الجـــــــــــــــــــــــــمهـوريـــــــة الجـــــــــــــــزائريـة الديمـــــــــقـراطيـة الشـــــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــــعليـم العـــــــالي و البـــــــــــحث العـــــلـمـــي

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

جـــــــــــــــامعة أبي بكـــر بـلـقـايد – تـلمســـــــــــــــان –

UNIVERSITÉ ABOUBAKR BELKAÏD – TLEMCEN –

FACULTÉ DE TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de MASTER

EN Télécommunication

SPÉCIALITÉ Réseaux et Télécommunication

Par BEDREDDINE Imad Eddine & BRAHMI Wissam

SUJET

Implémentation de politiques de sécurité réseaux CISCO

Soutenu par visioconférence, le 22/09/2020, devant le jury composé de :

M. BOUACHA A.	Professeur	Univ - Tlemcen	Président
M. ABDELMALEK A.	Maitre de Conférences	Univ - Tlemcen	Directeur de mémoire
M. BOUABDALLAH R.	Maitre de Conférences	Univ - Tlemcen	Examinateur

Année Universitaire 2019/2020

“ Nous avons construit un monde où l’intelligence est la première des facultés, où la science et la technique nous tirent en avant et nous chutons, en produisant plus de misères, de famines, de maladies. “

Michel Serres

“ La valeur d’une éducation universitaire n’est pas l’apprentissage de Nombreux faits, mais l’entrainement de l’esprit à penser. “

Albert Einstein

Toutes les lettres ne sauraient trouver les mots qu'il faut…
Tous les mots ne sauraient exprimer la gratitude, l'amour,
Le respect, la reconnaissance…
Aussi, c'est tout simplement que…

Nous Dédions ce Mémoire

A mes chers parents

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être.
Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

A mon cher grand-père maternel

Que ce modeste travail soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières. Que Dieu vous préserve santé et longue vie.

A mes chères Petites sœurs

Je vous dédie ce travail en témoignage de mon amour et mon attachement.
Puisse nos fraternels liens se pérenniser et consolider encore.
Je ne pourrais d'aucune manière exprimer ma profonde affection et mon immense gratitude pour tous les sacrifices consentis, votre aide et votre générosité extrêmes ont été pour moi une source de courage, de confiance et de patience.
J'implore DIEU qu'il vous apporte bonheur, amour et que vos rêves se réalisent.

A la mémoire de mes grands-parents paternels et ma grande–mère maternelle

J'aurais tant aimé que vous soyez présents.
Que Dieu ait vos âmes dans sa sainte miséricorde

A ma chère binôme « Wissam »

Ma douce amie qui a eu la patience de me supporter durant ce mémoire, et qui m'a soutenu et encouragé pendant tous les moments difficiles vécus.
Je te souhaite une vie pleine d'amour, de joie.de santé et de réussite

A tous mes amis

En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passés ensemble, Je vous souhaite un avenir plus brillant et plus heureux.

A la mémoire de « Hasni Chakroun »

Dédicace en hommage à ***Cheb Hasni*** *le roi de la chanson sentimentale pour son 26ème anniversaire, J'aurais tant aimé que tu sois présent dans cette époque.*
Que Dieu ait ton âme dans son vaste paradis.

IMAD

A mon cher papa

À qui quoi je dirai ne suffira pas pour exprimer ma gratitude et ma reconnaissance pour son soutien, qui était et restera toujours mon grand exemple, sa chaleur paternelle a été toujours pour moi un grand réconfort,
Qu'ALLAH te préserve et t'accorde santé et bonheur.

A ma chère maman

Qui n'a jamais cessé de ménager ses efforts pour que j'atteigne ce niveau. Ses sacrifices et privations ne l'ont pas empêchée d'accomplir son devoir de mères soucieuses de l'avenir de ses enfants.
Que Dieu, le tout puissant, te préserve, t'accorde santé, bonheur,
quiétude de l'esprit et te protège de tout mal.

A ma p'tite sœur et mon p'tit frère

En témoignage de mon amour et de ma grande affection, je vous prie de trouver dans ce travail l'expression de mon estime et mon sincère attachement.
Je prie Dieu, le tout puissant, pour qu'il vous donne bonheur et prospérité.

A mon cher mari

A mon soutien moral et source de joie et bonheur, pour l'encouragement et l'aide qu'il m'a toujours accordé.
Qu'ALLAH, te préserve et te procure santé et longue vie.

A Mon cher binôme « IMAD »

Qui était toujours à mes côtés et qui n'a jamais cessé de me soutenir et de m'encourager pendant tous les moments difficiles vécus. Jamais de simples mots ne permettront de t'exprimer mes remerciements.
Je te souhaite tout la réussite et le bonheur du monde.

A la mémoire de mes grands-parents paternels et mon grand-père maternel

Que Dieu ait vos âmes dans sa sainte miséricorde.

A toute ma grande famille et ma belle-famille, ainsi à tous mes ami(e)s

Pour l'amour et le respect qu'ils m'ont toujours accordé.

WISSAM

Remerciements

Avant tout nous tenons nos remerciements à notre dieu tout puissant de nous avoir donné le courage, la volonté, la force, la patience et la chance de suivre le chemin de la science, de mener à bien ce modeste travail, qui n'aurait jamais été réalisé sans sa bénédiction.

Nous remercions infiniment, ***M. ABDELMALEK Abdelhafid****, Maitre de conférences à L'université Abou-Bekr Belkaid-Tlemcen, qui nous a confié ce travail riche d'intérêt et nous a guidé à chaque étape de sa réalisation.*
Vous nous avez toujours réservé le meilleur accueil, malgré vos obligations professionnelles, vos encouragements inlassables, votre amabilité, votre gentillesse méritent toute admiration. Nous saisissons cette occasion pour vous exprimer notre profonde gratitude, tout en vous témoignant notre respect.

Nous remercions ***M. BOUACHA Abdelhafid****, Professeur à l'université Abou-Bekr Belkaid-Tlemcen, pour l'honneur que vous nous faites en acceptant de juger ce travail, Nous sommes très honorées de vous avoir comme président de jury de notre mémoire.*

Nos vifs remerciements à ***M. BOUABDALLAH Réda****, Maitre de conférences à l'université Abou-Bekr Belkaid-Tlemcen, c'est pour nous un grand honneur de vous voir siéger dans notre jury.*

On profite de cette opportunité pour exprimer notre profonde gratitude à tous les enseignants qui ont contribué par leur collaboration, disponibilité et sympathie, à notre formation.

Nous tenons à exprimer nos sincères remerciements à tous ceux qui ont contribué, de près ou de loin, à l'élaboration de ce mémoire de fin d'études.
Aussi, nous tenons à remercier infiniment, nos chers parents, pour leurs contributions, leurs soutiens et leurs patiences au long de nos études.

Résumé

Suite à notre étude sur la sécurité des réseaux informatiques ainsi que les différentes menaces auxquelles les réseaux d'entreprises sont exposés, nous nous rend compte qu'il n'est pas évident d'assurer une sécurité optimale à un réseau informatique et de le protéger contre d'éventuelles intrusions et menaces. Avoir un réseau complètement sécurisé est pratiquement irréalisable. Par conséquent, il est nécessaire de pouvoir détecter les intrusions lorsqu'elles se produisent. Cela est rendu possible grâce aux mécanismes de sécurité. Ces mécanismes consistent à détecter, prévenir et lutter contre les attaques.

Dans ce travail, nous nous intéressons à l'implémentation purement software sur une plate-forme configurable basée sur CISCO dans laquelle nous allons configurer les différentes solutions de sécurité et nous testons la fiabilité de chaque solution.

Mots-clés : Sécurité informatique, politique de sécurité, mécanismes de sécurité, attaques, ACL, Cryptographie, par-feu, IDS, VPN, SSH et antivirus.

Abstract

Following our study on the security of computer networks as well as the various threats to which business networks are exposed, we realize that it is not easy to ensure optimal security for a computer network and to protect it. Against possible intrusions and threats. Having a completely secure network is practically impossible. Therefore, it is necessary to be able to detect intrusions when they occur. This is made possible by the security mechanisms. These mechanisms consist of detecting, preventing and combating attacks.

In this work, we are interested in the pure software implementation on a configurable platform based on CISCO. In which the various security solutions are configured and the reliability of each solution is tested.

Keywords : Computer security, security policy, security mechanisms, attacks, ACL, Cryptography, firewall, IDS, VPN, SSH and antivirus.

Table des matières

CHAPITRE II Modèles & Mécanismes de Sécurité Réseaux

CHAPITRE III Conception & Implémentation des Mécanismes de Sécurité Réseaux CISCO

Liste des figures

Liste des tableaux

Introduction générale

De nos jours les entreprises dès leur création n'hésitent pas à mettre en place un réseau informatique pour faciliter la gestion de leur infrastructure, c'est pour cela que la sécurité de ces réseaux constitue un enjeu crucial.

La sécurité informatique consiste à s'assurer que les ressources d'une machine ou d'un réseau sont uniquement utilisées par les personnes autorisées et dans le cadre où il est prévu qu'elles le soient. Cela n'est pas toujours facile à réaliser vu qu'actuellement, de plus en plus d'ordinateurs et des réseaux sont reliés entres aux ou à Internet. Cette connectivité a facilité, certes, l'échange entre ces composants, mais elle a augmenté en même temps les risques d'attaques contre ces réseaux. Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter des composants essentiels qui sont les mécanismes de sécurité. Ces mécanismes ont pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr.

En plaçant ces mécanismes limitant ou interdisant l'accès aux différents services de l'entreprise, donc elle peut avoir un contrôle sur les activités se déroulant dans son enceinte.

Dans ce cadre s'inscrit notre projet de fin d'études qui consiste à mettre en place les mécanismes de sécurité. Pour mener à bien notre travail, nous allons l'articuler autour de quatre chapitres:

Le premier chapitre est un chapitre descriptif pour la sécurité des réseaux, sur lequel on va définir une politique de sécurité, les risques, les menaces, les attaques, les logiciels malveillants et ainsi la gestion de la sécurité.

Le second chapitre est consacré à la présentation des différentes techniques de protection des réseaux informatiques contre les attaques, en expliquant en détaille les solutions de sécurité (mécanismes de sécurité).

Le troisième chapitre est composé de deux parties : la première explique en détaille le logiciel de construction des réseaux physique virtuel (Packet Tracer CISCO) et son fonctionnement ainsi que la deuxième partie est consacré à la conception et l'implémentation des différents mécanismes de sécurité dans les réseaux Cisco ainsi tous les paramétrages nécessaires afin de rendre le réseau informatique fonctionnel et sécurisé.

Dans le dernier chapitre, nous allons présenter deux architectures qui regroupent la majorité des solutions à la fois pour un bon fonctionnement sécurisé des réseaux Cisco et nous examinerons la fonctionnalité générale de cette dernière par la mise en œuvre de politiques et des règles de sécurité.

Nous finirons notre travail par une conclusion générale et un ensemble des perspectives ouvertes par ce thème de recherche.

CHAPITRE I
Généralités sur la Sécurité Réseaux

I.1 Introduction

La sécurité de l'information est une préoccupation primordiale dans le domaine des réseaux. La sécurité d'un équipement demandait une isolation complète de l'environnement extérieur, et aucune communication avec une machine externe n'était possible. Avec la généralisation d'Internet et des moyens de communication modernes, une nouvelle forme d'insécurité s'est répandue, qui s'appuie sur l'utilisation de codes informatiques pour perturber ou pénétrer dans les réseaux et les systèmes qui les composent.

Aujourd'hui, les réseaux sont toujours devants des menaces. Il y a de plus en plus de techniques pour les protéger, mais il y a aussi de plus en plus de techniques pour les attaquer car il est pratiquement impossible d'avoir un réseau complètement sûr et de le protéger contre toutes les attaques possibles. C'est pour ça le réseau informatique nécessite plusieurs mécanismes pour le protéger contre les risques qui les engendre (forte sécurité). Pour évaluer et assurer les besoins de sécurité d'une entreprise, il faut considérer Les services de sécurité, Les attaques de sécurité et Les mécanismes de sécurité pour la prévention, la détection des attaques et la réponse à ces attaques.

Dans ce premier chapitre, nous introduisons les concepts élémentaires de la sécurité des réseaux informatiques. Nous commençons par décrire la notion de politique de sécurité, les dimensions de la sécurité réseau (confidentialité, authentification, etc.). Ensuite nous présentons les différents types de menaces, vulnérabilités, attaques et les grands ennuis causés par ces derniers.

I.2 Notions de politique de la sécurité réseaux

Compte tenu de la nouvelle importance accordée à la sécurité et à la manière stratégique et globale de l'appréhender, une politique de sécurité devient l'expression de la stratégie sécuritaire des organisations. Elle constitue pour les organisations un outil indispensable non seulement la gouvernance de la sécurité mais aussi à la réalisation du plan stratégique de sécurité. [1]

I.2.1 Définition de la sécurité réseaux

La sécurité d'un réseau informatique est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir sa sécurité veut dire réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Elle s'occupe de la prévention d'actions non autorisées par les utilisateurs d'un système informatique, afin d'assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information traitée. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie. [1] [2]

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système.
- De sécuriser les données pour éviter la perturbation ou des pannes.
- De garantir la non-interruption d'un service.

I.2.2 Définition d'une politique de sécurité

Une politique de sécurité est un document qui établit un ensemble de règles. Ces règles expriment la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressources, procédures, outils) qui répondent de façon complète et

cohérente aux objectifs stratégiques de sécurité. Elle découle des grands principes de sécurité qui permettent de protéger le système d'information en évitant qu'il ne devienne une cible d'attaques. [2]

Elle a pour finalité de : [3]

- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation.
- Définir les actions à entreprendre et les personnes à contacter dans le cas d'une attaque informatique.
- Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information.

I.2.3 Principaux services de la sécurité

Les services de sécurité représentent les logiciels et matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin. Alors pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace. Les principaux services sont : [2]

- **Authentification :** Est l'assurance de l'identité d'un objet, ce service a pour objectif de vérifier l'identité des processus communicants. Plusieurs solutions simples sont mises en œuvre pour cela, comme l'utilisation d'un identifiant et d'un mot de passe.
- **Autorisation** : Information permettant de déterminer quelles sont les ressources de l'entreprise aux quelles l'utilisateur identifié et autorisé a accès, ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise.
- **Confidentialité** : Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer leur confidentialité des données.
- **Disponibilité** : Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.
- **Intégrité** : Ensemble des mécanismes qui assurent que les informations transmises entre la source et la destination n'ont pas été altérées. Garantir l'intégrité des données implique la prévention et la détection de la modification, l'ajout ou la suppression des informations.
- **La Traçabilité** (ou **« Preuve** ») **:** Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose de garantir que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
- **La non-répudiation :** Mécanisme permettant de garantir qu'aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur. Généralement cette opération utilise une signature asymétrique en chiffrant l'empreinte du message avec la clé RSA privée de son auteur.

Remarque : L'évaluation de la sécurité d'un système informatique est un processus très complexe basé en général sur une méthodologie. Cette évaluation passe par une analyse de risques. Cette dernière pesant sur un système informatique elle-même s'appuie sur un ensemble de règles définies au préalable.

I.3 Raisons de la sécurité réseaux

I.3.1 Enjeux

Pour se protéger des pirates, il faut connaître les possibilités d'attaques. Aussi, pour se défendre d'elles, il faut commencer par accepter le danger. La mise en place d'une politique (plan) de sécurité consiste en : [5]

a. **L'identification des éléments à protéger** (matériels, logiciels, données, personnes, etc.).

b. **L'identification des attaques éventuelles** des pirates dont :

   - **La dégradation** qui consiste à perturber le réseau informatique via une panoplie de programmes parasites tels que les virus, les chevaux de Troie, les vers (WORM), les bombes, les bactéries, etc.
   - **L'altération** des données qui s'effectue soit pendant la transmission des données sur un réseau, soit avant leur émission, soit pendant le passage sur un nœud du réseau.
   - **L'écoute** qui consiste à surveiller et intercepter des données soit sur un poste (cheval de Troie), soit sur une ligne de communication (sniffer et probe).

c. **Le choix d'une approche de sécurité** détermine si la sécurité du réseau nécessite de : ne rien autoriser, n'autoriser que, autoriser tout sauf, ou tout autoriser.

d. **Le choix des moyens nécessaires pour pallier aux défaillances de sécurité** s'agit d'acheter le matériel et les logiciels appropriés aux besoins et à la politique adoptée.

I.3.2 Vulnérabilités

Tous les systèmes informatiques sont vulnérables. Peu importe le niveau de vulnérabilité de ceux-ci. Une vulnérabilité appelée parfois faille ou brèche représente le niveau d'exposition face à la menace dans un contexte particulier. Une vulnérabilité informatique est spécifiquement une faiblesse dans un composant matériel ou logiciel qui permet d'atteindre l'intégrité et la confidentialité des données personnel. C'est-à-dire un attaquant se permet d'avoir accès non autorisé ou vole et contourner l'information, mais généralement un attaquant cherche l'exploitation des bugs dans un logiciel. Exemples de vulnérabilités : [11]

- Utilisation des mots de passe non robustes ;
- Présence de comptes non protégés par mot de passe ;
- La sécurité est chère et difficile: Les organisations n'ont pas de budget pour ça ;
- La sécurité ne peut être sûre à 100%, elle est même souvent inefficace ;
- La politique de sécurité est complexe et basée sur des jugements humains ;
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre) : [1]

a. **Vulnérabilités humaines** : L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, sur exploitation, etc.). Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI.

b. **Vulnérabilités technologiques :** Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT (Computer Emergency Readiness ou Response Team).

c. **Vulnérabilités organisationnelles :** Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées.

d. **Vulnérabilités mise en œuvre :** Les vulnérabilités au niveau mise en œuvre peuvent être dues au non prise en compte de certains aspects lors de la réalisation d'un projet.

I.3.3 Risques

Les risques sont la combinaison des menaces et des pertes qu'elles peuvent engendrer c'est-à-dire de la potentialité de l'exploitation de vulnérabilité par un élément menaçant et de l'impact sur l'organisme. On remarquera que la notion de risque dépend de l'impact une menace ayant une grande probabilité de se concrétiser, mais ayant un impact nul ne constitue pas un risque nul. Dans le langage courant, l'acceptation du mot "risque" peut-être différente et ne pas intégrer la notion d'impact. Les risques dépendent des paramètres que l'on peut maitriser. Il existe deux types de risques : [11]

- ✓ **Le risque structurel** : dépend de l'organisation de l'entreprise.
- ✓ **Le risque accidentel** : indépendant de tous les facteurs de l'entreprise.

Et il existe quatre niveaux de risque :

- **Acceptables** : Pas de conséquences graves pour les utilisateurs de réseau.
  Exemple : Panne électrique, perte de liaison.
- **Courants** : Pas de préjudices graves au réseau, on répare facilement.
  Exemple : Gestion de réseau, mauvaise configuration, erreur utilisateur.
- **Majeurs** : Dus à des facteurs graves et qui causent de gros dégâts mais récupérable.
  Exemple : Foudre qui tombe sur un routeur.
- **Inacceptables** : Fatals pour l'entreprise, ils peuvent entrainer son dépôt de bilan.
  Exemple : Perte ou corruption des informations importantes.

I.3.4 Menaces

Les menaces représentent les types d'actions susceptibles de nuire dans l'absolu. Ce sont des événements, d'origine accidentelles ou délibérées, capables s'ils se réalisent de causer un dommage au sujet étudié. Le réseau informatique comme tout autre réseau informatique est en proie à des menaces de toutes sortes qu'il convient de recenser. Ceux sont les résultantes d'actions et d'opération du fait d'autrui. [5]

L'expertise sécurité permet de renforcer la protection de l'environnement et de bénéficier d'une meilleure maitrise des risques informatiques tels que : [5]

- Vol de données sensibles.
- Fuite d'information.

- Piratage des équipements par l'utilisation malveillante d'une faille de sécurité d'un logiciel, phishing (réception d'un email qui invite l'utilisateur à naviguer sur un site web contrefait).
- Maladresse, malveillance interne.

I.3.4.1 Catégories de menace

Il existe deux catégories :

➢ **Les menaces accidentelles :** Ne supposent aucune préméditation. Dans cette catégorie, sont repris les bugs logiciels, les pannes matérielles, et autres défaillances "incontrôlables". [4]

➢ **Les menaces intentionnelles :**

- **Les menaces passives** : Consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. [5]

- **Les menaces actives** : Consistent à altérer des informations ou le bon fonctionnement d'un service. Elles reposent sur l'action d'un tiers désirant s'introduire et relever des informations. Dans le cas d'une attaque passive, l'intrus va tenter de dérober les informations par audit, ce qui rend sa détection relativement difficile. En effet, cet audit ne modifie pas les fichiers, ni n'altère les systèmes. Elles se traduisent par différents types d'attaques. [4]

  Parmi ces attaques on distingue : [4]

  ✓ Le brouillage,
  ✓ Le déguisement permettant ainsi la modification des données au cours de leur transmission et la modification de l'identité de l'émetteur ou du destinataire,
  ✓ L'interposition qui consiste en la création malveillante de messages en émission ou en réception.

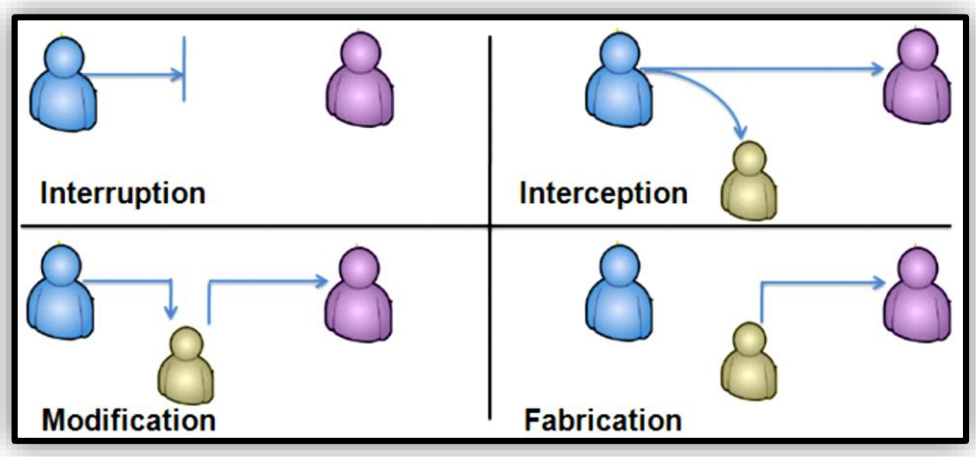


Figure I.1 Types de menaces actives

- Interruption = problème lié à la disponibilité des données
- Interception = problème lié à la confidentialité des données
- Modification = problème lié à l'intégrité des données
- Fabrication = problème lié à l'authenticité des données

I.4 Intrusions

Une intrusion est définie comme une faute malveillante d'origine interne ou externe résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis de la sécurité, c'est-à-dire une violation de la politique de sécurité du système. Le terme d'intrusions sera employé dans le cas où l'attaque est menée avec succès et/ou l'attaquant a réussi à s'introduire et/ou compromettre le système. [1]

Qualifiée d'intrusion, toute action qui a pour fin de compromettre la disponibilité, l'utilité, l'intégrité, l'authenticité, la confidentialité et/ou la possession d'un système d'information. Généralement, une intrusion se manifeste sous l'une formes suivantes : [3]

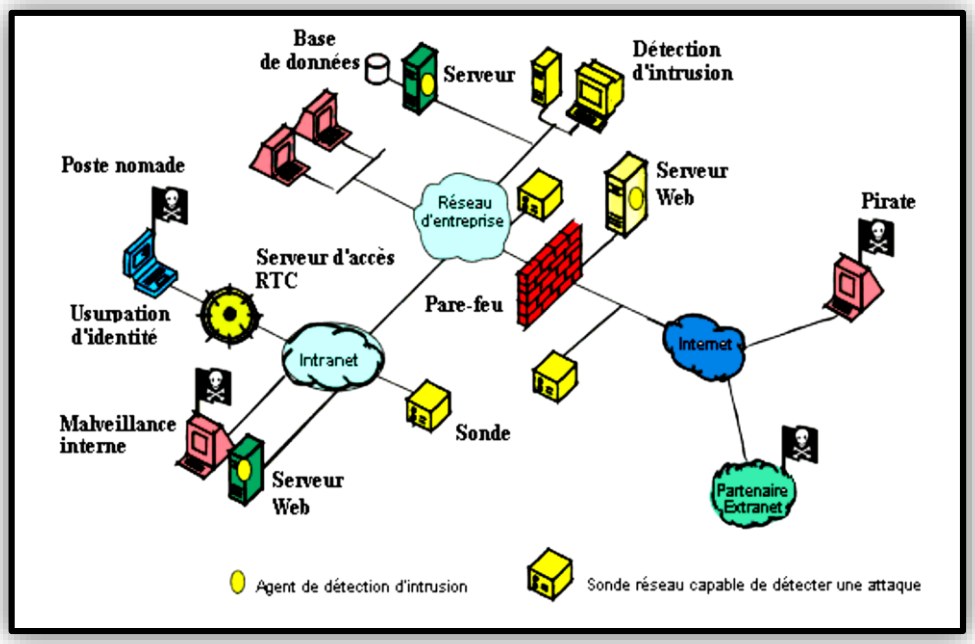


Figure I.2 Environnement dans lequel les intrusions prennent place

- Lire des informations protégées : ces informations peuvent être les données internes d'une compagnie, des numéros de cartes de crédit, des données financières ou des fichiers de mots de passe.
- Changer des informations protégées : modifier ou supprimer des informations protégées d'un système.
- Arrêter un service : empêcher le fonctionnement d'une machine ou d'un service.
- Usurper l'identité d'un ordinateur pour attaquer d'autres systèmes derrière un système de pare-feu.

Le principal moyen pour prévenir les intrusions est le coupe-feu. Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés ne politique de gestion des accès et des mots de passe est complémentaire. [7]

I.5 Logiciels malveillants

Ce sont des logiciels développés par des hackers dans le but de nuire à un système d'informations. Parmi ces logiciels on peut citer :

- **Les Virus :** Un virus est un segment de programme parasite. Il n'est pas forcément auto propage-able. Son but est de grignoter des ressources système : CPU, mémoire, espace disque, bande passante... Ces petits bouts de programme sont dépendants du système d'exploitation ou d'un logiciel. Ils se propagent, comme toutes données binaires, par disquettes, CD ROM, réseaux. [8]

Les virus peuvent être classés suivant leur mode de propagation et leurs cibles : [1]

  - **Le virus de boot** : Il est chargé en mémoire au démarrage et prend le contrôle de l'ordinateur.
  - **Le virus d'application** : Il infecte les programmes exécutables, c'est-à-dire les programmes (.exe, .com où .sys) en remplaçant l'amorce du fichier, de manière à ce que le virus soit exécuté avant le programme infecté. Puis ces virus rendent la main au programme initial, camouflant ainsi leur exécution aux yeux de l'utilisateur.
  - **Le macro virus** : Il infecte des logiciels de la suite Microsoft Office les documents bureautiques en utilisant leur langage de programmation, qui contaminera tous les documents basés sur lui, lors de leur ouverture.

- **Les Vers :** Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour dupliquer. Le ver a habituellement un objectif malicieux, par exemple : [6]

  - Espionner l'ordinateur dans lequel il réside ;
  - Offrir une porte dérobée à des pirates informatiques ;
  - Détruire des données sur l'ordinateur infecté ;
  - Envoyer de multiples requêtes vers un serveur internet dans le but de le saturer.

- **Les chevaux de Troie :** Un cheval de Troie est une forme de logiciel malveillant déguisé en logiciel utile. Son but, se faire exécuter par l'utilisateur, ce qui lui permet de contrôler l'ordinateur et de s'en servir pour ses propres fins. Généralement d'autres logiciels malveillants seront installés sur votre ordinateur, tels que permettre la collecte frauduleuse, la falsification ou la destruction de données. Un cheval de Troie peut par exemple : [6]

  - Voler des mots de passe ;
  - Copier des données sensibles ;
  - Exécuter toute autre action nuisible.

- **Les logiciels espions :** (Espiogiciel ou logiciel espion) est un programme ou un sous-programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs. [1]

- **Le Keylogger :** Un keylogger (littéralement enregistreur de touches) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage. Certains keyloggers sont capables d'enregistrer les URL visitées,

les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur. [11]

- **Le logiciel publicitaire :** Est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur. [5]

- **Le spam :** Est correspond à l'envoi intempestif de courriers électroniques, publicitaires ou non, vers une adresse mail. Le spam est une pollution du courrier légitime par une énorme masse de courrier indésirable non sollicité. [5]

- **Une bombe logique :** Est la partie d'un virus, d'un cheval de Troie ou de tout autre logiciel malveillant qui contient les fonctions destinées à causer des dommages dans l'ordinateur ou le réseau infecté. Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de bombe à retardement ou de bombe temporelle), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur. [5]

I.6 Attaques

I.6.1 Définition

Une attaque est définie comme faute d'interaction malveillante visant à violer une/ou plusieurs propriétés de sécurité veut dire que les attaques représentent les moyens d'exploiter une vulnérabilité. Ils s'appuient sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation ou bugs et les Mauvaises configurations. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.). [7]

I.6.2 Principe de fonctionnement d'une attaque

I.6.2.1 Motivations d'une attaque

Les motivations des attaques peuvent être liées à divers objectif : [1]

- Obtenir un accès au système ;
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Collectionner des informations personnelles sur un utilisateur ;
- Espionnage ou faire du chantage ;
- Troubler le bon fonctionnement d'un service ;
- Le désir d'argent (voler un système bancaire par exemple) ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

I.6.2.2 Différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma et le même principe : [10]

- Identification de la cible
- Le scanning
- L'exploitation
- La progression

I.6.3 Scénarios d'attaques

Les réseaux sont susceptibles aux différentes attaques qui tentent d'exploiter ses différentes vulnérabilités pour mener des manipulations malicieuses. Les attaques peuvent se produire de différentes manières (scénarios). La classification de ces attaques dépend de plusieurs paramètres : [12]

- **Interne vs Externe :** Les attaques peuvent aussi être classées en deux catégories, à savoir les attaques externes et les attaques internes, selon le domaine de l'attaque. Les attaques externes sont effectuées par des nœuds qui n'appartiennent pas au domaine du réseau. Les attaques internes sont entreprises par des nœuds compromis, qui font partie du réseau. Les attaques internes sont plus graves par rapport aux attaques externes car l'attaquant connaît des informations précieuses et secrètes, et possède un accès privilégié au réseau.

- **Individuelle vs Distribuée :** Les attaques peuvent enfin être classées en attaques individuelles ou attaques distribuées. Les attaques individuelles sont simples et ils sont issus d'une seule source et par un chemin simple sans utiliser des stations intermédiaires. Par contre, une attaque distribuée est une attaque évoluée invoquant plusieurs stations ou provenant de plusieurs sources. Les attaques distribuées sont plus dangereuses et difficiles à détecter puisqu'ils utilisent plusieurs stations intermédiaires, ce qui a pour effet la difficulté de déterminer la source d'une telle attaque.

- **Active vs Passive :** Une attaque passive obtient les données échangées dans le réseau sans perturber le fonctionnement de la communication, tandis qu'une attaque active implique l'interruption d'information, la modification, ou la fabrication, ce qui perturbe le fonctionnement normal du réseau.

Il existe quatre cas possible pour mener une attaque active : [6]

- **Attaque par interruption :** C'est une attaque protée à la disponibilité. La destruction d'une pièce matérielle (tel un disque dure), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichier en sont des exemples.

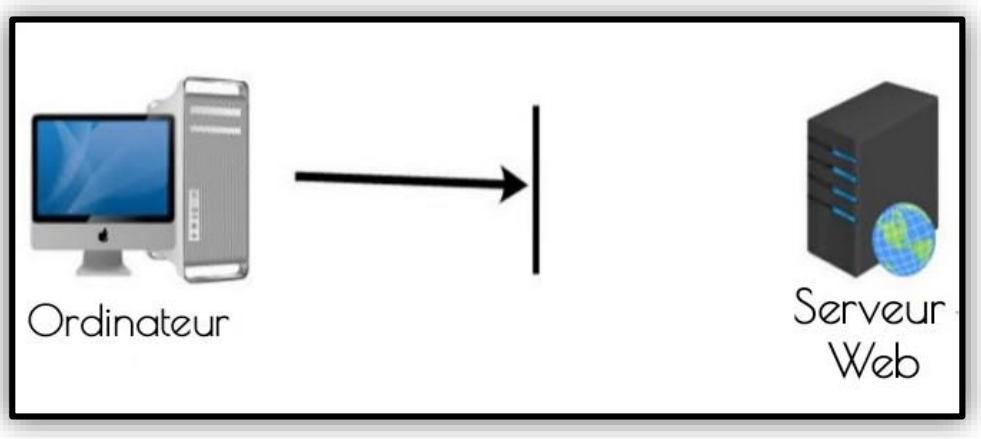


Figure I.3 Attaque par interruption

- **Attaque par interception :** C'est une attaque portée à la confidentialité. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichier ou de programme en sont des exemples.

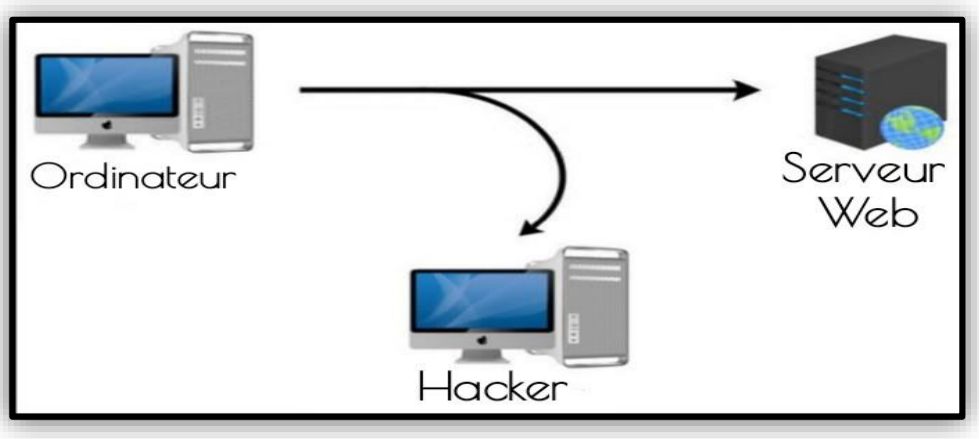


Figure I.4 Attaque par interception

- **Attaque par modification :** Il s'agit d'une attaque portée à l'intégrité. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques.

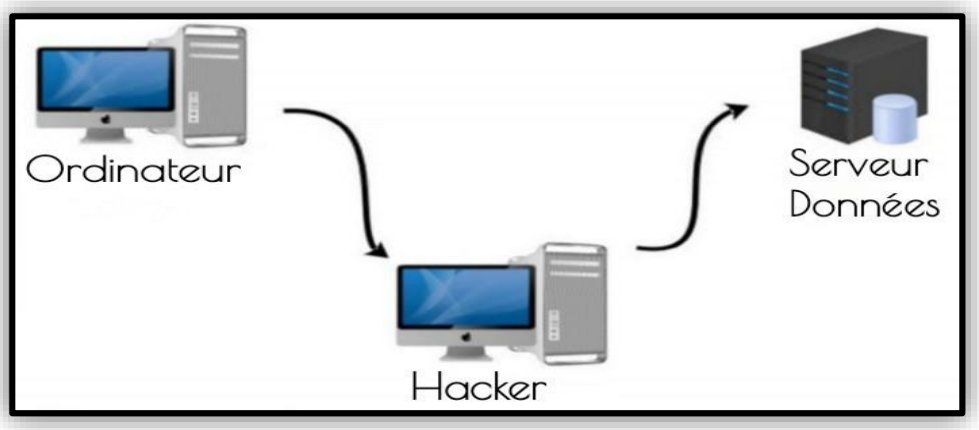


Figure I.5 Attaque par modification

- **Attaque par fabrication :** C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier.

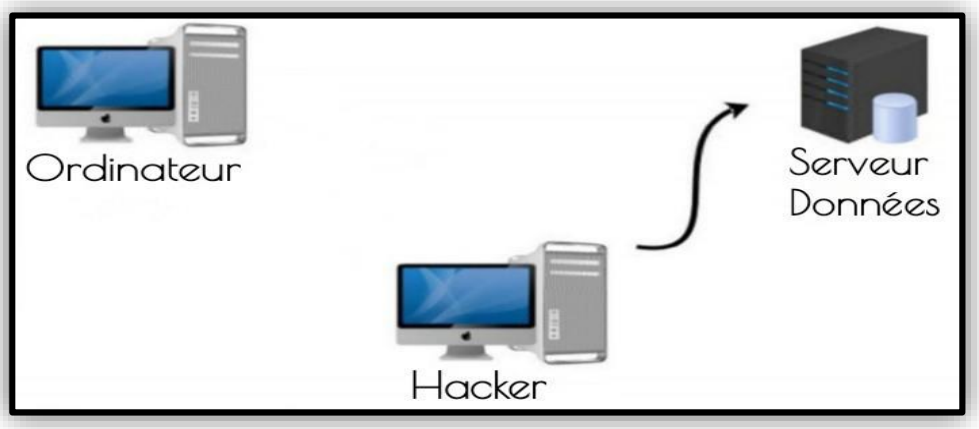


Figure I.6 Attaque par fabrication

I.6.4 Types d'attaques

Les pirates utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois familles différentes : [8]

- **Attaque directe :** C'est la plus simple des attaques. Le pirate attaque directement sa victime à partir de son ordinateur. La plupart des hackers utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

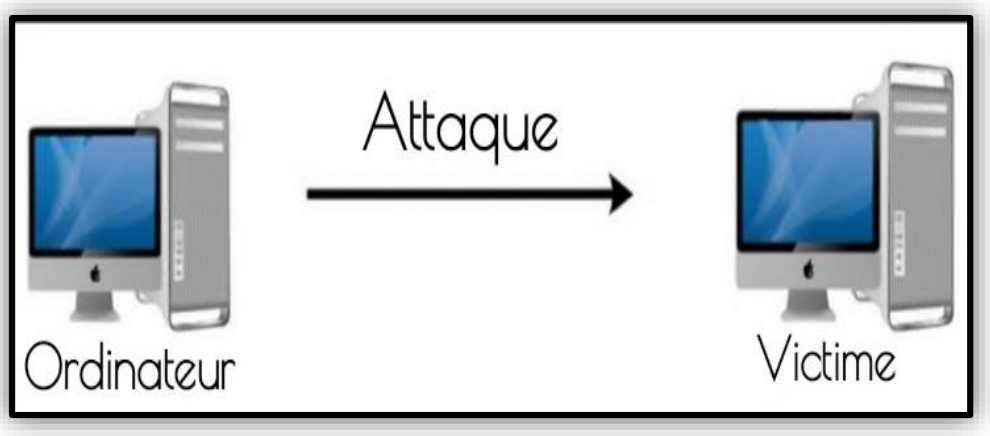


Figure I.7 Attaque directe

- **Attaque indirecte par rebond :** Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

  - Masquer l'identité du pirate
  - Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant pour attaquer.

Le principe en lui-même, est simple car Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme par rebond.

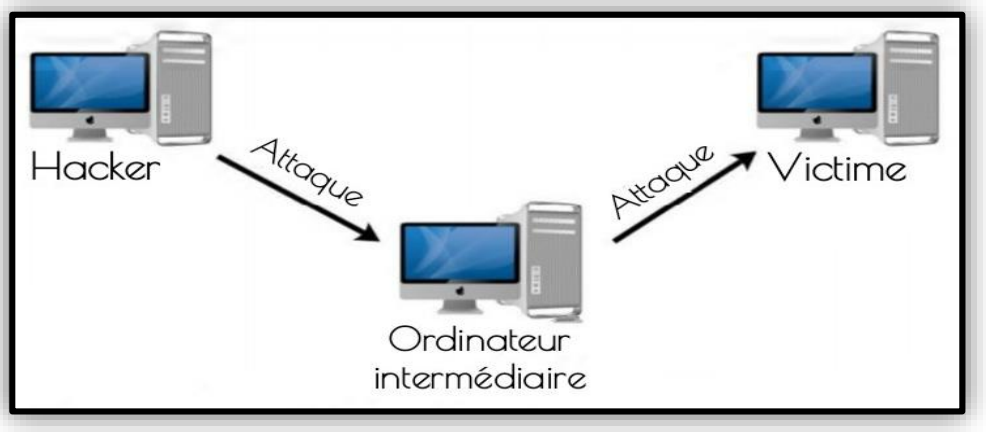


Figure I.8 Attaque indirecte par rebond

- **Attaque indirecte par réponse :** Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du pirate. Mais au lieu d'envoyer une attaque à l'ordinateur

intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

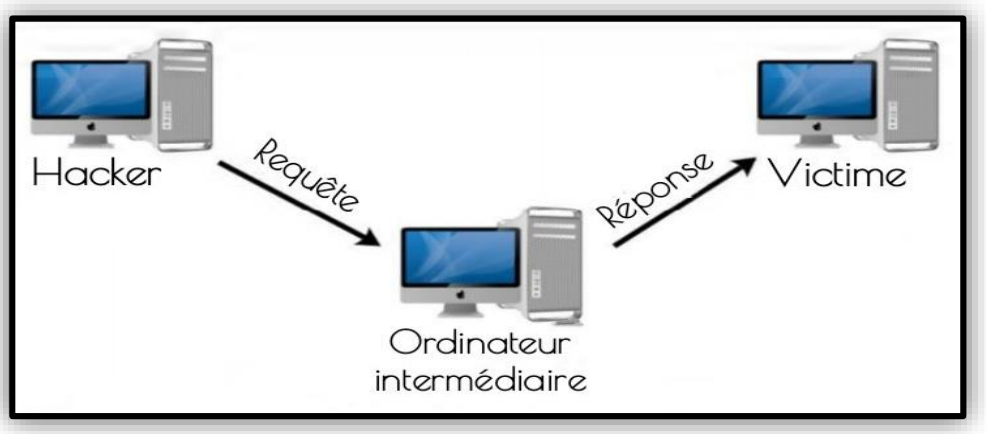


Figure I.9 Attaque indirecte par réponse

I.6.5 Modèles d'attaques

I.6.5.1 Les attaques réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation. Nous présenterons dans ce qui suit quelques attaques bien connues comme : [2]

- **Les techniques de scan :** Le scan de ports est une méthode pour déterminer le type d'attaque que l'on peut lancer sur une machine ciblée. Cette technique consiste à rapporter des informations sur les machines scannées, et en particulier le système d'exploitation et les services installés. On peut donc déterminer avec précision les failles de sécurités et donc les types d'attaques possibles sur la machine en question. [2]

- **IP Spoofing** : L'usurpation d'une adresse IP d'une machine est utilisée pour cacher sa véritable identité, et donc de se faire passer pour quelqu'un d'autre, le plus souvent une machine de confiance du réseau attaqué. Le principe de cette attaque consiste à la création des paquets IP en modifiant l'adresse IP Source. Cependant, d'autres mécanismes doivent être mis en place, sinon la réponse au paquet ne retournera pas à son émetteur, du fait de la falsification de l'adresse IP. De ce fait la réponse est retournée à la machine "spoofée". Cette technique peut être utile dans le cas d'authentification basée sur une adresse IP. Pour ce faire, il existe des utilitaires qui permettent de modifier les paquets IP ou de créer ses propres paquets tels que "hping2". Grâce à ces utilitaires, il est possible de spécifier une adresse IP différente de celle que l'on possède, et ainsi se faire passer pour une autre machine. [2]

- **DNS spoofing :** Le but de cette attaque est de fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine afin de rediriger à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer ses informations en toute confiance tel que les identifiants. Il existe deux techniques pour effectuer cette attaque. [2]

  - **DNS cache poisoning** : Les serveurs DNS possèdent un cache permettant de garder pendant un certain temps la correspondance entre un nom de machine et son adresse IP. Le DNS Cache Poisoning consiste à corrompre ce cache avec de fausses informations. Ces fausses informations

sont envoyées lors d'une réponse d'un serveur DNS contrôlé par le pirate à un autre serveur DNS, lors de la demande de l'adresse IP d'un domaine. Le cache du serveur ayant demandé les informations sera alors corrompu. [2]

- **DNS ID Spoofing** : Pour communiquer avec une machine, nous devons disposer de son adresse IP. Nous pouvons toutefois avoir son nom, et grâce au protocole DNS, nous pouvons obtenir son adresse IP. Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste à récupérer ce numéro d'identification (en sniffant le réseau) lors de la communication entre un client et un serveur DNS, puis, envoyer des réponses falsifiées au client avant la réponse du serveur DNS légitime. [2]

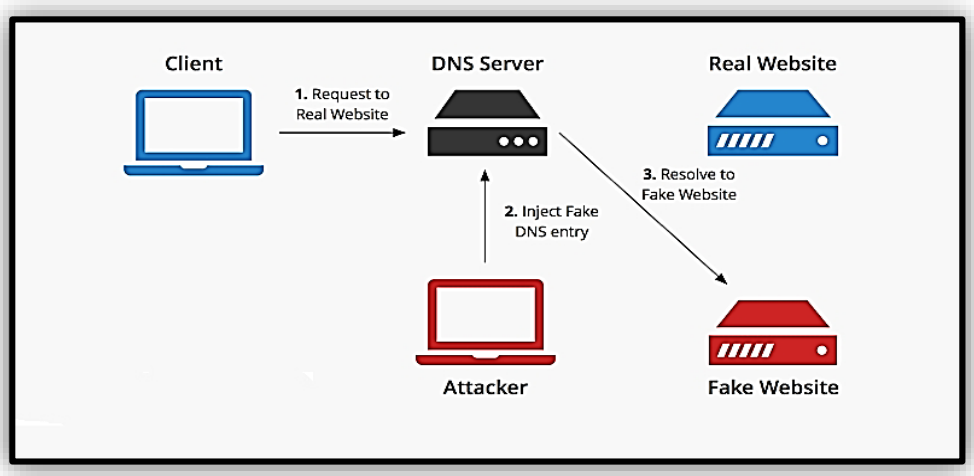


Figure I.10 Attaque DNS spoofing

➢ **ARP spoofing :** Est une attaque très puissante qui permet en général de sniffer le trafic sur le réseau en s'interposant entre une/ou des victimes et la passerelle. Elle permet même de sniffer et récupérer des mots de passes sur des connexions sécurisés SSL. L'attaque inonde le réseau avec des trames ARP liant l'adresse physique de l'attaquant avec la passerelle. De cette manière, le cache ARP des victimes est corrompu et tout le trafic est redirigé vers le poste de l'attaquant. [8]

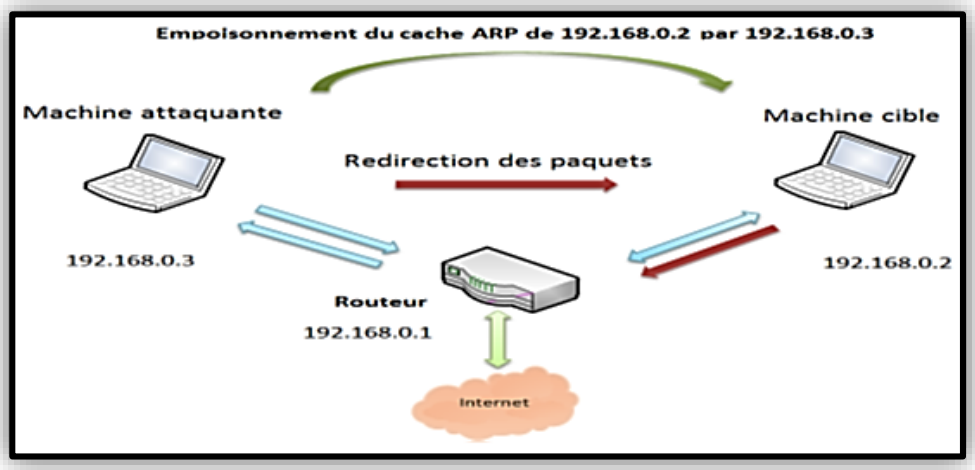


Figure I.11 Attaque ARP spoofing

- **DHCP spoofing** : Une des possibilités pour une personne malveillante d'accéder au trafic réseau est de s'approprier les réponses envoyées par un serveur DHCP autorisé sur le réseau. Le périphérique de mystification DHCP répond aux requêtes DHCP clientes. Le serveur légitime peut lui aussi répondre, mais si le périphérique de mystification agit sur le même segment que le client, sa réponse au client peut parvenir en premier. La réponse DHCP du pirate fournit des informations de prise en charge et une adresse IP qui le désignent comme passerelle par défaut ou serveur DNS (Domain Name System). S'il s'agit d'une passerelle, les clients transmettent alors les paquets au périphérique " attaquant " qui, à son tour, les transmet vers la destination voulue. Nous parlons alors d'attaque de l'intercepteur. Ce type d'attaque peut passer complètement inaperçu puisque le pirate intercepte le flux de données sur le réseau. [2]

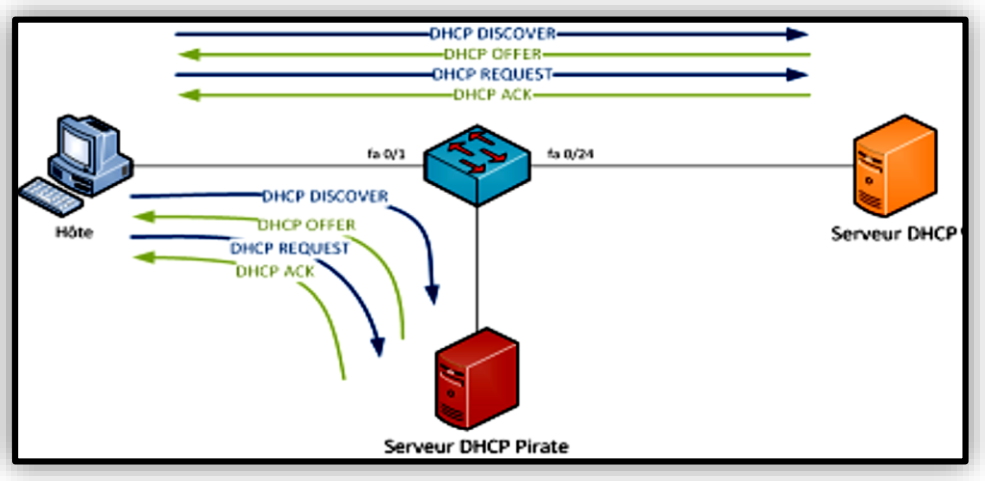


Figure I.12 Attaques DHCP spoofing

- **Tear Drop Attack :** Elle consiste à envoyer des paquets IP invalides à la cible, ces paquets peuvent être fragmentes, ou contenir des données corrompues ou qui dépassent la taille réglementaire. Sur certains systèmes comme les Windows avant 98 ou les Linux avant 2.0.32, ces paquets ne peuvent être interprétés et rendrons la machine inopérante. [8]

I.6.5.2 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, comme précédemment, il est possible de classifier ces attaques selon leur provenance. [2]

- **Les problèmes de configuration** : Il est très rare que les administrateurs réseaux configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. D'autant plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants ou mettant en jeu l'intégrité du système d'exploitation. [2]

- **Les buffers overflow :** Appelées aussi les dépassements de la pile, sont une catégorie de bug particulière issus d'une erreur de programmation, ils permettent l'exploitation d'un shellcode à distance. Ce shellcode permettra à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction. [2]

- **Man in the middle :** L'un des actes de piratage les plus sophistiqués qu'un utilisateur non autorisé puisse commettre est celui que l'on appelle l'attaque de l'intercepteur (L'homme au milieu). C'est une attaque qui a pour but de récupérer des données sensibles qui transitent sur le réseau local. Cette attaque fait intervenir trois machines : un serveur cible, un poste client et la machine où se trouve l'attaquant. L'objectif de cette attaque est d'intercepter les communications par la machine de l'attaquant entre le serveur cible et le poste client, sans que les entités concernées ne puissent se douter de la compromission du canal de communication. [2]

Figure I.13 Man in the middle

I.6.5.3 Le Déni de Service

Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières : par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable ou bien de manière applicative en crashant l'application à distance. L'utilisation d'un buffer overflow peut permettre de planter l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie, etc.) voire un système complet. Nous présenterons dans ce qui suit quelques attaques réseaux connues permettant de rendre indisponible un service. [2]

- **Le Smurf :** Les attaques Smurf profite d'une faiblesse d'IPv4 et d'une mauvaise configuration pour profiter des réseaux permettant l'envoi de paquets au broadcast. Le broadcast est une adresse IP qui permet de joindre toutes les machines d'un réseau. L'attaquant envoie au broadcast des paquets contenant l'IP source de la victime ainsi chaque machine sur le réseau va répondre à la cible à chaque requête de l'attaquant. On se sert du réseau comme un amplificateur pour perpétrer l'attaque, cette méthode porte aussi le nom d'attaque réfléchie permettant à l'attaquant de couvrir ces traces et de rendre l'attaque plus puissante. [8]

- **UDP Flooding :** Le but de cette attaque consiste à envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP. [2]

- **Le PING flood** : Elle consiste à simplement envoyer un nombre maximal de PING simultané jusqu'à saturer la victime. On utilise généralement la commande Ping sous Linux mais une des conditions pour que l'attaque soit efficace est de posséder plus de bande passante que la victime. [8]

- **Le SYN flood** : Cette attaque utilise des paquets TCP contenant le flag SYN. Ce flag signifie initier une connexion avec la cible. En envoyant un nombre très important de ces paquets, on oblige le serveur

à démarrer un socket de connexion pour chaque requête, il enverra donc des paquets contenant les flags SYN, ACK pour établir la connexion mais ne recevra jamais de réponses. Le serveur ayant arrivé à saturation à cause de la grande fille d'attente de connexion ne pourra plus pouvoir répondre aux connexions légitimes des utilisateurs. [W1]

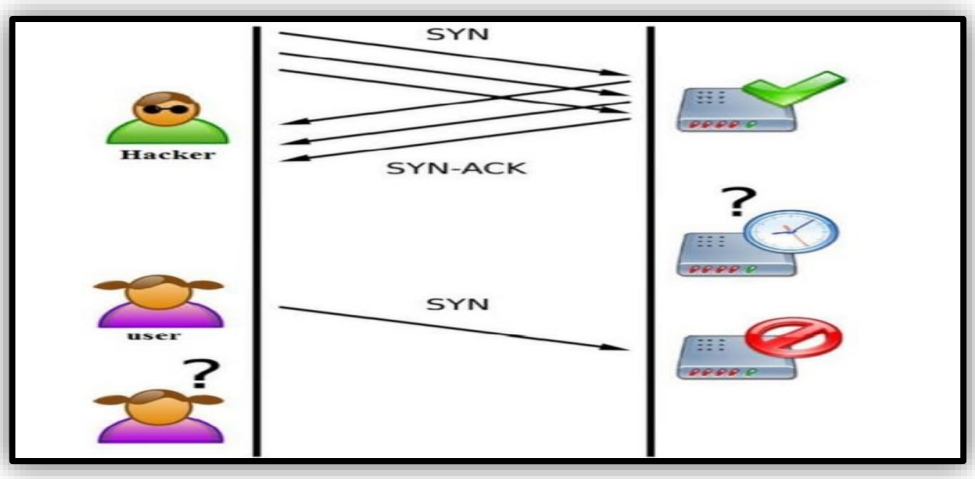


Figure I.14 Attaque SYN Flood

- **Les attaques distribuées :** La plupart des attaques citées plus haut, peuvent être exécutés de manière distribuée, on parle de DDoS (Distributed Denial of Service). Les attaques distribuées se basent sur le fait d'attaquer une cible toute seule se traduit souvent par un échec, alors que si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir.

  Le but de cette attaque consiste à reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles (buffer overflows, failles RPC, etc) il va pouvoir prendre le contrôle de machines à distance et ainsi pouvoir les commander à sa guise. Une fois ceci effectué, il ne reste qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flood pourra rendre une machine ou un réseau totalement inaccessible. [W2]

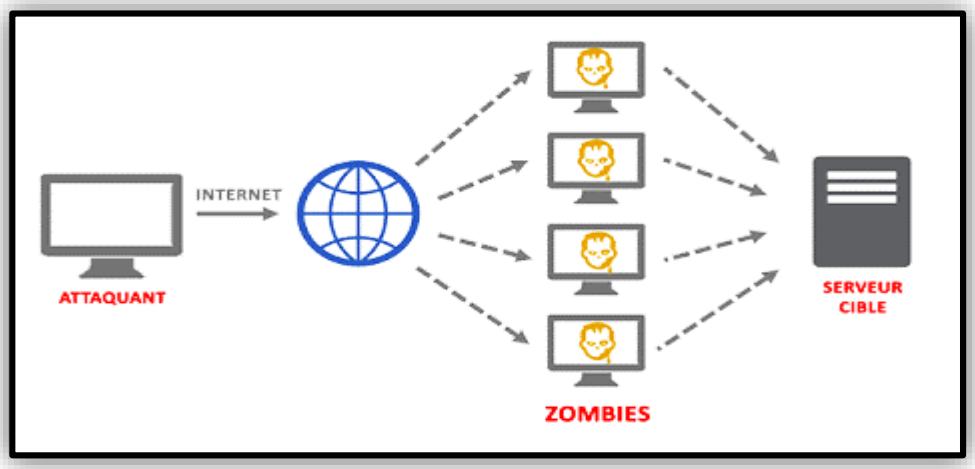


Figure I.15 DDoS Attaque

I.6.5.4 Autres attaques courantes

- **Port scanning** : Ceci constitue en fait une « pré-attaque » (étape de découverte). Elle consiste à déterminer quels ports sont ouverts afin de déterminer quelles sont les vulnérabilités du système. Le firewall va, dans quasiment tous les cas, pouvoir bloquer ces scans en annonçant le port étant comme « fermé ». Elles sont aussi aisément détectables car elles proviennent de la même source faisant les requêtes sur tous les ports de la machine. Il suffit donc au firewall bloquer temporairement cette adresse afin de renvoyer aucun résultat au scanner. [27]

- **Les Exploits** : Se font en exploitant les vulnérabilités des logiciels installés, par exemple un serveur http, FTP … etc. Le problème est que ce type d'attaque est très souvent considéré comme des requêtes tout à fait « valides » et que chaque attaque est différente d'une autre, vu que le bug passe souvent par reproduction de requêtes valides non prévues par le programmeur du logiciel. Autrement dit, il est quasiment impossible au firewall d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent.la seule solution est la mise à jour périodique des logiciels utilisées afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes. [27]

- **Porte dérobée :** C'est un moyen de contourner les mécanismes de contrôle d'accès. Elle s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle. [38]

- **Le Mail Bombing** (Bombardement de courriels) : Elle consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires. L'objectif étant de : [8]

    - Saturer le serveur de mails ;
    - Saturer la bande passante du serveur et du ou des destinataires ;
    - Rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

- **Ingénierie sociale*:*** C'est une technique qui a pour but d'extirper des informations à des personnes. Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par internet et par contact direct. [1]

I.7 Gestion de la sécurité

La gestion de la sécurité est un processus permettant d'assurer la sécurité en intégrant les aspects organisationnels et technologiques. Ce processus permet d'identifier les biens à protéger et de développer des stratégies de protection contre les menaces éventuelles. L'objectif principal de la gestion de la sécurité est de cadrer les besoins de sécurité et de définir une stratégie globale afin d'assurer le niveau de sécurité requis sur réseaux et les systèmes d'informations. Dans le cadre de la gestion de la sécurité d'un système d'information. Les six principes à la base de la gestion de la sécurité réseaux sont : [37]

1. **Adapter une démarche globale** : L'objectif est la cohérence d'ensemble de la démarche de sécurisation des systèmes d'information. Il convient à ce titre de n'oublier aucun élément pertinent, pour éviter toute faille qui réduirait la sécurité globale du système d'information.

2. **Adapter la sécurité du système d'information selon les enjeux** : Il est recommandé que la sécurité du système d'information soit adaptée aux enjeux du système et aux besoins de sécurité, afin d'y consacrer les moyens financiers et humains juste nécessaires mais suffisants.

3. **Gérer les risques** : Il est obligatoire de suivre une démarche qui consiste à :
    - Identifier l'ensemble des risques pesant sur le système ;
    - Fixer les objectifs de sécurité, pour répondre de manière proportionnée aux besoins de protection du système et des informations face aux risques identifiés ;
    - En déduire les fonctions de sécurité et leur niveau de mise en œuvre pour atteindre ces objectifs.

4. **Élaborer une politique de Sécurité du Système d'Information (SSI)** : Élaborer une stratégie globale de sécurité permet de définir le cadre d'utilisation du système d'information. Les politiques définissent entre autres les rôles et les responsabilités des différents acteurs, les règles d'utilisation des systèmes et de l'information, les règles permettant de contrôler l'accès sur l'information, les règles d'utilisation des données privées, les règles d'audit, de sauvegarde, etc.

5. **Utiliser les produits et prestataires labellisés pour leur sécurité** : La certification de produits ou prestataires permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à la compétence des professionnels en matière de SSI.

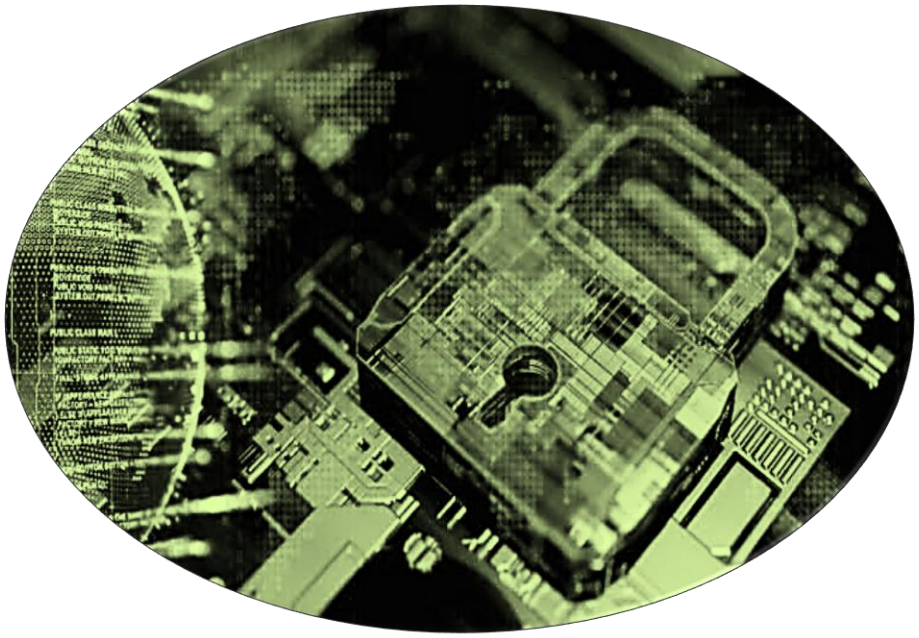
6. **Viser une amélioration continue** : Il est recommandé de chercher une amélioration constante de la SSI, par exemple en mettant en place un « système de management de la sécurité de l'information » (SMSI) pour planifier les actions de sécurisation et les mettre en œuvre puis les vérifier et améliorer la SSI.

I.8 Conclusion

Dans ce chapitre, nous avons présenté un aperçu sur la sécurité des réseaux, ainsi les notions de base et l'importance de la mise en place d'une politique de sécurité en traçant les besoins et les objectifs voulus afin de remédier aux menaces constantes que subi un réseau informatique. Ces menaces se manifestent généralement sous forme d'attaques informatiques que nous avons illustrées dans le but de montrer l'intensité de danger car ces derniers pouvant corrompre le bon fonctionnement d'un réseau.

Dans le but de protéger les réseaux contre les différents types d'attaque, nous allons détailler dans le chapitre qui suit les différentes techniques et solutions existantes (mécanismes de sécurité) pour réduire les risques et lutter contre les attaques.

CHAPITRE II
Modèles & Mécanismes de Sécurité Réseaux



II.1 Introduction

Les messages sur un réseau informatique sont toujours des suites de données binaires, ce qui implique la difficulté de la distinction entre l'original et celui qui est dupliqué. Il faut donc adapter les solutions de sécurité (mécanismes de sécurité) au monde électronique car l'objectif de la sécurité réseaux vise à garantir la confidentialité, l'intégrité et la disponibilité des services. C'est pour cela Il faut mettre en place des mécanismes pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est rendu correctement.

Les mécanismes de sécurité ont une importance capitale dans toute solution de sécurité réseaux. Dans ce chapitre, nous allons survoler les plus pertinents d'entre eux, notamment ceux basés sur la cryptographie symétrique et asymétrique, et ceux basés sur les fonctions à sens unique, les protocoles associés ainsi que les outils de protection des réseaux.

II.2 Mécanisme de sécurité cryptographique (Le Cryptage)

Le cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Bien que le cryptage puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. Pour vérifier l'intégrité ou l'authenticité d'un document, on utilise respectivement un Message Authentification Code (MAC) ou une signature numérique. La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme, suppose en effet que l'ennemi (ou la personne qui veut déchiffrer le message codé) connaisse l'algorithme utilisé. [5]

II.2.1 Cryptographie

Dans les télécommunications modernes, l'information est codée en binaire. Donc, contrairement à la cryptographie classique, la cryptographie moderne manipule des séquences binaires (le message à chiffrer est une suite de bits). [7]

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible, c'est ce qu'on appelle le chiffrement, qui à partir d'un texte en clair donne un texte chiffré ou cryptogramme. [4]

La cryptographie est essentiellement basée sur l'arithmétique, Il s'agit dans le cas d'un texte de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique car le fonctionnement des ordinateurs est basé sur le binaire), puis ensuite de faire des calculs sur ces chiffres pour les modifier de telle façon à les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme par opposition au message initial, appelé message en clair (en anglais plaintext), faire en sorte que le destinataire saura les déchiffrer. [11]

Dans cette partie, nous donnons un aperçu des techniques de cryptographie moderne et de ses deux types à savoir cryptographies symétrique et asymétrique tout en définissant les algorithmes de chiffrement les plus connus. Les techniques de cryptographie moderne se composent de deux grandes parties comme le montre la **figure II.1** :

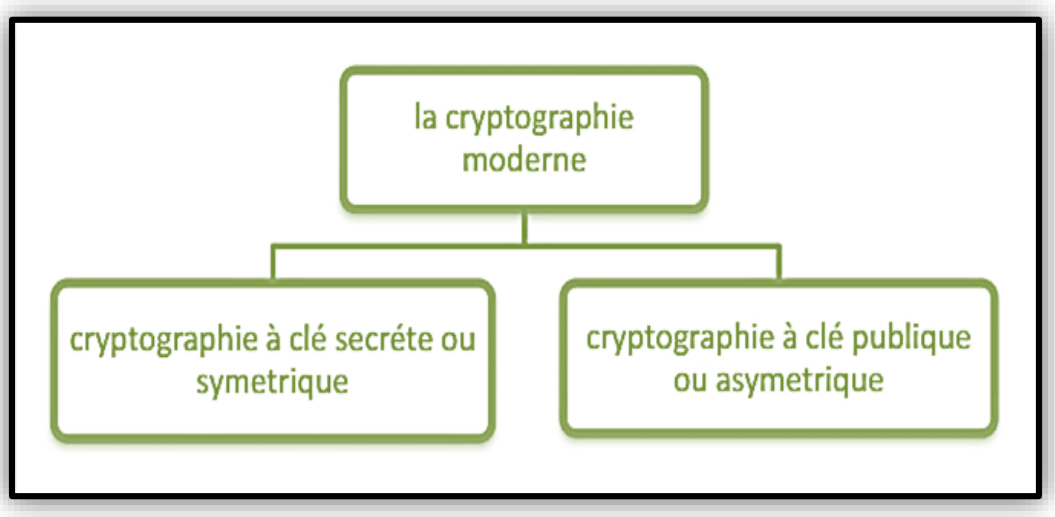


Figure II.1 Techniques de la cryptographie moderne

II.2.1.1 Cryptographie Symétrique

Dans la cryptographie symétrique, la clé de chiffrement est la même que la clé de déchiffrement. De ce fait, la clé doit être un secret partagé uniquement entre l'émetteur et le destinataire. Il existe plusieurs algorithmes qui fonctionnent sur ce principe : DES, 3DES, RC4, RC5, IDEA, AES. [4]

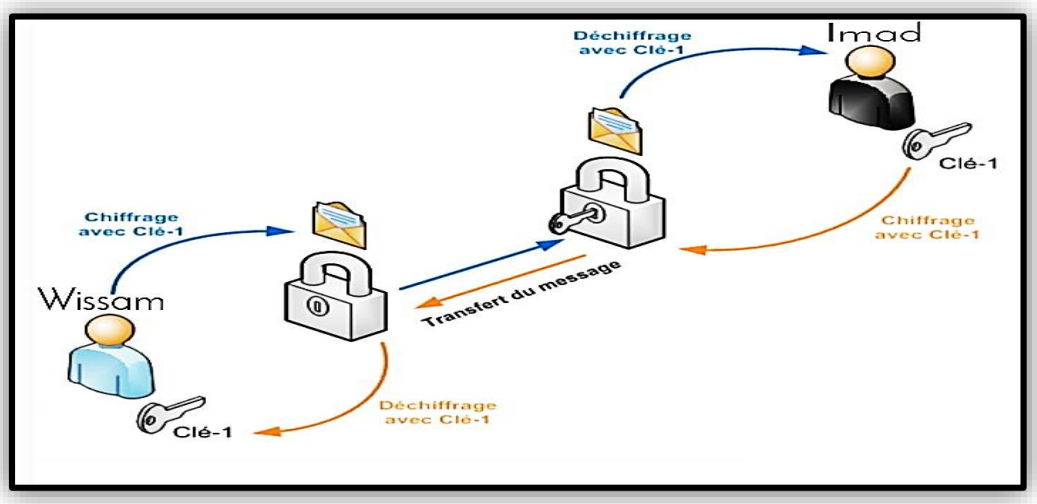


Figure II.2 Principe du chiffrement symétrique

- **Types de chiffrement symétrique**

Les méthodes de chiffrement symétrique se divisent naturellement en deux familles, le chiffrement par bloc et le chiffrement par flot décrites ci-dessous :

1. **Chiffrement par bloc**

Dans un algorithme de chiffrement par bloc, chaque message clair est découpé en blocs de taille fixe de même longueur et chiffré à l'aide d'une clé unique. Ces algorithmes sont en général construits sur un modèle itératif. Il utilise une fonction « F » qui prend une clé secrète « K » et un message « M » de « n » bits. La fonction « F » est itérée un certain nombre de fois (nombre de tours). Lors de chaque tour, la clé « K » est

différente et on chiffre le message qui vient d'être obtenu de l'itération précédente. Les différentes clés « k(i) » qui sont utilisées sont déduites de la clé secrète « K ». [9]

2. Chiffrement par flot

Dans un crypto système par flots, le cryptage des messages se fait caractère par caractère ou bit par bit, au moyen de substitutions générées aléatoirement, la taille de la clé est donc égale à la taille du message. [9]

3. Comparaisons de chiffrement par bloc et par flot :

Le tableau suivant regroupe les caractéristiques de chaque famille. Il est toutefois à remarquer qu'au niveau des applications, chaque type de chiffrement peut être utilisé dans toutes les applications. [4]

Chiffrement par bloc	Chiffrement par flot
Bloc de bit	1 bit à la fois
Débit moyen	Débit élevé
« soft »	Bien adapté à une implémentation « hard »
Transfert de fichiers	Chiffrement de canal de communication
+Réutilisation des clés	+Rapidité, -de code d'implémentation

Tableau II.1 Comparaisons de chiffrement par blocs et par flots

➢ Algorithmes de chiffrement symétrique

Les algorithmes les plus utilisées par le chiffrement symétrique par bloc sont :

- **DES** (Data Encryption Standard) : L'algorithme DES a été adopté comme standard en 1976 par le NBS. Le DES est un réseau de « Feistel » à 16 rondes, à clef « K » de 56 bits diversifiée en 16 clefs de 48 bits, codant des blocs de 64 bits. Il utilise des tables de substitution fixes pour rendre la confusion. Aujourd'hui, l'algorithme DES n'est plus recommandé à cause de sa longueur trop petite de clé et de sa lenteur d'exécution. [25]

- **Triple DES ou 3DES** : C'est l'application successive de trois passes dans l'algorithme DES avec des clés en principes différentes (mais c'est parfois la même qui soit utilisée selon les implémentations). La longueur de la clé est de 168 bits (3*56 bits). Aujourd'hui, l'algorithme 3DES est en passe de disparaître également, parce qu'il est lent et son niveau de sécurité est peu performant. [28]

- **IDEA** (International Data Encryption Algorithm) : Proposé en 1992 par Lai et Massey, il utilise une clé de 128 bits, des données de 64 bits. [4]

- **AES** (Advanced Encryption Standard) : L'algorithme AES est le nouveau standard de chiffrement à clef secrète. Il a été choisi en octobre 2000 parmi les 15 systèmes proposés en réponse à l'appel d'offre lancé par le NIST *(*National Institute of Standards and Technology). Cet algorithme, initialement appelé

RIJNDAEL, a été conçu par deux cryptographes belges, V. Rijmen et J.Daemen. Il opère sur des blocs de message de 128 bits et disponible pour trois tailles de clé différentes: 128, 192 et 256 bits. [33]

Parmi les algorithmes de chiffrement symétrique par flot les plus connus est :

- **RC4** (Rivest Cipher 4) : Cet algorithme a été conçu par Ronald Rivest en 1987. Il est utilisé dans des protocoles comme WEP, WPA ainsi que TLS. Les raisons de son succès sont liées à sa grande simplicité et à sa vitesse de chiffrement. Les implémentations matérielles ou logicielles étant faciles à mettre en œuvre. Le RC4 permet d'initialiser un tableau de 256 octets en répétant la clé autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de mélanger autant que possible le tableau. Au final on obtient une suite de bits pseudo-aléatoires qui peuvent être utilisés pour chiffrer le message via un « XOR ». [10]

II.2.1.2 Cryptographie Asymétrique

Les algorithmes asymétriques sont basés sur une clé pour le chiffrement et une clé associée différent, pour le déchiffrement. La clé publique sert à chiffrer des messages cependant la clé privée sert à déchiffrer les messages chiffrés avec la clé publique correspondante comme le montre la **figure II.3**. La clé publique est connue par tout le monde. Par contre la clé privée doit rester confidentielle, c'est la seule qui permet de déchiffrer les messages. En plus il est impossible de déduire la clé privée de la clé publique. [9]

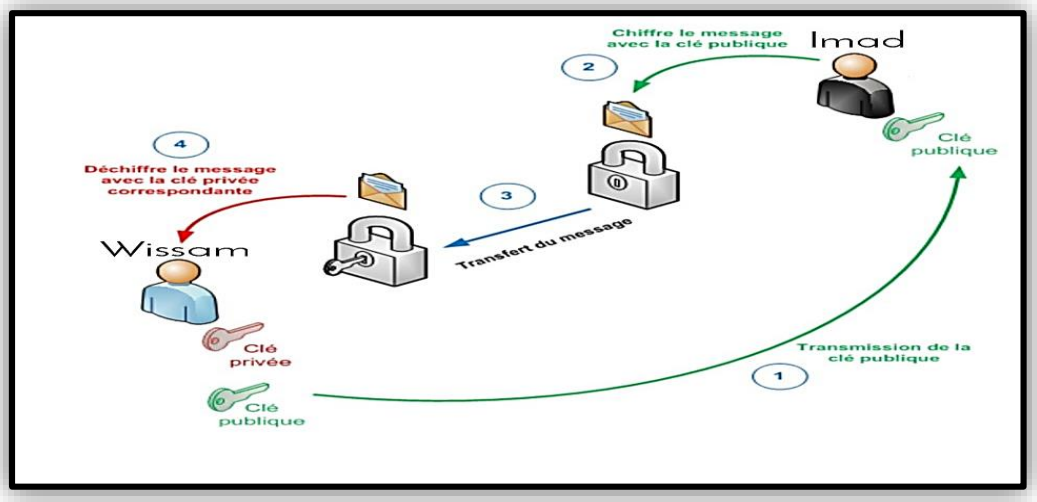


Figure II.3 Principe du chiffrement asymétrique

➢ **Algorithmes de chiffrement asymétrique**

Parmi les algorithmes de cryptographie asymétrique le plus connus est :

- **RSA :** L'algorithme RSA (nommé par les initiales de ses trois inventeurs: Ronald Rivest, Adi Shamir et Leonard Adleman) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme est utilisé pour l'échange sécurisé des clefs, et pour assurer la fonction d'authentification. L'algorithme RSA très efficace pour l'échange des clés des algorithmes symétriques comme l'AES. [25]

- **Principe du RSA :** On possède une paire de clés, l'une publique (e,n) et une privée (d,n). La première étape revient à choisir « n ». Il doit s'agir d'une valeur assez élevée, produit de 2 nombres premiers

très grands « p » et « q ». En pratique, si « p »et « q » ont 100 chiffres décimaux, « n » possèdera 200 chiffres. Selon le niveau de sécurité souhaité, la taille de « n » peut varier : 512, 768, 1024 ou 20483 bits. Dans un second temps, on choisira un très grand entier « e », relativement premier à (p-1) * (q-1). La clé publique sera formée par (e,n). On choisira ensuite un « d » tel que $e*d \equiv 1 \bmod (\Phi(n))$, la clé privée sera donnée par (d,n). [10]

- **Comparaison entre le chiffrement symétrique / asymétrique**

Pour le cryptage la meilleure méthode consiste à combiner les systèmes de clés privés et de clé publique de façon à avoir les avantages concernant la sécurité des clés publiques ainsi que la rapidité des clés privées. Le tableau suivant regroupe les avantages et inconvénients de chaque famille : [4]

Systèmes de chiffrement	Avantages	Inconvénients
Symétrique	▪ Rapidité du système de chiffrement et déchiffrement. ▪ Clé unique pour le chiffrement et déchiffrement. ▪ Taille de clé utilisé pour le chiffrement et déchiffrement est courte. ▪ Facile à implémenter au niveau matérielle car il se base sur des opérations simples.	▪ Nécessite un canal secret pour envoyer les clés secrètes. ▪ Il ne garantit pas la propriété de non-répudiation. ▪ Le changement de clé à chaque communication. ▪ Echange des clés. ▪ Utilisation une signature numérique limitée.
Asymétrique	▪ Aucun canal secret n'est nécessaire pour l'échange des clés publiques. ▪ Assure la signature de message. ▪ Une clé connue de tous et une clé personnelle. ▪ La vérification d'une signature n'exige pas de secret. ▪ Quiconque peut envoyer un message « confidentiel » (chiffré) à un autre utilisateur.	▪ La taille de la clé utilisée pour le chiffrement et le déchiffrement est très grande. ▪ Algorithme très lent par rapport au chiffrement symétrique. ▪ Nécessite des machines puissantes. ▪ Nécessité d'un annuaire et/ou certification de clés publiques.

Tableau II.2 Comparaison entre le chiffrement symétrique/asymétrique

II.2.2 Fonction de hachage

Les fonctions de hachages ou les fonctions à sens unique, sont la quatrième primitive cryptographique. Une fonction de hachage est un algorithme qui prend en entrée un message de taille quelconque et applique un ensemble de transformations pour qu'il revoie en sortie un texte de taille fixe qui varie selon l'algorithme appliqué (128 bits pour MD5 et 160 bits pour SHA-1). Cette sortie est appelée le condensé, valeur de hachage ou résumé de message. [16]

Le résultat de cette fonction est par ailleurs aussi appelé somme de contrôle, empreinte, résumé de message, condensé ou encore empreinte cryptographique lorsque l'on utilise une fonction de hachage

cryptographique. Les fonctions de HASH peuvent être utilisées pour l'authentification de message, dérivation de clé, génération de nombre pseudo aléatoire et génération de la signature numérique. [11]

Une fonction de hachage devrait satisfaire les quatre propriétés suivantes : [16]

- Facilite de calculer l'empreinte du message ;
- Impossible de reconstruire un message d'un condensé donné ;
- Impossible de trouver deux messages différents avec le même condensé ;
- La taille du condensé (par une fonction de hachage donnée) est toujours la même (indépendamment de la longueur du message initial).

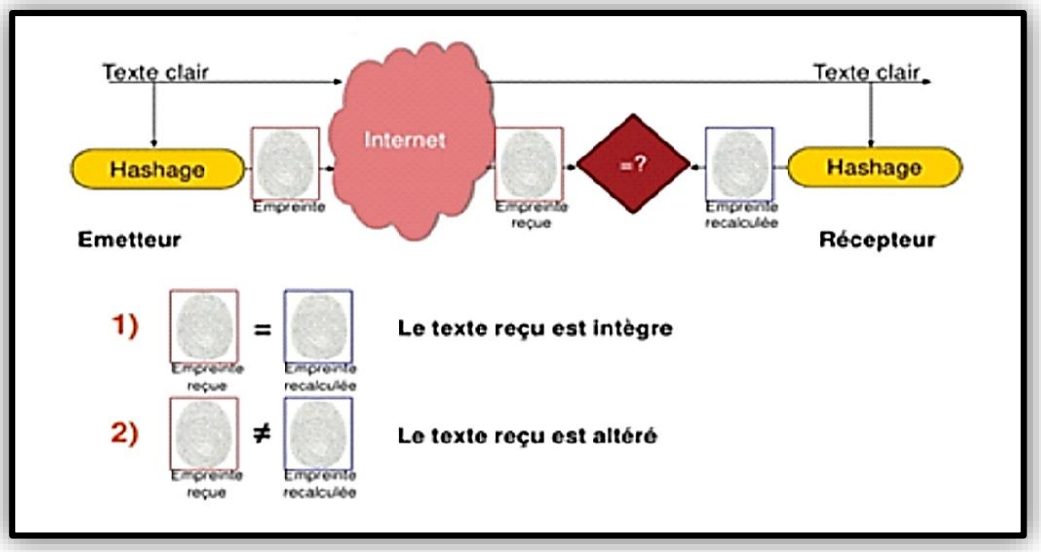


Figure II.4 Fonction de hachage

II.2.2.1 MD5 (MD signifiant Message Digest)

MD5 Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier). [11]

II.2.2.2 SHA (Secure Hash Algorithm)

L'algorithme SHA (Algorithme de hachage sécurisé) a été conçu par NSA, standardisé par NIST. La liste des algorithmes SHA est : SHA-1, SHA-256, SHA-384 et SHA-512. A cause des calculs intensifs dans SHA-384 et SHA-512, ces deux algorithmes ne sont pas recommandés pour être utilisés sur les dispositifs mobiles.

SHA-1 est l'algorithme le plus utilisé dans la famille des algorithmes SHA. SHA-1 prend en entrée un message de taille inférieure à $\mathbf{2^{64}}$ bits et produit une empreinte de 160 bits. SHA-256 prend aussi en entrée un message de taille inférieure à $\mathbf{2^{64}}$ bits mais produit une empreinte de 256 bits.

Il y a une nouvelle attaque sur SHA-1 sans utiliser la force brute, qui trouve des collisions à l'intérieur de 269 opérations hash. A cause de l'avancement technologique et les attaques, NIST a planifié d'abandonner SHA-1 la fin 2010, et recommande des fonctions HASH plus fortes comme SHA-256. Les algorithmes SHA-256, SHA-384 et SHA-512 sont relativement nouveaux et sont aussi standardisés par NIST mais ils sont plus intensifs en calcul et crypto analyses. [11]

II.2.2.3 MAC (Message Authentication Code)

Un code d'authentification de message (MAC) est un code accompagnant des données dans le but d'assurer l'intégrité de ces dernières, en permettant de vérifier qu'elles n'ont subi aucune modification, après une transmission par exemple. Le MAC assure non seulement une fonction de vérification de l'intégrité du message, comme le permettrait une simple fonction de hachage mais de plus authentifie l'expéditeur, détenteur de la clé secrète. Il peut également être employé comme un chiffrement supplémentaire (rare) et peut être calculé avant ou après le chiffrement principal, bien qu'il soit généralement conseillé de le faire avant. [11]

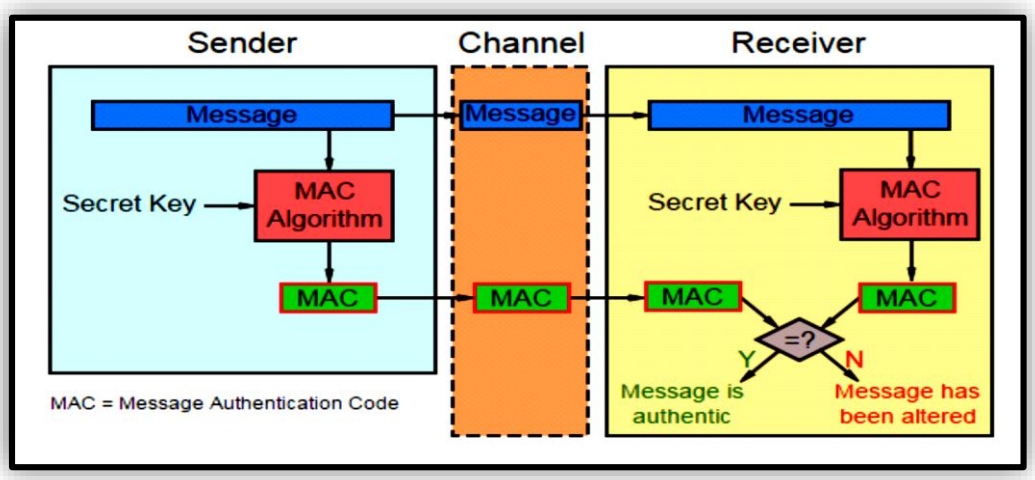


Figure II.5 Code d'authentification de message (MAC)

II.2.2.4 HMAC (keyed-hash message authentication code)

Un HMAC (code d'authentification d'une empreinte cryptographique de message avec clé), est un type de code d'authentification de message MAC, calculé en utilisant une fonction de hachage cryptographique en combinaison avec une clé secrète. Comme avec n'importe quel CAM, il peut être utilisé pour vérifier simultanément l'intégrité de données et l'authenticité d'un message. N'importe quelle fonction itérative de hachage, comme MD5 ou SHA-1, peut être utilisée dans le calcul d'un HMAC ; le nom de l'algorithme résultant est HMAC-MD5 ou HMAC-SHA-1. La qualité cryptographique du HMAC dépend de la qualité cryptographique de la fonction de hachage et de la taille et la qualité de la clé. [11]

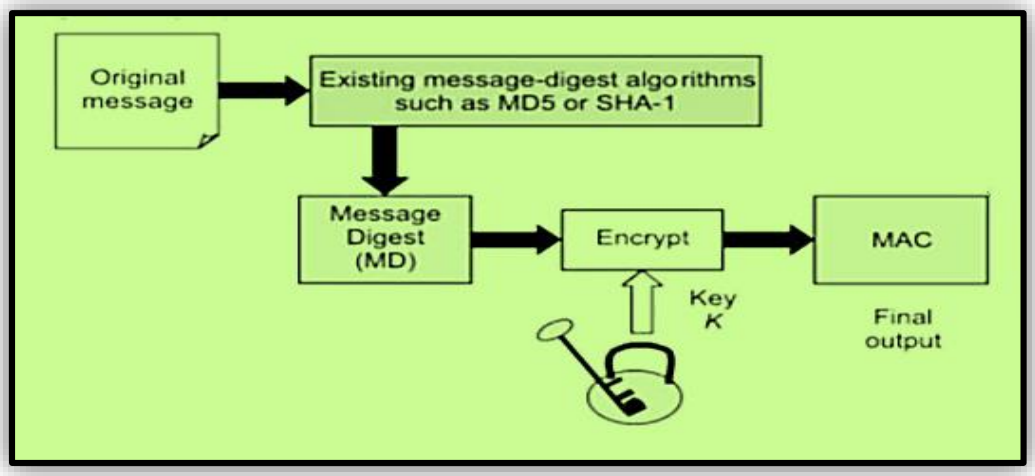


Figure II.6 Code d'authentification d'une empreinte cryptographique de message avec clé

II.2.3 La signature numérique

La signature numérique est un code digital permet à la personne qui reçoit une information de contrôler l'authenticité de son origine, et également de vérifier que l'information en question est intacte. Aussi, les signatures numériques permettent l'authentification et le contrôle de l'intégrité et également la non-répudiation. [15]

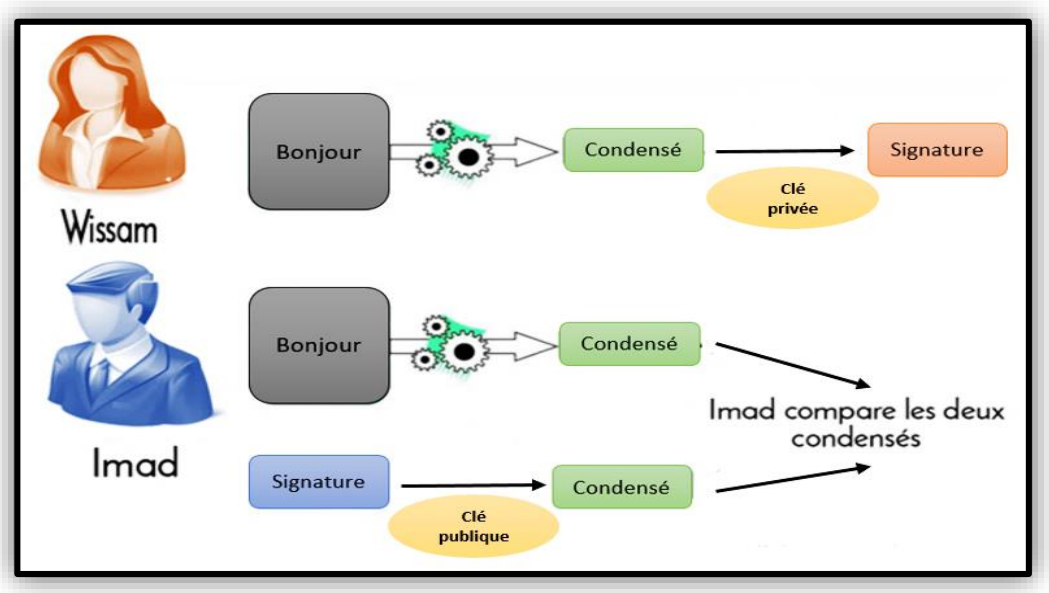


Figure II.7 La signature numérique

➢ **Les principaux algorithmes de signature**

- **Digital Signature Standard (DSS) :**

Proposé par le NIST en 1991, puis finalement adopté en 1994, DSS est la norme de signature numérique du gouvernement Américain. Elle se base sur l'algorithme DSA (Digital Signature Algorithm), qui utilise SHA comme fonction de hachage à sens unique et Elgamal pour la génération et la vérification de la signature. Le DSS, plus connu sous le sigle DSA fait partie de la spécification DSS adoptée en 1993. Une révision mineure a été publiée en 1996 (FIPS 186-1) et le standard a été amélioré en 2002 dans FIPS 186-2. Le DSA est similaire à un autre type de signature développée par « Claus Schnorr » en 1989. Il a aussi des points communs avec la signature ElGamal. Le processus se fait en trois étapes : [10]

- Génération des clés ;
- Signature du document ;
- Vérification du document signé.

- **La signature RSA :**

La signature RSA consiste à appliquer la méthode de RSA. Elle utilise la clé privée pour créer la signature et la clé publique pour la vérification de signature. La procédure de chiffrement est comme se suit : [16]

✓ **L'algorithme de signature RSA :**

1. Calcule h = H(m) où H est une fonction de hachage ;
2. Calcule $S = h^d \bmod n$;
3. Retour (s).

✓ **La vérification de signature de RSA :**

1. Calcule H = H(m) ;
2. Calcule h' = s^e mod n ;
3. Accepte la signature si et seulement si h = h'.

II.2.4 Certificat numérique

Le problème de clés publiques est qu'un pirate peut arriver à remplacer la clé publique d'un utilisateur X par la sienne, par exemple sur un annuaire. Et toutes les personnes croyant encrypter pour l'utilisateur X encrypterons pour le pirate. Les systèmes à clés publiques ne garantissent donc pas que la clé est bien celle de l'utilisateur à qui elle est censée appartenir.

Les certificats électroniques servent à cela: ils permettent de lier de façon sûre une clé publique à une entité (utilisateur, serveur, etc.). Un certificat contient les informations suivantes: un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification émettrice du certificat, la signature du certificat à l'aide de la clé privée de l'autorité de certification. Toutes ces informations sont signées et délivrées par un tiers de confiance appelé: autorité de certification (souvent notée **CA** pour Certification Authority). La clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification. [12]

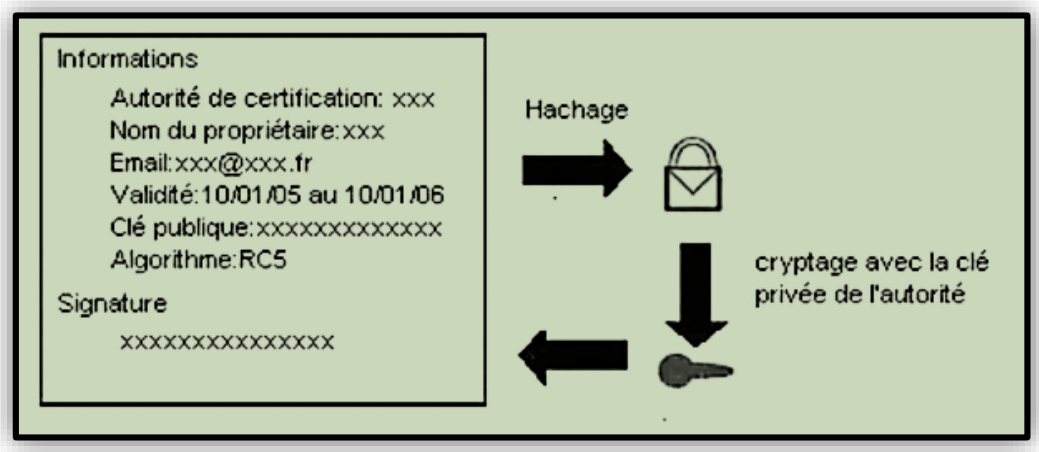


Figure II.8 Création d'un certificat numérique

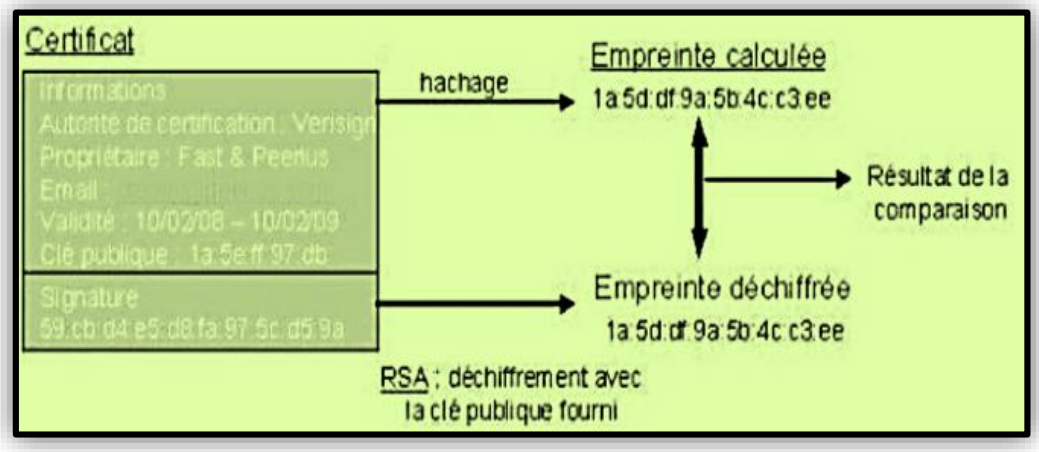


Figure II.9 Vérification du certificat numérique

II.2.5 Objectifs de la cryptographie

Les objectifs de la cryptographie sont multiples, on peut les citer dans le tableau suivant : [10]

Vie privée ou confidentialité	Tenir l'information secrète pour tous sauf pour ceux qui sont autorisés à la voir.
Intégrité de données	L'assurance que l'information n'a pas été changée par des moyens non autorises ou inconnus.
Authentification d'entité ou identification	Confirmation de l'identité d'une entité (par exemple, une personne, un terminal d'ordinateur, une carte de crédit, etc.).
Authentification de message	Corroboration de la source d'information; aussi connue comme authentification d'origine de données.
Validation	De fournir opportunité d'autorisation d'employer ou manipuler information ou ressources.
Témoignage	Vérification de la création ou de l'existence de l'information par une entité autre que le créateur.
Propriété	Moyen de fournir une entité au droit légal d'employer ou transférer une ressource à d'autres.
Signature	Moyen de lier l'information a une entité.
Certification	Endossement d'information par une entité crue.
Contrôle d'accès	Limitation d'accès a ressources de favorise entités.
Horodatage	Enregistrement du temps de création ou l'existence d'information.
Non reniement	Prévention du démenti d'obligation précédentes ou actions.
Révocation	Rétraction de certification ou autorisation.

Tableau II.3 Objectifs de la cryptographie

II.3 Contrôle d'accès

II.3.1 Définition d'un contrôle d'accès

Le contrôle d'accès consiste à vérifier si une entité que ce soit une personne ou un ordinateur demandant d'accéder à une ressource a les droits nécessaires pour le faire. Avec le contrôle d'accès, on s'intéresse à garantir deux propriétés fondamentales : La confidentialité et l'intégrité des informations contenues dans un système informatique. [31]

Le service de contrôle d'accès empêche l'utilisation non autorisée des ressources accessibles par le réseau. On entend par « utilisation » les modes de : lecture, écriture et création et/ou suppression ; et par ressources : les systèmes d'exploitation, les fichiers, les bases de données et les applications. Et pour contrôler les accès aux ressources, il faut d'abord authentifier les utilisateurs afin de s'assurer de leur

identité qui est transportée dans les messages d'initialisation et ensuite établir une liste des droits d'accès associés à chaque utilisateur. [28]

II.3.2 Définition d'une politique de contrôle d'accès

Les politiques de contrôle d'accès sont définies comme étant des directives (règles) de haut niveau qui spécifient qui a la permission d'exercer quoi sur quelle donnée. A partir de cette définition nous dégageons trois concepts fondamentaux d'une politique de contrôle d'accès qui sont : [31]

1. Sujet : Entité active qui accède aux données du système.
   Le sujet peut être un utilisateur, une application, une adresse IP. . .
2. Objet : Entité passive qui représente les données à protéger.
   L'objet peut être, par exemple, un fichier, une table relationnelle, une classe . . .
3. Action : Représente l'action à traiter par le sujet sur l'objet.
   L'action peut être lire, écrire, exécuter.

II.3.3 Listes de contrôle d'Accès (ACL)

Le mécanisme des listes de contrôle d'accès (ACL, Access Control List) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées. [28]

II.3.4 Les modèles fondamentaux du contrôle d'accès

On distingue principalement trois familles de modèles de contrôle d'accès qualifiés respectivement de discrétionnaire, mandataire ou basé sur les rôles.

II.3.4.1 Contrôle d'accès obligatoire (MAC)

Le contrôle d'accès obligatoire ou MAC (Mandatory Access Control) repose sur le principe que la politique de sécurité appliquée sur un système ne doit pas pouvoir être modifiée par les utilisateurs du système.

Pour garantir les propriétés de confidentialité et d'intégrité différents modèles ont été proposées : [20]

- **Bell-Lapadula :** Le modèle de Bell-Lapadula (BLP), formalise la propriété de confidentialité des données dans les milieux militaires.
- **Biba :** Le modèle Biba formalise le dual de Bell et Lapadula pour garantir la propriété d'intégrité d'un système.
- **Domain et Type de renforcement "Domain Type Enforcement-DTE" :** Le modèle Domain and Type Enforcement (DTE) un modèle de contrôle d'accès basé sur une abstraction des ressources du système et créé spécifiquement pour l'écriture de politiques de sécurité.

✓ **Les limites du modèle de contrôle d'accès MAC :** Le contrôle d'accès obligatoire est un système de contrôle d'accès dans lequel la décision de protection ne revient pas au propriétaire de cet outil. Les autorisations d'accès sont établies par l'examen d'attributs de sécurité. [20]

II.3.4.2 Contrôle d'accès discrétionnaire (DAC)

Le contrôle d'accès discrétionnaire ou DAC (Discretionary Access Control) permet de surveiller l'accès des utilisateurs aux ressources d'un système sur la base de l'identité des utilisateurs et des autorisations accordées à ces utilisateurs. Dans ce modèle de contrôle d'accès, c'est l'utilisateur propriétaire de ses ressources qui décide des droits d'accès accordés aux autres utilisateurs sur ses ressources. [29] [20]

- ✓ **Les limites du modèle de contrôle d'accès discrétionnaire :** Ce modèle convient à des systèmes gèrent l'accès d'objet peu sensibles et donne l'avantage de minimiser les couts d'administration car celle-ci peut être déléguée aux utilisateurs. Par contre, ses principes ont, malheureusement, l'inconvénient de ne pas fournir une assurance réelle sur le flux de l'information dans un système et il est souvent facile de contourner les restrictions d'accès. Comme le modèle de contrôle d'accès discrétionnaire limite l'accès aux objets uniquement en se basant sur l'identité de l'utilisateur. Pour cela, le modèle DAC est appelé également IBAC (Identity Based Access Control). [31]

II.3.4.3 Contrôle d'accès basé sur les rôles (RBAC)

Le modèle RBAC (Role Based Access Control) est une politique tels que les droits d'accès sont attribués aux utilisateurs en fonction du rôle qu'ils jouent dans le système d'information est appelée politique par rôle. [29]

Le cœur du RBAC est le rôle. Ce dernier représente d'une façon abstraite une fonction particulière dans une organisation (par exemple : médecin, infirmière, statisticien). Le rôle est une entité intermédiaire entre les permissions d'accès, appelées aussi privilège ou droit d'accès, et les utilisateurs. Il regroupe un ensemble de privilèges qui va être ensuite attribué aux utilisateurs en fonction de leurs positions organisationnelles. Par conséquent, contrairement au contrôle d'accès discrétionnaire, l'utilisateur ne reçoit pas directement ses permissions d'accès, mais les reçoit via des rôles. [31]

II.3.5 Le protocole AAA

Le contrôle d'accès à un système d'information se base sur les trois phases du mécanisme (Authentication Authorization Accounting). Ces phases sont les suivantes :

- ❖ **Authentification**

La première phase qui est l'identification consiste pour un système informatique à vérifier l'identité d'une entité (personne, ordinateur ou Smartphone), afin d'évaluer la sécurité du périphérique "posture" et authentifier l'utilisateur pour l'autoriser à accéder à des ressources protégées du système d'information. Cette première phase consiste à vérifier si l'utilisateur correspond bien à l'identité qui cherche à se connecter. Le plus simple ici consiste à vérifier une association entre un mot de passe et un identifiant. [20]

Il y'a deux méthodes d'authentification sont les suivants :

- **Mot de passe** : L'utilisation de mots de passe est l'une des briques de base dans la sécurisation d'un système et il doit être difficile à retrouver, même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. Le mot de passe doit possède certaines caractéristiques qui sont : non trivial, difficile à deviner et régulièrement modifié. [28] [15]
- **Biométrie** : Est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les

unes plus fiables que d'autres, mais toutes doivent être infalsifiables et unique pour pouvoir être représentatives d'un et un seul individu. Par exemple : empreintes digitales. [27]

❖ **Autorisation**

C'est la fonction spécifiant les droits d'accès vers les ressources liées à la sécurité de l'information et la sécurité des systèmes d'information en général et au contrôle d'accès en particulier. [31]

❖ **Traçabilité**

Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau. [31]

✓ **Les différents algorithmes du protocole AAA**

Les protocoles d'authentification utilisent différentes manières d'authentifier un utilisateur ou une machine. Il existe différents algorithmes, différentes techniques, mais tous dans un souci de sécurité utilisant le principe de chiffrement qui est à base de clés. Les protocoles les plus connus sont : [11]

1. **Protocole PAP** (Password Authentication Protocol) : Le protocole PAP est comme son nom l'indique, basé sur l'authentification par mot de passe. Les mots de passe sont envoyés en clair sur le réseau, ce qui représente un danger important. AP est un protocole d'autorisation d'accès pour l'ouverture d'une session sur le réseau. Il est de moins en moins utilisé au profit CHAP.
2. **Protocole CHAP** (Challenge-Handshake Authentiction Protocol) : Le protocole CHAP est basé sur le mode d'authentification « Défi-Réponse ». Le serveur d'authentification envoie un identifiant au hasard, c'est le défi. Le client transforme le défi avec sa clé et l'algorithme MD5 puis le renvoie au serveur : c'est la réponse. Le serveur applique le même algorithme avec la clé de client, compare les deux résultats puis accorde ou rejette la connexion, ce qui le rend relativement.
3. **Protocole TACACS** (Terminal Access Controller Access Control System) : Est le plus ancien des protocoles d'authentification. Il a été récemment actualisé dans une nouvelle variante appelée TACACS supporte plusieurs types d'authentification. L'authentification dite classique avec nom d'utilisateur/mot de passe complétée par l'utilisation des challenges. Le mécanisme d'authentification donne la possibilité après la transaction du login (nom d'utilisateur) et du mot de passe, de vérifier son identité en lui posant un certain nombre de questions.
4. **Protocole RADIUS** (Remote Authentication Dial-User Service) : Est un protocole d'authentification standard qui fonctionne selon le mode Client/Serveur. Un point d'accès (routeur, switch, serveur) fonctionne comme un client RADIUS qui effectue des requêtes sur le serveur. Le standard RADUIS est basé sur un ensemble d'attributs relatifs aux utilisateurs mais beaucoup d'implémentations spécifiques du protocole apportent leur propre jeu d'attributs. De plus, toutes les transactions RADUIS entre le client et le serveur sont protégées par un secret partagé qui n'est jamais transmis sur le réseau, ce qui représente une sécurité supplémentaire.

II.4 Sécurisation de l'interconnexion des réseaux

II.4.1 Pare-feu (Firewall)

Un pare-feu est une solution matérielle ou logicielle mise en place au sein de l'infrastructure du réseau afin de filtrer l'accès à des ressources réseau définies. Il ne laisse entrer que les utilisateurs autorisés,

disposant d'une clef ou d'un badge et crée une couche protectrice entre le réseau et le monde extérieur. De plus, un pare-feu permet de journaliser le trafic réseau en enregistrant les tentatives de connexions afin de pouvoir mieux l'analyser. La mise en œuvre d'un pare-feu nécessite un certain nombre de choix faits par l'administrateur réseau : type du pare-feu, l'emplacement du pare-feu, la politique de sécurité et le cout financier du pare-feu. [10] [2]

II.4.1.1 Fonctionnement du pare-feu

1. Principe de fonctionnement

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance grâce à une application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité. [34]

2. Rôles d'un pare-feu : [13]

- ✓ Déterminer le type de trafic qui sera achemine ou bloqué.
- ✓ Limiter le trafic réseau et accroitre les performances.
- ✓ Contrôler le flux de trafic.
- ✓ Fournir un niveau de sécurité d'accès réseau de base.
- ✓ Autoriser un administrateur à contrôler les zones aux quelles un client peut accéder sur un réseau.

3. Types de filtrage

Les principales technologies de contrôle d'accès à un réseau se répartissent en trois catégories :

a. Le filtrage statique de paquets : L'avantage de ce type de filtre est qu'il est transparent à l'utilisateur et aux applications. Tous les logiciels existants dans un réseau ne doivent subir aucune modification. Par contre, l'administrateur du pare-feu doit avoir une bonne connaissance des logiciels installés afin de mettre à jour les règles du filtre pour garantir le fonctionnement des bits logiciels. [2]

Le filtrage statique de paquets contrôle le trafic sur un réseau donné grâce aux informations des en−têtes qui sont : [23]

- L'adresse IP de la destination ;
- L'adresse IP de la source ;
- Le port de destination ;
- Le port source ;
- Les drapeaux (TCP uniquement).

b. Le filtrage dynamique de paquets : Un filtre dynamique se « souvient » des paquets qui le traversent. Il peut alors n'autoriser que les paquets−réponse aux requêtes sortantes. Pour avoir valeur de réponse, les informations d'en−tête de ces paquets doivent concorder avec celles des paquets−requête. Par conséquent le filtre dynamique sera particulièrement utile dans le filtrage des paquets UDP. [23]

c. Le mandatement (proxying) : Le mandatement donne l'accès à l'Internet à un nombre très restreint de machines tout en paraissant y connecter tous les hôtes d'un site. Un pare-feu est un

serveur intermédiaire avec qui les deux machines hôtes interne et externe communiquent. L'utilisateur croit qu'il utilise directement une machine hôte externe, mais tout passe par une machine proxy qui peut demander un mot de passe pour permettre l'accès. [23] [2]

II.4.1.2 Types de pare-feu

Il existe trois types de pare-feu qui sont les suivants : [17]

1. **Pare-feu sans état (Stateless Firewall) :** Regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.
2. **Pare-feu à états (Stateful Firewall) :** Vérifie que chaque paquet est bien la suite d'un précédent paquet et la réponse à un paquet dans l'autre sens.
3. **Pare-feu applicatif :** Vérifie-la complète conformité du paquet à un protocole attendu.
    - Pour ouverture de ports dynamique (FTP).
    - Contre ceux qui utilisent un tunnel TCP pour contourner le filtrage par ports.
    - Couteux en ressource.

II.4.1.3 Emplacement d'un pare-feu

L'emplacement d'un pare-feu est l'une des tâches importantes d'un administrateur réseau. Ce choix dépend de la fonction du pare-feu. Ce dernier peut être placé à la frontière de sorte qu'il protège le réseau de toutes les connexions venant d'Internet. La **figure II.10** représentée la situation correspondante. [17]

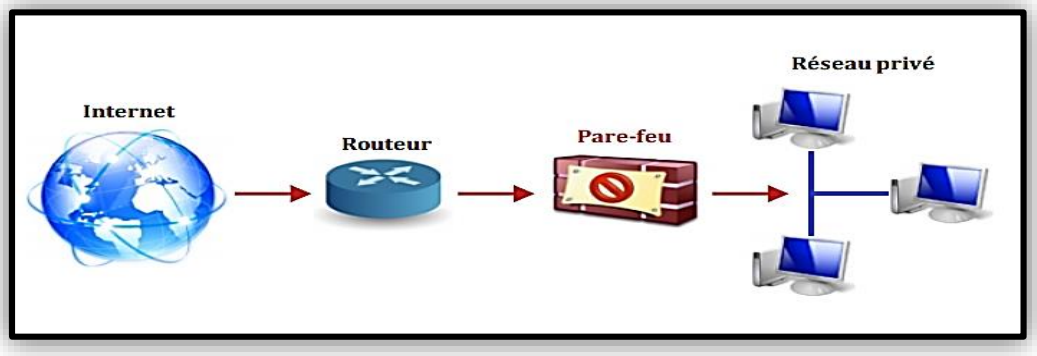


Figure II.10 Emplacement d'un pare-feu à la frontière

Un pare-feu peut aussi être placé à l'intérieur d'un réseau pour le diviser en plusieurs sous-réseaux et contrôler les différents accès entre eux. La **figure II.11** représente la disposition correspondante. [17]

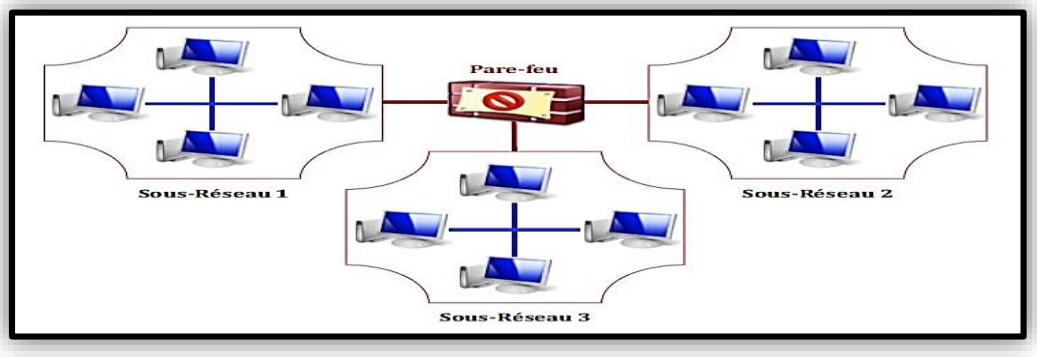


Figure II.11 Emplacement d'un pare-feu au centre d'un réseau

II.4.1.4 Fonctions d'un pare feu

Les fonctions du pare-feu les plus répondues sont : [17]

- **Blocage de trafic entrant en fonction de l'origine et de la destination :** Il s'agit de contrôler le trafic entrant d'un réseau et empêcher certains nœuds extérieurs de se connecter à un réseau local.
- **Blocage de trafic sortant en fonction de l'origine et de la destination :** Il s'agit de contrôler le trafic sortant d'un réseau en direction d'internet, et notamment éviter que les utilisateurs accèdent à certains sites inappropriés.
- **Blocage de trafic en fonction du contenu :** Un pare-feu peut inspecter le contenu du paquet IP en utilisant par exemple un scanner de virus intègre. Il peut aussi intégrer un filtre pour empêcher les emails indésirables.
- **Etablir des rapports sur les trafics et l'activité du pare-feu :** Un pare-feu doit incorporer un mécanisme de report. Ce mécanisme permet d'établir des rapports sur son activité et les archiver dans un journal pour pouvoir l'examiner ultérieurement.

II.4.2 Zone Démilitarisée DMZ

II.4.2.1 Définition

DMZ est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et pour certains depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne. [13]

II.4.2.2 Architecture DMZ

DMZ est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu, ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité et les services susceptibles d'être accédés depuis Internet seront situés en DMZ. La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des zones démilitarisées en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi les intrusions venant de l'intérieur. [7]

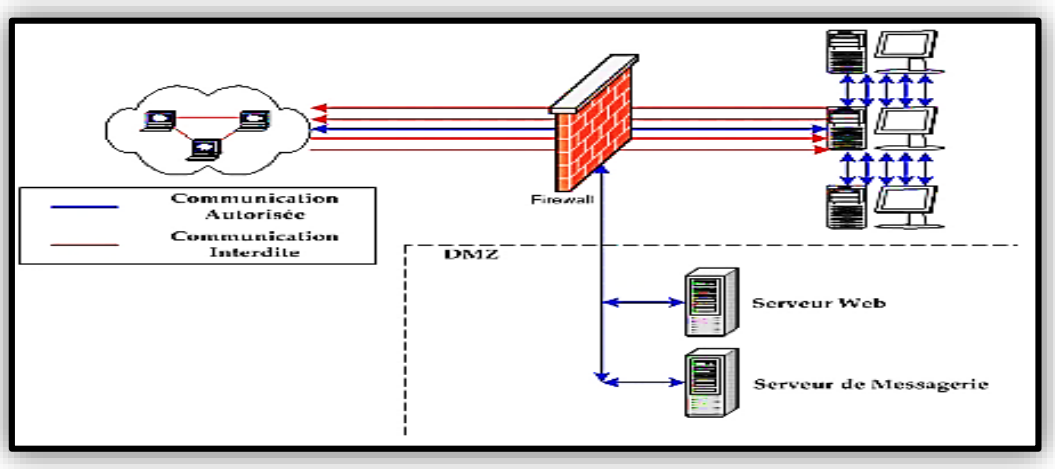


Figure II.12 Architecture d'une DMZ

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante : [7]

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

II.4.3 IDS (Intrusion Détection System)

II.4.3.1 Définition d'un IDS

IDS s'agit d'un mécanisme ou d'un équipement (matériel ou logiciel) permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion et éventuellement de réagir à cette tentative (avoir une stratégie de prévention sur les risques d'attaques).

IDS possède généralement soit une base de données de signatures qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées, soit un système à approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur. [34]

II.4.3.2 Caractéristiques d'un système de détection d'intrusion

Les caractéristiques suivantes sont souhaitables dans un IDS : [15]

- Fonctionner en permanence avec une supervision manuelle minimale ;
- Etre tolérant aux pannes dans le sens où il doit récupérer après une défaillance ou une réinitialisation de la machine ;
- Résister aux tentatives de corruption c'est à dire il doit pouvoir détecter s'il a subi lui-même une modification indésirable ;
- Utiliser un minimum de ressources du système sous surveillance ;
- Être facilement configurable pour implémenter une politique de sécurité spécifique d'un réseau.

II.4.3.3 Les principales tâches d'un IDS

Un IDS permet de repérer des anomalies dans le trafic réseau comme suit : [1]

- Détecter les tentatives de découvertes du réseau ;
- Détecter dans certains cas, si l'attaque a réussi ou non ;
- Détecter le Déni de Service ;
- Détecter le niveau d'infection du système informatique et les zones réseaux touchées ;
- Repérer les machines infectées ;
- Alerter de façon centrale pour toutes les attaques ;
- Réagir aux attaques et corriger les problèmes éventuels.

II.4.3.4 Emplacement d'un IDS

Il existe plusieurs endroits stratégiques où il convient de placer un IDS. Le schéma suivant illustre un réseau local ainsi que les positions que peut y prendre un IDS : [1]

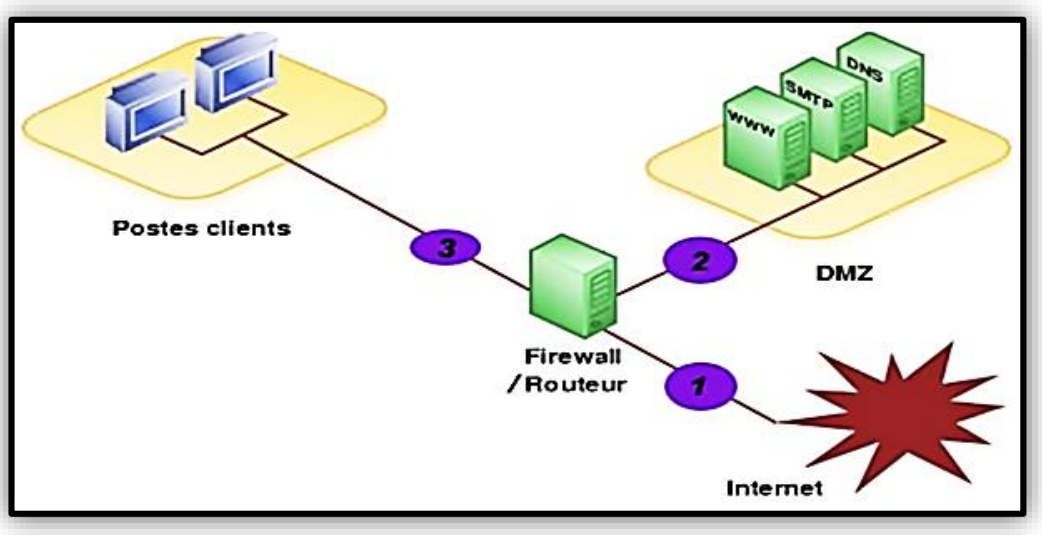


Figure II.13 Endroits typiques pour un système de détection d'intrusions

- **Position (1) :** Sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur en amont du firewall. Ainsi, beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.
- **Position (2) :** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le pare-feu et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénignes ne seront pas recensées.
- **Position (3) :** L'IDS peut ici rendre compte à des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80% des attaques proviennent de l'intérieur. De plus, si des trojans ont contaminé le parc informatique (navigation peu méfiante sur internet) ils pourront être ici facilement identifiés pour être ensuite éradiqués.

II.4.3.5 Types des IDS

Plusieurs types des IDS ont été développés depuis les années 80, chacun a ses propres fonctions, caractéristiques et champs d'application. L'emplacement d'un IDS dans un réseau dépend fortement du type de protection qu'il offre. Ainsi, on peut distinguer deux grands types d'IDS à savoir :

1. **Les systèmes de détection d'intrusions de type réseau (NIDS) :** Ce sont des IDS réseaux permettant d'analyser et d'interpréter le trafic de tout un réseau afin de repérer des signatures d'attaques déjà connues à différents endroits sur le réseau ou des anomalies dans les entêtes des paquets IP. [17]

   ➢ **Les avantages des NIDS sont :** [15]

   - Ils peuvent être complètement cachés sur le réseau, donc un attaquant ne saura pas qu'il est contrôlé ;
   - Il peut capturer le contenu de tous les paquets envoyés à un système cible ;
   - Une seule tache à effectuer : regarder le trafic et le traiter ;
   - Les NIDS sont des systèmes à temps réel.

- **Les inconvénients des NIDS sont :** [15]

  - Ils ne peuvent donner d'alarme que si le trafic correspond aux règles ou aux signatures préconfigurées ;
  - Ils peuvent manquer le trafic intéressant si le trafic est important sur la bande passante ou si des routes altérées sont utilisées ;
  - Il ne peut pas déterminer si une attaque a réussi ;
  - Il ne peut pas examiner le trafic chiffré.

2. **Les systèmes de détection d'intrusions de type hôte (HIDS) :** Ce sont des IDS permettant d'examiner le fonctionnement d'une machine donnée et signaler tout comportement malveillant pouvant compromettre sa sécurité. Les HIDS sont généralement placés sur les serveurs. Ils sont considérés plus complets et plus efficaces que les NIDS puisqu'ils implémentent un système de protection pour chaque hôte du réseau. [17]

   De plus, les HIDS sont extrêmement complémentaires des NIDS. En effet, ils permettent de détecter plus facilement les attaques de type "Cheval de Troie", alors que ce type d'attaque est difficilement détectable par un NIDS. [1]

- **Les avantages des H-IDS sont :** [15]

  - Les HIDS peuvent souvent fonctionner dans des environnements avec un trafic réseau chiffré ;
  - Ils permettent également de détecter des attaques impossibles à détecter avec un NIDS, car elles font partie du trafic crypté ;
  - Ils génèrent peu de faux positifs, permettant d'avoir des alertes pertinentes.

- **Les inconvénients des H-IDS sont :** [15]

  - Ils peuvent être identifiés et mis hors service par un attaquant ;
  - Ils ne peuvent donner l'alerte que si les entrées des journaux d'événements ou les appels au système correspondent à des signatures ou des règles préconfigurées ;
  - Ils sont assez gourmands en CPU et peuvent parfois altérer les performances de la machine hôte.

II.4.4 IPS (Intrusion Prevention System)

II.4.4.1 Définition d'un IPS

Un système de prévention d'intrusion est un dispositif capable de détecter des attaques, connues et inconnues, et de les empêcher d'être réussies. L'IPS n'est pas un observateur car il fait partie intégrante du réseau.

IPS est placé en ligne et examine tous les paquets entrants ou sortants. Aussi il est pour la Protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions comme la plupart des IDS. [1] La principale différence entre un IDS (réseau) et un IPS (réseau) tient principalement en deux caractéristiques : [38]

- Le positionnement en coupure sur le réseau de l'IPS et non plus seulement en écoute sur le réseau pour l'IDS (traditionnellement positionné comme un sniffer sur le réseau).

- La possibilité de bloquer immédiatement les intrusions et quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que l'IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocages.

II.4.4.2 Contrôle des connexions réseau avec Les NIPS

Les N-IPS (Network Intrusion Prevention System) incarnent une nouvelle génération d'équipements réseau qui combine les fonctionnalités des IDS et celles des pare-feu. Ils présentent au minimum deux interfaces réseau (entrante et sortante) et se positionnent en passerelle/coupure de niveau d'OSI du trafic réseau. Bien qu'un NIPS reste invisible pour le trafic IP, le trafic réseau est analysé en son sein afin de contrôler les données et de détecter des attaques potentielles.

Un NIPS peut agir directement sur le trafic lors de la détection d'un trafic malicieux en agissant en coupure sur ce trafic. Cela permet de réduire la propagation de l'attaque au plus vite. L'objectif de tels équipements est ainsi d'offrir des contre-mesures en temps réel. [2]

II.4.5 Réponses des IDS/IPS

Lors de la détection d'une attaque, un système IDS/IPS, peut adopter plusieurs comportements. Les IDS peuvent émettre des réponses actives qui influent directement sur la source d'attaque, par exemple IDS peut réagir en ré-paramétrant un pare-feu, pour mettre en place des règles de blocage temporaire de certains flux réseau anormaux, comme ils peuvent se restreindre à des réponses passives en diffusant une alerte identifiant l'attaque détectée. Une liste des réponses actives et passives est présentée dans le **tableau II.4** : [15]

Réponse passive	Réponse active
▪ Emettre un rapport ▪ Générer une alarme ▪ Activer un archivage plus détaillé ▪ Activer un archivage à distance ▪ Créer des fichiers de sauvegarde	▪ Bloquer le compte d'un utilisateur ▪ Suspendre des processus malveillants ▪ Terminer une session ▪ Bloquer une adresse IP ▪ Arrêter la machine ▪ Déconnecter la machine du réseau ▪ Mettre hors service les ports et les services attaqués ▪ Avertir l'utilisateur ▪ Tracer l'origine de la connexion ▪ Forcer une nouvelle authentification ▪ Restreindre les activités d'un utilisateur

Tableau II.4 Réponses aux attaques des systèmes de détections d'intrusions

II.5 Journalisation/Log

II.5.1 Définition des termes utilisés

- **Log :** Est une collection d'enregistrement de journal. Les termes tels que « journal de données », « journal d'activité », « journal d'audit », « fichier journal », « journal des événements » sont souvent utilisés pour signifier la même chose que log (journal). [30]

- **Journalisation :** C'est le fait de stocker les fichiers logs dans une base de données ou autres supports d'information. [30]
- **Fichier log :** C'est un fichier informatique utilisé pour l'exploitation d'un serveur d'hébergement. Ce fichier conserve la trace de toutes les requêtes qui ont été adressées à ce serveur. Chacune des requêtes génère une ligne de codes dans le fichier journal. Ces fichiers sont très utiles pour analyser l'audience d'un site Internet, car ils fournissent des indications précises sur le trafic du site. [19]

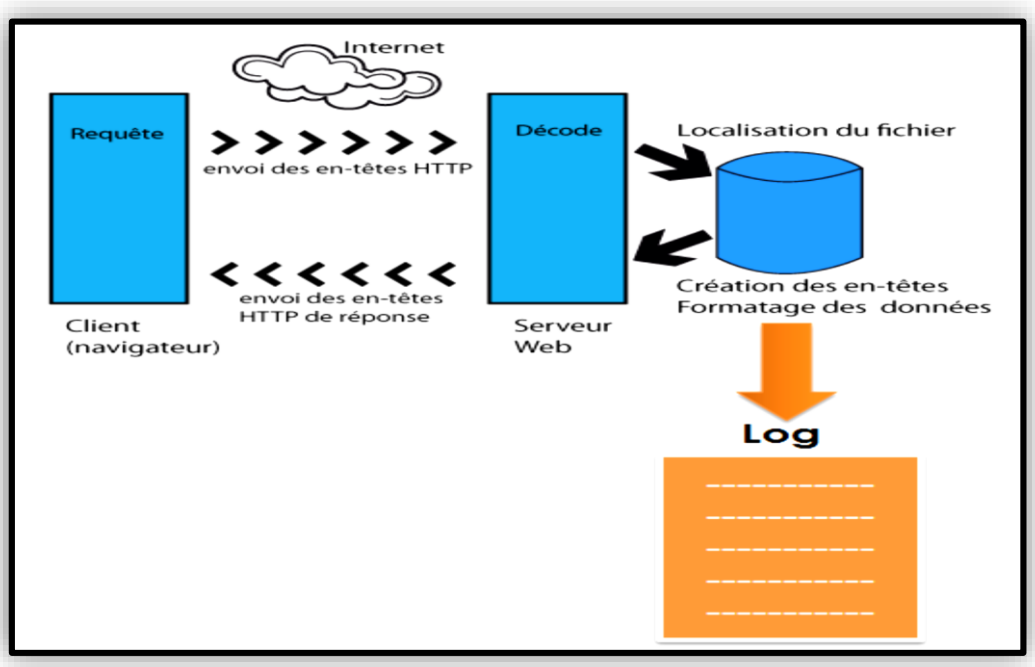


Figure II.14 L'enregistrement des informations dans un fichier log

II.5.2 Les types des fichiers log

Les systèmes informatiques génèrent de nombreux types de fichiers log afin de fournir les informations essentielles sur le système. Parmi ses types, on peut citer les exemples suivants : [18]

- Les fichiers log issus des serveurs ;
- Les fichiers log issus des sites web ;
- Les fichiers log issus des systèmes de détection d'intrusion ;
- Les fichiers log issus des systèmes de surveillance de réseau ;
- Les fichiers log issus des pare-feu ;
- Les fichiers log d'accès ;
- Les fichiers log d'erreurs.

II.5.3 La collecte et la transmission des fichiers log

Les protocoles utilisés pour la transmission des fichiers logs sont : [30]

1. **SNMP (Simple Network Management Protocol) :** SNMP a été créé à l'origine pour être utilisé dans la gestion des périphériques réseau. Cependant au fil des années, de nombreux systèmes qui ne sont pas mis en réseau ont adopté SNMP comme moyen d'émettre des messages de journalisation.
2. **Windows Event Log :** Format de journalisation propriétaire de Microsoft a décidé il y a longtemps d'inventer son propre système de collecte et d'enregistrement de journaux.

3. **Syslog :** C'est un protocole qui se compose d'une partie cliente et d'une partie serveur. La partie cliente émet les informations sur le réseau via le port UDP 514. Les serveurs collectent l'information et se chargent de créer les journaux.

Il existe plusieurs implémentations du protocole **Syslog** :

- **Syslog-ng :** Est une amélioration de Syslog. Certaines des fonctionnalités incluent la prise en charge du protocole IPv6, la possibilité de transférer des messages de journal avec fiabilité à l'aide de TCP et le filtrage du contenu des journaux à l'aide d'expressions régulières.
- **Syslog-pseudo :** Est également une amélioration de Syslog qui propose une architecture de journalisation pour pseudonymiser les fichiers journaux.
- **Reliable-syslog :** A pour objectif de la mise en œuvre d'une livraison fiable des messages Syslog, qui se repose sur les blocs du protocole BEEP (Extensible Exchange Protocol) qui s'exécute sur TCP pour fournir le service de livraison fiable requis.

II.5.4 Les composants d'un fichier log

Un fichier log se compose de : [19]

- Le nom du domaine ou l'adresse de Protocole Internet (IP) de la machine appelante ;
- Le nom et le login HTTP de l'utilisateur (en cas d'accès par mot de passe) ;
- La date et l'heure de la requête ;
- La méthode utilisée dans la requête (GET, POST, etc.) et le nom de la ressource Web demandée (l'URL de la page demandée) ;
- Le statut de la requête i.e. le résultat de la requête (succès, échec, erreur, etc.) ;
- La taille de la page demandée en octets ;
- Le navigateur et le système exploitation utilisé par le client.

II.5.5 Format de fichier journal

La structure et le contenu de fichier log permettent d'obtenir de plus amples informations après certains traitements. Il existe deux types de format : [19]

a. **CLF (Common Log File) :** Ceci a la même structure que ELF mais ne contient pas le « référer » désignant le navigateur, le système exploitation du l'ordinateur client et ainsi d'autres paramètres éventuelles.

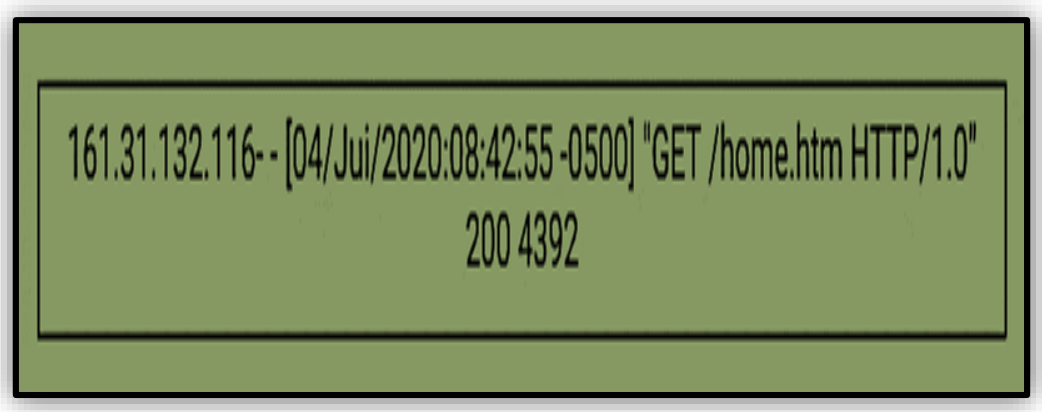


Figure II.15 Extrait d'un fichier log de format CLF

b. ELF (Extended Log Format) : Chaque ligne de ce fichier donne une information sur l'utilisateur, son matériel, la date et l'heure de la requête, la page requise, le statut de la page requise, la page de référence ainsi que quelques informations liées au protocole d'échange de données.

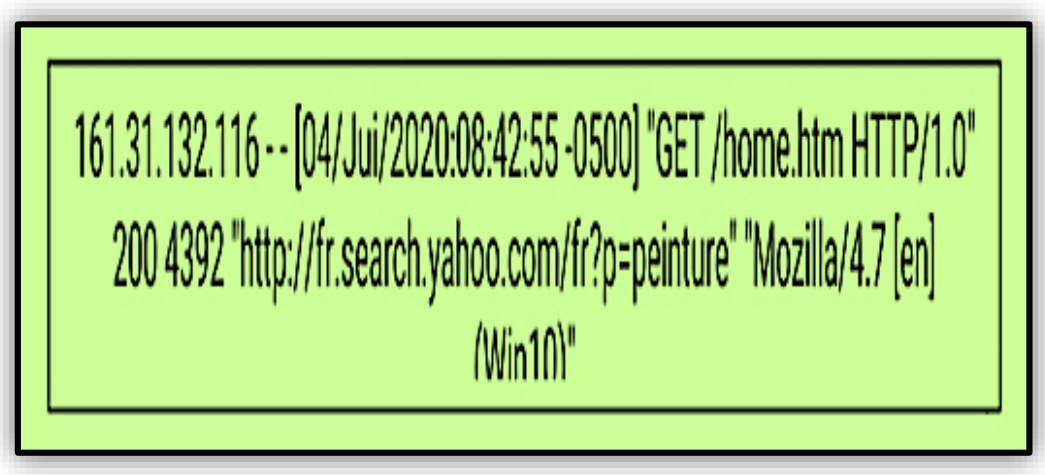


Figure II.16 Extrait d'un fichier log de format ELF

La figure II.15 montre un exemple de format **CLF** de fichier log, ce format est composé, pour chaque requête d'un utilisateur par les champs suivants : [18]

- **161.31.132.116 :** L'adresse IP de l'utilisateur qui a envoyé la requête.
- **[04/Jui/2020:08:42:55 -0500] :** La date et l'heure de la requête.
- **GET /home.htm HTTP/1.0 :** La méthode de requête, la page demandée et le protocole utilisé.
- **200 :** Le numéro de code de réponse de serveur.
- **4392 :** La taille de la page demandée en octets.

Le format **ELF** a les mêmes champs que le format **CLF**, en rajoutant d'autre paramètres pour plus de détails, tel que : [18]

- **http://fr.search.yahoo.com/fr?p=peinture :** La page de référence qui à partir de laquelle la requête est lancée.
- **Mozilla/4.7 [en] (Win10) :** Le navigateur et le système d'exploitation utilisés par l'utilisateur.

Dans l'exemple de la **figure II.16**, la machine ayant l'adresse IP **161.31.132.116** a émis la requête **GET /home.htm HTTP/1.0** le **04 juillet 2020 à 8 heures, 42 minutes et 55 secondes**. Sa requête a été accepté par le serveur (code **200** signifie l'acceptation) et la machine a reçu un fichier de taille **4392 octets**. La page de référence qui à partir de laquelle la machine lance la requête est **http://fr.search.yahoo.com/fr?p=peinture** en utilisant le navigateur **Mozilla 4.7** version **anglais** sous l'environnement **Windows 10.**

II.6 Audit de sécurité

II.6.1 Définition de l'audit

Un audit de sécurité consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité. Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres. [1]

II.6.2 Rôles et objectifs de l'audit

Une mission d'audit vise différents objectifs. En effet nous pouvons énumérer à ce titre : [26]

- La détermination des déviations par rapport aux bonnes pratiques de sécurité.
- La proposition d'actions visant l'amélioration du niveau de sécurité du système d'information.

Egalement, une mission d'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité par rapport à une politique de sécurité ou par rapport à un ensemble de règles de sécurité.

II.6.3 Principes de l'audit

Pour réaliser leur mission, les auditeurs doivent disposer d'une marge de manœuvre entière leur permettant de s'exprimer sur tout sujet ayant un impact négatif sur le fonctionnement, voire la survie de l'entreprise au regard des objectifs qu'elle s'est fixés. Ceci nous conduit à présenter quelques principes fondamentaux : [2]

- ✓ Le principe de la déontologie ;
- ✓ Le principe de la présentation impartiale ;
- ✓ Le principe de l'approche fondée sur la preuve ;
- ✓ Le principe de l'indépendance.

II.6.4 Intérêt et nécessité de l'audit

L'audit peut être envisagé à la suite de problèmes techniques, pour l'établissement d'une documentation dans le but d'évaluer les besoins en ressources en fonction de la tâche à effectuer. Mais il s'agit également souvent d'aider les entreprises à définir et à adopter un plan stratégique informatique. Ce plan identifiera les objectifs de l'entreprise à moyen terme et indiquera comment l'informatique peut aider à atteindre les objectifs posés. [2]

II.6.5 Types d'audit existants

Du point de vu général, il existe deux types d'audit : [2]

1. **L'audit Interne :** L'audit interne se base sur la tâche d'évaluation, de contrôle, de conformité et de vérification. Il est exercé d'une façon permanente par une entreprise. Cet audit a pour mission de déceler les problèmes et de donner des solutions.
2. **L'audit Externe :** L'audit externe est une opération volontaire décidée par la direction d'une entreprise pour faire apprécier la conformité de son système avec un référentiel, et ce par une firme d'audit tiers reconnu pour ses compétences et sa notoriété dans les secteurs d'activités concernés.

II.6.6 Cycle de vie d'un audit de sécurité des systèmes d'information

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie qui est schématisé à l'aide de la **figure II.17**. L'audit de sécurité se présente essentiellement suivant deux parties :

1. L'audit organisationnel et physique.
2. L'audit technique.

Une troisième partie optionnelle peut être également considérée. Il s'agit de l'audit Intrusif (test d'intrusions). Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit. Il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées. [26]

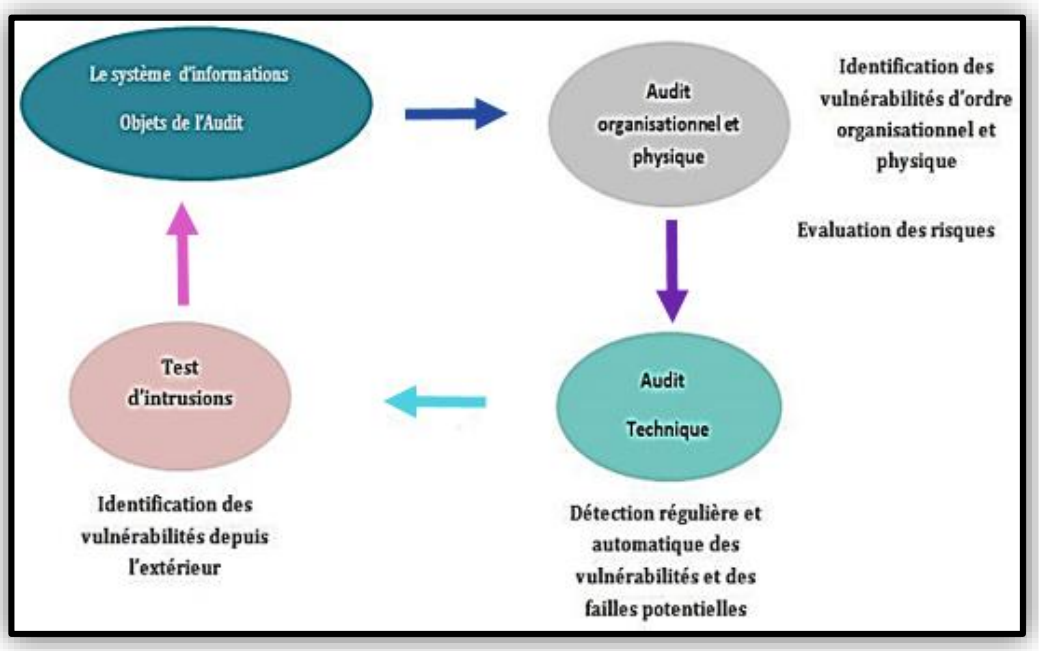


Figure II.17 Cycle de vie d'audit de sécurité

II.7 Outils de sécurité

II.7.1 VPN (Virtual Private Network)

II.7.1.1 Définition

VPN (Réseau Privé Virtuel) désigne un réseau crypté dans le réseau Internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complétement sécurisée comme s'il n'y avait qu'un local avec un réseau interne. Les VPN sont très utilisés par les multinationales et les grandes sociétés. Le VPN garantie la sécurité et la confidentialité des données qui circulent de manière cryptée par Internet afin que personne de malintentionné ne puisse intercepter les informations. [13]

II.7.1.2 Fonctionnement du VPN

Un réseau VPN est réalisé avec des mécanismes de chiffrement et d'authentification. En chiffrant les données, tout se déroule comme si la machine se trouvait directement sur son réseau privé sans qu'aucune personne extérieure à ce réseau puisse accéder aux données qu'elle envoie et reçoit. On peut réaliser un VPN à l'aide de matériels spécifiques (cartes réseaux, routeurs),de logiciels ou d'une combinaison des deux (hardware/software). Le VPN fait référence à l'usage du protocole IPSec afin de créer un canal de communication sécurisé « Tunnel » à usage privé, dans un réseau public non sécurisé, veut dire le VPN repose sur un protocole de tunneling qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux. [27]

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les

VPNs simulent un réseau privé alors qu'ils utilisent une infrastructure partagée et ceux afin d'assurer un accès aisé et peu couteux au intranet ou aux extranets. [13]

Figure II.18 Tunnel VPN

II.7.1.3 Types des réseaux privés virtuels

On peut dénombrer trois grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie.

1. **L'intranet VPN (site à site)** : C'est un réseau VPN entre les différents services d'une entreprise, les bureaux des filiales, les bureaux situés à l'étranger, etc. Sans VPN, les entreprises seraient forcées d'utiliser des lignes dédiées entre leurs filiales (procédé très onéreux, surtout lorsqu'il s'agit de lignes internationales). Avec les réseaux VPN, ces mêmes communications peuvent passer par l'Internet sans souci de confidentialité ou d'intégrité des transferts et c'est pour un coût bien moindre. [13]

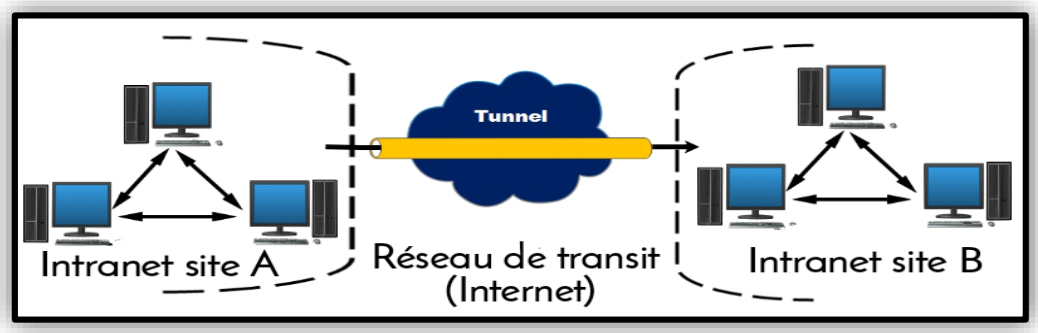


Figure II.19 L'intranet VPN

2. **L'extranet VPN (poste à poste)** : C'est l'extension du VPN Intranet et ce type de VPN est utilisé par les entreprises afin de communiquer avec ses clients en ouvrant son réseau local à ses clients ou partenaires. [13]

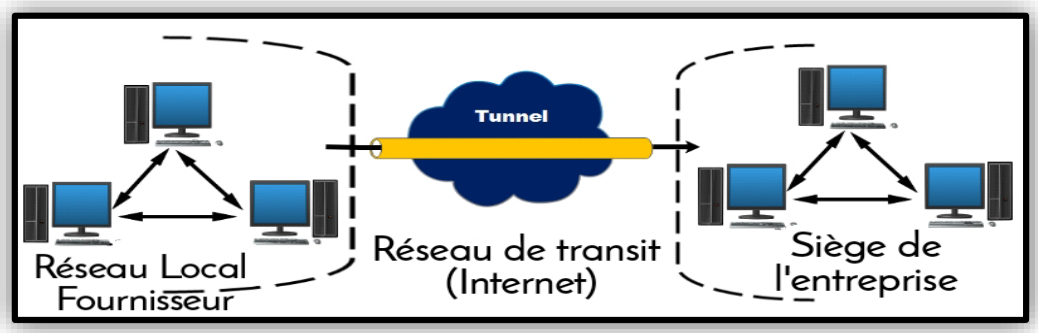


Figure II.20 L'extranet VPN

3. **Le VPN d'accès (poste à site)** : C'est l'extension du VPN Intranet, qui permet de connecter les utilisateurs nomades aux bureaux de l'entreprise. Ce type de réseaux VPN peut être utilisé pour accéder à certaines ressources prédéfinies d'une entreprise sans y être physiquement présent. Cette opportunité peut ainsi être très utile au commercial ou au cadre qui souhaite se connecter au réseau de son entreprise lors d'un déplacement. [15]

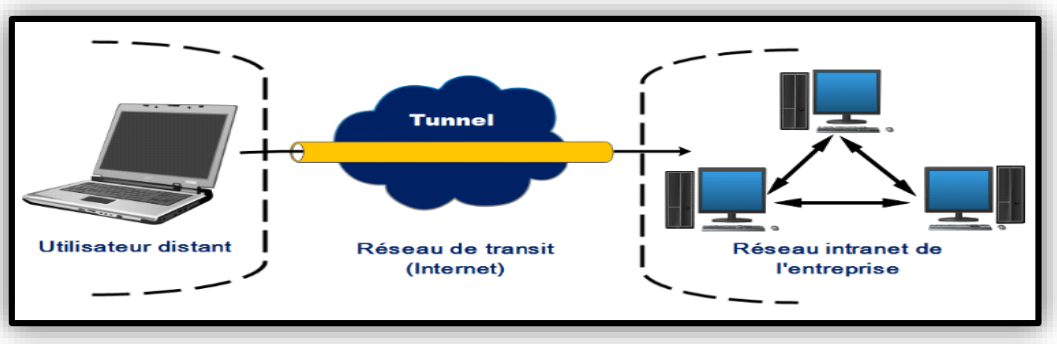


Figure II.21 VPN d'accès distant

II.7.1.4 Fonctionnalités du VPN

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes : [13]

- Authentification des entités communicantes : Le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa.
- Authentification des utilisateurs : Seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.
- Gestion des adresses : Tous les utilisateurs doivent avoir une adresse privée et les nouveaux clients en obtenir une facilement.
- Cryptage du tunnel : Les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa.
- Les clés de cryptage doivent être régénérées souvent (automatiquement).
- Le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

II.7.1.5 Principaux protocoles du VPN

Les principaux protocoles de tunneling VPN sont les suivants : [13]

1. **Le protocole PPTP**

Le protocole PPTP pour "Point-to-Point Tunneling Protocol" a été créé par Microsoft, qui avait comme objectif la création de VPN sur les réseaux communautaires. Le protocole PPTP a d'ailleurs longtemps été le protocole standard utilise en interne pour les entreprises. Ce protocole est proposé par la plupart des VPNs et présente l'avantage d'être supporté par la majorité des OS.

✓ **Avantages du protocole PPTP**

- PPTP est intégré dans la plupart des OS donc son utilisation ne nécessite pas l'installation d'une application spécifique.

- PPTP est très simple à utiliser et à mettre en place.
- PPTP est un système rapide.

✓ **Inconvénients du protocole PPTP**

- PPTP est mal sécurisé.
- PPTP a certainement déjà été craqué par la NSA.

2. Le protocole OpenVPN

Comme son nom l'indique, OpenVPN est un protocole VPN open source qui utilise Secure Socket Layer (SSL) pour créer une authentification pour une connexion Internet cryptée. Etablir une connexion OpenVPN peut être difficile pour les utilisateurs qui n'ont pas de compétences techniques alors le VPN le rend simple avec notre logiciel. Dans l'ensemble, le protocole OpenVPN offre l'une des meilleures combinaisons de performance et de sécurité et il peut être utilisé pour contourner facilement les pare-feu ainsi que les restrictions des FAI.

✓ **Les avantages du protocole OpenVPN**

- OpenVPN est totalement configurable.
- OpenVPN est très bien sécurisé.
- OpenVPN permet de contourner les pare-feu.
- OpenVPN peut utiliser un large choix d'algorithmes de chiffrement.

✓ **Les inconvénients du protocole OpenVPN**

- OpenVPN nécessite l'installation d'un logiciel tiers.
- OpenVPN est assez complexe à mettre en place.
- OpenVPN est supporté par certains appareils mobiles, mais n'est pas aussi puissant que sa version fixe.

3. Les protocole IPsec, L2TP & L2TP/IPsec

Le protocole IPSec est un protocole de niveau 3 issu des travaux de l'IETF permettant de transporter des données chiffrées pour les réseaux IP.

Le protocole L2TP est un protocole de tunneling utilisé pour soutenir les réseaux privés virtuels (VPN) ou dans le cadre des prestations de services des FAI. Le protocole VPN L2TP est un protocole qui ne chiffre pas les informations qu'il fait transiter, c'est donc pour cette raison qu'il est généralement utilisé avec le cryptage IPsec.

Le protocole L2TP/IPsec qui comprend le système de cryptage est intégré à tout OS modernes et a tous les appareils qui sont capables d'utiliser un VPN. Le protocole L2TP/IPsec est donc aussi simple à utiliser que le protocole PPTP, puisqu'il utilise généralement le même client. Par contre, il utilise le port UDP 500 qui peut être bloqué par les pare-feu, ce qui peut nécessiter une configuration spécifique.

Pour finir, il faut préciser que le protocole L2TP/IPsec est un peu plus lent que les solutions basées sur SSL comme OpenVPN et SSTP.

✓ **Avantages du protocole L2TP/IPsec**

- L2TP/IPsec offre une bonne protection.
- L2TP/IPsec est totalement intégré dans les principaux OS.
- L2TP/IPsec permet de contourner la majorité des pare-feu

✓ **Inconvénients du protocole L2TP/IPsec**

- L2TP/IPsec est encore une propriété de Microsoft, il n'est donc pas possible de verrier l'absence de portes dérobées dans le code.

II.7.1.6 Comparaison entre les différents protocoles du VPN

D'après une évaluation des différents protocoles effectués par VyprVPN nous vous proposons une comparaison des protocoles définis auparavant : [13]

	PPTP	L2TP/IPsec	Open VPN
Cryptage VPN	182 bits	256 bits	160 Bits, 256 bits
Application VYPRVPN supportées	Windows, Routeur	Windows, Mac, iOS (seulement IPsec IKEV2)	Windows, Mac, Routeur, Anonabox
Sécurité VPN	Encryptage de base	Le chiffrement le plus élevé, Vérifie l'intégrité des données et les encapsule deux fois.	Le chiffrement le plus élevée, Authentifie les données à l'aide de certifiât numérique
Vitesse VPN	Rapide grâce à un plus bas cryptage.	Nécessite plus de processeur pour le double encapsulage des données.	Le protocole le plus performant, Débits rapides même sur des connexions latence élevée et sur des grandes distances.
Stabilité	Fonctionne bien sur la plus part des hotspots WIFI, très stable.	Stable sur les appareils supportant le NAT.	Plus fiable et plus stable sur les réseaux moins protégés et sur les hotspots WIFI, même derrière des routeurs sans fil
Compatibilité	Intégrité dans la plus part des systèmes d'exploitation.	Intégrité dans la plus part des systèmes d'exploitation	Compatible avec la plus part des systèmes d'exploitation.

Tableau II.5 Comparaison entre les protocoles PPTP, Open VPN, L2TP/IPsec

II.7.2 VLAN (Virtual Local Area Network)

II.7.2.1 Définition

Un VLAN (Virtual LAN) est un réseau local regroupant un ensemble de machines de façon logique et non physique. En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage,) en définissant une

segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.). [13]

II.7.2.2 Types de VLAN

Plusieurs et différents types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'exécute : [13]

- **VLAN de niveau 1** (aussi appelés VLAN par port) : Définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.
- **VLAN de niveau 2** (également appelé VLAN MAC) : Consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.
- **VLAN de niveau 3 :** On distingue plusieurs types de VLAN de niveau 3 :
  - Le VLAN par sous-réseau (Network Address-Based VLAN) associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

II.7.2.3 Avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants : [13]

- Plus de souplesse pour l'administration et les médications du réseau car toute l'architecture peut être modifiable par un simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.
- La régulation de la bande passante.

II.7.3 Anti-virus

II.7.3.1 Définition de l'Anti-virus

L'antivirus est un logiciel conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus ne sont qu'un exemple). Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité. Les antivirus fondent sur des fichiers de signatures et comparent alors les signatures génétiques du virus aux codes à vérifier. Certains programmes appliquent également la méthode heuristique tendant à découvrir un code malveillant par son comportement. [10]

Un bon antivirus doit intervenir au moment même de l'entrée ou de la tentative d'entrée d'une peste quelconque. Lorsque le virus a été découvert, l'antivirus peut : [5]

- Nettoyer les fichiers infectés en éradiquant les virus.
- Supprimer les fichiers infectés (attention aux problèmes que cela peut poser).
- Écarter le virus dans une zone du disque dur où il ne peut pas nuire.

II.7.3.2 Fonctionnement d'un antivirus

Le programme est composé de trois parties ayant chacune un rôle essentiel : [14]

- Un "moteur" qui a pour rôle la détection des virus.
- Une base de données contenant des informations sur les virus connus. C'est cette base de données qu'il faut maintenir à jour le plus régulièrement possible, afin de permettre à l'antivirus de connaître les virus les plus récents.
- Un module de nettoyage qui a pour but de traiter le fichier infecté.

A chaque fichier testé, si le programme pense voir un virus, il regarde dans sa base de données si le virus est connu (chaque virus ainsi que ses variantes à une signature particulière et c'est cette signature qui est comparée avec la base). Si le virus est connu, il y a de fortes chances qu'un antidote soit connu.

- ✓ Si le virus est connu, il est supprimé et le fichier est donc nettoyé.
- ✓ Si le virus n'est pas connu, le logiciel emploie une méthode heuristique.

II.7.3.3 Techniques de détection utilisées par un antivirus

Les antivirus utilisent principalement cinq méthodes pour détecter les virus :

1. **Recherche par signature :** Il s'agit de la méthode la plus ancienne et la plus utilisée dans la plupart des antivirus. La signature est un morceau de code ou une chaîne de caractères du virus qui permet de l'identifier. Chaque virus a sa propre signature, qui doit être connue de l'antivirus. [12]

2. **Recherche heuristique :** C'est la méthode la plus puissante car elle permet de détecter d'éventuels virus inconnus par votre antivirus. Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes. [5]

3. **Analyse spectrale :** Tout code généré automatiquement contiendra des signes révélateurs du compilateur utilisé. Il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code. [14]

4. **Contrôle d'intégrité :** L'antivirus, pour contrôler l'intégrité des fichiers, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations qui peuvent changer lorsque le fichier est modifié :

   - La taille ;
   - La date et heure de la dernière modification ;
   - La somme de contrôle (CRC : code de redondance cyclique) éventuelle.

   Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus recalcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé. [5]

5. **Moniteur de comportement :** Les moniteurs de comportement ont pour rôle d'observer l'ordinateur à la recherche de toute activité de type viral, et dans ce cas de prévenir l'utilisateur. Un moniteur de comportement est un programme réside que l'utilisateur charge à partir du fichier **AUTOEXEC.BAT** et qui reste actif en arrière-plan, surveillant tout comportement inhabituel. [14]

II.7.4 Plan de sauvegarde

II.7.4.1 Définition

Le plan de sauvegarde est un ensemble de règles qui définissent la manière dont les données spécifiques seront protégées sur une machine spécifique. Ces règles englobent des principes généraux de sauvegarde et un ensemble des procédures liées à la sauvegarde et à la restauration pour un périmètre identifié sur lequel ils doivent être appliqués. Outre, le plan de sauvegarde peut être appliqué à plusieurs machines, soit au moment de sa création, soit plus tard. [24]

II.7.4.2 Politique & fonctionnement d'un plan de sauvegarde

La définition d'une politique de sauvegarde impose d'établir le niveau de sensibilité du patrimoine informationnel de l'entreprise afin de répondre à ses besoins essentiels d'activité, et de déterminer les moyens de protection les mieux adaptés aux différents composants de ce patrimoine. Son principe de fonctionnement est le suivant : [21]

- Formuler la problématique de sécurité posée :
  - Les risques d'indisponibilité, de perte d'intégrité, d'interruption de service ;
  - La gestion du plan de continuité de service de l'entreprise ;
  - Le respect d'engagements d'activité et les enjeux métier plus les obligations juridiques.
- Donner une solution, faire des copies régulières des ressources informationnelles critiques pour les activités de l'entreprise.
- Formaliser, publier les règles et les modalités de gestion précises à respecter pour garantir la fiabilité de cette action essentielle, définir, publier et gérer le plan de sauvegarde de l'entreprise.
- Faire valoir l'objectif poursuivi, répondre à deux situations :
  - Pouvoir récupérer le plus rapidement possible une information.
  - Etre capable en cas de perte totale de reconstituer un environnement informationnel identique.

II.7.4.3 Principes d'un plan de sauvegarde

Les principes de sécurité de la sauvegarde sont regroupés en quatre thématiques : [22]

1. **Identification du besoin de sauvegarde et de restauration :** Afin de définir les processus et dispositifs de sauvegarde adaptés, il est indispensable de mener une analyse préalable des besoins de sauvegarde incluant notamment :
   - ✓ La définition du périmètre métier concerné.
   - ✓ Le niveau de service attendu pour la sauvegarde et la restauration (délai maximum de restauration des données, perte admissible de données non sauvegardées entre deux

sauvegardes, durée de conservation des sauvegardes, intégrité des sauvegardes, confidentialité des sauvegardes).

2. **Formalisation des procédures de sauvegarde et restauration :** Cette étape consiste à adopter une méthodologie permettant d'élaborer le plan de sauvegarde en :

   ✓ Identifiant exhaustivement les composants logiciels systèmes et applicatifs, et les données à sauvegarder.
   ✓ Formalisant les procédures de sauvegarde, de restauration et de gestion des supports de sauvegarde.

3. **Adoption de pratiques conformes à l'état de l'art :** Cette procédure identifie les bonnes pratiques conformes à l'état de l'art. Pour tenir compte de la diversité des SIS et identifier rapidement les règles applicables, des éléments de contexte sont fournis (par exemple serveur, poste de travail).

4. **Restauration et contrôle :** Il est essentiel d'avoir l'assurance permanente que le dispositif de sauvegarde et restauration permet de revenir à un état stable antérieur. Alors il est obligatoire d'identifie les règles et les points de contrôle qui permettent de s'assurer que les sauvegardes restent utilisables dans le temps, en particulier par des tests de restauration réguliers.

II.7.4.4 Externalisation de la sauvegarde

Au vu de la complexité de la mise en œuvre de dispositifs de sauvegardes efficaces par rapport aux moyens dont dispose le responsable, le recours à un prestataire peut être une solution adaptée. Les avantages offerts par une telle solution sont nombreux : [22]

- Expertise pour la formalisation des procédures de sauvegarde et de restauration ;
- Garantie de cohérence et d'exhaustivité du périmètre sauvegardé accrue ;
- Conformité aux bonnes pratiques de sauvegardes et de restauration ;
- Contractualisation des engagements ;
- Coût du service optimisé avec la possibilité de bénéficier de services étendus comme la sauvegarde permanente sous forme de synchronisation de données.

Pour garantir les moyens de garder la maîtrise de ce type de solution, des informations sur le suivi des dispositions de sauvegarde et de continuité de l'hébergeur, mais aussi : [21]

✓ La protection des données sensibles ;
✓ Le droit d'audit ;
✓ La réversibilité de la solution ;
✓ La propriété des informations ;
✓ La traçabilité des opérations.

II.7.5 Mises à jour du système

Pour éviter les dénis de services applicatifs, on doit maintenir tous les logiciels de son système à jour puisque les mises à jour permettent souvent de corriger des failles logicielles, qui peuvent être utilisées par un attaquant pour mettre l'application hors service, ou pire, le serveur. Il est donc impératif de mettre son système à jour très régulièrement car c'est un moyen très simple à mettre en place pour se protéger des attaques applicatives.

L'édition des options dans les fichiers de configuration qui stocke des données concernant chaque connexion reçue par la machine telle l'adresse IP source, le numéro de port, l'âge de la connexion. En analysant ces données, on peut facilement détecter les comportements suspects et éviter certains types d'attaque. [1]

II.8 Protocoles de sécurité

II.8.1 IPsec (Internet Protocol Security)

II.8.1.1 Définition & rôle

IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait, d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges. Sa position dans les couches basses du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux basés sur IP sans distinction. IPSec est très largement utiliser pour le déploiement de réseau VPN à travers Internet a petite et grande échelle. [13]

IPSec est conçu pour sécuriser le protocole IPv6. La lenteur de déploiement de ce dernier a imposé une adaptation d'IPSec à l'actuel protocole IPv4. On établit un tunnel entre deux sites (voir **figure II.22**) dont l'IPSec gère l'ensemble des paramètres de sécurité associés à la communication. Deux machines passerelles, situées à chaque extrémité du tunnel, négocient les conditions de l'échange des informations : quels algorithmes de chiffrement, quelles méthodes de signature numérique ainsi que les clés utilisées pour ces mécanismes. [1]

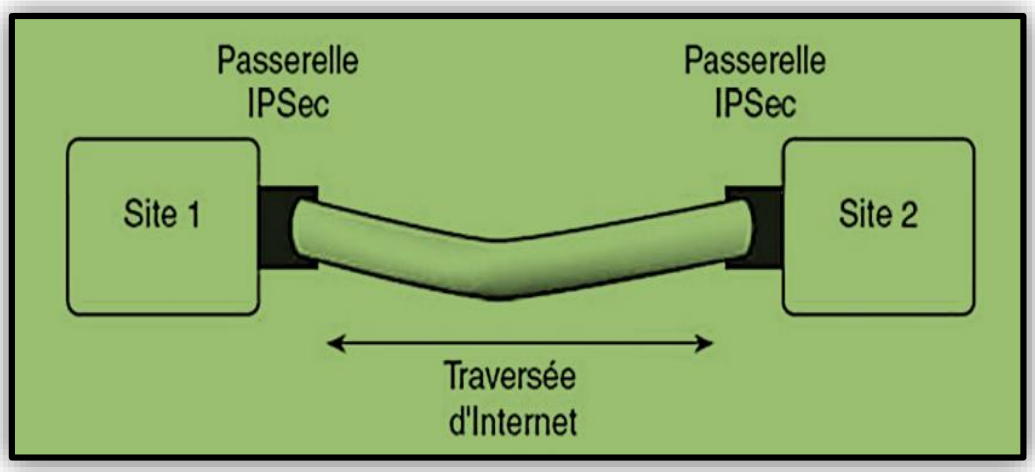


Figure II.22 Un tunnel IPSec entre deux sites d'entreprise

II.8.1.2 Fonctionnalités d'IPSec

Les principales fonctions que peut assurer le protocole IPsec sont : [13]

- **Authentification des données** : Permet de s'assurer pour chaque paquet échangé qu'il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.
- **Authentification des extrémités** : Cette authentification mutuelle permet à chacun de s'assurer de l'identité de son interlocuteur à l'établissement du tunnel. Elle s'appuie sur le calcul d'intégrité pour garantir l'adresse IP source.

- **Confidentialité des données** : IPSec permet si on le désire de chiffrer le contenu de chaque paquet IP pour éviter la lecture de ceux-ci par quiconque. Elle est assurée par un chiffrement symétrique des données.
- **Intégrité des données** : IPSec permet de s'assurer qu'aucun paquet n'a subi de modification quelconque durant son trajet en rajoutant à chaque paquet IP le résultat d'un calcul de hachage (SHA-1 ou MD5) portant sur tout ou partie du datagramme.
- **Protection contre les écoutes et analyses de trafic** : IPsec permet de chiffrer les adresses IP réelles de la source et de la destination, ainsi que tout l'en-tête IP correspondant.
- **Protection contre le rejeu** : IPSec permet de se prémunir des attaques consistantes à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau pour bénéficier des mêmes avantages que l'envoyeur initial. Elle est assurée par la numérotation des paquets IP et la vérification de la séquence d'arrivée des paquets.

II.8.1.3 Modes d'IPSec

Il existe deux modes d'utilisation d'IPSec : [13]

1. **Mode Transport :** Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiés et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté. Ce mode est souvent utilisé pour sécuriser une connexion Point-To-Point.
2. **Mode Tunnel** : Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliqué sur un tunnel IP. Ainsi, les entêtes IP originaux ne sont pas modifiés et un entête propre à IPSec est créé. Ce mode est souvent utilisé pour créer des tunnels entre réseaux LAN distant. Effectivement, il permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc, pas forcément prêtes à utiliser le protocole IPSec.

II.8.1.4 Les protocoles utilisés par IPSec

IPSec fait appel à deux mécanismes de sécurité pour le trafic IP : [13]

- **AH** (Authentication header) : Le protocole AH assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification. Tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejeu.
- **ESP** (Encapsulation Security Payload) : Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel. C'est pour ces raisons que ce protocole est le plus largement employé.

II.8.2 SSH (Secure Shell)

II.8.2.1 Definition du SSH

SSH (Secure Shell) est une approche populaire puissante basé sur un logiciel de sécurité du réseau. A chaque fois que les données sont envoyées par ordinateur au réseau, SSH crypte automatiquement ces

données. Lorsque les données atteignent leur destinataire, SSH décrypte ces données automatiquement. SSH utilise des algorithmes de cryptage modernes et il est suffisamment efficace pour être trouvé dans les applications à mission critique dans les grandes sociétés. Le protocole SSH a été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet, rcp, ftp et rsh. [16]

II.8.2.2 Développement du SSH

SSH-1 (Secure Shell) a été développé en 1995 par Tatu Ylonen, un chercheur dans laboratoire informatique à l'université d'Helsinki en Finlande. En Juillet 1995, la première version de SSH (SSH-1) a été publiée au public autant que un logiciel libre avec son code source permettant aux gens de le copier et utiliser le programme sans frais dans le but de sécuriser les communications distantes. A cause de plusieurs faiblesses et limites découvertes dans la première version de SSH, l'IETF a formé un groupe de travail appelé SECSH (Secure Shell) pour normaliser le protocole et guider sont développement dans l'intérêt public. Le groupe de travail a présenté le premier SECSH Projet Internet pour le protocole SSH-2.0 en Février 1997. [16]

- **Comparaisons entre les deux versions du SSH**

	SSH-1	SSH-2
Encapsulation	X11	X11, Forwarding, Transfert de Fichiers
Algorithmes	DES, 3DES, IDEA, Blowfish	3DES, Blowfish, CAST128, AES-256
Authentification	RSA (Faille de sécurité)	RSA, DSA, Diffie-Helman
Echange de clés	Pour la session	Renouvelées périodiquement
Intégrité	CRC4 (Faille de sécurité)	MD5, MD5-96, SHA1, SHA1-96

Tableau II.6 Comparaisons entre SSH-1 et SSH-2

II.8.2.3 L'architecture & le fonctionnement de base du protocole SSH

Le protocole SSH est un protocole applicatif (la couche 7 du modèle OSI) qui permet d'établir une connexion sécurisée entre un client SSH et un serveur SSH à distant. Il assure l'authentification, le chiffrement et l'intégrité des données transmises dans un réseau. Dans ce qui suit, nous présentons en trois protocoles SSH-2 (Voir la **Figure II.23**). Ce protocole est subdivisé en trois protocoles : [16]

- **SSH Transport Layer Protocol (SSH-TRANS)** : Définit le protocole de la couche transport. Ce protocole fournit un canal confidentiel sur un réseau non sécurisé. Il effectue l'authentification du serveur, l'échange de clé, le chiffrement, la protection de l'intégrité et la compression. Il tire aussi un identifiant de session unique qui peut être utilisé par les protocoles du niveau supérieur. La couche de transport sera généralement exécutée sur une connexion TCP/IP, mais peut aussi être utilisée au-dessus de tout autre flux de données fiable.

- **SSH Authentication Protocol (SSH-AUTH)** : Définit le protocole d'authentification. Ce protocole fournit un ensemble des mécanismes qui peuvent être utilisés pour authentifier le client pour le serveur. Les mécanismes individuels précisés dans le protocole d'authentification utilisent l'identifiant de la session fournie par le protocole de transport.

- **SSH Connection Protocol (SSH-CONN)** : Définit le protocole de connexion, ce protocole permet de multiplexer de canaux de communication logiques sur une seule connexion SSH sous-jacente.

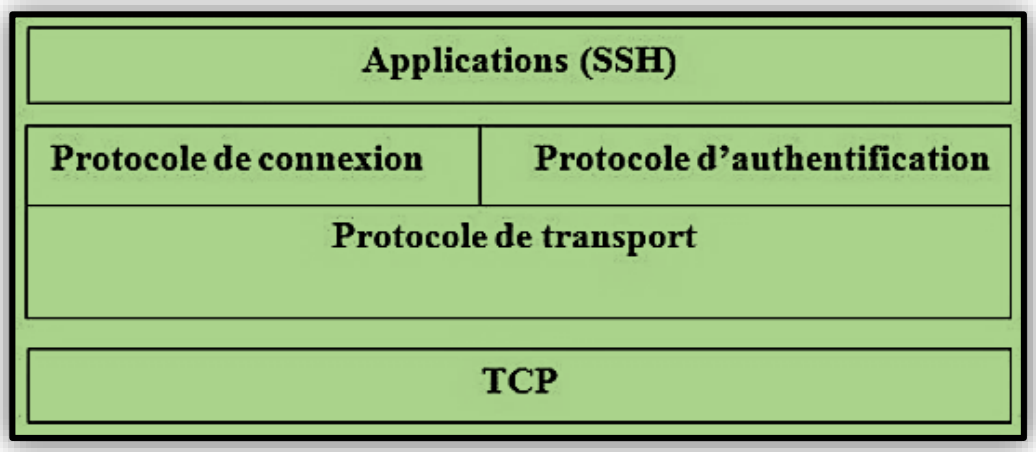


Figure II.23 L'architecture du protocole SSH-2

II.8.2.4 Adoption d'une Solution SSH pour sécuriser l'accès à distance

Implémentation du protocole "SSH" qui offre la possibilité de se connecter en toute sécurité à un hôte distant, en chiffrant toute la communication y compris la séquence d'authentification, ceci dans le but de palier aux vulnérabilités que présente le protocole "Telnet" définis pour assurer l'accès distant à un équipement. [2]

Dans ce qui suit nous allons présenter (dans la **figure II.24**) la configuration du SSH sur un commutateur "CISCO Catalyst 2960" :

```
Catalyst2960 (config)#  ip domain name  nom_du_domaine
Catalyst2960 (config) # crypto key generate rsa general-keys modulus modulo
Catalyst2960 (config)#  ip ssh version 2
Catalyst2960 (config)# live vty 0  4
Catalyst2960 (config-line)# transport input ssh
Catalyst2960 (config-line)# login local
Catalyst2960 (config-line)# exec-timeout 0 30
Catalyst2960 (config)# access-class 10 in
Catalyst2960 (config-line)#exit
Catalyst2960 (config)# username nom_d'utilisateur  password  mot_de_passe
Catalyst2960 (config)# service password-encryption
Catalyst2960 (config)# enable secret mot_de_passe
```

Figure II.24 La configuration du SSH sur un commutateur

II.8.2.5 Phase d'initialisation du protocole SSH

Pendant la phase d'initialisation du protocole SSH (Voir la **Figure II.25**), la procédure de négociation des informations entre la machine cliente et la machine serveur se déroule comme suit : [16]

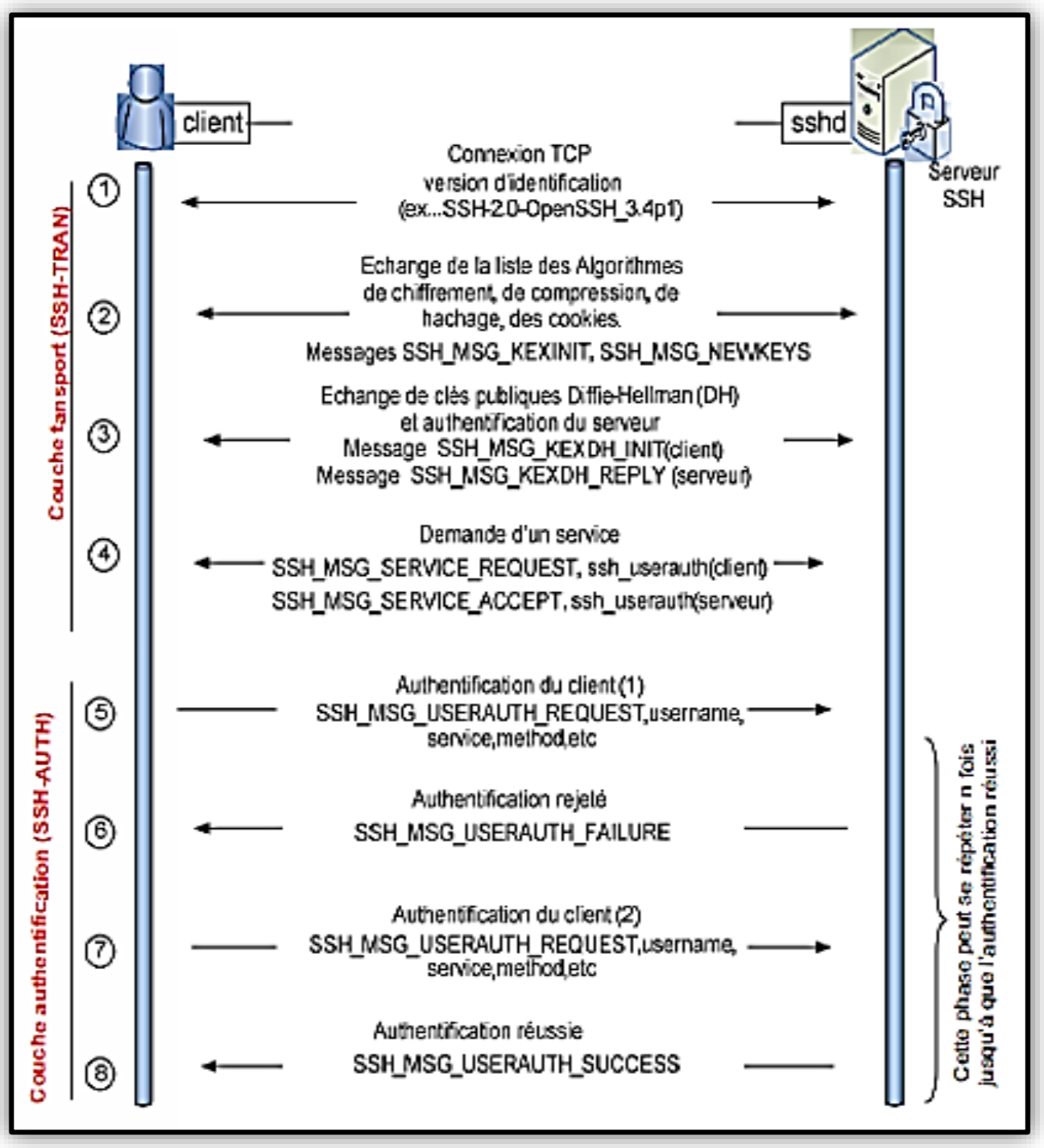


Figure II.25 La phase d'initialisation du protocole SSH-2

1. Le client et serveur se mettent d'accord sur la version du protocole SSH ;
2. Le serveur envoie au client la liste des méthodes d'authentification proposées, la liste des algorithmes de chiffrement proposés, des indicateurs d'extensions du protocole (par exemple, la méthode de compression, etc) et un cookie codé sur 64 bits dans le but de protéger le serveur contre l'attaque DoS ;

3. Le client envoie au serveur une copie du cookie, la liste des algorithmes de chiffrement sélectionnés et la liste des méthodes d'authentification sélectionnées ;
4. Le client et le serveur sélectionnent les meilleurs algorithmes parmi les algorithmes proposés ;
5. Le client et le serveur échangent les valeurs de Diffie-Hellman ; puis, ils calculent un identifiant de session à partir de ces valeurs ;
6. Le serveur envoie au client sa clé publique et il signe les valeurs échangées précédemment avec sa clé privée ;
7. Le client passe en mode crypté après la vérification de la signature de serveur ;
8. Le serveur envoie au client un message de confirmation crypté ;
9. Les deux entités passent en mode crypté ;
10. Le client envoie au serveur la demande d'un service ;
11. Le serveur sélectionne les méthodes d'authentification ;
12. Finalement, le client envoie au serveur la méthode d'authentification choisie qui peut être acceptée ou rejetée par le serveur.

II.8.2.6 Méthodes d'authentification de la version 2 normalisée par l'IETF

Le protocole SSH-2 supporte plusieurs méthodes d'authentification avec des propriétés de sécurité différentes. [16]

1. **Password**

- Il s'agit de l'authentification classique, le client envoie d'une maniéré sécurisée au serveur sur mot de passe ;
- Le serveur récupère le mot de passe et calcule son hash ; puis, il compare le hash calculé avec l'empreinte du mot de passe du client stocké dans sa base de données ;
- Notons que :

  ✓ Dans le système Unix, les mots de passe stockés dans la base de données sont chiffrés à l'aides de l'algorithme DES (via la fonction crypt ()).
  ✓ D'autres systèmes utilisent des fonctions de hachage telles que MD5 ou SHA-1.

2. **Publickey**

- L'authentification à clé publique est basée sur la cryptographie asymétrique (RSA ou DSA) où aucun secret ne circule sur le réseau. En effet, la clé publique du client doit être stockée sur le serveur SSH et sa clé privée doit être stockée sur sa machine d'une manière sécurisée ;
- Publickey (RSA ou DSA) possède un niveau de sécurité plus élevé que le système par mot de passe.

II.8.3 SSL (Secure Sockets Layer) & TLS (Transport Layer Secure)

II.8.3.1 Définition

SSL/TLS sont des protocoles de sécurisation des échanges sur internet. Ils sont utilisés pour apporter plusieurs fonctions de sécurité lors de l'échange de données. SSL/TLS fonctionnent suivant un mode client-serveur avec l'interdiction d'une nouvelle couche de communication entre celle du transport et celle d'application du modèle TCP/IP dédié à la sécurité. SSL assure la confidentialité et l'intégrité des données, l'authentification et la non répudiation, SSL est supporté par les principaux navigateurs. De plus, SSL peut être adapté à n'importe quelle plate−forme de serveur Web car son code source est disponible. [36] [23]

II.8.3.2 Fonctionnement de SSL/TLS

Avant d'expliquer le fonctionnement de TLS, il est important de faire un point sur l'état actuel des choses et comprendre pourquoi on a besoin de cette couche de sécurité supplémentaire. Sans SSL/TLS, les informations sont envoyées en clair lors d'un échange entre un client et un serveur.

Le problème est que si quelqu'un se connecte au réseau, il lui serait facile d'intercepter les données échangées (**Sniffing attack**) et récupérer des informations. L'autre problème qu'on peut rencontrer est si quelqu'un pourrait faire semblant de se mettre à la place de serveur de destination (**Phishing attack**), alors il pourrait facilement faire croire à la victime qu'elle s'adresse à un tiers de confiance. Afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit. Donc l'enjeu de SSL/TLS est double.

D'une part, il permet de chiffrer les informations échangées entre le client et le serveur, et de l'autre part, une authentification est de s'assurer que l'ordinateur avec lequel on communique est bien celui qu'on prétend. [36]

II.8.3.3 Présentation des protocoles SSL/TLS

SSL/TLS est un protocole qui prend place entre le protocole de la couche de transport et la couche application, comme le montre la **figure II.26.** Le protocole SSL supporte l'utilisation d'un grand nombre d'algorithmes de cryptographie, ou de chiffrement, pour des opérations telles que l'authentification réciproque d'un serveur et d'un client, la transmission de certificat, et l'établissement d'une clef de session. Les clients et les serveurs peuvent supporter différentes suites de chiffrement, c'est à dire différents ensembles d'algorithmes, selon la version de SSL qu'ils intègrent, le protocole de négociation SSL détermine comment serveur et client choisissent l'algorithme de chiffrement utilisé pour s'authentifier l'un à l'autre, pour transmettre des certificats et pour établir les clefs de session.

Les données qui vont et viennent entre le client et le serveur sont chiffrées à l'aide d'un algorithme symétrique tel que DES ou RC4. Un algorithme de clé publique (généralement RSA) est utilisé pour l'échange des clés de chiffrement et pour les signatures numériques. L'algorithme utilise la clé publique du certificat numérique du serveur. Ce dernier permet également au client de vérifier l'identité du serveur. Les versions 1 et 2 du protocole SSL offrent uniquement l'authentification serveur. La version 3 inclut l'authentification client, utilisant les certificats numériques du client et du serveur. [11]

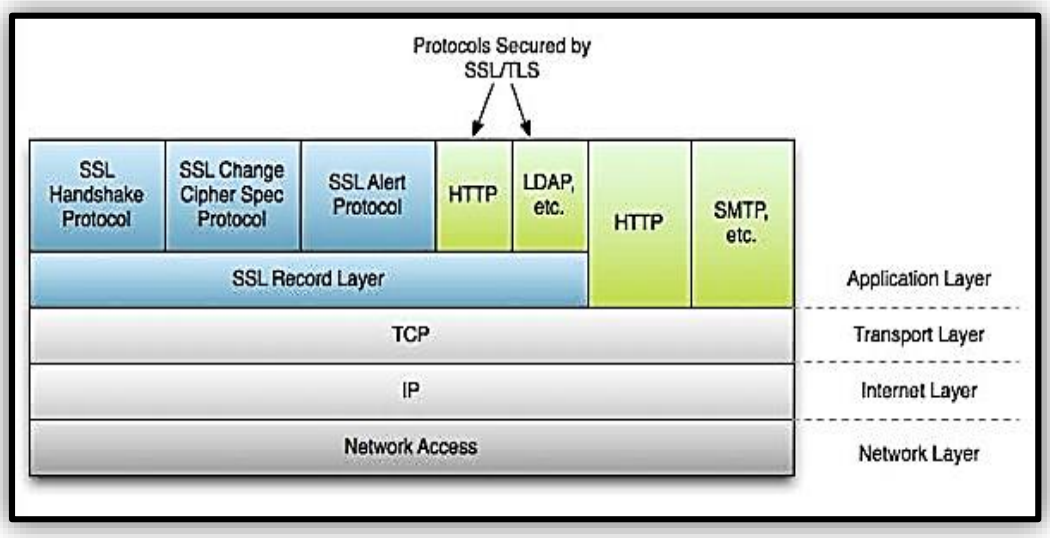


Figure II.26 Place du protocole SSL dans la suite TCP/IP

II.8.3.4 Protocoles de SSL/TLS

SSL/TLS utilise plusieurs protocoles pour la protection et la mise en place de la session sécurisée :

Le premier protocole **« SSL handshake »** permet l'échange des paramètres de sécurité (Nombres aléatoires, liste des algorithmes). Il permet aussi l'authentification des deux communicateurs. Cependant, dans la plupart des cas, le serveur est uniquement authentifié. Ce protocole fait intervenir les échanges suivants entre le client et le serveur (Voir la **figure II.27**). [W3]

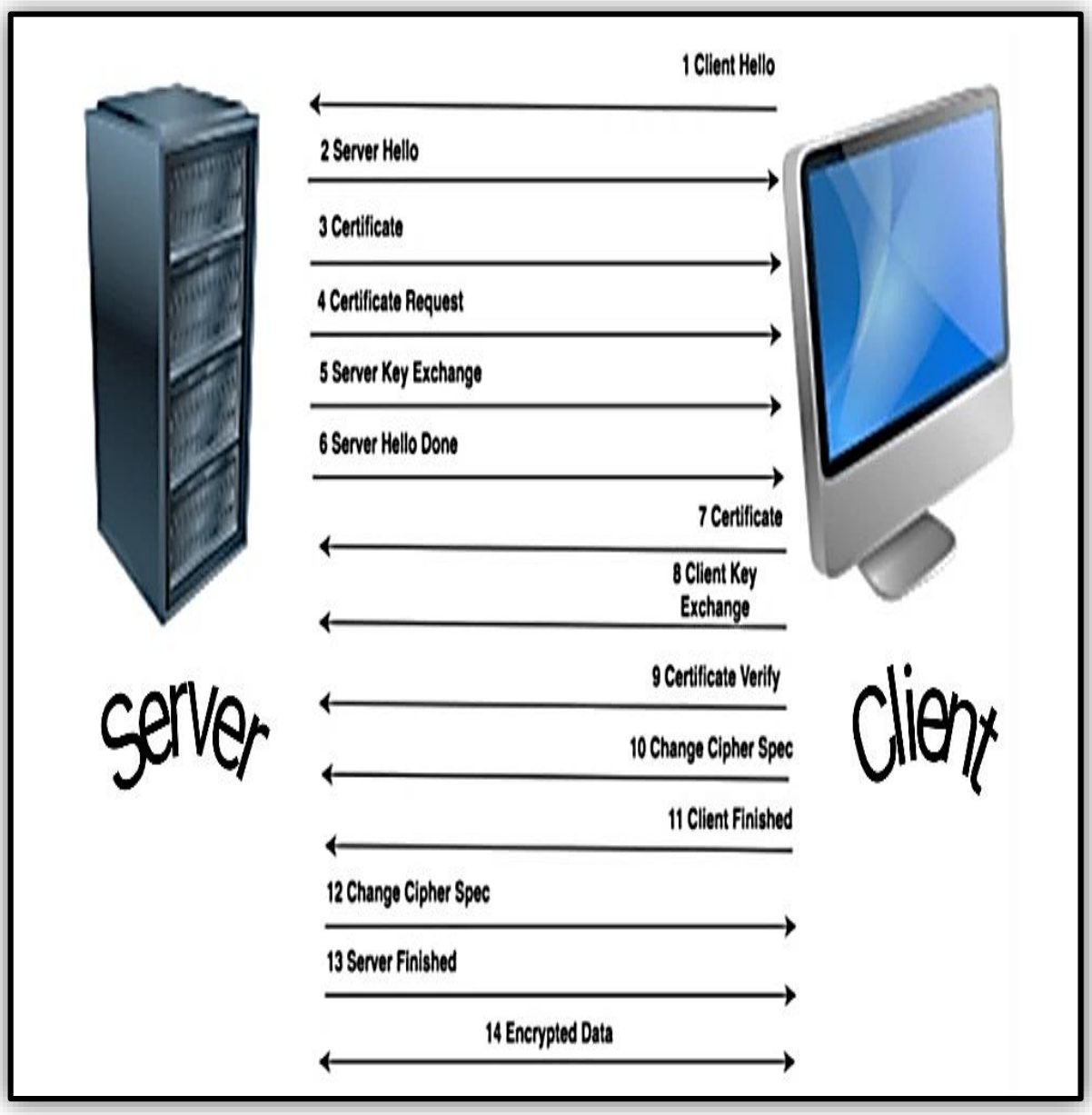


Figure II.27 Les étapes de SSL handshake

1. **Client Hello** : Envoi de la version maximale supportée (SSL = 3.0), de la suite d'algorithmes supportés (par ordre de préférence décroissant) et une valeur aléatoire de 32 octets.
2. **Server Hello** : Choix de la version de la suite d'algorithmes (Cipher Suite) et d'une valeur aléatoire.
3. **Certificate (optionnel)** : Envoi d'une chaîne de certificats par le serveur. Le premier certificat est celui du serveur, le dernier est celui de l'autorité de certification.

4. **Certificate Request (optionnel)** : Demande un certificat au client pour l'authentifier.
5. **Server Key Exchange (optionnel) :** Message complémentaire pour l'échange des clés. Ce message contient la clé publique du serveur utilisée par le client pour chiffrer les informations de clé de session.
6. **Server Hello Done** : Fin des émissions du serveur.
7. **Certificate (optionnel)** : Certificat éventuel du client si le serveur demande une authentification.
8. **Client Key Exchange** : Le client produit un secret pré-maître (encrypted pre-master key) et le crypte avec la clé publique du certificat du serveur. Ces informations sont chiffrées une deuxième fois avec la clé publique du serveur (et non la clé publique du certificat du serveur) reçue dans le message Server Key Exchange**.**
9. **Certificate Verify (optionnel)** : Message contenant une empreinte (hash) signée numériquement et créée à partir des informations de clé et de tous les messages précédents. Ce message permet de confirmer au serveur que le client possède bien la clé privée correspondante au certificat client.
10. **Change Cipher Spec** : Passage du client en mode chiffré avec la clé master comme clé symétrique.
11. **Client Finished** : Fin des émissions du client, ce message est chiffré à l'aide des paramètres de la suite de chiffrement.
12. **Change Cipher Spec** : Passage du serveur en mode chiffré avec la clé master.
13. **Server Finished** : Confirmation au client du passage en mode chiffré. Ce message est chiffré à l'aide des paramètres de la suite de chiffrement.
14. **Encrypted Data** : Le tunnel SSL/TLS est établi, c'est maintenant le Record Protocol qui prend le relais pour chiffrer les données.

Le deuxième protocole **« SSL change Cipher Spec Protocol »** est utilisé pour indiquer un changement dans les algorithmes de chiffrement cryptographique, immédiatement après le changement toutes les données sont cryptées avec le nouveau chiffrement sélectionné. Le troisième protocole **« SSL Alert Protocol »** est responsable de la signalisation des problèmes dans la session SSL. Le dernier protocole **« SSL Record Layer Protocol »** une fois négocier ce protocole chiffre toutes les informations échanger et effectuer divers contrôles. [36]

II.8.3.5 Certificat SSL

Le certificat SSL est un certificat électronique qui permet de sécuriser les communications entre des serveurs web et des navigateurs. Techniquement, le certificat SSL se résume à un fichier de données utilisé pour crypter des informations sensibles sur la Toile. C'est ce certificat qui se cache derrière le protocole https (avec le petit cadenas dans la barre d'adresse), assurant une certaine sécurité de la connexion sur un serveur Web et sur un site Web.

La plupart du temps, le certificat SSL est utilisé pour sécuriser au maximum les transactions bancaires lors d'achats effectués en ligne. Mais il sert également à un nom d'utilisateur et un mot de passe, notamment sur les réseaux sociaux. Des entreprises comme OVH, se sont spécialisées dans le développement de certificat SSL destinés à sécuriser les contenus en ligne. [W4]

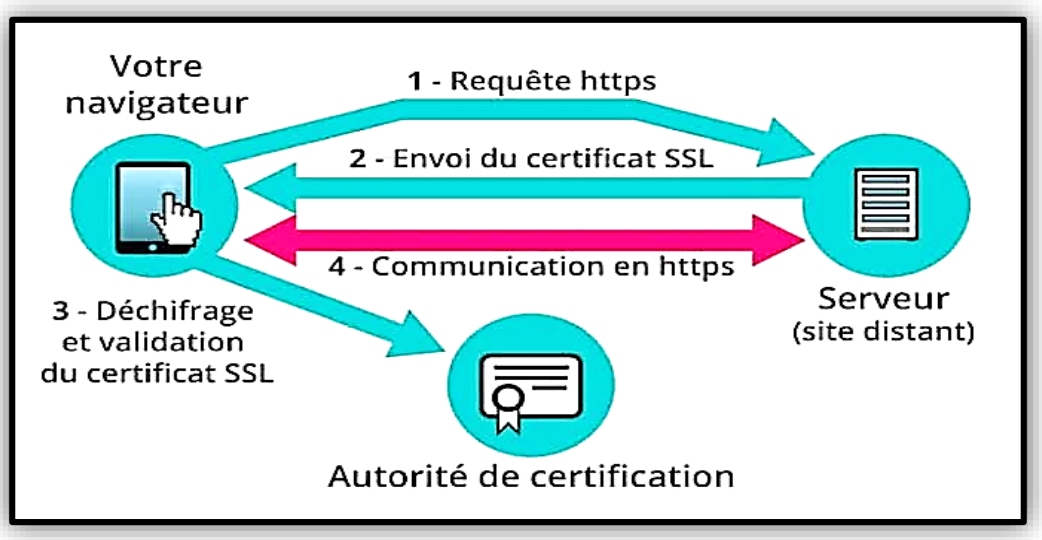


Figure II.28 Certificat SSL

II.9 Conclusion

Aujourd'hui il est devenu plus difficile de garantir la sécurité d'un système dans un réseau, pour cela les laboratoires de recherche essayent toujours de développer de nouvelles techniques pour faire face aux différentes attaques qui peuvent perturber ou menacer un réseau. Ces techniques de parades et contre-mesures qui permettent de contrer les attaques ont une démarche capitale et primordiale pour le bon fonctionnement d'un réseau, dans ce chapitre nous avons présenté un aperçu des différentes solutions et caractéristique des mécanismes de sécurité.

Dans le chapitre suivant, nous allons étudier et décrire le fonctionnement de chaque mécanisme de sécurité. Aussi la réalisation et l'implémentation de ces mécanismes et leurs rôles dans les réseaux Cisco.

CHAPITRE III

Conception & Implémentation des Mécanismes de Sécurité Réseaux CISCO

III.1 Introduction

Dans ce chapitre, nous allons passer à la seconde étape de notre travail qui est la réalisation de notre projet. Cette dernière est une cruciale pour la mise en place de tout ce que nous avons vu dans le précédent chapitre.

Nous implémentons les solutions précédemment proposés et conçus, pour ce faire, nous commençons par la présentation du simulateur utilisé (l'environnement matériel et logiciel du projet), puis nous allons expliquer en détails les différentes étapes suivies pour la réalisation des réseaux LANs et nous finirons par la configuration des différents mécanismes et protocole de sécurité dans les réseaux CISCO.

III.2 Présentation de simulateur Cisco Packet Tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipement tels que les routeurs, les commutateurs, les ordinateurs. Ces équipements doivent ensuite être reliés, il est possible pour chacun d'entre eux de configurer les adresses IP, les services disponibles, etc.

Le but de Packet Tracer est d'offrir aux étudiants et aux professeurs un outil permettant de créer des réseaux virtuellement. La **figure III.1** montre un aperçu général de Packet Tracer. [7] [W5]

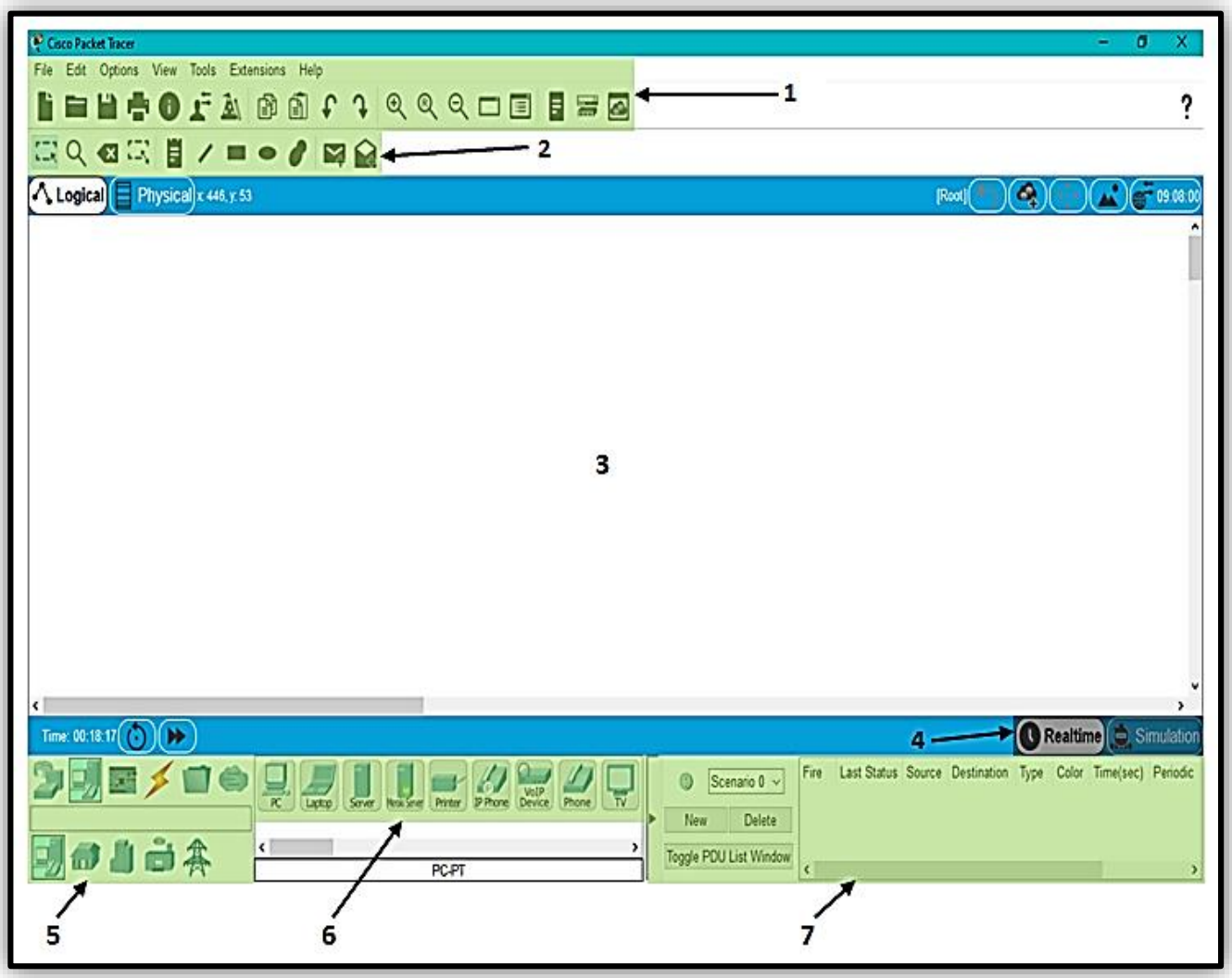


Figure III.1 Interface Cisco Packet Tracer

- **Zone (1) : La barre de menu**

Dans cette zone on retrouve les fonctions standards présentent dans n'importe quel logiciel. On retrouve aussi la fonction « sauvegarder », « ouvrir un fichier », « nouveau fichier » et d'autres fonctions de base.

- **Zone (2) : Barre D'outils**

La barre d'outils se décompose en plusieurs outils :

1. **Select** « le carré avec flèche » : Sert à sélectionner un élément aussi Permet de déplacer ou d'éditer des équipements ;
2. **Inspect** « la loupe » : Sert à inspecter un équipement, un paquet, une table. Autrement dit elle Permet d'ouvrir une fenêtre d'inspection (table ARP, routage) sur un équipement ;
3. **Delete** « la croix » : Sert à supprimer un élément (un équipement ou une note) ;
4. **Resize** « le carré avec la flèche de deux coté » : Sert à redimensionner une forme créée ;
5. **Place note «** la page » : Sert à ajouter une zone de texte sur le réseau ;
6. **Move layout** « Le déplacement de disposition » : Permet de déplacer le plan de travail ;
7. **Draw line** : Sert à dessiner une ligne ;
8. **Draw rectangle** : Sert à dessiner un rectangle ;
9. **Draw ellipse** : Sert à dessiner une ellipse ;
10. **Draw freeform** : Sert à créer des formes libres ;
11. **Add Simple PDU** « enveloppe fermée » : Sert à ajouter un PDU « Protocol Data Unit » simple (ICMP) ;
12. **Add Complex PDU** « enveloppe ouverte » : Sert à ajouter des PDU complexes (Telenet, SSH …).

- **Zone (3)** : **Zone de travail**

La zone de travail est l'endroit où nous plaçons les équipements pour les connecter entre eux et les configurer pour créer le réseau souhaité veut dire c'est la partie ou est construit.

- **Zone (4) : Temps réel / Simulation**

Cette fonction sert à passer du temps réel au mode Simulation. En temps réel on configure nos équipements et on les tests. Le mode simulation est un mode pas à pas qui permet d'étudier plus en détails les échanges fait entre les équipements.

- **Zone (5) : Choix d'équipement**

Une fois la catégorie de l'équipement choisit la zone 6 nous permet de choisir notre modèle souhaité en fonction des besoins nécessaires à la création de notre réseau.

- **Zone (6) : Types d'équipements**

Dans cette zone il y a toutes les catégories d'équipement disponible dans le logiciel. Par exemple La première image en haut à droite dans la zone 5 sélectionne la catégorie PC-PT.

- **Zone (7) : Affichage des paquets**

Dans cette fenêtre on voit les paquets qui seront utilisés lors des simulations du réseau.

III.2.1 Construction d'un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer qui sont : les routeurs, les switches, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multi-utilisateurs.

Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi. La figure suivante correspond à la zone décrite. [39]

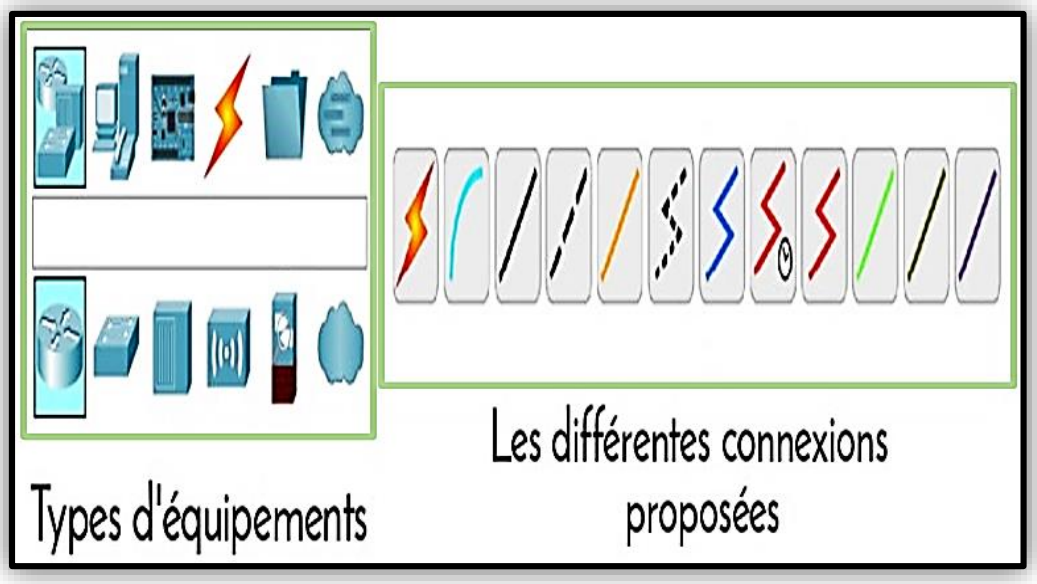


Figure III.2 Différents types d'équipements et connexions

III.2.2 Mode simulation

Packet Tracer permet de simuler le fonctionnement d'un réseau par l'échange de trames Ethernet et la visualisation de celles-ci. Il existe deux modes de simulation :

- La simulation en temps réel (**RealTime**) : Elle visionne immédiatement tous les séquences qui se produisent en temps réel ;
- La simulation permet de visualiser les séquences au ralenti entre deux ou plusieurs équipements.

III.2.2.1 Simulation en temps réel

1. **Réalisation d'un PING :** Un PING fait appel au protocole ICMP. Packet Tracer permet de faire un Ping rapidement avec l'outil **Add Simple PDU**. Premièrement on sélectionne l'outil ensuite on clique sur l'ordinateur émetteur du PING. Outre, on clique sur l'ordinateur destinataire du PING et par la fin on regarde la fenêtre d'état qui nous montre de la réussite (Successfull) ou de l'échec (Failed) de la transaction. [39]
2. **Simulation en ligne de commande :** Comme sur un vrai ordinateur, il est possible par ligne de commande saisir des commandes réseau (IPCONFIG, PING, ARP...). Cette opération se déroule en ouvrant la fenêtre de configuration de l'ordinateur en cliquant sur sa représentation, ensuite, on choisit l'onglet **Desktop** après il faut sélectionner l'outil **Command Prompt** ou on peut saisir la commande souhaitée et on la valide par la touche **ENTREE.** [39]

III.2.2.2 Simulation et analyse de trame

En activant le mode **Simulation**, les échanges de trames sont simulés par des déplacements d'enveloppes sur le schéma. Les manipulations peuvent être les mêmes qu'en mode **RealTime** mais des animations visuelles montrent le cheminement des informations. [39]

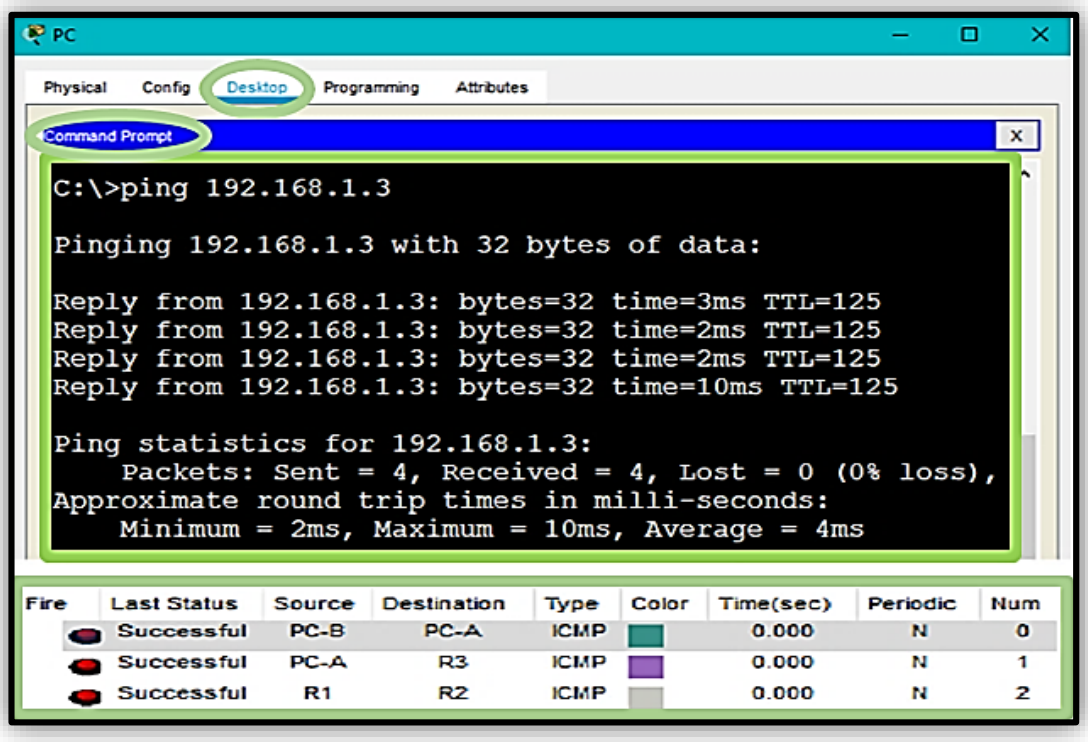


Figure III.3 Mode simulation en temps réel (RealTime)

III.3 Description de matériels utilisés dans la simulation

III.3.1 Routeur

Le routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets. Un routeur est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en utilisant le meilleur chemin possible selon l'adresse destination et l'information contenue dans sa table de routage. [W6] La **figure III.4** illustre ça forme :

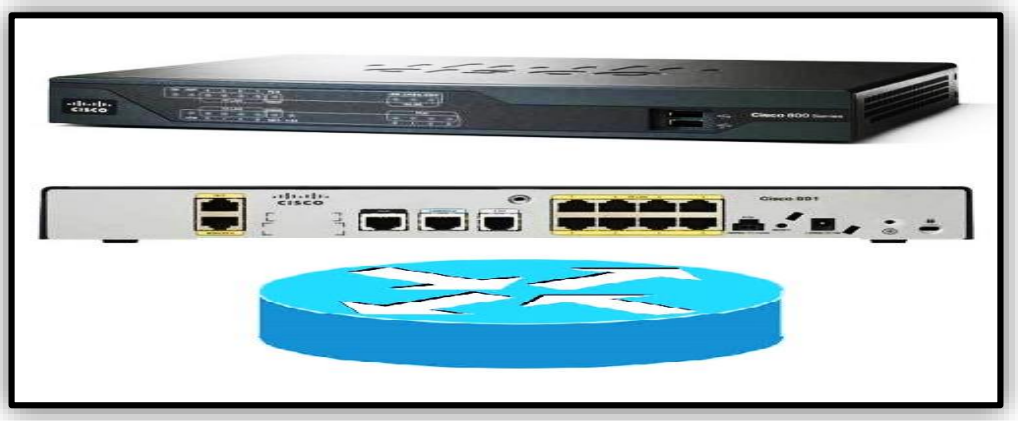


Figure III.4 Routeur Cisco

➢ **Architecture des routeurs Cisco**

Les routeurs Cisco ont une architecture interne qui peut être représenté par la **figure III.5** :

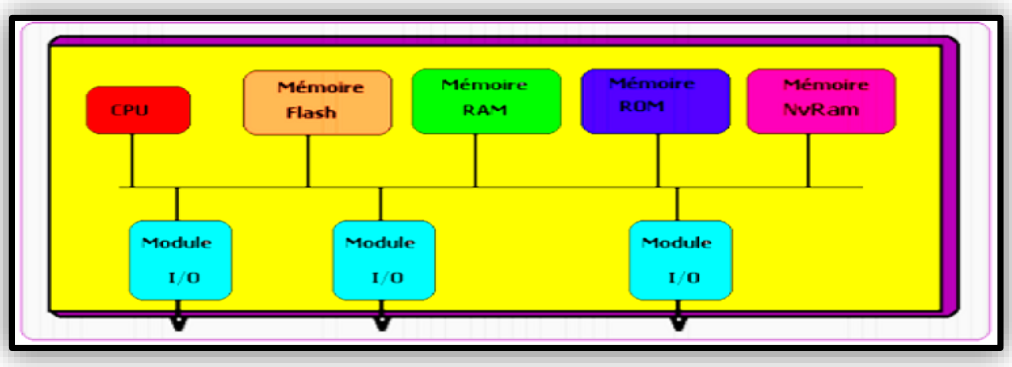


Figure III.5 Architecture interne d'un routeur Cisco

Les routeurs Cisco contiennent : [w6]

- Une mémoire NVRam pour Ram non Volatile et sur laquelle l'administrateur organisation va stocker la configuration qu'il aura mise dans le routeur. Elle contient également la configuration de l'IOS ;
- Une carte mère qui est en général intégrée au châssis ;
- Une CPU qui est un microprocesseur Motorola avec un BIOS spécial nommé I.O.S « Pour Internetwork Operating System » ;
- Une mémoire RAM principale contenant le logiciel IOS, c'est dans laquelle tout sera exécuté un peu à la manière d'un simple ordinateur ;
- Une mémoire FLASH, également une mémoire non volatile sur laquelle on stocke la version courante de l'IOS du routeur ;
- Une mémoire ROM non volatile et qui, quant à elle, contient les instructions de démarrage (bootstrap) et est utilisée pour des opérations de maintenance difficiles de routages, ARP, etc, mais aussi tous les buffers utilisés par les cartes d'entrée.

III.3.2 Serveur informatique

Un serveur informatique est un dispositif informatique (matériel et logiciel) qui offre des services à un ou plusieurs clients (parfois des milliers) en réseau Internet ou intranet. [W7] La **figure III.6** représente un serveur :

Figure III.6 Serveur Cisco

III.3.3 Switch

Appelé aussi commutateur, est un multiports c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de commutation ou de réseaux commutés). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité. [40] La **figure III.7** représente un Switch :

Figure III.7 Switch Cisco

III.3.4 ASA 5505

Les Serveurs de Sécurité Adaptatifs Cisco ASA 5505 combinent les meilleurs services de VPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (le réseau qui se défend tout seul), la gamme Cisco ASA 5505 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible.

Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises tout en réduisant l'ensemble des frais de déploiement et d'exploitation et en simplifiant les tâches généralement associées à un tel niveau de sécurité. [W8]

Figure III.8 Cisco ASA 5505

III.3.5 PC Ordinateur / Laptop

1. **PC Ordinateur** : Un ordinateur de bureau ou ordinateur fixe (Desktop Computer) est un ordinateur personnel destiné à être utilisé sur un bureau ou tout autre endroit fixe à cause de ses dimensions, de sa masse et de son alimentation électrique. Les ordinateurs de bureau ne sont pas conçus pour être portables; ils utilisent un écran, un clavier et une souris externes. Les ordinateurs de bureau sont conçus pour un large éventail d'applications domestiques et bureautiques, y compris en matière de courrier électronique, de navigation sur le web, de traitement de texte, de graphisme, de jeu, etc. [W9]

2. **Laptop** : Un ordinateur portable est un ordinateur personnel dont le poids et les dimensions limitées permettent un transport facile. Les ordinateurs portables ont plusieurs usages, à la fois professionnels, personnels et éducatifs. [W10]

Figure III.9 Ordinateur fixe / Laptop

III.3.6 Câbles de connexions

III.3.6.1 Câble réseau cuivre à connexion directe (DAC)

Le DAC (Direct Attach Copper) est un câble en cuivre qui se présente en tant que câble Twinax actif ou passif et qui se connecte directement au logement du transceiver de l'équipement réseau. Cette connectique est souvent appelée DAC. Le câble Twinax actif a des composants électroniques dans le logement du transceiver pour améliorer la qualité des signaux ; le câble Twinax passif est un simple « fil » dénué de composants pouvant redresser les signaux. [W11]

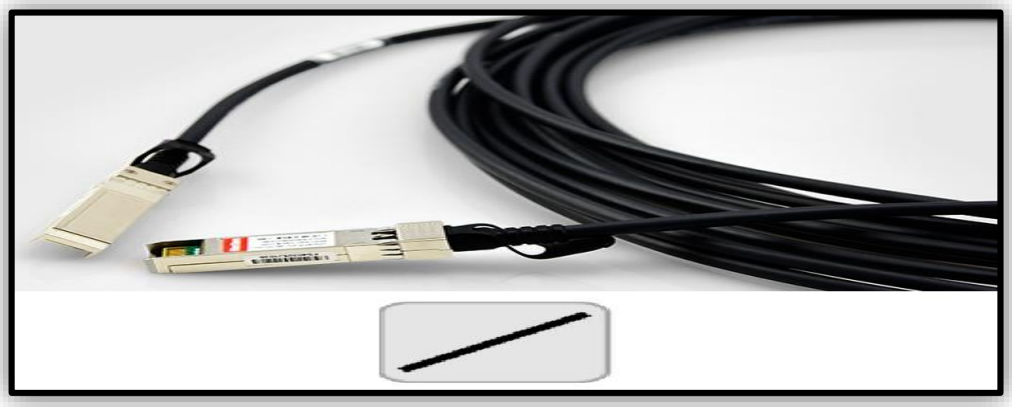


Figure III.10 Câble DAC

III.3.6.2 Câble réseau croisé en cuivre

Un câble croisé relie deux appareils du même type, par exemple DTE-DTE ou DCE-DCE, généralement connectés asymétriquement (DTE-DCE), par un câble modifié appelé réticulation. Une telle distinction entre les périphériques a été introduite par IBM. Le croisement de fils dans un câble ou dans un adaptateur de connecteur permet : [W12]

- Connexion directe de deux appareils, sortie de l'un à l'entrée de l'autre,
- Permettant à deux terminaux (DTE) de communiquer sans nœud de concentrateur d'inter-connexion, c'est-à-dire des PCs,
- Reliant deux ou plusieurs concentrateurs, commutateurs ou routeurs (DCE) ensemble, éventuellement pour fonctionner comme un appareil plus large.

Figure III.11 Câble croisé

III.3.6.3 Câble de survol

Le câble de survol (également appelé câble Yost, câble Cisco ou câble de console) est un type de câble null-modem qui est souvent utilisé pour connecter un terminal d'ordinateur au port de console d'un routeur.

Ce câble est généralement plat (et a une couleur bleu clair) pour aider à le distinguer des autres types de câblage réseau. Il obtient le survol du nom car les broches à une extrémité sont inversées de l'autre, comme si le fil avait été renversé et que vous le regardiez de l'autre côté. [W13]

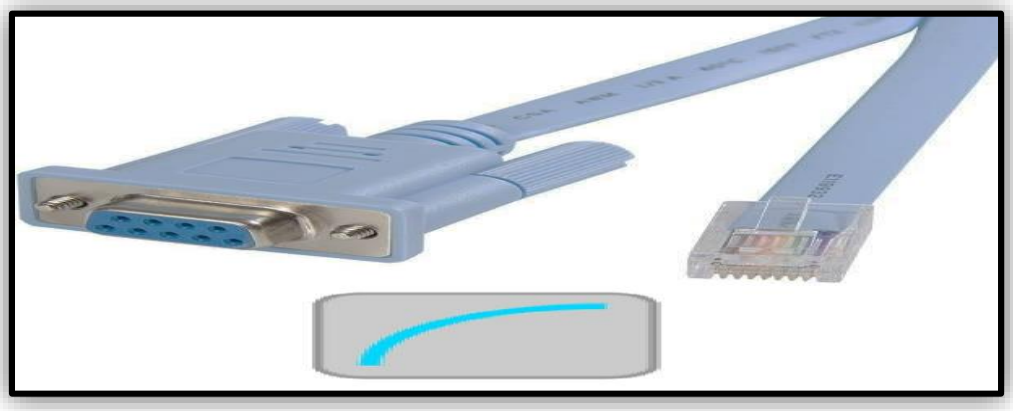


Figure III.12 Câble de console

III.3.6.4 Câble série DTE / DCE

DTE (Data terminating equipment) ou **ETTD** et **DCE** (Data circuit equipment) ou ETCD les deux termes sont fréquemment utilisés dans la communication de données et la mise en réseau; ces termes peuvent être considérés comme un type de dispositifs de communication série sur lesquelles reposes la connectivité WAN entre l'abonné et le fournisseur. La différence clé entre **DTE** et **DCE** est que **DCE** est généralement situé chez le fournisseur de service alors que **DTE** situé chez le client. [W14]

- **DTE** (Data Terminating Equipment) : Un équipement terminal de données (DTE) ou ETTD est un équipement qui est soit une source, soit une destination pour les données numériques. Les DTE ne communiquent généralement pas les uns avec les autres, ils doivent donc utiliser DCE pour établir la communication. Le DTE n'a pas besoin de savoir comment les données sont envoyées ou reçues; les détails de la communication sont laissés au DCE. Un exemple typique de DTE est un ordinateur
- **DCE** (Data Terminating Circuit Equipment) : Les équipements de communication de données (DCE) ou ETCD peuvent être classés comme des équipements qui transmettent ou reçoivent des signaux analogiques ou numériques via un réseau. DCE peut également être responsable de la synchronisation sur une liaison série. Dans un réseau complexe qui utilise des routeurs directement connectés pour fournir des liaisons série, une interface série de chaque connexion doit être configurée avec une fréquence d'horloge pour permettre la synchronisation.

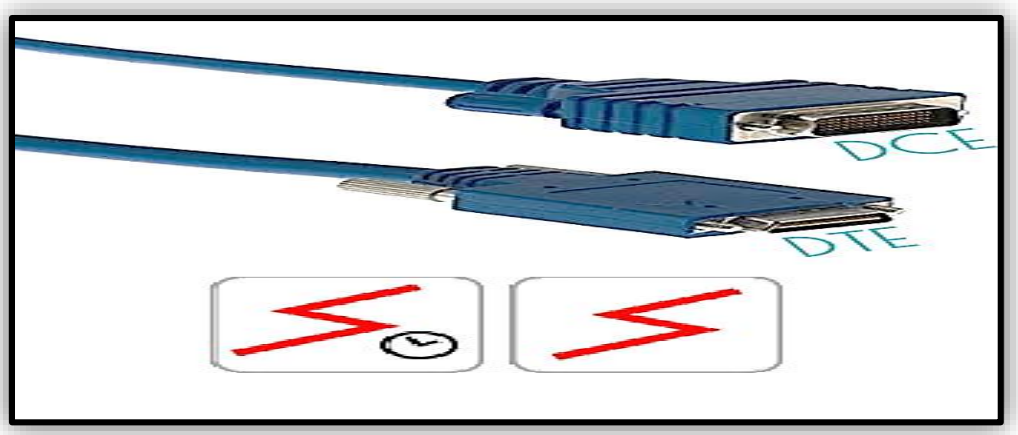


Figure III.13 Câble DTE / DCE

Le **Tableau III.1** illustre en détail les différents matériels utilisés dans notre simulation :

Equipement	Modèle et type
Routeurs (Routers)	Cisco 1941,1841
Commutateurs (switchs)	Cisco 2960-24TT, 2950-24TT, 3560-24TT
Serveur (Server)	Server-PT
Machines (Hôtes)	PC-PT, Laptop-PT
Emulation WAN	Cloud-PT

Serveur sécurité	5505
Connexions (Connections)	Direct en cuivre, Cross-Over en cuivre, Console, DCE série, DTE série

Tableau III.1 Présentation des équipements de la simulation

Nous nominons les équipements par des noms significatifs ou des abréviations pour faciliter la conception de l'architecture de chaque site. Le **Tableau II.2** résume les noms des équipements utilisés pour effectuer l'architecture réalisée.

Equipement	Nomination
Routeur	R1, R2, R3 …
Switch	S1 S2 S3, SW-1 SW-2, SW-A SW-B …
Hôtes	PC-A, PC-B PC-B1… ; PC C1, PC C2, PC C3, … ; laptop 1 …
Serveurs	Syslog server, RADIUS server, DMZ server, …

Tableau III.2 Nomination des équipements de la simulation

III.4 Réalisation des architectures LANs

Avant de commencer à configurer les différents mécanismes de sécurité et leurs implémentations dans les réseaux CISCO, nous sommes obligés de créer d'abord les architectures LANs. Ceci dit qu'à présent, nous allons lancer une série de configuration de bases (la configuration des routeurs, des Switchs et des PCs et des serveurs), pour réaliser les réseaux locaux que nous allons les présenter par la suite et une interconnexion de ces derniers.

III.4.1 Configuration de bases des équipements

La configuration des équipements du réseau sera faite au niveau des commutateurs (niveau 2), et au niveau des routeurs (niveau 3), ainsi qu'au niveau des PCs et serveurs. En effet, une série de configuration sera réalisée sur ces équipements, en montrant des exemples de chaque configuration.

La configuration d'un switch ou bien d'un routeur se fait par l'onglet CLI (Command Line Interface) on l'apercevra juste après dans la **figure III.14.**

L'accès au CLI se fait par console. Le port console permet de se connecter au CLI du Switch/Routeur même si celui-ci n'est pas déjà en réseau.

Tout switch/Routeur Cisco a un port console qui est physiquement un port RJ-45. Un câble console relie un PC (via le port série ou USB) au switch (via le port console).

Une fois que le PC est physiquement connecté au port console du switch/Routeur, on pourra commencer la configuration.

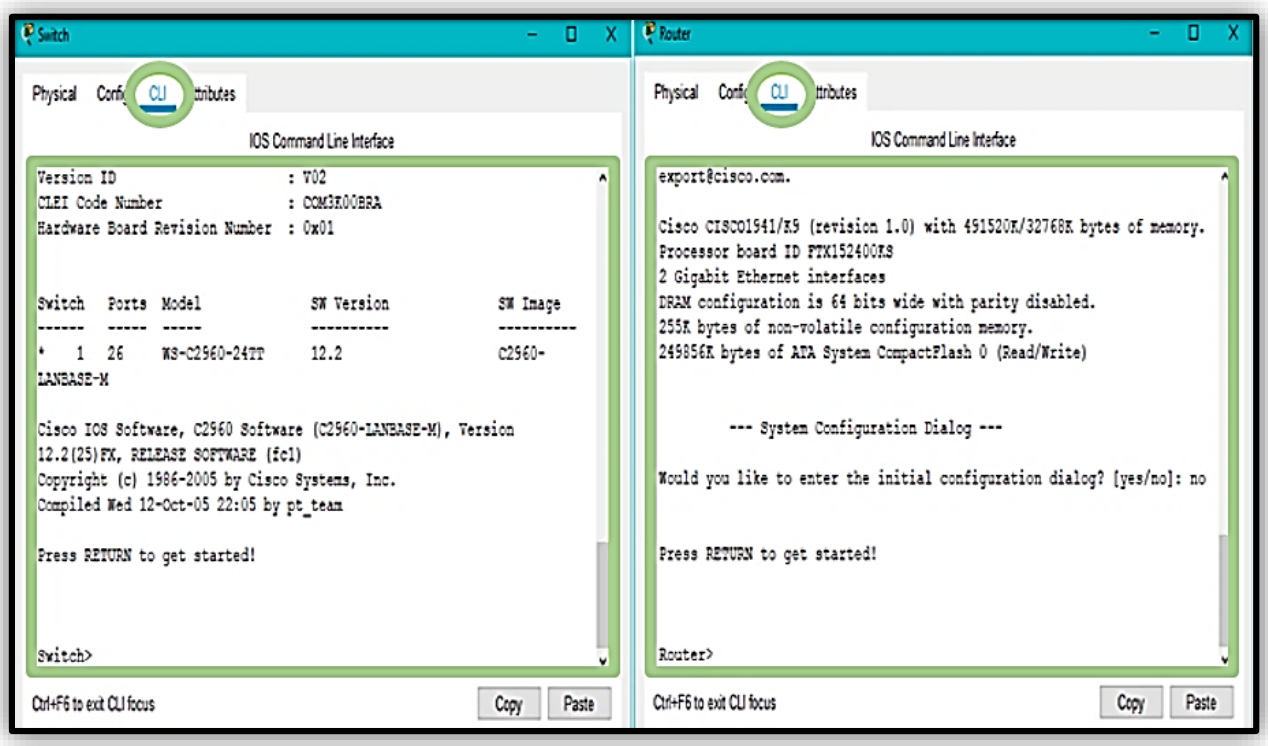


Figure III.14 L'onglet CLI

III.4.1.1 Configuration des hostnames

Le but de cette configuration est de renommer les commutateurs et les routeurs par des noms significatifs comme le montre la **figure III.15**. Sachant que c'est la même chose pour tous les autres switchs et routeurs.

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

Figure III.15 Nomination du Switch / Routeur

III.4.1.2 Configuration des mots de passe

Nous avons choisi « **reseaux_telecommunications_2020** » comme mot de passe via la console et « **master_2_telecommunications »** comme de passe pour accéder au mode privilégié pour les switches ou bien routeurs. La **figure III.16** montre les commandes de mise en place du mot de passe. La même chose sera faite pour tous les autres switchs et routeurs.

```
R1(config-line)#security password min-length 4
R1(config)#enable secret master_2_telecommunications
R1(config)#service password-encryption
R1(config)#line console 0
R1(config-line)#password reseaux_telecommunications_2020
R1(config-line)#exec-timeout 10 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#end
```

Figure III.16 Attribution des mots de passe

Remarque : La même configuration sera faite pour le switch.

III.4.1.3 Configuration des interfaces

Dans cette étape nous allons attribuer les adresses IP aux interfaces des routeurs et les activer par la suite. La **figure III.17** illustre cette configuration.

```
R1(config)#int giga 0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config)#int se 0/0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

Figure III.17 Adressage et activation des interfaces du routeur

III.4.1.4 Configuration de routage EIGRP/RIP

A présent, nous allons configurer le protocole de routage EIGRP et RIP version 2 au niveau des routeurs, on prend par exemple la configuration de routage EIGRP et RIPv2 sur le routeur R1 comme la montre la **figure III.18.**

```
R1(config)#router eigrp 101
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.0.0.0

R1(config)#router rip
R1(config-router)#version 2
```

Figure III.18 Routage EIGRP/RIPv2

III.4.1.5 Attribution d'adresse IP pour PCs & Serveurs

Pour attribuer les adresses IP aux PCs ainsi que les serveurs et les laptops, on clique tout d'abord sur l'équipement ensuite sur le bouton **DEKSTOP** et on ouvre l'onglet **IP Configuration** (l'application de la configuration des adresses IP). La **figure III.19** illustre cette configuration.

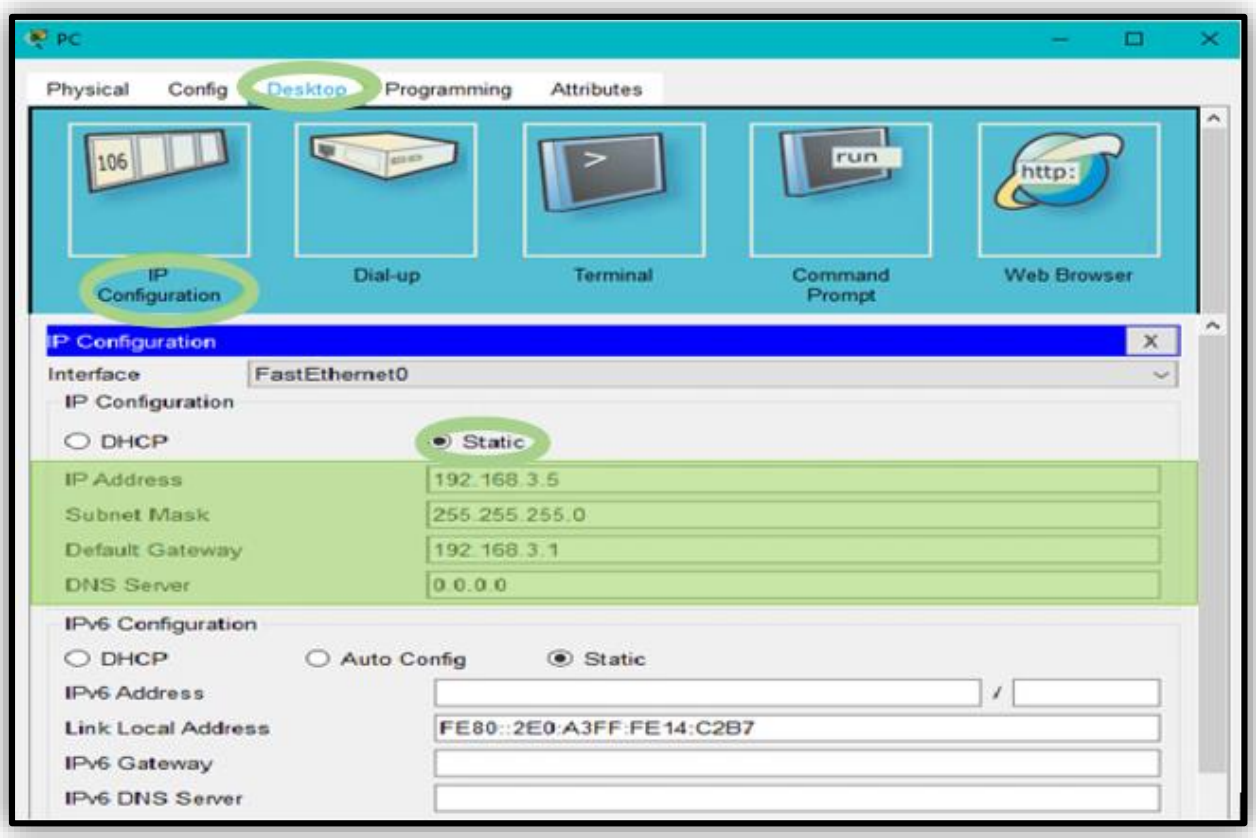


Figure III.19 Attribution d'une adresse iP statique au PC

III.4.2 Mise en place des protocoles Syslog, NTP & SSH

1. Contexte & Scénario

Dans cette réalisation, nous allons configurer l'authentification OSPF MD5 pour des mises à jour de routage sécurisées.

Le serveur NTP (Network Time Protocol) permet aux routeurs du réseau de synchroniser leurs paramètres d'heure avec un NTP serveur. Un groupe de clients NTP qui obtiennent des informations d'heure et de date à partir d'une seule source ont plus de cohérence les paramètres d'heure et les messages Syslog générés peuvent être analysés plus facilement. Cela peut aider lorsque le dépannage des problèmes liés aux problèmes de réseau et aux attaques.

Le serveur Syslog fournira la journalisation des messages. Nous allons configurer les routeurs pour identifier la télécommande hôte (serveur Syslog) qui recevra les messages de journalisation.

Le routeur R2 est un FAI (Fournisseur d'accès à internet) connecté à deux réseaux distants qui sont R1 et R3. L'administrateur local de R3 peut effectuer la plupart des configurations de routeur et dépannage, Cependant, puisque R3 est un routeur géré, le FAI doit avoir accès à R3 pour un dépannage ou des mises à jour occasionnels. Pour fournir cet accès de manière sécurisée, on va utiliser le protocole de sécurité Secure

Shell (SSH). Nous utilisons la CLI pour configurer le routeur pour qu'il soit géré en toute sécurité à l'aide de SSH au lieu de Telnet. SSH est un réseau protocole qui établit une connexion d'émulation de terminal sécurisée avec un routeur ou un autre périphérique réseau. SSH crypte toutes les informations qui transitent par la liaison réseau et assure l'authentification de l'ordinateur distant.

Les serveurs sont configurés pour les services NTP et Syslog respectivement. Les routeurs doivent êtres préconfigurés avec les éléments suivants :

- Activation du mot de passe pour accéder au mode privilégié : **master_2_telecommunications** ;
- Activation du mot de passe pour la console : **reseaux_telecommunications_2020** ;
- Activation du mot de passe pour les lignes VTY : **reseaux_telecommunications_2020_vty** ;
- Routage statique.

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de configurer :

- L'authentification OSPF MD5 ;
- Les routeurs en tant que clients NTP ;
- Les routeurs pour mettre à jour l'horloge matérielle à l'aide de NTP ;
- Les routeurs pour consigner les messages sur le serveur syslog ;
- Les routeurs pour horodater les messages du journal ;
- Les utilisateurs locaux ;
- Les lignes VTY pour accepter uniquement les connexions SSH ;
- La paire de clés RSA sur le serveur SSH et vérifier la connectivité SSH du client PC et du client routeur.

L'objectif de cette configuration simulé est de lutter contre les attaques de type déni de service, de bloquer les attaques par force brute et le vol du mot passe.

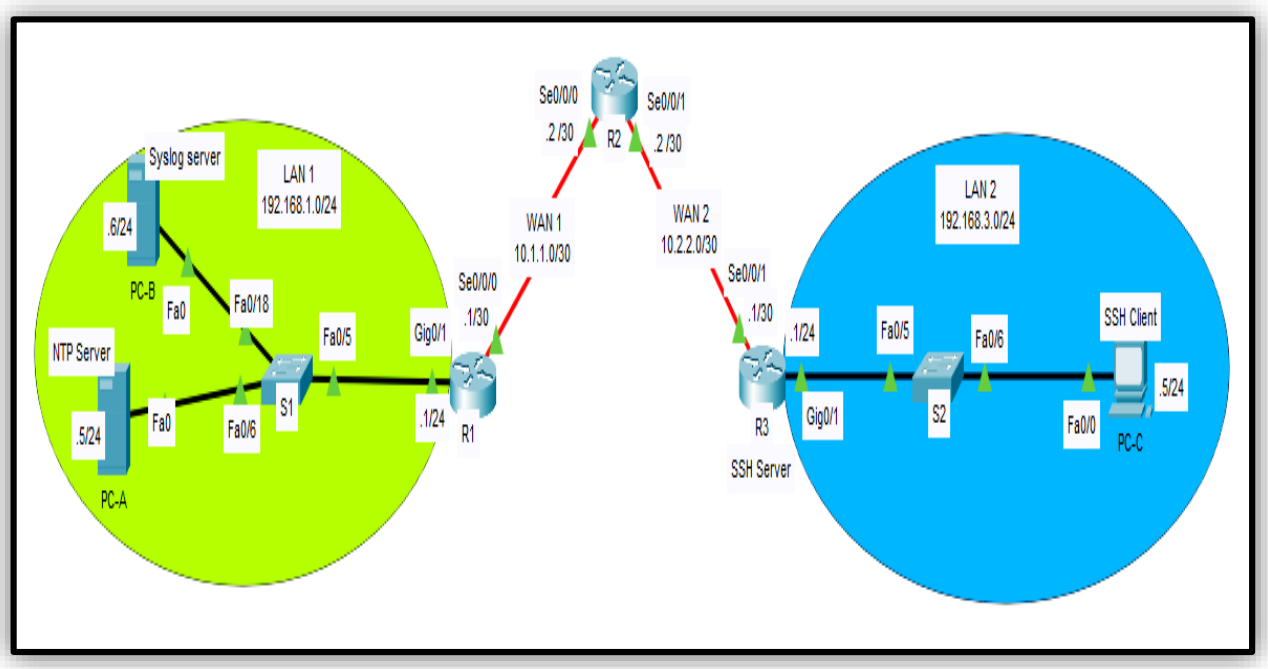


Figure III.20 Architecture du réseau serveur NTP, Syslog et SSH

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.3** suivant.

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	Se0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	Se0/0/0	10.1.1.2	255.255.255.252	N/A
	Se0/0/1(DCE)	10.2.2.2	255.255.255.252	N/A
R3	Gig0/1	192.168.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Tableau III.3 Table d'adressage pour le réseau serveur NTP, Syslog et SSH

4. Configuration des routeurs pour NTP, Syslog & SSH

❖ **Configuration d'authentification OSPF MD5** : La configuration se déroule comme suit :

a. **Configuration d'authentification OSPF MD5 pour tous les routeurs de la zone 0** : Nous allons configurer l'authentification OSPF (Open Shortest Path First) pour tous les routeurs de la zone 0, puis configurer la clé MD5 sur les interfaces série sur R1, R2 et R3, en utilisant le mot de passe « **MD5pa55 »** pour la clé **1**, comme le montre la figure ci-dessous.

```
R1(config-router)#router ospf 1
R1(config-router)#area 0 authentication message-digest
R1(config-router)#int se 0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
R2(config-router)#int se 0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#int se 0/0/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55

R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
R3(config-router)#int se 0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
```

Figure III.21 Configuration d'authentification OSPF MD5

Remarque : MD5 est le cryptage le plus puissant pris en charge dans la version de Packet tracer. Bien que MD5 présente des vulnérabilités connues, nous devons utiliser le chiffrement qui répond aux exigences de sécurité de notre organisation.

b. Vérification des configurations : À l'aide de la commande « **show ip ospf** », nous vérifions les configurations d'authentification MD5 comme le montre la figure suivante.

```
R1#sh ip ospf
 Routing Process "ospf 1" with ID 192.168.1.1
 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
```

Figure III.22 Vérification des configurations ospf

❖ **Configuration du NTP** : Les étapes suivantes expliquent cette configuration :

a. Activation d'authentification NTP : Sur PC-A, on clique sur le service **NTP**, nous activons le service en cliquant sur le bouton **On**. Ensuite, le bouton **Enable** pour activer l'authentification NTP. A la fin, nous tapons les paramètres : clé **1** et mot de passe « **NTPpa55 »** comme indiqué ci-dessous :

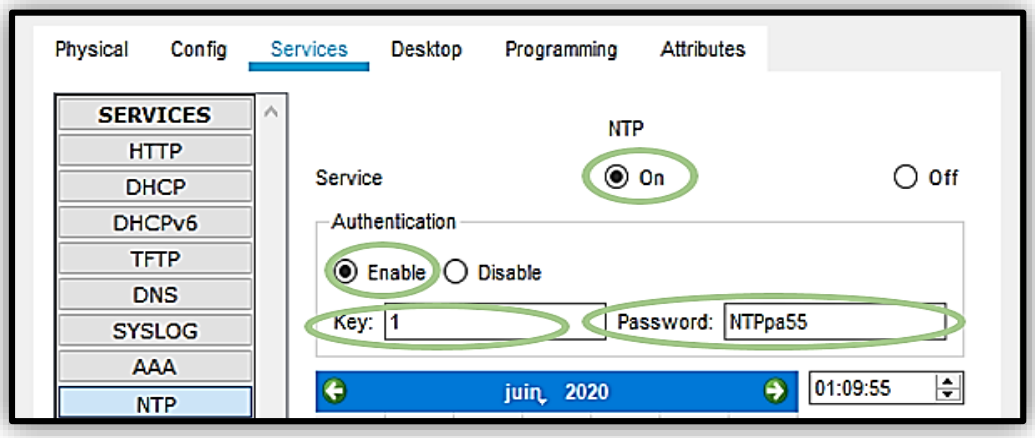


Figure III.23 Activation d'authentification NTP

b. Configuration des routeurs en tant que clients NTP, mise à jour d'horloge matérielle et d'authentification NTP : Dans cette partie, nous allons configurer tous les routeurs (R1, R2 et R3) en tant que des clients NTP à l'aide de la commande « **ntp server 192.168.1.5** », puis « **ntp update-calendar** » pour mettre à jour périodiquement l'horloge matérielle avec l'heure apprise de NTP et configuration de l'authentification NTP à l'aide des commandes : « **ntp trusted-key 1** » et « **ntp authencation-key 1 md5 NTPpa5** ».

c. Vérification des configurations : nous allons quitter la configuration globale et nous vérifions la configuration du client à l'aide de la commande « **show ntp status** » et « **show clock** » pour vérifier que l'horloge matérielle a été mise à jour.

Les deux figures ci-dessous montrent un exemple de la configuration sur le routeur R2 plus la vérification de cette dernière.

```
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpa55
```

Figure III.24 Configuration du NTP, l'horloge et l'authentification NTP

```
R2#sh ntp status
Clock is synchronized, stratum 16, reference is
192.168.1.5
nominal freq is 250.0000 Hz, actual freq is
249.9990 Hz, precision is 2**24
reference time is 0C6E348D.00000387 (23:41:1.903
UTC dim. sept. 15 2047)
clock offset is -4.00 msec, root delay is 10.00
msec
root dispersion is 151.54 msec, peer dispersion
is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled
Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 16 sec ago.
R2#sh clock
13:52:34.182 UTC Mon Jun 8 2020
```

Figure III.25 Vérification de l'horloge matérielle

Remarque : Nous faisons pareil sur le reste des routeurs.

❖ Configuration des routeurs pour consigner les messages sur le serveur Syslog

a. **Configuration des routeurs pour identifier l'hôte distant (serveur Syslog)** : Nous allons configurer tous les routeurs pour identifier l'hôte distant (serveur Syslog) qui recevra les messages de journalisation en tapant la commande « **logging host 192.168.1.6** » sur chaque routeur.

```
R3(config)#logging host 192.168.1.6
R3(config)#end
R3#
*juin 08, 14:17:23.1717: SYS-5-CONFIG_I:
Configured from console by console
*juin 08, 14:17:23.1717:  %SYS-6-
LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
```

Figure III.26 Configuration des routeurs pour la journalisation

Nous observons que la console du routeur affichera un message indiquant que la journalisation a commencé.

Remarque : Les messages de journal peuvent être générés sur le serveur en exécutant des commandes sur le routeur. Par exemple, l'entrée et la sortie du mode de configuration globale génèreront un message de configuration informatif.

b. **Examen des journaux du serveur Syslog** : Dans l'onglet services de la boîte de dialogue du serveur Syslog, nous sélectionnons le bouton services « Syslog » et nous observons les messages de journalisation reçus des routeurs.

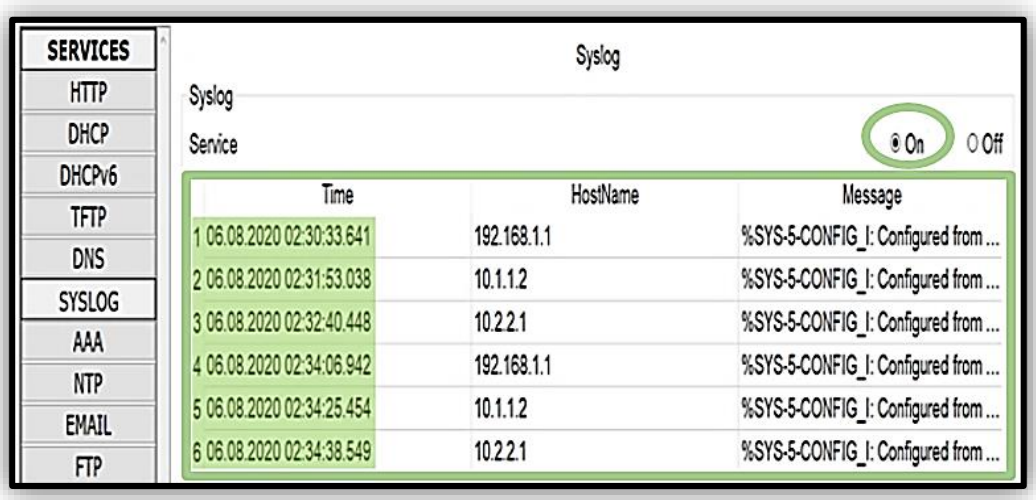


Figure III.27 Examen des journaux du serveur Syslog

❖ **Configuration du routeur R3 pour prendre en charge les connexions SSH** : Pour configurer le protocole SSH sur R3 qui est le serveur SSH nous suivons les étapes suivantes :

a. **Configuration du nom du domaine, des clients SSH & la connexion SSH sur les lignes VTY** : Sur le routeur R3 nous faisons rentrer les commandes suivantes pour :

- « **ip domain-name ccnasecurity.com** » : Pour configurer le nom du domaine ccnasecurity.com.
- « **username SSHadmin privilege 15 secret ciscosshpa55** » : Pour créer un ID utilisateur « **SSHadmin** » avec le niveau de privilège le plus élevé possible et un mot de passe secret de **ciscosshpa55**.
- « **line vty 0 15** », « **login local** » et « **transport input ssh** » : Pour configurer les lignes VTY entrantes sur R3.
- « **crypto key zeroize rsa** » : Pour écraser les paires de clés RSA existantes sur R3.
- « **crypto key generate rsa** » : Pour générer la paire de clés de chiffrement RSA pour R3.

Le routeur utilise la paire de clés RSA pour l'authentification et le cryptage des données SSH transmises. Nous configurons le RSA avec un module de 1024. La valeur par défaut est 512 et la plage est comprise entre 360 et 2048.

b. **Vérification de la configuration SSH** : Sur R3, nous allons taper la commande « **show ip ssh** » pour voir les paramètres actuels et vérifier que le délai d'authentification et les tentatives sont à leurs valeurs par défaut de 120 et 3.

Les deux figures ci-dessous montrent la configuration SSH sur le routeur R3 plus la vérification de cette dernière.

```
R3(config)#ip domain-name ccnasecurity.com
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
R3(config)#line vty 0 15
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Figure III.28 Configuration du SSH

```
R3#sh ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication
retries: 3
```

Figure III.29 Vérification de la configuration SSH

c. **Configuration des délais d'expiration SSH et les paramètres d'authentification** : Les délais d'expiration SSH et les paramètres d'authentification par défaut peuvent être modifiés pour être plus restrictifs. Nous définissons le délai d'expiration à **90** secondes, le nombre de tentatives d'authentification à **2** et la version à **2**. Ensuite, en exécutant à nouveau la commande « **show ip ssh** » pour confirmer que les valeurs ont été modifiées. La figure suivante illustre cette étape de configuration.

```
R3(config)#ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#end

R3#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication
retries: 2
```

Figure III.30 Configuration des délais d'expiration SSH et les paramètres d'authentification

❖ **Test de connexion SSH**

a. **La connexion à R3 via Telnet à partir du PC-C** : Nous allons ouvrir le bureau de PC-C, nous sélectionnons l'icône d'invite de commandes et nous tapons la commande « **telnet 192.168.3.1** » pour la connexion à R3 via Telnet.

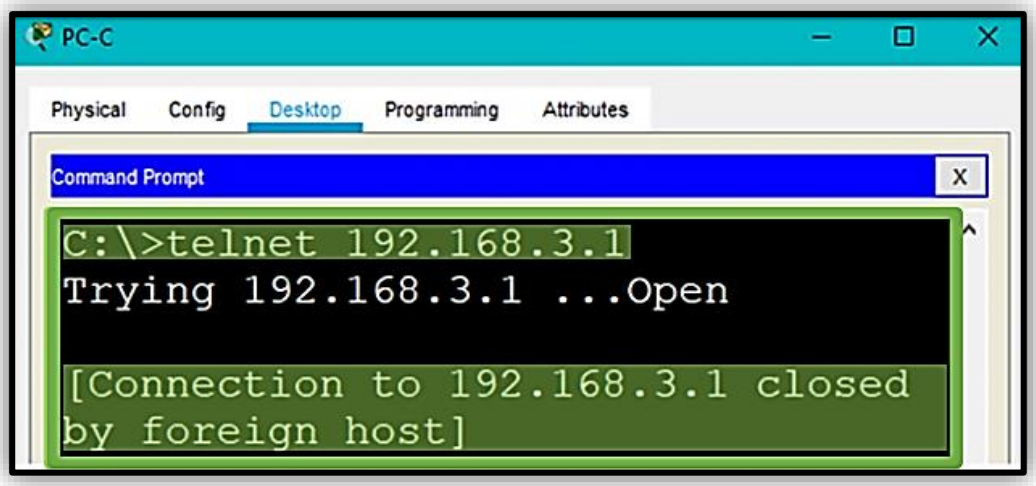


Figure III.31 La connexion à R3 via Telnet

Cette connexion est échouée, car R3 a été configuré pour accepter uniquement les connexions SSH sur le serveur virtuel et les lignes terminales.

b. **La connexion à R3 à l'aide de SSH à partir du PC-C** : A partir du bureau de PC-C, nous allons ouvrir la fenêtre d'invite de commandes et nous tapons la commande « **ssh –l SSHadmin 192.168.3.1 »** pour connecter à R3 via SSH. Lorsque nous sommes invités à entrer le mot de passe, nous devrons entrer le mot de passe configuré pour l'administrateur « **ciscosshpa55 »**.

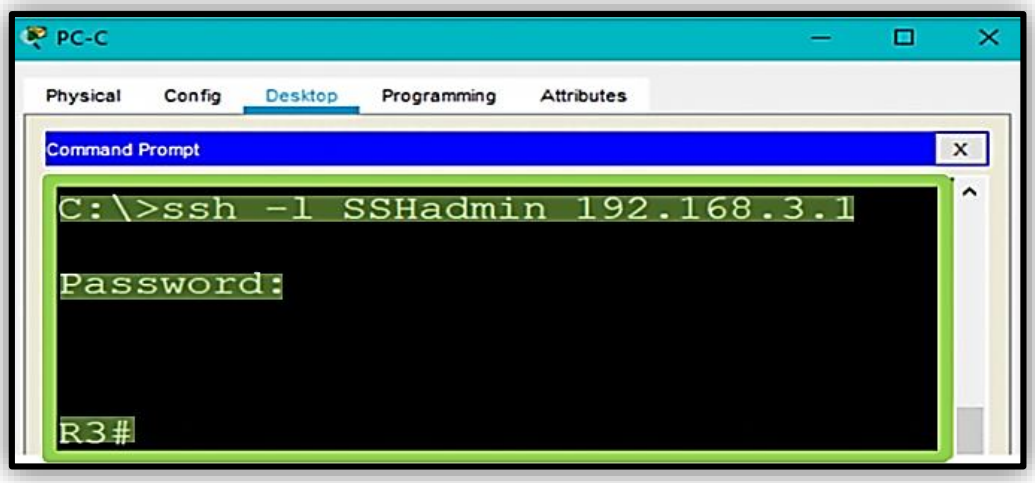


Figure III.32 La connexion à R3 à l'aide de SSH

c. Afin de dépanner et d'entretenir le routeur R3, l'administrateur du FAI doit utiliser SSH pour accéder au routeur CLI. Depuis la CLI du routeur R2, nous tapons la commande « **ssh –v 2 –l SSHadmin 10.2.2.1** » pour connecter à R3 via SSH version 2 à l'aide de « **SSHadmin »** compte d'utilisateur. Lorsque nous sommes invités à entrer le mot de passe, nous devrons entrer le mot de passe configuré pour l'administrateur « **ciscosshpa55 ».**

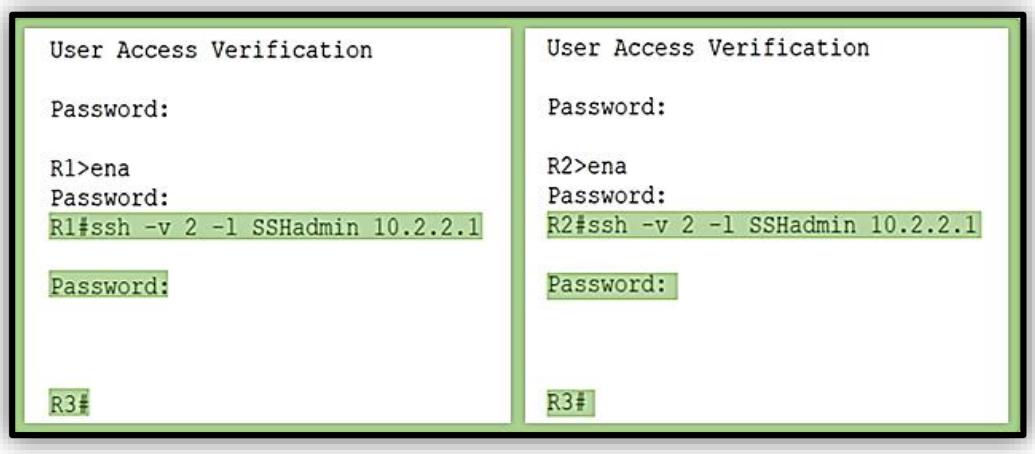


Figure III.33 La connexion à R3 à l'aide du SSH via un routeur

III.4.3 Mise en place du protocole d'authentification AAA

1. Contexte & Scénario

Nous allons réaliser au cours de cette partie un réseau de trois routeurs avec la configuration et le test des solutions AAA locales.

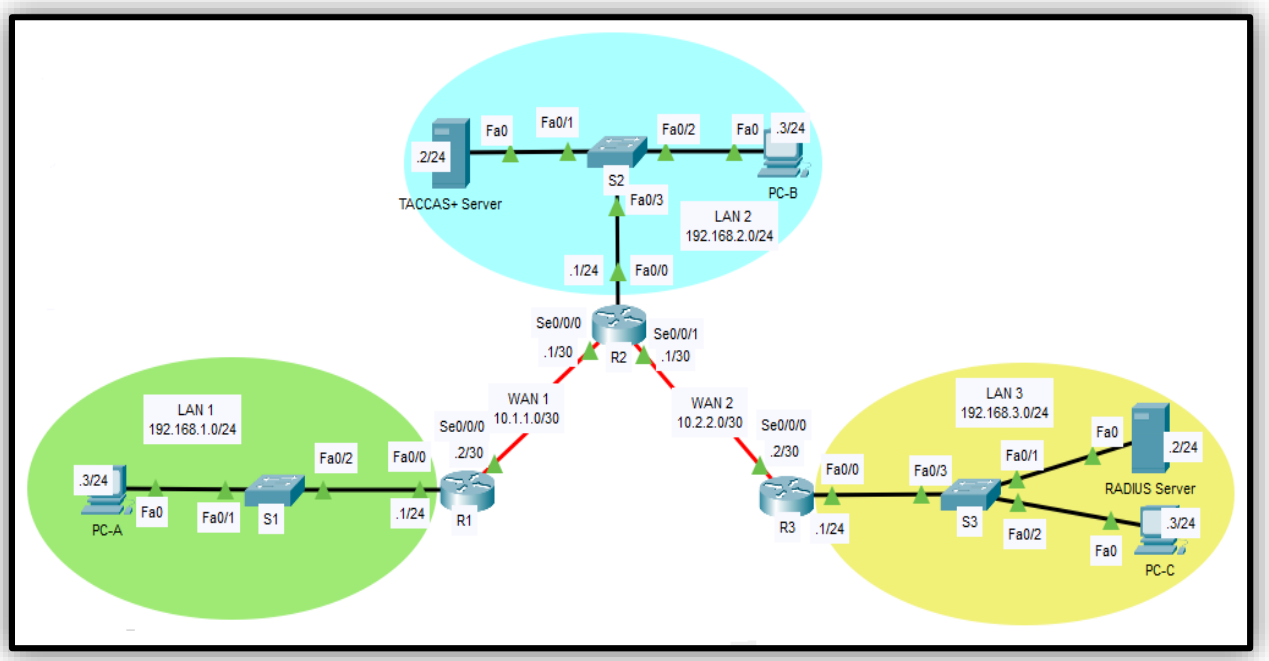


Figure III.34 Architecture du réseau d'authentification AAA

La topologie du réseau affiche les routeurs R1, R2 et R3. Actuellement, toute la sécurité administrative est basée sur les connaissances du mot de passe secret d'activation. Notre tâche consiste à configurer et tester des solutions AAA locales et basées sur le serveur.

Nous allons créer un compte d'utilisateur local et configurer AAA local sur le routeur R1 pour tester la console et les connexions VTY (Compte utilisateur « **Admin1 »** et mot de passe « **admin1pa55 »**).

Ensuite, nous allons configurer le routeur R2 pour prendre en charge l'authentification basée sur le serveur à l'aide du protocole TACACS+. Le serveur TACACS+ est préconfiguré avec les éléments suivants :

- Client : **R2** en utilisant le mot-clé « **tacacspa55 »**
- Compte utilisateur « **Admin2 »** et mot de passe « **admin2pa55 »**

Enfin, nous allons configurer le routeur R3 pour prendre en charge l'authentification basée sur le serveur à l'aide du protocole RADIUS. Le serveur RADIUS a été préconfiguré avec les éléments suivants :

- Client : **R3** utilisant le mot-clé « **radiuspa55 »**
- Compte utilisateur « **Admin3 »** et mot de passe « **admin3pa55 »**

Les routeurs doivent être également configurés avec les éléments suivants :

- Activation du mot de passe pour accéder au mode privilégié : **master_2_telecommunications** ;
- Activation du mot de passe pour la console : **reseaux_telecommunications_2020** ;
- Routage statique et RIP version 2.

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Configurer d'un compte d'utilisateur local sur R1 et s'authentifier sur la console et les lignes VTY en utilisant AAA local ;
- Vérifier l'authentification AAA locale à partir de la console R1 et du client PC-A ;
- Configurer l'authentification AAA à l'aide du serveur TACACS+ ;
- Vérifie l'authentification AAA basée sur le serveur à partir du client PC-B ;
- Configurer l'authentification AAA à l'aide du serveur RADIUS ;
- Vérifier l'authentification AAA basée sur le serveur à partir du client PC-C.

L'objectif de cette configuration simulé est de lutter contre les attaques de type déni de service, vol du mot passe et les attaques par rejeu.

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.4** suivant.

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	Se0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	Se0/0/0	10.1.1.2	255.255.255.252	N/A
	Se0/0/1(DCE)	10.2.2.2	255.255.255.252	N/A
R3	Gig0/1	192.168.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
TACACS + Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Tableau III.4 Table d'adressage pour le réseau d'authentification AAA

4. Configuration l'authentification AAA sur les routeurs Cisco

❖ **Configuration de l'authentification AAA locale pour l'accès à la console sur R1** : La configuration se déroule comme suit :

a. **Configuration du nom d'utilisateur local sur R1** : Nous allons configurer un nom d'utilisateur **« Admin1 »** et un mot de passe secret **« admin1pa55 »** à l'aide de la commande « **username Admin1 password admin1pa55 »**

b. **Configuration de l'authentification AAA locale et la console** : Nous activons AAA sur R1 et nous configurons l'authentification AAA pour la connexion à la console pour utiliser la base de données locale en tapant ces deux commandes « **aaa new-model** » et « **aaa authentication login default local** ». Ensuite, nous passons à la configuration de cette dernière pour la connexion à la console méthodes par défaut à l'aide de la commande « **line console 0** » et « **login authentication default** ». Finalement, nous allons vérifier la connexion d'utilisateur à l'aide de la base de données locale en quittant la configuration globale.

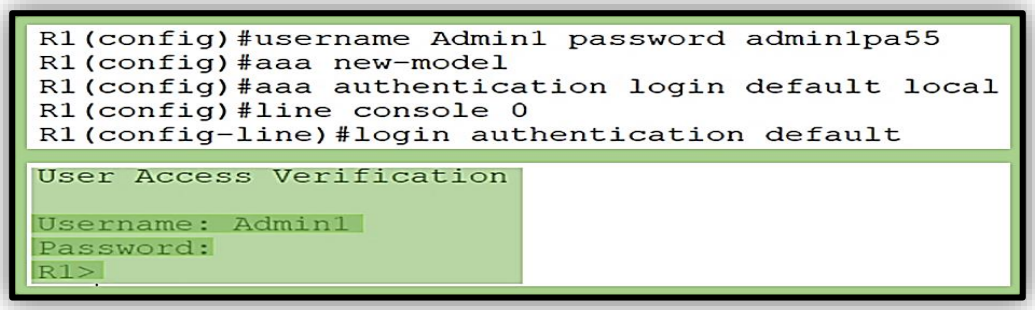


Figure III.35 Configuration d'authentification AAA locale pour les accès consoles

❖ **Configuration d'authentification AAA locale pour les lignes VTY**

a. **Configuration la méthode d'authentification nommée AAA pour les lignes VTY sur R1** : Nous allons Configurer une liste nommée appelée **TELNET-LOGIN** pour authentifier les connexions à l'aide d'AAA local.

b. **Configuration des lignes VTY pour utiliser la méthode d'authentification AAA** : Nous allons configurer les lignes VTY pour utiliser la méthode AAA nommée. Ensuite, nous allons vérifier la configuration Telnet. Depuis l'invite de commande de PC-B, Telnet vers R2. (Voir La **figure III.36)**

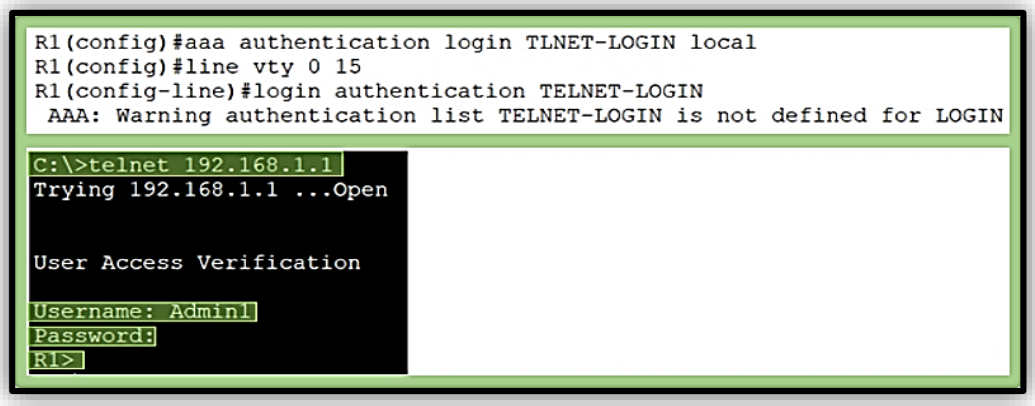


Figure III.36 Configuration d'authentification AAA locale pour les accès consoles

❖ **Configuration d'authentification AAA à l'aide du serveur TACACS+ sur le routeur R2**

a. **Configuration d'une entrée de base de données locale de sauvegarde** : Au cours de cette étape, nous allons configurer une entrée de base de données locale de sauvegarde appelée « **Admin2 »**, en utilisant les éléments suivants :

- Nom d'utilisateur local : **Admin2**
- Mot de passe secret : **admin2pa55**

b. **Vérification de la configuration du serveur TACACS+** : Nous sélectionnons le serveur TACACS+. Dans l'onglet Config, nous cliquons sur **AAA** et nous notons qu'il existe un réseau entré de configuration pour R2 et une entrée de configuration utilisateur pour **« Admin2 »**. Comme il est indiqué dans la figure ci-dessous.

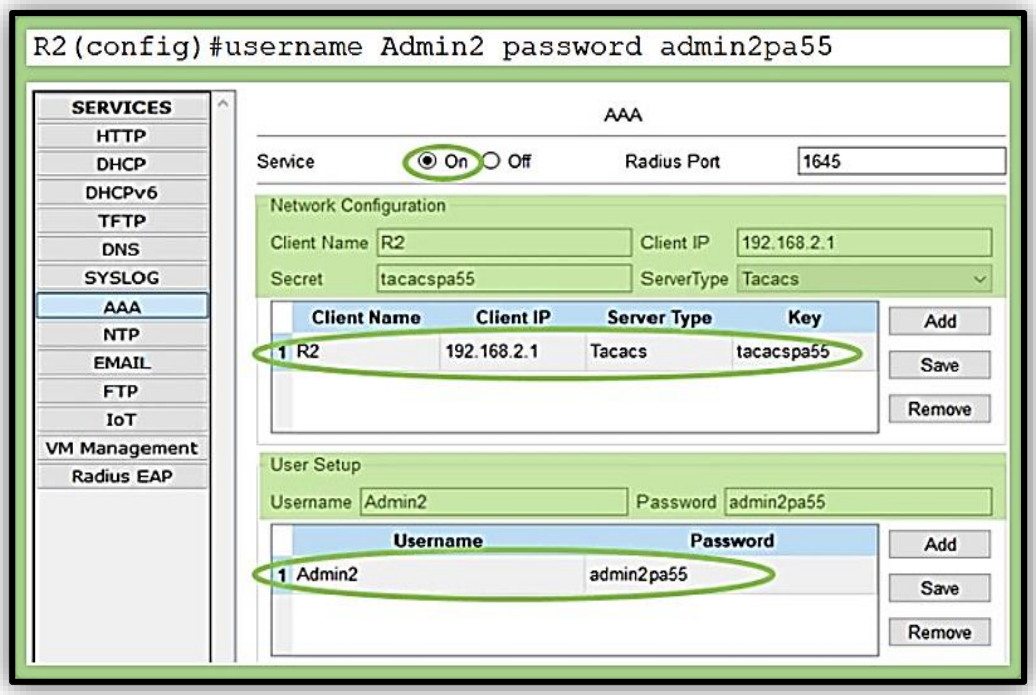


Figure III.37 Configuration d'une entrée de base de données locale de sauvegarde

c. **Configuration des spécificités du serveur TACACS+ sur R2 et de l'authentification de connexion AAA pour les accès consoles** : Sur le routeur R2, nous allons rentrer les commandes suivantes :

- **« tacacs-server host 192.168.2.2 »** et **« tacacs-server key tacacspa55 »** : Pour configurer l'adresse IP et la clé secrète du serveur AAA TACACS.
- « **aaa new-model »** et « **aaa authentication login default group tacacs+ local »** : Pour activer AAA et configurer l'authentification de connexion pour les accès consoles.
- **« line console 0 »** et **« login authentication default »** : Pour configurer la console en ligne à l'aide de la méthode d'authentification AAA par défaut.

d. **Vérification de la méthode d'authentification AAA** : Après avoir taper tous les commandes précédentes, nous sortons de la configuration globale pour vérifier la connexion de l'utilisateur à l'aide du AAA TACACS+ serveur.

La **figure III.38** nous résume les deux étapes précédentes.

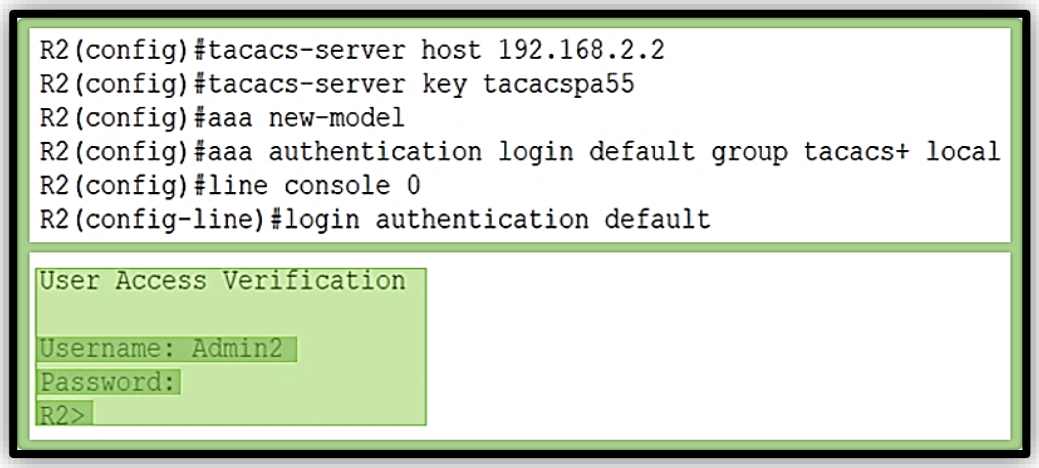


Figure III.38 Configuration serveur TACACS+ et de l'authentification de connexion AAA

❖ **Configuration d'authentification AAA à l'aide du serveur RADIUS sur le routeur R3**

a. **Configuration d'une entrée de base de données locale de sauvegarde** : Nous allons maintenant configurer une entrée de base de données locale de sauvegarde appelée « **Admin3 »**, en utilisant les éléments suivants :

- Nom d'utilisateur local : **Admin3**
- Mot de passe secret : **admin3pa55**

b. **Vérification de la configuration du serveur RADIUS** : Cette fois, nous sélectionnons le serveur RADIUS+. Dans l'onglet Config, nous cliquons sur **AAA** et nous notons qu'il existe un réseau entré de configuration pour R3 et une entrée de configuration utilisateur pour **« Admin3 »**.

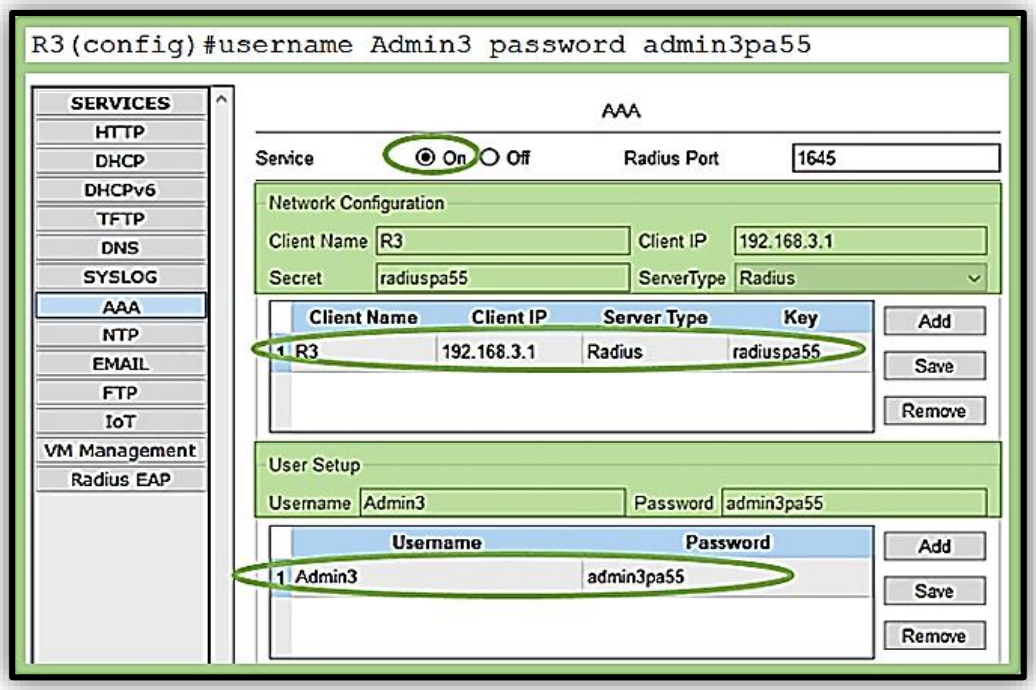


Figure III.39 Configuration d'une entrée de base de données locale de sauvegarde

c. **Configuration des spécificités du serveur RADIUS+ sur R2 et de l'authentification de connexion AAA pour les accès consoles** : Sur le routeur R3, nous configurons :

- L'adresse IP et la clé secrète du serveur AAA RADIUS ;
- Les connexions pour s'authentifier à l'aide du serveur AAA RADIUS ;
- La console en ligne à l'aide de la méthode d'authentification AAA définie ;
- L'authentification AAA pour la connexion à la console pour utiliser la méthode d'authentification AAA par défaut.

La **figure III.40** ci-dessous montre les commandes utilisées pour cette partie et la vérification de la méthode d'authentification AAA.

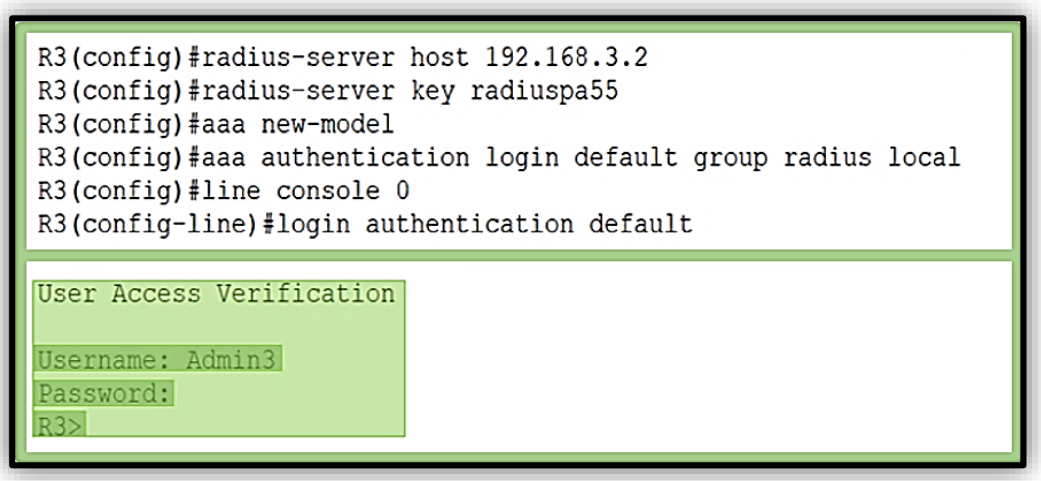


Figure III.40 Configuration du serveur RADIUS et de l'authentification de connexion AAA

III.4.4 Mise en place du contrôle d'accès basé sur le contexte (CBAC)

1. Contexte & Scénario

Le contrôle d'accès basé sur le contexte (CBAC) est utilisé pour créer un pare-feu IOS. Au cours de cette partie, nous allons créer une configuration CBAC de base sur le routeur de périphérie R3. Ce dernier fournit un accès aux ressources en dehors du réseau pour les hôtes sur le réseau intérieur. R3 empêche les hôtes externes d'accéder aux ressources internes. Une fois qu'on termine la configuration, nous allons vérifier la fonctionnalité du pare-feu des hôtes internes et externes. Les routeurs sont préconfigurés avec les éléments suivants :

- Activation du mot de passe : **master_2_telecommunications** ;
- Activation du mot de passe pour la console : **reseaux_telecommunications_2020** ;
- Mot de passe pour les lignes VTY : **reseaux_telecommunications_2020_vty** ;
- Adressage IP ;
- Routage statique ;
- Tous les ports de commutateur sont dans le VLAN 1 pour les commutateurs S1 et S3.

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Vérifier la connectivité entre les appareils avant la configuration du pare-feu.

- Configurer un pare-feu IOS avec CBAC sur le routeur R3
- Vérifier la fonctionnalité CBAC à l'aide de Ping, Telnet et HTTP.

L'objectif de cette configuration simulé est de bloquer les attaques DOS, SYN flood, PING flood, porte dérobée et man in the middle.

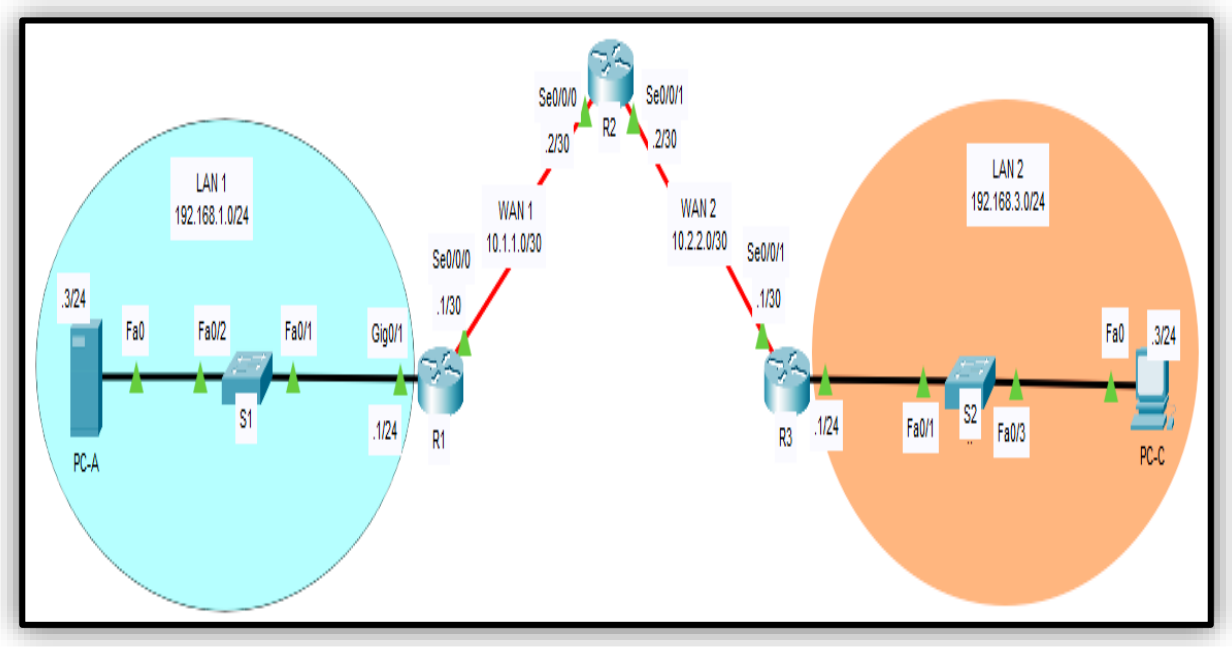


Figure III.41 Architecture du réseau du contrôle d'accès basé sur le contexte (CBAC)

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.5** suivant :

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Se0/0/0	10.1.1.2	255.255.255.252	N/A
	Se0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Gig0/1	192.168.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Tableau III.5 Table d'adressage pour le réseau du contrôle d'accès basé sur le contexte (CBAC)

4. Configuration du CBAC sur les routeurs CISCO

❖ **Blocage du trafic de l'extérieur** : la configuration se déroule comme le suivant :

a. Vérification de la connectivité réseau de base : Avant de configurer le pare-feu IOS, nous allons vérifier la connectivité réseau en appliquant les tests suivants :

- À l'invite de commande PC-C, nous allons envoyer une requête Ping au serveur PC-A. (Ping réussi)
- Depuis l'invite de commande PC-C, nous nous connectons via Telnet à l'interface S0/0/1 du routeur R2 (L'adresse IP 10.2.2.2/30).
- Depuis PC-C, nous ouvrons un navigateur Web sur le serveur PC-A pour afficher la page Web.
- À l'invite de commande du serveur PC-A, nous envoyons une requête Ping à PC-C. (Ping réussi)

b. Configuration d'une ACL IP nommée : Sur le routeur R3, nous tapons la commande **« ip access-list extended »** pour créer une ACL IP nommée et pour bloquer tout le trafic que soit de l'extérieur vers l'intérieur ou bien le contraire. Nous appliquons l'ACL à l'interface S0/0/1. (Voir la **figure III.42**)

```
R3(config)#ip access-list extended OUT-IN
R3(config-ext-nacl)#deny ip any any
R3(config-ext-nacl)#exit
R3(config)#int se 0/0/1
R3(config-if)#ip access-group OUT-IN in
R3(config-if)#exit
```

Figure III.42 Configuration d'une ACL IP nommée

c. Confirmation de la suppression du trafic entrant dans l'interface Serial 0/0/1 : Depuis l'invite de commande PC-C, nous allons envoyer une requête Ping au serveur PC-A pour confirmer que le trafic entrant dans l'interface S0/0/1 est supprimé. La figure ci-dessous montre que les réponses d'écho ICMP sont bloquées par l'ACL.

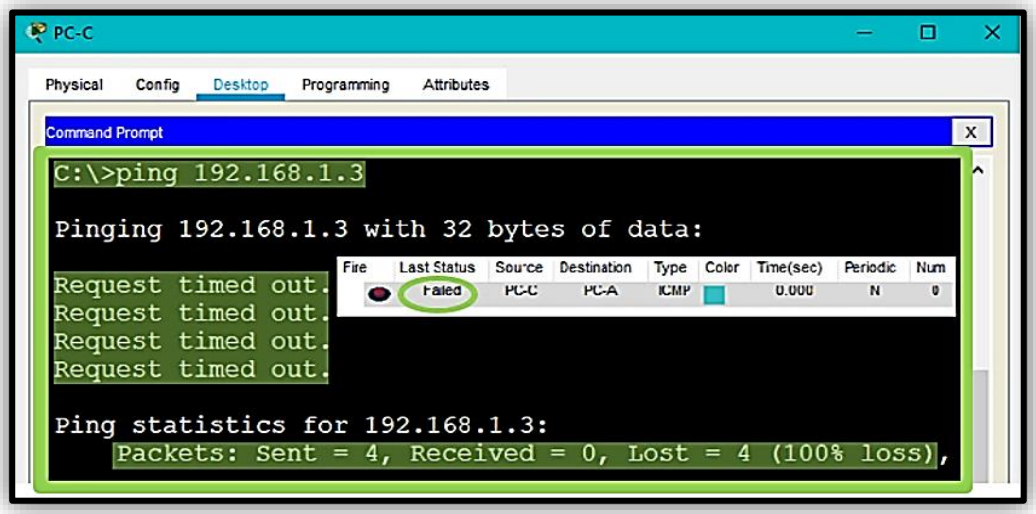


Figure III.43 Configuration d'une ACL IP nommée

❖ Création d'une règle d'inspection du CBAC

a. Sur le routeur R3, nous allons tout d'abord créer une règle d'inspection pour inspecter le trafic ICMP, Telnet et http. À l'aide des commandes **« ip inspect name IN-OUT-IN icmp », « ip inspect name IN-OUT-IN telnet »** et **« ip inspect name IN-OUT-IN http ».** (Voir la **figure III.44**)

b. **Activation de la journalisation passée dans le temps et les messages de piste d'audit CBAC** : Nous utilisons la commande **« ip inspect audit-trail »** pour activer les messages d'audit CBAC afin de fournir un enregistrement du réseau l'accès via le pare-feu, y compris les tentatives d'accès illégitimes. Ensuite, nous activons la journalisation sur le serveur syslog, (192.168.1.3/24), avec la commande **« logging host »,** puis nous vérifions que les messages enregistrés sont horodatés. Enfin, nous appliquons la règle d'inspection au trafic de sortie sur l'interface S0/0/1. (Voir la **figure III.44**)

```
R3(config)#ip inspect name IN-OUT-IN icmp
R3(config)#ip inspect name IN-OUT-IN telnet
R3(config)#ip inspect name IN-OUT-IN http

R3(config)#ip inspect audit-trail
R3(config)#service timestamps debug datetime msec
R3(config)#logging host 192.168.1.3

R3(config)#int se 0/0/1
R3(config-if)#ip inspect IN-OUT-IN out
```

Figure III.44 Création d'une règle d'inspection du CBAC

c. **Vérification des messages de piste d'audit sont enregistrés sur le serveur Syslog** : Premièrement, à partir du PC-C, nous allons tester la connectivité au PC-A avec Ping, Telnet et HTTP. Nous notons la réussite du Ping et HTTP plus le PC-A rejettera la session Telnet. (Voir la **Figure III.45**)

Deuxièmement, depuis PC-A nous envoyons une requête Ping et Telnet pour tester la connectivité au PC-C, cette opération va être bloquée. Ensuite, passant en revue des messages syslog sur le serveur PC-A en cliquant sur l'onglet **Config**, puis sur l'option **SYSLOG.** (Voir la **Figure III.46**)

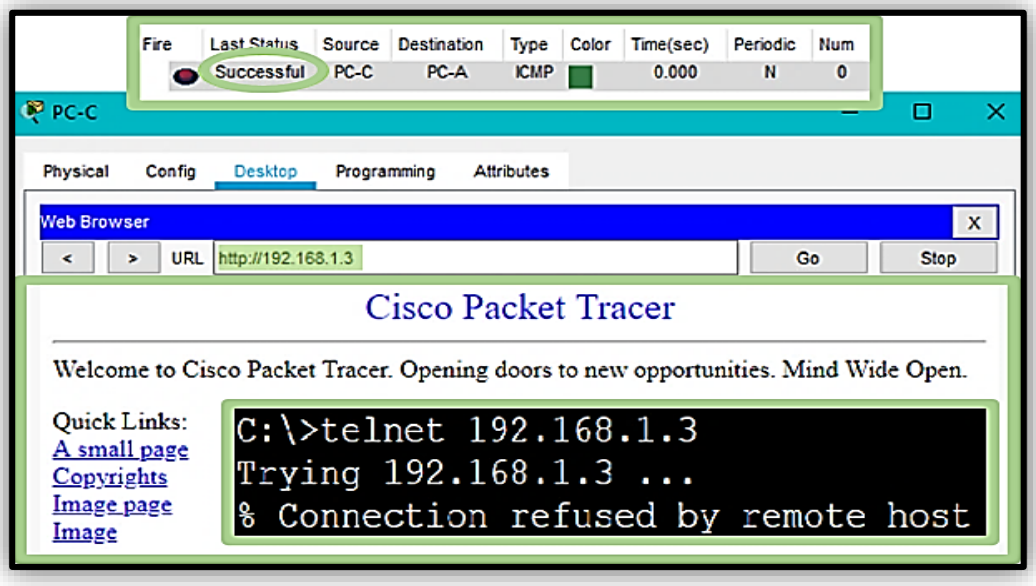


Figure III.45 Test avec une requête Ping, Http et Telnet

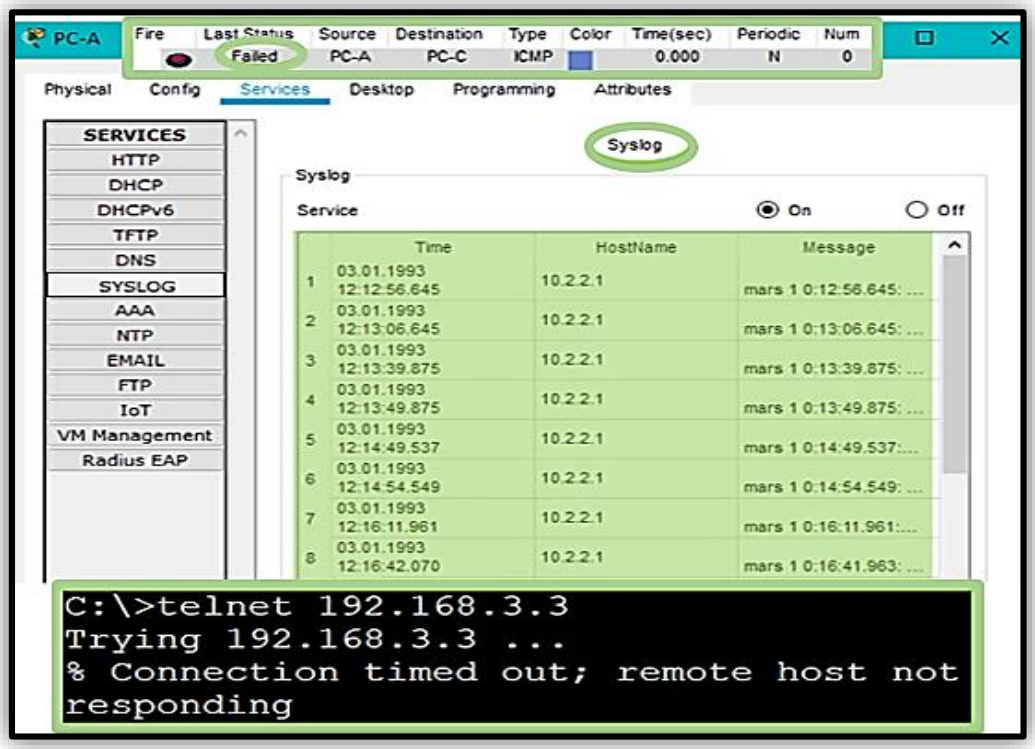


Figure III.46 Test du Ping, Telnet et l'affichage des messages Syslog

❖ **Vérification de la fonctionnalité du pare-feu**

a. **Ouverture d'une session Telnet de PC-C à R2** : Pendant que la session Telnet est active, nous allons émettre la commande **« show ip inspect sessions »** sur le routeur R3. Cette commande affiche les sessions existantes qui sont actuellement suivies et inspectées par le CBAC. (Telnet réussi)

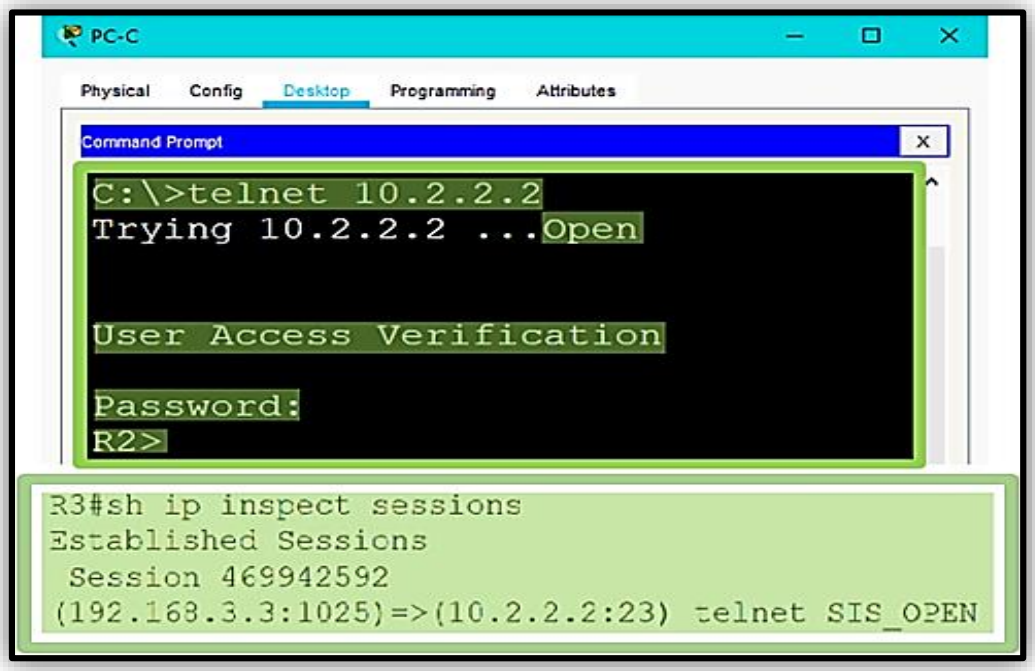


Figure III.47 Ouverture d'une session Telnet de PC-C à un routeur

b. Depuis PC-C, nous ouvrons un navigateur Web sur la page Web du serveur PC-A en utilisant l'adresse IP du serveur. Pendant que la session HTTP est active, nous émettons la commande **« show ip inspect sessions »** sur le routeur R3. (Voir la **figure III.48**)

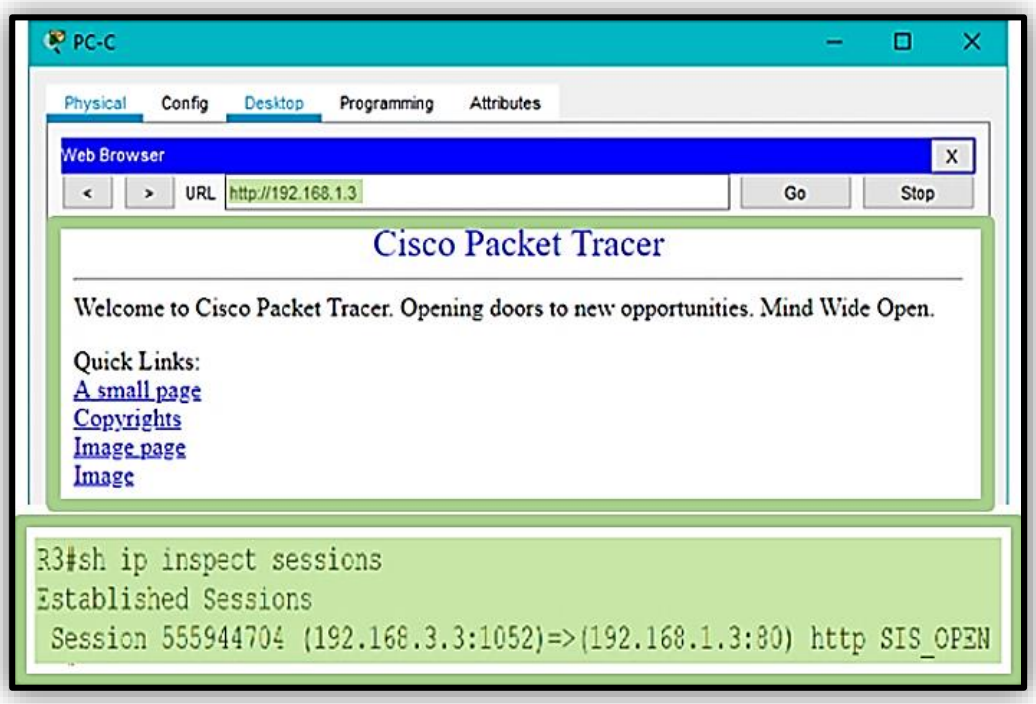


Figure III. 48 Ouverture d'une page web du serveur avec l'affichage de la session sur le routeur

c. **Affichage de la configuration de l'interface et les temporisateurs des règles d'inspection** : Sur le routeur R3, nous tapons la commande **« show ip inspect interfaces »** pour afficher la configuration de l'interface et les temporisateurs des règles d'inspection. La figure ci-dessous montre les sessions existantes qui sont actuellement suivies et inspectées par le CBAC.

```
R3#sh ip inspect interfaces
Interface Configuration
 Interface Serial0/0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is IN-OUT-IN
    icmp alert is on audit-trail is on timeout 10
    telnet alert is on audit-trail is on timeout 3600
    http alert is on audit-trail is on timeout 3600
  Inbound access list is OUT-IN
  Outgoing access list is not set
```

Figure III.49 Affichage de la configuration de l'interface et les règles d'inspection

❖ **Révision de la configuration du CBAC**

a. **Affichage de la configuration CBAC** : Sur le routeur R3, nous tapons la commande **« show ip inspect config »** pour afficher la configuration complète d'inspection CBAC. (Voir la **figure III.50**)

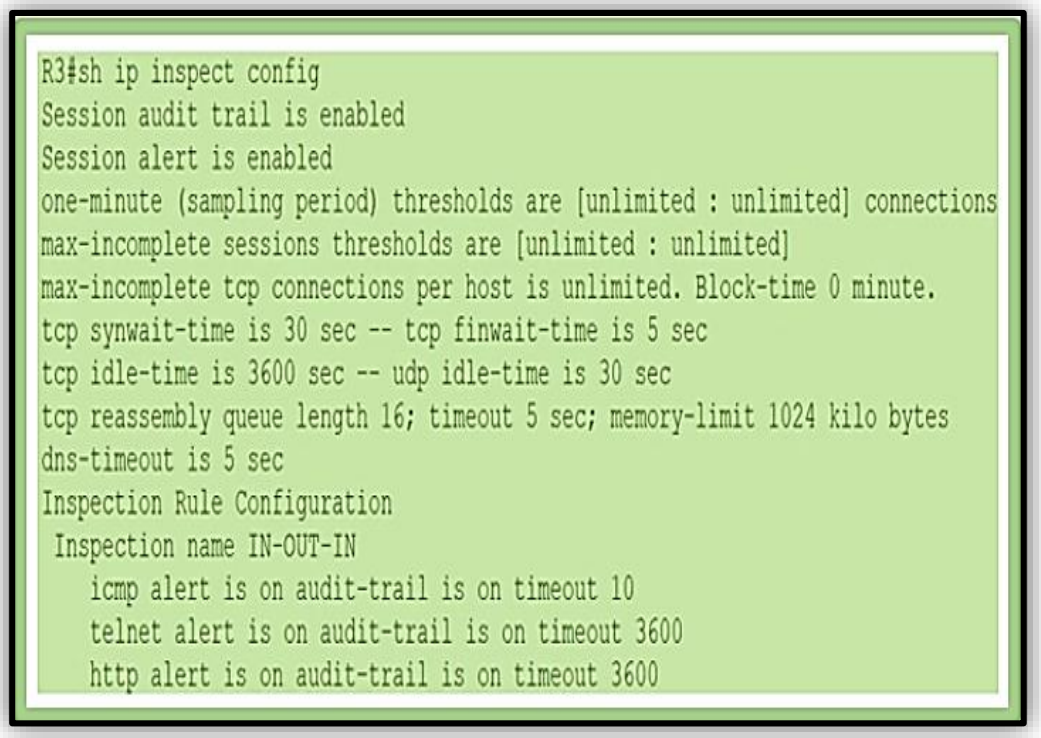


Figure III.50 Affichage de la configuration CBAC

b. **Affichage d'une sortie en temps réel qui peut être utilisée pour le dépannage** : Sur le routeur R3, nous allons taper la commande **« debug ip inspect detailed »** pour afficher des messages détaillés sur les événements du logiciel CBAC, y compris des informations sur le traitement des paquets CBAC.

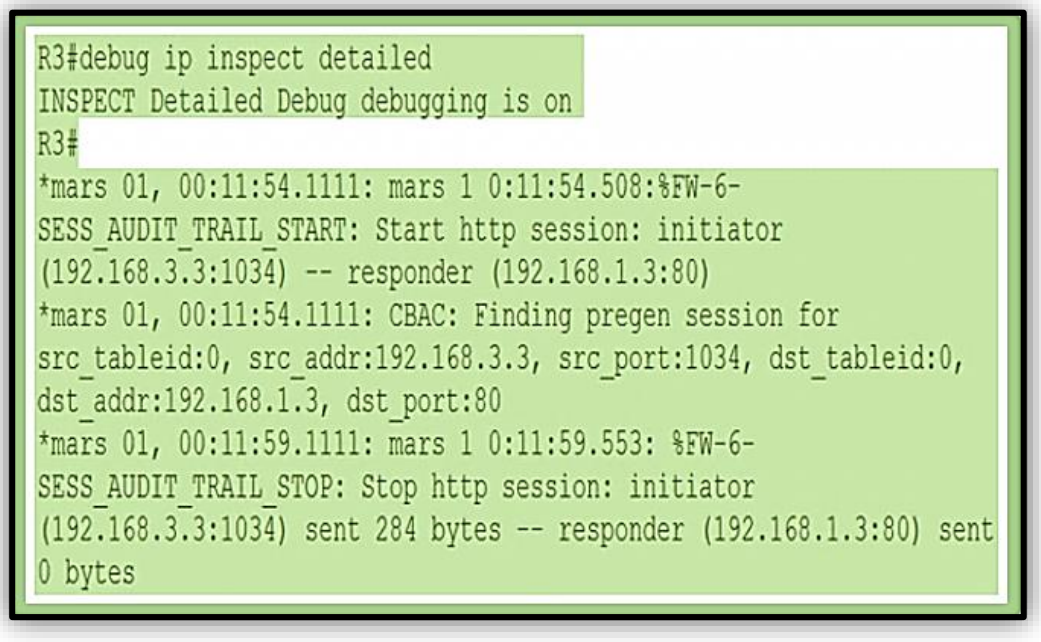


Figure III.51 Affichage d'une sortie en temps réel qui peut être utilisée pour le dépannage

III.4.5 Mise en place du pare-feu (Fire Wall) & du IPS

III.4.5.1 Mise en place d'un pare-feu de stratégie basé sur une zone (ZPF)

1. Contexte & Scénario

Le pare-feu de politique basée sur la zone (ZPF) est le dernier développement dans l'évolution des technologies de pare-feu Cisco. Dans cette configuration simulée, nous allons configurer un ZPF de base sur un routeur de périphérie R3 qui permet aux hôtes internes d'accéder aux ressources externes et empêche les hôtes externes d'accéder aux ressources internes. Nous allons ensuite vérifier la fonctionnalité du pare-feu des hôtes internes et externes. Les routeurs sont préconfigurés avec les mêmes éléments de la configuration du contrôle d'accès basé sur le contexte (CBAC). (Voir la **page 90**)

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Vérifier la connectivité entre les appareils avant la configuration du pare-feu ;
- Configurer un pare-feu de stratégie basée sur une zone (ZPF) sur le routeur R3 ;
- Vérifier la fonctionnalité du pare-feu ZPF en utilisant Ping, Telnet et un navigateur Web.

L'objectif de cette configuration simulé est de se protéger contre l'attaque smurf qui fait partie de la grande famille des attaques DOS, ARP Spoofing, DHCP Snooping.

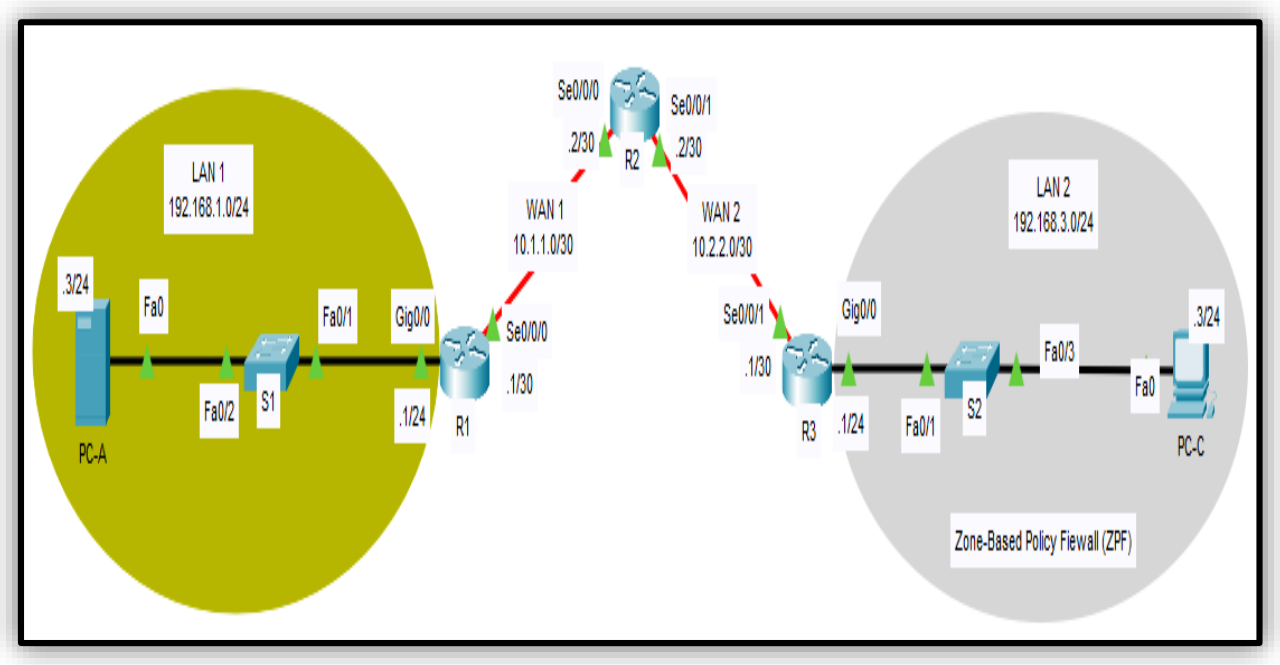


Figure III.52 Architecture d'un réseau pare-feu de stratégie basé sur une zone (ZPF)

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.6** suivant.

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/0	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.1	255.255.255.252	N/A

R2	Se0/0/0	10.1.1.2	255.255.255.252	N/A
	Se0/0/1	10.2.2.2	255.255.255.252	N/A
R3	Gig0/0	192.168.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Tableau III.6 Table d'adressage pour le réseau pare-feu de stratégie basé sur une zone (ZPF)

4. Configuration d'un pare-feu de stratégie basé sur une zone (ZPF)

❖ **Vérification de la connectivité réseau de base** : Avant de configurer le pare-feu de stratégie basé sur la zone, nous allons vérifier la connectivité réseau en appliquant les tests suivants :

- À partir de l'invite de commande PC-A, nous envoyons une requête Ping à PC-C (Ping réussi).
- À partir de l'invite de commande PC-C, Telnet à l'interface S0/0/1 du routeur R2 à (10.2.2.2/30) (Telnet réussi).
- Depuis PC-C, nous ouvrons un navigateur Web sur le serveur PC-A pour afficher la page d'accueil de Packet Tracer du serveur Web.

❖ **Création des zones de pare-feu sur le routeur R3** : Dans cette première tâche, nous allons tout d'abord créer une paire de zones (Zone interne et zone externe) en utilisant les commandes : **« zone security IN-ZONE »** et **« zone security OUT-ZONE ».** (Voir la **figure III.53**)

❖ **Définition d'une classe de trafic et une liste d'accès**

a. **Création d'une ACL qui définit le trafic interne** : Nous allons créer une ACL 101 étendue pour autoriser tous les protocoles IP du réseau source (192.168.3.0/24) vers n'importe quelle destination à l'aide de la commande **« access-list »**. (Voir la **figure III.53**)

b. **Création d'une carte class référençant l'ACL de trafic interne** : Maintenant, nous allons créer un mappage de classe nommé « **IN-NETCLASS-CARTE »** en utilisant la commande **« class map type inspect »** avec l'option match-all et la commande **« match access-group »** pour faire correspondre l'ACL 101. (Voir la **figure III.53**)

```
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#zone security OUT-ZONE
R3(config-sec-zone)#exit

R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
```

Figure III.53 Création des zones de pare-feu avec la classe de trafic et la liste d'accès

- **Spécification des stratégies du pare-feu** : Nous allons créer à l'aide de la commande **« policy-map type inspect »** une carte de stratégie nommée « **IN-2-OUT-PMAP »** pour déterminer quoi faire avec le trafic correspondant et spécifier un type de classe d'inspection, une référence classe de mappage « **IN-NET-CLASS-MAP »** et une action d'inspection pour cette carte en utilisant la commande **« inspect »** pour invoquer le contrôle d'accès basé sur le contexte. (Voir la **figure III.54**)

```
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
```

Figure III.54 Spécification des stratégies du pare-feu

- **Application des stratégies du pare-feu** : Pour appliquer les stratégies du pare-feu, nous allons commencer par la création d'une paire de zones à l'aide de la commande « **zone-pair security »** nommée « **IN-2-OUT-ZPAIR »**. Ensuite, nous spécifions la carte de stratégie pour gérer le trafic entre les deux zones en attachant un « **policy-map »** et ses actions associées à la paire de zones à l'aide de la commande **« service-policy type inspect »** et référencer le policy map précédemment créé **« IN-2-OUT-PMAP »**. (Voir la **figure III.55**)

  Enfin, nous attribuons des interfaces aux zones de sécurité appropriées en utilisant la commande **« zone-member security »** en mode de configuration d'interface pour affecter G0/0 à **IN-ZONE** et S0/0/1 à **OUT-ZONE**. (Voir la **figure III.55**)

```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit

R3(config)#int giga 0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#int se 0/0/1
R3(config-if)#zone-member security OUT-ZONE
```

Figure III.55 Application des stratégies du pare-feu

- **Test de la fonctionnalité du pare-feu de IN-ZONE à OUT-ZONE** : Après avoir configuré le pare-feu de stratégie basé sur la zone. Nous allons vérifier que les hôtes internes peuvent toujours accéder aux ressources externes. Suivant les étapes suivantes :

a. **Envoie d'un Ping** : Depuis le PC-C interne, nous envoyons une requête Ping au serveur PC-A externe à (192.168.1.3/24).

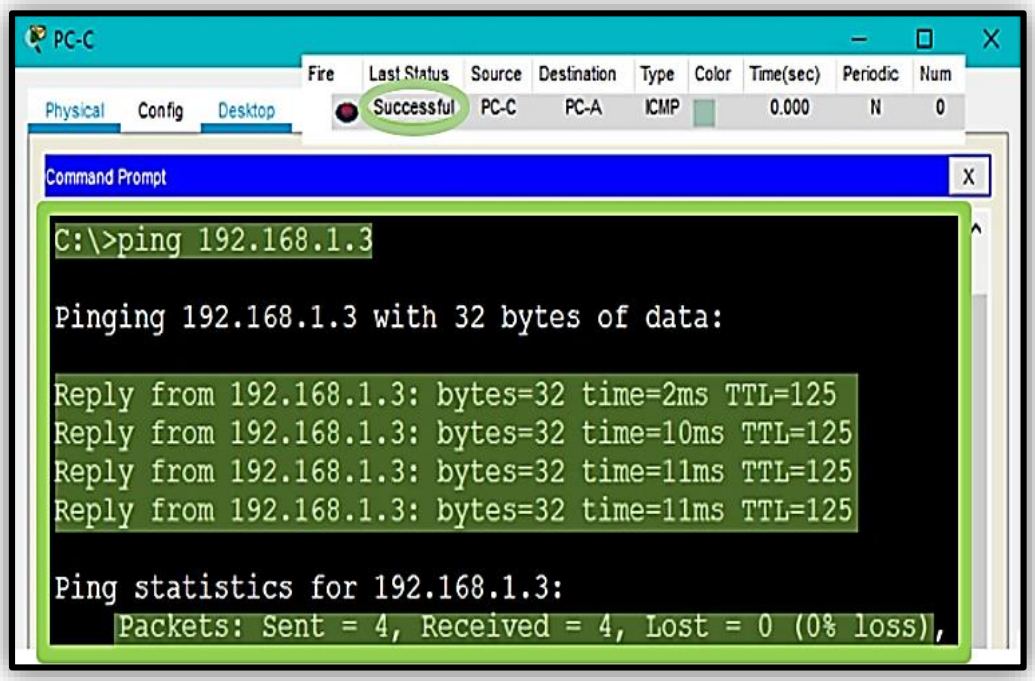


Figure III.56 Envoie d'un Ping

b. **Connexion Telnet** : À partir de l'invite de commande PC-C, nous allons se connecter au routeur R2 à l'interface S0/0/1 (10.2.2.2) en fournissant le mot de passe vty « **ciscovtypa55 ».**

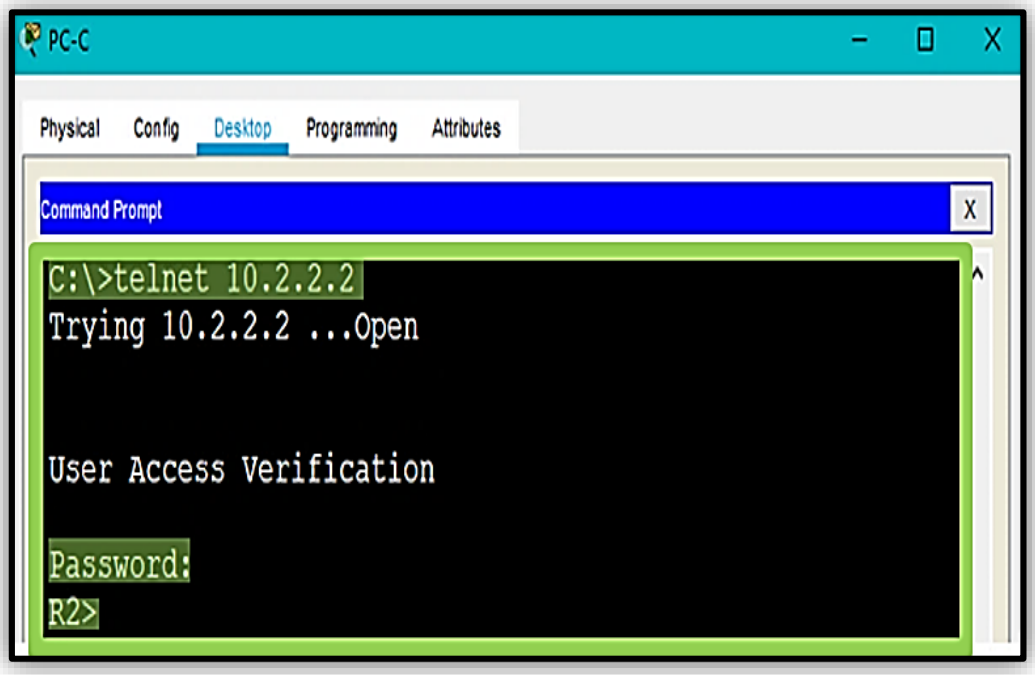


Figure III.57 Connexion Telnet

Pendant que la session Telnet est active, nous allons exécuter la commande **« show policy-map type inspect zone-pair sessions »** sur le routeur R3 pour afficher les sessions établies.

```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 470365872 (192.168.3.3:1029)=>(10.2.2.2:23) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:10, Last heard  00:00:06
          Bytes sent (initiator:responder) [1217:822]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Figure III.58 Affichage des sessions établies du TELNET

c. **Test http** : Depuis le PC-C interne, nous allons ouvrir un navigateur Web sur la page Web du serveur PC-A en tapant l'adresse IP (192.168.1.3/24) dans le champ URL. (Voir la **figure III.59**)

Pendant que la session Telnet est active, nous allons exécuter la commande **« show policy-map type inspect zone-pair sessions »** sur le routeur R3 pour afficher les sessions établies. (Voir la **figure III.60**)

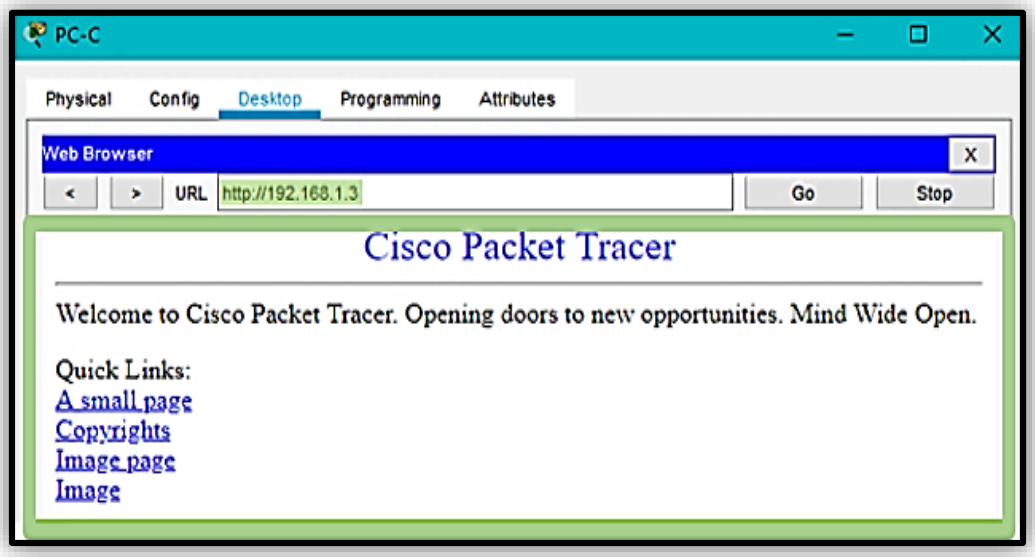


Figure III.59 Test HTTP

```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 335030528 (192.168.3.3:1036)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:02, Last heard  00:00:02
          Bytes sent (initiator:responder) [284:575]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Figure III.60 Affichage des sessions établies du HTTP

❖ **Test de la fonctionnalité du pare-feu de OUT-ZONE à IN-ZONE** : Après avoir configuré le pare-feu de stratégie basé sur la zone. Nous allons vérifier que les hôtes externes ne peuvent pas accéder aux ressources internes par un test Ping.

- À partir de l'invite de commande du serveur PC-A, nous envoyons une requête Ping à PC-C à (192.168.3.3/24). (Ping échoué)
- Depuis le routeur R2, nous envoyons une requête Ping à PC-C à (192.168.3.3/24). (Ping échoué)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Failed	PC-A	PC-C	ICMP		0.000	N	1
●	Failed	R2	PC-C	ICMP		0.000	N	2

Figure III.61 Test de connectivité avec Ping

III.4.5.2 Mise en place du système de prévention des intrusions IOS (IPS)

1. Contexte & Scénario

Notre tâche consiste à configurer le routeur R1 pour IPS afin d'analyser le trafic entrant dans le réseau (192.168.1.0/24). Le serveur intitulé « **Syslog Server** » est utilisé pour enregistrer les messages IPS. Nous devrons configurer le routeur pour identifier le serveur syslog afin de recevoir les messages de

journalisation. L'affichage de l'heure et de la date correcte dans les messages syslog est vital lors de l'utilisation de syslog pour surveiller le réseau. Nous réglons l'horloge et nous configurons le service d'horodatage pour la connexion aux routeurs. Enfin, nous permettons à l'IPS de produire une alerte et de supprimer les paquets de réponse d'écho ICMP en ligne. Les routeurs sont préconfigurés avec les éléments suivants :

- Activation du mot de passe : **master_2_telecommunications** ;
- Mot de passe de la console : **reseaux_telecommunications_2020** ;
- Mot de passe de la ligne VTY : **reseaux_telecommunications_2020_vty** ;
- EIGRP 101.

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Vérifier et activer l'IOS IPS ;
- Configurer la journalisation ;
- Modifier la signature IPS ;
- Vérifier l'IPS.

L'objectif de cette configuration simulé est de se protéger contre les virus, les chevaux de troie, les exploits, les attaques scan et les buffers overflow.

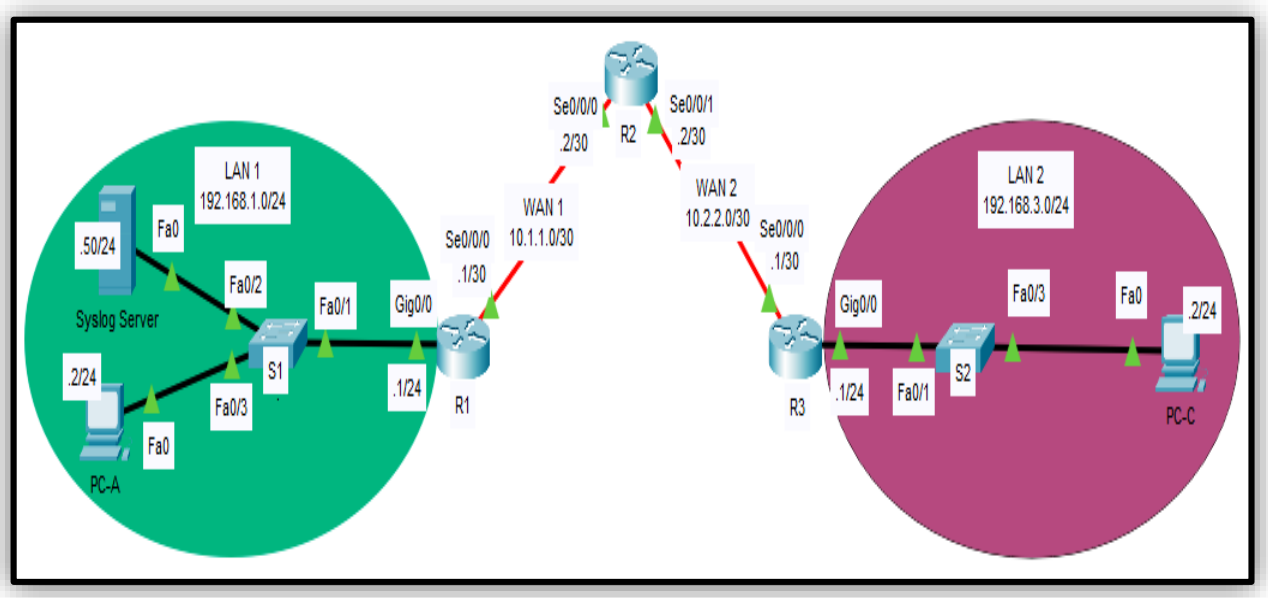


Figure III.62 Architecture du système de prévention des intrusions IOS (IPS)

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.7** suivant.

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/0	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.1	255.255.255.252	N/A

R2	Se0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Se0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A
R3	Gig0/0	192.168.3.1	255.255.255.0	N/A
	Se0/0/0	10.2.2.2	255.255.255.252	N/A
Syslog Server	NIC	192.168.1.50	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Tableau III.7 Table d'adressage pour le réseau du système de prévention des intrusions IOS

4. Configuration d'IOS (IPS) à l'aide de la CLI

Dans Packet Tracer, les routeurs ont déjà les fichiers de signature importés et en place. Ce sont les fichiers xml par défaut en flash. Pour cette raison, il n'est pas nécessaire de configurer la clé de chiffrement publique et effectuer une importation manuelle des fichiers de signature.

❖ Activation d'IOS IPS

a. **Création d'un répertoire de configuration IOS IPS en flash** : Pour activer le système de prévention des intrusions IOS IPS sur le routeur R1, nous devant créer un répertoire de configuration en flash nommée « **ipsdir** » à l'aide de la commande **« mkdir »**. Ensuite, nous allons configurer l'emplacement de stockage des signatures IPS en tapant la commande **« ip ips config location flash:ipsdir »**. Enfin, en mode de configuration globale, nous allons créer un nom de règle IPS nommée « **iosips »** à l'aide de la commande **« ip ips name »**. (Voir la **figure III.63**)

```
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
```

Figure III.63 Création d'un répertoire de configuration IOS IPS en flash

b. **Activation de la journalisation :** Sur le routeur R1, nous allons taper la commande **« ip ips notify log »**, l'IOS IPS prend en charge l'utilisation de syslog pour envoyer une notification d'événement. La notification Syslog est activée par défaut.

Si la console de journalisation est activée, nous voyons des messages IPS syslog. En quittant le mode de configuration globale, nous tapons la commande **« clock set »** pour réinitialiser l'horloge si nécessaire. Nous allons vérifier que le service d'horodatage pour la journalisation est activé sur le routeur à l'aide de la commande **« show run »**. Puis, nous tapons la commande **« service timestamps log datetime msec ».** Nous envoyons des messages de journal au serveur Syslog à l'adresse IP (192.168.1.50/24) par la commande **« logging host 192.168.1.50 »**. (Voir la **figure III.64**)

```
R1(config)#ip ips notify log

R1#clock set 01:20:05 20 april 2020

R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.50
```

Figure III.64 Activation de la journalisation

c. **Configuration d'IOS IPS pour utiliser les catégories de signature** : Nous allons supprimer la catégorie de toutes les signatures avec la commande **« retired true »** (toutes les signatures dans la version de signature) et annuler le retrait de la catégorie « **IOS_IPS Basic »** avec la commande **« retired false ».**

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned
```

Figure III.65 Configuration d'IOS IPS pour utiliser les catégories de signature

d. **Application de la règle IPS à une interface** : Sur l'interface G0/0 du routeur R1, nous appliquons la règle sortante à l'aide de la commande **« ip ips name direction »**. Après avoir activé IPS, certains messages de journal seront envoyés à la ligne de console indiquant que les moteurs IPS sont en cours d'initialisation. (Voir la **figure III.66**)

```
R1(config)#int giga 0/0
R1(config-if)#ip ips iosips out

*avr. 20, 01:43:06.4343:  %IPS-6-ENGINE_BUILDS_STARTED:  01:43:06 UTC avr. 20 2020
*avr. 20, 01:43:06.4343:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*avr. 20, 01:43:06.4343:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for
this engine will be scanned
*avr. 20, 01:43:06.4343:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

Figure III.66 Application de la règle IPS à une interface

Remarque : La direction **IN** signifie qu'IPS inspecte uniquement le trafic entrant dans l'interface. De même, **OUT** signifie uniquement le trafic sortant de l'interface.

❖ Modification de la signature

a. **Modification de l'action-événement d'une signature** : Nous allons annuler le retrait de la signature de la demande d'écho (signature 2004, ID de sous-signature 0) l'activer et modifier l'action de signature en alerte, puis supprimer.

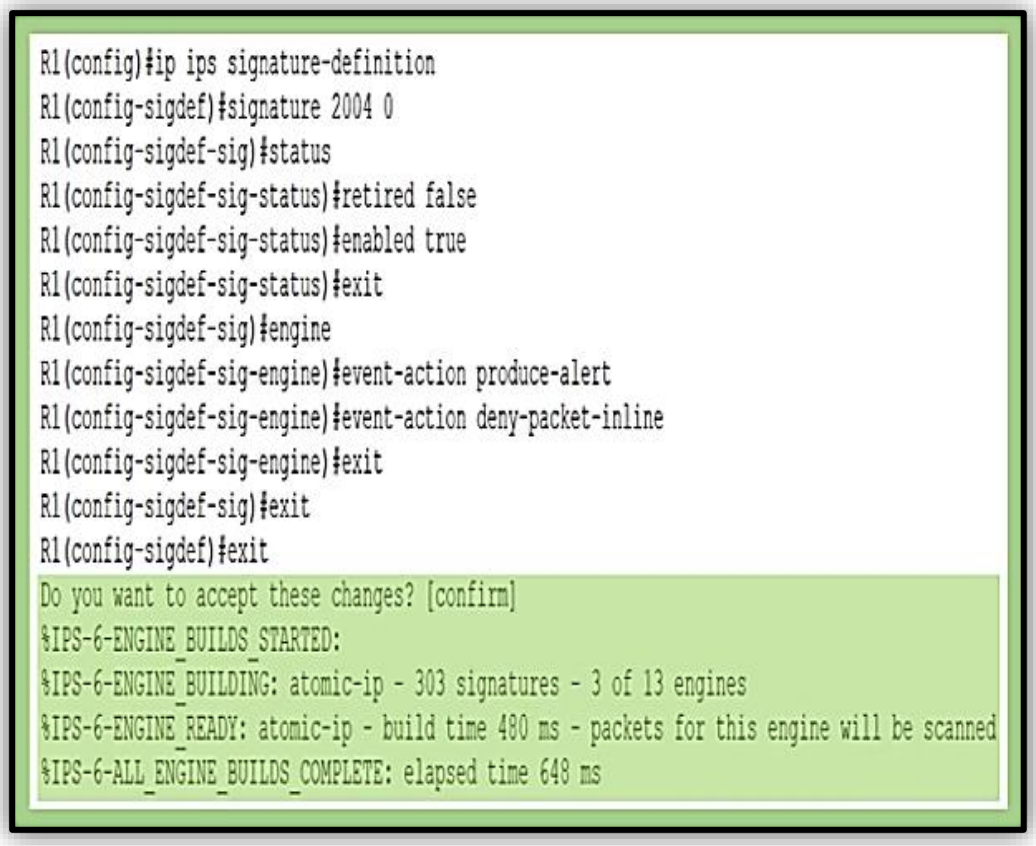


Figure III.67 Modification de l'action-événement d'une signature

b. **Vérification d'IPS** : Nous allons utiliser la commande **« show ip ips all »** pour voir un résumé de l'état de la configuration IPS. (Voir la **figure III.68**)

c. **Vérification du fonctionnement d'IPS (Giga0/0 sortant**): Nous allons vérifier si l'IPS fonctionne correctement. Pour cela, nous envoyons une requête Ping de PC-C à PC-A, puis de PC-A à PC-C. (Voir la **figure III.69**)

Nous remarquons que Les Pings :

- Du PC-C à PC-A sont échoués. Cela est dû au fait que la règle IPS pour l'action sur événement d'une demande d'écho a été définie sur « deny-packetinline ».
- Du PC-A à PC-C sont réussis, car la règle IPS ne couvre pas la réponse d'écho. Lorsque PC-A envoie une requête Ping à PC-C, PC-C répond avec une réponse d'écho.

d. **Affichage des messages Syslog :** Sur le serveur Syslog, nous allons sur l'onglet **Config** puis sur le service **SYSLOG** pour afficher le fichier journal comme le montre la **Figure III.70**.

```
R1#sh ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
      Retire: True
    Category ios_ips basic
      Retire: False
```

Figure III.68 Vérification d'IPS

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC-C	PC-A	ICMP		0.000	N	0
	Successful	PC-A	PC-C	ICMP		0.000	N	1

Figure III.69 Vérification du fonctionnement d'IPS

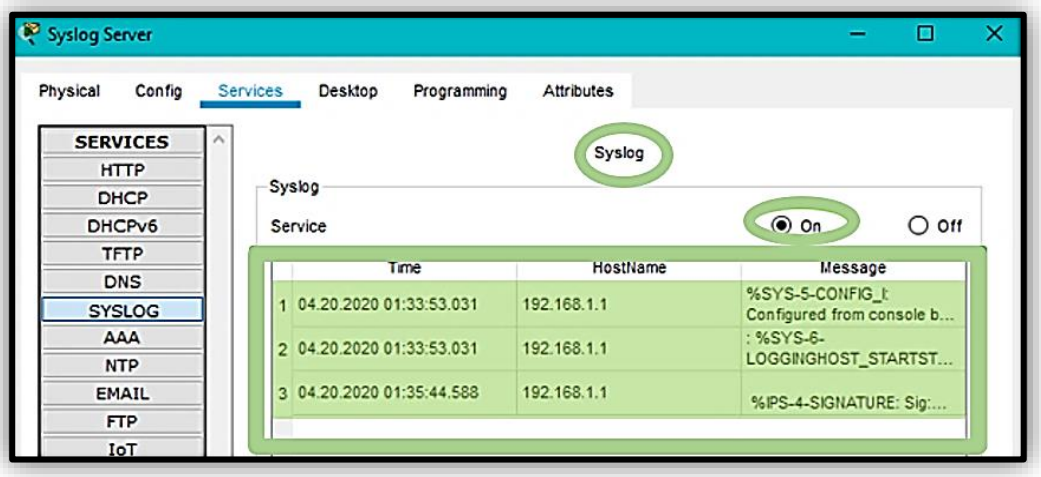


Figure III.70 Affichage les messages Syslog

III.4.6 Mise en place d'un IPsec VPN de site à site

1. Contexte & Scénario

La topologie du réseau montre trois routeurs. Notre tâche consiste à configurer le routeur R1 et R3 pour prendre en charge un VPN IPsec de site à site lorsque le trafic circule entre leurs réseaux locaux respectifs. Le tunnel VPN IPsec aille de R1 à R3 via R2. R2 agit comme un intermédiaire et n'a aucune connaissance du VPN. IPsec fournit une transmission sécurisée d'informations sensibles sur des réseaux non protégés, tels qu'Internet. IPsec fonctionne au niveau de la couche réseau, il protège et authentifie les paquets IP entre les périphériques IPsec participants (homologues), tels que les routeurs Cisco. Les routeurs sont préconfigurés comme la configuration d'IOS IPS**.** (Voir **la page 103**)

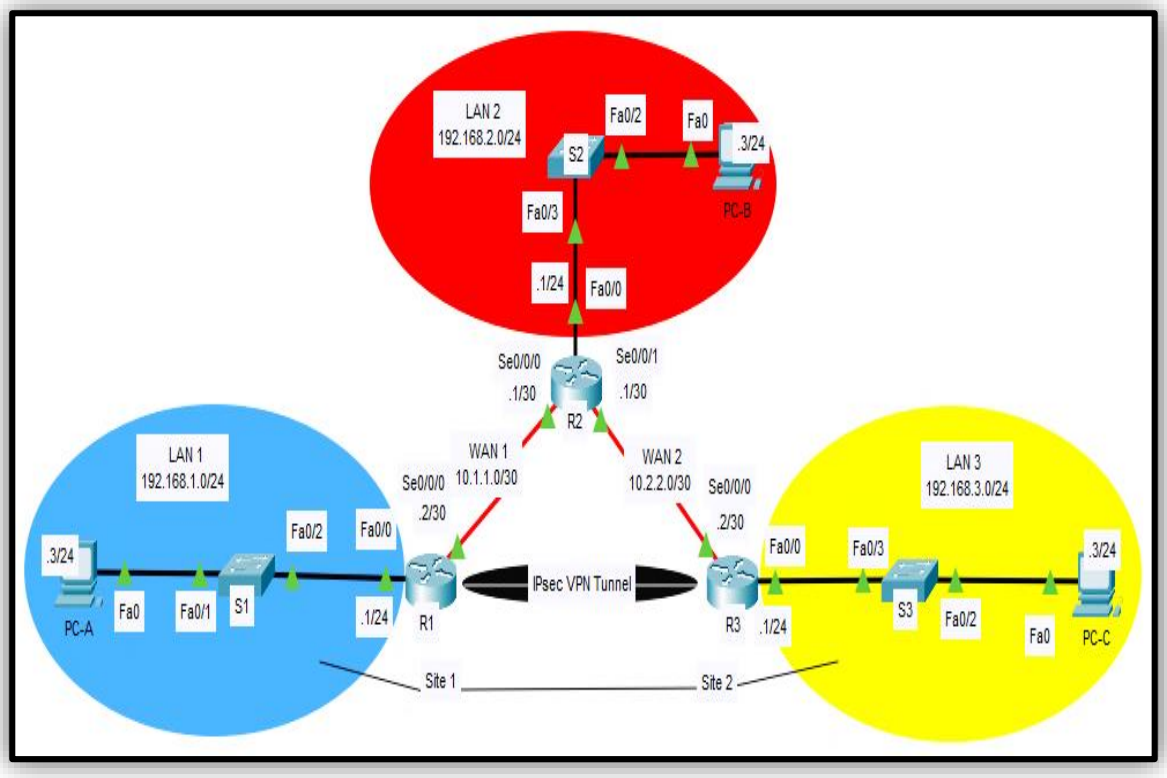


Figure III.71 Architecture d'un réseau IPsec VPN site à site

Le **tableau III.8** indique les paramètres de stratégie ISAKMP Phase 1, les paramètres en gras sont les valeurs par défaut. Seuls les paramètres en gras doivent être configurés explicitement. Et le **tableau III.9** indique les paramètres de stratégie IPsec Phase 2.

Paramètres		R1	R3
Méthode de distribution des clés	Manual ou **ISAKMP**	**ISAKMP**	**ISAKMP**
Algorithme de chiffrement	**DES**, 3DES, ou AES	AES	AES
Algorithme de hachage	MD5 ou **SHA-1**	**SHA-1**	**SHA-1**
Méthode d'authentification	Clés Pre-shared ou **RSA**	Pre-share	Pre-share
Échange de clés	Groupe DH 1, 2, ou **5**	DH 5	DH 5
Durée de vie de IKE SA	86400 secondes ou moins	**86400**	**86400**
Clé ISAKMP	/	vpnpa55	vpnpa55

Tableau III.8 Paramètres de stratégie ISAKMP Phase 1

Paramètres	R1	R3
Ensemble de transformation (Transform Set)	VPN-SET	VPN-SET
Nom d'hôte homologue (Peer Hostname)	R3	R1
Adresse IP homologue (Peer IP Address)	10.2.2.2/30	10.1.1.2/30
Réseau à chiffrer (Network to be encrypted)	192.168.1.0/24	192.168.3.0/24
Nom de la carte cryptographique (Crypto Map name)	VPN-MAP	VPN-MAP

Tableau III.9 Paramètres de stratégie IPsec Phase 2

2. Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Vérifier la connectivité à travers le réseau ;
- Configurer le routeur R1 pour prendre en charge un VPN IPsec de site à site avec R3.

L'objectif de cette configuration simulé est de bloquer les attaques Dos, les buffers overflow, man in the middle et les craques des mots passe.

3. Désignation des interfaces & de la table d'adressage

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau III.10** suivant.

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.2	255.255.255.252	N/A
R2	Se0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
R3	Fa0/0	192.168.3.1	255.255.255.0	N/A
	Se0/0/0 (DCE)	10.2.2.2	255.255.255.252	N/A

PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Tableau III.10 Table d'adressage pour le réseau IPsec VPN site à site

4. Configuration & vérification d'IPsec VPN site à site à l'aide de la CLI

❖ Configuration des paramètres IPsec sur le routeur R1

a. **Identification du trafic intéressant** : Au cours de cette partie, nous allons configurer une liste ACL **110** pour identifier le trafic du LAN sur R1 au LAN sur R3 comme intéressant. Ce trafic intéressant déclenchera la mise en œuvre du VPN IPsec chaque fois qu'il y a du trafic entre les réseaux locaux R1 et R3. Tout autre trafic provenant des réseaux locaux ne sera pas chiffré. (Voir la **figure III.72**)

b. **Configuration des propriétés ISAKMP Phase 1** : Maintenant, à l'aide du tableau des paramètres de stratégie ISAKMP Phase 1 « **Tableau III.8** » nous allons configurer les propriétés de la politique **10** de cryptage ISAKMP sur R1 avec la clé de cryptage partagée « **vpnpa55 »**. Les valeurs par défaut ne doivent pas être configurées, par conséquent, seuls le chiffrement, la méthode d'échange de clés et la méthode DH doivent être configurés.

Le groupe DH le plus élevé actuellement pris en charge par Packet Tracer est le groupe 5. Dans un réseau de production, nous devrons configurer au moins DH 14. (Voir la **figure III.72**)

```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
```

Figure III.72 Configuration des paramètres IPsec et des propriétés ISAKMP Phase 1 du R1

c. **Configuration des propriétés ISAKMP Phase 2 :** Nous allons créer le jeu de transformations « **VPN-SET** » pour utiliser « **esp-aes »** et « **esp-sha-hmac »** et créer par la suite la carte cryptographique « **VPNMAP »** qui lie tous les paramètres de la phase 2 ensembles. Nous allons utiliser le numéro de séquence **10** et l'identifier comme une carte « **ipsec-isakmp ».** (Voir la **figure III.73**)

d. **Configuration de la carte cryptographique sur l'interface sortante :** Enfin, nous allons lier la carte de chiffrement « **VPN-MAP »** à l'interface S0/0/0 sortante. (Voir la **figure III.74**)

```
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
```

Figure III.73 Configuration des propriétés ISAKMP Phase 2 du R1

```
R1(config-crypto-map)#int se 0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure III.74 Configuration de la carte cryptographique sur l'interface sortante du R1

❖ **Configuration des paramètres IPsec sur le routeur R3**

a. **Configuration du routeur R3 pour prendre en charge un VPN de site à site avec R1** : Maintenant, nous allons configurer les paramètres alternatifs sur le routeur R3 et l'ACL **110** en identifiant le trafic du LAN sur R3 au LAN sur R1 comme intéressant. (Voir la **figure III.75**)

b. **Configuration des propriétés ISAKMP Phase 1 :** Suivant la table des paramètres de stratégie ISAKMP Phase 1 « **Tableau III.8** », nous allons configurer les propriétés de la politique **10** de cryptage ISAKMP sur le routeur R3 avec la clé de cryptage partagée « **vpnpa55 »**. (Voir la **figure III.75**)

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
```

Figure III.75 Configuration des paramètres IPsec et des propriétés ISAKMP Phase 1 du R3

c. **Configuration des propriétés ISAKMP Phase 2 :** Comme nous l'avons fait sur le routeur R1, nous allons créer le jeu de transformations « **VPN-SET »** pour utiliser » **esp-aes »** et « **esp-sha-hmac ».** Ensuite, nous allons créer la carte cryptographique « **VPN-MAP »** qui lie tous les paramètres de la phase 2 ensembles. Nous utilisons le numéro de séquence **10** et l'identifier comme une carte « **ipsec-isakmp »**.

```
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
```

Figure III.76 Configuration des propriétés ISAKMP Phase 2 sur R3

C. **Configuration de la carte cryptographique sur l'interface sortante :** Nous allons lier la carte de chiffrement « **VPN-MAP »** à l'interface S0/0/0 sortante.

```
R3(config-crypto-map)#int se 0/0/0
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure III.77 Configuration de la carte cryptographique sur l'interface sortante du R3

❖ Vérification du VPN IPsec

a. **Vérification du tunnel avant le trafic intéressant :** Sur le routeur R1, nous tapons la commande **« show crypto ipsec sa »** et nous remarquons que le nombre de paquets encapsulés, cryptés, décapsulés et décryptés sont tous définis sur 0.

```
R1#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

Figure III.78 Vérification du tunnel avant le trafic intéressant

b. **Création d'un trafic intéressant** : Depuis PC-A, nous envoyons une requête Ping à PC-C. (Voir la **figure III.79**)

c. **Vérification du tunnel après un trafic intéressant** : Sur le routeur R1, nous lançons la commande **« show crypto ipsec sa »** et nous remarquons bien que le nombre de paquets est supérieur à 0, ce qui indique que le tunnel VPN IPsec fonctionne. (Voir la **figure III.80**)

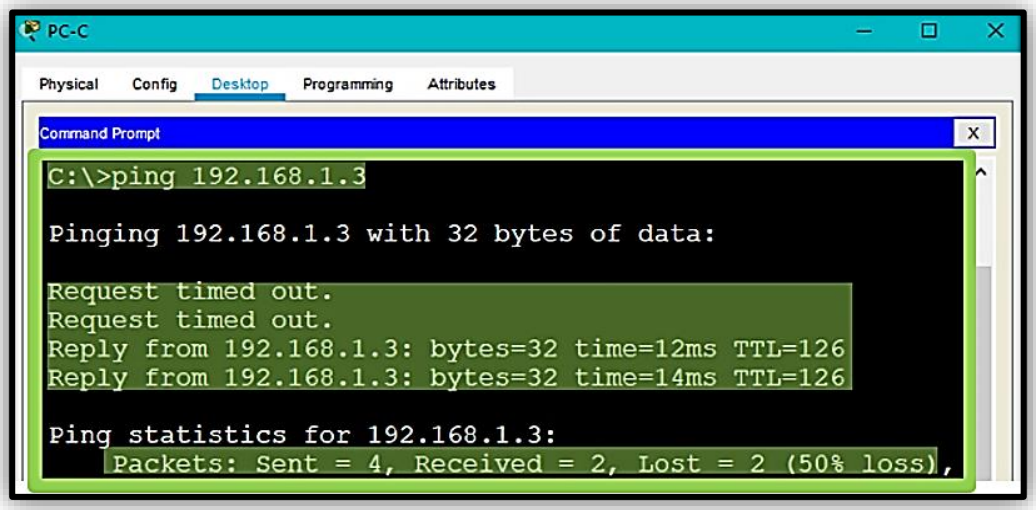


Figure III.79 Vérification du tunnel avant le trafic intéressant

Figure III.80 Vérification du tunnel après le trafic intéressant

a. **Création du trafic non intéressant** : Depuis PC-A, nous envoyons une requête Ping à PC-B.

b. **Vérification du tunnel** : Sur le routeur R1, nous allons relancer la commande **« show crypto ipsec sa »**, nous remarquons que le nombre de paquets n'a pas changé, ce qui vérifie que le trafic non intéressant n'est pas chiffré. (Voir la **figure III.82**)

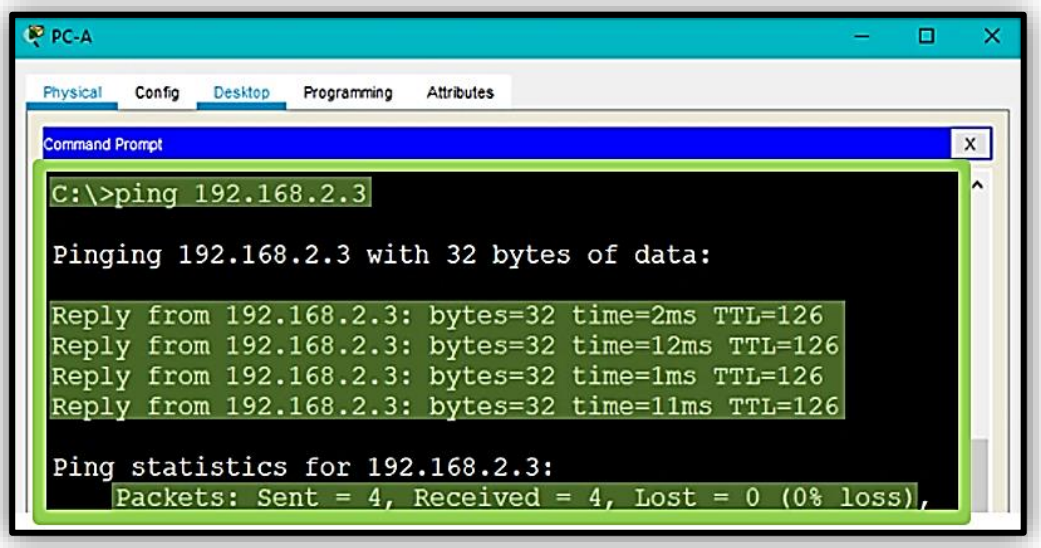


Figure III.81 Création du trafic non intéressant

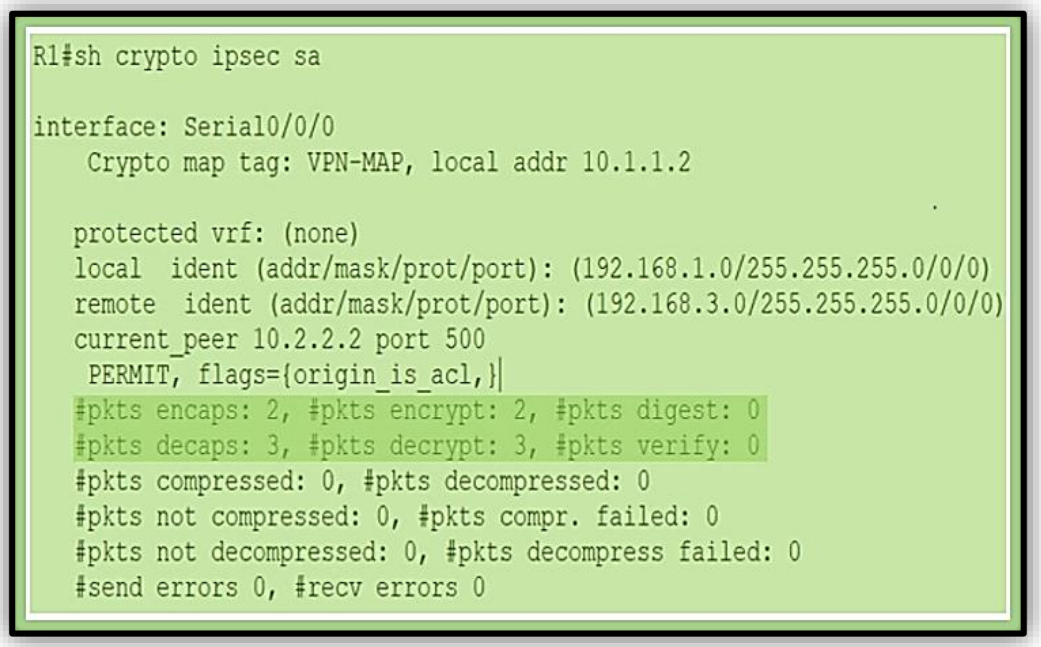


Figure III.82 Vérification du tunnel après un trafic non intéressant

III.5 Conclusion

Nous avons consacré ce chapitre pour présenter un aperçu sur l'importance de l'implémentation des mécanismes de sécurité dans un réseau informatique. Pour cela, nous avons commencé par introduire le simulateur Packet tracer avec la description du plan de travail.

Ensuite, nous avons étudier chaque mécanisme séparément en fonction des différentes configurations de nos architectures réseaux précédentes ainsi que les tests de vérification du bon fonctionnement des protocoles et solutions les plus répandues actuellement pour avoir une forte sécurisation sachant que ces mécanismes sont déployés à grande échelle car se trouvant déjà sur la plupart des plateformes de la toile, aussi bien au niveau des serveurs qu'au niveau des clients.

Le prochain chapitre sera consacré à une simulation générale avec la mise en œuvre de politiques de sécurité réseaux Cisco pour un but d'améliorer la stratégie visant à maximiser et assurer la sécurité des différents réseaux d'entreprises.

CHAPITRE IV

Mise en œuvre de Politiques de Sécurité Réseaux CISCO

IV.1 Introduction

La politique de sécurité est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'entreprise en matière de sécurité des systèmes d'informations (SSI). Outre, Une politique de sécurité globale est un ensemble de politiques de sécurité indépendantes mais cohérentes.

Au cours de ce dernier chapitre, nous allons passer à la dernière étape de notre travail qui est l'achèvement de notre projet. Cette dernière est une cruciale pour la mise en œuvre de politiques de sécurité réseaux Cisco. Ce chapitre est divisé en deux configuration globale la première s'agit de configurer un réseau pour un fonctionnement sécurisé et la deuxième est conçue pour la configuration des paramètres de base ASA et du pare-feu avec la sécurité de la couche 2.

IV.2 Configuration d'un réseau pour un fonctionnement sécurisé

IV.2.1 Synopsis de la configuration simulée

A travers de cette simulation, nous allons appliquer une combinaison de mesures de sécurité qui ont été introduites dans le chapitre précèdent. Ces mesures sont énumérées dans les objectifs.

Dans notre topologie, le routeur R1 est le bord extérieur pour la société « A » tandis que R3 est le routeur de bord pour la société « B ». Ces réseaux sont interconnectés via le routeur R2 qui représente le FAI. Nous allons configurer les différentes sécurités sur les routeurs et commutateurs des sociétés « A » et « B ». Toutes les fonctions de sécurité ne seront pas configurées sur R1 et R3. Les routeurs doivent êtres préconfigurés avec les éléments suivants :

- Noms d'hôtes sur tous les appareils ;
- Adresses IP sur tous les appareils ;
- Mot de passe de la console R2 : **reseaux_telecommunications_2020** ;
- Mot de passe R2 sur les lignes VTY : **reseaux_telecommunications_2020_vty** ;
- Activation du mot de passe sur R2 : **master_2_telecommunications** ;
- Routage statique ;
- Services Syslog sur PC-B.

IV.2.2 But de la configuration simulée

Cette réalisation a pour l'objectif de :

- Sécuriser les routeurs avec des mots de passe forts, un cryptage de mot de passe et une bannière de connexion ;
- Sécuriser la console et les lignes VTY avec des mots de passe ;
- Configurer l'authentification AAA locale ;
- Configurer le serveur SSH ;
- Configurer le routeur pour syslog et pour NTP ;
- Configurer les pare-feux CBAC et ZPF ;
- Configurer la sécurité des commutateurs réseau.

L'objectif de cette configuration simulé est de lutter contre les attaques de type déni de service, vol du mot passe, les attaques par rejeu, SYN flood, Ping flood, porte dérobée et man in the middle. De plus, ARP Spoofing et DHCP Snooping.

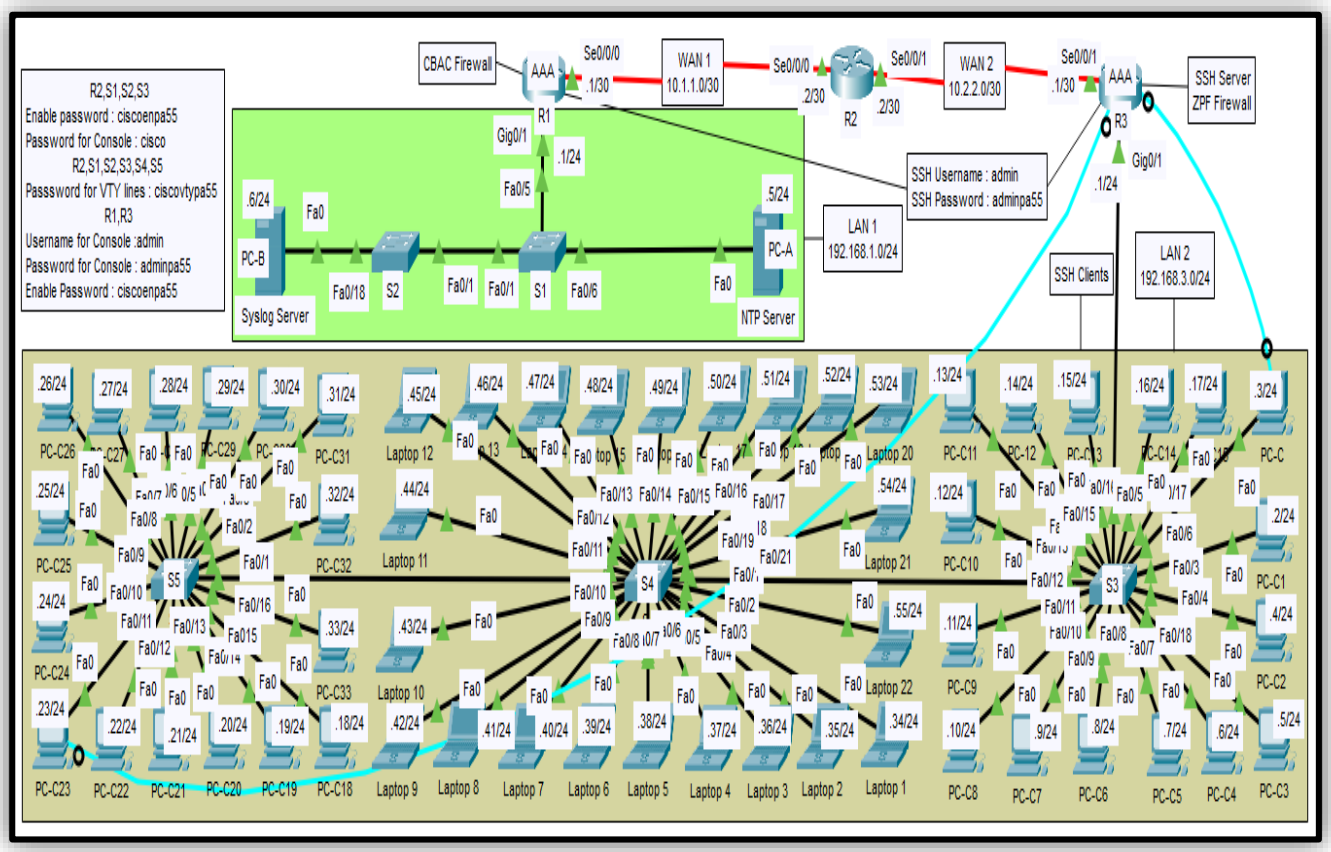


Figure IV.1 Architecture d'un réseau pour un fonctionnement sécurisé

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau IV.1** suivant

Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/1	192.168.1.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Se0/0/0(DCE)	10.1.1.2	255.255.255.252	N/A
	Se0/0/1(DCE)	10.2.2.1	255.255.255.252	N/A
R3	Gig0/1	192.168.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.2	255.255.255.252	N/A
Laptop 1 ……. Laptop 22	NIC	192.168.3.34 … 192.168.3.55	255.255.255.0	192.168.3.1
PC-C ……. PC-C33	NIC	192.168.3.3 …. 192.168.3.33	255.255.255.0	192.168.3.1

Tableau IV.1 Table d'adressage pour le réseau pour un fonctionnement sécurisé

IV.2.3 Configuration des paramètres de sécurité sur les routeurs & les commutateurs

IV.2.3.1 Sécurisation des routeurs

a. **Identification d'un mot de passe sur le routeur R1 et R3 :** Au cours de cette partie, nous allons définir une longueur d'épée minimale de quatre caractères sur les deux routeurs. Ensuite, configurer une épée de pas secret d'activation en utilisant le mot de passe secret **« master_2_telecommunications »**. En fin, nous allons crypter les mots de passe en texte brut.

b. **Configuration des lignes de console et des lignes VTY sur le routeur R1 et R3 :** Premièrement, nous allons configurer un mot de passe **« reseaux_telecommunications_2020 »** pour la ligne de console, nous activons la connexion et nous allons par la suite définir le délai d'exécution pour la déconnexion après **10** minutes d'inactivité.

Deuxièment, nous configurons le mot passe **« reseaux_telecommunications_2020_vty »** pour les lignes vty, l'activation de la connexion, définition du délai d'exécution pour nous déconnecterons après **10** minutes d'inactivité et nous allons définir aussi l'authentification de connexion pour utiliser une liste AAA par défaut.

c. **Configuration de la bannière de connexion sur le routeur R1 et R3 :** Nous allons configurer un avertissement pour les utilisateurs non autorisés avec une bannière de message du jour (MOTD) qui dit: "Pas d'accès non autorisé!".

La **figure IV.2** montre la configuration des étapes (a,b,c) sur le routeur R1.

```
R1(config)#security password min-length 4
R1(config)#enable secret master_2_telecommunications
R1(config)#service password-encryption
```

```
R1(config)#line console 0
R1(config-line)#password reseaux_telecommunications_2020
R1(config-line)#exec-timeout 10 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password reseaux_telecommunications_2020_vty
R1(config-line)#exec-timeout 10 0
R1(config-line)#login authentication default
 AAA: Warning authentication list default is not defined for LOGIN
R1(config-line)#exit
```

```
R1(config)#banner motd $No Unauthorized Access!$
```

Figure IV.2 Sécurisation du routeur R1

IV.2.3.2 Configuration de l'authentification locale sur le routeur R1 et R3

Pour la configuration de la base de données d'utilisateurs locale, nous devant créer un compte d'utilisateur local nommée « **Admin »** avec un mot de passe secret « **Adminpa55** » et activer les services AAA. Puis, nous allons créer une liste des méthodes d'authentification de connexion par défaut à l'aide de l'authentification locale sans méthode de sauvegarde. (Voir la **figure IV.3**)

```
R1(config)#username Admin privilege 15 secret Adminpa55
R1(config)#aaa new-model
R1(config)#aaa authentication login default local none
```

Figure IV.3 Configuration de l'authentification locale

IV.2.3.3 Configuration du NTP

a. **Activation d'authentification NTP :** Sur l'onglet **Config** du PC-A, nous allons activer le service NTP en tapant sur le bouton **« Activé »**, activer aussi l'authentification et entrer une clé de **1** plus un mot de passe de « **NTPpa55 ».**

Ensuite, nous allons configurer le routeur R1 en tant que client NTP. Cela se fait à l'aide de la configuration de la clé d'authentification NTP **1** et le mot de passe « **NTPpa55 »** puis, la configuration du routeur R1 pour qu'il se synchronise avec le serveur NTP et s'authentifie à l'aide de la clé **1**.

Enfin, pour la configuration des routeurs pour mettre à jour l'horloge matérielle, nous allons configurer le routeur pour mettre à jour périodiquement l'horloge matérielle avec l'heure apprise du NTP à l'aide de la commande « **ntp update-calendar ».**

```
R1(config)#ntp authenticate
R1(config)#ntp authentication-key 1 md5 NTPpa55
R1(config)#ntp trusted-key 1
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
```

Figure IV.4 Configuration du NTP

IV.2.3.4 Configuration du routeur R1 en tant que client Syslog

a. **Configuration du routeur R1 pour multiplier les messages de journal de tamponnage :** Nous allons configurer le service d'horodatage pour la connexion aux routeurs à l'aide de la commande « **service timestamps log datetime msec »**. (Voir la **figure IV.5**)

b. **Configuration du R1 pour consigner les messages sur le serveur de journalisation :** Maintenant, nous allons configurer les routeurs pour identifier l'hôte distant (serveur syslog) qui recevra les messages de journalisation. (Voir la **figure IV.5**)

c. **Vérification des messages syslog sur PC-B :** En quittant le mode de configuration pour la génération d'un message syslog sur le routeur R1. Nous allons ouvrir le serveur syslog sur PC-B pour afficher le message envoyé par R1. (Voir la **figure IV.6**)

```
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.6
R1(config)#exit
R1#
*juin 22, 15:32:41.3232: SYS-5-CONFIG_I: Configured from console by console
*juin 22, 15:32:41.3232:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514
started - CLI initiated
```

Figure IV.5 Configuration du routeur en tant que client Syslog

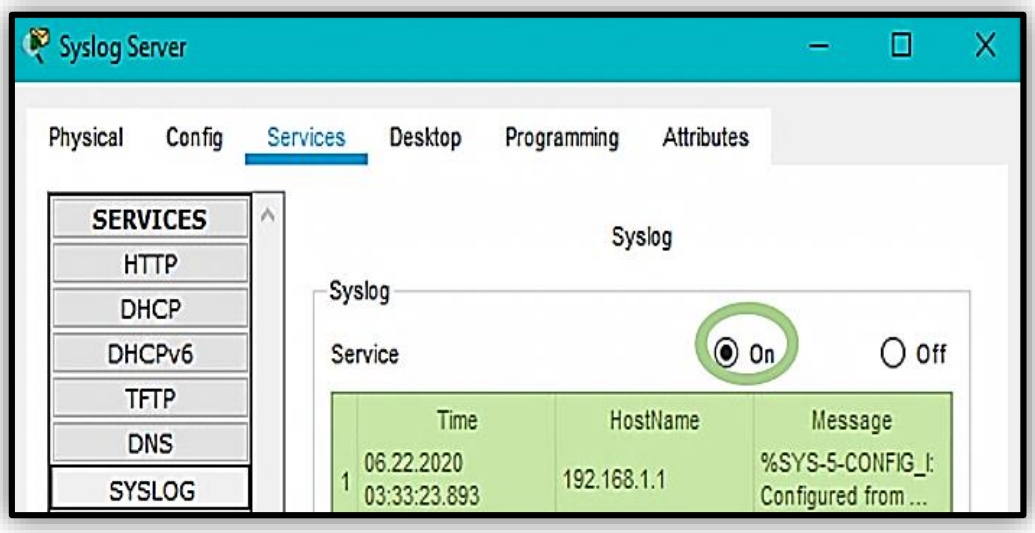


Figure IV.6 Affichage des messages syslog

IV.2.3.5 Configuration du SSH sur le routeur R3

a. **Configuration d'un nom de domaine :** Nous allons configurer un nom de domaine ccnasecurity.com sur le routeur R3 en tapant la commande « **ip domain-name ccnasecurity.com ».** (Voir la **figure IV.7**)

b. **Configuration des lignes vty entrantes** : Sur le routeur R3, nous allons utiliser les comptes d'utilisateurs locaux pour la connexion et la validation obligatoires pour que uniquement les connexions SSH soient acceptées. Tout cela en appliquant les commandes suivantes par ordre « **line vty 0 15 », « exec-timeout 10 0 », « login local », « transport input ssh ».** (Voir la **figure IV.7**)

Figure IV.7 Configuration du SSH

c. **Configuration de la paire de clés de chiffrement RSA :** Toutes les paires de clés RSA existantes doivent être effacées sur le routeur R3. S'il n'y a aucune clé actuellement configurée, un message s'affiche pour l'indiquer. Nous allons configurer les clés RSA avec un module de 1024. (Voir la **figure IV.8**)

d. **Configuration des délais d'expiration SSH et des paramètres d'authentification** : Nous allons définir le délai d'expiration SSH sur 90 secondes, le nombre de tentatives d'authentification sur **2** et la version sur **2**. (Voir la **figure IV.9**)

Figure IV.8 Configuration de la paire de clés de chiffrement RSA

```
R1(config)#ip ssh time-out 90
R1(config)#ip ssh authentication-retries 2
R1(config)#ip ssh version 2
```

Figure IV.9 Configuration des délais d'expiration SSH et des paramètres d'authentification

IV.2.3.6 Configuration du CBAC sur le routeur R1

a. **Configuration d'une ACL IP :** Nous allons créer une ACL IP nommée « **OUT-IN** » pour bloquer tout le trafic provenant du réseau extérieur et appliquer la liste d'accès au trafic entrant sur l'interface S0/0/0.

```
R1(config)#ip access-list extended OUT-IN
R1(config-ext-nacl)#deny ip any any
R1(config-ext-nacl)#exit
R1(config)#int se 0/0/0
R1(config-if)#ip access-group OUT-IN in
R1(config-if)#exit
```

Figure IV.10 Configuration d'une ACL IP

b. **Vérification de la suppression du trafic entrant dans l'interface série 0/0/0** : À l'invite de commande du PC-A, on envoie une requête **Ping** à PC-C. Nous allons remarquer que les réponses d'écho ICMP sont bloquées par l'ACL. (Voir la **figure IV.11**)

c. **Création d'une règle d'inspection pour inspecter le trafic ICMP, Telnet et http :** Nous allons créer une règle d'inspection nommée « **IN-OUT-IN »** pour inspecter le trafic **ICMP**, **Telnet** et **HTTP**. (Voir la **figure IV.12**)

d. **Application de la règle d'inspection à l'interface extérieure :** Nous appliquons la règle d'inspection « **IN-OUT-IN »** à l'interface où le trafic sort vers les réseaux extérieurs. (Voir la **figure IV.12**)

e. **Test de fonctionnement de la règle d'inspection :** A l'invite de commande du PC-A, nous allons envoyer une requête **Ping** à PC-C. Les réponses d'écho ICMP doivent être inspectées et autorisées. (Voir la **figure IV.13**)

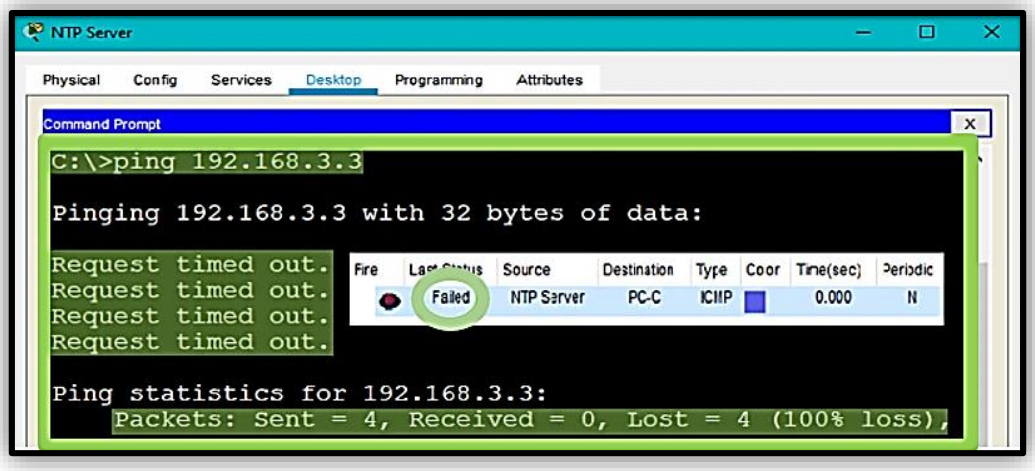


Figure IV.11 Vérification de la suppression du trafic entrant

```
R1(config)#ip inspect name IN-OUT-IN icmp
R1(config)#ip inspect name IN-OUT-IN telnet
R1(config)#ip inspect name IN-OUT-IN http
R1(config)#int se 0/0/0
R1(config-if)#ip inspect IN-OUT-IN out
```

Figure IV.12 Création d'une règle d'inspection

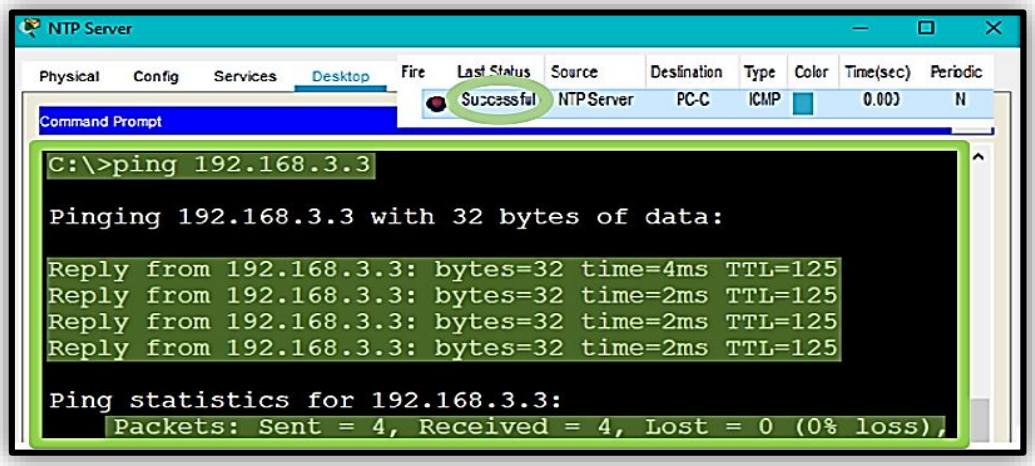


Figure IV.13 Test de fonctionnement de la règle d'inspection

IV.2.3.7 Configuration du ZPF sur le routeur R3

a. **Test de connectivité :** Pour vérifier que l'hôte interne peut accéder aux ressources externes, nous allons appliquer les tests suivants :

- Depuis PC-C, nous envoyons une requête Ping et Telnet vers le routeur R2.
- Une requête Ping du routeur R2 au PC-C.

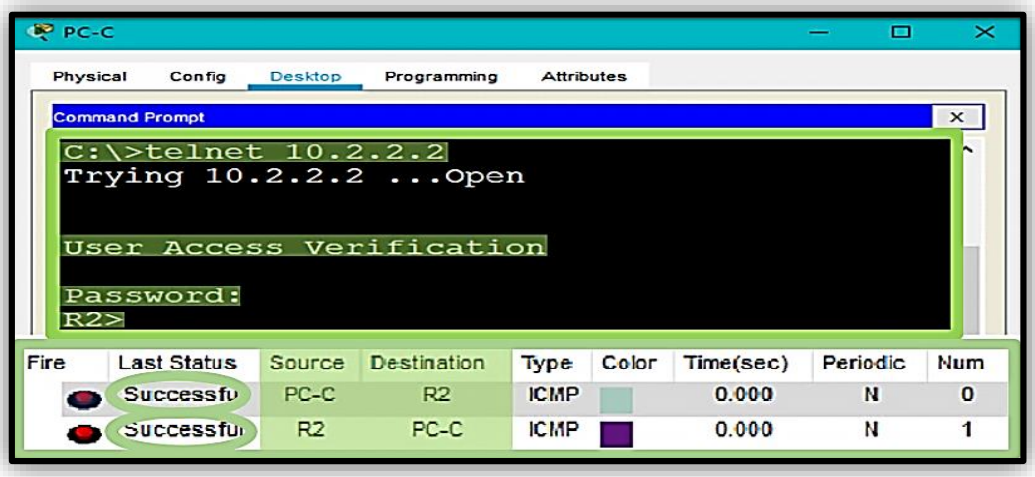


Figure IV.14 Test de connectivité

b. **Création des zones du pare-feu :** A l'aide de la commande « **zone security IN-ZONE »** nous allons créer une zone interne nommée « **IN-ZONE »** et une zone externe nommée « **OUT-ZONE »** en tapant la commande suivante « **zone security OUT-ZONE ».** (Voir la **figure IV.15**)

```
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#zone security OUT-ZONE
R3(config-sec-zone)#exit
```

Figure IV.15 Création des zones du pare-feu

c. **Création d'une ACL qui définit le trafic interne :** A l'aide de la commande « **access-list 101 permit ip 192.168.3.0 0.0.0.255 any** », nous allons créer une liste de contrôle d'accès étendue et numérotée qui autorise tous les protocoles IP du réseau source (192.168.3.0/24) vers n'importe quelle destination. Nous utilisons **101** pour le numéro ACL. Ensuite, nous passons à la création d'une carte de classe référençant l'ACL de trafic interne où nous allons créer un mappage de classe nommé « **IN-NET-CLASS-MAP** » pour correspondre à ACL 101. En tapant la commande « **class-map type inspect match-all IN-NET-CLASS-MAP** » et « **match access-group 101** ». (Voir la **figure IV.16**)

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
```

Figure IV.16 Création d'une ACL et d'une classe de trafic interne

d. **Spécification des politiques du pare-feu :** Dans cette étape, on va créer une carte de stratégie nommée « **IN-2-OUT-PMAP »** pour déterminer quoi faire avec le trafic correspondant**.** Ensuite, nous allons spécifier un type de mappage de classe d'inspection et de référence « **IN-NET-CLASS-MAP ».** Enfin, nous spécifions l'action d'inspection pour cette carte de stratégie. (Voir la **figure IV.17**)

```
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
```

Figure IV.17 Spécification des politiques du pare-feu

e. **Application des stratégies de pare-feu :** Premièrement, nous allons créer une paire de zones nommée « **IN-2-OUT-ZPAIR ».** Deuxièmement, nous spécifions les zones source et de destination créées précédemment. Finalement, nous allons attacher une carte de stratégie et des actions à la paire de zones faisant référence à la carte de stratégie précédemment créée « **IN-2-OUT-PMAP »**, nous quittons la configuration globale et nous allons affecter les interfaces internes et externes aux zones de sécurité.

```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#int giga 0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#int se 0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
```

Figure IV.18 Application des stratégies du pare-feu

f. **Test de fonctionnalité du pare-feu :** Pour vérifier que l'hôte interne peut toujours accéder aux ressources externes, nous appliquons les tests comme nous les montre la figure ci-dessous.

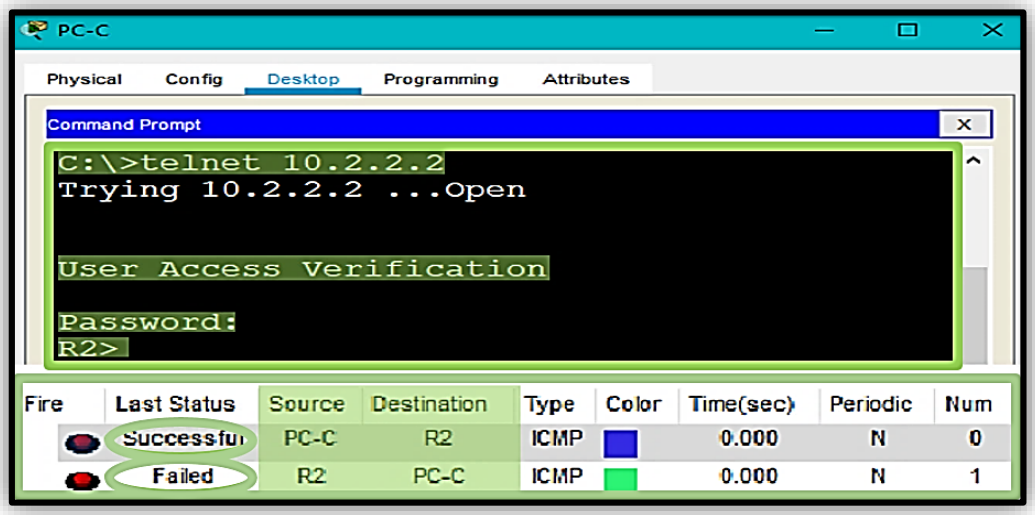


Figure IV.19 Test de fonctionnalité du pare-feu

IV.2.3.8 Sécurisation des commutateurs

a. **Configuration d'un mot de passe secret d'activation sur tous les commutateurs :** Tout d'abord, nous utilisons un mot de passe secret activé « **master_2_telecommunications »** et le crypter en texte brut. Ensuite, passant à la configuration des lignes de console sur tous les commutateurs, nous configurons un mot de passe de console « **reseaux_telecommunications_2020 »** et activons la connexion puis nous allons définir le délai d'exécution pour nous déconnecterons après **10** minutes d'inactivité. Enfin, nous allons configurer un mot de passe de ligne vty « **reseaux_telecommunications_2020_vty »** et activer la connexion puis nous allons définir le délai d'exécution pour la déconnection après **10** minutes d'inactivité. (Voir la **figure IV.20**)

```
S1(config)#enable secret master_2_telecommunications
S1(config)#service password-encryption
S1(config)#line console 0
S1(config-line)#password reseaux_telecommunications_2020
S1(config-line)#exec-timeout 10 0
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password reseaux_telecommunications_2020_vty
S1(config-line)#exec-timeout 10 0
S1(config-line)#login
S1(config-line)#exit
```

Figure IV.20 Configuration d'un mot de passe secret d'activation sur des commutateurs

NB : Nous allons appliquer la même opération pour tous les autres commutateurs.

b. **Fixation des ports de jonction sur le commutateur S1 et S2 :** Nous allons configurer le port Fa0/1 sur S1 comme port de jonction, définir le VLAN natif sur les ports de jonction S1 et S2 sur un VLAN 99 inutilisé et les ports de jonction sur S1 et S2 afin qu'ils ne négocient pas en désactivant la génération de trames DTP. En terminant par activer le contrôle des tempêtes pour les diffusions sur les ports de jonction S1 et S2 avec un niveau de suppression croissant de 50%. (Voir la **figure IV.21**)

```
S1(config)#int fa 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with
S2 FastEthernet0/1 (1).

S1(config-if)#switchport nonegotiate
S1(config-if)#storm-control broadcast level 50
S1(config-if)#exit
S1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99), with
S2 FastEthernet0/1 (1).
```

Figure IV.21 Fixation des ports de jonction sur un commutateur

NB : Nous appliquons la même opération sur le commutateur S2.

c. **Ports d'accès sécurisés :** Maintenant, nous allons désactiver la jonction sur les ports d'accès S1, S2 et S3 comme c'est mentionner dans la **figure IV.22.** Ensuite, nous activons le PortFast sur les mêmes ports

d'accès S1, S2 et S3. Outre, nous activons la protection BPDU sur les ports de commutateur précédemment configurés en tant qu'accès uniquement comme il est illustré dans la **figure IV.23.**

```
S1(config)#int fa 0/5
S1(config-if)#switchport mode access
S1(config-if)#int fa 0/6
S1(config-if)#switchport mode access
```

Figure IV.22 Désactivation de la jonction sur les ports d'accès

NB : Nous faisons le même travail sur tous les autres ports d'accès switches S2 et S3.

```
S1(config)#int fa 0/5
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#int fa 0/6
S1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#spanning-tree bpduguard enable
```

Figure IV.23 Activation du PortFast et de la protection BPDU sur les ports d'un Switch

NB : Nous faisons le même travail sur tous les autres switches.

Enfin, nous activons la sécurité de port par défaut de base sur tous les ports d'accès d'utilisateur final en cours d'utilisation. Nous allons utiliser l'option collante et réactiver chaque port d'accès auquel la sécurité du port a été appliquée. (Voir la **figure IV.24**)

```
S1(config)#int fa 0/5
S1(config-if)#sh
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#no sh
S1(config-if)#int fa 0/6
S1(config-if)#sh
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#no sh
```

Figure IV.24 Activation de la sécurité de port par défaut

NB : Nous appliquons la même opération sur les autres switchs.

IV.2.3.9 Vérification de connectivité

a. **Test de la configuration SSH :** A partir du PC-C, nous allons connecter à R3 via Telnet à l'adresse IP (192.168.3.1/24). Nous remarquons que cette connexion est **échouée**, car le routeur R3 est configuré pour accepter uniquement les connexions **SSH** sur les lignes de terminal virtuel. (Voir la **figure IV.25**)

b. Autrement, nous allons entrer la commande « **ssh -l Admin 192.168.3.1 »** pour la connexion à R3 via SSH. Nous remarquons maintenant que la connexion est **réussite**, donc, nous entrons le mot de passe « **Adminpa55 »** configuré pour l'administrateur local. (Voir la **figure IV.25**)

Ensuite, nous tapons la commande « **show ip ssh »** pour voir les paramètres configurés du protocole SSH sur R3. (Voir la **figure IV.26**)

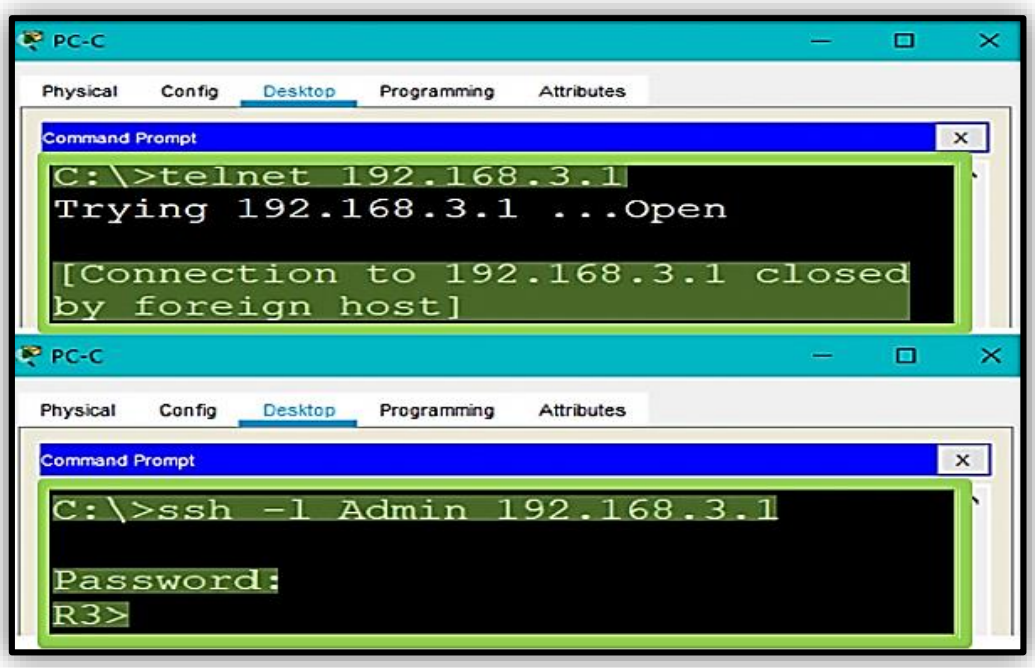


Figure IV.25 Test de la connectivité SSH et Telnet

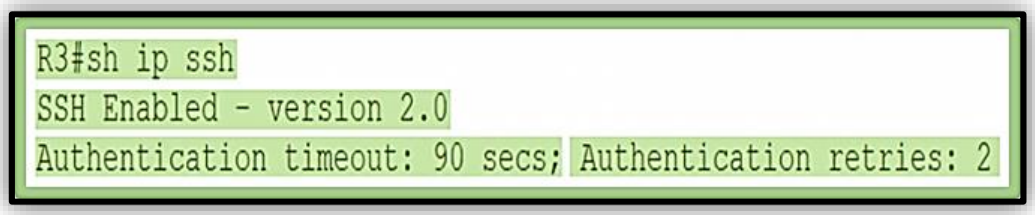


Figure IV.26 Affichage des paramètres SSH configurés

c. **Vérification des horodatages et d'état NTP pour le routeur R1 et le PC–A :** Sur R1, nous tapons la commande **« show clock »** pour vérifier l'heure et la date, puis nous allons rentrer la commande **« show ntp status »** pour le but de voir l'état NTP. (Voir la **figure IV.27**)

d. **Test de pare-feu CBAC sur le routeur R1 :** (Voir la **figure IV.28**)

- A partir du PC-A, nous envoyons une requête Ping vers R2 à (10.2.2.2/30). (Test réussie)
- Une Telnet de PC-A à R2 (10.2.2.2/30). (Connexion réussie)
- A partir du R2, nous envoyons une requête Ping vers PC-A à (192.168.1.3/24). (Test échoué)

e. Test de pare-feu ZPF sur le routeur R3 : (Voir la **figure IV.29**)

- Un Ping de PC-C vers R2 à (10.2.2.2/30). (Test réussie)
- Telnet de PC-C à R2 à (10.2.2.2/30). (Connexion réussie)
- Un Ping de R2 vers PC-C à (192.168.3.5/24). (Test échoué)
- Telnet de R2 à R3 à (10.2.2.1/30). (Test échoué - seul SSH est autorisé)

```
R1#sh clock
16:26:5.850 UTC Mon Jun 22 2020
R1#sh ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 0C6DCEA8.000001D8 (16:26:16.472 UTC lun. juin 22 2020)
clock offset is -2.00 msec, root delay is 0.00  msec
root dispersion is 61.15 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 14 sec ago.
```

Figure IV.27 Vérification des horodatages et d'état NTP

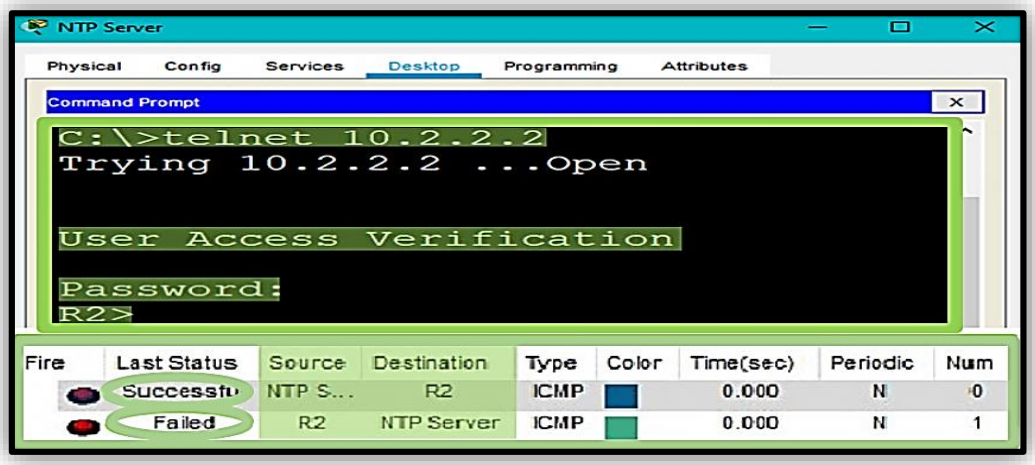


Figure IV.28 Test du pare-feu CBAC

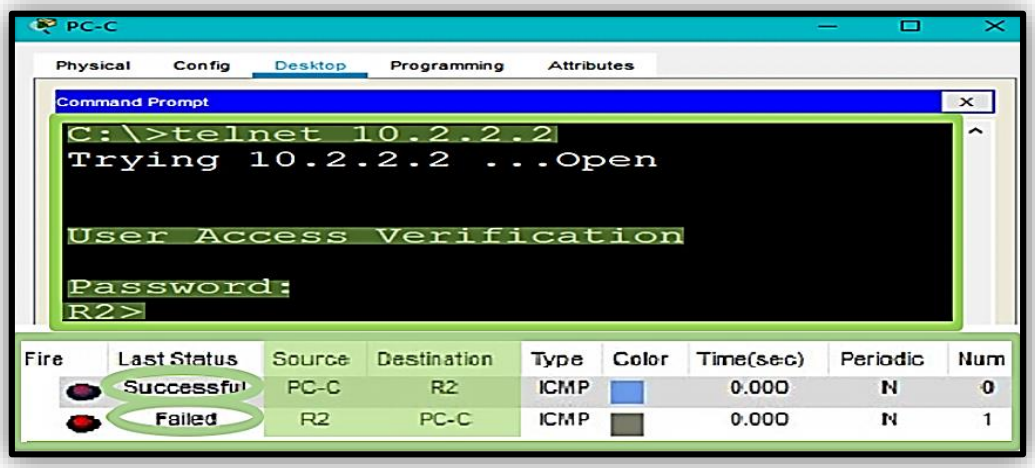


Figure IV.29 Test du pare-feu ZPF

IV.3 Configuration des paramètres d'ASA et du pare-feu avec la sécurité de la couche 2

IV.3.1 Scénario de la configuration simulée

Le réseau d'une entreprise a un emplacement connecté à un FAI. Le routeur R1 représente un appareil CPE géré par le FAI, R2 représente un routeur Internet intermédiaire et R3 représente un FAI qui connecte une administration d'une société d'où le PC-C est l'administrateur de gestion de réseau qui a été embauché pour gérer à distance notre réseau. L'ASA est un périphérique de sécurité CPE de bord qui connecte le réseau d'entreprise interne et la DMZ au FAI tout en fournissant des services NAT et DHCP aux hôtes internes. L'ASA sera configuré pour la gestion par un administrateur sur le réseau interne et par l'administrateur distant. Les interfaces VLAN de couche 3 permettent d'accéder aux trois zones créées dans la configuration : Intérieur, Extérieur et DMZ. L'ISP a attribué l'espace d'adressage IP public de (209.165.200.224/29), qui sera utilisé pour la traduction d'adresse sur l'ASA.

De plus, Le réseau d'une entreprise X est connecté aussi à R2, il y a eu un certain nombre d'attaques sur le réseau récemment. Pour cette raison, l'administrateur réseau a vu que la configuration de sécurité de la couche 2 est une solution pour bloquer ces attaques. Pour des performances et une sécurité optimales, l'administrateur souhaite s'assurer que le pont racine est bien le 3560 Interrupteur central. Pour éviter les attaques de manipulation de spanning-tree, ensuite, il souhaite s'assurer que les paramètres STP sont sécurisés. Outre, l'administrateur réseau veut activer le contrôle des tempêtes pour empêcher les tempêtes de diffusion. Enfin, pour éviter les attaques par débordement de la table d'adresses MAC, le réseau administrateur a décidé de configurer la sécurité des ports pour limiter le nombre d'adresses MAC pouvant être apprises par port de commutateur. Si le nombre d'adresses MAC dépasse la limite définie, l'administrateur souhaite que le port soit arrêté. Tous les périphériques sont préconfigurés avec les éléments suivants :

- Activation du mot de passe : **master_2_telecommunications** ;
- Mot de passe de la console : **reseaux_telecommunications_2020** ;
- Mot de passe de la ligne VTY : **reseaux_telecommunications_2020_vty** ;
- Nom d'utilisateur et mot de passe administrateur : **admin01, 02, 03 / admin01, 02, 03pa55** ;
- Activation du pare-feu ZPF et IPS sur R2.

IV.3.2 Objectifs de la configuration simulée

Cette réalisation a pour le but de :

- Vérifier la connectivité et l'exploration d'ASA ;
- Configurer les paramètres ASA de base et les niveaux de sécurité d'interface à l'aide de la CLI ;
- Configurer le routage, la traduction d'adresses et la politique d'inspection à l'aide de la CLI ;
- Configurer DHCP, AAA et SSH
- Configurer une DMZ, un NAT statique et les ACLs ;
- Configurer un VPN de site à site entre R1 et R3 ;
- Attribuer le commutateur central comme pont racine ;
- Configurer les paramètres de spanning-tree sécurisés pour empêcher les attaques de manipulation STP et activer le contrôle des tempêtes pour éviter les tempêtes diffusées ;
- Activer la sécurité des ports pour empêcher les attaques par débordement de la table d'adresses MAC.

L'objectif de cette configuration simulé est de se protéger contre les virus, les chevaux de troie, les exploits, les attaques scan et les buffers overflow. Et de lutter contre les attaques de type déni de service, vol du mot passe, SYN flood, PING flood, porte dérobée, man in the middle, ARP Spoofing, DHCP Snooping et les attaques STP.

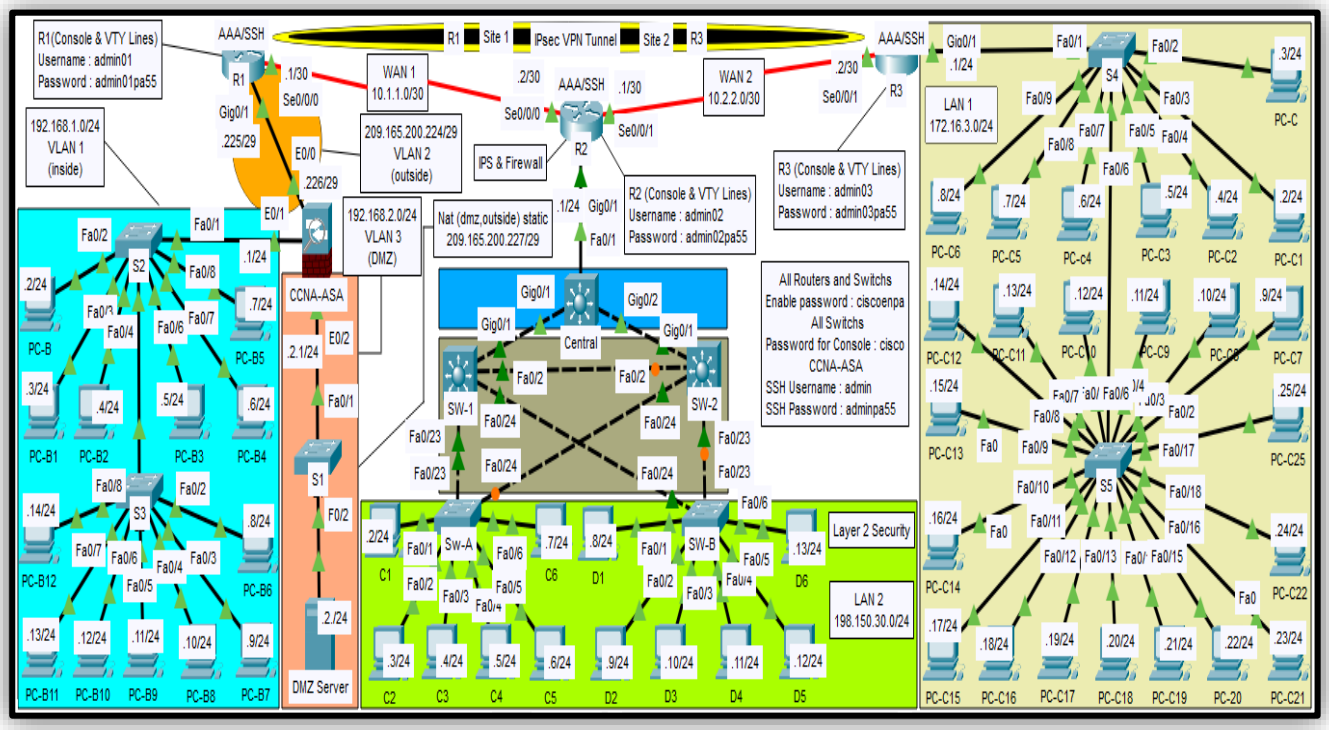


Figure IV.30 Architecture du réseau ASA et du pare-feu avec la sécurité de la couche 2

Les interfaces des différents routeurs des différents sites sont indiquées dans le **tableau IV.2** suivant

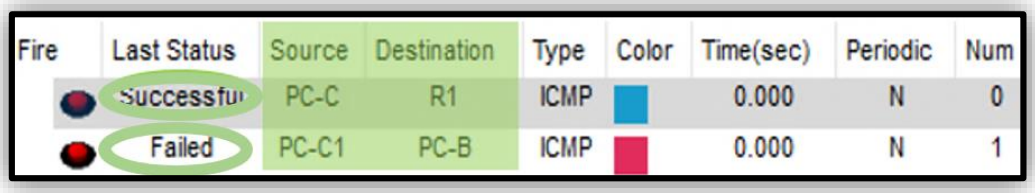
Dispositif	Interface	Adresse IP	Masque	Passerelle
R1	Gig0/1	209.165.200.225	255.255.255.248	N/A
	Se0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Gig0/1	198.150.30.1	255.255.255.0	N/A
	Se0/0/0	10.1.1.2	255.255.255.252	N/A
	Se0/0/1	10.2.2.1	255.255.255.252	N/A
R3	Gig0/1	172.16.3.1	255.255.255.0	N/A
	Se0/0/1	10.2.2.2	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	N/A
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	N/A
DMZ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC-B PC-B12	NIC	192.168.1.2 ... 192.168.1.14	255.255.255.0	192.168.1.1
PC-C PC-C25	NIC	172.16.3.3 .... 172.16.3.25	255.255.255.0	192.168.3.1
C1 ... C6 / D1 ... D6	NIC	198.150.30.2 .... 198.150.30.13	255.255.255.0	198.150.30.1

Tableau IV.2 Table d'adressage du réseau ASA et du pare-feu avec la sécurité de la couche 2

IV.3.3 Mettre en œuvre les paramètres de base ASA et du pare-feu à l'aide de la CLI

IV.3.3.1 Vérification de connectivité et d'exploration d'ASA

a. **Vérification de connectivité :** L'ASA n'est pas actuellement configuré. Cependant, tous les routeurs, PC et serveur DMZ sont configurés. Nous allons vérifier que n'importe machine du réseau (172.16.3.0/24) peut envoyer une requête **Ping** à n'importe quelle interface de routeur. PC-C1 est incapable de cingler l'ASA, le PC-B ou le serveur DMZ.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successfu	PC-C	R1	ICMP		0.000	N	0
	Failed	PC-C1	PC-B	ICMP		0.000	N	1

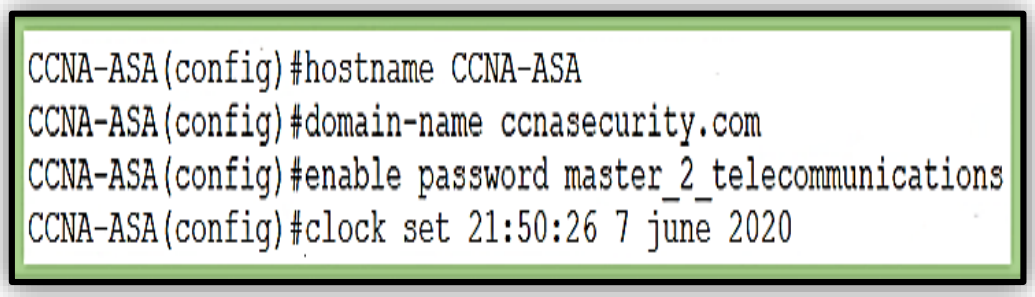
Figure IV.31 Vérification de connectivité

b. **Détermination de la version, les interfaces et la licence ASA :** Nous utilisons la commande **« show version »** pour déterminer divers aspects de ce périphérique ASA.

c. **Détermination du système de fichiers et du contenu de la mémoire flash :** Passant en mode d'exécution privilégié. Lorsque nous sommes invités à entrer un mot de passe, nous appuyons sur « **Entrée ».** Nous tapons la commande « **show file system »** pour afficher le système de fichiers ASA et déterminer les préfixes pris en charge. Ensuite, nous exécutons la commande « **show flash**: » ou « **show disk0**: » pour afficher le contenu de la mémoire flash.

IV.3.3.2 Réglages des paramètres ASA et de la sécurité d'interface

a. **Configuration du nom d'hôte, nom de domaine, mot de passe, date et de l'heure :** Nous allons tout d'abord configurer le nom d'hôte ASA comme « **CCNA-ASA »** et le nom de domaine en tant que « **ccnasecurity.com »**, ensuite, à l'aide de la commande « **enable password** » nous allons configurer un mot de passe « **master_2_telecommunications »** pour le mode d'activation et au final, nous allons régler l'horloge pour régler manuellement la date et l'heure. (Voir la **Figure IV.32**)



```
CCNA-ASA(config)#hostname CCNA-ASA
CCNA-ASA(config)#domain-name ccnasecurity.com
CCNA-ASA(config)#enable password master_2_telecommunications
CCNA-ASA(config)#clock set 21:50:26 7 june 2020
```

Figure IV.32 Configuration du nom d'hôte, nom de domaine, mot de passe et l'horloge

b. **Configuration des interfaces internes et externes :** Pour le moment, nous allons configurer que les interfaces VLAN 1 (intérieur) et VLAN 2 (extérieur). L'interface VLAN 3 (DMZ) sera configurée dans la prochaine partie. Commençons par configurer une interface logique VLAN 1 pour le réseau intérieur (192.168.1.0/24) et définir le niveau de sécurité sur le paramètre le plus élevé de **100**. Ensuite, créer une interface logique VLAN 2 pour le réseau extérieur (209.165.200.224/29) et définir le niveau de sécurité sur le paramètre le plus bas de **0** et activer l'interface VLAN 2.

```
CCNA-ASA(config)#int vlan 1
CCNA-ASA(config-if)#nameif inside
CCNA-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNA-ASA(config-if)#security-level 100

CCNA-ASA(config-if)#int vlan 2
CCNA-ASA(config-if)#nameif outside
CCNA-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
CCNA-ASA(config-if)#security-level 0
```

Figure IV.33 Configuration des interfaces internes et externes

c. **Vérification de notre configuration :** Maintenant, nous utilisons la commande **« show interface ip brief »** pour afficher l'état de toutes les interfaces ASA.

```
CCNA-ASA#sh int ip brief
Interface              IP-Address      OK? Method Status                Protocol

Ethernet0/0            unassigned      YES unset  up                    up

Ethernet0/1            unassigned      YES unset  up                    up

Vlan1                  192.168.1.1     YES manual up                    up

Vlan2                  209.165.200.226 YES manual up                    up
```

Figure IV.34 Affichage d'état des interfaces ASA

Ensuite, nous voulons afficher les informations des interfaces VLAN de la couche 3 en tapant la commande « **show ip address »**. Et pour l'affichage des VLAN intérieurs et extérieurs configurés sur l'ASA et les ports attribués on tape la commande « **show switch vlan »**.

```
CCNA-ASA#sh ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   manual
Vlan2                  outside             209.165.200.226 255.255.255.248 manual

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   manual
Vlan2                  outside             209.165.200.226 255.255.255.248 manual

CCNA-ASA#sh switch vlan

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

Figure IV.35 Vérification des informations des interfaces VLAN

d. Test de connectivité à l'ASA : nous envoyons une requête Ping du PC-B à l'adresse d'interface interne ASA (192.168.1.1/24). (Test réussi)

Outre, toujours à partir du PC-B, nous envoyons une requête Ping à l'interface VLAN 2 (externe) à l'adresse IP (209.165.200.226/29). (Test impossible)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successfu	PC-B	CCNA-ASA	ICMP		0.000	N	0
	Failed	PC-B	R1	ICMP		0.000	N	1

Figure IV.36 Test de connectivité de l'ASA

IV.3.3.3 Configuration de la stratégie de routage, de traduction d'adresses et d'inspection

a. Configuration d'une route par défaut statique pour l'ASA : Nous allons configurer une route statique par défaut sur l'interface extérieure ASA vers l'adresse IP R1 G0/1 (209.165.200.225/29) pour permettre à l'ASA d'atteindre les réseaux externes. Nous allons par la suite émettre la commande « **show route »** pour vérifier que la route par défaut statique est dans la table de routage ASA.

```
CCNA-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNA-ASA(config)#exit

CCNA-ASA#sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
     209.165.200.0/29 is subnetted, 2 subnets
C       209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C       209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
S*   0.0.0.0/0 [1/0] via 209.165.200.225
```

Figure IV.37 Configuration et affichage d'une route par défaut statique pour l'ASA

Après avoir configuré la route statique, nous vérifions si l'ASA peut cingler l'adresse IP (10.1.1.1/30) de R1 S0/0/0 en envoyant un Ping.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	CCNA...	R1	ICMP		0.000	N	0

Figure IV.38 Test de connectivité

b. **Configuration de la traduction d'adresses à l'aide des objets NAT et réseau :** Nous allons créer un objet réseau à l'intérieur du réseau et l'attribuer des attributs à l'aide des commandes « **subnet »** et « **nat »**.

```
CCNA-ASA(config)#object network inside-net
CCNA-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
CCNA-ASA(config-network-object)#nat (inside,outside) dynamic interface
CCNA-ASA(config-network-object)#end
```

Figure IV.39 Configuration de la traduction d'adresses

Ensuite, à partir du PC-B, nous envoyons une requête **Ping** à l'interface G0/1 à l'adresse IP (209.165.200.225/29). (Test échoué)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Failed	PC-B	R1	ICMP		0.000	N	0

Figure IV.40 Test de vérification

c. **Modification de la stratégie globale de service d'inspection d'application MPF par défaut :** Pour l'inspection de la couche d'application et d'autres options avancées, Cisco MPF est disponible sur les ASA. Le périphérique Packet Tracer ASA n'a pas de carte de stratégie MPF en place par défaut. En guise de modification, nous pouvons créer la carte de stratégie par défaut qui effectuera l'inspection sur le trafic intérieur-extérieur. Lorsqu'il est correctement configuré, seul le trafic initié de l'intérieur est autorisé à revenir vers l'interface externe. Pour cela nous devrons ajouter un ICMP à la liste d'inspection. Nous allons créer le **class-map**, le **policy-map** et le **service-policy** et ajouter l'inspection du trafic ICMP à la liste de mappage de stratégies. La figure ci-dessous montre les commandes nécessaires pour cette opération.

```
CCNA-ASA(config)#class-map inspection_default
CCNA-ASA(config-cmap)#match default-inspection-traffic
CCNA-ASA(config-cmap)#exit
CCNA-ASA(config)#policy-map global_policy
CCNA-ASA(config-pmap)#class inspection_default
CCNA-ASA(config-pmap-c)#inspect icmp
CCNA-ASA(config-pmap-c)#exit
CCNA-ASA(config)#service-policy global_policy global
```

Figure IV.41 Modification de la stratégie globale de service d'inspection d'application MPF

A partir de PC-B, nous envoyons une requête Ping à l'interface R1 G0/1 à l'adresse IP (209.165.200.225/29). Cette fois le test est réussi car le trafic ICMP est maintenant inspecté et le trafic de retour légitime est autorisé.

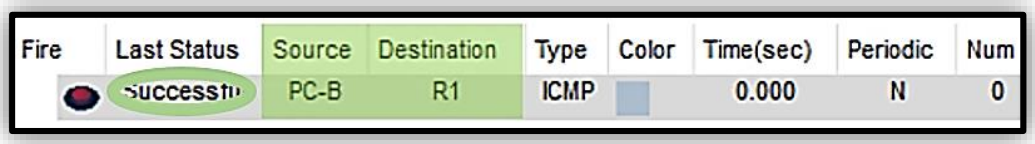


Figure IV.42 Test de vérification

IV.3.3.4 Configuration du DHCP, AAA et SSH

a. **Configuration d'ASA en tant que serveur DHCP :** Au cours de cette partie, nous allons configurer un pool d'adresses DHCP, l'activer sur l'interface intérieure ASA et spécifier l'adresse IP du serveur DNS à donner aux clients. Ensuite, nous allons activer le démon DHCP dans l'ASA pour écouter les demandes de client DHCP sur l'interface activée (à l'intérieur).

```
CCNA-ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
CCNA-ASA(config)#dhcpd dns 209.165.201.2 interface inside
CCNA-ASA(config)#dhcpd enable inside
```

Figure IV.43 Configuration d'ASA en tant que serveur DHCP

A la fin, nous allons remplacer le PC-B d'une adresse IP statique par un client DHCP et vérifier qu'il reçoit les informations d'adressage IP.

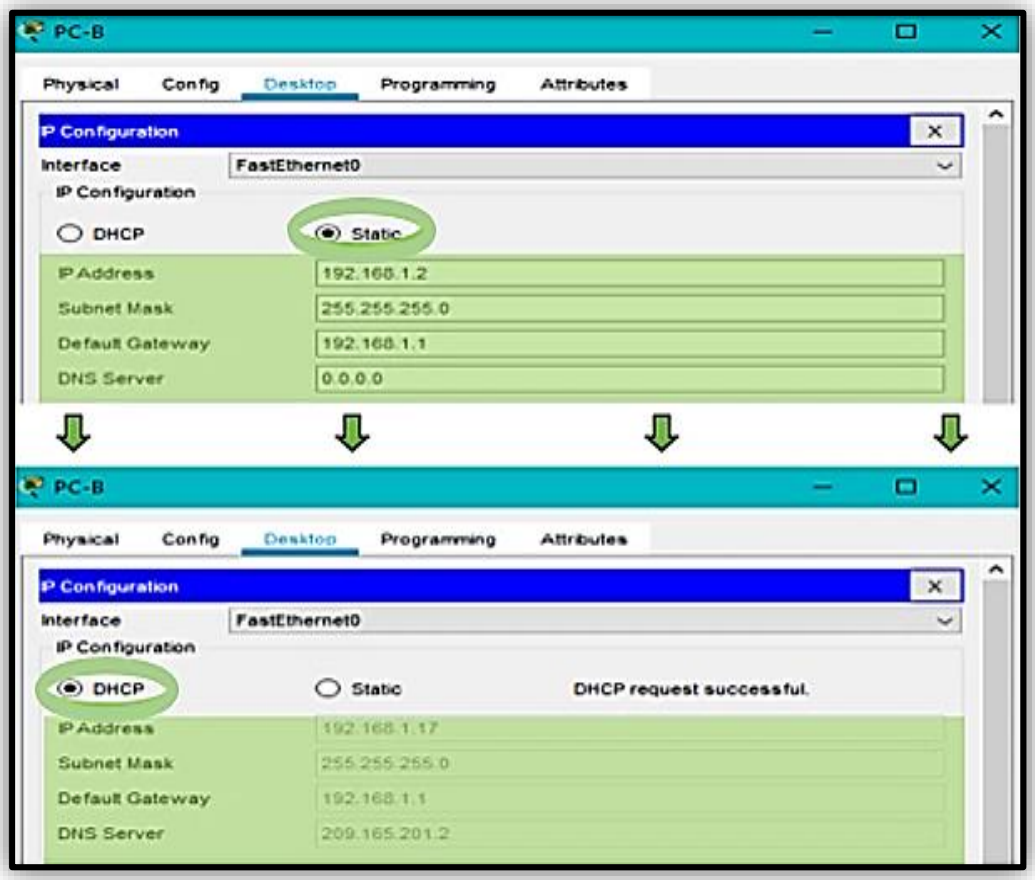


Figure IV.44 Vérification d'une adresse IP statique par une adresse DHCP

b. **Configuration de l'AAA pour utiliser la base de données locale pour l'authentification :** Maintenant, nous allons définir un utilisateur local nommé « **admin »** en entrant la commande **« username »**, nous allons spécifions un mot de passe « **adminpa55 »** et nous configurons configure l'AAA pour utiliser la base de données ASA locale pour l'authentification des utilisateurs SSH.

```
CCNA-ASA(config)#username admin password adminpa55
CCNA-ASA(config)#aaa authentication ssh console LOCAL
```

Figure IV.45 Configuration de l'AAA la base de données locale pour l'authentification

c. **Configuration de l'accès à distance à l'ASA :** Le serveur ASA peut être configuré pour accepter les connexions d'un hôte unique ou d'une gamme d'hôtes sur le réseau intérieur ou extérieur.

Dans cette étape, les hôtes du réseau extérieur peuvent uniquement utiliser SSH pour communiquer avec l'ASA. Les sessions SSH peuvent être utilisées pour accéder à l'ASA depuis le réseau intérieur.

Premièrement, nous allons générer une paire de clés RSA, qui est requise pour prendre en charge les connexions SSH. Parce que le périphérique ASA a déjà des clés RSA en place. (Entrons sur le bouton non lorsque nous sommes invités à les remplacer).

Deuxièmement, nous allons configurer l'ASA pour permettre des connexions SSH de n'importe quel hôte sur le réseau intérieur (192.168.1.0/24) et de l'hôte de gestion à distance à la succursale (172.16.3.3/24) sur le réseau extérieur. En définissant le délai d'expiration SSH sur **10 minutes**.

```
CCNA-ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

```
CCNA-ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
CCNA-ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
CCNA-ASA(config)#ssh timeout 10
```

Figure IV.46 Configuration de l'accès à distance à l'ASA

Finalement, nous allons établir une session SSH du PC-C vers l'ASA (209.165.200.226/29) et du PC-B à l'ASA (192.168.1.1/24).

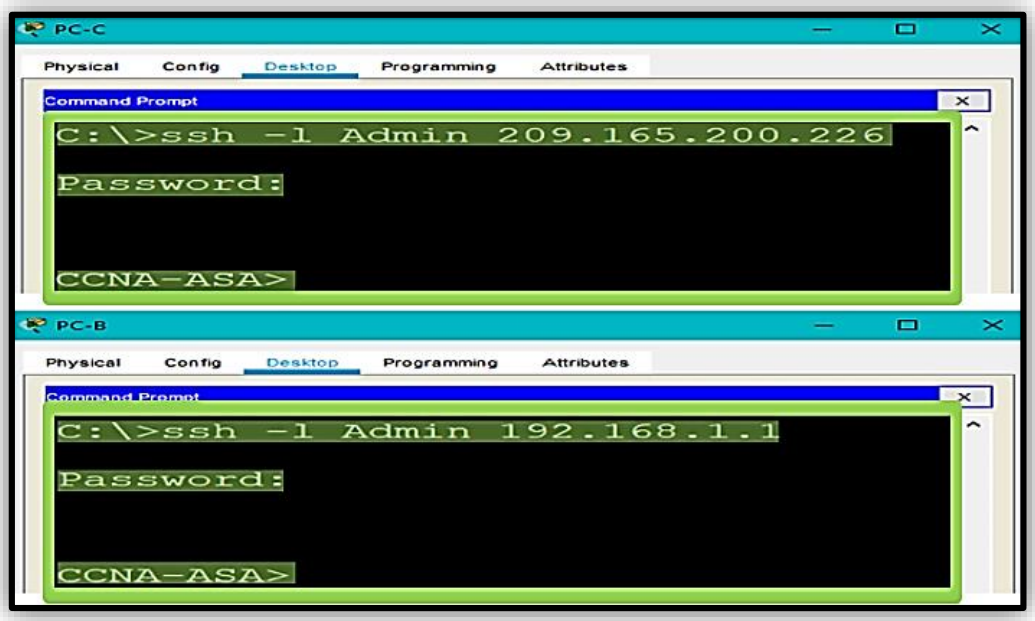


Figure IV.47 Test de vérification SSH

IV.3.3.5 Configuration d'une DMZ, d'un NAT statique et des ACLs

Le routeur R1 G0/1 et l'interface externe ASA utilisent déjà respectivement (209.165.200.225/29) et (209.165.200.226/29). Nous allons utiliser l'adresse publique (209.165.200.227/29) et le NAT statique pour fournir un accès de traduction d'adresse au serveur.

a. **Configuration de l'interface DMZ VLAN 3 sur l'ASA :** Nous allons configurer DMZ VLAN 3, où résidera le serveur Web d'accès public, l'attribuer l'adresse IP (192.168.2.1/24), le nommer DMZ et l'attribuer un niveau de sécurité de **70**.

   Étant donné que le serveur n'a pas besoin d'initier la communication avec les utilisateurs internes, nous désactivons le transfert vers l'interface VLAN 1. Et par la suite, nous allons assigner l'interface physique ASA E0/2 au DMZ VLAN 3 et activer l'interface.

```
CCNA-ASA(config)#int vlan 3
CCNA-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNA-ASA(config-if)#no forward interface vlan 1
CCNA-ASA(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNA-ASA(config-if)#security-level 70
```

```
CCNA-ASA(config-if)#int Ethernet 0/2
CCNA-ASA(config-if)#switchport access vlan 3
```

Figure IV.48 Configuration de l'interface DMZ VLAN 3 sur l'ASA

b. **Configuration du NAT statique sur le serveur DMZ à l'aide d'un objet réseau :** Dans cette étape, nous configurons un objet réseau nommé « **dmz-server »** et l'attribuer l'adresse IP statique du serveur DMZ

(192.168.2.3/24). En mode de définition d'objet, nous allons utiliser la commande « **nat »** pour spécifier que cet objet est utilisé pour traduire une adresse DMZ en une adresse externe à l'aide d'un NAT statique et spécifier une adresse publique traduite de (209.165.200.227/29).

```
CCNA-ASA(config)#object network dmz-server
CCNA-ASA(config-network-object)#host 192.168.2.3
CCNA-ASA(config-network-object)#nat (dmz,outside) static 209.165.200.227
CCNA-ASA(config-network-object)#exit
```

Figure IV.49 Configuration du NAT statique sur le serveur DMZ

c. **Configuration d'une ACL pour autoriser l'accès au serveur DMZ depuis Internet :** Nous allons configurer une liste d'accès nommée « **OUTSIDE-DMZ »** qui autorise le protocole TCP sur le port **80** depuis n'importe quel hôte externe vers l'adresse IP interne du serveur DMZ et appliquer la liste d'accès à l'interface extérieure ASA dans la direction **« IN ».**

```
CCNA-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNA-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNA-ASA(config)#access-group OUTSIDE-DMZ in interface outside
```

Figure IV.50 Configuration d'une ACL pour autoriser l'accès au serveur DMZ depuis Internet

Remarque : Contrairement aux listes de contrôle d'accès IOS, la déclaration d'autorisation ASA ACL doit autoriser l'accès à l'adresse DMZ privée interne. Les hôtes externes accèdent au serveur en utilisant son adresse NAT statique publique, l'ASA le traduit en adresse IP d'hôte interne, puis applique l'ACL.

d. **Test d'accès au serveur DMZ :** Dans cette simulation, la possibilité de tester avec succès l'accès extérieur au serveur Web DMZ n'était pas en place; par conséquent, un test réussi n'est pas nécessaire.

IV.3.4 Configuration du protocole VPN IPsec de site à site

IV.3.4.1 Configuration des paramètres IPsec sur le routeur R1

a. **Identification du trafic intéressant :** Au premier lieu, nous allons configurer une liste ACL **110** pour identifier le trafic du LAN1 sur R1 au LAN 3 sur R3 comme intéressant. Ce trafic intéressant déclenchera la mise en œuvre du VPN IPsec chaque fois qu'il y a du trafic entre les réseaux locaux R1 à R3. Tout autre trafic provenant des réseaux locaux ne sera pas chiffré.

b. **Configuration des propriétés ISAKMP Phase 1 :** Ensuite, à l'aide du tableau des paramètres de stratégie ISAKMP Phase 1 (Voir la **page 109**) nous allons configurer les propriétés de la politique **10** de cryptage ISAKMP sur R1 avec la nouvelle clé de cryptage partagée **« ipsecvpn55 »**.

```
R1(config)#access-list 110 permit ip 209.165.200.224 0.0.0.255 172.16.3.0 0.0.0.255

R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key ipsecvpn55 address 10.2.2.2
```

Figure IV.51 Configuration des propriétés ISAKMP Phase 1

c. **Configuration des propriétés ISAKMP Phase 2 :** Nous allons créer le jeu de transformations « **VPN-SET** » pour utiliser « **esp-aes** » et « **esp-sha-hmac** » et créer par la suite la carte cryptographique **VPNMAP** qui lie tous les paramètres de la phase 5 ensembles. Nous utilisons le numéro de séquence **10** et l'identifier comme une carte « **ipsec-isakmp ».** (Voir la **Figure IV.52**)

Remarque : Nous vérifions que la licence du package Security Technology est activée. Après, nous allons répéter les configurations VPN de site à site sur R3 afin qu'elles reflètent toutes les configurations de R1.

```
R1(config)#access-list 110 permit ip 209.165.200.224 0.0.0.255 172.16.3.0 0.0.0.255

R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key ipsecvpn55 address 10.2.2.2
```

Figure IV.52 Configuration des propriétés ISAKMP Phase 2 et de la carte cryptographique

IV.3.4.2 Sécurisation contre les attaques par connexion

Dans cette tâche, nous allons configurer les paramètres de sécurité pour bloquer les attaques par connexion sur tous les routeurs donc si un utilisateur ne parvient pas à se connecter **trois** fois dans un délai de **60** secondes, les connexions seront désactivées pendant **30** secondes et consignons toutes les tentatives de connexion ayant échoué. (Voir la **Figure IV.52**)

```
R1(config)#login block-for 30 attempts 3 within 60
R1(config)#login on-failure loG
```

Figure IV.53 Sécurisation contre les attaques par connexion

NB : Nous faisons le même travail sur tous les autres routeurs.

IV.3.5 Mettre en œuvre la sécurité de la couche 2

IV.3.5.1 Configuration du pont racine

a. **Détermination du pont racine actuel :** Depuis Central, nous allons exécuter la commande « **show spanning-tree »** pour déterminer le pont racine actuel et pour voir les ports utilisés et leur état. Nous remarquons que le root-bridge (racine) actuel est le commutateur SW-1.

b. **Assignation du Central comme pont racine principal :** En utilisant la commande « **spanning-tree vlan 1 root primary »**, nous allons affecter le commutateur central 3560 comme pont racine.

c. **Assignation du commutateur SW-1 comme pont racine secondaire :** nous allons attribuer le commutateur SW-1 comme pont racine secondaire à l'aide de la commande « **spanning-tree vlan 1 root secondary ».**

```
Central(config)#spanning-tree vlan 1 root primary

SW-1(config)#spanning-tree vlan 1 root secondary
```

Figure IV.54 Configuration du pont racine principal et du pont secondaire

d. **Vérification de la configuration de l'arbre panoramique :** Nous allons émettre la commande **« show spanning-tree »** pour vérifier que le commutateur central 3560 est le pont racine.

```
Central#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00E0.B071.9B31
              This bridge is the root
```

Figure IV.55 Vérification de la configuration de l'arbre panoramique

IV.3.5.2 Protection contre les attaques STP

Au cours de cette partie, nous allons sécuriser les paramètres STP pour empêcher les attaques de manipulation STP.

a. **Activation du PortFast sur tous les ports d'accès :** PortFast est configuré sur les ports d'accès qui se connectent à un seul poste de travail ou serveur pour leur permettre de devenir actif plus rapidement. Sur les ports d'accès connectés des commutateurs SW-A et SW-B, nous utilisons la commande **« spanning-tree portfast ».**

b. **Activation de la protection BPDU sur tous les ports d'accès » :** La protection BPDU est une fonctionnalité qui peut aider à empêcher les commutateurs non autorisés et l'usurpation d'identité sur les ports d'accès. Pour cela, nous allons activer la protection BPDU sur les ports d'accès SW-A et SW-B.

```
SW-A(config)#int range fa 0/1 - 6
SW-A(config-if-range)#spanning-tree portfast
SW-A(config-if-range)#spanning-tree bpduguard enable
```

Figure IV.56 Activation du PortFast et de la protection BPDU

NB : Nous appliquons la même opération sur le commutateur SW-B.

Remarque : Spanning-tree bpduguard peut être activé sur chaque port individuel à l'aide de la commande « **spanning-tree bpduguard enable »**, ou en mode de configuration globale avec la commande « **spanning-tree portfast bpduguard default »**. Dans cette simulation nous avons utilisé la commande « **spanning-tree bpduguard enable »**.

c. **Activation de la protection radiculaire :** La protection racine peut-être activée sur tous les ports d'un commutateur qui ne sont pas des ports racine. Il est préférable de le déployer sur les ports qui se connectent à d'autres commutateurs non root. Nous allons utiliser la commande « **show spanning-tree »** pour déterminer l'emplacement du port racine sur chaque commutateur. Commençant par activer le **root guard** sur les ports Fa0/23 et Fa0/24 du commutateur SW-1.

```
SW-1(config)#int fa 0/23
SW-1(config-if)#spanning-tree guard root
SW-1(config-if)#int fa 0/24
SW-1(config-if)#spanning-tree guard root
```

Figure IV.57 Activation de la protection radiculaire

NB : Nous appliquons la même opération sur le commutateur SW-2.

IV.3.5.3 Activation du contrôle des tempêtes

Maintenant, nous allons activer le contrôle des tempêtes pour les émissions et les diffusions sur tous les ports connectant les commutateurs (ports de jonction), définir un niveau de suppression croissant de **50%** à l'aide de la commande de diffusion **« Storm-Control »** et activer le contrôle des tempêtes sur les interfaces connectant Central, SW-1 et SW-2.

```
SW-1(config)#int giga 0/1
SW-1(config-if)#storm-control broadcast level 50
SW-1(config-if)#int fa 0/2
SW-1(config-if)#storm-control broadcast level 50
SW-1(config-if)#int fa 0/23
SW-1(config-if)#storm-control broadcast level 50
SW-1(config-if)#int fa 0/24
SW-1(config-if)#storm-control broadcast level 50
```

Figure IV.58 Activation du contrôle des tempêtes pour les émissions

NB : Nous appliquons la même opération sur le commutateur SW-2 et le central.

IV.3.5.4 Configuration de la sécurité des ports et de la désactivation des ports inutilisés

a. **Activation de la sécurité des ports de base sur tous les ports connectés aux machines :** Cette procédure doit être effectuée sur tous les ports d'accès sur le commutateur SW-A et SW-B. Nous allons définir le nombre maximum d'appris l'adresse MAC à **2**, permettre à l'adresse MAC d'être apprise dynamiquement et définir la violation à **l'arrêt**.

NB : Un port de commutateur doit être configuré en tant que port d'accès pour activer la sécurité du port.

```
SW-A(config)#int fa 0/1
SW-A(config-if)#switchport mode access
SW-A(config-if)#switchport port-security
SW-A(config-if)#switchport port-security maximum 2
SW-A(config-if)#switchport port-security violation shutdown
SW-A(config-if)#switchport port-security mac-address sticky
```

Figure IV.59 Configuration de la sécurité des ports de base

NB : Nous appliquons la même opération sur le commutateur SW-B.

b. **Vérification de la sécurité du port :** Les ports connectés à d'autres périphériques de commutation et routeurs peuvent et doivent avoir une multitude d'adresses MAC apprises pour ce port unique. La limitation du nombre d'adresses MAC pouvant être apprises sur ces ports peut avoir un impact significatif sur la fonctionnalité réseau. Sur le commutateur SW-A, nous allons émettre la commande « **show port-security** » sur l'interface fa0/1 pour vérifier que la sécurité du port a été configurée.

```
SW-A#sh port-security int fa 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure IV.60 Vérification de la sécurité du port

c. **Désactivation des ports inutilisés :** Dans cette dernière tache, nous désactivons tous les ports actuellement inutilisés pour des raisons d'efficacité.

```
SW-A(config)#int range fa 0/7 - 22
SW-A(config-if-range)#sh
SW-B(config)#int range fa 0/7 - 22
SW-B(config-if-range)#sh
```

Figure IV.61 Désactivation des ports inutilisés

IV.4 Conclusion

Au cours de ce dernier chapitre, nous avons mis en place tous les solutions de sécurité (mécanismes et protocoles) décrits et présentés dans les chapitres précédents pour montrer et prouver la nécessité de la mise en œuvre de politiques de sécurité dans les réseaux Cisco.

Notre but de cette simulation générale qui englobe tous les différents mécanismes et protocoles est d'implémenter une stratégie basée sur un fort plan de sécurité pour la protection contre les menaces et la lutte contre les attaques qui engendrent les réseaux Cisco.

Après nous avons pu décrire la procédure de configuration concernant la mise en place de politiques de sécurité sur les réseaux locaux et les réseaux Internet de l'entreprise ainsi que les résultats de ces configurations. Notre but était d'améliorer et assurer le fonctionnement sécurisé des réseaux configurés donc nous avons atteint notre objectif comme nous avons pu le constatés grâce au captures ci-haut.

Conclusion générale

A travers ce mémoire, nous avons étudié la sécurité informatique qui est quasi-indispensable pour le bon fonctionnement d'un réseau, elle permet de lier la stratégie de sécurité de l'entreprise à sa réalisation opérationnelle. Elle doit être dynamique et remise en question de manière permanente afin de suivre l'évolution des systèmes, de l'environnement et des risques.

Notre projet peut être divisé en trois grands volets, le premier sur une étude de la sécurité informatique qui nous a permis d'exposer un large panorama sur les différentes attaques qui peuvent affecter un réseau informatique, sans oublier les différentes solutions de protection (mécanismes de sécurité), le deuxième est une partie d'installation et d'implémentation dans lequel nous avons fait un petit aperçu sur les différentes topologies et les équipements d'interconnexion des réseaux LANs et la mise en place des solutions de sécurité de ces réseaux. Un dernier volet sur les tests de validation ainsi que l'optimisation de la sécurité et des services.

Au terme de ce travail qui a été réalisé dans le cadre du projet de fin d'étude niveau master au sein du département de Télécommunications au niveau de l'université de TLEMCEN d'où l'option de spécialité est réseaux et Télécommunications, nous pouvons conclure que nous avons acquis des connaissances en termes de configuration dans un environnement « CISCO ». De plus, nous avons enrichi nos connaissances sur le domaine de « Routing & Switching » et avoir une bonne base dans le domaine de sécurité CISCO « ccnasecurity v1, v2 et v3 » grâce à la mise en place de politiques de sécurité.

Dans ce présent projet, nous n'avons fait que des simulations avec le simulateur packet-tracer, Dans l'avenir, nous souhaitons faire une vraie réalisation sur des équipements réels, des équipements matériels afin d'appliquer concrètement ce que nous avons fait au cours de ce mémoire.

Glossaire

A

AAA	**A**uthentication **A**uthorization **A**ccounting
ACL	**A**ccess **C**ontrol **L**ist
ACK	**ACK**nowledgement
AH	**A**uthentication **H**eader
AIM	**A**daptive **I**dentification and **M**itigation
ANSSI	**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
AP	**P**rotocole d'**A**utorisation
ARP	**A**ddress **R**esolution **P**rotocol
AS	**A**dvanced **E**ncryption **S**tandard
ASA	**A**daptive **S**ecurity **A**ppliance

B

BEEP	**B**locks **E**xtensible **E**xchange **P**rotocol
BLP	**B**ell-**La**padula
BPDU	**B**ridge **P**rotocol **D**ata **U**nit

C

CA	**C**ertification **A**uthority
CAM	**C**omputer **A**ided **M**anufacturing
CBAC	**C**ontext-**B**ased **A**ccess **C**ontrol
CD	**C**ompact **D**isc
CERT	**C**omputer **E**mergency **R**eadiness ou **R**esponse **T**eam
CHAP	**C**hallenge-**H**andshake **A**uthentication **P**rotocol
CLF	**C**ommon **L**og **F**ile
CLI	**C**ommand **L**ine **I**nterface
CPE	**C**ustomer-**P**remises **E**quipment
CPU	**C**entral **P**rocessing **U**nit
CRC	**C**ode de **R**edondance **C**yclique

D

DAC	**D**irect **A**ttach **C**opper
DAC	**D**iscretionary **A**ccess **C**ontrol
DCE	**D**ata **C**ircuit **E**quipment
DDoS	**D**istributed **D**enial **o**f **S**ervice
DES	**D**ata **E**ncryption **S**tandard
DH	**D**iffie-**H**ellman

DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DMZ	**D**e**M**ilitarized **Z**one
DNS	**D**omain **N**ame **S**ystem
DTE	**D**omain **T**ype **E**nforcement
DTE	**D**ata **T**erminating **E**quipment
DTP	**D**ynamic **T**runk **P**rotocol
DSA	**D**igital **S**ignature **A**lgorithm
DoS	**D**enial **o**f **S**ervice
DSS	**D**igital **S**ignature **S**tandard

E

EIGRP	**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol
ELF	**E**xecutable and **L**inking **F**ormat
ESP	**E**ncapsulation **S**ecurity **P**ayload

F

FAI	**F**ournisseur d'**A**ccée à **I**nternet
FIPS	**F**ederal **I**nformation **P**rocessing **S**tandard
FTP	**F**ile **T**ransfer **P**rotocol

H

H-IDS	**H**ost-**B**ased **I**ntrusions **D**etection **S**ystem
HMAC	**k**eyed-hash **M**essage **A**uthentication **C**ode
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol

I

IBAC	**I**dentity **B**ased **A**ccess **C**ontrol
IBM	**I**nternational **B**usiness **M**achines
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
ID	**ID**entifiant
IDEA	**I**nternational **D**ata **E**ncryption **A**lgorithm
IDS	**I**nternational **D**ata **C**orporation
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IEEE	**I**nstitute of **E**lectrical and **E**lectronic **E**ngineers
IOS	**I**nternetwork **O**perating **S**ystem
IP	**I**nternet **P**rotocol
IPS	**I**ntrusion **P**revention **S**ystem
IPsec	**I**nternet **P**rotocol **Sec**urity
IPX	**I**nternetwork **P**acket **E**xchange
ISAKMP	**I**nternet **S**ecurity **A**ssociation and **k**ey **M**anagement **P**rotocol
ISP	**I**nternet **S**ervice **P**rovider

L

LAN	**L**ocal **A**rea **N**etwork
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
L2F	**L**ayer **T**wo **F**orwarding
L2TP	**L**ayer **2** **T**unneling **P**rotocol

M

MAC	**M**andatory **A**ccess **C**ontrol
MD5	**M**essage **D**igest **5**
MPF	**M**odular **P**olicy **F**rame-work

N

NAT	**N**etwork **A**ddress **T**ranslation
NBS	**N**etwork **B**ased **S**ervices
N-IDS	**N**etwork-**B**ased **I**ntrusions **D**etection **S**ystem
N-IPS	**N**etwork **I**ntrusion **P**revention **S**ystem
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NSA	**N**ational **S**ecurity **A**gency
NTP	**N**etwork **T**ime **P**rotocol
NVRam	**N**on **V**olatile **R**am

O

OS	**O**perating **S**ystem
OSI	**O**pen **S**ystems **I**nterconnection
OSPF	**O**pen **S**hortest **P**ath **F**irst
OVH	**O**les **V**an **H**erman

P

PAP	**P**assword **A**uthentication **P**rotocol
PC	**P**ersonal **C**omputer
PDMA	**P**erte de **D**onnées **M**aximale **A**dmissible
PDU	**P**rotocol **D**ata **U**nit
Ping	**P**acket **In**ternet **g**roper
PME	**P**etites et **M**oyennes **E**ntreprises
PMI	**P**etites et **M**oyennes **I**ndustries
PPP	**P**oint to **P**oint **P**rotocol
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol

Q

QoS	**Q**uality **o**f **S**ervice

R

RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
RAM	**R**andom **A**ccess **M**emory
R-BAC	**R**ole-**B**ased **A**ccess **C**ontrol
RC4	**R**ivest **C**ipher **4**
RC5	**R**ivest **C**ipher **5**
RIP	**R**outage **I**nformation **P**rotocol
ROM	**R**ead **O**nly **M**emory
RPC	**R**emote **P**rocedure **C**all
RSA	**R**ivest, **S**hamir & **A**dleman
RTC	**R**éseau **T**éléphonique **C**ommuté

S

SA	**S**ecurity **A**ssociation
SHA-1	**S**ecure **H**ash **A**lgorithm-**1**
SI	**S**ystème d'**I**nformation
SIS	**S**ociété d'**I**nformatique et de **S**ystème
SMSI	**S**ystème de **M**anagement de la **S**écurité de **l'I**nformation
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SSH	**S**ecure **Sh**ell
SSI	**S**écurité du **S**ystème d'**I**nformation
SSL	**S**ecure **S**ockets **L**ayer
SSTP	**S**ecure **S**ocket **T**unneling **P**rotocol
STP	**S**panning **T**ree **P**rotocol
SYN	**Syn**chronize

T

TACACS	**T**erminal **A**ccess **C**ontroller **Ac**cess **C**ontrol **S**ystem
TCP	**T**ransmission **C**ontrol **P**rotocol
Telnet	**Tel**ecommunication **net**work
TLS	**T**ransport **L**ayer **S**ecurity

U

UDP	**U**ser **D**atagram **P**rotocol
URL	**U**niform **R**esource **L**ocator

V

VLAN	**V**irtuel **L**ocal **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork
VTY	**V**irtuel **T**eletype

W

WAN	**W**ide **A**rea **N**etwork
WEP	**W**ired **E**quivalent **P**rivacy
WIFI	**Wi**reless **Fi**delity
WPA	**W**iFi **P**rotected **A**ccess
WWW	**W**orld **W**ide **W**eb

X

XOR	e**X**clusive **OR**

Z

ZPF	**Z**one-Based **P**olicy **F**ire-wall

Bibliographie

[1] TOUATI Azeddine, « Détection d'intrusions dans les réseaux LAN: Installation et configuration de l'IDS-SNORT », Mémoire de Master professionnel en Informatique, Université A /Mira de Bejaïa, 2016.

[2] BORDJAH Dahia & BOUDJADI Amel, « Audit et définition d'une politique de sécurité. Cas d'étude SONATRACH DP », Mémoire de Master en Informatique, Université Abderrahmane Mira de Béjaïa, 2013.

[3] Adnane EL KABBAL, « Un système de type pour l'analyse des pare-feu », Mémoire en vue de l'obtention de grade de Maitre (es) Science (M.Sc.), Université de Québec, 2005.

[4] Aicha TEKKOUK, « Etude et Implémentation d'une méthode cryptanalyse pour le chiffrement continu », Mémoire de Master en Informatique, Université d'Oran, 2010.

[5] BAHAZ Salma & MAMMERI Tidjani, « Déploiement d'une solution Anti-virus au sein du réseau de campus universitaire de Ouargla », Mémoire de Master Professionnel, Université Kasdi Merbah Ouargla, 2015.

[6] Laurent Poinsot, « Introduction à la sécurité informatique », Support de cours, Université Paris 13.

[7] BOUNOUNI Sara & MECHEROUH Katia, « Simulation d'un pare-feu d'entreprise Cas de SONATRACH de Béjaïa », Mémoire de Master professionnel en Informatique, Université A/Mira de Béjaïa, 2016.

[8] Le grand livre de la sécurité informatique, « SecuriteInfo », Editions du 6 nouvembre 2006.

[9] BOUSALAH Malika & TIFOUR Yamina, « Contribution à la conception d'un crypto système symétrique flexible sur circuit FPGA », Mémoire de Master en Systèmes Informatiques, Université M'HAMED BOUGARA de BOUMERDES, 2016.

[10] Mahdi Hamza, « Etude et Comparaison des principaux systèmes de cryptage et les techniques y afférentes », Mémoire de Master en Informatique, Université MOHAMED BOUDIAF M'SILA, 2016.

[11] ALI Kheirr-dinne Mouhamed, « Etude et implémentation d'une solution de sécurisation des communications par SSL/TLS », Mémoire de Master en Réseaux Mobiles et Services de Télécommunications, Université de Tlemcen,2015.

[12] Houda HAFI, « Protocole pour la sécurité des réseaux sans fil peer to peer », Mémoire de magister en Informatique, Université Kasdi Merbah Ouargla,2014.

[13] SLIMANOU Dehia, « Mise en place d'une solution VPN sur pare feu; Cas d'étude : Entreprise Tchin-Lait(Candia) », Mémoire de master Professionnel en informatique », Université Abderrahmane Mira Béjaïa, 2016.

[14] ADDAD Nesrine, « La mise au point d'un antivirus », Mémoire de Master en Informatique, Université Abou Bakr Belkaid – Tlemcen, 2015.

[15] HADAOUI Rebiha, « Un IDS basé sur un algorithme inspiré du fonctionnement de colonies des fourmis », Mémoire de magister en Informatique, Université M'hamed BOUGARA de Boumerdes, 2008.

[16] Ahmim Marwa, « Etude du protocole IPSec et métriques de sécurité », Thèse en vue de l'obtention du diplôme de Doctorat 3ème cycle informatique, Université BADJI Mokhetar Annaba, 2016.

[17] MAJDA MOUSSA, « Vérification et Configurations Automatiques de PARE-FEUX par Model CHECKING et Synthèse de Contrôleur », Mémoire en vue de l'obtention du diplôme de Maitrise en Sciences Appliqués / Génie Informatique, Université de Montréal, 2014.

[18] Basma Mezni, « Etude et développement d'une plateforme d'analyse des fichiers logs » Rapport du Projet de Fin d'études pour l'obtention du diplôme de Mastère Professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR), Université Virtuelle de Tunis, 2014.

[19] Djerbaoui Imad Eddine & Herrouz Hichem, « Exploration des traces de navigation sur le Web », Mémoire de Master Académique en Informatique, Université KASDI Merbah OUARGLA, 2015.

[20] Abdelmajid LAKBABI, « Contrôle d'Accès Réseau de Nouvelle Génération Convergence vers un Ecosystème de Sécurité », Thèse de Doctorat en Informatique, Université Mohammed V faculté des sciences Rabat MAROC, 2017.

[21] Lionel GUILLET, « Pour maitriser les risques dans vos activités : IL FAUT TOUJOURS AVOIR UN BON PLAN … DE SAUVEGARDE », Livre , www.bcp-expert.com, 2012.

[22] La Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) & l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé), **«** Règles de sauvegarde des Systèmes d'Information de Santé (SIS) », Guide Pratique, France, 2014.

[23] Adiel A. AKPLOGAN (Ingénieur Réseau − Directeur des NTIC)**, «** LA SECURITE DES RESEAUX », 2002.

[24] GUIDE DE L'UTILISATEUR, « Acronis Backup 12.5 / Update 4 », 2003-2019.

[25] BOUKHATEM Mohammed Belkaid, « Application des techniques de cryptage pour la transmission sécurisée d'images MSG », Mémoire e de Magister en Electronique, Université MOULOUD MAMMERI TIZI-OUZOU, 2015.

[26] Abbes RHARRAB, « Audit Sécurité des Systèmes d'Information », Mémoire de Projet de Fin d'Etudes LICENCE PROFESSIONNELLE Administration de Systèmes Informatiques, Université Mohammed V Agdal Rabat MAROC, 2012.

[27] BELALIA Mohamed cherif & MAACHE Khaled, « Etude et Conception d'un Firewall », Mémoire de Master en Réseaux et Télécommunications, Université SAAD DAHLEB de BLIDA, 2011.

[28] BOUFOUDI Sihem & BRAHAMI Nabila, « La sécurité des Réseaux Informatique à Base de Kerberos », Mémoire de Master professionnel en Informatique, Université de BEJAIA, 2015.

[29] Sourour JEMILI, « Analyse de risque dans les systèmes de contrôle d'accès », Mémoire en vue de l'obtention du diplôme de Maitrise en Informatique, Université de QUEBEC en OUTAOUAIS / Laboratoire de Recherche en Sécurité, 2013.

[30] SI-AHEMED Ayoub & SI-AHMED Idris, « Conception et Réalisation d'un Système de Gestion et d'Analyse de LOGS », Mémoire de Master en Sécurité des Systèmes d'Information, Université SAAD DAHLAB BLIDA 1, 2019.

[31] AINENNAS Faiza & ZIDI Nassima, « Contrôle d'accès aux services sensibles au contexte », Mémoire de Master en Informatique, Université Abderahman Mira de Béjaia, 2015.

[32] YACINE CHALLAL, « Pare-feux : Translation, Filtrage, Mandataires et Détection d'Intrusions », Cours, 2014.

[33] DAHMANE Zouhir & ABDELLI Lyamine, « Implémentation d'un algorithme de cryptage sur un circuit FPGA », Mémoire de Master Electronique, Université Mohamed Boudiaf - M'sila, 2017.

[34] BEN HMIDA Slah, « Etude, Conception et implémentation d'une architecteur réseau sécurisée et un cloud privé », Mémoire de Stage de Fin d'Etudes en vue de l'obtention du Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR), Université Virtuelle de TUNIS, 2017.

[35] Djedjiga BENZID, « Le Réseau Privé Virtuel (VPN) sur les Réseaux Maillés Sans Fil WMN », Mémoire en vue de l'obtention Maitrise en Génie Concentration Réseaux de Télécommunication, École de TECHNOLOGIE SUPÉRIEURE, Université du QUÉBEC, 2014.

[36] ALLAL Nadjib & EL BLIDI Othmene, « Détection de l'utilisation du Réseau Tor dans une entreprise », Mémoire de Master en Électronique, Université SAAD DAHLAB de BLIDA, 2018.

[37] Pascal Bou Nassar, « Gestion de la sécurité dans une infrastructure de services dynamique : Une approche par gestion des risques », Thèse de Doctorat, L'institut national des sciences appliquées (INSA) de Lyon - France, 2012.

[38] BENDELLA Zineb, « Gestion de la sécurité d'une application Web à l'aide d'un IDS comportemental optimisé par l'algorithme des K-means », Mémoire de Master en Informatique, Université de Tlemcen, 2013.

[39] Réseaux LPSIL ADMIN, « Présentation et utilisation de Packet Tracer », IUT Nice Côte d'Azur, 2012/2013.

[40] KACED Kahina & KHELILI Yasmina, « Etude sur la technologie MSAN et Réalisation d'une plate-forme VoIP simulée à base de la solution Vlan et le protocole DHCP », Mémoire de master académique en Réseaux et Télécommunication, Université MOULOUD MAMMERI TIZI-OUZOU, 2015.

Webographie

[W1] http://blog.octo.com/syn-flood/, Consulté le 27/03/2020

[W2] https://www.securiteinfo.com/attaques/hacking/ddos.shtml, Consulté le 01/04/2020

[W3] https://blog.eleven-labs.com/fr/comprendre-le-ssltls-partie-4-handshake-protocol/, Consulté le 03/04/2020

[W4] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203445-certificat-ssl-certificat-secure-socket-layer-definition-traduction-et-acteurs/, Consulté le 05/03/2020

[W5] https://www.geektech.fr/reseaux/cisco-packet-tracer-presentation-generale/, Consulté le 19/02/2020

[W6] https://www.institut-numerique.org/partie-2-etude-et-configuration-des-routeurs-cisco 51dbb79874cca, Consulté le /04/2020 , Consulté le 01/05/2020

[W7] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203337-serveur informatique-définition-traduction/, Consulté le 24/04/2020

[W8] https://www.cisco.com/c/dam/global/fr/assets/documents/pdfs/guides/Cisco_ASA5500, Consulté le 14/08/2020

[W9] http://www.marche-public.fr/Terminologie/Entrees/ordinateur-bureau.htm, Consulté le 15/03/2020

[W10] https://www.linternaute.fr/dictionnaire/fr/definition/laptop/, Consulté le 24/04/2020

[W11] http://millysu.e-monsite.com/blog/centre-de-donees-et-cloud/definition-du-cable-sfp-10-gigabits-ethernet-types-guide-de-deploiement.html, Consulté le 22/06/2020

[W12] https://msm-medias.com/dvd/n10/sources/reseaux/Recherche/C%C3%A2bles%20droit%20et%20croi s%C3%A9.pdf, Consulté le 02/07/2020

[W13] https://reussirsonccna.fr/se-connecter-a-un-equipement-cisco-en-console/, Consulté le 05/07/2020

[W14] https://waytolearnx.com/2018/07/difference-entre-dte-et-dce.html, Consulté le 16/05/2020

Dieu Merci