

## Rapport PFE 2021

# Sécurisation d'une infrastructure DMZ avec ASA Cisco



### Réalisation

- Ayoub Elbouzi
- Yassin Ouaddi

### Encadrement

- Ismail Kouza

# SOMMAIRE

<b>Chapitre 1 : Analyse et spécification des besoins</b>	<b>4</b>
Introduction générale au projet	4
Objective de la sécurité informatique	5
La zone DMZ et le pare-feu sure Cisco ASA	5
Besoins fonctionnels	8
Besoins techniques	8
<b>Chapitre 2 : Conception d'architecture</b>	<b>9</b>
Introduction d'architecture	9
La politique d'architecture	9
Présentation du model utilise	10
Présentation des équipements utilise	10
<b>Chapitre 3 : Réalisation du projet</b>	<b>13</b>
Présentation de la topologie	13
Etablir le plan d'adressage	14
Mise en place des routeurs	15
Mise en place des commutateurs	15
Mise en place des serveurs	18
Mise en place des ordinateurs	18
Configuration de Pare-feu	19
<b>Chapitre 4 : Test et validation</b>	<b>30</b>
Test du fonctionnement du réseau	30
Types attaques probable	34
Test des attaques	36
<b>Conclusion</b>	<b>38</b>

# REMERCIEMENT

Nous tenons à exprimer nos remerciements avec un grand plaisir et un grand respect à notre encadreur Le Directeur ABDERAHIM ZHALI pour ses conseils, sa disponibilité et ses encouragements qui nous ont permis de réaliser ce travail dans les meilleures conditions.

Nous exprimons de même notre gratitude envers tous ceux qui nous ont accordé leur soutien, tant par leur gentillesse que par leur dévouement.

A tous les enseignants qui nous ont aidés pendant les deux années passées au BTS, surtout notre encadrant prof. ISMAIL KOUZA

A toute personne ayant contribué de près ou de loin à l'avancement de notre projet.

A nos trois familles et amis pour leur aides.

Nous ne pourrions nommer ici toutes les personnes qui nous ont aidés et encouragés de près ou de loin et nous les remercions vivement.

# CHAPITRE 1 : ANALYSE DES BESOINS

## Introduction Générale

Les réseaux informatiques sont devenus un élément très important dans toutes les entreprises modernes qui possèdent un parc informatique et qui sont localisés dans plusieurs sites éloignés géographiquement. Le terme réseau définit un ensemble d'entités (machines, personnes, etc.)

interconnectées les unes avec les autres et qui permet circuler les données.

L'ordinateur c'est la machine qui permet de manipuler des données.

L'homme, qui utilise l'ordinateur pour se communiquer, a rapidement compris l'intérêt de ces ordinateurs reliés entre eux afin de pouvoir échanger les informations. Avec ces changements, le traitement de l'information est devenu facile, les évolutions en technologies des informations n'ont pas cessé de se développer. Ainsi, les données numériques, qui sont échangées entre les entités communicantes, circulent dans le réseau. Les administrateurs des réseaux assurent la fiabilité, la sécurité et la rentabilité. Mais, le passage au numérique impose à l'entreprise de rationaliser son système d'information car le pirate informatique peut s'infiltrer dans les réseaux. De ce fait, la sécurité est devenue un souci à tous les experts.

Aujourd'hui, il est de plus en plus difficile d'administrer un réseau informatique tant les solutions sont complexes tel que le pare-feu et l'antivirus, de même les attaques sont multiples et diversifiées, par exemple des virus, ou le déni de service. Pour traiter ce problème on a choisi que notre projet de fin d'études sera orienté vers un sujet de la sécurité des réseaux informatiques.

L'objectif de notre projet est d'établir une architecture réseau convenable aux besoins de notre centre BTS du lycée MED V (Utilisation optimale des adresses IP, la gestion et le dépannage facile du réseau, la protection du réseau contre les attaques, implémentation des différents serveurs, permet au réseau l'accès à l'internet...)

## Objectifs de la sécurité informatique

La sécurité informatique fait référence à l'utilisation de l'architecture réseau, des logiciels et d'autres technologies pour protéger les organisations et les individus contre les cyberattaques. L'objectif de la cybersécurité est de prévenir ou d'atténuer les dommages ou la destruction des réseaux informatiques, des applications, des appareils et des données pour garantir le bon fonctionnement des équipements du réseau et la protection des données des utilisateurs

Les objectifs de la sécurité informatiques sont :

- **Confidentialité** : Les informations confidentielles ne doivent être disponibles qu'à un nombre prédéfini de personnes. La transmission et l'utilisation non-autorisées d'informations devraient être restreintes au maximum. Par exemple, la confidentialité des données garantit que des informations personnelles ou financières ne soient accessibles par aucune personne non-autorisée et dotée d'intentions malveillantes, comme c'est le cas lors de l'appropriation d'identité ou des fraudes de cartes de crédit ou des données sensibles.
- **Intégrité** : Les informations ne devraient être modifiées d'aucune manière les rendant incomplètes ou incorrectes. La possibilité pour tout utilisateur non-autorisé de modifier ou détruire des informations confidentielles devrait être limitée au maximum.
- **Disponibilité** : Les utilisateurs autorisés devraient avoir accès aux informations lorsqu'ils en ont besoin. La disponibilité est la garantie que toute information peut être obtenue à une fréquence et opportunité établies préalablement. Ces valeurs sont généralement mesurées en termes de pourcentages et sont décidées de manière formelle dans les accords (SLA) utilisés par les fournisseurs de services réseau et leurs clients.

## La zone DMZ et les pare-feux sur ASA Cisco

Dans le domaine des réseaux informatique la zone démilitarisée est un sous réseau physique ou logique qui sépare un réseau local interne d'autre réseaux non sécurisés par exemple l'internet.

Les serveurs et les services qui ont un contact avec l'internet seront placé dans cette zone afin d'être accessible depuis le réseau internet, tandis que le reste du LAN interne n'est pas accessible.

Cette option donne à notre architecture réseau un niveau de sécurité supplémentaire, en empêchant les pirates d'accéder directement aux serveurs et aux données sensibles des utilisateurs à partir d'internet. Les serveurs qui sont concernés par la zone DMZ sont les serveurs WEB, DNS.

Le pare feu est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines du réseau. Il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur.

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** » (le terme *isolation* est parfois également utilisé).

Il y a plusieurs types de firewall réseaux et applicatifs, matériels et logiciels : Sophos, Fortigate, ces deux solutions sont payantes, cependant il y a plusieurs firewalls gratuits comme pfSense, Endian, IPCOP qui proposent un contrôle sur le trafic entre machines et l'Internet avec des règles entrantes et sortantes.

- Un firewall software s'installe sur les ordinateurs et vérifie les logiciels qui connectent sur internet et plus généralement sur le réseau, ces programmes détectent et bloquent les trojans les spywares et adwares, par contre ils ne détectent pas les manipulations spécifiques comme les modifications sur les programmes existants, les modifications sur les trames TCP/IP...

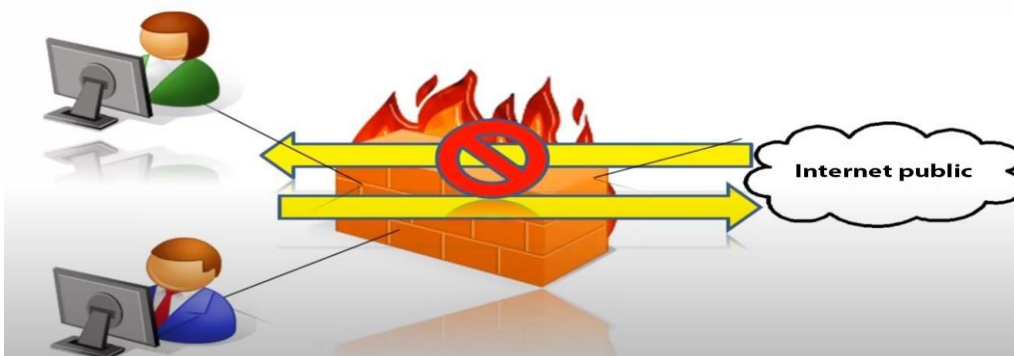


- Un firewall hardware permet de vérifier les portes d'accès en UDP et TCP et de les bloquer éventuellement en fonction de l'adresse de départ et l'adresse d'arrivée, contrairement au premier type, ces équipements hardware bloquent généralement une large partie des failles de sécurité et des modifications des trames en ferment les ports d'accès.

Ces deux types des pare feus sont complémentaires, et il est recommandé de les utiliser les deux pour une protection optimale contre les attaques.

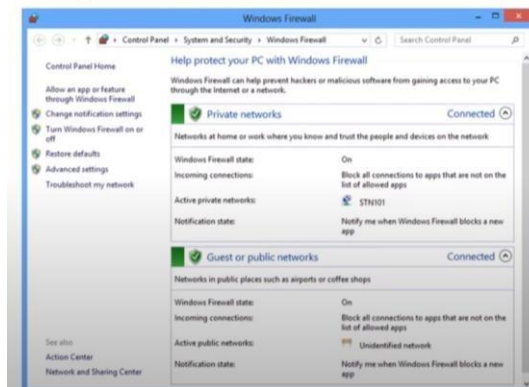
Le pare-feu ASA utilise les listes de contrôle d'accès (ACL) pour déterminer si le trafic est autorisé ou refusé. Par défaut, le trafic qui passe d'un niveau de sécurité inférieur à un niveau de sécurité supérieur est refusé. Cette règle peut être contournée par une ACL appliquée à l'interface de sécurité inférieure. L'ASA, par défaut, autorise également le trafic d'interfaces de sécurité supérieure vers des interface de sécurité inférieure. Ce comportement peut également être outrepassé par une ACL, l'ASA compare une connexion ou un paquet entrant à l'ACL sur une interface, et ce, sans annuler la traduction du paquet au préalable. En d'autres termes, l'ACL devait autoriser le paquet, comme si vous alliez le capter sur l'interface.

### Fonctionnement basique d'un pare-feu



## Types des pare-feux

### Logiciel



### Matériel



## Besoin fonctionnelle

- ✓ Proposer une architecture convenable au centre BTS.
- ✓ Installer et configurer le matériel nécessaire (routeurs, commutateurs, serveurs)
- ✓ Garantir le dépannage facile en cas de panne.
- ✓ La protection des machines et des serveurs et des données.
- ✓ La gestion et l'administration optimale du réseau.
- ✓ Limité l'accès au réseau pour les utilisateurs parvenant du réseau l'internet.
- ✓ La communication entre les différents périphériques du réseau.

## Besoin technique

- ✓ 1 routeur Cisco 1941 avec module HWIC-2T ajouté.
- ✓ 4 commutateurs Cisco 2960.
- ✓ 130 ordinateurs bureaux.
- ✓ 1 serveur WEB.
- ✓ 1 serveur DHCP.
- ✓ 1 serveur DNS.
- ✓ 1 pare-feu Cisco ASA 5505.
- ✓ 1 point d'accès.
- ✓ 130 prises RJ45.
- ✓ Câble coaxiale cat6



# CHAPITRE 2 : LA CONCEPTION DE L'ARCHITECTURE

## Introduction d'architecture

Notre centre BTS contient deux filières : systèmes et réseaux informatiques et management touristique, donc les groupes sont SRI1, SRI2, MT1, MT2. Le centre contient 5 salles : 4 salles des cours et une administration, chaque salle des cours contient 30 ordinateurs bureaux pour les étudiants, et l'administration contient 10 ordinateurs pour les professeurs et le cadre administratif du centre.

Le centre possède des serveurs et des commutateurs et des routeurs qui acheminent les données vers les différentes parties du réseau.

Pour des finalités de la sécurité de l'architecture on va séparer les réseaux internes (réseau du centre) du réseau externe (l'internet), et on attribue une administration externe du réseau BTS.

## Politique d'architecture

La politique sécurité mise en œuvre sur notre architecture est la suivante :

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

## Présentation du model utilisé

On peut définir, ici, la façon dont les équipements sont interconnectés et la représentation spatiale du réseau (topologie physique). On peut aussi définir la façon dont les données transitent dans les lignes de communication (topologies logiques).

La topologie d'un réseau correspond à son architecture physique. En ce sens où leur structure détermine leur type.

Il existe 2 modes de propagation classant ces topologies :

### Mode de diffusion (par exemple topologie en bus ou en anneau)

Ce mode de fonctionnement consiste à n'utiliser qu'un seul support de transmission. Le principe est que le message est envoyé sur le réseau, ainsi toute unité réseau est capable de voir le message et d'analyser selon l'adresse du destinataire si le message lui est destiné ou non.

### Mode point à point (par exemple topologie en étoile ou maillée)

Dans ce mode, le support physique ne relie qu'une paire d'unités seulement. Pour que deux unités réseaux communiquent, elles passent obligatoirement par un intermédiaire (le nœud).

Pour notre entreprise, on utilise le mode point à point grâce à l'avantage que le panne d'une station ne cause pas la panne du réseau et on peut retirer ou ajouter facilement une station sans perturber le réseau.

## Présentation des équipements utilisés

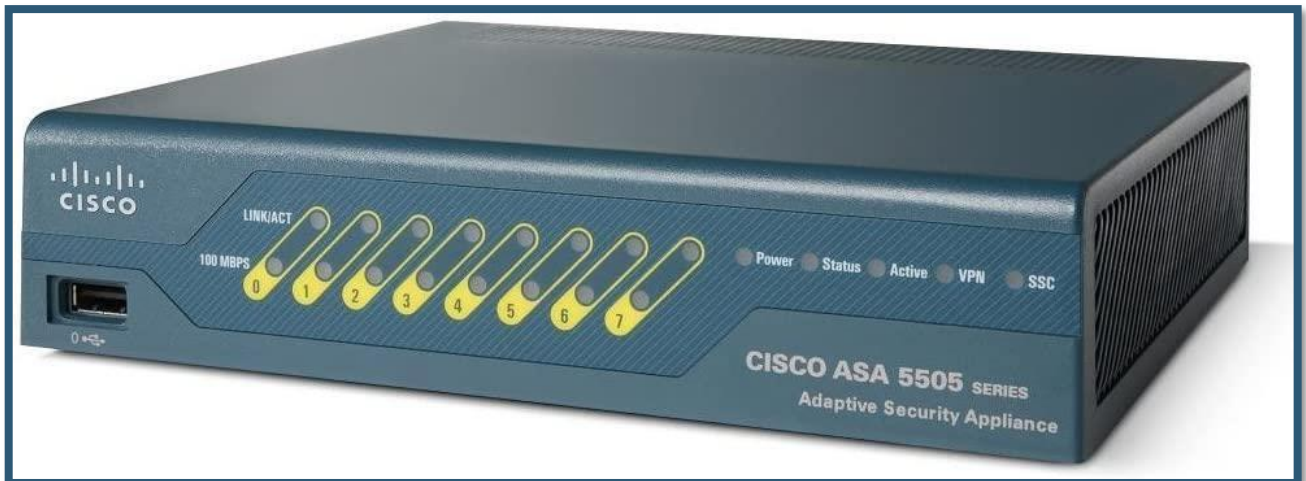
**Serveur DNS :** Par défaut, le serveur DNS utilisé par une connexion est géré par le FAI (Fournisseur d'Accès à Internet). Cela permet généralement de bonnes performances.

**Serveur Web :** Servir des ressources du Web et pour faire fonctionner en parallèle d'autres services liés comme l'envoi d'e-mails, l'émission de flux streaming, le stockage de données via des bases de données, le transfert de fichier.



**Firewall** : fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.

Dans cette topologie on va utiliser Cisco ASA Firewall 5505 :

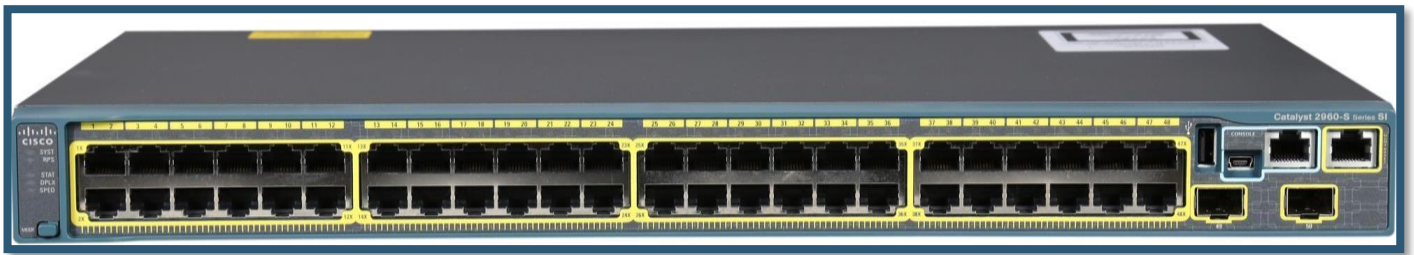


**Commutateur** : Un commutateur réseau (ou switch, de l'anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs (entre 4 et 100) ports Ethernet. Il a donc la même apparence qu'un concentrateur (hub).

Contrairement à un concentrateur, un commutateur ne se contente pas de reproduire sur tous les ports chaque trame (informatique) qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs.

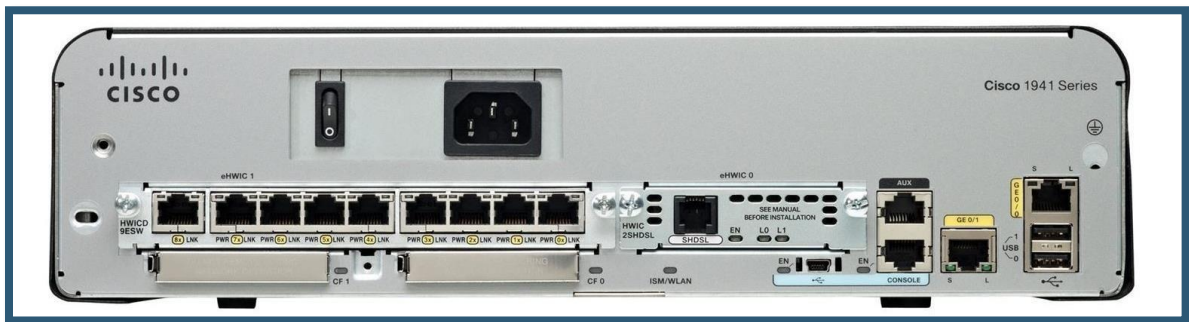
Contrairement à un routeur, un commutateur de niveau 2 ne s'occupe pas du protocole IP. Il utilise les adresses MAC et non les adresses IP pour diriger les données. Les commutateurs de niveau 2 forment des réseaux de niveau 2 (Ethernet). Ces réseaux sont reliés entre eux par des routeurs (ou des commutateurs de niveau 3) pour former des réseaux de niveau 3 (IP).

On va utiliser un commutateur Cisco Catalyst 2960 :



**Routeur** : Un routeur est un équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau. Il permet, entre autres, de faire circuler des données entre deux interfaces réseau.

On va utiliser un routeur Cisco 1941 avec un module HWIC-2T ajouté :

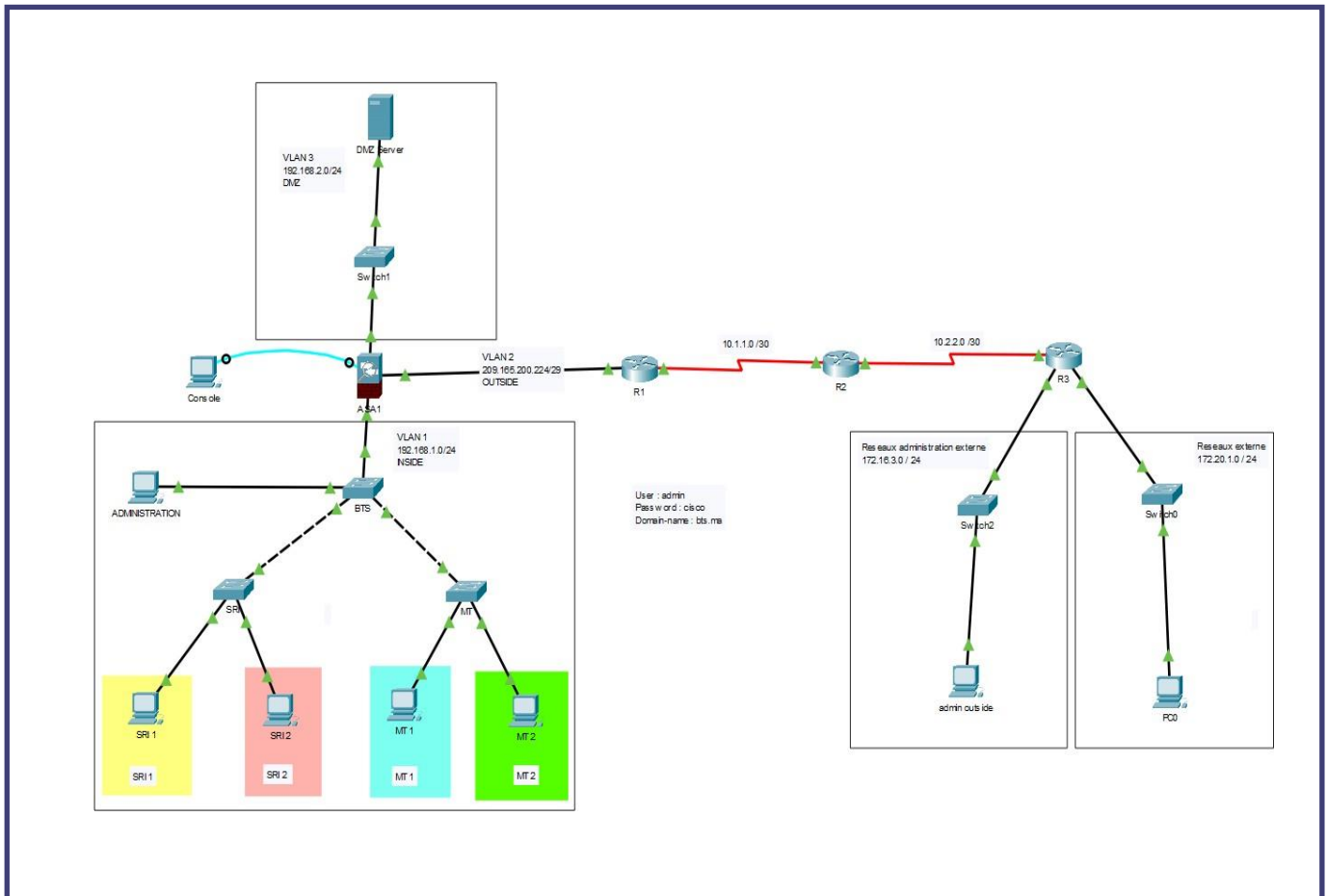


**Point d'accès** : un appareil qui permet la communication sans fil entre les différentes parties du réseau.



# CHAPITRE 3 : REALISATION DU PROJET

## Présentation de topologie utilisée



La topologie ci-dessus présente l'architecture étudiée ; un réseau de BTS contient une 2 commutateurs, un ordinateur qui présente l'administration, un ordinateur qui présente SRI-1 et un qui présente SRI-2 et le même pour MT-1 et MT-2.

Le pare-feu ASA sépare entre le réseau BTS et DMZ ; celui qui filtre et contrôle l'accès au réseau DMZ où situe le serveur DMZ et WEB.

Pour le réseau externe on attribue un ordinateur qui présente l'administration externe du réseau BTS ainsi que la gestion du pare-feu, en même temps un réseau externe pour tester la sécurité et l'accès aux réseaux DMZ et BTS.

## Etablir le plan d'adressage

Avec un plan d'adressage IP fixe cet identifiant est évidemment l'adresse IP.

Ceci épargne aux administrateurs la mise en place d'un plan d'adressage IP spécifique, notamment dans le cadre d'une infrastructure déployée à travers plusieurs centres de données. Il permet de calculer et de planifier des plans d'adressage de réseaux IP. Les informations d'adressage IP partagées définissent des gammes respectives différentes d'adresses IP locales attribuées à une pluralité de tels réseaux d'accès.

Portion de l'espace d'adressage IP Internet inoccupé (aucun équipement présent). Cette découverte est basée sur la préanalyse de tout l'espace d'adressage IP.

Notre architecture se base sur :

- 192.168.1.0 / 24 pour le LAN interne (BTS)
- 192.168.2.0 / 24 pour le LAN DMZ
- 172.16.3.0 / 24 pour le LAN administration externe
- 172.20.1.0 / 24 pour le LAN externe (test)
- 209.165.200.224 / 29 pour le WAN entre le pare-feu et R1
- 10.1.1.0 / 30 pour le WAN entre R1 et R2
- 10.2.2.0 / 30 pour le WAN entre R2 et R3



## Mise en place des routeurs

Pour les routeurs, on établit 3 routeurs ; R1 pour le réseau interne et DMZ, R2 relie entre R1 et R3, et R3 pour le réseau externe. L'emplacement des routeurs est mentionné dans la topologie. Chaque routeur mise en œuvre a sa configuration. On la montre comme suivant ;

- Routeur R1 :

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#hostname R1
R1(config)#
R1(config)#enable password cisco
R1(config)#
R1(config)#int gig0/0
R1(config-if)#ip add 209.165.200.225 255.255.255.248
R1(config-if)#exit
R1(config)#int se0/0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#exit
R1(config)#
R1(config)#ip route 172.16.3.0 255.255.255.0 10.1.1.2
R1(config)#ip route 10.2.2.0 255.255.255.252 10.1.1.2
R1(config)#ip route 172.20.1.0 255.255.255.0 10.1.1.2
R1(config)#exit
```

- Routeur R2 :

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#hostname R2
R2(config)#
R2(config)#enable password cisco
R2(config)#
R2(config)#int se0/0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#exit
R2(config)#int se0/0/1
R2(config-if)#ip add 10.2.2.1 255.255.255.252
R2(config-if)#exit
R2(config)#
R2(config)#ip route 209.165.200.224 255.255.255.248
% Incomplete command.
R2(config)#ip route 209.165.200.224 255.255.255.248 10.1.1.1
R2(config)#ip route 172.16.3.0 255.255.255.0 10.2.2.2
R2(config)#ip route 172.20.1.0 255.255.255.0 10.2.2.2
R2(config)#exit
R2#
```

- Routeur R3 :

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#hostname R3
R3(config)#
R3(config)#enable password cisco
R3(config)#
R3(config)#int se0/0/0
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#exit
R3(config)#int gig0/1
R3(config-if)#ip add 172.16.2.1 255.255.255.0
R3(config-if)#exit
R3(config)#int gig0/0
R3(config-if)#ip add 172.20.1.1 255.255.255.0
R3(config-if)#exit
R3(config)#
```

## Mise en place des commutateurs

Cet équipement relie plusieurs segments (câbles ou fibres) dans le permet de créer des circuits virtuels. On établit 3 commutateurs au sein du réseau interne (BTS) ; deux pour SRI et MT, et un pour l'administration ; les commutateurs sont reliés entre eux. On établit aussi un commutateur par chaque réseau restant. L'emplacement de chaque commutateur est mentionné dans la topologie.

Tant qu'il n'y a qu'un Vlan, la configuration des commutateurs sera juste une configuration de base (établir un nom et un mot de passe).

- Commutateur d'administration :

```
Switch>
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname administration
administration(config)#
administration(config)#enable password admin-cisco
administration(config)#
administration(config)#exit
administration#
%SYS-5-CONFIG_I: Configured from console by console
```

- Commutateur de SRI 1

```
Switch>
Switch>enable
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#hostname SRI-1
SRI-1(config)#
SRI-1(config)#enable password admin-sri
SRI-1(config)#
SRI-1(config)#exit
SRI-1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Commutateur de SRI 2

```
Switch>
Switch>enable
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#hostname SRI-2
SRI-2(config)#
SRI-2(config)#enable password admin-sri
SRI-2(config)#
SRI-2(config)#exit
SRI-2#
%SYS-5-CONFIG_I: Configured from console by console
```

- Commutateur de MT 1

```
Switch>
Switch>enable
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname MT-1
MT-1(config)#
MT-1(config)#enable password admin-mt
MT-1(config)#
MT-1(config)#exit
MT-1#
%SYS-5-CONFIG_I: Configured from console by console
```

- Commutateur de MT 2

```
Switch>
Switch>
Switch>enable
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#hostname MT-2
MT-2(config)#
MT-2(config)#enable password admin-mt
MT-2(config)#
```

## Mise en place des serveurs

Le serveur est un élément matériel ou logiciel informatique qui fournit des fonctionnalités à d'autres programmes ou appareils, appelés « clients ». En accumule dans notre architecture un seul serveur située dans le réseau DMZ, il joue le rôle de serveur WEB, son adresse IP est 192.168.2.3. Il reçoit les paquets depuis le réseau interne (BTS). Il ne reçoit aucune configuration.

## Mise en place des ordinateurs

Dans notre architecture on a 4 salles des cours et une administration, chaque salle des cours contient 30 ordinateurs bureaux pour les étudiants, l'administration contient 10 ordinateurs pour les professeurs et le cadre administratif du centre, et un ordinateur d'administration externe. Alors, on va présenter chaque salle par un seul ordinateur. L'adressage sera avec la configuration DHCP au sein du pare-feu.

## Configuration de Pare-feu

Un pare-feu est un dispositif de sécurité réseau qui surveille le trafic réseau entrant et sortant et décide d'autoriser ou de bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité.

Les pare-feux constituent la première ligne de défense en matière de sécurité des réseaux depuis plus de 25 ans. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés auxquels on peut faire confiance et les réseaux extérieurs non fiables, comme Internet.

Un pare-feu peut être matériel, logiciel ou les deux.

La configuration de pare-feu représente la moitié de configuration de notre r topologie, pour cela on va la partager en 5 étapes comme suivant :

- Etape 1 : vérifier la connectivité et explorer ASA
- Etape 2 : Configurer les paramètres ASA de base et les niveaux de sécurité d'interface
- Etape 3 : Configurer le routage, la traduction d'adresses et la politique d'inspection
- Etape 4 : Configurer DHCP, AAA, et SSH
- Etape 5 : Configurer DMZ, Nat statique, et les ACLs

✓ Etape 1 :

Au début, rien n'était configuré, alors tous les tests de ping entre les réseaux et DMZ ne passe pas alors on passe à la configuration basic de ASA et les niveaux de sécurité.

✓ Etape 2 :

A la configuration du ASA on notent qu'il nécessite un mot de passe pour accès au mode privilégié. Par default, pas de mot de passe défini ; alors on tape entrer et continuer.

```
ciscoasa>enable
Password:
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#
ciscoasa(config)#
```

Les périphériques de Cisco sont parfois basiquement configuré, alors on

tape la commande « show run » pour afficher la configuration actuelle d'un appareil. C'est l'une des premières commandes que vous entrerez lorsque vous essayez de comprendre comment un périphérique est configuré.

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
```

On constate quelques basiques configurations mais ils ne posent aucun effet.

Alors, correctement le premier endroit pour commencer est créer un nom d'hôte et établir un mot de passe pour le pare-feu. Donc, nous allons utiliser la ligne de commande suivante :

```
ciscoasa(config)#
ciscoasa(config)#hostname ASA
ASA(config)#
ASA(config)#
ASA(config)#domain-name ciscosecurity.com
ASA(config)#
ASA(config)#
ASA(config)#
ASA(config)#enable password cisco
ASA(config)#exit
ASA#
ASA#exit
```



Basiquement, on a 3 réseaux liée au pare-feu ; réseau interne de BTS qui est le plus fiable, le réseau DMZ qui est semi-fiable et le réseau externe non-fiable car il est connecté à l'internet ; nous ne pouvons pas le contrôler.

Alors ce qu'on va configurer est le suivant ;

- Vlan 1 interne avec l'adresse 192.168.1.1 et niveau de sécurité 100 car il est fiable

```
ASA#conf t
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA(config-if)#ip add 192.168.1.1 255.255.255.0
ASA(config-if)#sec
ASA(config-if)#security-level 100
```

- Vlan 2 (externe) avec l'adresse 209.165.200.226 et niveau de sécurité 0 car il est non-fiable (connecte à l'internet)

```
ASA(config)#int vlan 2
ASA(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA(config-if)#ip add 209.165.200.226 255.255.255.248
ASA(config-if)#secur
ASA(config-if)#security-level 0
```

Pour une vérification on utilise la commande « show switch vlan » :

```
ASA(config-if)#
ASA(config-if)#show 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

On note ici que le port Et0/0 (qui est dirigée au réseau externe) est déjà affectée au vlan 2.

Pour confirmer l'adressage de vlan on établit la commande « show int ip brief »

```
ASA(config)#show int ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	down	down
Ethernet0/4	unassigned	YES	unset	down	down
Ethernet0/5	unassigned	YES	unset	down	down
Ethernet0/6	unassigned	YES	unset	down	down
Ethernet0/7	unassigned	YES	unset	down	down
Vlan1	192.168.1.1	YES	manual	up	up
Vlan2	209.165.200.226	YES	manual	up	up

On peut le confirmer aussi depuis un ordinateur interne si on lui donne une adresse statique et on le ping ;

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::206:2AFF:FE1B:9577
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.1.3
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

```
C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Mais si on ping l'interface externe depuis l'ordinateur interne, on ne reçoit aucune réponse grâce à la sécurité par défaut de pare-feu qui ferme les ports sauf ils ont été configurée.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

### ✓ Etape 3 :

Si on ping depuis un ordinateur interne vers R1, le routeur ne connaît pas leur adresse puisqu'elle est une adresse privée, alors on peut configurer une table de routage au sein de pare-feu pour ce réseau afin qu'il puisse communiquer avec le routeur R1 et alors R2 et R3.

« Show route » nous affiche les réseaux directement connectés par défaut jusqu'à ce qu'on configure avec le routage statique suivant ;

```
asa(config-if)#show 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 not set

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
    209.195.200.0/29 is subnetted, 2 subnets
C      209.195.200.0 255.255.255.248 is directly connected, outside, Vlan2
C      209.195.200.224 255.255.255.248 is directly connected, outside, Vlan2
```

Le routage statique s'effectue avec la commande `route outside + adresse du réseau interne`, dans ce cas on attribue l'adresse par défaut 0.0.0.0 pour toute trafic qui vient du réseau interne se traduit à l'adresse 209.165.200.226

Alors on entre ici dans la configuration de NAT statique pour s'effectuer la traduction ; pour cela on crée un objet network qui va traduire toute adresse venant du réseau interne

```
asa(config-if)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
asa(config)#object network inside-net
asa(config-network-object)#subnet 192.168.1.0 255.255.255.0
asa(config-network-object)#nat (inside,outside) dynamic interface
asa(config-network-object)#end
asa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
   translate_hits = 0, untranslate_hits = 0
```

Si on teste le ping maintenant, il ne passera pas encore car on a besoin d'une configuration qui autorise le trafic icmp à passer, et ce sera avec la politique d'inspection ce qu'on voit dans la ligne de commande suivante ;

```
asa#conf t
asa(config)#class-map i
asa(config)#class-map inspec
asa(config)#class-map inspection-traffic
asa(config-cmap)#match default-inspection-traffic
asa(config-cmap)#ex
asa(config)#policy-map global_policy
asa(config-pmap)#class inspection_default
ERROR: % class map inspection_default not configured
asa(config-pmap)#ex
asa(config)#class-map inspection-traffic
asa(config-cmap)#ex
asa(config)#class-map inspection_default
asa(config-cmap)#match default
asa(config-cmap)#match default-inspection-traffic
asa(config-cmap)#ex
asa(config)#policy-map global_policy
asa(config-pmap)#class inspection_default
asa(config-pmap-c)#inspect icmp
asa(config-pmap-c)#ex
asa(config)#service
asa(config)#service-policy global_policy global
asa(config)#
```

On lance le ping cette fois avec la configuration de Class Map, Policy Map et service Policy, nous pouvons voir maintenant que c'est en fait de passage. On peut vérifier le succès de traduction avec la commande show Nat :

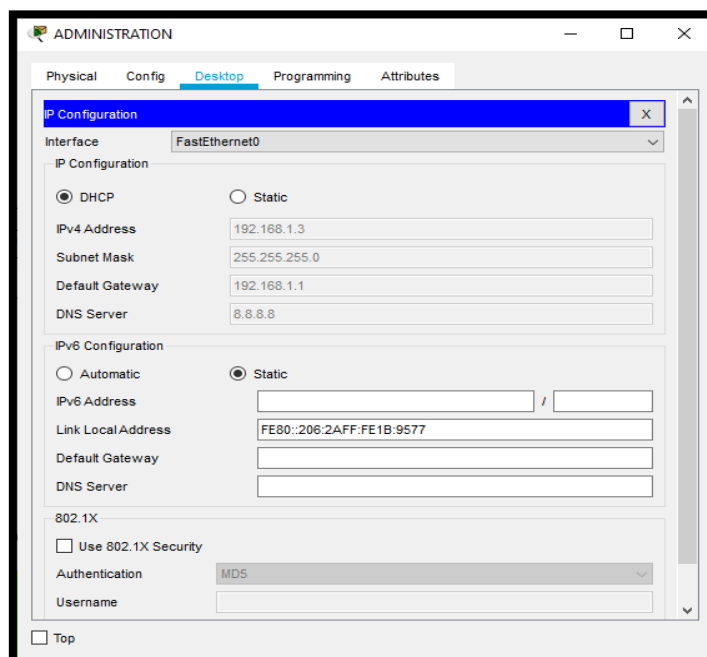
```
ASA(config)#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
  translate_hits = 2, untranslate_hits = 2
```

#### ✓ Etape 4 :

L'un des avantages de l'exécution de DHCP sur un pare-feu est qu'il ne nécessite aucun matériel supplémentaire (comme le fait un serveur Windows). De plus, l'exécution de DHCP sur un routeur peut faire économiser à votre organisation le coût d'un serveur DHCP dédié. Il fournit également DHCP localement sur chaque site, que le WAN soit ou non opérationnel. La configuration se met en ligne de commande suivante ;

```
ASA(config)#dhcpd add 192.168.1.2 inside
ASA(config)#dhcpd dns 8.8.8.8
ASA(config)#dhcpd dns 8.8.8.8 interface inside
ASA(config)#dhcpd enable inside
```

Les ordinateurs de réseau reçoivent dynamiquement l'adresse IP selon le DHCP configuré ;



La partie suivante est évidemment gérer le pare-feu depuis les deux ordinateurs d'administration ; le premier à l'interne du réseau comme une direction du centre, et le deuxième depuis un réseau extérieur au cas où il n'y a pas un expert technique à l'intérieur.

L'administration interne à l'adresse 192.168.1.3 tant que l'extérieur a 172.16.2.3.

On va utiliser le protocole SSH, puisqu'il est le plus sécurisé, et on fonde l'authentification AAA qui est basé sur l'authentification, autorisation et comptabilité.

Alors sur ASA, on va établir un nom d'utilisateur : admin, et un mot de passe : cisco, et autorise l'authentification AAA avec SSH.

```
ASA(config)#username greg password cisco
ASA(config)#
ASA(config)#
ASA(config)#
ASA(config)#aaa auth
ASA(config)#aaa authentication ?

configure mode commands/options:
  ssh      SSH
  telnet   Telnet
ASA(config)#aaa authentication ssh con
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#
```

Alors ici, seulement l'utilisateur « admin » a l'accès SSH au pare-feu afin de gestion.

Nous pourrions utiliser une clé cryptographique type RSA pour une sécurité mieux ;

```
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
```

Mais on réalise qu'il y a une clé par default déjà installé, alors on choisit de ne pas le remplacer (puisque on a juste dans un simulateur).

Maintenant on va spécifier les ordinateurs ou les adresse IP qui ont l'autorisation d'accès SSH au pare-feu. Par default, tous les hôtes sont refusés sauf ceux qui ont configurée comme suivant ;



```
ASA(config)#ssh 192.168.1.3 255.255.255.255 inside
ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
```

Ces deux lignes de commandes autorisent l'accès SSH aux ordinateurs d'administration (interne et externe) puisque leurs adresses sont 172.16.3.3 et 192.168.1.3

Pour tester l'accès, on tape sur les deux ordinateurs la ligne de commande :  
ssh -l admin [adresse de l'interface pare-feu]

- Ordinateur d'administration interne :

```
C:\>ssh -l admin 192.168.1.1
Password:

ASA>enab
Password:
ASA#
ASA#conf t
ASA(config)#
```

- Ordinateur d'administration externe :

```
[Connection to 209.165.200.226 closed by foreign host]
C:\>ssh -l admin 209.165.200.226
Password:

ASA>enab
Password:
ASA#conf t
ASA(config)#
```

#### ✓ Etape 5

Notre scénario ici, l'ordinateur d'administration externe a besoin d'accéder au serveur WEB situé dans la zone DMZ. Le serveur possède l'adresse 192.168.2.3

Si on ping au serveur depuis l'ordinateur, la destination sera inaccessible car les deux sont dans deux réseaux privés. Ainsi que le tableau de routage de R3 ne possède plus de réseau 192.168.2.0

```

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 172.16.3.1: Destination host unreachable.
Reply from 172.16.3.1: Destination host unreachable.
Reply from 172.16.3.1: Destination host unreachable.
Reply from 172.16.3.1: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

```

R3#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

    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.1.1.0/30 [110/128] via 10.2.2.2, 00:30:30, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.3.0/24 is directly connected, GigabitEthernet0/1
L       172.16.3.1/32 is directly connected, GigabitEthernet0/1
    172.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.20.1.0/24 is directly connected, GigabitEthernet0/0
L       172.20.1.1/32 is directly connected, GigabitEthernet0/0
    209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224/29 [110/129] via 10.2.2.2, 00:30:30,
Serial0/0/1

```

On établit premièrement la zone DMZ, puis on autorise le trafic arrivant d'ordinateur administration externe ; ICMP et TCP via l'adresse 209.165.200.227 puisque 209.165.200.226 et 209.165.200.225 sont déjà utilisée.

DMZ est un sous-réseau physique ou logique qui contient et expose les services externes d'une organisation à un réseau non fiable, généralement plus grand, tel qu'Internet. Le niveau de sécurité de DMZ entre 0 et 100 mais ni 0 ni 100. Alors la configuration sera comme suivant ;

```
asa(config)#interface vlan 3
asa(config-if)#ip add 192.168.2.1 255.255.255.0
asa(config-if)#no forward interface vlan 1
asa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
asa(config-if)#security-level 70
```

Si on tape la commande show switch vlan a nouveau on note ;

```
ASA(config-if)#show 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
3	dmz	down	

Le vlan DMZ est ajoutée, mais leur statut est éteint, alors on va affecter le port Et0/2 au vlan 3 (dmz) et active le vlan. Ainsi pour communiquer avec le serveur WEB, on besoin de donner une global adresse qui va mapper vers l'adresse de serveur. Puisque 209.165.200.226 et 209.165.200.225 sont déjà utilisée, alors 209.165.200.227 est disponible. Ça veut dire un nouvel objet qui va être mapper comme suivant ;

```
asa(config-if)#interface et0/2
asa(config-if)#switchport access vlan 3
asa(config-if)#object network dmz-server
asa(config-network-object)#host 192.168.2.3
asa(config-network-object)#nat (dmz,outside) static 209.165.200.227
asa(config-network-object)#ex
asa#
```

Si on essaie de tester le ping ; le trafic est toujours bloqué car le contrôle d'accès manquant. Alors on va établir les ACLs de trafic icmp et tcp ;

```
ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3
eq 80

ASA(config)#access-group OUTSIDE-DMZ in interface outside
ASA(config)#
```

## CHAPITRE 4 : TEST ET VALIDATION

### Test des fonctionnements de réseau

En premier lieu, le test sera effectué sur la communication entre les ordinateurs du réseau interne ainsi que leur communication avec les routeurs externe et la zone DMZ pour mesurer le temps minimum nécessaire pour envoyer la plus petite quantité possible de donner et recevoir une réponse.

Le premier test entre l'administration et les autres ordinateurs ;

- Administration – SRI 1

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Administration – SRI 2

```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Administration – MT 1

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=10ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

## Administration – MT 2

```
C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pour les tests des ordinateurs entre eux on les résume comme suivant ;

SRI 1 vers les autres								SRI 2 vers les autres							
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	SRI 1	SRI 2	ICMP		0.000	N		Successful	SRI 2	SRI 1	ICMP		0.000	N
	Successful	SRI 1	MT 1	ICMP		0.000	N		Successful	SRI 2	MT 1	ICMP		0.000	N
	Successful	SRI 1	MT 2	ICMP		0.000	N		Successful	SRI 2	MT 2	ICMP		0.000	N

MT 1 vers les autres								MT 2 vers les autres							
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	MT 1	SRI 1	ICMP		0.000	N		Successful	MT 2	SRI 1	ICMP		0.000	N
	Successful	MT 1	SRI 2	ICMP		0.000	N		Successful	MT 2	SRI 2	ICMP		0.000	N
	Successful	MT 1	MT 2	ICMP		0.000	N		Successful	MT 2	MT 1	ICMP		0.000	N

Au test suivant, on s'assure que la connectivité depuis le réseau interne au réseau externe passe, ainsi qu'avec la zone DMZ. On note ici que la connectivité se base sur le ping depuis l'interne vers l'externe et non pas l'inverse (au nom de la sécurité).

Puisque la connectivité entre les ordinateurs interne est parfaite, on choisit dans ce cas l'ordinateur d'administration, qui présente le réseau interne, pour tester la connectivité vers l'externe tandis que les autres ordinateurs ont le même résultat sauf l'accès de gestion qui est uniquement conçu pour l'administration.

Test de ping entre :

- Administration – R1 (209.165.200.226)

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=4ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

- Administration – R2 (10.1.1.2)

```
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=4ms TTL=253
Reply from 10.1.1.2: bytes=32 time=13ms TTL=253
Reply from 10.1.1.2: bytes=32 time=17ms TTL=253
Reply from 10.1.1.2: bytes=32 time=11ms TTL=253

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 17ms, Average = 11ms
```

- Administration – R3 (10.2.2.1)

```
C:\>ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:

Reply from 10.2.2.1: bytes=32 time=5ms TTL=252
Reply from 10.2.2.1: bytes=32 time=3ms TTL=252
Reply from 10.2.2.1: bytes=32 time=12ms TTL=252
Reply from 10.2.2.1: bytes=32 time=13ms TTL=252

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 13ms, Average = 8ms
```

- Administration – Serveur DMZ (192.168.2.3)

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=3ms TTL=127
Reply from 192.168.2.3: bytes=32 time=12ms TTL=127
Reply from 192.168.2.3: bytes=32 time=14ms TTL=127
Reply from 192.168.2.3: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 14ms, Average = 9ms
```



On passe au test sur la connectivité de l'ordinateur d'administration externe vers le pare-feu et la zone DMZ ;

- Admin externe – Pare-feu (209.165.200.227)

On prend l'adresse 209.165.200.227 à pinger à cause de l'indisponibilité d'adresse de l'interface Et0/0 (209.165.200.226) pour être une interface d'accès à la zone DMZ

```
C:\>ping 209.165.200.227

Pinging 209.165.200.227 with 32 bytes of data:

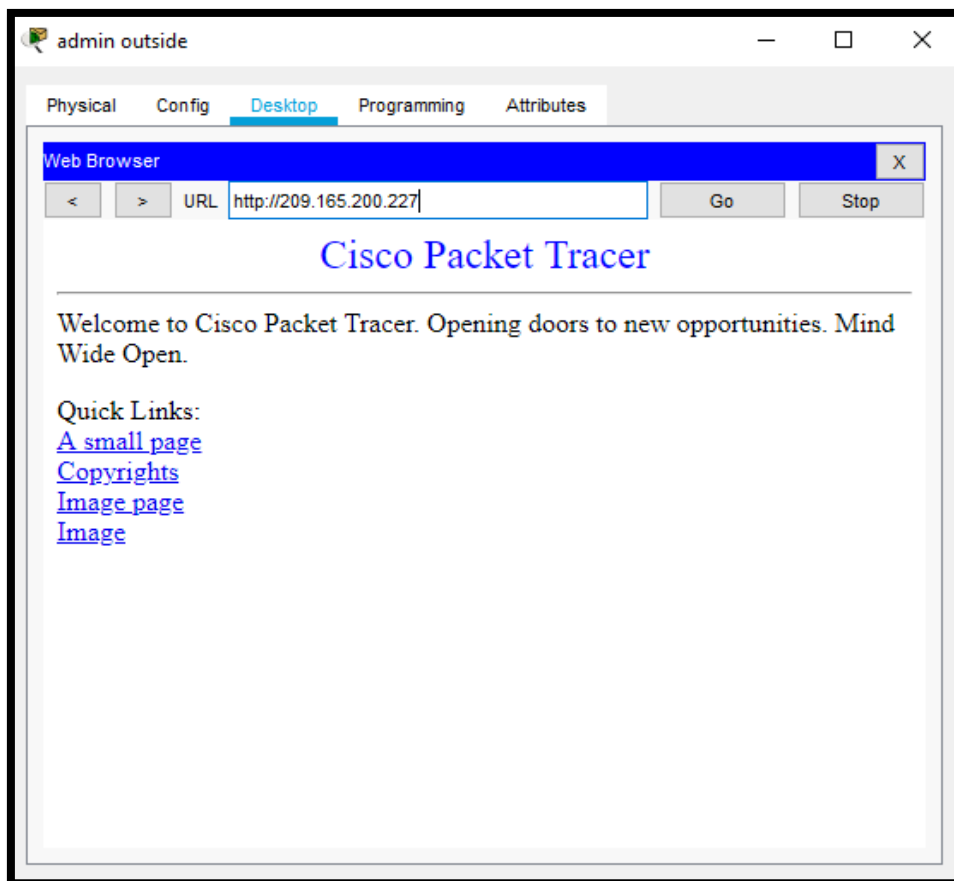
Reply from 209.165.200.227: bytes=32 time=3ms TTL=124
Reply from 209.165.200.227: bytes=32 time=17ms TTL=124
Reply from 209.165.200.227: bytes=32 time=14ms TTL=124
Reply from 209.165.200.227: bytes=32 time=13ms TTL=124

Ping statistics for 209.165.200.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 17ms, Average = 11ms
```

- Admin externe – Zone DMZ

La zone DMZ est un réseau privé, alors pour accéder, On besoin d'une adresse globale qui peut être traduite en adresse privée, cette étape est déjà mentionnée précédemment, donc l'adresse 209.165.200.227 était choisi pour être cette adresse globale. Pour cela, lors de test de ping on test sur 209.165.200.227.

A ce moment, on passe au dernier teste de validation qui concerne l'accès au WEB situé dans la zone DMZ. On a testé le ping qui a passé parfaitement, mais le teste suivant sera en accédant au navigateur et tapant l'adresse 209.165.200.227 puisqu'elle est l'adresse globale qui nous permettra d'accéder au serveur WEB. Le teste alors, sera au niveau d'administration externe ;



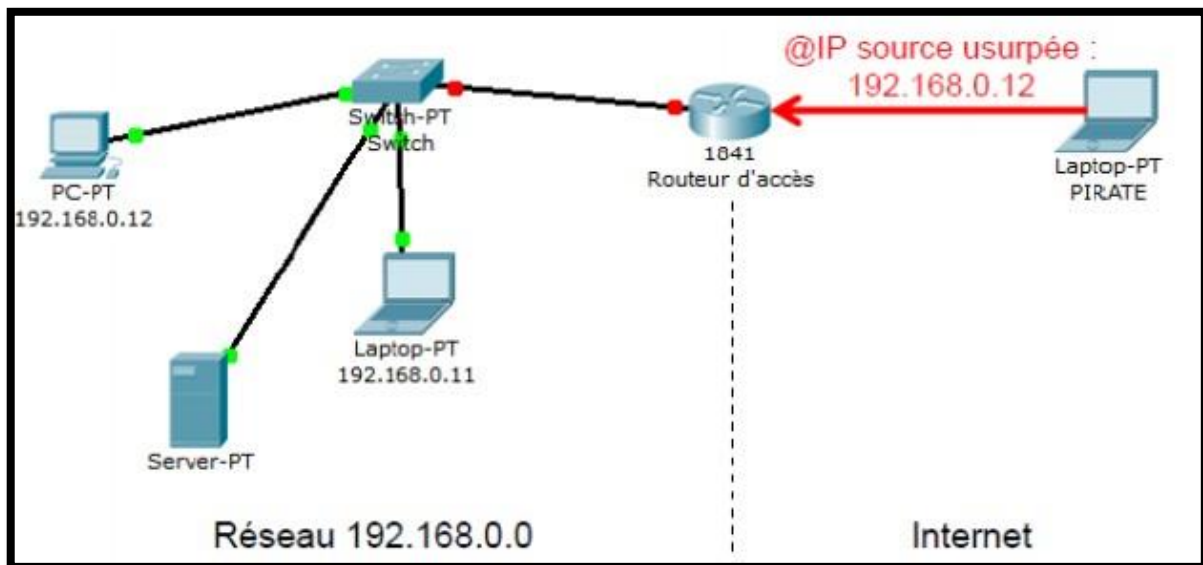
## Types des attaques probables

Les attaques peuvent être classées en deux grandes catégories : les techniques d'intrusion dont l'objectif principal est de s'introduire sur un réseau pour découvrir ou modifier des données et les dénis de service (DoS : Denial of Service attaque) qui ont pour but d'empêcher une application ou un service de fonctionner normalement. Cette deuxième catégorie agit donc sur la disponibilité de l'information tandis que la première concerne essentiellement la confidentialité et l'intégrité.

Ces techniques peuvent être classées suivant le niveau d'intervention :

- **L'usurpation d'identité, le vol de session, le détournement ou l'altération de messages (spoofing) ;**

L'attaque basique de ce type est la falsification d'adresse IP : l'agresseur prétend provenir d'une machine interne pour pénétrer sur le réseau privé. Cette attaque peut être simplement bloquée avec un firewall au niveau du routeur d'accès qui éliminera les paquets entrants avec une IP source interne.



Le web spoofing est une version élaborée de l'IP spoofing : il s'agit de remplacer un site par une version pirate du même site. Cette technique est notamment utilisée dans la dernière étape du phishing. La falsification se déroule en plusieurs temps : - Amener la victime à entrer dans le faux site web (grâce à l'utilisation du DNS spoofing par exemple) - Intercepter les requêtes HTTP - Récupérer les vraies pages web et modifier ces pages - Envoyer de fausses pages aux victimes.

Pour cela, on a utilisé l'authentification AAA avec SSH, seuls qui ont une adresse spécifique et nom d'utilisateur spécifiques peuvent accéder au Pare-feu, dans notre cas.

- **L'écoute du trafic sur le réseau (sniffing) ;**

Sur la plupart des réseaux, les trames sont diffusées sur tout le support (câble Ethernet, transmission radio Wifi, ...). En fonctionnement normal, seul le destinataire reconnaît son adresse et lit le message. La carte Ethernet ou Wifi d'un PC peut être reprogrammée pour lire tous les messages qui traversent le réseau (promiscuous mode).

La limite dans ce cas est le dispositif d'interconnexion utilisé sur le LAN ou le segment de LAN (switch, routeur). Les hackers utilisent des sniffers ou analyseurs réseau qui scannent tous les messages qui circulent sur le réseau et recherchent ainsi des identités et des mots de passe.

La commande « tcpdump » sous GNU/Linux (bien entendu !) et le logiciel « Wireshark », par exemple permettent le sniffing.

Exemple d'activation du promiscuous mode (sous GNU/Linux) :

```
ifconfig eth0 promisc ou ip link set wlan0 promisc on
```

Pour la désactivation :

```
ifconfig eth0 -promisc ou ifconfig eth0 promisc off
```

Afin de défense cette attaque, on a attribué les ACLs sur le Pare-Feu ce qui lui charge de filtrer les accès entre l'Internet et le LAN. Le firewall, qui est souvent un routeur intégrant des fonctionnalités de filtrage, possède autant d'interfaces que de réseaux connectés. Suivant la politique de sécurité, le filtrage est appliqué différemment pour chacune des interfaces d'entrée et de sortie.

## Test des attaques

- L'usurpation d'identité ;

Le test se base sur essayer d'accéder aux gestions du Pare-Feu autant qu'administration. Le trafic doit être bloqué grâce aux sécurités contre les hôtes externes. On test l'attaque depuis l'ordinateur de réseau externe en accédant Pare-feu comme un administrateur ;



```
C:\>ssh -l admin 209.165.200.227

% Connection timed out; remote host not responding
C:\>
```

On reconnait ici qu'on n'a pas le droit totalement d'accéder aux gestions du Pare-Feu depuis une autres hôtes hors les deux ordinateurs autorisés

- L'écoute du trafic sur le réseau

Ce test évalue la sécurité finale du Pare-feu ainsi que la zone DMZ, alors on va établir les ACLs pour bloquer toute Traffic externe non connue qui veux accéder à l'interface du Pare-Feu. Le test est effectué sur l'ordinateur externe avec la commande de ping qui affiche la connectivité entre eux.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Failed	PC0	ASA1	ICMP		0.000	N

## CONCLUSION

En conclusion, Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** » (le terme *isolation* est parfois également utilisé). Ainsi que Les défenses matérielles qui interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de données centralisée sur le disque dur d'un serveur par exemple), sur les médias servant à transporter cette information (sécurisation du réseau sans fil) et sur les équipements intermédiaires traversés lors du transport (utilisation d'un firewall installé sur le routeur d'accès).

Cependant, le problème est de correctement définir les risques engendrés par la criminalité informatique. Il faut pour cela avoir une vision globale du problème et connaître globalement les techniques utilisées par les nouveaux flibustiers. Il s'agira ensuite d'analyser correctement les vulnérabilités propres à chaque site, de définir le niveau de sécurité requis et enfin de mettre en place une politique de sécurité acceptable.

Lors de cette étape il faut bien veiller à examiner le problème tant du côté de l'administrateur que de celui du simple utilisateur afin de ne pas en créer de nouveaux.

