

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU



FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :

**Mise en place d'un tunnel VPN implémenté sur
ASA Cisco.**

Encadré par :

Mr. M.LAHDIR

Mr. M.Kibouh

Présenté par :

M^{elle}. AIT DAHMANE Nouara

M^{elle}. CHEKKAL Saida

Année universitaire 2011/2012

Remerciements

REMERCIEMENT

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage pour terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr.Lahdir, qui nous a aidées tout au long du travail.

Un grand merci à notre Co-promoteur Mr.Kibouh pour ses encouragements et ses orientations qui nous ont beaucoup aidées au cours de notre projet.

Nous tenons à remercier également nos amis (es) et nos familles pour leurs aides considérables.

Dédicaces

Je dédie ce travail

- *A mes très chère parents, pour leurs sacrifie et leurs dévouement pour mon bonheur. Que Dieu les garde.*
- *A mes frères et ma sœur houria*
- *A tous mes cousins*
- *A tous mes amis*
- *A toute ma promotion Master II*
- *A ceux qui m'aiment*

Saida

Dédicaces

Je dédie ce travail

- *A mes très chère parents, pour leurs sacrifie et leurs dévouement pour mon bonheur. Que Dieu les garde.*
- *A mes frères et mes soeurs*
- *A tous mes cousins*
- *A tous mes amis*
- *A toute ma promotion Master II*
- *A ceux qui m'aiment*

Nouara

Sommaire

SOMMAIRE

Introduction

Chapitre I : LE RESEAU PRIVE VIRTUEL

I.1-Préambule	1
I.2-Définition	1
I.2.1-Réseau privé	1
I.2.2- Réseau privé virtuel	1
I.2.3- Intérêt de VPN	2
I.3-Le principe fonctionnement d'un VPN	3
I.4-Les contraintes d'un VPN	4
I.5-les différents types de VPN	4
I.5.1- Le VPN d'accès	5
I.5.2- L'intranet VPN.....	6
I.5.3- L'extranet VPN	7
I.6-Protocoles utilisés et sécurité des VPN.....	8
I.6.1- PPP (Point To Point Protocol)	8
I.6.2-PPTP (Point To Point Tunneling Protocol).....	9
I.6.3 -L2F (Layer Two Forwarding)	11
I.6.4- L2TP (Layer Two Tunneling Protocol).....	11
I.6.4.1 - Concentrateurs d'accès L2tp	11
I.6.4.2 - Serveur réseau L2tp	12
I.6.5- IPSEC	12
I.6.5.1– Vue générale.....	12
I.6.5.2- Services offerts par IPsec.....	12
I.6.5.3- Les sous-protocoles d'IPsec	13
I.6.5.3.1- Le protocole Ah	13
I.6.5.3.2- Protocole Esp	13
I.6.5.4-IPsec en mode tunnel et transport	14
I.6.5.4.1-Mode transport	14
I.6.5.4.2-Mode tunnel	15

SOMMAIRE

I.6.6-Le protocole SSH	15
I.6.7- Le protocole SSL	16
I.6.7.1 – Fonctionnement	16
I.7- Comparaison des différents protocoles	17
I.7.1 VPN-SSL	17
I.7.2- PPTP	18
I.7.3 L2tp / Ipsec	19
I.8-Les avantages et les inconvénients de VPN	19
I.9-Discussion	20

CHAPITRE II : LES fonctionnalité d'ASA Cisco

II- Préambule	21
II-1- Les différentes familles de Cisco ASA	21
II.1.1- Cisco ASA 5505	21
II.1.2- Cisco ASA 5540	24
II.1.3- Cisco ASA 5580-40	25
II.2- Avantage d'ASA Cisco pour l'entreprise	26
II.3- Principe fonctionnalité d'ASA	28
II.3.1 – transformation les adresses de réseau NAT	29
II.3.2 – qualités de services QoS	29
II.3.3 – Sécurité Contexte	29
II.3.4 – ACL	30
II.3.5 – IPS	30
II.3.5.1 – AIP SSM	31
II.3.5.2 – CSC SSM	31
II.3.6 - La détection des menaces	31
II.3.7 – Protection contre l'IP Spoofing	32
II.3.8 – Normalisation TCP	32
II.3.9 – AAA (Authentication, Authorization, Accounting).....	32
II.3.9.1 – Authentification	33

SOMMAIRE

II.3.9.2 – Autorisation	33
II.3.9.2 – Surveillance	33
II.3.10 – Les filtres HTTPS, FTP	33
II.3.11 – Limites de connexions	34
II.4 – Gestion du trafic	35
II.4.1 – Le principe des niveaux de sécurité	35
II.4.2-liste de contrôle d'accès	36
II.4.3– Droits des utilisateurs	36
II.5- Discussion	37

CHAPITRE III : Etablissement d'un tunnel vpn lan-to lan

III-1-Préambule	37
III-2- le logiciel de simulation GNS3	37
III.3-Etablissement d'un tunnel LAN-TO-LAN	40
III.3.1-La topologie	40
III.3.2 – Cahier des charges	41
III.3.3– Adressage et connectivité 42	
III.3.3.1 - Présentation 42	
III.3.3.2-Adressage des pc 42	
III.3.3.3 - Configuration des routeurs 43	
III.3.4 -Configuration des ASA45	
III.3.4.2 Etablissement du NAT45	
III.3.4.1-Adressage 51	
III.3.5 – Etablissement du tunnel VPN52	
III.3.5.1– Présentation 52	
III.3.5.2 – Paramètres ISAKMP 54	
III.3.5.3-Transform set 55	
III.3.5.4-Tunnel group 56	
III.3.5.5-Crypto map 57	
III.4- Discussion.....	58

SOMMAIRE

Conclusion

Glossaire

Annexe 1

Annexe 2

Liste de figure

Figure I.1 : VPN connectant un utilisateur distant à un intranet privé	6
Figure I.2 : VPN connectant 2 sites distants par l'Internet	7
Figure I.3 : VPN connectant des sites clients au site de l'entreprise	7
Figure I.4 : la trame PPP	8
Figure I.5 : La trame PPTP	10
Figure I.6 : les différences entre le mode tunnel et transport	15
Figure II.1: Cisco asa 5505	22
Figure II.2: Schéma Cisco 5505	23
Figure II.3 : Cisco asa 5540.....	24
Figure II.4 : Cisco asa 5580-40	25
Figure III.1 : Détail de la fenêtre du simulateur.....	38
Figure III.2 : localisation du binaire de qemu.....	39
Figure III.3 : localisation de IOS and hypervisors.....	40
Figure III.5 : topologie du réseau choisi	41

*Introduction
générale*

INTRODUCTION

Aujourd'hui, l'Internet est largement utilisé dans le monde, et plus orienté métier. Les organismes offrant la connexion Internet sont intéressés par la tarification où les clients payent pour les ressources qu'ils consomment.

Indéniablement, ce grand réseau est rentré dans nos mœurs. A travers, lui tout un monde parallèle s'est développé : des sites marchands ont fleuri, les services pour les particuliers comme les guides d'itinéraire pour nos voyages nous simplifient bien la vie. Enfin on en vient à échanger des données à travers des programmes d'échange de fichiers. Nous retiendrons de tout ça qu'Internet est un véritable outil de communication. A la fois High-tech est démodé par sa technique, internet n'a pas su évoluer dans l'utilisation de ses protocoles, la plupart des protocoles utilisés ont plusieurs années d'existence et certains n'ont pas été créés dans une optique où le réseau prendrait une telle envergure. Les mots de passe traversent ainsi les réseaux en clair, et là où transitent des applications de plus en plus critiques sur le réseau, la sécurité, elle a peu évolué.

Il y a peu de temps, les entreprises pouvaient encore se permettre de construire leurs propres LAN, supportant leurs propres systèmes de nomination, système de messagerie, voir même leur propre protocole réseau. Cependant, comme de plus en plus de données étaient stockées sur ordinateurs, les entreprises ressentirent le besoin d'interconnecter leurs différents bureaux. Grâce à l'utilisation de lignes dédiées, une entreprise avait la garantie que la connexion entre ses départements serait toujours disponible et privée. Cependant, cette solution peut être très coûteuse, notamment si l'entreprise a plusieurs bureaux à travers tout un pays. De plus, les réseaux privés manquent de souplesse par rapport aux situations que l'on peut rencontrer dans une entreprise. En effet, si un représentant a besoin d'accéder à distance au réseau privé de son entreprise alors qu'il est à des milliers de kilomètres de celle-ci, le coût de l'appel téléphonique sera extrêmement élevé.

L'un des solutions proposé par Cisco on trouve l'ASA 5500 séries VPN permet aux entreprises de profiter des avantages en termes de connectivité et de coût, sans compromettre l'intégrité des règles de sécurité d'entreprise. En faisant converger

INTRODUCTION

les services Cisco WebVPN, composés des services VPN IPSec et SSL, avec les technologies complètes de défense contre les menaces, la gamme Cisco ASA 5500 séries fournit un accès réseau entièrement personnalisable. Adaptée aux besoins de différents environnements de déploiement, elle propose un VPN totalement sécurisé avec une sécurité complète au niveau du réseau et du point d'extrémité.

L'objet de ce projet est l'établissement d'un tunnel VPN site à site on utilisant l'ASA Cisco afin de pouvoir interconnecter deux sites distants d'une entreprise avec une assurance de la sécurité des données à transmettre.

Notre mémoire est structuré de trois chapitres le premier chapitre consiste à une étude générale sur les VPN, le deuxième chapitre représente les fonctionnalités d'un ASA Cisco et le troisième chapitre est consacré à une application qui est une configuration d'ASA Cisco afin d'établir un tunnel VPN site –à-site.

Enfin nous terminerons par une conclusion générale.

Chapitre 1

Généralités sur les VPNs

I.1-Préambule

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

Nous allons présenter dans la suite un état de l'art des technologies VPN les plus répandues. Elles seront résumées afin d'en obtenir une vue générale, formant une base pour lancer notre projet sur les ASA.

I.2-Définition

I.2-1-Réseau privé

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

I.2.2- Réseau privé virtuel

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

entre deux entités sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

I.2.3- Intérêt de VPN

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

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

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

I.3-Le principe fonctionnement d'un VPN

Le VPN repose sur un protocole de tunnellation (*tunneling*), c'est-à-dire un protocole qui permet le passage de données cryptées d'une extrémité du VPN à l'autre grâce à des algorithmes de cryptage. On emploie le terme « tunnel » pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public.

Dans le cas d'un VPN établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client), et *serveur VPN* l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. La machine distante va alors fournir les données au serveur VPN de son réseau local, qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur. Pour émuler une liaison point à point, les données sont encapsulées, à l'aide d'un en-tête qui contient les informations de routage pour leur permettre de traverser le réseau partagé ou public jusqu'à leur destination finale. Pour émuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets interceptés sur le réseau partagé ou public restent indéchiffrables sans clé de décryptage. La liaison servant à l'encapsulation et au cryptage des données privées est une connexion VPN.

Etant donné que chaque point d'un réseau VPN est relié au réseau central par le biais d'un tunnel, reliant la machine à une passerelle. Ainsi, tous les utilisateurs passent par le même point, ce qui permet de gérer la sécurité des accès, ainsi que le trafic utilisé par chacun. En effet, malgré son aspect sécurisé.

Les principaux avantages d'un VPN :

- **Sécurité** : assure des communications sécurisé et chiffrées.
- **Simplicité** : utilise les circuits de télécommunication classiques.
- **Economie** : utilise internet en tant que média principal de transport, ce qui évite les couts liés à une ligne dédiée.

I.4-Les contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur** : seuls les utilisateurs autorisés doivent avoir l'accès au canal VPN.
- **Cryptage de données** : lors de leurs transports sur le réseau public, les données doivent être protégées par un cryptage efficace.
- **Gestion des clés** : les clés de cryptage pour le client et le serveur doivent être générées et régénérées.
- **Prise en charge multi protocole** : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux public en particulier IP.

I.5-les différents types de VPN

Parmi ces différents types on peut citer les :

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

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

I.5.1- Le VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas:

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un Nas compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le Nas n'est pas cryptée Ce qui peut poser des problèmes de sécurité.

Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée.

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le Vpn d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

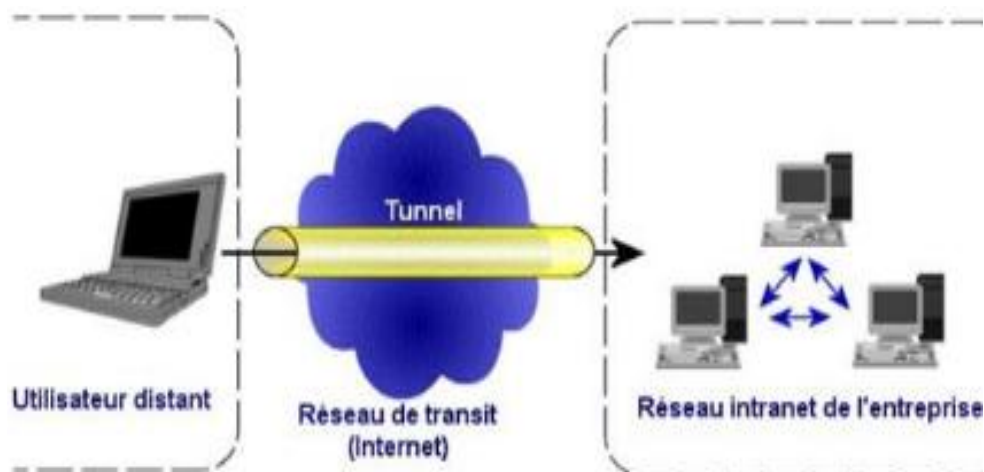


Figure I.1 : VPN connectant un utilisateur distant à un intranet privé

I.5.2- L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est aussi basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation Ip dans IP pour assurer une sécurité raisonnable.

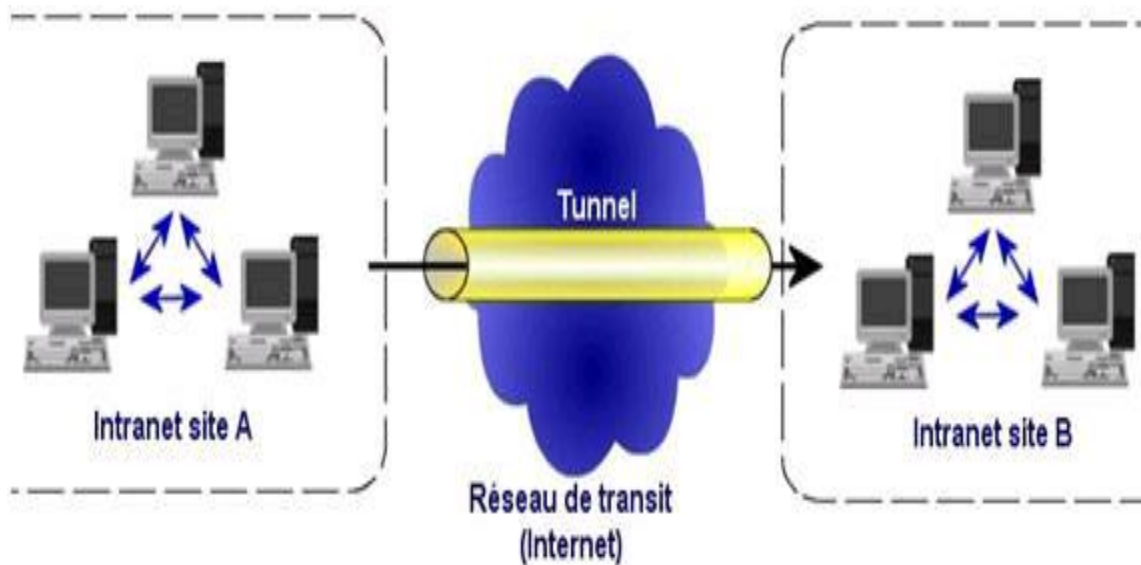


Figure I. 2: VPN connectant 2 sites distants par l'Internet

I.5.3- L'extranet VPN

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

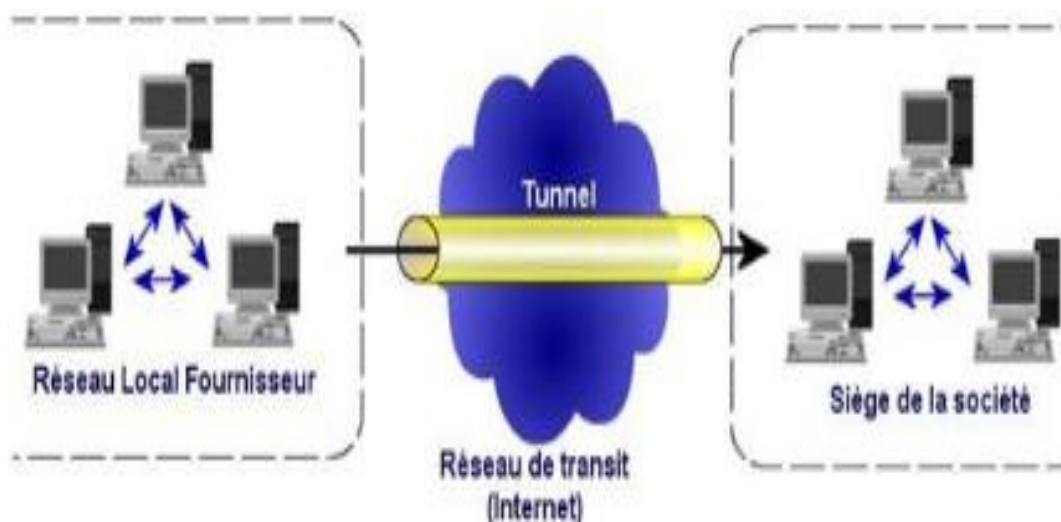


Figure I.3 : VPN connectant des sites clients au site de l'entreprise

I.6-Protocoles utilisés et sécurité des VPN

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

I.6.1- PPP (Point To Point Protocol)

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

PPP est en réalité un ensemble de trois protocoles :

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

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

Une trame PPP ressemble à ceci :

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

Figure I.4 : la trame PPP.

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

- Lors de la connexion, un paquet LCP est envoyé.

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

Voici la liste des services pouvant être offerts par PPP :

- ✓ permet à un serveur d'accès à distance de recevoir des appels entrants et de garantir l'accès au réseau à des logiciels d'accès distant d'autres éditeurs, conformes aux normes PPP.
- ✓ Les normes PPP autorisent des fonctions avancées qui ne sont pas disponibles avec l'ancienne norme, notamment SLIP.
- ✓ Le protocole PPP prend en charge plusieurs méthodes d'authentification ainsi que la compression des données et leur cryptage.
- ✓ La plupart des versions du protocole PPP permettent d'automatiser l'ensemble de la procédure d'ouverture de session.
- ✓ Le protocole PPP prend également en charge plusieurs protocoles de réseau local. Nous pouvons utiliser TCP/IP ou IPX comme protocole réseau. PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions VPN (Virtual Private Network) sécurisées.

I.6.2-PPTP (Point To Point Tunneling Protocol)

PPTP est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. Ainsi, PPTP est une solution très

employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet le cryptage de données ainsi que leur compression.

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

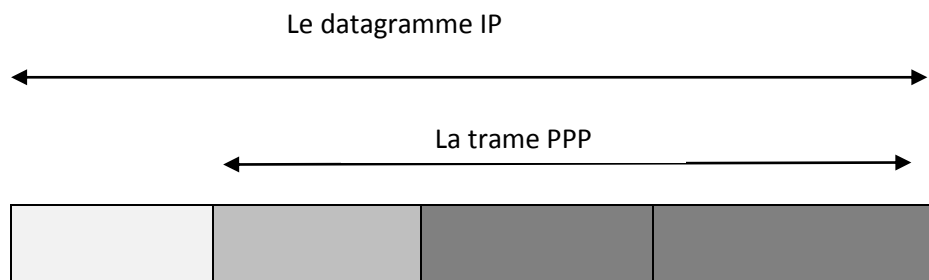


Figure I.5 : La trame PPTP

Le tunnel PPTP se caractérise par:

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

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

Plusieurs protocoles peuvent être associés à PPTP afin de sécuriser les données ou de les compresser. Ainsi, pour le processus d'identification, il est possible d'utiliser les protocoles PAP (Password Authentication Protocol). Pour le cryptage de données, il est possible d'utiliser les fonctions de MPPE (Microsoft Point to Point Encryption).

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

I.6.3 -L2F (Layer Two Forwarding)

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

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

I.6.4- L2TP (Layer Two Tunneling Protocol)

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

I.6.4.1 - Concentrateurs d'accès L2tp (LAC : L2TP Access Concentrator)

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

I.6.4.2 - Serveur réseau L2TP (LNS : L2TP Network Server)

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

I.6.5- IPSEC (Internet protocol security)

I.6.5.1– Vue générale

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

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

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

I.6.5.2- Services offerts par IPsec

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

➤ **Authentification des extrémités** : Chaque extrémité du tunnel va s'identifier avant d'entamer la communication des données. Cela permet de s'assurer que l'on dialogue avec la personne convenue. De plus, pour chaque paquet échangé, IPsec

permettra de s'assurer qu'il a été émis par la bonne machine (authenticité des données).

➤ **Confidentialité des données** : Evite que quelqu'un qui intercepterait les données ne puisse les interpréter. On utilisera pour cela des techniques de cryptographie.

➤ **Intégrité des données** : IPsec permet de s'assurer qu'un paquet n'a subi aucune modification durant son trajet.

➤ **Protection contre le replay** : permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

I.6.5.3- Les sous-protocoles d'IPsec

I.6.5.3.1- Le protocole Ah (Authentication Header)

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

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

I.6.5.3.2- Protocole ESP (Encapsulating Security Payload)

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

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

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

Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets.

Les données d'authentification ne sont présentes que si Ce service a été sélectionné. Voyons maintenant comment est appliquée la confidentialité dans ESP.

L'expéditeur :

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

I.6.5.4-IPsec en mode tunnel et transport

I.6.5.4.1-Mode transport

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

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

I.6.5.4.2-Mode tunnel :

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

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

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

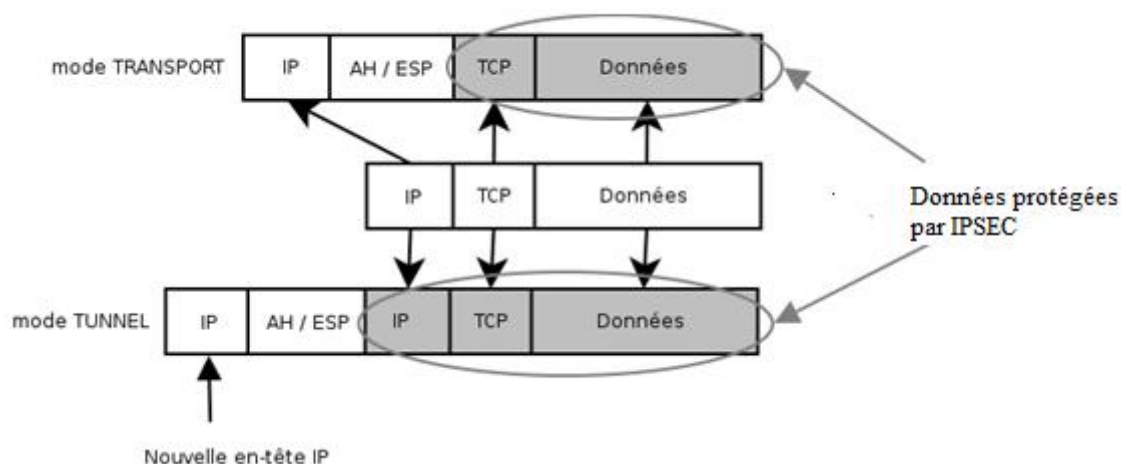


Figure I.6 : les différences entre le mode tunnel et transport

I.6.6-Le protocole SSH

SSH est une version sécurisée de ces outils ; il permet de se connecter à distance sur une machine donnée suivant une architecture client/serveur. Il se compose d'un client qui sera invoqué sur la machine initiatrice de la communication et d'un serveur qui doit tourner sur la machine destinataire. Il va créer une communication

sécurisée, en authentifiant les deux parties et en garantissant le secret de la communication et son intégrité.

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

I.6.7- Le protocole SSL

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

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

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

I.6.7.1 - Fonctionnement

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

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

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

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

I.7- Comparaison des différents protocoles

Chaque protocole présenté permet de réaliser des solutions performantes de VPN. Nous allons ici aborder les points forts et les points faibles de chacun de ses protocoles.

I.7.1 VPN-SSL

Présentée comme la solution miracle pour permettre aux itinérants de se connecter aux applications réparties de l'entreprise, les VPN-SSL souffrent de problèmes principalement liés aux navigateurs web utilisés. Le but d'utiliser des navigateurs web est de permettre aux utilisateurs d'utiliser un outil dont ils ont l'habitude, et qui ne nécessite pas de configuration supplémentaire. Cependant lorsqu'un certificat expire l'utilisateur doit aller manuellement le renouveler. Cette opération peut poser un problème aux utilisateurs novices. De plus sur la majorité des navigateurs web la consultation des listes de certificats révoqués n'est pas activée par défaut : toute la sécurité de SSL reposant sur ces certificats ceci pose un grave problème de sécurité. Rien n'empêche de plus le client de télécharger une version

modifiée de son navigateur pour pouvoir utiliser de nouvelles fonctionnalités. Rien ne certifie que le navigateur n'a pas été modifié et que son autorité de certification en soit bien une. Enfin Un autre problème lié à l'utilisation de navigateurs web comme base au VPN est leur spécificité au monde web. En effet par défaut un navigateur n'interceptera que des communications http ou éventuellement FTP. Toutes les communications venant d'autre type d'applications (MS Outlook, ou une base de données par exemple) ne sont pas supportées. Ce problème est généralement contourné par l'exécution d'une applet Java dédiée dans le navigateur. Mais ceci implique également la maintenance de cette applet (s'assurer que le client possède la bonne version, qu'il peut la re-télécharger au besoin).

L'idée suivant laquelle le navigateur web est une plate-forme idéale pour réaliser des accès VPN est donc sérieusement à nuancer.

I.7.2- PPTP

PPTP présente l'avantage d'être complètement intégré dans les environnements Windows. Ceci signifie en particulier que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS et sa gestion de droits et de groupe. Cependant comme pour beaucoup de produit Microsoft la sécurité est le point faible:

- Mauvaise gestion des mots de passe dans les environnements mixtes WIN 95/NT
- Faiblesses dans la génération des clés de session : réalisé à partir d'un hachage du mot de passe au lieu d'être entièrement générées au hasard. (Facilite les attaques « force brute »)
- Identification des paquets non implémentée : vulnérabilité aux attaques de type « spoofing ».

I.7.3 L2TP / IPsec

Les mécanismes de sécurité mis en place dans IPsec sont plus robustes et plus reconnus que ceux mis en place par Microsoft dans PPTP. Par défaut le protocole L2TP utilise le protocole IPsec. Cependant si le serveur distant ne le supporte pas, L2TP pourra utiliser un autre protocole de sécurité. Il convient donc de s'assurer que l'ensemble des équipements d'un VPN L2TP implémente bien le protocole IPsec. IPsec ne permet d'identifier que des machines et non pas des utilisateurs. Ceci est particulièrement problématique pour les utilisateurs itinérants. Il faut donc prévoir un service d'authentification des utilisateurs. Dans le cas de connexion dial-up c'est l'identifiant de connexion qui sera utilisé pour authentifier l'utilisateur. Mais dans le cas de connexion via Internet il faudra prévoir une phase d'authentification supplémentaire à l'établissement du tunnel. D'autre part IPsec n'offre aucun mécanisme de QOS Ce qui limite ses applications : toutes les applications de voix sur IP ou de vidéo sur IP sont impossibles ou seront amenées à être complètement dépendantes des conditions de trafic sur l'internet public.

Enfin IPsec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux. L'achat de périphériques dédiés, coûteux est souvent indispensable.

I.8-Les avantages et les inconvénients de VPN

Comme nous venons de le voir les VPN disposent de nombreux avantages :

- Gratuité ou coût assez faible.
- Confidentialité.
- Sécurité.
- Simplicité de la mise en place.

Cependant ils peuvent aussi représenter quelques inconvénients :

- Faille de sécurité (si mal sécurisé).
- Utilisation de ressources matérielles importantes.
- Du matériel dédié peut être obligatoire.

I.9-Discussion

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

Chapitre 2

Les fonctionnalités d'ASA Cisco

II- Préambule

L'idée de la conception de l'Adaptative Security Appliance (ASA) est apparue lors de la mise en place, par Cisco, de la solution Self-Defending Network (le réseau qui se défend tout seul). En effet, en associant un pare-feu très puissant à un système qui offre les services VPN, l'ASA est la solution proposée par Cisco pour garantir un réseau accessible de l'extérieur et sécurisé.

L'ASA met en place une défense face aux menaces, et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau. Grâce à une interface graphique et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises qui souhaitent sécuriser leur réseau un outil complet et raisonnablement facile d'utilisation.

II.1- Les différentes familles de Cisco ASA

La gamme étant assez large, sept références différentes (sans compter les versions les plus sécurisées de certain modèles), nous allons juste voir trois références, bas, milieu et haut de la gamme.

II.1.1- Cisco ASA 5505

L'ASA 5505 est le plus petit modèle de la gamme. Il y a exactement deux modèles, le 5505 *Base* et la version *security plus*, qui accepte plus de connexions, de sessions VPN, et liens VLANs et point plus intéressant supporte les services de haute disponibilité.

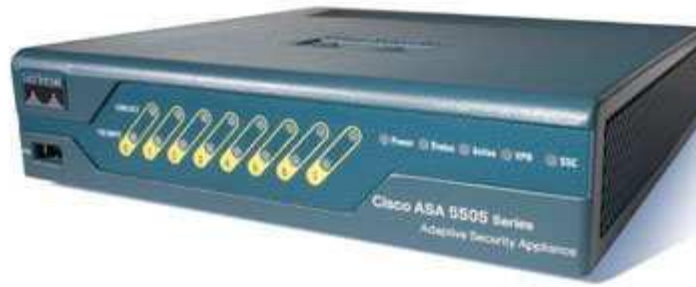


Figure II.1: Cisco asa 5505

Introduit dans la gamme en 2006

Matériel

CPU : AMD Geode LX @ 500MHz

Chipset : Geode CS5536

Chipset Réseau : Marvell 88E6095

RAM (par défaut) : 256 Mo

Périphérique Flash de boot : ATA CompactFlash

Flash (par défaut) : 64 Mo

Version minimale de l'OS : 7.2.1

Interfaces Max : 3 (trunk désactivé) / 20 (trunk activé)

Supporte les VPN SSL : Oui, 25

Performances

Bande passante maximale du firewall : 150 Mbps

Connexions maximales : 1 000 / 25 000 (pour la version Security Plus)

Connexions maximales par secondes : 4 000

Paquets par secondes (64 octets) : 85 000

Bande passante maximale VPN 3DES/AES : 100 Mbps

Nombre de sessions VPN maximales (site à site et accès distant) : 10 / 25
(pour la version Security Plus)

Nombre maximale de sessions utilisateur VPN SSL : 25

Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions

Extension SSC/SSM/IC : 1 SSC

Support SSC/SSM/IC : AIP, SSC

Prévention des intrusions : Oui (avec AIP SSC)

Version de l'ASA OS supportée : 8.2

Haute disponibilité supportée : Non, Actif/Passif (pour la version Security Plus)

VPN clustering et équilibrage de charge : Non

Ce modèle est donc intéressant pour les petites structures, aussi bien au vu de ses capacités que de son prix. De plus un point qui peut être intéressant pour les particulier ou petites sociétés, il n'est pas rackable, donc facile à mettre en œuvre au vu de sa petite taille.

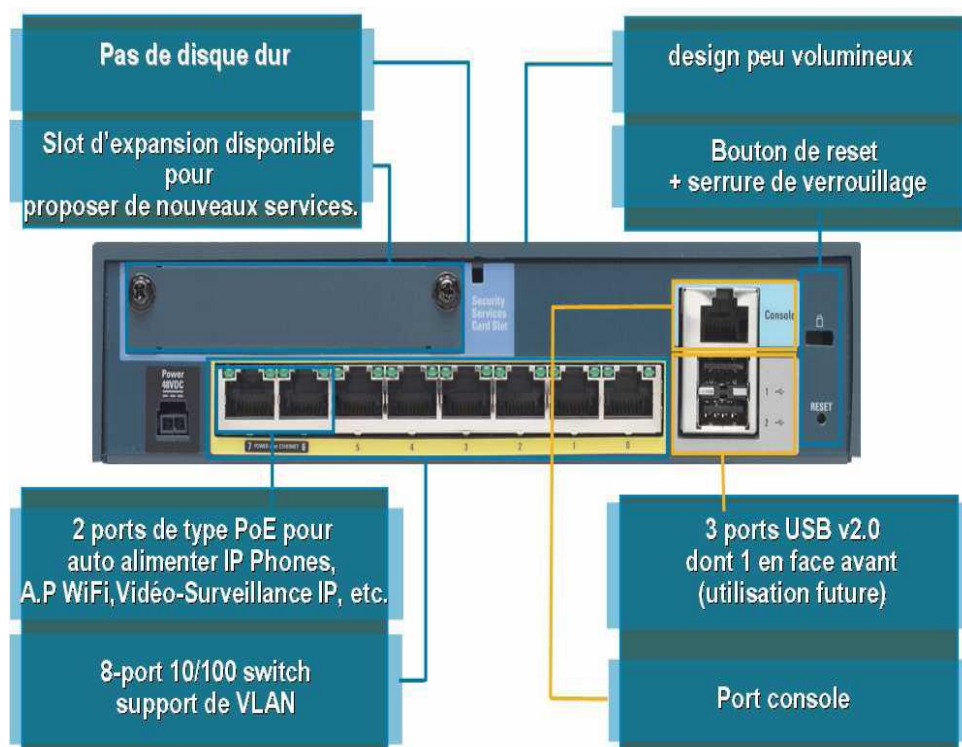


Figure II.2: Schéma Cisco 5505

II.1.2- Cisco ASA 5540

Au vu de ses caractéristiques et performances impressionnantes cette Appliance est vraiment dédiée aux très grands groupes ayants de très nombreux collaborateurs nomades, ou la base de leur méthode de travail est le télétravail.



Figure II.3 : Cisco asa 5540

Introduit dans la gamme en 2005

Matériel

CPU : Intel Pentium 4 @ 2,0 GHz

RAM (par défaut) : 1 Go

Périphérique Flash de boot : ATA CompactFlash

Flash (par défaut) : 64 Mo

Version minimale de l'OS : 7.0.1

Interfaces Max : 200

Supporte les VPN SSL : Oui, 2500

Performances

Bande passante maximale du firewall : 650 Mbps

Connexions maximales : 400 000 utilisateurs

Connexions maximales par secondes : 25 000

Paquets par secondes (64 octets) : 500 000

Bande passante maximale VPN 3DES/AES : 325 Mbps

Nombre de sessions VPN maximales (site à site et accès distant) : 5 000

Nombre maximale de sessions utilisateur VPN SSL : 2 500

Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions :

Extension SSC/SSM/IC : 1 SSM

Support SSC/SSM/IC : CSC SSM, AIP SSM, 4GE SSM

Prévention des intrusions : Oui (avec AIP SSM)

Version de l'ASA OS supportée : 8.2

Haute disponibilité supportée : Actif/Passif, Actif/Actif

VPN clustering et équilibrage de charge : Oui

II.1.C Cisco ASA 5580-40

Cette référence de la gamme ASA est le plus gros équipement possible. Il est dédié aux Datacenter ou pour les très grands campus, et au vu de ses performances il serait totalement inutile hors de ce rôle.



Figure II.4 : Cisco asa 5580-40

Introduit dans la gamme en 2008

Matériel :

CPU : 4 AMD Opteron (4 x 2 coeurs) @ 2,6 GHz

RAM (par défaut) : 12 Go

Périphérique Flash de boot : ATA CompactFlash

Flash (par défaut) : 1 Go

Version minimale de l'OS : 8.1.1

Interfaces Max : 250

Supporte les VPN SSL : Oui, 10 000

Performances

Bande passante maximale du firewall : 10 Gbps (en application http standard)

20 Gbps (en Jumbo Frames)

Connexions maximales : 2 000 000

Connexions maximales par secondes : 150 000

Paquets par secondes (64 octets) : 4 000 000

Bande passante maximale VPN 3DES/AES : 1 Gbps

Nombre de sessions VPN maximales (site à site et accès distant) : 10 000

Nombre maximale de sessions utilisateur VPN SSL : 10 000

Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions

Extension SSC/SSM/IC : 6 IC

Support SSC/SSM/IC : 4 10/100/1000, 4 GE SR LC, 2 10GE SR LC

Prévention des intrusions : NA

Version de l'ASA OS supportée : 8.2

Haute disponibilité supportée : Actif/Passif, Actif/Actif

VPN clustering et équilibrage de charge : Oui (Avec la version Security Plus)

II.2- Avantage d'ASA Cisco pour l'entreprise

Voici les avantages que procure la solution Cisco ASA 5500 séries VPN Edition :

- **Un accès distant à l'ensemble du réseau, basé sur les protocoles SSL et IPSec :** l'accès complet au réseau offre une connectivité d'utilisateur distant de la couche réseau à la quasi-totalité des applications ou ressources réseau. La connectivité est fournie via le client VPN SSL Cisco pour Web VPN ou par le client VPN IPSec Cisco. L'accès complet au réseau est généralement étendu aux postes de travail gérés (par exemple, les ordinateurs portables fournis aux employés). Grâce à la prise en charge des technologies VPN d'accès distant basées sur les protocoles SSL et IPSec, la gamme Cisco ASA 5500 séries offre une flexibilité et peut ainsi répondre aux exigences des scénarii de déploiement les plus variés.
- **Un accès réseau supérieur sans client :** l'accès distant sans client offre un accès aux ressources et applications réseau quel que soit l'emplacement de l'utilisateur, le

poste de travail n'étant pas nécessairement équipé d'un logiciel client VPN. Grâce à l'importance du chiffrement SSL disponible dans les navigateurs internet, la gamme Cisco ASA 5500 séries peut offrir un accès sans client à n'importe quelle ressource ou application Web, aux applications de services de terminal. Elle permet également l'accès aux applications client les plus courantes, comme la messagerie électronique, la messagerie instantanée, les calendriers et Telnet. D'autre part, les fonctionnalités supérieures de réécriture du contenu proposées par la gamme Cisco ASA 5500 séries permettent d'assurer le rendu fiable de pages Web complexes avec du contenu Java, Java Script et Active X.

- **Des VPN de site à site orientés réseau** : ils permettent de mettre en place une communication haut débit sécurisée entre plusieurs sites d'entreprise. La prise en charge de la qualité de service (QOS) et du routage à travers le VPN permet à la gamme Cisco ASA 5500 séries d'assurer une transmission fiable et de qualité professionnelle d'applications sensibles à la latence, comme les services de voix, de vidéo et de terminal.
- **Un VPN protégé contre les menaces** : les VPN constituent une source majeure d'infiltration de programmes nuisibles dans les réseaux des entreprises. Grâce à ses fonctionnalités de prévention des intrusions, d'antivirus, de pare-feu orienté application et de sécurité du point d'extrémité des VPN, la gamme Cisco ASA 5500 série permet de s'assurer que la connexion VPN ne devient pas la plaque tournante des menaces de sécurité.
- **Un fonctionnement et un déploiement plus économiques des VPN** : le dimensionnement et la sécurisation des VPN requièrent souvent un équilibre de charge et des équipements de sécurité supplémentaires, entraînant une augmentation des frais d'équipement et des charges d'exploitation. La gamme Cisco ASA 5500 séries intègre déjà ces fonctions, offrant ainsi un niveau d'intégration réseau et de sécurité sans précédent parmi les produits VPN actuellement sur le marché. Et en proposant les technologies VPN SSL et IPSec sur une seule plate-forme, la gamme Cisco ASA 5500 séries offre aux clients des alternatives économiques au déploiement d'infrastructures VPN parallèles.

- **Évolutivité et résistance** : prise en charge de 5 000 sessions utilisateur simultanées et possibilité d'évoluer vers des dizaines de milliers de sessions grâce aux fonctionnalités intégrées de cluster et d'équilibrage de charge. Les fonctions de « Stateful failover » (correction automatique sans changement d'état en cas de panne) offrent une grande disponibilité pour un temps de fonctionnement sans équivalent.[8]

II.3 - Principe fonctionnalité d'ASA

L'ASA offre deux modes pour ses utilisateurs :

- Le mode « routed » est de niveau 3 : quand il y a du trafic, l'ASA est comme un saut sur un routeur (« router hop in the network »)
- Le mode « transparent » est de niveau 2 : Il facilite la configuration du réseau. Le mode transparent permet de cacher le pare-feu (aux intrus éventuels). On utilise aussi le mode transparent pour du trafic qui ne serait pas autorisé par un routeur. Par exemple, il permet d'autoriser du multicast en utilisant une ACL EtherType.

Par défaut, l'ASA est en mode « routed ».

L'ASA offre de nombreuses fonctionnalités, majoritairement de sécurité. Nous vous présenterons dans la suite de cette partie celles qui nous paraissent les plus intéressantes, en soulignant que l'ASA offre beaucoup de fonctionnalités qui ne seront pas abordées.

II.3.1 – transformation les adresses de réseau NAT (Network address translation)

L'ASA est en partie un routeur. Il est donc logique qu'il offre du NAT : Il permet de transformer les adresses privées en adresses publiques afin de pouvoir avoir accès à des réseaux externes (exemple : réseau internet).

II.3.2 – qualités de services QoS (Quality of Service)

La QOS est un gestionnaire de trafic qui permet d'allouer les ressources réseau aux applications selon leur poids et leur priorité. En effet, dans le cas d'une

vidéoconférence, il doit faire de telle sorte à fournir un débit suffisamment important pour obtenir une image et une voix acceptable.

Pour implémenter la QoS, il faut :

- Spécifier Les classes de trafic
- Associer des actions à chaque classe de trafic afin de former une politique QoS

Une classe de trafic est un ensemble de trafics qui peut être identifié par le contenu de ses paquets. Par exemple, le trafic TCP dont le port à une valeur de 80 peut être mis dans la classe « trafic http ».

II.3.3 – Sécurité Contexte

Un ASA peut être partitionné en de multiples périphériques virtuels, appelés « Security Context ». Chaque contexte est un périphérique indépendant, ayant ses propres règles de sécurité, interfaces, et administrateurs. Avoir de multiples contextes équivaut à avoir plusieurs appareils indépendants. Plusieurs fonctionnalités peuvent y être utilisées, comme les tables de routage, les fonctionnalités de pare-feu, l'IPS et l'administration. Par contre, le VPN et les protocoles de routage dynamiques ne sont pas supportés.

II.3.4 – ACL (Access Control Lists)

A chaque interface connectée à l'ASA, un numéro de sécurité (entre 0 et 100) est attribué. Le réseau intérieur se voit attribué par défaut le numéro 100 et le réseau extérieur le numéro 0. Sans aucune spécification de la part de l'utilisateur, l'ASA interdit le trafic d'une interface vers une autre interface dont le numéro de sécurité est supérieur. Il autorise d'un autre côté le trafic vers un niveau de sécurité inférieur. Les Access Lists (ACL) ont été mises en place pour pouvoir interdire ou autoriser certains trafics d'une interface vers une autre. Elles sont composées d'ACE (Access Entries). Chaque ACE autorise ou refuse un trafic, en spécifiant l'adresse source et destination ainsi que le protocole.

Il existe deux types d'ACL :

- Standard.
- Etendue.

Listes de contrôle d'accès standard : Les listes de contrôle d'accès standard permettent d'autoriser et de refuser le trafic en provenance d'adresses IP source. La destination du paquet et les ports concernés n'ont aucune incidence.

Listes de contrôle d'accès étendues : Les listes de contrôle d'accès étendues filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP de destination, les ports TCP ou UDP source, les ports TCP ou UDP de destination, et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

II.3.5 – IPS (Intrusion Prevention Services)

Les ASA de la gamme 5500 peuvent utiliser l'AIP SSM. C'est un module de prévention d'intrusion qui surveille et effectue des analyses en temps réel du trafic sur le réseau.

Lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l'hôte attaquant, enregistrer l'incident, et envoyer une alerte au gérant du réseau. Les autres connexions légitimes continuent à fonctionner indépendamment, sans interruption.

II.3.5.a – AIP SSM

L'AIP SSM utilise un logiciel d'IPS (Intrusion Prevention Services) avancé qui fournit un service de protection pour stopper le trafic malicieux, notamment les vers et les virus réseau, avant qu'ils n'affectent le reste du réseau.

II.3.5.b – CSC SSM

Il fournit une protection contre les virus, les spywares, les spams et tout autre trafic non désiré en scannant les paquets FTP, HTTP, POP3, Et SMTP Que l'utilisateur lui demande de scanner.

II.3.6 La détection des menaces

L'ASA fournit une fonctionnalité très importante sous deux formes : la détection de menaces et la détection basique de menaces.

❖ La détection basique de menaces est celle qui est installée par défaut sur l'ASA. C'est celle-ci que l'on abordera rapidement, l'autre détection de menaces est à configurer par l'utilisateur.

❖ La détection basique de menaces détecte les activités qui pourraient être liées à une attaque, comme une attaque DoS (Deny of Service). Elle surveille le taux de paquets abandonnés et les événements liés à sécurité, à la recherche des éléments suivants :

- Refus par une ACL.
- Mauvais format de paquet.
- Attaque Dos détectée.
- Paquets ICMP suspects.
- Surcharge sur une interface.
- Paquets ayant échoué l'inspection d'applications.
- Attaque « scanning » détectée.
- Détection de session incomplète (ex : attaque TCP SYN détectée).

Lorsque l'ASA détecte une menace, il envoie un log au système. La détection basique de menaces n'a un impact, sur les performances de l'ASA, que lorsqu'il y a des abandons de paquets ou qu'une menace est détectée. Mais même dans ce cas, l'impact est quasi-insignifiant.

II.3.7 – Protection contre l'IP Spoofing

Pour se protéger contre cette menace, l'ASA inclut l'Unicast Reverse Path Forwarding (Unicast RPF), que l'on peut activer sur une interface. L'Unicast RPF donne l'instruction à l'ASA de regarder également l'adresse source (et non pas uniquement l'adresse de destination). En effet, pour chaque trafic que l'on autorise l'ASA à laisser passer, il crée une table de routage qui contient également la route vers l'adresse source. Il lui suffit donc d'observer l'adresse source et la table de routage afin de détecter les menaces.

II.3.8 – Normalisation TCP

La normalisation TCP est une fonctionnalité qui permet à l'administrateur réseau de rajouter des critères à la liste de ceux existants pour le scan d'un paquet TCP. En effet, cela offre la possibilité par exemple de :

- ✓ Vérifier le checksum
- ✓ Autoriser les paquets dont la taille des données dépasse la limite des paquets TCP
- ✓ Abandonner les paquets SYN contenant des données.

II.3.9 – AAA (Authentication, Authorization, Accounting)

AAA permet à l'ASA de savoir qui est l'utilisateur (authentification), ce qu'il est autorisé à faire (autorisation), ainsi que ce qu'il fait. Il offre ainsi une sécurité supplémentaire.

En effet, supposons que l'ACL autorise le trafic Telnet du réseau interne vers un réseau externe. N'ayant pas accès aux adresses IP des quelques utilisateurs étant autorisés à se connecter par Telnet, AAA permet l'authentification au moment de la connexion.

L'ASA peut également transmettre ces données à un serveur Radius ou TACACS.

II.3.9.a – Authentification

Elle vérifie le nom d'utilisateur et le mot de passe. On peut configurer l'ASA à mettre en place l'authentification :

- ✓ Les connexions administratives : SSH, Telnet, Console série, ASDM (avec https), gestion du VPN.
- ✓ La commande enable.
- ✓ L'accès au réseau et/ou au VPN.

II.3.9.b – Autorisation

Elle vérifie les autorisations pour chaque utilisateur (après authentification) pour les sessions suivantes :

- ✓ Les commandes de management
- ✓ L'accès au réseau et/ou au VPN

II.3.9.c – Surveillance

Elle permet de garder des traces du trafic qui passe à travers l'ASA. En activant l'authentification, l'ASA peut surveiller le trafic d'un ou plusieurs utilisateurs spécifiques.

II.3.10 – Les filtres HTTPS, FTP

Etant donnée la grande taille et la nature dynamique du net, l'utilisation des ACL n'est pas suffisante pour filtrer les sites web ou les serveurs ftp. Il est donc conseiller d'utiliser l'ASA en parallèle avec un serveur utilisant un produit de filtrage internet (ex : Websense Entreprise, Secure Computing SmartFilter).

Les performances du réseau peuvent être réduites considérablement par le serveur externe. Plus il est éloigné du réseau, plus son impact est important.

II.3.11 – Limites de connexions

L'ASA offre la possibilité de limiter le nombre de connexions TCP et UDP, le nombre de connexions à l'état embryonnaire, le nombre de connexions par utilisateur, ainsi que détecter les connexions mortes.

Les fonctionnalités supplémentaires qu'apporte la mise à jour d'ASA version 7.0 vers la version 8.0(2), voici celles que l'on considère les plus intéressantes :

- Le protocole de routage EIGRP.
- Fonctionnalités VPN :
 - Possibilité de demander un nom d'utilisateur et un mot de passe en plus du certificat pour les clients désirant se connecter par SSL VPN.
 - Clavier virtuel sur la page de connexion, pour éviter tout risque de piratage (ex : logiciels qui enregistrent ce qui est tapé).
 - Une autorité de certification pour le SSL VPN.

- Dynamic Access Policies (DAP) : les politiques d'accès peuvent être configurées dynamiquement.
- Possibilité de différencier les utilisateurs des administrateurs lors de l'accès à une base de donnée (ex : RADIUS ou LDAP (service d'annuaire)).
- Aide pour tagger le trafic client. Fonctionne pour les connexions clientless, IPSec et SSL.
- Possède une interface plus claire et plus facile d'utilisation.
- Autorise le trafic FTP.
- Un framework supplémentaire permet d'accepter les applications basée sur du TCP sans avoir à installer l'application cliente.
- Permet de créer des tunnels SSL juste pour certaines applications.
- Les administrateurs peuvent inclure au portail clientless des flux RSS.
- Les utilisateurs peuvent sauvegarder leurs favoris sur le serveur.
- Autorise des ressources IPv6 au dessus d'une connexion publique IPv4.

➤ Fonctionnalités du pare-feu :

- Inspection du trafic http.
- Permet de renommer une ACL.
- Permet de compter le nombre de paquets pour lesquels l'ASA vérifie s'ils sont autorisés par une ACE.
- de configurer du NAT en mode transparent.
- Permet de configurer plusieurs règles de sécurité sur l'AIP SSM.
- L'inspection SIP gère le protocole IPv6.

II.4 – Gestion du trafic

La configuration des interfaces, la mise en place des règles d'accès au réseau, et la gestion des utilisateurs sont autant de notions que nous avons du nous approprier avant de pouvoir débiter la configuration des VPNs.

II.4.1 – Le principe des niveaux de sécurité

Les ASA sont des périphériques orientés Sécurité. Cela engendre de nombreuses différences dans la philosophie des commandes les plus basiques telles que la configuration des interfaces. Ainsi, à chaque interface est associé un nom et un niveau de sécurité, qui déterminent les politiques de sécurité associées.

Les niveaux de sécurité vont de 0 à 100. 100 correspond à une confiance totale et un besoin accru de protéger ce réseau – ex : réseau interne – tandis que 0 correspond à un réseau dont on se méfie et dont la protection ne nous concerne pas – ex : Internet. Donner le nom `inside` à une interface lui attribue automatiquement un niveau de sécurité de 100. Tout autre nom d'interface, notamment `outside`, implique un niveau de sécurité de 0. Toutefois, il est possible de modifier le niveau de sécurité manuellement. Les niveaux de sécurité des interfaces influent sur les points suivants :

- **Accès réseau** : par défaut seules les communications depuis les interfaces de plus haut niveau vers celle de plus bas niveau peuvent avoir lieu. On dit que ces communications sont sortantes. Si les interfaces ont le même niveau, le trafic peut être autorisé entre elles avec la commande `same-security-traffic permit inter-interface`.
- **Moteurs d'inspection** : les comportements de certains moteurs d'inspection s'adaptent en fonction du niveau :
 - NetBIOS : s'applique seulement aux connexions sortantes.
 - SQL*Net : seule une connexion entrante de données est autorisée.
- **Filtrage** : les filtres HTTP et FTP s'appliquent uniquement aux connexions sortantes.
- **Contrôle NAT** : doit être configuré pour les connexions sortantes.
- **Commande established** : cette commande autorise les communications des interfaces de plus bas niveau vers celles de plus haut niveau si la connexion a été établie auparavant par l'interface de plus haut niveau.

II.4.2-liste de contrôle d'accès

Par défaut, les ASA bloquent tout trafic depuis une interface de faible niveau de sécurité vers une interface de plus haut niveau de sécurité. Les Access Control Lists (ACL) permettent d'affiner ce fonctionnement, voire de s'y opposer, si nécessaire.

Elles s'avèrent donc nécessaires dès que deux interfaces sont configurées et que l'on souhaite établir une communication entre les deux réseaux associés.

Bien qu'offrant des fonctionnalités plus étendues, leur fonctionnement général est identique à celui des ACLs présentes sur les autres routeurs Cisco.

II.4.3– Droits des utilisateurs

L'ASA supporte plusieurs types de serveurs AAA : Radius, LDAP, TACACS, etc. Comme son nom l'indique (AAA est l'acronyme de « Authentication, Authorization, Accounting »), un serveur AAA est responsable de l'identification, de la gestion des autorisations et de la sauvegarde des actions effectuées par les utilisateurs.

Nous avons limité notre étude au serveur AAA proposé par Cisco sur l'ASA. Il est possible de créer des utilisateurs sur l'ASA, leur associer un mot de passe, un niveau de privilège, une politique de groupe.

Le niveau de privilège varie entre 0 et 15, 0 correspondant à aucun accès à l'administration du routeur, et 2 étant la valeur par défaut. Les politiques de groupe régissent les conditions d'accès au réseau, et des propriétés relatives aux connexions VPN.

II.5-Discussion

Les Serveurs de Sécurité Adaptatifs Cisco ASA combinent les meilleurs services de VPN et de sécurité. Conçue comme l'élément principal de la solution « le réseau qui se défend tout seul ». Le résultat est une gamme de puissants serveurs de sécurité, réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux des grandes entreprises, tout en réduisant l'ensemble des frais de déploiement et d'exploitation, et en simplifiant les tâches généralement associées à un tel niveau de sécurité.

Chapitre 3

*La mise en œuvre d'un
tunnel Lan-to-Lan*

III.1-Préambule

L'objectif de cette partie était d'arriver à mettre en œuvre un tunnel VPN site-à-site. Nous avons donc décidé d'opter pour la configuration d'une entreprise ayant deux sites distants afin de pouvoir mettre en œuvre le tunnel site-à-site. Par ailleurs, nous avons opté pour un adressage privé, ce qui allait nous permettre de mettre en œuvre du NAT pour l'accès web, et de faire des exceptions au NAT pour l'accès au site distant.

III-2- Logiciel de simulation GNS3

GNS3 est un simulateur graphique d'équipement réseaux qui nous permet de créer des topologies de réseaux complexes et d'en établir des simulations. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS est le système d'exploitation des **routeurs, Switch et firewall** Cisco. Pour entrer dans l'interface graphique de chaque élément il faut télécharger son IOS.

GNS3 est compatible avec : **Windows, Linux,...**

La figure III.1 c'est la première figure qui s'ouvre lorsque on click sur le logiciel « GNS3 », cette figure nous présente l'emplacement des différentes icônes qu'on utilise pour créer un réseau :

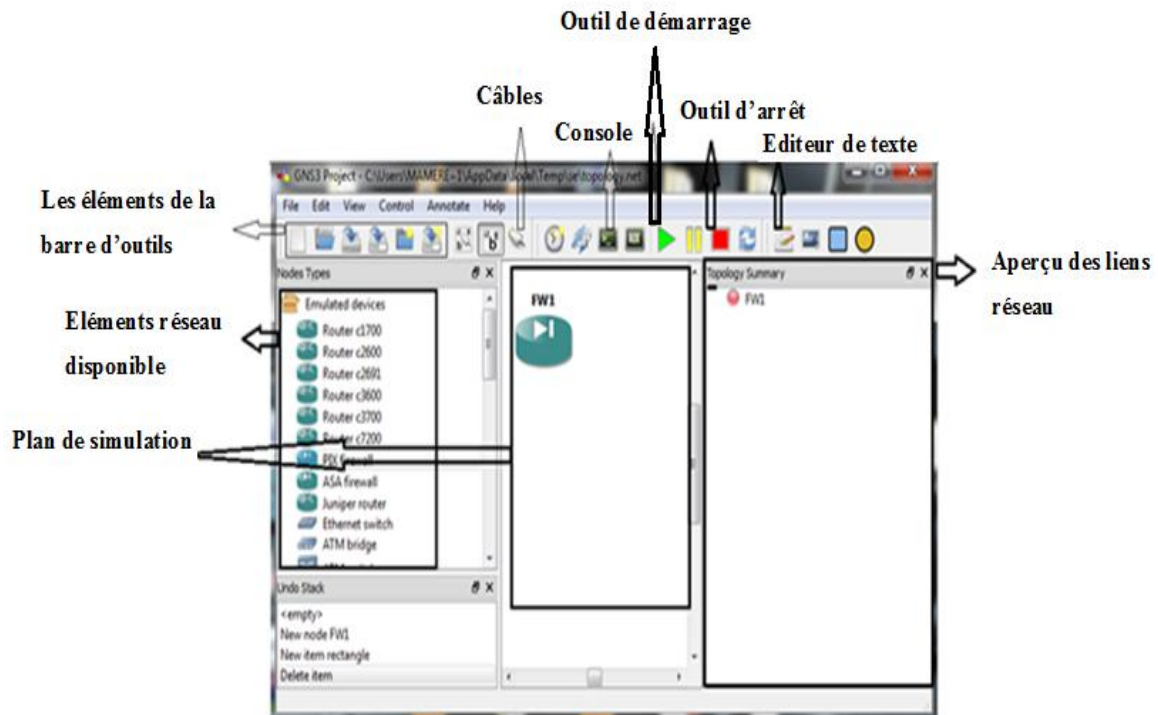


Figure III.1 : Détail de la fenêtre du simulateur

Pour ce qui concerne la configuration d'un ASA, on click sur EDIT → Préférences et la figure 2 s'ouvre. Puis en suit les étapes suivantes :

- Sélectionner l'onglet **Qemu**.
- Dans le champ ASA seting on donne le nom par exemple asa1
- Dans le champ ASA specific and seting on click sur parcourir () pour indiquer l'emplacement d'initrd et kernel.
- On click sur « APPLY » puis « OK ».

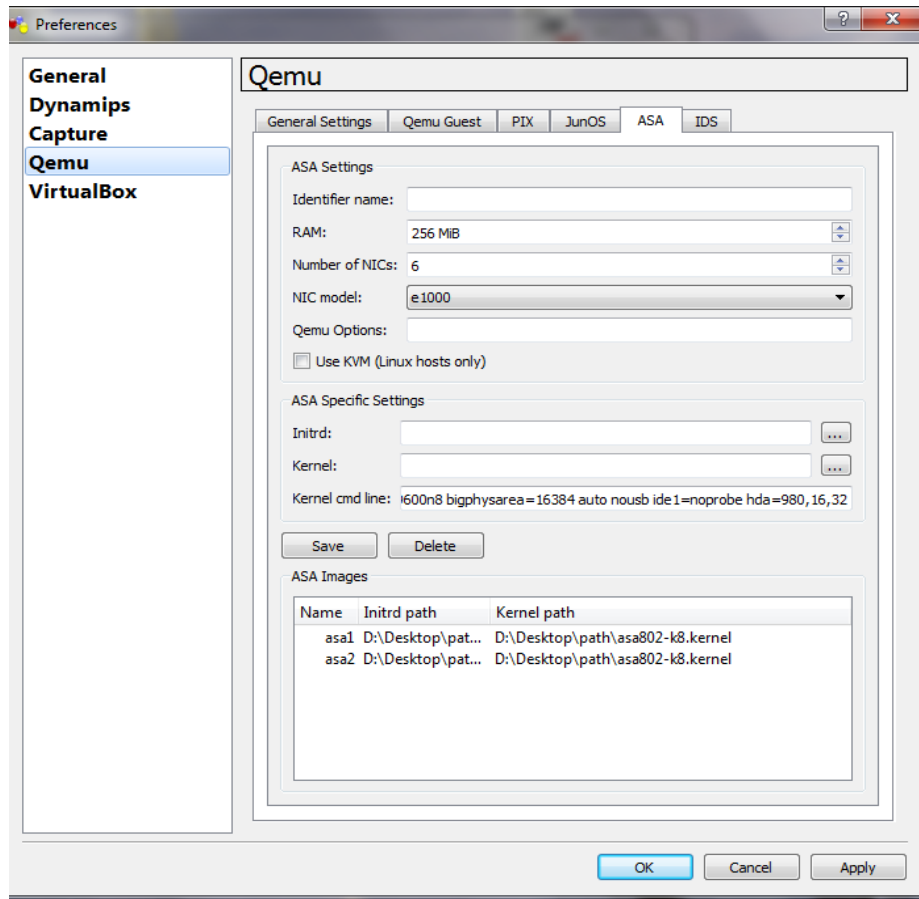


Figure III.2 : localisation du binaire de qemu

Maintenant on doit fournir notre propre IOS de Cisco à l'utilisation en GNS3. Une fois que nous avons obtenu notre propre copie d'un IOS de Cisco pour une des plateformes soutenues. Sur le menu edit on choisi IOS image and hypervisors.

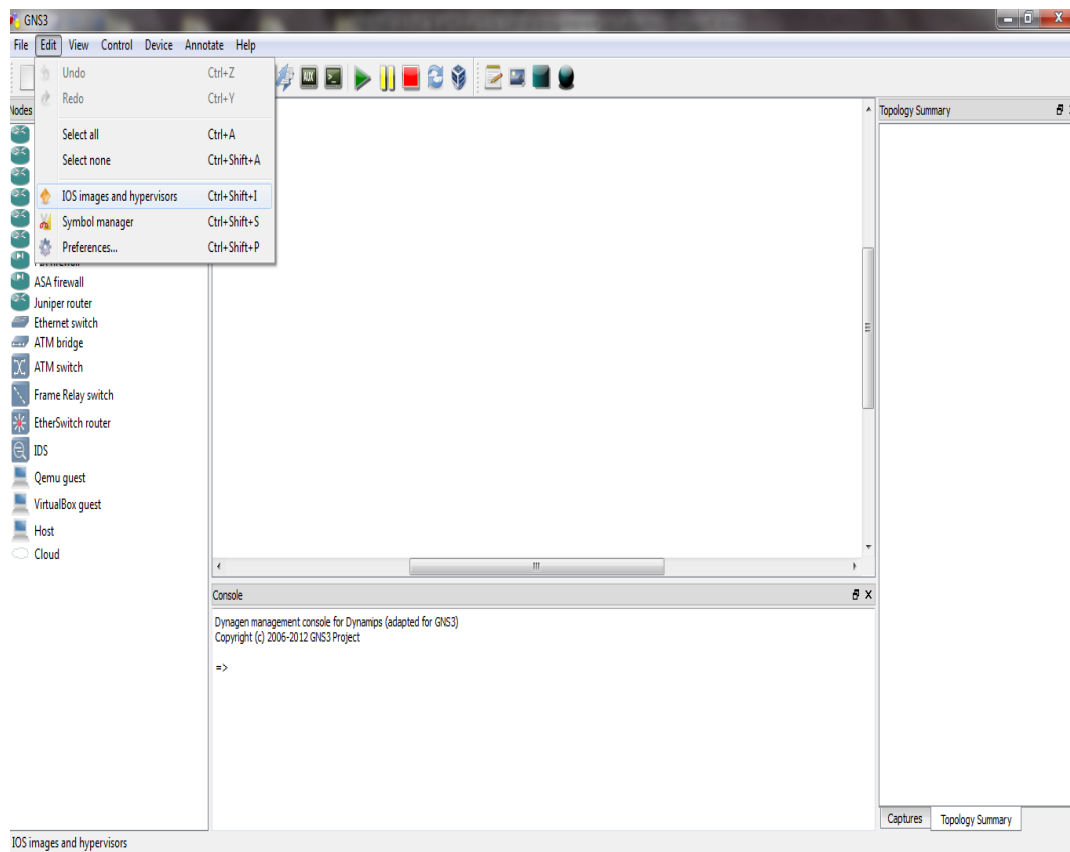


Figure III.3 : localisation de IOS and hypervisors

Sous l'étiquette *d'images d'IOS*, on click sur parcourir [...] pour indiquer l'emplacement de notre dossier d'image IOS puis on clic save et close.

Enfin notre logiciel gns3 est prés pour simuler notre réseau.

III.3-Mise en œuvre d'un tunnel LAN-TO-LAN

III.3.1-La topologie

Voici la topologie que nous avons choisi à mettre en place pour créer notre réseau :

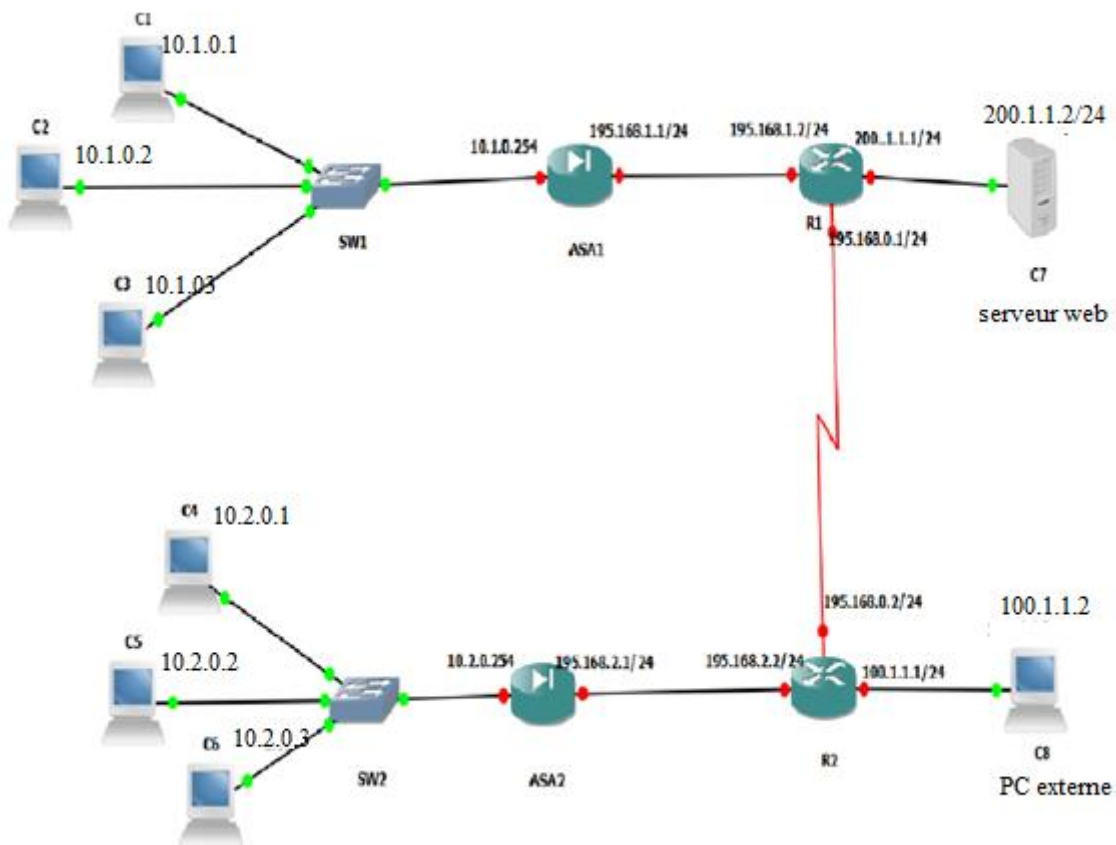


Figure III.5 : topologie du réseau choisi

On y retrouve :

- Les deux sites distants, possédant chacun trois PC, un switch et un ASA.
- Deux routeurs.
- Un serveur web, pour les tests NAT.
- Un pc externe pour le teste.

III.3.2 – Cahier des charges

Nous voulons faire communiquer les deux sites de l'entreprise de la même manière que s'ils étaient sur un réseau local. Nous utiliserons pour cela IPSec en mode tunnel. De plus, chaque site doit pouvoir accéder à Internet. Comme on veut conserver des adresses privées sur nos machines, nous allons faire du NAT sur les ASA pour l'accès web, et passer par le tunnel pour l'accès au site distant.

III.3.3– Adressage et connectivité

III.3.3.1 - Présentation

La première partie consiste à arriver à créer le réseau et réussir les tests de connectivité. Pour cela , deux routeur était utilisé entre les ASA, sur lesquels étaient implantées les routes statiques vers les réseaux 10.1.0.0/16 et 10.2.0.0/16.

Pour cela, il fallait réussir l'adressage des interfaces des ASA, découvrir et comprendre les mécanismes de sécurité, notamment les security levels, et arriver à passer outre.

III.3.2-Adressage des pc

La configuration des pc se fait comme indiquer dans le tableau suivant :

pc	Adresse ip	La passerelle par défaut	Le masque sous réseau
1	10.1.0.1	10.1.0.254	255.255.0.0
2	10.1.0.2	10.1.0.254	255.255.0.0
3	10.1.0.3	10.1.0.254	255.255.0.0
4	10.2.0.1	10.2.0.254	255.255.0.0
5	10.2.0.2	10.2.0.254	255.255.0.0
6	10.2.0.3	10.2.0.254	255.255.0.0
Serveur	200.1.1.2	200.1.1.1	255.255.255.0
Pc distant	100.1.1.2	100.1.1.1	255.255.255.0

Une fois que l'adressage des pc est terminé on passera à la configuration des routeurs.

III.3.3.3 - Configuration des routeurs

a- Le routeur 1

La première étape consiste à donner l'adresse IP pour chaque interface de routeur.

La configuration est la suivante :

```
*Sep  4 15:35:37.127: %LINK-5-CHANGED: Interface Serial1/7, changed state to administratively down
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname router1
router1(config)#interface fastethernet 0/0
router1(config-if)#ip address 195.168.1.2 255.255.255.0
router1(config-if)#no shutdown
router1(config-if)#interf
*Sep  4 15:38:04.255: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
router1(config-if)#interfac
*Sep  4 15:38:04.255: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Sep  4 15:38:05.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
router1(config-if)#interface fastethernet 0/1
router1(config-if)#ip address 200.1.1.1 255.255.255.0
router1(config-if)#no shutdown
router1(config-if)#
*Sep  4 15:40:12.847: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
router1(config-if)#
*Sep  4 15:40:12.847: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/1 Physical Port Administrative State Down
*Sep  4 15:40:13.847: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
router1(config-if)#exit
router1(config)#interface serial 1/0
router1(config-if)#ip address 195.168.0.1 255.255.255.0
router1(config-if)#clock rate 1255000
%Clockrate bestfitted (rounded) to 1344000
router1(config-if)#no shutdown
```

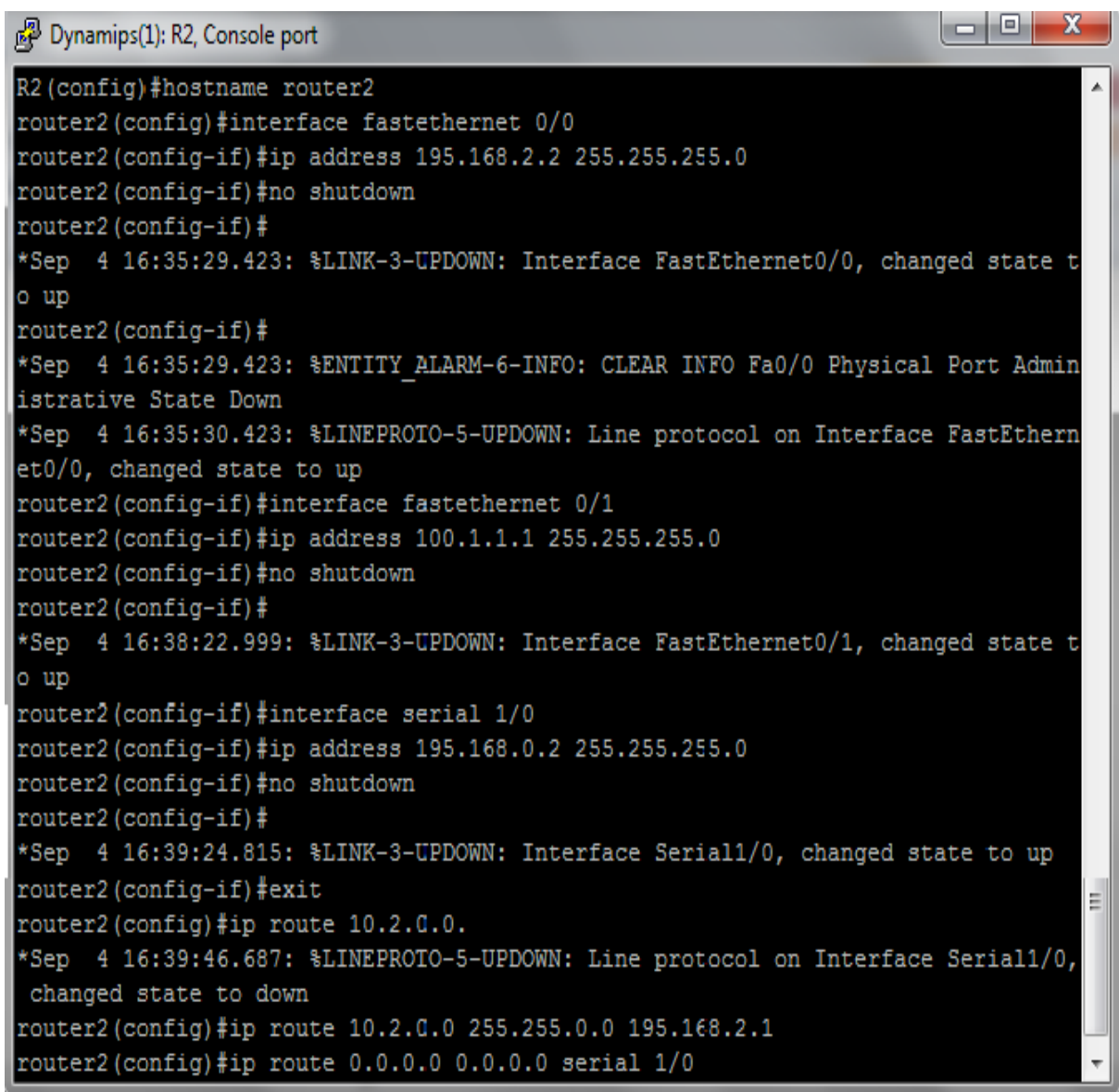
Dans la deuxième étape nous devons implanter deux routes statiques pour réussir la connectivité. Une route de réseau 10.1.0.0 vers l'interface de sortie de l'asa (195.168.1.1), et l'autre c'est la route par défaut vers la sortie du routeur (le serial).

La configuration est la suivante :

```
router1(config)#ip route 10.1.0.0 255.255.0.0 195.168.1.1
router1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

b- Le routeur 2

De même pour le routeur 2 nous devons adresser les interfaces ensuite les routes statiques comme suit :



```
Dynamips(1): R2, Console port
R2(config)#hostname router2
router2(config)#interface fastethernet 0/0
router2(config-if)#ip address 195.168.2.2 255.255.255.0
router2(config-if)#no shutdown
router2(config-if)#
*Sep  4 16:35:29.423: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
router2(config-if)#
*Sep  4 16:35:29.423: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Admin
istrative State Down
*Sep  4 16:35:30.423: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
router2(config-if)#interface fastethernet 0/1
router2(config-if)#ip address 100.1.1.1 255.255.255.0
router2(config-if)#no shutdown
router2(config-if)#
*Sep  4 16:38:22.999: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
router2(config-if)#interface serial 1/0
router2(config-if)#ip address 195.168.0.2 255.255.255.0
router2(config-if)#no shutdown
router2(config-if)#
*Sep  4 16:39:24.815: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
router2(config-if)#exit
router2(config)#ip route 10.2.0.0.
*Sep  4 16:39:46.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
changed state to down
router2(config)#ip route 10.2.0.0 255.255.0.0 195.168.2.1
router2(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0
```

III.3.4 -Configuration des ASA

III.3.4.1-Adressage

Passons maintenant à la configuration des ASA. Nous devons nous rappeler une règle de base : chaque interface d'ASA possède un niveau de sécurité compris entre 0 et 100. Si nous accordons une grande confiance au réseau se trouvant derrière une interface (le réseau dont nous avons la maîtrise par exemple), nous pouvons lui attribuer un niveau de sécurité élevé (ex : 100). A l'inverse, si nous n'avons pas confiance en un réseau (par exemple Internet), il serait judicieux d'affecter à l'interface à laquelle il est connecté un niveau de sécurité de 0. Par défaut, une fois les interfaces configurées, un paquet sera autorisé à passer d'une interface ayant un niveau de sécurité m vers une interface ayant un niveau de sécurité n si $m > n$. Pour que cela marche si $m = n$, nous devons en plus entrer la commande :

```
ASA(config)# same-security-traffic permit inter-interface
```

Ces petites précisions étant acquises, nous pouvons maintenant configurer les interfaces de nos ASA.

Voilà ce que cela donne sur ASA1 :

```

127.0.0.1 - PuTTY
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# conf t
ciscoasa(config)# clear configure all
WARNING: Config register and NV boot data structure damaged, it has been recreated.

Failed to write offset 218 to IDPROM ARRAY slot 0, I2C addr 0x4, dev 0xb0, error 7
ERROR: Password recovery was not changed, unable to access the configuration register.
ciscoasa(config)# hostname asal
asal(config)# interface ethernet 0/0
asal(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
asal(config-if)# ip address 10.1.0.254 255.255.0.0
asal(config-if)# no shutdown
asal(config-if)# exit
asal(config)# interface ethernet 0/1
asal(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
asal(config-if)# ip address 195.168.1.1 255.255.255.0
asal(config-if)# no shutdown
asal(config-if)# exit
asal(config)# route outside 0.0.0.0 0.0.0.0 195.168.1.2

```

Et ce que se donne sur ASA2

```

i2c_read_byte_w_suspend() error, slot = 0x4, device = 0xb0, address = 0 byte count = 1. Reason: I2C_SMBUS_UNSUPPORT
i2c_read_byte_w_suspend() error, slot = 0x4, device = 0xb0, address = 0 byte count = 1. Reason: I2C_SMBUS_UNSUPPORT
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# conf t
ciscoasa(config)# clear configure all
WARNING: Config register and NV boot data structure damaged, it has been recreated.

Failed to write offset 218 to IDPROM ARRAY slot 0, I2C addr 0x4, dev 0xb0, error 7
ERROR: Password recovery was not changed, unable to access the configuration register.
ciscoasa(config)# hostname asa2
asa2(config)# interface ethernet 0/0
asa2(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
asa2(config-if)# ip address 10.2.0.254 255.255.0.0
asa2(config-if)# no shutdown
asa2(config-if)# exit
asa2(config)# interface ethernet 0/1
asa2(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
asa2(config-if)# ip address 195.168.2.1 255.255.255.0
asa2(config-if)# no shutdown
asa2(config-if)# exit
asa2(config)# route outside 0.0.0.0 0.0.0.0 195.168.2.2

```

CHAPITRE III LA MISE EN ŒUVRE D'UN TUNNEL LAN-TO-LAN

Nous devons normalement pouvoir pinguer l'interface inside de l'ASA depuis un PC du site 1, et l'interface outside depuis le routeur1. Sachons que les interfaces de l'ASA ne répondent aux ping uniquement s'ils proviennent du même sous-réseau. Donc nous ne pourrons pas effectuer de ping du PC vers l'interface outside par exemple.

Nous allons tester alors les actions suivantes :

- Ping d'un PC vers un routeur.
- Ping d'un PC du site 1 vers un PC du site 2.
- Ping d'un routeur vers un PC.

Le ping d'un pc vers un routeur (195.168.1.2) :

```
PC>ping 195.168.1.2

Pinging 195.168.1.2 with 32 bytes of data:

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

Ping statistics for 195.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

Le ping d'un pc du site1 vers un pc du site2 (10.2.0.1) :

```
PC>ping 10.2.0.1

Pinging 10.2.0.1 with 32 bytes of data:

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

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

Le ping d'un pc du site2 vers un pc du site1

```
PC>ping 10.2.0.1

Pinging 10.2.0.1 with 32 bytes of data:

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

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>|
```

Nous constatons que cela ne fonctionne pas. Plusieurs problèmes sont en cause. Pour le premier cas, puisque le ping est initié du côté le plus sécurisé, cela devrait normalement marcher. Mais par défaut, l'ASA ne fait pas de suivi d'état ICMP, et n'autorise pas le ping du routeur. Pour remédier à ce problème, nous entrons les commandes suivantes, afin d'activer l'inspection ICMP :

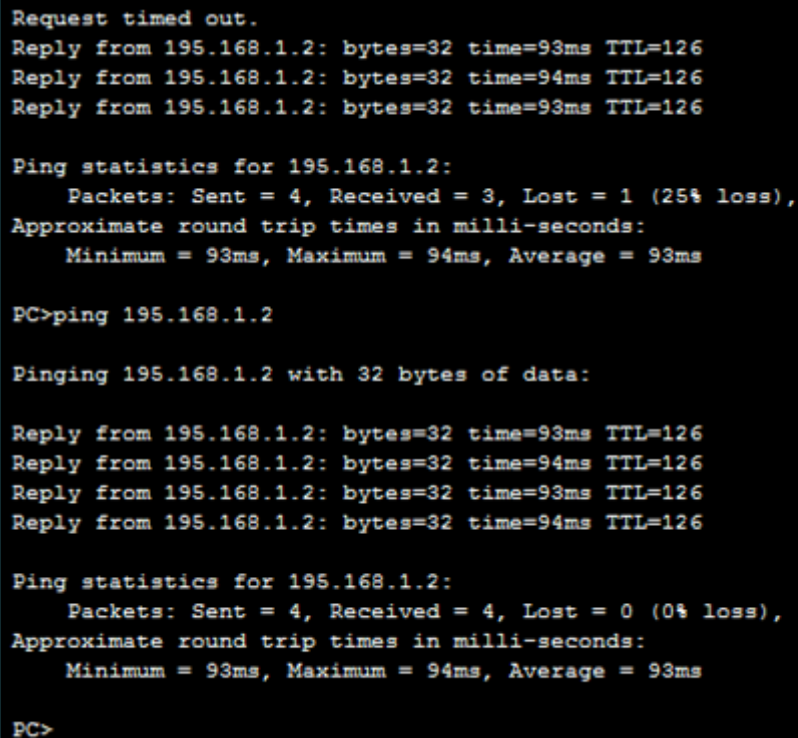
```
ASA(config)#policy-map global_policy
```

```
ASA(config)#class inspection_default
```

```
ASA(config)#inspect icmp
```

Vérifions que cela résoudre le premier problème.

Le ping d'un PC de site 1 vers un routeur 195.168.1.2 :



```
Request timed out.
Reply from 195.168.1.2: bytes=32 time=93ms TTL=126
Reply from 195.168.1.2: bytes=32 time=94ms TTL=126
Reply from 195.168.1.2: bytes=32 time=93ms TTL=126

Ping statistics for 195.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 94ms, Average = 93ms

PC>ping 195.168.1.2

Pinging 195.168.1.2 with 32 bytes of data:

Reply from 195.168.1.2: bytes=32 time=93ms TTL=126
Reply from 195.168.1.2: bytes=32 time=94ms TTL=126
Reply from 195.168.1.2: bytes=32 time=93ms TTL=126
Reply from 195.168.1.2: bytes=32 time=94ms TTL=126

Ping statistics for 195.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum = 94ms, Average = 93ms

PC>
```

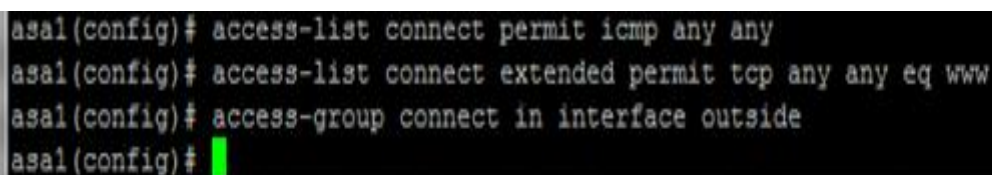
Le premier problème est résolu.

Les deux autres problèmes viennent du fait que l'on tente d'initier un ping d'une interface de faible niveau de sécurité vers une interface de haut niveau de sécurité, ce qui est interdit par l'ASA. Pour autoriser ces paquets, nous devons créer des access-list adaptées au type de trafic que l'on veut faire passer, puis les affecter à une interface, nous allons créer des access- list.

Nous allons autoriser ICMP pour les tests de connectivité, et HTTP pour les tests NAT.

Et voila les commandes à entrer :

ASA1 :



```
asa1(config)# access-list connect permit icmp any any
asa1(config)# access-list connect extended permit tcp any any eq www
asa1(config)# access-group connect in interface outside
asa1(config)#
```

ASA2 :

```
asa2(config)# access-list connect permit icmp any any
asa2(config)# access-list connect extended permit tcp any any eq www
asa2(config)# access-group connect in interface outside
asa2(config)#
```

Le test :

Vérifions qu'un pc d'un site 1 peu pinger un pc de site 2,

```
Request timed out.
Reply from 10.2.0.1: bytes=32 time=13ms TTL=126
Reply from 10.2.0.1: bytes=32 time=14ms TTL=126
Reply from 10.2.0.1: bytes=32 time=10ms TTL=126

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 12ms

PC>ping 10.2.0.1

Pinging 10.2.0.1 with 32 bytes of data:

Reply from 10.2.0.1: bytes=32 time=15ms TTL=126
Reply from 10.2.0.1: bytes=32 time=12ms TTL=126
Reply from 10.2.0.1: bytes=32 time=10ms TTL=126
Reply from 10.2.0.1: bytes=32 time=9ms TTL=126

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 11ms
```

Et que les deux sites ont accès au serveur web 200.1.1.2.

```
PC>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time=14ms TTL=126
Reply from 200.1.1.2: bytes=32 time=10ms TTL=126
Reply from 200.1.1.2: bytes=32 time=13ms TTL=126
Reply from 200.1.1.2: bytes=32 time=8ms TTL=126

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 11ms

PC>|
```

III.3.4.2 Etablissement du NAT

Nous supposons que chaque site dispose d'une unique adresse IP routable, ce qui impose d'utiliser un NAT dynamique (n IP privées pour m IP publiques, pour tout m et n > 0), contrairement à un NAT statique, où chaque IP privée possède exactement un équivalent public. Les deux versions du NAT sont implémentées par les ASA.

La configuration du NAT dynamique au niveau d'ASA1 est illustrée dans la figure qui suit :

```
ASA1(config)# nat (inside) 1 10.1.0.0 255.255.0.0
ASA1(config)# global (outside) 1 195.168.1.3
INFO: Global 195.168.1.3 will be Port Address Translated
ASA1(config)# access-list NONATVPN extended permit ip 10.1.0.0 255.255.0.0 10.$
ASA1(config)# nat (inside) 0 access-list NONATVPN
```

La configuration du NAT dynamique au niveau d'ASA2 est illustrée dans la figure qui suit :

```
ASA2(config)# nat (inside) 1 10.2.0.0 255.255.0.0
ASA2(config)# global (outside) 1 195.168.2.3
INFO: Global 195.168.2.3 will be Port Address Translated
ASA2(config)# access-list NONATVPN extended permit ip 10.2.0.0 255.255.0.0 10.$
ASA2(config)# nat (inside) 0 access-list NONATVPN
```

III.3.5 – Etablissement du tunnel VPN

III.3.5.1– Présentation

Nous allons présenter le principe de configuration d'un VPN LAN to LAN. Il ne s'agit pas ici d'effectuer un recueil de commandes, mais de présenter les quelques étapes clef de cette configuration.

La première étape est la configuration du protocole ISAKMP. Ce dernier est utilisé pour trouver une politique de sécurité commune entre les deux extrémités du tunnel. Cette politique de sécurité définit un ensemble de méthodes visant à protéger et authentifier les données. Une politique ISAKMP regroupe une méthode d'authentification, une méthode de cryptage, une méthode de hachage, un groupe de Diffie-Hellman et une limite de temps pour le remplacement des clefs de cryptage. Mis à part des exceptions sur le temps de renouvellement des clefs, les autres paramètres de la politique de sécurité doivent être les mêmes sur les deux hôtes pour qu'ils puissent poursuivre la communication.

Une fois la politique ISAKMP déterminée, il nous faut maintenant créer notre tunnel. Pour cela, on doit configurer un ensemble de paramètres, regroupés dans ce que l'on appelle une association de sécurité (SA). Sur les ASA, une SA regroupe les éléments suivants, qu'il nous faudra configurer :

- Un ou plusieurs transform sets.
- Une ou plusieurs crypto maps.
- Une ou plusieurs access-lists.
- Un tunnel group.

En fait, une crypto map regroupe un transform set, une ou plusieurs ACL et un hôte distant. Chaque crypto map permet de protéger le trafic spécifié dans son ACL, pour le tunnel spécifié par l'hôte distant, avec les moyens indiqués par son transform set. On pourra ainsi se servir de plusieurs crypto map attribuées au même tunnel, afin de protéger plusieurs types de trafic de manière différente.

Un transform set est une combinaison de protocoles de sécurité et d'algorithmes qui définissent comment l'ASA protège les données (une méthode d'authentification et une méthode de cryptage). Pendant la phase de négociation de l'association de sécurité, les deux pairs doivent identifier un transform set commun. Les ASA appliquent alors le transform set élu pour protéger les flux de données identifiés dans l'ACL associée à la crypto map qui implémente le transform set. Un exemple de transform set pourrait être d'utiliser ESP, avec 3des comme méthode de cryptage, et sha1 comme méthode de hachage. Il est par ailleurs à noter que les transform set de l'ASA ne proposent pas AH pour le protocole IPSec.

Il nous reste donc à expliquer ce qu'est un tunnel group. Il regroupe un ensemble de paramètres qui spécifient la politique de connexion au tunnel, comme par exemple un serveur d'authentification, des politiques de groupe, etc ... Deux types de tunnel group sont déjà pré-configurés sur les ASA, un concernant les VPN Lan-to-Lan, l'autre les VPN Remote Access. Pour notre projet, nous intéressent à créer un tunnel-group de type Lan-to-Lan, et de spécifier les paramètres de la méthode d'authentification. Comme nous avons choisi une authentification par clef pré-partagée, il nous fallait par exemple spécifier la clef.

En résumé, pour configurer un tunnel VPN Lan-to-Lan basique, il faut suivre les étapes suivantes :

- Définir une politique ISAKMP.
- Définir un transform set et spécifier les méthodes de protection des données.
- Définir un tunnel group et spécifier les paramètres d'authentification.
- Définir une ACL définissant le trafic à protéger.
- Associer l'ACL, le transform set et l'adresse de l'autre extrémité dans une crypto map.

III.3.5.2 – Paramètres ISAKMP

ISAKMP (Internet Security Association and Key Management Protocol) est le protocole de négociation nécessaire pour que les deux hôtes se mettent d'accord sur une politique de sécurité. ISAKMP sépare la négociation en deux phases. La première phase crée un premier tunnel, qui protégera les négociations du protocole ISAKMP. La deuxième phase crée le tunnel qui protégera les données.

Nous allons donc devoir créer une ou plusieurs politiques ISAKMP, qui regroupent les éléments suivants :

- une méthode d'authentification (pre-share, crack, rsa-sig).
- une méthode de cryptage (aes, aes-192, aes-256, des, 3des).
- une méthode de hachage (md5, sha).
- un groupe de Diffie-Hellman (1, 2, 5, 7).
- une limite de temps pour le remplacement des clefs de cryptage (en secondes).

Comme plusieurs politiques de sécurité peuvent être créées, il faudra définir leur priorité (plus petit c'est la plus prioritaire). Ici, nous ne créerons qu'une seule politique ISAKMP. Tous les paramètres ISAKMP doivent être les mêmes des deux côtés du tunnel, mis à part la durée de remplacement des clefs, qui doit être plus petite (ou égale) sur le répondeur que sur l'initiateur de la connexion.

Voici les commandes que nous devons exécuter pour établir une politique ISAKMP sur ASA1 :

```
asa1(config)#  
asa1(config)# crypto isakmp policy 1 encryption 3des  
asa1(config)# crypto isakmp policy 1 hash sha  
asa1(config)# crypto isakmp policy 1 authentication pre-share  
asa1(config)# crypto isakmp policy 1 group 2  
asa1(config)# crypto isakmp policy 1 lifetime 86400
```

CHAPITRE III LA MISE EN ŒUVRE D'UN TUNNEL LAN-TO-LAN

Les commandes que nous devons exécuter pour établir une politique ISAKMP sur ASA2 :

```
asa2(config)# crypto isakmp policy 1 encryption 3des
asa2(config)# crypto isakmp policy 1 hash sha
asa2(config)# crypto isakmp policy 1 authentication pre-share
asa2(config)# crypto isakmp policy 1 group 2
asa2(config)# crypto isakmp policy 1 lifetime 86400
```

Une fois notre politique de sécurité créée, nous pouvons activer le protocole ISAKMP sur l'interface outside avec la commande :

Sur asa1 :

```
asa2(config)# isakmp enable outside
```

Sur asa2 :

```
asa1(config)# isakmp enable outside
```

III.3.5.3-Transform set

Lorsque nous créons un tunnel VPN, nous voudrions que des données moins sensibles soient moins bien protégées que des données très sensibles, afin d'économiser le temps du processeur et de la bande passante. C'est à cela que servent les transform set. Ils sont associés à des ACL, elles-mêmes associées à des crypto map. Un transform set combine une méthode de cryptage et une méthode de hachage. Sachons simplement qu'au moins un transform set doit être créé pour pouvoir faire fonctionner un tunnel VPN, et que les deux ASA aux extrémités du tunnel doivent avoir au moins un transform set en commun. Sur chacun des ASA, nous créerons donc le transform set suivant :

ASA1 :

```
asa1(config)# crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
```

ASA2 :

```
asa2(config)# crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
```

III.3.5.4-Tunnel group

Un tunnel group est une liste de paramètres de connexion pour la création de tunnel VPN. Là encore, la configuration est assez complexe, et nous ne rentrerons pas dans le détail. Par défaut , un ASA contient deux tunnels groups déjà enregistrés : le premier est utilisé pour les tunnels End-to-Lan, le second pour les tunnels Lan-to-Lan.

Créez un tunnel group de type Lan-to-Lan sur chaque ASA, à l'aide de la commande suivante :

asa1 :

```
asa1(config)# tunnel-group 195.168.2.1 type ipsec-l2l
```

ASA2 :

```
asa2(config)# tunnel-group 195.168.1.1 type ipsec-l2l
```

Comme nous avons pu le remarquer, certaines contraintes sur le matériel cisco semblent douteuses. Dans le cas des tunnels groups, le nom du tunnel doit être une adresse IP, sauf si nous sommes en mode ISAKMP. Dans ce cas là, nous pouvons mettre une chaîne de caractères quelconque. Dans notre projet nous choisissons de mettre sur chaque ASA une adresse IP de l'autre extrémité du tunnel comme nom de tunnel group.

Nous devons maintenant définir la clef pré-partagée entre les deux extrémités du tunnel :

ASA1 :

```
asa1(config)# tunnel-group 195.168.2.1 ipsec-attributes
asa1(config-tunnel-ipsec)# pre-shared-key toto
```

ASA2 :

```
asa2(config)# tunnel-group 195.168.1.1 ipsec-attributes
asa2(config-tunnel-ipsec)# pre-shared-key toto
```

La clef pré-partagée toto est utilisée ici pour éviter des erreurs et des pertes de temps. Dans la réalité, si nous sommes amenés à choisir une clef pré-partagée, choisissons une combinaison de chiffres et de lettres suffisamment longue, ne figurant pas dans un dictionnaire et n'ayant aucune signification particulière.

III.3.5.5-Crypto map

Avant d'expliquer ce qu'est une crypto map, nous devons configurer une ACL permettant le trafic dans le tunnel. Rappelons que tout est interdit sur les ASA, et depuis le début de ce projet, nous n'avons autorisé que le trafic ICMP et certaines requêtes HTTP. Nous devons donc autoriser les paquets IP entre les deux sites distants. Cette ACL sera associée à une crypto map, et c'est le trafic spécifié par cette ACL qui sera protégé avec les méthodes spécifiées par le transform set de la crypto map.

Nous utiliserons l'ACL suivante sur l'ASA1, et son miroir sur l'ASA2 :

```
asa1(config-tunnel-ipsec)# access-list ipvpn extended permit ip 10.1.0.0 255.255.255.255 10.2.0.0 255.255.255.255
```

```
asa2(config-tunnel-ipsec)# access-list ipvpn extended permit ip 10.2.0.0 255.255.255.255 10.1.0.0 255.255.255.255
```

CHAPITRE III LA MISE EN ŒUVRE D'UN TUNNEL LAN-TO-LAN

La crypto map est l'élément qui rassemble tous les paramètres d'association de sécurité IPsec que nous avons créés précédemment. Elles peuvent être assez complexes, donc nous n'étudierons que les paramètres les plus basiques, en protégeant tous les flux traversant le tunnel de la même manière. La crypto map définit quel trafic à protéger (défini dans une access-list), où envoyer le trafic protégé (adresse publique de l'autre extrémité du tunnel) et quelles sécurités appliquer au trafic (application du transform set). Les crypto map doivent bien entendu être compatibles entre les deux extrémités du tunnel. Pour éviter les erreurs, nous définirons exactement les mêmes paramètres sur les deux ASA, mais cela n'est pas obligatoire.

Voici les commandes à entrer sur l'ASA1 :

```
asa1(config)# crypto map mymap 1 match address ipvpn
asa1(config)# crypto map mymap 1 set peer 195.168.2.1
asa1(config)# crypto map mymap interface outside
```

Et les commandes à entrer sur l'ASA2 :

```
asa2(config)# crypto map mymap 1 match address ipvpn
asa2(config)# crypto map mymap 1 set peer 195.168.1.1
asa2(config)# crypto map mymap 1 set transform-set esp-3des-sha
asa2(config)# crypto map mymap interface outside
asa2(config)#
```

III.3.6-Vérification

Nous allons tester les actions suivantes :

- Ping d'un PC du site 1 vers un PC du site 2.
- Ping d'un PC du site 1 vers un PC externe
- Ping d'un PC du site 2 vers un PC du site 2.
- Ping d'un PC du site 1 vers un PC externe.
- Ping d'un pc du site 1 vers le serveur.
- Ping d'un PC du site 2 vers le serveur.
- Ping d'un PC externe vers un PC du site 1

- Ping d'un PC externe vers un PC du site 2

Ping d'un PC du site 1 vers un PC du site 2.

```
Request timed out.
Reply from 10.2.0.1: bytes=32 time=13ms TTL=126
Reply from 10.2.0.1: bytes=32 time=14ms TTL=126
Reply from 10.2.0.1: bytes=32 time=10ms TTL=126

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 12ms

PC>ping 10.2.0.1

Pinging 10.2.0.1 with 32 bytes of data:

Reply from 10.2.0.1: bytes=32 time=15ms TTL=126
Reply from 10.2.0.1: bytes=32 time=12ms TTL=126
Reply from 10.2.0.1: bytes=32 time=10ms TTL=126
Reply from 10.2.0.1: bytes=32 time=9ms TTL=126

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 15ms, Average = 11ms
```

Ping d'un PC du site 2 vers un PC du site 1

```
PC>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:

Reply from 10.1.0.1: bytes=32 time=125ms TTL=128
Reply from 10.1.0.1: bytes=32 time=62ms TTL=128
Reply from 10.1.0.1: bytes=32 time=63ms TTL=128
Reply from 10.1.0.1: bytes=32 time=62ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 125ms, Average = 78ms|

PC>
```

CHAPITRE III LA MISE EN ŒUVRE D'UN TUNNEL LAN-TO-LAN

Ping d'un pc du site 1 vers le serveur 200.1.1.2 :

```
PC>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time=14ms TTL=126
Reply from 200.1.1.2: bytes=32 time=10ms TTL=126
Reply from 200.1.1.2: bytes=32 time=13ms TTL=126
Reply from 200.1.1.2: bytes=32 time=8ms TTL=126

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 11ms

PC>|
```

Ping d'un PC du site 1 vers un PC externe

```
PC>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time=125ms TTL=128
Reply from 100.1.1.2: bytes=32 time=47ms TTL=128
Reply from 100.1.1.2: bytes=32 time=62ms TTL=128
Reply from 100.1.1.2: bytes=32 time=63ms TTL=128

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 125ms, Average = 74ms

PC>|
```

Ping d'utilisateur distant vers un pc du site 1

```
PC>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:

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

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping d'utilisateur distant vers un PC du site 2

```
PC>ping 10.2.0.1

Pinging 10.2.0.1 with 32 bytes of data:

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

Ping statistics for 10.2.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Nous constatons qu'un PC du site 1 peut pinguer un PC du site 2, un serveur web et un utilisateur distant et de même pour un pc de site 2. Mais un utilisateur externe n'a pas accès aux PC du site 1 ni aux PC du site 2. Cela est l'objectif de notre projet.

III.4-Discussion

LA configuration de l'Adaptative Security Appliance (ASA) permet à une entreprise de créer des tunnels VPN économiques, simples, et plus sécurisés contre les attaques de réseau extérieur : vers, virus, logiciels espions, enregistreurs de frappe, chevaux de Troie, pirates informatiques.

Conclusion générale

CONCLUSION

Dans notre mémoire nous nous sommes intéressés à garantir un échange d'information sécurisé entre les différents réseaux d'entreprise .Pour cela on a choisit un matériel cisco qui est l'ASA (adaptive security appliance).

Ce projet nous a permet d'acquérir des connaissances dans de nombreux domaines, il nous a initié au mode de recherche sur les réseaux surtout en ce qui concerne leurs sécurisations, la configuration de divers matériel Cisco , tels que : routeur , switch et l'ASA .De plus on s'est familiariser avec des logiciels de simulation :**Packet Tracer** et **GNS3**.

Annexe 1

1-Introduction :

L'objectif de ce chapitre est d'apprendre les différentes fonctionnalités des équipements matériels utilisés ainsi que leurs configuration de base.les équipements a décrire sont :

Le routeur ; l' ASA ; le switch.

2-le routeur cisco :

2-a-La description de routeur cisco :

Un routeur Cisco est un équipement dédié aux tâches de routage des paquets IP. Les routeurs Cisco sont conçus à sur base d'une architecture de processeurs (CPU) Motorola Risc. Le CPU communique à travers un Bus sur une carte mère qui connecte différents types de mémoire et des interfaces de communication détaillés ci-après.

Type de mémoires :

Mémoire	Contenu	Commande
RAM (DRAM)	Fichier de configuration courante	#show running-config
	Tables de routage	#show ip route
	Cache ARP	#show arp
	Mémoire de travail	#show memory

ROM EPROM	Post Bootstrap Mode Rom Monitor ou RXBoot Trouve et charge l'ios	
Flash EPROM , SIMM ou PCMCIA	Emplacement de l'image IOS Fichiers de configuration supplémentaires Images supplémentaires de l'IOS	#show flash
NVRAM	Fichier de configuration de démarrage Registre de configuration	#show startup-config #show version

Les interfaces

Les interfaces permettent au routeur d'interconnecter les réseaux pour le routage et la commutation. Elles sont utiles à la transmission des données sur le média.

En fonction des technologies, on trouvera différents type d'interfaces LAN ou WAN :

- Ethernet, Token Ring, WLAN, FDDI, etc.
- Série, Asynchrone, BRI (ISDN), etc

Les ports

Les ports, à proprement parler, permettent de gérer le routeur à distance.

On trouvera :

- Le **port console** qui autorisera une communication physique sérielle vers une station de travail sur laquelle est installé un logiciel de communication comme [Putty](#).
 - Le **port auxiliaire (AUX)** qui permettra une connexion via modem.
 - Les **ports virtuels (VTY)**, donnant accès à la console à travers TCP/IP.
- Les services (Telnet, SSH, RLOGIN, etc.) sont activés à travers les lignes.



Figure : Vue de l'arrière du routeur

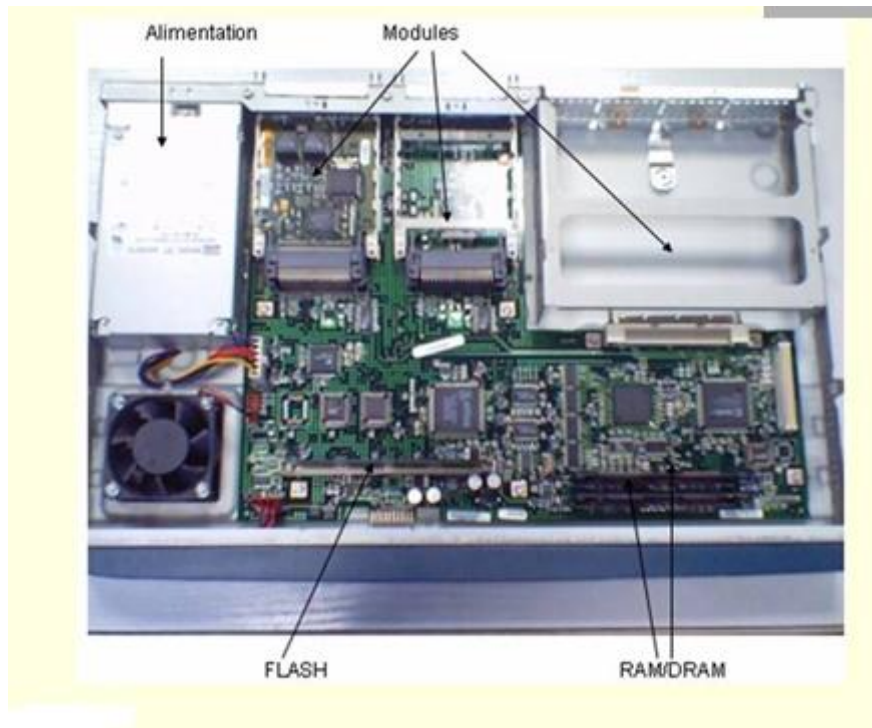


Figure 5 : Vue de l'intérieur du routeur

2-b - les fonctionnalités :

La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- Déterminant le meilleur chemin pour l'envoi des paquets,
- Transférant les paquets vers leur destination.

3- le Switch Cisco:

Les commutateurs intelligents Cisco Catalyst, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité FastEthernet et GigabitEthernet optimisent les services de LAN sur les réseaux d'entreprise.

Et ces caractéristiques sont :

- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de Contrôle d'accès (ACL) élaborées et une sécurité optimisée

- Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.



4-Les modes configuration de matériel Cisco :

- mode utilisateur, accès restreint avec un prompt en '>'
- mode enable ou privilège, accès par la commande 'enable' avec un prompt en '#'
- mode de configuration, accessible à partir de enable par la commande 'configure', prompt en 'configure#'; le mode de configuration le plus utilisé est 'configure terminal', il existe aussi 'memory' et 'network'

5- les commandes utiliser pour la configuration d'un Switch et d'un routeur :

- Le tableau suivant représente les différentes commandes utilisé pour la configuration d'un Switch et d'u routeur Cisco.

<i>Commandes</i>	<i>Descriptions</i>
configure terminal ou conf t ou conf term	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet fastethernet Serial loopback <interface> ou int e fa s lo	Entre dans le mode de configuration de l'interface
ip address <address> <mask> ou ip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type>] ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	
copy running-config startup-config ou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM

copy running-config tftp ou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-config tftp ou copy star tftp	Sauvegarde la configuration situé en NVRAM vers un serveur TFTP
copy tftp startup-config ou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-config ou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration courante
Commandes	Descriptions
erase startup-config ou erase star	Efface la configuration de la NVRAM
Configuration d'une connexion en telnet:	
router# conf t	
router(config)# line console 0	
router(config)# login	
router(config)# password xyz	
Les commandes de configurations du routage :	
router <xxx> [<process- id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur

<i>exemple de configuration du routage RIP:</i>	
router# conf t	
router(config)# router rip	
router(config-router)# version 1-2	la version 2 apporte le routage CIDR et l'utilisation de VLSM, un nombre de sauts à 128
router(config-router)#network networknumber	
<i>exemple de configuration du routage OSPF:</i>	
router# conf t	
router(config)# router ospf 10	
router(config-router)# network network number	
<i>exemple de configuration du routage IGRP:</i>	
router# conf t	
router(config)# router igrp autonomous system	
router(config-router)# network networknumber	
<i>exemple de configuration du routage EIGRP:</i>	
router# conf t	
router(config)# router eigrp	

<i>autonomous system</i>	
router(config-router)# network <i>networknumber</i>	
<i>exemple de configuration du routage BGP:</i>	
router# conf t	
router(config)# router bgp <i>autonomous system</i>	
router(config-router)# network <i>networknumber</i> [mask <i>network-mask</i>] [route-map <i>route-map-name</i>]	
<i>D'autres commandes de routage</i>	
ip multicast-routing	Permet de faire du routage multicast
ip rsvp bandwidth [<i>interface-kbps</i>] [<i>singleflow-kbps</i>]	Active la réservation RSVP sur une interface
Les commandes sur un Switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan :	

switch# vlan database switch(vlan)# vlan <number> <name> switch(vlan)# exit switch(config)#interface fa<iface-number> switch(config)#interface range fa... switch(config-if)#switchport mode access	affectation sur un port affectation sur un ensemble de ports on passe le mode de configuration de l'interface
Commandes	Descriptions
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le trunking sert dans l'extention d'un domaine VLAN sur d'autre switch, pour se faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchport trunk encap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	On active le mode trunk sur le port du commutateur serveur et client qui font le trunk le reste des ports sont en mode

	access
vlan database vtp domain <domain-name> vtp server	Création d'un serveur VTP
vlan database vtp domain <domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	
reload	Redémarre l'équipement réseau
setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
Les commandes show :	
show interfaces ou sh int	Donne une description détaillé sur les interfaces
show running-config ou sh run	affiche la configuration courante
Commandes	Descriptions
show startup-config ou sh star	affiche la configuration en NVRAM

show ip route ou sh ip route	affiche la table de routage
show ip <routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ip protocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

Annexe 2

1-introduction :

L 'objectif du ce chapitre c'est de se familiariser avec le modèle théorique O.S.I. qui décrit comment l'O.S. réseau, encore appelé N.O.S. doit être construit. On décrit dans ce qui suit l'architecture en 7 couches logicielles qui présentant chacune des interfaces standard pour communiquer entre elles.

2-La communication sur un réseau :

Le fondement d'un bon réseau, c'est que le système d'exploitation soit capable:

- De gérer la transmission de données.
- De fournir aux applications des interfaces standard pour leur permettre d'exploiter les ressources du réseau.

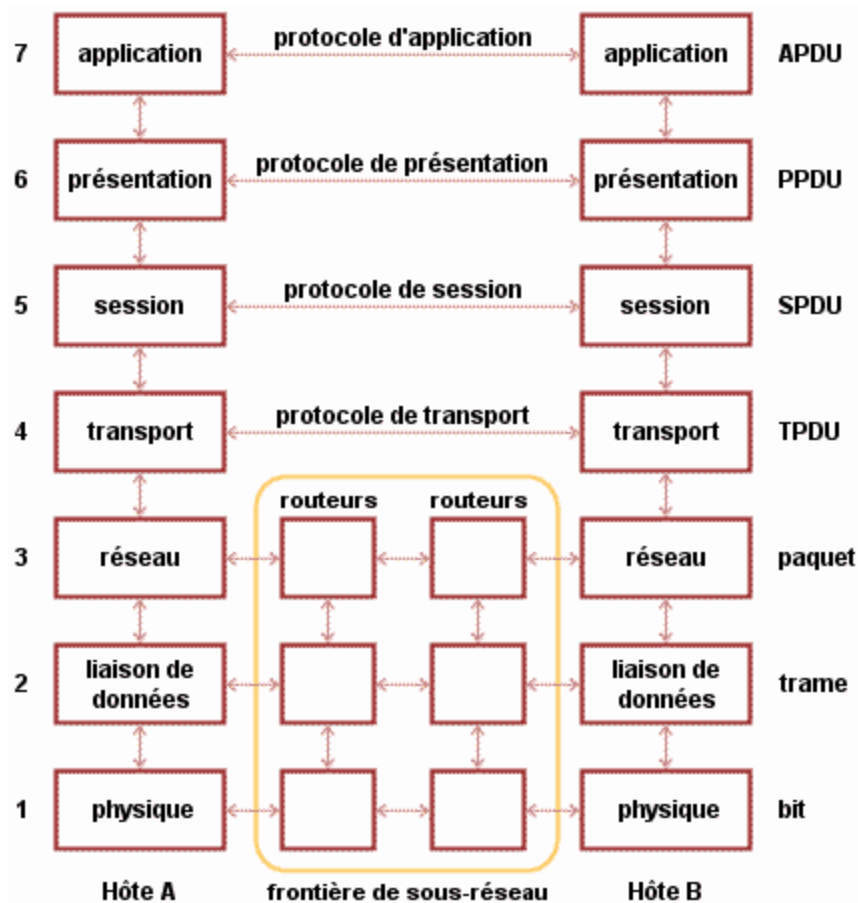
C'est le cas de tous les systèmes d'exploitation à jour.

A priori, rien ne devrait obliger les plates formes client et serveur à fonctionner avec le même système d'exploitation. C'était le cas pour les solutions propriétaires, c'est impensable aujourd'hui. Même si un réseau Microsoft dispose d'outils qui lui sont spécifiques, les hôtes de ce réseau peuvent tout de même dialoguer avec ceux d'un réseau Unix.

Pour arriver à cette interopérabilité, il faut que les divers protagonistes se mettent d'accord sur les fonctionnalités à implanter dans leurs applications et leurs fonctions réseau. C'est le rôle des RFC (Request For Comment) et des normes que de définir ces critères.

3-Les couches du modèle osi :

Le modèle OSI comporte **7 couches** :



La couche physique (Couche 1) :

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

une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

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

La couche liaison de données (Couche 2)

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

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

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

La couche réseau (Couche 3)

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

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

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

Couche transport (Couche 4)

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

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

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

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

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

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

La couche session (Couche 5)

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

La couche présentation (Couche 6)

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

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

La couche application (Couche 7)

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

GLOSSAIRE

GLOSSAIRE

ACL : Access Control List. Liste des adresses et ports autorisés ou interdits par un pare-feu.

AH : Authentication Header. Protocole basé sur des méthodes cryptographiques ,qui assure l'authentification et l'intégrité des paquets transitant sur le réseau.

ASA : Adaptative Security Appliance. Matériel crée par l'entreprise Cisco dans le but d'améliorer la sécurité du réseau. Possède de nombreuses possibilités, notamment pare-feu, VPN et inspection applicative des paquets.

ESP : Encapsulating Security Payload. protocole qui assure l'authenticité et la confidentialité des donnéesS.

FAI :Fournisseur d'Accès Internet.

FTP :File Transfert Protocole. Protocole de transfert de fichiers.

HTTP : Hypertexte Transfert Protocole. protocole de transfert de fichier hypertexte.

IP : Internet Protocol . Protocole couche 3 permet le routage des données.

L2F :Layer Two Forwarding. protocole d'encapsulation .

L2TP: Layer Two Tunneling Protocol. Protocole d'encapsulation des données.

LAC : L2TP Access Concentrator.

LCP : Link Contrôle Protocol. Un sous protocole de PPP , permet le contrôle de test et de configuration de la communication.

LDAP ;TACACS : deux serveurs d'authentification et de gestion des accès et permet d'enregistrer les taches effectuées par les utilisateurs.

LNS : L2TP Network Server.

MPPC :Microsoft Point to Point Compression .protocole associé à PPTP pour assurer une compression de données de bout en bout.

MPPE :Microsoft Point to Point Encryption: des fonctions de cryptage de données.

GLOSSAIRE

NAS : Network Access Server. Serveur d'accès réseau.

NCP : Network Control Protocol. Protocole permet l'intégration de PPP au sein des protocoles de couches supérieurs.

PAP : Password Authentication Protocol. Protocole d'authentification de mot de passe des utilisateurs.

PPP : Point To Point Protocol. protocole d'encapsulation de niveau 2 de modèle OSI.il garanti la sécurité des échanges.

PPTP: Point To Point Tunneling Protocol. protocole d'encapsulation de données et de sécurité.

QOS : Quality Of Service . La QoS est un gestionnaire de trafic qui permet d'allouer les ressources réseau aux applications selon leur poids et leur priorité

RADIUS :serveur d'authentification qui permet de contrôler les accès aux réseau local.

SSH : Secure Shell. Protocole de communication sécurisé conçu avec l'objectif de remplacer les différents programmes rlogin, telnet et rsh

SSL : Secure Socket Layer. Protocole de sécurisation des échanges opérant au niveau de la couche transport du modèle OSI.

TCP : Transfert Contrôle Protocol. Protocole qui assure le transfert de fichier en mode connecté.

UDP: User Datagramme Protocol. protocole de transport de données en mode non connecté.

VLAN :Virtual Local Area Network. Un mécanisme qui permet de traduire une adresse IP non routable en une adresse routable pour garantir l'accès web.

VPN : Virtual Private Network. Ensemble de technologies permettant d'établir une communication sécurisée entre deux hôtes distants.

GLOSSAIRE

VPN Lan-to-Lan : technologie permettant à deux sites distants de communiquer entre eux de la même manière que sur un réseau local, en assurant intégrité, confidentialité et authentification des données.

WAN : Wide Area Network . réseaux étendus

Bibliographie

Bibliographie

- William Landri : « Mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passante utilisateur », Master Européen en Informatique, l'année 2009 à partir de site : www.memoireonline.com.
- Jean-françois- Pillou : « tout sur les réseaux informatique et internet", Paris, l'année 2006.
- Xavier Lasserre, Thomas Klein et _SebF : « Réseaux Privés Virtuels – Vpn » à partir du site www.ipframe.com/vpn.
- M. Vincent Nicomette : « la configuration d'asa cisco » Département de Génie Electrique et Informatique, Université de Toulouse, l'année 2008-2009.
- Bernard Cousin : « sécurité des réseaux informatiques »,à partir de site www.netasr.net/Cours/Plateforme/heterogene/IPSec.pdf
- Mekceme Kaissa, Menad lyla : « Conception D'une Interface De Configuration D'un Serveur SSH Sous windows XP », université Mouloud Mammeri Tizi ousou l'année 2010-2011.
- M. Mostefai, : « Réalisation d'un VPN SSL Host to LAN sur un Cisco ASA 5505 » université François-Rabailais; a partir de site : www.widip.fr/pdf/guide_vpn_ipsec_mpls.pdf.
- www.cisco.com/AdaptativeSecurityAppliance.
- www.commentcamarche.com/vpn.ean-françoi.

