REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA



Faculté des sciences

Mémoire de fin d'études de Master

Département : Math et informatique

Filière :**Ingénierie des systèmes et des technologies web**

AUDIT DE SECURITE POUR LE RESEAU DE L'UNIVERSITE DE MEDEA

Présenté par :

AMRI AMEL

LAKEHAL FATMA ZAHRA

Proposé et dirigé par :

SADOUKI FATIHA

Promotion : 2021

Remerciement

Nos premiers remerciements s'adressent au Dieu le tout puissant, qui nous a permis d'avoir la santé, le courage et la volonté de mener à bien ce travail. Nous tenons aussi à remercier notre promotrice Mme Sadouki-F qui nous a aimablement orienté et assidument dirigés notre travail et qui a été présente à tout moment de la réalisation de ce projet et surtout sans laquelle ce modeste travail n'aurait jamais vu le jour, ainsi que les membres du jury pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions. Nous tenons compte à remercier vivement Mr khir Eddine l'administrateur réseau au sein de l'université de Médéa, pour l'accueil, pour ces judicieux conseils et sa confiance, et Mr Djelloul pour le temps consacré et le partage de son expertise au quotidien.

Nous remercions également tous les professeurs du département Math et Informatique MI qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous ont aidés à mener à terme notre projet.

Merci à tous.

Dédicaces

Je dédie ce modeste travail à:Mes très chers parents à qui je dois tout, je profite l'occasion de les remercier pour leurs encouragements, leurs aides, que Dieu les protège et les entoure de sa bénédiction. A mon mari pour le soutien qu'il m'a porté et le sacrifice qu'il a fait pour moi, Mes enfants, Mes frères et sœurs et toute la famille. Toutes mes amies ainsi qu'à tous ceux qui nous sont chers. A mes collègues de L'insfp de Médéa, Et à toute personne nous ayant fait part de son savoir.

Amri Amel

Dédicaces

Je dédie ce modeste travail à:Mes très chers parents à qui je dois tout, je profite l'occasion de les remercier pour leurs encouragements, leurs aides, que Dieu les protège et les entoure de sa bénédiction, Mes frères et sœurs Surtout Lamis et toute la famille. Toutes mes amies ainsi qu'à tous ceux qui nous sont chers. Et à toute personne nous ayant fait part de son savoir.

Lakhal fatma Zahra

ملخص

يعد أمن البيانات مؤشر مهم جدًا و حاسم داخل المؤسسة ، نظرًا للكم الهائل من المعلومات المتبادلة يوميا.

تستقبل جامعة المدية سنويا آلاف الطلبة (جزائريين وأجانب) وتضع شبكتها تحت تصرفهم باختلاف مستوياتهم كمستعملين. لحماية هذه الشبكة ينبغي الحصول على نضام امان قوي للشبكة .

الهدف من عملنا هذا هو توفير نظام شبكة آمن للجامعة ، ولهذا قمنا بإجراء دراسة للشبكة الحالية ، وكذلك الأجهزة الأمنية الموجودة فيها . سمح لنا هذا بانتقاد الموجود واقتراح حلول من أجل بنية شبكة جديدة توفر نضام حماية اكبر

قمنا بتنفيذ الحلول المقترحة حسب المستويات ، بدءاً بأجهزة الشبكات المحلية التى

قمنا بتفعيل أمن المنافذ عليها و كذا الإجراءات الوقائية ضد الهجمات المختلفة على هذا المستوى . كما اقترحنا إجراءات أمنية لحماية الولوج للأجهزة من اجل برمجتها ، أخيرًا قمنا بتنفيذ حلول لأمن الشبكات الواسعة .

هناك مؤسسات تنقسم لعدة هياكل وقد تكون بعيدة في عن بعضها في المسافة . من أجل تأمين البيانات والاتصالات بشكل أفضل بين اقسام المؤسسة وحجبها عن أي متدخل خارجي ظهرت العديد من التقنيات والمفاهيم ، مثل الشبكة الخاصة الافتراضية **PNS** .

اخترنا إنشاء شبكات **VPN** من موقع إلى موقع لربط مواقع الجامعة فيما بينها , معتمدين على بروتوكول **IPsec** في وضع النفق.

كذلك اقترحنا جدار حماية الشبكة **Parfeu** لتعزيز الأمان عن طريق التحكم بالسماح او المنع لمرور البيانات الواردة إلى الشبكة وكذا لتوفير وظائف الأمان **IPS**, **IDS.**

في مشروعنا ، عملنا في بيئة محاكات **GNS3 على** الجهاز الافتراضي **VM WORKSTATION**

الكلمات المفتاحية:الشبكة , الامن السيبيرانى , منفذ التبذيل , الشبكة المحلية الافتراضية ,قائمة نضام الدخول, النفق

جدار حماية الشبكة , جهاز أمان متكيف, برتوكول الانترنت المحمي.

Résumé

La sécurité des données est un paramètre très important voire cruciale au sein d'une organisation, compte tenu des échanges d'informations qui se font au quotidien.

L'université de MEDEA accueille chaque année des milliers des étudiants (Algériens et étrangers). Elle met à leur disposition son réseau qui est alors à la merci de tout genre d'utilisateurs. Pour protéger ce réseau, il est indispensable d'acquérir un système de sécurité robuste pour le réseau.

L'objectif de notre travail consiste à proposer un audit de sécurité pour le reseau de l'université de medea, pour cela nous avons procédé à une étude du réseau existant, ainsi que les dispositifs de sécurité mis en place. Ce qui nous a permis de critiquer l'existant et de suggérer des solutions afin de proposer une nouvelle architecture réseau qui donne une meilleure fluidité pour le trafic ainsi que sa sécurité.

Nous avons implémenté les solutions proposées par niveaux, commençant par les dispositifs du réseau LAN, sur lesquels nous avons activé la sécurité des ports et les mesures de prévention contre les différents attaques á ce niveau, ensuite nous avons implémenté des mesures de sécurité pour l'accès de gestion, enfin nous avons mis en place des solutions pour la sécurité des réseaux WANs. A cet effet, pour une entreprise possédant plusieurs sites distants, afin de sécuriser au mieux les communications entre ces derniers et les rendre transparentes à une entité étrangère, plusieurs techniques et concepts sont apparus à savoir les

VPNs. Nous nous sommes opté pour la création de VPNs site à site pour interconnecter les sites de l'université, en se basant sur le protocole IPSec dans son mode tunnel. Un par feu ASA est proposé aussi et configuré pour le réseau dans le but de renforcer la sécurité en filtrant le trafic entrant vers le réseau et en assurant ainsi des fonctions de sécurité comme l'IPS et l'IDS.

Dans notre projet, nous avons travaillé dans l'environnement de simulation GNS3 avec la machine virtuelle VM Workstation.

Mots clés : Réseau, cyber sécurité, switchport , Vlan, ACL, Réseaux Privés Virtuels, Tunnel, ASA, Pare feu, IPsec,AAA.

Abstract

The safety of the data is very important parameter even crucial within an organization, considering the information exchanges which are made on a daily basis.

The University of MEDEA welcome every year thousands of students (from Algeria and around the world) and makes available its network for them. To protect the network, one idea would be to acquire a management mechanism that is both sturdy and safe for the network.

The goal of our work is to propose a security audit for the network of the University of Medea in order to achieve that, we conducted a study of the current architector and safety devices put in place. This allowed us to criticism it and to suggest solutions in order to propose a new network architector that gives a better flow for traffic and safety.

We have implemented the solutions proposed by levels, starting with the devices of the LAN network, on which we have activated the port's security and the preventive measures against the various attacks at this level. Then we have implemented security measures for management access. Finally we have implemented solutions for the security of WAN networks. For that purpose, for a company possessing several distant sites, to secure at best the communications between the latter and make them transparent to a foreign entity, several techniques and concepts appeared, namely the VPNs. We were opted for the creation of VPNs site-to-site in order to interconnect the sites of the university, by basing it on the protocol IPsec in its tunnel mode. In our project. A firewall ASA is proposed and configured with the aim of strengthening the network security from the external traffic, ASA provides also IPS and IDS's sevices.

We worked in the environment of simulation GNS3 on the virtual machine VM workstation.

Key words: Network, Cybersecurity, Switchport, Virtual Private Networks, Tunnel, IPsec.

Vlan, ACL, ASA, Firewall, IPsec, AAA.

Table de matiere

Chapitre 01

Introduction général.....1

1.1 Introduction.....3

1.2 Définition d'un réseau 3

1.3 Intérêts d'un réseau 3

1.4 Classification des réseaux 4

1.4.1 LAN (Local Area Network ou réseau local en français).....4

1.4.2 MAN (Metropolitan Area Network ou réseau métropolitain en français) 4

1.4.3 WAN (Wide Area Network ou réseau étendu au public en français) 5

1.4.4 SAN Storage Area Network (SAN).....5

1.4.5 WPAN(Wireless Personnel Area Network ou réseau personnel sans fil) 5

1.5 Les supports de transmission.....5

1.5.1 Le Câble coaxial 6

1.5.2 La paire torsadée 7

1.5.2.1 La paire torsadée non blindées (UTP) 7

1.5.2.2 La paire torsadée blindée (STP) 7

1.5.2.3 Les connecteurs pour paire torsadé.....7

1.5.3 La fibre optique.....7

1.5.3.1 Caractéristiques de la fibre optique 8

1.5.3.2 types de fibre optique 8

1.5.3.3 Connecteurs pour la fibre optique 9

1.5.4 Les ondes radio 9

1.5.5 Carte réseau 10

1.6 Les topologies d'un réseau 11

1.6.1 La topologie logique 11

1.6.2 La topologie physique 11

1.6.2.1 Topologie en bus 11

1.6.2.2 Topologie en étoile (la plus utilisée) 11

1.6.2.3 Topologie en anneau 11

1.6.2.4 Topologie maillée 12

1.7 Réseau fiable 12

1.7.1 Tolérance aux pannes 12

1.7.2 Évolutivité 12

1.7.3 Qualité de service (QOS).....13

1.7.4 Sécurité 13

1.8 Le Modèle OSI 13

1.9 Le modèle TCP/IP 15

1.9.1 Présentation du protocole TCP/IP 15
1.9.1.1 Le protocole IP (Internet Protocol).....15
1.9.1.2 Le protocole TCP (Transmission Control Protocol).....15
1.9.2 Descriptions du modèle TCP/IP 15
1.9.2.1 La couche application 15
1.9.2.2 La couche transport.....16
1.9.2.3 La couche internet 16
1.9.2.4 La couche accès réseau 16

1.10 Equipements d'Interconnexion des réseaux 16
1.10.1 Le répéteur (repeater) 16
1.10.2 Les concentrateurs (hubs).....17
1.10.3 Modem 17
1.10.4 Les ponts (bridges).....18
1.10.5 Les commutateurs (en anglais switch) 18
1.10.6 Les passerelles (Gateway) 19
1.10.7 Les routeurs.....19

1.11 Les protocoles de routage 21
1.11.1 La Distance Administrative (AD).....22

1.12 Conclusion.....23

chapitre 02

2.1 INTRODUCTION 24

2.1 Objectifs du cyber sécurité.....24

2.2 Terminologie 25
2.2.1 Vulnérabilité 25
2.2.2 Menace 25
2.2.3 Risque 25
2.2.4 Attaque 25

2.3 Les solutions de sécurité 27
2.3.1 Définition d'un DMZ 27
2.3.2 Les listes de contrôles d'accès (ACL) 28
2.3.2.1 L'intérêt d'utiliser des ACL.....29
2.3.2.2 Les types des listes de contrôle d'accès.....29
2.3.3 Les VLAN 30
2.3.3.1 VLAN par port.....30
2.3.3.2 VLAN par adresse.....30
2.3.3.3 VLAN par protocole.....30
2.3.4 Présentation du protocole AAA 30

2.3.5 Le VPN (Virtuel Private Network) 31
2.3.5.1 VPN client to site ou VPN nomade ou VPN Remote-Access 32
2.3.5.2 L'intranet VPN ou VPN Site-to-Site.....33
2.3.6 Les protocoles de tunnelisation 33
2.3.6.1 SSL (Secure Socket Layer) / TLS.....33
2.3.6.2 IP Sec.....34
2.3.6.3 GRE 35
2.3.7 Le Proxy 36
2.3.8 Les pare-feu 36
2.3.8.1 Définition et fonctionnement.....36
2.3.8.2 Les types de Par-feu.....38
2.3.9 Les systèmes de détection de l'intrusion(IDS).....39
2.3.10 Un système de prévention d'intrusion (IPS en anglais) 40
2.3.11 La cryptographie 40
2.3.11.1 Fonctions cryptographiques et terminologie 40
2.3.11.2 certificats numériques :.....42
2.3.11.3 Signatures numériques.....42
2.3.12 Le NAT.....42
Conclusion.....43

chapitre 03

3.1 Introduction 45
3.2 Présentation globale du réseau 45
3.2.1 Architecture réseau de l'université 46
3.2.2 Situation informatique 46
3.3 Critiques et suggestions 48
3.3.1 Sécurité au niveau des réseaux LAN et WLAN.....48
3.3.1.1 Les points d'accés 48
3.3.1.2 Securisation des switches 48
3.3.1.2.1 Les attaques.....48
3.3.1.2.2 Les solutions contre ces types d'attaques 51
3.3.1.2.2.1 Protection contre l'usurpation d'adresses MAC 51
3.3.1.2.2.2 Protection contre STP manipulation 52
3.3.1.2.2.3 Protection contre les tempêtes 54
3.3.1.2.2.4 Protection contre les attaques Vlans 54
3.3.1.3 La redondance 55
3.3.1.4 Les VLAN de données 55
3.3.2 Sécurité de l'accès pour la gestion 57
3.3.2.1 Les mots de passe et les message de jour 57
3.3.2.2 Transmission par protocol telnet 59

3.3.3 Sécurité au niveau des réseaux WAN (trafic des réseaux distants) 61
3.3.3.1 Les switches fédérateurs 61
3.3.3.2 Interconnexion des sites (VPNs) 61
3.3.3.3 L'authentification (AAA) 66
3.3.3.4 Le filtre du trafic (ACLs) 64
3.3.3.5 Protection contre les risques du réseau externes.....70

Conclusion.....

chapitre 04

4.1 Introduction 75

4.2 Description de l'environnement de travail 75
4.2.1 Présentation de GNS3 75
4.2.2 Fonctionnement 75
4.2.3 Versions de GNS3 76
4.2.4 Architecture Client / Serveur 76
4.2.5 Composants GNS3 76

4.3 Configuration 77

4.3.1 Configuration initial 79
4.3.2 Sécurité des ports switches (Niveau LAN).....80
4.3.3 Sécurité de la gestion d'accès 82
4.3.4 Protection contre la manipulation STP 83
4.3.5 Protection contre les tempêtes 84
4.3.6 Création des VLAN 85
4.3.7 AAA authentification 87
4.3.8 Configuration du protocole de routage 87
4.3.9 Configuration de Cisco Adaptative Security (ASA) 88
4.3.9.1 Configuration de base.....88
4.3.9.2 Configuration des interfaces 90
4.3.9.2.1 Test de connectivité.....90
4.3.9.3 Configuration de routage pour ASA.....90
4.3.9.4 configurations d'un objet NAT 91
4.3.9.5 Création d'une carte de politique d'inspection (MPF : Map Policy Framework) 92
4.3.9.6 Configuration d'ASA comme un serveur DHCP 94
4.3.9.7 Configuration d'authentification AAA pour SSH avec la base de données locale 93
4.3.9.8 Configuration de l'Access vers ASA par le protocole SSH 93
4.3.9.9 configuration du vlan DMZ 95
4.3.9.10 Configuration des ACLs sur ASA.....95

4.3.10 Configuration de VPN IPsec site á site 96
4.3.10.1 Configuration des paramètres d'IPsec sur le routeur POLE 96
4.3.10.2 Configuration des paramètres d'IPsec sur le routeur Ouzera 99
4.2.10.3 Vérification de IPsec VPN 100

4.4 Réalisation sur matériels ……...100
4.5 conclusion……105

Conclusion général……106

ANNEXE A

ANNEXE B

ANNEXE C

ANNEXE E

ANNEXE F

Liste des figures

Figure 1.1 : réseau LAN.....4

Figure 1.2 : réseau MAN.....4

Figure 1.3 : réseau WAN.....4

Figure 1.4 : Câble coaxial 6

Figure 1.5 : câble coaxial avec ses connecteurs.....6

Figure 1.6 : paire torsadée.....7

Figure 1.7: fibre optique.....8

Figure 1.8 : Fibre optique monomode et multi mode.....8

Figure 1.9 : connecteurs de la fibre optique.....9

Figure 1.10 :ondes radio.....10

Figure 1.11 : une carte réseau filaire.....10

Figure 1.12: Topologie en bus.....11

Figure 1.13 : Topologie en étoile.....11

Figure 1.14 : Topologie en anneau.....12

Figure 1.15 : Topologie maillée.....12

Figure 1.16 :Diagramme du modèle OSI.....13

Figure 1.17: La communication entre les périphériques finaux.....14

Figure 1.18 :Comparaison entre le modele OSI et TCP/ IP 15

Figure 1.19 :Répéteur.....16

Figure 1.20 : concentrateur.....17

Figure 1.21 : modem.....17

Figure 1.22 : pont.....18

Figure 1.23 : commutateur catalyst.....18

Figure 1.24: routeurs.....19

Figure 1.25 : composants internes d'un routeur 2600.....20

Figure 1.26 : ports d'un routeur 2600.....20

Figure 1.27:Diagram de décision de routage.....21

Figure 1.28 : protocoles de routage pour IPV6.....22

Figure 1.29: Distance Administrative (AD)……...23

Figure2.1 : Attaque par déni de service……...26

Figure 2.2 : Exemples sur les ACL……28

Figure 2.3 : VLAN dans un reseau……30

Figure 2.4: VPN client to site……31

Figure 2.5: VPN Site-to-Site……33

Figure 2.6 : Encapsulation IPSec……35

Figure 2.7 : proxy……36

Figure 2.8: par –feu……37

Figure 2.9 : par feu dans un réseau……39

Figure 2.10 : schéma de principe d'un crypto-système……41

Figure 2.11 : Chiffrement/déchiffrement symétrique avec une clé secrète……41

Figure 2.12 : Chiffrement à clé publique et déchiffrement à clé privé……43

Figure 2.13 : Traduction d'adresses réseau (Nat) entre un réseau privé et Internet……44

Figure 3.1 : Topologie physique du réseau de l'université……46

Figure 3.2 : Etat initial avant spoofing……49

Figure 3.3 : B spoof l'adresse MAC de A……49

Figure 3.4 : switch voit l'hôte A dans le port 2……49

Figure 3.5 : Principe d'attaque BPDU STP……50

Figure 3.6 : attaque DTP Rogue switch……51

Figure 3.7 : Principe d'attaque double-tagging……51

Figure 3.8 : Désactivation des ports inutiles……52

Figure3.9 : exemple de port-Security d' une interface d'un switch……52

Figure 3.10 : Adresses MAC dynamiques et rémanentes……53

Figure 3.11 : Comparaison entre les modes de violation……54

Figure 3.12 :PortFast sur les ports d'accès et entre des switches……54

Figure 3.13 : Exemple d'activation de contrôle……55

Figure 3.14 : exemple de désactivation de DTP……55

Figure 3. 15: configuration d'un Vlan natif……55

Figure 3.16 : chemins redondants……56

Figure 3. 17 : exemple de Vlans……57
Figure 3.18 : Méthodes d'accès au routeur pour la configuration……58
Figure 3.19 : Désactivation du procédure de récupération d'un mot de passe……60
Figure 3.20 : exemple de tentatives échouées……60
Figure 3.21 : Capture Wireshark pour Telnet……61
Figure 3.22 : Capture wireshark pour SSH……61
Figure 3.23 : Exécution de la commande show version……62
Figure 3.24 : Accès par le protocole SSH……62
Figure 3.25 : Solution VPN proposée……63
Figure 3.26 : Exemple de configuration d'un tunnel GRE……64
Figure 3.27 :Implementation d'IPsec……65
Figure 3.28 : Algorithmes d'encryption……65
Figure 3.29 : Méthode PSK……66
Figure3.30 : Methode RSA……66
Figure 3.31 : Mot de passe pour lignes vty……67
Figure 3. 32: Méthode base de données locale……67
Figure 3. 33: Athentification locale……67
Figure 3. 34 : AAA basé sur un serveur……68
Figure3.35 : Authentification Tacacs +……68
Figure 3.36 : Authentification Radius……69
Figure 3.37 : ACL Standard et ACL Etendue……70
Figure 3.38 : exemple d'une ACL……71
Figure 3.39 : positionnement d'un par feu ASA……71
Figure 3.40 :Modèles Cisco ASA……72
Figure 3.41 : Ensembles et options recommandés pour la version Anti-X Edition……73
Figure3. 42: Modeles ASA……74
Figure3.43 :Modules IPS……74
Figure 4.1 : interface graphique du GNS3……77
Figure 4.2 : configuration de base……80
Figure 4.3 : Vérification des mots de passe et le message du jour……80

Figure 4.4 : Vérification des mots de passe et le message du jour……80
Figure 4.5 : Désactivation du protocole DNS……81
Figure 4.6 : longueur minimale d'un mot de passe……81
Figure 4.7 : Contrainte de longueur minimale……81
Figure 4.8 : Désactivation des interfaces inutiles……81
Figure 4.9: Activation de la sécurité des ports……81
Figure 4.10 : configuration du maximum des adresses MAC sur un port……81
Figure 4.11: Adresses sticky……82
Figure 4.12 : régler mode violation……82
Figure 4.13 : Affichage des paramètres de sécurité d'une interface……82
Figure 4.14 : time out de la ligne console……82
Figure 4. 15 : Bloque des connections……82
Figure 4.16 : Vérification de la configuration du bloque……83
Figure 4. 17 : Access liste d'autorisation pour l'administrateur……83
Figure 4.18: Activation de STP portfast……83
Figure 4.19 : Activation de la fonction Bpdugard……84
Figure 4.20 : Affichage du résumé STP……84
Figure 4.21 : Désactivation d'une interface……84
Figure 4.22: Configuration d'un seuil maximum du trafic de diffusion……84
Figure 4.23 : Vérification de contrôle……85
Figure 4.24 : Création des vlans……85
Figure 4.25 : Affichage des vlans……85
Figure 4.26 : Affectation des ports……85
Figure 4.27 : Vérification de l'affectation des ports……86
Figure 4.28 : vlan natif……86
Figure 4.29 : Interface en mode trunk……86
Figure 4.30 : Désactivation du protocole DTP……86
Figure 4.31 : Vérification de la désactivation du DTP……86
Figure 4.32 : Configuration de l'authentification……87
Figure 4.33: Vérification de l'authentification……87

Figure 4.34 : configuration du protocole de routage……87
Figure 4.35 : Vérification de la connectivité……87
Figure 4.36 : Intégration d'un par feu dans un réseau……88
Figure 4.37 : Version d'IOS ASA……88
Figure 4.38 : License ASA……89
Figure 4.39: configuration de base ASA……89
Figure 4.40: Vérification du mot de passe……89
Figure 4.41 : Configuration des interfaces……89
Figure 4.42 : Vérification des interfaces……90
Figure 4.43 : Test de connectivité……90
Figure 4.44 : configuration d'une route dar défaut……90
Figure 4.45 : table de routage……90
Figure 4.46 : Ping réussit depuis ASA vers l'extérieur……91
Figure 4.47: Capture du Ping depuis ASA vers un hôte externe……91
Figure 4.48: configuration de NAT……91
Figure 4. 49:Verification de NAT……91
Figure 4.50 : Vérification par la commande show Nat……92
Figure 4.51 : Etapes de MPF……92
Figure 4.52 : configuration d'une carte de politique……92
Figure 4.53 : activation du serveur DHCP……92
Figure 4.54 : Vérification de l'adressage automatique……93
Figure 4.55 : configuration AAA pour l'utilisateur SSH……93
Figure4.56 : accès SSH depuis Inside……93
Figure 4.57 : accès SSH depuis Outside……94
Figure 4.58 : Accès SSH depuis un serveur……94
Figure 4.59: Création de Vlan DMZ……94
Figure 4.60: affichage des interfaces……95
Figure 4.61 : Création d'objet NAT pour DMZ……95
Figure 4.62 : Configuration des ACLs……95
Figure 4.63: Vérification de la License……96

Figure 4.64 : Acl pour le trafic VPN……96
Figure 4.65 : Activation d'ISAKMP et négociation de clé……..97
Figure 4.66: Clé pré-partagée……..97
Figure 4. 67: Politique IPsec……..97
Figure4.68 : Affectation du MAP á l'interface de sortie……98
Figure 4.69 : Configuration d'IP sec sur le routeur Ouzera……98
Figure 4.70 : Configuration du VPN sur le routeur Ouzera……99
Figure 4.71: VPN établit……99
Figure 4.72 : Vérification de transform-set sur le routeur Ouzera……99
Figure 4.73 : Vérification de transform-set sur le routeur POLE……99
Figure 4.74: Vérification de crypto map sur le routeur POLE……100
Figure 4.75 : Vérification de crypto map sur le routeur Ouzera……100
Figure 4.76 : Ping entre POLE et Ouzera……100
Figure 4.77 : Vérification des associations de sécurité……..101
Figure 4.78: Verification d'encapsulatin et d'encryption……..101
Figure 4.79 : Ping etendu entre pole et ouzera……101
Figure 4.80 : Vérification des Sas sur le routeur POLE0……102
Figure 4.81 :Verification des paquets encapsulés et cryptés……102
Figure 4.82 : Vérification des Sas sur Ouzera……102
Figure 4.83 : Matériel utilisé……..103
Figure 4.84 : Branchement des périphériques……103
Figure 4.82 : Emulateur de terminal Putty……103

Liste des abréviations :

ARP :Adress resolution protocole.

AAA: Authentication, authorisation, accounting.

ASA: Appliance security adaptative.

ACL : Access Control List.

AH: Authentication Header.

CLI : Commande Langage Interface.

DHCP: Dynamic Host Configuration Protocol.

DMZ: Demilitarized Zone.

DNS: Domain Name System.

DoS: Deny of service.

ESP: Encapsulation Security Payboad.

FTP: File Transfer Protocol.

HIDS: Host Intrusion Detection Systems.

Http: Hyper Text Transfer Protocol.

ICMP: Internet Control Message Protocol.

IP : Internet Protocol .

IKE : Internet Key Exchange.

IEEE: Institute of Electrical and Electric Engineers.

IETF: Internet Engineering Task Force.

IPsec: Internet Protocol Security.

LAN: Local Area Network.

L2TP: Layer two Tunneling Protocol.

MAC: Media Access Control.

MAN: Metropolitan Area Network.

NAS: Network Access Server.

NAT: Network Address Translation.

NIDS: Network Intrusion Detection Systems.

OS: Operating System.

OSI : Open Systems Interconnection.

PPTP: Point- To Point Tunneling Protocol.

PSK : Pre-shared Key.

QoS: Quality of Service.

RFCs: Request for Comments.

RIP: Routing Information Protocol.

SA: Security Association.

SHA: Secure Hash Standard.

SMTP: Simple Mail Transfer Protocol.

SSH : Secure Shell.

SSL : Secure Socket Layer.

TCP: Transmission Control Protocol.

TLS : Transport Layer Security.

TCP/IP: Transmission Control Protocol /Internet Protocol.

Telnet : Telecommunication network.

UDP: User Datagram Protocol.

URL: Uniform Resource Locater.

USB: Universal Serial Bus.

VLAN: Virtual Local Area Network.

VM: Virtual Machine.

VPN : Virtual Private Network.

WAN : Wide Area Network.

Introduction générale

Introduction générale

Les avancées remarquables de la technologie ont favorisé le développement des réseaux informatiques de façon prodigieuse. En effet ils prennent de plus en plus une place stratégique au sein des entreprises qui les utilisent pour partager des informations, généralement selon le modèle client-serveur, dans lequel les stations de travail des employés accèdent à de puissants serveurs situés dans une salle informatique. Alors que l'informatique est devenue pour l'entreprise un outil incontournable de gestion, d'organisation, de production et de communication, les données mises en œuvre par le système d'information ainsi que les échanges internes et externes et les données professionnelles stockées sont exposés aux actes de malveillance de différentes types et dont la nature et la méthode d'intrusion sont sans cesse changeantes. La sécurité informatique en entreprise est une problématique importante car les effets sont de plus en plus lourds.

Notamment avec le développement de l'utilisation d'internet, de nombreuses entreprises connectent leur réseau, respectivement une partie du réseau, ce qui l'expose à une multitude de menaces potentielles qui sont de plus en plus ciblées et de plus en plus sophistiquées. Mais le réseau peut également être ciblé par des menaces venantes de l'intérieur de l'organisme. Il est donc indispensable pour les entreprises de se munir d'un pare-feu qui occupe une place stratégique pour parer certaines menaces et garantir une protection pour le réseau en cloisonnant certaines parties de ce dernier.

Parfois l'entreprise est située sur plusieurs sites géographiques. Par conséquent, l'interception ou l'altération des données sensibles qui transitent sur internet á destination de ses filiales représentent des risques non négligeables dans un contexte ou` les cyber-attaques sont de plus en plus nombreuses et sophistiquées. Par ailleurs, les nouvelles tendances de l'informatique permettent non seulement, aux utilisateurs d'avoir accès aux ressources. Mais, aussi, de transporter une partie du système d'information en dehors de l'infrastructure s´sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité á atteindre. Pour pallier á ce problème de sécurité et d'interconnexion, il est primordial d'implémenter des mécanismes et des solutions sûres assurant la confidentialité et la sécurité du transfert entre deux ou plusieurs entités d'un réseau public.

L'objectif de notre projet consiste donc á implémenter Audit de securité pour le reseau de l'université de medea garantissant l'interconnexion des différents sites de l'Université de MEDEA en toute sécurité, et de sécuriser les différents réseaux locaux de chaque site en sécurisant les différents périphériques intermédiaires et aussi l'accès distant aux ressources de l'entreprise pour les utilisateurs, et ceux d'une manière fiable et à moindre cout.

Pour présenter notre travail, nous avons organisé notre mémoire en quatre chapitres qui sont précédés par une introduction générale : Le premier chapitre est subdivisé en deux parties : Dans la première partie :nous présentons l'organisme d'accueil Université de Médea.la deuxième partie est dédiée á la présentation des généralités sur les réseaux : des notions de base sur le réseau informatique, des définitions, ses différentes classes ou typologies et les differents équipements d'interconnexion .Dans le deuxième chapitre nous nous intéresserons á la sécurité des réseaux, ses enjeux, scénario d'attaques et les outils de sécurisation. Le troisième chapitre consiste á étudier les moyens existants et ceux que nous avons choisi de mettre en œuvre pour la concrétisation de la solution proposée.

Le quatrième chapitre est partie pratique, dans laquelle nous entamons la configuration des vlans, du vpn site á site et clients site, des périphériques intermédiaires (sécurité d'accès au périphérique, sécurité des ports) et la configuration du pare feu. Enfin, notre mémoire s'achève avec une conclusion générale qui résume les connaissances acquises durant la réalisation du projet ainsi que les perspectives.

Chapitre 01

CHAPITRE 1 : Généralités sur les réseaux informatiques

1.1 Introduction

En reliant toutes les stations de travail, les périphériques, les terminaux et les autres unités de contrôle du trafic, le réseau informatique a permis aux entreprises de partager efficacement différents éléments (des fichiers, des imprimantes, …) et de communiquer entre elles, notamment par courrier électronique et par messagerie instantanée. Il a permis aussi de relier les serveurs de données, de communication et de fichiers.

Dans cette première partie, nous allons définir quelques notions sur les réseaux informatiques :

1.2 Définition d'un réseau

Un réseau informatique est un ensemble de moyens matériels et logiciels mis en œuvre pour assurer les communications (échange de messages entre utilisateurs, l'accès à distance à des bases de données ou encore le partage de fichiers) de données, et le partage de services entre ordinateurs, terminaux informatiques. Ces communications étaient, bien avant, destinées aux transports de données informatiques, bien qu'aujourd'hui, cela a évolué vers des réseaux qui intègrent, à la fois, des données, la voix, et la vidéo[1].

1.3 Intérêts d'un réseau

Un réseau informatique peut servir à plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels) ;
- La communication entre personnes (courrier électronique, discussion en direct) ;
- La communication entre processus (entre des machines industrielles par exemple) ;
- La garantie de l'unicité de l'information (bases de données) ;
- Le jeu vidéo multi-joueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de group-ware. Par exemple, la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement. Voici les avantages qu'offrent de tels systèmes :

- Diminution des couts grâce aux partages de données et de périphériques ;
- Standardisation des applications ;
- Accès aux données en temps utile ;

- Communication et organisation plus efficace.

1.4 Classification des réseaux

Les réseaux sont plus ou moins vastes et on en distingue trois catégories. Selon la couverture géographique qu'occupe un réseau, on peut les classer dans les grandes catégories suivantes [w1] :

1.4.1 LAN (Local Area Network, Réseau local)

Il s''étend sur quelques dizaines à quelques centaines de mètres. C'est un réseau local, il correspond par sa taille aux réseaux intra-entreprises et permet l'échange de données et le partage de ressources avec un débit entre une dizaine de Mb/s et Gb/s. Un réseau local est souvent administré par une seule entreprise.

Ethernet (IEEE 802.3) est l´une des technologies de LAN la plus répandue, Token-Ring (IEEE 802.5) est aussi l`une des technologies de LAN (topologie anneau).

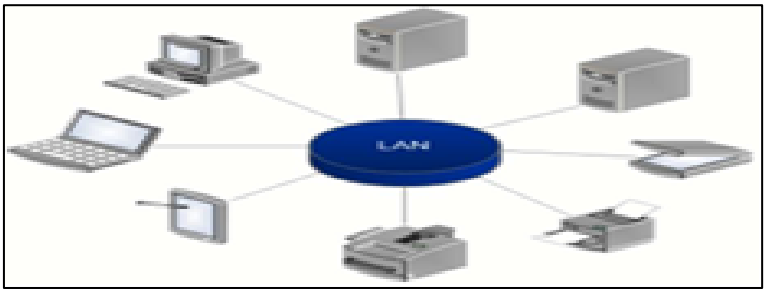


Figure 1.1 : Réseau LAN.

1.4.2 MAN (Metropolitan Area Network, Réseau métropolitain)

Le réseau métropolitain qui est également nommé réseau fédérateur, assure les communications de plusieurs sites à l'échelle d'une ville (quelques dizaines de kilomètres) [w2]**.**

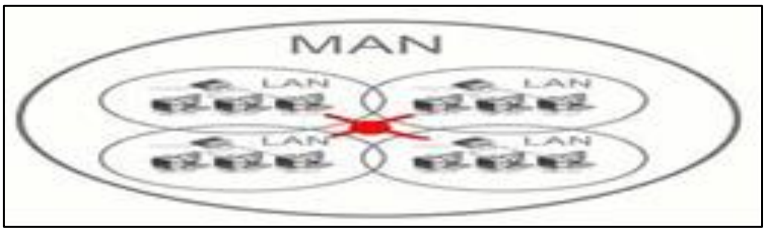


Figure 1.2 : Réseau MAN.

1.4.3 WAN (Wide Area Network, Réseau étendu ou public)

Réseau typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière, généralement celui des opérateurs. Le plus connu des WAN est Internet. Un WAN est en fait une succession de plusieurs LAN [2]**.**



Figure 1.3 : Réseau WAN.

1.4.4 SAN (Storage Area Network)

Un SAN est un réseau spécialisé qui fournit un accès au stockage de niveau bloc-réseau partagé ou stockage cloud qui, pour l'utilisateur, ressemble et fonctionne comme un disque de stockage physiquement connecté à un ordinateur [w2**]**.

1.4.5 WPAN (Wireless Personnel Area Network, Réseau personnel sans fil)

Les tout petits réseaux sans fil qui ont une portée d´une dizaine de mètres. Parmi ces réseaux nous trouvons :

- **Bluetooth (norme 802.15.1) :** Nous trouvons ce type de réseau dans beaucoup d´ordinateurs portables et dans de nombreux périphériques comme les appareils photos, les téléphones portables, …, il offre un débit de 1 Mb/s et une portée d´environ 30 mètres [w2].
- **ZigBee (norme 802.15.4) :** ZigBee est un protocole de haut niveau permettant la communication d'équipements personnels ou domestiques équipés de petits émetteurs radios à faible consommation ; Il est basé sur la norme IEEE 802.15.4 pour les réseaux à dimension personnelle (Wireless Personnel Area Networks : WPAN) [w1].

1.5 Les supports de transmission

Pour relier les diverses entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. Une de ses possibilités est l'utilisation de câbles. Il existe de nombreux types de câbles, mais on distingue généralement [3] :

- Le câble de type coaxial ;
- Le câble de type pair torsadé ;
- La fibre optique.

En plus des liaisons physiques, actuellement il y'a des réseaux qui utilisent la liaison sans fil comme support de transmission.

1.5.1 Le Câble coaxial

Le câble coaxial (en Anglais coaxial cable) a longtemps été le câblage de prédilection, pour la simple raison qu'il soit peu coûteux et facilement manipulable (poids, flexibilité, …). Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.



Figure 1.4 : Câble coaxial.

La capacité de transmission d'un câble coaxial dépend de sa longueur et les caractéristiques physiques des conducteurs et l'isolant. Il existe deux grands types de câbles coaxiaux [w3] :

- **Le câble coaxial fin (Thinnet ou 10base 2)** : est un câble de diamètre de 6 mm et peut transmettre un signal sur une distance d'environ de 185 mètres.
- **Le câble coaxial épais (Thicknet ou 10base5)** : Thick Ethernet est de diamètre de 12 mm et peut transmettre jusqu'à 500 mètre sa bande passante est de 10 Mb/s. Le thinnet et le thicknet utilisent les deux des connecteurs BNC (bayonet Neill concelman) servant à relier les câbles aux ordinateurs.

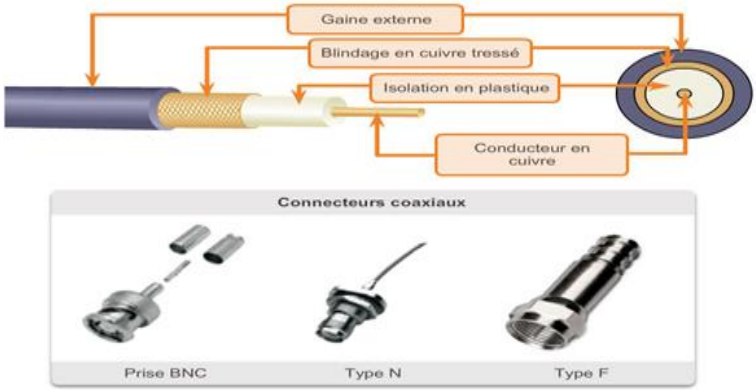


Figure 1.5 : Câble coaxial avec ses connecteurs.

1.5.2 La paire torsadée

Dans sa forme la plus simple, le câble à paire torsadée (Twisted Pair Cable) est constitué de deux brins de cuivre entrelacés de torsade et recouverts d'isolant. Le câble est souvent fabriqué à partir de plusieurs paire torsadées regroupées et placer à l'intérieur de la gaine productrice.

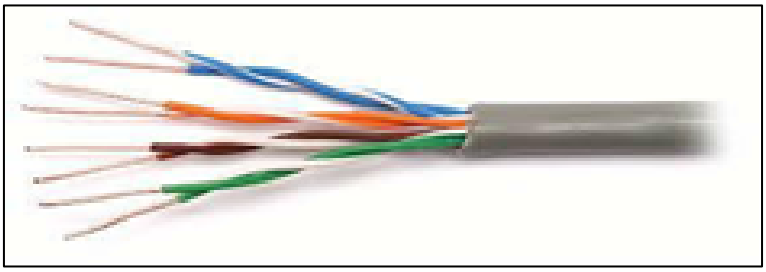


Figure 1.6 : Paire torsadée.

L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou aux autres sources (moteur, relais, transformateur, …) du réseau informatique. Nous distinguons plusieurs types de câbles à paires torsadées, UTP et STP sont les plus utilisées et les plus répondus pour les réseaux locaux.

1.5.2.1 La paire torsadée non blindées (UTP) : Les caractéristiques d'UTP :

- l'UTP est composé de deux fils de cuivre recouverts d'isolant ;
- La longueur maximale d'un segment est de 100 mètres.

1.5.2.2 La paire torsadée blindée (STP) : Le câble STP utilise une gaine de cuivre de meilleure qualité et plus protectrice que celle utilisé par le câble UTP. Les caractéristiques de ce câble :

- Les fils du cuivre d'une paire sont eux même torsadée ce qui fournit un excellent blindage pour le STP ;
- Il permet une transmission plus rapide et sur une longue distance.

1.5.3 La fibre optique

Le support de transmission le plus récent et apprécié. Il permet de transmettre des données sous forme d'impulsions lumineuses avec un débit supérieur à celui des autres supports filaires.

La fibre optique et constitué d'un cœur, d'une gaine optique, et d'une enveloppe protectrice comme présentée par la figure suivante [w3] :



Figure 1.7 : Fibre optique.

1.5.3.1 Caractéristiques de la fibre optique : Elle est caractérisée par :

- Légèreté ;
- Immunité au bruit ;
- Faible atténuation ;
- Tolère des débits de l'ordre de 100Mbits/s ;
- Largeur de bande de quelques dizaines de MH à plusieurs GH.

1.5.3.2 Types de fibre optique : Nous distinguons deux types de fibre optique :

- **La fibre multimode (MMF : Multi mode fiber) :**
  Le cœur de la fibre est volumineux que celui du deuxième type SMF (50/62.5 microns) ce qui permet la propagation de plusieurs modes (trajets) simultanément mais avec une plus grande dispersion et donc une perte de signal, elle utilise habituellement des LED (des diodes électroluminescentes) comme source du signal lumineux. La MMF est utilisée couramment dans des réseaux locaux ou dans des distances de quelques centaines de mètres au sein d'un réseau de campus [w3].
- **La fibre monomode (SMF : Single mode fiber) :**
  Elle a un cœur fin et ne peut transporter le signal que sur un seul trajet mais avec moins de dispersion, elle permet donc de transporter le signal à une distance plus longue que celle de la multimode (50 fois plus). Elle est adaptée couramment aux réseaux fédérateurs sur campus pour des distances de plusieurs milliers de mètres.

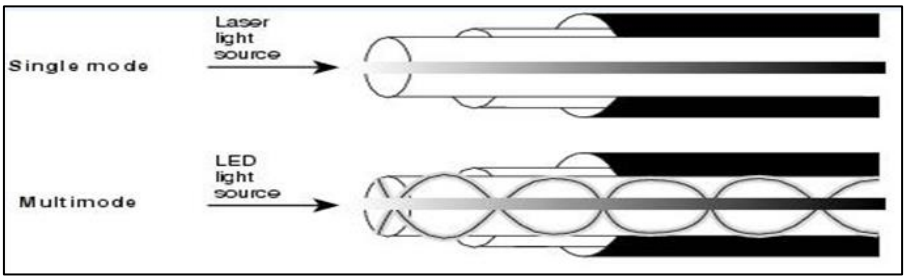


Figure 1.8 : Fibre optique monomode et multimode.

1.5.3.3 Connecteurs pour la fibre optique :

La lumière ne pouvant pas circulé que dans une seule direction, deux fibres sont requises pour prendre en charge le fonctionnement en mode duplex intégral. Par conséquent, les câbles de brassage en fibre regroupent deux câbles en fibre optique raccordés par une paire de connecteurs.

Nous distinguons différents types de connecteurs de la fibre optique [w3] :

a) **Connecteur ST (Straight-Tip) :** L´un des premiers types de connecteurs, il offre un verrouillage sécurisé grâce à un mécanisme de type baïonnette à tourner.
b) **Connecteur SC (Subscriber Connector) :** appelé aussi connecteur carré ou connecteur standard, il est largement utilisé dans des réseaux locaux et étendus. Ce type de connecteur peut être utilisé avec la fibre multimode et monomode.
c) **Connecteur LC unidirectionnel (Lucent Connector) :** version réduite du connecteur SC, il est parfois appelé petit connecteur ou connecteur local, il est de plus en plus répandu en raison de sa petite taille.
d) **Connecteur LC bidirectionnel multimode :** similaire au connecteur LC unidirectionnel mais avec un connecteur bidirectionnel

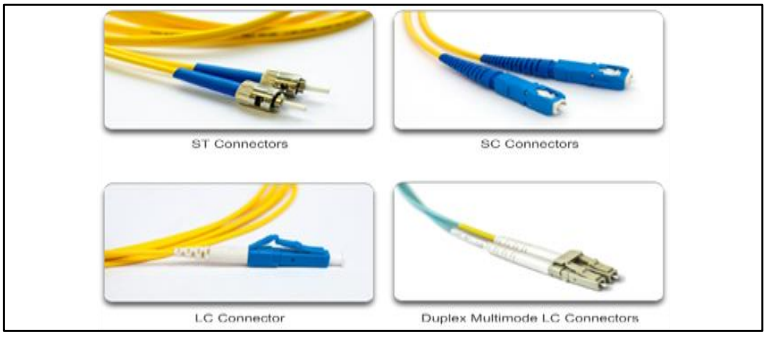


Figure 1.9 : Connecteurs de la fibre optique.

1.5.4 Les ondes radio

Les ondes radio sont des supports sans fil utilisées avec des réseaux de toutes tailles. Elles servent à relier des ordinateurs distants dans une zone géographique étendue [w1] :

- Ces ondes peuvent atteindre une vitesse de transmission de 11 Mbits/s ;
- Les liaisons radio sont utilisées pour à permettre plusieurs réseaux de communiquer ensemble sans avoir à passer par un câble ;
- Les ondes radio utilisent des fréquences radio pour l'émission.

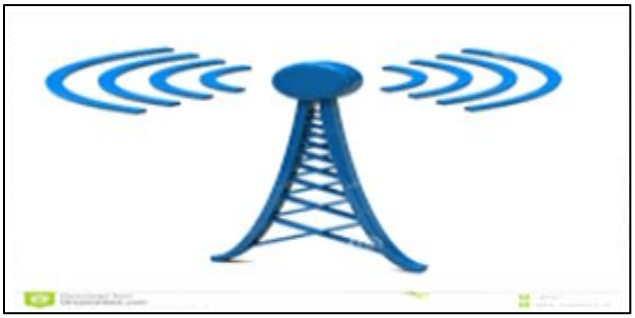


Figure 1.10 : Ondes radio.

1.5.5 Carte réseau

Une carte réseau (NIC: Network Interface Card) également nommée adaptateur réseau, est nécessaire à l'ordinateur pour envoyer des informations au réseau et en recevoir de celui-ci. Dans les ordinateurs de bureau, il s'agit d'une carte de circuits imprimés insérée dans un emplacement de la carte mère pour établir la connexion avec le média réseau [W1].

Dans les ordinateurs portables, ce composant est généralement intégré à l'ordinateur ou disponible sous la forme d'une carte PCMCIA (Personal Computer Memory Card International Association).

Les cartes PCMCIA sont également désignées sous le nom de cartes PC. Le type de carte doit être choisi en fonction du média et du protocole utilisés par le réseau local.

La carte communique avec le réseau via une connexion série et avec l'ordinateur par le bus interne de celui-ci. Elle utilise une demande d'interruption ou IRQ, une adresse d'entrée/sortie (E/S) et de l'espace en mémoire.



Figure 1.11 : Une carte réseau filaire.

Les critères ci-après sont à prendre en compte pour choisir une carte réseau :

- ✓ Protocoles : Ethernet, Token Ring ou FDDI ;
- ✓ Types de média câble : à paires torsadées, câble coaxial ou fibre optique ;
- ✓ Type de bus système : PCI ou ISA.

1.6 Les topologies d'un réseau

Les topologies d'un réseau fournissent une représentation visuelle des connexions réseau. Il existe deux types de diagrammes de topologie : topologie physique et topologie logique [w4].

1.6.1 Topologie logique

Par opposition à la topologie physique, représente la façon dont les données transitent sur les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

1.6.2 Topologie physique

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau. Il y a quatre topologies physiques qui sont habituellement connues [w1] :

1.6.2.1 Topologie en bus : Dans une topologie en bus tous les périphériques sont connectés à un seul canal de transmission par des câbles intermédiaires.

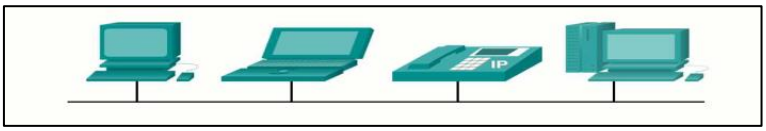


Figure 1.12 : Topologie en bus.

1.6.2.2 Topologie en étoile (la plus utilisée) : Dans un réseau en étoile, la forme physique du réseau ressemble à une étoile. Pour parler à une autre entité on passe par le matériel central (qui peut être le routeur, switch, ...). En pratique, dans un réseau d'entreprise en étoile, on trouve un switch au centre**.**

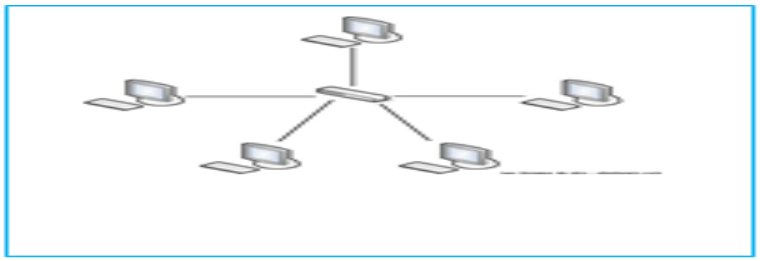


Figure 1.13 : Topologie en étoile.

1.6.2.3 Topologie en anneau : Un réseau en anneau a la forme d'un anneau. Dans un tel réseau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour (en utilisant un jeton).

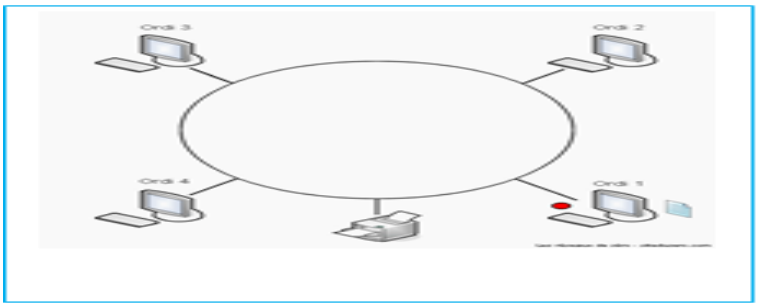


Figure 1.14 : Topologie en anneau.

1.6.2.4 Topologie maillée : est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Le principe de la topologie maillée est de relier tous les ordinateurs entre eux (aucun risque de voir une isolation du réseau si un des points névralgiques tombe en panne.

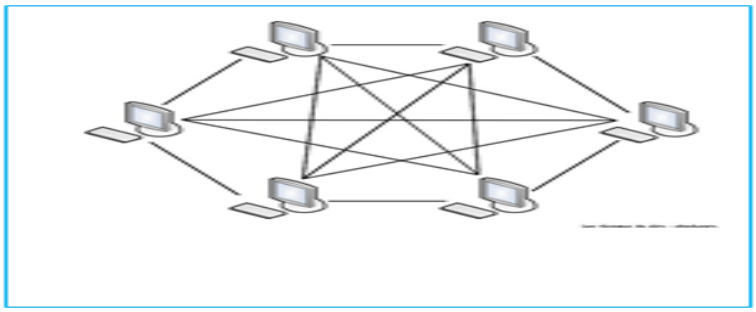


Figure 1.15 : Topologie maillée.

1.7 Réseau fiable

L'exécution d'une suite d'applications sur un réseau nécessite qu'il répand aux certains exigences au but de garantir l'ensemble des services adoptés par ce dernier. Par conséquence un réseau pour qu'il soit fiable, il doit avoir quatre caractéristiques de base [w3].

1.7.1 Tolérance aux pannes

Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes, de telle sorte que le nombre de périphériques affectés soit le plus faible possible. Il est également conçu de façon à permettre une récupération rapide en cas de panne.

1.7.2 Évolutivité

Un réseau évolutif est un réseau qui donne la possibilité d'ajouter des utilisateurs supplémentaires et de prendre en charge des nouvelles applications sans perdre des performances des services fournis aux utilisateurs de réseau ou de qualité de service.

1.7.3 Qualité de service (QoS)

La qualité de service (QdS) (ou Quality of Service (QoS)) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets.

1.7.4 Sécurité

La sécurité d'une infrastructure réseau repose sur plusieurs points. Elle implique non seulement une sureté des périphériques par une interdiction de tout accès non autorisé , mais aussi la disponibilité des données aux utilisateurs confirmés, bien sûr sans menace, tout en garantissant que les données ne soient pas modifiées lors d'une opération de transmission.

1.8 Modèle OSI

L'organisme ISO (International Organization for Standardization) en français (Organisation Internationale de Normalisation) a défini en 1984 un modèle de référence, nommé modèle OSI (de l'anglais Open Systems Interconnection) destiné à normaliser les échanges entre deux machines dans les systèmes informatiques. La normalisation émane de la volonté des gouvernements d'harmoniser les technologies afin d'assurer la compatibilité des équipements. Le modèle OSI décrit la manière dont deux éléments d'un réseau (station de travail, serveur, ...) communiquent, en décomposant les différentes opérations à effectuer en sept étapes successives, qui sont nommées [4].

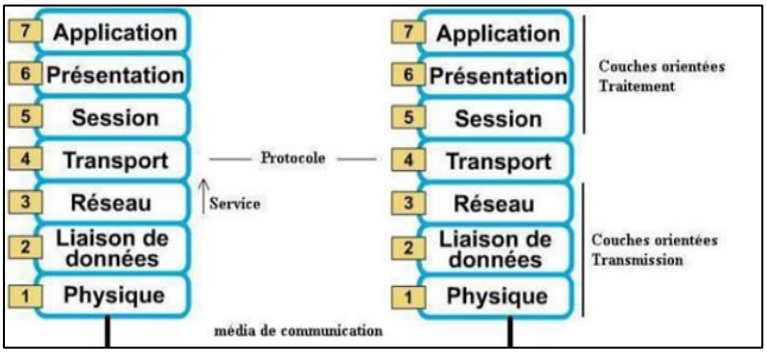


Figure 1.16 : Diagramme du modèle OSI

Les couches 1, 2, 3, 4 sont dites basses et sont orientées transmission. Les couches 5, 6 et 7 sont dites hautes et sont orientées traitement.

Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au-dessus d'elle en lui évitant les détails d'implémentation nécessaires.

Deux couches de même niveau sont appelées couches homologues et chaque couche de niveau N d'une machine gère la communication avec la couche de niveau N d'une autre machine en suivant un protocole de niveau N.

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

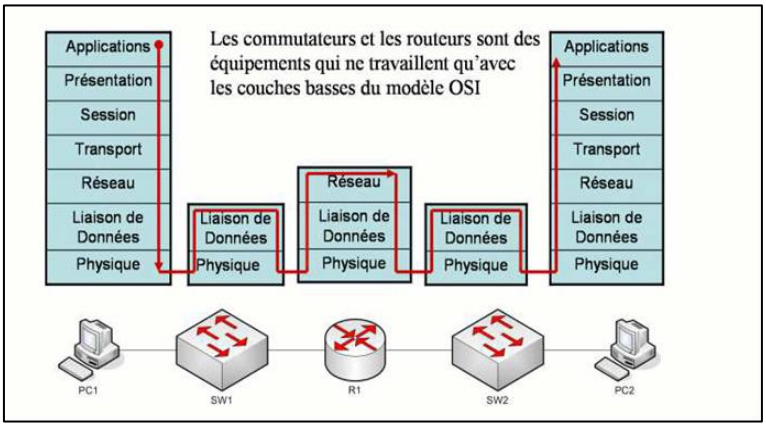


Figure 1.17 : Communication entre les périphériques finaux.

L'évolution de l'information de la couche application à la couche physique se nomme l'encapsulation. Ce processus est inversé lorsque les données sont arrivées à la destination, dans laquelle l'ensemble des changements appliqués sur les trames arrivés est dite dé-encapsulation.

Le modèle OSI se compose de sept couches suivantes [5] :

- **La couche liaison des données** : Les protocoles de cette couche sont les responsables de la construction des trames et la gestion d'adressage physique.
- **La couche réseau** : Cette couche s'intéresse aux données utiles dans la trame et les adresses des périphériques sur le réseau pour assurer l'échange des données entre des périphériques finaux bien identifiés.
- **La couche transport** : Son rôle est de rassembler et segmenter les données pour les préparer à la couche réseau, ainsi qu'elle indique les fautes de transport et les corriger.
- **La couche session** : Elle s'occupe non seulement de dialogue et la gestion d'échange des données entre les périphériques mais aussi de la sureté de connexion.
- **La couche présentation** : Elle donne une représentation compréhensible des données pour l'utilisateur ainsi que les applications.
- **La couche application** : Cette couche fait l'interface entre l'homme et la machine. exemple : navigateur (Firefox, Safari, Chrome, …), logiciel de messagerie (Outlook, Thunderbird, …).

1.9 Modèle TCP/IP

C'est au début des années 1970 que le premier modèle de protocole possédant plusieurs couches pour les communications inter-réseau a été créé. Celui-ci est appelé modèle Internet ou encore modèle TCP/IP grâce aux protocoles TCP et IP qui sont les plus dominants dans ce modèle. Il est défini sous la forme de quatre catégories de fonctions ou quatre couches [6].

1.9.1 Présentation du protocole TCP/IP

Au contraire des protocoles qui sont spécifiques chacun à un fournisseur ou une entreprise, le protocole TCP/IP est une norme ouverte.

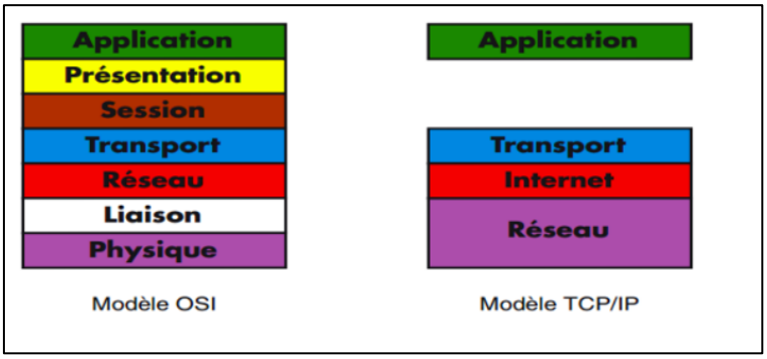


Figure 1.18 : Comparaison entre le modèle OSI et TCP/ IP.

1.9.1.1 Le protocole IP (Internet Protocol) : Ce protocole permet de gérer L'acheminement des paquets d'une machine à une autre, ainsi que l'adressage.

1.9.1.2 Le protocole TCP (Transmission Control Protocol) : TCP est le protocole responsable de transmission des données contenues dans les paquets envoyés ainsi que leur ordre de réception. Le protocole TCP exige la confirmation de la réception des données et assure ainsi une fiabilité de communication entre les différents hôtes du réseau. En cas de perte de données lors de leur transfert, la retransmission des données perdues est assurée par ce protocole.

1.9.2 Descriptions du modèle TCP/IP

Le modèle TCP/IP contient une suite de quatre couches comme suit [4] :

1.9.2.1 La couche application :

- ✓ Elle est la couche de communication qui s'interface avec les utilisateurs. Exemples de protocoles applicatifs : HTTP, DNS, DHCP, FTP, …
- ✓ Elle s'exécute sur les machines hôtes.

1.9.2.2 La couche transport : Le TCP est un de ses protocoles.

- ✓ Elle est responsable du dialogue entre les hôtes terminaux d'une communication. Les applications utiliseront TCP pour un transport fiable et UDP sans ce service.
- ✓ Les routeurs et les pare-feu opèrent un filtrage au niveau de la couche transport

1.9.2.3 La couche internet : Parmi ses protocoles elle contient le protocole IP.

- ✓ Elle permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IPv4 ou IPv6.
- ✓ Les routeurs transfèrent le trafic IP (IPv4, IPv6).

1.9.2.4 La couche accès réseau :

- ✓ Le protocole TCP/IP ne s'occupe pas de la couche accès réseau.
- ✓ Elle organise le flux binaire et identifie physiquement les hôtes.
- ✓ Elle place le flux binaire sur les supports physiques.
- ✓ Les commutateurs, cartes réseau, connecteurs, câbles, … font partie de cette couche.

1.10 Equipements d'Interconnexion des réseaux

Il faut rappeler que l'interconnexion est un mécanisme qui consiste à mettre en relation, indépendamment de la distance qui les sépare et des protocoles qu'elles utilisent, des machines appartenant à des réseaux physiquement distincts.

Dans ce qui suit, nous présenterons les principaux équipements matériels mis-en place dans les réseaux locaux et qui sont [w5] :

1.10.1 Le répéteur (Repeater)

Les câbles ont une distance maximale de fonctionnement due à l'affaiblissement du signal, le répéteur permet d'amplifier ce signal et d'augmenter la taille d'un réseau, afin d'étendre la distance du câblage. C'est un équipement simple qui opère au niveau 1 du modèle OSI (couche physique), et qui ne nécessite aucune administration. Le répéteur génère de nouveau un signal à partir du signal reçu. On distingue deux catégories du répéteur.



Figure 1.19 : Répéteur.

1.10.2 Les concentrateurs (hubs)

Le concentrateur est un périphérique qui opère au niveau 1 du modèle OSI (couche physique), il permet de connecter plusieurs machines entre elles ; il a pour but de concentrer le trafic réseau qui provient de plusieurs hôtes, et aussi de régénérer le signal. Il réduit le trafic (segmentation). Son unique but est de récupérer les données binaires provenant d'un port et de les diffuser sur l'ensemble des ports. Ils servent à raccorder deux segments de câbles ou deux réseaux identiques (Ethernet) qui constituent alors un seul réseau logique. Ils sont en général dotés d'un port spécial appelé "Up Link".



Figure 1.20 : Concentrateur.

1.10.3 Modem

Le modem ou modulateur-démodulateur est un équipement nécessaire pour relier l'ordinateur à une ligne téléphonique. Il convertit les signaux numériques formés par les données issues de l'ordinateur en signaux analogiques compatibles avec une ligne téléphonique standard. Dans l'ordinateur qui reçoit les données, le modem démodule les signaux, autrement dit les retransforme en données numériques. Les modems peuvent être installés comme des composants internes [w6].



Figure 1.21 : Modem.

1.10.4 Les ponts (bridges)

Un pont est un équipement informatique d'infrastructure de réseaux de type passerelle, il opère au niveau logique c'est-à-dire au niveau de la couche 2 du modèle OSI (couche liaison de données), il permet de relier deux réseaux identiques ou deux parties de même réseau. Le pont travail comme un relais qui transmet d'un réseau à l'autre les trames dont l'adresse ne figure pas dans le premier réseau et permet donc aux deux éléments qu'il relie de fonctionner indépendamment. Son usage le rapproche fortement de celui d'un commutateur (switch), à l'unique différence que le commutateur ne convertit pas les formats de transmissions de données. Le pont ne doit pas être confondu avec le routeur.

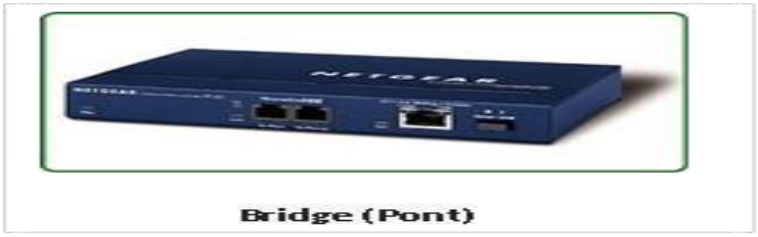


Figure 1.22 : Pont.

1.10.5 Les commutateurs (Switch)

C'est un équipement qui relie plusieurs segments dans un réseau informatique. Il analyse les trames arrivant sur les ports d'entrées et les filtre pour aiguiller sur les ports adéquats. Il dispose d'une table d'adresses MAC des machines connectés, et qui opère au niveau 2 du modèle OSI (couche liaison de données). La commutation est un des deux modes de transport de trames au sein des réseaux informatiques et de communication, l'autre étant le routage.

Dans les réseaux locaux (LAN), il s'agit le plus souvent d'un boîtier disposant de plusieurs ports RJ45 (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub). Il existe aussi des commutateurs pour tous les types de réseau en mode point à point comme pour les réseaux ATM, relais de trames, ... Il est fréquent qu'un commutateur intègre, par exemple, le Spanning Tree Protocol que l'on rencontre dans les ponts. Le commutateur est d'ailleurs souvent vu d'une manière réductrice comme un pont multiport. Sa présence permet d'optimiser les performances des réseaux et d'autoriser les utilisateurs d'un réseau à accéder à toutes les ressources disponibles sur le réseau.



Figure 1.23 : Commutateur catalyst.

1.10.6 Les passerelles (Gateway)

Permettant de relier des réseaux informatiques de types différents, par exemple un réseau local et le réseau internet. Une passerelle est toujours spécifique aux deux architectures qu'elle permet de réunir. Une passerelle peut agir sur toutes les couches du modèle OSI. Donc il existe différents types de passerelles [w6] :

- Un répéteur est une passerelle de niveau 1.
- Un pont est une passerelle de niveau 2.
- Un routeur est une passerelle de niveau 3.

La passerelle reformate les paquets, les données entrantes sont « dépouillées » de leur pile de protocole (dés-encapsulées) et « rhabillées » (ré-encapsulées) avec l'autre pile de protocole.

La passerelle remplace une pile de protocole par une autre. Les passerelles sont des traducteurs de protocoles. Les passerelles sont souvent utilisées pour les réseaux qui ne disposent pas de TCP/IP (par exemple, les réseaux NetWare qui fonctionnent sous SPX/IPX et qui veulent avoir un accès à Internet).

1.10.7 Les routeurs

Un routeur est un élément intermédiaire dans un réseau informatique, assurant le routage des paquets en choisissant le chemin selon un ensemble de règles formant la table de routage. Il opère au niveau 3 du modèle OSI (couche réseau). C'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter .il est capable d'interconnecter plusieurs réseaux utilisant le même protocole. Il permet d'interconnecter deux entités de la couche Réseau, deux réseaux proprement dits [7].



Figure 1.24: Routeurs.

Le routeur assure les fonctions de routage comme son nom l'indique. Il sélectionne un parcours approprié pour diriger les messages vers leurs destinations. La fonction de routage traite les paquets en fonction de leur adresse réseau définie par le masque de sous-réseau et les redirige selon l'algorithme de routage et sa table associée. Ces protocoles de routage sont mis en place selon l'architecture des réseaux et les liens de communication inter sites et inter-réseaux.

Un routeur est un type spécial d'ordinateur. Il possède les mêmes composants de base qu'un ordinateur de bureau standard. Il est doté d'un processeur (UC), de mémoire, d'un système de bus, ainsi que de diverses interfaces d'entrée/sortie. Cependant, les routeurs sont conçus pour assurer des fonctions très spécifiques que n'effectuent pas en général les ordinateurs de bureau. Par exemple, des routeurs peuvent se connecter, assurer la communication entre deux réseaux et déterminer le meilleur chemin pour les données à travers les réseaux connectés.

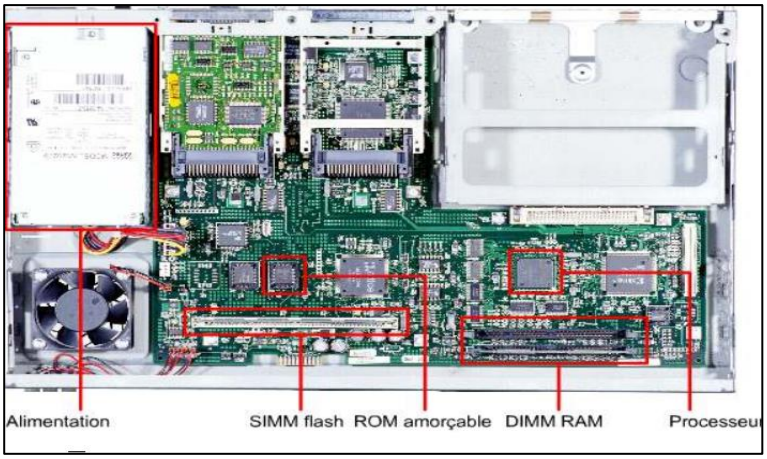


Figure 1.25 : Composants internes d'un routeur 2600.

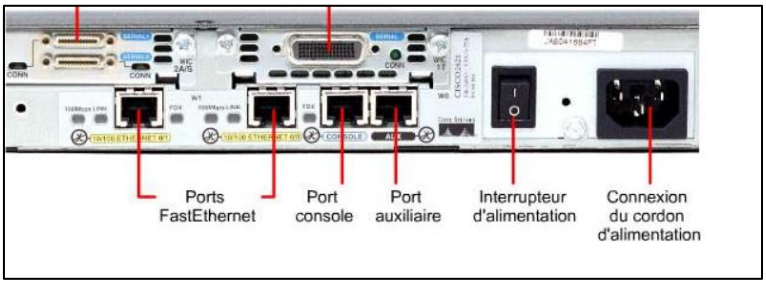


Figure 1.26 : les ports d'un routeur 2600.

Les principaux composants internes du routeur sont la mémoire vive (RAM), la mémoire vive rémanente (NVRAM), la mémoire morte (ROM), la mémoire Flash, le processeur et les interfaces [w6] :

- **RAM :** La mémoire RAM est utilisée pour les informations de table de routage, la mémoire cache à commutation rapide, la configuration courante et les files d'attente de paquets.

- **NVRAM :** La mémoire NVRAM est utilisée pour stocker un fichier de configuration de démarrage/sauvegarde
- **ROM :** la mémoire ROM est utilisée pour stocker de manière permanente le code diagnostic de démarrage.
- **Flash :** la mémoire flash est utilisée pour stocker les images de l'IOS.
- **Interfaces :** les interfaces fournissent la connectivité LAN et WAN, on distingue les interfaces Ethernet (10 MB/s), interfaces Fast-Ethernet (100 MB/s), interfaces Giga byte Ethernet (plus 1 Gb/s).
- **Console :** le port console fournit un accès physique pour la configuration initiale via un câble console (câble inverse) qui est propriétaire Cisco.
- **Port auxiliaire (AUX) :** il fournit un accès à distance via une ligne téléphonique pour la configuration des routeurs.

1.11 Les protocoles de routage

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. Nous retenons les protocoles suivants [w3] :

- ✓ **États de lien** : ils s'appuient sur la qualité et les performances du média de communication qui les séparent. Ainsi chaque routeur est capable de dresser une carte de l'état du réseau pour choisir la meilleure route comme OSPF.
- ✓ **Vecteur de distance** : chaque routeur communique aux autres routeurs la distance qui les sépare. Ils élaborent intelligemment une cartographie de leurs voisins sur le réseau comme le RIP.
- ✓ **Hybride des deux premiers** : comme EIGRP.

Le routeur route les paquets reçus depuis ses interfaces selon l'organigramme suivant :

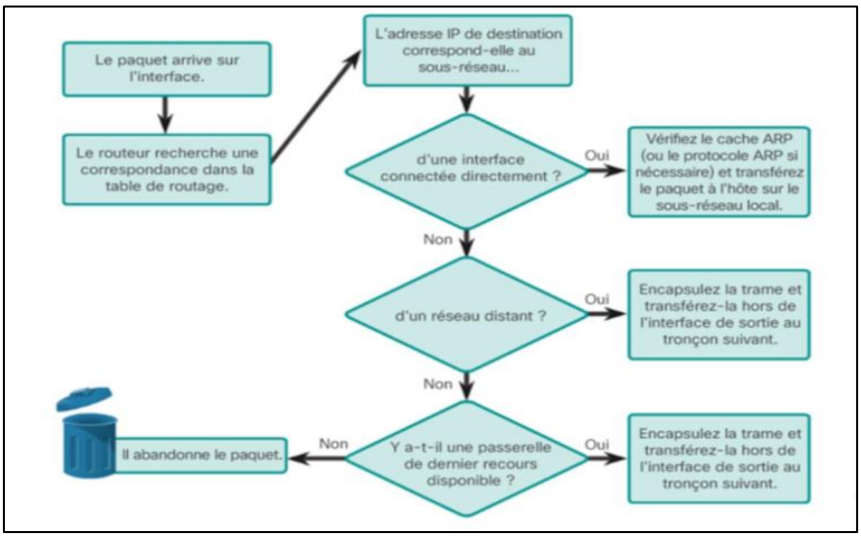


Figure 1.27 : Diagramme de décision de routage.

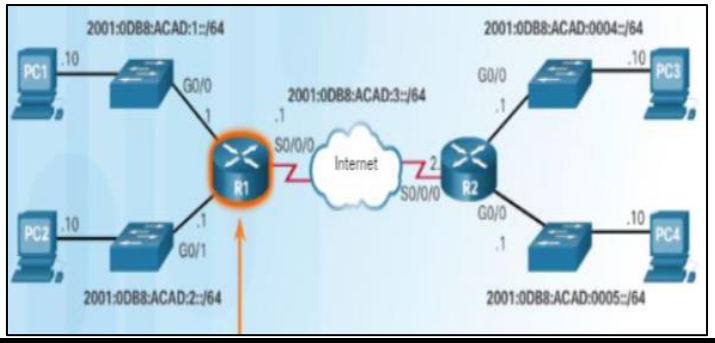
Les protocoles couramment utilisés sont :

- ✓ Routing Information Protocol (RIPV1, RIPV2) ;
- ✓ Open Shortest Path First (OSPFV4, OSPFV6) ;
- ✓ Enhanced Interior Gateway Routing Protocol (EIGRPV4, EIGRPV6).
  Plus de detail sur les protocoles de routage est présenté dans **l'annexe B**.

Les périphériques ISR (routeurs à services intégrés) prennent en charge les protocoles de routage IPV6 dynamiques suivants :

- RIPng (protocole RIP nouvelle génération) ;
- OSPF V3 ;
- EIGRP V6.

La prise en charge des protocoles de routage IPV6 dynamiques dépend du matériel et de la version du logiciel IOS (Version ≥ 15). Pour permettre aux routeurs IPV6 de transmettre le trafic, nous devons configurer la commande de configuration globale IPV6 unicast-routing.




```
R1(config)# ipv6 router ?
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  ospf      Open Shortest Path First (OSPF)
  rip       IPv6 Routing Information Protocol (RIPv6)
```

Figure 1.28 : Protocoles de routage pour IPV6.

1.11.1 La Distance Administrative (AD)

Il est possible de configurer un routeur avec plusieurs protocoles de routage et des routes Statiques. Dans ce cas, la table de routage peut disposer de plusieurs sources de route pour le même réseau de destination. Le logiciel Cisco IOS utilise la distance administrative (AD) pour déterminer la route à installer dans la table de routage.

La distance administrative représente le degré de fiabilité de la route. Plus il est faible, plus la source de la route est fiable. Si le routeur doit choisir entre une route statique et une route EIGRP, la route statique est prioritaire [w1].

Origine de la route	Distance administrative
Connecté	0
Statique	1
Résumé du routage EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
protocole de routage IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

Figure 1.29 : Distance Administrative (AD).

1.12 Conclusion

Dans ce chapitre, nous avons présenté les différentes notions sur les réseaux informatiques, les types de réseaux, les topologies réseaux, les périphériques d`interconnexion, les supports de transmission. Nous avons présenté aussi les deux principaux modèles OSI et TCP/IP avec leurs différentes couches ainsi que les protocoles de routage. Le chapitre suivant sera consacré à la sécurité des réseaux et les différents risques qui peuvent cibler un réseau.

Chapitre 02

Chapitre 02

CHAPITRE 02 : Cyber sécurité du réseau

2.1 Introduction

La sécurité des réseaux depuis quelques années, a vu son importance s'accroître au point de devenir une priorité. Des outils automatisés de plus en plus complexes, des risque cible la sécurité des réseaux et menacent en permanence l'intégrité des systèmes d'information. Les mécanismes de la sécurité deviennent fortement consommatrices de temps. Donc, il faut améliorer la gestion de la sécurité pour garantir la qualité de service.

La cyber sécurité englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données, sensibles ou non, au sein d'une infrastructure numérique. Et cela nécessite d'utiliser des protocoles, des technologies, des périphériques et des programmes permettant de sécuriser les données et de limiter les risques qu'ils soient externes ou internes. La plus part des menaces externes sont diffusées par internet comme les virus, chevaux de troie, les logiciels espions et publicitaires, attaques zero-day, attaques de pirates et attaques par déni de service. Non seulement les menaces externes doivent être prisent en considération lors de la sécurisation d'un réseau mais aussi celles qui sont internes, dont l'expérience montre que la plupart des violations des données est une conséquence principalement d'une mal utilisation à l'intérieur du réseau à cause d'une perte ou d'un vol de périphériques, de la mauvaise utilisation d'un périphérique par un employé ou dans un contexte professionnel, d'un employé malveillant.

Par conséquent, lors d'une création d'une politique de sécurité, il est important de prendre en compte à la fois les menaces externes et internes. La protection d'un réseau ne consiste pas à utiliser une solution unique pour toutes les menaces existantes. Pour cette raison, plusieurs solutions de sécurité sont appliquées en plusieurs couches, en cas d'une faille au niveau d'un des composants de sécurité d'autres peuvent prendre la relève. Au niveau des entreprises et afin d'augmenté le degré de sécurité, tous les périphériques du réseau doivent être sécurisés, cela inclut les routeurs, les commutateurs, les périphériques finaux et même les dispositifs de sécurité.

2.1 Objectifs

Les informations ou données représentent un patrimoine essentiel de n'importe quel organisme, qu'il convient de protéger. La sécurité de ces informations vise à assurer la sécurité du réseau de l'organisme en assurant les propriétés suivantes [7] :

- **L'authentification :** L'identification des utilisateurs est primordiale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- **L'intégrité :** S'assurer que les données ne sont pas altérées de façon fortuite, les éléments considérés doivent être exactes et complets.
- **La confidentialité :** Limiter l'accès aux informations qu'aux personnes autorisées.
- **La disponibilité :** Garantir le fonctionnement du système sans faille, et l'accès aux services et ressources installées avec le temps de réponse voulu.
- **La non-répudiation** : permettant de garantir qu'une transaction ne peut être niée.

2.2 Terminologie

L'ensemble des termes utilisés dans le domaine de la cyber sécurité peut se résumer comme suite [w7] :

- **Vulnérabilité** :Une vulnérabilité ou une faille est une faiblesse dans un système ou un logiciel permettant à un attaquant de porter atteinte à la sécurité d'une information ou d'un système d'information.
- **Menace** :Ce sont les actions potentiellement nuisibles à un système informatique. Les menaces peuvent être le résultat de plusieurs actions en provenance de plusieurs origines.
- **Risque :**Un risque désigne la probabilité d'un événement dommageable ainsi que les coûts qui s'ensuivent, le risque dépend également des montants des valeurs à protéger.
- **Attaque :**Une attaque est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant des systèmes et généralement préjudiciables, les virus est un exemple d'attaque. Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives.

    - **Attaques passives** : Ce type d'attaque consiste à surveiller et analyser les communications non protégées, décrypter le trafic au cryptage faible, le but de l'attaquant est d'obtenir les informations transmises sur le réseau surtout les informations d'authentification comme les mots de passe, numéro de carte, Email, …. L'attaque peut entrainer la divulgation des informations à un attaquant sans l'autorisation ou la connaissance de l'utilisateur. Exemple : Ecoutes indiscrètes ou surveillance de transmissions [8].
    - **Attaques actives :** Ces attaques impliquent certaines modifications du flot de données ou création d'un flot frauduleux [9].

Nous distinguons les types d'attaques suivants :

- **Attaques par rebond** : Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond, consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond [w8].
- **Attaque par déni de service** : Une « attaque par déni de service » est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou les ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés. Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

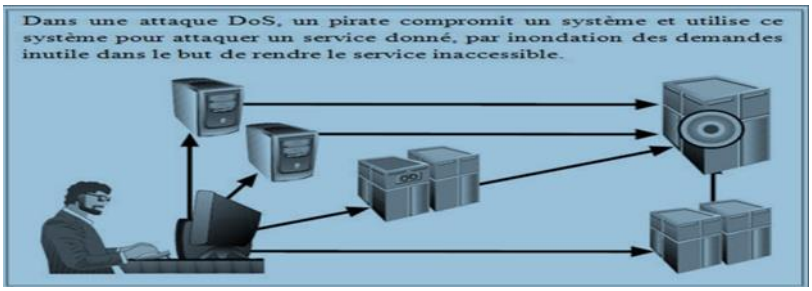


Figure 2.1 : Attaque par déni de service

- **La technique dite « par réflexion** » : La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau [w8].
- **Attaque par usurpation d'adresse IP (IP spoofing)** : L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis. La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu) [w8].
- **Virus** : un virus est un logiciel malveillant intégré à un autre programme afin d'exécuter des fonctions particulières indésirables sur l'ordinateur de l'utilisateur.

- **Cheval de Troie** : se distingue uniquement des vers et des virus par le fait qu'il a été entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un instrument d'attaque [w9].
- **Attaques de programmes malveillants** : Un ver exécute un code et installe des copies de lui-même dans la mémoire de l'ordinateur infecté, ce qui infecte par la suite d'autres ordinateurs hôtes.
- **Analyseurs réseau " sniffers "** : c'est un dispositif permettant d'écouter le trafic sur un réseau, c'est-à-dire d'y capturer les informations qui y circulent.
- **Attaque Man In The Middle " Homme au milieu "** : est un scenario d'attaque où lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

2.3 Les solutions de sécurité

Les exigences de sécurité du réseau doivent prendre en compte l'environnement réseau, ainsi que les différentes applications et les exigences informatiques. Les réseaux domestiques et professionnels doivent pouvoir sécuriser leurs données tout en garantissant la qualité de service attendue de chaque technologie. En outre, la solution de sécurité mise en œuvre doit être capable de s'adapter aux nouvelles tendances et à l'évolution du réseau. Les composants de sécurité réseau d'un réseau domestique ou d'un réseau de petit bureau doivent inclure, au minimum des antivirus et des logiciels de protection contre les programmes malveillants où leur fonction est d'empêcher la contamination des périphériques finaux par un programme malveillant. Les réseaux plus étendus et les réseaux des grandes entreprises ont souvent d'autres exigences relatives à la sécurité [w1].

2.3.1 Définition d'un DMZ

Si une entreprise doit héberger elle-même un site web public complet avec des serveurs tel qu'un serveur de messagerie, elle pourra envisager l'emploi d'un pare-feu avec deux interfaces (interne et externe) et lui laisser la tâche de créer les règles de traduction qui dirigent le trafic en entrée vers les serveurs appropriés au réseau d'entreprise. Cela peut s'avérer désastreux si un pirate a des vues sur ce réseau. D'où l'idée de recourir à une DMZ (DeMilitarized Zone).

Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne). La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante [w10] :

- ✓ Trafic du réseau externe vers la DMZ autorisé.
- ✓ Trafic du réseau externe vers le réseau interne interdit.
- ✓ Trafic du réseau interne vers la DMZ autorisé.
- ✓ Trafic du réseau interne vers le réseau externe autorisé.
- ✓ Trafic de la DMZ vers le réseau interne interdit.
- ✓ Trafic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais il n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

2.3.2 Listes de contrôles d'accès (ACL)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter [10].

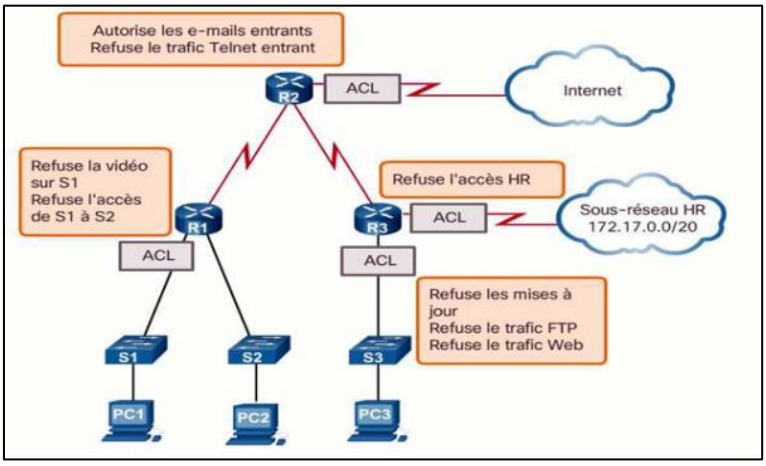


Figure 2.2 : Exemples sur les ACL.

L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie. Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internet work Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau.

2.3.2.1 L'intérêt d'utiliser des ACL : Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès [w11] :

- ✓ Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances.
- ✓ Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée.
- ✓ Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section.
- ✓ Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- ✓ Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- ✓ Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

2.3.2.2 Les types des listes de contrôle d'accès : Il existe trois types d'ACL [w11] :

- ➢ **Listes de contrôle d'accès étendues** : Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.
- ➢ **Listes de contrôle d'accès standard** : Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.
- ➢ **Listes de contrôle d'accès nommées** : Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

2.3.3 VLAN

Les VLAN représentent un procédé de regroupement des périphériques dans un LAN d'une manière indépendante de la localisation géographique sur le réseau. Un VLAN permet aux administrateurs de segmenter le réseau en groupes par rapport à ses fonctions, quel que soit l'emplacement physique des utilisateurs ou des périphériques avec une garantie de communication entre ces dernies comme s'ils étaient sur la même section. Les VLAN entrainent un certain niveau de sécurité. En effet, les attaques utilisant le broadcast sont contenues au sein d'un VLAN (DHCP spoofing, overflow, …) [w12].

De plus, des règles de sécurité pourront être ajoutées sur les communications entre les VLAN permettant ainsi d'apporter une nouvelle couche de sécurité à la défense en profondeur de l'entreprise. Par Conséquent les données sensibles seront séparés du reste du réseau ce qui réduit les menaces de violation. Il existe différents types de VLAN tels que [w12] :

- **VLAN par port :** Chaque port des commutateurs est configuré pour être affecter à un VLAN.
- **VLAN par adresse** : Chaque adresse MAC représente un VLAN ce qui crée une indépendance par rapport à la localisation géographique.
- **VLAN par protocole** : Dans ce type la segmentation est faite par rapport aux hôtes qui utilisent un protocole similaire ou par mot de passe.

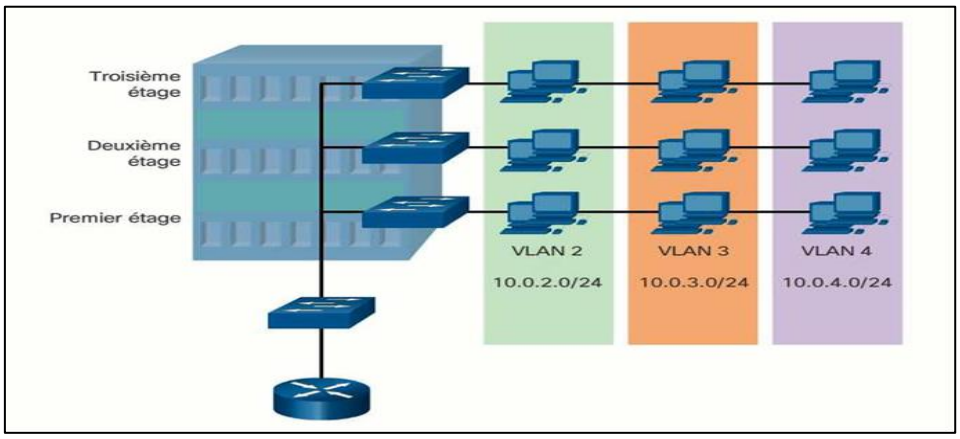


Figure 2.3 : Les VLAN dans un réseau.

2.3.4 Présentation du protocole AAA

AAA est un protocole de sécurisation des équipements dont les trois lettres signifient : Authentication, Authorization et Accounting [11].

- **Authentication (authentification en français)** : fait référence à la capacité que l'équipement aura de vérifier l'identité de l'utilisateur. C'est un processus qui va décider si un utilisateur donné peut accéder au réseau ou à l'équipement sur lequel AAA est configuré.
- **Authorization (autorisation en français) :** fait quant à lui référence aux ressources auxquelles l'utilisateur va pouvoir accéder, et les opérations qu'il va être en mesure d'effectuer.
- **Accounting (gestion des comptes)** : concerne les données et les informations se rapportant au profil de l'utilisateur.

2.3.5 VPN (Virtuel Private Network)

Un VPN est une technologie réseau qui crée un tunnel chiffré entre une machine sur Internet dotée d'une adresse IP quelconque et une passerelle d'accès d'un réseau privé. La machine distante se voie dotée lors de l'établissement du tunnel d'une adresse supplémentaire appartenant au réseau privé qu'elle cherche à atteindre [w13].

Le but d'un réseau virtuel (VPN) est de fournir aux utilisateurs et administrateurs du système d'administration des conditions d'exploitation, d'utilisation et de sécurité à travers un système public identique à celle disponible sur un réseau privée. En d'autres termes, nous voulons regrouper des réseaux privés, séparé par un réseau public (Internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et tout en gardant l'aspect sécurisé qui était assuré par la coupure logique au réseau Internet [w13].

Il existe 02 grandes catégories d'utilisation des VPN. En étudiant ces schémas d'illustration, il est possible d'isoler les fonctionnalités indispensables des VPN.

2.3.5.1 VPN client à site ou VPN nomade ou VPN Remote-Access : Le VPN nomade est utilisé pour permettre à des utilisateurs nomades d'accéder au réseau privé. Il est utilisé pour accéder à certaines ressources prédéfinies d'une entreprise sans y être physiquement présent. Cette opportunité peut ainsi être très utile au commercial ou au cadre qui souhaite se connecter au réseau de son entreprise tout en étant géographiquement éloigné. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN.

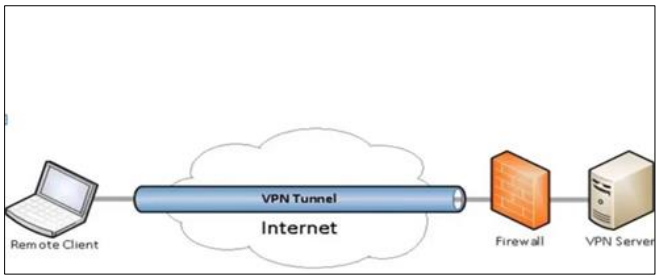


Figure 2.4 : VPN client to site.

Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise. Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

  - La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée ce qui peut poser des problèmes de sécurité.
  - La deuxième méthode, ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Pour pallier à ce genre de problème, certaines entreprises mettent en place des VPN à base du protocole SSL, technologie implémentée dans la majorité des navigateurs Internet du marché [2].

Quelle que soit La méthode de connexion choisie, ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

2.3.5.2 L'intranet VPN ou VPN Site-to-Site

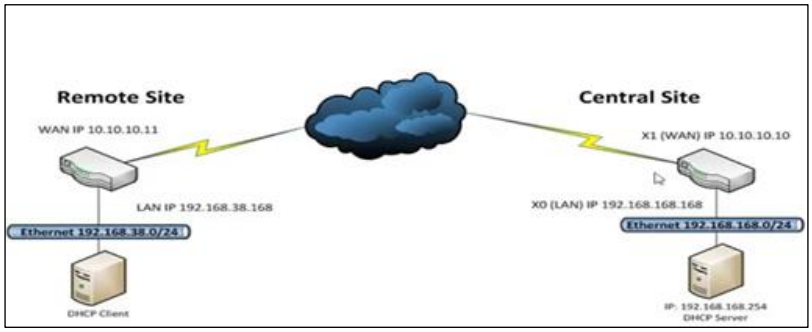


Figure 2.5 : VPN Site-to-Site.

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières, ...).

Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées, on parle d'intégralité. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation.

La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie.

La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Généralement pour la confidentialité, le codage en lui-même pourrait être moyen voir faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable [2].

2.3.6 Protocoles de tunnelisation

Les principaux protocoles de tunneling sont nombreux, il est à noter par ailleurs que dans le VPN les trames ne sont pas envoyées telles quelles, elles sont d'abord encapsulées par le protocole de tunneling, et décapsulé par ce même protocole à l'arrivée.

2.3.6.1 SSL (Secure Socket Layer) / TLS : Le SSL est un protocole de sécurité. Il est aujourd'hui nommé TLS (Transport Layer Security), version du SSL plus sécurisée.

Le SSL / TLS créé un canal sécurisé entre le client et un serveur. Les informations échangées dans ce canal sont chiffrées pour empêcher toute interception de données "en clair" par un pirate informatique. Seul le serveur est en mesure de déchiffrer les informations transmises [w13].

Il existe quatre Protocoles qui utilisent le SSL / TLS :

- **HTTPS (Navigation web sécurisée)** : Cryptage des données transitant entre un navigateur web (Chrome, Firefox, Microsoft Edge, ...) et un serveur web (Apache, Nginx, ...).
- **SMTPS (Envoi d'e-mails sécurisé)** : Cryptage des données transitant entre un outil de messagerie (Outlook, Mail, Thunderbird, ...) et un serveur SMTP (Postfix, Exim ...).
- **POPS / IMAPS (Réception d'e-mails sécurisée)** : Cryptage des données transitant entre un outil de messagerie (Outlook, Mail, Thunderbird, ...) et un serveur mail (Dovecot, ...).
- **FTPS (Echange de fichiers sécurisé)** : Cryptage des données transitant entre un client FTP (Filezilla, WinSCP, ...) et un serveur FTP (proFTPd, vsFTPd, PureFTPd, ...).

L'utilisation de ces protocoles sécurisés permettent de chiffrer les identifiants (login / mot de passe) envoyés au serveur lors des authentifications, mais aussi de crypter les données qui transitent entre l'utilisateur et l'application.

2.3.6.2 IP Sec : est un protocole destiné à fournir différents services de sécurité. Son intérêt principal reste sans contexte, le mode de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (ou VPN en anglais) [11].

Citons quelques propriétés générales des tunnels destinées aux VPN :

- Les données transitant sont chiffrées (confidentialité) et protégées (intégrité).
- Les 2 extrémités sont authentifiées.
- Les adresses sources et destination sont chiffrées Il ne faut pas négliger les aspects pratiques tels que la charge processeur dû au chiffrement, le débit théorique possible, l'overhead induit et donc le débit effectif… De plus IPSec n'est pas le seul protocole permettant d'établir des tunnels, il en existe d'autres comme les « point-à-point » tel que L2TP, L2F ou encore PPTP qui peut induire un overhead non négligeable.

IPSec est un protocole au niveau de la couche réseau qui offre :

- **Intégrité des paquets** : les paquets sont protégés de sorte que tous les changements pendant leur transmission aient pu être détectés.
- **Confidentialité des paquets** : les paquets sont chiffrés avant d'être transmis sur les réseaux [11].

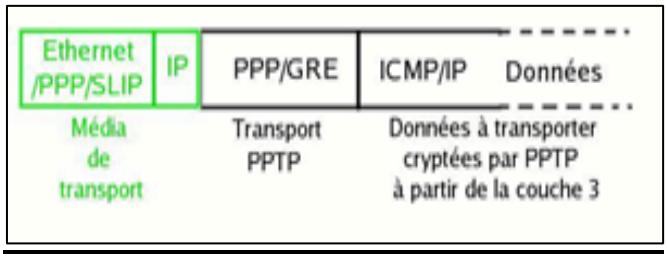


Figure 2.6 : Encapsulation IPSec.

2.3.6.3 GRE (Generic Routing Encapsulation « encapsulation générique de routage ») : est un protocole d'encapsulation de paquets de données qui utilise un protocole de routage à l'intérieur des paquets d'un autre protocole. « Encapsuler » signifie envelopper un paquet de données à l'intérieur d'un autre paquet de données, comme si on mettait une boîte dans une autre boîte. Le GRE est un moyen d'établir une connexion directe point à point dans un réseau, dans le but de simplifier les connexions entre des réseaux séparés. Il fonctionne avec une variété de protocoles de la couche réseau [W14].

Le GRE permet d'utiliser des protocoles qui ne sont normalement pas pris en charge par un réseau, parce que les paquets sont enveloppés dans d'autres paquets qui utilisent des protocoles pris en charge. Pour comprendre comment cela fonctionne, songez à la différence entre une voiture et un ferry. Une voiture circule sur la terre ferme, tandis qu'un ferry circule sur l'eau. Une voiture ne peut pas rouler sur l'eau, mais elle peut être chargée sur un ferry qui en est capable.

Dans cette analogie, le type de milieu (l'eau, la terre) est le réseau qui prend en charge certains protocoles de routage, et les véhicules sont les paquets de données. Le GRE est un moyen de charger un type de paquet dans un autre type de paquet afin que le premier paquet puisse circuler sur un réseau sur lequel il ne pourrait normalement pas circuler, tout comme un type de véhicule (la voiture) est chargé sur un autre type de véhicule (le ferry) pour traverser un milieu qu'il ne pourrait pas traverser autrement.

Par exemple, supposons qu'une entreprise ait besoin d'établir une connexion entre les réseaux locaux (LAN) de ses deux bureaux. Les deux réseaux locaux utilisent la dernière version du protocole Internet, IPv6. Mais pour passer d'un réseau de bureau à un autre, le trafic doit transiter via un réseau géré par un tiers, or, ce réseau est quelque peu dépassé et ne prend en charge que l'ancien protocole IPv4.

Avec le GRE, la société pourrait envoyer du trafic par ce réseau en encapsulant des paquets IPv6 dans des paquets IPv4. Pour revenir à l'analogie, les paquets IPv6 sont la voiture, les paquets IPv4 sont le ferry et le réseau tiers est l'eau.

2.3.7 Le Proxy

Un système mandataire (Proxy) repose sur un accès à l'internet par une machine dédiée, le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières [8]. Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (HTTP, FTP, SMTP, ...) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, ...).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés [12].

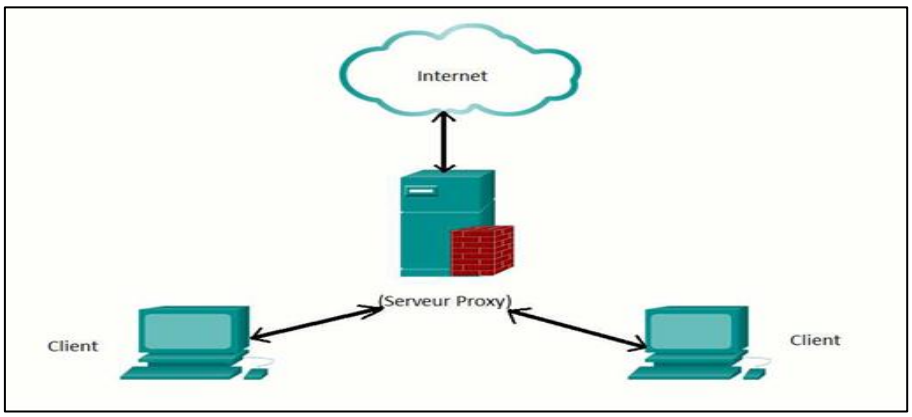


Figure 2.7 : Proxy.

2.3.8 Pare-feu

2.3.8.1 Définition et fonctionnement

Un pare-feu (firewall, en anglais) est une solution de sécurité qui s'occupe des menaces externes, c'est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de

contrôle d'accès. Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système. Il peut être sous forme de programme installé sur les hôtes ou encore tout un dispositif indépendant installé au bord du réseau et lié aux autre périphériques du réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé. C'est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit aussi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes [11] :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

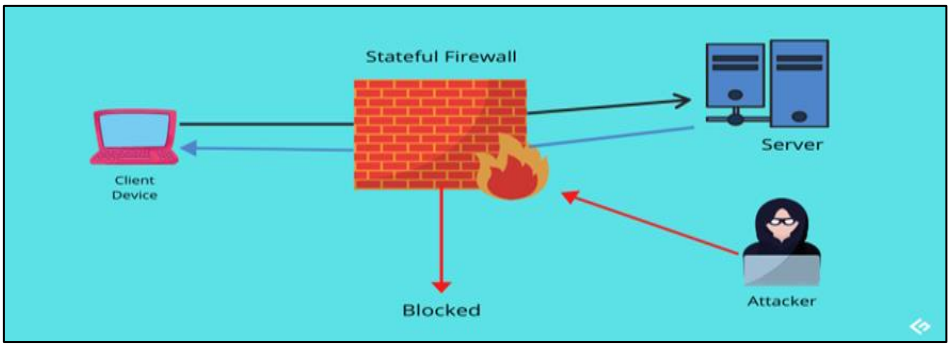


Figure 2.8 : Pare-feu.

Un pare-feu met en vigueur une politique de sécurité qui laisse passer, ou arrête les trames ou les paquets d'information selon cette politique. Il peut donc autoriser ou empêcher des communications selon leur origine, leur destination ou leur contenu. Dans la pratique, un pare-feu lit et analyse chacun des paquets qui arrivent. Après analyse, il décide du passage ou de l'arrêt selon l'adresse IP de l'émetteur, du récepteur, selon le protocole de transport (TCP ou UDP) et le numéro de port, en relation avec le type d'application réseau. Quand la politique de sécurité ne concerne que les couches basses, la seule analyse du paquet permet d'autoriser, de rejeter ou d'ignorer le paquet.

Quand la politique décrit des règles de sécurité qui mettent en jeu le transport fiable, les sessions ou les applications, le pare feu doit connaître l'état momentané de la connexion et doit garder en mémoire de nombreux paquets pendant un certain temps de façon qu'il puisse décider de l'autorisation ou du rejet des paquets.

Les pare-feu ont des limitations, ils doivent être très puissants en termes de ressources pour ne pas ralentir le trafic, dans un sens ou dans un autre, puisqu'ils ont en coupure sur le réseau. Ils ne doivent pas être court-circuités par d'autres passerelles ou des modems connectés directement à l'extérieur. Ils sont des « bastions », c'est-à-dire des cibles pour les attaquants qui peuvent les assaillir pour saturer leur ressource. Un pare-feu doit posséder un système de journalisation (.log) sophistiqué à posteriori tous les faits importants qui jalonnent

la vie de cette passerelle filtrante : tentatives d'intrusion, événements anormaux, attaques par saturation, attaques par balayage.

Un pare feu est en général architecturé de telle manière que l'on puisse distinguer physiquement les communications avec l'extérieur, celles avec le réseau à protéger et enfin celles qui sont déviées vers une zone tampon de parking.

2.3.8.2 Les types de Pare-feu

- **Pare-feu par proxy** :Il sert de passerelle entre les utilisateurs finaux qui demandent les données et la source des données. Tous les périphériques hôtes se connectant au proxy auront une connexion séparée à la source des données. Ce pare-feu peut les filtrer pour appliquer les politiques et masquer l'emplacement de l'appareil du destinataire et également protéger l'appareil et le réseau du destinataire.

- **Pare-feu dynamique** :Ce pare-feu garde la trace d'un ensemble d'informations sur les connexions et rend inutile l'inspection de chaque paquet par le pare-feu. De cette façon, il réduit le délai introduit par le pare-feu. Un pare-feu dynamique examine simplement le trafic réseau afin de déterminer si un paquet est lié à un autre paquet.

- **Pare-feu d'applications Web** :Il protège les serveurs qui prennent en charge les applications Web et Internet contre les attaques HTML spécifiques telles que les scripts intersites, les injections SQL et autres. Ceci détermine si chaque client essayant d'atteindre le serveur doit avoir accès.

- **Pare-feu de nouvelle génération** :Ce type de pare-feu incorpore les règles de ce que les applications individuelles et les utilisateurs ne sont autorisés à faire. Il intègre des données recueillies à partir d'autres technologies afin de prendre des décisions plus éclairées sur le trafic à autoriser et sur le trafic à réduire. Le pare-feu de nouvelle génération fonctionne également en filtrant le trafic réseau et Internet en fonction des applications ou des types de trafic utilisant les ports spécifiques [11].

Les pare-feu emploient différentes manières pour autorisé ou interdire les accès à un réseau. Ces méthodes sont les suivantes :

- **Filtrage des paquets** : interdit ou autorise l'accès pour les trames reçus selon les adresses IP ou MAC.
- **Filtrage des applications** : interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
- **Filtrage d'URL** : interdit ou autorise l'accès à des sites web en fonction d'URL ou de mots clés spécifiques.

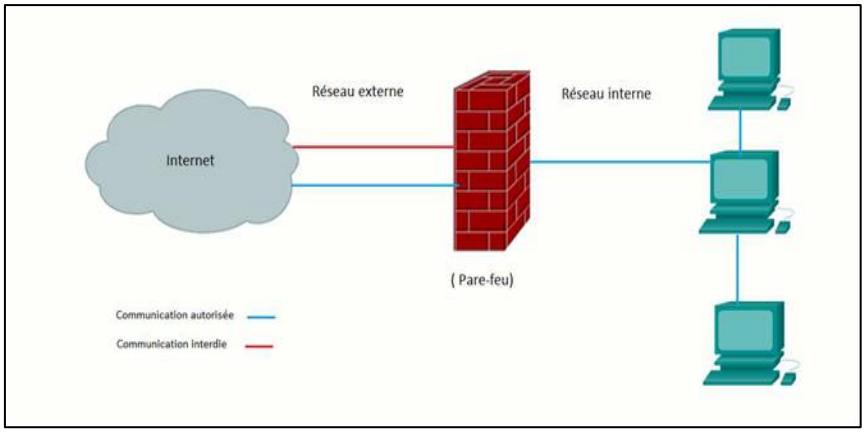


Figure 2.9 : Pare-feu dans un réseau.

2.3.9 Les systèmes de détection et de prévention de l'intrusion (IDS en anglais)

Un système de détection d'intrusion est un dispositif matériel et/ou logiciel de surveillance qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion en temps réel, dans un SI ou dans un ordinateur seul, de présenter des alertes à l'administrateur, voire pour certains IDS plus sophistiqué, de neutraliser ces pénétrations éventuelles et de prendre en compte ces intrusions afin de sécuriser davantage le système agressé. Un IDS réagit en cas d'anomalie, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau [11].

Les techniques sont différentes selon que l'IDS inspecte un réseau ou que l'IDS contrôle l'activité d'une machine (hôte, serveur).

- **Sur un réseau**, il y a en général plusieurs sondes qui analysent de concert, les attaques en amont d'un pare-feu ou d'un serveur.
- **Sur un système hôte**, les IDS sont incarnés par des démons ou des applications standards furtives qui analysent des fichiers de journalisation et examinent certains paquets issus du réseau.

Il existe deux grandes familles distinctes d'IDS :

- **Les N-IDS (Network Based Intrusion Detection system),** ils assurent la sécurité au niveau du réseau.
- **Les H-IDS (Host Based Intrusion Detection system),** ils assurent la sécurité au niveau des hôtes.

2.3.10 Les IPS (Intrusion Prevention Systems)

Agissent dans la même zone du réseau qu'un pare-feu, entre le monde extérieur et le réseau interne. Les IPS rejettent de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue [W15].

2.3.11 La cryptologie

La cryptologie est définie comme l'art et la science de l'écriture secrète. La possibilité d'appliquer la cryptologie pour assurer la sécurité des communications est évidente. La cryptologie regroupe [13] :

- **la cryptographie**: c'est une technique de communication secrète de l'information, et une science relative à la sécurité des messages.
- **La cryptanalyse** : analyse des systèmes cryptographiques afin de trouver des faiblesses. La cryptanalyse essaie de casser les systèmes existants, et recherche constamment sur de nouveaux moyens pour attaquer les systèmes. La cryptanalyse contribue indirectement à la conception de nouveaux systèmes encore plus performants.

2.3.11.1 Fonctions cryptographiques et terminologie : Dans un système de cryptage, nous trouvons souvent les notions suivantes :

- Espace de texte en clair ou message M : est un sous-ensemble de l'ensemble des chaînes binaires {0,1}*. Par exemple chaque lettre de l'alphabet français peut être assignée à un mot de cinq bits (codage binaire).
- Espace de texte chiffré (ou cryptogramme) C : est également un sous-ensemble de {0,1}*.
- Espace des clés de chiffrement K : est aussi un sous-ensemble de {0,1}*.
- Fonction (ou algorithme) de chiffrement E, permet de calculer C avec différentes fonctions E.
- Fonction (ou algorithme) de déchiffrement D, permet de retrouver le message en clair à partir du cryptogramme C.
- Un crypto-système est un procédé pour transformer un texte en clair en un texte chiffré et inversement, il se compose de tous ce qui précède, c.à.d. (M, C, K, E, D).

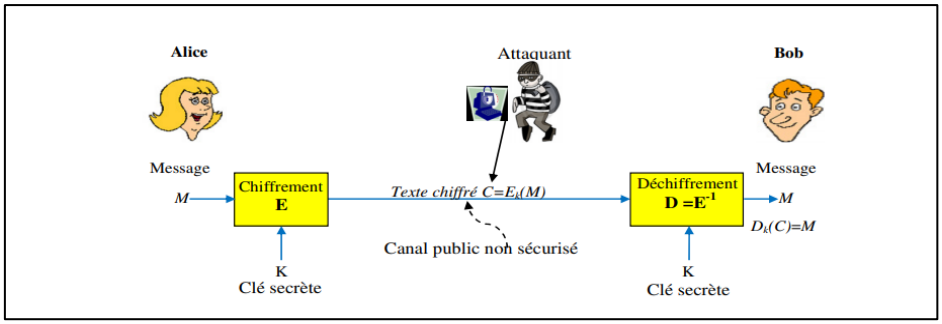


Figure 2.10 : Schéma de principe d'un crypto-système.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui, repose sur un code à deux clés, une privée et l'autre publique.

- **La cryptographie symétrique** [W1] **:** Le cryptage à clé privée ou symétrique est basé sur une clé partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.

  L'avantage de la cryptographie symétrique est sa rapidité d'exécution car elle met en œuvre des opérations simples. Les algorithmes développés pour réaliser les opérations de cryptographie sont : DES, 3DES, AES.

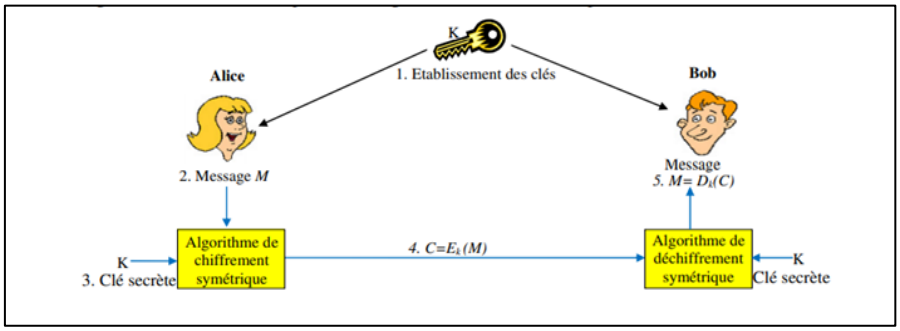


Figure 2.11 : Chiffrement / déchiffrement symétrique avec une clé secrète.

- **La cryptographie asymétrique :** Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par l'utilisateur ; l'autre est publique et donc accessible par tout le monde. Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypte avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Ce cryptage présente l'avantage de permettre la signature numérique des messages et ainsi permettre l'authentification de l'émetteur. Les trois algorithmes à clé publique suivants sont les plus fréquemment employés : RSA, DSA, DH [13].

2.3.11.2 Certificats numériques [W7] : Le certificat est un document signé par une autorité de confiance et contenant des informations d'identification de l'entité (comme son nom, son adresse e-mail, l'employeur, ...) groupées avec la clé publique de cette entité. Ce certificat est délivré et signé numériquement par un tiers de confiance (TTP) indépendant appelé l'autorité de certification (CA). Mais ceci suppose que le CA a déjà vérifié (souvent physiquement) l'identité de l'entité en question. Rappelons que l'entité peut être une personne ou une organisation.

Un certificat est essentiellement un véhicule pour le transport de clés publiques d'une façon vérifiable comme les certificats standard X.509 qui contient aussi le nom de l'émetteur du certificat (comme Verisign ou Thawte), des conditions de validité et d'autres attributs additionnels. Donc les certificats sont utilisés pour éviter les problèmes d'usurpation d'identité. Il y a des certificats personnels, délivrés à des personnes et souvent appelés identifiants numériques et d'autres délivrés à des organisations, implémentés dans le serveur de l'organisation. Le certificat doit être installé dans l'ordinateur ou dans un équipement de communication. Parfois, la clé privée d'un utilisateur est compromise (par exemple volée), dans ce cas, le certificat doit être révoqué. Cela se fait souvent en incluant les certificats révoqués dans une liste des certificats révoqués (CRL, Certificate Revocation List) qui est gérée et signée par le CA, permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité.

Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).

2.3.11.3 Signatures numériques : La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier**.** Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères. Elle ne doit pas être confondue avec la signature électronique manuscrite.

2.3.12 Le NAT (Network Address Translation)

Dans les entreprises de grandes tailles, différent réseaux interconnecté peuvent utiliser les même adresse IP. Pour que la communication soit possible entre nœuds des deux côtés, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable [W16].

Des équipements de translation d'adresse NAT (Network Address Tranlation) sont chargés d'adopter cette fonctionnalité. Ils permettent le changement d'une adresse IP par une autre. Trois types d'adresse sont possibles :

- La translation de port PAT (Port Address Traslation), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- La conversion dynamique d'adresses (NAT dynamique), change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe.
- Simplicité d'installation et d'administration.
- La mise à jour du système sans le réinstaller, package téléchargeable depuis le web.
- Solution riche et performante (basé sur un logiciel libre).

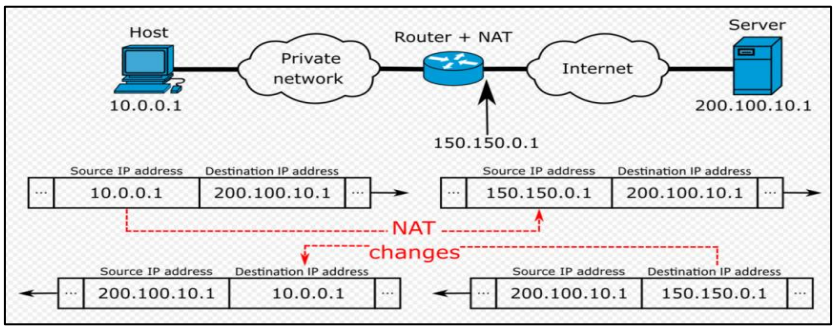


Figure 2.12 : Traduction d'adresses (NAT) réseau entre un réseau privé et Internet.

2.4 Conclusion

L'objet de la sécurité peut se définir comme une contribution à la préservation des forces, des moyens organisationnels, humains, financiers, technologiques et informationnels, dont s'est dotée une organisation pour la réalisation de ses objectifs.

Les attaques contre les réseaux informatiques et leurs ressources sont en augmentation remarquable, elles deviennent de plus en plus sophistiquées. Cette affirmation est confirmée par les rapports annuels du « Computer Emergency Response Team » (CERT), qui mentionnent aussi l'insuffisance des mesures destinées à contrer ces attaques et mettent en évidence la nécessité de toujours améliorer la protection des systèmes d'information.

Au cours de ce chapitre nous avons présenté d'abord les différents types d'attaques qui menacent la sécurité d'un réseau, ensuite nous avons exposé plusieurs solutions de sécurité qu'une entreprise peut exploiter dans sa politique de sécurité pour diminuer les risques des attaques, comme les pare-feu, les VPNS, les VLANS, les systèmes IDS/IPS, les technologies de cryptographie, ….

Dans le chapitre suivant nous allons présenter la topologie du réseau de l'organisme d'accueil ainsi que les solutions proposées pour mieux sécuriser ce réseau.

Chapitre 03

Chapitre03 : Etude de l'architecture existante et proposition de solutions

3.1 Introduction :

Dans ce chapitre, nous allons présenter la topologie globale du réseau Intranet de l'université de Médéa, nous expliquerons l'interconnexion entre les différents sites et à l'intérieur de chaque site, ensuite nous essayerons de détecter les points faibles du réseau et de proposer des suggestions afin d'améliorer sa sécurité et de rendre le trafic plus efficace, enfin nous présenterons l'architecture améliorée du réseau de l'université.

3.2 Présentation globale du réseau :

L'université de Médéa est constituée de cinq sites éloignés : **site Msallah**(faculté Droit), **hall technologie**, **pôle universitaire**, **site d'Ain d'heb**, et un nouveau site à **Ouzera** qui est en cour de réalisation. Sa topologie physique est en étoile étendue.

Chaque site présente une architecture d'arbre composé de plusieurs zones (départements), interconnectés entre eux via un switch couche 3 et (switch multi couche), chaque zone est composé de plusieurs blocs, un bloc est interconnecté par un réseau local dont les utilisateurs peuvent se connecter au réseau Lan filaire via un switch couche 2 (commutateur) ou au réseau **Wlan (sans fil**) via un point d'accès AP Dlink.

Les différents sites sont interconnectés entre eux dans des réseaux étendus (WAN) via des fédérateurs tous les sites sont connectés à un site principal appelé backbonne. Le site backbonne représente la zone d'interconnexion de tous les autres sites vers l'extérieur (internet).

Dans ce site on trouve le routeur de périphérie connecté directement au cloud internet via la fibre optique, on trouve aussi un par feu qui permet de filtrer le trafic entrant vers le réseau intranet de l'université, une interface de par feu est relié directement a un réseau local dans lequel tous les serveurs de l'université (16 serveurs) sont reliées par un switch qui est lui-même connecté au switch du site Pole. Ce site représente donc la DMZ (Démilitalized zone) qui est une interface entre le réseau intranet de l'université et le réseau externe (internet).

3.2.1 Architecture réseau de l'université :

Le réseau de l'université peut être schématisé par la topologie suivante :

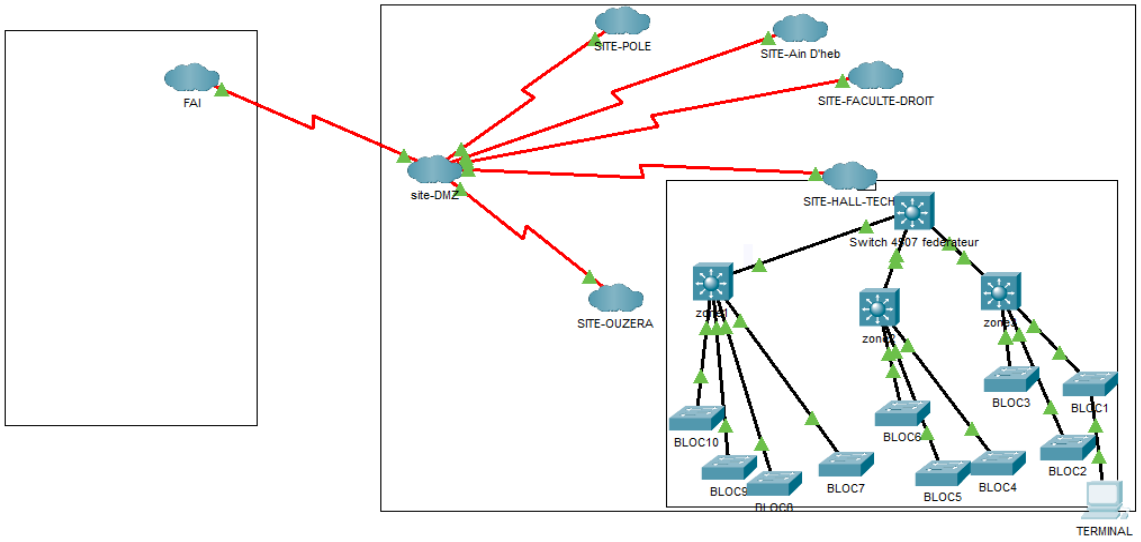


Figure 3.1 : Topologie physique du réseau de l'université.

- Le site DMZ contient serveurs de l'université, le pare feu palo-alto, et le routeur de périphérie.
- Le site pole .
- Le site Ain Dheb .
- Le site Msallah(Faculté_droit) .
- Le site Hall_technologie .
- Le site Ouzera

Comme exemple de zone on a : Rectorat qui se trouve dans le site pole, et contient cinq blocs. Et de bloc : bloc bibliothèque du site Faculté_droit qui contient des PC pour les travailleurs, des PC pour les responsables bibliothèque, des PC pour les étudiants ainsi que des points d'Access wifi pour les utilisateurs sans fil.

3.2.2 **Situation informatique** :

Le réseau informatique de l'université est constitué des équipements suivants :

1) Un(1) routeur Cisco.

2) Deux (2) switches

3) Deux switches(2) .

4) Quaswitches couche 2 (Ethernet switch).

5) switches couche 2 (Ethernet switch) .

6) points d'accès AP Wifi de type Dlink .

7) Un pare feu.

8) Des imprimantes et des PC

9) Un convertisseur TP-LINK fibre.

10) Câbles fibres optiques monomodes et multimodes et des câbles en cuivre UTP.

11) serveurs

3.3 Critiques et suggestions :

L'Union Internationale de Télécommunication (ITU) a défini un ensemble vaste des dimensions de sécurité telle que : le contrôle d'accès, l'authentification, la non répudiation, la confidentialité, la sécurité des communications, l'intégrité des données, la disponibilité et la vie privée, plusieurs autres facteurs influent sur la sécurité des systèmes d'information, comme la responsabilisation, la vérification, la contrôlabilité, l'exactitude, l'identification , la récupération, la robustesse, la supervision, ainsi que la fonctionnalité(ITU-2003) [14].

Après l'analyse de la topologie du réseau informatique de l'université, et après une discussion avec les responsables, nous avons pu faire le point sur quelques failles de sécurité :

3.3.1 Sécurité au niveau des réseaux LAN et WLAN:

3.3.1.1 Les points d'accès :

La multitude des points d'accès Internet représente un passage potentiel que va emprunter un pirate pour accéder au système d'informations du réseau interne. Il convient d'en limiter l'accès en le filtrant selon le type utilisateur, et ceci en utilisant des Listes de Contrôle d'Accès(ACL), ou en exploitant le filtre des pare feu intégrés dans les points d'accès pour refuser l'accès non fiable d'une part et pour bien gérer la consommation de la bande passante d'autre part (éviter la surcharge du réseau par un trafic inutile).

3.3.1.2 Sécurisation des switches :

Les Switches de couche 2 et 3 sont sensibles à de nombreuses attaques identiques à celles de la couche 3. La plupart des techniques de sécurité pour les routeurs s'appliquent également aux Switches. Toutefois, les Switches ont aussi leurs propres types d'attaques, la plupart de ces attaques proviennent des utilisateurs internes au réseau.

3.3.1.2.1 Les attaques:

1) MAC address spoofing(usurpation d'adresse MAC) :

un hôte B peut 'spoofer' (usurper)l'adresse MAC d'un autre hôte avec une fausse réponse ARP ,dans ce cas l'haute B peut recevoir le trafic envoyé vers l'haute A.

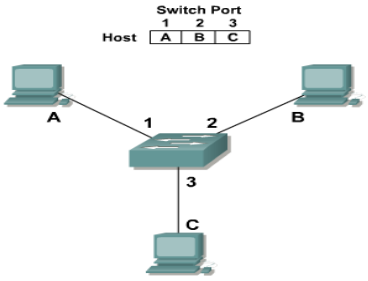


Figure 3.2 : Etat initial avant spoofing.

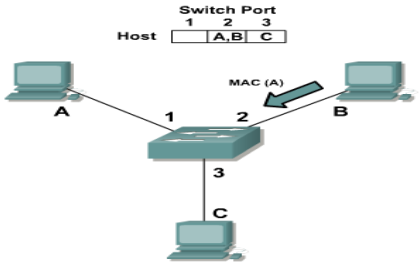


Figure 3.3 : B spoof l'adresse MAC de A.

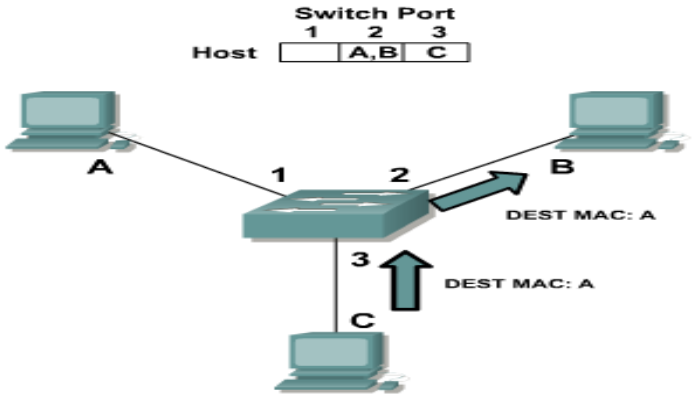


Figure 3.4 : Le switch voit l'haute B dans le port 2.

2) **MAC adress table overflows (surcharge de la table)** : due á la génération des paquets avec MAC sources usurpées (spoof).Sur une courte période de temps la table MAC est remplie et n'accepte plus de nouvelles entrées. Tant que l'attaque se poursuit , la table reste pleine. Le switch rediffuse (inonde) les paquets qu'il reçoit sur chaque port, il se comporte comme un hub. L'attaquant peut maintenant enifler les paques désirés.

3) **STP manipulation** : Une attaque STP implique généralement la création d'un pont racine malveillant .Ceci peut être accompli en utilisant un logiciel comme 'stp-paquet'. Ces programmes peuvent être utilisés pour simuler un Switch qui peut transmettre BPDU STP et devenir Root [W1].

   L'attaquant diffuse des BPDU de configuration STP et de changement de topologie pour forcer des recalcules spanning-tree. En cas de succès, l'hôte attaquant devient le pont racine et voit une variété de Trames qui ne le sont pas autrement.

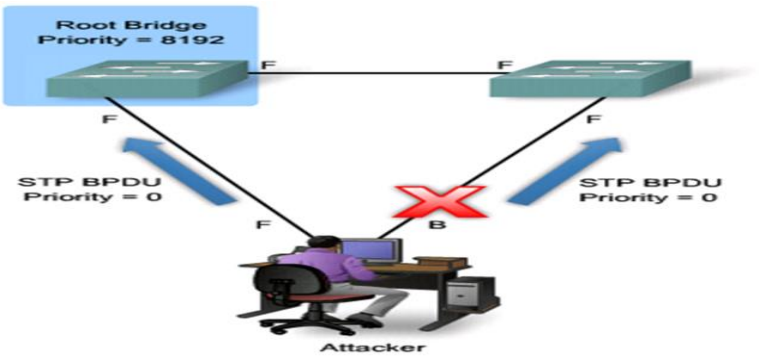


Figure 3.5 : Principe d'attaque BPDU STP.

4) **LAN storms** : Des paquets inondent le réseau, créant un trafic excessif qui dégrade les performances du réseau, il s'agit généralement d'une tempête de paquets de diffusion (broadcast) envoyés par des programmes qui simulent des requêtes de certains protocoles comme le protocole ARP (Adress résolution protocole) et le protocole DHCP (Dynamic host configuration protocole),on parle ici d'une attaque de Dos(Denial of service :déni de service).

5) **VLAN attacks** : Ce type d'attaque peut être lancé de l'une des deux façons suivantes:

- **Attaque Rogue switch (Switch malveillant)** :Il s'agit de transformer une interface « accès »en une interface « trunk » á l'aide de protocole DTP(Dynamic Trunking Protocol),déjà signalé comme « LA » faille. l'attaquant a accès donc á tous les vlan connus du switch attaqué **[w17].** Les ports Trunk propagent le trafic de tous les VLAN en utilisant l'encapsulation 802.1Q.

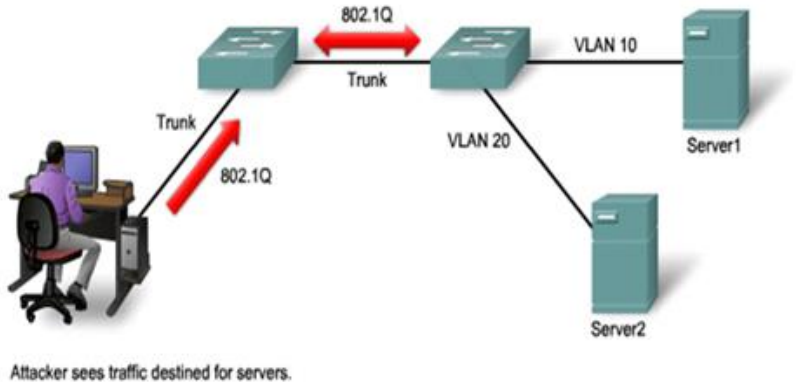


Figure 3.6 : attaque DTP Rogue switch.

- **Attaque double-Tagging (étiquetage doublé)** : Implique la transmission de Trame avec deux en-têtes afin de conduire la trame au mauvais VLAN.

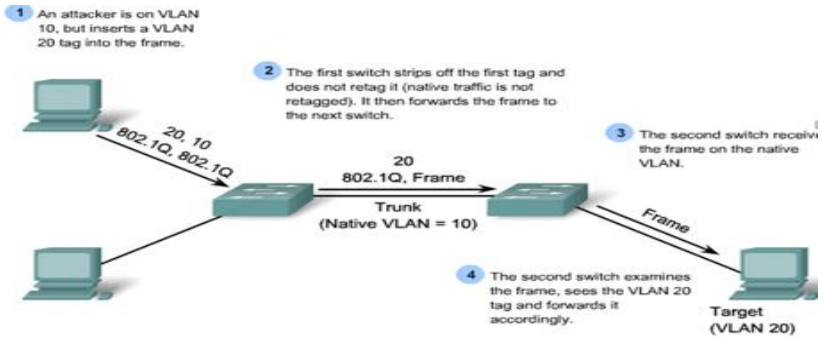


Figure 3.7 : Principe d'attaque double-tagging.

3.3.1.2.2 Les solutions contre ces types d'attaques :

Pour protéger le réseau contre ces différents types d'attaques, une stratégie de sécurité de ports switch doit être implémentée pour tous les commutateurs du réseau, pour cela on propose ce qui suit:

3.3.1.2.2.1 Protection contre l'usurpation d'adresses MAC et surcharge dLa table des adresses MAC :

1) Une méthode simple pour mieux protéger le réseau contre tout accès non autorisé est de désactiver tous les ports qui ne sont pas exploités sur un commutateur en exécutant la commande Cisco IOS shutdown. Si plus tard, un port doit être réactivé, il peut être activé à l'aide de la commande no shutdown. La commande Interface Range peut être utilisée pour appliquer la configuration sur plusieurs ports á la fois.

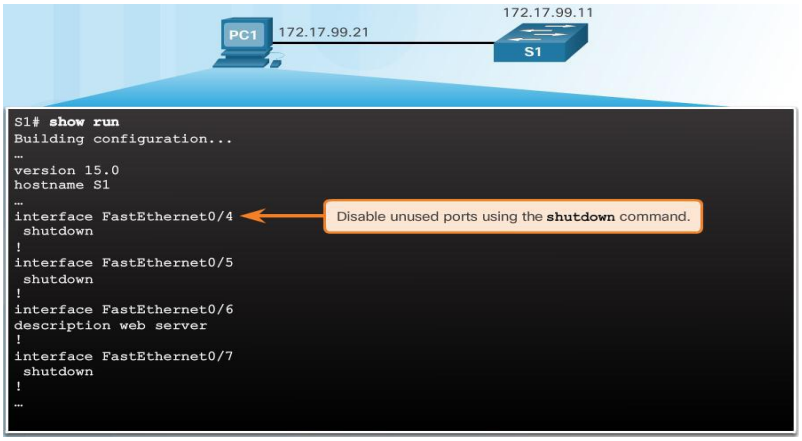


Figure 3.8 : Désactivation des ports inutiles.

2) On doit restreindre le nombre d'adresses MAC autorisées sur un port. Les adresses MAC des périphériques légitimes sont ainsi autorisées. Toutes les autres sont refusées. Une interface d'un switch peut être configurée pour autoriser une ou plusieurs adresses MAC, si le nombre d'adresses MAC autorisées sur un port est limité à 1, un seul périphérique peut se connecter au port. Si un port est sécurisé et si le nombre maximum d'adresses MAC est atteint pour ce port, toute tentative de connexion supplémentaire réalisée depuis une adresse MAC inconnue générera une violation de sécurité.

La fonction de sécurité des ports ne fonctionnera pas si la sécurité des ports n'est pas activée sur l'interface avec la commande switchport port-Security, le nombre par défaut des adresses MAC sécurisées autorisées est 1.

```
S1# show port-security interface fastethernet 0/18
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0025.83e6.4b01:1
Security Violation Count     : 0
```

Figure3.9 : exemple de port-Security une interface d'un switch.

3) Pour certains ports (le cas des périphériques inchangeables, toujours utilisés), et comme mesure de sécurité des adresses contre la violation, il faut fixer les adresses MAC fiables qui peuvent être configurées de différentes manières :

a. Adresses MAC sécurisées statiques : Configurées manuellement à l'aide de la commande switchport port-Security mac-address mac address en mode de configuration d'interface, ces adresses MAC sont stockées dans la table d'adresses et sont ajoutées à la configuration en cours **[w1].**

b. Adresses MAC sécurisées dynamiques : Apprises de manière dynamique et stockées uniquement dans la table d'adresses, ces adresses MAC configurées ainsi sont supprimées au redémarrage du commutateur **[w1].**

c. Adresses MAC sécurisées rémanentes : Apprises dynamiquement, stockées dans la table d'adresses et ajoutées à la configuration en cours, elles peuvent être enregistrées dans la configuration de démarrage pour les conserver définitivement. La commande switchport port-security mac-address sticky est utilisée dans ce cas.

Si l'apprentissage rémanent est désactivé à l'aide de la commande de configuration d'interface no switchport port-security mac-address sticky, les adresses MAC sécurisées rémanentes restent intégrées à la table d'adresses mais sont supprimées de la configuration en cours **[w1]**.

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan   Mac Address       Type            Ports   Remaining Age
                                                    (mins)
----   -----------       ----            -----   -------------
1      0025.83e6.4b01    SecureDynamic   Fa0/18      -
1      0025.83e6.4b02    SecureSticky    Fa0/19      -
-----------------------------------------------------------
```

Figure 3.10 : Adresses MAC dynamiques et rémanentes.

Des modes de violation peuvent être aussi configurés sur les interfaces á sécurisé :

- **Protect :** les données provenant des adresses MAC de source Inconnue sont supprimées; une notification de sécurité n'est pas signalé par le commutateur.
- **Restrict :** les données provenant des adresses MAC source inconnues sont supprimées; une notification de sécurité est signalé par le commutateur et le compteur de violation s'incrémente.
- **Shutdown :**(mode par défaut), l'interface est désactivée error-disabled et le voyant du port s'éteint. Le compteur de violation s'incrémente, lancez la commande shutdown puis no shutdown sur l'interface pour la sortir de l'état d'erreur.

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Figure 3.11 : Comparaison entre les modes de violation.

Pour modifier le mode de violation d'un port de commutateur, on utilise la commande de mode de configuration d'interface switchport port- Security violation **{protect | restrict | shutdown}.**

3.3.1.2.2.2 Protection contre STP manipulation :

La commande **spanning-tree portfast** permet à une interface de couche de passer immédiatement de l'état de blocage à transmission, sans passer par les états d'écoute et d'apprentissage. Elle doit être utilisé sur les ports accès qui se connectent à une Workstation ou serveur. Si PortFast est activé sur un port connecté à un autre Switch, il existe un risque de créer une boucle Spanning Tree.

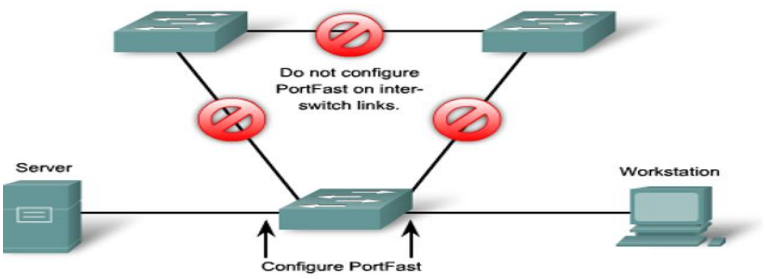


Figure 3.12 :PortFast sur les ports d'accès et entre des switches.

La commande **spanning-tree portfast bpduguard** default peut etre aussi utilisée pour protèger un réseau commuté d'une réception de BPDUs sur les ports qui ne devraient pas les recevoir.

La réception de BPDUs peut être accidentelle ou faire partie d'une attaque.Si un port configuré avec PortFast et BPDU Guard reçoit un BPDU, le Switch placera le port en état désactivé **[15]**.

BPDU Guard est meilleur déployé sur les ports utilisateur, empêchant l'extension du réseau avec des Switches malveillants via un hôte attaquant.

3.3.1.2.2.3 Protection contre les tempêtes :

Utiliser **storm-control** pour activer le contrôle et définir la valeur de seuil pour chaque type de trafic. Les Attaques de tempête (Broadcast, Multicast, Unicast) LAN peuvent être atténuées avec Storm Control en surveillant des seuils de déclanchement prédéfinis. Seuil de hausse et seuil de baisse peuvent être réglés.

Si,trap est configuré, le Switch envoie des messages de log SNMP quand une tempête survient.

shutdown est configuré, le port est désactivé lors d'une tempête. No shutdown doit être utilisé pour réactiver l'interface.

```
SW1(config-if)# storm-control broadcast level 75.5
SW1(config-if)# storm-control multicast level pps 2k 1k
SW1(config-if)# storm-control action shutdown
```

Figure 3.13 : Exemple d'activation de contrôle.

3.3.1.2.2.4 Protection contre les attaques Vlans :

Pour atténuer les attaques Vlans, il faut s'assurer que le trunking est activé uniquement sur les ports nécessaires. L'administrateur peut aussi désactiver DTP (trunking automatique) et activer manuellement les agrégations (trunks).

```
config-if)# switchport nonegotiate
```

Figure 3.14 : exemple de désactivation de DTP.

Il est conseillé de désactiver également tous les ports inutilisés et les placer dans un VLAN inutilisé, et d'utiliser un Vlan natif dédié pour tous les ports Trunk (exp: vlan99).

```
config-if)# switchport trunk native vlan vlan_number
```

Figure 3. 15: configuration d'un Vlan natif.

3.3.1.3 La redondance :

L'absence des chemins redondants dans le réseau peut causer l'indisponibilité des services en cas de panne d'un périphérique intermédiaire, exemple en cas de panne d'un switch multicouche tout un département sera isolé du réseau. Pour remédier á ce problème, nous proposons la création des chemins redondants dans chaque site au niveau des switches couche 3, la redondance est considéré comme l'un des critères d'un réseau fiable, car il devient un réseau tolérant aux pannes c'est á dire il permet une récupération rapide en cas de panne.

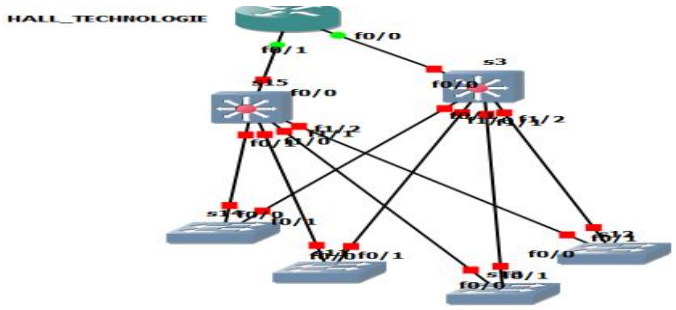


Figure 3.16 : chemins redondants.

3.3.1.4 Les VLAN de données :

Pour mieux gérer les services, il faut penser á repartir les utilisateurs du réseau selon leur fonction dans des réseaux LAN virtuels (VLAN) quel que soit l'emplacement physique de l'utilisateur ou du périphérique, et assurer le routage inter-vlans, Ce mode de segmentation des réseaux locaux modifie entièrement la manière dont les réseaux sont conçus, administrés et maintenus.

La technologie de VLAN comporte ainsi de nombreux avantages. Parmi les avantages liés à la mise en œuvre d'un VLAN, on notamment **[w18]**:

1) **Augmentation des performances**: La segmentation créée par les VLAN réduit la taille des domaines de diffusion (broadcast), les VLANS améliorent les performances réseau en divisant de vastes domaines de diffusion en

domaines plus petits. Chaque VLAN est un domaine de diffusion logique distinct avec son propre réseau IP.

2) **Réduction des coûts**: L'utilisation de VLAN permet de simplifier l'administration du réseau. A chaque fois qu'un utilisateur change de LAN, il faut modifier l'adresse du poste et certains paramètres des routeurs. Tandis que si un utilisateur change de lieu physique mais pas de VLAN, il peut ne pas y avoir de modifications à faire (sous réserve de disposer de bons outils de gestion des VLAN).De plus, l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches.

3) **Formation de groupes virtuels**: Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements. Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe.

4) **Gain de sécurité**: Périodiquement, des données sensibles sont envoyées en broadcast sur le réseau par les machines (et plus particulièrement les serveurs). Les VLAN permettent d'isoler les serveurs dans un même domaine de broadcast et de les isoler par service. Les VLAN apportent donc une grande flexibilité dans la gestion des réseaux ; les utilisateurs pourront être regroupés selon leur centre d'intérêt. Ils permettent ainsi une simplification de la gestion des projets et des applications, et la sécurité sera donc optimisée.



Figure 3. 17 : exemple de Vlans.

3.3.2 Sécurité de l'accès pour la gestion :

3.3.2.1 Les mots de passe et les messages de jour :

L'accès pour gestion aux périphériques intermédiaires (switches, routeurs, par feu) (pour la configuration) doit être aussi sécurisé : L'accès peut être direct via le port console ou indirect via le protocole Telnet ou SSH, ou via le port auxiliaire AUX en utilisant une ligne téléphonique. La configuration initiale (première configuration) doit être via la console pour configurer les paramètres de l'accès á distance.

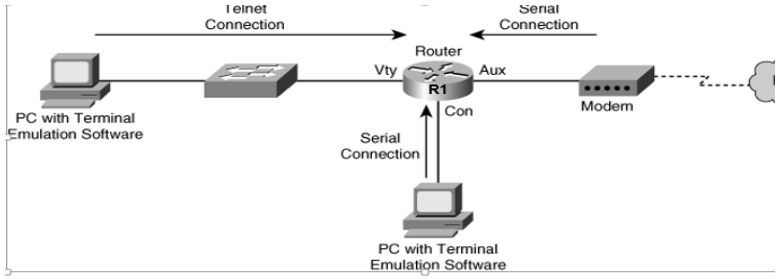


Figure 3.18 : Méthodes d'accès au routeur pour la configuration.

Dans les deux cas il s'agit de la sécurité de l'accès au mode d'exécution utilisateur (exp : Router>):

1) Sécuriser l'accès par la ligne console 0(le zéro sert á représenter la première et le plus souvent, la seule interface de console) avec un mot de passe á l'aide de la commande de configuration globale line console 0, et la commande login pour activer l'accès au mode d'exécution utilisateur.

2) Sécuriser les lignes VTY qui correspondent à toutes les connexions distantes qui ont ouvert un port virtuel de vty 0 à vty 4(un routeur cisco peut prendre jusqu'á 5 lignes vty numérotées de 0 á 4) pour un routeur ou de vty 0 á vty 15(un commutateur cisco peut prendre en charge jusqu'á 16 lignes vty numérotées de 0 á 15) pour un switch pour la configuration via Telnet ou SSH, par un mot de passe, et ceci á l'aide de la commande de configuration globale line vty 0 4 ou line vty 0 15, password password , et la commande login pour activer l'accès vty.

3) Sécuriser l'accès au mode d'exécution privilégié (exp :Router #) par un mot de passe , ce mot de passe peut être considéré comme étant le plus important parce qu'il permet d'accéder au mode qui ouvre la porte pour les commandes show (comme show Run)pour l'affichage, et la configuration . Pour cela, on peut configurer un mot de passe en clair á l'aide de la commande enable password [password]ou un mot de passe chiffré á l'aide de la commande enable secret [password].

4) Les fichiers startup-config et running-config affichent les mots de passes en clair, c'est une menace á la sécurité dans la mesure où n'importe quel utilisateur peut les afficher s'il a accès pour remédier á ce problème on doit chiffrer tous les mots de passe configurés par la commande service password-encryption. Cette commande permet d'appliquer un chiffrement simple á tous les mots de passe du fichier de configuration. En plus les mots de passe utilisés doivent être forts et non pas facile á deviner, il est conseillé aussi de ne pas utiliser le même mot de passe pour plusieurs niveaux de sécurité.

5) Les mots de passe doit être longs, pour IOS 12.3 et ultérieur les mots de passe peuvent être de 0 à 16 caractères. La commande security passwords min-length length permet

d'imposer une longueur minimale pour les mots de passe á configurer. La meilleure pratique est d'avoir un minimum de 10 caractères.

6) Bien que les mots de passe soient un moyen pour empêcher l'Accès non autorisé, il est vital de mettre en place une méthode pour déclarer que l'accès á un périphérique est réservé aux seule personnes autorisées. Á cet effet, une bannière (message du jour) doit être ajoutée aux informations affichées par le périphérique á l'aide de la commande banner motd # (Message of the day). Les bannières peuvent constituer une pièce importante dans un procès intenté á une personne qui aurait accédé illégalement á un périphérique. En effet, dans certains systèmes juridiques, il est impossible de poursuivre des utilisateurs s'ils n'ont pas reçu de notification appropriée au préalable [**w1].**

7) Il faut mettre fin à une connexion console ou Telnet non utilisée après un certain délai, le délai par défaut est de 10 minutes. Ceci consiste á terminer une connexion sans surveillance (console ou vty) pour fournir un niveau supplémentaire de sécurité si un administrateur s'éloigne d'une session de la console active en exploitant la commande Exit timeout minutes secondes. Exec-timeout 0 0 signifie qu'il n'y aura pas de délai d'attente et la session restera active pendant une durée illimitée.

8) Les accès console, auxiliaire, et vty / ports doivent être protégés. Par défaut, les ports consoles permettent un signal « BREAK » dans les premières 60 secondes du boot. Ce qui permet d'obtenir le mode « Rom Monitor ». Cependant, si un malveillant a un accès physique au routeur il peut utiliser la procédure "recovery password" pour obtenir la configuration. Ce type d'attaque laisse le routeur dans un état intact et est difficile à détecter.

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)
```

Figure 3.19 : Désactivation du procédure de récupération d'un mot de passe.

9) Un administrateur peut atténuer cette faille de sécurité potentielle en utilisant la commande de configuration globale no service password-recovery qui peut être utilisée pour désactiver la procédure de récupération de mot de passe.

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username        SourceIPAddr    lPort Count TimeStamp
admin           1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2011
Admin           10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2011
admin           10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2011
cisco           10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2011

R1#
```

Figure 3.20 : exemple de tentatives échouées.

10) Les routeurs et les switches doivent être configuré pour un nombre limité de tentatives d'accès par un mot de passe, toutes les connections doivent être bloquées après un nombre donné des échecs. Cette solution contribue également à fournir une détection et une prévention DoS. Ainsi un administrateur peut identifier le nombre de défaillances, les noms d'utilisateurs essayés, et les adresses IP, ainsi qu'un horodatage ajouté pour chaque tentative, en utilisant la commande show login failures.

11) L'accès administratif pour la gestion á distance des périphériques (switch, routeur) est assuré via une interface virtuelle SVI (switch virtuel interface) qui est appelée aussi vlan de gestion (management). Par défaut, le commutateur est configuré de telle sorte que sa gestion est régie par le Vlan1, mais pour des raisons de sécurité, il est recommandé d'utiliser un Vlan autre que le Vlan1 (exp : Vlan 99). Cette interface doit être configurée avec une adresse IP pour permettre la gestion du périphérique distance via le protocole Telnet ou SSH.

3.3.2.2 Transmission par protocole Telnet :

Le protocole **Telnet** , attribué au port TCP 23,utilise un mode de transmission en texte clair non sécurisé des informations ce qui engendre une menace pour les informations d'identifications comme les mots de passe et le nom d'utilisateur qui peuvent être intercepté via un logiciel analyseur (exp :wireshark)par un pirate. Pour ces raisons le protocole SSH doit remplacer Telnet.

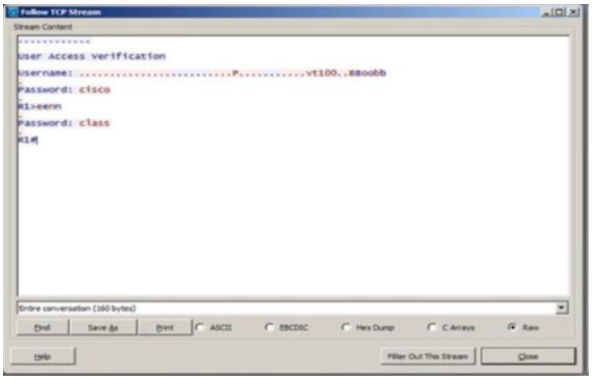


Figure 3.21 : Capture Wireshark pour Telnet.

SSH permet de sécuriser les connexions distantes grâce à une méthode de chiffrement fort pour l'authentification des périphériques (nom d'utilisateur et mot

de passe), mais également pour la transmission des données entre les périphériques de communication

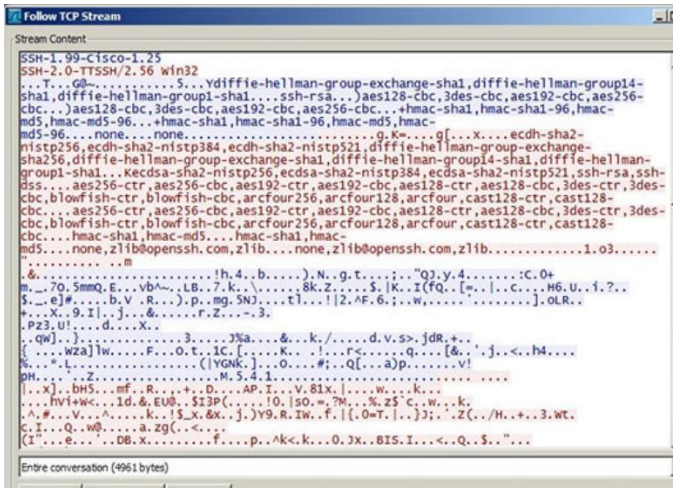


Figure 3.22 : Capture wireshark pour SSH.

Pour activer SSH sur un commutateur ou un routeur, il doit utiliser une version du logiciel IOS qui prend en charge les fonctionnalités de cryptographie (chiffrement).La commande show version permet d'afficher la version de l'IOS exécutée ainsi que le nom du fichier IOS dans lequel figure la combinaison « K9 », indiquant la prise en charge des fonctionnalités et des capacités de chiffrement.



Figure 3.23 : Exécution de la commande show version.



Figure 3.24 : Accès par le protocole SSH

3.3.3 Sécurité au niveau des réseaux WAN (trafic des réseaux distants) :

3.3.3.1 Les switches fédérateurs :

Le réseau actuel de l'université utilise deux switches fédérateurs dans la couche de distribution pour relier les différents sites, l'un pour le site Ain Dheb et l'autre pour les autres sites ce qui rend la gestion du deuxième switch difficile et lourde .En plus un IOS switch ne peut pas assurer toutes les options de sécurité comme un IOS Routeur.

Nous proposons un routeur comme périphérique de périphérie pour relier chaque site avec l'extérieur ,dont L|IOS permet de faire une mise á jour périodique avec les nouvelles options de sécurité ainsi que les nouvelles technologies comme la VoIP(trafic vocal) .

Dans la nouvelle topologie réseau chaque site respecte une architecture de trois couches (distribution, cœur et accès), pour cela cinq routeurs sont nécessaires plus le routeur existant.

3.3.3.2 Interconnexion des sites (VPNs) :

La topologie du réseau est de type Hub and Spoke, les différents sites ne sont pas interconnectés entre eux directement, chaque site doit passer par le site backbone pour communiquer avec un autre site .

Un VPN site á site peut être une solution sécurisé qui permet de relier les sites deux á deux en mettant en place une liaison permanente distante et sécurisée entre les sites. Avant l'arrivée des VPN, les entreprises devaient utiliser des liaisons appelées TRANSPAC, ou bien des lignes louées avec un coût très élevé. Les VPN ont alors permis de démocratiser ce type de liaison. Le terme VPN sera notamment utilisé pour l'accès à des structures de type cloud computing.

On propose une architecture d'un tunnel entre le site Pole et celui d'Ouzera pour une communication sécurisée qui garantit la confidentialité, la sécurité et l'intégrité des données sur des canaux privés á moindre cout en comparant avec une ligne didiée.(Cette solution peut être etablit entre tous les autres sites deux á deus).

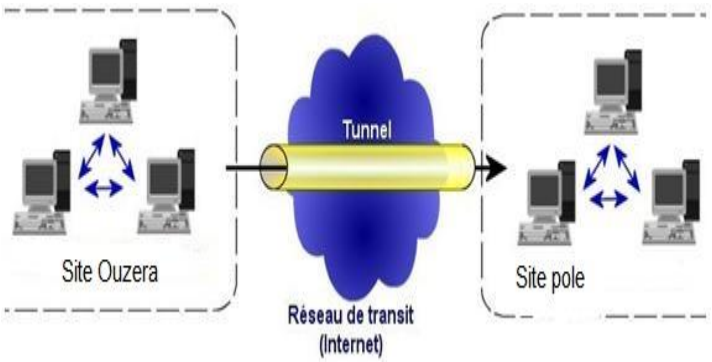


Figure 3.25 : Solution VPN proposée.

Parmi les avantages procurés par cette configuration nous pouvons citer:

- Le cryptage est souvent pris en charge par des processeurs spécialisés,
- ce qui améliore notablement les performances.
- Une grande facilité pour le contrôle de trafic autorisé.
- Aucun impact sur les performances des postes puisque ceux-ci ne font pas de cryptage.
- La possibilité d'initier le VPN d'un côté ou de l'autre.

Mais cette solution présente aussi quelques inconvénients:

- Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux sites. (une autre stratégie de sécurité complémentaire doit être implémentée dans les sites).
- L'établissement des VPN nécessite que les deux extrémités soient bien Identifiées soit par une adresse IP publique fixe, soit par un nom Référencé dans des DNS officiels

Deux protocoles major sont le plus souvent utilisés pour les tunnels VPN site á site :

- **GRE** : Défini dans le RFC (Request For Comment) 1702 et RFC 2784, il peut encapsuler n'importe quel type de paquets, il utilise IP pour créer une liaison virtuelle point-to-point entre les routeurs Cisco. Il supporte multi protocoles autre qu'IP, donc il peut transporter en tunnel un trafic non-IP via un réseau IP, en monodiffusion (unicast), multidiffusion (Multicast) et donc les paquets des protocoles de routage ou en diffusion (broadcast).

  Le GRE ne fait pas le chiffrement, le trafic est transporté en claire. Ce qui implique qu'il a besoin d' IPsec pour le chiffrement.



R1 configuration:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Figure 3.26 : Exemple de configuration d'un tunnel GRE.

- **IPsec** : L'IPSec a été défini par le groupe de travail d'IETF (Internet Engineering Task Force) depuis 1992. En 1995, une première version basique a été développée sous forme de RFC sans la partie de la gestion des clés. Plusieurs défauts ont été déclarés dans cette version; afin de les corriger, une première amélioration de ce protocole a été faite en 1998, où ils ont proposé le protocole IKEv1, qui permet d'ajouter un système dynamique pour la gestion des paramètres confidentiels de l'IPSec **[14].**

  On peut résumer le fonctionnement de IPsec dans la pile de cinq blocs (niveaux) comme suite :

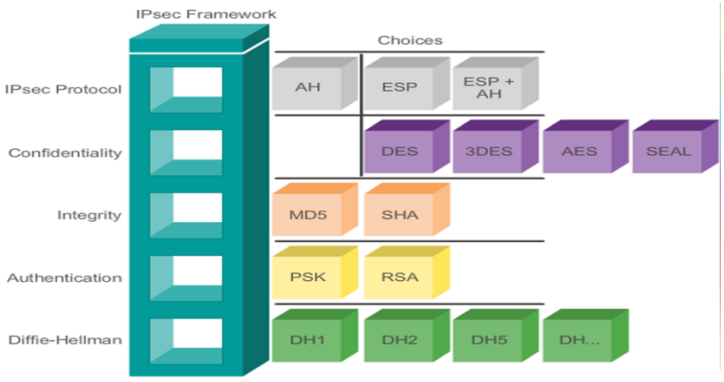


Figure 3.27 : Implémentation d'IPsec.

✓ **IP sec** assure la confidentialité du trafic transporté, en utilisant les algorithmes suivants pour l'encryption dans : DES, 3 DES, AES, Software Optimized Encryption Algorithme(SEAL) .

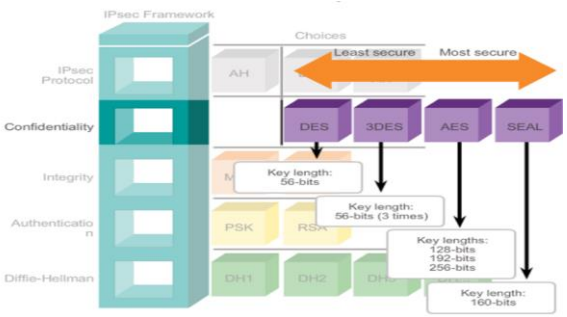


Figure 3.28 : Algorithmes d'encryption.

✓ **IPsec** assure l'intégrité des données (le contenu du paquet ne sera pas modifié) en utilisant des algorithmes de hachage HMAC (Hached Message Authentication Code). Deux algorithmes sont souvent utilisés :**MD5(Message**

Digest 5) avec une clé longueur 128 bits, et **SHA-1(SecureHach Algorithme)** avec une clé de 160 bits(plus sécurisé).

Pour l'authentification, IPsec utilise l'une des deux méthodes:

PSK (Pre-shard Keys), ou RSA signatures.

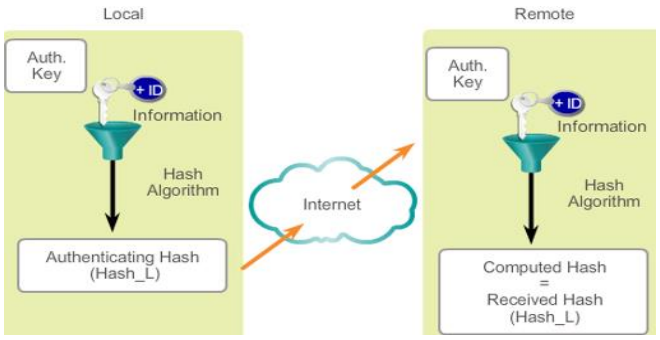


Figure 3.29 : Méthode PSK.

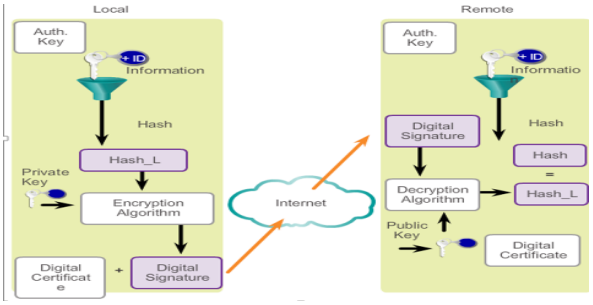


Figure3.30 : Méthode RSA.

Les deux extrémités d'un VPN doivent partager une clé pour le cryptage et le décryptage, pour se faire, IPsec utilise la méthode Diffie-Hellman (DH) clé, qui est une méthode d'exchange de clés secrets partagés entre deux extrémités. IPsec utilise aussi l'un des deux protocoles suivants pour créer un cadre sécurisé (Security Framework) :

1) **AH (Authentication Header)** :Avec un numéro de port 51,il assure l'authentification et l'intégrité mais pas l'encryption, il ne supporte pas le NAT.

2) **ESP (Encapsulating Security Payload)** : Avec un numéro de port 50, il assure les mêmes services que AH mais avec encryption.

3.3.3.3 L'authentification (AAA) :

Gérer l'accès administratif au réseau est cruciale, pour sécuriser l'accès plusieurs méthodes sont disponibles :

- **Mot de passe seulement** : Les mode d'accès utilisateur ou privilégié avec mot de passe est limité et n'est pas évolutif.

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

Figure 3.31 : Mot de passe pour lignes vty.

- **Base de données locale :** Offre une plus grande sécurité qu'un simple mot de passe. C'est une solution de sécurité rentable et facilement mise en œuvre. Le problème est que cette base de données locale doit être répliquée sur plusieurs appareils.

```
R1(config)# username Admin secret Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# login local
```

Figure 3. 32: Méthode base de données locale.

- **Authentification locale AAA (autonome AAA)** : Dans ce mode, Le client établit une connexion avec le routeur. le routeur AAA invite l'utilisateur à entrer un login et un mot de passe.le routeur authentifie le nom d'utilisateur et le mot de passe en utilisant la base de données locale et l'utilisateur est autorisé à accéder sur la base des informations contenues dans la base de données locale **[w1].**

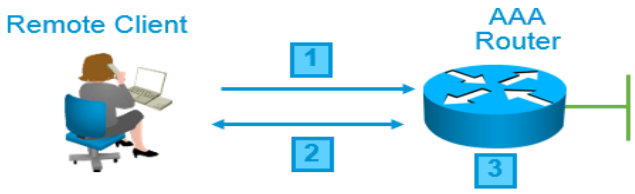


Figure 3. 33: Authentification locale.

- **AAA basée sur serveur :** Le client établit une connexion avec le routeur, le routeur AAA demande à l'utilisateur un identifiant et un mot de passe, il authentifie le nom d'utilisateur et le mot de passe sur un serveur AAA distant appelé Cisco Access Control Server (ACS).L'utilisateur est autorisé à accéder en fonction des informations sur le serveur distant.

  Cette méthode est la plus évolutive car tous les périphériques de l'infrastructure accèdent à un serveur central. De nombreux serveurs d'authentification au niveau des entreprises sont disponibles sur le marché aujourd'hui, Les plus populaires parmi ceux-ci sont :

  1) Cisco Secure Access Control Server/System (ACS).

2) Juniper Steel-Belted radius server.

3) Microsoft Network Policy Server – NPS.

4) Internet Authentication Service (IAS) sur Windows Server 2003.



Figure 3. 34 : AAA basé sur un serveur.

AAA supporte les protocoles de sécurité standardisés :

1) **Terminal Access Controller Access Control System Plus (TACACSP)**: est considéré comme le protocole le plus sécurisé car tous les échanges sont cryptés. il remplace TACACS et XTACACS [**16].**

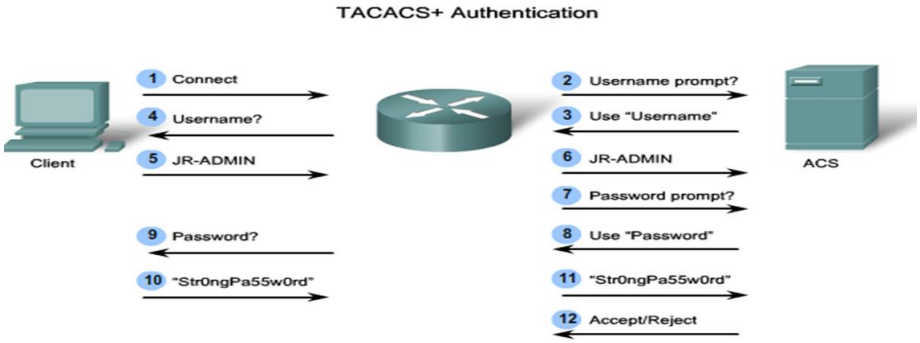


Figure3.35 : Authentification Tacacs+.

2) **Remote Authentication Dial-In User Service (RADIUS):**développé par Livingston Enterprise, est un protocole ouvert de l'IETF, aux standards AAA, pour des applications telles que l'accès au réseau ou à la mobilité IP. RADIUS est actuellement défini par les RFCs 2865, 2866, 2867 et 2868. Radius crypte seulement le mot de passe de l'utilisateur. Il ne chiffre pas les noms d'utilisateur, les informations de compte, ou toute autre information dans le message de Radius **[w1].**

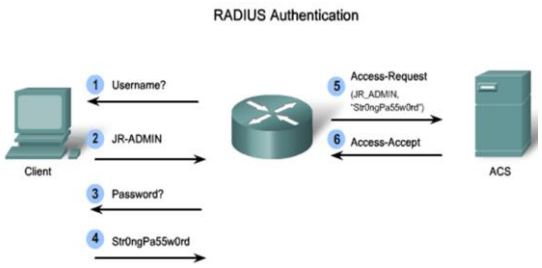


Figure 3.36 : Authentification Radius.

Dans notre cas, nous avons opté pour la configuration de la méthode d'authentification AAA (locale et basé sur un serveur).

3.3.3.4 Le filtre du trafic (ACL) :

Le trafic circulant sur le réseau (interne ou externe) doit être filtré au niveau des routeurs selon les décisions d'administrateur. Pour cette raison des listes de contrôle d'accès ACLs doivent être configurées sur certains routeurs.

Une ACL est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet, elles ne sont pas configurées par défaut sur un routeur. Une fois configurées, les ACLs assurent les tâches suivantes :

1) Elles limitent le trafic réseau pour accroître les performances réseau. Si la stratégie de l'entreprise interdit, par exemple, le trafic vidéo, vous pouvez configurer et appliquer des ACL pour bloquer ce trafic. Ainsi, la charge réseau est nettement réduite.

2) Elles contrôlent le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage, si aucune mise à jour n'est requise vu les conditions du réseau, la bande passante est préservée.

3) Elles fournissent un niveau de sécurité de base pour l'accès réseau. Les ACLs permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'y avoir accès.

4) Elles filtrent le trafic en fonction de son type. Une ACL peut autoriser le trafic des e-mails, mais bloquer tout le trafic Telnet.

5) Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau. Les ACL peuvent autoriser ou refuser à un utilisateur l'accès à certains types de fichier, tels que FTP ou HTTP.

Une ACL est configurée sous forme d'une séquence d'instructions de refus (Deny), ou d'autorisation (Permit).Sur la base de ces instructions appelées aussi entrées de contrôle d'accès (ACE), le routeur filtre les paquets. La dernière instruction d'une ACL est toujours implicite deny. Cette instruction est automatiquement ajoutée à la

fin de chaque ACL, même si elle n'est pas physiquement présente, elle bloque l'ensemble du trafic restant.

La position de l'ACL et le type de l'ACL utilisé peuvent également dépendre des caractéristiques suivantes:

a) Le contrôle de l'administrateur réseau: la position de l'ACL peut être différente si l'administrateur réseau contrôle à la fois les réseaux source et de destination.

b) Bande passante des réseaux concernés: le filtrage du trafic indésirable à la source empêche la transmission du trafic avant qu'il consomme de la bande passante sur le chemin vers une destination. Cela est particulièrement important sur les réseaux à faible bande passante.

c) Facilité de configuration: si un administrateur réseau souhaite refuser le trafic provenant de plusieurs réseaux, il est possible d'utiliser une seule ACL standard sur le routeur le plus proche de la destination. L'inconvénient est que le trafic de ces réseaux «gaspille» de la bande passante. Une ACL étendue peut être utilisée sur chaque routeur d'où provient le trafic. Cela permet d'économiser de la bande passante en filtrant le trafic à la source, mais nécessite la création des ACLs étendues sur plusieurs routeurs.

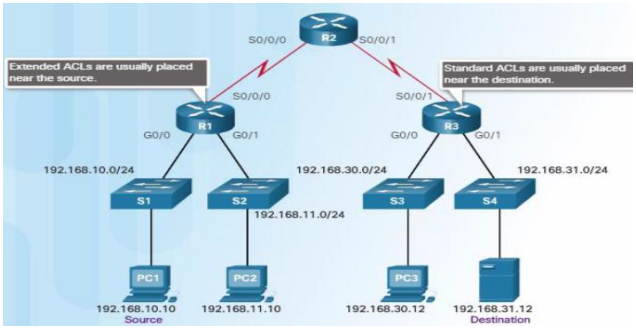


Figure 3.37 : ACL Standard et ACL Etendue.

Une ACL Peut être appliqué dans un sens entrant ou sortant sur une interface à l'aide de la commande ip access-group.

Elle peut également être appliquée sur un port VTY utilisant la commande access-class Dans l'exemple suivant une ACL est défini pour autoriser tous les hôtes du réseau 192.168.10.0.0 avec un masque de sous réseau 255.255.255.0 á accéder, et de refuser l'accès pour l'hôte ayant l'adresse 192.168.10.10, l'ACL est appliquée á une interface de sortie S0/0/0 d'un routeur R1.

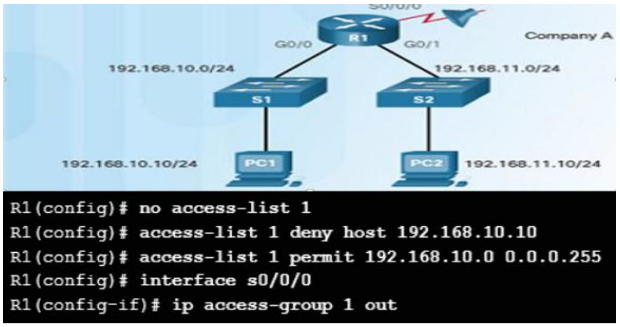


Figure 3.38 : exemple d'une ACL.

3.3.3.5 Protection contre les risques du réseau externes:

- Pour protéger le réseau des risques de l'extérieur, un par feu doit être mis en place, nous proposons le Par feu **ASA 5500** (Appliance de Sécurité Adaptative), l'un des produits de Cisco lancé en mai 2005 qui a remplacé le PIX , il utilise le même système d'exploitation que ce dernier appelé Finese et offre plusieurs avantages.

  Le par feu ASA doit être mis en place entre le réseau interne et le réseau externe pour assurer une meilleure sécurité contre les risques du trafic de l'extérieur.

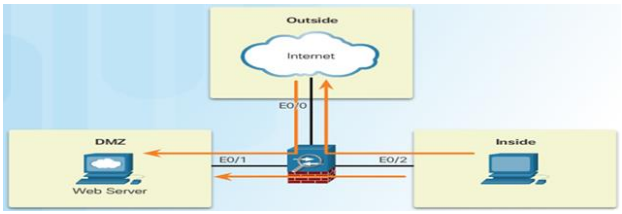


Figure 3.39 : positionnement d'un par feu ASA.

La gamme Cisco **ASA 5500 Anti-X** Edition permet aux entreprises de tirer pleinement avantage de leurs activités Internet tout en fournissant une solution complète de sécurité et de connectivité VPN. Grâce à ses fonctionnalités intégrées de pare-feu, de protection anti-X et de VPN, elle 5500 élimine les logiciels malveillants ou espions, le spam et les tentatives de phishing qui transitent par le courrier électronique et le trafic Internet. Cette solution garantit une continuité et une sécurité maximale dans les activités. Avec son filtrage intégré des URL (qui permet à l'entreprise de contrôler l'utilisation d'Internet par ses collaborateurs en interdisant l'accès aux sites Web indésirables).



Figure 3.40 : Modèles Cisco ASA.

La gamme Cisco ASA 5500 Anti-X Edition offre une sécurité périmétrique souple tout en assurant la gestion de la productivité des collaborateurs. L'intégration de services VPN au sein de cette solution permet également de protéger l'accès à distance contre les différentes menaces. Parmi ses avantages on cite :

A. **Technologie de pare-feu éprouvée la plus largement déployée** : s'appuyant sur les fonctionnalités éprouvées des serveurs de sécurité dédiés Cisco PIX®, la gamme Cisco ASA 5500 facilite l'entrée du trafic professionnel tout en rejetant les visiteurs indésirables. Grâce au contrôle intégré des applications, cette solution peut aussi limiter les transmissions P2P, la messagerie instantanée et le trafic malveillant qui sont autant de sources de vulnérabilités et qui favorisent l'introduction de menaces sur le réseau.

B. **Fonctions anti-X parmi les meilleures du marché** : sur les serveurs de la gamme Cisco ASA 5500, la technologie de passerelle de sécurité de Trend Micro a été associée aux fonctionnalités Cisco de prévention des menaces. Ces serveurs proposent ainsi une solution complète de protection contre les logiciels malveillants (logiciels espions, virus, spam ou contenus indésirables) avec filtrage intégré des URL et des contenus :

    a. **Antivirus et anti-logiciels espions** : grâce à la technologie de protection contre les virus et les logiciels espions fournie par Trend Micro, les serveurs de la gamme Cisco ASA 5500 sont en mesure de bloquer pratiquement tous les codes malveillants avant qu'ils n'atteignent Internet. Le système évite ainsi l'interruption des applications et des services de l'entreprise et réduit le processus particulièrement onéreux de nettoyage après une infection.

    b. **Filtrage des URL et des contenus et « anti-phishing »** : le filtrage intégré des URL et des contenus ainsi que la technologie « anti-phishing » protègent l'entreprise et ses collaborateurs contre le vol d'informations confidentielles et contribuent à limiter leur responsabilités juridiques potentielles. Ils permettent également à l'entreprise de se conformer aux réglementations telles que le HIPAA (Health Insurance Portability and Accountability Act.

    c. **Protection anti-spam** : la technologie anti-spam élimine la plupart des courriers électroniques indésirables avant qu'ils n'atteignent le serveur de courrier. Vous améliorez ainsi la productivité de vos collaborateurs tout en évitant le gaspillage de la bande passante et des capacités de stockage du réseau.

C. **Protection des VPN contre les menaces** : s'appuyant sur les fonctionnalités VPN de la gamme des concentrateurs Cisco VPN 3000, la gamme Cisco ASA 5500 Anti-X Edition garantit une connectivité sécurisée et l'accès des utilisateurs distants au réseau et aux services de l'entreprise. Cette solution apporte à l'entreprise un maximum de souplesse et de sécurité pour ses connexions, en associant la prise en charge des fonctionnalités VPN SSL (Secure Socket Layer) et IPSec (IP Security) .

D. **Simplicité de déploiement et de gestion** : la suite logicielle de gestion et de surveillance centralisées autorise les déploiements et l'utilisation à grande échelle des serveurs de la gamme Cisco ASA 5500 Anti-X Edition avec un personnel et des dépenses d'exploitation réduits au minimum. Cisco propose ainsi, sur un appareil unique, une solution complète de gestion et de surveillance avec le gestionnaire Cisco ASDM (Adaptive Security Device Manager), interface navigateur puissante, facile à gérer et à contrôler **[19]**.

Description	Capacité utilisateurs	Référence
Ensembles Anti-X Edition		
Ensemble Cisco ASA 5510 Anti-X Edition (serveur ASA 5510, CSC-SSM-10, antivirus 50 utilisateurs, anti-logiciels espions, abonnement d'un an au service *)	jusqu'à 500 utilisateurs	ASA5510-CSC10-K9
Ensemble Cisco ASA 5520 Anti-X Edition (serveur ASA 5520, CSC-SSM-20, antivirus 500 utilisateurs, anti-logiciels espions, abonnement d'un an au service *)	jusqu'à 1 000 utilisateurs	ASA5520-CSC20-K9
Licences de mise à niveau en option		
Licence CSC-SSM-10 Plus pour Cisco ASA 5500 (avec, en plus, filtrage des URL, filtrage des contenus, anti-phishing et anti-spam, et abonnement d'un an au service *)		ASA-CSC10-PLUS=
Licence CSC-SSM-20 Plus pour Cisco ASA 5500 (avec, en plus, filtrage des URL, filtrage des contenus, anti-phishing et anti-spam, et abonnement d'un an au service *)		ASA-CSC20-PLUS=
Mises à niveau de la licence utilisateur de CSC-SSM-10 pour la gamme Cisco ASA 5500 (total d'utilisateurs **)		ASA-CSC10-USR-100= ASA-CSC10-USR-250= ASA-CSC10-USR-500=
Mises à niveau de la licence utilisateur de CSC-SSM-20 pour la gamme Cisco ASA 5500 (total d'utilisateurs **)		ASA-CSC20-USR-750= ASA-CSC20-USR-1k=

Figure 3.41 : Ensembles et options recommandés pour la version Anti-X Edition.

Différents modèles de la gamme **ASA 5500** sont disponibles sur marché, le choix dépend du besoin de l'organisation selon :

- ✓ Le débit maximum.
- ✓ Le nombre maximum des connections par seconde.
- ✓ Le budget disponible.

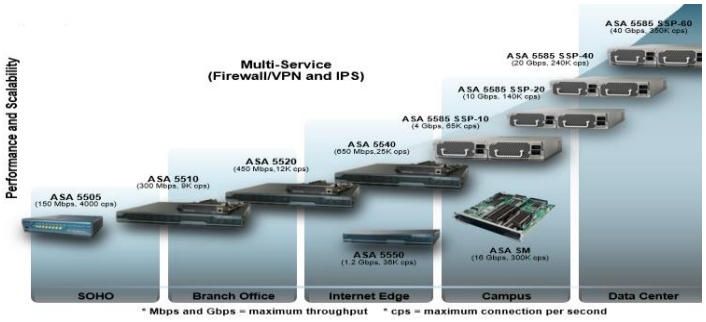


Figure3. 42: Modèles ASA.

Des fonctionnalités IPS (Inspection and Prevention Security) sont assurées par le ASA en intégrant des modules spéciaux : un module Advanced Inspection and Prevention Security Services Module(AIP-SSM) pour ASA 5540 ,et une carte (AIP-SSC) pour ASA 5505.

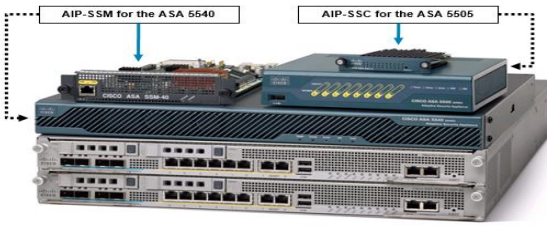


Figure3.43 : Modules IPS.

L'Appliance ASA est préinstallé avec une licence de base (Base licence), et une autre licence de sécurité (Security Plus licence).

Des licences optionnelles peuvent être achetées et ajoutées pour créer une licence permanente, qui est activée en installant une clé permanente avec la commande activation-key. Pour vérifier les informations sur la licence, la commande show version et show activation-key sont utilisées.

Enfin, la topologie finale proposée est la suivante :

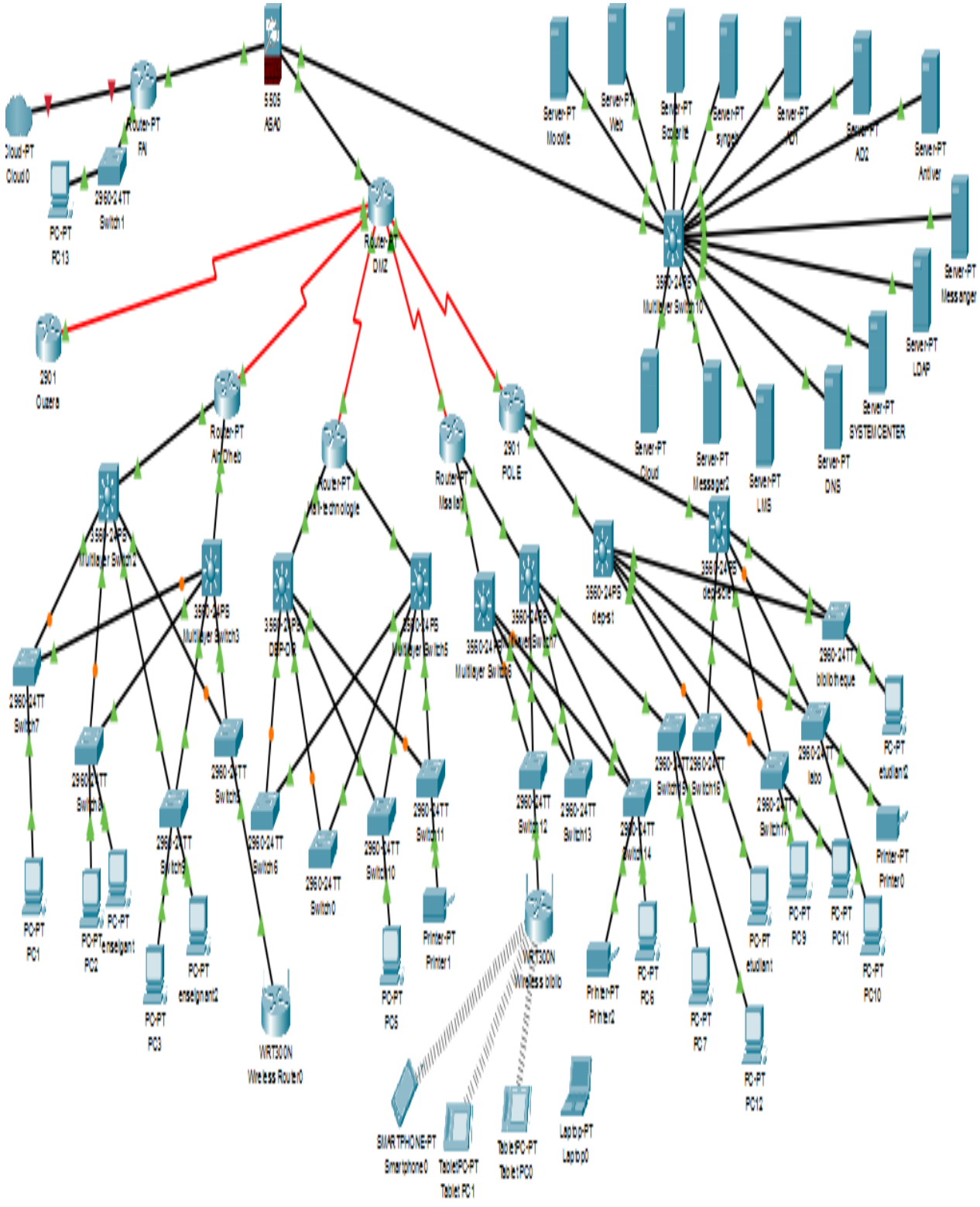


Figure 3.44 : topologie réseau finale.

Conclusion :

Au cours de ce chapitre, nous avons d'abord défini l'environnement du travail, l'existant et la situation informatique, ensuite nous avons critiqué, et proposé des solutions pour pallier aux problèmes de failles du réseau. Pour chaque solution proposée nous avons présenté la méthode d'implémentation et les protocoles utilisés avec une comparaison entre ces protocoles pour justifier le choix.

Le chapitre suivant sera consacré á l'implémentation des solutions proposées.

Chapitre 04

Chapitre 04 : Configuration et tests.

4.1 Introduction :

Dans ce qui suit, nous allons entamer la configuration des différentes solutions proposées dans le chapitre précédant. Nous décrirons les outils et les protocoles utilisés, et les principales étapes de la configuration et la vérification nécessaires á l'implémentation de ces solutions.

Dans cette partie, nous allons utiliser le logiciel GNS3 comme simulateur, et le logiciel VMware comme logiciel de virtualisation.

4.2 Description de l'environnement de travail :

4.2.1 Présentation de GNS3 :

GNS3, "Graphical Network Simulator-3", est une interface graphique frontale et une plateforme de contrôle écrites en Python pour simuler des infrastructures informatiques. Les technologies de virtualisation utilisées par GNS3 sont Dynamips, VPCS, VMWare Workstation/ESXi, VirtualBox, QEMU/KVM, Docker, …

Le logiciel émule aussi des technologies LAN/WAN comme Ethernet, Frame-Relay, ATM, HDLC, Il permet d'interconnecter les ordinateurs émulés sur des commutateurs virtuels ou des interfaces physiques du serveur.

Une topologie peut être distribuée sur plusieurs serveurs. Il permet de construire des topologies complexes.

Il est possible de capturer en temps réel le trafic qui passe par les interfaces des périphériques.

Les topologies créées (on parle de *projets GNS3*) sont importables/exportables [19].

4.2.2 Fonctionnement :

Le logiciel GNS3 peut s'installer en "standalone" avec une interface graphique client et un serveur en local. Mais la méthode actuellement préconisée est d'utiliser un serveur GNS3 installé localement dans une machine virtuelle ou dans le nuage chez un prestataire comme OVH (mais aussi Packet, AWS, GCP, etc.). Le serveur est alors commandé à travers un tunnel VPN avec une installation locale du client GUI.

Une interface Web client vise à terme à remplacer le client graphique lourd de telle sorte que le serveur se suffise à lui-même et que l'utilisateur puise manipuler les topologies et les consoles des périphériques uniquement avec un navigateur Web (Firefox ou Chrome).

Le serveur GNS3 commande les machines virtuelles exécutées par les logiciels de virtualisation et d'émulation. GNS3 est développé en Python.

4.2.3 Versions de GNS3 :

La dernière version recommandée est la 2.2.8 pour GNS3-SERVER et GNS3-GUI, elle offre une interface web, une nouvelle manière d'intégrer les modèles d'Appliance, une meilleure gestion des machines Qemu/KVM et Hyper-V, de nouveaux diagrammes de périphériques et beaucoup d'autres fonctionnalité.

4.2.4 Architecture Client / Serveur :

GNS3 fonctionne selon un modèle client / serveur. Les deux logiciels client et serveur doivent fonctionner dans une version identique.GNS3 évolue rapidement en plusieurs branches. Pour une meilleure expérience, on peut aisément installer les dernières versions en développement.

4.2.5 Composants GNS3 :

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à [20] :

- **Dynamips** : Emulateur d'IOS Cisco.
- **Dynagen** : Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.
- **Qemu** : Emulateur de système.
- **Virtualbox** : Logiciel permettant la création de machines virtuelles.
- **Wireschark** : est un logiciel pour analyser les trames.

Voici l'interface graphique du logiciel GNS3 :

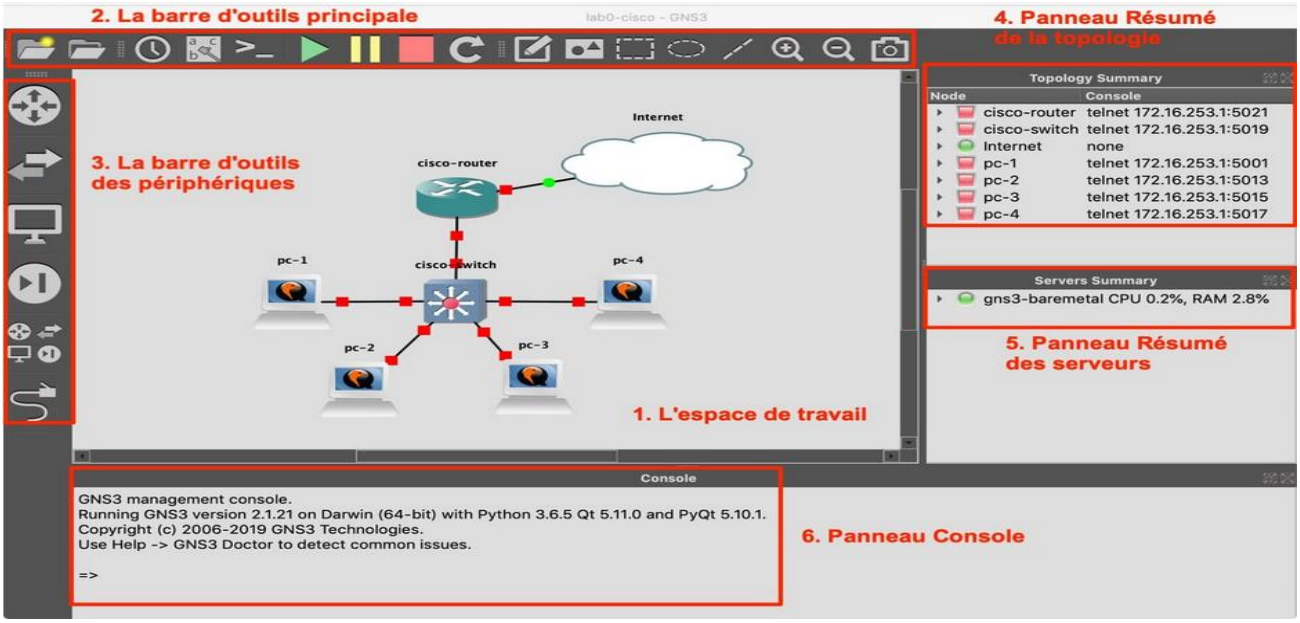


Figure 4.1 : Interface graphique du GNS3.

Grâce à ces composants, GNS3 nous permet :

- Le design de topologies réseaux de haute qualité et complexes.

- Emulation de plusieurs plateformes de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.
- Simulation de switches Ethernet, ATM et Frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireshark.
  Remarque : Pour la simulation de ce travail, on peut utiliser un autre simulateur qui est propriétaire Cisco appelé Packet tracer que nous avons présenté dans **l'annexe E**.

Remarque :

Pour les switches de couches 3 l'adresse attribuée á l'interface virtuelle SVI int Vlan 1est de la forme 192.168.x.15/24 pour chaque réseau, exp : 192.168.11.15/24 pour le switch Dep-sci (département science).

Pour les switches de couche 2 l'adresse est de la forme 192.168.x.17, exp : 192.168.11.17 pour l'interface int Vlan 1sur le switch Bibliothèque.

Nous avons proposé de configurer ASA comme serveur DHCP .

4.2.6 Configuration initial :

Dans cette partie nous avons configuré un mot passe pour le mode enable pour la ligne console et la ligne vty. Nous avons renommé les périphériques, enfin nous avons chiffré les mots de passes utilisés et un message de jour « Access non autorisé » est configuré. Et ceci pour les switches et les routeurs.

```
Ouzera(config-line)#pass
Ouzera(config-line)#password cisco
Ouzera(config-line)#login
Ouzera(config-line)#line vty 0 4
Ouzera(config-line)#pass
Ouzera(config-line)#password cisco
Ouzera(config-line)#login
Ouzera(config-line)#service pass
Ouzera(config-line)#exit
Ouzera(config)#ser
Ouzera(config)#service pass
Ouzera(config)#service password-encryption
Ouzera(config)#
Ouzera(config)#bann
Ouzera(config)#banner motd#access authorise pour l'admin seulement#
```

Figure 4.2 : configuration de base.

Après la configuration, si on quitte la console puis on lance une autre session, un mot de passe doit être introduit :

```
access authorise pour l'admin seulement

User Access Verification

Password:

Switch>en
Password:
Switch#
```

Figure 4.3 : Vérification des mots de passe et le message du jour.

Les mots de passe apparaissent chiffrés dans le fichier de configuration actuelle running-config :



Figure 4. 4: Mot de passe chiffré.

Nous avons désactivé le protocole DNS pour ne pas avoir des conflits, comme suite :

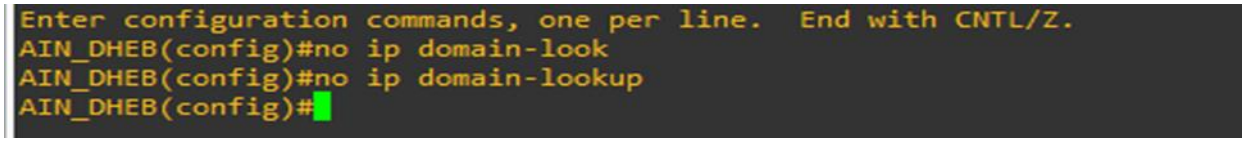


Figure 4.5 : Désactivation du protocole DNS.

Nous avons fixé une langueur minimale de 10 caractères pour la configuration de mot passe:

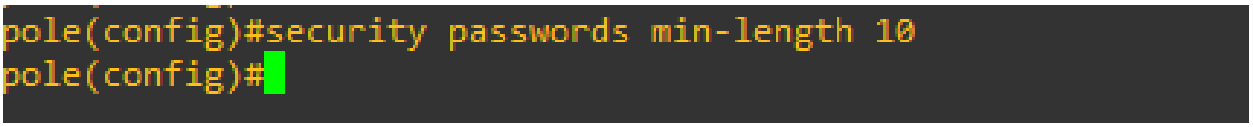


Figure 4.6 : longueur minimale d'un mot de passe.

Si un mot de passe est configuré avec une longueur inférieure à 10 caractères, un message de console est affiché pour informer l'utilisateur que la langueur minimale n'est pas respectée.

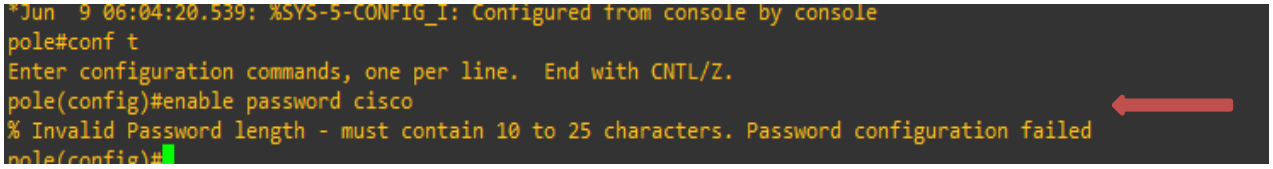


Figure 4.7 : Contrainte de longueur minimale.

4.2.7 Sécurité des ports switches (Niveau LAN):

Les interfaces non utilisées des switches sont désactivées avec la commande **shutdown :**

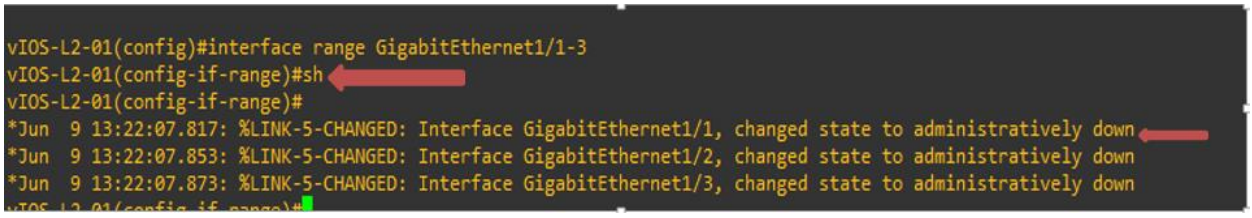


Figure 4.8 : Désactivation des interfaces inutiles.

Nous avons activé la sécurité des ports de switches, en appliquant la commande suivante :



Figure 4.9: Activation de la sécurité des ports.

Nous avons fixée le nombre maximum des adresses mac autorisées sur un port d'un switch à 1 :

```
bibliotheque(config-if)#int f0/4
bibliotheque(config-if)#switchport port-security maximum 1
bibliotheque(config-if)#
```

Figure 4.10 : configuration du maximum des adresses MAC sur un port.

Pour la sécurité des switches, la commande **switch port port-Security mac-address sticky** peut être utilisé sur une interface pour permettre un apprentissage rémanent des addresses MAC sur l'interface.

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
Switch(config-if)#
```

Figure 4.11: Adresses sticky.

Nous avons régler le mode de violation sur le mode Shutdown :

```
Switch(config-if)#
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
```

4.12 : régler mode violation

On peut vérifier la configuration, en affichant les paramètres de sécurité d'une interface :

```
bibliotheque#sh port-security int f0/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0006.2A90.7E72:1
Security Violation Count   : 0
```

Figure 4.13 : Affichage des paramètres de sécurité d'une interface.

4.2.8 Sécurité de la gestion d'accès :

Un délai de 5 min et 30s de time out pour les trois lignes vty, console, auxiliaire est activé.

```
vIOS-L2-01(config-if)#exit
vIOS-L2-01(config)#line console 0
vIOS-L2-01(config-line)#exec-timeout 5 30
```

Figure 4.14 : time out de la ligne console.

Comme mesure de sécurité contre les attaques de type force brute (plusieurs tentatives), on a configuré les routeurs et les switches de telle façon que les connections seront désactivé durant 120s après 5 tentatives échouées qui se produisent dans les 60s.

```
AIN_DHEB(config)#login block-for 120 attempts 5 within 60
AIN_DHEB(config)#exit
```

Figure 4. 15 : Bloque des connections.

Pour vérifier cette configuration, la commande show login est utilisée :

```
AIN_DHEB#sh login
    A default login delay of 1 seconds is applied.
    No Quiet-Mode access list has been configured.

    Router enabled to watch for login Attacks.
    If more than 5 login failures occur in 60 seconds or less,
    logins will be disabled for 120 seconds.

    Router presently in Normal-Mode.
    Current Watch Window
        Time remaining: 41 seconds.
        Login failures for current window: 0.
    Total login failures: 0.
```

Figure 4.16 : Vérification de la configuration du bloque.

L'hôte administrative ayant l'adresse 192.168.1.30 (comme exemple) est exclu du bloque de la connexion. PERMIT-ADMIN permet au Station administrative de garder une connexion possible.

```
AIN_DHEB(config)#ip access-list standard PERMIT-ADMIN
AIN_DHEB(config-std-nacl)#remark Permit only ADministrative hosts
AIN_DHEB(config-std-nacl)#permit 192.168.1.30
AIN_DHEB(config-std-nacl)#exit
AIN_DHEB(config)#login quiet-mod access-class PERMIT-ADMIN
AIN_DHEB(config)#login delay 10
AIN_DHEB(config)#login on-success log
AIN_DHEB(config)#login on-failure log
AIN_DHEB(config)#exit
AIN_DHEB#
*Mar  1 00:37:27.951: %SYS-5-CONFIG_I: Configured from console by cons
AIN_DHEB#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
AIN_DHEB#
```

Figure 4. 17 : Access liste d'autorisation pour l'administrateur.

Toutes les tentatives de login, faites en Telnet, SSH ou http sont refusées,

4.2.9 Protection contre la manipulation STP :

Comme mesure de sécurité contre les attaques de type STP manipulation, nous avons activé

la fonction portfast sur les ports d'accès de couche 2, comme il est montré dans la figure :

```
bibliotheque(config-if-range)#int range f0/4-10
bibliotheque(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION
```

Figure 4.18: Activation de STP portfast.

Ensuite nous avons activé la fonction **Bpdugard** sur tous les ports avec portfast active, qui empêche les hôtes du modes accès de recevoir les messages BPDUS .

```
bibliotheque(config-if-range)#spanning-tree portfast bpduguard default
bibliotheque(config)#
```

Figure 4.19 : Activation de la fonction Bpdugard.

Pour vérifier notre configuration, la commande show spanning-tree summary totals est utilisée.

```
bibliotheque#show spanning-tree summary totals
Switch is in pvst mode
Root bridge for: default
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
4 vlans                     0         0        0          1          1
```

Figure 4.20 : Affichage du résumé STP.

Voici un exemple de désactivation d'une interface qui a reçu un Bpdu STP :

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/1
with BPDU Guard enabled. Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/1, putting 0/1 in
err-disable state


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
```

Figure 4.21 : Désactivation d'une interface.

4.2.10 Protection contre les tempêtes :

Pour faire face aux attaques de type tempête (exp : DoS), nous avons limiter un seuil maximum de 75 pour le trafic de diffusion (broadcast) , en utilisant la commande **storm-control** au niveau du mode de configuration spécifique d'interface sur les switches et les routeurs .

```
bibliotheque(config-if)#storm-control broadcast level 75
bibliotheque(config-if)#
```

Figure 4.22: Configuration d'un seuil maximum du trafic de diffusion.

On peut vérifier l'activation de contrôle avec la commande **show storm-control** comme suit :

```
bibliotheque#sh storm-control broadcast
Interface   Filter State    Upper          I
----------  ---------------  -------------  -
Fa0/2       Link  Down        75.00%
Fa0/20      Link  Down        75.00%
```

Figure 4.23 : Vérification de contrôle.

4.2.11 Création des VLAN :

Nous avons créé les vlans appropriés dans chaque bloc au niveau des switches de couche 2

Comme exemple : sur le switch bibliothèque dans le site pole on a créé les vlans suivants :

VLAN étudiant, vlan travailleurs, vlan imprimante, vlan scolarité.

```
bibliotheque(config)#vlan 10
bibliotheque(config-vlan)#name etudiant
bibliotheque(config-vlan)#vlan 40
bibliotheque(config-vlan)#name travailleur
bibliotheque(config-vlan)#vlan 60
bibliotheque(config-vlan)#name imprimante
VLAN #30 and #60 have an identical name: imprimante
bibliotheque(config-vlan)#vlan 30
bibliotheque(config-vlan)#name imprimante
bibliotheque(config-vlan)#vlan 70
bibliotheque(config-vlan)#name scolarite
```

Figure 4.24 : Création des vlans.

On peut visualiser ces vlans, avec la commande **show vlan** :

```
sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   etudiant                          active
30   imprimante                        active
40   travailleur                       active
60   VLAN0060                          active
70   scolarite                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figure 4.25 : Affichage des vlans.

Les ports d'un switch sont affectés par défaut au vlan1, il faut les affecter aux vlans correspondants .Pour le switch bibliothèque, on a affecté les ports comme suite :

```
bibliotheque(config)#int range f0/5-8
bibliotheque(config-if-range)#sw
bibliotheque(config-if-range)#switchport mode acc
bibliotheque(config-if-range)#switchport mode access
bibliotheque(config-if-range)#sw
bibliotheque(config-if-range)#switchport acce
bibliotheque(config-if-range)#switchport access vlan 10
```

Figure 4.26 : Affectation des ports.

On peut vérifier l'affectation des ports au vlans, en utilisant la commande **show vlan** :

```
bibliotheque#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   etudiant                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
30   imprimante                       active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
40   travailleur                      active    Fa0/22
```

Figure 4.27 : Vérification de l'affectation des ports.

On a défini le vlan 99 comme vlan natif dédie pour tous les ports trunk comme suite :

```
bibliotheque(config)#int f0/3
bibliotheque(config-if)#switchport trunk native vlan 99
```

Figure 4.28 : vlan natif.

Sur le switch bibliothèque le port f0/3 qui le relie avec le switch couche 3 doit être configuré en mode trunk :

```
bibliotheque(config-if)#int f0/3
bibliotheque(config-if)#switchport mode trunk
```

Figure 4.29 : Interface en mode trunk.

Le protocole DTP doit être désactivé sur les ports d'accès avec la commande **switch port nonegotiate,** dans le but de les empêcher de négocier l'agrégation (Trunk).

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport nonegotiate
Switch(config-if)#
```

Figure 4.30 : Désactivation du protocole DTP.

La commande **show interface <interface> switchport** nous a permis de vérifier la désactivation :



Figure 4.31 : Vérification de la désactivation du DTP.

4.2.12 AAA authentification :

Pour activer l'authentification AAA, on utilise la commande **aaa new model,** ensuite, on doit définir la méthode d'authentification á l'aide de la commande **aaa-authentification** :

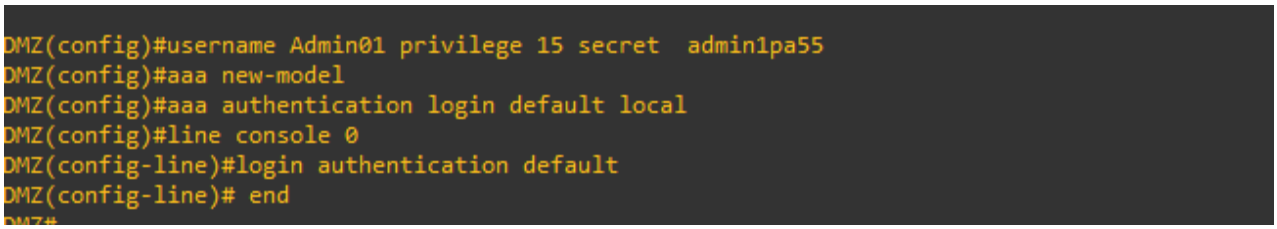


Figure 4.32 : Configuration de l'authentification.

Pour vérifier, on quitte la console et on réinitialise la session :

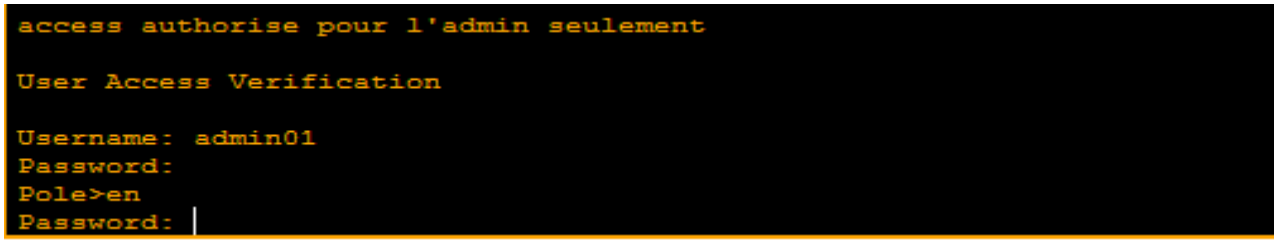


Figure 4.33: Vérification de l'authentification.

4.2.13 Configuration du protocole de routage :

Pour le routage inter-réseaux, nous avons configuré le protocole EIGRP qui est un protocole de routage propriétaire Cisco. Il suffit de configurer un id pour chaque routeur, les interfaces passives qui ne doivent pas passer les messages de mise á jour EIGRP, et enfin annoncer les réseaux directement connectés et désactiver le résumé automatiques des adresses :

```
POLE(config)#router eigrp 1
POLE(config-router)# eigrp router-id 6.6.6.6
POLE(config-router)# passive-interface GigabitEthernet0/0
POLE(config-router)# passive-interface GigabitEthernet0/1
POLE(config-router)# network 192.168.2.0
POLE(config-router)# network 10.0.1.0 0.0.0.3
POLE(config-router)# network 192.168.11.0
POLE(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.0.1.2 (Serial0/0/0) is up: new adjacency

POLE(config-router)#no auto
POLE(config-router)#no auto-summary
```

Figure 4.34 : configuration du protocole de routage.

La connectivité doit être établit entre les routeurs :

Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Ouzera	Ain D'heb	ICMP		0.000	N	0
	Successful	Ouzera	Msallah	ICMP		0.000	N	1
	Successful	Ouzera	Pole	ICMP		0.000	N	2

Figure 4.35 : Vérification de la connectivité.

4.2.14 Configuration de Cisco Adaptative Security (ASA) :

Le par feu **ASA** filtre le trafic entre trois réseaux : interne, externe, et le réseau des serveurs qui sont représentés par les interfaces virtuelles (SVI) :

- **Interface vlan1** : nommée Inside avec un niveau de sécurité (sécurity level) 100 ,pour connecter le réseau interne .
- **Interface vlan2** : nommée outside avec un niveau de sécurité égale à 0,pour se connecter à Internet.
- **Interface vlan3** : nommée DMZ avec un niveau de sécurité égale à 50 pour connecter le réseau des serveurs.

Le réseau peut être schématisé comme suit :

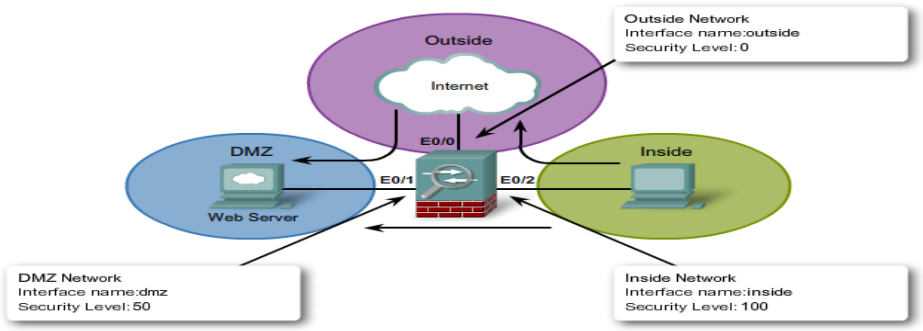


Figure 4.36 : Intégration d'un par feu dans un réseau.

4.2.14.1 Configuration de base :

D'abord on doit vérifier la version IOS et les caractéristiques hardwares du ASA avec la commande show version :

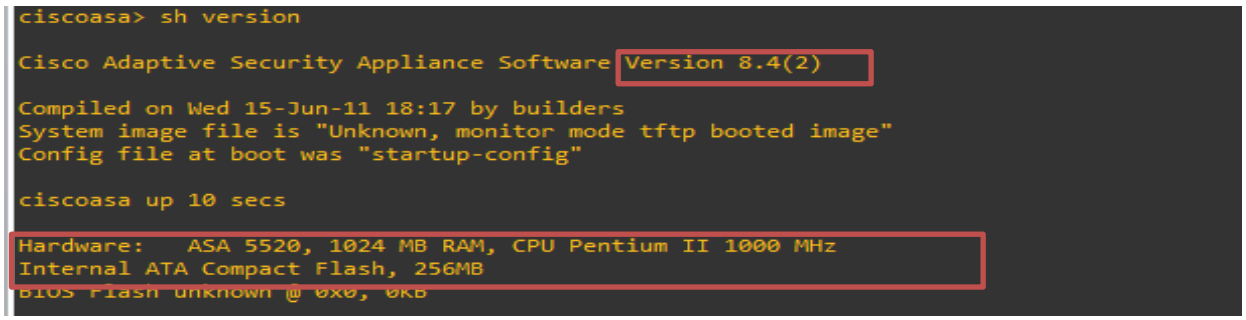


Figure 4.37 : Version d'IOS ASA.

Cette commande permet aussi d'afficher le la License ASA et les options de sécurité.

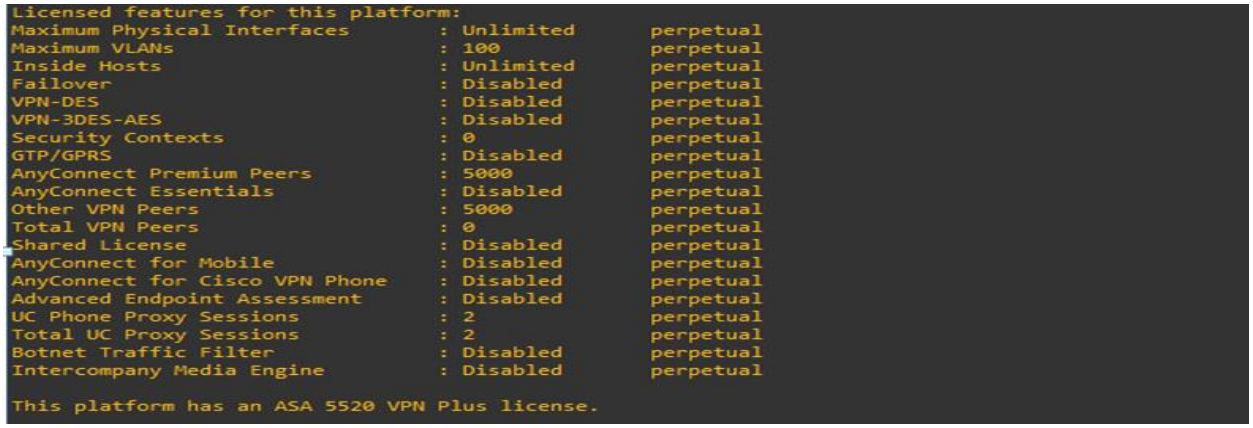


Figure 4.38 : License ASA.

Ensuite on configure les paramètres de base comme le nom et le mot de passe du mode enable et les interfaces de sécurité de ASA :



Figure 4.39: configuration de base ASA.

Après un nouvel accès à la console ASA, un mot de passe est demandé pour le mode enable.



Figure 4.40: Vérification du mot de passe.

4.2.14.2 Configuration des interfaces :

Nous avons configuré l'interface vlan1 comme inside (réseau interne), l'interface vlan2 comme outside (réseau externe) comme ci montré en dessous :

```
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#int vlan 1
ciscoasa(config-if)#security-level 100
```

Figure 4.41 : Configuration des interfaces.

Pour vérifier notre configuration, la commande show switch vlan est utilisée:

```
ciscoasa#sh switch vlan

VLAN Name                                Status    Ports
---- ----------------------------------- ---------
-------------------------------
1    inside                              up        Et0/1, Et0/2, Et0/3,
Et0/4
                                                   Et0/5, Et0/6, Et0/7
2    outside                             up        Et0/0
ciscoasa#
```

Figure 4.42 : Vérification des interfaces.

4.2.14.2.1 Test de connectivité :

Le Ping de routeur DMZ vers l'interface Inside (192.168.1.1) doit maintenant aboutir, mais vers l'interface Outside (209.165.200.226) ne doit pas aboutir

```
DMZ#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

DMZ#ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figure 4.43 : Test de connectivité.

4.2.14.3 Configuration de routage pour ASA:

Nous avons configuré une route statique par défaut sur l'interface Outside vers le réseau externe.

```
ciscoasa#conf t
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ciscoasa(config)#
```

Figure 4.44 : configuration d'une route dar défaut.

Cette route est affichée après la configuration dans la table de routage d'ASA :

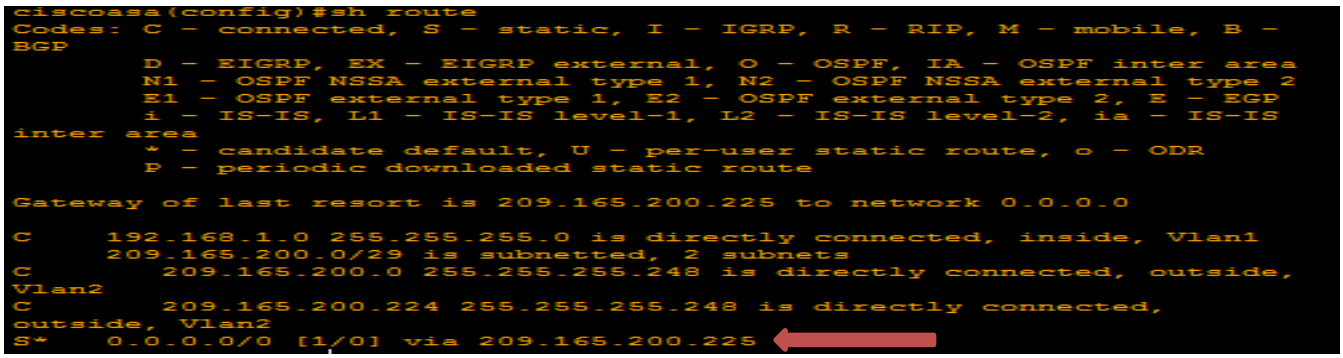


Figure 4.45 : la table de routage.

Maintenant ASA peut envoyer un Ping à n'importe quel hôte du réseau externe. On prend le pc 13 ayant l'adresse 172.16.3.3 comme exemple :

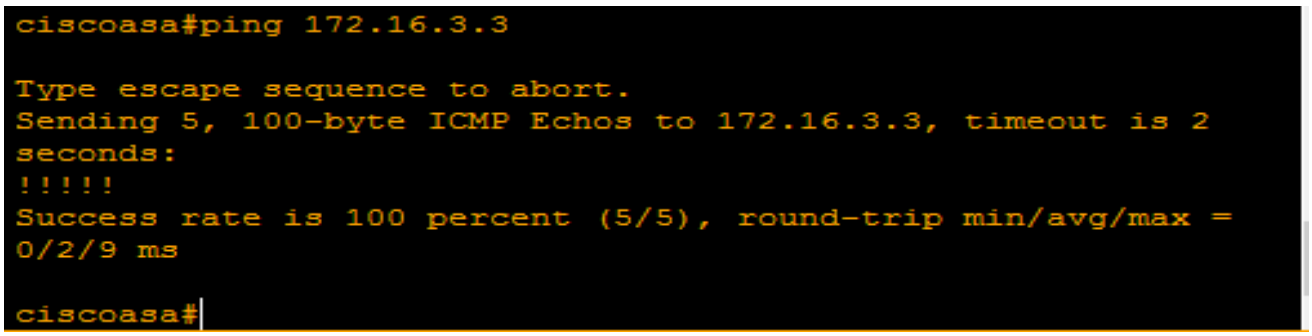


Figure 4.46 : Ping réussit depuis ASA vers l'extérieur.

Et voici une capture de ce Ping :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	ASA0	PC13	ICMP		0.000	N	0	(edit)
	Successful	ASA0	PC13	ICMP		0.000	N	1	(edit)

Figure 4.47: Capture du Ping depuis ASA vers un hôte externe.

4.2.14.4 configurations d'un objet NAT :

Nous avons défini un objet NAT (Network Adresse Translation) pour le réseau Inside,

Le trafic d'origine Inside vers le réseau Outside sera traduit par l'adresse configurée au niveau de l'interface Outside (209.165.200.226).

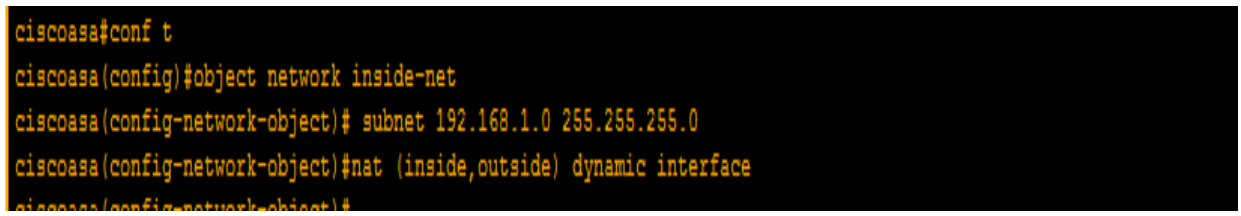


Figure 4.48: configuration de NAT.

La commande **show xlate** permet d'afficher les adresses traduises par la fonction NAT :

```
ciscoasa#show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net
NAT from dmz:192.168.12.0/24 to outside:209.165.200.227/24 flags s idle 00:29:26,  timeout 0:00:00
NAT from inside:192.168.1.0/24 to outside:209.165.200.228/24 flags s idle 00:01:19,  timeout 0:00:00

ciscoasa#
```

Figure 4. 49:Verification de NAT.

La commande **show Nat** peut être aussi utilisée pour vérifier la fonction NAT :

```
ciscoasa#SH NAT
Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source static inside-net 209.165.200.228
    translate_hits = 0, untranslate_hits = 0
```

Figure 4.50 : Vérification par la commande show Nat.

4.2.14.5 Création d'une carte de politique d'inspection (MPF : Map Policy Framework) :

Pour l'inspection au niveau de la couche application, et pour d'autres options, Cisco ASA offre le service MPF qui permet d'inspecter le trafic entre le réseau Inside et le réseau Outside. La configuration du MPF regroupe trois étapes :



Figure 4.51 : Etapes de MPF.

Pour cela, nous avons créé une classe-map, une politique-map, et un service map pour inspecter le trafic du réseau Inside vers le réseau Outside, et nous avons ajouté le service du protocole ICMP(Ping) á la liste d'inspection, avec les commandes suivantes :

```
ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
```

Figure 4.52 : configuration d'une carte de politique.

4.2.14.6 Configuration d'ASA comme un serveur DHCP :

Le routeur ASA peut être configuré pour servir le réseau comme étant un serveur DHCP. Un pool d'adresses pour le réseau 192.168.12.0 est configuré et activé (comme exemple) :

```
ciscoasa(config)#dhcpd address 192.168.12.3-192.168.12.30 dmz
ciscoasa(config)#dhcpd dns 209.165.201.2 interface dmz
ciscoasa(config)#dhcpd enable inside
ciscoasa(config)#dhcpd enable dmz
```

Figure 4.53 : activation du serveur DHCP.

Pour vérifier la configuration, un hôte de ce réseau, est configuré avec un adressage automatique et on verifie ensuite l'adresse attribué par la **commande ipconfig / all :**

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0090.2100.C2A7
   Link-local IPv6 Address.....: FE80::290:21FF:FE00:C2A7
   IP Address.....: 192.168.12.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.12.1
   DNS Servers.....: 209.165.201.2
   DHCP Servers.....: 192.168.12.1
   DHCPv6 Client DUID.....: 00-01-00-01-C7-B1-A5-CA-00-90-21-00-C2-A7
```

Figure 4.54 : Vérification de l'adressage automatique.

4.2.14.7 Configuration d'authentification AAA pour SSH avec la base de données locale :

D'abord, un nom utilisateur (username) local est défini, suivi par un mot de passe, ensuite on configure AAA pour qu'il utilise la base de données locale pour l'authentification des utilisateurs SSH :

```
ciscoasa(config)#username admin password cisco
ciscoasa(config)#aaa authentication ssh console LOCAL
ciscoasa(config)#
```

Figure 4.55 : configuration AAA pour l'utilisateur SSH.

4.2.14.8 Configuration de l'Access vers ASA par le protocole SSH :

Nous avons configuré ASA pour qu'il permettre un accès depuis quelques hôtes du réseau Inside ou Outside ou DMZ pour la gestion via le SSH.

Nous avons pris comme exemple le pc 13(172.16.3.3), le serveur0 (192.168.12.20) et le routeur DMZ(192.168.1.2 pour int f0/0).

Depuis inside on lance une session SSH vers l'adresse 192.168.1.1 :



Figure4.56 : accès SSH depuis Inside.

Depuis Outside, on lance une session SSH vers l'adresse 209.165.200.226 :

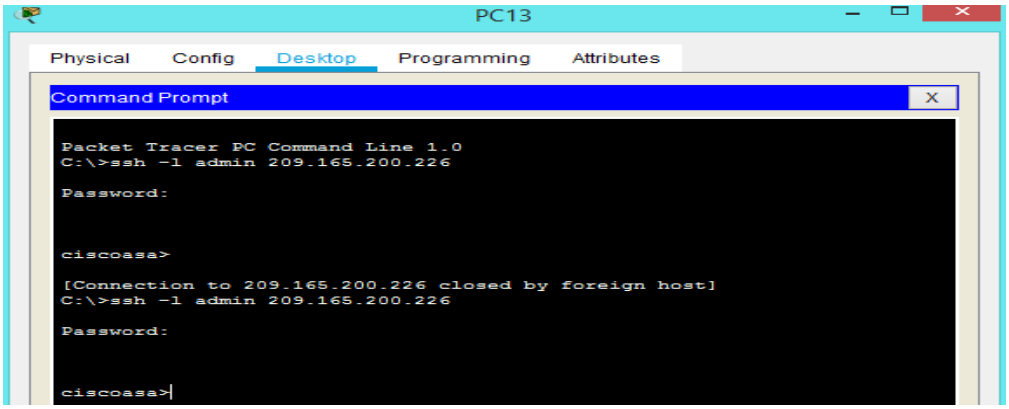


Figure 4.57 : accès SSH depuis Outside.

Depuis le serveur 0, on lance une session SSH vers l'adresse 192.168.12.1 :

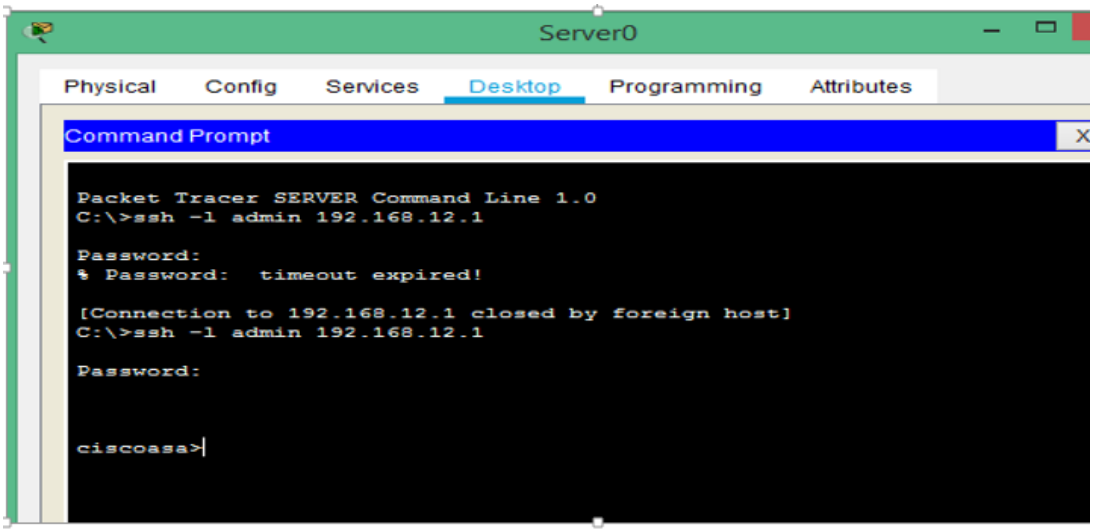


Figure 4.58 : Accès SSH depuis un serveur.

4.2.14.9 configuration du vlan DMZ :

Nous avons regroupé les serveurs du réseau dans un réseau lan sécurisé par l'ASA, l'interface vlan 3 est configuré de ce côté :

```
ciscoasa(config)#interface vlan 3
ciscoasa(config-if)#ip address 192.168.12.1 255.255.255.0
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 70
ciscoasa(config-if)#interface Ethernet0/2
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#
```

Figure 4.59: Création de Vlan DMZ.

Le vlan 3 doit apparaitre dans l'affichage des vlans :

```
VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------------------------
1    inside                          up        Et0/1, Et0/3, Et0/4,
Et0/5
                                               Et0/6, Et0/7
2    outside                         up        Et0/0
3    dmz                             up        Et0/2
```

Figure 4.60: affichage des interfaces.

Ensuite, nous avons définir un objet de NAT statique pour le réseau DMZ.

```
ciscoasa(config)#object network dmz-server
ciscoasa(config-network-object)#subnet 192.168.12.0 255.255.255.0
ciscoasa(config-network-object)#nat (dmz,outside) static
209.165.200.227
ciscoasa(config-network-object)#exit
```

Figure 4.61 : Création d'objet NAT pour DMZ.

4.2.14.10 Configuration des ACLs sur ASA:

Á ce niveau, plusieurs ACLs peuvent être configuré sur l'ASA dans le but de filtrer le trafic entrant ou sortant.

A titre d'exemple, nous avons configuré une ACL nommé Outside-DMZ, qui permet le protocole TCP sur le port 80, depuis n'importe quel hôte du réseau Outside vers le serveur Moodlle.

```
access-list OUTSIDE-DMZ extended permit icmp any host 192.168.12.3
access-list OUTSIDE-DMZ extended permit tcp any host 192.168.12.3 eq www
!
!
access-group OUTSIDE-DMZ in interface outside
```

Figure 4.62 : Configuration des ACLs.

Á ce niveau, le ASA peut être configuré pour qu'il accepte l'accès par http, avec la commande **http server enable**, pour permettre á l'administrateur d'accéder á l'interface graphique GUI D'ASA pour la configuration d'autres options.

4.2.15 Configuration de VPN IPsec site á site :

Les VPN site-à-site sont un autre type d'infrastructure WAN (réseau étendu). Ils remplacent et améliorent les réseaux privés existants utilisant les lignes louées(dédiée). Ils permettent la prise en charge de la tunnellisation et du cryptage en utilisant les protocoles standard du marché, tels que IPsec (Internet Protocol Security), 3DES (Digital Encryptions Standard 3) et AES.

Nous avons proposé la solution VPN site á site pour relier les différents sites de l'université entre eux . Dans ce qui suit nous allons configurer un VPN entre le site POLE et le nouveau site Ouzera, Les mêmes étapes sont á suivre pour les autres sites avec un changement des adresses.

la configuration de la création de VPN est faite juste sur les deux routeurs POLE et Ouzera, aucune configuration sur les autres routeurs n'est faite.

La configuration passe par cinq phases :

4.2.15.1 Configuration des paramètres d'IPsec sur le routeur POLE :

1ere Etape : Activation du paquet de technologie de sécurité (Security Technology package):

On doit d'abord vérifier la version d'IOS par la commande **Show version** pour s'assurer que l'option technologie de securité est activé, sinon on doit l'activé par la commande :

License boot module c1900 technology-package securityk9.

Dans notre cas, l'option de securité est active.

```
Technology Package License Information:

------------------------------------------------------------------------
Technology    Technology-package                Technology-package
              Current             Type          Next reboot
------------------------------------------------------------------------
appxk9          None              None           None
uck9            None              None           None
securityk9      securityk9        Permanent      securityk9
ipbase          ipbasek9          Permanent      ipbasek9
security        securityk9        Permanent      securityk9
ipbase          ipbasek9          Permanent      ipbasek9
```

Figure 4.63: Vérification de la License.

2ere Etape : Identification du trafic qui doit passer dans le tunnel(ACL) (Trafic intéressant):

Nous avons défini une ACL qui permet d'identifier le trafic á crypter dans le tunnel du VPN, c'est le trafic ayant source le réseau 192.168.11.0 255.255.255.0 ou le réseau 192.168.2.0 255.255.255.0 vers la destination le réseau de l'interface loopback du routeur Ouzera 192.168.9.1 comme suite :

```
Pole(config)#access-list 110 permit ip 192.168.11.0 0.0.0.255 192.168.9.0 0.0.0.255
Pole(config)#access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.9.0 0.0.0.255
Pole(config)#
```

Figure 4.64 : Acl pour le trafic VPN.

3eme Etape : activation du protocole ISAKMP :

Avant d'entamer la création des VPNs, nous avons activé le protocole ISAKMP qui gére l'échange des clés qui seront utilisées entre les deux extrémités du tunnel (routeur POLE et routeur Ouzera) dynamiquement.

```
POLE(config)#crypto isakmp policy 10
POLE(config-isakmp)#encryption aes 256
POLE(config-isakmp)#authentication pre-share
POLE(config-isakmp)#group 2
POLE(config-isakmp)#exit
```

Figure 4.65 : Activation d'ISAKMP et négociation de clé.

Sachant que :

- **Policy:** qui définit la politique de connexion pour les SA (Security Association) de ISAKMP. Un numéro indiquant la priorité de l'utilisation est attribué à la fin de la commande.
- **ipsec-isakmp :** Créer une nouvelle carte de chiffrement.
- **Encryption:** l'algorithme de chiffrement utilisé est aes 256.
- **Pre-share:** utilisation d'une clé pré-partagée comme méthode d'authentification.
- **Groupe 2:** L'algorithme d'échange de clé Diffie-Hellman est utilisé, par défaut c'est le groupe 1 qui est utilisé (768 bits), dans notre cas nous avons utilisé le groupe 2 (1024 bits).

Ensuite, nous avons attribué un mot de passe qui est partagé entre les deux extrémités appelée clé pré-partagée (pre-shared key).

```
POLE(config)#crypto isakmp key vpnpa55 address 10.0.5.1
POLE(config)#
```

Figure 4.66: Clé pré-partagée.

4eme Etape : Configuration de la politique d'IPsec (IPsec policy) :

Pour configurer IPsec les éléments suivants doivent être configurés dans l'ordre.

- configurer la méthode de cryptage des données «transform-set», que l'on nomme VPN-SET.
- Création de crypto-MAP qui va regrouper tous les paramètres. C'est une carte cryptographique « crypto-map » qui associe le trafic qui correspond à une liste d'accès.
- Définition d'une extrémité de l'ACL déjà configuré110.

```
POLE(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
POLE(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
POLE(config-crypto-map)#description VPN connection to R3
POLE(config-crypto-map)#set peer 10.0.5.1
POLE(config-crypto-map)#set transform-set VPN-SET
POLE(config-crypto-map)#match address 110
POLE(config-crypto-map)#exit
POLE(config)#exit
```

Figure 4. 67: Politique IPsec.

•**crypto ipsec transform-set vpnset** : Créer un ensemble de transformation appelé VPN-SET.

•**esp-aes-** :la méthode de cryptage AES et le protocole ESP IPSec seront utilisés.

•**esp-sha-hmac**- L'algorithme de hachage SHA sera utilisé

•**Sha**: l'algorithme de hachage.

•**Set peer :** définir une extrémité du VPN.

•**match address :** Associe l' ACL précédemment crée 110.

Nous prenons soin de vérifier d'avoir utilisé les mêmes protocoles d'encryptions et de Hash utilisés dans la première étape.Cette politique d'IPsec est attribuée á l'interface de sortie du routeur Pole S 0/0/0.

```
POLE(config)#int s0/0
POLE(config-if)#crypto map VPN-MAP
POLE(config-if)#
*Mar  1 00:01:47.795: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure4.68 : Affectation du MAP á l'interface de sortie.

4.2.15.2 Configuration des paramètres d'IPsec sur le routeur Ouzera :

Pour le routeur Ouzera qui représente la deuxième extrémité, nous avons suivi les mêmes étapes du routeur POLE comme ci montré dans la figure suivante :

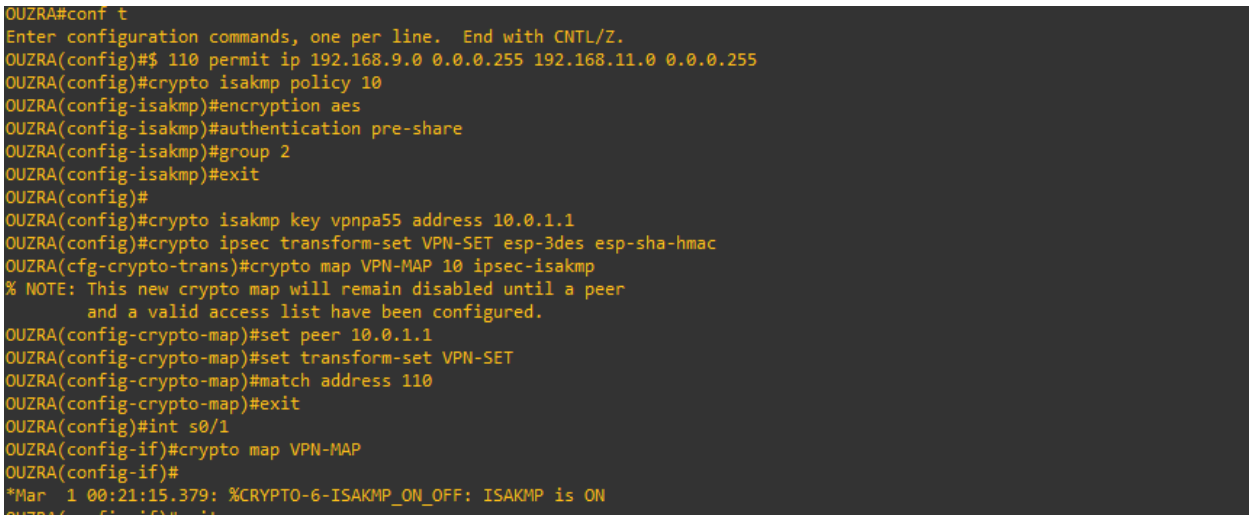


Figure 4.69 : Configuration d'IP sec sur le routeur Ouzera.

Pour le routeur Ouzera l'ACL est défini sur le trafic ayant l'adresse source 192.168.9.0 et l'adresse de destination 192.168.11.0,ou l'adresse 192.168.2.0, et la IP sec-MAP est attribuée á l'interface de sortie S0/0/0 du routeur Ouzera.

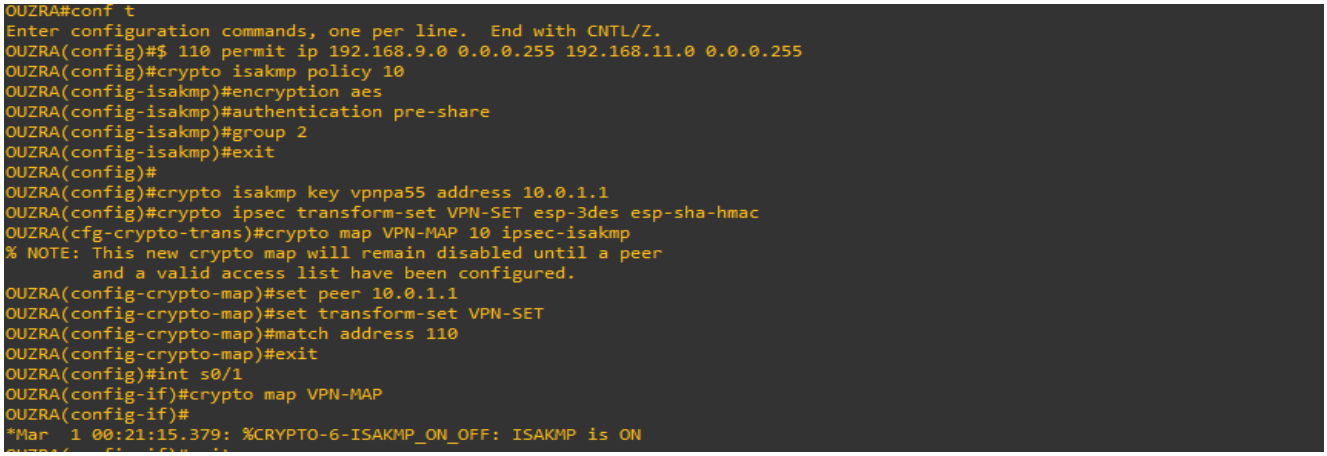


Figure 4.70 : Configuration du VPN sur le routeur Ouzera.

Á ce niveau le VPN est établit entre les deux extrémités.



Figure 4.71: VPN établit.

4.2.15.3 Vérification de IPsec VPN :

Nous avons vérifié d'abord la politique d'ISAKMP sur les deux routeurs par la commande **show crypto ipsec transform-set**:

```
Ouzera#sh crypto ipsec transform-set
Transform set VPN-SET: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Figure 4.72 : Vérification de transform-set sur le routeur Ouzera.

```
POLE#sh cryp
POLE#sh crypto ip
POLE#sh crypto ipsec tr
POLE#sh crypto ipsec transform-set
Transform set VPN-SET: {    { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Figure 4.73 : Vérification de transform-set sur le routeur POLE.

Ensuite, nous avons affiché le résumé du crypto-MAP appliqué sur les deux routeurs, en utilisant la commande **show crypto map**:

```
POLE#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        WARNING: This crypto map is in an incomplete state!
                (missing peer or access-list definitions)
        Peer = 10.0.5.1
        No matching address list set.
        Current peer: 10.0.5.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/0/0
```

Figure 4.74: Vérification de crypto map sur le routeur POLE.

```
Ouzera#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
       WARNING: This crypto map is in an incomplete state!
               (missing peer or access-list definitions)
       Peer = 10.0.1.1
       No matching address list set.
       Current peer: 10.0.1.1
       Security association lifetime: 4608000 kilobytes/3600 seconds
       PFS (Y/N): N
       Transform sets={
              VPN-SET,
       }
       Interfaces using crypto map VPN-MAP:
              Serial0/0/0
```

Figure 4.75 : Vérification de crypto map sur le routeur Ouzera.

La commande **show crypto isakmp sa** nous a permis d'afficher s'il existe des Sas (Associations de sécurité), aucune Sa n'est affichée si le trafic envoyé n'est pas intéressant (n'est pas inclus dans l'ACL 110).

Pour cela nous avons envoyé un Ping entre le routeur POLE et Ouzera (c-à-dire entre l'adresse 10.0.1.1 et l'adresse 10.0.5.1) ce qui génère un trafic **non intéressant** pour notre cas, le Ping est abouti:

```
POLE#ping 10.0.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.5.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/3/11 ms
```

Figure 4.76 : Ping entre POLE et Ouzera.

Mais le trafic n'est pas encapsulé dans le tunnel car il **n'est pas intéressant** par apport au VPN (n'est pas indiqué dans l'ACL), aucune association de sécurité SA n'est affichée :

```
POLE#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Figure 4.77 : Vérification des associations de sécurité.

Et aucun paquet n'est crypté :

```
POLE#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.9.0/255.255.255.0/0/0)
   current_peer 10.0.5.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.1.1, remote crypto endpt.:10.0.5.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:
```

Figure 4.78: Verification d'encapsulatin et d'encryption.

Ensuite, nous avons générer un trafic **intéressant** (depuis le réseau 192.168.11.1 ou 192.168.2.1 vers l'interface loopback du routeur Ouzera ou l'inverse), pour cela nous avons exploité la commande Ping étendu qui permet de personnaliser l'adresse source et destination comme suite :

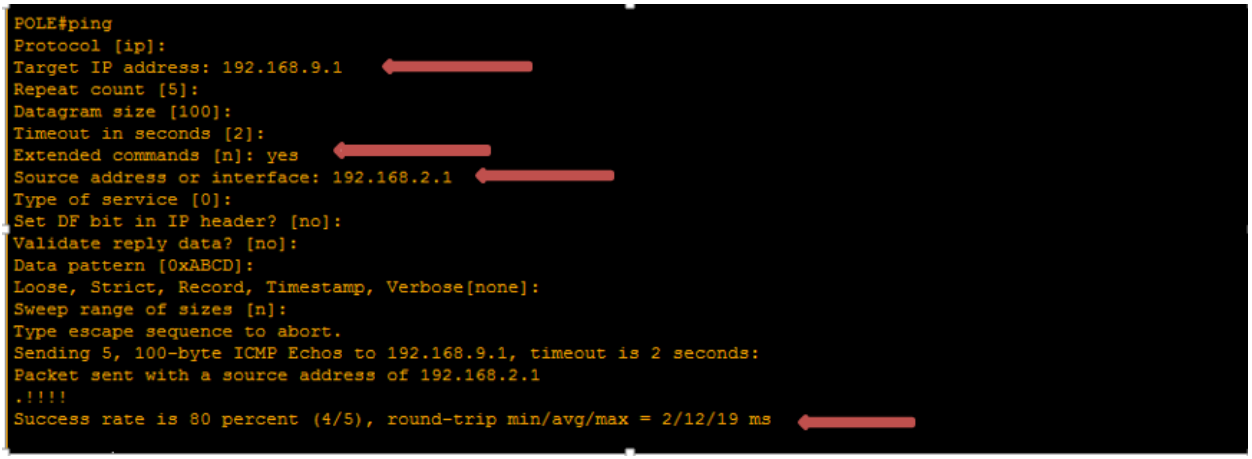


Figure 4.79 : Ping etendu entre pole et ouzera.

Ce trafic ICMP (Ping) est un trafic intéressant par apport au VPN donc une association de sécurité est affiché après la réexécution de la commande **:**

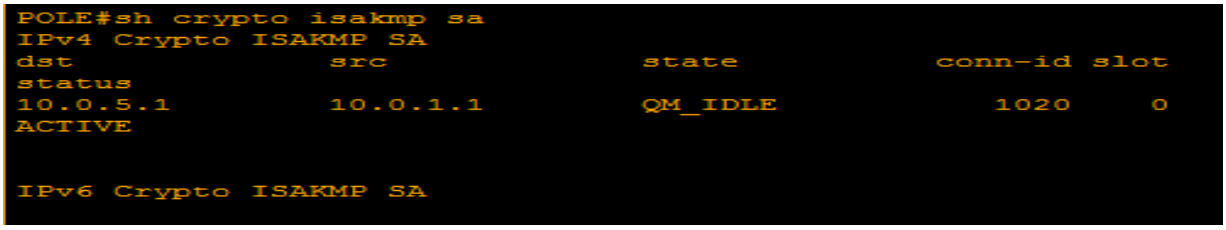


Figure 4.80 : Vérification des Sas sur le routeur POLE.

Le nombre des paquets encapsulés est diffèrent de zéro :

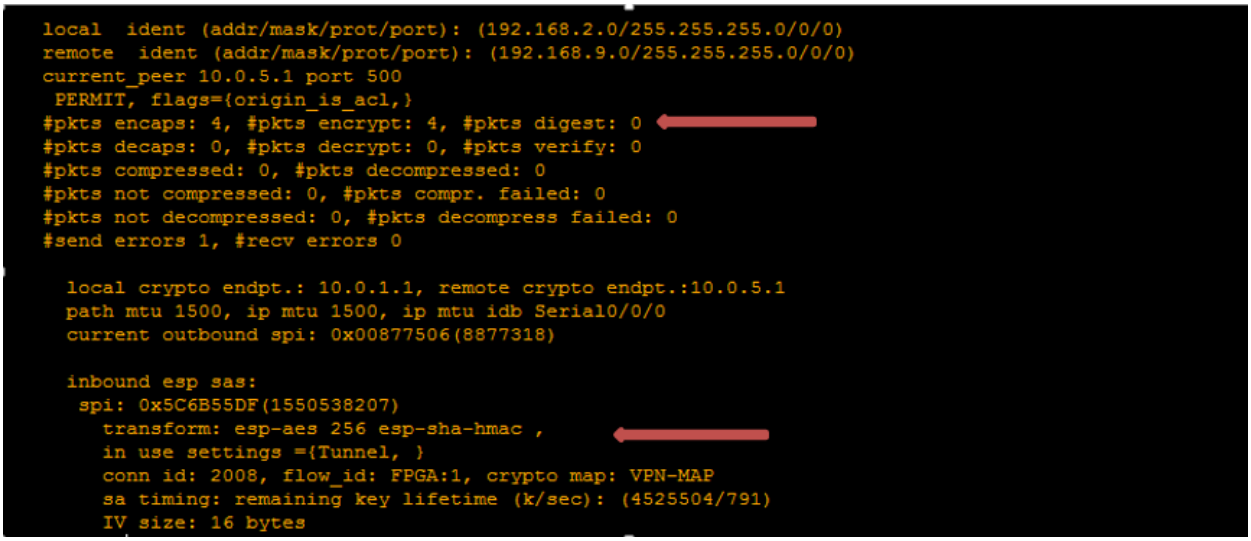


Figure 4.81 :Verification des paquets encapsulés et cryptés.

Nous avons vérifié l'affichage des **Sas** après un Ping depuis le routeur Ouzera aussi :

```
Ouzera#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.1.1        10.0.5.1        QM_IDLE           1072    0 ACTIVE (deleted)


IPv6 Crypto ISAKMP SA
```

Figure 4.82 : Vérification des Sas sur Ouzera.

Remarque : le trafic intéressant de ce VPN peut être un trafic ICMP, FTP, HTTP….etc.

4.3 Réalisation sur matériels :

Pour la réalisation réelle, nous avons travaillé sur des switches **Cisco Catalyst 2960**, des routeurs **Cisco 2800**, et des routeurs **ISR linksys**. Des câbles **UTP** catégorie **5** et des câbles séries sont utilisés pour le branchement, et un câble console pour la configuration.

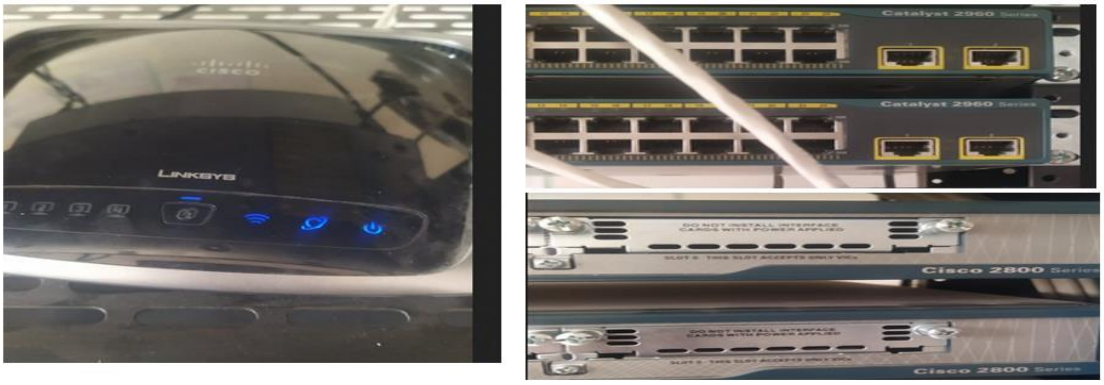


Figure 4.83 : Matériel utilisé.

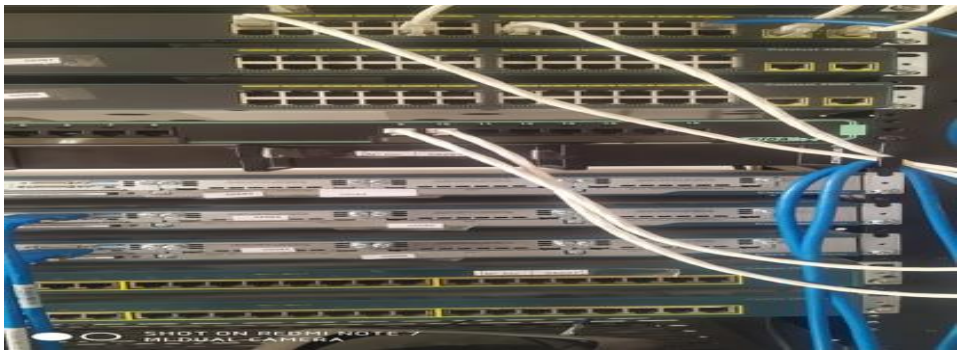


Figure 4.84 : Branchement des périphériques.

Nous avons utilisé Putty comme émulateur de terminal, qui permet un accès par protocole SSH, Telnet, ou par connexion directe par liaison série.

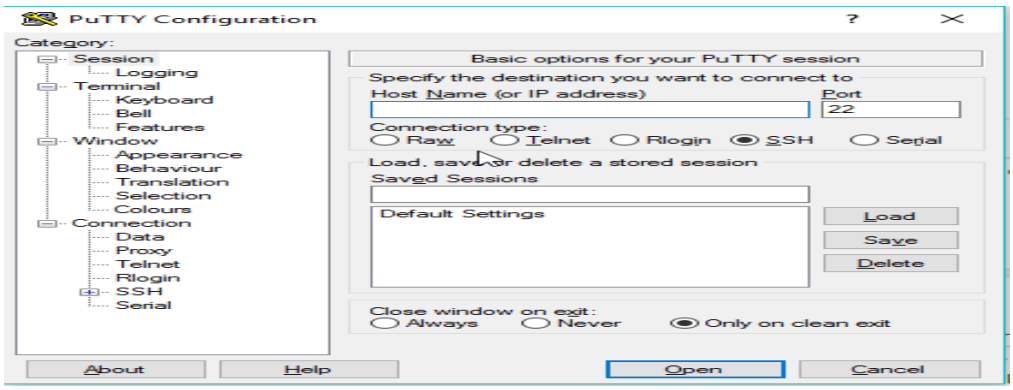


Figure 4.85 : Emulateur de terminal Putty.

Des captures de la configuration sont présentées dans **l'annexe D**.

Conclusion :

Dans ce chapitre, nous avons concrétisé les solutions proposées dans le chapitre précédent, en présentant la configuration des dispositifs concernés par les solutions par étapes.

Nous avons commencé par la sécurité au niveau LAN, ensuite la sécurité de l'Access pour la gestion des périphériques intermédiaires et enfin la sécurité au niveau WAN dans laquelle nous avons configuré le routage, le VPN site á site, l'authentification et le par feu ASA.

Enfin, on a vérifié les résultats de notre configuration, en utilisant différentes commandes.

Conclusion générale

Conclusion générale

Le travail que nous avons accompli avait pour principal objectif la proposition d'un audit de sécurité pour le réseau de l'université de Médéa. ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde sur la sécurité des réseaux.

Ce stage nous a permis d'abord de faire une étude détaillée du réseau informatique et de relever les différentes insuffisances présentées en terme de sécurité. Ensuite, nous avons abordé différentes solutions permettant de faire face aux insuffisances, pour cela, nous avons procédé á une étude d'efficacité de chacune de ces solutions en vue de choisir la plus adéquate permettant de rendre le réseau plus sécurisé. En outre, ce stage nous a permis de nous familiariser davantage aux équipements CISCO, et au simulateur GNS3 avec le logiciel VMware Workstation pour la machine virtuelle.

Nos solutions proposés ciblent les différents niveaux de l'architecture réseau pour faire face aux attaques de chaque niveau, commençant par la sécurité des réseaux LAN et WLAN où on a proposé la sécurité des ports des switches, la sécurité contre les attaques STP, et et les attaques de tempêtes, ainsi que la création des Vlans pour faciliter la gestion .Ensuite on a proposé des solutions pour sécuriser l'accès pour la gestion par les mots de passe cryptés ,le choix d'un protocole chiffré pour sécuriser le trafic de gestion qui est le protocole SSH.

Au niveau des réseaux WAN, une solution VPN site á site est proposée pour relier les différents sites de l'université, en créant un tunnel qui crypte et sécurise le trafic, et en plus de par feu logiciel, un par feu hardware ASA est proposé entre le réseau interne et l'extérieur, et enfin un système d'authentification en exploitant le protocole AAA jugé indispensable pour la sécurité de réseau.

De ce fait, pour une sécurité optimale, ces outils doivent être couplés à d'autres, comme les systèmes de surveillance du réseau informatique qui permettent á l'administrateur de garder œil sur toutes les les sources du trafic en particulier internet ,et sur toutes les tentatives d'accès au réseau. Comme logiciels de surveillance, SNMP (Simple Network Management Protocole) avec les stations d'administration réseau NMS (Network Management Station), Sys log (), Net flow(),peuvent être utilisés (**Voir Annexe F**).

Ces solutions de surveillance réseau étaient parmi nos objectifs dans ce travail, mais la courte période de stage ne nous a pas permis de les réaliser.

La réalisation de ce projet a été bénéfique et fructueuse pour nous dans le sens où elle nous a permis d'apporter une contribution à l'université Médéa, d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

Pour finir, nous pensons que la mise en œuvre de ces solutions que nous proposons est d'une importance capitale pour le bon fonctionnement du réseau informatique de l'université de Médéa. Evolutif, cette architecture pourra faire l'objet d'une future étude d'amélioration et de modification en fonction des besoins future de l'université.

Bibliographie

[1] : TanenbaumAndrew, Les réseaux, interdiction, 3ème Edition, 1998, Page 1.

[2] : DENAGNON Franck, MISE EN PLACE D'UN VPN (SITE-TO-SITE) AU SEIN D'UNE ENTREPRISE : CAS DE LA SOROUBAT (SOCIETE DE ROUTES ET BATIMENTS) MEMOIRE Pour l'obtention du Bachelor de l'Ecole Supérieure de Génie Informatique (ESGI - PARIS) Discipline Systèmes, Réseaux et Cloud Computing

[3] : S.Ikhalef. sécurité informatique Proxy, mémoire de fin d'études Ingéniorat, université de Bejaia 2003

[4] : université d'El-Oued Faculté de sciences exactes, 2 L.INFORMATIQUE, Réseaux, [Page consultée le 1/06/2017] le document est disponible sur internet :http://elearning.univeloued.dz/.../RESEAUXDECOMMUNICATI/.../Reseaux%20de%20com.

[5] : P.ATELEN, Réseaux informatique notion fondamental, 3eme édition ENI, janvier 2009.

[6] : Kassem AHMAD, Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS,Thèse de Doctorat l'Université de Nantes

[7] : JF.PILLOU, Tout sur les systèmes d'information, Paris Dunod 2006.

[8] : Van Quang-2005,Etude de la qualité de service pour les protocoles sécurisés de télécommunications. Application á IPSec, Université Paris ,online :http://doxa.u-pec.fr/these//th0231084.pdf

[9] : Laurent Poinsot, Cours " Sécrypt ", Chap. I : Introduction á la sécurité informatique.

[10] : KHELOUFI F, IKHLEF Y. Proposition de solution de sécurité pour le Réseau local de L'hôpital d'Amizour. Mémoire de Master d'Université Abderrahmane Mira de Béjaïa. Université Abderrahmane Mira de Béjaïa : 2016. 68 p.

[11] : imad Bou Akl , Etude des protocoles et infrastructures de sécurité dans les réseaux, DEA d'Informatique Année universitaire 2005/2006, Coopération dans les sciences de traitement de l'information Université libanaise Université Paul Sabatier _ I.R.I.T. Faculté des science.

[12] : Abdlmalek benzrki, . Creation des VPN pour la cyber sécurité d'Amizour. Mémoire de Master d'Université de Béjaïa: 2018,75 p

[13] : Kassem AHMAD, Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS,Thèse de Doctorat l'Université de Nantes.

[14] : Ahmim Marwa,Etude du protocole IPSec et métriques du sécurité ,thèse de doctorat,2016

[15] : [ROBIN Eric,Tourres Grégoire, Vernerie Matthieu, laboratoire Supinfo des technologie, reseaux et technologie Wan.]

[16] : CCSP Self-Study: CCSP SNRS Exam Certification Guide par: Greg Bastien; SaraCCIE No. 5824 Nasseh,; Christian Abera Degu , Publier par: Cisco Press

Webographie

[W1] : https://www.netacad.com/fr Dernier accès mars 2021

[W2]: https://www.malekal.com/les-differents-types-de-reseaux-lan-wan-man/

[W3] :http://supeinfo.com/

[W4] :A.ZBAKH. Module Informatique, Prince Molay Rchid,2007,http ://lycee.voila.net/mod4_chap1.pdf

[W5] :Frédéric Jacquenod. Cours Réseaux No5, les matériels d'interconnections,http ://www.netalya.com/fr/reseaux5.asp

[W6]: www.phpmaroc.com

[W7] :https://www.securiteinfo.com Dernier accès mars 2021

[W8] :http://aidesecurite.blogspot.com/2013/03/types-dattaques-dun-reseau.html

[W9] :http : //www-igm.univ-mlv.fr Dernier accès mai 2021

[W10]:http://www.linux-france.org Dernier accès mars 2021

[W11] :http : //www-igm.univ-mlv.fr Dernier accès mai 2021

[W12] :https://www.editions-eni.fr/open/mediabook.aspx

[W13]: www.certificat-ssl.info

[W14]:https://www.cloudflare.com/fr-fr/learning/network-layer/ /what-is-gre-tunneling/

[W15]:https://blog.varonis.fr/ids-et-ips-en-quoi-sont-ils-differents

[W16]:https://culture-informatique.net/cest-quoi-le-nat /

[W17] :orange-business.com/la vérité sur l'attaque VLAN hopping.

[W18]: [https://shms-rod.s3.amazonaws.com]

[W19]://www.cisco.com/c/dam/global/fr_ch/assets/docs/cisco_asa_5500_anti_x.pdf.

[W20]:cisco.goffinet.org/ccna/cisco-ios-cli/installer-et-configurer-gns3/

[W21] :A.Ksiks. Etude et simulation sur GNS3 du service MP-BGP/VPN-IP , 2011.

ANNEXE A

Présentation de l'organisme d'accueil :

L'enseignement supérieur à Médéa a vu le jour au cours de l'année universitaire 1988-1989, en vertu du décret 48-89 du 04 novembre 1989 dans les structures administratives qui ont accueilli l'Institut National de l'Enseignement Supérieur (INES) de l'électrotechnique, à l'époque où cet institut fut affilié à l'école moyenne El Fârâbî, dans le but d'offrir un enseignement supérieur dans les spécialités suivantes:

- Tronc commun Technologie.
- Formation à court terme en l'électrotechnique.

En juillet 2000, l'Institut National de l'Enseignement Supérieur a été promu en centre universitaire en vertu du décret exécutif N° 198-2000 du 23 Rabie Ethani 1421 correspondant au 25 juillet 2000. Le centre comprenait quatre instituts:

- L'institut des sciences et de la technologie.
- L'institut des sciences économiques, des sciences commerciales et de gestion.
- L'institut des sciences juridiques et administratives.
- L'institut des lettres et des Langues.

En vertu du décret exécutif N° 09-11 du 7 Moharram 1430 correspondant au 4 janvier 2009, portant création de l'universitéde Médéa, le nombre et la vocation des facultés composant l'université de Médéa sont fixés comme suit :

- Faculté des sciences et de la technologie ;
- Faculté des sciences économiques, des sciences commerciales et des sciences de gestion ;
- Faculté des lettres et des langues et des sciences sociales et humaines ;
- Faculté de droit ;

En vertu du décret exécutif N° 13-403 du 27 Moharram 1435 correspondant au 1 Décembre 2013 modifiant et complétant le décret exécutif N° 09-11 du 7 Moharram 1430 correspondant au 4 Janvier 2009, le nombre et la vocation des facultés composant l'université de Médéa sont fixés comme suit :

- Faculté des lettres et des langues;
- Faculté des sciences humaines et sociales;
- Faculté des sciences et de la technologie;

- Faculté des sciences économiques, des sciences commerciales et des sciences de gestion ;
- Faculté de droit ;

En vertu du décret exécutif n° 16-74 du 13 Joumada El Oula 1437 correspondant au 22 février 2016 modifiant et complétant le décret exécutif n°09-11 du 7 Moharram 1430 correspondant au 4 janvier 2009 ,le nombre et la vocation des facultés composant l'université de Médéa sont fixés comme suit :

- Faculté des lettres et des langues;
- Faculté des sciences humaines et sociales;
- Faculté des sciences économiques, des sciences commerciales et des sciences de gestion ;
- Faculté des sciences;
- Faculté de la technologie;
- Faculté de droit et des sciences politiques ;

ANNEXE B

Partie 1 :

Terminologies réseaux :

1) **IPv4 :**Pv4 est la quatrième version de la norme IP, qui établit les règles de fonctionnement des réseaux informatiques selon le principe de l'échange de paquets. Il peut identifier de manière unique les appareils connectés au réseau grâce à un système d'adressage. Chaque fois qu'un appareil accède à l'internet (qu'il s'agisse d'un commutateur, d'un PC ou d'autres appareils), une adresse IP numérique unique lui est attribuée, par exemple 192.149.252.76, comme indiqué ci-dessous. IPv4 utilise un système d'adresses de 32 bits permettant de stocker 2^32 adresses (4,19 milliards d'adresses). L'augmentation du nombre d'utilisateurs connectés sur Internet conduit à l'épuisement des adresses IPv4. C'est la raison pour laquelle le nouveau système d'adressage Internet, IPv6, est en cours de déploiement pour répondre au besoin d'un plus grand nombre d'adresses Internet.[1]

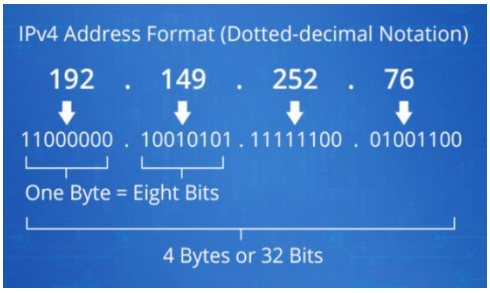


Figure01 :IPV4.

2) **Ipv6 :**IPv6 (Internet Protocol Version 6) a été déployé en 1999, en raison du fait que la demande d'adresses IP allait dépasser l'offre disponible. Il permet la communication et le transfert de données sur un réseau. IPv6 se compose d'une adresse IP de 128 bits qui prend en charge 2^128 adresses Internet au total. L'utilisation du protocole IPv6 permet non seulement de résoudre le problème des ressources limitées en adresses réseau, mais aussi de surmonter les obstacles permettant à de multiples dispositifs d'accès de se connecter à l'internet. Une adresse IPv6 ressemble à ceci : 3ffe:1900:fe21:4545:0000:0000:0000:0000.[2]

[1] **https://community.fs.com/fr/ Quelle est la différence entre l'IPv4 et l'IPv6 /FS Communauté**
[2] **https://www.ionos.fr/digitalguide/serveur/know-how/quels-sont-les-avantages-de-ipv6**

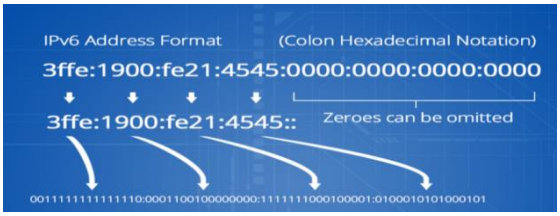


Figure02 :IPV6

3) **La passerelle par défaut :** Dans un réseau informatique **la passerelle par défaut** est le premier routeur rencontré par un ordinateur ou un smartphone. Son rôle est de permettre à cet appareil de communiquer avec les autres appareils présent dans d'autres sous-réseaux.[3]

4) **Le DHCP :** Le DHCP, pour « **Dynamic Host Configuration Protocol** » en anglais, est un protocole réseau permettant de distribuer une adresse IPv4 ou IPv6 à chaque hôte réseau faisant appel à ses services.[4]

   En effet un ordinateur afin de communiquer sur un réseau informatique doit posséder une adresse IP. Ainsi il est possible d'attribuer une **adresse IP** de manière statique ou bien par le biais d'un DHCP. Il est également chargé de distribuer l'adresse IP de la passerelle par défaut et du DNS.

5) **Le DNS :** DNS, pour « Domain Name Service » en anglais, est une des pièces maitresses d'internet. Ainsi son rôle est de traduire une adresse URL en adresse IP**.** [5]

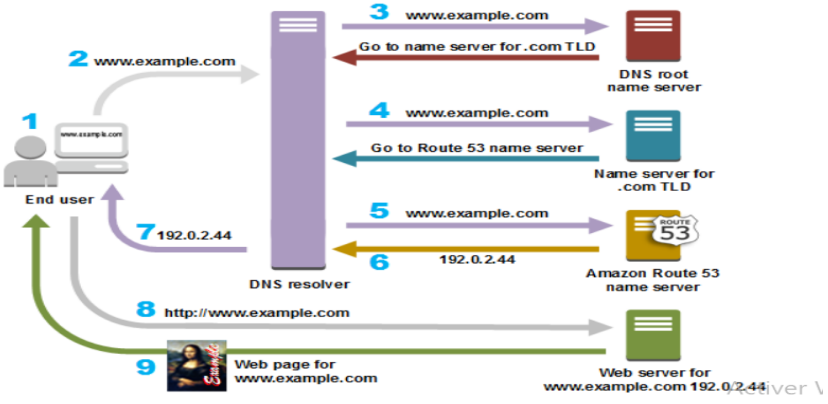


Figure03 : DNS.

Partie 2:

Les protocoles de routage :

Les **protocoles de routage réseau** sont essentiels ordinateurs connecté à un **réseau informatique local** souhaitant communiquer avec un ou plusieurs **réseaux distants**.[6]

---

[3] **Passerelle par défaut : définition et configuration - malekal.com**
[4] **https://www.frameip.com/dhcp/**
[5] **https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/**
[6] **https://www.le-hacking.fr/les-protocoles-de-routage-reseau**

En effet un **réseau local** n'a par définition connaissance que des réseaux auxquels il est directement connecté. Pour bien comprendre tout cela je dois vous expliquer la structure d'un réseau.

Deux catégories de routages existent: le routage statique et le routage dynamiques.

I. Le routage statique et dynamique :

A. Le **routage statique** a comme particularité que chaque sous-réseau présent doit être enregistré dans les routeurs manuellement. Il est utilisé dans de petits réseaux où l'on sait que peu de changement dans la topologie apparaitront au cours du temps.

B. Le routage dynamique se fait par l'intermédiaire des protocoles de **routage dynamiques**. Contrairement au routage statique, ils sont capable d'évolués au grès des changements de **topologies** des réseaux sans interventions extérieur comme un technicien réseau. Ils sont principalement configurés dans des réseaux de grandes ampleurs et permettent ainsi une plus grande flexibilité. En revanche ils sont plus lourds et long à configurer que les protocoles statiques.

II. Les protocoles de routage interne :

Les protocoles de routages interne ou « Internal Gateway Protocol » en anglais sont des protocoles de routage fonctionnant à l'intérieur d'un réseau. Ils ne sont donc pas faits pour relier plusieurs réseaux entre eux mais plutôt afin de permettre une communication entre les différents sous-réseaux.

1. **Le protocole de routage RIP :**Le protocole de routage RIP, abrégé de « **Routing Information Protocol** » en anglais, est défini dans le RFC 1058. Il fait partie des protocoles de routage dit « à vecteur de distance ».

   En effet la métrique utilisé par RIP afin de déterminé le chemin le plus court est le **nombre de saut** séparant le routeur source du routeur destination. RIP est basé sur l'algorithme de Bellman-Ford.

   Chaque routeur envoie aux routeurs auquel il est rattaché la liste de ses réseaux voisins. Ainsi chaque routeur possède une table de routage.

   Les routeurs gardent un lien entre eux par le biais d'envoi de **paquet** toutes les 180 secondes. RIP considère un routeur comme déconner s'il ne reçoit aucun message pendant 6 cycles de 180 secondes.

   De plus les routeurs RIP actualisent leur **table de routage** toutes les 15 secondes par envoie/réception des nouvelles tables.

2. **Le protocole OSPF :** OSPF pour « **Open Shortest Path First** » est un protocole de routage interne développé en 1987 par l'IETF, et décrit dans la **norme RFC 2328**. OSPF est dit à « état de lien ».

Le protocole OSPF est basé sur un algorithme plus efficace que celui de RIP: **Dijiksrta**.

La particularité d'OSPF par rapport à RIP est sa capacité à de mettre à jour sa table de routage de manière incrémentielle. En effet OSPF est capable de ne mettre à jour que les routes qui ont changé et non l'entièreté de la table de routage. Ainsi OSPF permet d'économiser la bande de passante.

Il permet également d'éviter les **boucles de routage**: phénomène ou un routage A envoi un paquet IP à un routeur B qui lui-même envoi au routeur A, causant ainsi une boucle de routage infini.

3. **Le protocole de routage EIGRP :** EIGRP est un protocole de routage interne propriétaire et optimisé pour le matériel Cisco. Il est multi-protocoles IPv4/IPv6. Ainsi il se place en concurrent direct du protocole OSPF, lui Open Source.

4. Contrairement à OSPF, EIGRP possède 3 tables:

    1. **Neighbors Table** : contenant l'adresse de ses voisins.
    2. **Topologie Table** : contenant toutes les routes EIGRP sans boucles.
    3. La table de routage accueille les meilleures routes EIGRP.

De plus l'algorithme d'EIGRP prend en compte de multiples facteurs influant sur la « qualité » du chemin:

- Le délai
- Charge
- Bande passante
- Fiabilité

Finalement, cet algorithme permet un meilleur calcul du chemin le plus court.

Partie 3 :

Protocole de cryptage :

1. **Iskamp (internet sécurity Association and key management protocol)**: ISAKMP définit des procédures et des formats de paquets pour établir, négocier, modifier et supprimer des associations de sécurité. Les SA contiennent toutes les informations requises pour l'exécution de divers services de sécurité réseau, tels que les services de couche IP (tels que l'authentification d'en-tête et l'encapsulation de charge utile), les services de transport ou de couche application, ou l'autoprotection du trafic de négociation.

Il définit des charges utiles pour l'échange de données de génération et d'authentification de clés. Ces formats fournissent un cadre cohérent pour le transfert

des données de clé et d'authentification qui est indépendant de la technique de génération de clés, de l'algorithme de chiffrement et du mécanisme d'authentification.

Il est distinct des protocoles d'échange de clés afin de séparer proprement les détails de la gestion des associations de sécurité (et de la gestion des clés) des détails de l'échange de clés. Il peut y avoir de nombreux protocoles d'échange de clés différents, chacun avec des propriétés de sécurité différentes. Toutefois, un cadre commun est nécessaire pour accepter le format des attributs SA et pour négocier, modifier et supprimer les SA. ISAKMP sert de cadre commun. [7]

[7] **http://www.networksorcery.com/enp/protocol/isakmp.html**

ANNEXE C

Quelques captures de la réalisation :

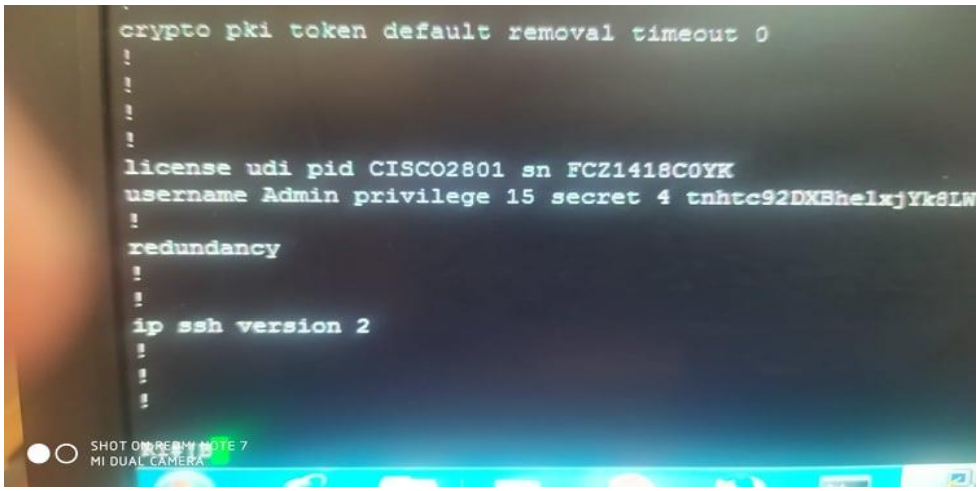


Figure 1 : Activation de SSH.

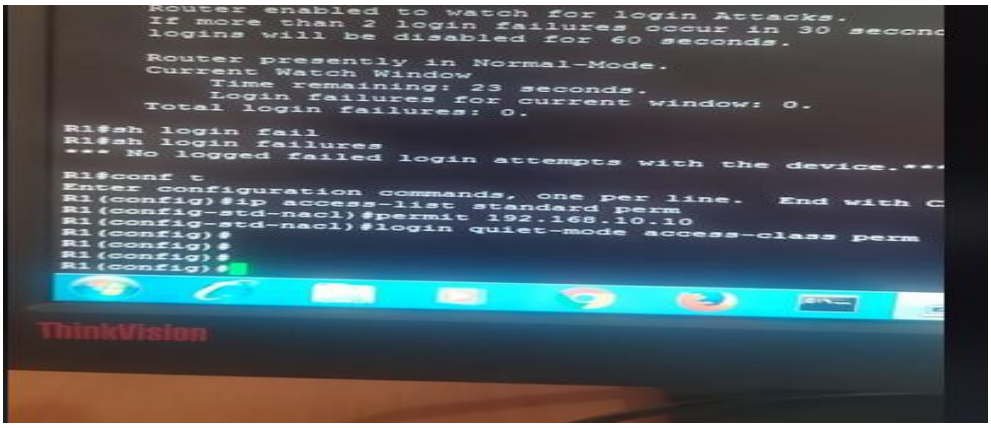


Figure 2 : Restriction de l'administrateur du bloque.

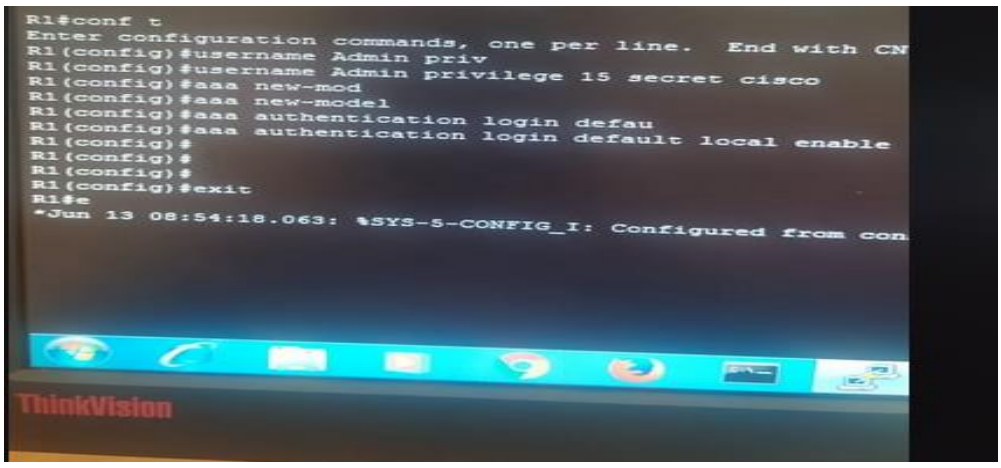


Figure 3 : Configuration de l'authentification.

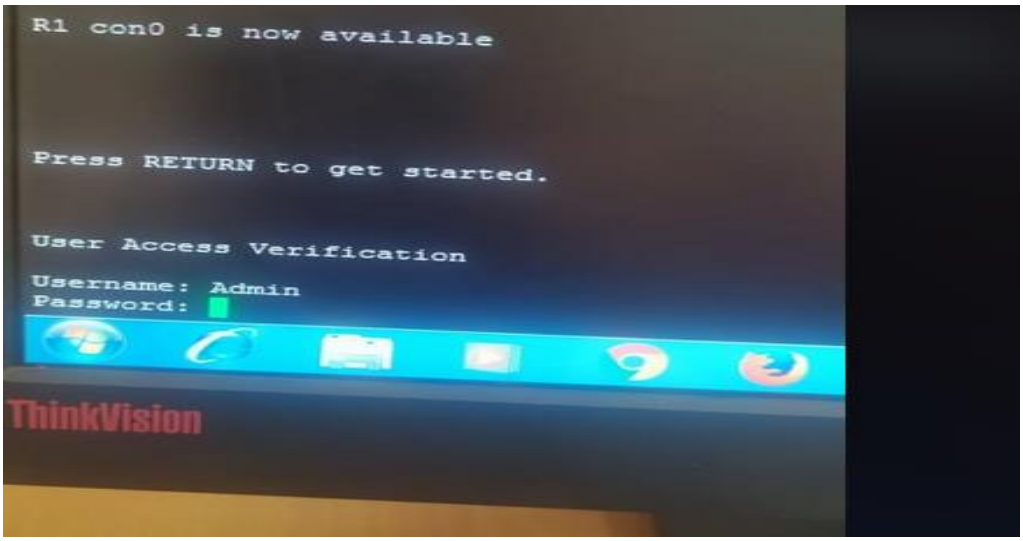


Figure 4 : Vérification de l'authentification.

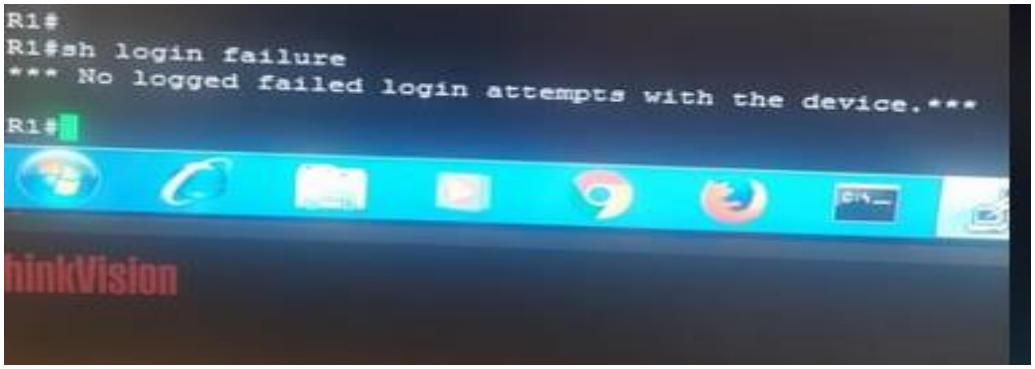


Figure 5 : Affichage des login échoués.

ANNEXE D

Packet tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau.

L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique).

Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc .[8]

1)Description générale :

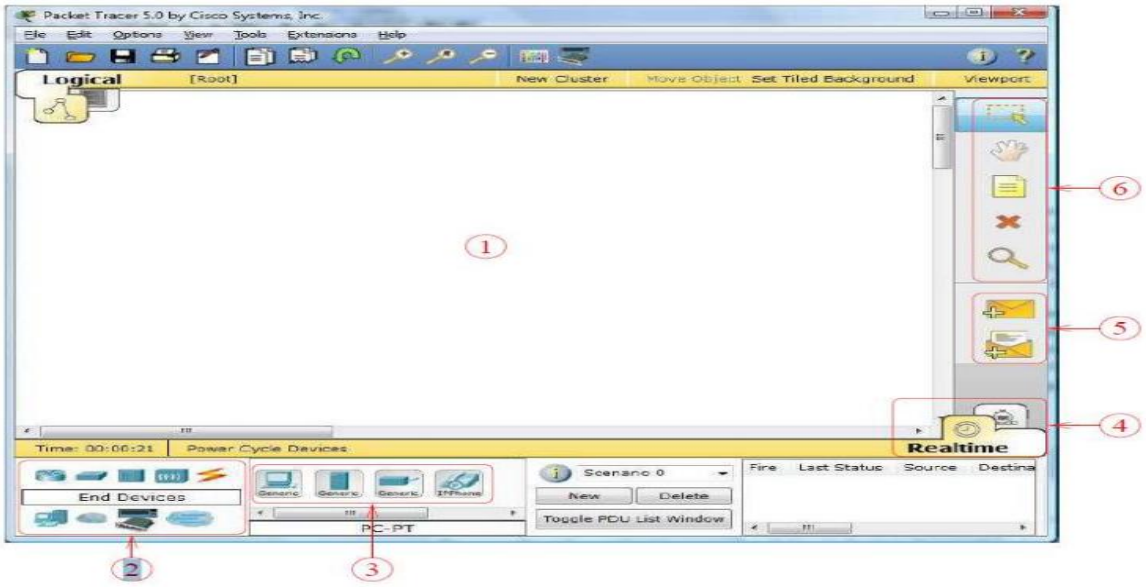


Figure1 : Interface de packet tracer.

La figure 1 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2).

Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils :

- **Select** : pour déplacer ou éditer des équipements
- **Move Layout** : permet de déplacer le plan de travail
- **Place Note** : place des notes sur le réseau
- **Delete** : supprime un équipement ou une note
- **Inspect** : permet d'ouvrir une fenêtre d'inspection sur un équipement (table

ARP, routage)

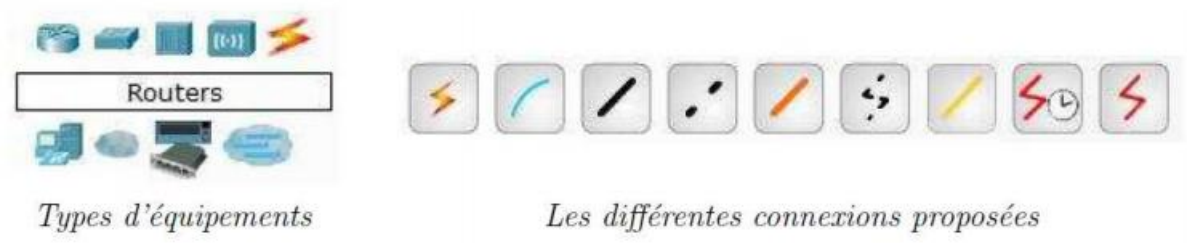
La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4)

permet de passer du mode temps réel au mode simulation.

2) Construire un réseau :

[8] **https://www.i3s.unice.fr/map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf**

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi-utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi.



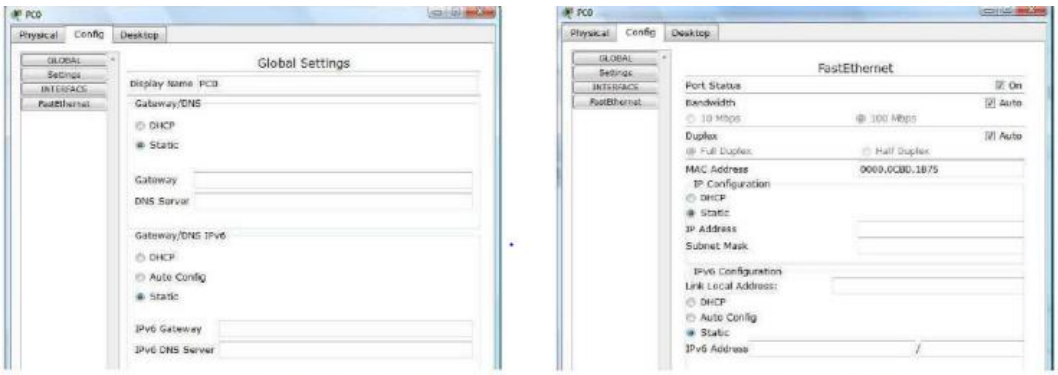
Types d'équipements *Les différentes connexions proposées*

Figure 2 : Boutons équipements et câblages.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée. Dans nos différents travaux pratiques, nous n'utiliserons que 2 sortes de connexions : les câbles droits (Copper StraightThrough) et les câbles croisés (Copper Cross-Over). Ils sont en position 3 et 4 sur la partie droite de la figure 2.

3) Configuration d'un équipement :

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web). Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet endessous du bouton INTERFACE.



Configuration passerelle et DNS *Configuration IP*

Figure 3 : Configuration d'un hôte.

4) Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure 4 montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici HTTP).

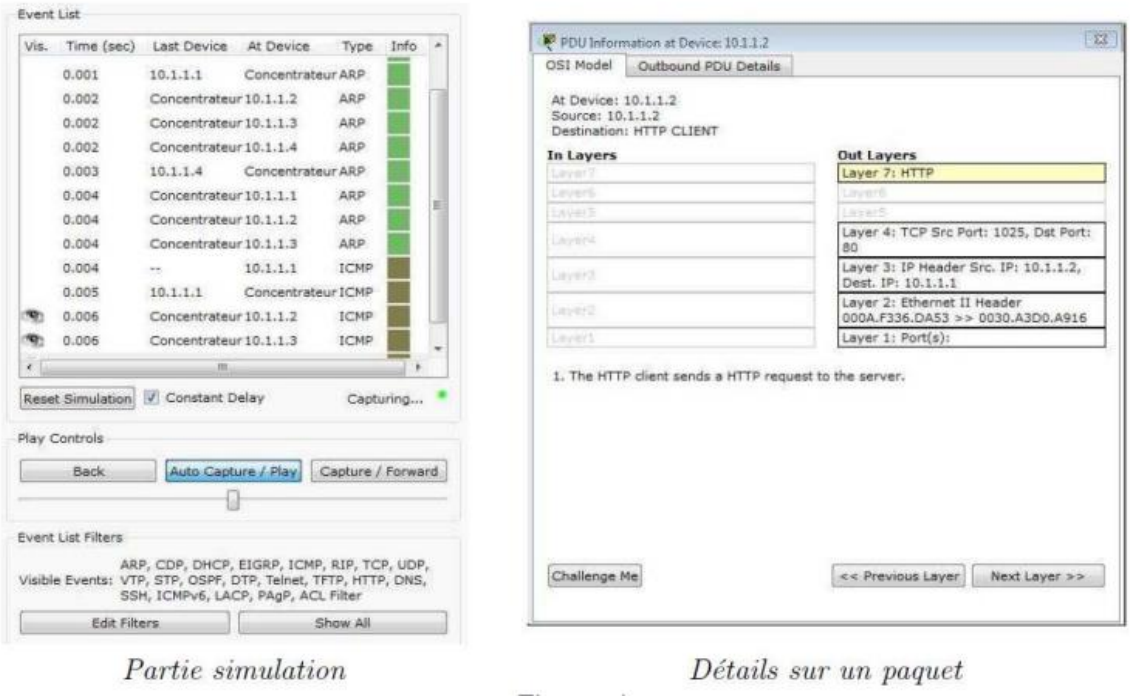


Figure 4 : Capture du trafic.

5)Invite de commandes :

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser). L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

ANNEXE E

Les logiciels de contrôle des réseaux

La surveillance du fonctionnement du réseau fournit à un administrateur réseau les informations nécessaire à la gestion proactive du réseau et à l'établissement de rapports relatifs au statistique d'utilisation du réseau.

L'activité des liaisons, les taux d'erreur et l'état de liaisons sont quelques-uns des facteurs qui permettent à un administrateur réseaux de déterminer l'état et l'utilisation d'un réseau.

La collecte et l'analyse d ces informations au fil du temps permettent à un administrateur réseaux d'observer la croissance du réseau et de détecter et remplacer un élément défaillant avant qu'il ne soit complétement inopérant.

01. syslog [9]

A. Définition :

Syslog est un terme utilisé pour décrire une terme, il sert également à décrire le protocole développé pour les systèmes UNIX dans les années 1980, mais a été documenté pour la première fois dans la RFC 3164 par GPI'IETF en 2001, il utilise le port UDP 514 pour envoyer des messages de notification d'événement sur des réseaux IP à des collecteurs de messages d'événement.



Figure01 : Syslog

B. Le fonctionnement du syslog :

le protocole syslog se compose d'une partie cliente et d'une partie serveur .la partie cliente émet les informations sur le réseau. via le port UDP 514. Les serveur collectent l'information et se chargent de créer les journaux.

[9] **https://www.paessler.com/it-explained/syslog**

L'intérêt de syslog est de centraliser les journaux des évènements, permettant de repérer plus rapidement et efficacement les défaillances des dispositifs présents sur un réseau.

Le service de journalisation du protocole syslog assume trois fonctions principales :

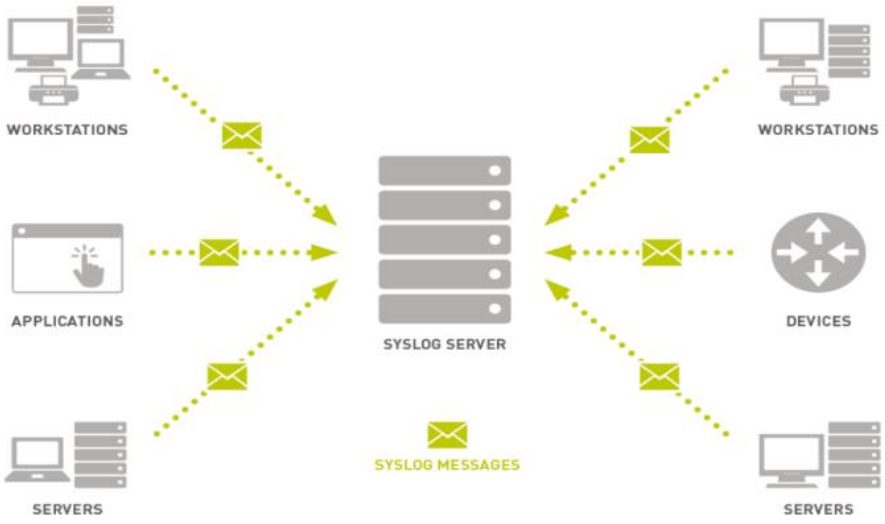
- La capacité à collecter les informations de journalisation pour la surveillance et le dépannage.
- La capacité à sélectionner le type d'information de journalisation capturée.
- La capacité à spécifie les destinations des messages syslog capturés.

02. SNMP

A. Définition SNMP[10]

SNMP (Simple Network Management Protocol) : Signifie que nous allons étudier plus en détails dans la partie suivante, a pour rôle exclusif la gestion réseau, et offre en conséquence un grand nombre d'avantages que n'ont pas les autres protocoles. SNMP propose une interface de transaction commune à tous les matériels, et donc le plus homogène possible. Son utilisation reste peu importante suite à des débuts difficiles, mais SNMP tend à devenir à terme l'une des références en matière de gestion réseau.

Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau e de faciliter l'échange d'information d'administration entre différents entités d'un réseau ainsi de détecter, diagnostiquer et résoudre les problèmes de réseau.



[10] **Définition | SNMP - Simple Network Management Protocol | Futura Tech (futura-sciences.com)**

Figure 02 : SNMP

B. Principe de fonctionnement :

Le système de gestion de réseau est basé sur deux éléments principaux :

Le superviseur : est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management.

Les agents : sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets.

Switches, hubs, routeurs et serveurs sont des exemples d'équipement contenant des objets manageable. Ces objets manageables peuvent être des informations matérielles, des paramètre de configurations, des statistique de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question.

Ses objet sont classés dans une sorte de base de données appelée MIB« Management Information Base »

SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB

03. NETFLOW

A. **Définition :** est une technologie Cisco IOS qui fournit des statistiques sur les paquets traversant un routeur ou un commutateur multicouche Cisco, Net Flow est la norme pour la collecte de données opérationnelles IP à partir de réseau IP [11]

Historiquement, la technologie Net Flow a été développée parce que les professionnels des réseaux avaient besoin d'une méthode efficace permettant d'assurer le suivi des flux TCP/IP

Au sein du réseau et que le protocole SNMP tente d'offrir une très large gamme de fonctionnalités et d'options de gestion du réseau, Net Flow se concentre sur la fourniture de statistique relatives aux paquets IP circulant entre les périphériques réseaux.

NetFlow fournit des données permettant la surveillance du réseau et de la sécurité, la planification réseau, l'analyse du trafic destinée à identifier les goulots d'étranglements du réseau ainsi que la comptabilité IP à des fins de facturation .

[11] **https://www.solarwinds.com/fr/netflow-traffic-analyzer/use-cases/what-is-netflow**

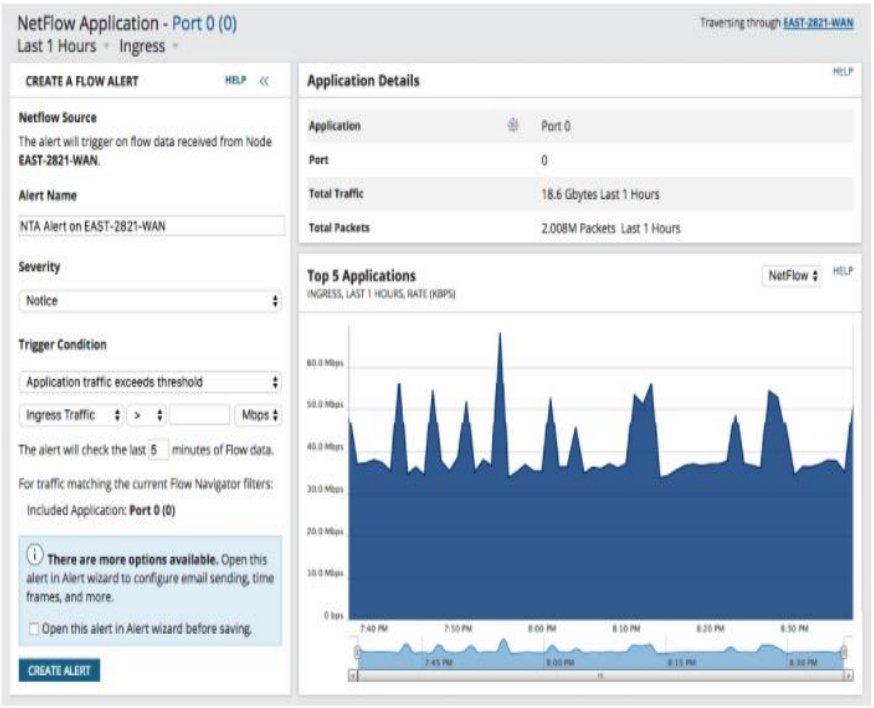


Figure 03 : NETFLOW