RAPPORT DE PROJET DE FIN DE MODULE PROTOCOLES DE SÉCURITÉ ET SÉCURITÉ DES RÉSEAUX ET DES COMMUNICATIONS

Architecture D’entreprise H.A

Réalisé par:

ADIL EL KHAIDER

AYMEN BOURHAT

JIHANE ELMOURABIT

SANOGO CHEIKNA

ZAKARIA OUAHI

Encadré par:

Pr. AZOUGAGHE Ali

Année universitaire : 2024/2025

Remerciement

Nous tenons à exprimer nos sincères remerciements à M. Ali Azougaghe, notre encadrant, pour son précieux soutien et ses conseils avisés tout au long de la réalisation de ce projet. Sa disponibilité, son expertise et ses encouragements constants ont été des éléments clés dans la conception et la mise en œuvre de l'architecture haute disponibilité (HA) avec FortiGate.

Grâce à ses orientations, nous avons pu surmonter les défis techniques et approfondir nos connaissances dans les domaines du réseau et de la sécurité. Son encadrement a non seulement contribué à la réussite de ce projet, mais aussi enrichi notre apprentissage en nous permettant de développer des compétences essentielles pour notre future carrière.

Nous souhaitons également remercier chaleureusement nos collègues du groupe de travail pour leur collaboration étroite, leur détermination et leur expertise partagée. Chaque membre a apporté une contribution précieuse qui a enrichi notre projet et renforcé notre compréhension des défis liés à ce projet.

Enfin, nous tenons à exprimer notre gratitude envers l'École Nationale des Sciences Appliquées de Marrakech pour nous offrir un environnement propice à l'apprentissage et à l'exploration de projets innovants en Protocoles de sécurité .

Résumé

Ce projet vise la conception et la mise en œuvre d'une architecture réseau à haute disponibilité (HA) intégrant des dispositifs FortiGate, dans le cadre de la sécurisation et de l'optimisation des infrastructures informatiques. L'objectif principal est d'assurer une continuité de service, même en cas de défaillance matérielle ou logicielle, tout en garantissant une sécurité renforcée pour les données et les communications.

Dans ce cadre, nous avons étudié les principes fondamentaux de la redondance et de la tolérance aux pannes, ainsi que les fonctionnalités avancées offertes par les pare-feu FortiGate, telles que le basculement automatique (failover), la gestion centralisée et les politiques de sécurité. La solution a été conçue et simulée dans un environnement virtualisé utilisant GNS3, ce qui a permis de valider les performances et la résilience de l'architecture.

Le projet inclut également une réflexion sur la segmentation réseau à travers VLANs, la configuration des routes dynamiques et statiques, ainsi que l'implémentation de politiques de sécurité adaptées aux besoins de l'entreprise.

Les résultats obtenus démontrent la robustesse et l'efficacité de l'architecture mise en place, offrant un modèle exploitable pour les entreprises cherchant à renforcer la disponibilité et la sécurité de leurs systèmes.

Table des Matières

Liste des Figures

1 *Introduction Générale*

Dans un monde où les technologies de l'information jouent un rôle crucial dans le fonctionnement des entreprises et des organisations, la disponibilité et la sécurité des infrastructures informatiques sont devenues des priorités stratégiques. Les pannes, les cyberattaques et les défaillances matérielles ou logicielles peuvent avoir des conséquences graves, allant de la perte de données à l'arrêt des activités critiques. Pour faire face à ces défis, l'adoption d'architectures réseau à haute disponibilité (HA) et sécurisées s'impose comme une nécessité incontournable.

Ce rapport s'inscrit dans le cadre d'un projet ayant pour objectif la conception et la mise en œuvre d'une architecture réseau à haute disponibilité, en utilisant les solutions FortiGate. Cette approche vise à garantir une continuité de service, même en cas de défaillances, grâce à des mécanismes avancés tels que le basculement automatique (failover), la redondance des composants critiques et la segmentation réseau via VLANs. En parallèle, des politiques de sécurité rigoureuses ont été intégrées pour protéger les données et les communications contre les menaces internes et externes.

La réalisation de ce projet repose sur une démarche méthodique, combinant une étude approfondie des concepts théoriques avec une implémentation pratique simulée dans un environnement virtualisé utilisant GNS3. Les étapes clés incluent la configuration des pare-feu FortiGate, la mise en place de routage dynamique et statique, ainsi que l'application de stratégies de sécurité adaptées. Ce rapport présente en détail les défis rencontrés, les solutions apportées et les résultats obtenus, tout en mettant en lumière les avantages d'une telle architecture pour répondre aux besoins des entreprises modernes.

Pour structurer ce rapport, nous proposons le plan suivant :

1. **Chapitre 1 : Contexte Général**
   Nous décrirons le contexte du projet, notamment la présentation de l'établissement, des filières, et des problématiques spécifiques auxquelles répond ce projet. Une analyse des besoins sera également réalisée.

2. **Chapitre 2 : Conceptions, Outils et Technologies**
   Ce chapitre détaillera les concepts de haute disponibilité, les technologies et protocoles

utilisés, ainsi que les outils comme GNS3, VMware, et FortiGate.

3. **Chapitre 3 : Implémentation et Réalisation**
   Nous présenterons ici les étapes pratiques du projet, incluant la configuration réseau, la mise en place des VLANs et des mécanismes de haute disponibilité.

4. **Conclusion Générale et Perspectives**
   Enfin, nous synthétiserons les résultats obtenus et proposerons des pistes d'amélioration pour de futures réalisations.

Ce rapport vise à présenter en détail les défis rencontrés, les solutions apportées, et les résultats obtenus, tout en mettant en lumière les avantages d'une telle architecture pour répondre aux besoins des entreprises modernes. En conclusion, ce projet constitue non seulement une réponse aux exigences de résilience et de sécurité des systèmes actuels, mais aussi une opportunité d'approfondir nos compétences techniques et de mieux comprendre les enjeux liés à la gestion des infrastructures critiques.

Chapitre 1 : Contexte Général

2 Chaptire 1: Contexte Général

2.1 Introduction

Dans ce chapitre est consacré à la présentation du contexte général dans lequel s'inscrit ce projet. Il vise à situer l'importance de la haute disponibilité (HA) dans les environnements informatiques modernes et à expliquer les raisons pour lesquelles les solutions FortiGate ont été choisies pour répondre à ces besoins. Nous aborderons également les problématiques clés liées à la continuité de service, à la gestion des pannes et aux menaces croissantes dans le domaine de la cybersécurité.

2.2 Présentation de l'établissement

Créée en 2000, l'École Nationale des Sciences Appliquées de Marrakech (ENSA Marrakech) est un établissement public rattaché à l'Université Cadi Ayyad. Sa vocation est de former des ingénieurs d'État compétents et capables d'innover. L'école met un point d'honneur à promouvoir l'excellence à tous les niveaux de formation et dans ses activités de recherche. Première école de ce type dans la région de Marrakech-Safi, l'ENSA Marrakech s'est distinguée par son engagement à tisser des liens solides avec le tissu socio-économique local et national. Son objectif actuel est de consolider sa réputation parmi les grandes écoles d'ingénieurs du Maroc.

Figure 1: l'École Nationale des Sciences Appliquées de Marrakech

2.3 Présentation des filières

2.3.1 Génie Cyber-Défense et Systèmes de Télécommunications Embarqués

La filière de génie cyberdéfense et systèmes de télécommunications embarqués vise à former des ingénieurs hautement qualifiés avec de solides compétences scientifiques. Elle combine des méthodes et techniques de sécurité et de gestion des risques liés aux systèmes d'information, tout

en enseignant la conception de systèmes de télécommunications embarqués. Cette formation prépare chaque élève ingénieur à utiliser des méthodes et des outils pour lutter contre la cybercriminalité, combler les failles des systèmes d'information, et résoudre les problèmes de sécurité numérique. En outre, elle leur permet de mettre en œuvre des systèmes embarqués dans diverses applications telles que l'avionique et l'automobile.

2.3.2 Génie Industriel et Logistique

Le programme de Génie Industriel et Logistique forme des ingénieurs polyvalents capables d'optimiser les processus de production et de gérer les chaînes d'approvisionnement. Les étudiants développent des compétences en gestion de la qualité, en logistique et en amélioration continue, et apprennent à répondre aux besoins des entreprises tout en respectant les principes de durabilité. Cette formation leur permet d'acquérir une vision globale et systémique des processus industriels, les préparant à travailler dans divers secteurs. Les diplômés sont particulièrement bien équipés pour contribuer à la transformation de l'industrie marocaine vers l'Industrie 4.0, en alliant efficacité et innovation.

2.3.3 Génie Informatique

La filière Génie Informatique prépare les étudiants à concevoir et développer des solutions logicielles et systèmes informatiques innovants. Les diplômés acquièrent des compétences solides en programmation, gestion des systèmes d'information et en technologies émergentes. Grâce à une formation axée sur la pratique, ils sont capables d'identifier et de répondre aux besoins des utilisateurs en matière de technologies numériques. Ils apprennent également à gérer des projets complexes, à travailler en équipe, et à appliquer des méthodologies modernes de développement. La polyvalence de cette formation permet aux ingénieurs en informatique de s'intégrer aisément dans divers secteurs d'activité, que ce soit au niveau national ou international.

2.3.4 Réseaux, Systèmes Services Programmables

Cette filière forme des ingénieurs spécialisés dans la conception, la gestion et l'optimisation des infrastructures de réseaux et systèmes de communication. Les étudiants acquièrent une maîtrise des technologies réseaux, des systèmes programmables et des services informatiques. La formation comprend des stages en entreprise, permettant aux étudiants de mettre en pratique leurs connaissances dans des contextes réels. Les diplômés possèdent les compétences

nécessaires pour intervenir dans des domaines variés tels que les télécommunications, le cloud computing et l'informatique embarquée, répondant ainsi aux besoins croissants de connectivité et de flexibilité des entreprises modernes.

2.3.5 Systèmes Electroniques Embarqués et Commande des Systèmes

La filière Génie des Systèmes Electroniques Embarqués et Commande des Systèmes offre une formation pluridisciplinaire, préparant les étudiants aux secteurs dynamiques tels que l'électronique, la robotique, l'aéronautique, les énergies renouvelables et l'automobile. Les cours intègrent des compétences en systèmes automatisés, réseaux électriques et systèmes embarqués. Les étudiants acquièrent des connaissances techniques de pointe, alliant théorie et pratique, afin de s'adapter aux nouvelles technologies et aux exigences des industries modernes. La formation met également l'accent sur le développement de l'esprit critique et de l'innovation, assurant ainsi que les diplômés soient prêts à relever les défis d'un environnement en constante évolution.

2.4 Presentation du projet

2.4.1 Problematique

La mise en œuvre d'une architecture de Haute Disponibilité dans un environnement informatique comporte plusieurs défis complexes qui doivent être abordés de manière structurée :

- **Redondance et Tolérance aux Pannes**
  Comment minimiser les interruptions en cas de défaillance d'un composant essentiel ?
  Quelles stratégies de redondance permettent de garantir la continuité des services ?

- **Évolutivité et Scalabilité**
  Comment adapter l'architecture à la croissance de l'entreprise sans compromettre la disponibilité des systèmes ?
  Comment gérer l'augmentation de la charge de travail de manière dynamique et efficace?

- **Gestion de la Charge**
  Comment répartir équitablement les charges de travail entre différents composants pour éviter les goulets d'étranglement ?
  Quels outils et algorithmes sont nécessaires pour un équilibrage optimal des charges?

- **Sécurité et Protection des Données**

  Comment assurer la sécurité des informations tout en garantissant une disponibilité continue des services?

  Quelles mesures de chiffrement et de contrôle d'accès conviennent à une architecture HA?

- **Surveillance et Maintenance**

  Comment détecter rapidement les anomalies grâce à une surveillance proactive?

  Comment effectuer des opérations de maintenance sans compromettre la continuité des services?

- **Coûts et Ressources**

  Comment équilibrer les investissements nécessaires avec les besoins réels et les contraintes budgétaires?

  Quels compromis peuvent être faits pour optimiser le rapport coût-efficacité ?

  Ces problématiques reflètent la complexité inhérente à la conception d'une architecture informatique robuste et performante, où les compromis entre sécurité, disponibilité et coût doivent être finement équilibrés.

2.4.2 Solutions Proposées par l'Application

Pour relever ces défis, plusieurs approches et solutions technologiques sont proposées dans le cadre de ce projet :

- **Redondance et Réplication**

  Mise en place de serveurs de secours avec réplication en temps réel pour garantir la continuité des données et services en cas de panne.

- **Basculement Automatique**

  Implémentation de mécanismes de basculement automatiques pour assurer une transition fluide vers des systèmes de secours en cas de défaillance.

- **Surveillance Proactive**

  Utilisation d'outils avancés pour surveiller en temps réel la santé des systèmes, anticiper les problèmes et intervenir de manière préventive.

- **Scalabilité Horizontale**

  Conception d'une architecture flexible permettant d'ajouter des ressources (serveurs, stockage) sans interruption de service.

- **Plan de Reprise d'Activité (PRA)**

  Élaboration d'un plan structuré pour rétablir les services critiques rapidement après une catastrophe majeure.

- **Sécurité Renforcée**

  Mise en œuvre de pare-feu, protocoles de chiffrement, et systèmes d'authentification pour protéger les données sensibles tout en assurant un accès rapide.

Ces solutions s'appuient sur des technologies modernes et des bonnes pratiques éprouvées pour répondre efficacement aux besoins spécifiques de Haute Disponibilité.

2.5 Étude d'existence :

Le paysage informatique moderne exige une disponibilité ininterrompue des services critiques. Les interruptions de service peuvent entraîner des pertes financières et endommager la réputation d'une entreprise. Dans ce contexte, la mise en oeuvre d'une solution de Haute Disponibilité (HA) pour notre infrastructure apparaît comme une nécessité pour garantir une continuité opérationnelle sans faille. Pour ce faire, il est crucial de considérer les différentes approches disponibles sur le marché dont on trouve :

Architecture N-Tiers : Cette approche vise à répartit les composants d'une application sur plusieurs niveaux pour isoler les fonctions et réduire les points de défaillance.

Mise en oeuvre de Clusters : Cette approche implique la création de clusters de serveurs interconnectés qui travaillent ensemble pour fournir une disponibilité continue. En cas de défaillance d'un serveur, le trafic est redirigé vers d'autres serveurs du cluster.

Virtualisation : La virtualisation permet de créer des machines virtuelles (VM) indépendantes du matériel physique. En cas de défaillance matérielle, les VM peuvent être migrées vers d'autres hôtes sans interruption de service.

Équilibreurs de Charge (Load Balancers) : Répartit équitablement la charge de travail entre plusieurs serveurs pour éviter la surcharge et améliorer les performances. Les

équilibreurs de charge peuvent également rediriger le trafic en cas de défaillance d'un serveur.

Utilisation de Services Cloud : Externaliser l'infrastructure vers des services cloud tels que AWS, Azure ou Google Cloud, qui offrent souvent des solutions de HA intégrées

Utilisation de Pare-feu : Intégrer des pare-feu haute performance comme Fortinet FortiGate ou Sophos XG pour renforcer la sécurité et garantir une haute disponibilité

2.6 Analyse des besoins

2.6.1 Analyse des besoins fonctionnelle

- **Configuration de Fortigate Firewall** : Le système doit permettre la configuration aisée des paramètres de Fortigate Firewall, y compris les règles de sécurité, les listes d'accès, et les politiques de filtrage. Il doit être possible de définir des configurations spécifiques pour chaque instance de Firewall dans le cadre de l'architecture de haute disponibilité.

- **Intégration avec l'Architecture de Haute Disponibilité** : Le système doit permettre l'intégration fluide de Fortigate Firewall dans une architecture de haute disponibilité, assurant une redondance et une continuité opérationnelle maximales.

- **Mécanismes de Basculement Automatique** : Le système doit prendre en charge des mécanismes de basculement automatique en cas de défaillance d'une instance de Firewall, assurant ainsi un accès ininterrompu aux services.

- **Gestion Centralisée des Politiques de Sécurité** : AIl doit être possible de gérer centralement les politiques de sécurité de toutes les instances de Fortigate Firewall, facilitant ainsi une administration cohérente.

2.6.2 Analyse des besoins non fonctionnels

- **Performances** : Le pare-feu FortiGate doit garantir des performances exceptionnelles même sous des charges élevées, assurant une réactivité en temps réel et la gestion de grandes quantités de trafic sans compromettre la sécurité ou la stabilité du réseau.

- **Sécurité** : Les politiques de sécurité mises en place sur FortiGate doivent être rigoureusement appliquées, offrant une protection avancée contre une large gamme de menaces, notamment les attaques DDoS, les malwares, et les intrusions, grâce à des fonctionnalités

telles que la prévention des intrusions (IPS), l'analyse en temps réel et le filtrage des contenus.

- **Évolutivité** : Le système FortiGate doit être conçu pour évoluer avec les besoins croissants de l'entreprise. Il doit permettre l'ajout d'instances supplémentaires et la gestion de multiples déploiements de pare-feu, tout en maintenant la stabilité et les performances globales du réseau.
- **Gestion des Autorisations d'Accès** : Permettre aux administrateurs du système de gérer les autorisations d'accès en définissant les utilisateurs et les groupes autorisés à visualiser les caméras dans différentes zones du campus.
- **Disponibilité** : La disponibilité du réseau doit être maximale grâce à des mécanismes de haute disponibilité intégrés dans FortiGate, notamment le basculement automatique (failover) et la réplication des configurations entre les pare-feu. Cela permet de réduire au minimum les temps d'arrêt et d'assurer la résilience face aux incidents.
- **Simplicité d'Administration** : L'interface d'administration de FortiGate doit être intuitive et conviviale, permettant aux administrateurs de gérer efficacement la configuration du pare-feu, de surveiller les performances et de répondre rapidement aux alertes de sécurité. Des outils de gestion centralisée, tels que FortiManager, doivent être utilisés pour simplifier les tâches complexes.
- **Conformité aux Normes de Sécurité** : FortiGate doit être conforme aux normes de sécurité reconnues, telles que celles édictées par le NIST et l'ISO/IEC 27001, garantissant ainsi la fiabilité et la légitimité des opérations du pare-feu. Cela assure une conformité continue aux exigences réglementaires de sécurité des données et de la confidentialité.

2.7 conclusion

Ce premier chapitre a permis de poser le cadre général du projet en identifiant les problématiques clés et les solutions envisageables pour l'implémentation d'une architecture informatique hautement disponible. En mettant l'accent sur des aspects essentiels comme la redondance, la scalabilité et la sécurité, ce projet cherche à répondre aux besoins des entreprises modernes, confrontées à des défis croissants en matière de continuité de service et de protection des données. Les différentes solutions analysées ont

permis de dégager une approche adaptée pour garantir une infrastructure résiliente et performante. Les étapes suivantes de ce projet consisteront à détailler les méthodologies et outils choisis pour la mise en œuvre de l'architecture, ainsi qu'à évaluer la performance de la solution dans un environnement simulé. Cette démarche structurée et progressive assurera que l'architecture proposée répond non seulement aux objectifs fixés, mais aussi aux contraintes spécifiques liées à la sécurité et à la gestion des infrastructures informatiques.

Chapitre 2 : Conception, Outils et Technologies

3 Chaptire 2: Conceptions, Outils et Technologies

Ce chapitre explore les concepts fondamentaux et les technologies associés à la Haute Disponibilité (H.A.), au routage, et aux types de liaisons (redondance et agrégation). Ces éléments constituent les bases théoriques nécessaires pour concevoir et mettre en œuvre une architecture informatique résiliente et performante.

3.1 Conception d'haute disponibilité :

La Haute Disponibilité désigne la capacité d'un système informatique à rester opérationnel, même en cas de défaillances matérielles, logicielles ou de catastrophes. Elle repose sur trois principes fondamentaux :

- **Redondance** La duplication des composants critiques (serveurs, bases de données, réseaux) permet d'assurer la continuité des services en cas de panne.
- **Fiabilité** Les systèmes H.A. doivent minimiser les temps d'arrêt grâce à des mécanismes tels que la détection rapide des pannes et des plans de reprise automatisés.
- **Tolérance aux pannes** Une architecture H.A. intègre des mécanismes qui permettent au système de continuer à fonctionner même en cas de défaillance partielle.

3.1.1 Technologies et Protocoles associés à la H.A :

- **Clusterisation** : Permet de regrouper plusieurs serveurs pour répartir la charge et assurer la redondance.
- **Load Balancing** (équilibrage de charge) : Redistribue dynamiquement les demandes sur plusieurs ressources pour éviter la surcharge d'un composant unique.
- **Virtualisation** : Favorise la migration de machines virtuelles en cas de panne.
- **Protocoles H.A**. : VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Router Protocol).

3.2 Routage

Le routage est un processus essentiel pour acheminer les données d'un point à un autre sur un réseau. Il détermine le chemin optimal pour transmettre les paquets tout en garantissant performance et fiabilité.
Types de Routage :

- **Routage Statique** Les chemins sont configurés manuellement par l'administrateur réseau. Avantages : Simplicité et contrôle.
  Inconvénients : Manque de flexibilité en cas de changement dans le réseau.
- **Routage Dynamique** Les routes sont apprises et ajustées automatiquement grâce à des protocoles de routage. Protocoles courants :
  - RIP (Routing Information Protocol) : Utilise le nombre de sauts pour déterminer le chemin optimal.
  - OSPF (Open Shortest Path First) : Se base sur l'état du réseau pour calculer les chemins les plus courts.
  - BGP (Border Gateway Protocol) : Principalement utilisé pour interconnecter les réseaux sur Internet.

  Avantages : Adaptabilité aux changements.
  Inconvénients : Complexité de configuration.
- **Routage basé sur des politiques** (Policy-Based Routing) Permet de définir des règles spécifiques pour contrôler les flux de trafic en fonction de critères (IP source/destination, protocole, etc.).

3.3 Types de Liaison : Redondance et Agrégation

3.3.1 Redondance

La redondance consiste à dupliquer les chemins ou composants critiques pour assurer la continuité des services en cas de défaillance.

- **Redondance Active-Passive** : Un composant reste en veille et n'intervient qu'en cas de panne du composant actif.

- **Redondance Active-Activ**e : Tous les composants redondants sont utilisés simultanément pour optimiser les performances tout en garantissant la tolérance aux pannes.

Technologies courantes :

1. Spanning Tree Protocol (STP) : Empêche les boucles dans les réseaux redondants.
2. Multi-Chassis Link Aggregation (MLAG) : Répartition des charges sur plusieurs liaisons tout en assurant la redondance.

3.3.2 Agrégation

L'agrégation consiste à combiner plusieurs liaisons physiques pour créer une liaison logique plus performante.

Objectifs de l'agrégation :

- Augmentation de la bande passante.
- Répartition de la charge sur plusieurs liaisons.
- Amélioration de la tolérance aux pannes.

Protocole associé : Link Aggregation Control Protocol (LACP)

Permet d'automatiser la création et la gestion des liaisons agrégées. Assure une redondance et une résilience accrues en répartissant dynamiquement les charges.

3.4 Outils et Technologies Utilisés

3.4.1 GNS3

Définition :

GNS3, Graphical Network Simulator-3, est une plateforme de simulation réseau open-source qui joue un rôle crucial dans notre environnement de travail. Cet outil offre une interface graphique intuitive pour concevoir, modéliser et tester des topologies réseau complexes.

L'utilisation de GNS3 dans notre projet s'articule autour des axes suivants :

1. **Virtualisation des réseaux** : GNS3 permet l'intégration de dispositifs virtuels tels que des routeurs, commutateurs et pare-feu. Ces périphériques, sous forme d'images logicielles, reproduisent fidèlement le comportement d'appareils réels.
2. **Simulation réaliste** : Il permet de simuler et d'interconnecter des équipements réseau pour valider des configurations ou analyser des scénarios diversifiés sans matériel physique.
3. **Flexibilité et accessibilité** : Compatible avec plusieurs systèmes d'exploitation (Windows, macOS, Linux), GNS3 s'adapte à différents besoins, qu'il s'agisse d'apprentissage, de recherche ou de tests avancés.
4. **Communauté active** : Une base d'utilisateurs mondiale partage des ressources et des topologies, facilitant la collaboration et l'apprentissage.

Dans notre projet, GNS3 est utilisé pour modéliser une architecture H.A, tester les configurations, et valider les politiques de sécurité avant leur déploiement réel.

Figure 2: GNS3

3.4.2 VMware Workstation

Définition :

VMware Workstation est un outil de virtualisation qui joue un rôle complémentaire à GNS3 en fournissant un environnement robuste pour tester les configurations réseau et services essentiels.

Fonctionnalités : Les principales fonctionnalités utilisées dans ce projet incluent :

1. **Création de machines virtuelle**s : Il permet d'héberger des serveurs dédiés à des rôles critiques (serveurs DHCP, DNS, ou HTTP) pour simuler une architecture réseau complète.
2. **Snapshots et tests avancés** : Les instantanés facilitent les scénarios de basculement et les tests de redondance sans compromettre l'intégrité des configurations.

3. **Simulation de réseaux complexes** : L'intégration réseau avancée permet de connecter les machines virtuelles entre elles ou avec GNS3, notamment pour valider les performances de protocoles de redondance comme HSRP et des mécanismes de commutation comme 802.1Q.

Figure 3: VM Ware

3.4.3 PC:

- **Description** : Un ordinateur personnel est utilisé pour la gestion et la configuration des équipements réseau.
- **Rôle** : Sert d'interface pour accéder aux différents dispositifs via des protocoles comme SSH, HTTP ou une console CLI. Il est également utilisé pour la surveillance et l'analyse du réseau.

Figure 4: Webterm

3.4.4 Switch (Cisco IOU 15.2d)

- **Description** :Un commutateur réseau Cisco utilisant une version IOU (IOS on Unix) pour les tests et simulations.
- **Rôle** : Connecte plusieurs appareils dans un réseau local (LAN).
  Transfère les données de manière intelligente en se basant sur les adresses MAC.
  Supporte la segmentation du réseau en VLANs pour améliorer la performance et la sécurité.

Figure 5: Switch Cisco

3.4.5 Firewall (Fortigate 7.0.0)

- **Description** :Un pare-feu FortiGate est un dispositif de sécurité réseau capable de contrôler le trafic entrant et sortant en se basant sur des politiques de sécurité définies.
- **Rôle** : Filtrer les données pour empêcher les accès non autorisés et protéger le réseau contre les attaques ou intrusions.
  Fournir des fonctionnalités supplémentaires telles que l'inspection des paquets, la prévention des intrusions (IPS), et des VPN pour une connectivité sécurisée.
- **Caractéristiques principales** : Fonctionnalités avancées comme la gestion unifiée des menaces (UTM), la détection des malwares et la gestion centralisée..

Figure 6: fortigate firewall

3.4.6 Cloud

- **Description** :Le Cloud est utilisé comme une extension du réseau local pour offrir des services à distance, notamment le stockage, l'accès aux applications, et la gestion centralisée.
- **Rôle** :
  Fournir une solution flexible pour les sauvegardes et les services distants.
  Réduire les besoins en infrastructures physiques tout en offrant une haute disponibilité et une évolutivité rapide.

– **Caractéristiques principales** : Accès sécurisé via des protocoles comme HTTPS et VPN. Supporte des services comme la sauvegarde automatique et la synchronisation.

Figure 7: cloud

3.5 Protocoles

3.5.1 Protocoles de gestion et de surveillance

HTTP (Hypertext Transfer Protocol) :

- **Définition** : Protocole de communication utilisé pour transférer des données sur le web. Dans les réseaux, il est utilisé pour accéder aux interfaces web des équipements comme les routeurs et les commutateurs.
- **Objectif** : Fournir une interface utilisateur conviviale permettant aux administrateurs de surveiller et de configurer les périphériques réseau à distance via un navigateur.
- **Fonctionnalités** :
  Supporte la consultation et la configuration des paramètres réseau via une interface graphique.
  Compatible avec des protocoles sécurisés comme HTTPS (HTTP sécurisé).
- **Exemple d'utilisation** : Configuration initiale d'un commutateur via son interface web.

SSH (Secure Shell) :

- **Définition** : Protocole sécurisé permettant l'administration distante des équipements réseau.
- **Objectif** : Garantir une communication sécurisée entre un administrateur et un appareil, même dans un environnement réseau non sûr.
- **Fonctionnalités** :
  Offre une connexion chiffrée, protégeant les informations sensibles.
  Permet de gérer les routeurs et commutateurs via une interface en ligne de commande.

- **Exemple d'utilisation** : Administration d'un routeur depuis un poste distant pour modifier ses règles de routage.

3.5.2 Protocoles de redondance et haute disponibilité

HSRP (Hot Standby Router Protocol) :

- **Définition** : Protocole de redondance propriétaire de Cisco qui assure une passerelle par défaut virtuelle.
- **Objectif** : Garantir une continuité de service en cas de défaillance du routeur principal.
- **Fonctionnalités** :
  Élection d'un routeur actif et d'un routeur en veille. Surveillance continue pour basculer automatiquement vers le routeur et Mise en place d'une passerelle redondante pour les utilisateurs dans un réseau d'entreprise.e secours en cas de panne.

3.5.3 Protocoles de commutation

VLAN (802.1Q):

- **Définition** : Protocole utilisé pour créer des réseaux locaux virtuels (VLAN) en segmentant logiquement un réseau physique.
- **Objectif** : Améliorer la gestion, la sécurité et la performance du réseau.
- **Fonctionnalités** : Permet le marquage des trames pour identifier leur VLAN d'appartenance. Assure l'isolation des données entre différents VLANs.
- **Exemple d'utilisation** : Création d'un VLAN pour les employés du département IT et d'un autre pour le département RH afin de segmenter le trafic réseau.

STP (Spanning Tree Protocol) :

- **Définition** : Protocole de couche 2 utilisé pour éviter les boucles dans les réseaux Ethernet et assurer la redondance des chemins.
- **Objectif** : Prévenir les boucles réseau tout en maintenant des chemins alternatifs pour améliorer la résilience.

- **Fonctionnalités** : Élection d'un commutateur root et désactivation des chemins redondants. Réactivation des chemins alternatifs en cas de panne.
- **Exemple d'utilisation** : Réseau commuté avec plusieurs connexions redondantes pour garantir une connectivité constante.

3.5.4 Protocoles de commutation

DHCP (Dynamic Host Configuration Protocol) :

- **Définition** : Protocole réseau qui attribue automatiquement des adresses IP aux appareils connectés.
- **Objectif** : Simplifier la gestion des adresses IP et garantir qu'aucun conflit d'adresse ne se produit.
- **Fonctionnalités** :
  Attribue dynamiquement des adresses IP, des masques de sous-réseau, et des passerelles par défaut.
  Gère automatiquement les plages d'adresses pour différents VLANs.
- **Exemple d'utilisation** : Attribution automatique des adresses IP pour les appareils connectés aux VLANs IT et RH.

DNS (Domain Name System) :

- **Définition** : Protocole qui traduit les noms de domaine en adresses IP pour permettre une navigation simplifiée.
- **Objectif** : Faciliter l'accès aux services réseau et applications en utilisant des noms lisibles au lieu d'adresses IP complexes.
- **Fonctionnalités** :
  Résolution des noms de domaine locaux et externes.
  Haute disponibilité grâce à la redondance des serveurs DNS.
- **Exemple d'utilisation** : Accès à une application interne via un nom de domaine

3.6 conclusion

Ce chapitre a présenté les technologies essentielles utilisées pour concevoir et déployer une architecture réseau robuste et sécurisée. Chaque composant, qu'il s'agisse d'équipements matériels comme les commutateurs et les routeurs, ou de solutions logicielles comme les pare-feu FortiGate et les services Cloud, joue un rôle clé dans l'atteinte des objectifs du projet. L'intégration de ces outils et technologies permet de garantir une connectivité fiable, une sécurité renforcée, et une gestion optimisée du réseau. Ce chapitre souligne également l'importance de combiner ces technologies pour répondre efficacement aux défis modernes en matière de réseaux et de sécurité.

Chapitre 3: Implémentation et Réalisation

4 Chaptire 3 : Implémentation et Réalisation

4.1 Introduction

La configuration des outils informatiques constitue le socle essentiel de tout projet, définissant les paramètres, les fonctionnalités et les performances nécessaires à la réalisation des objectifs fixés. Dans le cadre de notre projet, une attention minutieuse a été accordée à la mise en place et à l'optimisation des outils choisis pour garantir une infrastructure solide et fonctionnelle. Ce chapitre se penche sur les détails et les spécifications de configuration des différents éléments clés que nous avons déployé. De la configuration des pare-feu et des équipements réseau tels que les routeurs et les switches, à l'intégration de logiciels spécifiques et de plateformes de virtualisation, chaque aspect a été soigneusement étudié pour assurer une performance optimale, une sécurité renforcée et une conformité aux exigences du projet. Ce chapitre offre un aperçu approfondi des choix technologiques opérés et des paramètres de configuration adoptés pour soutenir et faciliter la réalisation réussie de notre projet.

4.2 Configuration :

4.2.1 Architecture réseau :

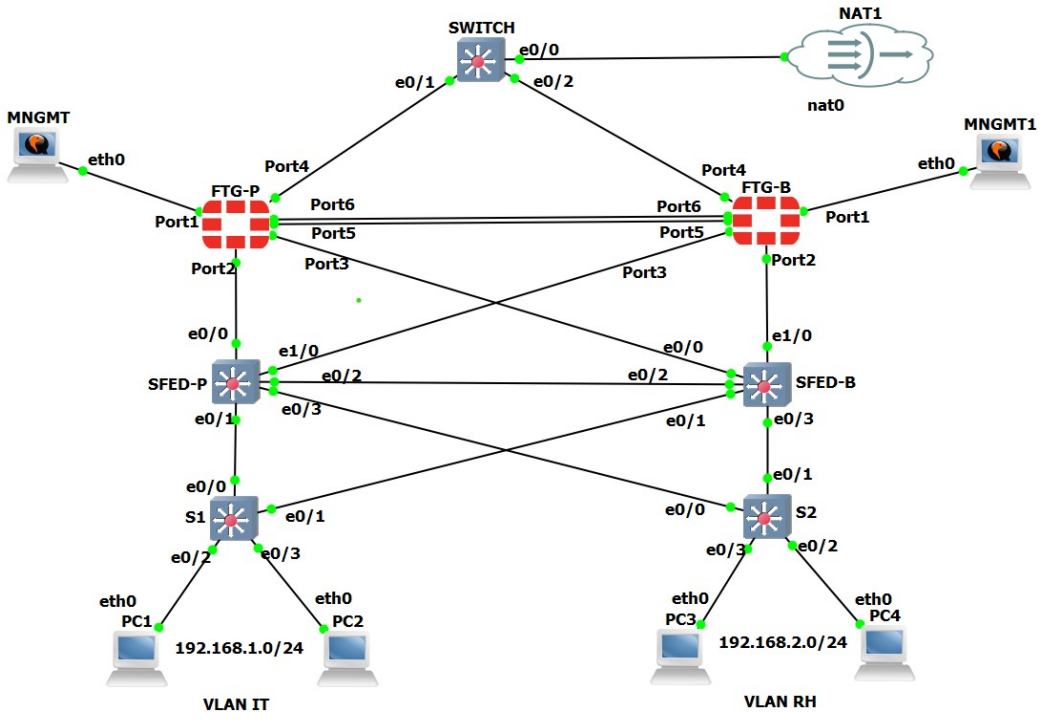

Figure 8: architecture H.A

L'architecture réseau mise en place repose sur un modèle de Haute Disponibilité (HA), intégrant des équipements redondants et des configurations optimisées pour assurer une tolérance aux pannes et une continuité de service. Voici les principaux éléments et leur rôle dans l'infrastructure:

4.2.2 Firewall FortiGate (FTG-P et FTG-B) :

- Deux firewalls FortiGate ont été configurés en mode actif-passif pour assurer la redondance.
- Chaque firewall est connecté à des switches via plusieurs ports (Port1, Port2, Port3, etc.), garantissant une disponibilité en cas de défaillance de l'un des firewalls.
- Ces firewalls gèrent le filtrage du trafic réseau et assurent la sécurité des données entre les VLANs et les accès externes via le NAT.

4.2.3 Switches SFED-P et SFED-B :

- Les switches principaux (SFED-P et SFED-B) sont connectés en redondance avec les firewalls et les switches de distribution (S1 et S2).
- Ils jouent un rôle essentiel dans la communication inter-VLAN et assurent un acheminement rapide et efficace du trafic grâce à la segmentation des VLANs.

4.2.4 Switches de distribution (S1 et S2) :

- Chaque VLAN (IT et RH) est connecté à un switch dédié, permettant de séparer les flux réseau entre les deux départements.
- Ces switches garantissent une connexion stable et sécurisée pour les postes de travail (PC1, PC2, PC3, PC4).

4.2.5 VLANs IT et RH :

Deux VLANs distincts sont configurés :

- VLAN IT (192.168.1.0/24) pour les postes de l'équipe IT (PC1, PC2).
- VLAN RH (192.168.2.0/24) pour les postes de l'équipe RH (PC3, PC4).

4.2.6 VLANs IT et RH :

Deux VLANs distincts sont configurés :

- VLAN IT (192.168.1.0/24) pour les postes de l'équipe IT (PC1, PC2).
- VLAN RH (192.168.2.0/24) pour les postes de l'équipe RH (PC3, PC4).

4.2.7 Cloud NAT :

- La connexion au cloud (via NAT1) permet d'accéder à des ressources externes tout en masquant les adresses IP internes grâce à la translation d'adresse réseau (NAT).

4.2.8 Postes de gestion (MNGMT et MNGMT1) :

- Deux postes de gestion sont dédiés à la supervision et à la configuration des équipements réseau.
- Ils sont connectés directement aux firewalls pour garantir un accès sécurisé à l'administration des dispositifs.

4.3 Configuration de FTG-P:

4.3.1 Configuration des interfaces :

Port 1 (Management - MGMT) :

- Le port 1 a été configuré pour la gestion en mode DHCP, permettant l'obtention automatique d'une adresse IP auprès d'un serveur DHCP.
- Mode : DHCP Client.
- Accès autorisé via HTTPS et SSH pour l'administration à distance

```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode dhcp

FortiGate-VM64-KVM (port1) # set allowaccess http ping

FortiGate-VM64-KVM (port1) # end

FortiGate-VM64-KVM #
```

Figure 9: configuration du port1 pour l'acces MNGMT

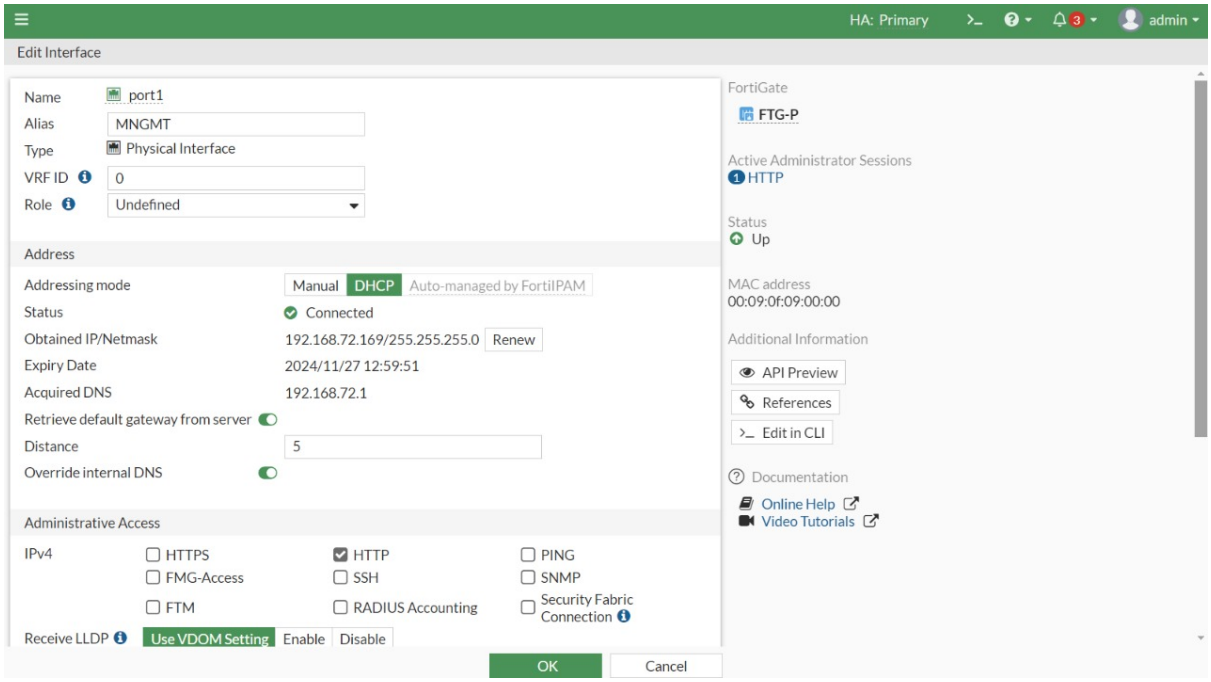

Figure 10: configuration du MNGMT1

Port 4 (Connexion au WAN via le switch lié au Cloud) :

Configuration du port 4 pour le trafic vers le WAN :

- Mode : DHCP Client.
- Permet la connectivité entre le réseau local et Internet via le switch.

```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port4

FortiGate-VM64-KVM (port4) # set mode dhcp

FortiGate-VM64-KVM (port4) # end

FortiGate-VM64-KVM #
```

Figure 11: configuration du port4 pour l'acces WAN

Ports 2 et 3 COMME INTERFACE REDONDANTE : HA) :

Pour assurer la redondance et la communication entre les deux pare-feux FTG-P (primaire) et FTG-B (backup), les ports 2 et 3 ont été configurés en tant qu'interfaces redondantes (Heartbeat) pour la synchronisation dans le cadre de la Haute Disponibilité (HA)

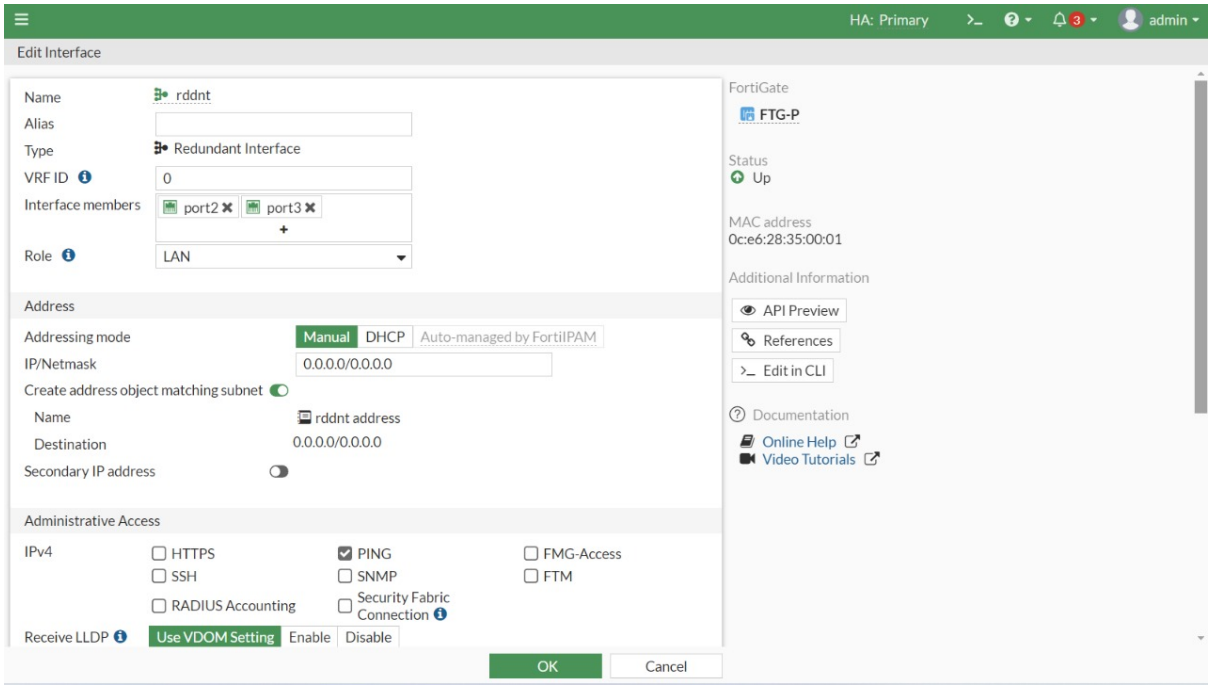

Figure 12: configuration du port2 et port3 en redondante

Création des VLANs :

VLAN IT :

- ID VLAN : 10.
- Adresse IP : 192.168.1.1/24.

- Role :LAN

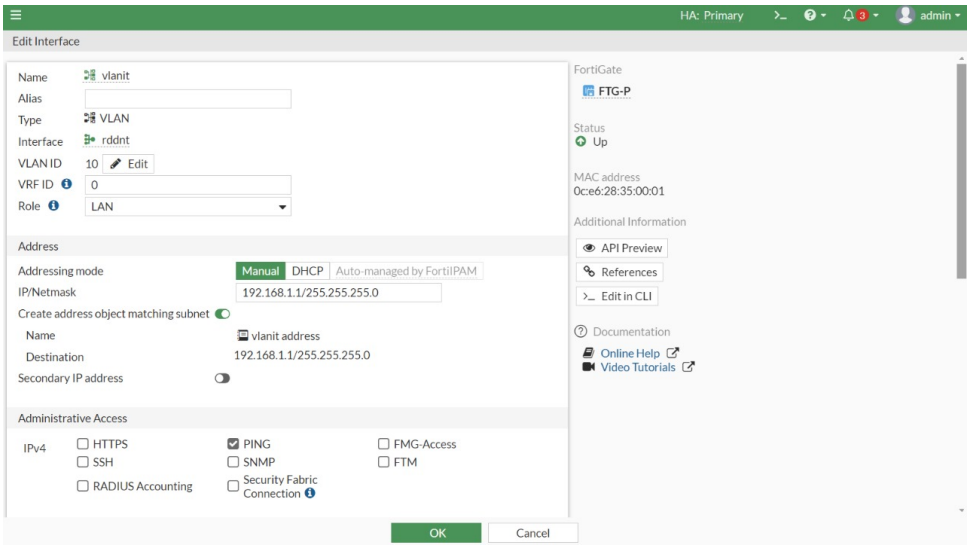

Figure 13: configuration du VLAN IT

VLAN RH :

- ID VLAN : 20.
- Adresse IP : 192.168.2.1/24.
- Role :LAN

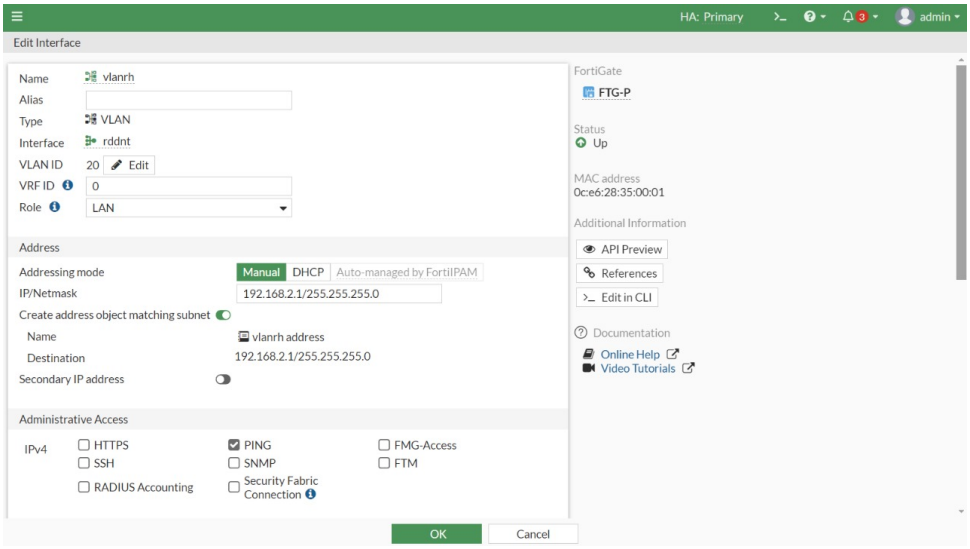

Figure 14: configuration du VLAN RH

Politique de sécurité :VLAN IT - WAN :

Règle autorisant le trafic sortant du VLAN IT vers le WAN.

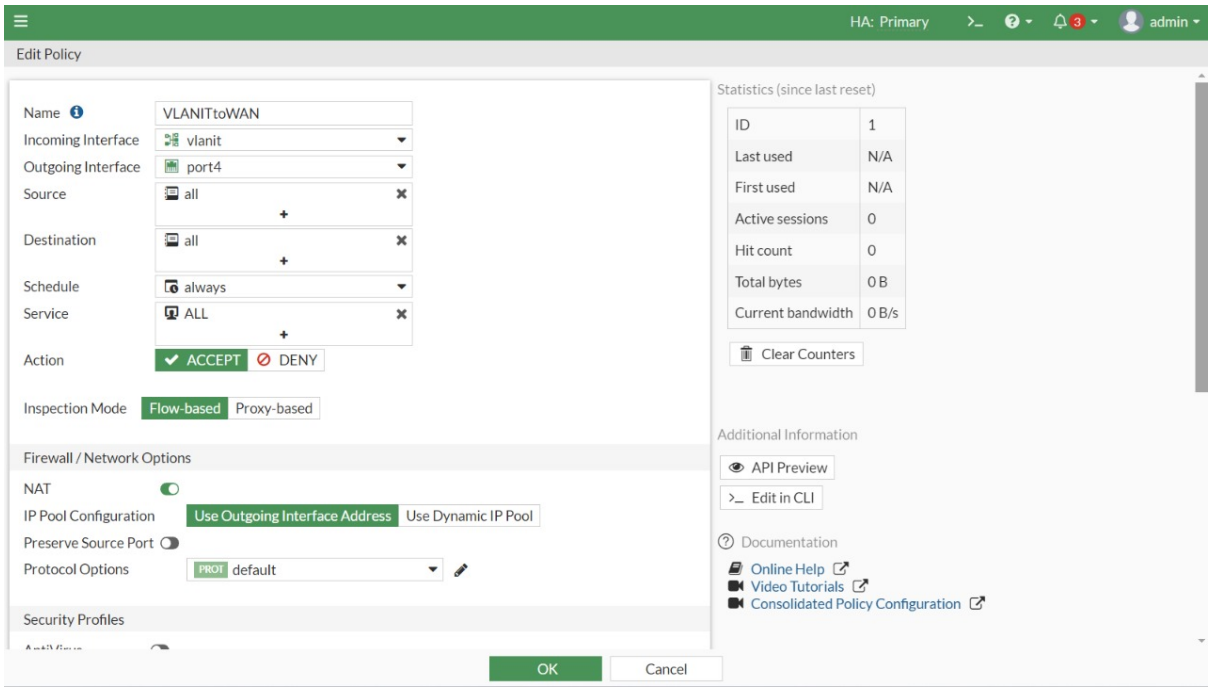

Figure 15: Politique de sécurité :VLAN IT - WAN

Politique de sécurité :VLAN RH - WAN :

Règle autorisant le trafic sortant du VLAN RH vers le WAN.

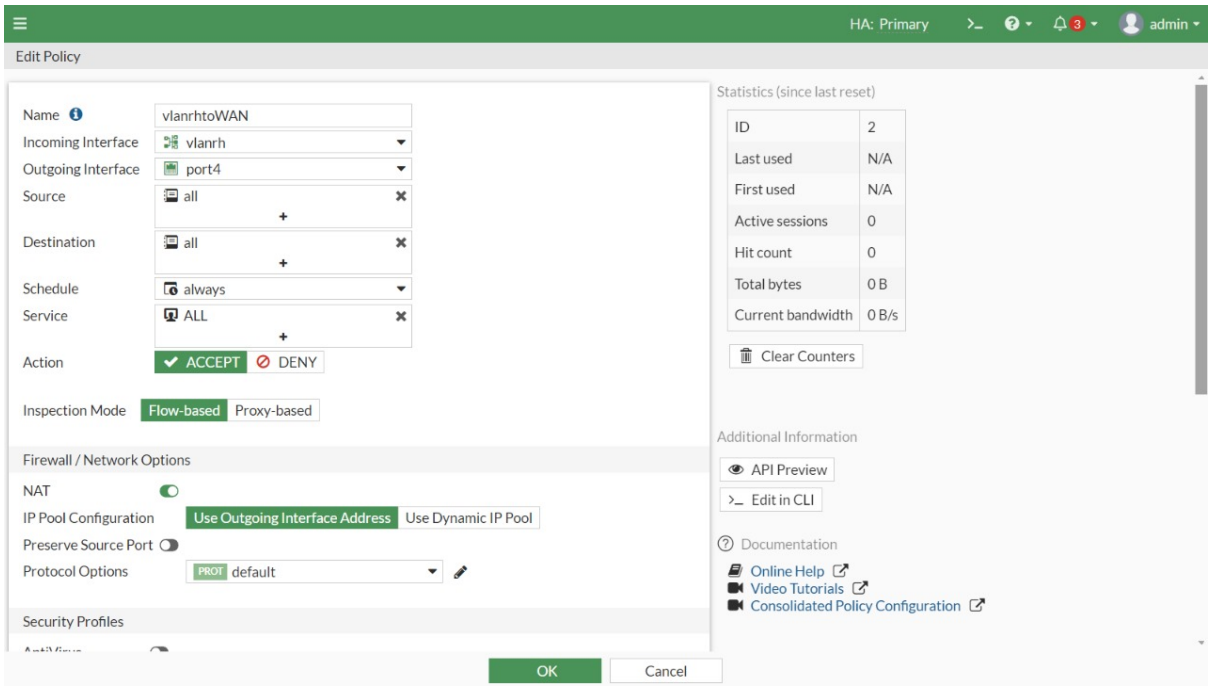

Figure 16: Politique de sécurité :VLAN RH - WAN

4.4 Configuration de FTG-B:

4.4.1 Configuration des interfaces :

Port 1 (Management - MGMT) :

- Le port 1 a été configuré pour la gestion en mode DHCP, permettant l'obtention automatique d'une adresse IP auprès d'un serveur DHCP.
- Mode : DHCP Client.
- Accès autorisé via HTTPS et SSH pour l'administration à distance

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port1
FortiGate-VM64-KVM (port1) # set mode dhcp
FortiGate-VM64-KVM (port1) # set allowaccess http ping
FortiGate-VM64-KVM (port1) # end
FortiGate-VM64-KVM #
```

Figure 17: configuration du port1 pour l'acces MNGMT

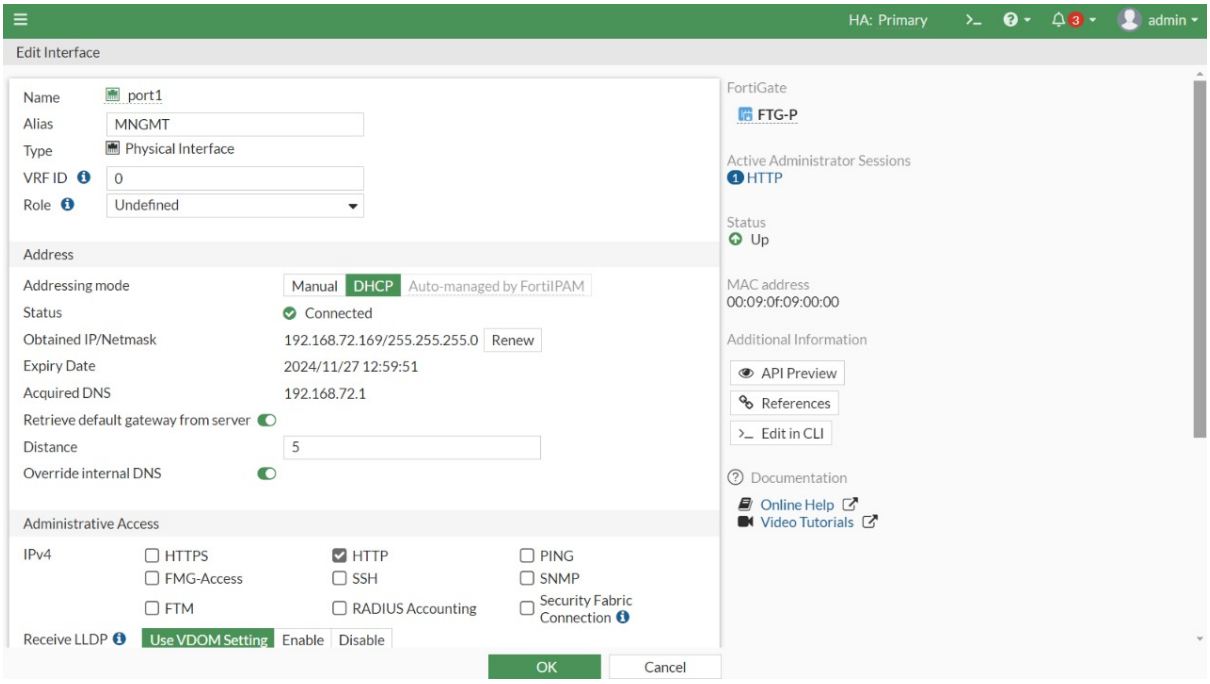

Figure 18: configuration du MNGMT2

Port 4 (Connexion au WAN via le switch lié au Cloud) :

Configuration du port 4 pour le trafic vers le WAN :

- Mode : DHCP Client.
- Permet la connectivité entre le réseau local et Internet via le switch.

```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port4

FortiGate-VM64-KVM (port4) # set mode dhcp

FortiGate-VM64-KVM (port4) # end

FortiGate-VM64-KVM #
```

Figure 19: configuration du port4 pour l'acces WAN

4.5 Configuration des switches :

4.5.1 POUR LE SWITCH SFED - P

- VLAN IT : Port trunk configuré pour transmettre le trafic VLAN 10.
- VLAN RH : Port trunk configuré pour transmettre le trafic VLAN 20.

```
IOU1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
10   VLAN0010                         active
20   VLAN0020                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
IOU1#
```

Figure 20: configuration des vlan sur SFED-P

```
IOU1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    trunk        auto   auto unknown
Et0/2                        connected    trunk        auto   auto unknown
Et0/3                        connected    trunk        auto   auto unknown
Et1/0                        connected    trunk        auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
IOU1#
```

Figure 21: configuration des interfaces sur SFED-P

```
IOU1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     aabb.cc00.0100
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     aabb.cc00.0100
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr Peer(STP)
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr Peer(STP)
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
 --More--
```

Figure 22: configuration du Spanning Tree Protocol (STP) sur SFED-P

4.5.2 POUR LE SWITCH SFED - B

- VLAN IT : Port trunk configuré pour transmettre le trafic VLAN 10.

- VLAN RH : Port trunk configuré pour transmettre le trafic VLAN 20.

```
IOU1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
10   VLAN0010                         active
20   VLAN0020                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
IOU1#
```

Figure 23: configuration des vlan sur SFED-B

```
IOU1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    trunk        auto   auto unknown
Et0/2                        connected    trunk        auto   auto unknown
Et0/3                        connected    trunk        auto   auto unknown
Et1/0                        connected    trunk        auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
IOU1#
```

Figure 24: configuration des interfaces sur SFED-B

```
SFED-B#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     aabb.cc00.0100
             Cost        100
             Port        3 (Ethernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     aabb.cc00.0200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr Peer(STP)
Et0/2               Root FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr Peer(STP)
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
 --More--
```

Figure 25: configuration du Spanning Tree Protocol (STP) sur SFED-B

4.5.3 CONFIGURATION DU SWITCH S1 :

Switch S1 : Connecté au FTG-P et FTG-B, configuré pour supporter le VLAN IT et assurer une connexion stable au réseau interne.

- VLAN IT : Port trunk configuré pour transmettre le trafic VLAN 10.

```
S1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    trunk        auto   auto unknown
Et0/2                        connected    10           auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
S1#
```

Figure 26: configuration de vlan it sur S1

4.5.4 CONFIGURATION DU SWITCH S2 :

Switch S2 : Connecté au FTG-P et FTG-B, configuré pour supporter le VLAN RH et assurer une connexion stable au réseau interne.

- VLAN IT : Port trunk configuré pour transmettre le trafic VLAN 10.

```
S2#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    trunk        auto   auto unknown
Et0/2                        connected    20           auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
S2#
```

Figure 27: configuration de vlan rh sur S2

4.5.5 CONFIGURATION DU SWITCH VERS CLOUD :

Pour permettre la connectivité entre les VLAN internes (IT et RH) et le WAN (Internet/Cloud), le switch est configuré pour se connecter au pare-feu FTG-P via le port WAN (port 4) et FTG-B. Cette configuration garantit la transmission fluide du trafic depuis les VLAN internes vers le Cloud.

```
IOU5#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    1            auto   auto unknown
Et0/1                        connected    trunk        auto   auto unknown
Et0/2                        connected    trunk        auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
Et1/0                        connected    1            auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    1            auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    1            auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
IOU5#
```

Figure 28: configuration de switch vers le cloud

4.6 Configuration de la Haute Disponibilité (H.A):

4.6.1 CONFIGURATION FTG-P :

Pour configurer la haute disponibilité sur le FTG-P :

1. On accède à l'onglet System ¿ HA dans l'interface de gestion.
2. On active le mode Actif-Passif.
3. On configure les paramètres suivants :

- Priorité : 150 pour définir le FTG-P comme pare-feu principal.
- Interfaces Heartbeat : on sélectionne les ports 5 et 6 pour assurer la communication Heartbeat entre les deux pare-feux.
- Enfin, on valide les configurations pour activer la redondance.

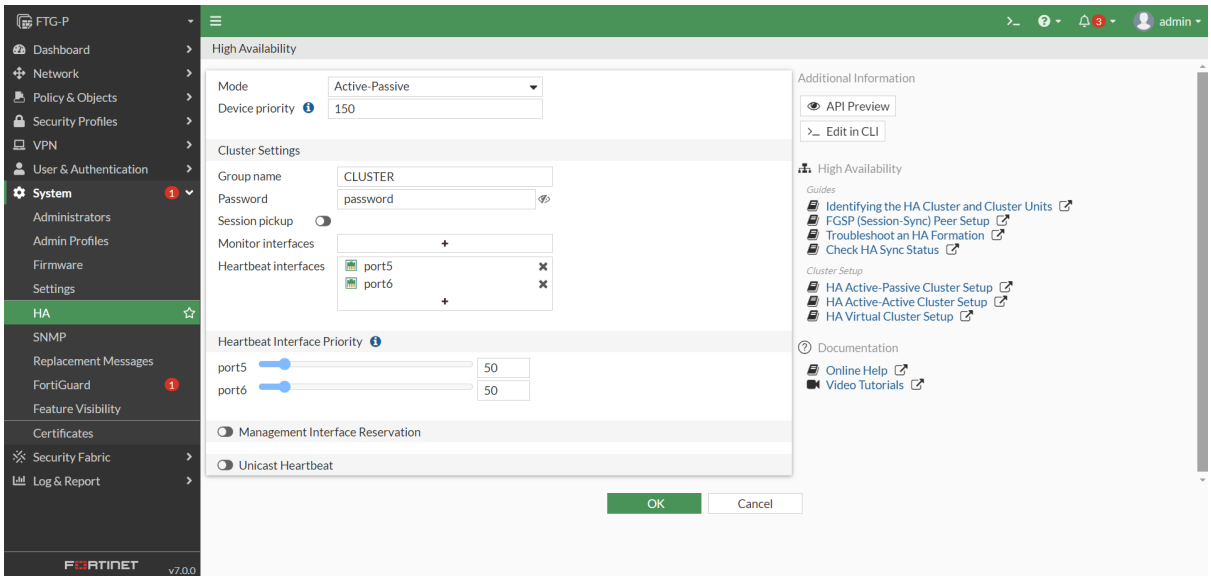

Figure 29: configuration de HA sur FTG-P

Le port de gestion (port 1) a peut-être modifié l'adresse IP, vérifiez donc les points suivants :

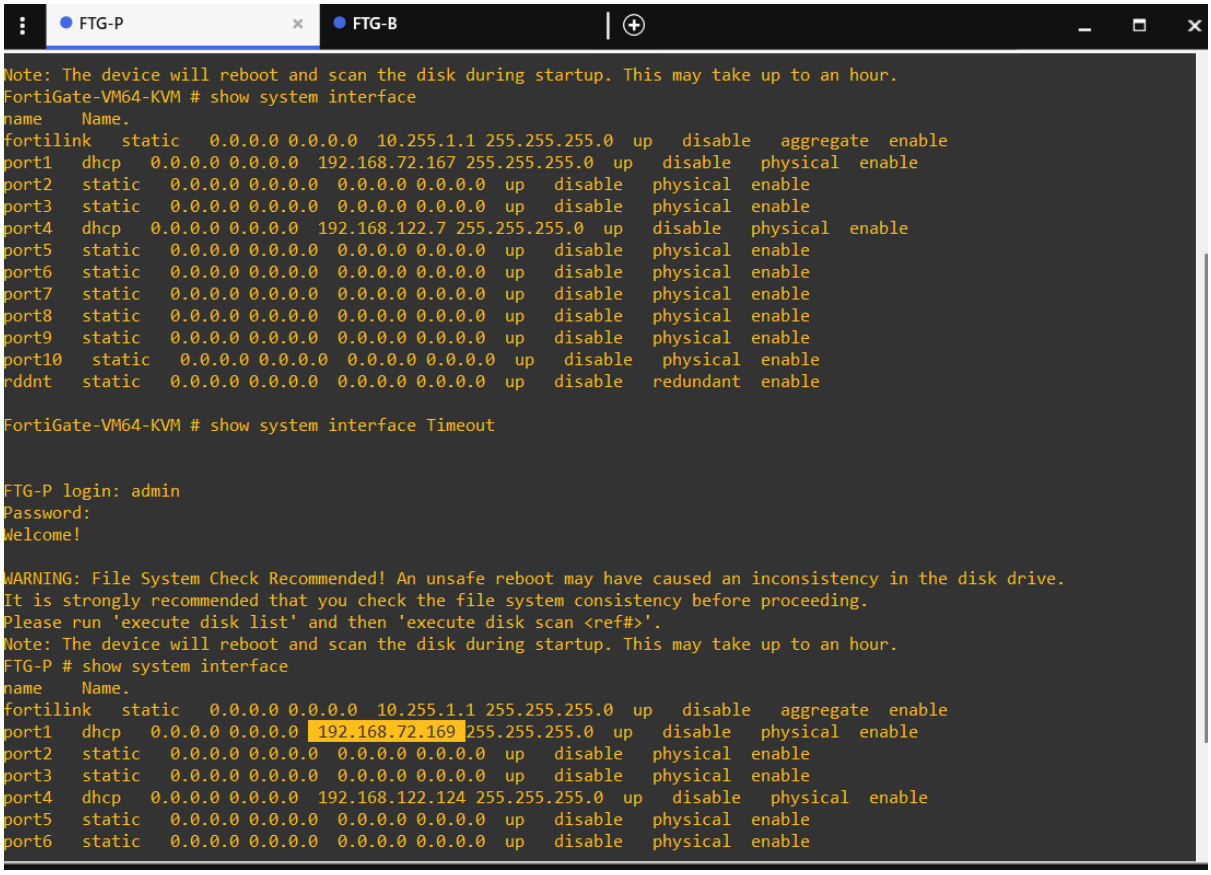

Figure 30: la modification auto de port1 apres configuration de HA

4.6.2 CONFIGURATION FTG-B :

Nous pouvons accéder au système FTG-B et modifier les paramètres de haute disponibilité (HA) comme suit.

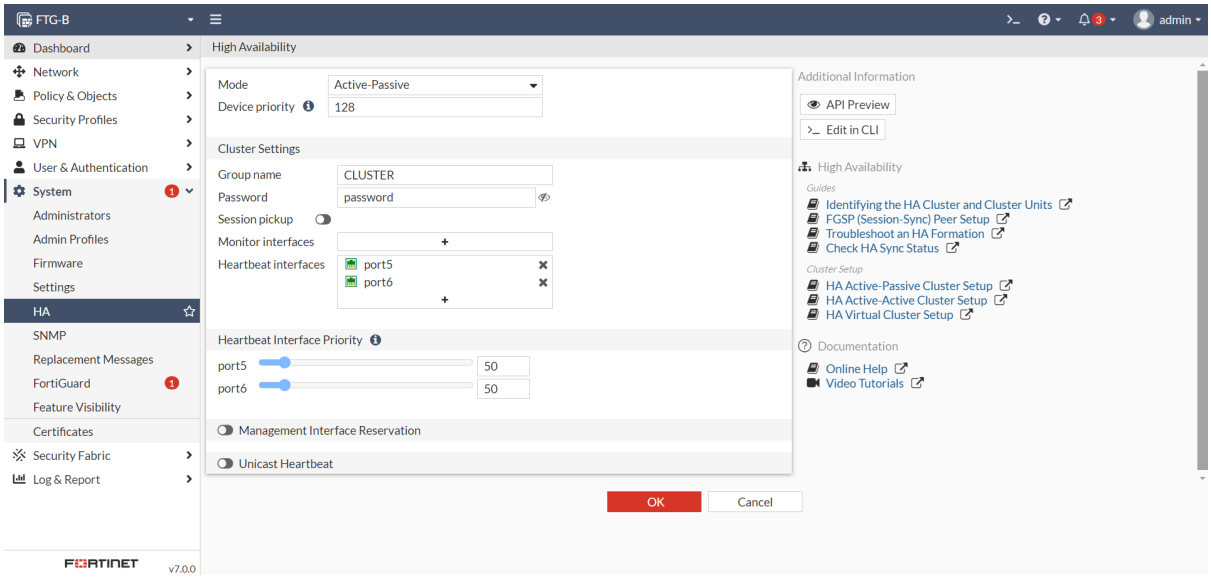

Figure 31: configuration de HA sur FTG-B

4.6.3 Validation de la configuration HA :

On Vérifie que les ports sont correctement reconnus comme Heartbeat Interfaces via la commande :

```
FTG-B # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:16:9
Cluster state change time: 2024-11-26 14:19:04
Primary selected using:
    <2024/11/26 14:19:04> FGVMEVUTBNAIAC35 is selected as the primary because its override priority is larger than peer m
ember FGVMEVLRKYDMDR83.
ses_pickup: disable
override: disable
Configuration Status:
    FGVMEVLRKYDMDR83(updated 0 seconds ago): out-of-sync
    FGVMEVUTBNAIAC35(updated 1 seconds ago): in-sync
System Usage stats:
    FGVMEVLRKYDMDR83(updated 0 seconds ago):
        sessions=4, average-cpu-user/nice/system/idle=0%/0%/2%/31%, memory=35%
    FGVMEVUTBNAIAC35(updated 1 seconds ago):
        sessions=19, average-cpu-user/nice/system/idle=9%/0%/5%/2%, memory=36%
HBDEV stats:
    FGVMEVLRKYDMDR83(updated 0 seconds ago):
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=2311173/5163/0/0, tx=188686/617/0/0
        port6: physical/1000auto, up, rx-bytes/packets/dropped/errors=2191651/4856/0/0, tx=145094/327/0/0
    FGVMEVUTBNAIAC35(updated 1 seconds ago):
        port5: physical/1000auto, up, rx-bytes/packets/dropped/errors=186497/611/0/0, tx=2308527/5157/0/0
        port6: physical/1000auto, up, rx-bytes/packets/dropped/errors=142779/321/0/0, tx=2189461/4852/0/0
Secondary   : FTG-B           , FGVMEVLRKYDMDR83, HA cluster index = 1
Primary     : FTG-P           , FGVMEVUTBNAIAC35, HA cluster index = 0
number of vcluster: 1
vcluster 1: standby 169.254.0.1
Secondary: FGVMEVLRKYDMDR83, HA operating index = 1
Primary: FGVMEVUTBNAIAC35, HA operating index = 0

FTG-B #
```

Figure 32: Validation de la configuration HA

Une fois la configuration de la haute disponibilité terminée, la synchronisation entre le FTG-P (principal) et le FTG-B (secondaire) peut nécessiter quelques secondes à quelques minutes pour se compléter. Pour vérifier si la synchronisation est correctement établie, on utilise la commande suivante dans le terminal : get system ha status

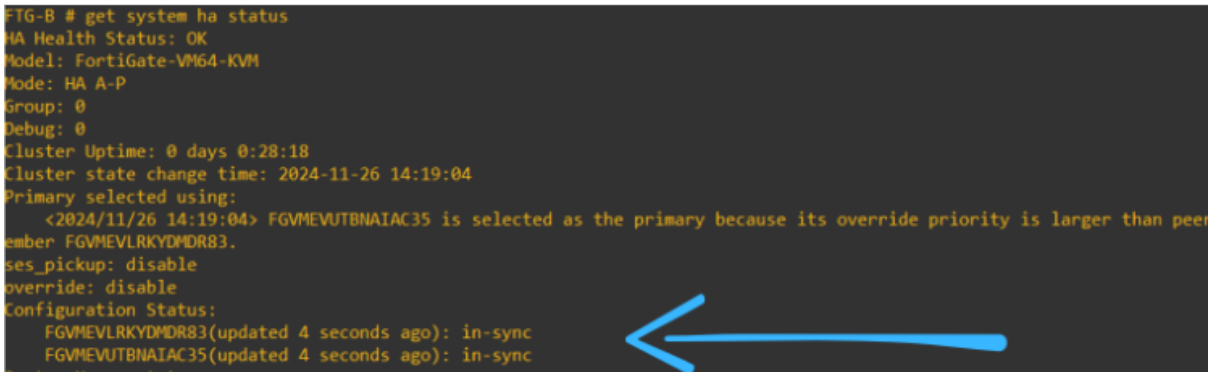

Figure 33: Vérification de synchronisation de FTG-P avec FTG-B

Une fois la commande get system ha status exécutée, on peut constater que les deux pare-feux, FTG-P (principal) et FTG-B (secondaire), sont désormais en synchronisation. Cela signifie que les configurations et les politiques de sécurité sont répliquées sur les deux dispositifs, assurant ainsi la haute disponibilité. L'état HA (High Availability) est désormais stable, ce qui permet au pare-feu secondaire de prendre automatiquement le relais en cas de défaillance du pare-feu principal, garantissant une continuité de service sans interruption. Désormais, les deux pare-feu sont synchronisés:

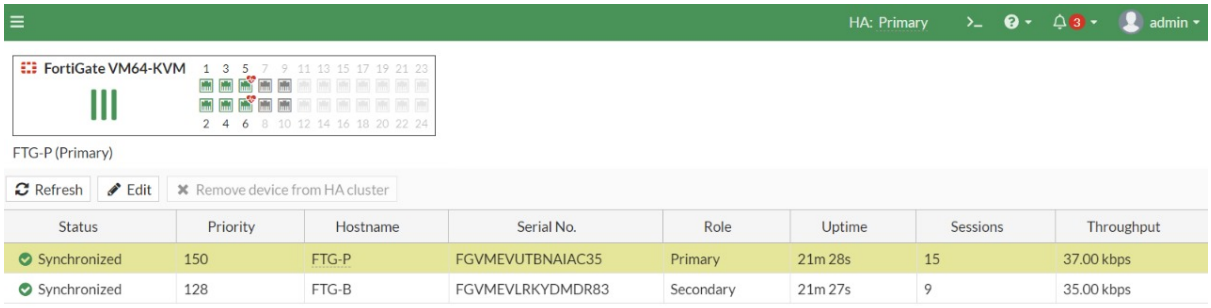

Figure 34: Vérification de synchronisation de FTG-P avec FTG-B dans GUI

4.7 conclusion

Au terme de ce chapitre consacré à la configuration de notre infrastructure, il est évident que la fiabilité et l'efficacité de notre projet reposent sur des choix de paramètres soigneusement élaborés. La configuration précise des pare-feu, des routeurs, des switches et l'intégration des solutions de haute disponibilité (HA), ainsi que l'optimisation des interfaces réseau, ont constitué les éléments clés de notre mise en place. Chaque configuration, chaque paramètre ajusté a été choisi avec soin pour répondre aux exigences spécifiques de notre projet, qu'il s'agisse de renforcer la sécurité, d'assurer une performance optimale ou de garantir une interconnexion fluide entre les différents composants. Le processus de configuration que nous avons suivi, détaillé et rigoureux, a permis de relever avec succès les défis techniques rencontrés tout au long du projet, tout en renforçant la stabilité et la résilience de notre infrastructure. À travers cette étape, nous avons démontré notre capacité à concevoir un environnement performant, sécurisé et flexible, essentiel pour garantir le bon fonctionnement et la pérennité de notre projet à long terme.

5 *Conclusion générale*

Ce projet de conception et de mise en œuvre d'une architecture réseau à haute disponibilité (HA) avec FortiGate vise à répondre aux défis croissants auxquels les entreprises font face en matière de sécurité, de continuité de service et de résilience. À travers une approche systématique, nous avons défini les besoins fonctionnels et non fonctionnels nécessaires pour concevoir une solution adaptée aux exigences spécifiques de l'organisation.

Les éléments clés de cette architecture incluent la redondance des composants réseau, l'intégration de politiques de sécurité avancées, et la gestion de la haute disponibilité via des mécanismes tels que le basculement automatique (failover) et la réplication des configurations. La mise en œuvre de cette solution permet non seulement de protéger les infrastructures contre les menaces externes, mais aussi de garantir un fonctionnement stable même en cas de défaillances matérielles ou logicielles.

L'implémentation dans un environnement simulé, à l'aide d'outils comme GNS3, a permis de tester les performances, d'évaluer la résilience du système et d'identifier des axes d'amélioration. Grâce à une approche structurée et une sélection minutieuse des technologies (FortiGate), nous avons pu proposer une solution non seulement sécurisée, mais aussi évolutive et capable de s'adapter aux besoins futurs de l'entreprise.

En conclusion, ce projet offre une solution viable pour les entreprises cherchant à renforcer leur infrastructure réseau, tout en maintenant une sécurité optimale et une disponibilité maximale. La prochaine étape consistera à approfondir l'évaluation de cette solution dans un environnement réel et à proposer des recommandations pour son déploiement à grande échelle.

6 *Perspectives*

La réalisation de ce projet de mise en œuvre d'une architecture réseau à haute disponibilité avec FortiGate marque une étape importante dans l'étude et l'application des technologies modernes de cybersécurité. Cependant, pour maximiser les bénéfices de cette solution et répondre aux évolutions rapides du domaine, plusieurs axes de développement peuvent être envisagés à l'avenir.

1. Déploiement dans un environnement réel

Une prochaine étape essentielle consisterait à tester et à déployer cette architecture dans un environnement opérationnel réel. Cela permettrait de valider les performances et la fiabilité de la solution en conditions réelles, tout en évaluant sa capacité à répondre aux besoins spécifiques des utilisateurs finaux.

2. Intégration de technologies avancées

Pour renforcer encore davantage la sécurité et la performance, il serait intéressant d'intégrer des technologies avancées, telles que :

L'intelligence artificielle (IA) pour détecter et réagir aux menaces en temps réel.

Les solutions SD-WAN (Software-Defined Wide Area Network) de FortiGate pour une gestion optimisée des connexions réseau et des performances améliorées pour les entreprises multi-sites.

3. Automatisation et gestion centralisée

L'automatisation des tâches administratives et la gestion centralisée à travers des outils comme FortiManager pourraient permettre d'optimiser l'efficacité des administrateurs système. Cela inclurait l'automatisation des mises à jour de sécurité, des sauvegardes et des politiques de gestion des incidents.

4. Renforcement de la résilience face aux menaces avancées

Avec l'émergence de cybermenaces toujours plus complexes (APT, ransomwares, etc.), il serait pertinent d'explorer des solutions complémentaires comme l'intégration avec des systèmes de détection et de réponse aux menaces (EDR/XDR) pour une défense proactive.

5. Formation continue et sensibilisation

Une autre perspective clé est d'accompagner le déploiement de cette solution par des initiatives de formation continue pour les administrateurs système et de sensibilisation pour les utilisateurs finaux. Cela permettra de réduire les erreurs humaines et d'optimiser

l'efficacité des mesures de sécurité mises en place.

7 Références

Voici des liens provenant de la documentation officielle Fortinet pour comprendre et configurer la haute disponibilité (High Availability - HA) sur les pare-feux FortiGate :

- https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/459750/high-availability
- https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/513053/high-availability-with-two-fortiga
- https://docs.fortinet.com
- https://www.cisco.com/c/en/us/support/switching/spanning-tree-protocol-stp/tsd-products-support-seri html