Institut **S**upérieur d'**I**nformatique,
de **M**odélisation et de leurs **A**pplications

Rapport de stage/Projet d'Ingénieur ISIMA 2ième année

Filière : F5 cybersécurité et réseaux informatique

Conception et déploiement d’un réseau multi-entreprise sécurisé

Présenté par : **BEN TALB Abdelaziz, COMBE Axelle, NDAO Aly**

Responsable ISIMA : Patrice Laurencot

6 mars 2025

ISIMA - Campus des Cézeaux. 1 rue de la Chebarde. TSA 60125. 63178 Aubière CEDEX

Résumé

Dans le cadre de notre projet de deuxième année à l'ISIMA, nous avons conçu et déployé une architecture réseau multi-entreprise sécurisée. L'objectif était de mettre en place une infrastructure intégrant des pare-feux Stormshield*, tout en assurant la communication et la protection des différents segments du réseau. Le projet s'est articulé autour de plusieurs services tels que la gestion des VPN*, la configuration des serveurs mail, FTP*, web et NFS*, ainsi que l'intégration d'un annuaire Active Directory. Malgré certaines difficultés rencontrées, notamment sur le lien entre l'Active Directory et pare-feu, nous avons adapter notre approche et proposer une solution fonctionnelle et sécurisée.

Mots-clés : Réseau, Pare-feu, Protocole, stormshield, VPN, sécurité

Abstract

As part of our second-year project at ISIMA, we designed and deployed a secure multi-company network architecture. The objective was to implement an infrastructure integrating Stormshield firewalls while ensuring communication and protection across different network segments. The project focused on several services, including VPN management, mail, FTP, web, and NFS server configuration, as well as the integration of an Active Directory. Despite some challenges, particularly on the link between Active Directory and Firewall, we adapted our approach and provided a functional and secure solution.

Keywords : Network, firewall, protocol, stormshield, VPN, security

Remerciements

Nous tenions à remercier Patrice LAURENCOT pour sa disponibilité lors du projet, et les enseignants dont les cours nous ont servi en particulier Mathieu RUE.

Table des matières

Résumé..... iii
Abstract..... iii
Remerciements..... iv
Table des figures..... vi
INTRODUCTION..... 1
1. Contexte..... 2
1.1. Le sujet..... 2
1.2. Notre architecture..... 2
1.3. Organisation..... 3
1.4. Outils mobilisé..... 4
2. Réalisation..... 5
2.1. Pare-feux..... 5
2.2. Différents services..... 8
3. Difficultés et pistes d'amélioration..... 11
3.1. Difficulté rencontré 11
3.2. Pistes d'amélioration..... 12
CONCLUSION..... 13
ANNEXE A..... vii
Lexique..... vii
Bibliographie..... viii
Webographie..... viii
ANNEXE B..... vii
ANNEXE C..... vii
ANNEXE D..... vii
ANNEXE E..... vii
ANNEXE F..... vii

Table des figures

Figure 1: Diagramme de GANTT prévisionnel.....3
Figure 2: Diagramme de GANTT réel.....3

INTRODUCTION

Au cours de notre projet de deuxième année, nous avons deux objectifs. Le premier est de passer, lors des deux premières semaines, la formation CSNA*, qui a pour objectif de nous former à l'utilisation du pare-feu Stormshield. Le deuxième est de concevoir et déployer un réseau en utilisant tout ce que nous avons appris lors de notre formation mais aussi de pouvoir réutiliser ce qu'on a vu en cours tout au long de l'année. Ce rapport portera sur le deuxième point et a pour but d'expliquer ce que nous avons fait pour répondre à l'intitulé du projet mais aussi nos difficultés.

1. CONTEXTE

1.1. Le sujet

Lors de notre projet, nous devons concevoir une architecture avec quelques contraintes. Elle doit au moins comprendre un pare-feu Stormshield pour montrer ce que nous avons fait et/ou appris lors de la formation. Elle doit aussi avoir une partie sur des équipements physiques. Étant donné que nous avons accès au pare-feu uniquement par machine virtuelle, l'architecture doit de ce fait inclure à la fois une partie physique et une partie virtuelle. Pour mettre en place tout cela, nous disposions :

- La machine virtuelle du pare-feu,
- La documentation fournie pendant la formation CSNA qui explique le fonctionnement des pare-feu Stormshield [1],
- Du matériel Cisco de la salle A214 de l'ISIMA.

1.2. Notre architecture

Nous avons conçu deux réseaux « entreprise ». Chacun intègre un pare-feu Stormshield, qui sert d'interface entre l'extérieur et le réseau interne. Ce réseau interne regroupe les PC des employés ainsi que les services internes de l'entreprise. Une DMZ* a également été mise en place pour exposer certains services à l'extérieur, tout en garantissant la sécurité du réseau interne.Dans les deux entreprises la baie de serveurs contient un serveur mail, FTP, WEB et DNS propre à l'entreprise. De plus, elles ont chacune une spécificité. L'entreprise A contient un accès VPN SSL* pour permettre à un employé souhaitant travailler à distance de se connecter directement au réseau interne. L'entreprise B, elle ne fonctionne pas sur l'annuaire de base fournie par le pare-feu mais grâce à un Active Directory. De plus les deux entreprises sont liées grâce à un VPN IPSec* permettant de simuler deux entreprises très proches qui pourraient vouloir créer un lien entre leurs deux réseaux internes.

En complément, nous avons ajouté un réseau physique ((appelé réseau C) connecté aux deux entreprises par l'intermédiaire d'un routeur ayant pour but de contenir un serveur GLPI et d'autres machines qui vont être protégées par un pare-feu firewalld*. Le schéma correspondant est disponible en annexe (ANNEXE B).

En résumé, toutes les entreprises disposent, dans leur DMZ, d'un serveur mail, web, DNS et FTP ainsi que d'autres services spécifiques :

• L'entreprise A contient un accès VPN SSL* pour permettre à un employé souhaitant travailler à distance de se connecter directement au réseau interne.

• L'entreprise B possède en plus un annuaire spécifique sous Active Directory.

En termes de communication :

• L'entreprise A et l'entreprise B communiquent via un VPN IPsec site-à-site.

1.3. Organisation

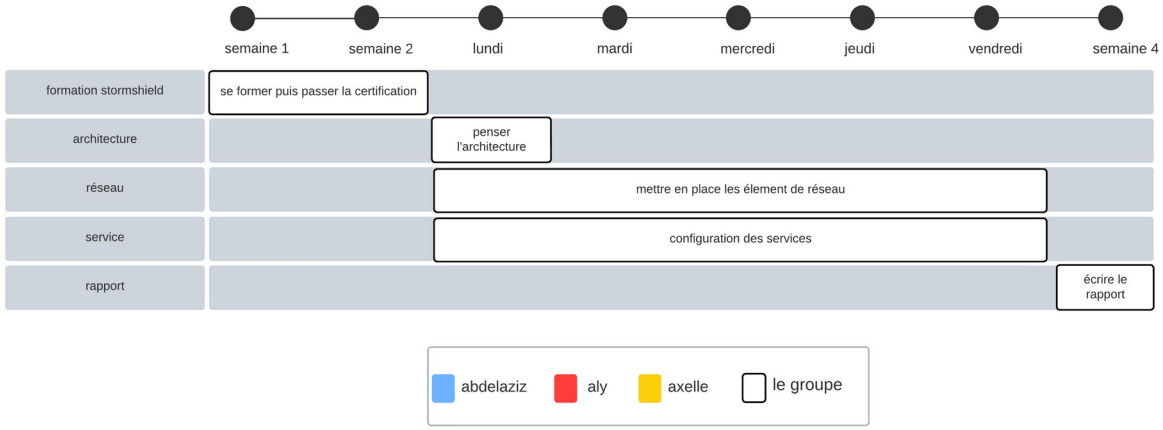


Figure 1: Diagramme de GANTT prévisionnel

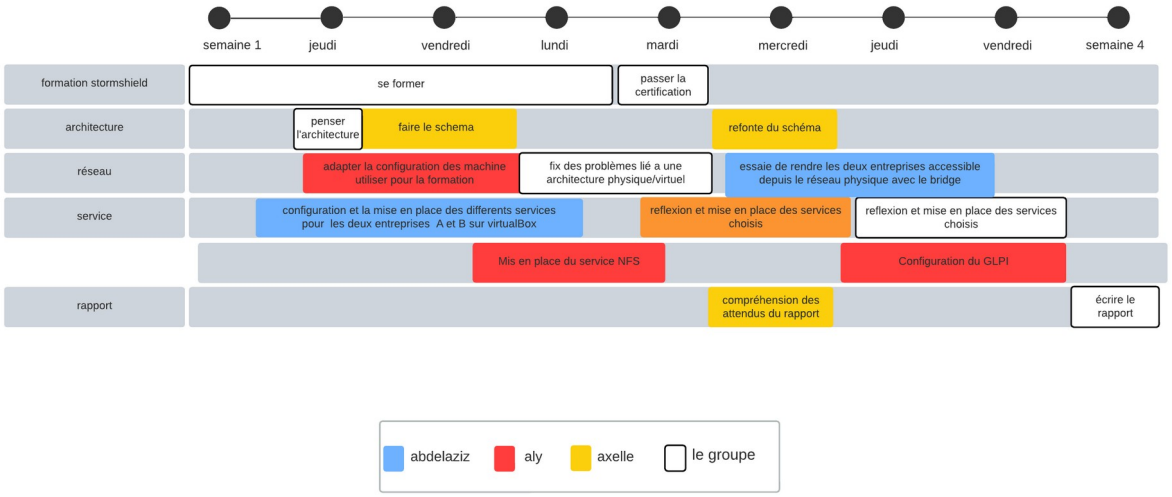


Figure 2: Diagramme de GANTT réel

1.4. Équipements et technologie

Dans le cadre de notre projet, nous avons utilisé du matériel de Stormshield, plus précisément un pare-feu virtuel. Stormshield est une entreprise française spécialisée dans la cybersécurité, fondée en 1998. Elle est reconnue pour ses solutions de pare-feu certifiées par l'ANSSI*, utilisées principalement par les administrations publiques et les entreprises sensibles.

Pour la partie physique de notre projet, nous avons utilisé des routeurs et des commutateurs Cisco. Cisco est une entreprise spécialisée dans les équipements réseau, fondée en 1984 et basée aux États-Unis. Elle est leader mondial sur le marché des commutateurs et routeurs utilisés principalement dans les réseaux d'entreprise et les infrastructures d'Internet.

2. RÉALISATION

2.1. Pare-feux

Dans le cadre de la conception et du déploiement du réseau, nous avons mis en place différents pare-feux en fonction des besoins spécifiques de chaque entité. La sécurité étant un élément fondamental de l'architecture, le choix des pare-feux a été effectué en tenant compte des contraintes de chaque entreprise et des services qu'elle héberge. Deux solutions principales ont été utilisées : Stormshield pour les entreprises A et B, et Firewalld pour le réseau C.

2.1.1. Pare-feu Stormshield

Stormshield est une solution UTM* qui permet un contrôle avancé du trafic réseau en intégrant plusieurs mécanismes de défense. Son filtrage dynamique repose sur des règles strictes qui définissent quels flux sont autorisés ou bloqués. Grâce à son inspection approfondie des paquets DPI*, il est capable d'analyser les protocoles en profondeur afin de détecter toute anomalie ou activité suspecte.

L'un de ses atouts majeurs est son système de prévention d'intrusion IPS*, qui permet d'identifier et de bloquer automatiquement les tentatives d'exploitation de vulnérabilités ou d'intrusion malveillantes. En complément, Stormshield embarque un moteur d'analyse des menaces en temps réel, capable de détecter et neutraliser les logiciels malveillants et les attaques Zero-Day* avant qu'ils ne compromettent le réseau.

Outre sa capacité à filtrer et analyser le trafic, Stormshield offre également une gestion avancée des VPN, prenant en charge les protocoles IPSec et SSL, permettant ainsi de sécuriser les communications entre sites distants ou avec des utilisateurs externes. Son interface intuitive et son administration centralisée facilitent la gestion des politiques de sécurité et des utilisateurs, rendant l'ensemble de la configuration plus efficace et flexible.

2.1.1.1 Rôle du pare-feu dans Stormshield

Dans chaque entreprise, le pare-feu Stormshield assure la segmentation et la protection des différentes zones réseau. Cette organisation repose sur une séparation

stricte des flux entre le réseau interne, où évoluent les ressources sensibles, et la DMZ, qui héberge les services accessibles depuis l'extérieur.

Le réseau interne des entreprises A et B constitue l'espace où se trouvent les postes de travail et les services internes essentiels. Parmi ces services, on retrouve notamment le partage de fichiers, l'authentification des utilisateurs et la gestion des ressources informatiques. Le pare-feu Stormshield a été configuré pour protéger cette zone en restreignant strictement les accès entrants et sortants. Seuls les utilisateurs autorisés ont la possibilité d'accéder aux ressources qui leur sont nécessaires, empêchant ainsi toute communication indésirable ou dangereuse. Ce cloisonnement garantit qu'aucune attaque externe ne puisse compromettre la confidentialité des données internes.

Pour sécuriser l'accès aux services publics, une DMZ a été déployée au sein de chaque entreprise. Cette zone isolée permet d'héberger les services accessibles depuis l'extérieur, tout en maintenant une barrière protectrice entre eux et le réseau interne. La DMZ contient plusieurs services stratégiques comme un serveur de messagerie (mail), un serveur web, un serveur DNS* et un serveur FTP. Les règles de filtrage associées sont en annexe (ANNEXE E).

2.1.1.2 Gestion des VPN

L'une des fonctionnalités clés du pare-feu Stormshield est sa capacité à gérer les VPN. Ce dispositif permet aux entreprises de garantir des communications sécurisées, tant pour les employés travaillant à distance que pour les connexions entre les sites distants.

- Dans l'entreprise A, un VPN SSL a été mis en place afin de permettre aux utilisateurs nomades de se connecter de manière sécurisée au réseau interne. Ce **VPN SSL** repose sur un tunnel chiffré, garantissant la **confidentialité et l'intégrité des données** échangées entre l'utilisateur distant et les serveurs de l'entreprise. Afin de renforcer cette sécurité, une **authentification forte** a été mise en place, limitant l'accès aux **s**euls employés autorisés.
- L'entreprise A et l'entreprise B doivent pouvoir échanger des ressources en toute sécurité, tout en maintenant des réseaux distincts. Pour cela, un **VPN IPSec site-à-site** a été configuré à travers les pare-feux Stormshield des deux entreprises. Ce tunnel chiffré permet aux deux sites de communiquer comme s'ils faisaient **partie du même réseau interne**, tout en préservant un haut niveau de segmentation et de contrôle d'accès.

Le VPN IPSec mis en place garantit plusieurs aspects de sécurité :

- Une connexion chiffrée entre les deux entreprises, empêchant toute interception des données sensibles.
- Une authentification renforcée, validant uniquement les connexions provenant des pare-feux Stormshield autorisés.
- Un routage strictement défini, interdisant tout trafic non prévu entre les sous-réseaux.

Grâce à cette liaison sécurisée et performante, les ressources critiques peuvent être partagées en toute confiance entre les deux entreprises.

Les figures associées à cette section sont disponibles en annexe (ANNEXE F).

2.1.2. Pare-feu Firewalld

Le réseau physique C est un réseau indépendant, conçu pour héberger des services partagés accessibles par les entreprises A et B. Ce réseau abrite notamment un serveur NFS, un serveur web et une plateforme de gestion GLPI*, qui est accessible uniquement en HTTPS* afin de garantir la confidentialité des échanges et la sécurité des accès.

Pour assurer la protection de ce réseau, le pare-feu Firewalld a été choisi. Contrairement à Stormshield, Firewalld est une solution intégrée aux systèmes Linux modernes, offrant une gestion dynamique des règles de filtrage. Cette solution a été privilégiée en raison de sa flexibilité et de sa capacité à appliquer des modifications sans interrompre les connexions en cours.

La configuration de Firewalld sur le réseau C a été réalisée de manière à contrôler strictement l'accès aux services hébergés. Seules les machines appartenant au réseau C sont autorisées à accéder au serveur NFS, ce qui garantit que ce dernier est uniquement utilisé à des fins internes. En revanche, le serveur web et la plateforme GLPI sont accessibles depuis les entreprises A et B, mais exclusivement via une connexion HTTPS afin d'assurer la sécurité et l'intégrité des communications. Pour ce faire nous avons suivis les documentations [2] et [3].

Firewalld repose sur un système de zones de sécurité, chacune étant configurée en fonction du niveau de confiance attribué aux connexions. Dans notre cas, le réseau interne de l'entreprise C est placé dans une zone de confiance élevée, où les communications internes sont autorisées sans restriction. En revanche, les connexions provenant des entreprises A et B passent par une zone intermédiaire, avec des règles

spécifiques limitant l'accès uniquement aux services web et GLPI en HTTPS. Cette approche garantit un contrôle efficace du trafic et réduit les risques d'intrusion.

L'un des avantages majeurs de Firewalld est sa simplicité de gestion. Contrairement aux pare-feux traditionnels basés sur des chaînes et des règles statiques, Firewalld permet d'ajouter ou de modifier des règles dynamiquement, sans nécessiter un redémarrage du service. Cette capacité est particulièrement utile dans un environnement où les besoins peuvent évoluer rapidement, garantissant ainsi une protection adaptative et efficace du réseau C.

2.2. Différents services

Dans cette section, nous détaillons la mise en œuvre des différents services utilisés dans notre projet. L'objectif principal était de déployer et de configurer des serveurs répondant aux besoins spécifiques de notre infrastructure, en s'appuyant sur les TPs réalisés lors du premier semestre et sur les outils fournis dans le cadre de la formation Stormshield.

2.2.1. Mail et FTP

Pour les serveurs Mail et les serveurs FTP, nous avons opté pour les serveurs fournis par la formation Stormshield pour les deux entreprises virtuelles A et B. L'avantage de cette approche est de disposer d'une plateforme déjà éprouvée et adaptée aux exigences de sécurité et de performance requises par notre projet.

Configuration et mise en œuvre :

Mail : Les serveurs mail ont été configurés pour gérer la distribution et la réception des courriers électroniques entre les deux entreprises A et B. La configuration inclut l'authentification des utilisateurs ainsi que les règles de filtrage pour garantir la sécurité des échanges.

FTP : Pour les serveurs FTP, la configuration a été orientée vers la facilité d'accès et la gestion sécurisée des transferts de fichiers entre les deux entreprises virtuelles A et B. La configuration inclut également des règles de filtrage pour garantir la sécurité des échanges.

2.2.2. NFS

Le serveur NFS a été ajouté pour permettre le partage de fichiers sur le réseau local de l'entreprise physique. Ce choix répond au besoin d'un accès centralisé et sécurisé aux ressources partagées par l'ensemble des utilisateurs du réseau.

Implémentation basée sur le TP :

- Nous nous sommes appuyés sur le TP réalisé avec notre professeur lors du premier semestre, ce qui nous a permis d'avoir une base solide pour la mise en œuvre.
- La configuration NFS a inclus la définition des répertoires partagés, la gestion des permissions d'accès (en lecture et écriture) et l'optimisation des performances pour le réseau local.

  Les figures associées à cette section sont disponibles en annexe (ANNEXE D).

2.2.3. WEB

Les serveurs web ont été mis en place pour héberger des applications et des services pour les trois entreprises. La sécurisation des échanges via le protocole HTTPS était primordiale pour assurer la confidentialité et l'intégrité des données transmises.

- Pour **les entreprises virtuelles A et B**, nous avons opté pour les serveurs web fournis par la formation Stormshield. Ces serveurs ont permis une intégration rapide et efficace dans notre infrastructure virtuelle.
- Pour **l'entreprise physique**, nous avons choisi de déployer un serveur web, en nous inspirant d'un TP réalisé lors du premier semestre. Concrètement, cela signifie que nous avons installé et paramétré le serveur web sur une machine dédiée au sein de l'infrastructure physique, plutôt que d'utiliser une solution préconfigurée.

Afin de sécuriser les échanges de données entre le serveur et les utilisateurs, nous avons activé le protocole HTTPS. Ce protocole permet de chiffrer les informations transmises, garantissant ainsi qu'elles ne puissent pas être interceptées ou altérées par des tiers.

Pour mettre en place HTTPS, nous avons utilisé un certificat auto-signé. Un certificat auto-signé est un certificat numérique généré par nos soins, et non délivré par une autorité de certification reconnue.

2.2.4. GLPI

GLPI est un outil open source destiné à la gestion et au suivi de l'ensemble des machines et équipements informatiques d'un réseau. Dans notre projet, nous l'avons déployé pour centraliser l'inventaire des PC et autres périphériques présents sur le réseau.

Pour mettre en place cette solution, nous avons d'abord installé GLPI sur un serveur dédié en suivant une vidéo tutorielle [4]. L'objectif était de disposer d'une interface centralisée où toutes les informations relatives aux machines pourraient être enregistrées et mises à jour. Une fois l'installation réalisée, il a fallu configurer l'outil pour qu'il réponde aux besoins spécifiques de notre infrastructure.

Une des étapes clés a été la configuration de la base de données. Pour cela, nous avons utilisé MariaDB, un système de gestion de bases de données relationnelles performant et compatible avec GLPI. MariaDB stocke toutes les données relatives aux machines, aux utilisateurs et aux incidents, ce qui permet une gestion efficace et structurée des informations.

Le suivi des machines sur le réseau nécessite une mise à jour régulière des informations. Dans notre cas, les PC et autres équipements ne sont pas automatiquement détectés par GLPI ; il faut donc les ajouter manuellement dans l'interface. Cela permet de s'assurer que chaque machine est bien enregistrée, avec ses caractéristiques techniques et son état d'utilisation, facilitant ainsi la gestion du parc informatique.

Les figures associées à cette section sont disponibles en annexe (ANNEXE C).

2.2.5. Active Directory

Au cours de notre deuxième année, nous avons suivi un cours centré sur Active Directory, un service d'annuaire proposé par Microsoft permettant la gestion des identités, des ressources et des autorisations au sein d'un réseau Windows. Souhaitant intégrer ce service à notre infrastructure, nous avons étudié sa faisabilité. Lors de la formation pour la certification Stormshield, il est mentionné que cette intégration est possible. En approfondissant nos recherches, nous avons trouvé une documentation officielle [5] confirmant cette possibilité.

Nous avons alors installé une machine Windows Server et recréé notre Active Directory en suivant les enseignements dispensés en cours. Ce serveur virtuel a été intégré au réseau interne de l'entreprise B. Les connexions virtuelles étaient correctes, comme en témoignait la réussite des tests de connectivité (ping) entre les différentes machines du réseau, y compris le pare-feu.

Cependant, malgré le respect des instructions, l'Active Directory, une fois configuré comme annuaire sur le pare-feu, ne pouvait être joint. Cette anomalie rendait impossible son utilisation en tant qu'annuaire centralisé. Après plusieurs tentatives infructueuses, nous avons finalement opté pour l'annuaire natif du pare-feu.

3. DIFFICULTÉS ET PISTES D'AMÉLIORATION

3.1. Difficulté rencontré

Au cours de la mise en place de notre architecture réseau, plusieurs problématiques ont été rencontrées, nécessitant des ajustements et des choix stratégiques afin de garantir la stabilité et la sécurité de l'infrastructure.

Problème de connectivité entre Active Directory et pare-feu :

L'une des principales difficultés observées concernait l'intégration de l'Active Directory avec le pare-feu Stormshield. Bien que les tests réseau classiques, tels que les pings entre les machines, aient fonctionné correctement, le service d'annuaire n'a pas pu être joint par le pare-feu. Cette anomalie laissait supposer un problème de connectivité plus complexe, potentiellement lié aux règles de filtrage ou à une configuration spécifique des flux sur Stormshield.

Face à cette situation, nous avons envisagé d'investiguer plus en profondeur les causes de cette incompatibilité. Cependant, en raison des contraintes de temps et de la nécessité de finaliser d'autres services essentiels, nous avons choisi de prioriser la mise en place de GLPI et des autres éléments du projet.

Problème d'interconnexion entre les machines virtuelles et physiques :

Nous avions initialement configuré deux entreprises virtuelles sous VirtualBox en mode NAT*, en espérant une meilleure isolation des flux. Par la suite, dans le but de permettre un accès direct à ces entreprises depuis l'environnement de l'entreprise physique, nous avons tenté de les passer en mode bridge. Malheureusement, cette configuration a rapidement engendré des problèmes de connectivité et de routage, et nous n'avons pas réussi à stabiliser les échanges. Après plusieurs tests et ajustements, nous avons finalement décidé de revenir à la solution NAT, qui, malgré ses limites en termes d'isolation, a permis d'assurer une communication fiable et sécurisée entre les différentes entités.

3.2. Pistes d’amélioration

Bien que notre infrastructure réponde aux objectifs fixés, certaines améliorations pourraient être apportées pour renforcer la segmentation réseau, optimiser les performances et enrichir les services proposés.

Mise en place de VLAN* pour une meilleure segmentation du réseau :

L’ajout de VLAN dans les réseaux internes permettrait une isolation plus fine des flux entre les différentes zones fonctionnelles. Par exemple, la séparation des postes de travail, des serveurs et des équipements administratifs via des VLAN dédiés réduirait le risque de propagation d’éventuelles attaques et améliorerait la gestion des droits d’accès.

Ajout de services physiques pour enrichir l’infrastructure :

Afin de rendre notre infrastructure plus représentative d’un environnement réel en entreprise, nous aurions pu intégrer des équipements physiques supplémentaires, tels qu’une imprimante réseau ou un système de téléphonie IP (VoIP). L’utilisation d’un VLAN voix aurait également permis d’expérimenter les mécanismes de priorisation du trafic et d’observer l’impact de la segmentation sur la qualité de service.

Investigation approfondie du problème Active Directory – Stormshield :

L’erreur rencontrée lors de l’intégration de l’Active Directory aurait nécessité une analyse plus poussée des logs et des flux réseau afin d’identifier précisément l’origine du problème. Une étude complémentaire sur les configurations avancées de Stormshield aurait pu être menée afin d’envisager des solutions alternatives, telles que des ajustements au niveau des règles de filtrage ou des paramètres DNS.

En conclusion, malgré ces défis, les choix réalisés nous ont permis de livrer une infrastructure fonctionnelle et conforme aux attentes du projet. Ces pistes d’amélioration pourraient être explorées dans un cadre ultérieur afin d’approfondir les connaissances acquises et d’optimiser davantage notre architecture.

CONCLUSION

Ce projet nous a permis d'appliquer concrètement les compétences acquises durant notre formation en réseau et sécurité informatique. La mise en place d'une infrastructure sécurisée impliquant plusieurs entreprises virtuelles nous a confrontés à des problématiques réelles, telles que la gestion des pare-feux, l'implémentation de VPN, et la configuration des services critiques.

Nous avons notamment pu approfondir nos connaissances sur les solutions Stormshield et Firewalld, tout en testant des mécanismes avancés de protection des réseaux. Malgré des défis techniques, comme l'intégration d'Active Directory sur Stormshield, nous avons su nous adapter et trouver des solutions alternatives efficaces.

Ce projet nous a également sensibilisés à l'importance de la planification et de la documentation dans la gestion d'un projet réseau. Il nous a préparés à des scénarios professionnels réels où la sécurisation et la gestion des ressources informatiques sont essentielles.

ANNEXE A

Lexique

Active Directory : Service de gestion centralisée des utilisateurs et ressources réseau proposé par Microsoft.

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information): L'Agence Nationale de la Sécurité des Systèmes d'Information est une institution française qui a pour mission de renforcer la cybersécurité des administrations publiques et des entreprises stratégiques.

Bridge (Virtual Box) : Mode de connexion réseau permettant à une machine virtuelle d'être connectée directement au réseau physique de l'hôte, avec sa propre adresse IP.

CSNA (Certification Stormshield Network Administrator): Certification attestant de la maîtrise des solutions de pare-feu Stormshield, notamment en matière de filtrage, VPN et gestion des règles de sécurité.

DMZ (Zone Démilitarisée) : Sous-réseau isolé contenant des services accessibles depuis l'extérieur, tout en protégeant le réseau interne contre des attaques potentielles.

DNS (Domain Name System) : Système permettant de traduire les noms de domaine (exemple.com) en adresses IP pour l'acheminement du trafic réseau.

DPI (Deep Packet Inspection) : Technique d'analyse approfondie des paquets réseau permettant d'identifier les protocoles et de détecter des menaces potentielles.

Firewalld : Outil de gestion de pare-feu intégré aux systèmes Linux modernes, permettant une administration dynamique des règles de filtrage.

FTP (Transfer Protocol) : Protocole permettant le transfert de fichiers entre un client et un serveur sur un réseau.

GANTT (Diagramme de GANTT) : Outil de gestion de projet permettant de planifier les différentes tâches dans le temps sous forme de diagramme.

GLPI (Gestionnaire Libre de Parc Informatique) : Outil open-source permettant la gestion des ressources informatiques et la supervision d'un parc de machines.

IPS (Intrusion Prevention System) : Système de prévention des intrusions analysant et bloquant en temps réel les menaces détectées dans le trafic réseau.

NAT (Virtual Box) : Technique permettant de traduire plusieurs adresses IP privées en une seule adresse IP publique pour accéder à Internet.

NFS (Network File System): Protocole permettant le partage de fichiers sur un réseau entre machines Linux/Unix.

Stormshield : Entreprise française spécialisée dans les solutions de cybersécurité, notamment les pare-feux et la protection des réseaux.

UTM (Unified Threat Management): Solution de sécurité réseau tout-en-un intégrant plusieurs fonctionnalités (pare-feu, filtrage, antivirus, VPN).

VLAN (Virtual Private Network) : Technologie permettant de segmenter un réseau physique en plusieurs sous-réseaux logiques indépendants.

VPN (Virtual Private Network) : Technologie permettant de créer une connexion sécurisée entre deux réseaux via un tunnel chiffré.

VPN SSL (Virtual Private Network utilisant Secure Sockets Layer) : Type de VPN utilisant le protocole SSL pour sécuriser la connexion entre un client et un réseau distant.

VPN Ipsec (Internet Protocol Security Virtual Private Network) : Protocole permettant de sécuriser les communications sur un réseau IP grâce à des mécanismes d'authentification et de chiffrement.

Zero-Day : Vulnérabilité logicielle inconnue des éditeurs et exploitée par des attaquants avant la publication d'un correctif.

Bibliographie

[1] **Stormshield.** (2023). Documentation CSNA – Certified Stormshield Network Administrator (Version 4.0). Stormshield. Document interne, non publié.

Webographie

[2] **Linuxtricks.fr.** (s.d.). *Firewalld : Le pare-feu facile sous Linux – Wiki.* Consulté le 17 février 2025, à l'adresse https://www.linuxtricks.fr/wiki/firewalld-le-pare-feu-facile-sous-linux

[3] **Boucheron, B.** (2020, 1 mai). *Comment configurer un pare-feu en utilisant firewalld sur CentOS 8.* DigitalOcean. Consulté le 17 février 2025, à l'adresse https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-8-fr

[4] **syncbricks.** (2022, 5 mai). *GLPI 10 Assets Management & Ticketing System // Tutorial Installation and Setup* [Vidéo]. YouTube. Consulté le 19 février 2025, à l'adresse https://www.youtube.com/watch?v=fTZV3_B_85M

[5] **Stormshield.** (s.d.). *Connexion à un annuaire Microsoft Active Directory.* Consulté le 17 février 2025, à l'adresse https://documentation.stormshield.eu/SNS/v4/fr/Content/User_Configuration_Manual_SNS_v4/Directory_configuration/Connecting_to_a_Microsoft_Active_Directory.htm

ANNEXE B

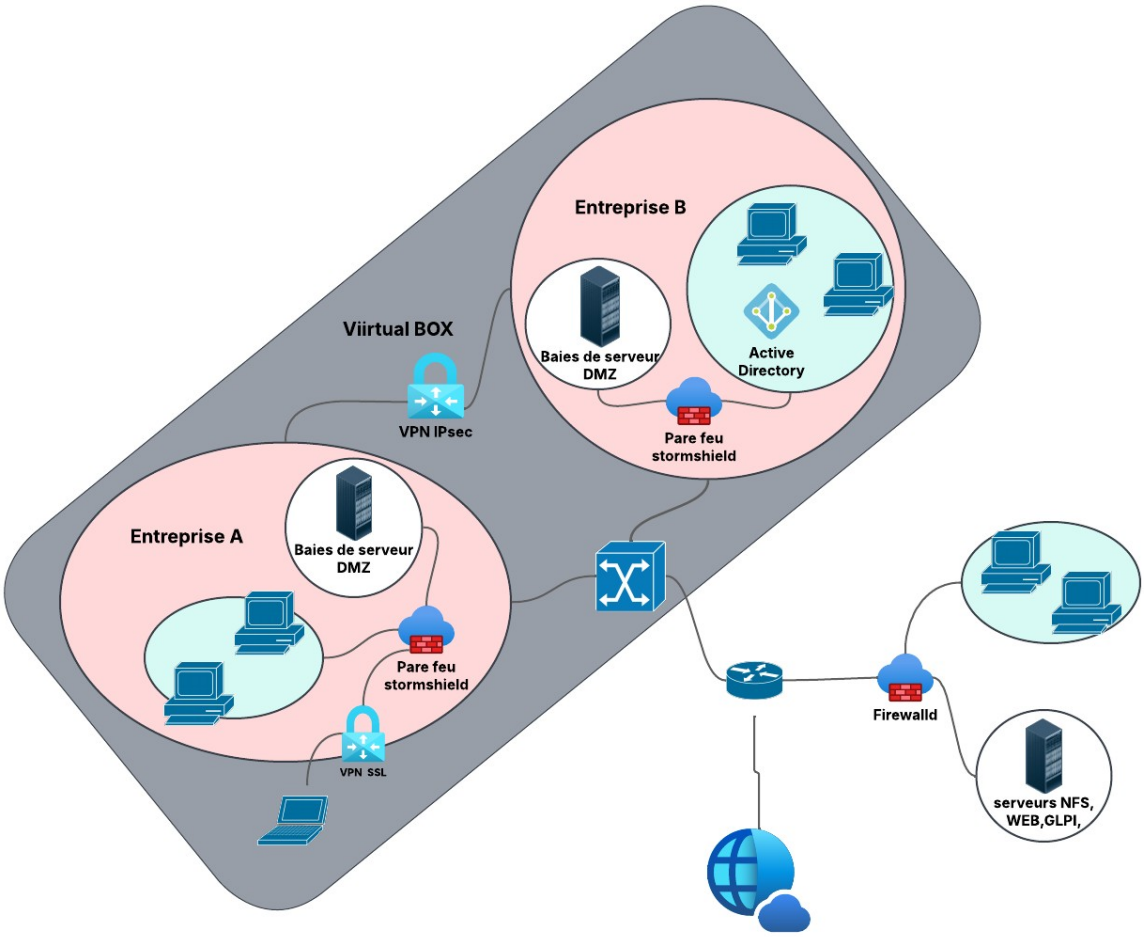
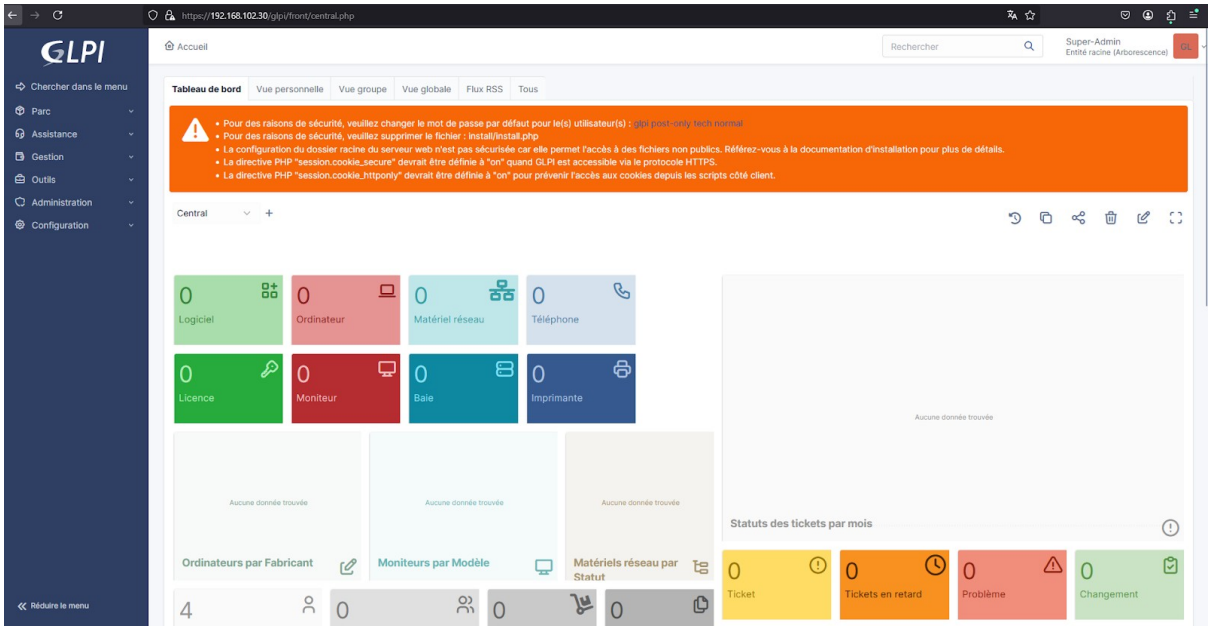
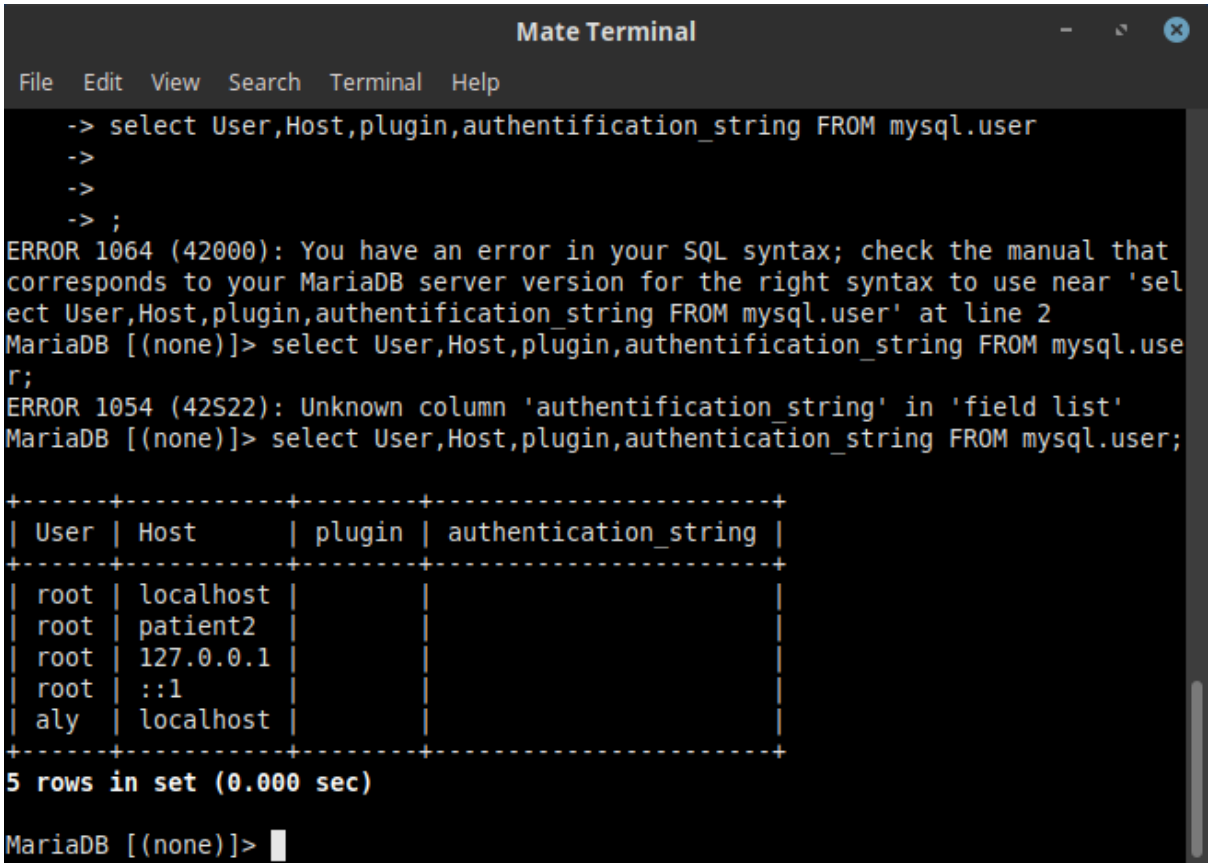


schéma de notre archtecture fait sur lucidchart.com

ANNEXE C

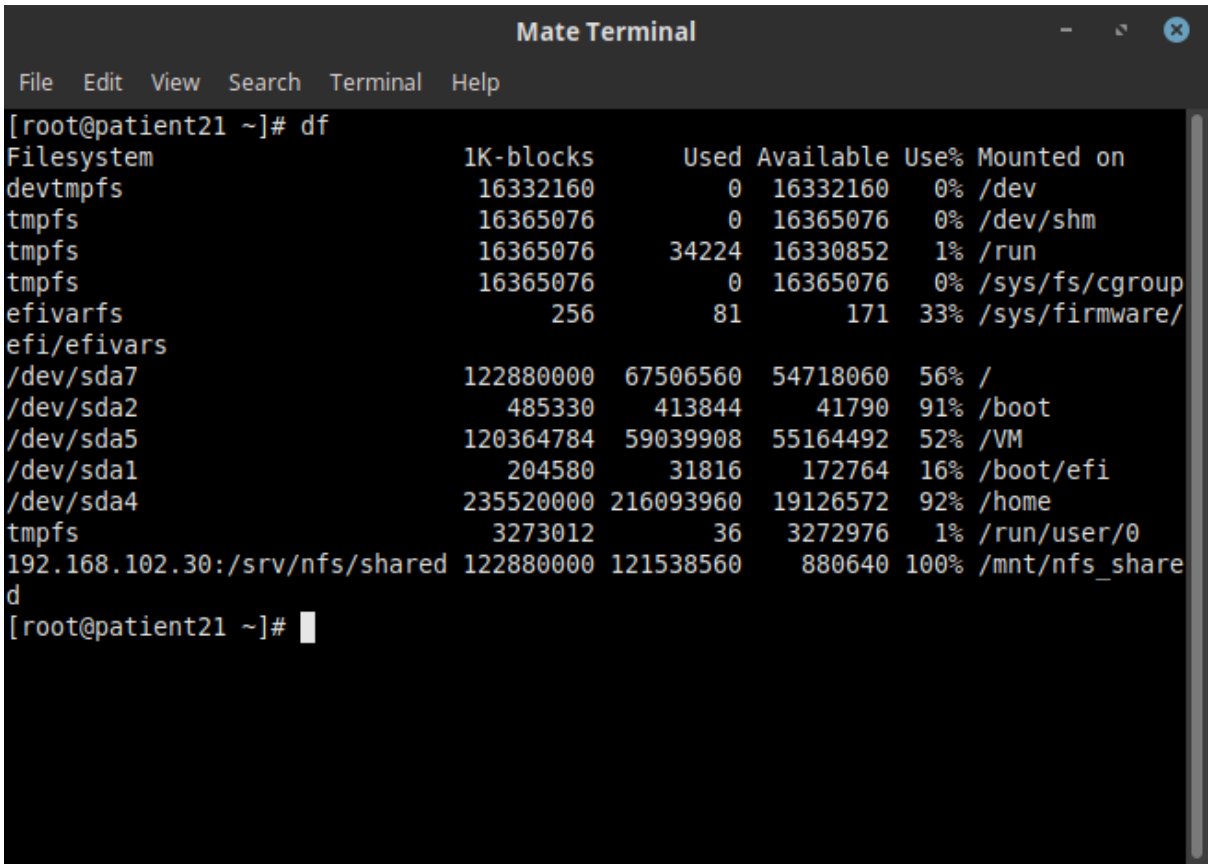


Interface du GLPI



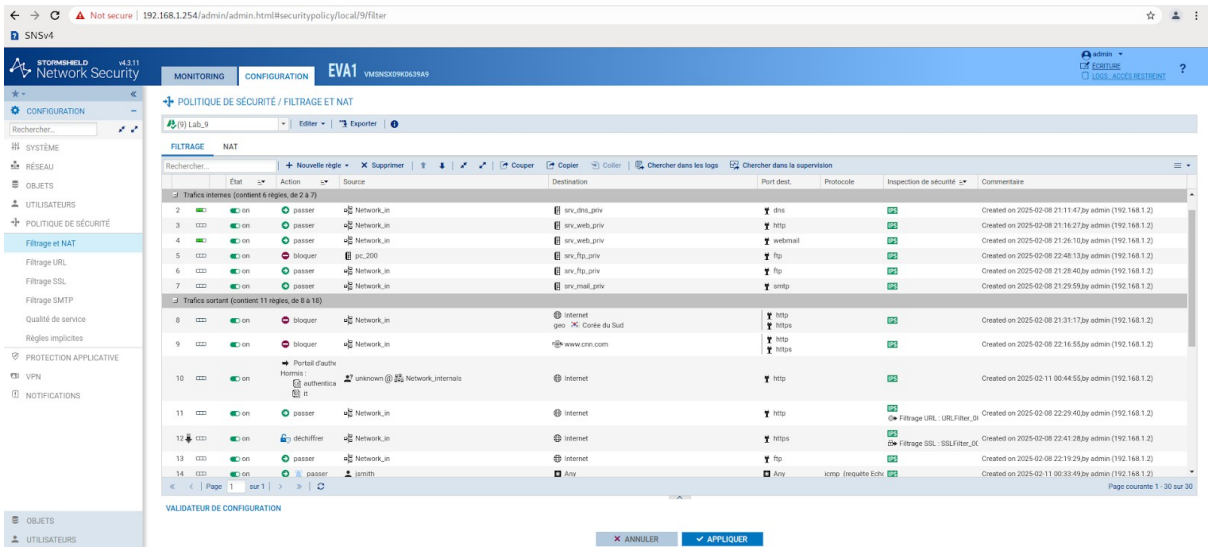
MaraiDB pour la mise en place du glpi

ANNEXE D

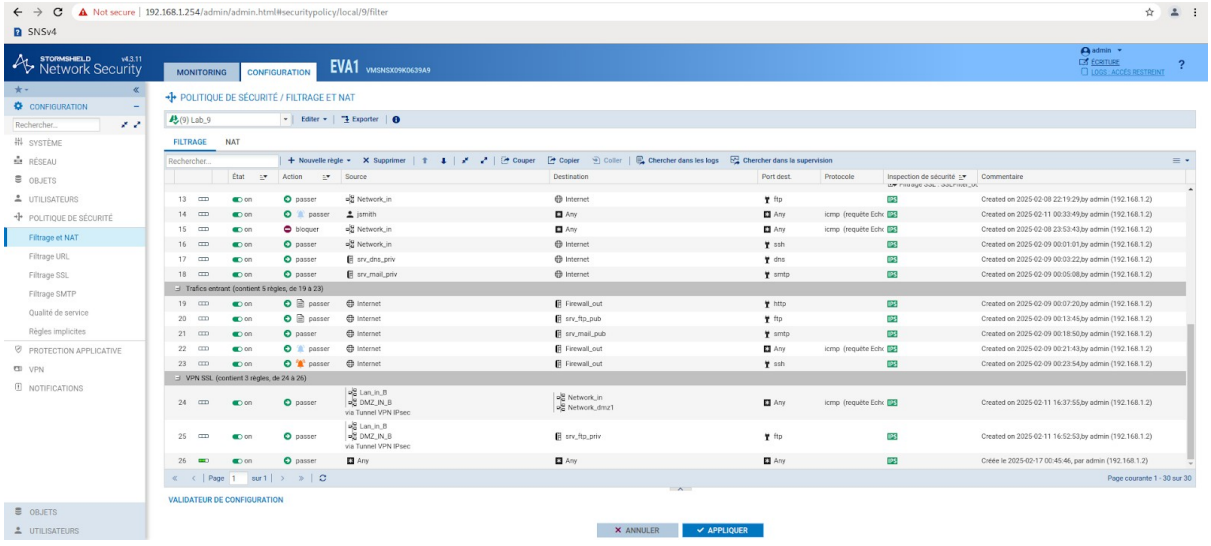


Vérification du montage des fichiers du serveur NFS

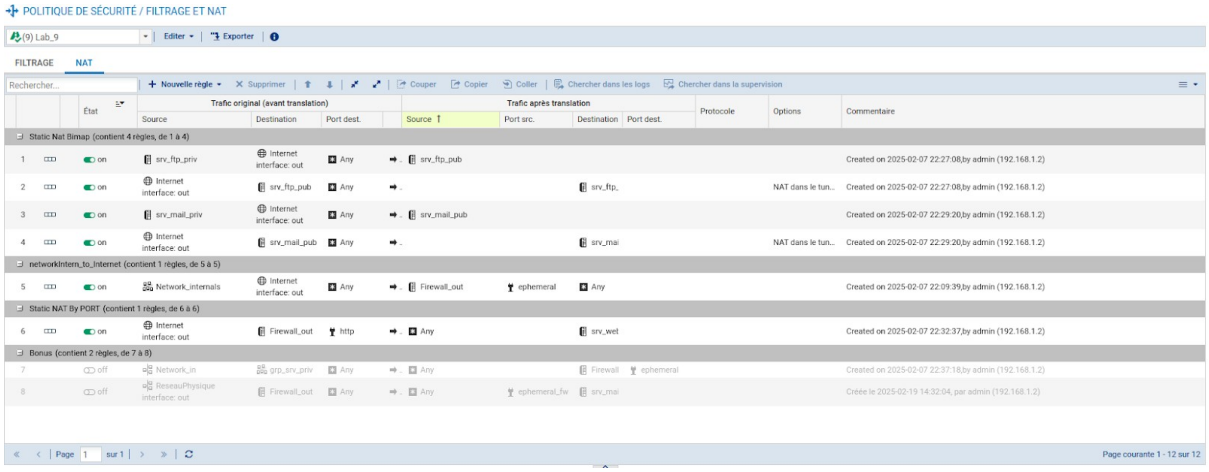
ANNEXE E



Règles de filtrage définie dans l'entreprise A (partie 1)

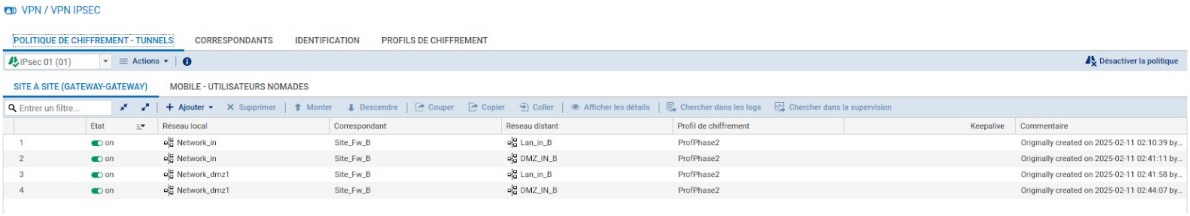


Règles de filtrage définie dans l'entreprise A (partie 2)

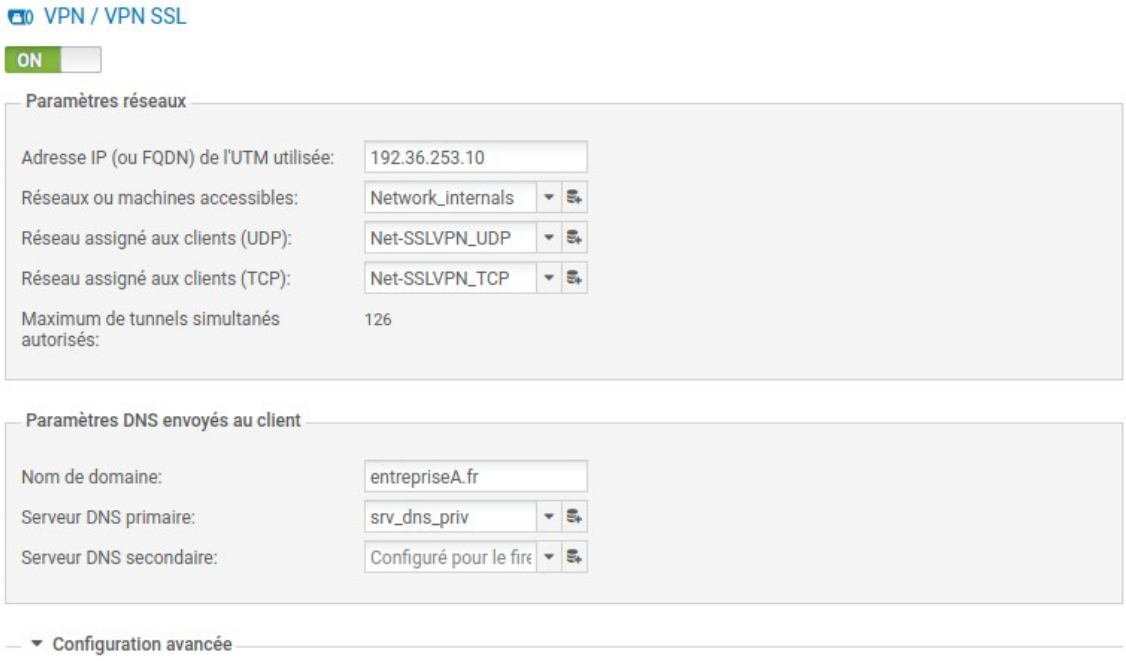


Filtrage NAT

ANNEXE F



Règles VPN IPSec



Mise en place du VPN SSL