Comment créer un environnement auto-hébergé sous Linux avec Proxmox

Salut! Je vais commencer cet article par une courte histoire personnelle.

Mon voyage dans le monde de l'informatique a commencé en 2009. À presque 21 ans, fraîchement sorti de l'école, je me suis retrouvé à la croisée des chemins. Mes études de gestion, d'économie et de droit ne
a suscité mon intérêt intrinsèque, mais l'attrait de l'informatique m'avait captivé. Dès mes premières années passées à bricoler des ordinateurs personnels C64, IBM XT (clones) et tout appareil doté d'un clavier, je savais que j'avais trouvé ma passion.

Au fil des années, mes compétences ont évolué grâce à l'auto-apprentissage. Je suis passé d'ingénieur d'installation au rôle multiforme d'administrateur réseau et système, en apprenant tout grâce à
les essais et erreurs inhérents au processus.

Un moment charnière de mon parcours s'est déroulé lors de ma première mission pour une compagnie d'assurance. En réfléchissant à la meilleure approche, j'ai décidé d'installer le réseau du client chez moi, dans mon bureau mansardé. Configuration réussie du serveur et des postes de travail, le résultat a été satisfaisant ; j'ai implémenté la solution sur site en une seule tentative.

Sans surprise, mon approche est restée largement inchangée au fil des années. Je m'immerge dans la compréhension des objectifs d'une organisation, en les alignant sur les solutions informatiques les plus adaptées.
Élaborer des propositions, obtenir l'approbation de la direction, construire l'infrastructure informatique et enfin réaliser le projet : cette méthodologie a résisté à l'épreuve du temps.

Mon parcours a été façonné non seulement par une expérience pratique, mais également par le soutien inestimable que j'ai reçu des livres, de la documentation et principalement d'Internet. C'est avant tout l'open source
des communautés qui m'ont aidé dans mon cheminement, alimentant mon désir de redonner. Dans cet esprit, j'ai choisi de documenter les éléments fondamentaux de la configuration du réseau, en espérant que cet article s'avérera bénéfique pour l'individu solitaire cherchant de l'aide pour démarrer son propre parcours informatique. Mon objectif est qu'il soit une source d'inspiration et d'informations pratiques pour ceux qui liront cet article.

1. Introduction

Dans cet article, nous examinons les aspects pratiques de la création d'un environnement auto-hébergé abordable, adapté aux laboratoires à domicile, aux bureaux à domicile et aux petites et moyennes entreprises. Donner la priorité à un approche « Lean » qui minimise à la fois les efforts et les coûts, notre objectif est de gérer les complexités dans un délai raisonnable.

S'appuyant sur des années d'expérience pratique au sein de petites et moyennes entreprises (PME), nous mettons l'accent sur l'intégration de solutions open source lorsque cela est viable. Il est crucial de reconnaître que des alternatives à sources fermées sont également explorées, la décision finale étant guidée par ce qui correspond le mieux aux exigences de l'entreprise, à l'expérience pratique et aux préférences technologiques.

Malgré la passion de l'auteur pour les solutions open source, nous reconnaissons qu'il peut y avoir des cas où une solution fermée s'avère plus optimale. Le message sous-jacent souligne le
Il est important de donner la priorité aux intérêts de l'entreprise plutôt qu'aux préférences personnelles, renforçant ainsi la nécessité d'aligner les décisions technologiques sur les besoins commerciaux plus larges.

Les environnements auto-hébergés, semblables aux configurations traditionnelles sur site, sont souvent associés à des coûts initiaux élevés. Bien qu'il existe des configurations hybrides sur site, l'approche auto-hébergée, s'appuyant sur vers une configuration hybride, peut offrir une rentabilité.

De plus, nous examinerons brièvement des alternatives telles que la migration vers des fournisseurs SaaS comme Microsoft et Google, en pesant soigneusement les avantages et les coûts associés. Qu'il s'agisse d'opter pour un Solution auto-hébergée indépendante ou forme hybride, elle offre liberté et contrôle, exigeant une prise en compte réfléchie de facteurs tels que la sécurité, la maintenance et les sauvegardes.

1.1. Point de départ

Passons maintenant aux rouages de notre environnement auto-hébergé. Nous devons concevoir un environnement informatique. L'idée est de s'assurer que notre configuration informatique s'aligne sur les objectifs commerciaux et répond efficacement aux besoins. Pour bien faire les choses, nous devons comprendre les tenants et les aboutissants de l'organisation.

Lors de l'introduction de solutions, il est essentiel d'aller au-delà des spécifications techniques et des exigences commerciales. Nous devons également prendre en compte les préférences et les besoins des personnes au sein de notre organisation. Trouver le bon équilibre est essentiel, car faire accepter les solutions par les utilisateurs est à la fois important et difficile.

Dans les sections à venir, nous approfondirons les spécificités de la conception de notre environnement auto-hébergé. Nous parlons de solutions rentables, d'une mise en œuvre rationalisée et d'un œil attentif sur ce dont notre organisation a réellement besoin. Commençons par concevoir un environnement informatique efficace et économique !

1.1.1. Conception de réseau et connectivité Internet

Notre conception commence par l'épine dorsale de notre configuration : le réseau. Cela englobe tout, de notre connexion Internet et de notre pare-feu/routeur aux commutateurs physiques et à leurs configurations,
y compris la configuration des VLAN. Nous plongeons dans les éléments essentiels qui maintiennent notre environnement auto-hébergé connecté et sécurisé. Décomposons chaque composant pour garantir une solution robuste et conception de réseau efficace au chapitre 2.

1.1.2. Routage

Passons maintenant à un aspect crucial : le routage vers et depuis Internet. Cela implique d'approfondir les complexités d'une ou plusieurs adresses IPv4 fixes, ainsi que la discussion sur les pointeurs.
enregistrements. Nous explorons diverses options, telles que les sous-réseaux (routés), qui pourraient être fournis par le FAI ou établis séparément via GRE. Nous examinerons également la transmission du trafic à l'aide d'iptables sous Linux.

Face aux défis, tels que les connexions Internet limitées où le FAI peut ne pas fournir plusieurs adresses IPv4 ou définir l'enregistrement de pointeur DNS souhaité, nous explorerons des solutions de contournement. Il peut
il y a même des défis où nous ne sommes pas en mesure d'établir un tunnel GRE. Nous devrons peut-être examiner des alternatives, comme opter pour une adresse IPv4 fixe via l'un des fournisseurs VPN disponibles.
Passons en revue ces considérations de routage pour garantir que notre environnement auto-hébergé communique efficacement avec le paysage numérique plus large.

1.1.3. Segmentation du réseau

En déplaçant notre attention, approfondissons le domaine crucial de la segmentation des réseaux et soulignons l'importance d'une DMZ (zone démilitarisée). Considérez essentiellement une DMZ comme un VLAN spécialisé, mais qui joue un rôle central dans la gestion du trafic entrant (et sortant) et dans le renforcement de nos mesures de sécurité.

La segmentation du réseau est importante !

La segmentation du réseau implique de diviser notre réseau en segments distincts ou VLAN, chacun servant un objectif spécifique. Cette pratique n'est pas seulement une question d'organisation ; c'est une décision stratégique
améliorer la sécurité, l'efficacité et les performances globales du réseau.

Note spéciale sur DMZ

Zoomons maintenant sur la DMZ – un VLAN avec une mission unique. Cette zone agit comme un tampon entre notre réseau interne et le monde extérieur, ajoutant une couche de défense supplémentaire. C'est l'endroit idéal pour les services qui nécessitent une accessibilité publique, tels que les serveurs Web et de messagerie. En isolant ces services, nous atténuons les risques potentiels associés à une exposition directe à notre réseau interne.

En nous aventurant dans les complexités de la segmentation du réseau et le rôle central de la DMZ, nous ne créons pas seulement une structure ; nous renforçons la posture de sécurité de nos serveurs auto-hébergés
environnement. Explorons comment cette conception stratégique peut protéger efficacement notre paysage numérique (au chapitre 2).

1.1.4. Serveur physique versus hyperviseur (VM)

Nous devrons également inviter un serveur à notre fête. Un seul serveur physique avec un seul système d'exploitation peut s'avérer inefficace et ne dispose pas de la flexibilité nécessaire aux environnements informatiques dynamiques. Dans cet article, nous travaillerons sous l'hypothèse d'un serveur équipé d'un hyperviseur, et un choix populaire pour ce rôle est Proxmox.

Un hyperviseur nous permet de créer et de gérer de manière transparente plusieurs machines virtuelles sur un seul serveur physique. Proxmox, en particulier, se démarque comme un puissant hyperviseur open source, optimisant l'utilisation des ressources et permettant la coexistence harmonieuse de systèmes d'exploitation indépendants. Essentiellement, cela change la donne en termes d'efficacité et de flexibilité de notre serveur.
Infrastructure.

1.1.5. Des débuts modestes

Dans notre voyage, nous commençons par des débuts modestes, ancrés par un ordinateur fidèle affectueusement nommé Scrappy. Scrappy, notre nœud dédié de 19 pouces, dispose d'un processeur Intel i3-4170, de 24 Go de RAM, d'un SSD M.2 de 500 Go et de 3 disques SSD SATA de 500 Go de 2,5 pouces. Cette modeste « centrale matérielle » assumera le rôle d'hyperviseur Proxmox pour nos machines virtuelles. Ce modeste serveur est utilisé pour démontrer qu'un environnement serveur ne dépend pas uniquement de la puissance brute.

Sur le plan réseau, nous optons pour la robustesse open source, en utilisant le logiciel polyvalent pfSense pour le routage et le pare-feu. Il convient de noter que les mêmes résultats peuvent être obtenus avec OPNsense. Nos configurations VLAN sur les commutateurs physiques sont influencées par la conception d'un commutateur HP ProCurve. En plus de réutiliser un commutateur HP, on peut explorer d'autres alternatives économiques telles que les commutateurs de ZyXEL ou TP-Link. Dans ce dernier cas, TP-Link Omada apparaît comme un choix louable, surtout lorsqu'il est géré de manière centralisée avec le contrôleur Omada. Vous pouvez acquérir le contrôleur Omada en tant que contrôleur matériel (OC200 ou OC300). Alternativement, le logiciel Omada est disponible sous forme de progiciels pouvant être
installé sur des plates-formes comme une VM Linux.

Ces choix matériels constituent l'épine dorsale de notre environnement auto-hébergé, démontrant que même avec des débuts modestes, nous pouvons construire une infrastructure informatique robuste et flexible.

2. Conception du réseau

Maintenant que nous avons terminé l'introduction, il est temps de commencer le voyage dynamique de la conception de réseau !

2.1. VLAN et sous-réseaux

Avant de procéder à la conception d'un réseau, nous devons savoir ce qui « vit » dans « notre » réseau ? Il peut s'agir de serveurs, de stockages, de postes de travail, d'imprimantes, d'équipements invités (téléphones portables, tablettes ou même téléviseurs), d'onduleurs de panneaux solaires et bien sûr de commutateurs et de points d'accès. Dès qu'un inventaire a été réalisé, les nœuds peuvent être classés. L'idée est d'utiliser des VLAN et des sous-réseaux logiques pour le

mise en page.

Sur la base d'une inventaire, l'aménagement pourrait ressembler à ceci.

VLAN	Description	Subnet	Explanation (by example)
0001	Management 1	172.21.1.0/24	Switches, access points
0002	Management 2	172.22.2.0/24	Hypervisor(s), KVM-over-IP (eg iLO, IPMI)
0016	Servers	10.10.16.0/24	Server VMs
0018	Storage	10.10.18.0/24	Network Attached Storage (NAS)
0032	Office LAN	10.10.32.0/24	Workstations (desktop and laptop computers)
0036	Peripherals	10.10.36.0/24	Printers
0251	IoT	172.31.251.0/24	Solar panel inverters
0252	DMZ	172.31.252.0/24	Web and mail server
0253	GuestNET	172.31.253.0/24	Guest Wi-Fi network

2.1.1. VLAN

Dans cette conception de réseau, la principale distinction réside dans la séparation des composants critiques, notamment les équipements réseau, les hyperviseurs, les machines virtuelles des serveurs, les périphériques (tels que les imprimantes), les postes de travail et les services accessibles sur Internet.

> Dans le contexte d'un ou plusieurs serveurs de bureau à distance (anciennement appelés serveurs de terminaux), il devient évident qu'il est crucial d'établir un VLAN distinct. Cette décision découle de la envisager de classer un serveur de bureau à distance non seulement comme un serveur traditionnel, mais plutôt comme un poste de travail spécialisé. Bien qu'il fonctionne comme un serveur, le placer directement dans le réseau local du bureau n'est peut-être pas l'approche la plus appropriée, ce qui souligne la nécessité d'un VLAN distinct.
>
> De plus, le placement stratégique des contrôleurs de domaine mérite un examen attentif. Placer un contrôleur de domaine dans le VLAN général du serveur peut potentiellement l'exposer à la sécurité vulnérabilités. Pour renforcer les mesures de sécurité, il est conseillé d'attribuer un VLAN dédié aux contrôleurs de domaine. Cette approche minimise la surface d'attaque en ouvrant uniquement les ports les plus essentiels, contribuant ainsi à une infrastructure réseau plus robuste et sécurisée.
>
> Pour plus de sécurité, le concept de création de VLAN distincts pour les contrôleurs de domaine en écriture et les contrôleurs de domaine en lecture seule peut être exploré. Cette segmentation garantit que l'exposition à les autres serveurs et clients sont méticuleusement contrôlés, renforçant ainsi la sécurité globale du réseau.

Comprendre la raison d'être des numéros de VLAN et des sous-réseaux est crucial. S'il est pratique de regrouper les VLAN de gestion, les sous-réseaux sont volontairement variés. Pour les VLAN de gestion, l'identification du VLAN est intuitive ; on peut déterminer l'emplacement de leur VLAN en observant le troisième (et également le deuxième) octet, indiquant le VLAN de gestion 1 ou le VLAN de gestion 2.

Cette même approche logique s'étend au troisième octet sur d'autres VLAN, fournissant une structure systématique et facilement interprétable sur l'ensemble du réseau.

2.1.2 Sous-réseaux

Dans le paragraphe précédent, nous avons brièvement évoqué les sous-réseaux.

> Ce n'est pas grave si ce paragraphe n'est pas entièrement compris immédiatement. Utilisez simplement le calculateur IP recommandé ci-dessous et revisitez la théorie plus tard si nécessaire. Comprendre l'essentiel de ce sujet est suffisant et utiliser un calculateur IP et du bon sens suffisent pour réussir !

Les sous-réseaux nécessitent un calcul réfléchi et une conception logique, chacun définissant une plage IP spécifique. Par exemple, le réseau local d'Office s'étend de 10.10.32.0 à 10.10.32.255, pouvant accueillir jusqu'à 254 hôtes avec un masque CIDR de /24 (équivalent à un masque de sous-réseau de 255.255.255.0), établissant ainsi un sous-réseau structuré. Pour répondre à une croissance potentielle, envisagez d'étendre la plage IP de 10.10.32.0 à 10.10.35.255 avec un masque CIDR de /22 (traduit par un masque de sous-réseau de 255.255.252.0), garantissant ainsi l'adaptabilité à l'évolution des besoins de l'organisation.

Comprendre comment calculer les sous-réseaux est crucial pour la conception du réseau. Le processus consiste à déterminer la taille de chaque sous-réseau, ce qui est essentiel pour la gestion des adresses IP.

Formule

La formule pour calculer la taille du sous-réseau est la suivante : Taille du sous-réseau = 2^(32 - CIDR). Ici, CIDR (Classless Inter-Domain Routing) représente la notation utilisée pour spécifier la taille d'un sous-réseau.

Par exemple, si vous avez une notation CIDR de /24, le calcul serait : Taille du sous-réseau = 2^(32 - 24) = 2^8 = 256 adresses. Cela signifie que le sous-réseau peut accueillir 256 hôtes.

Nous devons prendre en compte les éléments suivants : adresses des hôtes : 256 - 2 = 254 hôtes

- La soustraction de 2 comptes pour l'adresse réseau et l'adresse de diffusion !

Ainsi, lorsque nous disons qu'un sous-réseau /24 peut accueillir 254 hôtes, c'est une manière simplifiée d'exprimer que 256 adresses sont disponibles, mais que deux sont réservées aux adresses réseau et de diffusion. Ceci peut être déroutant au début pour ceux qui découvrent les réseaux, mais c'est une pratique standard en matière d'adressage IP.

Une autre variable à prendre en compte est que le comptage commence à « zéro » : 0-255 signifie 256.

Pour explorer d'autres possibilités...

- Recalcul pour /23 : Taille du sous-réseau = 2^(32 - 23) = 2^9 = 512 adresses.
- Recalcul pour /22 : Taille du sous-réseau = 2^(32 - 22) = 2^10 = 1 024 adresses.
- Recalcul pour /21 : Taille du sous-réseau = 2^(32 - 21) = 2^11 = 2 048 adresses.

De plus, en considérant une notation CIDR plus petite comme /29 : Taille du sous-réseau = 2^(32 - 29) = 2^3 = 8 adresses. Cela implique que le sous-réseau peut accueillir 8 hôtes.

> Concernant le CIDR/29, il est important de noter qu'un minimum de deux IP est inutilisable en raison du réseau et de l'adresse de diffusion. De plus, une adresse IP est réservée au routeur, ce qui laisse de la place pour un total pratique de cinq nœuds utilisables.

Notez qu'à mesure que la valeur CIDR diminue, la taille du sous-réseau augmente, fournissant plus d'adresses d'hôte mais nécessitant potentiellement plus d'adresses IP de l'espace réseau global. Un calculateur IP, comme celui disponible sur jodies.de, peut accélérer ces calculs pour une planification efficace du réseau.

Ce dernier point est important lorsque l'on examine la DMZ. On pourrait préconiser de conserver les sous-réseaux de plusieurs DMZ aussi petits que possible pour une sécurité renforcée. Une approche judicieuse pour améliorer davantage sécurité en séparant logiquement les différents services au sein de DMZ distinctes. Il ajoute une couche d'isolement, minimisant les risques potentiels et contenant toute faille de sécurité sur des segments spécifiques.

Une note sur le calcul binaire

En coulisses, les calculs de sous-réseaux impliquent des opérations binaires. Décomposons l'exemple d'une notation CIDR /24 :

Notation CIDR : /24

Représentation binaire : 11111111.11111111.11111111.00000000

La série de 1 dans la représentation binaire signifie la partie réseau, tandis que la série de 0 représente les adresses d'hôte disponibles. La taille du sous-réseau est déterminée en comptant le nombre de zéros. Dans un sous-réseau /24, il y a 8 zéros, ce qui se traduit par 2^8, ce qui équivaut à 256 adresses.

Comprendre cet aspect binaire donne un aperçu des mécanismes fondamentaux du sous-réseau. Bien qu'il ne soit pas essentiel pour les calculs quotidiens, il offre une compréhension plus approfondie de la façon dont le CIDR la notation influence la taille du sous-réseau dans le domaine des chiffres binaires (bits). Si les lecteurs souhaitent approfondir les nuances binaires, ces connaissances peuvent améliorer leur compréhension des principes de mise en réseau.

Comme le calculateur IP mentionné, l'utilisation d'un aide-mémoire de sous-réseau peut aider. Veuillez jeter un œil à l' aide-mémoire sur les sous-réseaux IPv4. [PDF] du site Web populaire de Jeremy Strectch, packetlife.net !

2.1.3 Démêler les VLAN

Poursuivant notre exploration des VLAN, nous approfondissons le domaine de la configuration des VLAN. Les VLAN, ou réseaux locaux virtuels, servent d'outils essentiels pour segmenter logiquement les réseaux, améliorant ainsi l'organisation et la sécurité. Pour naviguer efficacement dans la complexité des VLAN, une compréhension fondamentale des concepts clés, notamment le trunking VLAN, est importante.

> Ce n'est pas grave si ce paragraphe n'est pas entièrement compris immédiatement. Dans le chapitre suivant, nous mettrons la théorie en pratique ! Comprendre l'essentiel de ce sujet est suffisant.
>
> En fin de compte, c'est la pratique qui rend parfait ! Il est normal que vous ne compreniez pas immédiatement comment appliquer la théorie dans la pratique. Plus d'explications avec des exemples pratiques suivront dans le chapitres suivants.

Comprendre IEEE 802.1Q

Les VLAN fonctionnent dans le cadre de la norme IEEE 802.1Q, un protocole conçu pour intégrer de manière transparente les informations VLAN dans les trames Ethernet. Ce mécanisme de marquage permet des commutateurs et des routeurs pour discerner l'appartenance au VLAN de chaque paquet, garantissant ainsi le routage et le transfert précis du trafic au sein du réseau.

VLAN balisés et non balisés

VLAN balisés :
Dans une configuration VLAN balisée, chaque trame Ethernet transporte des informations supplémentaires sous forme de balises, indiquant clairement son appartenance au VLAN. Cette méthode s'avère indispensable entre les commutateurs et les routeurs, permettant aux appareils d'identifier et de traiter le trafic provenant de divers VLAN.

VLAN non balisés :
À l'inverse, les VLAN non balisés omettent des informations supplémentaires dans les trames Ethernet. Cette configuration trouve une application lors de la liaison de périphériques finaux, tels que des postes de travail ou des imprimantes, à un port de commutateur associé à un VLAN spécifique.

Liaison VLAN

L'agrégation VLAN apparaît comme un concept essentiel, en particulier dans les scénarios où plusieurs VLAN traversent la même liaison physique. Les liaisons réseau spécialisées sont configurées pour acheminer efficacement le trafic vers plusieurs VLAN, favorisant ainsi une communication efficace entre les commutateurs et les routeurs.

Présentation de la configuration

Configuration du routeur/pare-feu :
Les VLAN nécessitent une configuration sur le routeur/pare-feu pour faciliter la communication inter-VLAN. Chaque VLAN reçoit un sous-réseau IP attribué, accompagné de règles de routage établies régissant le flux de trafic entre les VLAN.

Configuration du commutateur :
Les ports de commutation liés aux périphériques au sein d'un VLAN peuvent être désignés comme étant balisés ou non. En revanche, les ports trunk sont configurés pour transporter des trames balisées pour plusieurs VLAN, améliorant ainsi la flexibilité et l'évolutivité du réseau.

Configuration de l'hyperviseur :
Dans le paysage de la virtualisation, les hyperviseurs doivent connaître les configurations VLAN, en particulier lorsqu'ils supervisent plusieurs machines virtuelles. Les interfaces réseau virtuelles sont allouées à des VLAN spécifiques, reflétant les principes de balisage observés dans les réseaux physiques.

En démêlant les complexités de la norme IEEE 802.1Q, en approfondissant les nuances entre les VLAN balisés et non balisés et en comprenant l'importance de la liaison VLAN, nous posons une base solide pour la création d'une infrastructure réseau bien organisée et sécurisée. Ces connaissances fondamentales préparent le terrain pour les étapes de configuration ultérieures de notre parcours complet de conception de réseau.

2.1.4. Routage

Dans notre exploration de la conception des réseaux, le routage occupe une place centrale, présentant deux stratégies distinctes : la méthode du « routeur sur une clé » et le routage de couche 3. De plus, nous adoptons une approche centrée sur le pare-feu, en orchestrant le flux de trafic entre les VLAN via des règles de pare-feu.

Routeur sur clé ou routage de couche 3

2.1.4.1. Routeur sur clé

Cette stratégie implique une seule interface physique sur un routeur, desservant plusieurs VLAN. Le routeur traite le trafic inter-VLAN et prend des décisions de routage basées sur les balises VLAN internes. Bien que pratique, cela peut introduire un goulot d'étranglement potentiel, car tout le trafic converge vers une seule liaison.

2.1.4.2. Routage de couche 3

Ici, les commutateurs de couche 3 gèrent le routage inter-VLAN. Chaque VLAN dispose d'une interface de couche 3 dédiée, favorisant le traitement parallèle du trafic. Cela minimise les goulots d'étranglement et améliore l'efficacité globale du réseau.

2.1.4.3. Approche centrée sur le pare-feu

Notre conception de réseau met l'accent sur une approche centrée sur le pare-feu. Les règles de pare-feu régissent méticuleusement le trafic entre les VLAN, garantissant que toutes les données traversent le pare-feu. Cela offre non seulement un contrôle granulaire sur les communications, mais améliore également la sécurité en examinant et en filtrant le trafic à la périphérie du réseau.

Dans les sections suivantes, nous approfondirons la configuration, illustrant comment ces stratégies de routage et ces principes centrés sur le pare-feu interagissent pour renforcer la structure et la posture de sécurité de notre réseau.

3. Construire une infrastructure réseau

Dans cette phase passionnante, nous retroussons nos manches et lançons la construction proprement dite de notre réseau.

Lancement de la construction du réseau

Nous sommes au point où la théorie se transforme en infrastructure tangible. Cela marque le début de l'assemblage des éléments qui formeront l'épine dorsale de notre réseau.

- 3.1. Téléchargement et installation de pfSense

  Notre première tâche implique le déploiement de pfSense, un logiciel open source robuste pour le routage et le pare-feu. Nous vous guiderons tout au long du processus de téléchargement et d'installation, garantissant une configuration transparente.

- 3.2. Configuration de base de pfSense et intégration VLAN

  Une fois pfSense en place, nous passons à la configuration de base. Cela inclut la configuration de pfSense avec les détails essentiels et l'intégration de réseaux locaux virtuels (VLAN).
  De plus, nous mettrons en œuvre des règles de pare-feu cruciales pour réguler le flux de trafic entre les VLAN, renforçant ainsi les mesures de sécurité.

- 3.3. Configuration du commutateur et déploiement du VLAN

  Maintenant, l'attention se tourne vers les interrupteurs. Nous allons nous plonger dans la configuration des VLAN sur les commutateurs, en les alignant sur notre structure de réseau prédéterminée. Cette étape cruciale garantit que la segmentation logique définie par les VLAN est étendue de manière transparente sur l'ensemble du réseau.

En progressant dans ces étapes, vous posez les bases d'un réseau résilient, sécurisé et bien organisé. Au fur et à mesure que chaque composant se met en place, la conception complexe conçue dans les chapitres théoriques prend une forme tangible. Préparez-vous à voir votre projet de réseau prendre vie !

3.1. Téléchargement et installation de pfSense

Nous allons télécharger et installer pfSense.

3.1.1. Configuration matérielle minimale requise

Lorsque vous réfléchissez à la question de la configuration matérielle minimale requise, soyez assuré que la distribution du pare-feu logiciel pfSense fonctionne efficacement avec un matériel modeste. Pour des détails précis, reportez-vous à la page dédiée : pfSense Minimum Requirements. Cependant, ce qui est vraiment crucial, c'est le guide de dimensionnement du matériel, fournissant des informations sur les prérequis matériels adaptés pour atteindre le débit souhaité.

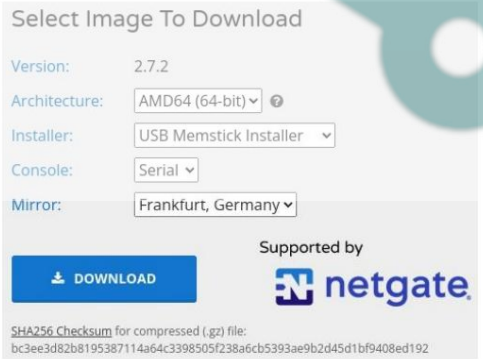
Tout au long de ce chapitre, nous utiliserons un PC Engines APU3 doté d'un processeur AMD GX-412TC et de 4 Go de RAM. Le stockage est un seul SSD M.2 de 250 Go. Bien qu'un SSD M.2 de 16 Go soit généralement utilisé, cet APU fonctionnait auparavant comme un nœud Linux exécutant Debian.

Il convient de noter que les cartes APU sont livrées sans connecteur vidéo, ce qui nécessite une interface via une connexion série. Cette caractéristique unique rend ce tableau idéal pour démontrer le processus d'installation.

3.1.2. Obtention de l'image d'installation de pfSense

Pour acquérir l'image d'installation de pfSense, visitez l'emplacement de téléchargement officiel : page de téléchargement de pfSense.

La page de téléchargement fournit une interface conviviale pour sélectionner et télécharger l'image appropriée. Choisissez les options souhaitées en fonction de l'architecture (AMD64 - 64 bits ; Netgate ADI), du type d'installateur (Installateur USB Memstick ; Installateur d'image DVD (ISO)), des préférences de console (Série ; VGA) et sélectionnez un miroir à télécharger.



Pour la carte système APU, il est recommandé d'opter pour le programme d'installation USB Memstick AMD64 (64 bits) configuré pour une console série. Cependant, si le matériel comporte une carte vidéo, l'option VGA est préférable pour une configuration plus conventionnelle.

3.1.3. Préparation du support d'installation

Avant de lancer le processus d'installation, s'assurer que votre support d'installation est prêt devient une étape cruciale.

3.1.3.1. Décompresser l'image Gzip

L'image d'installation de pfSense arrive compressée avec Gzip, et voici comment vous pouvez la décompresser en fonction de votre système d'exploitation.

Pour Linux ou Mac :

Utilisez la commande `gzip -d` ou `gunzip` dans le terminal.

```
gzip -d pfSense-CE-memstick-serial-2.7.2-RELEASE-amd64.img.gz
```

pfSense-CE-memstick-serial-2.7.2-RELEASE-amd64.img.gz Windows :
Pour les utilisateurs Windows, des outils comme 7-Zip sont idéaux car ils prennent en charge la compression GZip. Utilisez simplement 7-Zip pour décompresser l'image d'installation.

3.1.3.2. Écrire une image sur une clé USB

Une fois décompressée, vous devrez écrire l'image sur une clé USB pour l'installer sur le système cible. Cette étape cruciale garantit que votre support d'installation est prêt et prépare le terrain pour un processus d'installation fluide.

Écrivez l'image d'installation sur USB Memstick

3.1.3.2.1. Écrire une image avec Linux

Voici comment installer l'image sur une clé USB avec un ordinateur Linux.

1. Ouvrez un terminal (par exemple `xterm` ou `xfce4-terminal`)

2. Devenez root en exécutant « sudo su » ou « su -u » dans le terminal.

```
sudo su
```

3. Accédez au répertoire Téléchargements, créez un dossier (pfSense), déplacez l'image vers le dossier, cd dans le dossier

```
cd Downloads/
mkdir pfSense
mv pfSense-CE-memstick-serial-2.7.2-RELEASE-amd64.img.gz pfSense/.
cd pfSense/
```

4. Décompressez l'image

```
gzip -d pfSense-CE-memstick-serial-2.7.2-RELEASE-amd64.img.gz
```

Vérifiez le résultat avec la commande `ls` .

```
ls -lahsi
```

Ensuite, vous devez identifier le nom de périphérique correct pour votre clé USB, qui, dans cet exemple, est /dev/sdb.

```
fdisk -l
```

Le résultat ressemblera à quelque chose comme ce qui suit.

```
[..]
Disk /dev/sdb: 7,2 GiB, 7736072192 bytes, 15109516 sectors
Disk model: DataTraveler 3.0
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x90909090

Device Boot Start End Sectors Size Id Type
/dev/sdb1 1 66584 66584 32,5M ef EFI (FAT-12/16/32)
/dev/sdb2 * 66585 2047848 1981264 967,4M a5 FreeBSD
/dev/sdb3 2047849 2178920 131072 64M b W95 FAT32
```

Enfin, utilisez la commande `dd` pour écrire l'image sur la clé USB (remplacez "sdX" par le nom de votre appareil spécifique).

> Attention concernant la commande `dd` ! Soyez extrêmement prudent pour éviter de sélectionner par inadvertance le mauvais périphérique lors de l'écrasement. Cet incident pourrait entraîner une perte de données importante ou rendre votre ordinateur impossible à démarrer. Vérifiez et confirmez toujours le périphérique cible avant d'exécuter la commande `dd` . Votre diligence dans cette étape est cruciale pour éviter toute conséquence imprévue.

```
dd if=pfSense-CE-memstick-serial-2.7.2-RELEASE-amd64.img of=/dev/sdX status=progress ;sync
```

La commande `dd` peut prendre un certain temps, alors soyez patient. Une fois terminé, votre clé USB Memstick sera prête pour le processus d'installation de pfSense.

Le résultat ressemblera à quelque chose comme ce qui suit.

```
0735232 bytes (41 MB, 39 MiB) copied, 5 s, 8,1 MB/s
[..]
1112005120 bytes (1,1 GB, 1,0 GiB) copied, 257 s, 4,3 MB/s
2178921+0 records in
2178921+0 records out
1115607552 bytes (1,1 GB, 1,0 GiB) copied, 273,834 s, 4,1 MB/s
```

3.1.3.2.2. Écrire une image avec Windows

Le processus sur un ordinateur Windows diffère de celui sur un système Linux.

Imageur de disque Win32 est l'un des outils documentés dans Netgate Docs, et vous pouvez trouver une description détaillée de la procédure sous Écriture d'une image d'installation sur Flash Media. dans les documents Netgate.

3.1.3.3. Processus d'installation de pfSense

Passons maintenant au processus d'installation (car il est temps de démarrer et de devenir root) ! Allez-y et branchez la clé USB Memstick sur l'ordinateur qui est sur le point de prendre le relais. pare-feu. Avant d'allumer l'ordinateur, il est conseillé d'identifier la touche sur laquelle appuyer pour accéder au menu de démarrage. Cette étape est cruciale pour pouvoir démarrer depuis la clé USB Memstick.

Dans le cas de l'APU, dépourvu de connexion vidéo, il doit être exploité via une connexion de console série. Sous Linux, la commande screen peut être utilisée. Vous pouvez également utiliser PuTTY, disponible sur différentes plateformes. Par souci de simplicité, nous utiliserons PuTTY pour vous guider tout au long du processus. Cette approche fonctionne de la même manière, que vous ayez ou non une carte vidéo, avec juste quelques nuances dans l'affichage.

> L'installation de la console série a été choisie à dessein dans l'espoir de supprimer les barrières pour ce type d'installation. En démontrant la procédure, vous remarquerez qu'il ne s'agit pas compliqué. L'inconvénient est qu'un câble série approprié est nécessaire. PC Engines propose une solution simple pour cela sous la forme d'un câble USB vers DB9F . PC Engines fournit même un schéma [PDF] et pilotes.

L'ordinateur portable choisi pour cette démonstration n'a pas de port série. Présentons un adaptateur USB vers série Tripp Lite Keyspan (USA-19H). Cet adaptateur pratique comble le fossé, permettant un connexion série pour notre processus d'installation. Maintenant, ajoutons ce super-héros technologique au mélange et procédons à la magie de l'installation !

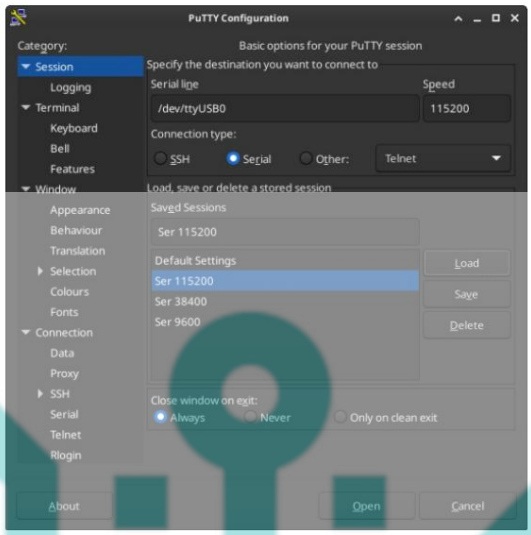
Pour vous connecter à l'APU à l'aide de la commande « screen » sous Linux, vous devez exécuter « screen /dev/ttyUSB0 115200 ». Cependant, pour cette démonstration, nous opterons pour PuTTY.

L'importance de `/dev/ttyUSB0` réside dans le fait qu'il s'agit du nom du périphérique sur l'ordinateur portable Linux. Sous Windows, vous pouvez accéder à Gestion des périphériques pour localiser le périphérique série. Au lieu de `/dev/ttyUSB0`, le nom du périphérique peut apparaître comme quelque chose comme `COM3 :`. Dans les deux cas, l'établissement d'une connexion à l'APU est vital.

A côté du port, connaître la vitesse est crucial. La vitesse, dans ce cas, est fixée à 115 200 bauds. Intégrons ces composants de manière transparente dans notre parcours d'installation !

1. Ouvrez un terminal.
2. Devenez root (`sudo su` ou `su -`)
3. Connectez l'adaptateur série USB à l'ordinateur et à l'APU.
4. Branchez la clé USB.
5. Démarrez PuTTY

6. Définissez le type de connexion sur série, mettez le nom de l'appareil dans la zone de texte Ligne série et enfin réglez la vitesse sur 115200.



7. Cliquez sur le bouton [Ouvrir].
8. Allumez l'APU en branchant le câble d'alimentation.
9. Appuyez sur <F10> pendant le démarrage (spamez simplement la touche <F10> jusqu'à ce que le menu de démarrage apparaisse)
10. Sélectionnez le périphérique de démarrage (entrez le numéro correspondant)

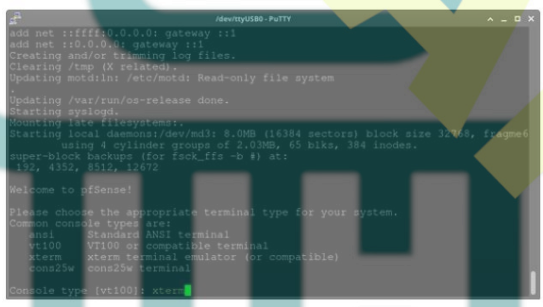
Ce qui suit représente le menu de démarrage. La première option est la clé USB. La deuxième option est le SSD M.2 SATA de 250 Go.

```
SeaBIOS (version rel-1.16.0.1-0-g77603a32)

Press F10 key now for boot menu

Select boot device:

1. USB MSC Drive Kingston DataTraveler 3.0
2. AHCI/0: Samsung SSD 850 EVO mSATA 250GB ATA-9 Hard-Disk (232 GiBytes)
3. Payload [setup]
4. Payload [memtest]
```

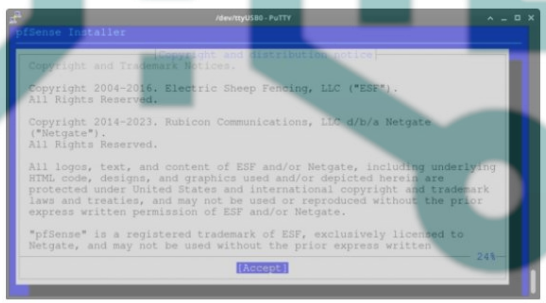
Si votre matériel comprend une carte vidéo, l'option VGA est plus pratique. Branchez simplement la clé USB Memstick, allumez l'ordinateur et commencez à spammer la clé de démarrage. Le reste du processus est similaire, avec seulement quelques nuances dans l'affichage.

pfSense démarrera automatiquement.

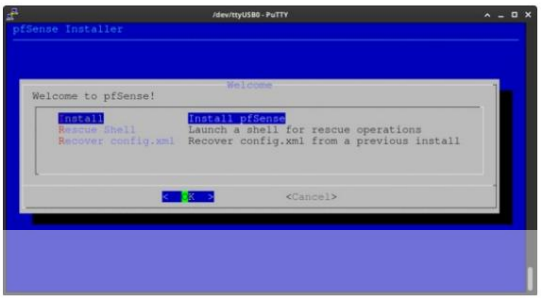
Sélectionnez le type de console. Tapez "xterm" et appuyez sur Entrée pour continuer.



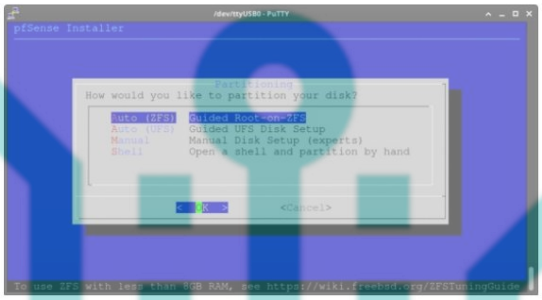
Passez à l'étape suivante en acceptant l'avis de droit d'auteur et de distribution. Appuyez sur Entrée pour continuer.



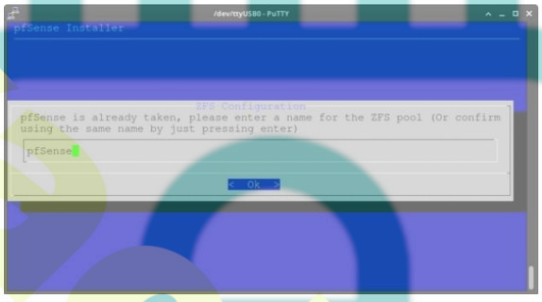
Appuyez sur Entrée sur l'écran de bienvenue pour lancer le processus d'installation.



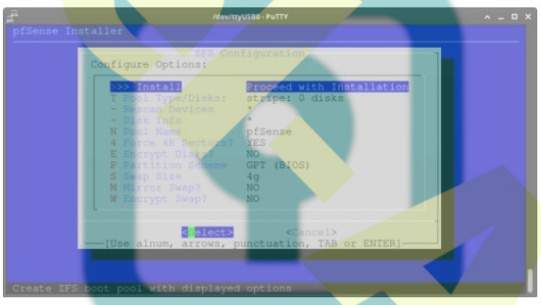
Appuyez sur la touche Entrée pour choisir Auto (ZFS). Si vous utilisez eMMC (ou une option similaire), sélectionnez Auto (UFS).



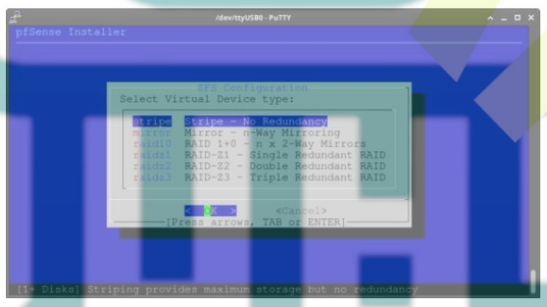
Appuyez simplement sur Entrée pour continuer. Le programme d'installation repartitionnera et écrasera automatiquement le SSD M.2.



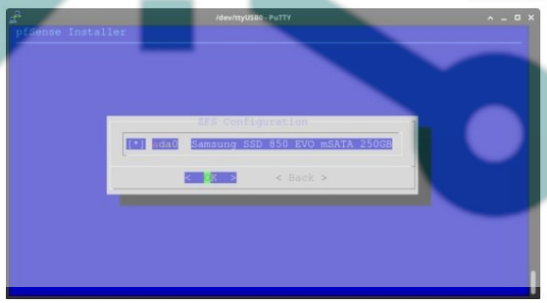
Appuyez sur Entrée pour continuer. Remarque : envisagez d'augmenter la taille du swap pour remédier à un épuisement potentiel de la RAM.



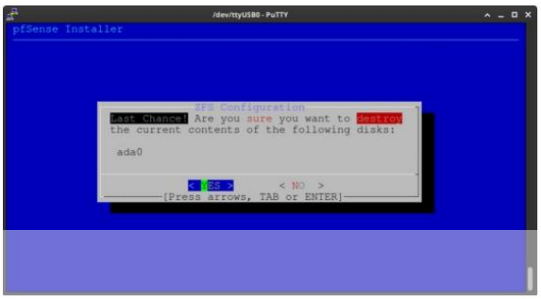
Vous ne remarquerez qu'un seul appareil. Appuyez simplement sur Entrée pour confirmer l'option "Pas de redondance".



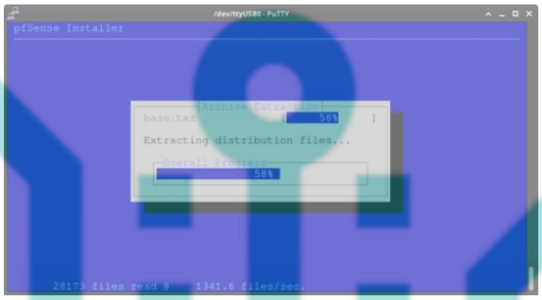
Appuyez sur la barre d'espace pour sélectionner l'appareil. Appuyez ensuite sur Entrée pour continuer.



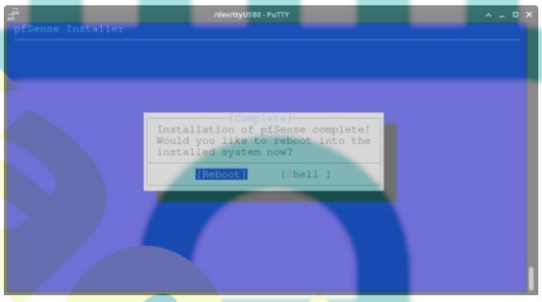
Appuyez sur la touche TAB pour sélectionner "OUI". Appuyez ensuite sur la touche Entrée pour continuer.



Le programme d'installation continuera. Veuillez patienter.



Appuyez sur Entrée pour redémarrer.



N'hésitez pas à retirer la clé USB Memstick une fois que vous avez repéré la ligne "Tous les tampons synchronisés".

Toutes nos félicitations! pfSense démarre avec succès à partir du stockage interne. Nous sommes maintenant sur le point de configurer pfSense selon la conception de notre réseau.

Lors du démarrage initial, vous serez peut-être invité à configurer les VLAN ainsi que les interfaces WAN et LAN.

pfSense affichera les informations suivantes via la console :

- Default interfaces not found --- Running interface assignment option.
  [..]
- Valid interfaces are:
  [..]
- Do VLANs need to be set up first?
  If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the WebConfigurator to configure VLANs later, if required.
  [..]
- Shoud VLANs be setup now [y|n]?

  *Just type **n** and press Enter.*

- [..]
  Enter the WAN interface name or 'a' for auto-detction.

  Just enter the name of the desired interface for WAN and press ENTER.

- Enter the LAN interface name or 'a' for auto-detction.

  Just enter the name of the desired interface for WAN and press ENTER.

- If there are more interfaces, you will be asked to set the Optional 1 interface.
  Just press Enter to skip, if this is the case.

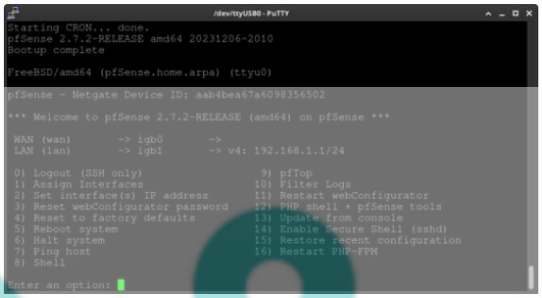
- The interfaces will be assigend as follows:

[..]

Voulez-vous continuer [o|n] ?

Tapez y et appuyez sur Entrée.

Le résultat final devrait ressembler à la capture d'écran suivante.



3.2. Configuration de pfSense

Maintenant que pfSense est installé avec succès, nous pouvons passer à la configuration du routeur/pare-feu à l'aide du webConfigurator. Le webConfigurator est accessible sur le port 443 et est accessible via l'adresse IPv4 par défaut du pare-feu, qui est 192.168.1.1.

Remarque : différentes terminologies sont utilisées de manière interchangeable pour le webConfigurator, telles que "WUI", "WebUI", "WebGUI" ou simplement "Web Interface".

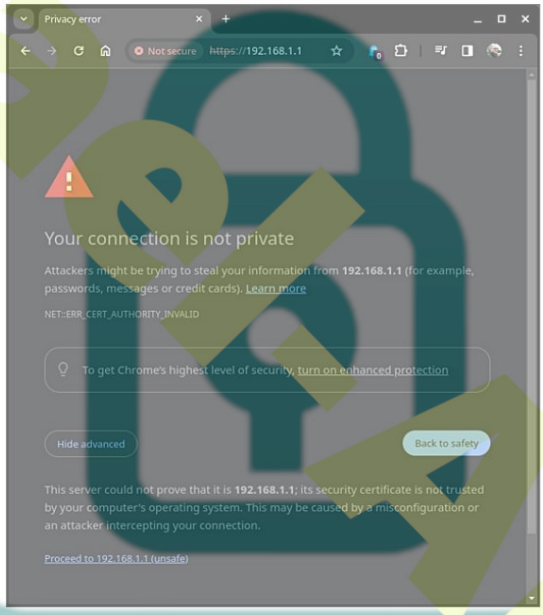
3.2.1. Interface Web

Assurez-vous que votre ordinateur est connecté au port LAN du pare-feu, généralement identifié comme la deuxième interface réseau. Si tout va bien, une adresse IPv4 sera attribuée à votre ordinateur. Maintenant, ouvrez un navigateur Web et accédez à https://192.168.1.1 pour ouvrir l'interface Web.

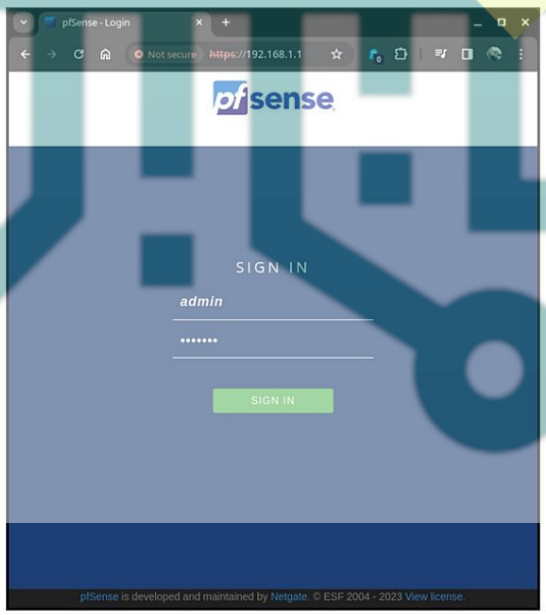
3.2.1.1. Assistant de configuration pfSense

L'écran initial peut sembler un peu prudent, mais ne vous inquiétez pas, considérez-le simplement comme un rappel amical. Puisqu'un certificat auto-signé est utilisé, cliquez sur Avancé , puis sélectionnez en toute confiance Passer à 192.168.1.1 (dangereux) pour continuer.

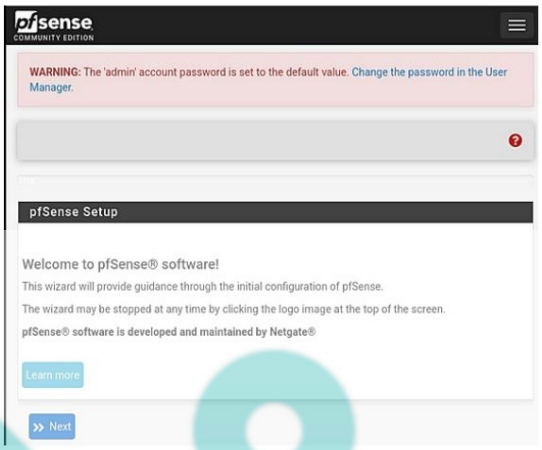
Pour les utilisateurs de Firefox, le processus est tout aussi fluide. Cliquez simplement sur Avancé..., puis optez pour « Accepter le risque et continuer » pour procéder en toute confiance.



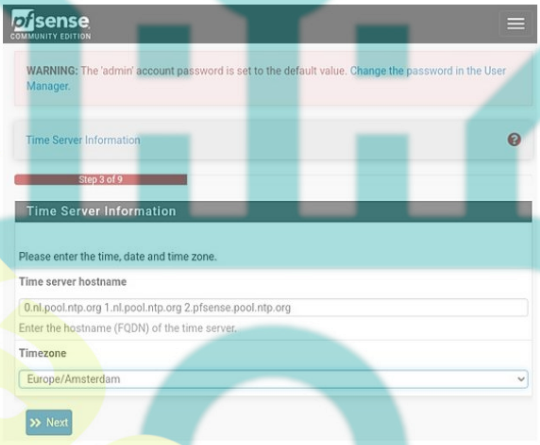
Il est maintenant temps de vous connecter. Entrez « admin » pour le nom d'utilisateur et « pfsense » pour le mot de passe. Ensuite, cliquez sur « Connexion » pour accéder au WebUI.



Vous pouvez ignorer en toute sécurité le message d'avertissement concernant le mot de passe pour le moment. Continuez en cliquant sur "Suivant" pour continuer avec l'assistant de configuration pfSense.

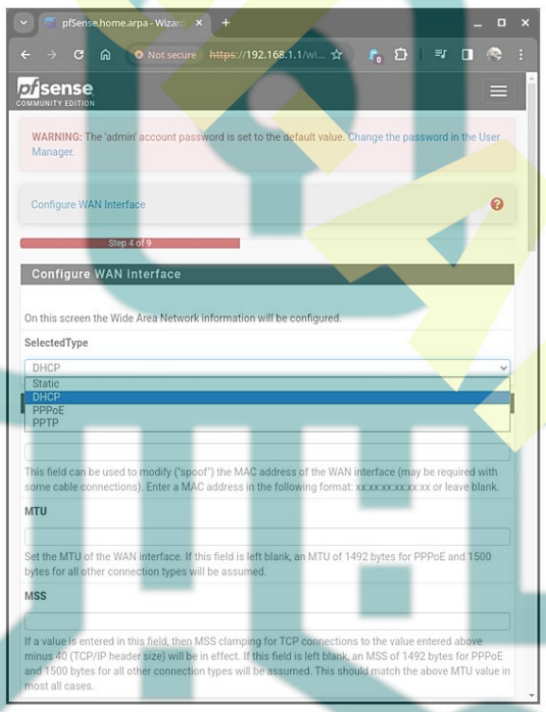


Il est crucial de garantir des paramètres précis de l'heure et de la date. Vous pouvez soit accepter la source de temps par défaut, soit en ajouter d'autres si nécessaire. Ensuite, procédez à la définition du fuseau horaire et cliquez sur « Suivant ».

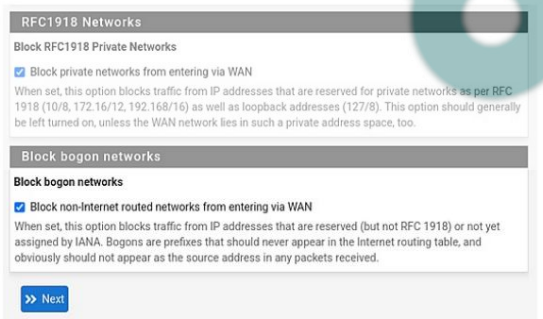


Le prochain sur notre liste est la configuration de l'interface WAN. Vous devrez choisir parmi des options telles que Statique, DHCP, PPPoE et PPTP, en fonction de votre connexion Internet ou du réseau auquel le le pare-feu est connecté. Sélectionnez l'option appropriée en conséquence, cliquez sur "Suivant" une fois définie.

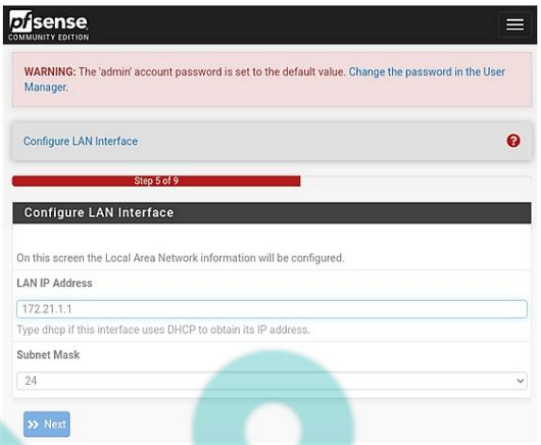
Dans cet exemple, nous sélectionnerons l'option DHCP, connectant le pare-feu au réseau du laboratoire via l'un des ports du commutateur. Le réseau du laboratoire, à son tour, est lié à un autre pare-feu qui se connecte au Internet.



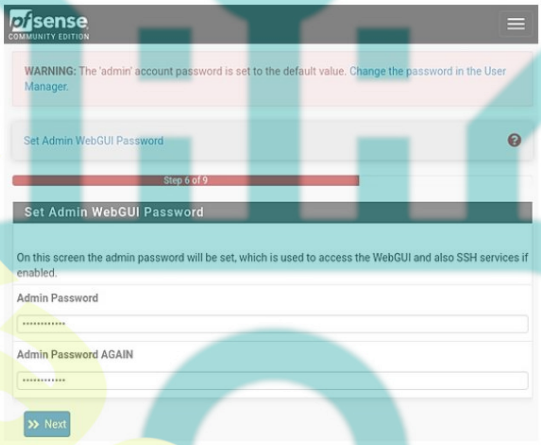
Ensuite, nous devons décider comment gérer les réseaux et les bogons RFC1918. Pour maintenir la sécurité, il est conseillé de garder les deux options cochées, en garantissant que le trafic de ces réseaux soit bloqué. Cependant, si l'interface WAN est connectée à un réseau RFC1918, vous pouvez envisager de décocher la première case. Une fois votre sélection effectuée, cliquez sur « Suivant » pour continuer.



Nous entrerons la passerelle par défaut IPv4 "172.21.1.1" de notre VLAN de gestion principal, en configurant l'interface LAN. Définissez le masque de sous-réseau sur 24, puis cliquez sur « Suivant » pour continuer.

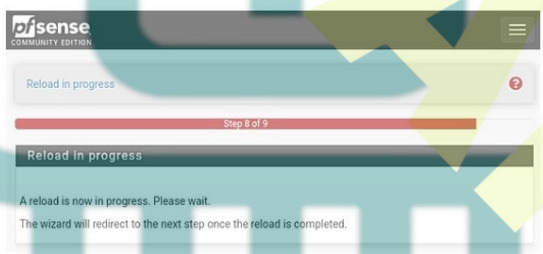


Il nous sera demandé de définir le mot de passe pour l'interface Web. Suivez simplement les instructions à l'écran.

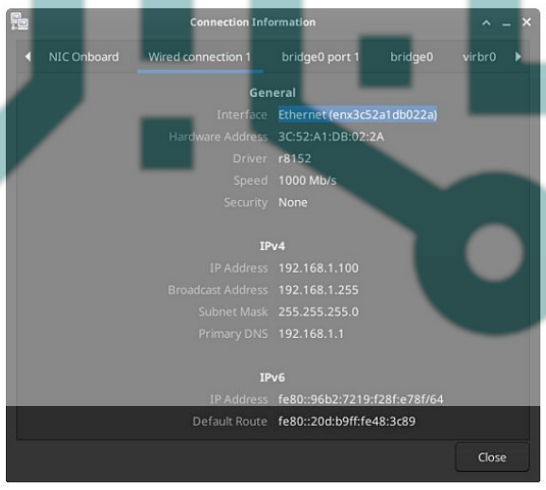


Nous sommes presque à la fin de l'assistant de configuration de pfSense. Cliquez simplement sur « Recharger » pour appliquer les nouvelles modifications et recharger pfSense.

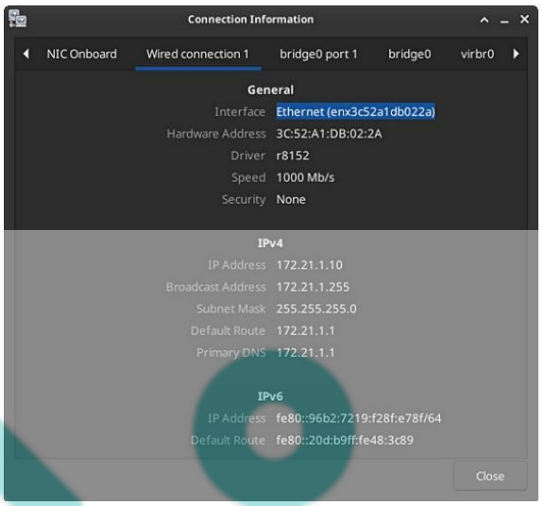
Une fois le rechargement terminé, l'assistant devrait automatiquement rediriger. Cependant, dans certains cas, cette redirection peut ne pas fonctionner comme prévu.



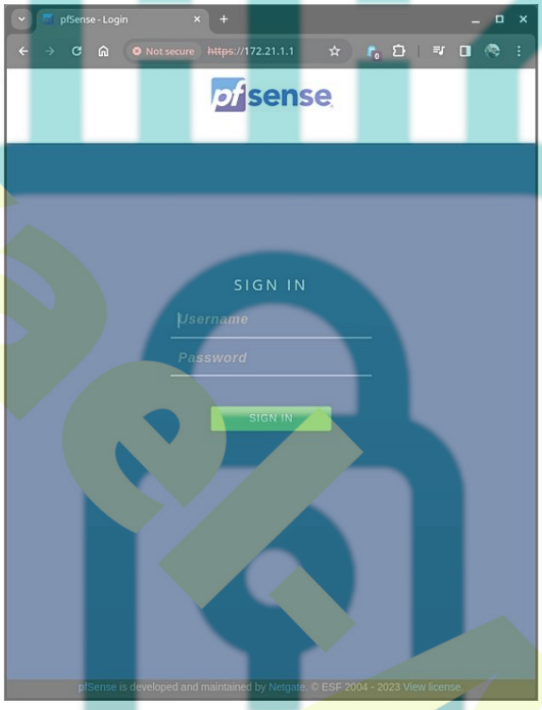
En y regardant de plus près, il apparaît que l'adresse IPv4 de la carte réseau n'est pas renouvelée. Ce problème est attribué à NetworkManager sur l'ordinateur portable Linux utilisé, plutôt qu'à un problème avec pfSense.



Après avoir débranché le câble réseau, attendu quelques secondes et l'avoir rebranché sur l'ordinateur portable, l'adresse IPv4 semble avoir été renouvelée avec succès.

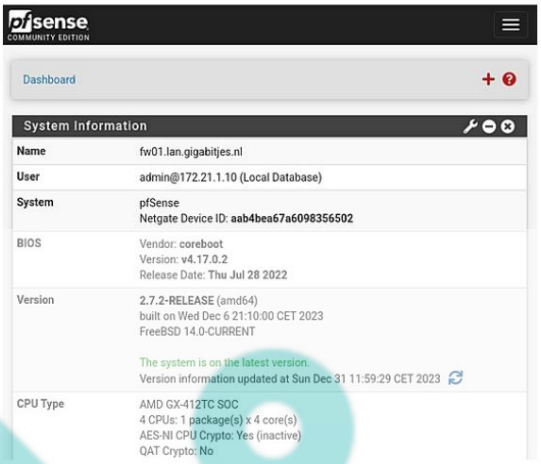


Après avoir saisi l'URL correcte « https://172.21.1.1 » dans la barre d'adresse du navigateur, appuyez sur la touche Entrée. Saisissez ensuite le nom d'utilisateur « admin » et le mot de passe précédemment défini. Enfin, cliquez sur « Connexion » pour accéder à la WebUI.



Une fois connecté, vous serez accueilli avec une certaine génialité que vous devrez simplement accepter. Cliquez sur « Accepter » puis continuez en cliquant sur « Fermer ».

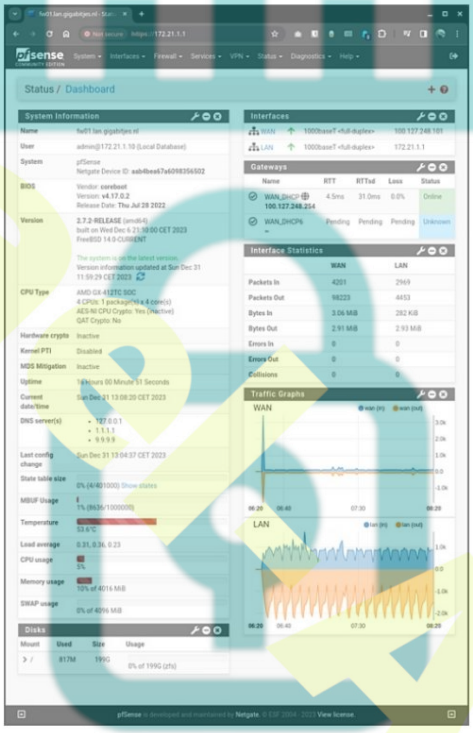
Toutes nos félicitations! L'assistant de configuration pfSense se termine ici. Nous procéderons à quelques personnalisations.



3.2.1.2. personnalisations

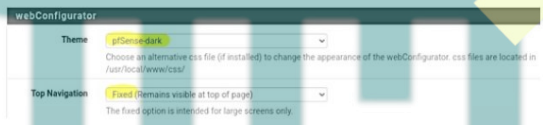
Tableau de bord

Le tableau de bord de pfSense est fonctionnel mais peut être amélioré par l'ajout de divers widgets. Si vous préférez, vous pouvez supprimer le widget Services et support en cliquant sur le "X" dans le coin supérieur droit.
Pensez à ajouter des widgets utiles tels que "Passerelles", "Statistiques d'interface" et "Graphiques de trafic" pour enrichir votre tableau de bord. Bien qu'il existe d'autres widgets bénéfiques, nous laisserons à l'administrateur le soin d'explorer et de choisir ceux qui correspondent à ses préférences.



Thème et navigation supérieure

Certains préféreront peut-être utiliser un thème en mode sombre. Le thème peut être sélectionné via l'option de menu "Système" > "Configuration générale". Faites défiler jusqu'à "webConfigurator" et sélectionnez le thème souhaité en en faisant défiler les options disponibles. Choisir "pfSense-dark" entraînera un arrière-plan sombre.



De plus, faites attention à l'option "Top Navigation". Opter pour "Fixe" garantit que le menu de navigation reste à tout moment en haut de la page. Faites défiler vers le bas et cliquez sur "Enregistrer" pour stocker et appliquer les modifications.

Pour actualiser le tableau de bord et apprécier l'apparence améliorée, cliquez simplement sur le logo pfSense situé dans le coin supérieur gauche. Profitez de l'interface mise à jour !

Explorez de nombreuses options de personnalisation dans pfSense webConfigurator pour une expérience personnalisée. Pensez à améliorer l'esthétique en ajoutant une jolie image à l'aide des widgets Image. Peut-être faudrait-il garder la créativité pour plus tard, car il y a du travail à faire.

Prenez un moment pour explorer les options du menu ; c'est une étape précieuse pour se familiariser avec la navigation. Comprendre le menu s'avérera utile à mesure que nous approfondirons d'autres configurations.

Passons à la section suivante sur les VLAN et les sous-réseaux.

3.2.2. Définir des VLAN et des sous-réseaux

Vous vous souvenez de la conception de notre réseau ? Nous avons inclus une colonne supplémentaire pour la passerelle par défaut.

Dans notre conception de réseau, chaque réseau possède sa propre passerelle par défaut désignée. La passerelle par défaut sert de point central pour la sortie et l'entrée du trafic réseau, garantissant ainsi une communication entre différents réseaux. Cette configuration individualisée améliore l'organisation et les fonctionnalités du réseau.

VLAN	Description	Subnet	Gateway	Explanation (by example)
0001	Management 1	172.21.1.0/24	172.21.1.1	Switches, access points
0002	Management 2	172.22.2.0/24	172.22.2.1	Hypervisor(s), KVM-over-IP (eg iLO, IPMI)
0016	Servers	10.10.16.0/24	10.10.16.1	Server VMs
0018	Storage	10.10.18.0/24	10.10.18.1	Network Attached Storage (NAS)
0032	Office LAN	10.10.32.0/24	10.10.32.1	Workstations (desktop and laptop computers)

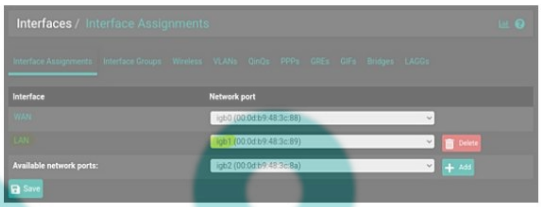
0036	Peripherals	10.10.36.0/24	10.10.36.1	Printers
0251	IoT	172.31.251.0/24	172.31.251.1	Solar panel inverters
0252	DMZ	172.31.252.0/24	172.31.252.1	Web and mail server
0253	GuestNET	172.31.253.0/24	172.31.253.1	Guest Wi-Fi network

Nous utiliserons notre conception de réseau pour ajouter les VLAN et les sous-réseaux.

3.2.2.1. Interfaces

Commençons par sélectionner l'interface de nos VLAN. Accédez à « Interfaces » > « Affectation » pour afficher les interfaces disponibles.

L'interface LAN est actuellement associée à igb1. Par conséquent, nous utiliserons igb1 pour configurer nos VLAN.



3.2.2.2. VLAN

Sélectionnez « VLAN » sous « Interfaces » > « Assignment », puis cliquez sur « Ajouter » pour configurer le VLAN.

Choisissez l'interface parent appropriée, qui dans ce cas est "igb1". Entrez la balise VLAN comme « 2 » et laissez la priorité VLAN non définie.

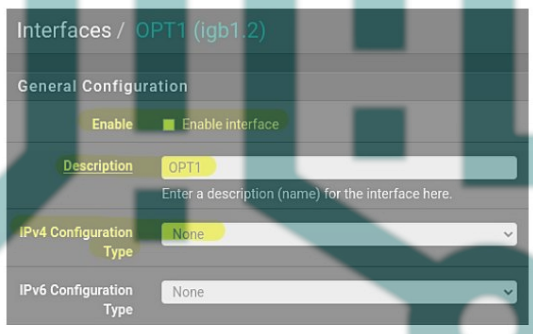
Portez une attention particulière au champ Description, où il est recommandé d'utiliser un format clair. Par exemple, vous pouvez utiliser « L1_0002_MNG2 », où « L1 » désigne « LAN 1 », « 0002 » signifie le VLAN et « MNG2 » représente « Management LAN 2 ». Cette approche structurée facilite la reconnaissance et la gestion du réseau.

Cliquez enfin sur "Enregistrer" pour enregistrer les modifications.

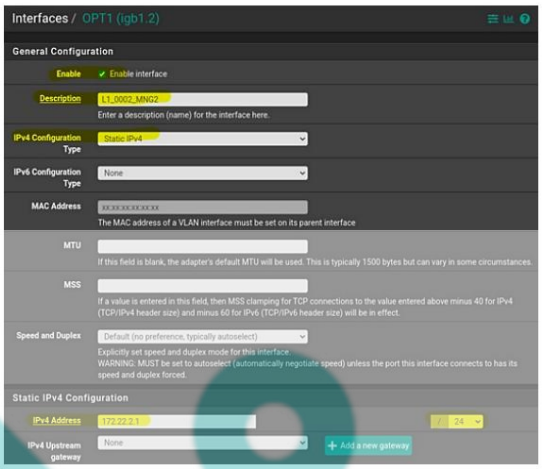
Accédez à « Affectations d'interface » sous « Interface » > « Affectations » pour attribuer le nouveau VLAN à une interface. Dans la section « Ports réseau disponibles », sélectionnez le VLAN et cliquez sur « Ajouter ». Ensuite, enregistrez et appliquez les paramètres.

Activez l'interface en cochant la case. Portez une attention particulière au champ Description, où il est recommandé d'utiliser un format clair. Par exemple, vous pouvez utiliser "L1_0002_MNG2"

Une fois les options de configuration visibles, procédez aux étapes suivantes.



1. Activez l'interface en cochant la case.
2. Portez une attention particulière au champ Description, où il est recommandé d'utiliser un format clair. Par exemple, vous pouvez utiliser "L1_0002_MNG2".
3. Sélectionnez « IPv4 statique » comme « Type de configuration IPv4 ».
4. Entrez la passerelle IPv4 par défaut sous la forme « 172.22.2.1 » dans le champ de texte à côté de l'étiquette Adresse IPv4.
5. Choisissez « 24 » à droite de l'adresse IPv4 ; cela représente le masque de sous-réseau au format CIDR.
6. Enfin, faites défiler vers le bas, puis enregistrez et appliquez les modifications.



Le résultat ressemblera à ceci.

Il est recommandé de renommer également les interfaces LAN et WAN.

Cliquez simplement sur "LAN" et modifiez la description de l'interface en "L1_0001_MNG1".
Ensuite, faites quelque chose de similaire à l'interface WAN en modifiant la description en "W1_0001_ISP1".
Cela fournira un aperçu cohérent.

N'oubliez pas de sauvegarder et d'appliquer chaque modification.

Voici un résumé du processus de création de VLAN et d'interfaces :

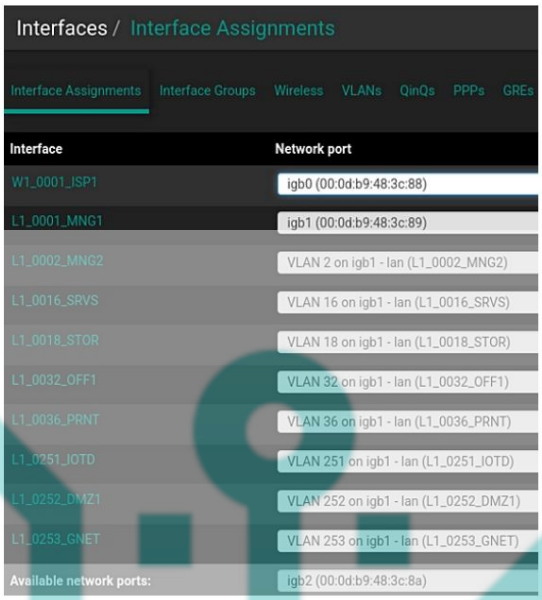
1. Créez le VLAN :
   - Accédez à « Interfaces » > « Affectations ».
   - Cliquez sur l'onglet "VLAN".
   - Cliquez sur "Ajouter" pour définir un nouveau VLAN.
   - Sélectionnez l'interface parent (par exemple, igb1), entrez la balise VLAN et fournissez une description claire.
2. Exprimez le VLAN dans une interface :
   - Allez dans « Interfaces » > « Affectations ».
   - Cliquez sur "Affectations d'interface".
   - Choisissez le VLAN dans la liste "Ports réseau disponibles" et cliquez sur "Ajouter".
   - Enregistrez et appliquez les paramètres.
3. Configurez les options d'interface :
   - Dans la section "Interfaces", une nouvelle interface (par exemple OPT2) apparaîtra.
   - Cliquez sur l'interface (par exemple, OPT2).
   - Activez l'interface en cochant la case.
   - Définissez une description claire, telle que "L1_00016_SRVS. pour les serveurs"
   - Choisissez « IPv4 statique » comme « Type de configuration IPv4 ».
   - Saisissez l'adresse IPv4 de la passerelle par défaut (par exemple, 10.10.16.1).
   - Choisissez le masque de sous-réseau au format CIDR (par exemple /24).
   - Faites défiler vers le bas, puis enregistrez et appliquez les modifications.
4. Répétez l'opération pour les autres VLAN et interfaces :
   - Répétez l'ensemble du processus pour chaque VLAN et interface correspondante.
   - Soyez cohérent en fournissant des descriptions claires pour une meilleure organisation.

En suivant ces étapes, vous pouvez systématiquement créer des VLAN, les exprimer dans des interfaces et configurer les paramètres nécessaires. Si vous disposez de VLAN ou d'interfaces spécifiques dont vous souhaitez des informations détaillées mode d'emploi, n'hésitez pas à préciser !

La présentation du VLAN ressemblera au tableau suivant.

Balise VLAN	d'interface	Priorité		Description
igb1 (lan)		2	-	L1_0002_MNG2
igb1 (lan)		16	-	L1_0016_SRVS
igb1 (lan)		18	-	L1_0018_STOR
igb1 (lan)		32	-	L1_0032_OFF1
igb1 (lan)		36	-	L1_0036_PRNT
igb1 (lan)		251	-	L1_0251_IOTD
igb1 (lan)		252	-	L1_0252_DMZ1
igb1 (lan)		253	-	L1_0253_GNET

L'affectation de l'interface ressemblera à la capture d'écran suivante.



Le widget du tableau de bord « Interfaces » résume un aperçu similaire au tableau suivant.

Interface	Speed / Duplex	Default Gateway
W1_0001_ISP1	1000baseT <full-duplex>	100.127.248.101
L1_0001_MNG1	1000baseT <full-duplex>	172.21.1.1
L1_0002_MNG2	1000baseT <full-duplex>	172.22.2.1
L1_0016_SRVS	1000baseT <full-duplex>	10.10.16.1
L1_0018_STOR	1000baseT <full-duplex>	10.10.18.1
L1_0032_OFF1	1000baseT <full-duplex>	10.10.32.1
L1_0036_PRNT	1000baseT <full-duplex>	10.10.36.1
L1_0251_IOTD	1000baseT <full-duplex>	172.31.251.1
L1_0252_DMZ1	1000baseT <full-duplex>	172.31.252.1
L1_0253_GNET	1000baseT <full-duplex>	172.31.253.1

Nous continuerons notre configuration de pfSense dans la section suivante.

3.3 Configuration du pare-feu dans pfSense

Dans pfSense, la politique de pare-feu par défaut pour les interfaces consiste à refuser par défaut tout le trafic entrant. Cela signifie qu'à moins que des règles de pare-feu spécifiques ne soient configurées pour autoriser le trafic, tous les les connexions aux interfaces seront bloquées.

Lorsque vous créez des règles de pare-feu, vous spécifiez essentiellement quel trafic est autorisé ou refusé pour une interface particulière. Les règles sont traitées dans l'ordre, de haut en bas, et les la première règle qui correspond aux critères de trafic est appliquée. Si aucune règle ne correspond, la règle de refus par défaut à la fin de l'ensemble de règles est appliquée.

Il est important de configurer les règles de pare-feu de manière appropriée en fonction des exigences de votre réseau pour garantir que le trafic circule comme prévu et que votre réseau reste sécurisé.

3.3.1. Règles de pare-feu par défaut

Établissons un ensemble standard de règles de pare-feu qui peuvent être appliquées universellement sur toutes les interfaces. Certains types de trafic sont intrinsèquement autorisés, et notre objectif est de créer des règles de pare-feu efficaces. Pour y parvenir, nous commencerons par définir les IP et les alias de port. Cette approche stratégique améliore la clarté et l'optimisation de la configuration de nos règles de pare-feu.

3.3.1.1. Alias IP

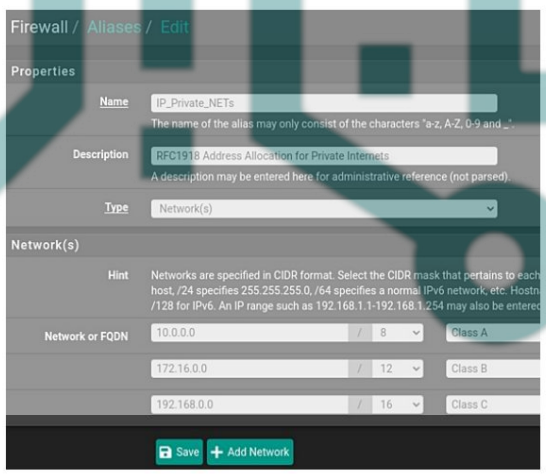
Nous allons créer l'alias IPv4 suivant :

- **Name: IP_Private_NETs**
  Description: RFC1918 Address Allocation for Private Internets
- Type: Networks
- Network or FQDN: 10.0.0.0 /8
  Descripton: Class A
- Network or FQDN: 172.16.0.0 /12
  Description: Class B
- Network or FQDN: 192.168.0.0 /16
  Description: Class C

Accédez d'abord à "Pare-feu" > "Alias" et cliquez ensuite sur "Ajouter" (dans l'onglet "IP").

Remplissez les détails. Pour ajouter plusieurs réseaux, cliquez sur "Ajouter un réseau". Cela ajoutera une nouvelle ligne.

Enregistrez et appliquez les modifications. Le résultat final ressemblera à la capture d'écran suivante.



3.3.1.2. Alias de ports

Nous allons créer les alias de ports suivants :

- **Name: Port_Core_Services_TCP**
- Description: Core Services, TCP
- Type: Port(s)
- Port: 53

Description: DNS over TCP

- **Name: Ports_Core_Services_UDP**
- Description: Core Services, TCP
- Type: Port(s)
- Port: 53
  Description: DNS over UDP
- Port: 123
  Description: NTP

Accédez d'abord à "Pare-feu" > "Alias" et cliquez ensuite sur "Ajouter", dans l'onglet "Ports".

Remplissez les détails. Pour ajouter plusieurs ports, cliquez sur « Ajouter un port ». Cela ajoutera une nouvelle ligne.

Enregistrez et appliquez les modifications.

Le résultat final ressemblera aux captures d'écran suivantes.

3.3.1.3. Ajouter des règles de pare-feu (flottant)

Les règles de pare-feu peuvent être implémentées sur une interface spécifique ou sous forme de règles flottantes. Le premier s'applique au trafic entrant sur l'interface désignée (appelée « entrant » ou entrant dans la documentation pfSense), tandis que le second peut être appliqué sur n'importe quelle interface. Il est essentiel de reconnaître que les règles flottantes ont priorité sur les règles d'interface classiques. De plus, il convient de noter que
les règles flottantes sont polyvalentes et ne se limitent pas au trafic entrant uniquement ; ils peuvent également être configurés pour le trafic sortant en sélectionnant « sortie » ou pour le trafic bidirectionnel en choisissant « n'importe lequel ».

Soyez prudent lorsque vous travaillez avec des règles flottantes, car leur comportement peut ne pas être immédiatement intuitif pour tout le monde.

Établissons une règle flottante pour ICMP. Il s'agit de permettre gracieusement aux hôtes d'échanger des pings entre les VLAN – à moins, bien sûr, qu'il s'agisse d'une entité mystérieuse qui frappe à la porte du réseau. Pas d'entrée pour les grands méchants hackers !

Accédez d'abord à « Pare-feu » > « Règles ». Cliquez ensuite sur "Flottant". Nous pouvons maintenant créer la règle en cliquant sur "Ajouter". Ne vous inquiétez pas de la flèche vers le haut ou vers le bas. C'est la première règle. S'il y a plus
règles, celles-ci peuvent être déplacées en faisant glisser les règles spécifiques de haut en bas.

Nous allons construire la règle suivante :

- Action: Pass
- Quick: check the tickbox
- Interface: select all the local interfaces
  These are all the interfaces **excluding** "Any" and the WAN
  Use the SHIFT to define a range of interfaces.
  Use the CTRL to select or deselect individual interfaces.
- Direction: in
  We will look at traffic which enters the interface.
- Address Family: IPv4
- Protocol: ICMP
- ICMP Subtypes: select both "Echo request" and "Traceroute" using CTRL.
- Source: Address Alias; IP_Private_NETs
- Destination: Address Alias; IP_Private_NETs
- Description: Allow ICMP across VLANs (Private NETs)

Enregistrez et appliquez les modifications.

Cela devrait aboutir à la règle flottante suivante.

Maintenant, étant donné la nature spécialisée des règles flottantes et étant donné que de nombreuses configurations de pare-feu peuvent ne pas en nécessiter, nous allons procéder avec des règles d'interface normales. Si vous trouvez des règles flottantes intriguant, vous pouvez explorer plus de détails dans la documentation : Documentation sur les règles flottantes.

3.3.1.4. Ajouter des règles de pare-feu (interface)

Vous souvenez-vous de nos alias IP et de port ? Nous les intégrons désormais dans nos règles d'interface. Bien que nous puissions créer des règles flottantes, nous avons opté pour des règles d'interface afin de conserver une configuration plus simple, même si cette
approche nécessite un peu plus d'efforts. L'avantage réside toutefois dans la possibilité de dupliquer facilement les règles de pare-feu entre les interfaces, compensant ainsi la charge de travail supplémentaire.

Naviguons vers « Pare-feu » > « Règles ». Pour l'instant, nous allons laisser les interfaces de gestion intactes et commencer par "L1_0032_OFF1". Cette approche s'aligne sur le point de vue de l'utilisateur, en se concentrant sur règles spécifiques au LAN Office.

Commencez par cliquer sur « Ajouter » (soit sur le bouton avec la flèche vers le haut, soit vers le bas).

Rule 1:

- Action: Pass
- Interface: L1_0032_OFF1
- Address Family: IPv4
- Protocol: TCP
- Source: L1_0032_OFF1 subnets
- Destination: This Firewall (self)
- Destination Port Range: (other); Port_Core_Services_TCP
- Description: Allow Core Services TCP

Please Save and Apply the changes.

Now, click the "Add" button with the arrow pointing downwards.

Rule 2:

- Action: Pass
- Interface: L1_0032_OFF1
- Address Family: IPv4
- Protocol: UDP
- Source: L1_0032_OFF1 subnets
- Destination: This Firewall (self)
- Destination Port Range: (other); Port_Core_Services_UDP
- Description: Allow Core Services UDP

Veuillez enregistrer et appliquer les modifications.

Ces deux règles autorisent le trafic TCP et UDP spécifique depuis le réseau local du bureau une fois qu'il circule dans l'interface. La destination est le pare-feu lui-même, servant de serveur DNS et NTP.

Vous remarquerez peut-être l'absence de règle pour DHCP et le trafic sortant. Aucune règle n'est nécessaire pour le trafic DHCP, car pfSense le gère par défaut. Nous n'avons besoin de créer une règle sortante que si nous voulons pour autoriser le trafic depuis l'interface vers Internet.

Rule 3:

- Action: Reject
- Interface: L1_0032_OFF1
- Address Family: IPv4
- Protocol: Any
- Source: Address or Alias; IP_Private_NETs
- Destination:
  - Select "Address or Alias"
  - Destination Address: IP_Private_NETs
- Description: Prevent Leakage

Maintenant, cliquez sur le bouton "Ajouter" avec la flèche pointant vers le bas.

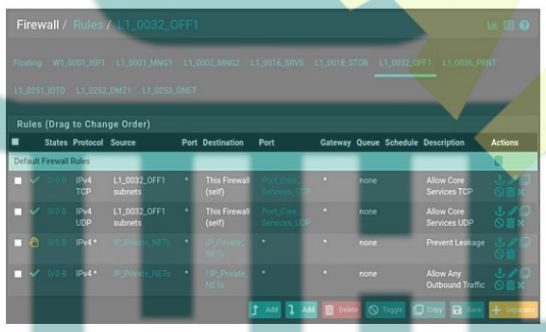
Rule 4:

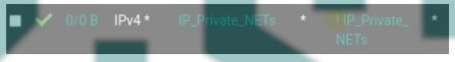
- Action: Pass
- Interface: L1_0032_OFF1
- Address Family: IPv4
- Protocol: Any
- Source: Address or Alias; IP_Private_NETs
- Destination:
  - Check the tick box "Invert match"
  - Select "Address or Alias" Destination
  - Address: IP_Private_NETs
- Description: Allow Any Outbound Traffic

Nous pourrions vouloir ajouter un séparateur pour clarifier nos règles.

Cliquez sur "Séparateur". Ensuite, saisissez la description suivante : « Règles de pare-feu par défaut ». Cliquez sur la boule de couleur verte. Ensuite, cliquez sur "Enregistrer". Enfin, faites glisser le nouveau séparateur vers le haut de l'ensemble de règles et cliquez sur Enregistrer.

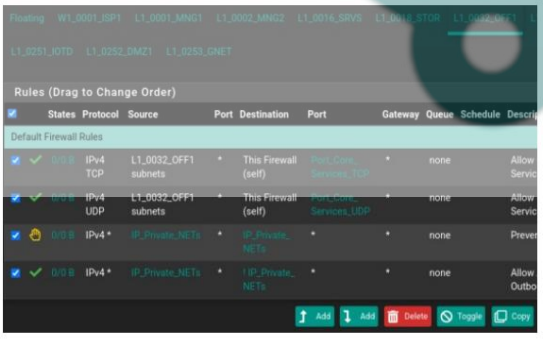
L'apparence finale doit refléter la capture d'écran ci-dessous, en accordant une attention particulière au point d'exclamation indiquant la règle inverse à la fin de l'ensemble de règles.



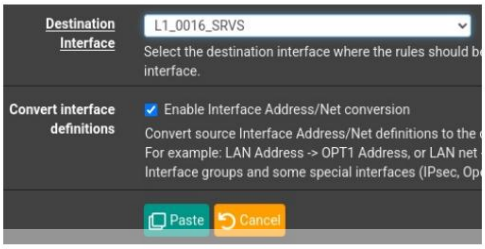


3.3.1.4. Répliquer les règles de pare-feu

Pour répliquer cet ensemble de règles de pare-feu pour une autre interface, cochez la case en haut à gauche et cliquez sur « Copier ».



Assurez-vous de sélectionner l'option « Convertir les définitions d'interface », puis cliquez sur « Coller » et appliquez les modifications.



Notez que le séparateur ne sera pas copié, car ce n'est actuellement pas possible. Veuillez créer le séparateur « Règles de pare-feu par défaut » pour cette interface afin de terminer les étapes.

Répétez ces étapes pour les autres interfaces commençant par "L1_"

Bien que nous conservions cette règle pour le trafic sortant telle quelle pour le moment, il est conseillé de la remplacer par un ensemble de règles autorisant uniquement le trafic sortant nécessaire pour les serveurs.

Dans ce contexte, une approche largement recommandée consiste à établir un séparateur « Exceptions » en haut de l'ensemble de règles du pare-feu et à positionner les règles sortantes directement en dessous. Cette pratique fournit une manière structurée de gérer les exceptions, facilitant ainsi la localisation et la modification des règles si nécessaire. Pour obtenir l'effet souhaité, désactivez simplement la règle sortante à la fin, garantissant ainsi un flux de trafic équilibré et contrôlé.

Pour plus de détails sur la gestion des règles de pare-feu, reportez-vous aux documents Netgate. Explorez ce lien pour une étude approfondie, car il s'agit d'un aspect crucial de la configuration de pfSense.

Dans la section suivante, nous explorerons brièvement certains services importants du pare-feu pfSense, tels que DHCP et DNS.

3.4. Services pfSense

DHCP et DNS sont cruciaux pour la fonctionnalité du réseau, assurant l'automatisation et l'organisation de l'attribution des adresses IP et de la traduction des noms de domaine en adresses IP.

3.4.1. DHCP

DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui attribue automatiquement des adresses IP et d'autres informations de configuration réseau aux appareils d'un réseau. Dans pfSense, le service DHCP permet de gérer et de distribuer les adresses IP de manière dynamique, facilitant ainsi la connexion des appareils au réseau sans configuration manuelle.

Dans le cadre de cet article, il est important de savoir comment activer et configurer DHCP.

Étapes pour activer et configurer DHCP.

1. Accédez à « Services » > « Serveur DHCP ».
2. Cochez la case "Activer le serveur DHCP sur (sélectionnez l'interface)" pour activer le service DHCP pour l'interface souhaitée.
3. Configurez les paramètres DHCP, y compris la plage d'adresses IP à attribuer, la durée du bail et les options supplémentaires si nécessaire.
4. Enregistrez et appliquez les modifications pour rendre le service DHCP opérationnel.

Ces étapes vous aideront à configurer efficacement DHCP dans pfSense.

Pour le réseau Office (L1_0032_OFF1), cela devrait ressembler à ce qui suit.

1. Navigate to "Services" > "DHCP Server".
2. Check the "Enable DHCP server on (select the interface)" box to activate the DHCP service for the desired interface.
3. Configure the DHCP settings:
   - Address Pool Range: (from) 10.10.32.101 (to) 10.10.32.200
   - NTP Server 1: 10.10.32.1
4. Save and Apply the changes to make the DHCP service operational.

Il est important de noter que ISC DHCP a atteint la fin de sa vie et sera supprimé dans une future version de pfSense. Les administrateurs sont encouragés à passer à Kea DHCP. Le changement est une question de quelques clics : « Système » > « Avancé » > « Réseau » : cochez « Kea DHCP » et cliquez sur « Enregistrer ».

3.4.2. DNS

DNS (Domain Name System) est un système qui traduit les noms de domaine lisibles par l'homme (comme www.ict-diensten.com) en adresses IP que les ordinateurs utilisent pour s'identifier sur un réseau. Dans pfSense, le service DNS garantit une résolution efficace et précise des noms de domaine, facilitant une communication transparente entre les appareils utilisant des noms de domaine plutôt que des adresses IP.

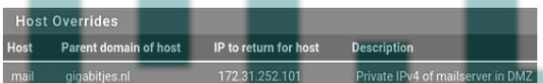
Dans le cadre de cet article, il est important de savoir comment ajouter des remplacements d'hôte et de domaine au serveur DHCP de pfSense.

Étapes pour ajouter des remplacements d'hôte et des remplacements de domaine :

1. Accédez à « Services » > « Résolveur DNS ».
2. Dans la section « Remplacements d'hôte » ou « Remplacements de domaine », cliquez sur « Ajouter » pour ajouter une nouvelle entrée.
3. Saisissez les informations nécessaires, notamment le nom d'hôte, le domaine et l'adresse IP correspondante.
4. Enregistrez et appliquez les modifications pour mettre à jour les paramètres DNS.

Ces étapes vous aideront à configurer efficacement les services DNS dans pfSense.

Imaginez que vous utilisez un serveur de messagerie nommé mail.gigabitjes.nl et que son IPv4 publique dans l'enregistrement A est 123.123.123.101. Cependant, au sein du LAN, ce serveur est reconnu avec l'adresse IPv4 172.31.252.101. Dans un tel scénario, se référer à l'IPv4 public depuis le LAN n'est pas pratique. Définir un remplacement d'hôte sur l'IPv4 privé est une solution utile. Ce remplacement d'hôte ressemblerait à la capture d'écran suivante.



Dans la section suivante, nous examinerons brièvement la configuration du VLAN sur les commutateurs. Nous basculerons entre l'interface du switch et l'interface web de pfSense pour les règles de pare-feu requises.

3.5. Configuration du commutateur

Dans notre réseau, les commutateurs réseau jouent un rôle crucial dans la prise en charge d'une variété de périphériques tels que les commutateurs, les points d'accès, les serveurs et les postes de travail.

Pour une conception de réseau efficace, il est essentiel d'établir un schéma de connexion réseau structuré afin d'éviter les commutateurs en série et les goulots d'étranglement potentiels. Dans cette configuration, nous désignons un noyau interrupteur qui sert de point central. Tous les autres commutateurs se connectent à ce commutateur principal, fonctionnant comme des commutateurs d'accès. Les connexions du commutateur principal aux commutateurs d'accès sont référencées comme liaisons descendantes, tandis que les connexions des commutateurs d'accès au commutateur principal sont appelées liaisons montantes. Cette configuration hiérarchique garantit un réseau bien organisé et évolutif Infrastructure.

Nous commencerons par attribuer une adresse IPv4 au commutateur et intégrer des VLAN dans la configuration VLAN du commutateur.

3.5.1. Préparatifs

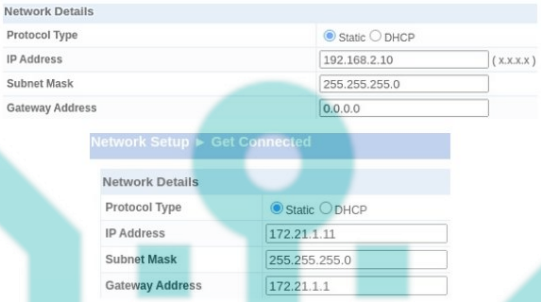
Avant de configurer notre (premier) commutateur, il doit se voir attribuer une adresse IPv4 du VLAN de gestion [L1_0001_MNG1].

Pour commencer, j'ai connecté le port 24 d'un switch HP 1810-24g à l'interface LAN du pare-feu pfSense. Par la suite, j'ai connecté mon ordinateur portable au port 23. J'ai attribué une adresse IPv4 statique, 192.168.2.123, avec un masque de sous-réseau de 255.255.255.0 [/24] à mon ordinateur portable. Cette étape permet de modifier l'adresse IPv4 par défaut du commutateur.

Suite à cela, j'ai changé l'adresse IPv4 du commutateur en 172.21.1.11, avec un masque de sous-réseau de 255.255.255.0 [/24]. La passerelle IPv4 par défaut a été définie sur 172.21.1.1.

Pour garantir des paramètres IPv4 précis, j'ai brièvement déconnecté le câble réseau de mon ordinateur portable. Étant donné que j'utilise Linux, je pourrais conserver les paramètres DHCP tout en définissant un IPv4 statique au sein du réseau 192.168.2.0/24 initialement utilisé par le commutateur.

Les paramètres par défaut et mis à jour sont décrits dans les captures d'écran ci-dessous.



Pour éviter les conflits DHCP, j'ai ajusté le pool DHCP de L1_0001_MNG1, en modifiant la plage de 172.21.1.201 à 172.21.1.230 dans le pare-feu pfSense. Pour ce faire, j'ai navigué vers "Services" > "Serveur DHCP" > "L1_0001_MNG1" et modifié la plage dans la section "Pool d'adresses primaires". De plus, j'ai remarqué que le serveur NTP 1 n'était pas défini. Bien que facultatif, je l'ai défini sur 172.21.1.1. Enfin, j'ai enregistré et appliqué les modifications.

3.5.2. Configuration du VLAN

Nous sommes prêts à mettre en œuvre les modifications requises sur notre commutateur. L'accent sera mis sur les VLAN.

3.5.2.1. Présentation du réseau

L'aperçu suivant sera utilisé.

Interface	VLAN tag	Priority	Name	Subnet	Gateway	Description	Examples
igb1 (lan)	1	-	L1_0001_MNG1	172.21.1.0/24	172.21.1.1	Management 1	Switches, access points
igb1 (lan)	2	-	L1_0002_MNG2	172.22.2.0/24	172.22.2.1	Management 2	Hypervisor(s), KVM-over-IP
igb1 (lan)	16	-	L1_0016_SRVS	10.10.16.0/24	10.10.16.1	Server VMs	Server VMs
igb1 (lan)	18	-	L1_0018_STOR	10.10.18.0/24	10.10.18.1	Storage	Network Attached Storage (NAS)
igb1 (lan)	32	-	L1_0032_OFF1	10.10.32.0/24	10.10.32.1	Workstations	Desktop and laptop computers
igb1 (lan)	36	-	L1_0036_PRNT	10.10.36.0/24	10.10.36.1	Peripherals	Printers
igb1 (lan)	251	-	L1_0251_IOTD	172.31.251.0/24	172.31.251.1	Internet of Things	Solar panel inverters
igb1 (lan)	252	-	L1_0252_DMZ1	172.31.252.0/24	172.31.252.1	DMZ	Web and mail server
igb1 (lan)	253	-	L1_0253_GNET	172.31.253.0/24	172.32.253.1	Guest Network	Guest Wi-Fi network

Avant de commencer, nous devons déterminer quels VLAN seront configurés sur quels ports. Ce commutateur HP particulier dispose de 24 ports Ethernet Gigabit (ports 1 à 24) et de deux emplacements SFP+ (ports 25 à 26). Notre configuration de port sera la suivante. Vous remarquerez que le commutateur principal sera également utilisé comme commutateur d'accès.

Port	PVID	Tagged VLANs	Purpose
01	32		Access Port, Workstations
02	32		Access Port, Workstations
03	32		Access Port, Workstations
04	32		Access Port, Workstations
05	32		Access Port, Workstations
06	32		Access Port, Workstations
07	32		Access Port, Workstations
08	32		Access Port, Workstations
09	32		Access Port, Workstations
10	32		Access Port, Workstations
11	32		Access Port, Workstations
12	32		Access Port, Workstations
13	36		Access Port, Printer
14	36		Access Port, Printer
15	251		Access Port, IoT, NVR camera system
16	251		Access Port, IoT, Inventor (solar panels)
17	18		Access Port, Storage
18	18		Access Port, Storage (reserved)
19	1	2,16,18,32,36,251,252,253	Downlink, hypervisor
20	1	2,16,18,32,36,251,252,253	Downlink, hypervisor (reserved)
21	1	2,16,18,32,36,251,252,253	Downlink, switch or AP (reserved)
22	1	2,16,18,32,36,251,252,253	Downlink, switch or AP (reserved)
23	1	2,16,18,32,36,251,252,253	Downlink, switch (reserved)
24	1	2,16,18,32,36,251,252,253	Uplink, firewall
25	1	2,16,18,32,36,251,252,253	Downlink, switch (reserved)
26	1	2,16,18,32,36,251,252,253	Downlink, switch (reserved)

3.5.2.2. Configuration du VLAN

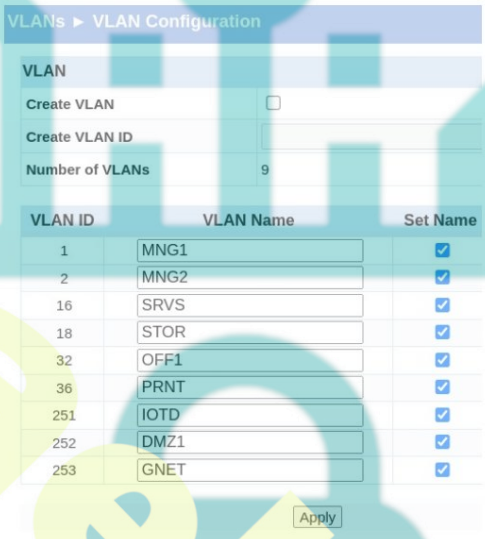
Passons à la configuration du VLAN sur le commutateur HP 1810-24g. Des commutateurs supplémentaires, tels que ZyXEL et TP-Link, seront intégrés dans ce document dans la prochaine révision.

Accédez à l'interface Web du commutateur en accédant à son adresse IPv4. Une fois connectés, nous pouvons commencer à ajouter des VLAN.

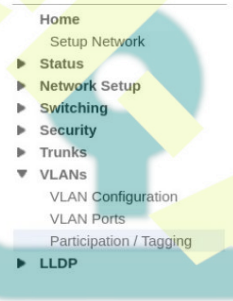
Sur ce commutateur HP, accédez directement à « VLAN » > « Configuration VLAN ». La création d'un VLAN est un processus simple : cochez la case à côté de "Créer un VLAN", entrez l'ID du VLAN et cliquez sur "Appliquer".

Répétez ce processus pour les VLAN restants.

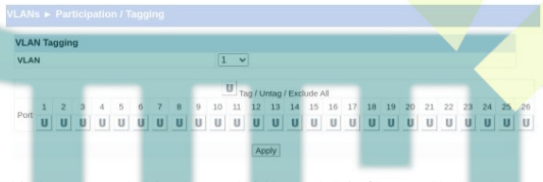
Gardez à l'esprit que le nom du VLAN n'est pas défini initialement. Activez le champ de texte correspondant en cochant la case, remplissez la colonne Nom du VLAN et cliquez sur « Appliquer » pour terminer le processus.



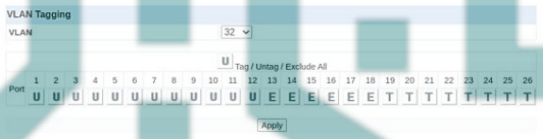
Maintenant, cliquez sur « Participation-/Tagging ».



Sélectionnez le VLAN et définissez le balisage. L'écran initial ressemble à la capture d'écran suivante.



Modifiez le VLAN de 1 à 32 et commencez à étiqueter le VLAN sur les ports. Les ports 01 à 12 ne seront pas balisés et les ports 20 à 26 seront balisés. Cliquez sur "Appliquer".



Le commutateur peut afficher un avertissement concernant le VLAN de gestion, ce qui est attendu. Ignorez cet avertissement, car notre ordinateur portable n'est connecté à l'un des ports de la plage 01-12.

172.21.1.11 says

Management port is not configured.
Configuring untagged membership on non-management VLAN may disrupt the web connectivity.

Do you wish to continue?

Cancel OK

Another warning may appear, indicating that a port cannot be a member of two untagged VLANs.

172.21.1.11 says

Ports - 1,2,3,4,5,6,7,8,9,10,11,12 can have only one untagged VLAN membership.
If the port is already untagged VLAN member in one VLAN and any other new VLAN is selected for untagged membership,
then the port will be excluded from previously untagged VLAN if any).

Do you wish to continue?

Cancel OK

Proceed to change the participation for VLAN 36.

As shown in the screenshot below, you'll observe that ports 13 and 14 are untagged. This allows us to connect a device to either port 13 or 14, making it suitable for accommodating two printers.

Ensuite, modifiez la participation des VLAN restants. Notez que les VLAN 252 et 253 doivent uniquement être ajoutés avec une balise sur les ports 19 à 26.

Toutes nos félicitations! Pour l'instant, nous avons terminé la construction de notre réseau. Des modifications supplémentaires seront appliquées une fois que notre hyperviseur sera opérationnel. Passons rapidement à la construction de notre hyperviseur Proxmox dans le chapitre suivant !

4. Construire une infrastructure de serveur

Ce chapitre couvre la procédure d'installation et de configuration de Proxmox Virtual Environment (VE).

4.1. Configuration matérielle minimale requise

Reportez-vous au site Web Proxmox pour connaître les recommandations matérielles minimales pour les environnements de production et d'évaluation.

À des fins de test, les exigences sont modestes :

- CPU : 64 bits (Intel EMT64 ou AMD64), CPU/carte mère compatible Intel VT/AMD-V (pour prise en charge complète de la virtualisation KVM)
- Au moins 1 Go de RAM
- Disque dur
- Une carte réseau

Les exigences de production sont également raisonnables ; veuillez consulter la configuration matérielle requise pour plus de détails.

4.2. Obtention de l'image d'installation de Proxmox

L' image d'installation de Proxmox est disponible sur le site Proxmox. L'obtention de l'ISO de l'environnement virtuel Proxmox est simple. L'étape suivante consiste à écrire l'image ISO sur une clé USB.

4.3. Préparation du support d'installation

Reportez-vous à la page Wiki Proxmox et le site Proxmox pour connaître les procédures recommandées pour préparer le support d'installation. Veuillez consulter la section sur la préparation du support d'installation. Notez que la procédure est similaire à pfSense, la principale différence étant que Proxmox n'est disponible qu'au format ISO.

4.3.1. Linux

Pour Linux, le processus recommandé implique l'utilisation de la commande « dd » :

dd bs=1M conv=fdatasync if=./proxmox-ve_*.iso of=/dev/sdX

Reportez-vous à la section Préparer le support sur le site Web de Proxmox pour plus de détails exacts.

Au lieu de la procédure recommandée, Ventoy a été utilisé. Ventoy n'est pas répertorié dans la documentation Proxmox. Bien qu'il ne soit pas répertorié dans la documentation de Proxmox, il a été utilisé avec succès; bien qu'une version CI de Ventoy devait être utilisé comme décrit dans le numéro 2657.

4.3.2. Mac OS

Pour MacOS, utilisez la commande hdiutil.

hdiutil convert proxmox-ve_*.iso -format UDRW -o proxmox-ve_*.dmg

Veuillez consulter la section Préparer les médias sur le site Proxmox pour les détails exacts.

4.3.3. les fenêtres

Pour Windows, une recommandation est d'utiliser Rufus en mode DD.

Une note du Guide d'administration Proxmox conseille de sélectionner le « Mode DD » lorsque vous y êtes invité et d'éviter le téléchargement d'une version différente de GRUB.
Source : Guide d'administration Proxmox, section : Préparer le média.

4.4. Processus d'installation de Proxmox VE

Le processus d'installation de Proxmox VE est simple et moins intensif que celui de pfSense.

4.4.1. Démarrage

Démarrez l'ordinateur avec le support d'installation préparé. Sélectionnez « Installer Proxmox VE (graphique) » pour commencer l'installation.

Remarque : pendant le démarrage, si le processus s'arrête lors de la détection du pays, débranchez le câble réseau, redémarrez, sélectionnez à nouveau « Installer Proxmox VE (graphique) » et reconnectez le câble après la présentation du contrat d'utilisateur final (CLUF).

4.4.2. CLUF

Cliquez sur "J'accepte" dans le CLUF.

4.4.3. Partitionnement

Sélectionnez le disque dur cible. La configuration de stockage du serveur est la suivante :

- /dev/sda 465,76 Gio SSD Samsung 860
- /dev/sdb 465,76 Gio SSD Samsung 860
- /dev/sdc 465,76 Gio SSD Samsung 860
- /dev/sdd 465,76 Gio CT500MX500SSD4

Le disque dur cible choisi est /dev/sdd.

Un une autre option consiste à utiliser "zfs (RAIDZ-1)" pour les trois premiers SSD et ext4 pour ce dernier SSD. Cliquez sur "Suivant" pour procéder.

4.4.4. Sélection de l'emplacement et du fuseau horaire

Lors de l'installation, sélectionnez l'emplacement et le fuseau horaire. Par exemple:

- Pays : Pays-Bas Fuseau
- horaire : Europe/Amsterdam
- Disposition du clavier : anglais américain

Cliquer sur Suivant pour continuer.

4.4.5. Mot de passe d'administration et adresse e-mail

Définissez un mot de passe et fournissez une adresse e-mail lorsque le programme d'installation vous y invite. Cliquez ensuite sur "Suivant".

4.4.6. Configuration du réseau de gestion

La configuration du réseau est cruciale. Sélectionnez les éléments suivants, en veillant à ajuster le nom d'hôte (FQDN).

- Interface de gestion : eno1 {mac} (e1000e)
- Nom d'hôte (FQDN) : pve101.lan.gigabitjes.nl
- Adresse IP (CIDR) : 172.21.1.101 Passerelle :
- 172.21.1.1 Serveur DNS :
- 172.21.1.1

Cliquez sur Suivant".

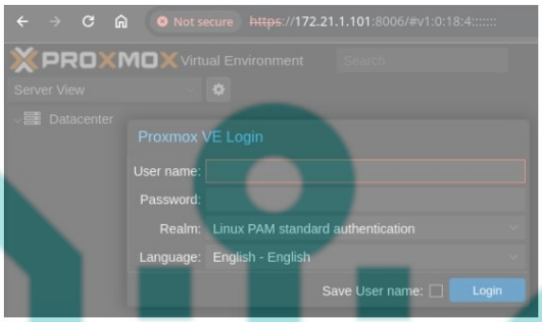
Veuillez noter que notre hyperviseur sera positionné dans une configuration VLAN1, différent du conception de réseau originale, qui spécifiait VLAN2. À cette étape, en optant pour VLAN2 pourrait être trop complexe, il faut comme un VLAN plus compliquée.

4.4.7. Finalisation de l'installation

Passez en revue les décisions résumées et cliquez sur « Installer ». Une fois l'installation terminée, le système redémarrera.

4.5. Procédure de configuration Proxmox

Une fois Proxmox VE installé, le processus de configuration commence. Ouvrez un navigateur Web et connectez-vous à https://172.21.1.101:8006.



4.5.1. Abonnement et mises à jour

Abonnements Proxmox VE

Il est conseillé d'opter pour un abonnement Proxmox, fournissant un accès au référentiel Proxmox Enterprise stable pour des mises à jour logicielles fiables, des améliorations de sécurité et des informations de niveau entreprise soutien technique.

Référentiel sans abonnement Proxmox VE

Pour les tests et une utilisation hors production, le référentiel sans abonnement Proxmox VE est recommandé. Il ne nécessite pas de clé d'abonnement.

Pour cet article, le référentiel sans abonnement Proxmox VE sera utilisé.

Pour définir le référentiel sans abonnement :

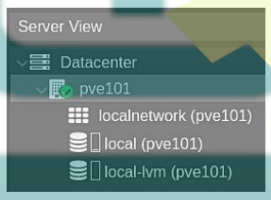
1. Navigate to PVE under Datacenter and click on Shell.
2. Open sources.list with a text editor like vi or nano.
3. Add the Proxmox VE No-Subscription Repository to /etc/apt/sources.list:
   deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription
   Save the changes and close the editor.
4. Disable enterprise repositories for Ceph and Proxmox:
   Open /etc/apt/sources.list.d/ceph.list and comment out the repository:
   #deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise
   Open /etc/apt/sources.list.d/pve-enterprise.list and comment out the repository:
   #deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
   Save the changes and close the editor.
5. Check and install updates:
   apt update && apt -y upgrade
6. Optional: remove the subscription nag:

   sed -Ezi.bak "s/(Ext.Msg.show\(\{\s+title: gettext\('No valid sub)/void\(\{ \/\/\1/g" /usr/share/javascript/proxmox-widget-toolkit/proxmoxlib.js && systemctl restart pveproxy.service

   Référez-vous au service informatique de John en ce qui concerne la suppression du problème d'abonnement.

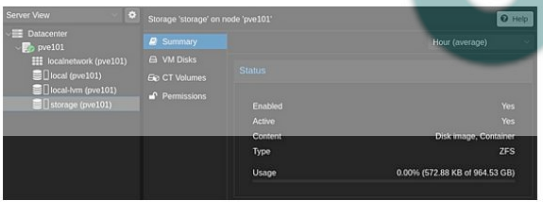
4.5.2. Stockage

Lorsque vous développez PVE dans le volet de gauche, remarquez le stockage local. Ajoutez les trois SSD pour le stockage de VM et de conteneur.



1. Cliquez sur ZFS (sous Disques) dans le deuxième volet.
2. Cliquez sur Créer ZFS, sélectionnez les disques, le nom (par exemple, « stockage »), choisissez le niveau RAID (par exemple, RAIDZ) et cliquez sur Créer.

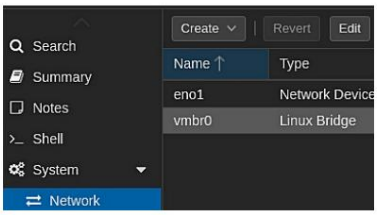
Maintenant, créez des machines virtuelles et des conteneurs et stockez leurs disques et volumes sur le stockage ZFS.



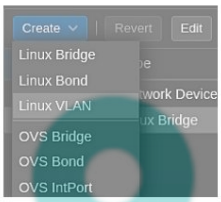
4.5.3. VLAN

Avant de créer des VM et des CT, triez les VLAN pour les connecter aux réseaux appropriés.

Cliquez sur Réseau pour ouvrir l'aperçu (notez le Linux Bridge vmbr0).

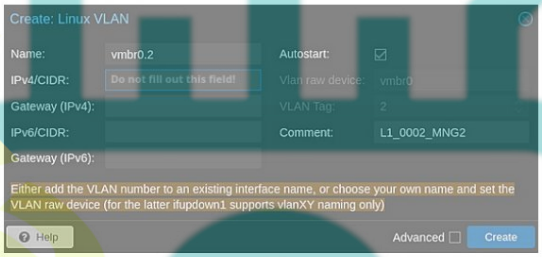


Cliquez sur Créer et sélectionnez Linux VLAN.

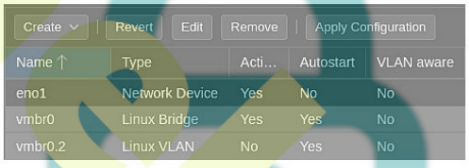


Entrez les détails du VLAN et cliquez sur Créer.

- Commencez par le nom du pont , puis entrez le numéro de VLAN (séparé par un point).
- N'entrez pas l' IPv4/CIDR.
- Pour plus de clarté, entrez le nom du VLAN dans le champ de commentaire.
- Cliquez sur Créer.

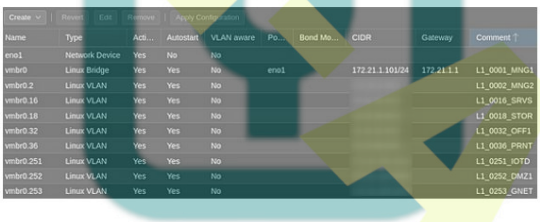


Une fois l'ajout réussi du VLAN 2, la configuration résultante ressemblera à la capture d'écran ci-dessous.



Répétez cette procédure pour les autres VLAN.

Appliquez la configuration en cliquant sur Appliquer la configuration.



Quelques considérations importantes :

1. Des problèmes de routage peuvent survenir dès que les informations IPv4/CIDR sont saisies pour les VLAN. Cela n'affecte pas le trafic entre les machines virtuelles et les nœuds physiques du réseau, mais cela affecte le trafic entre les machines virtuelles et les nœuds physiques du réseau. le PVE et les VM/nœuds de réseau physique. Cela peut prêter à confusion lors du dépannage. Être averti!

2. Ouvrez vSwitch (OVS) comme alternative à la commutation Linux :
   Un pont Linux et des VLAN Linux sont utilisés. Vous pouvez envisager de choisir un pont OVS et des InstPorts OVS. Le fait est que le pont existant doit d'abord être supprimé. Ainsi, si vous préférez pour utiliser OVS : n'appliquez les modifications qu'une fois qu'au moins le nouveau OVS Bridge a été créé correctement. Vous êtes invité à créer une copie de « /etc/networking/interfaces » à l'avance. Vous devrez peut-être utiliser un clavier (physique) et un moniteur au cas où quelque chose se passerait vraiment mal avec la configuration du réseau.

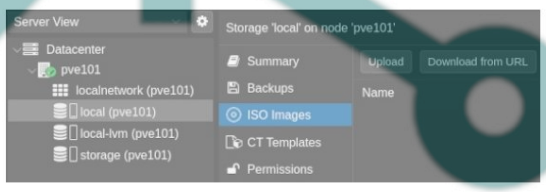
4.5.4. Sources d'installation de VM et CT

Les images ISO sont utilisées pour nos VM. Les modèles CT sont utilisés pour les conteneurs.

4.5.4.1. Images ISO

Utilisez des images ISO des CD/DVD d'installation pour installer les machines virtuelles.

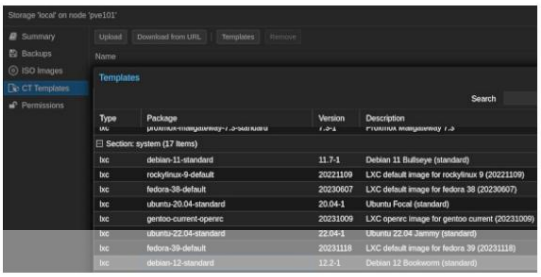
Cliquez sur Images ISO sous « local (pve101) » et sur Télécharger ou Télécharger à partir d'une URL pour ajouter une image ISO.



4.5.4.2. Modèles CT

Les conteneurs sont économes en ressources. Les modèles CT sont requis pour créer des conteneurs.

Cliquez sur Modèles CT, puis sur Modèles pour répertorier les modèles disponibles. Téléchargez le modèle souhaité.

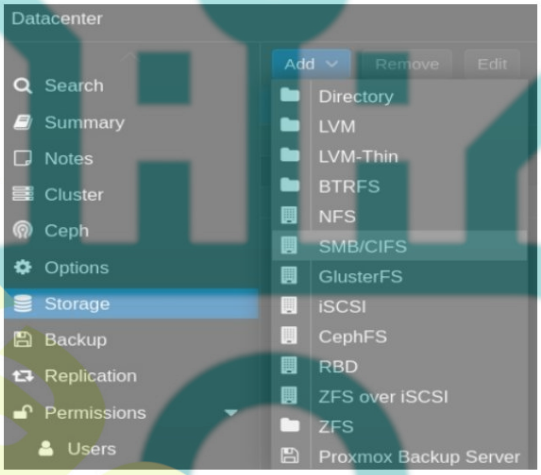


4.6. Sauvegardes Proxmox

Les sauvegardes sont indispensables. Ajoutez du stockage de sauvegarde et activez les sauvegardes pour les machines virtuelles et les CT.

4.6.1. Cibles et tâches de sauvegarde

Une méthode de sauvegarde simple consiste à ajouter un emplacement de stockage SMB/CIFS. Ajoutez un NAS via le stockage sous Datacenter. Pour plus de détails, consultez le chapitre Wiki Proxmox VE sur le stockage.



Recherchez l'option Sauvegarde sous Stockage et reportez-vous à la section Sauvegarde et restauration. dans le Wiki Proxmox pour un aperçu détaillé.

L'intégration d'une cible de sauvegarde et la création de planifications de sauvegarde sont un processus simple. Pour améliorer les notifications par courrier, il est conseillé d'utiliser un hôte relais. Un exemple informatif peut être trouvé sur le forum Proxmox dans le tutoriel intitulé [TUTORIEL] Obtenir Postfix pour envoyer des notifications (e-mail) en externe). La configuration des notifications par courrier est cruciale pour surveiller le succès des sauvegardes. Il est à noter que le relayhost peut être notre serveur de messagerie auto-hébergé, un sujet que nous aborderons dans le prochain chapitre !

5. Services exposés à Internet

Considérations relatives à l'hébergement de votre courrier et de votre serveur Web

Une décision importante à considérer est de savoir si vous souhaitez héberger votre propre serveur de messagerie et votre propre serveur Web. Bien que des alternatives existent, comme l'utilisation d'un serveur privé virtuel (VPS) ou le recours à un hébergement externe services, cet article fonctionne sous l'hypothèse d'un auto-hébergement sur du matériel dédié.

Si vous ne vous sentez vraiment pas à l'aise avec l'utilisation de services exposés à Internet, il serait peut-être préférable de vous abstenir de le faire. La sécurité et le confort sont des considérations primordiales pour décider comment et où héberger les services critiques !

Concept d'auto-hébergement

Dans notre réseau, il y aura à la fois des services exposés à Internet et des services internes. Le premier comprendra des services tels que les serveurs Web et de messagerie, qu'il est essentiel de configurer et de sécuriser dès le début du processus.
Ces services exposés à Internet constituent le visage de notre réseau, nécessitant une configuration minutieuse pour l'accessibilité et la protection.

Nous commencerons par nous concentrer sur les services exposés à Internet, en traitant la configuration d'un serveur de messagerie et d'un serveur Web comme des exercices précieux. Cette approche nous permet de mettre en œuvre et de sécuriser des services critiques avant de nous lancer dans des services internes tels que les contrôleurs de domaine et les serveurs de fichiers, que nous préférons ne pas exposer à Internet. Prioriser la configuration et la sécurité de ceux-ci orientés vers l'extérieur
les services sont une pratique fondamentale pour garantir à la fois l'accessibilité et la protection.

Au fur et à mesure de notre progression, nous explorerons également les services internes dans le chapitre suivant, garantissant une infrastructure réseau complète et bien organisée.

5.1. Acheminement du trafic

Pour permettre le routage de nos services exposés à Internet, certaines exigences doivent être remplies. Dans certains cas, les connexions Internet existantes peuvent ne pas répondre à ces critères et il peut être impossible de modifier la connexion. Dans de telles situations, une solution de contournement est nécessaire.

Un exemple est la nécessité d'établir un enregistrement de pointeur (PTR) valide dans DNS pour héberger un serveur de messagerie. Généralement, cet enregistrement PTR est configuré par l'opérateur de l'IP publique, souvent le fournisseur d'accès Internet (FAI). Il est essentiel de s'assurer que l'adresse IP publique associée à la connexion Internet dispose d'un enregistrement PTR valide. Le nom de domaine complet (FQDN) du serveur doit correspondre au résultat d'une recherche PTR effectuée sur l'adresse IP publique. Ne pas parvenir à cet alignement présente un risque pour la bonne livraison des messages électroniques. Dans les cas où le
Le fournisseur d'accès Internet ne peut pas configurer un enregistrement PTR, une solution de contournement devient impérative. Cette section détaille les stratégies potentielles pour mettre en œuvre une telle solution de contournement.

L'une des solutions possibles consiste à introduire un tunnel GRE. Generic Routing Encapsulation (GRE) est un protocole de tunneling conçu pour encapsuler divers protocoles de couche réseau dans des liaisons virtuelles point à point ou point à multipoint sur un réseau de protocole Internet.

La sélection de GRE est intentionnelle. Bien qu'il ne crypte pas le trafic entre les points de terminaison, GRE est léger et polyvalent, ce qui le rend bien adapté au routage du trafic de courrier électronique et Web.

Nous établirons un tunnel GRE pour acheminer efficacement le trafic entre notre pare-feu pfSense et un serveur privé virtuel (VPS) rentable. En tirant parti de l'adresse IPv4 publique du VPS, nous gérerons le trafic entrant. Ce trafic sera transporté via le tunnel GRE jusqu'à notre serveur VM, fonctionnant sur Proxmox.

En résumé, nous devons configurer les composants suivants.

1. Configurez un VPS avec (Debian) Linux, y compris la configuration réseau et GRE.
2. Établissez des règles de pare-feu IPTables sur le VPS.
3. Configurez GRE et les règles sur pfSense.
4. Configurez une VM exécutant le serveur ISPConfig sur (Debian) Linux, responsable de l'hébergement du serveur de messagerie et du serveur Web.

5.1.1. Choisir un fournisseur VPS

Exigences

Lors de la sélection d'un fournisseur de serveur privé virtuel (VPS), il est crucial d'en choisir un qui correspond à des exigences spécifiques. Recherchez un fournisseur qui permet l'utilisation d'une adresse IPv4 publique, permet la configuration d'un enregistrement Pointer (PTR), et offre un trafic illimité.

Pour les besoins de cet article, Strato a été choisi comme fournisseur VPS. Strato, une société d'hébergement Web réputée, propose une gamme de solutions, notamment des serveurs privés virtuels (VPS).
Parmi les produits disponibles, le VPS LINUX MINI VC1-1 et VC1-2 sont des choix appropriés. Au moment de la rédaction de cet article, le coût mensuel d'un VC1-1 n'est que de 1 €. Bien que ce mini VPS réponde aux exigences spécifiées, le VC1-2 est sélectionné pour sa polyvalence supplémentaire, car l'auteur a l'intention d'utiliser également ce VPS pour divers autres services.

Disponibilité

Les plans VPS VC1-1 et VC1-2 sont disponibles sur les sites Web néerlandais et allemand de Strato. Bien qu'il existe un site Web espagnol, il n'est pas certain qu'il propose la catégorie mini-VPS. Notamment, les sites Web britanniques et français de Strato ne semblent proposer aucune option de serveur privé virtuel. Bien que l'auteur de cet article n'ait aucune expérience avec Ionos, il semble que ce soit l'un des
options rentables à considérer (comme alternative à Strato UK).

Informations de facturation pour Strato VPS (VC1-2)

Strato facture trimestriellement et la facture initiale pour le VPS VC1-2 est de 6 €. Le cycle de facturation s'étend sur un an, ce qui entraîne un coût annuel total de 24 € HT. Aucun frais d'installation supplémentaire ne s'applique.

Processus de commande de Strato

Lors du processus de commande, un compte client sera créé. Une fois cette étape franchie, la commande subit un traitement qui peut prendre plusieurs heures. Le serveur privé virtuel (VPS) est
puis provisionné, arrivant dans un état « nu ». A ce stade, le système d'exploitation peut être installé. Une fois la configuration du système d'exploitation terminée, l'utilisateur root peut se connecter. Strato impose SSH
accès à l'aide d'un certificat pour des connexions sécurisées, ce qui est une mesure de sécurité judicieuse.

Voici comment créer un certificat SSH pour le VPS sous Linux :

1. Ouvrez un terminal et tapez la commande suivante :

```
ssh-keygen -t ecdsa
```

2. Entrez un nom de fichier dans lequel enregistrer la clé, tel que « id_strato_vps », et appuyez sur Entrée lorsqu'une phrase secrète est demandée.
3. Copiez la clé publique générée sur le VPS. Il s'agit d'une étape cruciale dans le processus de mise en scène.
4. Enfin, connectez-vous au VPS à l'aide de la commande suivante :

```
ssh root@server.ext -i $HOME/.ssh/id_strato_vps
```

Assurez-vous d'ajuster le nom du serveur et la clé si nécessaire pour établir la connexion.

Attention : Il est indispensable de mettre en place un enregistrement DNS A pour le serveur, correspondant au domaine choisi. L'enregistrement A doit pointer vers l'adresse IPv4 publique du VPS. Cela garantit une résolution de domaine appropriée et permet aux utilisateurs d'accéder à votre serveur en utilisant le nom de domaine désigné. Une autre étape essentielle consiste à définir l'enregistrement du pointeur (PTR). Dans la plupart des cas, cela doit être fait dans le panneau d'administration du fournisseur VPS.

5.1.2. Personnalisations (VPS)

Des personnalisations spécifiques sont requises pour le VPS.

5.1.2.1. Personnalisation de Strato VPS

Paquets

Assurez-vous d'installer les packages requis.

```
apt update && apt -y install \
bzip2 \
cron \
dnsutils \
fail2ban \
iproute2 \
iptables \
mc \
nano \
net-tools \
unzip \
whois
```

Suppression de Cloud-init

Il est recommandé de supprimer Cloud-init, un progiciel automatisant l'initialisation des instances cloud lors du démarrage du système, car il n'est pas nécessaire pour nos besoins.

```
touch /etc/cloud/cloud-init.disabled
dpkg-reconfigure cloud-init
apt-get purge cloud-init
rm -rf /etc/cloud/ && rm -rf /var/lib/cloud/
```

Bien que cela ne soit pas obligatoire, il est conseillé de redémarrer.

```
reboot
```

Plan réseau

Configurez les paramètres réseau via Netplan, spécifiquement dans le fichier par défaut `/etc/netplan/50-cloud-init.yaml`. Ce fichier sera modifié pour inclure la configuration du tunnel GRE.

```
réseau:
    ethernets:
        all:
            dhcp4: true
            dhcp6: true
            match:
                name: en*

    version: 2
```

Any warnings referencing Cloud-init can be ignored since it has been removed.

Now, add a GRE tunnel using the following example:

```
network:
    ethernets:
        all:
            dhcp4: true
            dhcp6: true
            match:
                name: en*

    tunnels:
        gre1:
        mode: gre
        local: 217.nnn.nnn.27
        remote: 77.nnn.nnn.155
        addresses: [172.30.250.2/29]
```

version 2

Assurez-vous d'ajuster l'IPv4 pour le local et le distant. Ici, « local » représente le VPS, « distant » représente l'autre point de connexion du tunnel (par exemple, un pare-feu), et l' adresse représente l'adresse interne du tunnel GRE côté VPS. Utilisez 172.30.250.1/29 comme adresse interne pour l'autre côté du tunnel (par exemple, un pare-feu).

Règles de pare-feu

Pour faciliter le routage du trafic, des règles de pare-feu spécifiques doivent être configurées pendant le processus de démarrage du VPS. Ceci peut être réalisé via un script de pare-feu. Téléchargez le fwall.sh script de Github et placez-le dans `/opt/scripts`. Assurez-vous que le script est exécutable.

```
mkdir /opt
mkdir /opt/scripts
cd /opt/scripts
wget "https://raw.githubusercontent.com/bhenstra/LiFiWall-Scripts/main/IPTables%20Forwarding%20GRE/fwall.sh"
nano fwall.sh
chmod +x fwall.sh
```

Ajustez au moins les variables "WL_SSH", "WL_GRE" et "INT_PUB". Les variables sont explicites, avec un bref commentaire précédant chacune d'entre elles dans les champs "BEGIN SETTINGS" et "END".
blocs « PARAMÈTRES ».

Enfin, ajoutez le script à la crontab de root.

```
crontab -e
```

Ajoutez la ligne suivante :

```
@reboot /opt/scripts/fwall.sh > /dev/null 2>&1
```

Avec ces configurations en place, le VPS est prêt à accepter et à acheminer le trafic efficacement.

5.1.3. Configuration de pfSense

L'autre extrémité de notre tunnel GRE est le routeur/pare-feu pfSense. Pour établir cette connexion, nous devons configurer une interface GRE, la reliant à l'IPv4 public du VPS.

Ajoutez et configurez l'interface GRE requise via l'option "GRE", située sous "Interfaces" > "Affectations".

1. Interface parent : sélectionnez l'interface WAN (par exemple W1_0001_ISP1)
2. Adresse distante : l'adresse publique du VPS
3. Adresse du tunnel IPv4 local : 172.30.250.1
4. Adresse du tunnel IPv4 distant : 172.30.250.2
5. Sous-réseau au format CIDR : /29
6. Cochez l'option "Ajouter un itinéraire statique"
7. Entrez une description pour référence administrative. 8. Enregistrez et appliquez les paramètres.

Exprimez le tunnel GRE comme une interface (la raison étant de nous permettre d'appliquer des règles de pare-feu).

1. Cliquez sur "Interfaces" > "Affectations".
2. Sélectionnez le tunnel GRE dans « Ports réseau disponibles » et cliquez sur « Ajouter ».
3. Enregistrez et appliquez les modifications.
4. Modifiez la nouvelle interface en cliquant dessus.
5. Activer l'interface 6. Définir une description "W1_0001_GRE0"
7. Définissez le MTU sur 1476.

Enregistrez et appliquez les modifications.

Bien que cela ne soit pas obligatoire pour l'interface WAN, définissez des règles de pare-feu pour le nouveau tunnel GRE. Tout d'abord, créez un alias de port représentant le trafic accepté.

Cliquez sur « Pare-feu » > « Alias » > « Ports ». Cliquez sur "Ajouter".

1. Nom : Ports_Ingress_GRE_TCP
2. Description : ports TCP acceptés pour GRE
3. Tapez : Port(s)
4. Ajoutez les ports suivants, un par ligne : cliquez sur "Ajouter un port" pour ajouter une ligne :
    - 25
    - 80
    - 443
    - 465
    - 587
    - 993

Enregistrer et appliquer les modifications

Ajoutez une règle pour accepter le trafic ICMP en cliquant sur "Pare-feu" > "Règles" > "W1_0001_GRE0". Cliquez sur "Ajouter" pour créer la règle suivante.

1. Action: Pass
2. Interface: "W1_0001_GRE0"
3. Address Family: IPv4
4. Protocol: ICMP
5. ICMP Subtypes:
    - Echo Request
    - Traceroute
6. Source: W1_0001_GRE0 subnets
7. Destination: W1_0001_GRE0 subnets
8. Description: Allow ICMP from GRE0 subnets

Enregistrer et appliquer les modifications

Nous appliquerons l'alias de port pour la règle NAT suivante en cliquant sur "Pare-feu" > "NAT". Cliquez sur "Ajouter" pour créer la règle NAT suivante.

1. Interface: W1_0001_GRE0
2. Address Family: IPv4
3. Protocol: TCP
4. Destination: W1_0001_GRE0 address
5. Destination port range:
    - From port: other
    - Custom: Ports_Ingress_GRE_TCP
6. Redirect IP: Address or Alias: 172.31.252.103
7. Redirect target port:
    - Port: Other
    - Custom: Ports_Ingress_GRE_TCP
8. Description: Allow ingress traffic via GRE

Enregistrer et appliquer les modifications

Remarque : L'IPv4 172.31.252.103 représente notre VM exécutant le serveur ISPConfig dans DMZ. N'hésitez pas à choisir un autre IPv4 selon vos besoins.

5.2. Installation d'ISPConfig

FAIConfig, un panneau Linux open source pour la gestion de plusieurs serveurs, sera installé dans un conteneur Linux sur Proxmox. Personnalisez l'IPv4 (par exemple 172.31.252.103) et le FQDN (par exemple s3.gigabitjes.nl) selon les besoins.

5.2.1. Télécharger le modèle de conteneur

Veuillez vous référer à « 4.5.4.2. Modèles CT » et télécharger « debian-12-standard ». Cette tâche prendra quelques secondes.

L'emplacement par défaut des modèles CT se trouve sous « Modèles CT » de l'option de stockage « local » sous le PVE.

5.2.2. Créer un conteneur

- Cliquez sur "Créer CT" pour créer un nouveau conteneur.
- Entrez les paramètres requis.

Général

1. Entrez l'ID CT : 103
2. Entrez le nom d'hôte : s3
3. Entrez et confirmez le mot de passe root souhaité
4. Cliquez sur Suivant

Modèle

5. Sélectionnez le modèle : debian-12-standard_12.2-1_amd64.tar.zst 6. Cliquez sur Suivant

Disques

7. Sélectionnez le stockage (dans notre cas c'est "stockage")
8. Définissez la taille du disque (Go) : par exemple "200"
9. Cliquez sur Suivant

CPU

10. Réglez les noyaux : par exemple "2"
11. Cliquez sur Suivant

Mémoire

12. Définissez la quantité de mémoire (MiB) : par exemple "4096"
13. Définir le swap (MiB) : par exemple "8192"
14. Cliquez sur Suivant

Réseau

15. Laissez le nom et le pont tels qu'ils sont. 16. Définissez la balise VLAN : 252.
17. Entrez l'IPv4/CIDR : 172.31.252.103/24
18. Entrez la passerelle IPv4 : 172.31.252.1
19. Cliquez sur Suivant

DNS

20. Entrez le domaine DNS : par exemple "gigabitjes.nl"
21. Entrez le serveur DNS : 172.31.252.1
22. Cliquez sur Suivant

Confirmer

23. Vérifiez et confirmez les options en cliquant sur Terminer.

- Sélectionnez le nouveau conteneur et cliquez sur "Console".
- Cliquez sur "Démarrer" pour démarrer le conteneur.

5.2.3. Installation automatisée d'ISPConfig 3 sur Perfect Server

Les étapes suivantes sont dérivées de l'installation automatisée de Perfect Server ISPConfig 3 sur Debian 10 à Debian 12, Ubuntu 20.04 et Ubuntu 22.04. Didacticiel.

Cliquez sur le conteneur (s3) et sélectionnez "Console". Connectez-vous en tant que root.

5.2.3.1. Mettre à jour les sources appropriées

Editez le fichier apt sources.list

```
nano /etc/sources.list
```

pour refléter la liste suivante :

deb http://deb.debian.org/debian bookworm contribution principale

deb http://deb.debian.org/debian bookworm-updates contribution principale

deb http://security.debian.org bookworm-security contribution principale

deb http://deb.debian.org/debian bookworm-backports contribution principale

5.2.3.2. Paquets

À mesure que nous avançons, nous suivrons les étapes décrites au paragraphe 5.2.3.2.2 pour mettre à niveau de manière transparente les progiciels essentiels, garantissant ainsi le maintien de la sécurité du système et l'optimisation des performances globales. Soulignant l'importance des mises à niveau régulières des packages, cette pratique est cruciale pour maintenir à la fois la sécurité du système et des performances optimales.

5.2.3.2.1. Noyau

Les conteneurs sont légers et utilisent le noyau de l'hyperviseur. Il n'est pas nécessaire d'installer un nouveau noyau pour un conteneur. Sautez les étapes suivantes et passez au paragraphe 5.2.3.2.2.
Mise à niveau des packages.

Lorsqu'une VM est utilisée, vous pouvez envisager d'installer le dernier noyau cloud. Recherchez le dernier noyau Linux bruyant avec la commande suivante :

```
apt update && apt-cache search linux-image | grep "cloud"
```

Choisissez et installez la dernière version. Au moment de la rédaction, il s'agissait de "linux-image-6.5.0-0.deb12.4-cloud-amd64" :

```
apt -y install linux-image-6.5.0-0.deb12.4-cloud-amd64
```

5.2.3.2.2. Mise à niveau des packages

```
apt update && apt -y upgrade 5.2.3.3.
```

Redémarrez le conteneur.

```
reboot
```

5.2.3.4. Exécutez le programme d'installation automatique

Connectez-vous en tant que root après le redémarrage. La procédure ci-dessous est presque la même que celle décrite dans le didacticiel original. Les différences résident dans la manière dont le nom d'hôte et le domaine sont définis et dans le fait que les quotas ne peuvent pas être utilisés dans un conteneur. Vous remarquerez que "--no-quota" a été ajouté à la commande d'installation.

Nous pouvons maintenant exécuter l'installateur automatique. La configuration de base contient les packages logiciels suivants (ainsi que leurs dépendances) : Apache2, PHP (versions 5.6 à 8.0), MariaDB, Postfix, Dovecot, Rspamd, BIND, Jailkit, Roundcube, PHPMyAdmin, Mailman, Webalizer, AWStats et GoAccess. Vous pouvez facilement choisir de ne pas utiliser certaines fonctions ou d'installer des services supplémentaires en passant des arguments au installateur. Voir le chapitre 6 du didacticiel original pour connaître les options de ligne de commande disponibles.

Optez soit pour ISPConfig avec le serveur Web Apache (5.2.3.4.1), soit avec le serveur Web Nginx (5.2.3.4.2).

5.2.3.4.1. Installer ISPConfig avec le serveur Web Apache

Vous pouvez maintenant exécuter le script avec des arguments. Par exemple, si vous souhaitez une installation normale avec le serveur Web Apache et une plage de ports pour FTP passif + mises à niveau sans surveillance, exécutez :

```
wget -O - https://get.ispconfig.org | sh -s -- --use-ftp-ports=40110-40210 --unattended-upgrades --no-quota
```

Les étapes suivantes sont décrites dans « 5.2.3.4.3. Exécution du programme d'installation automatique ».

5.2.3.4.2. Installer ISPConfig avec le serveur Web Nginx

Vous pouvez maintenant exécuter le script avec des arguments. Par exemple, si vous souhaitez une installation normale avec le serveur Web Nginx et une plage de ports pour FTP passif + mises à niveau sans surveillance, exécutez :

```
wget -O - https://get.ispconfig.org | sh -s -- --use-nginx --use-ftp-ports=40110-40210 --unattended-upgrades --no-quota
```

Les étapes suivantes sont décrites dans « 5.2.3.4.3. Exécution du programme d'installation automatique ».

5.2.3.4.3. Exécution de l'installateur automatique

Après un certain temps, lorsque vous êtes invité à reconfigurer le serveur complet, tapez « oui » et appuyez sur Entrée pour démarrer le programme d'installation.

AVERTISSEMENT! Ce script reconfigurera votre serveur complet !
Il doit être exécuté sur un serveur fraîchement installé et toute la configuration actuelle que vous avez effectuée sera très probablement perdue !
Tapez « oui » si vous souhaitez vraiment continuer :

Une fois terminé, notez les mots de passe administrateur ISPConfig et root MySQL.

[INFO] Votre mot de passe administrateur ISPConfig est : 8ZxSEWakDgSLXv
[INFO] Votre mot de passe root MySQL est : EhFrU3KYVLPVBbcJr2Js

5.2.3.5. Configuration du pare-feu

Configurez le pare-feu via l'interface utilisateur ISPConfig (Web). Pour l'accès au port 8080, autorisez le port dans le pare-feu VPS et pfSense ou ajoutez un remplacement d'hôte dans pfSense. À la lumière de cet article, nous opterons pour cette dernière.

Ouvrez l'interface Web de pfSense et cliquez sur "Services" > "DNS Forwarder". Faites défiler jusqu'à « Remplacements d'hôte » et cliquez sur Ajouter. Saisissez le nom d'hôte (par exemple "s3"), le domaine (par exemple "gigabitjes.nl") et l'IPv4 (par exemple "172.31.252.103"). Saisissez une description (par exemple "Serveur d'hébergement interne s3"). Enregistrez et appliquez les modifications.

Saisissez soit le FQDN, soit l'IPv4 (par exemple "https://s3.gigabitjes.nl:8080" ou "https://172.31.252.103:8080"). Vous pouvez ignorer l'avertissement « le certificat n'est pas fiable ». Cliquez sur Avancé et accédez au site Web.

Connectez-vous à l'interface utilisateur d'ISPConfig et accédez à « Système » > « Pare-feu ». Cliquez ensuite sur "Ajouter un nouvel enregistrement de pare-feu".

Pour une configuration normale, les ports à ouvrir sont :

- TCP : 20,21,22,25,80,443,40110 : 40210,110,143,465,587,993,995,53,8080,8081
- UDP : 53

Veuillez consulter le chapitre cinq du didacticiel original pour plus de détails.

5.2.3.6. Lectures complémentaires

Reportez-vous aux chapitres six et sept du didacticiel original pour les options avancées, des conseils utiles (sous Finalisation) et des notes importantes concernant la configuration du courrier (rDNS, SPF, DKIM). Les considérations DNS sont cruciales en raison de la division du DNS, ce qui a un impact sur la façon dont le DNS est résolu pour notre serveur d'hébergement au sein de notre réseau local.

Référez-vous au manuel utilisateur ISPConfig 3 disponible pour seulement 5 € (hors TVA).

5.3. Sites Web et domaines de messagerie

Les sites Web peuvent être ajoutés sans effort à l'aide de l'option « Sites », tandis que les domaines de messagerie peuvent être incorporés via l'option « E-mail ». Le processus est simple et correspond aux fonctionnalités intuitives attendues d'un panneau d'hébergement. En plus du manuel mentionné dans le paragraphe précédent, un excellent support communautaire est disponible.

Bien qu'ISPConfig prenne en charge DNS, il est supposé que les domaines sont gérés en dehors d'ISPConfig via un gestionnaire DNS, généralement un registraire ou un fournisseur d'hébergement.

Pour utiliser un tel domaine, les enregistrements DNS doivent pointer vers l'IPv4 publique du VPS.

5.3.1. Brève illustration des enregistrements A et CNAME

Un exemple d'enregistrement A pour un site Web est :

exemple.com. 86400 IN A 93.184.216.34

Lorsque quelqu'un accède à "example.com", l'IPv4 "83.184.216.34" est résolu. Remplacez simplement "exemple.com". avec votre propre domaine et "93.184.216.34" avec l'IPv4 de votre VPS.

En plus des enregistrements A, il est courant de travailler avec des enregistrements CNAME, fonctionnant comme des alias. Par exemple, les noms de domaine complets tels que « www.example.com » peuvent servir d'alias pour « example.com ». Le fait de ne pas définir un tel enregistrement CNAME peut entraîner la disparition de visiteurs.

5.3.2. Brève illustration des enregistrements MX

Voici un exemple d'enregistrement MX pour un domaine de messagerie :

exemple.com. 300 IN MX 0 mail.example.com.

Lorsque quelqu'un envoie un e-mail à, par exemple, info@example.com, le serveur de messagerie essaiera de transmettre le message à mail.example.com. L'hôte mail.example.com, en revanche, nécessite un enregistrement A valide.

Remplacez « exemple.com ». par le domaine de messagerie et remplacez "mail.example.com". avec le FQDN de votre VPS, dans le cadre de cet article, ce serait s3.gigabitjes.nl.

5.3.3. Brève illustration de SPF, DKIM et DMARC

Le spam est un problème moderne. Il existe plusieurs techniques pour atténuer le spam. De telles techniques sont indispensables à mettre en œuvre. Ne pas mettre en œuvre une politique appropriée entraînera une livraison du courrier problématique.

Divers enregistrements de texte DNS (TXT) sont nécessaires à la bonne distribution du courrier. L'enregistrement SPF est crucial et doit inclure le FQDN ou l'IPv4 public du VPS en tant qu'expéditeur autorisé. DMARC et DKIM sont deux autres protocoles essentiels. Ce dernier peut être facilement activé via ISPConfig. Une fois activée, une signature numérique est attachée au corps et à l'en-tête de chaque message sortant pour le domaine de messagerie en question. ISPConfig générera l'enregistrement DNS requis qui doit être publié dans DNS (la publication de l'enregistrement DNS n'est pas un événement automatique).

DMARC établit une politique informant les passerelles MX de réception sur ce qu'il faut faire avec tout message entrant qui ne peut pas être validé conformément à DKIM ou SPF. Cela peut impliquer de rejeter ou de mettre en quarantaine tout le courrier non validé. La politique DMARC est publiée dans DNS et peut inclure une adresse e-mail à laquelle les systèmes de messagerie peuvent signaler les messages rejetés. Ceci est précieux pour l'opérateur du domaine car cela permet de surveiller la livraison des messages.

Les détails sont brièvement décrits dans les paragraphes suivants. Bien qu'une certaine redondance existe dans l'élaboration, elle a pour objectif d'expliquer le sujet quelque peu complexe en utilisant une terminologie différente, tout en restant concis.

5.3.3.1. SPF (cadre de politique de l'expéditeur)

SPF est un mécanisme permettant d'empêcher la falsification de l'adresse de l'expéditeur. Il permet aux propriétaires de domaines de spécifier quels serveurs de messagerie sont autorisés à envoyer des e-mails au nom de leur domaine.

Exemple d'enregistrement SPF :

v=spf1 ip4:203.0.113.101 include:_spf.example.com -all

Dans cet exemple, l'enregistrement SPF indique que le courrier peut être envoyé à partir de l'adresse IPv4 203.0.113.101 et inclut les enregistrements SPF de _spf.example.com. Le -all indique un échec matériel, ce qui signifie que si le serveur n'est pas répertorié dans l'enregistrement SPF, l'e-mail sera rejeté.

5.3.3.2. DKIM (courrier identifié par DomainKeys) :

DKIM ajoute une signature numérique aux e-mails, permettant au destinataire de vérifier que le message n'a pas été modifié pendant le transit et qu'il provient réellement du domaine dont il prétend provenir.

Exemple d'enregistrement DKIM :

v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCxLXFhjjUrU4yEh28qOrSXrJAEi9YZ5zOZkx3WENrRIZ6jyBQT35gYWvDjM6TAgDgSpwCjtgmAwr6JuFTEPTXvmSUGuJrkSj9rgjrgE+HxHjYsPFJmlq IwI+ywOo5e3C5L8vJzWvI98ZAF/ZdD+XW+D

Il s'agit d'une clé publique DKIM. La clé privée est utilisée pour signer les emails sortants et la clé publique est publiée dans le DNS. Le sélecteur (s=) est souvent utilisé pour identifier la clé spécifique pour un service d'envoi donné.

5.3.3.3. DMARC (authentification, reporting et conformité des messages basés sur le domaine) :

DMARC s'appuie sur SPF et DKIM pour fournir aux expéditeurs d'e-mails un moyen d'authentifier leurs e-mails et de demander des rapports sur les e-mails qui échouent dans les tentatives d'authentification.

Exemple d'enregistrement DMARC :

v=DMARC1; p=quarantaine ; rua=mailto:dmarc@example.com; ruf=mailto:dmarc-forensics@example.com; sp=quarantaine ; adkim=s; aspf=s; fo=1

Cet enregistrement DMARC demande que les e-mails ayant échoué à l'authentification soient mis en quarantaine, et que les rapports globaux et médico-légaux soient envoyés à dmarc@example.com et dmarc-forensics@example.com, respectivement. L'adkim et l'aspf spécifient un alignement strict pour DKIM et SPF.

N'oubliez pas de remplacer les exemples de domaines, de clés et d'adresses e-mail par vos informations réelles. De plus, la propagation des enregistrements DNS peut prendre un certain temps, il est donc conseillé de tester et de surveiller la mise en œuvre.

Lectures complémentaires : SIDN a publié un article informatif sur les différents protocoles permettant d'assurer la sécurité du trafic de courrier.

5.3.4. Interrogation des enregistrements DNS

Sous Linux, la commande « dig » peut être utilisée pour interroger les enregistrements DNS. C'est très utile, car cela permet de voir comment les choses ont été mises en place par les autres partis.

Microsoft utilise par exemple le domaine contoso.com dans de nombreuses documentations. Il est utile d'effectuer des requêtes sur le domaine contoso pour savoir à quoi ressemblent les enregistrements DNS.

5.3.4.1. Exemple : interrogation d'un enregistrement de contoso.com :

```
dig A contoso.com.
```

Resultats :

```
; <<>> DiG 9.19.17-1-Debian <<>> A contoso.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46943

;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;contoso.com. IN A

;; ANSWER SECTION:
contoso.com. 3394 IN A 20.112.250.133
contoso.com. 3394 IN A 20.236.44.162
contoso.com. 3394 IN A 20.231.239.246
contoso.com. 3394 IN A 20.70.246.20
contoso.com. 3394 IN A 20.76.201.171

;; Query time: 0 msec
;; SERVER: 172.21.1.1#53(172.21.1.1 (UDP
;; [..]
```

5.3.4.2. Exemple : interrogation de l'enregistrement CNAME de www.contoso.com :

```
dig cname www.contoso.com.
```

Restults in:

```
; <<>> DiG 9.19.17-1-Debian <<>> cname www.contoso.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2164
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.contoso.com. IN CNAME

;; ANSWER SECTION:
www.contoso.com. 3600 IN CNAME contoso.com.

;; Query time: 24 msec
;; SERVER: 172.21.1.1#53(172.21.1.1) (UDP)
;; [..]
```

5.3.4.3. Incorporer `grep`

Nous pouvons facilement trouver l'enregistrement SPF pour contoso.com en incorporant la commande « grep » à la commande « dig ».

```
dig TXT contoso.com | grep spf
```

Résulte en:

```
contoso.com. 3030 DANS TXT "v=spf1 include:spf.protection.outlook.com -all"
```

5.3.4.4. Utiliser d'autres outils

Il existe d'autres outils qui nous permettent de faire nos recherches sur les enregistrements DNS.

DNSdumpster.com

Un exemple est le site Web DNSdumpster.com. DNSdumpster.com est un outil de recherche de domaine GRATUIT qui permet de découvrir des hôtes liés à un domaine. La recherche d'hôtes visibles du point de vue des attaquants est une partie importante du processus d'évaluation de la sécurité.

MXToolbox.com

MXToolbox.com peut être utilisé comme un outil pour vérifier la validité des enregistrements MX et détecter les problèmes de courrier.

Mail-Tester.com

Mail-Tester.com est lié à MXToolbox.com . Les outils nous permettent de tester la distribution du courrier. C'est un bon test pour vérifier si la signature DKIM fonctionne.

6. Services internes

À mesure que nous progressons dans la configuration de notre infrastructure informatique, nous tournons désormais notre attention vers les services internes.

Un aspect clé du support aux utilisateurs finaux implique la gestion centralisée des ordinateurs et des comptes d'utilisateurs. Lorsqu'il s'agit d'environnements centrés sur Windows, l'introduction d'Active Directory devient un choix logique. Alternativement, on peut envisager Microsoft Azure AD et Microsoft 365. Une autre option consiste à implémenter un système de surveillance et de gestion à distance (RMM), en déployant un agent sur chaque ordinateur. Dans certains scénarios, une combinaison de gestion Microsoft 365 et RMM peut s'avérer efficace.

Ces considérations nécessitent une évaluation minutieuse. Cependant, pour les besoins de cet article, nous mettrons en place un contrôleur de domaine, en optant pour une approche lean avec le Samba DC, en nous éloignant du Serveur Windows classique.

6.1. Contrôleur de domaine Samba

Traditionnellement, un serveur Windows sert de contrôleur de domaine, gérant l'authentification des utilisateurs, les services DNS et DHCP. Dans les environnements plus petits, un seul contrôleur de domaine suffit, mais il est préférable d'en avoir au moins deux pour la redondance.

La configuration de Samba en tant que contrôleur de domaine Active Directory implique un travail en ligne de commande sur le terminal Linux. Cependant, l'administration quotidienne peut être effectuée à partir d'un ordinateur Windows Pro sur lequel les outils d'administration de serveur distant (RSAT) sont installés, facilitant ainsi l'utilisation d'outils tels que les utilisateurs et ordinateurs Active Directory (dsa.msc) et la console de gestion des stratégies de groupe.(gpmc.msc). Cela permet également l'application de stratégies de groupe.

La documentation SambaWiki offre des conseils complets sur la configuration d'un contrôleur de domaine sous Debian Linux. Il répertorie même les packages Debian à installer dans la section Listes de packages spécifiques à la distribution gérées manuellement .

Notez que la réplication SysVol n'est pas implémentée dans Samba. Pour résoudre ce problème, réplication SysVol bidirectionnelle à l'aide de RSync et Unison être prêt.

6.1.1. Créer un conteneur

Pour créer un conteneur, suivez un processus similaire à celui décrit au paragraphe 5.2.2. La principale différence est de décocher l'option de conteneur non privilégié.

- Click "Create CT" to initiate a new container.
- Enter the required settings.

General

1. Enter the CT ID: 201
2. Enter hostname: sdc1
3. Unpriviledged container: **uncheck** [this is important]
4. Enter and confirm the desired root password
5. Click Next

Note: in this case a privileged container is used. The resources outside the container can be changed. If this aspect does not appeal to you, it is better to opt for a VM instead of a Container.

Template

6. Select the template: debian-12-standard_12.2-1_amd64.tar.zst
7. Click Next

Disks

8. Select the storage (in our case it is "storage")
9. Set the disk size (GB): eg "48"
10. Click Next

CPU

11. Set the cores: e.g. "4"
12. Click Next

Memory

13. Set the amount of Memory (MiB): e.g. "8192"

    Note: Allocate ample RAM initially for the database repacking process, which requires a significant amount of RAM during provisioning.

14. Set swap (MiB): e.g. "8192"
15. Click Next

Network

16. Leave the name and brdige as they are
17. Set VLAN Tag: 16
18. Enter the IPv4/CIDR: 10.10.16.201/24
19. Enter the gateway IPv4: 10.10.16.1
20. Click Next

DNS

21. Enter the DNS domain: e.g. "ad.lan.gigabitjes.nl"
22. Enter the DNS server: 10.10.16.1
23. Click Next

Confirm

24. Review and confirm the options by clicking on Finish.

- Select the new container and click "Console".
- Click "Start" to start the container.

6.1.2. Préparatifs et contrôles

Accédez au conteneur en cliquant dessus (sdc1) et en sélectionnant « Console ». Connectez-vous en tant que root.

6.1.2.1. Mettre à jour sources

Editez le fichier apt sources.list

```
nano /etc/apt/sources.list
```

Update it to reflect the following list:

deb http://deb.debian.org/debian bookworm main contrib non-free

deb http://deb.debian.org/debian bookworm-updates main contrib non-free

deb http://security.debian.org bookworm-security main contrib non-free

deb http://deb.debian.org/debian bookworm-backports main contrib non-free

6.1.2.2. Paquets

Pour les conteneurs, il n'est pas nécessaire d'installer un nouveau noyau. Ignorez les étapes liées au noyau et passez à l'étape suivante.

Lorsqu'une VM est utilisée, vous pouvez envisager d'installer le dernier noyau cloud. Recherchez le dernier noyau Linux bruyant avec la commande suivante :

```
apt update && apt-cache search linux-image | grep "cloud"
```

Choisissez et installez la dernière version. Au moment de la rédaction, il s'agissait de "linux-image-6.5.0-0.deb12.4-cloud-amd64" :

```
apt -y install linux-image-6.5.0-0.deb12.4-cloud-amd64
```

6.1.2.2.2. Mise à niveau des packages

```
apt update && apt -y upgrade
```

6.1.2.3. Masquer la connexion système

```
systemctl mask systemd-logind
```

Cela résout les redémarrages et les connexions lents. Ignorez le message d'erreur concernant dbus après avoir émis la commande reboot ; il est sécuritaire de le faire.

6.1.2.4. Redémarrez le conteneur.

```
reboot
```

6.1.2.4. Vérifier les paramètres

Connectez-vous en tant que root et vérifiez les paramètres du conteneur.

Après le redémarrage, connectez-vous en tant que root et vérifiez les paramètres essentiels du conteneur. Corrigez toutes les erreurs via l'interface utilisateur Web de Proxmox plutôt que via la console du conteneur.

6.1.2.4.1. Vérifier le nom d'hôte et les paramètres réseau

```
hostname && hostname -f
```

Cela doit refléter le nom d'hôte (par exemple, « sdc1 ») et le nom de domaine complet (FQDN) avec le suffixe (par exemple, « sdc1.ad.lan.gigabitjes.nl »).

sdc1
sdc1.ad.lan.gigabitjes.nl

6.1.2.4.2. Vérifier les paramètres réseau

```
ip a
```

Cela devrait afficher l'adresse IPv4 et le CIDR, par exemple :

```
 [..]
2: eth0@if28: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000  link/ether
bc:24:11:0c:56:f2 brd ff:ff:ff:ff:ff:ff link-netnsid 0
 inet 10.10.16.201/24 brd 10.10.16.255 scope global eth0
 valid_lft forever preferred_lft forever
[..]
```

6.1.2.4.3. Vérifier l'itinéraire par défaut

```
spectacle de route IP
```

Cela doit refléter la passerelle par défaut, telle que :

par défaut via 10.10.16.1 dev eth0 onlink
10.10.16.0/24 dev eth0 proto noyau portée lien src 10.10.16.201

6.1.2.4.4. Vérifier le DNS

Vérifiez le contenu du fichier resolv.conf :

```
cat /etc/resolv.conf
```

Cela devrait répertorier le domaine de recherche et le serveur de noms :

[..]
rechercher ad.lan.gigabitjes.nl
serveur de noms 10.10.16.1
[..]

Assurez-vous que la résolution DNS fonctionne :

```
creuser + court contoso.com.
```

Cela devrait répertorier une ou plusieurs adresses IPv4.

20.70.246.20
20.76.201.171
20.112.250.133
20.236.44.162
20.231.239.246

Vérifiez la résolution, car elle est cruciale.

6.1.3. Installation et configuration de Samba

Les étapes suivantes sont dérivées de Configuration de Samba en tant que contrôleur de domaine Active Directory.

6.1.3.1. Installer les packages requis

```
apt update && apt -t bookworm-backports -y install acl attr samba winbind libpam-winbind libnss-winbind krb5-config krb5-user dnsutils python3-setproctitle net-tools smbclient
```

Lors de la configuration du package, appuyez sur Entrée lorsque vous êtes invité à saisir les détails relatifs à Kerberos. Le fichier de configuration Kerberos sera écrasé après le provisionnement de Samba AD.

[..]
Configuration du package : configuration de l'authentification Kerberos

6.1.3.2. Approvisionnement de Samba AD

Lancez le processus de provisionnement interactif :

```
samba-tool domain provision --use-rfc2307 --interactive
```

Appuyez sur Entrée pour le domaine, le domaine, le rôle de serveur, le backend DNS et le redirecteur DNS. Saisissez et confirmez le mot de passe.

Realm: AD.LAN.GIGABITJES.NL
Domain: AD
Server Role: dc
DNS backend: SAMBA_INTERNAL
DNS forwarder IP address: 10.10.16.1
Administrator password: $trongPas5w0rd!
Retype password

Le processus devrait prendre quelques secondes à quelques minutes.

Le processus devrait prendre quelques secondes à quelques minutes. Si cela prend plus de temps (heures), il peut y avoir un problème de disponibilité de la RAM lors du reconditionnement de la base de données. Dans de tels cas, supprimez le conteneur, ajoutez plus de RAM et idéalement plus de processeurs avant de recommencer.

6.1.3.3. Configurer Kerberos

Copiez le fichier de configuration généré sur le fichier existant :

```
cp /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

6.1.3.4. Démarrez le service Samba

Exécutez les commandes suivantes :

```
systemctl enable samba-ad-dc
systemctl start samba-ad-dc
```

Certains processus nécessaires peuvent ne pas s'exécuter. Redémarrez le conteneur :

```
reboot
```

6.1.3.5. DNS (pfSense)

Pour le transfert DNS, assurez-vous que les requêtes pour le domaine sont redirigées vers le contrôleur de domaine. Ajoutez un remplacement de domaine dans pfSense :

1. Open pfSense
2. Click "Services" > "DNS Resolvers"
3. Scroll down and add the following domain override by clicking add.
    - Domain: ad.lan.gigabitjes.nl
    - IP Address: 10.10.16.201
    - Description: Active Directory
4. Save and Apply Changes

Nous ajouterons également une entrée de remplacement de domaine pour la zone de recherche inversée :

1. Click "Services" > "DNS Resolvers"
2. Scroll down and add the following domain override by clicking add.
    - Domain: 16.10.10.in-addr.arpa
    - IP Address: 10.10.16.201
    - Description: Active Directory - Reverse Zone Lookup
3. Save and Apply Changes

C'est également une bonne idée de définir le nom de domaine et la liste de recherche de domaine dans DHCP pour le réseau local du bureau (L1_0032_OFF1) dans pfSense.

1. Click "Services" > "DHCP Server"
2. Click "L1_0032_OFF1"
3. Scroll down to the section "Other DHCP Options"
4. Enter the following at "Domain Name" option:
   ad.lan.gigabitjes.nl
5. Enter the following at "Domain Seach List" option:
   lan.gigabitjes.nl
6. Save and Apply Changes

Cette configuration est avantageuse pour les scénarios avec des hôtes associés à différents suffixes de domaine, rationalisant le processus d'accès aux ressources sur différents sous-domaines.

6.1.3.6. DNS (contrôleur de domaine)

Connectez-vous à la console du nouveau contrôleur de domaine pour ajouter une zone inversée et un enregistrement de pointeur.

Dans les exemples, nous travaillerons avec le sous-réseau « 10.10.16.0/24 », en inversant les octets de l'adresse IPv4 et en n'utilisant pas le quatrième octet. Le suffixe est toujours « .in-addr.arpa ».

6.1.3.6.1. Créez une zone inversée :

```
samba-tool dns zonecreate sdc1 16.10.10.in-addr.arpa -U Administrator
```

Résultat:

```
Password for [AD\Administrator]:
Zone 16.10.10.in-addr.arpa created successfully
```

6.1.3.6.2. Ajouter un enregistrement de pointeur (PTR) :

```
samba-tool dns add sdc1 16.10.10.in-addr.arpa 201 PTR sdc1.ad.lan.gigabitjes.nl -U Administrator
```

Résultat:

```
Password for [AD\Administrator]:
Record added successfully
```

6.1.4. Configuration de NTP

Les conteneurs partagent l'horloge de leur système hôte. Vous n'avez pas besoin d'exécuter ntpd dans un conteneur.

Supprimez tous les démons NTP :

```
apt -y remove --purge systemd-timesyncd chrony ntp
```

Une synchronisation correcte de l'heure est très importante. Assurez-vous que NTP fonctionne correctement sur l'hyperviseur (hôte) et sur le pare-feu pfSense. Configurez de préférence les mêmes sources NTP.

6.1.5. Test du nouveau contrôleur de domaine Active Directory

Connectez-vous à la console du nouveau contrôleur de domaine pour exécuter des tests et vous assurer que tout fonctionne comme prévu.

6.1.5.1. Liste des partages :

```
smbclient -L localhost -N
```

Result:

```
Anonymous login successful
Sharename Type Comment
--------- ---- -------
sysvol Disk
netlogon Disk
IPC$ IPC IPC Service (Samba 4.19.3-Debian)
SMB1 disabled -- no workgroup available
```

6.1.5.2. Vérifiez l'authentification :

```
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

Result:

```
Password for [AD\Administrator]:
  .   D 0 Sun Jan 7 21:00:46 2024
.. D 0 Sun Jan 7 21:00:46 2024
50331648 blocks of size 1024. 49794560 blocks available
```

6.1.5.3. Vérifier le DNS

Un système de noms de domaine (DNS) robuste et efficace est indispensable.

6.1.5.3.1. Interrogez l'enregistrement SRV _ldap basé sur TCP dans le domaine :

```
host -t SRV _ldap._tcp.ad.lan.gigabitjes.nl.
```

Result:

```
_ldap._tcp.ad.lan.gigabitjes.nl has SRV record 0 100 389 sdc1.ad.lan.gigabitjes.nl.
```

Instead of `host` the command `dig`can be used too.

```
dig SRV _ldap._tcp.ad.lan.gigabitjes.nl.
```

Result:

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> SRV _ldap._tcp.ad.lan.gigabitjes.nl.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7431
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_ldap._tcp.ad.lan.gigabitjes.nl. IN SRV

;; ANSWER SECTION:
_ldap._tcp.ad.lan.gigabitjes.nl. 312 IN SRV 0 100 389 sdc1.ad.lan.gigabitjes.nl.

;; Query time: 0 msec
;; SERVER: 10.10.16.1#53(10.10.16.1 (UDP
;; WHEN: Mon Jan 08 20:33:02 UTC 2024
;; MSG SIZE rcvd: 105
```

6.1.5.3.2. Interrogez l'enregistrement de ressource _kerberos SRV basé sur UDP dans le domaine :

```
host -t SRV _kerberos._udp.ad.lan.gigabitjes.nl.
```

Result:

```
_kerberos._udp.ad.lan.gigabitjes.nl has SRV record 0 100 88 sdc1.ad.lan.gigabitjes.nl.
```

6.1.5.3.3. Interrogez l'enregistrement A du contrôleur de domaine :

```
host -t A sdc1.ad.lan.gigabitjes.nl.
```

Result:

```
sdc1.ad.lan.gigabitjes.nl has address 10.10.16.201
```

6.1.5.3.4. Interroger l'enregistrement PTR du contrôleur de domaine

```
host -t PTR 10.10.16.201
```

Result:

```
201.16.10.10.in-addr.arpa domain name pointer sdc1.ad.lan.gigabitjes.nl.
```

Cela fonctionne comme prévu car nous avons ajouté une entrée de remplacement pour la zone de recherche inversée (6.1.3.5).

6.1.5.3.5. Vérifiez Kerberos :

```
klist
```

Result:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@AD.LAN.GIGABITJES.NL

Valid starting Expires Service principal
01/07/24 21:34:31 01/08/24 07:34:31 krbtgt/AD.LAN.GIGABITJES.NL@AD.LAN.GIGABITJES.NL
 renew until 01/08/24 21:34:24
```

6.1.6. Rejoindre un DC Samba à un Active Directory existant

La prochaine révision du document intégrera le processus décrit. À l'heure actuelle, une description détaillée n'est pas fournie.

6.1.6.1. Approvisionnement de Samba AD

Il est recommandé de configurer un contrôleur de domaine secondaire. La procédure est similaire à celle décrite dans le paragraphe précédent et est détaillée dans SambaWiki sous Rejoindre un DC Samba.
à un Active Directory existant

6.1.6.2. Réplication SysVol

Portez une attention particulière à la réplication SysVol, comme expliqué dans le SambaWiki sous Réplication SysVol (DFS-R).

6.2. Serveur de fichiers

Compte tenu du rôle central de la gestion de fichiers dans notre environnement, un serveur de fichiers traditionnel reste indispensable. Malgré l'évolution contemporaine vers des solutions basées sur le Web comme Microsoft 365, Google Workspace ou des alternatives auto-hébergées telles que NextCloud ou ownCloud, cet article se concentre sur le choix entre TrueNAS et Samba. OuvrirMediaVault (OMV) est également à l'étude, mais il ne répond pas à nos besoins en raison du manque de support officiel pour Active Directory.

Pour rester bref et s'aligner sur les principes Lean de notre configuration, Samba apparaît comme le choix préféré par rapport à TrueNAS.

Une fois le serveur de fichiers opérationnel, notre attention se porte sur le prochain chapitre : « Utilisateurs et ordinateurs ». La première étape consiste à intégrer un ordinateur Windows dans Active Directory basé sur Samba, en approfondissant les subtilités du partage de fichiers.

Dans les sections précédentes, nous avons utilisé des conteneurs. Nous allons plutôt créer une VM pour notre serveur de fichiers. Ensuite, nous installerons Debian Linux à partir d'une image ISO. Enfin, nous installerons Samba et le provisionnerons en tant que serveur de fichiers joint à un domaine.

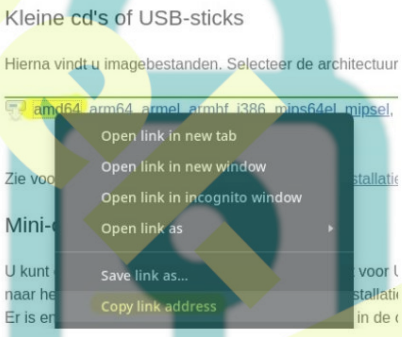
6.2.1. Créer une VM

L'exécution d'une VM diffère de l'exécution d'un conteneur, même si elle partage un objectif commun. Une distinction notable réside dans l'utilisation d'un fichier ISO au lieu d'un modèle. Commençons par obtenir le fichier ISO nécessaire.

6.2.1.1. Téléchargez l'ISO Debian NetInst

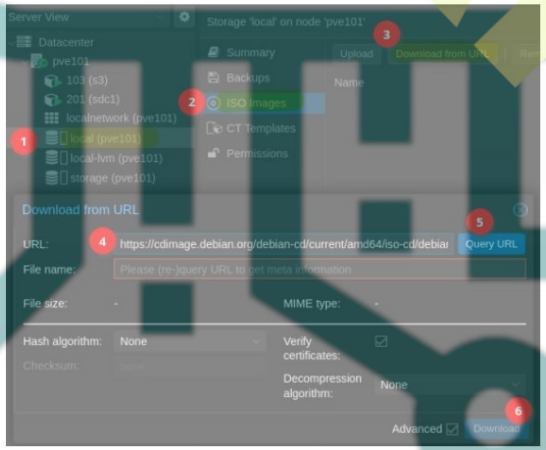
Pour commencer, identifiez l'URL du fichier ISO requis :

1. Accédez à https://www.debian.org/distrib/netinst.
2. Faites un clic droit sur amd64 et cliquez sur « Copier l'adresse du lien » (voir capture d'écran).



Ensuite, collez l'URL dans Proxmox :

1. Accédez au stockage local 2.
Accédez à « Images ISO »
3. Choisissez « Télécharger depuis l'URL »
4. Collez l'URL dans le champ URL
5. Cliquez sur « URL de requête »
6. Enfin, sélectionnez « Télécharger »



6.2.1.2. Créer une VM

Créons la VM :

- Cliquez sur "Créer une VM"

- Général:
  - ID de machine virtuelle : 301
  - Nom : fichier1
  - Cliquez sur Suivant'
- ——
  - Sélectionnez l'image ISO : debian-xx.yz-amd64-netinst.iso Cliquez
  - sur "Suivant".
- Système:
  - Contrôleur SCSI : VirtIO SCSI
  - Cochez la case 'Agent Qemu'
  - Cliquez sur Suivant'
- Disque:

- Stockage : stockage
- Taille du disque (Gio) : par exemple
- 640 Cache : réécriture
- Cliquez sur « Suivant »

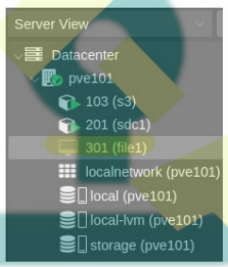
- Processeur : Prises : 1
  - Noyaux : 4
  - Cliquez sur Suivant'
- Mémoire:
  - Mémoire (Mio) : 2048
  - Mémoire minimale (MiB) : 2048
  - Cliquez sur Suivant'
- Réseau:
  - Pont : vmbr0
  - Balise VLAN : 16
  - Modèle : Intel E1000 (pas « virtio » ; ne fonctionne pas)
  - Cliquez sur Suivant'
- Confirmer
  - Revoir
  - Cliquez sur "Terminer"

Veuillez être partie prenante pendant la création de la VM.

6.2.1.3. Installer Debian à partir de l'ISO

Démarrez la VM :

1. Select '301 (file1)' from the list
2. Select 'Console'
3. Click 'Start Now'

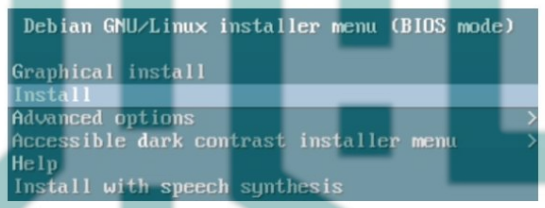


Processus d'installation:

L'hypothèse est que vous appuyez sur Entrée pour exécuter les étapes décrites ci-dessous. Le déclarer explicitement à chaque étape pourrait être excessif. Utilisez les touches fléchées et la touche de tabulation pour sélectionner les options.

1. Debian Installer:

   Sélectionnez « Installer » une fois que le programme d'installation Debian apparaît



2. Select a language

   Select the prefered language:
   e.g. English

3. Select your location

   Select the prefered country:
   e.g. Other > Europe > Netherlands

4. Configure locales

   Select system local:
   e.g. United States

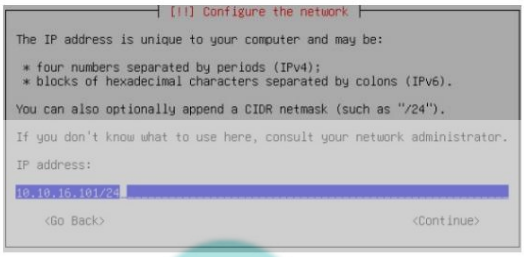
5. Configure keyboard

   Select the keyboard:
   e.g. American English

6. Configure the network

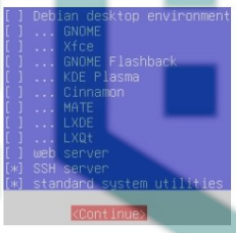
   - Le programme d'installation se plaindra de l'échec de la configuration automatique. C'est correct car DHCP n'est pas activé (dans pfSense).
     Appuyez sur Entrée, et continuer...

- The default selection is 'Configure network manually'
  Press Enter to continue...
- IP address:
  10.10.16.101/24



- Gateway:
- *10.10.16.1*
- Name server address (mind the space):
  10.10.16.201 10.10.16.1

7. Hostname:
   - Hostname:
     file1
8. Domain name
   - Domain name:
     ad.lan.gigabitjes.nl
9. Set up users and Passwords
   - Enter the root password:
     ****
   - Re-enter the root password:
     ****
   - Enter the full name of new user:
     Maintenance User
   - Enter the username of the account:
     main
   - Enter the new password for the new user:
     ****
   - Re-enter the same password [..]
     ****
   - Partitioning method:
     Guided - user entire disk
   - Select disk partition:
     SCSI [..] QEMU HARDDISK
   - Partitioning Scheme:
     All files in one partition [..]
   - Overview:
     Finish partitioning and write changes to disk
   - Write changes to disk?
     Yes
   - Scan extra installation media?
     No
   - Select mirror
     E.g. 'Netherlands'
   - Debian Archive mirror:
     E.g. 'deb.debian.org' or one of the other available options
   - HTTP Proxy information
     Just press Enter
   - Participate in the package usage survey?
     No
   - Deselect: Debian desktop environment
   - Deselect: GNOME
   - Select: SSH server
   - Keep selected: standard system utilities



14. Configuring grub-pc
    - Install the GRUB boot loader to your primary drive?
      Yes
    - Device for boot loader installation:
      /dev/sda (scsi-QEMU [..])
15. Finishing installation
    - Please chose <Continue> to reboot
      Press Enter

La VM va redémarrer. Continuons avec la section suivante.

6.2.2. Configurer Debian

Nous exécuterons des commandes à la fois en tant qu'utilisateur et en tant que root. Chaque commande commençant par un "$" sera en mode utilisateur. Chaque commande commençant par "#" est exécutée en tant que root.

6.2.2.1. Se connecter

Utilisez SSH pour vous connecter au serveur de fichiers. Depuis un terminal Linux, vous pouvez facilement vous connecter avec la commande suivante :

```
$ ssh main@10.10.16.101
```

Vous pouvez également utiliser PuTTY ou vous connecter via la console dans Proxmox.

Acceptez l'empreinte digitale lorsque cela vous est demandé.

6.2.2.2. Ajouter un utilisateur à la liste des sudoers

Nous ajouterons l'utilisateur principal à la liste des sudoers.

Nous allons d'abord installer `sudo` :

1. $ su -
2. Enter the root password
3. # apt update
4. # apt install sudo

Nous sommes maintenant prêts à ajouter l'utilisateur au groupe suoers :

1. # adduser main sudo
2. # exit; exit

Avec la commande `exit; exit` nous nous déconnecterons. Cela mettra fin à la session SSH root et principale.

Connectez-vous à nouveau et testez si sudo fonctionne :

1. $ ssh main@10.10.16.101
2. $ sudo su
3. Enter the password of user main to elevate

6.2.2.3. Vérifier et corriger les paramètres

Vérifiez le nom d'hôte, avec et sans préfixe :

```
hostname && hostname -f
```

Result:

```
file1
file1.ad.lan.gigabitjes.nl
```

Verify the IPv4 address:

```
# ip a
```

Result:

```
[..]
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether bc:24:11:10:15:34 brd ff:ff:ff:ff:ff:ff
 altname enp0s18
 inet 10.10.16.101/24 brd 10.10.16.255 scope global ens18
[..]
```

Verify DNS resolving:

```
# cat /etc/resolv.conf
```

Result:

```
search ad.lan.gigabitjes.nl
nameserver 10.10.16.201
nameserver 10.10.16.1
```

Note : Le premier serveur de noms IPv4 se rapporte au contrôleur de domaine. Le second serveur de noms IPv4 se rapporte au résolveur DNS fonctionnant sur le pare-feu.
Vérifiez et corrigez la permutation :

```
# cat /proc/sys/vm/swappiness
```

Result:

```
60
```

Change this to something sensible:

```
# echo 10 > /proc/sys/vm/swappiness
# sysctl -p
# cat /proc/sys/vm/swappiness
```

Result:

```
10
```

Store the settings to file:

```
# echo "vm.swappiness=10" >> /etc/sysctl.d/80-sysctl-swappiness.conf
```

Note : Le fichier 80-sysctl-swappiness.conf sera appliqué au moment du démarrage.

6.2.2.4. NTP

La gestion du temps est cruciale. Le service NTP par défaut est systemd-timesyncd. Configurons rapidement systemd-timesyncd pour notre serveur de fichiers.

- Même si systemd-timesyncd est déjà installé, cela ne fera pas de mal d'exécuter la commande d'installation :
  apt installer systemd-timesyncd
- Maintenant, modifions timesyncd.conf :
  nano /etc/systemd/timesyncd.conf
- Décommentez les lignes NTP et FallbackNTP et définissez le serveur NTP sur 10.10.16.1.

```
NTP=10.10.16.1
FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
```

- Vérifiez la configuration :

```
timedatectl show-timesync --al
```

- Activez et démarrez systemd-timesyncd :

```
timedatectl set-ntp true
```

- Pour faire bonne mesure, activez et redémarrez de force systemd-timesyncd :

```
systemctl enable systemd-timesyncd
systemctl restart systemd-timesyncd
```

- Vérifiez l'état :

```
systemctl startus systemd-timesyncd
```

- Et l'état de synchronisation :

```
timedatectl timesync-statut
```

Cela garantit que notre serveur de fichiers est bien synchronisé avec l'heure du réseau.

6.2.3. Installer et configurer le serveur de fichiers Samba

Vous exécuterez probablement toujours des commandes en tant que root. Entrez « exit » pour revenir au mode utilisateur :

```
# exit
```

Installez les packages requis :

```
$ sudo apt update && sudo apt -y install acl samba winbind libnss-winbind krb5-user
```

Configurez Kerberos :

```
$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak
$ sudo nano /etc/krb5.conf
```

Ajoutez les lignes suivantes et enregistrez les modifications :

```
[libdefaults]
 default_realm = AD.LAN.GIGABITJES.NL
 dns_lookup_realm = false
 dns_lookup_kdc = true
```

Configurez NSS :

```
$ sudo nano /etc/nsswitch.conf
```

Modifiez les lignes suivantes et enregistrez les modifications :

```
passwd: files winbind
group: files winbind
hosts: files dns wins
```

Configurez Samba :

```
$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
$ sudo nano /etc/samba/smb.conf
```

ajouter les lignes suivantes changer et sauvegarder.

```
# Global parameters
[global]
 dedicated keytab file = /etc/krb5.keytab
 kerberos method = secrets and keytab
 realm = AD.LAN.GIGABITJES.NL
 security = ADS
 server role = member server
 winbind refresh tickets = Yes
 workgroup = AD
 idmap config * : backend = tdb
 idmap config * : range = 3000-7999
 idmap config ad : backend = rid
 idmap config ad : range = 10000 - 999999
 map acl inherit = Yes
 vfs objects = acl_xattr
```

Vérifiez Kerberos (1) :

```
$ sudo kinit administrator
```

Résultat (la sortie peut varier) :

Mot de passe pour administrateur@AD.LAN.GIGABITJES.NL :
Attention : votre mot de passe expirera dans 32 jours le dim. 18 février 2024 22:00:50 CET

Vérifiez Kerberos (2) :

```
$ sudo klist
```

Result (output may vary):

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@AD.LAN.GIGABITJES.NL

Valid starting Expires Service principal
01/17/2024 21:37:46 01/18/2024 07:37:46 krbtgt/AD.LAN.GIGABITJES.NL@AD.LAN.GIGABITJES.NL
```

renew until 01/18/2024 21:37:42
Vérifiez la configuration de Samba

```
$ sudo testparm
```

Result:

```
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
 dedicated keytab file = /etc/krb5.keytab
 kerberos method = secrets and keytab
 realm = AD.LAN.GIGABITJES.NL
 security = ADS
 winbind refresh tickets = Yes
 workgroup = AD
 idmap config * : range = 3000-7999
 idmap config ad : backend = rid
 idmap config ad : range = 10000 - 999999
 idmap config * : backend = tdb
 map acl inherit = Yes
 vfs objects = acl_xattr
```

Rejoindre le domaine

```
$ sudo /usr/bin/samba-tool domain join ad.lan.gigabitjes.nl MEMBER -U administrator
```

Résultat (la sortie peut varier) :

```
Password for [AD\administrator]:
Joined domain ad.lan.gigabitjes.nl (S-1-5-21-1971466082-2551851020-532596661)
```

Redémarrez les services et assurez-vous qu'ils sont démarrés lors du démarrage du système :

```
$ sudo systemctl restart smbd nmbd winbind
$ sudo systemctl enable smbd nmbd winbind
```

Result:

```
Synchronizing state of smbd.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /lib/
systemd/systemd-sysv-install enable smbd

Synchronizing state of nmbd.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /
lib/systemd/systemd-sysv-install enable nmbd

Synchronizing state of winbind.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /
lib/systemd/systemd-sysv-install enable winbind
```

Nous sommes heureux d'annoncer que notre serveur de fichiers a été intégré avec succès au domaine.

6.2.4. Configurer des partages

Il est temps de configurer un partage de fichiers.

Nous allons d'abord préparer un dossier :

```
$ sudo mkdir -p /srv/samba/data
$ sudo chmod -R 775 /srv/samba/data
$ sudo chown -R "AD\administrator":root /srv/samba/data
```

Cette dernière commande ne fonctionnera que lorsque la configuration est correcte. L'administrateur des utilisateurs est un membre du domaine.

Modifiez le fichier smb.conf pour ajouter le partage :

```
$ sudo nano /etc/samba/smb.conf
```

Ajoutez ce qui suit à la fin du fichier et enregistrez les modifications :

```
[Data]
   acl_xattr:ignore system acl = Yes
   acl allow execute always = Yes
   acl group control = Yes
   inherit acls = Yes
   inherit owner = windows and unix
   inherit permissions = Yes
   path = /srv/samba/data
   read only = No
```

C'est une bonne pratique d'activer l'énumération des partages basée sur l'accès. Cela empêche les utilisateurs sans accès en lecture ou en écriture de visualiser les fichiers et les dossiers.

Ajoutez la ligne suivante aux paramètres [globaux]. C'est bien d'être ajouté à la fin de la section :

```
access based share enum = yes
```

Maintenant, testez les modifications :

```
sudo testparm
```

Result:

```
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
 dedicated keytab file = /etc/krb5.keytab
 kerberos method = secrets and keytab
 realm = AD.LAN.GIGABITJES.NL
 security = ADS
 server role = member server
 winbind refresh tickets = Yes
 workgroup = AD
 idmap config ad : range = 10000 - 999999
 idmap config ad : backend = rid
 idmap config * : range = 3000-7999
 idmap config * : backend = tdb
 access based share enum = Yes
 map acl inherit = Yes
 vfs objects = acl_xattr

[Data]
 acl allow execute always = Yes
 acl group control = Yes
 inherit acls = Yes
 inherit owner = windows and unix
 inherit permissions = Yes
 path = /srv/samba/data
 read only = No
 acl_xattr:ignore system acl = Yes
```

Redémarrez les services

```
$ sudo systemctl restart smbd nmbd winbind
```

La procédure suivante consiste à se connecter à un ordinateur Windows intégré au domaine en tant qu'administrateur. Dans cette étape, nous créerons des dossiers et incorporerons des groupes de domaine ou des utilisateurs de domaine pour faciliter l'accès. Une exploration complète de ce processus sera entreprise dans le prochain chapitre.

7. Gestion des utilisateurs et des ordinateurs

Au sein de notre réseau, les utilisateurs et les ordinateurs jouent un rôle essentiel.

7.1. Machine virtuelle Windows d’administration

Pour commencer, nous devons introduire un ordinateur Windows désigné à des fins administratives. Cette machine particulière sera spécifiquement dédiée aux tâches d'administration.

Dans le cadre de cette configuration, nous lancerons une machine virtuelle exécutant Windows 11 Pro. De plus, vous avez la possibilité de connecter un ordinateur Windows directement au commutateur comme approche alternative.

7.1.1. Obtenir le support d'installation

L'acquisition du support d'installation pour Windows Pro est un processus simple. Le support peut être obtenu sur https://www.microsoft.com/software-download/windows11. Accédez au site, faites défiler vers le bas et choisissez l'option de téléchargement. Plus précisément, sélectionnez « Windows 11 (ISO multi-édition pour les appareils x64) » et cliquez sur « Télécharger maintenant ». Choisissez votre langue préférée et cliquez sur « Confirmer ».

Ne lancez pas le téléchargement en cliquant sur le bouton « Téléchargement 64 bits » ; optez plutôt pour une méthode alternative, cliquez avec le bouton droit et sélectionnez « Copier l'adresse du lien ».

Maintenant, dans Proxmox, désignez le stockage et accédez aux « images ISO ». Optez pour « Télécharger depuis l'URL », collez l'URL copiée dans le champ « URL », puis cliquez sur « URL de requête ». Enfin, lancez le

téléchargez en cliquant sur « Télécharger ». Cela lancera le processus de téléchargement.

7.1.2. Pilotes VirtIO

Nous utiliserons des périphériques virtuels qui nécessitent des pilotes. Cliquez avec le bouton droit sur le lien suivant et choisissez « Télécharger depuis l'URL » : https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso

Maintenant, dans Proxmox, désignez le stockage et accédez aux « images ISO ». Optez pour « Télécharger depuis l'URL », collez l'URL copiée dans le champ « URL », puis cliquez sur « URL de requête ». Enfin, lancez le téléchargement en cliquant sur « Télécharger ». Cela lancera le processus de téléchargement.

7.1.3. Créer une VM

Il est temps de créer la VM pour Windows dans Proxmox :

1. Cliquez sur « Créer une VM »
2. Général : ID
    - de VM : 901
    - Nom : wadm1 Suivant
    -
3. Système d'exploitation :
    - Image ISO : Win11_23H2_English_x64v2.iso Type : Microsoft
    - Windows Version : 11/2022 Cochez
    - l'option « Ajouter un
    - lecteur supplémentaire pour les pilotes VirtIO »
    - Image ISO : virtio-win.iso Suivant 4.
    - Système
    - Carte graphique :
        - sélectionnez « SPICE » si vous souhaitez utiliser le Virtual Machine Viewer.
        - Sélectionnez « Par défaut » si vous souhaitez simplement utiliser la console Proxmox par défaut.
    - Appareil : q35
    - BIOS : OVMF (UEFI)
    - Stockage EFI : stockage
    - Contrôleur SCSI : VirtIO SCSI
    - Cochez l'option 'Agent Qemu'
    - Stockage TPM : stockage
    - Suivant
5. DisksStorage : stockage
    - Taille du disque (Gio) : par exemple "200"
    - Cache : Réécrire Suivant 6.
    - CPU
    - Prises : par exemple "1"
    - Noyaux : par exemple "4"
    - Suivant
7. Mémoire
    - Mémoire (GiB) : par exemple 8192
    - Suivant
8. Réseau
    1. Pont : vmbr0
    2. Balise VLAN : nous n'entrerons pas de balise, car nous voulons exécuter cette VM dans le VLAN de gestion
    3. Modèle : VirtIO (paravirtualisé)
    4. Suivant
9. Confirmer
    - Vérifiez les paramètres et cliquez sur « Terminer »
    - Attendez que la VM soit créée

7.1.4. Installer Windows 11 Professionnel

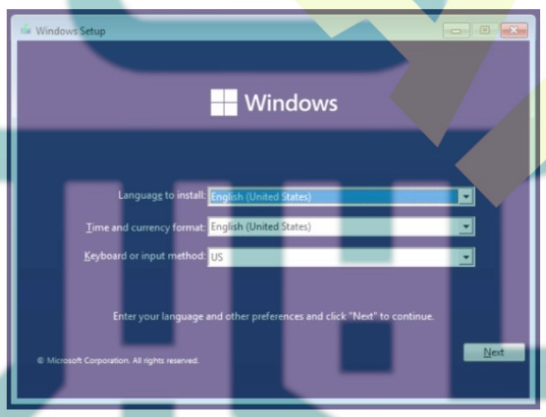
Cliquez sur « Démarrer maintenant » pour lancer la VM. Cliquez rapidement sur l'écran de la console et appuyez sur une touche lorsque vous êtes invité à démarrer à partir du CD/DVD.

Si « SPICE » est sélectionné comme carte graphique, le curseur de la souris peut être flou. Pour résoudre ce problème, cliquez sur la petite flèche vers le bas à côté de « >_ Console » dans le coin supérieur droit de l'écran.
Maintenant, cliquez sur « épice ». Ensuite, ouvrez le fichier dans Virtual Machine Viewer.

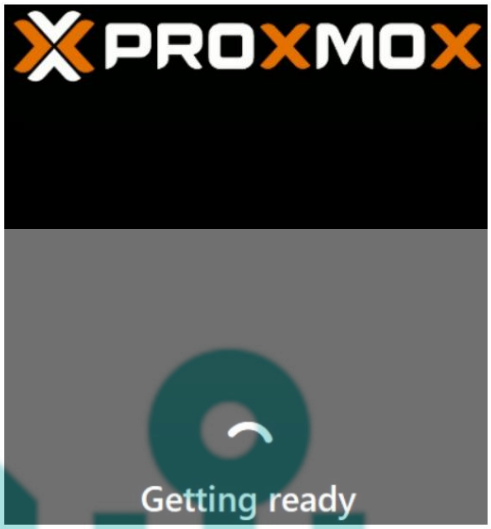
Remarque : appuyez sur "ALT" + "CTRL" + "R" pour libérer le curseur de la souris de Virtual Machine Manager.

Maintenant, procédez à l'installation de Windows comme d'habitude. Chargez le pilote de stockage pour le contrôleur VirtIO SCSI.

1. Entrez la langue et les autres préférences et cliquez sur « Suivant » pour continuer.



2. Cliquez sur « Installer maintenant ».
3. Cliquez sur « Je n'ai pas de clé de produit » lorsque vous êtes invité à saisir la clé de produit.
4. Sélectionnez « Windows 11 Pro » et cliquez sur Suivant.
5. Acceptez la licence et cliquez sur « Suivant ».
6. Cliquez sur « Personnalisé : installer Windows uniquement (avancé).
7. Cliquez sur « Charger le pilote » pour charger le pilote de stockage. Cliquez ensuite sur « OK ». Sélectionnez « Contrôleur pass-through Red Hat VirtIO SCSI (D:\amd64\w11\vioscsi.info) et cliquez sur « Suivant ».
8. Cliquez sur Suivant pour allouer l'espace.
9. Windows s'installera et redémarrera une fois terminé.



Windows lancera l'expérience Out of Box :

1. Appuyez sur « Shift » + « F10 » pour ouvrir une invite de commande

   Remarque : Cette combinaison de touches fonctionne à la fois dans la console Web de Proxmox (noVNC) et dans Virtual Machine Viewer.
   Vous pouvez également appuyer sur « Touche Win » + « R » et exécuter « CMD » via la boîte de dialogue Exécuter.

2. Entrez la commande suivante et appuyez sur Entrée :
   oobe\BypassNRO.cmd

   Windows redémarrera et poursuivra l'expérience Out of Box.
   Cela permet de configurer Windows sans connexion Internet.

3. Sélectionnez le pays ou la région et cliquez sur « Oui »
4. Sélectionnez la disposition du clavier et cliquez sur « Oui »
5. Cliquez sur « Ajouter une disposition » pour ajouter une deuxième disposition de clavier. La sélection par défaut est « Sauter ».
6. Cliquez sur « Je n'ai pas Internet »
7. Cliquez sur « Continuer avec une configuration limitée »
8. Entrez un nom lorsqu'on vous demande qui va utiliser cet appareil : par exemple,
   « LocalAdmin »
9. Cliquez sur

Suivant. 10. Entrez un mot de passe et cliquez sur « Suivant » ; ou alternativement, cliquez simplement sur « Suivant et définissez un mot de passe plus tard.
11. Répondez aux questions (Oui/Non ; Accepter, et cetera).

Windows continuera et vous informera de la progression. Le résultat devrait être quelque chose de similaire à la capture d'écran ci-dessous.

Maintenant, installez les pilotes VirtIO en démarrant « virtio-win-guest-tools » à partir du CD virtio-win :

1. Acceptez les termes de la licence et cliquez sur « Installer ».
2. Cliquez sur « Oui »
3. Cliquez sur « Suivant »
4. Acceptez l'accord et cliquez sur « Suivant »
5. Suivez les instructions à l'écran (en cliquant simplement sur suivant...)

Le résultat est une installation Windows 11 Pro fonctionnant parfaitement.

Une fois les pilotes VirtIO installés, la résolution de l'écran devrait s'améliorer et la connectivité réseau devrait fonctionner.

Vérifiez la connectivité réseau en regardant l'icône de réseau dans le coin inférieur droit de l'écran. Vous pouvez également ouvrir l'invite de commande et interroger la configuration IP avec 'ipconfig /all'. commande.

```
C:\>ipconfig /all
```

Configuration IP Windows

```
Nom d'hôte . . . . . : BUREAU-J6P9KU3
   Suffixe DNS principal. . . . . :
   Type de nœud . . . . . : Hybride
   Routage IP activé. . . . . : Non
   Proxy WINS activé. . . . . : Non
   Liste de recherche de suffixes DNS. . . . . : lan.gigabitjes.nl
```

Adaptateur Ethernet Ethernet :

```
   Suffixe DNS spécifique à la connexion. : ad.lan.gigabitjes.nl
   Description . . . . . : Adaptateur Ethernet Red Hat VirtIO
   Adresse physique. . . . . : BC-24-11-3F-BA-6F
   DHCP activé. . . . . : Oui
   Configuration automatique activée. . . . : Oui
   Adresse IPv6 lien-local. . . . . : fe80::3846:3c84:5c40:3d1a%20 (Souhaité)
   Adresse IPv4. . . . . : 172.21.1.204(Souhaité)
   Masque de sous-réseau . . . . . : 255.255.255.0
   Bail obtenu. . . . . : jeudi 18 janvier 2024 09:05:25
   Le bail expire. . . . . : jeudi 18 janvier 2024 11:05:25
   Passerelle par défaut. . . . . :fe80::20d:b9ff:fe48:3c89%20
                                   172.21.1.1
   Serveur DHCP . . . . . : 172.21.1.1
   DHCPv6 IAID. . . . . : 347874321
   DUID du client DHCPv6. . . . . : 00-01-00-01-2D-3A-94-1D-BC-24-11-3F-BA-6F
   Serveurs DNS . . . . . : 172.21.1.1
   NetBIOS sur TCP. . . . . : Activé
   Liste de recherche de suffixes DNS spécifique à la connexion :
                                   lan.gigabitjes.nl
```

7.1.5. Outils d'administration de serveur distant (RSAT)

Pour gérer les utilisateurs et les ordinateurs et définir des stratégies de groupe pour notre domaine, nous utiliserons PowerShell pour ajouter des fonctionnalités Windows.

Démarrez PowerShell en tant qu'administrateur et recherchez les outils requis :

```
Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property DisplayName, Name, State
```

Installez ces deux outils :

```
Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"
Add-WindowsCapability -Online -Name "Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0"
```

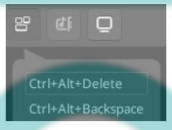
Maintenant, procédez à la connexion de la machine virtuelle Windows à AD.

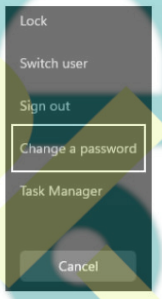
7.1.6. Rejoindre un domaine

S'assurer qu'un compte d'administrateur local est en place est une étape prudente, en particulier en cas d'échec de la relation de confiance entre le poste de travail et le domaine. Procédez en définissant un mot de passe pour le compte utilisateur LocalAdmin.

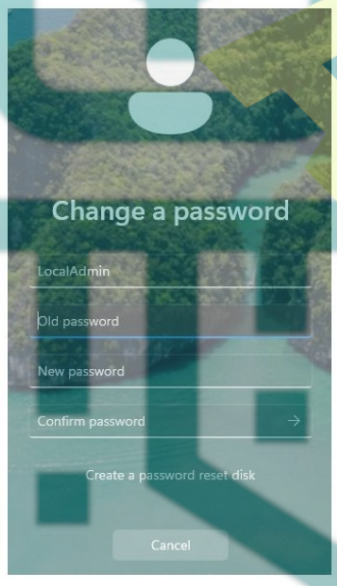
7.1.6.1. Compte administrateur local

Appuyez sur « CTRL » + « ALT » + « SUPPR » dans la VM. Cela peut être exécuté via les boutons à l'écran de noVNC ou le menu de boutons dans Virtual Machine Viewer.





Ensuite, cliquez sur « Modifier un mot de passe ».



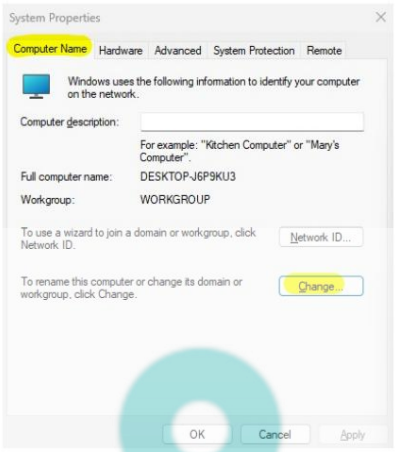
Ignorez simplement « Ancien mot de passe » si aucun mot de passe n'est défini. Saisissez et confirmez le nouveau mot de passe.

7.1.6.2. Rejoindre le domaine informatique

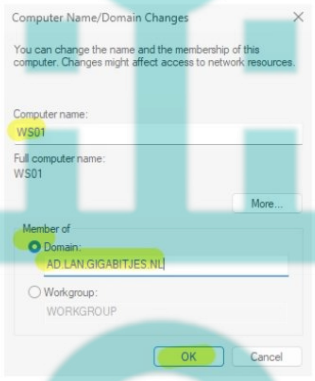
Appuyez sur <Win-key> + <R> et ouvrez les propriétés système :

```
sysdm.cpl
```

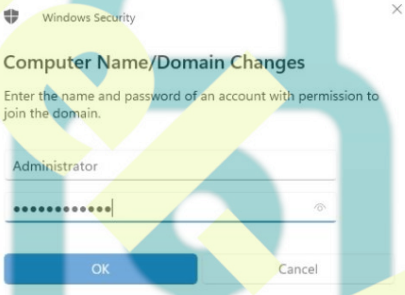
Cliquez sur « Modifier... » dans l'onglet « Nom de l'ordinateur ».



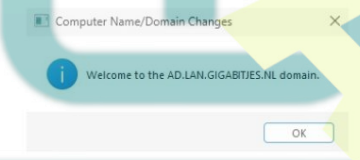
Entrez le nom de l'ordinateur souhaité (par exemple, WS01). Cochez le bouton radio « Domaine » et saisissez le nom de domaine. Enfin, cliquez sur « OK ».

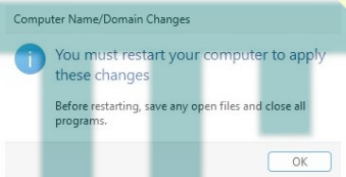


Saisissez le nom d'utilisateur et le mot de passe de l'administrateur du domaine (par défaut : « Administrateur » avec le mot de passe défini lors du provisionnement du domaine).

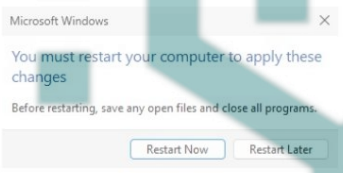


Suivez les instructions à l'écran.

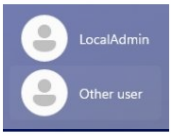




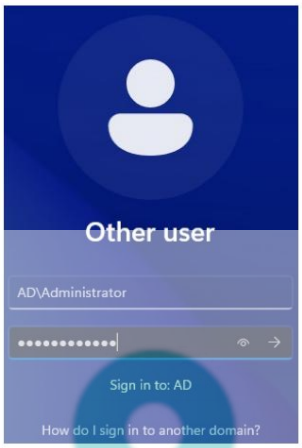
Cliquez sur « Fermer » et « Redémarrer maintenant ».



Après le redémarrage de l'ordinateur, cliquez sur « Autre utilisateur » dans le coin inférieur gauche de l'écran. Connectez-vous avec le compte et le mot de passe de l'administrateur du domaine.



Une mise en garde est nécessaire lors de la connexion avec le nom d'utilisateur « Administrateur » ; ajoutez le nom NetBIOS du domaine au nom d'utilisateur, séparé par une barre oblique inverse (par exemple, "AD\Administrateur"). Vous pouvez également saisir le nom d'utilisateur suivi du FQDN du domaine, séparé par un signe at-(par exemple, "Administrator@AD.LAN.GIGABITJES.NL").



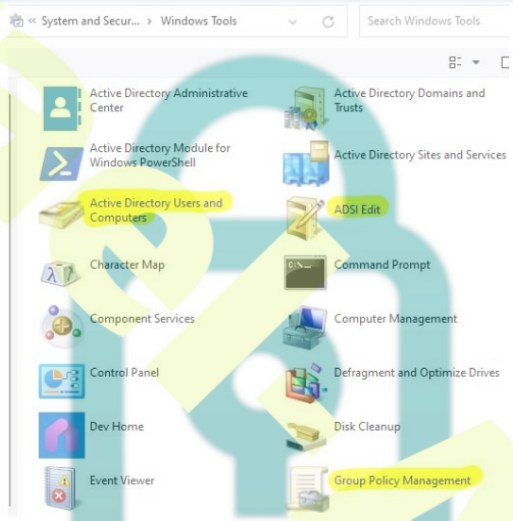
7.1.7. Utilisation des outils d'administration de serveur distant (RSAT)

Accédez aux outils suivants via « Outils Windows » ou « Gestionnaire de serveur », tous deux idéalement situés dans le menu Démarrer.

7.1.7.1. Aperçu

Nous nous concentrons sur ces outils :

- Utilisateurs et ordinateurs Active Directory
  dsa.msc
- ADSIModifier
  adsiedit.msc
- Gestion des politiques de groupe
  gpmsc.msc

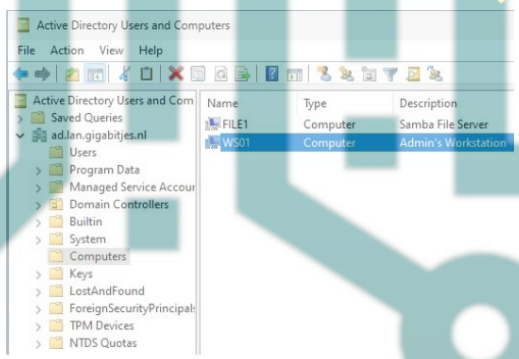


Épinglez ces outils sur Démarrer ou sur la barre des tâches, ou faites-les simplement glisser sur le bureau.

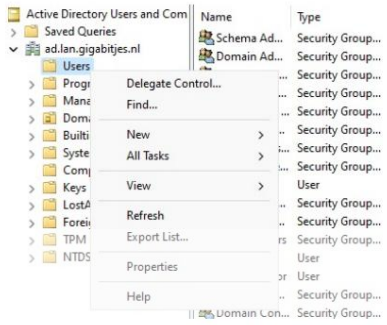
7.1.7.2. Utilisateurs et ordinateurs Active Directory (ADUC)

« Utilisateurs et ordinateurs Active Directory » est un outil de gestion du système d'exploitation Windows qui permet aux administrateurs d'effectuer des tâches liées aux comptes d'utilisateurs, aux groupes et aux objets informatiques dans un environnement Active Directory. Il fournit une interface graphique pour gérer et organiser ces objets d'annuaire, permettant aux administrateurs de créer, modifier et supprimer des comptes d'utilisateurs, de réinitialiser les mots de passe, de gérer les adhésions aux groupes et d'organiser les objets informatiques au sein d'unités organisationnelles (OU). Cet outil est crucial pour maintenir la structure et la sécurité d'un domaine Active Directory.

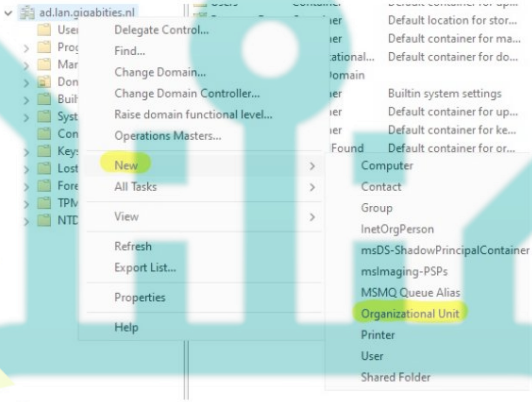
Lorsque vous utilisez « Utilisateurs et ordinateurs Active Directory », assurez-vous que les « Fonctionnalités avancées » sont activées via « Affichage » > « Fonctionnalités avancées ». Notez qu'il existe un bug qui peut initialement faire planter l'outil. Fermez et rouvrez « Utilisateurs et ordinateurs Active Directory », puis réactivez « Fonctionnalités avancées ».



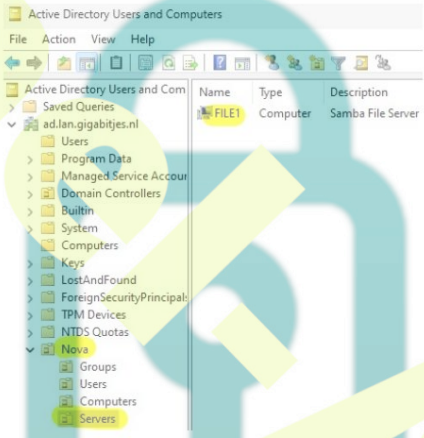
Bien que la création de comptes d'ordinateur à l'avance soit facultative (puisqu'un compte d'ordinateur est créé lors de la jointure de domaine), les comptes d'utilisateurs peuvent être facilement générés via le menu contextuel. Clic-droit « Utilisateurs » et sélectionnez « Nouveau » > « Utilisateur ».



Pour plus de clarté organisationnelle, envisagez de créer de nouvelles unités organisationnelles (UO). Par exemple, dans mon bureau à domicile, je pourrais créer une unité d'organisation nommée « Nova » et imbriquer des unités d'organisation supplémentaires pour les utilisateurs, les groupes et les ordinateurs.

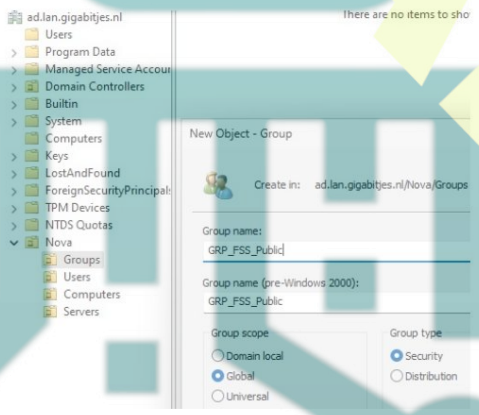


Ensuite, déplacez « WS01 » vers l'unité d'organisation « Ordinateurs » nouvellement créée sous « Nova » et le serveur de fichiers Samba « FILE1 » vers l'unité d'organisation « Serveurs ».

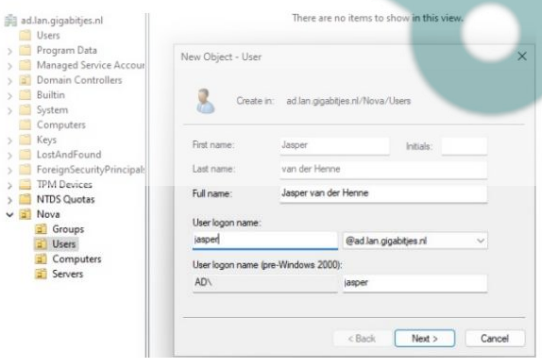


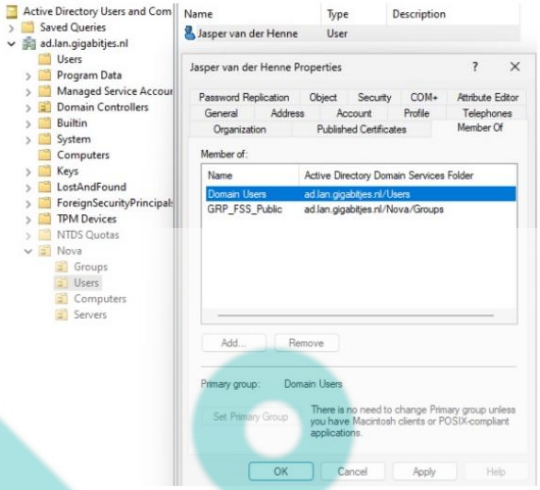
Une pratique efficace consiste à créer des groupes d'accès au sein de l'unité d'organisation « Groupes ». Par exemple, établissez « GRP_FSS_Public » pour accorder l'accès aux dossiers publics sur le serveur de fichiers.

Remarque critique : ne déplacez jamais un contrôleur de domaine à une autre unité organisationnelle (OU) ! Conservez-le toujours dans l'unité d'organisation « Contrôleurde domaine » par défaut. Microsoft déconseille fortement de déménager les contrôleurs de domaine de cette norme OU, comme Ce faisant peut compromettre le bon fonctionnement et n'est pas recommandé.



L'étape suivante consiste à créer des comptes d'utilisateurs et à organiser les adhésions aux groupes.





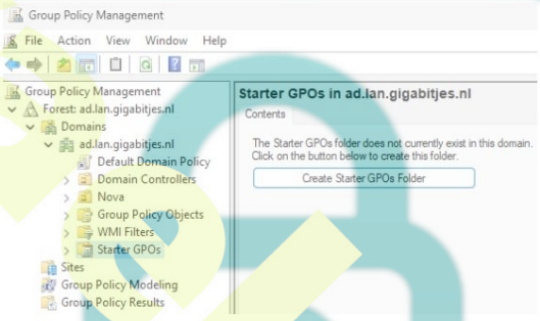
7.1.7.3. ADSIModifier

ADSI Edit est un outil puissant conçu pour les utilisateurs avancés et les administrateurs qui doivent apporter des modifications de bas niveau à Active Directory. En raison de son impact potentiel sur le système, il doit être utilisé avec prudence et les modifications doivent être effectuées uniquement par des personnes ayant une compréhension approfondie de la structure et des opérations d'Active Directory.

Si vous rencontrez une situation dans laquelle le nom d'affichage d'un ordinateur renommé ne reflète pas le nouveau nom dans Utilisateurs et ordinateurs Active Directory (ADUC), vous pouvez utiliser ADSI Edit pour corriger il.

7.1.7.4. Gestion des politiques de groupe

« Gestion des stratégies de groupe » est un outil d'administration Windows conçu pour configurer et gérer les paramètres de stratégie de groupe dans un environnement Active Directory. Il permet aux administrateurs de définir et d'appliquer des politiques de sécurité, des paramètres système et des configurations utilisateur sur un réseau d'ordinateurs Windows. Avec la gestion des stratégies de groupe, les administrateurs peuvent créer, modifier et organiser des objets de stratégie de groupe (GPO), qui sont des ensembles de stratégies pouvant être appliquées à des utilisateurs, des groupes ou des comptes d'ordinateur spécifiques. Cet outil fournit un contrôle centralisé sur divers aspects du système d'exploitation Windows, garantissant des paramètres cohérents et sécurisés sur l'ensemble du réseau d'une organisation.

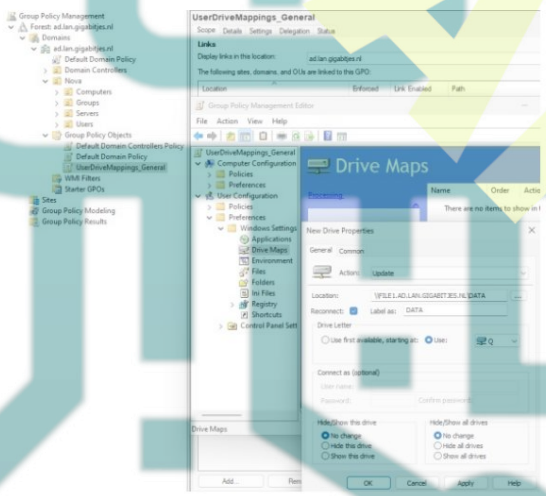


Créez le dossier des GPO de démarrage et procédez à l'ajout d'objets de stratégie de groupe (GPO) si nécessaire. Il est recommandé de créer des GPO individuels pour chaque élément de politique plutôt que de consolider tout sous « Politique de domaine par défaut », car cette approche favorise de meilleures pratiques d'organisation et de gestion.

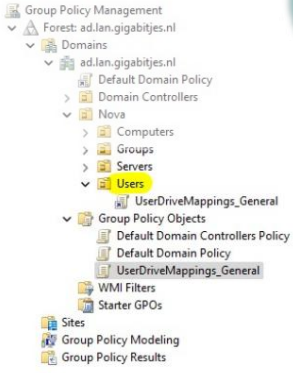
Bien qu'il soit possible de créer un objet de stratégie de groupe (GPO) directement au sein d'une unité organisationnelle (OU), il est recommandé de le créer initialement dans le conteneur « Objets de stratégie de groupe ». Ensuite, liez le GPO à l'unité d'organisation souhaitée pour une configuration et une gestion appropriées.

De plus, il est recommandé d'adopter une convention de dénomination structurée pour les objets de stratégie de groupe (GPO). Une convention de dénomination bien définie permet aux administrateurs de discerner facilement l'objectif et la cible (ordinateurs ou utilisateurs) d'un GPO à partir de son nom.

Pour les mappages de lecteurs généraux, envisagez d'utiliser un GPO nommé « UserDriveMappings_General.



Lier un objet de stratégie de groupe (GPO) est un processus simple de glisser-déposer de l'élément. Bien que cette méthode soit efficace, elle devient moins pratique à mesure que la liste s'allonge. Dans un tel Dans certaines instances, il est recommandé de lier un GPO à l'aide du menu contextuel, où l'option "Lier un GPO existant..." peut être sélectionnée pour une gestion plus efficace.



8. Partage de fichiers

Lors d'une étape précédente, nous avons établi un partage DATA sur notre serveur de fichiers et mis en œuvre une politique pour mapper ce partage sur la lettre de lecteur Q, améliorant ainsi le confort de l'utilisateur. Cependant, une limitation délibérée a été introduit : les utilisateurs ne peuvent actuellement pas créer de fichiers et de dossiers. Cette limitation n'est pas un problème technique mais plutôt un choix de conception. L'approche envisagée consiste à créer manuellement les dossiers principaux de notre partage et configurer les droits d'accès nécessaires pour nos utilisateurs.

Sur notre poste de travail administratif, nous allons naviguer vers \file1.ad.lan.gigabitjes.nl\data et créer un dossier nommé « Général ». Par la suite, nous accéderons aux « Propriétés » depuis le menu contextuel du nouveau dossier.

Maintenant, nous ouvrons l'onglet « Sécurité » et cliquons sur « Avancé ».

La tâche initiale implique la « Désactivation de l'héritage », dans laquelle les autorisations héritées sont converties en autorisations explicites sans suppression.

Ensuite, nous exclurons « Tout le monde » de la liste des autorisations et le remplacerons par « GRP_FSS_Public ». En appliquant les autorisations à « Ce dossier uniquement », nous sélectionnons des autorisations de base spécifiques :

Lire et exécuter Liste
du contenu du dossier
Lecture
Écriture
Cette configuration interdit aux utilisateurs de supprimer le dossier.

Ensuite, nous cliquons à nouveau sur « Ajouter », en appliquant les autorisations aux sous-dossiers et aux fichiers exclusivement. Nous sélectionnons « Contrôle total » et implémentons les paramètres.

Pour vérifier les ajustements, on passe à l'utilisateur précédemment créé. L'utilisateur peut créer des fichiers et des dossiers dans le répertoire « Général », mais il ne peut pas renommer, supprimer ou déplacer le répertoire. dossier. Cependant, l'utilisateur possède un contrôle total sur le contenu du dossier.

9. Connexion des postes de travail

Dans les sections précédentes, nous avons utilisé un poste de travail directement lié au VLAN de gestion. Lors de la connexion du poste de travail d'un utilisateur, celui-ci est dirigé vers le VLAN du bureau (32). Cependant, la connexion au contrôleur de domaine depuis ce réseau est actuellement impossible en raison de l'absence de règles fondamentales de pare-feu. En plus de ces services internes, nous souhaitons établir des connexions aux serveurs de messagerie et Web.

Établissons maintenant des règles de pare-feu pour faciliter l'enregistrement des postes de travail sur le domaine, permettant ainsi aux utilisateurs de commencer leurs tâches en toute transparence.

Nous utiliserons notre aperçu des VLAN ainsi qu'une liste des adresses IP de nos serveurs et les ports correspondants qui doivent être inclus dans nos règles de pare-feu pour plusieurs serveurs.

9.1. Aperçus

Nous utiliserons notre aperçu des VLAN ainsi qu'une liste des adresses IP de nos serveurs et les ports correspondants qui doivent être inclus dans nos règles de pare-feu pour plusieurs serveurs.

9.1.1. Présentation du VLAN

Interface	VLAN tag	Priority	Name	Subnet	Gateway	Description	Examples
igb1 (lan)	1	-	L1_0001_MNG1	172.21.1.0/24	172.21.1.1	Management 1	Switches, access points
igb1 (lan)	2	-	L1_0002_MNG2	172.22.2.0/24	172.22.2.1	Management 2	Hypervisor(s), KVM-over-IP
igb1 (lan)	16	-	L1_0016_SRVS	10.10.16.0/24	10.10.16.1	Server VMs	Server VMs
igb1 (lan)	18	-	L1_0018_STOR	10.10.18.0/24	10.10.18.1	Storage	Network Attached Storage (NAS)
igb1 (lan)	32	-	L1_0032_OFF1	10.10.32.0/24	10.10.32.1	Workstations	Desktop and laptop computers
igb1 (lan)	36	-	L1_0036_PRNT	10.10.36.0/24	10.10.36.1	Peripherals	Printers
igb1 (lan)	251	-	L1_0251_IOTD	172.31.251.0/24	172.31.251.1	Internet of Things	Solar panel inverters
igb1 (lan)	252	-	L1_0252_DMZ1	172.31.252.0/24	172.31.252.1	DMZ	Web and mail server
igb1 (lan)	253	-	L1_0253_GNET	172.31.253.0/24	172.32.253.1	Guest Network	Guest Wi-Fi network

9.1.2. Server IP addresses

Servername	VLAN	LAN IP	WAN IP	Description
103 s3.gigabitjes.nl	252	172.31.252.103	217.nnn.nnn.27	ISPConfig Mail and Web Server
201 sdc1.ad.lan.gigabitjes.nl	16	10.10.16.201	-	Domain Controller
301 file1.ad.lan.gigabitjes.nl	16	10.10.16.101	-	File Server

9.1.3. Admin Computer

Servername	VLAN	LAN IP	WAN IP	Description
901 ws01.ad.lan.gigabitjes.nl	16	172.21.1.{...}	N/A	Admin computers, DHCP, in management VLAN

9.1.4. Ports

Port	Protocol	Purpose	Server	Description
53	TCP	DNS over TCP	Domain Controller	DNS data exceeding 512 bytes
88	TCP	Kerbores	Domain Controller	
135	TCP	End Point Mapper	Domain Controller, File Server	
139	TCP	NetBIOS Session	Domain Controller, File Server	
445	TCP	SMB	Domain Controller, File Server	
464	TCP	Kerberos kpasswd	Domain Controller	
636	TCP	LDAPS	Domain Controller	
3268	TCP	Global Catalog	Domain Controller	
3269	TCP	Global Catalog SSL	Domain Controller	
49152:65535	TCP	Dynamic RPC Ports	Domain Controller	
53	UDP	DNS over UDP	Domain Controller	
88	UDP	Kerberos	Domain Controller	
123	UDP	NTP	Domain Controller	
137	UDP	NetBIOS Name Service	Domain Controller, File Server	
138	UDP	NetBIOS Datagram	Domain Controller, File Server	
389	UDP	LDAP	Domain Controller	
464	UDP	Kerberos kpasswd	Domain Controller	

Les ports TCP 135, 139, 445 + UDP 137, 138 seront utilisés par le serveur de fichiers.

Pour améliorer l'efficacité de l'impression, veuillez vous assurer que la plage de ports TCP 49152:65535 lorsque les imprimantes sont servies. Cela garantit un traitement fluide et rapide des travaux d'impression, éliminant tout retards potentiels (30 à 45 secondes).

Veuillez vous abstenir de partager des imprimantes via DNS dans environnements mixtes, en particulier lors de l'utilisation d'un serveur DHCP non Windows. Au lieu de cela, pour utiliser l'adresse IP du serveur de partage d'imprimantes.

Pour accéder aux services de messagerie et Web, nous devons ouvrir les ports suivants.

Port	Protocol	Purpose	Server	Description
25	TCP	SMTP	ISPConfig	Debatable
143	TCP	IMAP	ISPConfig	
465	TCP	SMTPS	ISPConfig	
587	TCP	MSA	ISPConfig	
993	TCP	IMAPS	ISPConfig	
80	TCP	HTTP	ISPConfig	
443	TCP	HTTPS	ISPConfig	

Il est conseillé d'organiser les ports en alias de port, puis de construire les règles de pare-feu dans pfSense.

9.2. Règles de pare-feu

F paragraphe 3.3.1 pour la création d'alias étapes et pourde règles de pare-feu.

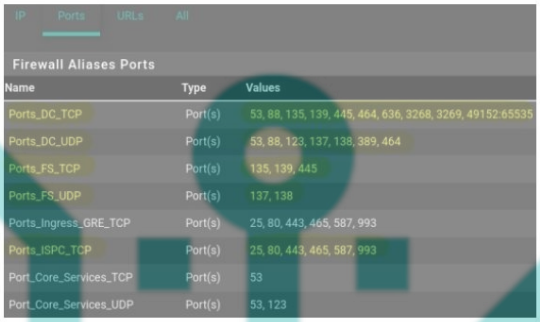
Ouvrez l'interface Web de pfSense et accédez à « Pare-feu » > « Alias » > « Ports ».

Ajoutez les alias de port et ajoutez les ports comme indiqué ci-dessus :

- Ports_DC_TCP (Ports, contrôleur de domaine, TCP)
- Ports_DC_UDP (Ports, contrôleur de domaine, UDP)
- Ports_FS_TCP (Ports, serveur de fichiers, TCP)
- Ports_FS_UDP (Ports, serveur de fichiers, UDP)
- Ports_ISPC_TCP (Ports, ISPConfig, TCP)

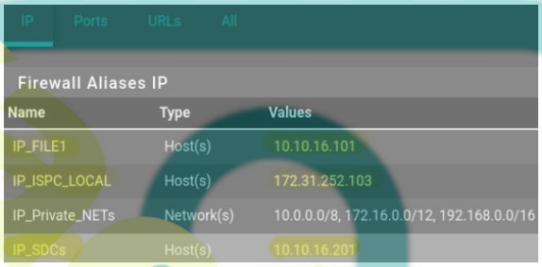
Remarque : vous pouvez simplement copier « Port_Ingress_GRE_TCP » vers « Ports_ISPC_TCP ».

Résultat:



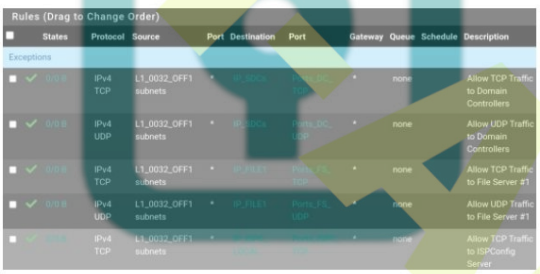
Ensuite, ajoutez les alias IP suivants :

- IP_SDC
- IP_FILE1
- IP_ISPC_LOCAL



Créez enfin les règles de pare-feu en utilisant les alias sur l'interface L1_0032_OFF1 :

- Autoriser le trafic TCP vers les contrôleurs de domaine
- Autoriser le trafic UDP vers les contrôleurs de domaine
- Autoriser le trafic TCP vers le serveur de fichiers n°1
- Autoriser le trafic UDP vers le serveur de fichiers n°1
- Autoriser le trafic TCP vers le serveur ISPConfig



10. Conclusion

En conclusion de cet article, il est évident que notre réseau, bien que fonctionnel, reste un peu rudimentaire. Il existe de nombreuses possibilités d'amélioration, depuis l'introduction d'un deuxième contrôleur de domaine et explorer des variantes de commutateur supplémentaires pour répliquer la configuration du pare-feu dans OPNsense, intégrer les boîtes aux lettres, affiner les configurations des postes de travail et, ne l'oublions pas, étendre nos politiques Active Directory.

J'apprécie vos précieux commentaires, et il est prévu de les intégrer dans la prochaine révision de cet article. N'oubliez pas que je ne parcoure pas ce voyage seul ; la communauté HowtoForge est un espace de collaboration où nous pouvons nous soutenir mutuellement. N'hésitez pas à partager vos réflexions, laisser des commentaires ou lancer des discussions sur le forum. Jusqu'à la prochaine fois! Bravo, Bouke