REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIR

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par

- **HAMDOUD Med Amine**
- **HAMADACHE Hichem**

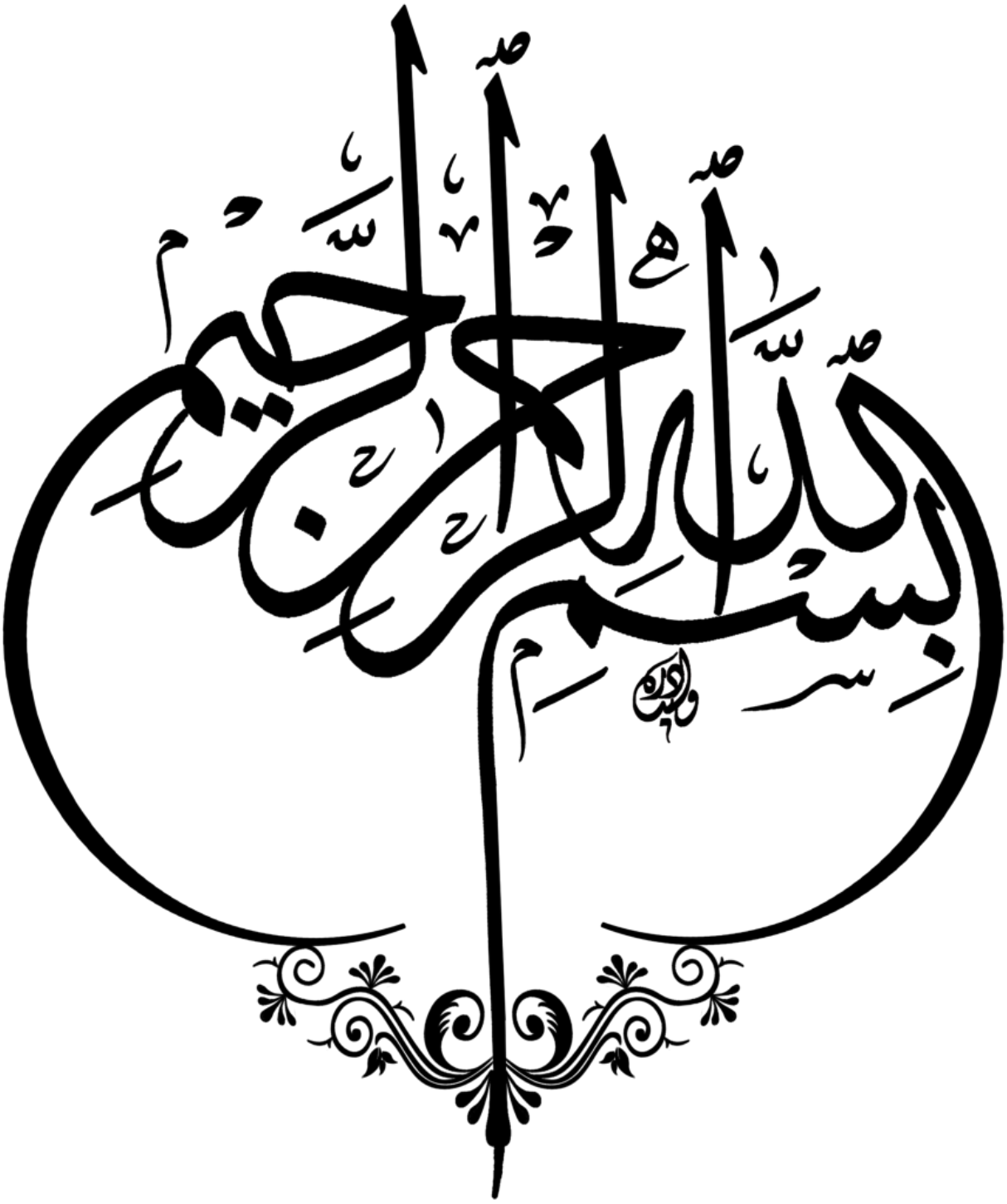
Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Mise en œuvre de la sécurité d'un réseaux WAN par des exigences de sécurité : Pare-feu ASA, VPN ...

HAMADACHE	M'Hamed	Professeur	UMBB	Président
MECHID	Samira	MAA	UMBB	Examinateur
RIAHLA	Med Amine	MCA	UMBB	Rapporteur

Année Universitaire : 2020/2021


بسم الله الرحمن الرحيم

Remerciements :

« Louange à DIEU, le seul et unique »

*Au nom de **Allah** le Miséricordieux, Nous remercions d'abord **Dieu** le tout Puissant pour Sa faveur imméritée, Son amour, Son assistance, Sa grâce, pour la santé et l'intelligence, la force et le courage, Lui grâce à qui j'ai pu surmonter toutes les difficultés rencontrées au long de cette période pour mener bien d'accomplir ce modeste travail.*

*Avant tout je tiens à remercier Mon cher père **HAMDOUD Mohamed** et à Ma chère mère **MESSAOUD NACER Dahbia (Meriem)**, eux qui n'ont jamais cessé de me soutenir, grâce à qui je ne baisserai jamais les bras. Vos prières et vos bénédictions m'ont été d'un grand soutien pour mener à bien mes études.*

Notre profonde *gratitude s'adresse à mon promoteur* académique, *Monsieur **Riahla Mohamed Amine** Docteur de l'université de Limoges/France, enseignant chercheur à l'université UMBB en réseaux et sécurité informatique et Expert consultant en TIC. Pour son encadrement, son orientation, ses conseils, pour la confiance, la patience, et la disponibilité qu'il nous a témoignée pour nous permettre de mener à bien ce travail. Merci également à lui pour ses efforts consentis pour la réussite de notre cursus scolaire. Nous avons admiré sa disponibilité malgré ses nombreuses occupations. Qu'il trouve dans ce travail un hommage vivant à sa haute personnalité ;*

Je tiens à remercier profondément mon encadrante professionnel, *Madame **ATBA Sara** Responsable de la Direction des Télécommunications de la direction général de la Banque Extérieure d'Algérie. Pour ses conseils intéressants, son encouragement continu, son support moral nos énormément aidé à mener à terme ce travail ainsi que fournir les conditions favorables au bon déroulement du projet, ainsi que le temps qu'il m'a réservé malgré ses grandes occupations. Et un grand merci à Monsieur **BOUTELDJA Abderahmane,** pour être toujours là pour m'écouter, m'aider, et me guider à retrouver le bon chemin par sa sagesse et ses précieux conseils, Merci pour votre dignité et votre pure gentillesse.**,** C'est avec un réel plaisir que j'ai effectué ce stage sous votre direction.*

Nous remercions ceux qui, de près ou de loin, nous ont aidés ou soutenus d'une manière ou d'une autre pour l'élaboration de ce mémoire. Notre gratitude va particulièrement à :

- *Tout le **personnel** de la BEA en particulier la Direction des Télécommunications pour leur* encouragement à faire toujours de notre mieux, *leur gentillesse et l'excellente ambiance de travail.*
- *Notre cher chef du Département du Génie électrique Monsieur **MESSAOUDI Noureddine**.*
- *Nos vifs remerciements aux membres du **jury** d'avoir accepté d'examiner et d'évaluer notre travail.*
- C'est l'occasion de remercier tous les **enseignants** qui on laissez leur positive touche dans notre vie depuis les études primaires.
- Mon frère **Nassim** qui m'a sauvé avec leur Laptop quand j'ai perdu mon PC.

Enfin, Je tiens à remercier également **ma famille** et **mes amis** pour leurs aides considérables.

Dédicaces

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie à :

A la mémoire de ma grande mère MADJA qu'Allah fasse miséricorde à son âme, qu'elle ait souhaité me voir réussir mes études, qu'ALAHE l'accueille dans son vaste paradis. Tu représentes la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi. Ta prière et ta bénédiction m'ont été d'un grand secours pour mener à bien mes études. Je t'aime énormément.

Ma très chère mère *qui n'a pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude,* ***« Ce modeste travail est grâce à ta lettre que tu m'as donnée quand j'ai eu le BAC »,*** *que Dieu me la garde en très bonne santé ;*

Mon très cher père *qui malgré les difficultés de la vie s'est engagé corps et âme dans mon éducation. Que Dieu me les garde en très bonne santé ;*

Aucune dédicace ne pourra compenser les sacrifices de mes parents ;

Mon adorable petite sœur Khadija *qui sait toujours comment procurer la joie et le bonheur pour toute la famille.*

Ma chère tante Thoria *qui n'a pas cessé de m'encourager et soutenir tout au long de mes études, Que Dieu la protège et leur offre la chance et le bonheur.*

Mes frères HAMDOUD Nassim et Sid Ahmed*.*

Chères amis Ahmed et Walid.

Toute ma famille et à tous mes amis qui mon aidé de près ou de loin durant toute ma vie.

L'ensemble de mes enseignants qui m'ont nourri de leurs savoirs et de leurs expériences.

A tous ceux qui m'ont encouragé, je ne saurais citer tous les noms de peur d'en oublier, mais

Je vous remercie du fond du cœur.

Table des matières

Chapitre 2 : sécurité des réseaux

Chapitre 3 : Généralité sur les VPN

Chapitre 4 : Les firewalls

Chapitre 5 : Le pare-feu ASA 5505

Partie II : Contribution

Chapitre 6: Analyse de l'existant

Chapitre 7 : Réalisation et Mise en place des solutions de sécurité

LA 1er ETAPE

Liste des figures

Liste des tableaux

Glossaire des abréviations

Abréviations	*Significations*
AAA	Authentication, Authorization, Accounting
ACK	Acknowledgement « accusé de réception »
ACL	Access Control List « liste de contrôle d'accès »
AES	Advanced Encryption Standard « norme de chiffrement avancé »
AH	Authentication Header
AH	Application Header
AIM	Association Information et Management
AIP	Advanced Inspection and Prevention
AND	le ET logique
ANSI	American National Standards Institute
AOL	American Online Lunches
APWG	L'Anti-Phishing Working Group
ARPANET	Advanced Research Projects Agency Network
ASA	Adaptive Security Appliances
AVC	Application Visibility and Control
BAC	Baccalauréat
BCV	Business Copy Volume
BEA	Banque Extérieure d'Algérie
BIAM	Banque Industrielle de l'Algérie et de la Méditerranée
BNA	Banque Nationale d'Algérie
CARP	Common Address Redundancy Protocol
CBAC	Context-based access control
CC	Coordination Center
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CID	Confidentialité, Intégrité et Disponibilité
CIPA	Children's Internet Protect Act

CLI	Command-Line Interface(interface en ligne de commande)
CMAP	Class Map
CMD	Command
CNEP	Caisse Nationale Epargne et de Prévoyance-Banque
CPA	Crédit Populaire d'Algérie
CPU	Central Processing Unit
CRL	Certificat Révocation List
CSC	Content Security and Control
CSD	Cisco Secure Desktop
CSM	Cisco Security Manager
CUCM	Cisco Unified Communications Manager
DAR	Data Access Right
DAS	Direct Attached Storage
DEC	Digital Equipment Corporation
DES	Data Encryption Algorithm
DHCP	Dynamic Host configuration Protocol
DIN	Deutsches Institut für Normung
DIT	Donné Information Transfert
DLP	Data Loss Prevention
DMZ	DeMilitarized Zone
DNA	Digital Network Architecture
DNS	Domain Name service
DOD	Department of Defense
DOS	Denial Of Service
DOS	Distributed Denial Of Service
DPI	Deep Packet Inspection
DRBD	Distributed Replicated Block Device
DVBRCS	Digital Video Broadcast - Return Channel System
ESP	Encapsulating Security Payload
FAI	Fournisseur d'Accès à Internet
FDDI	Fiber Distributed Data Interface
FR	France

GAB	Guichet Automatique Bancaire
GAP	Guichet Automatique Bancaire
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IDS	Intrusion detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IPX	Internetwork Packet Exchange
ISA	Industrial Security Appliance
ISAKMP	Internet Security Association and Key Management Protocol
ISKAMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ISP	Internet service provider
JVM	Java virtual machine
LAC	L2TP Access Concentrator
LCP	Link Contrôle Protocole
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LNS	L2TP Network Server
MAC	Media Access Control
MAN	Metropolitan Area Network
MAPI	Messaging Application Programming Interface

MID	Medium Dependent Interface
MIDX	Medium Dependent Interface Crossover
MITM	Man In The Middle
MPLS	Multiprotocol Label Switching
MPPC	Microsoft Point to Point Compression
MPPE	Microsoft Point to Point Encryption
MTA	Metropolitan Transportation Authority
MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NCP	Network Control Protocol
NGFW	Next Generation Firewall
NGIPS	Nouvelle Génération Firepower
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PABX	Private Automatic Branch EXchange
PAP	Password Authentification Protocol
PAT	Port Address Translation
PC	Personel computer
PCI	Peripheral Component Interconnect
PDU	Peripheral Component Interconnect
PFS	Perfect Forward Secrecy
PIX	Private Internet Exchange
POE	Power over Ethernet
PPP	protocole point à point
PPTP	Point-to-point tunneling protocol
PSH	Push
p0f	passive OS fingerprinting
QOS	Quality of Service
RAID	Redundant Array of Independent Disks
RDP	Remote Desktop Protocol

RED	Remote Ethernet Device
RFC	Request for comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RPV	Remote Procedure Call
RSA	Rivest–Shamir–Adleman
RST	Romance Standard Time
RTC	Reseau Telephonique Commuté
RTT	Round-Trip Delay time
RVP	Reseau Virtuel Privé
SACK	Selective Acknowledgment
SAN	Storage Area Network
SCCP	Skinny Call Control Protocol
SCP	Secure Copy Protocol
SDI	Serial Digital Interface
SEO	Search Engine Optimization
SHA	Secure Hash Algorithme
SIP	Session Initiation Protocol
SLIP	Serial Line Internet Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet eXchange
SQL	Structed Query Language
SRDF	Symmetrix Remote Data Facility
SRV	Serveur informatique
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSLVPN	Secure Socket Layer Virtual Private Network
SSO	Single Sign-On
STM	Synchronous Transport Module

SVC	Static VAR Compensator
SYN	SYNchronisation
TCP	Transmission Control Protocol
TCPIP	Transmission Control Protocol Internet Protocol
FTP	File Transfer Protocol
TFTP	Trivial File Transport Protocol
TIC	Technologies de l'Information
TLS	Transport Layer Security
TOR	The Onion Router
UDP	User datagram protocol
UMBB	Université m'hamed bougera boumerdes
URG	URGent : Pointeur de données urgentes valide
URL	Universal Serial Bus
USB	Unified Threat Management
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	virtual private network
VSAT	Very Small Aperture Terminal
VTP	Vlan trunking protocol
VTY	Virtual TeletYpe
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XML	eXtended Markup Language
XSS	Cross-Site Scripting
ZBF	Zone Based Firewall
ZBFW	Zone Based Fire wall
ZBPF	Zone Based Policy Firewalls

Résumé :

Face à l'émergence de diverses formes d'attaques informatiques aujourd'hui, le renforcement de la sécurité informatique est devenu un besoin primordial. Les entreprises, les institutions et les réseaux gouvernementaux ont plus besoin de ce type de sécurité car ils sont souvent la cible d'attaques par intrusion. Lors de notre stage effectué à la Banque Extérieure d'Algérie, nous avons étudié et mis en place des outils de sécurité informatique. Les pares-feux sont très populaires en tant qu'outils permettant de mettre en place des stratégies efficaces de sécurité des réseaux informatiques. Les pare-feux assurent la protection du réseau contre certaines intrusions externes, grâce à des techniques de filtrage rapides et intelligentes.

L'objectif de ce travail est d'étudier d'abord les concepts de la sécurité informatique en générale et en particulier les pare-feux ainsi que une généralité sur les VPNs la mise en place des exigences de sécurité dont le firewall ASA 5505 de Cisco. Ce pare-feu offre un panel de fonctionnalités avancées de type NAT, DMZ, ...etc, auquel nous avons ajouté une licence de sécurité «Une licence Security Plus » pour des fonctions de haute disponibilité et bénéficier des spécificités, des restrictions sur le VLAN. On a aussi doublé le nombre de tunnels VPN IPSec,…..etc. Le pare-feu est une solution de premier choix, mais il nécessite quand même une intervention humaine.

Abstract

Faced with the emergence of various forms of computer attacks today, the strengthening of computer security has become a primary need. Companies, institutions and government networks need this type of security most because they are often the target of intrusion attacks. During our internship at the External Bank of Algeria, we studied and implemented IT security tools. Firewalls are very popular as tools to implement effective IT network security strategies. Firewalls protect the network against certain external intrusions, thanks to fast and intelligent filtering techniques.

The objective of this work is to study first the concepts of computer security in general and in particular firewalls as well as a general on VPNs the implementation of security requirements including the Cisco ASA 5505 firewall. This firewall offers a range of advanced features such as NAT, DMZ, ...etc, to which we have added a security license «A Security Plus license» for high availability functions and benefit from specifics, restrictions on the VLAN. We also doubled the number of IPSec VPN tunnels,…. .etc. The firewall is a first choice solution, but it still requires human intervention.

Introduction générale :

I. Contexte général sur la sécurité et les télécommunications :

Parmi les éléments essentiels à l'existence humaine, le besoin de communiquer arrive juste après le besoin de survie. Le besoin de communiquer est aussi important pour nous que l'air, l'eau, la nourriture et le gîte.

Les télécommunications (abrév. fam. télécoms), sont considérées comme des technologies et techniques appliquées et non comme une science.

On entend par télécommunications toute transmission, émission et réception à distance, de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toutes natures, par fil électrique, radioélectricité, liaison optique, ou autres systèmes électromagnétiques.

I.1 TÉLÉCOMMUNICATIONS ET SCIENCES

Le domaine des télécommunications est un lieu de convergence et d'interaction entre différentes technologies et disciplines scientifiques.

Les mathématiques et plus particulièrement les mathématiques appliquées sont à la base du développement des théories du traitement du signal (modernisation des télécommunications), de la cryptologie (sécurisation des échanges), de la théorie de l'information et du numérique.

La physique a permis grâce au développement des mathématiques d'édifier la théorie de l'électromagnétisme. Sont apparus alors les premiers postes à galène, puis les tubes à vides, les semi-conducteurs et l'opto-électronique, qui sont à la base de l'électronique. L'électromagnétisme, en particulier l'étude des phénomènes de propagation, permet de modéliser la propagation des ondes à travers un canal, qu'il soit filaire (coaxial, fibre optique...) ou sans fil (propagation hertzienne). De même, l'invention du laser par les physiciens a ouvert la voie aux communications par fibres optiques modernes (prix Nobel de physique 2008).

La chimie, par le biais de l'affinement des processus chimiques, a permis de réduire le poids et d'allonger l'autonomie des batteries, autorisant l'emploi d'appareils portables de télécommunications.

L'informatique fondamentale et appliquée quant à elle a révolutionné le monde de la communication à distance par le développement des langages de programmation et des programmes informatiques (génie logiciel) associés à la microélectronique. (1)

Aujourd'hui, grâce aux réseaux, nous sommes plus connectés que jamais. Les personnes qui ont des idées peuvent instantanément communiquer avec d'autres pour les concrétiser. Les

événements et les découvertes font le tour du monde en quelques secondes. Il est possible de se connecter et de jouer avec ses amis dans le monde entier.

Donc avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

La menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace. (2)

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

II. *Problèmes de sécurités rencontrés par la BEA et la nécessité d'avoir une politique de sécurité cohérente en utilisant des mesures comme les firewalls :*

Les banques font traditionnellement face à des enjeux importants dans le domaine de la gestion de la relation clients. En vue de tirer au mieux partie des nouvelles technologies, et de sécuriser les réseaux bancaires. Elles doivent disposer d'un système d'information sécurisé à travers des équipements réseau fiable et moderne.

La sécurité des réseaux informatique est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Un seul mot " sécurité " recouvre des aspects très différents à la fois techniques, organisationnels et juridiques. La perception de la sécurité est donc un élément important à prendre en compte dans le développement des systèmes informatique, La BEA est une entreprise constituée de plusieurs sites distants permettant l'échange des données qui doit être de façon sécurisée sans qu'un intrus puisse altérer l'information interne du réseau.

D'un point de vue technique, la sécurité recouvre à la fois l'accès aux informations par les postes de travail, sur les serveurs ainsi que sur le réseau de transport des données. Dans ce projet il est question d'administrer et sécuriser le réseau de la Banque Extérieure d'Algérie BEA.

III. *L'objectif De Notre Travail*

Ce mémoire englobera plusieurs étapes. Nous les développons dans différents chapitres ou nous essayons de toucher le côté administration et sécurité du réseau de la Banque Extérieure d'Algérie. Dans la Partie II : Contribution, Nous allons dans une première étape présenter le réseau existant de la banque, l'architecture, la topologie, ainsi que les protocoles utilisés. Dans une seconde étape, nous allons nous concentrer sur les la sécurité utilisée par la BEA de leur configuration pour ensuite appliquer des règles de sécurité réseau avec Cisco ASA 5505 et l'implémentation d'un tunnel VPN Site to Site. La dernière étape consiste à proposer des solutions adéquates aux problèmes détectées au sein du réseau de la BEA afin de maintenir les performances du réseau de la banque.

Partie I : Etat de l’art.

Chapitre 1 : Généralités sur les réseaux de communication

I. Introduction :

Dans ce chapitre ont va discuter des réseaux informatique on va voir leurs définitions ;classifications ;avantages ; ainsi que le modèle OSI et le model TCP/IP avec une explication de chaque couche on va voir aussi les protocoles TCP et UDP et on dernier les équipements d'interconnexion .

II. Définition des réseaux informatiques :

Un réseau informatique est un ensemble d'équipements reliés entre eux afin d'assurer la communication et l'échange des informations sous forme de données numériques.

Par analogie avec un nœud qui est l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un Ordinateur, Routeur, Concentrateur ou Commutateur).

III. Avantages d'un réseau informatique :

- Le partage de ressources (fichiers, Multimédia, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Les jeux vidéo multi-joueurs

III.1 Les différents types de réseaux :

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On utilise généralement trois catégories de réseaux :

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

III.1.1 Les LANs (Local Area Network) :

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ‘’Fiber Distributed Data Interface’’ ou Gigabit Ethernet par exemple).

Il est possible de distinguer deux modes de fonctionnement dans les réseaux LAN :

- dans un environnement "d’égal à égal" (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur à un rôle similaire

- dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseau aux Utilisateurs

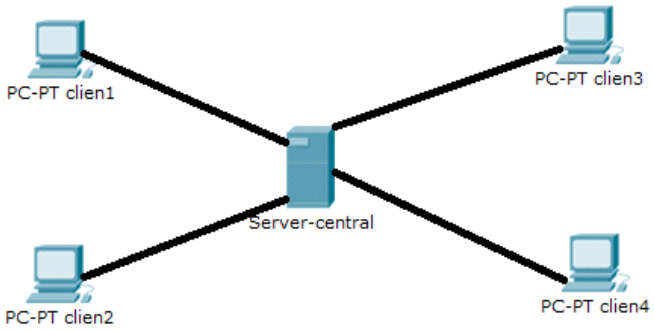


Figure III-1: Les réseaux LAN

III.1.2 Les MAN :

Les MAN (Métropolitaine Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.

Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient

partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

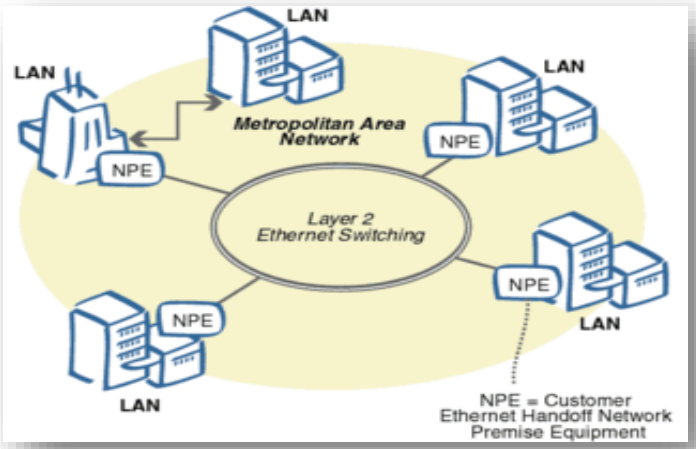


Figure III-2: Les réseaux MAN

III.1.3 Les WAN :

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LAN à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet.

Figure III-3: Les réseaux WAN

IV. Modèle OSI: (3)

Les constructeurs informatiques ont proposé des architectures réseaux propres à leurs équipements. Par exemple, IBM a proposé SNA, DEC a proposé DNA… Ces architectures ont toutes le même défaut : du fait de leur caractère propriétaire, il n'est pas facile des les interconnecter, à moins d'un accord entre constructeurs. Aussi, pour éviter la multiplication des solutions d'interconnexion d'architectures hétérogènes, l'ISO (International Standards Organisation), organisme dépendant de l'ONU et composé de 140 organismes nationaux de normalisation, a développé un modèle de référence appelé modèle OSI (Open Systems Interconnection). Ce modèle décrit les concepts utilisés et la démarche suivie pour normaliser l'interconnexion de systèmes ouverts (un réseau est composé de systèmes ouverts lorsque la modification, l'adjonction ou la suppression d'un de ces systèmes ne modifie pas le comportement global du réseau).

Au moment de la conception de ce modèle, la prise en compte de l'hétérogénéité des équipements était fondamentale. En effet, ce modèle devait permettre l'interconnexion avec des systèmes hétérogènes pour des raisons historiques et économiques. Il ne devait en outre pas favoriser un fournisseur particulier. Enfin, il devait permettre de s'adapter à l'évolution des flux d'informations à traiter sans remettre en cause les investissements antérieurs. Cette prise en compte de l'hétérogénéité nécessite donc l'adoption de règles communes de communication et de coopération entre les équipements, c'est à dire que ce modèle devait logiquement mener à une normalisation internationale des protocoles.

Le modèle OSI n'est pas une véritable architecture de réseau, car il ne précise pas réellement les services et les protocoles à utiliser pour chaque couche. Il décrit plutôt ce que doivent faire les couches. Néanmoins, l'ISO a écrit ses propres normes pour chaque couche

Les premiers travaux portant sur le modèle OSI datent de 1977. Ils ont été basés sur l'expérience acquise en matière de grands réseaux et de réseaux privés plus petits ; le modèle devait en effet être valable pour tous les types de réseaux. En 1978, l'ISO propose ce modèle sous la norme ISO IS7498. En 1984, 12 constructeurs européens, rejoints en 1985 par les grands constructeurs américains, adoptent le standard.

IV.1 Les différentes couches du modèle OSI

IV.1.1 Les 7 couches :

Le modèle OSI comporte 7 couches :

Les principes qui ont conduit à ces 7 couches sont les suivants :

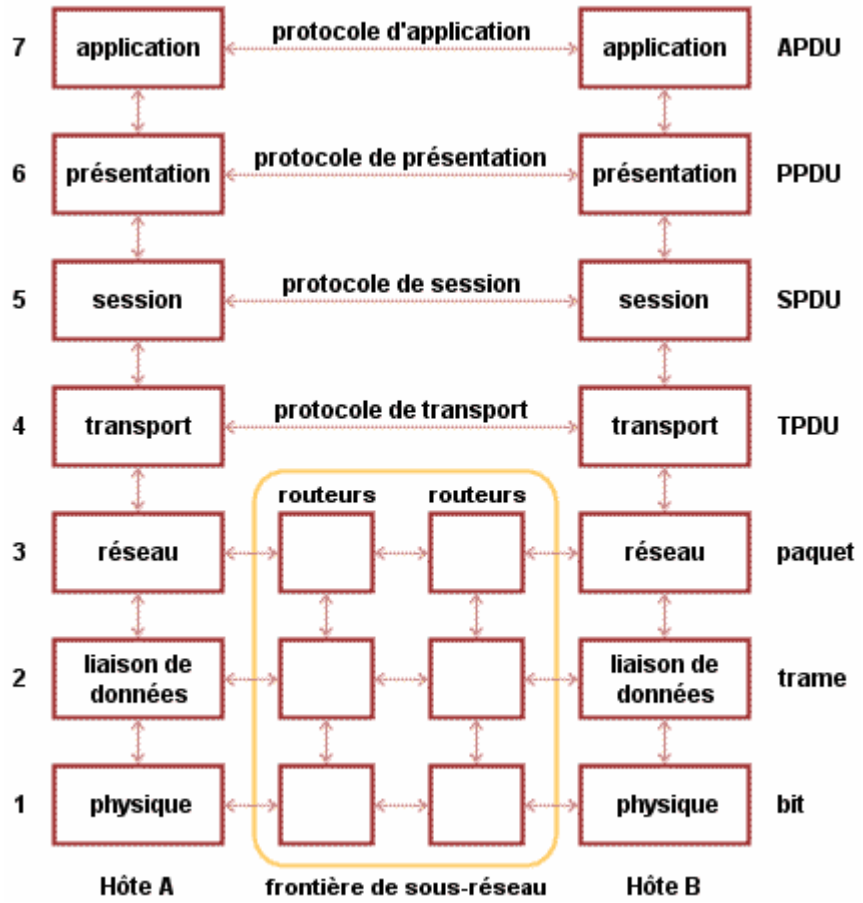


Figure IV-1: Schéma explicatif du 7 couches de modèle

Une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire, chaque couche a des fonctions bien définies, les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles, les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces, le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

IV.1.2 La couche physique :

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les

caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie…), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

IV.1.3 La couche liaison de données :

Son rôle est un rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d'octets maximum.

IV.1.4 La couche réseau

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques…).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.

L'unité d'information de la couche réseau est le paquet.

IV.1.5 La couche transport :

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois… Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau.

Un des tout derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.

L'unité d'information de la couche transport est le message.

IV.1.6 La couche session :

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle…). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

IV.1.7 La couche présentation :

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

IV.1.8 La couche application :

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie…

IV.2 Transmission de données au travers du modèle OSI :

Le processus émetteur remet les données à envoyer au processus récepteur à la couche application qui leur ajoute un entête application AH (éventuellement nul). Le résultat est alors transmis à la couche présentation.

La couche présentation transforme alors ce message et lui ajoute (ou non) un nouvel entête (éventuellement nul). La couche présentation ne connaît et ne doit pas connaître l'existence éventuelle de AH ; pour la couche présentation, AH fait en fait partie des données utilisateur. Une fois le traitement terminé, la couche présentation envoie le nouveau « message » à la couche session et le même processus recommence.

Les données atteignent alors la couche physique qui va effectivement transmettre les données au destinataire. A la réception, le message va remonter les couches et les entêtes sont progressivement retirés jusqu'à atteindre le processus récepteur :

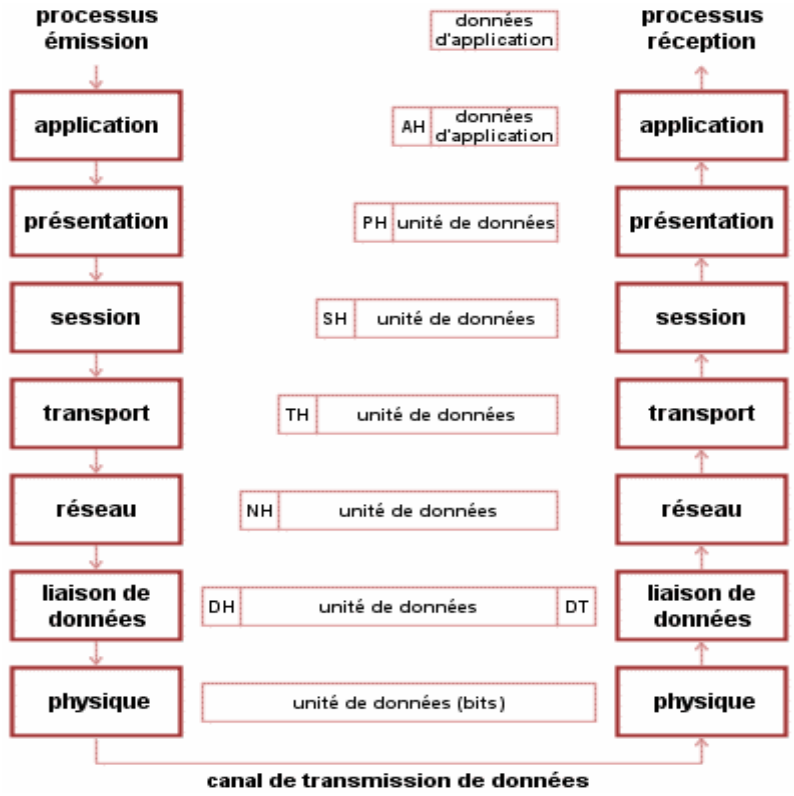


Figure IV-2: Encapsulation OSI

V. le modele TCP/IP :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise « par-dessus » un protocole réseau, IP (Internet Protocol). Ce qu'on entend par « modèle TCPIP », c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante.

Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

L'origine du modèle TCPIP remonte au réseau ARPANET. ARPANET est un réseau de télécommunication conçu par l'ARPA (Advanced Research Projects Agency), l'agence de recherche du ministère américain de la défense (le DOD : Department of Defense). Outre la possibilité de connecter des réseaux hétérogènes, ce réseau devait résister à une éventuelle guerre nucléaire, contrairement au réseau téléphonique habituellement utilisé pour les télécommunications mais considéré trop vulnérable. Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergeante promettante. C'est donc dans cet objectif et ce choix technique que les protocoles TCP et IP furent inventés en 1974.

V.1 Description du modèle TCP/IP :

V.1.1 TCP/IP, un modèle en 4 couches :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

V.1.1.1 La couche hôte réseau :

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau.

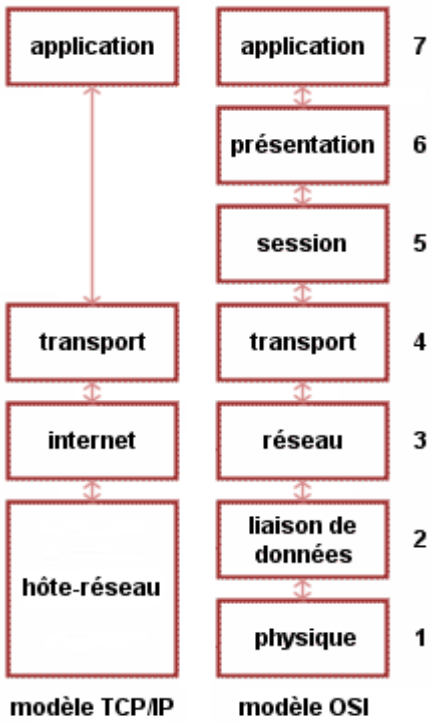


Figure V-1:Comparaison entre les couches des deux modèles.

V.1.1.2 La couche internet :

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique

de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI.

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

Remarquons que le nom de la couche (« internet ») est écrit avec un i minuscule, pour la simple et bonne raison que le mot internet est pris ici au sens large (littéralement, « interconnexion de réseaux »), même si l'Internet (avec un grand I) utilise cette couche.

V.1.1.3 La couche transport :

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là une avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

V.1.1.4 La couche application :

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent

intégralement et sans erreurs.Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

VI. Le protocole UDP :

Le protocole UDP est basé en couche 4 du modèle OSI. Il n'ouvre pas de session et n'effectue pas de control d'erreur. Il est alors appelé « mode non connecté ». Il est donc peu fiable, cependant, il permet aux applications d'accéder directement à un service de transmission de Datagrammes rapide.

UDP est utilisé pour transmettre de faibles quantités de données où le coût de la création de connexions et du maintient de transmissions fiables s'avèrent supérieur aux données à émettre. UDP peut également être utilisé pour les applications satisfaisant à un modèle de type « interrogation réponse ». La réponse étant utilisée comme un accusé de réception à l'interrogation. On y trouve classiquement les protocoles SNMP et DNS. UDP est aussi utilisé dans un second cas, tel que la voix sur IP. L'envoi en temps réel est primordiale, donc si une trame n'arrivait pas, la retransmission serait inutile.

VI.1 Structure de l'entête UDP :

Voici la structure de l'entête UDP basé sur 8 octets :

VI.2 Définition des différents champs

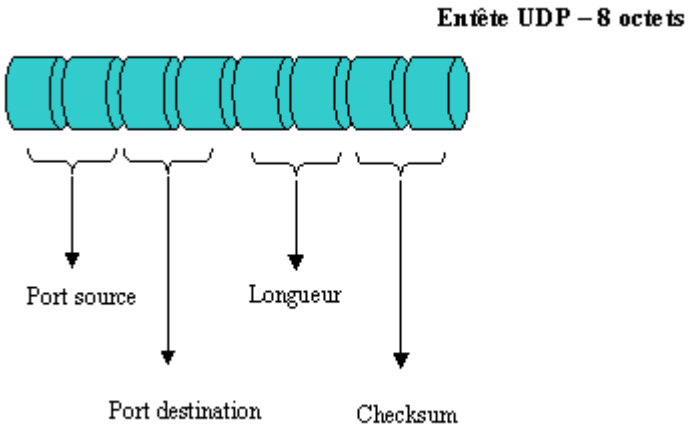


Figure VI-1:La structure de l'entête UDP basé sur 8 octets.

VI.2.1 Port source UDP :

Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.

VI.2.2 Port destination UDP :

Le champ Port destination est codé sur 16 bits et il correspond au port relatif à l'application en cours sur la machine de destination.

Vous trouverez la liste des ports TCP officialisées par l'IANA, organisation gérant mondialement les adressage IP.

VI.2.3 Longueur :

Le champ Longueur est codé sur 16 bits et il représente la taille de l'entête et des données. Son unité est l'octet et sa valeur maximale est 64 Koctets (216).

VI.2.4 Checksum :

Le champ Checksum est codé sur 16 bits et représente la validité du paquet de la couche 4.

Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des

compléments à 1 des octets de l'entête et des données pris deux par deux (mots de 16 bits). Si le message entier contient un nombre impair d'octets, un 0 est ajouté à la fin du message pour terminer le calcul du Checksum. Cet octet supplémentaire n'est pas transmis. Lors du calcul du Checksum, les positions des bits attribués à celui-ci sont marquées à 0.

Le Checksum couvre de plus, une pseudo entête de 96 bits préfixée à l'entête UDP. Cette pseudo entête comporte les adresses Internet source et destinataires, le type de protocole et la longueur du message UDP. Ceci protège UDP contre les erreurs de routage.

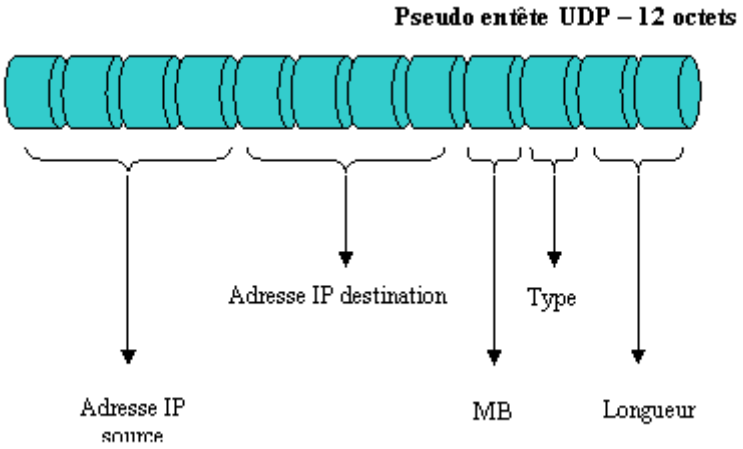


Figure VI-2: La structure de l'entête pseudo entête UDP basé sur 12 octets

VII. Le protocole TCP :

Le protocole TCP est basé en couche 4 du modèle OSI. Il ouvre une session et effectue lui-même le control d'erreur. Il est alors appelé « mode connecté ». Vous trouverez tous les détails du protocole TCP dans la RFC 793.

VII.1 Structure de l'entête TCP :

Voici la structure de l'entête TCP basé sur 20 octets:

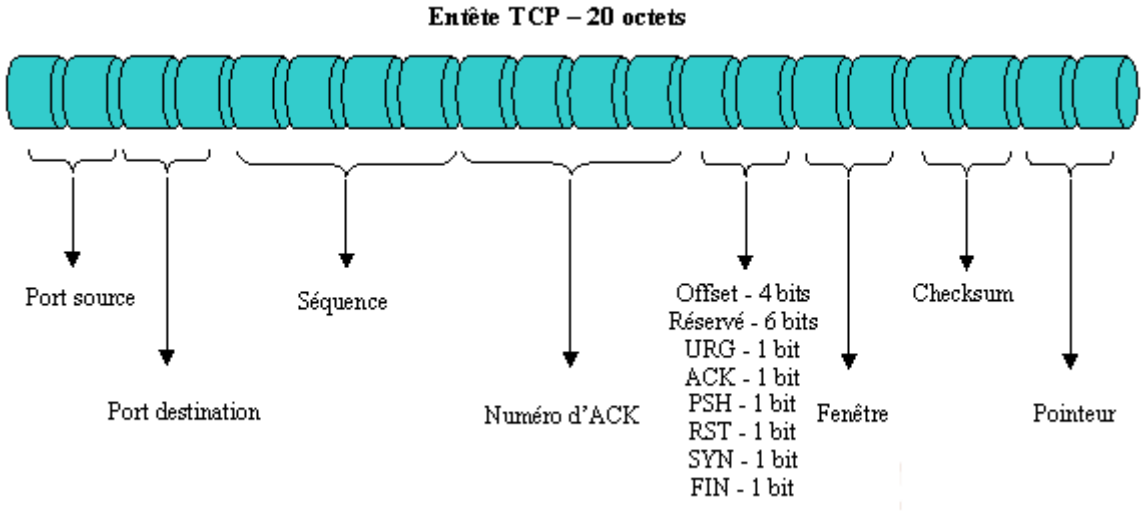


Figure VII-1: La structure de l'entête TCP basé sur 20 octets.

Voici le complément de l'entête TCP qui est optionnelle basé sur 4 octets.

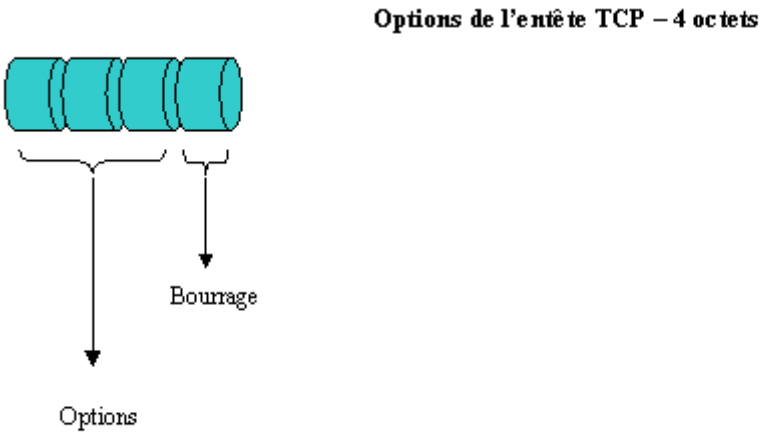


Figure VII-2: Le complément optionnelle de l'entête TCP basé sur 4 octets.

VII.2 Mode de transfert TCP

Voici les différents types de communication basés sur le mode connecté de TCP :

VII.2.1 Ouverture de session :

==> SYN=1 – ACK=0 – SeqNum=100 – AckNum=xxx

<== SYN=1 – ACK=1 – SeqNum=300 – AckNum=101

==> SYN=0 – ACK=1 – SeqNum=101 – AckNum=301

VII.2.2 Transfert des données :

==> ACK=1 – SeqNum=101 – AckNum=301 – Data=30 octets

<== ACK=1 – SeqNum=301 – AckNum=131 – Data=10 octets

==> ACK=1 – SeqNum=131 – AckNum=311 – Data=5 octets

<== ACK=1 – SeqNum=311 – AckNum=136 – Data=10 octets

VII.2.3 Fermeture de session :

==> ACK=1 – FIN=1 – SeqNum=321 – AckNum=136

<== ACK=1 – FIN=0 – SeqNum=136 – AckNum=321

Puis le receveur de la demande de fermeture de session demande à son tour la fermeture de session :

<== ACK=1 – FIN=1 – SeqNum – AckNum

==> ACK=1 – FIN=0 – SeqNum – AckNum

VII.2.4 Fermeture brutale de connexion :

1ère cas possible :

==> ACK=1 – RST=0 – SeqNum=200 – AckNum=400

<== ACK=0 – RST=1 – SeqNum=400 – ACKNum=xxx

2nd cas possible :

<== ACK=0 – RST=0 – SeqNum=200 – Data=30 octets

==> ACK=0 – RST=1 – SeqNum=230 – Data=xxx

VII.3 La fenêtre coulissante :

La fenêtre coulissante, plus connue sous le nom de « Sliding Windows » est employée pour transférer des données entre les hôtes. La fenêtre définit le volume de données susceptibles d'être passées via une connexion TCP, avant que le récepteur n'envoie un accusé de réception. Chaque hôte comporte une fenêtre d'émission et une fenêtre de réception qu'il utilise pour bufférisier les données en continu, sans devoir attendre un accusé de réception pour chaque paquet. Cela permet au récepteur de recevoir les paquets dans le désordre et de profiter des délais d'attente pour réorganiser les paquets. La fenêtre émettrice contrôle les données émises, si elle ne reçoit pas d'accusé de réception au bout d'un certain temps, elle retransmet le paquet.

VII.3.1 Considérations sur le débit :

Le protocole TCP a été conçu pour offrir des performances optimales en présence de conditions de liaison variées et les systèmes d'exploitations comportent des améliorations telles que celles prenant en charge la RFC 1323. Le débit réel d'une liaison dépend d'un certain nombre de variables, mais les facteurs les plus importants sont les suivants :

- Vitesse de la liaison (bits par seconde pouvant être transmis)
- Retard de propagation
- Dimension de la fenêtre (quantité de données n'ayant pas fait l'objet d'un accusé de réception et qui peuvent être en attente sur une connexion TCP)
- Fiabilité de la liaison
- Encombrement du réseau et des périphériques intermédiaires
- MTU du parcours

Voici quelques considérations fondamentales sur le calcul du débit TCP :

La capacité d'un canal de communication est égale à la bande passante multipliée par le temps de transmission aller-retour. Elle est connue sous le nom de produit bande passante-retard. Si la liaison est fiable, pour obtenir des performances optimales, la dimension de la fenêtre doit être supérieure ou égale à la capacité du canal de communication, de manière à permettre à la pile d'envoi de le remplir. La plus grande dimension de fenêtre pouvant être spécifiée, en raison du champ de 16 bits de l'entête TCP, est de 65535. Des fenêtres plus larges peuvent toutefois être négociées grâce au redimensionnement des fenêtres.

Le débit ne peut jamais excéder la taille de la fenêtre divisée par le temps de transmission aller-retour. Si la liaison n'est pas fiable ou est encombrée et que des paquets sont perdus, l'utilisation fenêtre de taille supérieure ne garantit pas nécessairement un meilleur débit. Windows 2000 prend en charge non seulement le dimensionnement des fenêtres, mais également les accusés de réception sélectifs (SACK, décrits dans la RFC 2018) pour améliorer les performances au sein d'environnements qui présentent des pertes de paquets. Il prend également en charge l'horodatage (décrit dans la RFC 1323) pour une meilleure évaluation RTT.

Le retard de propagation dépend de la vitesse de la lumière, des latences de l'équipement de transmission, etc. Le retard de transmission dépend donc de la vitesse du support.

Pour un parcours spécifique, le retard de propagation est fixe, mais le retard de transmission dépend de la taille du paquet. À des vitesses réduites, le retard de transmission constitue un facteur limitatif. À des vitesses élevées, le retard de propagation peut devenir un facteur de limitation.

En résumé, les piles TCP/IP peuvent s'adapter à la plupart des conditions de réseau et fournir dynamiquement le meilleur débit et la meilleure fiabilité possibles pour chaque connexion. Les essais de mise au point manuelle sont souvent contre-productifs, sauf lorsqu'un ingénieur réseau qualifié procède préalablement à une étude précise du flux de données.

VII.4 Définition des différents champs :

VII.4.1 Port source TCP :

Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.

VII.4.2 Port destination TCP :

Le champ Port destination est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine de destination.

Vous trouverez la liste des ports TCP officialisées par l'IANA, organisation gérant mondialement les adressage IP.

VII.4.3 Numéro de séquence :

Le champ Numéro de séquence est codé sur 32 bits et correspond au numéro du paquet. Cette valeur permet de situer à quel endroit du flux de données le paquet, qui est arrivé, doit se situer par rapport aux autres paquets.

VII.4.4 Numéro de l'accusé de réception :

Le champ Numéro de séquence est codé sur 32 bits et définit un acquittement pour les paquets reçus. Cette valeur signale le prochain numéro de paquet attendu. Par exemple, si il vaut 1500, cela signifie que tous les Datagrammes <1500 ont été reçus

VII.4.5 Offset :

Le champ Offset est codé sur 4 bits et définit le nombre de mots de 32 bits dans l'entête TCP. Ce champ indique donc où les données commencent.

VII.4.6 Réservé :

Le champ Réservé est codé sur 6 bits et il servira pour des besoins futurs. Ce champ doit être marqué à 0. Au jour d'aujourd'hui, on peut considérer que les besoins futurs se transforment en un champ non utilisé.

3 bits – Réservé

1 bit – ECN/NS

1 bit – CWR

1 bit – ECE

VII.4.7 Flags :

Voici la liste des flags :

- Le champ URG est codé sur 1 bit et indique que le champ Pointeur de donnée urgente est utilisé.
- Le champ ACK est codé sur 1 bit et indique que le numéro de séquence pour les acquittements est valide.
- Le champ PSH est codé sur 1 bit et indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.
- Le champ RST est codé sur 1 bit et demande la réinitialisation de la connexion.
- Le champ SYN est codé sur 1 bit et indique la synchronisation des numéros de séquence.
- Le champ FIN est codé sur 1 bit et indique fin de transmission.

VII.4.8 Fenêtre :

Le champ Fenêtre « Windows » est codé sur 16 bits et correspond au nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir. Le destinataire ne doit donc pas envoyer les paquets après Numéro de séquence + Window.

VII.4.9 Checksum :

Le champ Checksum est codé sur 16 bits et représente la validité du paquet de la couche 4 TCP.

Le Checksum est constitué en calculant le complément à 1 sur 16 bits de la somme des compléments à 1 des octets de l'entête et des données pris deux par deux (mots de 16 bits). Si le message entier contient un nombre impair d'octets, un 0 est ajouté à la fin du message pour terminer le calcul du Checksum. Cet octet supplémentaire n'est pas transmis. Lors du calcul du Checksum, les positions des bits attribués à celui-ci sont marquées à 0.

Le Checksum couvre de plus, une pseudo entête de 96 bits préfixée à l'entête TCP. Cette

pseudo entête comporte les adresses Internet sources et destinataires, le type de protocole et la longueur du message TCP (incluant la data). Ceci protège TCP contre les erreurs de routage.

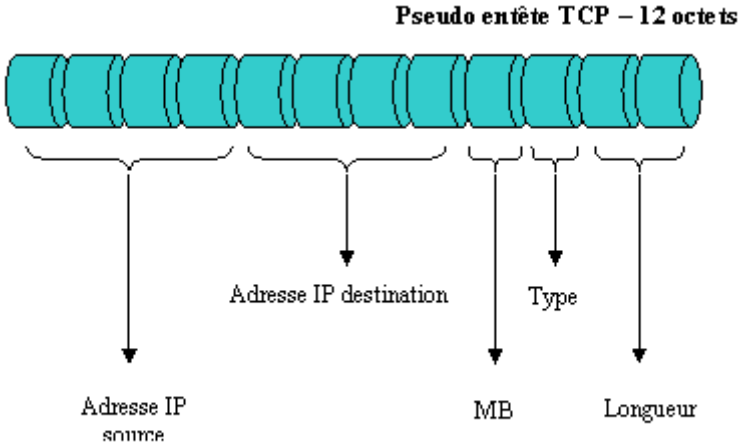


Figure VII-3: La structure de l'entête pseudo entête TCP basé sur 12 octets

La longueur TCP compte le nombre d'octets de l'entête TCP et des données du message, en excluant les 12 octets de la pseudo entête.

VII.4.10 Pointeur de donnée urgente :

Le champ Pointeur de donnée urgente est codé sur 16 bits et communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence. Le pointeur doit pointer sur l'octet suivant la donnée urgente. Ce champ n'est interprété que lorsque le Flag URG est marqué à 1. Dès que cet octet est reçu, la pile TCP doit envoyer les données à l'application.

VII.4.11 Options :

Les champs d'options peuvent occuper un espace de taille variable à la fin de l'entête TCP. Ils formeront toujours un multiple de 8 bits. Toutes les options sont prises en compte par le Checksum. Un paramètre d'option commence toujours sur un nouvel octet. Il est défini deux formats types pour les options:

Cas 1 – Option mono-octet.

Cas 2 – Octet de type d'option, octet de longueur d'option, octet de valeur d'option.

La longueur d'option prend en compte l'octet de type, l'octet de longueur lui-même et tous les octets de valeur et est exprimée en octet.

La liste d'option peut être plus courte que ce que l'offset de données pourrait le faire supposer. Un octet de remplissage « Bourrage » devra être dans ce cas rajouté après le code de fin d'options.

VII.4.12 Bourrage :

Le champ Bourrage est de taille variable comprise entre 0 et 7 bits. Il permet de combler le champ option afin d'obtenir une entête TCP multiple de 32 bits. La valeur des bits de bourrage est 0.

VIII. Les equipements d'interconnexion reseau :

VIII.1 Le modem (modulateur / démodulateur) :

Figure VIII-1: Modem (modulateur / démodulateur)

Un modem permet la transformation des signaux binaires (suite des 0 et des 1) manipulables par l'ordinateur vers des signaux analogiques indiquent également des valeurs numérique. Il sert de lien entre deux ordinateurs via la ligne téléphonique.

VIII.2 Répéteur (repeater) :

Répéteur (en anglais repeater) est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau, le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'information. D'autre part un répéteur peut permettre de constituer une interface entre deux supports physiques de type différents exemple : relier un segment de paire torsadée a un brin de fibre optique.

VIII.3 Les concentrateurs hub :

Figure VIII-2: Hub (panneaux avant)

Les Hub regroupent tous les câbles en provenance des stations des réseaux, ils sont des éléments actifs permettant de connecter un ensemble de machines sur un réseau Ethernet. Il amplifie le signal pour pouvoir le renvoyer vers tous les PC connectés ce qui augmente le trafic (broadcast).

Figure VIII-3: Hub (panneaux arrière).

Le Hub possède parfois un connecteur spécifique qui permet le branchement d'un autre Hub nécessite soit un câble croisé entre les Hub, soit un poussoir sur le Hub (MID/MIDX) qui effectue ce croisement sur un câble normal dans le connecteur approprie, c'est dans cet esprit que l'on trouve des Hub dit (empilable).Il est dans le niveau 1.

VIII.4 Les Commutateurs (Switch) :

Les Commutateurs ou Switch ont but d'interconnecter des machines en réseau. Ils ont la même apparence que les Hubs, et le même but, qui est de faire communiquer les machines entre elles mais avec un principe de fonctionnement différent.

Ils sont administrables et programmable à distance par des programmes comme TELENET ou SNMP (Simple Network Management Protocol).

Figure VIII-4: Commutateurs (Switch)

Les commutateurs fonctionnent différemment pour remédier au problème de surcharge. Les données émises par une machine ne vont pas être transmises à toutes les autre machines sur le réseau mais seulement à la machine destinatrice. La bande passante n'est donc plus partagée mais reste disponible exemple 100 Mbit/s pour chacune des machines.

VIII.5 Routeur (Router) :

Le routage c'est l'acheminement des données entre plusieurs réseaux, même si ceux-ci utilisent des protocoles de communication ou des caractéristiques de transmission différentes. Pour simplifier : il s'agit de la passerelle que l'on doit renseigner dans la configuration IP de nos cartes réseaux.
Ainsi que le routage est une tâche exécutée dans de nombreux réseaux, tels que le reseaux

téléphonique , les réseaux de données électroniques comme l'Internet , et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants.

Ce routage peut être statique ou dynamique comme il peut être direct ou indirect. Le routeur décode l'entête d'un paquet pour trouver l'adresse IP. Il travaille dans le niveau 3.

IX. Conclusion :

La sécurité informatique est un domaine très vaste qui nécessite beaucoup de prudence et de vigilance. Dans ce chapitre, nous avons présenté des généralités sur les réseaux informatiques, et on a défini les réseaux, leur rôle, leur fonctionnement et leur différent type, ainsi que les diffèrent équipements d'interconnexion réseau, Vu la fiabilité de communication qu'ils assurent, ils sont devenus aujourd'hui une nécessité dans le monde de travail.

Mais il existe beaucoup de vulnérabilités et des différentes menaces et attaques sur divers systèmes auxquelles il faut faire face en utilisant les différents outils et techniques de sécurité informatique cela nous ont ramené à parler de la nécessité de garantir certains besoins de sécurisation : tels que l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que les méthodes d'attaques et comment se protéger contre elles.

Dans le deuxième chapitre nous allons dégager quelques définitions basiques sur la sécurité, les attaques d'une part et les solutions « mesure de sécurité » contre ces dernières d'autre part.

Chapitre 2 : sécurité des réseaux

I. Introduction :

Comme des informations confidentielles circulent dans les réseaux, la sécurité des ces communications est devenue une préoccupation importante des utilisateurs et des entreprises. Ce chapitre explique ce qu'est la cybersécurité et les objectifs de la sécurité des réseaux, on parle également dans ce chapitre, des données d'entreprise et pourquoi il faut les protéger. Nous allons évoquer et définir les trois dimensions du cube maccumber. La principale responsabilité d'un administrateur de la cybersécurité est de protéger les systèmes et les données d'une entreprise, Nous allons expliquer comment es ce que chacune de ses trois dimensions apporte sa pierre à l'édifice.

Ce chapitre propose également un contenu expliquant brièvement les différents types de menace, générales, applicatives, les menaces réseaux et les menaces visant les terminaux sans fil et mobiles, attaques mixtes …, et bien sur les solutions à mener et les mesures des exigences de sécurités.

II. Definitions:

Le réseau d'information est devenu une partie intégrante de notre vie quotidienne. Les entreprises en tout genre, comme les instituts médicaux ou les établissements financiers et scolaires, utilisent ce réseau pour leur bon fonctionnement. Elles utilisent le réseau en recueillant, en traitant, en stockant et en partageant d'énormes quantités d'informations numériques. Comme de plus en plus d'informations numériques sont rassemblées et partagées, la protection de ces informations devient encore plus essentielle pour notre sécurité nationale et pour la stabilité économique.

Nos réseaux sont particulièrement difficiles à sécuriser pour différentes raisons :

- Les réseaux sont de plus en plus intégrés et complexes.
- Les réseaux sont connectés à des appareils physiques.
- Les cybercriminels peuvent accéder aux réseaux partout dans le monde.

III. Objectifs de la sécurité :

La sécurité réseaux consiste en l'effort continu pour protéger les systèmes mis en réseau et les données contre l'utilisation ou le méfait non autorisés. À titre personnel, nous devrons protéger notre identité, les données et notre périphériques informatiques. Au niveau de l'entreprise, tout le monde est responsable de la protection de la réputation, des données et des

clients de l'entreprise. Au niveau national, la sécurité nationale, ainsi que la sécurité et le bien-être des citoyens sont en jeu.

IV. Les différents types de données d'entreprise:

IV.1.1 Données traditionnelles :

Les informations de l'entreprise incluent les informations personnelles, les propriétés intellectuelles et les données financières. Les informations personnelles incluent des dossiers de candidature, des fiches de paie, des lettres d'offre, des contrats de travail et toute information utilisée dans les prises de décisions sur l'embauche. La propriété intellectuelle, comme les brevets, les marques déposées et les plans produit, permet à une entreprise d'avoir un avantage économique sur ses concurrents. Elle peut être considérée comme un secret commercial et la perdre serait désastreux pour l'avenir de l'entreprise. Les données financières, dont les comptes de résultat, les bilans comptables et les tableaux de trésorerie d'une entreprise, donnent un aperçu de la santé de l'entreprise.

IV.2 Internet des objets et Big Data :

Avec l'émergence de l'Internet des objets (IoT, Internet of Things), les données à gérer et à sécuriser sont de plus en plus nombreuses. L'IoT est un vaste réseau d'objets physiques, dont les capteurs et les équipements qui s'étendent au-delà du réseau informatique traditionnel. Toutes ces connexions, en plus du fait que nous avons des capacités et des services de stockage élargis grâce au cloud et à la virtualisation, entraînent la croissance exponentielle des données. Ces données ont créé un nouveau centre d'intérêt dans la technologie et l'entreprise. C'est ce qu'on appelle le « Big Data ». En raison de la vitesse, du volume et de la variété de données générés par l'IoT et les opérations quotidiennes de l'entreprise, la confidentialité, l'intégrité et la disponibilité de ces données sont vitales pour la survie de l'entreprise.

Figure IV-1: Services financiers big data

V. Le cube McCumber :

En 1991, John McCumber a créé un cadre modèle pour établir et évaluer la sécurité de l'information (assurance de l'information), maintenant connus sous le nom de Le cube McCumber. Ce modèle de sécurité est décrit comme un tridimensionnel Rubik's Cube comme grille. (4)

La première dimension du cube magique de la cybersécurité comprend les trois principes de la sécurité de l'information, que les professionnels de la cybersécurité désignent sous le nom de «Triade CID ». La deuxième dimension identifie les trois états des informations ou des données. La troisième dimension du cube identifie les « pouvoirs de sécurité » qui assurent la protection du cyberespace. Il s'agit, en fait, des trois catégories de protections en matière de cybersécurité.

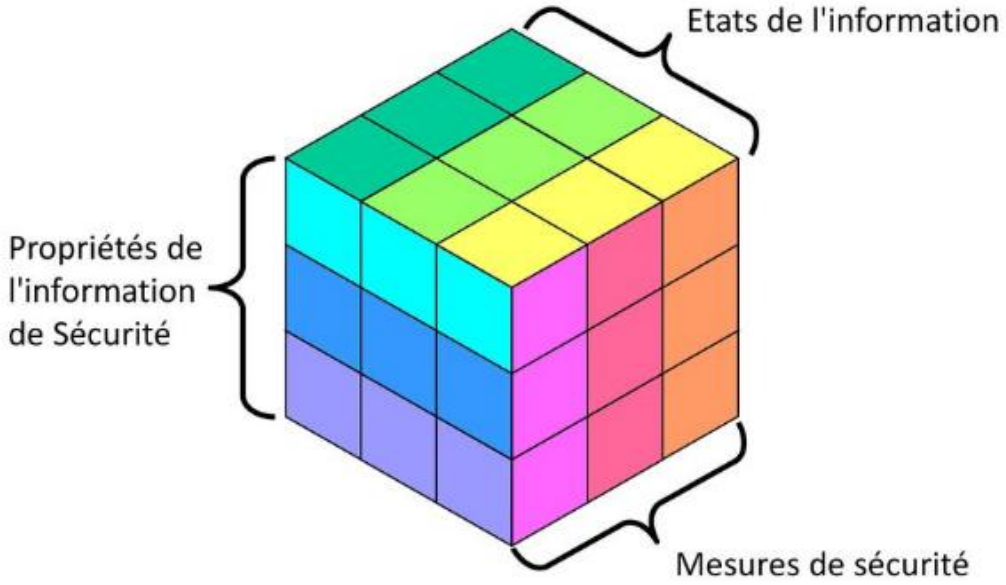


Figure V-1: Cube de mccumber.

V.1 Les principes de la sécurité « Propriétés de l'information de Sécurité » :

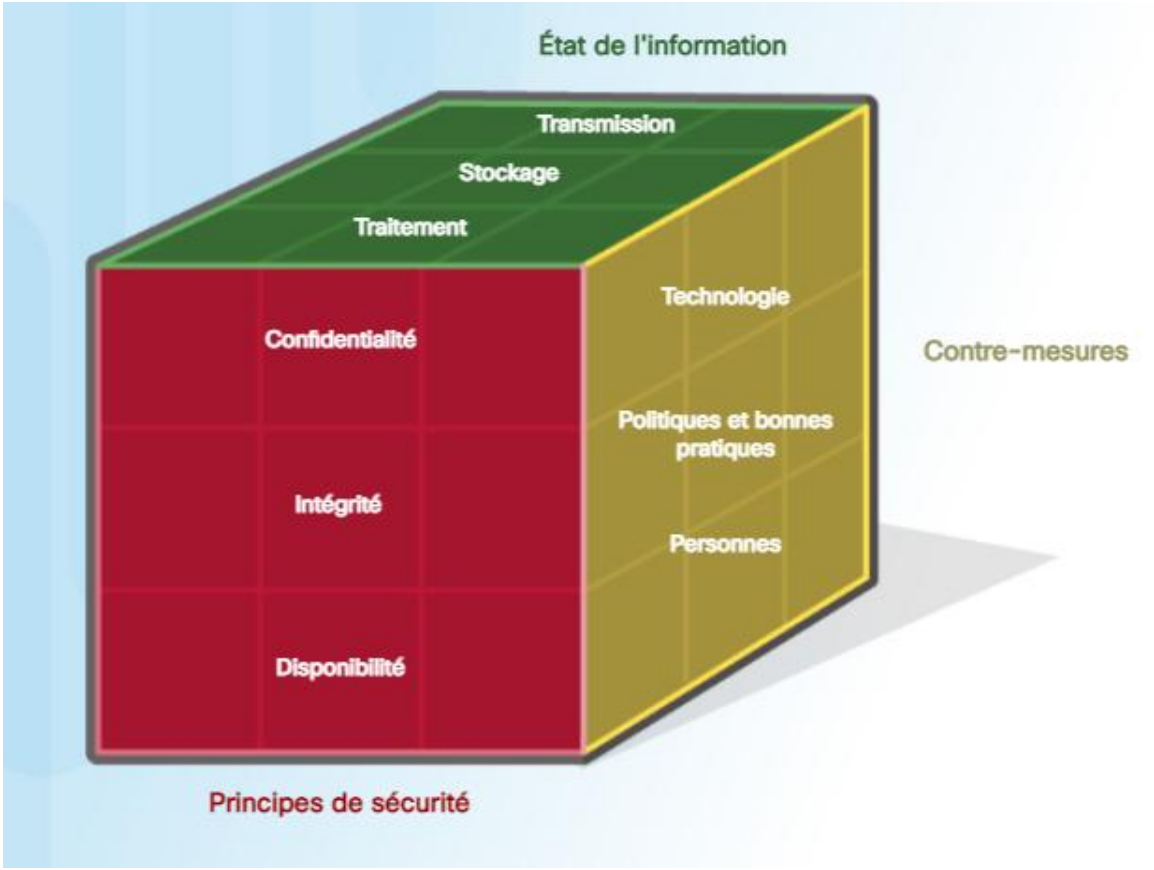


Figure V-2:La première dimension du cube McCumber.

La première dimension du cube McCumber identifie les objectifs à protéger sur Internet. Les objectifs identifiés dans la première dimension constituent les principes fondateurs du monde de la cybersécurité. Ces trois principes sont la confidentialité, l'intégrité et la disponibilité. Ces principes permettent à l'administrateur de la cybersécurité de cibler ses efforts et d'établir des priorités dans les mesures à prendre pour assurer la protection de ses ressources sur Internet.

V.1.1 Confidentialité, intégrité et disponibilité :

Confidentialité, intégrité et disponibilité, appelées ensemble la triade CIA « Figure V-3» sont une directive pour la sécurité de l'information pour une entreprise.

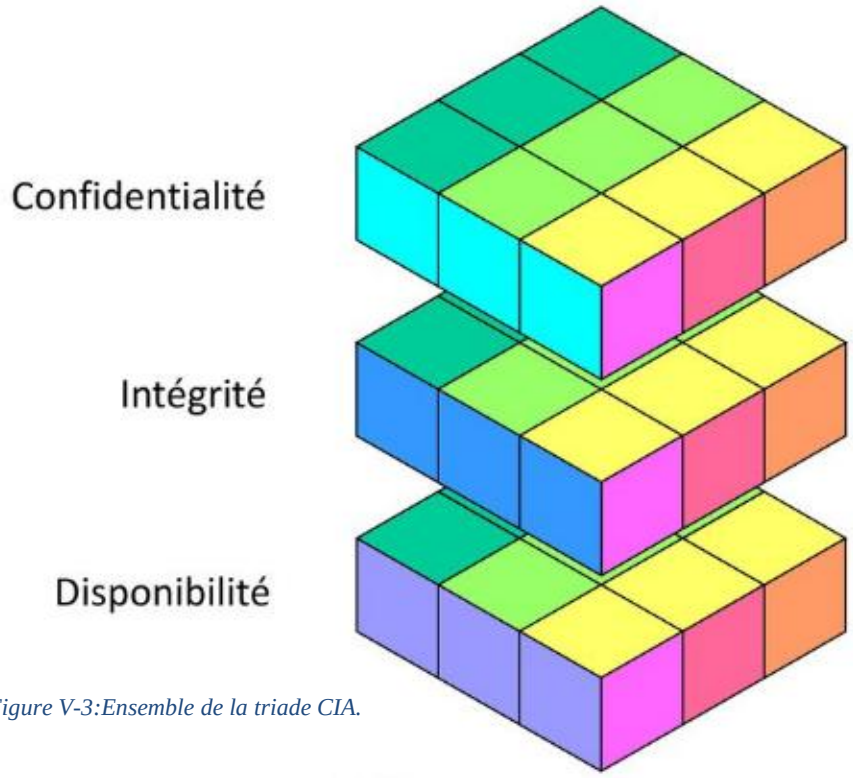


Figure V-3:Ensemble de la triade CIA.

La confidentialité garantit l'anonymat des données en limitant l'accès par le chiffrement de l'authentification. L'intégrité garantit que l'information est exacte et fiable. La disponibilité garantit que les personnes autorisées peuvent accéder à l'information.

V.1.1.1 Confidentialité:

Un autre terme pour la confidentialité serait l'anonymat. Les politiques d'entreprise devront limiter l'accès à l'information au personnel autorisé et garantir que seules ces personnes autorisées consultent ces données. Les données peuvent être compartimentées selon le niveau de sécurité ou de sensibilité de l'information. Par exemple, un programmeur java ne doit pas avoir accès aux informations personnelles de tous les employés. Par ailleurs, les employés doivent suivre une formation pour comprendre les bonnes pratiques en matière de protection des informations sensibles pour se protéger et pour protéger l'entreprise contre les attaques. Parmi les méthodes permettant de garantir la confidentialité, il y a le cryptage des données, l'ID et le mot de passe liés au nom d'utilisateur, l'authentification à deux facteurs et la réduction au minimum de l'exposition des informations sensibles.

V.1.1.1.1 Contrôle d'accès :

Le contrôle d'accès définit plusieurs dispositifs de protection conçus pour interdire les accès non autorisés à un ordinateur, un réseau, une base de données ou d'autres ressources de données. Les concepts désignés par AAA correspondent à trois services de sécurité : l'authentification, l'autorisation et la journalisation (Authentification,Authorization, Accounting). Ces services fournissent le cadre principal pour le contrôle d'accès.

Le premier « A » désigne l'authentification.

L'authentification vérifie l'identité d'un utilisateur afin d'empêcher tout accès non autorisé.

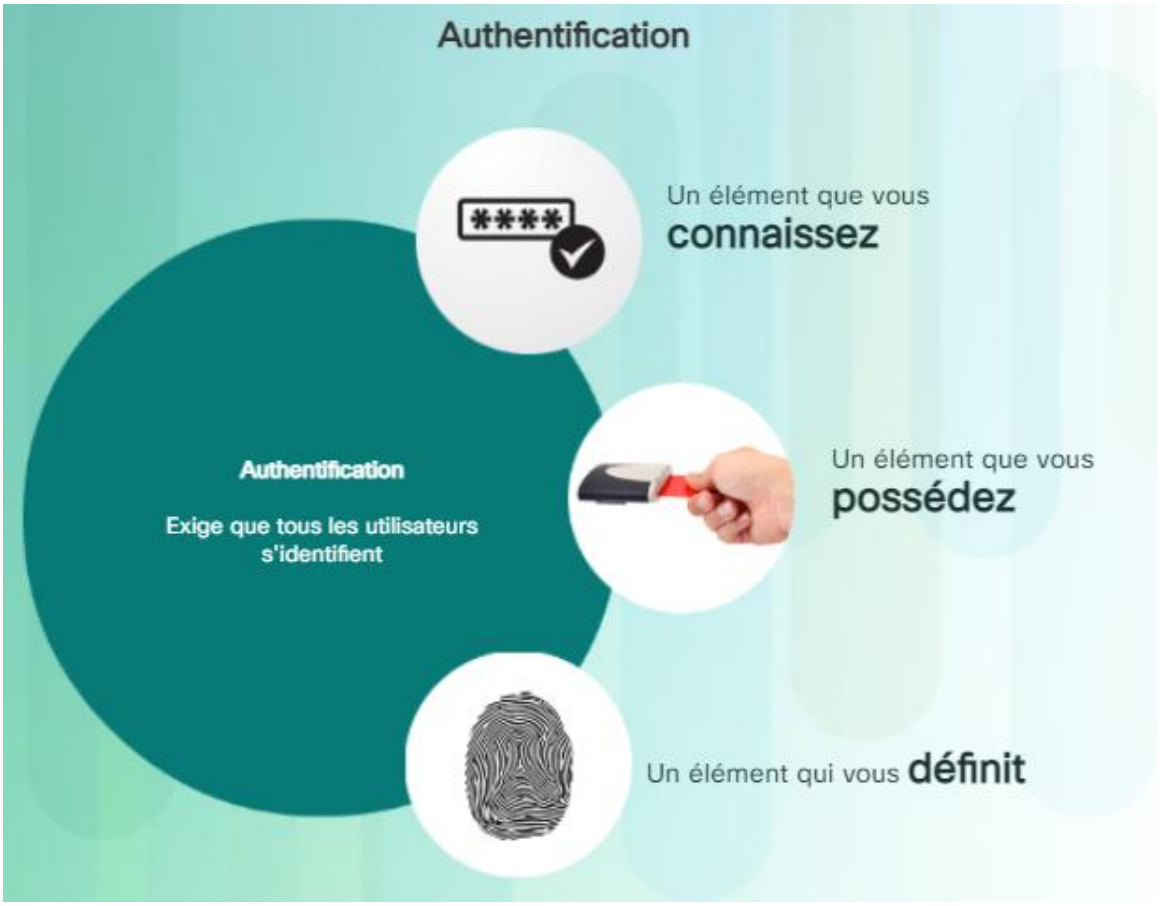


Figure V.1-2: Contrôle d'accès

Les utilisateurs prouvent leur identité au moyen d'un nom d'utilisateur ou d'un ID. Ils doivent, en outre, confirmer leur identité en fournissant l'un des éléments suivants, comme illustré à la « Figure V.1-2» :

- ☞ Un élément qu'ils connaissent (comme un mot de passe)
- ☞ Une chose qu'ils possèdent (comme un jeton ou une carte)
- ☞ Un élément qui les caractérise (comme une empreinte digitale)

Par exemple, pour retirer de l'argent à un guichet automatique, vous avez besoin de votre carte de crédit (c'est-à-dire une chose que vous possédez) et vous devez connaître votre code secret. Il s'agit également d'un exemple d'authentification multi facteur, en ce sens qu'elle nécessite plusieurs types d'authentification. La forme d'authentification la plus répandue est l'utilisation de mots de passe.

Les services d'autorisation identifient les ressources auxquelles les utilisateurs peuvent accéder, ainsi que les opérations qu'ils peuvent effectuer (comme le montre la « Figure V.1-3 »). Pour ce faire, certains systèmes utilisent une liste de contrôle d'accès ou ACL. Cette liste détermine si, une fois authentifié, un utilisateur dispose de certains privilèges d'accès. Le fait que vous puissiez vous connecter au réseau d'entreprise ne signifie pas nécessairement que vous êtes autorisé à utiliser l'imprimante couleur haut débit. L'autorisation permet également de contrôler les périodes au cours desquelles un utilisateur peut accéder à une ressource spécifique. Par exemple, il est possible que les employés puissent accéder à une base de données des ventes pendant les heures de travail, mais que cet accès leur soit interdit en dehors des heures de bureau.

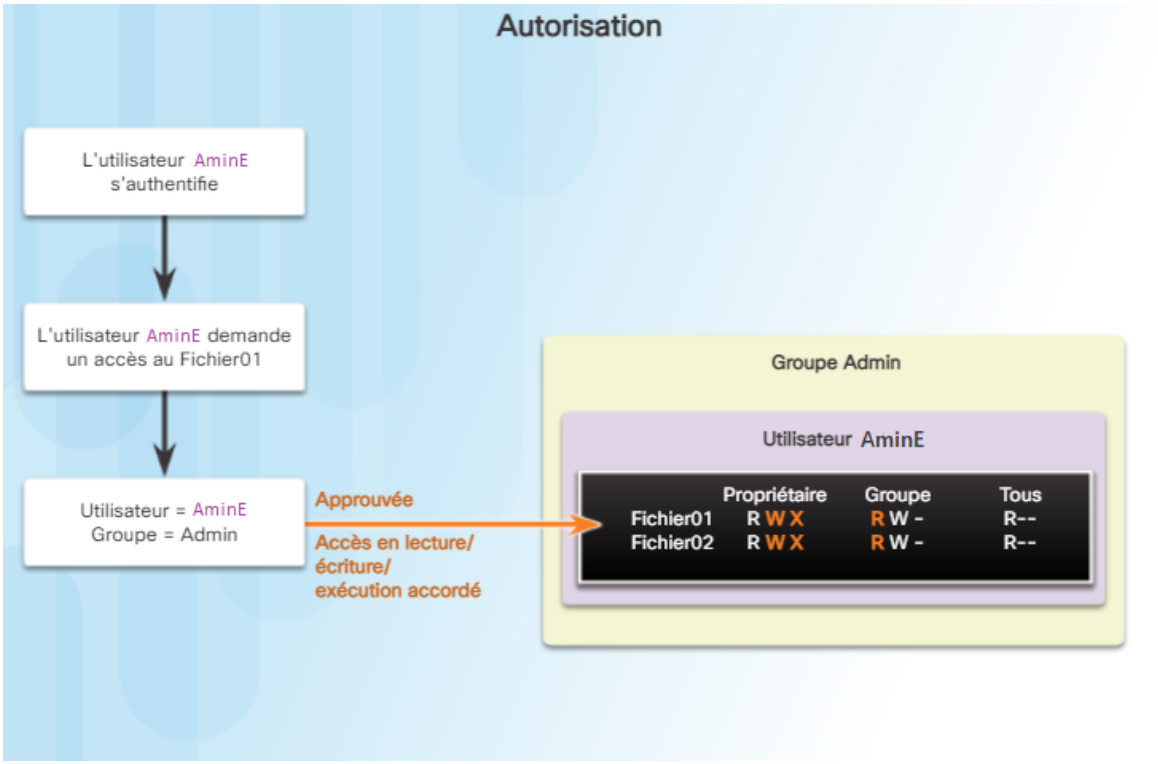


Figure V.1-3: Les propriété des permissions « UID et GID et Other »

La journalisation consiste à suivre les actions des utilisateurs : les éléments auxquels ils accèdent, le temps d'accès aux ressources, les modifications effectuées. Une banque, par exemple, opère ce type de contrôle pour chaque compte client. Un audit de ce système peut révéler l'heure et le montant de toutes les transactions, ainsi que l'employé ou le système responsable de leur exécution. Dans le domaine de la cybersécurité, les services de journalisation adoptent un fonctionnement identique. Le système effectue le suivi de chaque transaction de données et fournit des résultats d'audit. Un administrateur peut configurer des politiques informatiques, comme illustré à la « figure V.1-4 », pour activer l'audit du système. (5)

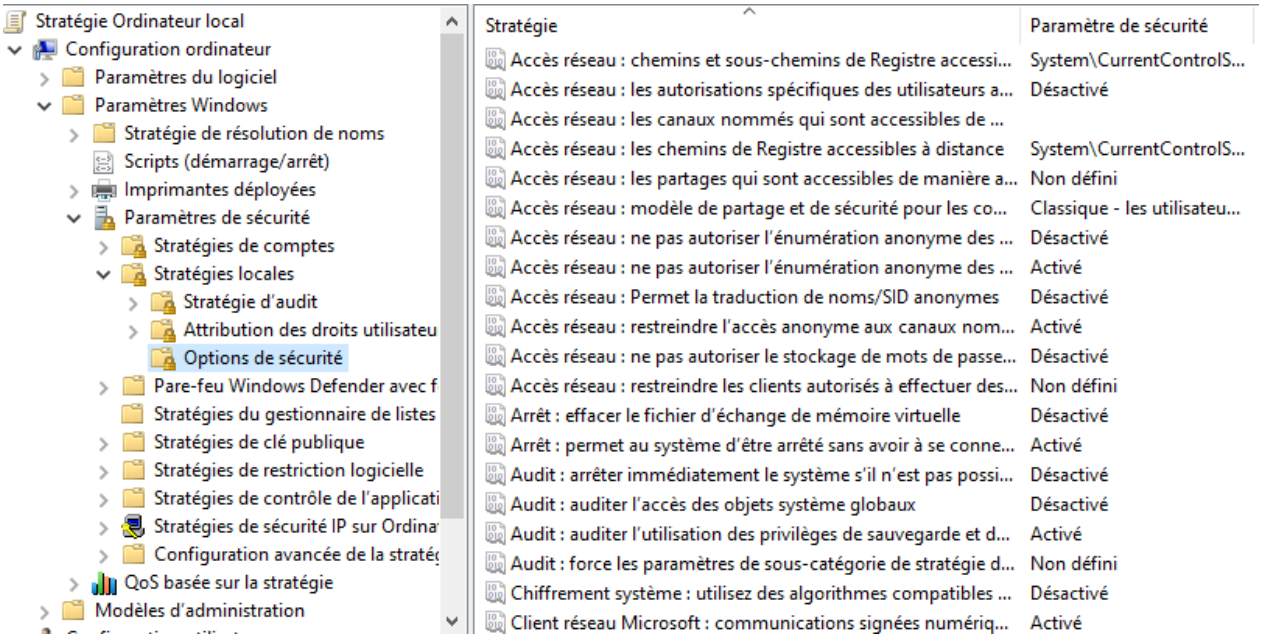
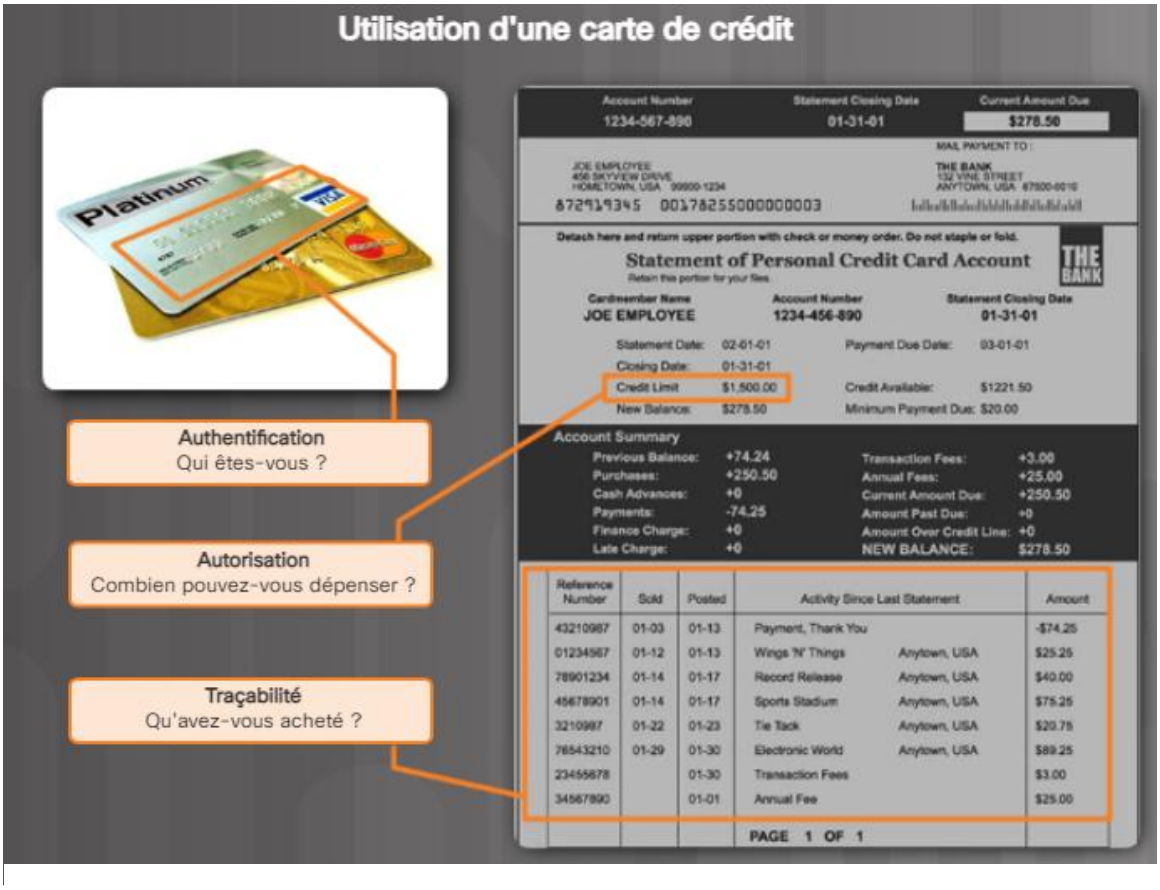


Figure V-4: Editeur de stratégie de groupe local sous Windows 10

Le concept désigné par les initiales anglaises AAA (Authentication, Authorization, Accounting) est semblable à l'utilisation d'une carte de crédit, comme le montre la « Figure V.1-5 ». La carte de crédit identifie qui est autorisé à l'utiliser, combien cet utilisateur peut dépenser et tient une comptabilité des achats de l'utilisateur.



V.1.1.2 Intégrité :

L'intégrité représente l'exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie « Un autre terme utilisé pour l'intégrité est la qualité » (6) . Les données ne doivent pas être altérées durant le transfert ni être modifiées par des entités non autorisées. Les permissions de fichiers et le contrôle d'accès pour les utilisateurs peuvent empêcher l'accès non autorisé. Le contrôle des versions peut être utilisé pour empêcher des modifications accidentelles par des utilisateurs autorisés. Les sauvegardes doivent être disponibles pour restaurer les données corrompues et le hachage des sommes de contrôle peut permettre de vérifier l'intégrité des données pendant le transfert.

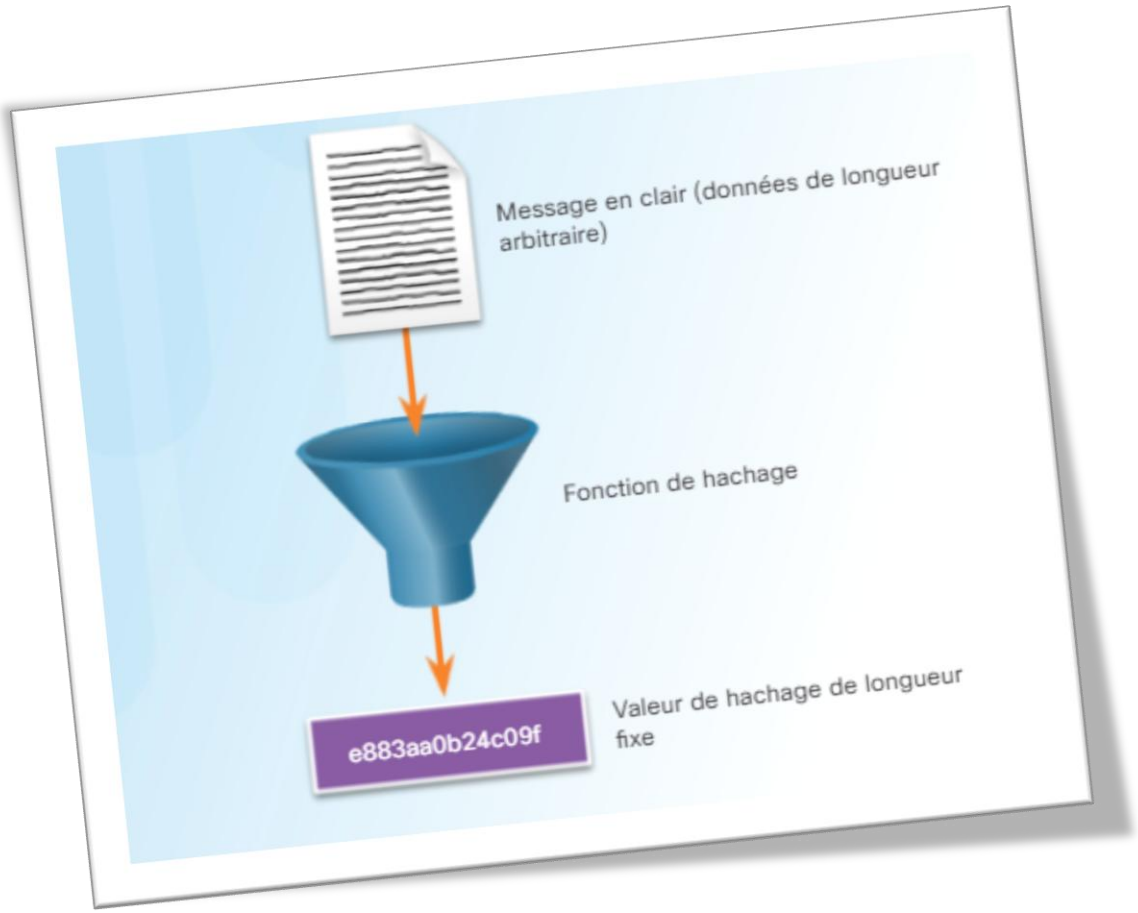


Figure V-6: Création d'un hachage

Une somme de contrôle est utilisée pour vérifier l'intégrité des fichiers ou des chaînes de caractères après leur transfert d'un périphérique à un autre dans votre réseau local ou sur Internet. Les sommes de contrôle sont calculées grâce à des fonctions de hachage. Parmi les sommes de contrôle les plus courantes, il y a MD5, SHA-1, SHA-256 et SHA-512. Une fonction de hash utilise un algorithme mathématique pour transformer les données en une valeur de longueur fixe qui représente les données, comme illustré à la « Figure V.1-6 ». La valeur hachée est simplement présente pour comparaison. Il est impossible d'extraire directement les données d'origine à partir de la valeur hachée. Par exemple, si vous avez oublié votre mot de passe, vous ne pourrez pas le récupérer à partir de la valeur hachée. Il vous faut réinitialiser le mot de passe.

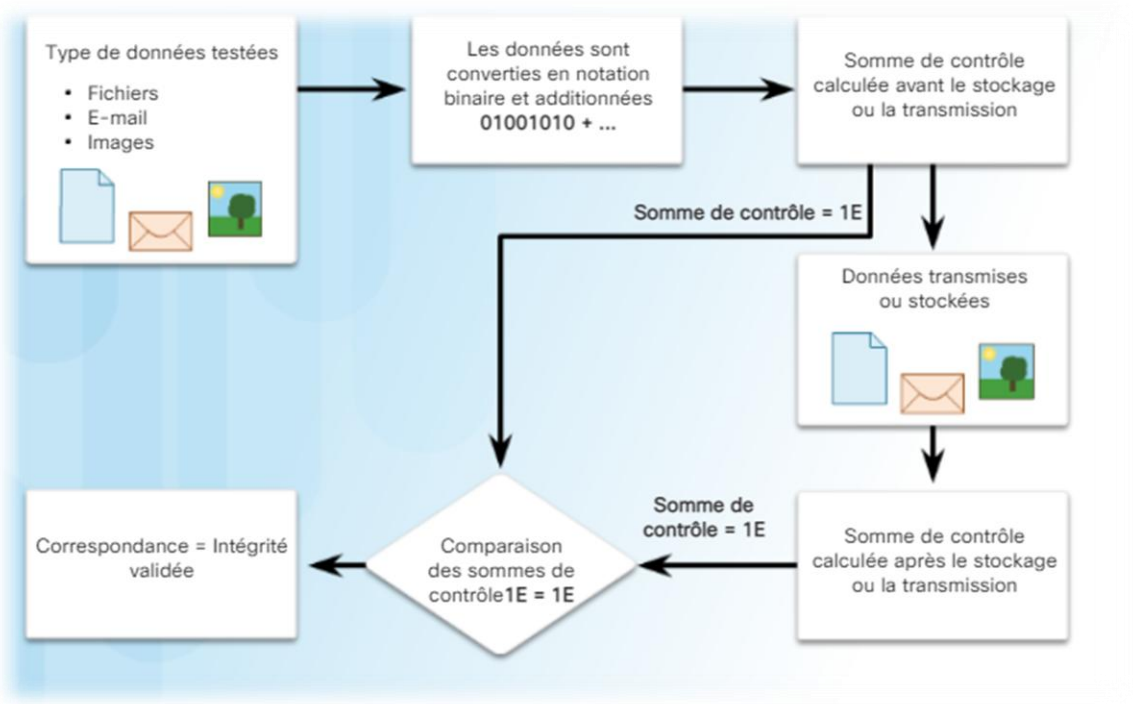


Figure V-7: Processus de somme de contrôle Validé

Après le téléchargement d'un fichier, vous pouvez vérifier son intégrité en vérifiant les valeurs hachées à partir de la source en fonction de celles générées en utilisant un calculateur de hachage. En comparant les valeurs de hachage, vous pouvez être sûr que le fichier n'a pas été altéré avec le transfert ou corrompu pendant celui-ci. Si les deux sommes sont égales, les données sont valides « Figure V.1-7 ». Dans le cas contraire, une modification s'est produite à un moment donné « Figure V-11 ».

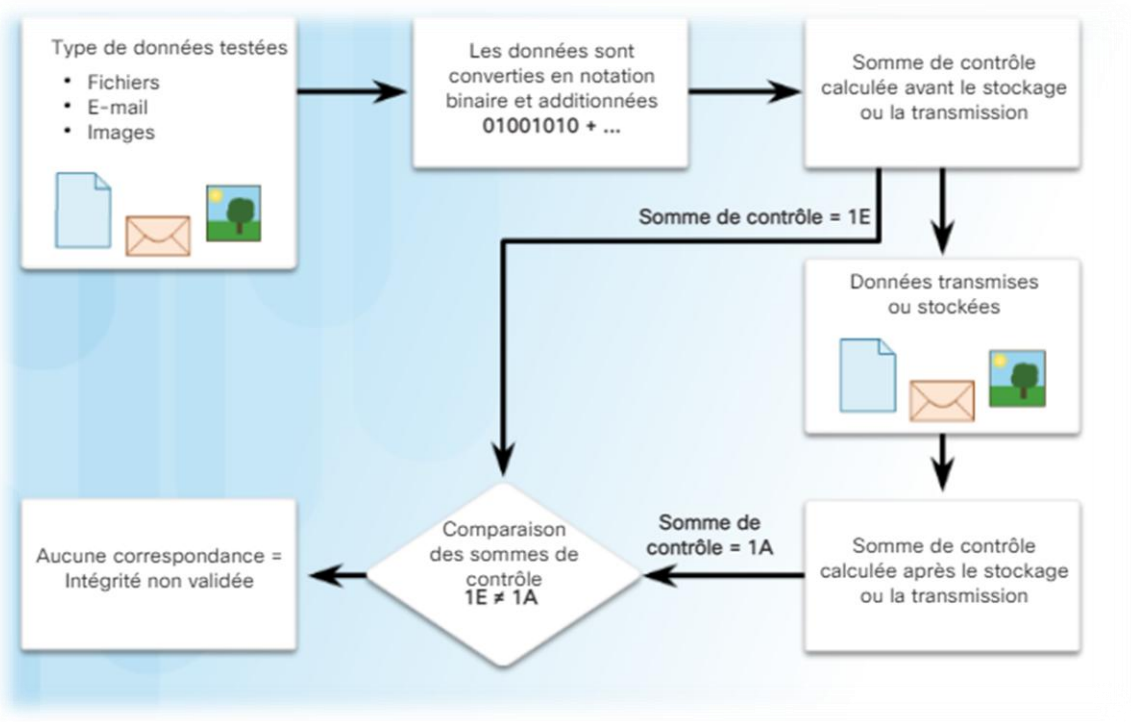


Figure V-8: Processus de somme de contrôle non Validé

L'exécution rigoureuse de sauvegardes permet de préserver l'intégrité des données en cas de corruption de ces dernières. L'entreprise doit vérifier sa procédure de sauvegarde pour en garantir l'intégrité avant une perte de données.

L'autorisation détermine les personnes autorisées à accéder aux ressources d'une entreprise en fonction de leurs besoins. Par exemple, les autorisations de fichiers et les contrôles d'accès d'utilisateur font en sorte que seuls certains utilisateurs peuvent modifier les données. Un administrateur peut définir les autorisations d'un fichier en lecture seule. Par conséquent, un utilisateur qui y accède ne pourra y apporter aucune modification.

V.1.1.3 Disponibilité:

La maintenance des équipements, la réparation des matériels, la mise à jour des systèmes d'exploitation et des logiciels, et la création de sauvegardes permettent de garantir la disponibilité du réseau et des données pour les utilisateurs autorisés. Des plans doivent être mis en place pour reprendre rapidement les activités après des catastrophes naturelles ou d'origine humaine. Des équipements ou des logiciels de sécurité, notamment les pares-feux, évitent les interruptions dues aux attaques comme le déni de service (DoS). Le déni de service survient lorsqu'un hacker tente de saturer les ressources pour que les services ne soient pas disponibles pour les utilisateurs.

Figure V-9: Raisons du problème de disponibilité

V.1.1.4 Les « cinq neuf » :

Les utilisateurs se servent de divers systèmes d'information dans la vie de tous les jours. Communications, transports, fabrication de produits… L'informatique est aujourd'hui présente à tous les niveaux ! La disponibilité continue des systèmes d'information est donc cruciale dans le monde moderne. Le terme de haute disponibilité décrit des systèmes conçus pour éviter les interruptions. Ce concept garantit un niveau de performances sur une période plus longue que la normale. Les systèmes à haute disponibilité répondent en général à ces trois principes de conception :

- Supprimer les points de défaillance uniques.
- Fournir des solutions de substitution fiables.
- Détecter les défaillances avant qu'elles ne surviennent.

Disponibilité en %	Indisponibilité par année	Indisponibilité par mois[3]	Indisponibilité par semaine
90 % (« un neuf »)	36,5 jours	72 heures	16,8 heures
95 %	18,25 jours	36 heures	8,4 heures
98 %	7,30 jours	14,4 heures	3,36 heures
99 % (« deux neuf »)	3,65 jours	7,20 heures	1,68 heure
99,5 %	1,83 jour	3,60 heures	50,4 minutes
99,8 %	17,52 heures	86,23 minutes	20,16 minutes
99,9 % (« trois neuf »)	8,76 heures	43,2 minutes	10,1 minutes
99,95 %	4,38 heures	21,56 minutes	5,04 minutes
99,99 % (« quatre neuf »)	52,56 minutes	4,32 minutes	1,01 minute
99,999 % (« cinq neuf »)	5,26 minutes	25,9 secondes	6,05 secondes
99,9999 % (« six neuf »)	31,5 secondes	2,59 secondes	0,605 seconde

Figure V-10: Mesure du taux de disponibilité

L'objectif est de garantir la continuité des activités, même dans des conditions extrêmes ; pendant une attaque, par exemple. Le concept des « cinq neuf » constitue l'une des pratiques de haute disponibilité les plus courantes. Ces cinq neuf correspondent à 99,999 %, soit un temps d'interruption inférieur à 5,26 minutes par an. De nombreuses techniques sont utilisées pour améliorer la disponibilité, On illustre 3 méthodes mises en œuvre pour atteindre les « cinq neuf » :

- √ la redondance des matériels et la mise en cluster;
- √ la sécurisation des données : RAID, snapshots, Oracle Data Guard **(en)**, BCV (Business Copy Volume), Symmetrix Remote Data Facility (SRDF), DRBD ;
- √ Pour chaque niveau de l'architecture, pour chaque composant, chaque liaison entre composants, il faut établir :
  - Comment détecter une panne ? Exemples : Tests de vie TCP Health Check implémenté par un boîtier Alteon, programme de test invoqué périodiquement (« ***heartbeat*** »), interface de type « diagnostic » sur les composants…

V.2 Les états des données :

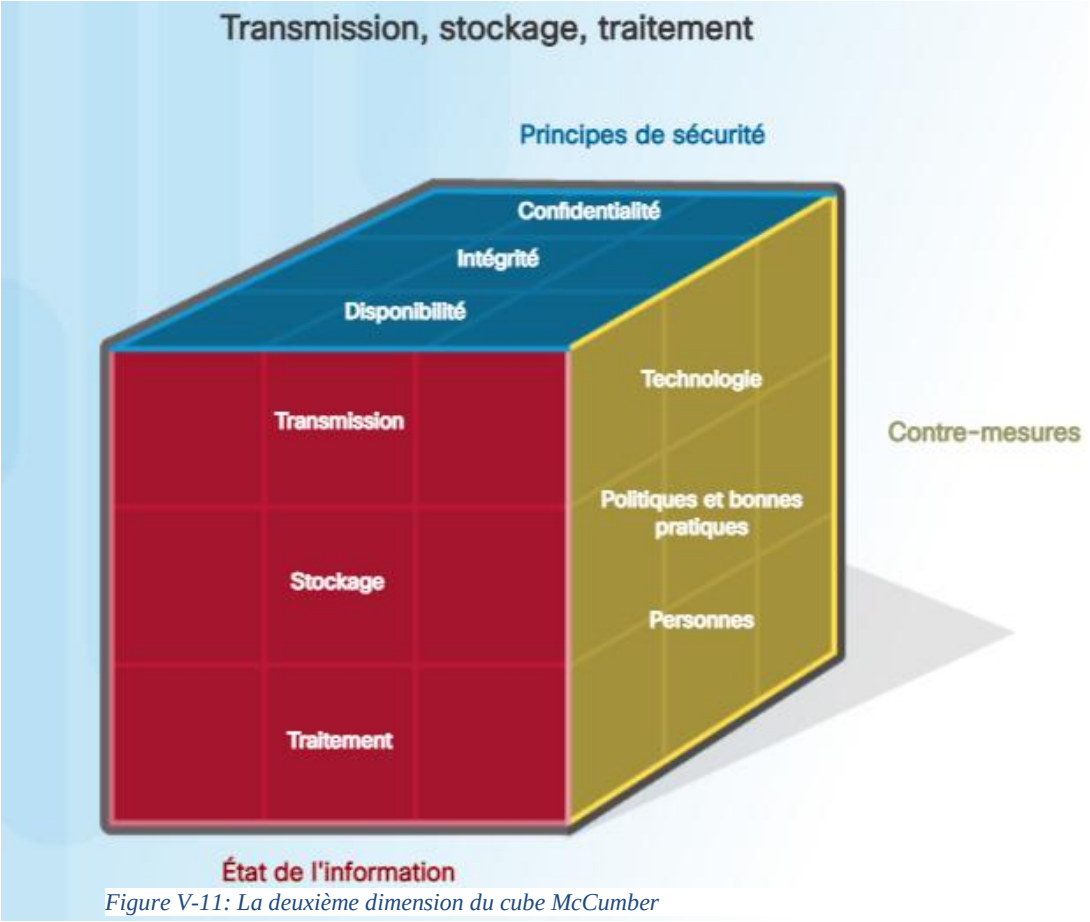


Figure V-11: La deuxième dimension du cube McCumber

Internet est constitué de données. La protection des données est donc la priorité des administrateurs de la cybersécurité. La deuxième dimension du cube de McCumber, la cybersécurité porte sur les problèmes liés à la protection des données sur Internet, quel que soit leur état.

Les données peuvent se présenter sous trois états différents :

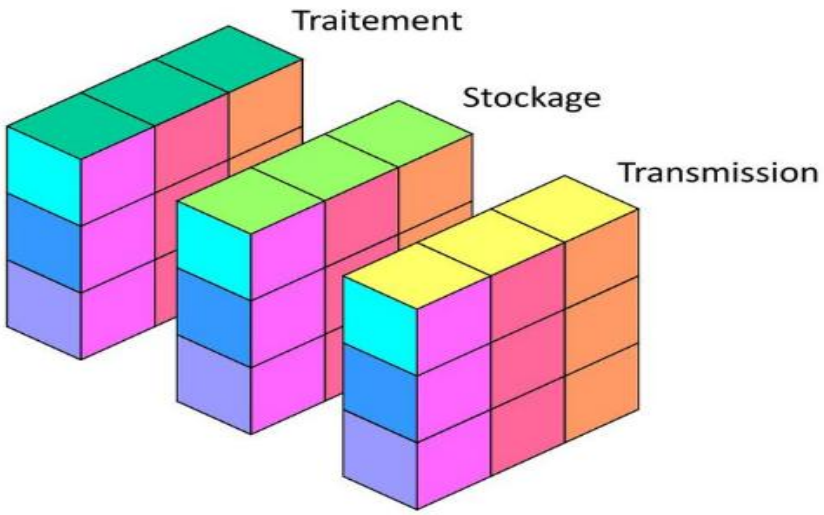


Figure V-12: Les trois états de la deuxième dimension du cube de McCumber

V.2.1 Stockage:

Données au repos dans un système d'information « data access right » (DAR), tel que celui stocké en mémoire ou sur une bande magnétique ou un disque :

V.2.1.1 Types de stockage des données :

Les données stockées sont des données au repos. Cela signifie qu'un équipement de stockage conserve les données lorsque celles-ci ne sont pas sollicitées par un utilisateur ou un processus. L'équipement de stockage peut être local (terminal de type ordinateur) ou centralisé (sur le réseau). Plusieurs options sont possibles pour le stockage de données.

Le stockage à connexion directe (DAS) est un mode de stockage connecté à un ordinateur. Un disque dur ou une clé USB sont des exemples de stockages à connexion directe Par défaut, les systèmes ne sont pas configurés pour le partage du stockage à connexion directe (DAS).

Un RAID (Redundant Array of Independent Disks) utilise plusieurs disques durs associés en baie et pris en charge comme un disque unique par le système d'exploitation. Un RAID permet de bénéficier d'une performance et d'une tolérance aux pannes améliorées.

Un stockage en réseau NAS est composé d'un terminal de stockage connecté à un réseau pour permettre le stockage et la récupération de données depuis un emplacement centralisé par les utilisateurs réseau autorisés. Les terminaux NAS sont flexibles et évolutifs, ce qui permet aux administrateurs d'augmenter la capacité si nécessaire.

Une architecture de réseau de stockage SAN est un système de stockage basé sur le réseau. Les systèmes SAN se connectent au réseau via des interfaces haut débit, ce qui leur permet de gagner en performance et de relier plusieurs serveurs à un référentiel de stockage sur disque centralisé.

Le stockage cloud est une option de stockage à distance qui utilise l'espace disponible auprès d'un fournisseur de data center. Ce stockage est accessible à partir de n'importe quel ordinateur avec accès à Internet. Google Drive, iCloud et Dropbox sont des exemples de fournisseurs de stockage cloud.

V.2.1.2 Défis relatifs à la protection des données stockées :

Pour les entreprises, la protection des données stockées représente un défi de taille. Pour améliorer le stockage, l'une des solutions consiste à automatiser et centraliser les sauvegardes de données.

Le stockage à connexion directe (DAS) peut être l'un des types de stockage les plus difficiles à gérer et à contrôler. Il est, en effet, vulnérable aux attaques malveillantes sur l'hôte local. Les données stockées peuvent également inclure des données de sauvegarde. Les

sauvegardes peuvent être manuelles ou automatiques. Les entreprises doivent limiter les types de données stockées sur un stockage à connexion directe (DAS). Les données essentielles, notamment, ne doivent pas y être stockées.

Les systèmes de stockage réseau (RAID, SAN et NAS) sont plus sécurisés. Ce type de stockage garantit de meilleures performances et une redondance accrue. Cependant, leur configuration et leur gestion s'avèrent plus complexes. Ils gèrent également davantage de données, ce qui fait courir un plus grand risque à l'entreprise en cas de panne de l'appareil. La configuration, les tests et la surveillance sont les principaux défis que les entreprises doivent relever avec les systèmes de stockage réseau.

V.2.2 Transmission:

Transfert de données entre systèmes d'information, également appelé données en transit (DIT) :

V.2.2.1 Méthodes de transmission des données:

Transmettre des données signifie envoyer des informations d'un appareil à un autre. C'est à dire transmettre des informations entre des appareils de bien des manières, notamment :

Sneaker net : des supports amovibles sont utilisés pour déplacer physiquement des données d'un ordinateur vers un autre.

Réseaux filaires : les données sont transmises au moyen de câbles.

Réseaux sans fil : les données sont transmises par le biais d'ondes radioélectriques.

Les entreprises ne parviendront jamais à éliminer le recours au « sneaker net ».

Les réseaux filaires sont composés de fils de cuivre et de câbles optiques. Ils desservent une aire géographique limitée (réseaux locaux ou LAN) ou ils peuvent couvrir de grandes distances (réseaux étendus ou WAN).

Les réseaux sans fil remplacent progressivement les réseaux filaires. Leur débit ne cesse d'augmenter et ils sont capables de traiter plus de bande passante. Ces réseaux augmentent le nombre d'utilisateurs invités équipés de terminaux mobiles sur les réseaux à domicile/de petits bureaux et sur les réseaux d'entreprise.

Les réseaux filaires et sans fil utilisent tous deux des paquets ou unités de données. Le terme « paquet » désigne une unité de données qui circule entre un point d'origine et un point de destination sur le réseau. Les protocoles standard, comme IP (Internet Protocol) et HTTP (HyperText Transfer Protocol), définissent la structure et la mise en forme des paquets de données. Il s'agit de standards Open Source à la disposition du public. La protection de la confidentialité, de l'intégrité et de la disponibilité des données transmises est l'une des tâches les plus importantes qui incombent à un professionnel de la sécurité réseau.

V.2.2.2 Défis relatifs à la protection des données en transit :

La protection des données transmises fait partie des tâches les plus ardues pour un professionnel de la cybersécurité. Avec la croissance du nombre de terminaux mobiles et sans fil, les professionnels de la cybersécurité doivent aujourd'hui protéger d'énormes quantités de données transitant quotidiennement sur leur réseau. S'agissant de la protection de ces données, les défis que doivent relever les professionnels de la sécurité réseau sont multiples :

Protection de la confidentialité des données : les cybercriminels peuvent capturer, enregistrer et voler les données en transit. Les professionnels de la cybersécurité doivent donc prendre les mesures adéquates pour contrer ces actions.

Protection de l'intégrité des données : les cybercriminels peuvent intercepter et altérer les données en transit. Les professionnels de la cybersécurité déploient des systèmes d'intégrité des données qui testent l'intégrité et l'authenticité des données transmises afin de contrer ces actions.

Protection de la disponibilité des données : les cybercriminels peuvent utiliser des appareils non autorisés pour interrompre la disponibilité des données. Un simple terminal mobile peut faire office de point d'accès sans fil local et pousser, par la ruse, les utilisateurs peu méfiants à s'y connecter. Les cybercriminels peuvent détourner une connexion autorisée à un appareil ou un service protégé. Les professionnels de la sécurité du réseau peuvent implémenter des systèmes d'authentification mutuelle pour contrer ces actions. Ces systèmes exigent de l'utilisateur qu'il s'authentifie sur le serveur et demandent à ce dernier de s'authentifier auprès de l'utilisateur.

Figure V-13: Donnée en transite

V.2.3 Traitement:

Le troisième état des données correspond aux données en cours de traitement. Effectuer des opérations sur des données afin d'atteindre un objectif souhaité :

V.2.3.1 Formes de calcul et de traitement des données :

Cela fait référence aux données lors de la saisie initiale, de la modification, du calcul ou de la sortie.

La protection de l'intégrité des données commence lors de la saisie initiale des données. Les entreprises collectent des données via différentes méthodes, comme la saisie manuelle, l'analyse des formulaires, le chargement de fichiers et la collecte de données par capteurs. Chacune de ces méthodes met potentiellement en péril l'intégrité des données. Des erreurs de saisie de données et des capteurs système déconnectés, défaillants ou inutilisables sont des exemples de corruption de données pouvant survenir pendant le processus de saisie. Un mauvais étiquetage et des formats de données incorrects ou incompatibles en sont d'autres exemples.

La modification des données fait référence à tout changement apporté aux données d'origine. On peut citer, par exemple, la modification manuelle des données par les utilisateurs, le traitement et la modification des données par les programmes ou encore les pannes matérielles engendrant une modification des données. Les processus comme le codage/décodage, la compression/décompression et le chiffrement/déchiffrement sont des exemples de modification des données. Le code malveillant engendre également la corruption des données.

Une corruption des données se produit également lors du processus de sortie. La sortie des données correspond à leur transmission vers des imprimantes, des dispositifs d'affichage électronique ou directement vers d'autres appareils. L'exactitude des données en sortie est essentielle, dans la mesure où elles fournissent des informations et influencent la prise de décision. Voici quelques exemples de corruption de données en sortie : utilisation incorrecte de séparateurs de données, configurations incorrectes des communications, erreur de configuration des imprimantes…

V.2.3.2 Défis relatifs à la protection des données en cours de traitement :

Se prémunir contre la modification incorrecte de données en cours de traitement peut également avoir des effets négatifs. Les erreurs logicielles sont, en effet, à l'origine de nombreux incidents et sinistres. Ainsi, seulement deux semaines avant Noël, le prix des articles proposés par certains partenaires commerciaux d'Amazon a été ramené à un centime. Le problème a duré une heure. Plusieurs milliers d'acheteurs ont toutefois pu profiter de cette offre exceptionnelle, ce qui a fait perdre beaucoup d'argent à la société. En 2016, le thermostat Nest a connu un dysfonctionnement, laissant de ce fait les utilisateurs sans chauffage. Le thermostat Nest est une technologie intelligente détenue par Google. Un petit « pépin » logiciel aux conséquences glaçantes ! En fait, une mise à jour logicielle s'est mal passée, entraînant la décharge forcée des piles de l'appareil, ce dernier étant alors incapable de réguler la température. Par conséquent,

les clients n'ont pas pu chauffer leur maison, ni avoir d'eau chaude pendant l'un des week-ends les plus froids de l'année.

Pour protéger les données en cours de traitement, la conception des systèmes doit être parfaitement étudiée. Les politiques et procédures conçues par les professionnels de la cybersécurité prévoient que les systèmes soient testés, maintenus et mis à jour pour qu'ils continuent de fonctionner avec un minimum d'erreurs.

Figure V-14: Contre-mesures des données en traitement

Pour protéger le cyberespace, les professionnels de la cybersécurité doivent tenir compte de la protection des données dans les trois états.

V.3 Dispositifs de protection en cybersécurité « Mesures de sécurité » :

La troisième dimension du cube de mccumber la cybersécurité définit les types de pouvoirs auxquels un administrateur de la sécurité réseau peut avoir recours pour protéger le cyberespace.

Les professionnels de la cybersécurité doivent utiliser tous les pouvoirs dont ils disposent pour protéger les données du cyberespace.

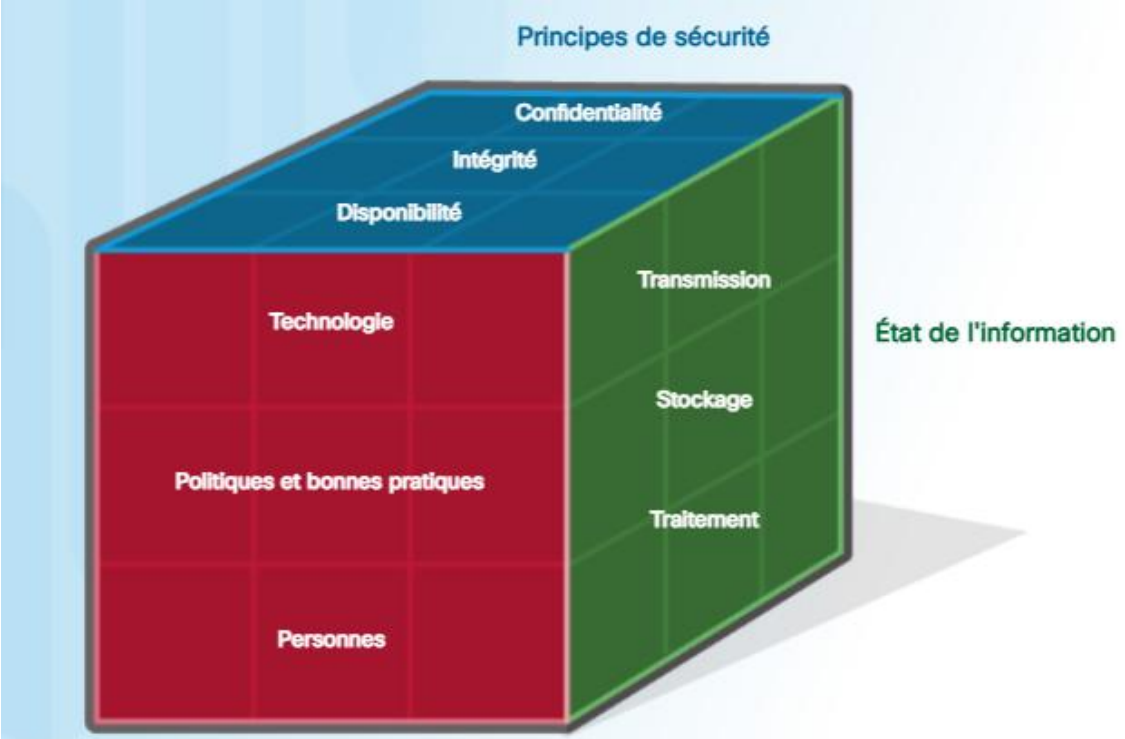


Figure V-16: Les exigence de sécurité selon La troisième dimension de la cube de mccumber

Le cube de mccumber identifie les trois types de pouvoirs, ou armes, utilisés pour assurer leur protection :

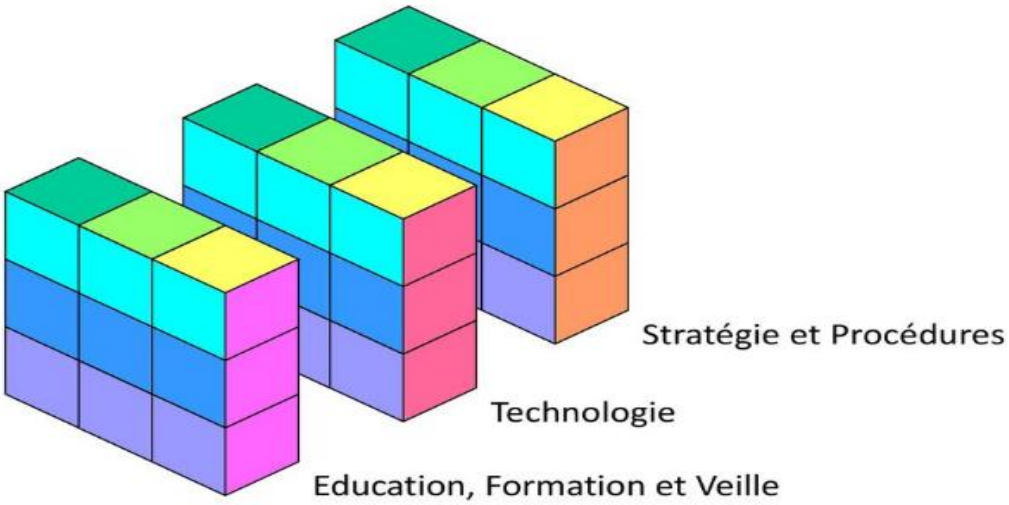


Figure V-15: La troisième dimension du cube de mccumber "Mesure de sécurité"

V.3.1 Technologie:

Le premier type de pouvoir comprend les technologies, les appareils et les produits disponibles pour protéger les systèmes d'information et repousser les cybercriminels. Les professionnels de la cybersécurité sont connus pour maîtriser les outils technologiques mis à leur disposition.

V.3.1.1 Des protections technologiques logicielles :

Les protections logicielles englobent les programmes et les services qui protègent les systèmes d'exploitation, les bases de données et les autres services exécutés sur les postes de travail, les appareils portables et les serveurs. Les administrateurs mettent en place des mesures ou des mécanismes de protection logiciels sur les différents hôtes ou serveurs. Plusieurs technologies logicielles sont utilisées pour protéger les ressources d'une entreprise (et on va se détaillée sure le sous-chapitre mesure de sécurité) :

- ☞ Les pares-feux logiciels contrôlent l'accès à distance à un système. Les systèmes d'exploitation intègrent généralement un pare-feu. Sinon, l'utilisateur peut en acheter un ou le télécharger auprès d'un tiers.
- ☞ Les scanners réseau et les scanners de ports détectent et contrôlent les ports ouverts sur un hôte ou un serveur.

- ☞ Les analyseurs de protocole, ou analyseurs de signature, sont des appareils qui collectent et examinent le trafic réseau. Ils identifient les problèmes de performances, détectent les erreurs de configuration, identifient les applications au comportement suspect, établissent des modèles de trafic de référence et normaux, et résolvent les problèmes de communication.

- ☞ Les scanners de vulnérabilité sont des programmes informatiques conçus pour évaluer les faiblesses des ordinateurs ou des réseaux.

- ☞ Les systèmes de détection d'intrusion (IDS) basés sur l'hôte examinent l'activité sur les systèmes hôtes uniquement. Ils génèrent des fichiers journaux et des messages d'alarme lorsqu'ils détectent une activité inhabituelle. Un système qui stocke des données sensibles ou qui fournit des services stratégiques est un bon candidat au titre de système IDS basé sur l'hôte.

V.3.1.2 Des protections technologiques matérielles :

Plusieurs technologies matérielles sont utilisées pour protéger les ressources d'une entreprise :

Les Appliance de pare-feu bloquent le trafic indésirable. Les pare-feu intègrent des règles qui définissent le trafic entrant et sortant autorisé sur le réseau.

Les systèmes de détection d'intrusion (IDS) dédiés détectent les symptômes d'une attaque ou d'un trafic inhabituel sur un réseau et envoient une alerte.

Les systèmes de prévention des intrusions (IPS) détectent les symptômes d'une attaque ou d'un trafic inhabituel sur un réseau, génèrent une alerte et prennent des mesures correctives.

Les services de filtrage du contenu contrôlent l'accès et la transmission de contenu considéré comme choquant ou répréhensible.

Plus de détail sur les mesure de sécurité…

V.3.1.3 Des protections technologiques basées sur le réseau :

Plusieurs technologies basées sur le réseau sont utilisées pour protéger les ressources de l'entreprise :

- **Le réseau privé virtuel (VPN)** est un réseau virtuel sécurisé qui utilise le réseau public (c'est-à-dire Internet). La sécurité d'un VPN dépend du chiffrement du contenu du paquet entre les terminaux qui définissent le VPN.
- **Le contrôle d'accès réseau (NAC)** exige un ensemble de vérifications avant d'autoriser un appareil à se connecter à un réseau. Parmi les contrôles courants, on compte l'installation de mises à jour du système d'exploitation ou du logiciel antivirus.
- **La sécurité du point d'accès sans fil** inclut l'implémentation de l'authentification et du chiffrement.

V.3.1.4 Des protections technologiques dans le cloud :

Les technologies dans le cloud déplacent la technologie de l'entreprise au fournisseur cloud. Les trois principaux services de cloud computing sont les suivants :

Le logiciel proposé comme un service (SaaS) permet aux utilisateurs d'accéder au logiciel d'application et aux bases de données. Les fournisseurs cloud gèrent l'infrastructure. Les utilisateurs stockent les données sur les serveurs du fournisseur cloud.

L'infrastructure en tant que service (IaaS) fournit des ressources informatiques virtualisées sur Internet. Le fournisseur héberge le matériel, les logiciels, les serveurs et les composants de stockage.

La plate-forme proposée comme un service (PaaS) fournit l'accès aux services et outils de développement utilisés pour la diffusion des applications.

Les fournisseurs de services cloud ont étendu ces options de manière à inclure l'IT en tant que service (ITaaS), lequel fournit une prise en charge informatique pour les modèles de service IaaS, PaaS et SaaS. Dans le modèle ITaaS, une entreprise charge le fournisseur de cloud de réaliser des services individuels ou groupés.

Les fournisseurs de services cloud utilisent des appliances de sécurité virtuelles qui s'exécutent à l'intérieur d'un environnement virtuel avec un système d'exploitation renforcé prêt à l'emploi, exécuté sur du matériel virtualisé.

V.3.2 Politiques et procédures de cybersécurité :

Cependant, John McCumber leur rappelle que les outils technologiques seuls ne suffisent pas pour mettre en échec les cybercriminels. En effet, ils doivent également ériger de solides défenses en développant des politiques, des procédures et des directives permettant aux citoyens du cyberespace de rester protégés et de respecter de bonnes pratiques d'utilisation.

V.3.2.1 Politiques :

Une politique de sécurité regroupe les différents objectifs de sécurité définis par l'entreprise. Elle comprend des règles de comportement à l'intention des utilisateurs et des administrateurs, et définit une configuration système requise. Ces objectifs, ces règles et ces exigences assurent ensemble la sécurité du réseau, des données et des systèmes informatiques d'une entreprise.

Une politique de sécurité exhaustive porte sur plusieurs points :

- Elle montre l'engagement de l'entreprise envers la sécurité.
- Elle définit les règles relatives au comportement attendu.
- Elle garantit la cohérence au niveau des opérations du système, de l'achat et de l'utilisation de composants matériels et logiciels, ainsi que de la maintenance.
- Elle définit les conséquences juridiques des infractions.
- Elle garantit au personnel de sécurité le soutien de la direction.

Les politiques de sécurité informent les utilisateurs, le personnel et les dirigeants des exigences de l'entreprise quant à la protection des ressources d'informations et technologiques. Une politique de sécurité spécifie également les mécanismes requis pour répondre aux exigences en matière de sécurité.

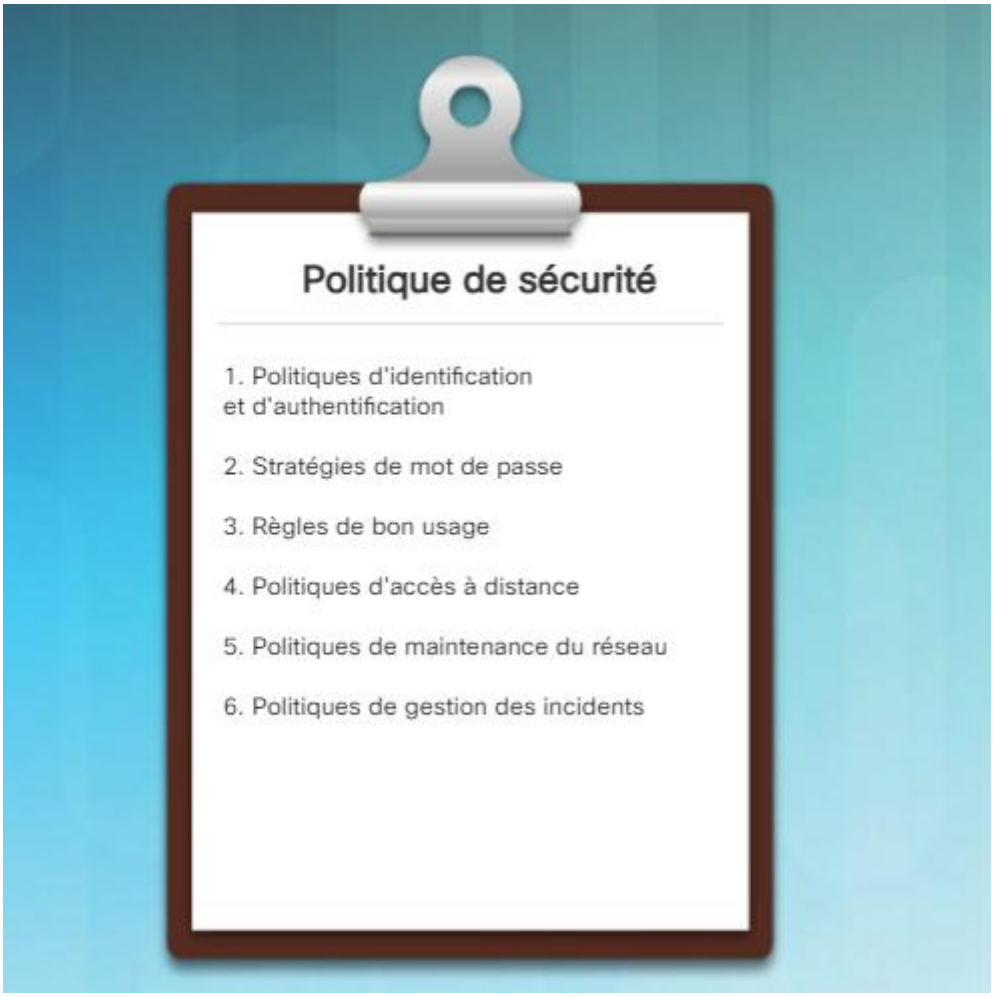


Figure V-17:exemplaire d'une politique de sécurité

Comme illustré sur cette figure, une politique d'audit crée un fichier journal de sécurité utilise de sécurité se compose généralement des éléments suivants :

Politiques d'identification et d'authentification: elles spécifient les personnes autorisées à accéder aux ressources réseau et décrivent les procédures de vérification.

Politiques de mot de passe: elles garantissent que les mots de passe remplissent les conditions minimales requises et sont changés régulièrement.

Règles de bon usage: elles identifient les ressources réseau et l'utilisation considérées comme acceptables par l'entreprise. Elles peuvent également identifier les conséquences d'une infraction.

Politiques d'accès à distance: elles indiquent la manière dont les utilisateurs distants peuvent accéder à un réseau, ainsi que les ressources accessibles à distance.

Politiques de maintenance du réseau: elles spécifient les procédures de mise à jour des systèmes d'exploitation des appareils réseau et des applications.

Politiques de gestion des incidents: elles décrivent la manière dont sont gérés les incidents liés à la sécurité.

La règle d'utilisation acceptable est l'une des composantes les plus courantes de la politique de sécurité. Cette règle définit les autorisations des utilisateurs au niveau des divers composants système. La règle d'utilisation acceptable doit être aussi explicite que possible pour éviter tout malentendu. Elle peut ainsi répertorier les sites web, groupes de discussion et autres applications gourmandes en bande passante auxquels les utilisateurs ne peuvent pas accéder à l'aide des ordinateurs ou du réseau de l'entreprise.

V.3.2.2 Standards :

L'utilisation de standards aide le personnel informatique à garantir une utilisation cohérente du réseau. Les documents standard définissent les technologies dont des utilisateurs ou programmes spécifiques ont besoin, en plus de tout critère ou exigence qu'une entreprise doit respecter. Cela permet au personnel informatique de simplifier les opérations de conception, de maintenance et de dépannage, et d'en améliorer l'efficacité. (7)

La cohérence est l'un des principes de sécurité les plus importants. C'est pourquoi il est essentiel pour les entreprises d'établir des normes. Chaque entreprise élabore des normes adaptées à son environnement de fonctionnement. Elle peut, par exemple, établir une politique relative aux mots de passe. Le standard veut que les mots de passe aient une longueur minimale de huit caractères alphanumériques majuscules et minuscules, avec au moins un caractère spécial. Un utilisateur doit modifier son mot de passe tous les 30 jours et un historique des 12 derniers mots de passe lui évite de réutiliser un même mot de passe pendant un an.

V.3.2.3 Directives :

Les directives détaillent une liste de suggestions visant à effectuer les opérations de manière plus efficace et plus sécurisée. Ils s'apparentent à des normes, mais sont plus flexibles et généralement pas obligatoires. Des directives définissent la manière dont les normes sont développées et garantissent leur conformité aux politiques de sécurité générales.

Certaines des directives les plus utiles constituent les bonnes pratiques de l'entreprise. Outre les bonnes pratiques définies par l'entreprise, des directives sont disponibles auprès des sources suivantes :

- Computer Security Resource Center du NIST (National Institute of Standards and Technology)
- Security Configuration Guides de la NSA (National Security Agency)
- Standard des Critères Communs

Pour reprendre l'exemple de la politique relative aux mots de passe, une directive suggère à l'utilisateur de choisir une phrase telle que « I have a dream » et de la transformer en mot de passe fort, Ihv@dr3@m. L'utilisateur peut créer d'autres mots de passe à partir de cette entité en changeant le chiffre, en déplaçant le symbole ou encore en modifiant la ponctuation.

V.3.2.4 Procédures :

Les documents de procédure sont plus longs et plus détaillés que les standards et les directives. Les documents de la procédure englobent des informations sur l'implémentation qui contiennent habituellement des instructions pas-à-pas et des graphiques.

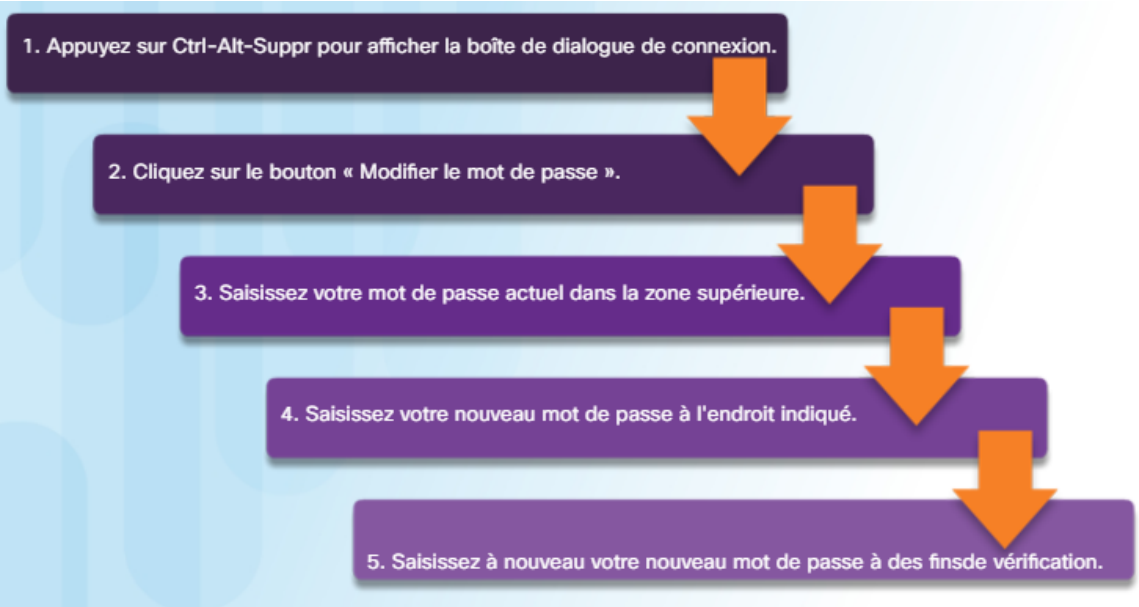


Figure V-18: Procédure pour changer un mot de passe

Cette figure montre un exemple de la procédure utilisée pour modifier un mot de passe. Au sein des grandes entreprises, l'utilisation de documents de procédure est requise afin de préserver un déploiement cohérent, ce qui s'avère nécessaire pour un environnement sécurisé.

V.3.3 Education, Formation et Veille:

Enfin, comme c'est le cas dans le réseau, les utilisateurs de réseau ou employeur de l'entreprises doivent en apprendre toujours plus sur la sécurité de leur réseau et sur les dangers qui le menacent. Ils doivent être assoiffés de connaissances, et établir une culture d'apprentissage et de prise de conscience, on va prendre ça « La formation des utilisateurs » on détail sur Les mesures de sécurité.

VI. le profil d un agresseur informatique et l'impact de leur sophistication :

Au début de la sécurité réseau, les cybercriminels étaient généralement des adolescents ou des amateurs agissant depuis leur ordinateur à domicile, et les attaques se limitaient à des canulars et du vandalisme. Les profils et les motivations d'agresseurs ont changé au fil des ans. Le hacking a commencé dans les années 1960 par le piratage téléphonique (phone freaking ou phreaking). Cette pratique consistait à utiliser différentes fréquences audios pour manipuler les systèmes téléphoniques. Dans le milieu des années 1980, les criminels utilisaient des modems commutés pour connecter des ordinateurs à des réseaux et utilisaient des programmes de

piratage de mots de passe pour accéder aux données. Aujourd'hui, le monde des cybercriminels est devenu plus dangereux, les criminels sont des individus ou des groupes qui tentent d'exploiter des vulnérabilités à des fins personnelles ou financières et ne se contentent plus de voler des informations. Les criminels utilisent maintenant les malwares et les virus comme armes technologiques. Toutefois, la plus grande motivation de la plupart des cybercriminels est financière. La cybercriminalité est devenue plus lucrative que le trafic de stupéfiants.

VI.1 Les différents types d'agresseurs (les cybercriminels) :

VI.1.1 Amateurs :

Ces personnes sont quelques fois appelées Script Kiddies. Ce sont généralement des agresseurs avec peu ou pas de compétence. Ils utilisent souvent des outils ou des instructions découverts sur Internet pour lancer des attaques. Certains d'entre eux sont simplement curieux, tandis que d'autres essaient de démontrer leurs compétences et entraînent des méfaits. Ils peuvent utiliser des outils basiques, mais le résultat peut quand même être dévastateur.

VI.1.2 Hackers :

Ce groupe de criminels s'introduit dans les ordinateurs et les réseaux. Leurs motifs sont variés. Selon le type d'intrusion, les hackers sont classés dans l'une des trois catégories suivantes : hackers au chapeau blanc, gris ou noir. Les hackers au chapeau blanc s'introduisent dans les systèmes réseau et informatiques pour en découvrir les faiblesses et en améliorer la sécurité. Les propriétaires du système leur donnent l'autorisation de s'y introduire et reçoivent les résultats du test. D'un autre côté, les hackers au chapeau noir profitent de toute vulnérabilité à des fins personnelles, financières ou politiques illégales. Les hackers au chapeau gris se trouvent entre les Chapeaux noirs et les Chapeaux blancs. Parfois, les hackers au chapeau gris détectent une vulnérabilité et en font part aux propriétaires du système si cela s'intègre à leurs objectifs Mais certains hackers au chapeau gris publient leurs découvertes sur Internet pour que d'autres hackers puissent les exploiter.

VI.1.3 Hackers organisés :

Ces criminels sont notamment des organisations de cybercriminels, des hacktivistes, des terroristes et des hackers financés par des gouvernements (8). Les cybercriminels sont généralement des groupes de criminels professionnels qui misent sur le contrôle, le pouvoir et la richesse. Ils sont très expérimentés et organisés, et ils peuvent même proposer leurs services dans le secteur du cybercrime. Les hacktivistes effectuent des déclarations politiques pour sensibiliser sur les questions qui leur sont importantes. Les hacktivistes rendent publiques des informations compromettantes sur leurs victimes. Les agresseurs financés par des gouvernements rassemblent des renseignements ou commettent des sabotages au nom de leurs gouvernements. Ces agresseurs sont généralement très entraînés et disposent de fonds importants. Leurs attaques ciblent des objectifs spécifiques présentant un avantage pour leur gouvernement. Certains hackers financés par des gouvernements sont même membres des forces armées de leurs pays.

VI.2 Menaces internes et externes :

Les attaques peuvent provenir de l'intérieur d'une entreprise ou de l'extérieur, comme illustré sur la « figure VI-1 ». Un utilisateur interne, par exemple un employé ou un partenaire contractuel, peut accidentellement ou intentionnellement :

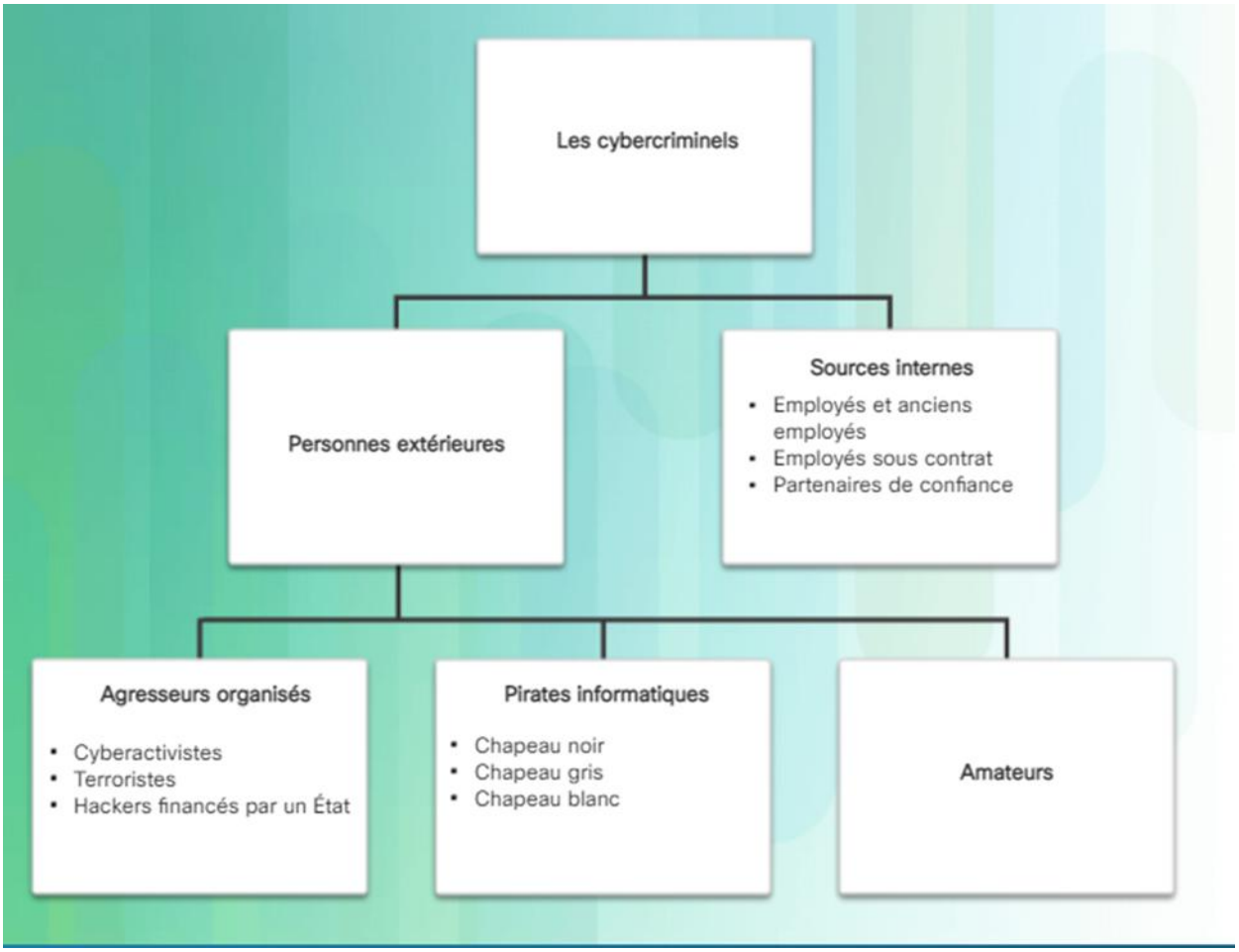


Figure VI-1: Menaces internes et externes

- ☞ Mal gérer les données confidentielles ;
- ☞ Menacer le fonctionnement des serveurs internes ou des périphériques de l'infrastructure réseau ;
- ☞ Faciliter les attaques venant de l'extérieur en connectant un support USB infecté dans le système informatique de l'entreprise ;
- ☞ Inviter accidentellement un malware dans le réseau par des e-mails ou des sites Web malveillants.

Les menaces internes sont susceptibles d'entraîner des dégâts plus importants que les menaces externes, car les utilisateurs internes disposent d'un accès direct au bâtiment et à l'équipement de l'infrastructure. Les hackers internes connaissent généralement le réseau de l'entreprise, ses ressources et ses données confidentielles. Ils connaissent aussi parfois les mesures de sécurité, les politiques et les privilèges administratifs de niveau supérieur.

VI.2.1 Menaces externes pour la sécurité :

Les menaces externes provenant de hackers amateurs ou expérimentés tirent parti des vulnérabilités des appareils réseau ou font appel à des techniques d'ingénierie sociale, comme la supercherie, pour accéder aux données. Les attaques externes exploitent les faiblesses ou les vulnérabilités pour accéder aux ressources internes.

VI.2.2 Données traditionnelles :

Les informations de l'entreprise incluent les informations personnelles, la propriété intellectuelle et les données financières. Les informations personnelles incluent des dossiers de candidature, des fiches de paie, des lettres d'offre, des contrats de travail et toute information utilisée dans les prises de décisions sur l'embauche. La propriété intellectuelle, comme les brevets, les marques déposées et les plans produits, permet à une entreprise d'avoir un avantage économique sur ses concurrents. La propriété intellectuelle peut être considérée comme un secret commercial ; la perdre serait désastreux pour l'avenir de l'entreprise. Les données financières, dont les comptes de résultat, les bilans comptables et les tableaux de trésorerie d'une entreprise, donnent un aperçu de la santé de l'entreprise.

VI.3 Une portée plus large et un effet domino :

La gestion des identités fédérées se définit de la manière suivante : les utilisateurs de plusieurs entreprises peuvent utiliser les mêmes informations d'identification pour accéder aux réseaux de toutes les entreprises du groupe. En cas d'attaque, cette situation augmente sa portée et la probabilité d'un effet domino.

L'identité fédérée relie l'identité électronique d'un sujet à plusieurs systèmes distincts de gestion des identifications. Par exemple, un sujet peut se connecter à Yahoo! avec ses informations d'identification Google ou Facebook. C'est un exemple de connexion sociale.

La gestion des identités fédérées a pour objectif de partager automatiquement les informations d'identification à plus grande échelle. Du point de vue de l'utilisateur, cela implique une connexion unique au web.Il est impératif que les entreprises étudient de près les informations d'identification partagées avec leurs partenaires. Les numéros de sécurité sociale, les noms et les adresses sont autant d'informations que les voleurs d'identité peuvent dérober aux partenaires pour perpétrer une fraude. Pour protéger les identités fédérées, il convient généralement de relier les autorisations de connexion à un appareil autorisé.

VI.4 Les conséquences d'une brèche dans la sécurité :

Il n'est pas possible de protéger une entreprise contre toute cyberattaque potentielle, et ce, pour certaines raisons. L'expertise nécessaire pour configurer le réseau et assurer sa sécurité peut être très chère. Les agresseurs découvriront toujours de nouvelles méthodes pour cibler les

réseaux. À terme, ils réussiront une cyberattaque avancée et ciblée. La priorité sera alors de déterminer à quelle vitesse votre équipe de sécurité peut répondre à l'attaque pour minimiser les pertes de données, le temps d'arrêt et la perte de chiffre d'affaires.

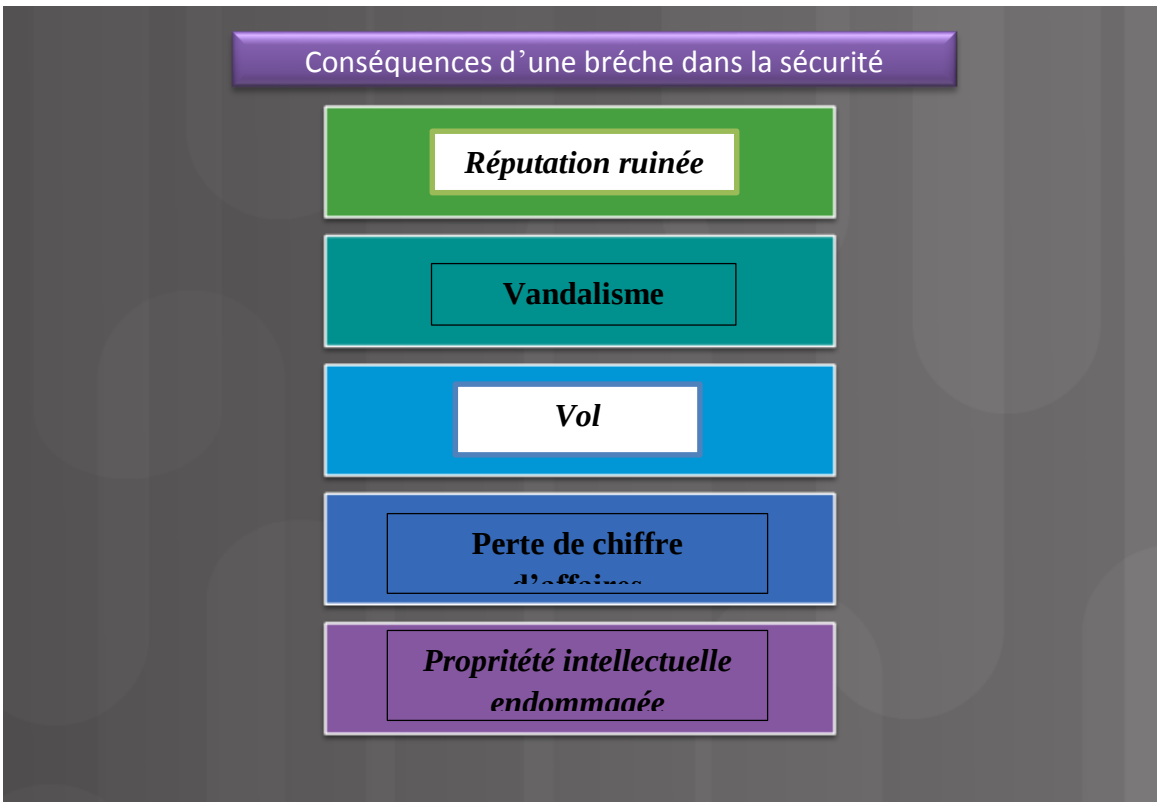


Figure VI-2: Conséquences d'une bréche dans la sécurité

Si les serveurs ont été piratés, les informations personnelles confidentielles peuvent devenir publiques. Un pirate informatique (ou un groupe de pirates) peut vandaliser le site Web d'une entreprise en publiant de fausses informations et ainsi, ruiner la réputation de cette entreprise qu'elle a mis des années à bâtir. Les pirates peuvent également arrêter le site Web de la société et lui causer des pertes du chiffre d'affaires. Si le site Web est en panne sur de plus longues périodes, l'entreprise peut paraître peu fiable et perdra éventuellement en crédibilité. Si le site Web ou le réseau de la société a été violé, cela pourrait entraîner la fuite de documents confidentiels, la révélation de secrets commerciaux et le vol de propriété intellectuelle. La perte de toutes ces informations peut entraver la croissance et l'expansion de l'entreprise.

Le coût d'une brèche est largement plus élevé que le remplacement des périphériques perdus ou volés, l'investissement dans la sécurité existante et le renforcement de la sécurité physique du bâtiment. L'entreprise peut être chargée d'informer tous les clients concernés de la brèche et pourrait avoir à faire face à des procédures judiciaires. Avec toute cette tourmente, les employés peuvent choisir de quitter l'entreprise. L'entreprise peut avoir besoin de se concentrer davantage sur la réparation de sa réputation que sur sa croissance.

VII. Les différents types de menaces :

VII.1 Les menaces Générale :

VII.1.1 Malware :

Le terme « malware » (ou programme malveillant) désigne un logiciel conçu pour perturber le bon fonctionnement d'un ordinateur ou obtenir l'accès à des systèmes informatiques à l'insu ou sans l'autorisation de l'utilisateur. Aujourd'hui, il est utilisé comme terme générique pour décrire tout logiciel hostile ou intrusif. Les virus informatiques, vers, chevaux de Troie, ransomwares, logiciels espions, logiciels publicitaires, scarewares et autres programmes malveillants sont autant d'exemples de malwares. Dans certains cas, la détection d'un malware ne pose aucun problème. Dans d'autres, en revanche, le malware peut être très discret et pratiquement impossible à détecter. ce qui suit Les types de programmes malveillants :

VII.1.1.1 Virus, vers et chevaux de Troie

Les cybercriminels ciblent les appareils des utilisateurs en y installant un malware.

VII.1.1.1.1 Virus :

Un virus est un code exécutable malveillant attaché à un autre fichier exécutable, tel qu'un programme légitime. La plupart des virus doivent être lancés par l'utilisateur et peuvent s'activer à une heure ou une date spécifique. Les trois modes de diffusion des virus informatiques sont les suivants : supports amovibles, téléchargements effectués sur Internet et pièces jointes dans un e-mail. Les virus peuvent être inoffensifs et afficher simplement une image, ou ils peuvent être destructeurs, comme ceux qui modifient ou suppriment des données. Pour éviter d'être détecté, un virus mute. Le simple fait d'ouvrir un fichier peut déclencher un virus. Un virus de secteur d'amorçage, ou de système de fichiers, infecte les clés USB et peut affecter le disque dur du système. L'exécution d'un programme spécifique peut activer un virus de programme. Une fois actif, ce virus infecte généralement d'autres programmes sur l'ordinateur qui l'héberge ou sur d'autres ordinateurs du réseau. Melissa est un exemple célèbre de virus diffusé par e-mail. Melissa a touché des dizaines de milliers d'utilisateurs et causé des dégâts estimés à 1,2 milliard de dollars.

VII.1.1.1.2 VERS :

Les vers sont des codes malveillants qui se répliquent en exploitant de façon indépendante les vulnérabilités au sein des réseaux. Les vers ralentissent généralement les réseaux. Alors que le virus nécessite un programme hôte pour s'exécuter, les vers peuvent fonctionner par eux-mêmes. À l'exception de l'infection initiale, les vers n'ont plus besoin d'intervention extérieure. Dès qu'un ver a infecté un hôte, il peut se répandre très rapidement sur le réseau. Les vers partagent des modèles similaires. Ils s'activent par la présence d'une vulnérabilité, un moyen pour eux de se propager et contiennent tous une charge utile.

Les vers sont responsables de certaines des attaques les plus dévastatrices sur Internet. En 2001, par exemple, le ver Code Red a frappé 658 serveurs. 19 heures plus tard, plus de 300 000 serveurs étaient infectés.

VII.1.1.1.3 CHEVAL DE TROIE :

Un cheval de Troie est un type de malware qui effectue des opérations malveillantes sous le couvert d'une opération souhaitée ; jouer à un jeu en ligne, par exemple. Ce code malveillant exploite les privilèges de l'utilisateur qui l'exécute. Un cheval de Troie est différent d'un virus parce qu'il se lie à des fichiers non exécutables, comme des fichiers images, audio ou des jeux.

VII.1.1.2 Bombes logiques :

Une bombe logique est un programme malveillant qui utilise un élément déclencheur pour réveiller le code malveillant. Par exemple, il peut se déclencher à certaines dates ou heures, lors de l'exécution d'autres programmes ou à la suppression d'un compte utilisateur. La bombe logique reste inactive jusqu'à l'événement déclencheur. Après activation, elle implémente un code malveillant qui endommage l'ordinateur. Une bombe logique peut saboter des enregistrements de base de données, effacer des fichiers et attaquer des systèmes d'exploitation ou des applications. Des administrateurs de sécurité réseaux ont récemment découvert des bombes logiques qui attaquent et détruisent les composants matériels d'un poste de travail ou d'un serveur, tels que les ventilateurs, le processeur, la mémoire, les disques durs et les systèmes d'alimentation. Les bombes logiques surchargent les appareils jusqu'à ce qu'ils surchauffent ou tombent en panne.

VII.1.1.3 Ransomware :

Un ransomware prend en otage un système informatique, ou les données qu'il héberge, jusqu'à ce que la victime verse une rançon. En général, le ransomware chiffre les données sur l'ordinateur à l'aide d'une clé inconnue de l'utilisateur. Ce dernier doit alors verser une rançon aux criminels pour lever la restriction.

D'autres versions de ransomware peuvent tirer parti des vulnérabilités spécifiques du système pour le verrouiller. Un ransomware se propage sous la forme d'un cheval de Troie. Il est le résultat d'un fichier téléchargé ou d'une faiblesse logicielle. L'objectif poursuivi par le cybercriminel est toujours le versement d'une rançon par le biais d'un système de paiement intraçable. Une fois le paiement effectué, le criminel fournit un programme qui permet de déchiffrer les données ou envoie un code de déblocage.

VII.1.1.4 Portes dérobées et rootkits :

Le terme « porte dérobée » fait référence au programme ou code introduit par un criminel qui a infiltré un système. La porte dérobée contourne le système d'authentification normal utilisé pour accéder à un système. NetBus et Back Orifice sont des programmes bien connus qui permettent à des utilisateurs non autorisés d'accéder à distance à un système. L'objectif d'une porte dérobée est de permettre aux cybercriminels d'accéder plus tard au système, même si l'entreprise corrige la vulnérabilité utilisée initialement pour attaquer le système. En règle

générale, les cybercriminels font en sorte que des utilisateurs autorisés exécutent, à leur insu, un cheval de Troie sur leur ordinateur afin d'installer une porte dérobée.

Un rootkit modifie le système d'exploitation pour créer une porte dérobée. Les agresseurs utilisent ainsi la porte dérobée pour accéder à distance à l'ordinateur. La plupart des rootkits profitent des vulnérabilités des logiciels pour effectuer une élévation de privilèges et modifier les fichiers système. L'élévation des privilèges exploite les erreurs de programmation ou les défauts de conception pour accorder au cybercriminel un accès élevé aux données et ressources du réseau. Il est également fréquent que les rootkits modifient les investigations du système et les outils de surveillance, ce qui rend très difficile leur détection. En cas d'infection par un rootkit, l'utilisateur doit généralement nettoyer et réinstaller le système d'exploitation du système.

VII.1.1.5 Bot :

Du mot robot, un bot est un type de malware conçu pour effectuer automatiquement une action, généralement en ligne. Alors que la plupart des bots sont inoffensifs, une utilisation croissante des bots malveillants constitue des réseaux de zombies. Plusieurs ordinateurs sont infectés de bots programmés pour attendre tranquillement les commandes fournies par l'agresseur.

VII.1.1.6 L'homme au milieu (MITM) :

L'attaque Man-in-the-Middle permet à l'agresseur de prendre le contrôle d'un appareil à l'insu de son utilisateur. Avec ce niveau d'accès, le pirate peut intercepter et s'emparer des informations de l'utilisateur avant de les relayer vers sa destination prévue. Les attaques MitM sont largement utilisées pour dérober des informations financières. De nombreux malware et des techniques existent pour permettre aux agresseurs d'avoir les fonctionnalités MitM.

VII.1.1.7 L'homme sur appareil mobile (MITMo) :

Une variante du MitM, MitMo est un type d'attaque utilisé pour prendre le contrôle d'un terminal mobile. Après l'infection, le terminal mobile peut recevoir l'instruction d'exfiltrer des informations sensibles de l'utilisateur et de les envoyer aux agresseurs. ZeuS, un exemple d'exploit avec des fonctionnalités MitMo, permet aux pirates de s'emparer discrètement des messages de vérification à 2 étapes envoyés aux utilisateurs. ar exemple, lorsqu'un utilisateur configure un identifiant Apple, il est invité à fournir un numéro de téléphone auquel sera envoyé un code de vérification temporaire par SMS afin de prouver son identité. Les malwares espionnent ce type de communication et transmettent les informations obtenues aux criminels.

VII.1.1.8 Les symptômes du malware :

Quel que soit le type de malware infectant le système, voici les symptômes communs des malware :

- Augmentation de l'utilisation du CPU
- Diminution de la vitesse de l'ordinateur
- L'ordinateur se fige ou tombe souvent en panne

- Diminution de la vitesse de navigation sur Internet
- Problèmes inexplicables avec les connexions réseau
- Des fichiers sont modifiés
- Des fichiers sont supprimés
- présence de fichiers, de programmes ou d'icônes de bureau inconnus ;
- Des processus inconnus sont exécutés
- Des programmes s'éteignent ou se reconfigurent
- Envoi d'e-mail à l'insu de l'utilisateur ou sans son consentement

VII.1.1.9 Protection contre les malwares :

Voici quelques outils et conseils permettant de se protéger contre toutes les formes de malwares, plus de détail sera effectué sur mesure de sécurité :

VII.1.1.9.1 Programme antivirus :

la majorité des solutions antivirus détectent les formes de malware les plus répandues. Cependant, les cybercriminels développent et déploient chaque jour de nouvelles menaces. Pour disposer d'une solution antivirus efficace, il faut donc veiller à ce que les signatures soient toujours à jour. Une signature est semblable à une empreinte digitale. Elle identifie les caractéristiques d'un code malveillant.

VII.1.1.9.2 Logiciels à jour:

pour commettre leurs méfaits, de nombreuses formes de malwares exploitent les vulnérabilités logicielles, tant au niveau du système d'exploitation que des applications. Alors que les vulnérabilités du système d'exploitation étaient autrefois la principale source de problèmes, les faiblesses au niveau des applications présentent, aujourd'hui, le plus grand risque en matière de sécurité. Malheureusement, force est de constater que les fournisseurs d'applications ne sont pas aussi réactifs que les éditeurs de système d'exploitation pour proposer des correctifs.

VII.1.2 Attaques par e-mail et via le navigateur:

VII.1.2.1 Attaques messagerie:

VII.1.2.1.1 Courrier indésirable :

Des milliards de personnes utilisent des services de messagerie dans le monde entier. Ce service étant l'un des plus populaires, il constitue l'une des plus grandes vulnérabilités des utilisateurs et des entreprises. Un courrier indésirable (ou « spam ») est un e-mail non sollicité. Dans la plupart des cas, le courrier indésirable est une forme de publicité. Toutefois, un courrier indésirable peut comporter des liens malveillants, un malware ou un contenu trompeur. L'objectif ultime est d'obtenir des informations sensibles, comme un numéro de sécurité sociale ou de compte bancaire. Les courriers indésirables (ou spam) proviennent généralement de plusieurs ordinateurs infectés par un virus ou un ver. Ces ordinateurs envoient autant d'e-mails que possible.

Mais même avec ces fonctionnalités de sécurité, certains messages peuvent passer entre les mailles du filet. Soyez vigilant et vérifiez les éléments suspects suivants :

- E-mail sans objet

- E-mail demandant des informations sur un compte
- E-mail contenant des mots mal orthographiés ou une ponctuation inhabituelle
- E-mail contenant des liens très longs ou difficiles à lire
- E-mail ayant l'apparence d'une correspondance émanant d'une entreprise connue
- E-mail demandant expressément à l'utilisateur d'ouvrir une pièce jointe

Si un utilisateur reçoit un e-mail contenant un ou plusieurs de ces indicateurs, il doit s'abstenir d'ouvrir le message et les éventuelles pièces jointes. La politique de messagerie d'une entreprise exige généralement qu'un utilisateur qui reçoit ce type d'e-mail en informe le personnel en charge de la cybersécurité. Pratiquement tous les fournisseurs de messagerie filtrent le courrier indésirable. Malheureusement, ce type de courrier consomme de la bande passante et le serveur du destinataire doit traiter le message.

VII.1.2.1.2 Logiciel espion « spyware », logiciel publicitaire « adware », et scareware :

Un logiciel espion (ou spyware) est un logiciel qui permet à un cybercriminel d'obtenir des informations sur les activités informatiques d'un utilisateur. Le logiciel espion inclut souvent le suivi des activités, la collecte de frappes sur clavier et la capture des données. Afin de contourner les mesures de sécurité, le logiciel espion modifie souvent les paramètres de sécurité. Le logiciel espion se regroupe souvent avec des logiciels légitimes ou avec des chevaux de Troie. De nombreux sites de partagiciels (ou sharewares) regorgent de logiciels espions.

Un logiciel publicitaire affiche généralement des fenêtres publicitaires intempestives afin de générer des revenus pour son développeur. Le malware analyse les centres d'intérêt des utilisateurs surveillant les sites web visités. Il envoie ensuite des publicités contextuelles relatives à ces sites. Certaines versions de logiciels installent automatiquement des logiciels publicitaires. Certains sont conçus pour ne diffuser que des publicités, mais il est également fréquent que d'autres soient associés à des logiciels espions.

Le scareware convainc l'utilisateur d'effectuer une action donnée en jouant sur la peur. Le scareware crée des fenêtres contextuelles factices avec la même apparence que les boîtes de dialogue du système d'exploitation. Ces fenêtres transmettent de faux messages indiquant que le système est vulnérable ou a besoin de l'exécution d'un programme spécifique pour reprendre un fonctionnement normal. En réalité, il n'existe aucune menace. Cependant, si l'utilisateur cède à la pression et autorise le programme mentionné à s'exécuter, le malware infecte son système.

VII.1.2.1.3 Phishing :

Le phishing est une forme de fraude. Les cybercriminels se servent des e-mails, de la messagerie instantanée ou d'autres réseaux sociaux pour essayer de recueillir des informations, comme les informations de connexion ou des informations relatives au compte des utilisateurs, en se faisant passer pour une entité ou une personne fiable. Le phishing consiste à envoyer un e-mail frauduleux comme s'il provenait d'une source de confiance légitime. L'objectif du

message est de piéger le destinataire pour qu'il installe un malware sur son appareil ou partage des informations personnelles ou d'ordre financier. Un exemple d'hameçonnage est un e-mail factice ayant l'apparence de celui envoyé par un magasin, demandant à l'utilisateur de cliquer sur un lien pour demander un prix. Le lien peut diriger vers un faux site demandant des informations personnelles, ou installer un virus.

L'hameçonnage ciblé est une attaque d'hameçonnage très ciblée. Même si le phishing et le phishing ciblé utilisent tous les deux des e-mails pour atteindre les victimes, le phishing ciblé personnalise les e-mails visant ainsi une personne spécifique. Le cybercriminel recherche les intérêts de la cible avant d'envoyer l'e-mail. Par exemple, un cybercriminel apprend que la cible s'intéresse aux voitures et qu'il recherchait un modèle spécifique de voiture. Le cybercriminel rejoint le même forum de discussion sur les voitures où la cible est membre, crée une fausse mise en vente de voiture et envoie un courrier électronique à la cible. L'e-mail contient un lien vers les photos de la voiture. Lorsque l'utilisateur ciblé clique sur le lien, il installe, à son insu, un malware sur son ordinateur.

VII.1.2.1.4 Phishing vocal, phishing par SMS (SMiShing), détournement de domaine et whaling :

Le phishing vocal (ou vishing) utilise la technologie de communication vocale. Les criminels peuvent usurper l'identité de sources légitimes en passant des appels via la technologie VoIP (voix sur IP). Les victimes peuvent également recevoir un message enregistré qui leur semble légitime. Les criminels souhaitent obtenir des numéros de carte de crédit ou d'autres informations afin de voler l'identité de la victime. Cette technique de phishing exploite la confiance du public envers le réseau téléphonique.

Le SMiShing est un type de phishing qui utilise des messages texte (SMS) sur des téléphones mobiles. Les criminels usurpent l'identité d'un contact légitime dans le but de gagner la confiance de la victime. Une attaque de ce type consiste, par exemple, à envoyer un lien de site web à la victime. Lorsque la victime consulte le site web en question, le malware est installé sur son téléphone mobile.

Le détournement de domaine (ou pharming) consiste à attirer la victime sur un site web maquillé de façon à ressembler à un site web légitime pour l'inciter, par la ruse, à saisir ses informations d'identification.

Le whaling est une technique de phishing qui cible les « gros poissons », en l'occurrence les dirigeants d'une entreprise. Les politiques et les célébrités peuvent également être la cible de ces attaques.

VII.1.2.2 Plug-ins et empoisonnement du navigateur :

Les failles de sécurité peuvent affecter les navigateurs web en affichant des fenêtres publicitaires, en collectant des informations permettant d'identifier une personne ou encore en

installant des logiciels publicitaires, des virus ou des logiciels espions. Un cybercriminel peut pirater le fichier exécutable d'un navigateur, ses composants ou ses plug-ins.

VII.1.2.2.1 Plugins :

Les plug-ins Flash et Shockwave d'Adobe permettent de développer de superbes animations qui améliorent sensiblement l'apparence d'une page web. Les plug-ins affichent le contenu développé à l'aide d'un logiciel approprié.

Jusqu'il y a peu, les plug-ins offraient un niveau de sécurité remarquable. Cependant, constatant la popularité du contenu Flash, les criminels ont examiné les logiciels et plug-ins Flash, détecté les vulnérabilités et exploité Flash Player. Une exploitation réussie peut entraîner une panne du système ou autoriser un criminel à prendre le contrôle du système infecté. On peut s'attendre à une augmentation des pertes de données à mesure que les criminels continueront d'étudier les protocoles et plug-ins populaires à la recherche de vulnérabilités.

VII.1.2.2.2 EMPOISONNEMENT PAR SEO :

Les moteurs de recherche comme Google fonctionnent en classant des pages et en présentant les résultats pertinents en fonction des requêtes de recherche des utilisateurs. En fonction de la pertinence du contenu du site Web, celui-ci peut se situer plus haut ou plus bas sur la liste des résultats de recherche. L'optimisation pour les moteurs de recherche ou SEO est un ensemble de techniques utilisées pour améliorer le classement d'un site Web par un moteur de recherche. Alors que de nombreuses entreprises légitimes se spécialisent dans l'optimisation de sites web pour un meilleur positionnement, l'empoisonnement par SEO (Search Engine Optimization) utilise la technologie de SEO afin de faire apparaître un site web malveillant en tête des résultats de recherche.

L'objectif le plus commun de l'empoisonnement par SEO est d'augmenter le trafic vers des sites malveillants qui peuvent héberger un malware ou effectuer une ingénierie sociale. Pour forcer un site malveillant à se classer au sommet des résultats de recherche, les agresseurs tirent parti des termes de recherche populaires.

VII.1.2.2.3 Piratage de navigateur :

Un pirate de navigateur est un malware qui modifie les paramètres du navigateur afin de rediriger l'utilisateur vers des sites web financés par les clients du cybercriminel. En règle générale, ces programmes sont installés à l'insu de l'utilisateur et font partie d'un téléchargement de type « drive-by ». Un téléchargement de type « drive-by » est un programme qui se télécharge automatiquement sur un ordinateur lorsqu'un utilisateur consulte un site web ou affiche un message électronique au format HTML. Pour éviter ce type de malware, lisez toujours attentivement les contrats d'utilisation lorsque vous téléchargez des programmes.

VII.1.2.3 Protection contre les attaques par e-mail et via le navigateur :

Il existe plusieurs méthodes pour lutter contre le courrier indésirable : filtrer les e-mails, apprendre aux utilisateurs à se méfier des e-mails envoyés par des inconnus ou encore utiliser des filtres d'hôte/serveur, S'il est difficile d'éradiquer le spam, certaines méthodes permettent

toutefois d'en limiter les effets. Par exemple, la plupart des fournisseurs d'accès Internet filtrent le courrier indésirable avant qu'il n'arrive dans la boîte de réception de l'utilisateur. De nombreux logiciels antivirus et de messagerie procèdent à un filtrage automatique des e-mails. Cela signifie qu'ils détectent et suppriment le courrier indésirable de la boîte de réception.

Les entreprises doivent également informer leurs employés des dangers que représentent les pièces jointes aux e-mails, qui peuvent contenir un virus ou un ver informatique. Soyez vigilant avec les pièces jointes des e-mails, même si les messages proviennent d'un contact de confiance. Il se peut qu'un virus tente de se propager en utilisant l'ordinateur de l'expéditeur. Analysez toujours les pièces jointes avec un programme antivirus avant de les ouvrir.

L'Anti-Phishing Working Group (APWG) est une association industrielle qui s'attache à éliminer l'usurpation d'identité et la fraude dues au phishing et à l'usurpation d'adresse électronique.

Encore une fois la mise à jour des logiciels permet de s'assurer que le système dispose de tous les correctifs de sécurité nécessaires pour éliminer les vulnérabilités connues.

VII.2 Les menaces applicatives :

VII.2.1 Cross-site Scripting :

Le cross-site scripting (XSS) est une vulnérabilité découverte dans les applications web. XSS permet aux hackers d'injecter des scripts dans les pages web visionnées par les utilisateurs. Ce script peut contenir du code malveillant.

Les scripts multisites nécessitent l'intervention de trois participants : le hacker, la victime et le site web. Le cybercriminel ne cible pas directement une victime. Il exploite la vulnérabilité d'un site ou d'une application web. Les hackers injectent des scripts côté client dans des pages web visionnées par les utilisateurs, qui deviennent alors victimes. Le script malveillant est transmis subrepticement au navigateur de l'utilisateur. Un script malveillant de ce type peut accéder à des cookies, à des jetons de session ou à d'autres informations sensibles. Si les criminels obtiennent le cookie de session de la victime, ils peuvent usurper son identité.

VII.2.2 Injection de code :

Une base de données permet de stocker des données sur un site web. Il existe plusieurs types de bases de données, comme les bases de données SQL (Structured Query Language) ou XML (Extensible Markup Language). Les attaques par injection de code XML et SQL tirent profit des faiblesses d'un programme, comme l'absence d'une validation appropriée des requêtes de bases de données.

VII.2.2.1 Injection XML :

Lors de l'utilisation d'une base de données XML, une injection XML désigne une attaque susceptible de corrompre les données. Dès que l'utilisateur a saisi des informations, le système accède aux données requises par le biais d'une requête. Le problème se produit lorsque le système n'analyse pas correctement la demande de saisie fournie par l'utilisateur. Les criminels peuvent programmer la requête pour l'adapter à leurs besoins et accéder aux informations de la base de données.

Ils ont alors accès à toutes les données sensibles stockées dans la base de données et peuvent apporter au site web toutes les modifications qu'ils désirent. Une attaque par injection de XML menace la sécurité du site web.

VII.2.2.2 Injection SQL :

Les cybercriminels exploitent une vulnérabilité en insérant une instruction SQL malveillante dans un champ de saisie. Ici encore, le système ne filtre pas correctement les informations saisies par l'utilisateur à la recherche des caractères d'une instruction SQL. Les criminels utilisent l'injection de code SQL sur des sites web ou sur toute base de données SQL.

L'exemple suivant va interroger une table qui contient la liste des cartes bancaires enregistrées dans la base de données de l'application Web d'un site marchand. Le script de création de cette table est le suivant :

```
CREATE TABLE IF NOT EXISTS `comptes` (
`id` int(11) NOT NULL AUTO_INCREMENT COMMENT 'identifiant',
`nom` varchar(30) NOT NULL COMMENT 'nom d''utilisateur',
`motdepasse` varchar(41) NOT NULL,
`typecarte` varchar(30) NOT NULL COMMENT 'type de carte',
`numerocarte` varchar(30) NOT NULL COMMENT 'numéro de carte',
PRIMARY KEY (`id`),
UNIQUE KEY `nom` (`nom`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=5 ;
```

Figure VII-1: Script SQL de création de la table « comptes »

Donc ils peuvent usurper une identité, modifier des données existantes, détruire des données ou bien devenir les administrateurs du serveur de base de données.

VII.2.2.3 injection de XPath:

L'attaque par injection de XPath suit le même principe que pour SQL. En effet, XPath est un langage de requête pour gérer les données stockées au format XML, comme le fait SQL pour les bases de données relationnelles. XPath et Xquery, dont XPath est un sous-ensemble, souffrent donc des mêmes vulnérabilités face à l'injection de code malicieux.

VII.2.2.4 Injection LDAP :

L'injection LDAP est une attaque utilisée pour exploiter des applications Web qui construisent des instructions LDAP basées sur l'entrée de l'utilisateur.

Le protocole LDAP (Lightweight Directory Access Protocol) permet d'accéder à des bases d'informations sur les utilisateurs d'un réseau, via l'interrogation d'annuaires. Il utilise pour cela un autre protocole, TCP/IP.

L'attaque par injection LDAP permet d'accéder à des informations privées qui sont enregistrées dans l'annuaire d'entreprise. En modifiant le comportement du filtrage dans la requête LDAP qui sera générée, il est possible de récupérer la liste exhaustive des adresses de courrier électronique d'une entreprise pour les saturer de spam par exemple. (9)

VII.2.3 Dépassement de la mémoire tampon :

Un buffer overflow se produit lorsque des données dépassent les limites d'un tampon. Les tampons sont des zones de mémoire affectées à une application. En modifiant les données au-delà des limites d'une mémoire tampon, l'application accède à la mémoire allouée à d'autres processus. Cela peut provoquer une panne du système, une compromission des données ou permettre une élévation des privilèges.

Selon les estimations du CERT Coordination Center (CERT/CC) de l'université Carnegie-Mellon, près de 50 % de tous les exploits de programmes informatiques trouvent leur origine dans une forme quelconque de buffer overflow. La classification générique des buffer overflows comprend de nombreuses variantes, telles que les dépassements de mémoire tampon statique, les erreurs d'indexation, les bogues de chaîne de format, les différences de taille de tampon Unicode et ANSI ou encore les dépassements de tas.

VII.2.4 Exécution de code à distance :

Les vulnérabilités permettent aux cybercriminels d'exécuter du code malveillant et de prendre le contrôle d'un système avec les privilèges de l'utilisateur qui exécute l'application. L'exécution de code à distance permet au cybercriminel de lancer la commande de son choix sur une machine cible.

Prenons l'exemple de Metasploit, un outil conçu pour développer et exécuter du code d'exploitation sur une cible distante. Meterpreter est un module d'exploitation intégré à Metasploit qui fournit des fonctionnalités avancées. Il permet aux hackers d'écrire leurs propres extensions sous la forme d'un objet partagé. Ils peuvent ainsi télécharger et injecter ces fichiers dans un processus actif sur la cible. Meterpreter charge et exécute toutes les extensions à partir de la mémoire, de sorte qu'elles ne mettent jamais à contribution le disque dur. Cela signifie également que ces fichiers échappent à la détection des logiciels antivirus. Meterpreter comprend un module permettant de contrôler la webcam d'un ordinateur distant. Dès qu'un hacker a installé Meterpreter sur le système de sa victime, il peut voir et capturer les images diffusées par la webcam.

VII.2.5 Contrôles ActiveX et Java :

Sur Internet, il est possible que certaines pages ne s'affichent pas correctement si aucun contrôle ActiveX n'est installé. Les contrôles ActiveX dotent Internet Explorer de fonctionnalités comparables à un plug-in. Les contrôles ActiveX sont des logiciels installés par les utilisateurs pour étendre les fonctionnalités d'un programme. Certains contrôles ActiveX créés par des tiers peuvent être malveillants. Ils surveillent les habitudes de navigation de l'utilisateur, installent des malwares ou enregistrent les frappes. Les contrôles ActiveX fonctionnent également dans d'autres applications Microsoft.

Java fonctionne par le biais d'un interprète, la machine virtuelle Java (JVM). JVM permet au programme Java de fonctionner. JVM crée des sandboxes ou isole le code non fiable du reste du système d'exploitation. Certaines vulnérabilités permettent au code non fiable de contourner les restrictions imposées par la sandbox. Il existe également des vulnérabilités dans la bibliothèque de classes Java qu'une application utilise pour sa sécurité. Java occupe la deuxième place au classement des vulnérabilités de sécurité les plus sérieuses, juste derrière le plug-in Flash d'Adobe.

VII.2.6 Enregistreur de frappe :

Un enregistreur de frappe est un logiciel qui enregistre ou consigne les saisies effectuées au clavier par l'utilisateur du système. Les hackers peuvent implémenter des enregistreurs de frappe via un logiciel installé sur un système informatique ou via du matériel connecté physiquement à un ordinateur. Ils configurent le logiciel enregistreur de frappe de sorte qu'il envoie le fichier journal par e-mail. Les frappes consignées dans le fichier journal divulguent les noms d'utilisateur, les mots de passe, les sites web visités et d'autres informations sensibles.

Les enregistreurs de frappe peuvent être des logiciels légitimes, disponibles dans le commerce. Il arrive fréquemment que des parents achètent ce type de logiciel pour analyser le comportement de leurs enfants sur le Net et les sites qu'ils ont consultés. De nombreux logiciels anti-espions sont en mesure de détecter et de supprimer les enregistreurs de frappe non autorisés. Bien que les enregistreurs de frappe soient des logiciels légaux, les criminels les utilisent pour commettre des actes répréhensibles.

VII.3 Les menaces réseaux :

VII.3.1 Mystification :

La mystification est une attaque par usurpation d'identité qui tire parti d'une relation de confiance entre deux systèmes. Si les deux systèmes acceptent l'authentification réalisée par l'un d'eux, il est possible que l'utilisateur connecté à l'un des systèmes ne soit pas obligé de s'authentifier une nouvelle fois pour accéder à l'autre système. Un hacker peut profiter de cette situation en envoyant, à un système, un paquet qui semble provenir d'un système fiable. La relation de confiance étant établie, le système ciblé peut effectuer la tâche demandée sans authentification.

Il existe de nombreux types d'attaques par mystification :

- On parle de mystification d'adresse MAC lorsqu'un ordinateur accepte des paquets de données sur la base de l'adresse MAC d'un autre ordinateur.
- L'usurpation d'adresse IP est une technique qui consiste à envoyer des paquets IP à partir d'une adresse source usurpée pour masquer sa propre identité.
- ARP (Address Resolution Protocol) est un protocole qui traduit les adresses IP en adresses MAC pour transmettre des données. L'usurpation ARP envoie des messages ARP mystifiés sur un réseau local afin de lier l'adresse MAC du criminel à l'adresse IP d'un membre autorisé du réseau.
- Le système de noms de domaine (DNS) associe des noms de domaine à des adresses IP. L'usurpation de serveur DNS est une technique qui modifie le serveur DNS afin de réacheminer un nom de domaine spécifique vers une autre adresse IP contrôlée par le criminel.

VII.3.2 Déni de service :

Les attaques par déni de service représentent un type d'attaque réseau. Une attaque par déni de service (DoS) se traduit par une interruption des services de réseau pour les utilisateurs, les appareils ou les applications. Il existe deux types majeurs d'attaques par déni de service :

Volume de trafic ingérable Le hacker envoie d'énormes quantités de données à un débit que le réseau, l'hôte ou l'application n'est pas en mesure de gérer. Cela provoque un ralentissement de la transmission ou de la réponse, ou une panne d'un appareil ou d'un service.

Paquets formatés de manière malveillante – Le pirate envoie un paquet formaté de manière malveillante à un hôte ou à l'application et le destinataire est incapable de le traiter. Par exemple, une application ne peut pas identifier des paquets contenant des erreurs ou des paquets mal formatés transmis par le hacker. Cela provoque un ralentissement de l'appareil récepteur ou une panne. Elles présentent un risque majeur, car elles peuvent facilement interrompre les communications et entraîner une perte importante de temps et d'argent. Ces attaques sont relativement simples à effectuer, même par un hacker non qualifié.

L'objectif d'une attaque de déni de service est de refuser l'accès aux utilisateurs autorisés en rendant le réseau indisponible (les trois principes de sécurité sous-jacents : confidentialité, intégrité et disponibilité).

Une attaque par déni de service distribuée (attaque DDoS) est similaire à une attaque par déni de service (attaque DoS), si ce n'est qu'elle provient de sources multiples et coordonnées. À titre d'exemple, une attaque par déni de service distribuée peut procéder comme suit :

Un agresseur établit un réseau d'hôtes infectés, appelé réseau de zombies. Les (ordinateurs) zombies sont les hôtes infectés. Le hacker utilise des systèmes gestionnaires pour commander les zombies. Les ordinateurs zombies analysent et infectent constamment plus d'hôtes, et créent

ainsi plus de zombies. Une fois prêt, le hacker demande aux systèmes de gestionnaire d'effectuer une attaque par déni de service distribuée par le biais du réseau de zombies.

VII.3.3 Repérage (sniffer):

Cette technique s'apparente aux écoutes clandestines. Dans ce cas, les hackers examinent tout le trafic réseau qui transite par leur carte réseau, que le trafic leur soit adressé ou non. Les criminels interceptent ce trafic réseau à l'aide d'une application logicielle, d'un appareil ou des deux. Comme on peut le voir sur cette figure :

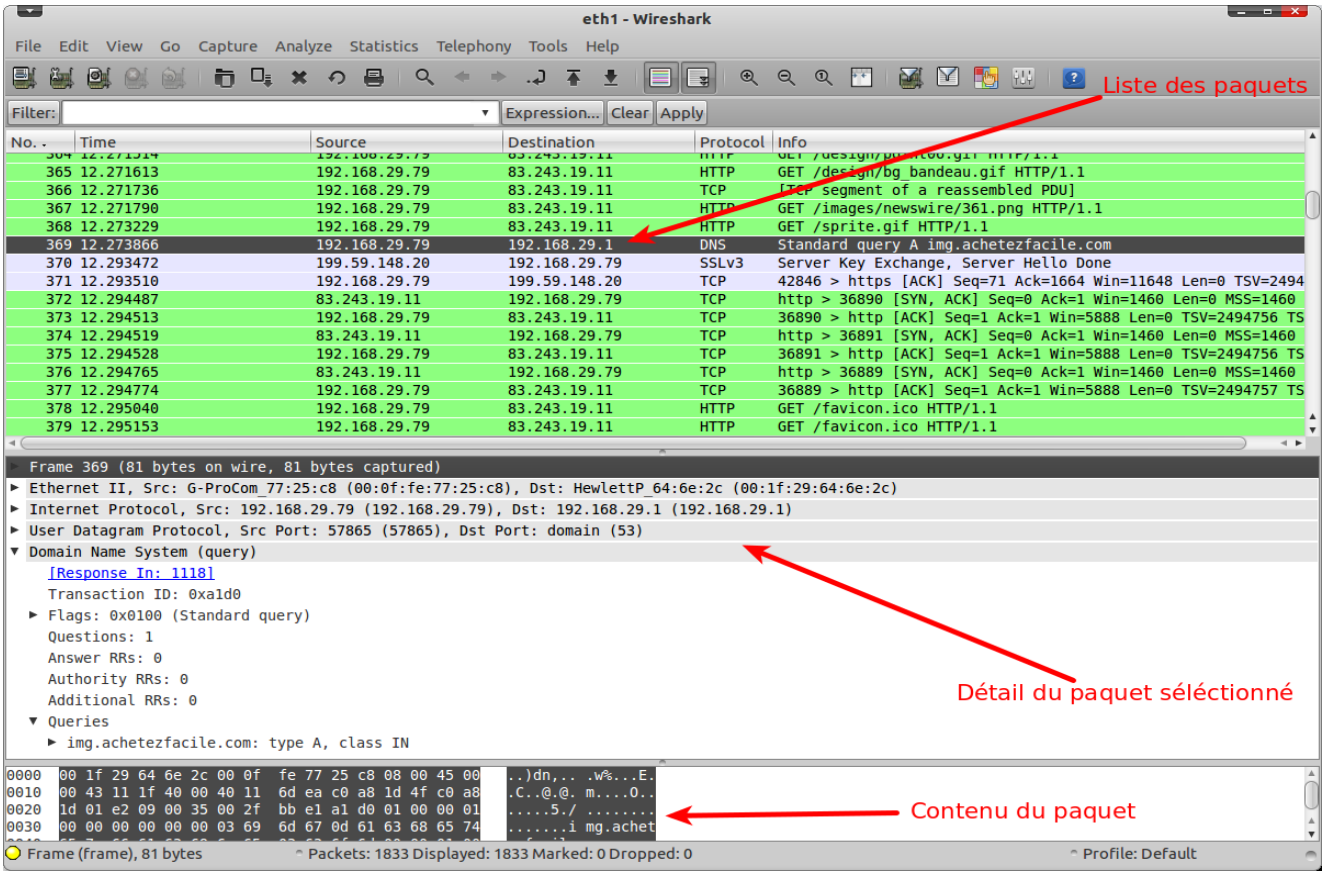


Figure VII-2: Analyse d'une trame wireshark

cette technique peut observer tout le trafic réseau ou cibler un protocole, un service, voire une chaîne de caractères spécifique, telle qu'un nom de connexion ou un mot de passe. Certains analyseurs réseau (ou sniffers) observent tout le trafic et le modifient intégralement ou en partie.

Le repérage présente également des bénéfices. Les administrateurs réseau peuvent utiliser des sniffers pour analyser le trafic réseau, identifier les problèmes de bande passante et résoudre d'autres problèmes affectant le réseau.

La sécurité physique est un facteur important pour empêcher l'introduction de sniffers sur le réseau interne.

VII.3.4 Menaces visant les terminaux sans fil et mobiles :

VII.3.4.1 Grayware et SMiShing :

Étant donné la grande popularité des smartphones, le grayware commence à poser problème dans le domaine de la sécurité mobile. Un grayware désigne les applications qui se comportent de manière indésirable ou agaçante. Il est possible que le grayware ne contienne pas de malware reconnaissable, mais il n'en est pas moins dangereux pour l'utilisateur. Un grayware peut, par exemple, suivre la position de l'utilisateur. Pour garder leur légitimité, les créateurs de graywares indiquent généralement les fonctionnalités d'une application en petits caractères dans la licence d'utilisation du logiciel. Les utilisateurs installent de nombreuses applications mobiles sans vraiment tenir compte de leurs fonctionnalités.

SMiShing désigne le phishing par SMS. Cette méthode consiste à envoyer de faux messages par SMS. Les hackers poussent les utilisateurs à visiter un site web ou à appeler un numéro de téléphone. Les victimes peu méfiantes fournissent alors des informations sensibles, comme le numéro de leur carte de crédit. En se rendant sur le site web indiqué, l'utilisateur peut télécharger à son insu un malware qui infecte son appareil.

VII.3.4.2 Points d'accès non autorisés :

Un point d'accès non autorisé est un point d'accès sans fil installé sur un réseau sécurisé sans autorisation explicite. Un point d'accès non autorisé peut être configuré de deux manières. Dans le premier cas, un employé bien intentionné essaie de se rendre utile en simplifiant la connexion des terminaux mobiles. Dans le second cas, un criminel parvient à s'infiltrer dans les locaux d'une entreprise et installe le point d'accès non autorisé. Aucune de ces actions n'étant autorisée, l'entreprise est, dans les deux cas, exposée à un risque.

Un point d'accès non autorisé peut également faire référence au point d'accès d'un criminel. Dans ce cas, le criminel configure le point d'accès en tant qu'appareil MitM pour intercepter les informations de connexion des utilisateurs , Dans le cas d'un phishing au point d'accès (ou attaque Evil Twin), l'intensité et la puissance du signal du point d'accès du criminel sont améliorées, de sorte qu'il apparaisse comme une meilleure option de connexion pour l'utilisateur. Une fois l'utilisateur connecté au point d'accès frauduleux, les criminels peuvent analyser le trafic et mener des attaques MitM.

VII.3.4.3 Brouillage par radiofréquence :

Les signaux sans fil sont sensibles aux interférences électromagnétiques et aux interférences sur les fréquences radioélectriques. Elles peuvent même être sensibles à la foudre ou au « bruit » des lampes fluorescentes. Les signaux sans fil sont également susceptibles de provoquer un brouillage délibéré. Le brouillage par radiofréquence perturbe la transmission d'une station radio ou satellite, ce qui empêche le signal d'atteindre son destinataire.

Pour brouiller le signal sans fil, la fréquence, la modulation et la puissance du brouilleur radio doivent être égales à celles de l'appareil que le criminel souhaite perturber.

VII.3.4.4 Bluejacking et bluesnarfing :

Bluetooth est un protocole de faible puissance et de faible portée. La technologie Bluetooth transmet des données au sein d'un réseau personnel (PAN). Elle est utilisée par des appareils tels que des téléphones mobiles, des ordinateurs portables et des imprimantes. Plusieurs versions du protocole Bluetooth ont déjà été publiées. Le Bluetooth se caractérise par sa facilité de configuration ; aucune adresse réseau n'est ainsi nécessaire. Une procédure de couplage est utilisée pour établir la connexion entre les appareils. Lors de cette procédure, les deux appareils utilisent le même code d'accès ,Des vulnérabilités ont certes été mises au jour mais, en raison de la portée limitée de la technologie Bluetooth, la victime et le hacker doivent se trouver à proximité l'un de l'autre.

Bluejacking est un terme qui désigne l'envoi de messages non sollicités vers un autre appareil Bluetooth. Une variante de cette technique consiste à envoyer une image choquante.

Dans le cas du bluesnarfing, le hacker copie les données de la victime depuis son appareil. Il peut s'agir, par exemple, des e-mails et des listes de contacts.

VII.3.4.5 Les attaques WEP et WPA :

WEP (Wired Equivalent Privacy) est un protocole de sécurité conçu pour garantir à un réseau sans fil (WLAN) le même niveau de sécurité qu'un réseau filaire. Des mesures de sécurité physique contribuent à protéger un réseau LAN filaire. WEP cherche à proposer une protection similaire pour les données transmises via le WLAN grâce au chiffrement.

WEP utilise une clé pour le chiffrement. Il n'existe aucune disposition concernant la gestion des clés WEP, c'est pourquoi le nombre de personnes qui partagent une clé ne cesse d'augmenter. Étant donné que tout le monde utilise la même clé, le criminel a accès à un plus grand volume de trafic pour les attaques analytiques.

Le vecteur d'initialisation (IV), qui est l'un des composants du système cryptographique, pose également quelques problèmes au protocole WEP :

- ☞ Il s'agit d'un champ de 24 bits, ce qui est trop peu.
- ☞ Il s'agit de texte en clair, ce qui signifie qu'il est lisible.
- ☞ Il est statique ; des flux de clés identiques se répètent donc sur un réseau chargé.

Le protocole WPA (Wi-Fi Protected Access) et, plus tard, le protocole WPA2 ont été publiés en remplacement du protocole WEP. WPA2 ne pose pas les mêmes problèmes de chiffrement, car un hacker ne peut pas récupérer la clé simplement en observant le trafic. WPA2 est susceptible d'être attaqué parce que les cybercriminels peuvent analyser les paquets qui transitent entre le point d'accès et un utilisateur légitime. Les cybercriminels utilisent un analyseur de paquets, puis lancent les attaques hors ligne au niveau du mot de passe. (10)

VII.4 Attaque mixte :

Les attaques mixtes sont des attaques qui utilisent les différents types de menaces pour compromettre une cible. En utilisant plusieurs techniques d'attaque différentes simultanément,

les agresseurs disposent de malware qui représentent un mélange de vers, de chevaux de Troie, de logiciels espions, d'enregistreurs de frappe, de pourriels et de plans d'hameçonnage. Cette tendance des attaques mixtes est révélatrice de malware plus complexes et met les données des utilisateurs en grand danger.

Le type d'attaque mixte le plus courant utilise des pourriels, des messages instantanés ou des sites légitimes pour distribuer des liens dans lesquels un malware ou un logiciel espion est secrètement téléchargé sur l'ordinateur. Une autre attaque mixte commune utilise les attaques par déni de service distribuée combinées à des e-mails d'hameçonnage. Tout d'abord, l'attaque par déni de service distribuée est utilisée pour détraquer le site Web d'une banque populaire et envoyer des e-mails aux clients de la banque en s'excusant pour la gêne occasionnée. L'e-mail dirige également les utilisateurs vers un site d'urgence factice où leurs vraies informations de connexion peuvent être volées.

La plupart des vers informatiques les plus néfastes comme Nimbda, CodeRed, BugBear, Klez et Slammer sont davantage catégorisés comme des attaques mixtes, comme indiqué ci-dessous :

- Certaines variantes de Nimbda ont utilisé les pièces jointes d'e-mail, les téléchargements de fichier à partir d'un serveur Web compromis et le partage de fichiers Microsoft (par exemple, des partages anonymes) comme méthodes de propagation.
- D'autres variantes de Nimbda ont été en mesure de modifier les comptes invités du système pour fournir à l'agresseur ou au code malveillant des privilèges administratifs.

Les récents vers Conficker et ZeuS/LICAT étaient également des attaques mixtes. Conficker a utilisé toutes les méthodes de distribution classiques.

VIII. Les mesures de sécurité :

VIII.1 La formation des utilisateurs:

Comme on vue dans la troisième dimension du cube de mccumber, parmi les types de pouvoirs auxquels un administrateur de la sécurité réseau peut avoir recours pour protéger le réseau c'est l'éducation, la sensibilisation et la formation des utilisateurs ;

VIII.1.1 Mise en œuvre de la cybersécurité – Formation :

Consentir de gros investissements technologiques ne sert à rien si ce sont les employés de l'entreprise qui constituent le maillon faible de la chaîne de cybersécurité. C'est pourquoi il est important pour les entreprises d'élaborer un programme de sensibilisation à la sécurité. Certains collaborateurs font preuve d'un comportement malveillant sans même le savoir, simplement parce qu'ils ne connaissent pas les procédures appropriées. Il existe plusieurs manières pour mettre en œuvre un programme de formation officiel :

- Sensibilisez les nouveaux collaborateurs à la sécurité lors de leur processus d'intégration

- ☞ Ajoutez la sensibilisation à la sécurité aux conditions requises pour un poste ou aux évaluations de performances
- ☞ Réalisez des sessions de formation en présentiel-Organisez des cours en ligneLa sensibilisation à la sécurité doit être continue, car de nouvelles menaces et de nouvelles techniques font constamment leur apparition.

Figure VIII-1: Enseignement des utilisateurs

VIII.1.2 Instaurer une culture de sensibilisation à la cybersécurité :

Les membres d'une entreprise doivent connaître les politiques de sécurité en vigueur et disposer des connaissances nécessaires pour intégrer la sécurité dans leurs activités quotidiennes.

Un programme de sensibilisation à la sécurité actif dépend de plusieurs facteurs :

- ✓ Environnement de l'entreprise
- ✓ Niveau de la menace

L'instauration d'une culture de sensibilisation à la cybersécurité est une tâche continue placée sous l'autorité des cadres supérieurs et qui nécessite l'implication de l'ensemble des utilisateurs et des employés. La mise en place d'une culture de cybersécurité au sein d'une entreprise commence par l'établissement de politiques et de procédures de la part des dirigeants. De nombreuses entreprises organisent ainsi des journées de sensibilisation à la sécurité réseau. L'entreprise peut également installer des affiches et publier des bannières visant à sensibiliser

davantage les collaborateurs à cette problématique. L'organisation de séminaires et d'ateliers consacrés à la cybersécurité est également encouragée.

VIII.2 L'antivirus :

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Il faut que on Vérifie régulièrement que les antivirus des équipements sont bien à jour et faire des analyses (scans) approfondies pour vérifier que on est pas été infecté. Le programme surveille en permanence les virus. Lorsque le programme détecte un virus, il en informe l'utilisateur et tente de le mettre en quarantaine ou de le supprimer, En plus d'analyser les fichiers et assurer une protection en temps réel, elles détectent les logiciels à mettre à jour, intègrent un gestionnaire de mots de passe, nettoie et optimise certains paramètres de l'ordinateur.

Les anti-virus utilisent différentes technologies pour rechercher les virus :

- La recherche de signatures. Le logiciel analyse les fichiers pour détecter la présence d'un virus. Pour que cette méthode soit efficace il faut que la base des signatures soit régulièrement mise à jour. Cette méthode ne permet pas de détecter les virus qui utilisent une nouvelle signature, mais la rapidité (quelques heures) de réaction entre la découverte d'un nouveau virus et la mise à jour de la base permet d'arrêter la plupart des virus.

- La méthode heuristique : elle consiste à chercher des instructions suspectes à l'intérieur des fichiers en se basant sur des règles générales de reconnaissance des virus. Cela permet dedétecter aussi bien des virus connus qu'inconnus, sans effectuer de fréquentes mises à jour. Toutefois, cette méthode génère parfois de fausses alertes. L'utilisateur doit être capable de faire la différence entre les vraies et les fausses alertes.

- Le contrôle d'intégrité : lors de son installation, l'antivirus crée une base de données de tous les fichiers présents sur la machine basée sur la longueur des fichiers et d'autres paramètres. Toute modification d'un fichier fera l'objet d'une alerte.

Les logiciels antivirus combinent ces méthodes pour proposer les produits aussi performants que possible, On peut notamment citer en exemple Avira Free Security, une suite de sécurité gratuite et très bien notée sur TrustPilot, le site indépendant de recommandations des utilisateurs. En plus, cette suite logicielle a reçu des récompenses de laboratoires de tests indépendants comme AV-Test et AV-Comparative. On apprécie aussi Avira Free Security pour sa flexibilité. Son interface simple et intuitive en français et en arabe, est accessible aux utilisateurs novices tandis que les réglages avancés sauront satisfaire les utilisateurs plus expérimentés.

Avira Free Security embarque une dizaine d'outils de protection et de surveillance pour votre ordinateur sous Windows ou Mac OS X. Analyse antivirus approfondie et surveillance en temps réel, font évidemment partie de cette suite de sécurité. Cette dernière dispose également d'un VPN (Virtual Private Network), d'un pare-feu, d'un système de détection des logiciels obsolètes et de mise à jour des pilotes, et d'un nettoyeur de fichiers. Elle se complète d'un gestionnaire de mots de passe, d'un assistant d'optimisation, et d'un effaceur de données sensibles.

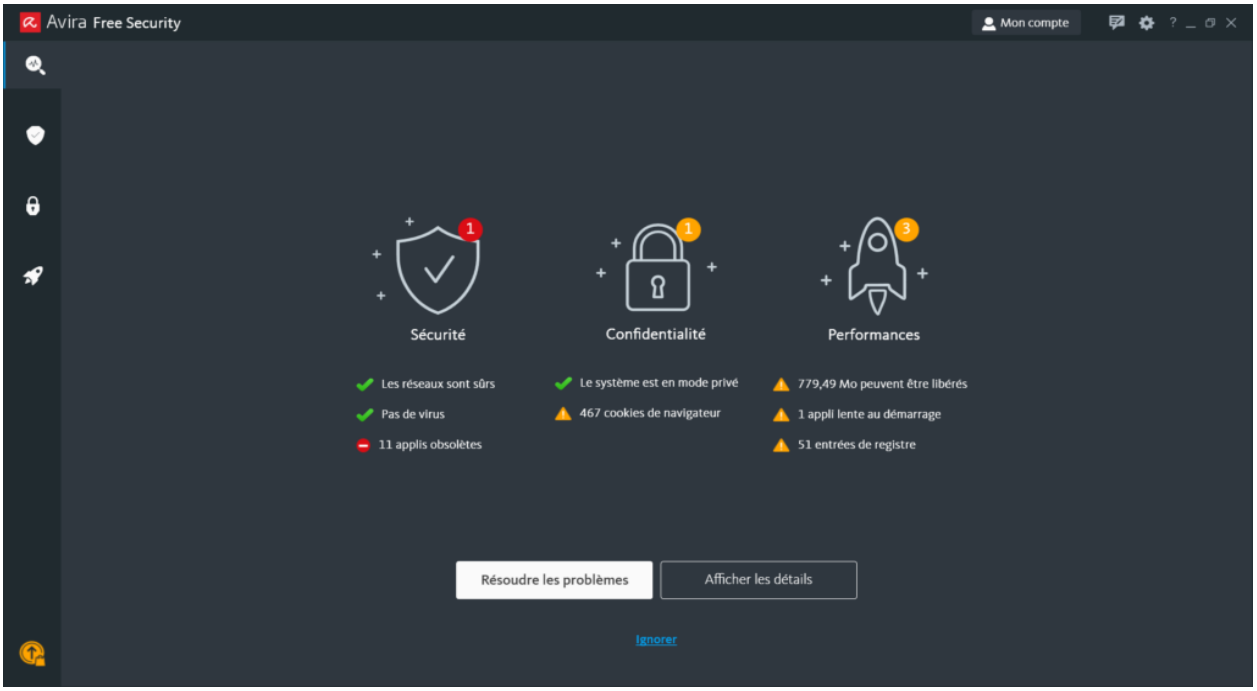


Figure VIII-2: L'interface graphiquie de l'anti-virus Avira Free Security

VIII.3 La sécurisation des postes de travail :

Le poste de travail en entreprise est la cible privilégiée des attaques informatiques. La mise en œuvre d'astuces simples et rapides de protection des postes de travail des collaborateurs constitue donc une des mesures principales pour sécuriser l'infrastructure, Avec des postes de travail mal protégés, l'entreprise prend le risque de voir ses données confidentielles subtilisées en cas de piratage. Plus grave encore, les postes peuvent devenir des portes d'entrée pour des attaques visant des systèmes plus sensibles au sein de l'entreprise. Pour se prémunir de ces risques, il existe quelques mesures simples à appliquer :

- Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
- Installer un « pare-feu » (« firewall ») logiciel, et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
- Utiliser des antivirus régulièrement mis à jour et prévoir une politique de mise à jour régulière des logiciels

- ❖ Configurer les logiciels pour que les mises à jour de sécurité se fassent automatiquement dès que cela est possible.
- ❖ Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation.
- ❖ Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable.
- ❖ Désactiver l'exécution automatique (« autorun ») depuis des supports amovibles.

Pour l'assistance sur les postes de travail :

- ✓ les outils d'administration à distance doivent recueillir l'accord de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran ;
- ✓ l'utilisateur doit également pouvoir constater si la prise de main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

Ce qu'il ne faut pas faire :

- ☮ Utiliser des systèmes d'exploitation obsolètes
- ☮ Donner des droits administrateurs aux utilisateurs n'ayant pas de compétences en sécurité informatique.

Pour aller plus loin :

- ☞ Interdire l'exécution d'applications téléchargées ne provenant pas de sources sûres.
- ☞ Limiter l'usage d'applications nécessitant des droits de niveau administrateur pour leur exécution.
- ☞ Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation à une autre personne.
- ☞ En cas de compromission d'un poste, rechercher la source ainsi que toute trace d'intrusion dans le système d'information de l'organisme, pour détecter la compromission d'autres éléments.
- ☞ Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d'information de l'organisme. Le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, publie sur son site web des alertes et des avis

sur les vulnérabilités découvertes dans des logiciels et matériels et donne, lorsque cela est possible, des moyens pour s'en prémunir.

- ☞ Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées.
- ☞ Installer les mises à jour critiques des systèmes d'exploitation sans délai en programmant une véri- fication automatique hebdomadaire.
- ☞ Diffuser à tous les utilisateurs la conduite à tenir et la liste des personnes à contacter en cas d'inci- dent de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information et de communication de l'organisme.

VIII.4 Les firewalls :

Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets), on va introduire les pares-feux en détail au chapitre suivant.

VIII.5 Les systèmes IDS/IPS :

Un système de détection d'intrusion (IDS), illustré dans la figure, est un périphérique réseau dédié ou l'un des nombreux outils dans le serveur ou dans le pare-feu qui analyse les données par rapport à une base de données de règles ou de signatures d'attaque pour détecter un trafic malveillant. Si une correspondance est détectée, l'IDS enregistrera la détection et enverra une alerte à un administrateur réseau. Le système de détection d'intrusion n'intervient pas lorsqu'une correspondance est détectée, c'est-à-dire qu'il n'empêche pas la survenue d'une attaque. La fonction de l'IDS est simplement de détecter, d'enregistrer et de rapporter. (11)

L'analyse effectuée par l'IDS ralentit le réseau (ralentissement appelé latence). Pour éviter le retard du réseau, un IDS est habituellement mis offline, séparé du trafic réseau normal. Les données sont copiées ou mises en miroir par un commutateur, puis envoyées à l'IDS pour une détection offline. Il y a également les outils IDS qui peuvent être installés en avant d'un système d'exploitation d'un ordinateur hôte, comme Linux ou Windows.

Figure VIII-3: IPS Cisco 4240

Un système de prévention des intrusions (IPS) dispose de la capacité de bloquer ou de refuser un trafic selon une règle positive et une correspondance de signature. Snort est l'un des systèmes IPS/IDS les plus connus. La version commerciale de Snort appartient à la filiale Sourcefire de Cisco. Sourcefire est capable d'effectuer une analyse en temps réel du trafic et des ports, une ouverture de session, une recherche et une mise en correspondance de contenus. Cet outil peut également détecter les sondes, les attaques et les balayages de ports. Sourcefire s'intègre également à d'autres outils tiers pour la création de rapport et pour l'analyse des performances et des enregistrements.

VIII.6 Les honypots et honynets :

Un « HoneyPot » ou « HoneyNet » (le pot de miel pour attirer les mouches) qui consiste à exhiber un leurre. ,Par des actions humaines ou des moyens logiciels, un honeypot a pour but de faire croire qu'une entreprise possède dans ses systèmes des points d'entrée qui ne sont pas correctement protégés , Un honeypot est comparable à une action de contre-espionnage dans le domaine de la cybersécurité : au moyen de leurres à l'apparence vulnérable, il attire les attaquants pour contrecarrer leurs attaques, tout en permettant d'analyser et de surveiller toutes leurs actions.

Figure VIII-4:Honeypot & Honeynet

Il s'agit d'une stratégie potentiellement utile surtout pour les grandes entreprises qui, du fait de leurs volumes importants d'activité et de données confidentielles, sont une cible de choix pour les attaquants.À titre de mesure préventive, une entreprise configure un ensemble de serveurs ou de systèmes pour qu'ils paraissent vulnérables. Il semble ainsi que l'entreprise n'a pas pris suffisamment de précautions pour certains aspects de sa sécurité. Une fois le piège posé, l'objectif consiste à attirer des attaquants.

Le criminel ne réalise cependant pas qu'il ne s'agit pas d'un point d'entrée vulnérable, mais d'un piège étroitement surveillé par l'entreprise en question.

La tactique du honeypot peut avoir trois avantages : elle confine d'abord les attaques vraiment dangereuses, elle fait ensuite perdre du temps aux attaquants, et enfin l'analyse de leurs actions lui permet de détecter de nouvelles formes d'attaques potentiellement employées dans son secteur.

En peut citer :

VIII.6.1 Pots de miel à faible interaction

Ils sont les plus simples de la famille des pots de miel. Leur but est de recueillir un maximum d'informations tout en limitant les risques en offrant un minimum de privilèges aux attaquants.

On peut ranger, par exemple, la commande netcat dans cette catégorie. **Netcat** peut écouter un port particulier et enregistrer dans un journal toutes les connexions, ainsi que les commandes entrées. Ce programme permet donc d'écrire dans un fichier toutes les commandes entrées par des agresseurs. Cependant, ce type d'écoute reste très limité car il faut exécuter la commande pour chaque port que l'on souhaite observer.

Dans la même famille, on peut citer :

Honeyd, de Niels Provost, qui est un pot de miel virtuel capable d'émuler des machines ou un réseau virtuel dans le but de leurrer les hackers. C'est l'un des pots de miel à faible interaction qui offre le plus de possibilités.

Specter, qui permet d'émuler des services classiques (web, FTP, etc.). Il ne permet pas à l'attaquant l'accès total à un système d'exploitation, ce qui limite son intérêt.

VIII.6.2 Pots de miel à forte interaction

Ce type de pot de miel peut être considéré comme le côté extrême du sujet puisqu'il repose sur le principe de l'accès à de véritables services sur une machine du réseau plus ou moins sécurisée.Les risques sont beaucoup plus importants que pour les pots de miel à faible interaction. Il apparaît donc nécessaire de sécuriser au maximum l'architecture du réseau pour que l'attaquant ne puisse pas rebondir et s'en prendre à d'autres machines.

VIII.6.3 Principes du pot de miel :

Les deux grands principes d'un tel pot de miel sont :

- le contrôle de données : pour observer le maximum d'attaques, le pot de miel à forte interaction doit accepter toutes les connexions entrantes et au contraire limiter les connexions sortantes pour éviter tout débordement. Cependant, il ne faut en aucun cas interdire toutes les connexions sortantes pour ne pas alerter l'attaquant. Un bon compromis entre sécurité et risque de découverte du leurre est donc nécessaire.

- la capture des données : avec un pare-feu ou un système de détection d'intrusion (SDI).le pare-feu permet de loguer et de rediriger toutes les tentatives d'attaque aussi bien internes qu'externes.

- le SDI permet d'enregistrer tous les paquets circulant pour pouvoir reconstruire la séquence d'attaque. Il peut permettre également, grâce aux iptables, de rediriger les paquets compromis vers le pot de miel. Il vient donc en complément d'un pare-feu et sert également de sauvegarde au cas où celui-ci tomberait.

- les informations générées seront redirigées vers une machine distante et non stockées sur la machine compromise en raison du risque de compromission de ces données.

- Il faut également relever l'existence de pots de miel plus spécifiques comme les pots de miel anti-spam ou anti-virus.

VIII.7 **DMZ :**

Zone démilitarisée, DMZ (en anglais, demilitarized zone) est un sous-réseau privée ne faisant partie ni du LAN privé ni de l'Internet, inspérier de la zone coréenne démilitarisée qui

Figure VIII-5:DMZ entre les deux Corée

sépare les deux pays la Corée du Nord et la Corée du Sud.

DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes.

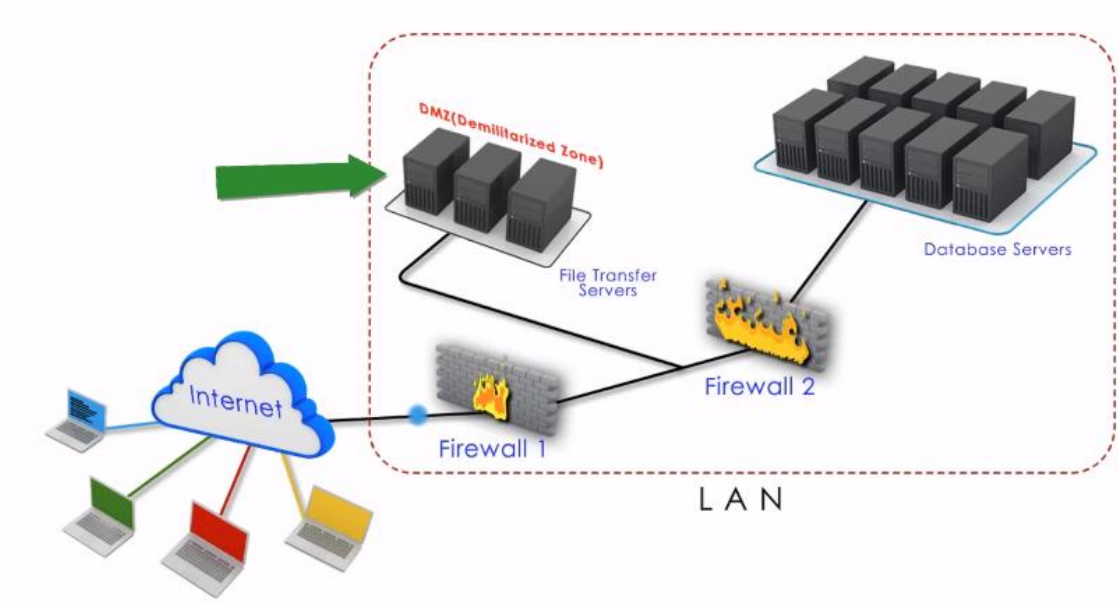


Figure VIII-6: Architecture réseau présente la DMZ

Un niveau supplémentaire de sécurité peut être introduit avec un deuxième firewall. Les règles d'accès sur le firewall du LAN privé sont plus restrictives. La DMZ est située entre deux firewalls (DMZ « en sandwich ») avec des règles moins restrictives introduites par le premier firewall.

VIII.8 Serveur proxy :

Un serveur proxy joue le rôle de passerelle entre Internet et réseau local. C'est un serveur intermédiaire qui sépare les utilisateurs, des sites Web sur lesquels ils naviguent. Les serveurs proxy assurent différents niveaux de fonctionnalité, de sécurité et de confidentialité, selon le type d'utilisation, besoins ou politique de l'entreprise, Si on utilise un serveur proxy, le trafic Internet passe par ce serveur avant d'atteindre l'adresse demandé. La réponse renvoyée passe par ce même serveur proxy (il y a des exceptions à cette règle), puis celui-ci transmet les données reçues depuis le site Web.

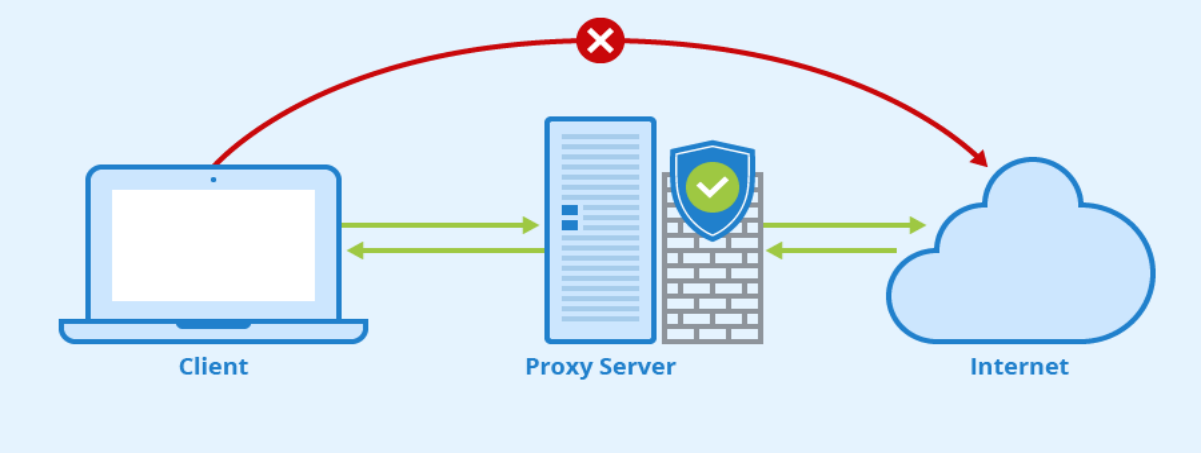


Figure VIII-7:Dessin explique le fonctionnement d'un Serveur Proxy

Le proxy se situe au niveau de la couche application (HTTP, FTP, SSH, etc. de niveau 7). Une erreur commune est d'utiliser la commande traceroute (ou tracert sous Windows) pour tenter de voir le proxy. Il n'apparaît pas, car cette commande, qui utilise le protocole réseau IP de niveau 3, ne peut pas connaître le proxy.

Dans l'environnement plus particulier des réseaux, un serveur proxy, serveur mandataire ou mandataire, est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

VIII.8.1 Les fonctions d'un serveur proxy :

Les serveurs proxys sont notamment utilisés pour assurer les fonctions suivantes:

- ☞ accélération de la navigation grace â : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (Java, Flash) ;
- ☞ la journalisation des requêtes (historique ,le cache "nous y reviendrons plus loin") ;
- ☞ le filtrage (filtrage applicatif), et l'anonymat: Avantages en termes de confidentialité, les particuliers et les entreprises utilisent des serveurs proxy pour naviguer de façon plus

confidentielle sur Internet. Certains serveurs proxy modifieront l'adresse IP et le lieu de connexion et d'autres informations d'identification contenues dans la requête Web. Cela signifie que le serveur de destination ne sait pas qui a réellement émis la requête originale, ce qui contribue à une meilleure confidentialité de vos informations personnelles et de vos habitudes de navigation...

- ☞ la sécurité du réseau local : on peut configurée le serveur proxy pour que les requêtes Web soit chiffré et empêche les yeux indiscrets de lire nos transactions, on peut également interdire l'accès à des sites connus pour héberger des malwares. ;

Dans les organisations, les serveurs proxy sont généralement utilisés pour le filtrage du trafic et l'amélioration des performances, pour assurer vraiment la sécurité on doit associe le serveur proxy à un réseau privé virtuel (VPN).

VIII.9 VPN :

Le réseau privé virtuel (RPV) ou réseau virtuel privé (RVP), plus communément abrégé en VPN (de l'anglais : virtual private network) est système qui permet de crée un chemin virtuel sécurisé direct entre la source et la destination grâce a un principe de tunnel (tunneling) qui isole leurs échanges du reste du trafic WAN Public qui se déroule sur des réseaux de plusieurs ISP dans le monde entier, On va s'introduire plus de détails a propos de cette mesure de sécurité sur le chapitre suivant

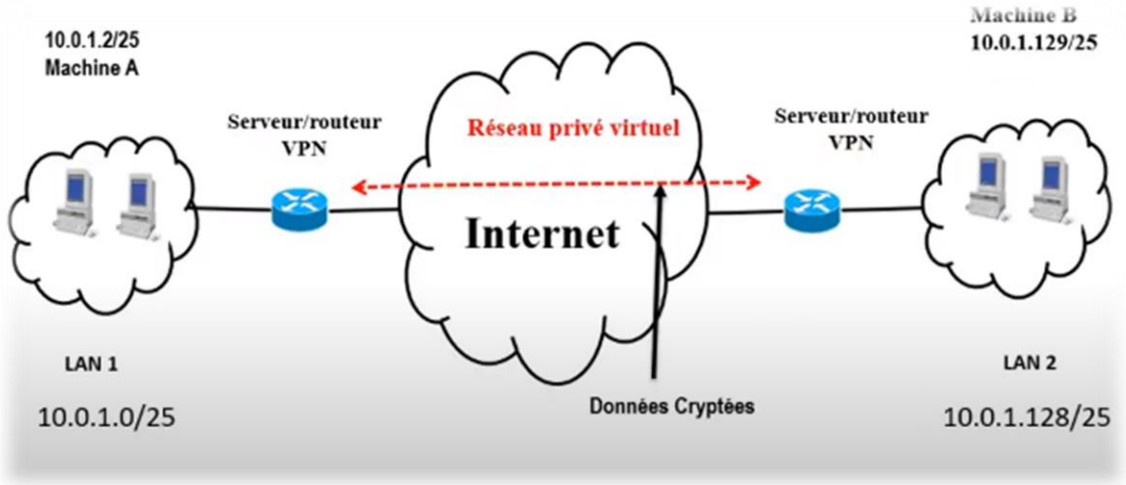


Figure VIII-8: Principe de VPN

IX. Conclusion:

Nous l'avons vu dans ce chapitre, la sécurisation d'un réseau qui est une étape délicate permettant de protéger une entreprise des risques les plus courants, émanant aussi bien de l'internet que de son propre réseau local. Une gamme "complète" de solutions telles que mesure de sécurité permet d'obtenir une sécurité presque convenable face aux attaques les plus courantes. Ces dernières sont d'ailleurs en évolution quotidiennes et de nombreuses failles sont découvertes et exploitées chaque jour. Dans le prochain chapitre, Nous allons présenter un état de l'art des technologies VPN les plus répandues. Elles seront résumées afin d'en obtenir une vue générale, formant une base pour lancer notre projet sur la sécurisation d'un réseaux WAN.

Chapitre 3 : Généralités sur les VPNs

I. Introduction :

Un réseau privé virtuel (VPN) comme on vue dans les mesure de sécurité est une sorte de tunnel privé qui traverse le réseau public, et qui permet de connecter les télétravailleurs à réseau d'entreprise ou les sites distants entre eux. Les utilisateurs du réseau peuvent se connecter en toute confidentialité et partager les ressources de l'entreprise.

II. Définition:

II.1 Réseau privé :

Les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise. De plus en plus, pour des raisons d'interopérabilité, on y utilise les mêmes protocoles que ceux utilisés dans l'Internet. On appelle alors ces réseaux privés « intranet ». Y sont stockés des serveurs propres à l'entreprise en l'occurrence des portails, serveurs de partage de données, etc. ... Pour garantir cette confidentialité, le réseau privé est coupé logiquement du réseau internet. En général, les machines se trouvant à l'extérieur du réseau privé ne peuvent pas accéder à celui-ci. L'inverse n'étant pas forcément vrai. L'utilisateur au sein d'un réseau privé pourra accéder au réseau internet.

II.2 Réseau privé virtuel :

L'acronyme VPN correspond à Virtual Private Network, c'est-à-dire un réseau privé virtuel. Dans les faits, cela correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation. Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet. Il permet d'échanger des données entre deux entités sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

II.2.1 Intérêt de VPN:

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des machines distantes au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.

Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombres d'applications possibles :

- √ Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et

de façon sécurisée pour les travailleurs nomades.

- √ Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante.
- √ Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.
- √ Les connexions VPN permettent également aux entreprises de disposer des connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'Internet, et de continuer à disposer des communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.
- √ Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante.

III. les différents types de VPN :

On'a 2 types de VPN:

- ☞ **Remote access VPN** « Host to LAN » : Le VPN peut être de type point à point, utilisé entre un client et un concentrateur VPN (routeur spécialisé, pare-feu, ou logiciel sur ordinateur), sur Internet par le biais d'un logiciel de VPN.

- ☞ **Site to Site VPN** « Lan to lan » : Dans une autre acception, le VPN peut exister sous la forme d'un réseau privé virtuel étanche et distribué sur un nuage MPLS. Les ordinateurs sur ce VPN y sont souvent raccordés physiquement, la notion de « virtuel » se rapportant alors au fait que l'infrastructure MPLS fait circuler plusieurs réseaux virtuels étanches entre eux.

De façon plus générale les VPN peuvent être classés selon les protocoles, services, et type de trafic (couche OSI 2 ou 3) pouvant circuler en son sein.

Par exemple on peut citer aussi parmi ces différents types les :

- ☞ VPN d'accès.
- ☞ Intranet VPN.
- ☞ Extranet VPN

Chacun ont leurs particularités, c'est ce que nous allons voir dans cette partie.

III.1 Le VPN d'accès :

C'est le meme que **Remote access VPN** « Host to LAN » est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. 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 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.

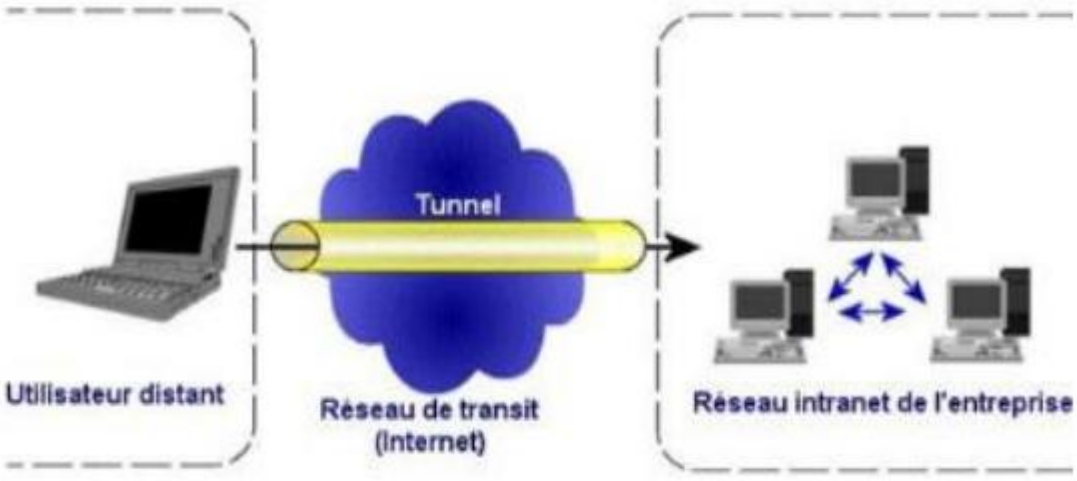


Figure III-1:VPN connectant un utilisateur distant à un intranet privé

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.

III.2 Intranet VPN :

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. 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 aussi basée sur des algorithmes de cryptographie.

La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation Ip dans IP pour assurer une sécurité raisonnable.

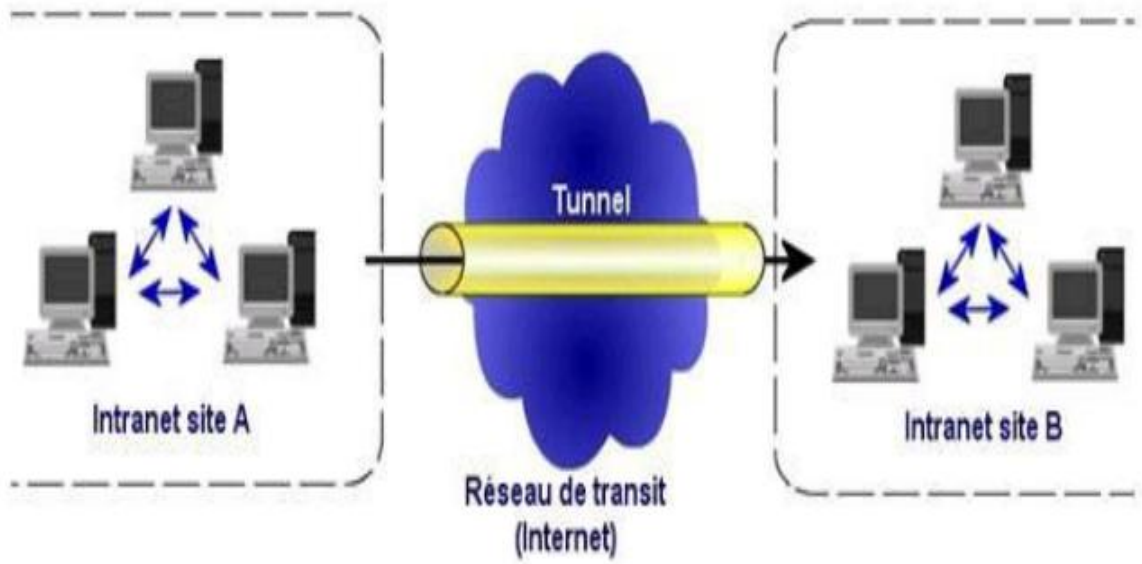


Figure III-2:VPN connectant 2 sites distants par l'Internet

III.3 Extranet VPN:

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

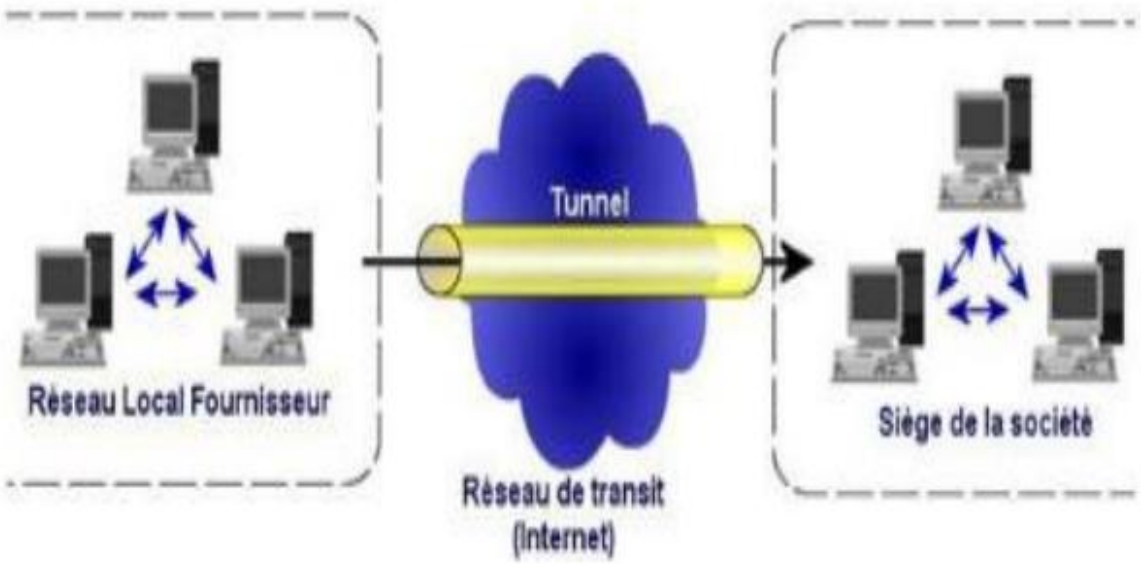


Figure III-3:VPN connectant des sites clients au site de l'entreprise

IV. Protocoles utilisés et sécurité des VPN :

Le VPN basé sur des protocoles du tunneling sont par définition de niveau 3 (réseau), tout comme IP qu'il sert à protéger. Utilisé en mode tunneling, la source utilise des protocoles de tunneling pour encapsule des paquets IP complets et les protège jusqu'à leur destination, où les paquets IP sont "décapsulés" et restitués, la figure suivante montre le principe du tunneling :

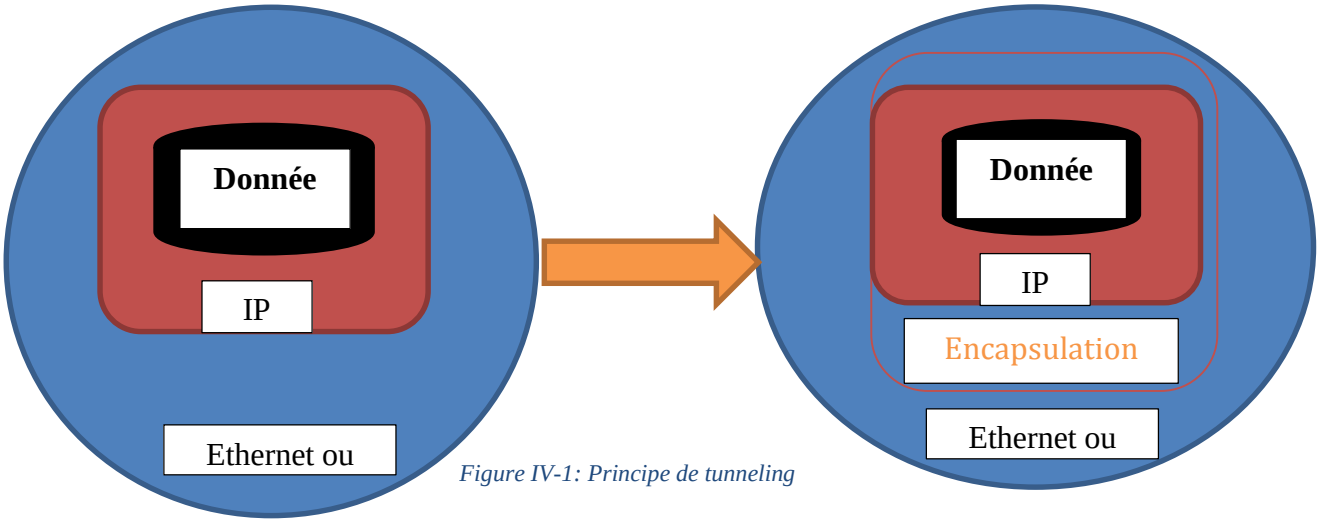


Figure IV-1: Principe de tunneling

Il existe plusieurs protocoles dit d'encapsulation (tunneling) qui permettent la création des réseaux VPN:

IV.1 PPP (Point To Point Protocol) :

Le protocole PPP (Point To Point Protocol) de Microsoft, traduisez protocole point à point, est un protocole beaucoup élaboré que SLIP dans la mesure où il transfère des données supplémentaires, mieux adaptées à la transmission de données sur internet.

PPP est en réalité un ensemble de trois protocoles :

- ☞ Un protocole d'encapsulation de datagramme.
- ☞ Un protocole de contrôle de liaison (LCP, Link Contrôle Protocole) permettre de contrôles de test et de configuration de la communication.
- ☞ Un ensemble de protocoles de contrôle de réseau (NCP Network Control Protocol) permettant des contrôles d'intégration de PPP au sein de protocolesde couches supérieurs.

Les données encapsulées dans une trame PPP sont appelées paquets. Ces paquets sont généralement des datagrammes.

Une trame PPP ressemble à ceci :

Protocole (1-2 octets)	Données à transmettre	Données de remplissage

Figure IV-2:la trame PPP

Une session PPP (de l'ouverture à la fermeture) se déroule comme suit :

- ➢ Lors de la connexion, un paquet LCP est envoyé.
- ➢ Dans le cas de demande de l'authentification de la part de serveur, un paquet correspondant à un protocole d'authentification peut être envoyé (PAP, Password Authentification Protocol)
- ➢ Une fois la communication établie, PPP envoie des informations de configuration grâce au protocole NCP.
- ➢ Les datagrammes à envoyer sont transmis sous forme de paquets.
- ➢ A la déconnexion un paquet LCP est envoyé pour mettre fin à la session.

Voici la liste des services pouvant être offerts par PPP :

- ❖ permet à un serveur d'accès à distance de recevoir des appels entrants et de garantir l'accès au réseau à des logiciels d'accès distant d'autres éditeurs, conformes aux normes PPP.
- ❖ Les normes PPP autorisent des fonctions avancées qui ne sont pas disponiblesavec l'ancienne norme, notamment SLIP.
- ❖ Le protocole PPP prend en charge plusieurs méthodes d'authentification ainsique la compression des données et leur cryptage.
- ❖ La plupart des versions du protocole PPP permettent d'automatiser l'ensemble de la procédure d'ouverture de session.

- Le protocole PPP prend également en charge plusieurs protocoles de réseau local. Nous pouvons utiliser TCP/IP ou IPX comme protocole réseau. PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN (Virtual Private Network) sécurisées.

IV.2 PPTP (Point To Point Tunneling Protocol):

PPTP est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet le cryptage de données ainsi que leur compression.

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation).

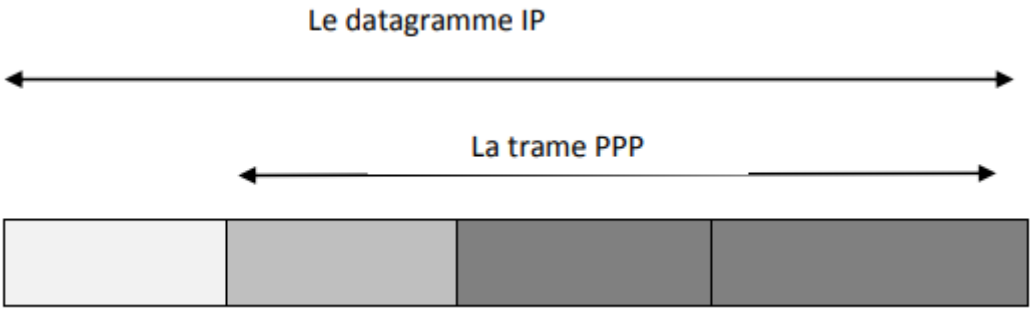


Figure IV-3: La trame PPTP

Le tunnel PPTP se caractérise par:

- une initialisation du client.
- une connexion de contrôle entre le client et le serveur.
- la clôture du tunnel par le serveur.

Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP.

Plusieurs protocoles peuvent être associés à PPTP afin de sécuriser les données ou de les compresser. Ainsi, pour le processus d'identification, il est possible d'utiliser les protocoles PAP

(Password Authentification Protocol). Pour le cryptage de données, il est possible d'utiliser les fonctions de MPPE (Microsoft Point to Point Encryption).

Enfin , une compression de bout en bout peut être réalisée par MPPC (Microsoft Point to Point Compression). Ces divers protocoles permettent de réaliser une connexion Vpn complète, mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

IV.3 L2F (Layer Two Forwarding)

Le protocole L2F est un protocole créé par Cisco. Il est assez similaire à PPTP étant donné qu'il démarre par l'ouverture d'une connexion PPP du client vers le fournisseur d'accès Internet.

Cependant, contrairement au protocole PPTP, le tunnel est ici transparent pour le client. C'est le NAS du FAI qui met en place le tunnel entre lui-même et le serveur d'accès du réseau distant : c'est le mode forcé, par opposition au mode volontaire utilisé par PPTP. Cela entraîne une perte de la maîtrise de la sécurité vu que les données seront visibles par le FAI. L2F est adapté aux intranet VPN.

IV.4 L2TP (Layer Two Tunneling Protocol):

L2TP est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft... Il permet l'encapsulation des paquets PPP au niveau des couches 2 (liaison de données) et 3 (réseau). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator) et les serveurs réseau L2TP (LNS : L2TP Network Server).

IV.4.1 Concentrateurs d'accès L2tp (LAC : L2TP Access Concentrator) :

Les périphériques Lac fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.

IV.4.2 Serveur réseau L2TP (LNS : L2TP Network Server) :

Les serveurs réseau L2TP ou LNS peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le LNS gère le protocole L2TP côté serveur. Le protocole L2TP

n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local (LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès LAC. Le LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification du tunnel.

IV.5 IPSEC (Internet protocol security):

Selon l'RFC de IETF IPSec est un ensemble de protocoles de sécurité au sein de la couche réseau, sécuriser l'envoi de donnés grâce â la cryptographie, garantie : l'authentification, l'intégrité, le contrôle d'accès et la confidentialité des données.

IV.5.1 Vue Générale:

IPsec est probablement le protocole VPN le plus utilisé aujourd'hui. Il fit son apparition en 1995. Il prend en charge les trois composantes d'un VPN :

- le transport.
- l'authentification.
- la sécurisation des données.

IPsec peut fonctionner selon deux modes, selon ce que l'on veut en faire : mode tunnel et mode transport. On pourra également faire une combinaison de ces deux modes, on parlera alors de mode nesting (il s'agit en fait d'encapsuler IPsec dans de l'IPsec).

IV.5.2 Services offerts par IPsec :

Voici la liste des services pouvant être offerts par IPsec. Notons bien que selon le mode utilisé, tout ou partie de ces services seront disponibles.

- ✓ **Authentification des extrémités** : Chaque extrémité du tunnel va s'identifier avant d'entamer la communication des données. Cela permet de s'assurer que l'on dialogue avec la personne convenue. De plus, pour chaque paquet échangé, IPSec permettra de s'assurer qu'il a été émis par la bonne machine (authenticité des données).
- ✓ **Confidentialité des données :** Evite que quelqu'un qui intercepterait les données ne puisse les interpréter. On utilisera pour cela des techniques de cryptographie.
- ✓ **Intégrité des données :** IPsec permet de s'assurer qu'un paquet n'a subit aucune modification durant son trajet.
- ✓ **Protection contre le rejeu :** permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

IV.5.3 Les sous-protocoles d'IPsec :

IV.5.3.1 Le protocole Ah (Authentication Header):

L'absence de confidentialité permet de s'assurer que Ce standard pourra être largement répandu sur Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité.

Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé "valeur de vérification d'intégrité". La protection contre le rejet se fait grâce à un numéro de séquence.

IV.5.3.2 Protocol ESP (Encapsulating Security Payload) :

Esp peut assurer au choix, un ou plusieurs des services suivants :

- √ Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- √ Intégrité des données en mode non connecté.
- √ authentification de l'origine des données.
- √ protection contre le rejeu.

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans Esp ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité.

Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets. Les données d'authentification ne sont présentes que si Ce service a été sélectionné. Voyons maintenant comment est appliquée la confidentialité dans ESP.

L'expéditeur :

- ☞ Encapsule, dans le champ "charge utile" d'ESP, les données transportées par le datagramme original et éventuellement IP (mode tunnel).
- ☞ Ajoute si nécessaire un bourrage.
- ☞ Chiffre le résultat (données, bourrage, champs longueur et en-tête suivant).
- ☞ Ajoute éventuellement des données de synchronisation cryptographiques (vecteur d'initialisation) au début du champ "charge utile".

IV.5.4 IPsec en mode tunnel et transport :

IV.5.4.1 Mode transport :

Le mode transport offre une protection aux protocoles de niveau supérieur (TCP, UDP). Il n'assure pas de protection contre l'analyse de trafic, car il ne modifie pas la partie IP.

On peut utiliser AH si la confidentialité des données n'est pas essentielle ou si elle est assurée par une autre couche, ou ESP si on veut s'assurer de la confidentialité des données. En mode transport, les données sont prises au niveau de la couche 4 du modèle OSI (couche transport). Elles sont cryptées et signées avant d'être transmises à la couche IP.

IV.5.4.2 Mode tunnel :

En mode tunnel, l'encapsulation IPsec a lieu après que les données envoyées par l'application aient traversé la pile de protocoles jusqu'à la couche IP incluse. On peut alors signer et crypter les adresses.

Ainsi, si on utilise AH, on signera l'intégralité du paquet IP encapsulé pour s'assurer de son intégrité et de son authenticité. Avec ESP, le paquet sera en plus entièrement crypté, permettant de s'assurer de la confidentialité des données, et de se protéger partiellement contre l'analyse du trafic en cryptant les adresses IP source et destination.

Les schéma ci-dessous permet de se faire une idée plus claire des différences entre les deux modes :

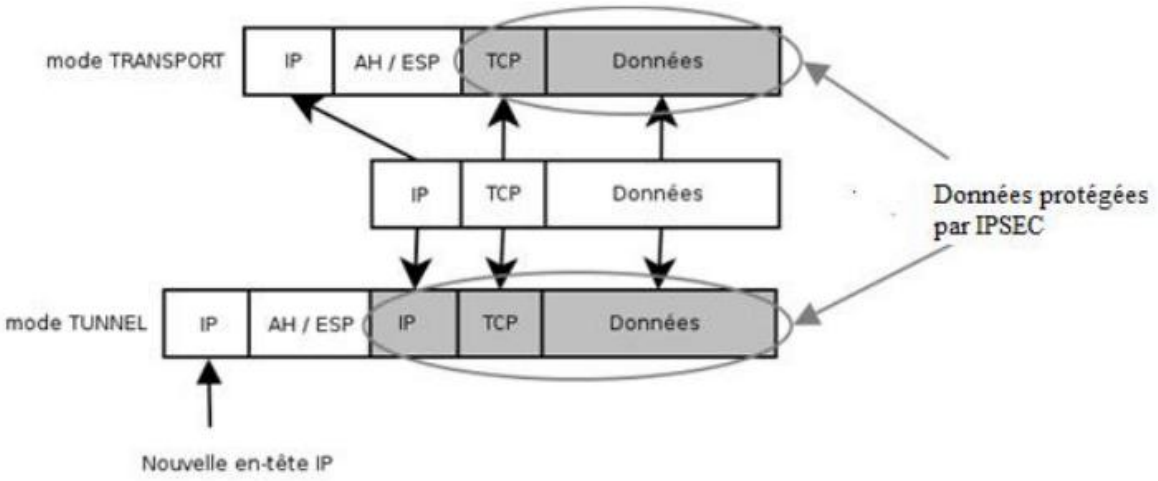


Figure IV-4:Les différences entre le mode tunnel et transport

Mode transport : (AH)n'a pas d'entête IP supplémentaire :

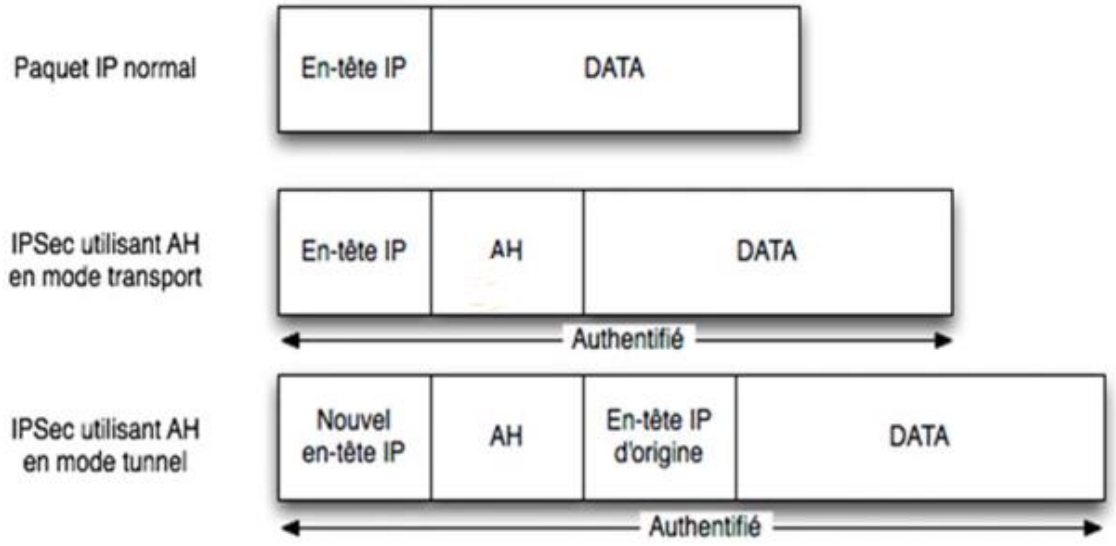


Figure IV-5: les différences entre le mode tunnel et transport en « mode transport : (AH) pas d'entête IP supplémentaire ».

Mode tunnel : (ESP) a une nouvel entête IP est rajouté.

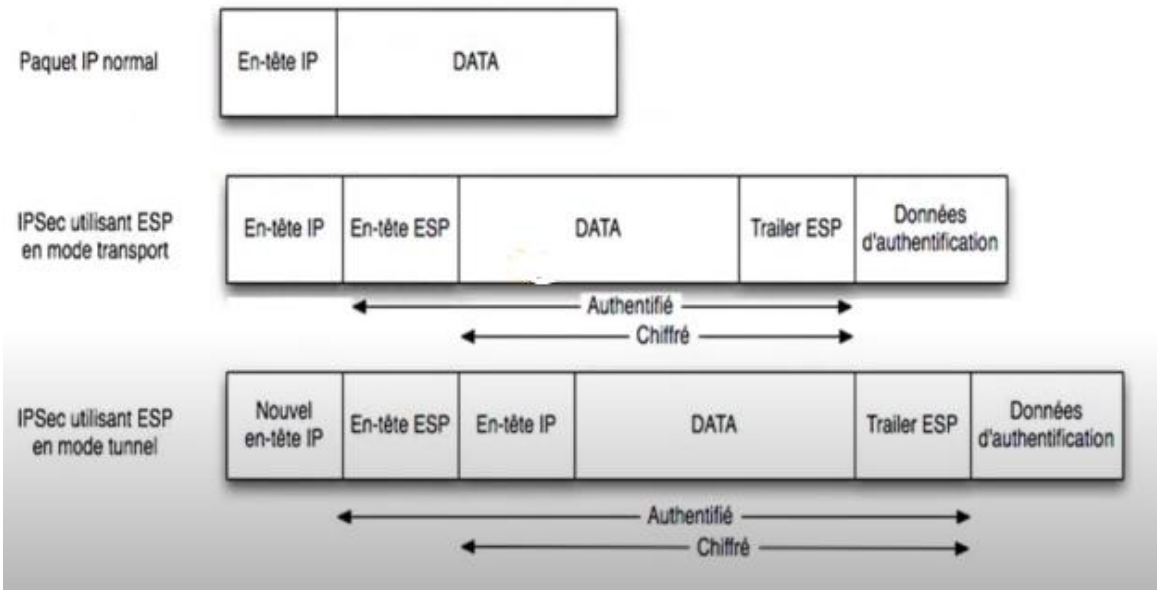


Figure IV-6: les différences entre le mode tunnel et transport en mode tunnel : (ESP) une nouvel entête IP est rajouté

IV.6 Le protocol SSH :

SSH est une version sécurisée de ces outils ; il permet de se connecter à distance sur une machine donnée suivant une architecture client/serveur. Il se compose d'un client qui sera invoqué sur la machine initiatrice de la communication et d'un serveur qui doit tourner sur la machine destinataire.il va créer une communication sécurisée, en authentifiant les deux parties et en garantissant le secret de la communication et son intégrité.

SSH est classiquement utilisé pour une fois la communication sécurisée établie, exécuter un interpréteur de commandes, un Shell, Mais il est possible de faire passer à travers un canal sécurisé n'importe quel trafic TCP(X11, SMTP, HTTP, etc.), ce qui offre une grande flexibilité ; On appelle cela créer un tunnel SSH.

IV.7 Le protocol SSL :

Récemment arrivé dans le monde des VPN, Les VPN SSL présentent en effet un gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur Internet est implémenté en standard dans les navigateurs modernes.

Ssl est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Ssl a deux grandes fonctionnalités :

- l'authentification du serveur et du client à l'établissement de la connexion.
- le chiffrement des données durant la connexion.

IV.7.1 Fonctionnement :

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par la vérification de la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi la date de validité du certificat et peut également consulter une CRL (Certificat Révocation List). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ceci est fait de façon à Ce que le serveur puisse authentifier le client.

De nombreux paramètres sont échangés durant cette phase : type de clé, valeur de la clé, algorithme de chiffrage ...

La phase suivante consiste à l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases du protocole sont :

- Segmentation des paquets en paquets de taille fixe.

- Compression.
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message, ...
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake.
- Ajout d'un en-tête SSL au paquet.

V. Conclusion :

L'accès distant et la connectivité VPN aux sites d'entreprise distants sont des points d'entrée des attaques de réseau : vers, virus, logiciels espions, enregistreurs de frappe, chevaux de Troie, pirates informatiques, en raison du mode de conception actuel des VPN. Bien trop souvent, les VPN sont déployés sans qu'une action appropriée d'inspection et de réduction des menaces soit menée au niveau du point d'extrémité du tunnel, au siège de l'entreprise. Cela permet aux programmes nuisibles provenant des utilisateurs ou des sites distants d'infiltrer le réseau et de se propager, Dans le prochain chapitre, nous allons élaborer une autre mesure de sécurité important « les firewalls ».

Chapitre 4 : Les Firewalls

I. Introduction :

Comme on déjà vue internet est un réseau de réseaux à l'échelle mondiale qui utilise le protocole de transmission TCP/IP (Transmission Control Protocol/Internet Protocol). Internet est un réseau vital et en pleine extension et qui est en train de changer la manière avec laquelle les organisations et les individus communiquent et traitent leurs affaires. Cependant, Internet souffre d'importants problèmes de sécurités. Les attaques subies par certaines organisations ont eu un impact important sur leur productivité et leur réputation par exemple Amazon comme on' a vue sure les défis relatifs à la protection des données en cours de traitement de La 2éme dimension du cube McCumber dans le chapitre 2 « sécurité des réseaux ». En effet, dans certains cas des organisations ont dû se déconnecter temporairement d'Internet et ont dû faire des investissements significatifs dans la réparation des dégâts subis par leurs systèmes et la révision de la configuration de leurs réseaux. Heureusement, des solutions aux problèmes de sécurité existent comme on 'a déjà vue sur les mesures de sécurité.

Un système firewall est l'une des techniques qui peut nettement améliorer le niveau de sécurité d'un site dans sa globalité, en obligeant toutes les connexions à passer à travers une passerelle pour être examinées, évaluées et authentifiées. Ce chapitre donne une présentation des différents aspects de la technique du firewall.

II. Définitions :

Un pare-feu (appelé aussi Coupe-feu, Garde-barrière) en Anglais (firewall) 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. Un pare-feu est installé en coupure sur un réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé. Dans le cas d'un pare-feu personnel, sur une machine cliente, il est installé en son cœur pour y contrôler et filtrer les accès au réseau. 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 type 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 (TCP), 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 pares-feux 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 sont 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 de manière à analyser a posteriori tous les faits importants qui jalonnent la vie de cette passerelle filtrante : tentatives d'intrusion, événements anormaux, attaques par saturation, 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, souvent comme on 'a vu la mesure de sécurité appelée zone démilitarisée (demilitarized zone, DMZ). C'est dans cette zone qu'on place le site Web , messagerie …… , ouvert sur Internet, à l'abri d'un pare-feu, mais nettement séparé du réseau interne à protéger.

III. Types de pare-feu :

Au fil des années, comme les attaques informatiques et les attaques du réseau sont devenues plus sophistiquées, de nouveaux types de pare-feu ont été élaborés pour répondre à différents objectifs dans la protection d'un réseau. Voici une liste des types de pare-feu courants :

III.1 Pare-feu de la couche réseau :

Filtrage basé sur les adresses IP sources et de destination.

III.2 Pare-feu de la couche transport :

Filtrage basé sur les ports de données sources et de destination et filtrage basé sur les états de connexion.

III.3 Pare-feu de la couche application :

Filtrage basé sur les applications, les programmes ou les services.

III.4 Pare-feu pour applications sensibles au contexte :

Filtrage basé sur l'utilisateur, l'appareil, le rôle, le type d'application et le profil de la menace.

III.5 Serveur proxy :

Filtrage des demandes de contenu Web comme les URL, les domaines, les médias, etc.

III.6 Serveur proxy inverse :

Placé à l'avant des serveurs Web, les serveurs proxy inverses protègent, masquent, déchargent et distribuent l'accès aux serveurs Web.

III.7 Pare-feu NAT (traduction d'adresses de réseau) :

Cache ou masque les adresses privées des hôtes du réseau.

III.8 Pare-feu propre à un hôte unique :

Filtrage des ports et des appels de service du système sur le système d'exploitation d'un seul ordinateur.

IV. Principes de base :

Le pare-feu est jusqu'à ces dernières années est considéré comme une des pierres angulaires de la sécurité d'un réseau informatique (il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur TLS, court-circuitant tout filtrage). Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs). Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante). Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège (12). On peut alors distinguer Les composants de principes de fonctionnement des pare-feu comme suit :

IV.1 Politique de sécurité du réseau :

Le but d'une politique de sécurité du réseau est de définir les prévisions de l'organisation en termes d'utilisation de ses propres systèmes et réseau ainsi que les procédures de prévention et d'intervention aux incidents de sécurité.

La politique de sécurité est définie en deux niveaux qui influent directement sur la conception et l'utilisation d'un système firewall :

IV.1.1 La politique d'accès aux services :

Il s'agit du niveau supérieur qui définit les services dont l'accès sera permis et ceux dont il sera interdit, comment ces services seront utilisés, et les conditions d'exception à cette politique. La politique définie doit être une extension à la politique globale concernant la protection des ressources informationnelles de l'organisation. Elle doit être réaliste dans la mesure où elle assurera une protection du réseau contre les risques connus d'attaques tout en préservant les intérêts de ses utilisateurs en matière d'accès aux services réseau, quand cela est nécessaire, moyennant des techniques d'authentification.

IV.1.2 La politique de conception du firewall :

Il s'agit du niveau le plus bas indiquant comment le firewall pourra mettre en œuvre les restrictions d'accès et le filtrage des services tels que définis par la

politique de sécurité. La conception d'une telle politique doit être faite en ayant connaissance des capacités et des limitations d'un firewall ainsi que, des risques et des vulnérabilités associées aux aux services et protocoles TCP/IP. Les firewalls implémentent généralement une des deux politiques de conception de base suivantes :

I. Ce qui n'est pas explicitement permis est interdit.

II. Ce qui n'est pas explicitement interdit est autorisé.

La première politique est beaucoup plus sûre, interdit par défaut, l'accès à tous les services excepté à ceux qui ont été explicitement identifiés comme étant accessibles. C'est le modèle d'accès classique qui est utilisé dans tous les domaines de sécurité de l'information. La seconde politique autorise, par défaut, tous les accès sauf ceux identifiés par la politique d'accès comme étant non autorisés. Cette solution est moins désirable est plus risquée car elle suppose que l'administrateur est certain d'avoir envisagé tous les cas pouvant engendrer des problèmes, car elle offre plus de possibilités pour contourner un firewall (par exemple, accéder à des services nouveaux non encore interdits d'accès).

IV.2 Authentification avancée :

Le système d'authentification traditionnel basé sur le mot de passe (password) statique n'est plus suffisant en particulier dans un environnement réseau. Des mesures d'authentification sont conçues pour pallier aux faiblesses de ce système. Malgré la diversité des nouvelles techniques d'authentification, leur similitude réside dans le fait que les mots de passe qu'elles génèrent ne peuvent être réutilisés par un attaquant qui aurait espionné la connexion. En effet, le mot de passe n'est généré qu'une seule fois à l'établissement de la connexion entre l'utilisateur et le système et n'est plus valable par la suite.

Au lieu d'implémenter les mécanismes d'authentification au niveau de chaque système hôte du site, il est plus pratique de centraliser ces techniques au niveau d'un firewall qui sera chargé de protéger l'ensemble des systèmes. Ces derniers peuvent alors continuer à implémenter en parallèle la technique classique des mots de passe à leur niveau, on peut citer par exemple « FortiGate I (Firewall Authentication) ».

IV.3 Filtrage de paquets :

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (**stateless packet filtring**). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangés entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le pare-feu :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- Type de paquet (TCP, UDP, etc.) ;
- Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

IV.3.1 Les problèmes de filtrage de paquets :

Les routeurs de filtrage de paquets présentent des inconvénients qui peuvent être résumées en ce qui suit :

- **L**a complexité de spécification des règles de filtrage dont la vérification se fait, en général, manuellement. Souvent, les exceptions aux règles d'accès rendent encore plus complexe leur gestion. Par exemple, il est relativement simple de spécifier une règle qui bloque l'accès au port 23 associé au serveur Telnet que de spécifier une règle pour chaque système auquel les appels Telnet sont autorisés.

- **L**'authentification sur les adresses IP identifie le système hôte mais pas l'utilisateur réel; d'où la nécessité de mécanismes d'authentification.

- **I**l n'est pas toujours possible de connaitre à priori les ports associés aux serveurs, dans ce cas un filtrage basé sur les adresses source/destination et sur les ports source/destination n'est souvent pas suffisant pour assurer un niveau de sécurité élevé.

- **L**es routeurs de filtrage de paquets ayant plus de deux interfaces réseaux, n'ont pas toujours l'aptitude de filtrer les paquets suivant l'interface à laquelle ils arrivent ou à partir dela quelle ils partent.
- **D**e manière général, il est plus difficile d'implémenter une politique rigoureuse, n'autorisant que les accès explicitement spécifiés, lorsque l'on ne dispose pas d'un routeur offrant la possibilité de filtrage sur les ports et les interfaces d'entrée et de sortie.

IV.4 Filtrage dynamique :

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine client.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir des ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur.

IV.5 Le filtrage du flux (Circuit Filtering) :

Le filtrage de flux ne prête pas attention au contenu des paquets transitant sur la connexion. De ce fait, ce type de filtrage ne peut être utilisé pour assurer l'authentification des parties, ou la sécurité du protocole par l'intermédiaire duquel a lieu la connexion. A la différence du filtrage de paquets, qui est considéré comme permissif, le filtrage de flux est restrictif. En effet, il n'autorisera le flux entre deux entités que si la connexion entre ces deux entités existe. On peut voir ce principe comme la création d'un tunnel entre deux machines. De ce fait, le circuit-filtering ne sera souvent utilisé qu'en complément de l'application Gateway.

IV.6 6-Les passerelles application (Application Gateway ou Bastion host) :

Pour parer à certains problèmes ne pouvant être traités au niveau des routeurs de filtrage, les firewalls utilisent le filtrage applicatif qui permet comme son nom l'indique de filtrer les communications application par application. Ce filtrage opère donc au niveau 7 (couche application) du modèle OSI. Le filtrage applicatif suppose donc, une connaissance des applications présentes sur le réseau, et notamment de la manière dont les données sont échangées (ports, etc.).

Un pare-feu effectuant un filtrage applicatif est appelé généralement passerelle applicative "application Gateway" et une application de ce type est appelée "proxy service", car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes, précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire. Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé. Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et connaître les failles afférentes pour être efficace.

L'utilisation simultanée d'un routeur de filtrage et d'une passerelle permet d'obtenir un niveau de sécurité et de flexibilité, dans l'implémentation de la politique d'accès, plus élevé que dans le cas de l'utilisation de l'un des deux mécanismes séparément. Soit par exemple, un site bloquant toutes les demandes de connexion à Telnet et FTP en utilisant un routeur de filtrage de paquets. Ce dernier autorise les paquets Telnet et FTP à se diriger sur un seul hôte, la passerelle Telnet/FTP. Un utilisateur désirant se connecter à un site devra d'abord se connecter à la passerelle et ensuite aux hôtes destinataires. Des proxys services peuvent être spécifiés pour tous les services réseaux Telnet, FTP, email, http, Gopher, X Windows, etc.

Enfin, dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu, également le pare-feu souvent situé à l'extrémité de tunnel IPsec ou TLS. L'intégration du filtrage de flux et de la gestion du tunnel est en effet nécessaire pour pouvoir à la fois protéger le trafic en confidentialité et intégrité et filtrer ce qui passe dans le tunnel. C'est le cas notamment de plusieurs produits du commerce nommés dans la liste ci-dessous.

Les pares feux récents embarquent de plus en plus de fonctionnalités, parmi lesquelles on peut citer :

- Filtrage sur adresses IP / protocole,
- Inspection *stateful* et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif :
  - HTTP (restriction des URL accessibles),
  - Courriel (Anti-pourriel),
  - Logiciel antivirus, anti-logiciel malveillant
- Traduction d'adresse réseau,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveurs de protocoles de connexion (telnet, SSH), de protocoles de transfert de fichier (SCP),
- Clients de protocoles de transfert de fichier (TFTP),
- Serveur Web pour offrir une interface de configuration agréable,
- Serveur mandataire (« *proxy* » en anglais),
- Système de détection d'intrusion (« IDS » en anglais)
- Système de prévention d'intrusion (« IPS » en anglais)

V. *Categories de PARE-FEU :*

Il existe 3 modèles de firewalls. Chacun possède des avantages et désagréments. Il faudra donc préalablement analyser les besoins réels en termes de sécurité, ainsi que les coûts engendrés avant toute utilisation :

V.1 Les firewalls Bridge :

Ce format de mur de feu a l'apparence d'un simple câble réseau, sans machine spécifique. Il est invisible et indétectable pour un pirate, son adresse MAC ne circulant jamais sur le réseau. Placé sur le réseau, le pirate devra donc automatiquement passer par lui pour transmettre des requêtes. On trouvera notamment ce type de firewalls dans des Switch. Ces formats de pare-feu ont pour avantages : Ils sont relativement peu coûteux et transparent lors de leurs mises en place. Ils présentent comme Inconvénients : Pour les contourner, il suffit d'adapter l'attaque ; et ses fonctionnalités sont souvent restreintes.

V.2 Les firewalls hardware :

Ils sont souvent assimilés à des boites noires, l'accès à leur code étant difficile. Ce type de matériel propriétaire renferme d'ailleurs souvent un système de protection permettant d'authentifier le logiciel associé (par signature RSA par exemple), et ainsi rendre toute

modification pratiquement impossible. Ils ont pour avantages : Ils sont facilement intégrables au réseau ; leur administration est souvent simplifiée et leur niveau de sécurité est assez élevé. Ils présentent comme Inconvénients : Ce type de firewall étant propriétaire, les mises à jour dépendent entièrement du constructeur et en raison de l'architecture hardware, peu de modifications sont autorisées.

V.3 Les firewalls logiciels :

Ces pare-feu existent autant sous forme commerciales que sous forme gratuites. Quel que soit leur origine, la sécurité pourra fortement varier. Un logiciel commercial pourra parfois mettre en avant sa facilité de mise en place et de configuration, mais ce sera souvent aux dépends de la sécurité. Au niveau des logiciels gratuits et/ou libres, ils seront souvent plus flexibles (c'est-à-dire plus fournis en options), mais nécessiteront la plupart du temps de bonnes connaissances en réseau afin de les configurer finement sans abaisser le niveau de sécurité.

VI. Les différents types de filtrages :

Depuis leur création, Comme on a déjà vue sur le principe de base les pares feux ont grandement évolué. Ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. De ce fait, comme on a vue aussi il existe maintenant différentes catégories et types de pare-feu. Chacune d'entre-elles disposent des avantages et des inconvénients qui lui sont propres. Le choix d'un type de pare-feu plutôt qu'un autre dépendra de l'utilisation que l'on souhaite en faire, mais aussi des différentes contraintes imposées par le réseau devant être protégé, on peut les classer en 6 différentes catégories :

VI.1.1 Pare-feu sans état (stateless firewall) :

Ce sont les pare-feu les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquets indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur .

Ces règles peuvent avoir des noms très différents en fonction du pare-feu :

- « ACL » pour Access Control List (certains pare-feux Cisco),
- politique ou policy (pare-feu Juniper/Netscreen),
- filtres,
- règles ou rules,
- etc.

La configuration de ces dispositifs est souvent complexe vient du fait une l'administrateur réseau est rapidement contraint â autoriser un trop grand nombre d'accès, pour que le firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec port supérieur à 1024. Ce qui laisse beaucoup de choix a un éventuel pirate. Et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pares feux ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation, cette méthode n'est pas

sécurisée par ce que l'agresseur il peut manipuler aux paquets selon les règles définies par l'administrateur.

VI.2 Pare-feu à états (stateful) :

Les pare-feu à états sont une évolution des pare-feu sans états. La différence entre ces deux types de pare-feu réside dans la manière dont les paquets sont contrôlés. Ils prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de « stateful inspection ». De ce fait, ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :

- ☞ NEW : Un client envoie sa première requête ;
- ☞ ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW ;
- ☞ RELATED : Peut-être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue ;
- ☞ INVALID : Correspond à un paquet qui n'est pas valide.

Le firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face a certains types d'attaques DOS.

Dans l'exemple précédant sue les connexions Internet, on va autoriser l'établissement des connexions à la demande, ce qui signifie que l'on aura plus besoin de garder tous les ports supérieurs à 1024 ouverts, Pour les protocoles UDP et ICMP, il n'y a pas de mode connecté.

La solution consiste à autoriser pendant un certain délai les réponses légitimes aux paquets envoyés. Les paquets ICMP sont normalement bloqués par le Firewall, qui doit en garder les traces. Cependant, il n'est pas nécessaire de bloquer les paquets ICMP de type 3(destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion TCP ou après l'envoi d'un paquet UDP.

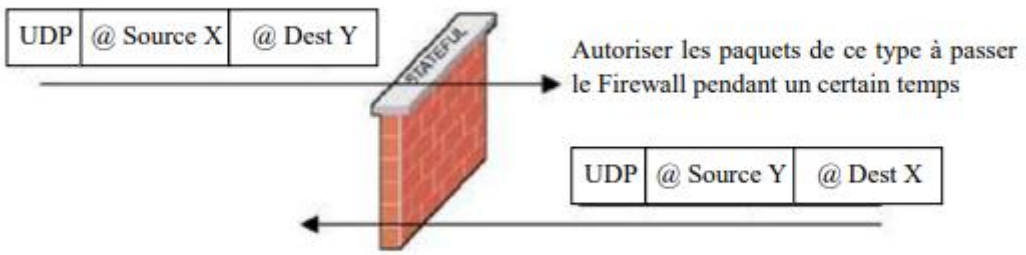


Figure VI-1: Filtrage de paquet avec état (UDP)

Pour le protocole FTP (et les protocoles fonctionnant de la même façon), c'est plus délicat puisqu'il va falloir gérer l'état de deux connexions. EN effet, le protocole FTP, géré un canal de contrôle établi par le client, et un canal de données établie par le serveur. Le firewall devra donc laisser passer le flux de données établi par le serveur. Ce qui implique que le Firewall connaisse le protocole FTP, et tous les protocoles fonctionnant sur le même principe.

Cette technique est connue sous le nom de filtrage dynamique (Stateful inspection) et a été inventée par Checkpoint. Mais cette technique est maintenant gérée par d'autres fabricants.

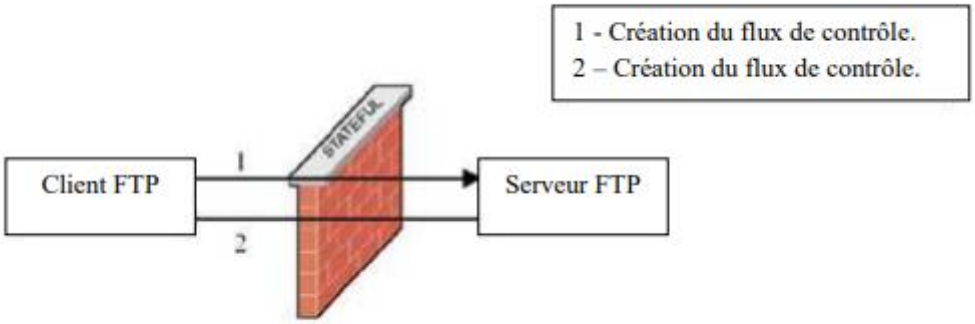


Figure VI-2/ Filtrage de paquet avec état (FTP)

Il convient de s'assurer que les deux techniques sont bien implémentées par le Firewalls, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur HTTP pourra donc être attaqué impunément. Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

VI.3 Pare-feu applicatif :

Dernière génération de pare-feu NGFW, ils vérifient la complète conformité du paquet à un protocole attendu. Aussi nommé pare-feu de type proxy ou passerelle applicative fonctionne sur la couche 7 du modèle OSI. Cela suppose que le pare-feu connaisse l'ensemble des protocoles utilisés par chaque application.

Parmi les raisons de l'inspection applicative est l'ouverture de ports dynamique. Certains protocoles comme FTP, en mode passif, échangent entre le client et le serveur des adresses IP ou des ports TCP/UDP. Ces protocoles sont dits « à contenu sale » ou « passant difficilement les pares-feux » car ils échangent au niveau applicatif (FTP) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports). Ce qui transgresse le principe de la séparation des couches réseaux. Pour cette raison, les protocoles « à contenu sale » passent

difficilement voire pas du tout les règles de NAT ...dynamiques, à moins qu'une inspection applicative ne soit faite sur ce protocole.

Chaque type de pare-feu sait inspecter un nombre limité d'applications. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver. La terminologie pour le concept de module est différente pour chaque type de pare-feu : par exemple : Le protocole HTTP permet d'accéder en lecture sur un serveur par une commande GET, et en écriture par une commande PUT. Un pare-feu applicatif va être en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

- ***Firewall as a Service*** (filtrage en fonction de l'origine et de la destination de chaque paquet)
- ***Conntrack*** (suivi de connexion) et l7 Filter (filtrage applicatif) sur Linux Netfilter
- ***CBAC*** sur Cisco IOS
- ***Fixup*** puis inspect sur Cisco PIX
- ***ApplicationLayerGateway*** sur ***Proventia M***,
- ***Predefined Services*** sur Juniper ScreenOS
- ***Stateful Inspection*** sur Check Point FireWall-1

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaitre les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100% proxy pour les réseaux a gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

On peut citer aussi comme des types de filtrages :

VI.4 Pare-feu authentifiant :

Un pare-feu réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur. Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple citer authpf (sous OpenBSD) qui utilise « ssh » pour faire l'association. Une autre méthode est l'identification connexion par connexion (sans avoir cette association IP = utilisateur et donc sans compromis sur la sécurité), réalisée par exemple par la suite NuFW, qui permet d'identifier également sur des machines multi-utilisateurs. On pourra également citer Cyberoam qui fournit un pare-feu entièrement basé sur l'identité (en réalité en réalisant des associations adresse MAC = utilisateur) ou Check Point avec l'option NAC Blade qui permet de créer des règles dynamiques basée sur l'authentification « Kerberos » d'un utilisateur,

l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patchs particuliers).

VI.5 Pare-feu personnel :

Les pares feux personnels sont installés directement sur les postes de travail. Leur principal but est de contrer les virus informatiques et logiciels espions (spyware). Leur principal à tout est qu'ils permettent de contrôler les accès aux réseaux des applications installées sur la machines. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau.

VI.6 Portail Captif :

Les portails captifs sont des pares-feux dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale (par exemple : avertissement, charte d'utilisation, demande d'authentification, etc.) avant de les laisser accéder à Internet. Ils sont utilisés pour assurer la traçabilité des connexions et/ou limiter l'utilisation abusive des moyens d'accès. On les déploie essentiellement dans le cadre de réseaux de consultation Internet mutualisés filaires ou Wi-Fi.

VII. Les firewalls Pfsense :

VII.1 Présentation générale de pfsense :

Développé par Chris Buechler et Scott UlIrich, Pfsense ou « Packet Filter Sense » est un applicatif qui fait office de routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il est une reprise du projet Monowall auquel il rajoute ses propres fonctionnalités. Il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il peut fonctionner sur du matériel de serveur ou domestique, sur des solutions embarquées, sans toutefois demander beaucoup de ressources ni de matériel puissant. La plate-forme doit être x86 ou x64, mais d'autres architectures pourraient être supportées à l'avenir. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. Pfsense convient pour la sécurisation d'un réseau domestique ou de petite entreprise. C'est une distribution dédiée qui peut être installée sur un simple poste de travail, un serveur ou même sur un boîtier en version embarquée. Ce qui séduit chez Pfsense est sa facilité d'installation et de configuration des outils d'administration réseau. Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN (802.1q).

La distribution Pfsense met ainsi à la disposition de l'administrateur réseau une multitude d'outils open source et de services permettant d'optimiser ses tâches. Pfsense assure une compatibilité multi-plates-formes, une personnalisation complète des pages accessibles aux utilisateurs ainsi qu'une simplicité d'utilisation grâce à une page de connexion succincte où on ne retrouve que deux champs (utilisateur / mot de passe).

Figure VII-1: Logo de pfsense

VII.2 Aperçu des fonctionnalités :

Pfsense, un routeur/pare-feu open source dispose plusieurs fonctionnalités. Parmi celles-ci, on peut noter :

- Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP :
  - Capable de limiter les connexions simultanées sur une base de règle ;
  - Pfsense utilise p0f, un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion ;
  - Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle ;

- Network Address Translation (NAT) :
  Rediriger les ports y compris les rangs et l'utilisation de plusieurs adresses IP publiques NAT pour les adresses IP individuelles ou des sous-réseaux entiers. Redirection NAT Par défaut, le NAT redirige tout le trafic sortant vers l'adresse IP WAN. Dans le cas de connexions WAN multiples, le NAT redirige le trafic sortant vers l'adresse IP de l'interface WAN utilisée. NAT réflexion : dans certaines configurations, NAT réflexion est possible si les services sont accessibles par IP publique à partir de réseaux internes.

- Basculement base sur CARP et pfsync
  CARP est un protocole permettant à un groupe d'hôtes sur un même segment réseau de partager une adresse IP. Le nom CARP est en fait un sigle qui signifie « Common Address Redundancy Protocol » (Protocole Commun De Redondance D'Adresse), à ne pas confondre avec « Cache Array Routing Protocol » utilisé pour faire de la répartition de charge de mandataires caches web Il a été créé pour contourner des brevets. Ce protocole peut être utilisé pour faire de la redondance et de la répartition de charge. Il supporte IPv4 et IPv6, et a le numéro de protocole 112. Il est supporté par pfsense

- Pfsync assure la table d'état du pare-feu qui est répliquée sur tous les pare-feu configurés de basculement. Cela signifie que vos connexions existantes seront maintenues dans le cas d'échec, ce qui est important pour prévenir les perturbations du réseau.

- Load Balancing/ Répartition de charge :
  La répartition de charge du trafic sortant est utilisée avec plusieurs connexions WAN pour assurer la répartition de charge et des capacités de basculement. Le trafic est dirigé vers la passerelle souhaitée ou le groupe d'équilibrage local.

- Pfsense offre quatre options de connectivité VPN : IPSec, OpenVPN, PPTP et L2TP.

- Dynamic DNS :Un client DNS dynamique est inclus pour vous permettre d'enregistrer votre adresse IP publique avec un certain nombre de fournisseurs de services DNS dynamiques.

- Captive Portal :
  Un Portail captif permet de forcer l'authentification, ou la redirection vers une page pour l'accès au réseau. Ceci est communément utilisé sur les réseaux de points chauds (Hot Spots), mais est également largement utilisé dans les réseaux d'entreprise pour une couche supplémentaire de sécurité sur l'accès sans fil ou Internet.

VIII. Les firewall SOPHOS :

VIII.1 SOPHOS :

Sophos est une société de logiciels et d'Appliance de sécurité fondée en 1985 basée à Abingdon en Angleterre. Ses fondateurs sont Jan Hruska et Peter Lammer, deux étudiants d'Oxford. Ses produits s'étendent aux antivirus, anti-spywares, anti-spam, pare-feux, UTM, gestion des flottes mobiles, et au chiffrement pour ordinateurs de bureau, serveurs, serveurs de courrier électronique, réseaux d'entreprise et passerelles.

VIII.2 Sophos XG Firewall :

Sophos XG Firewall est un périphérique de sécurité réseau complet, avec un pare-feu basé sur les zones et les politiques identitaires en son cœur. XG Firewall ne protège pas seulement les réseaux câblés, mais en tant que contrôleur sans fil pour les points d'accès Sophos, peut fournir un réseau sans fil sécurisé Fonctionnalité.

En plus de ses capacités anti-malware, le pare-feu XG permet de filtrer et de contrôler le contenu à travers une gamme de fonctions, y compris le filtrage Web, le contrôle des applications et la protection des e-mails.

Lorsqu'il est associé à Sophos Central, XG Firewall peut communiquer avec la sécurité des terminaux de Sophos logiciel pour améliorer la connaissance du réseau et appliquer des politiques basées sur la santé de la source et ordinateurs de destination.

XG Firewall comprend un moteur de rapport intégré complet, qui vous permet d'explorer facilement dans des rapports pour trouver les informations dont vous avez besoin, comme

montre la figure suivante, Ya t-il un grand choix de modules pour personnaliser la protection offerte par ce pare-feu, selon le besoins et le scénario de déploiement :

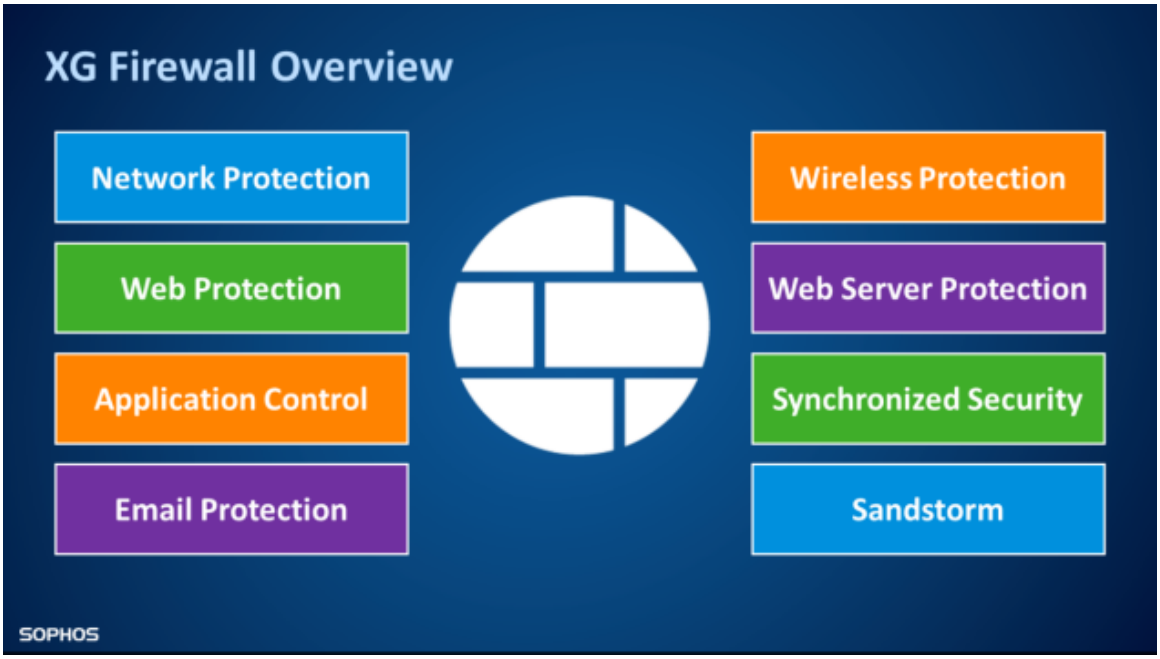


Figure VIII-1: Vue d'ensemble du pare-feu XG

VIII.2.1 Network Protection :

Toutes les protections nécessaires pour arrêter les attaques complexes et les menaces avancées, tout en fournissant un accès réseau sécurisé aux utilisateurs de confiance.

- ***Système de prévention des intrusions NextGen :***

Il fournit une protection avancée contre tous les types d'attaques modernes. Il va au-delà des ressources serveur et réseau traditionnelles pour également protéger les utilisateurs et les applications sur le réseau.

- ***Security Heartbeat:***

Il crée un lien entre vos systèmes d'extrémité protégés par Sophos Central et le pare-feu, afin d'identifier plus rapidement les menaces, de simplifier les analyses et de minimiser l'impact des attaques. Incorporez facilement le statut Heartbeat dans les politiques de pare-feu afin d'isoler automatiquement les systèmes compromis.

- ***Protection contre les menaces avancées :***

Il offre une identification instantanée et une réponse immédiate face à la majorité des attaques sophistiquées d'aujourd'hui. La protection multiniveaux identifie les menaces instantanément et Security Heartbeat fournit une réponse d'urgence.

- ***Technologies VPN avancées :***

Des technologies VPN simples et uniques, notamment le portail libre-service en HTML5 sans client pour un accès distant incroyablement aisé ou la technologie de sophos VPN SD-RED (Remote Ethernet Device) exclusive, légère et sécurisée

VIII.2.2 Web Protection :

Obtenez une visibilité et un contrôle sur l'ensemble des activités Web et applicatives des utilisateurs.

☞ *Politique Web puissante par utilisateur et par groupe :*

Elle fournit des contrôles de politique de la passerelle Web sécurisée de pointe pour aisément gérer les contrôles Web des utilisateurs et des groupes. Appliquez les politiques de sécurité en fonction de mots-clés Web chargés signalant un usage ou un comportement inappropriés.

☞ *Contrôle et QoS des applications :*

Ils permettent la visibilité et le contrôle sur des milliers d'applications grâce à des politiques de sécurité et des options de régulation du trafic (QoS) basées sur la catégorie des applications, les risques et d'autres caractéristiques. Le contrôle synchronisé des applications identifie automatiquement toutes les applications inconnues, évasives et personnalisées présentes sur le réseau.

☞ *Protection avancée contre les menaces Web :*

le moteur avancé s'appuie sur l'intelligence des SophosLabs et offre la protection ultime contre les menaces polymorphes et furtives du Web. Pour garder le réseau sécurisé, il dispose de techniques innovantes telles que l'émulation JavaScript, l'analyse comportementale et la réputation de l'origine.

☞ *Analyse puissante du trafic :*

Optimisée pour des performances optimales, l'inspection SSL Xstream (de sophos) permet une inspection à très faible latence et une analyse HTTPS tout en maintenant les performances.

VIII.2.3 Application control :

Pour empêcher les attaques d'ingénierie sociale via les applications, Sophos XG Firewall utilise des fonctions de contrôle des applications. Cela peut être utilisé pour restreindre ou restreindre les applications auxquelles les utilisateurs peuvent accéder sur le réseau.

Si une attaque d'ingénierie sociale oblige les utilisateurs à se connecter à leur compte Facebook, par exemple pour confirmer leur nom d'utilisateur, des filtres d'application peuvent être configurés pour bloquer l'accès aux applications Facebook, ce qui signifie que l'attaque ne réussira pas car les utilisateurs savent qu'ils ne peuvent pas accéder à Facebook via le réseau. Le contrôle des applications peut être utilisé pour empêcher :

VIII.2.3.1 Applications indésirables

- Certaines applications ne sont pas malveillantes et peuvent être utiles dans le bon contexte, mais sont ne convient pas aux réseaux d'entreprise. Les exemples sont les logiciels publicitaires, les outils pour administrer les PC à distance et des scanners qui identifient les vulnérabilités des systèmes informatiques

VIII.2.3.2 Applications de mise en réseau poste à poste :

- Les applications P2P peuvent contenir des vulnérabilités. Les applications peer-to-peer agissent comme des serveurs ainsi que les clients, ce qui signifie qu'ils peuvent être plus vulnérables aux exploits à distance

VIII.2.3.3 Applications à haut risque :

- Sophos catégorise toutes les applications, cela signifie que on peut appliquer le risque élevé politique de contrôle des applications et il bloquera toutes (et toute nouvelle) application classée comme à haut risque
- Un exemple de ceux-ci serait le site Web de la chaîne de télévision privée ennahar tv (live streaming), le site Web de la radio AOL le site Web de Bebo et Napster en streaming.

VIII.2.3.4 Applications à très haut risque

- De la même manière que pour la catégorie à haut risque, la catégorie à très haut risque permet vous bloquez toutes les applications classées à très haut risque
- Un exemple de ces applications serait le proxy TOR, SuperVPN et AppVPN…..

VIII.2.4 Protection Sandstorm :

Les techniques d'analyse dynamique et statique des fichiers basées sur l'IA s'associent pour apporter une intelligence sur les menaces sans précédent aux pare-feu et ainsi identifier et bloquer efficacement les ransomwares et les menaces connues et inconnues.

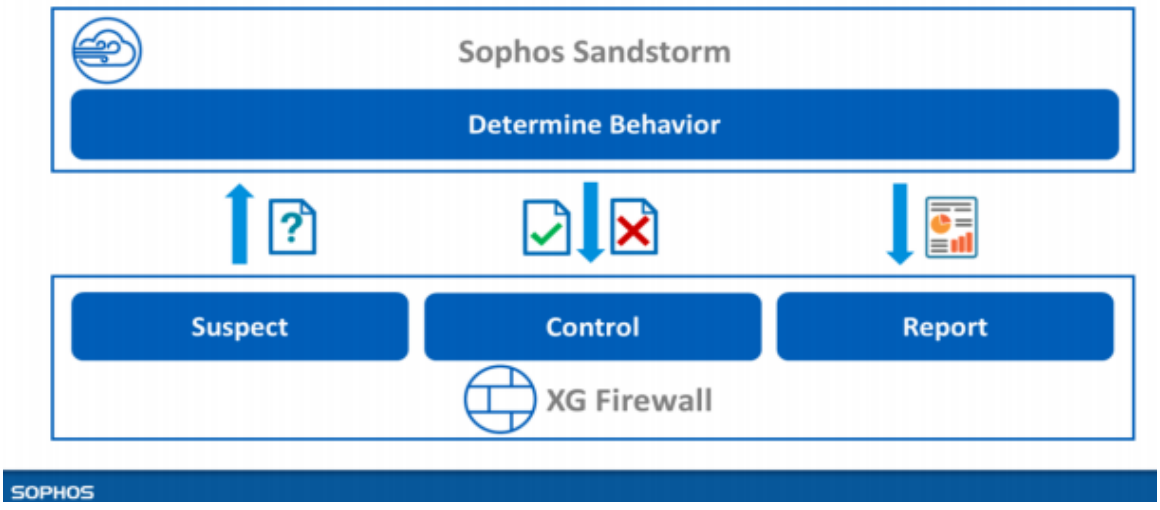


Figure VIII-2: La technique de sandstrom de sophos

Sophos Sandstorm utilise la technologie sandbox de nouvelle génération avec apprentissage automatique intégré, offrant l'organisation une couche de sécurité supplémentaire contre les ransomwares et les attaques ciblées. Ce s'intègre à votre pare-feu XG et est fourni dans le cloud, il n'y a donc pas de matériel supplémentaire obligatoire. C'est

la meilleure défense contre les derniers malwares basés sur la charge utile qui se cachent dans le phishing attaques, spam et téléchargements de fichiers.

VIII.2.5 Email Protection:

Consolidez la protection de la messagerie avec un antispam, la protection contre la fuite des données (DLP) et le chiffrement.

VIII.2.5.1 MTA (Message Transfer Agent) intégré:

Il garantit la continuité de la messagerie de l'entreprise, en permettant au pare-feu de mettre automatiquement les emails en attente lorsque vos serveurs rencontrent un problème.

VIII.2.5.2 Antispam Live:

Il protège contre les campagnes de spam, les tentatives de phishing et les pièces jointes malveillantes les plus récentes.

VIII.2.5.3 Quarantaine en libre-service:

Donnez aux utilisateurs un contrôle direct sur leur quarantaine de spams, vous faisant gagner du temps et des ressources.

VIII.2.5.4 Chiffrement de la messagerie SPX :

Exclusivité de Sophos, SPX permet l'envoi d'emails chiffrés vers n'importe quels destinataires, même ceux ne disposant pas d'une infrastructure de confiance, grâce à la technologie de chiffrement basée sur un mot de passe (brevet déposé).

VIII.2.5.5 Protection contre la perte de données (DLP) :

La DLP basée sur les politiques peut enclencher automatiquement le chiffrement ou le blocage/la notification en fonction de la présence de données sensibles dans les emails sortant de l'entreprise.

VIII.2.6 Sophos Wireless Protection :

Sophos XG Firewall peut fonctionner comme un contrôleur d'accès sans fil pour fournir une connexion sans fil sécurisée la mise en réseau. La protection sans fil peut également être associée à la gestion RED pour gérer de manière centralisée accès sans fil dans les bureaux distants. Les points d'accès Sophos fournissent un déploiement plug and play, et peut diffuser plusieurs SSID qui peuvent séparer en toute sécurité le trafic à l'aide de VLAN ou d'un VPN vers le Pare-feu XG.

Pour les réseaux invités, Wireless Protection vous permet également de configurer des portails captifs hotspot.

Les modèles de pare-feu XG dotés d'adaptateurs sans fil intégrés permettent d'analyser les points d'accès recherchez les points d'accès potentiellement indésirables sur le réseau.

VIII.2.7 Web Server Protection :

Renforcez les serveurs Web et les applications contre les tentatives de piratage, tout en offrant un accès sécurisé.

VIII.2.7.1 Modèles de politiques pour les applications d'entreprise :

Les modèles de politique de sophos permettent de rapidement et facilement protéger des applications courantes telles que Microsoft Exchange Outlook Anywhere ou SharePoint.

VIII.2.7.2 Protection contre le piratage et les attaques les plus récentes

Elle inclut toute une gamme de technologies avancées de protection, dont le durcissement des URL et des formulaires, la prévention contre les liens profonds et les traversées de répertoires, la protection contre les injections SQL et le Cross-Site Scripting (XSS), la signature des cookies, et bien plus.

VIII.2.7.3 Reverse Proxy

Doté d'options d'authentification, de déchargement SSL et de répartition de charge vers les serveurs, il garantit une protection et des performances maximales pour les serveurs accessibles depuis Internet.

VIII.2.8 Synchronized App Control :

En moyenne, 60 % du trafic applicatif n'est pas identifié. Les signatures d'application statiques ne fonctionnent pour des applications personnalisées, obscures, évasives ou toute autre application utilisant HTTP ou HTTPS générique. Application synchronisée Le contrôle sur XG Firewall identifie automatiquement toutes les applications inconnues, ce qui permet de bloquer les applications dont vous ne voulez pas et donnez la priorité à celles que vous voulez.

IX. Netfilter :

Netfilter est un module qui permet de filtrer et de manipuler les paquets réseau qui passent dans le système. Pour les noyaux Linux, Le filtrage se fait au sein même du noyau au niveau des couches 2, 3 et 4 du modèle OSI.

Il fournit à Linux :

- ✓ des fonctions de pare-feu et notamment le contrôle des machines qui peuvent se connecter, sur quels ports, de l'extérieur vers l'intérieur, ou de l'intérieur vers l'extérieur du réseau ;
- ✓ de traduction d'adresse (NAT) pour partager une connexion internet (masquerading), masquer des machines du réseau local ou rediriger des connexions ;
- ✓ et d'historisation du trafic réseau.

Iptables est la commande qui permet de configurer Netfilter. Dans les dernières versions de Linux il existe aussi une nouvelle commande qui s'appelle nft (pour nftables).

IX.1 Fonctionnement :

Netfilter intercepte les paquets réseau à différents endroits du système (à la réception, avant de les transmettre aux processus, avant de les envoyer à la carte réseau, etc.). Les paquets interceptés passent à travers des chaînes qui vont déterminer ce que le système doit en faire. En modifiant ces chaînes on va pouvoir bloquer certains paquets et en laisser passer d'autres.

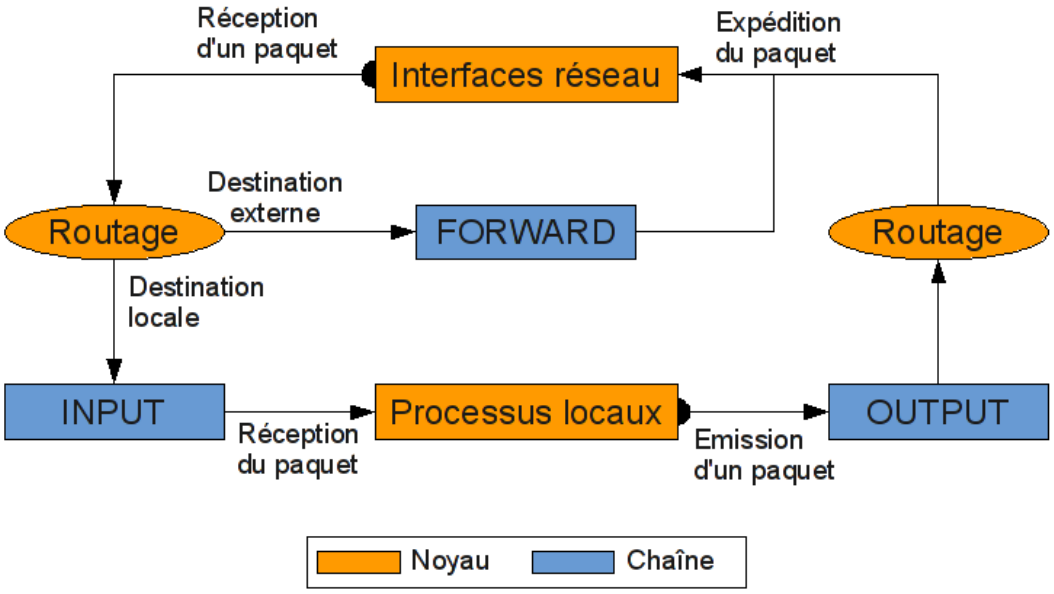


Figure IX-1:Filtrage du paquet « Netfilter ».

Filtrage :

Dans son fonctionnement le plus simple, Netfilter permet de jeter ou de laisser passer les paquets qui entrent et qui sortent.

Il fournit pour cela trois chaînes principales :

- Une chaîne INPUT pour filtrer les paquets à destination du système,
- Une chaîne OUTPUT pour filtrer les paquets émis par les processus du système,
- Et une chaîne FORWARD pour filtrer les paquets que le système doit transmettre.

En ajoutant des règles dans ces chaînes on pourra laisser passer ou jeter les paquets suivant certains critères.

Chaînes :

Une chaîne est un ensemble de règles qui indiquent ce qu'il faut faire des paquets qui la traversent.

Lorsqu'un paquet arrive dans une chaîne :

- Netfilter regarde la 1ère règle de la chaîne,
- puis regarde si les critères de la règle correspondent au paquet.
- Si le paquet correspond, la cible est exécutée (jeter le paquet, le laisser passer, etc.).
- Sinon, Netfilter prend la règle suivante et la compare de nouveau au paquet. Et ainsi de suite jusqu'à la dernière règle.
- Si aucune règle n'a interrompu le parcours de la chaîne, la politique par défaut est appliquée.

Règles :

Une règle est une combinaison de critères et une cible. Lorsque tous les critères correspondent au paquet, le paquet est envoyé vers la cible.

Les critères disponibles et les actions possibles dépendent de la chaîne manipulée.

D'autre part y a plusieurs types de firewall réseaux et applicatifs, matériels et logiciels : Sophos , forcepoint , Fortigate , ces troix solutions sont payantes, cependant il y a plusieurs firewalls gratuits comme pfSense , Endian , IPCOP .

X. Les firewall Nouvelle generation "Next-generation" :

NGFW (Next Generation Firewall) est la dernière génération de pare-feu. En français, on les appelle pares-feux applicatifs. Matériel ou logiciel capable de détecter et de prévenir les attaques sophistiquées en appliquant des règles de sécurité au niveau de l'application et du port ou du protocole de communication. Les pares-feux de nouvelle génération sont dotés de trois atouts clés : les fonctions de pare-feu d'entreprise, les systèmes de prévention des intrusions (IPS) et le contrôle des applications. Ils peuvent non seulement vérifier la conformité complète des paquets de données, mais ils peuvent également se conformer aux protocoles attendus. Par conséquent, les paquets de données devant passer par le port TCP 80 doivent utiliser le protocole HTTP. De même, ils permettent la gestion de la qualité de service (QOS : quality of service), le blocage d'URL, l'inspection approfondie des paquets (DPI : deep packet inspection), l'inspection SSL/SSH ou la détection de malware. Les options sont tellement nombreuses, que la configuration d'un tel dispositif peut devenir très complexe et nécessite l'intervention de spécialistes, c'est ce dont nous nous sommes assurés pendant notre formation.

En résumé Les pare-feu de nouvelle génération combinent les pare-feu traditionnels - filtrage de paquets, blocage d'URL et traduction d'adresse (NAT), VPN - avec des fonctionnalités de qualité de service (QoS), et des fonctionnalités absentes des pare-feu.. Cela recouvre notamment la prévention d'intrusion, l'inspection SSL et SSH, l'inspection de paquets en profondeur (DPI), la détection de logiciels malveillants basée sur la réputation, ou

encore la conscience des applications. Les fonctionnalités spécifiques aux applications sont conçues pour protéger contre des attaques de plus en plus nombreuses visant les couches 4 à 7 du modèle OSI.

Les NGFW ont la capacité de comprendre et prendre des décisions en analysant les détails du trafic. Cela à deux incidences majeures : premièrement un traitement gourmand en temps de calcul (en fonction du débit). Deuxièmement, un besoin de mises à jour régulières afin de pouvoir contrer les dernières menaces. D'ailleurs, Palo Alto Networks, un des leaders du NGFW et de la cyber sécurité publie régulièrement des mises à jour de son logiciel PAN-OS.

Dans l'état actuel des choses, les Firewall de première génération ont tendance à disparaître au profit des NGFW (Next Generation Firewall) bien qu'ils soient encore présents sur certains routeurs ou systèmes d'exploitation. Grâce à leurs systèmes de filtrage beaucoup plus avancé et leurs « compréhensions » du trafic, les NGFW agissent véritablement comme un premier mur de protection pour l'entreprise, avant même que les données arrivent sur votre réseau. Mais comme toujours en cyber sécurité, ce n'est pas une solution miracle et elle n'est efficace que si la politique de sécurité de l'entreprise est clairement définie et en complément d'autres solutions, Comme mettre en œuvre d'autres solutions de sécurité réseau à partir de ce que nous avons déjà vu dans mesures de sécurité de chapitre précédant.

Figure X-1: Comparaison de visibilité du trafic entre le simple pare feu et le NGFW

XI. Le firewall CISCO: avec ACL/policy:

La gamme Cisco Secure Firewall offre une meilleure protection de réseau contre un ensemble de menaces de plus en plus complexes et en constante évolution. Avec Cisco, vous investissez dans une base de sécurité à la fois agile et intégrée, menant à la posture de sécurité la plus solide disponible aujourd'hui et demain.

XI.1 Le edge firewall CISCO: ASA (avec ACL)

XI.1.1 Description de la gamme ASA :

Les serveurs de sécurité adaptifs de la gamme Cisco ASA 5500 s'appuient sur une plateforme modulaire capable de fournir des services de sécurité et de VPN de prochaine génération à tous les environnement.la gamme Cisco ASA 5500 met à la disposition de l'entreprise une gamme complète de services personnalisés à travers de ses diverses édition spécifiquement conçue pour le pare-feu, la prévention des intrusions, la protection des contenues et les VPN. Ces éditions offrent une protection de haute qualité en fournissant les services adaptés à chaque site. La gamme Cisco ASA 5500 permet la normalisation sur une unique plate-forme afin de réduire les frais opérationnels associés à la sécurité.

L'environnement commun de configuration simplifie la gestion et réduit les couts de formation du personnel tandis que la plate-forme matérielle commune de la gamme permet de réaliser des économies sur les pièces de rechange.

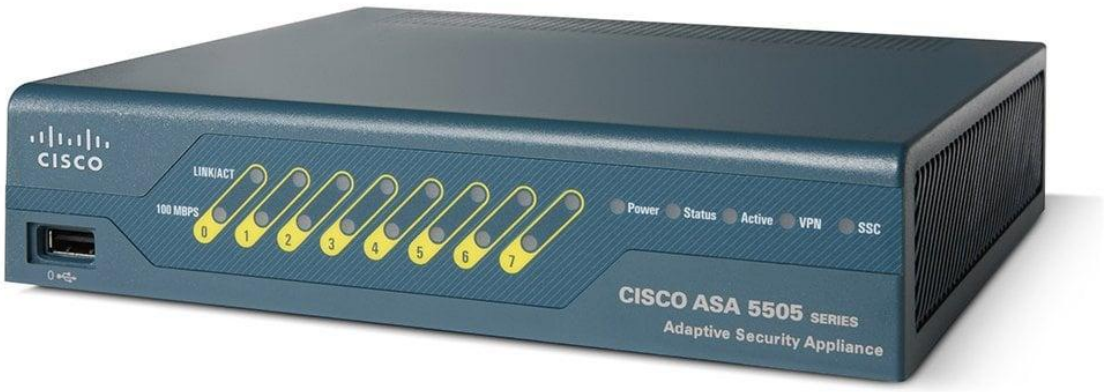


Figure XI-1: Exemple d'un périphérique Cisco la gamme de série ASA "5505"

XI.1.2 Fonctionnalités de la gamme ASA :

- ✓ Des fonctionnalités éprouvées de sécurité et de connectivité VPN
- ✓ La réduction des frais de déploiement et d'exploitation
- ✓ L'architecture évolutive des services AIM

Nous en parlerons en détail plus tard de cette gamme sur le prochain chapitre.

Les routeurs Cisco et les commutateurs de niveau 3 sont aptes à remplir le rôle de pare-feu entre les zones conçues par l'architecte de sécurité. Cependant, la limite des pare-feu est flagrante si l'on se place au niveau des couches dites hautes du modèle OSI. En effet u n filtrage même avec mémorisation de l'état ne protège aucunement un service contre une atta que purement applicative c'estàdire exploitant une faille dans un programme donné. Nous entr ons ici dans l'univers des attaques entre autres par injection de code malicieux d'un client vers une application. (13)

Il est devenu indispensable de protéger les applications contre ce type de malveillance qu i ne sont pas prise en compte par les firewalls classiques. Le déploiement (pour le protocole http) de relais (proxies) et de relais inversés (reverseproxies) dotés de fonctions de sécurité ré pond parfaitement à cette exigence de filtrage entre les clients et les serveurs. Ces équipemen ts embarquent de nombreux contrôles comme le filtrage d'URL et les scanners antivirus.

L'insécurité croît aussi avec l'utilisation intensive de la messagerie et des services Web dont les flux transitent entre applications grâce à la souplesse du langage XML embarqué à l'intérieur des protocoles HTTP ou HTTPS. Comme le montre le schéma ci-dessus, les flux 1 et 2 sont gérés par le contrôle d'état et sont autorisés à transiter dans des directions en fonction des règles de sécurité (ACL CBAC). Le flux 3, inconnu est arrêté. Le trafic, bien qu'étant conforme aux règles de sécurité , véhicule potentiellement du code malveillant et l'équipement de filtrage si perfectionné soit-il n'y verra que du feu.

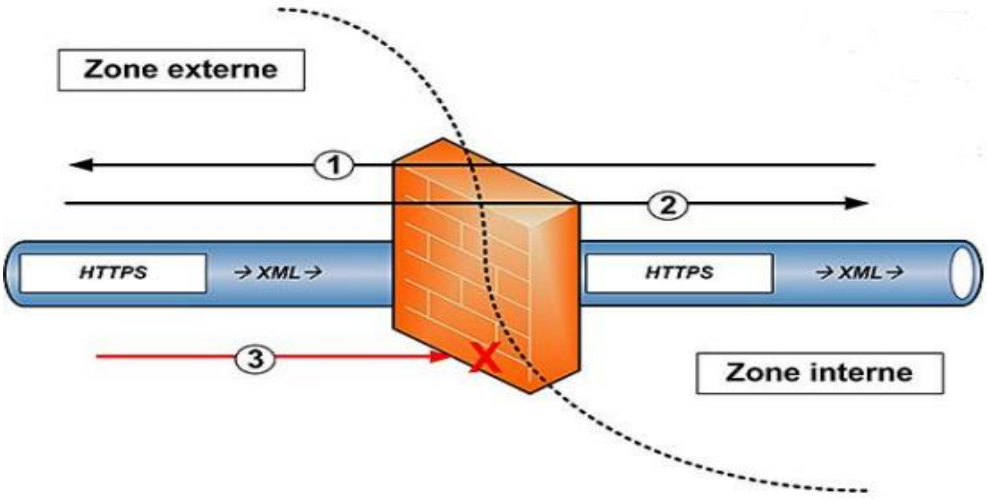


Figure XI-2:Schéma montre un pare-feu laissant passer les trafics faisant d'une session autorisée et bloquant un trafic d'une zone a faible niveau

XI.2 Le NGFW firewall CISCO: Firepower

XI.2.1 Description de la gamme Firepower :

Le pare-feu Cisco Firepower Next-Generation (NGFW) est le premier pare-feu entièrement intégré du secteur et un pare-feu de gestion unifiée pour les menaces de nouvelle génération. Il offre la visibilité et le contrôle des applications (AVC), la nouvelle génération de Firepower IPS (NGIPS), la protection avancée contre les logiciels malveillants Cisco® et le filtrage d'URL. Les pare-feux Cisco Firepower NGFW offrent une protection avancée contre les menaces avant, pendant et après une attaque.

Figure XI-3: panneaux arrière de la gamme Firepower

XI.2.2 Fonctionnalités de la gamme Firepower :

Tableau 1:Fonctionnalités de la gamme Firepower.

Bloquez plus de menaces	Confinent les programmes malveillants connus ou inconnus avec la protection AMP et le bac à sable de Cisco. Obtenez une application pare-feu (AVC) pour 4000 applications commerciales, en plus d'applications personnalisées supplémentaires.
Bénéficiez d'indices plus précis	Obtenez une visibilité supérieure dans votre environnement avec l'IPS de nouvelle génération Cisco Firepower. Définissez les priorités de votre équipe par le classement automatisé des risques et des indicateurs d'impact.
Détectez plus tôt, agissez plus rapidement	Le rapport de sécurité annuel de Cisco identifie un délai moyen de 100 jours de l'infection à la détection, au sein des entreprises. Cisco réduit ce délai à moins d'un jour.
Réduisez la complexité	Profitez d'une gestion unifiée et d'une corrélation automatisée des menaces pour toutes les fonctions de sécurité étroitement intégrées, notamment l'application pare-feu, NGIPS et AMP.
Optimisez le rendement de votre réseau	Améliorez la sécurité, et tirez avantage de vos investissements existants, grâce à l'intégration optionnelle d'autres solutions de Cisco et de tiers pour la mise en réseau et la sécurité.

XI.3 Le firewall CISCO:La gamme ISA 3000:

XI.3.1 Description de la gamme ISA 3000 :

Le Cisco® Secure Firewall ISA3000 « Industrial Security Appliance 3000 » est un véritable pare-feu industriel qui offre une protection ciblée OT basée sur une sécurité éprouvée de classe entreprise.

L'ISA3000, avec quatre liaisons de données, est un appareil robuste à montage sur rail DIN qui offre la plus large gamme de contrôles d'accès, de menace et d'application pour les environnements industriels les plus difficiles et les plus exigeants.

Figure XI-4: Cisco Secure Firewall ISA3000 avec deux ports cuivre et deux ports fibre (gauche) ou quatre ports cuivre (droite)

XI.3.2 Fonctionnalités de la gamme ISA3000 :

- ✓ Trafic contrôlé vers, depuis et entre les cellules de fabrication ou les zones industrielles
- ✓ Connectivité WAN sécurisée pour les sous-stations électriques et les actifs industriels isolés
- ✓ Accès à distance flexible et sécurisé de classe entreprise
- ✓ Services d'infrastructure réseau critiques tels que le routage IP, NAT, DNS, DHCP, etc.
- ✓ Protection contre les menaces inégalée pour tous les niveaux de mise en réseau et de calcul — du commutateur, routeur, système d'exploitation et infrastructure de calcul aux systèmes de contrôle industriels
- ✓ Prise en charge étendue des protocoles industriels pour une visibilité et un contrôle sur tous les niveaux de vos applications dans l'espace industriel et d'entreprise
- ✓ Plus de niveaux de sécurité de continuité du trafic que les autres offres dans l'espace industriel
- ✓ Critères communs de certification en sécurité informatique.

XI.4 Le firewall CISCO : gamme des routeurs firewall Meraki MX :

XI.4.1 Description de la gamme des routeurs firewall Meraki MX :

Le routeur pare-feu Cisco Meraki MX offre un contrôle complet sur la sécurité du réseau et des applications via un ensemble de services réseau. Vous n'avez donc plus besoin d'utiliser plusieurs appareils compliqués pour effectuer ce travail !

Figure XI-5: Routeurs firewall Cisco Meraki MX67W / MX67CW

Ces services incluent un pare-feu sur la couche 7, le filtrage du contenu, le filtrage des recherches web, la prévention des intrusions avec SNORT®, la mise en cache web, le WAN intelligent avec plusieurs liaisons ascendantes WAN et le basculement 4G.

Les routeur pare-feu Cisco Meraki MX est géré à 100 % dans le cloud. Leur installation et leur gestion sont réputées pour leur simplicité.

Enfin, les routeurs pare-feu Cisco Meraki MX peuvent améliorer les performances du WAN et réduire les coûts de bande passante.

XI.5 Fonctionnalités de la gamme Meraki MX :

Des fonctionnalités complètes de gestion unifiée des menaces :

- ✓ Contrôle du trafic en fonction des applications : définition de politiques en matière de bande passante selon le type d'application de couche 7 (par exemple, YouTube, Skype et connexions de personne à personne [P2P]).
- ✓ Filtrage de contenu : filtrage de contenu conforme à la législation américaine de protection des enfants vis-à-vis d'Internet (CIPA, Children's Internet Protect Act), recherches sécurisées (Google et Bing) et YouTube pour les écoles.
- ✓ Prévention des intrusions : capteur IPS compatible PCI utilisant la base de données de signatures avancée SNORT® de Cisco Sourcefire.
- ✓ Antivirus et anti-hameçonnage : moteur de protection basé sur les flux de Kaspersky.
- ✓ Politiques de sécurité et gestion des applications axées sur l'identité des utilisateurs. (14)

- ✓ Une gestion cloud à la pointe
- ✓ VPN site à site avec WAN intelligent Cisco
- ✓ Des services de passerelles pour succursales

XII. Conclusion :

Au cours de ce chapitre, nous avons pris connaissance des différents aspects liés à les Firewall. Nous avons découvert les principes de base et les catégories du pare feu et leur différents types de filtrages en effectuant une étude comparative. Nous avons étudié les Pare-feu une présentation des quelques pare-feu tel que pfsense, SOPHOS , Netfilter et la dernière génération de Firewall, et bien sûr le firewall cisco avec ACL (pour le edge firewall) et avec policy (pour le NGFW). La sécurité des systèmes informatiques est vitale pour le bon fonctionnement des systèmes d'information. Il est donc nécessaire d'assurer sa protection mais il ne faut pas perdre de vue qu'aucun firewall n'est infaillible et que tout firewall n'est efficace que s'il est bien configuré, de plus, un firewall n'apporte pas une sécurité maximale et n'est pas une fin en soi.

Toutes ces technologies sont et seront en pleine évolution, car la base même de tout cela est de jouer au chat et â la souris entre les hackers et les programmeurs de firewall ainsi que les administrateurs. Une grande bataille d'imagination qui n'aura certainement jamais de fin, Dans le chapitre suivant, nous débuterons l'étude du pare-feu Cisco ASA avant sa mise en place dans la Partie II : Contribution.

Chapitre 5 : Le Firewall ASA

I. Introduction :

La conception de l'appliance de sécurité adaptative (ASA) est née lorsque Cisco a mis en œuvre une solution réseau d'autodéfense. En effet, Cisco s'est imposé dans le domaine des firewalls, son célèbre modèle PIX (Private Internet Exchange) se présentant dès l'origine sous la forme d'un équipement compact et fiable, libérant les administrateurs de la limitation de la gestion des systèmes informatiques. « Opérations de bas niveau ». Ce n'est pas le cas pour les autres pare-feux qui sont presque exclusivement conçus pour être installés sur des plateformes Unix ou Windows. La série PIX a disparu en 2008. Il est remplacé par la série ASA (Adaptive Security Equipment), qui perpétue la tradition des équipements dédiés et autonomes.Cette nouvelle famille fait la part belle aux techniques émergentes et associant un pare-feu très puissant à un système qui offre les services VPN, Comme les VPN SSL qui ont pour vocation de remplacer les tunnels VPN basés sur IPSec dédiés aux utilisateurs distants. Le but avoué de cette technologie est de faciliter l'accès (sécurisé) aux applications publiées au format WEB à tous les employés et partenaires de l'entreprise en fonction de rôles préalablement définis et finement attribués. Le firewall est devenu ainsi au-delà de sa fonction de filtrage réseau une véritable passerelle multi niveau assurant des services d'accès et de sécurité sur toute l'étendue du modèle OSI, l'ASA est la solution proposée par Cisco pour garantir un réseau accessible de l'extérieur et sécurisé. Il met en place une défense face aux menaces, et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau. Grâce à une interface graphique et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises des services de sécurité du réseau avec un meilleur coût et une simplicité d'utilisation.

Quelques exemples de produits ASA :

Figure I-1: Quelques produits de la gamme ASA

Le développement du Modèles ASA :

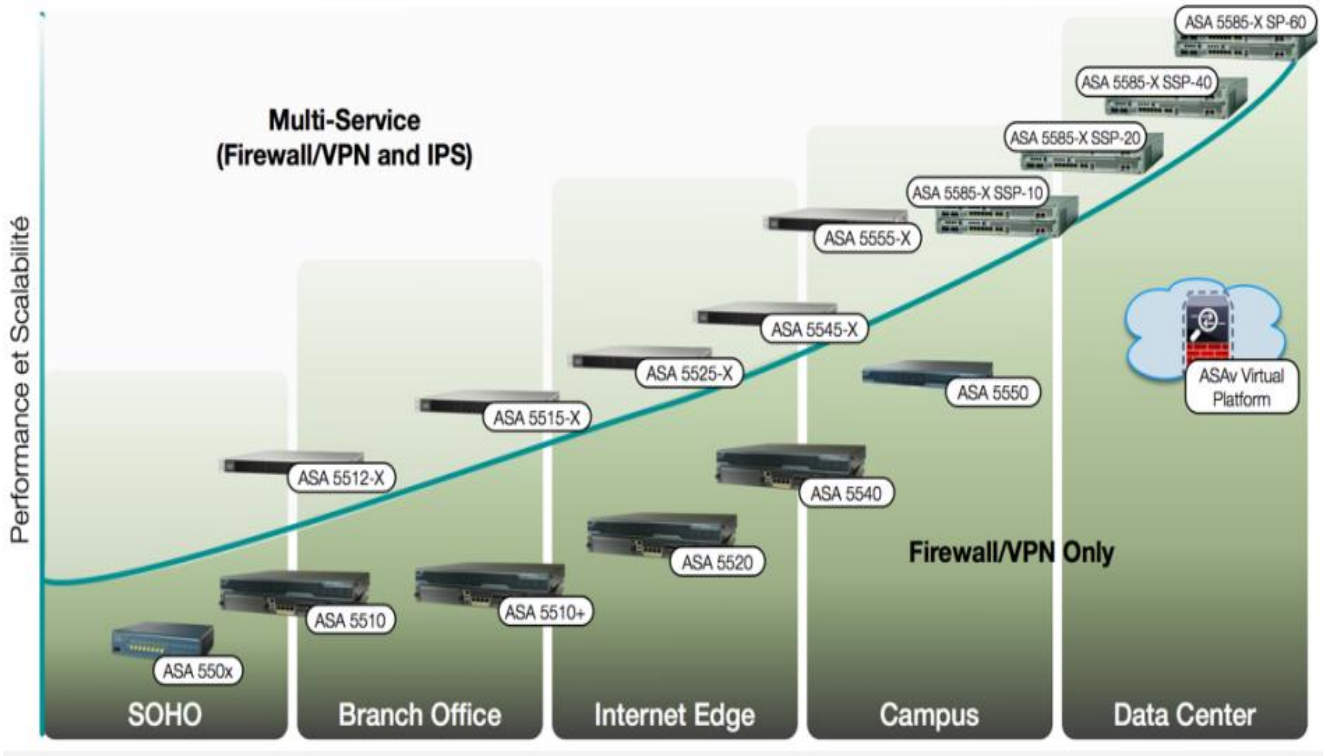


Figure I-2 : Graphe du développement du model par rapport a la performance et scalabilité

II. Fonctionnalités avancées :

II.1 Virtualisation :

Un même périphérique ASA peut être divisé en plusieurs ASA virtuels (Security context) permettant de servir par exemple trois clients différents

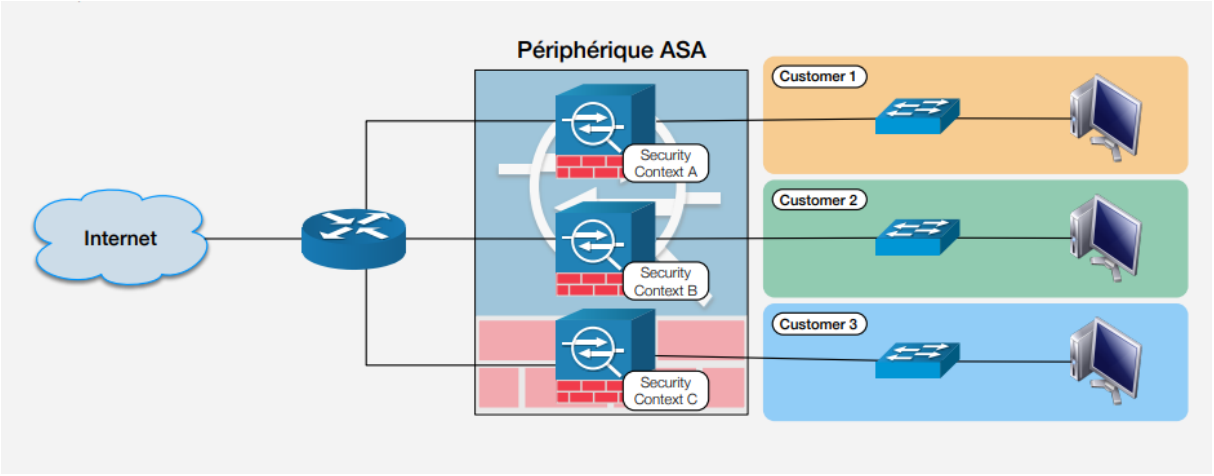


Figure II-1: Shéma d'un FW ASA divisé en plusieurs ASA virtuels (Security context) servir par 3 clients déférant

- ☞ Une Appliance physique peut être partition en plusieurs instances virtuelles appelés contextes de sécurité (Security Contexts)
- ☞ Chaque contexte est considéré comme un périphérique indépendant, avec ses propres règles, interfaces et administrateurs

- La plupart des fonctionnalités IPS sont supportées excepté VPN et les protocoles de routage dynamiques

II.2 Haute disponibilité :

Deux ASA peuvent être reliés dans un mode de fonctionnement Active/Standby pour permettre la redondance d'équipements et a la tolérance de pannes, un ASA est promu comme périphérique primaire (Active) tandis que l'autre est mis en mode StandBy,le software, les licences, la mémoire et les interfaces doivent être identiques sur les deux ASA.

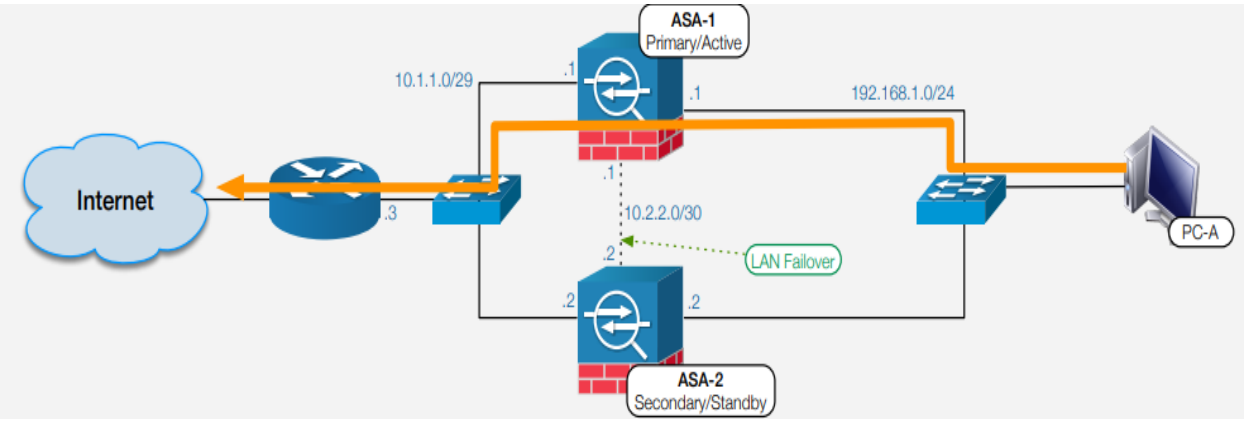


Figure II-2 : Le fonctionnement Active/Standby de ASA

- Le trafic provenant de PC 1 préfère utiliser le chemin passant par ASA-1
- ASA-1 et ASA-2 sont des périphériques identiques configurés pour la redondance. Chaque équipement surveille l'activité de l'autre via le lien LAN Failover
- Si ASA-2 détecte que ASA-1 est défaillant, alors ASA-2 devient périphérique Primary/Active et le trafic est redirigé par lui.

II.3 Identity Firewall :

L'ASA permet un contrôle d'accès en utilisant les informations d'authentification d'un annuaire Active Directory, permet de créer des règles permettant des utilisateurs ou groupes d'utilisateurs au lieu de règles traditionnels basées sur les adresses IP.

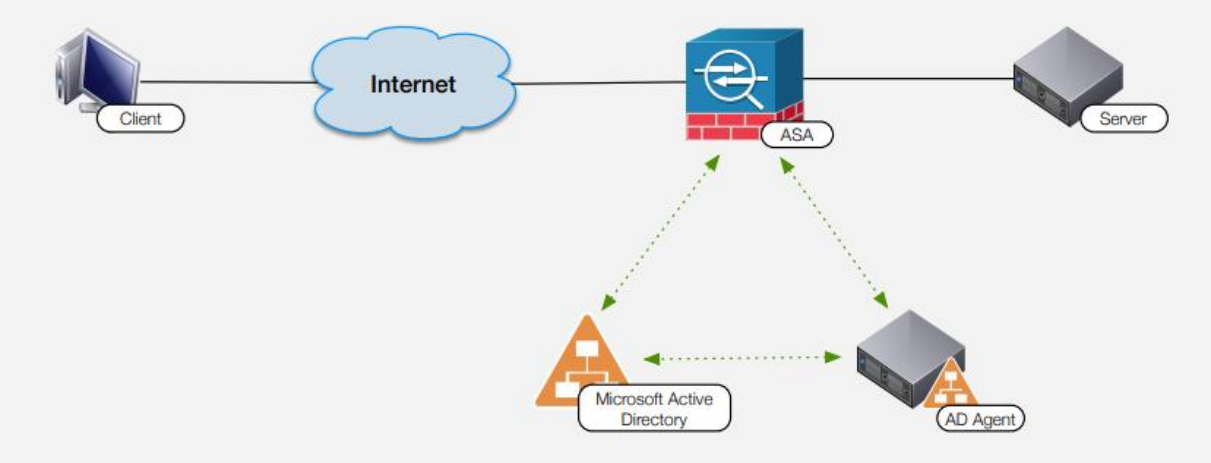


Figure II-3: exemple d'un client qui tente d'accéder à des ressources sur un serveur doit d'abord s'authentifier en utilisant Microsoft Active Directory

II.4 IDS/IPS :

Des fonctionnalités IPS peuvent être ajoutées via des modules additionnels :

- ☞ Le module Cisco Advanced Inspection and Prevention Security Services Modules (AIP-SSM) peut être utilisé sur le périphérique ASA 5540
- ☞ Le module Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC) peut être utilisé pour le périphérique ASA 5505

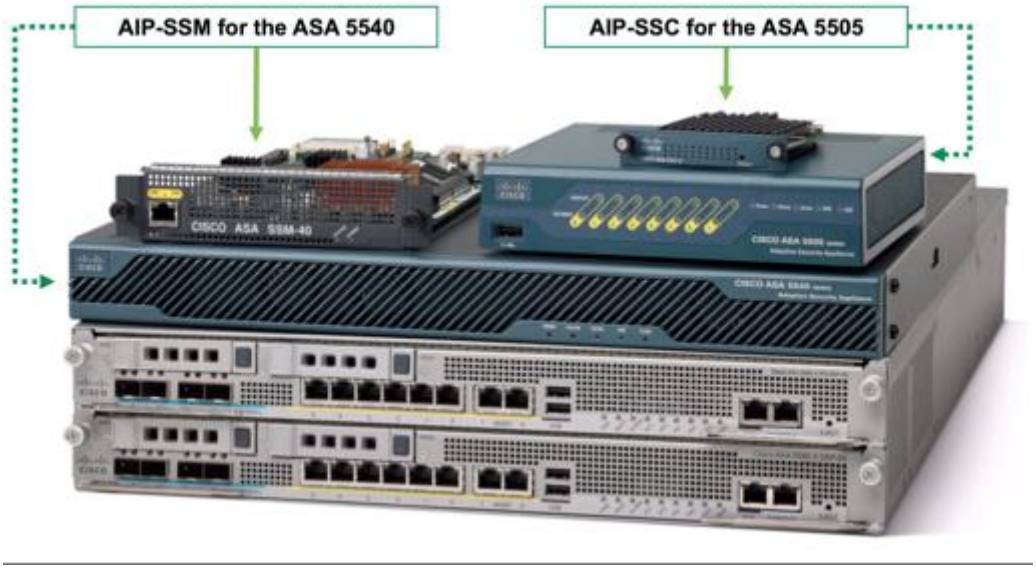


Figure II-4 : AIP-ssm pour l'ASA 5540 et aip-ssc pour l'ASA 5505

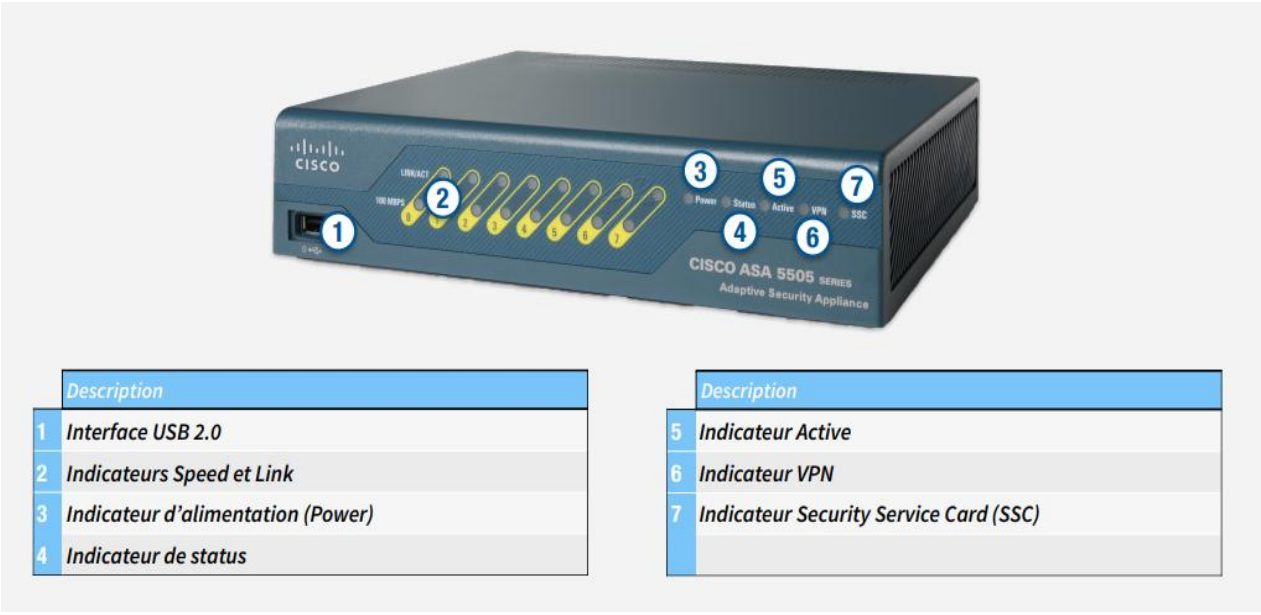
II.5 Threat Control :

En plus des fonctions IPS, des outils anti-malware et gestion des risques peuvent être ajoutés via le module Content Security and Control (CSC).

III. Présentation du Cisco ASA 5505 : (13)

Une entreprise qui dépend de son réseau a besoin d'une sécurité sans faille. Les Appareils de Sécurité Adaptative de la Gamme Cisco ASA 5505 garantissent une sécurité optimale suffisamment souple pour s'adapter à la croissance et à l'évolution de l'entreprise.

Le firewall ASA 5505 se présente sous la forme d'un petit boîtier dont les dimensions en font le plus compact du marché : 20 cm x 17 cm x 4,5 cm. Il s'adresse principalement aux petites et moyennes entreprises, aux travailleurs à distance et aux petites organisations. En revanche, ses possibilités sont proches de celles des modèles avancés. Cependant, les fonctionnalités de haute disponibilité ne sont pas fournies (avec une licence de base) et le nombre de VLAN gérés est limité. Il est également impossible d'utiliser la technologie de contexte de sécurité qui permet de créer plusieurs instances de pare-feu virtuels au sein du même périphérique physique. Le pare-feu ASA 5505 est un appareil d'entrée de gamme avec des capacités de configuration réseau relativement limitées par rapport aux modèles supérieurs. D'autre part, il utilise des outils de gestion très avancés..



	Description
1	Interface USB 2.0
2	Indicateurs Speed et Link
3	Indicateur d'alimentation (Power)
4	Indicateur de status

	Description
5	Indicateur Active
6	Indicateur VPN
7	Indicateur Security Service Card (SSC)

Figure III-1: ASA 5505 : Présentation (panneau avant)

La face avant du boîtier comporte des LED indiquant l'état de l'équipement et des conne xions réseau.

	Description
1	Alimentation électrique (48 VDC)
2	Slot pour Security Services Card (SSC)
3	Port Console série
4	Slot pour câble anti-vol (Kensington)

	Description
5	Bouton de réinitialisation (Reset)
6	2 ports USB 2.0
7	Ports Ethernet 10/100 (ports 0 - 5)
8	Ports PoE (Power of Ethernet) 10/100 (ports 6 et 7)

Figure III-2 : ASA 5505 : Présentation (panneau arrière)

Sur la face arrière nous trouvons les huit ports d'un commutateur Ethernet qui ont la possibilité d'être organisés en trois VLAN locaux. Le port zéro est par défaut réservé à l'interface externe connectée au réseau le moins sûr. Les sept autres ports sont considérés comme étant internes au réseau. Les deux derniers ports offrent une alimentation électrique afin d'alimenter un poste téléphonique IP. Le connecteur de la console est entouré de bleu et les deux ports USB sont réservés à de futures applications. Un emplacement est réservé pour accueillir une carte d'extension qui prend en charge un module dédié à l'inspection virale. Sur la droite du port console, la petite fente permet d'attacher le firewall à un support à l'aide d'un câble de sécurité du même type que ceux utilisés pour les ordinateurs portables.
Cisco annonce une capacité de traitement de 150 Mbps par le firewall et 100 Mbps lorsque le chiffrement est activé. En fonction des licences, le firewall est limité en nombre d'utilisateurs normaux ou utilisant les connexions protégées de type VPN IPSec ou VPN SSL.

III.1 Caractéristiques clés de la plateforme : (15)

L'ASA 5505 est idéal pour les environnements Broadband en supportant un débit en « firewalling » de 150 Mbps et de 100 Mbps pour le trafic VPN IPSec 3DES/AES-255 (soit un débit 2,5 fois supérieur au débit firewall et 33 fois plus que le débit VPN d'un Cisco PIX 501).

L'ASA 5505 inclut les mêmes technologies et les mêmes services firewall/IPSec/VPN SSL que le reste de la gamme Cisco ASA 5500, comme par exemple :

- ✓ Le support des moteurs d'inspection applicatif couvrant plus de 30 protocoles TCP/IP : DNS/FTP/SMTP/RPC/HTTP/Skinny/SIP/H323… pour valider la conformité des échanges par rapport aux RFC respectives, reconnaître les tentatives de mascarades et permettre d'interdire les commandes standards et étendues.

- ✓ Le support d'ajouts de motifs ou « patterns » basés sur les expressions régulières pour personnaliser les moteurs d'inspection applicatif.
- ✓ Les services d'identification et de contrôle d'accès, incluant la gestion d'objets et la corrélation des messages syslog avec les ACL respectives.
- ✓ Le support du mode Firewall routé (Layer 3) ou du mode Firewall transparent (Layer 2).
- ✓ Les services VPN Site à Site avec support de la QoS, le support d'OSPF pour le routage dynamique.
- ✓ Le fonctionnement en tant que client VPN Hardware pour proposer des tunnels à la demande ou permanents, avec support d'authentification des utilisateurs.
- ✓ Le support de connexions d'accès distant de type VPN IPSec, support de NAC, et support de multiples OS comme client IPSec.
- o Le support de connexions d'accès distant de type VPN SSL soit en mode sans client ou avec le client SVC (full-tunneling).

De facto, Comme on a vue dans la figure Figure III-3 l'ASA 5505 intègre 8 ports 10/100 switchés configurables dans des VLANs multiples (home,business,outside) :

- ✓ De base deux ports compatibles PoE (support de 802.3af) sont fournis pour auto-alimenter des téléphones IP, des points d'accès WiFi, des caméras de vidéo surveillance ou d'autres types d'équipements.
- ✓ Support futur de cartes de service (SSC) pour une expansion possible de l'unité 5505 vers d'autres services de sécurité type IPS ou Anti-X.
- ✓ Support du mécanisme de mise à jour automatique depuis Cisco Security Manager (CSM).
- ✓ Fourniture d'un client/serveur/relai DHCP, support de PPPoE, support de Dynamique DNS pour couvrir une échelle importante d'options de déploiement.
- ✓ Support d'une configuration FailOver de type Actif/Passif (sans échange d'états des connexions) et d'architecture Dual ISP pour fournir de la redondance.

III.2 Le principe de « licensing » : (15)

Le licencing est articulé autour du nombre d'utilisateurs, il existe 3 niveaux de licence : 10 utilisateurs, 50 utilisateurs, et illimité (comme sur le Cisco PIX 501).

Dans la licence de base, sont inclus :

- le support de 10 tunnels concurrents simultanés IPSec
- le support de 2 tunnels concurrents simultanés VPN SSL
- la possibilité d'augmenter le nombre de tunnels simultanés VPN SSL de 2 jusqu'à 25.

Introduction d'une licence optionnelle "Security Plus" permettant de bénéficier des spécificités suivantes:

- ✓ permet de doubler le nombre maximum de sessions concurrentes simultanées du firewall intégré (de 10K à 25K)
- ✓ permet de doubler le nombre maximum de tunnels VPN IPSec simultanées (de 10 à 25)
- ✓ permet de lever les restrictions sur le VLAN Home pour offrir des services autour d'une réelle zone démilitarisée. - Active le support de VLAN trunk 802.1q.
- ✓ Active le support d'architecture Dual ISP pour proposer la continuité des services fournis par l'ASA 5505 sur une connexion sortante Internet redondée.
- ✓ Active le support d'un FailOver de type Actif/Passif (sans échange d'états sur les connexions courantes), afin de fournir un service de haute disponibilité entre deux unités ASA 5505.

NB : la licence "Security Plus" peut être utilisée pour tous les niveaux de licence utilisateur (10, 50, ou illimité).

III.3 Les états de pare-feu ASA :

Comme on'a déjà vue sure « Les différents types de filtrages » dans le chapitre précédant, ASA nous permit deux états :

III.3.1 Statless « sans etat » :

Le pare feu ce basé que aux ACL's pour permit ou refuser le paquet, Cette méthode n'est pas sécurisé et n'est plus utile, par ce que l'agresseur il peut manipuler aux paquet, dépend aux acl attribuer aux pare feu et gérer une attaque (adresse spoofing attaque), On modifiant le port, Protocol, adresse source/destination ……

III.3.2 Statfull packet inspection FW « pare-feu a état »:

Il travaille avec des état (tableaux des états) Ils prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire (tableaux des états) les différents attributs de chaque connexion.

IV. Détail de fonctionnement :

IV.1 Le fonctionnement d'ASA :

L'ASA offre deux modes pour ces utilisateurs :

Le mode « **routed** »(par défaut) est de niveau 3 : quand il ya de trafic, l'ASA est comme un saut sur routeur (routeur hop in the network) il devine comme un routeur à côté de son rôle de sécurité, il peut faire le routage comme un Routeur.

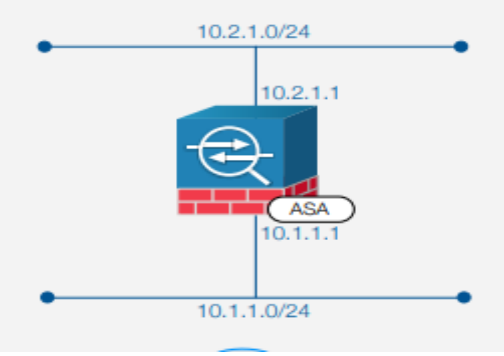


Figure IV-1: ASA en mode Routed.

Donc le mode routed est permet :

- Mode de déploiement traditionnel pour un firewall
- Sépare deux domaines de couche 3
- Permet également la configuration NAT
- Applique les règles aux flux de trafic qui transitent par ce firewall Ne permet pas le filtrage de paquets entre deux hôtes du même sous-réseau

Le mode « **transparent** » est de niveau 2 : il facilite la configuration du réseau et permet de cacher le pare-feu (le rôle d'un switch).on utiliser aussi le mode transparent pour autoriser le trafic qui est bloqué par un routeur en utilisent les ACLs.

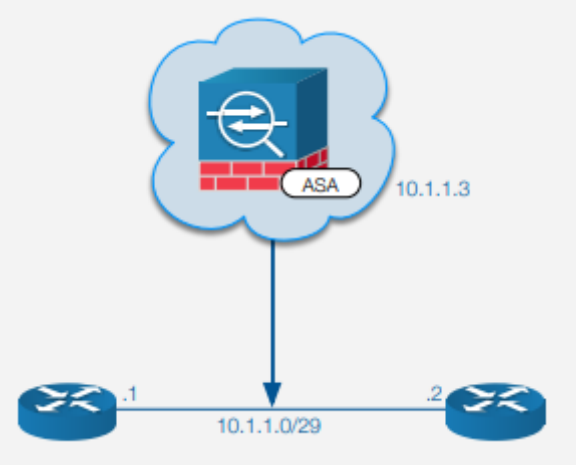


Figure IV-2 : ASA en mode transparent.

Donc le mode transparent permet :

Opère sur la couche 2

- S'intègre sur les réseaux existants sans devoir redéfinir l'adressage IP
- Simplifie le filtrage interne et la segmentation des réseaux
- Permet la protection et le filtrage sur un même sous-réseau

Mais les fonctions suivantes ne sont pas supportés en mode Transparent :

NAT

- Protocoles de routage dynamiques
- Routage multicast
- Pas de support d'adresses IPv6 Anycast ⊙ DHCP Relay
- Qualité de service (QoS)
- Point de terminaison VPN

IV.1.1 Configurer le mode de fonctionnement :

Le mode par défaut est Routed pour utiliser le mode Transparent on utilise la commande firewall transparent :

ASA(config)# firewall transparent

Switched to transparent mode

ASA# show firewall

Firewall mode : Transparent

Pour revenir au mode Routed, on doit utiliser la commande no firewall transparent :

ASA(config)# no firewall transparent

Switched to router mode

ASA# show firewall

Firewall mode : Router

IV.2 Configuration de base :

Nous présentons la configuration du firewall ASA en nous basant principalement sur la ligne de commande (CLI).

Le firewall est livré avec une configuration de base qui comporte deux interfaces routées. Ce sont des interfaces VLAN identiques à celles des commutateurs de la gamme. Chacune d'entre elle reçoit une désignation qui est reprise par exemple dans les commandes de traductions d'adresse.

Les deux interfaces VLAN de la configuration de base sont nommées inside et outside. Chacune d'elle est associée à un niveau de sécurité :

```
!
interface Vlan1
nameif inside
security-level 100
```

```
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
ERROR: This license does not allow configuring more than 2
interfaces with nameif and without a "no forward" command on this
interface or on 1 interface(s)
nameif outside
security-level 0
ipaddress 192.168.2.1 255.255.255.0
```

Dans cet extrait de configuration, nous avons remarqué que la commande nameif fournit des noms pour les deux interfaces. La commande security-level est suivie d'une valeur indiquant son niveau de sécurité. Plus le nombre est élevé, plus l'interface et le réseau qui y sont connectés sont fiables (le maximum est de cent). Veuillez noter que par défaut, le trafic est uniquement passé du niveau le plus élevé au niveau le plus bas entre les deux interfaces. Dans l'extrait de configuration ci-dessus, les membres du VLAN 1 (représentant l'intérieur du réseau) peuvent initier une connexion au VLAN 2 (représentant l'extérieur du réseau). Afin de déroger à cette règle de base, l'utilisation d'ACL est indispensable. Une caractéristique de l'ASA 5505 avec la licence de base est qu'elle nécessite un trafic à sens unique entre deux des trois interfaces VLAN qui peuvent être créées.Si l'on décide de configurer trois interfaces de type VLAN. Le message suivant apparaît alors :

Ce message nous met en garde et indique qu'il faut limiter le trafic entre deux des trois interfa ces.

```
interface Vlan3
 no forward interface Vlan1
nameif DMZ
 security-level 50
```

Ici, l'interface VLAN3 est configurée de telle sorte qu'elle ne puisse pas initialiser de commu nication vers l'interface VLAN1. D'autre part, son niveau de sécurité est de 50 ce qui la situe entre les valeurs des deux autres interfaces.

```
interface Ethernet0/0
switchport access vlan 2
!
 interface Ethernet0/1
!
 interface Ethernet0/2
switchport access vlan 3
```

Les interfaces physiques du commutateur Ethernet intégré dans l'ASA sont au final raccordées aux divers VLAN en utilisant la commande *switchportaccess vlan* suivie bien entendu d'un numéro de VLAN. Pour ce faire, il faut utiliser le mode de configuration d'une interface physique. Les interfaces dans le VLAN1 n'apparaissent pas dans le rappel de configuration.

Tout comme pour les autres équipements, le firewall ASA dispose du protocole SSH afin de sécuriser les accès administratifs.

```
ASA-5505(config)# domain-name bea.dz
ASA-5505(config)# crypto key generate rsa modulus 2048
ASA-5505(config)# username hma password riahla
ASA-5505(config)# aaa authentication ssh console LOCAL
ASA-5505(config)# ssh 192.168.1.2 255.255.255.255 inside
ASA-5505(config)# ssh timeout 5
ASA-5505(config)# ssh version 2
ASA-5505(config)# management-access inside security
```

Cet extrait de configuration est relativement explicite. Notons toutefois la simplification en comparaison avec un routeur. Ici, les interfaces VTY ont disparu. Il est simplement indiqué au protocole SSH l'adresse IP de la station d'administration et l'interface VLAN sur laquelle ce trafic aboutit. Il s'agit en l'occurrence de l'interface inside qui correspond à l'interface VLAN1.

```
username hma password Vtb/ZufSkY.w0v3m encrypted privilege 15
```

Le compte local (utilisateur hma) vu après un rappel de la configuration montre ici son mot de passe qui est chiffré et son niveau de privilège.

V. *Exigences de sécurité :*

Nous avons évoqué la place des firewalls dans l'architecture réseau en insistant sur le fait qu'elle ne se limite plus uniquement aux frontières traditionnelles. Des services hautement sensibles comme la téléphonie, bien qu'hébergés à l'intérieur du périmètre, nécessitent une protection accrue afin que rien d'autre que les protocoles associés à la voix ne pénètre dans la zone des serveurs dédiés à la voix. Il en va de même pour d'autres zones applicatives. Toutefois, les firewalls ne quitteront sans doute jamais les emplacements qui marquent la séparation du réseau d'une entreprise avec le monde extérieur. (16)

La valeur ajoutée des premiers équipements de filtrage était bien faible malgré l'adjonction des services de traduction d'adresses devenus indispensable avec l'avènement

d'Internet et les menaces qu'il ne manque pas de charrier. C'est pourquoi, les éditeurs de firewalls les ont dotés de fonctionnalités plus évoluées qui concentrent sur un équipement unique des fonctions annexes comme l'authentification des utilisateurs et la surveillance approfondie des protocoles applicatifs. (16)

Ce sont ces techniques que nous allons décrire mais auparavant, définissons comme de coutume des exigences de sécurité par rapport aux fonctionnalités que nous venons d'évoquer.

Tableau 2:Tableau IV.2 1 : Exigences de sécurité Firewall.

Exigences de sécurité Firewall pour les fonctions de filtrage IP	
Filtrage IP avec conservation de l'état des sessions	ACL
Implémentation de DMZ	Configuration
Traduction d'adresse et protection des serveurs publ ics	NAT
Le NAT Overload translater plusieurs adresses IP par une adresse IP	PAT
Détection et protection contre les menaces au sein des protocol es applicatifs Service d'inspection des protocoles applicatifs	Service d'inspection des protocoles ap plicatifs

V.1 Les ACL :

V.1.1 INTRODUCTION AUX ACL :

Les ACL (en anglais « Acces Control Lists ») ou en Français « Listes de Contrôle d'Accès » est un concept qui permet d'établir des règles de filtrage sur les routeurs, pour régler le trafic des datagrammes en transit.

Les ACL permettent de mettre en place un filtrage dit « statique » des datagrammes. C'est-à-dire d'instaurer un certain nombre de règles à appliquer sur les champs concernés des en-têtes

des divers protocoles.

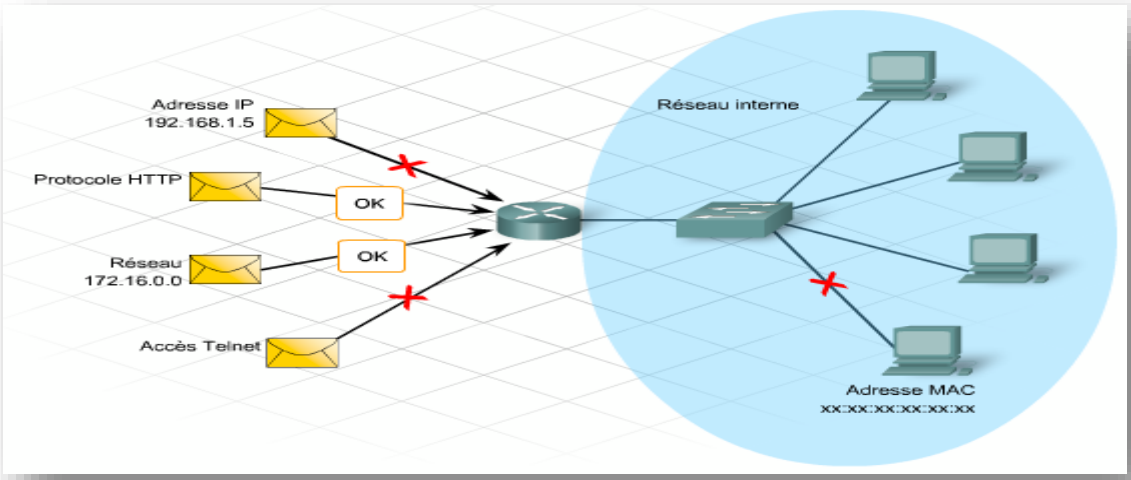


Figure V-1 : Schéma générale d'une ACL

Parmi les applications des ACL On peut citer :

- Interfaces.
- NAT.
- VPN.
- Router MAP.
- QOS ……

Tableau 3: Applications des ACLs sure ASA.

Utilisation ACL	Type d'ACL	Description
Gérer le trafic inter-réseaux	*Extended*	• Par défaut, l'ASA n'autorise pas le trafic provenant d'un niveau de sécurité plus faible vers une interface ayant un niveau de sécurité plus haut sauf si explicitement autorisé
Identifier le trafic des règles AAA	*Extended*	• Utilisé dans les listes d'accès AAA pour identifier le trafic
Identifier les adresses pour NAT	*Extended*	• Les règles NAT permettent d'identifier le trafic local pour effectuer la translation d'adresses
Etablissement d'un accès VPN	*Extended*	• Utilisé dans les commandes VPN
Identifier le trafic Modular Policy Framework (MPF)	*Extended*	• Utilisé pour identifier le trafic dans une Class Map, qui est utilisé dans les fonctionnalités qui supportent MPF
Identifier la redistribution de route OSPF	*Standard*	• Les ACL Standards n'incluent que l'adresse de destination • Utilisé pour contrôler la redistribution des routes OSPF
Contrôler l'accès réseau pour les réseaux IPv6	*IPv6*	• Utilisé pour contrôler le trafic sur les réseaux IPv6

Et on peut appliquer les ACL par :

- Par interface : fa0/2 gig ……
- Par direction : in ou out (entrant ou sortant).

- ☞ Par IP protocol :Ipv4/Ipv6.

V.1.2 Fonctionnement des ACL :

Quel que soit le type d'ACL; leur utilisation se fait toujours selon les mêmes principes généraux :

- Première étape : En mode « config »
  La création d'une ACL, exprime la détermination d'un ensemble de règles. Chaque règle est une (condition, action). Les règles sont interprétées séquentiellement. Si la condition analysée ne correspond pas, on passe à la règle suivante.

  Si la condition correspond, l'action est effectuée, et le parcours de l'ACL est interrompu. Par défaut, toutes les ACL considèrent la règle (VRAI, REJET). Si aucune des règles précédentes n'a été prise en compte, c'est-à-dire que tout datagramme non explicitement accepté par une règle préalable sera rejeté.

- Deuxième étape : En mode « config-int »,
  On applique une ACL en entrée (in) (respectivement en sortie (out)), c'est-à-dire que l'on décide d'activer la liste de règles correspondante à tous les datagrammes « entrant » dans le routeur (respectivement « sortant » du routeur) par l'interface considérée. En conséquence, sur un routeur il peut y avoir au maximum 2 ACLs (IP) par interface.

Lorsque l'on construit une ACL, les règles sont ajoutées à la fin de la liste dans l'ordre dans lequel on les saisit. On ne peut pas insérer de règle dans une ACL, ni même en supprimer. Le seul moyen reste d'effacer complètement l'ACL et de recommencer. En situation réelle, pour saisir une ACL assez longue, il peut être judicieux de créer un fichier texte et de le faire prendre en compte par la suite comme un fichier de capture de configuration de routeur …

V.1.3 Similarités entre ACL IOS et ACL ASA :

- ✓ Dans les deux cas, les ACL sont composés d'un ensemble de règles ACE
- ✓ Les ACL sont traités de manière séquentielle depuis le haut vers le bas
- ✓ Dès qu'une entrée ACE correspond, on sort de l'ACL sans consulter les règles suivantes
- ✓ Ils possèdent une entrée de refus par défaut à la fin de la liste
- ✓ Ils respectent la règle suivante : une ACL par interface, par protocole, par sens
- ✓ Ils peuvent être activés/désactivés selon des plages horaires définies

V.1.4 Différences entre ACL IOS et ACL ASA :

- ☞ Les ACL ASA utilisent un masque de sous-réseau (ex. 255.255.255.0)
  - ➢ Les ACL IOS utilisent un masque Wildcard (ex. 0.0.0.255)

- ☞ Les ACL sont toujours nommées au lieu d'être simplement numérotés

- Les ASA ACLs peuvent être numérotés mais contrairement aux ACL IOS, les numéros n'ont aucune signification

Par défaut, les niveaux de sécurité appliquent les contrôles d'accès sans configuration explicite d'ACL

V.1.5 Types des ACL :

V.1.5.1 Les ACL standards :

Les ACL standards n'offrent pas énormément de possibilités. Elles permettent simplement de créer des règles dont les conditions ne prennent en compte que les **adresses IP sources** des datagrammes IP analysés. C'est assez contraignant, mais cela permet déjà un certain nombre de manipulations intéressantes.

La commande pour créer une ACL standard (ou ajouter une règle à une ACL existante) est la suivante :

Access List<#ID> {permit/deny} <@IP source><masque>

Le numéro de liste (#ID) doit être compris entre 1 et 99 | 1300 et 1999 pour une ACL standard (tapez un ? après la commande « access-list » pour visualiser toutes les fourchettes possibles en fonctions des types d'ACL).

« Permit ou deny » indique l'action à prendre (deux seules actions sont possibles : autorisé ou refusé)

L'IP source + masque indique la condition.

V.1.5.2 Les ACL étendues:

La syntaxe un peu plus complète des ACL standards. Elle permet de créer des règles de filtrage plus précises. En utilisant des conditions applicables sur d'autres champs des en-têtes des divers protocoles (IP,TCP,UDP).

La commande pour créer une ACL (ou ajouter une règle à une ACL existante) est la suivante :

Access-list <#ID> {permit/deny} <protocole><@IPsource><masque> [port]<@IPdest><masque> [port] [established

- **Le numéro de liste (#ID)** doit être compris entre 100 et 199 | 1300 et 1999 pour une ACL étendue.
- **« Permit ou deny »** indique l'action à prendre (deux seules actions sont possibles : autorisé ou refusé par rapport aux trafique), on peut maitre un commentaire avec l'action **Remark .**

- **« protocole »** indique le protocole concerné par le filtre (tapez un ? pour avoir la liste des protocoles disponibles). Les protocoles indiqués peuvent être de différents niveaux jusqu'au niveau transport (ex : TCP ou UDP, mais également IP ou ICMP). La distinction sur les protocoles applicatifs (http, FTP …) se fera sur le champ « port ».
- **IP et masques** suivent les mêmes règles que pour les ACL standards,
- **« port »** permet d'indiquer un numéro de port (ou son nom symbolique si il est connu http, FTP, Telnet, …). Notez qu'un port doit être précédé d'un opérateur (ex : « eq http » ou « eq 80 » ou « lt 1024 ») avec « eq » (pour « equal »), « lt » (pour « (lowerthan), moins grand que») ou « gt » (pour (greaterthan), plus grand que), « neq » (pour non equal) …
- **« established »** indique qu'il s'agit d'une communication TCP déjà établie (et donc pas d'une demande de connexion avec le bit « syn » positionné).

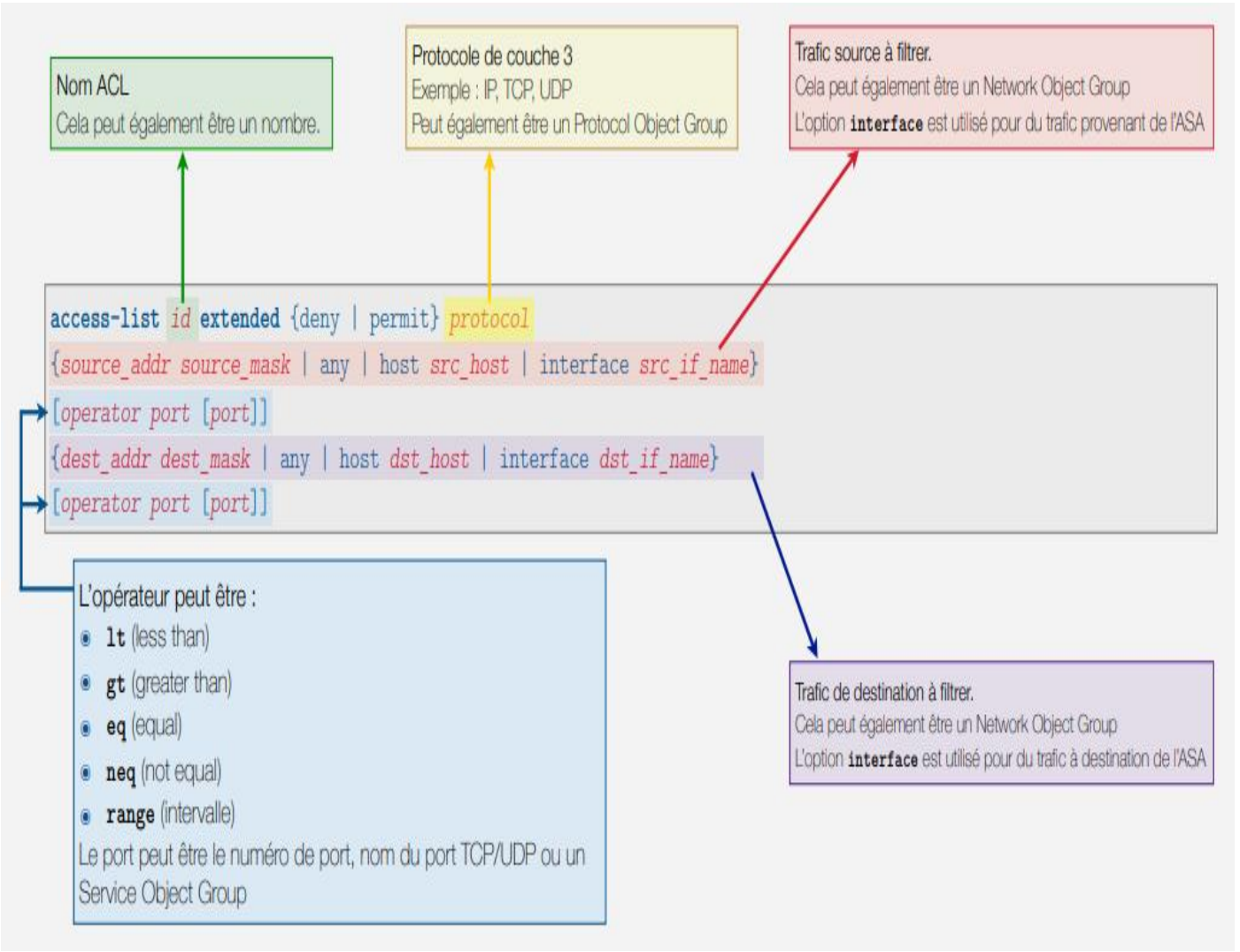


Figure V-2: Syntaxe ACL étendue

Remarque : Le masque est complètement inversé par rapport à la notion de masque que nous connaissons (On parle de masque générique) ex : 193.55.221.0 avec le masque 0.0.0.255 désigne toute adresse source du type 193.55.221.X.

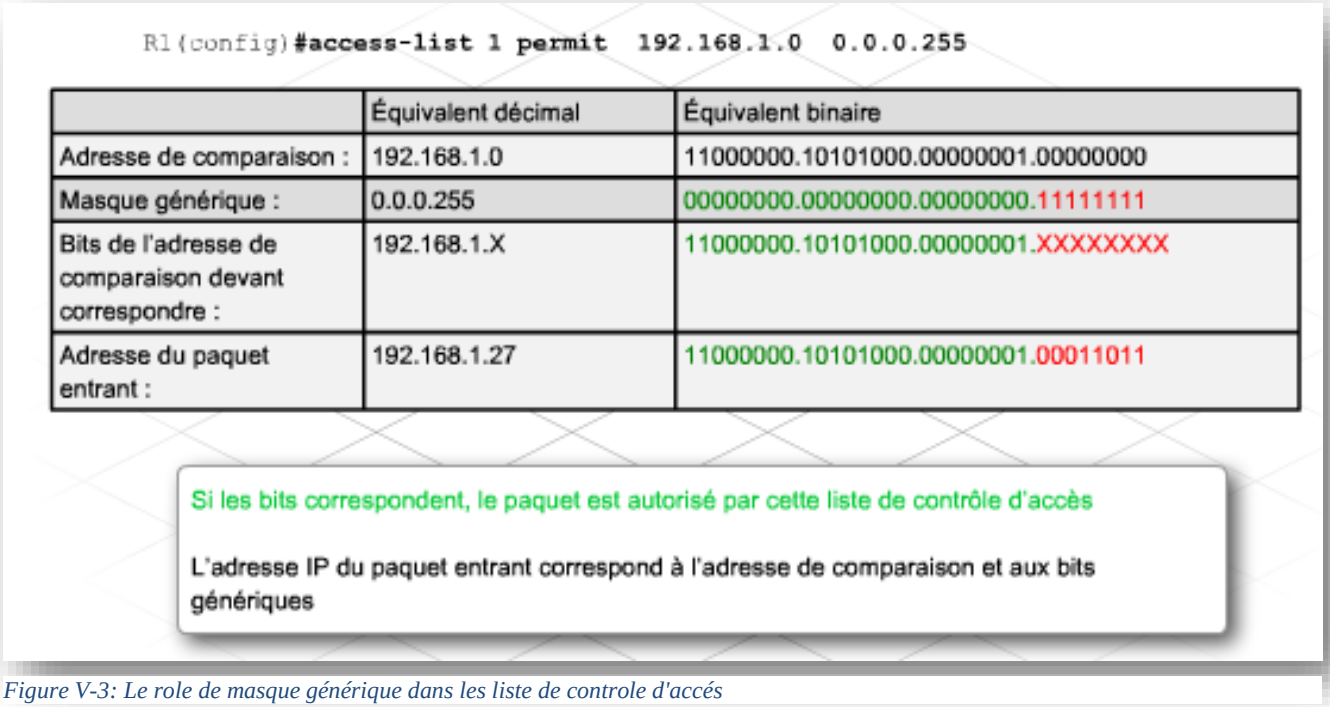


Figure V-3: Le role de masque générique dans les liste de controle d'accés

- Abréviations dans une règle :
  0.0.0.0 255.255.255.255 qui signifient « tout équipement » peut être remplacé par le mot clé « **any** ».
- **W.X.Y.Z 0.0.0.0** qui signifie « l'équipement W.X.Y.Z » peut être remplacé par « **host W.X.Y.Z** »
- Par défaut, la règle **« deny any »** est prise en compte par toutes les ACL. Le fait de créer une ACL vide et de l'appliquer à une interface interdit le passage à tout datagramme. Pour changer de politique par défaut d'une ACL, il suffit de mettre la règle **« permit any »** (ou **« permit ipanyany »** ? pour les ACL étendues) en fin de liste.

Cette règle sera prise en compte si aucune des précédentes ne l'est.

- En mode **« enabled »** la commande **« show access-list<#ACL> »** permet de visualiser (et donc de capturer le cas échéant …) le contenu de l'ACL dont vous donnez le numéro.

On peut citer aussi comme des types ACL :

V.1.5.3 IPv6 :

Utilisé pour supporter l'adressage IPv6

V.1.5.4 Webtype :

Utilisé pour SSL VPN Clientless

V.1.5.5 Ethertype :

- Spécifie le protocole de couche réseau
- Utilisé uniquement lorsque l'ASA est en mode transparent

V.1.6 Activation /Désactivation des ACL :

V.1.6.1 Activation d'une ACL

Pour activer une ACL sur une interface, il faut :

- Se positionner dans le mode de configuration de l'interface, grâce à la commande « interface <nom de l'interface> »
- Saisir la commande : « ipaccess-group <#ACL>< in | out> ».

- N'oubliez pas de vous considérer « à l'intérieur du routeur », pour choisir entre le mot clé « in » et le mot clé « out » …

V.1.6.2 Désactivation d'une ACL :

Pour désactiver une ACL, (comme toujours selon la logique Cisco), les manipulations sont les mêmes que pour l'activer, en utilisant le mot clé « no » devant la commande …, On peut la supprimer juste avec leur ID : No [#ID]

V.1.6.3 Appliquer des ACL standards et étendues dans une réalité :

Dans la pratique, étant donné que les ACL standards ne peuvent prendre en compte que les adresse IP sources, il est logique qu'elles soient souvent utilisées pour filtrer les datagrammes proches de la destination finale, sur un passage « obligé » pour joindre le destinataire final.

En revanche, les ACL étendues prenant aussi en compte les adresses destination, peuvent être utilisées au contraire sur les routeurs les plus proches des équipements sources concernés, ceci afin d'éviter du trafic superflu sur le réseau.

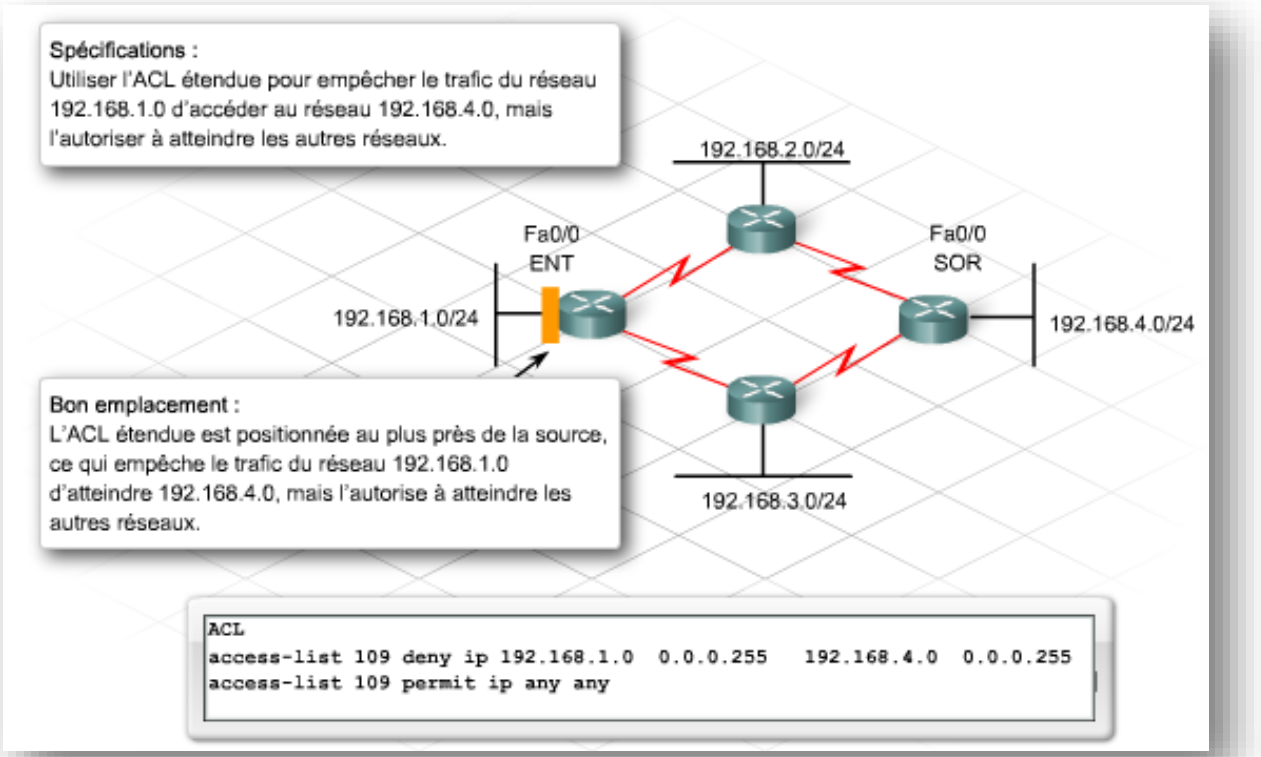


Figure V-4: Exemple d'utilisation de l'ACL étendue

Deux façons de configurer les ACL :

- Nambred (Identifier par Nom de l'ACL)
- Named (Identifier par numéros #ID)

On a déjà vue la syntexe de nombred ACL (Identifier par numéros #ID) sure les types des ACL pour les 2 types (standard et étendues).

La deusieme facons Named ACL permt d'identifier la configuration des ACL avec les noms :

V.1.7 Syntexe de Named ACL :

V.1.7.1 ACL standards :

#IPaccess-list standard <Nom de l'ACL> [Sequance#]

Apré dans le mode de configuration des ACL on va saisie les action a mené :

(config-exl-nacl) #

<Action> <Src><masque>

V.1.7.2 ACL étendue :

#IPaccess-list extended<Nom de l'ACL> [Sequance#]
<Action><Protocol><Src><Port><Dest><Port>

V.1.8 Pour modifier l'ordre de l'ACL :

#ip access-list resquence [#ID**]**

Et pour modifier le port :

#ip access-list resquence [nom ou l'id de l'ACL**]** [le numéro de séquence**] [port]**

V.2 Les DMZ et NAT :

Nous aborderons les deux concepts d'exigences et de mesures de sécurité qui sont étroitement liés à tous les réseaux sécurisés, à savoir la création d'une zone démilitarisée (DMZ) et l'utilisation de la traduction d'adresses (NAT).

La combinaison de ces deux techniques et l'appui des ACL permettent :

- ✓ de masquer le réseau interne à la vue du monde extérieur ;
- ✓ de créer une zone de sécurité intermédiaire entre l'intérieur et l'extérieur ;
- ✓ de publier des informations dans cette zone en la rendant accessible de l'extérieur.

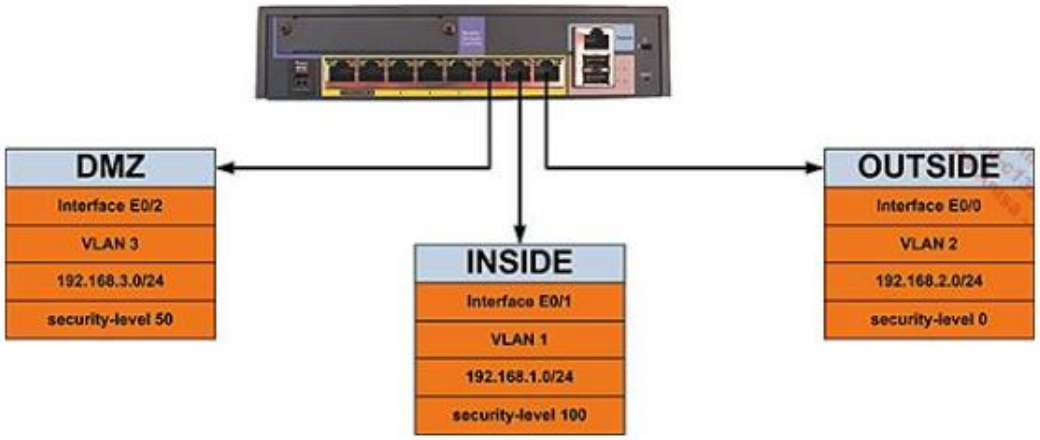


Figure V-5: Représentation d'un firewall ASA 5505 avec la création du trois zones.

Voici une représentation d'un firewall ASA 5505 sur lequel trois zones sont créées. Les interfaces physiques Ethernet 3 à 7 sont par défaut rattachées au VLAN1 et font partie de la zone INSIDE (intérieure).

Comme on vue dans le chapitre 2 sure les mesures de sécurité, Il existe une règle d'or concernant les DMZ, celle qui recommande de ne pas laisser une zone initialiser des communications vers une zone dont le niveau de sécurité est supérieur au sien. C'est le principe du moindre privilège.

La règles que le firewall applique par défaut à nos trois interfaces sont résumées dans le tableau "V.2 1". Cependant, dans certains cas, une communication doit être établie pour fournir des informations à la DMZ. Ces communications doivent aller de la zone INSIDE vers la zone DMZ. Parfois, il est nécessaire d'empêcher le trafic de circuler dans le sens autorisé par défaut. Si vous considérez que la zone DMZ est équipée d'un serveur WEB, vous pouvez demander si la zone est utilisée pour établir la communication avec le monde extérieur. En effet, ce type de serveur envoie des informations vers l'extérieur et ne communique jamais avec l'extérieur seul, ce qui est différent d'un serveur de messagerie. Un autre cas d'utilisation de cette règle empêcherait les zones externes de contacter la DMZ où l'utilitaire est déployé.. Il apparait clairement que l'organisation des flux (vue sous l'aspect sécurité) ne relève pas uniquement de la nature de la zone d'origine malgré le bien fondé du principe du moindre privilège. Afin de déroger à cette règle implémentée par défaut sur les Firewall ASA (avec les niveaux de sécurité), il faut déployer des ACL. Elles seules sont à même d'autoriser de manière granulaire des accès qui sont interdits par défaut.

La création de DMZ sur le firewall ASA s'opère par la configuration du niveau de sécurité des interfaces VLAN. Le schéma représente l'exemple type dans lequel la zone interne (INSIDE) reçoit la valeur de 100, la zone externe (OUTSIDE) la valeur minimale de 0, la DMZ quant à elle reçoit la valeur intermédiaire de 50.

Avec cette configuration, nous obtenons par défaut le tableau suivant qui respecte le principe de moindre privilège.

Tableau 4:Le principe de moindre privilège entre les 3 zone (INSIDE/OUTSIDE/DMZ).

	vers INSIDE	**vers DMZ**	**vers OUTSIDE**
de INSIDE	OK	OK	OK
de DMZ	NON	OK	OK
de OUTSIDE	NON	NON	N/A

Au début d'Internet, les équipements terminaux recevaient tous une adresse publique. Ils étaient de fait directement joignables. Ce n'est plus le cas de nos jours où la plupart des systèmes terminaux utilisent des adresses dites privées masquées (NAT) par une ou plusieurs adresses publiques. Nous allons décrire les deux cas les plus courants, il s'agit de la connexion d'un réseau privé à Internet et de la mise à disposition d'un service public sur une DMZ avec un adressage privé. Ces cas sont des classiques du genre, mais ont pour mérite d'aider grandement à la compréhension de cette technique.

V.2.1 Translation d'adresse (NAT) :

NAT (Network Address Translation) est considéré comme une fonction de sécurité à part entière car ses caractéristiques permettent une isolation entre les réseaux publics et privés. NAT est apparu avec la nécessité d'économiser les adresses IP publiques d'Internet. De plus, il est rapidement devenu inconcevable en matière de sécurité de laisser un ordinateur directement connecté à Internet. Des plages d'adresses IP ont été déclarées non routables (donc inutilisables) sur Internet et mise à disposition des entreprises pour un usage interne. Ces plages d'adresses sont connues sous l'appellation RFC 1918 et sont :

- 10.0.0.1 à 10.255.255.254 ;
- 172.16.0.1 à 172.31.255.254 ;
- 192.168.0.1 à 192.168.255.254.

NAT modifie les champs source ou destination des paquets IP au passage de ces derni ers sur le firewall. Dans les cas qui suivent, nous utiliserons NAT pour modifier l'adresse source des paquets IP sortant du réseau INSIDE vers le réseau OUTSIDE et pour modifier l'adresse destination des paquets IP en provenance du réseau OUTSIDE vers le réseau DMZ.

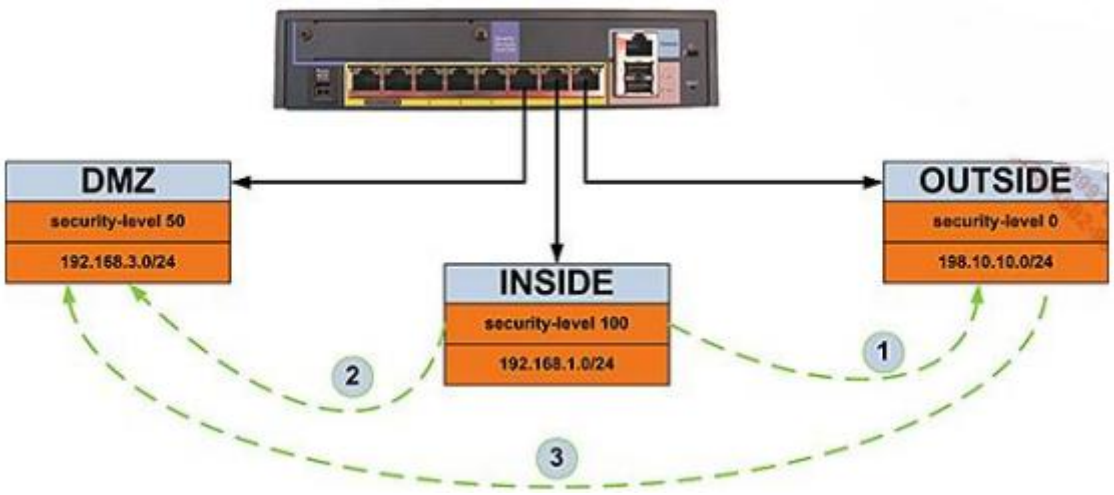


Figure V-6: Les trois cas les plus courants pour l'utilisation de NAT sous ASA.

Nous allons décrire les trois cas les plus courants, il s'agit comme ça se voit dans la figure « FigureV.7»(en 1) de la connexion du réseau INSIDE au réseau OUTSIDE, de la connexion (en 2) du réseau INSIDE vers le réseau DMZ et de la connexion (en 3) du réseau OUTSIDE vers la DMZ. Ces trois configurations utilisent la traduction d'adresse et les ACL.

Nous montrerons également comment ne pas utiliser NAT entre le réseau INSIDE et le réseau DMZ.

Cas N° 1 :

Le réseau INSIDE se connecte au réseau OUTSIDE. Ce cas montre une station de travail d'un réseau interne qui se connecte sur Internet. Comme elle ne dispose pas d'une adresse pu blique (routable sur Internet) il est absolument nécessaire de changer l'adresse IP source des paquets IP. Si tel n'était pas le cas, les paquets retour ne pourraient trouver leur destination.

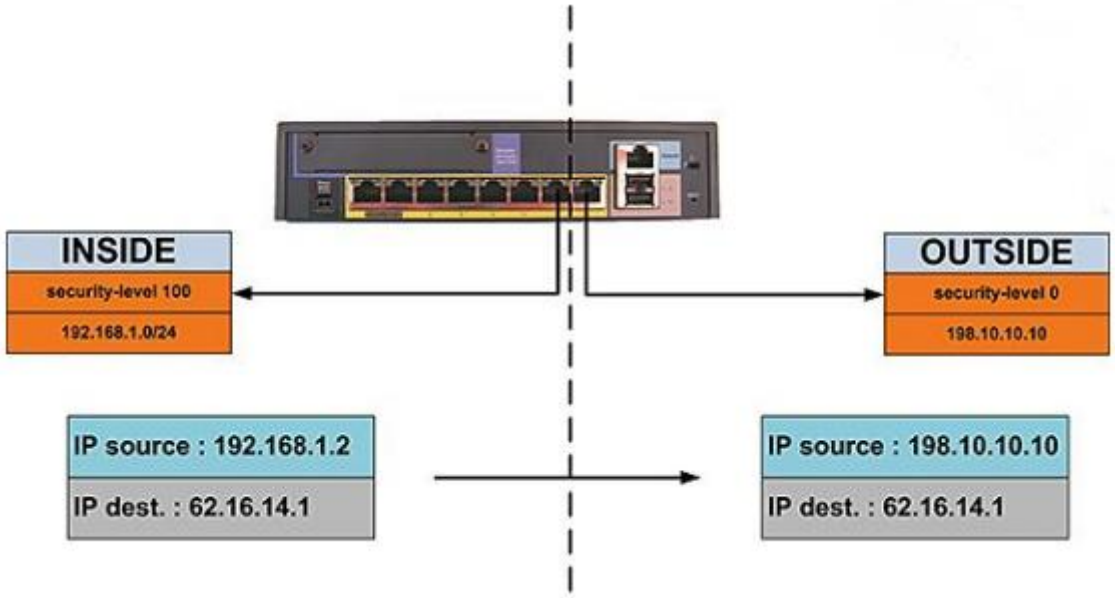


Figure V-7: Cas n°1 NAT pour la connexion du réseau INSIDE au réseau OUTSIDE

Lors de son passage à travers le firewall le paquet IP change d'adresse source. Son adresse de type RFC 1918 est transformée en adresse IP publique, en l'occurrence celle de l'interface *outside.* Aucune ACL n'est ici nécessaire car le réseau INSIDE bénéfice du niveau de sécurité maximal. Cet exemple montre le réseau INSIDE en correspondance avec l'adresse de l'interface OUTSIDE du firewall.

```
ASA-5505(config)# nat (inside) 1 192.168.1.0 255.255.255.0

ASA-5505(config)# global (outside) 1 interface
```

La syntaxe des commandes NAT n'est pas facile à retenir et mérite des explications appr ofondies.

Ici, nous déclarons un processus NAT qui porte le numéro 1. Il est indiqué que le réseau 192.168.1.0 résidant sur l'interface *inside* (commande *nameif* de l'interface VLAN1) est candidat pour la transformation des adresses sources (nat) au passage du firewall vers le réseau *outside* qui se situe en zone publique (*global*). Les deux lignes sont liées par le numéro 1. Lors du passage d'un paquet, la table de correspondance de NAT est renseignée afin de permettre la distribution correcte du paquet retour.

```
ASA-5505(config)# nat (inside) 1 192.168.1.0 255.255.255.0

ASA-5505(config)# global (outside) 1 198.10.10.10-198.10.10.240
```

Il est également possible de faire correspondre le réseau INSIDE à un groupe d'adresses publiques routées sur l'interface OUTSIDE. Dans cet extrait de configuration, aux adresses du réseau INSIDE correspondent une plage d'adresses publiques c'est-à-dire toutes les adresses entre 198.10.10.10 et 198.10.10.240

Cas N° 2 :

Faut-il activer les fonctions NAT pour tous les types de trafic ? Cela ne paraît pas indispensable entre deux réseaux qui possèdent des adresses IP privées. Le cas se présente dans notre architecture pour les communications entre le réseau INSIDE et le réseau DMZ. Le cas N°1 transforme toutes les adresses du réseau INSIDE. Si la fonction NAT n'est pas nécessaire entre le réseau INSIDE et le réseau DMZ, il faut indiquer au processus NAT qu'il ne doit pas traiter certains paquets.

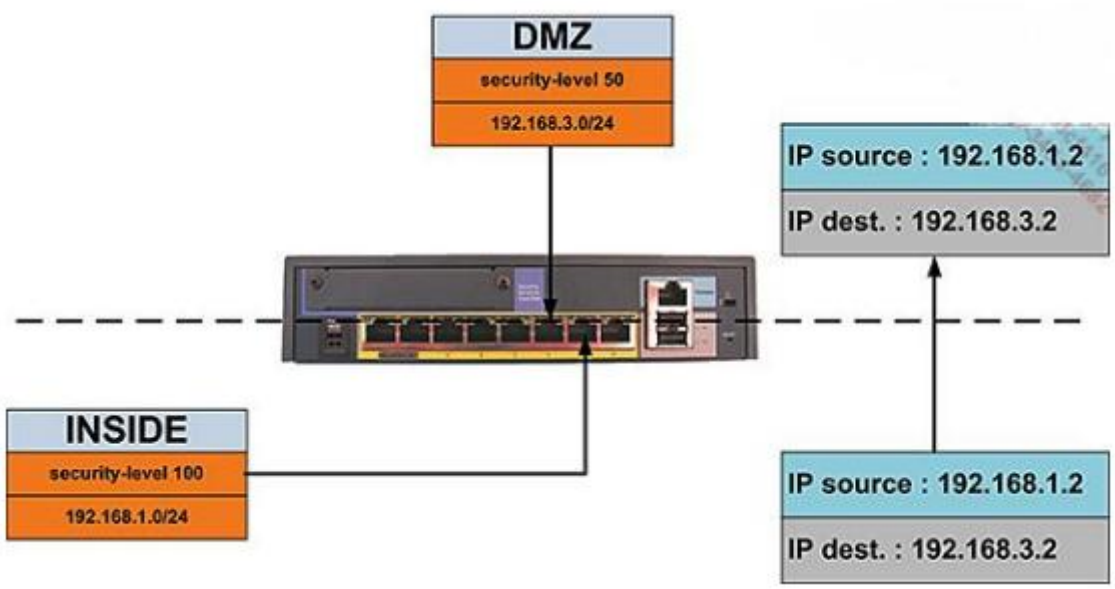


Figure V-8: Cas n°2 NAT pour la connexion du réseau INSIDE vers le réseau DMZ.

Nous observons ici que les paquets entre le réseau INSIDE et le réseau DMZ conservent leur adresse source.

```
ASA-5505(config)# access-list PasDeNat permit ip 192.168.1.0

255.255.255.0 192.168.3.0 255.255.255.0

ASA-5505(config)# nat (inside) 0 access-list PasDeNat
```

Une ACL (nommée PasDeNat) désigne le trafic entre le réseau INSIDE et le réseau DMZ. Puis, cette ACL est appliquée à une commande NAT s'appliquant sur l'interface inside suivie du chiffre 0 indiquant qu'il ne faut pas transformer les adresses sources correspondant à l'ACL PasDeNat.

Cas N° 3 :

Les services offerts au public sont généralement installés sur des zones démilitarisées afin de bénéficier de la protection offerte dans ces espaces. La traduction d'adresse est l'une de ces protections. Il faut que le serveur dans le réseau DMZ soit accessible de l'extérieur par son adresse publique. Puis NAT modifie l'adresse de destination publique vers l'adresse privée du serveur telle que configurée sur sa carte réseau. En outre, cette communication s'établit entre l'interface outside (security-level 0) et l'interface dmz (security-level 50) ce qui nécessite l'ajout d'une ACL pour déroger au principe du moindre privilège

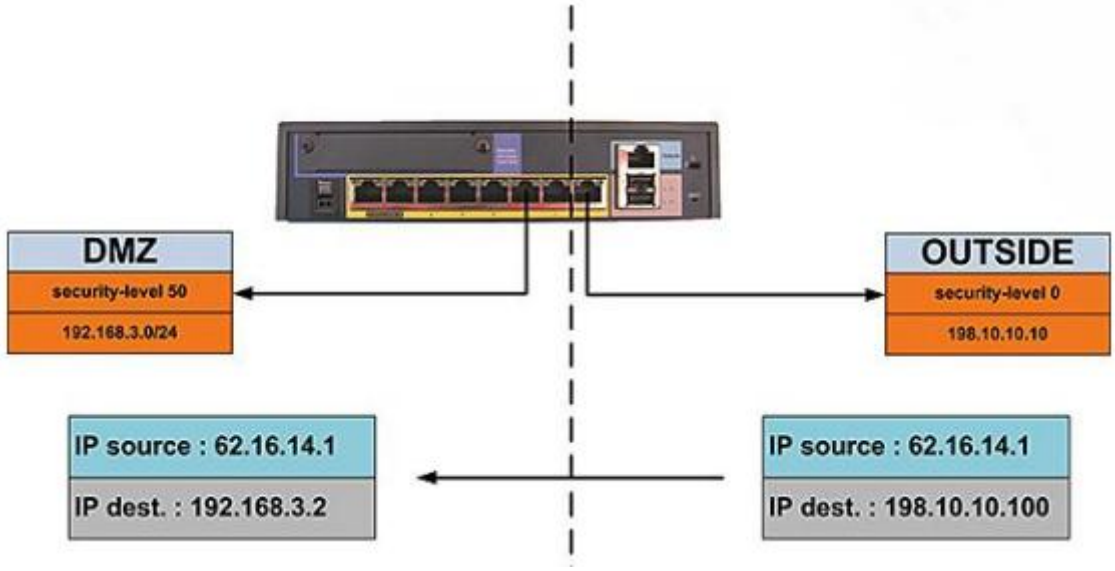


Figure V-9: Cas n°3 NAT pour la connexion du réseau OUTSIDE vers la DMZ

Nous constatons le changement du champ IP destination dans le paquet lors du passage au travers du firewall. Cette configuration nécessite un routage de l'adresse 198.10.10.100 sur l'adresse de l'interface *outside*.

```
static (inside,outside) 198.10.10.100 192.168.3.2 netmask 255.255.255.255

access-list VersDMZ extended permit tcp host 198.10.10.100 eq www

host 192.168.3.2 eq www

access-group VersDMZ in interface outside
```

Ces deux commandes décrivent :

- L'association entre l'adresse publique du serveur (198.10.10.100) et son adresse privée (192.168.3.2) ;
- L'indispensable ACL pour passer d'un niveau de sécurité à l'autre. Examinons-les dans le détail.

La première commande n'est pas aisée à mémoriser de prime abord. Elle indique au routeur qu'une adresse IP du côté de l'interface inside est statiquement traduite sur l'interface outside par NAT. Nous trouvons ensuite l'adresse IP publique du serveur suivie de son adresse privée. Cette syntaxe est quelque peu déroutante du fait de l'inversion des adresses par rapport à l'ordre des mots inside et outside.

La seconde commande est une ACL étendue classique qui autorise l'adresse publique du serveur à se connecter à son adresse privée, les ports sont précisés et correspondent au protocole HTTP (port 80).

Des contrôles supplémentaires existent pour les règles de traduction et concernent la couche session. Il est possible de configurer un nombre maximum de connexions TCP et UDP. La quantité de connexions à moitié ouvertes est également configurable.

V.3 PAT (Port Address Translation) ou Overloading

Le port adresse Translation vient complémenter le NAT. En effet, supposant que nous ne disposons pas d'adresse IP publique suffisantes pour toutes nos machines locales, il va donc falloir partager réutiliser nos adresses.

PAT permet à plusieurs hôtes internes de partage adresse unique sur une interface externe en ajoutant des numéros de port différent à chaque connexion c'est-à-dire que Pour distingue les requêtes des différentes machines, on va utiliser le numéro du port.

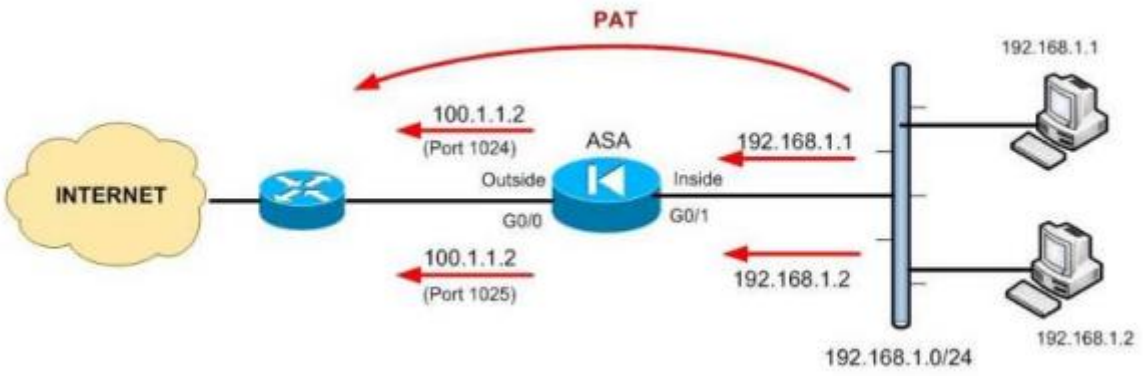


Figure V-10 : V.3 PAT "Port Address Translation".

V.4 Détection et protection contre les menaces :

Les attaques sur les protocoles réseau ne manquent pas. Ils vont de la simple identification de port à la fermeture du réseau en envoyant un grand nombre de paquets délibérément erronés. Si de telles attaques correspondent à un trafic autorisé, elles peuvent facilement traverser le pare-feu. Il peut sembler peu pratique d'enregistrer ce type de trafic légitime, mais l'augmentation soudaine du trafic d'un type est le message principal, hélas, submergé dans un flot incessant de dispositifs de sécurité. Ce principe est très séduisant, mais pour un firewall, quelle que soit la quantité de mémoire dont il dispose, c'est une charge de travail considérable. Il est préférable de déléguer la tâche de surveillance de la charge des liens réseau et même de la conformité du trafic applicatif à d'autres outils.. Parmi ces outils nous trouvons les dispositifs de corrélation de journaux qui présentent un avantage incontestable en comptabilisant les occurrences d'un même évènement au lieu de créer une ligne pour chacun d'entre eux. Après la détection d'une activité paraissant suspecte, il convient de prendre une décision quant au traitement du trafic incriminé. Il est envisageable de l'éliminer totalement ou de restreindre son taux de pénétration dans le réseau par le biais des outils de qualité de service.

Nous avons examiné sur les routeurs des ACL qui permettent de rejeter sur les interfaces externes, du trafic semblant provenir des réseaux internes. De même, nous avons souligné l'intérêt représenté par un filtrage à la source au plus près des connexions des utilisateurs. Nous allons à présent examiner les solutions proposées sur le firewall ASA.

Le taux de messages de sécurité concernant le nombre de paquets rejetés par des ACL est tout particulièrement intéressant car il indique une anomalie due ou non à une attaque sur le réseau.

```
ASA-5505(config)# threat-detection basic-threat
```

Cette première commande active la détection des menaces sur une liste prédéterminée d'irrégularité comme les rejets sur les ACL, un nombre trop important de paquets SYN en attente de synchronisation ou une reconnaissance par scan de ports. Un message est enregistré sur le journal du firewall. Les taux de détection sont très facilement paramétrables et portent sur la durée pendant laquelle seront calculées les moyennes, le taux moyen de paquets rejetés par seconde et un taux de pic sur un intervalle plus court. Ces commandes ne présentent aucune difficulté particulière mais nécessitent un paramétrage réaliste en fonction des seuils souhaités.

```
hostname(config)# threat-detection rate {acl-drop | bad-packet-drop
| conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop
|interface-drop | scanning-threat |
syn-attack} rate-interval rate_interval average-rate av_rate burstrate
burst_rate
threat-detection rate syn-attack rate-interval 1200 average-rate
100
```

Le détail de la commande est donné pour information. Nous trouvons au-dessous, une commande visant à remonter une alerte en cas de dépassement d'un certain réglage dans le cas d'une attaque par inondation de paquets SYN.

Après chaque mot clé et avant chaque valeur en secondes, l'utilisation du point d'interrogation fournit (en anglais) des explications très détaillées sur l'utilisation de chaque mot clé. Cette aide en ligne est d'une très grande qualité.

La commande en exemple se traduit de la manière suivante : le taux de détection des menaces pour une attaque SYN (présumée) est calculé sur un intervalle de 1200 secondes et déclenche une alarme pour un taux de 100 paquets par seconde.

```
ASA-5505(config)# threat-detection scanning-threat shun duration 60
```

Cette autre commande concerne plus particulièrement les reconnaissances par scan de port. Il est ici question non seulement de remonter un message en cas de reconnaissance mais aussi de déconnecter le gêneur pour une durée d'une minute grâce à l'option shun qui est optionnelle. Pour mémoire une reconnaissance est un nombre considérable de tentatives de connexions sur tous les ports connus afin de déterminer quels sont ceux sur lesquels le système d'exploitation visé est en écoute.

Cisco sous l'appellation de « normalisation du protocole TCP » offre une myriade d'options très intéressantes pour tenter de paramétrer finement la détection des attaques dont TCP est la victime. Ici aussi le point d'interrogation apporte beaucoup d'informations. Citons toutefois quelques options portant sur la détection des drapeaux ACK ou URGENT mal positionnés ainsi que la possibilité d'accepter une variation de la taille des fenêtres.
Le mécanisme d'application de la normalisation du protocole TCP à une interface suit le schéma utilisé pour ajuster la qualité de service. La syntaxe utilisée par Cisco est « à tiroir » et mérite que l'on s'y arrête quelques instants.

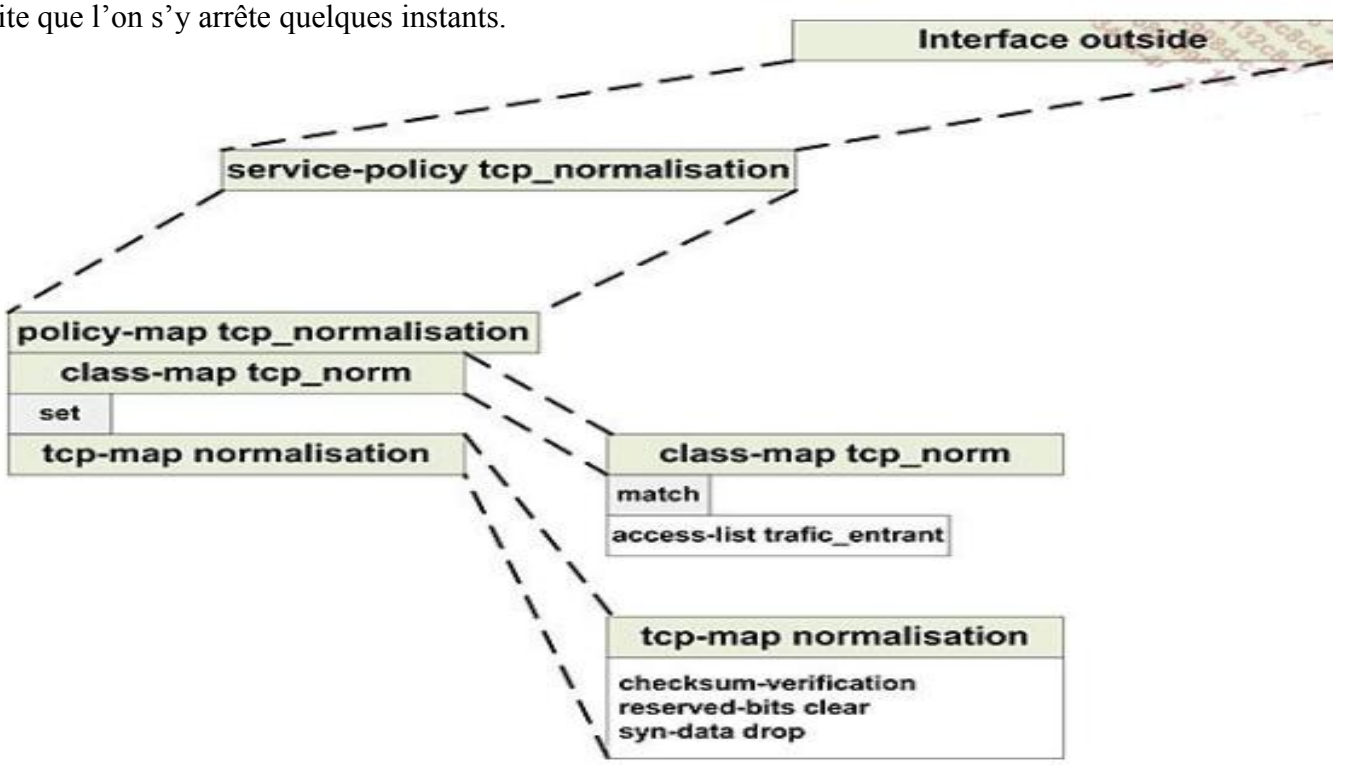


Figure V-11:Schéma explicatif de principe de fonctionnement

Tout d'abord, nous définissons les paramètres de normalisation (en bas à droite), puis une *class-map* est créée dans laquelle le trafic défini par une ACL est sélectionné pour la normalisation. Tout ceci est intégré dans une *policy-map* (qui peut contenir plusieurs entrées *class-map* et *set*). Pour terminer, une *service-policy* englobe la *policy-map* avant de se voir affectée à l'interface *outside*.

```
ASA-5505(config)# access-list trafic_entrant extended permit tcp
any host 198.10.10.100 eq www
ASA-5505(config)#tcp-map normalisation
ASA-5505(config-tcp-map)# checksum-verification
ASA-5505(config-tcp-map)# reserved-bits clear
ASA-5505(config-tcp-map)#syn-data drop
ASA-5505(config-tcp-map)# exit
ASA-5505(config)# class-map tcp_norm
ASA-5505(config-cmap)# match access-list trafic_entrant
ASA-5505(config-cmap)# exit
ASA-5505(config)# policy-map tcp_normalisation
ASA-5505(config-pmap)# class tcp_norm
ASA-5505(config-pmap-c)# set connection advanced-options
normalisation
ASA-5505(config-pmap-c)# exit
ASA-5505(config-pmap)# exit
ASA-5505(config)# service-policytcp_normalisation interface
outside
ASA-5505(config)#
```

Cette capture comporte la totalité des commandes qui correspondent au schéma d'organisation de cette configuration en cascade. Nous touchons ici aux séquences de commandes parmi les plus complexes introduites par Cisco.

V.5 La téléphonie sur IP :

Le firewall ASA offre des mesures de sécurité pour la téléphonie sur IP parmi lesquelles nous retiendrons la possibilité de déchiffrer à la volée la signalisation afin de l'inspecter (TLS-proxy), l'inspection protocolaire proprement dite et la fonction phone proxy.

a. TLSproxy :

TLS-proxy place le pare-feu en coupure entre un téléphone et le CUCM afin de « défaire et refaire » la session TLS qui protège la signalisation. Une fois en clair, la signalisation est inspectée puis chiffrée à nouveau avant d'être redirigée vers le CUCM. Cette architecture nécessite la mise en place d'un certificat sur le pare-feu à la manière de celui présent sur le CUCM et la mise à jour de la liste de confiance présente sur le téléphone. TLS-proxy nécessite
l'installation de certificats sur le pare-feu afin de représenter le CUCM pour les téléphones et une mise à jour de leur liste de sécurité interne.

b. Inspection protocolaire :

Il est ici question de vérifier la conformité du protocole de signalisation par rapport à des règles définies dans la configuration du pare-feu. Ces règles seront confrontées à la signalisation. L'inspection du protocole vérifie également les propriétés TCP de la connexion et offre l'opportunité de rendre aléatoire les numéros de séquences.
Enfin, une règle de qualité de service peut aussi être appliquée au trafic (en l'occurrence la signalisation).

```
class-map VoIP
match any
!
policy-map type inspect skinny Inspection-SCCP
parameters
enforce-registration
message-id max 0x141
sccp-prefix-len max 65536
timeout media 0:01:00
timeout signaling 0:05:00
rtp-conformance enforce-payloadtype
policy-map global-policy
descriptionTelephonie
class VoIP
inspect skinny Inspection-SCCP
set connection conn-max 100 embryonic-conn-max 20 per-client-max
3
set connection timeout tcp 1:00:00 reset dcd 0:15:00 5
set connection decrement-ttl
!
service-policy global-policy global
```

Cet extrait montre la configuration de la protection du protocole SCCP. Le schéma consiste à déclarer un *policy-map* de type *inspect* puis à l'insérer dans une *policy-map* nommée *global-policy*. Cette dernière est appelée dans une commande *service-policy* appliquée globalement (*global*). La *class-map* nommée *VoIP* désigne tout trafic sans distinction. Elle est appelée dans la *policy-map* nommée *global-policy*.

Les paramètres concernant SCCP sont sous le mot *parameters*. Ceux concernant TCP sont dans la class nommée VoIP. Cette inspection est bien entendu applicable sur du trafic en clair mais aussi sur du trafic chiffré à condition d'avoir activé la fonction TLS-proxy.

c. Phone proxy :

Cette technique est particulièrement utile pour sécuriser les réseaux au sein desquels sont présents des téléphones IP logiciel (SoftPhone). Les réseaux de téléphonie et ceux de données emploient en règle générale deux VLAN distincts. Si un téléphone logiciel est installé sur une station de travail (membre du VLAN « données ») il est alors

nécessaire de faire transiter la téléphonie d'un VLAN vers l'autre ce qui soulève quelques problèmes dus à la nature des ports UDP et à leur désignation dynamique par le CUCM. Cette configuration nécessite tout comme pour le TLS-proxy l'installation de certificats sur le pare-feu afin de représenter le CUCM pour les téléphones et une mise à jour de leur liste de sécurité interne.

Le CUCM est capable d'intercepter les messages en provenance d'un téléphone logiciel du VLAN de données et de le forcer à s'authentifier. À l'issue de cette séquence la signalisation indique au pare-feu les ports par lesquels le trafic téléphonique sera autorisé à passer. Cette technique évite donc l'ouverture statique d'une trop grande plage de ports UDP.

V.6 5. VPN SSL :

Les applications de type client-serveur nécessitent en temps normal l'installation d'un logiciel spécifique sur la machine cliente et cela ne va pas sans poser de nombreux problèmes de déploiement et de mise à jour des versions en production. De plus, les accès distants au réseau de l'entreprise sur lesquels résident des clients spécifiques nécessitent un supplément de configuration avec l'installation des logiciels dédiés à la communication. L'avènement des applications développées pour Internet a considérablement modifié la donne en simplifiant les accès aux réseaux distants. En effet, à partir d'un simple navigateur Web il est possible d'accéder en toute sécurité à un portail sur lequel des liens redirigent l'utilisateur vers ses applications. Pour certaines d'entre elles ce mode de fonctionnement n'est pas envisageable en raison du coût de migration ou des habitudes prises par les utilisateurs. La messagerie est un exemple typique pour lequel les utilisateurs ont quelques difficultés à troquer leur traditionnel client contre une messagerie en ligne offrant pourtant les mêmes facilités. Afin de palier à cet inconvénient, il est possible de télécharger à la demande des fonctionnalités additionnelles pour canaliser ces types de trafic dans la communication protégée par SSL.

Les pare-feu Cisco ASA offrent trois techniques que nous allons examiner sous le prisme de la sécurité réseau. Ces modes de fonctionnement sont : la connexion VPN SSL sans client, celle avec un ou plusieurs connecteurs spécifiques (plug-in) et celle avec un client lourd.

Le déploiement de cette technologie nécessite une bonne organisation afin de planifier avec soin les groupes d'utilisateurs et les droits d'accès aux ressources. Ici, la notion de groupe s'étend en fonction des projets bien au-delà des utilisateurs de l'entreprise. Ceci est dû au fait que la technologie VPN SSL repousse les limites des connexions traditionnelles et offre ainsi la possibilité à une entreprise d'ouvrir ses ressources à ses partenaires sans qu'il soit nécessaire de maîtriser leur infrastructure. Un tel projet s'accompagne aussi d'une étude sur les procédures de création et de changement concernant les ressources, les groupes d'utilisateurs et les relations qui les unissent. Ces études sont, soulignons-le, étroitement liées à l'organisation des annuaires d'entreprise et plus globalement à la gestion des identités.

Cette étude comporte bien entendu (et comme toujours) une définition préalable des exigences de sécurité.

Exigences de sécurité des VPN SSL	
Authentifier les utilisateurs Leur attribuer des droits d'accès	AAA (association groupes ressources) Gestion des mots de passe.
Valider un niveau de sécurité sur les stations distantes	Vérification de l'antivirus, niveau minimal de chiffrement, expiration des sessions, authentification mutuelle (certificats)
Renforcer la sécurité en cas d'accès à partir de machines publiques	Secure desktop, effacement du cache, clavier virtuel, détection des enregistreurs de clavier

Ces exigences couvrent les deux domaines que sont l'équipement VPN SSL central et la station distante.

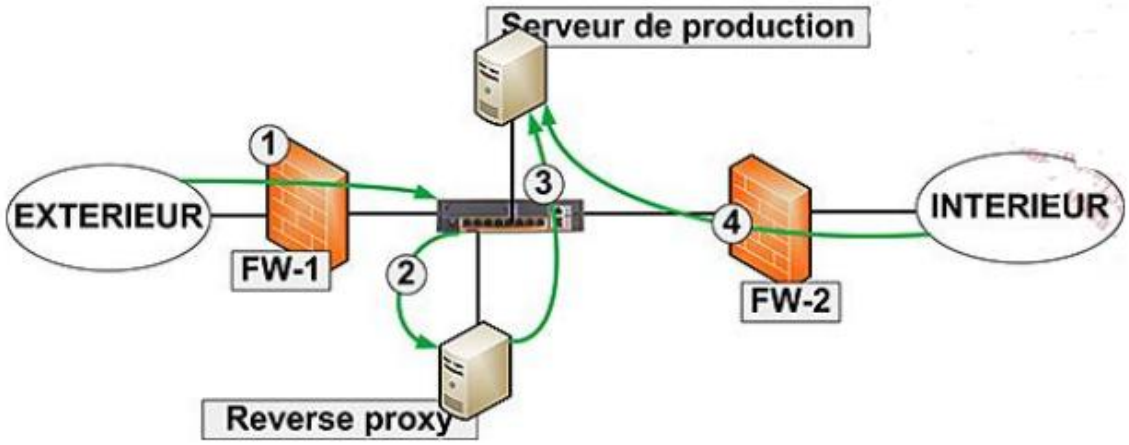


Figure V-12: Architecture VPN SSL.

Voici une représentation très schématique d'une architecture VPN SSL sur laquelle nous observons les éléments constitutifs et les flux associés en partant du principe que l'équipement VPN SSL est en mode routé et délègue quelques fonctions de sécurité. Si tel n'est pas le cas, il s'avère indispensable d'intercaler un routeur ou un commutateur Ethernet munis de fonctions de routage. Décrivons cette architecture:

- ☞ Les stations de travail passent au travers d'un premier firewall qui a pour vocation de filtrer le protocole entrant en veillant à la bonne conformité de la couche TCP/IP et en assurant une barrière contre les attaques par saturation.
- ☞ L'équipement terminal VPN SSL termine la session chiffrée avec l'utilisateur distant et examine ses droits généralement en fonction de son groupe d'appartenance. Les annuaires de l'entreprise sont mis à contribution. Ils ne sont pas ici représentés, mais sont positionnés dans une zone de sécurité, car rappelons le, aucun trafic externe ne doit

directement accéder au réseau Interne. Ces annuaires DMZ peuvent être des images des annuaires internes disposant d'un système de réplication de l'intérieur vers la DMZ.

- ☞ Le trafic est routé vers un équipement de type reverse proxy afin de passer de nouveaux services de sécurité comme l'analyse des caractères dangereux avant d'être (généralement en fonction de l'URI) vers le serveur de production. Il est recommandé de chiffrer cette communication pour assurer un maximum de confidentialité au sein même des DMZ.
- ☞ Ce dernier est alimenté en donnée par l'intérieur du réseau en application du principe de moindre privilège

Des mécanismes additionnels qui sortent du cadre de ce projet de fin d'étude offrent la possibilité de gérer les droits d'accès en fonction de l'application demandée lors des requêtes HTTP ainsi que l'authentification unique plus connue sous l'appellation de SSO (Single Sign On). Toutefois certaines approches du SSO sont prises en compte par le firewall ASA.

V.6.1 VPN SSL sans client:

Il s'agit du mode privilégié qui utilise les fonctions de chiffrement du navigateur Internet pour assurer la sécurité. Les clients se connectent à un portail personnalisé sur le firewall et en fonction de leur identité ont accès aux ressources pour lesquelles ils ont des droits. Il est également possible de parcourir des répertoires et des fichiers à la manière de l'explorateur d'une station de travail. Un avantage incontestable est l'accès aux données à partir de n'importe quel poste de travail reliée à Internet.

Nous allons décrire les configurations qui conduisent à la construction d'un exemple simple mettant en avant les fonctions de sécurité. Nous n'aborderons pas les multiples capacités de ce produit en matière de personnalisation des portails.

```
ASA-5505(config)#webvpn
ASA-5505(config-webvpn)# enable outside||||
```

Ces deux commandes activent le VPN SSL sur l'interface extérieure du firewall. Les paramètres de sécurité sont affectés à l'utilisateur une fois franchie la page d'authentification. Ils proviennent d'une combinaison des propriétés de l'utilisateur et du groupe auquel il appartient. C'est ce groupe d'appartenance qui fixe les règles de sécurité auxquelles est soumis l'utilisateur pendant sa session.

```
group-policy "BEA 1" internal
group-policy "BEA 1" attributes
banner value Bonjour bonjour
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-session-timeout 240
vpn-tunnel-protocol webvpn
group-lock none
vlan none
webvpn
url-list value template_entreprise_1
filter none
port-forward disable
customization value Entreprise_1
hidden-shares none
smart-tunnel disable
file-entry enable
file-browsing enable
url-entry enable
smart-tunnel auto-signon disable
username Riahla password NUNxeiV/zZIW3X5z encrypted
username Riahla attributes
vpn-group-policy "BEA 1"
vpn-access-hours none
vpn-simultaneous-logins 1
vpn-idle-timeout 30
vpn-session-timeout 240
vpn-filter none
vpn-tunnel-protocol webvpn
password-storage disable
group-lock BEA_1
service-type remote-access
webvpn
```

```
file-browsing enable
file-entry enable
url-entry enable
port-forward disable
homepage none
hidden-shares none
url-list none
customization value BEA_1
svc keep-installer installed
svc keepalive none
svc compression deflate
svcdtls enable
svcmtu 1406
svc profiles none
smart-tunnel disable
smart-tunnel auto-signon disable
tunnel-group BEA_1 type remote-access
tunnel-group BEA_1 general-attributes
default-group-policy "BEA 1"
password-management password-expire-in-days 3
tunnel-group BEA_1 webvpn-attributes
customization BEA_1
group-alias ent1 enable
```

Voici un large extrait de la configuration d'un ASA qui montre le paramétrage d'un VPN SSL.

Cette configuration minimaliste est donnée à titre informatif et ne propose aucune fonctionnalité web, elle a pour vocation d'illustrer la manière dont l'utilisateur hérite des paramètres du VPN SSL sur lequel il se connecte. Ces paramètres viennent s'ajouter aux siens et à ceux de son groupe d'appartenance.

Les attributs de l'utilisateur Paul sont clairement visibles et notamment la politique de groupe à laquelle il est rattaché. Les paramètres de personnalisation du portail ne sont pas visibles sur la configuration car ils sont stockés dans un fichier XML lui-même sauvegardé en mémoire flash. Par commodité, cette configuration ne fait pas appel à un annuaire centralisé mais utilise la base locale AAA. Le contrôle effectué sur l'expiration du mot de passe est basé sur la lecture des propriétés venant de l'annuaire. Le firewall permet à l'utilisateur de changer

lui-même son mot de passe.

Le détail de cette configuration est le suivant :

- Une politique de groupe est créée et nommée *BEA 1*. Elle reçoit quelques propriétés. Elles figurent sur les lignes qui sont décalées d'un caractère sur la droite.
- La commande vpn-tunnel-protocol *webvpn* appelle la commande *webvpn* située trois lignes plus bas laquelle reçoit également des propriétés (de nouveau décalées d'un caractère à droite).
- La commande *webvpn* est assortie de propriétés de personnalisation du portail comme la liste d'URL (*template_BEA_1*).
- L'utilisateur Riahla est défini et une série de caractéristiques lui sont appliquées dont son rattachement à la politique de groupe *BEA 1*.

- Le portail est finalement créé avec la commande *tunnel-group BEA_1* et reçoit la politique *BEA_1*.

Les exigences de sécurité indiquent que la sélection des paramètres de cryptographie participe à l'évaluation du niveau de sécurité de la station distante. Les navigateurs Internet et les serveurs négocient la suite de chiffrement et en fonction de leurs possibilités s'accordent sur une suite faible.

```
ASA5505(config)# ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ASA5505(config)# ssl server-version tlsv1-only
```

Ces deux lignes montrent la configuration SSL du côté du firewall ASA. La négociation est acceptée pour ces trois suites et le protocole général choisi est TLS V1 ce qui signifie qu'une station distante sera rejetée si elle se présente avec une suite différente des trois proposées. L'objectif ici est de forcer la négociation sur les suites les plus fortes.

Figure V-13 : Le menu de configuration du clavier virtuel

Figure V-14: Le résultat obtenu lors d'une tentative d'ouverture de session par l'utilisateur Riahla..

Ces deux captures montrent le menu de configuration du clavier virtuel et le résultat obtenu lors d'une tentative d'ouverture de session. Ce dispositif protège contre les enregistreurs de clavier dont le but est de capturer les mots de passe entrés par l'utilisateur Riahla.

V.6.1.1 Secure desktop :

Cisco Secure Desktop (CSD) est un environnement de travail sécurisé qui est téléchargé puis installé par un client distant. Cette technologie est souvent comparée à un bac à sable logiciel du quel on ne peut sortir. CSD est une machine virtuelle chiffrée qui une fois créée sur la station distante s'intercale entre l'utilisateur et le système d'exploitation. L'utilisateur dès lors, interagit avec ses applications à l'intérieur de cet espace virtuel local. Une fois la session terminée, l'environnement est détruit.

La mise en œuvre de CSD s'effectue en trois phases :

- Son téléchargement sur le site de Cisco, sa copie sur le système de fichier du firewall et son activation ;
- La création d'une politique de vérification entre le moment où l'utilisateur entame la connexion et le moment où il entre ses identifiants. Le principe est de procéder à des contrôles préalables définissant un niveau de sécurité dont dépendra le type de services disponibles ou la non connexion (si le niveau minimal n'est pas atteint) ;
- La connexion proprement dite dans le client sécurisé.

```
ASA5505(config)# webvpn
ASA5505(config-webvpn)# csd image disk0:/cte/securedesktop-asa3.3.0.129-k9.pkg
```

```
ASA5505(config-webvpn)# csd enable
```

Ces trois commandes activent CSD à partir d'une image logicielle préalablement téléchargée sur le site Internet de Cisco. Cette image est copiée dans un système de fichiers nommé disk 0 : La commande *csd enable* active globalement la fonction.

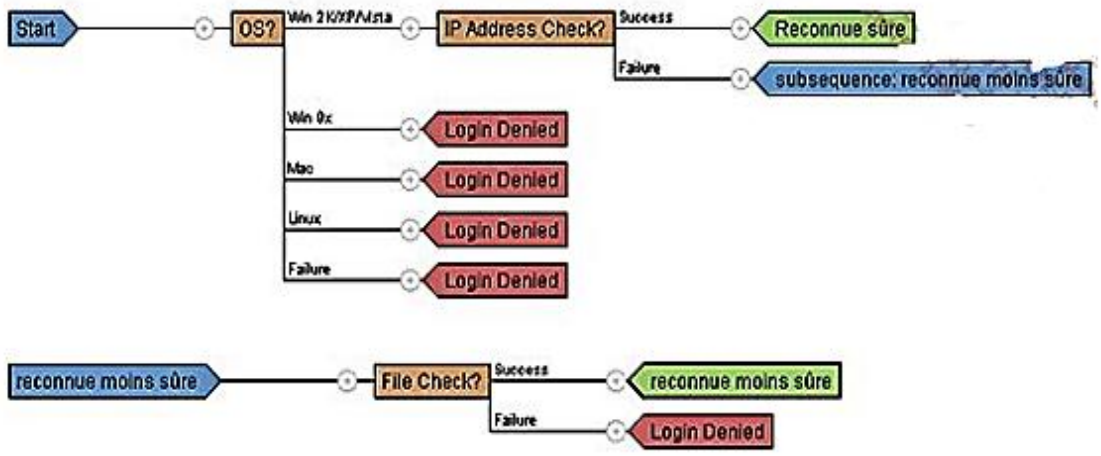


Figure V-15 : Extrait d'une logique graphique de la configuration de CSD.

Ici, une fois n'est pas coutume nous présentons un extrait graphique de la configuration de la phase numéro deux. Il est ici possible graphiquement de concevoir une logique afin de classer le niveau de sécurité de la station distante en fonction de certaines de ses caractéristiques. En fonction du niveau de sécurité, CSD autorisera certaines fonctionnalités. Dans cet exemple, CSD examine le système d'exploitation de la station distante et exige la présence d'un certain type (2K/XP/Vista) avant de poursuivre par un examen de l'adresse ou du réseau IP. Si ce réseau est conforme à celui configuré dans la règle la station est reconnue sûre. La chaîne de caractère « reconnue sûre » devient de fait le nom d'une politique CSD.

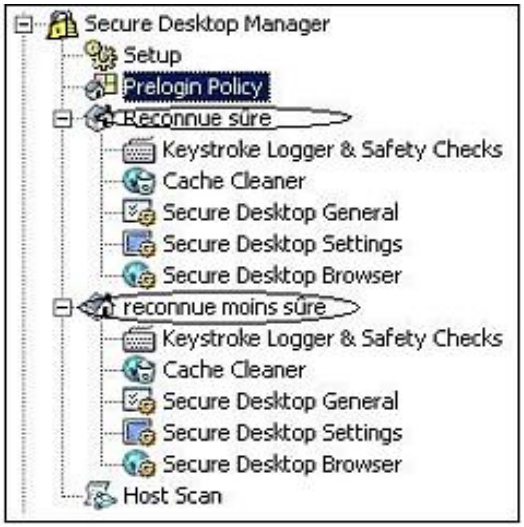


Figure V-16: Secure Desktop Manager.

La logique poursuit son cheminement en cas d'erreur sur l'adresse ou le réseau IP et la station est reconnue moins sûre. Afin de lui permettre d'accéder à un jeu réduit de fonctionnalités, cette nouvelle tentative recherche sur la station distante un fichier à un emplacement précis. S'il est trouvé, la station est affectée de l'étiquette « reconnue moins sûre » dont la chaîne de caractères devient à son tour le nom d'une politique CSD.

Il est possible de créer plusieurs politiques en fonction d'une analyse préliminaire de certaines caractéristiques du poste de travail. Par exemple, toute station ne possédant pas une clé spécifique dans sa base de registre est considérée comme étant dans un lieu non sécurisé. Cette politique ouvre par la suite le droit d'effectuer certaines actions comme la navigation sur Internet ou l'accès à des fichiers. L'image nous montre aussi les icônes de configuration des divers contrôles de sécurité de chaque politique. Nous y trouvons les dispositifs de nettoyage du cache de la station distante ainsi que divers autres contrôles visant à prémunir la station contre les enregistreurs de clavier ou l'introduction de médias amovibles.

Figure V-17: Secure Desktop for SSL VPN "utilisateur sur le point d'entrer.

Voici l'utilisateur sur le point d'entrer dans son environnement protégé par CSD. Il est indiqué qu'aucun enregistreur de clavier n'a été détecté sur la station.

V.6.1.2 Politique d'accès dynamique :

Ce type de politique permet d'affecter des droits d'accès et de circulation sur le réseau à un utilisateur en fonction de ses propriétés d'authentification (AAA) et de la présence sur sa machine d'un logiciel de sécurité correctement paramétré.

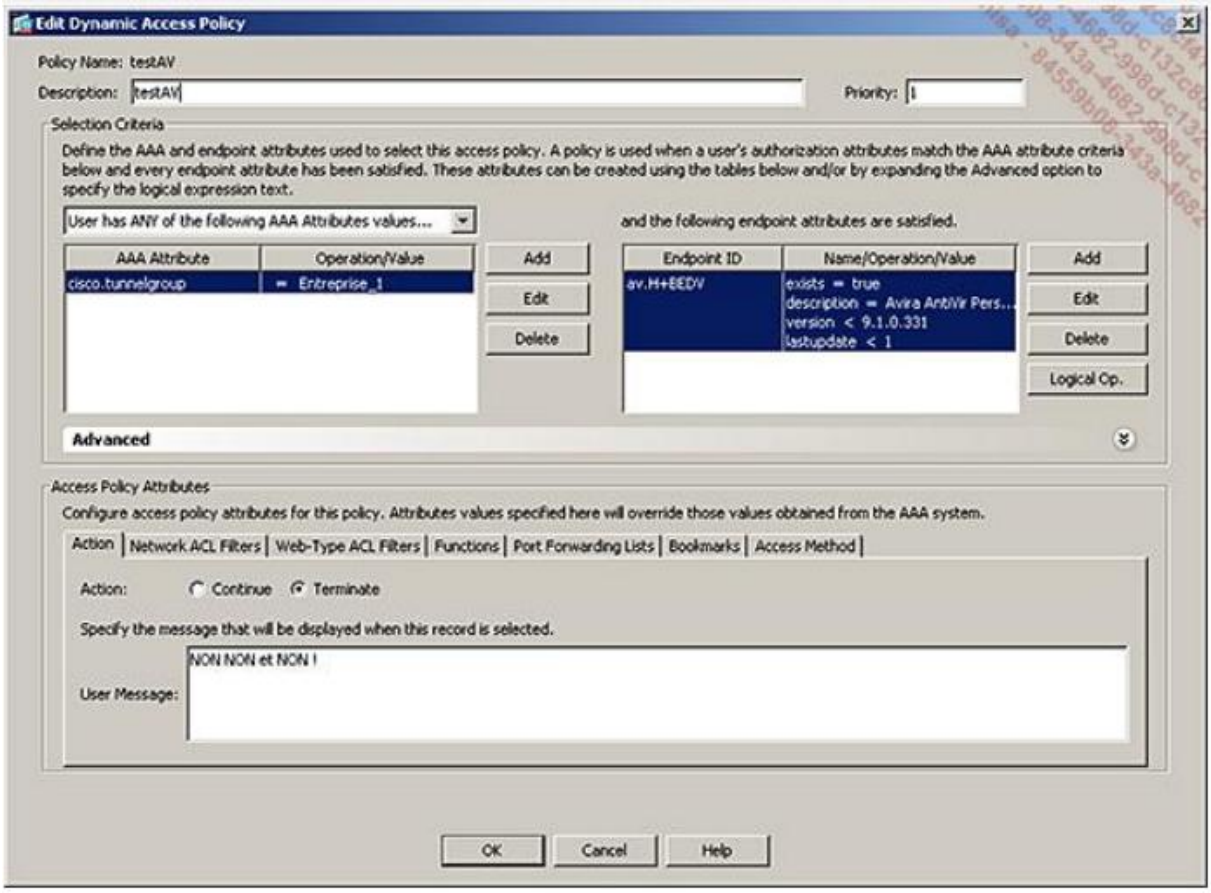


Figure V-18: Politique d'accès dynamique des utilisateurs

Voici l'exemple d'une politique d'accès dynamique concernant les utilisateurs d'un profil de connexion qui doivent également satisfaire à des conditions de version d'antivirus (moteur et signature). Si l'une des conditions n'est pas remplie ou au contraire est remplie, des attributs supplémentaires sont affectés à l'utilisateur et viennent prendre le dessus sur les valeurs obtenues par l'authentification AAA. Sur la capture d'écran, en cas de non-conformité, la connexion est coupée.

V.6.1.3 Protection applicative :

L'un des objectifs de l'inspection applicative est d'examiner le contenu des paquets (filtrés par une ACL) afin de permettre au pare-feu d'ouvrir les ports nécessaires à la communication. Cette ouverture dynamique est suivie d'une fermeture des ports une fois la communication achevée. Ce principe est appliqué lors de la traversée des protocoles associées à la téléphonie sur IP.

L'inspection va aussi confronter les paquets à un groupe de règles destinées à détecter d'éventuelles irrégularités le tout donnant lieu à une décision comme dans l'exemple à suivre qui concerne HTTP et SCCP.

```
class-map Inspection_SCCP
 match any
!
class-map Inspection_HTTP
 match any
!
!
policy-map type inspect http Niveau_de_securite_HTTP
 parameters
   protocol-violation action drop-connection log
 class asdm_high_security_methods
   drop-connection
 match request header non-ascii
   drop-connection
policy-map Inspection_SCCP_et_HTTP
 class Inspection_SCCP
  inspect skinny
  set connection conn-max 100 embryonic-conn-max 20 per-client-max
100
   set connection timeout tcp 1:00:00 reset dcd 0:15:00 5
 class Inspection_HTTP
   inspect http Niveau_de_securite_HTTP
!
service-policy Inspection_SCCP_et_HTTP global
```

Nous retrouvons ici le traditionnel schéma « class-map dans une policy-map dans une service-policy » (cette phrase est à retenir !). Toutefois, nous observons une petite nuance. Il s'agit de la policy-map de type inspect qui est appelée dans *la policy-map Inspection_SCCP_et_HTTP*. Cette policy-map définit des actions en cas d'irrégularité dans le protocole. Nous sommes donc en présence d'un petit arsenal de lutte contre les attaques dissimulées dans les protocoles applicatifs.

V.6.2 VPN SSL avec Smart Tunnels :

La technologie Smart Tunnel permet de faire transiter des applications TCP (non WEB) entre l'ordinateur distant et le site central. Smart Tunnel vient en remplacement du client léger précédent qui assurait des fonctions de redirection de port à la manière d'un client SSH. Malgré tout, il est toujours possible d'activer les fonctions de redirection de port pour les applications qui ne sont pas supportées par la technologie Smart Tunnel (Outlook MAPI).

Smart Tunnel ne nécessite pas de disposer des droits administrateurs sur le poste de travail et met à disposition de l'utilisateur des connecteurs (plugins) pour certaines applications prédéfinies. Les connecteurs dispensent l'utilisateur de l'installation d'un programme additionnel.

```
ASA5505(config)# webvpn
ASA5505(config-webvpn)# smart-tunnel list Messagerie 1
thunderbird.exe platform windows
ASA5505(config-webvpn)# group-policy "BEA 1" attributes
ASA5505(config-group-policy)# webvpn
ASA5505(config-group-webvpn)# smart-tunnel enable Messagerie
```

Ici, nous configurons Smart Tunnel pour faire transiter le trafic issu de l'application de messagerie thunderbird.exe qui fonctionne sur une plate-forme Microsoft Windows.

Les connecteurs s'installent dans la mémoire flash de l'équipement via l'interface graphique après les avoir téléchargés sur le site de Cisco. Une fois en place, ils apparaissent dans le portail et donnent à l'intérieur d'une page web la possibilité de lancer une connexion SSH, RDP, Citrix ou encore VNC.

V.6.3 VPN SSL avec le client AnyConnect :

Le client « lourd » AnyConnect s'installe manuellement ou automatiquement sur un poste client et crée sur celui-ci une interface réseau virtuelle ainsi qu'une route statique. Ce client possède un avantage certain par rapport à un client de type VPN IPSec car il est exempt de toute configuration. Une fois installé, l'utilisateur dûment authentifié est directement connecté sur le réseau local de l'entreprise. La configuration d'AnyConnect comporte plusieurs étapes.

```
ip local pool AnyConnect 192.168.1.10-192.168.1.20 mask
255.255.255.0
!
group-policy Client1 internal
group-policy Client1 attributes
 banner value Bonjour bonjour
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol svc
 group-lock value AnyConnect
 msie-proxy method no-proxy
 vlan none
 nac-settings none
 address-pools value AnyConnect
 webvpn
  url-list value template_entreprise_1
  svc dtls enable
  svc keep-installer installed
  svc keepalive none
  svc compression deflate
  svc profiles none
  svc ask none default svc
  customization value Entreprise_1
  deny-message value Des droits vous manquent
```

Tout d'abord, une politique de groupe est créée. Elle comporte quelques propriétés comme l'indication de la mise en place d'un tunnel SSL *vpn-tunnel-protocol svc* et l'affectation d'un groupe d'adresses IP *address-pools value AnyConnect*.
Les instructions sous *webvpn* concernent le client VPN et indiquent entre autre de laisser le programme d'installation sur la machine hôte et de forcer son installation.

```
Username Amine password bI0TiI3IJ4S1atiy encrypted
username Amine attributes
 vpn-group-policy Client1
```

Amine est rattaché à la politique de groupe précédemment créée.

```
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool AnyConnect
 authentication-server-group (outside) LOCAL
 default-group-policy Client1
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyC enable
```

Le tunnel est mis en place et reçoit les propriétés précédemment créées. La commande d'authentification appelle le serveur AAA interne (LOCAL) du firewall pour assurer cette fonction sur l'interface externe.

Figure V-19: fenêtre statistique de AnyConnect.

En cliquant sur le petit cadenas (première icône à gauche) nous obtenons la fenêtre qui fournit quelques indications comme l'adresse IP obtenue et celle du pare-feu sur laquelle se termine le tunnel SSLVPN.

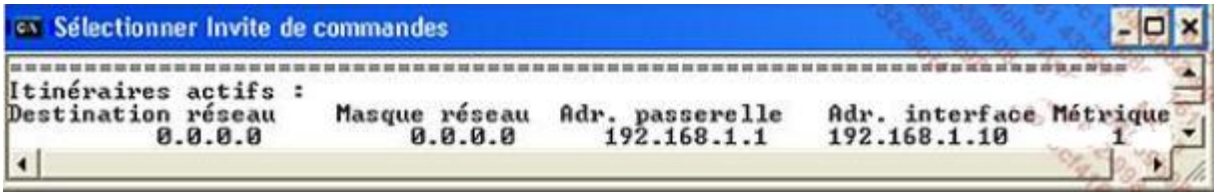


Figure V-20: Le résultat de la commande netstat sous CMD (windwos).

`Netstat` : permet de fournir des information utiles sur le réseaux, notamment pour afficher les numéro de port des sockets qui sont à l'écoute dans un ordinateur, On 'ajoute l'option -r (netstat -r) pour Affiche la table de routage.

Ici, nous observons le retour de la commande *netstat -n* sur la station de travail et nous constatons la présence d'une route par défaut pointant vers l'adresse interne du pare-feu.

```
ASA5505# sh vpn-sessiondb svc

Session Type: SVC

Username     : Amine                  Index        : 2
Assigned IP  : 192.168.1.10           Public IP    : 198.10.10.2
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : 3DES AES256            Hashing      : SHA1
Bytes Tx     : 53140                  Bytes Rx     : 22736
Group Policy : Client1                Tunnel Group : AnyConnect
Login Time   : 18:58:50 UTC Fri Oct 24 2008
Duration     : 0h:01m:25s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Figure V-21: Résultat de la commande show vpn-sessiondb svc.

Voici le résultat de la commande *show vpn-sessiondb svc* qui montre les caractéristiques de la connexion de Mr Amine. Les informations fournies sont très lisibles et directement exploitables toutefois, le mot clientless qui apparait ici porte à confusion.

Dans cette configuration ne figure aucune indication concernant le split-tunneling qui est la technique autorisant l'utilisateur d'un tunnel à en sortir pour accéder à certaines ressources. Cela signifie en l'état que ce choix n'est pas permis.

Le split-tunneling est utilisé pour les connexions à Internet à partir de la station de travail d'un utilisateur nomade.

En fonction de la politique de sécurité le trafic Internet de l'utilisateur nomade est soit contraint de passer par le site central ou bien autorisé à sortir directement ce qui ne va pas sans soulever quelques interrogations.

Ici, la politique de sécurité du réseau rejoint celle des stations de travail qui pour les accès nomades impose des protections comme les firewalls personnels, les antivirus et des mécanismes (ou procédures) de désactivation des interfaces autres que celle sur laquelle le tunnel est établi.

Signalons enfin qu'au niveau réseau en fonction de l'architecture les règles de traduction d'adresses devront être ajustée. La configuration présentée nécessite une règle d'exclusion car le réseau affecté à la station nomade existe sur le réseau interne.

VI. Conclusion :

ASA Cisco est un pare feu parmi plusieurs qui assure une sécurité des réseaux. Il nous permet d'appliquer un concept de règles de filtrage sur les routeurs, pour régler le trafic des datagrammes en transit, Nous avons exposé dans ce chapitre quelques-unes des multiples fonctionnalités avec leur configurations offertes par le pare-feu ASA qui vont bien au-delà de la simple confrontation du trafic à des règles de filtrage. Sans cette évolution, ce type de matériel serait sans doute tombé en désuétude. Le pare-feu ASA de Cisco est un équipement multifonction aux possibilités remarquables qui reprend les fonctions de base comme le filtrage et y ajoute celles issues des boîtiers VPN. Toutes les couches du modèle OSI sont couvertes et les protocoles applicatifs bénéficient d'un puissant service d'analyse permettant de parer aux problèmes d'irrégularités et d'attaques embarquées.

Le VPN SSL est une avancée significative permettant aux entreprises de fournir des accès applicatifs en toute sécurité à leurs partenaires avec ou sans l'installation d'un client spécifique. Ces accès sont également subordonnés à des contrôles de sécurité sur le poste client portant sur le type de système d'exploitation ou d'antivirus.Le pare-feu ASA vient également au service de la téléphonie sur IP avec une prise en compte des spécificités de ses protocoles parmi lesquelles figurent l'attribution dynamique des ports de communication.

Dans l'architecture de sécurité, le pare-feu ASA de Cisco occupe, de par ses capacités d'analyse multicouches, des positions qui ne se limitent pas aux frontières avec le monde extérieur car ses spécificités font de lui un appareil capable de protéger également l'intérieur du réseau. Dans ce chapitre donnera naissance à une nouvelle étape celle de la réalisation ou nous essayons de démontrer l'application et le test des exigences des sécurités sur notre réseau.

Partie II : Contribution

Chapitre 6 : Analyse de l'existant

I. Introduction :

Les réseaux informatiques comme on a déja vue sur la Partie I : Etat de l'art sont nés dû au besoin d'échanger des informations de manière simple et rapide entre des machines.

Le besoin d'échange d'information est en pleine expansion et ceci est constaté dans le mode de vie des sociétés modernes. Comment pourrait-on réserver un billet d'avion vers n'importe quelle destination ?, faire une transaction bancaire ?ou faire une inscription à distance ? Sans les réseaux informatiques ce serait très difficile.

La Banque Extérieure d'Algérie a ressenti ce besoin. Elle juge donc nécessaire et utile l'utilisation des mesures de sécurité pour sécuriser ses données.

Mais avant de répondre cette question, nous tenons à présenter cet organisme : ses missions et son organigramme.

II. I .HISTORIQUE

- Dénomination : Banque Extérieure d'Algérie « B E A ».
- Statut juridique : Société Par Actions (Etat Algérien actionnaire à 100%).
- Président Directeur Général : M. Mohamed Loukal.
- Capital : 24, 5 milliards de dinars.
- Siège Social : 11, Boulevard Amirouche - Alger, Algérie.
- Activité : Production bancaire et financement de tous les secteurs d'activité notamment des hydrocarbures, de la sidérurgie, des transports, des matériaux de construction et des services.
- Réseau d'agences : 86 agences (segmentées en agences *Corporate*, particuliers et universelles).

- Réseau de correspondants bancaires étrangers : 1500 correspondants.

La Banque Extérieure d'Algérie fut créée le 1er octobre 1967 par ordonnance n° 67.204, Elle avait pour Principale mission : faciliter, développer, les rapports économiques et financiers de l'Algérie avec le reste du monde.

Entre 1963 et 1966, plusieurs banques ont vu le jour ; tels que la CNEP en Août 1964, la BNA en Juin 1966 et le CPA en septembre de la même année.

La Banque Extérieure d'Algérie fut créée le 1er octobre 1967 par ordonnance n° 67.204, sous la forme d'une société nationale avec un capital de départ de 24 millions de dinars, constituée d'une dotation entièrement souscrite par l'état en reprise des activités du Crédit Lyonnais.

Dans le cadre du parachèvement du processus de nationalisation du système bancaire algérien, la BEA a repris successivement les activités des banques étrangères exerçant en Algérie ; celles de la Société Générale dans sa Situation au 31 décembre 1967, puis de la Barclay Bank Limited au 30 avril 1968, puis du Crédit Nord, de la Banque Industrielle de l'Algérie et de la Méditerranée (BIAM) dans leurs situations au 31 mai 1968.

BEA n'a eu cependant sa structure définitive qu'à partir du 1er Juin 1968. Le capital ayant été exclusivement souscrit par l'État.

Depuis 1970, la Banque Extérieure d'Algérie s'est vu confier la totalité des opérations bancaires des grandes sociétés industrielles nationales.

A la faveur de la restructuration des entreprises industrielles et des mutations profondes engagées par le pouvoir public dans les années 80, la BEA change de statut et devient, le 05 février 1989, Société Par Actions (Cf. disposition de la loi 88.01 du 17 janvier 1988 portant autonomie des entreprises) en gardant globalement le même objet que celui qui lui est fixé par l'ordonnance du 1er octobre 1967. Son capital, qui pouvait être augmenté en une ou plusieurs fois par la création d'actions nouvelles dont les conditions sont arrêtées par l'assemblée générale extraordinaire des actionnaires, est porté à 1 Milliard de dinars. Il était détenu par les ex-fonds de participation des principaux secteurs du portefeuille commercial de la BEA (outre les hydrocarbures), à savoir :

- Fonds de participation « Construction »
- Fonds de participation « Électronique, Télécommunication, Informatique »
- Fonds de participation « Transport et Services »
- Fonds de participation « Chimie, Pétrochimie, Pharmacie »

En 1991, le capital de la banque a augmenté de 600 millions de dinars passant ainsi de 1 milliard six cent millions de dinars (1, 6 milliards de Da).

En mars 1996, le capital de la BEA est passé à 5,6 milliards Da. Après la dissolution des fonds de participations, le capital demeure propriété de l'état. Le capital de la BEA n'a cessé de

croître depuis cette date passant de 12 milliards de Da en 2000 à 24,5 milliards de Da -en septembre 2001.

III. ORGANIGRAMME GENERAL:

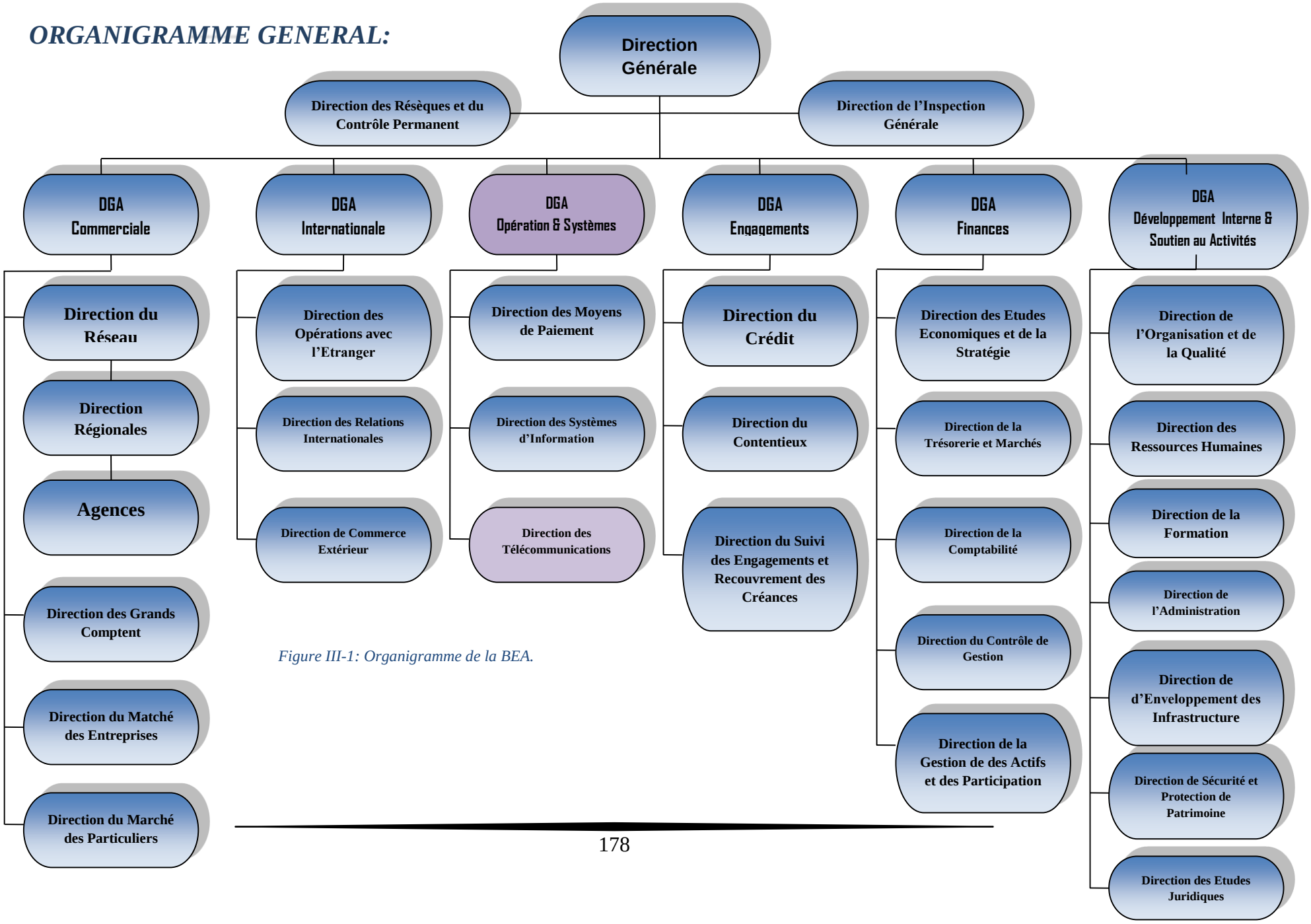


Figure III-1: Organigramme de la BEA.

CHAPITRE 6 : *Analyse de l'existant*

III.1 Présentation de la Direction de télécommunication

III.1.1 Le Département « TRANSMISSION DE DONNEES ET TELEPHONIE » :

Il a pour mission de :

- ☞ Réaliser des études portant sur l'architecture, la configuration et les évaluations économiques sues réseau de transmission de données.
- ☞ Assurer, en relation avec le prestataire de bande passante l'évolution du réseau de transmission des informations de la Banque.
- ☞ Assurer la maintenance et le suive de l'évolution des techniques (supports, équipements, etc …).
- ☞ Optimiser les coûts des prestations Télécom en fonction de l'évolution technologique.
- ☞ Etablir le rapport d'activité de déploiement des produits télécom.

III.1.2 le secteur « téléphonie et PABX » :

IL est chargé de :

- ☞ Prendre en charge les nouvelles installations et Recenser les dérangements des lignes téléphonique signalé par les structures et s'assurer de leur rétablissement ;
- ☞ Prosper de nouvelles solutions pour la téléphonie (téléphonie sur IP) à moindre cout et une bonne qualité de service ;
- ☞ Recenser les PABX installés au niveau des structures et agence, contrôle leur bon fonctionnement et assurer leur maintenance.

III.1.3 Le Secteur « Réseau Spatial (VSAT) » :

Il est chargé de:

- ☞ Assurer une continuité des transmissions en cas de défaillance du Réseau terrestre.
- ☞ Assurer le suivi des alarmes et la maintenance des équipements VSAT (Mini Hub et Station Distantes.
- ☞ Surveiller le débit réel et la bande passante garantie.
- ☞ Définir les nouveaux points de raccordement au Réseau VSAT.

- ☞ Tenir la documentation des points de présence et Assurer la sécurisation des antennes VSAT.

III.1.4 le secteur « réseau principal (haut débit terrestre) » :

IL est chargé de:

- ➢ Définir les topologies optimales et sécurisées des réseaux à mettre en place ;
- ➢ Assurer la coordination des travaux de maintenance avec les techniciens d'Algérie Télécom ;
- ➢ Suivre l'opération de mise en service des modems et convertisseurs ;
- ➢ Assurer l'aspect logistique pour la mise en place du réseau LS (pour les nouvelles réalisations)

III.1.5 Le département « administrations et sécurisation du réseau » :

Il a pour mission de :

- ☞ Assurer la Gestion et l'administration du Réseau de Télécommunication.
- ☞ Assurer l'installation et la supervision des Réseau de Télécommunication.
- ☞ Mettre en place la politique de sécurité du Réseau informatique de la Banque.
- ☞ Proposer les outils et les méthodes nécessaires à l'amélioration et à la modernisation des moyens de sécurité du Réseau.
- ☞ Prendre en charge la gestion de la partie sécurisation et installation du Réseau informatique.
- ☞ Superviser l'exploitation et l'administration des équipements de sécurité déployés sur les plates formes Agences/site Central.
- ☞ Mettre en place les procédures d'exploitation liées à l'aspect sécurité de l'information.
- ☞ Prendre des décisions adéquates en cas d'incidents
- ☞ Veiller au respect des règles de sécurité des données.

III.1.6 Le service «Administration du Réseau et Interconnexion » :

IL est chargé de:

- ☞ Prendre en charge la gestion et l'installation ainsi que la supervision des réseaux.
- ☞ Gérer les incidents télécom rencontrés par l'ensemble des structures de la banque.
- ☞ Gérer le réseau en fonction des nouveaux produits et des novelles application.
- ☞ Assurer l'optimisation du réseau et la configuration.
- ☞ Prendre en charge la configuration des serveurs et des routeurs (niveau3 : adressage).

III.1.7 Le secteur « sécurité des accès réseau » :

IL est chargé de :

- ☞ Installer est mettre en servies les outils de sécurité au niveau de l'ensemble des Agences /structures centrale concernées.
- ☞ Analyser l'impact de la mise en œuvre des solutions liées à la sécurité sur le réseau de Télécom existant ;
- ☞ Planifier les travaux d'installations et veiller au respect des délais de réalisation.
- ☞ Veiller au bon fonctionnement des équipements de sécurité et aux respects des règles de sécurité des données.
- ☞ Etablir une charte de Sécurité et Veiller au respect de cette dernière par tous les utilisateurs du Réseau.

IV. Organigramme de la Direction de Télécommunication :

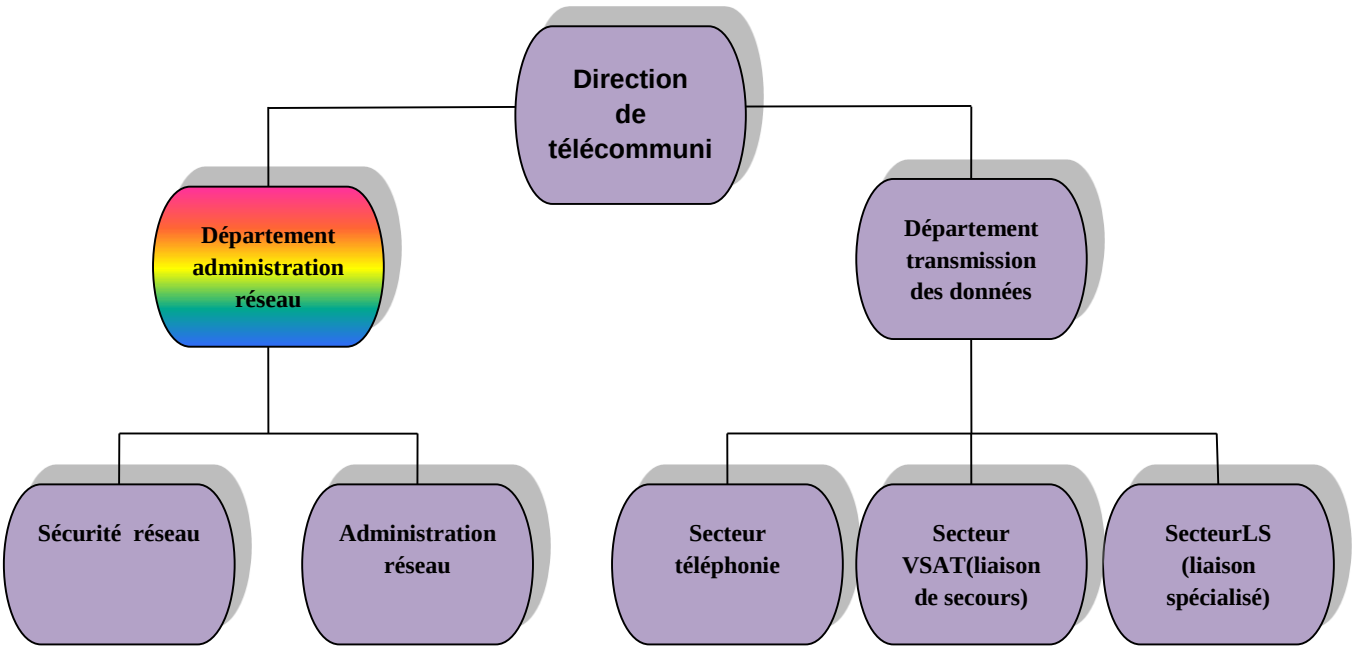


Figure III-1: Organigramme de la structure d'accueil.

IV.1 Schéma du réseau existant :

IV.1.1 Topologie :

Etoile « hub and spoke », centralisée sur un équipement de grande capacité (Cisco 7615).

IV.1.2 Equipement réseau :

IV.1.2.1 RT :

Equipement d'inter connexion et sécurité :

-Routeur : Cisco isr 4200

-Cisco 2911 Routeur de secours au niveau de l'Agence.

-Switch Cisco 2960 et switch Cisco 2960 x PoE.

IV.1.2.2 LS :

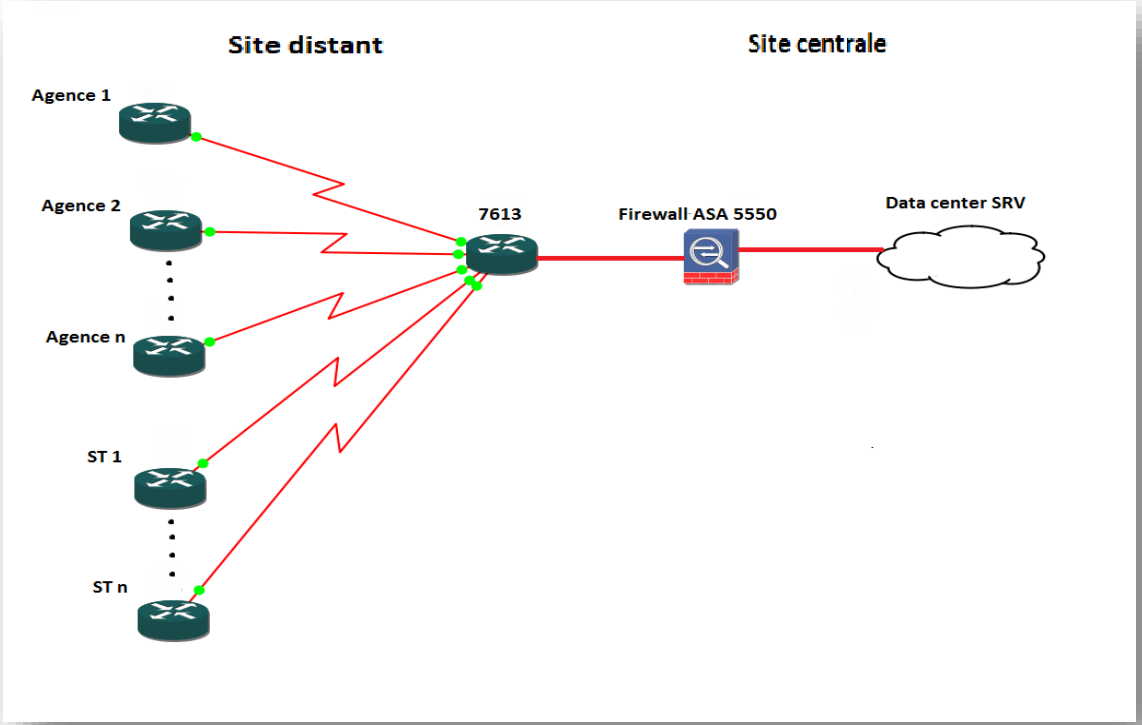
-Où toutes les Agences sont reliées au site central par une liaison spécialisée (LS) de 2Mbit/s cette liaison s'appelle VSAT.

Actuellement ; Le réseau de la BEA n'est pas centralisé c-à-dire que les agences travaillent sur un SRV celui d'un LAN. Chaque agence dispose d'un SRV de production.

IV.1.3 Architecture WAN :

- Topologie de la banque extérieure d'Algérie, est une architecture en étoile.
- Les liens utilisés sont des liaisons spéciales de 2Mbit/s entre chaque agence et/ou structure.
- Il existe aussi des liaisons de secours qui assure la continuité d'acheminement des données

Cette solution a l'avantage d'offrir la disponibilité est la continuité des services clients.



V. LES RESEAUX DE LA BEA :

Le site central est composé de trois directions :

- ❖ La direction des systèmes d'information (informatique) :

- Département infrastructure
- Département développement
- Département production

- ❖ La direction des moyens de paiement
- ❖ La direction de télécommunication

V.1 La propriété du réseau LAN du site centrale :

Figure IV-2: Schéma du réseaux existant..

✓ Tous les utilisateurs des trois directions sont connectés derrière plusieurs Switch suivant la configuration de chaque direction

- ✓ Le type de réseau adopté par l'entreprise est réseau client –serveur
- ✓ Chaque utilisateur possède sont propre poste de travail (Pc)
- ✓ La goulotte contient les câbles RJ45 partant du SWITCH jusqu'à la carte réseau de chaque machine
- ✓ Il y a cinq étages dans la direction, chaque etage contient un département donc plusieurs poste de travail
- ✓ Chaque Pc possède sa propre carte réseau qui lui permet de se connecter au réseau local via les câbles RJ45.
- ✓ Au niveau de quelques postes il existe des imprimantes connectées au réseau local de l'entreprise
- ✓ Au niveau des serveurs il existe un modem qui permet de se connecter à internet.
- ✓ Au sein du réseau local, il existe une salle de machine où se trouvent les SWITCH et des armoires de brassage.
- ✓ Chaque direction et département est séparé par des VLAN pour Faciliter la gestion de la mobilité des postes,Supprimer la possibilité de communication entre certaines parties du réseau et sécurisé des domaines.

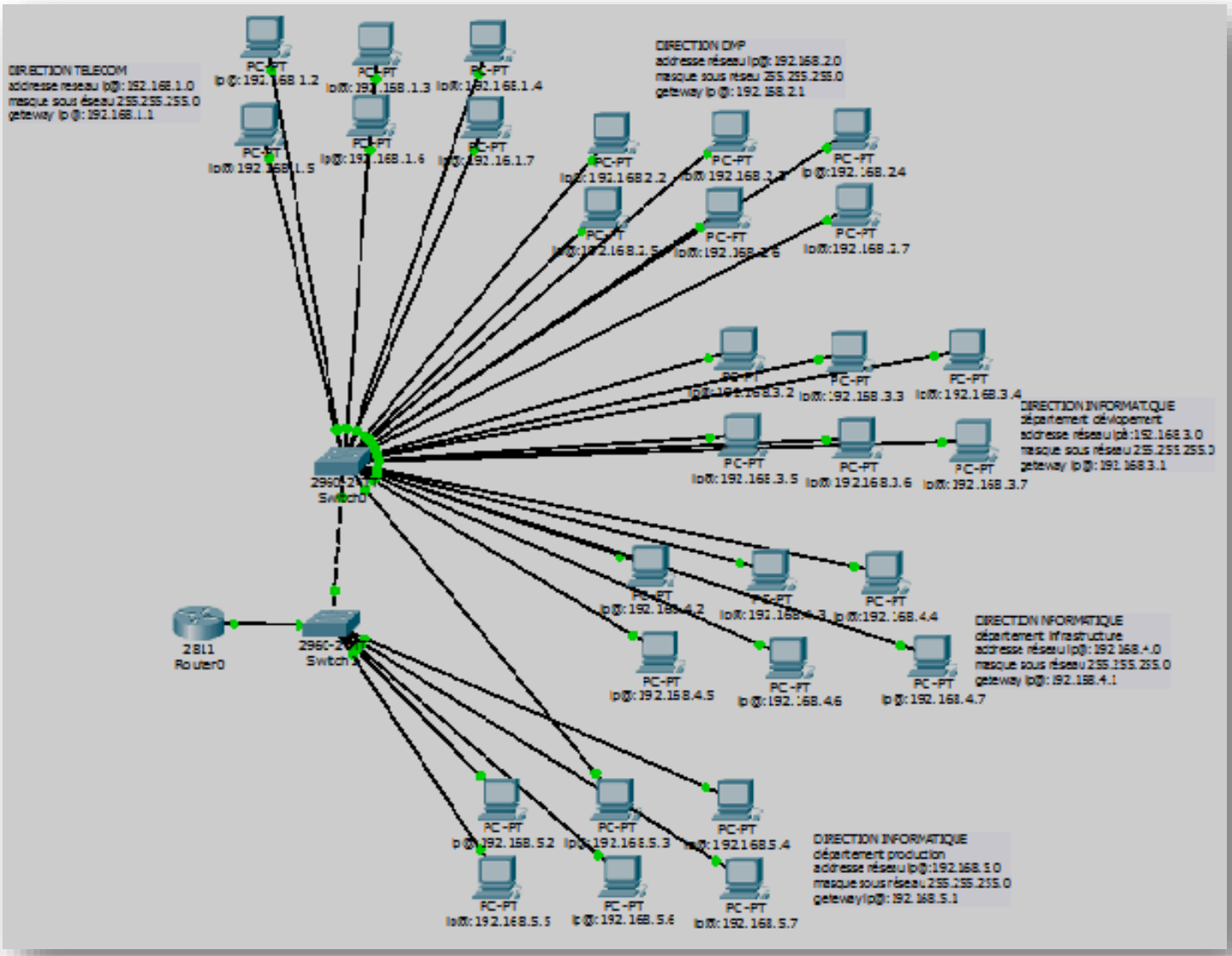


Figure V-1:Schéma du réseau LAN du site central.

Le réseau LAN du site central est reconnu par le nombre de poste de travail qui se trouve. Plus de cinquante postes séparés par des VLAN au niveau des Switch et le routeur pour assurer la sécurité interne du réseau et avoir une segmentation flexible du réseau LAN et une modifications logiques ou géographiques facilitées et gérées via une console d'administration plutôt que changer des câbles dans une armoire de brassage.

Tous ces câblages se retrouvent connectés dans la salle des machines à plusieurs Switch ou il y a des serveurs et routeurs pour se connecter à l'extérieure.

Les Switch sont raccordés en mode trunk,Un trunk est un lien entre deux équipements, le plus souvent entre deux Switch, configurés de telle sorte que l'on peut y faire circuler des trames Ethernet modifiées comportant des informations relatives au VLAN sur lequel elles transitent.

V.2 Réseau Wan :

V.2.1 Réseau ls :

Le réseau WAN de la BEA est composé d'un réseau terrestre qui est le réseau principal des liaisons spécialisées point à point, ils se concentrent au niveau du site central derrière l'équipement de transmission d'ALGERIE TELECOM HUAWEI sous forme de quatre STM qui se connectent au niveau d'un routeur de grande capacité CISCO 7600.

V.2.2 Réseau VSAT :

Le VSAT désigne "Very Small Aperture Terminal" qui se défini comme un équipement de télécommunication par satellite permettant de raccorder les réseaux terrestres.

Le VSAT se réfère à la réception et à la transmission des terminaux installé dans des sites dans la connexion à un concentrateur central par satellites au moyen de petites antennes paraboliques de diamètres variant entre 0.6 et 3.8 mètres. Le satellite envoie et reçoit des signaux provenant d'une station terrienne qui agit comme un hub pour le système. Chaque utilisateur est relié à la station centrale via le satellite. Pour un utilisateur final à communiquer avec un autre, chaque transmission doit d'abord aller à la station centrale qui la retransmet via le satellite VSAT pour l'utilisateur final. Le VSAT gère les données, la voix et des signaux vidéo.

Le réseau VSAT se présente sous deux principales formes :

- la forme (ou topologie) en étoile.
- la forme maillée.

Le rôle du VSAT dans le réseau WAN de la BEA :

Le réseau LS est secouru par un réseau spatial VSAT d'une technologie DVBRCS. Lorsque la liaison spécialisée tombe en dérangement le réseau bascule automatiquement sur le réseau VSAT.

Le VSAT de la BEA se présente sous forme en étoile comme indique la figure suivante :

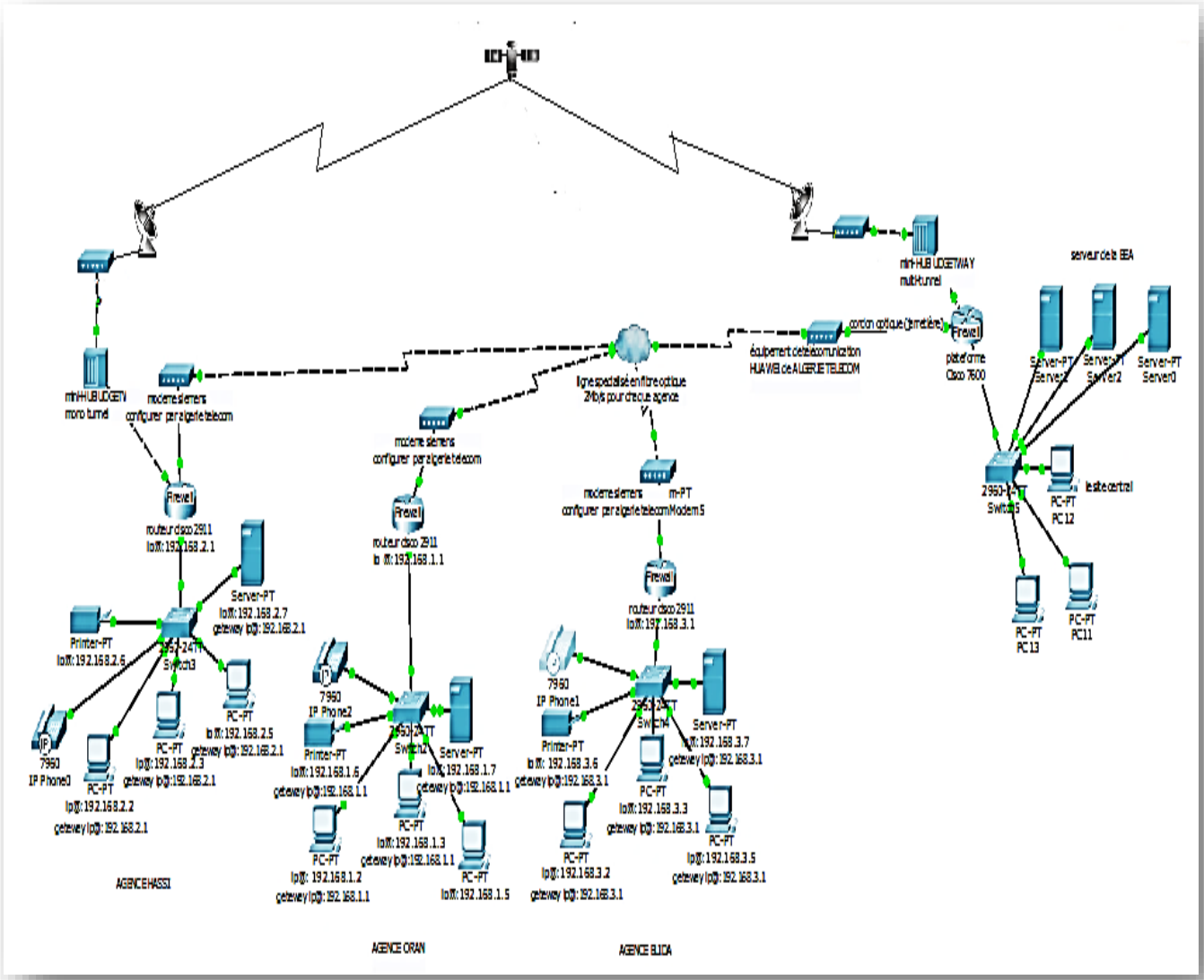


Figure V.2-2:Schéma d'architecture du réseau WAN de la BEA.

VI. PRESENTATION DES OUTILS DE SECURITE :

Au niveau du site central le réseau VSAT est sécurisé par un firewall Cisco ASA, le firewall Cisco ASA ce configure grâce a une interface graphique faite pour simplifier la manipulation du système firewall est en plus il assure une protection optimale, grâce à ses nombreuses fonctionnalités comme on a déjà vue en détail sur le chapitre précédant:

- **Inspection applicative** : contrôle application, support des protocoles voix et vidéo ;
- **Prévention des intrusions**: protection en temps réel contre les attaques des applications DOS, détection et filtrage de l'activité réseau des vers et des virus, détection des spywares, adwares et malwares ;
- **Sécurisation IPCom** : inspection avancée des protocoles voix, signatures IPs spécifiques ;
- **Connectivité SSL et IPsec** : services IPSec et SSL protégés, services SSL avec client ou avec portail ;
- **Gestion de 450 Mbps de trafic** ;
- **Activer ou désactiver votre firewall**, directement depuis votre Manager.

En plus il est sécurisé par les VPN par un équipement multi-tunnel UDGETEWAY au niveau du site central et mono-tunnel au niveau des agences.

VII. Détection des problèmes de sécurité et proposition de solutions :

1-La décentralisation des SRV (manque de la disponibilité des services bancaires) :

Actuellement ; Le réseau de la BEA n'est pas centralisé c-à-dire que les agences travaillent sur un SRV celui d'un LAN. Chaque agence dispose d'un SRV de production. Comme ça se voit sure la figure suivante :

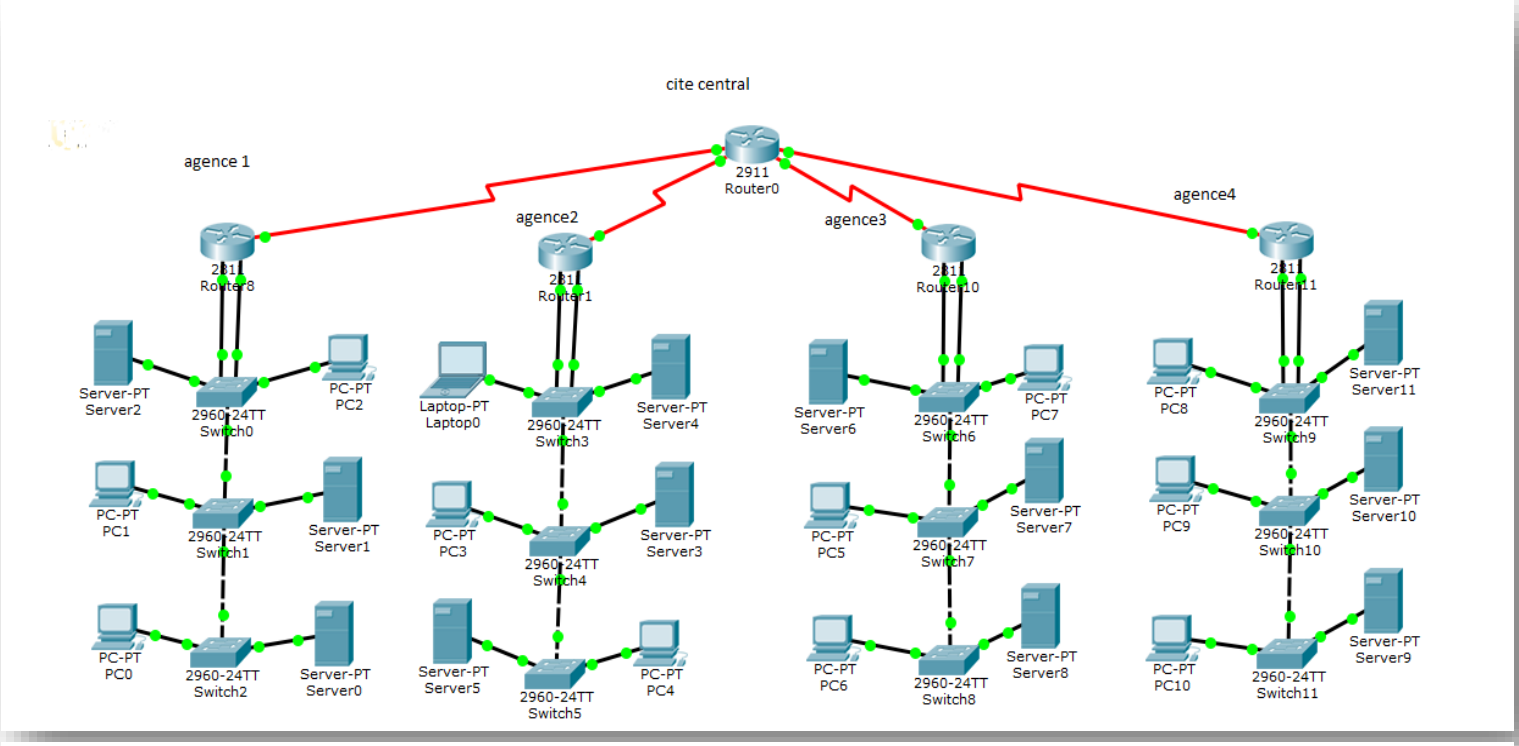


Figure VII-1: Schéma expliquant l'architecture existante « architecture décentralisé de la BEA ».

Cette architecture présente des inconvénients pour les clients (Détérioration de la qualité de services) et pour la banque (la sécurité des données est moins sûre dans le réseaux de l'agence par rapport au niveau de site central)

- Solution :

Afin de remédier à ces inconvénients, nous avons proposé la centralisation figure « FigureVII-2 » des données au niveau de site central dans notre réalisation « chapitre 07 », pour améliorer la qualité des services pour les clients de la banque et pour maitre les données des clients dans un milieux plus sûre. Ceci consiste à éliminer les serveurs au niveau des agences et de travailler directement sur le serveur central.

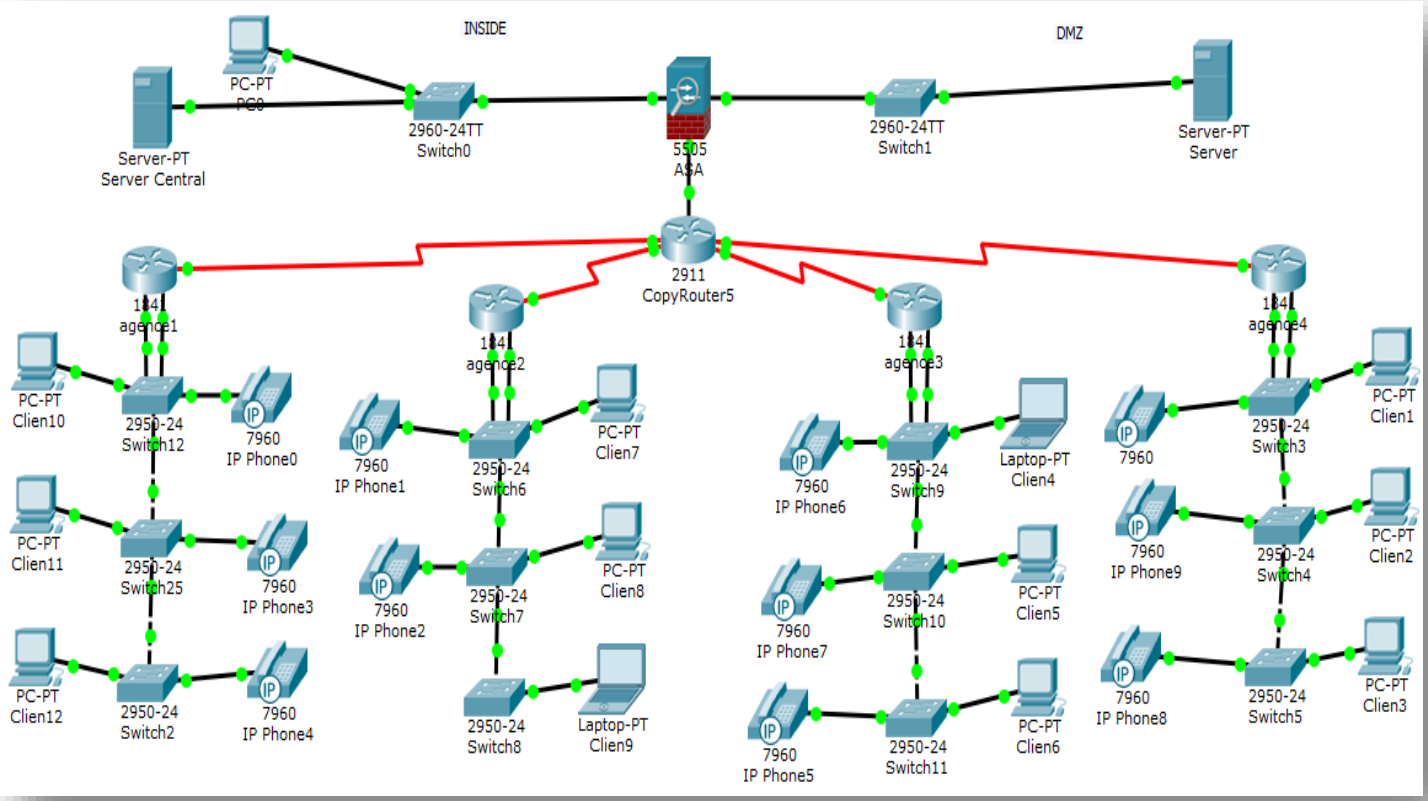


Figure VII-2:Schéma de l'architecture proposé « centralisation de l'architecture de la BEA ».

2- Besoin d'exigences de sécurité plus avancées et plus robustes :

Les agences contiennent des Configurations de sécurité basic basé sur des routeur (IOS sécurité) et d'après notre solution le cybercriminel n'a qu'une cible, donc le site central besoin des outils plus avancées pour convenir la solution centralisé et assurer la sécurité ..

- Perspectives et solutions :

Mètre on place un NGFW avec des exigences de sécurité stricte.

VIII. Conclusion :

Notre conclusion n'est qu'un préambule à notre étude qui s'étalera Dans le prochain chapitre ou on va essayer de réaliser et tester notre solution. Ce mémoire englobe plusieurs étapes. Nous l'avons développé dans les différents chapitres ou nous as essayer de toucher le côté administration et sécurité du réseau de la Banque Extérieure d'Algérie.

Chapitre 7 : Réalisation et Mise en place des solutions de sécurité

I. Introduction:

Dans ce chapitre, nous allons passer à la dernière étape de notre travail qui est la réalisation de notre projet, Notre objectif est de mettre en place des exigences de sécurité par rapport de ce que nous avons fait dans les précédents chapitres afin d'assurer la sécurité du réseau de la banque extérieure d'Algérie (site central) vis-à-vis des agences et surtout les clients de la banque.

Nous avons utilisé l'émulateur Packet Tracer. Ce logiciel Cisco modélisation de réseau pratique, mobile et flexible. Il permet de tester le comportement d'un réseau, de concevoir des modèles de réseau et de mettre en pratique des hypothèses comme notre cas ; la Voip, VPN, la mise en place des ACL ZBF…, La mise en place et la configuration de ASA.

La première étape dans ce chapitre consiste à la configuration basic (routage statique et dynamique...,) et réaliser des VLAN au niveau des agences et du site central, et l'implémentation de la Voip sur l'agence 3.

La deuxième étape illustre les différents ACL/ZBF appliquées au sein de la banque extérieure d'Algérie et la configuration de l'ASA 5505 et la Création d'un tunnel VPN IPsec entre deux sites.

I.1 Configuration des routes statiques et des routes dynamiques via le protocole OSPF :

La BEA présent une topologie de réseau hub-and-spoke « figure II-2 » qui signifie réseau en étoile, pour cela on a fait une combinaison de protocoles de routage dynamique et de routes statiques. Cela peut donner lieu à un routeur disposant de plusieurs chemins vers un réseau de destination via des routes statiques et des routes apprises dynamiquement. Toutefois, la distance administrative (AD) d'une route statique correspond à 1. Par conséquent, une route statique sera prioritaire par rapport à toutes les routes apprises dynamiquement.

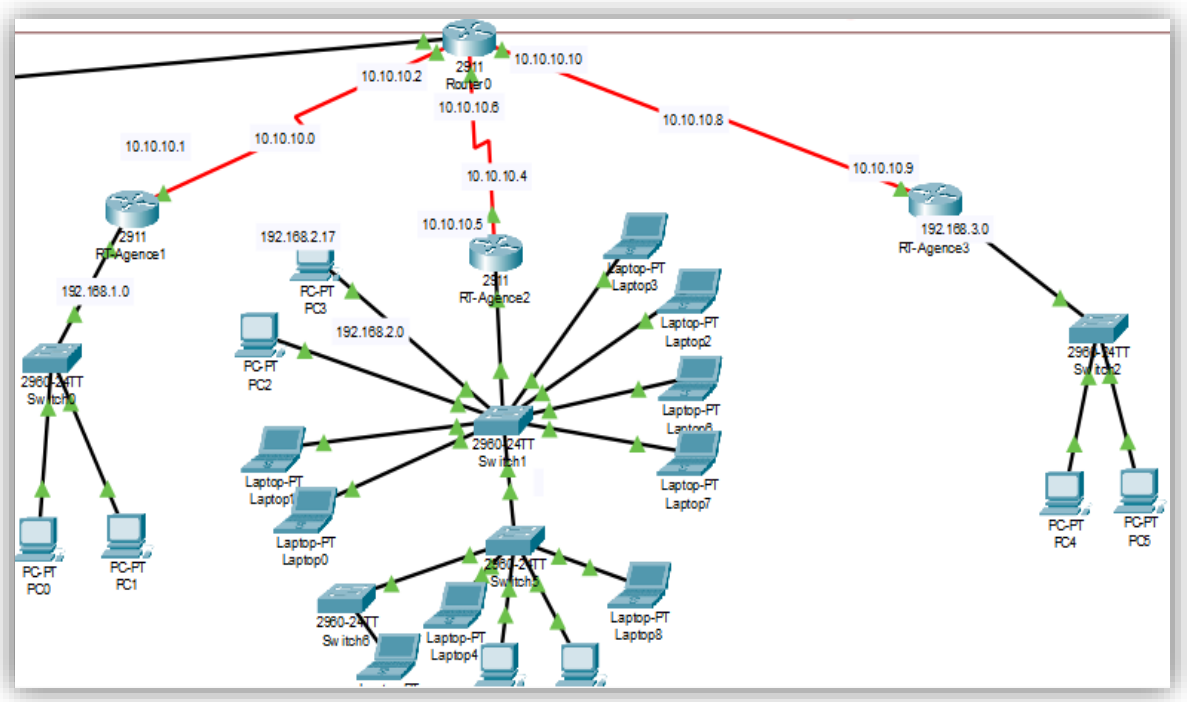


Figure I-1: Schéma du réseau existant.

Le routage est le processus permettant, à un datagramme d'être acheminé vers le destinataire, lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur, Les routeurs forment une structure coopérative, de telle manière qu'un datagramme transite d'une passerelle vers une autre, jusqu'à ce que l'une d'entre elles le délivre à son destinataire.

LA 1ER ÉTAPE:

I.1.1 Configuration des routes statiques :

Les routes statiques sont configurées au moyen de la commande de configuration globale ***ip route***. La syntaxe de la commande est la suivante :

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Figure I-2: La syntaxe de la commande ip route.

Tableau 5:Description de paramétre de la syntaxe ip route:

Paramètre	Description
network-address	Adresse de destination du réseau distant, à ajouter à la table de routage.
subnet-mask	• Masque de sous-réseau du réseau distant, à ajouter à la table de routage. • Le masque de sous-réseau peut être modifié pour récapituler un groupe de réseaux.
ip-address	• Généralement appelé adresse IP du routeur de tronçon suivant. • Généralement utilisé lors de la connexion à un support de diffusion (par exemple Ethernet). • Crée généralement une recherche récursive.
exit-intf	• Utilisez l'interface de sortie pour transférer les paquets vers le réseau de destination. • On parle également d'une route statique reliée directement. • Ces routes sont généralement utilisées pour la connexion dans une configuration point à point.

On commençant par le Router 0 (RT-Central) sur le mode configurable :

```
RT-Central>en
Password:
Password:
RT-Central#
RT-Central#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Central(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
RT-Central(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.5
RT-Central(config)#ip route 192.168.3.0 255.255.255.0 10.10.10.9
RT-Central(config)#end
RT-Central#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

En fait la même chose pour les autres Routeurs.

I.1.2 Configuration des routes dynamiques OSPF :

La technologie OSPF (Open Shortest Path First), est un protocole servant à déterminer le meilleur chemin que peuvent emprunter des paquets pour transiter par une série de réseaux connectés, Dans les réseaux d'entreprise, le protocole de routage OSPF a largement remplacé l'ancien protocole RIP (Routing Information Protocol) :

- ✓ La convergence en cas de problèmes est plus rapide qu'avec RIP.
- ✓ Le nombre de sauts n'est aucunement limité.
- ✓ L'envoi de la table ne se fait pas de manière régulière donc une meilleure utilisation de la bande passante.
- ✓ En plus de se baser sur l'état des liens, il se base aussi sur le cout de tel ou tel chemin. Il est calculé en fonction de la bande passante, plus la bande passante, plus le cout est faible.
- ✓ Si 2 chemins ont le même cout, il se basera sur le nombre de sauts. (17)

L'activation du protocole de routage OSPF et des réseaux participant aux annonces se fait de la manière suivante :

```
RT-Central(config)#router ospf 2
RT-Central(config-router)#network 10.10.10.8 0.0.0.3 area 0
RT-Central(config-router)# network 10.10.10.4 0.0.0.3 area 0
RT-Central(config-router)# network 10.10.10.0 0.0.0.3 area 0
RT-Central(config-router)#network 10.10.10.12 0.0.0.3 area 0
RT-Central(config-router)#do wr
Building configuration...
[OK]
```

Nous avons pris le numéro du processus ospf = 2, L'adresse IP des l'interfaces connectée à des autre routeurs est 10.10.10.10/30 | 10.10.10.6/30 | 10.10.10.2/30 | 10.10.10.13/30 et le numéro de l'aire est 0.

I.1.3 confirmer la configuration en tapant la commande (show running-config) :

Pour l'OSPF :

```
router ospf 2
 log-adjacency-changes
 network 10.10.10.8 0.0.0.3 area 0
 network 10.10.10.4 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.12 0.0.0.3 area 0
!
```

Et pour afficher des informations concernant ospf en tapant la commande (show ip ospf) :

```
RT-Central(config-router)#do sh ip ospf
 Routing Process "ospf 2" with ID 10.10.10.13
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 4
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x01864b
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Pour le routage statique :

```
ip classless
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 192.168.2.0 255.255.255.0 10.10.10.5
ip route 192.168.3.0 255.255.255.0 10.10.10.9
ip route 0.0.0.0 0.0.0.0 10.10.10.14
!
```

I.2 Configuration des VLAN :

Pour le Routeur de l'Agence 2 on va réaliser 4 VLANs

I.2.1 Diviser le Switch en 4 VLANS disposant chacun de 6 Interfaces Fa :

1. VLAN1: 192.168.2.0 / 255.255.255.0 Fa0/1 jusqu'à Fa0/6
2. VLAN2: 192.168.7.0 / 255.255.255.0 Fa0/7 jusqu'à Fa0/12
3. VLAN3: 192.168.8.0 / 255.255.255.0 Fa0/13 jusqu'à Fa0/18
4. VLAN4: 192.168.9.0 / 255.255.255.0 Fa0/19 jusqu'à Fa0/24

I.2.2 Créer les différents vlan :

- On va attribué également une adresse IP de manière à pouvoir les gérer à distance par la suite.
- (Rmq: les commandes utilisées ici sont celles disponibles sur un Switch Cisco 2960).

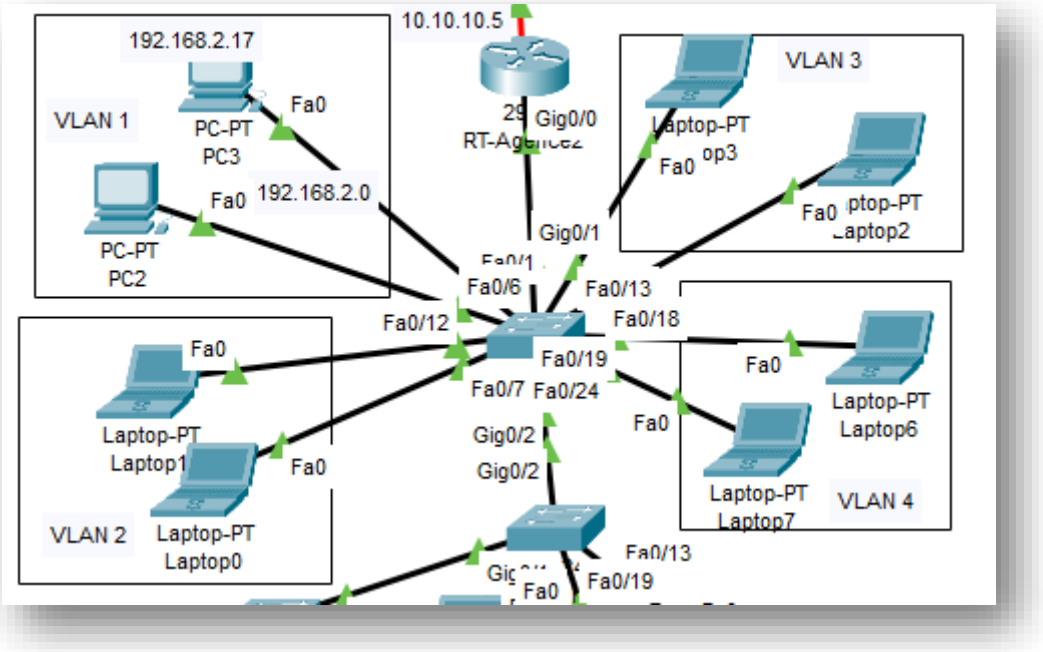


Figure I-3:Schéma des VLAN.

- Accéder en mode de configuration :

```
Switch>en
Switch#configure terminal
```

- Configurer l'IP du VLAN1 (qui existe par défaut) en 192.168.2.254 / 255.255.255.0

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.2.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

- Créer et configurer les VLAN2, 3 et 4 avec respectivement les adresses 192.168.7.254, 192.168.8.254 et 192.168.9.254 et un masque 255.255.255.0.

```
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.168.7.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.168.8.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#exit
Switch(config)#interface vlan 4
Switch(config-if)#ip address 192.168.9.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

I.2.3 Lancer maintenant les interfaces dans les vlans :

```
Switch(config)#interface range fastEthernet 0/7-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit

Switch(config)#interface range fastEthernet 0/13-18
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit

Switch(config)#interface range fastEthernet 0/19-24
Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 4
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
```

I.2.4 Test:

Vérifier si tout est bien mis en place. (on utilise ici « do show vlan » puisque la commande « ***show vlan*** » n'est pas disponible en mode config).

```
Switch(config)#do show vlan

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/6
2    vlan2                             active    Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12
3    vlan3                             active    Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18
4    vlan4                             active    Fa0/19, Fa0/20,
Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
```

Remarque :

Afin de permettre aux utilisateurs des différents VLANs de se communiquer entre eux. Nous devons utiliser un routeur. Ce dernier doit être connecté à un switch en **monde trunk** pour faire passer tous les VLANs.

```
Switch(config)#interfacegigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

En tape la commande « ***show interfaces switchport*** » pour vérifier le trunk sue l'interface GigabitEthernet 0/1 et voire la déférence sur l'interface GigabitEthernet 0/2.

GigabitEthernet 0/1:

```
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
.
.
.
```

GigabitEthernet 0/2:

```
Name: Gig0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
.
.
.
```

I.2.5 Création d'un VTP :

Le protocole VTP permet de créer les VLANs dans les deux Switch suivants :
- Le fonctionnement de VTP sur les Switch :

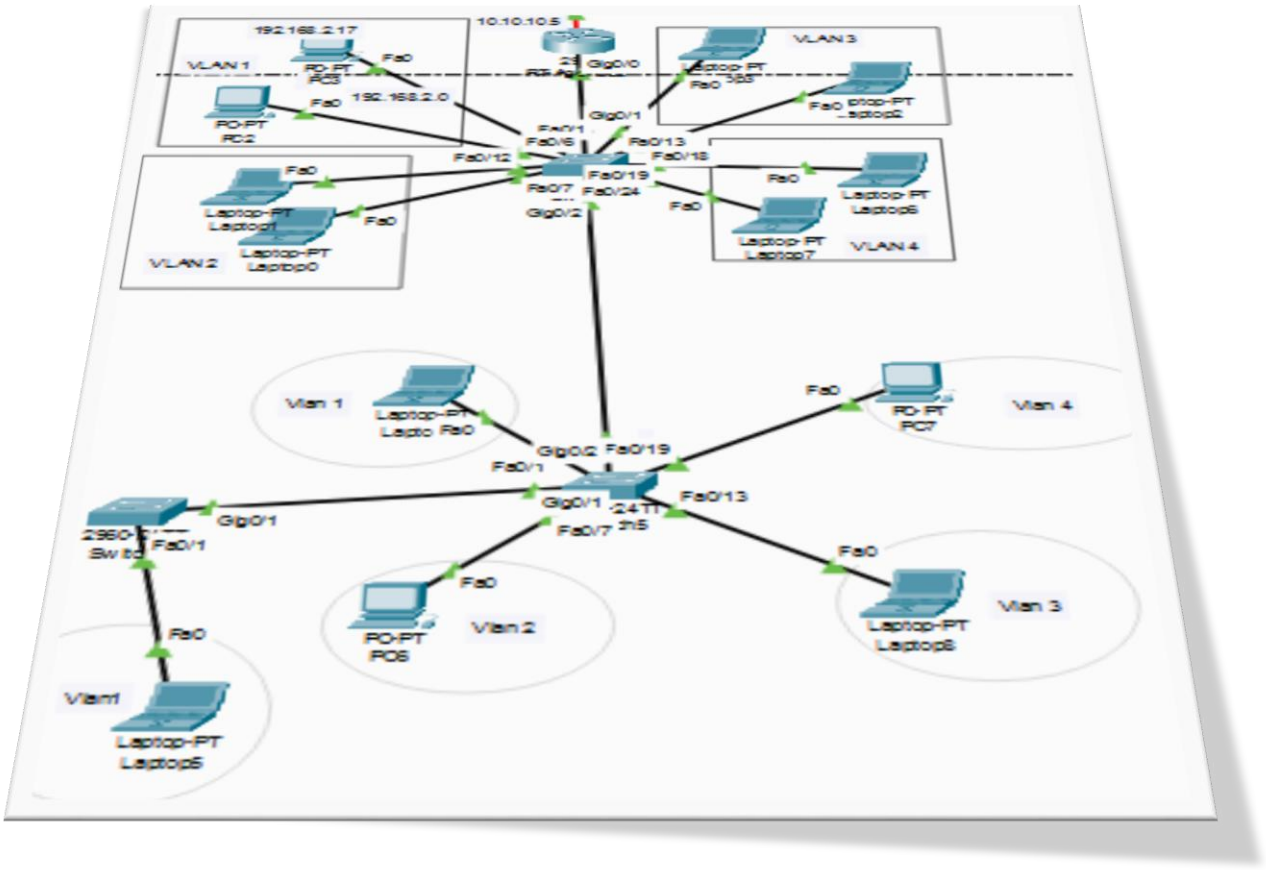


Figure I-4: Schéma de VLANs avec l'utilisation de protocole VTP.

Comme sa ce voit dans la « Figure II-5» sur le même schéma des VLANs on ajoute deux Switch :

Switch 1 :

Switch principale (mode serveur) :

-On tape les commandes suivantes : « ***vtp mode server*** » et « ***vtpdomain bea.dz*** » («bea.dz » c'est le nom de notre domaine)

```
Switche1#
Switche1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switche1(config)#vtp mode server
Device mode already VTP SERVER.
Switche1(config)#vtp domain bea.dz
Domain name already set to bea.dz.
Switche1(config)#
Switche1(config)#exit
Switche1#
%SYS-5-CONFIG_I: Configured from console by console

Switche1#wr
Building configuration...
[OK]
```

Switch 2 :

Sur les deux Switch (Switch2 & Switch3 mode client) sans créer les VLANs

- On tape les commandes suivantes « ***vtp mode client*** » et « ***vtpdomain bea.dz*** »

```
Switch2(config)#
Switch2(config)#vtp mode clien
Device mode already VTP CLIENT.
Switch2(config)#vtp domain bea.dz
Domain name already set to bea.dz.
```

Switch3 :

```
Switch3(config)#
Switch3(config)#vtp mode clien
Device mode already VTP CLIENT.
Switch3(config)#vtp domain bea.dz
Domain name already set to bea.dz.
```

- Accéder les portes de Switch2 & Switch3 au VLANs

- fastEthernet 0/1-6 ➔ VLAN 1
- fastEthernet 0/7-12 ➔ VLAN 2
- fastEthernet 0/13-18 ➔ VLAN 3
- fastEthernet 0/19-24 ➔ VLAN 4

et maitre en mode **trunk** les interfaces relient les switch .

I.2.6 Vérification de la création des VLAN :

On tape la commande « ***show vtp status*** » pour vérifier la configuration de Switch Serveur :

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : bea.dz
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x64 0xCB 0xD2 0xFA 0x66 0xFE 0x6F 0xF8
Configuration last modified by 192.168.8.1 at 3-1-93 02:07:26
Local updater ID is 192.168.2.254 on interface Vl1 (lowest numbered VLAN interface found)
Switch#
```

On tape la commande « ***show vtp status*** » pour vérifier la configuration de Switch2 et Switch3 :

Switch2 :

```
Switch#show vtp st
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : bea.dz
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x64 0xCB 0xD2 0xFA 0x66 0xFE 0x6F 0xF8
Configuration last modified by 192.168.8.1 at 3-1-93 02:07:26
Switch#
```

Switch3 :

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : bea.dz
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x64 0xCB 0xD2 0xFA 0x66 0xFE 0x6F 0xF8
Configuration last modified by 192.168.8.1 at 3-1-93 02:07:26
Switch#
```

On tape la commande « show vlan » dans les deux Switch. Le résultat est :

Switch2 :

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : bea.dz
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x64 0xCB 0xD2 0xFA 0x66 0xFE 0x6F 0xF8
Configuration last modified by 192.168.8.1 at 3-1-93 02:07:26
Switch#
```

Switch3 :

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Gig0/2
2    vlan2                             active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12
3    vlan3                             active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18
4    vlan4                             active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

I.3 Configuration du routeur:

Création des sous-interfaces pour chaque VLAN supplémentaires et les configurer (attribuer une adresse IP, et l'encapsulation de la sous interface).

```
RT-Agence2>en
RT-Agence2#conf t
RT-Agence2 (config)#intgigabitEthernet 0/0
RT-Agence2 (config-if)#ip address 192.168.2.1 255.255.255.0
RT-Agence2 (config-if)#no shutdown
```

Ceci correspond à l'adresse principale de l'interface, et également pare défaut au VLAN1.
Créons maintenant la sous-interface pour le VLAN2.

```
RT-Agence2 (config)#intgigabitEthernet 0/0.2
RT-Agence2 (config-subif)#encapsulation dot1Q 2
RT-Agence2 (config-subif)#ip address 192.168.7.1 255.255.255.0
RT-Agence2 (config-subif)#no shutdown
```

Dans la commande « encapsulation dot1Q 2 », le chiffre en fin de ligne correspond au numéro du VLAN.
On fait de même pour les interfaces relatives aux VLAN 3 et 4.

Vlan3 :

```
RT-Agence2 (config)#interface gigabitEthernet 0/0.3
RT-Agence2 (config-subif)#encapsulation dot1Q 3
RT-Agence2 (config-subif)#ip address 192.168.8.1 255.255.255.0
RT-Agence2 (config-subif)#no shutdown
RT-Agence2 (config-subif)#exit
```

Vlan4 :

```
RT-Agence2 (config)#interface gigabitEthernet 0/0.4
RT-Agence2 (config-subif)#encapsulation dot1Q 4
RT-Agence2 (config-subif)#ip address 192.168.9.1 255.255.255.0
RT-Agence2 (config-subif)#no shutdown
RT-Agence2 (config-subif)#exit
```

On tape la commande (***show runnig-config***):

```
!
!
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.7.1 255.255.255.0
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.8.1 255.255.255.0
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.9.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 --More--
```

Si tout s'est bien déroulé, la configuration des VLANs est maintenant terminée. Il ne suffit plus que de connecter les machines sur les différents VLANs et les configurer avec des adresses IP du même range que le VLAN où elles se trouvent.

I.4 La Téléphonie sur IP (Voip) :

Pour la configuration Voip on est besoin d'un routeur 2811, et pour permet aux téléphone analogique fonctionné avec la voip on est besoin d'un périphérique intermédiaire Home_Voip_PT pour convertie les signaux [Analogique = Numérique].

On va étape par étape certain configuration l'on ne peut pas faire de manière complète au niveau du routeur, il faut aller d'abord ver le commutateur puis ensuit revenir ver le routeur ….

I.4.1 Création des VLAN :

1erment on va configuré deux Vlan dans le commutateur, Vlan 20 pour la Voip et Vlan 10 « DATA » pour les données :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name donnees
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Voip
Switch(config-vlan)#
```

Ensuite dans le Routeur on va segmenter l'interface on deux sous interface avec les deux Vlan configurée dans le commutateur :

On va juste allumer l'interface, On ne va pas l'attribuer une adresse IP parce que on va utiliser les sous interfaces bien les interfaces logiques, on va diviser l'interface physique en plusieurs interfaces logique si non l'on peut connecter le routeur aux commutateurs via deux câbles, c'est-à-dire une interface qui sera dédiée aux Vlan 10 et une autre qui sera dédiée au vlan 20 et la on aura des ports en mode d'accès, mais c'est pas la configuration à privilégier.

La configuration de 1er interface pour vlan Donnée :

```
RT-Agence3(config)#interface fastEthernet 0/0
RT-Agence3(config-if)#no shutdown
RT-Agence3(config-if)#interface fastEthernet 0/0.1
RT-Agence3(config-subif)#encapsulation dot1Q 10
RT-Agence3(config-subif)#ip address 192.168.3.254 255.255.255.0
RT-Agence3(config-subif)#exit
RT-Agence3(config)#
```

Le chiffre 10 après dot1Q signifier le ID de Vlan « 10 Vlan donnée ».

La configuration de 2éme interface pour vlan Voip :

```
RT-Agence3(config)#interface fastEthernet 0/0.2
RT-Agence3(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

RT-Agence3(config-subif)#encapsualtion dot1Q 20
                                ^
% Invalid input detected at '^' marker.

RT-Agence3(config-subif)#encapsulation dot1Q 20
RT-Agence3(config-subif)#ip address 192.168.4.254 255.255.255.0
RT-Agence3(config-subif)#exit
```

Le chiffre 20 après dot1Q signifier le ID de Vlan « 20 Vlan Voip » .

I.4.2 Configurer le protocole DHCP :

Pour ne pas adresser les équipements un par un on va opter pour le protocole DHCP, Donc la faudrait crée deux Pool, crée une plage d'adresse « Pool » pour les équipements qui vont appartenir au Vlan 10, et une plage d'adresse « pool » pour les équipements qui vont appartenir au Vlan 20.

I.4.2.1 1er Pool « Donnée »:

```
RT-Agence3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Agence3(config)#ip dhcp pool Donnees
RT-Agence3(dhcp-config)#network 192.168.3.0 255.255.255.0
RT-Agence3(dhcp-config)#default-router 192.168.3.254
RT-Agence3(dhcp-config)#exit
RT-Agence3(config)#
```

I.4.2.2 2eme Pool « Voip »:

```
RT-Agence3(config)#ip dhcp pool Voip
RT-Agence3(dhcp-config)#network 192.168.4.0 255.255.255.0
RT-Agence3(dhcp-config)#default-router 192.168.4.254
RT-Agence3(dhcp-config)#
```

Pour le pool VoIP il faudra spécifier quel protocoles utilisé pour la Voip, qui sont identifier par des numéros par exemple ; SIP (Session Initiation Protocol) par le numéro 66, SCCP (Skinny Client Control Protocol) par le numéro 150 …, on utilise le protocole propriétaire de Cisco SCCP :

```
RT-Agence3(dhcp-config)#option ?
  <0-254>  DHCP option code
RT-Agence3(dhcp-config)#option 150 ip 192.168.4.254
RT-Agence3(dhcp-config)#exit
```

I.4.3 Configuration de commutateur :

Prochaine étape on va à configurer le switch :

I.4.3.1 Configure les interfaces:

Par défaut toute les interfaces appartient aux vlan 1, Pour notre cas on est besoin de séparer le trafique on va pas utiliser le Vlan 1, Donc on a fait en sort vlan 10 pour transporter les donnée brutes et on a fait en sort que vlan 20 transporte les paquet voix sur IP, on va configurer les équipements un par un :

```
Switch(config)#interface range fastEthernet 0/2-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport voice vlan 20
Switch(config-if-range)#exit
Switch(config)#
```

On configure l'interface fa0/1 qui relient le commutateur avec le routeur en mode agrégé « Trunk »

```
Switch(config)#interface range fastEthernet 0/1
Switch(config-if-range)#switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if-range)#
```

I.4.4 Activer adressage DHCP au niveau des équipements :

On va avoir une adresse de 1er vlan 10 :

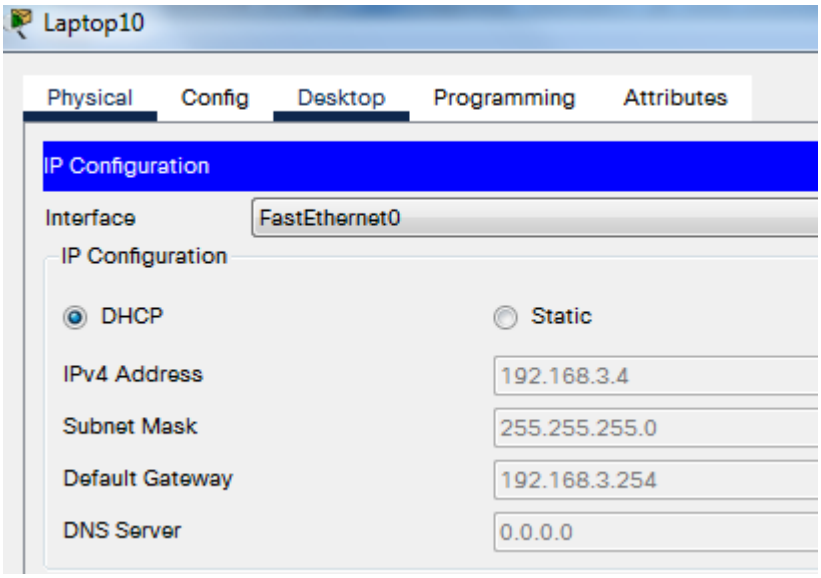


Figure I-5:la configuration de l'adressage DHCP au niveau de Laptop10.

I.4.5 Alimenter les téléphones IP :

Comme on voit sur la figure y on a des voyant rouges pare ce que les téléphones IP ne sont pas alimenter.

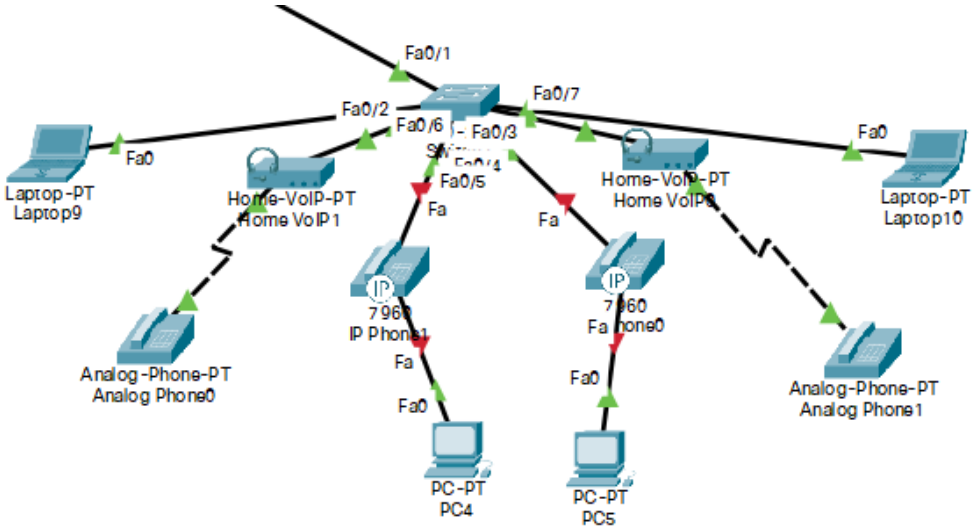


Figure I-6:Schéma de réseaux Voip avec IP phone éteint.

Il faut savoir que les téléphones IP possède la technologie POE « Power Over Internet » ne sont pas besoin d'une alimentation externe électrique, il peut fonctionnée simplement grâce aux câbles réseaux qui est dans notre cas relier aux commutateurs qui a lui aussi une fonctionne POE, Néanmoins dans packet tracer il faut ajouter une alimentation externe, il faudra les brancher manuellement, La dernier version de Cisco Packet Tracer 8.0.1 ne possède pas de cette fonctionnalité :

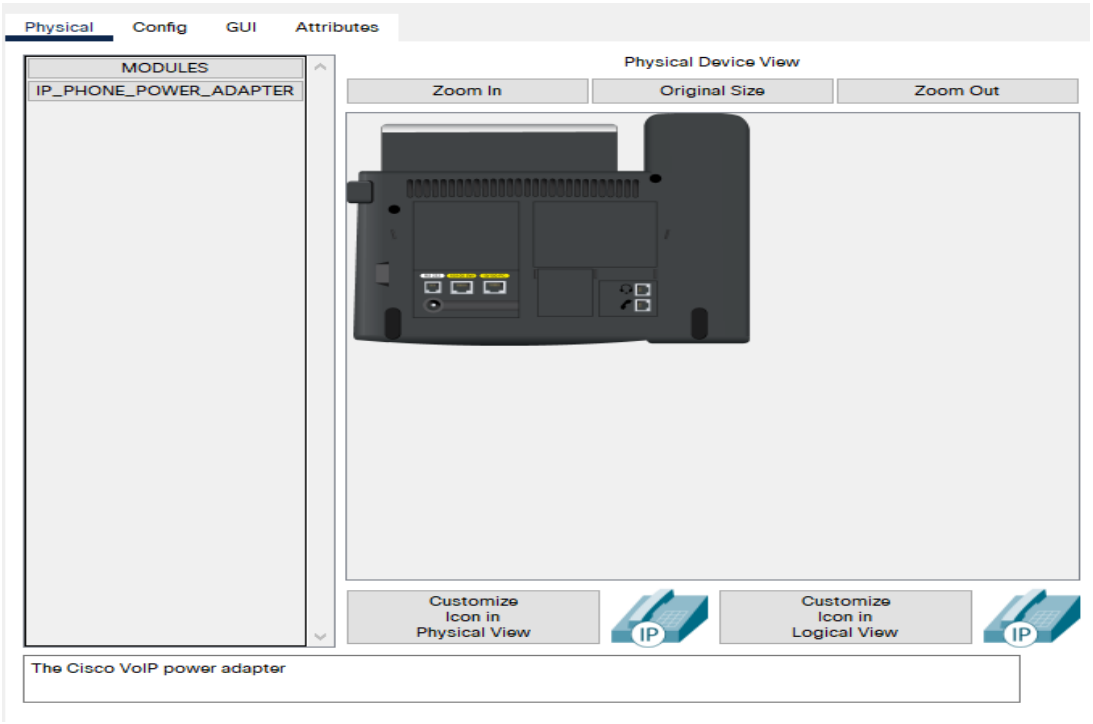


Figure I-7: Vue de l'appareil physique de téléphone IP avec Cisco Packet Tracer 8.0.1.

Pour cela on a utilisé l'ancienne version « Cisco Packet Tracer 7.3.1 » :

Alimenter IP Phone0:

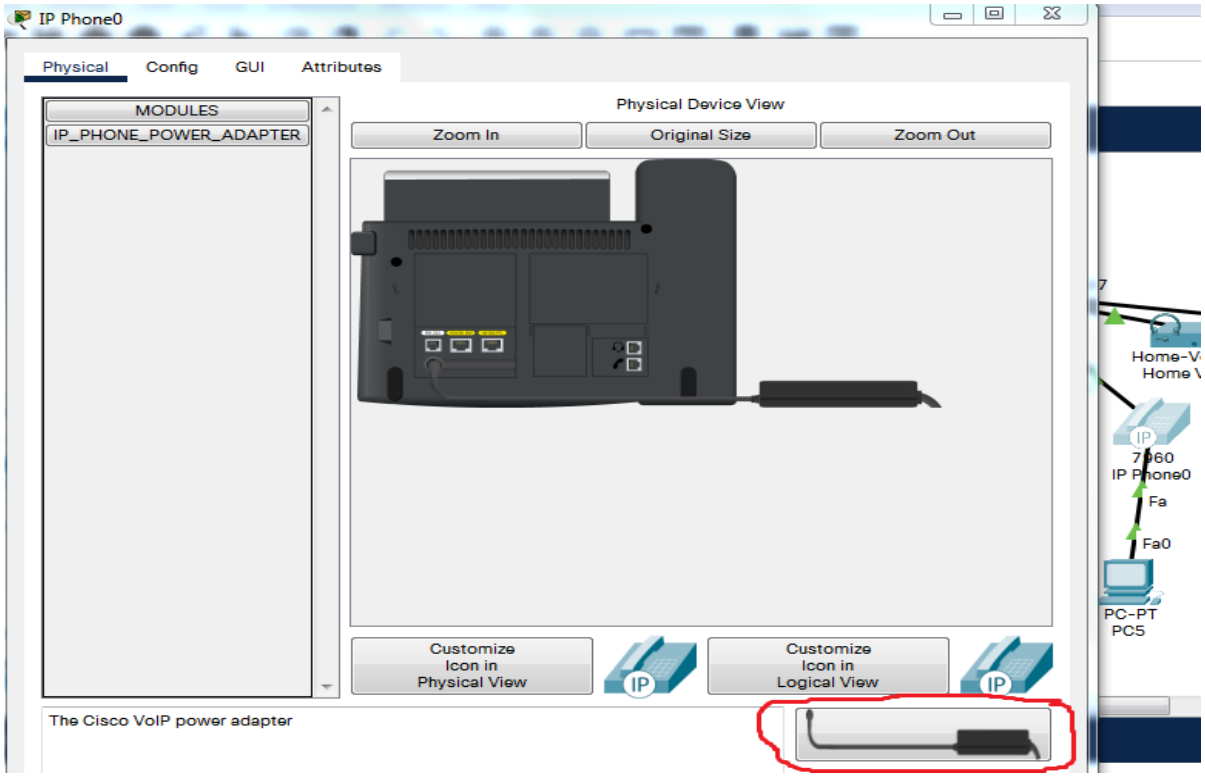
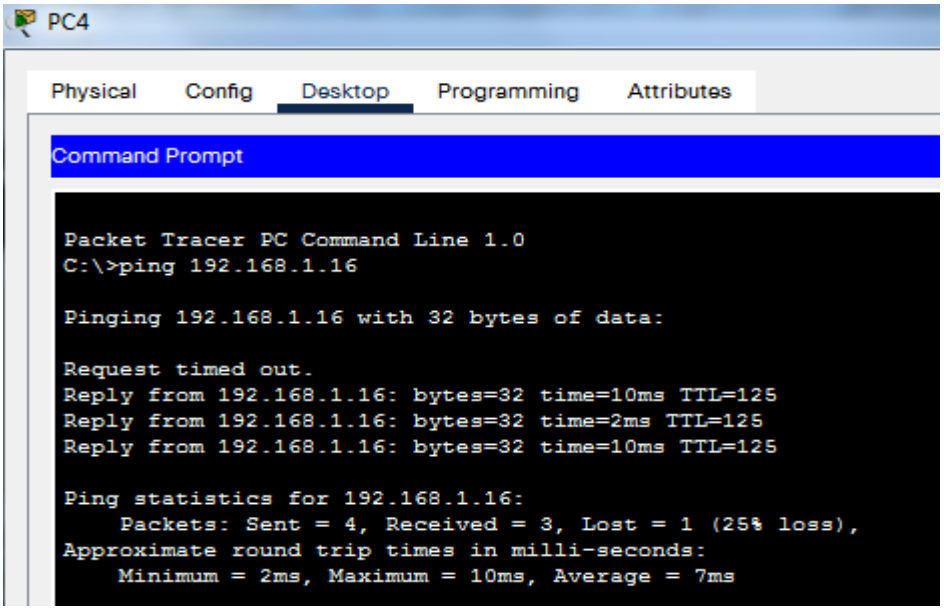


Figure I-8:Vue de l'appareil physique de téléphone IP avec Cisco Packet Tracer 7.3.1.

On fait la même chose au niveau de 2eme téléphone « IP phone 1 ».

I.4.6 Confirmer le routage et la connectivité de l'agence :

Pc4 de l'agence 3 ping PC0 de l'agence 1 :



Le ping a été effectuer donc en a une communication entre les agences.

I.4.7 La configuration des services de téléphonie :

On va accéder aux retour en mode de configuration terminal, Et on va passé a la configuration des services de téléphonie et pour cela on tape la commande *telephonie-service*« cette commande la marche uniquement sur les retours 2811 ».

```
RT-Agence3>en
RT-Agence3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Agence3(config)#telephony-service
RT-Agence3(config-telephony)#
```

On va spécifier des numéros de téléphones, On va définir le maximum des équipement téléphone IP et le maximum des numéros qu'on peut prendre en charge :

```
RT-Agence3(config)#telephony-service
RT-Agence3(config-telephony)#max-ephones 6
RT-Agence3(config-telephony)#max-dn 6
```

Saisir l'adresse de la passerelle au niveau de vlan voix sure IP et spécifier un port ce sera le port de TCP par défaut 2000, aussi on va faire en sorte d'ajouter au téléphone des numéros libre :

```
RT-Agence3(config-telephony)#ip source-address 192.168.4.254 po
RT-Agence3(config-telephony)#ip source-address 192.168.4.254 port 2000
RT-Agence3(config-telephony)#auto assign 1 to 6
RT-Agence3(config-telephony)#exit
```

I.4.7.1 Configurer les numéros de téléphones :

Définir pour chaque téléphone un numéro .

```
RT-Agence3(config)#ephone-dn 1
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state
to up

RT-Agence3(config-ephone-dn)#number 1001
RT-Agence3(config-ephone-dn)#
%IPPHONE-6-REGISTER: ephone-1 IP:192.168.4.1 Socket:2 DeviceType:Phone has registered.

RT-Agence3(config-ephone-dn)#ephone-dn 2
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state
to up

RT-Agence3(config-ephone-dn)#number 1002
RT-Agence3(config-ephone-dn)#ephone-dn 3
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state
to up

RT-Agence3(config-ephone-dn)#
%IPPHONE-6-REGISTER: ephone-2 IP:192.168.4.2 Socket:2 DeviceType:Phone has registered.
number 1003
RT-Agence3(config-ephone-dn)#ephone-dn 4
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state
to up

RT-Agence3(config-ephone-dn)#number 1004
RT-Agence3(config-ephone-dn)#ephone-dn 5
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state
to up

RT-Agence3(config-ephone-dn)#number 1005
RT-Agence3(config-ephone-dn)#ephone-dn 6
RT-Agence3(config-ephone-dn)#%LINK-3-UPDOWN: Interface ephone_dsp DN 6.1, changed state
to up

RT-Agence3(config-ephone-dn)#number 1006
RT-Agence3(config-ephone-dn)#EXIT
```

On va tester notre service de téléphonie :

On va accéder au téléphone IP pour vérifier que les équipements ont attribuée des numéro.

1001 pour IP phone 1:

Figure I-9:GUI IP Phone 1.

1002 pour IP Phone0 :

Figure I-10:GUI IP Phone 0..

Mais pour le téléphone analogique on n'a rien :

Figure I-11: GUI de Analog phone0 sans l'affichage de numéro.

Quand le téléphone n'est pas opérationnel il faut spécifier l'adresse de passerelle du vlan voix au niveau de convertisseur Home VoIP :

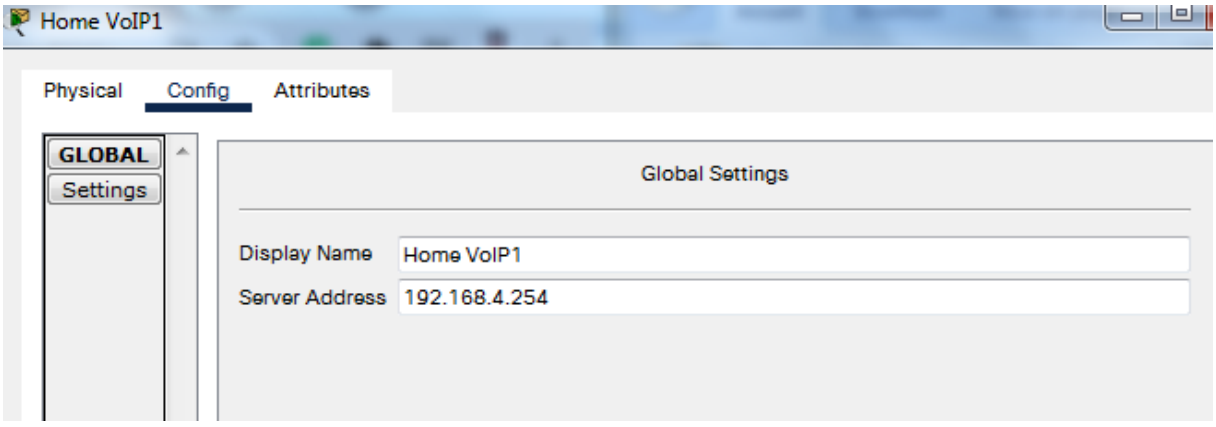


Figure I-12: configuration de passerelle de Home VoIP1.

Dès qu'on fait ça le téléphone analogique va recevoir un numéro :

Figure I-13: GUI Analog Phone0 avec l'affichage de numéro.

La même chose pour Analog Phone1 :

Figure I-14:L'affichage de numéro dans le GUI Analog Phone0.

I.4.7.2 Configuration les Pc :

On va faire en sorte que les pcs aussi puisse jouer le rôle de terminaux qui vont envoyer et recevoir des données voix, 1erment il faut les équiper ajouter un microphone et un casque :

Figure I-15:Vue de l'appareil physique de Laptop..

Pour pouvoir communiquer comme les téléphones IP on va utiliser Cisco IP Communicator « logiciel de téléphonie propriétaire de Cisco » qui permet d'utiliser l'ordinateur pour passer des appels vocaux et vidéo premium :

Figure I-16:Cisco IP Communicator.

On remarque que on a pas encore attribué de numéro de téléphone, parce que du moment que les téléphones ils sont connus pour être des équipements qui sont dédies a la téléphonie, donc on l'attribuer le Vlan 20 ce qu'on a spécifié au niveau des interfaces sur le commutateur *Switchport Voice Vlan 20* ,Mais les pc là c'est des terminaux qui sont généralement envoie des données différentes des données voix donc on l'attribuer des adresses du Vlan 10 comme on a vue dans la figure DHCP, Donc il faut faire des petit modification au niveau du Commutateur qui concerne les interfaces fa0/6 et fa0/7, elle vont pas appartenir au vlan 10 mais elle vont appartenir directement au Vlan 20 on va changer cela comme suit :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Dès que on fait ça on va resolliciter le DHCP qui nous attribue une adresse de deuxième vlan 20 :

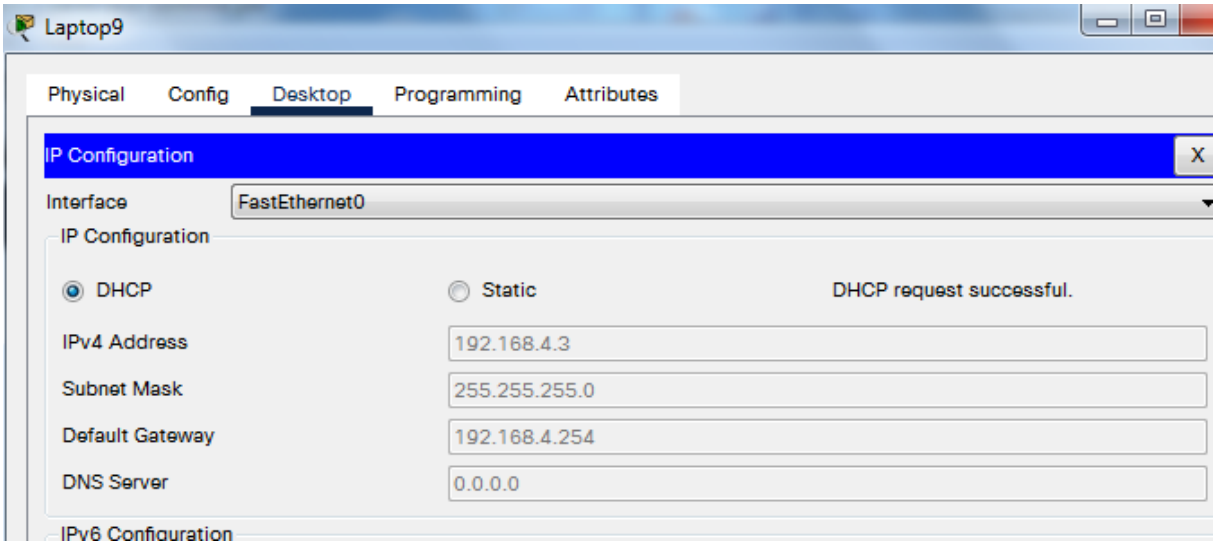


Figure I-17:Adressage DHCP de Laptop9.

On accède à l'utilitaire Cisco IP Communicator en remarque maintenant un numéro qui finalement attribué 1005 :

Figure I-18: Cisco IP Communicator de Laptop9 avec un numéro 1005 attribué.

I.4.8 Test la fonctionnalité de la Voip :

Laptop9 « 1005 » appellee Analog Phone1 « 1004 » :

Figure I-19:Laptop9 effectuer une appel ver le numéro 1004.

On voit « Figure I-20» qu'il indique Ring out donc ça sonne dans Analog Phone1 :

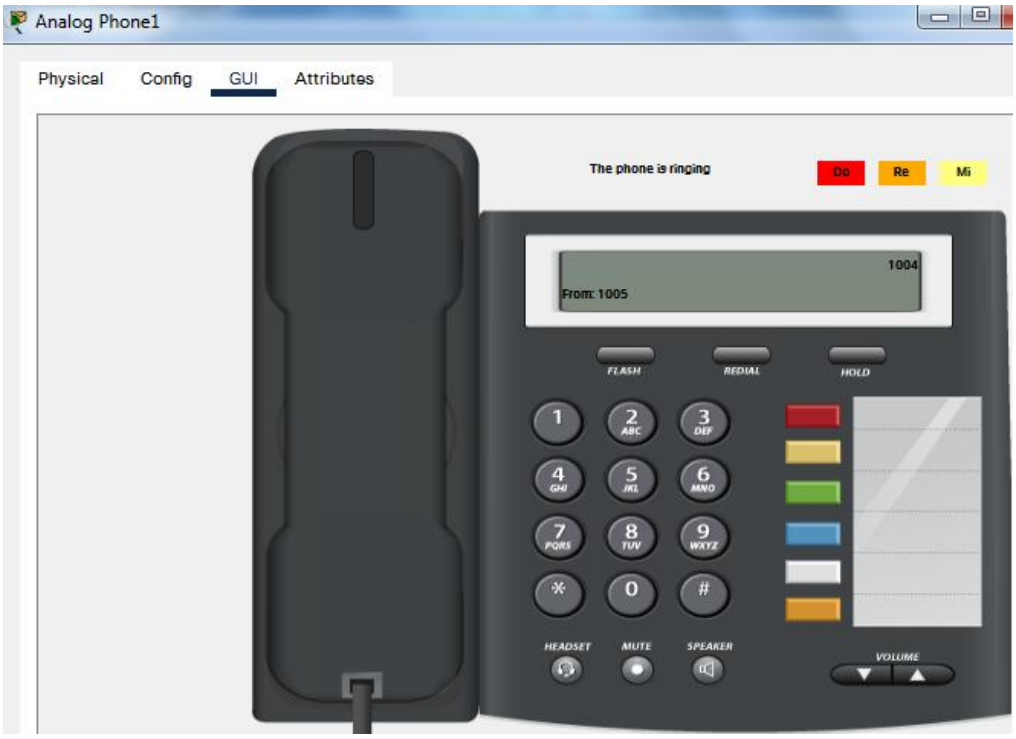


Figure I-21:Analog Phone1 récu une appel de 1005.

Dès qu'en décroche on a une connexion effectuer :

Figure I-22:Analog Phone1 en ligne avec Laptop9.

On fait la même chose pour l'agence 1, et pour permet la communication entre les deux agences on doit ajouter une petite configuration dans les routeurs des extrémités :

le homologues de la numérotation « dial-peer » :

(config)# dial-peer voice 1 voip

On va rentré dans le mode configuration de le homologue de numérotation :

Et on va spécifier les numéros de destination, par exemple on veut joindre l'agence3 :

(config-dial-peer) #destination-pattern 100.

Le point signifier la variable des numéros qu'il va changer

(config-dial-peer)#session target ipv4:«*adresse de déstination finale* »

LA 2ÉME ÉTAPE:

I.5 Mise en place des ACL sur les agences :

I.5.1 ZBF (Zone Based FireWall) :

Comme on déjà vue sur le chapitre 5 le fonctionnement des ACL et leur déférent types on a vue aussi sur (Détection et protection contre les menaces) l'utilisation des Class-map et l'exploitation des policiers et comment les intégré dans une *policy-map* ,Et comment englobe la *policy-map* dans une *service-policy* avant de se voir affectée à l'interface *outside* .

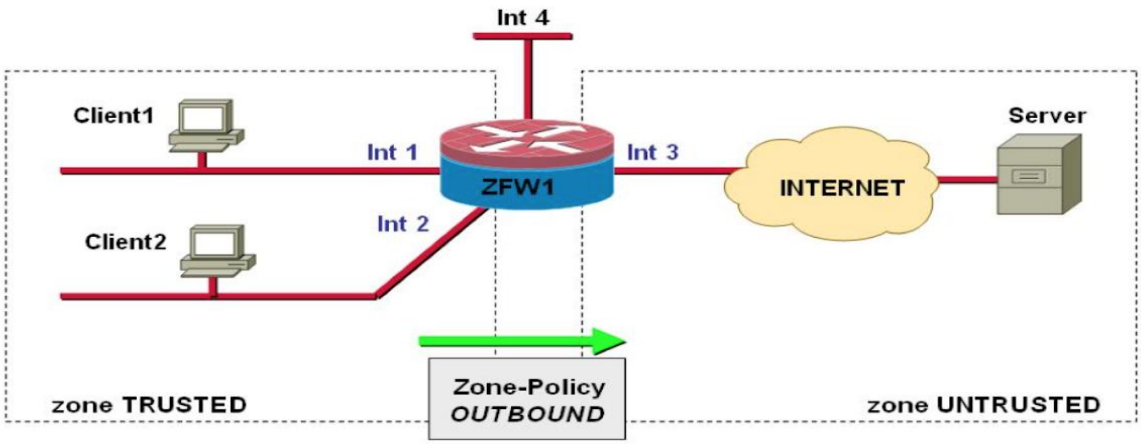


Figure 0-1: Cisco IOS et IOS-XE router as ZBFW.

De la même façon on verra avec les ZBF ou ZBPF (Zone Based Policy Firewalls) c'est une méthode développée à partir de l'ACL pour éviter la configuration de chaque interface.

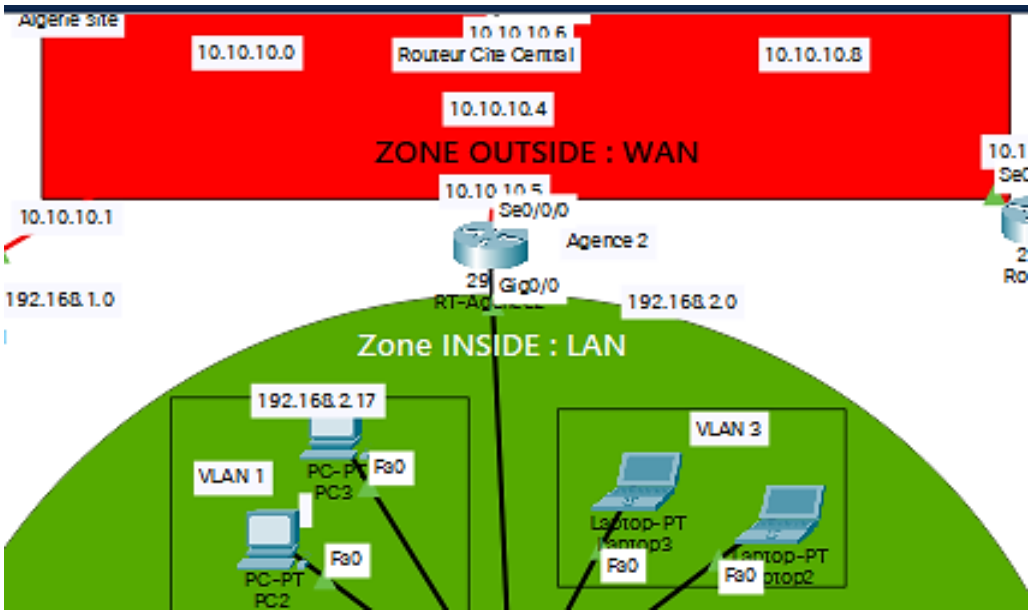


Figure 0-2:Schéma ZBF RT-Agence2 expliquant les zones inside outside pour les ZBF de notre réalisation .

I.5.1.1 Installer security technology package sur les routers :

Tout d'abord pour que le simulateur packet tracer permettre crée les ZBF (zone sécurisé) on doit activé une licence de sécurité, dans le console des routeurs on tape la commande suivante dans le mode configuration :

```
license boot module c2900 technology-package securityk9
```

```
RT-Agence1(config)#license boot module c2900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
%LICENSE-6-EULA_ACCEPTED: EULA for feature securityk9 1.0 has been accepted. UDI=CISCO2911/
K9:FTX1524XYI4-; StoreIndex=0:Evaluation License Storage

RT-Agence1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C2900 Next reboot
level = securityk9 and License = securityk9
```

Ensuit on va sauvegarder la modification effectué de running config vers le startup config par la commande *write* (ou n'importe quelle commande peut effectuer cette opération), Après on redémarrer le router par la commande reload.

Enfin on va confirmer l'activation avec la commande show version :

```
-------------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current       Type          Next reboot
-------------------------------------------------------------------
ipbase         ipbasek9      Permanent     ipbasek9
security       securityk9    Evaluation    securityk9
uc             disable       None          None
data           disable       None          None

Configuration register is 0x2102
```

Figure 0-3:Le résultat de la commande show version qu'il monte une licence de sécurité.

I.5.1.2 Création des ZBF :

On va créer les ZBF avec 5 étapes comme suit :

I.5.1.2.1 Définir les zones sécurisées avec n'importe quel nome logique :

On va prendre INSIDE pour la zone LAN et OUTSIDE pour la zone WAN

```
RT-Agence2(config)#zone security INSIDE
RT-Agence2(config-sec-zone)#zone security OUTSIDE
RT-Agence2(config-sec-zone)#
```

I.5.1.2.2 Classifier le trafic on utilisant Class-map :

On va créer deux Class-map et on 'va choisir le nome CLASS_MAP_IN_TO_OUT pour le trafic sortant et CLASS_MAP_OUT_TO_IN pour le trafic entrant. Ensuite on va matché le trafic soit directement avec le Protocol soit pour faciliter les choses comme dans notre cas on a utilisé les ACL dans le match et pour cela dans la 2éme partie on va créer deux ACL nommé comme suit **inside_access_in** pour le trafic intérieur et **outside_access_in** pour le trafic extérieur.

```
RT-Agence2(config)#Class-map type Inspect match-any CLASS_MAP_IN_TO_OUT
```

La *fonction Inspect est pour ZBF y'on a d'autres type pour d'autres utilité comme la QO…, par défaut class-map va créer une class map d'une classification match-all et si pour ça on a précisé la classification match-any (match-all : le AND logique / match-any : le OR logique)*

On utilisé la commande access-group pour matché les ACL.

```
match access-group name inside_access_in
```

La meme chose pour la class CLASS_MAP_OUT_TO_IN :

```
RT-Agence2(config)#class-map type inspect match-any CLASS_MAP_OUT_TO_IN
```

```
match access-group name outside_access_in
```

I.5.1.2.3 Definer la politique (Firewall policies) et les règles pour contrôler et classifier le trafics on utilisant Pollicy-maps :

On va crée deux policy-map nommé comme suit « **POLICY_MAP_IN_TO_OUT** » et « **POLICY_MAP_OUT_TO_IN** »

D'abord on va créer une policy-map **POLICY_MAP_IN_TO_OUT** :

```
RT-Agence2(config)#policy-map type inspect POLICY_MAP_IN_TO_OUT
```

Ensuite on donne la classe « **CLASS_MAP_IN_TO_OUT** » aux policie crée :

```
RT-Agence2(config-pmap)#class type inspect CLASS_MAP_IN_TO_OUT
```

On choisit l'action inspect pour la policier :

```
RT-Agence2(config-pmap-c)#inspect
```

Le trafic non classé sera matché avec «class-default » l'action par défaut « drop »

```
RT-Agence2(config-pmap-c)#class class-default
RT-Agence2(config-pmap-c)#drop
```

La meme chose pour POLICY_MAP_OUT_TO_IN :

```
RT-Agence2(config)#policy-map type inspect POLICY_MAP_OUT_TO_IN
RT-Agence2(config-pmap)#class type inspect CLASS_MAP_OUT_TO_IN
RT-Agence2(config-pmap-c)#inspect
RT-Agence2(config-pmap-c)#class class-default
RT-Agence2(config-pmap-c)#drop
```

I.5.1.2.4 Associez la zone et appliquez la politique de sécurité :

On utilise zone-pair pour définir la direction de la politique de sécurité par zone (zone source/destination).

D'abord on va créer une zone « ZONE_PAIR_IN_TO_OUT » et définir la zone « INSIDE » comme une zone source et « OUTSIDE » comme une zone destination :

```
RT-Agence2(config)#zone-pair security ZONE_PAIR_IN_TO_OUT source INSIDE destination OUTSIDE
```

Après on applique et on associer le policier a la zone pair :

R1(config-sec-zone-pair)#service-policy type inspect POLICY_MAP_IN_TO_OUT

La même chose pour la zone pair « ZONE_PAIR_OUT_TO_IN » :

RT-Agence2(config)#zone-pair security ZONE_PAIR_OUT_TO_IN source OUTSIDE destination INSIDE

R1(config-sec-zone-pair)#service-policy type inspect POLICY_MAP_OUT_TO_IN

I.5.1.2.5 Attaché les zones aux interfaces :

RT-Agence2(config-if)#zone-member security OUTSIDE

RT-Agence2(config-if)#zone-member security INSIDE

La zone peut avoir jusqu'à 7 interfaces, Par défaut le Traffic est refusé entre les 2 zones, Mais d'autre part par défaut tout le trafic est permit dans la zone elle-même (intra zone), Donc le trafic entre différent zone est Denay (refusé) par défaut.

Ps : L'ordre de ces étapes n'est pas obligatoire par exemple on peut remplacer l'étape (III.1.1.2.2) par (III.1.1.2.5).

I.5.1.3 Créer l'ACL suivante :

inside_access_in :

RT-Agence2(config)#ip access-list extended inside_access_in

outside_access_in :

RT-Agence2(config)#ip access-list extended outside_access_in

I.5.1.3.1 Lancer un test de Ping dans un pc de na porte qu'elle l'agence. Le résultat suivant :

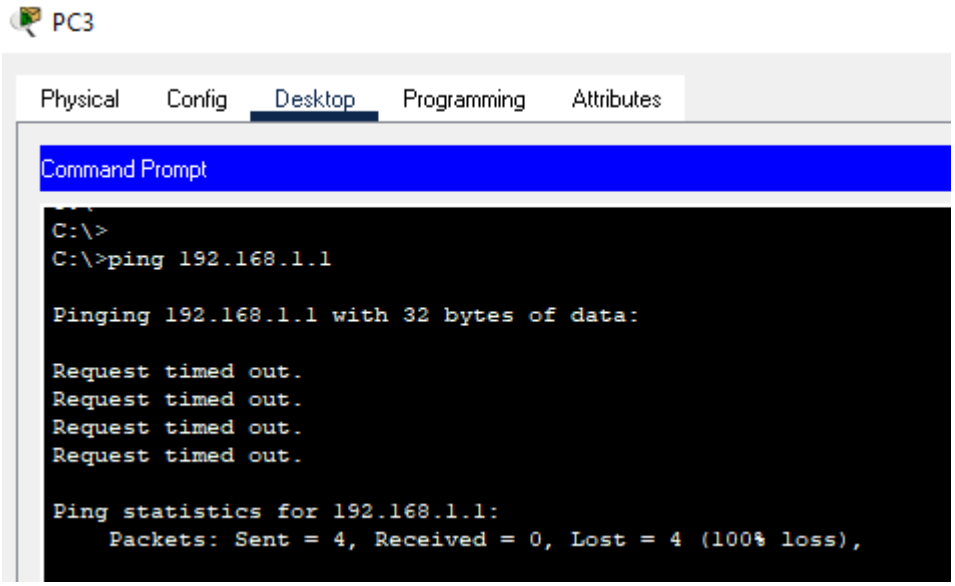


Figure 0-4: Ping échouer sur le CMD de PC3.

I.5.1.3.2 Appliquer une ACL qui permit la communication entre les clients de l'agence2 et l'agence1 :

ACL sur RT-Agence2 :

inside_access_in

RT-Agence1(config)#ip access-list extended inside_access_in

RT-Agence1(config-ext-nacl)#permit icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

RT-Agence1(config-ext-nacl)#permit udp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

outside_access_in

RT-Agence2(config)#ip access-list extended outside_access_in

RT-Agence2(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

RT-Agence2(config-ext-nacl)#permit udp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

ACL sur RT-Agence1 :

inside_access_in

RT-Agence1(config)#ip access-list extended inside_access_in

RT-Agence1(config-ext-nacl)#permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

RT-Agence1(config-ext-nacl)#permit udp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

outside_access_in

```
RT-Agence1(config)#ip access-list extended outside_access_in
RT-Agence1(config-ext-nacl)#permit icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
RT-Agence1(config-ext-nacl)#permit udp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

On ajoute permit icmp any any pour autoriser le Ping vers tous les réseau qu'il nous permet de tester les configuration suivants.

I.5.1.3.3 Lancer un test de Ping dans un pc de l'agence2 vers un pc de l'agence1 :

Le résultat est :

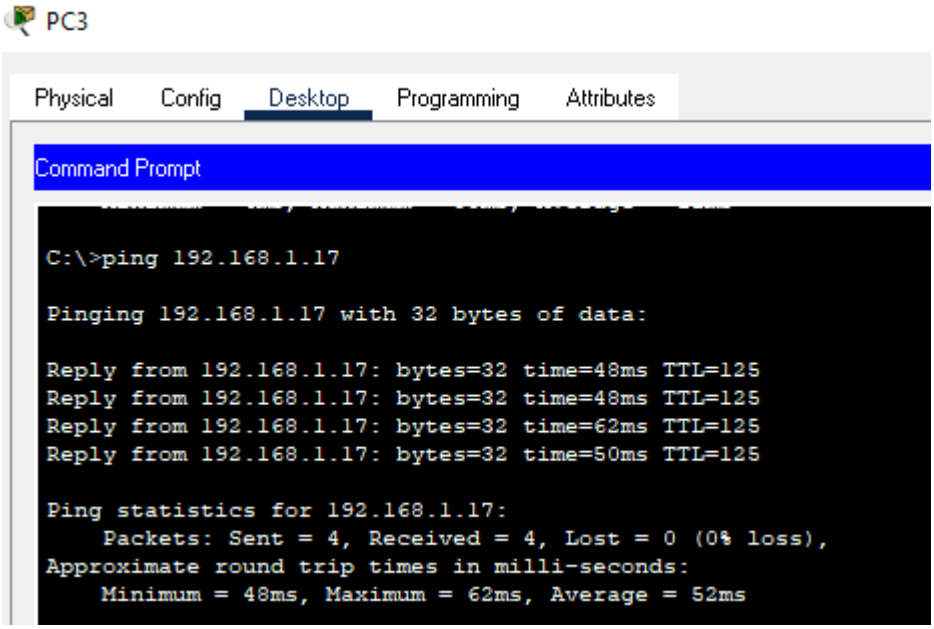


Figure 0-5: Ping effectuer sur le CMD de PC3.

I.5.1.3.4 Lancer un test de Ping de l'agence1 vers l'agence2. Le résultat est :

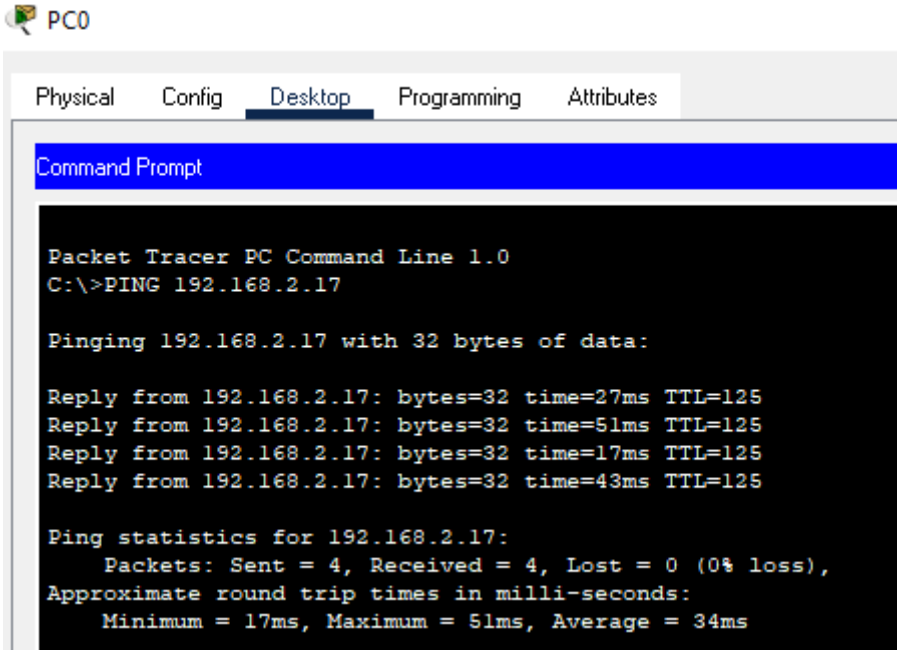


Figure 0-6:Ping effectuer sur le CMD de PC0.

CHAPITRE 7 : *Réalisation et Mise en place des solutions de sécurité*

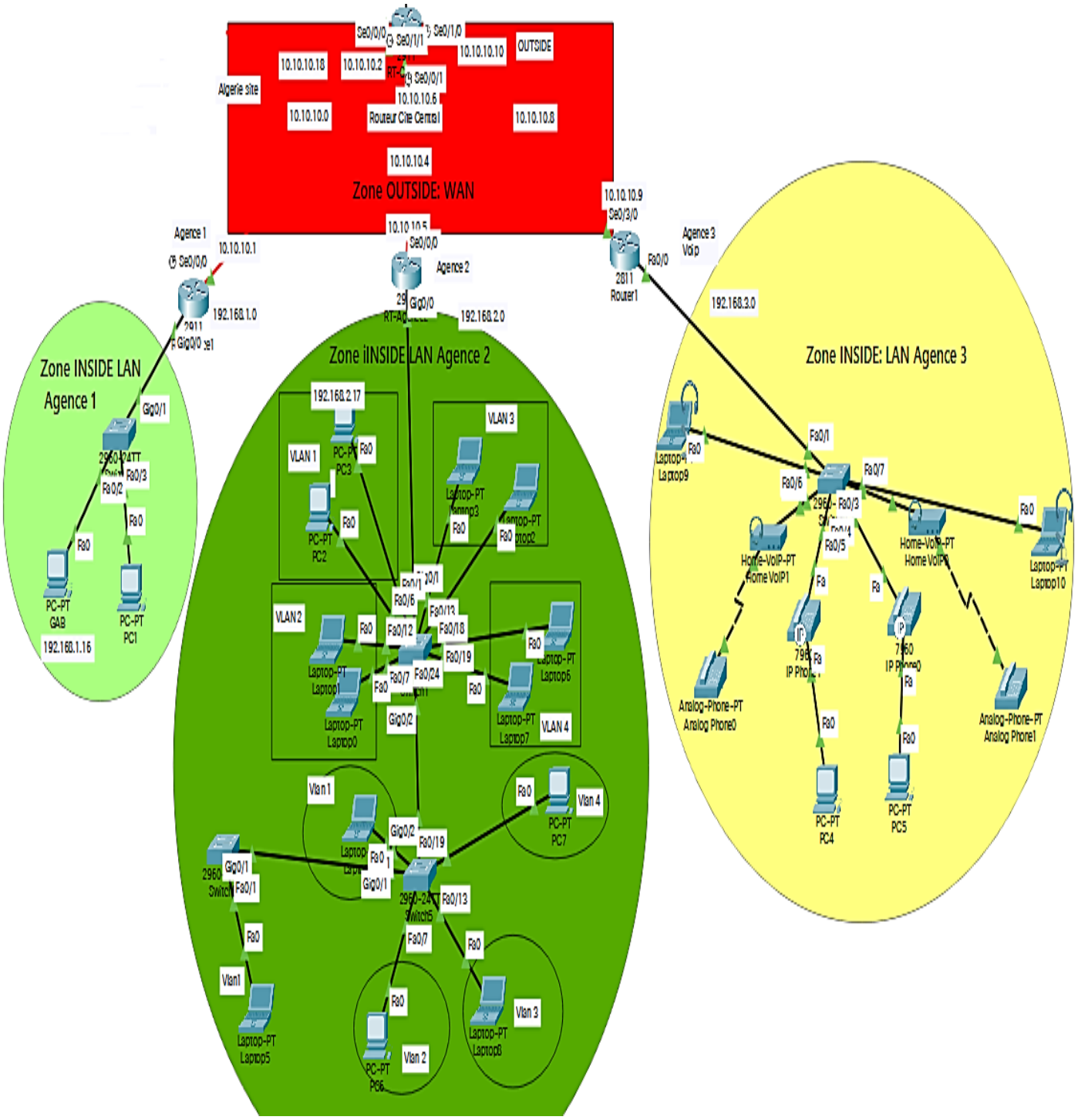


Figure 0-7:schema des ZBF.

I.6 Mise en place des ACL sur le Site central (ASA 5505) :

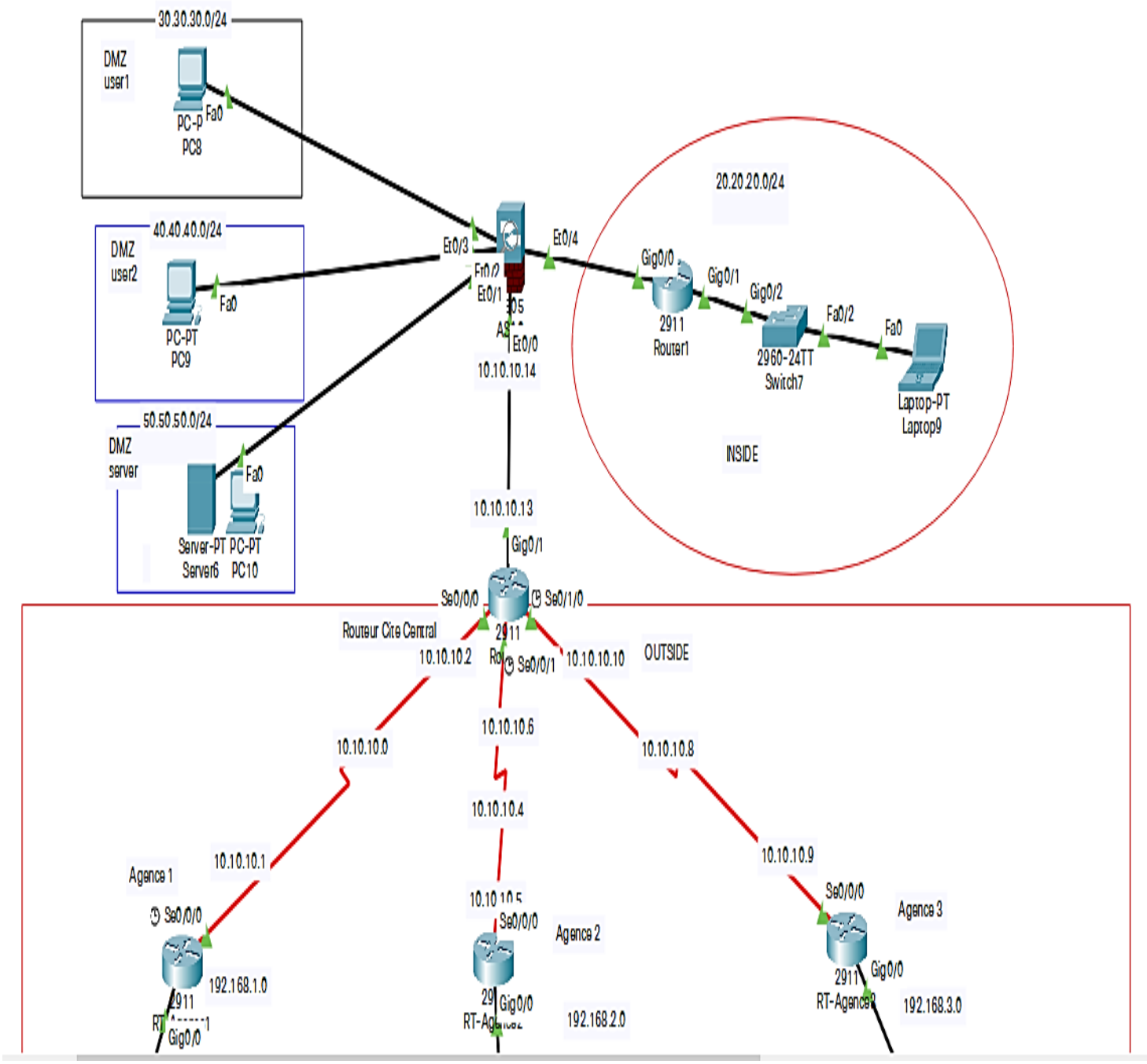


Figure 0-8:Schéma des ACLs.

I.6.1 Configuration d'ASA :

On a déjà vue dans le chapitre 05 sur le détail de fonctionnement de asa, La configuration de base et comment configurer le mode de fonctionnement, On utilise le mode Routed qui est par défaut et dans ce qui suit la configuration de base et la mise en place des ACL… basant sur ce qu'on étudier sur le chapitre 5, mais avant tout ça les Appliance ASA sont préinstallées avec soit :

- Une licence de base (Base Licence)
- Une licence Security Plus

Les licences peuvent être perpétuelles ou à durée limitée (time-based), Souvent, les licences à durée limitée sont utilisées pour des produits qui nécessitent un abonnement pour obtenir les mises à jour (Botnet Inspection par ex.), Pour voir les licences activées sur l'ASA, deux commandes permettent de vérifier :

ciscoasa#show activation-key

ciscoasa#show version

```
ciscoasa#show activation-key
Serial Number:  JMX153685WE-
Running Permanent Activation Key: 0x207765BB 0xD0BB16DA 0x2BC4AE1A 0x7ECEBD56 0x9A034781

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

Figure 0-9: Le résultat de la commande show activation-key.

Comme ce se voit on a une licence de base, pour obtenir une licence Security Plus :

- ✓ nous choisissons un key parmi ces deux :
- ✓ activation-key 0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D
- ✓ activation-key 682fd277 c4874bb7 f533b52c c660c844 8422d892

Confirmer la configuration en tapant la commande (show activation-key /show version) :

Le résultat:

```
ASA-BEA#show activation-key
Serial Number:  JMX1536UI7B-
Running Permanent Activation Key: 0x0X1321CF 0x730XFCB6 0x8F7E0X80 0x1111DC0X 0xB554E4A4
0x0X0F3E00

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 20             DMZ Unrestricted
Dual ISPs                         : Enabled        perpetual
VLAN Trunk Ports                  : 8              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Active/Standby perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has an ASA 5505 Security Plus license.

The flash permanent activation key is the SAME as the running permanent key.
ASA-BEA#
```

Figure 0-10: Le résultat de la commande show activation-key après effectuer une licence Security Plus.

I.6.1.1 Créer les VLANs :

Par défaut l'ASA ne fonctionne pas avec les ACL il fonctionne avec les niveaux des sécurité : en général d'habitude en donne **outside**=0 **inside**=100 **dmz**=50, Le Trafic est refusé de passé de niveau bas vers un niveau supérieur comme ça se voit sur la figure :

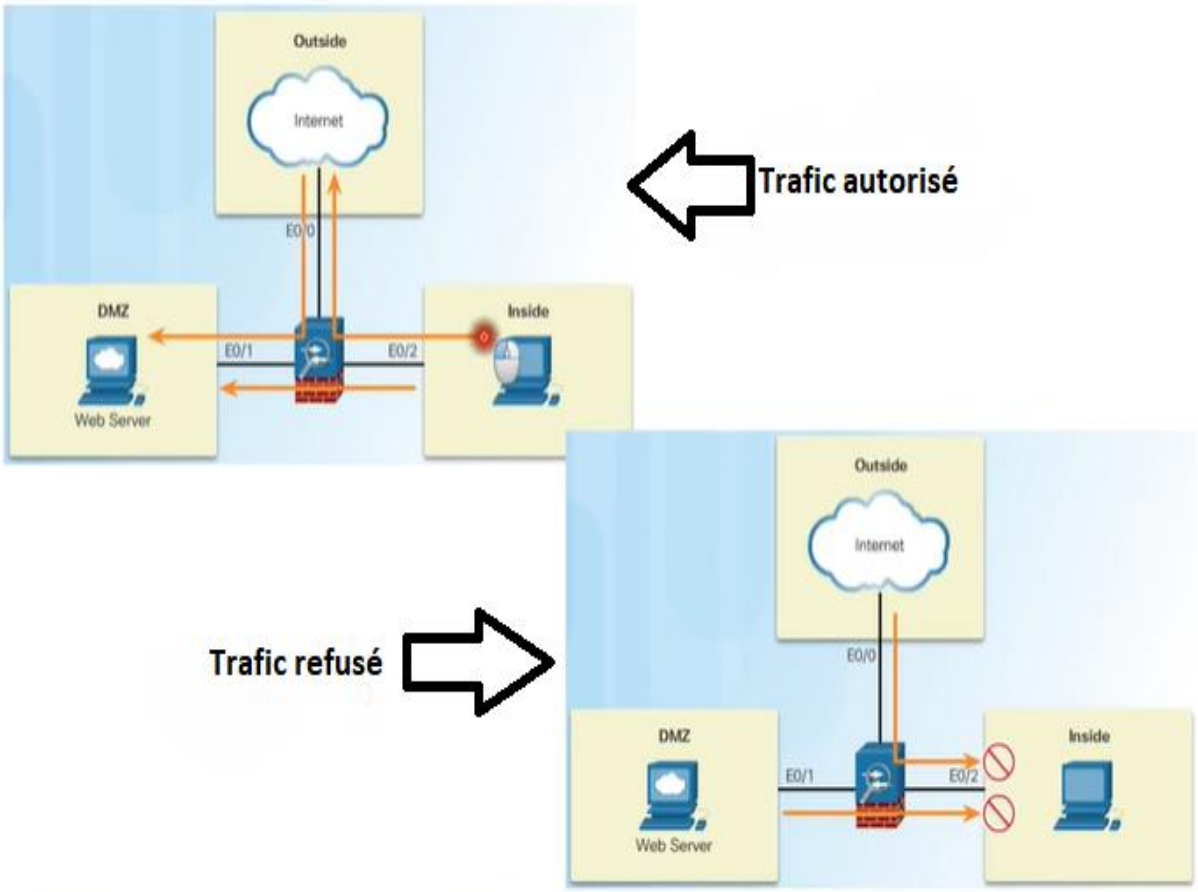


Figure 0-11: Les trafics refusé et autorisé pour les niveaux des sécurité de ASA.

Pour cela on va préciser d'abord les niveaux de sécurité par des vlan comme suit :

Vlan 1 : pour la zone inside avec un niveau de sécurité = 100.

```
ASA-BEA#conf t
ASA-BEA(config)#interface vlan 1
ASA-BEA(config-if)#ip address 20.20.20.1 255.255.255.0
ASA-BEA(config-if)#no shutdown
ASA-BEA(config-if)#nameif inside
ASA-BEA(config-if)#security-level 100
ASA-BEA(config-if)#copy r s
% Ambiguous command: "copy r s"
ASA-BEA#copy r s
% Ambiguous command: "copy r s"
ASA-BEA#write memory
Building configuration...
Cryptochecksum: 23d41bbb 652a12f0 57d152e5 60a13568

1528  bytes copied in 2.043 secs (747 bytes/sec)
[OK]
ASA-BEA#
```

Vlan 2 : pour la zone outside avec un niveau de sécurité = 0.

```
ASA-BEA(config)#interface vlan 2
ASA-BEA(config-if)#ip address 10.10.10.14 255.255.255.252
ASA-BEA(config-if)#no shutdown
ASA-BEA(config-if)#nameif outside
ASA-BEA(config-if)#security-level 0
ASA-BEA(config-if)#write memory
Building configuration...
Cryptochecksum: 23d41bbb 652a12f0 57d152e5 60a13568

1553  bytes copied in 2.007 secs (773 bytes/sec)
[OK]
ASA-BEA(config-if)#
```

Vlan 3 : pour la zone dmz1 avec un niveau de sécurité 50 .

```
ASA-BEA(config)#interface vlan 3
ASA-BEA(config-if)#ip address 30.30.30.1 255.255.255.0
ASA-BEA(config-if)#no shutdown
ASA-BEA(config-if)#nameif dmz1
ASA-BEA(config-if)#security-level 50
ASA-BEA(config-if)#write memory
Building configuration...
Cryptochecksum: 23d41bbb 652a12f0 57d152e5 60a13568

1553  bytes copied in 1.019 secs (1524 bytes/sec)
[OK]
```

Vlan 4 : pour la zone dmz2 avec un niveau de sécurité 50.

```
ASA-BEA(config)#interface Vlan4
ASA-BEA(config-if)#ip address 40.40.40.1 255.255.255.0
ASA-BEA(config-if)#no shutdown
ASA-BEA(config-if)#nameif dmz2
ASA-BEA(config-if)#security-level 50
ASA-BEA(config-if)#write memory
Building configuration...
Cryptochecksum: 23d41bbb 652a12f0 57d152e5 60a13568

1553  bytes copied in 1.95 secs (796 bytes/sec)
[OK]
```

Vlan 5 : pour la zone dmz3 avec un niveau de sécurité 50.

```
ASA-BEA(config-if)#exit
ASA-BEA(config)#interface Vlan5
ASA-BEA(config-if)#ip address 50.50.50.1 255.255.255.0
ASA-BEA(config-if)#no shutdown
ASA-BEA(config-if)#nameif dmz3
ASA-BEA(config-if)#security-level 50
ASA-BEA(config-if)#write memory
Building configuration...
Cryptochecksum: 23d41bbb 652a12f0 57d152e5 60a13568

1553  bytes copied in 1.222 secs (1270 bytes/sec)
[OK]
```

Confirmer la configuration on tapent la commands (show running-config / show interface ip brief) :

show running-config :

```
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 20.20.20.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.10.10.14 255.255.255.25
!
interface Vlan3
 nameif dmz1
 security-level 50
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan4
 nameif dmz2
 security-level 50
 ip address 40.40.40.1 255.255.255.0
!
interface Vlan5
 nameif dmz3
 security-level 50
 ip address 50.50.50.1 255.255.255.0
!
```

Figure 0-12: une partie de running-config affiché par la commande show running-config.

Show interface ip brief :

```
ASA-BEA#show int ip brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  up                    up
Ethernet0/1            unassigned      YES NVRAM  up                    up
Ethernet0/2            unassigned      YES NVRAM  up                    up
Ethernet0/3            unassigned      YES NVRAM  up                    up
Ethernet0/4            unassigned      YES NVRAM  up                    up
Ethernet0/5            unassigned      YES NVRAM  down                  down
Ethernet0/6            unassigned      YES NVRAM  down                  down
Ethernet0/7            unassigned      YES NVRAM  down                  down
Vlan1                  20.20.20.1      YES manual up                    up
Vlan2                  10.10.10.14     YES manual up                    up
Vlan3                  30.30.30.1      YES manual up                    up
Vlan4                  40.40.40.1      YES manual up                    up
Vlan5                  50.50.50.1      YES manual up                    up
```

Figure 0-13: le résultat de la commande Show interface ip brief.

I.6.1.2 Associer les vlan (zone) avec les interfaces de pare feu :

- Vlan 1 (inside) avec l'interface ethernet 0/4 :

```
ASA-BEA(config)#interface ethernet 0/4
ASA-BEA(config-if)#switchport access vlan 1
```

- Vlan 2 (outside) avec l'interface ethernet 0/0 :

```
ASA-BEA(config)#interface Ethernet0/0
ASA-BEA(config-if)#switchport access vlan 2
```

- Vlan 3 (dmz1) avec l'interface ethernet 0/3 :

```
ASA-BEA(config)#interface Ethernet0/3
ASA-BEA(config-if)#switchport access vlan 3
```

- Vlan 4 (dmz2) avec l'interface ethernet 0/2 :

```
ASA-BEA(config)#interface Ethernet0/2
ASA-BEA(config-if)# switchport access vlan 4
```

- Vlan 5 (dmz3) avec l'interface ethernet 0/1 :

```
ASA-BEA(config)#interface Ethernet0/1
ASA-BEA(config-if)# switchport access vlan 5
```

Confirmer la configuration en tapant la commande (show siwtch vlan) :

```
ASA-BEA#show switch vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    inside                              up        Et0/4, Et0/5, Et0/6, Et0/7
2    outside                             up        Et0/0
3    dmz1                                up        Et0/3
4    dmz2                                up        Et0/2
5    dmz3                                up        Et0/1
ASA-BEA#
```

I.6.2 Verifier la connectivité :

Comme on a vue sure la figure « Figure 0-14 » le pare feu ASA n'autorise que le trafic de niveau supérieur vers le niveau bas et n'autorise pas le trafic de passé de niveau bas vers un niveau supérieur :

On lance un ping de laptop de la zone inside vers un pc 09 de la zone dmz2 :

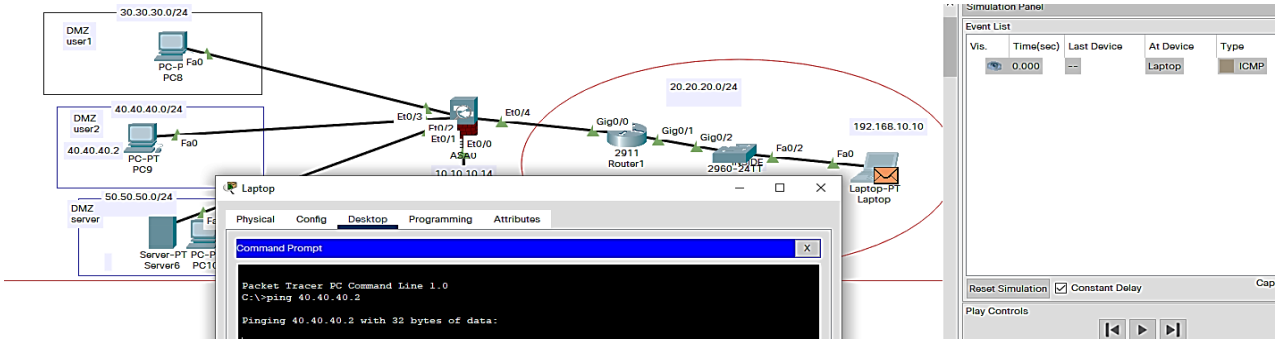


Figure 0-14:Mode simulation, le paquet ICMP aux niveaux de laptop.

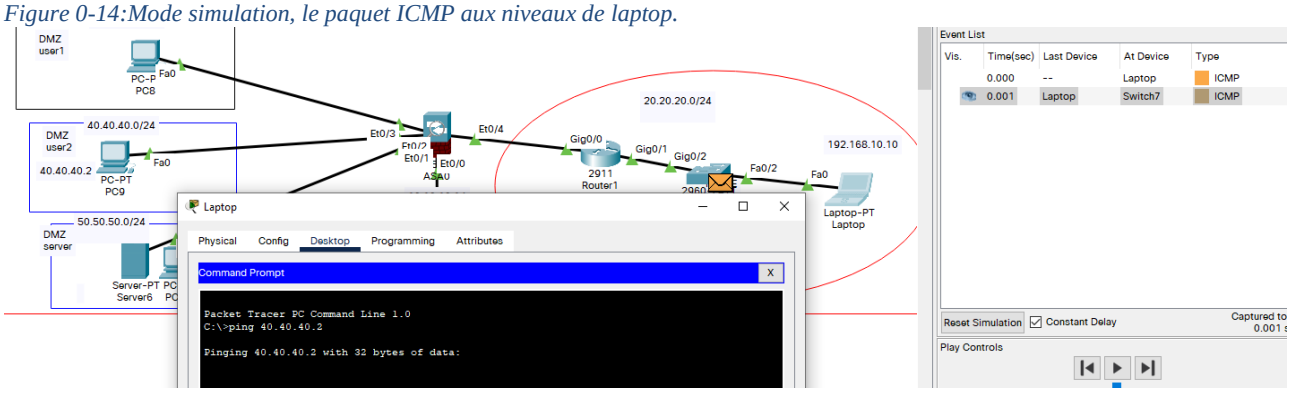


Figure 0-15:Mode simulation, le paquet ICMP aux niveaux de de switch..

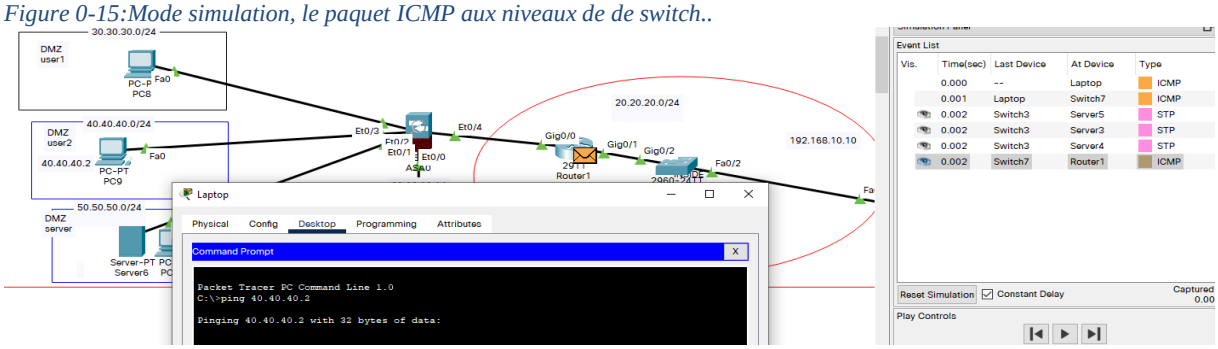


Figure 0-16:Mode simulation, le paquet ICMP aux niveaux de routeur.

On voit que le pare feu ne bloque pas le paquet ICMP :

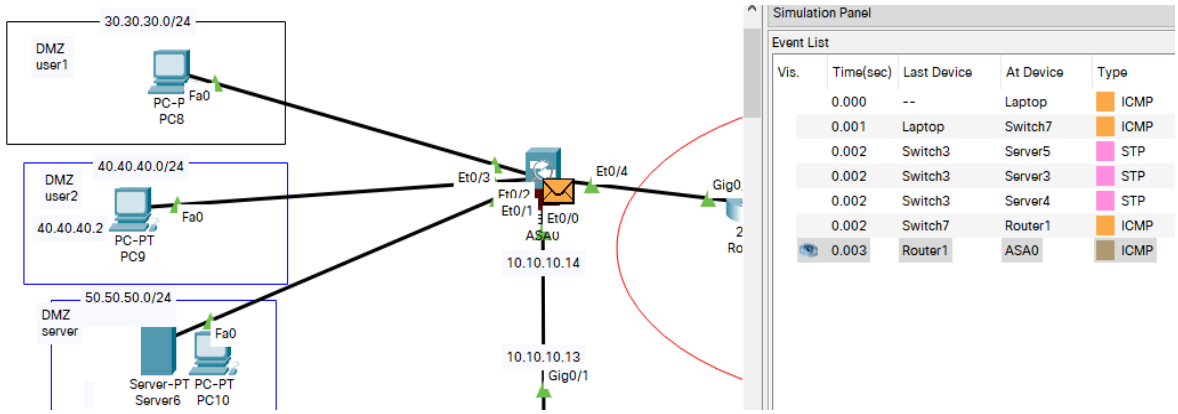


Figure 0-17: Mode simulation, le paquet ICMP aux niveaux de pare-feu ASA.

Le paquet Icmp arrive a la déstination sans aucun problem :

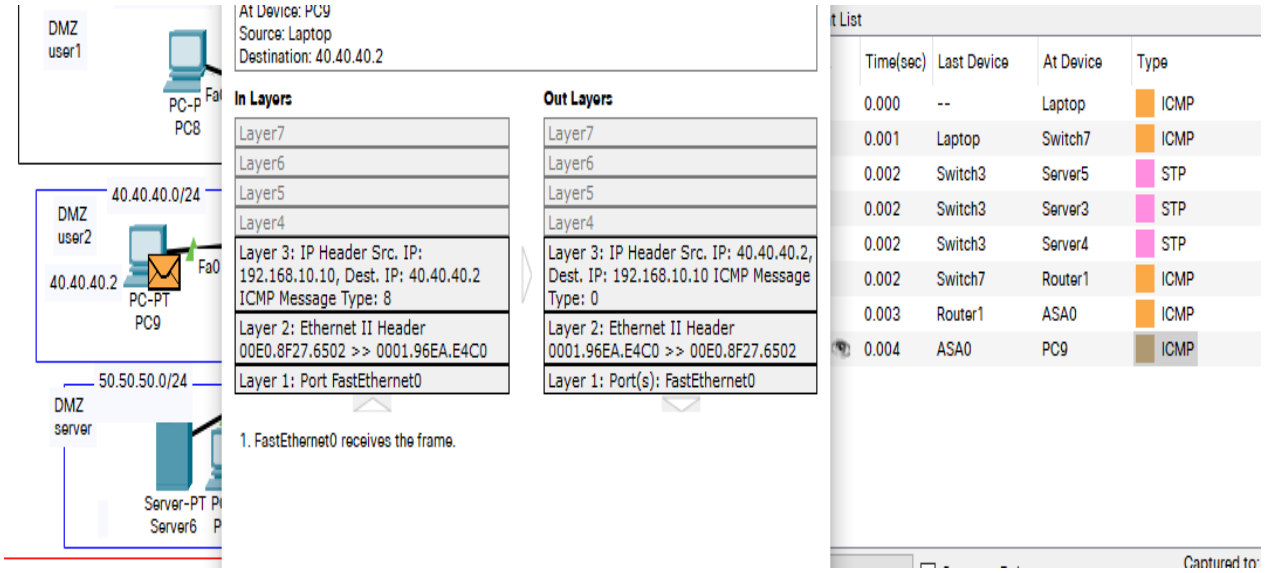


Figure 0-18:Mode simulation, et des informations de PDU ICMP aux niveaux de destination PC9.

Mais par contre ASA bloque le paquet ICMP écho de passée d'une source de niveaux inferieur « zone dmz2 » vers une destination d'un niveaux supérieur « zone inside » :

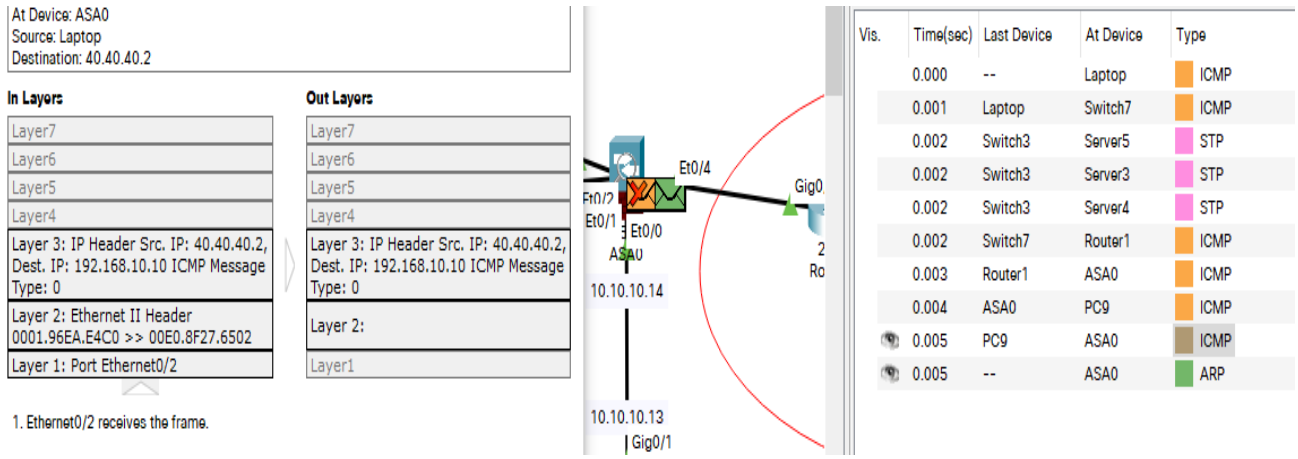


Figure 0-19:Mode simulation, le paquet ICMP écho est dropé aux niveaux de Pare-feu ASA.

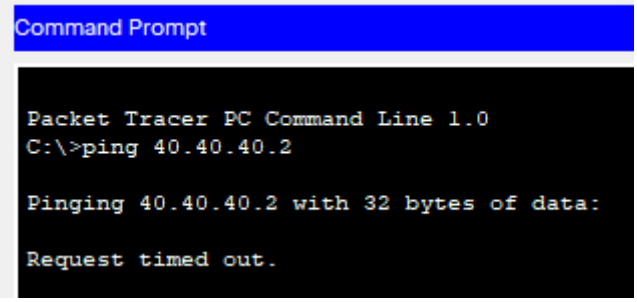


Figure 0-20:CMD de laptop, Le ping ver PC9 est échoué.

PS : Il est courant que le 1er Ping soit expiré si la résolution d'adresse (ARP, ND « ipv6 ») doit être effectuée avant envoyer la demande d'écho ICMP.

I.6.2.1 Créer les ACL suivantes sur ASA :

ASA Chèque d'abord l'ACL après il voit les niveaux de sécurité, Pour préciser certain flow « Par : Protocol, port, adresse … » de passer d'un niveau bas a un haut niveau en doit créer et configurer une liste de contrôle d'accès.

L'ACL « inside-access-in » pour le trafic d'entrée de la zone inside :

```
ASA-BEA(config)#access-list inside-access-in extended permit icmp any any
ASA-BEA(config)#access-group inside-access-in in interface inside
```

L'ACL« outside-access-in » pour le trafic d'entrée de la zone outside :

```
ASA-BEA(config)#access-list outside-access-in extended permit icmp any any
ASA-BEA(config)#access-group outside-access-in in interface outside
```

L'ACL « dmz1-access-in » pour le trafic d'entrée de la zone dmz1 :

```
ASA-BEA(config)#access-list dmz1-access-in extended permit icmp any any
ASA-BEA(config)#access-group dmz1-access-in in interface dmz1
```

L'ACL « dmz2-access-in » pour le trafic d'entrée de la zone dmz2 :

```
ASA-BEA(config)#access-list dmz2-access-in extended permit icmp any any
ASA-BEA(config)#access-group dmz2-access-in in interface dmz2
```

L'ACL « dmz3-access-in » pour le trafic d'entrée de la zone dmz3 :

```
ASA-BEA(config)#access-list dmz3-access-in extended permit icmp any any
ASA-BEA(config)#access-group dmz3-access-in in interface dmz3
```

I.6.2.1.1 Lancer le test de *ping* :

Le résultat est :

Router-Inside ping PC-DMZ1 :

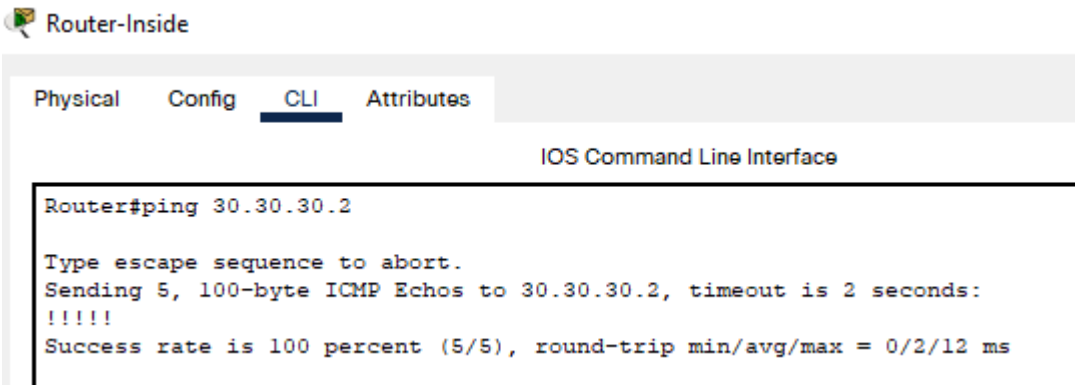


Figure 0-21: CLI de routeur de zone inside, ping effectuer avec souci ver PC-DMZ1.

Donc le trafic est autorisé entre les différentes zones.

I.6.3 Configuration du service NAT pour le pare-feu :

Avant de commencer la configuration du service NAT, On doit identifier des Route Statique et dynamique pour que les agences peuvent communique avec le site central(DMZ,INSIDE) :

I.6.3.1 Routage :

Dans ce qui suit la configuration d'une route statique et test de la connectivité avec un ping :

```
RT-Central#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Central(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.14
RT-Central(config)#do ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!.!..
Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/1 ms
```

On a déjà configuré une route dynamique OSPF :

```
!
router ospf 2
 log-adjacency-changes
 network 10.10.10.8 0.0.0.3 area 0
 network 10.10.10.4 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.3 area 0
 network 10.10.10.12 0.0.0.3 area 0
!
```

Pour que le trafic passe de Site central ver le grand réseau outside (les agences), on doit préciser une route de sortie sur notre pare-feu (route statique) :

```
ASA-BEA#conf t
ASA-BEA(config)#route outside 0.0.0.0 0.0.0.0 10.10.10.13 1
ASA-BEA(config)#
```

10.10.10.13 c'est l'adresse de la passerelle et 1 c'est la distance administrative.

I.6.3.2 Configuration du NAT:

Pour la configuration du service NAT (Network Address Translation) pour le pare-feu, nous avons deux cas :

1er cas : l'intérieur du réseau Nous allons créer la règle NAT pour que le réseau INSIDE puisse accéder au réseau OUTSIDE, pour ce faire nous allons préciser l'adresse de NAT ainsi que l'adresse de sortie de façon dynamique et ceci dans la configuration qui suit :

```
ASA-BEA(config)#object network bea-trans
ASA-BEA(config-network-object)#subnet 20.20.20.0 255.255.255.0
ASA-BEA(config-network-object)#nat (inside, outside) dynamic interface
```

On test le fonctionnement de NAT par la simulation d'un paquet ping (Router-Inside ver le RT-Central) illustré dans la « Figure 0-22 » :

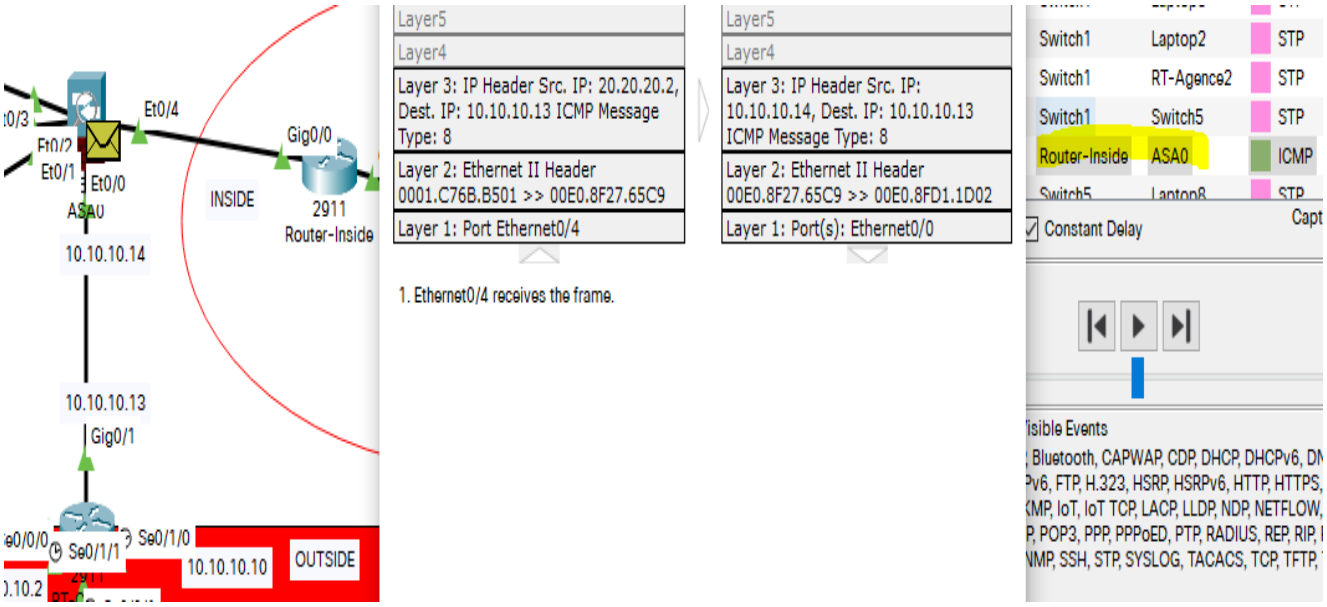


Figure 0-23:Simulation d'un ping routeur-inside ver le routeur central) en détail sous packet tracer.

On voit que dans le paquet d'entré qui est arrivé de Router-inside l'adresse source est tel du routeur inside 20.20.20.2 , mais dans le paquet de sortie qu'il va sortie de ASA, NAT a changé l'adresse source ver 10.10.10.14 .

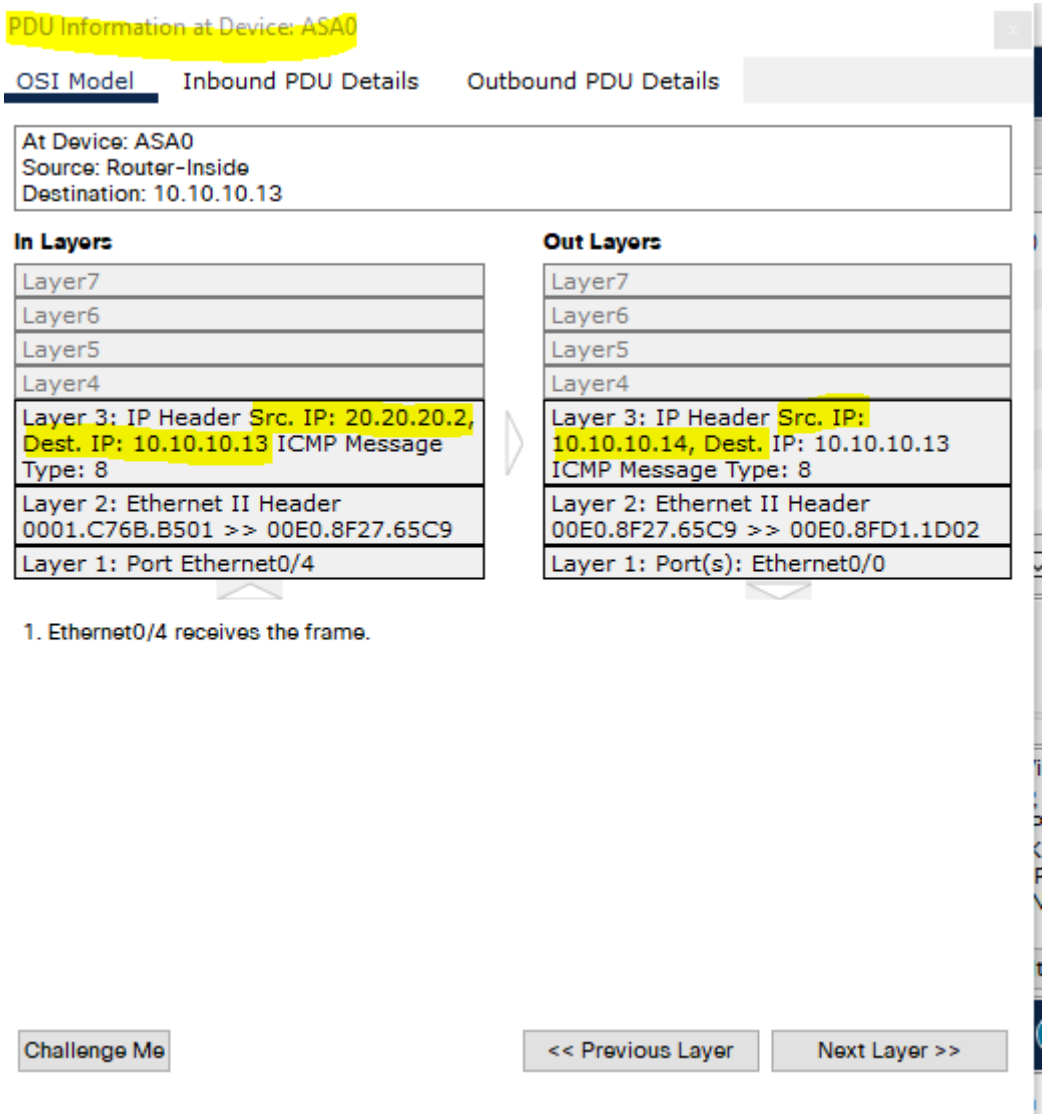


Figure 0-24: Les informations de PDU sous ASA.

II. Création d'un tunnel VPN IPsec:

Une entreprise peut avoir besoin d'une connexion WAN entre deux sites. Dans certains cas (liaison de secours ou liaison WAN pas cher) nous pouvons utiliser un tunnel IPSEC. IPSEC est une technologie VPN qui fonctionne au sein de la couche réseau comme on a vue sur les chapitres précédents « chapitres 3 » et dans les mesures de sécurité « chapitre 2 », IPSEC est un « framework » qui spécifie plusieurs protocoles à utiliser afin de fournir un standard de sécurité, Les protocoles spécifiés par IPSEC Comme on a déjà dédié en détails dans le chapitre 3 sont : IKE,ESP,AH.

Dans la BEA nous avons deux sites on prend le SITE1 GAB « Guichet Automatique Bancaire » sur Agence 1 en Algérie, Et SITE2 Server-visa en Tunisie :

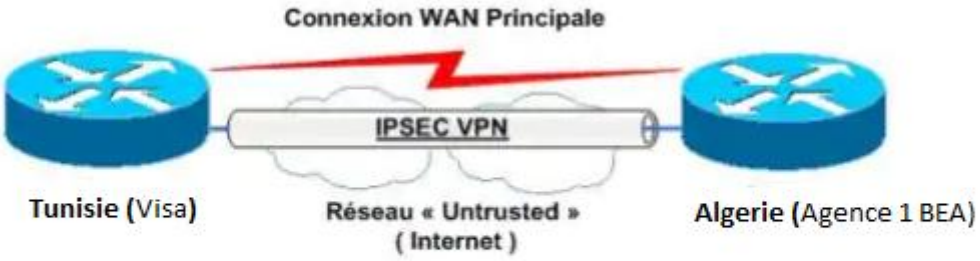


Figure II-1: Paire VPN (Algérie, Tunisie)

Nous avons déjà maitre en place des routeurs et les à configurer pour la connexion WAN qui fonctionne entre les deux sites.

II.1 Vérifier la connectivité entre les deux sites (sans VPN) :

GAB ping Server-visa :

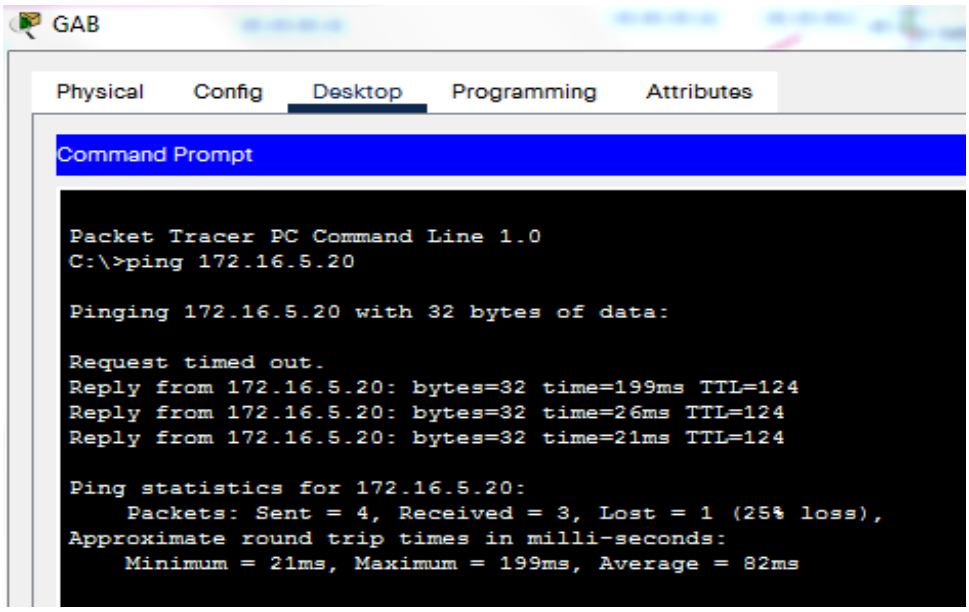


Figure II-2: CMD de GAB ping effectuer ver le server-visa.

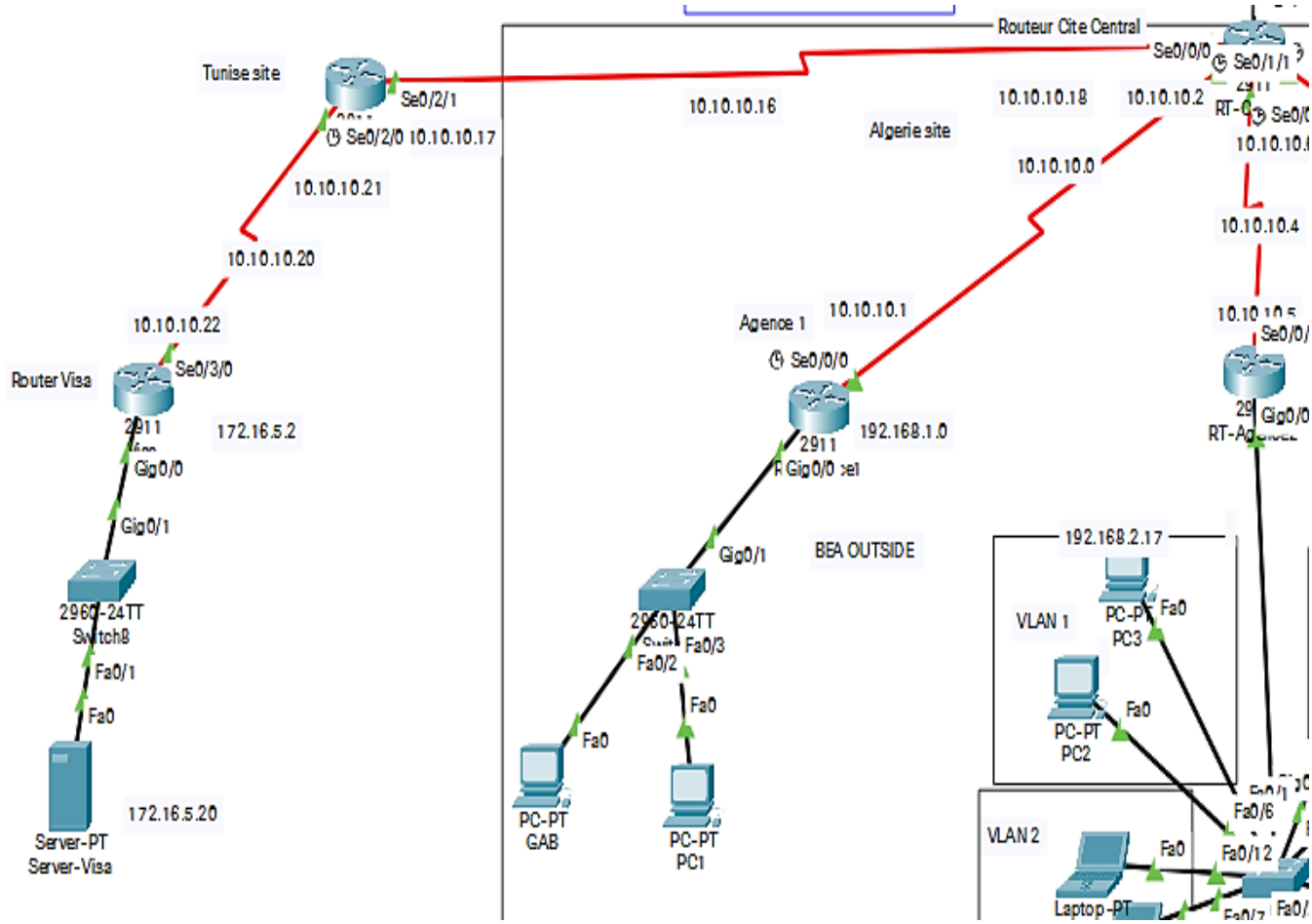


Figure II-3: Schéma des deux sites.

On confirme la route des paquets de GAB vers Visa par la commande tracert :

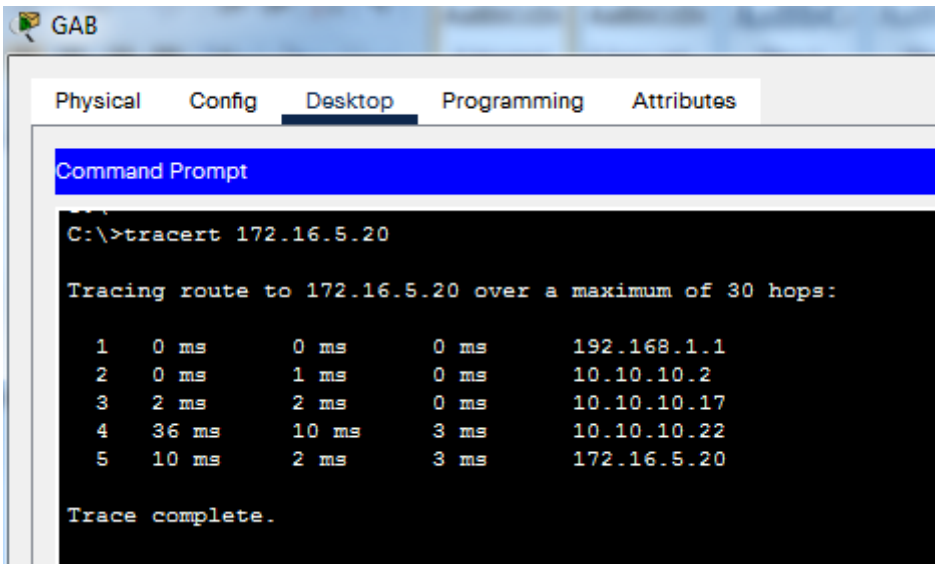


Figure II-4:Trace route de GAB ver Visa affiché par la commande tracert dans le CMD de GAB.

On remarque que le résultat c'est la même avec le schéma des deux site.

II.2 Installer security technology package sur les routers :

Comme d'habitude tout d'abord pour que le simulateur packet tracer permettre crée un tunnel VPN (VPN IPsec) on doit activé une licence de sécurité, dans les paires routeurs de VPN on tape la commande suivante dans le mode configuration :

```
license boot module c2900 technology-package securityk9
```

On a déjà activé une licence de sécurité sur le router de l'agence1 (RT-Agence1),on va l'activé juste sure le router Visa de l'autre site (VPN paire) :

```
ACCEPT? [yes/no]: y
% use 'write' command to make license boot config take effect on next boot
%LICENSE-6-EULA_ACCEPTED: EULA for feature securityk9 1.0 has been accepted.
UDI=CISCO2911/K9:FTX1524IB16-; StoreIndex=0:Evaluation License Storage

Visa-Router(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C2900
Next reboot level = securityk9 and License = securityk9

Visa-Router(config)#
```

Après la sauvegarde et la redémaration du routeur on va vérifier l'activation avec la commande show version :

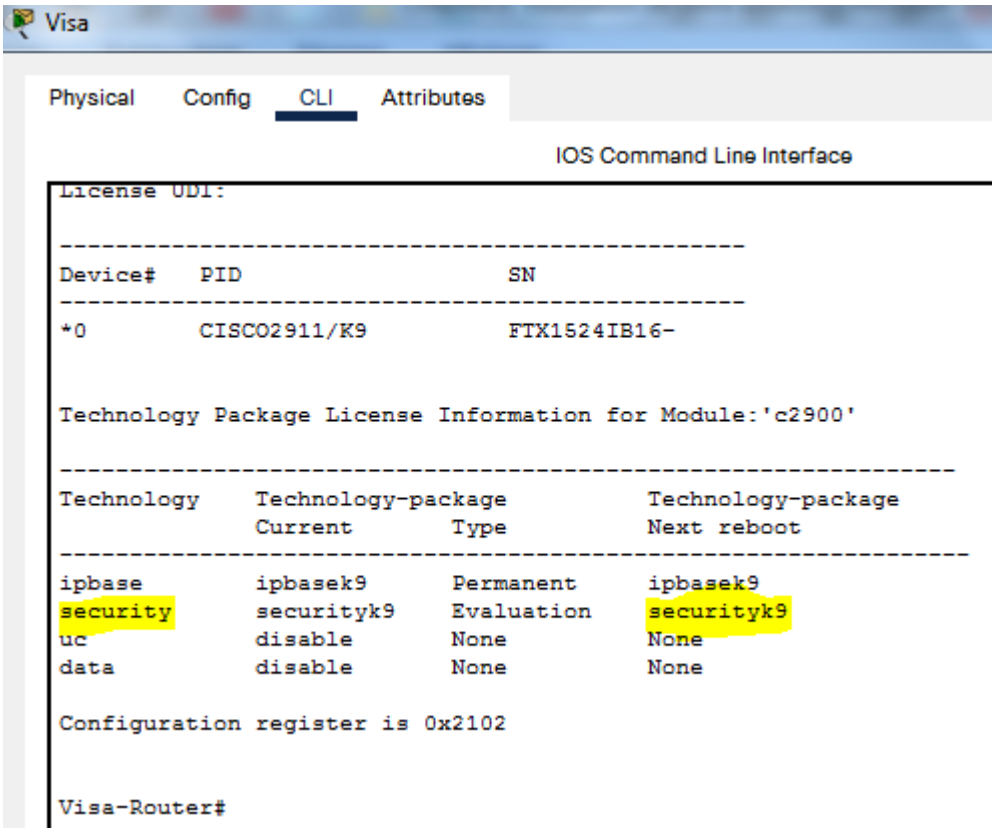


Figure II-5: le résultat de show version dans routeur Visa.

II.3 Identifier le trafic sur les deux routeurs de la paire VPN par une ACL :

On va créer une ACL étendue VPN-TRAFFIC qui servira à identifier le trafic passant sure le tunnel VPN IPSEC, Pour SITE1 VISA, ce sera le Traffic originaire de host serveur-visa 172.16.5.20 à destination de host GAB de la BEA 192.168.1.16 (Ce sera l'inverse pour SITE2 BEA) .

ACL dans le Visa Router :

```
Visa-Router>en
Visa-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Visa-Router(config)#ip access-list extended VPN-TRAFFIC
Visa-Router(config-ext-nacl)#permit icmp host 172.16.5.20 host 192.168.1.16
```

ACL dans le Agence 1 :

```
RT-Agence1(config)#ip access-list extended VPN-TRAFFIC
RT-Agence1(config-ext-nacl)#permit icmp host 192.168.1.16 host 172.16.5.20
RT-Agence1(config-ext-nacl)#
```

II.4 Phase 1: configure IKE (Internet Key Exchange) "ISAKMP POLICY/*Key*" H.A.G.L.E .(Hashing/ Authentication/ Groupe diffie-hellman/ life time/ encryption).

On va établir par le tunnel Phase 1 une sorte de plan de gestion et stratégie de négociation des clés et d'établissement de la liaison VPN entre le router BEA et Router Visa, (cette phase n'est pas utilisée pour crypter ou protéger les paquets).

Tableau 6:Phase 1 ISAKMP Policier les paramétre pour GAB et VISA.

ISAKMP Phase 1 Policy Paramètre		
Paramètre	BEA "GAB"	Visa
Encryption:	AES-256	AES-*256*
Encryption Scheme	IKE	IKE
Hash Algorithm:	SHA-1	SHA-1
Main or Aggressive Mode	Main	Main
Authentication Method:	Pre-Share	Pre-Share
Pre-Shared Key:	****amine-21	****amine-21
Key Exchange:	DH Group 2	DH Group 2
Lifetime:	28800 sec is fine	28800 sec is fine

IKE est un protocole hybride qui implémente des protocoles d'échange de clés a l'intérieur du protocole ISAKMP « Internet Security Association and Key Management Protocol».

On peut activer l'ISAKMP par la commande :

```
(config)# crypto isakmp enable
```

Si non on peut aller directement ver la configuration et il va activer automatiquement :

IKE dans le router Visa :

ISAKMP Policy:

```
Visa-Router>en
Visa-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Visa-Router(config)#crypto isakmp policy 1
Visa-Router(config-isakmp)# encr aes 256
Visa-Router(config-isakmp)# authentication pre-share
Visa-Router(config-isakmp)#hash sha
Visa-Router(config-isakmp)# group 2
Visa-Router(config-isakmp)# lifetime 28800
Visa-Router(config-isakmp)#exit
Visa-Router(config)#
```

Donc on a créé ici une stratégie avec un numéro de séquence 1. Ce numéro indique la grande priorité de l'utilisation de la stratégie. « Plus petit est ce nombre plus la priorité est grande ». On a défini ensuite les paramètres:

- Encryptage AES 256
- Authentification par clé pré-partagées
- Algorithme de hachage SHA (valeur par défaut)
- Méthode de distribution des clés partagées DH-2 (Algoritme de clé asymétriques Diffie-Hellman 1024bits)
- Durée de vie 28800 secondes (8 heurs)

On va défini ensuite si on identifie le routeur par son adresse ou bien par leur nom « hostname » (ici on a choisie l'adresse), l'identification par nom « hostname » peut être utile si on fonctionne avec une adresse publique dynamique, ce qui permet d'éviter trop de modifications de configuration en cas de changement d'adresse.

```
(config)# crypto isakmp identity address
```

Si non le routeur va identifier en même temps avec la configuration suivante.

ISAKMP Key :

On va crée ensuite la clé pré-partagée, « amine21 » qu'on associe avec l'adresse de l'autre bout du tunnel donc 10.10.10.1

```
Visa-Router(config)#crypto isakmp key amine21 address 10.10.10.1
```

Parmi les points important, SITE2 soit avoir une stratégie ISAKMP identique à celle de SITE1 et l'access-list qui identifie le trafic à traiter par le tunnel VPN est inversée d'un point de vue de la source et de la destination.

IKE dans le router BEA :

ISAKMP Policy :

La même configuration va effectuer pour ce Routeur.

```
RT-Agence1>
RT-Agence1>
RT-Agence1>en
Password:
RT-Agence1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RT-Agence1(config)#crypto isakmp policy 1
RT-Agence1(config-isakmp)# encr aes 256
RT-Agence1(config-isakmp)# authentication pre-share
RT-Agence1(config-isakmp)#hash sha
RT-Agence1(config-isakmp)# group 2
RT-Agence1(config-isakmp)# lifetime 28800
RT-Agence1(config-isakmp)#
```

ISAKMP Key :

```
RT-Agence1(config)#crypto isakmp key amine21 address 10.10.10.22
```

On a créé la même clé pré-partagée, « amine21 » qu'on associe avec l'adresse de l'autre bout du tunnel donc 10.10.10.22.

On a maintenant terminé la configuration de la phase 1 qui gère la négociation des clés etc. La deuxième phase consiste à définir comment les données seront cryptées :

II.5 Phase 2 : configure IKE "IPsec Policy":

On va établir par le tunnel Phase 2 le cryptage et la sécurité de donnée qui traversant le tunnel entre server visa et GAB de la BEA.

Tableau 7: Phase2 (IPSEC).

Phase2 (IPSEC):

Paramètre	VISA	BEA
Encasulation (ESP or AH)	ESP	ESP
Encryption:	AES-256	AES-256
Hash Algorithm:	SHA-1	SHA-1
Lifetime:	28800 sec	28800 sec
PFS:	No	No
VPN Peer/Public IP Address:	10.10.10.22	10.10.10.1
LAN	172,16,5,0/24	192,168,1,0/24

II.5.1 Creation de transform-set :

Tout d'abord on va créer la méthode de cryptage (transform-set) que l'on nomme VISA->GAP pour le Routeur Visa.

```
Visa-Router(config)#crypto ipsec transform-set VISA->GAP esp-aes 256 esp-sha-hmac
Visa-Router(config)#
```

Esp-aes est la méthode de cryptage, esp-sha-hmac est le protocole de hachage et la méthode d'authentification.

On va défini ensuite la durée de vie de la clé de cryptage :

```
Visa-Router(config)#crypto ipsec security-association lifetime seconds 28800
```

La durée de vie est ici limitée en secondes, on peut également définir une durée de vie par un volume en kilobytes par exemple 4096 (ex : crypto ipsec security-association lifetime kilobytes 4096).

La même méthode de cryptage et durée de vie de la clé pour le routeur BEA on modifie juste le nomme GAP->VISA :

```
RT-Agence1(config)#crypto ipsec transform-set GAP->VISA esp-aes 256 esp-sha-hmac

RT-Agence1(config)#crypto ipsec security-association lifetime seconds 28800
```

II.5.2 Crée une crypto map « CMAP » :

Créer une Crypto-map dont le but est de rassembler les différents éléments configurés pour pouvoir les appliquer enfin à une interface :

Pour le Routeur VISA :

```
Visa-Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Visa-Router(config-crypto-map)# set peer 10.10.10.1
Visa-Router(config-crypto-map)# set transform-set VISA->GAP
Visa-Router(config-crypto-map)# match address VPN-TRAFFIC
Visa-Router(config-crypto-map)#
```

On a donc créé ici une Crypto-map nommée CMAP dans laquelle on intègre une séquence 10 (une seule crypto-map par interface, mais on peut ajouter plusieurs maps en leur indiquant des numéros de séquence différents), avec les paramètres suivants :

- Activée pour le trafic correspondant à l'access-list VPN-TRAFFIC
- Destination du tunnel 10.10.10.1
- Cryptage selon le transform-set VISA->GAB

Pour le Routeur BEA :

```
RT-Agence1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RT-Agence1(config-crypto-map)# set peer 10.10.10.22
RT-Agence1(config-crypto-map)# set transform-set GAP->VISA
RT-Agence1(config-crypto-map)# match address VPN-TRAFFIC
```

II.5.3 Appliqué la crypto map sur l'interface de sortie :

La dernière étape consiste à appliquer cette crypto-map à l'interface WAN de SITE1(Pour le routeur BEA) :

```
RT-Agence1(config-crypto-map)#interface se0/0/0
RT-Agence1(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Et voilà (ISKAMP is ON) ISKAMP est allumé. SITE est prêt. Reste à faire l'équivalent sur SITE2(pour le routeur VISA) :

```
Visa-Router(config-crypto-map)#interface se0/3/0
Visa-Router(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

II.5.4 Vérification du tunnel VPN :

Une fois le tunnel configuré, deux commandes permettent de vérifier si le tunnel fonctionne :

- # show crypto isakmp sa
- # show crypto ipsec sa

Toutefois, pour que l'on pu vérifier le fonctionnement il faut que le VPN soit établi, et pour cela il faut que du trafic soit envoyé au travers de ce tunnel. D'abord on confirme la route des paquets de GAB vers Visa par la commande « tracert » :

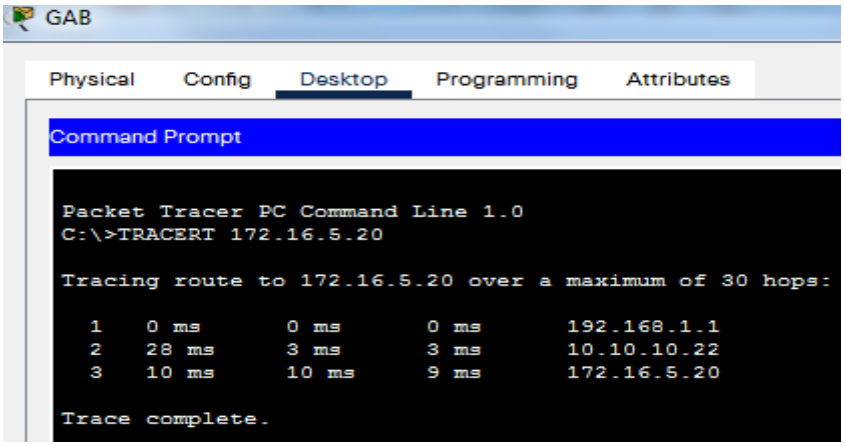


Figure II-6:CMD de GAB affiche la trace route de GAB ver Visa.

On remarque que la résultat est différant par rapport a la trace route de la « Figure II-4 » (sans VPN)

Donc le nouveau schéma sera comme suit :

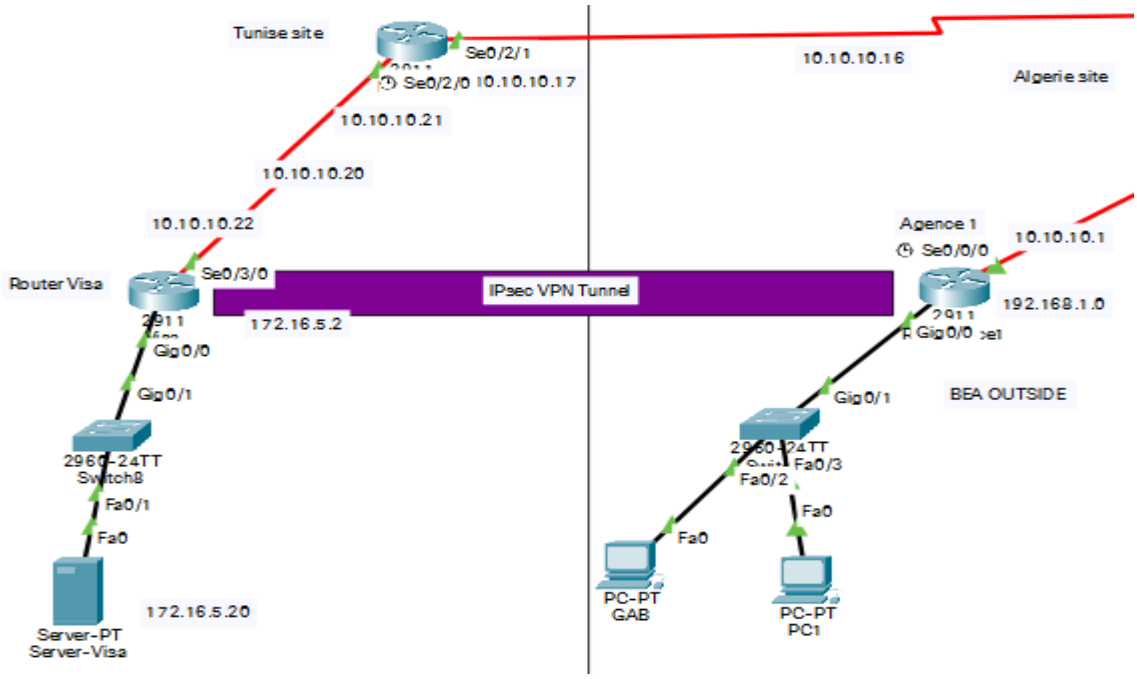


Figure II-7:Schéma des deux sites avec le tunnel VPN.

Une fois le tunnel configuré, deux commandes permettent de vérifier si le tunnel fonctionne :

- # show crypto isakmp sa
- # show crypto ipsec sa

On peut maintenant vérifier si le tunnel à bien fonctionné :

```
Visa-Router>en
Visa-Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.10.1      10.10.10.22     QM_IDLE           1082    0 ACTIVE


IPv6 Crypto ISAKMP SA


Visa-Router#sh crypto ipsec sa

interface: Serial0/3/0
    Crypto map tag: CMAP, local addr 10.10.10.22

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.5.20/255.255.255.255/1/0)
   remote  ident (addr/mask/prot/port): (192.168.1.16/255.255.255.255/1/0)
   current_peer 10.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
   #pkts decaps: 14, #pkts decrypt: 14, #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.: 10.10.10.22, remote crypto endpt.:10.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
     current outbound spi: 0xCC329D75(3425869173)

     inbound esp sas:
      spi: 0x956C3ECF(2506899151)
 --More--
```

Les deux lignes surlignées en jaune indiquent les paquets reçus et envoyés par le tunnel VPN.

Pour conclure voici des captures des PDU réalisée par le mode simulation de paquet tracer sur la liaison entre RT-Agence1 de SITE1 BEA et VPN lors de l'envoi de requêtes ICMP de 192.168.1.16 à 172.16.5.20:

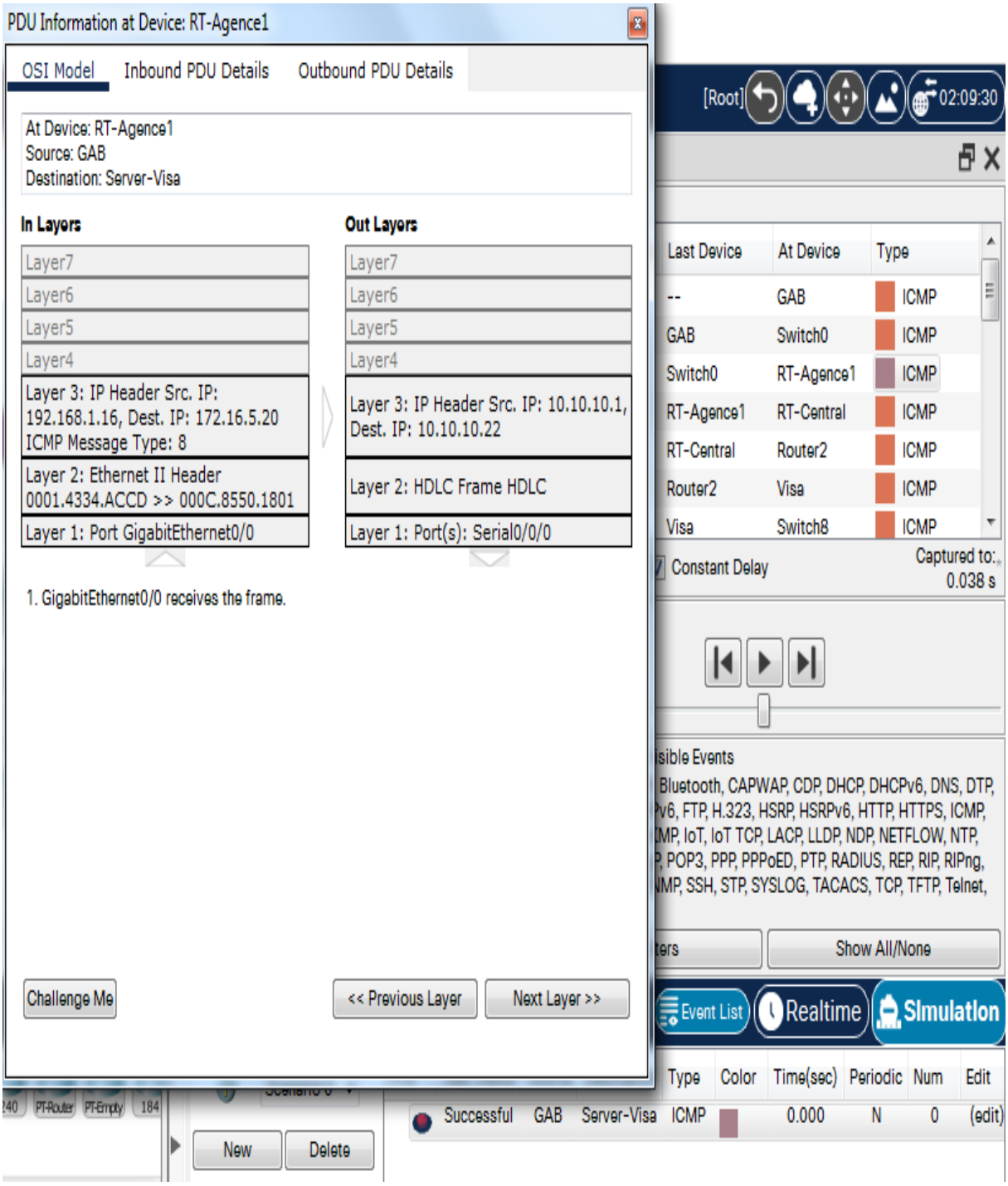


Figure II-8: PDU d'un ping dans le tunnel VPN effectué par GAB ver Visa-server.

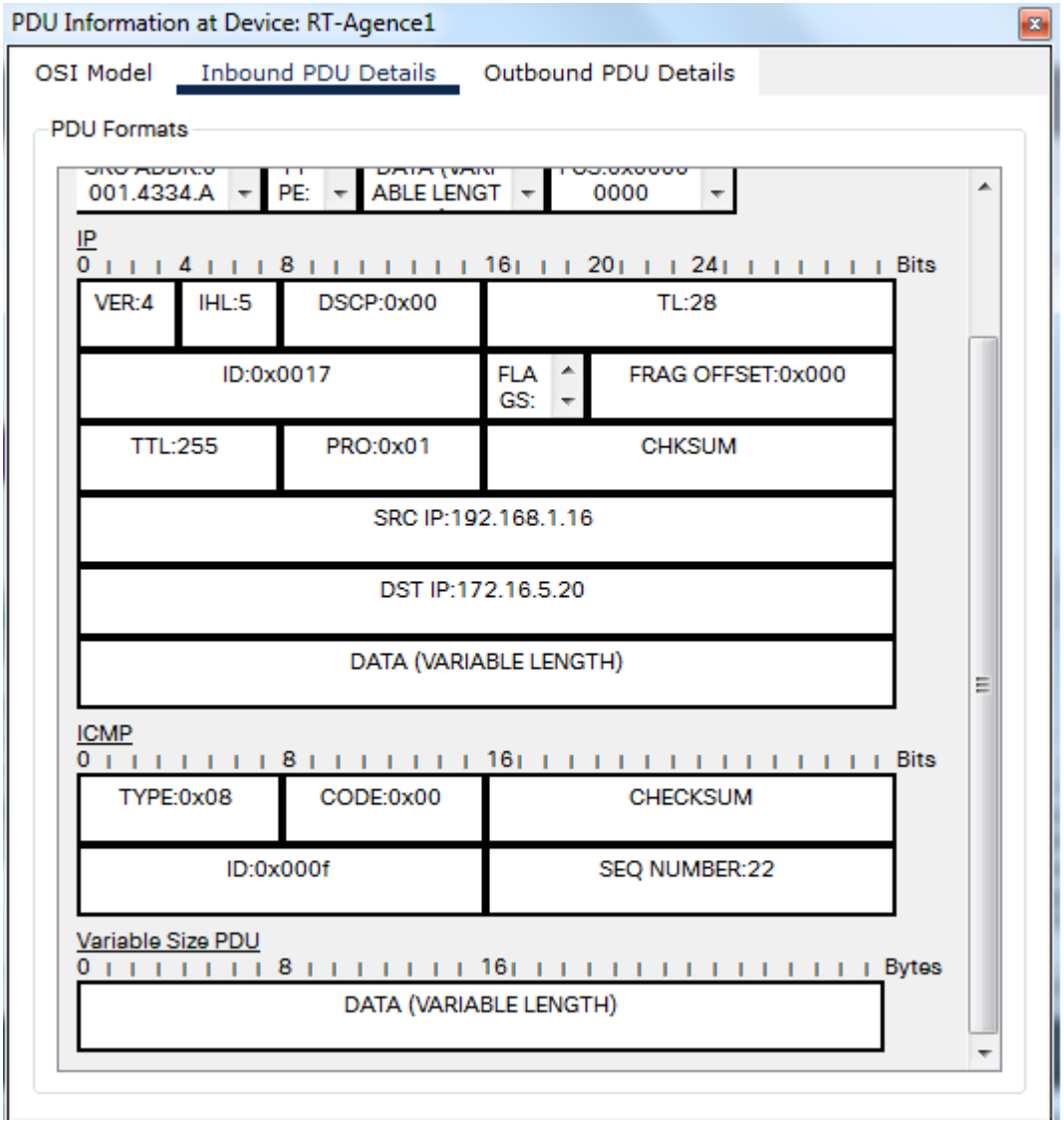


Figure II-9:Inbound PDU détail de la Figure II-10 « le détail de la PDU entrant ».

On remarque que les données de cette PDU sont exposées, Comme ça se voit-on des paquet ICMP « Figure III-9 ».

Par contre ici on peut pas connaitre le type de données, ils sont cryptés ESP Header :

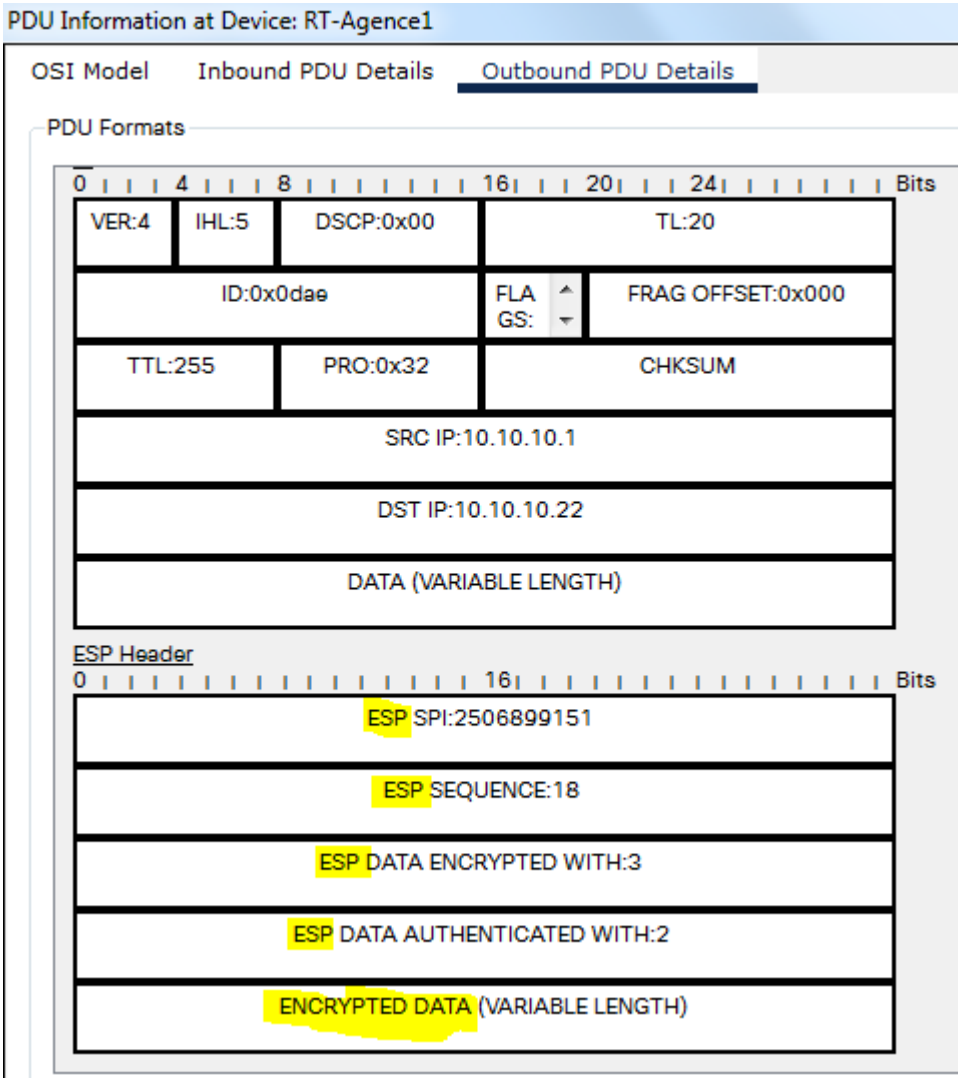


Figure II-11:Outbound PDU détail de la Figure IV.5 4 « le détail de la PDU sortant ».

Figure : outbound

Il est ici impossible de voir qu'il s'agit de paquets ICMP, la seule chose visible c'est qu'il y a un trafic crypté d'un bout à l'autre du tunnel.

III. Discussion:

Nous avons proposé la centralisation « Figure III-1» des données dans notre réalisation, pour améliorer la qualité des services pour les clients et renforcer la protection les données de la banque. Ceci consiste à éliminer les serveurs au niveau des agences et de travailler directement sur le serveur central.

CHAPITRE 7 : *Réalisation et Mise en place des solutions de sécurité*

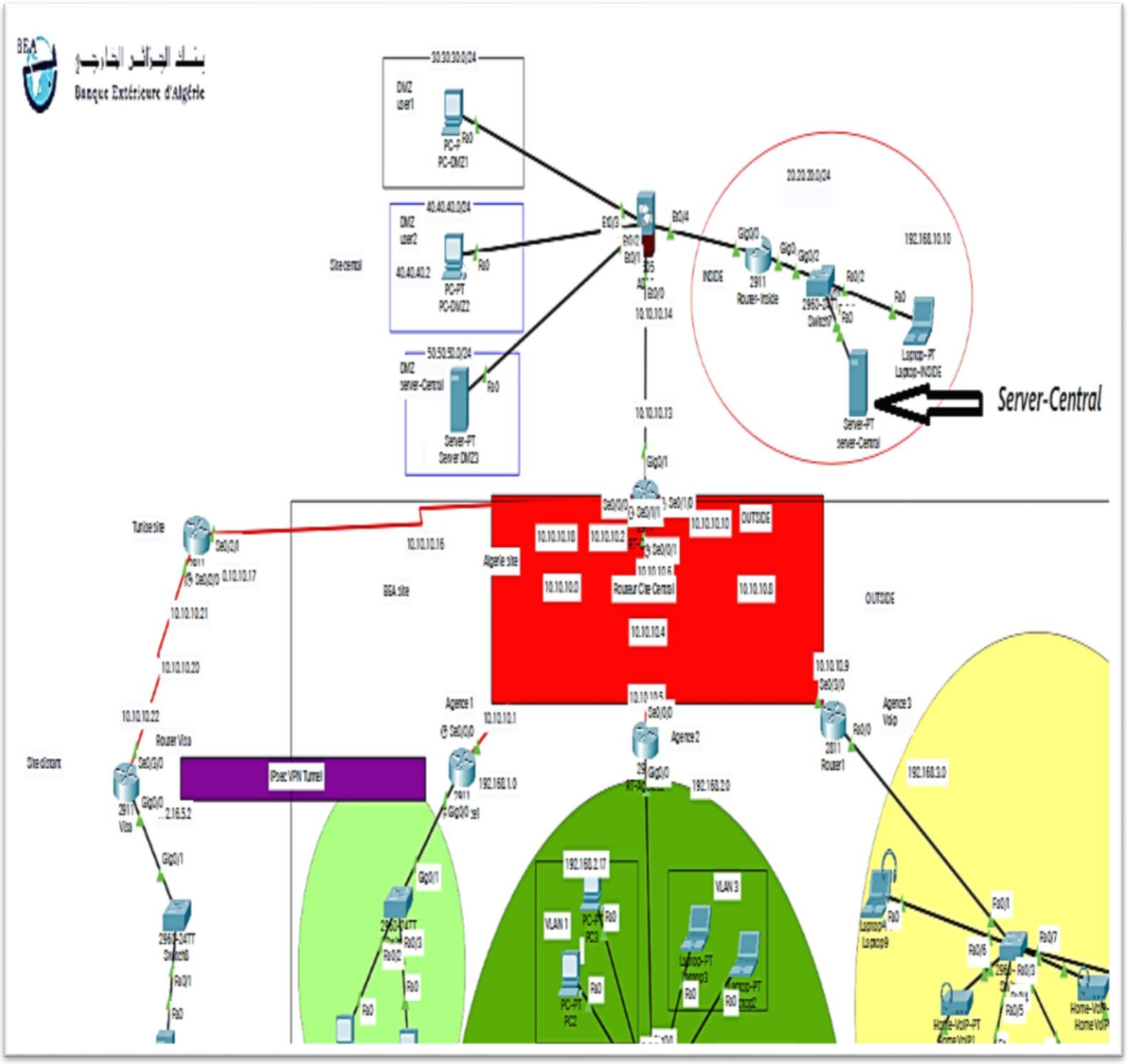


Figure III-1:Schéma de centralisation de notre architecture réaliser.

Cette nouvelle approche va permettre d'améliorer la qualité de services pour les clients de l'agence et d'augmenter la disponibilité des services bancaires.

Comme chaque solution, la centralisation des données a une architecture client-serveur. Elle présente des avantages et des inconvénients.

Cette structure très pratique pour l'organisation, pose toutefois des problèmes de sécurité du réseau :

- Si le serveur central tombe en panne le réseau ne fonctionne plus.
- S'il y a beaucoup de connexions simultanées ponctuellement non prévues, alors le serveur central peut être saturé.

IV. Conclusion:

Ce chapitre est le fruit de toute une étude consacrée à l'implémentation de la solution proposée. Il nous a permis de mettre en œuvre la plus parts des concepts vus en cours et au niveau du stage pratique. C'est l'étape de mettre en essai les différentes conceptions théorique (implémentation des VLAN, ACL sous ASA, Voip, VPN…).

Nous avons décri la configuration de nos architectures réseaux dans les deux parties. Dans la première, nous avons configuré les réseaux de la BEA agences et site central ainsi que des tests de vérification, et dans la deuxième partie nous sommes passé à la configuration des exigences de sécurité tel que la configuration de VPN IPsec et du pare-feu illustré par une présentation des différentes commandes de mise en place.

Notre plus grande satisfaction est le résultat estimant considérable est atteint. Notre perspectif est faire la 2^{éme} solutions qu'on a proposé dans le chapitre précédant, qui seront meilleurs pour plus de sécurité réseau.

Conclusion Générale et perspectives

La sécurité du réseau WAN via le pare feu ASA 5505 avec de l'aide d'une configuration d'un tunnel VPN IPsec Site to Site et d'autres aspects de sécurité au niveau de la Banque Extérieure d'Algérie et précisément au sein de la direction Télécom, nous a permis d'apprendre de nouveaux concepts aussi bien en termes de connaissances théorique et pratique,

Notre travail est considéré comme une expérience qui nous a permis de nous intégrer dans le milieu professionnel. Cette expérience en entreprise nous a offert une bonne préparation pour une insertion professionnelle car elle fut pour nous une expérience enrichissante et complète qui conforte notre désir d'exercer mon futur métier d'ingénieur dans le domaine de réseau et télécom et surtout la sécurité informatique.

Enfin, il me reste plus qu'à remercier notre cher enseignant encadrant M. RIAHLA pour sa disponibilité et son soutien ainsi que Mme ATBA pour ses encouragements et conseils tout au long de la période de stage. On tient aussi à exprimer notre satisfaction de pouvoir travailler dans de bonnes conditions matérielles et environnementales.

Dans envisageons dans le futur que le cybercriminel n'a qu'une cible, pour cela on va mètre on place un NGFW avec des exigences de sécurité stricte :

- ✓ Utiliser au niveau du site central un NGFW data center en cluster active/active.
- ✓ Doter les agences d'un NGFW destiné pour les agences pour renforcer la sécurité au niveau de l'agence.
- ✓ Sécuriser les connexions internet et mettre on place d'autres exigences de sécurité.

BIBLIOGRAPHIE ET WEBOGRAPHIE

V. Références

1. *L'informatique est-elle une science ? c.* **Milner, Robin.** 10 décembre 2007. conférence à l' ENS.

2. **Pillou, Jean-François.** *Introduction à la sécurité informatique.* 2015.

3. **Model OSI.** ***frameip.*** **[En ligne] https://www.frameip.com/osi/.**

4. ***A modified McCumber cube as a basis for a taxonomy of cyber attacks.*** **Easttom, C., & Butler, W. (. Janvie 2019, In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0943-0949.**

5. ***Un cadre de spécification et de déploiement de politiques d'autorisation (Doctoral dissertation.*** **Cheaito, M. 2012, Université de Toulouse, Université Toulouse III-Paul Sabatier).**

6. Goaziou, Y. ***Méthodes d'évaluation de l'intégrité biotique du milieu aquatique basées sur les macroinvertébrés benthiques: rapport de stage.*** **2004.**

7. ***Analyse critique des approches de l'acceptation des technologies: de l'utilisabilité à la symbiose humain-technologie-organisation.*** **. Brangier, E., Hammes-Adelé, S., & Bastien, J. M. 2, 2010, European review of applied psychology, Vol. 60, pp. 129-146.**

8. De Filippi, P., & Dulong de Rosnay, M. ***Le pirate informatique, un explorateur des courants juridiques du réseau.*** **Tracé : Revue de Sciences humaines,, 2014. pp. 43-65. Vol. 26.**

9. ***developpez.*** **[En ligne] https://web.developpez.com/tutoriels/web/failles-securite-application-web/.**

10. Anass, B. (n.d.). ***Kali Linux Pour DÉbutant: Le Guide Ultime du débutant Pour Apprendre le Système d'exploitation des Hackers.***

11. l, E. ***Hacking, sécurité et tests d'intrusion avec Metasploit.*** **s.l. : Montreuil: Pearson., 2017.**

12. Yende, R. SUPPORT DE COURS DE SÉCURITÉ INFORMATIQUE ET CRYPTO. 2018.

13. Remazeilles, V. ***La sécurité des réseaux avec Cisco.*** **s.l. : Editions ENI, 2009.**

14. La gamme des switches Cisco Meraki MS. ***everlink.*** **[En ligne] https://www.everlink-services.fr/cisco-meraki/gamme-switches-cisco-meraki-ms/.**

15. Ciscomag. Cisco ASA 5505 Adaptative Security Appliance. s.l. : Cisco, 24 mai 2007. pp. 2-4.

16. REMAZEILLES, Vincent. Cisco La sécurité des réseaux. ***editions-eni.fr.*** **[En ligne] Cisco. https://www.editions-eni.fr/open/mediabook.aspx?idR=ff39a2d5380463190eb402ae4e7a30d2.**

17. RIAHLA, Dr. Routage dynamique. 2008/2009.

18. ***acervolima.*** **[En ligne] https://fr.acervolima.com/ldap-et-ldap-injection-prevention/.**

- **Lanaspèze, M. (n.d.). Emotet et Matrix : Analyse, Protection Next-Gen, apports de l'IA et de l'EDR. sophos.**
- ***Mathon, P. (2002). ISA Server 2000 Proxy et Firewall: optimiser l'accès Internet et sécuriser son réseau d'entreprise. Editions ENI.***
- ***Headquarters, C. (2005). Cisco Security Appliance Command Line Configuration Guide.***
- ***Cisco ASA Configuration (Networking Professional's library) (DavidHucaby).***
- ***Eric, A. B. (2021). Une Solution Optimale Pour le Choix des Protocoles De Routage: Généralités sur les réseaux informatiques, Introduction sur MPLS, Les VPN MPLS, Mise en place de la solution (French Edition). Independently published.***
- ***www.cisco.com « Date de dernière navigation : 23/10/2021 »***
- ***https://www.netacad.com/courses/networking « Date de dernière navigation : 18/08/2021 »***
- ***https://cyber.gc.ca/fr/orientation/les-10-mesures-de-securite-des-ti-visant-proteger-les-reseaux-internet-et-0 « Date de dernière navigation : 15/09/2021 »***
- **https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique** ***« Date de dernière navigation : 18/09/2021 »***
- **https://www.cert.ssi.gouv.fr/** ***« Date de dernière navigation : 27/08/2021 »***
- **https://www.reseaucerta.org/** ***« Date de dernière navigation : 20/09/2021 »***
- **https://culture-informatique.net/cest-quoi-un-serveur-proxy/** ***« Date de dernière navigation : 02/10/2021 »***
- **https://www.securiteinfo.com/cryptographie/tunnel.shtml** ***« Date de dernière navigation : 12/10/2021 »***
- **https://www.universalis.fr/encyclopedie/reseaux-informatiques/6-securite-dans-les-reseaux/** ***« Date de dernière navigation : 27/08/2021 »***
- **http://www.technologuepro.com/reseaux/Configuration-avancee-dun-routeur/Configuration-routage-statique.html** ***« Date de dernière navigation : 16/10/2021 »***

- **- http://fr.scribd.com/doc/82449229/La-securite-des-reseaux-informatique#scribd**
  « Date de dernière navigation : 01/11/2021 »