Cisco Systems

SAFE Blueprint SMB

SAFE

Extension d'un **schéma directeur de sécurité** aux **réseaux de petite taille et de taille moyenne** ainsi qu'aux **réseaux distants**

Cisco Systems

LIVRE BLANC

SAFE

Extension d'un **schéma directeur de sécurité** aux **réseaux de petite taille et de taille moyenne** ainsi qu'aux **réseaux distant**

Table des matières

Auteurs

Les auteurs de ce Livre Blanc, Sean Convery et Roland Saville, sont également les architectes qui ont présidé à sa mise en œuvre pilote au siège social de Cisco à San Jose en Californie, Etats-Unis. Sean et Roland sont tous deux architectes de réseau, spécialisés dans les VPN et les questions de sécurité.

Résumé

L'objectif principal de ce livre blanc est de présenter aux personnes intéressées des pratiques optimales pour le design et la mise en œuvre de réseaux sécurisés. L'original du livre blanc SAFE pour les grandes entreprises est disponible à l'adresse suivante : http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm.

Le document suivant reprend les mêmes principes et les adapte aux réseaux de plus petite taille, aux installations des filiales des grandes entreprises ou aux déploiements de réseaux autonomes sécurisés de petite taille ou de taille moyenne. Il comprend également des informations sur les réseaux d'accès distants nécessaires aux télétravailleurs ou aux travailleurs mobiles. La lecture préalable du livre original SAFE pour les grandes entreprises n'est pas indispensable car toutes les questions abordées dans le document original sont reprises, lorsqu'elles sont nécessaires, dans le présent article.

SAFE adopte une démarche de défense en profondeur adaptée au design de réseaux sécurisés. Ce type de design met l'accent sur l'anticipation des menaces et les méthodes d'atténuation s'y rapportant, plutôt que sur une approche du type "Mettez le firewall ici, le système de détection d'intrusion là." Cette stratégie a pour conséquence une démarche sécuritaire par couches dans laquelle la défaillance d'un système de sécurité a peu de chance de compromettre les ressources du réseau. SAFE s'appuie sur des produits Cisco ainsi que sur ceux de ses partenaires.

Après une présentation générale de l'architecture, cet article aborde les designs spécifiques considérés. Les deux premières sections de chaque module décrivent les périphériques clés et les menaces prévisibles avec les diagrammes élémentaires d'atténuation. Vient ensuite une analyse technique détaillée du design, suivie d'autres techniques de réduction des risques et stratégies de migration plus détaillées. L'annexe A décrit en détail le laboratoire de validation de SAFE et présente des extraits de configuration. L'annexe B est une introduction à la sécurité réseau. Nous invitons ceux de nos lecteurs qui ne seraient pas familiarisés avec les concepts élémentaires de la sécurité réseau, à lire cette section avant le reste du document. L'annexe C contient un glossaire et des définitions des termes techniques utilisés dans cet article.

Ce livre blanc insiste particulièrement sur les menaces qui pèsent sur les réseaux actuels. Les concepteurs de réseaux qui comprennent ces menaces peuvent décider de manière plus rationnelle où et comment déployer les technologies d'atténuation des risques. Sans une parfaite compréhension des menaces qui visent la sécurité des réseaux, les mesures adoptées sont souvent déployées de manière incorrecte. Parce qu'il présente une démarche d'atténuation des menaces, cet article devrait apporter aux concepteurs de réseau des informations qui leur permettront de faire les bons choix en matière de sécurité réseau.

Public visé

Malgré sa nature technique, cet article peut être lu à plusieurs niveaux de détail qui dépendent du lecteur. Un administrateur réseau, par exemple, pourra lire les sections d'introduction de chaque domaine afin de dégager une bonne vue d'ensemble des stratégies et des problèmes de design de réseaux sécurisés. Un ingénieur réseau ou un concepteur lira cet article dans son intégralité pour y puiser des informations de design et une analyse détaillée des menaces, que viennent renforcer de véritables extraits de configuration des unités impliquées. Cet article peut également servir aux lecteurs du livre blanc SAFE original qui seraient intéressés par le design de réseau d'une taille moindre. Il peut être utile de lire en premier les sections d'introduction de l'article puis de passer directement au type de réseau que vous envisagez de déployer.

Avertissements

Cet article suppose que vous disposiez déjà d'une politique de sécurité active. Cisco Systems ne recommande pas de déployer des technologies de sécurité sans une politique de sécurité correspondante. Cet article traite directement des besoins des réseaux de petite taille et de taille moyenne, ainsi que des réseaux d'utilisateurs distants. Nous invitons les lecteurs qui seraient intéressés par le design de grands réseaux d'entreprise à consulter l'original du livre blanc SAFE à l'adresse suivante : http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm.

Nous ne pouvons vous garantir qu'en respectant les consignes de cet article vous réaliserez un environnement sûr, pas plus que nous ne vous certifions que vous éviterez toute intrusion. La seule manière de garantir une sécurité absolue consiste à déconnecter votre système du réseau, à l'enfermer dans un coffrage en béton et à déposer le tout dans les coffres les plus secrets de la Banque de France. Vos données seront alors particulièrement bien protégées, bien qu'inaccessibles. Vous pouvez toutefois obtenir une protection raisonnable en mettant en place une bonne politique de sécurité, en suivant les consignes de cet article, en vous informant régulièrement des derniers développements concernant les communautés de pirates et la sécurité, et en appliquant des méthodes raisonnables d'administration système pour la maintenance et le contrôle des unités. Ceci comprend la sensibilisation à des questions pratiques de sécurité qui ne sont pas abordées de manière exhaustive dans le présent article.

Bien que les réseaux privés virtuels (VPN) soient compris dans cette architecture, ils ne sont pas décrits en détail. Les informations concernant, par exemple, les problèmes d'évolutivité, les stratégies de résilience ainsi que d'autres sujets propres aux VPN, ne sont pas abordés ici. Les lecteurs intéressés peuvent se référer au Livre blanc VPN SAFE à l'adresse Internet suivante : http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm.
De même, les stratégies d'authentification (y compris les autorités de certification [AC]) ne sont pas présentées de manière particulière dans cet article. Comme les VPN, les AC exigent des explications poussées que le présent article ne peut fournir sans sacrifier la qualité de la présentation de tous les autres domaines importants de la sécurité réseau. De plus, comme la plupart des réseaux n'ont toujours pas déployé des environnements AC parfaitement fonctionnels, il est important de voir comment, sans eux, il est possible de créer des réseaux sécurisés. Le commerce électronique est un autre domaine que cet article n'aborde pas. Les recommandations de réseau pour le commerce électronique varient peu en fonction de la taille de l'entreprise, et les réponses apportées par l'original du livre blanc SAFE sont tout à fait satisfaisantes. Enfin, certaines applications et technologies évoluées de réseau – comme les réseaux de diffusion de contenus, de cache et d'équilibrage de charge– ne sont pas abordées dans ce document. Bien qu'elles seront certainement employées dans l'architecture SAFE, le présent article ne passe pas en revue l'étendue de leurs besoins spécifiques en matière de sécurité.

SAFE utilise les produits de Cisco Systems et de ses partenaires. Toutefois, ce document ne fait pas spécifiquement référence à ces produits par leurs noms, mais désigne les divers composants selon leur destination fonctionnelle plutôt que par un numéro de modèle ou une appellation commerciale. Au cours de la validation de SAFE, les véritables produits ont été configurés dans le respect strict de l'implémentation de réseau décrite dans cet article. Le laboratoire et les résultats obtenus, ainsi que des extraits de la configuration spécifique du laboratoire, sont présentés dans l'annexe A, "Laboratoire de validation".

Dans cet article, le terme de "pirate" désigne une personne qui cherche à obtenir, sans autorisation, un accès aux ressources du réseau dans une intention délictueuse. Bien que "cyberpirate" soit généralement considéré comme plus approprié pour ce type de personne, le mot pirate est utilisé ici pour sa meilleure lisibilité.

Description générale de l'architecture

Eléments de design fondamentaux

SAFE émule de manière aussi proche que possible les besoins fonctionnels des réseaux actuels. Les décisions prises en matière d'implémentation se sont adaptées aux besoins de fonctionnalités des réseaux. Toutefois, les objectifs conceptuels suivants, présentés dans l'ordre des priorités, ont guidé le processus de décision.

- Sécurité et atténuation des attaques basées sur une politique
- Mise en œuvre de la sécurité sur l'ensemble de l'infrastructure (et pas seulement sur des périphériques de sécurité spécialisés)
- Déploiement rentable
- Gestion et reporting sécurisés
- Accès des utilisateurs et des administrateurs aux ressources critiques du réseau soumis à authentification et à autorisation
- Détection des intrusions pour les ressources critiques et les sous-réseaux

Avant toute chose, SAFE est une architecture de sécurité. Elle a pour objectif d'empêcher la plupart des attaques d'affecter de manière significative les précieuses ressources du réseau. Les attaques qui parviennent à passer la première ligne de défense ou qui émanent de l'intérieur du réseau doivent être précisément détectées et rapidement contenues afin de minimiser leurs effets sur le reste du réseau. Toutefois, tout en restant protégé, le réseau doit continuer à fournir de manière transparente les services qu'en attendent ses utilisateurs. Il est possible d'obtenir en même temps une bonne protection et un bon fonctionnement du réseau. L'architecture SAFE n'est pas une méthode révolutionnaire de design des réseaux, mais plus précisément un guide pour leur protection.

La présente architecture SAFE pour les réseaux de petite taille et de taille moyenne, ainsi que pour les réseaux à distance, a été conçue sans résilience. Les lecteurs intéressés par le design de réseaux sécurisés dans un environnement résilient pourront consulter l'original du Livre blanc SAFE (désigné par la suite par "SAFE Entreprise").

A de nombreux moments dans le processus de design du réseau, vous devrez choisir entre l'utilisation des fonctionnalités intégrées à un équipement de réseau et l'emploi d'un équipement fonctionnel dédié. La fonctionnalité intégrée est souvent intéressante car il est possible de l'implémenter sur des équipements existants, ou parce que les caractéristiques permettent l'interopérabilité avec le reste des unités afin de fournir une meilleure solution fonctionnelle. Les équipements dédiés sont souvent utilisés lorsque la fonctionnalité nécessaire demande une profondeur particulièrement évoluée ou lorsque le niveau de performance souhaité exige l'emploi d'un matériel spécialisé. La décision doit être prise en comparant la capacité et les fonctionnalités de l'équipement dédié à l'avantage d'une intégration de l'unité. Par exemple, il peut parfois être avantageux de préférer un routeur Cisco IOS ® intégré haute capacité avec un logiciel pare-feu IOS plutôt qu'un routeur IOS plus petit avec un pare-feu séparé. Dans cette architecture, nous utilisons les deux types de systèmes. Lorsque les exigences en matière de design n'imposent pas de choix particulier, nous avons préféré la fonctionnalité intégrée afin de réduire le coût global de la solution.

Le concept de module

Bien que la plupart des réseaux évoluent avec l'accroissement des besoins informatiques de l'entreprise, l'architecture SAFE utilise une approche modulaire entièrement nouvelle. Cette approche modulaire présente deux avantages majeurs : tout d'abord, elle permet à l'architecture d'envisager les relations de sécurité entre les différents blocs fonctionnels du réseau. Ensuite, elle permet aux concepteurs d'évaluer et de mettre en œuvre la sécurité module par module au lieu d'essayer d'achever l'ensemble de l'architecture en une seule étape. Pour chaque module, le concept de sécurité est décrit séparément, mais il est validé en tant que partie du design d'ensemble.

Bien que la plupart des réseaux ne puissent pas être facilement décomposés en modules bien définis, cette approche constitue un guide pour l'implémentation des différentes fonctions de sécurité dans tout le réseau. Les auteurs ne suggèrent pas aux ingénieurs de calquer leurs réseaux sur l'implémentation SAFE, mais plutôt d'utiliser une combinaison des modules décrits et de les intégrer dans leurs réseaux existants.

Les axiomes SAFE

Les routeurs sont des cibles

Les routeurs contrôlent l'accès de n'importe quel réseau vers chacun des autres réseaux. Ils font connaître les réseaux, filtrent les personnes qui peuvent les utiliser, et sont potentiellement les meilleurs amis des pirates. La protection des routeurs est un élément essentiel de tout déploiement de sécurité. Par nature, le routeur donne accès et vous devez, par conséquent, le protéger pour réduire la probabilité que sa sécurité puisse être directement compromise. Vous pouvez consulter d'autres articles qui concernent la protection des routeurs et vous apporteront des détails supplémentaires sur les sujets suivants :

- Verrouillage de l'accès Telnet à un routeur
- Verrouillage de l'accès SNMP (Simple Network Management Protocol) à un routeur
- Contrôle de l'accès à un routeur grâce à l'utilisation de TACACS+ (Terminal Access Controller Access Control System Plus)
- Désactivation des services inutiles
- Ouverture de sessions sur le routeur avec des droits appropriés
- Authentification des updates de routage

L'article le plus récent se rapportant à la protection des routeurs est consultable à l'adresse Internet suivante :
http://www.cisco.com/warp/public/707/21.html

Les commutateurs sont des cibles

Comme les routeurs, les commutateurs (aussi bien de niveau 2 et 3) relèvent d'une problématique de sécurité qui leur est propre. A la différence des routeurs, toutefois, il n'existe pas autant d'informations publiques sur les risques qui menacent les commutateurs et sur ce que l'on peut faire pour réduire ces risques. La plupart des techniques de protection présentées dans la section précédente, “Les routeurs sont des cibles”, s'appliquent également aux commutateurs. De plus, il est préférable de prendre les précautions suivantes :

- Si un port n'a pas besoin d'être utilisé en mode trunk, tous ses paramétrages doivent être désactivés et non pas mis en automatique. Cette configuration évite qu'une station puisse se définir en port trunk et reçoive tout le trafic qui devrait normalement transiter par un port trunk.
- Si vous utilisez une version ancienne du logiciel de votre commutateur Ethernet, vérifiez que les ports de réseau utilisent un numéro de réseau local virtuel (VLAN) que personne d'autre n'utilise sur le commutateur. Cette configuration empêche que les paquets qui portent le même label de réseau local virtuel que le port de réseau puissent atteindre un autre VLAN sans traverser une unité de la couche 3. Pour plus de renseignements, consultez le site http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
- Désactivez tous les ports inutilisés d'un commutateur. Cette configuration évite qu'un pirate se connecte à un port inutilisé et puisse ainsi communiquer avec le reste du réseau.
- Evitez d'utiliser les VLAN comme seul moyen de garantir l'accès entre deux sous-réseaux. La possibilité d'une erreur humaine – ainsi que le fait que les considérations de sécurité n'ont pas été intégréesau design des réseaux locaux virtuels et de leurs protocoles de labelisation – rend leur utilisation peu recommandable dans les environnements sensibles. Lorsque les VLAN sont nécessaires dans le déploiement des dispositifs de protection, pensez à vérifier soigneusement leur configuration en fonction des conseils donnés plus haut.

Dans un réseau local virtuel, les private VLAN permettent de protéger un peu mieux certaines applications de réseau. Les VLAN de type " private VLAN " fonctionnent en réduisant le nombre de ports d'un réseau local virtuel autorisés à communiquer avec d'autres ports du même VLAN. Les ports isolés d'un réseau local virtuel ne peuvent communiquer qu'avec les ports promiscuous. Les ports appartenant à une communeauté ne peuvent communiquer qu'avec les autres membres de la même communauté et avec les ports promiscuous. Les ports promiscuous peuvent communiquer avec n'importe quel port. Ceci est un moyen efficace d'atténuer les effets d'une attaque réussie sur une station unique. Imaginons un segment de services publics standard avec Web, protocole FTP et serveur DNS. Si un pirate parvient à s'introduire dans le serveur DNS, il pourra attaquer les deux autres stations sans avoir à repasser par le pare-feu. Avec des private VLAN, si l'un des systèmes a été corrompu, il ne pourra pas communiquer avec les deux autres systèmes. Les seules cibles que le pirate pourra attaquer seront les stations situées de l'autre côté du pare-feu. Comme ils réduisent la connectivité de la couche de niveau 2, les private VLAN compliquent la résolution des problèmes de réseau. Souvenez-vous que les private VLAN ne sont pas supportés par tous les commutateurs Ethernet disponibles actuellement sur le marché, notamment la plupart des commutateurs "économiques".

Les stations sont des cibles

Cible la plus probable pendant une attaque, la station est un des éléments les plus difficiles à gérer du point de vue de la sécurité. Les plates-formes matérielles sont nombreuses, de même que les systèmes d'exploitation et les applications, chacune de ces dernières présentant des mises à jour, des " patches " et des correctifs disponibles à des instants différents. Les stations fournissent les services d'application aux autres stations qui les leur demandent, ce qui les rend extrêmement visibles sur le réseau. De nombreuses personnes ont, par exemple, visité le site de la Maison blanche (www.whitehouse.gov) qui est une station, mais très peu ont essayé d'accéder à s2-0.whitehouseisp.net, qui est un routeur. En raison de cette visibilité, les stations sont les unités du réseau les plus fréquemment attaquées au cours d'une tentative d'intrusion. En partie à cause des problèmes de sécurité mentionnés ci-dessus, les stations sont également les unités les plus souvent violées. Par exemple, un serveur Web sur l'Internet peut exploiter une plate-forme matérielle d'un constructeur donné, une carte réseau d'un autre, un système d'exploitation d'un troisième constructeur et un serveur Web qui est un logiciel soit libre, soit produit par encore un autre constructeur. De plus, le même serveur Web peut exécuter des applications disponibles gratuitement sur l'Internet et susceptibles de communiquer avec un serveur de base de données qui présente à son tour la même diversité. Nous n'affirmons pas que les vulnérabilités d'un système proviennent spécifiquement de la diversité des éléments qui le composent, mais plutôt que la probabilité d'une défaillance augmente avec la complexité d'un système.

Pour protéger les stations, portez une attention toute particulière à chacune des composantes de ses systèmes. Faites en sorte que chaque système soit constamment à jour grâce aux derniers " patches ", correctifs, etc. publiés. Faites plus particulièrement attention à la manière dont ces " patches " se répercutent sur le fonctionnement des autres composantes du système. Evaluez toutes les mises à jour sur les systèmes testés avant de les placer dans un environnement de production. A défaut, le " patch "lui-même pourrait être à l'origine d'un déni de service.

Les réseaux sont des cibles

Les attaques de réseau sont parmi les plus difficiles à maîtriser car elles exploitent le plus souvent une caractéristique du mode de fonctionnement de votre réseau : il s'agit, entre autres, des attaques sur la couche de niveau 2 par l'ARP (Address Resolution Protocol) et le MAC (Media Access Control), des sniffers et des attaques par déni de service distribué (DDoS). La portée de certaines des attaques sur la couche 2 par l'ARP et le MAC peut être atténuée grâce à l'emploi de pratiques optimales sur les commutateurs et les routeurs. Les sniffers sont présentés dans une section introductive à la fin de cet article. Les attaques par déni de service distibué constituent, en revanche, un type d'attaque original qui mérite une attention particulière.

La pire des attaques est celle que vous ne pouvez pas arrêter. Quand elle est bien réalisée, l'attaque par déni de service distribué fait partie de celles là. Comme le décrit l'annexe B, "Introduction à la sécurité réseau," l'attaque par déni de service distribué consiste à faire envoyer simultanément, sur une adresse IP, des données inutiles par des dizaines, voire des centaines, de machines. L'objectif d'une telle attaque n'est généralement pas de bloquer une station particulière, mais de paralyser l'intégralité du réseau. Imaginez, par exemple, une entreprise équipée d'une connexion Internet DS1 (1,5 Mbps) qui fournit des services de commerce électronique aux utilisateurs de son site Web. Un tel site est extrêmement préoccupé par sa sécurité et possède des systèmes de détection des intrusions, des pare-feu, des contrôles d'ouverture de session et un monitoring actif. Malheureusement, aucun de ces systèmes de protection n'est d'une quelconque utilité contre une attaque par déni de service distribué réussie.

Imaginez 100 unités de par le monde, chacune possédant une connexion Internet DSL (500 Kbps). Si tous ces systèmes sont programmés à distance pour inonder l'interface série du routeur Internet de l'entreprise de commerce électronique, ils peuvent facilement saturer la connexion DS1 de données erronées. Même si chaque hôte ne peut pas générer plus de 100 Kbps de trafic (les tests de laboratoire montrent qu'un PC de série peut facilement générer 50 Mbps à l'aide d'un utilitaire de déni de service distribué classique), le volume total est déjà près de 10 fois supérieur au trafic que le site de commerce électronique peut traiter. En conséquence, les requêtes Web légitimes sont perdues et le site apparaît indisponible à la plupart de ses utilisateurs. Le temps que le pare-feu local élimine toutes les données erronées, le mal est déjà fait. Le trafic a déjà passé la connexion longue distance et saturé le lien.

Pour espérer résister à une telle attaque, notre société fictive de commerce électronique ne peut compter que sur une coopération avec son fournisseur d'accès Internet (FAI). Le FAI peut configurer une limitation de débit sur l'interface de sortie vers le site de la société. Cette limitation de débit peut rejeter la plupart du trafic indésirable lorsque le débit dépasse une fraction prédéterminée de la largeur de bande disponible. La solution consiste à désigner convenablement le trafic comme indésirable.

Les formes les plus courantes ce ces attaques cherchent à saturer le protocole ICMP (Internet Control Message Protocol), la synchronisation TCP SYN ou le protocole UDP (User Datagram Protocol). Dans un environnement de commerce électronique, ce type de trafic est assez facile à identifier. Ce n'est qu'en cherchant à contenir une attaque TCP SYN sur le port 80 (HTTP [Hypertext Transfer Protocol]) que l'administrateur court le risque d'interdire, pendant l'attaque, l'accès aux utilisateurs autorisés. Même dans ce cas, il est préférable d'interdire l'accès aux nouveaux utilisateurs autorisés et de conserver une connectivité de routage et d'administration, plutôt que de mettre le routeur en surcharge et de perdre toute connectivité.

Certaines attaques plus élaborées exploitent le trafic sur le port 80 avec le bit ACK paramétré pour que le trafic apparaisse comme des transactions Web autorisées. Il est peu probable qu'un administrateur puisse identifier correctement ce type d'attaques car les communications TCP avec accusé de réception sont précisément celles que vous souhaitez faire entrer sur votre réseau.

L'une des possibilités pour contenir ce type d'attaques consiste à respecter les consignes de filtrage pour les réseaux, décrites dans les documents RFC 1918 et RFC 2827. Le document RFC 1918 précise les réseaux réservés à une utilisation privée et qui ne doivent jamais être visibles sur l'Internet public. Le filtrage préconisé par le document RFC 2827 est présenté dans la section “Usurpation d'adresse Internet” de l'annexe B, “Introduction à la sécurité réseau”. Vous pouvez utiliser le filtrage RFC 1918 et 2827, par exemple, sur le trafic entrant d'un routeur connecté à l'Internet afin d'empêcher le trafic illicite de parvenir jusqu'au réseau de l'entreprise. Lorsque ce filtrage est mis en œuvre au niveau du FAI, il empêche les paquets d'une attaque par déni de service distribué – qui utilisent ces adresses comme sources – de traverser le lien WAN, ce qui permet de préserver de la bande passante pendant l'attaque. Si, collectivement, les FAI du monde entier adoptaient les consignes de filtrage RFC 2827, ils réduiraient considérablement les usurpations d'adresse source (ou spoofing). Bien que cette stratégie ne prévienne pas directement les attaques par déni de service distribué, elle empêche de telles attaques de masquer leur source, ce qui facilite grandement l'authentification des réseaux hostiles. Demandez à votre FAI quelles sont les options d’atténuation des attaques par déni de service distribué qu'il propose à ses clients.

Les applications sont des cibles

Les applications sont (dans leur majorité) chiffrées par des êtres humains, et sont par conséquent sujettes à de nombreuses erreurs. Ces erreurs peuvent être superficielles – par exemple, si elles provoquent une mauvaise impression de votre document – ou graves – comme une erreur qui rend accessibles par FTP anonyme les numéros de carte de crédit conservés sur votre serveur de base de données. Ce sont les problèmes graves, ainsi que d'autres défauts, plus généraux, de protection qui nécessitent une attention particulière. Il faut veiller à ce que les applications commerciales et du domaine public soient constamment mises à jour à l'aide des correctifs de sécurité les plus récents. Le code des applications du domaine public, ainsi que celui des applications développées spécifiquement, doit être analysé pour s'assurer qu'il ne crée pas de risque sécuritaire engendré par une programmation de mauvaise qualité. Cette programmation peut comprendre des scénarios sur la manière dont une application en appelle d'autres ou le système d'exploitation lui-même, par exemple, le niveau de privilège auquel l'application s'exécute, le degré de confiance que l'application attribue aux systèmes qui l’entourent et, pour finir, la méthode qu'elle emploie pour transporter les données sur le réseau. La section suivante présente les systèmes de détection des intrusions (IDS) et la manière dont ils peuvent atténuer certaines attaques lancées contre les applications ainsi que d'autres fonctions du réseau.

Les systèmes de détection des intrusions

Les systèmes de détection des intrusions (IDS) se comportent comme un système d'alarme dans le monde physique. Lorsqu'un IDS détecte quelque chose qu'il considère comme une attaque, il peut soit prendre lui-même des mesures correctives, soit alerter un système administratif pour que l'administrateur règle le problème. Certains systèmes sont plus ou moins équipés pour réagir à de telles attaques et pour les prévenir. La détection des intrusions sur un système hôte peut agir en interceptant les appels du système d'exploitation ou d'une application sur une station donnée. Il peut également agir en analysant, après les faits, les fichiers journaux locaux. La première démarche permet une meilleure prévention des attaques, alors que la seconde impose un rôle plus passif d'attaque – réponse. En raison de leur rôle très particulier, les systèmes H-IDS (IDS hôte) sont souvent plus efficaces dans la prévention des attaques spécifiques que les systèmes N-IDS (IDS réseau) qui se contentent généralement de lancer une alarme lorsqu'ils découvrent une attaque. Toutefois, ce rôle particulier entraîne une perte de perspective pour l'ensemble du réseau. C'est là que se trouve la supériorité des systèmes N-IDS. Pour un système complet idéal de détection des intrusions, Cisco recommande d'associer les deux systèmes —H-IDS sur les stations critiques et N-IDS pour surveiller l'ensemble du réseau. Malheureusement, les budgets informatiques imposent le plus souvent le choix entre l'une ou l'autre de ces technologies. Dans ce cas, il faudra envisager soigneusement le coût global de chaque technologie, le nombre d'unités qui devront être surveillées et le personnel nécessaire pour répondre à une attaque.

Lorsque vous déployez un IDS, vous devez ajuster ses réglages pour améliorer son efficacité et supprimer les “faux positifs.” Les faux positifs sont définis comme des alarmes déclenchées par une activité ou un trafic légitime. Les faux négatifs sont les attaques que l’IDS ne détecte pas. Lorsque les réglages de l’ IDS sont ajustés, vous pouvez le configurer plus particulièrement de manière à ce qu’il remplisse son rôle d’atténuation des menaces. Comme nous l'avons indiqué plus haut, il est préférable de configurer un H-IDS pour bloquer la plupart des menaces valides au niveau de la station car il est bien conçu pour identifier les activités qui constituent, en réalité, des menaces.

Lorsque vous attribuez un rôle d'atténuation des menaces à un N-IDS, deux options principales s'offrent à vous. Rappelez-vous que la toute première étape, avant même de mettre en œuvre une option de réponse aux menaces est de bien régler le N-IDS pour garantir que toute menace perçue est une véritable menace.

La première option – potentiellement la plus dangereuse si elle est mal déployée – consiste à “bloquer” le trafic en ajoutant des filtres de contrôle d'accès sur les routeurs et les pare-feu. Lorsqu'un N-IDS détecte une attaque en provenance d'une station donnée sur un protocole particulier, il peut empêcher cet hôte de venir sur le réseau pendant une durée prédéterminée. Bien qu'en apparence, cette solution semble d'un grand secours pour un administrateur de sécurité, sa mise en œuvre doit en fait être réalisée avec le plus grand soin, si tant est que vous décidiez de l'adopter. Le premier problème est celui des adresses usurpées. Si le trafic correspondant à une attaque est perçu par le N-IDS, et que l'alarme correspondante déclenche une situation d'exclusion, le N-IDS déploiera la liste d'accès sur l'unité. Toutefois, si l'attaque qui a déclenché l'alarme a utilisé une adresse usurpée, le N-IDS n'aura fait que bloquer une adresse qui n'a jamais déclenché d'attaque. Si l'adresse IP utilisée par le pirate s'avère être celle du serveur proxy HTTP sortant d'un important FAI, un très grand nombre d'utilisateurs peuvent se retrouver bloqués. Cette option peut, en elle-même, constituer une intéressante attaque par déni de service entre les mains d'un pirate imaginatif.

Pour atténuer les risques de blocage, vous ne devez l'utiliser, de manière générale, que sur le trafic TCP, sur lequel une usurpation réussie est beaucoup plus difficile que sur l'UDP. Réservez cette méthode aux seuls cas où la menace est réelle et quand la probabilité d'un faux positif est très faible. Envisagez également de réduire au minimum la période d'exclusion. Cette configuration bloquera l'utilisateur suffisamment longtemps pour permettre à l'administrateur de décider des actions permanentes qu'il désire éventuellement prendre contre l'adresse IP en question. Toutefois, l'intérieur d'un réseau autorise de nombreuses autres options. Un filtrage RFC 2827 efficacement déployé permet de limiter considérablement le trafic par usurpation. De plus, comme les clients ne se trouvent généralement pas sur le réseau interne, vous pouvez adopter une position plus restrictive contre les tentatives d'attaque provenant de l'intérieur. Une autre raison est que les réseaux internes ne disposent pas souvent du même niveau de filtrage au plus bas niveau que celui des connexions en frontière de réseau. C'est pour cette raison qu'il convient de s'appuyer plus lourdement sur les IDS dans les réseaux internes que dans l'environnement externe.

La seconde option pour un N-IDS est d'utiliser les réinitialisations TCP. Comme leur nom l'indique, les réinitialisations TCP ne s'appliquent qu'au trafic TCP et mettent fin à une attaque active en envoyant des messages de remise à zéro TCP vers les stations agressives et agressées. Comme le trafic TCP est plus difficile à pirater, il est préférable d'utiliser plus souvent les réinitialisations TCP que l'exclusion. Rappelez-vous que dans un environnement commuté, les réinitialisations TCP sont plus difficiles à utiliser que dans un hub standard, car tous les ports ne peuvent pas voir la totalité du trafic sans l'utilisation d'un SPAN (Switched Port Analyzer) ou port miroring. Veillez à ce que ce port miroring supporte le trafic dans les deux sens et qu'il soit possible de désactiver l'apprentissage MAC du port SPAN.

Ces deux options d’atténuation des risques exigent la présence permanente (24 h sur 24) de personnel chargé de surveiller les consoles IDS. Comme le personnel informatique est souvent surchargé de travail (et plus particulièrement dans les petites entreprises), il peut être intéressant de confier la gestion IDS à une société tierce.

Du point de vue des performances, un N-IDS observe les paquets qui passent. Si les paquets sont envoyés plus vite qu'il n'est possible au N-IDS de les traiter, le débit du réseau n'en est pas affecté car le N-IDS ne réside pas directement sur les flux de données. Toutefois, le système de détection perdra de son efficacité et certains paquets peuvent être manqués, ce qui provoquera des faux négatifs et des faux positifs. Assurez-vous de ne pas dépasser les possibilités de l’IDS afin d'en tirer le meilleur parti. Du point de vue du routage, l’ IDS, comme beaucoup de moteurs sensibles à l'état, ne fonctionne pas convenablement dans un environnement de routage asymétrique. Lorsque les paquets sont expédiés par un groupe de routeurs et de commutateurs et reviennent par un autre groupe, les IDS ne voient qu'une moitié du trafic, ce qui engendre des faux positifs et des faux négatifs.

Administration et reporting de sécurité

“Si vous l'enregistrez dans un journal, lisez-le.” Cet aphorisme est si simple que presque tous ceux qui savent ce qu'est la sécurité réseau l'ont déjà prononcé au moins une fois. Toutefois, enregistrer l'information et la lire dans les journaux (logs) d'un grand nombre d'unités peut devenir très compliqué. Quels sont les journaux les plus importants ? Comment différencier les messages importants des simples notifications ? Comment s'assurer que les fichiers journaux n'ont pas été altérés ou consultés au cours de leur déplacement ? Comment garantir que les estampilles temporelles se correspondent lorsque plusieurs unités signalent le même problème ? Quelles sont les informations nécessaires pour exploiter les données du fichier journal dans une enquête criminelle ? Comment faire face au volume de messages générés lorsqu'un système est confronté à une attaque ? Vous devez répondre à toutes ces questions lorsque vous envisagez de gérer efficacement les fichiers journaux. Pour l'administrateur, une autre série de questions doit trouver réponse : Comment gérer une unité en toute sécurité ? Comment expédier du contenu vers d'autres serveurs publics et s'assurer qu'il ne sera pas altéré ou consulté en cours de route ? Comment assurer le suivi des modifications apportées aux unités afin de régler le problème en cas d'attaque ou de défaillance de réseau ?

Bien que l'architecture d'administration " out of band " décrite dans SAFE Enterprise offre le niveau le plus élevé de sécurité, nous ne la recommandons pas dans cet article car notre objectif est le déploiement d'un système de sécurité économique. Dans l'environnement out of band, chaque unité et chaque station de réseau possède sa propre interface d'administration dédiée qui se connecte au réseau d'administration privé. Cette configuration atténue le risque de laisser passer des protocoles de gestion peu sûrs – comme Telnet, TFTP (Trivial File Transfer Protocol), SNMP ou syslog – sur le réseau de production où ils pourraient être interceptés ou modifiés.

Dans l'architecture décrite ici, le trafic d'administration passe dans tous les cas “in band” où il est aussi protégé que possible à l'aide de protocoles de tunnellisation et de variantes sécurisées aux protocoles administratifs non protégés. Le protocole SSH (Secure Shell Protocol), par exemple, remplace Telnet chaque fois que cela est possible. Lorsque le trafic administratif passe “in band ” sur le réseau de production, il devient particulièrement important de suivre à la lettre les axiomes que nous avons mentionnés précédemment dans cet article.

Si vous devez administrer une unité située à l'extérieur du pare-feu, il est préférable d'envisager les questions suivantes. Premièrement, quels sont les protocoles d’administration supportés par l'unité ? Les unités équipées de IP Security (IPSec) doivent être administrées en créant simplement un tunnel qui part du réseau d'administration vers l'unité. Cette configuration permet à de nombreux protocoles non protégés de circuler sur un unique tunnel chiffré. Lorsqu'il n'est pas possible d'utiliser IPSec – par ce qu'il n'est pas supporté par l'unité – vous avez le choix entre plusieurs alternatives moins efficaces du point de vue de la sécurité. Pour configurer l'unité, les protocoles SSHou SSL (Secure Sockets Layer) peuvent souvent remplacer Telnet afin de coder les modifications de configuration apportées à l'unité. Ces mêmes protocoles peuvent également remplacer des protocoles peu sûrs comme TFTP et FTP lorsqu'il s'agit de pousser ou de tirer des données vers ou à partir d'une unité. Toutefois, il arrive souvent que TFTP soit nécessaire sur les équipements Cisco afin de sauvegarder des configurations ou de mettre à jour des versions de logiciels. Ceci nous amène à la seconde question : Ce canal d'administration doit-il rester actif en permanence ? Si ce n'est pas le cas, des ouvertures temporaires peuvent être placées sur le pare-feu pendant l'exécution des fonctions d'administration, après quoi elles seront retirées. Ce processus est toutefois incapable de s'adapter à un grand nombre d'unités. Si le canal doit rester actif en permanence, comme avec le protocole SNMP, une troisième question se pose : cet outil d'administration est-il véritablement nécessaire ? On utilise souvent des gestionnaires SNMP sur l'intérieur du réseau afin d'améliorer la recherche des pannes et la configuration. Mais est-ce vraiment indispensable pour un commutateur DMZ qui fournit des services de couche 2 à deux ou trois serveurs ? Si ce n'est pas le cas, il faut le désactiver. Si vous décidez en revanche que le canal doit rester actif, sachez que vous ouvrez une faille potentielle dans votre environnement. Les paragraphes suivants présentent avec plus de détails les types spécifiques d'administration.

En ce qui concerne le reporting, la plupart des unités de réseau peuvent transmettre des données syslog qui sont inestimables pour résoudre les problèmes du réseau ou faire face aux menaces. Faites parvenir à la station d'analyse syslog les données qui proviennent des unités dont vous voulez visualiser les journaux de consignation. Ces données peuvent être visualisées en temps réel ou bien sur des rapports à la demande ou programmés. Suivant l'unité concernée, vous pourrez choisir différents niveaux d'ouverture de session pour garantir que la quantité prévue de données soit expédiée à l'unité journal. Vous devez également signaler les données journal de l'unité au logiciel d'analyse afin de permettre la visualisation et le reporting de bas niveau. Au cours d'une attaque, par exemple, les données journal transmises par les commutateurs de couche 2 peuvent ne pas être aussi intéressantes que celles fournies par le système de détection des intrusions. Pour garantir que les messages journaux sont synchronisés les uns avec les autres, les horloges des stations et des unités de réseau doivent être synchronisées. Si les unités les supportent, le protocole NTP (Network Time Protocol) offre un moyen de s'assurer que les données horaires sont précisément entretenues sur toutes les unités. En cas d'attaque, il est important de suivre les événements à la seconde près car il est essentiel de déterminer l'ordre dans lequel l'attaque a été menée.

La gestion des changements de configuration est une autre question liée à l'administration de sécurité. Lorsqu'un réseau est attaqué, il est important de connaître l'état des unités critiques du réseau et l'instant où sont intervenues les dernières modifications. La création d'un plan de gestion des modifications doit faire partie de votre politique complète de protection, mais – et c'est un strict minimum – vous devez enregistrer les modifications à l'aide de systèmes d'authentification placés sur les unités, et archiver les configurations par FTP ou TFTP.

Comparaison site central / site distant

Les designs de réseau de petite taille et de taille moyenne évoqués ci-après peuvent être utilisés en deux configurations. Dans la première, le design est celui d’une organisation de réseau de type " site central ". Ce site central peut posséder des connexions VPN vers d'autres bureaux de la même entreprise. Un cabinet juridique important peut, par exemple, utiliser un design de réseau de taille moyenne pour le site central, et plusieurs designs de réseaux de petite taille pour ses autres sites. Dans la seconde configuration, le réseau se comporte comme un site secondaire d'une organisation plus importante et qui relève de la configuration décrite dans SAFE Enterprise.

Un autre exemple encore serait celui d'un grand constructeur automobile qui utiliserait le concept SAFE Enterprise pour ses sièges sociaux et les designs décrits dans cet article pour ses sites distants et ses télétravailleurs. Le cas échéant, les modifications spécifiques qu'il peut être nécessaire d'apporter au design sont présentées dans chaque section.

Les menaces prévisibles

Du point de vue des menaces, un réseau petit ou de taille moyenne ressemble à la plupart des réseaux connectés à l'Internet – certains de ses utilisateurs internes ont besoin d'accès vers l'extérieur et certains utilisateurs externes ont besoin d'y accéder. Plusieurs risques courants sont susceptibles de créer la situation initiale dont un pirate a besoin pour pénétrer plus avant dans un réseau et y poursuivre ses méfaits.

En premier lieu viennent les attaques lancées par les utilisateurs internes. Bien que les statistiques donnent des pourcentages différents, il est avéré que la plupart des attaques proviennent du réseau interne. Les employés mécontents, les espions industriels, les visiteurs et les utilisateurs maladroits sont autant de sources potentielles d'attaques. Un plan de sécurité bien conçu doit tenir compte du potentiel des menaces internes.

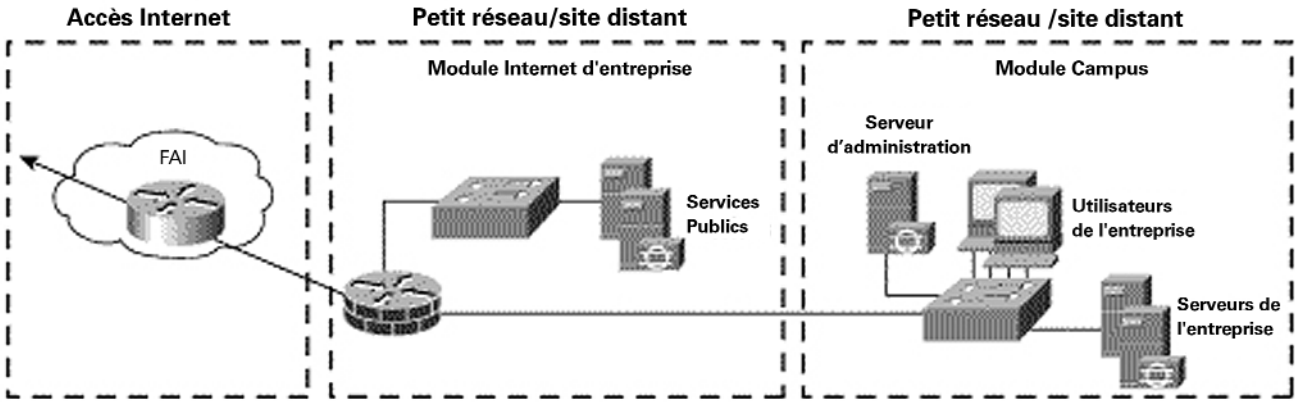
Vient ensuite la menace envers les stations publiquement adressables qui sont connectées à l'Internet. Les attaques sur ces systèmes porteront vraisemblablement sur les faiblesses de la couche application ou tenteront de saturer le réseau.

Pour une présentation complète et détaillée de ces menaces, consultez l'annexe B, “Introduction à la sécurité réseau.”

Design d'un petit réseau

Un petit réseau se compose de deux modules : le module Internet d'entreprise et le module de réseau étendu ou module Campus. Le module Internet d'entreprise possède des connexions vers l'Internet et raccorde le trafic des VPN et des services publics (DNS, HTTP, FTP, SMTP). Le module Campus contient le système de commutation de couche 2 et tous les utilisateurs, ainsi que les serveurs d'administration et intranet. Dans la présentation de ce design, nous supposerons que le petit réseau sert de site central pour une entreprise. Nous décrivons également les modifications spécifiques à apporter lorsque le réseau est utilisé comme un site distant.

Figure 1 - Modèle détaillé de petit réseau



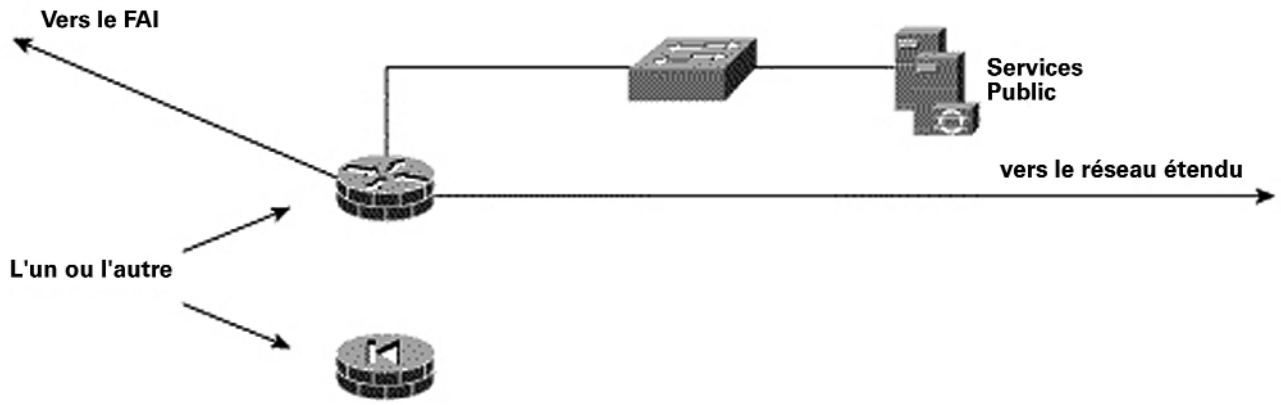
Module Internet d'entreprise

Le module Internet d'entreprise apporte aux utilisateurs internes la connectivité vers les services Internet et aux utilisateurs Internet un accès aux informations des serveurs publics. Il permet également aux sites distants et aux télétravailleurs d'accéder au réseau en VPN. Ce module n'est pas prévu pour servir des applications de type commerce électronique. Pour plus de détails sur la manière de fournir des services Internet de commerce électronique, consultez la section “ Module de commerce électronique” dans SAFE Enterprise.

Principales unités

- *Serveur SMTP* — Joue le rôle de relais entre l'Internet et les serveurs de courrier intranet
- *Serveur DNS* — Joue le rôle de serveur DNS externe pour l'entreprise ; relaie les requêtes internes vers l'Internet
- *Serveur FTP / HTTP* — Fournit des informations publiques sur l'entreprise
- *Pare-feu ou routeur pare-feu* — Offre au niveau réseau une protection des ressources, un filtrage adaptatif du trafic, et une connexion VPN pour les sites et les utilisateurs distants
- *Commutateur de couche 2 (avec support de réseau privé local virtuel)* — Garantit que les données des unités administrées transitent nécessairement par le pare-feu IOS.

Figure 2 - Modèle détaillé du module Internet d'entreprise d'un petit réseau

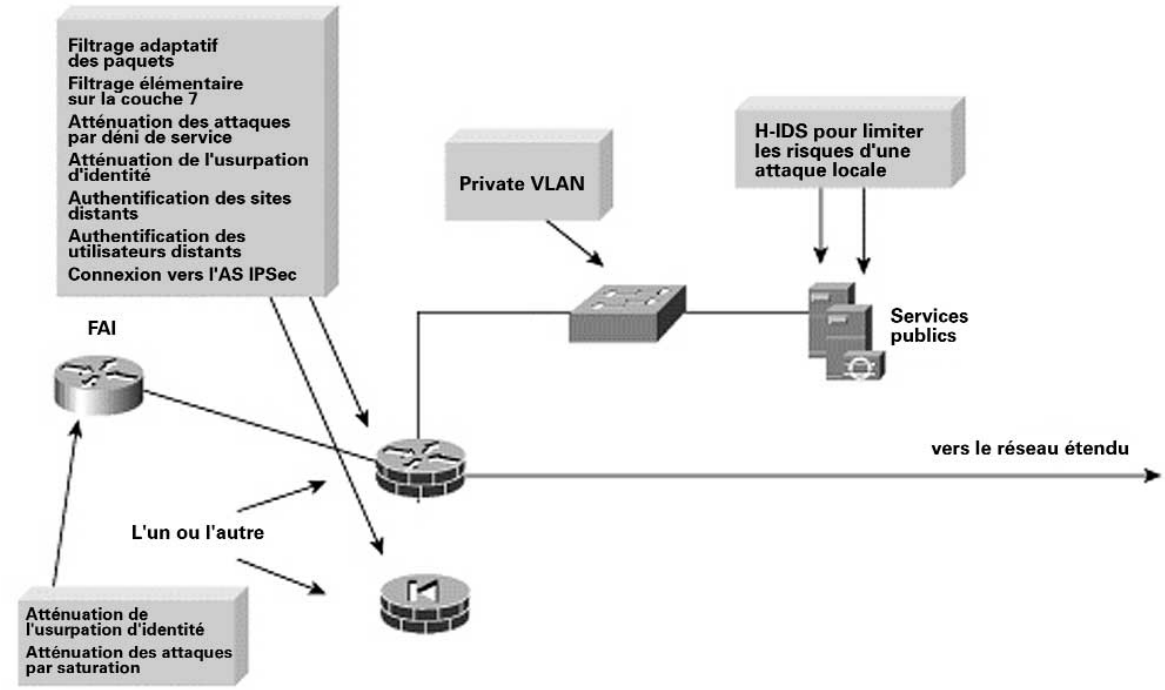


Atténuation des risques

Certains serveurs adressables publiquement sont les points d'attaque les plus probables. Voici une liste des risques envisagés :

- *Accès non autorisé* — Atténué par le filtrage au niveau du pare-feu
- *Attaques sur la couche application* — Atténuées grâce à une sonde H-IDS sur les serveurs publics
- *Attaques par virus ou par un cheval de Troie* — Atténuées par l'analyse anti-virus au niveau des stations
- *Attaques sur les mots de passe* — Atténuation du nombre de services accessibles par une attaque en force ; le système d'exploitation et le IDS peuvent détecter la menace
- *Déni de service* — Lissage du trafic (CAR : committed access rate) à la frontière du FAI et contrôles de configuration TCP au niveau du pare-feu pour limiter les risques
- *Usurpation d'adresse Internet* — Filtrage RFC 2827 et 1918 à la frontière avec le FAI et sur le pare-feu local
- *Sniffers de paquets* — Infrastructure commutée et H-IDS pour limiter les risques
- *Reconnaissance de réseau (scan)* — Le H-IDS détecte les tentatives de reconnaissance ; les protocoles sont filtrés pour limiter l'efficacité de l'attaque
- *Exploitation des relations de confiance* — Modèle de confiance restrictif et private VLAN pour limiter les risques d'attaque par exploitation de la confiance
- *Redirection des ports* — Filtrage restrictif et H-IDS pour limiter les risques d'attaquee

Figure 3 - Rôles des méthodes d'atténuation des risques d'attaque sur les petits réseaux pour les modules Internet d'entreprise



Lignes directrices du design

Ce module constitue le schéma le plus abouti en matière de design de réseau orienté sécurité à petite échelle : toute la sécurité et les services VPN sont contenus dans une même boîte. Deux choix principaux s'offrent à vous si vous êtes amené à mettre cette fonctionnalité en œuvre. Le premier consiste à utiliser un routeur avec une fonctionnalité pare-feu et VPN. Cette configuration confère aux petits réseaux une flexibilité maximale car le routeur supporte tous les services évolués (qualité de service, routage, support multiprotocoles, etc.) nécessaires à un réseau moderne. Dans l'autre solution, on remplace le routeur par un pare-feu dédié. Cette configuration impose quelques restrictions sur le déploiement. En premier lieu, les pare-feu supportent, en général, uniquement Ethernet, ce qui exige certaines conversions vers le protocole WAN que l'on utilise. Dans les environnements actuels, la plupart des routeurs modem câble et DSL (digital-subscriber-line) sont fournis par le FAI et peuvent être utilisés pour se connecter au pare-feu sur Ethernet. S'il est nécessaire de disposer d'une connectivité WAN sur l'équipement (comme dans le cas d'un circuit RNIS sur un opérateur téléphonique), il faut alors utiliser un routeur. L'utilisation d'un pare-feu dédié présente l'avantage de simplifier la configuration des services de sécurité, en plus d'améliorer les performances de ses fonctions spécifiques. Quelle que soit l'unité choisie, une inspection des paquets au plus bas niveau permet d'examiner le trafic dans toutes les directions, ce qui garantit que seul le trafic légitime traversera le pare-feu. En théorie, un premier filtrage de sécurité intervient au niveau du FAI avant même que le trafic atteigne le pare-feu. Rappelez-vous que la tendance première des routeurs est d'autoriser le trafic, tandis que, par défaut, celle des pare-feu est de le bloquer.

En commençant par le routeur à la frontière client du FAI, le routeur en sortie du FAI réduit le trafic non-essentiel qui dépasse les seuils prédéfinis afin de limiter les conséquences d'une attaque par déni de service. De plus, au point de sortie du routeur du FAI, le filtrage RFC 1918 et RFC 2827 atténue les risques d'usurpation d'adresses source des réseaux locaux et des plages d'adresses privées.

Au point entrant du pare-feu, un premier filtrage RFC 1918 et RFC 2827 permet de vérifier le filtrage du FAI. De plus, et en raison de l'importance du risque lié à la fragmentation des paquets, le pare-feu est configuré pour rejeter la plupart des paquets fragmentés qui ne sont pas couramment associés au trafic standard sur l'Internet. La perte éventuelle du trafic légitime occasionnée par ce filtrage est considérée comme acceptable en comparaison du risque d'admettre le trafic dangereux. Le trafic en provenance de l'extérieur et destiné au pare-feu lui-même est limité au trafic IPSec ainsi qu'aux protocoles nécessaires au routage.
Le pare-feu permet de faire appliquer les règles d'état de connexion et réalise un filtrage détaillé des sessions appelées à travers lui. Les serveurs publiquement adressables disposent d'une certaine protection contre les saturations de synchronisation TCP SYN grâce à des mécanismes tels que l'utilisation de systèmes de limitation des connexions semi-ouvertes sur le pare-feu. Quant au filtrage, en plus de contenir le trafic sur le segment des services publics vers les adresses et les ports autorisés, il s'exerce également dans la direction opposée. Si un pirate parvient à s'emparer d'un des serveurs publics (en contournant le pare-feu et l'IDS hôte), il ne faut pas permettre à ce serveur de poursuivre l'attaque du réseau. Pour limiter le risque d'une telle attaque, un filtrage spécifique interdit à tous les serveurs publics de générer des requêtes non-autorisées en direction des autres emplacements. Par exemple, le serveur Web doit être filtré afin qu'il ne puisse pas émettre de requêtes par lui-même et qu'il se contente de répondre aux requêtes des clients. Cette configuration permet d'éviter qu'un pirate puisse télécharger des utilitaires supplémentaires vers l'équipement dont il s'est emparé après l'attaque initiale. Elle contribue également à empêcher que des sessions indésirables puissent être ouvertes par le pirate au cours de l'attaque principale. Un exemple d'attaque de ce type est celle qui génère un xterm à partir du serveur Web et au travers du pare-feu vers l'ordinateur du pirate. De plus, un private VLAN sur le commutateur DMZ empêche qu'un serveur public compromis puisse attaquer d'autres serveurs du même segment. Même le pare-feu ne parvient pas à détecter ce type de trafic, une constatation qui montre l'importance critique des private VLAN.

Du point de vue serveur, chacun des serveurs du segment DMZ dispose d'un logiciel H-IDS afin de contrôler l'apparition d'activités suspectes au niveau du système d'exploitation, ainsi que d'activités dans les applications serveur communes (HTTP, FTP, SMTP, etc.). Le serveur DNS doit être configuré pour ne répondre qu'aux commandes autorisées et éliminer toutes les réponses inutiles qui pourraient faciliter la reconnaissance du réseau par les pirates. Ceci comprend l'interdiction des transferts de zone quelle que soit leur provenance, à l'exception des serveurs DNS secondaires autorisés. Pour les services de courrier, le pare-feu lui-même filtre les messages SMTP au niveau de la couche 7 pour ne transmettre au serveur de courrier que les commandes nécessaires.

Parmi leurs fonctions de sécurité, les pare-feu et les routeurs pare-feu disposent généralement de certaines capacités limitées de détection des intrusions sur le réseau. Ces capacités limitent les performances de l'unité mais offrent le cas échéant une visibilité supplémentaire sur des attaques éventuelles. Vous devez garder à l'esprit que vous privilégiez la visibilité des attaques au détriment des performances. Beaucoup de ces attaques peuvent être rejetées sans l'utilisation d'un système de détection d'intrusion, mais dans ce cas le poste de contrôle n'aura pas connaissance de l'attaque spécifique qui est lancée contre le réseau.

Le pare-feu ou le pare-feu routeur assure la connectivité VPN. Les sites distants authentifient les uns les autres par l'intermédiaire de clés préalablement échangées, tandis que les utilisateurs distants s'identifient par l'intermédiaire du serveur de contrôle d'accès du module Campus.

Autres possibilités

Toute modification de ce design doit avoir pour objectif d'accroître la capacité du réseau ou de répartir les différentes fonctions de sécurité sur des unités distinctes. Ce faisant, l'agencement du réseau se rapprochera de plus en plus de celle des réseaux de taille moyenne présentés ci-après. Plutôt que d'adopter pleinement cette configuration de réseau, il serait préférable dans une première étape d'ajouter un concentrateur dédié pour l'accès distant des VPN afin de faciliter l'administration de la communauté des utilisateurs distants.

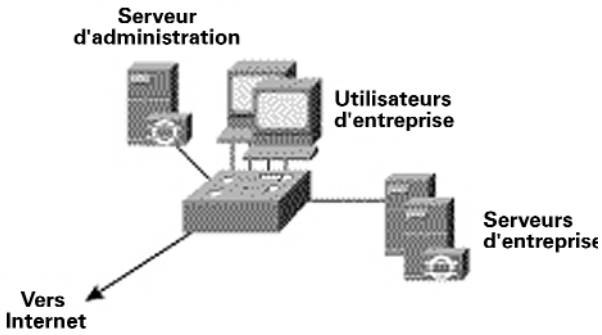
Module Campus

Le module Campus se compose de stations de travail pour les utilisateurs finaux, de serveurs intranet d'entreprise, de serveurs d'administration et de l'infrastructure de couche 2 nécessaire pour supporter les unités. Dans le design du petit réseau, cette fonctionnalité de couche 2 a été réunie dans un commutateur unique.

Principales unités

- *Commutateur de couche 2 (avec support pour les réseaux locaux virtuels privés)* — Fournit des services de couche 2 aux stations de travail utilisateur
- *Serveurs d'entreprise* — Fournissent les services de courrier électronique (SMTP et POP3) aux utilisateurs internes ainsi que les services de livraison de fichiers, d'impression et de DNS aux stations de travail
- *Stations de travail utilisateur* — Fournissent des services de données aux utilisateurs autorisés sur le réseau
- *Hôte d'administration* — Fournit les services de H-IDS, syslog, TACACS+ / RADIUS (Remote Access Dial-In User Service), ainsi que la gestion de configuration générale

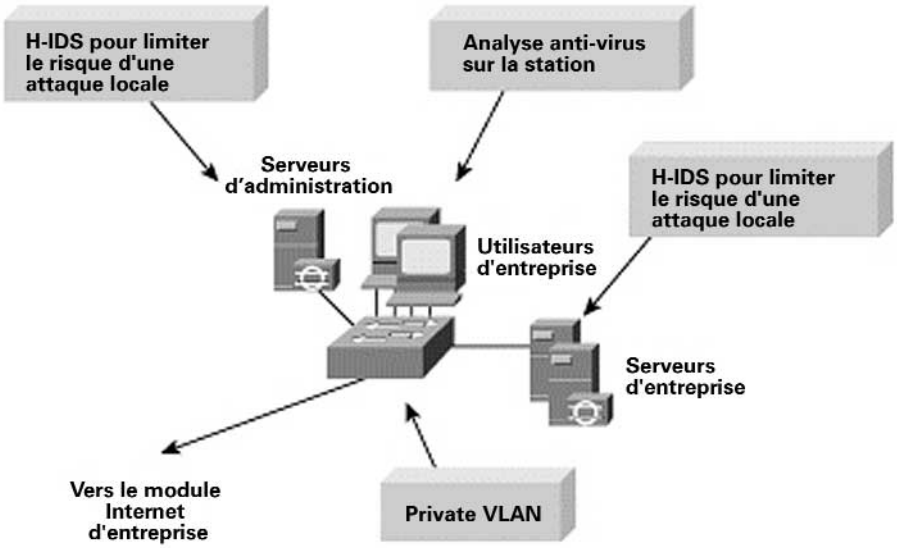
Figure 4 - Modèle détaillé du module Campus de petit réseau



Atténuation des risques

- *Sniffers de paquets* — Une infrastructure commutée limite l'efficacité des sniffers de paquets
- *Applications virus et cheval de Troie* — L'analyse anti-virus réalisé sur la station permet d'éliminer la plupart des virus et de nombreux chevaux de Troie
- *Accès non autorisé* — La détection des intrusions à partir de la station ainsi que le contrôle d'accès des applications permettent de réduire ce type d'accès
- *Attaques sur la couche application* — Les systèmes d'exploitation, les unités et les applications sont maintenues à jour grâce au derniers correctifs de sécurité et sont protégés par un H-IDS
- *Exploitation de la confiance* — Les Private VLAN empêchent que les stations d'un même sous-réseau puissent communiquer à moins que cela ne soit nécessaire
- *Réacheminement des ports* — Le H-IDS empêche l'installation d'agents de réacheminement des ports

Figure 5 - Rôles des méthodes d'atténuation des risques d'attaque sur les petits réseaux pour le module Campus



Lignes directrices du design

Les fonctions principales du commutateur de réseau étendu (Campus) consistent à commuter le trafic de production et de gestion et de fournir la connectivité nécessaire aux serveurs d'entreprise et de gestion ainsi qu'aux utilisateurs. Au sein du commutateur, il est possible d'activer des private VLAN afin d'atténuer les risques d'attaque par exploitation de la confiance entre les équipements. Par exemple, les utilisateurs d'entreprise peuvent avoir besoin de se parler sur les réseaux d'entreprise mais n'ont peut être pas la nécessité de communiquer entre eux.

Comme le module Campus ne comporte pas de service de couche 3, il est important de se rappeler que ce design met de plus en plus l'accent sur la sécurité des applications et de la station en raison de la nature ouverte du réseau interne. Pour cela, un H-IDS a également été installé sur les systèmes clé du réseau, y compris les serveurs d'entreprise et les systèmes de gestion.

Autres possibilités

L'installation d'un petit routeur ou pare-feu de filtrage entre les postes d'administration et le reste du réseau peut améliorer l'état général de la sécurité. Cette configuration permet au trafic d'administration de circuler la seule direction considérée comme indispensable par les administrateurs. Si le niveau de confiance est élevé dans l'entreprise, il est possible de supprimer le H-IDS, bien que cela ne soit pas recommandé.

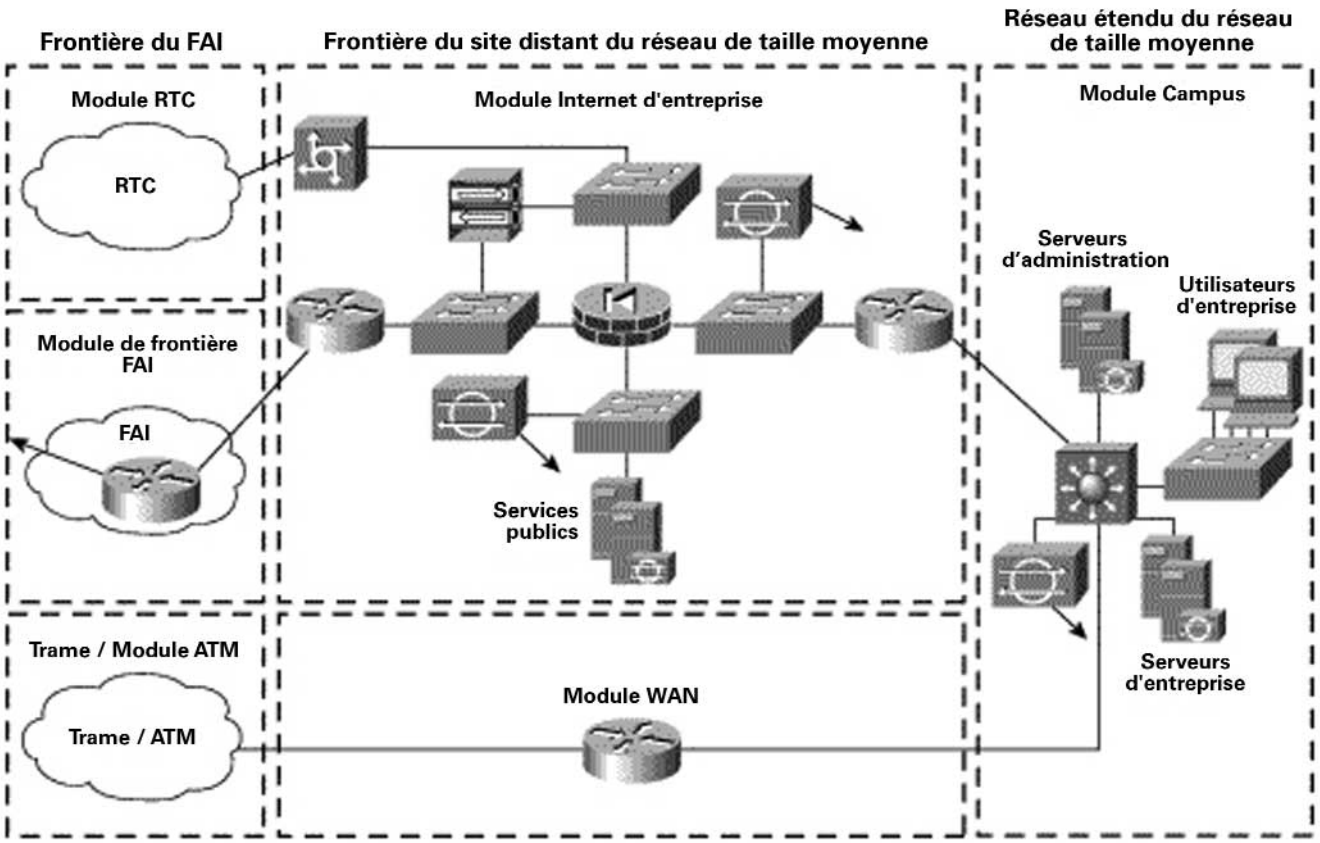
Comparaison site indépendant / site distant

Lorsqu'il est configuré en tant que site distant, le réseau n'a pas besoin d'une fonction d'accès VPN à distance car elle est généralement fournie par le réseau du siège social de l'entreprise. De plus, les stations d'administration sont le plus souvent placés sur le site central, une configuration qui exige que le trafic d'administration repasse par la connexion VPN de site à site pour revenir au siège social de l'entreprise.

Design d'un réseau de taille moyenne

Le design réseau de taille moyenne SAFE se compose de trois modules : le module Internet d'entreprise, le module Campus et le module WAN. Comme dans le design des petits réseaux, le module Internet d'entreprise dispose de la connexion vers l'Internet et raccorde les VPN et les trafics de services public (DNS, HTTP, FTP et SMTP). Le trafic commuté se raccorde également au module Internet d'entreprise. Le module Campus contient l'infrastructure de commutation des couches 2 et 3 ainsi que tous les utilisateurs de l'entreprise, les serveurs d'administration et les serveurs intranet. En ce qui concerne le réseau WAN, deux options de connexion au réseau de taille moyenne s'offrent aux sites distants. La première consiste en une connexion privée WAN qui exploite le module WAN, la seconde est un VPN IPSec vers le module Internet d'entreprise. Nous traiterons essentiellement dans cet article d'un réseau de taille moyenne opérant en tant que site centrald'une entreprise. Nous décrivons également les modifications spécifiques à apporter lorsque le réseau est utilisé comme un site distant.

Figure 6 - Modèle détaillé d'un réseau de taille moyenne



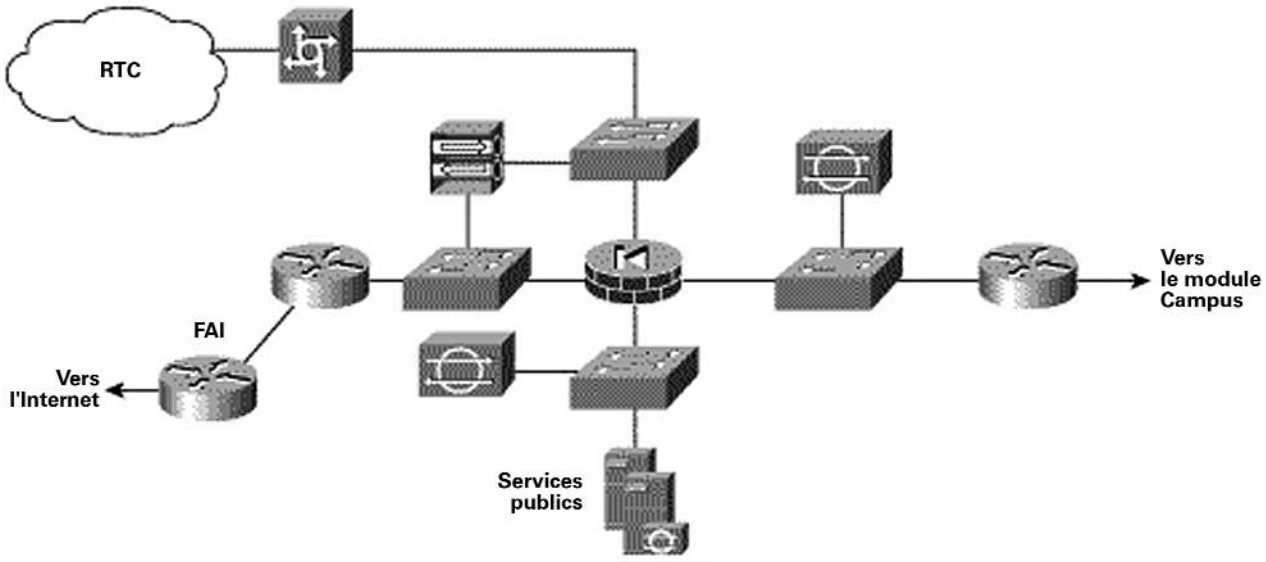
Module Internet d'entreprise

Le module Internet d'entreprise apporte aux utilisateurs internes la connectivité vers les services Internet et aux utilisateurs Internet un accès aux informations des serveurs publics (HTTP, FTP, SMTP et DNS). De plus, ce module raccorde le trafic VPN des utilisateurs distants et des sites distants ainsi que le trafic des utilisateurs classiques commutés. Le module Internet d'entreprise n'est pas prévu pour servir des applications de type commerce électronique. Pour plus de détails sur la manière de fournir des services Internet de commerce électronique, consultez la section " Module de commerce électronique" dans SAFE Enterprise.

Principales unités

- *Serveur commuté entrant* — Identifie les utilisateurs individuels distants et raccorde leurs connexions analogiques
- *Serveur DNS* — Joue le rôle de serveur d'autorisation DNS externe pour l'entreprise ; relaie les requêtes internes vers l'Internet
- *Serveur FTP / HTTP* — Fournit des informations publiques sur l'entreprise
- *Pare-feu* — Offre une protection des ressources au niveau du réseau et un filtrage adaptatif du trafic ; offre une différents types de sécurité pour les utilisateurs distants ; identifie les sites distants de confiance et offre une connectivité par l'intermédiaire de tunnels IPSec
- *Commutateur de couche 2 (avec support de réseau privé local virtuel support)* — Offre aux unités une connectivité de couche 2
- *Serveur dédié N-IDS* — Offre un contrôle des segments clé du réseau dans le module sur les couches de 4 à 7
- *Serveur SMTP* — Joue le rôle de relais entre l'Internet et les serveurs de courrier intranet ; inspecte les contenus
- *Concentrateur VPN* — Identifie les utilisateurs individuels distants et raccorde leurs tunnels IPSec
- *Routeur frontière* — Offre un filtrage élémentaire et une connectivité de couche 3 vers l'Internet

Figure 7 - Modèle détaillé du module Internet d'entreprise d'un réseau de taille moyenne



Atténuation des risques

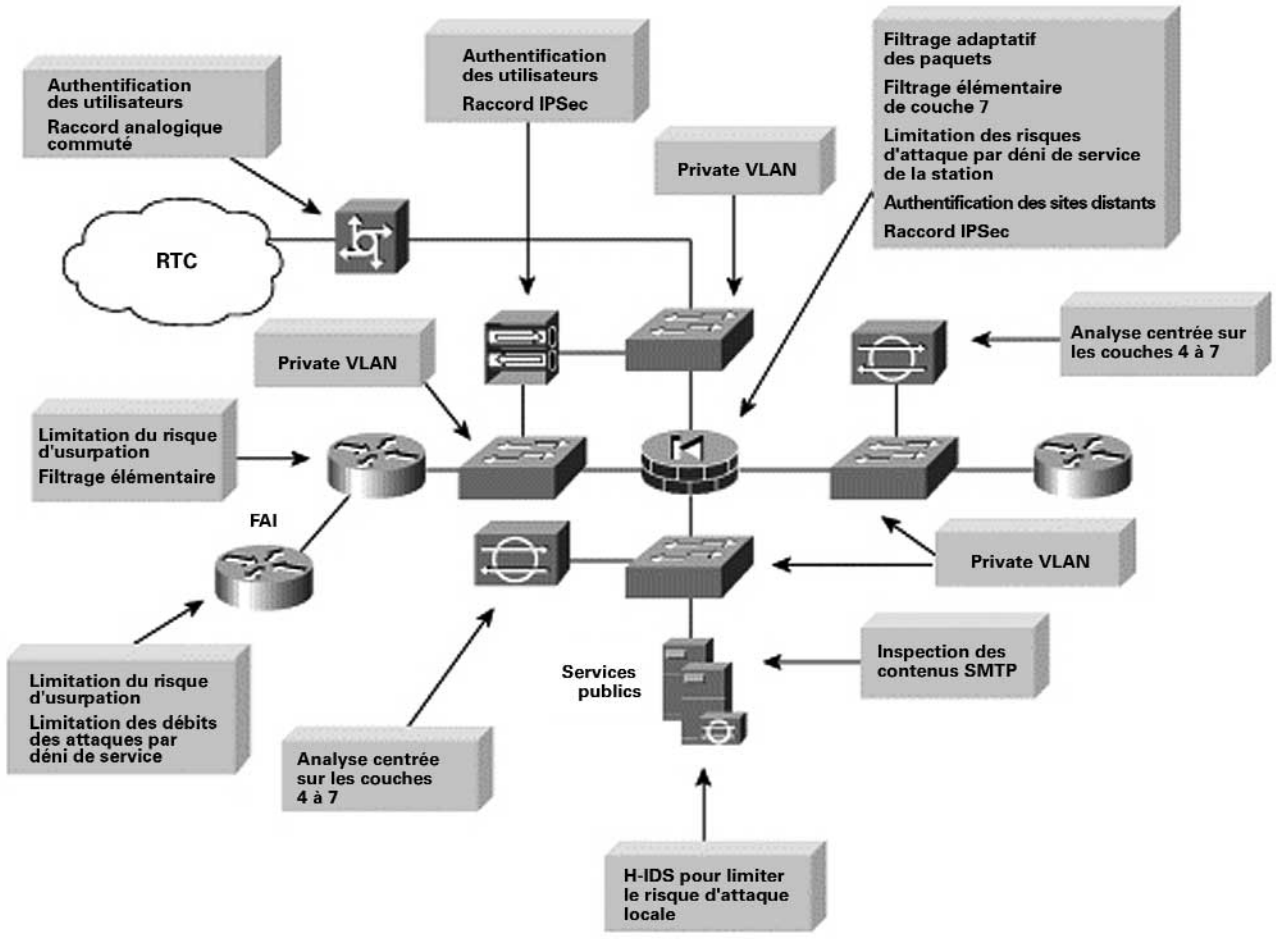
Les serveurs adressables publiquement sont les points d'attaque probables de ce module. Voici une liste des risques envisagés :

- *Accès non autorisé* — Limité par le filtrage au niveau du FAI, du routeur frontière et du pare-feu de l'entreprise
- *Attaques sur la couche application* — Limitées grâce à un H-IDS et un N-IDS
- *Attaques par virus ou par un cheval de Troie* — Limitées par le filtrage du contenu du courrier électronique, un H-IDS et une analyse anti-virus au niveau de la station
- *Attaques sur les mots de passe* — Limitation du nombre de services accessibles par la force brute ; le système d'exploitation et le IDS peuvent détecter la menace
- *Déni de service* — CAR à la frontière du FAI et contrôles de configuration TCP au niveau du pare-feu
- *Usurpation d'adresse Internet* — Filtrage RFC 2827 et 1918 à la frontière avec le FAI et routeur frontière de réseau de taille moyenne
- *Sniffers de paquets* — Infrastructure commutée et H-IDS pour limiter les risques
- *Reconnaissance de réseau* — Le H-IDS détecte la reconnaissance ; les protocoles sont filtrés pour limiter l'efficacité de l'attaque
- *Exploitation de la confiance* — Modèle de confiance restrictif et private VLAN pour limiter le risque d'attaque par exploitation de la confiance
- *Réacheminement des ports* — Filtrage restrictif et H-IDS pour limiter les risques d'attaque.

Les services d'accès à distance et de VPN de site à site sont également des points d'attaque de ce module. Voici une liste des risques envisagés :

- *Recherche de la topologie du réseau* — Les listes de contrôle d'accès (ACL) sur le routeur entrant limitent l'accès au pare-feu ou au concentrateur du VPN (lorsqu'ils sont utilisés pour raccorder les tunnels IPSec provenant des sites distants) aux seuls protocoles IKE (Internet Key Exchange) et ESP (Encapsulating Security Payload) à partir de l'Internet
- *Attaques sur les mots de passe* — L'utilisation de mots de passe à usage unique (OTP) atténue l'impact des attaques en force sur les mots de passes
- *Accès non autorisé* — Les services de pare-feu après décryptage des paquets limitent le trafic sur les ports non-autorisés
- *Attaques par le milieu* — Le codage du trafic distant permet d'atténuer les risques d'attaque de ce type
- *Sniffers de paquets* — Une infrastructure commutée limite l'efficacité des sniffers de paquets

Figure 8 - Rôles des méthodes d'atténuation des risques d'attaque sur les réseaux de taille moyenne pour les modules Internet d'entreprise



Lignes directrices du design

Les sections suivantes présentent les fonctions de chacune des unités du module Internet d'entreprise.

Routeur FAI

La fonction première du routeur à la frontière client du FAI est de fournir une connectivité vers l'Internet ou vers le réseau du FAI. Le routeur en sortie du FAI réduit le trafic non-essentiel qui dépasse les seuils prédéfinis afin de limiter les risques d'attaque par déni de service distribué. Enfin, au point de sortie du routeur du FAI, le filtrage RFC 1918 et RFC 2827 limite les risques d'une attaque par usurpation d'adresses source des réseaux locaux et des plages d'adresses privées.

Routeur frontière
La fonction du routeur frontière du réseau de taille moyenne est de fournir un point de démarcation entre le réseau FAI et le réseau de taille moyenne. Au point entrant du routeur frontière sur ce type de réseau, un filtrage élémentaire limite l'accès pour ne permettre que le passage du trafic IP escompté, ce qui représente un filtrage rudimentaire pour la plupart des attaques simples. Le filtrage RFC 1918 et RFC 2827 est également exécuté ici pour vérifier le filtrage réalisé par le FAI. De plus, et en raison de l'importance du risque lié à la fragmentation des paquets, le pare-feu est configuré pour rejeter la plupart des paquets fragmentés qui ne sont pas couramment associés au trafic standard sur l'Internet. La perte éventuelle du trafic légitime occasionnée par ce filtrage est considérée comme acceptable en comparaison du risque d'admettre le trafic dangereux. Enfin, le trafic IPSec destiné au pare-feu ou au concentrateur du VPN est autorisé. Le filtrage sur le routeur est configuré pour que seul le trafic IKE et IPSec puisse accéder au pare-feu ou au concentrateur du VPN. Comme sur les VPN à accès distant, l'adresse IP du système distant n'est généralement pas connue, le filtrage ne peut être défini que sur l'unité homologue de la site central(le concentrateur du VPN) avec laquelle les utilisateurs distants communiquent. Sur les VPN de site à site, l'adresse IP du site distant est généralement connue, et le filtrage peut, par conséquent, être défini pour le trafic VPN entre homologues et dans les deux sens.

Pare-feu
La fonction première d'un pare-feu est de faire appliquer les règles d'état de connexion et de réaliser un filtrage détaillé des sessions qui sont appelées à travers lui. Le pare-feu joue également le rôle de point de raccordement des tunnels IPSec des VPN de site à site, aussi bien pour le trafic du site de production distant que pour le trafic de gestion du site distant. De nombreux segments se situent en dehors du pare-feu. Le premier est le segment des services publics qui contient toutes les stations publiquement adressables. Le second concerne les VPN à accès distant et les réseaux commutés, dont il sera question par la suite. Les serveurs publiquement adressables disposent d'une certaine protection contre les saturations de synchronisation TCP SYN grâce à des mécanismes comme l'utilisation de systèmes de limitation des connexions semi-ouvertes sur le pare-feu. Quant au filtrage, en plus de limiter le trafic sur le segment des services publics vers les adresses et les ports concernés, il s'exerce également dans la direction opposée. Si un pirate parvient à s'emparer de l'un des serveurs publics (en trompant le pare-feu, le H-IDS et le N-IDS), il ne faut pas permettre à ce serveur de poursuivre l'attaque du réseau. Pour limiter le risque d'une telle attaque, un filtrage spécifique interdit à tous les serveurs publics de générer des requêtes non-autorisées en direction des autres emplacements. Par exemple, le serveur Web doit être filtré afin qu'il ne puisse pas émettre de requêtes par lui-même et qu'il se contente de répondre aux requêtes des clients. Cette configuration permet d'éviter qu'un pirate puisse télécharger des utilitaires supplémentaires vers l'unité dont il s'est emparé après l'attaque initiale. Elle contribue également à empêcher que des sessions indésirables puissent être ouvertes par le pirate au cours de l'attaque principale. Un exemple d'attaque de ce type est celle qui génère un xterm à partir du serveur Web et au travers du pare-feu vers l'ordinateur du pirate. De plus, un private VLAN empêche qu'un serveur public compromis puisse attaquer d'autres serveurs du même segment. Même le pare-feu ne parvient pas à détecter ce trafic, une constatation qui montre l'importance critique des private VLAN.

Détection des intrusions
Le segment des services publics comprend un système N-IDS. Sa fonction principale est de détecter les attaques sur les ports autorisés par la configuration du pare-feu. Il s'agit le plus souvent d'attaques sur la couche application contre des services particuliers. Le N-IDS sur le segment des services publics doit être configuré de manière restrictive car lorsqu'une signature est identifiée ici, cela signifie qu'elle a déjà réussi à passer le pare-feu. Chacun des serveurs possède également un H-IDS. La fonction première d'un H-IDS est de contrôler l'apparition d'activités suspectes au niveau du système d'exploitation, ainsi que d'activités dans les applications serveur communes (HTTP, FTP, SMTP, etc.). La station DNS doit être configurée pour ne répondre qu'aux commandes autorisées et éliminer toutes les réponses inutiles qui pourraient faciliter la reconnaissance de réseau par les pirates. Ceci comprend l'interdiction des transferts de zone quelle que soit leur provenance, à l'exception des serveurs DNS secondaires autorisés. Le serveur SMTP comprend des services d'inspection du contenu du courrier qui limitent les risques d'attaque – par virus ou par cheval de Troie – dirigées contre le réseau interne et qui sont généralement introduites par le système de courrier. Le pare-feu lui-même filtre les messages SMTP au niveau de la couche 7 pour ne transmettre au serveur de courrier que les commandes nécessaires.

Le serveur N-IDS dédié placé entre l'interface privée du pare-feu et le routeur interne exécute une dernière analyse des attaques. Il est probable que le nombre d'attaques détectées sur ce segment sera faible, car seules les réponses aux requêtes, quelques ports sélectionnés du segment des services publics et le trafic provenant du segment de l'accès à distance sont autorisés à l'intérieur. Les attaques qui parviendront sur ce segment seront certainement très élaborées car elles sous-entendent que le pirate a pu prendre le contrôle d'un système sur le segment des services publics et qu'il essaie d'exploiter cette position pour attaquer le
réseau interne. Par exemple, si un pirate a pu prendre le contrôle du serveur SMTP public, il peut chercher à attaquer le serveur de courrier interne sur le port TCP 25, qui est autorisé à permettre le transfert de courrier entre les deux stations. Si une attaque est décelée sur ce segment, la réponse qui y sera apportée doit être plus sévère que si elle apparaissait sur un autre segment, car elle signifie probablement que le pirate a déjà pris le contrôle d'une unité. Il convient alors d'envisager sérieusement d'utiliser des réinitialisations TCP ou des mesures d'exclusion pour contrer, par exemple, une attaque SMTP comme celle décrite plus haut.

Réseau privé virtuel à accès distant
La fonction première du concentrateur de VPN à accès distant est de fournir une connectivité sécurisée vers le réseau de taille moyenne pour ses utilisateurs distants. Le concentrateur du VPN démarre une session avec un serveur de contrôle d'accès sur le réseau interne qui identifie les utilisateurs avant de leur permettre l'accès au réseau. Le serveur de contrôle d'accès envoie ensuite une requête au système de mot de passe à usage unique (OTP) qui valide l'authentification de l'utilisateur. Les règles IPSec envoyées par le concentrateur au client empêchent les utilisateurs d'activer le dédoublement de tunnellisation et les forcent à accéder à l'Internet par l'intermédiaire de la connexion d'entreprise. Les paramètres IPSec utilisés sont l'algorithme 3DES (Triple Data Encryption Standard) pour le codage et SHA/HMAC (secure hash algorithm/hash-based message authentification code) pour l'intégrité des données. Une fois le tunnel VPN raccordé, le trafic passe par un pare-feu pour garantir un filtrage acceptable des utilisateurs. Cette configuration permet également d'effectuer un blocage IDS sur le pare-feu. Ce scénario s'oppose à de nombreux déploiements actuels qui placent le pare-feu devant l'unité VPN. Lorsque le pare-feu est placé devant, il est impossible de connaître les différents types de trafic utilisateur car le trafic est toujours chiffré.

Utilisateurs en accès entrant
Les utilisateurs en accès entrant sont généralement raccordés à un routeur d'accès équipé de modems intégrés. Lorsqu'une connexion de couche 2 est établie entre l'utilisateur et le serveur, une connexion en trois temps CHAP (Challenge Handshake Authentification Protocol) est établie pour identifier l'utilisateur. Comme pour le service VPN à accès distant, le serveur d'authentification, d'autorisation et de comptabilité (AAA) est sollicité pour l'authentification. Une fois identifié, l'utilisateur obtient une adresse IP provenant d'un ensemble d'adresses IP.

Commutateurs de couche 2
La fonction première des commutateurs du module Internet d'entreprise est de fournir une connectivité de couche 2 entre les différentes unités au sein du module. Nous avons choisi des commutateurs séparés, plutôt qu'un commutateur unique supportant plusieurs VLAN, afin de réaliser une séparation physique entre le segment extérieur, le segment des services publics, le segment VPN et le segment intérieur. Cette configuration limite les conséquences d'une éventuelle configuration défectueuse sur un commutateur qui aurait pour effet d'affaiblir la sécurité. De plus, chaque commutateur exécute la fonction de réseau local virtuel privé, une configuration qui permet de limiter les risques d'attaques reposant sur l'exploitation de la confiance.

Routeur intérieur
La fonction première d'un routeur intérieur est de fournir une séparation et un routage de couche 3 entre le module Internet d'entreprise et le module Campus. Cette unité fonctionne exactement comme un routeur sans qu'aucune liste d'accès ne restreigne le trafic avec l'une ou l'autre interface. Comme les informations de routage elles-mêmes peuvent être exploitées par une attaque par saturation, il est intéressant d'utiliser l'authentification des mises à jour de routage entre les unités afin de limiter les risques d'une telle attaque. Ce routeur fournit un point de démarcation final entre l'intranet routé et le monde extérieur. Comme la plupart des pare-feu sont configurés sans protocole de routage, il est important de fournir, à l'intérieur du module Internet d'entreprise, un point de routage qui ne dépende pas du reste du réseau.

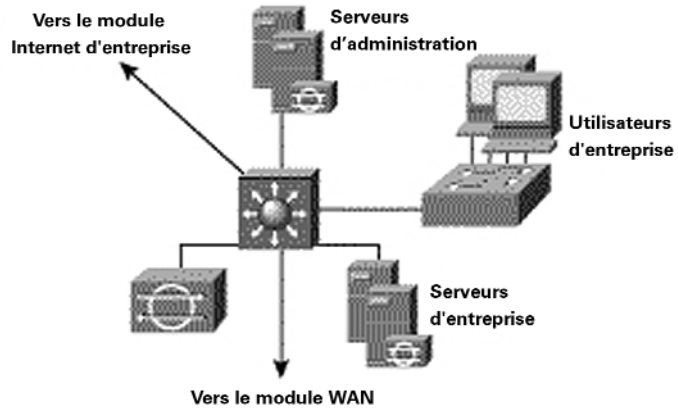
Autres possibilités
Il existe plusieurs choix possibles de design pour ce module. Au lieu de mettre en œuvre un filtrage sur le routeur frontière vers le réseau de taille moyenne, l'administrateur de réseau peut choisir d'installer également un serveur de filtrage adaptatif sur l'unité correspondante. La présence de deux serveurs de filtrage adaptatif offre une approche sécuritaire plus approfondie au sein du module. En fonction de la manière qu'a l'administrateur de réseau d'appréhender les attaques informatiques, il est possible d'installer un serveur N-IDS dédié devant le pare-feu. Grâce aux filtres élémentaires dédiés appropriés, l'IDS à l'extérieur du pare-feu peut fournir des renseignements importants concernant l'alerte et qui, sinon, pourraient être rejetées par le pare-feu. Comme ce segment génèrera probablement un nombre d'alertes élevé, il est préférable de leur accorder un niveau de gravité inférieur à celles qui sont détectées derrière le pare-feu. Vous pouvez également envisager de consigner les alarmes provenant de ce segment dans un journal conservé sur un poste de gestion distinct afin de s'assurer que les alarmes réelles des autres segments reçoivent l'attention qu'elles méritent. Grâce à la visibilité que fournit le N-IDS à l'extérieur du pare-feu, vous pourrez plus facilement évaluer les types d'attaques que suscite votre organisation. De plus, vous pourrez évaluer l'efficacité du filtrage du FAI et à la frontière de l'entreprise. Deux autres possibilités vous sont encore offertes. La première consiste à éliminer le routeur entre le pare-feu et le module Campus. Bien que ses fonctions puissent être intégrées dans le commutateur de couche 3 du module Campus, cette configuration a pour conséquence de supprimer la capacité du module Internet d'entreprise à fonctionner indépendamment des services de couche 3 provenant d'un autre secteur du réseau. La seconde consiste à ajouter une inspection de contenu en plus de l'inspection du contenu du courrier déjà programmée. Il est par exemple envisageable de placer un serveur de filtrage URL sur le segment des services publics afin de filtrer les types de pages Web auxquelles les employés ont le droit d'accéder.

Module Campus
Le module Campus contient les stations de travail pour les utilisateurs finaux, des serveurs intranet d'entreprise, des serveurs d'administration et l'infrastructure associée de couches 2 et 3 nécessaires au support des unités. Tous les modules Campus de SAFE Enterprise ont été regroupés dans un module unique. Cette configuration s'adapte de manière plus précise à la taille réduite des réseaux moyens, et limite le coût global du design. Comme dans le module Internet d'entreprise, la redondance qui apparaîtrait normalement dans un design de grande envergure a été supprimée du design du réseau de taille moyenne.

Principales unités

- *Commutateur de couche 3* — Assure le routage et la commutation du trafic de production et de gestion dans le module Campus, fournit des services au niveau de la couche distribution à destination des commutateurs d'immeuble, et supporte les services évolués comme le filtrage de trafic
- *Commutateurs de couche 2 (avec support pour les réseaux locaux virtuels privés)* — Fournissent des services de couche 2 aux stations de travail utilisateur
- *Serveurs d'entreprise* — Fournissent les services de courrier électronique (SMTP et POP3) aux utilisateurs internes ainsi que les services de livraison de fichiers, d'impression et de DNS aux stations de travail
- *Stations de travail utilisateur* — Fournissent des services de données aux utilisateurs autorisés sur le réseau
- *Hôte d'administration SNMP* — Fournit des services d'administration SNMP aux unités
- *Hôte N-IDS* — Assure l'agrégation des alarmes de toutes les unités N-IDS du réseau
- *Hôte(s) Syslog* — Regroupe(nt) les informations journal du pare-feu et des stations N-IDS
- *Serveur de contrôle d'accès* — Fournit des services d'authentification aux unités du réseau
- *Serveur de mots de passe à usage unique (OTP)* — Permet la transmission des informations de mot de passe de session au serveur de contrôle d'accès
- *Hôte d'administration système* — Assure les changements de configuration, de logiciel et de contenu sur les unités
- *Serveur N-IDS dédié* — Assure le contrôle de couche de 4 à 7 des segments clé du réseau dans le module

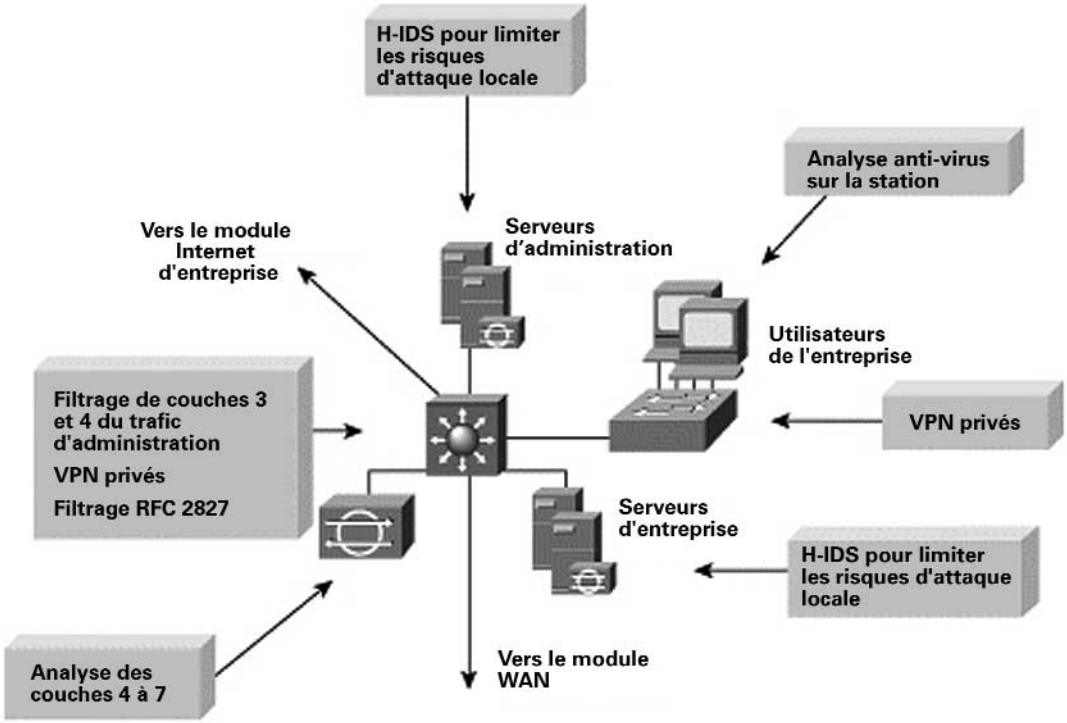
Figure 9 - Modèle détaillé du module Campus du réseau de taille moyenne



Atténuation des risques

- *Sniffers de paquets* — Une infrastructure commutée limite l'efficacité des sniffers de paquets
- *Application virus et cheval de Troie* — L'analyse anti-virus réalisé sur la station permet d'éliminer la plupart des virus et de nombreuses applications "cheval de Troie"
- *Accès non autorisé* — La détection des intrusions à partir de la station ainsi que le contrôle d'accès des applications permettent de réduire ce type d'accès
- *Attaques sur les mots de passes* — Le serveur de contrôle d'accès autorise l'authentification forte à deux facteurs pour les applications clé
- *Attaques sur la couche application* — Les systèmes d'exploitation, les unités et les applications sont maintenues à jour grâce aux derniers correctifs de sécurité et sont protégés par un H-IDS
- Usurpation d'adresse Internet — Le filtrage RFC 2827 évite l'usurpation d'adresses source
- *Exploitation de la confiance* — Les accords de confiance sont très explicites ; les Private VLAN empêchent que les stations d'un même sous-réseau puissent communiquer à moins que cela ne soit nécessité
- *Réacheminement des ports* — le H-IDS empêche l'installation d'agents de réacheminement des ports

Figure 10 - Rôles d'atténuation des risques d'attaque sur les réseaux de taille moyenne pour le module Campus



Lignes directrices du design

Les sections suivantes présentent les fonctions de chacune des unités du module Campus.

Commutateur de cœur de réseau

La fonction première du commutateur de cœur de réseau est de fournir des services de routage ou de commutation pour le trafic de production et de gestion, des services de la couche distribution (routage, qualité de service [QS] et contrôle d'accès) pour les commutateurs d'immeuble, la connectivité des serveurs d'administration et d'entreprise, et des services évolués comme le filtrage du trafic entre les sous-réseaux. Un commutateur de couche 3 a été préféré à un commutateur de couche 2 afin de réaliser un VLAN pour le(s) segment(s) des serveurs d'entreprise, le segment du serveur d'administration, le(s) segment(s) des utilisateurs d'entreprise, et la connectivité vers le module WAN et le module Internet d'entreprise. Le commutateur de couche 3 offre une ligne de défense et de prévention contre les attaques provenant de l'intérieur. Il peut réduire la probabilité que, dans une entreprise, un service parvienne à accéder aux informations confidentielles du serveur d'un autre service en exploitant le contrôle d'accès. Un réseau qui sert, par exemple, un service de marketing et un service recherche et développement peut créer un segment pour le serveur R&D vers un réseau local virtuel particulier et en filtrer l'accès pour s'assurer que seuls les personnels de la recherche et du développement pourront y accéder. Pour des questions de performances, il est important que ce contrôle d'accès puisse être mis en œuvre sur une plate-forme matérielle capable de fournir le trafic filtré à un débit proche du débit maximal. Cette configuration impose le plus souvent l'emploi d'une commutation de couche 3 par opposition aux unités de routage plus conventionnelles. Ce même contrôle d'accès doit également pouvoir empêcher l'usurpation d'adresses sources locales grâce au filtrage RFC 2827. Le filtrage RFC 2827 doit être installé sur les VLAN des utilisateurs d'entreprise et de serveur intranet d'entreprise.

Dans chacun de ces VLAN, des private VLAN peuvent servir à réduire les risques d'attaque par exploitation de la confiance entre les unités. Par exemple, sur le segment du serveur d'entreprise, il est possible d'interdire aux serveurs individuels de communiquer entre eux, car ils ont uniquement besoin de communiquer avec les unités connectées aux segments de l'utilisateur d'entreprise.

Afin de fournir une ligne de défense supplémentaire aux serveurs d'administration, un filtrage complet des couches 3 et 4 a été configuré en sortie sur l'interface du réseau local virtuel qui se connecte au segment du serveur d'administration. L'ACL ne réduit la connectivité en provenance et en direction des serveurs d'administration qu'avec les unités (par l'intermédiaire de leurs adresses IP) sous leur contrôle, et uniquement pour les protocoles et services (par l'intermédiaire du numéro de port) requis. Ceci comprend également le contrôle d'accès pour le trafic de gestion destiné aux unités du site distant. Ce trafic est chiffré par le pare-feu et envoyé aux sites distants. Un contrôle supplémentaire s'exerce sur les accès aux unités administrées en ne permettant qu'aux connexions déjà établies de revenir sur l'ACL.

Commutateurs d'immeuble
La fonction première des commutateurs d'immeuble du module Campus est de fournir des services de couche 2 aux stations de travail de l'utilisateur d'entreprise. Les private VLAN sont installés sur les commutateurs d'immeuble afin de limiter les risques d'une attaque par exploitation de la confiance, car les stations de travail individuelles des utilisateurs finaux n'ont généralement pas besoin de communiquer entre elles. En plus des consignes de sécurité réseau décrites dans l'axiome sur la sécurité des commutateurs, une analyse anti-virus au niveau de la station est également installé au niveau du poste de travail.

Détection des intrusions
Le module Campus possède également un serveur N-IDS dédié. Le port de commutateur connecté au serveur N-IDS dédié est configuré de telle sorte que le trafic à contrôler provenant de tous les VLAN est dupliqué dans le port de contrôle du serveur dédié. Il est probable que le nombre d'attaques détectées à cet endroit sera très faible car le serveur N-IDS dédié permet l'analyse des attaques provenant de l'intérieur du module Campus lui-même. Si, par exemple, un pirate a pu prendre le contrôle d'une station de travail utilisateur en raison d'une connexion modem inconnue sur cet hôte, le N-IDS pourra détecter une activité suspecte provenant de l'intérieur du réseau étendu. D'autres attaques internes peuvent provenir d'employés mécontents, de stations de travail installées dans des lieux où des personnes non autorisées peuvent y accéder, ou d'applications – cheval de Troie – enregistrées par inadvertance sur des PC portables. Chaque serveur d'administration et d'intranet d'entreprise est également équipé d'un H-IDS.

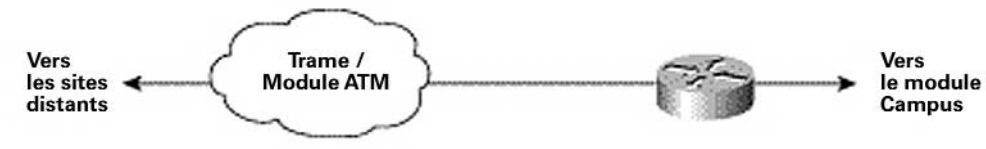
Autres possibilités
Si le réseau de taille moyenne est suffisamment petit, les commutateurs d'immeuble peuvent être supprimés en attribuant leurs fonctions au commutateur de cœur de réseau. Dans ce cas, les stations de travail des utilisateurs finaux seront directement connectés au commutateur de cœur de réseau. Les fonctions du réseau local virtuel seront installées sur le commutateur de cœur de réseau afin de limiter les risques d'attaque par exploitation de la confiance. S'il n'est pas nécessaire que le réseau interne soit particulièrement performant, il est possible d'utiliser un routeur et un commutateur de couche 2 distincts pour les fonctions de cœur de réseau et de distribution au lieu d'un commutateur de couche 3 à hautes performances.

Si on le désire, le serveur N-IDS dédié peut être remplacé par un module IDS intégré qui s'insère dans le commutateur de cœur de réseau. Cette configuration augmente le débit du trafic dans le module IDS car il s'installe sur le fond de panier du commutateur et non sur un unique port Ethernet à 10/100 Mbps. Les ACL du commutateur peuvent servir à contrôler le type de trafic envoyé au module IDS.

Module WAN
Le module WAN ne doit être inclus que s'il est nécessaire de réaliser des connexions sur un réseau privé vers des sites distants : par exemple lorsque les contraintes en termes de qualité de service ne peuvent pas être satisfaites par un VPN IPSec, où lorsque les connexions WAN existent déjà et que le coût d'une migration vers IPSec ne se justifie pas.

Principales unités
• *Routeur IOS* — Fournit les mécanismes de routage, de contrôle d'accès et de qualité de service aux sites distants

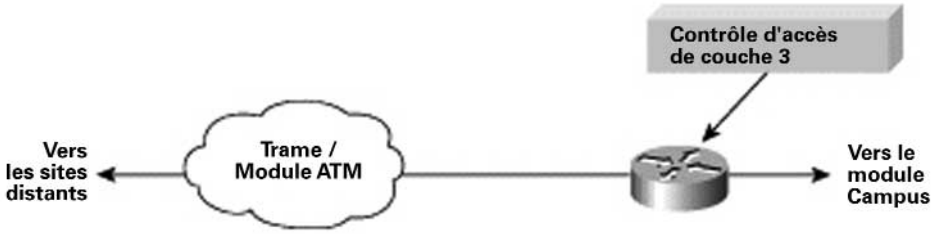
Figure 11 - Modèle détaillé du module WAN d'un réseau de taille moyenne



Atténuation des risques

- *Usurpation d'adresse Internet* — L'usurpation d'adresse Internet peut être atténuée par un filtrage de couche 3
- *Accès non autorisé* — Un simple contrôle d'accès sur le routeur peut limiter les types de protocoles auxquels les site distants ont accès

Figure 12 - Rôles d'atténuation des risques d'attaque sur le module WAN



Lignes directrices du design

Le niveau de protection installé dans le module WAN dépendra du niveau de confiance accordé aux sites distants et au FAI auquel vous êtes connecté. Cette protection est assurée par l'utilisation de fonctions de sécurité interentreprises. Dans ce design, on utilise des listes d'accès entrantes appliquées à l'interface série pour empêcher la totalité du trafic indésirable d'accéder au réseau de taille moyenne. Il est également possible d'utiliser des listes d'accès entrantes appliquées à l'interface Ethernet pour limiter davantage le type de trafic qui retourne du réseau de taille moyenne vers les sites distants.

Autres possibilités

Certaines entreprises qui sont extrêmement soucieuses de la confidentialité de leurs informations codent le trafic sur leurs liaisons classiques WAN. De même que sur un VPN de site à site, le protocole IPSec peut servir à obtenir ce niveau de confidentialité des informations. De plus, l'exécution d'un pare-feu sur le routeur WAN peut fournir des options supplémentaires de contrôle d'accès par rapport aux listes de contrôle d'accès élémentaires utilisées dans le design SAFE.

Comparaison site central site distant

Lorsque le réseau de taille moyenne est configuré en tant que site distant, plusieurs composants peuvent être éliminés. La première question consiste à déterminer si l'entreprise désire se connecter au siège social par une liaison privée WAN ou par un VPN IPSec. Parmi les raisons qui plaident en faveur du réseau privé WAN, citons un support adaptatif de la qualité de service, un support de diffusion multipoints, la fiabilité de l'infrastructure réseau ou la nécessité d'un protocole autre que IP. Rappelez-vous que si vous utilisez le protocole IPSec sur l'encapsulation GRE (generic routing encapsulation) – voir SAFE Enterprise – le trafic de diffusion multipoints et non-IP peut être supporté dans un environnement de VPN. Il existe plusieurs raisons de préférer un VPN IPSec à une connexion privée WAN. Tout d'abord, un VPN IPSec sur l'Internet offre un accès Internet local à tous les sites distants, ce qui économise la bande passante – et les coûts – au niveau du site central. De plus, dans de nombreuses applications nationales et dans la plupart des applications internationales, le VPN IPSec permet de réaliser des économies importantes par rapport aux connexions privées WAN.

Si vous optez pour une connexion privée WAN pour le réseau de taille moyenne opérant en tant que site distant, et à moins que vous n'ayez besoin d'un accès local à l'Internet à partir de ce site distant, il n'est pas nécessaire de conserver la totalité du module Internet d'entreprise. En revanche, si vous choisissez un VPN IPSec, le module WAN n'est pas nécessaire. En plus du module WAN, le réseau de taille moyenne opérant en tant que site distant n'a pas besoin d'un concentrateur VPN ou d'un routeur à accès commuté pour accéder aux services d'accès distants si les services sont fournis par le siège social.

Du point de vue de l'administration, la configuration et la gestion de sécurité du réseau de taille moyenne s'effectuent le plus souvent à partir du module de gestion du siège social, en supposant que les ressources informatiques y soient centralisées. Si vous choisissez une connexion privée WAN pour la connectivité entre les sites, le trafic de gestion peut facilement traverser le module WAN pour atteindre les unités à administrer. Si vous choisissez un VPN IPSec pour la connectivité entre les sites, l'essentiel du trafic de gestion peut circuler comme dans le cas d'une connexion privée WAN. Certaines unités, comme le routeur frontière à l'extérieur du pare-feu, ne seront pas intégrées au tunnel IPSec et devront être administrées d'une autre manière. Une telle configuration pourrait comprendre un tunnel IPSec distinct vers l'unité ou s'appuyer sur un codage de la couche application (SSH) afin d'effectuer les modifications de configuration nécessaire sur une telle unité. Comme nous l'avons rappelé dans les axiomes, certains protocoles d'administration ne possèdent pas de variante sécurisée.

Design pour l'utilisateur distant

Cette section présente quatre options différentes pour fournir une connectivité d'utilisateur distant dans le design SAFE. La connectivité à distance concerne aussi bien les travailleurs mobiles que les télétravailleurs. L'objectif principal de ces designs est de fournir une connectivité aux sites distants vers le siège social et, d'une certaine manière, à l'Internet. Les quatre options suivantes se décomposent en solutions logiciel seul, logiciel et matériel, et matériel seul :

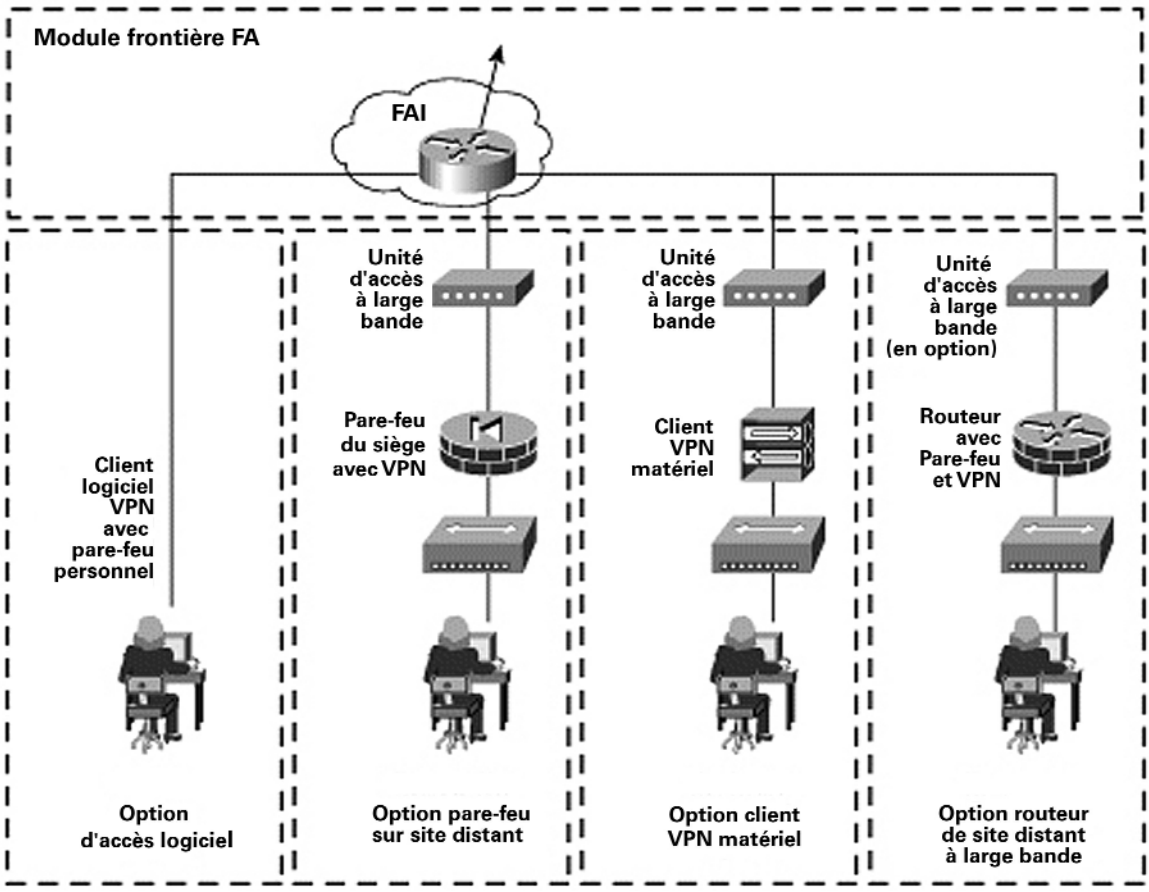
- *Option d'accès logiciel* — L'utilisateur distant possède un logiciel client VPN et un logiciel pare-feu personnel sur son PC
- *Option pare-feu sur site distant* — Le site distant est protégé par un pare-feu dédié qui fournit des services de pare-feu et une connectivité VPN IPSec vers le siège social ; la connectivité WAN est assurée par une unité d'accès à large bande fournie par le FAI (modem câble ou DSL, par exemple)
- *Option client VPN matériel* — Le site distant utilise un client VPN matériel dédié qui assure la connectivité VPN IPSec vers le siège social ; la connectivité WAN est assurée par une unité d'accès à large bande fournie par le FAI
- *Option routeur de site distant* — Le site distant utilise un routeur qui fournit des services de pare-feu et une connectivité VPN IPSec vers le siège social. Ce routeur peut fournir un accès direct à large bande ou bien passer par une unité d'accès à large bande fournie par le FAI.

Chacun de ces designs est présenté en détail dans la section sur les lignes directrices du design ci-dessous. Toutes les présentations supposent que la connectivité s'effectue par l'Internet. Si l'on utilise, en revanche, une connectivité WAN privé (RNIS, DSL privé, etc.), il est possible de se passer du codage du trafic. Rappelez-vous que dans chacune de ces options pour sites distants, le périmètre de sécurité de votre organisation est élargi pour inclure ces mêmes sites distants.

Principales unités

- *Unité d'accès à large bande* — Fournit un accès sécurisé au réseau à large bande (DSL, câble, etc)
- *Pare-feu avec support VPN* — Fournit des tunnels sécurisés chiffrés de bout en bout entre le site distant et le site central de l'entreprise ; assure une protection au niveau réseau des ressources des sites distants et un filtrage adaptatif du trafic
- *Concentrateur de couche 2* — Fournit une connectivité pour les unités au sein du site distant ; il peut être intégré au pare-feu ou au client VPN matériel)
- *Logiciel pare-feu personnel* — Apporte aux PC une protection individuelle au niveau de l'unité
- *Routeur avec pare-feu et support VPN* — Fournit des tunnels sécurisés chiffrés de bout en bout entre le site distant et la site centralde l'entreprise ; assure une protection au niveau réseau des ressources des sites distants et un filtrage adaptatif du trafic ; peut fournir des services évolués (voix, qualité de service, etc.)
- *VPN logiciel client* — fournit des tunnels sécurisés chiffrés de bout en bout entre les PC individuels et la site centralde l'entreprise
- *VPN matériel client* — fournit des tunnels sécurisés chiffrés de bout en bout entre le site distant et la site centralde l'entreprise

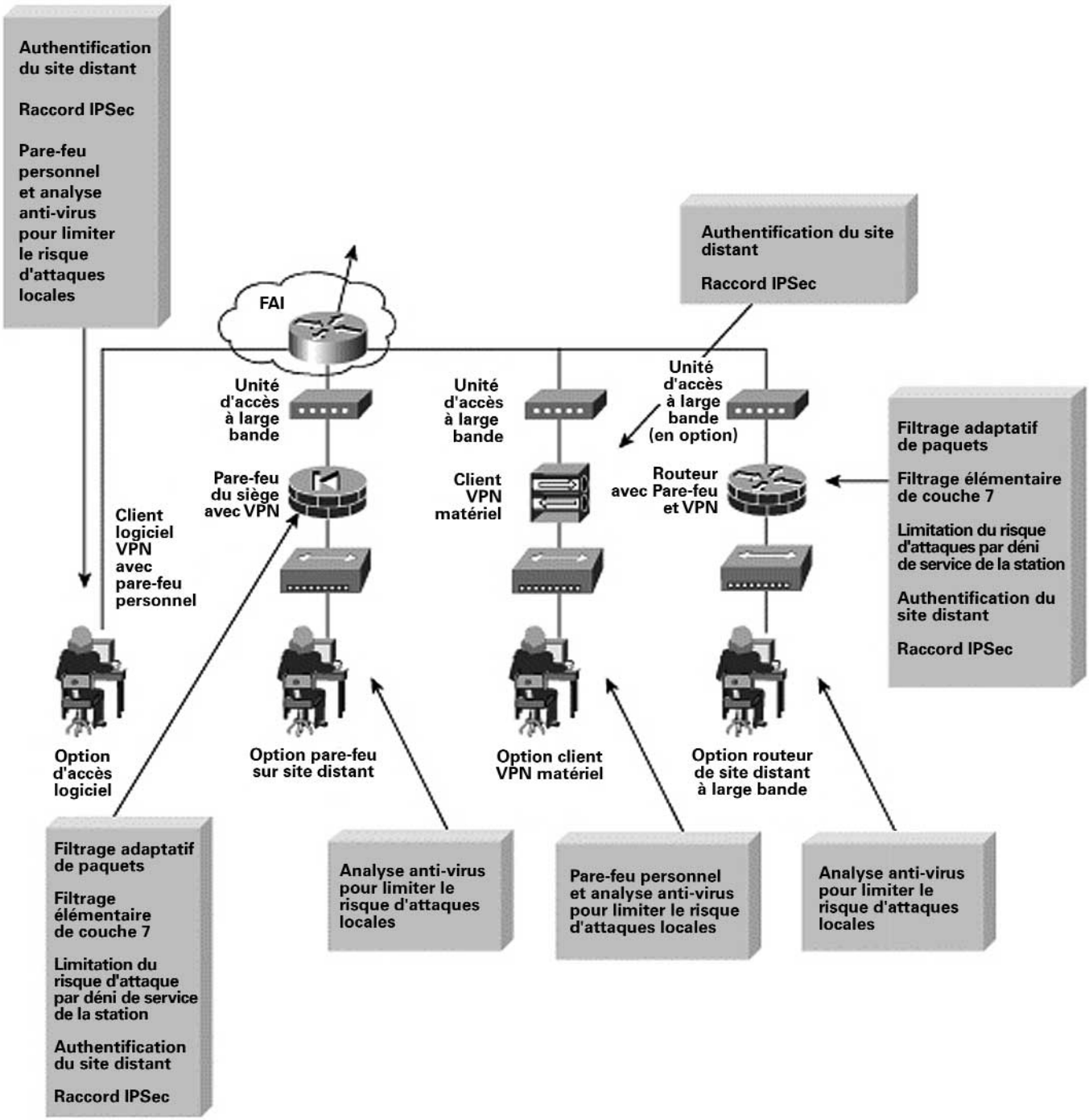
Figure 13 - Modèle détaillé de la configuration d'utilisateur distant



Atténuation des risques

- *Accès non autorisé* — Atténué par le filtrage et l'inspection adaptative des sessions sur le pare-feu ou le routeur du site distant, ou par le contrôle d'accès aux applications grâce au logiciel de pare-feu personnel.
- *Reconnaissance de réseau* — Les protocoles sont filtrés sur le site distant pour limiter l'efficacité de l'attaque
- *Attaques par virus ou par cheval de Troie* — Limitées par l'analyse anti-virus au niveau de la station
- *Usurpation d'adresse Internet* — Limitée grâce au filtrage RFC 2827 et 1918 à la frontière avec le FAI et sur les unités des sites distants
- *Attaques par le milieu* — Limitées par le codage du trafic distant

Figure 14 - Rôles d'atténuation des risques d'attaque dans le design pour utilisateurs distants



Lignes directrices du design

Les sections suivantes présentent les fonctions de chacune des options de connectivité de l'utilisateur distant.

Option d'accès logiciel
L'option d'accès logiciel concerne aussi bien les travailleurs mobiles que les télétravailleurs. L'utilisateur distant n'a besoin que d'un PC avec un logiciel de client VPN et d'une connectivité Internet ou de réseau FAI par l'intermédiaire d'une connexion commutée ou Ethernet. La fonction première du logiciel de client VPN est d'établir un tunnel chiffré et sécurisé entre l'unité client et une unité VPN du site central. L'accès et les autorisations de réseau sont contrôlés à partir du siège social au moment où s'effectue le filtrage sur le pare-feu et sur le client lui-même lorsque des droits d'accès sont poussés conformément à la politique de connexion du réseau. L'utilisateur distant est tout d'abord identifié avant de recevoir des paramètres IP comme une adresse IP virtuelle qui servira pour tout le trafic VPN, ainsi que l'emplacement des serveurs de noms (DNS et WINS [Windows Internet Name Service]). Le site central dispose également de la possibilité d'activer ou de désactiver le dédoublement de tunnellisation. Dans le design SAFE, le dédoublement de tunnellisation a été désactivé ce qui impose à tous les utilisateurs distants d'accéder à l'Internet par l'intermédiaire de la connexion d'entreprise lorsqu'un tunnel VPN a été établi. Comme l'utilisateur distant peut ne pas toujours vouloir qu'un tunnel VPN soit établi lorsqu'il se connecte à l'Internet ou au réseau du FAI, nous recommandons l'emploi d'un logiciel pare-feu afin de réduire le risque d'un accès non-autorisé au PC. Nous recommandons également un logiciel d'analyse anti-virus pour réduire le risque d'infection du PC par des virus ou des "chevaux de Troie".

Option pare-feu sur site distant
L'option pare-feu sur site distant concerne le télétravailleur, et éventuellement, une très petite filiale. Dans cette option, on suppose que le site distant dispose d'un moyen d'accès à large bande auprès d'un fournisseur d'accès. Le pare-feu est installé derrière le DSL ou le modem câble.

La fonction première du pare-feu est d'établir un tunnel chiffré et sécurisé entre lui-même et une unité VPN du site central, de faire appliquer les règles d'état de connexion et d'appliquer un filtrage détaillé aux sessions qui passent par lui. Les PC individuels du réseau du site distant n'ont pas besoin de logiciel client VPN pour accéder aux ressources d'entreprise. De plus, et comme le pare-feu adaptatif protège au plus bas niveau l'accès à l'Internet, un logiciel de pare-feu personnel n'est pas absolument indispensable sur chaque PC. Toutefois, si l'administrateur de réseau désire un niveau supplémentaire de protection, ces logiciels de pare-feu personnels peuvent être installés sur les PC du site distant. Cette configuration peut être utile si le travailleur à domicile se déplace également et se connecte directement à l'Internet sur un réseau public. Comme un pare-feu adaptatif protège les stations, le site distant peut obtenir un accès direct à l'Internet plutôt que de faire transiter tout le trafic par le siège de l'entreprise. A moins que vous n'utilisiez une traduction d'adresses réseau pour communiquer avec le siège, les adresses IP des unités du site distant doivent être assignées de manière à ne pas recouvrir l'espace d'adressage du siège social ou d'un autre site distant. Les unités de site distant qui nécessitent un accès direct à l'Internet auront besoin d'une traduction d'adresse vers une adresse enregistrée. Cette traduction peut s'effectuer en traduisant toutes les sessions en direction de l'Internet vers l'adresse IP publique du pare-feu lui-même.

L'accès et les autorisations du réseau d'entreprise et de l'Internet sont contrôlés par la configuration du pare-feu de site distant et par celle de l'unité VPN du site central. L'administration de la configuration et de la sécurité du pare-feu du site distant peut être réalisée grâce à un tunnel IPSec entre la partie publique du pare-feu et le siège social de l'entreprise. Cette configuration permet de s'assurer que l'utilisateur de site distant n'aura pas besoin de modifier la configuration du pare-feu installé dans son propre bureau. Une fonction d'authentification devra être installée sur le pare-feu afin d'empêcher un utilisateur local de modifier par inadvertance la configuration de son pare-feu et de compromettre par la même les modalités de sécurité de l'équipement. Cette option ne permet pas d'identifier les utilisateurs individuels du site distant qui accèdent au réseau d'entreprise. En revanche, le pare-feu du site distant et le VPN du site central effectuent une authentification de l'unité.

Nous recommandons l'utilisation d'un logiciel anti-virus pour réduire le risque d'infection par les virus ou les "chevaux de Troie", aussi bien sur le site distant que sur tous les PC de l'entreprise.

Option client VPN matériel
L'option client VPN matériel est identique à l'option pare-feu sur site distant à ceci près que le client VPN matériel ne dispose pas d'un pare-feu adaptatif résident. Cette configuration exige l'utilisation d'un pare-feu personnel sur chaque station, particulièrement lorsque le dédoublement de tunnellisation est autorisé. Sans pare-feu personnel, la sécurité de chacune des stations situées derrière l'unité VPN dépend de la capacité de l'agresseur à contourner la technique de traduction d'adresses de réseau. En effet, lorsque le dédoublement de tunnellisation est activé, les connexions vers l'Internet passent au travers d'un système de traduction d'adresses réseau simple à origines multiples mais à destination unique, et ne subissent aucun filtrage de couche 4 ou au-dessus. Lorsque le dédoublement de tunnellisation est désactivé, tous les accès vers l'Internet doivent passer par le siège social. Cette configuration réduit en partie la nécessité d'un pare-feu personnel sur les extrémités.
L'utilisation d'un client VPN matériel présente deux avantages principaux. Tout d'abord, comme pour le client VPN logiciel, l'accès et les autorisations concernant le réseau d'entreprise et l'Internet sont contrôlés de manière centralisée à partir du siège social. Les opérations de configuration et d'administration de sécurité de l'unité matérielle de client VPN elle-même sont assurées par l'intermédiaire d'une connexion SSL en provenance du site central. Cette configuration permet de s'assurer que l'utilisateur de site distant n'aura pas besoin de modifier la configuration du client VPN matériel.

Le second avantage de l'option client VPN matériel est que les PC individuels du réseau du site distant n'ont pas besoin de logiciel client VPN pour accéder aux ressources de l'entreprise. Toutefois, cette option ne permet pas d'identifier les utilisateurs individuels du site distant qui accèdent au réseau d'entreprise. En revanche, le client VPN matériel et le concentrateur de site central VPN s'identifient réciproquement.

Option routeur de site distant
L'option routeur de site distant est pratiquement identique à l'option pare-feu sur site distant à quelques rares exceptions près. Lorsqu'il est déployé derrière un équipement autonome d'accès à large bande, l'unique différence réside dans sa capacité à supporter des applications évoluées comme la qualité de service, le routage et d'autres options d'encapsulation. De plus, si le routeur est doté d'une capacité large bande, il n'est plus nécessaire d'employer un équipement autonome d'accès à large bande. Cette option exige que votre FAI vous autorise à gérer le routeur haut débit lui-même, un scénario peu commun.

Stratégies de migration

SAFE est un guide pour la mise en œuvre d'une sécurité sur les réseaux. SAFE n'est pas destiné à servir de politique de sécurité pour les réseaux, pas plus qu'il ne constitue un moyen exhaustif pour doter les réseaux existants d'un système complet de sécurité. En revanche, SAFE est un modèle qui permet aux concepteurs de réseaux d'envisager la manière dont ils vont concevoir et mettre en œuvre le réseau d'une entreprise afin de satisfaire à ses besoins en matière de sécurité.

La première étape de la migration d'un réseau vers une infrastructure sécurisée est l'établissement d'une politique de sécurité. Vous trouverez à la fin de ce document, à l'annexe B, “Introduction à la sécurité réseau”, des recommandations élémentaires pour l'établissement d'une politique de sécurité. Une fois cette politique mise en place, le concepteur de réseau devra étudier les axiomes de sécurité décrits dans la première section de ce document et comprendre dans quelle mesure ils apportent des détails supplémentaires pour adapter la politique sur l'infrastructure de réseau existante.

L'architecture est suffisamment souple pour permettre à SAFE de s'adapter à la plupart des réseaux. SAFE permet au concepteur de répondre aux besoins de sécurité de chaque fonction de réseau presque indépendamment l'une de l'autre. En général, chaque module est "monobloc" et suppose que tout module interconnecté est doté d'un niveau de sécurité élémentaire. Cette configuration permet aux concepteurs de réseaux d'adopter une démarche par étapes pour sécuriser le réseau de l'entreprise. Ils peuvent s'occuper d'assurer la protection des fonctions les plus importantes du réseau conformément à la politique de sécurité définie, sans avoir à redessiner l'ensemble du réseau.

Ceci est le second livre blanc qui décrit les caractéristiques de l'architecture SAFE. Associé à SAFE Enterprise, le présent document répond à toutes les questions concernant les besoins de sécurité et la mise en œuvre d'une protection pour des réseaux de tailles différentes. Les auteurs ont conscience que de nombreux autres domaines nécessitent de plus amples recherches, investigations et améliorations. En voici une liste non exhaustive :

- Analyse et mise en œuvre d'une gestion en profondeur de la sécurité
- Analyse et mise en œuvre en profondeur de l'authentification, des services d'annuaires, des technologies AAA et des autorités de certification
- Etude en profondeur du design, de l'administration et de la mise en œuvre du sans-fil.

Annexe A : Laboratoire de validation

Nous avons développé une mise en œuvre de référence pour valider les fonctionnalités décrites dans ce document. Cette annexe présente en détail les configurations des différentes unités de chaque module ainsi que les directives globales associées. Voici différents extraits de configuration provenant des équipements actifs du laboratoire. Les auteurs ne recommandent pas d'appliquer directement ces configurations à un réseau de production.

Directives globales

Les exemples de commandes présentés dans cette section correspondent, en partie, aux axiomes SAFE dont il a été question plus haut dans ce document.

Routeurs

Voici quelques exemples de commandes qui permettent l'activation de la plupart des options élémentaires de configuration présentes sur la plupart des routeurs du laboratoire.

```
! Désactivez les services inutiles
!
no ip domain-lookup
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-servers
no service tcp-small-servers

! Activez la journalisation et le protocole SNMP en lecture seule
!
service timestamp log datetime localtime
logging 10.3.8.254
logging 10.3.8.253
snmp-server community Txo~QbW3XM ro 98

! Générez les clés RSA et activez l'accès SSH. Ceci suppose que le routeur supporte les fonctions de codage.
! Un message s'affiche vous demandant la longueur de la clé RSA. Pour la mise en œuvre du laboratoire SAFE,
! nous avons choisi 1024 bits
!
crypto key generate rsa
ip ssh timeout 120
ip ssh authentication-retries 5

! Définissez les mots de passe et les restrictions d'accès
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
!
!
access-list 99 permit host 10.3.8.254
access-list 99 deny any log

!
access-list 98 permit host 10.3.8.253
access-list 98 permit host 10.3.8.254
access-list 98 deny any log
!
line vty 0 4
access-class 99 in
login authentication default
password 0 X)[^j+#T98
exec-timeout 2 0
transport input ssh
transport output none
line con 0
login authentication no_tacacs
password 0 X)[^j+#T98
exec-timeout 2 0
transport input none
line aux 0
transport input none
password 0 X)[^j+#T98
no exec
!
banner motd #
```

```
Ceci est un système privé administré pour et par l'unité métier Cisco VSEC.
L'utilisation de ce système est soumise à l'autorisation de la direction de Cisco VSEC.
L'utilisation par toute personne non autorisée est strictement interdite.

#
```

Activez le protocole NTP avec authentification et contrôle d'accès

```
!
clock timezone PST -8
clock summer-time PST recurring
!
ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 10.3.4.4 key 1
!
access-list 96 permit host 10.3.4.4
access-list 96 deny any log
```

Activez le protocole AAA

```
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs line
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting network start-stop tacacs+
aaa accounting exec start-stop tacacs+
!
tacacs-server host 10.3.8.253 single-connection
tacacs-server key SJj)j~t]6-
```

Les exemples de commande suivants définissent les paramètres d'authentification OSPF (Open Shortest Path First) pour les routeurs à l'intérieur du réseau. Notez que ces configurations utilisent l'authentification MD5 (message Digest 5).

```
interface FastEthernet1/0
ip address 10.3.3.3 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 8R%xi!0eUUxF
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 10.3.3.0 0.0.0.255 area 1
network 10.3.4.0 0.0.0.255 area 1
```

Commutateurs

Voici quelques exemples de commandes qui activent la plupart des options élémentaires de configuration présentes sur la plupart des commutateurs Catalyst ® IOS du laboratoire. Les commutateurs Cisco IOS ® utilisent une configuration presque identique à celle du routeur.

! Activez le protocole NTP

```
!
set timezone PST -8
set summertime PST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 10.3.4.4 key 1
set ntp client enable
```

Désactivez les services inutiles

```
!
set cdp disable
set ip http server disable
```

Activez la journalisation et le protocole SNMP

```
!
set logging server 10.3.8.253
set logging server 10.3.8.254
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 10.3.8.254 snmp
```

Activez le protocole AAA

```
!
set tacacs server 10.3.8.253 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
```

Définissez les mots de passe et les limitations d'accès

```
!
set banner motd <c>

Ceci est un système privé administré pour et par l'unité métier Cisco VSEC.
L'utilisation de ce système est soumise à l'autorisation de la direction de Cisco VSEC.
L'utilisation par toute personne non autorisée est strictement interdite.

<c>
```

! Le mot de passe de la console est défini par 'set password'
! Saisissez l'ancien mot de passe suivi du nouveau mot de passe
! Mot de passe de la console = X)[^j+#T98

```
!
```

! Le mot de passe d'activation est défini par 'set enable'
! Saisissez l'ancien mot de passe suivi du nouveau mot de passe
! Mot de passe d'activation = %Z<)|z9~zq

```
!
```

! Le mot de passe de configuration suivant ne fonctionne que la première fois

```
!
set password

X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
```

! Le mot de passe de configuration ci-dessus ne fonctionne que la première fois

```
!
set logout 2
set ip permit enable telnet
set ip permit 10.3.8.253 255.255.255.255 telnet
set ip permit 10.3.8.254 255.255.255.255 telnet
```

Stations

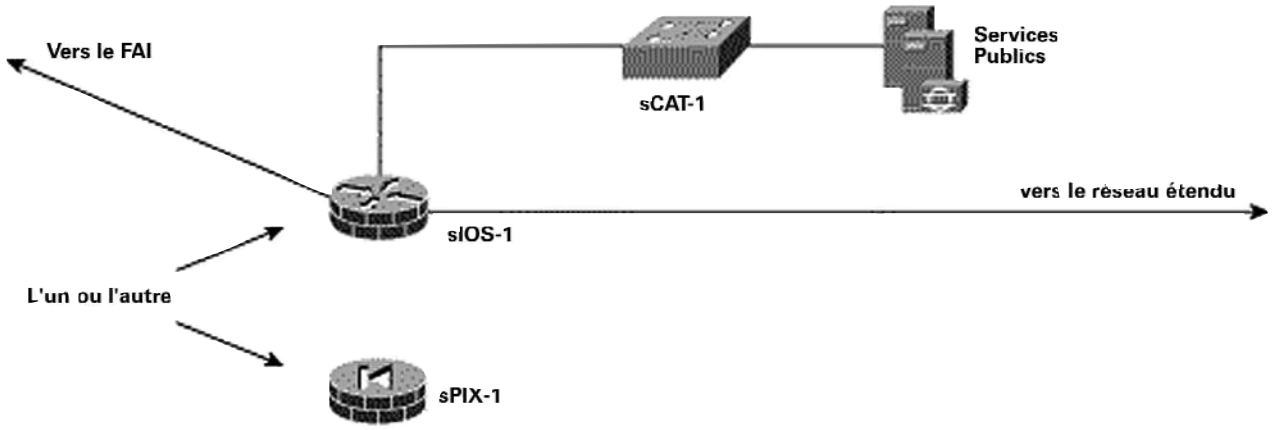
Comme nous l'avons décrit dans la section Axiomes, les systèmes d'exploitation et les applications des stations exécutaient un H-IDS et avaient intégré les patches et les correctifs les plus récents. L'application H-IDS utilisée au laboratoire est l'application Entercept de Entercept Security Technologies. Pour plus d'informations, consultez le site http://www.entercept.com.

Configurations de petit réseau

Voici quelques extraits de la configuration du petit réseau SAFE.

Module Internet d'entreprise

Figure 15 - Modèle détaillé du module Internet d'entreprise d'un petit réseau



Produits utilisés

- Commutateur de couche 2 Cisco Catalyst (sCAT-1)
- Routeur Cisco IOS avec support de codage 3DES (Triple Data Encryption Standard) (sIOS-1)
- Pare-feu sécurisé Cisco PIX (sPIX-1)
- H-IDS Entercept

sIOS-1

L'extrait de configuration suivant détaille les listes d'accès sur le routeur frontière du petit réseau qui contrôlent le trafic entrant et sortant du petit réseau.

Note : Les configurations du petit routeur ne montrent pas les configurations du VPN à accès distant ; cette fonctionnalité sera bientôt disponible sur le logiciel Cisco IOS.

```
! Configuration IOS élémentaire du IDS où syslog est utilisé pour le reporting
!
ip audit attack action alarm drop reset
ip audit notify log
ip audit name alarm1 info action alarm
ip audit name alarm1 attack action alarm drop
!
! Configuration cryptographique IPSec vers les sites distants distants du petit réseau
!
 crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.5
!
!
```

```
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
!
crypto map ent1 30 ipsec-isakmp
set peer 172.16.128.2
set transform-set remote1
match address 107
crypto map ent1 40 ipsec-isakmp
set peer 172.16.128.5
set transform-set remote1
match address 108
!
! Les listes d'accès ci-dessous permettent aussi bien le codage du trafic utilisateur
! que du trafic de gestion
!
access-list 107 permit ip 10.4.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 107 permit ip host 10.4.1.253 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 0.0.255.255 10.6.0.0 0.0.255.255
access-list 108 permit ip host 10.4.1.253 host 172.16.128.5
!
! Initialisations de l'interface interne du routeur. La traduction d'adresses de réseau, le IDS IOS et
! le pare-feu IOS sont activés.
!
interface FastEthernet0/0
description Inside Interface
ip address 10.4.1.1 255.255.255.0
ip access-group 109 in
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
!
! Autorise le protocole ICMP de l'intérieur du petit réseau vers l'Internet
!
access-list 109 permit icmp any any echo
!
! Autorise le serveur DNS interne à communiquer avec le serveur DNS public
!
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
!
! Autorise les utilisateurs internes à accéder aux services publics pour le trafic HTTP,
! SSL et FTP.

access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq 443
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq ftp
!
! Autorise le serveur de courrier interne à communiquer avec le serveur de courrier public
!
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
!
! Autorise l'accès Telnet à partir de la station d'administration vers le commutateur sCAT-1
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
!
! Refuse tous les autres accès au segment des services publics
!
access-list 109 deny ip any 10.4.2.0 0.0.0.255
!
! Autorise la synchronisation des horloges entre le routeur sIOS-1 et le commutateur sCAT-2
!
access-list 109 permit udp host 10.4.1.4 host 10.4.1.1 eq ntp
!
```

```
! Autorise l'accès SSH en provenance de la station d'administration vers le routeur sIOS-1
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.1.1 eq 22
!
! Autorise les connexions établies vers la station d'administration en retour sur le routeur sIOS-1
!
access-list 109 permit tcp host 10.4.1.253 eq tacacs host 10.4.1.1 established
!
! Nécessaire pour permettre l'accès TFTP en provenance de la station d'administration vers le routeur sIOS-1
!
access-list 109 permit udp host 10.4.1.253 gt 1023 host 10.4.1.1 gt 1023
!
! Bloque tous les autres accès vers l'interface intérieure sur le routeur sIOS-1 en provenance du
! réseau interne
!
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 10.4.1.1
!
! Bloque tous les autres accès vers l'interface extérieure sur le routeur sIOS-1 en provenance du
! réseau interne
!
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 172.16.132.2
!
! Autorise toutes les autres unités internes à accéder à l'Internet
!
access-list 109 permit ip 10.4.0.0 0.0.255.255 any
!
! Bloque et consigne dans un journal tout le reste du trafic
!
access-list 109 deny ip any any log
!
! Initialisations de l'interface de services publics du routeur. La traduction d'adresses de réseau, le IDS IOS et le pare-feu IOS sont activés.
!
interface FastEthernet0/1
description DMZ Interface
ip address 10.4.2.1 255.255.255.0
ip access-group 105 in
no ip redirects
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
!
! Autorise la synchronisation des horloges entre le routeur sIOS-1 et le commutateur sCAT-1
!
access-list 105 permit udp host 10.4.2.4 host 10.4.2.1 eq ntp
!
! Autorise les protocoles TACACS+, TFTP et syslog en provenance du commutateur sCAT-1 vers
! la station d'administration
!
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
!
! Autorise le trafic H-IDS du serveur de services public vers
! la station d'administration
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
!
! Autorise le serveur de courrier électronique public à envoyer du courrier au serveur de courrier interne
!
```

```
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
!
! Rejette toutes les autres connexions émanant du segment des services publics
! vers le réseau interne
!
access-list 105 deny ip any 10.4.0.0 0.0.255.255
!
! Autorise tout le trafic de courrier et de DNS en provenance du serveur de services
! public
!
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
!
! Interdit tout autre trafic et journalisation
!
access-list 105 deny ip any any log
!
! Initialisations de l'interface interne du routeur. La traduction d'adresses de réseau, le IDS IOS,
! le pare-feu IOS et IPSec sont activés.
!
interface Serial1/0
description Outside Interface
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
no ip redirects
ip nat outside
ip inspect smbranch_fw in
ip audit alarm1 in
crypto map ent1
!
! Autorise le trafic en provenance des sites distants vers le petit réseau. Nécessaire seulement
! lorsque le petit réseau joue le rôle de site centralpour les sites distants.
!
access-list 103 permit ip 10.5.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 103 permit ip 10.6.0.0 0.0.255.255 10.4.0.0 0.0.255.255
!
! Filtrage RFC 1918. Remarquez que le réseau 172.16.x.x n'a pas été inclus dans ce
! filtre car il joue le rôle du FAI dans le laboratoire.
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
!
! Autorise toute réponse par écho en provenance du réseau 172.16.132.0
! (adresses internes traduites).
!
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
!
! Autorise le trafic PMTUD (path MTU discovery )
!
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
!
! Autorise le trafic IPSec en provenance des sites distants à se raccorder sur le routeur sIOS-1
! Nécessaire seulement lorsque petit réseau joue le rôle de site central pour les
! sites distants.
!
access-list 103 permit esp host 172.16.128.2 host 172.16.132.2
access-list 103 permit udp host 172.16.128.2 host 172.16.132.2 eq isakmp
access-list 103 permit esp host 172.16.128.5 host 172.16.132.2
access-list 103 permit udp host 172.16.128.5 host 172.16.132.2 eq isakmp
!
!
```

```
! Autorise l'administration des sites distants. Nécessaire seulement
! lorsque le petit réseau joue le rôle de site centralpour les sites distants.
!
access-list 103 permit tcp host 172.16.128.2 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq syslog
access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq tftp
!
! Autorise l'accès au serveur de services publics (par l'intermédiaire
! du service de traduction des adresses de réseau du serveur) pour le trafic DNS,
! FTP, HTTP, SSL et de courrier
!
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
access-list 103 permit tcp any host 172.16.132.50 eq smtp
!
! Interdit tout autre trafic et journalisation
!
access-list 103 deny ip any any log

!
! La configuration suivante de traduction d'adresses de réseau crée un ensemble d'adresses publiques
! utilisées par les unités internes lorsqu'elles accèdent à l'Internet
!
ip nat pool small_pool 172.16.132.101 172.16.132.150 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool small_pool
!
! Traduction statique du serveur de services publics vers une adresse
! enregistrée accessible à partir de l'Internet
!
ip nat inside source static 10.4.2.50 172.16.132.50
!
route-map nat_internet permit 10
match ip address 104
!
! N'utilisez pas la traduction d'adresses de réseau pour les unités internes qui communiquent
! avec les autres unités 10.0.0.0 du réseau, ni pour le trafic de gestion. Utilisez la traduction d'adresses de réseau
! pour toutes les unités internes qui communiquent avec l'Internet.
!
access-list 104 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 deny ip host 10.4.1.253 host 172.16.128.2
access-list 104 deny ip host 10.4.1.253 host 172.16.128.5
access-list 104 permit ip 10.4.1.0 0.0.0.255 any
!
```

Modifications de configuration entre les designs de site distant et de site central

L'extrait de configuration suivant détaille les modifications nécessaires pour faire du petit réseau un site distant d'un réseau plus important à l'aide d'une connexion VPN redondante IPSec-sur -GRE.

```
!
! Paramètres des modalités de cryptage
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
```

```
crypto isakmp key 7Q!r$y$+xE address 172.16.226.28
crypto isakmp key 7Q!r$y$+xE address 172.16.226.27
!
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
mode transport
!
crypto map ent1 10 ipsec-isakmp
set peer 172.16.226.28
set transform-set 3dessha
match address 101
crypto map ent1 20 ipsec-isakmp
set peer 172.16.226.27
set transform-set 3dessha
match address 102
!
access-list 101 permit gre host 172.16.132.2 host 172.16.226.28
access-list 102 permit gre host 172.16.132.2 host 172.16.226.27
!
! Paramètres du tunnel GRE
!
interface Tunnel0
bandwidth 8
ip address 10.1.249.2 255.255.255.0
tunnel source 172.16.132.2
tunnel destination 172.16.226.27
crypto map ent1
!
interface Tunnel1
ip address 10.1.248.2 255.255.255.0
tunnel source 172.16.132.2
tunnel destination 172.16.226.28
crypto map ent1
!
! Application de mappe de codage vers l'interface physique
!
interface Serial1/0
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
crypto map ent1
!
! La liste d'accès 103 devra être modifiée aussi bien pour les connexions IPSec
! en provenance du siège social que pour le trafic GRE.
!
access-list 103 permit gre host 172.16.226.28 host 172.16.132.2
access-list 103 permit gre host 172.16.226.27 host 172.16.132.2
access-list 103 permit esp host 172.16.226.27 host 172.16.132.2
access-list 103 permit udp host 172.16.226.27 host 172.16.132.2 eq isakmp
 access-list 103 permit esp host 172.16.226.28 host 172.16.132.2
access-list 103 permit udp host 172.16.226.28 host 172.16.132.2 eq isakmp
!
! Notez que toutes les configurations relatives aux sites distants sont supprimées
!
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
access-list 103 permit tcp any host 172.16.132.50 eq smtp
```

```
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
access-list 103 deny ip any any log
```

Des modifications mineures doivent être également apportées aux autres listes d'accès, mais elles ne sont pas montrées ici.

sPIX-1

L'extrait de configuration suivant détaille les listes d'accès et la configuration cryptographique utilisées lorsque le pare-feu PIX sert d'unité de site central dans le petit réseau. Le pare-feu PIX dans cette configuration est capable de communiquer avec les sites distants et de terminer les connexions VPN IPSec commutées.

```
!
! Paramètres d'interface pour l'interface publique du pare-feu
!
ip address outside 172.16.144.3 255.255.255.0
access-group 103 in interface outside
!
! Autorise le trafic chiffré en provenance des sites distants et les utilisateurs à accès distant.
!
access-list 103 permit ip 10.5.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.6.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.4.3.0 255.255.255.0 10.4.0.0 255.255.0.0

! Filtrage RFC 1918. Remarquez que le réseau 172.16.x.x n'a pas été inclus dans ce
! filtre car il joue le rôle du FAI dans le laboratoire.
!
access-list 103 deny ip 10.0.0.0 255.0.0.0 any
access-list 103 deny ip 192.168.0.0 255.255.0.0 any
!
! Autorise l'accès au serveur de services publics (par l'intermédiaire
! du service de traduction des adresses de réseau du serveur) pour le trafic DNS,
! FTP, HTTP, SSL et de courrier
!
access-list 103 permit udp any host 172.16.144.50 eq domain
access-list 103 permit tcp any host 172.16.144.50 eq ftp
access-list 103 permit tcp any host 172.16.144.50 eq www
access-list 103 permit tcp any host 172.16.144.50 eq 443
access-list 103 permit tcp any host 172.16.144.50 eq smtp
!
! Autorise la réponse par écho générée par le réseau interne (par l'intermédiaire
! des adresses traduites) à revenir vers le pare-feu
!
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 echo-reply
!
! Autorise le trafic PMTUD (path MTU discovery ) à traverser le pare-feu.
!
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 unreachable
!
! Autorise le trafic d'administration syslog, TFTP et TACACS+ en provenance des sites distants.
!
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.2 host 172.16.144.51 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 172.16.144.51 eq tacacs

!
! Paramètres d'interface pour l'interface privée du pare-feu
```

```
!
ip address inside 10.4.1.1 255.255.255.0
access-group 109 in interface inside
!
! Autorise l'écho des unités internes
!
access-list 109 permit icmp any any echo
!
! Autorise le serveur DNS et le serveur de courrier internes à communiquer avec
! le serveur DNS et le serveur de courrier publics
!
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
!
! Autorise les unités internes à accéder au serveur de services publics pour les accès Internet, FTP
! et SSL
!
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq ftp
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq 443
!
! Autorise l'accès Telnet de la station d'administration vers le commutateur mCAT-1
!
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
!
! Bloque tous les autres accès au segment des services publics
!
access-list 109 deny ip any 10.4.2.0 255.255.255.0
!
! Autorise l'accès à l'Internet des unités internes
!
access-list 109 permit ip 10.4.0.0 255.255.0.0 any
!
!
! Paramètres d'interface pour l'interface de services publics (DMZ) du pare-feu
!
ip address pss 10.4.2.1 255.255.255.0
access-group 105 in interface pss
!
! Autorise les réponses par écho en provenance du réseau interne à repasser par le pare-feu
!
access-list 105 permit icmp 10.4.2.0 255.255.255.0 10.4.1.0 255.255.255.0 echo-reply
!
! Autorise les protocoles TACACS+, TFTP et syslog en provenance du commutateur sCAT-1 vers
! le serveur d'administration
!
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
!
! Autorise le trafic H-IDS du serveur de services public vers le
! serveur d'administration
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
!
! Autorise le serveur de courrier public à communiquer avec le serveur de courrier interne
!
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
!
! Bloque tous les autres accès en provenance de ce segment vers le réseau interne
!
```

```
access-list 105 deny ip any 10.4.0.0 255.255.0.0
!
! Autorise l'accès à l'Internet du serveur de services publics pour le
! courrier et le serveur DNS
!
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
!
! Paramètres IDS
!
ip audit name full info action alarm
ip audit name fullb attack action alarm drop
ip audit interface outside full
ip audit interface outside fullb
ip audit interface inside full
ip audit interface inside fullb
ip audit interface pss full
ip audit interface pss fullb
!
! La configuration de traduction des adresses de réseau suivante crée un ensemble d'adresses publiques qui
! sont utilisées par des unités internes lorsqu'elles accèdent à l'Internet
!
global (outside) 1 172.16.144.201-172.16.144.220
!
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (pss) 0 access-list nonat
!
! Traduction statique du serveur de services publics vers une adresse enregistrée
! accessible depuis l'Internet
!
static (pss,outside) 172.16.144.50 10.4.2.50 netmask 255.255.255.255 0 0
!
static (inside,pss) 10.4.1.253 10.4.1.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.4.1.201 10.4.1.201 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.144.51 10.4.1.253 netmask 255.255.255.255 0 0
!
! La liste d'accès nonat définit les adresses qui seront traduites
!
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.2.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.2.0 255.255.255.0
!
! Les paramètres de codage suivants sont utilisés lorsque le pare-feu met fin aux connexions VPN en provenance des sites distants
!
no sysopt route dnat
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
crypto dynamic-map vpnuser 20 set transform-set remote1
crypto map ent1 30 ipsec-isakmp
crypto map ent1 30 match address 107
crypto map ent1 30 set peer 172.16.128.2
crypto map ent1 30 set transform-set remote1
crypto map ent1 40 ipsec-isakmp
crypto map ent1 40 match address 108
crypto map ent1 40 set peer 172.16.128.5
crypto map ent1 40 set transform-set remote1
crypto map ent1 50 ipsec-isakmp dynamic vpnuser
```

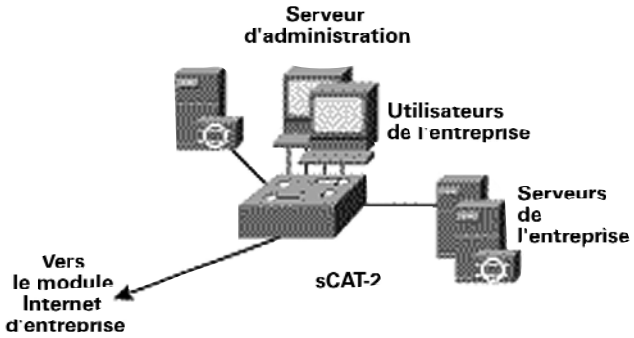
```
crypto map ent1 client configuration address initiate
crypto map ent1 client authentication vpnauth
crypto map ent1 interface outside
!
access-list 107 permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list 107 permit ip host 172.16.144.51 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list 108 permit ip host 172.16.144.51 host 172.16.128.5
!
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.28 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.27 netmask 255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
!
```

! Le bloc de configuration suivant configure le PIX pour terminer les utilisateurs VPN à
! accès distant

```
!
vpngroup VPN1 address-pool vpnpool
vpngroup VPN1 dns-server 10.4.1.201
vpngroup VPN1 default-domain safe-small.com
vpngroup VPN1 idle-time 1800
vpngroup VPN1 password Y0eS)3/i6y
ip local pool vpnpool 10.4.3.1-10.4.3.254
```

Module Campus

Figure 16 - Modèle détaillé du module Campus de petit réseau



Produits utilisés

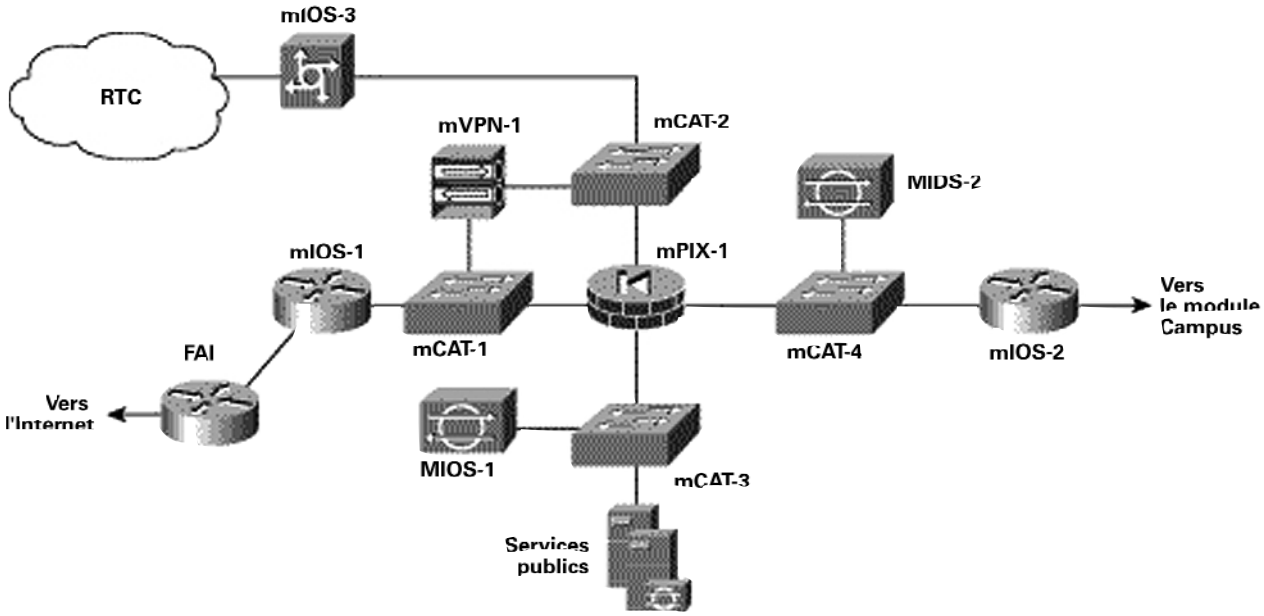
- Commutateur de couche 2 Cisco Catalyst (sCAT-2)
- H-IDS Entercept
- Serveur de contrôle d'accès sécurisé Cisco
- Cisco Secure Policy Manager Lite
- Utilitaire d'analyse syslog OpenSystems Private I
- Client SSH (Secure Shell Protocol) F-Secure

Configurations du réseau de taille moyenne

Vous trouverez ci-après quelques extraits de configuration du réseau de taille moyenne SAFE. Sauf mention contraire, il s'agit de configurations pour le réseau de taille moyenne jouant le rôle du site central.

Module Internet d'entreprise

Figure 17 - Modèle détaillé du module Internet d'entreprise d'un réseau de taille moyenne



Produits utilisés

- Commutateurs de couche 2 Cisco Catalyst (de mCAT-1 à mCAT-4)
- Routeurs Cisco IOS avec support de codage 3DES (mIOS-1 et mIOS-2)
- Routeur d'accès commuté Cisco IOS (mIOS-3)
- Concentrateur VPN Cisco série 3000 (mVPN-1)
- Pare-feu sécurisé Cisco PIX(mPIX-1)
- Capteurs SDI sécurisés Cisco (mSDI-1 et mSDI-2)
- SDI-H Entercept
- Filtrage de courrier électronique Baltimore MIMESweeper

mIOS-1

L'extrait de configuration suivant détaille les listes d'accès sur le routeur frontière du réseau de taille moyenne, mIOS-1, qui contrôlent le trafic entrant sur le réseau de taille moyenne en provenance du fournisseur d'accès Internet (FAI).

```
interface FastEthernet0/0
ip address 172.16.240.2 255.255.255.0
ip access-group 112 in
no ip redirects

no cdp enable
!
interface Serial1/0
ip address 172.16.131.2 255.255.255.0
ip access-group 150 in
dsu bandwidth 44210
framing c-bit
```

```
no cdp enable
!
! Filtrage RFC 1918. Remarquez que le réseau 172.16.0.0 a été utilisé pour simuler le FAI du réseau SAFE
! et n'a donc pas été inclus dans le filtrage RFC 1918.
!
access-list 150 deny ip 10.0.0.0 0.255.255.255 any
access-list 150 deny ip 192.168.0.0 0.0.255.255 any
!
!
! Empêche toute unité extérieure d'usurper une adresse semblant provenir de
! l'intérieur du réseau de taille moyenne.
!
access-list 150 deny ip 172.16.240.0 0.0.0.255 any
!
! Autorise le trafic IKE et ESP accepté à atteindre les unités VPN.
!
access-list 150 permit esp any host 172.16.240.3
access-list 150 permit udp any host 172.16.240.3 eq isakmp
access-list 150 permit esp host 172.16.128.2 host 172.16.240.1
access-list 150 permit udp host 172.16.128.2 host 172.16.240.1 eq isakmp
access-list 150 permit esp host 172.16.128.5 host 172.16.240.1
access-list 150 permit udp host 172.16.128.5 host 172.16.240.1 eq isakmp
!
!
! Interdit toute autre conversation avec mIOS-1, mVPN-1, mPIX-1 et mCAT-1.
!
access-list 150 deny ip any host 172.16.240.3
access-list 150 deny ip any host 172.16.240.4
access-list 150 deny ip any host 172.16.240.2
access-list 150 deny ip any host 172.16.240.1
!
!
! Permet toutes les autres connexions vers le sous-réseau 172.16.240, puisque les unités utilisateur internes
 ! traduisent les adresses en 172.16.240.0 dans le pare-feu lorsqu'elles accèdent à l'Internet.
!
access-list 150 permit ip any 172.16.240.0 0.0.0.255
!
!
! Bloque et enregistre dans le fichier de consignation toutes les autres tentatives d'accès.
!
access-list 150 deny ip any any log
!
!
```

L'extrait de configuration suivant détaille les listes d'accès qui contrôlent le trafic en provenance du réseau de taille moyenne vers le FAI sur le routeur frontière.

```
! Autorise les sessions TCP originaires du routeur vers les stations d'administration
! (TACACS+, etc.). Les stations d'administration 172.16.240.151 et 172.16.240.152 sont les
! adresses traduites (traduction des adresses de réseau) sur le pare-feu.
!
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 established
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 established
!
!
! Autorise les connexions SSH en provenance des stations d'administration vers le routeur.
!
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 eq 22
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 eq 22
!
!
```

```
! Nécessaire pour permettre au TFTP de revenir de la station d'administration vers le routeur.
!
access-list 112 permit udp host 172.16.240.151 host 172.16.240.2 gt 1024
!
!
! Autorise les autres unités du sous-réseau 172.16.240 à synchroniser les horloges sur cette unité.
!
access-list 112 permit udp 172.16.240.0 0.0.0.255 host 172.16.240.2 eq ntp
!
!
! Autorise les unités internes à lancer des requêtes ping sur l'Internet.
!
access-list 112 permit icmp 172.16.240.0 0.0.0.255 any
!
!
! Bloque toutes les autres tentatives d'accès à ce routeur et les consigne dans un journal.
!
access-list 112 deny ip any host 172.16.240.2 log
!
!
! Autorise tous les accès vers l'Internet à partir des stations possédant les adresses 172.16.240.0.
!
access-list 112 permit ip 172.16.240.0 0.0.0.255 any
!
!
```

mPIX-1

L'extrait de configuration du pare-feu suivant détaille les niveaux de sécurité des interfaces du pare-feu PIX, mPIX-1, ainsi que l'adressage de chaque interface.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pss security10
nameif ethernet3 vpn security15
!
ip address outside 172.16.240.1 255.255.255.0
ip address inside 10.3.4.1 255.255.255.0
ip address pss 10.3.6.1 255.255.255.0
ip address vpn 10.3.5.1 255.255.255.0
```

L'extrait de configuration du pare-feu suivant détaille la configuration de la traduction des adresses de réseau sur le pare-feu PIX.

```
! En association avec la liste d'accès nonat, la configuration suivante ne permet pas la
! traduction des adresses de réseau pour les sessions entre les unités internes (réseau 10.x.x.x vers réseau 10.x.x.x), mais
! permet cette traduction pour les sessions entre les unités internes ou distantes et l'Internet.
global (outside) 100 172.16.240.101-172.16.240.150 netmask 255.255.255.0
global (outside) 200 172.16.240.201-172.16.240.250 netmask 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 100 10.0.0.0 255.0.0.0 0 0
nat (pss) 0 access-list nonat
nat (vpn) 200 10.3.7.0 255.255.255.0 0 0
static (inside,vpn) 10.3.0.0 10.3.0.0 netmask 255.255.0.0 0 0
static (inside,pss) 10.3.8.253 10.3.8.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.3.8.254 10.3.8.254 netmask 255.255.255.255 0 0
!
!
! Traduit les adresses non-enregistrées des serveurs de services publics en adresse enregistrée
! et accessible par l'Internet.
!
static (pss,outside) 172.16.240.50 10.3.6.50 netmask 255.255.255.255 0 0
!
!
```

```
! Traduit les adresses non-enregistrées des stations d'administration en adresses enregistrées
! afin que les unités administrées en dehors du pare-feu puissent initier des sessions
! vers les serveurs d'administration.
!
static (inside,outside) 172.16.240.151 10.3.8.254 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.240.152 10.3.8.253 netmask 255.255.255.255 0 0
!
!
!
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.0.0.0 255.0.0.0 any
```

L'extrait de configuration suivant détaille le contrôle d'accès installé sur le pare-feu PIX. Le nom de la liste d'accès rappelle l'emplacement de la liste de contrôle d'accès (ACL) entrante.

La liste d'accès "out" est placée en direction entrante sur l'interface extérieure (publique) du pare-feu.

```
! Autorise le trafic chiffré en provenance des sites distants.
!
access-list out permit ip 10.5.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list out permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
!
! Filtrage RFC 1918. Remarquez que le réseau 172.16.0.0 a été utilisé pour simuler le FAI du réseau SAFE
! et n'a donc pas été inclus dans le filtrage RFC 1918.
!
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
!
! Autorise les stations externes à accéder au serveur de services publics pour les protocoles HTTP, SSL, FTP
! SMTP et DNS.
!
access-list out permit tcp any host 172.16.240.50 eq www
access-list out permit tcp any host 172.16.240.50 eq 443
access-list out permit tcp any host 172.16.240.50 eq ftp
access-list out permit tcp any host 172.16.240.50 eq smtp
access-list out permit udp any host 172.16.240.50 eq domain
!
! Autorise la réponse par écho générée par le réseau interne (par l'intermédiaire
! des adresses traduites) à revenir vers le pare-feu
!
access-list out permit icmp any 172.16.240.0 255.255.255.0 echo-reply
!
! Autorise le trafic PMTUD (path MTU discovery ) à traverser le pare-feu.
!
access-list out permit icmp any 172.16.240.0 255.255.255.0 unreachable
!
! Autorise le trafic de gestion syslog, TFTP et TACACS+ en provenance des sites distants.
!
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.5 host 172.16.240.152 eq tacacs
!
! Autorise syslog, TFTP et TACACS+ en provenance du routeur mIOS-1
! et du commutateur mCAT-1 vers les stations d'administration.
!
```

```
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.240.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.240.4 host 172.16.240.152 eq tacacs
!
```

La liste d'accès “in” est placée en position entrante sur l'interface intérieure (privée) du pare-feu.

```
! Autorise l'écho en provenance du réseau intérieur
!
access-list in permit icmp any any echo
!
!
! Autorise le serveur DNS interne à émettre des requêtes de traduction de noms
! auprès du serveur DNS externe.
!
access-list in permit udp host 10.3.2.50 host 10.3.6.50 eq domain
!
!
! Autorise l'accès Internet, SSL et FTP des utilisateurs d'entreprise internes vers le serveur externe de
! services publics.
!
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq 443
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq ftp
!
!
! Autorise le transfert de courrier du serveur de courrier externe vers le
! serveur de courrier interne.
!
access-list in permit tcp host 10.3.2.50 host 10.3.6.50 eq smtp
!
!
Autorise l'accès Telnet à partir des stations d'administration vers le commutateur mCAT-2 (qui ne supporte pas SSH) sur le segment des services publics.
!
access-list in permit tcp host 10.3.8.253 host 10.3.6.4 eq telnet
access-list in permit tcp host 10.3.8.254 host 10.3.6.4 eq telnet
!
!
! Refuse tout autre accès au segment des services en provenance du réseau interne.
!
access-list in deny ip any 10.3.6.0 255.255.255.0
!
!
! Autorise l'accès à l'Internet à tous les utilisateurs internes.
!
access-list in permit ip 10.0.0.0 255.0.0.0 any
!
```

La liste d'accès “pss” est placée en position entrante sur l'interface du segment des services publics du pare-feu.

```
! Autorise syslog, TFTP et TACACS+ en provenance du commutateur mCAT-2
! vers les stations d'administration.
!
```

```
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq syslog
access-list pss permit udp host 10.3.6.4 host 10.3.8.253 eq syslog
access-list pss permit tcp host 10.3.6.4 host 10.3.8.253 eq tacacs
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq tftp
!
!
! Autorise le commutateur mCAT-2 à synchroniser son horloge avec le routeur interne
! mIOS-2.
!
access-list pss permit udp host 10.3.6.4 host 10.3.4.4 eq ntp
!
!
! Autorise le trafic H-IDS en provenance de la station de services publics vers le
! réseau hôte d'administration.
!
access-list pss permit tcp host 10.3.6.50 host 10.3.8.253 eq 5000
!

! Autorise le passage du courrier en provenance de la station de services publics (serveur de courrier externe)
! vers la station d'entreprise des services intranet (serveur de courrier interne).
!
access-list pss permit tcp host 10.3.6.50 host 10.3.2.50 eq smtp
!
!
! Refuse tout autre trafic destiné aux adresses du réseau interne.
!
access-list pss deny ip any 10.3.0.0 255.255.0.0
!
.
!
! Autorise le courrier et le DNS générés par la station de services publics en direction de l'Internet.
!
access-list pss permit tcp host 10.3.6.50 any eq smtp
access-list pss permit udp host 10.3.6.50 any eq domain
!
```

La liste d'accès “vpn” est placée en position entrante sur l'interface du segment VPN à accès distant du pare-feu. Les utilisateurs du VPN distant reçoivent des adresses dans le sous-réseau 10.3.7.0 par l'intermédiaire d'un ensemble d'adresses défini dans le serveur de contrôle d'accès. Les utilisateurs distants qui se connectent par le réseau téléphonique reçoivent des adresses dans le sous-réseau 10.3.8.0.

```
! Autorise l'accès Internet, SSL et FTP aux utilisateurs distants mais vers le serveur de services publics seulement.
!
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn deny ip 10.3.7.0 255.255.255.0 10.3.6.0 255.255.255.0
access-list vpn deny ip 10.3.8.0 255.255.255.0 10.3.6.0 255.255.255.0
!
!
! Autorise l'accès au reste du réseau interne et à l'Internet aux utilisateurs distants.
!
access-list vpn permit ip 10.3.7.0 255.255.255.0 any
access-list vpn permit ip 10.3.8.0 255.255.255.0 any
!
!
! Autorise le trafic de gestion syslog, TFTP et TACACS+ en provenance du concentrateur VPN,
! mVPN-1, vers les stations d'administration.
!
```

```
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.5 host 10.3.8.253 eq tacacs
!
!
! Autorise le concentrateur VPN à synchroniser son horloge avec le
! routeur interne, mIOS-2.
!
access-list vpn permit udp host 10.3.5.5 host 10.3.4.4 eq ntp
!
!
! Autorise les données d'authentification RADIUS en provenance du concentrateur VPN à passer jusqu'à
! la station d'administration.
!
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq 1645
!
!
! Autorise le trafic de gestion syslog, TFTP et TACACS+ en provenance du routeur
! d'accès commuté, mIOS-3, vers les stations d'administration.
!
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.2 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.2 host 10.3.8.253 eq tacacs
!
!
! Autorise le routeur d'accès commuté, mIOS-3, à synchroniser son horloge avec le
! routeur interne, mIOS-2.
!
access-list vpn permit udp host 10.3.5.2 host 10.3.4.4 eq ntp
!
!
! Autorise le trafic d'administration syslog, TFTP et TACACS+ en provenance du commutateur mCAT-3
! vers les stations d'administration.
!
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.4 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.4 host 10.3.8.253 eq tacacs
!
!
! Autorise le commutateur mCAT-3 à synchroniser son horloge avec le routeur interne
! mIOS-2.
!
access-list vpn permit udp host 10.3.5.4 host 10.3.4.4 eq ntp
!
!
```

Remarques sur les VPN

Les configurations suivantes ont été ajoutées pour permettre les VPN IPSec de site à site vers les sites distants.

```
! Assure que le trafic utilisateur et le trafic de gestion est chiffré vers la première unité distante.
!
access-list remote1 permit ip 10.3.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.240.151 host 172.16.128.2
access-list remote1 permit ip host 172.16.240.152 host 172.16.128.2
!
!
! Assure que le trafic utilisateur et le trafic de gestion est chiffré vers la deuxième unité distante.
!
```

```
access-list remote2 permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list remote2 permit ip host 172.16.240.151 host 172.16.128.5
access-list remote2 permit ip host 172.16.240.152 host 172.16.128.5
!
!
```

! Définit la mappe de codage et l'applique à l'interface externe.

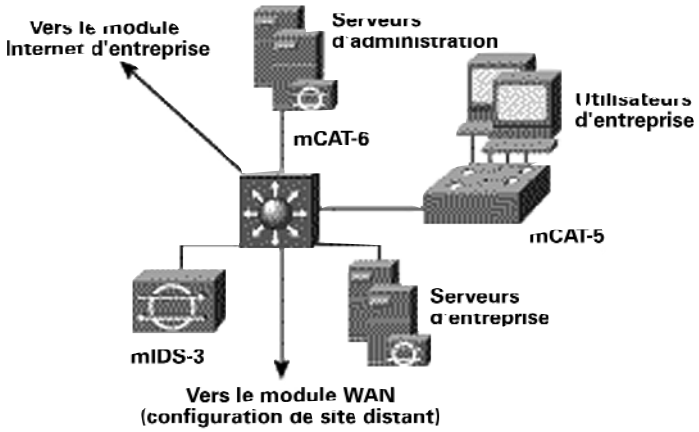
```
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.128.2
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 20 ipsec-isakmp
crypto map remote1 20 match address remote2
crypto map remote1 20 set peer 172.16.128.5
crypto map remote1 20 set transform-set 3dessha
crypto map remote1 interface outside
!
!
```

! Définit l'utilisation d'IKE à l'aide des clés préalablement partagées.

```
!
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
```

Module Campus

Figure 18 - Modèle détaillé du module Campus du réseau de taille moyenne



Produits utilisés
• Commutateur de couche 3 Cisco Catalyst (mCAT-6)
• Commutateurs de couche 2 Cisco Catalyst (mCAT-5)
• Capteurs SDI sécurisés Cisco (mSDI-3)
• SDI-H Entercept
• Cisco Secure Policy Manager
• Serveur de contrôle d'accès sécurisé Cisco
• CiscoWorks 2000
• Utilitaire d'analyse syslog OpenSystems Private I
• Client SSH F-Secure
• Système RSA MPS SecureID

L'extrait de configuration suivant détaille les listes d'accès installées sur le commutateur de couche 3 Cisco Catalyst qui contrôle l'accès au VLAN (réseau local virtuel) de la station d'administration, ainsi qu'au filtrage RFC 2827 sur le VPN du serveur public et sur le VPN du commutateur d'immeuble. Le réseau local virtuel 10 définit le sous-réseau d'utilisateur d'entreprise. Le réseau local virtuel 11 définit le sous-réseau d'entreprise du serveur intranet. Les VLAN 12 et 13 se connectent respectivement à l'Internet d'entreprise et au module WAN. Enfin, le réseau local virtuel 99 définit le sous-réseau de la station d'administration.

mCAT-6

```
! Réseau local virtuel de l'utilisateur d'entreprise.
!
interface Vlan10
ip address 10.3.1.1 255.255.255.0
ip access-group 101 in
no ip redirects
no cdp enable
!
!
! Réseau local virtuel du serveur intranet d'entreprise.
!
interface Vlan11
ip address 10.3.2.1 255.255.255.0
ip access-group 102 in
no ip redirects
no cdp enable
!
!
interface Vlan12
ip address 10.3.3.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 134E031F4158140119
no cdp enable
!
interface Vlan13
ip address 10.3.9.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
no cdp enable
!
! Réseau local virtuel de la station d'administration.
!
interface Vlan99
ip address 10.3.8.1 255.255.255.0
ip access-group 103 out
no ip redirects
no cdp enable
!
!
```

```
! Filtrage RFC 2827 sur le réseau local virtuel de l'utilisateur d'entreprise.
!
access-list 101 permit ip 10.3.1.0 0.0.0.255 any
access-list 101 deny ip any any
!
!
! Filtrage RFC 2827 sur le réseau local virtuel de serveur intranet d'entreprise.
!
access-list 102 permit ip 10.3.2.0 0.0.0.255 any
access-list 102 deny ip any any log
!
!
Exemple de filtrage pour l'accès au sous-réseau d'administration (incomplet).
!
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.253
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.254
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.253
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.254
access-list 103 permit tcp host 10.3.2.50 host 10.3.8.253 eq 5000
access-list 103 permit udp host 10.3.1.4 host 10.3.8.253 eq syslog
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 10.3.1.4 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq tftp
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 gt 1023
access-list 103 permit udp host 10.3.1.4 eq snmp host 10.3.8.254
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.253 established
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.254 established
access-list 103 deny ip any any
!
```

Site distant ou site central

Les remarques suivantes ont été ajoutées à la liste d'accès du commutateur de cœur de réseau afin de permettre le trafic de configuration et de gestion de sécurité à partir des unités administrées à distance vers les stations d'administration, lorsque le réseau de taille moyenne est configuré en tant que site central.

```
access-list 103 permit udp host 172.16.128.5 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.5 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.254 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.254 established
access-list 103 permit udp host 172.16.128.2 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.2 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.254 established
```

mCAT-5

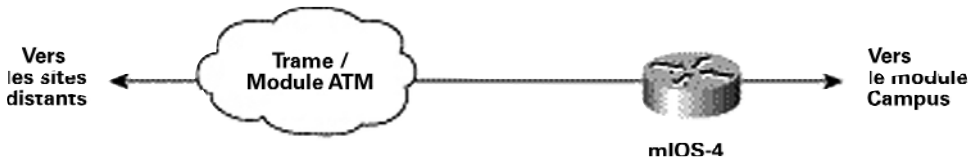
L'extrait de configuration suivant présente certains paramétrages du réseau local virtuel sur le commutateur de couche 2 de ce module. Notez que les ports inutilisés ont été désactivés. Les private VLAN sont utilisés sur tous les ports à l'exception de la liaison montante vers le commutateur de cœur de réseau.

```
! Ports du poste de travail utilisateur.
!
```

```
interface FastEthernet0/1
port protected
switchport access vlan 99
no cdp enable
!
interface FastEthernet0/2
port protected
switchport access vlan 99
no cdp enable
!
!
! Ports inutilisés
!
interface FastEthernet0/3
port protected
shutdown
no cdp enable
!
interface FastEthernet0/4
port protected
shutdown
no cdp enable
!
!
! Liaison montante vers le commutateur de cœur de réseau mCAT-1
!
interface GigabitEthernet0/1
switchport access vlan 99
no cdp enable
!
!
!
! Interface d'administration vers le commutateur.
!
interface VLAN99
ip address 10.3.1.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
!
```

Module WAN

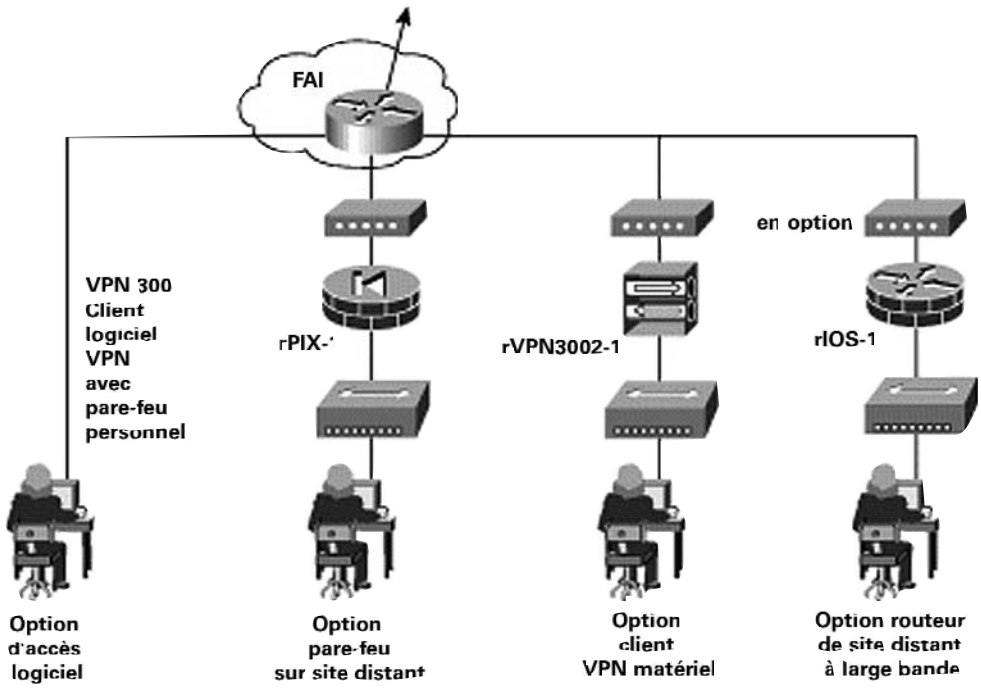
Figure 19 - Modèle détaillé de module WAN



Produits utilisés

• Routeur Cisco IOS (mIOS-4)

Figure 20 - Modèle détaillé des designs d'utilisateur distant



Produits utilisés
- Routeur Cisco IOS avec support de codage 3DES (rIOS-1)
- Client matériel VPN Cisco 3002 (rVPN3002-1)
- Pare-feu sécurisé Cisco PIX (rPIX-1)
- Client logiciel VPN Cisco 3000
- Microconcentrateur Cisco (ou intégré à l'unité de couche 3)
- Pare-feu personnel Zone Alarm Pro

Les extraits suivants montrent la configuration de certains designs SAFE pour utilisateur distant.

rIOS-1 (Option routeur de site distant)
Les extraits suivants montrent la configuration des tunnels IPSec en retour vers les sièges sociaux d'entreprise.

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.240.1
!
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
!
crypto map remote1 10 ipsec-isakmp
set peer 172.16.240.1
set transform-set 3dessha
match address 101
!
!
```

```
! Les premières lignes de la liste d'accès suivante précisent que tout le trafic
! en provenance du réseau 10.5.0.0 vers les réseaux 10.3.0.0 doit être chiffré.
!
! Les deux dernières lignes de la liste d'accès autorisent le codage de tout le trafic de configuration
! et de gestion de sécurité en provenance du routeur de site distant vers les
! stations d'administration du siège social.
!
access-list 101 permit ip 10.5.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 101 permit ip host 172.16.128.2 host 172.16.240.151
access-list 101 permit ip host 172.16.128.2 host 172.16.240.152
!
!
```

Les lignes suivantes montrent le contrôle d'accès sur la face privée (FastEthernet 0/0) et la face publique (FastEthernet 0/1) du routeur, ainsi que l'application du pare-feu Cisco IOS sur les interfaces.

```
interface FastEthernet0/0
ip address 10.5.1.2 255.255.255.0
ip access-group 105 in
ip nat inside
ip inspect remote_fw in
!
interface FastEthernet0/1
ip address 172.16.128.2 255.255.255.0
ip access-group 102 in
ip nat outside
crypto map remote1
!
! Le trafic IKE et ESP doit être autorisé à partir de l'homologue IPSec du siège social. Tout le
! trafic du réseau 10.5.0.0 vers les réseaux 10.3.0.0 doit également être
! autorisé. Enfin, le trafic de provenance des stations d'administration est autorisé.
!
access-list 102 permit ip 10.3.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 permit icmp any host 172.16.128.2 echo-reply
access-list 102 permit icmp any host 172.16.128.2 unreachable
access-list 102 permit esp host 172.16.240.1 host 172.16.128.2
access-list 102 permit udp host 172.16.240.1 host 172.16.128.2 eq isakmp
access-list 102 permit tcp host 172.16.240.151 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 eq tacacs host 172.16.128.2
access-list 102 permit udp host 172.16.240.151 host 172.16.128.2 gt 1023
access-list 102 deny ip any any log
!
!
! Le filtrage RFC 2827 n'autorise que les adresses 10.5.0.0 à accéder à la fois au siège
! social de l'entreprise et à l'Internet.
!
access-list 105 permit ip 10.5.0.0 0.0.255.255 any
access-list 105 deny ip any any log
!
```

Les lignes suivantes montrent la configuration de traduction d'adresses de réseau à origine multiple et à destination unique sur le routeur. Toutes les unités du site distant qui ont accès à l'Internet utiliseront l'adresse publique du routeur.

```
ip nat pool remote_pool 172.16.128.2 172.16.128.2 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool remote_pool
!
route-map nat_internet permit 10
match ip address 104
!
```

```
access-list 104 deny ip 10.5.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 permit ip 10.5.0.0 0.0.255.255 any
!
```

rPIX-1 (Option pare-feu sur site distant)

Les lignes suivantes présentent la configuration des tunnels IPSec en retour sur le siège social.

```
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.240.1
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 interface outside
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.240.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
! La première ligne de la liste d'accès suivante précise que tout le trafic
! en provenance du réseau 10.6.0.0 vers les réseaux 10.3.0.0 doit être chiffré.
!
! Les deux dernières lignes de la liste d'accès autorisent le codage de tout le trafic de configuration
! et de gestion de sécurité en provenance du routeur de site distant vers les
! stations d'administration du siège social.
!
access-list remote1 permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.151
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.152
!
```

Les lignes suivantes montrent l'adressage et le contrôle d'accès sur la face privée (intérieure) et sur la face publique (extérieure) du pare-feu.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!
ip address outside 172.16.128.5 255.255.255.0
ip address inside 10.6.1.1 255.255.255.0
!
access-group out in interface outside
access-group in in interface inside
!
! Le filtrage RFC 2827 n'autorise que les adresses 10.6.0.0 à accéder à la fois au siège
! social de l'entreprise et à l'Internet.
!
access-list in permit ip 10.6.0.0 255.255.0.0 any
!
Autorise le trafic chiffré en provenance du siège social.
!
access-list out permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
!
! Filtrage RFC 1918. Remarquez que le réseau 172.16.x.x n'a pas été inclus dans le filtre
! car il sert à simuler le FAI dans le laboratoire
!
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
!
```

```
Autorise les réponses par écho et le trafic PMTUD (path MTU discovery ).
!
access-list out permit icmp any host 172.16.128.5 echo-reply
access-list out permit icmp any host 172.16.128.5 unreachable
!
! Autorise le trafic ESP et IKE en provenance de l'homologue du siège social.
!
access-list out permit esp host 172.16.240.1 host 172.16.128.5
access-list out permit udp host 172.16.240.1 host 172.16.128.5 eq isakmp
```

Les lignes suivantes montrent la configuration de traduction d'adresses de réseau à origine multiple et à destination unique sur le pare-feu. Toutes les unités du site distant qui ont accès à l'Internet utiliseront l'adresse publique du pare-feu.

```
global (outside) 100 interface
nat (inside) 0 access-list nonat
nat (inside) 100 10.6.1.0 255.255.255.0 0 0
!
! La liste d'accès empêche que le trafic destiné au site d'entreprise puisse utiliser.
! la traduction d'adresses
!
access-list nonat permit ip 10.6.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.6.0.0 255.255.0.0 any
!
```

Annexe B : Introduction à la sécurité réseau

La sécurité réseau : une nécessité

L'Internet modifie en permanence la manière dont nous vivons et dont nous faisons du commerce. Ces changements se manifestent de la manière que nous connaissons actuellement (commerce électronique, accès à l'information en temps réel, apprentissage électronique, options de communication élargies, etc.), et d'autres manières qu'il nous reste encore à connaître. Imaginez ce jour où votre entreprise pourra passer tous ses appels téléphoniques par l'Internet, gratuitement. Ou alors, d'un point de vue plus personnel, que diriez-vous de pouvoir vous connecter au site Web de la crèche où votre enfant est gardé pour voir comment il se porte pendant la journée. En tant que société, nous commençons à peine à libérer le potentiel de l'Internet. Mais la croissance sans pareil que connaît le réseau mondial s'accompagne d'une mise en évidence sans précédent des données personnelles, des ressources vitales de l'entreprise, des secrets d'Etats, et bien d'autres encore. Chaque jour, les pirates représentent une menace croissante pour ces entités au travers de leurs différents types d'attaques. Ces attaques, décrites dans la section suivante, sont devenues à la fois plus prolifiques et plus faciles à mettre en œuvre. Deux raisons principales permettent d'expliquer ce phénomène.

En premier lieu vient l'omniprésence d'Internet. Avec les millions d'équipements actuellement connectés à l'Internet – et des millions d'autres à venir – les pirates auront toujours davantage accès aux équipements vulnérables. L'omniprésence d'Internet a également permis aux pirates de partager leurs connaissances à l'échelle mondiale. Une simple recherche Internet sur les mots clé “hack,” “crack” ou “phreak” fait remonter des milliers de sites, dont beaucoup contiennent des programmes rédigés dans l'intention de nuire ou les moyens d'utiliser ces programmes.

Vient ensuite la généralisation des systèmes d'exploitation et des environnements de développements faciles à utiliser. Ce facteur a réduit le niveau général d'ingéniosité et de connaissances dont ont besoin les pirates. Un pirate véritablement "doué" peut développer des applications faciles à utiliser qui seront distribuées au plus grand nombre. Plusieurs utilitaires pirates accessibles dans le domaine public ne demandent pratiquement qu'une adresse IP ou qu'un nom de station et un clic de souris pour lancer une attaque.

Terminologie des attaques de réseau

Les attaques réseau peuvent être aussi variées que les systèmes qu'elles tentent de pénétrer. Certaines attaques sont particulièrement complexes, tandis que d'autres sont exécutées par un opérateur bien intentionné et à son insu. Pour évaluer les différents types d'attaques, il est important de comprendre certaines des limitations inhérentes au protocole TCP/IP. Lorsqu'Internet a été créé, il reliait différents organismes gouvernementaux et universités les unes aux autres dans le seul but de faciliter l'apprentissage et la recherche. Les premiers architectes d'Internet n'ont jamais imaginé le type de croissance qu'Internet a atteint aujourd'hui. En conséquence, dans les premiers temps de l'Internet Protocol (IP), la sécurité ne faisait pas partie intégrante des spécifications. Pour cette raison, la plupart des mises en œuvre IP sont par nature exposées au danger. Ce n'est qu'après de nombreuses années et des milliers de RFC (Requests for Comments) que nous commençons à disposer des outils nécessaires pour déployer le protocole IP de manière sécurisée. Comme la sécurité n'a pas été prévue dès le départ dans le développement de l'IP, il est important de renforcer sa mise en œuvre par des pratiques, des services et des produits de sécurité réseau afin de limiter les risques inhérents. Les paragraphes suivants présentent les types d'attaques que sont susceptibles de subir les réseaux IP et la manière dont on peut en limiter les risques.

Les sniffers de paquets

Un sniffer de paquets est une application logicielle qui utilise une carte réseau en mode espion (un mode dans lequel la carte réseau envoie tous les paquets reçus sur la ligne physique du réseau vers une application chargée de leur traitement) afin de capturer tous les paquets de réseau qui sont envoyés vers un même domaine particulier. Les sniffers sont actuellement utilisés de manière légitime dans les réseaux pour dépister les pannes et analyser le trafic. Toutefois, comme certaines applications de réseau (Telnet, File Transfer Protocol [FTP], Simple Message Transfer Protocol [SMTP], Post Office Protocol [POP3], etc.) envoient leurs données en clair, c'est à dire sans codage, un sniffer de paquets peut fournir des informations utiles et souvent confidentielles, comme des noms d'utilisateur et des mots de passe.

L'un des inconvénients majeurs de l'acquisition de noms d'utilisateur et de mots de passe est que les utilisateurs réutilisent souvent leurs noms de connexions et leurs mots de passe pour accéder à des applications et des systèmes différents. En fait, de nombreux utilisateurs utilisent un unique mot de passe pour accéder à tous leurs comptes et applications. Si une application est exécutée en mode client-serveur et que les informations d'authentification sont envoyées sur le réseau en clair, il est alors probable que les mêmes informations d'authentification pourront être utilisées pour accéder à d'autres ressources de l'entreprise ou d'ailleurs. Comme les pirates connaissent et exploitent les failles humaines (des méthodes d'attaque connues de manière générique sous l'appellation d'attaques social engineering), comme l'utilisation d'un unique mot de passe pour des comptes différents, ils parviennent souvent à s'emparer d'informations confidentielles. Dans le pire des cas, un pirate pourra accéder à un compte utilisateur au niveau système dont il se servira pour créer un nouveau compte, lequel lui offrira une entrée dérobée qu'il utilisera à sa guise pour pénétrer dans le réseau et s'emparer de ses ressources.

Les risques liés aux sniffers de paquets peuvent être limités de plusieurs manières :

- *L'authentification* — L'authentification est la première option de défense contre les sniffers de paquets. Sans entrer dans les détails, l'authentification peut être définie comme une méthode d'authentification des utilisateurs qu'il est difficile de contourner. Le mot de passe à usage unique (OTP) est un exemple classique d'authentification. L'OTP est une sorte d'authentification à deux facteurs, autrement dit l'emploi de quelque chose que vous possédez, associé à quelque chose que vous savez. Les distributeurs à cartes bancaires utilisent une authentification à deux facteurs. Pour effectuer une transaction, le client doit posséder à la fois une carte d'authentification (carte bancaire) et un numéro personnel d'authentification. L'OTP fonctionne de la même manière : vous devez posséder un numéro personnel d'authentification ainsi que votre carte d'authentification pour vous identifier auprès d'une unité ou d'une application logicielle. Cette carte d'authentification est une unité matérielle ou logicielle qui génère à intervalles prédéfinis (généralement toutes les 60 secondes) des mots de passe chaque fois nouveaux et apparemment aléatoires. L'utilisateur associe ce mot de passe aléatoire à un numéro personnel d'authentification pour créer un mot de passe unique qui ne vaut que pour une instance d'authentification unique. Si un pirate prend connaissance de ce mot de passe à l'aide d'un sniffer de paquets, l'information ne lui est d'aucune utilité car le mot de passe en question n'est déjà plus valide. Remarquez que cette technique de réduction du risque n'est efficace que contre un sniffer destiné à saisir les mots de passe. Les sniffers installés pour s'emparer des informations confidentielles (comme les messages de courrier électronique) n'en seront pas affectés.
- *L'infrastructure commutée* — Une autre méthode pour contrer l'utilisation de sniffers de paquets dans votre environnement est le déploiement d'une infrastructure commutée. Si, par exemple, une entreprise déploie un Ethernet commuté sur l'ensemble de ses communications, le pirate ne peut accéder qu'au trafic qui passe par le port particulier auquel il se connecte. L'infrastructure commutée ne supprime évidemment pas la menace des sniffers de paquets, mais elle réduit considérablement leur efficacité.
- *Les utilitaires anti-sniffer* — Une troisième méthode contre les sniffers consiste à employer un logiciel et un matériel conçus pour détecter l'utilisation de sniffers sur le réseau. De tels utilitaires – logiciels et matériels – ne suffisent pas à éliminer complètement la menace mais ils font partie, comme de nombreux utilitaires de sécurité réseau, de l'ensemble du système. Ces utilitaires "anti-sniffers" détectent les modifications dans les temps de réponse des stations afin de déterminer si ces derniers traitent davantage de trafic qu'ils ne devraient. L'un de ces utilitaires logiciels de sécurité réseau, disponible auprès de Security Software Technologies, est appelé AntiSniff. Pour plus d'information, consultez le site http://www.securitysoftwaretech.com/antisniff/
- *La cryptographie* — La méthode la plus efficace contre les sniffers de paquets ne les détecte pas et n'empêche pas leur utilisation, mais elle les rend inopérants. Si un canal de communication est protégé par codage, le sniffer de paquets ne pourra détecter que des données chiffrées (une chaîne de bits apparemment aléatoire) au lieu du message original. Le déploiement Cisco d'une cryptographie de réseau repose sur IPSec (IP Security), qui est une méthode standard pour les unités en réseau qui leur permet de communiquer de manière privée à l'aide du protocole IP. Parmi les autres protocoles cryptographiques d'administration de réseau, citons SSH (Secure Shell Protocol) et SSL (Secure Sockets Layer).

Usurpation d'adresse Internet (IP Spoofing)

L'attaque par usurpation d'adresse Internet ou spoofing consiste, pour un pirate situé à l'intérieur ou à l'extérieur du réseau, à imiter les conversations d'un ordinateur de confiance. Le pirate peut opérer de deux manières. Soit il utilise une adresse IP située dans l'intervalle des adresses IP de confiance du réseau, soit il s'empare d'une adresse IP externe de confiance par laquelle il est possible d'accéder à des ressources données sur le réseau. L'usurpation d'adresse Internet est souvent un point de départ pour d'autres attaques. Dans un exemple classique, le pirate lance une attaque par déni de service à l'aide d'adresses sources usurpées qui lui permettent de dissimuler son identité.

Normalement, l'attaque par usurpation d'adresse Internet se limite à l'injection de données ou de commandes nuisibles dans un flux de données passé entre un client et une application serveur ou dans une connexion de réseau entre homologues. Pour autoriser les communications dans les deux sens, le pirate doit modifier toutes les tables de routage pour qu'elles pointent en direction de l'adresse IP usurpée. Une démarche souvent employée par les pirates consiste à ne pas se soucier des réponses des applications. Si un pirate cherche à obtenir un fichier confidentiel dans un système, les réponses de l'application n'ont pas tellement d'importance. Toutefois, si le pirate parvient à modifier les tables de routage pour qu'elles pointent vers l'adresse IP usurpée, il est capable de recevoir tous les paquets de réseau qui sont adressés à l'adresse usurpée, et de répondre exactement de la même manière qu'un utilisateur de confiance.

Le risque d'usurpation d'adresse Internet peut être réduit, mais pas éliminé, grâce aux mesures suivantes :

- *Le contrôle d'accès* — La méthode la plus répandue pour se prémunir contre l'usurpation d'adresse Internet consiste à configurer convenablement le contrôle d'accès. Pour réduire l'efficacité de l'usurpation d'adresse Internet, configurez le contrôle d'accès pour qu'il refuse tout trafic en provenance d'un réseau extérieur lorsque l'adresse source de ce réseau correspond à celle d'un réseau interne. Remarquez que cela ne permet de contrer les attaques par déni de service que si les adresses internes sont les seules adresses de confiance. Si certaines adresses extérieures font partie des adresses de confiance, cette méthode perd son efficacité.
- *Le filtrage RFC 2827* — Vous pouvez également empêcher les utilisateurs d'un réseau d'usurper les adresses des autres réseaux (et accomplir en même temps votre devoir de citoyen Internet !) en bloquant tout trafic sortant de votre réseau dont l'adresse source n'appartient pas à l'intervalle IP de votre propre entreprise.

Votre fournisseur d'accès Internet (FAI) peut également mettre en place ce type de filtrage qui porte le nom générique de filtrage RFC 2827. Ce filtrage refuse tout trafic qui ne possède pas l'adresse source attendue sur une interface donnée. Si, par exemple, le FAI fournit une connexion sur l'adresse IP 15.1.1.0/24, il est capable de filtrer le trafic de telle sorte que seul le trafic dont l'adresse source est 15.1.1.0/24 puisse entrer sur son routeur par cette interface. Notez que l'efficacité de cette méthode restera considérablement réduite tant que tous les FAI n'auront pas mis en place ce type de filtrage. De plus, à mesure que vous vous éloignez des unités que vous désirez filtrer, il devient plus difficile de réaliser ce filtrage granulaire. L'installation, par exemple, d'un filtrage RFC 2827 sur le routeur d'accès à l'Internet exige de laisser passer le trafic qui porte le numéro de la totalité de votre réseau (c'est à dire, 10.0.0.0/8). Si vous réalisez un filtrage au niveau de la couche distribution, comme dans cette architecture, vous réaliserez un filtrage beaucoup plus précis (autrement dit, 10.1.5.0/24).

La méthode la plus efficace pour limiter les risques d'attaque par usurpation d'adresse Internet est la même que celle qui contre le plus efficacement la menace des sniffers de paquets, autrement dit, en supprimer l'efficacité. Pour que l'usurpation d'adresse Internet puisse fonctionner correctement, il est nécessaire que les unités utilisent une authentification basée sur l'adresse IP. Si, par conséquent, vous utilisez des méthodes d'authentification supplémentaires, les attaques par usurpation d'adresse Internet cesseront de constituer une menace. L'authentification cryptographique est la meilleure forme d'authentification complémentaire, mais lorsque cela est impossible, une authentification forte à deux facteurs utilisant un OTP peut se révéler très efficace.

Déni de service

Certainement la forme d'attaque la plus médiatisée, les attaques par déni de service font partie des plus difficiles à éradiquer. Même au sein de la communauté des pirates, les attaques par déni de service sont considérées comme simples et de "mauvais genre" car elles ne nécessitent que peu d'efforts pour réussir. Toutefois, en raison de leur facilité de mise en œuvre et des dégâts potentiels importants qu'elles peuvent provoquer, les attaques par déni de service méritent que les administrateurs de sécurité leur portent une attention toute particulière. Si vous désirez en savoir davantage sur ces attaques par déni de service, il peut être utile d'étudier les méthodes employées par certaines des attaques les plus connues. Ces attaques comprennent :

- la saturation TCP SYN
- le Ping of Death
- Tribe Flood Réseau, TFN,Tribe Flood Réseau 2000, TFN2K
- Trinoo
- Stacheldraht
- Trinity

Le CERT (Computer Emergency Response Team) est une autre excellente ressource sur le sujet de la sécurité. Le CERT a publié un article remarquable sur la manière de faire face aux attaques par déni de service; vous trouverez cet article à l'adresse : http://www.cert.org/tech_tips/denial_of_service.html.

Les attaques par déni de service sont différentes de la plupart des autres attaques en ce qu'elles ne cherchent généralement pas à obtenir un accès à votre réseau ou aux informations qu'il contient. Elles ont pour objectif de rendre un service inaccessible à une utilisation normale et sont le plus souvent réalisées en saturant une limitation de ressource sur le réseau ou au sein d'un système d'exploitation ou d'une application.
Lorsqu'elles font intervenir des applications serveurs de réseau particulières, comme des serveurs Web ou FTP, ces attaques peuvent chercher à acquérir et à garder ouvertes toutes les connexions supportées par le serveur en question, et parviennent à empêcher les utilisateurs légitimes du serveur ou du service d'y accéder. Les attaques par déni de service peuvent être également déclenchées à l'aide des protocoles Internet courants, comme TCP et ICMP (Internet Control Message Protocol). La plupart des attaques par déni de service exploitent une faiblesse de l'architecture globale du système attaqué plutôt qu'une erreur logicielle ou une défaillance de la sécurité. Toutefois, certaines attaques remettent en question le fonctionnement de votre réseau en le saturant de paquets non-désirés — et souvent inutiles — et en fournissant des informations erronées sur l'état des ressources réseau. Ce type d'attaques est souvent le plus difficile à contrer car il demande une coordination avec le fournisseur de l'accès réseau en amont. Si le trafic destiné à occuper la totalité de votre largeur de bande n'est pas stoppé à cet endroit, il ne sera pas plus utile de lui interdire l'entrée sur votre réseau car l'essentiel de votre largeur de bande disponible aura déjà été consommée. Lorsque ce type d'attaques est lancé depuis un grand nombre de systèmes différents en même temps, on parle parfois d'attaque par déni de service distribué.

La menace que représentent les attaques par déni de service peut être réduite grâce aux trois méthodes suivantes :

- *Les fonctions anti-usurpation* — Une configuration adaptée des fonctions anti-usurpation de vos routeurs et pare-feu permet de réduire le risque. Une telle configuration comprend au minimum un filtrage RFC 2827. Si le pirate est incapable de masquer son identité, il est incapable de placer son attaque.

- *Les fonctions anti-saturation* — Une configuration adaptée des fonctions anti-usurpation sur les routeurs et les pare-feu permet de réduire l'efficacité d'une attaque. Ces fonctions impliquent souvent la mise en œuvre de limites sur la quantité de connexions semi-ouvertes qu'un système autorise en ouverture à un instant donné.

- *Limitation du débit du trafic* — Une entreprise peut mettre en place une limitation du débit du trafic avec son fournisseur d'accès Internet (FAI). Ce type de filtrage limite à un débit fixé à l'avance la quantité de trafic non-essentiel qui traverse les segments du réseau. Un exemple courant consiste à limiter la quantité de trafic ICMP autorisé sur le réseau car il ne sert qu'à des fonctions de diagnostic. Les attaques par saturation sur les adresses ICMP sont fréquentes.

Attaque sur les mots de passes

Les pirates disposent de plusieurs méthodes pour mettre en œuvre les attaques sur les mots de passes : attaques en force, programmes "cheval de Troie", usurpation d'adresse Internet ou sniffers de paquets. Bien que les sniffers de paquets et l'usurpation d'adresse Internet puisse fournir des comptes utilisateur et des mots de passe, les attaques sur les mots de passes désignent le plus souvent des tentatives répétées pour identifier un compte utilisateur ou un mot de passe. Ces tentatives répétées sont appelées des attaques en force.

Le plus souvent, une attaque en force consiste à utiliser un programme qui parcourt le réseau et tente d'ouvrir une connexion sur une ressource partagée comme un serveur. Lorsqu'une personne parvient à accéder à une ressource, il possède les mêmes droits que l'utilisateur dont le compte a été piraté pour obtenir cet accès. Si le compte piraté possède des privilèges suffisants, le pirate peut créer des portes dérobées et se ménager son propre accès sans plus s'inquiéter des modifications d'état ou de mot de passe qui pourraient intervenir sur le compte.

Un autre problème survient lorsqu'un utilisateur possède le même mot de passe (éventuellement) sur chacun des systèmes auxquels il se connecte, ce qui comprend souvent un système personnel, des systèmes d'entreprise et d'autres sur l'Internet. Comme ce mot de passe n'est pas mieux protégé que la station la plus mal administrée qui le contient, le pirate dispose, une fois qu'il a pénétré la station en question, d'un mot de passe qu'il peut essayer sur un grand nombre de stations différentes.

Vous pouvez le plus simplement du monde éliminer les attaques sur les mots de passe en commençant par ne pas choisir de mots de passe en clair. L'emploi d'une authentification cryptographique ou d'un OTP suffit pratiquement à éliminer la menace des attaques sur les mots de passe. Malheureusement, toutes les applications, les stations et les unités ne supportent pas ces méthodes d'authentification. Si vous utilisez un mot de passe standard, il est important de le choisir de telle manière qu'il ne soit pas facile à deviner. Un mot de passe doit posséder au moins huit caractères et contenir des lettres en majuscules, des lettres en minuscules et des caractères spéciaux (#, %, $, etc.). Les mots de passe obtenus par un générateur aléatoire sont les plus sûrs, mais ils sont très difficiles à mémoriser et leurs utilisateurs sont souvent amenés à les écrire pour s'en souvenir. Ces attaques peuvent également être contrées en désactivant le compte après un certain nombre de tentatives incorrectes.
L'entretien des mots de passe, aussi bien pour l'utilisateur que pour l'administrateur, a fait quelques progrès. Il existe maintenant des applications logicielles qui codent une liste de mots de passe pour la stocker sur un ordinateur de poche. Ce scénario autorise l'utilisateur à se souvenir d'un unique mot de passe complexe tandis que tous les autres sont stockés en toute sécurité dans l'application. Du point de vue de l'administrateur, il existe plusieurs méthodes qui permettent d'attaquer en force les mots de passe des utilisateurs du réseau. L'une de ces méthodes fait appel à un utilitaire exploité par la communauté des pirates et nommé LC3 (auparavant L0phtCrack). LC3 attaque en force les mots de passe de Windows NT et peut signaler qu'un utilisateur a choisi un mot de passe facile à deviner. Pour plus d'informations, consultez le site : http://www.atatake.com/research/lc3/index.html.

Attaque par le milieu

Une attaque par le milieu demande au pirate d'avoir accès aux paquets de réseau qui traversent un réseau. Un exemple caractéristique est celui de la personne qui travaille pour un FAI et qui a accès à tous les paquets de réseau transférés entre le réseau de son employeur et un autre réseau. De telles attaques sont souvent mises en œuvre à l'aide de sniffers de paquets de réseau et de protocoles de routage et de transport. Les attaques de ce type sont le plus souvent destinées à voler des informations, à s'emparer d'une session en cours pour accéder aux ressources privées du réseau, à effectuer une analyse du trafic pour en extraire des renseignements sur un réseau et sur ses utilisateurs, à lancer une attaque par déni de service, à corrompre les données transmises et à introduire de nouvelles informations dans les sessions de réseau.

La seule manière de lutter efficacement contre les attaques par le milieu est d'avoir recours à la cryptographie. Si le pirate s'empare des données au cours d'une session privée et chiffrée, il ne verra rien d'autre que du texte chiffré et non le message original. Notez que si le pirate parvient à obtenir des renseignements concernant le codage de la session (comme la clé de session), il lui sera possible de réussir son attaque.

Attaque sur la couche application

Les attaques sur la couche application peuvent être réalisées de différentes manières. L'une des plus courantes consiste à exploiter des faiblesses bien connues des logiciels que l'on trouve couramment sur les serveurs : sendmail, Hypertext Transfer Protocol (HTTP) et FTP, par exemple. En tirant parti de ces faiblesses, le pirate peut accéder à l'ordinateur avec les permissions du compte qui exécute l'application, lequel est généralement un compte avec privilèges au niveau système. Ces attaques sur la couche application sont souvent fortement médiatisées dans le souci d'amener les administrateurs à rectifier le problème grâce à un patch. Malheureusement, de nombreux pirates sont également abonnés aux mêmes listes de diffusion, ce qui leur permet de se tenir au courant de l'attaque en même temps (s'ils ne l'ont pas déjà découverte).

Le problème principal des attaques sur la couche application est qu'elles utilisent souvent des ports qui ont l'autorisation de traverser le pare-feu. Un pirate qui se sert, par exemple, d'une faiblesse connue contre un serveur Web fera souvent transiter son attaque par le port 80 TCP. Comme le serveur Web sert des pages aux utilisateurs, un pare-feu doit autoriser l'accès sur ce port. Pour le pare-feu, le trafic pirate est indiscernable du trafic normal du port 80.

Les attaques sur la couche application ne peuvent jamais être complètement supprimées, car de nouvelles faiblesses sont régulièrement découvertes et diffusées auprès de la communauté Internet. La meilleure manière de réduire le risque est d'administrer sainement le système. Voici quelques-unes des mesures que vous pouvez prendre :

- Lisez les fichiers journaux du réseau ou du système d'exploitation ou faites-les analyser par des applications spécialisées

- Abonnez-vous aux listes de publipostage qui diffusent les vulnérabilités comme Bugtraq (http://www.securityfocus.com) et le CERT (Computer Emergency Response Team) (http://www.cert.org)

- Maintenez votre système d'exploitation et vos applications à jour avec les patches les plus récents

En plus de l'administration rigoureuse de vos systèmes, l'utilisation de systèmes de détection des intrusions (IDS) peut vous aider à lutter contre le problème. Il existe deux technologies IDS complémentaires :

- Le IDS de réseau (N-IDS) qui observe tous les paquets qui traversent un domaine de collision particulier. Lorsque le N-IDS voit un paquet ou une série de paquets qui correspondent à une attaque connue ou potentielle, il peut déclencher une alarme ou mettre fin à la session.

- Le IDS hôte (H-IDS) qui fonctionne en insérant des agents dans la station à protéger. Il ne s'occupe alors que des attaques lancées contre cet hôte.

Les IDS opèrent en utilisant des signatures d'attaque. Les signatures d'attaque correspondent au profil d'une attaque particulière ou d'un type d'attaques. Elles définissent un certain nombre de conditions qui doivent être remplies avant que le trafic puisse être considéré comme une attaque. Les appareils du monde réel qui correspondent le mieux aux IDS sont les systèmes d'alarme ou les caméras de sécurité. Leur plus grand inconvénient est le nombre de faux positifs que ces systèmes sont capables de générer. Le réglage des IDS pour éviter ces fausses alarmes est une condition essentielle de leur bon fonctionnement dans un réseau.

Reconnaissance du réseau

La reconnaissance du réseau désigne l'activité globale qui consiste à prendre des renseignements sur un réseau cible en utilisant des informations et des applications disponibles dans le public. Lorsqu'un pirate cherche à pénétrer un réseau donné, il a souvent besoin de collecter autant d'informations qu'il le peut sur ce réseau avant de lancer ses attaques. Ceci peut prendre la forme de requêtes DNS (Domain Name System), d'un bombardement ping et de balayage de ports. Les requêtes DNS peuvent fournir des renseignements sur l'appartenance d'un domaine donné ou sur les adresses assignées à ce domaine. Un bombardement de requêtes ping sur les adresses révélées par les requêtes DNS peut aider à constituer une image des stations actifs d'un environnement donné. Une fois qu'une telle liste a été générée, les outils de balayage de ports peuvent faire le tour de tous les ports bien connus pour fournir une liste de tous les services qui s'exécutent sur les stations révélées par le bombardement ping. Enfin, les pirates peuvent examiner les caractéristiques des applications qui s'exécutent sur les stations. Ce scénario peut fournir des renseignements précis qui seront utiles au pirate lorsqu'il cherchera à prendre le contrôle de ce service.

Il est impossible d'empêcher totalement de reconnaître le réseau. Si l'on désactive l'écho et la réponse par écho ICMP sur les routeurs frontières, par exemple, on interdit le bombardement de requêtes ping, mais au détriment des données de diagnostic du réseau. Toutefois, il est facile d'exécuter des balayages de ports sans utiliser un bombardement ping complet ; ces balayages prennent un peu plus de temps car ils doivent balayer les adresses IP qui pourraient ne pas être actives. L'IDS au niveau du réseau ou de la station est généralement capable de signaler à l'administrateur qu'une attaque de reconnaissance est en cours, ce qui lui permet de mieux se préparer à l'attaque à venir ou de prévenir le FAI qui héberge le système à l'origine des coups de sonde.

Exploitation de la confiance

Bien qu'il ne s'agisse pas d'une attaque en elle-même, ni par elle-même, l'exploitation de la confiance fait référence à une attaque par laquelle un individu exploite à son avantage la relation de confiance au sein d'un réseau. L'exemple classique est celui d'une connexion de réseau périmétrique en provenance d'une grande entreprise. Ces segments de réseau hébergent souvent des serveurs DNS, SMTP (Simple Message Transfer Protocol) et HTTP. Comme tous ces serveurs résident sur le même segment, il peut suffir de prendre le contrôle de l'un d'entre eux pour accéder à d'autres serveurs qui accordent leur confiance aux systèmes rattachés au même réseau qu'eux. Un autre exemple est celui du système situé à l'extérieur d'un pare-feu et qui possède une relation de confiance avec un système placé de l'autre côté du pare-feu. Si le système extérieur tombe entre les mains du pirate, il peut user de cette relation de confiance pour attaquer le réseau intérieur.

Il est possible de limiter les risques d'attaque qui reposent sur l'exploitation de la confiance en imposant des restrictions sévères sur les niveaux de confiance au sein d'un réseau. Les systèmes situés à l'extérieur d'un pare-feu ne doivent jamais bénéficier de la confiance absolue des systèmes placés à l'intérieur. Une telle confiance doit être limitée à des protocoles spécifiques et doit être identifiée autrement que par une adresse IP chaque fois que cela est possible.

Redirection des ports

L'attaque par redirection des ports est une forme d'exploitation de la confiance qui utilise une station piratée pour faire passer au travers d'un pare-feu un trafic qui, sans cela, aurait été rejeté. Imaginez un pare-feu possédant trois interfaces et une station sur chacune de ces interfaces. La station située à l'extérieur peut atteindre la station située sur le segment des services publics (généralement appelé zone démilitarisée ou DMZ), mais pas la station du réseau intérieur. La station du segment des services publics peut atteindre les deux autres, à l'intérieur comme à l'extérieur. Si un pirate est capable de prendre le contrôle de la station du segment des services publics, il peut installer un logiciel qui réacheminera le trafic provenant de la station extérieure directement vers la station intérieure. Bien qu'aucune des communications n'enfreigne les règles mises en œuvre par le pare-feu, la station extérieure sera ainsi parvenue à réaliser une connectivité avec la station intérieure par l'intermédiaire du processus de redirection des ports sur la station des services publics. L'application netcat est un exemple de logiciel capable de fournir ce type d'accès. Pour de plus amples renseignements, rendez-vous sur le site http://www.avian.org.

Pour limiter le risque du redirection des ports, il suffit principalement d'utiliser des modèles de confiance adaptés, comme nous l'avons décrit dans la section précédente. Si vous pensez qu'un système subit une attaque de ce genre, un H-IDS peut aider à détecter la présence d'un tel utilitaire et à empêcher le pirate de l'installer sur la station.

Accès non autorisé

Bien que les attaques par accès non autorisé ne constituent pas un type spécifique d'attaques, elles représentent la plupart de celles qui sont actuellement dirigées vers les réseaux. Pour qu'un pirate puisse attaquer en force une connexion Telnet, il doit d'abord obtenir l'invite Telnet sur un système. Au moment de la connexion sur le port Telnet, il peut apparaître le message du type : “Une autorisation est nécessaire pour utiliser cette ressource.” Si le pirate poursuit sa tentative d'accès, ses actions deviennent “non autorisées.” Ce type d'attaques peut être lancé de l'intérieur comme de l'extérieur du réseau.

Les techniques de prévention des attaques par accès non-autorisé sont très simples. Elles consistent à réduire ou à éliminer la possibilité pour un pirate de pouvoir accéder à un système à l'aide d'un protocole non autorisé. On peut par exemple empêcher le pirate d'avoir accès au port Telnet sur un serveur qui doit fournir des services Web vers l'extérieur. Si le pirate ne peut pas atteindre ce port, il lui est très difficile de l'attaquer. La fonction principale d'un pare-feu sur un réseau est d'empêcher les attaques simples d'accès non autorisé.

L'un des pare-feu les plus courant est le serveur de filtrage adaptatif. Ces pare-feu inspectent le trafic dans les deux directions et ouvrent les ports de manière dynamique lorsque les applications le demandent. Imaginons, par exemple, qu'un FTP actif négocie un port particulier pour le transfert de données. Le serveur de filtrage adaptatif verra cette information dans le paquet et permettra au port correspondant de communiquer entre le serveur et le client. Ceci est très différent d'une unité de filtrage standard des paquets qui ne tient pas compte des applications. Ces unités se contentent de regarder les données des couches 3 et 4 lorsqu'elles prennent une décision de contrôle d'accès. Dans notre précédent exemple FTP, il faudrait que l'administrateur ouvre manuellement tous les ports TCP hauts (> 1023) de l'extérieur pour permettre la communication FTP.

Virus et cheval de Troie

Les principales vulnérabilités des stations de travail pour utilisateurs finaux sont les virus et les attaques par cheval de Troie. Un virus est un logiciel conçu pour nuire et qui est joint à un autre programme pour exécuter une fonction particulière et indésirable sur la station de travail d'un utilisateur. Cela peut être par exemple un programme joint au command.com (l'interpréteur principal du système Windows) et qui détruit certains fichiers et infecte toutes les autres versions de command.com qu'il peut trouver. Un cheval de Troie a ceci de différent que l'application tout entière a été écrite pour ne pas paraître ce qu'elle est, autrement dit un utilitaire d'attaque. Un cheval de Troie peut par exemple se présenter sous l'aspect d'une application logicielle qui exécute un jeu simple sur le poste de travail de l'utilisateur : pendant que celui-ci est occupé à jouer, le cheval de Troie envoie une copie de lui-même à tous les utilisateurs du carnet d'adresse de la victime. Lorsque les autres reçoivent le jeu et l'exécutent, ils perpétuent la diffusion du cheval de Troie.

Les applications de ce type peuvent être contenues grâce à l'utilisation efficace d'un logiciel anti-virus au niveau de l'utilisateur et, éventuellement, au niveau du réseau. Les logiciels anti-virus peuvent détecter la plupart des virus et de nombreuses applications du type cheval de Troie, et les empêcher de se propager dans le réseau. Se tenir au courant des développements les plus récents concernant ce type d'attaques peut également vous amener à adopter une attitude plus efficace contre ces attaques. A mesure que de nouveaux virus ou applications "troyennes" apparaissent, les entreprises doivent remettre à jour leurs logiciels anti-virus et se procurer les versions les plus récentes de leurs applications.

Qu'est-ce qu'une “politique de sécurité” ?
Une politique de sécurité peut être aussi simple que la définition d'un code acceptable pour l'utilisation des ressources du réseau ou aussi complexe qu'un document de plusieurs centaines de pages qui détaille chaque élément de connectivité et les modalités associées. Bien que d'une portée quelque peu limitée, le document RFC 2196 définit de manière acceptable une politique de sécurité de la manière suivante :

Une politique de sécurité est une déclaration officielle des règles qui doivent régir le comportement des personnes auxquelles on accorde un accès aux ressources technologiques et aux actifs informationnels d'une entreprise.

Le présent article ne cherche pas à entrer dans les détails du développement d'une politique de sécurité. Le document RFC 2196 propose quelques renseignements précieux sur le sujet, et de nombreux sites sur le Web présentent des exemples de politiques et de directives. Les pages Web suivantes peuvent fournir une aide au lecteur intéressé :

- RFC 2196 “Site Security Handbook” http://www.ietf.org/rfc/rfc2196.txt
- Un exemple de politique de sécurité pour l'université de l'Illinois http://www.aits.uillinois.edu/security/securestandards.html
- Design et mise en œuvre d'une politique de sécurité d'entreprise http://www.knowcisco.com/content/1578700434/ch06.shtml

La politique de sécurité : une nécessité
Il est important de comprendre que la sécurité réseau est un processus évolutif. Aucun produit ne peut, à lui seul, protéger entièrement une entreprise. La véritable sécurité réseau émerge d'une association de produits et de services, auxquels s'ajoutent une politique de sécurité complète et l'engagement de respecter cette politique dans l'entreprise, du plus haut au plus bas de l'échelle. En fait, une politique de sécurité convenablement mise en œuvre sans le matériel de sécurité dédié peut être plus efficace pour limiter les risques qui pèsent sur les ressources de l'entreprise qu'un produit de sécurité informatique complet installé sans politique de sécurité associée.

Fonctions et protocoles de gestion
- *SSH et SSL* — Fournissent un accès à distance chiffré et identifié vers l'unité administrée
- *Telnet* — Fournit un accès à distance en "clair" vers l'unité administrée
- *Syslog* — Fournit des informations de journalisation des unités et alerte les serveurs d'administration
- *Trivial File Transfer Protocol (TFTP)* — Permet aux administrateurs de transférer aux serveurs d'administration les fichiers de configuration des unités administrées
- *Simple Network Management Protocol (SNMP)* — Permet le transfert des informations relatives aux unités vers les serveurs d'administration
- *Network Time Protocol (NTP)* — Permet la synchronisation des horloges entre les unités

Les fonctions d'administration autorisées sur les unités sont présentées dans les sections suivantes :

Administration de la configuration (SSH, SSL, Telnet) — Chaque fois que cela est possible, il convient d'utiliser IPSec, SSH, SSL ou tout autre moyen de transport chiffré et authentifié qui permette aux informations d'administration de transiter vers les unités distantes. Toutefois, si l'unité ne supporte aucun de ces protocoles, il peut devenir nécessaire d'employer Telnet bien que ce protocole ne soit pas fortement recommandé. L'administrateur de réseau doit savoir que les données d'une session Telnet sont envoyées "en clair" et peuvent être interceptées par toute personne équipée d'un sniffer de paquets placé le long du trajet qu'empruntent les données entre l'unité et le serveur d'administration. Les données peuvent comprendre des informations confidentielles, comme la configuration de l'unité elle-même, des mots de passe, et d'autres choses encore. Indépendamment de l'utilisation de SSH, de SSL ou de Telnet pour l'accès à distance à cette unité, les listes de contrôle d'accès (ACL) doivent être configurées pour ne permettre qu'aux serveurs d'administration de se connecter à l'unité. Toutes les tentatives provenant d'autres adresses IP doivent être rejetées et consignées dans le fichier journal. Il convient également d'implanter le filtrage RFC 2827 sur le routeur d'entrée afin de réduire les chances d'un agresseur extérieur au réseau de parvenir à usurper les adresses des stations d'administration. Le protocole SSH utilise le port TCP 22, Telnet le port 23, et SSH le port 443.

Journalisation — Syslog est également expédié en clair entre l'unité administrée et la station d'administration. Syslog ne possède pas de fonction de vérification de l'intégrité des paquets pour garantir que le contenu des paquets n'a pas été modifié au cours du déplacement. Un pirate peut modifier les données de syslog afin de tromper l'administrateur de réseau au cours de l'attaque. Chaque fois que cela est possible, le trafic syslog peut être chiffré à l'intérieur d'un tunnel IPSec afin de réduire les chances qu'il puisse être modifié au cours de son déplacement. Si les données syslog ne peuvent pas être chiffrées dans le tunnel IPSec pour des questions de coûts ou de capacités de l'unité elle-même, l'administrateur de réseau doit tenir compte du fait qu'il existe un risque potentiel de falsification des données de syslog par un pirate. Si vous accordez l'accès aux données syslog en provenance de l'extérieur du pare-feu, il est indispensable d'établir un filtrage RFC 2827 sur le routeur de sortie.

Cette configuration permet de limiter la probabilité qu'un pirate puisse, de l'extérieur du réseau, usurper une adresse de l'unité administrée et envoyer des données syslog modifiées vers les stations d'administration. Des listes de contrôle d'accès doivent également être mises en place sur le pare-feu afin de permettre aux seules données syslog en provenance des unités administrées de parvenir aux stations d'administration. Ce scénario empêche l'éventuel pirate d'expédier des quantités importantes de données syslog erronées vers un serveur d'administration pour tromper l'administrateur de réseau au cours d'une attaque. Syslog utilise le port UDP 514.

TFTP — De nombreuses unités de réseau utilisent le protocole TFTP pour transférer les fichiers de configuration ou les fichiers système sur le réseau. TFTP utilise le port UDP (User Datagram Protocol) 69 ainsi que les ports UDP hauts (1023) pour le flux de données entre l'unité et le serveur TFTP, et transfère également les données en clair. L'administrateur de réseau doit savoir que les données d'une session TFTP peuvent être interceptées par toute personne qui gère un sniffer de paquets le long du parcours des données entre l'unité et le serveur d'administration. Les données peuvent comprendre des informations confidentielles, comme la configuration de l'unité elle-même, etc. Chaque fois que cela est possible, le trafic TFTP doit être chiffré à l'intérieur d'un tunnel IPSec afin de réduire la probabilité qu'il puisse être intercepté.

SNMP — SNMP est un protocole d'administration de réseau qui peut servir à récupérer des informations auprès d'une unité de réseau (ce que l'on désigne généralement par un accès en lecture seule) ou pour configurer à distance les paramètres sur l'unité (ce que l'on désigne par un accès en lecture / écriture). Les agents SNMP écoutent sur le port UDP 161. Avec chaque message, SNMP utilise des mots de passe, appelés chaînes communautaires, qui constituent une forme rudimentaire de protection. Malheureusement, la plupart des mises en œuvre actuelles de SNMP sur les unités en réseau envoient la chaîne communautaire en clair avec le message. Ainsi, les messages SNMP peuvent être interceptés par toute personne utilisant un sniffer de paquets placé sur le trajet des données entre l'unité et le serveur d'administration, et la chaîne communautaire peut être utilisée par un pirate. Dans ce cas, le pirate peut reconfigurer l'unité si elle permet l'accès en lecture / écriture par SNMP. Nous recommandons ainsi de configurer le protocole SNMP à l'aide de chaînes communautaires en lecture seule. Vous pouvez acquérir un degré supplémentaire de protection en définissant un contrôle d'accès sur l'unité à administrer par l'intermédiaire de SNMP afin que seuls les stations d'administration autorisées puissent y accéder.

NTP — Network Time Protocol permet de synchroniser les horloges des différentes unités du réseau. La synchronisation des horloges sur le réseau est un élément vital pour les certificats numériques, et pour une interprétation convenable des événements dans les données syslog. Une méthode sûre pour fournir ce service d'horloge au réseau consiste pour l'administrateur de réseau à installer sur le réseau privé sa propre horloge maîtresse et à la synchroniser par satellite ou par radio au temps universel coordonné (UTC, Coordinated Universal Time). Toutefois, si l'administrateur de réseau ne souhaite pas installer sa propre horloge maîtresse à cause de son coût ou pour toute autre raison, il peut avoir accès à des sources d'horloges qui permettent la synchronisation par Internet. Un pirate peut tenter d'effectuer une attaque par saturation sur un réseau en envoyant de fausses données NTP sur l'Internet, cherchant ainsi à modifier le réglage des horloges sur les unités de réseau pour rendre invalides les certificats numériques. De plus, pendant l'attaque, l'agresseur peut chercher à tromper l'administrateur de réseau en déréglant les horloges de ses unités de réseau. Ce scénario complique le travail de l'administrateur qui désire connaître l'ordre des événements syslog sur plusieurs unités. A partir de la version 3, le protocole NTP supporte un mécanisme d'authentification par codage entre homologues. Pour réduire les risques d'un tel scénario, nous recommandons l'emploi de mécanismes d'authentification ainsi que celui des listes de contrôle d'accès qui précisent les unités de réseau autorisées à se synchroniser avec les autres unités de réseau. L'administrateur de réseau doit évaluer le coût réel de l'économie qu'il réalise en obtenant les données d'horloge à partir de l'Internet avec le risque de leur permettre de passer au travers du pare-feu. De nombreux serveurs NTP sur l'Internet n'exigent aucune authentification des homologues. Ainsi, l'administrateur de réseau doit avoir la certitude que l'horloge elle-même est fiable, exacte et sûre. NTP utilise le port UDP 123.

Annexe C : Terminologie de l'architecture

Serveur d'application — Le serveur d'application fournit, directement ou indirectement, des services d'application aux entreprises qui en sont les utilisateurs finaux. Les services peuvent comprendre des applications de gestion des flux de travail, de services administratifs ou de sécurité.

Serveur de filtrage adaptatif (pare-feu) — Cette unité de filtrage de paquets de plus bas niveau conserve des tableaux d'état pour les protocoles à base IP. Le trafic n'est autorisé à traverser le pare-feu que s'il est conforme aux filtres de contrôle d'accès définis ou s'il fait partie d'une session déjà établie dans le tableau des états.

IDS - hôte — Le système de détection des intrusions sur la station (H-IDS) est une application logicielle qui contrôle l'activité sur une station donnée. Les techniques de contrôle peuvent comprendre la validation des appels au système d'exploitation et aux applications, et la vérification des fichiers journaux, des informations concernant le système de fichiers et les connexions de réseau.

IDS – réseau — L'IDS – réseau (N-IDS) est généralement utilisé de manière ininterrompue. Cette unité capture le trafic sur un segment de réseau local et tente de comparer le trafic en temps réel avec des signatures d'attaques connues. Les signatures recherchées vont du niveau atomique (un seul paquet dans une seule direction) jusqu'aux signatures composites (multipaquets) qui exigent des tableaux d'état et un suivi des applications de la couche 7.

Pare-feu Cisco IOS — Le pare-feu Cisco IOS est un serveur de filtrage adaptatif qui s'exécute de manière naturelle sur le logiciel Cisco IOS.

Routeur Cisco IOS — Le routeur Cisco IOS se compose d'une large gamme d'unités de réseau adaptables qui fournissent de nombreux services de routage et de sécurité pour toutes les conditions d'exploitation. La plupart des unités sont modulaires et possèdent une gamme d'interfaces physiques pour réseaux locaux et WAN.

Commutateur de couche 2 — Un commutateur de couche 2 fournit des services de bande passante et de réseau local virtuel (VLAN) aux segments de réseau au niveau Ethernet. En général, ces unités offrent des ports 10/100 individuels commutés, des liaisons montantes Gigabit Ethernet, une agrégation des ports pour les réseaux locaux virtuels et des fonctions de filtrage de couche 2.

Commutateur de couche 3 — Un commutateur de couche 3 fournit des fonctions à haut débit semblables à celles du commutateur de couche 2, auxquelles s'ajoutent des fonctions de routage, de qualité de service et de sécurité. Ces commutateurs possèdent souvent des capacités de processeurs de fonctions spéciaux.

Serveur d'administration — Le serveur d'administration fournit des services d'administration de réseau aux opérateurs des réseaux d'entreprise. Les services comprennent la gestion de configuration générale, le contrôle des unités de sécurité réseau et l'exécution des fonctions de sécurité.

Serveur de filtrage de contenu SMTP — Cette application serveur s'exécute le plus souvent sur un serveur SMTP externe qui contrôle le contenu (y compris les pièces jointes) du courrier entrant et sortant afin de décider si ce courrier est autorisé à poursuivre son chemin en l'état ou après modification, ou s'il doit être rejeté.

Serveur de filtrage URL — Cette application serveur s'exécute le plus souvent sur un serveur autonome qui contrôle les requêtes URL qui lui sont envoyées par l'unité de réseau : elle indique à cette unité de réseau si la requête peut être transmise sur l'Internet. Cette configuration permet à l'entreprise de mettre en place une politique de sécurité qui précise les catégories de sites Internet qui ne sont pas autorisées.

Unité de raccordement VPN — Cette unité assure le raccordement des tunnels IPSec pour les connexions VPN de site à site ou par accès distant. L'unité doit fournir des services supplémentaires pour offrir les mêmes fonctionnalités de réseau qu'un réseau WAN classique ou qu'une connexion commutée.

Poste de travail ou terminal utilisateur — Un poste de travail ou terminal utilisateur est une unité quelconque du réseau qui est utilisée directement par l'utilisateur final : il peut s'agir d'un PC, d'un téléphone IP, d'appareils sans fil, etc.

Figure 21 - Légende

Légende des diagrammes

Références

RFC

RFC 2196 “Site Security Handbook”	http://www.ietf.org/rfc/rfc2196.txt
RFC 1918 “Address Allocation for Private Internets”	http://www.ietf.org/rfc/rfc1918.txt
RFC 2827 “Réseau Ingress Filtering: Defeating DoS Attaques which Employ IP Source Address Spoofing”	http://www.ietf.org/rfc/rfc2827.txt

---

Références diverses

“Improving Security on Cisco Routers”	http://www.cisco.com/warp/public/707/21.html
“VLAN Security Test Report”	http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
“AntiSniff”	http://www.securitysoftwaretech.com/antisniff
“LC3”	http://www.atstake.com/research/lc3/index.html
“DoS Attacks”	http://www.cert.org/tech_tips/denial_of_service.html
“Computer Emergency Response Team”	http://www.cert.org
“Security Focus (Bugtraq)”	http://www.securityfocus.com
“Avian Research (netcat)”	http://www.avian.org
“University of Illinois Security policy”	http://www.aits.uillinois.edu/security/securestandards.html
“Design and Implementation of the Corporate Security policy”	http://www.knowcisco.com/content/1578700434/ch06.shtml

---

Références des produits partenaires

Système MPS RSA SecureID	http: //www.rsasecurity.com/products/securid/
Système de filtrage de courrier électronique Baltimore MIMESweeper	http://www.mimesweeper.com
Filtrage URL Websense	http://www.websense.com/products/integrations/ciscopix.cfm
Client SSH F-Secure	http://www.fsecure.com/products/ssh/
Utilitaire d'analyse syslog OpenSystems PrivateI	http://www.opensystems.com/products/index.asp
Pare-feu personnel Zone Alarm Pro	http://www.zonelabs.com/products/index.html
Sécurité générale AVVID Cisco et Renseignements sur les VPN de Solution Partners	http://www.cisco.com/go/securitypartners

Remerciements

Les auteurs aimeraient publiquement remercier toutes les personnes qui ont contribué à l'architecture SAFE et à la rédaction de ce document. Il ne fait aucun doute que sans les connaissances, les conseils et les commentaires précieux de tous les employés de Cisco, au siège social comme sur le terrain, il n'aurait pas été possible de mettre la dernière pierre à cette architecture. Par ailleurs, de nombreuses personnes ont contribué à la mise en œuvre et à la validation en laboratoire de cette architecture. Le cœur de l'équipe était composé de Rahimulah Rahimi, Jason Halpern, Mark Doering, Tom Hunter, Masamichi Kaneko, Alok Mittal et Mike Steinkoenig.
Merci à tous de vos efforts tout particuliers.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
11, rue Camille Desmoulins
92782 Issy les Moulineaux
Cedex 9
France
www.cisco.com
Tel: +33 (0)1 58 04 60 00
Fax: +33 (0)1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems possède plus de 190 bureaux dans les pays suivants. Les adresses, les numéros de téléphone et de télécopie sont accessibles sur le site Web de Cisco.com **à l'adresse www.cisco.com/go/offices.**

Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Chine • Colombie • Costa Rica • Croatie • République tchèque • Danemark • Dubaï, EAU • Finlande • France • Allemagne • Grèce • Hong Kong • Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Corée • Luxembourg • Malaisie • Mexico • Pays-Bas • Nouvelle Zélande • Norvège • Pérouo Philippines • Pologne • Portugal • Porto Rico • Roumanie • Russie • Arabie saoudite • Ecosse • Singapour • Slovaquie • Slovénie • Afrique du Sud • Espagne • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Royaume-Uni • Etats-Unis • Venezuela • Vietnam • Zimbabwe