République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MEMOIRE DE MASTER PROFESSIONNEL

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Solution SDN pour l'entreprise TCHIN-LAIT CANDIA

Présenté par :
Melle LOUBAR Lydia
M. MERABET Fawzi

Soutenu le 25 Juin 2023 devant le jury composé de :

Présidente	**Dr. S. LAHLAH**	**MCB**	**Université de Béjaia**
Promotrice	**S. OUYAHIA**	**MCB**	**Université de Béjaia**
Examinateur	**M. MOKTEFI**	**MCB**	**Université de Béjaia**

Béjaia, Juin 2023.

⁂ *Remerciements* ⁂

Nous tenons tout d'abord à remercier ALLAH le tout puissant et miséricordieux qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous remercions aussi notre encadreur Mme OUYAHIA SAMIRA pour ses suivis, ses conseils et encouragements durant la réalisation de ce mémoire.

Nos remerciements vont également a M.MERABET DJEBAR et M.MOUNSI MASSINISSA ainsi que toute l'équipe de TCHIN_LAIT pour leur disponibilité, leurs précieux conseils et pour nous avoir introduit au monde professionnel.

Aussi nos vifs remerciements aux membres du jurys pour l'intérêt accordé à notre travail en l'examinant minutieusement et avec attention. Nous tenons a exprimer nos sincères remerciements à tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu pour la réussite de nos études.

A nos parents, on espère qu'ils seront toujours fière de nous. nos chères familles pour leurs soutient, encouragements et leurs bienveillance pour notre bien-être et notre succès.A nos amis(e)s pour leur sincère amitié et confiance. Nous leur devons toute notre reconnaissance et notre attachement. Nous ne pourrons terminer sans remercier tous ce qui ont participer d'une manière ou d'une autre dans l'élaboration de ce projet de fin d'études.

MERCI !

⁂ *Dédicaces* ⁂

A mes chers parents. Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti à mon instruction et mon bien être. A l'homme de ma vie, celui qui s'est toujours sacrifier pour me voir réussir, à toi mon père. A la source de mes efforts, ma vie et mon bonheur, maman que j'adore. A vous mes frères AMINE et ANAIS pour votre soutien.

Je dédie ce modeste travail à toute ma famille petits et grands oncles et tantes qui m'ont porté dans leurs prières et qui m'ont encouragé tout au long de mes études. Dédicace plus précisément a ma tante ASSIA pour toute son aide et toute sa confiance en moi pour réussir merci infiniment. ainsi qu'à ma petite cousine NELIA pour l'amour qu'elle me porte je t'aime mon ange. Dedicace a mon petit amour ADAM.

A mes grands parents paternels BAYA et ABDERHMAN, j'espère que vous êtes fière de moi. A la mémoire de ma grande mère maternelle YEMMA TATA, j'espère que tu reposes en paix. Ainsi qu'à mon grand père maternelle BOUHOU.

A tous mes amis qu'ils soient toujours ici ou ailleurs je vous dédie ceci pour vous remercier de votre amitié.

A mon binôme FAWZI pour ton courage et ta rigueur.

M. LYDIA

⁂ *Dédicaces* ⁂

Al Hamdoulillah.
Je commence cette dédicace en exprimant ma profonde gratitude envers ALLAH pour m'avoir accordé la force, la persévérance et la clarté d'esprit tout au long de cette étude.
À mes chers parents, aucune dédicace ne saurait exprimer mon respect. Vous êtes la source de vie, mes sources d'inspiration. Vos sacrifices et votre amour inconditionnel ont été le moteur de ma réussite. Je vous suis infiniment reconnaissant pour tous les efforts que vous avez déployés afin de me donner les meilleures opportunités de réussite.
À mes chers frères RAZIK, ANIS, et à mes chères sœurs SIHAM, ASSIA, DALILA, ainsi qu'à leurs enfants, je souhaite exprimer ma profonde gratitude pour votre soutien constant.
À mes beaux-frères et mes belles-sœurs, qui m'ont soutenu sans condition.
À toute ma famille, petites et grandes, oncles et tantes, cousines, qui m'ont porté dans leurs prières et m'ont encouragé tout au long de mes études. Je dédie plus précisément cette dédicace à ma grand-mère maternelle OUM SAAD pour l'amour qu'elle me porte.
À mes amis fidèles, je vous remercie du fond du cœur. Votre amitié sincère et vos encouragements ont été une force motrice pour atteindre mes objectifs.
À ma binôme LYDIA, pour ton encouragement et ta rigueur.

M. FAWZI

Table des matières

Liste des figures

Liste des tableaux

Liste des acronymes

AAA	Authentification, autorisation et comptabilité .
ACI	Application Centric Infrastructure .
API	Application Programming Interface .
ARP	Adress Resolution Protocol .
BNSF	Basic Network Service Features .
CAO	Computer Aided Design .
CENTOS	Community Enterprise Operating System .
CLI	Command-line interface .
DDOS	Distributed Denial of Service attack .
DLUX	OpenDayLight User eXperience .
DMZ	DeMilitarized Zone .
DOS	Denial of Service attack .
FRM	Forwarding Rules Manager .
FTP	File Transfer Protocol .
GBP	Group-Based Policy .
GNS	Graphical Network Simulator .
ICMP	Internet Control Message Protocol .
IOS	Internetworking Operating Systems .
IP	Internet Protocol.
IPFIX	Internet Protocol Flow Information Export.
LACP	Link Aggregation Control Protocol.
LAN	Local Area Network .
LLDP	Link Layer Discovery Protocol .
MAN	Metropolitan Area Network .
MITM	Man In The Middle .
NB	North Bound .
ODL	OpenDayLight .
ONF	Open Networking Foundation .
ONOS	Open Network Operating System.
PDM	Product Data Management.
P2P	Peer To Peer.
QOS	Quality of Service .
RSPAN	Remote Switch Port Analyzer.
SAL	Service Abstraction Layer .
SDN	Software-Defined Networking.
SFC	Service Function Chaining .
SNMP	Simple Network Management Protocol.
TCP	Transmission Control Protocol .
UHT	Ultra Haute Température .

Introduction générale

Les réseaux SDN (Software-Defined Networking) sont une nouvelle approche de la gestion des réseaux, qui implique le déplacement du contrôle de réseau de commutation traditionnel de l'hyperviseur de commutation vers un contrôleur SDN centralisé. Cette approche permet de simplifier la gestion du réseau, d'améliorer l'efficacité et la détection proactive des menaces liées à la sécurité informatique.

De ce fait, on dira que le SDN est une forme d'automatisation des réseaux traditionnels. Il utilise une approche centralisée pour gérer les opérations de réseau. Cela permet une plus grande agilité et une meilleure gestion des opérations réseau, car les tâches de configuration sont automatisées et effectuées de manière programmée en utilisant des modèles de configuration, des politiques et des règles définis par l'utilisateur. Loin de la définition rigide initiale qui consistait uniquement à séparer les plans de contrôle et de données, le SDN est désormais beaucoup plus flexible. OpenFlow n'est qu'un élément du SDN, et le marché s'intéresse désormais davantage aux solutions qui offrent une programmation et une simplification réelles des infrastructures. Pour répondre à des usages spécifiques, plusieurs modèles de SDN se développent en parallèle et visent à améliorer les fonctionnalités du SDN.

Cette perspective d'un renouveau dans la conception même du réseau, nous a motivés à tenter d'étudier une solution SDN qui répond aux exigences des grandes entreprises. De ce fait, nous avons effectué un stage dans l'entreprise TCHIN_LAIT où nous avons étudié l'architecture de leur réseau et proposé de l'automatiser pour tirer profit des réseaux SDN. Cette solution que nous avons choisie nous permettra de centraliser et virtualiser le réseau de l'entreprise TCHIN_LAIT, grâce au contrôleur ONOS qui est le principal contrôleur SDN open source. En effectuant une étude bibliographique approfondie, nous présentons les différentes normes régissant le paradigme SDN ainsi que les cas d'utilisation les plus en vue. Par la suite, nous procédons à l'implémentation de cette solution dans un environnement virtuel dans le but de répondre aux problématiques actuelles.

De plus, la sécurité dans les réseaux SDN est vitale, car les pirates peuvent utiliser cette nouvelle architecture pour accéder à des informations sensibles et en provoquer des dom-

mages. Les défis de sécurité dans les réseaux SDN sont multiples et incluent la vulnérabilité des contrôleurs SDN, la nécessité de protéger les communications entre les contrôleurs SDN et les commutateurs, la conformité aux normes de sécurité, la détection des menaces et la réponse rapide aux attaques détectées.

Ce mémoire, sera réparti en 4 chapitres :

Le chapitre 1 a pour objectifs de définir tout les aspects de la sécurité informatique et les principales attaques qui surgissent.

Dans le 2éme chapitre, nous nous étalerons sur les principes fondamentaux du paradigme SDN. Il nous permettra d'avoir une idée globale sur son fonctionnement.

Le chapitre 3, portera sur la présentation de l'organisme d'accueil où nous avons effectué notre stage. Ainsi que sur la problématique que nous allons traiter.

Dans le dernier chapitre, l'implémentation de notre solution sera présentée. On évoquera tous ce que nous avons utilisé pour son implémentation. Ainsi que la topologie sur laquelle on a pu travailler. Nous allons sur tout sécuriser notre solution SDN et On fera également quelques tests.

Nous terminerons ce mémoire par une conclusion et une bibliographie.

Chapitre 1

La sécurité des réseaux

1.1 Introduction

Les réseaux d'entreprises sont des systèmes inter-connectant diverses machines dans le but de faciliter leur communication. Ces infrastructures permettent notamment le partage de fichiers et l'échange de messages, ce qui en fait un outil indispensable pour optimiser les performances d'une entreprise. Toutefois, la sécurité du transport des données ainsi que l'accès aux informations sur les différents postes de travail constituent aujourd'hui une préoccupation majeure.

L'avènement d'Internet a exacerbé ces problématiques en raison des risques liés à la sécurité lors des échanges au sein de réseaux privés ou publics. Dans ce contexte, il est impératif que soient mis en place différentes stratégies et mécanismes visant à garantir une protection adéquate contre toute forme d'intrusion malveillante.

Le présent chapitre se divise essentiellement en deux sections distinctes : la première aborde les principes fondamentaux relatifs aux réseaux informatiques tandis que la seconde s'intéresse plus particulièrement aux attaques réseau susceptibles d'affecter ces derniers ainsi qu'aux technologies disponibles pour y faire face efficacement.

1.2 Généralités sur les réseaux informatiques des entreprises

1.2.1 Définition d'un réseau

Un réseau informatique est un ensemble d'ordinateurs et de périphériques connectés entre eux afin de partager des ressources telles que des fichiers, des imprimantes ou encore une connexion internet. Les ordinateurs communiquent entre eux grâce à un protocole de communication tel que TCP/IP en utilisant différents types de câbles tels que le câble Ethernet. Le réseau peut être configuré selon différentes topologies comme la topologie en étoile où tous les périphériques sont reliés à un hub central ou la topologie en anneau où chaque ordinateur est connecté au suivant pour former une boucle fermée. La mise en place d'un réseau nécessite également l'utilisation d'équipements tels que des routeurs, switches et pare-feux pour assurer la sécurité du système ainsi qu'une bonne gestion du trafic sur le réseau [22].

1.2.2 Types de réseaux

Les réseaux peuvent être classés selon différents critères tels que leur taille, leur vitesse de transfert de données et leur étendue. Selon l'étendu, nous trouvons les classes suivantes.

1.2.2.1 LAN (Local Area Network)

Ou réseau local est un ensemble d'ordinateurs appartenant à une même organisation reliés dans une petite aire géographique par un réseau utilisant principalement la technologie Ethernet. Les vitesses de transfert des données sur les réseaux locaux varient entre 10 Mbit/s et 1 Gbit/s, avec une capacité pouvant atteindre jusqu'à 1000 utilisateurs [9] .

1.2.2.2 MAN (Metropolitan Area Network)

Ou réseau métropolitain interconnecte plusieurs LAN géographiquement proches sur des distances maximales d'environ quelques dizaines de kilomètres à des débits importants supérieurs à 100 Mbits/s. Un MAN est formé par l'interconnexion de commutateurs ou routeurs via des liens hauts débits en fibre optique [9] .

1.2.2.3 WAN (Wide Area Network)

Également appelé réseau étendu, relie plusieurs LAN situés sur des distances géographiques importantes. Les débits disponibles pour les WAN sont souvent limités en raison du coût élevé engagé pour maintenir ces liaisons distantes qui augmentent avec la distance parcourue. Les WAN fonctionnent grâce aux routeurs qui permettent le choix du chemin optimal vers un nœud donnée du réseau. Internet reste l'exemple le plus connu d'un tel système WAN performant et mondialisé aujourd'hui [9] .

1.2.3 Architecture des réseaux d'entreprise

On distingue également deux catégories de réseaux (voir figure 1.1) :

1.2.3.1 Réseaux poste à poste (peer to peer= P2P)

Sur un réseau poste à poste, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central, comme présenté dans la figure 1.1. L'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines il devient impossible à gérer [22].

1.2.3.2 Réseaux client-serveur

Sur un réseau à architecture client/serveur, tous les ordinateurs (client) sont connectés à un ordinateur central (le serveur du réseau), une machine généralement très puissante en terme de capacité. Elle est utilisée surtout pour le partage de connexion Internet et de logiciels centralisés. Ce type d'architecture est plus facile à administrer lorsque le réseau est important car l'administration est centralisée mais elle nécessite un logiciel coûteux spécialisé pour l'exploitation du réseau [22].

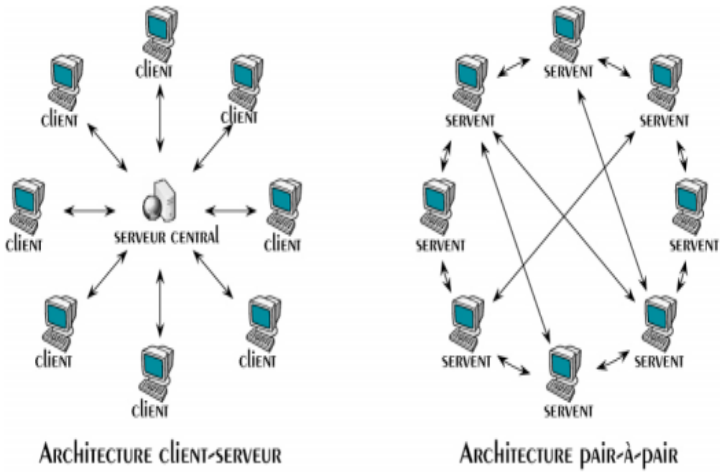

FIGURE 1.1 – Architecture réseau

1.2.4 Hiérarchie des équipements

La hiérarchie des équipements réseau concerne la structuration et la connexion des différents composants matériels d'un réseau afin de garantir son bon fonctionnement et une gestion efficace. Voici quelques éléments couramment présents dans la hiérarchie des équipements réseau [21] :

1.2.4.1 Commutateurs d'accès (Access Switches)

Ils sont situés au niveau le plus bas de la hiérarchie et sont utilisés pour connecter les appareils finaux tels que les ordinateurs, les imprimantes et les téléphones IP. Les commutateurs d'accès gèrent la connectivité locale dans un réseau local (LAN) et regroupent généralement les appareils au sein de VLAN (Virtual Local Area Network) [21].

1.2.4.2 Commutateurs de distribution (Distribution Switches)

Ils se trouvent au niveau intermédiaire de la hiérarchie et agissent comme des points de connexion entre les commutateurs d'accès et les commutateurs de cœur. Les commutateurs de distribution permettent de gérer la segmentation du réseau, le routage inter-VLAN et la gestion du trafic dans un réseau local [21].

1.2.4.3 Commutateurs de cœur (Core Switches)

Ils sont situés au niveau supérieur de la hiérarchie et sont responsables de la connectivité entre les différents segments du réseau, y compris les différentes parties d'un réseau local et les réseaux étendus (WAN). Les commutateurs de cœur doivent être hautement performants et redondants pour assurer une connectivité fiable et une capacité de transmission élevée [21].

1.3 Généralités sur la sécurité informatique

1.3.1 Définition de la sécurité

La sécurité informatique est un ensemble de mesures visant à protéger les systèmes d'information contre toute menace ou intrusion. Elle repose sur des technologies telles que les pare-feux, les anti-virus, la cryptographie et l'authentification forte pour garantir la confidentialité, l'intégrité et la disponibilité des données stockées dans ces systèmes. La mise en place de politiques de sécurité strictes ainsi que des audits réguliers permettent également d'évaluer le niveau de risque encouru par une entreprise ou une organisation face aux cyber-attaques. En somme, il s'agit d'un domaine crucial pour assurer le bon fonctionnement et la protection du patrimoine informationnel d'une entité donnée.

1.3.2 Objectifs de la sécurité

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants [7] :

- La disponibilité
- L'intégrité
- La confidentialité
- L'authentification
- La non répudiation

1.3.2.1 La disponibilité

L'information sur le système doit être toujours disponible aux personnes autorisées [19].

1.3.2.2 L'intégrité

L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées [19].

1.3.2.3 La confidentialité

"Est le maintien du secret des informations " (Le Petit Robert). Dans le cadre d'un système d'information, cela peut être vu comme une protection des données contre une divulgation non autorisée [19].

1.3.2.4 L'authentification

Permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- Un élément d'information que l'utilisateur connaît (mot de passe, etc.)
- Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat, etc.)
- Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (empreinte digitale, ADN, etc.) [19].

1.3.2.5 La non répudiation

C'est la propriété qui assure la preuve de l'authenticité d'un acte, c'est-à-dire que l'auteur d'un acte ne peut nier l'avoir effectué [19].

1.3.3 Principales menaces de la sécurité informatique

1.3.3.1 Les Utilisateurs

L'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur (par insouciance ou malveillance).

1.3.3.2 Les programmes malveillants

Un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données.

1.3.3.3 L'intrusion

Une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès.

1.3.3.4 Un sinistre

Une mauvaise manipulation, une malveillance ou des aléas naturels entraînant une perte de matériel et/ou de données.

1.4 La sécurité des réseaux d'entreprise

1.4.1 Attaques réseaux

Les attaques réseaux sont très nombreuses, il est donc très difficile de les recenser. Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité. Ces dernières peuvent être classifiées par catégories comme suit :

1.4.1.1 Faiblesse des protocoles

Certains protocoles de réseau n'ont pas été développés en tenant compte des problèmes de sécurité, ce qui les rend vulnérables à des attaques telles que :

Attaque par fragmentation La fragmentation d'attaque est une technique de saturation de réseau qui exploite la fragmentation du protocole IP. Le protocole IP est conçu pour fragmenter les paquets de données volumineux en plusieurs paquets IP, chacun ayant un numéro de séquence et un numéro d'identification commun. Lorsque les données sont reçues, le destinataire utilise les valeurs de décalage contenues dans les paquets pour les rassembler. Cependant, une attaque par fragmentation consiste à envoyer des paquets malveillants avec des valeurs de décalage incorrectes, ce qui peut entraîner une surcharge du réseau et une interruption des communications [22].

Attaque par déni de service Le déni de service est une attaque visant à empêcher les utilisateurs autorisés d'accéder aux informations ou aux services auxquels ils ont droit, ce qui affecte la disponibilité. Cette forme d'attaque est souvent la plus simple à exécuter, car elle

consiste simplement à envoyer un grand nombre de requêtes, valides ou non, pour saturer les ressources disponibles pour un service donné. On parle alors d'inondation ou de flooding. Cette attaque peut être très dommageable pour les entreprises et les organisations, car elle peut entraîner une perte de revenus, une perte de productivité et une détérioration de la réputation [22].

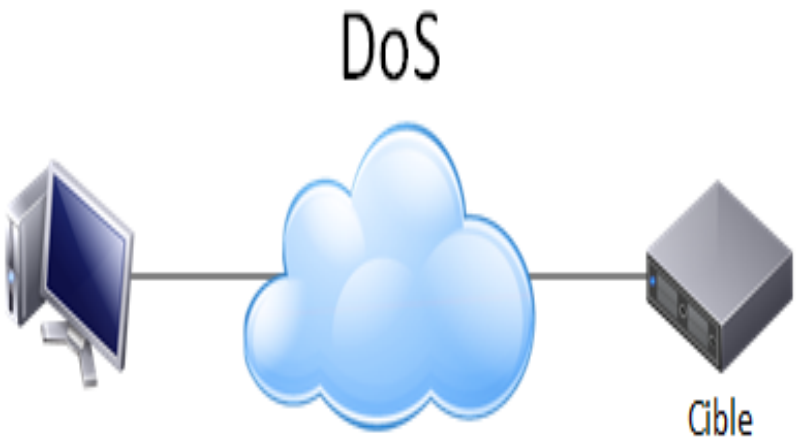

FIGURE 1.2 – Attaque par déni de service

1.4.1.2 Faiblesse d'authentification

Les versions actuelles des protocoles IP ou ICMP, ne dispose pas de mécanisme d'authentification, de ce fait elles subissent des attaques qui s'appuient sur ces faiblesses. Parmi les principales attaques on trouve :

Attaque ARP L'empoisonnement de cache ARP est une technique d'attaque simple qui exploite les vulnérabilités du protocole ARP. Cette technique tire parti de l'absence d'authentification des requêtes ARP, ce qui permet à un attaquant de duper une machine en lui faisant croire qu'une requête provient d'une autre machine avec laquelle elle communique. Cette technique est souvent appelée "empoisonnement de cache ARP". Cette attaque peut être utilisée pour intercepter ou modifier le trafic réseau, ou pour mener d'autres types d'attaques plus sophistiquées [22].

Attaque man-in-the-middle dite en français l'homme au milieu, elle consiste à passer les échanges entre deux personnes par le biais d'une troisième, sous le contrôle de l'entité

pirate, ce dernier intercepte et transforme les données, toute en masquant à chaque acteur la réalité de son interlocuteur [19].

Attaque par réflexion des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées.

Attaque par Rejeu de message Les attaques de type "rejeu" (ou "replay attacks" en anglais) sont des attaques "man in the middle" qui consistent à intercepter des paquets de données et à les renvoyer tels quels, sans les déchiffrer, au serveur destinataire. Cette technique permet à l'attaquant de tromper le serveur en lui faisant croire que les données sont légitimes et d'obtenir ainsi un accès non autorisé à des informations sensibles. Les attaques de type "rejeu" sont souvent utilisées pour contourner les mécanismes de sécurité tels que l'authentification ou le chiffrement des données [22].

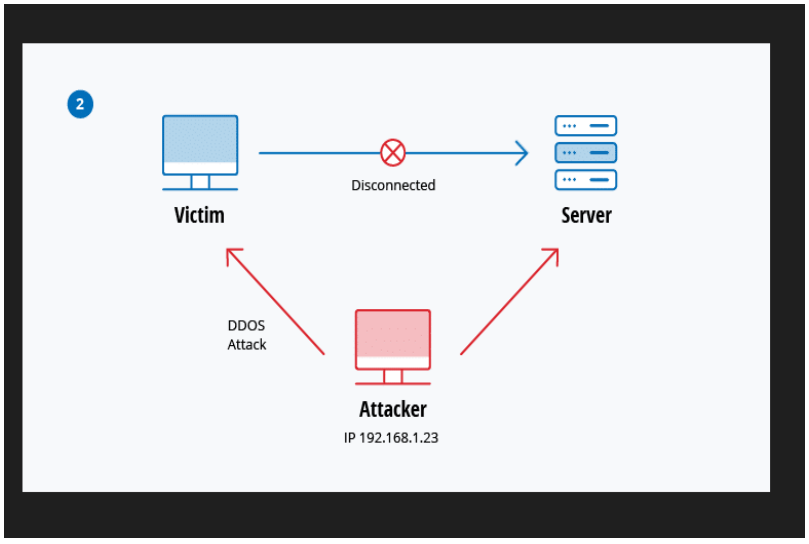

FIGURE 1.3 – Attaque par rejeu

1.4.1.3 Faiblesse d'implémentation

Parmi les attaques qui exploitent ce genre de faiblesse on trouve :

Attaque du ping de la mort c'est une des plus anciennes attaque réseau. Le principe consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille

maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage [22].

1.4.1.4 Faiblesse de configuration

Les équipements réseau tels que les pare-feu, les routeurs, etc. peuvent être la cible d'attaques si leur configuration est mal réalisée. Les erreurs de configuration peuvent être causées par des erreurs humaines, ce qui peut permettre à des attaquants de contourner les mesures de sécurité mises en place. Pour éviter cela, il est important que seuls les acteurs autorisés aient accès aux équipements réseau et soient chargés de les configurer. Cela permet de minimiser les risques d'erreur de configuration et de renforcer la sécurité du réseau [22].

1.4.2 Une politique de sécurité réseau

1.4.2.1 Qu'es ce que c'est une politique de sécurité

Toutes méthodes, techniques et outils concourant à la protection de l'information contre un large éventail de menaces afin de garantir la continuité d'activité de l'entreprise, réduire les dommages éventuels sur l'activité de l'entreprise et maximiser le retour sur investissement des systèmes d'Information [19].

1.4.2.2 0bjectifs d'une politique de sécurité

Une politique de sécurité a pour objectif de :

• S'assurer que les utilisateurs observent les bonnes pratiques et les règles concernant l'utilisation des technologies de l'information.

• S'assurer que les normes en matière de sécurité informatique soient dûrement mises en application.

• Réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents.

• Recommander les actions à prendre pour corriger les situations anormales ou dangereuses, notamment, les processus opérationnels et les grandes stratégies en matière informatique et les achats d'équipement.

• S'assurer que les éléments opérationnels qui requièrent une approbation des différentes directions soient respectés [22].

1.4.2.3 Mise en place d'une politique

Deux philosophies pour la mise en place d'une politique [19] :

Prohibitive : "tout ce qui n'est pas explicitement autorisé est interdit".

Permissive : "tout ce qui n'est pas explicitement interdit est autorisé".

Composantes Elles sont selon [22] :

- Politique de confidentialité
- Politique d'accès
- Politique d'authentification
- Politique d'intégrité
- Politique de disponibilité
- Politique de Non-répudiation
- Politique de responsabilité
- Politique de maintenance
- Politique de rapport de violations.

Établissement selon [22] :

- Identifier les risques et leurs conséquences.
- Évaluation des probabilités associées à chacune des menaces.
- Évaluation du coût d'une intrusion réussie.
- Élaborer des règles et des procédures à mettre en œuvre pour les risques identifiés (contre mesures).
- Évaluation des coûts des contre-mesures.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

1.4.3 Proposition de stratégie de sécurité réseau

Les sections suivantes présentent un ensemble de stratégies de sécurité axées sur des domaines spécifiques. Ces stratégies doivent être considérées comme des éléments de base pour établir une politique de sécurité solide.

1.4.3.1 Authentification

L'authentification contextuelle utilise des informations contextuelles pour vérifier l'authenticité de l'identité d'un utilisateur. Les profils de risque permettent aux entreprises de restreindre l'accès à des systèmes ou à des contenus spécifiques en fonction des critères de l'utilisateur. Cette approche permet de renforcer la sécurité en considérant le contexte dans lequel l'utilisateur tente d'accéder aux ressources de l'entreprise [19].

1.4.3.2 Cryptographie (chiffrement et signature)

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Dans toute transaction professionnelle, La signature numérique est un moyen d'identification de l'émetteur du message [22].

1.4.3.3 Contrôles d'accès aux ressources

Méthode pour restreindre l'accès à des ressources. On n'autorise que certaines entités privilégiées.

1.4.3.4 Firewalls

Pour prévenir les attaques provenant d'Internet via le routeur, il est recommandé d'isoler le réseau interne de l'entreprise. La méthode la plus courante pour y parvenir est d'utiliser un firewall et un serveur proxy. Le firewall, situé à l'entrée du réseau, constitue un point d'accès unique que tout le trafic doit emprunter. Le serveur proxy, quant à lui, agit comme un relais pour les applications afin de rendre les machines internes invisibles depuis l'extérieur. Cette approche permet de renforcer la sécurité du réseau en limitant les points d'entrée potentiels pour les attaquants [22].

1.4.3.5 Audit

L'audit de sécurité consiste à enregistrer toutes ou certaines des actions effectuées sur un système. L'analyse de ces informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation et certaines applications disposent généralement de systèmes d'audit intégrés. Les différents événements du système sont enregistrés dans un journal d'audit qui doit être analysé régulièrement, voire en temps réel. Pour les réseaux, il est essentiel d'avoir une base de temps commune pour estampiller les événements. Cette approche permet de renforcer la sécurité du système en détectant rapidement les activités suspectes et en prenant des mesures préventives pour éviter les attaques [22].

1.4.3.6 Logiciels anti-virus

Environ deux tiers des attaques informatiques sont causées par des virus. Pour prévenir ces attaques, il est essentiel que chaque poste de travail dispose d'un logiciel anti-virus régulièrement mis à jour. Les virus sont principalement transmis par des clés USB, mais peuvent également être propagés par e-mail. Les fichiers les plus susceptibles de contenir des virus sont les fichiers exécutables tels que les fichiers .com ou .exe. En adoptant ces mesures de sécurité, les entreprises peuvent réduire considérablement les risques d'attaques virales et protéger efficacement leurs systèmes informatiques [22].

1.4.3.7 Programmes de tests de vulnérabilité et d'erreurs de configuration

Utiliser des logiciels permettant de façon automatique de chercher les erreurs de configuration ou les vulnérabilités du système tel que Cops et Satan.

1.4.3.8 Détection d'intrusion

Utiliser un logiciel de détection des comportements anormaux d'un utilisateur ou des attaques connues. Ce logiciel émet une alarme lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau.

1.4.3.9 Les réseaux privés virtuels (VPN : Virtual Private Network)

Les tunnels VPN permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec l'avènement d'Internet, il est devenu essentiel de permettre un transfert de données sécurisé et fiable. Les tunnels VPN utilisent un principe de "tunnelling",

où chaque extrémité est identifiée, pour permettre le transit des données une fois qu'elles ont été chiffrées. Cette approche permet de renforcer la sécurité des communications en ligne et de protéger les données confidentielles contre les attaques potentielles [22].

1.4.3.10 Les DMZ (zone démilitarisé)

Lorsque certaines machines du réseau interne doivent être accessibles depuis l'extérieur, telles que des serveurs Web, des serveurs de messagerie ou des serveurs FTP publics, il est souvent nécessaire de créer une nouvelle interface réseau distincte. Cette interface doit être accessible à la fois depuis le réseau interne et depuis l'extérieur, sans compromettre la sécurité de l'entreprise. Cette zone isolée, qui héberge des applications mises à disposition du public, est appelée zone démilitarisée (DMZ). Cette approche permet de renforcer la sécurité en limitant l'accès direct aux ressources internes de l'entreprise depuis Internet, tout en permettant l'accès aux services nécessaires pour les utilisateurs externes [22].

1.5 Conclusion

Les réseaux d'entreprises sont des systèmes interconnectant diverses machines dans le but de faciliter leur communication. Ces infrastructures permettent notamment le partage de fichiers et l'échange de messages, ce qui en fait un outil indispensable pour optimiser les performances d'une entreprise. Toutefois, la sécurité du transport des données ainsi que l'accès aux informations sur les différents postes de travail constituent aujourd'hui une préoccupation majeure.

À l'issue de ce chapitre, on a présenté les premiers concepts des réseaux informatiques ainsi qu'une analyse des besoins de sécurité et des étapes importantes qui précèdent la mise en place des stratégies de sécurité dans un réseau d'entreprise.

Chapitre 2

Généralités sur les réseaux SDN

2.1 Introduction

Les réseaux SDN (Software-Defined Networking) sont une nouvelle approche de la conception des réseaux informatiques qui permettent une gestion centralisée et simplifiée des réseaux. Contrairement aux réseaux traditionnels, les réseaux SDN séparent le plan de contrôle du plan de données, ce qui permet une gestion plus flexible et dynamique des flux de données. L'architecture des réseaux SDN est basée sur des commutateurs intelligents qui sont contrôlés par un contrôleur SDN centralisé.

Entre les commutateurs et le contrôleur SDN, le protocole OpenFlow est utilisé pour communiquer entre eux. Ces contrôleurs SDN sont des logiciels qui permettent de gérer les réseaux SDN en fournissant une interface centralisée pour la configuration et le contrôle des commutateurs. Ils permettent également de mettre en place des politiques de sécurité et de qualité de service pour les flux de données.

Malgré les avantages offerts par les réseaux SDN, ils sont également vulnérables à des attaques malveillantes. Certaines des attaques les plus courantes sur les réseaux SDN incluent l'injection de paquets malveillants, la falsification de messages OpenFlow, la saturation de la bande passante et le vol de données sensibles.

Dans ce chapitre, nous allons explorer les réseaux SDN, leur architecture, le protocole OpenFlow, les contrôleurs SDN et les principales attaques auxquelles ils sont confrontés. Nous allons également examiner les mesures de sécurité qui peuvent être mises en place pour protéger les réseaux SDN contre ces attaques.

2.2 Définition de SDN

"SDN signifie littéralement Software Defined Network c'est à dire le réseau définie par le logiciel" [5] .

Chaque constructeur définie le SDN selon ses problématique et ses éventuels intérêts, à cet effet il est plus au moins difficile d'avoir une seule définition du SDN [6] .

Toute fois les constructeurs rejoignent leurs idées, sur le fait d'introduire une abstraction entre le plan de transmission (c'est-à-dire de données) et le plan de contrôle, traditionnellement liés. Le plan de contrôle est chargé de prendre les décisions de gestion de trafic qui permettent au second plan de le transférer [10].

Cette séparation permet d'avoir un contrôle sur le réseau, l'objectif est de tirer avantage afin de réduire la complexité et de permettre une innovation complète sur les deux plans. [10].

En effet dans cette architecture, il n'est plus nécessaire d'y implémenter des protocoles de routage car les équipements réseau sont chargés de cette implémentation des règles de traitement des flux des données injectées par les applications [6] .

La programmation de flux permet une flexibilité sans précédent, limiter uniquement aux capacités des tableaux de flux mise en œuvre [12] .

"Le SDN est donc une architecture qui permet d'ouvrir le réseau aux applications en intégrant deux principes à savoir : d'une part accorder aux applications la programmation du réseau de telle sorte à accélérer le déploiement. En effet, l'automatisation de la configuration est beaucoup plus rapide et moins sujette aux erreurs en comparaison avec la configuration manuelle traditionnelle. D'autre part permettre au réseau de bien identifier les applications transportées pour mieux les gérer (qualité de service, sécurité, ingénierie de trafic...)" [6] .

2.3 Architecture de SDN

Un réseau traditionnel est généralement constitué d'équipements tels que des switchs et des routeurs qui assurent à la fois la transmission et le contrôle du réseau. Dans ce modèle d'architecture, il est difficile d'introduire de nouveaux services en raison de l'étroite dépendance entre le plan de contrôle et le plan de transmission. Pour favoriser l'innovation dans les équipements réseau, l'architecture SDN (Software-Defined Networking) a été développée. Elle permet de séparer la partie de contrôle de la partie transmission des équipements d'interconnexion, ouvrant ainsi la voie à de nouvelles possibilités d'innovation. Le SDN est composé

principalement de trois couches et d'interfaces de communication, nous décrivons dans ce qui suit ces couches, ainsi que les interfaces de communications : [13]

2.3.1 Couche infrastructure (transmission)

Également connue sous le nom de "plan de données", cette couche est constituée d'équipements d'acheminement tels que des switches et des routeurs. Son rôle principal est d'assurer la transmission des données et de recueillir des statistiques [13] .

2.3.2 Couche de contrôle

Également désignée sous le nom de "plan de contrôle", cette couche est principalement constituée d'un ou plusieurs contrôleurs SDN. Son rôle est de superviser et de gérer les équipements de l'infrastructure via une interface appelée "south-bound API" [13] .

2.3.3 Couche application

Cette couche représente les applications qui permettent le déploiement de nouvelles fonctionnalités réseau telles que l'ingénierie du trafic, la qualité de service (QoS), la sécurité, etc. Ces applications sont construites en utilisant une interface de programmation appelée "north-bound API"[13] .

,

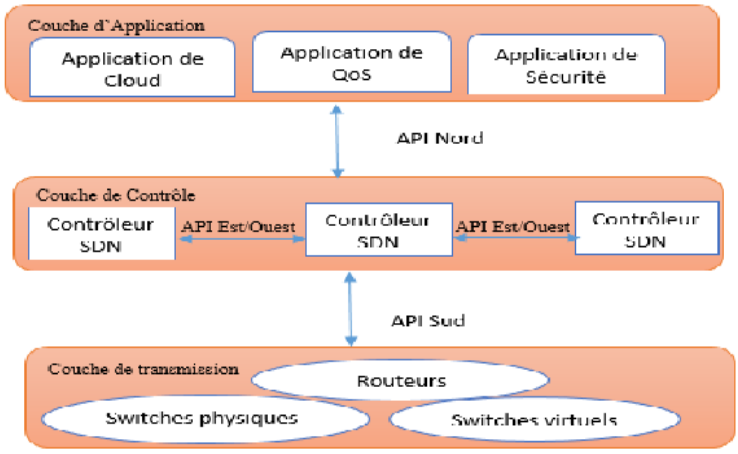

FIGURE 2.1 – Architecture SDN

2.3.4 Interfaces de communications

Dans l'architecture SDN (Software-Defined Networking), il existe plusieurs interfaces de communication qui permettent aux différentes couches de l'architecture de communiquer entre elles. Ces interfaces comprennent :

2.3.4.1 Interface sud

Les interfaces Sud, également connues sous le nom de Southbound APIs, permettent au contrôleur SDN d'établir une communication avec les équipements de la couche d'infrastructure tels que les switches et les routeurs. Le protocole le plus largement utilisé et déployé en tant qu'interface Sud est l'OpenFlow, qui a été standardisé par l'ONF. Sa dernière version est la 1.5, et des détails supplémentaires sur ce protocole seront fournis dans la prochaine section. Bien qu'il existe désormais d'autres alternatives d'interface Sud, comme ForCes ou Open vSwitch Database (OVSDB), le protocole OpenFlow reste le standard de facto qui est largement accepté et répandu dans les réseaux SDN [13] .

2.3.4.2 Interface nord

Les interfaces Nord sont utilisées pour programmer les équipements de transmission en exploitant l'abstraction du réseau fournie par le plan de contrôle. Contrairement à l'interface Sud, qui a été standardisée, l'interface Nord reste encore une question ouverte. Bien que la nécessité d'une telle interface standardisée fasse l'objet d'un débat considérable au sein de l'industrie, les avantages d'une API Nord ouverte sont également importants. Une API Nord ouverte permet plus d'innovation et d'expérimentation.Il existe plusieurs implémentations de cette interface, chacune offrant des fonctionnalités différentes. Parmi celles-ci, l'API RESTful est considérée comme l'interface Nord la plus répandue dans les réseaux SDN [13] .

2.3.4.3 interface est-ouest

Les interfaces Est/Ouest sont des interfaces de communication qui facilitent les échanges entre les contrôleurs dans une architecture multi-contrôleurs, permettant ainsi la synchronisation de l'état du réseau. Ces architectures sont relativement nouvelles et il n'existe actuellement aucun standard de communication inter-contrôleur disponible[13] .

2.4 Les avantages de SDN

2.4.1 Réseaux programmable

l'élément clé du SDN est l'aptitude à programmer le réseau, et cela en modifiant simplement une politique de haut niveau et non de multiple règles dans divers équipements de réseau [6] . de plus, la centralisation de la logique dans le contrôleur qualifie d'une personnalisation avec des connaissances globale et une puissance de calcul élevé, permet de simplifier des fonctions plus sophistiquées [11].

2.4.2 Flexibilité

SDN apporte également une grande flexibilité dans la gestion du réseau. Il devient facile de rediriger le trafic, d'inspecter des flux particuliers, de tester de nouvelles stratégies ou de découvrir des flux inattendus [18] .

2.4.3 Configuration automatique

Dans les réseaux SDN les programmes sont dynamiques, automatisés et développé par les administrateurs directement (ne dépendent pas de logiciels propriétaire). Et cela car SDN leurs permet de configurer, administrer, sécurisé et optimiser les réseaux rapidement grâce à ces programmes [6] .

2.4.4 Routage

SDN peut également être utilisé pour gérer les informations de routage de manière centralisée en déléguant le routage et en utilisant une interface pour le contrôleur [11].

2.4.5 Simplification matérielle

Le principe de SDN et d'utiliser des technologies standard pour contrôler les équipements du réseau, la puissance de calcul n'est requise qu'au niveau du contrôleur. Ainsi les équipements de réseau deviendront des produits à bas prix offrant des interfaces standard. Il serait plus simple d'ajouter de nouveaux périphériques, car ils ne sont pas spécialisés, de les connecter au réseau et de laisser les contrôleurs les gérer conformément a la politique définie. Par conséquent le réseau deviendra facilement évolutif dès que le contrôleur est évolutif [11].

2.4.6 Management centralisé

L'intelligence du réseau est centralisé dans le contrôleur SDN, qui maintien une vue globale du réseau.

2.4.7 Gestion de Cloud

SDN permet également une gestion simple d'une plateforme Cloud. En effet l'évolutivité, l'adaptation, ou des mouvements de machines virtuelles sont des problèmes lié au Cloud traité par la dynamique apportée par SDN.[11].

2.5 Protocole Openflow dans l'architecture SDN

OpenFlow est un protocole qui permet la liaison entre le plan de contrôle et le plan de données. Les messages sont échangés au cours d'une session TCP établie via le port 6633 du serveur contrôleur. OpenFlow est une composante du SDN, développée par l'université de Stanford et l'université de Californie à Berkeley. Un commutateur OpenFlow contient une ou plusieurs tables de flux où les en-têtes des paquets reçus sont comparés aux règles enregistrées.[25]

OpenFlow a été lancé en tant que projet à l'université de Stanford lorsque des chercheurs ont exploré des méthodes pour tester de nouveaux protocoles au sein du monde IP. L'objectif était de créer un réseau expérimental qui fonctionnerait en parallèle avec le réseau de production, permettant ainsi des tests sans interruption du trafic du réseau principal [17] .

C'est dans ce contexte que les chercheurs de Stanford ont découvert une méthode pour isoler le trafic de recherche du trafic du réseau de production, même s'ils utilisent le même réseau IP [17] .

Le résultat des travaux de recherche de l'équipe de Stanford a abouti à OpenFlow, un protocole ouvert conçu dans le but de séparer le trafic de recherche du trafic de production, chacun avec ses propres fonctionnalités et caractéristiques de flux distinctes [17] .

2.6 Contrôleurs SDN

Le contrôleur SDN (figure 2.2)permet de mettre en œuvre des modifications sur le réseau en traduisant une demande globale en une séquence d'opérations sur les équipements réseau, telles que l'ajout d'états OpenFlow ou la configuration en ligne de commande (CLI). Les ordres sont transmis au contrôleur par une application via une interface de programmation d'application (API) appelée "Northbound" ou nord. Le contrôleur communique ensuite avec les équipements via une ou plusieurs API dites "Southbound" ou sud. OpenFlow se présente comme une API sud qui agit directement sur le plan de données [14] .

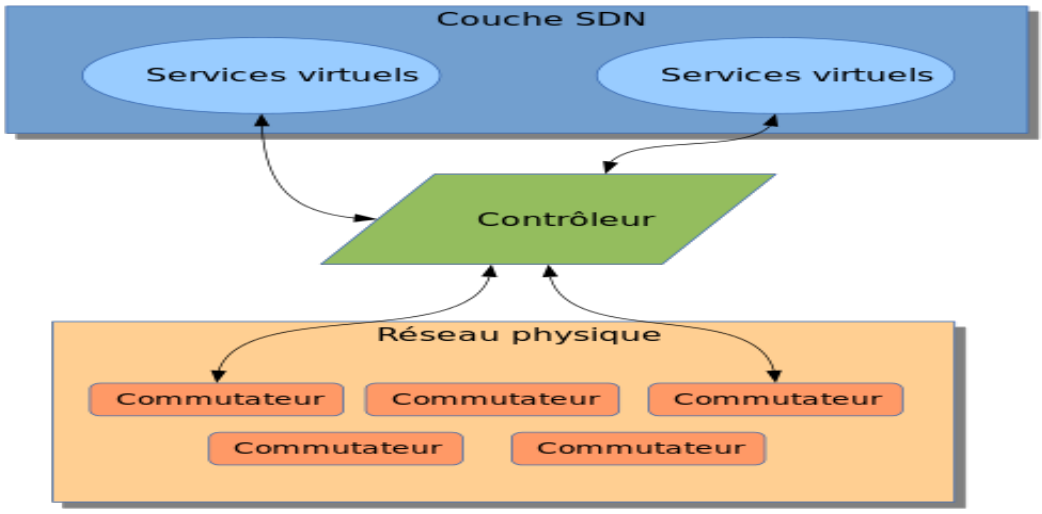

FIGURE 2.2 – Contrôleurs SDN

Il existe plusieurs contrôleurs SDN disponibles, dont certains parmi les plus populaires :

2.6.1 NOX

NOX est le premier contrôleur OpenFlow, a été initialement développé chez Nicira. Il est open-source et principalement codé en C++. En raison de sa large utilisation par de nombreux chercheurs, la plupart des applications SDN ou OpenFlow mentionnées dans les publications sont basées sur NOX.

Il offre un environnement convivial aux développeurs, ce qui facilite la modification des modules intégrés ou la création de nouveaux modules [20] .

2.6.2 POX

POX est le plus jeune frère de NOX. C'est un contrôleur open-source écrit en Python qui, tout comme NOX, offre un environnement pour le développement et le test d'un contrôleur OpenFlow. Cependant, les performances de POX sont considérablement inférieures à celles des autres contrôleurs, ce qui le rend inadapté au déploiement en entreprise [20] .

2.6.3 Beacon

Beacon, un contrôleur Java réputé pour sa stabilité, a été développé en 2010 et est continuellement maintenu. Il a été largement utilisé dans de nombreux projets de recherche. Grâce à ses excellentes performances, il constitue une solution fiable pour une utilisation dans des conditions réelles. De plus, ce contrôleur a également été intégré à d'autres projets tels que Floodlight ou OpenDaylight[20] .

2.6.4 Floodlight

Floodlight est un contrôleur OpenFlow open-source basé sur Java, développé par Big-Switch Networks. Il est distribué sous licence Apache [16]

Il est simple à configurer et offre des performances élevées. Grâce à ses nombreuses fonctionnalités, Floodlight peut être considéré comme une solution complète[20] .

2.6.5 OpenDaylight

OpenDaylight est un projet soutenu par l'industrie et hébergé par la Fondation Linux. Il s'agit d'un framework open source conçu pour faciliter l'accès aux réseaux définis par logiciel (SDN). De la même manière que Floodlight, il peut être considéré comme une solution complète [20] .

2.6.6 ONOS

ONOS est le principal contrôleur SDN open source qui permet de créer des solutions SDN de nouvelle génération.

Conçu pour répondre aux besoins des opérateurs, ONOS offre la possibilité de développer des solutions de classe opérateur en tirant parti de l'économie du matériel en silicium

marchand. Il offre également la flexibilité nécessaire pour déployer des services de réseau dynamiques avec des interfaces de programmation simplifiées.

ONOS assure à la fois la configuration et le contrôle en temps réel du réseau, ce qui élimine la nécessité d'exécuter des protocoles de routage et de contrôle de commutation à l'intérieur de l'infrastructure du réseau. Grâce à la centralisation de l'intelligence dans le contrôleur cloud ONOS, les utilisateurs bénéficient d'une plus grande capacité d'innovation et peuvent créer facilement de nouvelles applications réseau sans avoir à modifier les systèmes de plan de données.

Ce ne sont là que quelques exemples de contrôleurs SDN disponibles. Différents contrôleurs peuvent avoir des fonctionnalités, des capacités et des modèles de programmation différents.

2.7 Quelques attaques dans les réseaux SDN

2.7.1 Attaque de déni de service

2.7.1.1 Définition

Déni de service autrement dis DOS vise à paralyser le fonctionnement d'un serveur informatique ou toutes autres ressources en la saturant à outrance des requêtes erronées, tel qu'une bande passante, l'espace de stockage, la capacité de traitement d'une base de données, etc [6] . On trouve aussi des DDOS attaques de déni de service distribué. Ce sont des attaques très complexes car généralement il est difficile de découvrir la source de l'attaque ou de différencier une requête légitime d'une requête malicieuse. Cette attaque consiste à exploiter à distance plusieurs ordinateurs zombies infectés, à l'aide d'un virus de Cheval De Troie ou autre, pour attaquer simultanément la cible [6] .

FIGURE 2.3 – Attaque par déni de service distribué

2.7.1.2 Déni de service dans les réseaux SDN

Les attaques DOS sont due à la centralisation du contrôle dans l'architecture SDN, elles peuvent avoir de graves répercussions sur les performances du réseau allant jusqu'à l'incapacité du réseau à répondre aux besoins des utilisateurs. Ces attaques touchent les diffèrent élément du réseau SDN : Sur le plan de contrôle, en envoyant une grande quantité de flux, ce qui fera que le contrôleur sera surcharger et deviendra totalement paralyser et ne prendra aucune décision de routage. Sur le plat de données, là aussi l'attaquant inonde le commutateur avec des quantités de flux important. Le commutateur traduit le trafic de données reçu en règles de commutation fournit par le contrôleur une fois sa mémoire saturé il sera forer d'ajouter et de supprimer continuellement les règles de flux et d'envoyer plus de demandes vers le contrôleur. Par conséquent un retard dans le temps de transmission de données est engendrer. Sur la liaison contrôleur-commutateur, cette dernière sera exténuée et congestionnée à cause de la communication agressive entre le contrôleur et les commutateurs qui demandent des décisions de routage [6] .

2.7.2 Attaque de l'homme au milieu

2.7.2.1 Définition

Une attaque de l'homme au milieu ou Man In The Middle (MITM) en anglais, est l'une des techniques les plus courantes pour intercepter le flux de communication entre deux systèmes. Elle consiste à ce que l'attaquant se place au milieu d'un canal de communication et écouter, lire ou modifier le flux de données. Cette attaque peut avoir de nombreuses implications pour l'intégrité de l'ensemble du réseau [6] .

FIGURE 2.4 – Attaque de l'homme au milieu

2.7.2.2 MITM dans les réseaux SDN

L'attaque se produit au niveau du lien de transmission entre le contrôleur et les équipements d'infrastructure. Dans les paquets OpenFlow l'authentification n'existe pas ce qui permet à l'homme au milieu d'écouter le canal de communication entre le commutateur et le contrôleur et de capturer ainsi le trafic, le dupliquer et modifier les règles pour que tout passer par lui. Cela affectera l'intégrité et la confidentialité des données transitant sur le réseau.

2.7.3 Impact de la programmabilité sur la sécurité des SDN

La programmabilité en SDN est basée sur les applications logicielles qui programment le réseau, ce qui fait que l'attaquant peut parfaitement corrompre une application SDN pour reprogrammer le comportement des éléments du réseau. Les attaques de ce genre peuvent devenir persistantes car la programmabilité en SDN remplace entièrement la gestion du réseau par l'automatisation. Un attaquant peu injecter un code malicieux dans une application légitime réagir automatiquement aux événements du réseau. Cette application reprogramme dynamiquement les composants du réseau lorsqu'elle observe des évènements spécifiques. Les communications dans SDN doivent être sécurisées. Toutes ses interfaces et leurs protocoles doivent protéger les communications. Une interface vulnérable est une porte ouverte qui offre de grandes chances pour attaquer les composants de SDN [6] .

2.8 Conclusion

En conclusion, les réseaux SDN offrent une approche innovante de la conception des réseaux informatiques en permettant une gestion centralisée et simplifiée des réseaux. Leur architecture basée sur des commutateurs intelligents contrôlés par un contrôleur SDN centralisé permet une gestion plus flexible et dynamique des flux de données. Les contrôleurs SDN fournissent une interface centralisée pour la configuration et le contrôle des commutateurs, ainsi que la mise en place de politiques de sécurité et de qualité de service pour les flux de données. Cependant, malgré les avantages offerts par les réseaux SDN, ils sont vulnérables à des attaques malveillantes telles que l'injection de paquets malveillants, la falsification de messages OpenFlow, la saturation de la bande passante et le vol de données sensibles. Il est donc crucial de mettre en place des mesures de sécurité pour protéger les réseaux SDN contre ces attaques et assurer leur intégrité et leur disponibilité.

Chapitre 3

Présentation de l'organisme d'accueil

3.1 Introduction

L'étude de l'organisme d'accueil est une étape clé pour comprendre les contraintes auxquelles notre projet sera confronté. Dans ce chapitre, nous allons présenter l'entreprise TCHIN-LAIT, décrire ses différents départements et fournir des informations pertinentes pour notre approche du domaine et de l'environnement dans lequel nous souhaitons travailler.

3.2 Présentation de l'unité Tchin- Lait

Tchin-lait est une entreprise privée algérienne (SARL) fondée en 1999 par M. Fawzi BERKATI, qui en est le gérant. Elle est implantée sur le site de l'ancienne limonaderie Tchin-Tchin. À l'origine, Tchin-Tchin était une entreprise familiale spécialisée dans les boissons gazeuses depuis 1952, bénéficiant ainsi d'une longue expérience dans le conditionnement de produits liquides.

Face à l'arrivée des grandes multinationales sur le marché des boissons gazeuses, Tchin-Tchin a repensé sa stratégie et a décidé de se reconvertir dans la production de lait UHT (Ultra Haute Température). C'est ainsi qu'est née Tchin-lait, sous la marque "Candia", en mai 2001. La laiterie est construite sur une superficie totale de 6000 m2 et est située à l'entrée ouest de la ville de Bejaïa (Bir-Slam), le long de la route nationale n°12.

FIGURE 3.1 – Carte géographique.

3.3 Franchise CANDIA

L'entreprise TCHIN_LAIT a décidé de s'associer avec un professionnel du métier pour bénéficier de son savoir_faire et de son assistance. Ils ont choisi de devenir une franchise de la marque CANDIA, qui leur a apporté des compétences et des connaissances en matière de marketing, de notoriété, de prix, d'économies d'échelle et d'innovations. En signant un contrat de franchise avec CANDIA en 1999, TCHIN_LAIT a pu utiliser les marques et les formes distinctives de conditionnement et d'emballage de CANDIA, ainsi que leur savoir_faire en matière de fabrication, de marketing et de vente [14].

3.4 Organisation de TCHIN_LAIT

3.4.1 Situation juridique

L'entreprise TCHIN_LAIT a connu une croissance importante, mais son modèle organisationnel et structurel était considéré comme un frein à son expansion. En conséquence, l'entreprise a décidé de repenser son modèle organisationnel et a créé un groupe pour concentrer ses ressources, décentraliser la gestion et les responsabilités et bénéficier des avantages fiscaux accordés par la réglementation. L'année 2017 a été consacrée à la mise en œuvre de ces restructurations. C'est ainsi qu'il a été engagé et finalisé durant cette année là :

- La transformation juridique de TCHIN_LAIT Sarl, pour l'ériger en Société par Actions

- La filialisation en mars 2017 de la SPA Générale Laiterie Jugurtha
- L'augmentation du capital social de TCHIN_LAIT SPA
- L'absorption de Générale Laiterie Jugurtha par voie de fusion en dernière étape ; le 06 novembre 2017, accompagnée d'une nouvelle augmentation de capital

Dans le prolongement de cette réorganisation, deux nouvelles filiales dont TCHIN-LAIT est actionnaire majoritaire (90,1 %) ont été créées, au cours du 2ème trimestre, à l'effet de parachever le processus. Au terme de ce processus, TCHIN_LAIT dispose d'un capital social de 2 754 100 000 DA, entièrement libéré, se composant de 3 usines de production sises à BEJAIA, ALGER et SETIF, ainsi que de deux nouvelles filiales qui sont : [14]

3.4.1.1 TCHIN AGRO SPA

au capital de 20 Millions de DA, en charge du développement de la production de lait cru et de la collecte, localisée à Bordj Bou Arreridj et Msila pour l'agriculture.

3.4.1.2 TCHIN LOGISTIQUE SPA

avec pour mission de gérer et d'optimiser le parc transport et les flux matières et produits finis, dont le siège social est à OUED GHIR BEJAIA, qui a été cédé en 2020 [14].

3.4.2 Situation géographique

Le Groupe TCHIN_LAIT possède son Siège social dans le tissu urbain de Béjaia, à Bir SLAM et se répartit géographiquement comme suit [15] :

SPA TCHIN LAIT : regroupant les trois sites de production localisés respectivement à :

- BEJAIA : RN N° 12 Bir Slam
- ALGER : Zone d'activité Haouch El Amirate, BARA
- SETIF : Zone industrielle, Lotissement 163

SPA TCHIN AGR : deux sites situés à Bordj Bou Arréridj et Msila

SPA TCHIN LOGISTIQUE : un site situé à Oued Ghir.

3.4.3 Capacités de production

Le Groupe TCHIN_LAIT est dotée d'une capacité totale de 415 000 000 litres/an, tous produits confondus, dans différents conditionnements [14] :

- Brik de 1 Litre
- Brik de $\frac{1}{2}$ Litre
- Brik de 200 ml
- Brik de 125 ml

3.4.4 Evolution du chiffre d'affaire

Tchin_Lait est entrée en exploitation en mai 2001. Le graphe de la figure 3.2 représentent les évolutions de volumes depuis 2001 : [15]

FIGURE 3.2 – EVOLUTION DU CHIFFRE D'AFFAIRE

3.5 présentation du département informatique

Le département informatique THIN_LAIT est situé au deuxième étage de la direction générale. Il contient la salle machine où sont entreposé les armoires des serveurs et de brassage ainsi que les bureaux des quatre responsables informatique :

- Deux responsables du système d'information et des bases de données.
- Deux responsables de l'administration du réseau informatique [15] .

3.6 Étude de l'existant

Pour mener à bien l'étude de l'existant, nous avons procédé à une étude par site. La première tâche a été de rencontrer différent personnes qui entretiennent directement ou indirectement une relation avec le département informatique de TCHIN_LAIT. Il s'agit principalement de M. Raid BAROUTDJI responsable de service Réseaux ainsi que M.Massinissa MOUNSI responsable du service sécurité. Après quoi, nous avons réellement débuté le travail en menant différent recherches. Cette méthodologie de travail nous a permis d'avoir une connaissance large de l'existence.

3.6.1 Schéma général du réseau TCHIN_LAIT

réseau TCHINLAIT est partagé en sept sites (Site de Bejaia DG , Site de Bejaia-Oued Ghir ,Site de Bejaia-Aboudaou , Site de Bejaia-Akbou , Site de Setif , Site de Setif-Annexe , Site de Beraki)

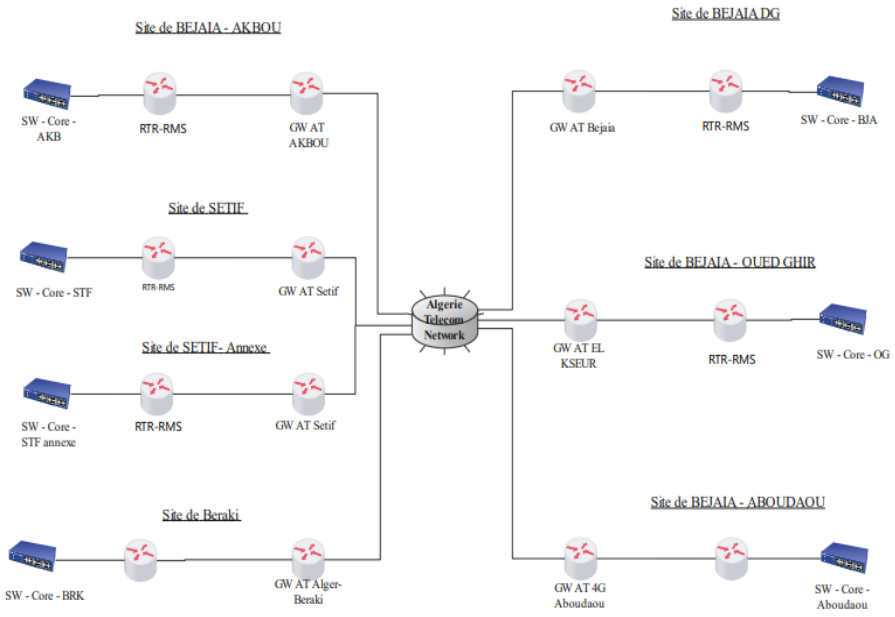

FIGURE 3.3 – Schéma Général du Réseau de TCHIN_LAIT

3.6.2 Le parc informatique TCHIN_LAIT

Le réseau Tchin-Lait contient un parc informatique composé d'une centaine d'ordinateurs (portables et bureaux), leurs configurations sont illustrés dans le tableau suivant :

Système d'exploitation	**RAM**	**Processeur**
Windows 10	4GO	INTELL Dual Core

TABLEAU 3.1 – Configurations des ordinateurs de Tchin-Lait

3.6.3 Les applications de TCHIN_LAIT

Les applications de Tchin-Lait sont diverses installées sur les serveurs contenus en salle machine, d'autres sur les machines des employés. Nous citons deux dans le tableau suivant :

Nom d'application	**Rôle**	**Description**
The Dude	Surveillance de réseau	The Dude est une application gratuite qui offre une très grande panoplie d'outils de surveillance de l'environnement réseau. Et en saisissant uniquement l'adresse d'une passerelle, The Dude est capable de dresser la carte de tous les composants réseau et d'en indiquer l'état ainsi que son Ping et éventuellement sa bande passante. Par simple glisser/déposer, il est possible de disposer les différents éléments selon leur configuration géographique et de les plaquer sur une carte pour une parfaite lisibilité.
WMS	Système de gestion d'entrepôts	C'est un logiciel qui sert à aider dans la gestion d'un entrepôt en utilisant les codes barre affecter aux lots de production, matières premières, etc.

TABLEAU 3.2 – Applications de Tchin-Lait.

3.6.4 Les serveurs de TCHIN_LAIT

Un serveur est un dispositif informatique matériels et logiciels, qui offre des services à différents clients. Les serveurs dont nous disposons dans le réseau de Tchin-Lait, présentent différentes caractéristiques énumérées comme suit :

Nom du serveur	**Rôle de serveur**	**Type de serveur**
Serveur FP	Serveur de base de données et fichiers partagés	Serveur HP ProlLiant ML350p Gen8
Serveur VID	Serveur de vidéo surveillance	Serveur HP ProlLiant ML350p Gen8
Serveur DOM	Contrôleur de domaines	Serveur HP ProlLiant ML350p Gen8
Serveur KAS	Serveur kaspersky	Serveur HP ProlLiant ML350p Gen8
Serveur MES	Serveur messagerie	Serveur HP ProlLiant ML350p Gen8
Serveur DON	serveur de base de données(ERP)	Serveur HP ProlLiant ML350p Gen8
Serveur ENT	Serveur du système de gestion d'entrepôts	Serveur HP ProlLiant ML350p Gen8
Serveur APP	Serveur qui contient quelques applications	Serveur HP ProlLiant ML350p Gen8

Tableau 3.3 – Serveurs du réseau Tchin-Lait.

3.6.5 Sites de stockages

Tchin-Lait se compose de plusieurs sites de stockages tels que site Usine, site Bouaoudia site de Simb, site de Yaici et site de Beraki ou sont stockés les produits finis qui sortes de la production et aussi les matières premières que vont être utilisées. Nous intéressons dans notre mémoire au site Usine qui est considéré comme la partie centrale du réseau. Le site Usine se compose de trois sites à savoir : direction générale, service technique, annexe qui sont reliés entre eux par fibre optique.

- **Liste des équipements de la direction générale**
  - **1. Equipements d'interconnexion de la direction générale**

Nom d'équipement	Type d'équipement	Modèles
Sophos	Routeur	Cisco
Routeur Cisco	Routeur	Cisco
Switch serveurs	Switch	Switch Cisco
Cisco Informatique	Switch	Switch Cisco
WDS usine	Assiette wifi	Bridge wifi
WMS DG	Point d'accès	AP-Motorol

Tableau 3.4 – Equipements d'interconnexion de la direction générale.

— **2. Equipements terminaux fixes de la direction générale**

Nom d'équipement	Type d'équipement	Modèles
CLP 620	DG Imprimante IP	SAMSUNG CLP 620
ZEBRA	Imprimante IP	ZEBRA
imprimante	Imprimante	ECOSYS P3145dn

Tableau 3.5 – Equipements terminaux fixes de la direction générale.

— **Liste des équipements du service technique**

— **1. Equipements d'interconnexion du service technique**

Nom d'équipement	Type d'équipement	Modèles
Cisco fédérateur	Switch	Cisco
Routeur Cisco	Switch	Switch Cisco
Cisco Technique	Switch	Switch Cisco
Cisco DAG	Switch	Switch Cisco
NetGear Archives	Switch	Switch Cisco
WMS Usine 1	Point D'accès	AP-Motorol
WMS Usine 2	Point D'accès	AP-Motorol
WMS Usine 3	Point D'accès	AP-Motorol
WMS Usine 4	Point D'accès	AP-Motorol
WMS Usine 5	Point D'accès	AP-Motorol

Tableau 3.6 – Equipements d'interconnexion du service technique.

— **2. Equipements terminaux fixes du service technique**

Nom d'équipement	Type d'équipement	Modèles
Prod 1	imprimante IP	ZEBRA
Prod 2	imprimante IP	ZEBRA
ML2850 Technique	imprimante IP	SAMSUNG 2850
CLP620 Personnel	imprimante IP	SAMSUNG CLP 620
MFC7460 DAG	imprimante IP	BROTHER 7460
ML3470 Chefs	imprimante IP	SAMSUNG 3470

TABLEAU 3.7 – Equipements terminaux fixes du service technique.

— **Liste des équipements de l'annexe**

— **1. Equipements d'interconnexion de l'annexe**

Nom d'équipement	Type d'équipement	Modèles
Cisco CDB	Switch	Switch Cisco
Switch	Switch	Switch Cisco
Switch	Switch	Switch Cisco
ProCure Switch	Switch	Switch Cisco
AP DMV	Point D'accès	AP-Motorola
WMS CDB1	Point D'accès	AP-Motorola
WMS CDB2	Point D'accès	AP-Motorola
WMS CDB3	Point D'accès	AP-Motorola
WMS CDB4	Point D'accès	AP-Motorola
WMS CDB5	Point D'accès	AP-Motorola
WMS CDB6	Point D'accès	AP-Motorola
WMS CDB7	Point D'accès	AP-Motorola

TABLEAU 3.8 – Equipements d'interconnexion de l'annexe.

— **2. Equipements terminaux fixes de l'annexe**

Nom d'équipement	**Type d'équipement**	**Modèles**
ML3710 CDB	imprimante IP	SAMSUNG 3710
Zebra CDB	imprimante IP	ZEBRA
HL22370 DMV	imprimante IP	BROTHER 2270
CLP660 DMV	imprimante IP	SAMSUNG 660
CLP660 Appros	imprimante IP	SAMSUNG 660
ML3710 GDS	imprimante IP	SAMSUNG 3710
ML2850 DFC	imprimante IP	SAMSUNG 2850
HL2270Idjraou	imprimante IP	BROTHER 2270
ML 3470 Bounia	imprimante IP	SAMSUNG 3470
Pointeuse Annexe	Pointeuse	ZKSOFTWARE

TABLEAU 3.9 – Equipements terminaux annexes.

3.7 Problématique

Lors de notre stage à l'entreprise TCHIN_LAIT, nous avons constaté qu'ils disposent d'un réseau local avec énormément d'équipement réseaux, a savoir des dizaines de switchs et routeurs, plein de serveurs plus un firewall.Nous avons constater certains problème :

-Leur configuration prends un temps considérable.

-Risque d'erreur humain lors de la configuration.

-Grand nombre d'effectif pour la vérification de la configuration.

-Réseau nos centraliser.

-Sécurité faible a cause du grand nombre d'équipements réseaux, et le nombre d'accès pour chaque équipement.

-L'évolution : la technologie informatique évolue donc l'entreprise dois suivre cette évolution.

3.8 Solution

Le principal défi d'une architecture de réseau virtualisé est de garantire sa sécurité. Pour ce faire,nous avons proposé une solution SDN facile a implimenté, avec le contrôleur ONOS . Notre choix c'est porter sur ce controleur de SDN pour ses différents caractéristique qui répond aux problèmes que nous avons déjà mentionnés :

-SDN permet la centralisation du réseau, c'est à dire que la configuration des réseau se fait sur un seul équipement (le contrôleur sdn) qui assurera la configuration de tout les autres.

-Le SDN permet de programmer et de configurer le réseau de manière flexible à l'aide d'interfaces de programmation (API). Cela facilite l'automatisation et la personnalisation du réseau pour répondre aux besoins spécifiques.

-Le SDN facilite l'orchestration et l'automatisation du réseau, ce qui permet de déployer rapidement de nouveaux services et de gérer efficacement les ressources réseau.

-Le SDN permet d'optimiser les performances du réseau en offrant une visibilité et un contrôle granulaires sur le trafic. Les politiques de contrôle peuvent être adaptées en temps réel pour garantir des performances optimales.

- A l'aide du contrôleur ONOS, toutes les configuration seront faites par l'injection des scriptes sur le contrôleurs.

-L'interface graphique de ONOS nous permettera de visualiser et la topologie de notre réseau et les différentes actions des utilisateurs.

-Réduire les investissements en matériel et en infrastructure.

3.9 Conclusion

L'étude de l'existant nous a permis de constater que le réseau existant utilise une technologie avancée, mais pourrais être plus a point. On entend par la l'automatisation . en effet, pour être a jour avec l'évolution de la technologie, il faudrait songer a un réseau plus virtuel et automatisé ; d'où notre proposition de mettre en place une solution SDN.

Chapitre 4

Implémentation d'une solution SDN

4.1 Introduction

Le chapitre présent a pour objectif d'améliorer l'architecture réseau de l'entreprise CANDIA . Nous détaillerons les outils que nous utiliserons , les installations et configurations nécessaires. Nous y aborderons les différentes étapes pour mettre en place la solution proposée dans le chapitre 3.

4.2 Environnement de travail

4.2.1 Présentation de logiciel de simulation

Dans ce qui suis, nous allons présenter les outils de travail que nous avons utilisés pour mener à bien notre solution.

4.2.1.1 VMware

VMware Workstation est un logiciel de virtualisation largement adopté permettant aux utilisateurs de faire fonctionner plusieurs machines virtuelles sur un seul ordinateur physique. Développé par VMware, il est disponible pour les systèmes d'exploitation Windows et Linux. Ce logiciel est fréquemment utilisé par les développeurs, les professionnels de l'informatique et les administrateurs système pour créer et gérer des environnements virtualisés dans un but de test, de développement et de production .

FIGURE 4.1 – Logo de VMware Workstation

Installation de VMware Workstation Pro version 15 Pour pouvoir créer des machines virtuelles sur un même ordinateur, il est nécessaire d'installer VMware Workstation. Une fois l'installation de VMware terminée, une page d'accueil s'affichera .

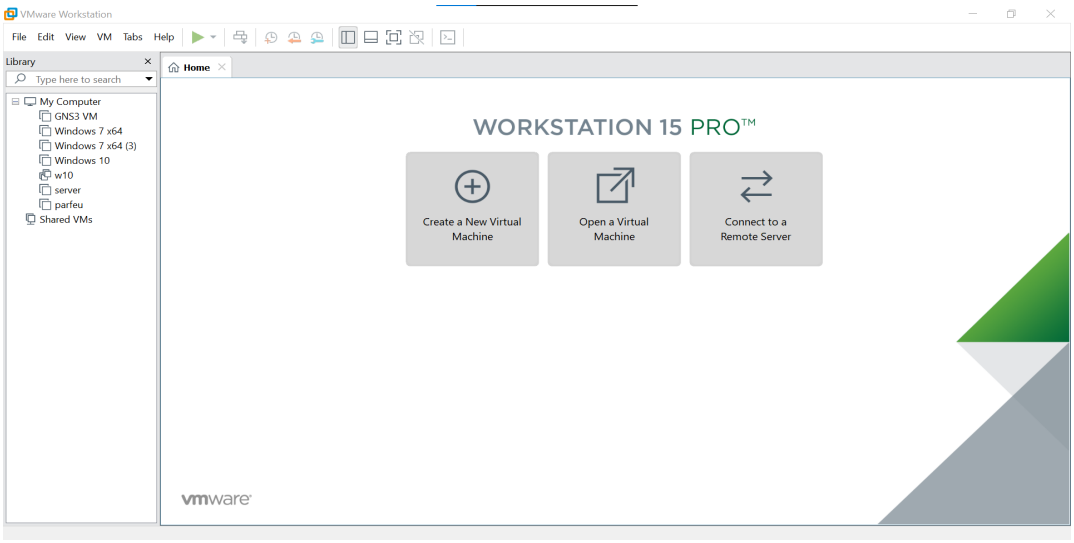

FIGURE 4.2 – Interface de VMWare Workstation Pro version 15

4.2.1.2 SecureCRT

SecureCRT est un logiciel disponible sur Windows, Mac et Linux, qui offre une émulation de terminal fiable aux professionnels de l'informatique. Il améliore la productivité grâce

à des fonctionnalités avancées de gestion des sessions et à plusieurs méthodes permettant d'économiser du temps et de simplifier les tâches répétitives. SecureCRT permet un accès à distance sécurisé, le transfert de fichiers et la création de tunnels de données, bénéfiques pour tous les membres de votre organisation.

4.2.1.3 Mininet

Mininet est une plateforme SDN largement utilisée par les chercheurs en raison de sa flexibilité, de sa disponibilité et de sa simplicité. Elle est spécifiquement dédiée à l'architecture OpenFlow. Dans Mininet, les utilisateurs ont la possibilité de créer, personnaliser et partager différentes topologies composées de contrôleurs, de commutateurs, de routeurs, de liens et d'hôtes virtuels, et de les tester facilement. Mininet inclut des topologies prédéfinies courantes telles que les topologies simples, linéaires et arborescentes. De plus, il est possible de créer des topologies personnalisées. Mininet peut être connecté à un contrôleur distant, et des contrôleurs locaux sont également disponibles. La documentation de Mininet est accessible sur le site officiel Mininet.

FIGURE 4.3 – Logo de Mininet

La figure suivante nous montre Mininet installé

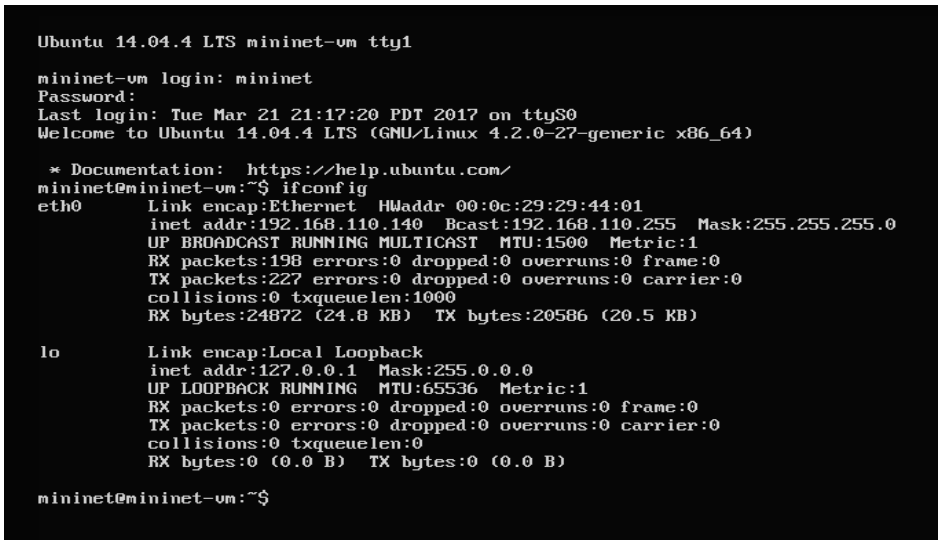

FIGURE 4.4 – Mininet installé

On aura besoin du client secureCRT afin de réaliser les commandes dessus directement.

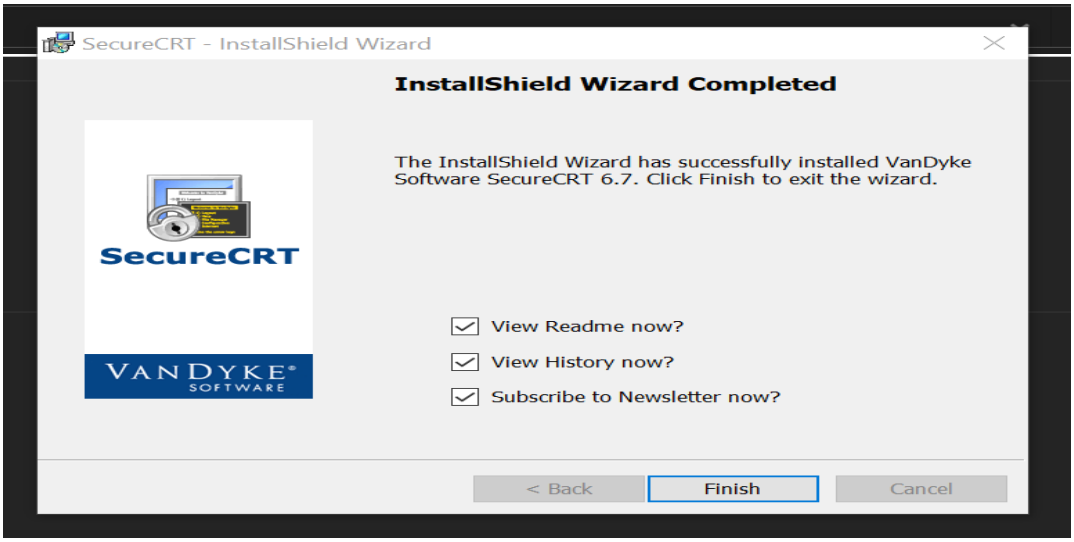

FIGURE 4.5 – Installation de SecureCRT

A présent, il faut le configurer pour qu'il se connecte à Mininet.

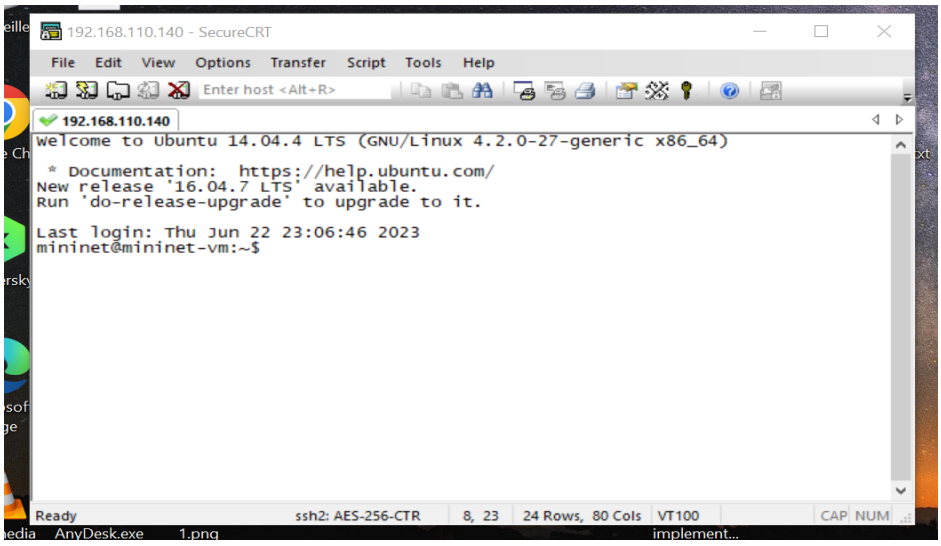

FIGURE 4.6 – SecureCRT connecté à Mininet

4.2.1.4 Installation ONOS

Pour l'installation du contrôleur ONOS, elle sera faite par des commandes sur le terminal de UBUNTU. L'interface est représenté par la figure suivante

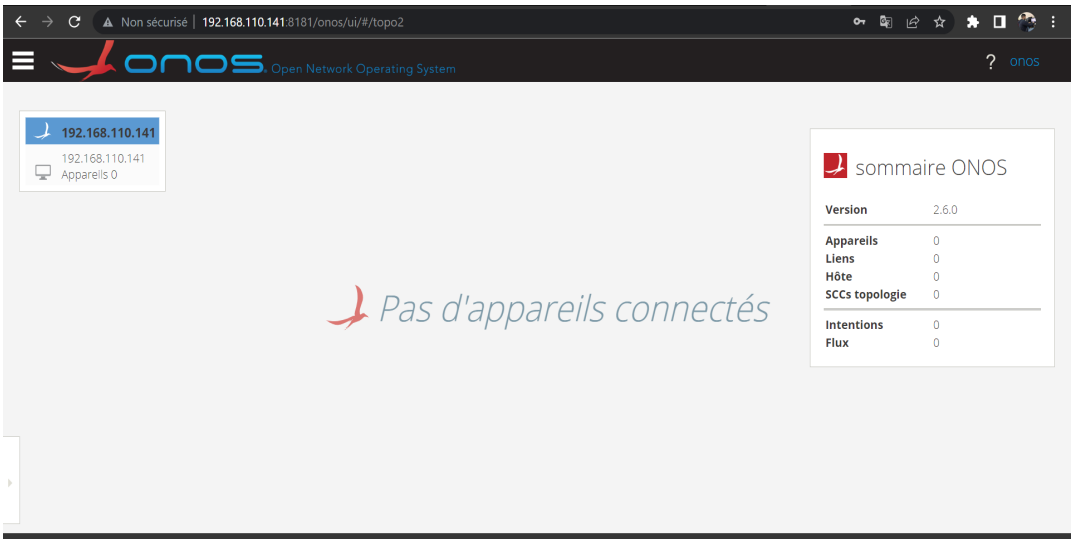

FIGURE 4.7 – Interface onos

4.2.1.5 Etape 1 : création de l'utilisateur

on a créé un utilisateur avec la commande <sudo adduser sdn –system –group>

4.2.1.6 Etape 2 : Installation de java

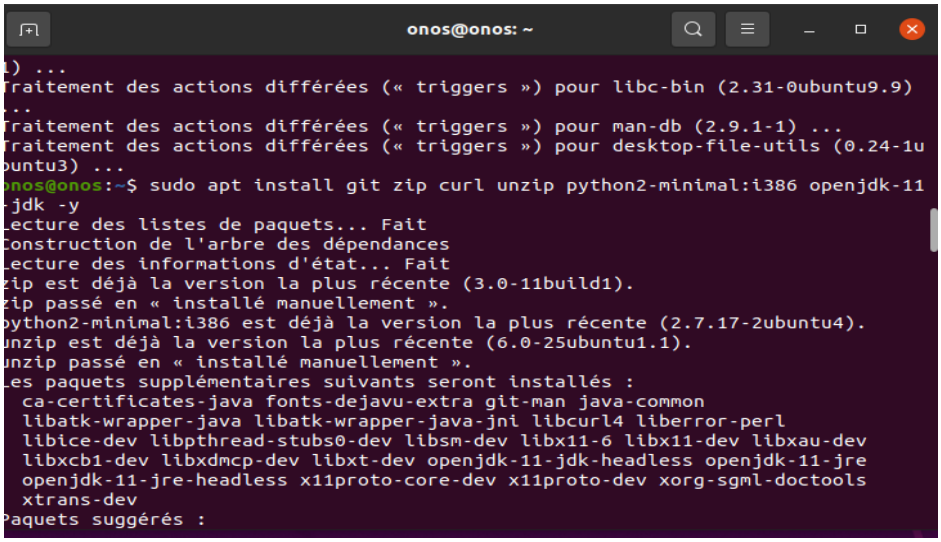

FIGURE 4.8 – Installation de java ONOS

4.2.1.7 Etape 3 : Installation du package MAVEN

En suivant les commandes illustrées dans la figure 4.9

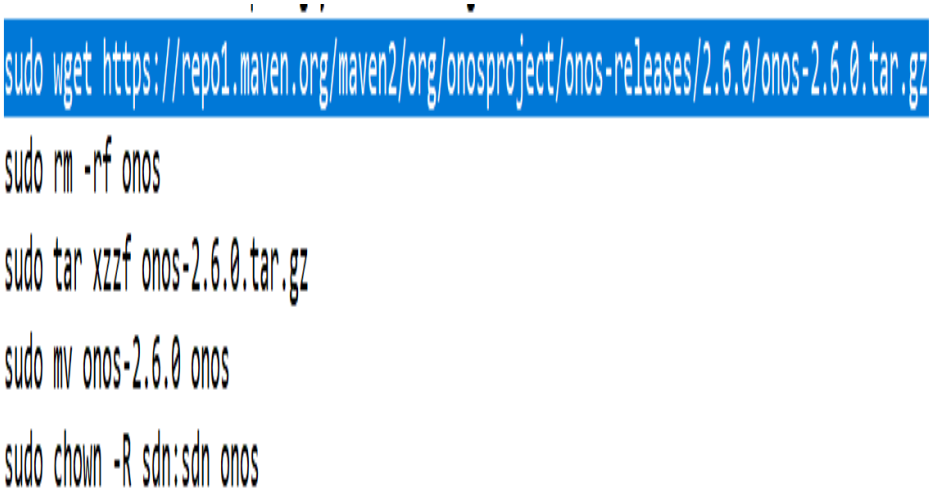

FIGURE 4.9 – Installation package MAVEN

4.2.1.8 Etape 3 : définition des options de démarrage

La figure 4.10 montre les informations saisies.

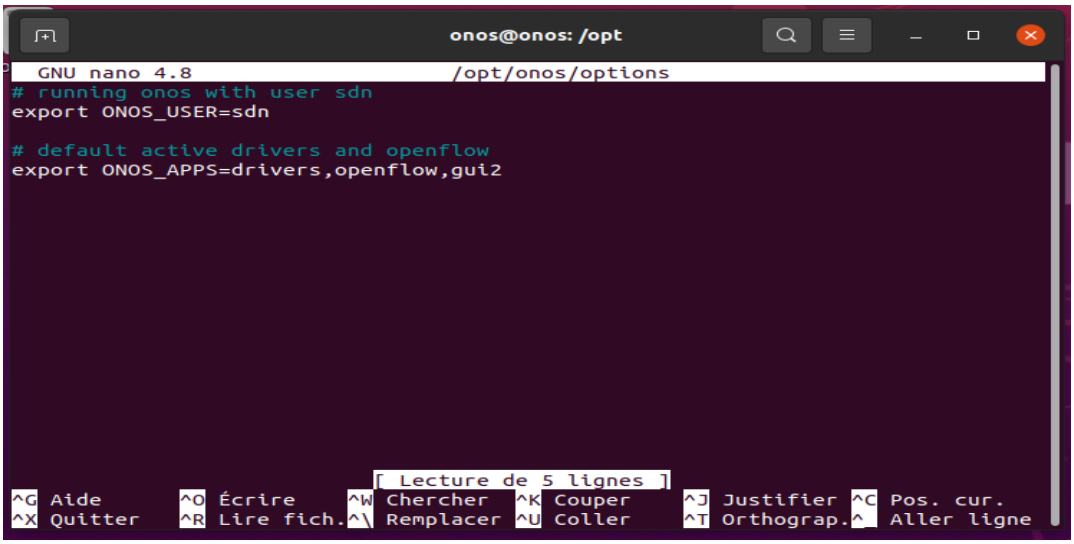

FIGURE 4.10 – Options de démarrage

4.2.1.9 Etape 4 : Start ONOS

Avec les commandes suivantes <sudo systemctl start onos> <sudo systemctl status onos>

Ensuite aller sur le navigateur et entrer par l'adresse de ONOS

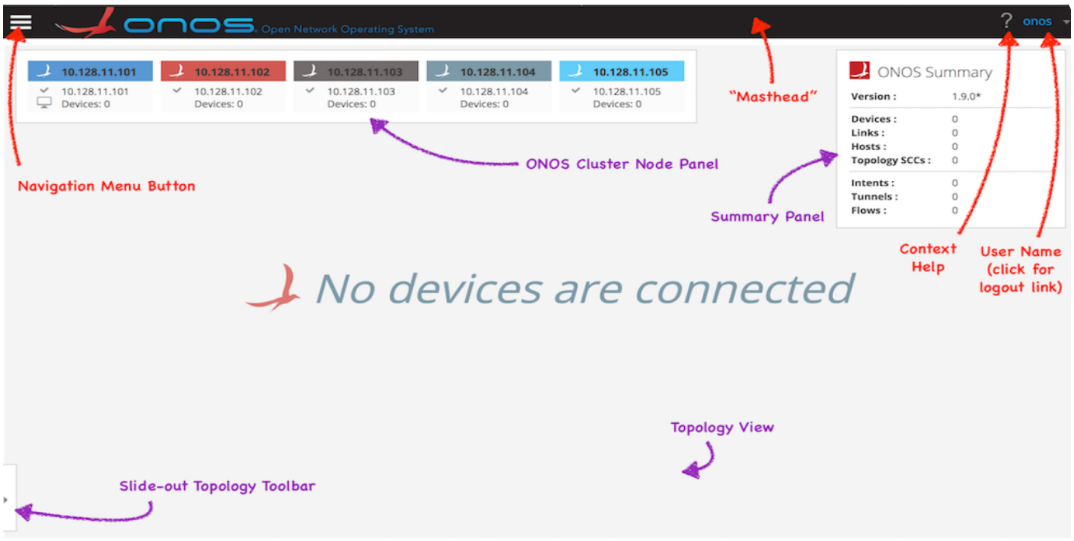

FIGURE 4.11 – Login ONOS

4.2.2 Serveur DHCP

est un protocole réseau qui attribue dynamiquement des adresses IP aux machines connectées à un réseau. Il fournit également d'autres paramètres réseau : masque de sous-réseau, adresse IP de la passerelle et DNS [8].

4.2.3 Serveur DNS (Domaine Name System)

est un protocole qui permet de convertir un nom de domaine en adresse IP pour simplifier la gestion de réseau.

4.2.4 Partie Hardware

4.2.4.1 Une carte réseau

est un élément matériel informatique de couche 1 du modèle OSI qui fournit l'interface entre le réseau et l'équipement.

4.2.4.2 Commutateur (Switch)

est un équipement d'interconnexion réseau de niveau 2 du modèle OSI. Il permet de rediriger les informations reçues seulement vers le port de la machine concernée [4].

4.2.4.3 Routeur (router)

est un périphérique réseau informatique de couche 3 du modèle OSI qui assure le routage des paquets de données [3].

4.2.5 Partie Software

4.2.5.1 Système linux

est un système d'exploitation open source qui représente l'interface entre l'application et le matériel [2].

FIGURE 4.12 – Logo linux

4.2.5.2 IOS

abréviation de Internetwork Operating System, « système d'exploitation pour la connexion des réseaux »), anciennement IOS, est le système d'exploitation produit par Cisco Systems et qui équipe la plupart de ses équipements. Cisco IOS fournit les principes unificateurs autour desquels un interréseau peut être maintenu de manière rentable dans le temps. Il s'agit d'une architecture logicielle, dissociée du matériel, qui peut être mise à niveau de manière dynamique pour s'adapter à l'évolution des technologies (matérielles et logicielles) à mesure qu'elles évoluent au sein d'une infrastructure réseau. Cisco IOS peut être considéré comme un cerveau d'interconnexion de réseaux, un administrateur hautement intelligent qui gère et contrôle des ressources et des fonctions réseau complexes et distribuées[1] .

4.2.5.3 Ubuntu

Ubuntu est probablement la plus populaire des distributions Linux avec Debian. C'est un système d'exploitation libre et open-source. Il fonctionne sur un ordinateur physique ou dans une machine virtualisée et se divise en 3 éditions : core, server et desktop. Le système d'exploitation se trouve donc sur une multitude d'appareils allant de l'ordinateur personnel au serveur internet. Il est caractérisé par son installation facile.Ubuntu est connu pour ses différentes versions, Ubuntu est connu pour ses différentes versions, et pour notre étude, nous avons choisi la version 20.04.(voir annexe2)

4.3 Équipements utilisés

4.3.1 Caractéristique du PC utilisé pour l'implémention

Pour l'implémentation de ce projet, nous avons utilisé un PC DELL équipé d'un processeur Intel Core i7 de 7e génération, une RAM de 8 Go et un disque dur SSD de grande capacité. De plus, sa carte graphique performante permet de manipuler des virtualisations complexes et de réaliser des analyses graphiques avancées. En ce qui concerne le système d'exploitation, il fonctionne sous Windows 10, assurant une compatibilité optimale avec les logiciels utilisés dans notre mémoire.

4.3.2 Open vSwitch (OVS)

Open vSwitch (OVS) est un commutateur virtuel de qualité de production, utilisant une licence open source Apache 2.0, qui dispose de nombreuses couches de données. Il est spécialement conçu pour permettre une automatisation massive de réseau avec une extension programmable, tout en étant capable de supporter des interfaces et des protocoles de gestion standards tels que IPFIX, RSPAN, CLI,et LACP. De plus, il a été créé pour prendre en charge la distribution sur plusieurs serveurs physiques, ce qui est similaire au vswitch distribué vNetwork de VMware ou au Nexus 1000V de Cisco [30].

4.3.2.1 Composantes d'Open vSwitch

Comme illustré sur la figure, OVS est composé principalement des éléments suivants :

- Un serveur de base de données qui stocke diverses configurations du commutateur. Cela permet de maintenir un comportement cohérent du switch au-delà de son redémarrage, et peut être atteint via la commande ovsdb-server.

- Le répertoire d'OVS est le processus principal qui permet la communication avec le contrôleur via OpenFlow, ou la récupération des données à partir de la base de données. Il peut être atteint via la commande ovs-vswitchd.

- Le Kernel est le coeur du système d'exploitation et la partie qui commute les paquets.

La communication des utilisateurs avec ces composants est une étape importante dans la mise en œuvre d'Open vSwitch qui peut être atteinte via la commande openvswitch.ko (Module Kernel). Trois outils d'espace utilisateur - ovs-vsctl, ovs-ofctl et ovs-dpctl - sont

disponibles pour configurer et surveiller l'état du commutateur. Chacun de ces outils fournit un ensemble de commandes pour interagir avec le commutateur.

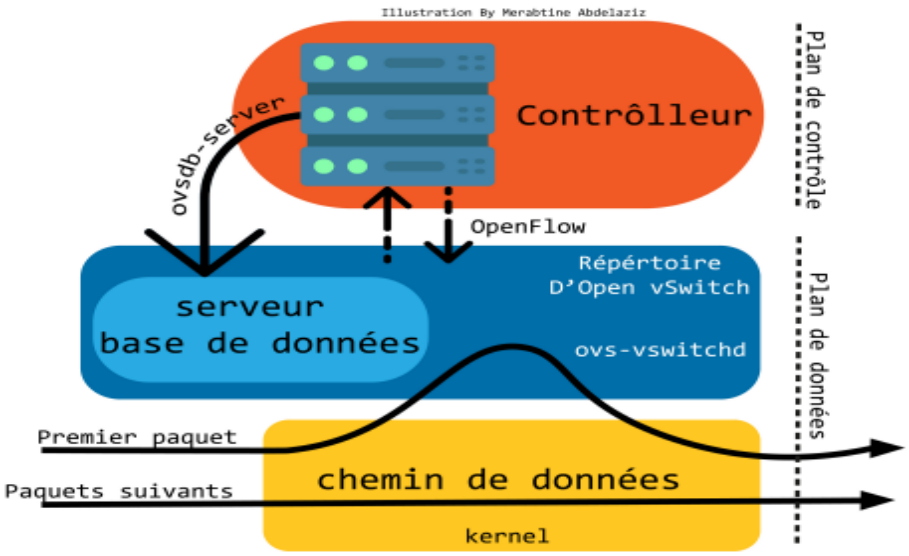

FIGURE 4.13 – OpenVSwitch

4.3.2.2 Fonctionnement d'Open vSwitch

Open vswitch permet de créer des bridges virtuels entre plusieurs VMs pour les relier ensemble tout en garantissant un isolement complet entre les bridges. Cela permet de créer plusieurs réseaux indépendants sur une même machine physique. Pour configurer l'OVS on communique avec ses différentes composantes en utilisant les outils de l'espace utilisateur.

4.3.3 Openflow Manager

Le Software Defined Networking (SDN) implique une application qui interagit avec un réseau composé d'appareils spécifiques à un domaine, dans le but de simplifier les opérations ou d'activer un service. Un contrôleur est placé entre l'application et le réseau, et interagit avec les éléments du réseau (par exemple, les commutateurs) dans la direction sud en utilisant une variété de protocoles différents. Le contrôleur présente une abstraction du réseau en utilisant des API REST communes dans la direction nord. ONOS est le contrôleur utilisé pour cette application. OpenFlow Manager (OFM) est une application qui utilise cette innovation pour gérer le réseau OpenFlow.

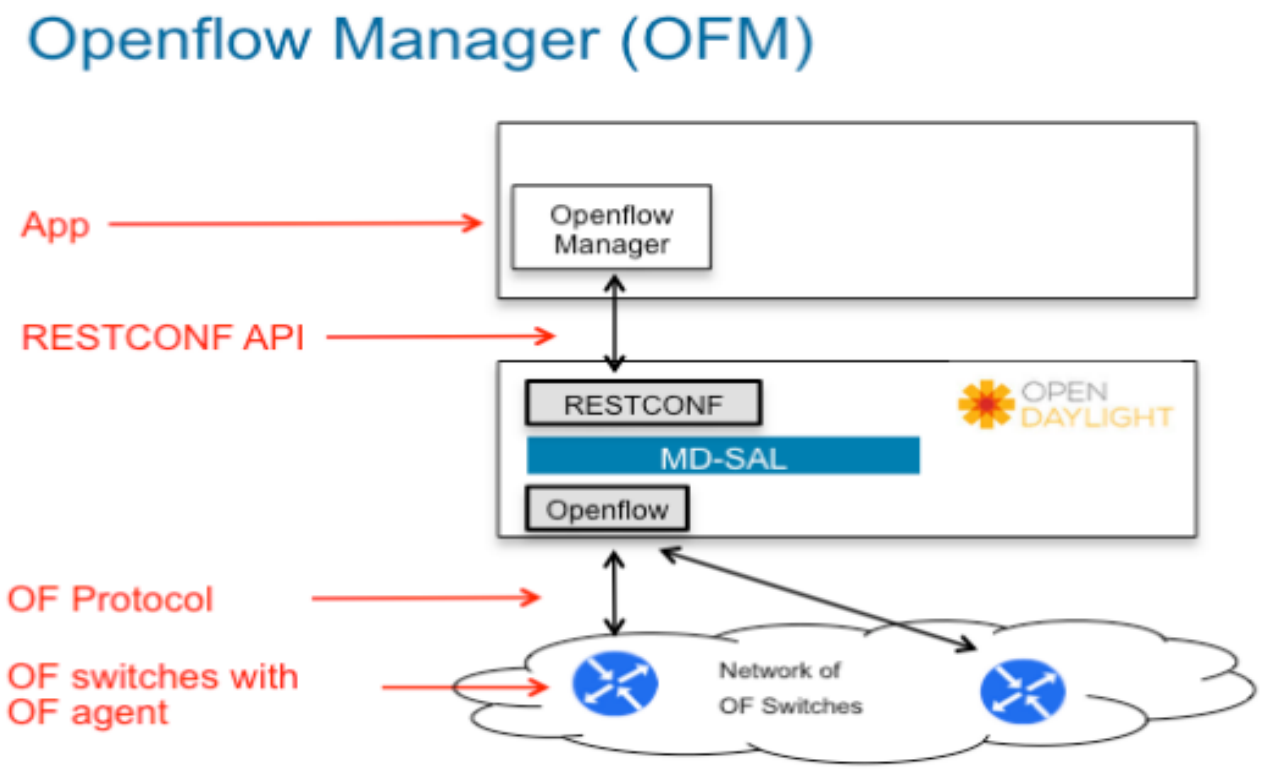

FIGURE 4.14 – OpenFlowManager

4.4 Topologie du réseau

La configuration de la topologie est conçue pour s'adapter à la structure de l'entreprise CANDIA, qui suit la topologie d'un centre de données (Data Center). Dans notre exemple, nous avons considéré une entreprise composée de 3 départements.

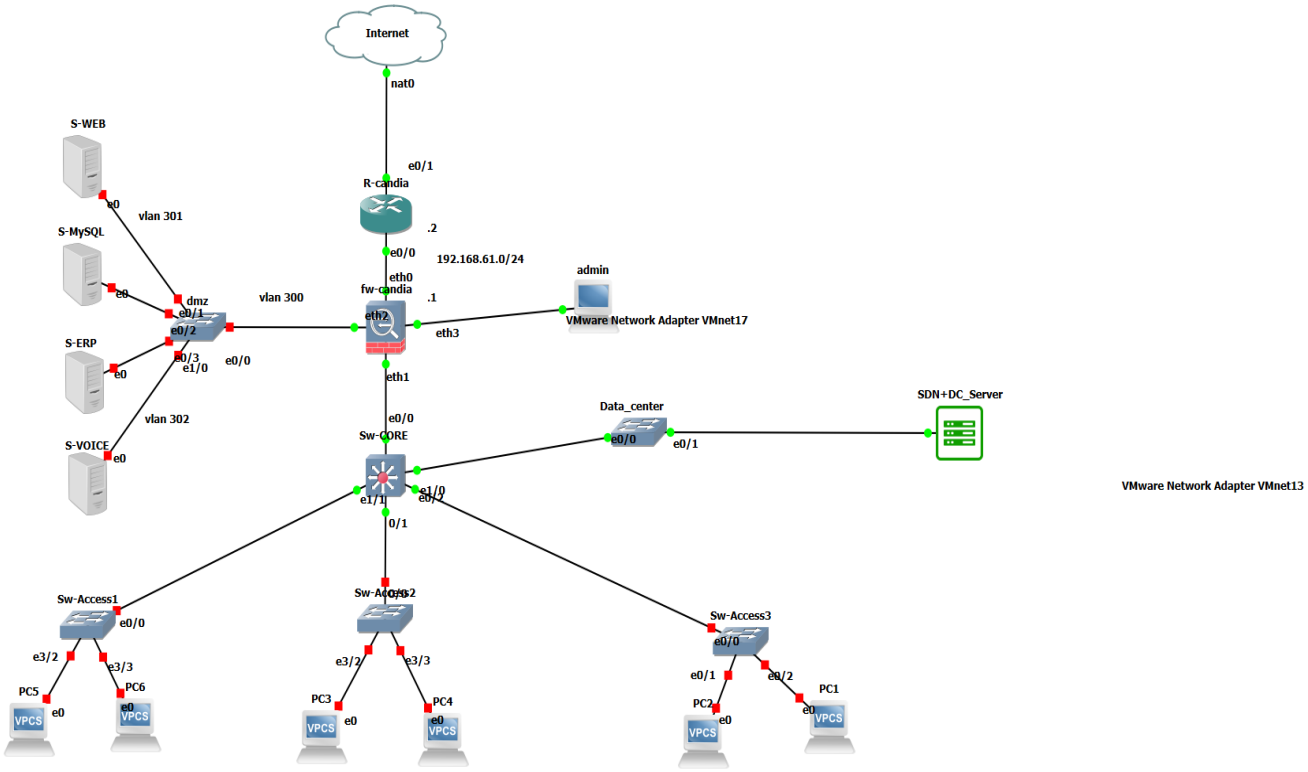

FIGURE 4.15 – Architecture

4.5 Création et exécution du scénario de la topologie

Dans cette section, nous présentons les efforts expérimentaux déployés pour évaluer l'expérience de mise en réseau SDN utilisant Mininet avec le contrôleur ONOS. Pour l'installation des flux dans ONOS, nous avons choisi d'utiliser l'API REST. Cette décision est principalement motivée par la visibilité offerte par les interfaces graphiques des applications, ce qui facilite la création et la suppression de flux installés. Il est possible d'installer différentes règles, que ce soit au niveau de la couche 2 ou de la couche 3 du modèle OSI, pour chaque Vswitch.

Pour lancer Mininet, utilisez la commande suivante : "sudo mn". Un large éventail d'options est disponible et peut être consulté en ajoutant le drapeau "-h". Mininet offre une interface en ligne de commande qui permet d'observer l'état du réseau et d'effectuer des tests. Voici les commandes principales pour créer différents types de topologies :

4.5.1 La ligne de commande de Mininet

Pour lancer Mininet, utilisez la commande suivante : "sudo mn". Un large éventail d'options est disponible et peut être consulté en ajoutant le drapeau "-h". Mininet offre une interface en ligne de commande qui permet d'observer l'état du réseau et d'effectuer des tests. Voici les commandes principales pour créer différents types de topologies :

Grâce à la commande mn et la multitude d'options offertes par l'émulateur, il est possible de réaliser différentes formes de topologies et de réseaux virtuels

4.5.2 Via l'API Mininet

Mininet, l'émulateur de réseau, propose une interface de programmation en Python. L'une des utilisations de cette interface consiste à créer des topologies personnalisées en définissant toutes les caractéristiques souhaitées des éléments du réseau. Cette approche présente l'avantage d'optimiser l'utilisation du temps et des ressources de la meilleure façon possible. Le fichier Python contenant la topologie doit être sauvegardé dans le répertoire "/mininet/custom". De plus, pour pouvoir appeler la topologie en utilisant l'option "–custom", la dernière ligne du script est essentielle. Les principales commandes du code Python permettant de créer la topologie réseau souhaitée sont les suivantes

build() : La méthode à surcharger pour créer des topologies personnalisées.

addSwitch() : Ajoute un switch et retourne son nom.

addHost() : Ajoute un hôte et retourne son nom.

addLink() : Ajoute un lien bidirectionnel entre les composants passés en argument.

start() : Démarre le réseau.

stop() : Arrête le réseau

4.5.3 Création des hôtes

sur SecureCRT, après connections avec Mininet ; les commande <cd mininet> <cd custom/> et <ls> nous permettrons d'accéder au scripte prédéfini ou nos modification serons porter selon le besoin.

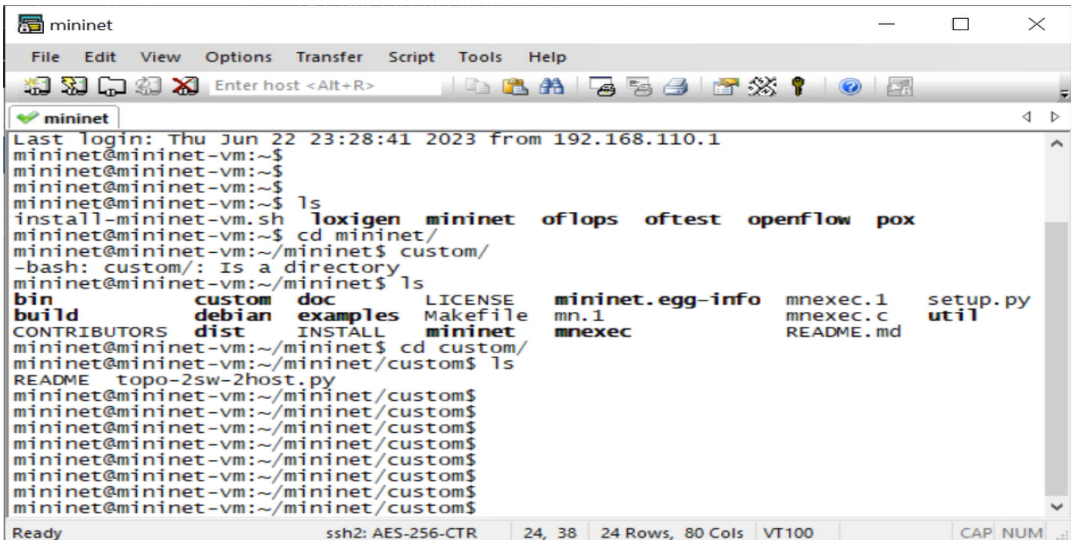

FIGURE 4.16 – Commandes

le scripte est le suivant

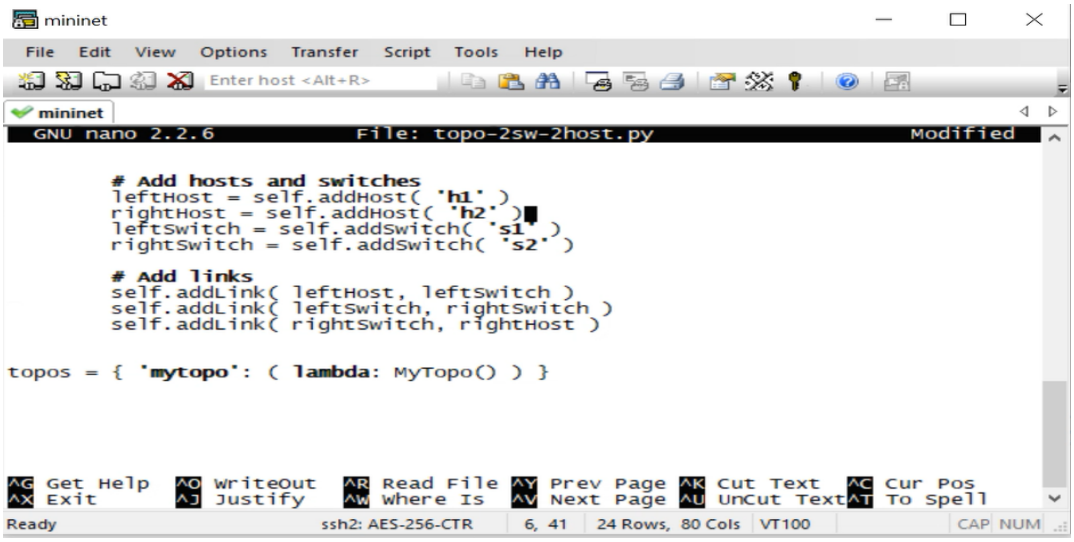

FIGURE 4.17 – Scripte 1

4.6 Mise en place de la topologie avec Mininet

Pour ce faire, il faut taper la commande suivante

```
mininet@mininet-vm:~/mininet/custom$ sudo mn --custom topo-2sw-2host.py --topo mytopo --controller=remote,ip=192.168.110.141:6633
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1 s2
*** Adding links:
(h1, s1) (s1, s2) (s2, h2)
*** Configuring hosts
h1 h2
*** Starting controller
```

FIGURE 4.18 – Commande sur Mininet

Ensuite, il faudera installer un package sur la platforme ONOS ongle application.

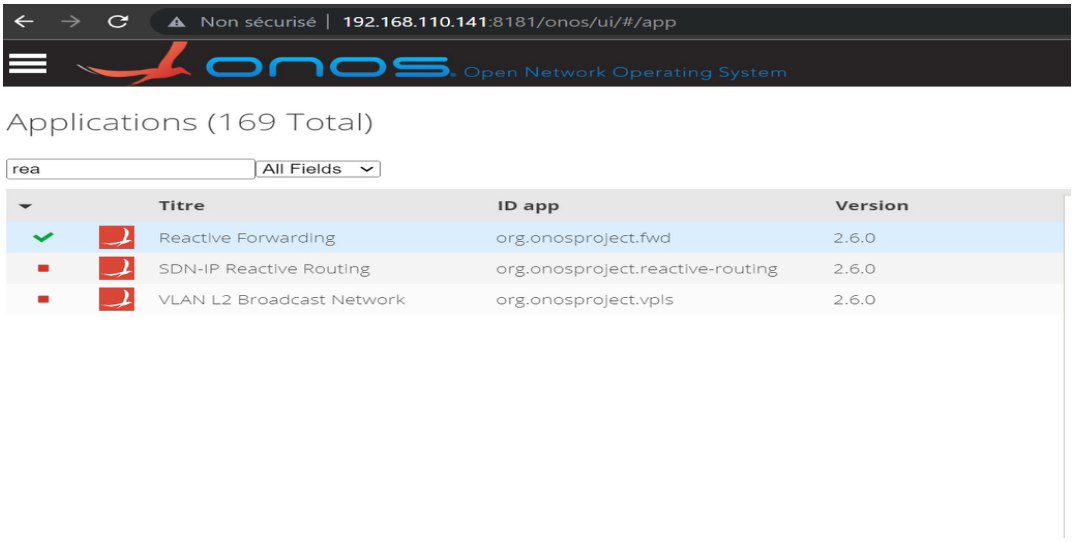

FIGURE 4.19 – Add Pachage

4.7 Réseau sous le contrôle d'ONOS avec 2 hôtes et 2 switches

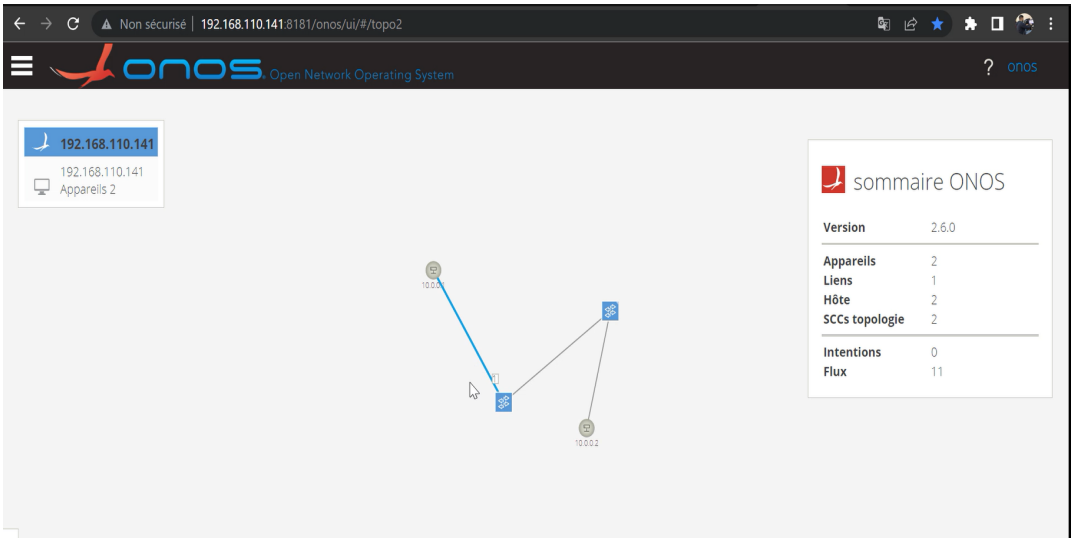

FIGURE 4.20 – Réseau sous onos

```
mininet
*** Starting controller
c0
*** Starting 2 switches
s1 s2 ...
*** Starting CLI:
mininet> pingall
*** Ping: testing ping reachability
h1 -> X
h2 -> X
*** Results: 100% dropped (0/2 received)
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=9.43 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=2.19 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=2.14 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=60.8 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=6.38 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=11.5 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=14.8 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=1.93 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=10.1 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=4.03 ms
64 bytes from 10.0.0.2: icmp_seq=11 ttl=64 time=6.40 ms
64 bytes from 10.0.0.2: icmp_seq=12 ttl=64 time=5.61 ms
64 bytes from 10.0.0.2: icmp_seq=13 ttl=64 time=3.56 ms
64 bytes from 10.0.0.2: icmp_seq=14 ttl=64 time=3.54 ms
64 bytes from 10.0.0.2: icmp_seq=15 ttl=64 time=2.42 ms
64 bytes from 10.0.0.2: icmp_seq=16 ttl=64 time=3.83 ms
64 bytes from 10.0.0.2: icmp_seq=17 ttl=64 time=8.11 ms
64 bytes from 10.0.0.2: icmp_seq=18 ttl=64 time=4.65 ms
64 bytes from 10.0.0.2: icmp_seq=19 ttl=64 time=2.49 ms
64 bytes from 10.0.0.2: icmp_seq=20 ttl=64 time=3.44 ms
64 bytes from 10.0.0.2: icmp_seq=21 ttl=64 time=2.53 ms
```

FIGURE 4.21 – Ping

Test du ping entre les hôtes Pour développer notre réseau il suffira d'apporter les modification sur ce scripte présenté dans la figure ci dessus.

FIGURE 4.22 – Scripte 2

4.8 Opérations d'administration

Le SDN implique une terminologie différente de celle du routage et de la commutation. La terminologie utilisée se réfère à la transmission, où la partie intelligente des équipements de réseau est séparée de leur partie de traitement. Ceci signifie que les équipements ne prennent plus de décisions de routage ou de commutation par eux-mêmes, ce qui rend les protocoles de routage et de commutation inutiles. Néanmoins, ces protocoles peuvent toujours être utilisés pour créer des réseaux hybrides avec des commutateurs OpenFlow, des routeurs et des commutateurs traditionnels. Les commutateurs OpenFlow étant multicouches, ils peuvent être combinés à un contrôleur pour permettre le contrôle des flux de données et ainsi affecter la gestion du comportement du réseau.

4.9 Conclusion

Ce chapitre est consacré à la pratique et, plus particulièrement à la mise en œuvre et à la sécurité de l'architecture réseau que nous avons présenté précédemment. Les détails de configuration pour chaque appareil et serveur dans l'architecture réseau, nous l'avons simulé avec Mininet.

Conclusion générale

Le Software Defined Networking annonce des changements importants sur les réseaux dans les années à venir, ce qui entraînera une évolution en profondeur de leur architecture et simplifiera l'adoption de nouveaux usages. Tout cela sera rendu possible grâce à la programmabilité, à l'ouverture, à la virtualisation et à l'orchestration. Aucun domaine ne semble épargné : WAN, data_centers, campus, sécurité, etc. Par conséquent, les administrateurs réseau doivent accompagner cette nouvelle étape pour profiter de ces capacités émergentes.

La sécurité du système d'information des entreprises est une exigence cruciale pour assurer la continuité de leurs activités sereinement. En effet, la protection de données clients, ainsi que la confidentialité des secrets de fabrication sont des préoccupations majeures. Une telle protection nécessite la satisfaction de besoins de sécurité tels que l'intégrité et la confidentialité des données transmises, ainsi que l'authentification des utilisateurs et la vérification de leurs actions.

Nous avons, également, fait certain tests pour vérifier la bonne implémentation de notre solution SDN.

Au terme de cette étude, notre principal gain a été d'acquérir une bonne compréhension de la vie professionnelle dans notre domaine. Nous avons pu évaluer les différentes étapes de réalisation d'un projet ainsi que les techniques développées par des spécialistes afin d'assurer l'efficacité et la bonne réalisation des travaux, tout en se limitant aux ressources et aux délais impartis. Dès lors, nous avons pu constater la complexité de la mise en route d'un nouveau projet et sa rapide évolution, ce qui nous a permis de mieux nous organiser pour être capables de finaliser notre travail.

Annexe1

Installation Ubuntu

Etape 1

,

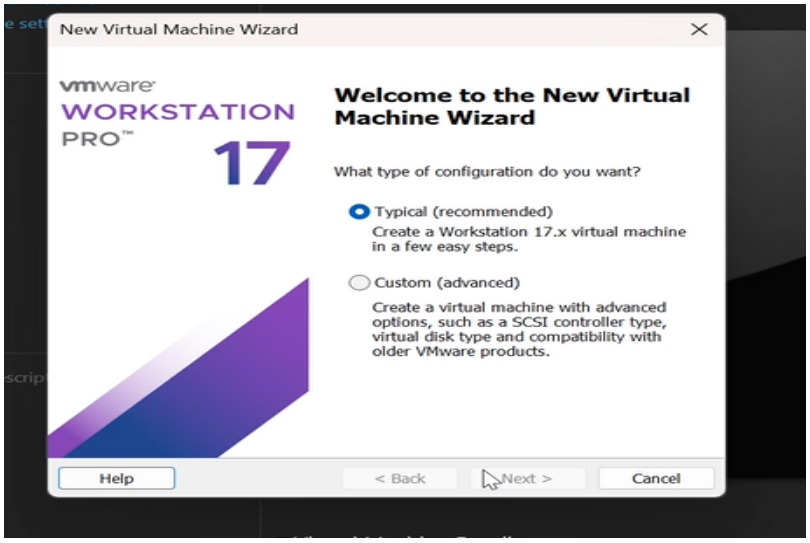

FIGURE 4.23 – Nouvelle machine virtuelle

Création d'une nouvelle machine virtuelle.

Etape 2

,

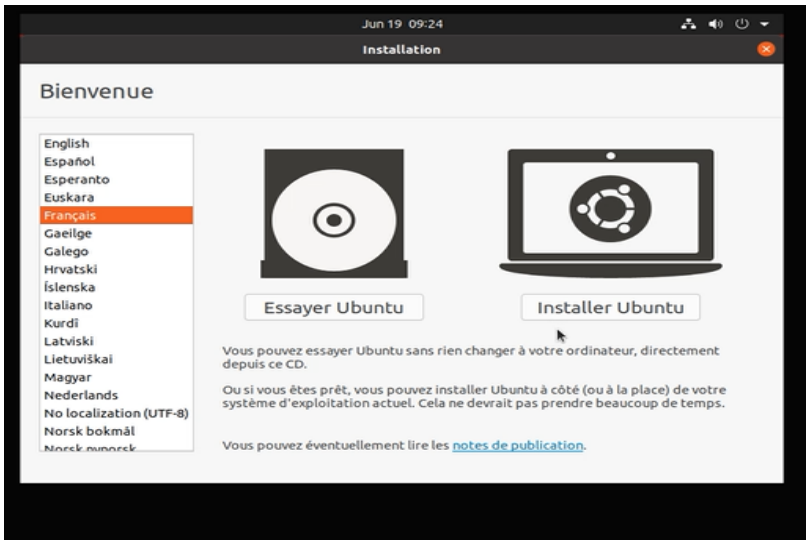

FIGURE 4.24 – Commencer l'installation

Choisir la langue Fraincaise et commencer l'installation.

Etape 3

,

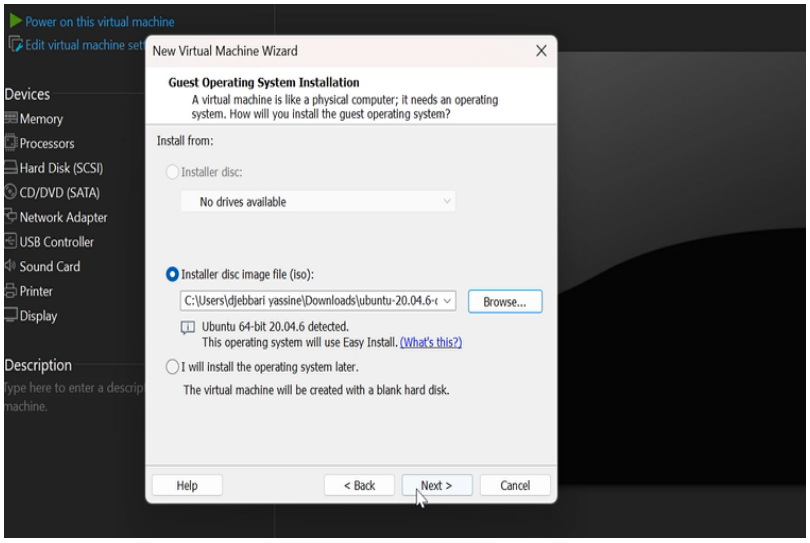

FIGURE 4.25 – Ajouter l'image pour la machine virtuelle

Importer l'image d'Ubuntu et l'ajouter a la machine virtuelle.

Etape 4

,

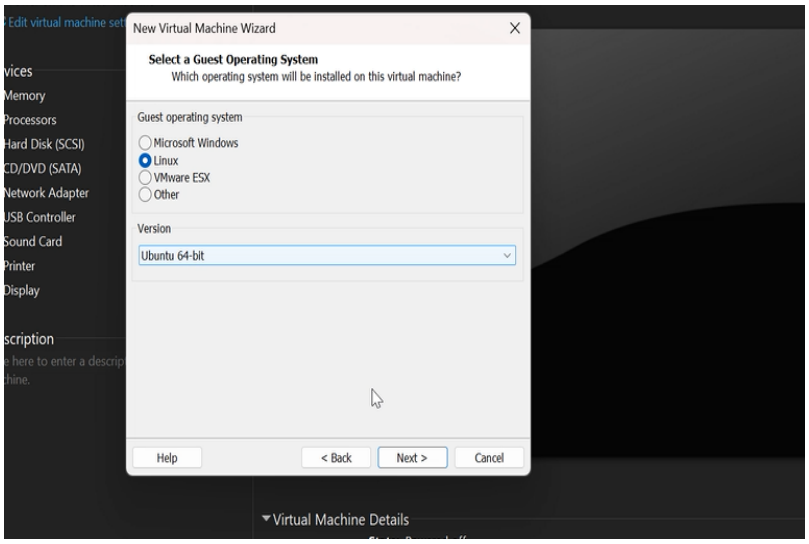

FIGURE 4.26 – Système d'exploitation choisi

Séléctionner le système d'exploitation Linux.

Etape 5

,

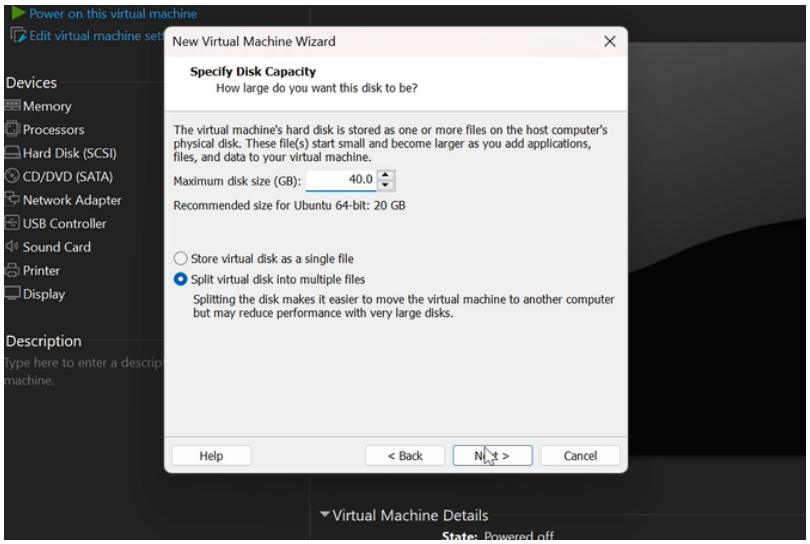

FIGURE 4.27 – Capacité du disque

Augmenter la capacité du disque a 40GB.

Etape 6

,

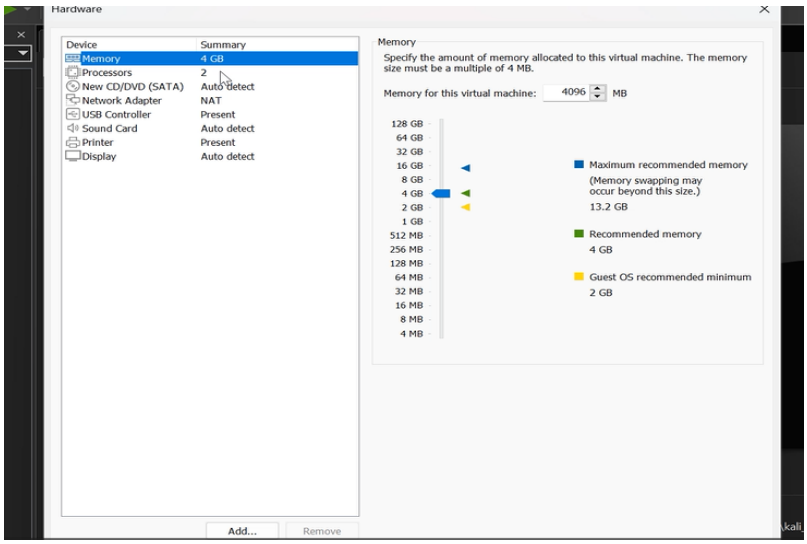

FIGURE 4.28 – Caratéristique de la machine virtuelle

Interface montrant la vue globale des caractéristique de la machine virtuelle crée.

Etape 7

,

FIGURE 4.29 – Interface de l'installation

L'installation commence.

Etape 8

Saisir les information de connection de la machine virtuelle sur cette interface. ,

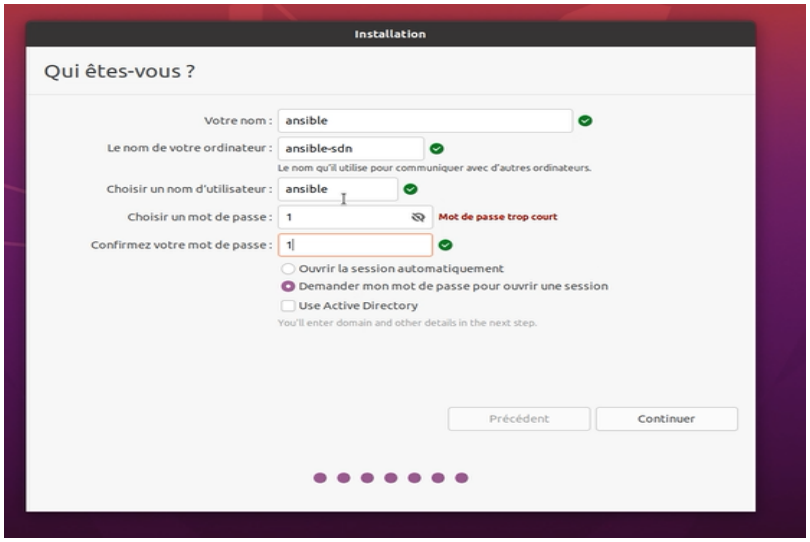

FIGURE 4.30 – Information de connection

Etape 9

Cette figure montre que l'instalation a été bien effectué.

,

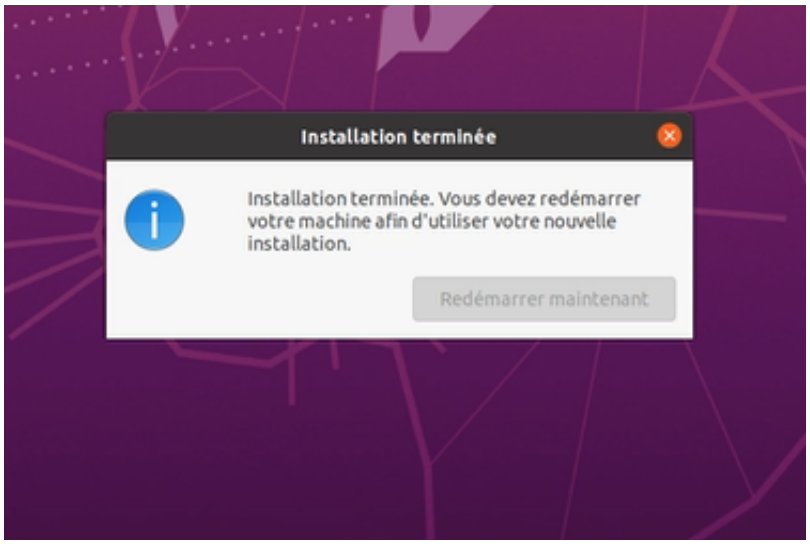

FIGURE 4.31 – Installation terminée

Etape 10

Aprés avoir redémarer notre machine on obtiendera cette figure.

,

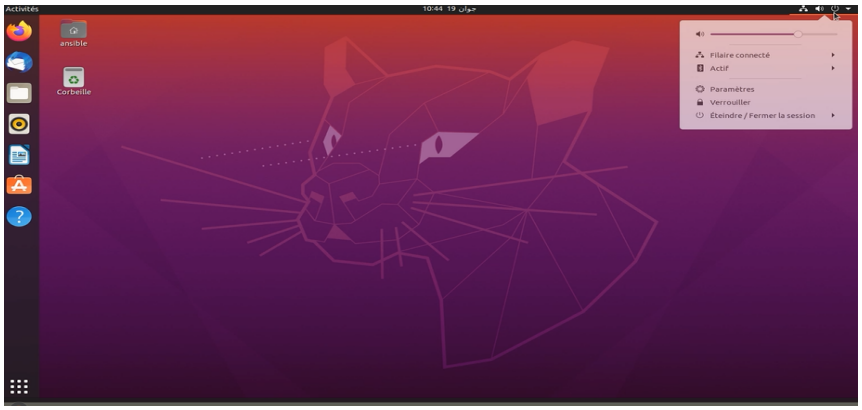

FIGURE 4.32 – Interface de UBUNTU

Annexe2

Connection de SecurCRT a Mininet

Etape 1

,

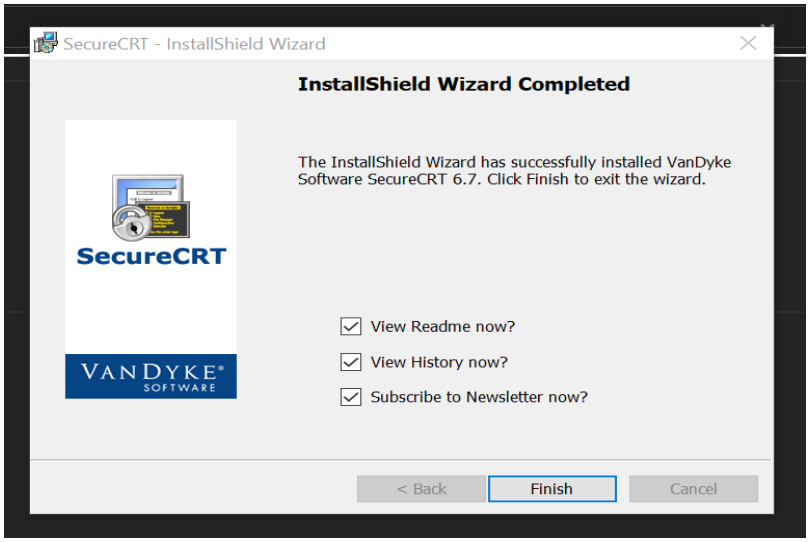

FIGURE 4.33 – Installation de SecureCRT

la figure nous montre l'installation de la figure.

Etape 2

,

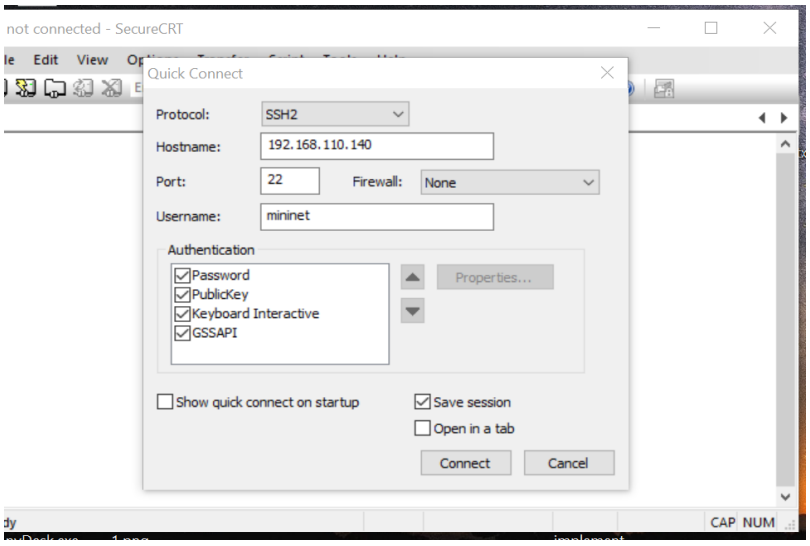

FIGURE 4.34 – Connexion a mininet

connecter mininet a SecureCRT par son adresse.

Etape 3

voici l'interface de secureCRT.

,

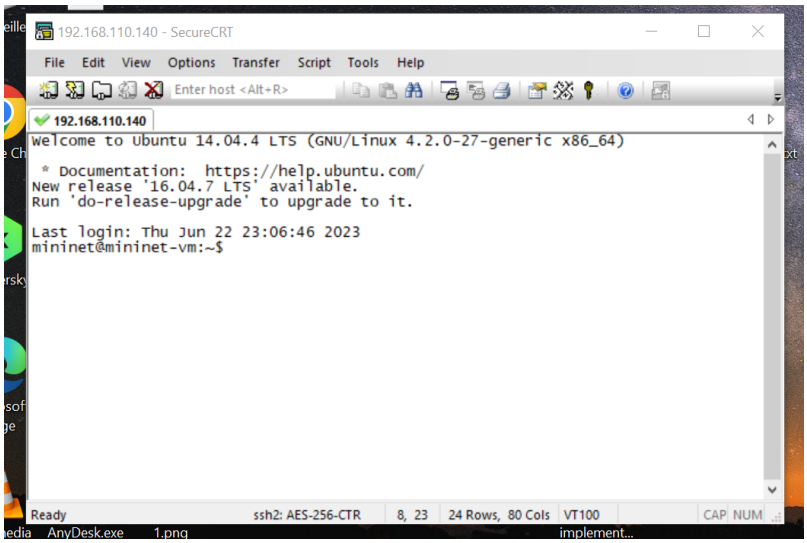

FIGURE 4.35 – Interface de SecureCRT

Bibliographie

[1] Definition ios. https://www.lemagit.fr/definition/iOS. Derniers accès le 2023-05-20.

[2] Définition du systeme linux. https://www.redhat.com/fr/topics/linux/what-is-linux#:~:text=Linux%20est%20un%20syst%C3%A8me%20d'exploitation%20Open%20Source%20et%20gratuit,la%20licence%20reste%20la%20m%C3%AAme. Derniers accès le 2023-05-20.

[3] Définition d'un routeur. https://support.google.com/googlenest/answer/6274087?hl=fr#:~:text=Un\%20routeur\%20est\%20un\%20appareil,ordinateurs\%2C\%20t\%C3\%A9l\%C3\%A9phones\%20et\%20tablettes). Derniers accès le 2023-05-30.

[4] Définition d'un switch. https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203321-switch-definition-traduction-et-acteurs/. Derniers accès le 2023-05-30.

[5] Définition sdn. http://www.opennetworking.org/sdn-definition/. Derniers accès le 2023-02-17.

[6] Etude et mise en oeuvre d'une solution sdn. http://dspace.univ-tlemcen.dz/handle/112/12600. Memoire de fin d'étude en informatique réalisé par Bouida Hafida née Saidi a l'université de Telemcen en 2017.

[7] Les objectives de la sécurité. https://www.dqsglobal.com/fr-be/blog/les-objectifs-de-protection-de-la-securite-de-l%22information-et-leur-signification#:~:text=En%20plus%20des%20objectifs%20de,responsabilit%C3%A9%22%2C%20qui%20se%20compl%C3%A8tent. Derniers accès le 2023-03-15.

[8] Serveur dhcp. `httpshttps://culture-informatique.net/cest-quoi-un-serveur-dhcp-niv1/`. Derniers accès le 2023-05-20.

[9] Type des réseaux. `https://www.infoexpress.fr/quels-sont-les-differents-reseaux-informatiques/`. Derniers accès le 2023-03-10.

[10] Yvon Zafimahefa Andrianirina. *Développement d'un réseau défini par logiciel (SDN) programmable, transparent et ouvert.* PhD thesis, Université du Québec en Outaouais, 2021.

[11] Hafida BOUIDA née SAIDI. *Etude et mise en oeuvre d'une solution SDN.* PhD thesis, 11-03-2018.

[12] Mehdi Chikhi, Adel Djemil, et al. *Etude et implementation de l'approche Software Defined Network dans un résreau local.* PhD thesis, Université de Blida, 2019.

[13] Ihssane Choukri, Mohammed Ouzzif, and Khalid Bouragba. Software defined networking (sdn) : Etat de l'art. In *Colloque sur les Objets et systèmes Connectés*, 2019.

[14] Jérôme Durand. Le sdn pour les nuls. *JRES 2015-Montpellier*, pages 1–12, 2015.

[15] Jugourta Haddad, Badreddine Touati, Abderrahmane Sider, et al. *Tolérance Aux Pannes Des Serveurs Cas THCIN-LAIT.* PhD thesis, Université A/Mira de Bejaia, 2014.

[16] Ouafae Ifrken. Software-defined network. In *Rapport du semestre, hepia Genevre*, 2016.

[17] Traore Issa, Kouassi Brou Médard, and Atta Ferdinand. Etude du nomadisme dans un cloud éducatif administré par la technologie sdn/openflow. In *Institut de recherches mathématique Université Félix Houphouët-Boigny, conférence WACREN*, 2016.

[18] abdelhalim Khouas, Ahmed Gacem, and Ramzi. *conception et réalisation d'un outil de gestion normalisé dédié a la plateforme de virtualisation des réseaux Open virtuel Switch* . PhD thesis, Université de Boumardes, 2016.

[19] Batat Nadia. Les systemes de sécurité. 2023.

[20] Tomas Paradis. Software-defined networkin. In *Memoire de Master, School of Information and Communication Technology KTH Royal Institue of Technology Stockholm, Sweden*, 2014.

[21] Philippe.A. *Réseaux informatiques notions fondamentales.* PhD thesis, Mai 2009.

[22] Siham Saoud, Amina Saoud, et al. *Etude et amélioration de l'architecture et sécurité du réseau de l'EPB*. PhD thesis, Universite de bejaia, 2016.

RÉSUMÉ

Ce document est rédigé en vue de l'obtention du diplôme de Master Administration et Sécurité des Réseaux et il présente le projet que nous avons réalisé. L'objectif de ce dernier est d'étudier une solution SDN et sa sécurité. Pour atteindre cet objectif, nous avons proposé une solution SDN avec le contrôleur ONOS qui a pour but de centraliser et virtualiser le réseau d'une entreprise .Pour ce faire, nous avons pris l'entreprise TCHIN_LAIT CANDIA comme cas d'étude pour notre application et nous avons utilisé le simulateur GNS3,Mininet et VMWARE WORKSTATION pour implémenter notre solution virtuellement. Nous avons par la suite, établie certain règles de sécurité.

Mots clés : SDN ; OPENFLOW ; ONOS ; virtualisation, sécurité ; contrôleur ;

ABSTRACT

This document is written for the purpose of obtaining a Master's degree in Network Administration and Security, and it presents the project that we have undertaken. The objective of this project is to study an SDN solution and its security. To achieve this objective, we have proposed an SDN solution using the ONOS controller, which aims to centralize and virtualize the network of a company. For this purpose, we have chosen the company TCHIN_LAIT CANDIA as a case study for our application, and we have used the simulators GNS3, Mininet, and VMWARE WORKSTATION to implement our solution in a virtual environment. Subsequently, we have established certain security rules.

re.

Keys words : SDN ; OPRNFLOW ; ONOS ; virtualize ; Security ; controller ;