D

Conception et mise en place d'une architecture de sécurité des services Intranet / Internet

Equipe Firewalling

A nos très chers parents…

A toutes nos familles…

A tous nos amis…

A La FST…

Avant propos

« Agir d’abord, rectifier ensuite s’il y a lieu, reprendre tout à zéro s’il le faut, mais ne jamais rester inactif à la recherche du parfait ».

Jean Cocteau

Remerciements

C’est une habitude saine que de rendre mérite, au début d’un tel travail, à tous ceux qui ont contribué à le rendre possible.

Le présent message traduit mon sincère reconnaissance et gratitude à mon encadrant externe Mr. Issam collaboration, et nos saisiront l’occasion pour les félicités pour son dynamismes, sa rigueur et son ouverture d’esprit, faisant de lui un exemple du jeune cadre motivé, et doté d’une mobilité et disponibilité remarquable. On vous remercie pour vos judicieux conseils et pour vos directives précieuses qui m’a été d’un appui considérable dans notre démarche.

On ne saurait oublier dans nos remerciements tout le cadre professoral de la FST, pour la formation qu’il mon a prodigué.

On exprime notre gratitude à tous les membres du jury pour avoir accepté de juger nous travail.

Cela va de soit, On remercie évidemment nos familles pour leur irremplaçable et inconditionnel soutien. Ce travail est un peu le leur aussi.

Et merci à toutes les personnes qui nous à aider d’une manière ou d’une autre.

Résumé

Notre projet a pour but de nous permettre de pratiquer nos acquis en réalisant les taches suivantes :

- Réalisation du plan d’adressage pour l’ensemble de l’infrastructure en minimisant le gaspillage d’adresses (adressage VLSM)

- Configuration du routeur lié au nuage internet

- Configuration du PIX 525

- Configuration du switch pour la création des vlans de la partie DMZ

Abstract

The purpose of our project is to enable us to practice our assets by carrying out the following spots:

- Realization of the plan of addressing for the whole of the infrastructure by minimizing the wasting of addresses (addressing VLSM)

- Configuration of the router related to cloud Internet

- Configuration of the PIX 525

- Configuration of the switch for the creation of the vlans of part DMZ

Sommaire

Introduction

La sécurisation des systèmes informatiques d'une entreprise ou d'une administration commence avec la sécurisation au niveau réseau. Le firewall est à ce sujet un outil indispensable. En effet son rôle est d'assurer un périmètre de protection entre le réseau interne à l'entreprise et le monde extérieur. Basé sur des technologies d'analyse des paquets à l'entrée du périmètre protégé, le firewall permet ou interdit l'accès de et vers ce périmètre.
Composé d'équipements matériels et/ou logiciels, le firewall va réaliser les tâches suivantes:
bloquer l'accès à des services non autorisés,
interdire l'accès à des systèmes,
protéger contre les attaques de type DoS (Deni de service),
etc.
Les firewall peuvent intégrer des techniques de détection d'intrusions et peuvent envoyer des alertes afin de prévenir les équipes de surveillance technique. Ces équipements prennent en compte un ensemble de règles qui doivent être définies en fonction des besoins d'une entreprise ou d'une administration.

Qu'est-ce qu'un firewall?

Un pare-feu est un outil utilisé afin d'empêcher tout accès non autorisé entre deux ou plusieurs réseaux. Aujourd'hui, nous avons trois types des technologies de pare-feu:
-Accès listes
-Stateful Inspection
-Proxy
* Le PIX pouvez utiliser les deux.

Qu’est ce qu’un PIX?

Cisco PIX est le pare-feu, qui utilise un système d'exploitation appelé finesse.
Les quatre principaux avantages du PIX sont les systèmes embarqués (qui est très "sécurisée"), l'ASA (Adaptive Security Algorithme), la cutthrough procuration et les options
disponibles pour la redondance.
Six modèles de pare-feu PIX sont disponibles: Cisco PIX 501.506.515.520.525.535

Les différentes catégories de firewall

Depuis leur création, les firewalls ont grandement évolué. Ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. De ce fait, il existe maintenant différentes catégories de firewall. Chacune d'entre-elles disposent d'avantages et d'inconvénients qui lui sont propre. Le choix du type d'un type de firewall plutôt qu'un autre dépendra de l'utilisation que l'on souhaite en faire, mais aussi des différentes contraintes imposées par le réseau devant être protégé.

Firewall sans états (stateless)

Ce sont les firewall les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquet indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control Lists).
Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination.
Les limites (à titre d’exemple):
Lors de la création des règles de filtrage, il est d'usage de commencer à spécifier que le firewall ne doit laisser passer aucun paquet. Ensuite, il faut ajouter les règles permettant de choisir les flux que nous souhaitons laisser passer. Il suffit alors d'autoriser l'ouverture des ports des serveurs devant être accessible depuis l'extérieur. Mais les connexions des postes vers l'extérieur poseront problèmes. Effectivement, il faudrait autoriser les ports utilisés par les postes clients lors des connexions vers les serveurs, ceci implique donc d'ouvrir tous les ports supérieurs à 1024. Ceci pose donc un réel problème de sécurité.

Firewall à états (stateful)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Les firewalls à états prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection. De ce fait, ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session
Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall. Les firewalls à états sont alors capables de déceler une anomalie protocolaire de TCP. De plus, les connexions actives sont sauvegardées dans une table des états de connexions. L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront acceptés.
Les limites (à titre d’exemple) :
La première limite de ce type de firewall ce situe au niveau du contrôle de la validité des protocoles.
Effectivement, les protocoles « maisons » utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du fonctionnement de ces protocoles particuliers.
Ensuite, il existe un coût supplémentaire lors de la modification des règles du firewall. Il faut que les firewalls réinitialisent leurs tables à état.
Pour finir, ce type de firewall ne protège pas contre l'exploitation des failles applicatives, qui représentent la part la plus importante des risques en terme de sécurité.

Firewall applicatif

Les firewall applicatif (aussi nommé pare-feu de type Proxy ou passerelle applicative) fonctionne sur la couche 7 du modèle OSI. Cela suppose que le firewall connaisse l'ensemble des protocoles utilisés par chaque application. Chaque protocole dispose d'un module spécifique à celui-ci. C'est à dire que, par exemple, le protocole HTTP sera filtré par un processus Proxy HTTP.
Ce type de firewall permet alors d'effectuer une analyse beaucoup plus fine des informations qu'ils font transiter. Ils peuvent ainsi rejeter toutes les requêtes non conformes aux spécifications du protocole. Ils sont alors capables de vérifier, par

exemple, que seul le protocole HTTP transite à travers le port 80. Il est également possible d'interdire l'utilisation de tunnels TCP permettant de contourner le filtrage par ports. De ce fait, il est possible d'interdire, par exemple, aux utilisateurs d'utiliser certains services, même s'ils changeant le numéro de port d'utilisation du services (comme par exemple les protocoles de peer to peer).
Les limites (à titre d'exemple) :
La première limitation de ces firewalls réside sur le fait qu'ils doivent impérativement connaître toutes les règles des protocoles qu'ils doivent filtrer. Effectivement, il faut que le module permettant le filtrage de ces protocoles soit disponible.
Ensuite, ce type de firewall est très gourmand en ressource. Il faut donc s'assurer d'avoir une machine suffisamment puissante pour limiter les possibles ralentissements dans les échanges.

Firewall authentifiant

Les firewall authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à travers le filtre IP. Il est alors possible de suivre l'activité réseau par utilisateur.
Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise. Il existe plusieurs méthodes d'association. Par exemple authpf, qui utilise SSH, ou encore NuFW qui effectue l'authentification par connexion.

Firewall personnel

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

PIX

La célèbre société Cisco, plus connu pour ses routeurs, à pr
matériels nommés PIX (Private Internet eXchange).
Ces firewalls sont des plateformes complètes basées sur ur
noyau propriétaire de Cisco. Ce sont des firewalls à état

(Stateful) utilisant l'algorithme de Cisco, l'ASA (Adaptive Security Algorithm). Ils disposent, entre autre, d'un Client/serveur DHCP, d'une gestion du PAT (Translation d'Adresse par Port) et NAT (Translation d'Adresse IP), de la prise en compte des réseaux privés virtuel (VPN) avec la gestion d'IPSec. Plusieurs classes de PIX existe, du plus simple pour les petites entreprise, au plus évolué pour les entreprises tel que les fournisseurs d'accès à Internet

Chapitre1

Cadre général du projet

Un projet de fin d’études, quels que soient sa taille et ses objectifs, peut être comparé à un organisme vivant : sa réalisation obéit à des Xconditions et des contraintes susceptibles de lui permettre d’évoluer, voire de muer en interaction directe avec les exigences sans cesse évolutives. Ce qui lui impose une méthodologie précise et une documentation conséquente pour lui assurer un caractère ouvert et évolutif et lui garantir une certaine pérennité.

La réponse à ces exigences étant, en partie, la vocation de ce document, on tentera dans ce chapitre de présenter au lecteur les éléments lui permettant d'appréhender de manière convenable ce projet.

Après une présentation de la FST, il conviendra donc de décrire le projet ainsi que les différentes étapes de son déroulement.

1. Fiche technique :

Raison social :

Forme juridique :

P.D.G :

Secteur d’activité :

Date de constitution :

Investissement globale :

Capital social :

Chiffres d’affaires :

Siège social :

Site Internet :

2. Cahier des charges

Cette section a pour but d’établir les spécifications du système à implémenter. A cette fin, nous nous efforcerons de définir aussi précisément que possible les besoins des futurs utilisateurs du système. Ce préalable nous permettra de détailler le cahier des charges en

inventoriant chaque fonctionnalité du programme. Enfin, nous terminerons en déterminant le planning des tâches à accomplir dans le cadre de ce stage ainsi que les fonctionnalités qu'il serait souhaitable d'implémenter par la suite.

- **Les utilisateurs et leurs attentes :**

Afin de définir précisément les fonctionnalités que devra offrir l'outil, une première analyse des besoins a été menée lors de réunions au cours desquelles les différents utilisateurs potentiels ont eu l'occasion d'évoquer leurs attentes dans le cadre de leurs missions respectives. Les utilisateurs potentiels peuvent être classés en fonction de leur poste de travail ; leurs besoins étant directement liés à ce dernier.

⇨ **Les fonctionnalités à implémenter :**

Typologie des besoins	Description détaillée des fonctionnalités
Localiser des sites	Zoomer, dézoomer, se déplacer, trouver un emplacement rapidement (raccourci), échelle.
Visualiser	Offrir plusieurs modes de visualisation alternatives (niveau de détail souhaité, choix des données à afficher, etc.)
Accéder aux données	Obtenir des informations techniques sur l'équipement sélectionné
Effectuer des mesures	Déterminer une distance, calculer une surface, afficher des statistiques relatives à la zone sélectionnée

Tableau 1: Liste des fonctionnalités à implémenter.

⇨ **Planning des tâches**

Semaines 1 :

- Prise de contact avec l'environnement professionnel
-

Semaines 2 :

- Recherche documentaire sur les systèmes d'information, le plan technique de la société et leur architecture afin d'envisager plus concrètement l'intégration d'un tel outil.
- Etude de l'existant applicatif corrélé au sujet du stage.
- Validation d'un premier projet de cahier des charges avec le prof Issam.
- Préparation de l'environnement de travail (Hardware, logiciels et drivers à installer, plugins nécessaires).

Semaines 3 :

- Schématisation de l'architecture du plan du travail à livrer.
- Correction du pré-rapport en fonction des remarques formulées par nos encadrant.

Chapitre2

Présentation du projet

Notre projet consiste à l'Etude et la mise en place de la plate-forme Firewalling.

Etudes des plates-formes :

⇨ **Etude du réseau**

Durant cette première phase, nous sommes amenées à étudier l'architecture du réseau on lançant son plan d'adressage réseau

⇨ **Contexte général du projet**

La mise en place de la Plate Forme Firewalling. est un besoin de la société qui permettra la diffusion en toute sécurité de l'information.

C'est dans ce contexte général que vient le besoin de se débarrasser des problèmes des vieilles architectures et tendre vers des nouvelles solutions.

Ainsi ce projet est lancé pour réaliser une plate forme solide évolutive dont les principaux sont :

- Backbone qualité du service et sécurité
- Redondance accès BLR
- Mise en place d'une plate-forme data et migration des serveurs

⇨ **Planification du projet**

La planification du projet doit bien entourer toutes les étapes d'étude et réalisation, Le projet étant réparti sur plusieurs sens nous a bien poussé à adopter une planification pour bien cerner les étapes de réalisations.

Cette planification est conforme aux phases du projet ainsi que les objectifs attendus, au cours de cette période, un ensemble de points de contrôle est mis en place pour bien établir un suivi du déroulement des étapes de projets.

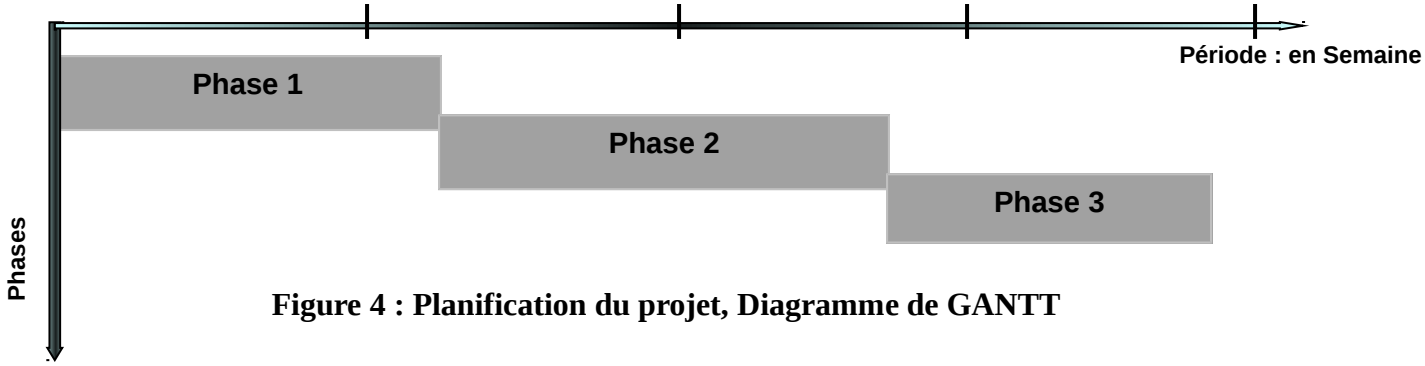


Figure 4 : Planification du projet, Diagramme de GANTT

- **Phase 1 :**

Il s’agit d’une première phase, mais l’une des plus importantes, elle permet de préparer un environnement convenable pour la bonne réalisation de projet, tout en évaluant la faisabilité et les contraintes attendues.
Cette phase comporte en principe les taches suivantes :

- Étude de l’existant.
- Ingénierie détaillé de la mise en place de la Plate Forme Firewalling.

- **Phase2 :**

La deuxième étape est celle de l’exploitation de l’étude établie en première partie et la réalisation technique des étapes de Projet.

Une évaluation des résultats est prévue à la fin de cette étape pour visualiser les difficultés de réalisation. Cette phase comporte en principe les taches suivantes :

- Adressage ip.
- Installation et configuration des équipements.
- Tester les configurations et les équipements.

- **Phase 3 :**

La dernière phase a pour but l’exploitation de la réalisation de la Plate Forme. Cette phase comporte en principe les taches suivantes :

- Fin de projet
- Test

Conclusion

Il s’agissait dans ce chapitre d’une présentation brève de l’ensemble des étapes du projet, après avoir mis la main sur l’environnement du travail et les caractéristiques de l’organisme d’accueil.

Chapitre3

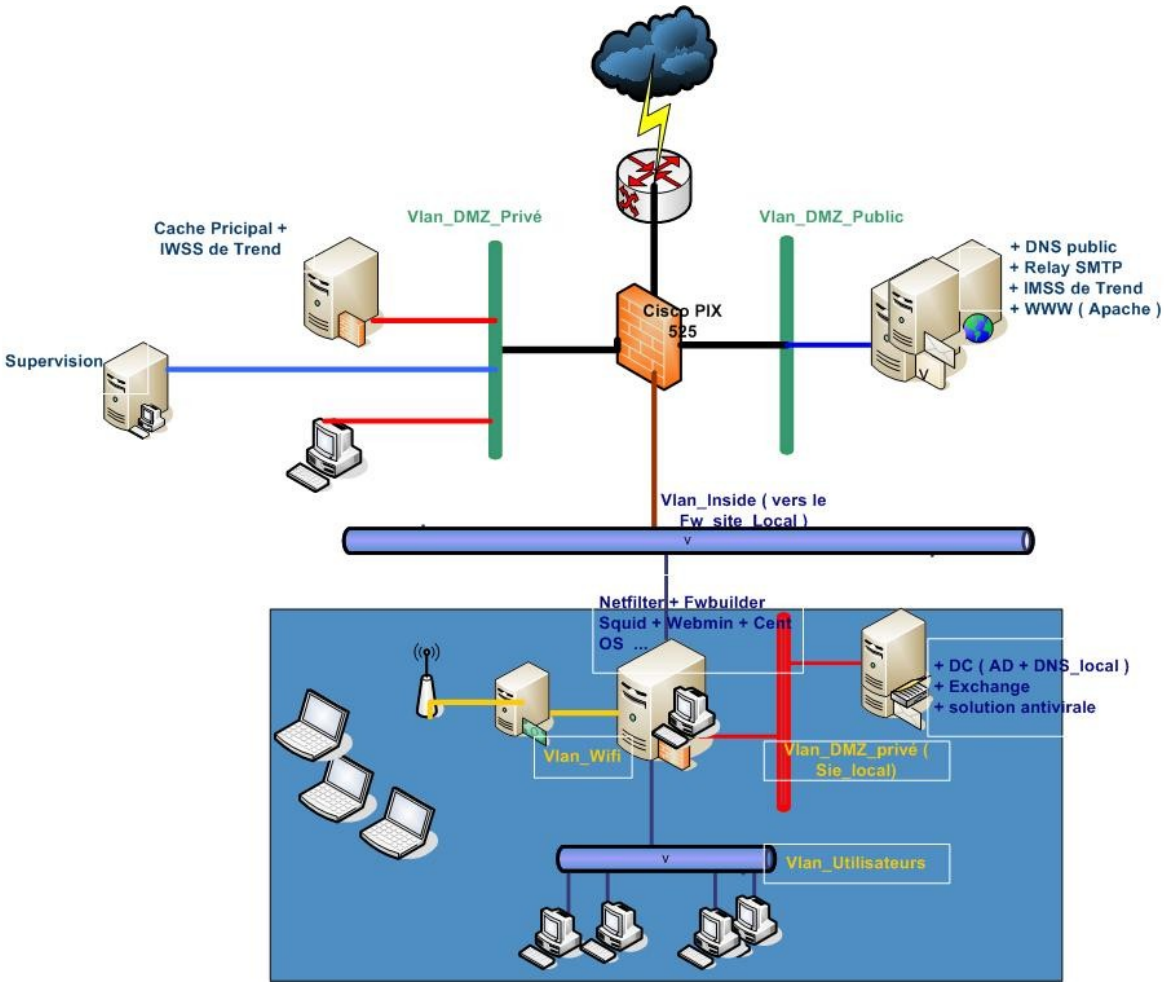
Plan d'adressage :

Il s'agit d'effectuer les opérations suivantes :

- Identifier les sous réseaux de l'infrastructure réseau
- Distinguer les sous réseaux à adresses publiques de ceux à adresses privées
- Définir la taille de chaque sous réseau concernant le nombre d'adresses Ip qui lui seront allouées, en tenant compte d'une éventuelle extension future.

Remarque :

Il faut minimiser le gaspillage d'adresses IP
Schéma du réseau :



En analysant le plan d'adressage adopté en classe on peut émettre les constatations suivantes :

- Le nombre d'adresses allouées à chaque sous réseau n'est pas justifié : par exemple le sous réseau PIX (DMZ privé) comporte 100 adresses alors que PIX (DMZ public) n'en compte que 6 …etc.

- Les plages d'adresses des sous réseaux publiques doivent être contigües afin d'être résumées par une adresse de sous réseau publique global.

- Les plages d'adresses des sous réseaux privés doivent être contigües afin d'être résumées par une adresse de sous réseau privé global.

Les plages des sous réseaux n'étant pas contigües nous obligent à utiliser un sous réseau global anormalement grand.
On peut apporter les améliorations suivantes au plan d'adressage :

Réseau	Nombre d'adresses max	Adresse sous réseau / Masque	Plage d'adresses IP
Routeur Outside	2	10.10.61.24 / 30	10.10.61.25 à 10.10.61.26
Routeur Inside	6	10.10.61.16 / 29	10.10.61.17 à 10.10.61.22
PIX Outside	6	10.10.61.16 / 29	10.10.61.17 à 10.10.61.22
PIX Inside	6	10.10.61.8 / 29	10.10.61.9 à 10.10.61.14
PIX (DMZ public)	6	10.10.61.0 / 29	10.10.61.1 à 10.10.61.6
PIX (DMZ privé)	100	172.16.0.0 /25	172.16.0.1 à 172.16.0.126
Lan (DMZ privé Local)	14	172.16.0.128 /28	172.16.0.129 à 172.16.0.142
Vlan_Wifi(users WIFI)	100	172.16.1.0 /25	172.16.1.1 à 172.16.1.126
Vlan_Utilisateurs	100	172.16.1.128 /25	172.16.1.129 à 172.16.1.254

Les sous réseau publique global est : 10.10.61.0 / 27. Le gaspillage d'adresses est minim.
Les sous réseau privé global devient : 172.16.0.0 /23. Le gaspillage d'adresses est minim.
Alors qu'il était : 172.16.0.0 /13. Le gaspillage d'adresses est important.
Les ports réseaux des équipements auront les adresses IP suivantes :

Routeur et PIX :

Réseau	Adresse IP
Routeur (Outside)	10.10.61.26/30
Routeur(Inside)	10.10.61.22/29
Pix (Outside)	10.10.61.17/29
Pix(DMZ Public)	10.10.61.6/29
Pix(DMZ Privé)	172.16.0.126/25
Pix(Inside)	10.10.61.14/29

Serveurs :

Serveur	Adresse IP	Passerelle
MX1	10.10.61.1/29	Prix (DMZ Public)
DNS Public	10.10.61.2/29	Prix (DMZ Public)
WEB	10.10.61.3/29	Prix (DMZ Public)
FTP	10.10.61.4/29	Prix (DMZ Public)
Cache Principal	172.16.0.1/25	Prix (DMZ Privé)
DC	172.16.0.129 /28	172.16.0.142
Zimbra	172.16.0.130 /28	172.16.0.142
Portail captif (Outside) ->Lan users	172.16.1.129	
Portail captif (Inside)->WIFI	172.16.1.1	
FW site (Outside)	10.10.61.10/29	
FW site (DMZ Privé Local)	172.16.0.129 /28	

Diagramme de flux :

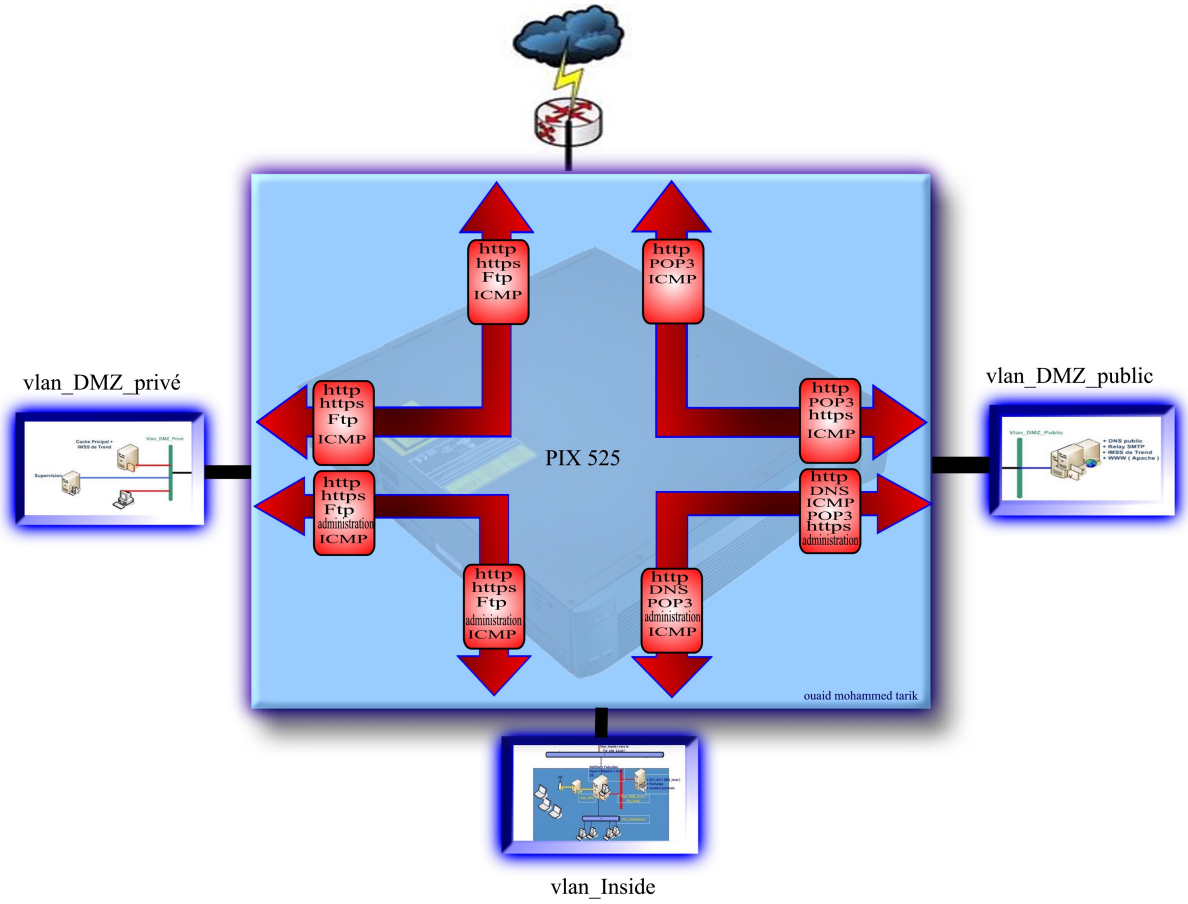


Diagramme de flux

vers ========== == de	Internet	Vlan DMZ public	Vlan Inside	Vlan DMZ privé
Internet		http ; https ; POP3		http ; https ; ftp
Vlan DMZ public	http ; POP3 ; https		http ; https ; ftp ; administration	
Vlan Inside		http ;dms ;icmp; pop3 ;https ; administration		http ; https ; ftp ; administration
Vlan DMZ privé	http ; ftp ; https		http ;DNS ; POP3 ; administration	

Chapitre5

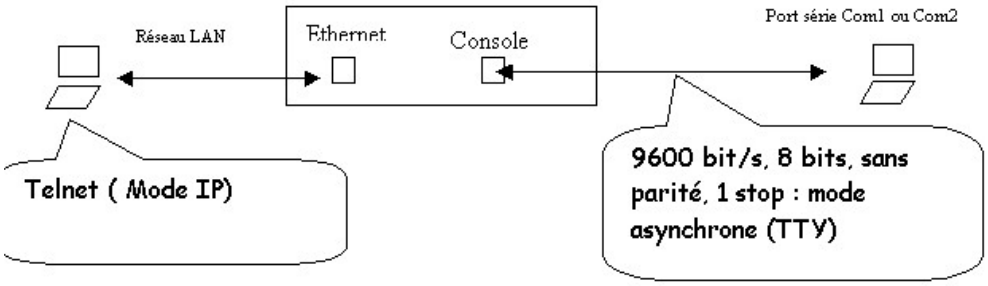
Configuration du routeur CISCO 801 et switch

Configuration du routeur CISCO 801

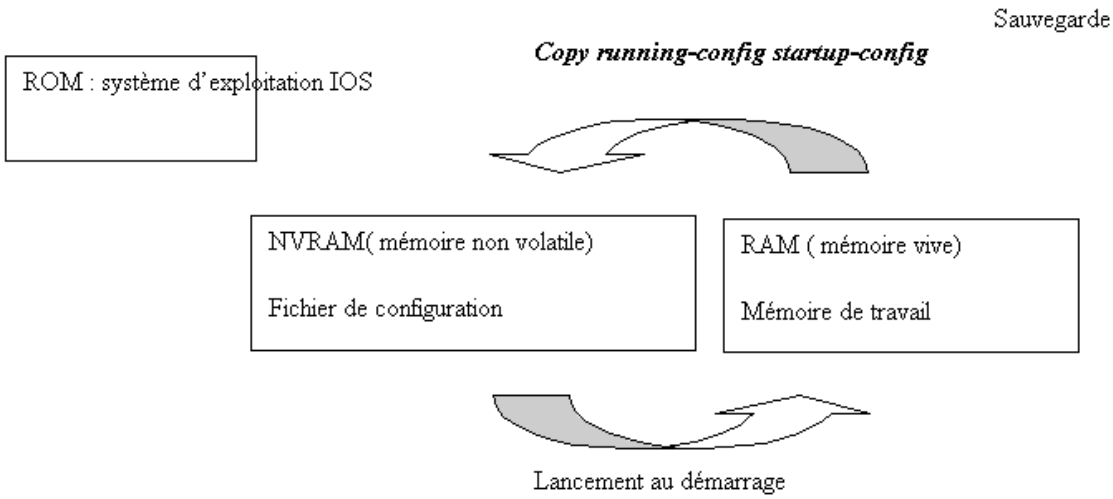
Caractéristiques de la gamme des routeurs cisco série 800 :

	Ports fixes LAN	Ports fixes WAN
Cisco 801	*1 port Ethernet*	*1 port RNIS BRI (S/T)*
Cisco 803	*4 ports Ethernet*	*1 port RNIS BRI (S/T)* 2 ports analogiques (POTS)
Cisco 805	*1 port Ethernet*	*1 port série (jusqu'à 512 Kbps)*
Cisco 827	*1 port Ethernet*	*1 port ADSL*

. Accès au routeur :



Mémoire des routeurs Cisco :



Initialisation du routeur via le port console :

- **Utiliser la fonction émulation de terminal (hyperterminal de windows).dans notre cas on a utilise secure crt**
- **Mettre le routeur sous tension.**
- **le routeur a demerae avec le mode setup**

II) Nommage et la sécurisation du routeur :

Hostname ISRS-router

Enable password cisco

III) Désactivation du débogage :

Via la commande : no logging consol 0

IV) Etiquetage des interfaces :

Interface ethernet 0

Description interne

Ip addresse 10.10.61.22 255.255.255.248

No shut down

Test d'interface via le ping : réussi

Interface ethernet 1

Description interne

Ip addresse 10.10.60.254 255.255.255.0

No shut down

Test d’interface via le ping : réussi

Ip root 0.0.0.0.0.0.0.0 10.10.60.1

Ip deffault getway 10.10.60.1

PS : problème rencontré :

Erreur d’adressage donnée par le chef du projet à bloqué le travail pour une durée de 30 minute .

Configuration du switch :

connecte le cable console au switch

: utilisation du hyper terminal secure crt afin d’y acceder

tape Conf t puis enter

: tape Int vlan 1 puis enter

: tape Ip address 10.10.60.252 255.255.255.0 puis enter

tape No shutdown puis enter

Création des vlans

1- VLAN5 description outside

2- Interface fastethernet0/2 -6

3- Switchport mode access

4- VLAN4 description inside

5- Interface fastethernet0/8 – 12

6- Switchport mode access

7- VLAN3 description DMZ PRIVé

8- Interface fastethernet0/14 - 18

9- Switchport mode access

10- VLAN2 description DMZ PUB

11- Interface fastethernet0/20 - 24

12- Switchport mode access

Chapitre5

Configuration du Pix :

Pré-configuration:

Avant de commencer, nous devons déterminer des choses: tous les exemples vont utiliser cette topologie de réseau:

Internet

|

DMZ Public -- Firewall -- DMZ Privé

|

Inside Network

Grâce à ces adresses IP:

Inside network 10.10.61.0/29 – Firewall Inside IP: 10.10.61.1
DMZ Network Public 10.10.61.0/29 - Firewall DMZ Public IP: 10.10.61.14
DMZ Network Privé 172.16.2.0/25 - Firewall DMZ Privé IP: 172.16.2.1
Outside network 10.10.61.0/29 – Firewall Outside IP: 10.10.61.17
Default route 10.10.61.22

Avant de commencer:

Avant de commencer, nous devons nous rappeler que sur le PIX Ethernet0 est l'interface de l'extérieur et de la ethernet1 est L'intérieur de l'interface. L'interface à l'extérieur de la sécurité

niveau de zéro et à l'intérieur de 100. Tout le trafic à partir d'une interface de sécurité de niveau inférieur à un niveau élevé de sécurité niveau est refusé (sauf si autorisé par une liste d'accès ou conduit). Circulation d'un haut niveau de sécurité à un moindre niveau de sécurité est toujours permis (à moins que refusé par un access-list).

Configuration du Pix :

1. **Insertion de l'IOS de PIX .**

Premièrement nous avant besoins de mettre une adresse sur l'interface de PIX , et une autre sur le PC dans la même plage, et relions les deux avec un câble réseau pour qu'il ont puisse communiqué, après cette opération en fait un test de ping pour être sur que la communication passe entre les deux Ci-dessous la configuration injecté :

```
pixfirewall# SHOW ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Ethernet1              inside              192.168.1.1     255.255.255.0   CONFIG
Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Ethernet1              inside              192.168.1.1     255.255.255.0   CONFIG
```

```
pixfirewall# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
pixfirewall#
```

- Après en a besoin de supprimer l'ancien IOS et insérer la nouvel version de l'IOS ci-dessous la configuration :

pixfirewall# copy tftp fl

pixfirewall# copy tftp flash:

Address or name of remote host []? 192.168.1.3

Source filename []? pix723.bin

Destination filename [pix723.bin]?

Accessing

tftp://192.168.1.3/pix723.bin...!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

Writing file flash:/pix723.bin...

!!

!!

!!

!!

!!

!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!!!!!!
8386560 bytes copied in 111.500 secs (75554 bytes/sec)
pixfirewall# sh fla
pixfirewall# sh flash:
Directory of flash:/

5   -rw- 8386560   09:08:03 Mar 22 2009 pix723.bin

16128000 bytes total (7739392 bytes free)

2. Insertion de l'IOS de PIX et de l'ASDM.

pixfirewall# copy tftp flash:
Address or name of remote host [192.168.1.3]?
Source filename [pix723.bin]? asdm-523.bin
Destination filename [asdm-523.bin]?
Accessing tftp://192.168.1.3/asdm-
523.bin...!!!
!!!

!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!

Writing current ASDM file flash:/asdm-523.bin

!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!

6287244 bytes copied in 80.710 secs (78590 bytes/sec)

pixfirewall#

3. Installation de l'ASDM :

Les étapes d'installation de ASDM :

3-1) Installation java JRE -6U7-Windows-I586-P.exe

3-2) Installation Mozilla firefox version 3 .0 .7r

3-3) Taper l'adresse de l'interface connecté avec l'ordinateur (https :// Adresse interface)

3-4) Lancer l'installation de L'ASDM depuis l'image afficher sur le navigateur web et suivre les étapes de l'installation.

3-5) S'identifier via l'adresse ip de PC, le login et le mot de passe.

4. Configuration global :

Ci-dessous la configration global du Pix :

```
FW-ISRS2# sh run
: Saved
:
PIX Version 7.2(3)
!
hostname FW-ISRS2
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 description connected to  internet
 nameif outside
 security-level 0
 ip address 10.10.61.17 255.255.255.248
!
interface Ethernet1
 description Vlan_interne
 nameif inside
 security-level 100
 ip address 10.10.61.1 255.255.255.248
```

```
!
interface Ethernet2
 description DMZ public
 nameif DMZ-Publique
 security-level 50
 ip address 10.10.61.14 255.255.255.248
!
interface Ethernet3
 description DMZ priv
 nameif DMZ-priv
 security-level 70
 ip address 172.16.2.1 255.255.255.128
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system flash:/image.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list DMZ-Publique_access_in remark Implicit rule
access-list DMZ-Publique_access_in extended permit ip any any
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
access-list outside_access_in extended permit icmp any any echo-reply
access-list outside_access_in_1 extended permit tcp any any inactive
access-list outside_access_in_1 extended permit ip any any
access-list outside_access_in_1 extended permit icmp any any inactive
access-list outside_access_in_1 extended permit ip host 10.10.61.3 any inactive
access-list outside_access_in_1 extended permit icmp any any echo-reply
access-list inside_access_in_1 extended permit ip host 10.10.61.3 host 10.10.61.18
inactive
access-list inside_access_in_1 extended permit ip host 10.10.61.18 host 10.10.61.3
inactive
access-list inside_access_in_1 extended permit icmp any any
access-list inside_access_in_1 extended permit ip any any
```

```
access-list inside_access_in_1 extended permit icmp any any echo-reply
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ-Publique 1500
mtu DMZ-priv 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-523.bin
no asdm history enable
arp timeout 14400
access-group outside_access_in_1 in interface outside
access-group inside_access_in_1 in interface inside
access-group DMZ-Publique_access_in in interface DMZ-Publique
route outside 0.0.0.0 0.0.0.0 10.10.61.22 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.10.61.2 255.255.255.255 inside
http 10.10.61.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
```

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
username cisco password 3USUcOPFUiMCO4Jk encrypted
prompt hostname context
Cryptochecksum:a92837bbbfe9a4f1294e23eb250180d6
: end
```

Conclusion

Au terme de ce travail et en guise de conclusion, nous devons rappeler que nous avons voulu inscrire notre étude dans un axe de recherche et d'étude.

Le but de notre projet consiste à l'Etude et la mise en place de la plate-forme Firewalling. Une telle étude vise à diffuser en toute sécurité.

Ce projet s'est déroulé en trois grandes phases. Un premier chapitre il fallait présenter le projet avec les objectifs attendus, ainsi qu'une brève présentation de l'organisme d'accueil. Le deuxième chapitre nous a permis de se familiariser avec le réseau attendu pour pouvoir entamer l'étude des plates-formes Firewalling. Le troisième chapitre concerne la partie de processus où nous avions décrit toutes les étapes du projet.

On espère, enfin, que la présente étude serait d'un quelconque intérêt pour la recherche dans le domaine des sécurités réseaux d'une manière générale, et contribuer tant soit peu à lever les zones d'ombre qui se dressaient et répondre au mieux aux objectifs.

Par ailleurs, ce projet de fin d'études a été, pour nous, une occasion intéressante pour acquérir sur le terrain de nouvelles connaissances dans le domaine de la sécurité réseau, et maîtriser celles que nous avions déjà. Il nous a également donné l'opportunité de nous intégrer au sein d'une équipe travaillant.

Mais on a aimé avoir plus de temps pour mieux tester notre projet et d'intervenir dans d'autre cas d'une panne ainsi qu'on souhaite que notre étude soit prise en charge pour appliqué dans d'autres sociétés.

Bibliographie

Livres :

- Cisco Pix Firewalls: Configure, manage, & Troubleshoot (**Syngress Media,U.S.** (21 juin 2005)).
- Cisco ASA and PIX Firewall Handbook (David Hucaby)

Ressources WEB :

- http://en.wikipedia.org/wiki/Cisco_PIXhttp://www.ietf.org/rfc/rfc3031.txt
- http://www.amazon.fr/Cisco-Pix-Firewalls-Configure-Troubleshoot/dp/1597490040
- http://www.cisco.com/warp/public/779/servpro/solutions/vpn/site_mpls.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mpls_te.htm
- http://portland.iu.nl/Brochures/Solarwinds/Orion_New.pdf
- http://www.naosa.com/?q=system/files/La+famille+de+produits+SSG.pdf
- http://www.cisco.com/web/CH/fr/assets/docs/C3750_DS_v3.pdf

Acronymes

A	
ADSL	Asymetric Digital Suscriber Line
ATM	Asynchronous Transfer Mode
B	
BFD	Bidirectional Forwarding Detection
BLR	Boucle Locale Radio
BSS	Business Support System
C	
CE	Customer Edge
CEF	Cisco Express Forwarding
D	
DCN	Data Communication Network
DSLAM	Digital Subscriber Line Access Multiplexer
E	
EDGE	Enhanced Data rates for Global Evolution
EGPE	Exterior Gateway Protocol
ELSR	Edge Label Switching Router
F	
FAI	Fournisseur d'Accès à Internet
FE	Fast Ethernet
FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
I	
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISDN	Integrated Services Digital Network (RNIS)
K	
Kbps	Kilo Bit Par Seconde
L	
L2L	Lan To Lan
L2TP	Layer 2 Tunneling Protocol
LSP	Label Switched Path
LSR	Label Switching Router
M	
MGBPS	Méga Bit Par Seconde
N	

NAT	Network Address Translation
NMS	Network Management System
NVL	Numéro de Voie Logique
O	
OSI	Open Systems Interconnection
P	
P	Provider
PE	Provider Edge
POC	Point Of Control
POS	Packet over SDH
PPTP	Point-to-point tunneling protocol
PSTN	Public Switched Telephone Network
Q	
QOS	Quality Of Service
R	
RSVP	Resource ReSerVation Protocol
S	
SMS	Short Message Service
STM	Synchronous Transfer Mode
T	
TTL	Time-To-Live
V	
VPN	Virtual Private Network
VLSM	Variable Length Subnet Mask
W	
WIMAX	Worldwide Interoperability for Microwave Access

Secure Services Gateway (SSG) 500 Series, nouvelle gamme de plates-formes de pare-feu/VPN, dotées d'interfaces LAN (réseau local) et WAN (réseau étendu) intégrées. Les nouvelles plates-formes Secure Services Gateway 550 permettent aux entreprises de répondre de manière aux besoins croissants des succursales et des filiales de taille moyenne en matière de connectivité ; et ce en combinant des fonctions de sécurité et de routage au sein d'une même plate-forme.

Les plates-formes Secure Services Gateway de Juniper Networks aident les entreprises réparties géographiquement à mettre en œuvre des services sécurisés basés sur des LAN et des WAN, au sein de leurs filiales, tout en offrant la possibilité de s'adapter à l'évolution de leurs besoins en matière de connectivité et de sécurité. Les nouvelles plates-formes supportent en outre l'environnement Enterprise Intranet, en facilitant un contrôle accru des menaces et des modes d'utilisation et de distribution, à travers l'ensemble du réseau.

Le Secure Services Gateway de Juniper Networks a été conçu dès le départ en considérant la sécurité comme une fondation de base et en s'appuyant sur le système d'exploitation sécurisé de Juniper ScreenOS. La plate-forme offre un débit routeur de 1Gb/s et un débit VPN de 500 Mb/s, tout en fournissant des fonctionnalités de prévention d'intrusion, de filtrage Web, d'antivirus et d'anti spam, protégeant les entreprises contre les menaces de sécurité basées sur le LAN en interne et sur le WAN en externe.

Le Secure Services Gateway permet à la fois aux pare-feux/VPN et aux fonctions de sécurité des contenus. Les zones de sécurité aident en outre les utilisateurs à diviser leurs réseaux filaires et sans fil en segments sécurisés, chacun d'eux étant doté de leur propre règle de sécurité. Ceci permet de mieux supporter différents groupes d'utilisateurs, qui peuvent inclure par exemple les revendeurs, les clients et les employés.

Cette solution propose des fonctions de routage logiciel et de multiples options hardware pour connecter les utilisateurs. Des cartes d'interface WAN optionnelles issues des routeurs de Juniper peuvent être intégrées à la plate-forme SSG et des protocoles d'encapsulation WAN inclus dans JUNOS, le système d'exploitation des routeurs de Juniper, sont intégrés dans le moteur de sécurité et de routage de ScreenOS. Le Secure Services Gateway inclut quatre interfaces Ethernet 10/100/1000 incorporées dans le châssis et six emplacements d'extension E/S fournissant des options de connexion T1/E1, DS3, série, cuivre et fibre Gigabit Ethernet. Le produit offre aux entreprises la possibilité de supporter des connexions WAN existantes et de migrer vers des connexions plus rapides de nouvelle génération.

SSG550

Figure 49 : Juniper SSG550

1. **Fonctions de sécurité intégrées :**

ScreenOS dispose de fonctions de sécurité UTM (Unified Threat Management) complètes, qui vous protègent des attaques dirigées contre votre réseau et vos applications, tout en bloquant les attaques orientées sur le contenu. Les fonctions de sécurité UTM comprennent les éléments suivants :

- Pare-feu assurant le contrôle des personnes et des éléments qui accèdent au réseau ;
- Système de prévention des intrusions (pare-feu à action approfondie) permettant de bloquer les attaques au niveau de l'application ;
- Antivirus (avec Anti-Phishing, Anti-Spyware, Anti-Adware) permettant de bloquer les virus, les chevaux de Troie et d'autres logiciels malveillants ;
- Anti-Spam permettant de bloquer les spammeurs et les hameçonneurs connus
- Filtre Web permettant de contrôler l'accès vers les sites de téléchargement malveillants ou présentant un contenu douteux ;
- VPN IPSec site-à-site pour une communication sécurisée entre les bureaux Capacité de traitement des dénis de service (DoS) ;
- Application Layer Gateways pour que H.323, SIP et MGCP puissent contrôler et protéger le trafic VoIP ;
- L'intégration du système d'exploitation et des applications à la plateforme matérielle améliore la productivité de la plateforme et élimine les failles de sécurité présentes dans certains systèmes de protection et de routage.

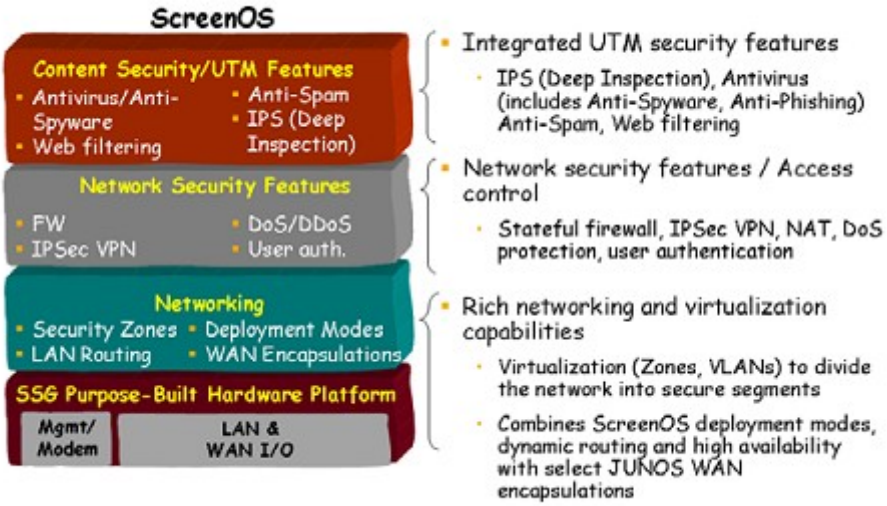


Figure 50 : Fonction de sécurité intégrée

2. **Juniper Configuration**

On peut accède au firewall soit par:

- L’utilisation d’une connexion de console

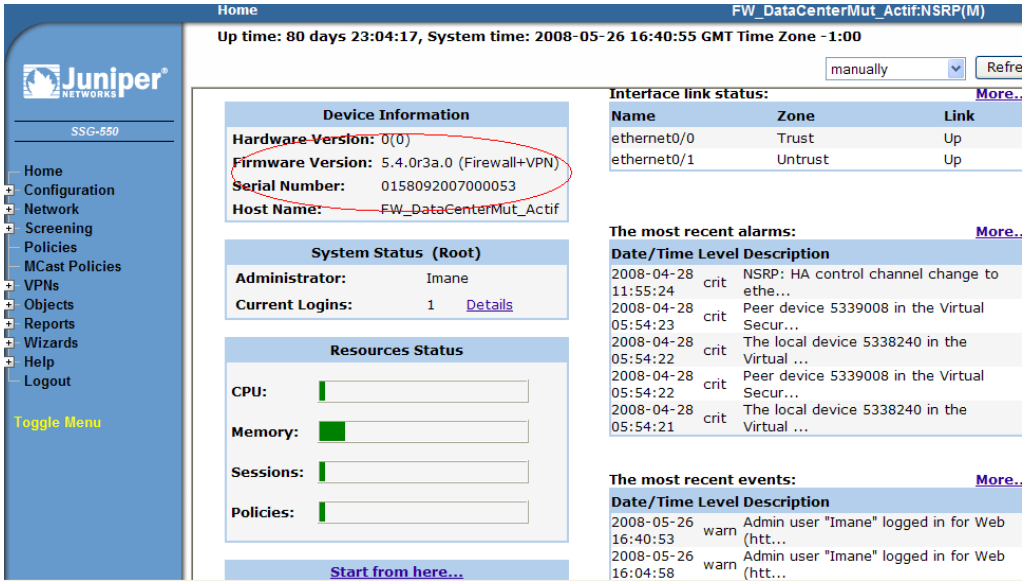
- L’utilisation de Telnet
- L’utilisation de l’interface utilisateur Web

On choisit l’accès par l’interface web, dans le cadre de l’utilisation de l’interface utilisateur Web, le poste de travail à partir duquel on gère l’appareil doit initialement être situé dans le même sous-réseau que l’appareil et procéder comme suit :
1. Connecter le poste de travail au port 0/2 — 0/6 (interface bgroup0 de la zone Trust) de l’appareil.
2. s’assurer que le poste de travail est configuré pour le protocole DHCP (Dynamic Host Configuration Protocol) ou est configuré de manière statique avec une adresse IP du sous-réseau 192.168.1.0/24.
3. Lancer le navigateur, saisir l’adresse IP de l’interface bgroup0 (l’adresse IP par défaut est 192.168.1.1/24), puis appuyer sur Entrée.
L’interface utilisateur Web affiche l’invite de connexion représentée à la Figure 51.

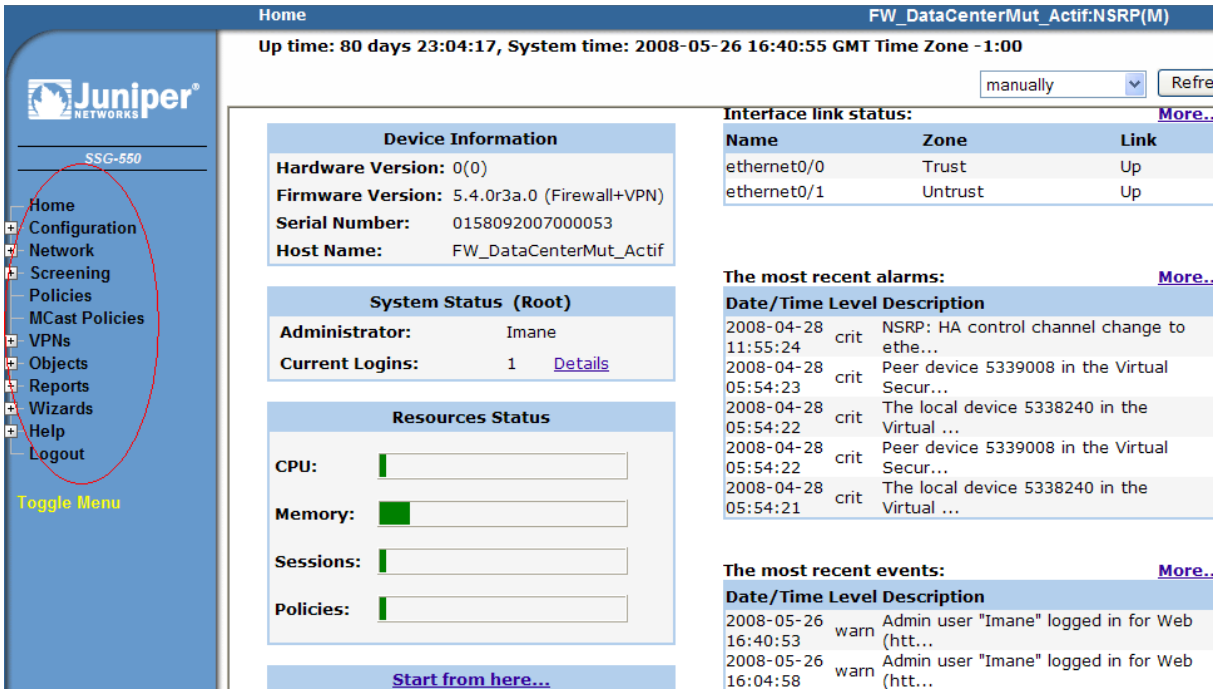
Figure 51 : Interface utilisateur Web

1. saisir le nom et le mot de passe afin d’accéder.

La première page qui apparait nous donne les informations sur Juniper



Configurer le firewall à l'aide du menu à gauche :



Par un seul click sur le menu on accède à l'interface de configuration.

Commutateur Cisco Catalyst 3750

La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel.

Figure 52 : Commutateur Cisco Catalyst 3750G de 48

Pour les réseaux de taille moyenne et les succursales d'entreprise, la gamme Cisco Catalyst 3750 facilite le déploiement d'applications convergées et s'adapte à l'évolution des besoins commerciaux en offrant flexibilité de configuration, prise en charge des fonctionnalités nécessaires aux réseaux convergés, et automatisation des configurations de services réseau intelligents. De plus, la gamme Cisco Catalyst 3750 est optimisée pour les déploiements Gigabit Ethernet de forte densité et comprend un large éventail de commutateurs qui répondent aux besoins de connectivités à l'accès, en agrégation ou pour la constitution de petit réseau fédérateur.

1. Technologie Cisco StackWise (un nouveau standard pour la résilience de pile de commutateurs) :

La technologie Cisco StackWise est une architecture d'empilement de commutateurs optimisée pour les réseaux Gigabit Ethernet. Elle a été conçue pour favoriser les ajouts, les suppressions et le redéploiement de commutateurs dans une pile tout en maintenant des performances constantes en son sein. La technologie Cisco StackWise assemble jusqu'à neuf commutateurs individuels dans une simple unité logique, en utilisant des câbles spécifiques d'empilement et un logiciel de gestion intelligente de la pile. Tous les commutateurs de la gamme Cisco Catalyst 3750 et de la nouvelle gamme Catalyst 3750-E sont empilables ensemble dans une même pile. Une pile fonctionne comme une unité de commutation unique gérée par un commutateur maître, élu parmi les commutateurs membres de la pile. Le commutateur maître crée et met à jour automatiquement toutes les tables de commutation et de routage. Une pile en fonctionnement peut accepter de nouveaux membres ou supprimer des membres existants sans interruption de service.

2. Fonctionnalités principales et avantages :

2.1 Facilité d'utilisation : Configuration « Plug-and-Play »

Une pile en fonctionnement se gère et se configure automatiquement. Lors de l'ajout ou de la suppression de commutateurs, le commutateur maître charge automatiquement dans le nouveau commutateur la version logicielle Cisco IOS utilisé par la pile, charge les paramètres de configuration globale, et met à jour toute les tables de routage pour prendre en compte les changements. Les mises à jour sont appliquées simultanément à tous les commutateurs de la pile.

La gamme Cisco Catalyst 3750 permet d'empiler jusqu'à 9 commutateurs comme seule unité logique pour un total de 468 ports Ethernet 10/100, 10/100/1000, PoE ou non, ou 9 ports 10 Gigabit Ethernet. Les commutateurs 10/100, 10/100/1000, et 10 Gigabit Ethernet peuvent être regroupés au sein d'une même pile dans toutes les combinaisons possible pour évoluer avec les besoins du réseau.

2.2 Retour sur investissement grâce au faible coût d'exploitation

L'automatisation de la vérification de la version logicielle Cisco IOS et du téléchargement des paramètres globaux de configuration apporte un gain de temps opérationnel.

Une seconde économie de temps est réalisée lors d'une action de maintenance. Quand vous enlevez un commutateur défectueux d'une pile existante et le remplacez par un nouveau commutateur de même modèle, le commutateur maître le détectera et rechargera automatiquement la configuration qui était sur le précédent commutateur sans avoir recours à une intervention extérieure. Ceci permet aux responsables réseaux de faire accomplir des tâches de maintenance au personnel local présent sur les sites éloignés, et ainsi faire l'économie du déplacement d'un technicien qualifié sur place.

2.3 Contrôleur LAN sans fil intégré

Un commutateur de la série Catalyst 3750 intègre un contrôleur de réseau sans fil pour fournir les fonctionnalités de contrôleur au réseau sans fil et y apporter une amélioration de l'efficacité opérationnelle, une sécurité du réseau sans fil renforcée, la mobilité, et une grande facilité d'utilisation.

Le contrôleur WLAN intégré au Catalyst 3750G fournit au réseau sans fil les politiques centralisées de sécurité, la prévention d'intrusion (IPS), la gestion de la radio (RF), la qualité de service (QoS), et la mobilité (roaming) sécurisée et rapide à travers un réseau de niveau 2 et 3.

Comme composant essentiel d'un réseau sans fil unifié Cisco, le contrôleur WLAN intégré au Catalyst 3750G apporte le contrôle, la sécurité, la redondance, et la fiabilité que les administrateurs réseaux ont besoin pour contrôler et faire évoluer leurs réseaux sans fil aussi facilement qu'ils le font avec leurs réseaux filaires traditionnels.

2.4 Disponibilité (Performance sans interruption de service des niveaux 2 et 3)

La gamme Cisco Catalyst 3750 améliore la disponibilité des commutateurs empilables. Tout commutateur de la pile peut fonctionner comme maître, créant une disponibilité 1:N pour le contrôle du réseau. En cas de défaillance d'un commutateur de la pile, toutes les autres unités continuent de transférer le trafic et maintiennent leur état opérationnel.

Gestion intelligente du trafic Multicast – Un nouveau niveau d'efficacité pour les réseaux convergés.
Avec la technologie Cisco StackWise, la gamme Cisco Catalyst 3750 offre une plus grande efficacité pour traiter les applications multicast, telles que la vidéo. Chaque paquet de données multicast transite une seule fois à travers le fond de panier, ce qui engendre un support plus efficace pour supporter d'avantage de flux multicast.

2.5 Qualité de service avancée sur l'ensemble de la pile et à la vitesse du média

La gamme Cisco Catalyst 3750 et 3750-E offre des débits Gigabit et 10 Gigabit Ethernet avec des services intelligents qui garantissent la fluidité d'acheminement des données, et ce, avec une vitesse pouvant être jusqu'à dix fois supérieure à celle d'un réseau classique. Des mécanismes uniques de marquage, de classification, de gestion des files d'attente assurent des performances de pointe pour les trafics données, voix et vidéo ; le tout à la vitesse du média.

2.6 Sécurité du réseau (Contrôle optimisée à l'accès du réseau)

La gamme Cisco Catalyst 3750 supporte un ensemble complet de fonctionnalités de sécurité pour contrôler la connectivité et l'accès au réseau, notamment les listes de contrôle d'accès (ACLs), l'authentification, la sécurité au niveau des ports, et les services réseaux basés sur l'identité via le standard 802.1x et ses extensions. Cet ensemble de fonctionnalités aident non seulement à se protéger des attaques extérieures, mais également à défendre le réseau contre les attaques « man-in-the-middle », une menace importante pour les réseaux d'entreprise aujourd'hui.

2.7 Gestion simplifiée (Plusieurs commutateurs, une seule adresse IP d'administration)

Chaque pile de la gamme Cisco Catalyst 3750 est gérée en tant qu'objet unique avec une seule adresse IP. La gestion IP unique est supportée pour les activités telles que la détection de défaillances, la création et la modification de réseaux locaux virtuels (VLAN), la sécurité, et la QoS.

2.8 Support IPv6

La gamme Cisco Catalyst 3750 traite en hardware le routage IPv6 pour des performances maximales. Les commutateurs Catalyst 3750 sont d'hors et déjà prêt à faire face à la croissance des équipements réseau, à la nécessité d'un adressage plus large et d'une sécurité accrue avec leur support d'IPv6.

2.9 Options d'administration

La gamme Cisco Catalyst 3750 (Figure 5) offre une interface par lignes de commande évoluée (CLI) pour les configurations détaillées, et le logiciel Cisco Network Assistant, outil orienté Web, pour les configurations rapides basées sur des modèles prédéfinis. De plus, CiscoWorks prend en charge la gamme Cisco Catalyst 3750 pour une administration globale du réseau.

Figure 53 : Empilement de commutateurs Cisco Catalyst 3750