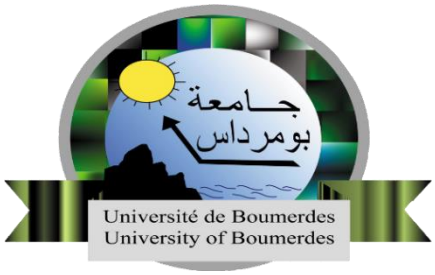
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE MINISTERE DE L'ENSEIGNEMENT SUPPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE M'HAMED BOUGARA



FACULTE DES SCIENCES

Domaine : Sciences et Technologie (ST)

Département de Génie Electrique

Spécialité : Réseaux et Télécommunications

Master 2

Mémoire de fin d'études en vue de l'obtention du diplôme de Master en Réseaux et Télécommunications

Simulation de Firewall ASA en vue de réaliser un réseau informatique sécurisé

Présenté par :

Mr OUARAB Yanis

Membres de jury :

Président : Mr GANA Massine

Examinateur : Mr TRIKI Yacine

Encadré par :

Mr DAFEUR Abdelhakim

Juillet 2024

Dédicaces

Je dédie ce modeste travail à :

Mes chers parents pour leurs encouragements et soutien qui ont cru en moi jusqu'au bout

Mes sœurs et toute ma famille.

«Votre affection et votre soutien m'ont été d'un grand réconfort tout au long de mon parcours.

Je vous remercie du fond du cœur d'être toujours à mes côtés et de me donner cette force pour continuer.

Je vous dédie ce travail en signe de reconnaissance».

Sans oublier mes amis.

Remerciements

Je tiens à remercier l'ensemble des enseignants qui ont contribué à ma formation universitaire et toutes les personnes qui m'ont aidé de près ou de loin à l'élaboration de ce mémoire.

En particulier à mon encadreur Mr DAFEUR, pour sa patience, sa disponibilité et surtout à ses judicieux conseils, qui ont contribué à alimenter ce projet tout au long de son élaboration.

Je remercie également les membres des jurys qui seront présent lors de ma présentation et qui me font l'honneur d'examiner mon travail.

TABLE DES MATIERES

INTRODUCTION GENERALE

Dans le domaine des télécommunications, nous nous intéressons à un espace bien défini : celui des communications numériques. Il s'agit des échanges d'informations déjà numérisées, qu'elles proviennent de données informatiques (d'origine digitale) ou qu'elles aient été échantillonnées et quantifiées préalablement (par exemple, un fichier vidéo compressé avant d'être stocké).

Les réseaux informatiques ont vu le jour pour relier des terminaux distants à un site central, puis pour connecter des ordinateurs entre eux, et enfin pour relier des machines terminales telles que des stations de travail ou des serveurs.

Pour protéger les réseaux informatiques, il existe plusieurs méthodes et outils essentiels. Parmi les plus courants, on retrouve les antivirus, qui détectent et éliminent les logiciels malveillants ; les réseaux privés virtuels (VPN), qui assurent une connexion sécurisée et anonyme sur Internet ; les pare-feu (Firewall), qui filtrent le trafic entrant et sortant pour empêcher les accès non autorisés ; et les réseaux locaux virtuels (VLAN), qui segmentent les réseaux pour améliorer la sécurité et la gestion. Bien que ces solutions soient toutes cruciales pour une protection efficace, notre mémoire se concentrera principalement sur les pare-feu. En effet, ces dispositifs jouent un rôle central dans la défense périmétrique des réseaux, empêchant les attaques potentielles et régulant le flux de données. Nous explorerons en profondeur les différents types de pare-feu, leurs mécanismes de fonctionnement, ainsi que les meilleures pratiques pour leur configuration et gestion.

Enfin, nous conclurons avec une simulation pratique d'un réseau informatique à l'aide de l'outil Packet Tracer. Ce logiciel nous permettra de créer un réseau virtuel réaliste, où nous pourrons tester et illustrer les concepts théoriques abordés. Nous montrerons comment sécuriser ce réseau en y intégrant un pare-feu, en détaillant toutes les configurations nécessaires pour une protection optimale. Cette étape pratique démontrera non seulement l'importance des pare-feu dans la sécurisation des réseaux, mais aussi la manière de les implémenter efficacement dans un environnement simulé. Par cette simulation, nous mettrons en évidence les avantages et les défis associés à l'utilisation des pare-feu, offrant ainsi une perspective complète et appliquée de leur rôle dans la cybersécurité.

CHAPITRE 1

Sécurité des réseaux informatiques

1.1 Introduction

La sécurité informatique est essentielle afin de garantir la confidentialité et la sauvegarde de données au sein de l'organisation.

La sécurité informatique est l'ensemble des moyens (méthodes, techniques et outils) mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces de l'internet Dans ce chapitre, nous allons présenter les concepts de base du réseau informatique et puis, nous allons détailler les bases de la sécurité informatique.

1.2 Définition d'un réseau informatique

Un réseau informatique relie différents équipements tels que des ordinateurs et des périphériques en utilisant des supports de communication comme les réseaux filaires ou sans fil. Ces réseaux permettent l'accès à internet, aux e-mails et aux documents partagés, ainsi que la collaboration entre utilisateurs.

On classe généralement les réseaux informatiques en deux catégories : les réseaux locaux (LAN) et les réseaux étendus (WAN).

1.3 Types de réseaux

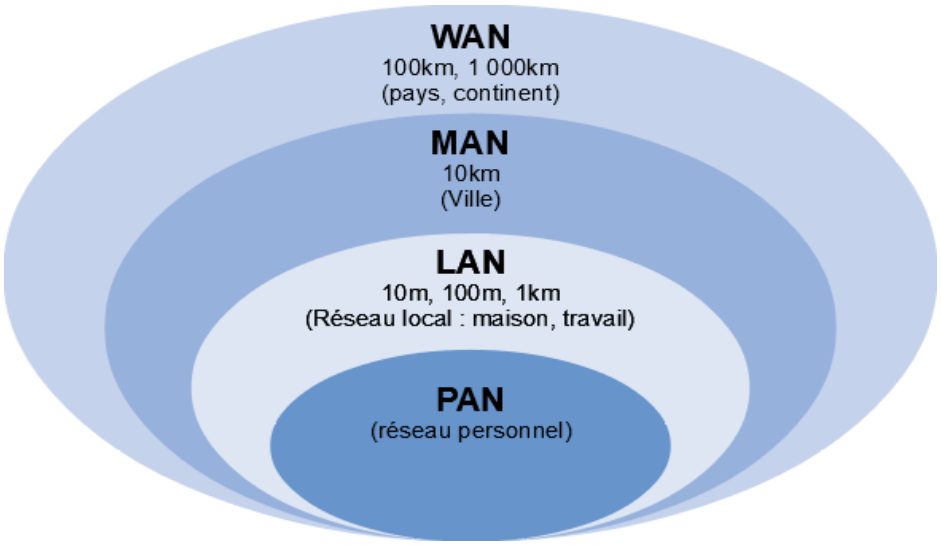


Figure 3: les différents types de réseaux

- **Les PAN (Personal Area Network)**

Ce type de réseau relie des périphériques tels que les terminaux GSM, portables, organiseurs, Bluetooth, etc., d'un même utilisateur. Il concerne les réseaux sans fil d'une faible portée, de l'ordre de quelques dizaines de mètres.

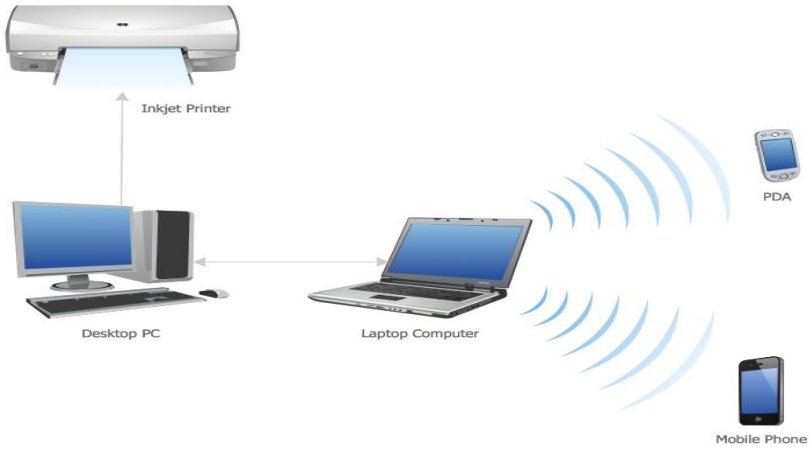


Figure 4: réseau PAN

- **Réseau LAN (Local Area Network en français Réseau Local)**

Un **réseau** local est un **réseau** compris au sein d'une petite zone géographique, généralement à l'intérieur d'un même bâtiment. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie, la plus répandue étant Ethernet.

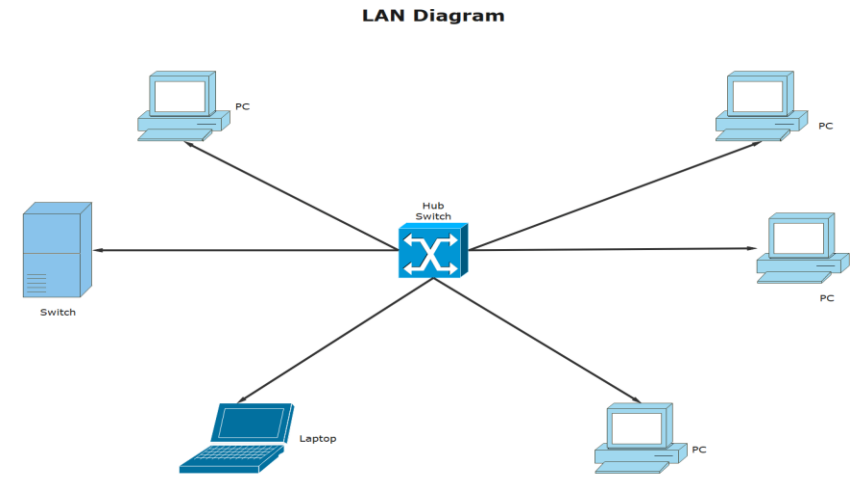


Figure 5 : réseau LAN

- **Réseau MAN (Métropolitain Area Network)**

Ce type de réseau permet d'interconnecter plusieurs LAN géographiquement proches à une portée de quelques dizaines de km au maximum à des débits importants. Un réseau MAN permet aussi à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est généralement composée de commutateurs ou de routeurs interconnectés par des liens hauts débits, en général en fibre optique.

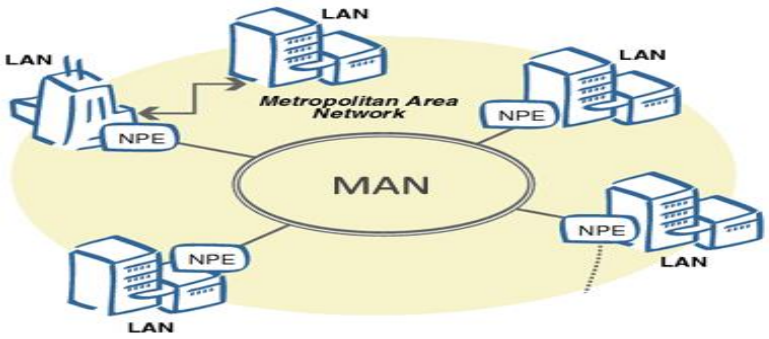


Figure 6 : réseau MAN

- **Réseau WAN (Wide Area Network ou réseau étendu)**

Un réseau WAN relie plusieurs LAN et MAN. Les WAN fonctionnent grâce à des routeurs qui relient les différents réseaux et permettent de sélectionner le trajet le plus approprié pour atteindre un nœud de destination. Le réseau WAN le plus connu est l'internet.

Figure 7 : réseau WAN

1.4 Les modèles de service

Nous avons compris qu'un réseau permet la connexion entre eux, mais les besoins sont très divers, d'un tout petit réseau ou entreprise jusqu'à un grand réseau.

Les réseaux peuvent être organisés selon deux principes, les réseaux **post à post** et réseaux **client/serveur**.

- **Réseau points à points « Peer to Peer »**

Cette architecture est en fait un réseau sans serveur constitué de deux ou plusieurs ordinateurs. Les ressources sont donc libres de partage ou non.

Les postes de travail sont simplement relies entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes.

C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attitré.

Dans l'exemple, chaque poste peut partager tout ou partie de sa mémoire de masse, le poste peut partager son imprimante.

Figure 1 : réseaux Peer to Peer P2P

Avantages	Inconvénients
✓ Il est facile de mettre en réseau des postes qui étaient au départ isolés. ✓ Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes. ✓ Dans un groupe de travail, l'imprimante peut être utilisée par tous. ✓ Cette méthode est pratique et peu coûteuse pour créer un réseau domestique	✓ Chaque utilisateur a la responsabilité du fonctionnement du réseau. ✓ Les outils de sécurité sont très limités. ✓ Si un poste est éteint ou s'il se "plante" ses ressources ne sont plus accessibles. ✓ Le système devient ingérable lorsque le nombre de postes augmente. ✓ Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer.

- **Réseau client/serveur**

L'architecture client/serveur désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs postes clients du serveur : chaque logiciel client peut envoyer des requêtes à un serveur.

Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique.

Des programmes qui accèdent au serveur sont appelés programmes clients (client FTP, client mail, … etc)

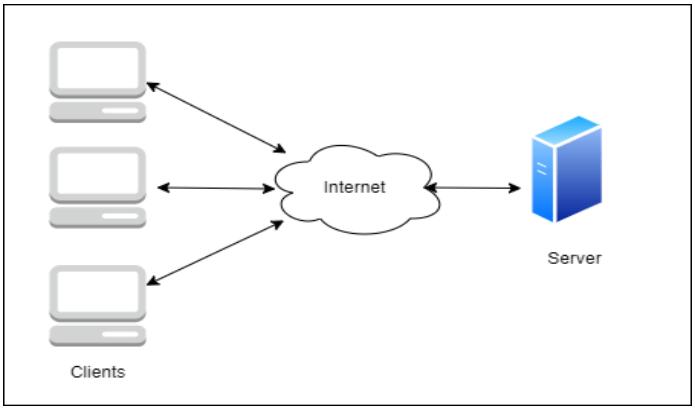


Figure 2 : réseau client serveur

Avantages

- ✓ Les serveurs sont conçus pour le partage de ressources et ne servent pas de station de travail. Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptibles de s'y connecter.
- ✓ Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "peer to peer".
- ✓ Ils proposent également des fonctions avancées à l'usage des utilisateurs comme par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.
- ✓ Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre.
- ✓ Les serveurs étant toujours en service (sauf en cas de panne...), les ressources sont toujours disponibles pour les utilisateurs

Inconvénients

- ✓ La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste".
- ✓ Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
- ✓ Le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.
- ✓ On peut distinguer différent types de réseaux selon plusieurs critères tels que (la taille de réseau, sa vitesse de transfert des données et aussi leur entendu)

1.5 Périphérique d'interconnexion

Les interconnexions de réseaux peuvent être locales : réseaux situés dans un même emplacement géographique. Dans ce cas, un équipement standard (répéteur, routeur, etc.) suffit à créer physiquement la connexion. Les interconnexions peuvent également impliquer des réseaux distants. Ces réseaux doivent ensuite être connectés via une connexion téléphonique (modem).

1.5.1 Les multiplexeurs (MUX)

Un multiplexeur est un dispositif électronique qui rassemble et organise diverses connexions, telles que celles utilisées pour l'informatique, la télécopie, la téléphonie et le télétex, sur un seul canal de transmission. Il fonctionne comme un chef d'orchestre, coordonnant une multitude de signaux pour produire une symphonie numérique harmonieuse et sans accroc.

1.5.2 Les concentrateurs (Hub)

Le hub, agissant comme un répéteur, joue un rôle essentiel dans le maintien de la connexion en transmettant les données entrantes à tous les éléments du réseau tout en les régénérant simultanément.

1.5.3 Les commutateurs (Switch)

En fonctionnant au niveau de la couche 2 OSI, ces tables de routage sont construites sur la base d'adresses MAC, permettant la connexion de différents composants tout en divisant efficacement le réseau.

1.5.4 Les ponts (Bridge)

Les appareils OSI niveau 2 permettent des connexions au même réseau (en utilisant les mêmes protocoles et en ayant des méthodes d'accès similaires). Ils permettent de filtrer les trames entre les segments à l'aide de la table de mappage port/adresse MAC de la station.

1.5.5 Les répéteurs (Repeater)

Un répéteur est un appareil simple utilisé pour régénérer les signaux entre deux nœuds de réseau afin d'étendre la distance de câble d'un réseau. Les répéteurs, quant à eux, peuvent créer une interface entre deux types différents de supports physiques.

1.5.6 Les passerelles (Gateway)

Il s'agit de systèmes matériels et/ou logiciels capables de se connecter à un réseau en utilisant différents protocoles. Une passerelle convertit les protocoles de communication en les convertissant d'un protocole à un autre (agissant comme un traducteur ou un convertisseur de formats de trames et de services).

1.5.7 Les routeurs (Router)

Les routeurs, fonctionnant au niveau de la couche 3 du modèle OSI, jouent un rôle essentiel en dirigeant efficacement le flux de données sur divers réseaux. En prenant des décisions logiques de manière stratégique, ils déterminent le chemin optimal pour la transmission des données. Afin

de connecter plusieurs réseaux, un routeur doit posséder une adresse IP pour chaque réseau IP qu'il interconnecte, ce qui le rend multi-hébergé. Ces appareils sont équipés à la fois d'interfaces réseau et de logiciels qui exécutent des fonctions de routage essentielles telles que le filtrage, la traduction d'adresses et la protection par pare-feu. [1].

1.6 Les Topologies physique d'un réseau

On distingue deux types de topologies « physique et logique ». La topologie physique est la manière dont le réseau est disposé. La topologie logique concerne la manière dont le support de transmission, par exemple un câble, est accessible aux ordinateurs connectés au réseau [2].

1.6.1 La topologie en Bus

Dans ce type de la topologie, les informations circulent dans le câble central. Il s'étend sur toute la longueur du réseau et les machines viennent s'y accrocher. Quand une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois.

Figure 8 : Topologie bus.

1.6.2 La topologie en étoile

C'est la topologie la plus utilise dans les réseaux informatique. Les stations sont reliées à un composant central généralement a un concentrateur ou routeur.

Ce type de réseau est facile à mettre en place et la panne d'une station ne met pas en cause la panne du réseau.

Figure 9 : Topologie étoile

1.6.3 La topologie en anneau

Dans la topologie en anneau, Les informations circulent de station en station, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin.

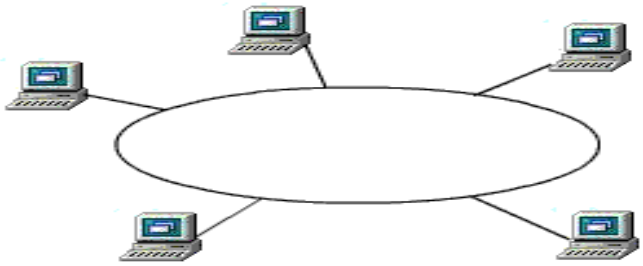


Figure 10 : Topologie Anneau.

1.7 Les architectures de réseaux

1.7.1 Modèles de référence OSI et TCP/IP

On utilise souvent un modèle sous forme de couches, tel que le modèle OSI et TCP/IP pour aider à visualiser l'interaction entre les différents protocoles. Ce modèle illustre le fonctionnement des protocoles intervenant dans chaque couche, ainsi que leur interaction avec les couches supérieures et inférieures. L'idée était que cet ensemble de protocoles serait utilisé pour développer un réseau international qui ne dépendrait pas de systèmes propriétaires.

- Le modèle de protocole TCP/IP (modèle Internet) définit quatre catégories de fonctions qui doivent intervenir pour que les communications aboutissent. Les principaux points communs entre les deux modèles de réseau se situent aux couches OSI 3 et 4.

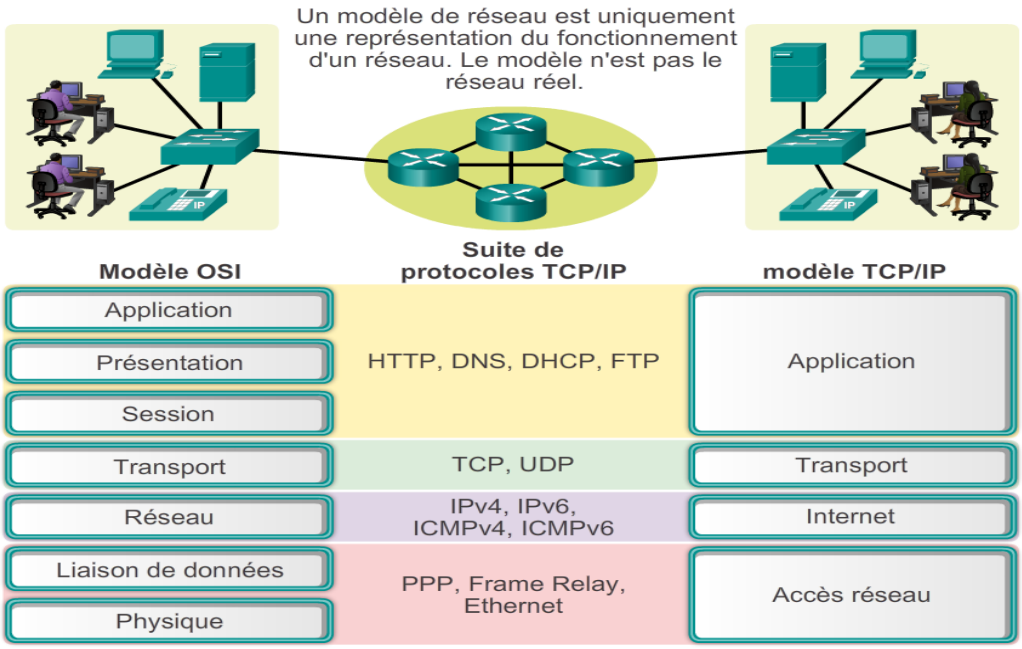


Figure 11: les modèles OSI et TCP/IP

- **Encapsulation :** lorsque les données d'application descendent la pile de protocoles en vue de leur transmission sur le support réseau, différents protocoles ajoutent des informations à chaque niveau. C'est ce qu'on appelle **l'encapsulation**. La forme que prend une donnée sur n'importe quelle couche est appelée **unité de données de protocole**. L'encapsulation de données est le processus qui ajoute aux données des informations d'en-tête de protocole supplémentaires avant leur transmission.
- **Segmentation :** La meilleure approche consiste à diviser les données en parties de taille moins importante et plus facilement gérables pour les envoyer sur le réseau. Cette division du flux de données en parties plus petites est appelée segmentation. La segmentation peut augmenter la fiabilité des communications réseau. Les différentes parties de chaque message n'ont pas besoin de parcourir le même chemin sur le réseau depuis la source jusqu'à la destination. Si une partie du message ne parvient pas à sa destination, seules les parties manquantes doivent être transmises à nouveau.
- **Unités de données de protocole (PDU) :** La forme que prend une donnée sur n'importe quelle couche est appelée unité de données de protocole.

- **La désencapsulation** : la désencapsulation est le processus utilisé par un périphérique récepteur pour supprimer un ou plusieurs des en-têtes de protocole.

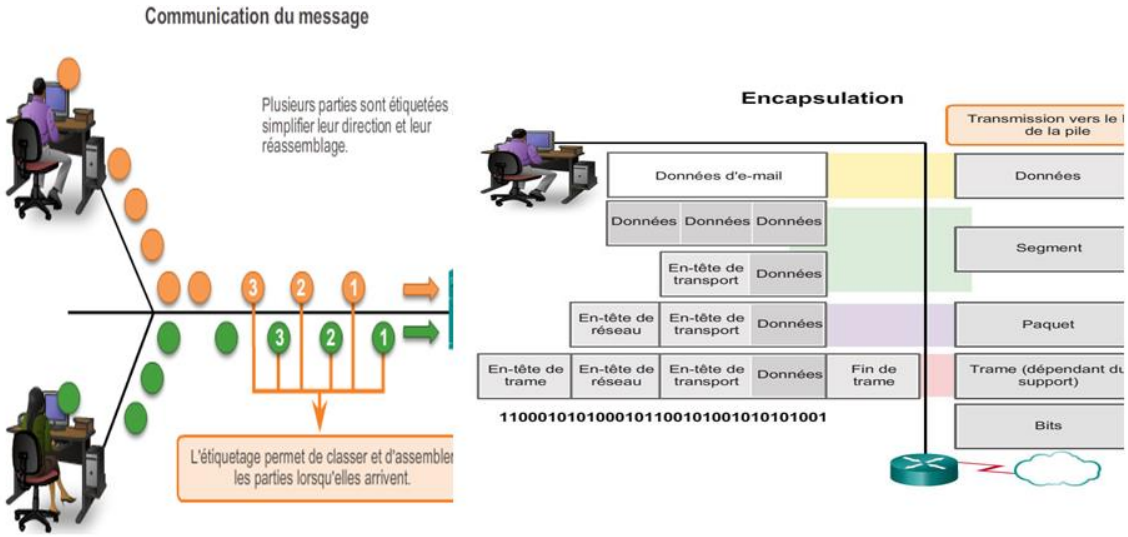


Figure 12 : segmentation et encapsulation des données

1.7.1.1 La couche physique

La couche physique contient les règles et procédures à mettre en œuvre pour acheminer les éléments binaires sur le medium physique. On trouve dans la couche physique les équipements réseau qui traitent l'élément binaire, comme les modems, concentrateurs, ponts, hubs, etc.

Les différentes topologies de support physique affectent le comportement de la couche physique. Dans les entreprises les palans de câblages ont une importance parfois déterminante pour le reste de l'architecture. La couche physique nécessite de surcroit un matériel fiable, et il faut parfois dupliquer ou mailler le réseau pour obtenir des taux de défaillances acceptables.

1.7.1.2 La couche liaison

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de donnes entre les entités du réseau.

Cette couche détecte et corrige, quand cela est possible, les erreurs de la coche physique et signale à la couche réseau les erreurs irrécupérables.

1.7.1.3 La couche réseau

Cette couche assure toutes les fonctionnalités de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche liaison pour préparer le travail de la couche transport.

1.7.1.4 La couche transport

Cette douche définit un transfert de données entre les entités en les déchargeant des détails d'exécution (contrôle entre l'OSI et le support de transmission).

Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche session.

1.7.1.5 La couche session

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données. Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

1.7.1.6 La couche présentation

Cette couche assure la transparence du format des données à la couche application, elle garantit que les communications en transit présentent une forme adaptée au destinataire. Par exemple, un programme de la couche présentation peut formater une demande de transfert de fichiers en code binaire afin que le transfert de ces fichiers aboutisse.

1.7.1.7 La couche application

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisables par l'application (transfert e données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

1.8 Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens (méthodes, techniques et outils) mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces de l'internet [3].

La sécurité a pour objectif d'assurer les propriétés suivantes :

- **La confidentialité** : L'information ne sera divulguée ou révélée qu'aux personnes autorisées.
- **L'authentification** : L'authentification assure que seules les entités autorisées ont accès au système.
- **L'intégrité** : L'information contenue dans les objets ne sera ni altérée, ni détruite de manière non autorisée.
- **La disponibilité** : L'accès par un sujet autorisé aux ressources et informations du système doit être toujours possible

- **Non répudiation** : La propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

1.9 Les attaques réseaux informatiques

Les entreprises craignent les attaques informatiques, sans toujours savoir quelles formes celles-ci peuvent prendre. Pour créer des solutions de sécurité des réseaux, il faut tout d'abord évaluer l'ensemble des attaques existantes et comprendre leur mode de fonctionnement. Ces attaques sont variées, mais on peut les catégoriser selon leur mode d'opération :

1.9.1 Attaques de reconnaissance

La reconnaissance est la découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou encore la découverte de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque. Parmi les attaques courantes de ce type, nous citons:

- **Requêtes internet** : l'assaillant peut utiliser des outils d'internet, comme les outils nslookup et whois, pour découvrir facilement les adresses IP attribuées à une entreprise ou à une entité donnée;
- **Balayages ping** : Une fois ces adresses IP connues, l'assaillant peut lancer des requêtes ICMP de type ping vers les adresses IP publiquement accessibles pour déterminer celles qui sont actives. Certains outils de balayage existent comme fping ou gping, permettant d'envoyer systématiquement des requêtes ping à une plage d'adresses ou à toutes les adresses d'un sous-réseau. Cette approche est similaire à celle qui consiste à utiliser un annuaire téléphonique et à appeler tous les numéros pour savoir qui répond.
- **Balayages de ports** : Lorsque les adresses IP actives sont identifiées, l'assaillant se sert d'un outil de balayage des ports pour détecter les services réseau ou les ports ouverts sur chaque adresse IP active. Nmap et Superscan sont des exemples d'outils de balayage conçus pour détecter les ports ouverts sur un hôte du réseau. Concrètement, l'outil de balayage interroge les ports pour connaître le type et la version des applications, le type et la version du système d'exploitation, etc. Grâce à ces informations, l'assaillant peut déterminer s'il existe des vulnérabilités qu'il peut exploiter.

- **Analyse des paquets** : L'assaillant peut aussi intercepter les paquets TCP/IP ou les paquets des autres protocoles et décoder leur contenu au moyen d'un analyseur de protocole comme Wireshark. Une fois les paquets interceptés, ils peuvent être analysés pour y rechercher des informations vulnérables. Afin de neutraliser l'analyse des paquets, il est conseillé de :
  - ✓ Utiliser des commutateurs au lieu de concentrateurs pour éviter de diffuser le trafic à tous les hôtes du réseau.
  - ✓ Utiliser une méthode de chiffrement adéquate au système qui ne consomme pas beaucoup de ressources.
  - ✓ Interdire l'utilisation de protocoles susceptibles d'être écoutés, comme le protocole SNMP.

1.9.2 Attaques d'accès

L'accès au système est la possibilité pour un assaillant d'accéder à un périphérique pour lequel il ne dispose pas d'autorisation, c'est-à-dire un compte ou un mot de passe. La pénétration non autorisée dans un système implique généralement l'utilisation d'un moyen hardware de piratage, d'un script ou d'un outil exploitant une vulnérabilité connue de ce système. Les attaques d'accès exploitent des vulnérabilités connues dans les services d'authentification, les services FTP et les services Web. On distingue quatre types d'attaques:

- **Attaques de mot de passe** : Pour obtenir le mot de passe d'un utilisateur, l'assaillant peut lancer différents types d'attaques :
  - ✓ Des attaques par force brute qui consistent à lancer plusieurs tentatives répétées de connexion à une ressource partagée, comme un serveur ou un routeur, afin d'identifier un compte utilisateur et/ou un mot de passe, en utilisant généralement des outils tels que L0phtCrack ou Cain.
  - ✓ Des analyses de paquets permettant de capter les comptes et les mots de passe utilisateurs transmis en clair, en utilisant des outils tels que Wireshark ou Cain.
  - ✓ Des programmes de type cheval de Troie pouvant sniffer la saisie des mots de passe sur la machine de l'utilisateur.
- **Exploitation de la confiance** : Elle consiste à compromettre un hôte de confiance et ensuite à travers ce dernier lancer des attaques sur d'autres hôtes du réseau. Par exemple,

dans le réseau d'une entreprise, si un hôte interne (protégé par un pare-feu) est accessible depuis un hôte de confiance externe (situé de l'autre côté du pare-feu), l'hôte interne peut être attaqué par le biais de l'hôte externe.

- **Redirection de port** : Cette attaque de type exploitation de la confiance consiste à utiliser un hôte compromis pour faire passer, au travers d'un pare-feu, un trafic qui serait normalement bloqué. Ce type d'attaque est principalement limité par l'utilisation de modèles de confiance appropriés. Le rôle d'un antivirus, installé sur un hôte, est de détecter et d'empêcher toute installation d'utilitaires de redirection de port sur cet hôte.
- **Attaque de l'homme du milieu (man-in-the-middle)** : Cette attaque est menée par un assaillant qui se place entre deux machines légitimes d'un réseau. Le déroulement des échanges pourrait être comme suit :
  - ✓ La victime demande une page Web du site Web légitime, mais la machine de cette victime la demande auprès de la machine de l'assaillant.
  - ✓ La machine de l'assaillant reçoit la demande et récupère la page du site Web d'origine.
  - ✓ En cas d'une attaque active, l'assaillant modifie la page d'origine et la transforme à sa façon les données qu'elle contient
  - ✓ L'assaillant envoie la page demandée falsifiée à la victime.

1.9.3 Attaques par déni de service (DoS)

L'attaque par déni de service (DoS) apparaît lorsqu'un assaillant désactive ou altère un réseau, des systèmes ou des services dans le but de refuser le service prévu aux utilisateurs normaux. Les attaques par DoS mettent le système en panne ou le ralentissent au point de le rendre indisponible et inutilisable, en empêchant l'utilisation d'un service par les personnes autorisées en raison de l'épuisement des ressources du système. C'est pour cette raison que les attaques par DoS sont les plus redoutées. Dans la plupart des cas, l'attaque se résume à exécuter un programme pirate ou un script.

Il existe plusieurs types d'attaques de DoS, parmi lesquelles :

- **Attaques par ping fatal** : Autrefois, elles profitaient des vulnérabilités des anciens systèmes d'exploitation (années 90). L'assaillant modifiait la partie IP de l'en-tête d'un paquet ping pour indiquer une quantité de données supérieure à la quantité réelle du

- paquet. En effet, un paquet ping contient normalement de 64 à 84 octets, tandis qu'un ping fatal peut atteindre 65 535 octets. Donc, l'envoi d'un ping de cette taille peut bloquer un hôte cible d'ancienne génération. La plupart des réseaux ne sont actuellement plus vulnérables à ce type d'attaque.
- **Attaques par inondation SYN (SYN Flooding)** : Sachant qu'une connexion TCP (handshake) suit trois étapes, une attaque par inondation SYN consiste à envoyer un grand nombre de requêtes SYN (plus de 1000) au serveur ciblé. Ce dernier répond par le message SYN-ACK habituel, mais l'hôte malveillant ne répond jamais par un message ACK final pour achever la procédure de connexion. Étant donné que ces connexions semi-ouvertes consomment des ressources mémoires, au bout d'un certain temps, le serveur est saturé et ne peut plus accepter de connexions car il se met dans un état d'attente infinie par manque de ressources pour répondre aux requêtes SYN valides
- **Attaques DDoS (Distributed DoS)** : Ce type d'attaques est conçu pour saturer le réseau de données illégitimes, qui submergent la liaison Internet au point d'empêcher tout trafic légitime. Les attaques DDoS s'appuient sur des méthodes similaires aux deux autres attaques DoS, mais elles se déploient toutefois à une plus grande échelle.

En général, des centaines ou des milliers de points d'attaque tentent de submerger une cible. Pour saturer le réseau victime, le principe est d'utiliser plusieurs sources pour l'attaque et des maîtres (masters) qui les contrôlent. L'assaillant utilise des maîtres pour contrôler plus facilement les sources. En effet, il a besoin de se connecter (en TCP) aux maîtres pour configurer et préparer l'attaque. Les maîtres se contentent d'envoyer des commandes aux sources en UDP. Les outils de type DDoS les plus connus sont Tribal Flood Network (TFN), TFN2K, Trinoo, Stacheldraht, etc.

1.9.4 Attaques de programmes malveillants (malware)

Il s'agit des programmes logiciels malveillants qui est installé sur une machine hôte dans le but d'endommager un système ou d'empêcher l'accès aux services de ce dernier.

Ces programmes essayent souvent de se reproduire et de se propager dont le but de causer des dégâts pour le réseau informatique, tels que :

1. **Gêne** : affiche des publicités, ralentit ou plante le système.
2. **Espionnage** : vole les mots de passe et les informations bancaires, ou envoie des documents sensibles.

3. **Contrôle d'une machine** : la machine infectée devient un zombie contrôlé par l'assaillant, et généralement enrôlée dans un botnet (robot network).

Un programme de ce type peut être :

- **Un virus** : C'est un programme malveillant intégré à un autre programme, afin d'exécuter des fonctions indésirables sur la machine de l'utilisateur. Il a besoin d'un mécanisme de livraison, comme une archive (zip, ...) ou un fichier exécutable joint à un e-mail, pour transmettre son code d'un système à un autre. Donc, il ne peut pas se reproduire sans l'aide d'un programme cible. Il Le virus se distingue fondamentalement du ver par le fait qu'une interaction humaine est nécessaire pour le propager. Cette propagation s'effectue principalement en trois phases : infection, activation, et duplication. Les types de virus sont :
  - **Virus parasite** : s'attaque aux codes source des fichiers exécutables et se réplique en exécutant ces derniers, en cherchant s'il y a d'autres fichiers exécutables à infecter.
  - **Virus résidant en mémoire** : hébergé en mémoire et considéré comme un programme du système, il infecte tous les programmes qui s'exécutent.
  - **Virus sur secteur de Boot (Boot Sector Virus)** : infecte le secteur de boot du disque, et se propage lorsque le système d'exploitation démarre.
- **Un ver (worm)** : exécute un code et installe des copies de lui-même dans la mémoire de la machine infectée, ce qui infecte par la suite d'autres machines hôtes. En effet, contrairement à un virus, il est autonome et se duplique à travers un réseau, par exemple: Code Red et Blaster. Les différentes phases de l'attaque d'un ver sont :
  - **Activation de la vulnérabilité** : un ver s'installe en exploitant les vulnérabilités connues d'un système, comme les utilisateurs naïfs qui exécutent sans vérification un fichier exécutable joint à un e-mail.
  - **Mécanisme de propagation** : l'accès à l'hôte étant acquis, le ver s'y reproduit, puis choisit d'autres cibles.
  - **Charge** : une fois l'hôte infecté par un ver, l'assaillant peut y accéder en tant qu'utilisateur privilégié. Il peut utiliser une faille locale pour augmenter son niveau de privilège jusqu'à celui de l'administrateur.

- **Un cheval de Troie (trojan)** est un programme malveillant conçu pour ressembler à une application normale et utile, alors qu'il s'agit d'un instrument d'attaque. Concrètement, c'est un code non autorisé placé dans un programme sain, ce qui le rend difficile à détecter. De plus, les fonctions non attendues d'un cheval de Troie ne s'exécutent qu'après une longue phase de sommeil. Par ailleurs, les chevaux de Troie peuvent être des attaques informatives, des attaques de DoS ou des attaques destructrices. Comme exemple, le cheval de Troie courant "Sub7" consiste à installer une porte dérobée sur la machine des utilisateurs. Il est utilisé d'une part, en tant que menace non organisée, où les assaillants inexpérimentés peuvent l'utiliser pour faire disparaître les pointeurs de souris. D'autre part, il peut être utilisé comme une menace organisée, permettant aux assaillants d'installer un enregistreur de frappes pour capturer la saisie des informations confidentielles.
- **Un logiciel espion (espiogiciel ou spyware)** est un logiciel ou un composant d'un logiciel qui permet de collecter des informations sur l'utilisateur d'une machine sur lequel il est installé afin de les envoyer vers son concepteur. Le concepteur d'un spyware peut être, par exemple, une société qui le diffuse pour lui permettre de dresser le profil des internautes. Il n'est en principe pas destiné à endommager une machine mais plutôt conçu pour le recueil de certaines informations sensibles ou non. On distingue généralement deux types de spywares:
  - **Spywares internes (ou intégrés)** comportant directement des lignes de codes dédiées aux fonctions de collecte de données.
  - **Spywares externes** correspondant à des programmes de collecte autonomes installés. Par exemples : Alexa, Doubleclick, NewDotNet, Flashpoint/ Flashtrack, Realplayer, SaveNow, WebHancer, etc.

Le défi de la sécurité des réseaux auquel les administrateurs réseau doivent faire face est de trouver un juste équilibre entre deux exigences importantes : garder une certaine ouverture pour permettre la prise en charge des opportunités de commerce évolutives ; et protéger les données privées et personnelles, ainsi que les données stratégiques des entreprises contre les différentes attaques.

1.10 Outils de la Sécurité des Réseaux Informatiques

10.1 1. Les antivirus

Les logiciels antivirus servent de protection contre diverses infections informatiques, notamment les virus, dans le but principal de protéger les machines. Néanmoins, des distinctions peuvent être trouvées entre ces logiciels, principalement en termes de gamme de fonctionnalités, de leur exécution et des techniques utilisées pour identifier les anomalies.

1.10.2 VPN (Réseau virtuel privé)

Un réseau privé virtuel (VPN) est un terme général qui fait référence à une communication réseau qui utilise diverses technologies pour établir une connexion sécurisée via un réseau autrement non sécurisé. Les protocoles de tunneling sont utilisés au niveau de la couche deux ou de la couche trois du modèle OSI. Les protocoles de tunneling les plus répandus incluent SSL, IPsec, PPTP et L2TP. En encapsulant un paquet contenant une adresse IP privée dans un paquet avec une adresse IP unique au monde, il devient possible d'étendre un réseau privé sur internet.

1.10.3 Cryptographie

La cryptographie englobe diverses méthodes utilisées pour modifier les données, assurer leur dissimulation, les protéger contre les altérations non autorisées ou les utilisations abusives. Grâce à ce processus, du texte crypté est généré, accessible uniquement à ceux qui possèdent les clés de cryptage, qui peuvent ensuite effectuer des transformations inverses ou des algorithmes de décryptage. La cryptographie garantit non seulement la confidentialité des données, mais garantit également leur intégrité et leur authenticité.

1.10.4 VLAN (Virtual Local Area Network)

Un réseau local virtuel (VLAN) est un regroupement logique de périphériques connectés au même réseau, quel que soit leur emplacement physique. Essentiellement, un VLAN permet la segmentation et le contrôle du trafic réseau. Chaque VLAN fonctionne comme un réseau virtuel indépendant, même s'il partage la même infrastructure physique avec d'autres VLAN. Les VLAN offrent plusieurs avantages, notamment une conception simple, une sécurité améliorée, une gestion efficace du trafic et une rentabilité. Par exemple, au sein d'une organisation, un VLAN peut séparer efficacement le trafic en fonction des utilisateurs individuels, de leurs rôles ou de caractéristiques spécifiques du trafic. De plus, les VLAN permettent le partage du câblage physique tout en garantissant que les appareils ne peuvent pas communiquer directement entre eux.

1.10.5 Pare feu (Firewall)

Un pare-feu ou pare-feu est un périphérique physique (matériel) ou logique (logiciel) utilisé comme système de protection pour les ordinateurs personnels. Il peut également être utilisé comme interface Un ou plusieurs réseaux d'entreprise qui contrôlent et éventuellement bloquent les flux de données en analysant les informations qu'ils contiennent (séparation réseau). Autrement dit, il bloque ou autorise toutes sortes de trafic entrant et sortant.

1.10.6 Système de détection d'intrusion (IDS)

La détection d'intrusion est la surveillance et l'analyse continues des événements survenant au sein d'un système informatique ou réseau afin d'identifier toute tentative de compromettre la sécurité du système. Ces intrusions peuvent prendre la forme d'un accès non autorisé via internet, d'utilisateurs autorisés tentant d'obtenir des privilèges non autorisés ou d'utilisateurs autorisés abusant des privilèges qui leur sont accordés. Un système de détection d'intrusion, qu'il soit sous forme logicielle ou matérielle, automatise les processus de surveillance et d'analyse. Son objectif est de protéger la confidentialité, l'intégrité, la disponibilité et les mécanismes d'évitement de l'ordinateur ou du système réseau.

1.11 Conclusion

Dans ce chapitre, nous avons citez les différents types de réseau informatique et présenter le modèle OSI et TCP/IP. Ensuite, nous avons focalisé sur les notions de base de la sécurité informatique et les moyens mise en ouvrent afin de limiter ces attaques.

Dans le chapitre suivant, nous allons étudier le pare-feu et son utilité dans un réseau informatique.

CHAPITRE 2

Firewall

2.1 Introduction

Un pare-feu informatique est nécessaire pour s'assurer que tout le trafic est surveillé efficacement. Sans pare-feu, le trafic réseau pourrait entrer et sortir de votre réseau sans restriction, même s'il transporte des menaces telles que les malwares et les sites Web malveillants.

Les pare-feu réseaux sont des composants essentiels de l'infrastructure de sécurité d'une organisation. Leur tâche principale est de surveiller le trafic entrant et sortant, et de l'autoriser ou de le bloquer.

Dans ce chapitre, nous allons présenter les notions générales sur les pare-feu.

2.2 Définition d'un firewall

Un pare-feu (firewall) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Un pare-feu est donc un élément pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système.

Un pare-feu met une politique de sécurité qui laisse passer, ou arrête le trafic réseau ou les paquets d'informations selon la politique adopté. Il peut donc autoriser ou empêcher des communications selon leur adresse source, leur adresse de destination ou leur contenu.

En effet, le pare-feu lit et analyse chaque paquet arrivant. Après analyse, il décide de basculer ou d'arrêter en fonction de l'adresse IP de l'expéditeur et du destinataire, du type de transmission (TCP ou UDP) et du numéro de port, ainsi que du type d'application réseau. Lorsque la politique de sécurité n'implique que des couches inférieures, l'analyse du paquet seule peut autoriser, refuser ou ignorer le paquet.

Lorsqu'une politique décrit des règles de sécurité impliquant un transport fiable (TCP), des sessions ou des applications, le pare-feu doit connaître l'état actuel de la connexion et doit mémoriser de nombreux paquets sur une certaine période de temps afin de pouvoir décider d'autoriser, d'ignorer ou refuser les paquets.

Les capacités des pare-feu ne sont pas sans limites. Afin de maintenir un flux de trafic optimal, les pare-feux nécessitent des ressources importantes pour éviter tout ralentissement. De plus, il est crucial que les pare-feu ne soient pas contournés par d'autres

passerelles ou modems externes. Malheureusement, les pare-feu deviennent des cibles privilégiées pour les attaquants qui cherchent à submerger leurs ressources. Pour surveiller et analyser efficacement les activités de ces passerelles de filtrage, un pare-feu doit posséder un système de journalisation avancé (.log). Cela permet un examen rétrospectif des événements significatifs tels que les tentatives d'intrusion, les occurrences anormales et les attaques par saturation.

L'architecture d'un pare-feu est généralement conçue pour créer une distinction claire entre les communications avec des entités externes, le réseau qui nécessite une protection et une zone tampon désignée appelée zone démilitarisée (DMZ). Dans cette zone spécifique, qui sert de mesure de sécurité, sont placés différents composants tels que des sites Internet et des systèmes de messagerie pour être accessibles depuis Internet. Ces composants sont protégés par un pare-feu tout en étant complètement isolés du réseau interne qui nécessite une protection. [4].

2.3 Principe de fonctionnement du firewall

Un système Pare-feu contient un ensemble de règles prédéfinies permettant :

- D’autoriser la connexion [allow],
- De bloquer la connexion [deny],
- De rejeter la demande de connexion sans avertir l’émetteur [drop].

Ces règles permettent de mettre une méthode de filtrage dépendant de la politique de sécurité adoptée par l’organisation. Généralement, Il existe deux types de politiques de sécurité permettant :

- Autoriser uniquement le trafic ayant été explicitement autorisées : « tout ce qui n’est pas autorisé est interdit »,
- Empêcher le trafic qui a été interdite.

La première méthode est la plus fiable, mais elle impose toutefois une définition précise des besoins en communication [5].

2.4 Listes de contrôle d'accès (Access Control Lists)

Une liste de contrôle d'accès (ACL) est une série de commandes qui déterminent si un pare-feu achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Il existe deux types deux types de listes "standard et étendues" :

2.4.1 Les listes de contrôle d'accès standard permettent d'autoriser ou d'interdire des adresses spécifiques ou bien un ensemble d'adresses source.

Une liste d'accès standard se crée par la commande suivante :

access-list num_acl {permit | deny} source {masque_source}

- Numéro_de_liste_d'accès : identifie la liste
- Permit | deny : autoriser ou interdire
- Source : identifie l'adresse IP source
- Masque_source : bits de masque générique

Exemple : access-list 1 deny 172.69.0.0 0.0.255.255

2.4.2 Les listes de contrôle d'accès étendues permet de faire un filtrage plus précis qu'une liste standard, elle permet également d'effectuer un filtrage en fonction du protocole, de l'adresse de destination ou de l'adresse source.

Une liste de contrôle d'accès étendue se crée par la commande suivante :

access-list *numéro_de_liste_d'accès {permit | deny} protocole source {masque_source} destination {masque_destination} {opérateur opérande} [established] [log]*

- Numéro_de_liste_d'accès : identifie la liste
- Permit | deny : autoriser ou interdire
- Protocol: indique le type de protocole « IP, TCP, UDP, ICMP, EIGRP, IGRP »
- Source et destination : identifient l'adresse IP source et destination
- Masque_source et masque_destination : bits de masque générique.

2.5 Les fonctions d'un pare-feu

Les fonctions du pare-feu les plus répondues sont :

- **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 `a 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. 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 qui permet d'´établir des rapports sur son activité et les archiver dans un journal pour pouvoir l'examiner ultérieurement.

2.6 Types de pare-feux

Il existe deux types de pare-feux :

2.6.1 Les firewalls matériels

Placé soit à la périphérie du réseau, soit entre Internet et un réseau informatique, un pare-feu matériel sert d'appareil tangible chargé de superviser le mouvement des paquets de données. Communément appelé pare-feu périmétrique, il protège l'ensemble de notre réseau en scrutant le trafic entrant et sortant au niveau du périmètre.
En adhérant à des directives spécifiques, il gère et protège efficacement notre environnement réseau. Grâce à l'examen des données par paquets, y compris les adresses source et de destination, il détermine s'il faut autoriser ou refuser leur transmission. En conséquence, il accorde à nos administrateurs réseau une autorité significative sur les activités réseau autorisées. En fin de compte, sa fonction principale est de renforcer les systèmes connectés et d'empêcher tout accès non autorisé.

La mise en œuvre d'un pare-feu matériel spécialisé peut nécessiter des compétences et une compréhension informatiques avancées, voire la présence d'une équipe ou d'un personnel informatique dédié. Par conséquent, les pare-feu matériels sont couramment utilisés par de grandes entreprises ayant des considérations de sécurité importantes, telles que les

institutions financières. Une fois l'installation réussie, un seul point de gestion suffit pour superviser la sécurité du réseau, ce qui entraîne d'importantes économies de ressources et de temps.

Exemples de pare feu materiels : Cisco ASA, Fortinet, SonicWall, etc…

2.6.2 Les firewalls logiciels

Un pare-feu logiciel est une solution logicielle installée en tant qu'Appliance virtuelle ou sur des ordinateurs individuels. Cette mesure de protection nous permet de réguler les actions d'applications spécifiques, nous donnant la possibilité de restreindre l'accès à des sites Web ou à des imprimantes particuliers au sein de notre réseau.

Agissant comme une formidable protection contre les cyberattaques, les pare-feu logiciels constituent une couche de protection supplémentaire. En croisant une base de données à jour, ces pare-feu sont capables d'évaluer la crédibilité des logiciels malveillants entrants et de prendre des décisions éclairées concernant leur accès à notre réseau. Cette puissante capacité leur permet de lutter efficacement contre les menaces potentielles provenant d'adresses sur liste noire, d'applications douteuses et de logiciels malveillants inconnus. De plus, les pare-feu logiciels offrent une adaptabilité remarquable lorsqu'il s'agit d'attribuer différents niveaux d'autorisations aux postes de travail et aux utilisateurs.

L'installation de pare-feu logiciels est une tâche plus simple que celle des pare-feu matériels, c'est pourquoi ils sont populaires auprès des petites entreprises et des particuliers. Ce type particulier de pare-feu offre une plus grande flexibilité en termes de personnalisation, permettant aux utilisateurs de mieux contrôler ses fonctionnalités et ses capacités de protection.

Exemples de pare feu logiciels : Cisco ASA, pfSense, OPNsense, iptables (linux), Windows Firewall (intégré dans le système d'exploitation Windows), etc..

Comparaison des deux types :

- **Simplicité d'installation :** Les pare-feu logiciels sont généralement plus simples à installer et à configurer que les pare-feu matériels.
- **Performance :** Les pare-feu matériels offrent généralement de meilleures performances grâce à du matériel dédié.

Ces types de pare-feu peuvent être utilisés individuellement ou combinés pour fournir une protection complète adaptée aux besoins spécifiques du réseau.

2.7 Types de filtrages

Il existe plusieurs types de filtrage de pare-feux:

2.7.1 Les pare-feux sans état

Ce type de pare-feu agit au niveau de la couche réseau et la couche transport. De ce fait ses règles sont basées sur les adresses IP source, adresse IP destination et les numéros de ports source et destination.

Inconvénients :

- Configuration complexe.
- Problème de flexibilité de filtrage.
- Devient de plus en plus obsolète.
- Traite les paquets indépendamment les uns des autres et les compare à une liste de règles appelées ACL (Access Control List).

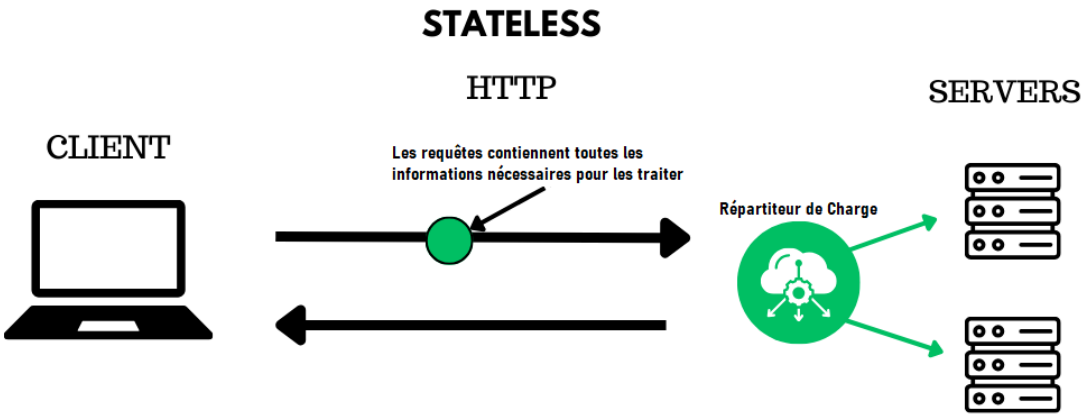


Figure 13 : pare- feux sans état

2.7.2 Les pare-feux avec état

Contrairement aux pare-feux à filtrage de paquets, ces dispositifs suivaient l'état des connexions actives et prenaient des décisions en se basant sur le contexte global du trafic réseau. Cela permettait de mieux comprendre l'état des connexions et de prendre des décisions plus informées et sécurisées.

Il prend des décisions de filtrage en fonction des informations récoltées lors des connexions précédentes en consultant le tableau des états. Cette façon de procéder lui permet de protéger le réseau de certaines attaques DDoS.

Inconvénients :

- Le tableau des états a une taille limitée.
- Il ne peut pas faire une inspection approfondie des paquets.

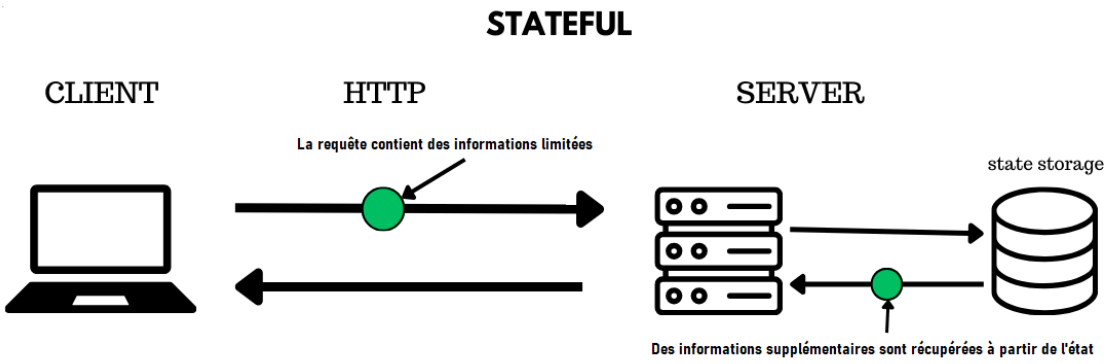


Figure 14 : pare- feux avec état

2.7.3 Les pare-feux applicatifs (Proxy)

Ce type de pare-feu permet de filtrer les communications au niveau de la couche application. Les requêtes sont vérifiées par un processus dédié.

Le pare-feu proxy fournit un point d'accès unique et permet d'évaluer le niveau de menace posé par les protocoles applicatifs, de détecter efficacement les menaces et de vérifier la validité du trafic réseau.

Un pare-feu proxy empêche aussi les communications directes entre l'ordinateur d'un utilisateur et les sites externes qu'il souhaite connecter, ce qui offre des avantages importantes en matière de sécurité.

Inconvénients :

- Plus le débit de connexion est important plus le temps de calcul du proxy est grand. [6]

2.8 Conclusion

Dans ce chapitre, nous avons défini et expliqué les fonctions de pare-feu. Ensuite, nous avons citez les différents types de pare-feux et les types de filtrage de données. La tâche principale de pare-feu est de surveiller le trafic entrant et sortant, et de l'autoriser ou de le bloquer.

Les pare-feux réseau sont des composants essentiels pour assurer la sécurité d'une organisation mais il reste insuffisant, les administrateurs réseau doit mettre d'autre moyens de sécurité comme les détecteurs d'intrusions.

CHAPITRE 3

Simulation

3.1 Introduction

Dans la partie simulation, nous avons simulé le réseau de la bibliothèque centrale sous Paquet Tracer. Le réseau de bibliothèque est composé de plusieurs salles informatiques, chaque salle contient un commutateur pour relier les différents équipements finaux (Ordinateur, imprimante, scanner, téléphones,…. etc.). Nous avons relié les commutateurs de chaque salle afin d'assurer la connectivité entre tous les salles informatiques.

Dans ce chapitre, nous allons citer les étapes essentielles de la simulation et la configuration de différents services et équipements (DHCP, routeur, VLAN, pare-feu, liste de contrôle d'accès).

3.2 Le logiciel Packet Tracer

Cisco Packet Tracer est un logiciel qui permet de créer des architectures réseau virtuelles, sans avoir besoin d'investir dans tous les équipements qui composent un réseau. Il permet de construire un réseau physique virtuel et de simuler le comportement des protocoles sur le réseau, aussi de créer des topologies plus ou moins complexe sans passer par l'achat des équipements, ainsi il permet une économie sur le plan financier. [7]

L'utilisateur construit son réseau à l'aide de différents équipements qui existe sur le logiciel, tels que les routeurs, les commutateurs ou des ordinateurs. L'ensemble de ces équipements sont reliés via plusieurs types de connexions (câbles divers, fibre optique).

La figure ci-dessous est la fenêtre qui présente les paramètres principaux de fonctionnement du simulateur Packet Tracer.

.

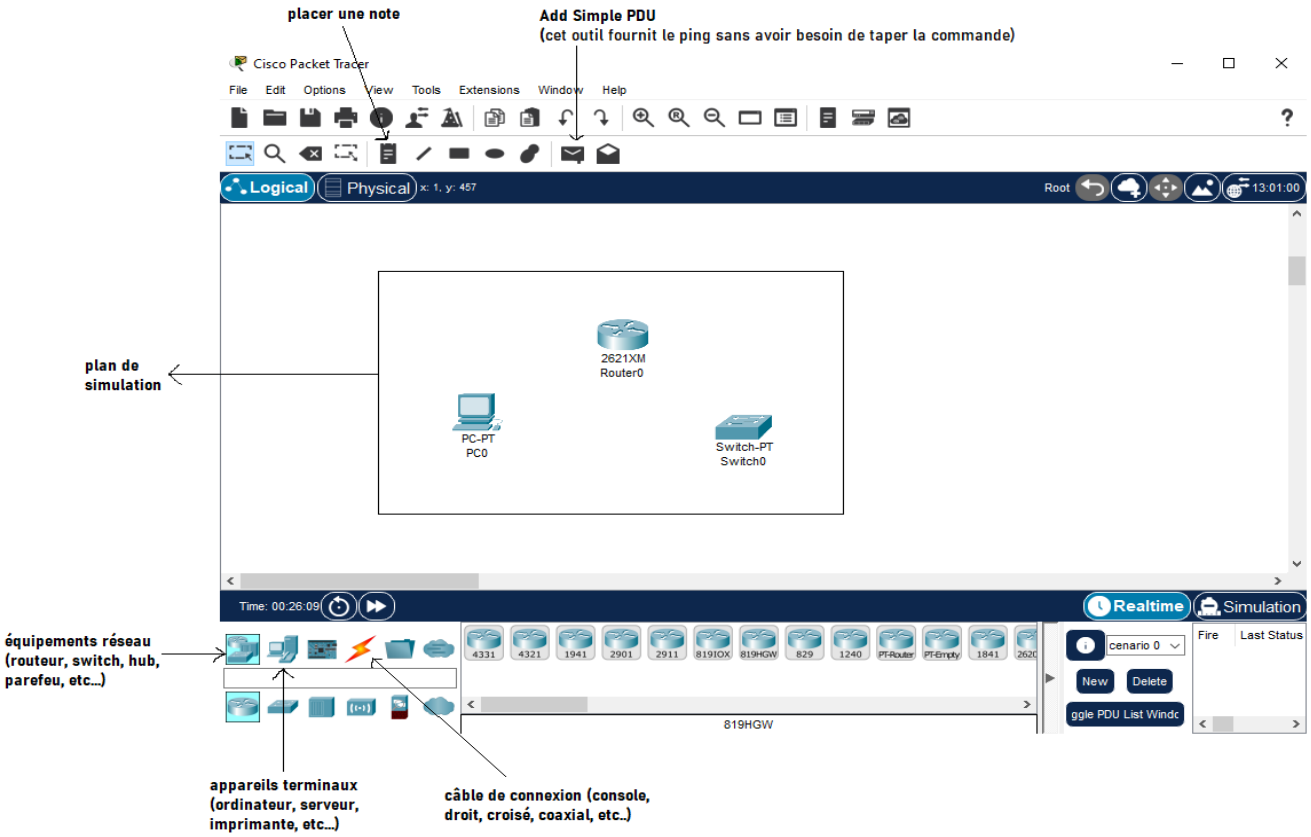


Figure 15 : La fenêtre principale du Packet Tracer

La barre d'outils comportant les outils minimaux nécessaires, Ainsi que trois boites à outils :

- Choix du type de matériel (ordinateur, routeurs, etc..).
- Choix du matériel en fonction du type.
- Les résultats de l'échange de données.

Afin de configurer l'équipement sélectionné on utilise l'onglet **config** et les boutons situées à gauche de la fenêtre qui déterminent le groupe de paramètres à configurer, comme le montre la figure ci-dessous :

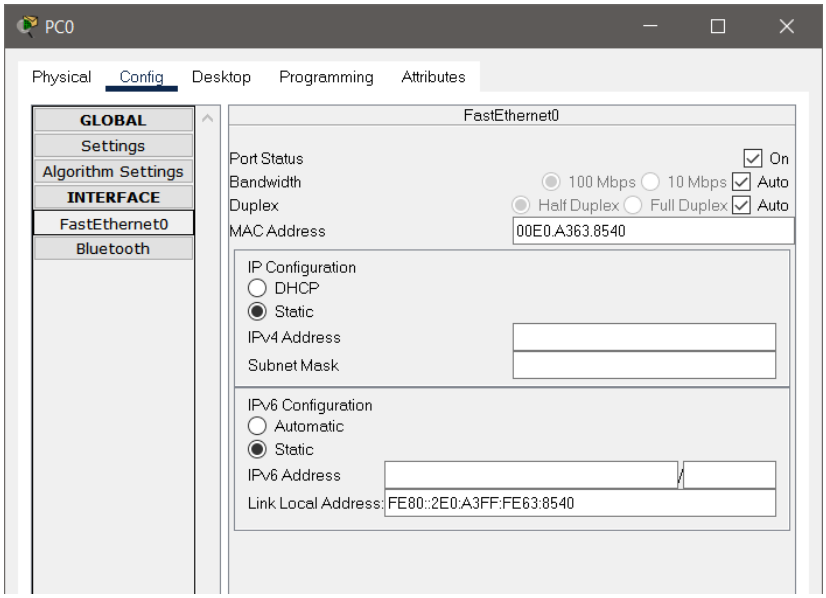


Figure 16 : Configuration de l'interface d'un PC.

L'onglet Desktop : Cet onglet met à la disposition les outils logiciels habituels de l'utilisateur.

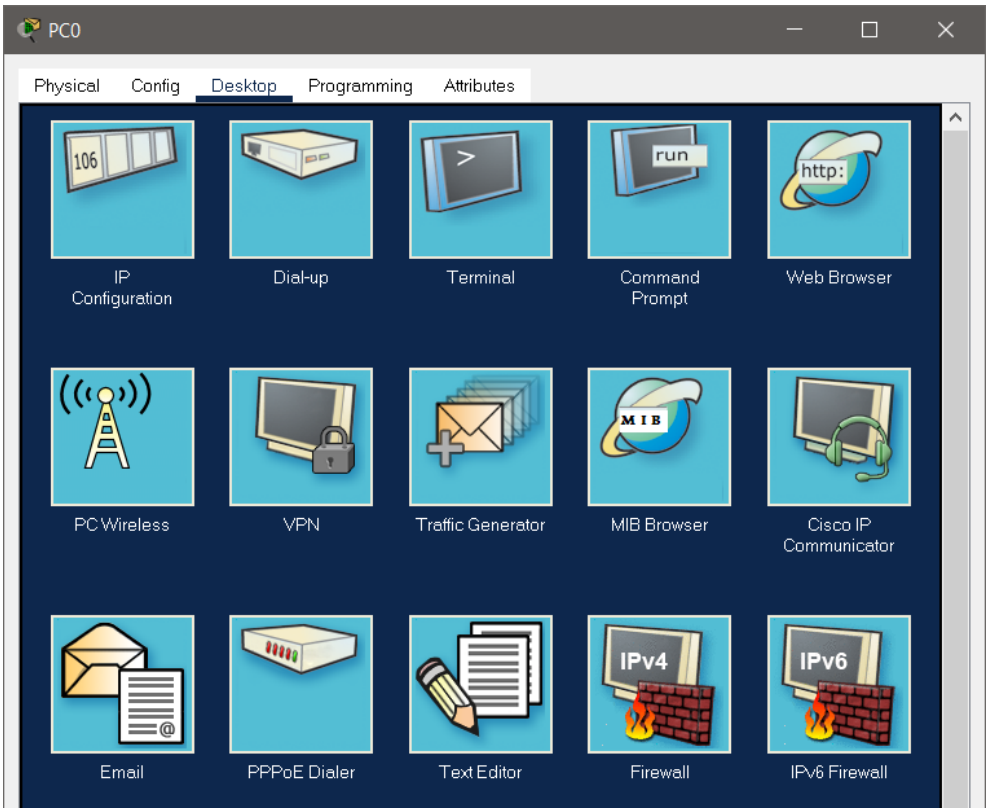


Figure 17 : Accès aux différents outils.

Ci-dessous, certaines utilités des outils de la figure ci-dessus :

- **IP configuration :** permet de configurer les paramètres réseau de la machine.
- **Dial-Up :** permet de configurer un modem s'il est présent dans l'équipement.
- **Terminal :** permet d'accéder à une fenêtre de programmation (HyperTerminal).
- **Command prompt :** est la fenêtre DOS classique permettant de lancer des commandes en ligne de commande (PING, IPCONFIG, ARP, etc..).
- **WEB Browser :** il s'agit d'un navigateur Internet.
- **PC Wireless :** permet de configurer une carte WIFI si elle est présente dans l'équipement.
- **VPN :** permet de configurer un canal VPN sécurisé au sein du réseau.
- **Traffic generator :** permet pour la simulation et l'équipement considéré de paramétrer des trames de communications particulières comme requête FTP vers une machine spécifiée.
- **MIB Browser :** permet par l'analyse des fichiers MIB d'analyser les performances du réseau.
- **CISCO IP Communicator :** Permet de simuler l'application logicielle de téléphonie développée par CISCO.
- **E-Mail :** client de messagerie.
- **PPPoE Dialer :** pour une liaison Point à Point.
- **Text Editor :** Editeur de texte.

Ce logiciel permet de simuler le fonctionnement d'un réseau et la visualisation par l'échange de trames Ethernet.

Il existe ainsi deux modes de simulations :

- La simulation en temps réel (Realtime) : Elle visionne instantanément toutes les séquences qui se produisent en temps réel.
- La simulation détaillée (Simulation) : Elle permet de visualiser au ralenti les séquences, entre deux ou plusieurs équipements.

3.3 Topologie de la bibliothèque centrale

Dans cette section, nous allons présenter le réseau de la bibliothèque centrale existant et la nouvelle topologie réseau proposée qui est base sur le pare-feu.

3.3.1 Topologie réseau sans pare-feu ASA

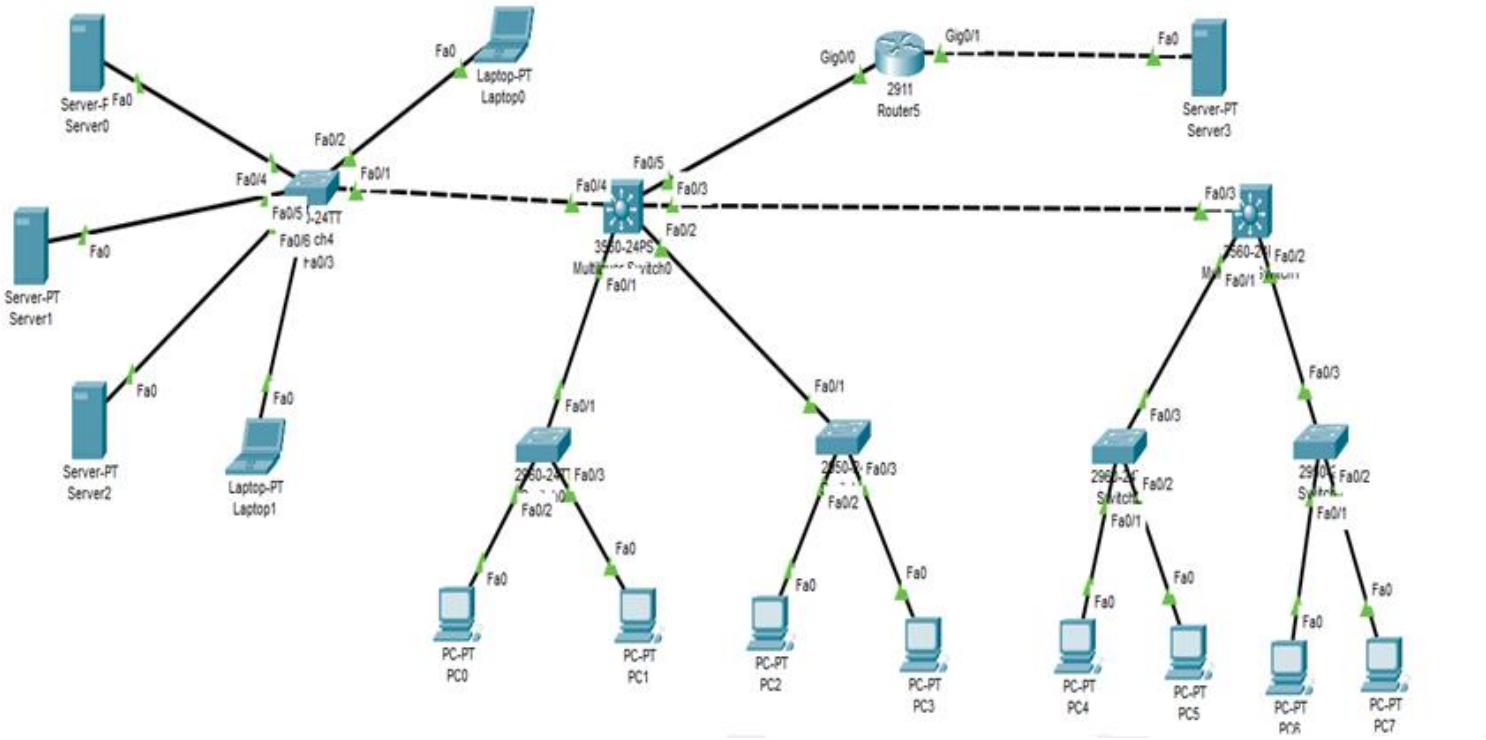


Figure 18 : Topologie réseau sans pare-feu ASA

3.3.2 Topologie réseau avec pare-feu ASA

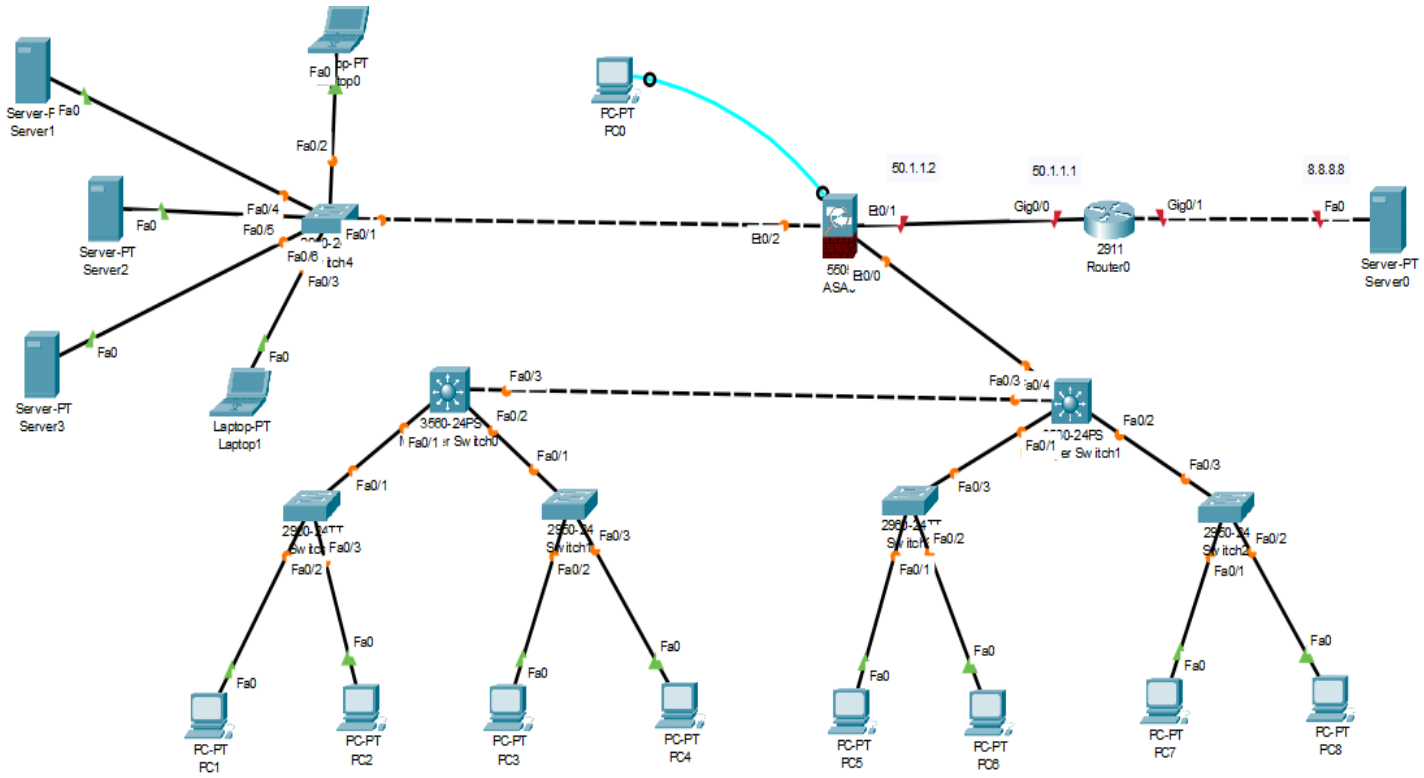


Figure 19 : Topologie réseau avec pare-feu ASA

3.4 Configuration du réseau de la faculté de Technologie

Dans la partie de simulation, nous commençons de réaliser la topologie « glisser les équipements et les relier avec les câbles de connexion». C'est en mode configuration globale que sont apportées toutes les modifications de la configuration de l'interface de commande en ligne, d'autres modes spécifiques sont activés tout dépend de la fonction de la modification de configuration requise mais ces modes sont tous des sous-ensembles du mode configuration globale. Au tout début, on nomme les routeurs. Ensuite, on configure les interfaces **GigabitEthernet0/0**, **Serial0/0/0**, **Serial0/0/1**, **Serial0/1/0** et **Serial0/1/1** avec leurs adresses IP et masques sous réseaux, ensuite on active toutes les interfaces avec la commande **no shutdown.**

Dans cette section nous allons présenter la configuration de notre réseau.

3.4.1 Configuration des interfaces des PCs

Etape 1 : On configure l'interface FastEthernet de chaque PC par son adresse IP et son masque réseau.

- **La configuration du PC0 :**

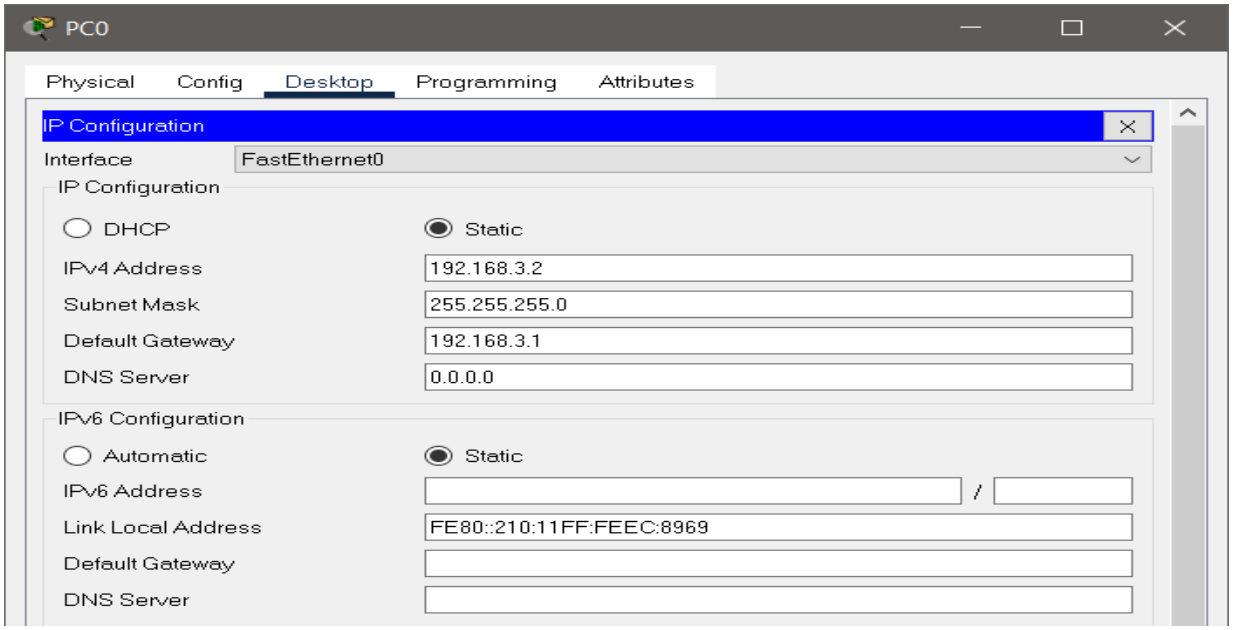


Figure 20 : La fenêtre de configuration d'un PC.

- **La configuration du Laptop0 :**

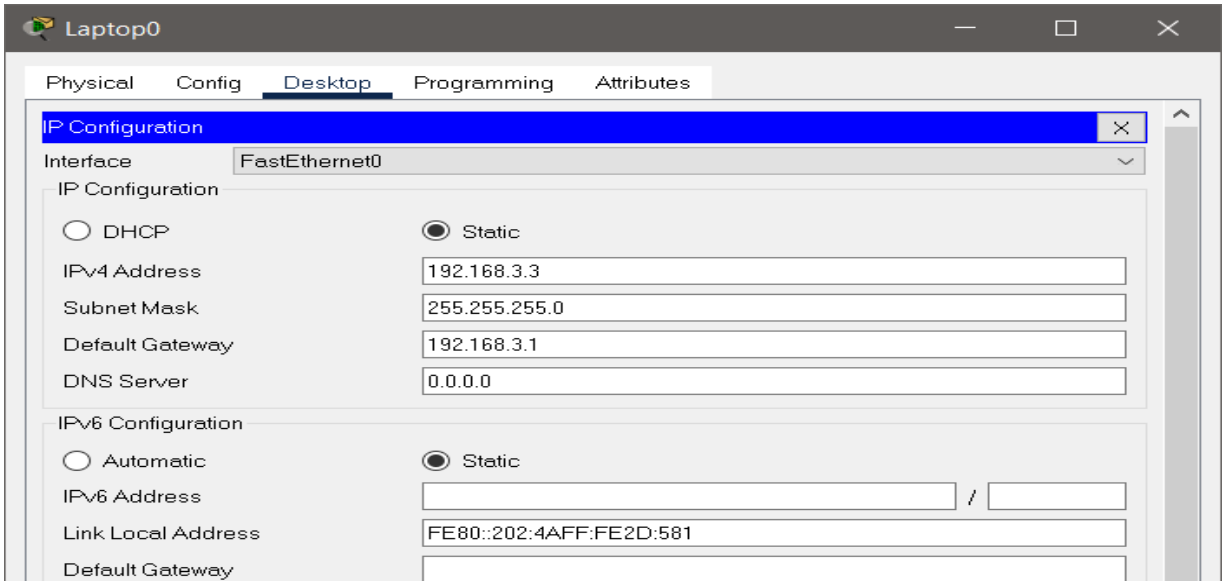


Figure 21 : La fenêtre de configuration d'un Laptop.

On applique la même configuration pour tous les autres PCs et Laptops mais avec différentes adresses IP mais le même masque sous réseaux. En ajoutant évidemment la passerelle par défaut en suivant la topologie.

Etape 2 : On exécute une requête ping sur les PCs du même LAN afin de tester la configuration, c'est-à-dire entre Le PC0 et Laptop0 par exemple, avec **command prompt** et on aura le résultat ci-dessous :

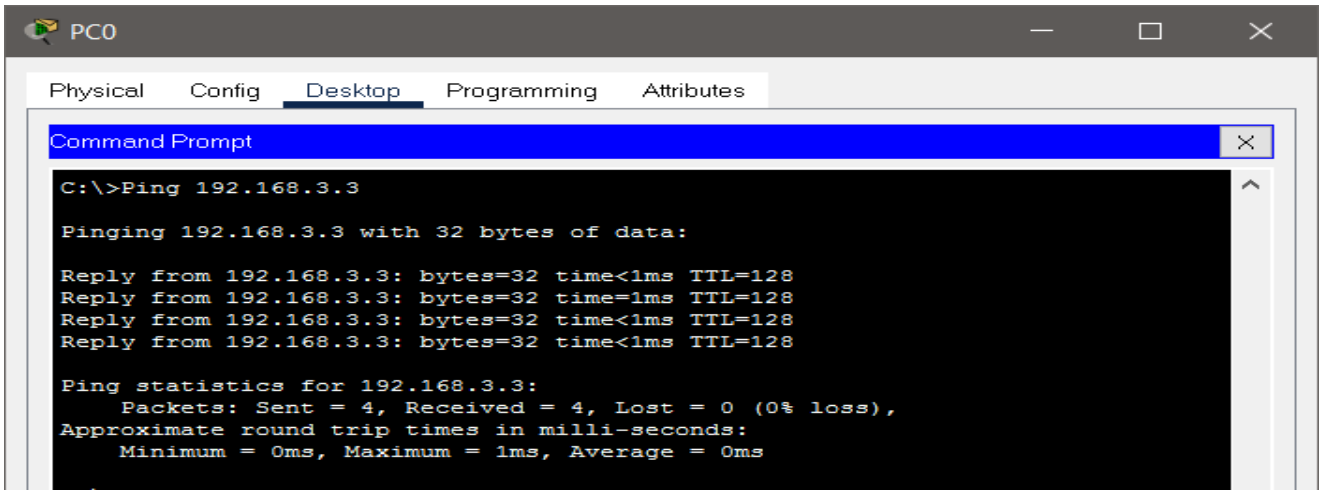


Figure 22 : L'exécution d'une requête PING.

3.4.2 Configuration des interfaces du routeur

interface gigabitEthernet0/0 (router vers asa) :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

Router(config-if)#ip address 50.1.1.1 255.0.0.0
Router(config-if)#description ASA
```

interface gigabitEthernet0/1 (router vers serveur) :

```
Router(config-if)#int g0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ip address 8.8.8.1 255.0.0.0
Router(config-if)#description SERVEUR
```

On vérifie si les adresses ip ont bien été changées avec la commande « show ip route » :

```
Router#show ip route
Codes: L - local, C - connected, S - static, 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 not set

     8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       8.0.0.0/8 is directly connected, GigabitEthernet0/1
L       8.8.8.1/32 is directly connected, GigabitEthernet0/1
     50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       50.0.0.0/8 is directly connected, GigabitEthernet0/0
L       50.1.1.1/32 is directly connected, GigabitEthernet0/0
```

Nous configurons les interfaces des routeurs avec les commandes suivantes :

- **Attribution d'un nom au routeur :** La commande **hostname**

  Router (config)# **hostname** R
- **Passage en mode de configuration d'interface**

  R (config) # **interface s0/0**

  R (config-if) # **ip address** <ip addressee ><masque reseau> R (config-if) # **no shutdown**

3.5 Configuration des VLAN d'accès et VLAN Trunk

Dans cette section, on présente la configuration des VLAN d'accès et VLAN Trunk pour avoir cette architecture réseau :

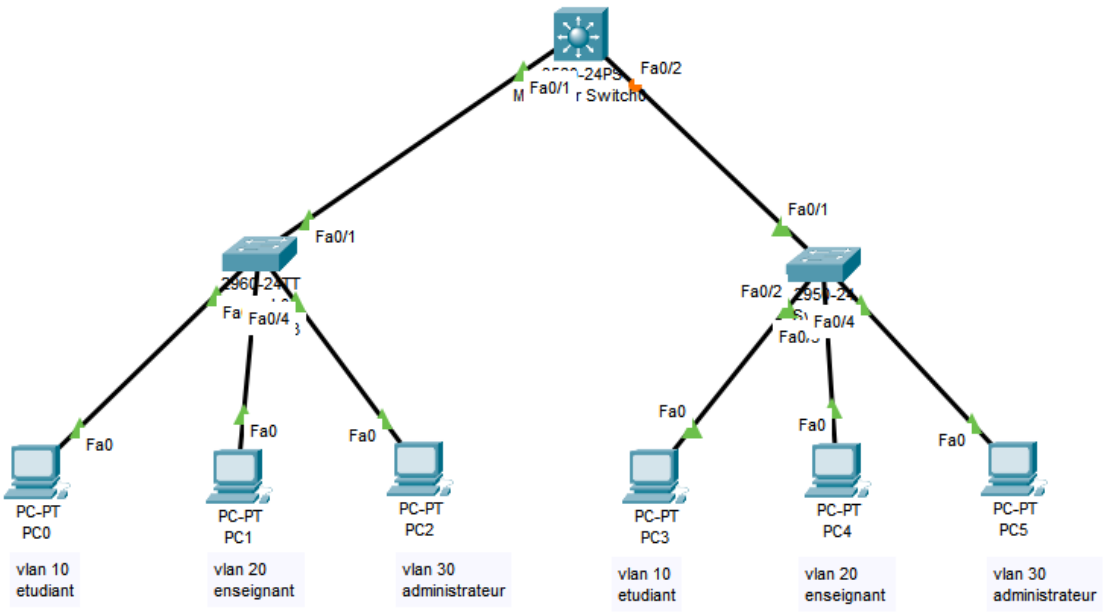


Figure 23 : Affectation des vlans et trunks dans les switchs de la zone inside

3.5.1 Configuration des VLAN d'accès du réseau interne

Dans le mode de configuration global du commutateur, nous allons saisir l'ensemble de ces commandes :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name etudiant
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name enseignant
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name administrateur
Switch(config-vlan)#
```

Figure 24 : Création des vlans dans le commutateur

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa 0/4
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
```

Figure 25 : Affectation des ordinateurs aux VLAN

3.5.2 Configuration des VLAN Trunk du réseau interne

La liaison Trunk est entre deux commutateurs. Voici les commandes afin de configurer les VLAN Trunk.

Dans le switch 1 :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Figure 26 : Affectation du switch 1 vers multilayer switch au Trunk

Dans le switch 2 :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Figure 27 : Affectation du switch 2 vers multilayer switch au Trunk

Dans le multilayer switch :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Switch(config-if)#int fa0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

Figure 28 : Affectation du multilayer switch vers les switch 1 et 2 au Trunk

3.6 Configuration des adresses IP des VLANs a partir de ASA

Avant toute chose on vérifie quelle est l'adresse dhcp par défaut à partir de ASA avec la commande « show running-config » :

```
dhcpd address 192.168.1.5-192.168.1.36 inside
```

Figure 29 : Adresse dhcpd par défaut dans le inside

On le désactive ensuite:

```
ciscoasa#conf t
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.36 inside
```

Figure 30 : Désactivation de l'adresse dhcpd

Configuration et attribution du vlan1 a l'interface Ethernet0/0 :

```
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#ip address 10.1.1.1 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/0
ciscoasa(config-if)#switchport access vlan 1
```

Figure 31 : Configuration du vlan1 et son attribution au l'interface e0/0

Configuration et attribution du vlan2 a l'interface Ethernet0/1 :

```
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)#ip address 50.1.1.2 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/1
ciscoasa(config-if)#switchport access vlan 2
```

Figure 32 : Configuration du vlan1 et son attribution au l'interface e0/1

On vérifie l'adresse ip de chaque vlan avec la commande « show ip address » :

```
ciscoasa#show ip add
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              10.1.1.1        255.0.0.0       manual
Vlan2                  outside             50.1.1.2        255.0.0.0       manual

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              10.1.1.1        255.0.0.0       manual
Vlan2                  outside             50.1.1.2        255.0.0.0       manual
```

Figure 33 : Adresse IP de chaque interface vlan

3.7 Configuration des zones : Inside (LAN) et Outside (WAN)

- **DANS LE SERVEUR,** catégorie « desktop/ip configuration » on configura ipv4 et default gateway

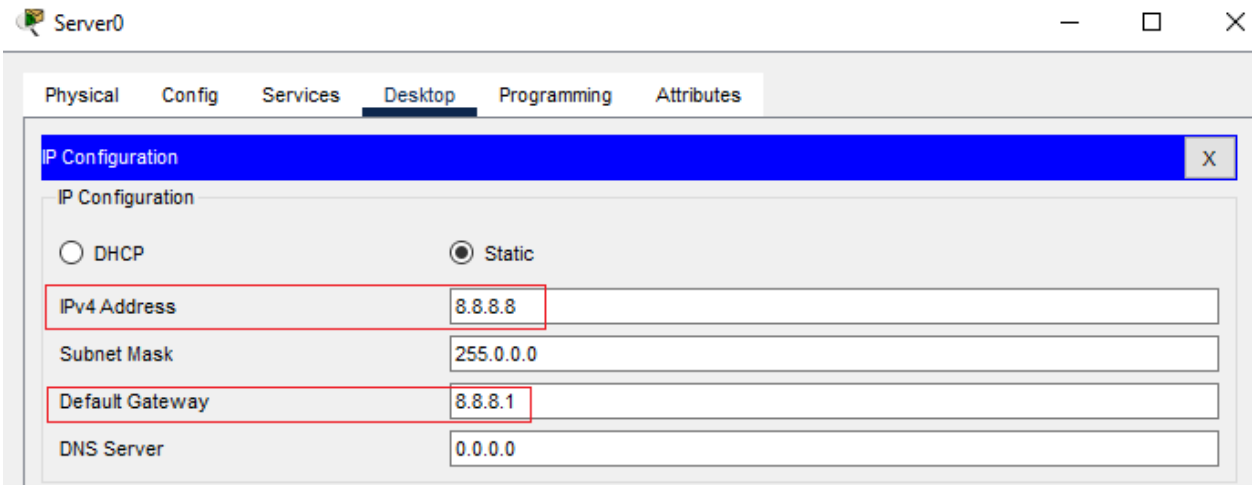


Figure 34 : Configuration de l'adresse ip dans le serveur

VERIFICATION dans le routeur

```
Router#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Figure 35 : L'exécution d'une requête PING du routeur vers le serveur

3.8 Configuration du DHCP

- **DANS LE ASA**

```
ciscoasa#conf t
ciscoasa(config)#dhcpd address 10.1.1.10-10.1.1.40 inside
ciscoasa(config)#dhcpd dns 8.8.8.8 interface inside
```

Figure 36 : Configuration de la nouvelle adresse dhcpd

Vérification DHCP dans chaque PC dans la catégorie « desktop/ip address" DHCP

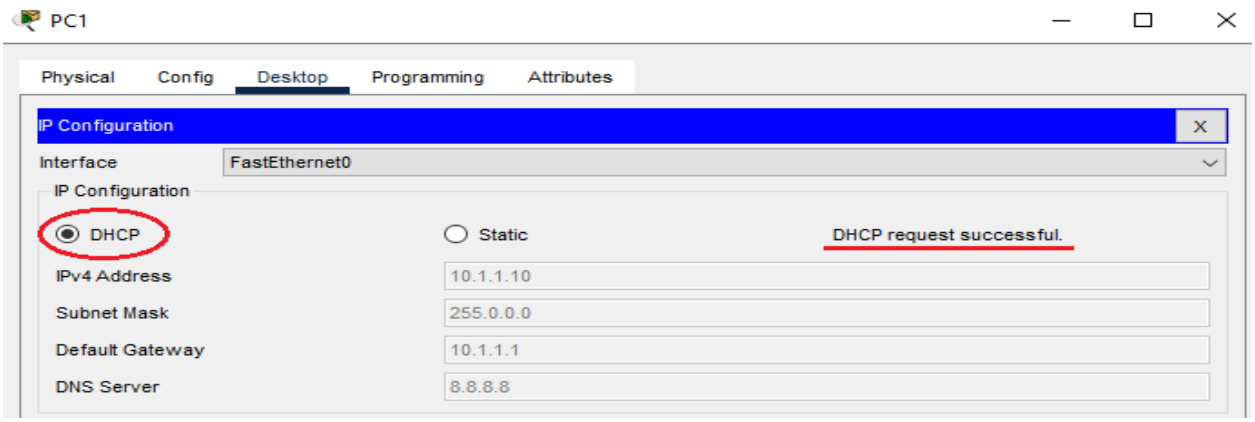


Figure 37 : Configuration des ordinateurs de Static a DHCP

3.9 Configuration de la route par défaut dans le ASA

- **DANS LE ASA**

```
ciscoasa#conf t
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 50.1.1.1
```

Figure 38 : Configuration de la route

3.10 Configuration du routage dynamique dans le routeur OSPF

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 50.0.0.0 0.255.255.255 area 0
Router(config-router)#network 8.0.0.0 0.255.255.255 area 0
```

Figure 39 : Configuration du routage dynamique dans le routeur

Vérification avec la commande « show ip protocols » dans le routeur :

```
Router#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 50.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    50.0.0.0 0.255.255.255 area 0
    8.0.0.0 0.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    50.1.1.1             110      00:00:46
  Distance: (default is 110)
```

Figure 40 : Adresse ip du routeur dynamique

3.11 Création d'un objet et activation du NAT dans le ASA

```
ciscoasa#conf t
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
```

Figure 41 : Création d'un objet et activation du NAT

3.12 Création un ACL dans le ASA

```
ciscoasa#conf t
ciscoasa(config)#access-list ASA extended permit tcp any any
ciscoasa(config)#access-list ASA extended permit icmp any any
ciscoasa(config)#access-group ASA in interface outside
```

Figure 42 : Création des ACL

Vérification dans le pc (command prompt)

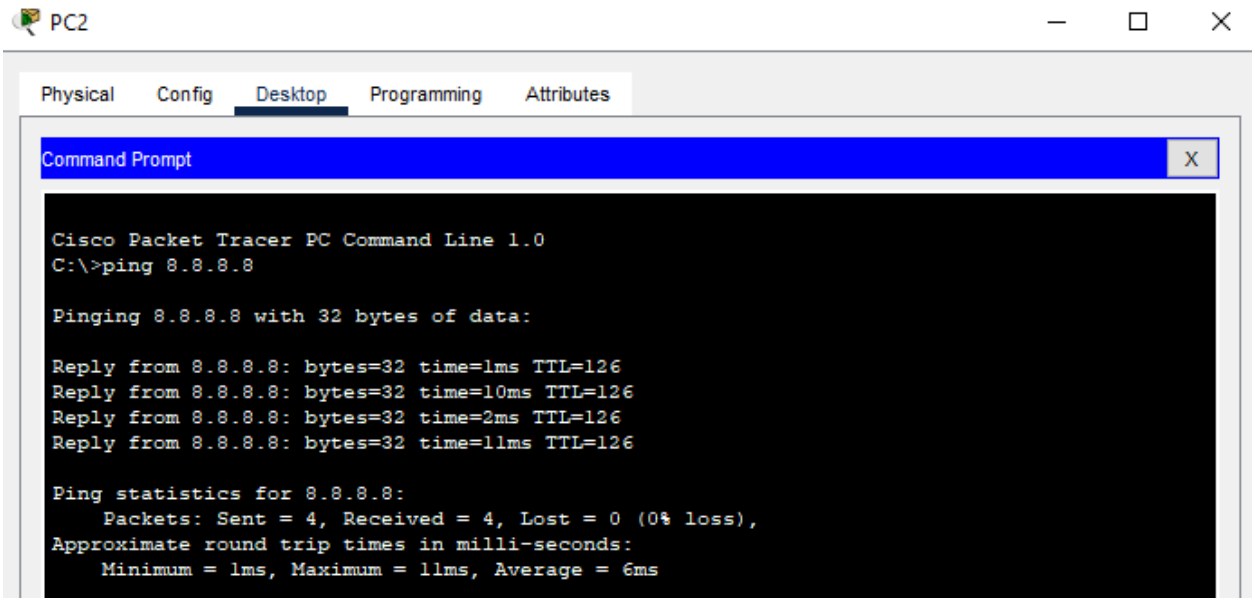


Figure 43 : L'exécution d'une requête PING du PC dans le inside vers le serveur outside

3.13 Configuration dans le DMZ

Configuration dans le ASA :

```
ciscoasa#conf t
ciscoasa(config)#interface vlan 3
ciscoasa(config-if)#ip add 11.1.2.1 255.0.0.0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 70
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport access vlan 3
```

Figure 44 : Configuration de l'interface vlan3 (dmz)

Configuration d'un NAT statique:

```
ciscoasa#conf t
ciscoasa(config)#object network dmz-server
ciscoasa(config-network-object)#host 11.1.2.3
ciscoasa(config-network-object)#nat (dmz, outside) static 50.1.1.3
```

Figure 45 : Configuration du NAT dans la zone dmz

Configuration d'un ACL pour autoriser l'accés au dmz server de l'internet enseignant

```
ciscoasa#conf t
ciscoasa(config)#access-list outside-dmz permit icmp any host 11.1.2.3
ciscoasa(config)#access-list outside-dmz permit tcp any host 11.1.2.3 eq 80
ciscoasa(config)#access-group outside-dmz in interface outside
```

Figure 46 : Configuration d'un ACL dans la zone dmz

3.14 Conclusion

Dans ce chapitre, nous avons simulé le réseau de la bibliothèque centrale en utilisant le pare-feu ASA. Puis, nous avons attribué le plan d'adressage aux équipements et configurer le serveur DHCP, les liste de contrôle et les trois zones (zone interne, zone externe et DMZ). Ensuite, nous avons configuré les VLAN d'accès et VLAN trunk entre les switch pour autoriser le trafic entre les PC de même VLAN.

CONCLUSION GENERALE

Dans cette étude, nous avons proposé une architecture sécurisée basée sur le pare-feu pour segmenter l'architecture existante en trois zones distinctes : la zone interne, la zone externe, et la zone démilitarisée (DMZ). La zone interne est dédiée aux ressources sensibles et aux utilisateurs internes, la zone externe est destinée aux utilisateurs et services externes, et la DMZ sert d'interface tampon où sont placés les services accessibles publiquement, comme les serveurs web. En outre, nous avons segmenté le réseau interne en plusieurs réseaux virtuels (VLANs) afin d'améliorer la gestion et la sécurité. Cette segmentation permet de limiter la portée des éventuels incidents de sécurité et de gérer plus finement les politiques d'accès entre les différents segments du réseau. Parallèlement, nous avons configuré le serveur DHCP pour attribuer automatiquement les paramètres réseau, tels que les adresses IP, les passerelles et les serveurs DNS, aux équipements finaux, ce qui simplifie grandement l'administration réseau et réduit les risques d'erreurs de configuration.

Nous avons approfondi notre compréhension de la sécurité des réseaux informatiques, en mettant un accent particulier sur les pare-feu. Cette étude nous a permis d'acquérir des connaissances théoriques et pratiques sur les différents types de pare-feu, leurs mécanismes de fonctionnement, et les meilleures pratiques pour leur configuration. Nous avons exploré comment les pare-feu peuvent filtrer le trafic réseau, bloquer les accès non autorisés, et protéger contre diverses menaces. De plus, nous avons examiné des scénarios réels d'attaques réseau et comment les pare-feu peuvent être utilisés pour les contrer, enrichissant ainsi notre compréhension des enjeux de la cybersécurité.

Par ailleurs, pour renforcer encore davantage la sécurité de notre réseau, il est recommandé d'utiliser des pare-feu à différents niveaux du réseau. Par exemple, en utilisant des pare-feu au niveau des routeurs, nous pouvons contrôler et filtrer le trafic entre les différents segments du réseau, assurant ainsi une protection plus granulaire. De plus, l'intégration de pare-feu au niveau des serveurs individuels et des postes de travail permet de renforcer la sécurité locale et de prévenir la propagation des menaces en cas de compromission d'un segment spécifique. Cette approche multicouche de la sécurité, où chaque niveau du réseau est protégé par un pare-feu adapté à son rôle et à ses risques spécifiques, offre une défense en profondeur et améliore significativement la résilience globale du réseau face aux cyberattaques.

ABREVIATIONS

LAN : Local Area Network
IP : Internet Protocol
TCP/IP : Transmission Control Protocol/Internet Protocol
VLAN : Virtual Local Area Network
DMZ : Demilitarized Zone
WAN : Wide Area Network
FTP : File Transfer Protocol
MAN : Metropolitan Area Network
PAN : Personal Area Network
GSM : Global System for Mobile communications
OSI : Open Systems Interconnection
PDU : Protocol Data Unit
VB : Visual Basic
ICMP : Internet Control Message Protocol
Fping : Fast Ping
Gping : Graphical Ping
Nmap : Network Mapper
Superscan : Super Scanner
SNMP : Simple Network Management Protocol
DoS : Denial of Service
SYN : Synchronize
ACK : Acknowledgment
DDoS : Distributed Denial of Service
TFN : Tribal Flood Network
TFN2K : Tribal Flood Network 2000
VPN : Virtual Private Network
SSL : Secure Sockets Layer
IPsec : Internet Protocol Security
PPTP : Point-to-Point Tunneling Protocol
L2TP : Layer 2 Tunneling Protocol
IDS : Intrusion Detection System
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
ACL : Access Control List
EIGRP : Enhanced Interior Gateway Routing Protocol
IGRP : Interior Gateway Routing Protocol
HTTP : HyperText Transfer Protocol
DHCP : Dynamic Host Configuration Protocol
NAT : Network Address Translation
OSPF : Open Shortest Path FirstS

LISTE DES FIGURES

BIBLIOGRAPHIE

[1]: https://www.journaldunet.fr/web-tech/dictionnaire-de-l-iot/1203387-gateway-informatique-definition-et-role-pour-les-donnees/

[2]: J. Cowley. (2012). Communications And Networking: An Introduction Undergraduate Topics In Computer Science (2nd ed.). UK: Springer-Verlag London

[3]: Lourent Bloch-Christophe Wolfhugel. EYROLLES, 2éme édition. 2005.

[4]. Davis Chapman, « Firewalls – La sécurité sur Internet », edition O'Reilly, 1997.

[5] : Jean-François Pillou et Jean-Philippe Bay. Sécurité informatique.3ème édition, Dunod, Paris 2013.

[6]: Cours université de batna https://cs.univ-batna2.dz/sites/default/files/web/files/cours4-les_systemes_de_filtrage_de_paquets_pare-feu.pdf

[7] : site OpenClassroom sur la conception d'un réseau https://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7235342-decouvrez-l-outil-de-simulation-packet-tracer