Sup'Technology
ECOLE SUPÉRIEURE

المملكة المغربية
وزارة التعليم العالي والبحث العلمي
وتكوين الأطر

Royaume du Maroc
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique
et de la Formation des Cadres

RAPPORT
PROJET FIN D'ANNEE

Developpement d'une infrastructure du FAI et de Data center avec migration vers IPv6

Realisation

Ayoub EL BOUZI

Encadrement

Asmae Kassid

Table des matières

Abstract

Au centre de l'évolution constante de l'infrastructure informatique, il est essentiel de garantir la stabilité et la performance des réseaux en se concentrant sur la sécurité et la préparation à l'avenir. Notre projet d'envergure aborde cette complexité en mettant l'accent sur deux axes principaux : renforcer la sécurité d'un réseau qui utilise différentes technologies et protocoles, tout en se préparant stratégiquement à passer inévitablement à IPv6.

Ce système englobe une pléthore de technologies et d'accessoires de la gamme de routeurs Cisco aux sistemas de sécurité Fortigate, en passant par les commutateurs ATM, quelques appareils DSLAM, des appareils SDN, un IDS, un IPS, quelques infrastructures d'adressage IP, et beaucoup d'autres choses. Il se spécialise également dans la gestion de réseau interne au public, avec un accent principal sur la migration d'IPv4 vers IPv6 au sein du système interne.

Nos applications répondent à des défis d'échelle, allant de la sécurité multicouche à l'intégration harmonisée des technologies, en passant par le routage de protocoles complexes tels que EIGRP, OSPF, RIP, BGP, IBGP, eBGP, et bien d'autres. L'importance de cette infrastructure réside dans sa capacité à améliorer la productivité, à protéger l'utilisation légitime des données et à se conformer aux futurs standards d'Internet.

Dans ce contexte, les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) jouent un rôle important. Cela garantit une surveillance constante du réseau, détectant moins d'activités malveillantes et réagissant immédiatement pour prévenir toute intrusion. Les systèmes Ses sont des gardes vigilants qui renforcent la sécurité et la fiabilité des zones d'infrastructure.

Les résultats de ces travaux vont au-delà de la simple titrisation des réseaux. Ils incluent également une plus grande efficacité d’adaptation, d’élasticité, et de préparation aux mutations. Cette affiche illustre les défis rencontrés, la philosophie des solutions qui s'applique et les principaux avantages qui en découlent.

Dans les sections qui suivent de ce rapport, nous décrivons en détail la méthodologie, les considérations relatives à la topologie du réseau, les travaux, les expériences et l'analyse des résultats. En conclusion, nous mettons en lumière l’importance indéniable de nos travaux, tant en termes de sécurité des réseaux que de transition inévitable vers IPv6 dans les réseaux internes.

Introduction

À l'heure de la connectivité omniprésente et de la digitalisation croissante des activités, la communication électronique joue un rôle important dans le fonctionnement des entreprises et des organisations. Cependant, cette omniprésence et cette interdépendance augmentent également l'exposition de ces réseaux à un éventail toujours croissant de menaces et de vulnérabilités. Dans ce contexte, la sécurité de l'infrastructure réseau devient une priorité, tout en préparant l'avenir d'Internet, la transition vers IPv6 devenant une stratégie importante.

Notre projet se positionne face à des défis souhaitables, embrassant la complexité inhérente de la gestation en utilisant plusieurs technologies, protocoles et différents matériaux. Nous nous efforçons d'atteindre deux objectifs majeurs : renforcer la sécurité de notre infrastructure réseau et préparer notre transition vers IPv6.

La palette de technologies et de composants impliqués dans notre projet est vaste, allant des routeurs Cisco aux routeurs Juniper, en passant par les systèmes de sécurité Fortigate, les commutateurs ATM, les appareils DSLM, la technologie SDN, IDS, IPS, etc. et bien d'autres encore. Notre portefeuille de services réseau s'étend également des réseaux internes aux réseaux public, avec le concept important de migration d'IPv4 vers IPv6 de nos infrastructures.

Le défi auquel nous sommes confrontés est multiforme, depuis la sécurité multicouche jusqu'à l'intégration unifiée des géants de la technologie, tous contrôlant des protocoles de routage avancés tels que EIGRP, OSPF, RIP, BGP, IBGP, eBGP et autres duplications. Au cœur de notre stratégie de sécurité se trouvent les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS), qui assurent une surveillance constante de nos réseaux et la protection des données sensibles.

Au sein de cet écosystème plus large, nous déployons également des serveurs cloud qui répondent aux besoins des plongeurs, tandis que le service Active Directory (AD) fournit des identités et des ressources pour la localisation. Le serveur de stockage, associé à notre base de don SQL, est le cœur de nos opérations de données, garantissant une disponibilité dans leur intégrité. De plus, le serveur DHCP public joue un rôle important dans l'attribution des adresses IP publiques.

De plus, notre infrastructure comprend des solutions Citrix pour la virtualisation des applications et des postes de travail, les technologies SDN mettent la gestion et l'optimisation dynamique du réseau, les téléphones VoIP assurent les communications unifiées, et les zones DMZ qui assurent la communication des systèmes classifiés, renforçant ainsi notre sécurité.

Dans les prochaines sections de ce rapport, nous passerons en revue la méthodologie, le concept de notre topologie de réseau, la mise en œuvre, les tests et l'analyse des résultats. Dans le cadre de cet examen, nous nous concentrerons sur les questions pour lesquelles notre travail vise à assurer la continuité des activités et la protection des données sensibles, tout en préparant nos réseaux internes à l'inévitable prochaine phase d'Internet, la migration vers IPv6. Ce rapport documente notre parcours au cour de la complexité, avec pour objectif ultime d'assurer la robustesse, la sécurité ne la pérennité de notre réseau industriel.

Ressources

Nous avons soigneusement sélectionné et déployé, dans le cadre des ressources nécessaires, une gamme complète des technologies pour concevoir un réseau sécurisé et résilient. L'accent principal de notre projet est la sécurité, mais nous tenons compte de la migration vers IPv6 dans notre planification.

Voici une liste détaillée de nos ressources clés :

- **Composants Réseau** :

- Routeurs Cisco 7200 :

Caractéristiques :

- ✓ Performances élevées pour gérer un trafic réseau intensif.
- ✓ Support avancé des protocoles de routage tels que OSPF, BGP, EIGRP, etc.
- ✓ Modularité permettant d'ajouter des interfaces et des modules personnalisés.
- ✓ Capacités de sécurité avancées, y compris le filtrage de paquets et les VPN.

- Routeurs Juniper

Caractéristiques

- ✓ Architecture orientée service offrant une flexibilité élevée pour la personnalisation des services.
- ✓ Système d'exploitation Junos reconnu pour sa stabilité et sa sécurité.
- ✓ Prise en charge des protocoles de routage tels que OSPF, BGP, IS-IS.
- ✓ Intégration de fonctions de sécurité avancées telles que le pare-feu intégré et la détection d'intrusion.

Les routeurs Cisco et Juniper sont deux choix populaires pour les réseaux d'entreprise en raison de leurs performances, de leur fiabilité et de leurs fonctionnalités avancées. Chacun offre des avantages spécifiques en fonction des besoins et des exigences de sécurité de votre réseau.

- Commutateurs Cisco :

Switchs Access : Utilisés pour segmenter le réseau en fonction des niveaux de sécurité et contrôler l'accès aux ressources sensibles.

Switchs Distribution : Assurent une gestion optimale du trafic au sein du réseau, garantissant des performances élevées et une résilience.

Switchs Core : Constituent la colonne vertébrale de notre réseau, garantissant la disponibilité et la latence minimale.

MikroTik : Ces dispositifs contribuent à la gestion fine de la connectivité et renforcer la sécurité au niveau du réseau.

Cisco ATM Switch : Gère la connectivité haut débit en utilisant le protocole ATM.

Modems ADSL et DSLAM : Assurent la connectivité Internet haut débit.

- **Serveurs et Services** :

NAS Storage Oracle : Stocke et sécurise les données sensibles de manière centralisée

Contrôleurs de Domaine Windows Server : Gèrent l'authentification, l'autorisation et la gestion des utilisateurs, renforçant ainsi la sécurité du réseau.

VirtualBox et VMware ESXi : Utilisés pour créer des environnements de test sécurisés et pour isoler les machines virtuelles.

Citrix : Facilite la virtualisation d'applications et de postes de travail en garantissant l'accès sécurisé aux ressources.

SDN (Software-Defined Networking) : Permet une gestion dynamique et sécurisée du réseau.

Disaster Recovery (DR) : Les mécanismes de récupération garantissent la continuité des opérations en cas de sinistre.

Microsoft SQL Server : La base de données SQL sécurisée stocke et gère nos données sensibles.

SCCM (System Center Configuration Manager) : Permet une gestion sécurisée des configurations et des déploiements logiciels.

Zones DMZ : Segmentent le réseau pour renforcer la sécurité et protéger les ressources internes.

Serveur Exchange : Assure la gestion sécurisée des communications électroniques.

Serveur DNS Public : Rend accessible notre réseau tout en maintenant la sécurité des noms de domaine publics.

Serveur Web : Héberge nos sites et services publics, garantissant leur sécurité.

- **Sécurité et Surveillance :**

Firewalls FortiNet : Jouent un rôle crucial en filtrant le trafic, en appliquant des règles de sécurité et en fournissant une protection multicouche contre les menaces.

Systèmes de Détection d'Intrusion (IDS) : Surveillent le réseau en temps réel pour détecter toute activité suspecte ou malveillante.

Systèmes de Prévention d'Intrusion (IPS) : Réagissent instantanément pour prévenir toute intrusion ou activité malicieuse.

- **Machines et Systèmes d'Exploitation** :

Téléphone IP: La VoIP est sécurisée pour les communications vocales au sein du réseau.

Machines Windows 8.1 : Ces systèmes d'exploitation sécurisés sont déployés pour répondre à divers besoins informatiques.

Chaque ressource mentionnée ci-dessus joue un rôle essentiel dans la création d'un réseau sécurisé et performant. Tout au long de ce rapport, nous détaillerons comment ces ressources sont utilisées pour renforcer la sécurité de notre infrastructure réseau.

Contexte

La construction d’une infrastructure d’entreprise complexe est importante à l’infrastructure informatique ce qui nécessite une planification minutieuse n’une mise en œuvre méticuleuse. Cette activité s'adapte à cet environnement exigeant, visant à développer une infrastructure informatique robuste et efficace pour répondre aux besoins d'une grande organisation.

L'objectif central de notre système est de garantir la continuité des opérations, la sécurité des données et la transparence de la connectivité de l'entreprise sur plusieurs éléments clés :

Main Data Center : Cœur des opérations, ce ventre de Data abrite les systèmes cruciaux, peu de métiers d'applications, moins de bases de construction essentielles et peu de systèmes de ressources. La disponibilité du centre de données interrompu de s’est impérative pour maintenir l’efficacité des opérations.

Standby Data Center : Conçu comme une mesure de sauvegarde, ce centre de données garantit la perte des services critiques. En cas d'incident majeur ou de panne du data center principal, le data center de secours prend le relais pour assurer la continuité du fonctionnement

Infrastructure du FAI (Internet Access Provider) : Une communication fiable et sécurisée est essentielle pour le personnel mis en place et le personnel utilisateur. L'infrastructure du FAI fournit la passerelle vers internet et promet la communication des emplois internes et externes.

Pour atteindre cet objectif, ce projet combine une variété de technologies, de systèmes et de ressources, chacun jouant un rôle clé dans la réalisation de notre vision. Depuis la sélection des routeurs Cisco et Juniper pour gérer le trafic réseau jusqu'au déploiement de mesures de sécurité avancées telles que les pare-feu FortiGate et les systèmes de détection d'intrusion (IDS), notre système est conçu pour être à la fois résilient et sécurisé.

Nous intégrons également des solutions de virtualisation, telles que VirtualBox et VMware ESXi, appliquons un optimiseur à la gestion des ressources informatiques et utilisons la technologie SDN pour mettre en œuvre une gestion dynamique du réseau. Les serveurs NAS Oracle et Base fournissent des données SQL garantissant la disponibilité et l'intégrité des données cruciales.

La transition vers IPv6 est également une composante de notre travail, nous permettant de préparer les réseaux internes au futur de l'Internet.

Nous approfondirons ensuite la méthodologie, les hypothèses de topologie, la mise en œuvre, les tests et l'évaluation de l'aba. Notre objectif ultime est de construire des systèmes informatiques qui répondent non seulement aux besoins actuels, mais qui sont également prêts à relever les défis futurs, qu'il s'agisse d'améliorations commerciales ou de percées technologiques.

Méthodologie

La méthodologie sous-tendant la mise en œuvre de notre infrastructure informatique complexe et sécurisée repose sur une série d'étapes bien définies, de la planification initiale à la réalisation et à l'évaluation continue. Cette méthodologie assure une gestion efficace du projet, garantissant que chaque composant est soigneusement intégré pour répondre à nos objectifs de sécurité et de performance.

1. Planification Initiale

La planification initiale a été une étape fondamentale de notre méthodologie. Elle a impliqué l'identification des besoins et des exigences spécifiques de notre organisation, y compris les besoins en matière de sécurité, de connectivité et de redondance. Nous avons également tenu compte de l'expansion future et des besoins en évolutivité.

2. Conception de la Topologie Réseau

La conception de la topologie réseau est le fondement de notre infrastructure. Elle a nécessité une analyse minutieuse de la manière dont les différents composants interagiront. Nous avons déterminé l'emplacement stratégique des routeurs Cisco et Juniper, des commutateurs Cisco, des serveurs NAS Oracle, et d'autres équipements pour garantir une connectivité optimale et une résilience face aux pannes.

3. Sélection des Technologies et des Composants

La sélection des technologies et des composants a été réalisée en tenant compte de la sécurité en tant que priorité principale. Nous avons choisi des solutions telles que les routeurs Cisco pour leur robustesse et leurs capacités de sécurité avancées. Les pare-feu FortiGate ont été déployés pour filtrer le trafic entrant et sortant. Les IDS et IPS surveillent activement le réseau pour détecter les menaces.

4. Migration vers IPv6

La migration vers IPv6 a été planifiée dans le cadre de notre méthodologie pour garantir la compatibilité future de notre réseau. Cela implique la mise à jour de nos routeurs, de nos serveurs DNS, et de nos autres composants pour prendre en charge IPv6.

5. Implémentation

L'implémentation a été une phase cruciale de notre projet. Nous avons configuré et déployé chaque composant selon les spécifications de notre plan de conception. Les routeurs, les commutateurs, les pare-feu, les serveurs NAS, les serveurs DNS, et d'autres éléments ont été intégrés dans notre infrastructure.

6. Tests et Validation

Des tests rigoureux ont été effectués à chaque étape de l'implémentation. Nous avons vérifié la connectivité, la sécurité, la performance et la résilience. Des tests d'intrusion ont été menés pour évaluer la robustesse de nos mécanismes de sécurité.

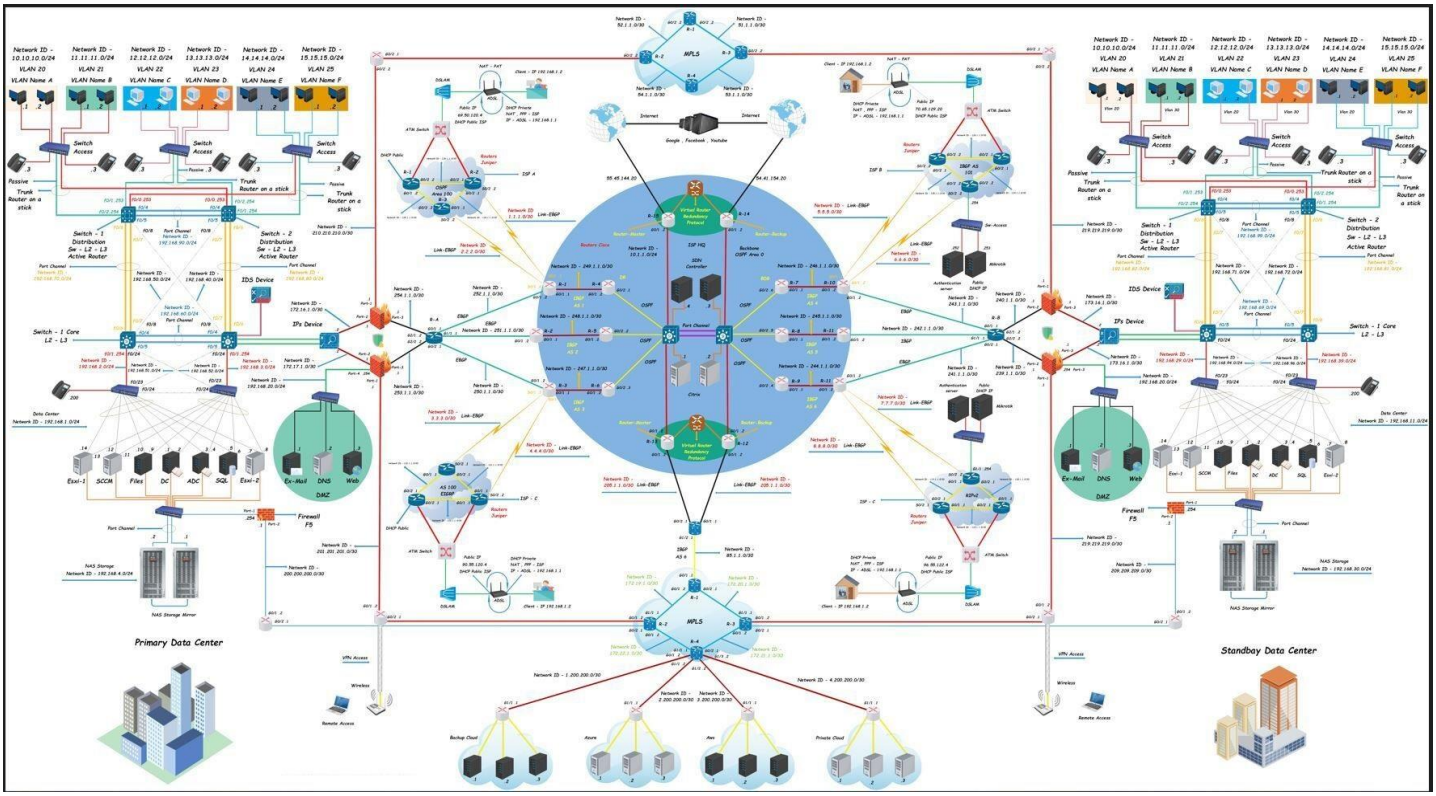
7. Surveillance Continue et Maintenance

Une fois l'infrastructure en place, la surveillance continue et la maintenance proactive sont essentielles pour garantir un fonctionnement fluide. Nous utilisons des outils de surveillance pour détecter les problèmes potentiels et des procédures de maintenance planifiées pour garantir la fiabilité à long terme.

Cette méthodologie globale est conçue pour garantir que l’infrastructure informatique est alignée sur les besoins de l'entreprise, sécurisée contre les menaces potentielles, résiliente en cas de pannes, et prête à évoluer pour répondre aux futurs défis technologiques. Les prochaines sections de ce rapport détailleront les aspects spécifiques de notre méthodologie, y compris la topologie réseau, la configuration des équipements, les tests et les résultats.

Topologies de réseaux

Dans cette section, on explorera la topologie du réseau, en mettant en évidence les différents équipements, les connexions et les configurations clés qui ont été déployés pour soutenir notre infrastructure informatique avancée. Ce réseau est conçu pour répondre aux besoins d'une grande entreprise et se compose de plusieurs composants et technologies essentiels, visant à établir une connectivité fiable et sécurisée entre le data center principal, le data center de secours et l'infrastructure du fournisseur d'accès Internet, tout en prenant en charge un large éventail de technologies et de services essentiels.



1. Routeurs Cisco 7200

Les routeurs Cisco 7200 jouent un rôle essentiel dans notre infrastructure en assurant le routage du trafic à l'échelle de l'entreprise. Ils sont configurés pour prendre en charge le protocole de routage BGP (Border Gateway Protocol) pour les connexions inter domaines.

- Configuration Générale :

Configuration BGP pour l'échange d'informations de routage avec d'autres AS (Systèmes Autonomes).

Définition des politiques de routage et des filtres de préfixes BGP.

Activation de la redondance pour garantir la haute disponibilité.

- Exemple

```
enable
configure terminal
!
interface GigabitEthernet0/0
 ip address 10.1.1.1
255.255.255.0
!
router bgp 65001
 neighbor 192.168.1.2 remote-as
65002
 network 10.0.0.0 mask
255.0.0.0
!
end
write memory
```

2. Routeurs Juniper

Les routeurs Juniper sont déployés pour établir des connexions VPN sécurisées avec nos succursales distantes.

- Configuration Générale :

Configuration d'un VPN IPSec pour assurer la confidentialité et l'authentification des données transitant par les connexions VPN.

Mise en place de politiques de sécurité pour contrôler le trafic VPN entrant et sortant.

Exemple de configuration Bash pour un routeur Juniper avec une configuration VPN

- Exemple

```
cli
configure
!
set interfaces ge-0/0/0 unit 0 family inet address 10.2.2.1/24
set security ike proposal ike-proposal1 authentication-method pre-shared-keys
set security ike proposal ike-proposal1 dh-group group2
set security ike proposal ike-proposal1 authentication-algorithm sha1
set security ike proposal ike-proposal1 encryption-algorithm aes-256-cbc
set security ike policy ike-policy1 mode aggressive
set security ike policy ike-policy1 proposals ike-proposal1
set security ike gateway ike-gateway1 ike-policy ike-policy1
set security ike gateway ike-gateway1 address 203.0.113.1
set security ike gateway ike-gateway1 external-interface ge-0/0/0
set security ike gateway ike-gateway1 pre-shared-key ascii-text "YourSecretKey"
set security ipsec proposal ipsec-proposal1 protocol esp
set security ipsec proposal ipsec-proposal1 authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-proposal1 encryption-algorithm aes-256-cbc
set security ipsec policy ipsec-policy1 proposals ipsec-proposal1
set security ipsec vpn vpn1 ike gateway ike-gateway1
set security ipsec vpn vpn1 ike ipsec-policy ipsec-policy1
set security ipsec vpn vpn1 establish-tunnels immediately
!
commit and-quit
```

3. **Commutateurs Cisco**

J’utilise des commutateurs Cisco à différents niveaux de ce réseau, notamment en tant que commutateurs d'accès, de distribution et de cœur.

- Configuration Générale (Commutateur d'Accès - Core) :

Configuration des ports d'accès pour les utilisateurs finaux.

Attribution de VLAN aux ports pour la segmentation du réseau.

Activation de la sécurité des ports pour prévenir les accès non autorisés

```
enable
configure terminal
!
vlan 20
 name A
!
vlan 21
 name B
!
vlan 22
 name C
!
vlan 23
 name D
!
vlan 24
 name E
!
vlan 22
 name F
!
interface range FastEthernet0/1 - 30
 switchport mode access
 switchport access vlan 20
!
interface Vlan 20
 ip address 10.10.10.1 255.255.255.0
!
interface range FastEthernet0/31 - 40
 switchport mode access
 switchport access vlan 21
!
interface Vlan 21
 ip address 11.11.11.1 255.255.255.0
!
interface range FastEthernet0/41 - 50
 switchport mode access
 switchport access vlan 22
!
interface Vlan30
 ip address 12.12.12.1 255.255.255.0
!
ip routing
!
end
write memory
```

4. Commutateurs Couche 3

Les commutateurs de couche 3 sont des éléments essentiels qui permettant le routage inter-VLAN et assurant une connectivité avancée.

- Configuration Générale :

Activation du routage sur les commutateurs de couche 3 pour permettre le transit des données entre les sous-réseaux VLAN.

Création de VLAN pour segmenter le réseau en fonction des départements et des besoins opérationnels.

Attribution des interfaces aux VLAN correspondants pour isoler le trafic et renforcer la sécurité.

Configuration des protocoles de routage dynamique tels qu'OSPF ou EIGRP pour gérer les routes entre les VLAN.

Mise en place de règles de pare-feu internes pour contrôler le trafic inter-VLAN et assurer la sécurité.

Utilisation de la qualité de service (QoS) pour prioriser le trafic en fonction des besoins des applications.

Activation du spanning tree protocol (STP) pour éviter les boucles réseau et garantir la disponibilité.

Configuration de l'agrégation de liens (port-channel) pour une bande passante accrue et une redondance

- Exemple :.

```
enable
configure terminal
!
interface range GigabitEthernet0/1 - 2
 channel-group 1 mode active
!
interface Port-channel1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
!
end
write memory
```

5. Les Firewalls

Les pare-feu FortiGate sont déployés pour sécuriser le réseau contre les menaces extérieures et intérieures.

- Configuration Générale :

Mise en place de règles de pare-feu strictes pour filtrer le trafic entrant et sortant.

Activation du système de prévention des intrusions (IPS) pour détecter et bloquer les tentatives d'intrusion.

Utilisation de la protection DDoS pour résister aux attaques de déni de service distribué

Configuration de la détection des attaques par force brute pour bloquer les tentatives répétées d'accès non autorisé.

Mise en place de VPN (Virtual Private Network) pour sécuriser les connexions entre les succursales distantes et notre réseau central.

Activation du Network Address Translation (NAT) pour la translation d'adresses IP, permettant ainsi la communication entre les réseaux internes et externes tout en masquant les adresses internes.

```
config system ddos
    set syn-flood enable
    set syn-cookie enable
    set icmp-flood enable
    set icmp6-flood enable
    set udp-flood enable
    set dns-servfail-threshold 50
    set dns-nxdomain-threshold 50
    set tcp-synthreshold 50
    set udp-floodthreshold 50
    set other-floodthreshold 50
    set max halfopen-sessions 400000
    set halfopen-sessions-age 5
    set halfopen-sessions-min 2000
    set syn-wait-time 30
end
config firewall address
    edit "Blocked_IPs"
        config entries
            edit 1
                set subnet 1.2.3.4 255.255.255.0
            next
        end
    next
end
config firewall addrgrp
    edit "Blocked_IP_Group"
        config member
            edit 1
                set name "Blocked_IPs"
            next
        end
    next
end
config firewall policy
    edit 1
        set name "Block_DDoS_Attacks"
        set srcintf "DMZ"  # Remplacez par votre
interface DMZ
        set dstintf "WAN"  # Remplacez par votre
interface WAN
        set srcaddr "all"
        set dstaddr "Blocked_IP_Group"
        set action drop
        set schedule "always"
        set service "ALL"
    next
```

```
    edit 2
        set name "Allow Authenticated Access"
        set srcintf "DMZ"
        set dstintf "internal"
        set srcaddr "Authenticated Hosts"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "SSH HTTP HTTPS"
        set utm-status enable
        set av-profile "default"
        set webfilter-profile "default"
        set ips-sensor "default"
        set ssl-ssh-profile "default"
    next
end

config user local
    edit "Admin_User"
        set password ENC <encrypted_password
        set accprofile "super_admin"
    next
end

config firewall policy
    edit 3
        set name "Block_Brute_Force_Attacks"
        set srcintf "DMZ"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "Authenticated_Hosts"
        set action drop
        set schedule "always"
        set service "SSH"
        set logtraffic all
        set logtraffic-start enable
        set logtraffic-end enable
    next
end
```

6. MikroTik

Les routeurs MikroTik sont déployés pour gérer les connexions vers nos succursales distantes.

- Configuration Générale :

Configuration du routage statique ou dynamique selon les besoins.

Paramétrage des règles de pare-feu pour la sécurité.

Activation du Network Address Translation (NAT) pour la translation d'adresses IP.

```
/system identity set name=MyRouter
/interface ethernet set [ find default-name=ether1 ]
name=LAN
/ip address add address=192.168.1.1/24 interface=LAN
```

7. ADSL / DSLAM

Les modems ADSL (Asymmetric Digital Subscriber Line) et les DSLAM (Digital Subscriber Line Access Multiplexer) jouent un rôle crucial dans la connectivité de nos réseaux à large bande passante.

- Configuration Générale :

Configuration des modems ADSL pour établir des connexions haut débit avec notre fournisseur d'accès Internet.

Attribution des adresses IP publiques et privées aux modems pour gérer le trafic entrant et sortant.

Activation de la sécurité du modem pour prévenir les accès non autorisés.

Configuration des modems pour fournir des services de téléphonie VoIP (Voice over IP) si nécessaire.

Mise en place de règles de pare-feu pour surveiller et filtrer le trafic Internet.

Configuration des DSLAM pour gérer les connexions ADSL des abonnés locaux.

Allocation de la bande passante aux abonnés en fonction de leurs forfaits et de leurs besoins.

Surveillance et gestion des performances des DSLAM pour garantir une connectivité stable.

```
enable
configure terminal
!
interface ATM0/0/0
 pvc 0/35
 encapsulation aal5mux ppp dialer
!
interface Dialer0
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap callin
 ppp chap hostname your_username
 ppp chap password 0 your_password
 ppp pap sent-username your_username password 0
your_password
!
end
write memory
```

8. NAS Storage Oracle

Le NAS Oracle est essentiel pour le stockage sécurisé et la gestion des données de l'entreprise.

- Configuration Générale :

Mise en place du NAS Oracle pour fournir un stockage partagé aux utilisateurs et aux serveurs.

Allocation des ressources de stockage en fonction des besoins de chaque service ou département.

Configuration de la sauvegarde automatique des données pour garantir la sécurité des informations.

Mise en œuvre de la redondance de disques pour prévenir les pannes matérielles.

Activation de la réplication des données pour une disponibilité continue en cas de sinistre.

Configuration des partages de fichiers et des autorisations d'accès.

Planification des sauvegardes automatisées pour la protection des données.

9. Contrôleurs de Domaine Windows Server

Les contrôleurs de domaine Windows Server gèrent l'annuaire Active Directory pour l'authentification et l'autorisation des utilisateurs.

- Configuration Générale :

Configuration des services Active Directory, DNS et DHCP.

Gestion des comptes d'utilisateurs et des stratégies de groupe.

10. VirtualBox et VMware ESXi

J'utilise VirtualBox et VMware ESXi pour la virtualisation des serveurs et la gestion des machines virtuelles.

- Configuration Générale :

Création et gestion des machines virtuelles.

Allocation de ressources aux machines virtuelles en fonction des besoins.

11. Citrix et SDN (Software-Defined Networking)

Citrix est utilisé pour la gestion des applications et du bureau à distance, tandis que la technologie SDN permet une gestion flexible et dynamique des réseaux.

- Configuration Générale (Citrix) :

Déploiement d'applications virtuelles et de bureaux à distance.

Gestion des licences et des politiques d'accès.

12. Disaster Recovery (DR)

Notre plan de reprise après sinistre (DR) garantit la disponibilité des données et des services en cas de catastrophe.

- Configuration Générale :

Planification des sauvegardes hors site.

Activation de la reprise après sinistre en cas de besoin.

13. Microsoft SQL Server et SCCM

Microsoft SQL Server est utilisé pour la gestion des bases de données, tandis que SCCM (System Center Configuration Manager) est utilisé pour la gestion de l'informatique d'entreprise.

- Configuration Générale (SQL Server) :

Configuration des bases de données et des autorisations.

Sauvegardes régulières des bases de données.

- Configuration Générale (SCCM) :

Déploiement de logiciels et de mises à jour.

Gestion des configurations et des stratégies.

14. Zones DMZ

J’ai mis en place des zones de démilitarisation (DMZ) pour isoler et sécuriser nos serveurs Web, DNS publics et autres services accessibles depuis Internet.

- Configuration Générale (Serveur Web DMZ) :

Autorisations d'accès depuis Internet.

Configuration du pare-feu pour la sécurité.

15. Serveur Exchange

Le serveur Exchange gère les communications de messagerie électronique de l'entreprise.

- Configuration Générale :

Configuration des boîtes aux lettres et des paramètres de messagerie.

Sécurisation des communications SMTP.

16. Systèmes de Détection d'Intrusion (IDS)

Les systèmes IDS jouent un rôle crucial dans cette infrastructure réseau en surveillant le trafic pour détecter les activités suspectes et les menaces potentielles.

- Configuration Générale :

Déploiement de systèmes IDS pour surveiller le trafic réseau en temps réel.

Activation des règles de détection pour identifier les signatures de menace connues.

Configuration des alertes pour signaler les activités anormales.

Analyse des journaux d'événements pour identifier les tentatives d'intrusion.

Mise à jour régulière des signatures de menace pour rester à jour avec les nouvelles menaces.

Réaction rapide en cas de détection d'activités malveillantes.

Génération de rapports sur les activités de détection des intrusions.

```
enable
configure terminal
!
interface GigabitEthernet0/0  # Interface pour la capture de trafic
 description Network Monitoring
 ip address 192.168.1.2 255.255.255.0
!
ip access-list extended IDS_ACL  # Liste d'access pour la capture
de trafic
 permit ip any any
!
ip ips name IDS_RULES  # Nom du jeu de règles IDS/IPS
!
ip ips configuration  # Configuration générale IDS/IPS
 signature-category
  all
!
!
interface GigabitEthernet0/1  # Interface connectée au réseau à
surveiller
 ip ips IDS_RULES in
 ip access-group IDS_ACL in
!
end
write memory
```

Les systèmes IDS jouent un rôle essentiel dans la détection précoce des menaces et dans la protection de notre réseau contre les activités malveillantes.

17. IPS (Systèmes de Prévention des Intrusions)

Les systèmes IPS complètent notre stratégie de sécurité en prévenant activement les intrusions et en bloquant les attaques en cours.

- Configuration Générale :

Déploiement de systèmes IPS pour surveiller le trafic et bloquer les activités malveillantes.

Activation des règles d'action pour réagir automatiquement aux menaces détectées.

Configuration de la prévention des intrusions pour bloquer activement les attaques en temps réel.

Gestion des alertes et des incidents de sécurité.

Mise à jour régulière des règles IPS pour une protection efficace.

Surveillance continue de l'efficacité des systèmes IPS.

Rapports détaillés sur les activités de prévention des intrusions.

```
enable
configure terminal
!
interface GigabitEthernet0/0  # Interface pour la surveillance du trafic
 description Network Monitoring
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1  # Interface connectée au réseau à surveiller
 description Connected to Internal Network
 ip address 192.168.1.1 255.255.255.0
!
ip access-list extended IPS_ACL  # Liste d'access pour la surveillance
 permit ip any any
!
class-map type inspect match-any IPS_CLASS_MAP  # Création de la classe de
trafic à surveiller
 match protocol http
 match protocol smtp
 match protocol dns
!
policy-map type inspect POLICY  # Création de la politique de surveillance IPS
 class type inspect IPS_CLASS_MAP
  ips promiscuous fail-open
!
zone security INSIDE  # Création de la zone de sécurité intérieure
!
zone-pair security ZONE-PAIR-IPS source INSIDE destination self  # Création de
la zone-pair
 service-policy type inspect POLICY
!
end
write memory
```

Les systèmes IPS jouent un rôle crucial dans la sécurisation de notre réseau en empêchant activement les tentatives d'intrusion et en renforçant notre posture de sécurité globale.

18. Téléphones IP

Les téléphones IP sont des éléments essentiels de notre infrastructure de communication, permettant des communications vocales de haute qualité via notre réseau IP, ils sont au cœur de nos communications internes et externes, offrant une connectivité vocale efficace et des fonctionnalités avancées pour améliorer la collaboration au sein de notre entreprise.

- Configuration Générale :

Déploiement de téléphones IP pour faciliter les appels vocaux entre les employés et les utilisateurs.

Configuration des paramètres réseau pour chaque téléphone IP.

Attribution d'adresses IP aux téléphones IP pour permettre la communication sur le réseau.

Intégration avec notre système de téléphonie VoIP (Voice over IP).

Activation de la sécurité des appels pour chiffrer les communications vocales.

Discussion

Le projet de construire une infrastructure informatique complexe pour une grande installation représente un défi de taille, mais aussi une opportunité d'amélioration majeure de notre environnement technologique. Dans cette section, nous examinons les progrès, les leçons apprises et nous concentrons sur l'avenir.

L'un des principes objectifs de ces travaux entité d'améliorer la sécurité de nos services. Avec l'intégration des pare-feu FortiGate, des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS), nous avons encore renforcé notre posture de sécurité. Ces dispositifs ont permis une détection précoce des menaces et une réponse rapide aux incidents, réduisant ainsi les risques potentiels pour nos sens. De plus, Les zones DMZ ont permis de mieux segmenter le réseau, limitant ainsi la surface d'attaque.

La création de Deux Centre de Data, Primary Data Center et Standby Data Center a considérablement amélioré notre capacité à continuer à fonctionner. En cas de panne sinistre ou majeure, notre infrastructure peut doucement se diriger sur la pointe des pieds vers le centre de données de secours, ce qui garantit que nos critiques de service restent disponibles. Cela représente un énorme avantage pour notre entreprise, réduisant et atténuant les problèmes potentiels.

La migration vers IPv6 fait partie du la stratégie de ce projet. À mesure que l'espace d'adressage IPv4 s'épuise, il est nécessaire de préparer nos réseaux internes à la transition vers IPv6. Cette préparation nous donne envie de vouloir l'avenir d'Internet et garantit que notre connectivité et notre accessibilité ne seront pas sur le point d'être compromises à mesure que l'adoption d'IPv6 se généralisera.

Ce projet a été un processus d'apprentissage continu. Nous avons constaté qu'une planification minutieuse et des procédures rigoureuses sont nécessaires au succès de projets de cette nature. Des tests et des évaluations continues sont également essentiels pour garantir la stabilité et la protection de l'infrastructure.

En conclusion, ce projet a constitué une étape importante dans l'amélioration de notre infrastructure informatique. Cela a renforcé nos défenses, amélioré notre résilience et préparé notre reprise des défis à venir. Avec une stratégie solide et une équipe dédiée, nous sommes prêts à affronter l'avenir avec confiance.

Conclusion

En conclusion, la construction de cette infrastructure informatique complexe et sécurisée pour l'entreprise a été un succès retentissant. Ce projet a permis d'atteindre nos objectifs majeurs, à savoir renforcer la sécurité, assurer la continuité des opérations et préparer le réseau à la transition vers IPv6. Les enseignements tirés et les résultats obtenus sont précieux et contribuent à renforcer notre position dans le monde en constante évolution de la technologie de l'information.

La sécurité a été au cœur de la préoccupation tout au long du projet. L'intégration de pare-feu, de systèmes de détection d'intrusion et de prévention d'intrusion a renforcé la posture de sécurité, protégeant les données et les actifs critiques contre les menaces potentielles. Les zones DMZ ont également amélioré la capacité à isoler et à contrôler le trafic, renforçant ainsi la sécurité globale.

La continuité des opérations a été renforcée grâce à la mise en place de deux centres de données fonctionnant en tandem. Cette redondance a considérablement réduit le risque de temps d'arrêt en cas de sinistre ou de panne, garantissant que les services critiques restent accessibles et que les activités peuvent continuer sans interruption majeure.

La préparation pour l'IPv6 place en première ligne de l'évolution de l'Internet. Alors que l'adoption d'IPv6 se généralise, l'infrastructure est prête à prendre en charge cette technologie, garantissant que nous restons connectés et accessibles sur l'ensemble du réseau mondial.

On a également profité de la virtualisation pour optimiser la gestion de des ressources informatiques, ce qui a contribué à réduire les coûts et à améliorer l'efficacité opérationnelle.

Enfin, nous avons constaté que la planification minutieuse et une méthodologie rigoureuse sont essentielles pour le succès d'un projet de cette envergure. Les tests continus et la surveillance proactive sont tout aussi importants pour maintenir la stabilité et la sécurité de l'infrastructure.

Références

- Tanenbaum, A. S., & Wetherall, D. J. (2018). Computer Networks. Pearson.
- Cisco. (n.d.). Cisco Networking Academy. https://www.netacad.com/
- Juniper Networks. (n.d.). Juniper Networks Education and Training. https://www.juniper.net/us/en/training/
- Fortinet. (n.d.). Fortinet Training and Certification. https://www.fortinet.com/training
- MikroTik. (n.d.). MikroTik Training. https://mikrotik.com/training
- Oracle. (n.d.). Oracle Storage Solutions. https://www.oracle.com/storage/
- Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.
- Cisco. (n.d.). Intrusion Detection and Prevention. https://www.cisco.com/c/en/us/products/security/intrusion-detection-system/index.html
- Juniper Networks. (n.d.). Intrusion Detection and Prevention. https://www.juniper.net/us/en/products-services/security/next-generation-firewall/intrusion-detection-prevention/
- Fortinet. (n.d.). Intrusion Prevention System (IPS). https://www.fortinet.com/products/security-fabric/fortigate/ips.html
- Cisco. (n.d.). Spanning Tree Protocol. https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/1244-813.html
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification. https://tools.ietf.org/html/rfc2460
- National Institute of Standards and Technology (NIST). (n.d.). NIST Computer Security Resource Center. https://csrc.nist.gov/
- Internet Assigned Numbers Authority (IANA). (n.d.). IPv4 Address Space. https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml
- Internet Assigned Numbers Authority (IANA). (n.d.). IPv6 Address Space. https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml
- Comité Consultatif de Réseau (Réf. [RFC1034]). (1987). Domain Names - Concepts and Facilities. https://tools.ietf.org/html/rfc1034
- Comité Consultatif de Réseau (Réf. [RFC1035]). (1987). Domain Names - Implementation and Specification. https://tools.ietf.org/html/rfc1035
- Sans Institute. (n.d.). Information Security Resources. https://www.sans.org/
- O'Reilly Media. (n.d.). IT Books and Videos. https://www.oreilly.com/
- Computer Security Resource Center (CSRC) - National Institute of Standards and Technology (NIST). (n.d.). https://csrc.nist.gov/

Remerciements

Je tiens à exprimer mes sincères remerciements à toutes les personnes qui ont contribué à la réalisation de ce projet ambitieux.

Tout d'abord, je remercie mes collègues administrateurs réseaux et systèmes dévoués, dont l'expertise au sein de notre entreprise, la persévérance et la collaboration ont été essentielles pour faire avancer ce projet avec succès. Leurs engagements envers l'excellence ont été exemplaire ainsi que leurs travails acharnés et la coopération ont été la clé de succès, et je suis honorés de travailler avec une équipe aussi exceptionnelle.

J’exprime également sincère reconnaissance envers nos professeurs qui ont fourni un encadrant de haute qualité et un soutien technique essentiel tout au long du projet. Votre collaboration a été inestimable.

Mes remerciements vont également à la direction de l'école pour son soutien continu et son engagement envers l'amélioration de nos études, votre vision stratégique a été un moteur puissant derrière notre succès.

Nous n'oublions pas nos collègues, nos amis et nos familles. Votre compréhension, votre patience et votre encouragement tout au long de ce projet ont été un soutien précieux.

Ce projet a été une étape importante dans l'évolution de ma carrière, et je suis impatients de continuer à travailler pour relever de nouveaux défis et réaliser de nouvelles réalisations à l'avenir.