Cisco PIX 515E Security Appliance

LE GUENNO Vincent & FRANCISCO Nelson

Le pare-feu Cisco PIX® 515E offre des services très perfectionnés de pare-feu à inspection d'état et de réseaux privés virtuels (VPN) IPsec. Conçu pour les petites et moyennes entreprises, ainsi que pour les agences de sociétés, le Cisco PIX 515E est doté d'une puissance de traitement renforcée et d'une accélération matérielle intégrée IPsec (pour certains modèles) ce qui procure des performances encore plus élevées pour répondre aux exigences de sécurité des accès haut débit

SOMMAIRE

I. Politique de sécurité

1. La politique de sécurité réseau

C'est une expression, un concept parfois un peu flou dont on entend parler lorsqu'il devient nécessaire de s'organiser.

Qu'est-ce qu'une politique de sécurité ? En avons-nous besoin ? La réponse est oui.

Une politique de sécurité est un document dans lequel se trouvent (s'il est bien élaboré) toutes les réponses aux questions qu'un ingénieur en charge d'une étude se pose lorsqu'il aborde le volet sécurité d'un projet informatique dont la réussite dépend entre autres de la prise en compte dès le début des contraintes de sécurité. (Nous parlons aussi d'exigences). Une politique de sécurité est donc un document confidentiel (largement diffusé toutefois) qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées par thèmes. La mise en pratique de la politique de sécurité est l'application des directives aux thèmes couverts par le projet.

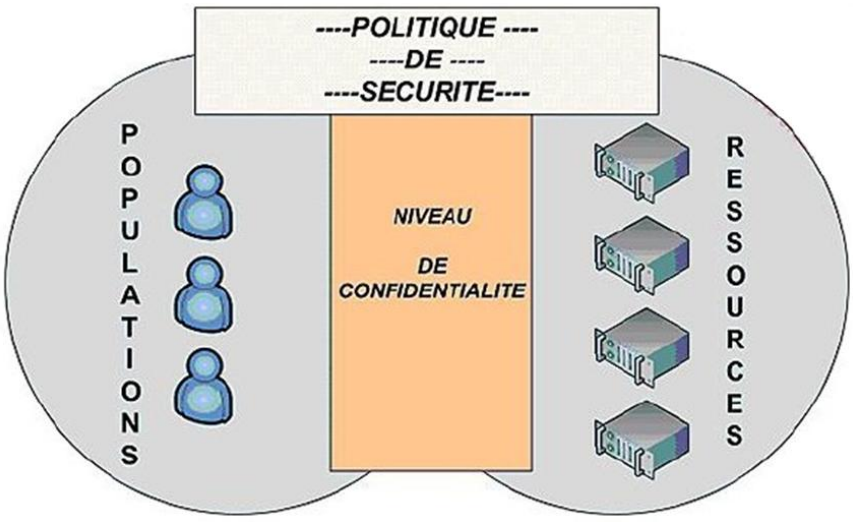
La thématique réseau dans la politique de sécurité englobe les recommandations pour l'exploitation des liens réseaux et des équipements. Les domaines abordés évoluent avec les intérêts économiques de l'entreprise et concernent entre autres :

- La gestion des accès au réseau et aux ressources (en relation avec la gestion des identités et des droits)
- la cryptographie ;
- la sécurité des équipements et des configurations ;
- la sécurité des systèmes terminaux.

Cependant, il serait illusoire et coûteux de vouloir à tout prix protéger l'entièreté d'une infrastructure informatique à la manière d'un Fort Knox. C'est pourquoi, la politique de sécurité s'applique à des degrés divers aux réseaux et aux équipements en fonction du niveau de confidentialité entre les populations et les ressources.

La conception de la politique de sécurité débute donc avec une classification du niveau de confidentialité des ressources et d'habilitation des populations. En fonction de cette classification, des règles sont émises et écrites dans le document. Ce travail est fastidieux mais ne revêt pas un caractère obligatoire. Il est envisageable de tout classifier à un niveau unique et ainsi de simplifier la politique de sécurité.

Le schéma suivant illustre cette notion.



Considérons un exemple simple :

Une population reçoit une habilitation de niveau confidentiel. Un ensemble de documents est également classé confidentiel.

La politique de sécurité indique :

- L'accès à des documents classés confidentiel n'est autorisé qu'aux personnels disposant d'une habilitation à ce niveau ou à un niveau supérieur ;
- La durée d'utilisation des documents classés de type confidentiel est enregistrée ;
- Les documents classés confidentiel sont uniquement accessibles en lecture seule ;
- Les documents classés confidentiel sont consultables à distance uniquement au travers d'un canal chiffré sur les réseaux de type LAN ou WAN.

Cet exemple illustre la relation entre une population, une ressource, un niveau de confidentialité et la politique de sécurité. Cette approche est primordiale dans la mesure où les réseaux d'entreprise ne sont plus limités à leurs frontières traditionnelles mais s'étendent vers les réseaux de leurs partenaires tout en recevant les connexions des employés en déplacement, couramment désignés comme "nomades".

Ces règles sont au-dessus de toute contingence technique. Une obligation de chiffrer les communications sur une liaison n'indique pas obligatoirement quel type de chiffrement sera utilisé dans la mesure où les techniques évoluent en permanence. Malgré tout, il est envisageable de le préciser à condition de veiller à la mise à jour périodique du document.

Complétons l'exemple précédent :

... au travers d'un canal chiffré sur les réseaux de type LAN ou WAN. Chiffrement en AES 256 sur les équipements du réseau avec authentification par certificats. Il est également possible, en complément de cette précision, que la mises-en œuvre du chiffrement relève d'une autre documentation définissant les standards en vigueur pour le déploiement. Enfin, la documentation technique précise la manière dont le protocole est configuré sur les équipements du réseau.

La rédaction d'une politique de sécurité est un travail sur mesure dont le document final est applicable à toutes les ressources et à toutes les populations de l'entreprise. Ce document est obligatoirement validé au plus haut niveau de la hiérarchie. Il est important de faire évoluer la politique de sécurité en fonction des liens qui ne manqueront pas de se tisser avec les partenaires et les clients. Une politique qui n'évolue pas perd tout son sens et devient peu à peu inapplicable. La littérature anglo-saxonne reprend à l'infini le concept du docteur DEMING « Plan, Do, Check, Act » ce qui dans notre langue se traduit par planifier, faire, vérifier, corriger. Ceci s'applique tout à fait à la politique de sécurité et constitue un véritable cycle d'évolution permanente.

La rédaction de la politique de sécurité n'en est pas pour autant une affaire de spécialistes extérieurs. Dans l'entreprise, il est recommandé de créer un groupe de travail autour de la rédaction de ce document.

2. Terminologie

Nous allons brièvement évoquer les quelques mots-clés qui sont largement repris dans la littérature informatique lorsque la sécurité est abordée.

Une ***vulnérabilité*** est une faiblesse le plus souvent cachée, touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de

passe vide ou trivial. L'expression faille de sécurité est également employée. Les moyens et les méthodes visant à éliminer les vulnérabilités sont faciles à mettre en pratique et requièrent :

- De se tenir au courant des vulnérabilités auprès du constructeur ;
- D'opérer une veille technologique à partir de sites Internet dédiés à la sécurité informatique ;
- De tester sur un environnement de validation les correctifs publiés ;
- De tester une procédure de retour en arrière ;
- D'installer le correctif ;
- D'observer le comportement de l'infrastructure de production.

Un ***risque*** est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tenterait de l'exploiter. Il existe d'autres définitions selon la norme à laquelle on se réfère. L'objectif de la sécurité informatique est de diminuer le plus possible le risque par tous les moyens disponibles.

Exploiter une vulnérabilité revient à utiliser cette faiblesse pour mettre à mal le dispositif visé par l'attaque. Concrètement, un **exploit** est un petit programme qui est lancé en direction de l'adresse réseau du système visé. Les équipements et les architectures informatiques comportent parfois de multiples vulnérabilités qui ne sont jamais révélées publiquement et ne sont donc jamais corrigées, en revanche les individus qui les ont découvertes les exploitent à leur guise pour leur propre compte.

Mettre à jour un système ou un équipement réseau consiste à appliquer les correctifs publiés par le constructeur et faisant suite à la révélation d'une vulnérabilité. En la matière, la prudence s'impose et avec elle toutes les séries de tests nécessaires afin de vérifier le bon fonctionnement de l'ensemble concerné une fois que les correctifs ont été appliqués. Quoi qu'il en soit, un suivi régulier des publications, des correctifs et des retours d'expérience sont fortement recommandés.

La politique de sécurité est élaborée en fonction d'une variable connue sous le nom d'**environnement**. L'environnement dans le domaine de la sécurité informatique est la définition de l'univers dans lequel évolue un système d'information. L'environnement, dans le domaine de la sécurité établit une carte des menaces potentielles qui planent sur un système d'information. Il s'agit au final de déterminer la portée de la politique de sécurité en fonction des menaces dont l'entreprise souhaite se prémunir. Par exemple, une entreprise décide d'instaurer des mesures de protection contre les menaces les plus courantes (et d'y consacrer un certain budget) mais décide de ne pas traiter les menaces émanant d'agences gouvernementales. La variable d'environnement est donc utilisée pour régler le degré de protection de la politique de sécurité face à une catégorie de menaces.

3. Cycle de la politique de sécurité

Comme nous l'avons évoqué, la politique de sécurité suit un cycle connu le nom de cycle de DEMING. Parcourons en les phases.

3.1 La planification (Plan…)

La planification commence avec la décision d'organiser formellement la sécurité. Elle consiste en un inventaire exhaustif des ressources à protéger et à la rédaction de directives pour chaque domaine concerné. À la fin de cette phase de planification, la politique de sécurité sera rédigée par le groupe de travail avec l'assistance éventuelle d'un consultant ayant une vue extérieure sur l'entreprise et son projet. Une fois écrite et relue, elle doit absolument être validée par la plus haute autorité afin qu'aucune contestation ne soit possible quant à son cadre d'application. L'étape suivante est sa publication sous la forme d'un document confidentiel mais

facilement accessible. Sa publication va de pair avec une large diffusion auprès des équipes en charge des projets et de l'exploitation de l'infrastructure informatique. Dès les premières phases, Il est primordial d'inclure les contraintes de sécurité qui jalonnent le déroulement d'un projet afin de ne pas risquer de l'interrompre s'il venait à prendre une voie contraire à la politique de sécurité en vigueur.

La politique de sécurité est déclinée en domaines fonctionnels qui représentent le modèle du système d'information de l'entreprise. Son organisation prend la forme de chapitres au sein desquels figurent les points à respecter. Citons par exemple, le chapitre sur la sécurité des systèmes d'exploitation, la sécurité des bases de données et la sécurité des communications qui nous intéresse au premier chef. Les divers intervenants lors de la phase de planification devront toujours avoir à l'esprit que leur texte servira de base aux travaux de sécurisation qui ne manqueront pas de se succéder. Ainsi la clarté et la précision des propos sont de mise lors de l'élaboration de la politique de sécurité.

3.2 La mise en œuvre (Do…)

La mise en œuvre de la politique de sécurité correspond point pour point à ce que nous venons de décrire précédemment. L'adhésion de tous au respect des règles décrites est le fondement d'une bonne prise en compte de la sécurité.

La politique de sécurité est principalement mise en œuvre lors des premières phases de progression d'un projet quel qu'il soit. Ce livre se cantonne à la sécurité des réseaux, mais le champ d'application de la politique de sécurité est vaste. La politique de sécurité est une référence qui doit être introduite dans chaque activité en relation avec le système d'information. À titre d'exemple, un projet partant d'une feuille blanche ou visant à modifier une partie de l'architecture doit impérativement se référer à la politique de sécurité. Ainsi, les spécifications techniques reprennent toutes les références utiles de la politique de sécurité afin de les intégrer naturellement. L'expérience montre que la sécurité si elle n'est pas prise en compte dès les prémices d'un projet peine par la suite à s'y intégrer. C'est la raison pour laquelle la diffusion de la politique de sécurité doit viser un large public et il est bon que chaque responsable de secteur (base de données, développement, réseaux) maîtrise la partie qui le concerne.

3.3 Le suivi (Check…)

Le suivi de la politique de sécurité consiste à s'assurer que les contraintes, imposées par le texte, sont prises en compte par les équipes en charge des projets et celles en charge de l'exploitation. Cela implique une présence systématique d'un représentant ou responsable de la sécurité aux réunions de suivi et un contrôle des processus d'exploitation en vigueur. Les menaces et les techniques évoluent perpétuellement et une politique de sécurité ne saurait, en aucun cas, rester figée. Le risque étant qu'elle ne soit tout simplement plus appliquée. Cette approche concerne donc le suivi de l'application de la politique de sécurité.

L'évolution de la politique est donc prise en compte dès sa définition par l'élaboration d'une méthode de révision accompagnée d'un facteur temps. Si l'entreprise surveille l'évolution des matériels et des technologies qu'elle met en œuvre, le suivi du processus de mise à jour de la politique de sécurité en sera grandement facilité. Toutefois, les menaces et les techniques de protection en perpétuelle évolution commandent de temps à autre une évolution de la politique de sécurité avant la date de révision planifiée. Ceci doit malgré tout rester exceptionnel car la politique de sécurité de par son mode d'élaboration balaye un large panel de mesures.

3.4 Agir (Act…)

Lorsque le besoin s'en fait sentir ou lorsque la date planifiée de révision approche, il s'agit après analyse et réflexion de modifier la politique de sécurité dans le but de l'adapter aux menaces qui pèsent sur les services qu'elle couvre ou sur de nouveaux services.

Prenons par exemple le cas des VPN SSL que nous aborderons lors du chapitre consacré aux pare-feu. Cette technique à part entière mérite de se voir consacrer un chapitre de la politique de sécurité car elle met en œuvre des fonctionnalités réparties sur de trop nombreux chapitres pour être exploitable en l'état. Sur ce point, il semble raisonnable d'anticiper l'évolution de la politique de sécurité pour ne pas avoir à gérer en même temps les questions inhérentes à un projet en cours avec celles qui ne manquent pas de se poser lors d'une refonte d'un tel document. L'équipe en charge du suivi de la politique de sécurité passe donc la main à celle en charge de son évolution et de sa révision. Une fois ce processus terminé, la politique de sécurité révisée est remise en service puis diffusée.

4. Conclusion

La politique de sécurité est un élément indispensable et préalable à toute entreprise (dans le sens du mot projet). Elle s'élabore à partir d'une réflexion portant sur la protection des ressources et le niveau d'accès des utilisateurs qui est lui-même fonction d'un niveau de confiance et de responsabilité. Ce document est le fruit d'un travail itératif et doit suivre, voire être en avance, sur l'évolution de l'architecture.

La politique de sécurité est mise à disposition des entités qui travaillent notamment à la planification ainsi qu'à la réalisation de projets. Ces dernières doivent impérativement saisir la nécessité de l'intégrer dès les premières phases en dérivant ses préconisations sous la forme d'exigences destinées à faciliter la rédaction d'appels d'offre ou l'élaboration de l'architecture choisie.

II. Cahiers des charges

1. Tâches à réaliser

- Configuration d'un serveur avec win2008 avec un service DNS, Active Directory et DHCP.
- Configuration d'un serveur win2008 avec les services WEB, FTP et Mail
- Configuration d'un serveur 2003 avec les services CSACS et autorité de certification
- Configuration de trois routeurs, deux simulant entre eux un réseau Frame Relay (Internet) et un troisième pour l'accès au site distant
- Configuration d'un PIX pour un accès sécurisé à internet (firewall, ACL, NAT/PAT)
- mise en place d'une DMZ avec serveur WEB, FTP et Mail.
- Accessibilité à la DMZ pour les clients extérieurs.
- Configuration d'un tunnel IPsec VPN de site à site.
- Configuration d'un tunnel reliant un client VPN au PIX

2. Contraintes

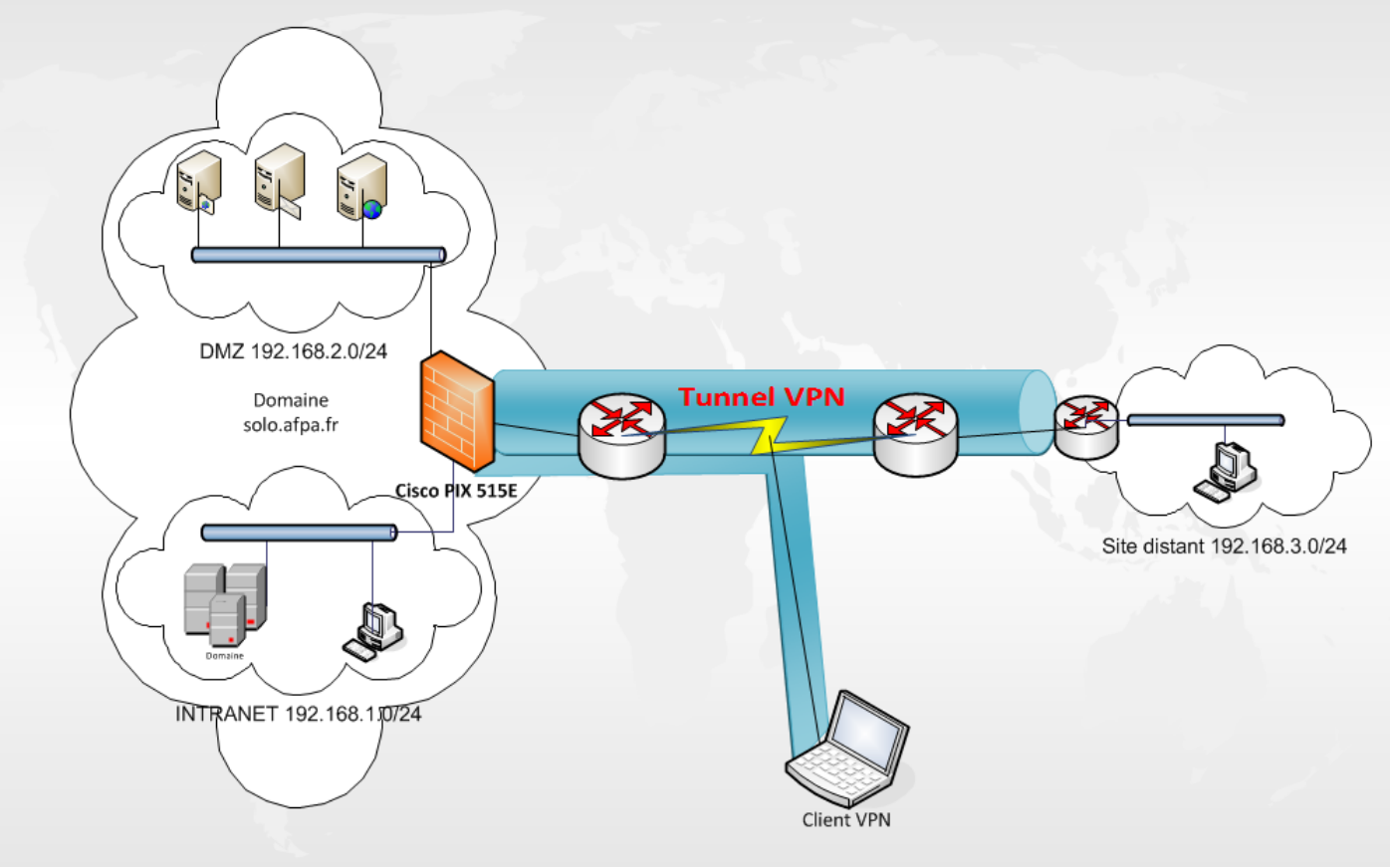
Le projet doit être réalisé et fonctionnelle dans un délai de 3 semaines. Comprenant la mise en place de la topologie, les tests, la capture de traces, et la rédaction d'un rapport. L'ensemble de la topologie doit tourner autour d'un PIX CISCO 515E.

3. Matériels utilisés

Nous utilisons pour mettre en place cette topologie :

- Deux postes fixes de la plateforme 4 avec win2008 en OS utilisé comme serveur.
- Deux ordinateur portable personnel recherche internet et virtualisation logiciel utilisé GNS3 et VMware, Windows Seven en OS, serviront de machine cliente.
- Un CISCO PIX 515E licence R, PIXOS 8.02
- Deux routeurs CISCO C2600 (2fast Ethernet un port série) Ios advsecurityK9-mz 12.3-7.T12
- Un routeur CISCO C2800 (2fast Ethernet, 4ports série) Ios adventreprisek9-mz.124-25b

4. Topologie de l'entreprise SOLO



III. Notions d'architecture réseau sécurisée

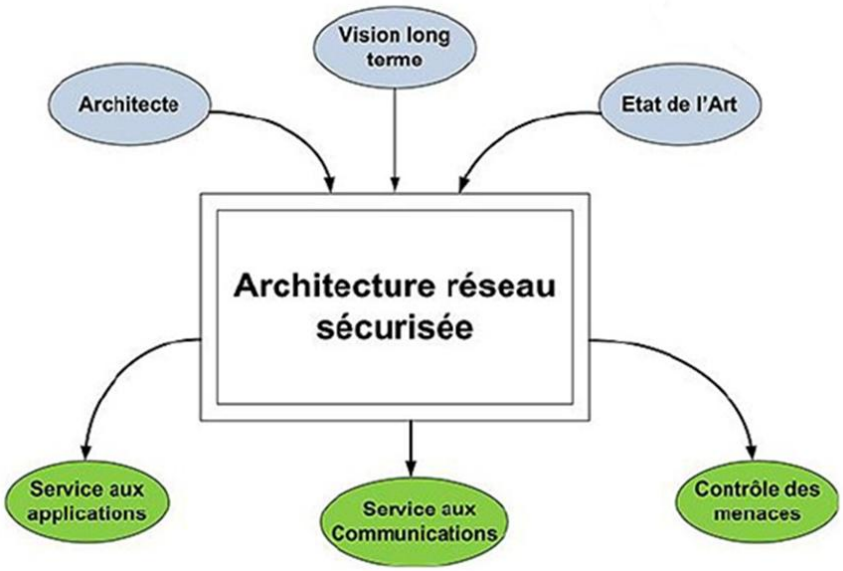
1. L'architecture réseau et sécurité

Un réseau est soumis régulièrement à de nombreuses évolutions et modifications qui sont le fruit d'une réflexion impliquant le travail du service d'architecture. Les entreprises les plus modestes ne sont pas dotées d'un tel service qui reste en règle générale l'apanage des groupes plus grands. Toutefois, la réflexion sur les tenants et les aboutissants d'une évolution relève de la même logique. Ce travail soulève principalement des questions concernant l'impact des modifications sur l'existant et la manière de procéder à l'intégration. Les tâches du service d'architecture s'il existe sont réparties autour de pôles liés aux spécialités qui composent le système d'information et nous y trouvons tout naturellement des spécialistes de la sécurité et des réseaux. Pour ces personnes, une connaissance approfondie de l'existant est impérative préalablement à toute étude d'évolution du réseau. Pour les entreprises de taille modeste, le responsable informatique fait office d'architecte et prend conseil auprès de ressources extérieures tout en restant maître de ses choix.

Les réseaux ont bénéficié ces dernières années d'avancées technologiques dans le domaine de la sécurité. Citons au passage les protections diverses et variées face à l'Internet, l'avènement de la téléphonie sur IP et des réseaux sans fil. De nos jours, de nombreuses sociétés ouvrent leur réseau à leurs partenaires dans le but de leur permettre d'accéder à des applications ou à des documents. Tout ceci soulève de multiples questions auxquelles les architectes du domaine réseau et sécurité sont sommés de répondre pour ne pas compromettre la bonne marche de l'entreprise.

Une approche méthodique consiste à scinder l'architecture globale en zones fonctionnelles recevant chacune un niveau de sécurité en fonction de sa position et de son rôle.

Les techniques que nous avons abordées lors des chapitres précédents vont ici être mise à contribution. À chaque zone de sécurité nous ferons correspondre un jeu de mesures techniques et organisationnelles.



Il est important de comprendre qu'au-delà de la protection du seul réseau, l'architecture de sécurité a pour objectif ultime la disponibilité des applications et des données. Le schéma montre en entrée (bulles supérieures) les composantes de l'architecture sécurisée et en sortie de celle-ci, les services fournis aux divers processus déployés par l'entreprise.

Nous allons présenter dans ce chapitre les zones de sécurité qui connectées les unes aux autres constituent le réseau sécurisé dans son entièreté. Nous allons mettre en correspondance pour chacune des zones les fonctions de sécurité abordées au cours des chapitres précédents.

2. La vision de Cisco

Cisco présente un concept nommé "the self-defending Network", le réseau qui se défend seul, le réseau à auto défense. Cette approche de la sécurité des réseaux s'étend à toutes les couches du modèle OSI et offre des services sécuritaires aux équipements, aux utilisateurs et aux applications. Cette offre est étroitement connectée à des systèmes de contrôle et de surveillance. Ce concept se décline en solutions c'est-à-dire en produits qui sont intégrés à l'architecture réseau. Il en résulte une architecture réseau sécurisée.

Les trois grandes familles de solutions introduites par Cisco sont :

- le contrôle des menaces pour les infrastructures, les équipements d'extrémité et la messagerie dont les produits entre autres englobent : les pare-feu, les systèmes de prévention et de détection d'intrusion, les contrôleurs d'accès au réseau, les agents de sécurité, les passerelles de messagerie ;
- la sécurité des communications dont les produits fournissent des services IP Sec ou VPN SSL : ce sont les routeurs et les pare-feu ;
- le contrôle d'accès au réseau avec l'équipement NAC (Network Access Control) qui contrôle la sécurité des équipements voulant se connecter au réseau.

Ces trois grandes familles de produits sont réparties sur des zones de sécurité qui correspondent aux zones de ségrégation habituelles. Pour mémoire, une zone de ségrégation correspond à un découpage fonctionnel du réseau de l'entreprise en régions. Ces régions sont connectées les unes aux autres avec un certain niveau de sécurité. Ce principe est diamétralement opposé à celui de réseau "à plat" ou schématiquement tous les équipements partagent le même réseau physique voire logique.

Cisco recommande donc de scinder le réseau en zones qui sont :

- L'infrastructure qui représente le réseau interne. Ce dernier étant à son tour divisé en trois zones.
- Les filiales
- Les réseaux longue distance (WAN). Il s'agit des zones d'interconnexions entre l'entreprise et ses filiales via des réseaux de données fournis par des prestataires de télécommunications (fournisseur de service Internet, opérateur Télécom)
- La zone DMZ
- les zones applicatives ou (Datacenter) qui comprennent les aires de stockage, les centres applicatifs et les services de téléphonie sur IP.

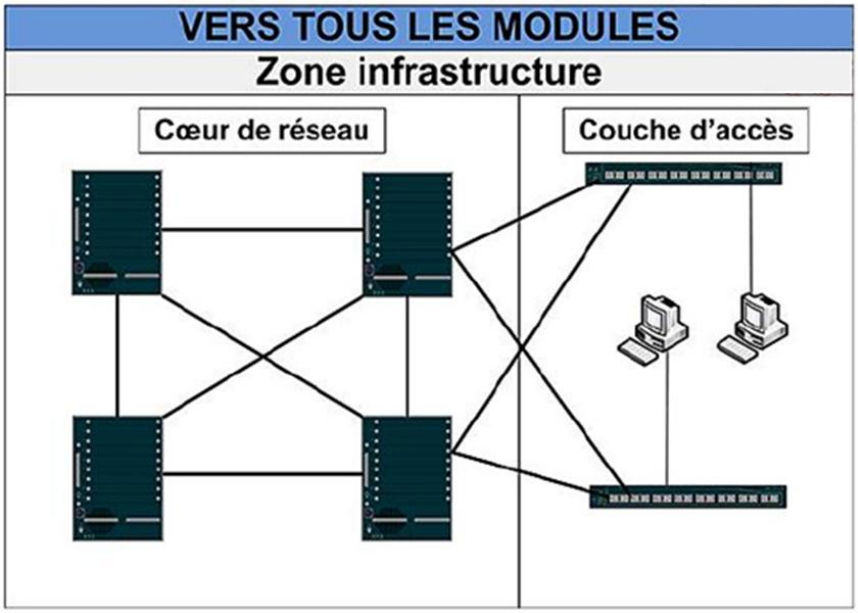
3. Découpage en zones de sécurité

Nous allons donner un aperçu du découpage qui permet d'affecter à chaque zone des fonctions de sécurité basées sur son rôle. Ce découpage fonctionnel facilite considérablement les tâches de surveillance et d'administration en ciblant les mesures de sécurité en fonction de la zone concernée. De plus, chaque zone obtient une certaine indépendance dans sa gestion ce qui ne remet pas en cause la gestion de la sécurité des autres zones qui l'entourent. Toutefois, il faut garder en mémoire que la sécurité d'une zone est étroitement dépendante de celle des zones qui l'entourent.

Quelques règles sont à observer en ce qui concerne la création et l'exploitation des zones de sécurité :

- Un équipement ou un hôte qui viendrait à changer de zone doit se conformer aux règles de sécurité de la nouvelle zone. Ceci est du ressort de la sécurité système et vise tout particulièrement les processus de renforcement (OS Hardening).
- Le trafic ne doit pas transiter entre deux zones dans le sens de la zone la moins sécurisée vers la zone la plus sécurisée.

3.1 La zone infrastructure



La zone infrastructure est la première des zones de sécurité à considérer car elle est au centre du système d'information. L'étendue de cette zone comprend, dans le cadre de ce livre, le cœur du réseau et la zone d'accès. Les documents publiés par Cisco ont introduit trois zones de base :

- Les zones d'accès sont à l'extrémité du réseau et comprennent les commutateurs sur lesquels sont connectés les postes de travail. Les zones d'accès sont dérivées en deux familles :
  - Les zones dans lesquelles sont fournis des accès filaires.
  - Les zones dans lesquelles sont fournis des accès sans fil.
- Les zones d'agrégation (aussi appelé distribution) sont constituées par le regroupement des zones d'accès et sont reliées au cœur du réseau avec un niveau de redondance.
- Le cœur de réseau est composé idéalement d'équipements rapides qui relaient le trafic d'une zone à l'autre.

Sur le schéma représentant la zone d'infrastructure, les zones d'accès et d'agrégation sont confondues. Cette architecture est conseillée pour les structures de taille moyenne.

Nous avons décomposé la zone infrastructure en trois sous zones en regard desquelles nous allons faire figurer un groupe d'équipement de sécurité ou de techniques évoquées dans les chapitres précédents.

La zone d'accès est essentiellement sécurisée autour du niveau 2. C'est ici qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. L'implémentation du protocole 802.1X est recommandée. Cette fonction est combinable avec les techniques qui limitent les communications une fois la connexion établie. Citons entre autres les VACL et les private ACL. Nous avons également à notre disposition toutes les mesures de protection contre les attaques par déni de service ou par usurpation de session que sont Dynamic ARP inspection et DHCP snooping.

La zone d'agrégation est située immédiatement à la suite de la zone d'accès à laquelle elle peut être combinée à des fins de simplification. Ici, l'architecture fait intervenir le routage entre les zones d'accès et le reste du réseau avec les limitations imposées par la politique de sécurité. Ce sont donc les techniques de sécurité au niveau 3 qui prévalent comme le filtrage inter VLAN, les ACL de tous types et bien sûr la protection des protocoles de routage.

Il va sans dire que la zone d'infrastructure bénéfice d'une sécurité physique renforcée eut égard à son rôle éminemment stratégique. Ici, la moindre interruption de service d'un lien, même prise en charge par la redondance, doit être remise en état le plus rapidement possible. En effet, la défaillance d'un lien bien que prise en compte par un dispositif de secours présente une prise de risque notable en cas de rupture du lien de secours. Ici, il est important de disposer d'un système d'alerte efficace en mesure de détecter tout défaut.

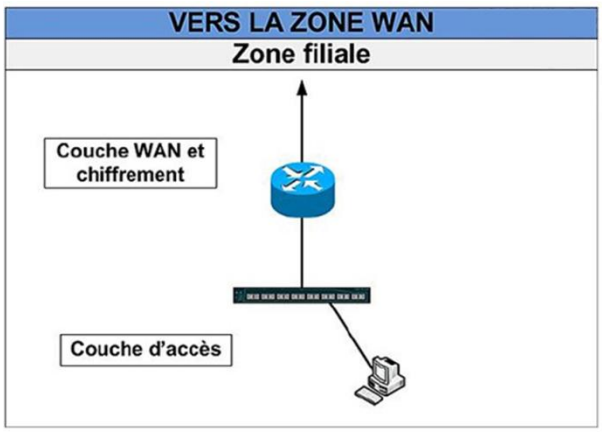
3.2 Filiales

Une filiale est une zone à part entière de l'entreprise et dispose en règle générale de moyens limités pour assurer sa propre sécurité. Ici, l'efficacité maximale est recherchée avec un nombre réduit d'équipements. La filiale est généralement traitée comme une extension du réseau local et à ce titre bénéficie de tous les services applicatifs. Toutefois, une filiale dispose rarement d'un cœur de réseau à part entière et s'appuie fréquemment sur un unique équipement multifonction qui a pour mission de gérer la sécurité et les connexions vers le site central. La sécurité d'une filiale (considérée comme une extension du réseau local) est sensiblement identique à celle des zones d'accès et d'agrégation. Ici, le protocole 802.1X est chargé d'assurer une stricte authentification des utilisateurs ainsi que la distribution de droits d'accès réseau sous la forme d'ACL reçues après le processus de connexion. Tout comme sur le réseau du site central, le panel des protections de la couche 2 est entièrement disponible pour opérer des séparations entre des zones aux degrés de confidentialité divers.

Les communications de la filiale vers le site central sont habituellement chiffrées. Cette mesure se justifie pleinement si le réseau Internet est voué à cette tâche d'interconnexion. Le protocole IPsec est tout naturellement indiquée pour accomplir cette tâche entre un équipement de la filiale (mutualisé) et un équipement dédié sur le site central. Bien entendu, des ACL opèrent une ségrégation entre le trafic à chiffrer et celui autorisé à transiter en clair. Ceci justifie amplement une étude préalable afin de déterminer les types de trafic à protéger.

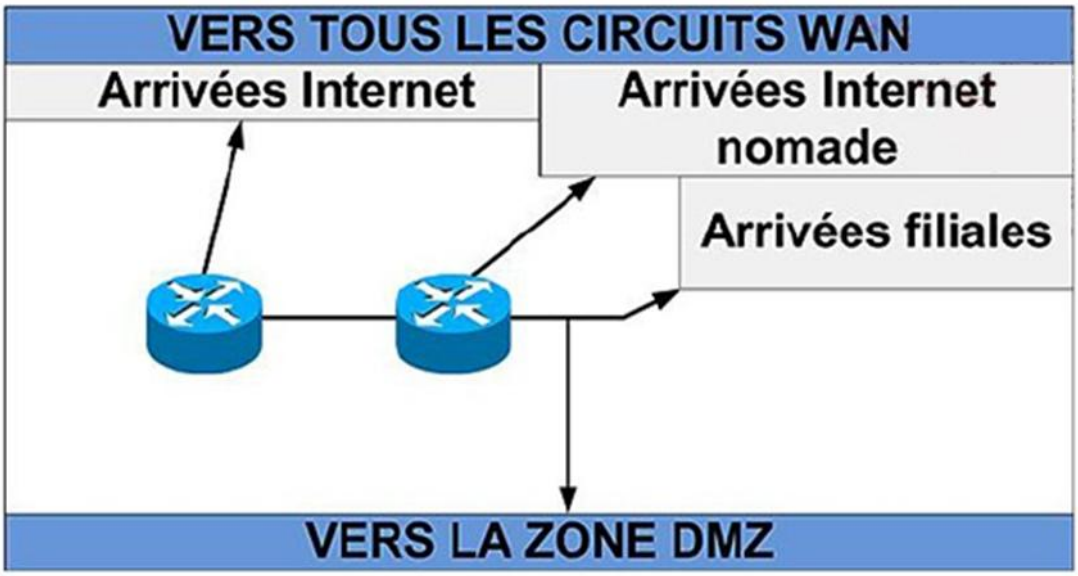
Cette notion est importante car les ressources consommées par les processus de chiffrement peuvent se révéler importantes. La zone filiale déploie sur l'équipement de connexion toutes les protections nécessaires vis-à-vis des réseaux extérieurs. Ceci s'applique tout particulièrement si l'Internet est utilisé pour la connexion vers le site central. Nous trouvons ici, les ACL dont le but est de filtrer les bogon networks et des mesures visant à limiter les tentatives de connexion frauduleuses utilisées à des fins de saturation.

La figure montre une zone filiale relativement simple pour laquelle deux équipements sont en service. Le commutateur Ethernet ainsi que le routeur sont parfois intégrés dans un équipement unique comme le pare-feu PIX.



3.3 WAN

La zone WAN est raccordée aux diverses interfaces qui la relient au monde extérieur.



Ainsi, un sous-réseau est attribué au recueil des collaborateurs nomades, un autre correspond aux arrivées Internet et un dernier est dédié aux filiales. La sécurité sur cette zone comprend les ACL qui écartent du réseau tous les trafics indésirables en provenance d'Internet et la protection logique des équipements. Ces ACL reprennent les bogon networks. Il est primordial de prendre les mesures de protection visant à limiter certains types de trafic en fonction de leur débit afin de se prémunir contre les attaques par saturation.

Les arrivées des personnels nomades s'effectuent sur les équipements dédiés que sont les concentrateurs VPN ou les pare-feu. Ces derniers embarquent des fonctions de chiffrement de type IPSEC ou SSL. Nous aborderons cette spécificité dans le chapitre consacré aux pare-feu. Chaque arrivée WAN est liée à une politique de sécurité relative aux technologies déployées qui portent par exemple sur la force du chiffrement, l'authentification des utilisateurs et les ACL spécifiques dont héritent les utilisateurs une fois qu'ils sont authentifiés.

La zone WAN assure également le recueil des connexions en provenance des filiales. Les liaisons sont établies sur des lignes louées ou sur Internet. En fonction du type de liaison, les mesures de protection diffèrent. Si la liaison utilise une voie louée, il est important de s'assurer auprès de l'opérateur de télécommunications de la bonne isolation entre le réseau d'interconnexion et les réseaux de l'opérateur voire ceux d'autres clients.

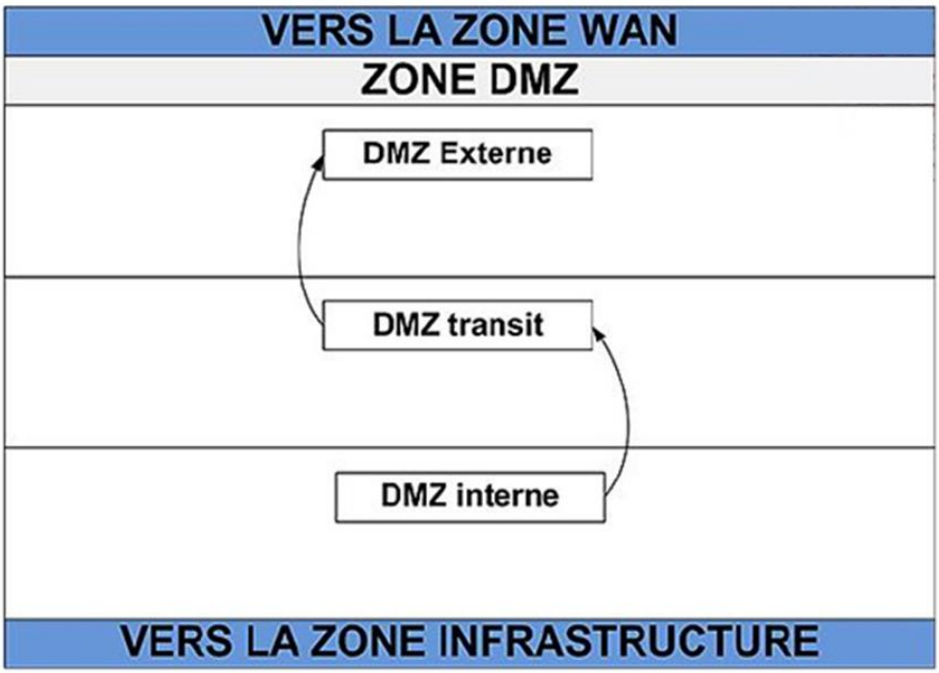
L'entrée de la zone WAN mérite une étroite surveillance des interfaces afin de visualiser toute irrégularité dans le trafic. Un pic ou un creux de trafic indiquent souvent l'imminence d'un problème plus grave.

Les pare-feu et les routeurs sont les principaux intervenants dans la zone WAN. Il est à noter que les deux fonctions peuvent figurer sur le même équipement.

3.4 La zone DMZ

Les DMZ (Demilitarized Zones) sont apparues avec la nécessité de mettre à disposition sur Internet des services applicatifs et de donner accès vers l'extérieur aux personnels de l'entreprise. Si l'on considère la fourniture de service, il est tout à fait inconcevable en termes de sécurité d'autoriser un accès interne à des clients échappant à tout contrôle. Ainsi naquit l'idée de positionner ces services sur une zone déportée formant écran entre le domaine public et le réseau interne de l'entreprise.

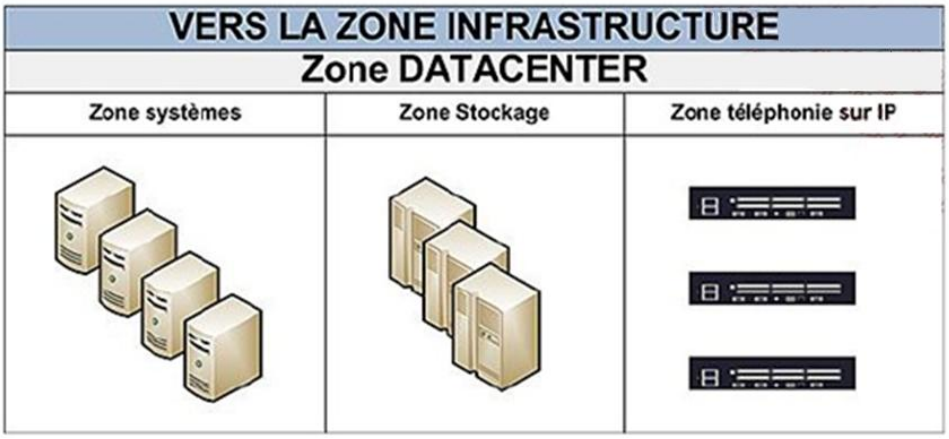
Une DMZ est donc une zone tampon située entre ce qui est considéré extérieur et ce qui est considéré intérieur à l'infrastructure centrale. Une DMZ dispose de divers dispositifs de filtrage réseau, mais aussi de relais applicatifs dans le but de ne rien laisser entrer directement au sein de l'infrastructure.



Les DMZ sont connectées par le haut à la zone WAN sur laquelle entrent les connexions en provenance de l'extérieur du réseau et par le bas à la zone d'infrastructure. Le schéma montre trois DMZ organisées comme suit : une DMZ externe, une DMZ de transit et une DMZ interne. Les deux zones d'extrémité hébergent des relais applicatifs (internes ou externes) qui sont habituellement des serveurs de messagerie, des relais HTTP (web proxies) et des relais de résolution de nom (DNS). Ces relais possèdent leur propre système de défense. La DMZ de transit quant à elle héberge opportunément des dispositifs de détection d'intrusion et de vérification de code comme par exemple les firewall XML de Cisco car le trafic n'est analysable qu'une fois qu'il est déchiffré. Les zones DMZ peuvent également héberger des applications autonomes dont les données proviennent de l'intérieur du réseau. Ici s'applique la règle du moindre privilège qui indique que le trafic ne saurait être initialisé d'une zone à faible niveau de sécurité vers une zone dont le niveau de sécurité est plus élevé. C'est pour cette raison que trois flèches sont dessinées sur le schéma, cela indique entre autres que les données présentes dans les DMZ proviennent de l'intérieur du réseau et qu'en aucun cas une entité de la DMZ (un serveur par exemple) ne va de son propre chef rechercher des données à l'intérieur de la zone infrastructure. Des exceptions existent toutefois afin de rendre visible de l'extérieur le réseau d'une entreprise. Il s'agit alors de laisser pénétrer dans les DMZ publiques le trafic en provenance de l'extérieur. Ces dérogations font l'objet de règles de sécurité dans les configurations des équipements et d'une étroite surveillance, elles sont de plus limitées aux premières zones, voire à une seule zone dite publique.

3.5 La zone Datacenter

La zone Datacenter héberge les serveurs centraux et des baies de stockage de grande capacité. La notion de Datacenter implique une concentration des moyens en un lieu unique dont la sécurité logique est l'une des composantes fortes. Un Datacenter combine en effet toutes les composantes de la sécurité et requiert un niveau de disponibilité à la hauteur de la confidentialité des informations qu'il héberge. Les mesures de protections associées au Datacenter vont de la protection physique des accès, à la redondance électrique en passant par la protection contre les incendies et la surveillance de la qualité de l'air ambiant pour n'en citer que quelques-unes. L'objectif du Datacenter est avant toute chose, la disponibilité de l'information.



Le Datacenter dispose de sa propre sécurité au niveau des systèmes d'opération et se repose sur la sécurité du réseau pour ne recevoir que des demandes sur les services qu'il offre. À titre d'exemple, une fraction du Datacenter fournissant des services de type http (WEB) attend uniquement des connexions sur le port 80. Celui-ci sera le seul autorisé en entrée sur ladite zone.

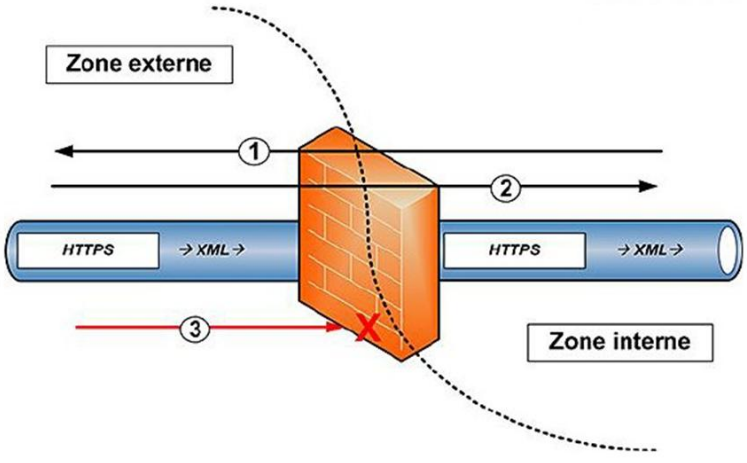
La sécurité au niveau réseau du Datacenter repose principalement sur le déploiement d'ACL qui vise à garantir que le trafic entrant autorisé correspond aux services fournis par le Datacenter. Il en va de même en sens inverse en s'assurant de la correspondance du trafic sortant avec les requêtes émises de l'extérieur.

C'est ici aussi la politique de sécurité qui dicte les choix en matière de sens d'initialisation du trafic. Le Datacenter étant une zone interne, le trafic qui y transite n'est habituellement pas chiffré. Cette disposition favorise le déploiement de dispositif d'analyse et de surveillance comme les sondes de détections d'intrusions finement ajustées sur les trafics caractéristiques de la zone. S'il est décidé de chiffrer le trafic, il conviendra de disposer de relais si la surveillance est souhaitée.

Une zone au sein du Datacenter se démarque, il s'agit de celle qui reçoit les services de téléphonie sur IP. Cette zone est idéalement isolée car la téléphonie est un service hautement stratégique tant par sa confidentialité que par la haute disponibilité qu'il nécessite.

4. Les pare-feu (Firewalls)

Le ciment entre les diverses zones que nous venons d'examiner est le pare-feu ou firewall en anglais. Les pare-feu ont pour rôle de filtrer le trafic en fonction des informations contenues dans les couches 3 et 4 du modèle OSI. L'évolution des pare-feu vers les modèles conservant l'état des sessions (modèles stateful) autorise un suivi du sens d'initialisation des connexions ce qui est très utile entre autres sur le modèle de chaînage des DMZ où chacune possède un niveau de sécurité qui lui est propre. Comme expliqué dans le chapitre sur la sécurité au niveau 3, la politique de sécurité impose que les flux soient toujours initialisés d'une zone dont le niveau de sécurité est élevé



vers une zone dont le niveau de sécurité est inférieur. Les contrôles d'état des connexions se charge de laisser entrer les paquets retours venant en réponse aux trafics initiaux.

Ce schéma montre un pare-feu laissant passer les trafics faisant partie d'une session autorisée et bloquant un trafic provenant d'une zone d'un faible niveau de sécurité et tentant de trouver un passage vers l'intérieur du réseau.

Les routeurs Cisco et les commutateurs de niveau 3 sont aptes à remplir le rôle de pare-feu entre les zones conçues par l'architecte de sécurité. Cependant, la limite des pare-feu est flagrante si l'on se place au niveau des couches dites hautes du modèle OSI. En effet un filtrage même avec mémorisation de l'état ne protège aucunement un service contre une attaque purement applicative c'est-à-dire exploitant une faille dans un programme donné. Nous entrons ici dans l'univers des attaques entre autres par injection de code malicieux d'un client vers une application.

Il est devenu indispensable de protéger les applications contre ce type de malveillance qui ne sont pas prise en compte par les firewalls classiques. Le déploiement (pour le protocole http) de relais (proxies) et de relais inversés (reverse-proxies) dotés de fonctions de sécurité répond parfaitement à cette exigence de filtrage entre les clients et les serveurs. Ces équipements embarquent de nombreux contrôles comme le filtrage d'URL et les scanners anti-virus.

L'insécurité croît aussi avec l'utilisation intensive de la messagerie et des services Web dont les flux transitent entre applications grâce à la souplesse du langage XML embarqué à l'intérieur des protocoles HTTP ou HTTPS. Comme le montre le schéma ci-dessus, les flux 1 et 2 sont gérés par le contrôle d'état et sont autorisés à transiter dans des directions en fonction des règles de sécurité (ACL CBAC). Le flux 3, inconnu est arrêté. Le trafic, bien qu'étant conforme aux règles de sécurité, véhicule potentiellement du code malveillant et l'équipement de filtrage si perfectionné soit-il n'y verra que du feu.

4.1 Les différents types de filtrages

4.1.1 Le filtrage simple de paquets (Stateless)

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sur le protocole de niveau 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des Access Control List (pour Cisco) ou Policy (pour Juniper).

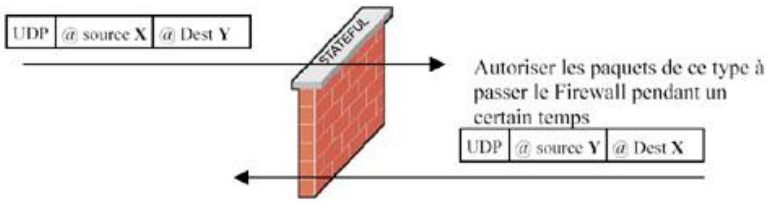
Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le Firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

Il est à noter que de définir des ACL sur des routeurs haut de gamme - c'est à dire, supportant un débit important - n'est pas sans répercussion sur le débit lui-même. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type IP Spoofing / IP Flooding, la mutilation de paquet, ou encore certaines attaques de type DoS. Ceci est vrai sauf dans le cadre des routeurs fonctionnant en mode distribué. Ceci permettant de gérer les ACL directement sur les

interfaces sans remonter à la carte de traitement central. Les performances impactées par les ACL sont alors quasi nulles.

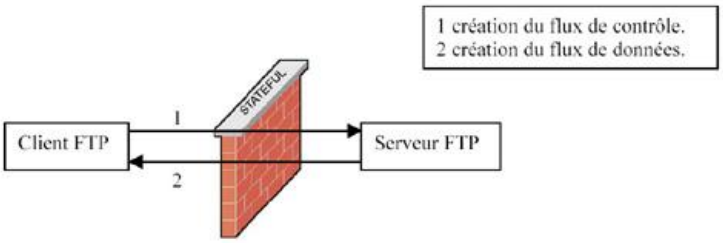
4.1.2 Le filtrage de paquet avec état (Stateful)

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.



Dans l'exemple précédent sur les connexions Internet, on va autoriser l'établissement des connexions à la demande, ce qui signifie que l'on aura plus besoin de garder tous les ports supérieurs à 1024 ouverts. Pour les protocoles UDP et ICMP, il n'y a pas de mode connecté. La solution consiste à autoriser pendant un certain délai les réponses légitimes aux paquets envoyés. Les paquets ICMP sont normalement bloqués par le Firewall, qui doit en garder les traces. Cependant, il n'est pas nécessaire de bloquer les paquets ICMP de type 3 (destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion TCP ou après l'envoi d'un paquet UDP.

Pour le protocole FTP (et les protocoles fonctionnant de la même façon), c'est plus délicat puisqu'il va falloir gérer l'état de deux connexions. En effet, le protocole FTP, gère un canal de contrôle établi par le client, et un canal de données établi par le serveur. Le Firewall devra donc laisser passer le flux de données établi par le serveur. Ce qui implique que le Firewall connaisse le protocole FTP, et tous les protocoles fonctionnant sur le même principe. Cette technique est connue sous le nom de filtrage dynamique (Stateful Inspection) et a été inventée par Checkpoint. Mais cette technique est maintenant gérée par d'autres fabricants.



Du point de vue des limites, il convient de s'assurer que les deux techniques sont bien implémentées par les Firewalls, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur HTTP pourra donc être attaqué impunément (Comme quoi il leur en arrive des choses aux serveurs WEB !). Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

4.1.3 Le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type HTTP sera filtrée par un processus proxy HTTP. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Au niveau des limites, le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau

7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100 % proxy pour les réseaux à gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

4.1.4 Le pare-feu identifiant

Un pare-feu identifiant réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et suivre l'activité réseau par utilisateur. Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple citer authpf (sous OpenBSD) qui utilise SSH pour faire l'association. Une autre méthode est l'identification connexion par connexion (sans avoir cette association IP=utilisateur et donc sans compromis sur la sécurité), réalisée par exemple par la suite NuFW, qui permet d'identifier également sur des machines multi-utilisateurs.

On pourra également citer Cyberoam qui fournit un pare-feu entièrement basé sur l'identité (en réalité en réalisant des associations adresse MAC = utilisateur) ou Check Point avec l'option NAC Blade qui permet de créer des règles dynamiques basée sur l'authentification Kerberos d'un utilisateur, l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patchs particuliers).

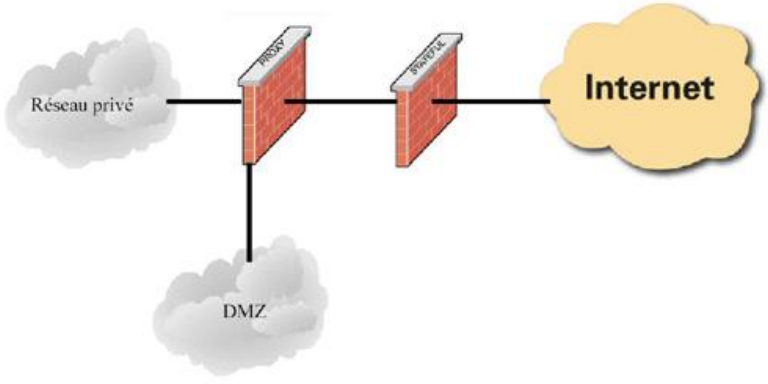
4.1.5 Le pare-feu personnel

Les pare-feu personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

4.1.6 Que choisir

Tout d'abord, il faut nuancer la supériorité du filtrage applicatif par rapport à la technologie Stateful. En effet les proxys doivent être paramétrés suffisamment finement pour limiter le champ d'action des attaquants, ce qui nécessite une très bonne connaissance des protocoles autorisés à traverser le firewall. Ensuite un proxy est plus susceptible de présenter une faille de sécurité permettant à un pirate d'en prendre le contrôle, et de lui donner un accès sans restriction à tout le système d'information.

Idéalement, il faut protéger le proxy par un Firewall de type Stateful Inspection. Il vaut mieux éviter d'installer les deux types de filtrage sur le même Firewall, car la compromission de l'un entraîne la compromission de l'autre. Enfin cette technique permet également de se protéger contre l'ARP spoofing.



5. Conclusion

L'architecture de sécurité du réseau est étroitement liée à l'architecture du réseau. Cette imbrication n'est pas sans soulever quelques problèmes lors des évolutions qui ne manquent pas de se produire dans les deux domaines. Les évolutions dans l'un ou l'autre domaine nécessitent une parfaite synchronisation ainsi qu'une parfaite documentation.

Les zones d'architecture que nous venons d'évoquer impliquent une division logique du réseau et le passage d'un réseau dit "à plat" à un réseau hiérarchisé. Ce remaniement s'accompagne opportunément d'une refonte du plan d'adressage IP et d'un renforcement du filtrage entre les zones.

Tout comme la politique de sécurité, l'architecture est en perpétuelle évolution car de nouvelles fonctionnalités et de nouveaux processus viennent enrichir les services dont l'entreprise bénéficie ou qu'elle offre à ses partenaires. Toutes ces ouvertures exposent le système d'information à de nouveaux risques et de nouvelles menaces lesquelles seront traitées pour un renforcement de la sécurité architecturale.

IV. Configuration du pare-feu Cisco PIX

1. Généralités et historique

Les pare-feu ou firewalls sont apparus et ont connu leur heure de gloire lorsque les réseaux d'entreprise se sont progressivement vus connectés à internet, ce réseau qui a toujours été perçu comme une menace. D'une manière générale, les firewalls protègent les réseaux internes des réseaux extérieurs et cet état de fait est toujours de mise aujourd'hui. Les architectures évoluant, les firewalls tout en restant à leur place originelle investissent l'intérieur du réseau. Les modes de travail tendent vers une étroite imbrication des acteurs qui gravitent autour du système d'information et il est devenu courant de fournir à des partenaires l'accès à des ressources internes. Cette situation entraîne un tel bouleversement dans les architecture de sécurité (et réseau) qu'une réflexion s'impose afin de redéfinir les nouvelles limites et les nouvelles règles de sécurité encadrant un trafic toujours plus dense et plus complexe au profit des applications qu'il véhicule.

Les firewalls trouvent toujours leur place dans cette redistribution des cartes et leurs capacités se sont au fil des années étoffées avec l'apparition des fonctionnalités devenues indispensables parmi lesquelles figurent l'authentification des utilisateurs, la surveillance des protocoles applicatifs et les VPN SSL (nouvelle fonctionnalité de l'ASA, dernier né des appliances Cisco, dont nous exposerons les évolutions par rapport à la technologie pare-feu éprouvée du PIX dans un prochain chapitre). Toutefois, les firewalls accomplissent toujours le filtrage des protocoles réseau qui est à l'origine de leur création.

Nous allons dans ce chapitre brosser un portrait des fonctionnalités proposées par les firewalls en débutant par leurs missions premières (le filtrage IP) jusqu'aux fonctionnalités plus avancées. Pour illustrer nos propos, nous avons construit une architecture d'entreprise autour du pare-feu PIX modèle 515E.

La gamme PIX a été originellement conçue par Brantley Coile et John Mayes de la société Network Translation Inc. Cette société a été achetée en 1995 par Cisco Systems qui a amené la gamme Cisco Secure PIX™ Firewall à la première place sur le marché des pare-feu autonomes, grâce à ses performances de pointe (ainsi que l'ont démontré les tests Firebench effectués par Key Labs, Inc.) et à sa position unique en tant qu'élément prépondérant dans les services sécurisés de bout en bout de Cisco.

La gamme Cisco Secure PIX, qui intègre des composants matériels et logiciels, assure un haut niveau de sécurité sans nuire aux performances des réseaux, et reste évolutive afin de pouvoir répondre à tous les besoins des clients.

Le marché des pare-feu a commencé à se développer avec l'apparition de réseaux privés virtuels et de petites et moyennes entreprises de plus en plus en nombreuses sur le marché Internet. Un nombre croissant de sociétés nécessitent aujourd'hui de puissantes fonctions de pare-feu à un prix abordable, pour mettre en œuvre des réseaux privés virtuels à l'échelle internationale et pour opérer une répartition au niveau des succursales régionales ou pour les PME qui recherchent la sécurité sans pour autant grever leur budget.

Le PIX 515 a été conçu pour répondre à ce besoin. Avec le PIX version 5.0 et toutes les versions ultérieures à la version 5.x, tous les équipements, y compris le PIX 515-R et le PIX 515-UR, prennent totalement en charge l'implémentation d'IPsec. Cette version permet au PIX de créer et/ou de suspendre des tunnels de réseaux privés virtuels entre deux PIX, entre un PIX et un routeur de réseau privé virtuel Cisco, et entre un PIX et un Cisco Secure VPN Client.

La gamme PIX s'est éteinte en 2008. Elle est remplacé par la gamme ASA (Adaptive Security Appliances) qui perpétue la tradition des équipements dédiés et autonomes. Cette nouvelle technologie fait la part belle aux techniques émergentes comme les VPN SSL qui ont pour vocation de remplacer les tunnels IPsec dédiés aux utilisateurs distants. Le but avoué de cette technologie est de facilité l'accès (sécurisé) aux applications publiées au format WEB à tous les employés et partenaires de l'entreprise en fonction de rôles préalablement définis et finement attribués. Le firewall

est devenu ainsi au-delà de sa fonction de filtrage réseau une véritable passerelle multi niveau assurant des services d'accès et de sécurité sur toute l'étendue du modèle OSI.

1.1 Produit de la gamme Cisco Pix Firewall

Modèle PIX	501	501-50	506E	515E-R	515E-UR	525-R	525-UR	535-R	535-UR
Marché	Petit bureau et bureau à domicile	Petit bureau et bureau à domicile	Succursale Bureau distant	Petite et moyenne entreprise	Petite et moyenne entreprise	Entreprise	Entreprise	Entreprise et prestataire de service	Entreprise et prestataire de service
Nb utilisateurs Par licence	10	50	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité	Illimité
Nb max de tunnel VPN	5	5	25	2000*	2000*	2000*	2000*	2000*	2000*
Connexions simultanées	3500	7.500	25.000	130.000	130.000	280.000	280.000	500.000	500.000
Processeur (MHz)	133	133	300	433	433	600	600	1000	1000
RAM (MB)	16	16	32	64	128	128	256	512	1024
Flash (MB)	8	8	8	16	16	16	16	16	16
Ports 10/100 intégré	1 10BaseT +Switch 4	1 10BaseT +Switch 4	2 10BaseT Full Duplex	2	2	2	2	0	0
Slot PCI	0	0	0	2	2	3	3	9	9
Port Eth Max	1+ 4 Switch	1+ 4 Switch	2	3	6	6	8	6	8
Redondance	Non	Non	Non	Non	Oui	Non	Oui	Non	Oui
Débit en clair (Mbps)	10	10	100	188	188	320	320	1700	1700
Context	Non	Non	Non	5	5	50	50	50	50
Débit 3DES	3	3	30	10	63	30	70	45	95
Version max IOS	6.3	6.3	6.3	8.x	8.x	7.x	7.x	7.x	7.x
Nb VLAN	0	0	2	10	25	25	100	50	150

*Utilisant une carte accélératrice VPN

2. Présentation du PIX 515E

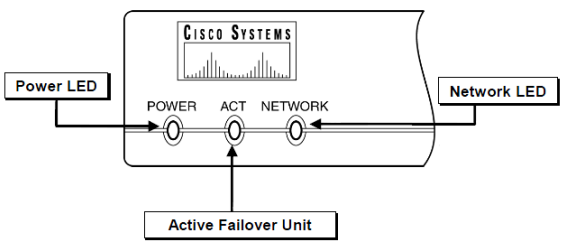
2.1 Aspect du pare-feu PIX

Face avant du PIX

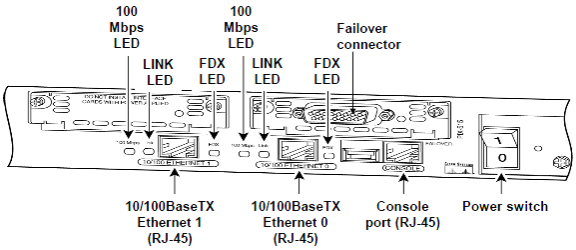
- Le logo du constructeur
- La gamme du produit sur lequel on travaille.
- Trois diodes

Ces diodes servent à définir différents statuts

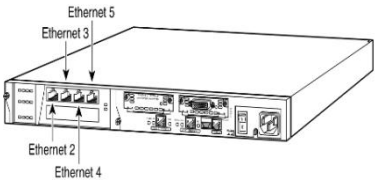
- POWER - Elle permet de savoir si l'appareil est en marche ou bien arrêté.
- ACT - Cette diode est utile si on utilise une architecture de redondance, c'est-à-dire plus d'un PIX. Si elle est allumée cela veut dire que le PIX est actif. Sinon le PIX est en veille ou la redondance n'est pas activée.
- NETWORK - Elle est active lorsqu'au moins une interface réseau du PIX laisse passer le trafic.



Face arrière du PIX

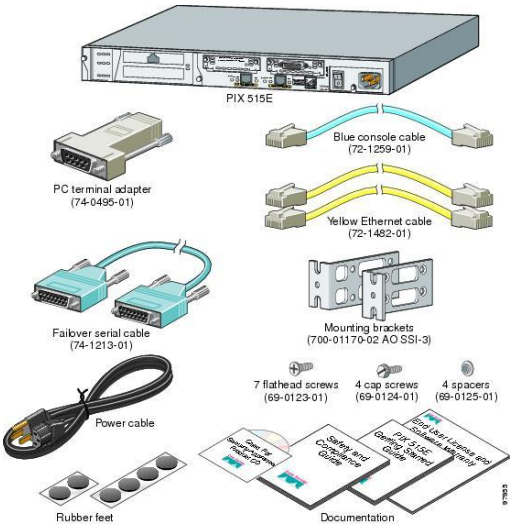


Version Unrestricted



Sur la face arrière du PIX, nous pouvons voir les différentes connectiques et les diodes qui représentent le statut des interfaces.

2.2 Comment fonctionne le PIX



Conçu pour les petites et moyennes entreprises, le pare-feu Private Internet Exchange (PIX) à l'avantage d'être modulaire, performant, économique et facile à installer et à utiliser.

Le châssis du Cisco PIX 515E peut intégrer jusqu'à six interfaces, ce qui en fait un choix excellent pour les sociétés qui requièrent une solution de sécurité rentable accompagnée d'un appui DMZ. Appartenant à la gamme PIX de Cisco, ce pare-feu apporte aux utilisateurs réseau des niveaux de sécurité, de fiabilité et de performance inégalés

Le pare-feu Cisco PIX 515E est conçu pour assurer un niveau de protection sans précédent. Il intègre le système d'exploitation PIX OS de Cisco. PIX OS est un système propriétaire renforcé capable d'éliminer les points de vulnérabilité et de faiblesse habituellement rencontrés dans les environnements d'exploitation généralistes.

Au cœur de ce système se trouve un dispositif de protection basé sur l'algorithme ASA (Adaptive Security Algorithm), qui offre un serveur de filtrage adaptatif orienté connexion avec blocage simultané contre les tentatives de piratage ou d'agression (DoS - Denial of Service).

Le PIX 515E est également une passerelle VPN complète capable de transporter en toute sécurité des données sur les réseaux publics. Qu'elles soient site à site ou à accès distant, les applications VPN sont protégées grâce à un cryptage des données (Data Encryption Standard) à 56 bits (DES) ou à 168 bits (3DES). Selon le modèle PIX 515E choisi, la fonctionnalité VPN est assurée par le système d'exploitation PIX OS de Cisco ou par une carte d'accélération VPN matérielle (VAC pour VPN Accelerator Card) intégrée qui procure des débits allant jusqu'à 63 Mbps pour 2 000 liaisons simultanées (tunnels) IPsec.

Le déploiement d'un second PIX en redondance pour le secours automatique garantit la disponibilité constante de votre système. Cette option de récupération (reprise sur incident) préserve en effet toutes les connexions simultanées grâce à une synchronisation automatique. Ce dispositif garantit, même dans le cas d'une défaillance du système, la poursuite des sessions en cours tandis que la commutation transitoire s'opère de manière totalement transparente pour l'utilisateur.

Ce pare-feu est disponible en trois modèles proposant différents niveaux de densité d'interface, de capacité de récupération et de débit VPN.

Résumé des performances
188 Mbps de débit en texte clair
63 Mbps de débit VPN 3DES à 168 bits (IPsec)
2000 tunnels VPN simultanés

De sortie	
Régime permanent	50 W
Crête maximale	65 W
Dissipation thermique maximale	410 BTU/h à pleine puissance (65W)

Caractéristiques techniques	
Processeur	433-MHz Intel Celeron
Mémoire RAM	32 MB ou 64 MB de SDRAM
Mémoire Flash	16 MB
Mémoire cache	128 KB niveau 2 à 433 MHz
BUS système	Monobus 32 bits, PCI 33 MHz

Dimensions et poids	
Hauteur	4,37 cm, 1 RU
Largeur	42,72 cm Standard montable en armoire
Profondeur	29,97 cm
Poids (une alimentation)	~ 4,11 kg

Conditions ambiantes	
En marche	
Température	-5º à 55ºC
Humidité relative	5 % à 95 % hors condensation
Altitude	0 à 3 000 m
Choc	1,14 m/s sinus 1/2
Vibration	0,41 Grms2 (3-500 Hz) aléatoire
Bruit acoustique	45 dBa max.
A l'arrêt	
Température	-5º à 55ºC
Humidité relative	5% à 95% hors condensation
Altitude	0 à 3000 m
Choc	30 G
Vibration	0,41 Grms2 (3-500 Hz) aléatoire

Extension	
Bus PCI	Deux PCI 32 bits/33 MHz
Mémoire RAM	Deux fentes DIMM 168 pin (64 MB : maximum supporté par le système d'exploitation PIX OS de Cisco)

Alimentation	
D'entrée (par source d'alimentation électrique)	
Plage de tension	100 V à 240 V CA ou 48 V CC
Tension nominale	100 V à 240 V CA ou 48 V CC
Intensité	~ 1,5 A
Fréquence	50 à 60 Hz, monophasé

Interfaces	
Ports réseau intégrés	Deux Fast Ethernet 10/100 (RJ-45)
Port console	RS-232 (RJ-45) 9600 bauds
Port récupération	RS-232 (DB-15) 115 Kbps (Câble Cisco spécial nécessaire)

Certifications	
Sécurité	UL 1950, CSA C22.2 Nº 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040
EMI	CFR 47 Part 15 Classe A (FCC), ICES 003 Classe A avec UTP, EN55022 Classe A avec UTP, CISPR 22 Classe A avec UTP, AS/NZ3548 Classe A avec UTP, VCCI Classe A avec UTP, EN55024, EN50082-1 (1997), marquage CE, EN55022 Classe B avec FTP, Cispr 22 Classe B avec FTP, AS/NZ 3548 Classe B avec FTP, VCCI Classe B avec FTP

2.3 Les différentes licences du PIX

Restricted (R)

Le PIX 515-R avec licence logicielle limitée est une solution d'entrée de gamme proposée par Cisco et destinée aux sociétés cherchant à déployer un dispositif sécurisé hautes performances avec des fonctionnalités de pare-feu de base. Il est suffisamment puissant pour supporter plus de 50 000 connexions simultanées avec un débit pouvant atteindre 170 Mbits/s. Prenant en charge jusqu'à trois interfaces Ethernet, le PIX 515-R-BUN représente une solution particulièrement économique pour les nombreuses petites entreprises qui ont choisi d'héberger leur site Web à l'extérieur de leur pare-feu ou chez un fournisseur de services Internet. Il convient également parfaitement aux sites distants ne nécessitant qu'une communication bidirectionnelle avec leur réseau d'entreprise et aux réseaux d'entreprise qui proposent tous leurs services Web sur leur pare-feu d'entreprise.

Unrestricted (UR)

Le PIX 515-UR avec licence logicielle illimitée comporte toutes les fonctionnalités du PIX 515-R-BUN, auxquelles viennent s'ajouter une fonction de correction automatique en cas de panne et jusqu'à six ports 10/100 Ethernet. Ces six ports supplémentaires sont destinés à des configurations de trafic plus puissantes, ainsi qu'à la prise en charge d'un DMZ protégé pour l'hébergement d'un site Web ou le filtrage des URL et la détection de virus. Conçu pour les moyennes entreprises, le PIX 515 UR supporte un débit d'environ 170 Mbits/s et plus de 100 000 connexions simultanées pour une protection rapide, fiable et à moindre coût.

Failover (FO) Fonction de correction automatique en cas de panne

La redondance du pare-feu est indispensable aux sociétés dont les connexions à Internet, à un intranet ou à un extranet constituent leur moyen unique et stratégique de communication en entreprise. Chaque panne de pare-feu entraîne une perte d'argent, d'opportunités ou de données critiques. Cisco a créé un nouveau logiciel de correction automatique en cas de panne pour le PIX 515 UR, permettant ainsi de résoudre ce problème en toute simplicité et à moindre coût. Ce logiciel fournit aux sociétés un deuxième pare-feu, spécialement conçu pour fonctionner exclusivement en mode de correction automatique en cas de panne, pour une modique somme

Les licences sont activés au moyen d'une clé d'activation d'une taille de 20 octets pour un PIX 7.x ou 16 octets pour une PIX 6.x et précédents.

2.4 Adaptive Security Appliance

ASA est l'algorithme de sécurité utilisé par les PIX Cisco.

Il se base sur un système de filtrage dit « stateful ». Cela signifie que le PIX utilise un système dynamique. Il maintient une table des connexions en cours permettant ainsi d'autoriser les paquets appartenant à une session créée préalablement.

Sans configuration explicite, ASA n'autorise que les liaisons intérieures vers extérieur. ASA est toujours en fonctionnement, surveillant le retour des paquets afin de s'assurer qu'ils sont valides. Il sélectionne de manière aléatoire des numéros de séquence TCP de manière à minimiser le risque d'attaque de numéro de séquence TCP.

ASA s'applique aux emplacements de traduction dynamique et de traduction statique. Vous créez des slots de traduction statique avec la commande « ***static*** » et des slots de traduction dynamique avec la commande « ***global*** ». Collectivement, les deux types de slots de traduction sont dénommés "xlates."

ASA suit les règles suivantes :

- Les connexions sortantes correspondent aux connexions établies sur une interface avec un haut niveau de sécurité vers une interface avec un niveau de sécurité bas. Par défaut ces connexions sont autorisées à moins qu'elles soient explicitement refusées.
- Les connexions entrantes correspondent aux connexions établies sur une interface avec un bas niveau de sécurité vers une interface avec un haut niveau de sécurité. Par défaut ces connexions sont refusées à moins qu'elles soient explicitement autorisées.
- Un paquet ne peut pas traverser le PIX sans connexion et état. L'état est supprimé au bout d'un certain temps d'inactivité.
- Tous les paquets ICMP sont refusés, sauf autorisation explicite avec les ACL (Listes d'accès)

Le pare-feu PIX gère les transferts de données UDP d'une manière similaire à TCP. Un traitement spécial permet à DNS, et certains protocoles de voix de travailler en toute sécurité. Le pare-feu PIX crée une information d'état de "connexion" UDP quand un paquet UDP est envoyé à partir du réseau Inside. Les paquets réponse résultant de ce trafic sont acceptés si elles correspondent aux informations d'état de connexion. Les informations d'état de connexion sont supprimées après une courte période d'inactivité.

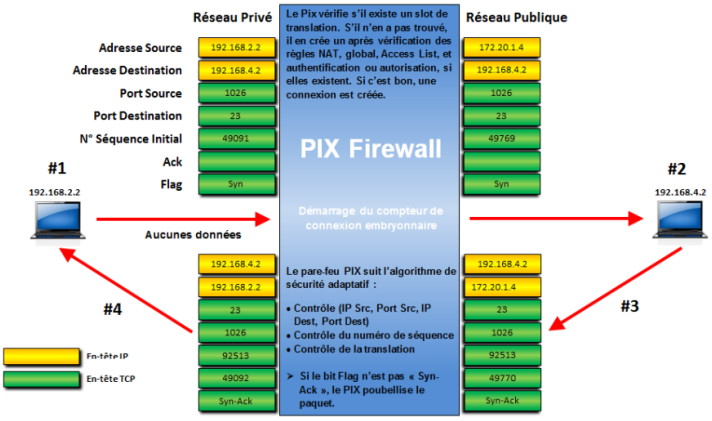
2.5 Passage des données à travers le PIX

Pour le passage des données dans le PIX, deux cas se présentent à nous.

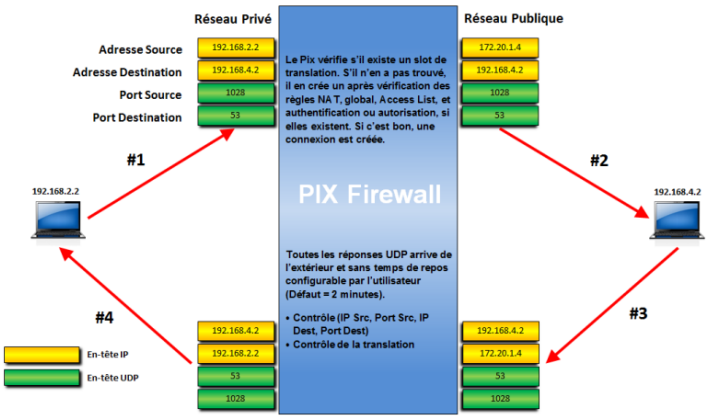
1. Les paquets arrivent sur une interface qui a un niveau de sécurité élevé.
2. Les paquets arrivent sur une interface avec un niveau de sécurité plus petit.

1. Dans le premier, ASA va commencer par vérifier si le paquet respecte les règles vues ci-dessus et dans le cas contraire le supprimer. Ensuite ASA regarde si une session n'a pas déjà été établie. Si ce n'est pas le cas, une nouvelle connexion est créée ainsi qu'un emplacement stocké dans la table avec les informations de translation. Une fois l'opération effectuée, ASA va modifier le champ IP du paquet en y mettant l'adresse globale, puis l'envoyer à l'interface destinatrice.

Initialisation TCP Inside to Outside



Transmission UDP Inside to Outside



L'adresse IP « 192.168.2.2 » correspond à la source et l'adresse globale « 172.20.1.4 » à l'adresse pour accéder à l'interface avec le niveau sécurité bas. Cette adresse globale est obtenue grâce au NAT (Translation d'adresse Réseau)

On peut utiliser soit la NAT statique, soit la NAT dynamique.

La NAT statique correspond à l'association de n adresses avec n adresses, soit une adresse interne pour une adresse externe. C'est utile par exemple pour associer une IP fixe internet à l'adresse privée d'un serveur de l'entreprise.

La Nat dynamique correspond quant à elle à l'association d'une adresse choisie dans un pool d'adresses à n adresses. La Nat dynamique est aussi connu sous le nom IP Masquering.

2. Dans le deuxième cas lorsqu'un paquet arrive sur une interface avec un niveau de sécurité bas pour aller sur une interface avec un niveau de sécurité haut, ASA va aussi vérifier si le paquet correspond aux attentes. Si le paquet passe toutes les règles avec succès, ASA enlève alors l'adresse de destination et insère à la place l'adresse interne.

Grâce à ces méthodes les adresses sont masquées et on augmente donc le niveau de sécurité.

2.6 Inspections des applications

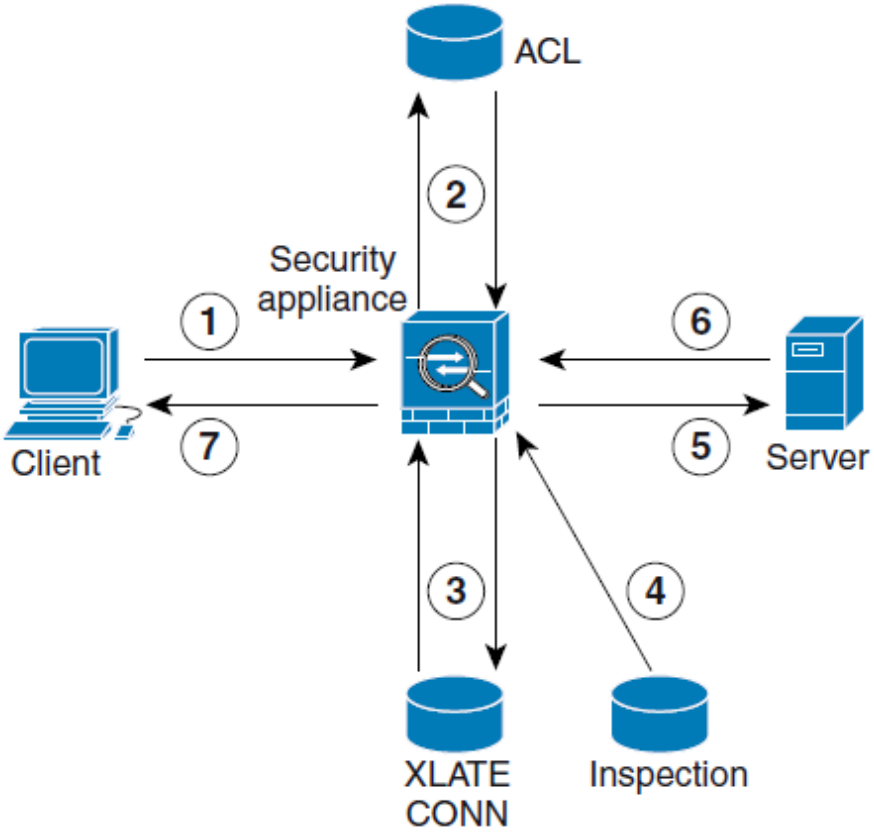
L'Adaptive Security Algorithm (ASA), utilisé par le pare-feu PIX pour l'inspection des applications stateful, assure la sécurité d'utilisation des applications et des services. Certaines applications nécessitent un traitement spécial par la fonction d'inspection des applications du pare-feu PIX. Les applications qui nécessitent la fonction d'inspections des applications sont celles qui intègrent des informations d'adressage IP dans le paquet de données utilisateur ou des canaux secondaires ouvert sur des ports attribués de façon dynamique.

La fonction d'inspection des applications fonctionne avec NAT pour l'aider à identifier l'emplacement des informations d'adressage intégrée. Cela permet à NAT de traduire ces adresses et de mettre à jour le checksum ou autre champs touchés par la traduction.

La fonction d'inspection des applications surveille également les sessions pour déterminer les numéros de port pour les canaux secondaires. De nombreux protocoles ouvrent des ports secondaire TCP ou UDP pour améliorer les performances. La première session sur un port bien connu est utilisée pour négocier les numéros de port attribué dynamiquement. La fonction d'inspection des applications surveille ces sessions, identifie les affectations de port dynamique, et permet l'échange de données sur ces ports pour la durée de la session spécifique.

ASA utilise trois bases de données pour son fonctionnement de base:

- Listes de contrôle d'accès (ACL) - Utilisé pour l'authentification et l'autorisation des connexions basées sur des réseaux, hôtes et services spécifiques (numéros de port TCP / UDP).
- Inspections - Contient un ensemble des fonctions d'inspection, statique et prédéfini, au niveau applicatif.
- Connexions (XLATE et tables CONN)- maintient l'état et tout autre informations sur chaque connexion établie. Cette information est utilisée par l'ASA et le proxy cut-through pour transférer le trafic de manière efficace dans les sessions établies.



Les opérations sont numérotées dans l'ordre où elles se produisent :

1. un paquet TCP SYN arrive au PIX Firewall pour établir une nouvelle connexion.
2. Le pare-feu PIX vérifie la base de données des listes de contrôle d'accès (ACL) afin de déterminer si la connexion est autorisée.
3. Le pare-feu PIX crée une nouvelle entrée dans la base de données de connexion (tables XLATE et CONN).
4. Le pare-feu PIX vérifie la base de données des inspections pour déterminer si la connexion nécessite une inspection au niveau applicatif.
5. une fois que la fonction d'inspection des applications ait achevé toutes les opérations nécessaires pour le paquet, le pare-feu PIX transfère le paquet à sa destination.
6. l'hôte destinataire répond à la demande initiale.
7. Le PIX Firewall reçoit le paquet de réponse, cherche la connexion dans la base de données de connexion, et transmet le paquet, car il appartient à une session établie.

La configuration par défaut du pare-feu PIX comprend un ensemble d’entrée d'inspection des applications qui associent les protocoles pris en charge avec les numéros de ports spécifique TCP ou UDP et qui permettent d'identifier toute manipulation nécessaire. La fonction d'inspection ne prend pas en charge NAT ou PAT pour certaines applications en raison des contraintes imposées par les applications. Vous pouvez modifier les affectations de port pour certaines applications, tandis que d'autres applications ont des affectations de ports fixes que vous ne pouvez pas changer.

3. Configuration de base du Cisco PIX 515E

3.1 Configuration par défaut du PIX

Les appliances de sécurité Cisco sont livrés par défaut avec une configuration d'usine qui leur permet un démarrage rapide. Cette configuration répond aux besoins de la plupart des environnements réseaux des petites et moyennes entreprises. Par défaut, l'appareil de sécurité est configuré comme suit :

L'interface interne est configuré avec un pool d'adresse DHCP par défaut

Configurez votre PC pour utiliser DHCP (pour recevoir automatiquement une adresse IP de l'appareil de sécurité), ou attribuer une adresse IP statique à votre PC en sélectionnant une adresse sur le réseau 192.168.1.0 (les adresses valides sont 192.168.1.2 à 192.168.1.254 avec un masque de 255.255.255.0 et la route par défaut 192.168.1.1.).

Cette configuration permet à un client du réseau interne d'obtenir une adresse DHCP de l'appareil de sécurité afin de s'y connecter. Les administrateurs peuvent alors configurer et gérer le dispositif de sécurité en utilisant ASDM

L'interface de sortie est configurée pour refuser tout trafic entrant par le biais de cette interface

Cette configuration protège votre réseau interne de tout trafic non sollicité

3.1.1 L'Adaptive Security Device Manager

L'Adaptive Security Device Manager (ASDM) est une interface graphique riche en fonctionnalités qui vous permet de gérer et de surveiller l'appareil de sécurité. De conception basée sur le web, il offre un accès sécurisé pour vous permettre de vous y connecter en toute sécurité de n'importe quel endroit en utilisant un navigateur web.

En complément des capacités de configuration et de gestion, ASDM simplifie et accélère le déploiement du dispositif de sécurité. Pour exécuter ASDM, vous devrez avoir une licence DES ou 3DES-AES. En outre Java et JavaScript doivent être activés dans votre navigateur web.

Nous avons décidé de ne pas trop s'attardé sur les configurations via ASDM, et avons préféré nous attaquer à la configuration du Cisco PIX 515E via l'interface de ligne de commande.

3.2 Configuration du Cisco PIX en mode CLI

Comme pour la plupart de ses produits, Cisco a muni le PIX d'interfaces physiques et logiques afin qu'un administrateur puisse se connecter et accéder à la ligne de commande. Après vous être connecter au PIX à l'aide d'un cordon console, un prompt devrait apparaitre. Essayez d'entrer en mode privilégié en entrant « enable », il ne devrait pas y avoir de mot de passe.

Pixfirewall > ***enable***

Password: ***<Enter>***

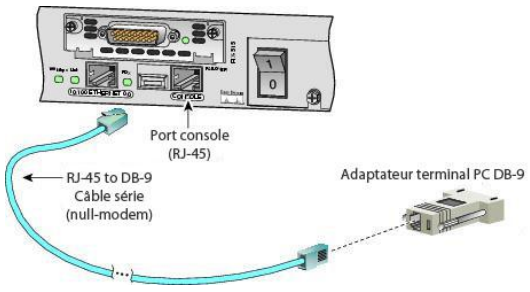
Pixfirewall # ***configure terminal***

Pixfirewall (config) # ***write erase***

Erase configuration in flash memory? [confirm] ***<Enter>***

[OK]

Pixfirewall (config) # ***reload***



System config has been modified. Save? [Y]es/[N]o: ***<N>***

Proceed with reload? [confirm]

Il est préférable quand on récupère un PIX d'effacer sa mémoire pour démarrer proprement avec une configuration vide. Nous avons eu plusieurs bugs concernant le mode interactif donc refusez l'invitation en tapant <Ctrl +Z>

Pre-configure Firewall now through interactive prompts [yes]? ***<Ctrl +Z>***

Après être repassé en mode configuration terminal, la première chose que nous allons faire, c'est de lui donner un nom.

Pixfirewall> ***enable***

Password: ***<Enter>***

Pixfirewall# ***configure terminal***

*Pixfirewall (config) #****hostname coruscant***

Coruscant (config) #

3.2.1 Configurations des interfaces

Pour configurer les interfaces du PIX nous devons leur assigner un nom et un niveau de sécurité :

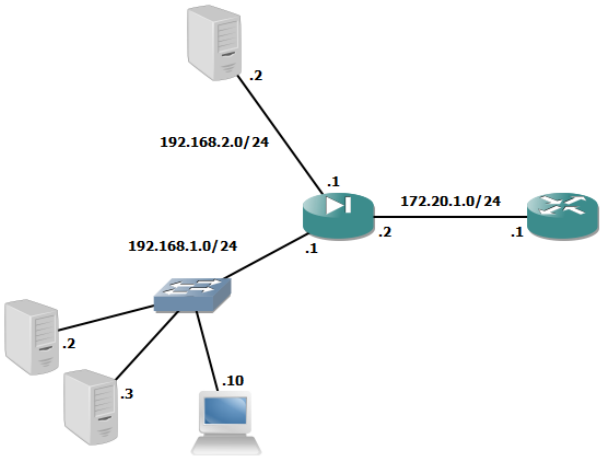
La commande nameif assigne un nom à chaque interface sur le PIX et indique son niveau de sécurité (excepté les interfaces intérieures et extérieures de PIX Firewall, qui sont déjà nommées par défaut). Les deux premières interfaces ont les noms par défaut *inside* et *outside*. L'interface *inside* a un niveau de sécurité par défaut de 100 ; l'interface *outside* a un niveau de sécurité par défaut de 0. Pour l'interface Ethernet 2 nous avons assignée un nom de *DMZ* avec un niveau de sécurité de 50.

La syntaxe pour la commande de nameif est comme suit :

nameif {hardware_id | vlan_id} if_name security_level

La commande interface identifie le matériel, fixe la vitesse du matériel, et active l'interface.

L'option *shutdown* neutralise une interface. Toutes les interfaces sont shutdown par défaut. Vous devez explicitement les activer en tapant la commande interface *no shutdown*.



coruscant(config)# ***interface ethernet 0***

coruscant (config-if)# ***nameif outside***

INFO: Security level for "outside" set to 0 by default.

coruscant(config-if)# ***ip address 172.20.1.2 255.255.255.0***

coruscant(config-if)# ***no shutdown***

coruscant(config-if)# ***exit***

coruscant(config)# ***interface ethernet 1***

coruscant(config-if)# ***nameif inside***

INFO: Security level for "inside" set to 100 by default.

coruscant(config-if)# ***ip address 192.168.1.1 255.255.255.0***

coruscant(config-if)# ***no shutdown***

coruscant(config-if)# ***exit***

coruscant(config)# ***interface ethernet 2***

coruscant(config-if)# ***nameif dmz***

INFO: Security level for "dmz" set to 0 by default.

coruscant(config-if)# ***security-level 50***

coruscant(config-if)# ***ip address 192.168.2.1 255.255.255.0***

coruscant(config-if)# ***no shutdown***

A tout moment, vous pouvez vérifier votre configuration à l'aide des commandes « *show* »

coruscant(config-if)# ***show interface ip brief***

Interface	*IP-Address*	*OK? Method Status*	*Protocol*
Ethernet0	*172.20.1.2*	*YES manual up*	*up*
Ethernet1	*192.168.1.1*	*YES manual up*	*up*
Ethernet2	*192.168.2.1*	*YES manual up*	*up*

coruscant(config-if)# ***show nameif***

Interface	*Name*	*Security*
Ethernet0	*outside*	*0*
Ethernet1	*inside*	*100*
Ethernet2	*dmz*	*50*

Comme dis précédemment le pare-feu ne laissera passer les données que si elles sont translatées. Pour cela, nous allons utiliser la commande « nat »

Network Address Translation (NAT) remplace l'adresse locale d'un paquet avec une adresse globale qui est routable sur le réseau de destination.

Lorsque les hôtes relié sur une interface qui a un niveau de sécurité élevé (ex : inside) désirent accéder à des hôtes relié à un niveau de sécurité plus faible (ex : outside), vous devez configurer NAT sur les hôtes inside ou configurer spécifiquement l'interface interne afin de contourner la translation.

La commande nat identifie les adresses locales pour la traduction en utilisant le NAT dynamique ou la traduction d'adresses de port (PAT). La commande global identifie les adresses globales utilisées pour la traduction sur une interface destination donnée. Each nat statement matches a global statement by comparing the NAT ID on each statement. Chaque déclaration nat correspond à une déclaration global en comparant les ID NAT sur chaque relevé. If you bypass NAT using identity NAT or NAT exemption, then no global command is required. Si vous ignorez

l'utilisation de NAT, en utilisant l'ID NAT (nat 0) ou la dérogation NAT (nat 0 access-list), aucune commande globale est nécessaire.

Nat [(local_interface)] id local_ip [mask [dns] [outside | [norandomseq] [max_conns [emb_limit]]]]

Nat [(local_interface)] id access-list acl_name [dns] [outside | [norandomseq] [max_conns [emb_limit]]]

Nat [(local_interface)] 0 access-list acl_name [outside]

coruscant(config)# ***nat (inside) 1 192.168.1.0 255.255.255.0***

coruscant(config)# ***nat (dmz) 1 192.168.2.0 255.255.255.0***

coruscant(config)# ***show run nat***
nat (inside) 1 192.168.1.0 255.255.255.0
nat (dmz) 1 192.168.2.0 255.255.255.0

coruscant(config)# ***global (outside) 1 172.20.1.5-172.20.1.254 netmask 255.255.255.0***

coruscant(config)# ***global (dmz) 1 192.168.2.5-192.168.2.254 netmask 255.255.255.0***

coruscant(config)# ***show run global***
global (outside) 1 172.20.1.5-172.20.1.254 netmask 255.255.255.0
global (dmz) 1 192.168.2.5-192.168.2.254 netmask 255.255.255.0

Nous avons décidé de ne pas translaté les adresses des réseaux internes et DMZ quand ils communiquent ensemble, pour cela nous avons utilisé la commande « static »

coruscant(config)# ***static (inside,dmz) 192.168.1.0 192.168.1.0***

coruscant(config)# ***static (dmz,inside) 192.168.2.0 192.168.2.0***

Après avoir ajouté une route par défaut, vérifions maintenant l'état de notre table de routage.

coruscant(config)# ***route outside 0 0 172.20.1.1***

coruscant(config)# ***show route***

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
** - candidate default, U - per-user static route, o - ODR*
P - periodic downloaded static route

Gateway of last resort is 172.20.1.1 to network 0.0.0.0

C 172.20.1.0 255.255.255.0 is directly connected, outside

C 192.168.1.0 255.255.255.0 is directly connected, inside
C 192.168.2.0 255.255.255.0 is directly connected, dmz
S 0.0.0.0 0.0.0.0 [1/0] via 172.20.1.1, outside*

Pour clore notre configuration de base, activons de serveur http du PIX et précisons qu'elles sont les hôtes qui sont autorisés à y accéder. Nous avons également renseigné les champs domain et dns du PIX. Pour sauvegarder votre configuration aidez-vous de la commande « write memory »

*coruscant(config)# **http server enable***

*coruscant(config)# **http 192.168.1.10 255.255.255.255 inside***

*coruscant(config)# **domain-name solo.afpa.fr***

*coruscant(config)# **dns domain-lookup inside***

*coruscant(config)# **dns name-server 192.168.1.2***

*coruscant(config)# **write memory***

Building configuration...

Cryptochecksum: ec445ac4 b6ac42d5 fddbc5ec 8a096673

1986 bytes copied in 0.780 secs

[OK]

3.2.2 Vérification de la connectivité

Du PIX vers les hôtes

coruscant(config)# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 msdom

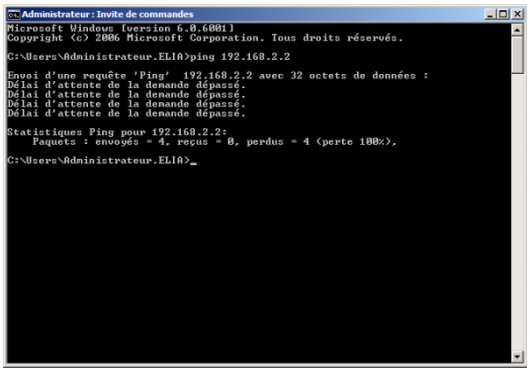
coruscant(config)# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms

coruscant(config)# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/20 ms

coruscant(config)# ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/14/30 ms

coruscant(config)# ping 172.20.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/22/40 ms

Entres les hôtes

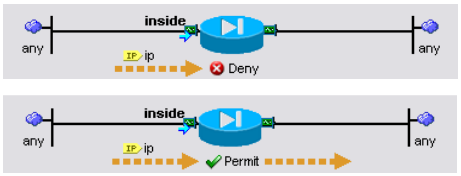


Comme expliqué plus haut (2.4) tous les paquets ICMP sont refusés par le PIX sauf autorisation explicite avec les ACL.

Toujours dans ce même paragraphe, nous avons vu que l'ASA suit des règles qui sont acquises par défaut par le PIX. Ces règles sont en fait des access-list implicites configurés sur le PIX sur chacune de ses interfaces.

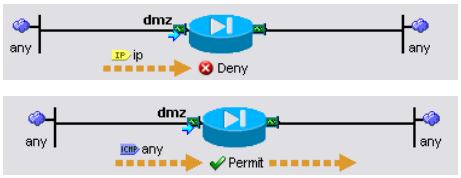
Interface Inside

No	Source	Destination	Service	Action
1	any	any	ip	Deny
2	any	Réseaux moins sécurisé	Ip	Permit



Interface DMZ

No	Source	Destination	Service	Action
1	any	any	ip	Deny
2	any	Réseaux moins sécurisé	Ip	Permit



Interface Outside

No	Source	Destination	Service	Action
1	any	any	ip	Deny

Revenons à nos problèmes de Ping. Pour autoriser les paquets à traverser le PIX, il va falloir écrire des access-list. Nous allons autoriser non pas tous les paquets ICMP mais seulement ceux qui résultent d'une réponse faite par un hôte relié à une interface de niveau de sécurité élevé. Pour les access-list qui seront positionnés sur l'interface outside, il n'y aura aucun danger. Par contre pour celles qui seront positionnés sur l'interface DMZ, pensez à recréer les access-list implicites (il ne peut y avoir qu'une seule access-list par interface, par direction t par protocole, règle des 3 P).

coruscant(config)# ***access-list dmz_access_in extended permit icmp any any echo-reply***

coruscant(config)# ***access-list dmz_access_in extended permit icmp any any time-exceeded***

coruscant(config)# ***access-list dmz_access_in extended permit icmp any any unreachable***

coruscant(config)# ***access-list dmz_access_in extended deny ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0***

coruscant(config)# ***access-list dmz_access_in extended permit ip 192.168.2.0 255.255.255.0 any***

coruscant(config)# ***access-group dmz_access_in in interface dmz***

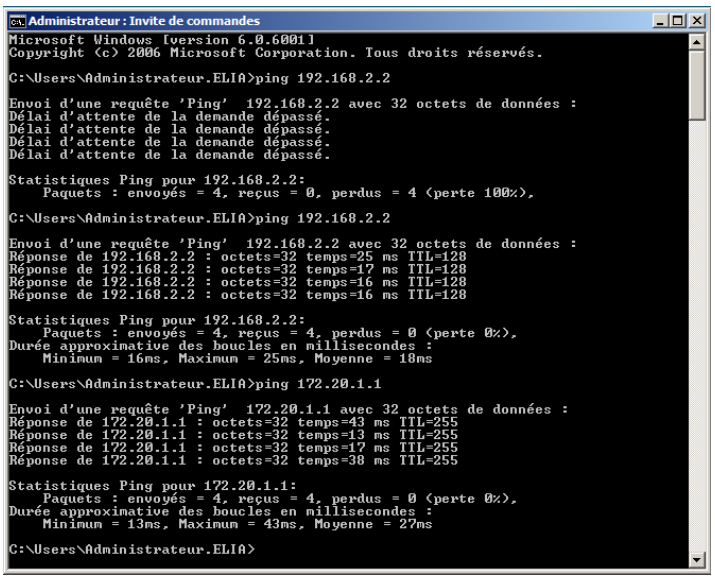
coruscant(config)# ***access-list outside_access_in extended permit icmp any any echo-reply***

coruscant(config)# ***access-list outside_access_in extended permit icmp any any time-exceeded***

coruscant(config)# ***access-list outside_access_in extended permit icmp any any unreachable***

coruscant(config)# ***show run access-list***
access-list dmz_access_in extended permit icmp any any echo-reply
access-list dmz_access_in extended permit icmp any any time-exceeded
access-list dmz_access_in extended permit icmp any any unreachable
access-list dmz_access_in extended deny ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list dmz_access_in extended permit ip 192.168.2.0 255.255.255.0 any
access-list outside_access_in extended permit icmp any any echo-reply
access-list outside_access_in extended permit icmp any any time-exceeded
access-list outside_access_in extended permit icmp any any unreachable

coruscant(config)# ***show run access-group***
access-group outside_access_in in interface outside
access-group dmz_access_in in interface dmz



Reprenons nos essais en testant la liaison entre un poste du réseau intranet et la DMZ, de même avec un hôte extérieur.

Nous pouvons voir que les Ping aboutissent.

3.2.3 Accès au serveur de la dmz pour les hôtes extérieurs

Nous allons commencer par donner un nom à notre serveur en utilisant la commande « name »

coruscant(config)# **name 192.168.2.2 webserver description Serveur2008 WEB et FTP**

coruscant(config)# **show run name**

name 192.168.2.2 webserver description Serveur2008 WEB et FTP

Ensuite nous allons configurer une translation static pour que le trafic provenant du serveur web ait toujours la même adresse d'origine sur l'interface extérieure du PIX, et nous configurerons une ACL pour permettre aux hôtes extérieurs de pouvoir accéder au serveur.

coruscant(config)# **static (dmz,outside) 172.20.1.4 webserver netmask 255.255.255.255**

coruscant(config)# **access-list outside_access_in extended permit tcp any host 172.20.1.4 eq www**

coruscant(config)# **access-list outside_access_in extended permit tcp any host 172.20.1.4 eq ftp**

coruscant(config)# **access-group outside_access_in in interface outside**

4. Configuration et installation AAA sur le PIX

4.1 Tour d'horizon d'AAA

- *L'authentification* : fournir d'une méthode pour valider l'identité les utilisateurs, comme par exemple le couple login/mot de passe, le chalenge réponse (comme CHAP) ou encore les mots de passe à usage unique (One Time Password)
- *L'autorisation* : contrôler à quel équipement ou service l'utilisateur accrédité a accès, à quelle zone du réseau il peut se connecter, etc…
- *Le comptage* (accounting) : pouvoir quantifier et qualifier les actions des utilisateurs authentifiés, à des fins de facturation ou d'audit par exemple.

Les deux protocoles plébiscités pour la communication entre un client et un serveur AAA sont RADIUS et TACACS+.

Radius

Le protocole RADIUS a été mis au point par Livingston Enterprises Inc (Lucent) et il est implémenté par de nombreux constructeurs de serveur d'accès. Il est utilisé par de nombreuses entreprises, notamment des fournisseurs d'accès et il est aujourd'hui considéré comme le standard pour supporter AAA.

Ce protocole s'appuie sur UDP (protocole de transmission de données sans connexion et sans mécanismes de fiabilité de transmission) pour transmettre les données sur le réseau.

Il combine les services d'authentification et d'autorisation.

Il souffre de quelques problèmes, telle qu'une limitation de l'encryption des mots de passe à 16 bits ou encore des problèmes de disponibilité ou de timeout sur les périphériques, lorsqu'ils tentent de contacter le serveur.

Il est généralement utilisé pour l'accès aux réseaux, par PPP ou VPN notamment.

Tacacs+

Le protocole TACACS+ a été mis au point par CISCO et c'est une amélioration des protocoles TACACS et Enhanced TACACS.

Il s'appuie sur TCP (protocole de transmission de données fiable, basé sur une connexion) pour véhiculer les données et crypte l'intégralité des informations avant leur transmission sur le réseau.

Ce protocole combine l'authentification, l'autorisation et l'accounting.

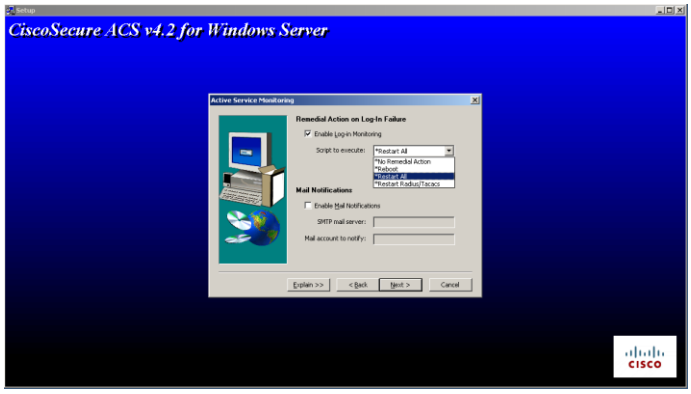
Il est généralement recommandé pour l'accès aux équipements.

4.2 Cisco Secure Access Control Server

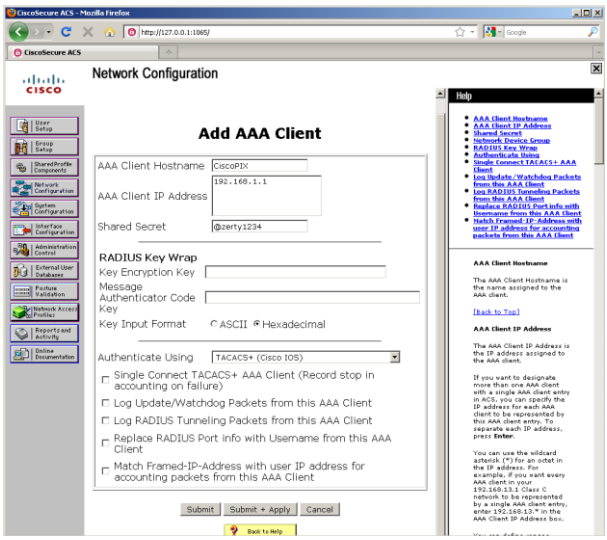
Le serveur de contrôle d'accès sécurisé est une solution centralisée d'identification sur le réseau qui simplifie la gestion des utilisateurs sur toutes les unités et les applications de gestion de sécurité Cisco. Souvent désigné sous le nom de services AAA (prononcé « triple A »). Composante essentielle de l'architecture Cisco IBNS (Identity Based Networking Services), elle élargit la protection des accès en associant l'authentification, l'accès utilisateur et administrateur, et le contrôle des politiques à partir d'un cadre centralisé d'identification de réseau. Elle offre ainsi une meilleure souplesse et une plus grande mobilité, améliore la sécurité et permet à l'utilisateur de réaliser des gains de productivité. Il y a deux composantes de base qui font ce travail : le serveur AAA (CSACS) et le client AAA (PIX). Le client AAA n'est pas un utilisateur ; c'est le dispositif qui permet à l'utilisateur de se connecter par son biais.

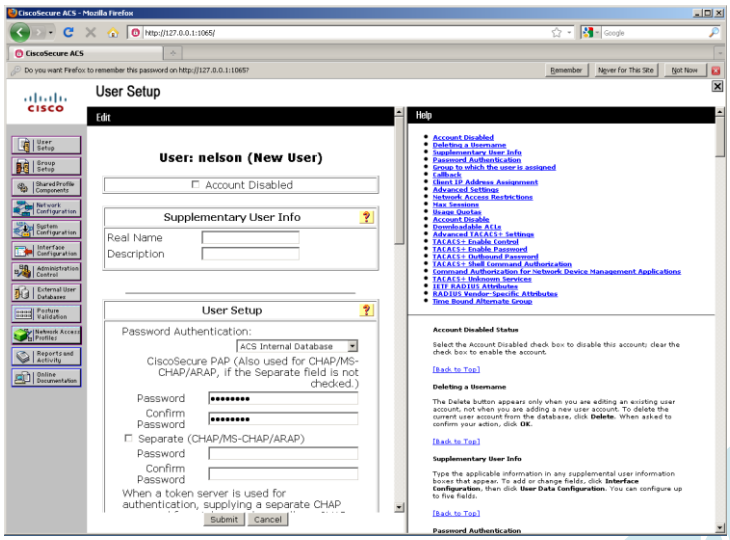
Installation de CSACS

Tôt dans le processus d'installation, une fenêtre vous demande de vous assurer que toutes les conditions nécessaires au bon fonctionnement de CSACS sont remplies. Le CSACS a l'option d'employer sa propre base de données pour l'authentification ou une base externe comme l'annuaire Active Directory. Ma configuration initiale emploiera la base de données locale. Plusieurs options avancées vous sont proposées à la suite, mais vous pouvez les laissez vide (vous pouvez y accéder après l'installation). Le prochain écran (montré ci-dessous) nous donne l'option d'avoir une surveillance des tentatives d'ouverture et permet l'exécution d'un script en cas de problème. Choisissez tous redémarrez. Après ces étapes accepter simplement les options par défaut pour le reste de l'installation.



La prochaine chose que je dois faire est de configurer mon serveur AAA pour travailler avec mon client AAA (PIX). D'abord je dois lancer la console (double-cliquez sur le raccourci « ACS Admin »). Les boutons sur la gauche vous permettent de configurer CSACS. Pour ajouter notre PIX, cliquez sur le bouton « Network Configuration ». une fenetre s'ouvre qui a une zone où je peux entrer mes informations et une autre plus grande avec une aide sensible au contexte. Cliquez sur « Add Entry » et renseignez le nom d'hôte, son adresse IP ainsi qu'une clef d'identification. Cliquez sur « Submit +Restart ». Maintenant je dois ajouter les utilisateurs (bouton « User Setup » sur la gauche). Après ouverture de la fenetre, entrez le pseudo désirez et cliquez sur « Add/Edit ». Puisque je n'ai pas besoin de mot de passe différent pour PAP et CHAP, je ne cocherais pas la case « Separate ». C'est tout ce que nous devons faire pour permettre l'authentification de base sur le CSACS pour chaque utilisateur. La dernière étape est de configurer le PIX pour employer CSACS pour l'authentification.





Modifier la configuration du PIX pour utiliser CSACS

D'abord je vais configurer le PIX pour utiliser le serveur AAA. Le PIX peut avoir jusqu'à 16 groupes indépendant de serveurs AAA lui permettant d'exécuter des fonctions AAA différentes basées sur le type de trafic (Telnet, VPN, http, etc.) ou la direction (inside, outside).

Chaque groupe peut avoir jusqu'à 16 serveurs AAA différents configurer comme membres pour tenir compte de la redondance et du Failover. Ce qui nous donne jusqu'à 256 serveurs TACACS+ ou RADIUS, au total, entre les deux protocoles.

Maintenant je veux créer un group AAA appelé « mytacacs » et le faire utiliser le serveur AAA 192.168.1.3 connecté derrière mon interface inside. @zerty1234 est la clé secrète renseigné dans ma configuration AAA (voir ci-dessus)

coruscant(config)# ***aaa-server mytacacs protocol tacacs+***

coruscant(config-aaa-server-group)# ***max-failed-attempts 4***

coruscant(config-aaa-server-group)# ***exit***

coruscant(config)# ***aaa-server mytacacs (inside) host 192.168.1.3***

coruscant(config-aaa-server-host)# ***timeout 5***

coruscant(config-aaa-server-host)# ***key @zerty1234***

coruscant(config-aaa-server-host)# ***exit***

coruscant(config)# ***access-list inside_authentication extended permit tcp 192.168.1.0 255.255.255.0 any eq www***

coruscant(config)# ***access-list outside_authentication extended permit ip any 192.168.1.0 255.255.255.0***

coruscant(config)# ***access-list outside_authentication extended permit ip any 192.168.2.0 255.255.255.0***

coruscant(config)# ***aaa authentication match inside_authentication inside mytacacs***

coruscant(config)# ***aaa authentication match outside_authentication outside mytacacs***

Authentification de l'accès aux consoles

Pixfirewall(config)# ***aaa authentication [serial | enable | telnet] console group_tag***

Définissons une méthode d'accès aux consoles qui exige l'authentification

coruscant(config)# ***aaa authentication enable console mytacacs***

coruscant(config)# ***aaa authentication telnet console mytacacs***

coruscant(config)# ***aaa authentication enable serial mytacacs***

Changement des Timeouts de l'authentification

Pixfirewall(config)# timeout uauth hh:mm:ss [absolute|inactivity]

- Poser l'intervalle de temps avant que les utilisateurs seront obligés de s'authentifier à nouveau.
  - Absolu: Temps de l'intervalle commence au login de l'utilisateur
  - L'inactivité : Temps de l'intervalle pour les sessions inactives sessions (pas de trafic)

*coruscant(config)# **timeout uauth 3:00:00 absolute***

*coruscant(config)# **timeout uauth 0:30:00 inactivity***

Changement du prompt d'authentification

Pixfirewall(config)# auth-prompt [accept | reject | prompt] string

- Définir le prompt utilisateur vu lors de l'authentification
- Définir le message utilisateurs donner quand ils authentifier avec ou sans succès
- Par défaut, seulement le prompt username et le password sont vues.

*coruscant(config)# **auth-prompt prompt << Authentifiez-vous >>***

*coruscant(config)# **auth-prompt accept << Bienvenue >>***

*coruscant(config)# **auth-prompt reject << essaye encore une fois... >>***

Activation de l'autorisation

pixfirewall(config)#aaa authorization include | exclude author_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask

- Définir le trafic qui exige l'authentification du serveur AAA
- author_service = protocol/port
  - protocol: tcp (6), udp (17), icmp (1), or others (protocol #)
  - port:
    - single port (e.g., 53), port range (e.g., 2000-2050), or port 0 (all ports)
    - ICMP message type (8 = echo request, 0 = echo reply)
    - port is not used for protocols other than TCP, UDP, or ICMP

Activation de la comptabilité

pixfirewall(config)# aaa accounting include|excludeacctg_service inbound |outbound|if_name local_ip local_mask foreign_ip foreign_mask group_tag

- Définir le trafic qui exige la comptabilité du serveur AAA
- acctg_service= any, ftp, http, or telnet
  - any: All TCP traffic

*coruscant(config)# **aaa accounting include any outbound 0 0 0 0 mytacacs***

*coruscant(config)# **aaa accounting exclude any outbound 192.168.1.10 255.255.255.255 0.0.0.0 0.0.0.0 mytacacs***

Vous pouvez voir les informations de comptabilité sur le serveur CSACS en cliquant sur le bouton « Reports and Activity »

Les commandes show

coruscant(config)# ***show aaa-server***

coruscant(config)# ***show aaa [authentication |authorization | accounting]***

coruscant(config)# ***show auth-prompt [prompt | accept | reject]***

coruscant(config)# ***show timeout uauth***

4.3 Telnet et SSH

Telnet est un protocole client-serveur qui nous semble provenir du fond des âges tant il est intégré dans les ordinateurs au point que son nom est entré dans le langage commun. Basé sur TCP/IP, Telnet rend d'innombrables services de par le monde et son côté pratique a largement contribué à sa distribution et à sa popularité. Toutefois, Telnet présente en termes de sécurité de très nombreux désavantages comme celui de ne pas chiffrer les communications. Ainsi, la séquence d'authentification entre le client et le serveur passant en clair sur le réseau révèle directement le mot de passe de l'utilisateur qui tente de se connecter.

Comme pour la plupart des appareils Cisco, le PIX implémente par défaut un service Telnet qui est disponible sur les interfaces virtuelles VTY (Virtual terminal). Il est malgré tout indispensable d'avoir entré un mot de passe dans la configuration ou de faire appel au service d'authentification. Tout ceci reste cependant insuffisant au regard des menaces actuelles qui planent sur les réseaux.

La protection des accès (via le réseau) à la ligne de commande est une nécessité et ce fait est universellement reconnu. C'est la raison pour laquelle le protocole SSH connaît depuis quelques années un franc succès.

L'implémentation du protocole SSH (Secure Shell) sur les produits Cisco offre la possibilité de se connecter en toute sécurité à un hôte distant en chiffrant toute la communication y compris la séquence d'authentification.

coruscant(config)# ***aaa authentication ssh console mytacacs***

coruscant(config)# ***crypto key generate rsa modulus 768***

INFO: The name for the keys will be: <Default-RSA-Key>

Keypair generation process begin. Please wait...

coruscant(config)# **ssh 192.168.1.10 255.255.255.255 inside**

5. Configuration avancé du Cisco PIX

5.1 Enregistrement du serveur web sur le DNS

On pourrait croire qu'il suffise juste de rajouter une access-list, mais ce serait trop simple. Nous savons qu'il va falloir en rajouter une sur l'interface DMZ. Mais si on le faisait, elle viendrait se rajouter à la fin de la liste déjà présente et donc n'aurait aucun impact (voir explication des règles implicites ASA).

Nous pouvons avoir un état des lieux en tapant : « show access-list <le nom de la liste placé sur l'interface DMZ> »

coruscant(config)# show access-list dmz_access_in

access-list dmz_access_in; 5 elements
access-list dmz_access_in line 1 extended permit icmp any any echo-reply (hitcnt=1) 0x848d298a
access-list dmz_access_in line 2 extended permit icmp any any time-exceeded (hitcnt=0) 0xf224abc3
access-list dmz_access_in line 3 extended permit icmp any any unreachable (hitcnt=0) 0x831a927f
access-list dmz_access_in line 4 extended deny ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=9) 0x8460f584
access-list dmz_access_in line 5 extended permit ip 192.168.2.0 255.255.255.0 any (hitcnt=4) 0xfef24096

Il nous faut intégrer notre access-list à la ligne 4, pour cela tapez :

coruscant(config)# access-list dmz_access_in line 4 permit udp host webserver host domainserver eq 53

Nous pouvons confirmer son emplacement en retapant la commande show :

coruscant(config)# show access-list dmz_access_in

access-list dmz_access_in; 6 elements
access-list dmz_access_in line 1 extended permit icmp any any echo-reply (hitcnt=2) 0x848d298a
access-list dmz_access_in line 2 extended permit icmp any any time-exceeded (hitcnt=0) 0xf224abc3
access-list dmz_access_in line 3 extended permit icmp any any unreachable (hitcnt=0) 0x831a927f
access-list dmz_access_in line 4 extended permit udp host webserver host domainserver eq domain (hitcnt=0) 0xc44f90e7
access-list dmz_access_in line 5 extended deny ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=21) 0x8460f584
access-list dmz_access_in line 6 extended permit ip 192.168.2.0 255.255.255.0 any (hitcnt=6) 0xfef24096

5.2 Installation d'un serveur de messagerie

Pour ne pas à avoir à ouvrir trop de portes, nous avons décidé d'installer le serveur de messagerie MDaemon dans la dmz.

MDaemon est une solution complète de messagerie et travail collaboratif fournissant des outils sécurisés et conformes aux standards actuels. Il inclut des listes de diffusion, supporte plusieurs domaines et peut s'administrer à distance par le web.

Il supporte les protocoles IMAP, SMTP et POP3 et garantit une sécurité optimale grâce à de nombreux outils : filtre anti-spam, filtre de contenu, listes blanches et listes noires, vérifications DNS inverses... Associé au module SecurityPlus for MDaemon, il garantit une protection proactive contre les virus et phishings.

Les clients internes pourront communiquer avec le serveur via leur client de messagerie sans aucun problème et les clients extérieurs pourront s'y connecter via « web mail »

Nous devons donc ouvrir le port 3000 pour cela

coruscant(config)#access-list outside_access_in extended permit tcp any host 172.20.1.4 eq 3000

5.3 Installation d'un serveur SYSLOG

Syslog se compose d'une partie cliente et d'une partie serveur. La partie cliente (notre PIX) émet les informations sur le réseau, via le port UDP 514. Le serveur collecte l'information et se charge de créer les journaux.

La première étape est d'activer le logging avec la commande logging on.

Indiquez un serveur pour recevoir les messages avec la commande logging host :

logging host [in_interface_name] ip_address [protocol / port]

Indiquez les niveaux de log qui seront expédiés au serveur syslog avec la commande logging trap level :

logging trap level

Le Logiciel utilisé dans notre cas est le Serveur SYSLOG (Kiwi Syslog Daemon) de Kiwi Enterprises.

Activation de la journalisation pour tous les emplacements de sortie configurée

```
coruscant(config)# logging enable
```

Définir le serveur KIWI comme serveur Syslog

```
coruscant(config)# logging host inside 192.168.1.3
```

Le PIX envoie des messages Syslog pour documenter les événements suivants :

- Sécurité : Paquets UDP perdus et connexions TCP abandonnées.
- Ressources : Notification d'épuisement de connexion et translation.
- Système : Console connexion Telnet ainsi que quand les redémarrages du PIX.
- Accounting : Octets transférés par connexion.

```
coruscant(config)# logging list kiwi level 4

coruscant(config)# logging list kiwi level 5

coruscant(config)# logging list kiwi level 6

coruscant(config)# logging list kiwi level 7
```

On demande à ce que les messages précédemment définie dans la liste soit envoyé au serveur Syslog

```
coruscant(config)# logging trap kiwi
```

5.4 Cisco intrusion prevention system

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives d'intrusion d'une entreprise. L'IDS n'a que le rôle d'alerter qu'une intrusion a lieu, il faut donc que l'administrateur réseau de l'entreprise intervienne afin de régler les problèmes. Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) a le même rôle de détection qu'un IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.

Le PIX possède un système de prévention d'intrusions. Il contient une base avec un ensemble de signatures, basées sur deux types de politique, « info » et « attack ». Comme tout bon IDS, il inspecte chaque paquet ou sessions traversant le routeur, à la recherche d'analogies avec l'une de ses 52 signatures.

*coruscant(config)# **ip audit signature ?***

configure mode commands/options:
<1000-9999> Valid signatures are in the following range: { 1000, 1006 }, { 1100, 1103 }, { 2000, 2012 }, { 2150, 2151 }, { 2154, 2154 }, { 3040, 3042 }, { 3153, 3154 }, { 4050, 4052 }, { 6050, 6053 }, { 6100, 6103 }, { 6150, 6155 }, { 6175, 6175 }, { 6180, 6180 }, { 6190, 6190 }

Avec les commandes suivantes on peut le configurer afin qu'il réalise une action dès qu'une intrusion est détectée.

ip audit info [action [alarm] [drop] [reset]]

ip audit attack [action [alarm] [drop] [reset]]

- « alarm » permet de remonter une alerte.
- « drop » permet de supprimer les paquets.
- « reset » permet de réinitialiser la connexion TCP.

Pour notre configuration, nous avons défini l'action par défaut pour les paquets qui correspondent à une signature d'attaque : alerte et réinitialisation de la connexion

*coruscant(config)#**ip audit attack action alarm reset***

La stratégie pour l'interface interne se substitute à la stratégie précédente pour alerter seulement, alors que la stratégie pour l'interface externe utilisera les paramètres par défaut défini dans la commande **ip audit attack**

*coruscant(config)#**ip audit name INSIDEPOLICY attack action alarm***
*coruscant(config)#**ip audit name OUTSIDEPOLICY attack***
*coruscant(config)#**ip audit interface inside INSIDEPOLICY***
*coruscant(config)#**ip audit interface outside OUTSIDEPOLICY***

Le serveur KIWI étant déjà défini, dans la configuration précédente, comme serveur Syslog. C'est lui qui recevra les alertes émises par l'IPS.

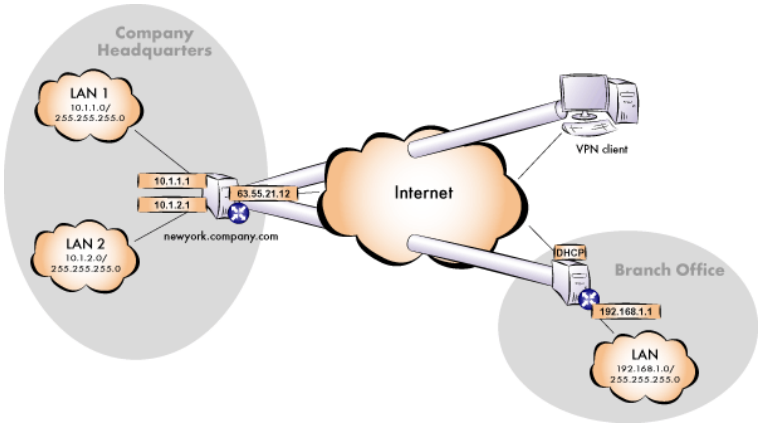
Commande SHOW :

coruscant(config)#show running-config ip audit count	*affiche le nombre de matches*
coruscant(config)#show running-config ip audit attack	*affiche la config IP pour signatures d'attaques*
coruscant(config)#show running-config ip audit interface	*affiche la config de l'interface*
coruscant(config)#show running-config ip audit name	*affiche la config de la stratégie nommée*

6. Virtual Private Network

5.1 Principe générale

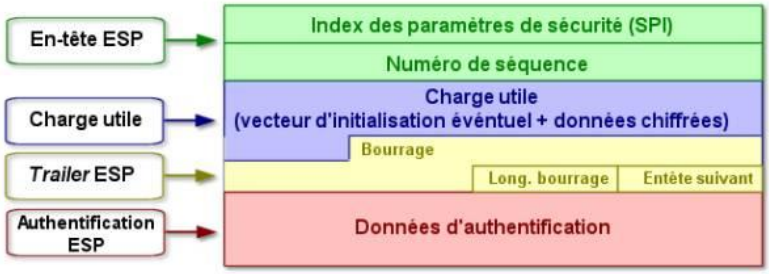
Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

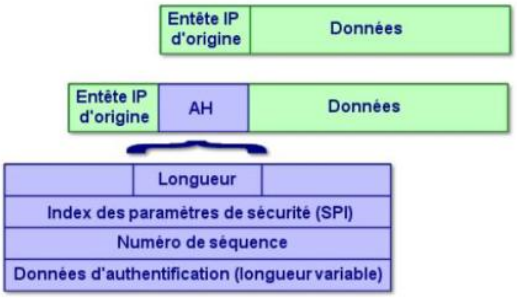


Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant Ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Pour réaliser une connexion VPN, nous pouvons utiliser plusieurs de niveau 2 (comme Pptp et L2tp) ou de niveau 3 (comme Mpls ou IPsec). Nous avons choisi d'utiliser IPsec, qui est un protocole qui vise à sécuriser l'échange des données au niveau de la couche réseau.

IPsec permet donc via le réseau internet de relier de façon sécurisée deux réseaux privés. IPsec est basé sur 2 mécanismes différents assurant les rôles de sécurisation des données : AH (Authentification header) et ESP

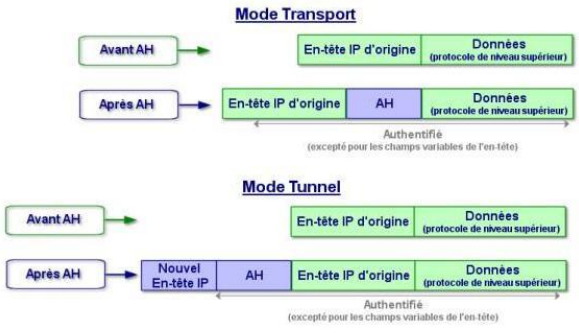




(Encapsuling Security Payload). IPsec est largement configurable. Ainsi, chacun des deux mécanismes AH et ESP peuvent être utilisés seuls ou combinés avec le second afin de définir le niveau de sécurité voulu. C'est deux mécanismes rendent divers services. L'AH permet une authentification, une vérification de l'intégrité des données, l'anti-rejeu, et la non-répudiation. L'ESP rend les mêmes services que l'AH et permet en plus l'encryption des données.

C'est sous-protocoles peuvent être mis en place dans deux modes le mode de fonctionnement :

- Le mode transport - les adresses destination et source circulent en clair, les hôtes sont donc connus,
- Le mode tunnel - ces adresses sont cryptées et un nouvel en-tête encapsule le paquet.

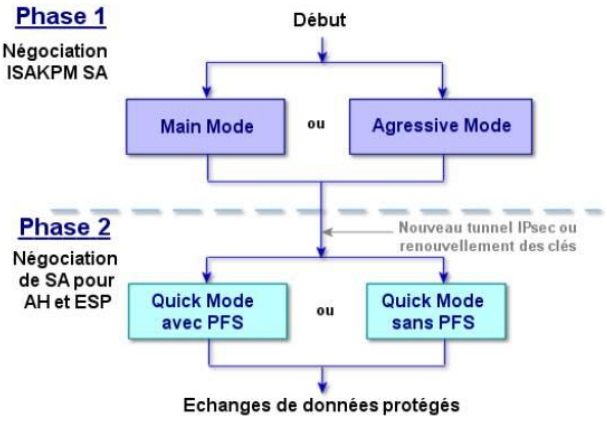


L'authentification peut se faire de plusieurs façon : par l'adresse source, une signature numérique, une clé pré-partagée, ou des certificats.

L'intégrité des données est assurée grâce à la fonction de hachage, qui consiste à vérifier d'une manière rapide si le paquet n'a pas été modifié, il est calculé de tel sorte que la probabilité d'obtenir un résultat identique si un bit est modifié soit presque nul. Le résultat (appelé empreinte digital) du calcule de hachage est adjoint au datagramme IP dans un champ supplémentaire appelé « valeur de vérification d'intégrité » (Integrity Check Value, ICV), il est donc calculé par la source après cryptage des données, il sera de nouveau calculé à destination avant décryptage de sorte que si le résultat calculé et la valeur dans le champ ICV ne soit pas identique le processus de décryptage, plus long, ne soit pas mis en œuvre. Les principaux protocoles de hachage utilisés sont MD5 et SHA-1.

L'encryption est faite par des algorithmes de cryptage. Les plus utilisé étant DES, 3DES, AES. AES étant aujourd'hui le standard. Pour crypter l'algorithme utilise une clé, il en existe deux types :

- Les clés symétriques, commune aux deux périphériques, servant à chiffré et déchiffré le message. La fiabilité de l'algorithme tient au secret de cette clé (ex DES, AES).
- Les clés asymétriques, un périphérique génère une paire de clé (une clé privé et une clé publique), il envoie la clé publique au périphérique distant. Cette clé ne sert qu'au cryptage, et le décryptage ne peut se faire qu'avec la clé privé (ex RSA, Deffie-Hellman). Le cryptage est une formule informatique qui permet de modifier le message initial en message codé à l'aide de la clé, et seul la clé permet de retrouver le message initial (clé identique avec un algorithme symétrique et la clé privée avec un algorithme asymétrique).



La mise en place d'un tunnel VPN avec IPsec se passe en 2 étapes. ISAKMP (Internet Security Association and Key Management Protocol) définit la façon de procéder pour ces deux étapes. Dans la première phase, un certain nombre de paramètres de sécurité propres à Isakmp sont mis en place, afin d'établir entre les deux tiers un canal protégé. Dans la deuxième phase, ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et ESP par exemple). Les données circuleront dans ce deuxième tunnel). Chaque échange unilatéral est identifié par une SA (Security association) une connexion bilatéral comprend donc deux SA. Une SA comprend toutes les données relative à la connexion, c'est-à-dire les adresses source et destination, les ports source et destination, la méthode d'authentification, les algorithmes de cryptage et de hachage, le SPI (Security Parameter Index) Security protocole identifier (AH ou ESP) ainsi que sa durée de vie. Toutes les SA d'un périphérique sont stocké dans une base de donnée la SADB (Security association data base)

5.2 Configuration d'un tunnel VPN Site à Site

Dans un premier temps il faut créer la police de sécurité qui déterminera les règles d'établissement du tunnel ISAKMP (voit théorie VPN). Nous donnerons un numéro à cette police et dans cette police il y aura la méthode d'authentification, l'algorithme de cryptage et de hachage, le groupe Deffie-Hellman.

(config#crypto isakmp policy <ID de la police> num de priorité entre 1 et 65535

(config-isakmp-policy)#authentication <méthode d'authentification>

(config-isakmp-policy)#encryption <algorithme de cryptage>

(config-isakmp-policy)#hash <algorithme de hashage>

(config-isakmp-policy)#groupe (n° du groupe deffie-hellman)

Pour connaître les différentes options accepter par le matériel faire un « ? » après la commande

Exemple dans notre topologie :

coruscant(config)# ***crypto isakmp policy 10***

coruscant(config-isakmp-policy)# ***authentication pre-share***

*coruscant(config-isakmp-policy)#****encryption 3des***

*coruscant(config-isakmp-policy)#****hash sha***

*coruscant(config-isakmp-policy)#****group 2***

Dans le cas d'une authentification en pre-share key il faut la définir avec la commande suivant

(config)#crypto isakmp key <mot ou phrase clé choisi sans espace> address <adresse de la cible>

Exemple dans notre topologie :

*coruscant(config)#****crypto isakmp key dagobah address 172.20.3.1***

Ensuite il nous faut créer les paramètres pour la négociation du 2ème tunnel. Pour cela nous allons définir des « transform-set », des ACL et une crypto map. Petite note sur les « transform-set », un « transform-set » est créé pour définir quels algorithmes de cryptage et de hachage seront utilisé, chaque « transform-set » sera nommé afin de les reconnaitre on peut en assigné autant que l'on veut à une crypto map, un « transform-set » comprend soit un algorithme de cryptage, soit un algorithme de hachage soit un de chaque. Une access-list définira les adresses autorisées à entrer dans le tunnel. La crypto map comprendra donc les « transform-set », l'adresse de la cible (bout du tunnel), et les adresses autorisé dans ce VPN (ACL). Il faudra enfin affecter cette crypto map à une interface (celle d'entrée du tunnel), elle sera nommé et aura un numéro de séquence qui définira l'ordre dans lequel elle sera appliquée si il y en plusieurs.

(config)#crypto ipsec transform-set <nom choisi> <algorithme 1> <algorithme2>

Faire « ? » pour savoir quels algorithmes sont supportés par le matériel

(config)#access-list <nom> permit ip <adresse source> <masque> <adresse destination> <masque>

(config)#crypto map <nom de la crypto map> <numéro de séquence> ipsec-isakmp

(config)#crypto map <nom de la crypto map> <num de séquence> match address <nom de l'ACL>

(config)#crypto map <nom de la crypto map> <num de séquence> set transform-set <nom du transform-set>

(config)#crypto map <nom de la crypto map> <num de séquence>set peer <adresse de la cible>

Exemple dans notre topologie :

coruscant(config)# ***crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac***

coruscant(config)# ***access-list outside_cryptomap_20 extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0***

coruscant(config)# ***access-list outside_cryptomap_20 extended permit ip 192.168.2.0 255.255.255.0 192.168.3.0 255.255.255.0***

Nous avons décidé de ne pas translaté les adresses qui rentrent dans le tunnel

coruscant(config)# ***nat (inside) 0 access-list outside_cryptomap_20***

coruscant(config)# ***nat (dmz) 0 access-list outside_cryptomap_20***

coruscant(config)# ***show run nat***

nat (inside) 0 access-list outside_cryptomap_20
nat (inside) 1 192.168.1.0 255.255.255.0
nat (dmz) 0 access-list outside_cryptomap_20
nat (dmz) 1 192.168.2.0 255.255.255.0

coruscant(config)# ***crypto map outside_map 20 match address outside_cryptomap_20***

coruscant(config)# ***crypto map outside_map 20 set transform-set ESP-DES-MD5***

coruscant(config)# ***crypto map outside_map 20 set peer 172.20.3.1***

coruscant(config)# ***crypto map outside_map 20 set pfs***

coruscant(config)# ***crypto map outside_map interface outside***

coruscant(config)# ***crypto isakmp enable outside***

coruscant(config)# ***crypto isakmp identity address***

Pour finir on peut vérifier nos configurations à l'aide des commandes :

coruscant(config)# ***show run crypto map***

crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 172.20.3.1
crypto map outside_map 20 set transform-set ESP-DES-MD5
crypto map outside_map interface outside (config)# show run Isakmp

coruscant(config)# ***show run crypto isakmp***

crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

ET *coruscant(config)#* ***show run crypto ipsec***

crypto ipsec transform-set ESP-DES-MD5-HMAC esp-des esp-md5-hmac

Pour vérifier le bon fonctionnement on peut utiliser les commandes suivantes :

(config)# show crypto isakmp sa

(config)# show crypto ipsec sa

Pour le routeur distant, la configuration est approximativement la même :

Configuration des access-list

access-list 120 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 120 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255

Configuration pre shared keys

Identique

Configuration IPsec

Identique

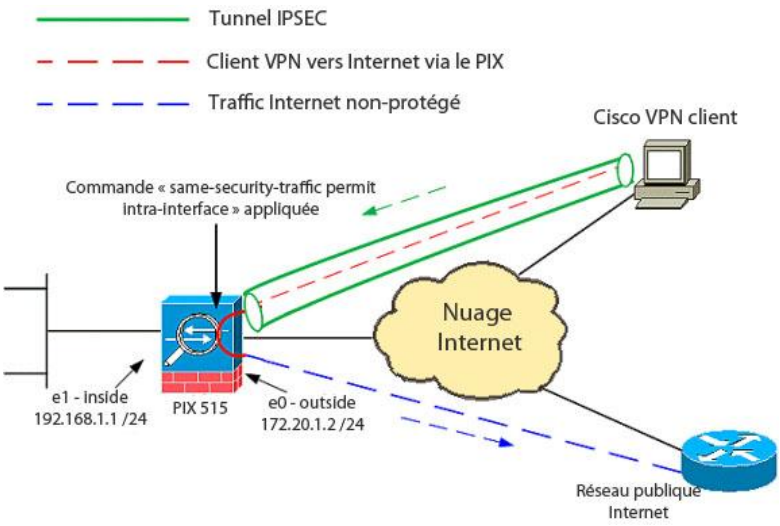
Configuration crypto map

Identique, ici le match address sera 120

Comme pour le PIX, ne pas oublier d'appliquer la crypto map sur l'entrée du tunnel (ou l'interface de sortie du routeur, tout dépend de quel point de vue on se place)

interface FastEthernet0/0
ip address 172.20.3.1 255.255.255.0
no ip route-cache cef
no ip route-cache
no ip mroute-cache
duplex auto
speed auto
crypto map outside_map

5.3 Configuration d'un VPN sécurisé à l'aide d'IPsec entre un PIX et un client VPN



L'installation du logiciel Cisco VPN client est assez simple, donc nous ne verrons pas ici les étapes de son installation.

La plus grande contrainte ici, est de forcer le client VPN à utiliser le tunnel pour accéder à Internet. Nous vous expliquerons les étapes à suivre pour atteindre cet objectif.

En premier lieu, il convient d'appliquer la commande qui permet au trafic IPsec d'entrer et de sortir par la même interface

coruscant(config)# ***same-security-traffic permit intra-interface***

Pour permettre à nos clients de pouvoir communiquer avec le réseau interne, il va falloir nater la liaison interne vers le réseau 192.168.10.0

coruscant(config)#access-list outside_cryptomap_20 extended permit ip 192.168.1.0 255.255.255.0 192.168.10.0 255.255.255.0

Note : nous avons utilisé ici une access-list déjà créer précédemment pour le VPN site à site. Pour mémoire elle est liée à un natage 0, ce qui nous intéresse pour notre configuration.

Ensuite décidons d'un pool d'adresses pour les clients VPN

coruscant(config)# ***ip local pool remote_vpn_pool 192.168.10.1-192.168.10.254 mask 255.255.255.0***

On autorise le réseau 192.168.10.0 à être translaté en une adresse appartenant au global 1

coruscant(config)# ***nat (outside) 1 192.168.10.0 255.255.255.0***

Configuration de la politique de groupe pour les clients VPN

coruscant(config)# ***group-policy remotevpn internal***

coruscant(config)# ***group-policy remotevpn attributes***

coruscant (config-group-policy)# ***dns-server value 192.168.1.2***

coruscant(config-group-policy)# ***vpn-idle-timeout 20***

On force le client VPN à utiliser le tunnel pour accéder à Internet

coruscant(config-group-policy)# ***split-tunnel-policy tunnelall***

Configuration IPsec Phase 2

coruscant(config)# ***crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac***

coruscant(config)# ***crypto dynamic-map outside_dyn_map 30 set transform-set ESP-3DES-SHA***

coruscant(config)# ***crypto dynamic-map outside_dyn_map 30 set reverse-route***

Set reverse-route met en place le RRI (Reverse Route Information), ce qui permet au PIX d'apprendre des informations de routage des clients connectés. Pour faire simple, il rajoute le réseau 192.168.10.0 dans sa table de routage.

coruscant(config)# ***crypto map outside_map 30 ipsec-isakmp dynamic outside_dyn_map***

coruscant(config)# ***tunnel-group remotevpn type ipsec-ra***

coruscant(config)# ***tunnel-group remotevpn general-attributes***

coruscant(config-tunnel-general)# ***authentication-server-group mytacacs***

coruscant(config-tunnel-general)# ***address-pool remote_vpn_pool***

coruscant(config-tunnel-general)# ***default-group-policy remotevpn***

coruscant(config-tunnel-general)# ***tunnel-group remotevpn ipsec-attributes***

coruscant(config-tunnel-ipsec)# ***pre-shared-key cisco1234***

En cas de souci avec le serveur TACACS pensez à ajouter un login local

coruscant(config)# ***username remoteuser password cisco123 privilege 0***

7. Procédure de restauration de mot de passe sur Cisco PIX 515E

Problématique :

Vous voulez configurer un équipement Cisco dont vous avez perdu le mot de passe

Sur les commutateurs et routeurs, la méthodologie pour bypasser la phase d'authentification via les login et mots de passe présent dans le fichier de configuration est d'interrompre la séquence de boot au démarrage (appuyez sur les touches CTRL + Pause au démarrage).

Vous rentrerez alors dans un mode appelé ROMMON (Rom monitor). A partir de ce menu, il faudra modifier le config-register. Cette valeur indique au Switch/routeur d'utiliser ou non le fichier de configuration. Par défaut le conf-register a pour valeur 0×2102. En modifiant cette valeur à 0×2142, on indique que l'on veut booter sans utiliser la start-up –config, puis on laisse l'équipement booter normalement, ce qui nous permet de travailler sur un fichier de configuration vide. Il suffira alors de passer en mode privilégié et de copier la start-up config dans la running-config, ainsi vous aurez accès à la configuration et vous pourrez effectuer vos modification : par exemple pour redéfinir le mot de passe d'un compte local ou alors pour modifier le mot de passe ENABLE. Une fois vos modifications faite, veuillez remettre la valeur du config-register à la valeur 2102 et de sauvegarder les changements que vous avez effectuez !

Sur un équipement de type PIX, la procédure de restauration de mot de passe est différente.

En effet, Dans le mode Rommon du PIX, on ne peut modifier la valeur de la clé du conf-reg rendant ainsi la précédente manipulation obsolète.

Afin de restaurer le mot de passe, Cisco fournit des fichiers de restauration avec l'extension .BIN, il suffit d'indiquer au firewall, l'adresse d'un serveur TFTP joignable qui contient le fichier de restauration (correspondant à la version du micro code de notre équipement).

Fichiers de restauration :

np70.bin (version 7.x et 8.0)
np63.bin (version 6.3)
np62.bin (version6.2)
np61.bin (version 6.1)
np60.bin (version 6.0)
np53.bin (version 5.3)
np52.bin (version 5.2)
np51.bin (version 5.1)
np50.bin (version 5.0)
np44.bin (version 4.4)
nppix.bin (version 4.3 et inférieur)

Typiquement, la marche à suivre est d'interrompre la séquence de boot (CTRL + Pause au démarrage), vous devriez tomber sur un prompt : **monitor >**

La commande interface vous permet d'identifier vos interfaces réseaux : **monitor > interface 1**

Spécifiez alors l'interface réseau qui communiquera avec le serveur TFTP ainsi que son adresse , le nom du fichier récupéré , la gateway (si le serveur est distant) , l'adresse IP du serveur TFTP , et enfin tapé TFTP pour procédé au transfert :

monitor >**address 192.168.1.1**
address 192.168.1.1
monitor > **server 192.168.1.10**
server 192.168.1.10
monitor >**ping 192.168.1.10**
Sending 5, 100-byte 0x2c9b ICMP
Echoes to 192.168.1.10, timeout is 4 seconds:
!!!!!
Success rate is 100 percent (5/5

Si le Ping n'est pas concluant c'est peut-être parce que vous n'êtes pas connecté en réseau directement de votre PC à votre routeur et que donc vous passez par le réseau de votre entreprise. Dans ce cas indiquez une passerelle avec la commande :

monitor > gateway [adresse IP]

Il faut ensuite indiquez quel fichier nous allons récupérer par TFTP, pour notre cas il s'agit du fichier np70.bin :

monitor > file np70.bin
file np70.bin

Il ne nous reste plus qu'à se connecter en TFTP, répondez oui aux questions demandé

```
Do you wish to erase the passwords? [yn] y
Passwords have been erased.
```

Le routeur récupère le fichier et l'exécute puis enfin redémarre.

Vous pouvez maintenant passez en mode privilégié et en mode de configuration sans entrer de mot de passe. En effet, après avoir tapé la commande « enable », pour passer au mode privilégié, le prompt « password » vous sera demandé et il vous suffira de valider pour entrer dans ce mode. Le mot de passe par défaut pour Telnet après ce processus est « cisco »

Conclusion

Vos mots de passes sont à présent réinitialiser à blancs. Vous pouvez maintenant reconfigurer le pare-feu comme vous le souhaitez. Cependant, n'oubliez pas de reconfigurer le mot de passe du mode enable avant de remettre votre routeur en activité :

pixfirewall(config)# **enable password class**
pixfirewall(config)# **write memory**
Building configuration
Cryptochecksum: ab89dad5 ca61ba32 c50a58fc bf16aca6
[OK]

La première commande correspond à votre mot de passe, ici « toto », puis on inscrit la nouvelle configuration dans la flash.

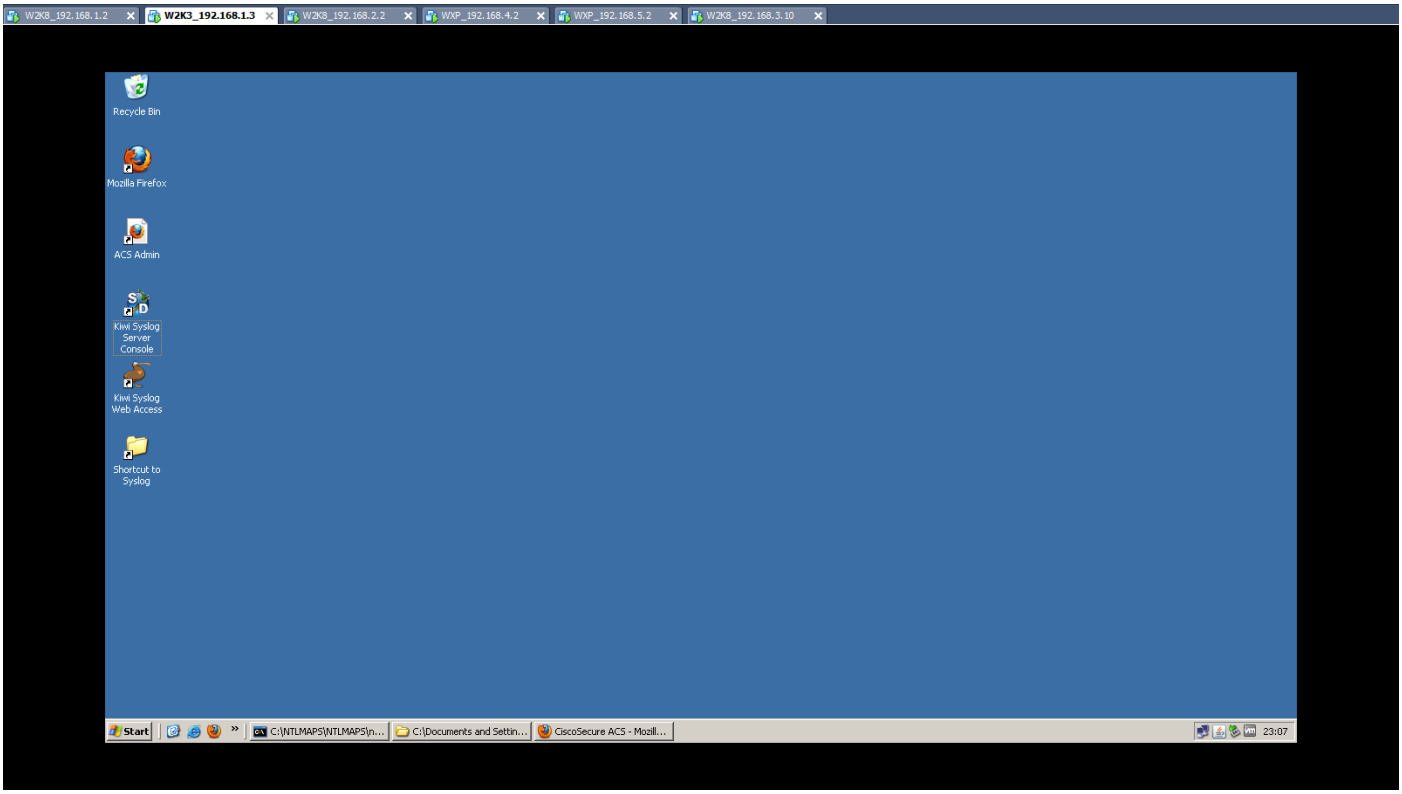
Votre routeur est ainsi configuré avec un nouveau mot de passe.

V. La virtualisation et les émulateurs

1. Virtualisation (VMware et Virtual Box)

Ce dossier a grandement bénéficié de l'essor des technologies de virtualisation et d'émulation. Nous allons dans ce chapitre décrire les méthodes qui nous ont permis de réaliser les maquettes destinées à concevoir et à valider les configurations présentées dans ce dossier. Deux logiciels particulièrement performants ont été mis à contribution. Nous citerons en premier l'incontournable VMware puis le couple Dynamips, GNS3.

La virtualisation consiste à utiliser un système d'exploitation afin de faire fonctionner en son sein d'autres systèmes d'exploitation. La virtualisation est apparue pour le grand public à la fin des années 90 avec l'avènement du logiciel VMware. Elle possède à son actif de nombreux avantages parmi lesquels nous pouvons citer une réduction du nombre de machines présentes dans les salles informatiques grâce aux regroupements effectués sur des machines hôtes. Outre le gain de place évident, la virtualisation simplifie la création et le déplacement de systèmes d'exploitation virtuels entre les machines hôtes diminuant ainsi les coûts associés à l'exploitation.



La virtualisation présente d'indéniables avantages en ce qui concerne la création de réseaux à des fins d'essais lors de phases d'intégration et de validation d'un projet informatique. Il est en effet facile de créer, de modifier, de déplacer et de supprimer un système d'exploitation virtuel. Un autre avantage est de pouvoir aisément déplacer un groupe de machines virtuelles dans le cadre de démonstrations car elles prennent la forme d'un ensemble de quelques fichiers. La capture d'écran montre six machines hôtes dont des serveurs Windows 2008 et 2003 et des Windows XP. Une septième machine était installé sur un autre bureau et virtualisait la machine management (192.168.1.10) avec ASDM. L'hôte fournissant le service d'hébergement est également désigné par l'appellation d'hyperviseur. Les machines virtuelles avec certaines versions de VMware (ACE) peuvent être chiffrées et recevoir des politiques de sécurité. VMware est aussi présenté sous une forme qui constitue elle-même un système d'exploitation. Il s'agit de la version ESX qui s'installe directement sur le matériel. Il n'est plus indispensable d'installer un système d'exploitation hôte comme Microsoft Windows (ce qui est le cas sur la capture d'écran).

L'autre avantage que présente VMware est qu'il offre une prise en charge avancée du réseau. Un serveur DHCP et jusqu'à 10 commutateurs virtuels permettent la connexion de machines virtuelles entre elles, à la machine hôte et aux réseaux publics.

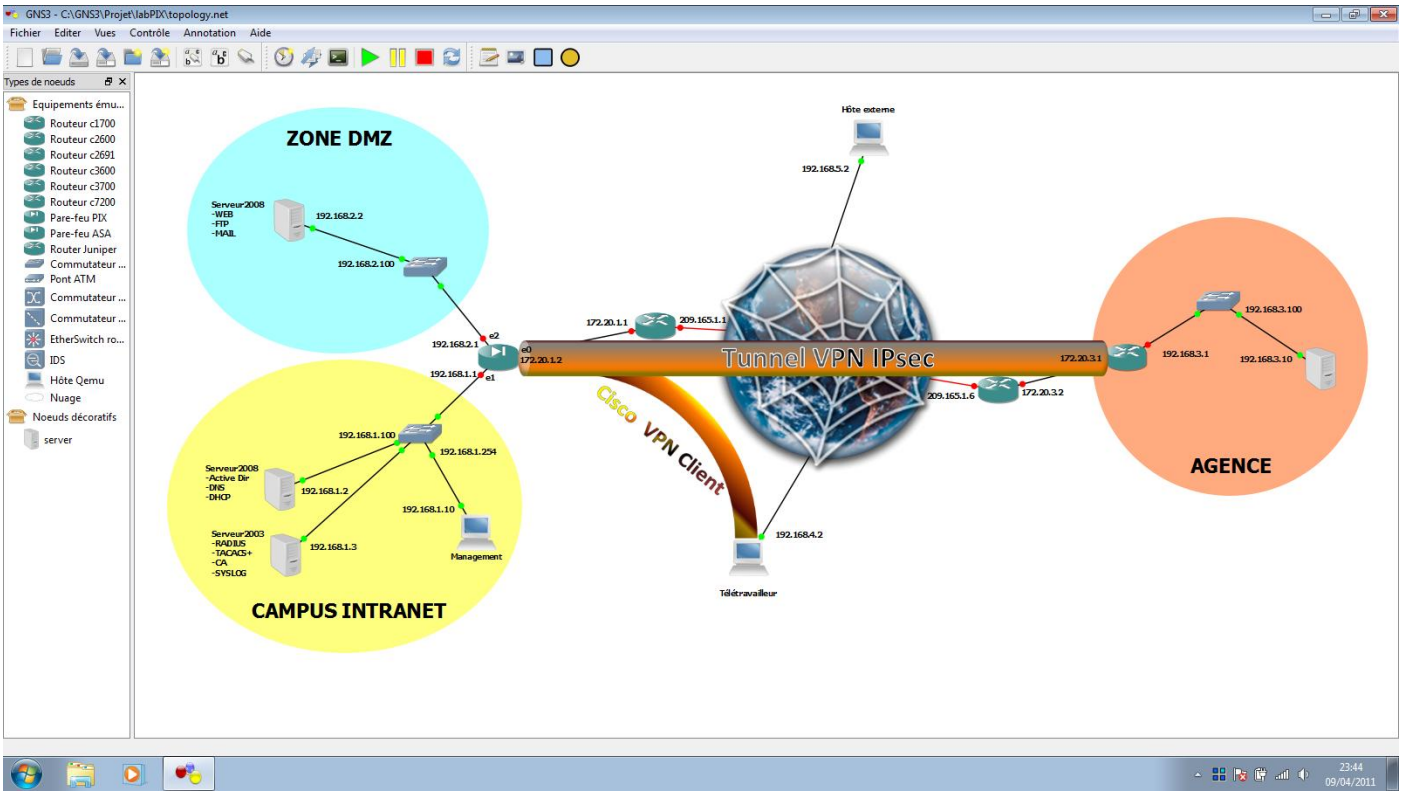
Toutes les machines virtuelles fonctionnait en mode « host only » et était relié via des Cloud à GNS3.

2. Emulation

Nous avons également fait usage de la technique d'émulation pour simuler un réseau de routeurs Cisco et surtout le PIX. La frontière est mince entre l'émulation et ce que nous venons de décrire avec la virtualisation. Ici, l'ordinateur va simuler l'électronique du routeur afin de faire fonctionner le logiciel IOS.

GNS3 est un simulateur graphique de réseaux qui vous permet de créer des topologies de réseaux complexes et d'en établir des simulations. Ce logiciel, en lien avec Dynamips (simulateur IOS), Dynagen (interface textuelle pour Dynamips) et Pemu (émulateur PIX), est un excellent outil pour l'administration des réseaux CISCO, les laboratoires réseaux ou les personnes désireuses de s'entraîner avant de passer les certifications CCNA, CCNP, CCIP ou CCIE. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou de tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment OpenSource et multi-plates-formes. Remarque importante : l'utilisateur doit fournir ses propres images IOS pour utiliser GNS3.

Il est important de préciser que le système d'exploitation IOS est sous licence. Pour utiliser Dynamips, il est donc indispensable de posséder légalement une image système.



On peut voir sur la capture d'écran la topologie utilisée pour faire les tests. Chaque ordinateur est en réalité un nuage. Chaque nuage est relié à une carte réseau VMnet, elle-même relié à une machine virtuelle.

Pour débuter avec le PIX sous gns3, nous vous conseillons un tutoriel à la page :

http://www.brainbump.net/tutorials/voice/asdm-gns3.htm

3. Conclusion

Les avantages des produits comme VMware ou Dynamips, GNS3 sont multiples, mais le revers de la médaille est une augmentation considérable des ressources (mémoire et processeur) qui sont consommées par ces programmes sur le système hôte (a noté que l'émulation d'un PIX occupe la totalité des ressources d'un processeur). Il devient possible dans un environnement réduit à une seule machine de mettre en œuvre une maquette réseau et système très complète et relativement complexe. Ces techniques permettent aisément de sauvegarder les diverses configurations et de les installer à loisir. Les techniques de virtualisation et d'émulation sont en quelque sorte respectueuse de l'environnement en permettant de réaliser des économies d'électricité et d'espace, c'est pour ces raisons qu'elles connaissent depuis quelques années déjà un franc succès.

VI. Conclusion

1. Conclusion d'ordre technique

Nous avons exposé dans ce dossier quelques-unes des multiples fonctionnalités offertes par le pare-feu PIX qui vont bien au-delà de la simple confrontation du trafic à des règles de filtrage. Sans cette évolution, ce type de matériel serait sans doute tombé en désuétude. Le pare-feu PIX de Cisco est un équipement multifonction aux possibilités remarquables qui reprend les fonctions de base comme le filtrage et y ajoute celles issues des boitiers VPN. Toutes les couches du modèle OSI sont couvertes et les protocoles applicatifs bénéficient d'un puissant service d'analyse permettant de parer aux problèmes d'irrégularités et d'attaques embarqués.

Dans l'architecture de sécurité, le pare-feu de Cisco occupe, de par ses capacités d'analyses multicouches, des positions qui ne se limitent pas aux frontières avec le monde extérieur car ses spécificités font de lui un appareil capable de protéger également l'intérieur du réseau.

Grace à sa configuration par défaut, Le PIX peut se configurer aisément à l'aide d'une interface graphique (ASDM), et ne nécessite pas de configuration préalable en mode CLI. Ce périphérique permet donc de sécuriser son réseau interne tout en laissant un accès par le web à une partie de ses données moins sécurisés grâce à l'utilisation d'une DMZ. Par défaut le PIX ne permet pas la communication entre les zones (interfaces) ce qui permet une fois branché d'avoir un réseau sécurisé. Mais si les malware ne peuvent pas rentrer, l'accès à l'extérieur n'est pas non plus possible. Pour le rendre possible, il faut donc dans un premier temps configurer les interfaces, et le NAT. A partir de ce moment-là, la communication sera possible des interfaces avec un security-level plus élevé vers des interfaces à security-level plus faible ; ce qui a été notre premier défi : comprendre ce fonctionnement et l'obligation d'instruction de natage pour pouvoir établir la connexion entre zones et pouvoir a l'aide de requêtes ICMP tester cet connectivité. Pour un retour des données de l'extérieur, le pare-feu est dit stateful, c'est-à-dire qu'il garde connaissance de la communication sortante pour permettre le retour des données demandé uniquement. Le PIX permet également de monter des connexions VPN et easy-VPN afin d'établir des connexions sécurisé via le réseau publique. Notre deuxième défi, monter une topologie réaliste quant à la simulation du réseau étendu et configurer un VPN sur le PIX mais également sur un routeur. Nous avons enfin testé les différentes autres fonctionnalités du PIX comme le proxy l'authentification AAA via un serveur CSACS, la remonter d'information sur un serveur Syslog.

2. Conclusion d'ordre personnel

Le Cisco PIX nous a permis une approche de la sécurité réseau à l'aide d'un périphérique dédié très complet et offrant de grande possibilité, que nous n'avons eu le temps d'explorer dans la durée du projet mais qu'au fil de la recherche documentaire nous avons pu observer. Une riche documentation et des tutoriaux abondant sur le Cisco PIX nous ont aidé à tester diverses configurations spécifiques. A mesure de notre progression dans le mini-projet , il nous est apparu que malgré son ancienneté le PIX 515E est très bon matériel réseau, et que son évolution le Cisco ASA doit être en pratique très performant. Nous avons également constaté qu'il y a de plus en plus de concurrence dans ce domaine et qu'au niveau spécification constructeur les périphériques de sécurité proposent globalement les mêmes fonctionnalités et que le choix doit se faire dans la facilité de configuration. Malgré que le PIX nous ai paru compliqué d'un premier abord par ses restriction implicite, une fois son principe de base assimilé, il s'est révélé plus simple à aborder.

VII. Annexes techniques

1. Le PIX devient l'ASA

Réunissant sur une même plate- Réunissant sur une même plate-forme une combinaison puissante de nombreuses technologies éprouvées, la gamme Cisco ASA 5500 (Adaptive Security Appliance) donne à l'entreprise les moyens opérationnels et économiques de déployer des services de sécurité complets vers un grand nombre de sites

- Plus de sécurité, avec le support de nouveaux services de sécurité, tels l'IPS et l'Anti-X avec accélération matérielle (modules optionnels).
- Plus de performances et d'évolutivité.
- Une solution VPN-SSL avec ou sans client, dotée de fonctionnalités de haut niveau.
- Une migration douce, préservant les compétences acquises autour du PIX.

1.1 Technologie reconnue de firewall et VPN protégé contre les menaces

Développée autour de la même technologie éprouvée qui a fait le succès du serveur de Développée autour de la même technologie éprouvée qui a fait le succès du serveur de sécurité Cisco PIX et de la gamme des concentrateurs Cisco VPN 3000, la gamme Cisco ASA 5000 est la première solution à proposer des services VPN SSL (Secure Sockets Layer) et IPsec (IP Security) protégés par la première technologie de firewall du marché. Avec le VPN SSL, l'ASA 5500 est une passerelle SSL performante qui permet l'accès distant sécurisé au réseau d'un navigateur web banalisé pour les utilisateurs nomades.

1.2 Service évolué de prévention des intrusions

Les services proactifs de prévention des intrusions offrent toutes les fonctionnalités qui permettent de bloquer un large éventail de menaces – vers, attaques sur la couche applicative ou au niveau du système d'exploitation, rootkits, logiciels espions, messagerie instantanée, P2P, et bien plus encore. En combinant plusieurs méthodes d'analyse détaillée du trafic, l'IPS de l'ASA 5500 protège le réseau des violations de politique de sécurité, de l'exploitation des vulnérabilités des systèmes et du trafic anormal. L'IPS collabore avec d'autres systèmes Cisco de gestion de la sécurité pour assurer une mise à jour constante de la posture de sécurité du réseau et une réactivité totale aux nouvelles attaques ou vulnérabilités.

1.3 Systèmes ANTI-X à la pointe de l'industrie

La gamme Cisco ASA 5500 offre des services complets Anti-X à la pointe de la technologie – protection contre les virus, les logiciels espions, le courrier indésirable et le phishing ainsi que le blocage de fichiers, le blocage et le filtrage des URL et le filtrage de contenu – en associant le savoir-faire de Trend Micro en matière de protection informatique à une solution Cisco de sécurité réseau éprouvée. Ces services Anti-X embarqués dans le module d'extension hardware CSC SSM et le renouvellement des abonnements Trend Micro pour la gamme ASA sont commercialisés par Cisco au travers de ses partenaires agréés.

1.4 Migration transparente pour l'utilisateur

Les utilisateurs actuels des serveurs de sécurité PIX n'auront aucune difficulté à s'adapter aux solutions Cisco ASA 5500. Les fichiers de configuration des Cisco PIX sont transposables sur les serveurs ASA 5500. Le logiciel d'administration graphique Cisco Adaptive Security Device Manager (ASDM) livré avec la gamme ASA est un logiciel puissant et facile à utiliser. Il accélère la création de politique de sécurité, et réduit la charge de travail et les erreurs humaines, grâce à des assistants graphiques, des outils de débogage et de surveillance. ASDM permet de gérer aussi bien des serveurs Cisco PIX que des serveurs ASA 5500, facilitant la migration vers la dernière génération de matériel et ses nouvelles fonctions.

1.5 Caractéristiques techniques

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Utilisateurs et nœuds	10, 50 ou illimité	Illimité	Illimité	Illimité	Illimité
Débit du firewall	Jusqu'à 150 Mbits/s	Jusqu'à 300 Mbits/s	Jusqu'à 450 Mbits/s	Jusqu'à 650 Mbits/s	Jusqu'à 1,2 Gbits/s
débit des services simultanés de limitation des risques (firewall et services IPS) Débit des VPN 3DES ou AES	Non disponible Jusqu'à 100 Mbits/s	Jusqu'à 150 Mbits/s avec le module AIP SSM (Advanced Inspection and Prévention Security Services Module) 10 (référence AIP SSM 10) pour la gamme Cisco ASA 5500 – Jusqu'à 300 Mbits/s avec le module AIP SSM 20 (référence AIP SSM 20) pour la gamme Cisco ASA 5500 Jusqu'à 170 Mbits/s	Jusqu'à 225 Mbits/s avec le module AIP SSM 10 – Jusqu'à 375 225 Mbits/s avec le module AIP SSM 20 Jusqu'à 225 Mbits/s	Jusqu'à 450 Mbits/s, avec le module AIP-SSM20 Jusqu'à 325 Mbits/s	Non disponible Jusqu'à 360 Mbits/s
Homologues VPN IPsec	10 ; 25*	250	750	5000	5000
Homologues VPN SSL * (inclus/maximum)	2/25	2/250	2/750	2/2500	2/5000
Sessions simultanées	10 000 ; 25 000*	50 000 ; 130 000*	280 000	400 000	650 000
Nouvelles sessions par seconde	3 000	6 000	9 000	20 000	28 000
Ports réseaux intégrés	Commutateur Fast Ethernet 8 ports (dont 2 ports PoE)	5 ports Fast Ethernet	4 ports Ethernet Gigabit + 1 port Fast Ethernet	4 ports Ethernet Gigabit + 1 port Fast Ethernet	8 ports Ethernet Gigabit, fibre SFP et 1 port Fast Ethernet
Interfaces virtuelles (VLAN)	3 (ligne réseau désactivée) / 20* (ligne réseau activée)	50/100 * 150	200	250	
Contextes de sécurité (intégrés / maximum)	0/0	0/0 (Base) ; 2/5 (Security Plus)	2/20	2/50	2/50
Haute disponibilité	Non supportée / Actif/Veille* à inspection d'état	Non supportée / Actif/Actif et Actif/Veille*	Actif/Actif et Actif/Veille	Actif/Actif et Actif/Veille	Actif/Actif et Actif/Veille
Emplacement d'extension	1, SSC	1, SSM	1, SSM	1, SSM	0

1.6 Chemin de migration pour le serveur de sécurité Cisco PIX 515E

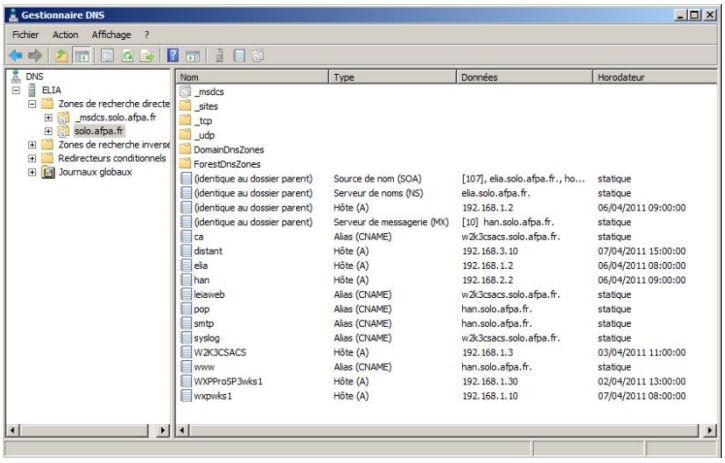
Cisco PIX 515E R/DMZ	**ASA5510**-K8	**Cisco ASA 5510 Firewall Edition, 3 ports Fast Ethernet, 250 homologues VPN IPsec et 2 SSL, DES**
	ASA5510-BUN-K9	**Cisco ASA 5510 Firewall Edition, 3 ports Fast Ethernet, 250 homologues VPN IPsec et 2 SSL, 3DES/AES**
	ASA5510-SEC-BUN-K9	**Cisco ASA 5510 Firewall Edition Security Plus, 5 ports Fast Ethernet, 250 homologues VPN IPsec et 2 SSL, haute disponibilité Actif / Veille, 3DES/AES**
	ASA5510-AIP10-K9	**Cisco ASA 5510 IPS Edition, module AIP SSM 10, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-CSC10-K9	**Cisco ASA 5510 Anti X Edition, module CSC SSM 10, 50 utilisateurs antivirus / anti logiciels espions avec un an d'abonnement, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-CSC20-K9	**Cisco ASA 5510 Anti X Edition, module CSC SSM 20, 500 utilisateurs antivirus / anti logiciels espions avec un an d'abonnement, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-SSL50-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 50 SSL, services de firewall, 3 ports Fast Ethernet**
	ASA5510-SSL100-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 100 SSL, services de firewall, 3 ports Fast Ethernet**
	ASA5510-SSL250-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 250 SSL, services de firewall, 3 ports Fast Ethernet**
Cisco PIX 515E UR/FO/FO AA	**ASA5510**-SEC-BUN-K9	**Cisco ASA 5510 Firewall Edition Security Plus, 5 ports Fast Ethernet, 250 homologues VPN IPsec et 2 SSL, haute disponibilité Actif / Veille, 3DES/AES**
	ASA5510-AIP10-K9	**Cisco ASA 5510 IPS Edition, module AIP SSM 10, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-CSC10-K9	**Cisco ASA 5510 Anti X Edition, module CSC SSM 10, 50 utilisateurs antivirus / anti logiciels espions avec un an d'abonnement, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-CSC20-K9	**Cisco ASA 5510 Anti X Edition, module CSC SSM 20, 500 utilisateurs antivirus / anti logiciels espions avec un an d'abonnement, services de firewall, 250 homologues VPN IPsec et 2 SSL, 3 ports Fast Ethernet**
	ASA5510-SSL50-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 50 SSL, services de firewall, 3 ports Fast Ethernet**
	ASA5510-SSL100-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 100 SSL, services de firewall, 3 ports Fast Ethernet**
	ASA5510-SSL250-K9	**Cisco ASA 5510 SSL/IPsec VPN Edition, 250 homologues VPN IPsec et 250 SSL, services de firewall, 3 ports Fast Ethernet**

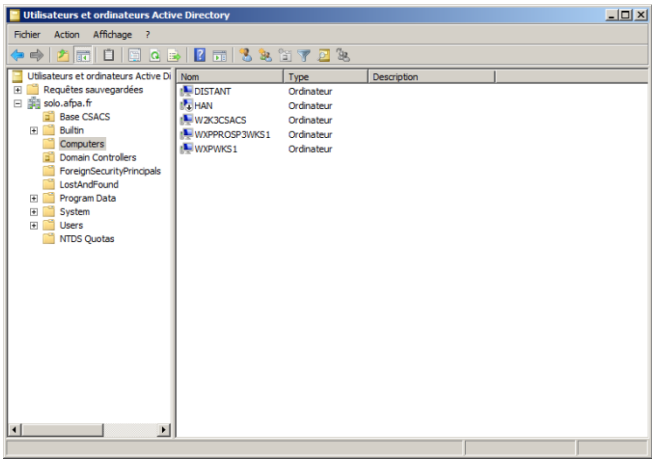
2. Comparatifs des principaux Firewall matériels du marché

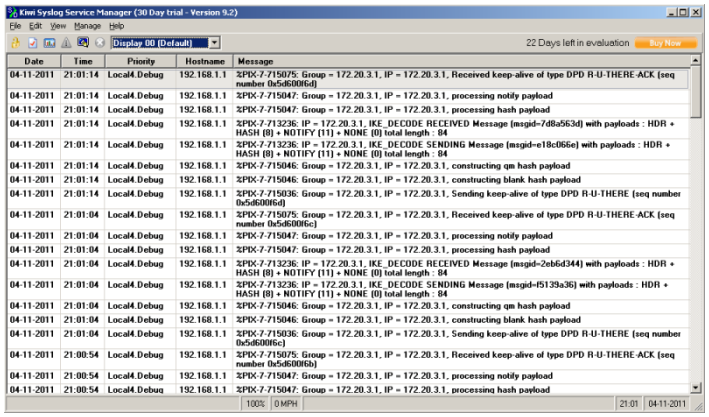
	ARKOON **A500**	NETASQ **U250**	CHECKPOINT **IP 297**	JUNIPER **S SG350m**	CISCO **ASA 5520**
Débit firewall	500Mo/s	850Mo/s	1,5Go/s	550Mo/s	450Mo/s
Débit VPN	150Mo/s	190Mo/s	1Go/s	225Mo/s	225Mo/s
interfaces	2fa, 3Gb, console	6G	6/8 fa	4 fa	1 fa et 4 G
nb de VPN simultané		1000		500	750
connexion VPN simultanée		512		350	
taille flash	48Mo				256Mo
RAM	256Mo			256Mo	2Go
firewall	stateful		stateful		stateful
protocole de routage	static, RIP, OSPF, BGP	static, RIP, OSPF, BGP	static, RIP, OSPF, BGP	static, RIP, OSPF, BGP	static, RIP, OSPF, BGP
algorithme de chiffrement	DES, 3DES, AES, blowfish, SSL	DES, 3DES, AES, blowfish, SSL	DES, 3DES, AES, blowfish, SSL ,CAST	DES, 3DES, AES	DES, 3DES, AES, SSL
méthode d'authentification	SSH, radius LDAP, certificats X.509	SSH, radius LDAP, certificats X.509	SSH, radius LDAP, certificats X.509	radius LDAP, certificats X.509	SSH, radius LDAP, certificats X.509
HDD	40Go	70Go	40Go		
principal caractéristique	firewall, VPN, IPS, PAT/NAT, filtrage de MAC, IDS, filtrage mail/antispam, 802.1q,	firewall, VPN, IPS, PAT/NAT, antispam, mode transparent, 802.1q	firewall, VPN, IPS	firewall, VPN, IPS, PAT/NAT, 802.1q, filtrage d'URL,	firewall, VPN, IPS, PAT/NAT, mode transparent, 802.1q
gestion graphique	Arkoon manager				ASDM
prix		2999€ HT	9642 $ (6695€)	4O5O€ HT	4 900 €

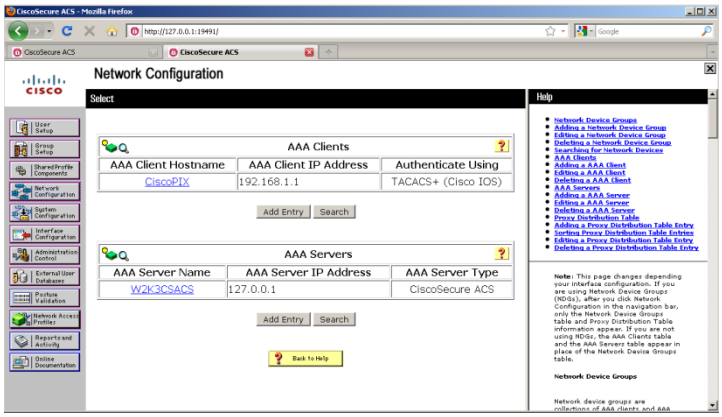
3. Capture d'écran de nos tests

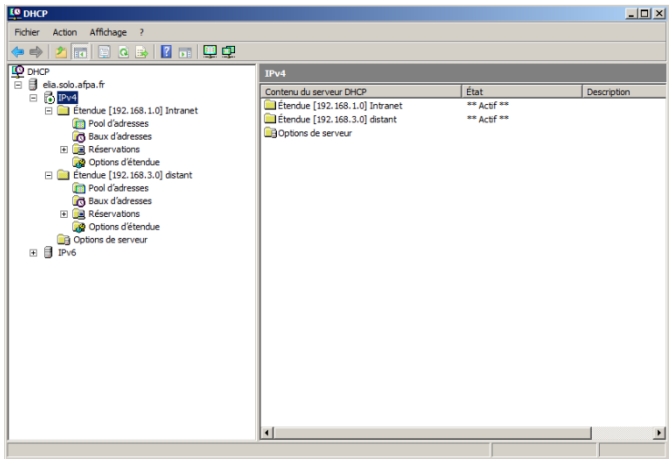
3.1 Nos différents serveurs

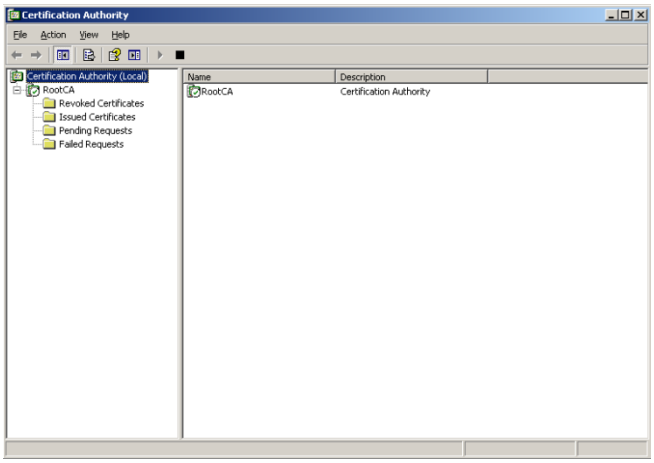


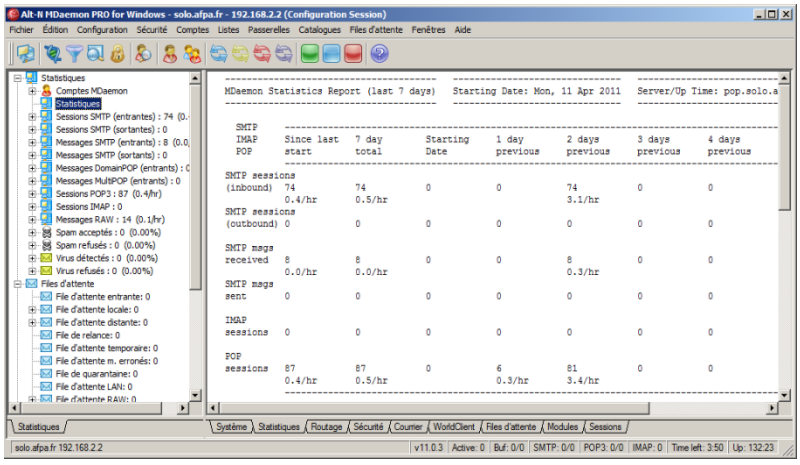






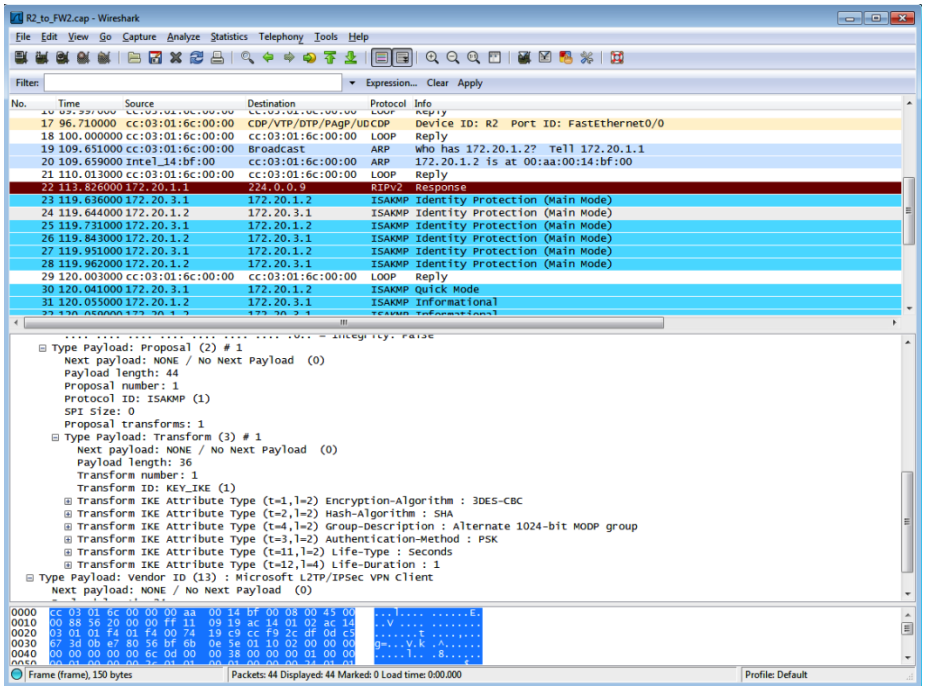




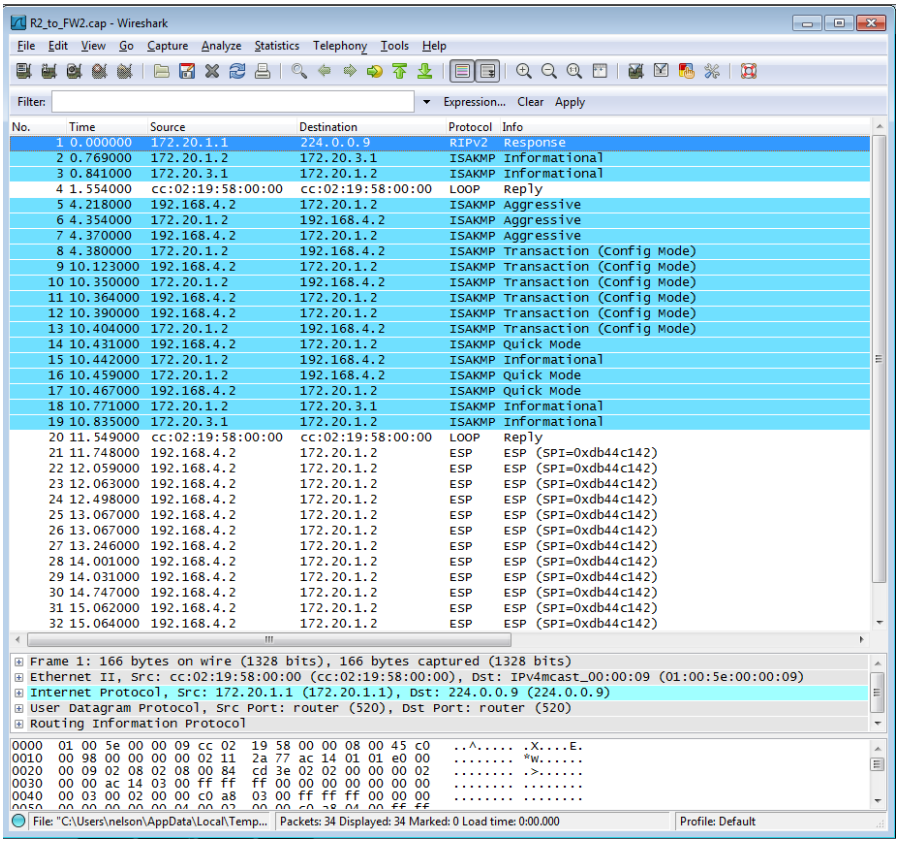


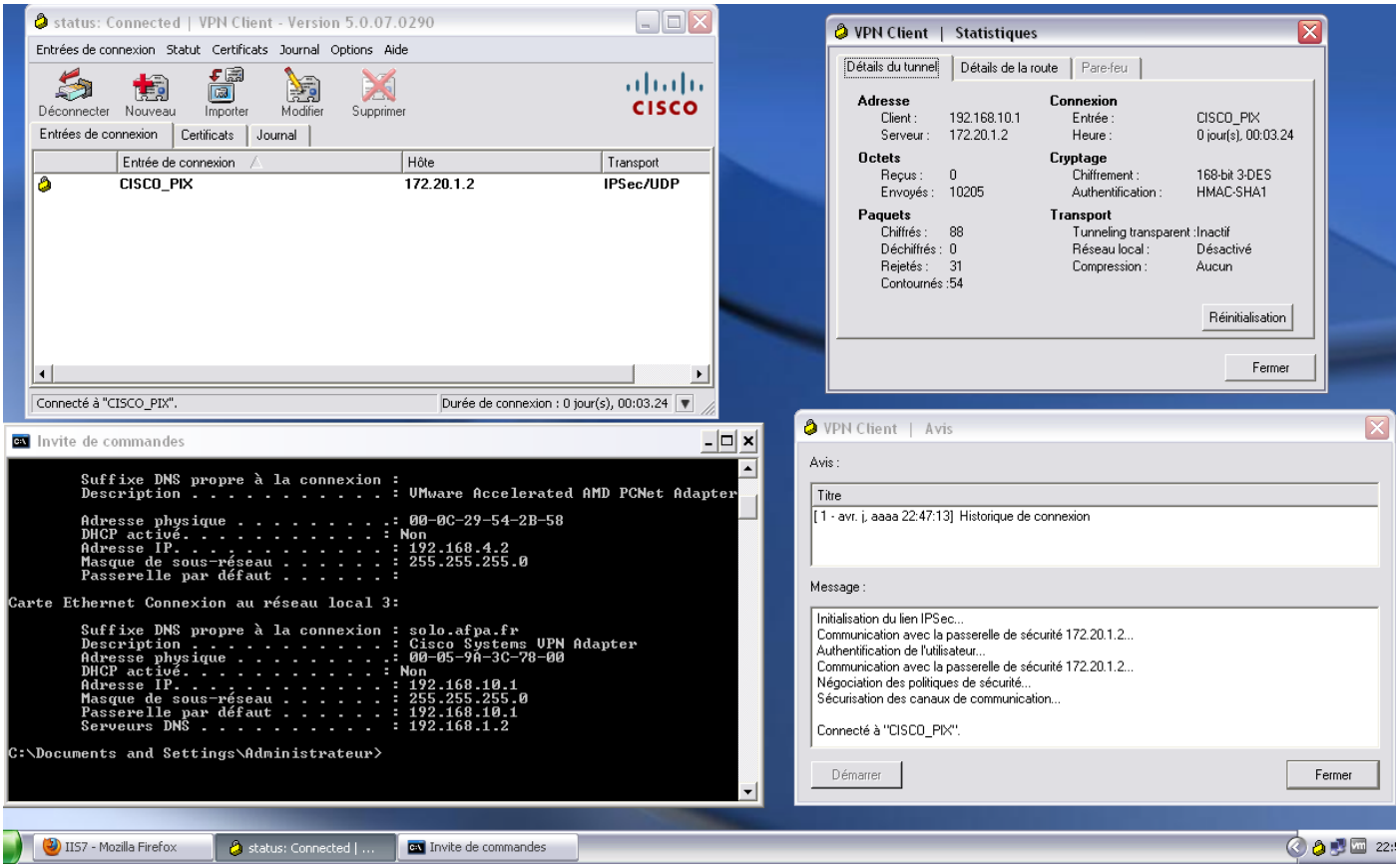
3.2 VPN site à site et VPN client

Construction du tunnel entre le réseau interne et le site distant. Nous pouvons voir sur cette capture wireshark les négociations de la phase 1 Isakmp. Sur l'image de droite un monitoring ASDM nous montre l'état des deux tunnels IKE et IPsec



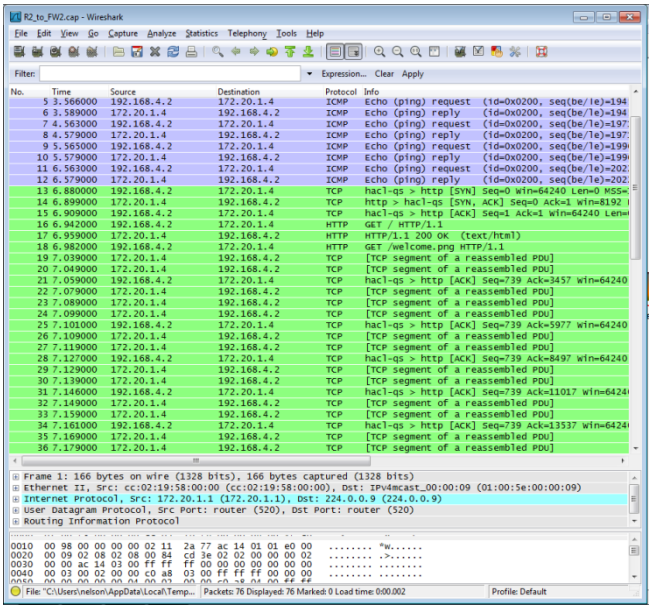
Négociations entre le PIX (172.20.1.2) et un remote (192.168.4.2) pour l'établissement d'une liaison VPN. Le monitoring ASDM nous montre l'activité des deux tunnels.

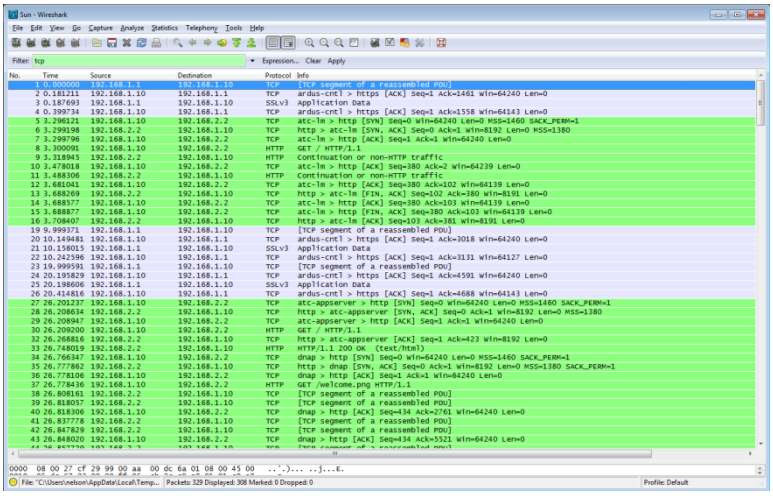




Nous sommes sur le bureau du Client VPN. Nous pouvons l'interface de connexion Cisco VPN Client en haut à gauche. Après connexion, une carte réseau virtuelle est créée et une adresse IP appartenant au pool configuré sur le PIX est attribuée à notre remote. En bas à droite, un petit icône informe l'utilisateur qu'il est connecté via VPN au site.

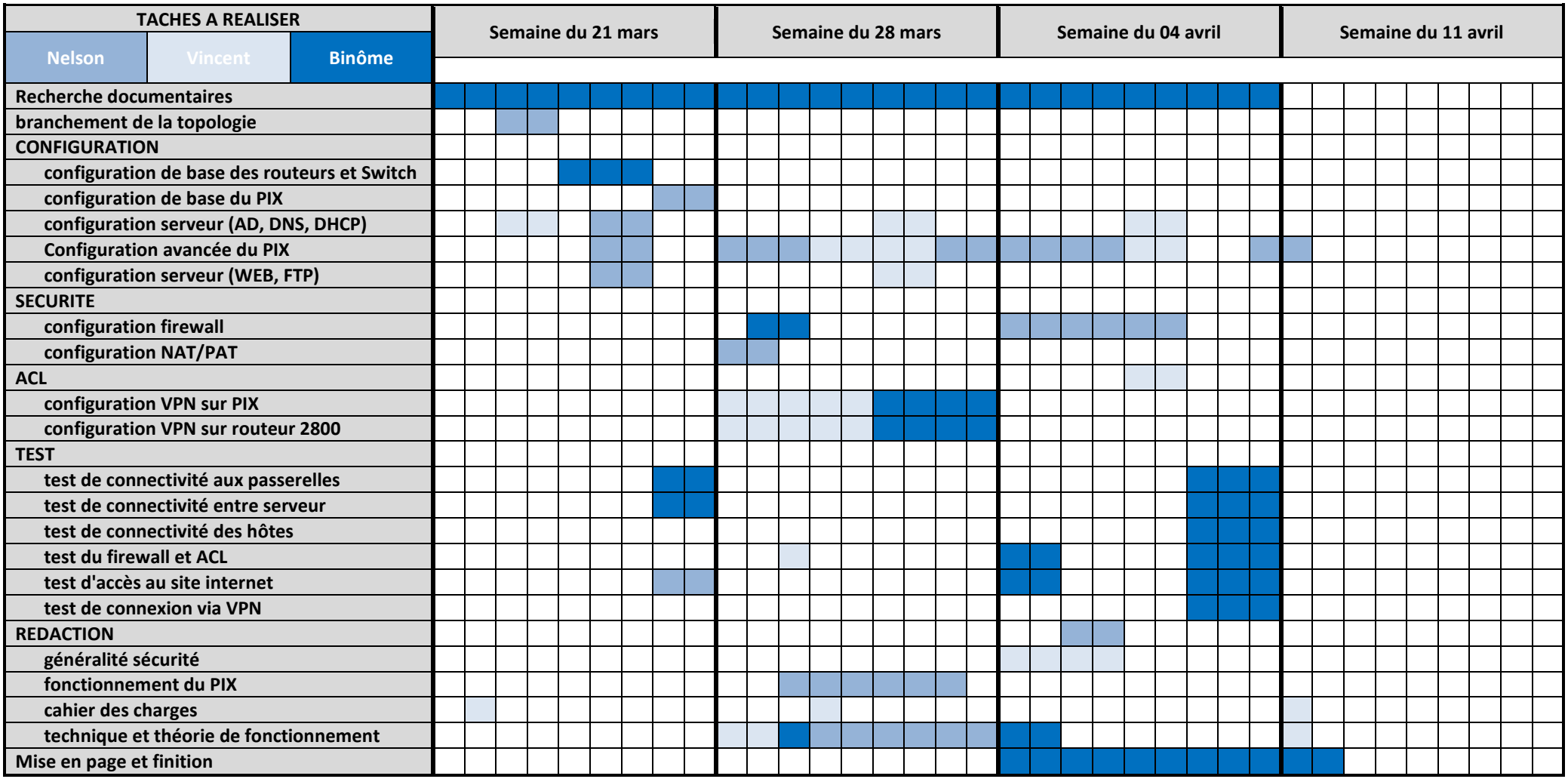
3.3 Captures diverses





A gauche, nous pouvons voir un extérieur qui accèdent au serveur web de la DMZ (ce serveur est accessible via l'adresse IP 172.20.1.4). Sur la droite, un utilisateur interne tente d'accéder à internet et se voit demander une authentification proxy.

4. Planning prévisionnel



VIII. Synthèse documentaire

Sujet	Langue	Type de ressource	Lien	§ pertinent	Commentaire	Intérêt
Politique de sécurité	Français et anglais	Cours Cisco Internet	http://www.cisco.com/web/learning/netacad/index.html	Semestre4 § 4	Petite révision, ça ne fait pas de mal	A lire
	Français	Livre	CISCO - Protocoles, concepts de routage et sécurité - CCNA 640-802	§ 11	Administration et sécurité	bof
	Français	Livre	CISCO - Sécurité des routeurs et contrôle du trafic réseau	§ 1 et 2	Intro sécurité et notion de chiffrement	A lire
	Français	Livre	La sécurité des réseaux avec Cisco	entier	Comme son titre le suggère… vision de Cisco	génial
	Français	Internet	http://www.doc-etudiant.fr/Informatique/Securite-des-systemes-informatiques/Cours-La-securite-des-reseaux-44679.html	entier	Sécurité des réseaux	bien
	Français	Internet	http://www.doc-etudiant.fr/Informatique/Securite-des-systemes-informatiques/Memoire-Les-strategies-de-securite-et-systemes-de-protection-contre-les-intrusions-78248.html	entier	Version plus avancé que le précédent	bien
Configuration de base	Français	magazine	Hakin9 N°1/2009	Page 48 - 57	Débuter avec un pare-feu Cisco	bien
	Anglais	Internet	http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html	§ 2-4	Configuration par défaut	A lire
	Français	Internet	http://www.doc-etudiant.fr/Informatique/Securite-des-systemes-informatiques/Rapport-configuration-dun-PIX-CISCO-6990.html	Entier	Première approche du Pix	bof
	Anglais	Internet	http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html	Entier	Config de base Pix	A lire
	Français	Internet	http://www.brainbump.net/tutorials/voice/asdm-gns3.htm	entier	Config de base pour le Pix avec GNS3	génial
	Anglais	Internet	http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html	§ 13-1	Commande de base IPv6 pour le Pix	A lire
	Anglais	Internet	http://it-audit.sans.org/community/papers/auditing-cisco-pix-firewall_31	entier	Fonctionnalité du Pix	bof
Configuration avancée	Anglais	Internet	http://it-audit.sans.org/community/papers/security-audit-cisco-pix-515-firewall_165	Entier	Audit sur fonctionnalité avancé du Pix 515	A lire
	Anglais	Internet	http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html	§ 10	Configuration routage IP	A lire
	Anglais	Livre	CCSP CSPFA Cisco Secure PIX Firewall Advanced Student Guide Version2.1(2002)	§ 15	Configuration VPN	A lire
	Anglais	Internet	http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html	§ 29	Configuration IPsec et ISAKMP	A lire
	Français	Internet	http://www.doc-etudiant.fr/Informatique/Reseaux-informatiques/Cours-Supprimer-mot-pass-r-cisco-81453.html	Entier	Récupération config et mot de passe	Bien
	Anglais	Internet	http://www.ekours.fr/index.php?option=com_content&task=view&id=133&Itemid=54	Entier	Intérêt d'une solution Pix Failover	Bien
	Anglais	Internet	http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094e7e.shtml	Entier	Guide config Tacacs et Radius	A lire
	Anglais	Internet	http://www.cisco.com/web/FR/documents/pdfs/guides/GuidedemigrationduPIXverslASA.pdf	Entier	Migration Pix 500 vers ASA 5500	A lire
	Anglais	Livre	Cisco PIX CCSP Secure Firewall Advanced Exam Certification Guide (CCSP Self-Study)	Entier	Supplément lecture pour curieux	Bien
	Anglais	Livre	Cisco - CCNA 640-553 Security Official Exam Certification Guide(2008)	Entier	Supplément lecture pour curieux	Bien
	Anglais	Livre	Cisco ASA All in One Firewall IPS Anti X and VPN Adaptive Security Appliance 2nd.(2009)	Entier	Supplément lecture pour curieux	Bien
	Anglais	Livre	CCSP CSPFA Self-Study Cisco Secure PIX Firewall Advanced Exam Certification Guide(2003)	Entier	Supplément lecture pour curieux	Bien
	Anglais	Livre	CCSP CSVPN Cisco Secure Virtual Private Networks Student Guide Version4.7(2005)	Entier	Supplément lecture pour curieux	Bien
	Anglais	Livre	CCSP CSVPN Self-Study Cisco Secure VPN Exam Certification Guide(2003)	Entier	Supplément lecture pour curieux	Bien

IX. Glossaire

A

AAA (Authentication, authorization, and accounting):
Eléments de sécurité généralement utilisés pour offrir un accès sécurisé aux ressources :
• Authentication (Authentification) : validation de l'identité d'un utilisateur ou d'un système (hôte, serveur, commutateur ou routeur).
• Authorization (Autorisation) : moyen permettant d'accorder l'accès à un réseau à un utilisateur, un groupe d'utilisateurs, un système ou un programme.
• Accounting (Gestion) : processus permettant d'identifier l'auteur ou la cause d'une action spécifique, tel que le pistage des connexions d'un utilisateur et la journalisation des utilisateurs du système.

Analyse de risque :
Processus comprenant l'identification des risques en matière de sécurité, leur impact et l'identification des zones nécessitant une protection.

Attaque par interruption de service (DoS):
Action malveillante visant à empêcher le fonctionnement normal de tout ou partie d'un réseau ou d'un système hôte. Cette attaque peut être comparée à une personne qui composerait sans arrêt le même numéro de téléphone pour saturer cette ligne.

Autorité de certification (CA):
Entité de confiance chargée de signer les certificats numériques et d'attester de l'identité d'autres utilisateurs autorisés.

C

CBAC (Context-Based Access Control):
Fonction intégrée au logiciel IOS de Cisco offrant le filtrage avancé de session de paquets pour tout le trafic routable. En configurant des ACL, il est possible d'autoriser ou de refuser le traitement ou le transfert du trafic.

Certificat :
Message signé numériquement au moyen d'une clé privée d'une tierce partie de confiance (voir autorité de certification) et indiquant qu'une clé publique spécifique appartient à une personne ou à un système possédant un nom et un ensemble d'attributs précis.

CHAP (Challenge Handshake Authentication Protocol):
Protocole d'authentification permettant d'empêcher les accès non autorisés. Le protocole CHAP authentifie et identifie l'entité distante. Le routeur ou le serveur d'accès détermine ensuite si l'utilisateur peut être autorisé à accéder au réseau.

Clé cryptographique :
Code numérique servant au cryptage, au décryptage et à la signature d'informations.

Clé privée :
Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé doit demeurer secrète et ne doit être connue que de son propriétaire.

Clé publique :
Code numérique utilisé pour décrypter les données et vérifier les signatures numériques. Cette clé peut être diffusée librement.

Compromission :
Dans le domaine de la sécurité informatique, ce terme signifie l'attaque d'un réseau par la violation de la politique de sécurité.

Confidentialité des données :
Moyen permettant de garantir que seules les entités autorisées peuvent voir les paquets de données dans un format intelligible.
Processus de protection des données d'un réseau contre l'espionnage ou l'altération.
Dans certains cas, la séparation des données à l'aide de technologies de tunnellisation, telles que GRE (generic routing encapsulation) ou le L2TP (Layer 2 Tunneling Protocol), offre une confidentialité des données efficace. Toutefois, il est parfois nécessaire d'augmenter la confidentialité à l'aide de technologies de cryptage numérique et de protocoles tels qu'IPsec, en particulier lors de la mise en œuvre de VPN.

Contrôle d'accès :
Limitation du flux de données des ressources d'un système uniquement vers les personnes, programmes, processus autorisés ou vers d'autres systèmes du réseau. Les ensembles de règles de contrôle d'accès des routeurs Cisco sont appelées listes de contrôle d'accès ou ACL.

Contrôle de la sécurité :
Procédure de sécurisation du réseau au moyen de tests réguliers et de SPA (Security Posture Assessments).

Cryptage :
Codage des données empêchant leur lecture par une autre personne que le destinataire prévu. De plus, les données sont uniquement lisibles après avoir été correctement décryptées.

Cryptographie :
Science de l'écriture et de la lecture de messages codés.

D - F

DES (Data Encryption Standard):
Système de cryptage à clé secrète normalisé par le National Institute of Standards and Technology (voir NIST et triple DES).

Diffie Hellman :
Système à clé publique permettant à deux utilisateurs ou équipements réseau d'échanger des clés publiques via un support non sécurisé.

DMZ (Demilitarized zone):
Sous-réseau isolé du réseau local par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Extranet :
Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet se fait via Internet, par une connexion sécurisée avec mot de passe dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise

En-tête d'authentification :
En-tête IPsec permettant de vérifier que le contenu d'un paquet n'a pas été modifié pendant le transport.

Filtrage :
Recherche dans le trafic réseau de certaines caractéristiques, telles que l'adresse source, l'adresse de destination ou le protocole, afin de déterminer, selon les critères définis, si le trafic de données concerné est accepté ou bloqué.

Filtrage de paquets :
Mécanisme de contrôle paquet par paquet du trafic routable.

G - I

GRE (Generic Routing Encapsulation):
Protocole de tunnellisation développé par Cisco permettant d'encapsuler des paquets utilisant de nombreux protocoles différents dans des tunnels IP, afin de créer un lien point à point virtuel entre des points distants et des routeurs Cisco via un réseau IP.

Hyperviseur :
Plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une machine physique en même temps.

Identité :
Identification précise des utilisateurs, hôtes, applications, services et ressources du réseau. Les nouvelles technologies, telles que les certificats numériques, les cartes à puces, les services répertoire jouent un rôle de plus en plus important dans les solutions d'identification.

IDS (Intrusion Detection System):
Sentinelle de sécurité en temps réel (semblable à un détecteur de mouvement) protégeant le périmètre du réseau, les extranets et les réseaux internes de plus en plus vulnérables. Les systèmes IDS analysent le flux de données du réseau à la recherche de signatures d'attaques ou d'activités considérées comme non autorisées, déclenchent l'alarme et lancent les actions nécessaires face à cette activité.

IETF (Internet Engineering Task Force):
Organisme de normalisation responsable de la conception de protocoles pour Internet. Les publications émises par l'IETF s'intitulent des RFC (Request for Comments).

Intégrité :
Moyen permettant de garantir que les données n'ont pas été modifiées, si ce n'est par les personnes explicitement autorisées à le faire. Le terme "intégrité du réseau" signifie qu'aucun service ou aucune activité contraire à la politique de sécurité n'est permise.

Intégrité des données :
Processus permettant de garantir que les données n'ont pas été modifiées ou détruites lors du transport via le réseau.

Intranet :
Réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle utilisant les techniques de communication d'Internet (IP, serveurs HTTP). Dans les grandes entreprises, l'intranet fait l'objet d'une gouvernance particulière en raison de sa pénétration dans l'ensemble des rouages des organisations.

IP (Internet Protocol):
Protocole basé sur l'utilisation de paquets permettant l'échange de données via des réseaux informatiques.

IPsec :
Ensemble de normes de sécurité offrant des services de confidentialité et de d'authentification au niveau de la couche IP (Internet Protocol).

ISAKMP (Internet Security Association and Key Management Protocol):
Protocole de gestion de clés pour IPsec. Ce protocole, nécessaire à la mise en œuvre complète d'IPsec, est également appelé IKE (Internet Key Management).

K - N

Kerberos :
Protocole d'authentification réseau à clé secrète développé par le MIT (Massachusetts Institute of Technology), basé sur l'utilisation de l'algorithme de cryptage DES pour le cryptage et une base de données de clés centralisée pour l'authentification.

L2F (Layer 2 Forwarding Protocol):
Protocole gérant la mise en place de réseaux virtuels privés commutés via Internet.

L2TP (Layer 2 Tunneling Protocol):
Norme IETF combinant les caractéristiques du protocole L2F de Cisco (Layer 2 Forwarding Protocol) et le protocole PPTP de Microsoft (Point-to-Point Tunneling Protocol) pour la mise en œuvre des VPN.

MD5 (Message Digest 5):
Algorithme de hachage utilisé pour l'authentification de données et la vérification de l'intégrité des communications.

NAT (Network Address Translation):
Mécanisme consistant à convertir une adresse IP en une autre. Le NAT est essentiellement utilisé pour connecter un espace d'adressage interne utilisant un protocole différent d'un autre réseau, tel qu'Internet.

Non-répudiation :
Caractéristique d'un système cryptographique permettant d'empêcher qu'un expéditeur puisse nier ultérieurement avoir envoyé un message ou effectué une action spécifique.

P

PAP (Password Authentication Protocol):

Protocole d'authentification permettant à des postes PPP de s'authentifier les uns auprès des autres. Le routeur distant qui effectue une tentative de connexion sur le routeur local doit envoyer une requête d'authentification. Contrairement à CHAP, PAP ne crypte pas le mot de passe et le nom d'hôte ou d'utilisateur. PAP détermine si un mot de passe est valide ou non.

Pare-feu :
Système matériel ou logiciel utilisé pour contrôler le trafic de données entre deux réseaux.

Périmètre de sécurité :
Périmètre dans lequel des contrôles de sécurité sont effectués afin de protéger les équipements réseau.

Ping :
Commande permettant de déterminer la présence et l'état de fonctionnement d'un autre système.

Ping of Death (Ping de la mort):
Attaque par interruption de service (DoS) consistant en l'envoi d'un paquet Ping de taille surdimensionnée, dans le but d'entraîner le blocage de la machine réceptrice lors de la tentative de réassemblage du paquet de données surdimensionné.

PKI (Public Key Infrastructure):
Infrastructure de gestion de clés offrant un environnement sûr et fiable.

Politique de sécurité :
Ensemble de directives de haut niveau permettant de contrôler le déploiement des services réseau. La maintenance et l'audit du réseau font également partie de la politique de sécurité.

PPP (Point-to-Point Protocol):
Protocole normalisé d'encapsulation de paquets IP via des liens point à point.

PPTP (Point-to-Point Tunneling Protocol):
Norme IETF soutenue par Microsoft pour la mise en œuvre des VPN à partir du système d'exploitation Windows 95/98 vers une passerelle VPN.

Proxy :
Equipement (mandataire) effectuant une tâche à la place d'un autre équipement. Dans le domaine des firewalls, le proxy est un processus effectuant un certain nombre de contrôles sur le trafic entrant. Ce mécanisme peut nuire aux performances du firewall.

R

RADIUS (Remote Access Dial-In User Service):
Protocole développé par Livingston Enterprises Inc., utilisé comme protocole d'authentification et de gestion de serveur d'accès.

Réinitialisation TCP :
Réponse possible à une attaque de hacker d'une sonde Cisco Secure IDS ou d'un routeur Cisco IOS Firewall. Une commande est émise par ces équipements afin d'arrêter la connexion par laquelle l'attaque est effectuée, obligeant ainsi l'attaquant à établir une nouvelle connexion.

RSA (Rivest, Shamir, Adelman):
Algorithme de cryptage à clé publique permettant de crypter ou de décrypter des données et d'appliquer ou de vérifier une signature numérique.

S

SHA (Secure Hash Algorithm):
Algorithme de hachage utilisé pour l'authentification et la vérification de l'intégrité des communications.

Signature d'attaque :
Système d'identification d'activité malveillante sur le réseau. Les paquets de données entrants sont examinés en détail à la recherche de modèles logarithmiques identiques.

Signature d'attaque :
Système d'identification d'activité malveillante sur le réseau. Les paquets de données entrants sont examinés en détail à la recherche de modèles logarithmiques identiques.

Signature numérique :
Chaîne de bits ajoutée à un message électronique (hachage crypté) permettant l'authentification et l'intégrité des données.

Spoofing (usurpation):
Tentative d'accès à un système réseau par usurpation (utilisateur, système ou programme autorisés).

Syslog :
Protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.

T

TACACS+ (Terminal Access Controller Access Control System Plus):
Protocole AAA principalement utilisé pour la gestion des connexions commutées.

Triple DES :
Algorithme DES combiné à une, deux ou trois clés pour le cryptage/décryptage de paquets de données.

Tunnel :
Connexion sécurisée et cryptée entre deux points passant par un réseau public ou tiers.

V

VPN (Réseau privé virtuel):
Réseau garantissant un trafic IP sécurisé via un réseau TCP/IP public grâce au cryptage des données entre les deux réseaux concernés. Le VPN utilise la tunnellisation pour crypter les informations au niveau IP.

Vulnérabilité :
Faille au niveau des procédures de sécurité, de la conception ou la mise en œuvre du réseau, pouvant être exploitée pour contourner la politique de sécurité d'une entreprise.