République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Mémoire de Fin d'études Master

Réalisé par :

Belhocine Amira

Chetta Lamia

Filière : Télécommunications

Option : Réseaux et télécommunications

Thème :

Développement d'un outil d'automatisation des configurations des équipements réseaux Cisco

Devant le jury :

Mme	Acheli	Dalila	Prof	UMBB	Président
Mme	Guerbai	Yasmine	MCA	UMBB	Examinateur
Mme	Mahdi	Ismahan	MCB	UMBB	Promotrice

Année Universitaire : 2022/2023

Remerciements

En préambule à ce mémoire, nous exprimons nos sincères remerciements à **ALLAH** pour nous avoir guidés, soutenus et accordé la patience et le courage nécessaires tout au long de nos années d'études.

Nous tenons à remercier notre promotrice **Mme. Ismahane Mahdi**, pour son encadrement précieux et son soutien constant tout au long de ce projet. Ses conseils éclairés et sa disponibilité ont joué un rôle essentiel dans la qualité de notre travail.

Nous tenons aussi à adresser nos sincères remerciements à nos encadreurs **M. Kesraoui Abdelkader** et **M. Benyahi Djamel** pour nous avoir donné l'occasion de travailler sur un projet aussi excitant et nous avoir fait découvrir le monde du travail.

Nos remerciements s'adressent également aux membres du jury, qui ont consacré leur temps et leur expertise pour évaluer notre mémoire.

Enfin, nous exprimons notre gratitude envers toutes les personnes qui, de près ou de loin, nous ont constamment soutenus et encouragés tout au long de ce parcours.

Veuillez accepter nos plus sincères remerciements.

Dédicace

Tout d’abord je tiens à remercier ALLAH le tout puissant, qui nous a donné la force la patience d’accomplir ce travail.

À celle qui m'a appris mes premières lettres pour que je me tiens ici, à mon paradis, à la prunelle de mes yeux et la source de ma joie et mon bonheur, ma moitié Maman.

À celui à qui je parle des étoiles, il m'apportera la lune, ma source de vie et d’amour, à mon support et mon inspirant, mon héro Papa.

À mon puits de secret, ma source d’énergie mes deux adorable sœurs Lina et Ikram, merci d'avoir été toujours là pour moi.

À mes deux petits frères Nadjib et Samy mes piliers inébranlables, mes compagnons de vie et mes meilleurs amis.

À tous les membres de ma grande famille pour leurs prières et encouragements.

À ma promotrices Mme Mahdi Ismahane pour sa guidance précieuse et son soutien constant.

À mes précieuses amies merci d'avoir toujours été là pour moi, à travers les hauts et les bas, à partager les rires et les larmes.

Sans oublier ma meilleure binôme Amira, qui a toujours su me comprendre, m'écouter et me soutenir, avec qui j’ai créé des souvenirs inoubliables.

Je suis profondément reconnaissante envers tous ceux qui ont contribué à ma réussite et qui m'entourent avec amour.

Chetta Lamia

Dédicace

Pour chaque début il y a une fin, et ce qui est beau dans toute fin c'est la réussite et +l'atteinte du but.

J’ai le grand plaisir de dédier ce modeste travail

A ceux qui ont fait de moi une femme …mes parents

Ma très chère mère pour ses encouragements, son soutien.

Mon très cher père qui me donne toujours l’espoir de vivre et qui n’a jamais cessé de m’aider.

Mes chères sœurs et à mes frères “Didin, Youcef, Farah et hala “ je vous aime.

A mon cher marie qui m’as accompagné et soutenu tout au long de ce parcours, Ton amour et ton soutien inébranlable sont ma force et ma motivation.

A mon binôme et ma meilleure amie Lamia pour sa présence et son soutien À travers les hauts et les bas, les moments de stress et de doute.

A toute ma famille ma chère grand-mère mes tantines et mes cousins.

A la fin je dédie, très chaleureusement, ce mémoire à tous ceux que j’aime et que je respecte.

Belhocine Amira

Sommaire

ملخص
Résumé
Abstract
Liste des figures
Liste des tableaux
Liste des abréviations
Introduction générale....1
CHAPITRE I : Généralités sur les réseaux SDN
I.1 Séparation de la logique de contrôle et de la couche physique....2
I.1.1 Comparaison entre les réseaux traditionnel et SDN....3
I.2 Composants d'un réseau SDN....4
I.2.1 Plan de contrôle....4
I.2.1.1 Contrôleur SDN....4
I.2.2 Plan de données....5
I.2.2.1 Commutateur SDN....5
I.2.3 Application Programming Interface (API)....5
I.3 Architecture d'un réseau SDN....6
I.3.1 Plan de données....6
I.3.2 Plan de contrôle....6
I.3.3 Plan de gestion....6
I.4 Contrôleur SDN....7
I.4.1 Fonctionnalités du contrôleur SDN....7
I.4.2 Les types de contrôleurs....8
I.5 Protocoles de communication dans un réseau SDN....9
I.5.1 OpenFlow....9
I.5.2 OVSDB....10

I.5.3 NETCONF 10

I.5.4 RESTCONF 10

I.5.5 BGP-LS 10

I.5.6 PCEP 11

I.5.7 P4Runtime 11

I.6 Programmation et automatisation des réseaux SDN 11

I.6.1 Réduction des coûts 12

I.6.2 Amélioration de la sécurité 12

I.6.3 Optimisation des performances 12

I.6.4 Flexibilité 12

I.7 SDN dans un Réseaux virtuels 13

I.8 Avantages et domaines d'utilisation des réseaux SDN 14

I.8.1 Datacenter 14

I.8.2 Campus 14

I.8.3 Fournisseurs de services 14

I.9 Défis de la mise en œuvre de réseau SDN 15

I.9.1 Fiabilité 15

I.9.2 Évolutivité 15

I.9.3 Performance et sécurité 15

I.10 Aléas de sécurité dans les réseaux SDN 16

CHAPITRE II : Présentation des équipements Cisco

II.1 Historique sur CISCO 18

II.2 Différents types d'équipements Cisco 19

II.2.1 Commutateur 19

II.2.1.1 Fonctionnement 19

II.2.1.2 Différents types de switch 20

II.2.2 Routeurs 23

II.2.2.1 Fonctionnement 23

II.2.2.2 Différents types de routeurs 24

II.2.3 Point d'accès sans fil 26

II.2.3.1 Fonctionnement 27

II.2.4 Firewalls 27

II.2.4.1 Principaux avantages des pare-feu matériels 27

II.3 Les certifications Cisco 28

II.4 Utilisation de l'interface utilisateur Cisco 29

II.4.1 Interface en ligne de commande 30

II.4.2 Interface graphique 30

II.5 Configuration des équipements Cisco 31

II.5.1 Comment accéder à la configuration d'un équipement 31

II.5.1.1 Via une Console série 31

II.5.1.2 Via une connexion réseau 32

II.6 Dépannage des équipements Cisco 33

II.6.2 Procédure de dépannage 33

CHAPITRE III : CIS control

III.1 Historique et évolution 36

III.1.1 Etapes d'évolution de CIS control 36

III.1.1.1 Développement initial des contrôles CIS 36

III.1.1.2 Révisions et mises à jour régulières 36

III.1.1.3 Alignement avec d'autres normes et cadres de sécurité 36

III.1.1.4 Extension du nombre de contrôles 36

III.1.1.5 Adoption croissante par les organisations 36

III.2 Rôle de CIS control 37

III.2.1 Les domaines d'expertise de CIS 37

III.2.1.1 Inventaire et contrôle des actifs 37

III.2.1.2 Gestion de la configuration 37

III.2.1.3 Gestion des correctifs et des vulnérabilités 37

III.2.1.4 Gestion des privilèges 37

III.2.1.5 Sécurisation des configurations de réseau 38

III.2.1.6 Surveillance continue 38

III.2.1.7 Protection anti-malware 38

III.2.1.8 Gestion des journaux de sécurité 38

III.2.1.9 Gestion de l'accès aux données 38

III.2.1.10 Formation et sensibilisation à la sécurité 38

III.3 Normes de CIS control 38

III.4 Dernière version des contrôles CIS 39

III.5 Avantages de l'utilisation des normes CIS 40

III.5.1 Standardisation 40

III.5.2 Meilleures pratiques de sécurité 40

III.5.3 Coûts réduits 40

III.5.4 Conformité 41

III.5.5 Facilité d'utilisation 41

III.5.6 Amélioration constante 41

III.6 Comment les normes CIS control peuvent aider à renforcer la sécurité des équipements Cisco 41

III.7 CIS Benchmark pour CISCO 42

III.8 Différence entre un équipement Cisco configuré avec ou sans CIS control 43

CHAPITRE IV : Développement de la solution d'automatisation

IV.1 Présentation des différents CIS Benchmarks utilisés par Cisco 45

IV.1.1 CIS Cisco IOS Router Benchmark 45

IV.1.2 CIS Cisco ASA Firewall Benchmark 46

IV.1.3 CIS Cisco Catalyst Switch Benchmark 46

IV.1.4 CIS Cisco Wireless LAN Controller Benchmark 46

IV.1.5 CIS Cisco Email Security Appliance Benchmark 46

IV.2 La maquette du réseau 46

IV.2.1 EVE-NG VM 47

IV.3 Les outils de développement 47

IV.3.1 Langage de programmation 47

IV.4 Environnement logiciel 48

IV.4.1 VMware Workstation Pro 48

IV.4.2 WinSCP 48

IV.4.3 PuTTY 49

IV.4.4 Visual Studio Code 49

IV.5 Etapes d'installation et de configuration 49

IV.6 Architecture d'un réseau 53

IV.7 Simulation et test des différents scénarios et commandes 54

IV.8 Résultats 55

Conclusion générale 58

Références bibliographiques

ملخص

تعتبر أمان شبكات الحواسيب تحديًا حاسمًا للشركات. يجب أن تتخذ هذه الشركات تدابير قوية للوقاية وحماية معداتها. وفي هذا السياق، قمنا بتطوير أداة تلقائية لتكوين معدات سيسكو بهدف تعزيز أمان الشبكات من خلال تحديد الأخطاء المحتملة وتقديم حلول مناسبة. استخدام لغة البرمجة بايثون سمح لنا بإنشاء عملية فعالة لاكتشاف وتصحيح التكوينات غير الصحيحة، مما يسهم في توفير حماية مثلى لمعدات الشبكة.

كلمات مفتاحية: أمان شبكات، أداة تلقائية، معدات سيسكو، بايثون، التكوينات.

Résumé

La sécurité des réseaux informatiques est un défi crucial pour les entreprises. Elles doivent mettre en place des mesures solides pour prévenir protéger leurs équipements. Dans cette optique, nous avons développé un outil d'automatisation des configurations des équipements Cisco vise à renforcer la sécurité des réseaux en identifiant les erreurs potentielles et en proposant des solutions adaptées. L'utilisation de Python comme langage de programmation nous a permis de créer un processus efficace pour détecter et corriger les configurations incorrectes, contribuant ainsi à une protection optimale des équipements réseau.

Mots clés : Sécurité des réseaux, Outil d'automatisation, Equipements Cisco, Python, Les configurations.

Abstract

The security of computer networks is a crucial challenge for companies. They must implement strong measures to prevent and protect their equipment. With this in mind, we have developed an automated tool for configuring Cisco equipment aimed at enhancing network security by identifying potential errors and proposing suitable solutions. The use of Python as the programming language has enabled us to create an efficient process for detecting and correcting incorrect configurations, thereby contributing to optimal protection of network equipment.

Keywords: Security of computer networks, Automated tool, Cisco equipment, Python, The configurations.

Liste des figures

Chapitre I : *Généralités sur les réseaux SDN*

Figure I.1 Comparaison entre un réseau traditionnel et un réseau SDN
Figure I.2 Les composants d'un réseau SDN
Figure I.3 Architecture d'un réseau SDN
Figure I.4 Architecture OpenFlow
Figure I.5 Architecture de base du réseau NETCONF
Figure I.6 Architecture du réseau RESTCONF
Figure I.7 Architecture BGP_LS
Figure I.8 Plateforme des réseaux virtuelles
Figure I.9 Fonctionnement des réseaux virtuels avec SDN

Chapitre II : *Présentations des équipements Cisco*

Figure II.1 Commutateur catalyste
Figure II.2 Commutateurs Nexus
Figure II.3 Commutateurs Meraki
Figure II.4 Commutateurs industriels
Figure II.5 Commutateurs de fournisseurs de services
Figure II.6 Routeur Cisco CRS-1 (2004)
Figure II.7 Routeur sans fil
Figure II.8 Routeur filaire
Figure II.9 Routeur central
Figure II.10 Routeur périphérique
Fig11re II.11 D-Link wireless access point
Figure II.12 Certifications Cisco
Figure II.13 Procédures de dépannage

Chapitre III : *CIS control*

Figure III.1 Top 20 CIS control
Figure III.2 Comparaison entre la version 7 et 8 de contrôle CIS

Chapitre IV : *Développement de la solution d'automatisation*

Figure IV.1 La façade de VMware Workstation pro
Figure IV.2 Virtual network editor
Figure IV.3 EVE-NG
Figure IV.4 Accès à l'interface de EVE-NG
Figure IV.5 Connecter WINSCP avec la machine
Figure IV.6 Transfert des fichiers entre la machine et le pc
Figure IV.7 L'interface de l'émulateur PuTTY
Figure IV.8 Connecter PUTTY avec la machine
Figure IV.9 Architecture de l'entreprise
Figure IV.10 Création de code python 01
Figure IV.11 Création de code python 02
Figure IV.12 La détection des vulnérabilités de routeur 01
Figure IV.13 La détection des vulnérabilités de routeur 02
Figure IV.14 La détection des vulnérabilités de switch layer3 01
Figure IV.15 La détection des vulnérabilités de switch layer3 02

Liste des tableaux

Chapitre I : *Généralités sur les réseaux SDN*

Tab I.1 Comparaison entre les deux interfaces (CLI et GUI)

Chapitre II : *Présentations des équipements Cisco*

Tab II.1 Comparaison entre les deux interfaces (CLI et GUI)

Liste des abréviations

ACI	Application Centric Infrastructure
ACL	Anterior cruciate ligament
AP	Advanced Placement
API	Application Programming Interface
BGP	Border Gateway Protocol
BGP-LS	Border Gateway Protocol - Link State
CD-ROM	Compact Disc Read-Only Memory
CIS	Computer Information System Company
Cisco	Computer Information System Company
CLI	Command Line Interface
DoS	Denial of Service
EVE-NG	Emulated Virtual Environment - Next Generation
FTP	File Transfer Protocol
GPL	General Public License
Grpc	Google Remote Procedure Call
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
IDE	Integrated Development Environment
IEc	International Electrotechnical Commission
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control address

NETCONF	Network Configuration Protocol
NVF	Network Virtualization Function
ONOS	Open Network Operating System
OVS	Open vSwitch
OVSDB	Open vSwitch Database Management Protocol
PCEP	Path Computation Element Protocol
PCI DSS	Payment Card Industry Data Security Standard
P4	Programming Protocol-Independent Packet Processors
P4Runtime	P4 Programmable Runtime Interface
QoS	Quality of Service
REST	Representational State Transfer
RESTCONF	RESTful Configuration Protocol
SCP	Secure Copy Protocol
SDN	Software-Defined Networking
SMSI	Système de Management de La Sécurité de l'Information
SPTF	SSH File Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual local area network Virtual Machine
VM	Virtual private network Virtual Machine
VPN	Virtual private network
VS	Visual Studio
VyOS	Vyatta on System
WAN	Wide Area Network

WAP	Wireless Access Point
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

Présentation d'Algérie Télécom

Algérie Telecom

Le GROUPE TELECOM ALGERIE est une entreprise publique économique fondé le 9 Novembre 2017, elle est société par actions algérienne de télécommunications ayant pour principal but la mise en œuvre, la coordination et le contrôle des grands projets de télécommunications en Algérie.

Le GROUPE TELECOM ALGERIE possède six sociétés économiques publiques dont quatre sont directement rattachées à lui tandis que les deux autres le sont indirectement par le biais de ses filiales en tant que sous-filiales. Le groupe compte actuellement plus de 25000 employés à travers tout le territoire national et à sa tête Monsieur Khaled ZARAT entant en tant que Président Directeur Général.

Sa création (GROUPE TELECOM ALGERIE) est à l'origine issue de la création de son actuelle filiale ALGERIE TELECOM durant l'année 2000 et cela suite à l'entrée en vigueur de la loi N°03/2000 du 5 août 2000 qui dispose la séparation complète des activités postales et télécommunications des anciens services de PTT.

Depuis lors, les principales activités d'ALGERIE TELECOM se résument à l'octroi de divers services tels que l'accès à internet haut débit et de connexions sans fil (4G LTE), la mise à disposition de lignes téléphoniques fixes et enfin divers services satellitaires (VSAT…)

Avant la séparation des activités postales des anciens services de PTT, le marché des télécommunications était témoin d'un énorme manque en terme de couverture réseau. En effet, seulement 6% de la population algérienne était couverte par le réseau de l'époque.

Au cours des années 2000, la principale technologie de télécommunication en Algérie était la méthode accès multiple par répartition temporelle sous le nom de TDM (Multi Time Division) « Technique de contrôle d'accès au support permettant de transmettre plusieurs flux de trafic sur un seul canal ou une seule bande de fréquence ».

Le 10 avril 2003, ALGERIE TELECOM a officiellement démarré ses activités commerciales en tant qu'Entreprise Nationale de Télécommunications et ce en vertu de la loi N°03/2000 comme précédemment mentionné.

Les premiers services de télécommunications d'ALGERIE TELECOM ont été assurés à travers de nombreuses technologies de réseaux telles que le RTPC (Real Time Transport Control Protocol) pour la téléphonie fixe, le GSM (Global System for Mobile Communications) pour la télécommunication mobile, le Dz-PAC et le MEGA-PAC pour les publications officielles et gouvernementales et enfin l'accès à l'internet haut-débit via sa filiale de l'époque 'DJAWEB'.

Missions et objectifs

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles.
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications .

- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

ALGERIE TELECOM est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales ;
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications ;
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.

Organisation d'Algérie Télécom

ALGERIE TELECOM est organisée en Divisions, Directions Centrales, et Régionales, à cette structure s'ajoutent trois filiales :

- ALGÉRIE TÉLÉCOM **: Fournisseur** de téléphonie fixe, d'internet haut-débit et de connexion sans fil.
- ALGÉRIE TÉLÉCOM MOBILE **: Opérateur** de réseau mobile et d'internet haut-débit sans fil.
- ALGÉRIE TÉLÉCOM SATELLITE (ATS**) : Entreprise** spécialisée dans les services de télécommunication par satellite.
- ALGÉRIE TÉLÉCOM EUROPE (ATE) **: Société** qui gère le câble sous-marin « ORVAL/ARVAL » reliant les télécommunications algériennes aux européennes.
- COMINTAL **SPA :** Entreprise répondant à la demande de solutions et dispositifs de fibre optique brute (fibre optique noire).
- SATICOM SPA **: Entreprise** spécialisée dans les solutions technologiques modernes permettant aux entreprises de communiquer de manière plus efficiente en interne et en externe. A l'image du Groupe Télécom Algérie, toutes les filiales travaillent d'arrache-pied pour assurer la satisfaction de leurs clients et ce en leur assurant une perpétuelle qualité de service.

Introduction générale

Les réseaux informatiques continuent d'évoluer pour répondre aux demandes croissantes d'efficacité des équipements et de gestion simplifiée. L'automatisation joue un rôle clé en permettant aux entreprises d'optimiser leurs opérations, de réduire les erreurs humaines et de libérer des ressources précieuses.

Dans le premier chapitre, un aperçu sera donné de la mise en réseau SDN (Software Defined Networking), qui sépare le plan de contrôle du plan de données pour offrir une plus grande flexibilité et agilité. L'automatisation dans les réseaux SDN permet le contrôle et la configuration par programmation des appareils, offrant une gestion centralisée et simplifiée. Cette automatisation apporte des avantages tels que la flexibilité de configuration et la réduction des erreurs humaines.

Le deuxième chapitre de notre projet se concentrera sur les équipements Cisco, qui jouent un rôle crucial dans notre infrastructure réseau. Nous passerons en revue les différents types d'équipements Cisco et leurs fonctionnalités avancées. Nous examinerons également comment ces équipements sont intégrés aux réseaux SDN et mettrons en évidence nos bonnes pratiques et recommandations pour l'administration et la configuration des équipements Cisco.

Dans le troisième chapitre, nous aborderons le CIS Control (Center for Internet Security Control) en relation avec notre outil d'automatisation des configurations des équipements Cisco. Le CIS Control fournit des directives et des mesures de sécurité pour protéger nos infrastructures réseau contre les menaces et les vulnérabilités. Nous étudierons comment notre outil d'automatisation peut faciliter la mise en œuvre des contrôles CIS et renforcer la sécurité globale de notre réseau.

Enfin, dans le quatrième chapitre, nous présenterons les résultats attendus de notre projet. Nous avons créé un programme automatisé en Python qui détecte les failles de configuration des machines Cisco. Notre outil évalue les options en place, détecte les circonstances où les règles de sécurité ne sont pas respectées et les remplace par des circonstances correctes. Cela facilite la gestion de nos infrastructures, renforce nos communications et préserve la cohérence de nos configurations. Grâce à cet outil, nous pouvons efficacement préserver des configurations correctes et réduire les dangers potentiels associés à des failles de sécurité.

Chapitre I

Généralités sur les réseaux SDN

Introduction

Les réseaux SDN (Software-Defined Networking) sont une nouvelle façon de gérer et de configurer les réseaux informatiques. Plutôt que de se concentrer sur le provisionnement de périphériques réseaux individuels, le SDN sert à séparer le plan de contrôle (logiciel) du plan de données (matériel). En SDN, le plan de contrôle consiste en un contrôleur centralisé qui gère l'ensemble du réseau. Les périphériques réseau, tels que les commutateurs et les routeurs, sont programmés pour transmettre des informations sur l'état du réseau à un contrôleur, qui décide ensuite comment déplacer les données sur le réseau. Cette architecture centralisée permet une gestion du réseau plus efficace et flexible et augmente l'automatisation des tâches de gestion.

Dans ce chapitre, nous allons présenter des notions et des concepts sur les réseaux SDN en commençant par donner une définition de ce type de réseaux et ses différentes composantes. Une architecture générale du SDN sera illustrée. La partie contrôleur SDN sera étudiée en détail ainsi que les protocoles de communication associés, sans oublier les réseaux virtuels dans un environnement SDN. Comme les réseaux SDN présentent plusieurs avantages, nous les avons cités avec quelques exemples de domaines d'application.

I.1 Séparation de la logique de contrôle et de la couche physique

Dans les réseaux classiques, le plan de contrôle est intégré dans chaque périphérique réseau, ce qui rend la gestion du réseau plus complexe et difficile à étendre. Dans le réseau SDN, la couche de contrôle est concentrée dans le contrôleur SDN, qui peut gérer le réseau de manière plus flexible et dynamique.

La couche physique comprend les périphériques réseau, tels que les commutateurs et les routeurs, qui transportent le trafic réseau. La logique de contrôle, quant à elle, est définie dans le contrôleur SDN et est chargée de décider comment acheminer le trafic à travers le réseau.

La communication entre les couches de contrôle et physique est réalisée à l'aide d'un protocole de communication tel qu'OpenFlow, qui permet au contrôleur SDN d'envoyer des messages de configuration aux périphériques réseau pour définir des règles de flux. Ces règles de flux spécifient comment le trafic doit être acheminé via le réseau en fonction de critères tels que l'adresse IP de destination, le port de destination, le type de protocole, etc.

La séparation des couches logiques et physiques de contrôle permet une plus grande flexibilité et efficacité dans la gestion du réseau car elle permet de centraliser la gestion des politiques de

contrôle et de les appliquer de manière cohérente sur l'ensemble du réseau. Cela facilite également l'expansion du réseau car les politiques de contrôle peuvent être mises à jour et modifiées de manière centralisée sans avoir à modifier chaque périphérique réseau individuellement.

I.1.1 Comparaison entre les réseaux traditionnel et SDN :

Ce tableau présente les principales différences entre les réseaux traditionnels et le SDN :

Réseaux traditionnels	**Réseaux SDN**
• Le contrôle du réseau est complexe • Une configuration manuelle et la possibilité de faire des erreurs qui vont entrainer un comportement erroné du réseau • Le problème de configuration statique • Difficulté d'implémentation de logiciel et des mises à jour dans le réseau • Environnement de test limité	• Découpler le plan de contrôle de celui du plan de donné • Offre un meilleur contrôle du réseau et la possibilité de la programmer • Configuration automatique à travers une centralisation de contrôle du réseau • Optimisation de la configuration • Contrôle global de l'information • L'implémentation facile de logiciels et des mises à jour dans le réseau • Environnement de test suffisant

Tab I.1 comparaison entre réseau traditionnel et réseau SDN

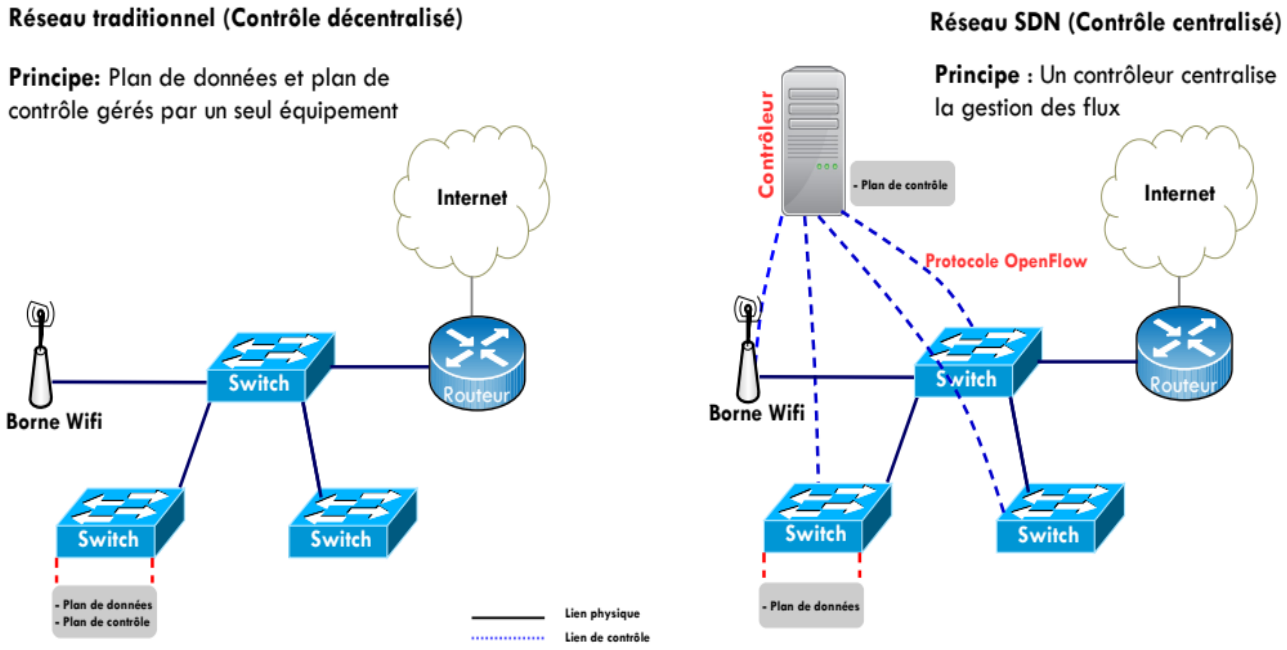

Figure I.1 Comparaison entre un réseau traditionnel et un réseau SDN

I.2 Composants d'un réseau SDN

I.2.1 Plan de contrôle

Le plan de contrôle est le logiciel qui permet au contrôleur SDN de communiquer avec le commutateur SDN et de configurer les règles de routage. Le plan de contrôle s'exécute généralement sur des serveurs distincts du plan de données.

Pour résumer, les composants clés d'un réseau SDN comprennent les contrôleurs SDN, les commutateurs SDN, les API, les plans de données et les plans de contrôle. Ces éléments fonctionnent ensemble pour fournir des solutions réseau flexibles et personnalisables qui répondent aux besoins spécifiques de l'entreprise.

I.2.1.1 Contrôleur SDN

C'est le cerveau du réseau SDN. Il gère l'ensemble du réseau et prend les décisions de routage. Les contrôleurs SDN sont programmables, ce qui signifie que les administrateurs réseau peuvent configurer et personnaliser les règles de routage pour répondre à leurs besoins réseau spécifiques.

I.2.2 Plan de données

Le plan de données est le réseau physique pour la transmission de données entre les commutateurs SDN. Le contrôleur SDN utilise les informations collectées par les commutateurs pour prendre des décisions de routage et de commutation.

I.2.2.1 Commutateur SDN

Le commutateur SDN est un périphérique réseau intelligent qui communique avec le contrôleur SDN et exécute les règles de routage définies par le contrôleur. Les commutateurs SDN sont souvent équipés de capacités de virtualisation de réseau pour simplifier la gestion et la configuration du réseau.

I.2.3 Application Programming Interface (API)

Une API est une interface de programmation qui permet aux développeurs de créer des applications personnalisées pour les réseaux SDN. Les applications peuvent être utilisées pour automatiser des tâches réseau spécifiques, telles que la surveillance du trafic ou la gestion de la qualité de service.

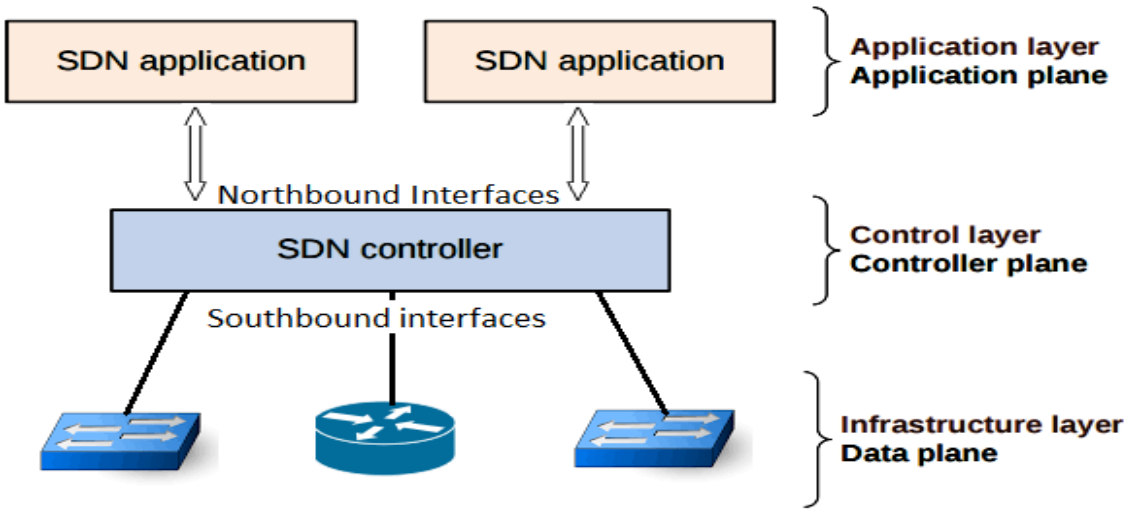

Figure I.2 Les composants d'un réseau SDN

I.3 Architecture d'un réseau SDN

L'architecture des réseaux SDN vise à séparer la gestion du trafic de la gestion des périphériques réseau. Cette approche offre aux administrateurs réseau une plus grande flexibilité et car ils peuvent programmer le comportement du réseau à partir d'une interface centralisée et unifiée. Elle possède plusieurs éléments :

I.3.1 Plan de données

C'est l'ensemble des équipements de réseau tels que les commutateurs, les routeurs et les points d'accès sans fil qui acheminent le trafic réseau. Dans un réseau SDN, les équipements du plan de données sont appelés des "switches intelligents" ou des "switches programmables" car ils sont capables de communiquer avec le contrôleur SDN pour recevoir des instructions de gestion du trafic.

I.3.2 Plan de contrôle

C'est la tête du réseau SDN. Il comprend le contrôleur SDN, qui est un logiciel exécuté sur le serveur.

I.3.3 Plan de gestion

Il s'agit de l'interface utilisateur permettant aux administrateurs réseau de gérer le réseau SDN. Cette interface permet à ces derniers de définir des politiques de gestion du trafic, d'afficher des statistiques de trafic et de surveiller l'état des périphériques de plan de données.

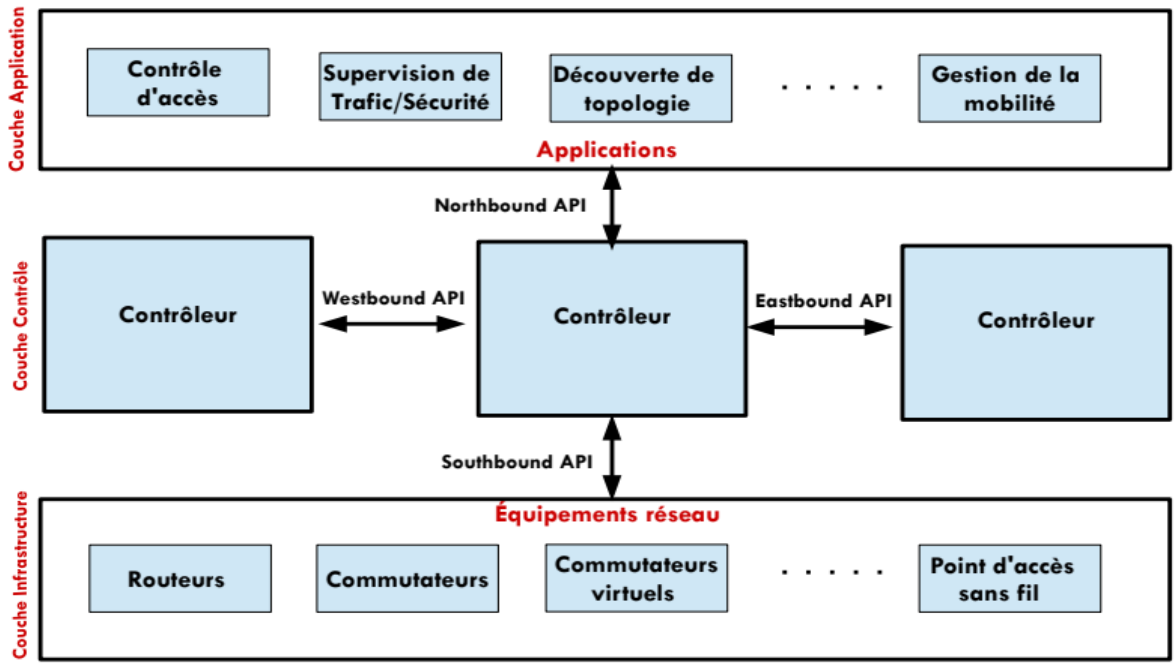

Figure I.3 Architecture d'un réseau SDN

I.4 Contrôleur SDN

Le contrôleur SDN est responsable de la gestion du trafic transitant par le réseau, en communiquant avec les commutateurs SDN à l'aide de protocoles de contrôle. Il fournit également une interface permettant aux administrateurs réseau de programmer et de configurer le réseau.

I.4.1 Fonctionnalités du contrôleur SDN

Il s'agit d'un logiciel qui permet de contrôler le plan de contrôle du réseau et la configuration des périphériques réseau conformément aux politiques définies par l'administrateur réseau. Les fonctionnalités du contrôleur SDN incluent :

- **Gestion du plan de contrôle**

Le contrôleur SDN est responsable de la gestion du plan de contrôle du réseau. Il permet aux manager réseau de définir des règles et des politiques de routage pour le réseau.

- **Planification des périphériques réseau**

Les contrôleurs SDN permettent de programmer les périphériques réseau, tels que les commutateurs, les routeurs, les fire Walls, etc., pour qu'ils fonctionnent conformément aux règles définies par les ingénieurs.

- **Gestion de la topologie du réseau**

Le contrôleur SDN surveille la topologie du réseau et utilise ces informations pour prendre des décisions de routage et de commutation.

- **Gestion de la sécurité**

Les contrôleurs SDN peuvent être utilisés pour gérer la sécurité du réseau. Il permet aux administrateurs réseau de définir des règles de sécurité pour les périphériques réseau et de surveiller les activités suspectes sur le réseau.

- **Gestion des performances**

Les contrôleurs SDN peuvent être utilisés pour surveiller les performances du réseau. Il permet aux administrateurs réseau de détecter les goulots d'étranglement en temps réel et d'optimiser les performances du réseau.

- **Gestion des événements**

Les contrôleurs SDN peuvent être utilisés pour gérer les événements du réseau, tels que les pannes d'appareils, les changements de topologie, etc. Il permet aux administrateurs réseau de réagir rapidement aux événements réseau.

I.4.2 Les types de contrôleurs

Il existe plusieurs contrôleurs SDN, tel que :

- **OpenDaylight** : est un contrôleur SDN open-source largement adopté. Il est soutenu par un large écosystème de contributeurs et offre une grande flexibilité pour construire des réseaux SDN personnalisés. Il est extensible et prend en charge un large éventail de protocoles et de fonctionnalités.
- **ONOS (Open Network Operating System)** : est un autre contrôleur SDN open-source qui vise à fournir une plateforme évolutive et hautement disponible pour les réseaux SDN. Il offre des fonctionnalités avancées pour la gestion du réseau.
- **Ryu** : est un contrôleur SDN open-source développé en Python. Il est facile à utiliser et à personnaliser, offrant ainsi une grande flexibilité pour développer des applications réseau personnalisées.
- **Cisco Application Centric Infrastructure (ACI)** : ACI est une solution SDN de Cisco qui offre une approche centrée sur les applications pour la gestion et l'automatisation du réseau. Elle s'appuie sur le contrôleur APIC (Application Policy Infrastructure Controller) pour fournir des fonctionnalités avancées de gestion et de sécurité.
- **VMware NSX** : NSX est une solution SDN de VMware qui offre une virtualisation du réseau et une gestion centralisée pour les environnements virtualisés. Elle s'appuie sur le contrôleur NSX Manager pour fournir des fonctionnalités de mise en réseau avancées. [1]

I.5 Protocoles de communication dans un réseau SDN

Dans un réseau SDN, les protocoles de communication permettent aux composants du réseau de communiquer et de collaborer. Les protocoles les plus utilisés dans un réseau SDN sont les suivants :

I.5.1 OpenFlow

C'est le protocole de communication principal utilisé dans un réseau SDN. Il permet au contrôleur SDN de communiquer avec les commutateurs SDN pour configurer les tables de flux, les règles de routage, les groupes de traitement, etc.

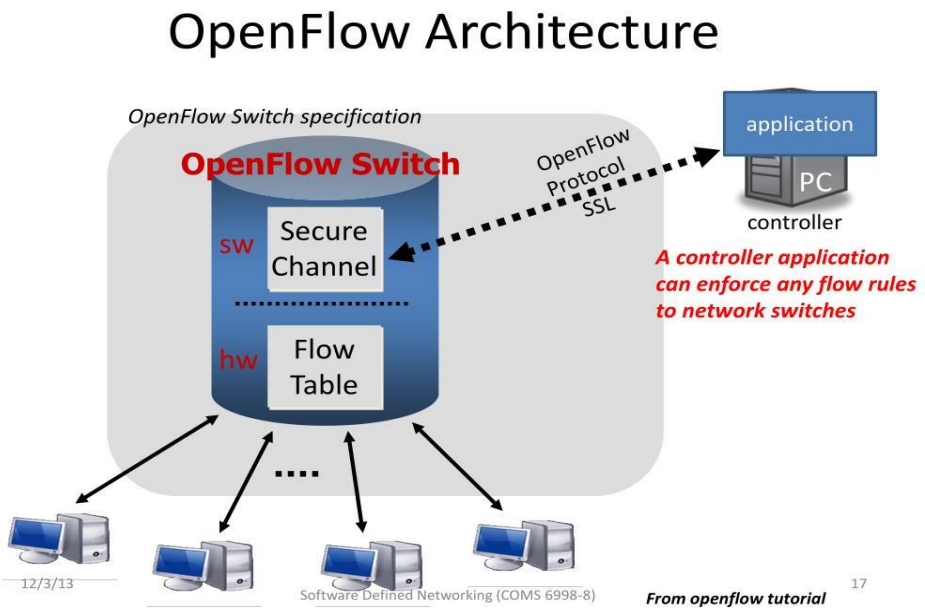

Figure I.4 Architecture OpenFlow

I.5.2 OVSDB

C'est un protocole de gestion de base de données utilisé pour la configuration et la gestion de commutateurs virtuels Open vSwitch (OVS).

I.5.3 NETCONF

C'est un protocole de gestion de configuration qui permet de configurer les équipements réseau à distance.

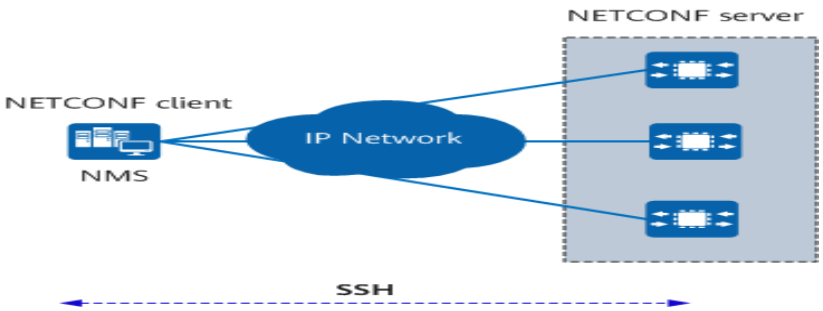

Figure I.5 Architecture de base du réseau NETCONF

I.5.4 RESTCONF

C'est un protocole de communication RESTful qui permet de configurer et de gérer des équipements réseau à l'aide d'API REST.

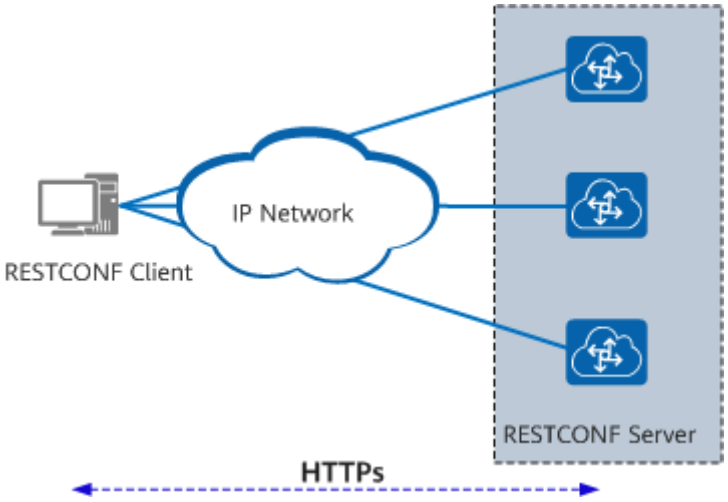

Figure I.6 Architecture du réseau RESTCONF

I.5.5 BGP-LS (Border Gateway Protocol - Link State)

C'est un protocole de routage qui permet de collecter des informations sur l'état du réseau, telles que les liens, les capacités, les contraintes, etc.

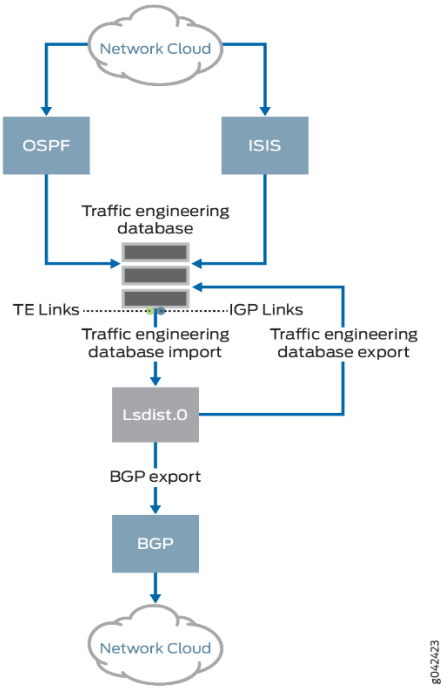

Figure I.7 Architecture BGP_LS

I.5.6 PCEP

Un protocole utilisé pour calculer les chemins de routage dans un réseau SDN.

I.5.7 P4Runtime

Un nouveau protocole qui permet aux contrôleurs SDN de configurer et de gérer des dispositifs P4 (Programming Protocol-Independent Packet Processors), qui sont des commutateurs programmables.

En utilisant ces protocoles, périphérique d'un réseau SDN peuvent communiquer de manière étroitement coordonnée, permettant une gestion et un contrôle centralisés du réseau.

I.6 Programmation et automatisation des réseaux SDN

Le principe de la programmation SDN c'est la création des applications personnalisées pour le contrôleur SDN qui manage le réseau. Généralement le but des applications c'est de crée des règles de flux de ceux qui définissent l'acheminement de trafic dans le réseau et cela peuvent être crée en utilisant des langages de programmation dédié, tel que P4(Programming Protocol-Independent Packet Processors).

La programmation d'un réseau SDN nécessite des connaissances approfondies des concepts fondamentaux de la programmation et les langages utilisé pour le programmer tels que python et java. De plus il faut savoir comment utiliser les API de programmation afin de communiquer avec le contrôleur SDN et pour la création des applications personnalisées sachant qu'il utilise à un API spécifique mais la plupart des contrôleurs SDN offrent des API standard tels que REST et gRPC.

L'automatisation de réseau SDN et une procédure nécessaire pour l'amélioration de l'efficacité et de la gestion de réseau informatique. Il utilise des logiciels pour permettre aux administrateur réseau de gérer le trafic, plutôt que d'avoir configurer chaque dispositif d'une manière individuelle et il permet aussi de manager les tâches répétitives et de surveiller les performances du réseau et l'optimisation de la configuration.

Les avantages de l'automatisation de SDN incluent :

I.6.1 Réduction des coûts

L'automatisation de SDN réduit les coûts en éliminant le besoin de personnel pour configurer les dispositifs individuellement. Les tâches répétitives sont automatisées, permettant aux administrateurs de se concentrer sur des tâches plus importantes.

I.6.2 Amélioration de la sécurité

L'automatisation de SDN peut améliorer la sécurité en permettant une réponse plus rapide aux menaces et en empêchant les erreurs de configuration. Les mises à jour de sécurité peuvent être rapidement appliquées à l'ensemble du réseau, réduisant ainsi les risques de failles de sécurité.

I.6.3 Optimisation des performances

L'automatisation de SDN peut optimiser les performances du réseau en permettant aux administrateurs de surveiller et de gérer la bande passante, les temps de réponse et les erreurs de paquets. Les configurations peuvent être rapidement ajustées pour améliorer les performances globales du réseau.

I.6.4 Flexibilité

L'automatisation de SDN permet une plus grande flexibilité dans la gestion des réseaux. Les configurations peuvent être facilement modifiées pour s'adapter aux changements des besoins de l'entreprise ou aux évolutions technologiques.

En résumé, La programmation et l'automatisation des réseaux SDN permettent de simplifier la gestion des réseaux, réduire les erreurs humaines et améliorer l'efficacité opérationnelle en utilisant des outils logiciels pour automatiser la configuration des commutateurs et la gestion du réseau.

I.7 SDN dans un Réseaux virtuels

Dans le contexte des réseaux virtuels, le SDN (Software Defined Networking) joue un rôle clé. Les réseaux virtuels sont des réseaux logiquement isolés qui peuvent être créés et gérés à l'aide de la technologie de virtualisation.

Le SDN simplifie et centralise la gestion des réseaux virtuels en séparant le plan de contrôle du plan de données. Cela signifie que la logique de contrôle et de gestion du réseau est déchargée sur un contrôleur SDN centralisé, tandis que les commutateurs ou les périphériques réseau exécutent les instructions du contrôleur pour transmettre les données.

Grâce au SDN, les réseaux virtuels peuvent être facilement créés, configurés et gérés de manière dynamique. Le contrôleur SDN permet de programmer des règles de flux et des politiques de sécurité par réseau virtuel, offrant une plus grande flexibilité et granularité de contrôle. Les réseaux virtuels basés sur SDN peuvent être configurés pour répondre aux besoins spécifiques des applications, des utilisateurs ou des groupes d'utilisateurs tout en maintenant une isolation et une sécurité adéquates.

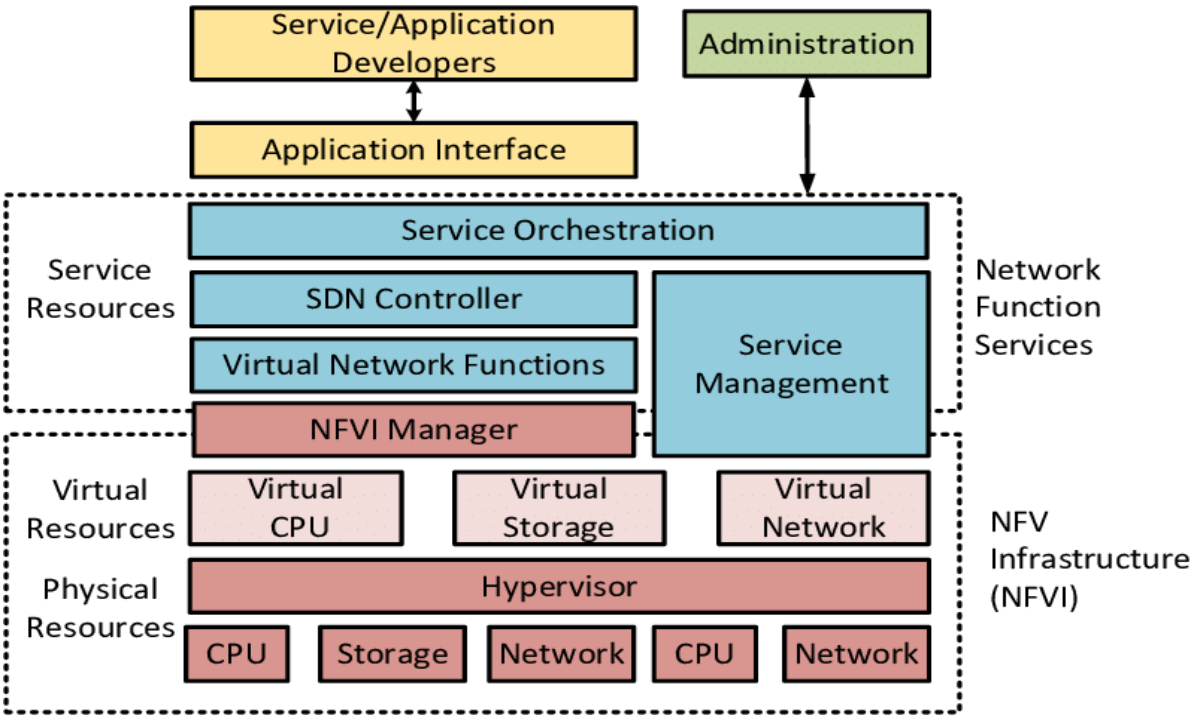

Figure I.8 SDN dans un Réseaux virtuels

I.8 Avantages et domaines d'utilisation des réseaux SDN

Les réseaux SDN (Software-Defined Networking) offrent plusieurs avantages et peuvent être utilisés dans différents domaines, notamment :

I.8.1 Datacenter

La mise en réseau SDN permet une gestion centralisée et dynamique des réseaux de centres de données. Cela améliore l'efficacité opérationnelle, réduit les coûts et permet une meilleure utilisation des ressources du réseau. Les centres de données peuvent également utiliser la mise en réseau SDN pour fournir une segmentation plus fine du réseau, une isolation de la charge de travail et une plus grande sécurité

I.8.2 Campus

La mise en réseau SDN peut être utilisée pour gérer les réseaux de campus en permettant une gestion centralisée des politiques de réseau. Cela permet une configuration réseau plus rapide et plus simple, une meilleure visibilité du réseau, une réduction des erreurs de configuration et une meilleure gestion de la qualité de service (QoS). Les réseaux SDN peuvent également faciliter la mobilité des utilisateurs et des appareils en permettant une gestion dynamique des adresses IP.

I.8.3 Fournisseurs de services

Les réseaux SDN peuvent être utilisés par les fournisseurs de services pour fournir des services de réseau dynamiques et adaptatifs, permettant le développement rapide de réseaux virtuels et l'extensibilité des services de réseau. Les réseaux SDN peuvent être utilisés par les fournisseurs de services pour assurer la virtualisation du réseau, la sécurité du réseau, le routage du réseau et le contrôle de la bande passante.

En somme, les réseaux SDN offrent une gestion centralisée et dynamique des réseaux, une sécurité renforcée, une meilleure efficacité opérationnelle et une flexibilité pour répondre aux besoins changeants des entreprises et des utilisateurs.

I.9 Défis de la mise en œuvre de réseau SDN

I.9.1 Fiabilité

La fiabilité joue un rôle majeur dans le développement d'un logiciel, Si une défaillance survient dans un système, ses utilisateurs doivent en être informés et la solution doit s'exécuter automatiquement.

La fiabilité d'un logiciel est la probabilité qu'il fonctionne Dans un environnement donné et pendant une durée déterminée de temps. La configuration du contrôleur SDN doit être intelligente Et valider la gestion du réseau afin d'accroître la disponibilité du réseau afin que les erreurs puissent être évitées et gérées. [2]

I.9.2 Évolutivité

Le réseau local traditionnel est déployé dans une architecture à plusieurs niveaux. Dans laquelle la fonctionnalité de routage de la couche 3 est utilisée pour connecter plusieurs réseaux de couche 2. Ces réseaux locaux traditionnels n'évoluent pas très bien lorsqu'ils prennent en charge le trafic est-ouest car au moins un dispositif de couche 3, et très probablement plusieurs

dispositifs de couche 3, se trouvent sur le chemin de bout en bout. Le réseau local traditionnel L'évolutivité est un attribut qui décrit la capacité d'un processus, d'un réseau, d'un logiciel ou d'une organisation à s'adapter à l'évolution du trafic. D'un processus, d'un réseau, d'un logiciel ou d'une organisation à se développer et à gérer une demande accrue. Un contrôleur SDN doit pouvoir prendre en charge un minimum de 100 commutateurs. Il doit également pouvoir atténuer l'impact de la surcharge de diffusion du réseau et de la prolifération des entrées de la table de flux [2]. La prolifération des entrées de la table de flux [2]. L'évolutivité est la Capacité d'un système, réseau ou processus à gérer et traiter une quantité croissante de travail, ou son potentiel d'expansion Pour faire face à cette croissance.

I.9.3 Performance et sécurité

Les interfaces ouvertes du réseau SDN Peuvent engendrer de nouveaux types d'attaques de réseau susceptibles de réduire les performances du réseau SDN. La sécurité dans l'informatique en nuage ' cloud computing ' est décrite et les différents problèmes et défis liés à la sécurité sont brièvement examinés par les auteurs [3].

Diverses attaques D-DOS peuvent perturber le fonctionnement des réseaux. Dans [4], les auteurs décrivent l'attaque SYN flood, qui peut mettre hors service le serveur d'une organisation en épuisant la file d'attente du serveur.

Serveur de toute organisation en épuisant la file d’attente du protocole TCP pour gérer et Résoudre ces problèmes, il faut développer un cadre SDN pour l'intégrité des logiciels.il convient de développer un cadre pour l'intégrité des logiciels, la gestion de l'accès à distance, la détection des menaces sur le réseau.

I.10 Aléas de sécurité dans les réseaux SDN

Les réseaux SDN peuvent présenter quelques aléas, tels que :

- Le trafic réseau peut être perturbé par des points d'accès ou des commutateurs, ce qui entraîne utilisateurs malveillants lancent des attaques par déni de service (DoS) qui peut entraîner une panne ou une perturbation du réseau.
- En raison de l'utilisation d'un contrôleur central, tout problème survenant dans le réseau entraîne la défaillance du contrôleur central. L'approche utilisée pour résoudre ce problème consiste à utiliser des distributions de contrôleurs horizontales ou hiérarchiques.

- SDN, comme le protocole OpenFlow, peut utiliser le protocole TLS pour sécuriser la communication du canal de contrôle des données. Cependant, il est souvent désactivé pour des raisons administratives et peut être vulnérable aux attaques de l'homme du milieu. Par conséquent, il n'est pas idéal pour la mise en œuvre de la sécurité des canaux.
- Faux flux de trafic fait référence à la génération de trafic malveillant ou non conforme aux spécifications du réseau, dans le but de perturber son fonctionnement normal. Cette attaque DoS peut entraîner une congestion du réseau, une dégradation des performances ou une saturation des ressources, affectant ainsi le bon fonctionnement du réseau.
- L'authenticité est une propriété essentielle pour assurer la confiance et la sécurité dans les réseaux. Si les dispositifs de transfert, tels que les commutateurs SDN, ne peuvent pas être authentifiés de manière fiable, cela peut entraîner des risques de sécurité et des perturbations dans les performances du réseau. Il est donc important de mettre en place des mécanismes d'authentification robustes pour garantir l'identité véritable des dispositifs dans un réseau SDN**.**

Conclusion

En conclusion, l'avenir de la mise en réseau SDN est brillant. Les avantages qu'ils offrent en termes de flexibilité, de gestion centralisée et de réduction des coûts sont de plus en plus recherchés par les entreprises et les prestataires de services.

Cependant, il reste encore des défis à relever, notamment en termes de fiabilité, d'évolutivité et de sécurité. Les fournisseurs de technologie SDN doivent s'efforcer d'améliorer la compatibilité et l'interopérabilité, ce qui peut également contribuer à augmenter le taux d'adoption de cette technologie.

En fin de compte, l'avenir de réseau SDN dépendra de la capacité des fournisseurs à répondre aux besoins organisationnels et à surmonter les défis de mise en œuvre, ainsi que l'adoption et de la demande du marché pour la technologie. Mais ce qui est certain, c'est qu'à l'avenir, les réseaux SDN continueront à jouer un rôle de plus en plus important dans l'infrastructure réseau des entreprises et des fournisseurs de services.

Chapitre II

Présentation des équipements Cisco

Introduction

Les équipements Cisco sont des dispositifs matériels et logiciels conçus et fabriqués par Cisco System, une entreprise de réseautage et de technologie de l'information. Cisco est l'un des leaders mondiaux des solutions réseau, offrant une large gamme d'équipements pour la construction, la sécurisation et la gestion des réseaux informatiques, l'équipement Cisco couvre le réseau local (LAN), le réseau étendu (WAN), le réseau sans fil, la sécurité du réseau, la collaboration, la vidéo, le centre de données, le service cloud et d'autres domaines différents. Ces appareils sont utilisés par de nombreuses entreprises et organisations à travers le monde pour construire et entretenir leur infrastructure réseau.

Dans ce chapitre, nous allons présenter une brève histoire de l'entreprise Cisco, ainsi que les différents équipements proposés par cette organisation. Nous aborderons également les certifications offertes par Cisco, ainsi que le support technique pour le dépannage.

II.1 Historique sur Cisco

L'histoire de la société Cisco a débuté en 1984 lorsque Leonard Bosack et Sandra Lerner, ont développé des routeurs et notamment le routeur multi protocoles que le couple d'informaticiens a inventés.

Le nom de l'entreprise est tiré de la ville où est implanté le siège social de la société : San Francisco. Cisco s'est développé au fil des années jusqu'à racheter plus de 80 start-up d'informatique. Malgré une baisse de ses actifs en 2001, l'entreprise a vu ses bénéfices augmenter de manière considérable de 2002 à 2010.

Les produits Cisco fonctionnent sous un système d'exploitation propriétaire : IOS. Les défenseurs du mouvement du logicielle libre négocient avec la firme depuis plusieurs années afin que celle-ci fournisse les codes source de leurs programmes aux clients conformément à la licence GPL. Un accord a finalement été trouvé en 2009 concernant les codes sources des produits Linksys.

Cisco a connu une période de licenciements en 2011, la société a réduit de 15 % son effectif et a cédé une de ses unités de production au Mexique à la firme Foxconn,2012 symbolise le retour de Cisco qui rachète l'équipementier de réseaux, américain Meraki. [W11]

II.2 Différents types d'équipements Cisco

Les appareils Cisco sont une partie essentielle des réseaux informatiques modernes, connectant les ordinateurs, les appareils et les utilisateurs dans les environnements d'entreprise et à grande échelle. Cisco est l'un des principaux fournisseurs mondiaux d'équipements de mise en réseau, offrant une gamme complète de produits de haute qualité, fiables et évolutifs. L'équipement Cisco est utilisé dans les entreprises, les universités, les centres de données et les fournisseurs de services pour fournir des solutions de mise en réseau supérieures. Les commutateurs, les routeurs, les points d'accès sans fil, les pare-feu et les serveurs Cisco sont parmi les appareils les plus couramment utilisés pour créer et entretenir des réseaux informatiques modernes. En utilisant l'équipement Cisco, les entreprises peuvent bénéficier d'un réseau fiable, sécurisé et évolutif pour répondre à leurs besoins commerciaux.

II.2.1 Commutateur

Un commutateur réseau est un équipement qui permet à deux appareils informatiques ou plus, tels que des ordinateurs, de communiquer entre eux. La connexion de plusieurs appareils informatiques crée un réseau de communication. Les ressources de calcul, d'impression, de serveur, de stockage de fichiers, d'accès Internet, en autres, peuvent être partagés sur le réseau.

Les appareils informatiques communiquent en échangeant des « paquets » de données sur le réseau. Les commutateurs de base transfèrent les paquets d'un périphérique à un autre, tandis que les opérations plus compliquées (telles que décider si un paquet est autorisé à atteindre sa destination prévue) sont traditionnellement du ressort d'autres types de périphériques réseau.

Les commutateurs existent en tant qu'appareils dédiés ou comme composant d'autres équipements, routeurs ou points d'accès sans fil (AP) par exemple, qui effectuent des opérations sur les paquets de données. La technologie classique de commutation existe depuis des décennies et constitue l'un des éléments fondamentaux de tous les réseaux informatiques modernes, y compris Internet. [W12]

II.2.1.1 Fonctionnement

Le commutateur établit et met à jour une table, dans le cas du commutateur pour un réseau Ethernet il s'agit de la table d’adresse mac, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC source des trames reçues

sur chaque port. Le commutateur construit donc dynamiquement une table qui associe numéro de port et adresses MAC.

Lorsqu'il reçoit une trame destinée à une adresse présente dans cette table, le commutateur renvoie la trame sur le port correspondant. Si le port de destination est le même que celui de l'émetteur, la trame n'est pas transmise. Si l'adresse du destinataire est inconnue dans la table, alors la trame est traitée comme un broadcast, c'est-à-dire qu'elle est transmise à tous les ports du commutateur à l'exception du port d'émission.

Un commutateur de niveau 2 est similaire à un concentrateur dans le sens où il fournit un seul domaine de diffusion. En revanche, chaque port a son propre domaine de collision. Le commutateur utilise la micro-segmentation pour diviser les domaines de collision, un par segment connecté. Ainsi, seules les interfaces réseau directement connectées par un lien point à point sollicitent le medium. Si le commutateur auquel il est connecté prend en charge le full-duplex, le domaine de collision est éliminé. [W13]

II.2.1.2 Différents types de switch

Il existe plusieurs types de commutateurs en informatique et en réseau. Voici les principaux :

- **Commutateurs de la série Catalyst :**

Les séries Catalyst de Cisco sont les plus courantes. Cela va des commutateurs d'entrée de gamme pour les petites entreprises aux commutateurs haut de gamme pour les grands centres de données. Les commutateurs Catalyst sont disponibles dans une variété de configurations, y compris les commutateurs de couche 2 et les commutateurs de couche 3.

Figure II.1 Commutateur catalyste

- **Commutateurs Nexus :**

La série Nexus de Cisco est conçue pour les grands centres de données et les réseaux de stockage. Ces commutateurs offrent des fonctionnalités avancées telles que la virtualisation du réseau et la haute disponibilité.

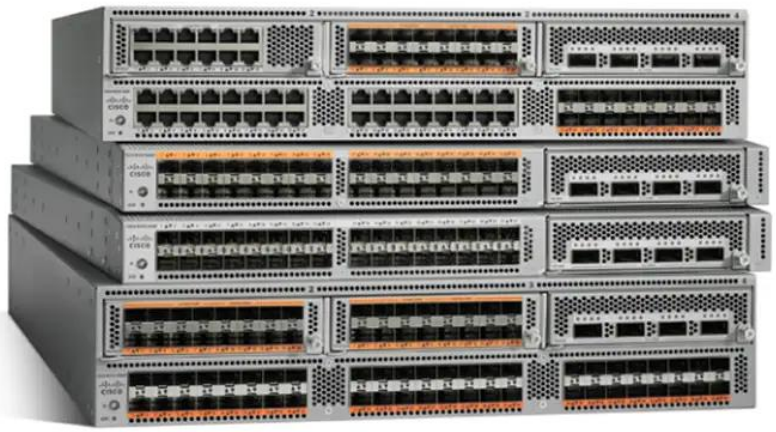

Figure II.2 Commutateurs Nexus

- **Commutateurs Meraki :**

Les commutateurs Meraki de Cisco sont des commutateurs gérés dans le cloud conçus pour les réseaux des petites et moyennes entreprises. Ils sont très faciles à installer et à gérer à distance depuis l'interface web.

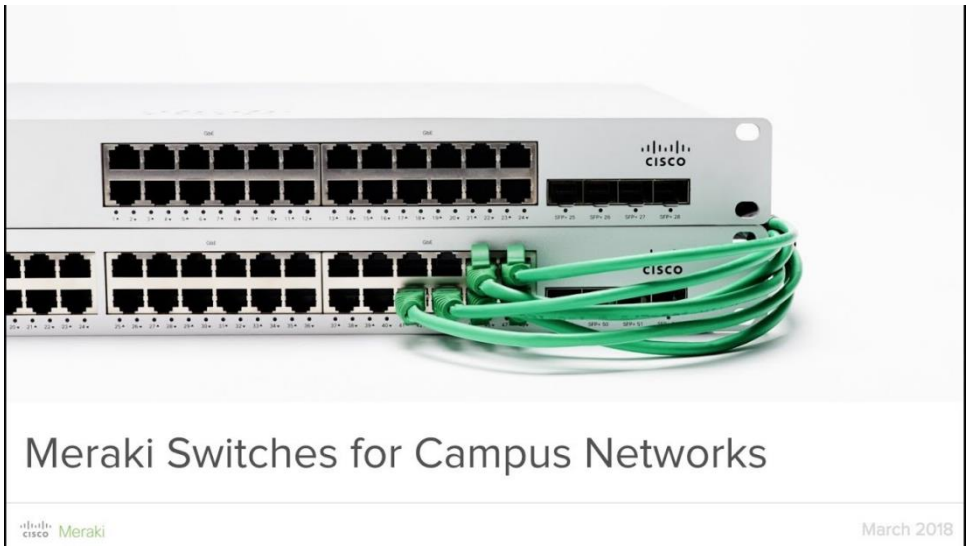

Figure II.3 Commutateurs Meraki

- **Commutateurs industriels :**

Cisco propose également une gamme de commutateurs industriels pour les environnements industriels difficiles tels que les usines, les centrales électriques et les mines. Ces interrupteurs sont conçus pour résister à des conditions extrêmes telles que les vibrations, les hautes températures et les environnements poussiéreux.

Figure II.4 Commutateurs industriels

- **Commutateurs de fournisseurs de services :**

Cisco propose également une gamme de commutateurs de fournisseurs de services pour fournir des services de connectivité haut débit aux clients. Ces commutateurs offrent des fonctionnalités de mise en réseau et de sécurité avancées pour répondre aux besoins des fournisseurs de services.

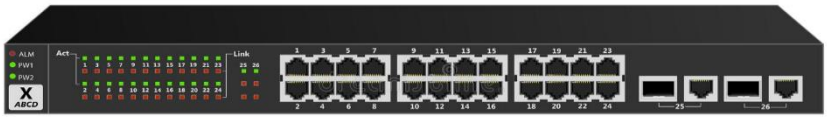

Figure II.5 Commutateurs de fournisseurs de services

II.2.2 Routeurs

Un routeur est un dispositif qui connecte deux ou plusieurs réseaux ou sous-réseaux pour la commutation de paquets. Il remplit deux fonctions principales : gérer le trafic sur ces réseaux en transférant les paquets de données aux adresses IP auxquelles ils sont destinés, et permettre à plusieurs appareils d'utiliser la même connexion internet.

Il existe plusieurs types de routeurs, mais la majorité d'entre eux transmettent des données entre les réseaux locaux (LAN) et les réseaux étendus (WAN). Un réseau local est un ensemble d'appareils connectés à une zone géographique spécifique. Un réseau local ne nécessite généralement qu'un seul routeur.

Figure II.6 Routeur Cisco CRS-1 (2004).

Un réseau étendu, en revanche, est un grand réseau réparti sur une vaste zone géographique. Les grandes organisations et les entreprises disposant de plusieurs sites à travers le pays, par exemple, ont besoin de ce type de réseau.

II.2.2.1 Fonctionnement

Imaginez un routeur comme un contrôleur aérien et les paquets de données comme des avions se dirigeant vers différents aéroports (ou réseaux). Tout comme chaque avion a une destination unique et suit un itinéraire unique, chaque paquet doit être guidé vers sa destination aussi efficacement que possible. De la même manière qu'un contrôleur du trafic aérien veille à ce que les avions atteignent leur destination sans se perdre ou subir une perturbation majeure en

cours de route, un routeur aide à diriger les paquets de données vers leur adresse IP de destination.

Afin de diriger efficacement les paquets, un routeur utilise une table de routage interne, c'est-à-dire une liste de chemins vers diverses destinations du réseau. Le routeur lit l'en-tête d'un paquet pour déterminer sa destination, puis consulte la table de routage pour trouver le chemin le plus efficace vers cette destination. Il transmet ensuite le paquet au réseau suivant sur le chemin.

II.2.2.2 Différents types de routeurs

Il existe différents types de routeurs, notamment :

- **Routeur sans fil :** Un routeur sans fil utilise un câble Ethernet pour se connecter à un modem. Il transmet des données en convertissant des paquets binaires de code en signaux radio, puis en les diffusant via des antennes. Les routeurs sans fil ne créent pas de réseaux locaux, mais créent plutôt des réseaux locaux sans fil qui connectent plusieurs appareils via une communication sans fil.

Figure II.7 Routeur sans fil

- **Routeur filaire :** Semblable à un routeur sans fil, un routeur filaire utilise également un câble Ethernet pour se connecter à un modem. Il utilise ensuite des câbles séparés

pour se connecter à un ou plusieurs appareils sur le réseau, créant un réseau local qui interconnecte les appareils sur le réseau et Internet.

Figure II.8 Routeur filaire

- **Routeur central :** Contrairement aux routeurs qui font partie d'un réseau local domestique ou de petite entreprise, un routeur central est utilisé par les grandes entreprises et les entreprises qui ont une grande quantité de données à transmettre sur leur réseau. Les routeurs centraux sont situés au "cœur" d'un réseau et ne communiquent pas avec les réseaux externes.

Figure II.9 Routeur central

- **Routeur périphérique :** contrairement à un routeur central, un routeur périphérique communique à la fois avec les routeurs centraux et les réseaux externes. Les routeurs

périphériques sont situés à la « limite » d'un réseau et utilisent le protocole BGP (Border Gateway Protocol) pour transmettre et recevoir des données d'autres LAN et WAN.

Figure II.10 Routeur périphérique

II.2.3 Point d'accès sans fil

Un point d'accès sans fil (WAP) est un périphérique réseau qui facilite la connexion d'appareils sans fil à un réseau câblé. Il est plus simple d'installer un site compatible WAP pour connecter tous les ordinateurs ou périphériques de votre réseau que d'utiliser des fils ou du câblage.

Figure II.11 D-Link wireless access point

II.2.3.1 Fonctionnement

Un point d'accès sans fil Cisco est un appareil qui facilite un réseau sans fil, en utilisant la technologie Wi-Fi. Il fonctionne comme un conduit entre les appareils compatibles Wi-Fi, tels que les ordinateurs portables, les smartphones et les tablettes, et le réseau filaire ou Internet.

Le point d'accès sans fil Cisco peut fonctionner comme un gestionnaire WLAN centralisé ou autonome, selon les besoins de l'entreprise. En tant que contrôleur du WLAN centralisé, il peut gérer plusieurs points d'accès sans fil pour fournir une couverture complète du réseau sans fil, tandis qu'en tant que point d'accès autonome, il peut être utilisé dans des espaces de petite à moyenne taille pour fournir une connectivité sans fil.

Les points d'accès sans fil Cisco ont des fonctionnalités avancées, notamment la capacité de gérer les utilisateurs, d'administrer les configurations réseau pour les invités, de fournir une QoS pour les applications critiques, d'avoir une connexion VPN et d'améliorer la sécurité.

II.2.4 Firewalls

Un firewall est un dispositif de sécurité qui permet de contrôler le trafic réseau entrant et sortant d'un réseau informatique. Il peut être matériel ou logiciel et conçu pour empêcher les accès non autorisés à un réseau, en bloquant les connexions non autorisées et en autorisant uniquement les connexions autorisées. [W25], [W26]

Les pare-feu Cisco offre une grande flexibilité et une évolutivité pour répondre aux besoins en constante évolution des réseaux d'entreprise [W25], [W26]

Ils permettent de limiter les coûts et la complexité de l'infrastructure avec une approche système et architecturale de la sécurité [W26]

Cisco est également reconnu pour son expertise en matière de sécurité informatique et propose de nombreuses solutions qualitatives pour améliorer la cyberdéfense des entreprises

II.2.4.1 Principaux avantages des pare-feu matériels

Les pare-feu matériels, déployés sous forme d'appareils physiques, présentent un certain nombre d'avantages par rapport aux pare-feu logiciels :

- **Sécurité cohérente :**

Les pare-feu logiciels installés sur différents ordinateurs peuvent tous être configurés différemment à moins qu'une organisation ne puisse mettre en œuvre et appliquer une configuration de sécurité cohérente, les pare-feu logiciels peuvent être désactivés où présenter des niveaux de sécurité variables. Un pare-feu matériel, en revanche, offre une protection cohérente à tous les dispositifs qu'il protège.

- **Protection autonome :**

Un pare-feu logiciel s'exécute généralement sur l'ordinateur protégé. Cela signifie qu'il occupe des ressources qui pourraient être utilisées à d'autres fins. Un pare-feu matériel fonctionne sur son propre matériel, ce qui signifie que l'augmentation du volume de trafic ou des exigences de sécurité n'a pas d'incidence sur les performances des machines protégées.

- **Gestion simplifiée :**

Avec un pare-feu logiciel, chaque ordinateur doit être configuré, géré et mis à jour individuellement pour assurer une protection efficace contre les cyber menaces. Un pare-feu matériel, en revanche, est une appliance unique qui protège l'ensemble du réseau. Toute mise à jour ou modification de configuration nécessaire peut être appliquée une seule fois et s'appliquera instantanément à tous les appareils protégés par le pare-feu.

- **Visibilité centralisée :**

L'utilisation de pare-feu logiciels indépendants sur chaque appareil du réseau d'une organisation signifie que l'équipe de sécurité ne dispose pas d'une visibilité complète du réseau ou doit déployer des efforts supplémentaires pour regrouper et assimiler les informations provenant de tous les appareils. Un pare-feu matériel centralise l'ensemble de la surveillance et de la journalisation du réseau dans un seul appareil.

II.3 Les certifications Cisco

La certification Cisco est une certification professionnelle délivrée par cette compagnie pour évaluer les capacités des professionnels de l'informatique dans les domaines de la mise en réseau, de la sécurité, des communications unifiées, des centres de données et du développement de logiciels.

Il y on a plusieurs niveaux de certification Cisco, du niveau débutant au niveau expert. Les niveaux de certification comprennent : [W27], [W28]

Cisco Certified Entry Networking Technician (CCENT) : Cette certification s'adresse aux débutants et évalue les compétences de base en réseautage.

Cisco Certified Network Associate (CCNA) : cette certification est destinée aux professionnels ayant une expérience réseau de base et évalue les compétences avancées en configuration réseau et en dépannage.

Cisco Certified Network Professional (CCNP) : cette certification s'adresse aux spécialistes ayant une expérience réseau avancée et évalue les compétences en matière de conception, de configuration et de gestion de réseaux.

Cisco Certified Internetwork Expert (CCIE) : conçue pour les professionnels des réseaux, cette certification évalue les compétences nécessaires pour concevoir, configurer, gérer et résoudre des problèmes de réseau complexes.

Cisco propose également des certifications spécialisées dans des domaines tels que la sécurité, les communications unifiées, les centres de données et le développement de logiciels. [W27], [W28]

Figure II.12 Certifications Cisco

II.4 Utilisation de l'interface utilisateur Cisco

L'interface utilisateur Cisco peut être servi pour gérer divers périphériques réseau Cisco comme les commutateurs, les routeurs et les pares-feux. Les utilisateurs peuvent accéder à l'interface utilisateur Cisco à travers la CLI (interface en ligne de commande) ou la GUI (interface graphique).

II.4.1 Interface en ligne de commande

La CLI une méthode pour interagir avec les équipements Cisco, elle permet aux administrateurs réseau de configurer et de gérer les appareils Cisco en entrant des commandes directement dans l'interface à l'aide d'un émulateur de terminal. Les commandes CLI peuvent être utilisées pour effectuer diverses tâches telles que la configuration d'interfaces réseau, l'ajout de routes, la configuration de protocoles de routage, la surveillance du trafic réseau et la résolution de problèmes.

Les CLI sont souvent privilégiées par les fonctionnaires réseau pour leur précision et leur automatisation. Les administrateurs peuvent créer des scripts pour automatiser les tâches répétitives ou effectuer des tâches complexes plus efficacement.

II.4.2 Interface graphique

La GUI est une méthode d'interaction avec le matériels Cisco, elle permet aux administrateurs réseau de configurer et de gérer les périphériques Cisco à l'aide d'icônes, de menus et de graphiques. Les administrateurs utilisent l'interface graphique pour effectuer différentes tâches telles que la configuration des interfaces réseau, l'ajout de VLAN, la création de règles de pare-feu et la surveillance du trafic réseau.

En raison de facilité l'utilisation de l'interface graphique et de la visualisation graphique des performances, elles sont souvent le premier choix des administrateurs sans expertise technique approfondie. L'interface graphique permet également aux administrateurs de visualiser rapidement les résultats de leurs actions en temps réel.

	Interface en ligne de commande (CLI)	Interface graphique (GUI)
Configuration	Permet une configuration précise et granulaire	Peut-être plus intuitive pour les utilisateurs novices
Surveillance	Permet une surveillance en temps réel et une collecte de données plus fine	Peut offrir une vue d'ensemble plus graphique et facile à comprendre
Gestion	Permet une gestion automatisée à grande échelle via des scripts et des programmes	Peut-être plus conviviale pour les tâches de gestion individuelles
Avantages	Permet une automatisation avancée et un contrôle précis de la configuration	Facilite la visualisation des performances et la gestion des tâches individuelles
Inconvénients	Peut être difficile à apprendre pour les utilisateurs novices	Peut-être moins précis et moins automatisable que la CLI

Tab II.1 comparaison entre les deux interfaces (CLI et GUI)

II.5 Configuration des équipements Cisco

La configuration des équipements Cisco est une tâche critique pour garantir le bon fonctionnement, la sécurité, la gestion et l'évolutivité du réseau. Voici quelques raisons pour lesquelles la configuration des équipements Cisco est importante : Opérations réseau, sécurité du réseau, gestion du réseau et évolutivité du réseau.

II.5.1 Comment accéder à la configuration d'un équipement

Pour accéder à la configuration de l'appareil Cisco, vous devez d'abord vous relier à l'appareil par une console série ou une connexion réseau. Voici les étapes générales pour entrer à la configuration de l'appareil.

II.5.1.1 Via une Console série

- Connectez le câble de la console série à l'appareil Cisco et à votre ordinateur. Vous pouvez utiliser un câble de console série et connecter une extrémité au port de console série de votre appareil Cisco et l'autre extrémité à un port série de votre ordinateur.
- Ouvrez un programme d'émulation de terminal sur votre ordinateur, tel que Putt ou Retâter.
- Configurez les paramètres de connexion de l'émulateur de terminal pour utiliser le port série auquel le câble de la console est connecté avec les paramètres appropriés pour la vitesse, les bits de données, la parité et les bits d'arrêt. Par défaut, ces paramètres sont généralement définis sur 9600 bauds, 8 bits de données, aucune parité et 1 bit d'arrêt.
- Allumez l'appareil Cisco.
- Lorsque vous y êtes invité, saisissez les informations d'identification requises pour entrer à la ligne de commande de l'Appliance. Par défaut, le nom d'utilisateur et le mot de passe sont tous deux "Cisco", mais il est recommandé de modifier ces renseignements pour des raisons de sécurité, Une fois connecté à la ligne de commande, vous pouvez saisir des commandes pour configurer le périphérique Cisco.

Il est important de noter que pour accéder à un appareil par la ligne de console, vous devez assurer que vous avez un accès physique à l'appareil et que vous y êtes connecté avec le câble de console série approprié. Cette méthode est particulièrement utile si vous devez accéder à votre appareil pour la première fois ou si vous devez effectuer une récupération à partir d'un appareil qui ne répond pas.

II.5.1.2 Via une connexion réseau

- Connectez-vous à l'appareil Cisco à partir d'un ordinateur ou d'un autre appareil connecté au même réseau que le périphérique.
- Configurez l'adresse IP sur l'interface de gestion des périphériques. Vous pouvez employer la commande "interface" pour accéder à l'interface de gestion, puis utiliser la commande "IP address" pour configurer l'adresse IP.
- Configurez un masque de sous-réseau adapté pour l'adresse IP.
- Configurez une passerelle par défaut pour permettre aux appareils Cisco de communiquer avec d'autres réseaux
- Mémorisez la configuration

- Sur votre ordinateur, utilisez un programme d'émulation de terminal pour vous connecter à l'appareil Cisco à l'aide de l'adresse IP de l'appareil. Vous pouvez utiliser un émulateur de terminal tel que PuTTY ou TeraTerm pour accéder à la ligne de commande de l'appareil.
- Entrez les informations d'identification nécessaire pour vous connecter à l'appareil. Par défaut, le nom d'utilisateur et le mot de passe sont tous deux "Cisco", mais il est conseillé de modifier ces informations pour des raisons de sécurité.

II.6 Dépannage des équipements Cisco

Le dépannage des équipements Cisco comprend le diagnostic et la résolution des problèmes opérationnels avec les équipements réseau Cisco tels que les routeurs, les commutateurs, les pares-feux, etc.

Il peut être effectué à distance ou sur site à l'aide d'outils tels que des consoles de gestion, des interfaces de ligne de commande (CLI), des logiciels de surveillance de réseau, des outils de simulation de réseau, etc. Les ingénieurs réseau utilisent des techniques et des outils pour résoudre ces problèmes.

II.6.2 Procédure de dépannage

Cette figure présente les six étapes de la procédure de dépannage.

Étape	Description
Étape 1. Identifier le problème	• La première étape de la procédure de dépannage. • Bien que les outils puissent être utilisés dans cette étape, une conversation avec l'utilisateur est souvent très utile.
Étape 2. Élaborer d'une théorie des causes probables	• Après que le problème est identifié, essayez d'établir une théorie de causes probables. • Cette étape donne souvent plus que quelques causes probables au problème.

Étape 3. Tester la théorie pour déterminer la cause	• Selon les causes probables, testez vos théories afin de dégager la véritable cause du problème. • Un technicien peut alors appliquer une rapide procédure et voir si cela permet de résoudre le problème. • Si une procédure rapide ne résoudre pas le problème, vous devrez peut-être effectuer des recherches complémentaires en vue de déterminer la cause exacte.
Étape 4. Établir un plan d'action pour résoudre le problème et implémenter la solution	• Après avoir déterminé la cause exacte du problème, établissez un plan d'action pour résoudre le problème et mettre en œuvre la solution.
Étape 5. Vérifier la solution et mettre en œuvre des mesures préventives	• Après avoir résolu le problème, vous devez vérifier le fonctionnement de l'ensemble. • Le cas échéant, mettre en œuvre des mesures préventives.
Étape 6. Documenter les résultats des recherches et des actions entreprises	• Au cours de la dernière étape du processus de dépannage, vous devez documenter les résultats de vos recherches ainsi que les actions entreprises. • Cette étape est très importante pour référence ultérieure.

Figure II.13 Procédures de dépannage.

Conclusion

En conclusion, les équipements Cisco sont nécessaires aux réseaux informatiques modernes. Ils connectent des ordinateurs, des appareils mobiles et des serveurs et fournissent des services de sécurité, de gestion et de surveillance pour le réseau. Cependant, pour garantir des performances optimales, il est important d'entretenir régulièrement cet équipement. Cela implique de suivre les consignes du fabricant, de surveiller les performances, de planifier les mises à jour et la maintenance préventive, et de sauvegarder régulièrement les configurations. En suivant ces meilleures pratiques, les appareils Cisco peuvent fournir aux organisations de toutes tailles une connectivité, une sécurité et une fiabilité réseau inégalées.

Chapitre III

CIS control

Introduction

Le Center for Internet Security (CIS) est une organisation à but non lucratif fondée. Leur mission est de fournir des outils et des ressources pour aider les associations à renforcer leurs systèmes d'information contre les cyber menaces. CIS est largement reconnu pour ses contrôles CIS, est un ensemble de bonnes pratiques et de lignes directrices développées par Center for Internet Security (CIS) pour aider les organisations à développer leur situation de sécurité informatique.

Les contrôles CIS sont un ensemble de 20 actions spécifiques, organisées en trois catégories, conçues pour aider les organisations à protéger leurs systèmes informatiques et leurs paramètres contre les menaces potentielles, à détecter les incidents de sécurité et à réagir efficacement aux incidents lorsqu'ils se produisent. Les trois catégories contrôlées par CIS sont : le Contrôle d'accès et authentification ; la Protection contre les logiciels malveillants ; et la Gestion continue des vulnérabilités. Les contrôles CIS sont régulièrement mis à jour pour refléter l'évolution des menaces et des technologies de sécurité. Ils sont largement utilisés comme référence pour évaluer et améliorer la sécurité informatique dans de nombreuses organisations à travers le monde. [5]

Figure III.1 Top 20 CIS control

III.1 Historique et évolution

Le CIS Control est fondée en 2000 par le Center for Internet Security à but non lucratif basé aux États-Unis. L'objectif majeur de CIS est de promouvoir la sécurité informatique et de fournir des ressources et des bons pratiques pour aider les associations à protéger leurs systèmes informatiques et leurs données contre les menaces potentielles.

CIS Control a été initialement développé en 2008 par une équipe d'experts en sécurité informatique dirigée par le Dr “Eric Cole”, sur la base d'une analyse approfondie des attaques informatiques courantes et des vulnérabilités les plus graves. Depuis lors, les contrôles CIS ont évolué et ont été mis à jour pour refléter l'évolution du paysage de la sécurité informatique et les menaces émergentes. [W32]

III.1.1 Etapes d'évolution de CIS control.

III.1.1.1 Développement initial des contrôles CIS : les contrôles CIS ont été initialement développés par le Center for Internet Security (CIS) en 2008 en tant que 20 contrôles de sécurité informatique conçus pour aider les organisations à se défendre contre les cyber menaces

III.1.1.2 Révisions et mises à jour régulières : Depuis sa création, CIS contrôles a subi plusieurs révisions et mises à jour pour s'adapter aux nouvelles menaces et amélioration technologiques. Les surveillances ont été révisés pour refléter les meilleures pratiques de sécurité et les vulnérabilités récemment découvertes.

III.1.1.3 Alignement avec d'autres normes et cadres de sécurité : CIS contrôles a été aligné sur d'autres normes et cadres de sécurité, tels que ISO/IEC 27001, NIST Cyber Security Framework et COBIT, pour simplifier leur intégration et leur adoption cohérente par les organisations.

III.1.1.4 Extension du nombre de contrôles : au fil du temps, le nombre de contrôles CIS a augmenté pour tenir compte des nouvelles menaces et des domaines émergents de la sécurité informatique. Par exemple, CIS contrôles v8 publié en 2020 contient 18 contrôles principaux et 5 contrôles de base.

III.1.1.5 Adoption croissante par les organisations : CIS contrôles est devenu un référentiel des meilleures pratiques largement adoptées par de nombreuses organisations à travers le monde pour optimiser leur posture de sécurité informatique et préserver leurs systèmes d'information.

III.2 Rôle de CIS control

Les contrôles CIS sont importants parce qu'ils minimisent le risque de violation de données, de fuite de données, de vol de propriété intellectuelle, d'espionnage d'entreprise, de perte de confidentialité, de déni de service et d'autres cyber menaces. Les contrôles CIS aident les entreprises à surveiller et à maintenir en permanence leurs cyberdéfenses, quel que soit le niveau d'alerte (faible, moyen ou élevé). Les contrôles CIS permettent d'aborder les points suivants :

- Les domaines critiques pour établir un programme de gestion des risques.
- Mesures défensives pour fournir la meilleure valeur.
- Suivi de la maturité du programme de gestion des risques.
- Cartographier les cadres réglementaires et de conformité des organisations.

III.2.1 Les domaines d'expertise de CIS

Les domaines d'expertise des contrôles CIS (Contrôles critiques de sécurité) sont :

III.2.1.1 Inventaire et contrôle des actifs

Cela implique de maintenir un inventaire à jour des actifs informatiques, de les surveiller et de les gérer de manière appropriée afin de minimiser les risques de sécurité.

III.2.1.2 Gestion de la configuration

Cela implique de développer des processus pour gérer la configuration de sécurité des systèmes et des applications, en gardant leurs configurations sécurisées à jours pour réduire les vulnérabilités.

III.2.1.3 Gestion des correctifs et des vulnérabilités

Cela implique une surveillance et une gestion proactives des correctifs de sécurité et des vulnérabilités connues afin de minimiser le risque d'exploitation.

III.2.1.4 Gestion des privilèges

Cela implique de limiter l'accès et les privilèges aux comptes utilisateur et système afin de minimiser le risque d'accès non autorisé.

III.2.1.5 Sécurisation des configurations de réseau

Cela implique la mise en place d'une configuration des réseaux sécurisée, y compris la segmentation du réseau, les pare-feu, les VPN et les configurations sans fil, pour protéger les données et les systèmes.

III.2.1.6 Surveillance continue

Cela implique la mise en place de systèmes de surveillance et de détection d'incidents pour détecter rapidement les actions suspectes et les incidents de sécurité et prendre des mesures pour les atténuer.

III.2.1.7 Protection anti-malware

Cela implique la mise en œuvre de mesures de protection anti-malware telles qu'un antivirus, un anti-spyware et un anti-malware pour protéger le système contre les attaques de logiciels malveillants.

III.2.1.8 Gestion des journaux de sécurité

Cela implique la collecte, la surveillance et l'analyse des journaux de sécurité pour détecter les activités suspectes et les incidents de sécurité.

III.2.1.9 Gestion de l'accès aux données

Cela concert des contrôles d'accès aux données appropriés pour protéger les données sensibles contre tout accès non autorisé.

III.2.1.10 Formation et sensibilisation à la sécurité

Il s'agit de former et d'éduquer les utilisateurs et les employés sur la sécurité informatique afin de minimiser le risque d'erreur humaine et d'attaques sociales. [W33]

III.3 Normes de CIS control

Les contrôles CIS sont alignés sur plusieurs normes et cadres de sécurité mondiaux reconnus, ce qui en fait une référence utile pour les associations qui essaient à améliorer leur posture de sécurité informatique et à se conformer à des normes et réglementations spécifiques. Cependant, les contrôles CIS ne sont pas des normes officielles, mais plutôt une globalité de meilleures pratiques développées par CIS pour aider les organisations à développer leur sécurité informatique. Voici quelques exemples de normes et de cadres de sécurité avec lesquels les CIS contrôlés sont généralement alignés :

- **ISO 27001** : Norme internationale pour les systèmes de gestion de la sécurité de l'information (SMSI), qui fonde un cadre pour la mise en œuvre d'un SMSI basé sur une approche de gestion des risques.
- **NIST Cyber sécurité Framework** : Un cadre de cyber sécurité développé par le National Institute of Standards and Technology (NIST) qui fournit des lignes directrices pour améliorer la cyber sécurité d'une organisation.
- **NIST SP 800-53** : Catalogue des contrôles de sécurité pour les systèmes et réseaux d'information, développé par le NIST, fournit des contrôles de sécurité pour la protection des données sensibles.
- **PCI DSS** : Payement Card Industry Data Security Standard, spécifie les exigences de protection des données des titulaires de cartes de paiement et de sécurisation de l'environnement de traitement des paiements.
- **HIPAA** : La loi sur la portabilité et la responsabilité en matière d'assurance maladie, qui définit les exigences de sécurité pour la protection des informations de santé protégées.
- **GDPR** : Règlement général sur la protection des données de l'Union européenne, qui définit les exigences en matière de protection des données personnelles des résidents de l'UE.

III.4 Dernière version des contrôles CIS

La dernière version de V8 a été lancée en 2018, améliorée par rapport à la version précédente (V7), alias le CIS Top 20. CIS Control V8 comporte les éléments suivants :

- Ensemble de 18 contrôles de cyberdéfense par rapport aux 20 contrôles précédents (recommandations).
- Groupe de mise en œuvre (IG) : Les IG sont divisés en trois groupes et constituent de nouvelles recommandations pour hiérarchiser la mise en œuvre des contrôles.
- La nouvelle version consolide les contrôles CIS en fonction des activités plutôt que de la personne qui gère les dispositifs.

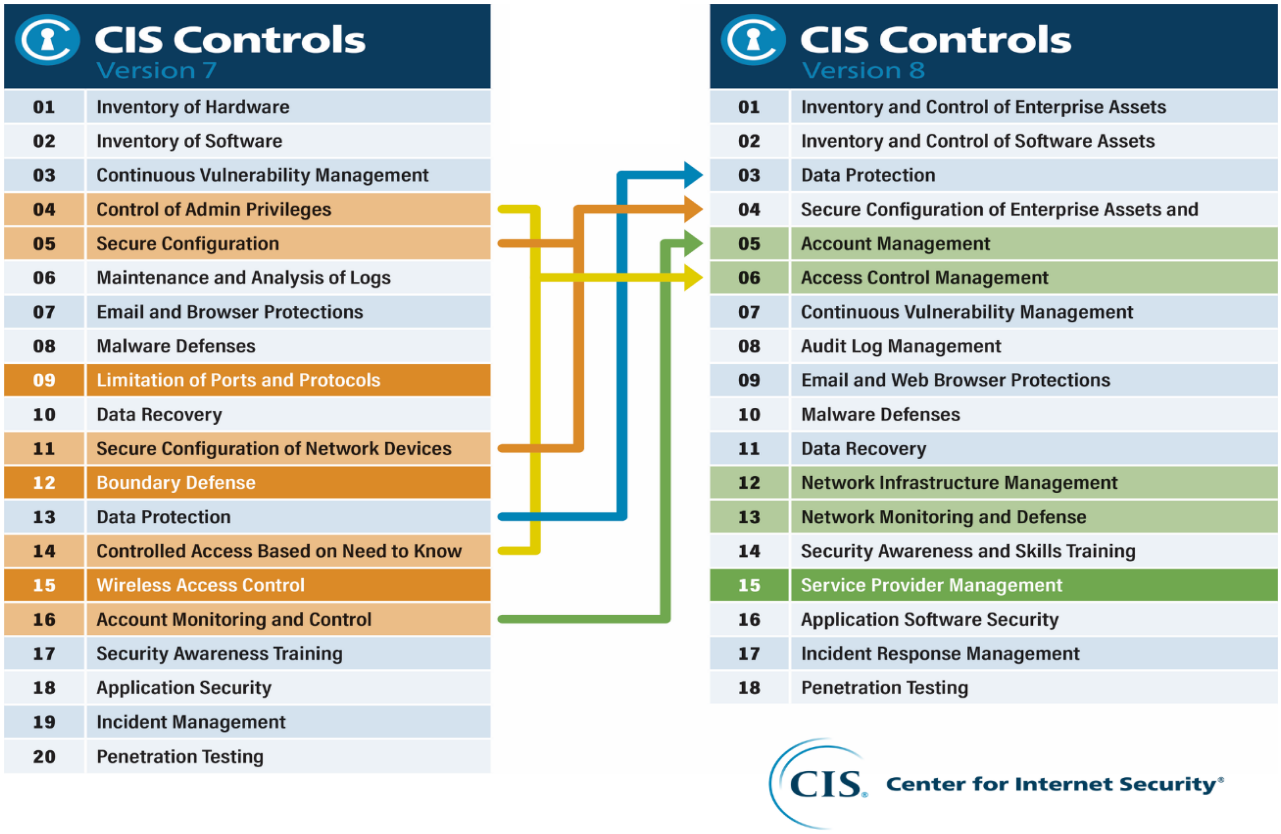

Figure III.2 Comparaison entre la version 7 et 8 de contrôle CIS

III.5 Avantages de l'utilisation des normes CIS

Les normes CIS présentent de nombreux avantages afin de renforcer la sécurité des systèmes d'information :

III.5.1 Standardisation

Les normes CIS garantissent une utilisation cohérente de certaines pratiques de sécurité courantes par les entreprises et les organisations.

III.5.2 Meilleures pratiques de sécurité

CIS fournit des conseils et des recommandations sur les meilleures pratiques de sécurité des systèmes d'information pour améliorer la sécurité et augmenter la résilience des systèmes attaqués.

III.5.3 Coûts réduits

Les mesures de sécurité recommandées par CIS peuvent réduire le coût de la protection de vos systèmes contre les cyberattaques.

III.5.4 Conformité

Les normes CEI sont souvent considérées comme des normes réglementaires, ce qui facilite la mise en conformité des entreprises et des organisations.

III.5.5 Facilité d'utilisation

Les normes CIS sont conçues pour être simples à utiliser par les entreprises et les organisations sans nécessiter de connaissances techniques avancées.

III.5.6 Amélioration constante

Les normes CIS sont continuellement affinées afin de maintenir leur pertinence face à l'évolution des menaces.

En fin de compte, l'utilisation des normes CIS peut améliorer considérablement la sécurité des systèmes d'information, diminuer le risque de cyberattaques et renforcer la résilience des entreprises et des organisations.

III.6 Comment les normes CIS control peuvent aider à renforcer la sécurité des équipements Cisco

Les normes CIS pour les contrôles sont un ensemble de mesures de sécurité créées par le Center for Internet Security (CIS) pour améliorer la sécurité des systèmes informatiques. Ces contrôles fournissent un ensemble de pratiques recommandées pour sécuriser le matériel Cisco, y compris les routeurs, les commutateurs, les pare-feu et les points d'accès sans fil.

Les normes CIS qui régissent le contrôle du matériel CIS peuvent aider à améliorer la sécurité du matériel Cisco en fournissant une base solide pour configurer la sécurité, surveiller les événements de sécurité, mettre à jour les correctifs et traiter les pannes. Information confidentielle. Les principaux avantages de l'utilisation de ces normes de sécurité sur les équipements Cisco incluent :

- **Détection des risques**

Les contrôles CIS fournissent une vue complète de la sécurité des appareils Cisco en reconnaissant les dangers et les menaces courants qui peuvent affecter le réseau. Cela vous permet de choisir les mesures de sécurité les plus efficaces pour contrer ces menaces.

- **Standardisation des pratiques**

Les contrôles CIS facilitent une approche cohérente de la sécurité sur les appareils Cisco, garantissant que tous les systèmes sont protégés de manière autonome et uniforme.

- **Priorisation des mesures de sécurité**

CIS contrôles classe les mesures de sécurité par importance, ce qui permet de concentrer les ressources sur les mesures les plus significatives.

- **Conformité réglementaire**

Les contrôles CIS sont de plus en plus pris en compte par les régulateurs lors de l'évaluation de la sécurité des périphériques du réseau et des périphériques. En utilisant les contrôles CIS pour protéger les équipements Cisco, les organisations peuvent améliorer le respect des réglementations de sécurité.

En somme, les CIS contrôles sont une méthode efficace pour renforcer la sécurité des équipements Cisco. En suivant ces normes, les organisations peuvent améliorer leur posture de sécurité, réduire les risques de cyber-attaque et garantir une conformité règlementaire accrue.-

III.7 CIS Benchmark pour CISCO

Les référentiels CIS sont un ensemble de lignes directrices et de bonnes pratiques pour la sécurisation des systèmes et réseaux informatiques. Il a été créé par le Center for Internet Security (CIS) et est utilisé par les associations (Cisco, Mozilla, Google et Oracle...etc.) pour améliorer leur posture de sécurité.

CIS Benchmark fournit un ensemble complet de recommandations de sécurité pour différents systèmes et plates-formes, y compris les systèmes d'exploitation, les bases de données, les serveurs Web, etc. Les conseils couvrent un certain nombre de contrôles de sécurité, y compris les stratégi0es de mot de passe, le renforcement du système, la sécurité du réseau et la configuration logicielle.

En suivant les lignes directrices de base du CIS, les organisations peuvent contribuer à réduire le risque de cyberattaques et à développer leur posture de sécurité globale. CIS fournit également plusieurs outils et ressources pour aider les organisations à mettre en œuvre les conseils, notamment des outils d'évaluation de la configuration, des outils d'automatisation de la sécurité et des programmes de formation.

Cisco utilise le CIS Benchmark pour établir des normes de sécurité pour ses produits et services. Le guide de référence CIS aide les entreprises à protéger leur infrastructure réseau en réduisant le risque de failles de sécurité. Cisco fournit des directives de configuration et des recommandations de sécurité pour de nombreux produits et plates-formes basées sur les directives de base CIS.

Par exemple, Cisco fournit des guides de configuration basés sur CIS Benchmark pour ses commutateurs, routeurs, pare-feu, serveurs et autres produits. Ces guides offrent des consigne étape par étape pour configurer les paramètres de sécurité, renforcer le système et se protéger contre les menaces courantes. En suivant les directives de base CIS de Cisco, les organisations peuvent améliorer la sécurité et diminuer le risque de cyberattaques.

Aussi des conseils de configuration basés sur le CIS Benchmark, Cisco fournit des outils et des techniques pour aider les organisations à mettre en œuvre des mesures de sécurité efficaces. Ces outils comprennent des produits de sécurité tels que Cisco Identity Services Engine (ISE), qui fournit des solutions de gestion des identités et des accès basés sur les rôles, et des solutions de sécurité réseau telles que Cisco Fire power Next-Generation Firewall, qui offrent une protection avancée contre les menaces. [W35]

III.8 Différence entre un équipement Cisco configuré avec ou sans CIS control

La principale distinction entre les équipements Cisco configurés avec ou sans CIS Control est le degré de sécurité qu'ils offrent. Le matériel Cisco configuré avec les normes et recommandations de sécurité CIS Control sera configuré pour suivre les meilleures pratiques de sécurité et protéger les réseaux et les données contre les dommages, contrairement les équipements Cisco qui ne sont pas configurés selon les recommandations de sécurité du CIS Control peuvent présenter des problèmes de sécurité, tels que des failles de sécurité ou des failles pouvant être exploitées par des attaquants.

Dans l'ensemble, le respect des normes de sécurité CIS et des recommandations concernant la configuration des équipements Cisco peut améliorer la sécurité du réseau et des données, ce qui conduira à un plus grand degré de protection contre les cyberattaques.

Conclusion

En conclusion, CIS Contrôle apporte une valeur ajoutée importante dans la sécurité des équipements. Grâce à son expertise technique, son expérience et son professionnalisme, CIS Contrôle est en mesure de garantir que les équipements sont conformes aux normes de sécurité en vigueur. En effectuant des contrôles réguliers et des audits de sécurité, CIS Contrôle contribue à réduire les risques d'accidents, à améliorer la fiabilité des équipements et à assurer la sécurité des travailleurs. De plus, en choisissant CIS Contrôle comme partenaire de confiance pour la sécurité de leurs équipements, les entreprises peuvent se concentrer sur leur cœur de métier en toute tranquillité d'esprit. En somme, CIS Contrôle est un acteur clé dans le domaine de la sécurité des équipements, offrant une valeur ajoutée considérable aux entreprises et aux travailleurs.

Chapitre IV

Développement de la solution d'automatisation

Introduction

Dans un réseau informatique, la gestion et la maintenance des périphériques peuvent être fastidieuses et compliqué, en particulier lors de la gestion d'un grand nombre de périphériques ou du maintien de configurations cohérentes et conformes à la sécurité. L'équipement réseau Cisco est largement utilisé dans les entreprises et les organisations pour garantir la connectivité et la sécurité du réseau.

Le Center for Internet Security (CIS) procure des normes de sécurité internationalement pour de multiples technologies, y compris les équipements de réseau Cisco. Les recommandations du CIS incluent des conseils sur les paramètres de sécurité à appliquer, les protocoles à utiliser, les configurations à éviter et d'autres fonctionnalités de sécurité pour protéger votre réseau contre les menaces potentielles.

Un outil d'automatisation (CIS Benchmark) développé pour la configuration des périphériques réseau Cisco permettra aux administrateurs réseau de vérifier et de faire en sorte que les périphériques Cisco soient conformes aux recommandations CIS de manière efficace et efficiente. L'outil sera capable de détecter les non-conformités, de proposer des actions correctives et de les appliquer automatiquement. De plus, cela contribuera à garantir que les configurations de sécurité restent uniformes et cohérentes sur l'ensemble du réseau, réduisant ainsi le risque de failles de sécurité.

IV.1 Présentation des différents CIS Benchmarks utilisés par Cisco

Cisco est un fournisseur mondial de solutions de réseaux et de technologies de l'information. Dans le cadre de ses offres de sécurité, Cisco utilise les Benchmarks CIS pour évaluer et améliorer la sécurité des systèmes d'exploitation et des périphériques réseau. Les référentiels CIS sont des normes de sécurité développées par le Center for Internet Security (CIS) pour diverses plates-formes et applications. [W36]

Voici un aperçu de quelques différents benchmarks CIS utilisés par Cisco :

IV.1.1 CIS Cisco IOS Router Benchmark

Ce benchmark fournit des recommandations de sécurité pour les routeurs Cisco exécutant le système d'exploitation Cisco IOS. Il couvre un large éventail de paramètres de sécurité tels que l'authentification, les services réseau, les protocoles de routage, les pares-feux, la gestion des journaux, etc.

IV.1.2 CIS Cisco ASA Firewall Benchmark

Ce benchmark se concentre sur les pare-feu Cisco Adaptive Security Appliance (ASA) et fournit des recommandations de sécurité pour la configuration et la gestion de ces appliances. Il couvre l'authentification, le contrôle d'accès, les services de sécurité, les journaux et les alertes et la gestion des correctifs etc.

IV.1.3 CIS Cisco Catalyst Switch Benchmark

Ce benchmark s'applique aux commutateurs Cisco Catalyst et fournit des recommandations pour la sécurisation de ces appareils. Il couvre les paramètres d'authentification, les services de sécurité, les protocoles de gestion, la surveillance, la gestion des correctifs, etc.

IV.1.4 CIS Cisco Wireless LAN Controller Benchmark

Ce benchmark est spécifique aux contrôleurs Cisco Wireless LAN (WLAN). Il fournit des recommandations de sécurité pour la configuration et la gestion des contrôleurs WLAN afin d'améliorer la sécurité du réseau sans fil. Couvre l'authentification, le chiffrement, la gestion des politiques, la surveillance, etc.

IV.1.5 CIS Cisco Email Security Appliance Benchmark

Ce benchmark concerne les appliances Cisco Email Security. Il fournit des recommandations pour la configuration et la gestion de ces périphériques afin d'améliorer la sécurité des communications par e-mail. Il couvre l'authentification, le filtrage des e-mails, la gestion des journaux, la protection contre les logiciels malveillants, etc.

Ces benchmarks Cisco CIS sont conçus pour aider les administrateurs réseau à renforcer la sécurité de leur infrastructure Cisco. Ils fournissent des recommandations détaillées sur la configuration et la gestion des appareils afin de réduire les vulnérabilités et de protéger les réseaux contre les menaces.

IV.2 La maquette du réseau

Le périmètre de stage consiste à créer une maquette virtuelle avec EVE-NG contenant un système d’information doté de ressources variées (Actifs informatiques). Plutôt que de travailler avec des équipements réels, cette méthode nous a permis de simuler un environnement réseau complet avec des équipements virtuels pour estimer le coût, plus de flexibilité, plus sécurisé.

IV.2.1 EVE-NG VM

EVE-NG (Emulated Virtual Environment - Next Generation) est une plateforme de virtualisation réseau open-source populaire utilisée pour créer des environnements de laboratoire virtuels pour les tests, la formation et la simulation de réseaux. EVE-NG permet aux utilisateurs de déployer des machines virtuelles (VM) et de les interconnecter pour simuler des topologies réseau complexes.

Il fournit une interface Web conviviale qui permet aux utilisateurs de concevoir, configurer et gérer des réseaux virtuels à l'aide de divers nœuds de réseau préconfigurés tels que des routeurs, des commutateurs, des pares-feux, des serveurs et d'autres périphériques réseau. Il prend en charge une large gamme de systèmes d'exploitation réseau populaires, notamment Cisco IOS, Juniper Junos, VyOS, Palo Alto PAN-OS, Fortinet FortiOS, etc.

IV.3 Les outils de développement

IV.3.1 Langage de programmation

- **Python**

Python est un langage de programmation créé en 1991. Contrairement à d'autres langages comme Java ou C++ (qui sont compilés), Python est lui un langage interprété, ce qui signifie que les instructions tapées sont transcrites en binaire au fur et à mesure de leur lecture Il a l'avantage d'être assez facile à comprendre et à apprendre, tout en restant puissant et adapté pour des projets importants, ce qui fait donc de lui le langage de programmation idéale pour les débutants.
Python est également apprécié pour sa vaste bibliothèque standard, qui comprend un large éventail de modules et d'outils pour effectuer une variété de tâches, allant de la manipulation de chaînes de caractères à la gestion de fichiers, en passant par le développement Web et l'analyse de données. De plus, la communauté Python est très active et offre de nombreuses bibliothèques tierces spécialisées dans divers domaines, ce qui facilite l'extension des fonctionnalités de base du langage. [W37]

Bibliothèque Python

- **Netmiko :**

Dans le code que nous avons fourni, la bibliothèque Netmiko est utilisée pour effectuer les opérations suivantes :

- Lecture du fichier XML contenant les configurations récupérées
- Remplacement des configurations non conformes
- Affichage des configurations corrigées
- Écriture des configurations corrigées dans un nouveau fichier

- **xml.etree. ElementTree**

Cette bibliothèque est utilisée pour analyser et traiter des fichiers XML. Elle est utilisée pour parcourir la structure XML des bonnes pratiques et extraire les informations nécessaires.

IV.4 Environnement logiciel

IV.4.1 VMware WorkStation Pro

VMware Workstation est un logiciel de machine virtuelle utilisé sur les ordinateurs x86 et x86-64 pour exécuter plusieurs systèmes d'exploitation sur un seul ordinateur hôte physique. Chaque machine virtuelle peut exécuter simultanément une seule instance de n'importe quel système d'exploitation (Microsoft, Linux, etc.). VMware Workstation prend fortement en charge la compatibilité matérielle et fonctionne comme un pont entre l'hôte et la machine virtuelle pour tous les types de ressources matérielles, y compris les disques durs, les périphériques USB et les CD-ROM. Tous les pilotes de périphériques sont installés via la machine hôte. [W38]

IV.4.2 WinSCP

WinSCP (Windows Secure Copy) est un client de transfert de fichiers graphique open source permettant de se connecter à des serveurs distants et de transférer des fichiers à l'aide des protocoles SSH, SFTP, SCP et FTP. Il est spécialement conçu pour le système d'exploitation Windows.

Il fournit une interface graphique facile à utiliser qui permet aux utilisateurs de se connecter à des serveurs distants, de parcourir leurs systèmes de fichiers, de copier des fichiers entre l'ordinateur local et des serveurs distants, de supprimer, renommer et modifier des fichiers, de créer et de gérer des répertoires et d'effectuer divers genres d'opération gestion de fichiers.

Il est populaire parmi les administrateurs système, les développeurs et les utilisateurs expérimentés car il offre une alternative conviviale à la ligne de commande traditionnelle pour le transfert sécurisé de fichiers.

IV.4.3 PuTTY

PuTTY est un client de terminal gratuit, légère et open source qui est utilisé pour communiquer avec des serveurs distants via SSH, Telnet, rlogin et SCP. Il est principalement utilisé sur les systèmes d'exploitation Windows, bien que d'autres versions soient également disponibles.

Il fournit une interface simple et efficace pour se connecter à des serveurs distants via des protocoles de communication sécurisés. Il facilite l'établissement d'une session permanente avec une connexion (comme les ports, les protocoles, etc.), ainsi que d'autres fonctionnalités.

PuTTY facilite des fonctionnalités supplémentaires telles que la gestion des sessions, la gestion des clés pour le chiffrement (clés SSH), la configuration des préférences d'utilisation du terminal, la configuration des options de connexion et de nombreuses autres fonctionnalités.

IV.4.4 Visual Studio Code

C'est un éditeur de code source léger, mais puissant qui est disponible sur Windows, MacOs et Linux. Il est livré avec une prise en charge intégrée de JavaScript, Type script et Node.js. Il dispose d'un écosystème d'extensions riche pour d'autres langages (tels que C++, Java, Python, PHP) et des environnements d'exécution (tels que .NET et Unity).

IV.5 Etapes d'installation et de configuration

1. Installation de la machine virtuelle pour exécuter EVE-NG.

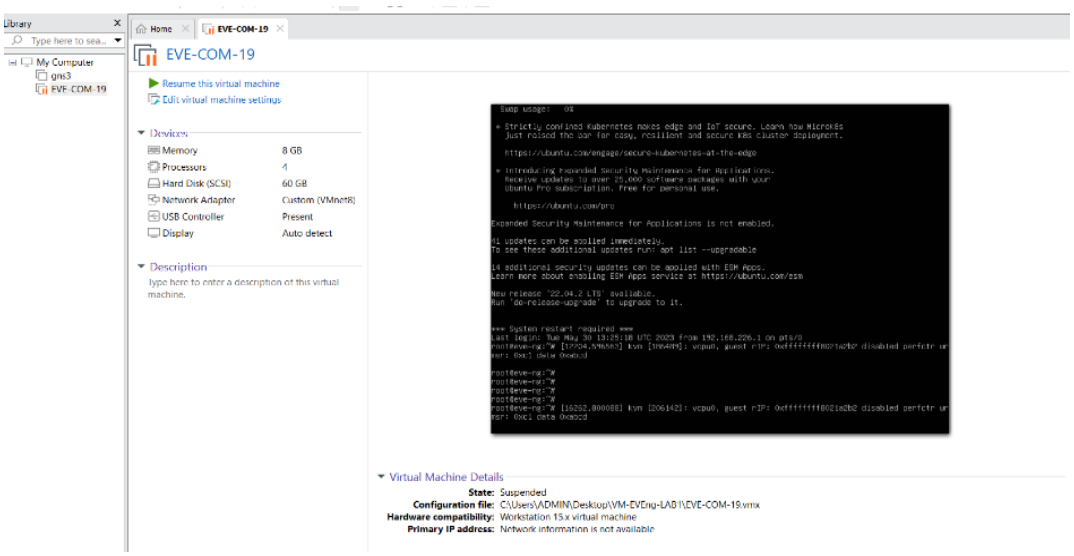

Figure IV.1 La façade de VMware Workstation pro

2.Editer la machine virtuelle pour assurer le bon fonctionnement

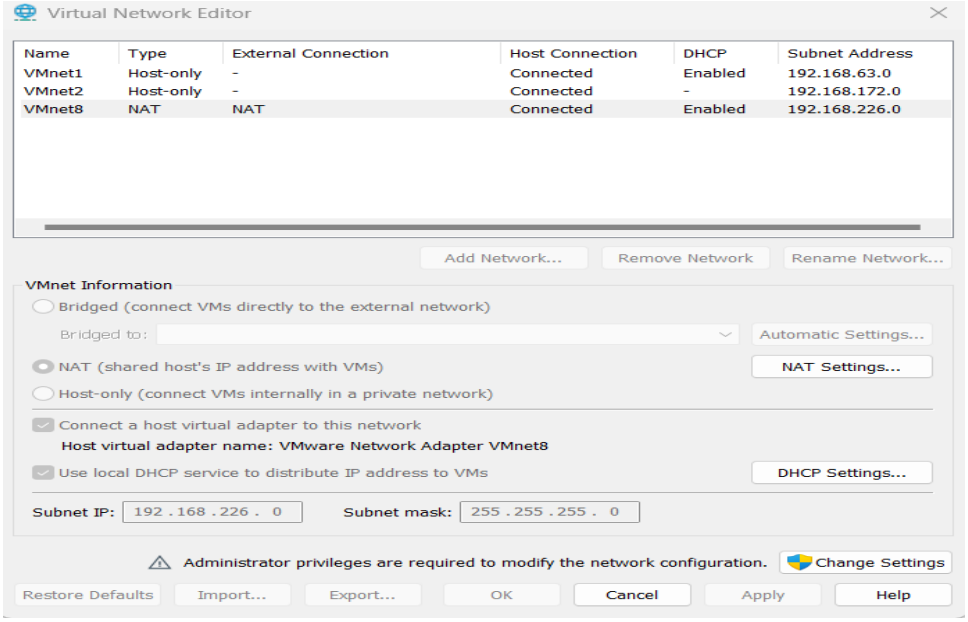

Figure IV.2 Virtuel network editor

3. Nous commençons le programme et obtenons l'adresse IP nécessaire pour la connexion.

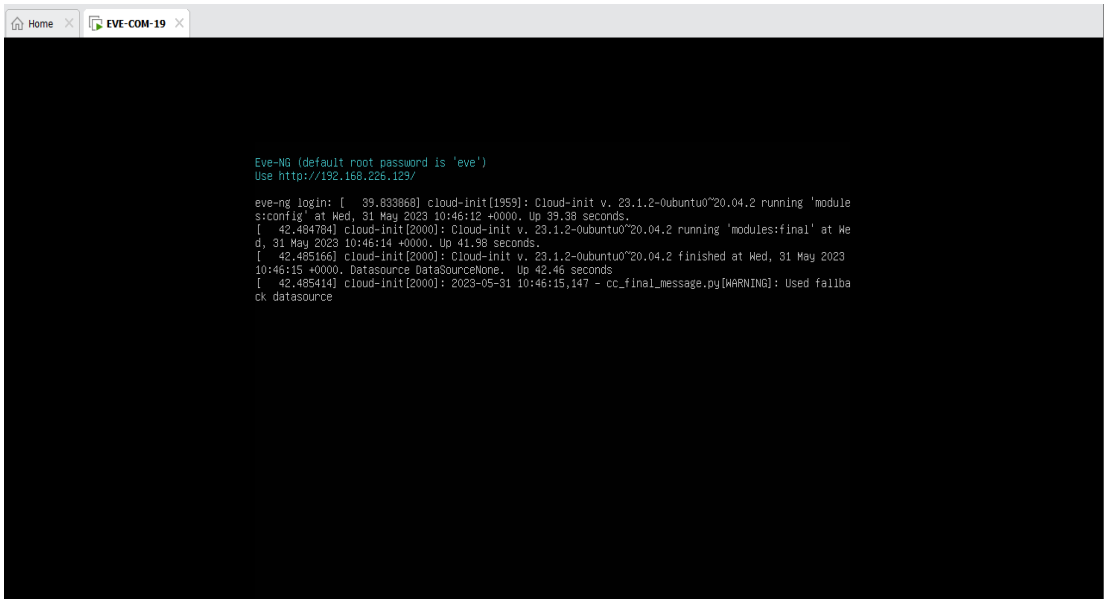

Figure IV.3 EVE-NG

4. Nous avons accédé au site en utilisant son adresse IP et on s'est connecté en tant qu'utilisateur "root" avec le mot de passe "eve". Cette procédure nous a permis d'établir une connexion sécurisée avec le site et d'interagir avec ses fonctionnalités en tant qu'utilisateur autorisé.

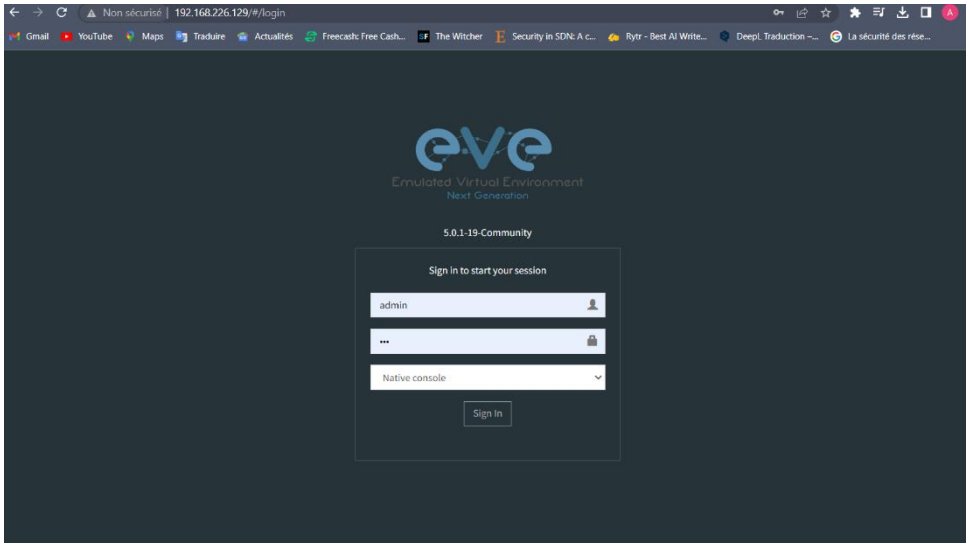

Figure IV.4 Accès à l'interface de EVE-NG

5. La configuration de WinSCP permet de faciliter le transfert de fichiers entre une machine virtuelle et un PC. Cela permet de déplacer les fichiers de manière pratique et facile en utilisant une interface conviviale.

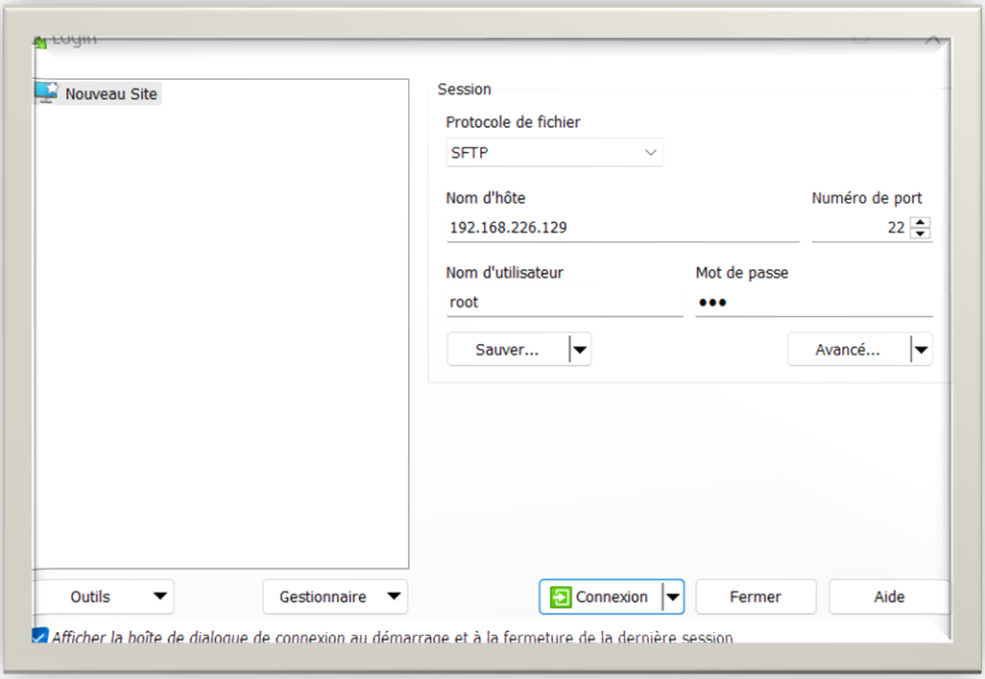

Figure IV.5 Connecter WINSCP avec la machine

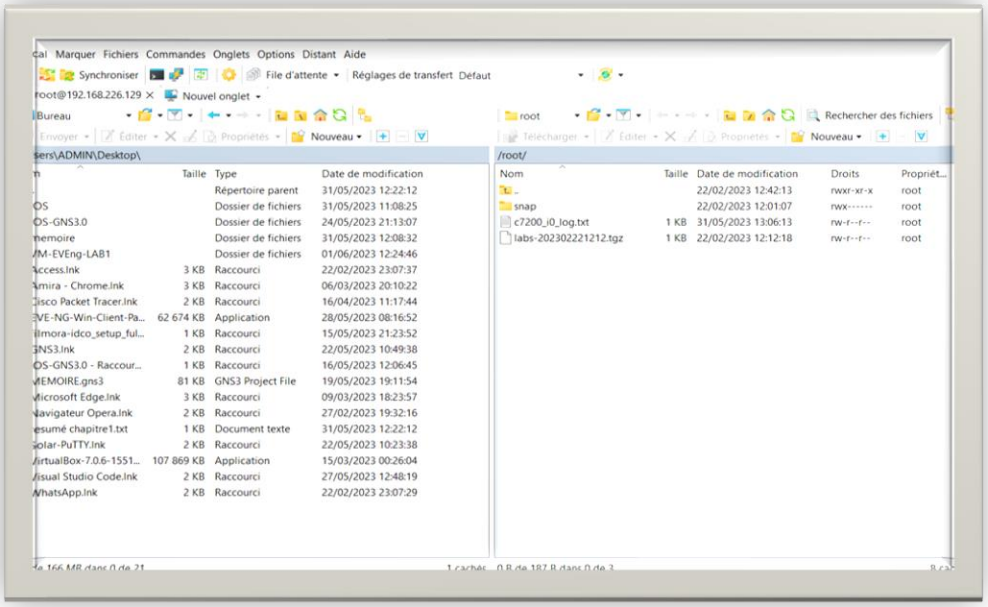

Figure IV.6 Transfert des fichiers entre la machine et le pc

6. L'utilisation de l'outil PuTTY permet de faciliter la connexion à une machine à distance dans le but de simplifier son utilisation.

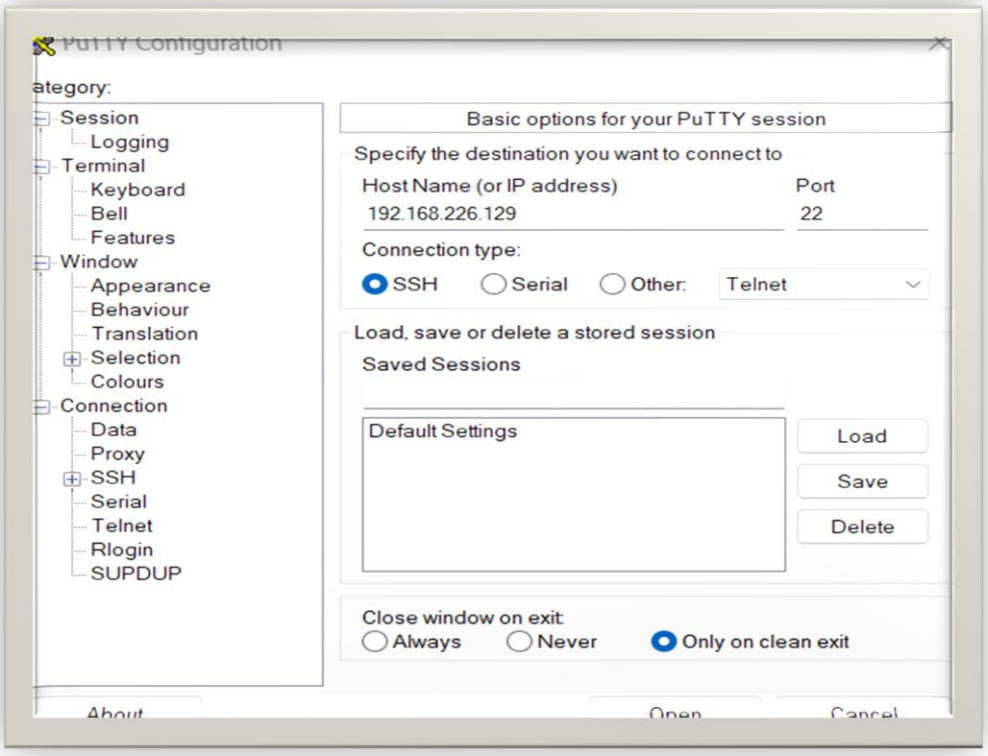

Figure IV.7 L'interface de l'émulateur Putty

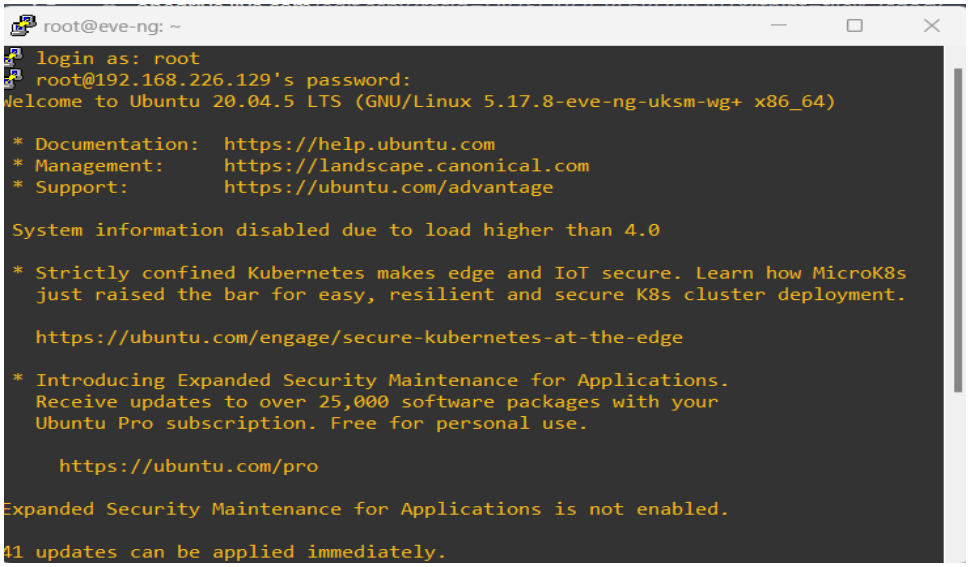

Figure IV.8 Connecter PUTTY avec la machine

IV.6 Architecture d'un réseau

- Pour garantir une connectivité réseau efficace, nous avons réalisé une architecture d'entreprise basique comprend généralement la mise en place d'un réseau LAN (Local Area Network).
- Nous avons configuré les équipements en introduisant délibérément des erreurs pour permettre à l'outil de les détecter.

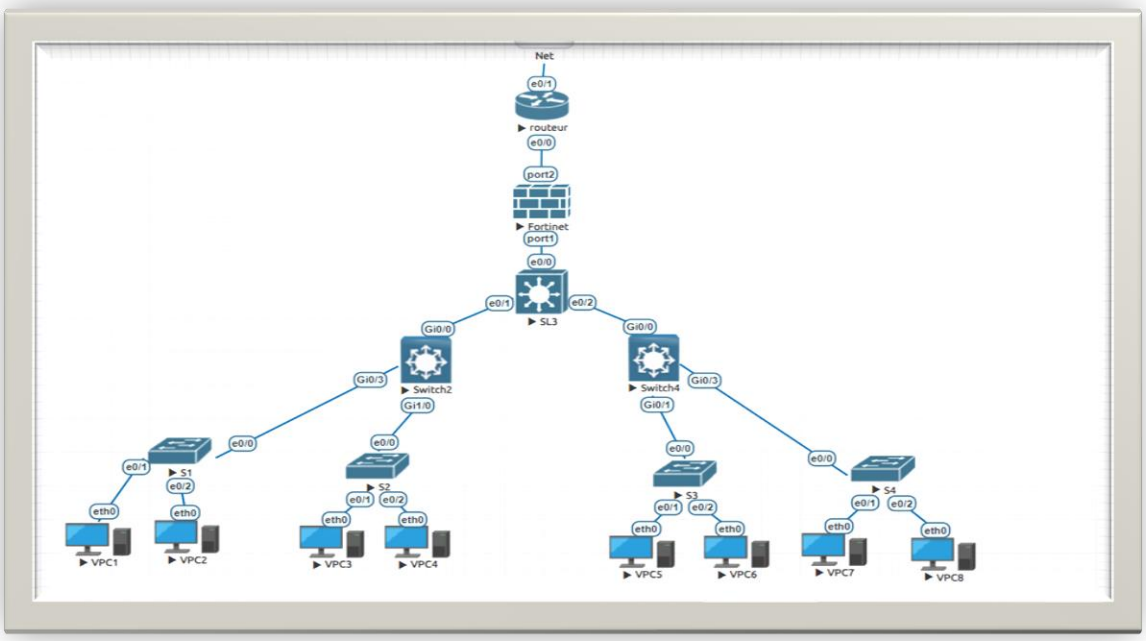

Figure IV.9 Architecture de l'entreprise

IV.7 Simulation et test des différents scénarios et commandes

- Nous avons réussi à crier ce code en utilisant le langage Python avec l'IDE VS Code

```python
import xml.etree.ElementTree as ET
import netmiko

# Chemin vers votre fichier XML contenant les bonnes pratiques
fichier_xml_bonnes_pratiques = "C:\Users\ADMIN\Downloads\configurations.xml"

# Lecture du fichier XML des bonnes pratiques
tree = ET.parse(fichier_xml_bonnes_pratiques)
root = tree.getroot()

# Dictionnaire pour stocker les bonnes pratiques (configuration: commande)
bonnes_pratiques = {}

# Parcours des balises <configuration> du fichier XML des bonnes pratiques
for config in root.findall("C:\Users\ADMIN\Documents\startup-config.txt"):
    # Récupération de la valeur de chaque balise <configuration>
    value = "C:\Users\ADMIN\Documents\startup-config.txt"
    # Récupération de la commande correcte associée à la configuration
    commande = config.get("commande")
    bonnes_pratiques[value] = commande

# Fichier Netmiko contenant les configurations récupérées
fichier_netmiko = "C:\Users\ADMIN\Downloads\configurations.xml"

# Lecture du fichier Netmiko
with open(fichier_netmiko, "r") as f:
    configurations_netmiko = f.readlines()

# Remplacement des configurations non conformes par les commandes correctes
configurations_corrigees = []
for config_netmiko in configurations_netmiko:
    config_netmiko = config_netmiko.strip()
    if config_netmiko in bonnes_pratiques:
        # Si la configuration est non conforme, remplacez-la par la commande correcte
        config_corrigee = bonnes_pratiques[config_netmiko]
        configurations_corrigees.append(config_corrigee)
```

Figure IV.10 Création de code python 01

```python
# Remplacement des configurations non conformes par les commandes correctes
configurations_corrigees = []
for config_netmiko in configurations_netmiko:
    config_netmiko = config_netmiko.strip()
    if config_netmiko in bonnes_pratiques:
        # Si la configuration est non conforme, remplacez-la par la commande correcte
        config_corrigee = bonnes_pratiques[config_netmiko]
        configurations_corrigees.append(config_corrigee)
        print(config_corrigee)
    else:
        # Si la configuration est conforme, conservez-la telle quelle
        configurations_corrigees.append(config_netmiko)
        print(config_netmiko)  # Affichage normal

# Écriture des configurations corrigées dans un nouveau fichier
fichier_netmiko_corrigee = "C:\Users\ADMIN\Desktop\correction.txt"
with open(fichier_netmiko_corrigee, "w") as f:
    f.write("\n".join(configurations_corrigees))

print("Les configurations ont été corrigées avec succès et enregistrées dans", "C:\Users\ADMIN\Desktop\corr
```

Figure IV.11 Création de code python 02

- Nous définissons le chemin vers le fichier XML qui contient les bonnes pratiques pour la configuration réseau. Cette information est stockée dans la variable "fichier_xml_bonnes_pratiques".
- Lecture du fichier XML des bonnes pratiques : Nous ouvrons et lisons le fichier XML à l'aide de la bibliothèque xml.etree.ElementTree. La structure XML est analysée et stockée dans la variable "tree". Cela nous permet d'accéder aux éléments et aux attributs du fichier XML.
- Parcours des balises de configuration : Notre code parcourt les balises <configuration> du fichier XML des bonnes pratiques en utilisant la méthode findall () de la variable "tree". Cela nous permet d'itérer sur chaque balise de configuration.
- Récupération des informations de configuration : Nous extrayons les valeurs des balises <configuration> et les stockons dans la variable "value". Ces valeurs représentent les configurations à vérifier.
- Remplacement des configurations non conformes : Nous vérifions les configurations extraites par rapport aux bonnes pratiques définies dans le fichier XML. Si une configuration est considérée comme non conforme, nous la remplaçons par une commande correcte associée. Les configurations corrigées sont stockées dans la liste "configurations_corrigees".
- Affichage des configurations corrigées : Nous utilisons la fonction print () pour afficher les configurations corrigées. Cela nous permet de visualiser les modifications effectuées.
- Écriture des configurations corrigées dans un fichier : Nous écrivons les configurations corrigées dans un nouveau fichier texte à l'aide de la fonction write ().

En résumé, ce code nous permet de lire un fichier XML qui contient des conseils de configuration de réseau, de contrôler les configurations récupérées et de les améliorer si nécessaire, après quoi nous pouvons afficher les changements et les enregistrer dans un nouveau document.

IV.8 Résultats

Le résultat du débogage de notre code a été le transfert des configurations de chaque équipement vers le fichier de correction mentionné dans le code, en remplaçant les fausses commandes par les commandes correctes. Comme vous pouvez le voir dans ces exemples, nous avons capturé les configurations de quelques équipements.

Scénario 01

Lors du scan, nous avons capturé les configurations du routeur et nous avons détecté une seule configuration qui était fausse c'est la commande "no shutdown". Nous avons délibérément écrit cette commande en "shutdown" pour tester la capacité de notre outil à identifier et corriger les erreurs de configuration. En détectant cette erreur et en appliquant la correction appropriée, notre outil a démontré son efficacité dans le processus d'automatisation de la gestion des configurations des équipements réseau.

```
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
!
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
redundancy
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown

!
interface Ethernet0/1
```

Figure IV.12 la détection des vulnérabilités de routeur 01

```
 ip address 203.0.113.10 255.255.255.0
 no shutdown

!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!
!
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 15
 login
 transport input none
!
!
end
```

Figure IV.13 la détection des vulnérabilités de routeur 02

Scénario 02

Notre outil a détecté la commande "no shutdown" et activé le chiffrement des mots de passe (service password-encryption) ainsi que le service SSH pour renforcer la sécurité.

```
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
*service password-encryption
!
hostname SL3
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
!
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
!
interface Ethernet0/0
 no shutdown
 ip address 10.0.0.2 255.255.255.0
!
interface Ethernet0/1
 no shutdown
 ip address 10.10.1.1 255.255.255.0
```

Figure IV.14 la détection des vulnérabilités de switch layer3 01

```
interface Ethernet0/1
 no shutdown
 ip address 10.10.1.1 255.255.255.0
!
interface Ethernet0/2
 no shutdown
 ip address 10.20.1.1 255.255.255.0
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
enable password azerty
login
crypto key generate rsa modulus 6
 logging synchronous
line aux 0
line vty 0 15
 transport input ssh
 end
write memory
 login
 transport input none
!
!
end
```

Figure IV.15 la détection des vulnérabilités de switch layer3

Conclusion

Dans ce chapitre nous avons développé un outil Python automatisé qui détecte les vulnérabilités dans la configuration du matériel Cisco. Cet outil analyse les configurations existantes, identifie les paramètres non conformes aux bonnes pratiques de sécurité et les remplace par des configurations valides. Cela simplifie la gestion du matériel, améliore la sécurité du réseau et garantit la cohérence de la configuration. Grâce à cet outil, les administrateurs réseau peuvent maintenir efficacement des configurations conformes et atténuer les menaces potentielles résultant de failles de sécurité.

Conclusion générale

Notre travail avait pour objectif de renforcer la sécurité de notre réseau en développant un outil de détection des vulnérabilités. Pour atteindre cet objectif, nous avons combiné deux éléments essentiels : le CIS Control (Center for Internet Security Control) et le SDN (Software-Defined Networking).

Le CIS Control fournit des directives et des mesures de sécurité pour protéger les infrastructures réseau contre les menaces et les vulnérabilités. En intégrant les recommandations du CIS Control dans notre outil, nous nous assurons de suivre les meilleures pratiques de sécurité et de maintenir un niveau élevé de protection pour notre réseau.

Nous avons utilisé le SDN pour améliorer notre approche de sécurité. Le SDN permet une gestion centralisée et programmable du réseau, offrant ainsi une plus grande flexibilité et une automatisation accrue des opérations. En adoptant le SDN, nous avons pu séparer le plan de contrôle du plan de données, ce qui nous a permis de gérer notre réseau de manière plus efficace et cohérente.

En combinant le CIS Control et le SDN, nous avons créé un environnement de sécurité robuste et dynamique. Notre outil de détection des vulnérabilités permet de maintenir la conformité avec les recommandations du CIS Control et d'identifier rapidement les failles de sécurité potentielles. Grâce au SDN, nous avons automatisé de nombreuses tâches de gestion et de configuration, ce qui nous permet de réduire les erreurs humaines et de consacrer nos ressources à des activités à plus forte valeur ajoutée.

En outre, notre travail ouvre des perspectives prometteuses pour les futurs étudiants et professionnels souhaitant se spécialiser dans la sécurité des réseaux. Voici quelques perspectives clés à prendre en compte :

-Approfondissement des connaissances sur le CIS control.

-Exploitation des avancées en matières de SDN.

-Intégrer l'outils de détection des vulnérabilités que nous avons développée dans le contrôleurs centralisé.

Références bibliographiques

Bibliographie

[1] : Mémoire de fin d'étude master télécommunication filière télécommunication spécialité réseau et télécommunication élaboré par : ARABI Nadjoua YAMOUTENE Naima.

[2]: Ashton, Metzler, and Associates, Ten Things to Look for in an SDN.

[3]: Vishal Kadam1, Makhan Kumbhkar, Security in Cloud Environment, International Journal of Scientific Research in Computer Science and Engineering uter Science and Engineering uter Science and Engineering, vol-2, issue-3, June-2014.

[4]: Rana, Deepak & Garg, Naveen & Chamoli, Sushil. (2012). A Study and Detection of TCP SYN Flood Attacks with IP spoofing and its Mitigations. International Journal of Computer Technology and Applications. Vol 3 (4), 1476-1480.

[5] :"Scott E. Donaldson", "SSiegel», «Chris, "Abdul Aslam"," Enterprise Cybersecurity", Ed°Apress,20/05/2015

Webographie

[W1] :https://www.riskinsight-wavestone.com/2013/10/le-sdn-ce-quil-faut-savoir-sur-le-cisco-killer/reseau-traditionnel-reseau-sdn/,consulté le 21/03/2023

[W2] :https://nutanshinde.wordpress.com/2016/01/31/building-blocks-of-sdn-network/,consulté le 24/03/2023

[W3] : https://opennetworking.org/sdn-definition/ consulté le 24/03/2023

[W4] :https://www.slideserve.com/elpida/software-defined-networking-coms-6998-8-fall-2013, Consulté le 31/03/2023

[W5]: https://info.support.huawei.com/info-finder/encyclopedia/en/NETCONF.html,consulté le 31/03/2023

[W6]:https://download.huawei.com/mdl/image/download?uuid=e04a7d66cec24637bbb1001e36d2b39a,consulté le 31/03/2023

[W7]:https://www.juniper.net/documentation/us/en/software/junos/bgp/images/g042423.png, consulté le 31/03/2023

[W8] :https://www.researchgate.net/figure/Extended-SDN-NFV-architecture-with-three-main-layers-i-NFV-Infrastructure-ii_fig1_321008006,consulté le23/03/2023

[W9] :https://in.pinterest.com/pin/what-is-network-virtualization--24136547978043712/ consulté le 23/03/2023

[W10] :https://www.aiophotoz.com/photos/download-network-virtualization-sdn-overlay-solutions-softarchive.html,consulté le 23/03/2023

[W11]: https://www.andlil.com/societe-cisco-129084.html,consuté le 25/03/2023

[W12] : https://www.juniper.net/fr/fr/research-topics/what-is-a-network-switch.html,consulté le 25/03/2023

[W13]:https://www.compufirst.com/rubrique-conseils/comment-choisir-son-switch/main.do?appTreeId=42570,consulté le 25/03/2023

[W14] : https://hifalindia.com/Electronics-Renewed-WSC3560V224TSS-Cisco-Catalyst-v2-280017-Switches/ consulté le 26/03/2023

[W15] : https://www.thegalleriamalljordan.com/?zg8035oqudrrhq1349,consulté le 07/04/2023

[W16]:https://grandvaultgroup.com/meraki-poe-switch-k.html,consulté le 07/04/2023

[W17] : https://www.looptelecom.com/fr/pswitch/Accs-et-Switch-Ethernet/Switch-industriel-DINL3/Commutateurs_industriels_DIN_Rail_commutateur_industriel_L2_L3_g%C3%A9r%C3%A9_Gigabit_PoE_PoE__%C3%A0_8_ports IP6818, consulté le 07/04/2023

[W18] :https://fr.dreamstime.com/commutateur-d-ethernet-grand-fournisseur-bureau-services-ports-client-deux-combin%C3%A9s-couleur-noire-image140723273,consulté 07/04/2023

[W19]:https://fr.wikipedia.org/wiki/Fichier:Cisco-rs1.jpg ,consulté le 27/03/2023

[W20] : https://fr.made-in-china.com/co_mobidatawireless/product_Broadband-4G-Lte-WiFi-Wireless-Router_esgnsroyg.html consulté le 07/04/2023

[W21] : https://www.ebay.fr/itm/401496710001 consulté le 07/04/2023

[W22] :https://www.mhzshop.com/shop/Reseaux/Routeur/Routeur-central-hautes-performances-MikroTik-Cloud-Core-CCR1009-7G-1C-1S.html consulté le 07/04/2023

[W23] : https://previews.123rf.com/images/pogrig/pogrig1703/pogrig170300013/73767461-routeur-de-p%C3%A9riph%C3%A9rique-internet-g%C3%A9n%C3%A9rique-isol%C3%A9-sur-fond-blanc.jpg,consulté le 07/04/2023

[W24] :https://www.dlink.com.my/product/dap-1360-n300-wireless-access-point-range-extender/,consulté le 07/04/2023

[W25]: https://www.intronaut.net/pourquoi-utiliser-les-solutions-cisco-en-entreprise/

[W26]: https://www.youtube.com/watch?v=PoHSoLneC7k

[W27] :https://www.cisco.com/ , consulté le 26/03/2023

[W28]:https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html#~stickynav=1 , consulté le 26/03/2023

[W29] :https://www.timigate.com/2019/06/cisco-certification-update-write-ccnp-without-having-ccna.html,consulté le 16/03/2023

[W30] : https://contenthub.netacad.com/itn-dl/17.6.1,consulté le 01/04/2023

[W31] : https://www.valeonetworks.com/wp-content/uploads/2019/10/Top-20-CIS-Controls-Chart.png,consulté le 14/04/2023

[W32] : https://www.securestatecyber.com/fr/cis-controls,consulté le 13/04/2023

[W33] : https://www.cis-integratedservices.com/fr/expertise,consulté le 14/04/2023

[W34] : https://i.pinimg.com/originals/07/78/4b/07784b0900d436bc67e6f9f4149f3f5e.png,consulté le 15/04/2023

[W35] : https://paper.bobylive.com/Security/CIS/CIS_Cisco_IOS_17_x_Benchmark_v1_0_0-%281%29.pdf,consulté le 26/04/2023

[W36]: https://paper.bobylive.com/Security/CIS/CIS_Cisco_IOS_17_x_Benchmark_v1_0_0-%281%29.pdf,consulté le 01/06/2023

[W37] : https://www.machaon.fr/isn/resume-cours/python/muniglia/resume.html,condulté le 12/06/2023

[W38] : https://www.techopedia.com/definition/25690/vmware-workstation CONSULT2 LE 03/05/2023