : Les adresses IP virtuelles sont des adresses IP partagées entre les deux pare-feux dans le cadre du CARP. C'est sur ces adresses que le trafic est dirigé, ce qui permet lors d'une bascule du master vers le backup que les communications ne soient pas interrompues, car l'adresse IP reste la même peu importe quel pare-feu est actif.

VPN : Le VPN (Virtual Private Network) est un outil qui permet de créer un tunnel sécurisé entre deux réseaux distants. Il permet de chiffrer les communications afin de garantir la confidentialité des données échangées entre les différents sites.

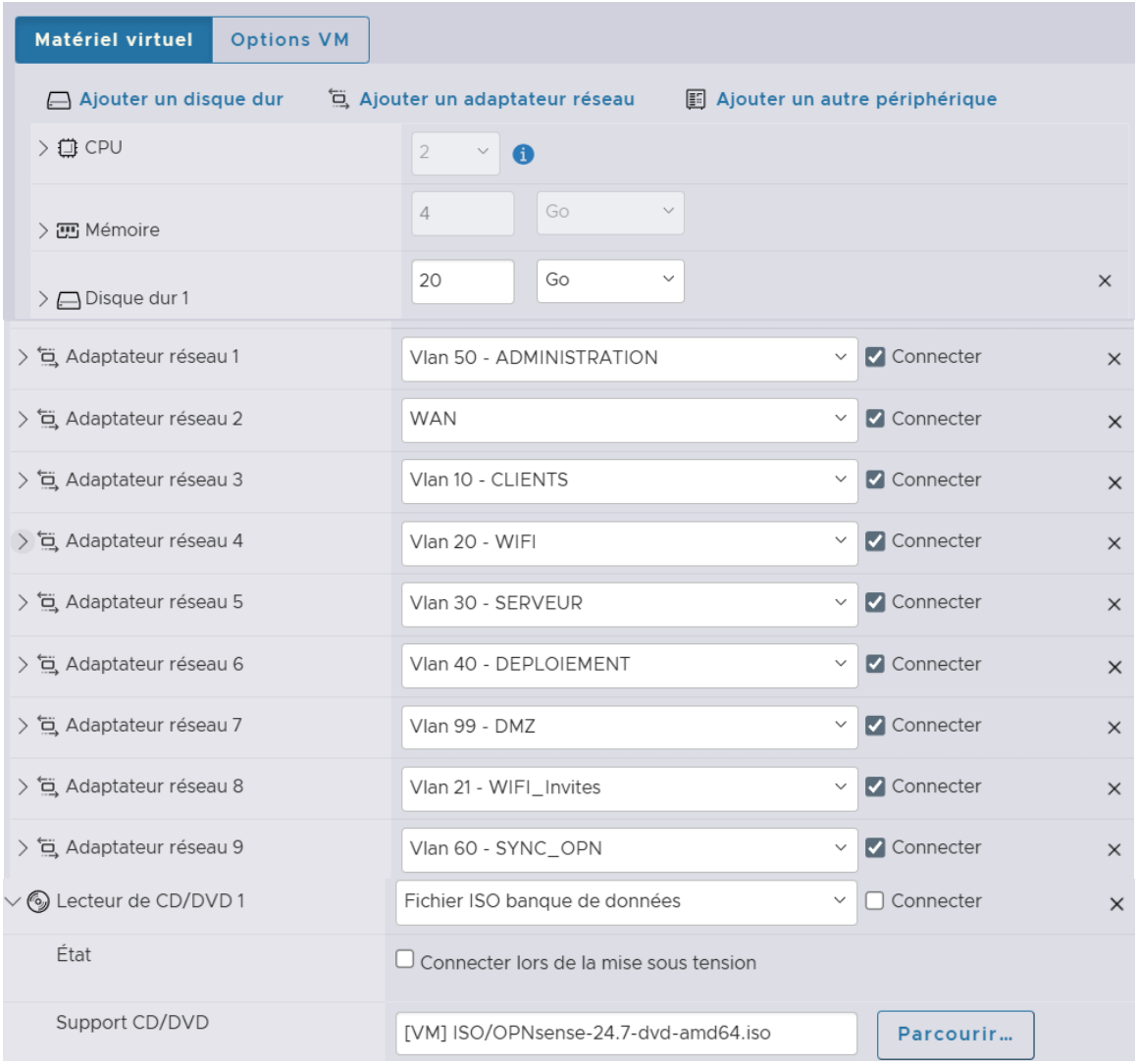
i) Liste du matériel à disposition

- 2 Hyperviseurs VMWare
- 2 Switch
- Câbles Réseaux
- Câbles d'alimentations

j) Installation et configuration OPNsense

1) Installation machine virtuelle

Pour l'installation du pare-feu OPNsense, j'ai pu créer une machine virtuelle sur notre ESXI01, j'ai pu mettre 40 Go de stockage pour cette machine, 4 Go de RAM et plusieurs cartes réseaux afin d'accueillir les différents réseaux que nous avons au sein de notre infrastructure comme nous pouvons le voir ci-dessous. J'ai également pu ajouter l'ISO correspondant à OPNsense.



Au total, il y a 9 cartes réseaux, cela fait une carte réseau pour chaque VLAN car le pare-feu fait aussi office de routeur. Voici les différents VLANs utilisés au sein de l'infrastructure.

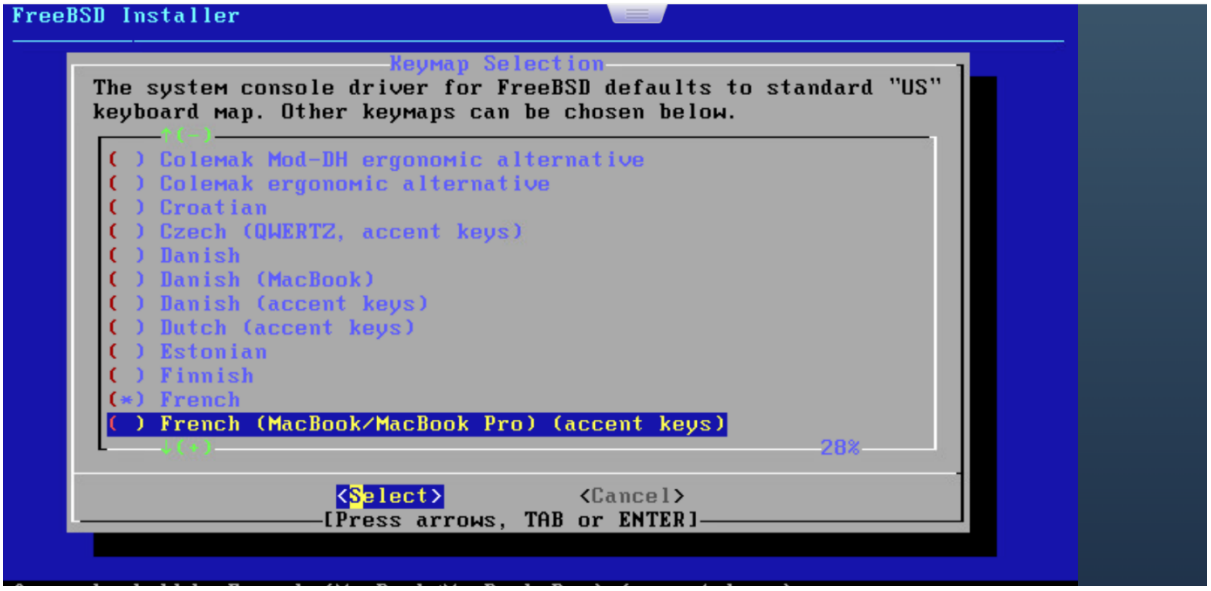
VLAN	Nom	Utilité
VLAN 10	CLIENTS	Accès réseau des postes clients
VLAN 20	WIFI	Accès réseau sans fil
VLAN 21	WIFI_INVITES	Accès réseau sans fil pour visiteurs
VLAN 30	SERVEUR	Hébergement des serveurs internes
VLAN 40	DEPLOIEMENT	Déploiement et configuration de nouveaux clients
VLAN 50	ADMINISTRATION	Administration des différents équipements
VLAN 60	SYNC_OPN	Synchronisation pares-feux OPNsense
VLAN 99	DMZ	Zone pour services exposés sur internet
WAN	WAN	Accès à internet

Une fois les différents paramètres configurés, j'ai pu lancer la machine virtuelle.

Au lancement de la machine virtuelle, j'ai pu atterrir sur la page ci-dessous, sur celle-ci il faut laisser le processus se dérouler et laisser la machine démarrer.

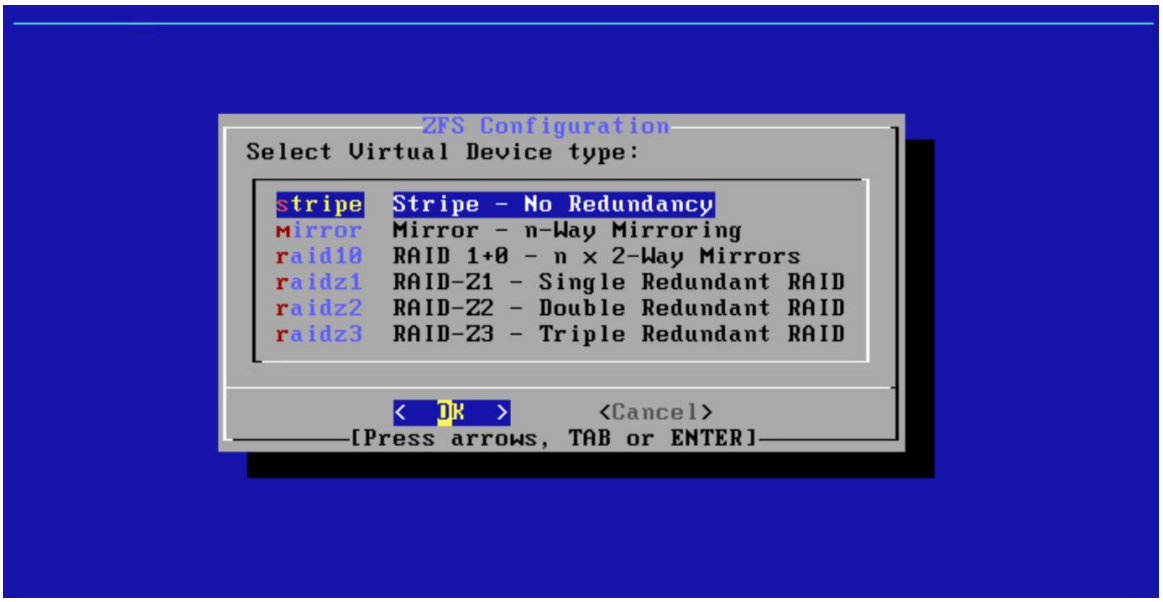
Ensuite, la page de login ci-dessous s'affiche, sur celle-ci il faut rentrer le login « installer » et le mot de passe « OPNsense », afin de vraiment installer le système sur le disque, pour rentrer les identifiants, le clavier est en QWERTY.

Après, une nouvelle page s'affiche, celle pour le langage du clavier, sur celle-ci, il faut choisir « French » puis valider deux fois afin d'avoir un clavier en AZERTY.



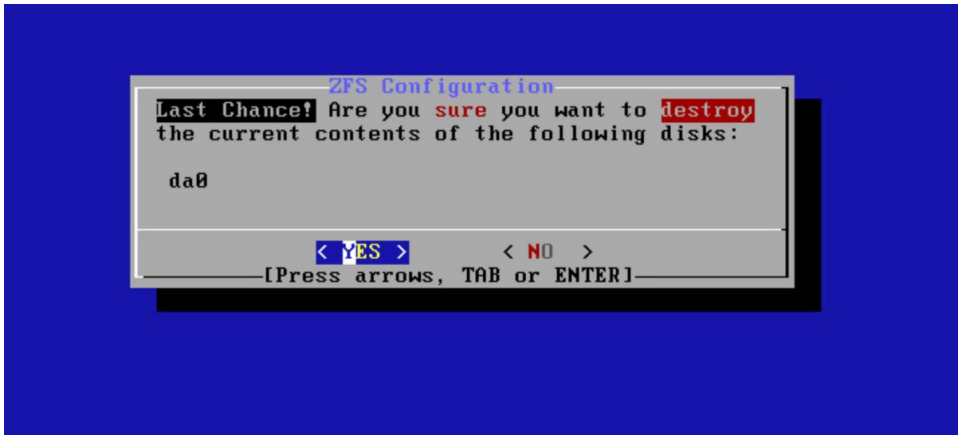
Une fois cela fait, il faut choisir la tâche à réaliser, ici, c'est une installation, c'est pour cela qu'il faut cliquer sur le paramètre correspondant à l'installation ZFS « Install (ZFS) », c'est le paramètre recommandé pour une installation basique.

Après, la page ci-dessous s'affichera, comme la machine est équipée d'un seul disque, il faut aller sur « stripe » puis faire « OK » car nous n'avons pas de redondance au niveau disque et c'est une machine virtuelle.

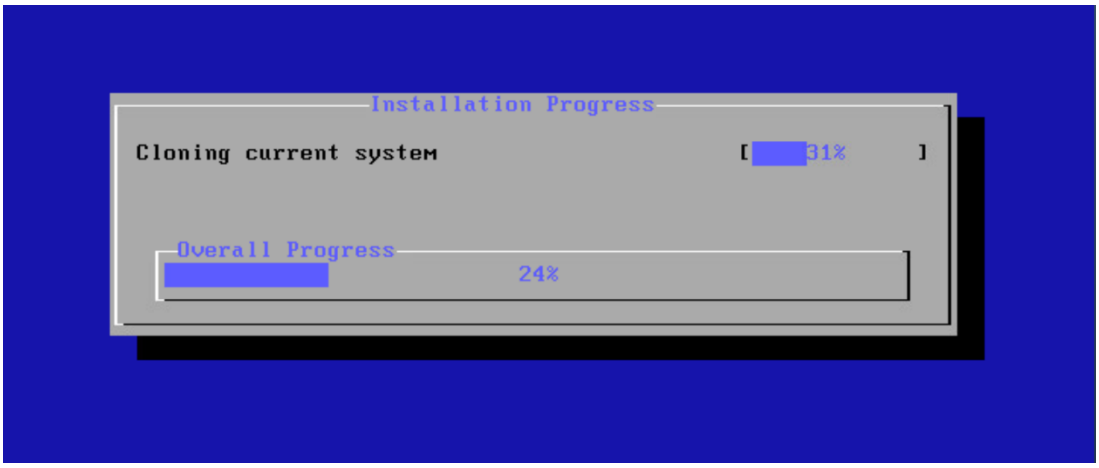


Après avoir fait cette configuration, le système nous demande quel disque choisir, nous en avons seulement un seul alors pour le choisir, il faut appuyer sur la touche « Espace » pour que l'étoile s'affiche puis sur « Entrée ».

Pour l'étape suivante, il faut aller sur « YES », c'est une machine virtuelle, elle vient d'être créée, le disque est vierge, il n'y a donc pas de données, c'est pour cela que tout peut être effacé.



Une fois cette configuration réalisée, la page ci-dessous s'affiche, il faut attendre que celle-ci se charge afin de poursuivre l'installation.



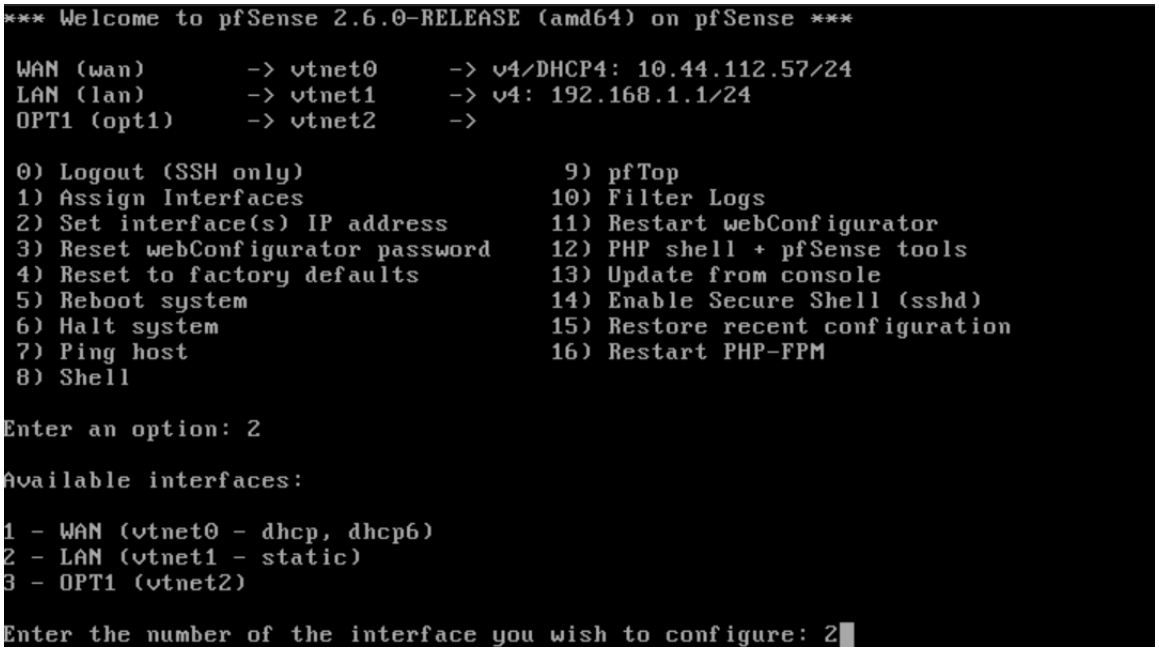
Ensuite, il est possible de changer le mot de passe ROOT ou de redémarrer pour terminer l'installation. Il est nécessaire de changer le mot de passe ROOT pour des raisons de sécurité, puis il faut aller sur « Complete Install » afin de finaliser l'installation.

Après avoir réalisé les différentes étapes ci-dessus, cette page devrait s'afficher, dans ce cas, l'installation est terminée. Il faut ensuite passer à la configuration de base du pare-feu.

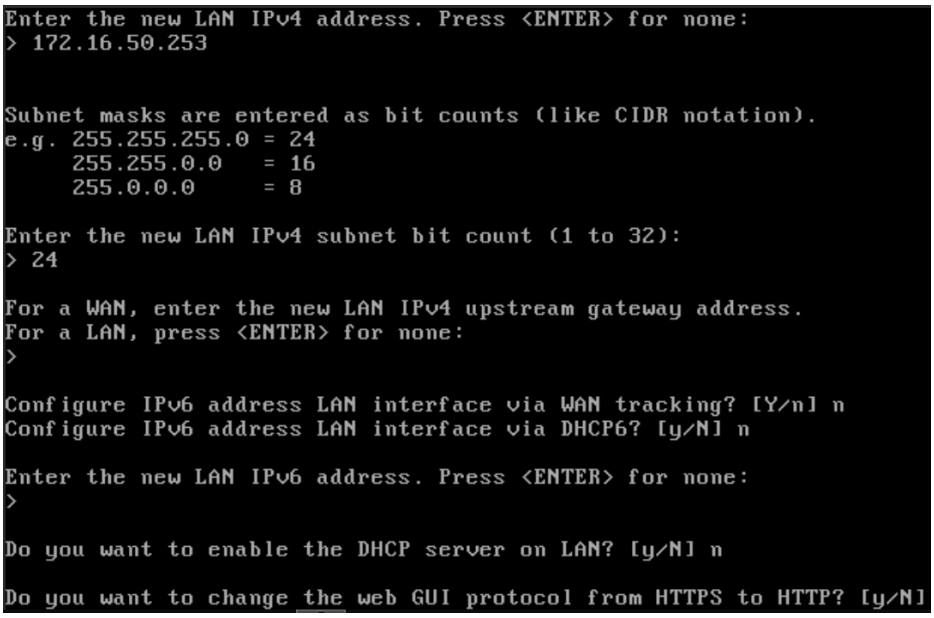
2) Configuration de base Pare-feu

Pour la configuration de base du pare-feu, il faut commencer par configurer les accès afin de pouvoir aller sur l'interface web. Il est également possible de faire cette configuration en ligne de commande pour chaque mais cela est moins pratique.

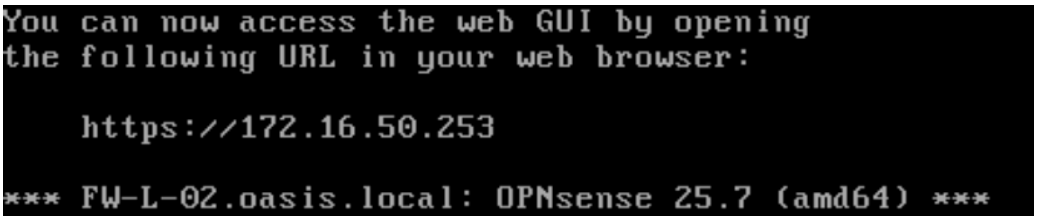
Afin de pouvoir se connecter, il faut configurer l'IP du LAN. Il faut la configurer en IP statique. Pour cela, il faut taper « 2 » pour « Set interface(s) IP address », ensuite il faut choisir la carte LAN à configurer, ici, la carte n°2.



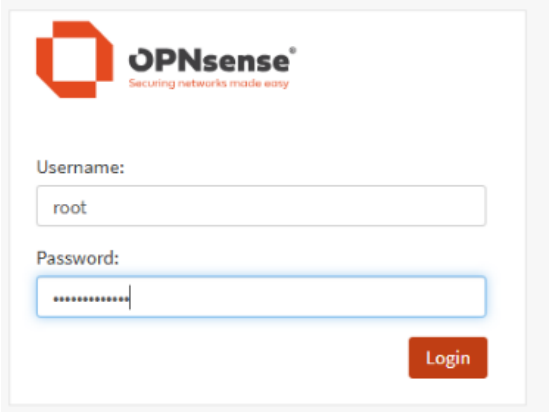
Après, il faut saisir l'IP du LAN de l'OPNsense, dans ce cas 172.16.50.253, ainsi que le masque CIDR du LAN, /24. Il faut ensuite appuyer une fois sur « Entrée » afin de passer la configuration de la partie WAN puis répondre à non aux configurations IPv6 car uniquement l'IPv4 est utilisé ici. Enfin, il faut taper « n » afin de ne pas activer le DHCP sur le Firewall pour le LAN.



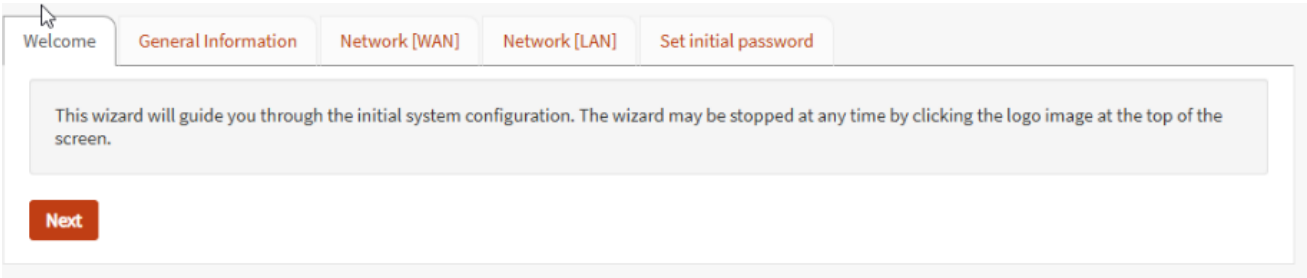
Après avoir réalisé ces configurations, la page ci-dessous avec l'IP, cela indique qu'il est maintenant possible d'accéder à l'interface Web depuis l'IP configuré, https://172.16.50.253/.

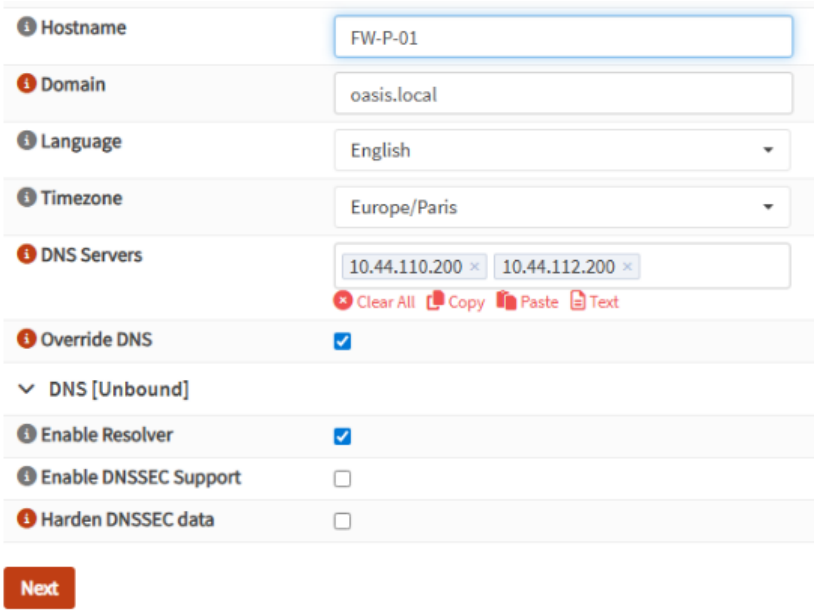


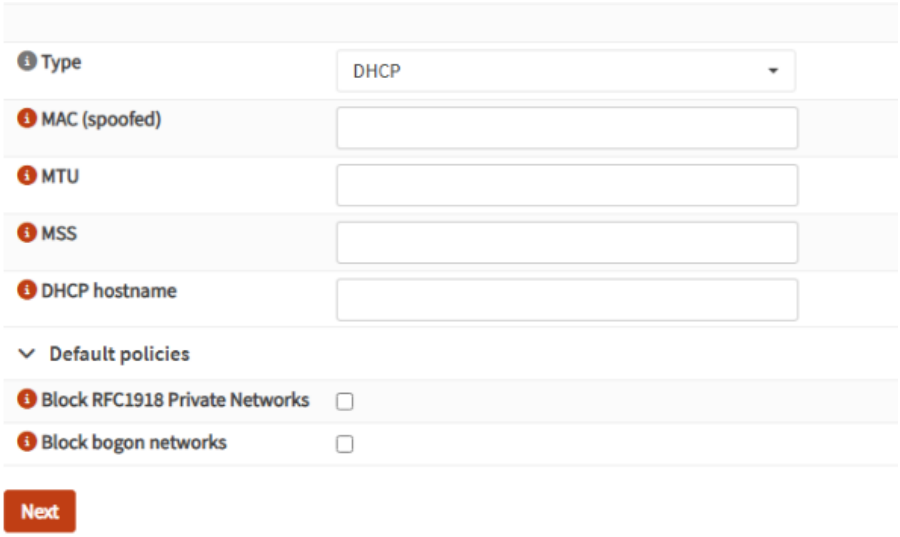
En testant avec une machine Windows qui est sur le même LAN que le Firewall OPNsense, il est possible d'accéder à l'interface web depuis l'IP 172.16.50.253, les identifiants par défaut sont « root » pour le nom d'utilisateur et « OPNsense » pour le mot de passe.



La page d'accueil de l'OPNsense devrait s'afficher après la connexion. Pour la configuration de base, il faut aller dans « System », « Configuration » puis « Wizard » dans les paramètres Wizard, il faut configurer le nom du pare-feu, les serveurs DNS auxquels il peut avoir accès et enlever le blocage du WAN sur un réseau privé. Comme il n'y a pas de réel WAN, ci-dessous la configuration réalisée sur le premier pare-feu du site de Paris.







Une fois les différentes étapes de l'assistant de configuration réalisées, la configuration de base du pare-feu est terminée. Il faut ensuite faire la configuration des interfaces.

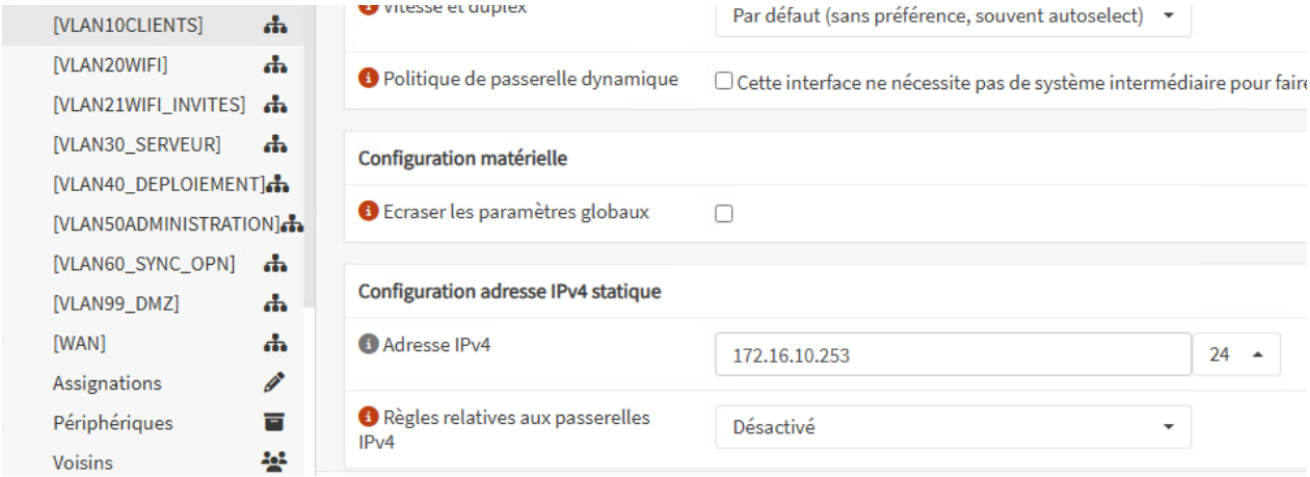
3) Configuration des interfaces

Après avoir réalisé la configuration de base, il faut paramétrer les différentes interfaces pour les différents VLAN.

Tout d'abord il faut assigner les interfaces, pour cela, il faut se rendre dans « Interfaces » puis « Assignations » et assigner chaque interface en fonction des cartes réseau qui ont été configurées sur l'ESXi lors de la création de la machine virtuelle. Ci-dessous les différentes cartes réseau assignées.

Interface	Identifiant	Dispositif
[VLAN10CLIENTS]	opt1	em2 (00:0c:29:d2:62:eb)
[VLAN20WIFI]	opt2	em3 (00:0c:29:d2:62:f5)
[VLAN21WIFI_INVITES]	opt6	em7 (00:0c:29:d2:62:1d)
[VLAN30_SERVEUR]	opt3	em4 (00:0c:29:d2:62:ff)
[VLAN40_DEPLOIEMENT]	opt4	em5 (00:0c:29:d2:62:09)
[VLAN50ADMINISTRATION]	lan	em0 (00:0c:29:d2:62:d7)
[VLAN60_SYNC_OPN]	opt8	em8 (00:0c:29:d2:62:27)
[VLAN99_DMZ]	opt5	em6 (00:0c:29:d2:62:13)
[WAN]	opt7	em1 (00:0c:29:d2:62:e1)

Une fois les cartes assignées, dans « Interfaces », les différentes interfaces devraient s'afficher comme ci-dessous. Il faut paramétrer une IP sur chacune des interfaces en cliquant sur l'interface souhaitée, puis en définissant une IP statique. Ces IP seront les passerelles de chaque réseau (voir plan d'adressage), comme sur la deuxième image ci-dessous.

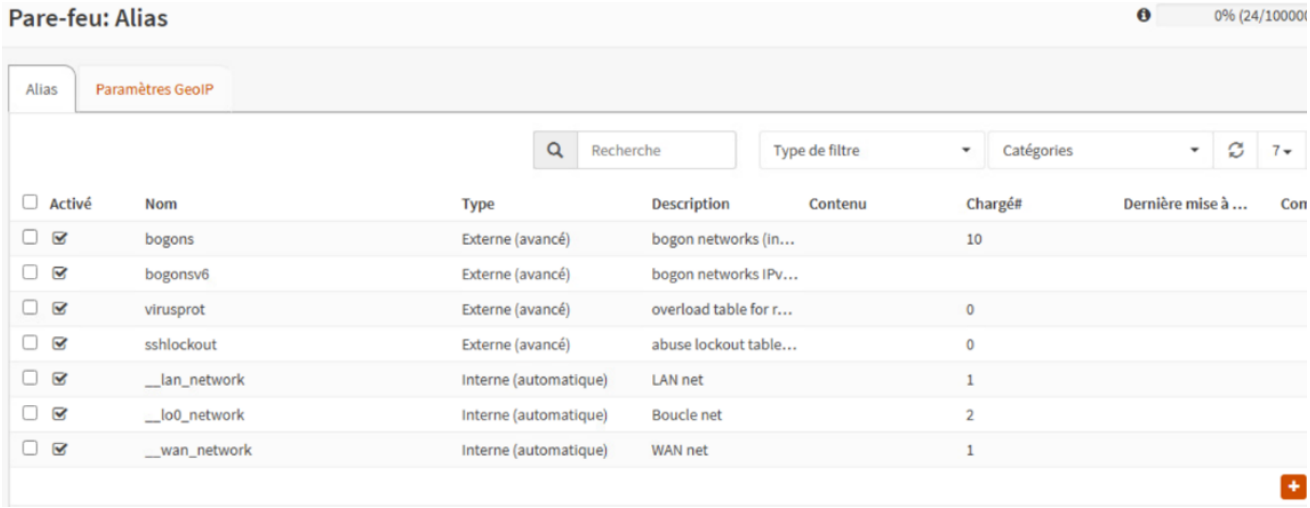


Après avoir effectué cela, le routage entre les réseaux devrait se faire automatiquement mais il n'est pas possible d'effectuer des communications entre les différents réseaux, car par défaut, tout le trafic est bloqué par les règles du pare-feu. C'est pour cela qu'il faut configurer des règles de pare-feu.

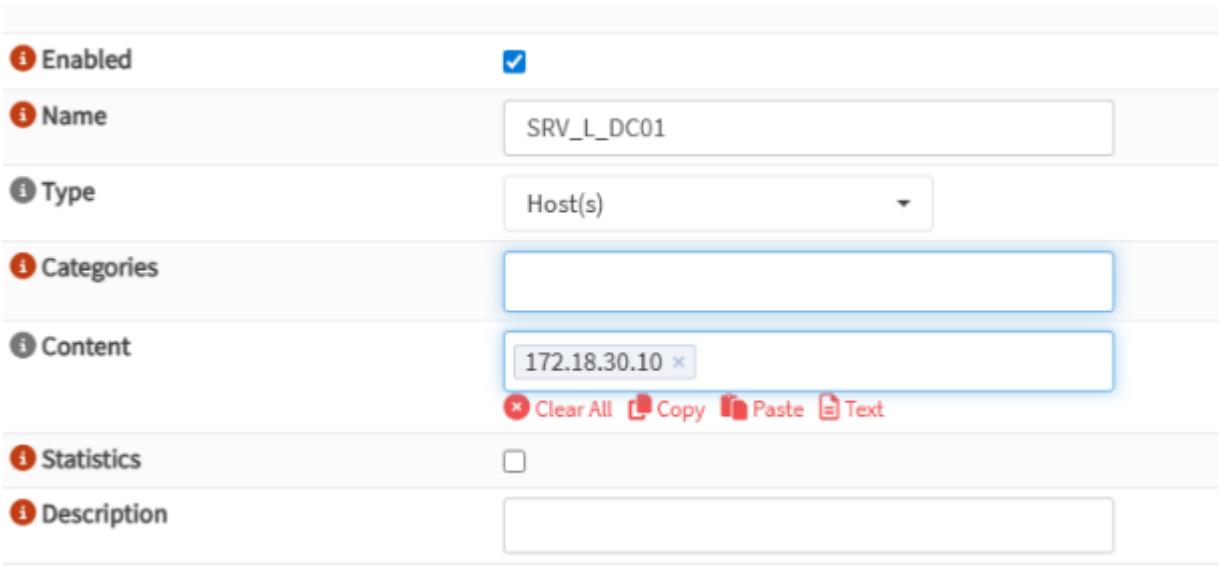
4) Règles de Firewall

Les règles de pare-feu sont utilisées pour définir le trafic autorisé ou non. Pour configurer ces règles, il faut mettre en place des alias afin de simplifier la configuration. Cela permet de remplacer les adresses IP et donc d'avoir directement des noms.

Pour cette configuration, il faut aller dans « Firewall » puis « Aliases ».



Sur cette, il est possible d'ajouter des alias que ce soit pour des réseaux, des hôtes ou encore des ports (groupe de ports), il suffit de remplir le champ « Content » avec les ports voulus ou l'adresse IP ou les réseaux voulus en fonction de la configuration comme ci-dessous pour une adresse IP.



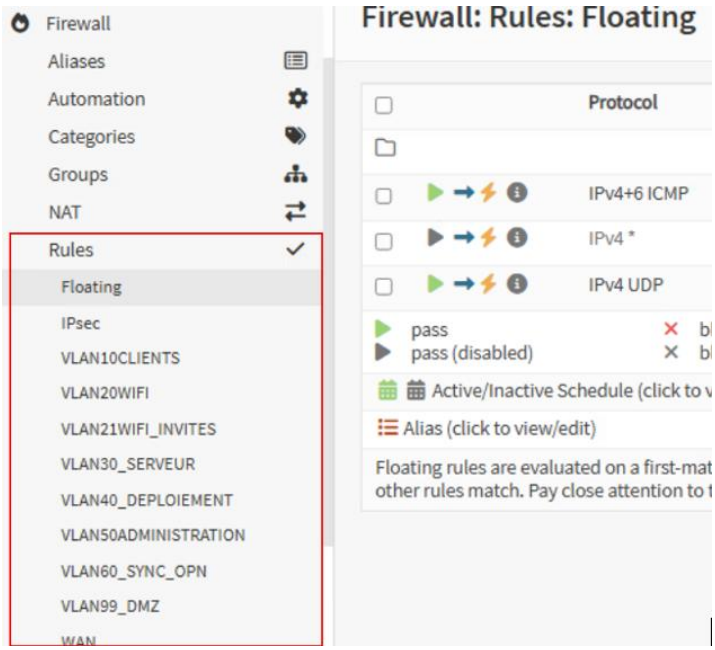
Voici tous les alias que configurés pour l'ensemble de l'infrastructure construite pour Oasis.

Il y a un alias pour chacun de des serveurs, pour différents groupes de ports utilisés par différents services et pour différents réseaux qui constituent l'infrastructure.

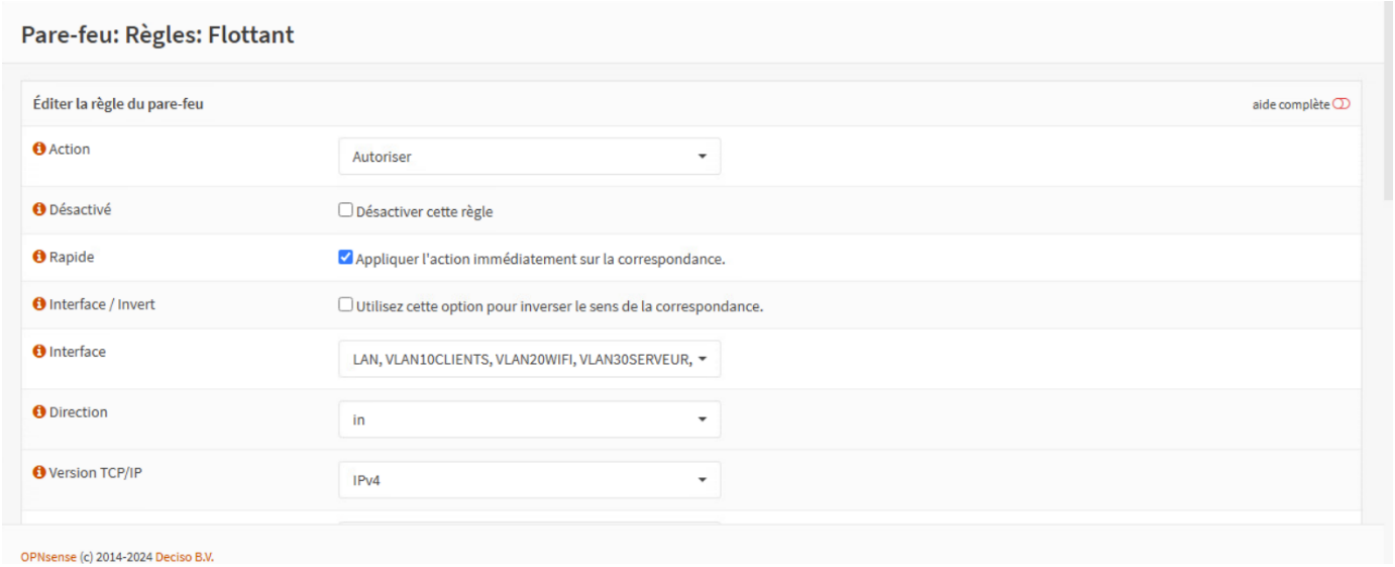
Activé	Nom	Type	Descript…	Contenu
☑	AP_NTxSystem	Hôte(s)		172.16.20.50
☑	DNS_Salle	Hôte(s)		10.44.112.200 10.44.110.200
☑	FW_M_01	Hôte(s)		172.17.10.254
☑	FW_P_01_ADMIN	Hôte(s)		172.16.50.253
☑	FW_P_01_SYNC	Hôte(s)		172.16.60.1
☑	FW_P_02_ADMIN	Hôte(s)		172.16.50.252
☑	FW_P_02_SYNC	Hôte(s)		172.16.60.2
☑	FW_P_ADMIN	Hôte(s)		Passerelle_VLAN50_ADMIN FW_…
☑	FW_P_SYNC	Hôte(s)		FW_P_02_SYNC FW_P_01_SYNC
☑	NAS_BCK	Hôte(s)		10.44.110.212
☑	Passerelle_VLAN2O_WIFI	Hôte(s)		172.16.20.254
☑	Passerelle_VLAN10_CLIENTS	Hôte(s)		172.16.10.254
☑	Passerelle_VLAN30_SERVEUR	Hôte(s)		172.16.30.254
☑	Passerelle_VLAN40_DEPLOIEMENT	Hôte(s)		172.16.40.254
☑	Passerelle_VLAN50_ADMIN	Hôte(s)		172.16.50.254
☑	Passerelle_WAN	Hôte(s)		10.44.150.254
☑	proxmox1_btssio_nte	Hôte(s)		10.44.112.241
☑	P_CENTREON	Port(s)	Ports po…	5669 5556 3306 5670
☑	P_DHCP	Port(s)	Ports DH…	67 68
☑	P_FOG	Port(s)		69 111 1024:65535
☑	P_IPSEC_CLIENTS	Port(s)		P_WEB P_WAZUH
☑	P_IPSEC_SRV	Port(s)		22 53 88 123 135 161 162 389 44…
☑	P_Partage_Reseau	Port(s)		88 389 135 445 49152:65535
☑	P_RADIUS	Port(s)		1812 1813
☑	P_SNMP	Port(s)	Ports SN…	161 162 5700
☑	P_VEEAM	Port(s)	Port pou…	22 135 443 445 902 6160 6162 61…
☑	P_WAZUH	Port(s)		1514 1515
☑	P_WEB	Port(s)		80 443
☑	Reseau_Grenoble_CLIENTS	Réseau(x)		172.20.10.0/24
☑	Reseau_Grenoble_SRV	Réseau(x)		172.20.30.0/24
☑	Reseau_Lille_CLIENTS	Réseau(x)		172.18.10.0/24
☑	Reseau_Lille_SRV	Réseau(x)		172.18.30.0/24

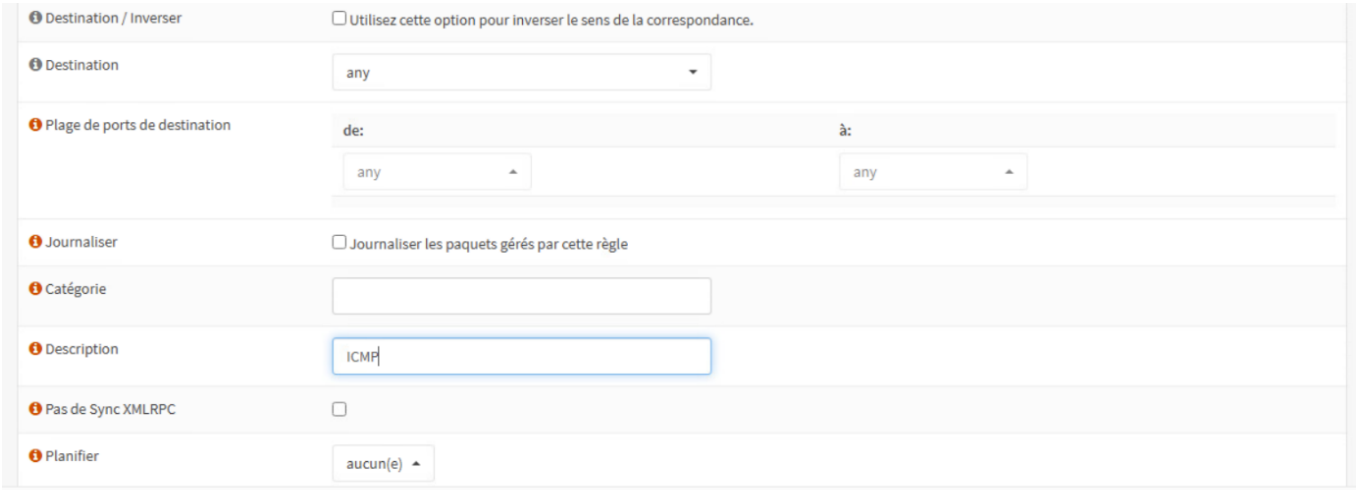
Reseau_Marseille	Réseau(x)		172.17.10.0/24
Reseau_Nantes_CLIENTS	Réseau(x)		172.19.10.0/24
Reseau_Nantes_SRV	Réseau(x)		172.19.30.0/24
Reseau_OASIS_CLIENTS	Hôte(s)		Reseau_Grenoble_CLIENTS Res...
Reseau_OASIS_SRV	Hôte(s)		Reseau_Lille_SRV Reseau_Nant...
Reseau_WAN	Réseau(x)		10.44.110.0/24 10.44.115.0/24 1...
SRV_P	Hôte(s)		SRV_P_DC01 SRV_P_DC02
SRV_P_ANS01	Hôte(s)		172.16.30.21
SRV_P_BCK01	Hôte(s)	Serveur ...	172.16.30.15
SRV_P_CLOUD01	Hôte(s)		172.16.30.16
SRV_P_DC01	Hôte(s)		172.16.30.10
SRV_P_DC02	Hôte(s)		172.16.30.20
SRV_P_DFS01	Hôte(s)		172.16.30.50
SRV_P_EDR01	Hôte(s)		172.16.30.19
SRV_P_ESXI01_WAN	Hôte(s)		10.44.150.1
SRV_P_ESXI02	Hôte(s)		10.44.150.3
SRV_P_FOG01	Hôte(s)	IP FOG	172.16.30.11
SRV_P_GLPI01	Hôte(s)		172.16.30.14
SRV_P_HAProxy	Hôte(s)		172.16.99.10
SRV_P_POL01	Hôte(s)		172.16.30.25
SRV_P_SUP01	Hôte(s)		172.16.30.12
SW_P_01	Hôte(s)		172.16.50.1

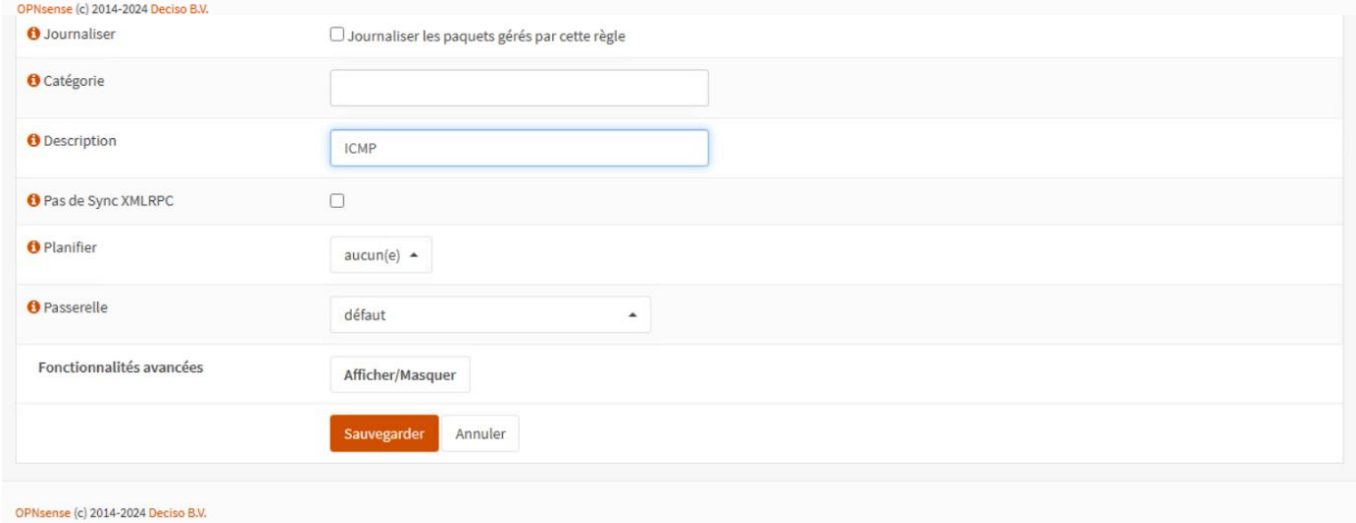
Ensuite, pour la partie filtrage, il existe deux types de règles configurables : les règles « Flottantes », qui s'appliquent à l'ensemble des réseaux, et les règles par VLAN (par réseau), qui s'appliquent uniquement à l'interface sur laquelle la règle est configurée. Ces règles peuvent être configurées dans « Firewall » puis « Rules ».



Ci-dessous, un exemple de configuration d'une règle flottante pour l'ICMP afin de permettre les tests de communication entre les différents réseaux. Dans cette règle, les réseaux concernés sont définis dans la partie « Interface ». La source doit rester sur « any », car elle n'est pas connue. La destination est définie avec le protocole ICMP, et la direction doit être configurée sur « in ».







Ci-dessous, les différentes règles de pare-feu qui ont été configurées pour chacune des interfaces de l'infrastructure.

Firewall: Rules: VLAN10CLIENTS

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 TCP/UDP	*	*	SRV_P	53 (DNS)	*	*	DNS Client vers SRV
	IPv4 TCP	VLAN10CLIENTS net	*	*	P_WEB	*	*	Ports WEB
	IPv4 TCP/UDP	VLAN10CLIENTS net	*	VLAN30_SERVEUR net	P_Partage_Reseau	*	*	Ports Partage Réseau
	IPv4 TCP	VLAN10CLIENTS net	*	Passerelle_VLAN50_ADMIN	10443	*	*	Accès FW Depuis VLAN 10
	IPv4 TCP/UDP	VLAN10CLIENTS net	*	SRV_P_EDR01	P_WAZUH	*	*	

Firewall: Rules: VLAN20WIFI

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rul
								Floating rules
	IPv4 TCP/UDP	VLAN20WIFI net	*	SRV_P_EDR01	P_WAZUH	*	*	
	IPv4 TCP/UDP	VLAN20WIFI net	*	VLAN30_SERVEUR net	P_Partage_Reseau	*	*	Ports Partage Réseau
	IPv4 TCP	VLAN20WIFI net	*	*	P_WEB	*	*	Ports WEB
	IPv4 TCP	VLAN20WIFI net	*	FW_P_ADMIN	10443	*	*	Accès FW Depuis VLAN 20
	IPv4 TCP/UDP	*	*	SRV_P	53 (DNS)	*	*	DNS Client vers SRV
	IPv4 UDP	AP_NTxSystem	*	SRV_P	P_RADIUS	*	*	Ports RADIUS
	IPv4 TCP/UDP	VLAN20WIFI net	*	VLAN30_SERVEUR net	22 (SSH)	*	*	
	IPv4 TCP/UDP	VLAN20WIFI net	*	Reseau_Nantes_SRV, VLAN30_SERVEUR net	3389 (MS RDP)	*	*	RDP Serveur > Wifi
	IPv4 TCP/UDP	*	*	proxmox1_btssio_nte	8006	*	*	

Firewall: Rules: VLAN21WIFI_INVITES

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated ru
								Floating rules
	IPv4 TCP	VLAN21WIFI_INVITES net	*	*	P_WEB	*	*	Ports WEB
	IPv4 TCP/UDP	*	*	SRV_P_DC01	53 (DNS)	*	*	DNS Client vers SRV
	IPv4 TCP	VLAN21WIFI_INVITES net	*	*	8000 - 8003	*	*	Accepter Portail Captif

Firewall: Rules: VLAN30_SERVEUR

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 TCP/UDP	SRV_P	*	DNS_Salle	53 (DNS)	*	*	DNS Interne vers Salle
	IPv4 TCP	VLAN30_SERVEUR net	*	*	P_WEB	*	*	
	IPv4 TCP/UDP	SRV_P_FOG01	*	VLAN40_DEPLOIEMENT net	P_FOG	*	*	Ouverture Ports FOG Déploiement
	IPv4 TCP/UDP	SRV_P_POL01	*	FW_M_01, VLAN50ADMINISTRATION net, VLAN20WIFI net, VLAN99_DMZ net	P_SNMP	*	*	Ouverture Ports pour la Supervision
	IPv4 UDP	SRV_P	*	AP_NTxSystem	P_RADIUS	*	*	
	IPv4 TCP/UDP	SRV_P_BCK01	*	SRV_P_ESXI01_WAN, SRV_P_ESXI02	P_VEEAM	*	*	Serveur Veeam vers ESXI
	IPv4 TCP/UDP	VLAN30_SERVEUR net	*	Reseau_Marseille, Reseau_Lille_SRV, Reseau_Nantes_SRV, Reseau_Grenoble_SRV	P_IPSEC_SRV	*	*	
	IPv4 *	SRV_P_BCK01	*	NAS_BCK	*	*	*	
	IPv4 TCP/UDP	SRV_P_ANS01	*	*	22 (SSH)	*	*	

Firewall: Rules: VLAN40_DEPLOIEMENT

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 TCP/UDP	VLAN40_DEPLOIEMENT net	*	SRV_P	53 (DNS)	*	*	DNS Client vers SRV
	IPv4 TCP/UDP	VLAN40_DEPLOIEMENT net	*	SRV_P_FOG01	P_FOG	*	*	
	IPv4 TCP	VLAN40_DEPLOIEMENT net	*	*	P_WEB	*	*	

Firewall: Rules: VLAN50ADMINISTRATION

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 TCP/UDP	VLAN50ADMINISTRATION net	*	SRV_P	53 (DNS)	*	*	DNS Client vers ADMIN
	IPv4 TCP	VLAN50ADMINISTRATION net	*	*	P_WEB	*	*	Ouverture Ports Web

Firewall: Rules: VLAN60_SYNC_OPN

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 CARP	FW_P_SYNC	*	FW_P_SYNC	*	*	*	
	IPv4 PFSYNC	FW_P_SYNC	*	FW_P_SYNC	*	*	*	
	IPv4 TCP	FW_P_SYNC	*	FW_P_SYNC	*	*	*	

Firewall: Rules: VLAN99_DMZ

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
	IPv4 TCP/UDP	VLAN99_DMZ net	*	SRV_P_EDR01	P_WAZUH	*	*	
	IPv4 TCP	SRV_P_ANS01	*	*	22 (SSH)	*	*	
	IPv4 TCP	VLAN99_DMZ net	*	*	P_WEB	*	*	Ports WEB
	IPv4 TCP/UDP	*	*	SRV_P	53 (DNS)	*	*	DNS Client vers SRV
	IPv4 *	DNS_Salle	*	SRV_P_HAProxy	*	*	*	
	IPv4 TCP	SRV_P_HAProxy	P_WEB	SRV_P_GLPI01	P_WEB	*	*	Pour HAProxy > GLPI
	IPv4 TCP	SRV_P_HAProxy	P_WEB	SRV_P_CLOUD01	P_WEB	*	*	Pour HAProxy > NEXTCLOUD

Firewall: Rules: WAN

Select category

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
								Floating rules
								Automatically generated rules (end of ruleset)
	IPv4 TCP/UDP	*	*	SRV_P_HAProxy	80 - 443	*	*	Redirection WAN - HAProxy

Avec ces différentes règles, il est possible de filtrer au maximum et de limiter les ouvertures en filtrant par port, par machine ou par réseau en fonction des besoins de chaque service.

5) NAT

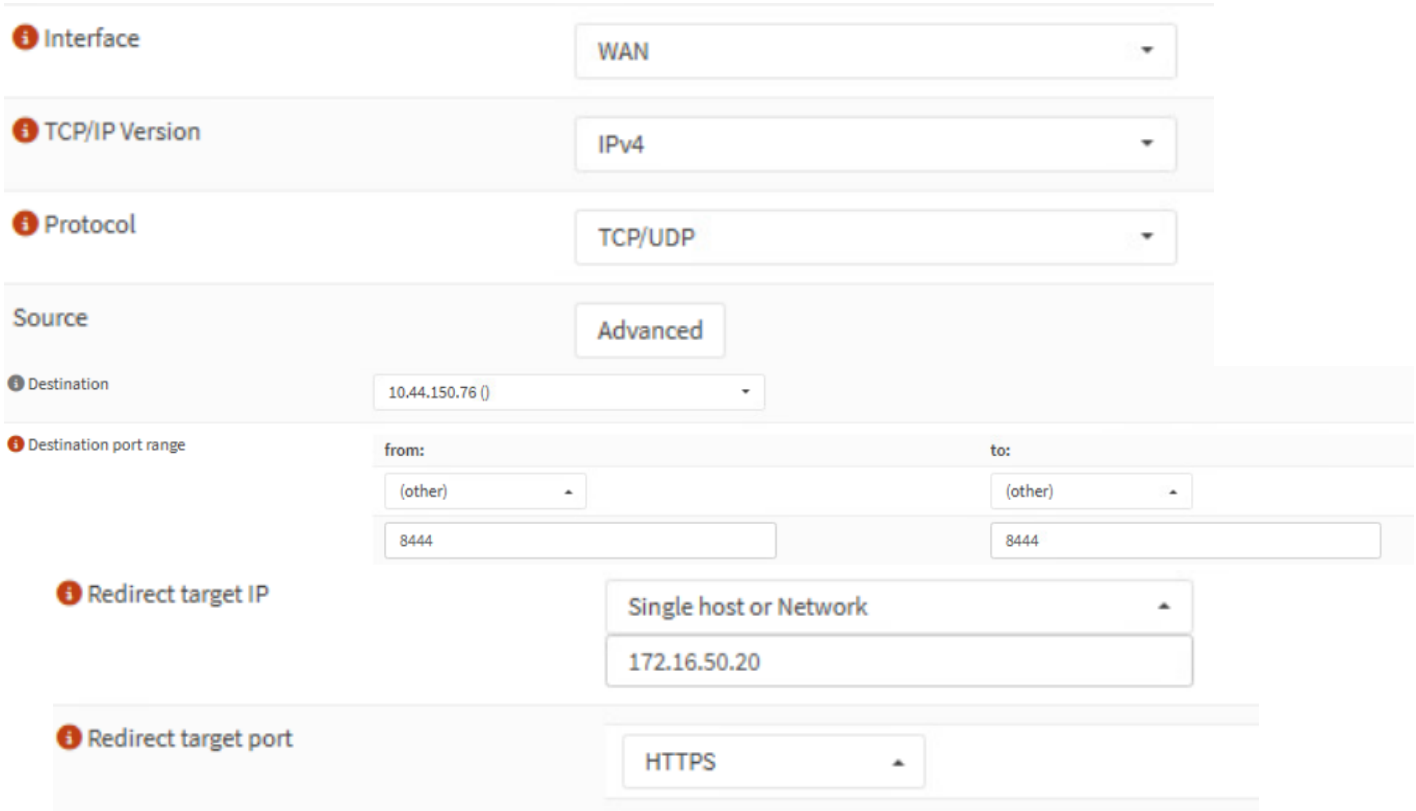
Le NAT (Network Address Translation) est une fonctionnalité permettant de faire de la redirection de port. Une configuration NAT a été faite afin de pouvoir se connecter sur certains outils depuis le WAN en tapant l'IP du pare-feu sur un port spécifique. Ci-dessous, les différentes règles NAT réalisées sur l'infrastructure.

Firewall: NAT: Port Forward

Select category

			Source		Destination		NAT		
	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
!	VLAN50ADMINISTRATION	TCP	*	*	VLAN50ADMINISTRATION address	10443	*	*	Anti-Lockout Rule
⇿	WAN	TCP/UDP	*	*	10.44.150.75/24	80 - 443	SRV_P_HAProxy	80 - 443	Redirection WAN - HAProxy
▶	WAN	TCP/UDP	*	*	10.44.150.76	8444	172.16.50.20	443 (HTTPS)	IP Local ESXI 2
▶	WAN	TCP/UDP	*	*	10.44.150.76	8443	172.16.50.10	443 (HTTPS)	IP Local ESXI 1

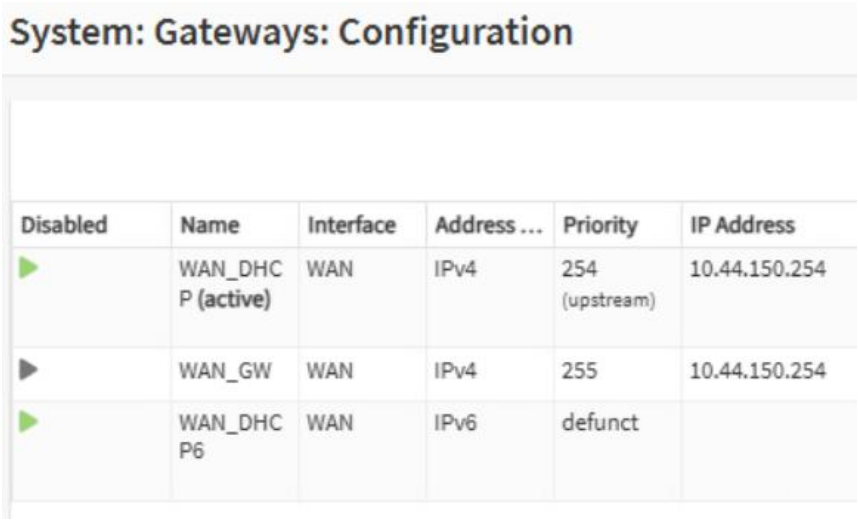
Cette configuration peut se faire sur OPNsense en allant dans « Firewall », « NAT » puis « Port Forward ». Pour faire une règle NAT correcte, il suffit de configurer l'interface concernée, l'IP avec laquelle on va communiquer qui va permettre de faire la redirection avec le port puis configurer l'IP de redirection avec le port de redirection. Ci-dessous la configuration réalisée pour une règle permettant de faire la translation vers l'IP locale du ESXi01.



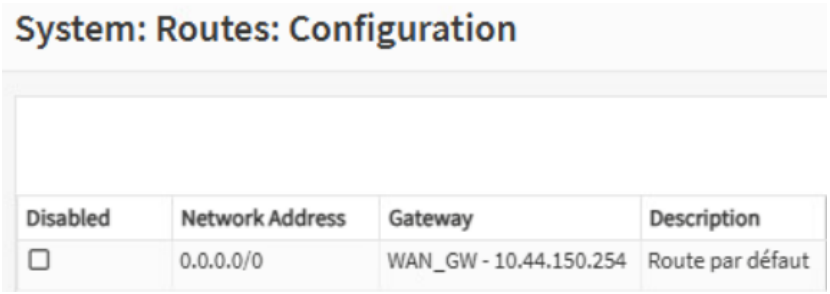
6) Accès à internet

Pour l'accès à internet, deux choses doivent être configurées en plus de ce qui a été réalisé lors de la configuration des interfaces.

Tout d'abord, dans « System », « Gateways » puis « Configuration », la WAN_GW ou la WAN_DHCP doit être activée avec la bonne passerelle côté WAN, comme ci-dessous avec la passerelle 10.44.150.254.



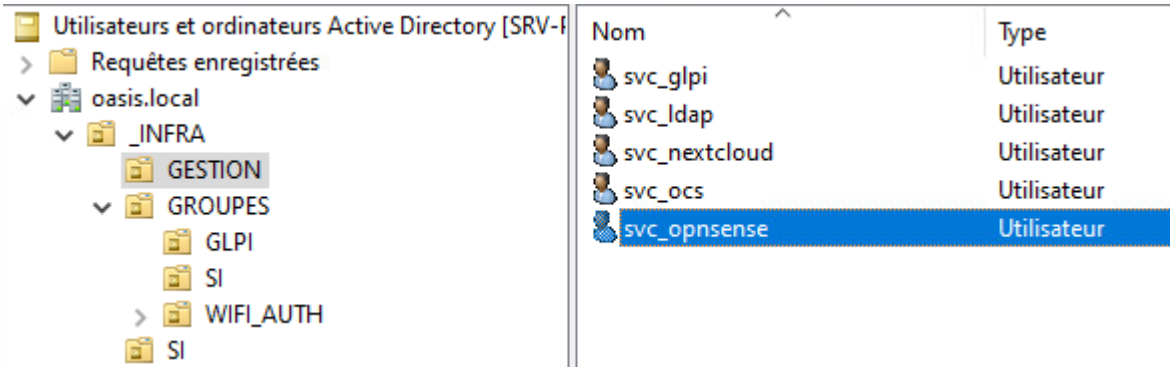
Ensuite, afin d'autoriser le trafic sortant vers internet et qu'il soit correctement dirigé, une route par défaut a été configurée avec l'adresse 0.0.0.0/0, associée à la passerelle 10.44.150.254. Cela peut être configuré dans « System », « Routes » puis « Configuration ».



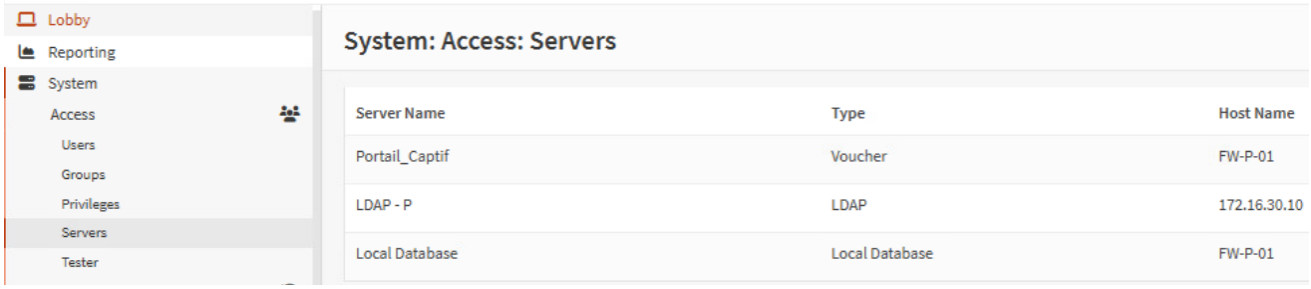
7) LDAP

Dans le but d'avoir une authentification centralisée sur l'OPNsense, celui-ci a été lié à l'Active Directory de l'infrastructure Oasis.

Pour activer le LDAP, il faut tout d'abord créer un utilisateur de service pour OPNsense sur l'Active Directory.



Puis, sur l'OPNsense, se rendre dans « System », « Acess » puis « Server » et cliquer sur le « + » pour ajouter un nouvel accès.



Dans la configuration, il faut rentrer les champs LDAP nécessaires :

Nom d'hôte ou adresse IP : L'adresse du serveur LDAP utilisé (Active Directory, OpenLDAP…)

Numéro de port :

389 pour LDAP standard (non chiffré)

636 pour LDAPS (chiffré SSL/TLS)

Transport :

TCP - Standard : connexion normale

TCP - STARTTLS : connexion non chiffrée puis upgrade vers SSL

SSL/TLS : chiffré dès le début

Version du protocole : Laisser sur 3 (version moderne de LDAP)

Identités de liaison :

> **DN de l'utilisateur :** Le compte utilisé par OPNsense pour se connecter au LDAP (ex: CN=svc_opnsense,OU=GESTION,OU=_INFRA,DC=oasis,DC=local)
>
> **Mot de passe :** Le mot de passe de ce compte

Étendue de la recherche :

"Un Niveau" : cherche uniquement dans l'OU spécifiée

"Sous-arbre entier" : cherche dans l'OU et tous ses sous-dossiers

DN de Base : Le point de départ de la recherche (ex: DC=oasis,DC=local)

Conteneurs d'authentification : Les OU où se trouvent les utilisateurs (ex: OU=SI,OU=_INFRA,DC=oasis,DC=local)

Requête Étendue : Filtre LDAP pour limiter les utilisateurs trouvés

&(memberOf=CN=GG_ADMIN,OU=SI,OU=GROUPS,...) = seuls les membres de ce groupe

Attribut de nom d'utilisateur :

sAMAccountName pour AD = vous tapez "AdminAF" pour vous connecter

uid pour OpenLDAP = idem

cn = vous tapez le nom complet

Gestion des groupes

Propriétés de lecture : Récupère les infos utilisateur (nom, email...)

Synchroniser les groupes : Importe les groupes LDAP dans OPNsense

Default groups : Groupe OPNsense attribué automatiquement aux nouveaux utilisateurs LDAP

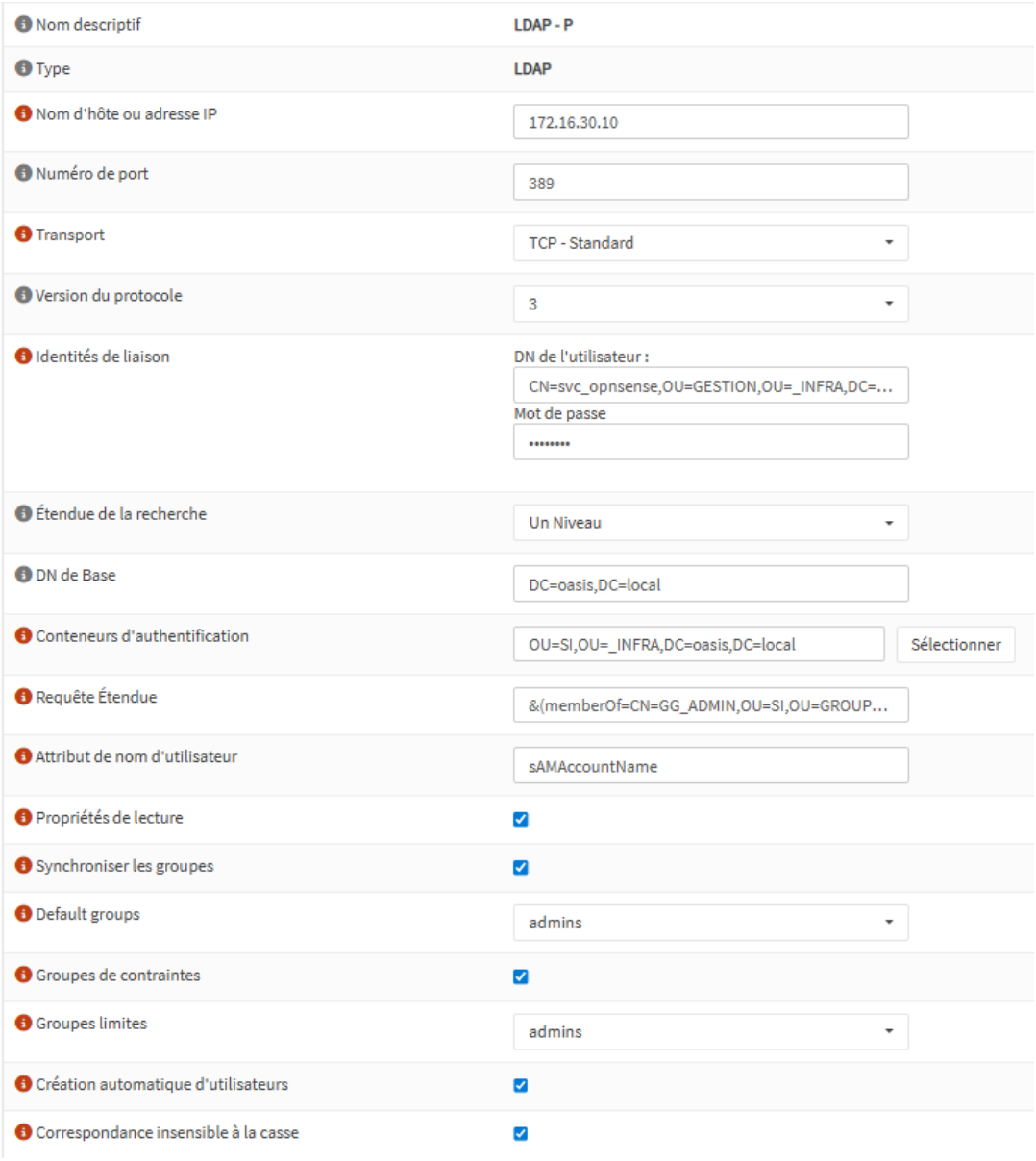
Groupes de contraintes : Active la restriction par groupe

Groupes limites : Seuls ces groupes LDAP peuvent se connecter

Création automatique d'utilisateurs : Crée automatiquement le compte local lors de la 1ère connexion

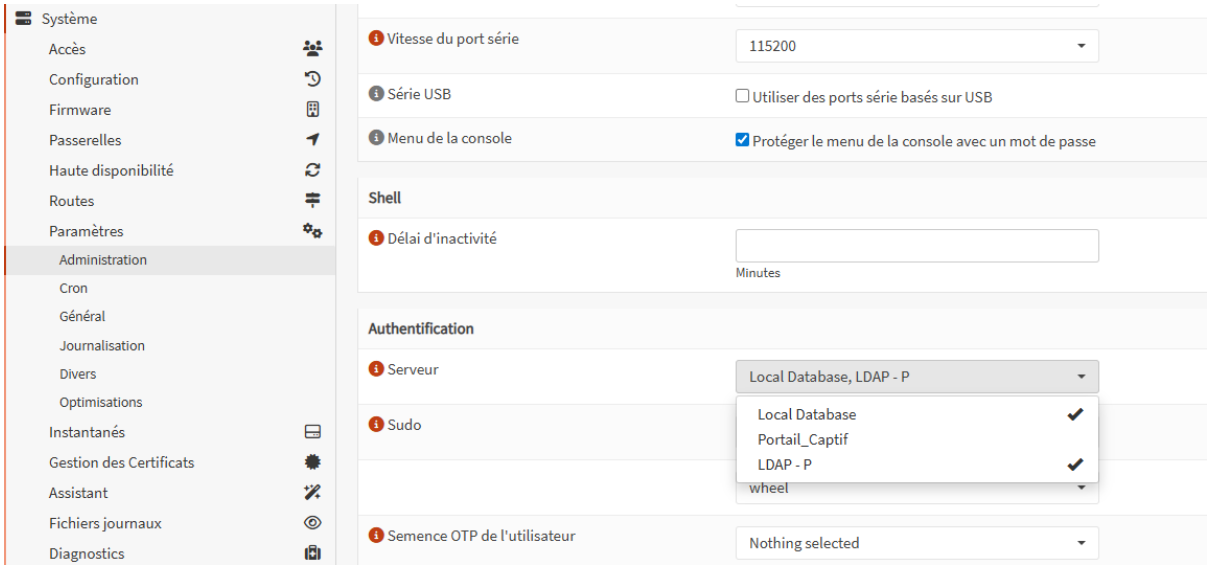
Correspondance insensible à la casse : "Admin" = "admin" = "ADMIN"

Ces différents paramètres donnent la configuration OPNsense pour le lien LDAP.



Pour terminer, il faut se rendre dans « System », « Settings » puis « Administration », ensuite dans « Authentication » et « Server », il faut choisir « Local Database » ainsi que la nouvelle liaison LDAP « LDAP-P ».

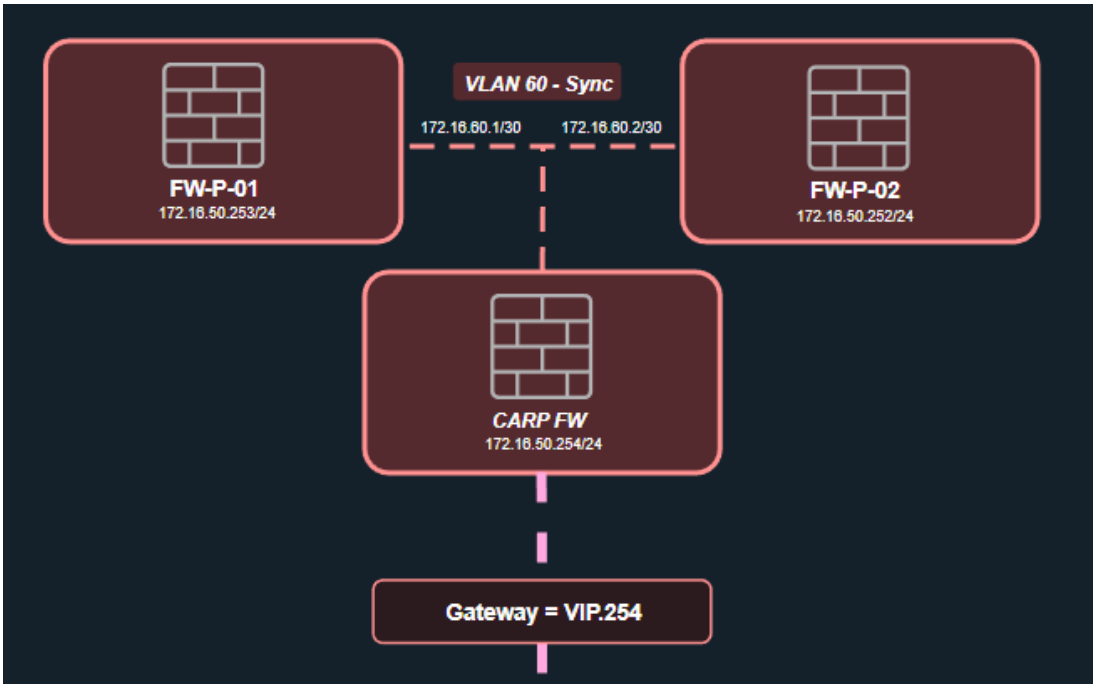
Cela permettra d'utiliser les deux pour l'authentification, la « Local Database » est gardée afin de ne pas avoir de soucis de connexions si l'authentification LDAP ne fonctionne plus.



8) Configuration Haute Disponibilité

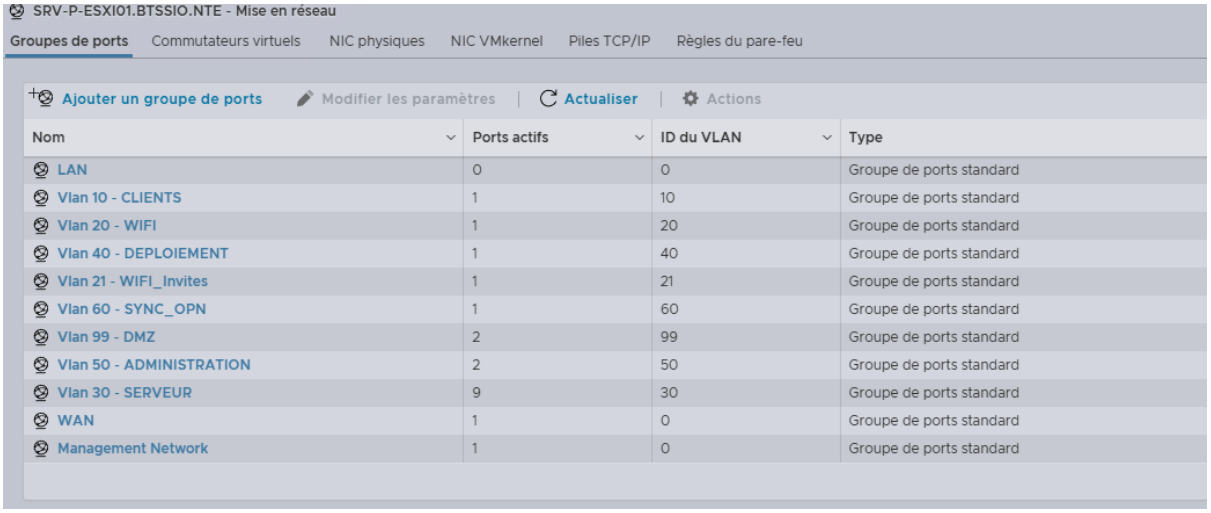
La haute disponibilité permet d'assurer une redondance matérielle. Il est possible de configurer deux pares-feux ou plus en groupe de basculement. Si une interface du pare-feu principal tombe en panne ou si ce dernier devient totalement hors service, le pare-feu secondaire prend le relais. Tout cela est possible avec le CARP (Common Address Redundancy Protocol).

Ci-dessous, il est possible de retrouver le fonctionnement de cette haute disponibilité, les clients vont tous se diriger sur la passerelle en .254 peu importe le VLAN. Cela va diriger par défaut les requêtes sur le FW-P-01 mais si celui-ci ne fonctionne pas alors toutes les requêtes iront le sur le firewall de backup, FW-P-02.

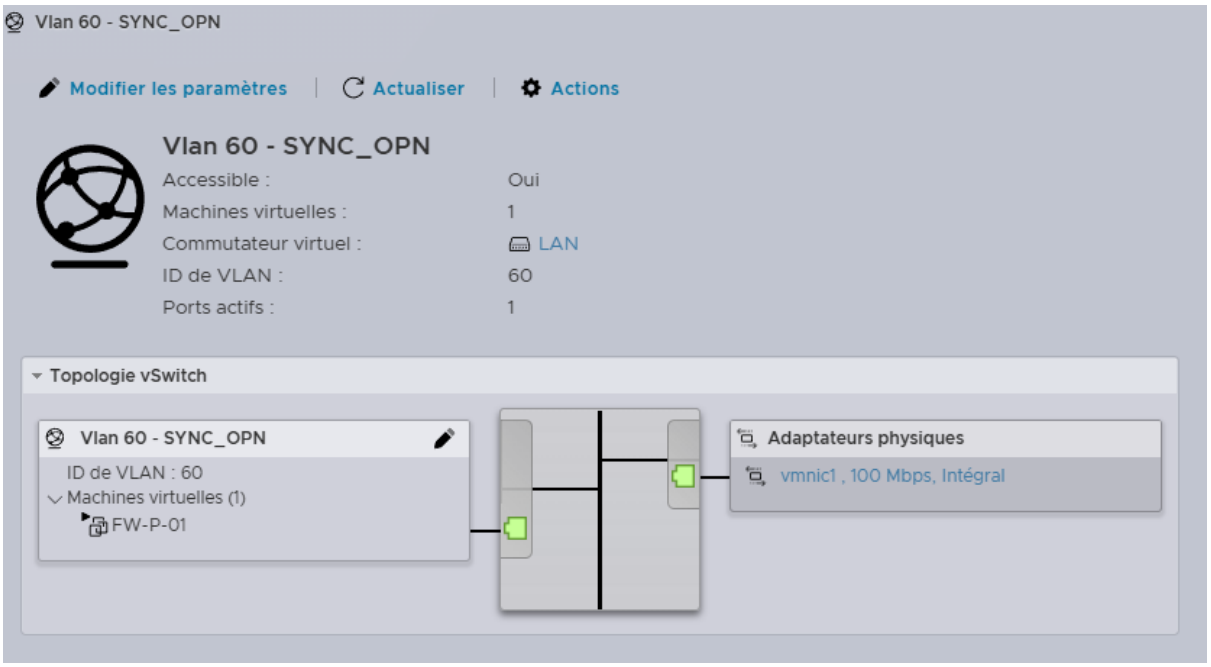


Afin de faire fonctionner le cluster de Firewall, il faut créer l'interface de synchronisation sur chaque Firewall, cette interface correspond au VLAN 60, SYNC_OPN.

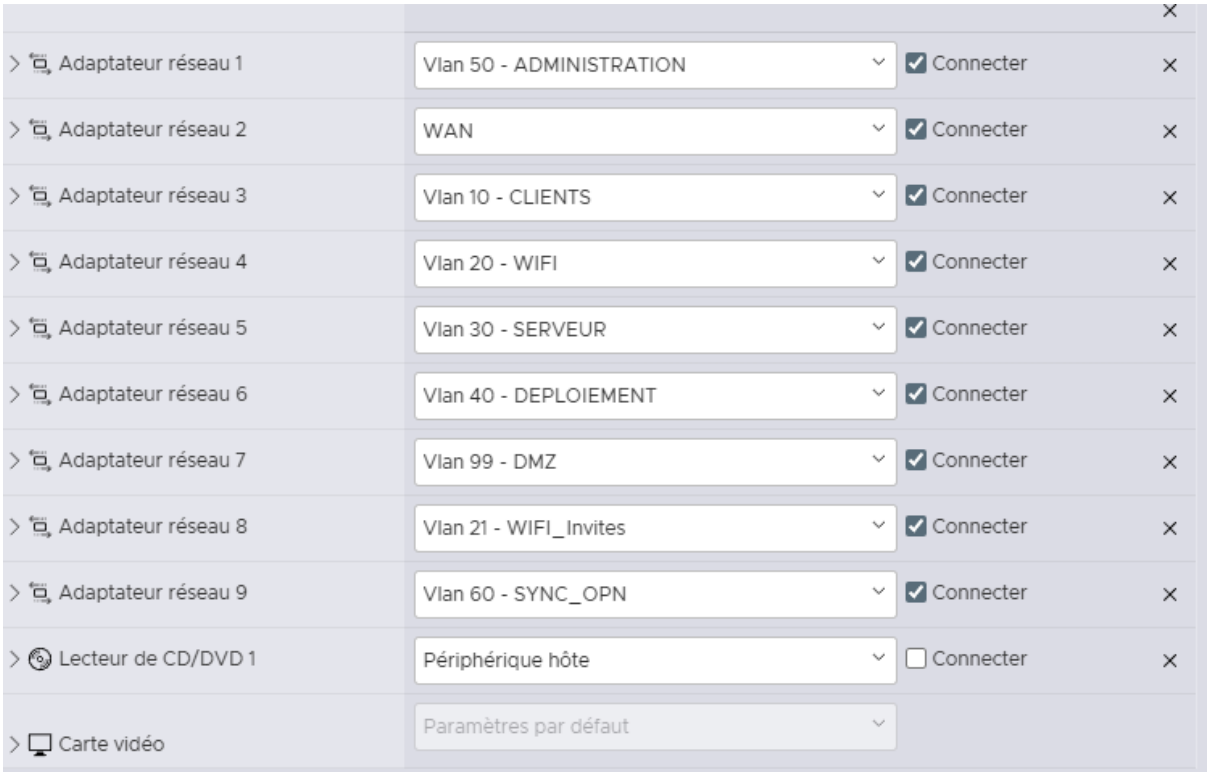
Pour la configuration de cette nouvelle interface, il faut ajouter un nouveau groupe de ports sur l'ESXI en Vlan 60 si celui-ci n'a pas déjà été ajouté et ajouter le nouveau VLAN sur les switchs.



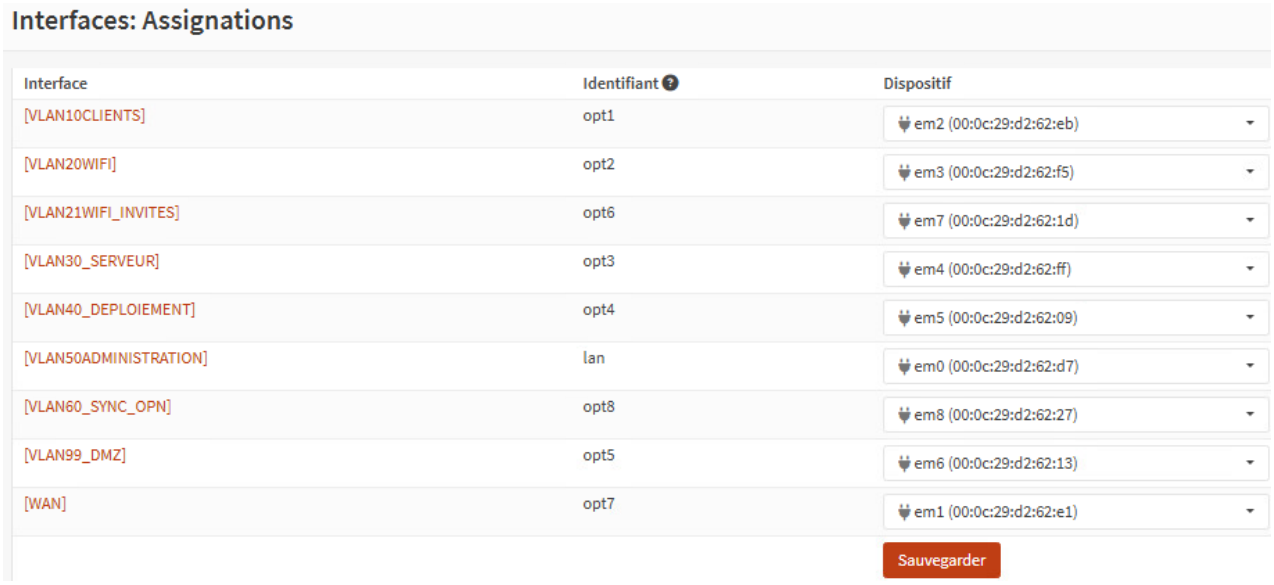
Nom	Ports actifs	ID du VLAN	Type
LAN	0	0	Groupe de ports standard
Vlan 10 - CLIENTS	1	10	Groupe de ports standard
Vlan 20 - WIFI	1	20	Groupe de ports standard
Vlan 40 - DEPLOIEMENT	1	40	Groupe de ports standard
Vlan 21 - WIFI_Invites	1	21	Groupe de ports standard
Vlan 60 - SYNC_OPN	1	60	Groupe de ports standard
Vlan 99 - DMZ	2	99	Groupe de ports standard
Vlan 50 - ADMINISTRATION	2	50	Groupe de ports standard
Vlan 30 - SERVEUR	9	30	Groupe de ports standard
WAN	1	0	Groupe de ports standard
Management Network	1	0	Groupe de ports standard



Une fois cela fait, si cela n'a pas été effectué auparavant, il faut créer une nouvelle machine virtuelle afin de faire office de second pare-feu, avec les mêmes ressources que le premier, 40 Go de stockage, 4 Go de RAM ainsi que les différentes cartes réseau ajoutées dans le même ordre que le premier pare-feu. Il faut ensuite ajouter une nouvelle carte réseau sur chaque pare-feu OPNsense pour la synchronisation. Il est important de faire attention à ce que les cartes réseau soient dans le même ordre sur les deux pares-feux. Ci-dessous, la configuration des cartes réseaux.



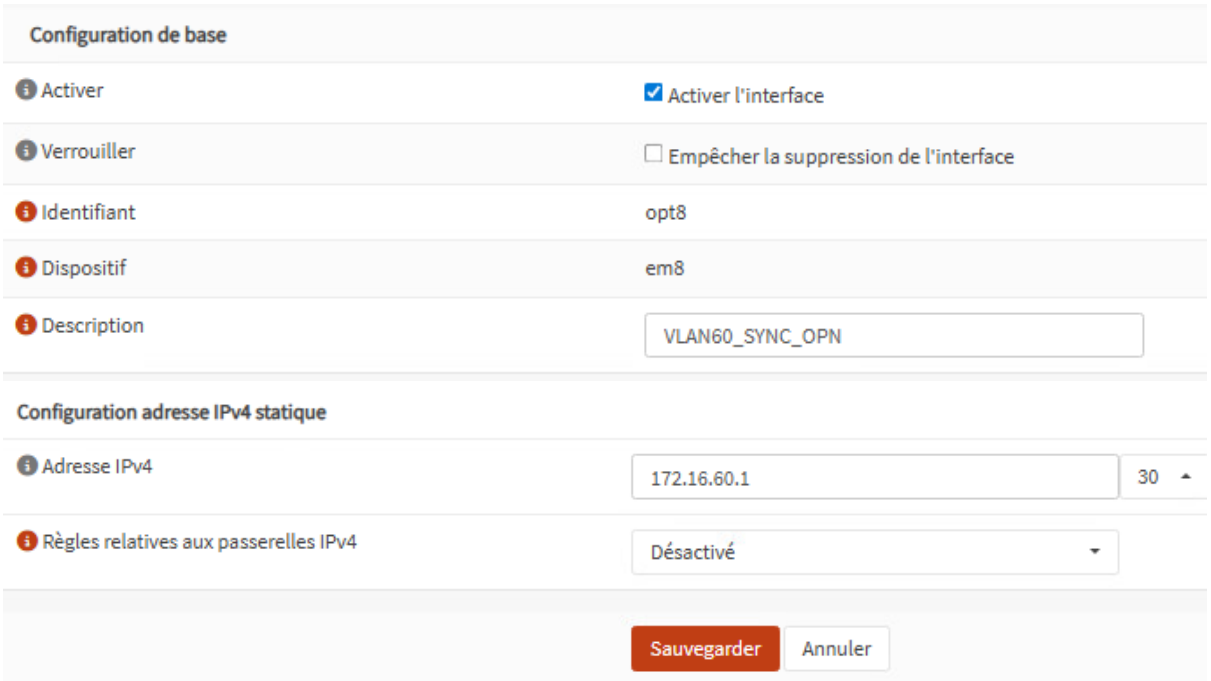
Après avoir ajouté ces cartes réseaux, il faut les assigner aux interfaces sur chaque Firewall, comme ci-dessous, si besoin voire l'étape sur la configuration de base et la configuration des interfaces.



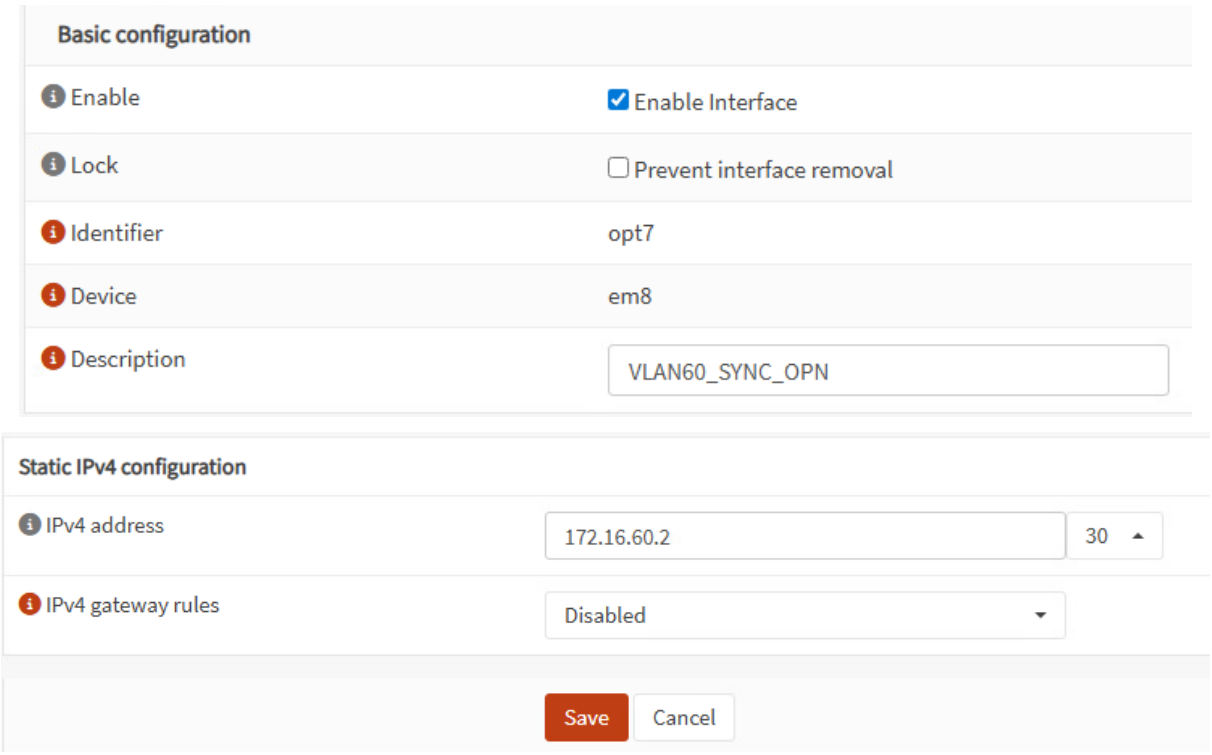
Ensuite, il faut activer les interfaces sur chaque pare-feu et attribuer les adresses IP statiques.

Pour cette configuration, le VLAN 60 a été mis en /30 afin de n'avoir que 2 adresses IP utilisables sur ce réseau, destinées au cluster et donc uniquement à la communication entre les deux pare-feux.

FW-P-01



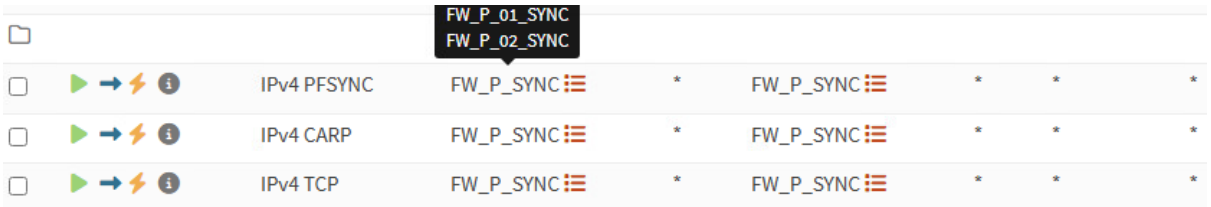
FW-P-02



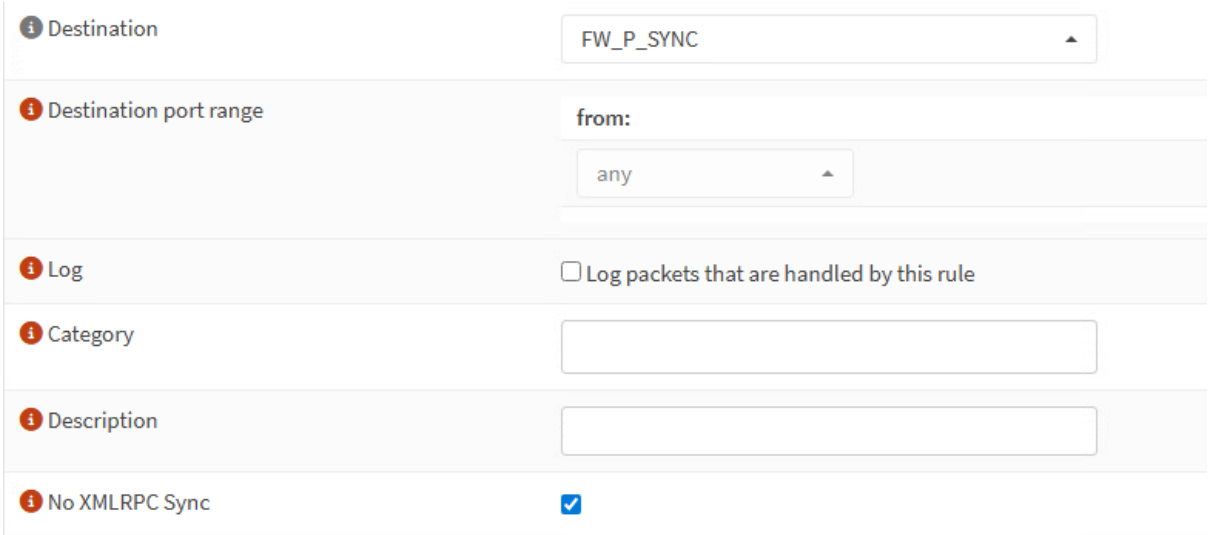
Une fois cela fait, il faut créer des règles sur chaque pare-feu afin que la connexion entre les deux puisse s'établir. Il est nécessaire de créer une règle pour le PFsync, correspondant à la synchronisation des configurations, une règle CARP pour la gestion du master et du backup, ainsi qu'une règle TCP pour la communication.

Pour ces règles, le protocole à utiliser a été spécifié ainsi que les machines autorisées à communiquer, c'est-à-dire les deux pare-feux.

Un alias a été créé pour chaque pare-feu, ainsi qu'un alias global afin de regrouper les deux machines.



Sur le pare-feu de backup (FW-P-02), il est nécessaire de cocher la case « No XMLRPC Sync ». Si celle-ci n'est pas cochée, les règles configurées seront effacées. Il est possible d'observer cela ci-dessous.



Après avoir configuré les différentes règles, il faut configurer la haute disponibilité dans « System », « High Availability » puis « Settings ».

Sur le master (FW-P-01), il faut configurer les « General Settings » et les « Synchronisation Settings ».

Sur le backup (FW-P-02), seuls les « General Settings » suffisent (il ne doit pas écraser la configuration du master).

IP de Synchronisation du Pair : IP de Synchronisation Firewall Distant

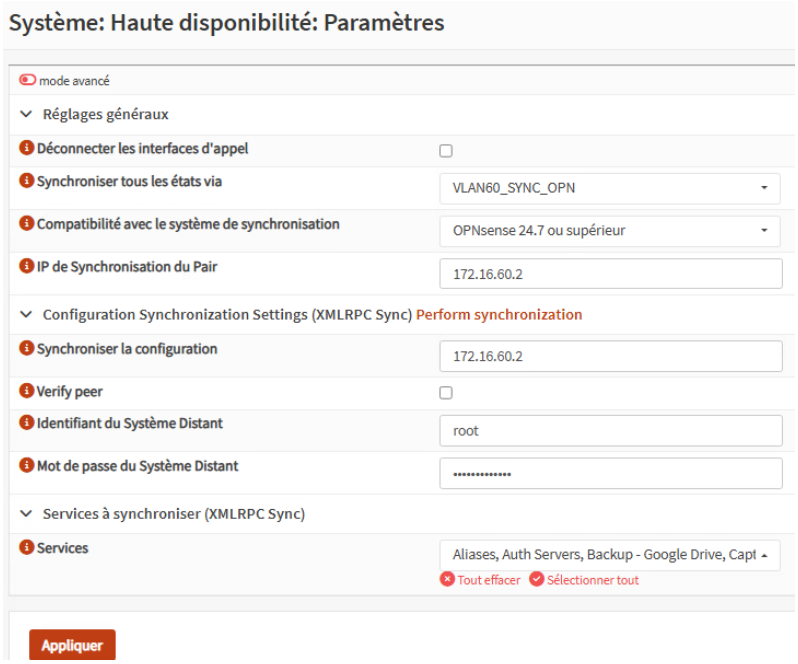
Synchroniser la configuration : Vers où synchroniser la configuration, IP Firewall Distant

Identifiant du Système Distant : Identifiant de connexion Firewall Distant

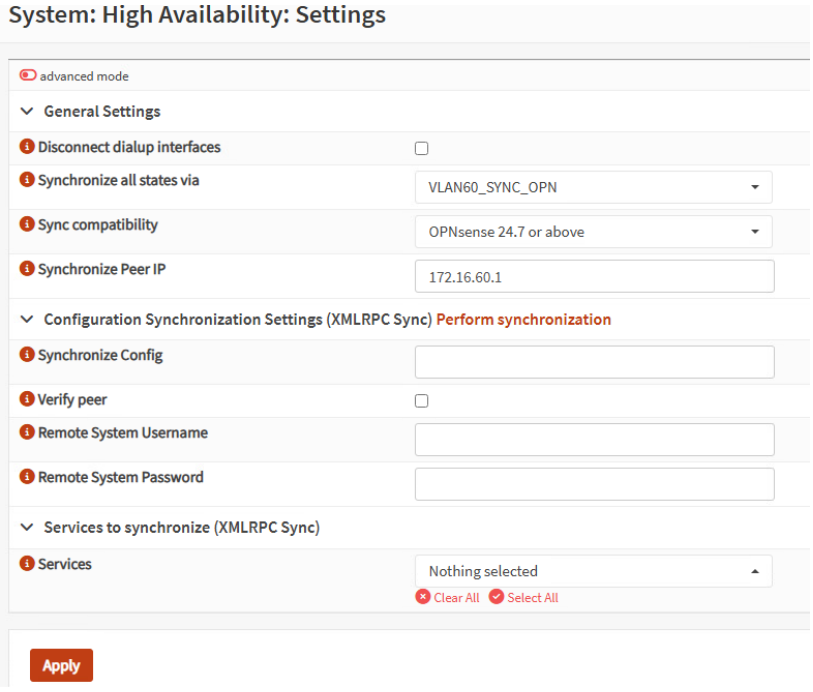
Mot de passe du Système Distant : Mot de passe de connexion Firewall Distant

Service à synchroniser (XMLRPC Sync) : Service à synchroniser sur Firewall Distant (Tout)

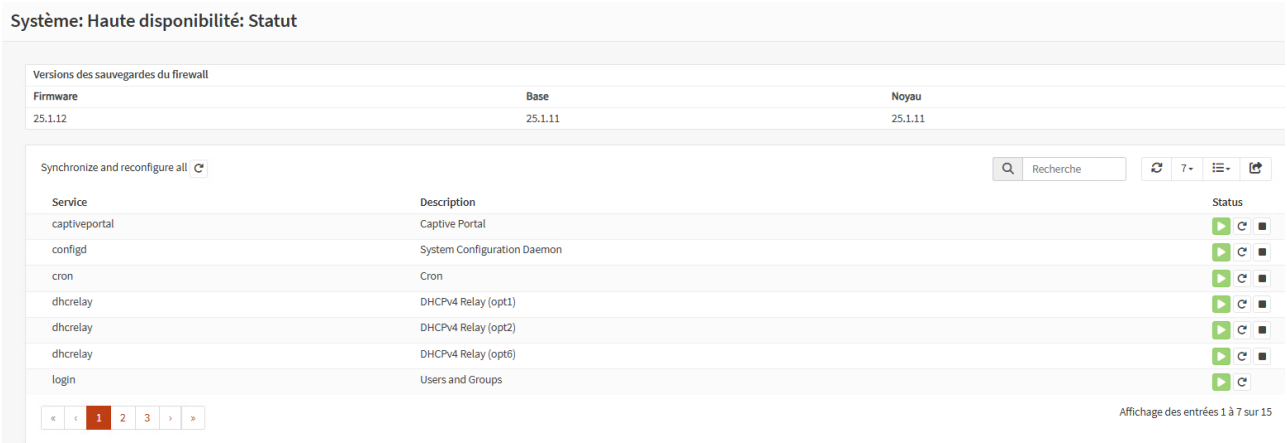
Configuration High Availability Master (FW-P-01)



Configuration High Availability Backup (FW-P-02)



Une fois ces deux configurations réalisées, il faut aller dans « System », « High Availability » puis « Status » sur le master (FW-P-01), afin de vérifier que le pare-feu distant est bien visible, comme ci-dessous. Si celui-ci n'apparaît pas, cela signifie qu'il y a un problème au niveau de la configuration « High Availability », de l'interconnexion entre les deux pare-feux ou des règles de pare-feu.



Si le pare-feu Master voit correctement le pare-feu de backup, il faut configurer les IP virtuelles.

Une IP virtuelle permet de fournir une passerelle partagée aux clients. Ici, toutes les passerelles partagées sont en .254 sur chaque VLAN (les pare-feux doivent avoir des IP en .253 pour le master et .252 pour le backup sur chaque interface)

Tout d'abord, il faut créer les adresses IP virtuelles sur le master. Pour cela, il faut se rendre dans « Interfaces », « Virtual IPs » puis « Settings » et créer une adresse IP virtuelle pour chaque interface, à l'exception de l'interface correspondant à la synchronisation entre les deux pare-feux OPNsense, le VLAN 60. Ci-dessous, un exemple avec l'interface correspondant au VLAN 10, suivi d'une image avec l'ensemble des adresses IP virtuelles créées.

Mode : CARP

Interface : Interface sur laquelle l'adresse IP virtuelle doit être créée

Réseau / Adresse : Correspond à la passerelle partagée

Mot de passe : Mot de passe entre les deux adresses IP virtuelles sur les pare-feux

Groupe VHID : Groupe qui sera partagé entre les deux machines pour cette IP virtuelle

Advbase : Correspond à la base d'intervalle d'annonce pour l'IP virtuelle (temps)

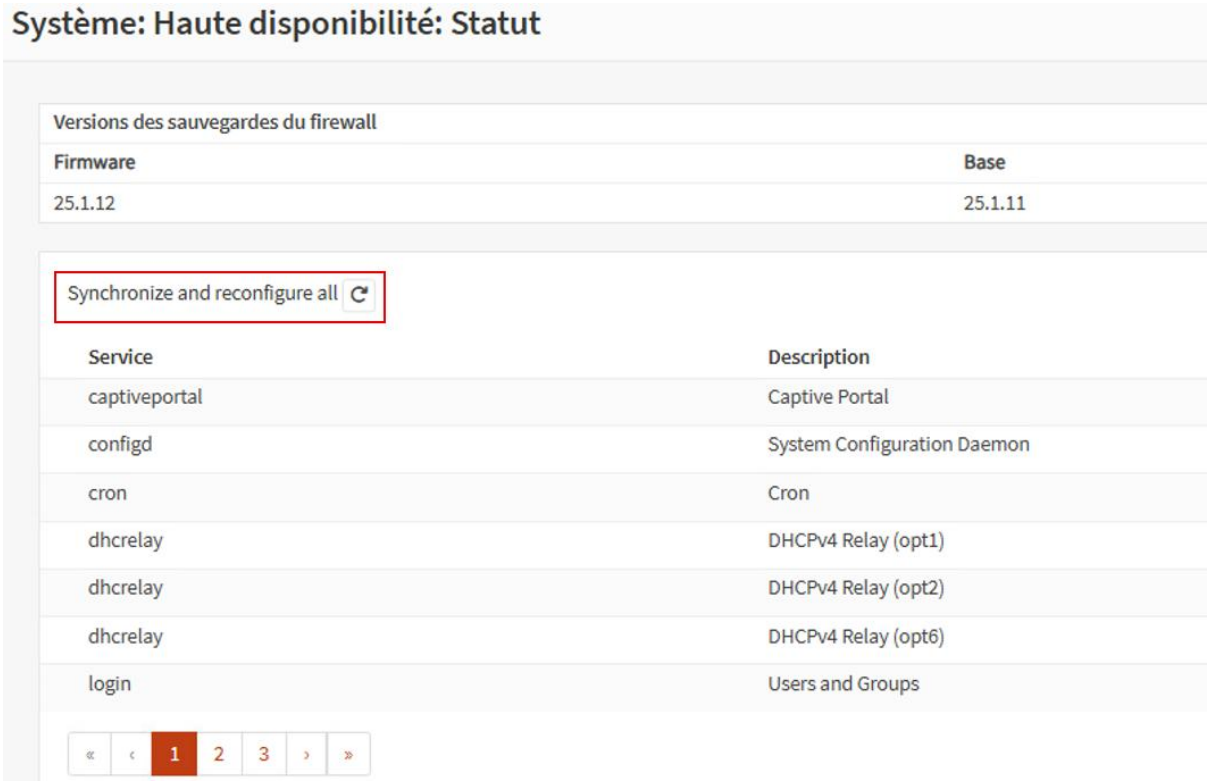
AdvSkew : Correspond à la priorité (ce qui définit le Backup et le Master), se configure automatiquement

Éditer l'IP virtuelle

mode avancé	
Mode	CARP
Interface	VLAN10CLIENTS
Réseau / Adresse	172.16.10.254/24
Pair (ipv4)	224.0.0.18
Pair (ipv6)	ff02::12
Refuser la liaison de service	☐
Mot de passe	••••••••••••
Groupe VHID	10 Sélectionnez un VHID non affecté
advbase	1
Pas de Sync XMLRPC	☐
Description	

☐	Réseau / Adresse	Groupe VHID	advbase	advskew	Interface	Mode
☐	172.16.10.254/24	10	1	0	VLAN10CLIENTS	CARP
☐	172.16.20.254/24	20	1	0	VLAN20WIFI	CARP
☐	172.16.30.254/24	30	1	0	VLAN30_SERVEUR	CARP
☐	172.16.40.254/24	40	1	0	VLAN40_DEPLOIEMENT	CARP
☐	172.16.50.254/24	50	1	0	VLAN50ADMINISTRATION	CARP
☐	172.16.21.254/24	21	1	0	VLAN21WIFI_INVITES	CARP
☐	172.16.99.254/24	99	1	0	VLAN99_DMZ	CARP
☐	10.44.150.76/24	150	1	0	WAN	CARP

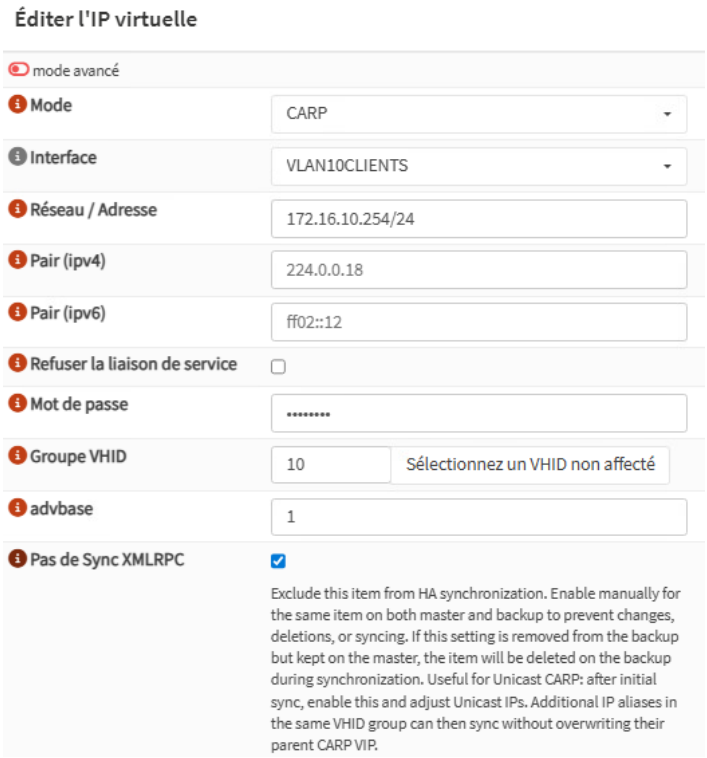
Une fois toutes les IP virtuelles créées, il faut répliquer la configuration depuis « System », « High Availability » puis « Status » avec le bouton « Synchronise and reconfigure all » afin d'envoyer toute la configuration du Master vers le Backup.



Une fois cela fait, l'ensemble de la configuration réalisée sur le pare-feu master (FW-P-01) devrait être synchronisée sur le pare-feu de backup. Afin d'éviter tout problème au sein du cluster de pare-feux, il faut passer l'ensemble des adresses IP virtuelles en advbase 2 sur le backup. Si cela n'est pas fait, il peut arriver que des conflits surviennent entre le backup et le master, comme nous pouvons le voir ci-dessous.

Network / Address	VHID Group	advbase	advskew	Interface	Mode
172.16.10.254/24	10	2	100	VLAN10CLIENTS	CARP
172.16.20.254/24	20	2	100	VLAN20WIFI	CARP
172.16.30.254/24	30	2	100	VLAN30_SERVEUR	CARP
172.16.40.254/24	40	2	100	VLAN40_DEPLOIEMENT	CARP
172.16.50.254/24	50	2	100	VLAN50ADMINISTRATION	CARP
172.16.21.254/24	21	2	100	VLAN21WIFI_INVITES	CARP
172.16.99.254/24	99	2	100	VLAN99_DMZ	CARP
10.44.150.76/24	150	2	100	WAN	CARP

Puis sur chaque pare-feu, il faut cocher la case « No XMLRPC Sync » sur chaque IP virtuelle sinon les adresses IP virtuelles seront recréées à chaque synchronisation du Firewall master vers le backup. Comme ci-dessous sur l'IP virtuelle correspondant au VLAN 10.



Pour terminer, dans « Interfaces », « Virtual IPs » puis « Status », toutes les Interfaces doivent être en master sur le pare-feu principal (FW-P-01) et toutes les interfaces doivent être en backup sur le pare-feu secondaire (FW-P-02).

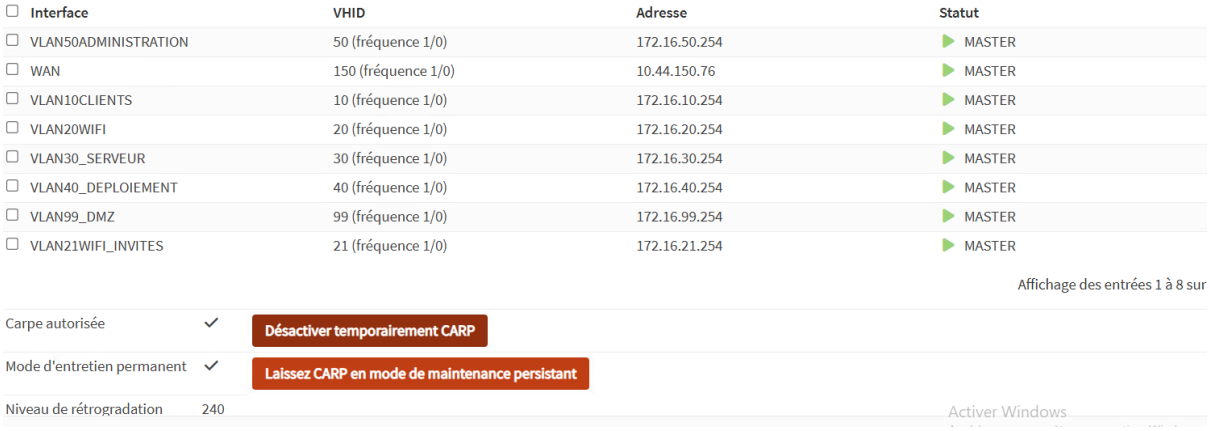
Interface	VHID	Adresse	Statut
VLAN50ADMINISTRATION	50 (fréquence 1/0)	172.16.50.254	MASTER
WAN	150 (fréquence 1/0)	10.44.150.76	MASTER
VLAN10CLIENTS	10 (fréquence 1/0)	172.16.10.254	MASTER
VLAN20WIFI	20 (fréquence 1/0)	172.16.20.254	MASTER
VLAN30_SERVEUR	30 (fréquence 1/0)	172.16.30.254	MASTER
VLAN40_DEPLOIEMENT	40 (fréquence 1/0)	172.16.40.254	MASTER
VLAN99_DMZ	99 (fréquence 1/0)	172.16.99.254	MASTER
VLAN21WIFI_INVITES	21 (fréquence 1/0)	172.16.21.254	MASTER

Interface	VHID	Address	Status
VLAN10CLIENTS	10 (freq. 2/100)	172.16.10.254	BACKUP
VLAN20WIFI	20 (freq. 2/100)	172.16.20.254	BACKUP
VLAN21WIFI_INVITES	21 (freq. 2/100)	172.16.21.254	BACKUP
VLAN30_SERVEUR	30 (freq. 2/100)	172.16.30.254	BACKUP
VLAN40_DEPLOIEMENT	40 (freq. 2/100)	172.16.40.254	BACKUP
VLAN50ADMINISTRATION	50 (freq. 2/100)	172.16.50.254	BACKUP
VLAN99_DMZ	99 (freq. 2/100)	172.16.99.254	BACKUP
WAN	150 (freq. 2/100)	10.44.150.76	BACKUP

9) Test Fonctionnement CARP

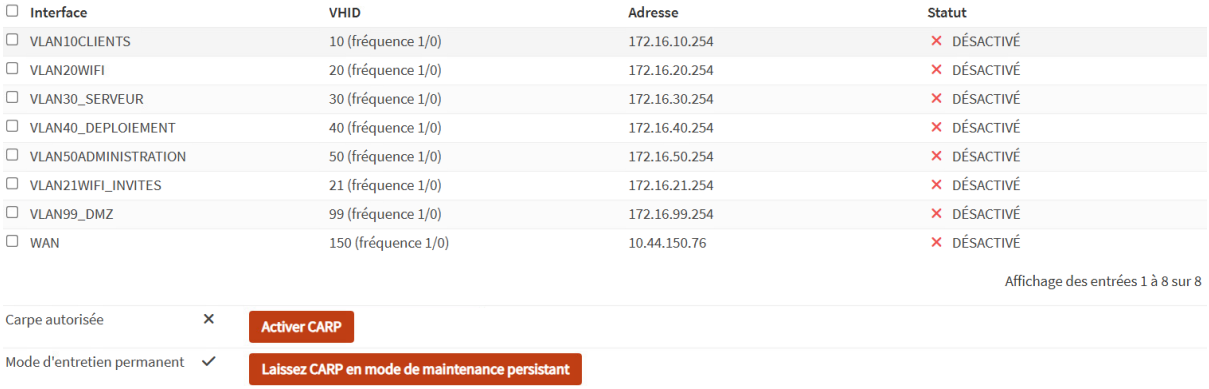
OPNsense propose de désactiver le CARP afin de tester le fonctionnement du cluster, il est possible de le désactiver sur le master comme ci-dessous. Si cela est fait, le pare-feu de Backup doit normalement récupérer la main et donc devenir master.

Firewall Master (FW-P-01)



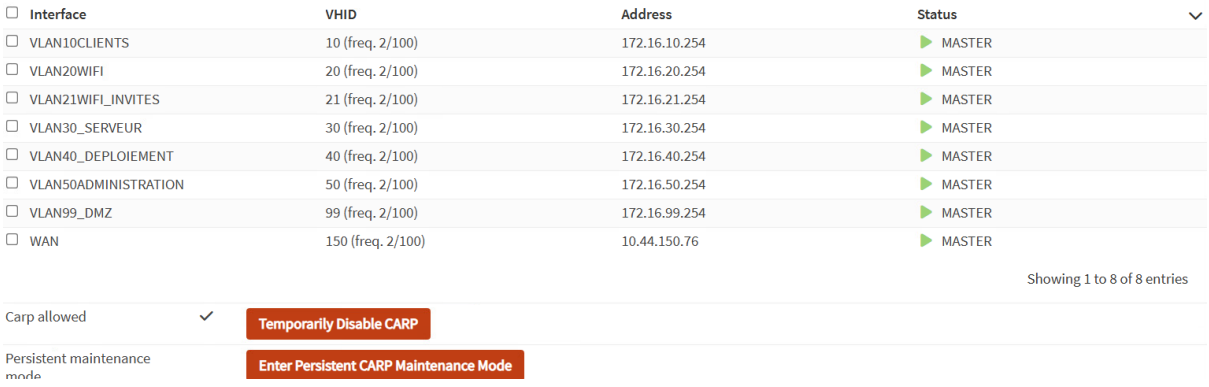
Interface	VHID	Adresse	Statut
VLAN50ADMINISTRATION	50 (fréquence 1/0)	172.16.50.254	MASTER
WAN	150 (fréquence 1/0)	10.44.150.76	MASTER
VLAN10CLIENTS	10 (fréquence 1/0)	172.16.10.254	MASTER
VLAN20WIFI	20 (fréquence 1/0)	172.16.20.254	MASTER
VLAN30_SERVEUR	30 (fréquence 1/0)	172.16.30.254	MASTER
VLAN40_DEPLOIEMENT	40 (fréquence 1/0)	172.16.40.254	MASTER
VLAN99_DMZ	99 (fréquence 1/0)	172.16.99.254	MASTER
VLAN21WIFI_INVITES	21 (fréquence 1/0)	172.16.21.254	MASTER

Firewall Master après désactivation (FW-P-01)



Interface	VHID	Adresse	Statut
VLAN10CLIENTS	10 (fréquence 1/0)	172.16.10.254	DÉSACTIVÉ
VLAN20WIFI	20 (fréquence 1/0)	172.16.20.254	DÉSACTIVÉ
VLAN30_SERVEUR	30 (fréquence 1/0)	172.16.30.254	DÉSACTIVÉ
VLAN40_DEPLOIEMENT	40 (fréquence 1/0)	172.16.40.254	DÉSACTIVÉ
VLAN50ADMINISTRATION	50 (fréquence 1/0)	172.16.50.254	DÉSACTIVÉ
VLAN21WIFI_INVITES	21 (fréquence 1/0)	172.16.21.254	DÉSACTIVÉ
VLAN99_DMZ	99 (fréquence 1/0)	172.16.99.254	DÉSACTIVÉ
WAN	150 (fréquence 1/0)	10.44.150.76	DÉSACTIVÉ

Firewall Secondaire après désactivation du CARP sur le Master



Interface	VHID	Address	Status
VLAN10CLIENTS	10 (freq. 2/100)	172.16.10.254	MASTER
VLAN20WIFI	20 (freq. 2/100)	172.16.20.254	MASTER
VLAN21WIFI_INVITES	21 (freq. 2/100)	172.16.21.254	MASTER
VLAN30_SERVEUR	30 (freq. 2/100)	172.16.30.254	MASTER
VLAN40_DEPLOIEMENT	40 (freq. 2/100)	172.16.40.254	MASTER
VLAN50ADMINISTRATION	50 (freq. 2/100)	172.16.50.254	MASTER
VLAN99_DMZ	99 (freq. 2/100)	172.16.99.254	MASTER
WAN	150 (freq. 2/100)	10.44.150.76	MASTER

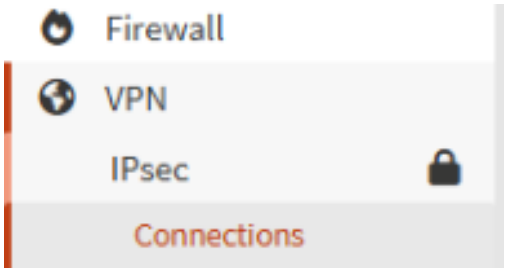
10) Configuration VPN

Dans cette configuration, l'IPsec est utilisé pour réaliser du VPN site à site.

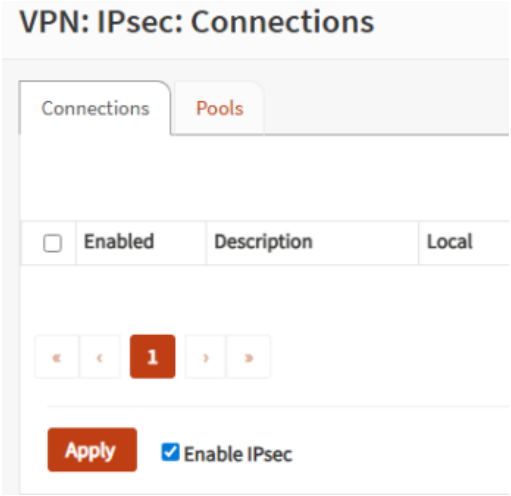
Cet outil correspond à différents protocoles de sécurité qui permettent de sécuriser les communications sur un réseau IP.

Cette configuration est réalisée directement sur le pare-feu OPNsense car celui-ci prend en charge l'IPsec pour du VPN site à site et dispose d'une IP WAN qui permet de faire du VPN entre les différents sites.

Pour cette configuration, il faut tout d'abord se rendre dans « VPN », « IPsec » puis « Connections ».

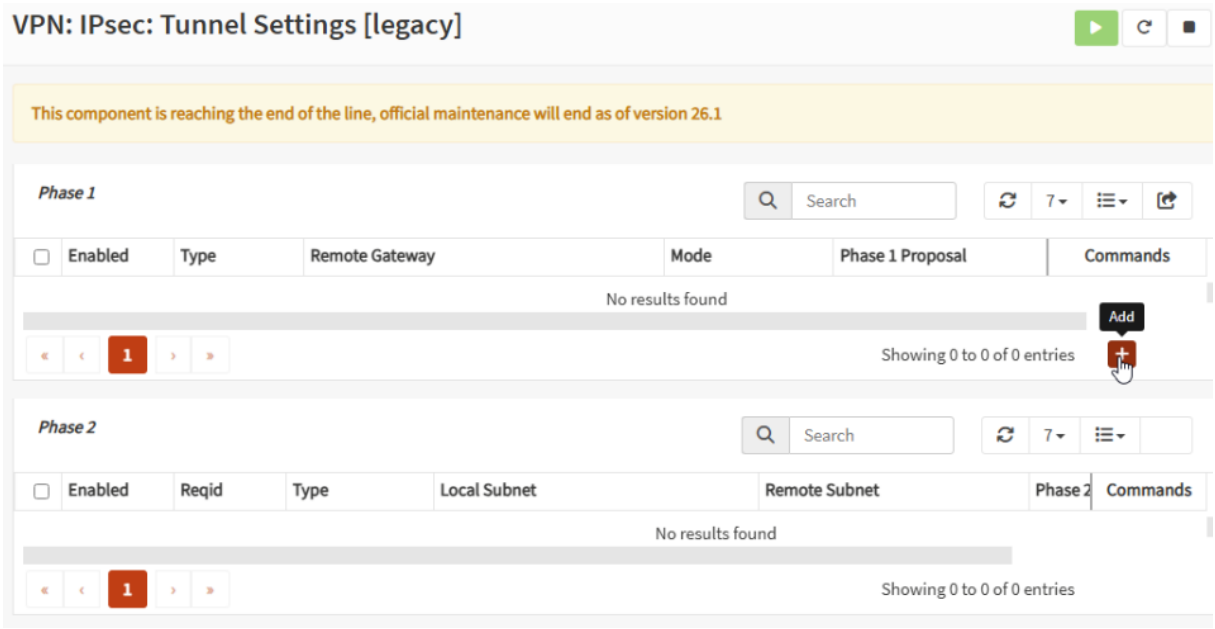


Une fois sur cette page, il faut cliquer sur le bouton « Enable IPSec » puis « Apply » afin d'activer le service IPSec sur le Firewall.



Ensuite, il faut aller dans l'onglet « VPN », « IPsec » puis « Tunnel Setting [legacy] » afin de configurer les paramètres VPN.

Sur la page correspondant aux paramètres de tunnels, il faut ajouter une phase 1 en cliquant sur le bouton. La phase 1 correspond à l'authentification qu'il va y avoir entre les deux équipements au bout du tunnel VPN, c'est ce qui permet d'établir le tunnel sécurisé.



La page ci-dessous doit s'afficher, sur cette page il faut renseigner différentes informations :

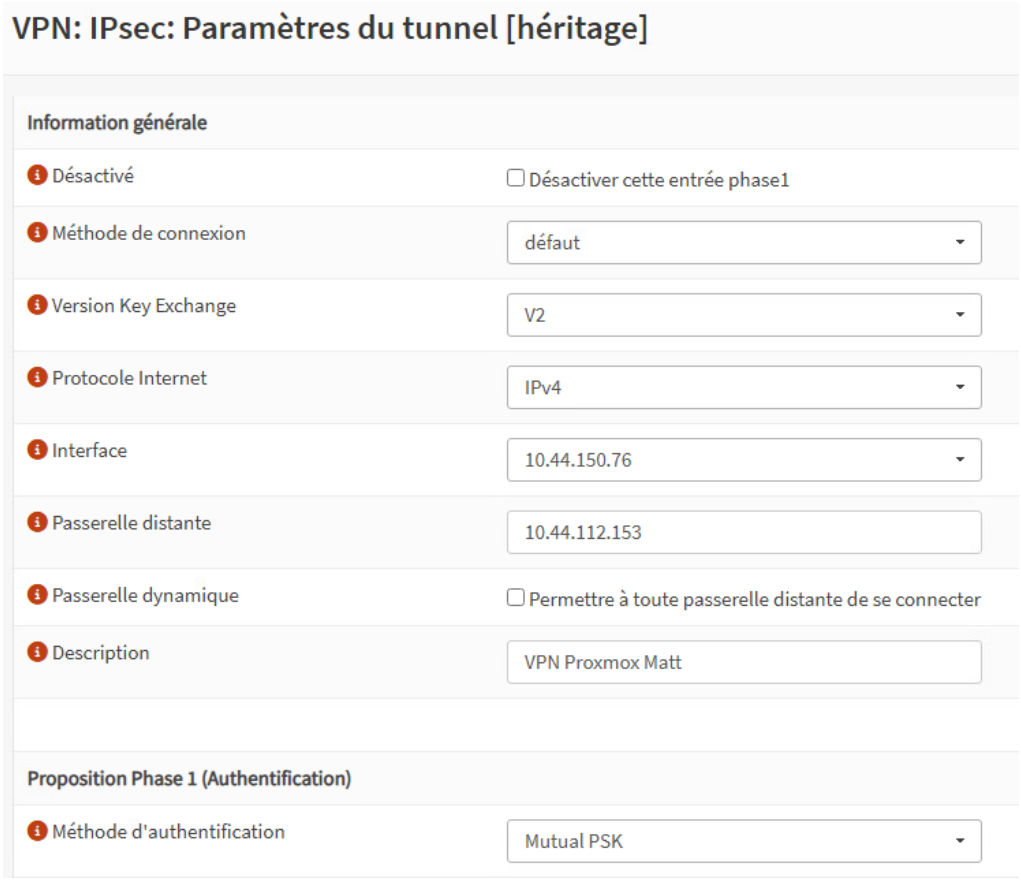
Version key Exchange : Définit la version du protocole Key Exchange à utiliser : V2

Protocole Internet : Type de protocole internet à utiliser : IPv4

Interface : Adresse IP à utiliser pour communiquer vers l'autre site, ici, l'IP du WAN du CARP, sinon l'interface WAN peut être utilisée

Passerelle distante : Adresse IP publique de la passerelle distante

Méthode d'authentification : Correspond au paramètre d'authentification défini côté distant pour monter le tunnel : Mutual PSK



Ensuite, plus bas sur la page, il y a d'autres paramètres à configurer :

Mon identifiant : Identifiant utilisé pour monter le tunnel VPN, utiliser l'adresse IP qui va être utilisée pour communiquer avec l'autre site

ID du correspondant : Identifiant utilisé du côté du site distant, mettre l'adresse IP distante avec laquelle s'établit les communications pour le tunnel VPN

Clé Pré-Partagée (PSK) : Clé partagée qui doit être semblable dans les deux configurations afin de monter le tunnel VPN

Algorithme de chiffrement : Algorithme de chiffrement utilisé pour le tunnel, doit être semblable côté distant : AES 256

Algorithme de hachage : Algorithme de hachage utilisé pour le tunnel, doit être semblable côté distant : SHA512

Groupe de clé DH : Méthode utilisée pour échanger des clés de chiffrement, doit être semblable côté distant : 14 (2048 bits)

Les autres paramètres ne sont pas utilisés ici, ils peuvent rester tel quel.

Méthode d'authentification	Mutual PSK
Mon identifiant	Adresse IP 10.44.150.75
ID du correspondant	Adresse IP 10.44.112.153
Clé Pré-Partagée (PSK)	NTxserveur44.

Proposition Phase 1 (Algorithmes)

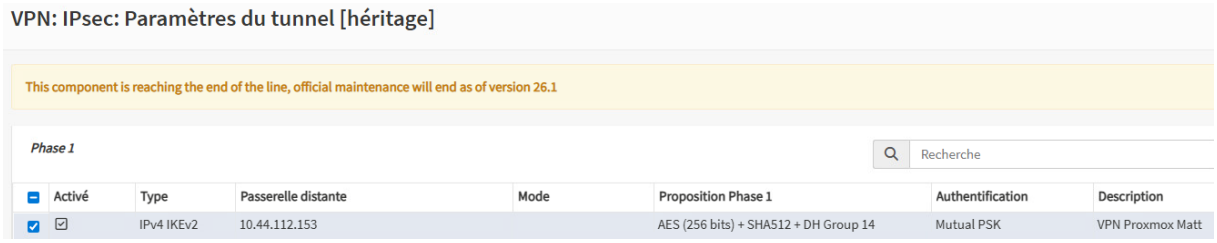
Algorithme de chiffrement	AES 256
Algorithme de hachage	SHA512
Groupe de clé DH	14 (2048 bits)

Options avancées

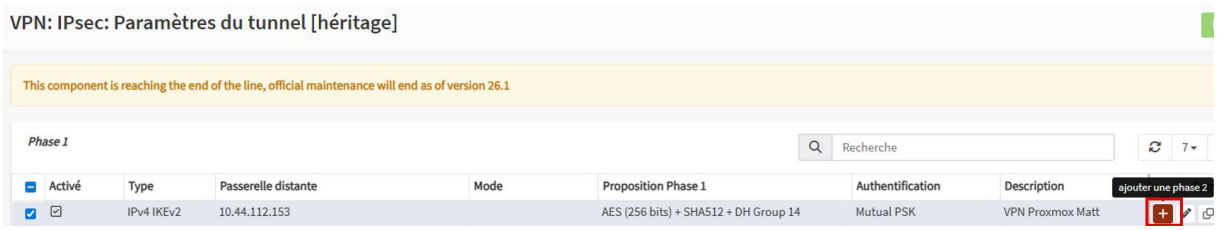
Installe les politiques	☑
Désactiver le Renouvellement de clé	☐
Désactiver Réauthentification	☐
Désactiver le Renouvellement de clé	☐
Désactiver Réauthentification	☐
Isolation de tunnel	☐
SHA256 Troncature de 96 bits	☐
NAT Traversant	Activer
Désactiver MOBIKE	☐
Action de fermeture	Aucun
Unique	Remplacer
Dead Peer Detection (Détection de la perte du correspondant)	☐
Délai d'inactivité	
Keyingtries	
Durée de vie	
Margintime	
Rekevfuzz	

Lorsque les différents champs sont remplis, il faut sauvegarder la configuration en bas de page afin de valider les paramétrages.

Une fois cela fait, la phase 1 doit apparaître sur la page, comme ci-dessous.



Après avoir réalisé la configuration de la phase 1, il faut ajouter une phase 2. Cette dernière s'appuie sur la première et permet de définir quel trafic passe dans le tunnel ainsi que la manière dont celui-ci est chiffré. Pour l'ajouter, il suffit de cliquer sur le bouton « + » se trouvant en face de la phase 1 créée précédemment.



La page ci-dessous devrait s'afficher, sur celle-ci, il faut réaliser différentes configurations :

Mode : Tunnel IPv4

Type de réseau local : Correspond au réseau local qui va communiquer avec le réseau local distant, dans cette situation, le VLAN 30

Type de réseau distant : Correspond au réseau local distant qui va communiquer avec le réseau local, dans cette situation, le réseau correspondant est le VLAN 30 distant

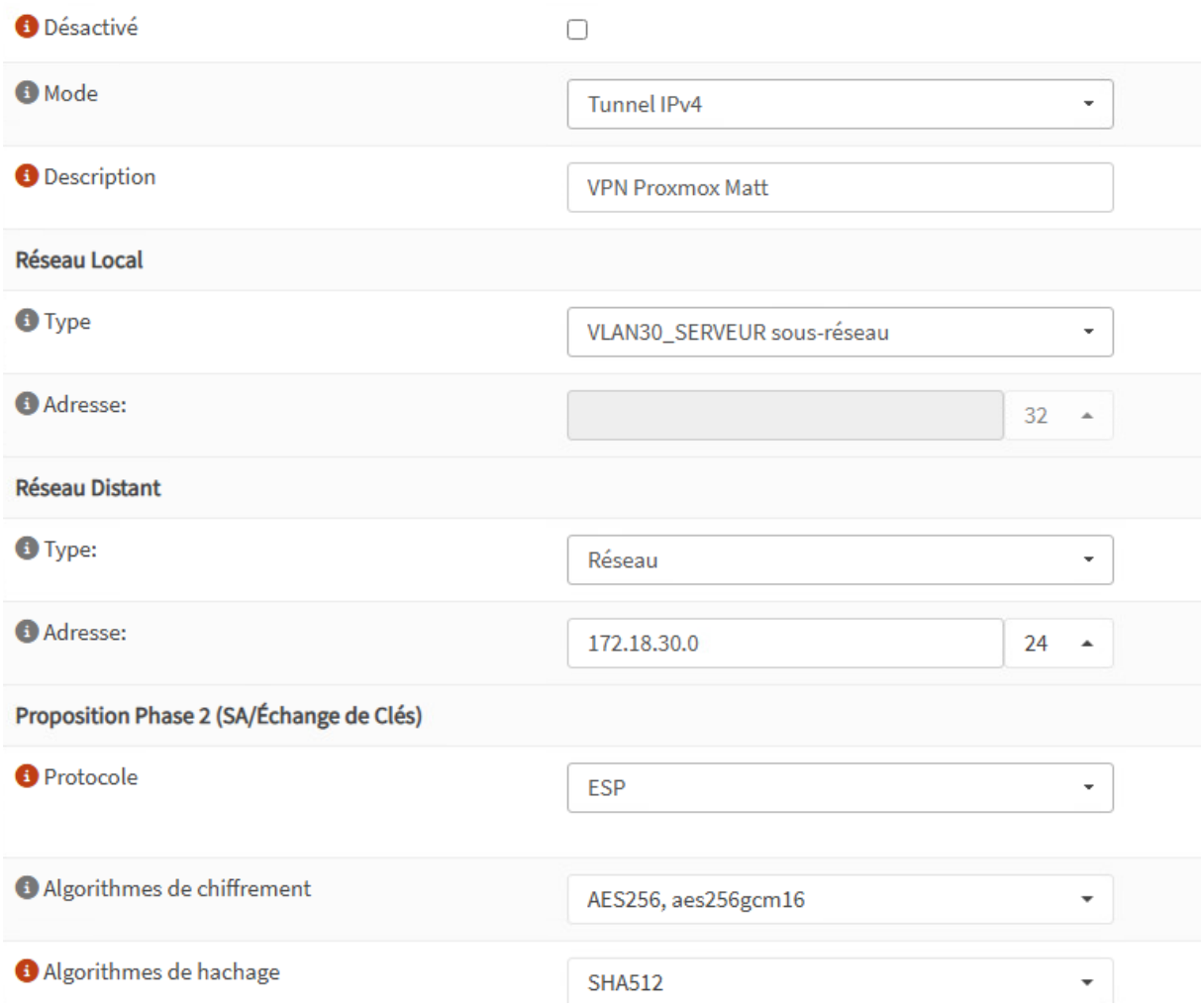
Protocole : ESP correspond au chiffrement

Algorithme de chiffrement : Algorithme de chiffrement utilisé pour cette phase 2 : AES256, aes256gcm16, ces deux algorithmes de chiffrement permettent de garantir un niveau de sécurité élevé pour les communications

Algorithme de hachage : Algorithme de hachage utilisé pour la phase 2 : SHA512, offre un niveau de sécurité correct par rapport aux autres algorithmes de hachage.

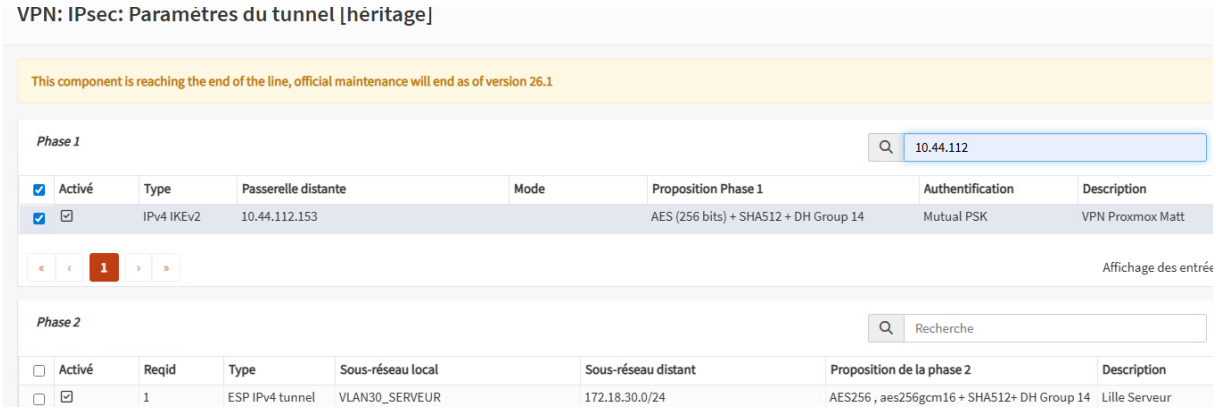
Groupe de clés PFS : 14 (2048 bits), offre un niveau de sécurité recommandé.

Durée de vie : 3600 secondes



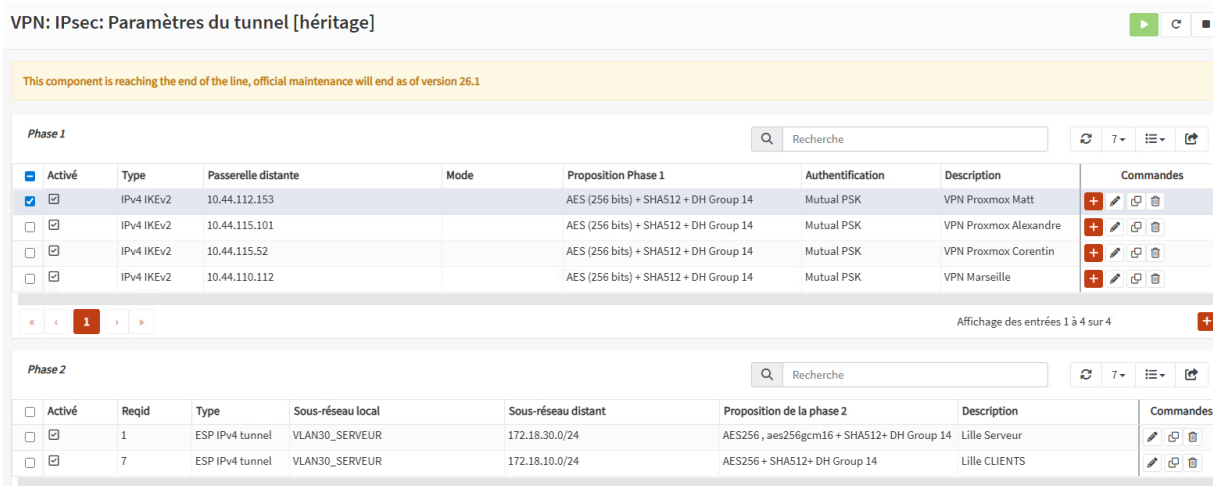
Après avoir renseigné les différents champs, il faut sauvegarder la configuration en bas de page.

Une fois la configuration enregistrée, il est normalement possible de voir la phase 1 et la phase 2.

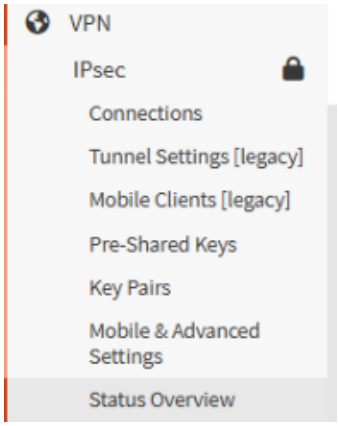


Il faut réaliser les mêmes actions sur le pare-feu distant pour la configuration VPN, tout en adaptant la configuration par rapport aux adresses IP.

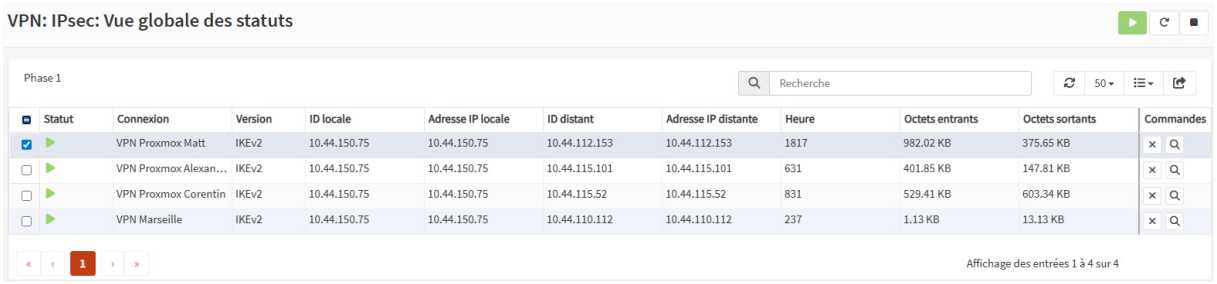
L'ensemble de la configuration réalisée correspond à l'image ci-dessous. La construction de l'infrastructure est sous forme de réseau maillé, il y a donc un tunnel VPN vers chaque site. Une deuxième phase 2 a également été établie, celle-ci va du serveur vers les clients pour la configuration de l'agent d'inventaire ou pour l'EDR.



A l'issue de cette configuration, il est possible de voir le statut des différents tunnels en allant dans « VPN », « IPsec » puis « Status Overview ».



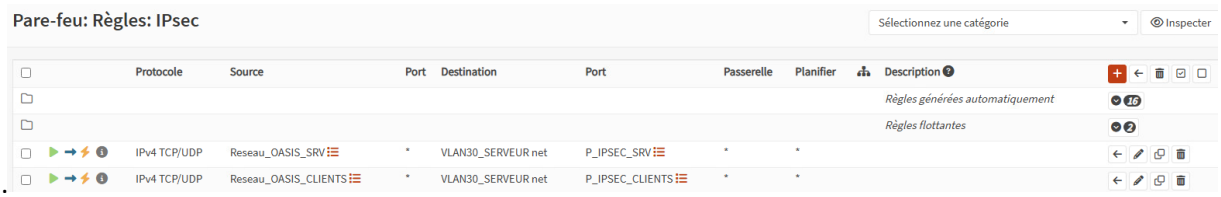
Sur cette page, il est possible de voir le statut de chaque tunnel et depuis combien de temps chaque tunnel est actif.

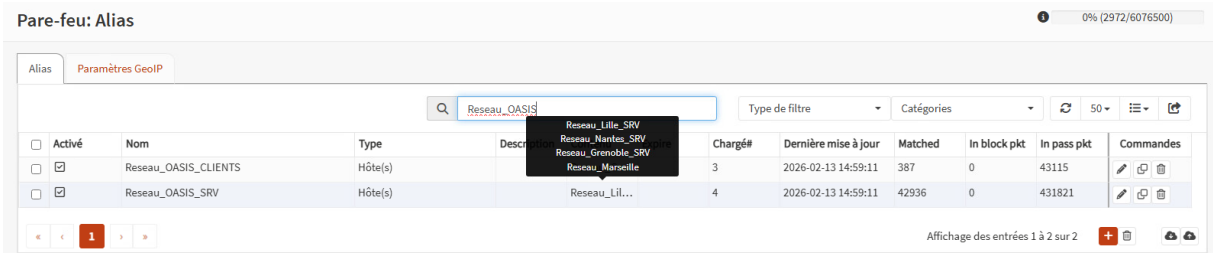


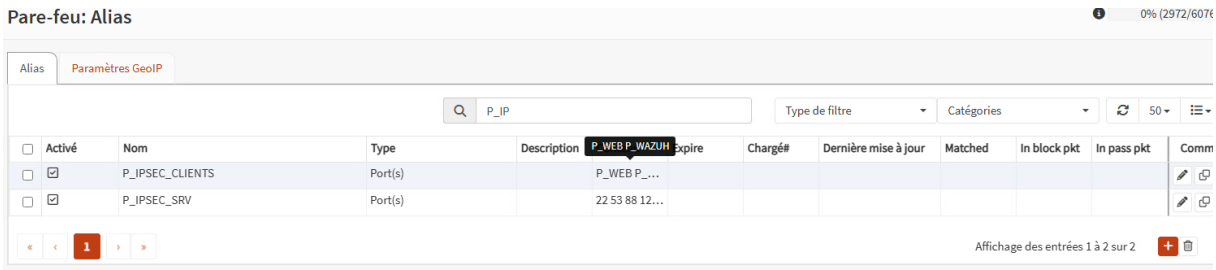
Avec cela, quelques règles de pare-feu ont été configurées pour l'IPsec. Il faut savoir que pour que le tunnel monte, aucune règle particulière n'est nécessaire.

Des règles ont donc été configurées afin d'ouvrir uniquement les ports souhaités et d'autoriser la communication entre les réseaux voulus. Deux alias sont utilisés pour l'ensemble des réseaux, un premier regroupant l'ensemble des réseaux du VLAN30 et un second pour l'ensemble des réseaux en VLAN10.

Pour les ports, deux groupes ont été créés afin de séparer les ports ouverts pour les clients et les serveurs. Des alias contenant les ports ouverts ont ensuite été ajoutés dans chacun de ces groupes, comme il est possible de le voir ci-dessous.




Pare-feu: Alias
0% (2972/6076500)
Alias
Paramètres GeoIP
Reseau_OASIS
Reseau_Lille_SRV
Reseau_Nantes_SRV
Reseau_Grenoble_SRV
Reseau_Marseille
Type de filtre
Catégories
50
Activé
Nom
Type
Chargé#
Dernière mise à jour
Matched
In block pkt
In pass pkt
Commandes
Reseau_OASIS_CLIENTS
Hôte(s)
3
2026-02-13 14:59:11
387
0
43115
Reseau_OASIS_SRV
Hôte(s)
Reseau_Lil...
4
2026-02-13 14:59:11
42936
0
431821
Affichage des entrées 1 à 2 sur 2


Pare-feu: Alias
0% (2972/6076
Alias
Paramètres GeoIP
P_IP
P_WEB P_WAZUH
Type de filtre
Catégories
50
Activé
Nom
Type
Description
Expire
Chargé#
Dernière mise à jour
Matched
In block pkt
In pass pkt
Comm
P_IPSEC_CLIENTS
Port(s)
P_WEB P_...
P_IPSEC_SRV
Port(s)
22 53 88 12...
Affichage des entrées 1 à 2 sur 2

Avec cela, l'ensemble des configurations sont réalisées. Il est possible de tester le fonctionnement en effectuant des tests de communication depuis une machine sur le VLAN 30, comme ci-dessous.

```
C:\Users\Administrateur>ping 172.17.10.254

Envoi d'une requête 'Ping'  172.17.10.254 avec 32 octets de données :
Réponse de 172.17.10.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.17.10.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.17.10.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.17.10.254 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 172.17.10.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\Administrateur>ping 172.18.30.254

Envoi d'une requête 'Ping'  172.18.30.254 avec 32 octets de données :
Réponse de 172.18.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.18.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.18.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.18.30.254 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 172.18.30.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\Administrateur>ping 172.19.30.254

Envoi d'une requête 'Ping'  172.19.30.254 avec 32 octets de données :
Réponse de 172.19.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.19.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.19.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.19.30.254 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 172.19.30.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\Administrateur>ping 172.20.30.254

Envoi d'une requête 'Ping'  172.20.30.254 avec 32 octets de données :
Réponse de 172.20.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.20.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.20.30.254 : octets=32 temps=1 ms TTL=63
Réponse de 172.20.30.254 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 172.20.30.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

k) Phase de test

11) Test accès à internet

Pour tester l'accès à internet, il faut tout d'abord tester si depuis le pare-feu directement on peut aller sur internet, pour cela il suffit de faire un test de communication depuis un serveur sur internet, par exemple google.fr.

```
root@FW-P-01:~ # ping google.Fr
PING google.Fr (142.251.209.131): 56 data bytes
64 bytes from 142.251.209.131: icmp_seq=0 ttl=115 time=32.509 ms
64 bytes from 142.251.209.131: icmp_seq=1 ttl=115 time=8.433 ms
64 bytes from 142.251.209.131: icmp_seq=2 ttl=115 time=9.084 ms
64 bytes from 142.251.209.131: icmp_seq=3 ttl=115 time=9.382 ms
64 bytes from 142.251.209.131: icmp_seq=4 ttl=115 time=8.863 ms
^C
--- google.Fr ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.433/13.654/32.509/9.432 ms
```

Ensuite, pour savoir si nos différents VLANs ont bien accès, il suffit de faire un test de communication depuis une machine sur un VLAN, par exemple depuis le DC01 de Paris.

```
C:\Users\Administrateur>ping google.fr

Envoi d'une requête 'ping' sur google.fr [142.251.142.3] avec 32 octets de données :
Réponse de 142.251.142.3 : octets=32 temps=27 ms TTL=114
Réponse de 142.251.142.3 : octets=32 temps=7 ms TTL=114
Réponse de 142.251.142.3 : octets=32 temps=7 ms TTL=114
Réponse de 142.251.142.3 : octets=32 temps=7 ms TTL=114

Statistiques Ping pour 142.251.142.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 27ms, Moyenne = 12ms
```

Grâce à cela, l'accès internet sur les différents VLANs du LAN est garanti.

12) Test différents services

Pour le test des différents services, il suffit de vérifier que depuis les serveurs si les services fonctionnent correctement. Par exemple, pour la gestion d'inventaire, il faut vérifier que les clients remontent correctement dans le serveur d'inventaire. De même, pour l'EDR, il faut s'assurer que les agents sont bien déployés et communiquent correctement avec le serveur Wazuh.

Ensuite, pour les services internes au pare-feu, il s'agit de vérifier leur bon fonctionnement depuis les clients ainsi que depuis les différents serveurs.

Par exemple, pour les règles de NAT, il faut tester chaque règle afin de vérifier que la translation est correcte. Pour les tunnels VPN IPsec, il faut vérifier que les tunnels montent correctement et que la communication entre les différents sites est fonctionnelle.

l) Axes d'amélioration

Pour ce projet, je pense qu'il y a différents axes d'amélioration. Tout d'abord, j'aurais pu implémenter un VPN Client-to-site, afin d'avoir directement un accès en VPN lorsque l'on est sur le réseau correspondant à notre WAN. Cela aurait permis de simplifier l'accès à certains outils.

Il aurait également été possible de mettre en place un filtrage DNS, c'est-à-dire de configurer un filtrage permettant de bloquer certains domaines potentiellement malveillants ou indésirables dans le cadre d'une entreprise.

Enfin, il aurait été possible d'activer un système de détection et prévention d'intrusions (IDS / IPS) via Suricata, qui est nativement intégré à OPNsense même si Wazuh est déjà présent au sein de l'infrastructure. Cela aurait permis d'analyser le trafic en temps réel et de bloquer de potentielles menaces.

m) Conclusion

En conclusion, j'ai trouvé que ce projet m'a permis d'apprendre de nombreuses choses. J'ai pu réaliser des tâches qui m'ont permis d'acquérir de nouvelles compétences sur la configuration d'un pare-feu de façon générale.

Au niveau des difficultés rencontrées, j'ai pu rencontrer des difficultés lors de la mise en place de règles sur OPNsense. En effet, il m'a été compliqué de savoir dans quel sens mettre les règles ou même de savoir quels ports ouvrir pour les différents services utilisés dans l'infrastructure.

J'ai également rencontré des difficultés lors de la mise en place de la redondance via le CARP. Il m'a été difficile de mettre en place cette redondance, cela n'était pas forcément correctement documenté sur OPNsense et j'avais loupé certaines notions sur cette partie-là, ce qui m'a fait faire tomber les interfaces du pare-feu quelques fois.

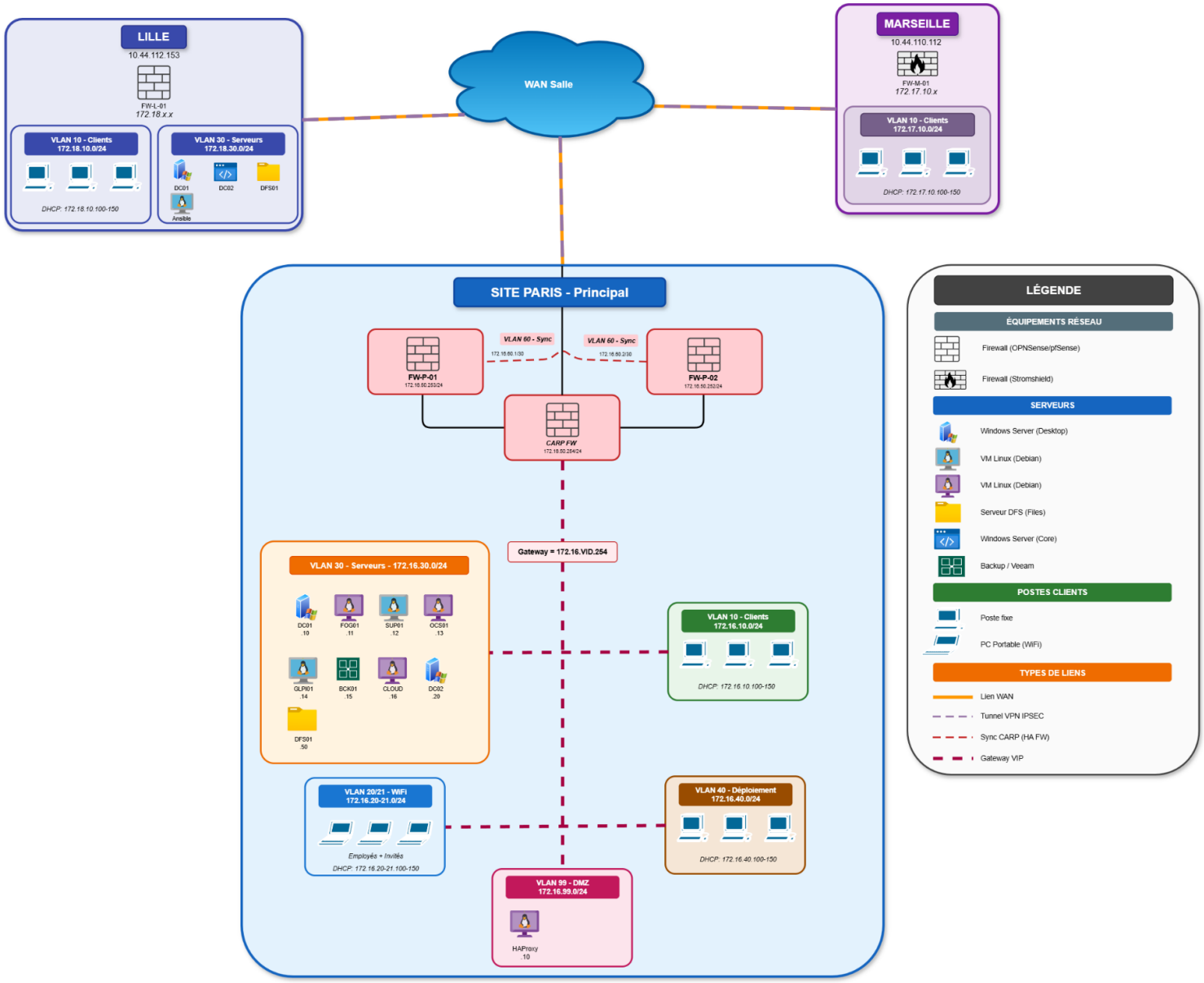
Malgré ces difficultés, je pense avoir répondu au cahier des charges ainsi qu'à l'objectif de la mission confiée, en mettant en place un équipement permettant de relier le WAN et le LAN de façon sécurisée.

Pour terminer, ce projet m'a permis de valider plusieurs compétences du référentiel BTS SIO Option SISR :

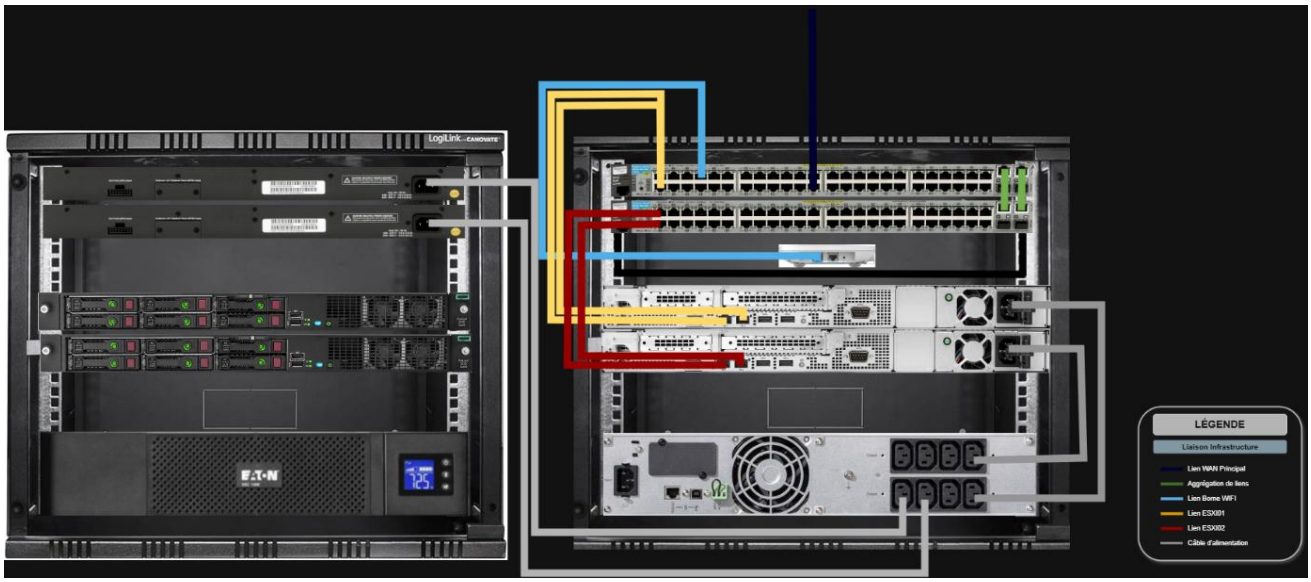
- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique

Annexes

a) Annexe n°1 : Schéma logique



b) Annexe n°2 : Schéma physique



c) Annexe n°3 : Plan d'adressage

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

Proxmox Matt (Lille)

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-L-DC01	172.18.30.10	255.255.255.0	172.18.30.0	172.18.30.254	DC1 Lille
SRV-L-DC02	172.18.30.20	255.255.255.0	172.18.30.0	172.18.30.254	DC2 Core Lille
SRV-L-ANS01	172.18.30.15	255.255.255.0	172.18.30.0	172.18.30.254	Ansible Lille
SRV-L-NETBOX01	172.18.30.30	255.255.255.0	172.18.30.0	172.18.30.254	Netbox Infrastructure
FW-L-01	172.18.10.254	255.255.255.0	172.18.10.0	172.18.10.254	IP FW-L-01 LAN Lille
FW-L-02	172.18.10.252	255.255.255.0	172.18.10.0	172.18.10.254	IP FW-L-02 LAN Lille
CARP Firewall Lille	172.18.10.254	255.255.255.0	172.18.10.0	172.18.10.254	Passerelle du VLAN 10
FW-L-01	172.18.30.254	255.255.255.0	172.18.30.0	172.18.30.254	IP FW-L-01 SRV Lille
FW-L-02	172.18.30.252	255.255.255.0	172.18.30.0	172.18.30.254	IP FW-L-02 SRV Lille
CARP Firewall Lille	172.18.30.254	255.255.255.0	172.18.30.0	172.18.30.254	Passerelle du VLAN 30
FW-L-01	172.18.60.1	255.255.255.252	172.18.60.0	-	IP FW-L-01 SYNC_OPN
FW-L-02	172.18.60.2	255.255.255.252	172.18.60.0	-	IP FW-L-02 SYNC_OPN
FW-L-01	172.18.99.254	255.255.255.0	172.18.99.0	172.18.99.254	IP FW-L-01 DMZ Lille
FW-L-02	172.18.99.252	255.255.255.0	172.18.99.0	172.18.99.254	IP FW-L-02 DMZ Lille
CARP Firewall Lille	172.18.99.254	255.255.255.0	172.18.99.0	172.18.99.254	Passerelle du VLAN 99
FW-L-01	10.44.115.50	255.255.255.0	10.44.115.0	10.44.115.254	IP WAN Lille
FW-L-02	10.44.112.100	255.255.255.0	10.44.112.0	10.44.112.254	IP FW-L-02 WAN
CARP Firewall Lille	10.44.112.153	255.255.255.0	10.44.112.0	10.44.112.254	CARP WAN

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	SS	172.18.10.254	172.18.30.10	172.18.30.20	Plage DHCP Client Lille

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille