République Algérienne Démocratique Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'Ibn Khaldoun – Tiaret

Faculté des Mathématiques et de l'Informatique

Département Informatique

Thème

Configuration d'une connexion VPN pour le réseau de la CNAS Tissemsilt

Pour L'obtention du diplôme de Master
Spécialité : Réseaux et Télécoms

Rédigé par : M^{elle}. ABROUS MOKHTARIA

M^{me}. SOFI FATIMA

Dirigé par : Mr. Bakar KHALED

Année universitaire: 2015-2016

Remerciement

Tout d'abord, nous tenons à remercier Dieu, De nous avoir donné la santé, la volonté et la patience pour mener à terme notre formation de master et pouvoir réalisé ce travail de recherche.

Nous tenons à exprimer nos profonds remerciements à notre encadreur Mr Bakar khaled qui nous a fourni le sujet de ce mémoire et nous a guidés de ses précieux conseils et suggestions, et la confiance qu'il nous a témoignés tout au long de ce travail.

Nous tenons à gratifier aussi les membres de jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail.

J'adresse aussi nos remerciements à Mr si Abde Elhadi chef de département de l'Informatique et à tous les enseignants de la filière de l'Informatique.

Enfin, on adresse nos sincères sentiments de gratitudes et de reconnaissances a toutes les personnes qui ont participé de prés ou de loin à la réalisation de ce travail

Dédicace

Je dédie ce modeste travail

A mes chers parents pour leur soutien, leur patience,

leur encouragement durant mon parcours scolaire.

A mes sœurs et mes frères ainsi à toute ma famille.

A tous mes amis,

A tous ceux qui m'aiment

A tous ceux que j'aime

Abrous mokhtaria

Dédicace

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu

arriver à réaliser ce Modeste travail que je dédie:

A la plus merveilleuse mère, que j'adore à en mourir qui m'a tout donné depuis mon enfance, que DIEU le protège et te garde pour nous.

Au plus adorable et gentil père au monde Allah yerehmo

A ma petite famille : mon mari larbi & ma petite fille alaa sodjoud
A mon très chère frère Mohamed
A mes très chères sœurs: khiera , fatima , fouzia et leurs enfants bien Sur leurs maris
A tout ma famille
A tout mes amis : mokha ,sara, rima , imen , fatima , tisso , houda , zahra…
A mes enseignants et surtout Mr Rouchou Abdelkader
Et à tous ceux qui m'aiment et qui me cannaient de proche ou de loin.

Soufi fatima

Résumé

Dans la gestion quotidienne de la CNAS, la direction ainsi un nombre important de pharmacies ont besoin d'échangés des informations indispensables pour bien servir la population. En plus de la sensibilité de ces informations, la rapidité du procédé nécessitée une liaison réseau sûre et permanente.

L'infrastructure VPN site-à-site est de nos jours très peu répandu pourtant elle apporte une nouvelle approche dans la méthode de transfert des données, elle revêt ainsi un caractère novateur pour les entreprises qui ont opté pour un partage optimal et sécurisé de leur information. C'est cette architecture que nous voulons l'intégrer au système informatique en place à la CNAS Tissemsilt

Liste des figures

Sommaire

Chapitre I : Généralité sur la sécurité des réseaux

Chapitre II : Les Firewalls et les VPN

Chapitre III : Topologie et Configuration

Introduction générale

Introduction Générale

Les réseaux et systèmes information sont devenus des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les entreprises de communication, les banques, les assurances, la médecine ou encore le domaine militaire. Initialement isoles les uns des autres, ces réseaux sont dans le présent interconnectes et le nombre de points d'accès ne cesse de croitre.

Ce développement phénoménal s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces utilisateurs, connus ou non, ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour essayer d'accéder à des informations sensibles dans le but de les lire, les modifier ou les détruire, pour porter atteinte au bon fonctionnement du système ou encore tout simplement par jeu.

Des lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable. Cette sécurisation va garantir la confidentialité, l'intégrité, la disponibilité et la non-répudiation. Et pour cela de nombreux outils et moyens sont disponibles, tels que les solutions matérielles, logiciels d'audits, ou les systèmes de détection d'intrusion(IDS), les antivirus, les réseaux privés(VPN) ou encore les firewalls (pare-feu) qui est un élément matérielle ou logiciel permettant de filtré les paquets de données qui traversent un réseau en bloquant certains et autorisant d'autres, cette mécanisme de sécurité offre plusieurs fonctionnement qui aide à mettre en place une politique de sécurité efficace, on trouve :

- Le filtrage des paquets
- La translation d'adresse IP (NAT)
- Le contrôle d'accès

Dans notre projet de fin d'étude on va voir comment mettre en place un réseau privé vpn au profil de la CNAS Tissemsilt afin de faciliter l'échange sécurisé des informations entre ces différents associes à savoir les pharmacies et les autres CNAS.

Notre mémoire est répartie sur trois chapitres

Le premier chapitre se fut une présentation de la sécurité des réseaux, leurs différents objectifs, les attaques qui peuvent atteindre un réseau d'une entreprise, leurs différents types ainsi que les méthodes de défense.

Le deuxième chapitre introduit les firewalls et leurs types, ainsi que les réseaux privés VPN.

Dans le troisième chapitre nous présentons l'état de l'existant à la CNAS Tissemsilt en termes de réseau exploité à leur niveau, nous proposons la configuration d'une liaison VPN pour améliorer la gestion et la mise à jour des cartes chifa par les pharmacies associées.

Chapitre I

Généralité sur la sécurité des réseaux

Chapitre I : Généralité sur la sécurité des réseaux

Introduction :

Notre société est de plus en plus dépendante de l'informatique. Quelles que soient nos activités, nous sommes confrontés directement ou indirectement à des ordinateurs: procédures administratives, virement d'argent, réservations, télécommunications, ...

De temps en temps, des problèmes de sécurité sont dévoilés, concernant les domaines les plus vastes, allant du vol de numéros de cartes de crédit à la découverte de nouveaux virus de plus en plus destructeurs.

Il est alors nécessaire de mettre au point des méthodes et des techniques pouvant réduire considérablement ces risques, en résolvant une vulnérabilité ou en contrant une attaque spécifique. La sécurité informatique se base sur ces solutions qui permettent de mettre en place une réponse appropriée à chaque menace.

Le choix de la protection adéquate est alors possible, nécessitant de bien connaître son environnement, les objectifs de l'entreprise et les technologies disponibles. Mettre en place une politique de sécurité efficace représente alors un long travail d'étude et de choix devant apporter la plus grande protection possible au système d'information.

Dans ce premier chapitre, on parlera sur la sécurité du réseau et ses objectifs, et on présentera quelques attaques et leurs types, ensuite, nous allons citer les mécanismes de défense.

I.1 La sécurité d'un réseau

I.1.1 Définition :

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs possèdent uniquement les droits qui leur ont été octroyés.

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante ;
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système ;
- De sécuriser les données en prévoyant les pannes ;
- De garantir la non-interruption d'un service ; **[1]**

I.1.2 Objectifs de la sécurité informatique :

L'expression d'objectif de sécurité est réalisée pour l'ensemble des flux d'informations sensibles transitant sur le réseau, suivant les critères de:

I.1.2.1 Disponibilité :

La disponibilité est le fait de garantir que la donnée est accessible (lisible, consultable). Une information disponible a une valeur et représente une plus-value et une force pour l'entreprise. Une information qui n'est pas ou plus consultable au moment où nous en avons besoin ne représente rien et revient au même point que la non possession de l'information. **[2]**

I.1.2.2 Confidentialité :

La confidentialité est la propriété d'une information de ne pas être révélée à des utilisateurs non autorisés à la connaître. Ceci signifie que le système informatique doit :

- Empêcher les utilisateurs de lire une information confidentielle (sauf s'ils y sont autorisés),
- Empêcher les utilisateurs autorisés à lire une information et de la divulguer à d'autres utilisateurs (sauf autorisation).

Le terme information doit être pris au sens le plus large : il recouvre non seulement les données elles-mêmes, mais aussi les flux d'information et la connaissance de l'existence des données ou des communications. Assurer la confidentialité d'un système est donc une tâche complexe. Il faut analyser tous les chemins qu'une information particulière peut prendre dans le système pour s'assurer qu'ils sont sécurisés. Il importe également de prendre en compte les connaissances qu'un ou plusieurs utilisateurs peuvent déduire à partir des informations qu'ils acquièrent. Il faut donc contrôler non seulement les informations présentes dans le système, mais aussi les liens logiques qui peuvent les relier entre elles ou à des informations publiques. **[3]**

I.1.2.3 Intégrité :

L'intégrité est la propriété d'une information de ne pas être altérée. Cela signifie que le système informatique doit :

- Empêcher une modification indue de l'information, c'est-à-dire une modification par des utilisateurs non autorisés ou une modification incorrecte par des utilisateurs autorisés,
- Faire en sorte qu'aucun utilisateur ne puisse empêcher la modification légitime de l'information. Par exemple, empêcher la mise à jour périodique d'un compteur de temps constituerait une atteinte à l'intégrité.

De plus, il faut avoir l'assurance que toute modification de donnée est approuvée et que chaque programme se comporte de manière correcte (c'est-à-dire conformément aux fonctions qu'il est censé remplir, y compris dans ses interactions avec les autres processus). Il faut également s'assurer qu'aucune information ne peut être modifiée par des intermédiaires, que cette altération soit intentionnelle (par exemple, un utilisateur intervient pour modifier une communication entre deux autres utilisateurs) ou accidentelle (une donnée modifiée lorsqu'elle est communiquée via un support de communication non-fiable).

Afin de se prémunir contre les fautes affectant l'intégrité des données, il importe d'intégrer dans le système des mécanismes permettant d'une part de détecter les modifications des informations, et d'autre part de contrôler les accès à ces dernières (en gérant les droits d'accès des programmes et utilisateurs). De plus, un travail de validation en amont peut également être réalisé pour prévenir les fautes accidentelles. **[3]**

Ces trois termes regroupent donc les fondements de la sécurité de l'information. Mais avec la prédominance des systèmes informatisés, d'autres termes viennent compléter ces fondations, cela vient du fait que les systèmes informatiques permettent aujourd'hui de combler des exigences supplémentaires et que ce sont les outils les plus performants pour gérer l'information :

I.1.2.4 Authentification :

Confirmation de l'identité supposée d'entités ou d'utilisateurs. Des méthodes d'authentification appropriées sont nécessaires pour de nombreux services et applications, comme la conclusion d'un contrat en ligne, le contrôle de l'accès à certains services et données (pour les télétravailleurs, par exemple) et l'authentification des sites Web (pour les banques Internet, par exemple). L'authentification doit également inclure la possibilité de rester anonyme, dans la mesure où de nombreux services ne nécessitent pas l'identité de l'utilisateur, mais seulement la confirmation de certains critères (pièces justificatives anonymes), telle la capacité de payement. **[2]**

I.1.2.5 Non répudiation :

La non répudiation permet d'assurer deux ou plusieurs membres d'un échange ou d'une communication que l'un comme l'autre ont bien envoyé et reçu l'information dans son intégralité. Cela permet le plus souvent d'éviter d'avoir des situations où dans lesquelles nous ne savons pas réellement si l'information a bien été transmise dans son intégralité. **[4]**

I.1.2.6 Contrôle d'accès :

Dans le contexte de la sécurité des réseaux, le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée, ou s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas. **[5]**

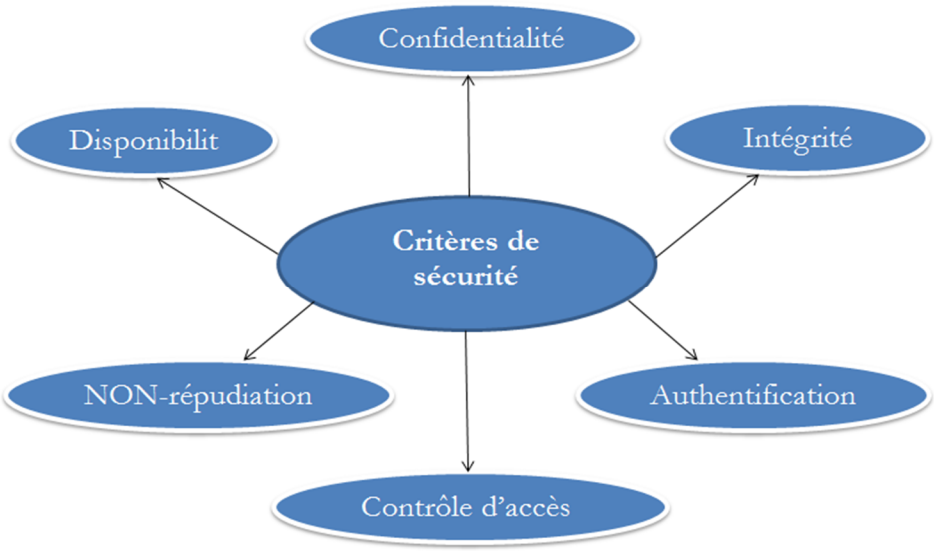


Figure 1 : Les objectifs de la sécurité informatique.

I.2 Les attaques réseau :

I.2.1 Définition d'une attaque :

Tout ordinateur connecté à un réseau informatique potentiellement vulnérable à une attaque, ce dernier est l'exploitation d'une faille d'un système informatique (système exploitation, logiciel ou bien même de l'utilisateur) a pour conséquence d'utiliser le système d'une façon qui n'a pas été prévue par ses concepteurs :

- Pour accumuler des informations qui ne sont pas censées être publiques
- Pour effectuer des actions auxquelles 'on n'est normalement pas autorisé
- Pour empêcher le dit système de fonctionner

I.2.2 Niveaux des attaques :

Une entreprise peut être victime d'une attaque à trois niveaux. **[6]**

- **L'attaque externe :** l'attaque est réalisée depuis l'extérieur et utilise les points d'ouverture (serveur mail, serveurs web, …). Très médiatisée, elle délicate et ne produit que très rarement un résultat.

- **L'attaque interne :** Elle se produit depuis l'intérieur du réseau, elle est généralement le fait d'un collaborateur. « Pour hacker, fais-toi engager ».Elle représente 87% des attaques efficaces.
- **L'attaque physique :** partir avec les machines reste toujours la méthode la plus efficace.

I.2.3 Classification des attaques :

I.2.3.1 Attaques passives *:*

Elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues, comme les attaques sur la confidentialité qui a pour objectifs d'obtenir d'informations sur un système, sur un utilisateur ou un projet. Les méthodes possibles de ce type d'attaques est : usurpation d'identité, écoute. **[7]**

I.2.3.2 Attaque active :

Elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critiques que les passives comme les attaques : **[7]**

- *Attaque sur l'intégrité :* qui a pour objectif de modifier ou détruire des données ou des configurations. Ses méthodes possibles : injection de code, action physique, et intrusion.
- *Attaque sur l'authentification :* qui a pour objectifs d'utiliser des ressources de façon clandestine sur un système. Ses méthodes possibles : intrusion…
- *Attaque sur la disponibilité :* qui a pour objectifs de perturber l'échange par réseau, le service ou l'accès à un service. Ses méthodes possibles : action physique, et intrusion

I.2.4 Auteurs des attaques :

I.2.4.1 Un Hacker :

Est un spécialiste de très haut niveau. Généralement programmeur,

- Il porte un énorme intérêt à maitriser tous les mécanismes de fonctionnement interne d'un système.
- Il peut découvrir des failles dans un système et leur origine.
- Il cherche à améliorer ses connaissances
- Partage généralement ses découvertes et ne cherche pas nuire

Les hackers sont fréquemment amenés à concevoir des outils d'analyse des systèmes et produit des attaques pour mettre au point la sécurité. **[6]**

I.2.4.2 Hacking :

C'est l'ensemble des techniques visant à attaquer un réseau, un site ou un équipement. Les attaques sont diverses, on y trouve :

- L'envoie de bombe logicielle, chevaux de Troie ;
- La recherche de trou de sécurité ;
- Détournement d'identité ;
- Les changements des droits d'accès d'un utilisateur d'un PC ;
- Provocation des erreurs ; **[6]**

I.2.5 Type d'attaque d'un réseau :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Cette dernière est l'exploitation d'une faille d'un système informatique à des fins non connues. Il existe plusieurs telle que :

I.2.5.1 Reconnaissance :

La reconnaissance est la découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou encore la découverte de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque. La reconnaissance est similaire**...** au repérage effectué par un cambrioleur à la recherche d'habitations vulnérables, comme des maisons inoccupées, des portes faciles à ouvrir ou des fenêtres ouvertes. **[8]**

I.2.5.2 Accès :

L'accès au système est la possibilité pour un intrus d'accéder à un périphérique pour lequel il ne dispose pas d'un compte ou d'un mot de passe. La pénétration dans un système implique généralement l'utilisation d'un moyen de piratage, d'un script ou d'un outil exploitant une vulnérabilité connue de ce système ou de l'application attaquée. **[8]**

I.2.5.3 Déni de service :

Le déni de service (DoS, en anglais) apparaît lorsqu'un pirate désactive ou altère un réseau, des systèmes ou des services dans le but de refuser le service prévu aux utilisateurs normaux. Les attaques par déni de service mettent le système en panne ou le ralentissent au point de le rendre inutilisable. Le déni de service peut consister simplement à supprimer ou altérer des informations. Dans la plupart des cas, l'attaque se résume à exécuter un

programme pirate ou un script. C'est pour cette raison que les attaques par déni de service sont les plus redoutées. **[8]**

I.2.5.4 Vers, virus et chevaux de Troie :

Des logiciels malveillants peuvent être installés sur un ordinateur hôte dans le but d'endommager ou d'altérer un système, de se reproduire ou d'empêcher l'accès à des réseaux, systèmes ou services. Ces programmes sont généralement appelés vers, virus et chevaux de Troie.

- **Un ver** est un petit programme qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et ne peut donc l'infecter, il va simplement se copier d'ordinateur en ordinateur par l'intermédiaire d'un réseau comme Internet ou même par les lecteurs de disquettes, graveur, lecteur zip...

Le ver peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances des réseaux. Comme un virus, le ver peut contenir une action nuisible qui peut être très grave comme le formatage de votre disque dur ou l'envoi de données confidentielles.**[9]**

- **Un virus** est un logiciel de petite taille, transmis d'ordinateur à ordinateur, qui perturbe le fonctionnement d'une machine. Un virus informatique peut endommager ou supprimer des données de l'ordinateur, utiliser un programme de messagerie électronique pour se transmettre à d'autres ordinateurs, voire effacer tout élément enregistré sur le disque dur.

Les virus informatiques se propagent fréquemment via les pièces jointes d'un message électronique ou via des messages instantanés. Voilà pourquoi vous ne devez en aucun cas ouvrir une pièce jointe sans connaître l'expéditeur du message électronique, ou si vous en attendiez la réception. Les virus peuvent apparaître en pièces jointes sous la forme d'images humoristiques, de cartes de vœux, de fichiers audio ou vidéo. Ils se propagent également par l'intermédiaire de téléchargements sur Internet. Ils peuvent être dissimulés dans un logiciel piraté ou dans d'autres fichiers ou programmes disponibles en téléchargement. **[10]**

- **Les chevaux de Troie** est un logiciel malveillant qui permet à un pirate informatique de perturber le fonctionnement d'un ordinateur ou d'en prendre le contrôle. Pour faire entrer ce programme espion, le pirate envoie le plus souvent un mail à la personne dont il cherche à infiltrer l'ordinateur et met son «cheval» en pièce jointe. L'ouverture de ce fichier (extension .rar, .zip, .exe, etc) lance en toute discrétion l'installation du mouchard sur la machine. Celui-ci va généralement se cacher dans la partie immergée les fichiers système de l'iceberg que

constitue le système d'exploitation (Windows, Linux). Pour une plus grande discrétion, le fichier d'installation du cheval de Troie («Trojan horse» en anglais) est parfois dissimulé dans un fichier ou un programme qui fonctionne tout à fait normalement - un jeu par exemple. **[11]**

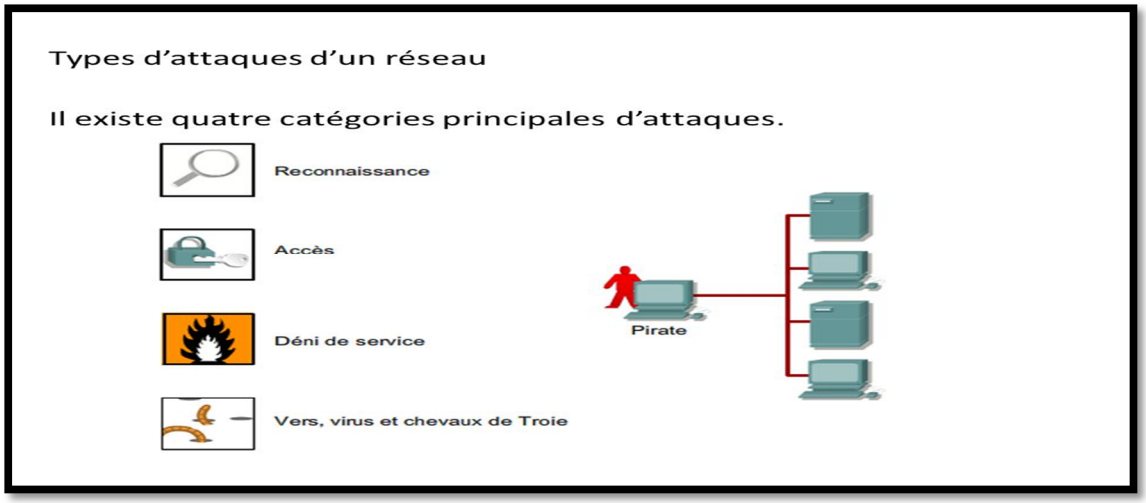


Figure 2 : type d'attaques d'un réseau.

I.2.5.5 Attaques de mot de passe :

Les attaques de mot de passe peuvent se faire à l'aide d'un analyseur de paquets pour glaner les comptes et les mots de passe utilisateur transmis en clair. Les attaques de mot de passe se rapportent en général aux tentatives de connexion répétées à une ressource partagée, comme un serveur ou un routeur, afin d'identifier un compte utilisateur, un mot de passe ou les deux. Ces tentatives répétées s'appellent attaques par dictionnaire ou attaques en force.

I.2.5.6 Attaque de l'homme du milieu :

Le pirate se place entre deux ordinateurs et se fait passer pour un afin d'obtenir le mot de passe de l'autre. Il peut alors se retourner contre le premier avec un mot de passe valide pour l'attaque.

I.3 Méthodes de défense :

Le but de la sécurité informatique est de préserver la confidentialité, l'intégrité et la disponibilité des données du réseau. Certaines méthodes de défense permettent de prévenir les attaques.

I.3.1 La cryptographie :

Est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à

travers des réseaux non sûrs (comme Internet) de telle qu'elles ne puissent être lues par personne à l'exception du destinataire convenu.

La cryptologie se compose de la cryptographie, l'art d'écrire des secrets pour les rendre inintelligibles à des tiers, et de la cryptanalyse, l'art de retrouver les secrets cachés dans des informations inintelligibles. Il ne sera ici question que des éléments de cryptographie, qui sont à la base de nombreux mécanismes de sécurité : le chiffrement, le hachage et la signature.

I.3.1.1 Le chiffrement :

Le chiffrement est un procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clef d'encodage (action de codé).

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe actuellement deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui, repose sur un codage à deux clés, une privée et l'autre publique.

- **Le cryptage symétrique :**

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) et RSA.

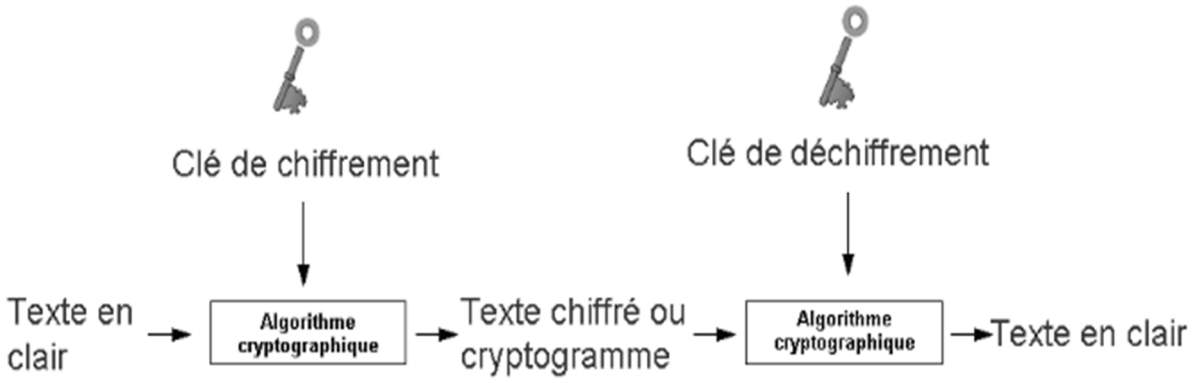


Figure 3 : chiffrement symétrique.

Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite les systèmes des clés privées surtout sur Internet.

Pour résoudre ces problèmes de transmission de clés, les mathématiciens ont inventé le cryptage asymétrique qui utilise une clé privée et une clé public.

- **Le cryptage asymétrique :**

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.

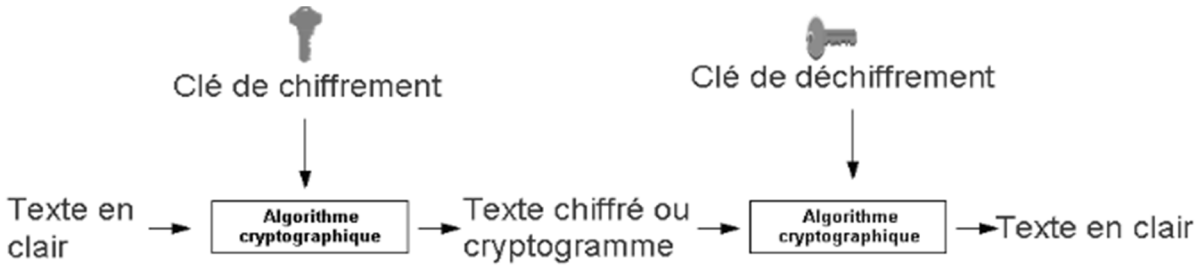


Figure 4 : Chiffrement asymétrique.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage. Les algorithmes à clés publiques RSA (des noms de ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adelman) et Diffie-Hellman.

Ce cryptage présente l'avantage de permettre le placement de signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Le cryptage à clé publique présente les avantages suivants :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs ;
- Authentification plus flexible (maniable) ;
- Supporte les signatures numériques ;

Ces mêmes algorithmes (à clé publique) sont souvent des milliers de fois plus lents que les algorithmes à clé privée d'une sécurité équivalente. C'est pour cette raison que les

deux types d'algorithmes sont utilisés de manière conjointe. Par exemple, le logiciel de chiffrement Pretty Good Privacy (PGP) fonctionne de cette façon. Pour envoyer un message chiffré à un destinataire, le programme PGP de l'expéditeur génère une « clé de session » aléatoire. Cette clé de session est utilisée avec un algorithme à clé privée pour chiffrer le message à envoyer (c'est rapide). La clé de session elle-même est chiffrée avec un algorithme à clé publique (c'est long mais la clé de session est petite en comparaison du message), en utilisant la clé publique du destinataire, et est envoyée avec le message chiffré. Le destinataire utilise d'abord l'algorithme à clé publique et sa clé secrète pour déchiffrer la clé de session (c'est long mais la clé de session est petite), puis utilise la clé de session et un algorithme à clé privée pour déchiffrer la totalité du message (c'est rapide).

I.3.1.2 Fonctions de hachage à sens unique :

Une fonction de hachage à sens unique est toute fonction mathématique, qui convertit une chaîne de caractères en une autre de taille fixe (souvent de taille inférieure). Le but de l'opération est de déterminer une empreinte digitale de la chaîne de caractères d'entrée. Cette empreinte permettrait de déterminer si une autre chaîne a des chances d'être identique à celle pour laquelle l'empreinte a été calculée.

Une fonction de hachage à sens unique est une fonction à sens unique ; il est aisé de calculer l'empreinte à partir de la chaîne d'entrée, mais il est difficile d'engendrer des chaînes qui ont certaines empreintes.

Il y a deux types principaux de fonctions de hachages à sens unique : celles avec clef et celles sans clef. Dans le deuxième type, l'empreinte n'est que fonction de la chaîne d'entrée, dans le premier elle est fonction de la chaîne d'entrée et de la clef ; seul celui qui possède la clé peut calculer l'empreinte.

Les fonctions de hachage à sens unique peuvent être un moyen d'associer une empreinte à un fichier.

I.3.1.3 Signature numérique :

La signature numérique (parfois appelée **signature électronique**) est à un document numérique, ce que la signature manuscrite est à un document papier. Tout comme une signature papier, une signature électronique a pour seul objectif de démontrer à un tiers que le document a été approuvé par une personne identifiée. Il s'agit d'un mécanisme d'engagement fiable faisant appel à des techniques cryptographiques.

La signature électronique permet, pour un document numérique, de garantir :

- L'identité du signataire ;
- La non-répudiation par le signataire du document signé ;
- L'intégrité́ du document signé, c'est-à-dire son absence de modification ;

I.3.2 Les mots de passe :

Ce sont des clés qui gèrent les accès, qui vous les autorisent alors qu'elles les refusent à d'autres, qui permettent de contrôler les accès aux informations (documents protégés par des mots de passe) ou les autres accès (des pages web protégées par mots de passe), ou encore qui gèrent les authentifications. **[7]**

I.3.2.1 Les différents types de mots de passe :

Il y 03 types principaux de mots de passe :

Chaînes de caractères : Les mots de passe les plus simples sont constitués de chaînes de caractères alphanumériques et de symboles qui sont fournis à partir d'un clavier. Ils vont du simple code à 3 chiffres utilisé pour ouvrir les portes de certains garages aux combinaisons complexe de caractères alphanumériques et de symboles recommandés pour protéger des applications hautement sensible.

Chaînes de caractères avec un jeton : En passent à la vitesse supérieure, nous avons des mots de passe composés de notre chaîne de caractères précédente à laquelle on rajoute un jeton. Un bon exemple est l'ATM, qui nécessite à la fois une carte (notre jeton).

Mots de passe biométriques : Plus complexe encore, nous avons les mots de passe biométriques. Ils utilisent des empreintes biologiques de certaines parties de notre corps, comme nos empreintes digitales afin de nous authentifier. Un autre exemple est l'empreinte rétinienne où c'est la rétine (c'est la partie qui est à l'arrière de l'œil, coté interne) qui photographiée. Cette rétine est constituée d'un réseau unique de vaisseaux sanguins et c'est ce réseau qui va être utilisé. Cette catégorie de mots de passe est considérée comme la plus sure, mais en réalité un mot de passe que vous portez sur vous n'est pas plus sécurisé qu'un mot de passe complexe que vous avez en tête, en assumant que le logiciel utilisé pour vérifier ce mot de passe est sécurisé

I.3.2.2 Construction d'un mot de passe solide :

Les meilleurs mots de passe :

- Ne figurent pas dans les dictionnaires ;
- Contiennent des nombres, des lettres et des symboles ;

- Contiennent des majuscules et minuscules ;
- Plus ils sont longs, plus ils sont sécurisés(en général) ;

I.3.3 Les anti-virus :

Est un logiciel ayant pour objectif principal de protéger une machine contre différents types d'infections informatiques telles que des virus. Cependant, des différences peuvent exister entre ces types de logiciels. Elles se situent principalement dans le nombre de fonctionnalités, leur mise en place ainsi que les méthodes utilisées pour la détection d'anomalies.

Figure 5 : Machine protégé par un anti-virus.

I.3.3.1 Principes de ces fonctionnements :

Afin de protéger une machine, les logiciels antivirus utilisent plusieurs techniques à savoir :

- Analyse en temps réel du contenu des opérations sur la machine tel que des ouvertures/fermetures de fichiers, des lancements de logiciels et tout type de téléchargements effectués sur la machine depuis Internet ou un autre réseau.
- Balayage des disques et autres périphériques de stockage et de la configuration système de la machine à des intervalles définis préalablement.
- Analyse du contenu ainsi que des volumes de courriers électroniques entrants et sortants afin de protéger contre des virus qui possèdent un processus opérationnel de propagation par messagerie.

En cas de détection d'anomalie ou de tentative d'infection informatique, dans la majorité des cas et selon la configuration choisie par l'utilisateur, l'antivirus affichera une alerte à l'utilisateur permettant de :

- Bloquer la tentative d'infection informatique ;

- Réparer le contenu infecté ou malicieux en effaçant toute trace du virus ;
- Supprimer définitivement le contenu infecté ;
- Mise sous quarantaine du contenu infecté ou malicieux ;

I.3.3.2 Composants d'un antivirus :

- **Scanner :** Il examine (scan) l'ordinateur à la demande : un fichier, un dossier ou tous les fichiers de votre disque. Un scan complet consomme beaucoup de ressources matérielles et de temps, mais il est conseillé de le faire de temps en temps.

- **Moniteur :** Il analyse en temps réel les fichiers auxquels vous accédez au cours de votre utilisation normale et stoppe immédiatement une exécution virale. Il est composé de plusieurs modules dont le nom change suivant les logiciels. Par exemple McAfee VirusScan en a quatre, chacun dédié à une tache : email, web, téléchargement, système. En fonction de sa configuration et de la puissance de votre ordinateur, il ralentit plus ou moins vos applications.

- **Base de signatures de virus :** Une signature est un bout de code permettant d'identifier un virus, un peu comme une empreinte digitale humaine. La base de signatures référence des dizaines de Milliers de virus, troyens et variantes. Elle doit être mise à jour fréquemment pour reconnaître les nouveaux spécimens.

I.3.4 Réseau privé virtuel « VPN » :

Le VPN (Virtual Private Network ou en français Réseau privé virtuel) est un moyen de communication assurant la sécurité des transferts de données sur des réseaux publics ou partagés. C'est le concept d'un tunnel (route) sécurisé entre deux points, les données qui entre d'un bout ressortant d'un autre

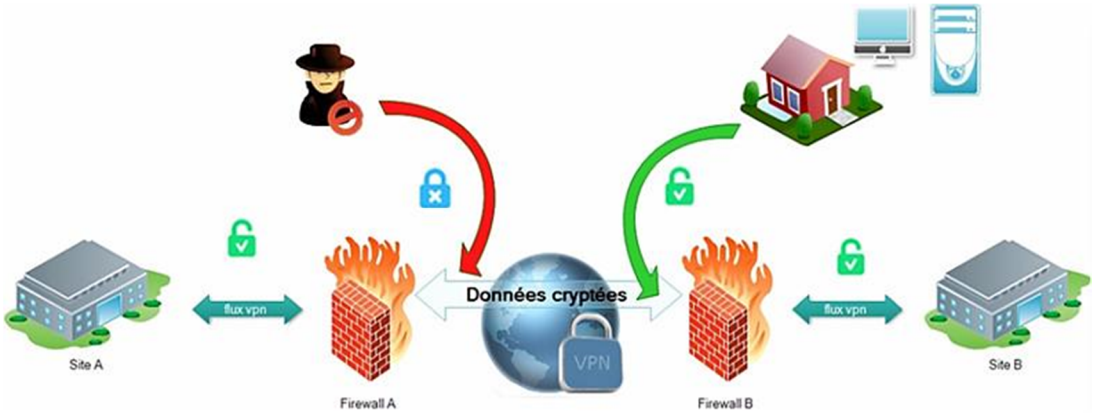


Figure 6 : VPN entre deux firewalls.

I.3.4.1 Principe de fonctionnement :

Un VPN utilise la cryptographie pour assurer la confidentialité, l'intégrité et l'authentification des données, même si celles-ci sont envoyées sur l'Internet.

- **Confidentialité des données :** Le chiffrement assure que le contenu des données transmises n'est connu que des parties qui échangent l'information. De ce fait, un tiers interceptant le trafic du VPN n'aura pas la possibilité d'en déterminer la teneur.

- **Intégrité des données :** Le chiffrement et le hachage assurent, que les données reçues au travers du VPN par le destinataire sont identiques à celles envoyées par l'expéditeur : il n'y aura ainsi aucune possibilité, pour une tierce partie, de changer les données en transit dans le VPN.

- **Authentification des utilisateurs du VPN :** Pour certains VPN, (dans le cas du télétravail par exemple), il est important de savoir quels sont ceux qui participent au processus afin d'éviter les problèmes de sécurité liés à l'usurpation d'identité et par la même à l'accès illicite aux réseaux privés.

I.3.5 NAT « Network Address Translation » :

Le Traduction d'adresses de réseau (NAT) est conçu pour l'économie d'adresse IP. Elle active les réseaux IP privés qui utilisent des adresses IP non enregistrées pour se connecter à Internet. NAT fonctionne sur un routeur, qui en général connecte deux réseaux ensemble, et traduit les adresses privées (pas globales uniques) au sein du réseau interne en adresses légales, avant que des paquets soient transférés à l'autre réseau.

I.3.6 Firewall :

Un firewall (appelé aussi coupe-feu, garde-barrière ou pare-feu), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le firewall est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe ; **[12]**

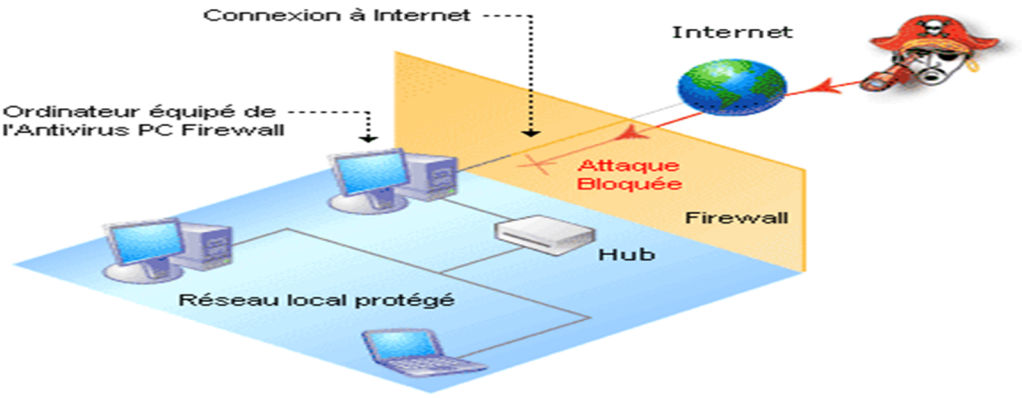


Figure 7 : Attaque bloquée par firewall.

❖ **Type de firewalls :**

– Les firewalls bridge ;

– Les firewalls logiciels ;

– Les firewalls matériels :

❖ **Fonctions principale d'un firewall :**

Un firewall implémente trois fonctions basiques :

– Le filtrage ;

– Translation d'adresse ;

– Contrôle d'accès ;

I.3.7 DMZ « zone démilitarisée » :

Est un sous-réseau isolé par firewall. Ce sous-réseau se trouvant entre le réseau local et le réseau extérieur.

– **Propriétés :**

▪ Les connexions à la **DMZ** sont autorisées de n' importe où ;

▪ Les connexions à partir de la **DMZ** ne sont autorisées que vers l'extérieur ;

– **Intérêt :**

Rendre des machines accessible à partir de l'extérieur (possibilité de mettre en place des serveurs (DNS, STMP,…)).

I.3.8 Les systèmes de détection d'intrusion (IDS) :

Un système de détection d'intrusions (IDS, de l'anglais Intrusion Detection System) est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un IDS détecte

des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout IDS est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources.

Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus. **[13]**

Il existe deux niveaux d'IDS : les IDS systèmes et les IDS réseaux.

- **Network based IDS (NIDS) :** L'IDS réseau ou Network based IDS (NIDS) surveille comme son nom l'indique le trafic réseau. Il se place sur un segment réseau et "écoute" le trafic. Ce trafic sera ensuite analysé afin de détecter les signatures d'attaques ou les différences avec le fonctionnement de référence. On notera une contrainte à ce système, en effet le cryptage du trafic sur les réseaux commutés rend de plus en plus difficile l‘ "écoute" et donc l'analyse du segment réseau à analyser, car le contenu des paquets est crypté. De plus, un trafic en constante augmentation sur les réseaux contraint les NIDS à être de plus en plus performants pour analyser le trafic en temps réel. Enfin, avec sa ou ses cartes d’interface réseau en mode promiscuous (permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.), qui n’ont donc pas d’adresses IP, ni de pile de protocole attaché, il peut écouter tout le trafic qui arrive à l’interface en restant invisible.

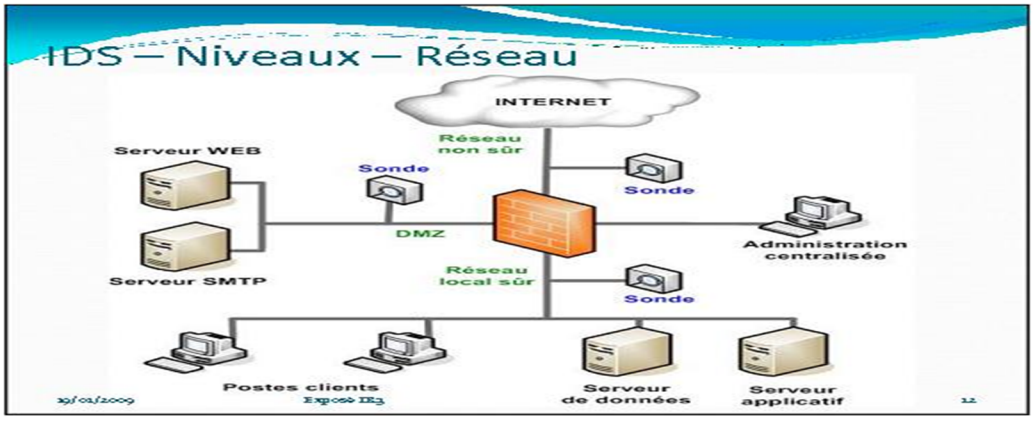


Figure 8 : IDS Niveaux Réseau.

- **Host Based IDS (HIDS) :** L'IDS Systèmes ou Host Based IDS (HIDS) surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels systèmes et enfin vérifie l'intégrité des systèmes de fichiers. Les HIDS sont de par leur principe de fonctionnement dépendant du système sur lequel ils sont installés. Ce système peut s'appuyer ou non sur le système propre au système d'exploitation pour en vérifier l'intégrité et générer des alertes. Il

peut aussi capturer les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, chevaux de Troie…).

L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées.

Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux.

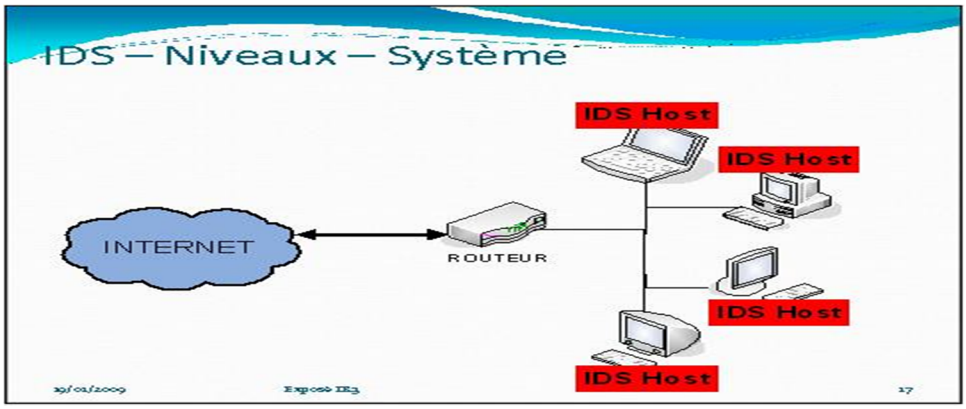


Figure 9 : IDS Niveau Système

I.3.8.1 Principe de fonctionnement :

Un IDS est placé en général derrière le firewall, il fournit des informations sur les données circulant à l'intérieur du réseau après avoir été filtrées. Une alerte sera déclenchée si ces données présentent un danger, notamment une tentative d'intrusion. De manière générale, un système de détection des intrusions assure les taches suivantes :

- Détection des techniques de scan des ports, prise d'empreintes des OS, etc.
- Détection de paquets non-conformes aux RFCs (paquets de taille anormale, etc.)
- Détection des manipulations suspectes internes à un réseau (par exemple, les actions jugées dangereuses d'un salarié connecté au réseau interne d'une entreprise)
- Détection de la présence de virus dans le réseau interne.
- Analyse des fichiers de journaux (les fichiers logs) générés par les firewalls, les routeurs, etc.
- Corrélation de multiples sources d'évènements de sécurité. **[7]**

Conclusion :

Le système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources.

La malveillance informatique est souvent à l'origine de ces menaces, qu'il s'agisse de vol d'information ou de sabotage, n'importe qui pouvant s'improviser pirate informatique avec des outils adaptés.

Beaucoup de compétences sont nécessaires pour assurer une sécurité optimale, mais il est impossible de garantir la sécurité de l'information à 100%. Malgré tout, il existe des moyens efficaces pour faire face à ces agressions.

Dans le prochain chapitre, on va détailler l'une des solutions de protection de réseaux la plus efficace et qui est très fortement conseillée de déployer même sur le PC personnel: le firewall et vpn.

Chapitre II

Les Firewalls et les VPN

Chapitre II : Les Firewalls et les VPN

Introduction

De nos jours, toutes les entreprises possédant un réseau local qui ont aussi un accès à internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indisponible, et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise.

Et pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un VPN et firewall et de mieux un firewall matériel qui propose un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Dans ce chapitre on va présenter le firewall et VPN, avec leurs principales caractéristiques.

II.1 Les firewalls :

II.1.1 Définition

Le Firewall est un système physique (matériel) ou logique (logiciel) qui permet à une organisation de mettre en place un périmètre de sécurité entre Internet et son réseau informatique interne, afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3,4 et 7 du modèle OSI.

Il détermine :

- Les services internes pouvant accéder à l'extérieur (Internet).
- Les services externes pouvant accéder au réseau Interne.

Figure 10 : Réseau protégé par le firewall.

Le firewall doit donc contrôler tout le trafic Internet qu'il soit entrant ou sortant. Une fois le trafic autorisé à entrer, il n'est plus possible de revenir en arrière. Toute action est donc irréversible.

Le firewall contient un ensemble des règles prédéfinies permettant :

- D'autoriser la connexion
- De bloquer la connexion
- De rejeter la demande de connexion sans avertir l'émetteur. **[7]**

II.1.2 Utilisation d'un firewall

Les firewalls sont utilisés principalement dans 4 buts :

- Se protéger des malveillances "externes"
- Eviter la fuite d'information non contrôlée vers l'extérieur
- Surveiller les flux internes/externes
- Faciliter l'administration du réseau

II.1.3 Emplacement d'un firewall

L'emplacement d'un firewall est l'une des tâches importantes d'un administrateur réseau. Ce choix d´dépend de la fonction du firewall. Ce dernier peut être placé à la frontière de sorte qu'il protège le réseau local de toutes les connexions venant d'Internet. La situation correspondante est présentée par la Figure 11.

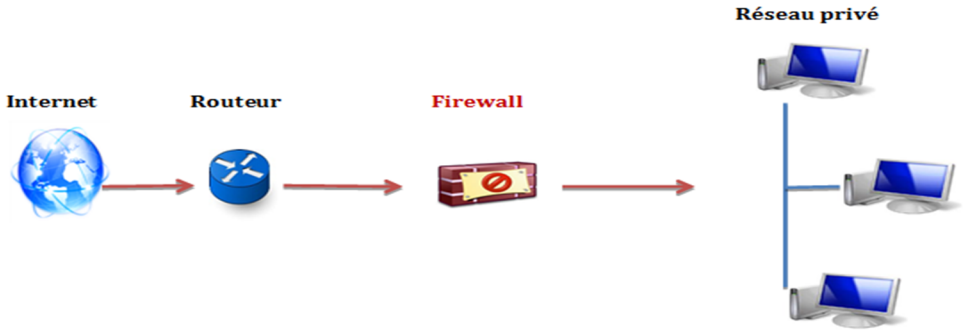


Figure 11 : Emplacement d'un firewall à la frontière.

Un firewall peut aussi être placé à l'intérieur d'un réseau pour le diviser en plusieurs sous-réseaux et contrôler les différents accès entre eux. La disposition correspondante est représentée par la Figure 11.1.

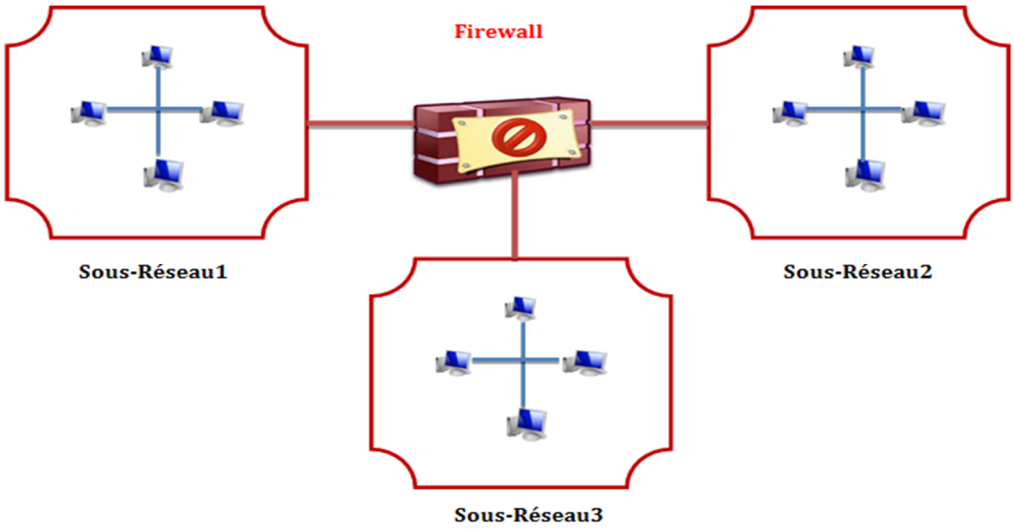


Figure 11.1 : Emplacement d'un firewall au centre d'un réseau.

II.1.4 Fonctions principale d'un firewall :

Un firewall implémente trois fonctions basiques :

- Le filtrage
- Translation d'adresse
- Contrôle d'accès **[7]**

II.1.4.1 Filtrage :

Les types de filtrage les plus courants sont :

II.1.4.1.1 Le filtrage simple de paquets

Analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure. Ainsi, les paquets de donnée transitent par le firewall et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice
- Adresse IP de la machine réceptrice
- Type de paquet (TCP, UDP, etc…)
- Numéro de port

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

II.1.4.1.2 Le filtrage dynamique (stateful inspection, filtrage de paquets avec état)

Le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Il est ainsi capable d'assurer un suivi des échanges, c'est-à-dire : de tenir compte d'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du firewall ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le firewall.

II.1.4.1.3 Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application. Et des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc…).

II.1.4.1.4 Translation d'adresse :

Le firewall est souvent l'endroit où l'on implémente un **NAT** (**N**etwork **A**ddress **T**ranslation, ou en français, Translation d'adresse réseau). Ceci permet d'éviter l'obligation de fournir une adresse IP officielle à chaque machine du réseau internet. A partir de ce point on en vient au concept de sécurité périphérique. La traduction d'adresse qui consiste à réécrire les champs adresse IP source et/ou destination pour permettre le routage d'adresses privées, répondre à la pénurie d'adresse IPv4, tenter de dissimuler le plan d'adressage interne. Et cette technique et définis par la solution **NAT**.

II.1.4.1.5 Différents types de NAT :

A. NAT statique :

Où un ensemble d'adresses internes est traduit dans un ensemble de même taille d'adresses externes. Ces NAT sont dites statiques car l'association entre une adresse interne et son homologue externe est statique (première adresse interne avec première externe…).

La table d'association est assez simple, de type un pour un et ne contient que des adresses. Ces NAT servent à donner accès à des serveurs en interne à partir de l'extérieur.

Il existe trois types de NAT Statiques :

- NAT Statique Unidirectionnelle qui traduit uniquement les connexions de l'extérieur vers l'intérieur (attention, les paquets de retour sont aussi traduits). Le plus souvent lorsque la machine interne initie une connexion vers l'extérieur la connexion est traduite par une autre NAT dynamique.

- NAT Statique Bidirectionnelle qui traduit les connexions dans les deux sens.

- NAT Statique PAT (Port Address Translation du port serveur). Conjonction d'une NAT Statique Uni Bidirectionnelle et d'une transformation du port serveur. (Remarque : le nom PAT vient du fait que le port serveur/destination est modifié. A ne pas confondre avec la NAT Dynamique PAT).

B. NAT dynamique :

Où un ensemble d'adresses internes est traduit dans un plus petit ensemble d'adresses externes. Ces NAT sont dits Dynamiques car l'association entre une adresse interne et sa contrepartie externe est créée dynamiquement au moment de l'initiation de la connexion. Ce sont les numéros de ports qui vont permettre de d'identifier la traduction en place : le numéro du port source (celui de la machine interne) va être modifie par le routeur. Il va servir pour identifier la machine interne.

Il existe plusieurs types de NAT Dynamiques :

- NAT Dynamique PAT (Port Address Translation du port client/source) ou les adresses externes sont indifférentes (le plus souvent la plage d'adresse que votre fournisseur d'accès vous a attribuée). (Remarque: le nom PAT vient du fait que le port source est modifié. À ne pas confondre avec la NAT Statique PAT).

- Masquerading où l'adresse IP du routeur est seule utilisée comme adresse externe. Le Masquerading est donc un sous cas de la Dynamique PAT.

- NAT Pool de Source est la plus vieille des NAT. La première connexion venant de l'intérieur prend la première adresse externe, la suivante la seconde, jusqu'à ce qu'il n'y ait plus d'adresse externe. Dans ce cas exceptionnel le port source n'est pas modifié. Ce type de NAT n'est plus utilisé.

- NAT Pool de Destination permet de faire de la répartition de charge entre plusieurs serveurs. Peu d'adresses externes sont donc associées avec les adresses internes des serveurs. Le firewall se débrouille pour répartir les connexions entre les différents serveurs. **[WIKI]**

II.1.4.2 Contrôle d'accès :

Le firewall défini un contrôle d'accès par une liste qui contiens des adresse IP ou des numéros de ports autorisés ou interdits par le dispositif de filtrage.

Les ACL (Access Control Liste, ou en français, liste de contrôle d'accès) sont divisés en deux grandes catégories :

- **ACL standard** : Ne peut contrôler que deux ensembles, l'adresse IP source et une partie de l'adresse IP source, au moyen de masque générique.

- **ACL étendue** : Peut contrôler l'adresse IP de destination, la partie de l'adresse de destination (masque générique), le type de protocole (TCP, UDP, ICMP, etc.), le port source et de destination.

II.1.5 Types de firewall:

On va distinguer par la suite trois différents types de firewall :

- Les firewalls bridge
- Les firewalls logiciels
- Les firewalls matériels

II.1.5.1 Les firewalls bridge :

Ces derniers sont assez répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Ils ne disposent pas d'adresse IP sur leurs interfaces, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le firewall est indétectable sur le réseau. Ces firewalls se trouvent typiquement sur les Switch.

❖ **Les Avantages**

- Impossible de l'éviter (les paquets passeront par ses interfaces)
- Peu coûteux

❖ **Les Inconvénients :**

- Possibilité de le contourner (il suffit de passer outre ses règles)
- Configuration souvent contraignante
- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

II.1.5.2 Les firewalls logiciels :

Présents à la fois dans les serveurs et les machines, on peut les classer en plusieurs catégories :

II.15.2.1 Les firewalls personnels

Ils sont pour la plupart commerciaux et ont pour but de sécuriser un ordinateur particulier, souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, pour rester accessible à l'utilisateur final, ils s'orientent plus vers la simplicité d'utilisation, et donc mettent de côté l'aspect technique.

- **Avantages :**
  - Sécurité en bout de chaîne (le poste client).
  - Personnalisable assez facilement.
- **Inconvénients :**
  - Facilement contournable.
  - Difficiles à départager de par leur nombre énorme.

II.1.5.2.2 Les firewalls plus « sûre »

Ils se trouvent généralement sous Linux, car ce système d'exploitation offre une sécurité réseau plus élevée et aussi un contrôle plus précis.

- **Avantages :**
  - Personnalisables
  - Niveau de sécurité très bon
- **Inconvénients :**
  - Nécessite une administration système supplémentaire

Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le firewall. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications... chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du firewall.

Figure 12 : Exemple de firewall logiciel.

II.1.5.3 Les firewalls matériels :

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intègres directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement difficile, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur.

- **Avantages**
  - Intégré au matériel réseau
  - Administration relativement simple
  - Bon niveau de sécurité
- **Inconvénients**
  - Dépendant du constructeur pour les mises à jour
  - Souvent peu flexibles.

Figure 13 : Quelques firewalls "matériels"

II.2 Les VPN :

II.2.1 Définition :

Un VPN (Virtual Private Network) ou Réseau Privé Virtuel en français est une connexion inter-réseau permettant de relier 2 réseaux locaux différents de façon sécurisé par un protocole de tunnelisation. **[14]**

II.2.2 La tunnelisation :

La tunnelisation est un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

II.2.2.1 Principe :

Le terme tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc normalement incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. De plus, créer un tunnel signifie aussi encapsuler un protocole dans un protocole de même niveau du modèle OSI (IP dans IPSec par exemple). Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément déchiffrant les données en sortie.

II.2.2.2 Différentes protocoles de tunnelisation :

Il existe de nombreuses implémentations de VPN selon les protocoles utilisés pour Chiffrer les données. De nos jours principalement trois protocoles sont utilisés à grande échelle :

- Le Point-to-Point Tunneling Protocol (PPTP)
- Le Layer Two Tunneling Protocol (L2TP)
- Le protocole Secure Sockets Layer (SSL) et IPsec

II.2.2.2.1 Le protocole PPTP :

Est un protocole développé par US Robotics, 3Com, Microsoft et Ascend Communications. C'est un protocole d'encapsulation de bout en bout sur IP qui permet la mise en place de VPN au-dessus d'un réseau public. L'idée de base du protocole est de permettre l'encapsulation de datagrammes non TCP/IP, comme AppleTalk et IPX, pour être téléportés à travers un réseau IP. Ce protocole utilise quelques concepts de base :

II.2.2.2.2 PPP (Point to Point Protocol):

Est un protocole de couche 2 qui permet l'échange de paquets entre deux extrémités. Ce protocole est souvent utilisé pour échanger des données entre deux ordinateurs reliés par une ligne sérielle ou téléphonique.

II.2.2.2.3 Le protocole L2TP (Layer Two Tunneling Protocol):

Le protocole L2TP est un protocole standard de tunnelisation très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS). Il faut deux types de serveur pour utilise L2TP :

- LAC (L2TP Access Concentrator) : Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS.
- LNS (L2TP Network Server) : Il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel.

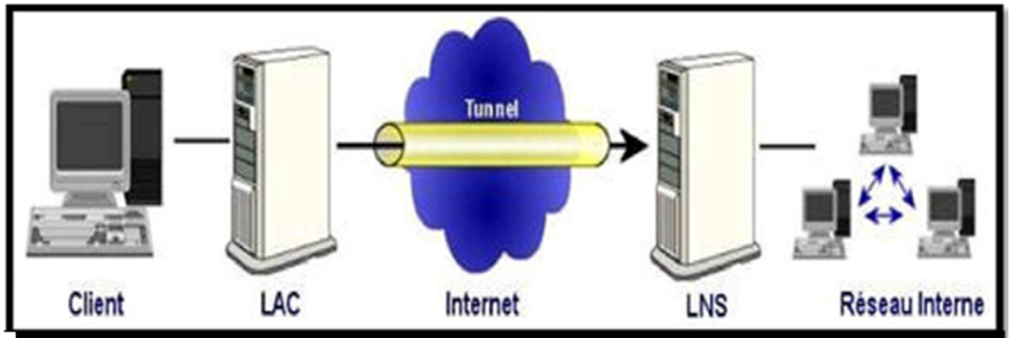


Figure 14 : Exemple pour le protocole L2TP

II.2.2.2.4 Le protocole SSL : Secure Socket Layer

Il permet de crypter toutes les données échangées entre le client et le serveur de façon à ce que seul le serveur puisse décrypter ce qui vient du client et inversement. Un éventuel

pirate ne peut pas, dans un temps raisonnable, décrypter les informations. SSL peut servir de support à n'importe quel protocole en clair comme, HTTP, POP ou IMAP afin de le sécuriser. Il permet d'assurer les trois fonctionnalités suivantes :

- La confidentialité des échanges grâce au cryptage symétrique.
- L'intégrité des données grâce aux fonctions de hachage.
- L'authentification des entités communicantes grâce aux certificats.

Depuis quelques années protocole ssl est utilisé pour sécuriser les VPN. Ce protocole n'est utilisable que pour la sécurisation de flux TCP. Il est largement utilisé pour HTTP, qui devient HTTPS, mais peut être implémenté pour d'autres protocoles comme POP, SMTP.

II.2.2.2.5 Le protocole IPSec (Internet Protocol Security) :

IPsec est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Il est compatible IPv4 et IPv6. IPsec est basé sur deux mécanismes. Le premier

AH (Authentification Header) pour vise à assurer l'intégrité et l'authenticité des datagrammes IP. Le second ESP (Encapsulating Security Payload) aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement

IPSec est nativement un protocole de tunnelage. Pourtant, ce protocole propose aussi des mécanismes de sécurisation des échanges entre utilisateurs des VPN. IPSec assure l'authenticité des extrémités, la confidentialité et l'intégrité des échanges grâce aux algorithmes et mécanismes de chiffrement.

II.2.3 Les différents types de VPN :

Il existe trois types standards d'utilisation des VPN :

II.2.3.1 Le VPN d'accès :

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée.

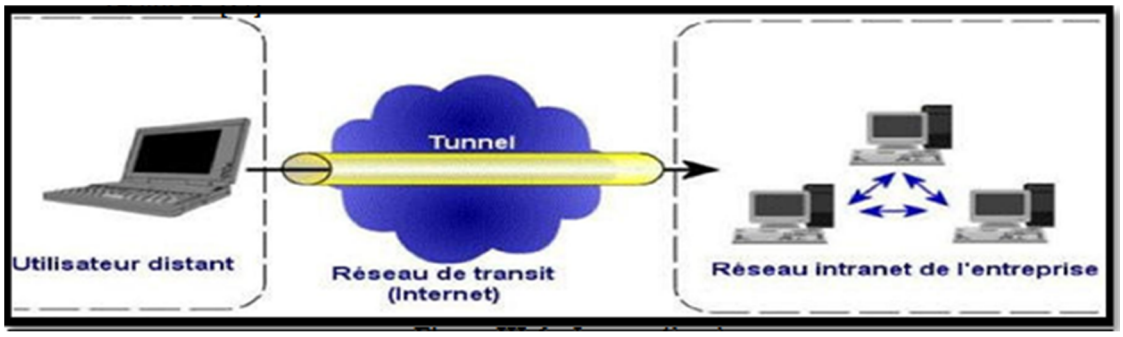


Figure 15 : Le VPN d'accès

II.2.3.2 L'intranet VPN :

Il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

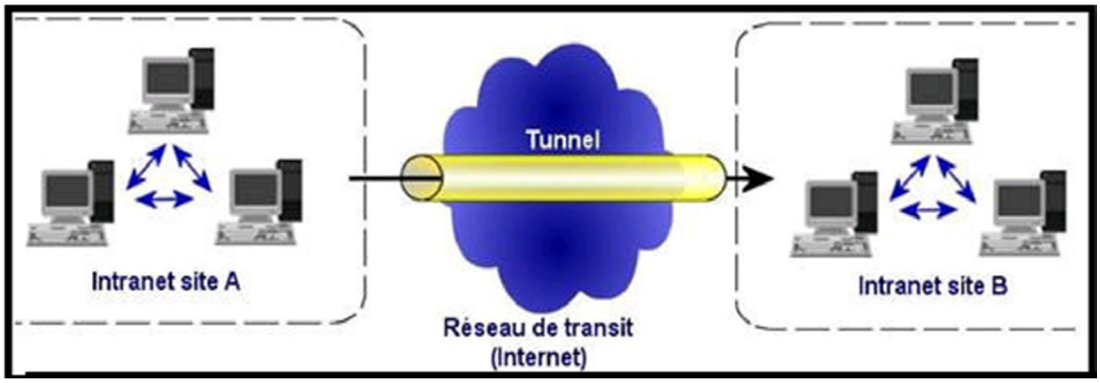


Figure 16 : L'intranet VPN

II.2.3.3 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 cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

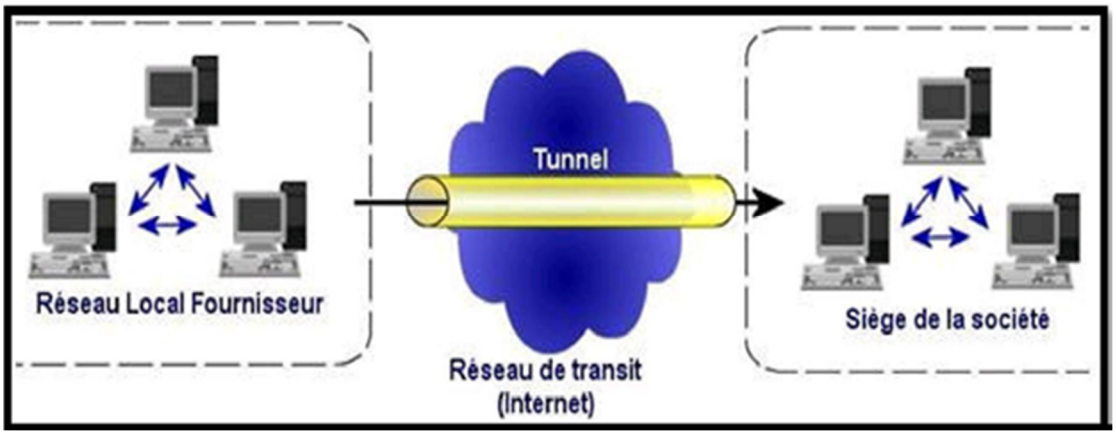


Figure 17 : L'extranet VPN

II.2.4 Avantages et inconvénients de VPN :

- **Cout :** Pour mettre en place un VPN, il est nécessaire avant tout de disposer d'une connexion à Internet. Le coût d'une telle connexion est abordable pour l'ensemble des entreprises et des particuliers avec l'avènement de l'ADSL et du câble.
- **Temps de mise en œuvre :** Lorsque la connexion Internet existe, le temps de mise en œuvre du VPN est fonction de la complexité de la solution ou de la technologie choisie. Il peut aller de quelques jours à quelques semaines en fonction de la complexité de l'environnement. En revanche, l'ajout d'un site dans un VPN existant peut se faire en quelques heures.
- **Performances :** La performance d'un VPN est globalement liée à la performance d'Internet. En conséquence, il est impossible de garantir une bande passante ou un temps de réponse entre deux sites interconnectés.
- **Sécurité :** Les VPN s'appuient sur des technologies de chiffrement robustes et la génération et la mise en place des clés de chiffrement est sous le contrôle du propriétaire du VPN. Le niveau de confidentialité est donc très élevé. Les lignes louées sont également considérées comme très sûres parce que non mutualisées. Mais rien n'empêche une personne mal intentionnée située chez le fournisseur de service d'écouter le trafic.

Conclusion

Nous avons vu dans ce chapitre les firewalls et les vpn, leurs différents types, il est nécessaire de préciser que le firewall est seulement un composant de sécurité, il ne protégera donc pas à lui seul un réseau. Il est nécessaire de l'inclure dans une démarche qui prendra en compte d'autres paramètres tel que la mise à jour des applications.et les VPN qui permettent donc aux réseaux privés de s'étendre et de se relier entre eux au travers Internet. Pour s'équiper, les grandes entreprises auront tendance à se tourner vers des solutions clés en main ou des équipements dédiés (boitiers électroniques, routeurs).Les petites entreprises ou les particuliers, quant à eux, iront plutôt vers des solutions logicielles moins coûteuses.

Chapitre III

Topologie et configuration

Chapitre III : Topologie et Configuration

Introduction :

La nouvelle technologie de l'information et de la communication (NTIC) nous introduit dans un siècle de vitesse en communiquant l'information au sein de nos organisations (entreprises). C'est l'univers immatériel du savoir, de la gestion, de la prise de décision par objectif, du contrôle, de la coopération, de la qualité et de la résolution des problèmes. Aucune personne n'ignore l'importance de l'information dans une organisation ou institution qui nécessite l'organisation, la fiabilité et le bon fonctionnement du système d'information par la capacité de traiter ses informations. Les applications distribuées font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces techniques ont pu se développer grâce aux performances des réseaux locaux. En effet, si les applications distribuées deviennent le principal outil du système d'information de l'entreprise. Voilà quelques questions que nous avons retenues qui traduisent et reflètent nos préoccupations :

- Comment assurer les accès sécuritaires au sein de structures parfois reparties sur de grandes distances géographiquement éloignés ?
- Concrètement, comment une succursale d'une entreprise peut- elle accéder aux données situées sur un serveur distant de plusieurs milliers de kilomètres ?
- Quel serait alors l'impact de ce nouveau système d'information ?
- Quels protocoles et quelle configuration assurent-ils l'accès sécurisé à l'information à travers ces technologies ?

Dans ce chapitre nous venons de faire une étude de fonds sur les contraintes de sécurité lies au système d'information que nous étudions. Nous ne pouvons bien évidement pas revenir sur les détails de l'étude complète d'un projet, mais nous travaillerons sur les parties fondamentales faisant ressortir les points saillants du travail qui nous a été confié.

Dans la gestion quotidienne de la CNAS, la direction ainsi un nombre important de pharmacies ont besoin d'échangés des informations indispensables pour bien servir la population. En plus de la sensibilité de ces informations, la rapidité du procédé nécessitée une liaison réseau sûre et permanente.

L'infrastructure VPN site-à-site est de nos jours très peu répandu pourtant elle apporte une nouvelle approche dans la méthode de transfert des données, elle revêt ainsi un caractère novateur pour les entreprises qui ont opté pour un partage optimal et sécurisé de leur

information. C'est cette architecture que nous voulons l'intégrer au système informatique en place à la CNAS Tissemsilt

III.1 Présentation de la CNAS :

Le régime de la sécurité social à été unifier suite à la loi N°83-11 du 02 juillet 1983 relative aux assurances sociales et la mise en place de la caisse nationale des assurances sociales, des accidents du travail et maladies professionnelles par abréviation CNASAT suit au décret N°85-233 du 20 aout 1985. Devenue caisse nationale des assurances sociales des travailleurs salaries par abréviation CNAS suite au décret N°92-07 du 04 juillet 1992.

En aout 1978 fut la création de la structure de Tissemsilt qui été reliée à la caisse de la wilaya de Tiaret, puis en 06-10-1978 fut la création de la structure de Theniet El Had situé à 48km de la structure de Tissemsilt.

En 1984 et par loi 84/09 signe le 04/04/1984 et suit au découpage des nouvelles wilayas fut la création de la wilaya de Tissemsilt.

Ce découpage de 1984 a permis la création des caisses pour les nouvelles wilaya, en fin de l'année 1986 fut la création de la caisse de l'agence de TISSEMSILT avec la création d'autre structures qui sont BORDJ-BOUNAAMA créée le 01-03-1988 situé à 58km du chef-lieu de la wilaya, KHEMISTI situé à 17km de chef-lieu de la wilaya créée le 05-06-1988 et la structure de LARDJEM situé à 32km du chef-lieu de wilaya qu'était rattachée à l'entreprise des mine créée en 1948 (ex: CASOMINE) a été par la suite transféré au patrimoine de la caisse.

Avec le temps et le nombre d'assurés existant au niveau des localités d'AMARI et Bordj EMIR AEK, a été procédé à procédé à l'ouverture des correspondances afin d'alléger les déplacements des assurés et rapprochement de l'administration aux assurés.

A cette date l'agence CNAS de la wilaya de Tissemsilt compte 03CP, 03antennes et 02 correspondances qui chiffrent d'un nombre de 118.218 assurés affiliés et 202 708 ayant-droit des assurés.

III.1.1 Les Missions de la CNAS :

- Gérer les prestations en nature et en espèces des assurances sociales des accidents du travail et des maladies professionnelles.
- Gérer les prestations familiales.
- Assurer le recouvrement, le contrôle et le contentieux du recouvrement des cotisations destinées au financement des prestations prévues aux alinéas précédents.

- Contribuer à promouvoir la politique des préventions des accidents du travail et des maladies professionnelles et de gérer le fonds des préventions des accidents du travail et des maladies professionnelles.
- Gérer les prestations dues aux personnes bénéficiaires des accords bilatéraux de sécurité sociale.
- Organiser, coordonner et exercer le contrôle médical.
- Entreprendre des actions sous forme de réalisations à caractère sanitaire et sociale.
- Entreprendre des actions de prévention, d'éducation et d'information sanitaire après proposition du conseil d'administration de la caisse.
- Gérer les fonds d'aide et de recours.
- Conclure les conventions

III.1.2 L'infrastructure Nationale de la CNAS :

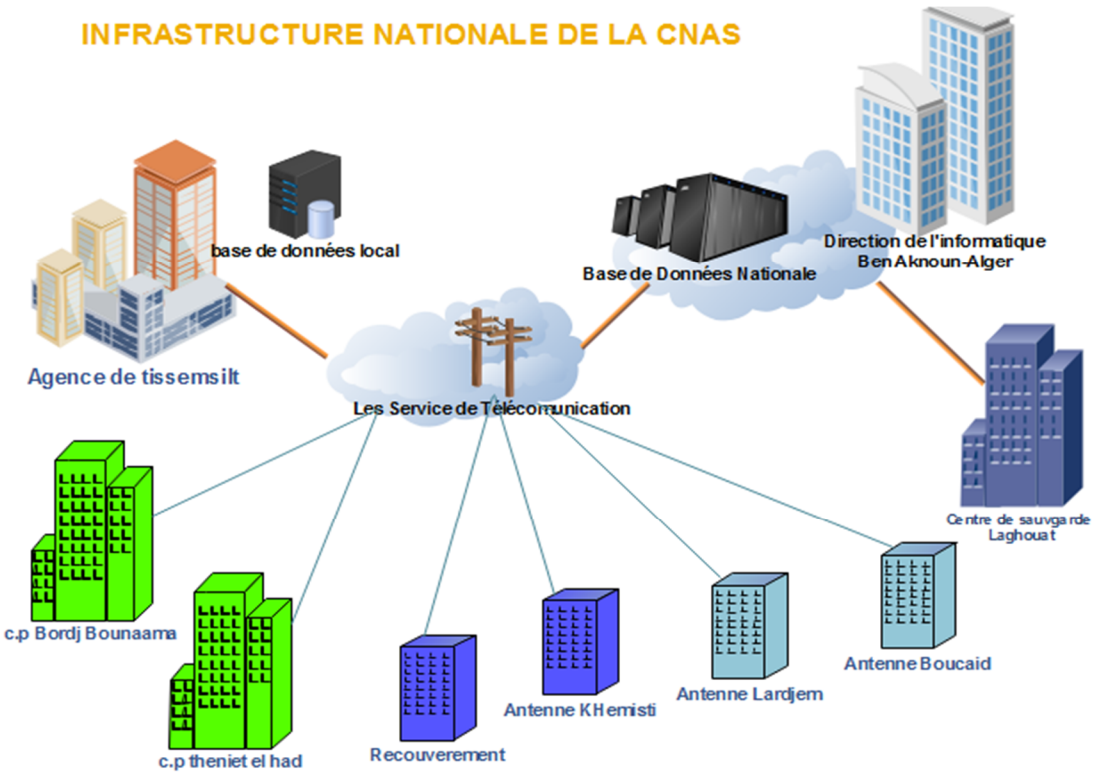


Figure 18 : Infrastructure Nationale de la CNAS

III.1.3 Présentation du réseau de la CNAS Tissemsilt :

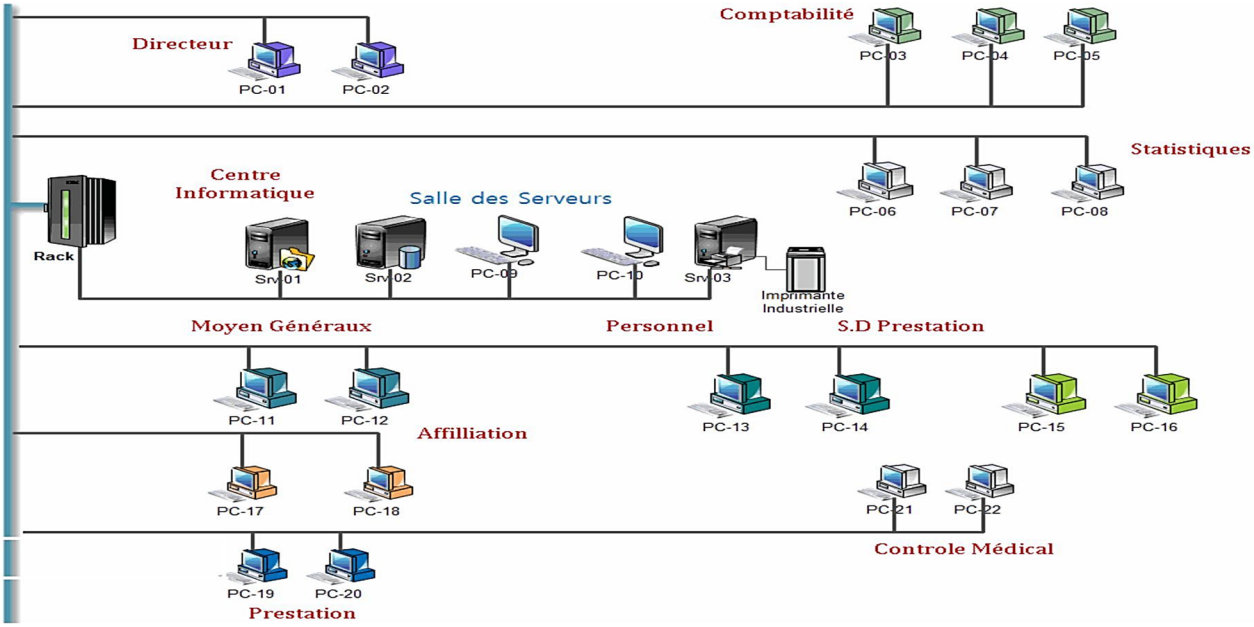


Figure 19 : Présentation du Réseau de la CNAS

III.2 La solution VPN :

Nous avons opté pour la solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de la CNAS ainsi que les pharmacies associées ; afin de résoudre au mieux aux différentes préoccupations manifestées par les responsables informatiques de la CNAS et aussi pour pallier aux différents problèmes relevés au niveau de la critique de l'existant.Mettre en avant le nombre d'utilisateurs potentiels du lien VPN, les applications concernées et le débit maximum à consommer.

Faire un monitoring des flux de données et une gestion des priorités doit s'adapter aux différents usages et aux remontées des utilisateurs ; la gestion de la bande passante et des équipements ; mettre en place un mécanisme de surveillance et de détection de connexion suspecte qui s'établie sur un lien VPN.

Il est néanmoins important de préciser que la solution retenue garantie la confidentialité, la sécurité et l'intégrité des données sur des canaux privés. Cette solution VPN site-à-site permet d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux.

La solution VPN site-à-site permet de mettre à niveau, à moindre coût, les architectures multipoints utilisant le réseau commuté limité en bande passante et généralement obsolètes, employée par la CNAS.

La mise en place d'un VPN permettra de distribuer un accès à Internet et des applications Web depuis leurs emplacements. Les VPN site-à-site étendent le WAN à moindre coût et en toute sécurité vers des entités non desservies, telles que des succursales et des partenaires commerciaux (extranet).

La solution VPN site-à-site de Cisco, totalement intégrée et composée d'un équipement unique, peut être déployée et configurée en toute simplicité.

Dans notre projet, on va configurer une connexion VPN dans une partie d'architecture de réseau interne parmi l'architecture globale de CNAS Tissemsilt, et la figure suivante l'indique :

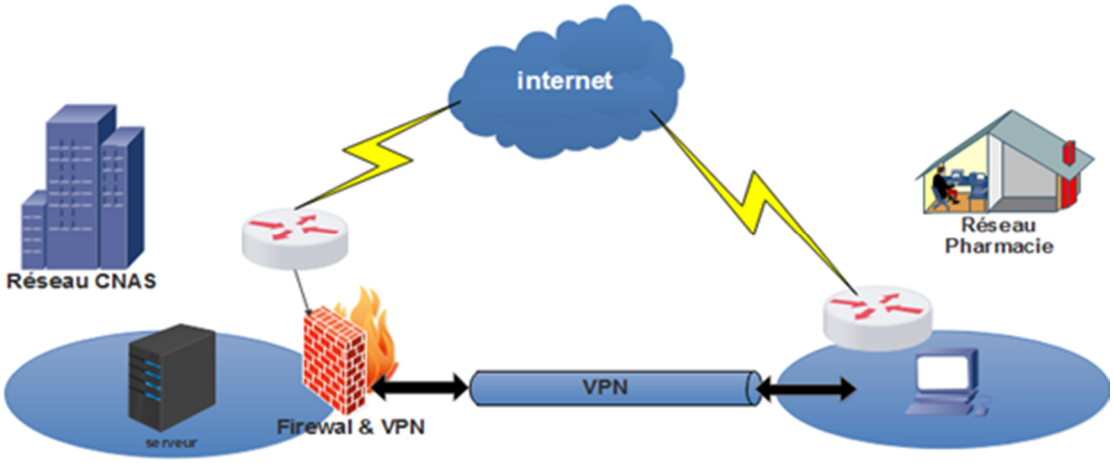


Figure 20 : Architecture de solution proposée

L'objectif de cette connexion vpn est de permettre à un utilisateur distant du centre CNAS Tissemsilt de mettre à jour les cartes Chifa par exemple. Si une pharmacie est associée à la CNAS, il suffit d'avoir un droit d'accès à la base de données de la CNAS pour faire le travail à son niveau sans en avoir besoin de se déplacer. Cette solution est bénéfique pour tout le monde, la CNAS en premiers, les pharmacies et les assurés. Evidemment, il est clair qu'il faut développer une application spécifique à ce cas de figure en exploitant les avantages mis à disposition par le réseau VPN

III.3 Simulation de la configuration:

Nous avons réalisé une maquette simulant la solution VPN à l'aide de l'émulateur GNS3 de Cisco, CCP et VMWARE, une étude a était entamée concernant les différents protocoles de routages et leur configuration sur les routeurs Cisco

- **Logiciel GNS3** : GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Vous connaissez peut-être avec VMWare ou Virtual Box qui sont utilisées pour émuler les différents systèmes d'exploitation dans un environnement virtuel. Ces programmes vous permettent d'exécuter plusieurs systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type de d'émulation à l'aide de Cisco Internetwork Operating Systems.

Il vous permet d'exécuter un IOS Cisco dans un environnement virtuel sur votre ordinateur. GNS3 est une interface graphique pour un produit appelé Dynagen. Dynamips est le programme de base qui permet l'émulation d'IOS. Dynagen s'exécute au-dessus de Dynamips pour créer un environnement plus convivial, basé sur le texte environnement. Un utilisateur peut créer des topologies de réseau de Windows en utilisant de simples fichiers de type ini.

- **VMware Workstation:** VMware Workstation est un environnement de test et de développement qui permet aux administrateurs de systèmes pour créer et exécuter des machines virtuelles (VM) directement sur un ordinateur de bureau.
- **CCP :** Cisco Configuration Professional est un outil de gestion de périphérique de l'interface graphique à base de routeurs d'accès Cisco. Il simplifie routeur, firewall, IPS, VPN, communications unifiées, WAN, LAN et configuration sans fil de base par le biais facile à utiliser sorciers.
- **ASA :** Adaptative security appliance. Matériel crée par l'entreprise Cisco dans le but d'améliorer la sécurité du réseau. Possède de nombreuses possibilités, notamment firewall, VPN et inspection applicative des paquets.
- **ASAv :** Le Cisco Virtual Appliance Adaptive sécurité (ASAV). Cet appareil apporte la puissance de l'ASA au domaine virtuel et les environnements de Cloud privé. Il utilise le même logiciel que l'appareil physique pour offrir des fonctionnalités de sécurité éprouvée. Vous pouvez l'utiliser pour protéger les charges de travail virtuelles au sein de votre centre de données. Plus tard, vous pouvez développer, contrat, ou changer l'emplacement de ces charges de travail au fil du temps et étendre les infrastructures physiques et virtuelles.et pour l'installation d'ASAv dans Vmware consulter le site suivant :

https://www.youtube.com/watch?v=uMiu9G3N_Gw

- **Mode de base pour configurer Cisco ASA :**

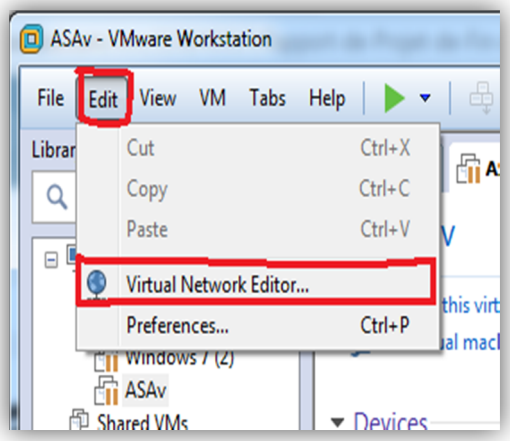
Pour configurer les Appareils de Sécurité Adaptative, Cisco a défini deux modes de base, le premier c'est le mode graphique appelé ASDM (Adaptive Security Device Manager) et le deuxième par invite de commande CLI (Commande-Line Interface).

Le mode ASDM : les cisco ASA Firewall sont livrés avec un logiciel d'administration graphique ASDM, il est chargé de l'Appliance de sécurité, puis utilisé pour configurer, surveiller et gérer l'appareil. Il permet de récupérer, modifier et administrer les politiques de sécurité ainsi que de faire du monitoring.

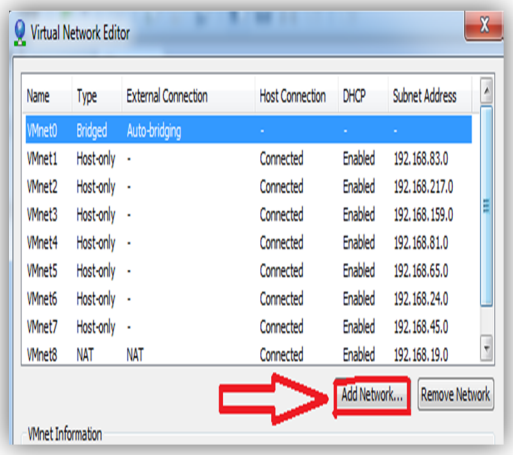
Le mode CLI : un interpréteur de commande et c'est un programme généralement fait partie des composantes de base d'un système d'exploitation. Son rôle est de traiter les commandes tapées au clavier par l'utilisateur. Ces commandes, une fois interprétée auront pour effet de réaliser telle tâche d'administration, ou bien de lancer l'exécution d'un logiciel.

III.3.1 La topologie :

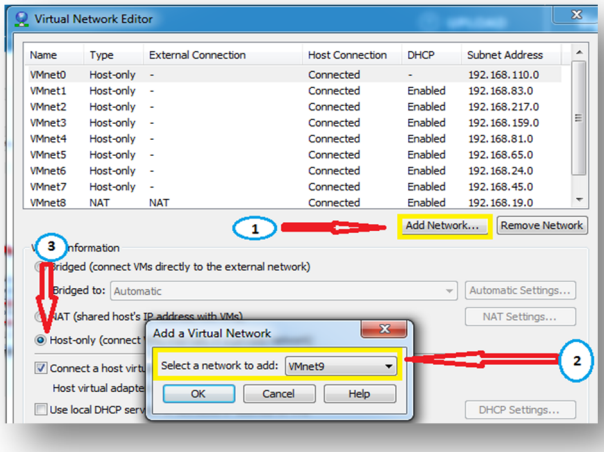
Création de la topologie : Connecter les hôtes GNS3 a Vmware



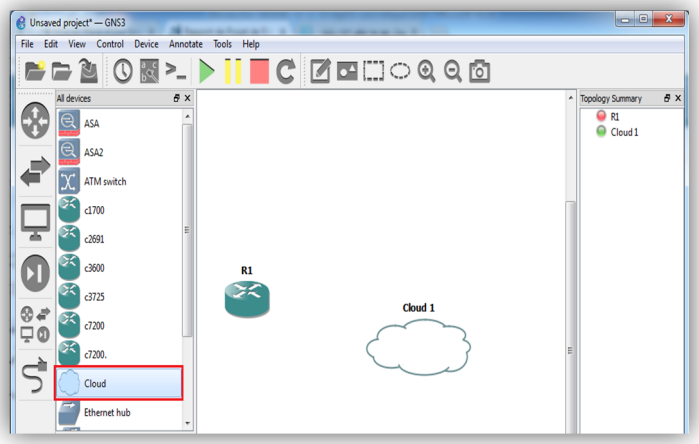
À partir de l'Edit sélectionné **Virtual Network Editor**



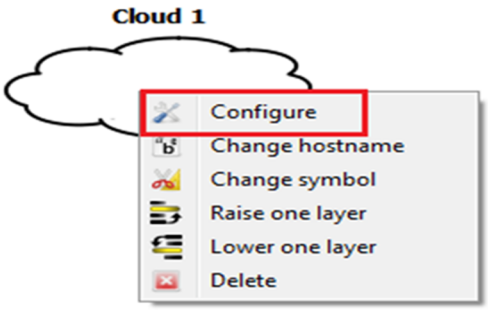
Cliquer sur pour ajouter des cartes réseaux



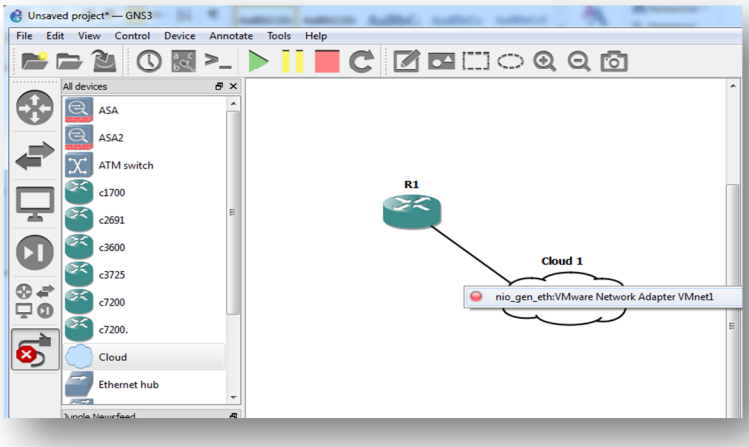
A partir du de l'Onglet Réseau dans les configurations de la machine virtuel attribuer à elle une carte réseau de votre choix.



Dans GNS3 faire glisser et déposer un routeur à partir du menu de gauche, puis un nuage, à travers lequel gns3 sera Connecté à un hôte VMware



Bouton droit sur le nuage et sélectionner Configure



Maintenant manuellement interconnecter l'interface du routeur (par exemple Fa0 / 0) avec le nuage, En déplaçant le curseur à la ligne sur le nuage d'une ligne avec un adaptateur réseau précédemment configuré apparaît.

III.3.2 Configuration des équipements:

Qu'il s'agisse de sécuriser une connexion ou encore de créer une liaison entre deux sites au travers d'un réseau non sécurisé tel qu'Internet, le passage par un tunnel VPN se révèle être une arme redoutable. Chaque site étant une image d'un petit réseau disposant d'un accès à internet Voilà comment se présente la topologie :

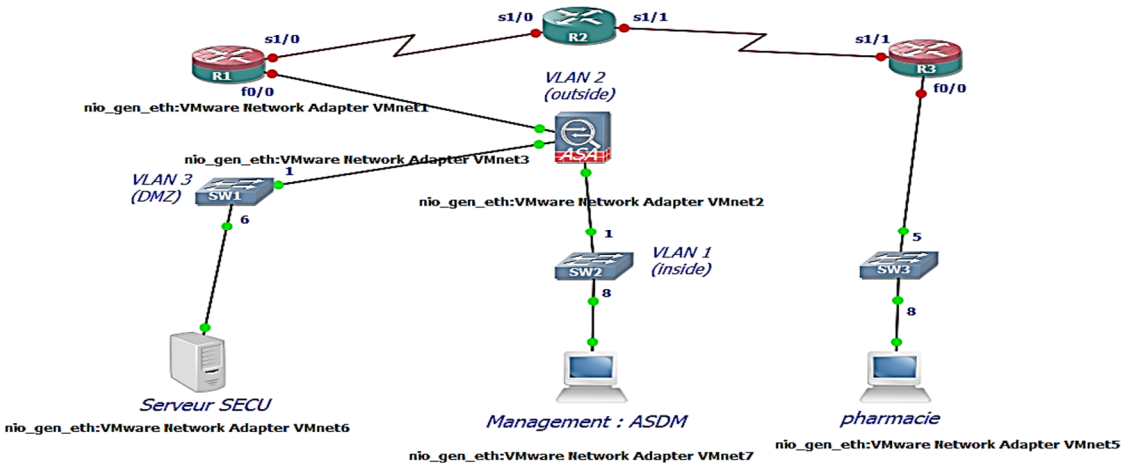


Figure 21 : Schéma réalisé avec le simulateur GNS3

Sur cette illustration, nous pouvons voir les éléments suivants :

- 3 routeurs (cisco 7200)
- 3 switches
- Serveur -secu : windows serveur 2003
- Pc (management :ASDM) : windows 7, java 7 (ASDM install)
- Pc (pharmacie): Windows 7, java 7 et CCP version 2.8
- ASAV (version 9 et ASDM version 7.3(1)

Tableau des adresses IP :

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	209.165.200.225	255.255.255.248	/
	S1/0	10.1.1.1	255.255.255.252	/
R2	S1/0	10.1.1.2	255.255.255.252	/
	S1/1	10.2.2.2	255.255.255.252	/
R3	F0/0	172.16.3.1	255.255.255.0	/
	S1/1	10.2.2.1	255.255.255.252	/
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	/
ASA	VLAN2 (E0/0)	209.165.200.226	255.255.255.248	/
ASA	VLAN3 (E0/2)	192.168.2.1	255.255.255.0	/
Serveur Secu	NIC	192.168.2.3	255.255.255.0	192.168.2.1
Management ASDM	NIC	192.168.1.3	255.255.255.0	192.168.1.1
Pharmacie	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Configuration de base d'un routeur:

La configuration d'un périphérique Cisco IOS commence par l'activation du mode d'exécution privilégié. Le mode privilégié accorde l'accès à plusieurs modes de configurations utilisés pour configurer le périphérique.

a. Configurer les adresses IP d'interface du routeur, comme indiqué dans le tableau des adresses IP

b. Configurer clock rate pour les routeurs par exemple :

R1 (config) # interface S1/0

R1 (config) # clock rate 64000

c. Configurer la route statique par défaut de R1 à R2 et de R3 à R2 :

R1 (config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

R1 (config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2

d. configurer la route statique de R2 à R1 Fa0/0 et de R2 à R3

R2 (config)# ip route 209.165.200.224 255.255.255.248 10.1.1.1

R2 (config)# ip route 172.16.3.0 255.255.255.0 10.2.2.1

e. Sur R3, définissez le mot de passe permettant de classe et la console et les mots de passe vty (telnet) à cisco. Configurer ces paramètres sur R1 et R2. R3 est montré ici comme un exemple.

le mot de passe enable secret sont utilisés pour limiter l'accès au mode privilégié

R3(config)# enable secret class

Pour que les utilisateurs puissent accéder à distance au routeur à l'aide de Telnet, un mot de passe doit être défini sur une ou plusieurs lignes de terminal virtuel (vty)

R3(config)# line vty 0 4

R3(config-line)# password cisco

R3(config-line)# login

Les commandes suivantes permettent de définir un mot de passe facultatif mais crecommandé sur la ligne de console

R3(config)# line con 0

R3(config-line)# password cisco

R3(config-line)# login

Configuration de R3 pour diriger Cisco CP

Exécutez ces étapes de configuration afin de diriger Cisco CP sur un routeur de Cisco

R3(config)# ip http server

R3(config)# ip http authentication local

Router(config)# username admin privilege 15 password cisco123

Configuration de ASAv:

Installer ASAv sur vmware

Copiez et collez les commandes pré-VPN de script de configuration

hostname CNAS-ASA }

!

domain-name cnasecurity.com

!

enable password class}

passwd cisco

!

interface GigabitEthernet0/0

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

no shut

!

interface GigabitEthernet0/1

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

```
no shut
!
interface GigabitEthernet0/2
nameif dmz
security-level 70
ip address 192.168.2.1 255.255.255.0
no shut
!
object network inside-net
subnet 192.168.1.0  255.255.255.0
!
object network dmz-server
host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
nat (inside,outside) dynamic interface
!
object network dmz-server
nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
```

username admin password cisco123

!

aaa authentication telnet console LOCAL

aaa authentication ssh console LOCAL

aaa authentication http console LOCAL

!

http server enable

http 192.168.1.0 255.255.255.0 inside

ssh 192.168.1.0 255.255.255.0 inside

telnet 192.168.1.0 255.255.255.0 inside

telnet timeout 10

ssh timeout 10

!

class-map inspection_default

match default-inspection-traffic

policy-map type inspect dns preset_dns_map

parameters

message-length maximum client auto

message-length maximum 512

policy-map global_policy

class inspection_default

inspect icmp

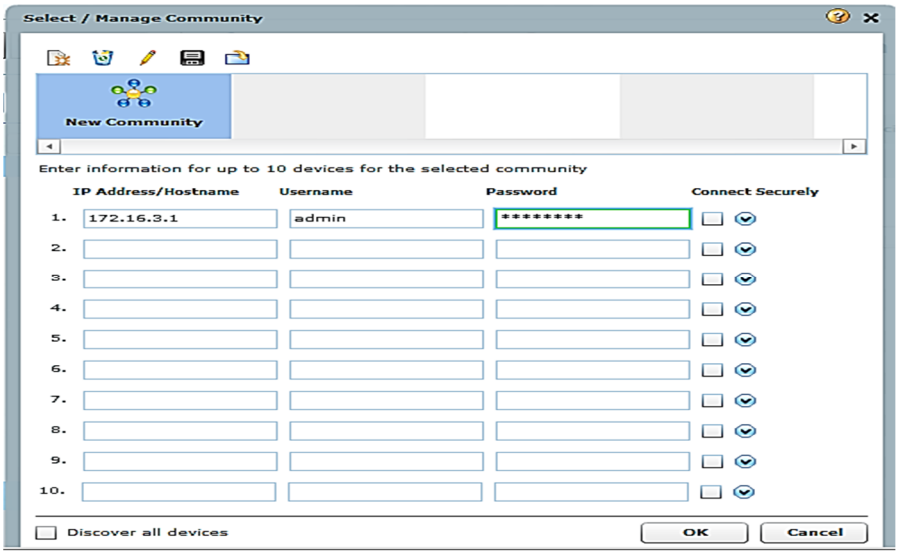
!

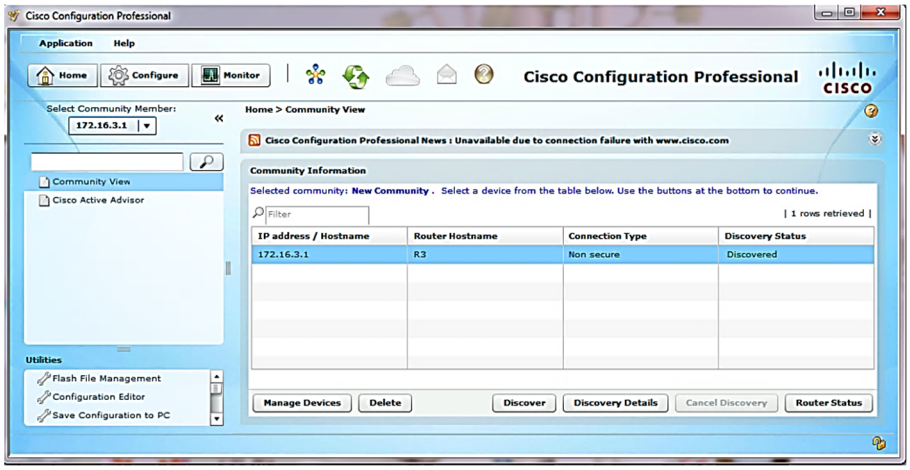
prompt hostname context

no call-home reporting anonymous

Configuration de VPN :

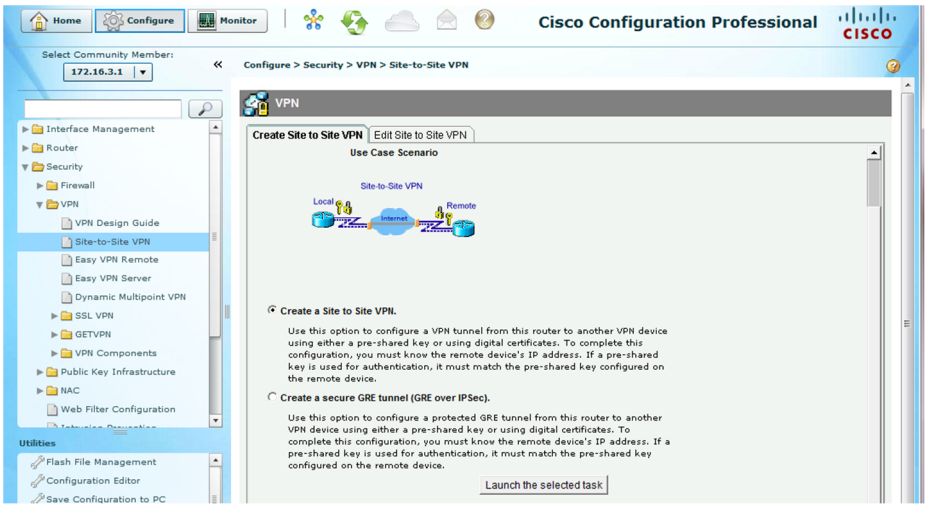
Lancez Cisco CP dans pc (pharmacie) qui va installer dans vmware et choisissez la Communauté qui a le routeur que vous voulez configurer.

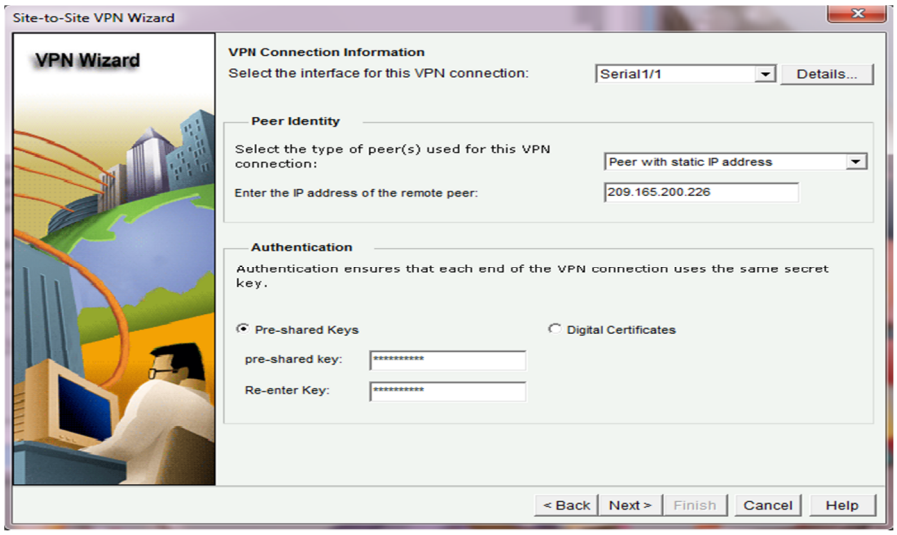




Lancez CCP VPN wizard pour configurer R3 choisir Security > VPN > Site-to-Site VPN et clique launch the selected task .Configurer les paramètres de base VPN d'information de connexion, Entre IP adresse de ASA interface E0/0 (209.165.200.226) et Clé Pré-Partagée (cisco12345)

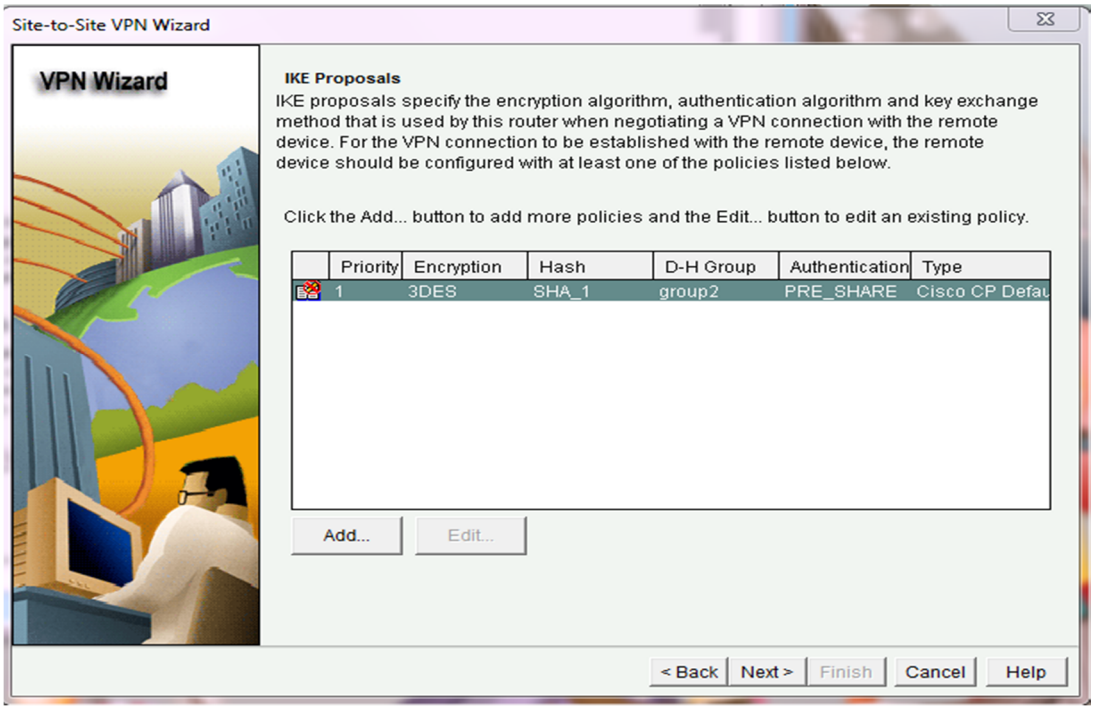
Dans la section Authentification, cliquez clés pré-partagées, et entrez la clé cisco12345 VPN pré-partagée. Retaper la clé pour la confirmation. Cette clé authentifie l'échange initial pour établir la sécurité Association entre les appareils. Une fois terminé, votre écran doit ressembler à ce qui suit. Lorsque vous sont entrés correctement ces paramètres, cliquez sur Suivant.





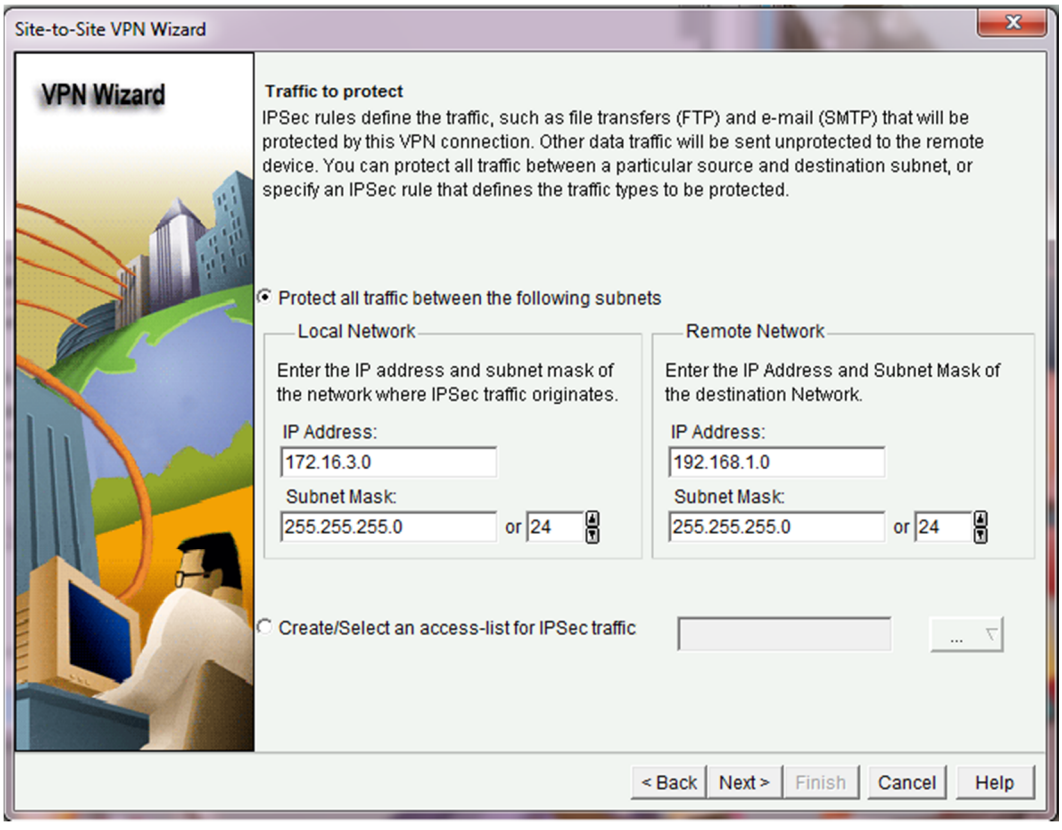
Spécifiez la politique IKE :

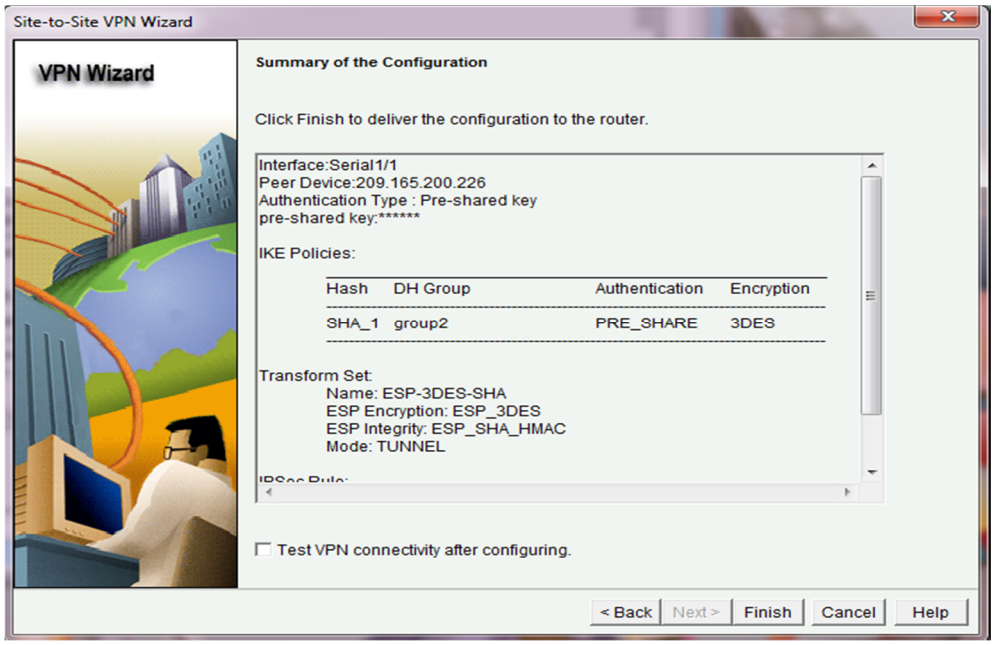
Politique IKE : définit la méthode d'authentification et génère automatiquement les clés de cryptage

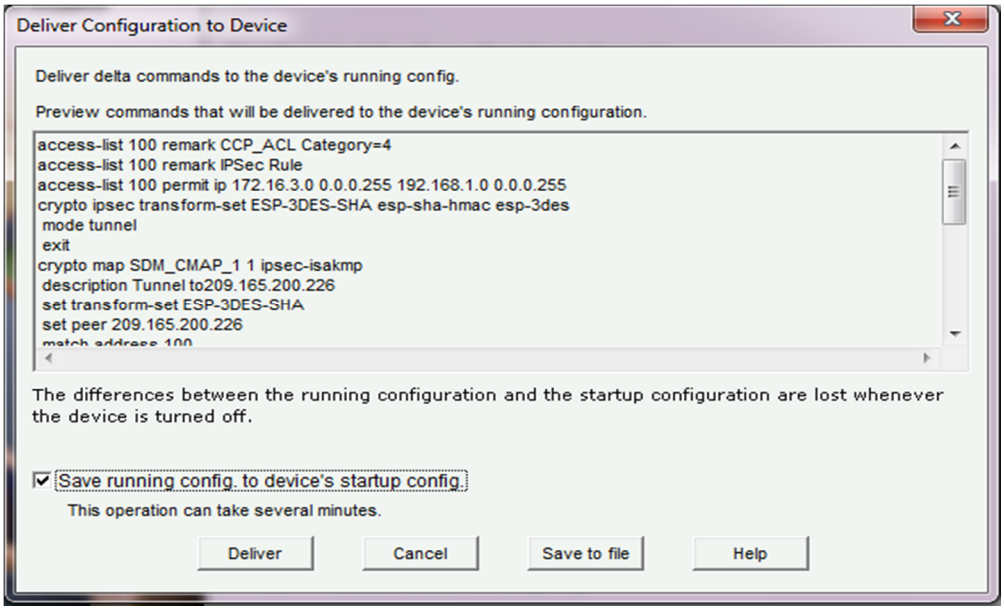


Spécifiez le trafic à protéger.

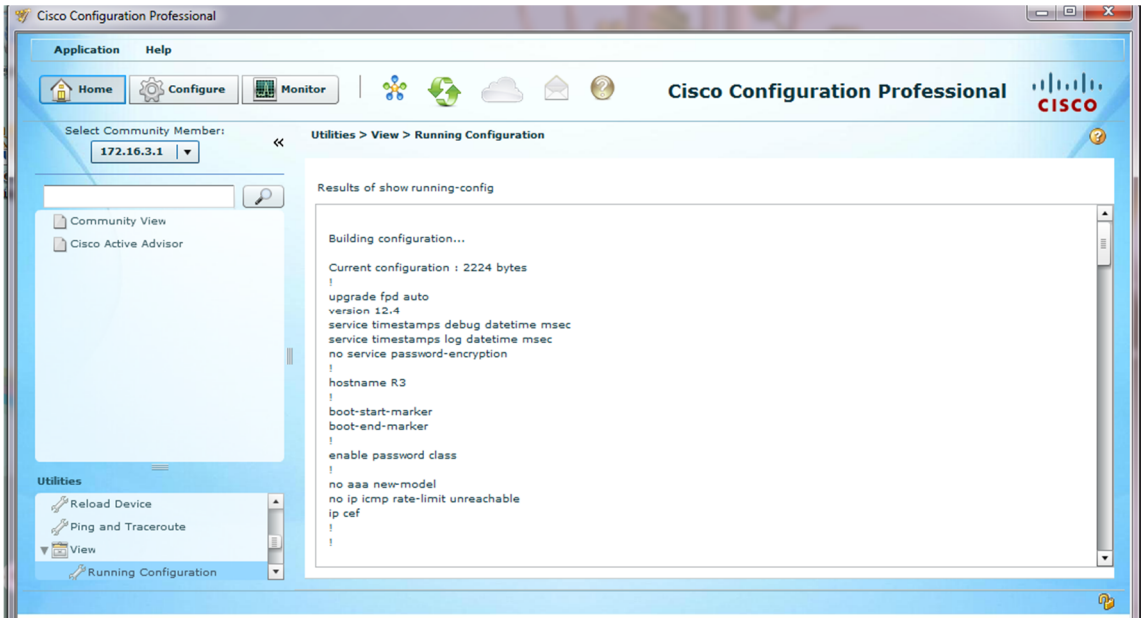
Passez en revue le résumé de l'écran de configuration. Il devrait ressembler à celui ci-dessous. Vous pouvez faire défiler vers le bas pour voir la règle IPsec (ACL) que CCP crée pour R3, qui permet tout le trafic de réseau 172.16.3.0/24 au réseau 192.168.1.0/24.



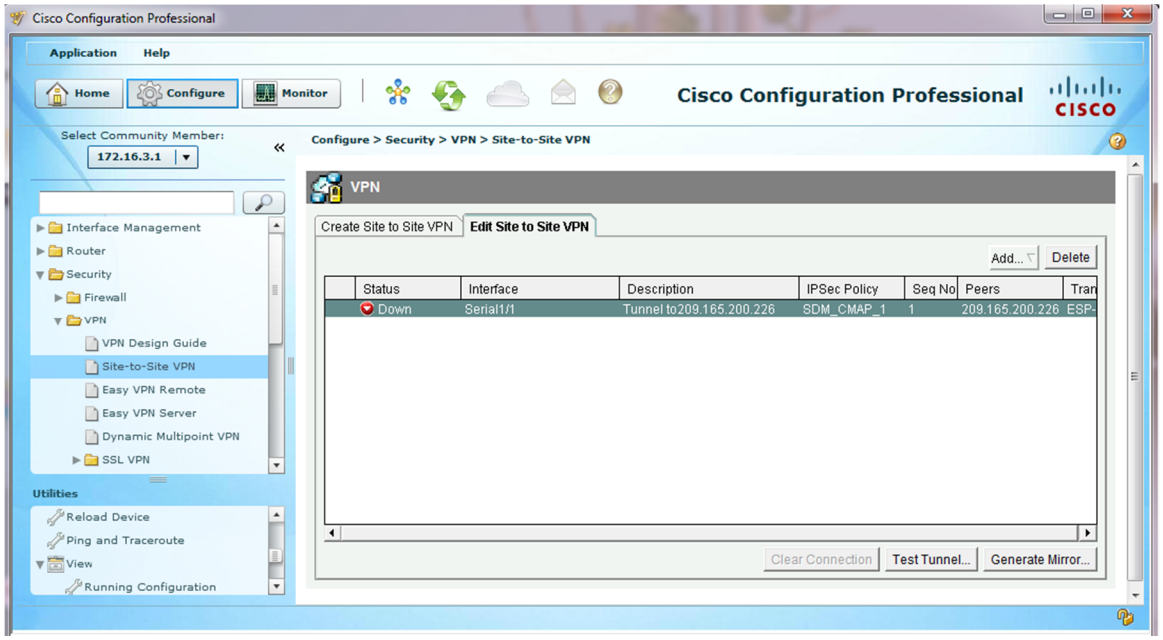




Pour afficher la configuration de démarrage, cliquez sur Home > Utilities > View > IOS Show Commands



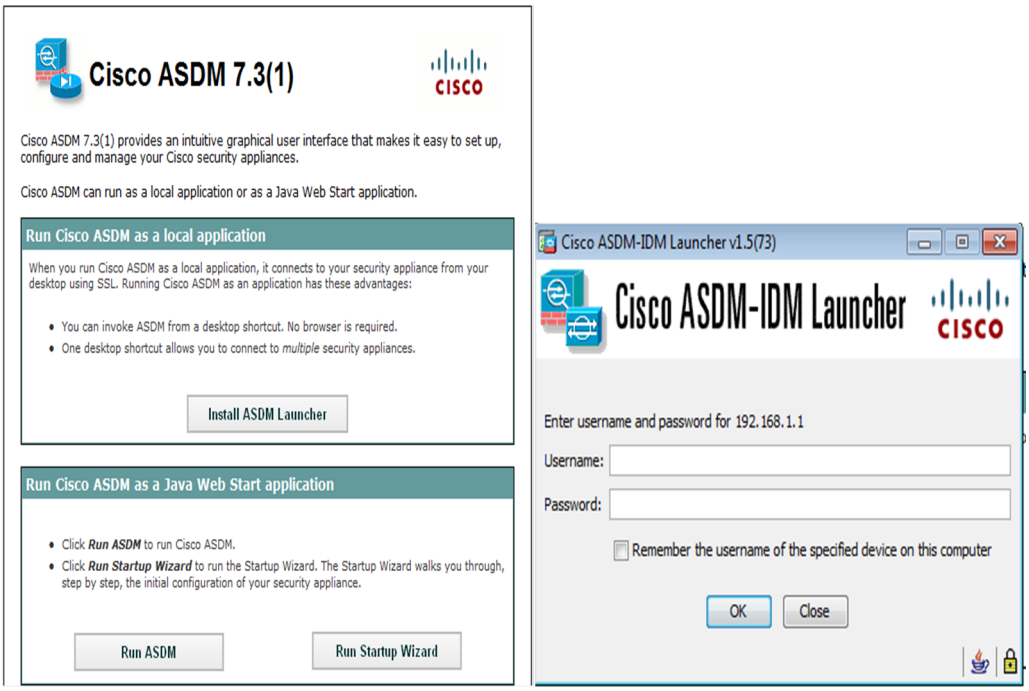
Clique sur Test Tunnel pour vérifier la fonctionnalité VPN



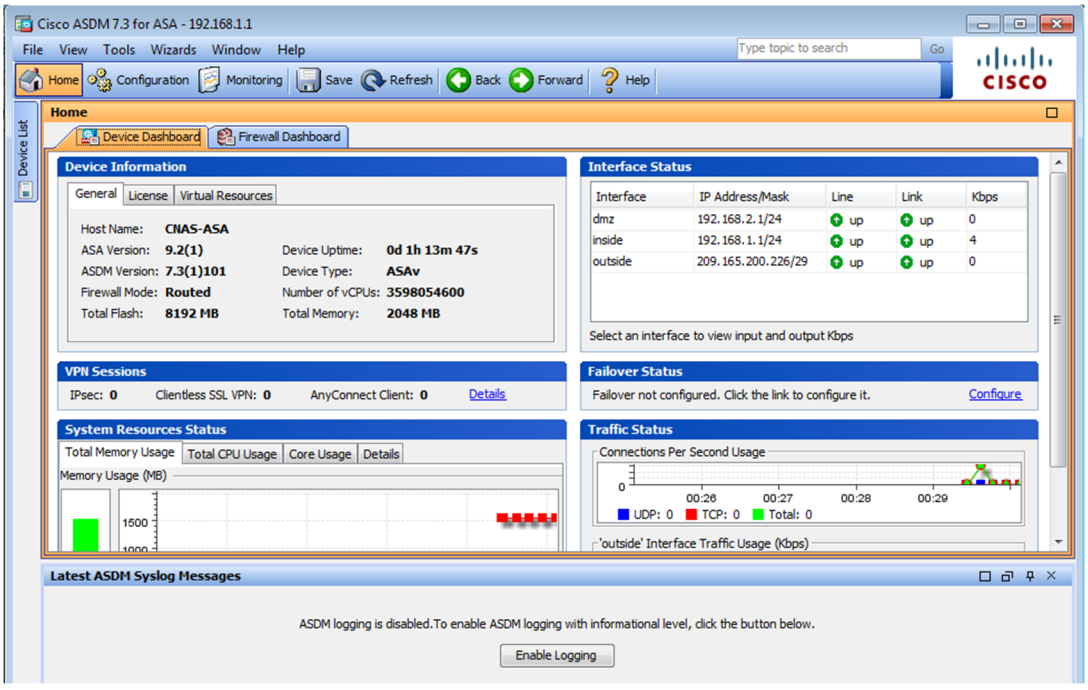
Dans la partie , vous allez configurer l'ASA comme une extrémité du tunnel VPN IPsec. Le tunnel entre l'ASA et R3 passe par R1 et R2

ASDM :

Ouvrez un navigateur sur PC (Management : ASDM) et de tester l'accès HTTPS à l'ASA en entrant https://192.168.1.1. Et clique run ASDM

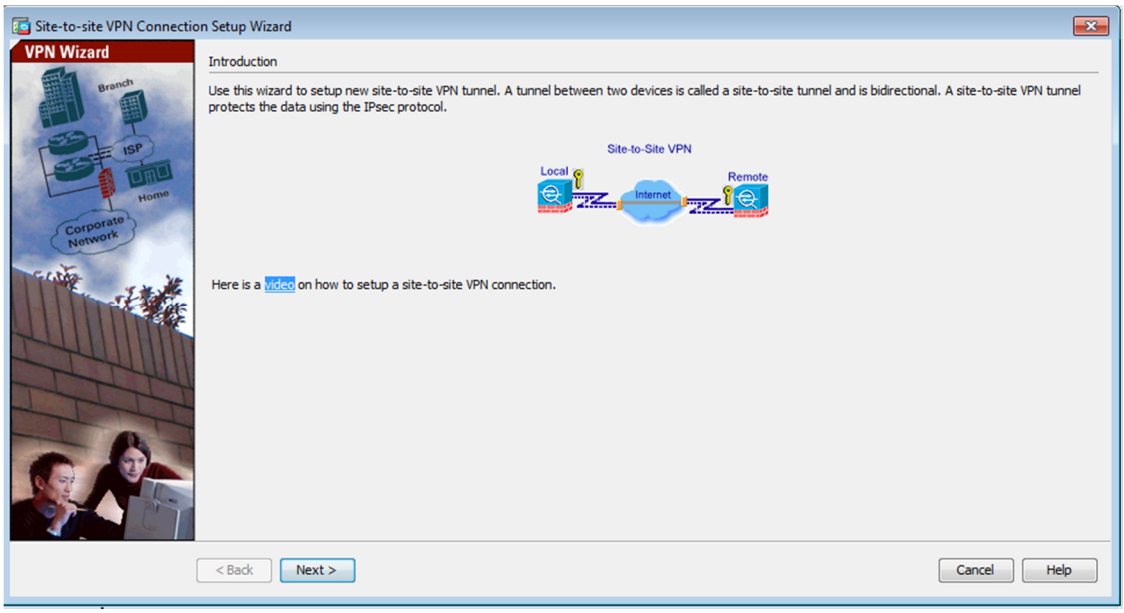


Consultez l'écran ASDM Accueil

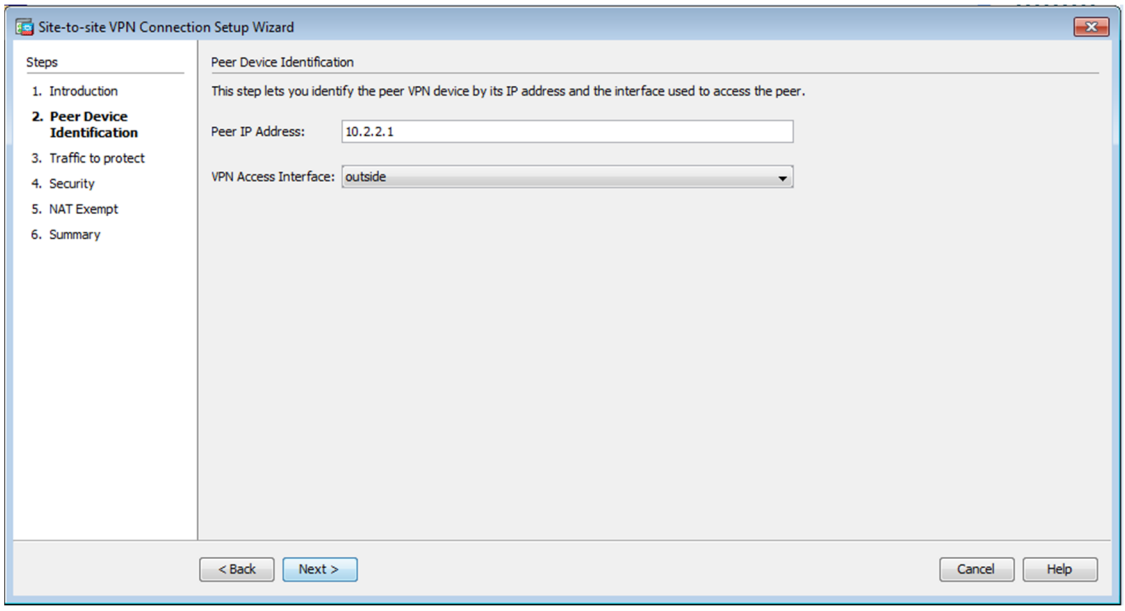


Lancez wizard VPN.

Dans le menu principal ASDM, cliquez sur Assistants Wizards > VPN Wizards > Site-to-Site VPN Wizard

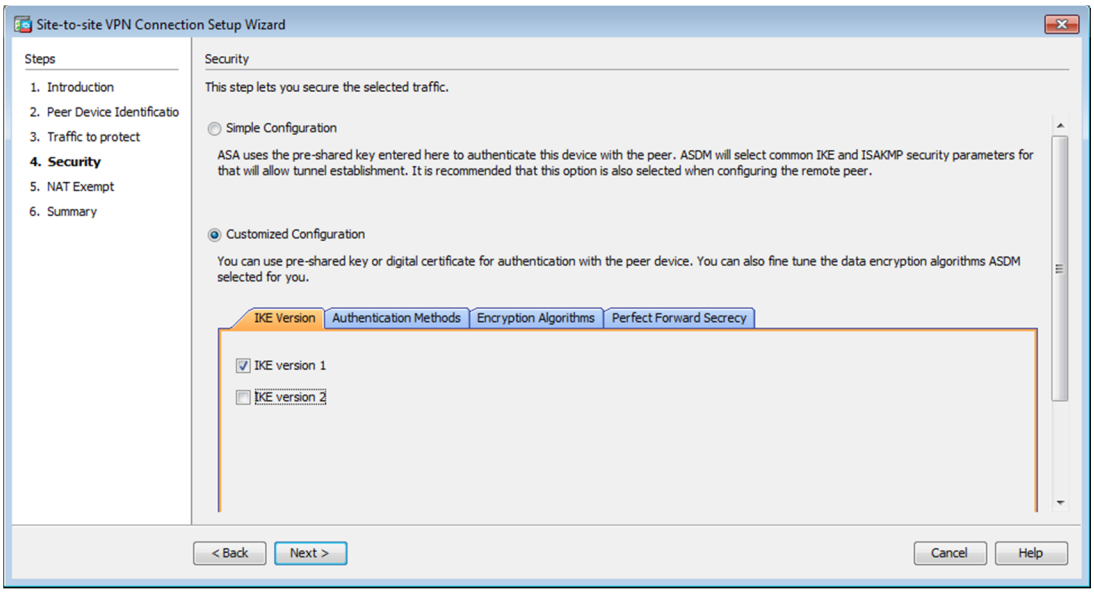


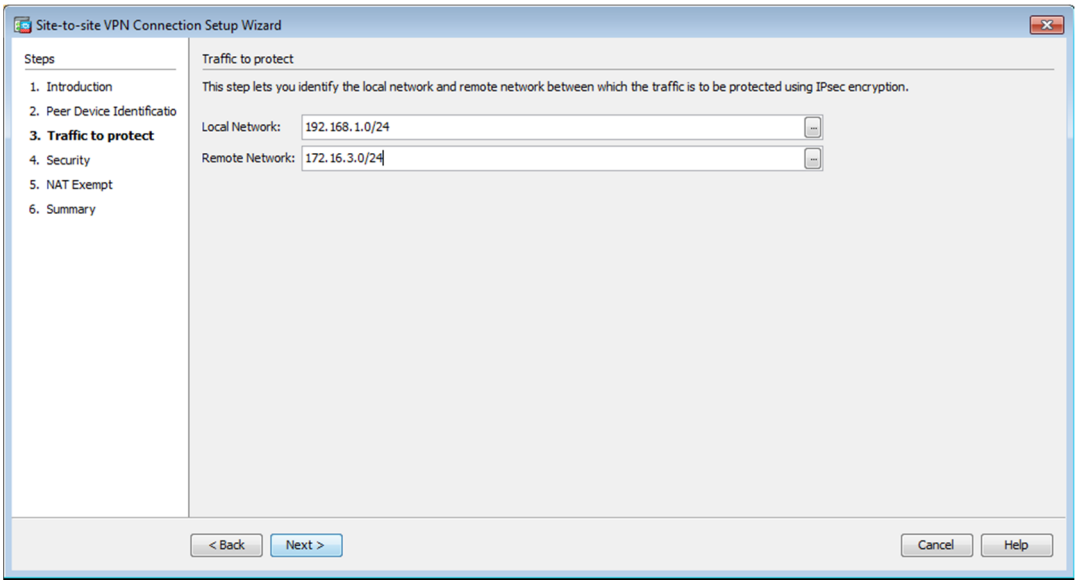
Configurer peer device identification entre ip adresse de R3 interface S1/1



Presque chaque client VPN IPsec utilise la norme Internet Key Exchange (IKE) pour établir automatiquement des tunnels. IKE authentifie pairs, négocie des algorithmes pour protéger les paquets IP, et génère des clés utilisées par ces algorithmes. IKE est l' endroit où vous trouverez la plus grande diversité entre les clients IPsec et les passerelles.

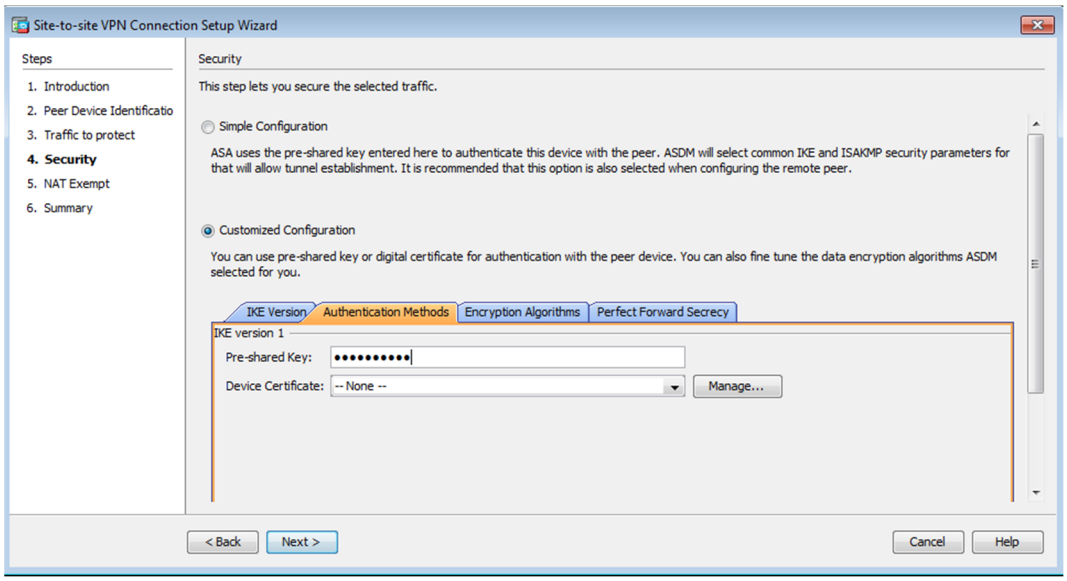
La plupart des clients IPsec peuvent être authentifiés avec des secrets partagés; certains soutiennent également les certificats numériques. Si vous avez besoin authentification de certificat, veillez à sélectionner un client IPsec fonctionne avec votre autorité de certification choisie.

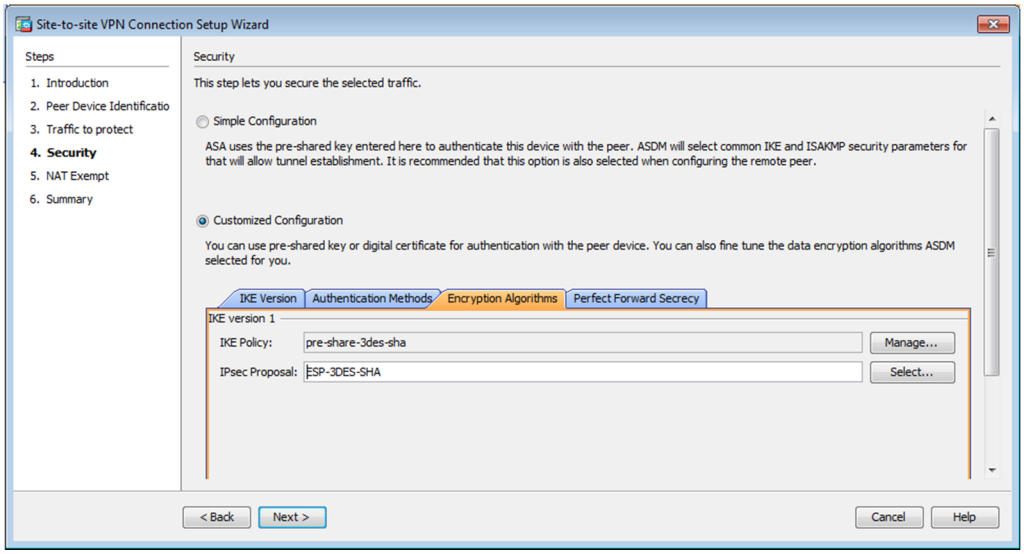


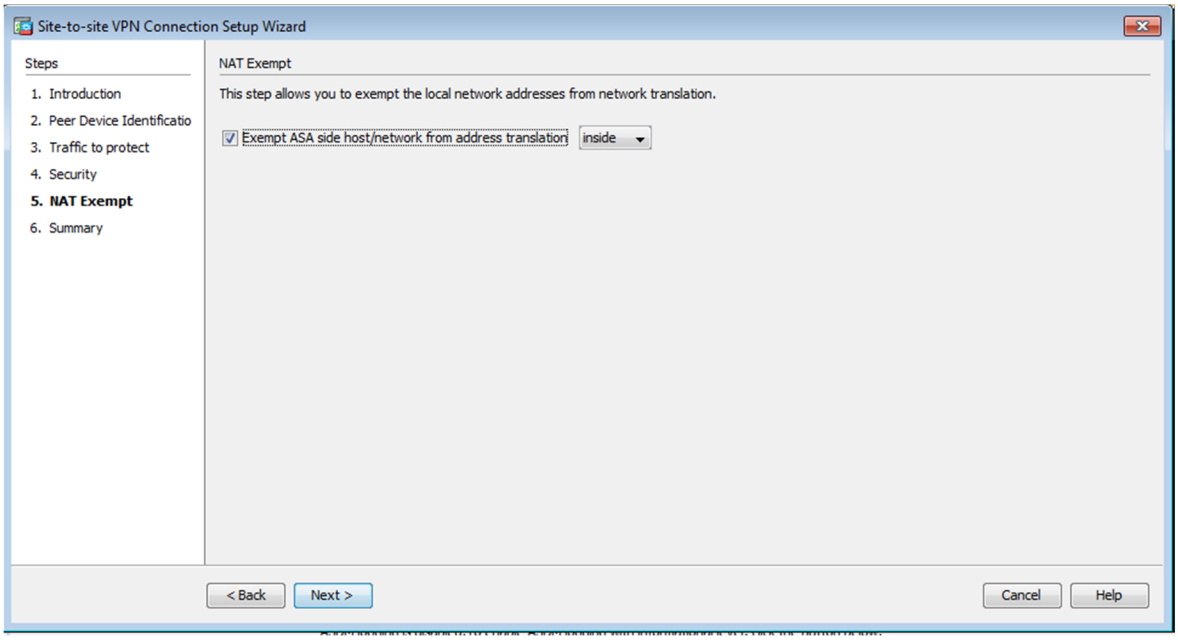


Configurer l'authentification

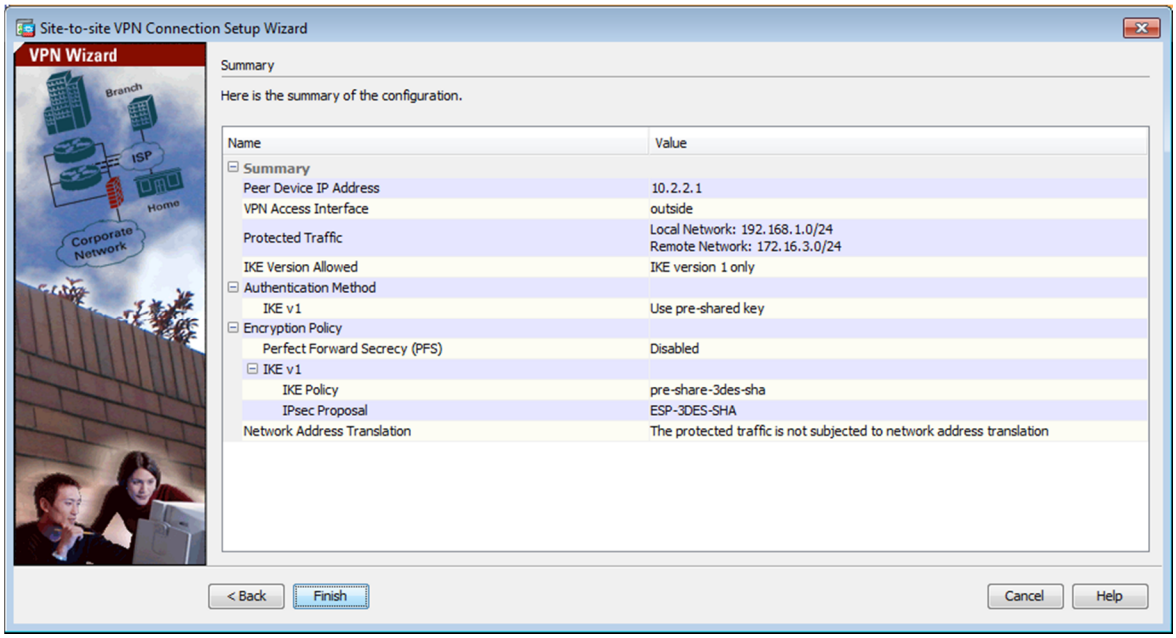
L'authentification est la tâche la plus importante que IKE accomplit, et il est le plus compliqué. Chaque fois que vous négociez quelque chose, il est important de savoir avec qui vous négociez. IKE peut utiliser une des nombreuses méthodes pour authentifier les parties à la négociation à l'autre. Nous avons en utilisant la méthode de clé partagé. Clé partagée - IKE utilise une technique de hachage pour assurer que seule une personne qui possède la même clé peut envoyer les paquets IKE.


Site-to-site VPN Connection Setup Wizard
Steps
1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary
Security
This step lets you secure the selected traffic.
Simple Configuration
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.
Customized Configuration
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.
IKE Version
Authentication Methods
Encryption Algorithms
Perfect Forward Secrecy
IKE version 1
Pre-shared Key:
Device Certificate:
-- None --
Manage...
< Back
Next >
Cancel
Help

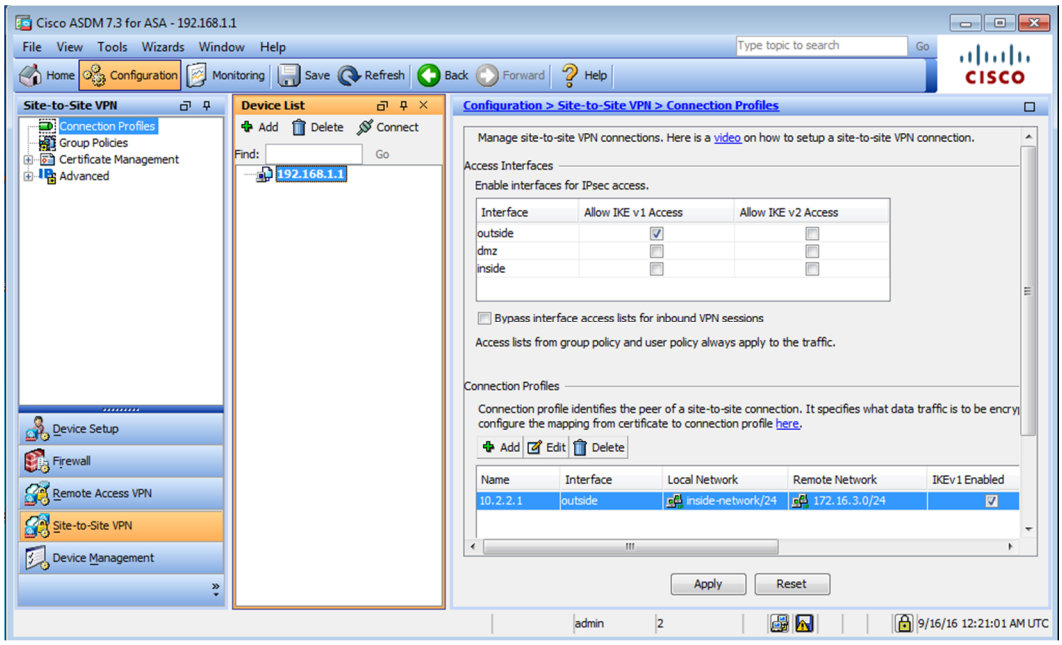

Site-to-site VPN Connection Setup Wizard
Steps
1. Introduction
2. Peer Device Identificatio
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary
Security
This step lets you secure the selected traffic.
Simple Configuration
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.
Customized Configuration
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.
IKE Version
Authentication Methods
Encryption Algorithms
Perfect Forward Secrecy
IKE version 1
IKE Policy:
pre-share-3des-sha
Manage...
IPsec Proposal:
ESP-3DES-SHA
Select...
< Back
Next >
Cancel
Help



Revoir le résumé de la configuration et de livrer les commandes à l'ASA

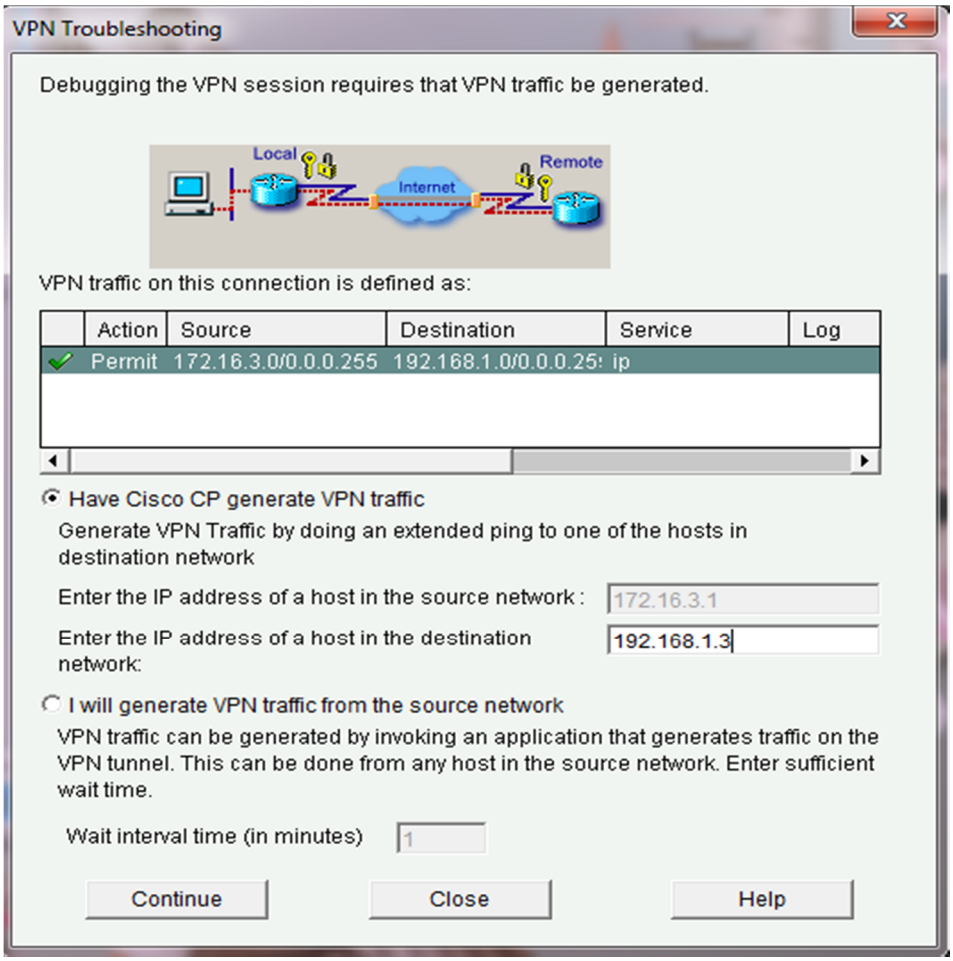


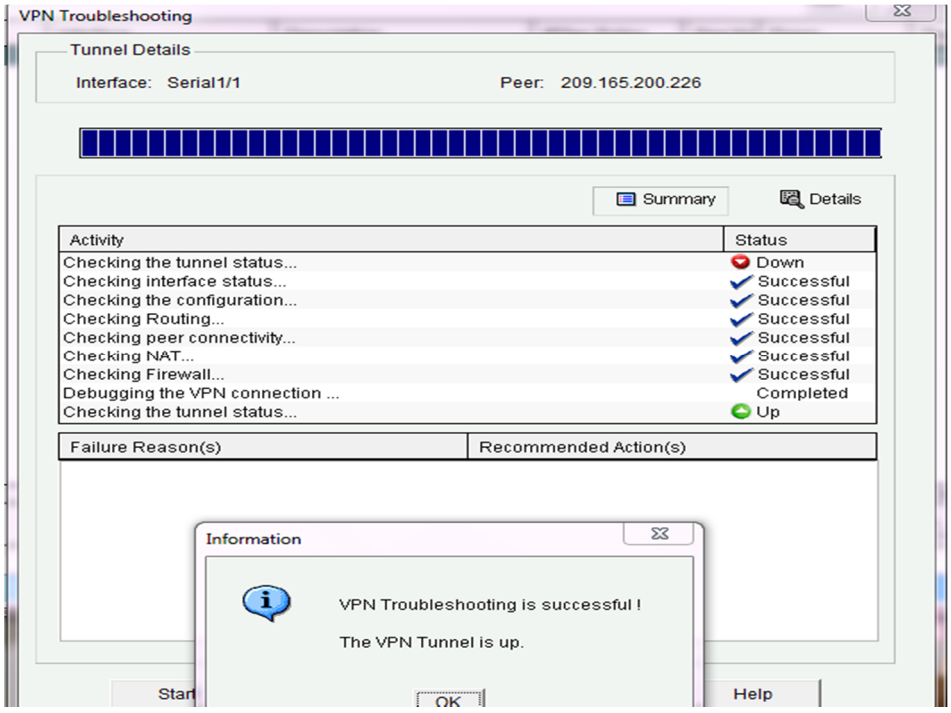
Vérifiez le profil de connexion VPN ASDM, cliquez sur Configurations > Site-to-Site VPN > Connection Profiles

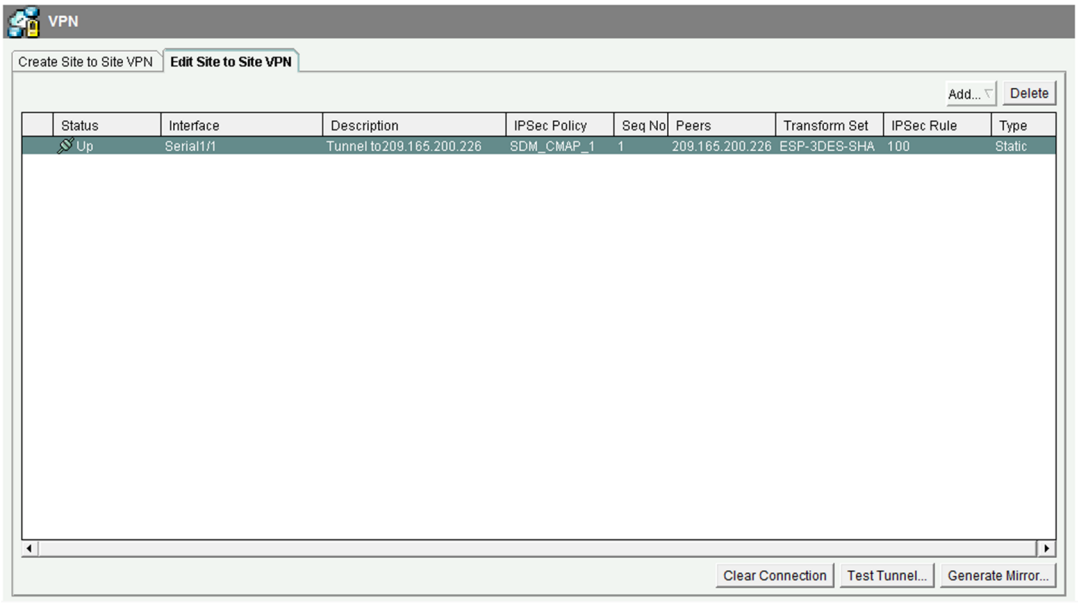


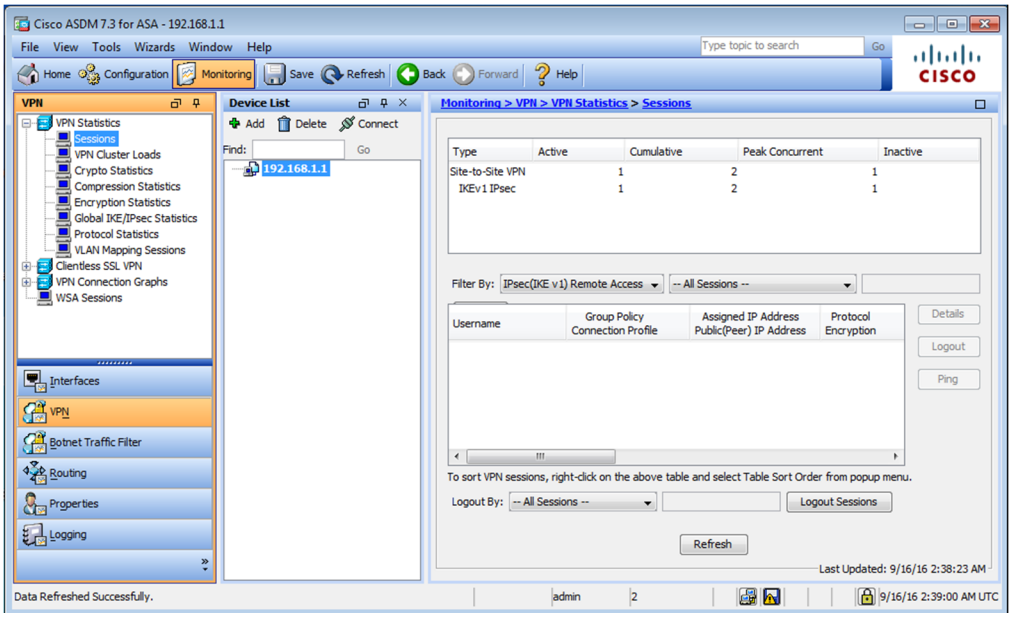
Tester la configuration VPN de R3 en utilisant CCP

Sur PC (pharmacie), utiliser CCP pour tester le tunnel VPN IPsec entre le R3 ISR et l'ASA. Cliquez sur Configure> Sécurity> VPN> Site to site VPN et sélectionnez Edit Site-to-Site VPN


VPN Troubleshooting
Debugging the VPN session requires that VPN traffic be generated.
Local
Internet
Remote
VPN traffic on this connection is defined as:
Action
Source
Destination
Service
Log
Permit 172.16.3.0/0.0.0.255 192.168.1.0/0.0.0.25: ip
Have Cisco CP generate VPN traffic
Generate VPN Traffic by doing an extended ping to one of the hosts in destination network
Enter the IP address of a host in the source network : 172.16.3.1
Enter the IP address of a host in the destination network: 192.168.1.3
I will generate VPN traffic from the source network
VPN traffic can be generated by invoking an application that generates traffic on the VPN tunnel. This can be done from any host in the source network. Enter sufficient wait time.
Wait interval time (in minutes) 1
Continue
Close
Help


VPN Troubleshooting
Tunnel Details
Interface: Serial1/1
Peer: 209.165.200.226
Summary
Details
Activity
Status
Checking the tunnel status... Down
Checking interface status... Successful
Checking the configuration... Successful
Checking Routing... Successful
Checking peer connectivity... Successful
Checking NAT... Successful
Checking Firewall... Successful
Debugging the VPN connection ... Completed
Checking the tunnel status... Up
Failure Reason(s)
Recommended Action(s)
Information
VPN Troubleshooting is successful !
The VPN Tunnel is up.
OK
Help





Conclusion

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de la mise place d'un réseau VPN site-à-site à la CNAS Tissemsilt. Nous avons en effet grâce à cette nouvelle technologie permis aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outils permettant d'implémenter les VPN, ce partage était possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs dit « distants » situés en dehors du réseau local. En effet, la mise en place de VPN site-à-site

permet aux réseaux privés de s'étendre et de se relier entre eux au travers d'internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basé sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

Conclusion Générale

Conclusion générale

A travers ce travail, nous avons pu simuler le déploiement d'un VPN au profit de la CNAS Tissemsilt afin d'assurer la sécurité de l'information partages avec les ces associes. Nous avons commencé par donner les concepts qui tournes autour de cette solution et de proposer un exemple de déploiement et sa configuration. Certes cette solution est la plus utilisée et est une référence. Mais le VPN est avant tout un concept et ne précise rien concernant ses moyens. Nous avons travaillé sur la plateforme matérielle de Cisco disponible sur le marché, et facile à configurer.

En effet, nous avons présenté ce travail en deux parties, à savoir la partie théorique qui était subdivisé en deux chapitres dont le premier a été consacrer à la sécurité des réseaux informatiques ; le second présente les firewall & les VPN (Virtual Private Network) ainsi leurs fonctionnements et les différents protocoles utilisés.

Dans la partie pratique, nous avons effectués une 'étude préalable dans laquelle nous avons présenté l'entreprise et nous avons fait l'analyse de l'existant, critique les faiblesses du système d'information de la CNAS à savoir leurs relations avec les pharmacies associées. Nous avons leur proposé une solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de la CNAS. Le reste du chapitre détaille la topologie et sa configuration.

Ainsi s'achève notre étude sur les VPNs. Néanmoins, le choix d'une solution basé sur la technologie VPN dépendra évidement de l'utilisation que vous en ferez et de l'investissement financier que vous y mettrez.

Références bibliographiques

Bibliographie

[1] http://www.commentcamarche.net/contents/995-protection-introduction-a-la-securite-des-reseaux, consulte le 18/03/2016.

[2] http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX%3A52001DC0298

[3] Thèse de Doctorat D'Anas ABOU EL KALAM « MODÈLES ET POLITIQUES DE SECURITE POUR LES DOMAINES DE LA SANTE ET DES AFFAIRES SOCIALES » 04 décembre 2003, pp.10, 3.

[4] https://www.information-security.fr/quest-ce-que-la-securite-de-linformation/

[5] Laurent Poinsot, Cours " Sécrypt ", UMR 7030 - Université Paris 13 - Institut Galilée.

[6] http://fr.slideshare.net/HossinMzaourou/1-rseaux-et-protocolesscuritpartie-1-v2

[7] mémoire, B.Nadjet « la configuration de base d'un firewall Cisco ASA 5550 » C.F.C Bab Ezzouar, 2008,2009, pp.33, 46, 54,63,64.

[8] http://aidesecurite.blogspot.com/2013/03/types-dattaques-dun-reseau.html, consulté le 23/03/2016.

[9] http://www.vulgarisation-informatique.com/attaques-informatiques.php

[10] https://support.microsoft.com/fr-fr/kb/129972

[11] http://www.lefigaro.fr/secteur/high-tech/2011/03/07/01007-20110307ARTFIG00537-comment-fonctionne-un-cheval-de-troie-informatique.php

[12] http://www.commentcamarche.net/contents/992-firewall-pare-feu

[13] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/ch-detection.html#S1-IDS-DEFN, consulté le 08/05/2016.

[WIKI] https://fr.wikipedia.org/wiki/Network_address_translation

[14] mémoire, Melle BELHARIZI Asmaà «La sécurité réseau, étude le cas de service Openvpn », 2012, 2013, pp.27.