Livre blanc

Cisco **SAFE** : Description détaillée de la sécurité pour les réseaux locaux sans fil

Les auteurs

Sean Convery (CCIE #4232), Darrin Miller (CCIE #6447) et Sri Sundaralingam sont les principaux rédacteurs de ce livre blanc. Mark Doering, Pej Roshan, Stacey Albert, Bruce McMurdo et Jason Halpern, qui ont apporté leur importante contribution à ce document, sont les responsables de la définition des architectures de référence chez les architectes en chef de l'implantation de référence Cisco à San Jose en CalifornieSystems. Tous sont des architectes réseaux spécialisés dans les réseaux locaux sans fil, les VPN ou les problèmatiqueses de sécurité.

Résumé

Ce livre blanc décrit les meilleures pratiques pour concevoir et mettre en œuvre des réseaux locaux sans fil (WLAN) sécurisés en reprenant des éléments du schéma directeur Cisco SAFE pour la sécurité des réseaux. Tous les livres blancs SAFE sont disponibles sur le site Web SAFE :

http://www.cisco.com/go/safe

Ces documents ont été rédigés dans le souci de présenter les meilleures pratiques de la sécurité des réseaux et de l'architecture des réseaux privés virtuels (VPN). Bien qu'il soit possible de lire le présent document en n'ayant consulté aucun des deux principaux livres blancs sur l'architecture des réseaux sécurisés, nous vous recommandons d'étudier soit « SAFE Entreprise » soit « SAFE Small, Midsize and Remote-User Networks » avant de continuer.

Le présent livre blanc inscrit la mise en œuvre des réseaux WLAN dans le cadre d'une architecture de sécurité globale. En matière de sécurité et d'architecture des VPN, SAFE adopte une démarche système qui donne la priorité aux objectifs généraux d'architecture et traduit ces objectifs en configurations et en topologies spécifiques. Dans le domaine du sans fil, Cisco recommande d'envisager également les éléments architecturaux du réseau comme la mobilité et la qualité de service (QoS) avant de choisir une architecture générale de réseau WLAN. La méthode SAFE s'appuie sur les produits Cisco et sur ceux de ses partenaires.

Le présent document commence par un descriptif de l'architecture avant d'examiner en détail les architectures spécifiques envisageables. Le présent document s'articule autour de deux principales variantes que nous décrirons de manière générale dans un premier temps, puis dans leur relation avec SAFE. Les architectures suivantes sont étudiées en détail :

- grand réseau WLAN
- réseau WLAN de taille moyenne
- petit réseau WLAN
- réseau WLAN pour utilisateurs distants

Chacune peut prévoir de multiples modules faisant appels à différents aspects de la technologie des réseaux WLAN. Le concept de modules est décrit dans les livres blancs sur la sécurité SAFE.

Après la présentation des architectures spécifiques, l'annexe A décrit un laboratoire de validation de la sécurité sans fil SAFE et fournit divers clichés exemples de configuration. L'annexe B est une introduction aux WLAN. Si vous n'êtes pas familiarisé avec les concepts de base des réseaux locaux sans fil, il est préférable de

lire cette section avant le reste de ce livre blanc. L'annexe C fournit des détails supplémentaires sur la détection des points d'accès illégaux et les techniques de prévention. Enfin, l'annexe D examine les critères architecturaux de haute disponibilité pour les services comme RADIUS et DHCP dans l'optique de la sécurisation des WLAN.

A qui ce document s'adresse-t-il ?

Bien que de nature technique, ce livre blanc peut être lu à différents niveaux en fonction de l'intérêt que vous portez au sujet. Un administrateur réseau, par exemple, pourra se contenter des introductions de chaque section pour obtenir une bonne vision d'ensemble des stratégies et des éléments à prendre en compte pour la sécurisation des réseaux WLAN. L'ingénieur ou l'architecte réseau, en revanche, lira ce document dans son intégralité pour en tirer des informations détaillées sur l'architecture de réseau et l'analyse des menaces – informations étayées par des clichés exemples de configuration réelle des équipements utilisés. Ce document couvre un éventail large de déploiements WLAN : il peut donc être intéressant de commencer par lire les introductions de chaque section avant d'étudier en détail celles qui traitent du type de réseau WLAN que vous cherchez à déployer.

Mises en garde

Ce document suppose que vous avez mis en place une politique de sécurité. Cisco Systems ne saurait recommander le déploiement de réseaux WLAN – ou de n'importe quelle technologie de réseau – sans une politique de sécurité associée. Bien que le présent document rappelle des principes fondamentaux de sécurité, il ne les décrit pas en détail. La sécurité dont il est question ici fait systématiquement référence à celle des WLAN.

Bien que les réseaux WLAN laissent la porte ouverte à certains risques de sécurité, de nombreuses organisations choisissent de les déployer en raison des avantages qu'ils procurent en termes de productivité utilisateur et de simplicité de déploiement pour les petits réseaux. Même si vous suivez les principes directeurs décrits ici, nous ne saurions garantir la sécurité de votre environnement WLAN, pas plus que votre capacité à bloquer toute tentative de pénétration : ces principes vous permettront en revanche de limiter autant que possible les risques de sécurité sur les réseaux WLAN.

Bien que le présent document contienne des informations nombreuses et détaillées sur la plupart des aspects de la sécurité sans fil, il ne prétend pas à l'exhaustivité. Notamment, nous ne parlons pas ici des ponts sans fil, des ordinateurs de poche (PDA), ni des technologies WLAN qui ne reposent pas sur la norme 802.11. Par ailleurs, ce document n'offre aucun conseil particulier sur les problèmes généraux d'architecture et de déploiement des WLAN qui ne seraient pas liés à la sécurité.

Au cours de la validation de SAFE, les véritables produits ont été configurés dans l'exacte mise en œuvre de réseau décrite dans cet article. L'annexe A, « Laboratoire de validation », présente des clichés exemples de configuration spécifiques tirés de notre laboratoire.

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 une meilleure lisibilité.

Description générale de l'architecture

Principes fondamentaux

Cisco SAFE WLAN émule de manière aussi proche que possible les besoins fonctionnels des réseaux actuels. Les décisions de mise en œuvre 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 :

- la sécurité et la limitation des risques doivent s'appuyer sur une politique ;
- l'accès des utilisateurs aux ressources du réseau filaire doit être soumis à l'identification et aux autorisations ;
- la confidentialité des données sans fil doit être assurée ;
- les utilisateurs doivent être différenciés ;

- les points d'accès doivent être gérés ;
- les utilisateurs doivent être authentifiés avant d'accéder aux ressources du réseau ;
- des options de haute disponibilité doivent être prévues (pour les grandes entreprises seulement).

Le plus important pour un réseau SAFE WLAN est de fournir une option de connectivité WLAN sécurisée vers les réseaux d'entreprise. En tant qu'option de connectivité, l'accès au réseau WLAN doit respecter aussi étroitement que possible la politique de sécurité de l'organisation. De plus, cet accès doit être aussi sécurisé que possible tout en reconnaissant la nécessité de conserver le plus grand nombre des caractéristiques d'un réseau LAN filaire traditionnel. Enfin, les WLAN doivent pouvoir s'intégrer à un réseau existant conçu autour de l'architecture de sécurité SAFE.

Les axiomes SAFE WLAN

Les réseaux sont des cibles

Les réseaux sans fil sont désormais l'une des cibles les plus intéressantes pour les pirates. Les organisations déploient aujourd'hui la technologie sans fil à un rythme soutenu, souvent sans tenir compte de l'ensemble des considérations de sécurité. Cet engouement est en partie dû au faible coût des unités, à la simplicité de leur déploiement et à leurs avantages décisifs en termes de productivité. La communauté des pirates, qui sait que les fonctions de sécurité sont désactivées sur les unités WLAN livrées aux clients, s'intéresse de près à la prolifération des réseaux sans fil. Plusieurs sites Web dressent l'inventaire des connexions sans fil librement accessibles dans tous les Etats-Unis.

Si la plupart des pirates se servent de ces connexions pour accéder gratuitement à Internet ou pour masquer leur identité, un petit groupe d'entre eux voit dans cette situation la possibilité de pénétrer sur des réseaux qui, sans cela, seraient difficiles à attaquer à partir d'Internet. A la différence des réseaux filaires, le réseau WLAN transmet ses données par voie aérienne et peut être accessible à l'extérieur du périmètre « physique » de l'organisation. Si les données qui transitent sur le réseau WLAN ne sont pas cryptées, toute personne capable de capter l'émission radiofréquence peut les consulter. Avec un ordinateur portable sous Linux, une carte WLAN et un programme comme TCPDUMP, n'importe qui peut recevoir, visualiser et stocker la totalité des paquets qui circulent sur un WLAN donné.

Interférence et brouillage

Il est également facile d'interférer avec les communications sans fil. Un simple émetteur de brouillage peut rendre toute communication impossible. En envoyant, par exemple, à un point d'accès des demandes d'accès en grand nombre – acceptées ou non – le pirate finit par épuiser son spectre radiofréquence et le « décroche » du réseau. D'autres services sans fil de la même gamme de fréquences que le réseau WLAN peuvent limiter la portée et la bande passante utilisable du réseau. « Bluetooth », qui permet de communiquer d'un combiné à l'autre ou entre plusieurs serveurs d'informations, n'est que l'une des nombreuses technologies modernes qui utilisent la même gamme de fréquences de 2,4 GHz que les unités WLAN, et peut ainsi interférer avec les transmissions.

Authentification MAC

Les points d'accès WLAN peuvent identifier n'importe quelle carte sans fil grâce à son adresse MAC (Media Access Control) unique qui est gravée et imprimée sur son support. Certains WLAN exigent qu'une carte soit enregistrée avant de lui permettre l'accès aux services sans fil. Le point d'accès identifie alors la carte par son utilisateur, mais ce scénario demeure complexe car chaque point d'accès doit pouvoir accéder à la liste de ces utilisateurs. Même si le système est mis en place, un pirate peut le contourner avec un logiciel qui n'utilise pas l'adresse véritable de la carte WLAN, mais une adresse aléatoire ou même délibérément usurpée. Grâce à cette vraie « fausse » adresse, il peut chercher à insérer du trafic réseau ou se faire passer pour un utilisateur légitime.

Mode ad hoc ou mode infrastructure

La plupart des organisations déploient leurs WLAN dans un mode appelé « infrastructure » : chaque client sans fil se connecte alors par l'intermédiaire d'un point d'accès pour toutes ses communications. Il est toutefois possible de déployer la technologie WLAN afin qu'elle crée un réseau peer-to-peer indépendant, ce que l'on appelle plus généralement un WLAN ad hoc. Sur un WLAN ad hoc, les ordinateurs portables ou de bureau, équipés de cartes

compatibles WLAN et placés à portée l'un de l'autre, peuvent directement échanger des fichiers sans passer par un point d'accès. Cette portée est variable en fonction du type de système WLAN. Les ordinateurs portables ou de bureau équipés de cartes WLAN 802.11b ou 802.11a peuvent réaliser un réseau ad hoc s'ils se trouvent à moins de 150 m l'un de l'autre environ.

Les conséquences des WLAN ad hoc sur la sécurité sont considérables. De nombreuses cartes sans fil, notamment celles fournies de série par les constructeurs de PC, prennent en charge le mode ad hoc. Lorsqu'une telle carte passe en mode ad hoc, n'importe quel pirate disposant d'une carte configurée pour ce mode et avec les mêmes paramètres que les autres, peut accéder sans autorisation aux clients.

Attaques par saturation

Les messages d'administration 802.11 – trame Beacon, demande ou réponse à une sonde, demande ou réponse d'association ou de ré-association, désassociation, désauthentification, etc. – ne sont pas authentifiés et laissent la porte ouverte aux attaques par saturation. Des outils à source ouvertegratuits, comme WLAN-jack, ont montré leur « utilité » pour ce genre d'attaques par saturation.

Les réseaux sans fil sont des armes

Un point d'accès illégal est une ouverture sur le réseau qui est accessible aux employés d'une organisation mais non gérée par elle de manière sécurisée. La plupart de ces points d'accès illégaux sont installés par des employés lorsque le service informatique ne leur fournit pas un accès WLAN. Ainsi le point d'accès illégal le plus courant est un appareil bon marché, acheté par un employé et branché par lui sur un port de commutation disponible, le plus souvent sans s'inquiéter des mesures de sécurité. Même de l'extérieur des locaux de l'entreprise, il suffit au pirate de s'associer à un point d'accès illégal pour pénétrer sur le réseau sécurisé. L'autre type de point d'accès illégal est celui qui se fait passer pour un point d'accès sécurisé pour amener les utilisateurs du WLAN à s'associer avec lui : le pirate peut alors manipuler les trames sans fil à mesure qu'elles transitent par le point d'accès.

La menace que constituent les points d'accès sauvages peut être atténuée en empêchant leur déploiement et en détectant ceux qui sont déjà déployés. Pour ce faire, les composants suivants sont indispensables. L'annexe C, « Autres informations sur les points d'accès illégaux », présente une étude détaillée de ces éléments.

Prévention

- Politique d'entreprise
- Sécurité matérielle
- Infrastructure WLAN supportée
- Sécurité 802.1X au niveau des ports sur les commutateurs de périphérie

Détection

- Utilisation d'analyseurs de réseau sans fil
- Utilisation d'outils avec script sur l'infrastructure filaire
- Observation physique du placement et de l'utilisation des points d'accès sans fil

La norme 802.11 n'est pas sécurisée

Comme nous le disons dans notre introduction aux WLAN (annexe B), les normes 802.11b et 802.11a sont actuellement les technologies WLAN les plus répandues. Classiquement, la sécurité des WLAN 802.11 est obtenue par l'authentification ouverte ou à clé partagée, et par des clés WEP (Wired Equivalent Privacy) statiques. L'association de ces modes offre un niveau rudimentaire de contrôle d'accès et de confidentialité, mais chaque élément du système présente des failles. Les sections suivantes décrivent ces éléments et les problèmes qu'ils peuvent poser dans un environnement d'entreprise.

Authentification

La norme 802.11 supporte deux types d'authentification client : l'authentification ouverte et par clé partagée. L'authentification ouverte consiste en substance à fournir le bon identificateur SSID (Service Set ID). Avec ce type d'authentification, WEP permet d'empêcher le client d'envoyer des données au point d'accès ou d'en recevoir à moins qu'il ne possède la bonne clé WEP. Avec l'authentification à clé partagée, le point d'accès lance à l'unité client un défi sous la forme d'un paquet texte qu'il doit crypter avec la bonne clé avant de le renvoyer. Si le client ne possède pas la bonne clé, ou pas de clé du tout, l'authentification échoue et le client n'est pas autorisé à s'associer au point d'accès. L'authentification par clé partagée n'est pas considérée comme sûre car si le pirate parvient à capturer le message texte envoyé en clair par le point d'accès et la réponse cryptée, il sera en mesure de déchiffrer la clé WEP.

Gestion des clés

Un autre type de clé fréquemment utilisé – mais pas davantage plus sûr – est la clé WEP « statique ». Cette clé, composée de 40 ou de 128 bits, est définie de manière statique par l'administrateur réseau sur le point d'accès et sur tous les clients qui communiquent avec celui-ci. L'administrateur réseau qui utilise les clés WEP statiques doit s'atteler à une longue et pénible tâche : entrer les mêmes clés sur chaque unité du WLAN.

Si quelqu'un trouve une unité à clé WEP statique, ou s'il la vole, il peut accéder au réseau WLAN. L'administrateur sera incapable de savoir qu'un utilisateur non autorisé a infiltré son réseau tant que la disparition de l'unité ne lui aura pas été signalée. Il lui faudra alors changer les clés WEP de toutes les unités qui se servent de cette même clé statique. Sur un grand réseau WLAN d'entreprise, servant des centaines voire des milliers d'utilisateurs, c'est une tâche impressionnante. Pire encore, si le pirate parvient à déchiffrer la clé WEP statique – à l'aide d'un outil comme AirSnort – l'administrateur ne pourra jamais deviner qu'un intrus a pénétré ses défenses.

WEP

Les différentes normes 802.11 définissent WEP comme un simple mécanisme destiné à protéger les transmissions aériennes entre les points d'accès du WLAN et les cartes réseaux. WEP, qui s'exécute au niveau de la couche liaison de données, exige que toutes les parties en communication partagent la même clé secrète. Pour éviter d'enfreindre la réglementation américaine sur les exportations en vigueur au moment où la norme était en cours de développement, IEEE 802.11b exigeait des clés de 40 bits, bien que de nombreux constructeurs proposent désormais la version 128 bits en option. Dans ses deux variantes – 40 et 128 bits – WEP peut facilement être piraté avec des outils tout prêts, aisément disponibles sur Internet. Sur un réseau actif, 15 minutes suffisent pour obtenir des clés WEP statiques à 128 bits, selon les estimations actuelles. Les paragraphes suivants décrivent plus en détail ce type d'attaques.

Comme nous l'avons dit dans notre introduction sur les réseau WLAN (annexe B), le cryptage WEP utilise le chiffrement continu RC4 inventé par Ron Rivest de RSA Data Security, Inc. (RSADSI). L'algorithme de cryptage RC4 est un chiffrement en continu symétrique qui supporte les clés de longueur variable. La norme IEEE 802.11 décrit l'utilisation de l'algorithme et des clés RC4 dans WEP, mais ne précise aucune méthode particulière pour la distribution des clés. En l'absence de méthode automatisée de distribution des clés, tout protocole de cryptage se heurte à des problèmes de mise en œuvre en raison du potentiel d'erreur humaine dans la saisie, le dépôt et la gestion des clés. Comme nous en parlerons par la suite, le 802.1X a été ratifié par l'IEEE (Institute of Electrical and Electronics Engineers) et la communauté des fournisseurs d'équipements WLAN est en train de l'adopter comme une solution possible à ce problème de distribution.

Le vecteur d'initialisation est au centre de la plupart des problèmes concernant WEP car il est transmis en clair et placé dans l'en-tête 802.11 : toute personne qui surveille le WLAN peut le voir. D'une longueur de 24 bits, le vecteur d'initialisation peut prendre 16 777 216 valeurs possibles. Un article de l'Université de Californie à Berkeley montre que lorsque le même vecteur d'initialisation est utilisé avec la même clé sur un paquet crypté (ce que l'on appelle une collision de vecteur d'initialisation), un pirate peut capturer les trames de données et en tirer des renseignements sur les données comme sur le réseau. Cet article est disponible en ligne à l'adresse :

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Au cours de l'année passée, les analystes cryptographiques de l'Université de Californie à Berkeley, de l'Université du Maryland et de Cisco Systems, Inc. ont signalé des faiblesses dans les dispositifs d'authentification et de cryptage WEP de la norme WLAN IEEE 802.11. Ces chercheurs ont recommandé l'utilisation de solutions élaborées de gestion des clés pour parer à ces carences. Vous trouverez l'article de l'Université du Maryland à l'adresse :

http://www.cs.umd.edu/~waa/wireless.pdf

Les cryptoanalystes Fluhrer, Mantin et Shamir (FMS) ont découvert des faiblesses inhérentes à l'algorithme RC4 de programmation des clés. Or l'algorithme RC4 utilisé par WEP se sert d'un vecteur d'initialisation de 24 bits et ne renouvelle pas les clés de cryptage de manière dynamique. Fluhrer, Mantin et Shamir ont pu montrer que ces faiblesses pouvaient avoir des applications pratiques dans le décryptage des trames 802.11 qui utilisent WEP. L'attaque présentée dans l'article se concentre sur une classe élargie de vecteurs d'initialisation faibles qui peuvent être générés par RC4 et met en évidence les méthodes qui permettent de « casser » la clé en utilisant certaines formes récurrentes des vecteurs d'initialisation. L'attaque – appelée attaque FMS dans l'article – est pragmatique, mais le plus déconcertant est qu'elle est totalement passive. L'attaque FMS présente la dérivation théorique d'une clé WEP sur un éventail de paquets – entre 100 000 et 1 000 000 – cryptés avec la même clé. Pour plus de détails, lisez l'article à l'adresse :

http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

De récentes mises en œuvre pratiques de l'attaque FMS ont pu extraire la clé WEP statique en saisissant environ un million de paquets, comme le montre un article de AT&T Labs et Rice University, que vous pouvez consulter à l'adresse suivante :

http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Plusieurs développeurs indépendants ont alors créé leurs propres versions de l'attaque FMS ; la plus répandue est AirSnort, disponible sur :

http://airsnort.sourceforge.net/

Bien que cette sécurité WLAN classique – qui repose sur les clés ouvertes ou partagées et sur les clés WEP statiques – soit toujours meilleure que l'absence complète de protection, l'entreprise ne peut s'en contenter. Les très petites sociétés, ou celles qui ne confient pas leurs données vitales aux réseaux WLAN, peuvent se satisfaire de ces modes de sécurisation. Toutes les autres doivent investir dans une solution de sécurité WLAN robuste et de qualité entreprise.

Extensions de sécurité : une nécessité

Cisco reconnaît le bien-fondé des résultats publiés dans les articles cités plus haut et recommande de déployer les éléments des trois technologies décrites ci-dessous en remplacement de la solution WEP préconisée par la norme IEEE 802.11. Les technologies dont il est question comprennent le cryptage IPsec (IP security) de la couche réseau, une méthode de distribution des clés à authentification mutuelle appuyée sur la norme 802.1X, ainsi que plusieurs améliorations propriétaires du protocole WEP et récemment mises en œuvre par Cisco. De plus, le groupe de travail IEEE 802.11 "i" et la commission Wi-Fi Alliance pour les tests de conformité se penchent actuellement sur la normalisation des améliorations de l'authentification et du cryptage WLAN.

IPsec

IPsec est un cadre de normes ouvertes pour assurer la sécurité des communications privées sur les réseaux IP. Les VPN IPsec utilisent les services définis dans IPsec pour garantir la confidentialité, l'intégrité et l'authenticité des communications de données sur les réseaux publics comme Internet. L'une des autres applications pratiques d'IPsec est la protection des réseaux WLAN en cryptant les textes en clair du trafic 802.11 sans fil.

Pour déployer une solution IPsec dans un environnement WLAN, il faut placer un client IPsec sur chaque PC connecté au réseau sans fil ; l'utilisateur doit alors établir un tunnel IPsec pour acheminer le trafic à destination du réseau filaire. Des filtres permettent d'éviter que le trafic sans fil atteigne une autre destination que la passerelle VPN et le protocole DHCP (Dynamic Host Configuration Protocol) ou le serveur DNS (Domain Name System). IPsec assure la confidentialité du trafic IP et offre également des fonctions d'authentification et de protection contre les réémissions. La confidentialité est obtenue par cryptage à l'aide d'une variante de la norme DES (Data Encryption Standard) appelée

3DES (Triple DES) ou encore de la norme AES (Advanced Encryption Standard).

Bien qu'IPsec soit essentiellement destinée à assurer la confidentialité des données et l'authentification des unités, plusieurs extensions de cette norme permettent de réaliser l'authentification et l'autorisation des utilisateurs dans le cadre du processus IPsec. Pour plus d'informations sur IPsec, consulter l'introduction sur les VPN dans l'article SAFE VPN disponible à l'adresse suivante :

http://www.cisco.com/go/safe

802.1X/EAP

Une autre approche de la sécurisation des réseaux WLAN met l'accent sur le développement d'un cadre d'authentification centralisée et de distribution dynamique des clés. Cette approche repose sur le cadre de bout en bout élaboré par le groupe de travail IEEE 802.11 "i" qui exploite les fonctionnalités du 802.1X et du protocole EAP (Extensible Authentication Protocol). Cisco a intégré le 802.1X et le protocole EAP dans sa solution de sécurité pour les réseaux WLAN intitulée Cisco Wireless Security Suite. Les trois principaux éléments d'une démarche 802.1X et EAP sont les suivantes :

- l'authentification mutuelle entre le client et le serveur d'authentification RADIUS (Remote Access Dial-In User Service),
- la dérivation dynamique des clés de cryptage après l'authentification,
- un contrôle centralisé des politiques où l'expiration du temps de session imparti déclenche une nouvelle procédure d'authentification et la génération d'une nouvelle clé.

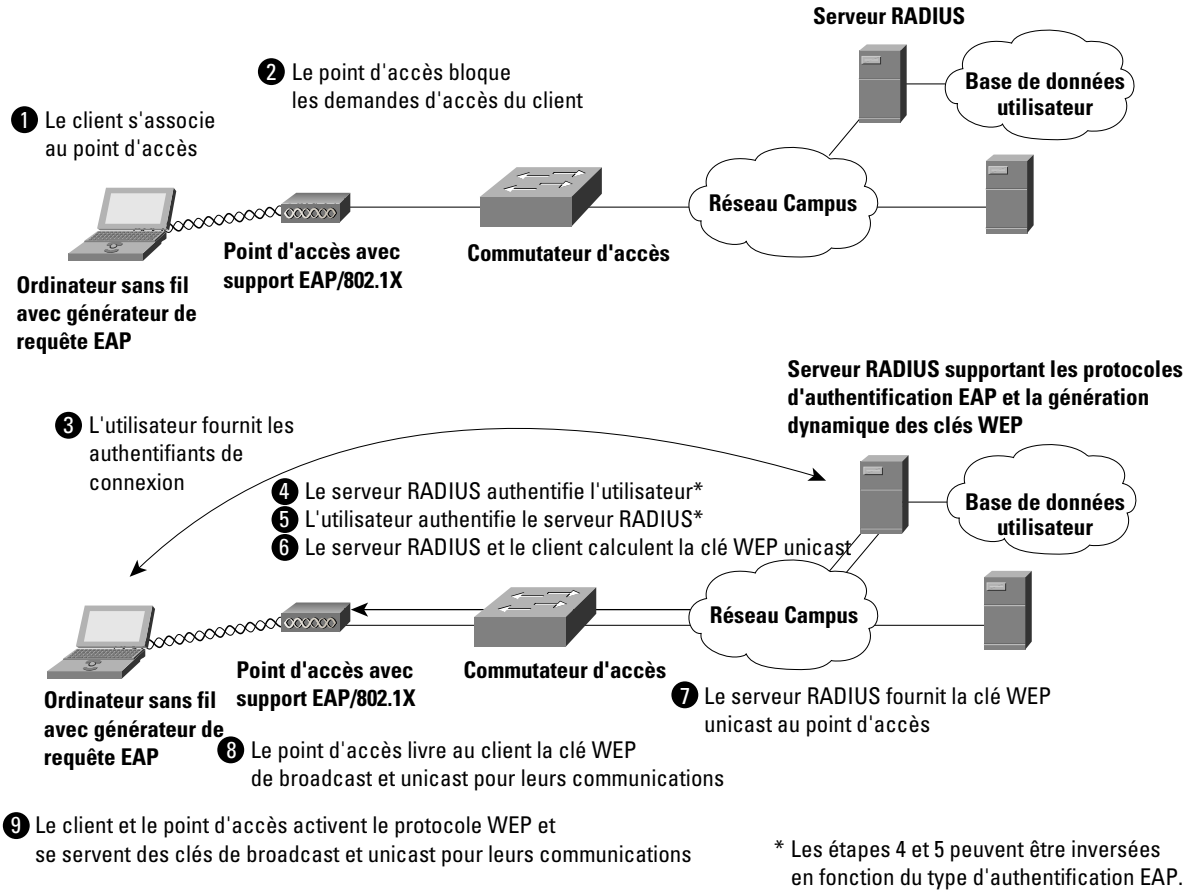
Lorsque ces fonctionnalités sont mises en oeuvre, un client sans fil qui s'associe à un point d'accès ne peut accéder au réseau avant que l'utilisateur réalise une connexion au réseau. Une fois l'association réalisée, le client et le réseau (point d'accès ou serveur RADIUS) échangent des messages EAP pour s'authentifier mutuellement : le client vérifie l'authentifiant du serveur RADIUS et inversement. L'ordinateur client utilise un générateur de requêtes EAP pour obtenir l'authentifiant de l'utilisateur (nom d'utilisateur et mot de passe, nom d'utilisateur et mot de passe de sessionunique [MPSOTP – One Time Password], ou certificat numérique). Lorsque le client et le serveur se sont authentifiés avec succès, le serveur RADIUS et le client calculent une clé WEP spécifique qui sera utilisée par le client pour la connexion réseau en cours. Les mots de passe utilisateurs et les clés de session ne sont jamais transmis en clair sur la liaison sans fil.

Les événements s'enchaînent de la manière suivante (voir la Figure 1) :

- le client sans fil s'associe au point d'accès ;
- le point d'accès empêche le client d'obtenir un accès aux ressources du réseau jusqu'à ce qu'il ait ouvert une session ;
- l'utilisateur sur le client fournit au réseau ses authentifiants de session (nom d'utilisateur et mot de passe, nom d'utilisateur et mot de passe de sessionunique (MPSOTP – One Time Password) ou certificat numérique) par l'intermédiaire d'un générateur de requêtes EAP ;
- en utilisant les protocoles 802.1X et EAP, le client sans fil et un serveur RADIUS du réseau LAN filaire s'authentifient mutuellement par l'intermédiaire du point d'accès. Cette authentification mutuelle se déroule en deux phases : au cours de la première phase de l'authentification EAP, le serveur RADIUS vérifie les authentifiants du client ou l'inverse. Au cours de la deuxième phase, le client vérifie les authentifiants du serveur RADIUS, ou l'inverse ;
- lorsque l'authentification s'achève avec succès, le serveur RADIUS et le client déterminent une clé WEP spécifique au client. Le client charge cette clé et se prépare à l'utiliser pour la session de connexion ;
- le serveur RADIUS envoie la clé WEP, appelée clé de session, au point d'accès sur le LAN filaire ;
- le point d'accès crypte sa clé de transmission broadcast avec la clé de session et envoie la clé cryptée au client qui utilise la clé de session pour la décrypter ;
- le client et le point d'accès activent le protocole WEP et utilisent les clés de session et de transmission broadcast pour toutes leurs communications pendant le reste de la session ou jusqu'à ce que le délai soit dépassé – dans ce cas de nouvelles clés WEP sont générées ;

les clés de session et de transmission broadcast sont modifiées à intervalles réguliers. A la fin de la phase d'authentification EAP, le serveur RADIUS précise au point d'accès le délai d'expiration de la clé de session tandis que la fréquence de renouvellement de la clé de transmission broadcast peut être configurée sur le point d'accès.

Figure 1
Processus d'authentification EAP



EAP offre trois avantages majeurs par rapport à la sécurité 802.11 de base :

- le premier est la procédure d'authentification mutuelle que nous venons de décrire et qui contre efficacement les « attaques par l'intermédiaire » (« man-in-the-middle ») réalisées à l'aide de points d'accès ou de serveurs RADIUS illégaux ;
- le deuxième est la gestion et la distribution centralisées des clés de cryptage. Même si la mise en œuvre WEP de RC4 était sdans faille, la distribution des clés statiques à tous les points d'accès et à tous les clients du réseau constituerait encore une sérieuse pénalité administrative : si un utilisateur égarait une unité sans fil, il faudrait que toutes les clés du réseau soient renouvelées pour éviter que cette unité puisse accéder de manière illégale au réseau ;
- le troisième avantage est la possibilité de définir un contrôle centralisé des politiques avec des délais d'expiration de session entraînant une nouvelle authentification et la génération de nouvelles clés.

Les protocoles d'authentification EAP

De nombreux types de protocoles EAP sont aujourd'hui disponibles pour réaliser l'authentification d'identité sur les réseaux filaires et sans fil. Voici les plus courants :

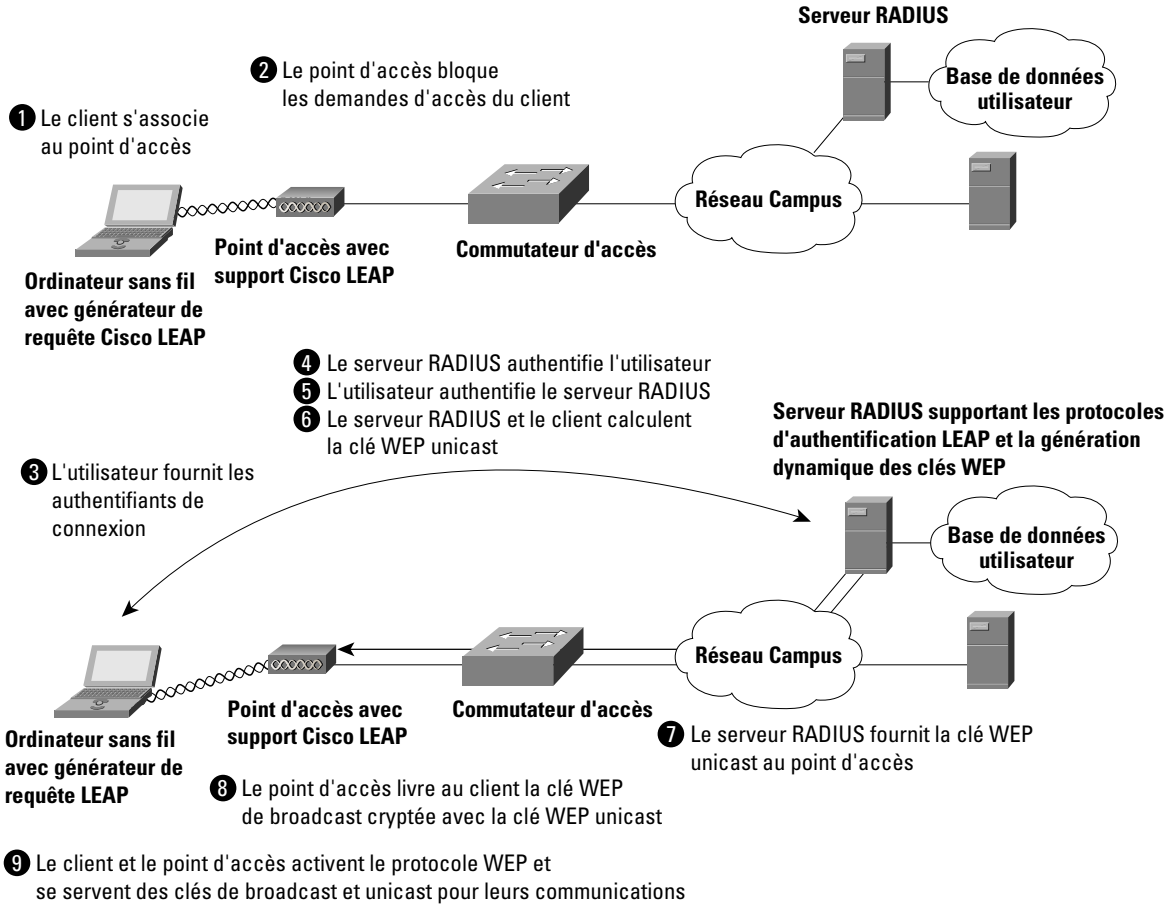
- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunnelled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Les protocoles d'authentification mutuelle LEAP, EAP-TLS et PEAP ont été testés dans le cadre de l'architecture Cisco SAFE WLAN, et ont prouvé qu'ils étaient adaptés au déploiement des WLAN.

Cisco LEAP

Cisco LEAP est le type de protocole EAP largement déployé actuellement dans les réseaux WLAN. LEAP supporte les trois éléments de la démarche 802.1X / EAP précédemment mentionnée. Avec LEAP, l'authentification mutuelle repose sur un secret partagé – le mot de passe de connexion de l'utilisateur, qui n'est connu que du client et du réseau. Comme le montre la Figure 2, le serveur RADIUS envoie au client un test d'authentification. Le client utilise un algorithme de hachage à sens unique sur le mot de passe fourni par l'utilisateur pour générer une réponse au test avant d'envoyer cette réponse au serveur RADIUS. A partir des informations de sa base de données utilisateurs, le serveur RADIUS crée sa propre réponse et la compare à celle du client. Lorsque le serveur RADIUS a authentifié le client, le processus recommence dans l'autre sens pour permettre au client d'authentifier le serveur RADIUS. Une fois les deux processus achevés, le client reçoit un message de confirmation EAP-Success du serveur RADIUS et tous deux génèrent la clé WEP dynamique.

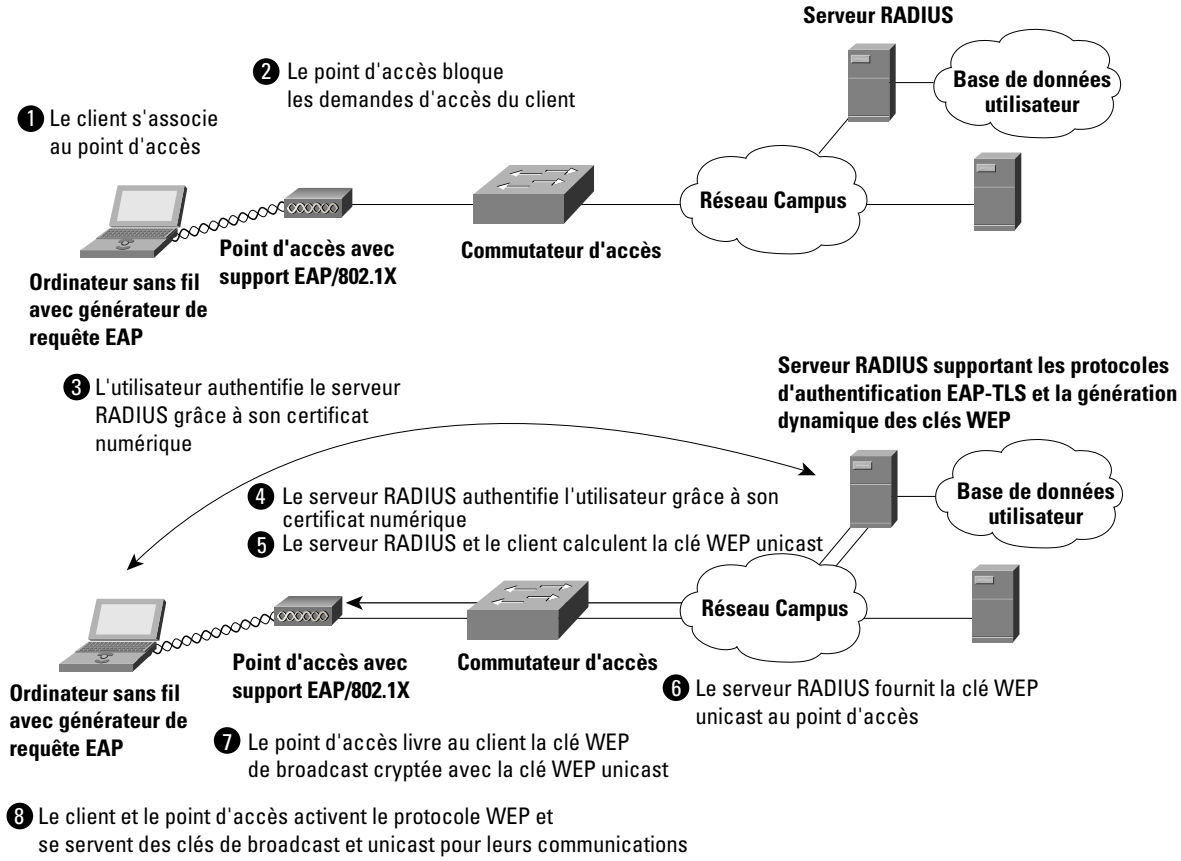
Figure 2
Processus d'authentification LEAP



EAP-TLS

EAP-TLS est une norme de l'IETF (Internet Engineering Task Force) (RFC 2716) appuyée sur le protocole TLS (RFC 2246). EAP-TLS utilise des certificats numériques pour authentifier l'utilisateur et le serveur et supporte les trois éléments clés de la démarche 802.1X/EAP décrite ci-dessus. Comme le montre la Figure 3, le serveur RADIUS envoie son certificat au client au cours de la phase 1 de la séquence d'authentification (TLS côté serveur). Le client valide le certificat du serveur RADIUS en vérifiant l'émetteur du certificat – une entité serveur de certificats – et le contenu du certificat numérique. Ceci fait, le client envoie son certificat au serveur RADIUS au cours de la phase 2 de la séquence d'authentification (TLS côté client). Le serveur RADIUS valide le certificat du client en vérifiant l'émetteur du certificat et le contenu de celui-ci. Une fois les deux processus achevés, le client reçoit un message de confirmation EAP-Success du serveur RADIUS et tous deux génèrent la clé WEP dynamique.

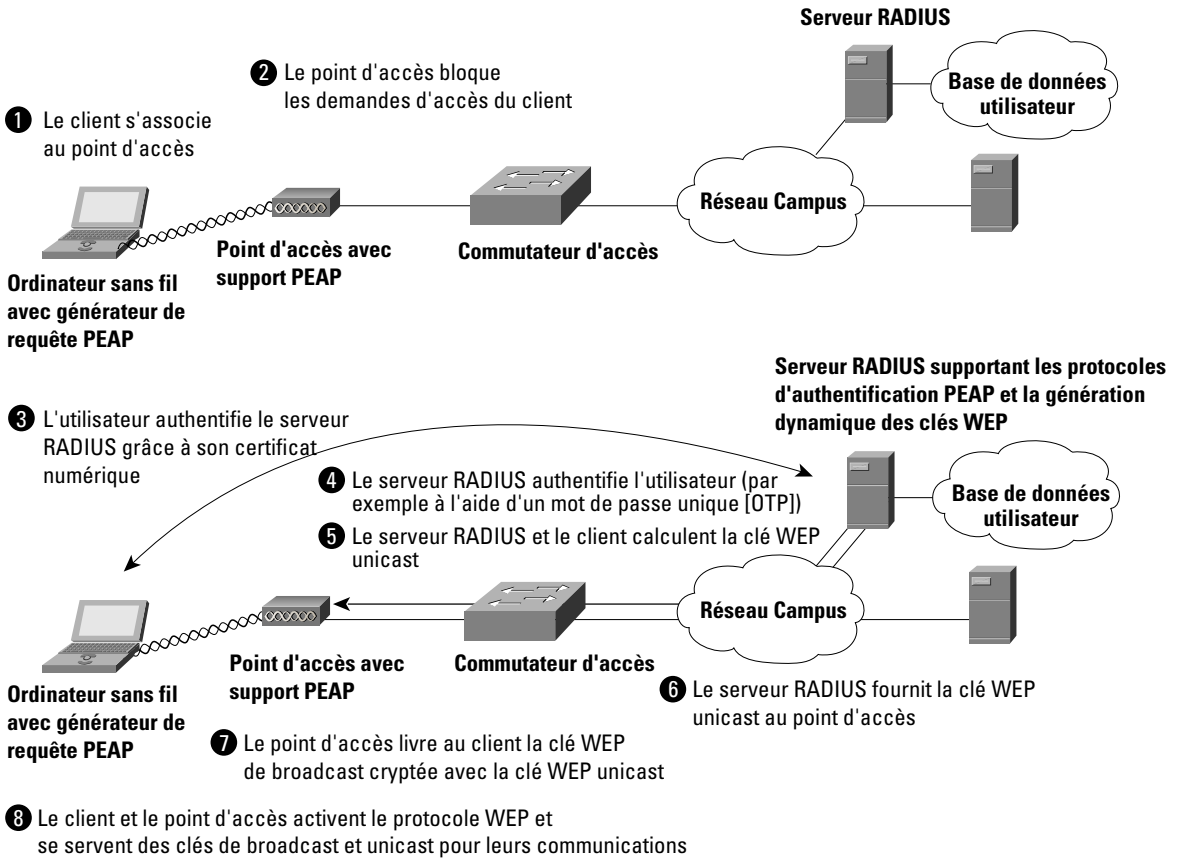
Figure 3
Processus d'authentification EAP-TLS



PEAP

PEAP est un projet de RFC de l'IETF réalisé par Cisco Systems, Microsoft et RSA Security. PEAP utilise un certificat numérique pour l'authentification du serveur. Pour l'authentification utilisateur, PEAP supporte diverses méthodes d'encapsulation EAP au sein d'un tunnel TLS protégé. PEAP supporte les trois éléments de la démarche 802.1X / EAP précédemment mentionnée. Comme le montre la Figure 4, la phase 1 de la séquence d'authentification est identique à celle d'EAP-TLS (TLS côté serveur). A la fin de la phase 1, un tunnel TLS crypté est établi entre l'utilisateur et le serveur RADIUS pour le transport des messages d'authentification EAP. Dans la phase 2, le serveur RADIUS authentifie le client par le tunnel TLS crypté grâce à un autre type d'EAP. Par exemple, l'authentification utilisateur peut faire intervenir un mot de passe de sessionunique (MPSOTP) utilisant le sous-type EAP-GTC (défini par le projet PEAP). Dans ce cas, le serveur RADIUS relaie les authentifiants de session (nom d'utilisateur et mot de passe de sessionunique) à un serveur spécialisé qui valide la connexion. Une fois les deux processus achevés, le client reçoit un message de confirmation EAP-Success du serveur RADIUS et tous deux génèrent la clé WEP dynamique. Pour plus d'informations sur PEAP, visitez le site Web de l'IETF Web qui contient les versions les plus récentes du projet.

Figure 4
Processus d'authentification PEAP



Pour des informations plus détaillées sur les protocoles EAP, les caractéristiques de mise en œuvre et des principes de déploiement sur les réseaux WLAN, consulter :

http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml/

Les améliorations du protocole WEP

Des améliorations sont nécessaires pour limiter les faiblesses du protocole que nous avons désignées dans notre section axiomatique « La norme 802.11 n'est pas sécurisée ». Le projet de norme IEEE 802.11i présente deux améliorations en termes de cryptographie :

1. le protocole TKIP (Temporal Key Integrity Protocol) qui est un ensemble d'améliorations logicielles du protocole WEP RC4,
2. AES, qui remplace RC4 en étant plus efficace.

En décembre 2001, Cisco a intégré le support TKIP dans Cisco Wireless Security Suite. Comme la norme TKIP n'était pas encore finalisée à cette date, sa mise en œuvre est une forme pré-normalisée et parfois désignée sous le nom de Cisco TKIP. En 2002, l'IEEE achevait la spécification TKIP pour la norme 802.11i et Wi-Fi Alliance annonçait qu'il intégrait TKIP dans WPA (Wi-Fi Protected Access), qui deviendra une exigence de conformité Wi-Fi avant la fin 2003.

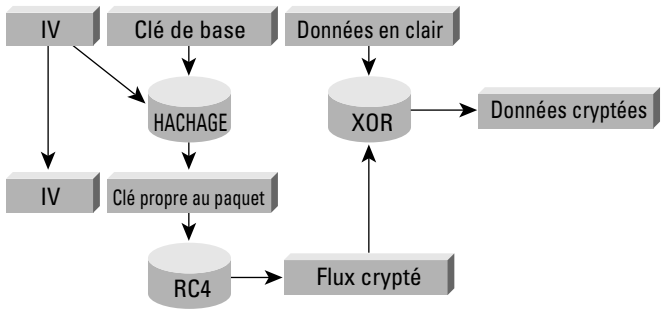
La version entreprise de WPA exige également 802.1X pour le 802.11. Cisco TKIP et WPA TKIP adoptent l'attribution de clé par paquet (PPK : per-packet keying) et le code MIC (Message Integrity Check). WPA TKIP introduit un troisième élément : l'allongement du vecteur d'initialisation de 24 à 48 bits. Cette section décrit les caractéristiques de la version Cisco TKIP qui mettent en évidence l'amélioration de la sécurité apportée par TKIP. Pour plus d'informations sur WPA, visitez le site Web WECA :

http://www.weca.net

Cisco TKIP : l'attribution de clés par paquet

Les attaques les plus fréquentces subies par le protocole WEP exploitent la faiblesse des vecteurs d'initialisation transmis dans un flux de trafic crypté avec la même clé : pour atténuer cette menace, on peut envisager d'utiliser des clés différentes selon les paquets. La Figure 5 montre comment le vecteur d'initialisation et la clé WEP sont soumis à un algorithme de hachage pour produire une clé spécifique au paquet – ce que l'on appelle une clé temporelle. Celle-ci est ensuite combinée au vecteur d'initialisation avant d'être traitée par une fonction mathématique appelée XOR en même temps que le texte en clair. La méthode 802.11 standard de cryptographie RC4 pour les clés WEP est décrite dans l'introduction aux WLAN (Annexe B).

Figure 5
Hachage de la clé WEP par paquet



Ce scénario évite qu'un pirate puisse se servir de la faiblesse des vecteurs d'initialisation pour en déduire la clé WEP de base car : avec cette méthode, il ne peut calculer que la clé WEP propre au paquet. Pour éviter les attaques dues aux collisions de vecteurs d'initialisation, la clé de base doit être modifiée avant la répétition des vecteurs d'initialisation. Sur un réseau très actif, cette répétition peut intervenir en quelques heures et il convient d'utiliser des mécanismes comme les protocoles d'authentification EAP pour le renouvellement des clés.
Comme la clé unicast, la clé de transmission broadcast WLAN – utilisée par les points d'accès et les clients pour les transmissions de couche 2 et les communications multicast – est sensible aux attaques liées aux collisions de vecteurs d'initialisation. Les points d'accès Cisco supportent la rotation des clés de transmission broadcast pour réduire cette vulnérabilité. Le point d'accès calcule de manière dynamique la clé WEP de transmission broadcast – à partir d'un nombre aléatoire – et envoie aux clients la nouvelle clé WEP de transmission broadcast dans un message EAPOL-Key. Ainsi, la rotation des clés WEP transmission de broadcast n'est possible qu'avec des protocoles EAP comme LEAP, EAP-TLS et PEAP, qui supportent le calcul dynamique des clés de cryptage.

Cisco TKIP – Le code d'intégrité des messages (MIC)

L'autre problème majeur posé par le protocole WEP est sa vulnérabilité aux attaques par réémission. Le code MIC protège les trames WEP contre toute altération. Le code MIC est calculé à partir d'une valeur initiale, de l'adresse MAC de destination, de l'adresse MAC source et de la longueur du texte : toute modification de ces valeurs génère un nouveau code MIC. De plus, le code MIC est inclus dans le texte crypté par WEP. La valeur du code MIC est obtenue à partir d'un algorithme de hachage – une nette amélioration par rapport à la fonction de somme de contrôle CRC (Cyclic Redundancy Check)-32 exécutée par le protocole WEP normalisé. Avec CRC-32, il est « possible de calculer la

différence en bits de deux sommes de contrôle CRC en fonction de la différence en bits des messages sur lesquels elles sont prélevées. En d'autres termes, l'inversion du bit n dans le message entraîne de manière déterministe l'inversion d'un certain nombre de bits du CRC pour produire une somme de contrôle correcte sur le message modifié. Comme l'inversion de bits est conservée au cours du décryptage RC4, l'agresseur peut inverser arbitrairement un certain nombre de bits dans le message crypté et ajuster la somme de contrôle pour constituer un message d'apparence valide.»

En résumé

Les organisations ont le choix entre déployer soit IPsec, soit 802.1X/EAP avec TKIP ou encore Cisco TKIP, mais généralement pas les deux. Des architectures spécifiques utilisant les deux en même temps ont été testées dans le laboratoire SAFE : elles sont présentées dans les sections « Solutions alternatives » correspondantes. L'entreprise doit choisir IPsec lorsque la confidentialité des données transportées est de la plus haute importance. Il faut toutefois rappeler que cette solution est plus complexe à déployer et à administrer que 802.1X/EAP avec TKIP. 802.1X/EAP avec TKIP convient aux entreprises qui souhaitent garantir une confidentialité raisonnable en offrant à leurs utilisateurs une sécurité transparente. Les améliorations apportées au protocole WEP de base peuvent être mises en œuvre partout où WEP est implanté. Pour la grande majorité des réseaux, la sécurité fournie par 802.1X/EAP avec TKIP est suffisante. Le Tableau 1 donne une description détaillée des avantages et des inconvénients d'IPsec et des protocoles d'authentification EAP dans les architectures de WLAN :

Tableau 1 Comparatif des technologies de cryptage sans fil

	Cisco LEAP avec TKIP	EAP-TLS avec TKIP	EAP-PEAP avec TKIP	IPsec-based VPN IPsec
Longueur des clés (en bits)	128	128	128	168/128, 192, 256
Algorithme de cryptage	RC4	RC4	RC4	3DES ou AES
Intégrité des paquets	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/ SHA-HMAC
Authentification serveur	Non	Certificat	Non	Secret partagé ou certificats
Authentification utilisateur	Nom d'utilisateur mot de passe	Certificat	Nom d'utilisateur / mot de passe ou mot passe unique (OTP)	Nom d'utilisateur / mot de passe ou de passe unique
Certificats exigés	Aucun	Serveur RADIUS / client WLAN	Serveur RADIUS	En option
Différentiation des utilisateurs 1	Groupe	Groupe	Groupe	Utilisateur
Signature unique	Oui	Oui	Non	Non
Liste de contrôle d'accès	En option	En option	En option	Exigée
Matériel supplémentaire	Non	Serveur de certificats	Serveur de certificats	Concentrateur IPsec
Attribution de clés par utilisateur	Oui	Oui	Oui	Oui
Protocoles supportés	Tous	Tous	Tous	IP unicast
Support des systèmes d'exploitation clients	Large gamme	Large gamme	Large gamme	Large gamme
Norme ouverte	Non	Oui	Projet de RFC IETF	Oui

1. La différenciation des utilisateurs fait l'objet d'une discussion dans la section « Différentiation des utilisateurs du réseau WLAN », ci dessous.

La disponibilité du réseau a une incidence sur le sans fil

L'architecte réseau soucieux de concevoir et de mettre en œuvre des réseaux sans fil à haute disponibilité doit tenir compte dans ses projets des éléments filaires et sans fil. Dans le cadre de Cisco SAFE WLAN, le présent livre blanc ne s'intéresse qu'aux exigences de disponibilité des éléments de réseau qui fournissent les services en relation avec la sécurité. Trois services sont plus particulièrement concernés par ces questions de disponibilité :

- DHCP
- RADIUS
- IPsec

L'annexe D « Disponibilité réseau », aborde ce sujet plus en détail.

Différentiation des utilisateurs du réseau WLAN

Les réseaux filaires permettent souvent de regrouper les utilisateurs par communauté grâce à la segmentation de couche 3. L'architecture SAFE Entreprise, par exemple, prévoit une séparation entre le segment marketing et le segment Recherche et Développement. Cette segmentation intervient au niveau du module de distribution, qui est le premier point de la couche 3 du réseau pour la communauté des utilisateurs. Dans le reste de l'architecture SAFE Entreprise, elle peut être maintenue par un filtrage sur l'adresse IP utilisée par les différentes communautés d'utilisateurs pour accéder au réseau. De surcroît, ce type de segmentation peut se révéler complexe à administrer car les séparations fonctionnelles et physiques sont généralement deux choses distinctes. Par exemple, un contrôleur financier qui doit pouvoir accéder aux systèmes comptables de l'organisation peut être installé à côté d'un poste réservé aux visiteurs de passage et qui ne fournit donc que des services de base.

De même que celle du monde filaire, la différentiation utilisateur sans fil peut être réalisée par l'intermédiaire de réseaux locaux virtuels (VLAN) sans fil associés aux VLAN filaires. Le déploiement mixte de normes de sécurité (802.1X/EAP et VPN IPsec) s'effectue par des VLAN multiples, chacun d'eux supportant une architecture de sécurité spécifique. Un réseau VLAN sans fil est identifié de manière unique par un identificateur SSID et associé à une identification de VLAN filaire. Dans notre précédent exemple, le contrôleur financier et le visiteur utilisent des identificateurs SSID différents pour accéder au réseau. Chaque identificateur SSID est associé à un unique identificateur VLAN. De plus, le serveur RADIUS permet de mettre en œuvre des mécanismes de contrôle d'accès au réseau VLAN. Le point d'accès peut, par exemple, associer de manière dynamique le contrôleur financier à un identificateur VLAN renvoyé par le serveur RADIUS une fois l'authentification 802.1X/EAP achevée avec succès. Par ailleurs, la création de VLAN sur le point d'accès permet à l'entreprise de séparer le trafic de gestion du point d'accès du trafic utilisateur normal. L'annexe A présente un exemple de mise en œuvre de différentiation utilisateur (sur les groupes utilisateurs Ingénierie et R&D) dans l'architecture EAP d'entreprise. Pour plus d'informations sur la mise en œuvre des VLAN sur les plates-formes sans fil Cisco, consultez le « Wireless VLAN Deployment Guide » sur Cisco.com :

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

En l'absence de VLAN sans fil, les VPN IPsec peuvent servir à attribuer des privilèges de groupes utilisateurs. En exigeant des utilisateurs qu'ils exécutent un client VPN sur leurs hôtes finals, le réseau sans fil peut servir exclusivement au transit et laisser le VPN gérer tous les contrôles de sécurité. Cette architecture est présentée en détail dans la suite de ce document.

Approche architecturale

Cisco SAFE WLAN répond aux préoccupations générales de sécurité des WLAN comme nous l'avons développé dans notre section axiomatique. Cette section « architecturale » reprend les problèmes et les techniques de limitation des risques développés dans la section axiomatique pour les appliquer à un éventail diversifié de réseaux. La taille du réseau WLAN projeté et les problèmes de sécurité qui lui sont spécifiques imposent les techniques de limitation des risques à lui appliquer. L'architecte réseau est ainsi amené à choisir entre différentes technologies de limitation des risques, chacune avec les avantages et les inconvénients des technologies propres à l'architecture SAFE. Ces technologies de limitation des risques sont cohérentes d'une architecture SAFE à une autre, et nous commencerons donc par présenter les éléments de mise en réseau de chacune des deux principales options technologiques. Après avoir analysé ces technologies, l'architecte réseau doit étudier chaque architecture SAFE ainsi que les avantages et les inconvénients associés à la mise en place des technologies spécifiques de limitation des risques au sein de l'architecture SAFE. Nous présentons également les caractéristiques propres à la mise en œuvre des technologies de limitation des risques au sein des architectures SAFE. Les deux principaux choix architecturaux sont :

- la mise en œuvre d'un modèle à clé WEP dynamique avec 802.1X/EAP et TKIP
- la mise en œuvre d'un réseau VPN de recouvrement avec IPsec

Principes directeurs pour une architecture WLAN standard

Cette section décrit les éléments génériques des architectures WLAN car un très grand nombre d'entre eux sont communs à l'ensemble des architectures SAFE. Après avoir lu cette section, vous pourrez passer au concept de réseau WLAN qui vous intéresse le plus. Ce découpage permet de présenter les concepts de base en une seule fois et d'étudier les spécificités et les autres solutions possibles dans chacune des architectures SAFE. Dans l'architecture WLAN standard, on suppose que tous les équipements WLAN sont connectés à un unique sous-réseau IP qui permet la mobilité de l'utilisateur final. De plus, la plupart des services disponibles sur le réseau filaire le sont aussi pour l'extension sans fil. Chaque architecture comprend les principes de sécurité WLAN suivants :

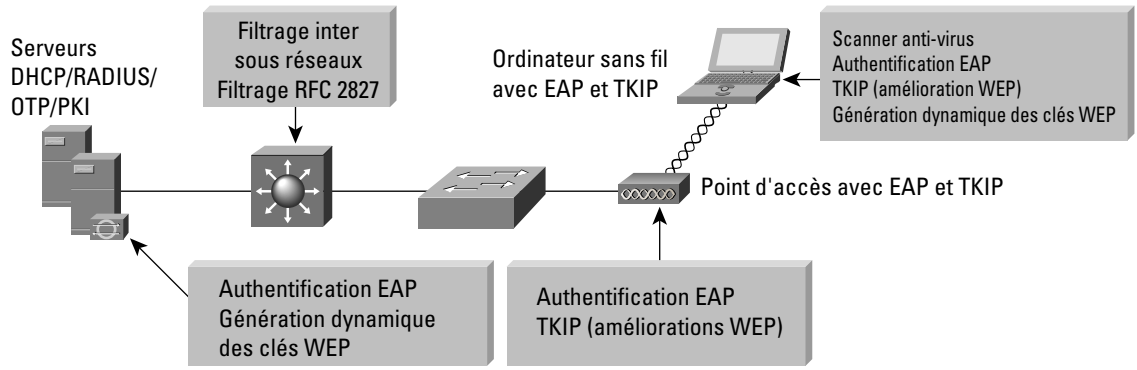
- Recommandations sur la sécurité des points d'accès :
  - activez l'authentification utilisateur centralisée (RADIUS, TACACS+) pour l'interface d'administration,
  - choisissez des identifiants de communauté forts pour le protocole SNMP (Simple Network Management Protocol) et changez-les souvent,
  - envisagez le recours au protocole SNMP Read Only si votre infrastructure d'administration le permet,
  - désactivez tous les protocoles d'administration non sécurisés et non indispensables fournis par le constructeur,
  - utilisez des protocoles d'administration sécurisés comme SSH (Secure Shell Protocol),
  - limitez le trafic d'administration à un sous-réseau filaire dédié,
  - isolez le trafic d'administration du trafic utilisateur et cryptez le trafic d'administration chaque fois que cela est possible,
  - activez le cryptage des trames sans fil si cela est possible,
  - assurez la sécurité matérielle du point d'accès.
- Recommandations de sécurité client :
  - désactivez le mode ad hoc,
  - activez le cryptage des trames sans fil si cela est possible,

Architecture standard de réseau WLAN EAP avec TKIP

Cette architecture décrit une méthode générique pour l'utilisation d'EAP avec TKIP en tant que mécanisme de sécurité pour l'accès au réseau productif de l'entreprise (voir la Figure 6).

Figure 6

Rôles de limitation des risques d'attaques dans un architecture standard de WLAN EAP



Principales unités EAP

- *Carte et logiciel client sans fil* – Cette solution fournit le matériel et le logiciel nécessaires pour les communications sans fil vers le point d'accès ; elle permet l'authentification mutuelle auprès du point d'accès par l'intermédiaire d'un type EAP ; un générateur de requêtes EAP adapté est nécessaire sur l'ordinateur client.
- *Point d'accès sans fil* – Il assure l'authentification mutuelle avec les clients sans fil par l'intermédiaire d'EAP et peut supporter plusieurs réseaux VLAN de couche 2 pour différencier les utilisateurs.
- *Commutateur de couche 2 ou 3* – Ce commutateur fournit une connectivité Ethernet et réalise un filtrage de couche 3 ou 4 entre le point d'accès au WLAN et le réseau d'entreprise.
- *Serveur RADIUS* – Ce serveur assure l'authentification des clients sans fil en fonction de l'utilisateur et authentifie le point d'accès auprès de ceux-ci ; de plus, le serveur RADIUS peut servir à préciser les paramètres de contrôle d'accès aux VLAN pour les utilisateurs et les groupes d'utilisateurs.
- *Serveur DHCP* – Il fournit les informations de configuration IP aux clients LEAP sans fil.
- *Serveur de mot de passe de sessionunique (MPSOTP – One Time Password) (en option)* – Il autorise les informations MPS OTP relayées par le serveur RADIUS (pour les clients PEAP seulement)
- *Serveur PKI (en option)* – Fournit un certificat numérique X.509v3 pour l'identification de l'utilisateur et du serveur

Les risques qu'il est possible de limiter

- *Renifleurs de paquets sans fil* – Les renifleurs de paquets sans fil peuvent tirer parti de n'importe quelle attaque WEP connue pour déduire la clé de cryptage. Les améliorations WEP – et plus particulièrement l'attribution de clé par paquet PPK qui fait partie de TKIP (voir la section « Extensions de sécurité : une nécessité ») – et la rotation des clés avec EAP permettent de limiter les risques associés à cette menace.
- *Accès sans authentification* – Seuls les utilisateurs authentifiés peuvent accéder au réseau sans fil et au réseau filaire. Le contrôle d'accès en option sur le commutateur de couche 3 limite l'accès au réseau filaire.
- *Attaques par l'intermédiaire (« man-in-the-middle »)* – La capacité d'authentification mutuelle de plusieurs types d'authentification EAP associée au code MIC permet d'empêcher les pirates de se placer en intermédiaire des communications sans fil.

- *Usurpation d'identité IP* – Un pirate ne peut usurper une identité IP (« spoofing ») sans commencer par s'authentifier auprès du réseau WLAN. S'il y parvient, le filtrage d'authentification RFC 2827 en option sur le commutateur de couche 3 interdit toute usurpation d'identité dans la zone de couverture du sous-réseau local.
- *Usurpation d'identité auprès du protocole ARP (Address Resolution Protocol)* – Un pirate ne peut usurper une identité ARP sans commencer par s'authentifier auprès du réseau WLAN. S'il y parvient, il peut lancer une attaque de ce type comme dans un environnement filaire pour intercepter les données des autres utilisateurs.
- *Analyse de la topologie du réseau* – Le pirate ne peut analyser la topologie du réseau s'il ne s'est pas authentifié au préalable. Il peut remarquer l'existence d'un réseau WLAN en recherchant ou en observant l'identificateur SSID du point d'accès, mais il ne peut pas accéder ainsi au réseau. S'il parvient à s'authentifier par l'intermédiaire d'EAP, il peut analyser la topologie du réseau de la même manière que dans un environnement filaire.

Les risques qui ne sont pas atténués

- *Attaque sur les mots de passe* – Plusieurs types EAP tiennent compte du fait qu'un pirate peut surveiller de manière passive les échanges 802.1X/EAP entre le client et le point d'accès, et utilisent plusieurs méthodes pour atténuer ce risque. PEAP établit pour cela un tunnel TLS entre le client et le serveur avant de demander les identifiants utilisateurs. De plus, comme EAP-PEAP utilise d'autres types EAP pour l'authentification client – serveur, l'architecte réseau peut choisir de mettre en œuvre une méthode forte d'authentification comme les MPSOTP. EAP-TLS limite cette menace à l'aide du cryptage à clé publique (voir le Tableau 2).

Tableau 2 Limitation des risques de sécurité des WLAN déployés sous EAP/802.1X avec TKIP

Attaque	Cisco LEAP avec TKIP	EAP-TLS avec TKIP	EAP-PEAP (authentification client par MPSOTP) avec TKIP
Attaques (actives) par l'intermédiaire (MITM)	Risque réduit	Risque réduit	Risque réduit
Falsification d'authentification	Risque réduit	Risque réduit	Risque réduit
Attaques passives (attaques FMS)	Risque réduit	Risque réduit	Risque réduit
Points d'accès illégaux	Risque réduit	Risque réduit	Risque réduit
Attaques en force par dictionnaire de mots de passe	Vulnérable[1]	Risque réduit	Risque réduit

1 Une politique de mots de passe forts est recommandée avec LEAP pour contrer les attaques en force par dictionnaire de mots de passe. L'administrateur IT doit également limiter le nombre de tentatives d'ouverture de session et bloquer le compte en cas de dépassement.

Principes directeurs d'architecture EAP avec TKIP

Dans la plupart des cas, les points d'accès au WLAN sont connectés à des commutateurs d'accès de couche 2. Des serveurs RADIUS et DHCP sont installés dans le module de services de réseau du réseau d'entreprise. La sécurité est assurée en empêchant l'accès au réseau des clients non authentifiés, même dans le cas d'une défaillance du service RADIUS. Cette politique est indispensable car l'essentiel de la limitation des risques de sécurité repose sur le service RADIUS. En règle générale, une défaillance des services DHCP gêne l'administration de la solution. Les clients sans fil et les points d'accès authentifient les unités clients WLAN et les utilisateurs finals par l'intermédiaire d'EAP en fonction des données des serveurs RADIUS. Pour des raisons d'évolutivité et de facilité de gestion, le paramétrage des unités clients WLAN reprend le protocole DHCP pour la configuration IP. Le protocole DHCP intervient une fois que l'unité et l'utilisateur final sont correctement authentifiés par l'intermédiaire du protocole EAP. Une fois la configuration DHCP établie, l'utilisateur final sans fil est autorisé à accéder au réseau de l'entreprise et un filtrage intervient, s'il est configuré. L'architecte réseau doit accorder une importance particulière à la détermination de l'emplacement des

serveurs RADIUS et DHCP utilisés par EAP afin de garantir la haute disponibilité des services de réseau pour les utilisateurs de WLAN.

Pour éviter les attaques dues aux collisions des vecteurs d'initialisation, nous recommandons le renouvellement des clés unicast et de transmissionbroadcast. Dans le cas de EAP avec Cisco TKIP, le délai recommandé de renouvellement de ces deux types de clés WEP est de 4 heures et 40 minutes. Pour plus d'informations, consultez les livres blancs à l'adresse :

http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml/

Pour un projet de réseau de grande taille, l'architecte réseau doit tenir compte de la capacité d'évolution du serveur RADIUS et utiliser, par exemple, des outils d'équilibrage de charge serveur pour répartir le travail entre les différents serveurs RADIUS.

Voici quelques principes directeurs propres au protocole EAP :

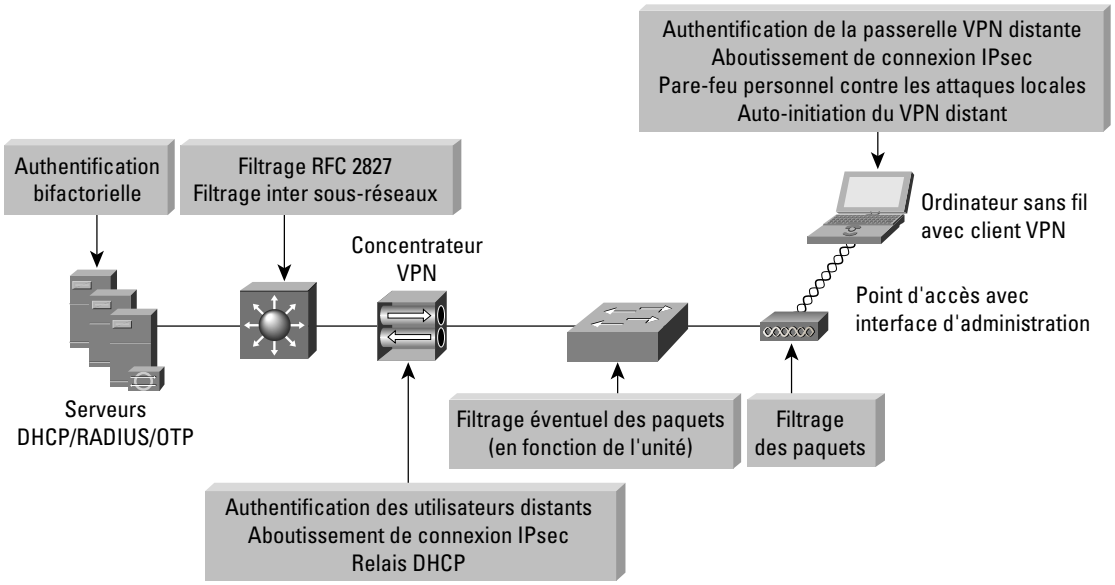
- Avec EAP-TLS, nous recommandons l'utilisation d'une infrastructure PKI privée pour l'émission des certificats numériques, ce qui permet d'intégrer cette infrastructure PKI avec les bases de données utilisateurs d'arrière guichetexternes (par exemple, Microsoft Windows 2000 AD) existantes pour la gestion des certificats.
- Pour EAP-TLS et EAP-PEAP, il est préférable de configurer les clients sans fil avec le certificat numérique du serveur sécurisé de certificats et d'empêcher l'utilisateur courant de modifier ces paramètres. Seul l'administrateur doit disposer des privilèges de modification de ces paramètres sur le générateur de requête EAP du client sans fil. Si le certificat du serveur sécurisé de certificats n'a pas été configuré, le pirate peut, en usurpant une identité, lancer des attaques par l'intermédiaire « man-in-the-middle ».
- Pour EAP-LEAP et EAP-PEAP – avec des mots de passe statiques – nous recommandons de bloquer le compte après un petit nombre de tentatives incorrectes d'ouverture de session, afin d'empêcher les attaques en force sur le compte concerné. Le nombre de tentatives autorisées est précisé sur le serveur RADIUS et nous recommandons également une politique agressive de péremption de ces mots de passe. Le risque en question peut être encore limité en exigeant un mot de passe de sessionunique pour l'authentification client.
- Avec EAP-TLS, nous recommandons de configurer le serveur RADIUS pour vérifier la liste de révocation des certificats de l'autorité de certification afin de déterminer les certificats clients périmés.

Eventuellement, l'architecte réseau peut envisager la mise en œuvre de VLAN sans fil uniques avec l'architecture EAP. Des VLAN dynamiques peuvent être attribués aux utilisateurs EAP qui utilisent le serveur RADIUS et les paramètres des groupes d'utilisateurs. Cette solution présente l'avantage de répartir les utilisateurs sans fil en communautés d'utilisateurs et de faire appliquer les politiques relatives à ces groupes au niveau de la couche de distribution. Les VLAN permettent également d'isoler le trafic d'administration du trafic utilisateur en réalisant des VLAN d'administration sur les points d'accès.

Architecture standard de WLAN avec VPN

Cette architecture décrit une méthode générique pour l'utilisation des VPN IPsec en tant que mécanisme de sécurité pour l'accès au réseau productif de l'entreprise à partir du WLAN (voir la Figure 7).

Figure 7
Rôles de limitation des risques d'attaques dans une architecture standard de WLAN avec VPN



Principales unités VPN

- *Carte client sans fil et logiciel* – Cette solution fournit le matériel et le logiciel nécessaires pour les communications sans fil vers le point d'accès.
- *Client VPN à accès distant avec logiciel pare-feu personnel* – Logiciel client qui réalise des tunnels cryptés de bout en bout entre un PC et les passerelles VPN sans fil d'entreprise ; le logiciel pare-feu personnel assure la protection des PC individuels.
- *Point d'accès sans fil* – Réalise un filtrage initial sur le protocole IP entre le réseau WLAN et le réseau d'entreprise.
- *Commutateur de couche 2* – Assure la connectivité Ethernet entre les points d'accès du WLAN et le réseau d'entreprise ; de plus, les récents modèles de commutateurs de couche d'accès peuvent mettre en œuvre une technologie appelée VLAN ACL (VACL) qui offre une couche supplémentaire de filtrage IPsec.
- *Commutateur de couche 3* – Assure le routage et la commutation des données du réseau productif d'un module à l'autre ; permet un renforcement de la politique par l'intermédiaire du filtrage du trafic sans fil au niveau du protocole.
- *Serveur RADIUS* – Authentifie les utilisateurs sans fil qui se connectent à la passerelle VPN ; échange, en option, des informations avec le serveur MPSOTP.
- *Serveur de mots de passe de sessionuniques (MPSOTP – One Time Password)* – Autorise les informations MPS OTP relayées par le serveur RADIUS.
- *Serveur DHCP* – Fournit les informations de configuration IP aux clients VPN sans fil avant et après l'établissement du VPN.
- *Passerelle VPN* – Authentifie les utilisateurs distants et assure l'aboutissement de leurs tunnels IPsec ; elle peut également assurer des fonctions de relais DHCP pour les clients sans fil.

Les risques qu'il est possible de limiter

- *Renifleurs de paquets sans fil* – Le cryptage IPsec du trafic sans fil client permet de contrer ce type de menaces. Par ailleurs, de nouvelles fonctions du logiciel client VPN permettent à l'architecte réseau d'imposer l'établissement automatique du tunnel VPN dès qu'une adresse IP de WLAN est attribuée au client. Ceci évite à l'utilisateur d'avoir à créer lui-même le tunnel IPsec et empêche également le PC client de diffuser sur le médium sans fil des données qui pourraient être utilisées pour des attaques par inférence.
- *Attaques par l 'intermédiaire (« man-in-the-middle »)* – Le cryptage et l'authentification IPsec du trafic sans fil client permet de contrer ce type de menaces.
- *Accès non autorisé* – Seuls les protocoles connus pour la configuration IP initiale (DHCP) et l'accès VPN (DNS, Internet Key Exchange [IKE] et Encapsulating Security Payload [ESP]) sont autorisés du WLAN au réseau d'entreprise grâce à un filtrage sur le point d'accès et sur le commutateur de la couche d'accès. Des politiques d'autorisation différentes selon les groupes d'utilisateurs peuvent éventuellement être appliquées sur la passerelle VPN.
- *Usurpation d'identité IP* – Un pirate peut maquiller du trafic sur le réseau WLAN, mais seuls les paquets IPsec valides et authentifiés peuvent atteindre le réseau productif filaire.
- *Usurpation d'identité ARP* – Ce type d'attaque est réalisable ; toutefois, les données sont cryptées jusqu'à la passerelle VPN, et le pirate ne pourra pas les lire.
- *Attaques par mots de passe* – De bonnes politiques de mots de passe, l'audit et, éventuellement, les mots de passe de sessionuniques (MPSOTP) permettent de contrer ces menaces.
- *Analyse de la topologie de réseau* – Seuls les protocoles IKE, ESP, DNS et DHCP sont autorisés à accéder au réseau d'entreprise en provenance de ce segment. Nous recommandons de n'autoriser le protocole ICMP (Internet Control Message Protocol) que sur l'interface extérieure du concentrateur VPN et pour des questions de dépannage.

Les risques qui ne sont pas atténués

- Usurpation d'adresse MAC ou IP provenant d'utilisateurs non authentifiés – les attaques par usurpation d'identité ARP et IP demeurent efficaces sur le sous-réseau WLAN jusqu'à ce que le client sans fil sécurise sa connexion avec IPsec.

Principes directeurs de l'architecture standard de WLAN avec VPN

Les points d'accès WLAN se connectent sur les commutateurs de couche 2 dans le module d'accès par l'intermédiaire d'un VLAN filaire dédié et transmettent le trafic IPsec provenant du client WLAN. Le trafic demeure séparé du trafic filaire normal jusqu'à ce qu'il soit décrypté par l'unité de connexion VPN. Il est important de noter que WEP n'est pas activé dans cette architecture. Le réseau sans fil lui-même est considéré comme non sécurisé et ne sert que de réseau de transit pour le trafic IPsec. Pour isoler ce réseau non sécurisé, l'administrateur doit éviter de mélanger le VLAN des utilisateurs du WLAN avec le réseau filaire. Une telle configuration donnerait en effet la possibilité à un pirate installé sur le réseau sans fil d'attaquer les utilisateurs sur le réseau filaire. Le client WLAN s'associe à un point d'accès sans fil pour établir une connexion avec le réseau campus au niveau de la couche 2. Il utilise ensuite les services DHCP et DNS du module serveur pour établir une connexion avec le réseau campus au niveau de la couche 3. Après la configuration initiale de couche 3, le tunnel VPN s'authentifie auprès de la passerelle VPN. La passerelle VPN peut utiliser des certificats numériques ou des clés pré-partagées pour authentifier les unités sans fil. Si la passerelle VPN se sert de clés pré-partagées, nous recommandons que les utilisateurs s'authentifient auprès d'elle à l'aide de mots de passe de sessionuniques (OTP). A défaut, la passerelle VPN est vulnérable aux tentatives d'ouverture de session en force si le pirate a obtenu la clé IPsec partagée qu'elle utilise. La passerelle VPN exploite les fonctions du serveur RADIUS qui, à son tour, contacte le serveur MPS OTP pour authentifier l'utilisateur. Elle utilise le protocole DHCP pour la configuration des adresses IP afin que le client WLAN puisse communiquer au travers du tunnel VPN. La sécurité est assurée en empêchant l'accès au réseau en cas de défaillance de la passerelle VPN ou du service RADIUS. Ces deux services sont indispensables pour permettre au client d'envoyer du trafic de production sur le réseau filaire. Notez que

lorsque le client sans fil communique avec le réseau campus, mais avant l'établissement du tunnel IPsec, le trafic client n'est pas considéré comme sécurisé. Aucun des problèmes de sécurité des WLAN n'est résolu tant que le client sans fil ne parvient pas à sécuriser ses communications par l'intermédiaire d'un VPN IPsec. Pour ces raisons, nous recommandons les trois techniques suivantes de limitation des risques :

En premier lieu, le point d'accès doit être configuré avec des filtres de type Ethernet, de protocole et de ports appliquant la politique de l'entreprise en matière d'utilisation du sans fil. SAFE WLAN recommande des filtres restrictifs qui n'autorisent que les protocoles indispensables à l'établissement de tunnels sécurisés en direction de la passerelle VPN. Ces protocoles sont DHCP pour la configuration client initiale, DNS pour la résolution de noms des passerelles VPN, les protocoles spécifiques au VPN, IKE (User Datagram Protocol [UDP] port 500) et ESP (IP Protocol 50), et ICMP pour le dépannage. Même avec ce type de filtrage, les serveurs DNS et DHCP restent vulnérables à des attaques directes sur les protocoles d'application eux-mêmes. Un soin tout particulier doit être apporté pour assurer la meilleure sécurité possible de ces systèmes au niveau des hôtes. Notamment, leurs systèmes d'exploitation et les correctifs logiciels des applications doivent être régulièrement mis à jour, et un système de détection des intrusions au niveau des hôtes (HIDS) doit être mis en place. Par ailleurs, les récents modèles de commutateurs de couche d'accès sont équipés de la technologie VLAN ACL (VACL). Ces listes de contrôles d'accès VLAN appliquées aux protocoles VPN ainsi qu'aux adresses IP spécifiques des concentrateurs VPN offrent une couche de filtrage supplémentaire qui garantit que seul le trafic IPsec destiné aux concentrateurs VPN d'entreprise concernés parvient à franchir le commutateur. Le trafic DNS est facultatif, selon que le client VPN doit être configuré à l'aide d'un nom DNS pour la passerelle VPN ou que l'adresse IP est seule acceptable. Nous recommandons de n'autoriser le protocole ICMP que sur l'interface extérieure du concentrateur VPN et pour des questions de dépannage et d'analyse MTU (Maximum Transmission Unit) du chemin.

Deuxièmement, une fonction du client VPN doit établir automatiquement un tunnel lorsqu'il reçoit du serveur DHCP une adresse IP de WLAN correcte. Cette fonction évite à l'utilisateur final d'établir « manuellement » le tunnel VPN après la mise en route de l'ordinateur. Enfin, le client sans fil doit exécuter un logiciel pare-feu personnel pour se protéger tant qu'il est connecté sans protection IPsec au réseau WLAN non sécurisé. De manière générale, la passerelle VPN est la frontière entre le réseau filaire sécurisé et le WLAN non sécurisé. Le client sans fil établit une connexion VPN vers la passerelle VPN pour commencer des communications sécurisées sur le réseau d'entreprise. Au cours de ce processus, la passerelle VPN assure l'authentification de l'utilisateur et de l'unité par l'intermédiaire d'un VPN IPsec. La tunnellisation partagée (« split tunneling ») doit être désactivée sur le client – l'intégralité du trafic doit passer par le tunnel.

Les autres possibilités

On peut toujours envisager l'activation de clés WEP statiques sur toutes les unités afin de compliquer un peu plus la tâche des pirates. Le surcroît de travail d'administration lié à la modification des clés statiques rend toutefois cette solution peu attractive pour les déploiements WLAN de grande taille. On pourrait imaginer d'éviter ce travail supplémentaire en ne changeant jamais les clés WEP statiques, mais on entrerait alors de plain-pied dans la catégorie « sécurité par l'obscurité ».

L'architecte réseau peut également considérer l'installation d'une couche 802.1X/EAP sur le déploiement du VPN IPsec afin de protéger l'environnement WLAN. L'inconvénient principal de cette solution est la nécessité de gérer deux infrastructures de sécurité distinctes pour les déploiements WLAN.

Pour renforcer encore la protection des services DNS et DHCP, il est également possible d'installer des hôtes dédiés au déploiement des protocoles de WLAN VPN DHCP et DNS. L'intérêt est de réduire le risque associé à deux menaces susceptibles d'affecter les ressources filaires :

- les attaques par saturation contre les services DHCP et DNS capables de toucher les utilisateurs filaires,
- la reconnaissance de réseau par l'intermédiaire de requêtes DNS ou de recherches inversées.

S'il n'est pas possible de disposer de serveurs DNS dédiés, on peut opter pour un cryptage matériel de l'adresse IP de la passerelle VPN pour les clients VPN. Toutefois, si l'adresse IP de la passerelle VPN change, chaque client devra remettre à jour son point d'entrée de passerelle.

Autres architectures de sécurité pour les WLAN

Parmi les solutions de remplacement qui s'offrent à lui pour la protection de son réseau sans fil, l'architecte peut également évaluer la faisabilité d'installer un protocole de sécurité de la couche applicative comme SSL (Secure Socket Layer) ou un protocole de tunnellisation comme SSH. La mise en œuvre efficace de ces protocoles dans un environnement sans fil exige une authentification mutuelle forte pour réduire le risque d'une attaque par l'intermédiaire. Pour le déploiement de SSL en vue de protéger la couche applicative, on utilisera des certificats côté client. Il est de plus à remarquer que SSL est fourni gratuitement avec la plupart des systèmes d'exploitation client d'entreprise en tant qu'élément du navigateur. A l'inverse, la plupart des systèmes d'exploitation des ordinateurs de bureau d'entreprise ne prennent pas SSH en charge de manière native et il faudra prévoir un coût par client pour utiliser un client SSH. Cisco ne recommande pas l'utilisation de SSL ou de SSH avec l'architecture SAFE WLAN en raison du nombre limité de technologies qui peuvent être facilement sécurisées avec ces protocoles.

Architecture de réseau WLAN pour grande entreprise

L'architecture de réseau WLAN pour grande entreprise superpose les WLAN au-dessus de la partie campus du schéma directeur SAFE Enterprise. Toutes les composantes nécessaires à la mise en œuvre des techniques d'atténuation des risques sont contenues dans les modules d'accès, de distribution et serveur. Ces composantes sont prévues pour permettre aux utilisateurs de l'entreprise d'accéder au WLAN au sein du campus. Les sections suivantes précisent les caractéristiques de mise en œuvre de chaque technique d'atténuation des risques.

Principes directeurs

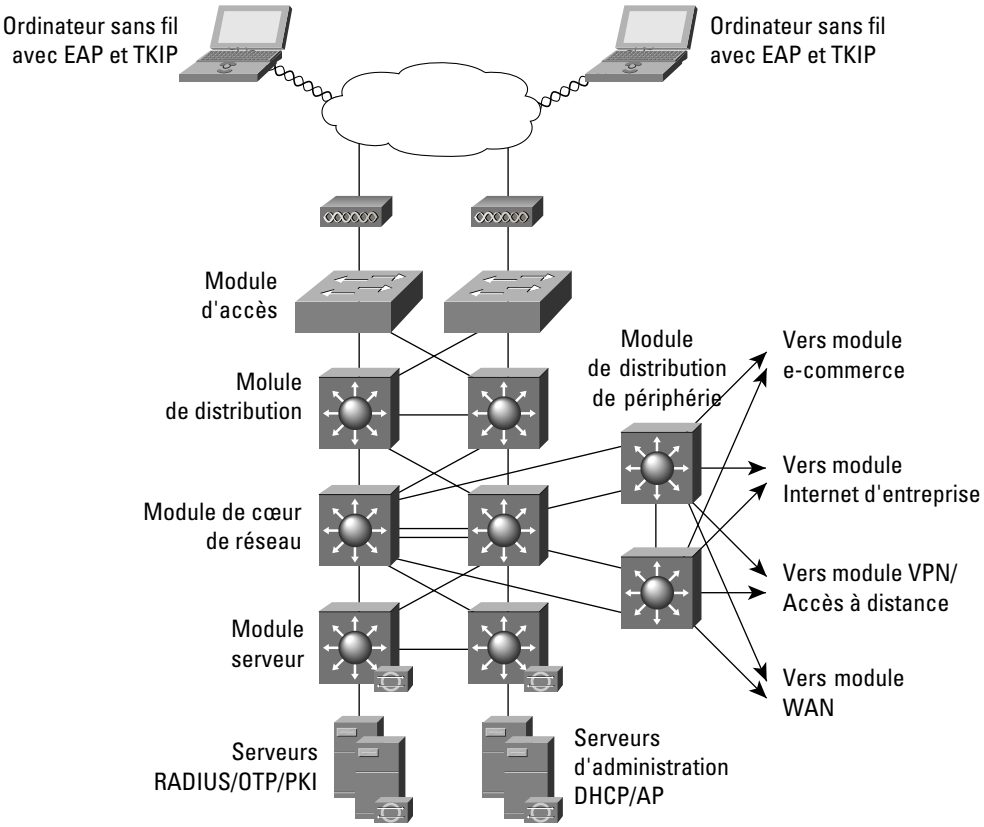
Dans une architecture WLAN pour grande entreprise, la mise en œuvre de technologies de limitation des risques doit répondre à des conditions rigoureuses d'évolutivité et de haute disponibilité. LEAP et les VPN sont considérés comme de bonnes solutions pour ce type d'architecture. Les avantages pour l'entreprise de ces deux technologies doivent être analysés en fonction de la politique de sécurité avant d'opter pour la solution la mieux adaptée au réseau.

Administration du réseau

Pour isoler le trafic d'administration du trafic utilisateur, nous recommandons d'utiliser des VLAN sur les points d'accès, de créer un VLAN d'administration pour l'accès aux points d'accès et d'empêcher l'accès à ces derniers par le sous-réseau d'administration grâce à des listes de contrôle d'accès sur le commutateur de distribution de couche 3 . Les listes de contrôle d'accès doivent porter exclusivement sur l'adresse IP et les protocoles exigés par l'utilitaire de configuration centralisée du point d'accès. Notez que comme les points d'accès ne supportent qu'une seule interface filaire, le travail d'administration s'effectue en bande et non hors bande comme le recommande SAFE Enterprise. Cette disposition présente un risque de sécurité car une partie du trafic d'administration (SNMP, Trivial File Transfer Protocol [TFTP], Hypertext Transfer Protocol [HTTP]) doit être envoyé en clair afin de pouvoir administrer chaque point d'accès par l'intermédiaire d'un poste central. Le point d'accès doit être configuré pour fournir à l'administrateur des fonctions centrales AAA (authentification, autorisation et administration) par l'intermédiaire de RADIUS ou de TACACS+, suivant ce que supportent les points d'accès déployés. Enfin, l'administrateur réseau doit assurer la protection du trafic d'administration – par SSH, par exemple – pour pouvoir gérer les points d'accès à partir de la ligne de commande.

Option EAP avec TKIP

Figure 8
Architecture de réseau WLAN EAP pour grande entreprise



L'accès EAP par l'intermédiaire du réseau sans fil exploite les trois composantes de l'architecture SAFE Enterprise :

- Le module d'accès
- Le module de distribution
- Le module serveur

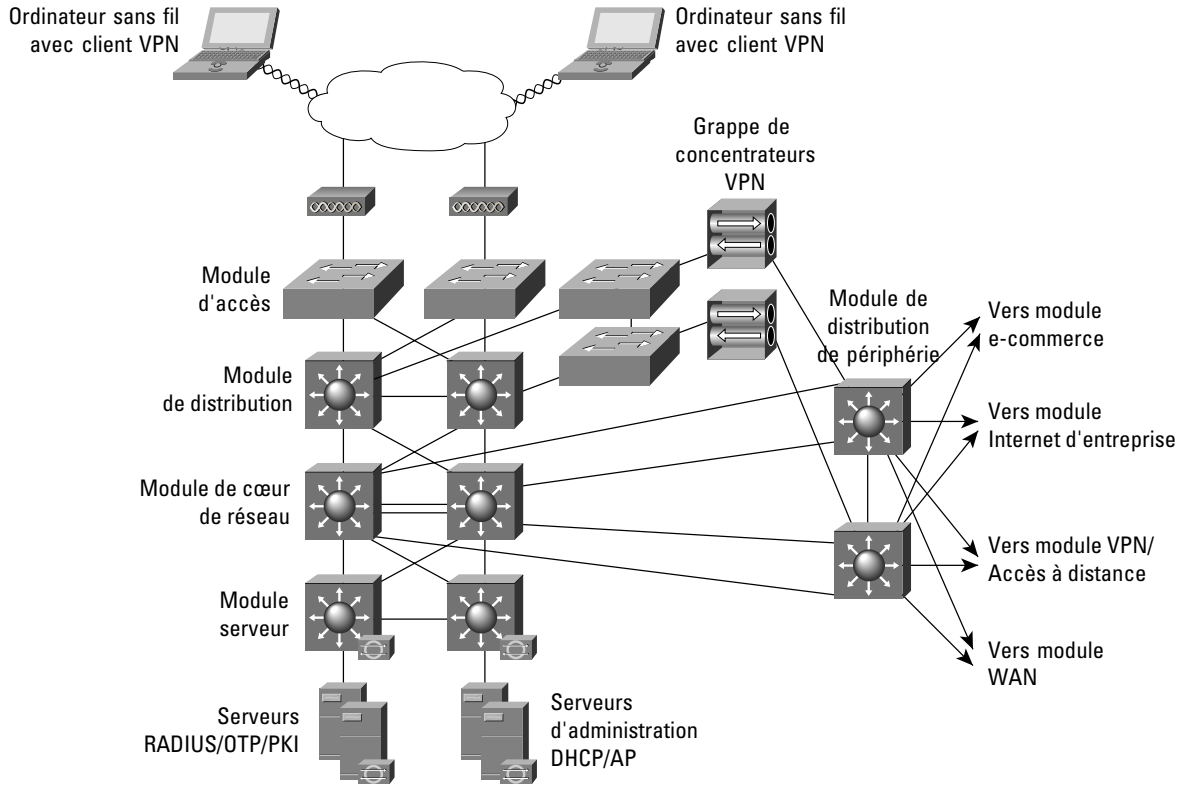
Dans l'architecture de grand réseau WLAN, les points d'accès sans fil sont connectés aux commutateurs d'accès de couche 2 existants dans le module d'accès sur l'ensemble du réseau campus. Les serveurs RADIUS, MPSOTP, PKI et DHCP sont installés dans le module serveur. Le principal problème dans une architecture de grand réseau WLAN EAP est la disponibilité et l'évolutivité de la configuration réseau et des serveurs d'authentification. Conformément aux remarques de la section axiomatique, les serveurs RADIUS, MPSOTP, PKI et DHCP sont déployés de manière redondante sur différents sous-réseaux afin de garantir la disponibilité et l'évolutivité. De plus, des produits d'équilibrage de la charge serveur peuvent améliorer l'évolutivité des serveurs RADIUS en répartissant de manière uniforme les requêtes d'authentification sur un ensemble de serveurs RADIUS. Au-delà des remarques précédentes, la méthode de connectivité est identique à celle de l'architecture standard de réseau WLAN EAP décrite auparavant.

Les autres possibilités

Comme nous l'avons décrit dans la section sur les principes directeurs généraux de l'architecture EAP, l'architecture EAP complétée par des VLAN sur les points d'accès permet de mettre en œuvre une différentiation utilisateur – à l'aide de VLAN filaires et sans fil – et de faire gérer par le serveur RADIUS l'attribution des VLAN aux utilisateurs et aux groupes d'utilisateurs. Il est par ailleurs possible de créer un VLAN « visiteur » qui permettra à un visiteur d'accéder au réseau d'entreprise et ainsi à un ensemble limité de ressources, ou encore d'établir un VPN par Internet pour accéder au réseau de sa propre entreprise. Dans ces deux cas, nous recommandons l'installation de filtres de paquets sur le commutateur d'accès et sur le commutateur de distribution de couche 3 – ou au point ou aboutit le VLAN visiteur – pour n'autoriser que le trafic compatible avec la politique de sécurité de l'entreprise applicable aux visiteurs, c'est à dire le trafic IPsec seul. De même, il est possible de créer un VLAN réservé aux appareils sans fils traditionnels qui ne supporte que les clés WEP statiques, et de faire également appliquer sur ce VLAN une politique de sécurité adaptée. Vous trouverez dans l'annexe A un exemple de mise en œuvre de l'architecture EAP qui utilise des VLAN sur les points d'accès.

Option VPN IPsec

Figure 9
Architecture de réseau WLAN VPN pour grande entreprise



L'accès VPN IPsec par l'intermédiaire du réseau sans fil reprend plusieurs modules de l'architecture SAFE Enterprise :

- Le module d'accès
- Le module de distribution
- Le module de distribution de périphérie
- Le module serveur

Principes directeurs

Le principal objectif de l'architecture de grand réseau WLAN consiste à trouver le juste équilibre entre la limitation des risques et la réalisation d'un réseau évolutif à un coût acceptable pour l'entreprise. Les principes directeurs pour une architecture standard de WLAN avec VPN que nous avons décrits précédemment montrent de manière générale comment utiliser les VPN pour sécuriser l'environnement WLAN. Lorsque l'environnement WLAN est de grande taille, la mise en pratique de ces principes devient prohibitive pour la plupart des entreprises, car l'architecture exige l'installation de câbles et la réalisation d'une infrastructure de commutation de couche 2 distinctes. La faisabilité économique d'un réseau WLAN avec VPN dans un environnement de grande taille impose donc des compromis de sécurité. Les paragraphes suivants présentent les compromis acceptables pour aider l'architecte réseau à décider si l'option VPN convient à son environnement.

Les clients WLAN s'associent à un point d'accès sans fil dans le module d'accès pour établir une connexion avec le réseau campus au niveau de la couche 2. Il utilise ensuite les services DHCP et DNS du module serveur pour établir une connexion avec le réseau campus au niveau de la couche 3. Notez que lorsque le client sans fil communique avec le réseau WLAN, mais avant l'établissement du tunnel IPsec, le trafic client n'est pas considéré comme sécurisé. Aucun des problèmes de sécurité des WLAN n'est résolu tant que le client sans fil ne parvient pas à sécuriser ses communications par l'intermédiaire d'un VPN IPsec. La fonction d'auto-initialisation du client VPN doit être utilisée pour réduire au minimum les communications échangées en dehors d'un tunnel VPN. En plus des filtres sur le point d'accès – dont nous avons parlé avec l'architecture générale de WLAN avec VPN – les commutateurs de couche 3 du module de distribution doivent être configurés avec des listes de contrôle d'accès pour n'autoriser que les protocoles nécessaires à la connectivité et à l'administration des VPN. Le client sans fil établit une connexion VPN vers les passerelles VPN qui connectent les modules de distribution et de distribution de périphérie. Les passerelles VPN redondantes doivent être configurées en équilibrage de charge pour garantir la haute disponibilité et l'évolutivité. Ces passerelles VPN représentent des ressources centralisées et partagées par un nombre potentiellement élevé de modules d'accès de couche 2. Les serveurs RADIUS, MPS OTP et DHCP utilisés par les passerelles VPN doivent être déployés de manière redondante sur différents sous-réseaux dans le module serveur pour garantir la haute disponibilité et l'évolutivité de leurs services respectifs aux tunnels des clients VPN.

Les autres possibilités

Pour renforcer sa sécurité, l'entreprise peut déployer un système de détection des intrusions réseau (Network-IDS) ainsi que des pare-feu derrière les passerelles VPN qui interviendront avant que le trafic sans fil utilisateur atteigne le réseau productif filaire. Cette disposition permet au réseau d'assurer l'audit, l'inspection et le filtrage en fonction de la politique de sécurité définie, du trafic utilisateur envoyé par les clients sans fils vers le réseau d'entreprise. Après avoir assuré l'authentification de l'unité et de l'utilisateur, la passerelle VPN peut éventuellement attribuer des droits d'autorisation en fonction du groupe auquel l'utilisateur sans fil est associé. Nous recommandons vivement de mettre en œuvre ces améliorations de sécurité si la politique d'authentification des utilisateurs VPN ne fait pas appel aux mots de passe de session.

Par ailleurs, si vous recherchez une sécurité plus forte que celle offerte par cette architecture, considérez les avantages d'une infrastructure distincte pour l'accès WLAN. La séparation physique des segments des couches 2 et 3 sur des équipements de réseau dédiés permet d'isoler totalement le réseau WLAN non sécurisé jusqu'à ce que le trafic soit décrypté au niveau des passerelles VPN et routé vers le réseau productif filaire.

De plus, en disposant sur un même point d'accès de plusieurs identificateurs SSID et de VLAN distincts, il est possible de créer un VLAN « visiteur » qui permettra à un visiteur d'accéder au réseau d'entreprise et ainsi à un ensemble limité de ressources, ou encore d'établir un VPN par Internet pour accéder au réseau de sa propre entreprise. Dans ces deux cas, nous recommandons l'installation de filtres de paquets sur le commutateur d'accès et sur le commutateur de couche 3 du bâtiment – ou au point où le VLAN visiteur aboutit – pour n'autoriser que le trafic compatible avec la politique de sécurité de l'entreprise applicable aux visiteurs. De même, il est possible de créer un VLAN réservé aux appareils sans fils traditionnels qui ne supportent que les clés WEP statiques, et de faire également appliquer sur ce VLAN une politique de sécurité adaptée. Vous trouverez dans l'annexe A un exemple de mise en œuvre de l'architecture VPN qui utilise des VLAN sur les points d'accès (architecture VPN pour grande entreprise).

Architecture de réseau WLAN de taille moyenne

L'architecture de réseau WLAN de taille moyenne superpose les WLAN au-dessus de la partie campus du schéma directeur SAFE pour réseau de taille moyenne. Toutes les composantes nécessaires à la mise en œuvre des techniques d'atténuation des risques sont contenues dans le module de campus de taille moyenne. Ces composantes sont prévues pour permettre aux utilisateurs de l'entreprise d'accéder au WLAN au sein du campus. La section suivante précise les caractéristiques de mise en œuvre de chaque technique d'atténuation des risques.

Principes directeurs

Dans l'architecture de réseau WLAN de taille moyenne, on suppose que tous les équipements WLAN sont connectés à un unique sous-réseau IP qui permet la mobilité de l'utilisateur final. De plus, la plupart des services disponibles sur le réseau filaire de taille moyenne le sont aussi pour l'extension WLAN de taille moyenne. Si elle doit respecter l'architecture de base SAFE pour les réseaux de taille moyenne, l'architecture WLAN n'offre pas une disponibilité très élevée. EAP et les VPN sont considérés comme de bonnes solutions pour ce type d'architecture. Les unités essentielles aux options EAP et VPN sont supportées dans le module campus de l'architecture SAFE pour les réseaux de taille moyenne. Pour ces deux options, il est important d'étudier avec attention l'emplacement des serveurs RADIUS et DHCP utilisés avec les solutions WLAN EAP et VPN. L'emplacement des serveurs dépend du type de bureau – entreprise de taille moyenne ou succursale d'entreprise – desservi par le réseau WLAN. Dans le cas d'une entreprise de taille moyenne, les serveurs DHCP et RADIUS doivent être installés sur le réseau local. S'il s'agit d'une succursale, ils peuvent être placés dans le siège social de l'entreprise avec une connectivité sur le module WAN ou par un VPN dans le module Internet d'entreprise. Lorsque les serveurs DHCP et RADIUS sont installés au siège social, les utilisateurs sans fil ne doivent pas obtenir l'accès au réseau local si, pour une raison quelconque – comme une défaillance de connectivité WAN – le point d'accès ou les passerelles VPN ne peuvent pas communiquer avec le serveur RADIUS. De plus, si les serveurs DHCP sont indisponibles pour le réseau de taille moyenne, les clients sans fil ne doivent pas pouvoir établir de connectivité IP avec le réseau campus. La sécurité de cette architecture est assurée en empêchant l'accès au réseau en cas de défaillance du service RADIUS. Cette politique est indispensable car l'essentiel de la limitation des risques de sécurité repose sur le service RADIUS. En règle générale, une défaillance des services DHCP gêne l'administration de la solution. La section sur les techniques de limitation des risques précise comment réaliser ces objectifs.

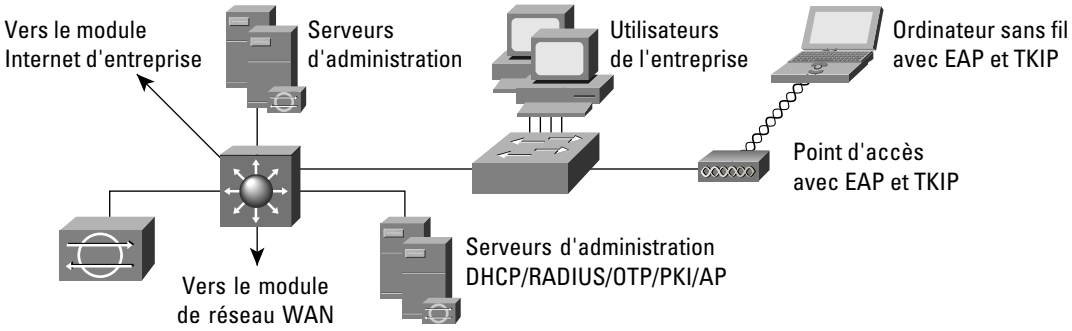
Administration du réseau

Pour isoler le trafic d'administration du trafic utilisateur, nous recommandons l'utilisation de VLAN sur les points d'accès. Nous recommandons de même de créer un VLAN d'administration sur le point d'accès et de restreindre l'accès par le sous-réseau d'administration à cette unité grâce à des listes de contrôle d'accès sur le commutateur de couche 3 du module de distribution. Les listes de contrôle d'accès doivent porter exclusivement sur l'adresse IP et les protocoles exigés par l'utilitaire de configuration multi-unités centralisé du point d'accès. Notez que comme les points d'accès ne supportent qu'une seule interface filaire, le travail d'administration s'effectue en bande et non hors bande comme le recommande SAFE Enterprise. Cette disposition présente un risque de sécurité car une partie du trafic d'administration (SNMP, TFTP) doit être envoyée en clair afin de pouvoir administrer chaque point d'accès par l'intermédiaire d'un

poste central. Le point d'accès doit être configuré pour fournir à l'administrateur des fonctions centrales AAA par l'intermédiaire de RADIUS ou de TACACS+, suivant ce que supportent les points d'accès déployés. Enfin, l'administrateur réseau doit assurer la protection du trafic d'administration – par SSH, par exemple – pour pouvoir gérer les points d'accès à partir de la ligne de commande.

Option EAP avec TKIP

Figure 10
Architecture de réseau WLAN EAP de taille moyenne



Dans l'architecture de WLAN de taille moyenne, l'accès EAP prévoit la connexion des points d'accès sans fil au commutateur de couche 2 installé dans le module de campus de taille moyenne. Les serveurs RADIUS et DHCP sont également placés dans ce module, mais à proximité d'un sous-réseau de couche 3 distinct sur le commutateur central de couche 3 du campus. Les utilisateurs EAP sans fil doivent demander les services d'authentification DHCP et RADIUS pour accéder au réseau campus de taille moyenne. Dans le cas d'une succursale entreprise, les serveurs DHCP et RADIUS peuvent être installés au siège social.

Le processus d'accès au réseau de taille moyenne est identique à celui décrit dans les principes directeurs de l'architecture standard de réseau WLAN de taille moyenne.

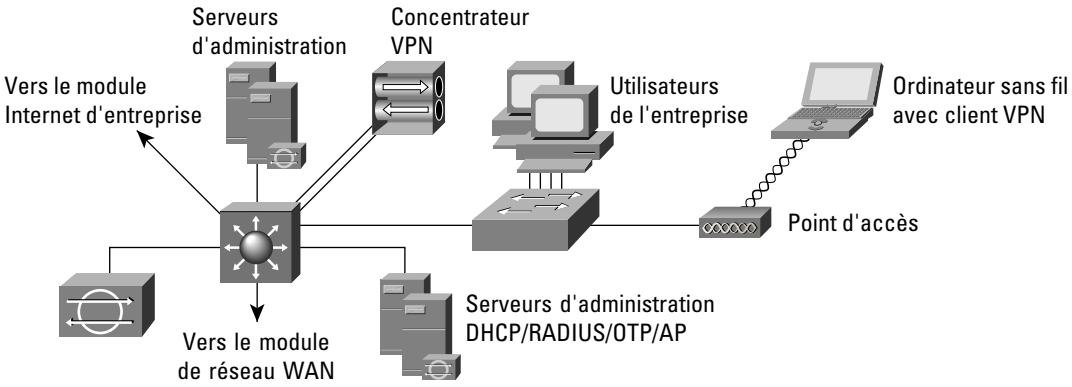
Les autres possibilités

Dans le cas d'une succursale d'entreprise et si les serveurs RADIUS et DHCP sont installés au siège social, il convient d'envisager la redondance de ces serveurs. A défaut, on peut choisir d'installer localement des serveurs RADIUS et DHCP afin de fournir un accès WLAN dans le cas d'une défaillance de la liaison de réseau étendu vers le réseau d'entreprise. Dans ce cas, il faut envisager les contraintes d'administration et de maintenance de multiples serveurs RADIUS et DHCP – voire de centaines d'entre eux dans le cas d'un réseau de détaillants.

Comme nous l'avons décrit dans la section sur les principes directeurs de l'architecture EAP pour grande entreprise, l'architecture EAP complétée par des VLAN sur les points d'accès permet de mettre en œuvre une différentiation utilisateur – à l'aide de VLAN filaires et sans fil – et de faire gérer par le serveur RADIUS l'attribution des VLAN aux utilisateurs et aux groupes d'utilisateurs. De plus, il est possible d'appliquer sur chaque groupe d'utilisateurs des filtres appropriés de couche 3 aux couches d'accès et de distribution.

Option VPN IPsec

Figure 11
Architecture de réseau WLAN VPN de taille moyenne



L'option VPN IPsec pour les réseaux de taille moyenne est très semblable à celle proposée pour les réseaux WLAN de grande taille. Les principales différences résident dans la connectivité physique de la passerelle VPN qui isole le réseau sans fil du réseau filaire. La passerelle VPN connecte ses interfaces au commutateur de couche 3 du module campus à l'aide de deux VLAN distincts. Il est à noter que cette recommandation est en conflit direct avec l'axiome « Les commutateurs sont des cibles » des livres blancs SAFE. Lorsque vous amenez un VLAN à jouer un rôle dans la protection du réseau, vous élargissez en fait le périmètre de sécurité pour qu'il intègre le commutateur lui-même. Si un pirate parvient à s'emparer du commutateur, il peut contourner le concentrateur VPN. Cette option VLAN a pourtant été retenue car l'autre solution n'est pas financièrement viable pour les sociétés susceptibles de déployer un réseau de taille moyenne. La section « Les autres possibilités » ci-dessous présente une solution plus sûre mais qui utilise des équipements supplémentaires.

La passerelle VPN connecte son interface publique à un VLAN qui se connecte aux points d'accès sans fil. Dans l'architecture WLAN VPN standard, nous recommandons que le concentrateur VPN assure le relais DHCP entre le côté public et le côté privé du concentrateur. Ceci permet de déployer et d'administrer plus efficacement les services DHCP en direction du WLAN. L'interface privée de la passerelle VPN se connecte à un VLAN avec accès vers le réseau filaire. Les points d'accès sans fil se connectent sur les commutateurs de couche 2 dans le module campus par l'intermédiaire d'un VLAN dédié et transmettent le trafic du client WLAN au VLAN sur une connectivité VPN. Comme dans l'architecture WLAN de grande taille et l'architecture générale de WLAN avec VPN, les commutateurs d'accès et les commutateurs de couche 3 du module de distribution doivent être configurés avec les listes de contrôle d'accès pour n'autoriser que les protocoles nécessaires à la connectivité et à l'administration des VPN.

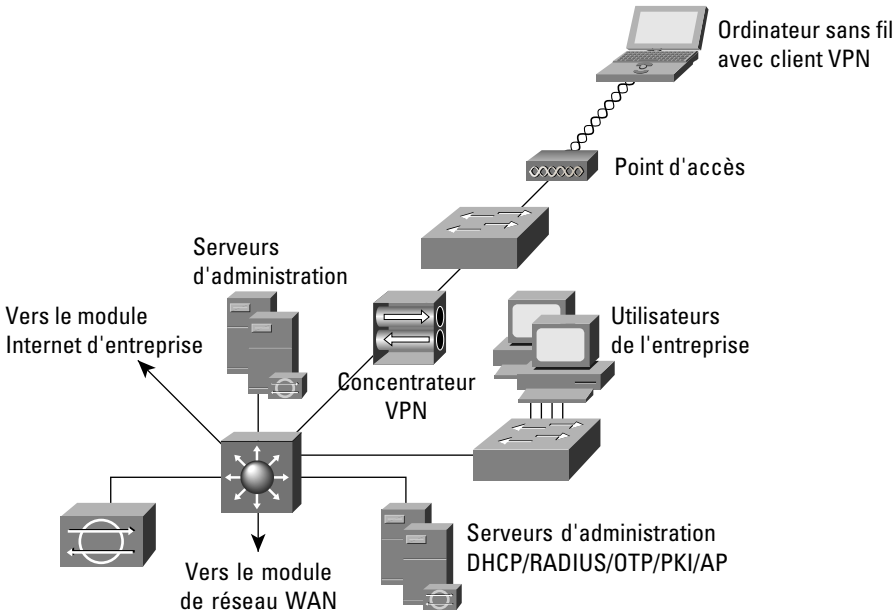
Le client sans fil établit une connexion IPsec vers la passerelle VPN sans fil. Au cours de ce processus, la passerelle VPN assure l'authentification de l'utilisateur et de l'unité par l'intermédiaire d'un VPN IPsec. La passerelle VPN peut utiliser des certificats numériques ou des clés pré-partagées afin d'authentifier les unités clients sans fil. L'utilisateur VPN final s'authentifie auprès de la passerelle VPN grâce à un mot de passe deunique session (MPSOTP). La passerelle VPN utilise les fonctions du serveur RADIUS qui, à son tour, contacte le serveur MPS OTP pour authentifier l'utilisateur. Elle utilise le protocole DHCP pour les informations d'adressage IP pour que le client WLAN puisse communiquer au travers du tunnel VPN.

Les autres possibilités

Pour renforcer sa sécurité, l'entreprise peut déployer un système de détection des intrusions réseau (Network-IDS) ainsi que des pare-feu derrière les passerelles VPN qui interviendront avant que le trafic sans fil utilisateur atteigne le réseau productif filaire. Cette disposition permet au réseau d'assurer l'audit, l'inspection et le filtrage, en fonction de la politique de sécurité définie, du trafic utilisateur envoyé par les clients sans fil vers le réseau de taille moyenne. Nous recommandons vivement de mettre en œuvre ces améliorations de sécurité si la politique d'authentification des utilisateurs VPN ne fait pas appel aux mots de passe de session.

Par ailleurs, si vous recherchez une sécurité plus forte que celle offerte par cette architecture, considérez les avantages d'une architecture analogue à l'option WLAN avec VPN standard. La Figure 12 présente une architecture spécifique au réseau WLAN de taille moyenne. Son principal avantage est la séparation claire entre les interfaces publiques et privées de la passerelle VPN. L'inconvénient majeur de cette architecture est le coût potentiellement élevé du déploiement de commutateurs de couche 2 supplémentaires destinés à connecter les points d'accès sans fil. De nouvelles fonctionnalités des concentrateurs VPN leur permettent de relayer les services DHCP vers des serveurs DHCP placés derrière eux. Cette option de déploiement a l'inconvénient d'exposer le serveur DHCP aux risques de sécurité décrits dans l'architecture VPN standard, mais elle est préférable au déploiement d'un serveur DHCP en aval du concentrateur VPN.

Figure 12
Architecture de réseau WLAN VPN de taille moyenne



Architecture de petit réseau WLAN

L'architecture de petit réseau WLAN superpose le WLAN au-dessus de l'architecture SAFE pour petit réseau. L'architecture de petit réseau WLAN est contenue dans le module campus. Cette section présente une seule option – EAP avec TKIP – pour fournir une connectivité d'utilisateur distant au réseau campus filaire. IPsec n'est pas envisagé ici en raison de la charge financière que représente la mise en œuvre d'un réseau WLAN avec VPN dédié dans un environnement de cette taille.

Principes directeurs

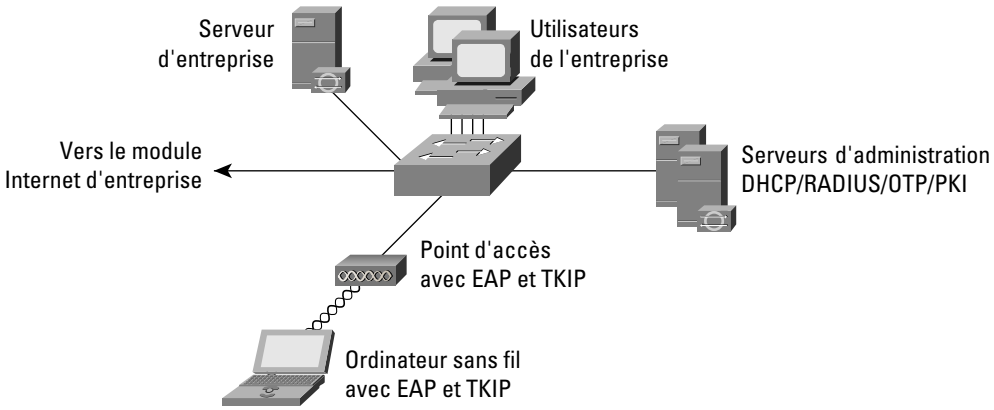
Les sections suivantes décrivent l'architecture de petit réseau WLAN. L'architecture de petit réseau comporte un unique commutateur de couche 2 pour sa connectivité campus – comme le montre la Figure 13 – et nous supposerons donc que toutes les unités disposent d'un unique sous-réseau IP pour permettre le roaming entre les points d'accès.

Administration du réseau

L'absence d'une unité de couche 3 sur le petit réseau de campus empêche la protection du trafic d'administration en provenance des serveurs d'administration vers les points d'accès. Une partie du trafic d'administration est envoyée en clair à chaque point d'accès, comme c'est le cas pour le reste de l'architecture SAFE pour petits réseaux.

Option EAP avec TKIP

Figure 13
Architecture de petit réseau WLAN EAP



Dans l'architecture de petit réseau WLAN, l'accès EAP prévoit la connexion des points d'accès sans fil au commutateur de couche 2 installé dans le module de petit réseau campus. Les utilisateurs EAP sans fil doivent demander les services d'authentification DHCP et RADIUS pour accéder au petit réseau campus. Les petits réseaux sont par nature limités à un seul bâtiment et les serveurs RADIUS et DHCP sont implantés localement et connectés au commutateur de couche 2 du module campus.

Le processus d'accès au petit réseau est identique à celui décrit dans les principes directeurs de l'architecture standard de réseau WLAN.

Les autres possibilités

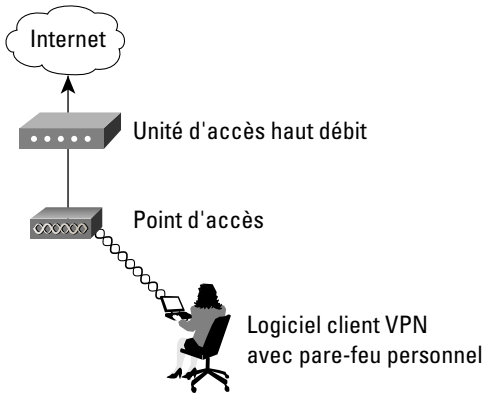
Bien que nous ne le recommandions pas, et si l'entreprise se sent capable de gérer les questions de distribution de clés, elle peut utiliser des clés WEP statiques – moyennant les améliorations cryptographiques précisées plus haut – en remplacement de la solution EAP.

Architecture de réseau WLAN distant

L'architecture de réseau WLAN distant offre des solutions sans fil pour les deux principaux types de connectivité VPN distante définis par SAFE : les VPN logiciels et les VPN matériels. Cette section présente les deux options pour fournir aux utilisateurs du réseau WLAN une connectivité vers un bureau central (de petite taille, de taille moyenne ou d'entreprise) dans le cadre de l'architecture SAFE.

Architecture de réseau WLAN distant avec VPN logiciel

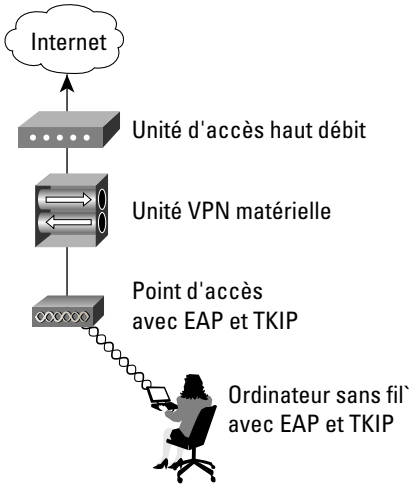
Figure 14
Architecture de réseau WLAN distant avec VPN logiciel



Nous recommandons d'adopter l'option VPN IPsec pour le réseau distant lorsque l'utilisateur exige une protection de ses communications entre l'unité sans fil et le réseau d'entreprise (comme le montre la Figure 14). Cette configuration est la plus courante pour les travailleurs distants qui peuvent ne pas avoir accès à des ressources matérielles gérées par le service informatique sur le lieu où ils se connectent. Les télétravailleurs à temps partiel appartiennent à cette catégorie. Le point d'accès peut recevoir pratiquement toute configuration qui autorise une connectivité vers l'unité haut-débit car la sécurité est assurée par le logiciel client VPN avec pare-feu personnel. De plus, l'architecte réseau peut envisager de placer des filtres sur le point d'accès afin de n'autoriser que le trafic IPsec, DHCP et DNS et réduire ainsi les risques d'attaques du réseau LAN filaire en provenance du WLAN. L'annexe A, « Laboratoire de validation », présente en détail les filtres des points d'accès.

Architecture de réseau WLAN distant avec VPN matériel

Figure 15
Architecture de réseau WLAN distant avec VPN matériel



Dans les configurations où le service informatique de l'entreprise administre les équipements VPN et sans fil installés chez l'utilisateur distant, une solution de sécurité robuste consiste à utiliser EAP du PC vers le point d'accès puis IPsec de l'unité VPN matérielle jusqu'au bureau central (comme sur la Figure 15). Une telle configuration est particulièrement adaptée aux télétravailleurs à temps plein. Lorsque le site distant utilise un VPN matériel et le protocole EAP pour la liaison sans fil, l'architecture est pratiquement identique à celle d'un petit réseau WLAN. Il est à noter que les mêmes mises en garde s'appliquent en ce qui concerne l'accès au serveur RADIUS. Les utilisateurs sans fil ne doivent pas pouvoir accéder au réseau local si, pour une raison quelconque – comme une défaillance de connectivité VPN IPsec– le point d'accès ne peut pas communiquer avec le serveur RADIUS. Cette architecture exige également que le réseau distant possède une unique adresse IP pour faciliter l'administration du point d'accès distant par le service informatique. Si l'unité matérielle utilise la traduction des adresses de réseau NAT (Network Address Translation) pour l'ensemble du trafic entre le site distant et une adresse IP, le service informatique sera incapable d'administrer le point d'accès.

Annexe A : Laboratoire de validation

Une implantationL'architecture de référence du schéma directeur Cisco SAFE WLAN a été développée mise en oeuvre pour valider les fonctionnalités décrites dans le présent document. Nous présentons dans cette annexe les détails de la configuration des diverses unités – dans le cadre des fonctionnalités WLAN de chaque module – ainsi que les principes généraux de configuration des unités. Vous trouverez ici les clichés exemples de configuration des unités actives de notre laboratoire. Cisco ne recommande pas d'appliquer directement ces configurations à un réseau productif.

Principes généraux

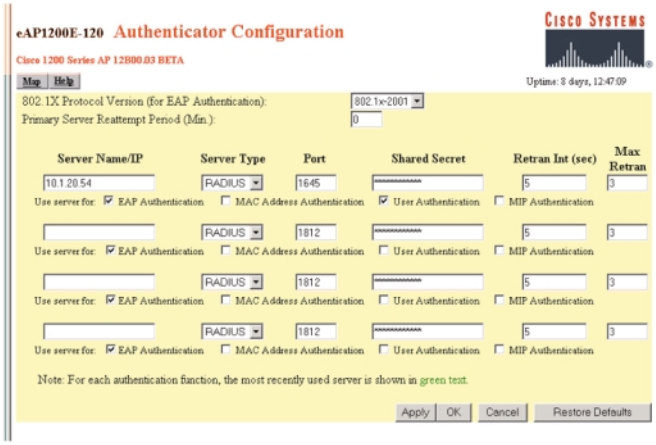
Les exemples de commandes présentés dans cette section correspondent en partie aux principes directeurs SAFE WLAN exposés plus haut dans ce document.

Configuration SAFE WLAN standard pour les points d'accès

Point d'accès EAP

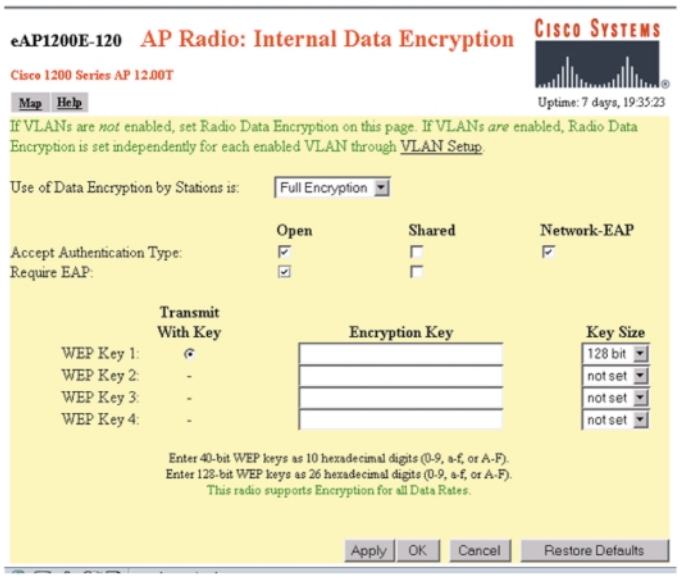
La Figure A-1 montre la fenêtre Authenticator Configuration (dans Setup >> Security section) sur un point d'accès configuré pour autoriser les clients EAP (Extensible Authentication Protocol) sans fil à s'authentifier auprès d'un serveur RADIUS (Remote Access Dial-In User Service). Nous supposons que le serveur RADIUS lui-même, ou bien un serveur MPS externeréseau – comme un serveur Windows NT – contient une base de données des utilisateurs autorisés ainsi que leurs mots de passe.

Figure A-1
Fenêtre Authenticator Configuration pour un point d'accès EAP



La Figure A-2 présente la configuration de sécurité pour un point d'accès EAP. Le point d'accès demande l'option de cryptage complet (« Full Encryption » avec WEP [Wired Equivalent Privacy]) ; de plus, le point d'accès n'autorise que Network-EAP comme méthode d'authentification. Les types de protocoles EAP configurés dans ce déploiement sont : Cisco-EAP (LEAP), Protected EAP (PEAP), et EAP-Transport Layer Security (EAP-TLS).

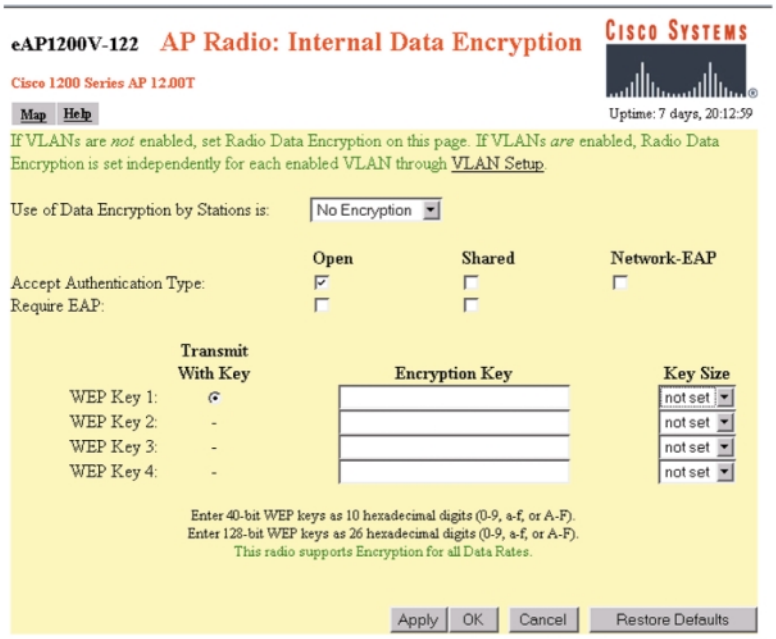
Figure A-2
Configuration WEP pour un point d'accès EAP



Point d'accès VPN

Comme le montre la Figure A-3, un point d'accès est configuré pour permettre une authentification ouverte et le cryptage WEP n'est pas activé pour les clients VPN sans fil qui s'authentifient auprès d'un réseau filaire.

Figure A-3
Configuration WEP pour un point d'accès VPN



Les sections suivantes montrent le détail des configurations nécessaires sur les points d'accès pour activer EAP ou les VPN (voir les captures d'écran) comme nous l'avons précisé dans la section axiomatique et dans les principes directeurs de ce document. Les copies d'écran ci-dessous correspondent à l'architecture pour grande entreprise.

Comme nous l'avons exposé dans la partie architecture de ce document, le point d'accès VPN doit être configuré avec des filtres de type Ethernet, de protocole et de ports appliquant la politique de l'entreprise en matière d'utilisation du sans fil. SAFE WLAN recommande des filtres restrictifs qui n'autorisent que les protocoles indispensables à l'établissement de tunnels sécurisés en direction de la passerelle VPN. Le protocole ICMP (Internet Control Message Protocol) est autorisé pour des questions de dépannage. Les Tableaux A-1 et A-2 donnent la liste des filtres entrants (réception) et sortant (transmission) à définir sur l'interface radio du point d'accès VPN :

Tableau A-1 Filtres de protocoles radio pour point d'accès VPN – entrant (réception)

Type de filtre	Protocole	Valeur	Position
EtherType	ARP	0x0806	Forward
EtherType	IP	0x0800	Forward
Protocole IP	UDP	17	Forward
Protocole IP	ESP	50	Forward
Protocole IP	ICMP	1	Forward
Port IP	BootPC	68	Forward
Port IP	DNS	53	Forward
Port IP	IKE	500	Forward

Tableau A-2 Filtres de protocoles radio pour point d'accès VPN – sortants (transmission)

Type de filtre	Protocole	Valeur	Position
EtherType	ARP	0x0806	Forward
EtherType	IP	0x0800	Forward
Protocole IP	UDP	17	Forward
Protocole IP	ESP	50	Forward
Protocole IP	ICMP	1	Forward
Port IP	BootPC	68	Forward
Port IP	DNS	53	Forward
Port IP	IKE	500	Forward

Lorsque vous créez ces ensembles de filtres sur les points d'accès VxWorks, veillez bien à :

- placer le paramètre « Default Disposition » du filtre sur « block »,
- autoriser le passage des types de trafic spécifiques en ajoutant les valeurs précisées (dans le Tableau A-1 ou A-2) à « Special Cases » et sélectionner « forward » comme position pour chaque cas particulier,
- appliquer à l'interface radio du point d'accès – ou au VLAN VPN – tous les ensembles de filtres créés.

Configuration SAFE WLAN standard pour les clients

Les sections suivantes montrent le détail des configurations nécessaires sur les clients sans fil pour activer EAP ou les VPN (voir les captures d'écran) comme nous l'avons précisé dans la section axiomatique et dans les principes directeurs de ce document. Les copies d'écran ci-dessous correspondent à l'architecture pour grande entreprise. Toutefois, la configuration d'un client VPN sans fil (ou d'un client LEAP sans fil) est identique pour toutes les architectures.

Client VPN

Lorsqu'un utilisateur sans fil se connecte sur un réseau filaire à l'aide d'un client VPN, le cryptage et l'authentification de couche 2 sont généralement désactivés. Toutefois, l'administrateur IT peut opter pour une clé WEP statique, pour le protocole TKIP (Temporal Key Integrity Protocol) ou pour EAP avec TKIP au niveau de la couche 2 du réseau. Les Figures A-4 et A-5 présentent un exemple de configuration.

Figure A-4
Configuration des paramètres systèmes sur un client VPN

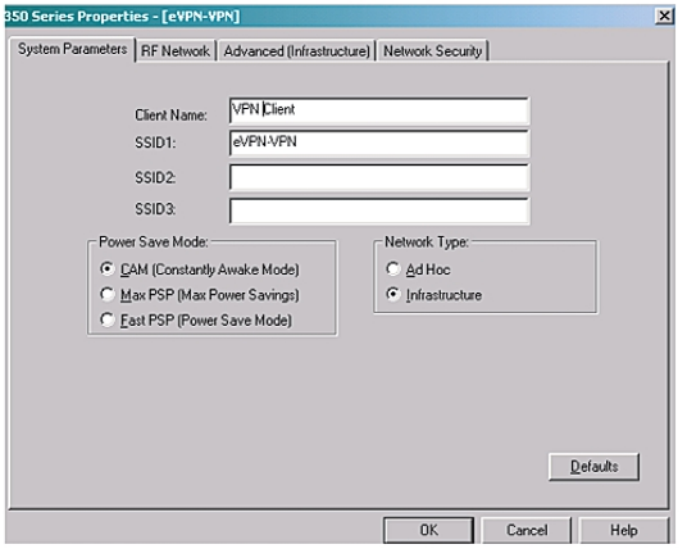
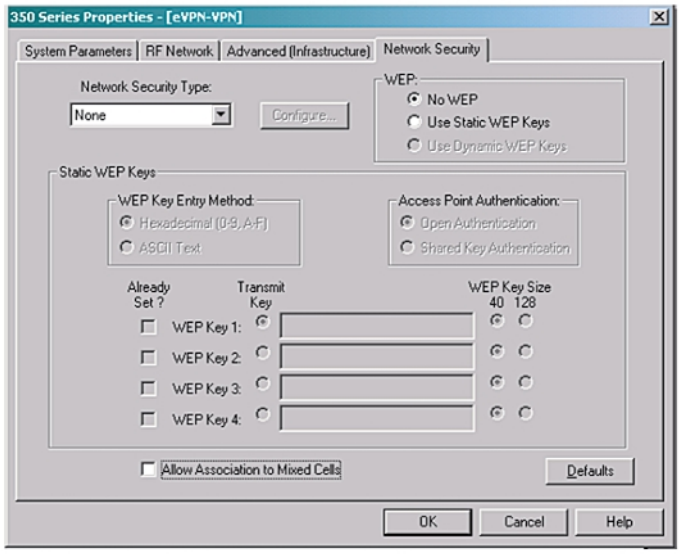


Figure A-5
Configuration de la sécurité réseau sur un client VPN



Client EAP

Pour configurer un client sans fil pour EAP, l'identificateur SSID approprié ainsi que les paramètres de sécurité doivent être précisés à l'aide de l'utilitaire client Cisco Aironet®. Notez toutefois que la configuration au niveau du système d'exploitation est généralement indispensable pour EAP-TLS et PEAP – par exemple, en configurant le client Microsoft Windows XP à l'aide des paramètres EAP-TLS ou PEAP appropriés. Les Figures A-6, A-7 et A-8 présentent un exemple de configuration pour un client LEAP. Les Figures A-9 et A-10 présentent un exemple de configuration pour un client EAP-TLS ou PEAP.

Figure A-6
Configuration des paramètres systèmes sur un client EAP sans fil

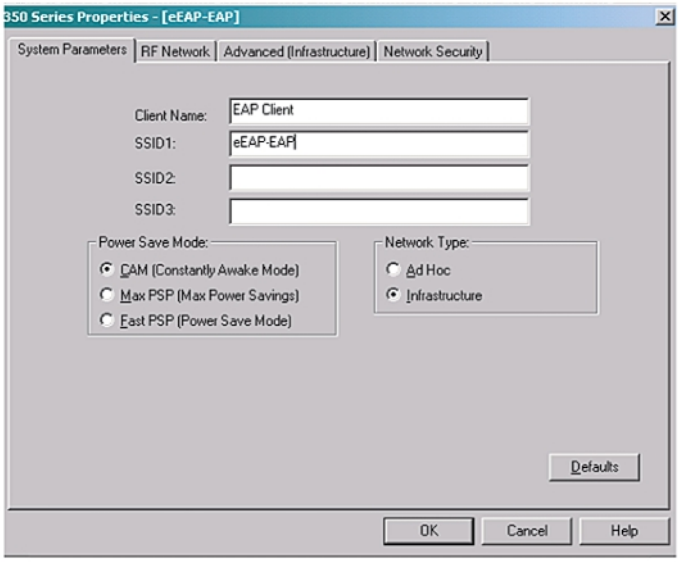


Figure A-7
Configuration de la sécurité réseau sur un client EAP sans fil

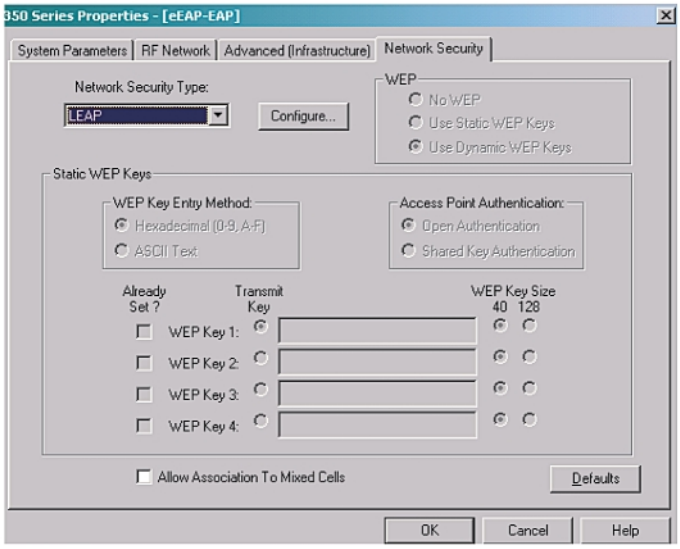


Figure A-8
Configuration des paramètres LEAP sur un client LEAP sans fil

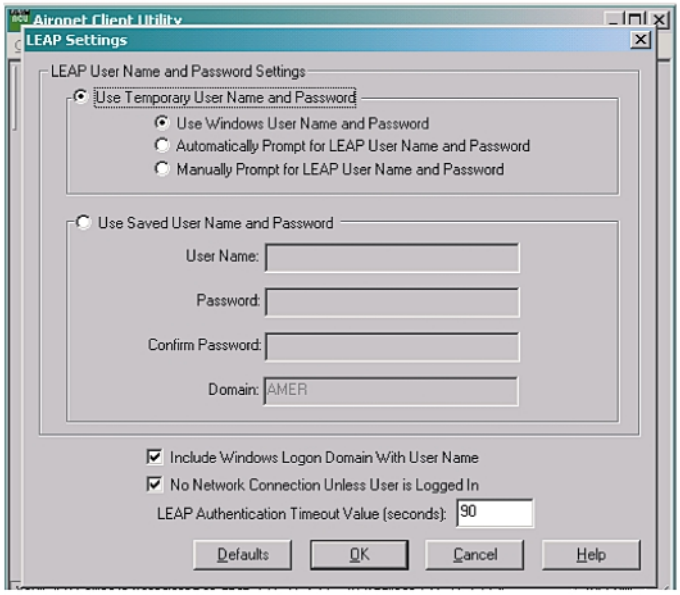


Figure A-9
Configuration de la sécurité réseau sur un client PEAP ou EAP-TLS sans fil

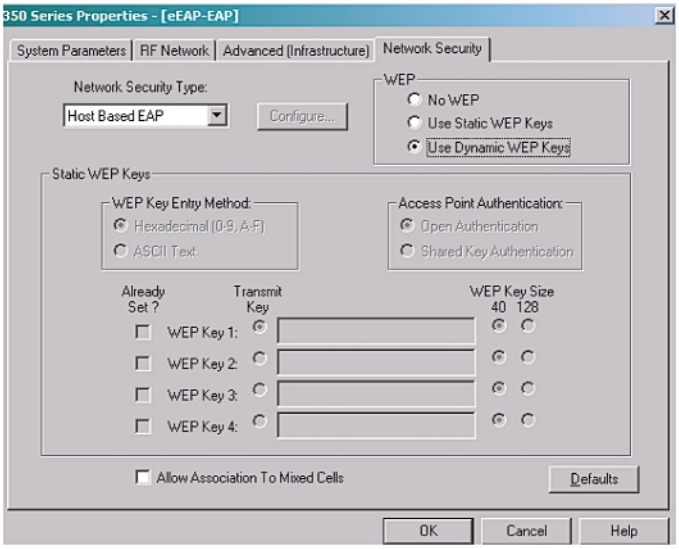
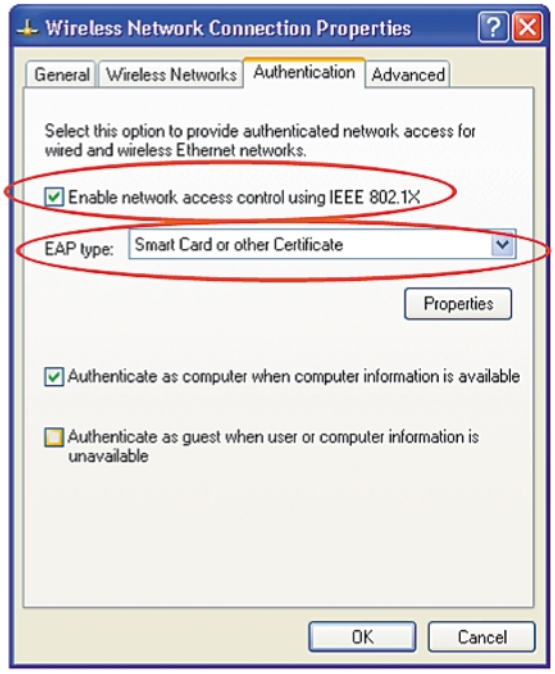


Figure A-10
Configuration d'authentification sur un client PEAP ou EAP-TLS sans fil pour Windows



Configurations des modules avec l'architecture grande entreprise

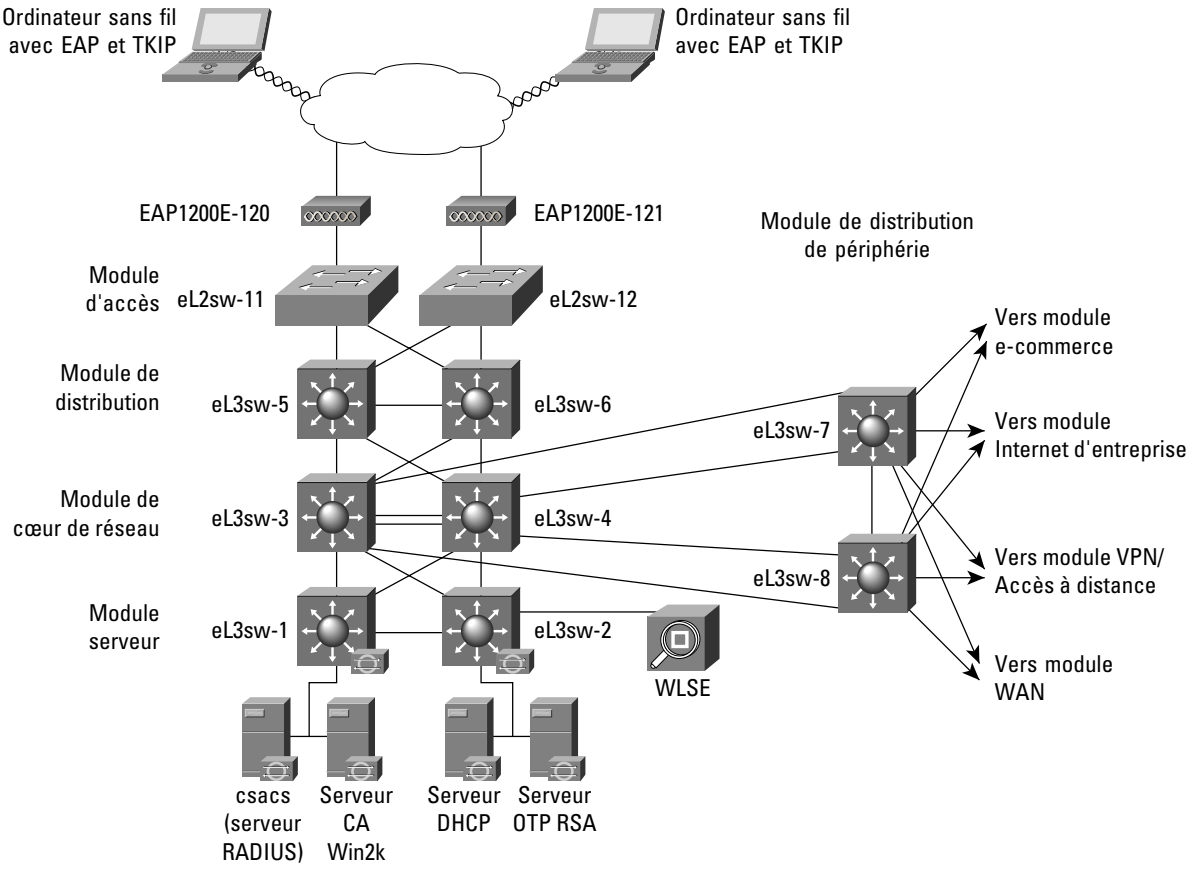
Nous donnons dans cette section les configurations d'architecture EAP et VPN de bout en bout pour une architecture de réseau de grande entreprise.

Architecture EAP avec TKIP

Vous trouverez ci-dessous un cliché exemple de configuration pour l'architecture SAFE WLAN EAP pour grande entreprise. La Figure A-11 présente l'architecture EAP pour un réseau de grande entreprise.

Figure A-11

Architecture de réseau WLAN EAP pour grande entreprise



Les produits utilisés dans cette architecture comprennent :

- des commutateurs de couche 3 Cisco Catalyst® 6506 (de eL3sw-1 à eL3sw-8)
- des commutateurs de couche 2 Cisco Catalyst® 4003 (de eL2sw-11 à eL2sw-12)
- des points d'accès et des clients Cisco Aironet 1200 (de eAP1200E-120 à eAP1200V-121) et des clients sans fil)
- un serveur ACS (Access Control Server) (ACS v3.1)
- un serveur DHCP (Dynamic Host Configuration Protocol) Windows 2000
- un serveur de certificats Windows 2000 (CA Win2k)
- un serveur de mot de passe de sessionunique (MPSOTP) RSA
- Cisco Wireless LAN Solution Engine (WLSE)

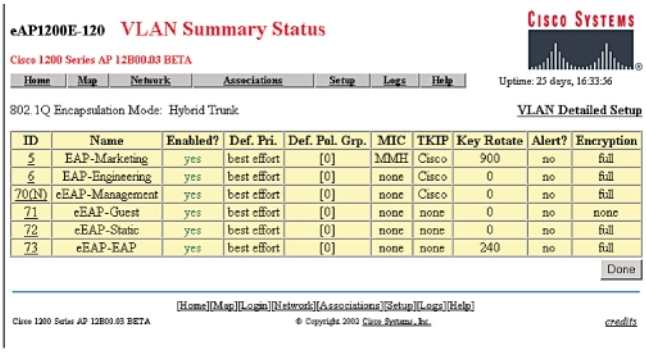
Les sections suivantes présentent les caractéristiques de configuration de l'architecture SAFE WLAN pour grand réseau. Les principes directeurs généraux de configuration pour un réseau de grande entreprise sont décrits dans « Cisco SAFE : A Security Blueprint for Enterprise Networks »

Points d'accès Cisco Aironet 1200 (de eAP1200E-120 à eAP1200V-121) et clients sans fil :

Pour la configuration EAP des points d'accès Cisco Aironet et des clients sans fil, consultez les exemples de configuration de la section « Principes généraux » de la présente annexe. Dans le laboratoire du schéma SAFE, l'architecture de réseau WLAN EAP pour grande entreprise a été mise en œuvre avec des VLAN sans fil. La présente section décrit les caractéristiques de la mise en œuvre des VLAN ainsi que celle de l'architecture de réseau WLAN EAP.

Comme le montrent les Figures A-12 et A-13, la configuration de chaque point d'accès présente plusieurs profils de sécurité corrélés à l'aide d'associations SSID et d'identifiants de VLAN. La configuration d'utilisateur EAP authentifié prévoit un cryptage à 128 bits.

Figure A-12
Page récapitulative de la configuration VLAN d'un point d'accès EAP

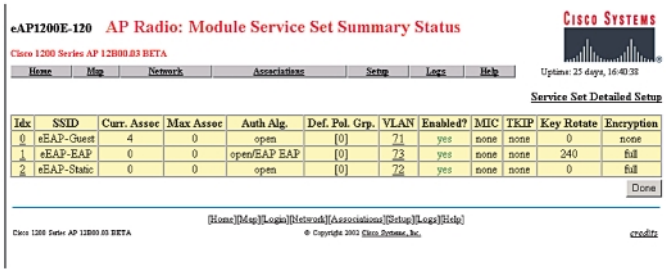


Comme nous l'avons décrit dans la section « architecture » de ce document, des VLAN Marketing et Ingénierie ont été créés pour les groupes d'utilisateurs correspondants du serveur Cisco Secure ACS. Ainsi, lorsqu'un utilisateur EAP sans fil s'associe, il est provisoirement placé dans le VLAN 73, tandis que sa demande d'authentification est transmise au serveur ACS. Une fois l'utilisateur authentifié en fonction du nom d'utilisateur configuré, il est placé sur le VLAN correspondant – Marketing ou Ingénierie. Un VLAN d'administration (VLAN 70) a également été créé pour la gestion des points d'accès. Pour des détails supplémentaires, consultez le guide sur le déploiement des VLAN :

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

Une autre configuration possible consiste à créer des identificateurs SSID WEP d'invité (eEAP-Guest) et statiques (eEAP-Static) associés avec des VLAN et des profils de sécurité distincts afin de différentier l'accès utilisateur.

Figure A-13
Page récapitulative de la configuration Service Set d'un point d'accès EAP



Commutateurs de couche 3 Cisco Catalyst® 6506 (de eL3sw-5 et eL3sw-6) (interconnexion entre le module d'accès et le module de distribution) :

```
! Management VLAN for APs in the campus network
interface Vlan70
ip address 10.1.70.5 255.255.255.0
ip access-group 170 in
ip access-group 171 out
ip helper-address 10.1.11.50
no cdp enable

!EAP VLAN for authenticated users
interface Vlan73
ip address 10.1.73.5 255.255.255.0
ip access-group 172 in
ip access-group 173 out
ip helper-address 10.1.11.50
no cdp enable
```

Nous donnons ici les listes de contrôle d'accès pour le VLAN d'administration (interface 70) :

```
! Permit only authentication and accounting requests from APs to RADIUS server on the management
VLAN
access-list 170 permit udp host 10.1.70.120 gt 1023 host 10.1.20.54 eq 1645
access-list 170 permit udp host 10.1.70.120 gt 1023 host 10.1.20.54 eq 1646
access-list 170 permit udp host 10.1.70.121 gt 1023 host 10.1.20.54 eq 1645
access-list 170 permit udp host 10.1.70.121 gt 1023 host 10.1.20.54 eq 1646

! Permit only SNMP and TFTP traffic from wireless APs to WLSE* in out of band management network
access-list 170 permit udp host 10.1.70.120 eq snmp host 10.1.20.150
access-list 170 permit udp host 10.1.70.121 eq snmp host 10.1.20.150
access-list 170 permit udp host 10.1.70.120 host 10.1.20.150 eq tftp
access-list 170 permit udp host 10.1.70.121 host 10.1.20.150 eq tftp

! Permit outgoing traffic for AP web management in the out of band management network
access-list 170 permit tcp host 10.1.70.120 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.1.70.121 eq www 10.1.20.0 0.0.0.255 gt 1023 established

!Permit SSH traffic from the APs to out of band management network
access-list 170 permit tcp host 10.1.70.120 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.1.70.121 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
```

```
! Permit only BOOTP requests to pass through to DHCP server
access-list 170 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

! Deny all other traffic
access-list 170 deny ip any any log

! Permit only SNMP and TFTP traffic from WLSE* to APs in out of band management network
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.120 eq snmp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.121 eq snmp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.120 eq tftp
access-list 171 permit udp host 10.1.20.150 gt 1023 host 10.1.70.121 eq tftp

! Permit outgoing web traffic from out of band network to APs for management
access-list 171 permit tcp 10.1.20.0 0 .0.0.255 gt 1023 host 10.1.70.120 eq www
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.121 eq www
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.120 eq 22
access-list 171 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.70.121 eq 22

! Permit RADIUS responses from AAA Server
access-list 171 permit udp host 10.1.20.54 eq 1645 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1646 host 10.1.70.120 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1645 host 10.1.70.121 gt 1023
access-list 171 permit udp host 10.1.20.54 eq 1646 host 10.1.70.121 gt 1023

! Deny all other IP traffic to APs
access-list 171 deny ip any host 10.1.70.120 log
access-list 171 deny ip any host 10.1.70.121 log
access-list 171 deny ip any any log
```

Nous donnons ici les listes de contrôle d'accès pour le VLAN EAP (interface 73) :

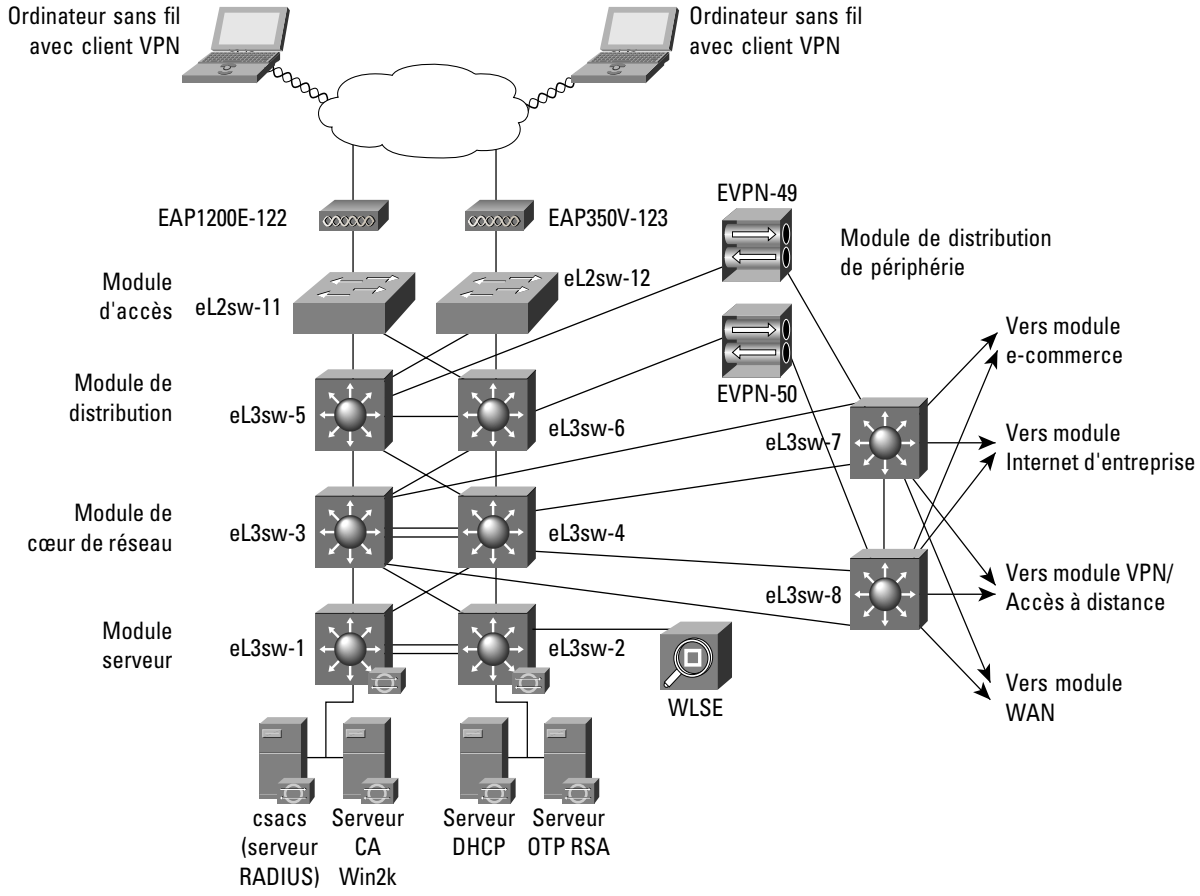
```
!Deny user access to APs management VLAN
access-list 172 deny ip 10.1.73.0 0.0.0.255 10.1.70.0 0.0.0.255 log
! Permit all IP traffic from EAP VLAN in wireless network to any destination
access-list 172 permit ip 10.1.73.0 0.0.0.255 any
! Permit only BOOTP requests to pass through to DHCP server
access-list 172 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
!Deny all other traffic
access-list 172 deny ip any any log
```

```
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 173 permit ip any 10.1.73.0 0.0.0.255
!Deny all other traffic
access-list 173 deny ip any any log
```

Architecture VPN

Vous trouverez ci-dessous un cliché de configuration pour l'architecture SAFE WLAN VPN pour grande entreprise. La Figure A-14 présente l'architecture VPN pour un réseau WLAN de grande entreprise.

Figure -14
Architecture de réseau WLAN VPN pour grande entreprise



Les produits utilisés dans cette architecture comprennent :

- des commutateurs de couche 3 Cisco Catalyst® 6506 (de eL3sw-1 à eL3sw-8)
- des commutateurs de couche 2 Cisco Catalyst® 4003 (de eL2sw-9 à eL2sw-14)
- des concentrateurs Cisco VPN 3015 (de eVPN-49 à 50)
- des points d'accès et des clients Cisco Aironet 1200 (de eAP1200V-120 à eAP350V-121) et des clients sans fil)

- un serveur ACS (Access Control Server) (ACS v3.1)
- un serveur DHCP Windows 2000
- un capteur Cisco IDS (Intrusion Detection System) Host Sensor
- un serveur de certificats Windows 2000 (CA Win2k)
- un serveur MPS OTP RSA
- Cisco Wireless LAN Solution Engine (WLSE)

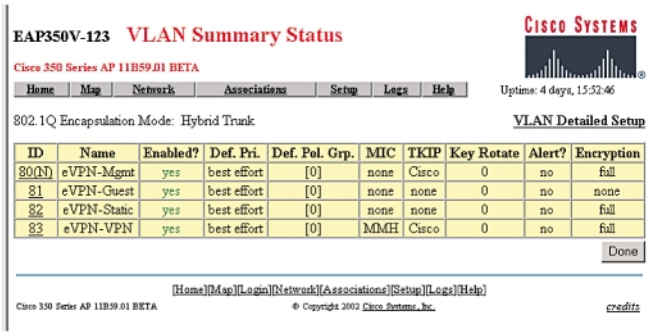
Les sections suivantes présentent les caractéristiques de configuration de l'architecture SAFE WLAN pour réseau VPN de grande entreprise. Les principes directeurs généraux de configuration pour un réseau de grande entreprise sont décrits dans « Cisco SAFE : A Security Blueprint for Enterprise Networks »

Points d'accès Cisco Aironet 1200 (de eAP1200V-120 à eAP350V-121) et clients sans fil :

Pour la configuration des points d'accès Cisco Aironet et des clients sans fil dans le cadre d'une connectivité VPN sur un WLAN, consultez les exemples de configuration de la section « Principes généraux » de la présente annexe. Dans le laboratoire de l'architecture SAFE, l'architecture de réseau WLAN VPN pour grande entreprise a été mise en œuvre avec des VLAN sans fil. La présente section décrit les caractéristiques de la mise en œuvre des VLAN ainsi que celle de l'architecture de réseau WLAN VPN.

Comme le montre la Figure A-15, la configuration de chaque point d'accès présente plusieurs profils de sécurité corrélés à l'aide d'associations SSID et d'identifiants de VLAN. Comme nous l'avons indiqué dans la section « Principes directeurs de l'architecture standard de WLAN avec VPN », le cryptage et l'authentification de couche 2 sont généralement désactivés pour les déploiements des WLAN VPN avec sécurité IP (IPsec). Toutefois l'administrateur peut, s'il le désire, activer ces fonctions. Dans le laboratoire de l'architecture SAFE, l'architecture de réseau WLAN VPN pour grande entreprise a été mise en œuvre en activant le cryptage de couche 2. Chaque utilisateur VPN est configuré avec un cryptage WEP à 128 bits, Cisco TKIP et code MIC (Message Integrity Check).

Figure A-15
Page récapitulative de la configuration VLAN d'un point d'accès VPN

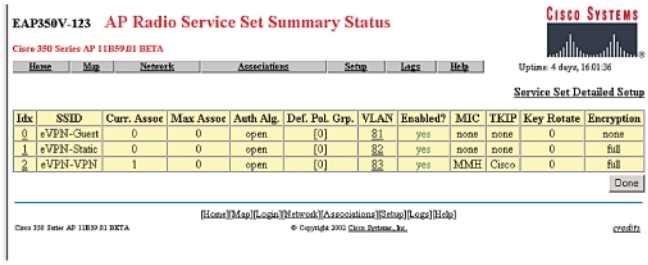


Comme nous l'avons indiqué dans la section « architecture », les utilisateurs VPN peuvent être placés sur des VLAN distincts en fonction de l'identificateur SSID avec lequel ils sont associés. Un VLAN d'administration (VLAN 80) a également été créé pour la gestion des points d'accès. Pour des détails supplémentaires, consultez le guide sur le déploiement des VLAN :

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

Une autre configuration possible consiste à créer des identificateurs SSID WEP d'invité (eVPN-Guest) et statiques (eVPN-Static) associés avec des VLAN et des profils de sécurité distincts afin de différentier l'accès utilisateur.

Figure A-16
Page récapitulative de la configuration Service Set d'un point d'accès VPN



Commutateurs de couche 3 Cisco Catalyst® 6506 (de eL3sw-5 et eL3sw-6) (interconnexion entre le module d'accès et le module de distribution) :

```
! Management VLAN for APs in the campus network
interface Vlan80
ip address 10.1.80.5 255.255.255.0
ip access-group 180 in
ip access-group 181 out
ip helper-address 10.1.11.50
no cdp enable

! VLAN for VPN users
interface Vlan83
ip address 10.1.83.5 255.255.255.0
ip access-group 182 in
ip access-group 183 out
ip helper-address 10.1.11.50
no cdp enable
```

Nous donnons ici les listes de contrôle d'accès pour le VLAN d'administration (interface 80) :

```
! Permit only authentication and accounting requests from AP to RADIUS server
access-list 180 permit udp host 10.1.80.122 gt 1023 host 10.1.20.54 eq 1645
access-list 180 permit udp host 10.1.80.122 gt 1023 host 10.1.20.54 eq 1646
access-list 180 permit udp host 10.1.80.123 gt 1023 host 10.1.20.54 eq 1645
access-list 180 permit udp host 10.1.80.123 gt 1023 host 10.1.20.54 eq 1646

! Permit only SNMP and TFTP traffic from wireless APs to WLSE* in out of band management network
access-list 180 permit udp host 10.1.80.122 eq snmp host 10.1.20.150
access-list 180 permit udp host 10.1.80.123 eq snmp host 10.1.20.150
access-list 180 permit udp host 10.1.80.122 host 10.1.20.150 eq tftp
access-list 180 permit udp host 10.1.80.123 host 10.1.20.150 eq tftp
```

```
! Permit outgoing web management traffic from AP to out of band management network
access-list 180 permit tcp host 10.1.80.122 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 180 permit tcp host 10.1.80.123 eq www 10.1.20.0 0.0.0.255 gt 1023 established

!Permit SSH traffic from the APs to out of band management network
access-list 180 permit tcp host 10.1.80.122 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
access-list 180 permit tcp host 10.1.80.123 eq 22 10.1.20.0 0.0.0.255 gt 1023 established

! Deny all other traffic
access-list 180 deny ip any any log

! Permit incoming web traffic from out of band management network to APs
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.122 eq www
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.123 eq www
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.122 eq 22
access-list 181 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.80.123 eq 22

! Permit only SNMP and TFTP traffic from WLSE to wireless APs
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.122 eq snmp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.123 eq snmp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.122 eq tftp
access-list 181 permit udp host 10.1.20.150 gt 1023 host 10.1.80.123 eq tftp

! Permit RADIUS responses from AAA Server to APs
access-list 181 permit udp host 10.1.20.54 eq 1645 host 10.1.80.122 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1645 host 10.1.80.123 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1646 host 10.1.80.122 gt 1023
access-list 181 permit udp host 10.1.20.54 eq 1646 host 10.1.80.123 gt 1023

! Deny all other IP traffic to APs
access-list 181 deny ip any host 10.1.80.122 log
access-list 181 deny ip any host 10.1.80.123 log
access-list 181 deny ip any any log
```

Nous donnons ici les listes de contrôle d'accès pour le VLAN VPN (interface 83) :

```
! Permit IPsec traffic to VPN gateway subnet
access-list 182 permit esp 10.1.83.0 0.0.0.255 10.1.50.0 0.0.0.255
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq isakmp 10.1.50.0 0.0.0.255 eq isakmp

! Permit full ICMP for troubleshooting
access-list 182 permit icmp 10.1.83.0 0.0.0.255 10.1.50.0 0.0.0.255

! Permit DHCP requests for initial IP assignment for wireless client
access-list 182 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq bootpc host 255.255.255.255 eq bootps
access-list 182 permit udp 10.1.83.0 0.0.0.255 eq bootpc host 10.1.11.50 eq bootps

! Deny all other traffic, don't log Windows file share broadcasts
access-list 182 deny udp 10.1.83.0 0.0.0.255 any eq netbios-ns
access-list 182 deny udp 10.1.83.0 0.0.0.255 any eq netbios-dgm
access-list 182 deny ip any any log

! Permit IPsec traffic from VPN gateway subnet to wireless subnet
access-list 183 permit esp 10.1.50.0 0.0.0.255 10.1.83.0 0.0.0.255
access-list 183 permit udp 10.1.50.0 0.0.0.255 eq isakmp 10.1.83.0 0.0.0.255 eq isakmp

! Permit Full ICMP for troubleshooting
access-list 183 permit icmp 10.1.50.0 0.0.0.255 10.1.83.0 0.0.0.255

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 183 permit udp host 10.1.11.50 eq bootps host 255.255.255.255 eq bootpc
access-list 183 permit udp host 10.1.11.50 eq bootps 10.1.83.0 0.0.0.255 eq bootpc

! Deny all other traffic
access-list 183 deny ip any any log
```

*Cisco Wireless LAN Solution Engine (WLSE) est un serveur dédié d'administration des réseaux sans fil qui permet la configuration et l'administration d'un réseau local sans fil de 500 points d'accès par unité. Cisco WLSE a été intégré dans l'architecture SAFE pour simplifier la configuration et l'administration de tous les points d'accès.

Nous donnons ici les caractéristiques de configuration de Cisco WLSE :

```
admin@wlse_safe:show config
hostname wlse_safe
interface ethernet0 192.168.253.150 255.255.255.0 default-gateway 192.168.253.57 up
ip domain-name safe-enterprise.com
ip name-server 10.1.11.50
!
snmp-server configuration:
RW community string: private
RO community string: public
!
telnet disabled
CLI auth: local
HTTP auth: local
admin@wlse_safe:show cdp run
!
CDP protocol is enabled...
broadcasting interval is every 60 seconds.
time-to-live of cdp packets is 180 seconds.
```

Veuillez noter que le protocole CDP (Cisco Discovery Protocol) a été activé car il appartient au réseau d'administration hors bande.

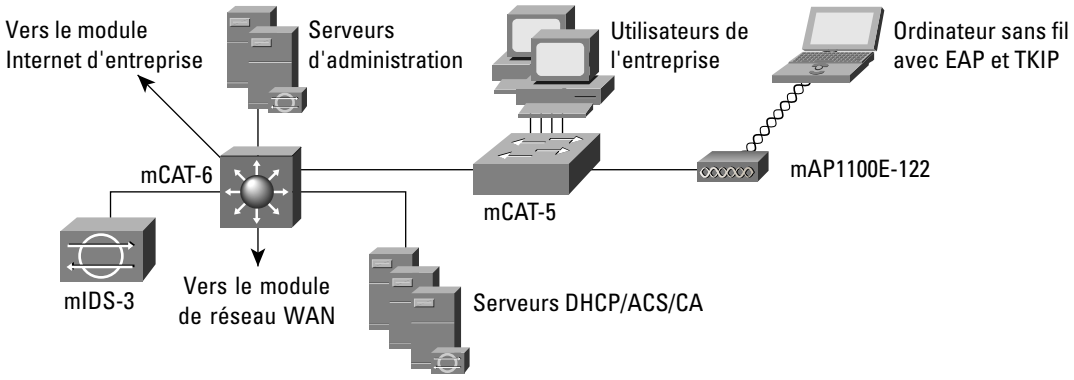
Configurations des réseaux de taille moyenne

Nous donnons dans cette section les configurations d'architecture EAP et VPN de bout en bout pour une architecture de réseau de taille moyenne.

Architecture EAP avec TKIP

Vous trouverez ci-dessous un cliché de configuration pour l'architecture SAFE WLAN EAP pour entreprise de taille moyenne. La Figure A-17 présente l'architecture WLAN EAP pour un réseau de taille moyenne.

Figure A-17
Architecture de réseau WLAN EAP pour entreprise de taille moyenne



Les produits utilisés dans cette architecture comprennent :

- un commutateur de couche 3 Cisco Catalyst (mCAT-6)
- un commutateur de couche 2 Cisco Catalyst (mCAT-5)
- un point d'accès et client Cisco Aironet (mAP1100E-122) et un client sans fil
- un serveur ACS (Access Control Server) (ACS v3.1)
- un serveur DHCP Windows 2000

Les sections suivantes présentent les caractéristiques de configuration de l'architecture SAFE WLAN pour réseau de taille moyenne (avec option EAP). Les principes directeurs généraux de configuration pour un réseau de taille moyenne sont décrits dans « SAFE : Extending the Security Blueprint to Small, Midsize, and Remote-User Networks »

Point d'accès et client Cisco Aironet (mAP1100E-122) et client sans fil :

Pour la configuration EAP des points d'accès Cisco Aironet et des clients sans fil, consultez les exemples de configuration de la section « Principes généraux » de la présente annexe. Dans le laboratoire de l'architecture SAFE, l'architecture de réseau WLAN EAP pour entreprise de taille moyenne a été mise en œuvre avec des VLAN sans fil. La présente section décrit les caractéristiques de la mise en œuvre des VLAN ainsi que celle de l'architecture de réseau WLAN EAP.

Sortie de l'interface de commande en ligne de mAP1100E-122 (AP1100) :

```
MAP1100E-120#sh run
!
ssid mEAP-EAP
vlan 73
authentication open eap eap_methods
authentication network-eap eap_methods
accounting acct_methods
!
ssid mEAP-Guest
vlan 71
authentication open
accounting acct_methods
guest-mode
!
ssid mEAP-Static
vlan 72
authentication open
accounting acct_methods
!
interface Dot11Radio0.73
encapsulation dot1Q 73
no ip route-cache
no cdp enable
bridge-group 73
```

```
bridge-group 73 subscriber-loop-control
bridge-group 73 block-unknown-source
no bridge-group 73 source-learning
no bridge-group 73 unicast-flooding
bridge-group 73 spanning-disabled
!
interface FastEthernet0.73
encapsulation dot1Q 73
no ip route-cache
no cdp enable
bridge-group 73
no bridge-group 73 source-learning
bridge-group 73 spanning-disabled
```

Comme le montre la sortie ci-dessus, les points d'accès de l'architecture de réseau de taille moyenne ont également été configurés avec de multiples identificateurs SSID (par mEAP-Guest, mEAP-Static, etc.) associés à des VLAN spécifiques et des profils de sécurité particuliers pour permettre la différentiation des utilisateurs.

Commutateur de couche 6506 Cisco Catalyst (mCAT-6) :

```
! Management (default) VLAN of the APs
interface Vlan70
ip address 10.3.70.1 255.255.255.0
ip access-group 170 in
ip access-group 171 out
ip helper-address 10.3.2.50
no ip redirects
no cdp enable

!Permit only authentication and accounting requests from AP to RADIUS server
access-list 170 permit udp host 10.3.70.120 gt 1023 host 10.3.8.253 eq 1645
access-list 170 permit udp host 10.3.70.120 gt 1023 host 10.3.8.253 eq 1646
! Permit outgoing web and SSH management traffic from AP to the out of band management network
access-list 170 permit tcp host 10.3.70.120 eq www 10.3.8.0 0.0.0.255 gt 1023 established
access-list 170 permit tcp host 10.3.70.120 eq 22 10.3.8.0 0.0.0.255 gt 1023 established

!Deny all other traffic
access-list 170 deny ip any any log

! Permit inbound management traffic (both http and SSH) to the AP
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq www
access-list 171 permit tcp 10.3.8.0 0.0.0.255 gt 1023 host 10.3.70.120 eq 22
```

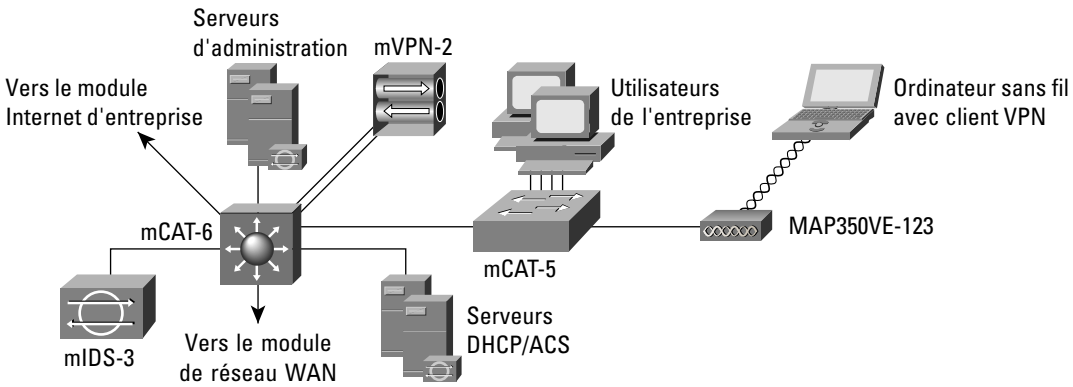
```
! Permit RADIUS responses from AAA Server to the AP
access-list 171 permit udp host 10.3.8.253 eq 1645 host 10.3.70.120 gt 1023
access-list 171 permit udp host 10.3.8.253 eq 1646 host 10.3.70.120 gt 1023

! EAP VLAN definition
interface Vlan73
ip address 10.3.73.1 255.255.255.0
ip access-group 172 in
ip access-group 173 out
ip helper-address 10.3.2.50
no ip redirects
no cdp enable

! Permit only BOOTP requests to pass through to DHCP server
access-list 172 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
!Deny access to the management VLAN of the AP from the EAP VLAN
access-list 172 deny ip 10.3.73.0 0.0.0.255 10.3.70.0 0.0.0.255 log
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 172 permit ip 10.3.73.0 0.0.0.255 any
!Deny all other traffic
access-list 172 deny ip any any log

! Permit DHCP responses for the initial IP assignment for the wireless client
access-list 173 permit udp host 10.3.2.50 eq bootps host 255.255.255.255 eq bootpc
! Permit all IP traffic from any destination to EAP VLAN in wireless network
access-list 173 permit ip any 10.3.73.0 0.0.0.255
!Deny all other traffic
access-list 173 deny ip any any log
```

Architecture VPN

Vous trouverez ci-dessous un cliché de configuration pour l'architecture SAFE WLAN VPN pour entreprise de taille moyenne. La Figure A-18 présente l'architecture WLAN VPN pour un réseau de taille moyenne.

Figure A-18

Architecture de réseau WLAN VPN pour entreprise de taille moyenne



Les produits utilisés dans cette architecture comprennent :

un commutateur de couche 3 Cisco Catalyst (mCAT-6)

un commutateur de couche 2 Cisco Catalyst (mCAT-5)

un point d'accès et client Cisco Aironet (mAP350V-123) et un client sans fil

un concentrateur de la gamme Cisco VPN 3000 (mVPN-2)

un serveur ACS (Access Control Server) (ACS v3.1)

un serveur DHCP Windows 2000

Cisco IDS Host Sensor

Point d'accès Cisco Aironet (mAP350V-123) et client sans fil :

Pour la configuration VPN des points d'accès Cisco Aironet et des clients sans fil, consultez les exemples de configuration de la section « Principes généraux » de la présente annexe.

Concentrateur de la gamme Cisco VPN 3000 (mVPN-2) :

Le concentrateur de la gamme Cisco VPN 3000 (mVPN-2) a été configuré de la manière suivante : l'interface publique est sur le même VLAN que celui de l'utilisateur VPN (mVPN-VPN), l'interface privée est sur un VLAN distinct et le relais DHCP du concentrateur VPN est activé pour permettre la transmission des requêtes DHCP en provenance des clients WLAN vers le serveur DHCP sur le réseau sans fil. Ainsi il n'est pas nécessaire de configurer la couche 3 sur le commutateur Catalyst (MCAT-6). Les Figures A-19 et A-20 présentent la configuration du concentrateur VPN.

Figure A-19
Configuration du concentrateur VPN

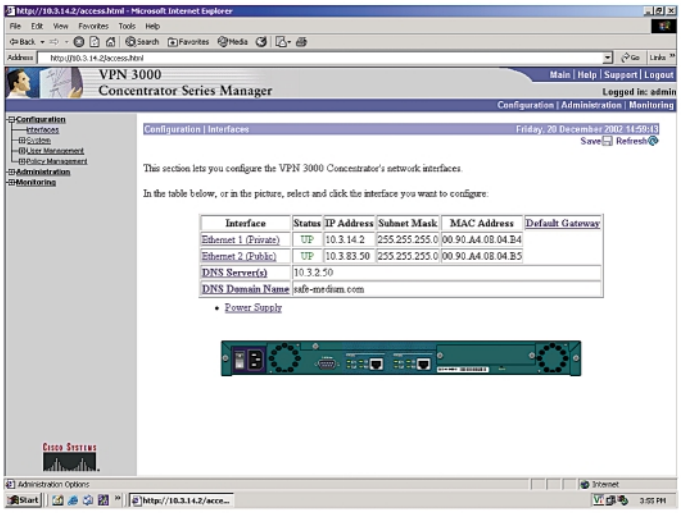
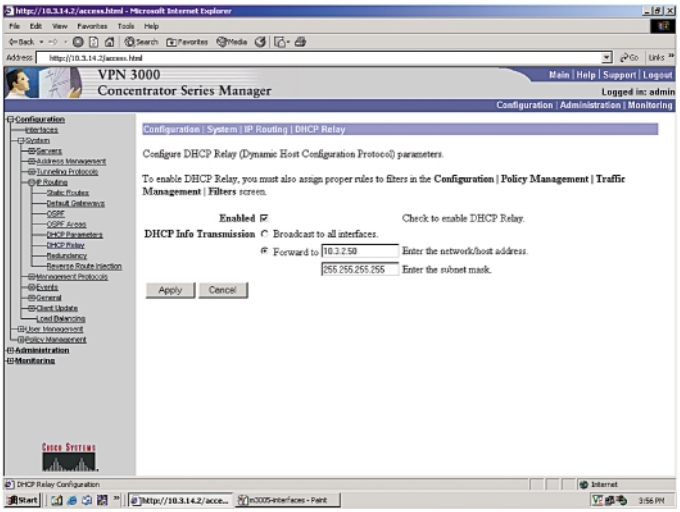


Figure A-20
Configuration du concentrateur VPN



Configuration pour petits réseaux et réseaux distants

Les configurations pour les petits réseaux et les réseaux distants ne sont pas fournies ici car ces architectures n'offrent pas d'éléments de configuration particuliers. Vous trouverez des conseils relatifs à ces architectures dans les recommandations générales au début de cette section.

Annexe B : Introduction à la sécurité des réseaux WLAN

Le sans fil est une nécessité

Les réseaux locaux sans fil (WLAN) développés autour de la norme 802.11 offrent la mobilité aux utilisateurs du réseau tout en leur garantissant la connectivité indispensable avec les ressources de l'entreprise. Les ordinateurs portables sont de plus en plus courants sur le lieu de travail et les utilisateurs les préfèrent à leurs machines habituelles car ils peuvent s'en servir pendant les réunions, les conférences et en voyage d'affaires. Les WLAN apportent aux organisations une meilleure productivité par employé en assurant le lien permanent avec les réseaux traditionnels dans des lieux où aucune connectivité n'était jusqu'à présent possible.

L'intérêt d'une connectivité de réseau sans fil ne se limite pas à l'entreprise. Les gains de productivité réalisés interviennent non seulement avant et après les réunions mais également en dehors de l'environnement classique du bureau. De nombreux fournisseurs de services Internet sans fil (WISP) font leur apparition dans les aéroports, les cafétérias, les hôtels et les centres de conférences ou les salons professionnels, et permettent aux utilisateurs d'entreprise de se connecter dans les lieux publics.

Les différents types de technologie sans fil

Les réseaux locaux sans fil existent depuis de nombreuses années, réalisant une connectivité vers les infrastructures filaires dans des environnements de travail spécifiques où la mobilité est indispensable. Ces premiers réseaux étaient appuyés sur deux technologies radio concourantes que nous décrirons par la suite : le saut de fréquences et le séquençage direct. Ces premiers réseaux sans fil n'étaient pas normalisés et leurs débits restaient entre 1 et 2 Mo. En l'absence de normes pour piloter les technologies WLAN, ces premières réalisations se limitaient aux implantations propres à chaque constructeur, sans souci d'interopérabilité – un facteur limitatif pour le développement de technologies WLAN normalisées. Plusieurs normes permettent actuellement la mise en œuvre d'applications WLAN : 802.11, HiperLAN, HomeRF SWAP et Bluetooth.

Description fonctionnelle

D'un point de vue fonctionnel, les WLAN se répartissent en trois grandes catégories : les réseaux locaux « peer-to-peer » sans fil, les réseaux locaux sans fil multicellulaires et les réseaux sans fil d'un bâtiment à l'autre (de point à point et de point à multipoint). Dans un réseau sans fil « peer-to-peer », les clients sans fil équipés de carte réseau sans fil communiquent entre eux sans passer par un point d'accès. Dans ce type de réseau, la zone de couverture est limitée et les clients sans fil n'ont pas accès aux ressources filaires. Le réseau local sans fil multicellulaire élargit la zone de couverture grâce à des cellules en recouvrement. La zone de couverture d'une cellule est déterminée par les caractéristiques du point d'accès (un pont sans fil) qui coordonne l'utilisation des ressources filaires par les clients sans fil.

Les réseaux sans fil de bâtiment à bâtiment répondent aux besoins de connectivité entre les réseaux locaux (bâtiments) d'un réseau campus. Il existe deux types de réseaux sans fil de bâtiment à bâtiment : les réseaux de point à point et de point à multipoint. Les réseaux sans fil de point à point d'un bâtiment à un autre sont des liaisons radio ou laser de point à point. Dans leur version radio, ils utilisent des antennes directionnelles pour concentrer la puissance du signal dans un faisceau étroit afin de maximiser la distance de transmission. Le pont laser d'un bâtiment à l'autre utilise un faisceau laser (généralement à infrarouge) comme porteuse pour les transmissions de données. Dans le réseau radio de point à multipoint, des antennes à faisceau large connectent plusieurs bâtiments (LAN) dans un réseau campus.

Bien que l'essentiel de ce document s'intéresse aux WLAN 802.11 que nous décrivons par la suite, il est intéressant de comprendre les autres normes sans fil actuellement sur le marché.

HiperLAN

HiperLAN est une norme de l'Institut européen des normes de télécommunications (ETSI) adoptée en 1996. La norme HiperLAN/1 opère dans la bande radio des 5 GHz jusqu'à 24 Mbits/s. L'ETSI a récemment adopté la norme HiperLAN/2, qui opère dans la bande des 5 GHz jusqu'à 54 Mbits/s et utilise un protocole orienté connexion pour le partage d'accès entre les terminaux utilisateurs.

HomeRF SWAP

Le groupe HomeRF SWAP Group a publié en 1988 le protocole normalisé SWAP (Shared Wireless Access Protocol) pour les communications numériques sans fil entre les PC et les appareils électroniques ménagers grand public. SWAP supporte la voix et les données sur une interface sans fil commune à des débits de 1 et 2 Mbits/s. Il utilise le saut de fréquence et les techniques à étalement de spectre dans la bande des 2,4 GHz.

Bluetooth

Bluetooth est un réseau humain (PAN) défini par le Bluetooth Special Interest Group qui fournit une connectivité sans fil basse puissance et à courte portée avec les technologies de sauts de fréquence et d'étalement de spectre sur la gamme des 2,4 GHz.

Technologie sans fil 802.11

L'IEEE assure le développement de la norme 802.11, ainsi que d'autres normes de réseau du type 802 comme Ethernet 802.3. Wi-Fi Alliance, une organisation à but non lucratif et indépendante des constructeurs, fournit une marque pour la technologie développée autour du 802.11 et plus connue sous le nom de Wi-Fi. Une unité compatible Wi-Fi doit passer avec succès des tests d'interopérabilité dans le laboratoire de Wi-Fi Alliance. Tous les produits certifiés Wi-Fi offrent une garantie de fonctionnement avec tous les autres produits certifiés Wi-Fi – quel qu'en soit le constructeur.

Les technologies sans fil développées autour du 802.11 exploitent le spectre radio utilisable par le grand public et connu sous le nom de bande ISM (Industrielle, Scientifique et Médicale). La norme 802.11 travaille spécifiquement dans deux des trois bandes de fréquences : la bande UHF de 2,4 GHz à 2,4835 GHz pour les réseaux 802.11 et 802.11b, et la bande SHF de 5,15 GHz à 5,825 GHz pour les réseaux 802.11a.

Ces gammes de fréquences sont classées sans licence, ce qui signifie qu'elles n'appartiennent à personne et que chacun peut les utiliser avec des appareils conformes aux réglementations de la FCC. Parmi les domaines régulés par la FCC figurent la puissance maximale d'émission des radios et le type de cryptage et de modulations de fréquence.

Méthodes radiofréquences pour réseau local sans fil

La bande ISM des 2,4 GHz, exploitée par le 802.11b, utilise la technologie à étalement de spectre. Cette technologie prévoit l'étalement des transmissions de données sur plusieurs fréquences car la bande des 2,4 GHz a d'autres bénéficiaires principaux, c'est-à-dire des entités qui ont acheté la bande pour leur propre usage ou ont légalement obtenu un accès prioritaire à ce spectre. Parmi les bénéficiaires principaux de la bande des 2,4 GHz figurent les fabricants de fours à micro-ondes. Ces appareils émettent dans la même gamme de fréquences mais à des puissances très nettement supérieures – une carte réseau 802.11 classique opère à 100 mW, contre 600 W pour un four à micro-ondes. Avec la technologie à étalement de spectre, en cas de recouvrement avec le bénéficiaire principal, celui-ci a ce que l'on peut véritablement appeler une « priorité de passage radiofréquence (RF) ».

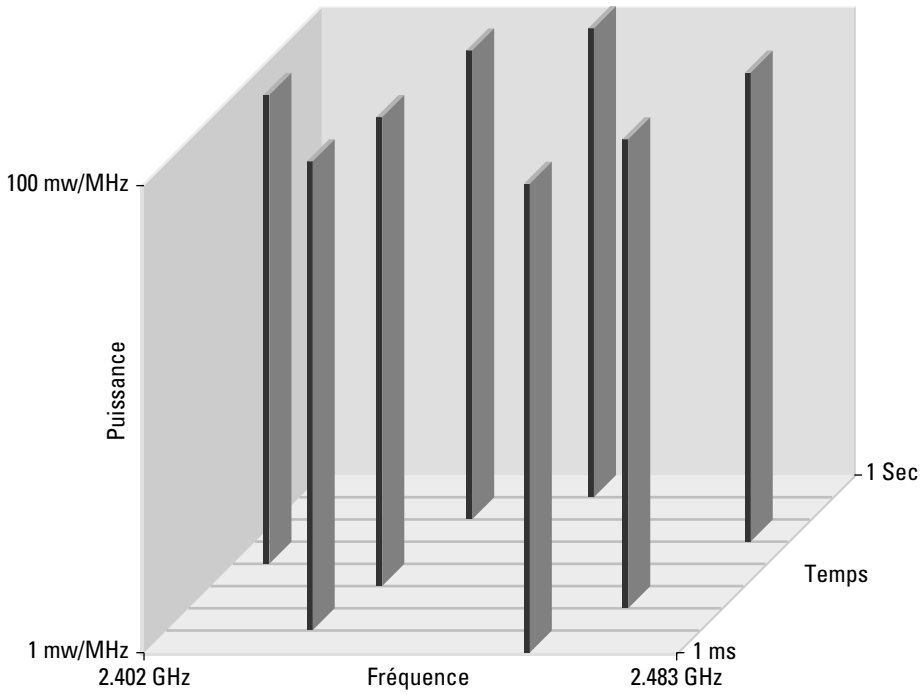
La norme 802.11 définit deux types distincts d'interfaces physiques de couche 1 pour les équipements radio. L'une s'appuie sur une architecture à sauts de fréquence tandis que l'autre exploite une démarche plus simple, monofréquence, appelée séquençage direct.

Sauts de fréquence

La bande ISM des 2,4 GHz offre 83,5 MHz de spectre de fréquence disponible. L'architecture à sauts de fréquence utilise la gamme de fréquences disponible en créant des modèles de sauts pour transmettre sur l'une des 79 fréquences de 1 MHz de largeur pendant 0,4 secondes au maximum (voir la Figure B-1). Ce système confère au réseau une tolérance aux interférences. Si l'un des canaux rencontre une interférence, celle-ci ne durera qu'un très bref laps de temps car la radio à sauts de fréquence pourra rapidement changer de fréquence pour réémettre ses données.

L'inconvénient majeur de la technologie à sauts de fréquence est que son débit ne peut dépasser 2 Mbits/s. Bien que l'on puisse placer des points d'accès à sauts de fréquence sur les 79 bandes accessibles par sauts, ce qui réduit la probabilité des interférences et offre un débit agrégé plus élevé, l'évolutivité des technologies à sauts de fréquence pose un problème de déploiement. Des travaux sont en cours sur le saut de fréquence sur bande large – une technologie qui promettrait des débits de l'ordre de 10 Mbits/s – mais ce concept ne fait pas encore l'objet d'une norme de l'IEEE.

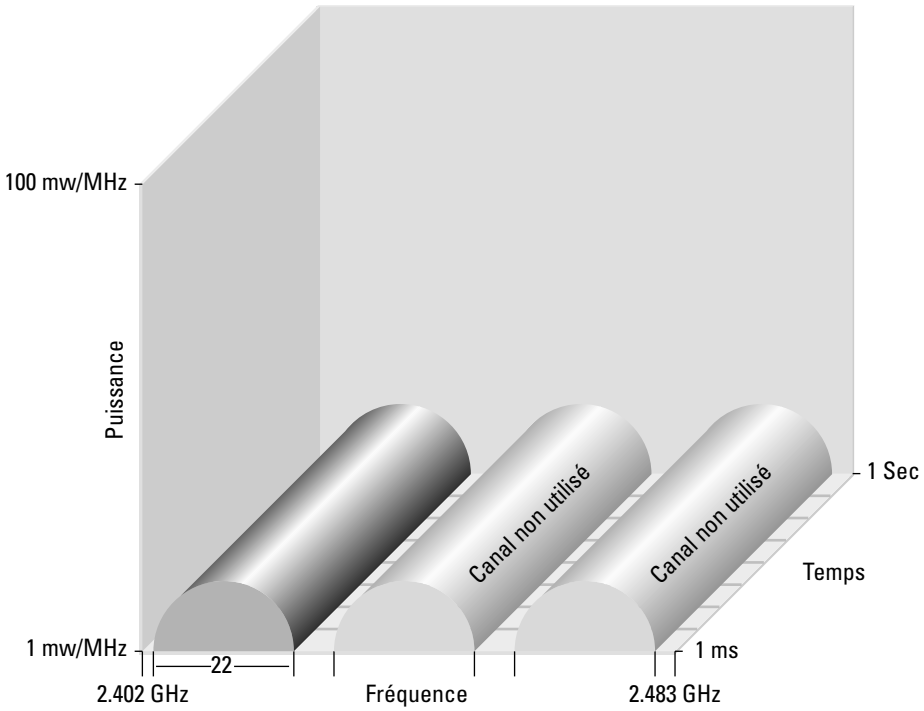
Figure B-1
Saut de fréquence



Le séquençage direct et le 802.11b

Les réseaux à séquençage direct ont une approche différente de la transmission de données. Dans ce mode, 11 canaux (13 en France) de 83 MHz se chevauchent sur le spectre des 2,4 GHz. Parmi ces 11 canaux (13 en France) se trouvent 3 canaux de 22 MHz de largeur qui ne se chevauchent pas (voir la Figure B-2). Grâce à sa grande largeur de bande ainsi qu'à la modulation évoluée reposant sur le procédé CCK (Complementary Code Keying), le séquençage direct supporte des débits de données plus élevés que le saut de fréquences. De plus, comme les trois canaux ne se chevauchent pas, trois points d'accès peuvent être utilisés de manière simultanée pour fournir un débit de données qui agrège les capacités des trois canaux disponibles. En 1999, l'IEEE a ratifié la norme 802.11b qui offrait des types de modulation nouveaux et plus élaborés pour permettre aux réseaux à séquençage direct d'atteindre des débits de 11 Mbits/s, soit 33 Mbits/s lorsque les trois canaux sans chevauchement sont utilisés ensemble. Le séquençage direct présente toutefois un inconvénient par rapport au saut de fréquence : son intolérance aux interférences. Même si les deux modes sont touchés par les interférences, le débit des réseaux à séquençage direct chute considérablement en présence de ce phénomène.

Figure B-2
Séquençage direct



Les réseaux 802.11a

L'IEEE a également adopté en 1999 une autre interface physique de couche 1 appelée 802.11a. La norme 802.11a utilise la bande SHF à 5 GHz pour fournir des débits pouvant atteindre 54 Mbits/s.

A la différence des normes 802.11 et 802.11b, le 802.11a utilise un type de multiplexage à division fréquentielle qualifié d'orthogonal (OFDM). Dans un système de multiplexage à division fréquentielle, la largeur de bande disponible est divisée en plusieurs porteuses de données. Les données à transmettre sont alors réparties entre ces sous-porteuses. Chaque porteuse est traitée indépendamment des autres et une bande de fréquence réservée doit être placée pour la protéger. Cette bande réservée réduit l'efficacité de la largeur de bande. En mode OFDM, plusieurs porteuses (ou tonalités) sont utilisées pour répartir les données en fonction du spectre disponible, comme pour le multiplexage à

division fréquentielle. Toutefois, dans un système OFDM, chaque tonalité est considérée comme orthogonale – c'est-à-dire indépendante ou sans relation – aux tonalités adjacentes et n'a donc pas besoin de bande réservée. Le mode OFDM offre ainsi une meilleure efficacité spectrale que le multiplexage à division fréquentielle ainsi qu'une bonne résistance aux interférences de radiofréquences et une plus faible distorsion multi-chemin.

La FCC a subdivisé en trois parties le spectre des 5 GHz, dans le cadre de l'infrastructure UNII (Unlicensed National Information Infrastructure). Chacune des trois bandes UNII dispose d'une largeur de 100 MHz et se compose de quatre canaux sans chevauchement de 20 MHz de large. Ainsi, chacun des canaux de 20 MHz comporte 52 sous-canaux de 300 kHz de largeur. Quarante-huit d'entre eux sont affectés à la transmission de données, tandis que les quatre suivants servent à la correction d'erreurs. Trois bandes UNII sont utilisables :

- Les unités UNII 1 opèrent dans la gamme de fréquence de 5,15 à 5,25 GHz. Leur puissance à l'émission est de 50 mW au maximum, le gain d'antenne ne peut dépasser 6 dBi et l'antenne et la radio doivent former une unité complète (pas d'antenne amovible). Les unités UNII 1 ne peuvent être utilisées qu'en intérieur.
- Les unités UNII 2 opèrent dans la gamme de fréquence de 5,25 à 5,35 GHz. Leur puissance à l'émission est de 250 mW au maximum, et le gain d'antenne ne peut dépasser 6 dBi. Contrairement aux unités UNII 1, les unités UNII 2 peuvent être utilisées à l'intérieur ou à l'extérieur et leurs antennes peuvent être amovibles. La FCC permet à un même appareil de couvrir les spectres UNII 1 et UNII 2 mais exige que, dans ce cas, l'unité soit conforme à la réglementation UNII 1.
- Les unités UNII 3 opèrent dans la gamme de fréquence de 5,725 à 5,825 GHz. Leur puissance maximale à l'émission est de 1 W et les antennes amovibles sont autorisées. Contrairement aux unités UNII 1 et UNII 2, les unités UNII 3 ne peuvent être utilisées qu'à l'extérieur. Dans ce cas, la FCC autorise une antenne de 23 dBi de gain pour les installations de point à point, et une antenne de 6 dBi pour les installations de point à multipoint.

Il est à noter qu'en Europe l'ETSI n'autorise actuellement que l'usage de la bande UNII-1 en intérieur à la condition que l'on implémente des mécanismes de contrôle de puissance (TPC) et de sélection de fréquences (DFS). Ces mécanismes sont définis dans le standard 802.11h, mais ne sont généralement pas encore disponible dans les équipements. Certains pays comme la France, tolèrent l'usage du 802.11a dans le bande UNII-1 sans ces mécanismes TPC et DFS (Voir ART – www.art-telecom.fr).

Roaming WLAN

Les spécifications 802.11 ne précisent aucun mécanisme particulier en ce qui concerne le roaming et chaque constructeur est libre de définir un algorithme pour permettre à ses clients WLAN de prendre les décisions de roaming.

Pour mieux comprendre le roaming sous 802.11, commençons par étudier l'architecture de réseau Ethernet 802.3. Les réseaux locaux Ethernet 802.3 utilisent l'architecture détection de porteuse avec accès multiple et détection de collisions (CSMA/CD). Lorsqu'une station souhaite transmettre des données vers une autre station, elle commence par vérifier si le médium est utilisé – la détection de porteuse de l'architecture CSMA/CD. Toutes les stations connectées au médium dispose d'un même accès à celui-ci – la partie « accès multiple » de CSMA/CD. Si la station constate que le médium est disponible, elle commence à transmettre. Si deux stations constatent que le médium est disponible et commencent à transmettre en même temps, il se produit une collision de trames qui rend inutilisables les données transmises. Les stations émettrices peuvent détecter les collisions – grâce à la fonction de détection de collisions de CSMA/CD – et exécutent un algorithme de retrait pour retransmettre leurs trames.

L'architecture Ethernet 802.3 a été conçue pour les réseaux filaires. Ses concepteurs ont supposé le médium filaire suffisamment fiable pour transmettre les trames d'une station émettrice vers la destination souhaitée. C'est pourquoi le 802.3 ne dispose d'aucun mécanisme pour déterminer si la trame a atteint la station de destination. La norme 802.3 s'appuie sur les protocoles de couches supérieures pour gérer la retransmission des trames.

Les réseaux 802.11 standard transmettent par voie aérienne et sont donc sujets à de nombreuses sources d'interférences. Les concepteurs de la norme 802.11 ont compris ce problème et élaboré une fonction d'acquittement sur la couche liaison qui notifie l'expéditeur que la destination a reçu la trame. A chaque trame transmise, la station de réception répond par une trame d'acquittement (ACK).

Les stations clients utilisent les messages ACK pour déterminer à quelle distance du point d'accès elles se trouvent. A mesure que la station émet ses données, elle s'attend à recevoir de la destination un message ACK dans un laps de temps donné. Lorsque ces messages ACK ne parviennent plus dans les délais prévus, le client sait qu'il s'est suffisamment éloigné du point d'accès et que les communications commencent à se détériorer.

Les points d'accès aussi envoient périodiquement des trames d'administration appelées trames Beacon. Les trames Beacon contiennent des informations propres au point d'accès comme l'identificateur SSID, les débits de données de support, le mode de transmission – saut de fréquence ou séquençage direct – supporté par le point d'accès, et la capacité. Les trames Beacon sont émises par le point d'accès à intervalles réguliers définis par l'administrateur.

Les trames ACK et Beacon fournissent à la station client un point de référence pour déterminer la nécessité d'une décision de roaming. Dès que le client a « manqué » un nombre prédéfini de messages Beacon, il peut considérer qu'il est sorti de la zone de couverture du point d'accès avec lequel il s'était associé. Il peut faire la même hypothèse lorsque les messages ACK attendus ne lui parviennent plus.

L'action de roaming par elle-même peut différer d'un constructeur à l'autre. En soi, cette action consiste à prendre la décision de roaming, puis à localiser un nouveau point d'accès auquel s'associer. Ce scénario peut comprendre l'initiation d'une nouvelle recherche de point d'accès, de la même manière que le client le fait lorsqu'il ouvre sa première connexion, ou d'autres méthodes comme se référer à une table acquise au cours de l'association précédente.

La fréquence du roaming des WLAN varie également selon les constructeurs mais dans la plupart des cas elle intervient plus d'une fois par seconde et, dans les meilleurs cas, plus d'une fois toutes les 200 millisecondes. Il est également important de rappeler que le roaming – qui est propre à chaque constructeur – entre des points d'accès de marques différentes peut intervenir à des fréquences différentes.

La sécurité sans fil

Conformément à la normalisation de l'IEEE, la sécurité des réseaux 802.11 s'appuie, en première analyse, sur deux composants principaux : le cryptage et l'authentification. De nombreux articles montrent que l'ensemble des professionnels de la sécurité s'accordent sur un point : la mise en œuvre de ces composants n'offre pas de garanties suffisantes de sécurité. Nous rappelons ici leur fonctionnement pour permettre au lecteur de mieux comprendre les défauts fondamentaux du système tels qu'ils sont présentés dans la section axiomatique de ce livre blanc.

Cryptage des trames

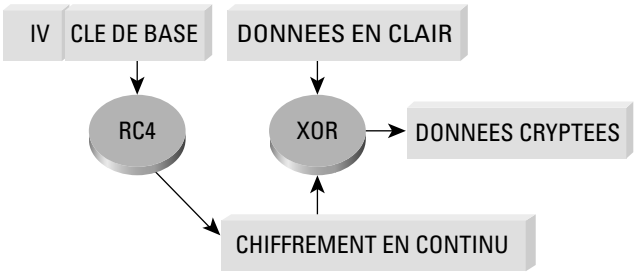
Un bon cryptage garantit la confidentialité des données. Le cryptage consiste à prendre un message, dit « en clair », et à le soumettre à un algorithme mathématique pour produire un texte « crypté ». Le décryptage est la transformation inverse. Les algorithmes de cryptage se servent le plus souvent d'une valeur, appelée clé, qui sert à crypter et à décrypter les données. Les deux principales méthodes de cryptage utilisées actuellement sont le cryptage symétrique (également appelé cryptage à clé partagée) et le cryptage asymétrique (également connu sous le nom de cryptage à clé publique ou à clé privée). Le cryptage symétrique est environ 1000 fois plus rapide que le cryptage asymétrique et est donc utilisé pour le cryptage en masse des données. De manière générale, lorsque l'algorithme de cryptage est bien conçu, la protection est d'autant plus grande que la clé est longue car le pirate devra utiliser davantage de « force brute » pour essayer toutes les clés possibles afin de décrypter le message. L'IEEE a spécifié que le protocole WEP (Wired Equivalent Privacy) serait utilisé pour crypter les trames de données 802.11. Le cryptage WEP utilise le chiffrement continu RC4 inventé par Ron Rivest de RSA Data Security, Inc. (RSADSI). L'algorithme de cryptage RC4 est un chiffrement en continu symétrique qui supporte les clés de longueur variable. Le chiffrement en continu consiste à exécuter la fonction de cryptage ou de décryptage sur une unité du texte en clair (dans ce cas, la trame 802.11b). Ce mode est différent du chiffrement par bloc qui traite un nombre prédéfini d'octets en cryptage ou en décryptage. Dans le cryptage symétrique, la clé est un élément d'information qui doit être partagé par les unités d'extrémité pour réaliser le cryptage et le

décryptage. RC4 autorise une clé de longueur variable, qui peut atteindre 256 octets – contrairement à d'autres algorithmes dont la clé a une longueur fixe. L'IEEE a spécifié que les unités 802.11 devaient supporter les clés de 40 bits, avec la possibilité d'accepter des clés plus longues. Plusieurs constructeurs proposent le cryptage WEP à 128 bits dans leurs solutions WLAN.

Le protocole WEP est un chiffrement en continu, et il est indispensable de disposer d'un mécanisme pour garantir que le même texte en clair ne générera pas le même texte crypté. L'IEEE a stipulé l'utilisation d'un vecteur d'initialisation qui doit être concaténé avec la clé symétrique avant de générer le texte crypté en continu.

Ce vecteur d'initialisation est un nombre de 24 bits – qui prend donc une valeur entre 0 et 16 777 215. L'IEEE suggère – mais n'exige pas – de modifier le vecteur d'initialisation pour chaque trame. Comme l'émetteur génère le vecteur d'initialisation sans schéma ni calendrier prédéfini, ce vecteur doit être envoyé en clair au récepteur, dans la partie en-tête de la trame de données 802.11. Le récepteur peut ensuite concaténer le vecteur d'initialisation reçu avec la clé WEP (la clé de base) stockée localement pour décrypter la trame de données. Comme le montre la Figure B-3, l'algorithme RC4 ne crypte pas le texte en clair lui-même mais sert à générer un flux de clé unique pour la trame de données 802.11 concernée en reprenant le vecteur d'initialisation et la clé de base comme clé de cryptage. Le flux de clé unique ainsi obtenu est ensuite combiné avec le texte en clair et le tout est transformé par une fonction mathématique appelée XOR qui produit le texte chiffré.

Figure B–3
Processus de cryptage WEP



Mécanisme d'authentification

L'IEEE a spécifié deux algorithmes d'authentification pour les réseaux 802.11. Le premier type est une authentification ouverte qui correspond à un algorithme nul : toute station qui demande une authentification obtient un accès. La seconde forme d'authentification est dite « à clé partagée » et exige que la station qui demande et celle qui accorde l'accès soient toutes deux configurées avec des clés WEP identiques. La première station envoie une demande d'authentification à la deuxième qui lui renvoie une trame test en clair. Le demandeur crypte la trame test avec sa clé WEP et la renvoie à la station d'authentification. Celle-ci tente de décrypter la trame : si le texte décrypté correspond au texte en clair initialement envoyé, elle en conclut que le demandeur possède une clé WEP valide et lui accorde l'accès.

Notez que l'authentification à clé partagée présente un défaut conceptuel connu. Le paquet test est en effet envoyé en clair au demandeur qui renvoie un texte crypté : le pirate peut donc déduire le code de chiffrement en analysant les deux textes. Cette information peut permettre de créer des dictionnaires de décryptage associés à la clé WEP en question. La section axiomatique de ce document présente les problèmes de sécurité connus du protocole WEP tel qu'il est normalisé par l'IEEE.

Composants des réseaux locaux sans fil

Un réseau local sans fil se compose de points d'accès, de cartes réseaux ou de cartes clients, de ponts et d'antennes.

- Point d'accès – Un point d'accès opère dans une gamme de fréquence donnée et utilise une technique de modulation prévue par la norme 802.11. Il informe également les clients sans fil de sa disponibilité et assure les fonctions d'authentification et d'association des clients sans fil auprès du réseau WLAN. Un point d'accès coordonne également l'utilisation des ressources filaires par les clients sans fil.
- Carte réseau ou carte client – Un PC ou un poste de travail utilise une carte réseau sans fil pour se connecter au réseau WLAN. La carte réseau balaye le spectre de fréquences disponibles à la recherche d'une connectivité et s'associe à un point d'accès ou à un autre client sans fil. La carte réseau est couplée au système d'exploitation du PC ou du poste de travail par l'intermédiaire d'un pilote logiciel.
- Point – Les ponts sans fils servent à connecter plusieurs réseaux locaux (LAN) filaires ou sans fil au niveau de la couche MAC (Media Access Control). Utilisé dans les connexions sans fil de bâtiment à bâtiment, les ponts sans fil ont une zone de couverture plus élargie que celle des points d'accès. Notez que la norme IEEE 802.11 limite à 1,6 km (1 mile) la portée maximale d'un point d'accès.
- Antenne – L'antenne émet le signal modulé dans l'air pour permettre aux clients sans fil de le recevoir. Les caractéristiques d'une antenne sont définies par son mode de propagation (directionnelle ou omnidirectionnelle), son gain, sa puissance à l'émission, etc. Les points d'accès, les ponts et les clients sans fil ont besoin d'une antenne.

Annexe C – Autres informations sur les points d'accès illégaux

Comme nous l'avons déjà exposé dans ce document, il est possible de réduire les menaces que représentent les points d'accès illégaux. Nous donnons dans cette annexe des conseils détaillés pour minimiser le risque que les points d'accès illégaux font courir aux réseaux d'entreprise. Les méthodes préconisées comprennent :

La prévention

- Politique d'entreprise
- Sécurité matérielle
- Infrastructure WLAN supportée
- Sécurité à la norme 802.1X au niveau des ports sur les commutateurs de périphérie

La détection

- Utilisation d'analyseurs de réseau sans fil
- Utilisation d'outils avec script sur l'infrastructure filaire
- Observation physique du placement et de l'utilisation des points d'accès sans fil

Vous trouverez à la fin de cette annexe une liste des analyseurs de réseau sans fil et les adresses MAC (Media Access Control) connues. Cette information peut vous aider à détecter et à prévenir les points d'accès illégaux.

La prévention des points d'accès illégaux

Pour le service informatique de l'entreprise, la priorité doit être de commencer par prévenir l'installation de points d'accès illégaux. La prévention des points d'accès illégaux passe par l'association des éléments suivants :

- la rédaction et la publication d'une politique de sécurité interdisant aux employés d'installer tout type d'équipement de réseau local sans fil (WLAN),
- la mise en place d'une sécurité matérielle,
- la mise en place d'une infrastructure WLAN supportée – afin que les employés n'aient plus de raison d'installer leurs propres équipements,

- la mise en œuvre d'une sécurité IEEE 802.1X au niveau des ports,
- l'utilisation de filtres sur les commutateurs de couches 2 et 3.

Rédaction d'une politique WLAN pour l'entreprise

La rédaction d'une politique d'entreprise sur les installations WLAN est une première étape cruciale pour prévenir les points d'accès illégaux. Cette politique WLAN doit préciser les personnes autorisées à installer des points d'accès WLAN et la liste des mesures de sécurité à respecter pour ces installations. La politique WLAN doit par exemple prévoir les méthodes de sécurité utilisées par le point d'accès pour réaliser une connectivité client sécurisée.

Sécurité matérielle

La sécurité matérielle joue également un rôle dans la prévention des points d'accès illégaux. Des normes de sécurité matérielle doivent être établies pour éviter qu'une personne puisse pénétrer sans autorisation dans les locaux de l'entreprise, ou pour détecter un intrus s'il parvenait à entrer.

Mise en place d'une infrastructure WLAN supportée

La plupart des points d'accès illégaux sont installés par des personnes « bien intentionnées », généralement des utilisateurs internes frustrés de ne pas disposer de ce type d'accès : le meilleur moyen de prévenir ces installations illégales consiste à supprimer leur motivation en réalisant un réseau WLAN géré, supporté et sécurisé sur l'ensemble de l'entreprise. Les utilisateurs qui posent un point d'accès non autorisé cherchent le plus souvent à obtenir une couverture sans fil là où aucune n'existe officiellement – par exemple dans une salle de réunion, une cafétéria, une esplanade ou dans d'autres parties communes. Le faible coût des points d'accès que l'on trouve aisément dans le commerce a rendu particulièrement simple ce type d'installation. Le danger provient de ce que la personne qui installe le point d'accès ignore le plus souvent quelles sont les fonctions de sécurité nécessaires pour empêcher des éléments extérieurs d'accéder au réseau de son entreprise. Par ailleurs les points d'accès grand public généralement utilisés ne possèdent pas les fonctions suffisantes pour fournir un niveau de sécurité de qualité entreprise.

Utilisation de la norme IEEE 802.1X

Les commutateurs de couche d'accès les plus récents supportent une norme IEEE appelée 802.1X qui offre une sécurité au niveau des ports. Lorsque le 802.1X est activé sur les commutateurs et les points d'accès de la périphérie du réseau, aucune unité ne peut être connectée à moins de s'authentifier conformément à la norme 802.1X auprès d'un serveur RADIUS (Remote Access Dial-In User Service) placé derrière le commutateur. Nous recommandons que le 802.1X ne soit désactivé que sur les ports de commutation des points d'accès autorisés. Ceci impose par conséquent l'authentification utilisateur de type 802.1X au niveau de la périphérie filaire et sans fil de l'entreprise. Une étude plus détaillée de la technologie 802.1X est présentée plus loin dans ce document à la section « Extensions de sécurité : une nécessité ».

Utilisation de filtres sur les commutateurs de couches 2 et 3

Nous étudions dans cette section comment utiliser les caractéristiques des commutateurs de couches 2 et 3 pour prévenir l'installation de points d'accès illégaux. Le Tableau C-1 donne la liste des méthodes analysées.

Tableau C-1 Méthodes analysées

Méthode	Résumé de la méthode
Utilisation des filtres de commutateurs Cisco Catalyst pour limiter le nombre d'adresses MAC par port	En limitant le nombre d'adresses MAC qui peuvent être utilisées sur un port, on empêche le commutateur de laisser passer le trafic en provenance des clients des points d'accès illégaux.
Utilisation des filtres des commutateurs Cisco Catalyst pour rejeter les trames provenant des points d'accès tiers	Nous avons étudié la possibilité de configurer le commutateur pour qu'il rejette les trames provenant des points d'accès et des cartes réseaux fournies par des constructeurs tiers. Cette option s'est avérée irréalisable car les commutateurs ne supportent pas les masques génériques sur les filtres d'adresses MAC.

Limitations de la capacité des filtres à empêcher les points d'accès illégaux de se connecter au réseau d'entreprise

- Les filtres destinés à bloquer les points d'accès d'un constructeur bloquent également les cartes réseaux de ce constructeur. Par exemple, si les points d'accès de la marque A sont bloqués, ses cartes réseaux Ethernet le seront aussi.
- Le trafic qui provient d'un point d'accès porte l'adresse MAC de la carte réseau sans fil, pas celle du point d'accès. Par exemple, si un point d'accès de la marque A est connecté à un port qui filtre les adresses MAC de cette marque, il sera malgré tout en mesure de laisser passer le trafic d'une carte réseau sans fil de la marque B ou C. Une solution à ce problème serait – à la condition qu'il soit possible d'utiliser des masques génériques MAC – d'utiliser une commande de fermeture du port en présence d'une adresse MAC non autorisée.
- Parmi les constructeurs de points d'accès WLAN, certains disparaîtront et de nouveaux entreront sur le marché, mais il n'existera jamais une liste faisant autorité de tous les identifiants uniques d'organisation OUI des constructeurs de points d'accès avec leurs adresses MAC.
- Les adresses MAC peuvent être modifiées ou usurpées.

Détection des points d'accès illégaux

En plus des mécanismes de prévention des points d'accès illégaux décrits dans la précédente section, l'administrateur de sécurité informatique devrait combiner les méthodes de détection suivantes :

- Détection sans fil des points d'accès illégaux
- Détection sans fil des points d'accès illégaux à partir du réseau filaire
- Détection des points d'accès illégaux par l'observation

Détection sans fil des points d'accès illégaux

Ce processus utilise du matériel et des logiciels de réseau sans fil pour détecter les points d'accès illégaux.

Le Tableau C-2 présente les avantages et les inconvénients de la détection sans fil des points d'accès illégaux.

Tableau C-2 Avantages et inconvénients de la détection sans fil des points d'accès illégaux

Avantages de la détection sans fil	Problèmes éventuels avec la détection sans fil
• Repère souvent des points d'accès illégaux que les autres méthodes ne détectent pas. • Très efficace pour détecter les points d'accès installés par des utilisateurs internes sans mauvaise intention (options de sécurité par défaut ou transmission de l'identificateur SSID).	• La méthode exige que l'unité WLAN soit à portée du point d'accès pour pouvoir le détecter et peut obliger un responsable de la sécurité informatique à parcourir à pied l'ensemble du campus d'entreprise, un analyseur sans fil à la main. • De nombreux outils ne « voient » pas les points d'accès qui ne transmettent pas leur identificateurSSID. • Les sites distants sont plus difficilement analysables par le responsable de la sécurité. • Les signaux des points d'accès WLAN peuvent être difficiles à capter car certains matériaux de construction bloquent les signaux 802.11.

Il existe un grand nombre d'analyseurs WLAN sur le marché et tous sont capables, avec des réussites différentes, de détecter les points d'accès illégaux. La section « Analyseurs sans fil » de cette annexe donne une liste de plusieurs appareils qui peuvent être utilisés à cet effet. Une antenne directionnelle est une aide précieuse pour localiser précisément un point d'accès supposé illégal et détecté par l'analyseur WLAN.

Détection sans fil des points d'accès illégaux à partir du réseau filaire

Les points d'accès illégaux peuvent être détectés à partir du réseau filaire en utilisant :

- les adresses MAC
- la reconnaissance de systèmes d'exploitation (OS fingerprinting)
- le protocole SNMP (Simple Network Management Protocol)
- la détection des intrusions

Il existe un grand nombre d'outils logiciels qui vous aident à détecter les points d'accès illégaux à partir d'un poste filaire d'administration sur la partie Ethernet du réseau.

Le Tableau C-3 présente les avantages et les inconvénients de la détection filaire des points d'accès illégaux.

Tableau C-3 Avantages et inconvénients de la détection filaire des points d'accès illégaux

Avantages	Inconvénients
• Il est plus facile de surveiller le réseau en «temps réel». • La méthode utilise des scripts automatisés et demande donc moins de personnel. • Elle permet de surveiller les sites distants.	• Cette méthode risque de « manquer » certains points d'accès illégaux. • La plupart des logiciels n'ont pas atteint un haut niveau de maturité ou n'ont pas été spécifiquement écrits pour la détection des points d'accès illégaux. • La méthode peut générer un grand nombre de faux positifs sur les systèmes de détection des intrusions et les pare-feu personnels.

Utilisation des adresses MAC

Les outils de contrôle qui surveillent les adresses MAC détectent les points d'accès illégaux en recherchant une adresse MAC connue ou en cataloguant toutes les adresses MAC autorisées sur le réseau et en en recherchant de nouvelles. Cette dernière méthode présente l'avantage de déclencher l'alerte lorsqu'une unité non autorisée – autre qu'un point d'accès – comme un ordinateur portable, est connectée au réseau. Elle présente toutefois des problèmes importants de faux positifs. Le Tableau C-4 donne une liste d'outils de surveillance des adresses MAC connues.

Tableau C-4 Outils de surveillance des adresses MAC connues

Access Point tools	• http://aptools.sourceforge.net/wireless.ppt • http://aptools.sourceforge.net/ Access point tools repère un point d'accès en fonction de son adresse MAC et vérifie qu'il s'agit bien d'un point d'accès – et non d'une carte réseau sans fil – à l'aide du protocole http (Hypertext Transfer Protocol). Ce produit peut également vérifier les paramètres de sécurité (WEP) et SNMP par HTML.
Arpwatch	• http://www-nrg.ee.lbl.gov/ Arpwatch surveille l'activité Ethernet et conserve une base de données des couples d'adresses Ethernet et IP ; il peut également signaler certaines modifications par e-mail.

Reconnaissance des systèmes d'exploitation (OS Fingerprinting)

Ces outils peuvent servir à prendre les « empreintes digitales » d'un système d'exploitation comme celui qui s'exécute sur un point d'accès. Cette reconnaissance s'appuie sur l'observation des caractéristiques propres à chaque système d'exploitation, comme la manière dont ils répondent aux paquets TCP arborant d'obscurs options ou indicateurs TCP. Les outils de reconnaissance de système d'exploitation sont capables d'identifier correctement certains points d'accès, mais ils ne peuvent associer le système d'exploitation à un point d'accès illégal que s'ils disposent d'une empreinte digitale du système utilisé par son constructeur. Le Tableau C-5 donne la liste des outils connus de reconnaissance par empreintes digitales.

Tableau C-5 Outils connus de reconnaissance par empreintes digitales

NMAP	• http://www.insecure.org/nmap/index.html • http://www.insecure.org/nmap/nmap-fingerprinting-article.html NMAP est un outil bien connu et d'excellente réputation ; s'il n'a pas été habilité en tant qu'outil de détection des points d'accès illégaux, il peut toutefois être utile en association avec d'autres techniques de détection. Il génère un grand nombre d'alertes sur les systèmes de détection des intrusions et sur les pare-feu personnels.
Xprobe	• http://www.sys-security.com/html/projects/X.html Xprobe 1 associe différentes méthodes actives de reconnaissance des systèmes d'exploitation à distance en utilisant le protocole ICMP (Internet Control Message Protocol) qui s'est avéré au cours du projet de recherche «ICMP Usage in Scanning» un moyen simple, rapide, efficace et puissant pour détecter le système d'exploitation sous-jacent utilisé par un hôte ciblé. Xprobe 2 est un outil actif de reconnaissance de système d'exploitation qui repose sur une autre approche de la méthode ; il s'appuie sur la reconnaissance floue des signatures, la reconnaissance probabiliste, les appariements multiples et simultanés et une base de données de signatures. Xprobe n'a pas été habilité en tant qu'outil de détection des points d'accès illégaux, il peut toutefois être utile en association avec d'autres techniques de détection. Il génère un grand nombre d'alertes sur les systèmes de détection des intrusions et sur les pare-feu personnels.

Utilisation du protocole SNMP

SNMP n'a pas la réputation d'un moyen efficace de détection des points d'accès illégaux. Sur la plupart des points d'accès illégaux, il y a peu de chances que le protocole SNMP soit activé et même s'il l'est, il est peu probable que les identifiants de communauté SNMP soient reconnus. Si un outil SNMP est nécessaire pour la détection des points d'accès illégaux, les paquets d'administration du réseau d'entreprise doivent avoir la possibilité d'effectuer une découverte IP et SNMP.

Détection matérielle des points d'accès illégaux

L'administrateur de sécurité informatique peut également détecter une activité WLAN illégale en observant l'environnement de travail d'un point de vue matériel. Il doit rester vigilant :

- à la présence visible de points d'accès WLAN non autorisés,
- aux employés qui utilisent un accès WLAN là où ils ne sont pas sensés disposer de ce type d'accès,
- aux « signes de piste » qui signalent la disponibilité d'un accès WLAN (pour plus d'informations, voir http://www.warchalking.org/)

En résumé, les méthodes actuelles de prévention ou de détection des points d'accès illégaux sont limitées lorsqu'elles sont utilisées seules. Nous recommandons aux architectes réseaux de prévoir une combinaison d'outils de prévention et de détection pour leurs réseaux. Comme nous l'avons vu, chaque outil de prévention ou de détection possède des capacités différentes. L'architecte peut les combiner pour se fabriquer une panoplie complète et raisonnablement efficace.

Analyseurs sans fil

Le Tableau C-6 présente la liste des analyseurs sans fil couramment utilisés.

Tableau C-6 Liste des analyseurs sans fil

Airmagnet	• www.airmagnet.com Produit commercial, Airmagnet est un outil d'analyse de site WLAN possédant toutes les fonctions nécessaires et qui s'exécute sur un Compaq iPaq.
Boingo	• www.boingo.com Boingo est un logiciel gratuit que vous pouvez télécharger sur Internet; il recherche tous les réseaux disponibles et vous avertit lorsque vous êtes dans la zone de couverture d'un signal de service à haute vitesse – ou vous indique où trouver le signal le plus proche.
Netstumbler	• http://www.netstumbler.org/ Très répandu et bien connu, Netstumbler est un logiciel gratuit que vous pouvez télécharger sur Internet ; il détecte les points d'accès WLAN et fournit diverses informations sur eux.
Sniffer	• www.sniffer.com Cet analyseur sans fil professionnel peut être utilisé pour rechercher les points d'accès illégaux en définissant des filtres pour la recherche de trames Beacon, mais en excluant les identificateurs SSID autorisés, ou des filtres qui recherchent les identifiants uniques d'organisation (OUI) MAC des constructeurs connus de points d'accès.
Wildpackets	• http://www.wildpackets.com/products/airopeek Cet analyseur sans fil professionnel peut être utilisé pour rechercher les points d'accès illégaux en définissant des filtres pour la recherche de trames Beacon, mais en excluant les identificateurs SSID autorisés, ou des filtres qui recherchent les identifiants uniques d'organisation (OUI) MAC des constructeurs connus de points d'accès.

Tableau C-6 Liste des analyseurs sans fil

Observer	• http://www.networkinstruments.com/ Cet outil peut être utilisé pour rechercher les points d'accès illégaux en définissant des filtres pour la recherche de trames Beacon, mais en excluant les identificateurs SSID autorisés, ou des filtres qui recherchent les identifiants uniques d'organisation (OUI) MAC des constructeurs connus de points d'accès.
Finisar Surveyor	• http://www.gofinisar.com/products/protocol/wireless/surveyor_w.html Cet outil peut être utilisé pour rechercher les points d'accès illégaux en définissant des filtres pour la recherche de trames Beacon, mais en excluant les identificateurs SSID autorisés, ou des filtres qui recherchent les identifiants uniques d'organisation (OUI) MAC des constructeurs connus de points d'accès.
Wellenreiter	• http://www.remote-exploit.org/ Analogue à Netstumbler mais moins répandu et moins réputé, Wellenreiter détecte les points d'accès WLAN et fournit des informations sur eux.
Kizmet	• http://www.kismetwireless.net/ Kismet est un analyseur sans fil à source ouvert qui peut être utilisé pour la détection des points d'accès illégaux en définissant des filtres de recherche de trame Beacon mais en excluant les identificateurs SSID autorisés.
dachb0den	• http://www.dachb0den.com/projects/bsd-airtools.html Cet outil, qui n'est pas très connu, semble combiner les fonctionnalités de Netstumbler et de Airsnort.
Hornet	• http://www.bvsystems.com/Products/WLAN/Hornet/hornet.htm Matériel dédié qui effectue des recherches à partir d'une liste d'adresses MAC de points d'accès configurés que l'on télécharge à partir d'un PC. Il ne semble pas faire beaucoup plus que ce que fait un analyseur sans fil.
IBM Distributed Wireless Security Auditor	• http://www.research.ibm.com/gsal/dwsa/ Cet outil est un prototype : il n'est pas disponible à la vente. Il utilise le logiciel client des cartes réseaux d'entreprise pour détecter et signaler tous les points d'accès et leur système de sécurité ; un système d'arrière guichet compare la liste des points d'accès détectés avec celle des points d'accès autorisés et signale les points d'accès inconnus. Cet outil également est susceptible de déclencher des faux positifs.
IBM TP General—IBM Access Connections for Windows 2000/XP	• http://www.pc.ibm.com/qtechinfo/MIGR-4ZLNJB.html Access Connections est un assistant de connectivité pour les ordinateurs ThinkPad. Il permet de basculer rapidement les paramètres de réseau et Internet en sélectionnant un profil de site. Les paramètres réseaux et Internet peuvent être définis dans un profil (Location Profile) pour unités de réseau modem ou LAN filaire ou WLAN, que vous restaurez lorsque vous en avez besoin. En basculant le profil de site, vous pouvez vous connecter instantanément au réseau sans avoir à reconfigurer vos paramètres lorsque vous passez du bureau à votre domicile ou lorsque vous êtes en déplacement.

Adresses MAC connues pour les points d'accès

Le Tableau C-7 fournit une liste partielle des identifiants uniques d'organisation (OUI) MAC utilisés par les constructeurs de points d'accès. Cette liste provient du site aptools à l'adresse aptools.sourceforge.net.

Tableau C-7 Identifiants OUI MAC utilisés par les constructeurs de points d'accès

Fabricant	Plage d'adresses MAC
3Com	0001.03l0004.76l0050.dal0800.02
Addtron	0040.33l0090.d1
Advanced Multimedia Internet	0050.18
Apple	0030.65
Atmel	0004.25
Bay Networks	0020.d8
BreezeNet	0010.e7
Cabletron (Enterasys)	0001.f4l00e0.63
Camtec	0000.ff
Cisco Aironet	0040.96
Compaq	0050.8b
D-Link	0005.5dl0040.05l0090.4b
Delta Networks	0030.ab
Intel	0002.b3
Linksys	0003.2fl0004.5a
Lucent	0002.2dl0060.1dl0202.2d
Nokia	00e0.03
Samsung	0000.f0l0002.78
Senao Intl	0002.6f
SMC	00e0.29l0090.d1
SOHOware	0080.c6
Sony	0800.46
Symbol	00a0.f8l00a0.0f
Z-Com	0060.b3
Zoom	0040.36

Annexe D – Disponibilité de réseau

Les sections suivantes décrivent en détail divers éléments que vous devrez envisager pour déployer des services sur un réseau local sans fil WLAN sans compromettre sa sécurité. Notez que pour les architectures de réseau distant, de petite taille ou de taille moyenne, le schéma directeur Cisco SAFE pour la sécurité des réseaux filaires ne prévoit pas la notion de haute disponibilité, et qu'elle n'est pas non plus prise en compte pour les réseaux sans fil.

Protocole DHCP (Dynamic Host Configuration Protocol)

- *Requêtes par seconde* – Le matériel et le logiciel serveur DHCP (Dynamic Host Configuration Protocol) doivent être capables de traiter le nombre prévu de nouvelles requêtes DHCP par seconde associées à l'introduction d'un réseau WLAN. Si le serveur DHCP est surchargé, les utilisateurs sans fil ne pourront pas obtenir d'adresse DHCP : les utilisateurs EAP (Extensible Authentication Protocol) ne pourront pas obtenir de connectivité IP après leur authentification et les utilisateurs IPsec ne pourront pas établir de tunnel sécurisé avec la passerelle VPN.
- *DHCP Safe Failover Protocol* – L'architecte réseau doit installer des serveurs DHCP de manière redondante à l'aide du projet de protocole RFC DHCP Safe Failover Protocol. Ce protocole permet d'accroître la disponibilité du réseau pour les utilisateurs sans fil.
- *Gestion d'adresses* – L'installation d'un WLAN s'accompagne d'exigences supplémentaires en matière d'adressage IP, et l'architecte réseau doit en tenir compte. S'il décide d'utiliser des VPN IPsec pour sécuriser l'environnement sans fil, il doit prévoir l'adressage IP supplémentaire des tunnels VPN ainsi établis. Dans tous les cas, si les services DHCP ne sont pas disponibles, les utilisateurs sans fil ne pourront pas accéder au réseau d'entreprise.
- *Considérations propres à l'architecture du réseau* – L'architecte réseau doit étudier l'endroit du réseau où seront implantés les services DHCP sollicités par les utilisateurs finals. Pour garantir la haute disponibilité, il est indispensable d'installer un réseau redondant entre les deux sites. Nous recommandons également de ne pas grouper tous les services DHCP sur le même sous-réseau car une attaque par saturation contre ce sous-réseau bloquerait l'ensemble du service DHCP vers les utilisateurs sans fil.

RADIUS

- *Requêtes par seconde* – Le matériel et le logiciel serveur RADIUS (Remote Access Dial-In User Service) doivent être capables de traiter le nombre prévu de nouvelles requêtes RADIUS par seconde associées à l'introduction d'un réseau WLAN. Si les serveurs RADIUS sont surchargés, les points d'accès sans fil et les passerelles VPN seront incapables d'authentifier les utilisateurs sans fil et les empêcheront de se connecter au réseau de l'entreprise. Par ailleurs, si l'architecte réseau décide d'utiliser une base de données d'arrière guichet pour l'authentification utilisateur, celle-ci doit pouvoir traiter le nombre prévu de demandes d'authentification utilisateur par seconde associé à l'offre WLAN.
- *Déploiement redondant des serveurs* – Il est nécessaire de déployer plusieurs serveurs RADIUS pour permettre aux unités d'authentification – points d'accès sans fil ou passerelles VPN – de disposer de plusieurs choix pour le traitement des demandes. L'architecte réseau doit également grouper les unités d'authentification pour alterner la liste des serveurs RADIUS primaires et secondaires. Cette configuration présente deux avantages : elle limite l'incidence d'une défaillance serveur et donne également à chaque serveur RADIUS de meilleures possibilités d'évolutivité.
- *Gestion des utilisateurs* – Les serveurs RADIUS doivent offrir un accès haute disponibilité à la base de données utilisateur qui sert pour l'authentification. L'architecte réseau doit envisager d'installer des serveurs qui synchronisent les données si la base de données utilisateur doit être hébergée localement. Cette configuration offre l'avantage d'un unique point d'administration et élimine l'éventualité que les paramètres d'un utilisateur figurent sur un serveur RADIUS mais pas sur l'autre. Si la base de données utilisateur est hébergée de manière externe (Lightweight Directory Access Protocol [LDAP], domaine NT), l'architecte réseau doit installer les serveurs RADIUS en fonction de la base de données d'arrière guichet car, en cas de défaillance réseau entre les deux ressources, les utilisateurs sans fil ne pourront pas accéder au réseau d'entreprise.

Protocole IPsec

- *Connexions par seconde* – Le matériel et le logiciel de passerelle VPN doivent être capables de traiter le nombre prévu de nouvelles connexions IPsec par seconde associées à l'introduction d'un réseau WLAN.
- *Débit de cryptage* – Le matériel et le logiciel de passerelle VPN doivent être capables de traiter le débit de cryptage prévu associé à l'introduction d'un réseau WLAN. Une passerelle VPN travaille plus longtemps à crypter plusieurs petits paquets qu'un grand, ce qui a des conséquences sur son débit de cryptage. Il est important que l'architecte réseau connaisse la répartition par taille des paquets de son réseau filaire pour dimensionner la passerelle VPN de manière adaptée à l'environnement de réseau sans fil.
- *Sessions IPsec simultanées* – Le matériel et le logiciel de passerelle VPN doivent être capables de traiter le nombre prévu de sessions IPsec simultanées associées à l'introduction d'un réseau WLAN. Les passerelles VPN sont conçues pour gérer un nombre fini de sessions IPsec simultanées.

Si l'environnement IPsec n'est pas conçu en tenant compte de ces exigences, les utilisateurs sans fil seront incapables d'accéder au réseau d'entreprise ou, s'ils y parviennent, devront subir des performances sérieusement dégradées. Les constructeurs de VPN ont cherché à résoudre les trois problèmes précédents en introduisant des technologies de groupement propriétaires. Ces technologies confient à la passerelle VPN la moins chargée les nouvelles connexions IPsec pour leur garantir le meilleur service possible.

Vous trouverez des informations plus détaillées sur l'architecture des réseaux IPsec dans le livre blanc « SAFE VPN: IPsec Virtual Private Networks in Depth ».

Références

Livres blancs Cisco SAFE

SAFE : A Security Blueprint for Enterprise Networks :

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

SAFE : Extending the Security Blueprint to Small, Midsize, and Remote-User Networks :

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm

SAFE VPN : IPsec Virtual Private Networks in Depth :

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

Cisco Aironet® Wireless LAN Security white papers :

http://www.cisco.com/go/aironet/security

SAFE : Nimda Attack Mitigation :

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/snam_wp.htm

SAFE : Code-Red Attack Mitigation :

http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/scdam_wp.htm

Références diverses

Security of the WEP Algorithm :

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Your 802.11 Wireless Network has No Clothes :

http://www.cs.umd.edu/~waa/wireless.pdf

Weaknesses in the Key Scheduling Algorithm of RC4 :

http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

Using the Fluhrer, Mantin, and Shamir Attack to Break Wired Equivalent Privacy (WEP) :

http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

AirSnort :

http://airsnort.sourceforge.net/

Références des produits de nos partenaires

RSA SecureID OTP System

http://www.rsasecurity.com/products/securid/

Remerciements

Les auteurs souhaitent remercier publiquement toutes les personnes qui ont contribué à la présente extension du schéma directeur SAFE ainsi qu'à la rédaction de ce document. En tout état de cause, ce livre blanc n'aurait jamais pu voir le jour sans les précieuses contributions et les analyses judicieuses de l'ensemble des collaborateurs de Cisco, que ce soit au siège social ou sur le terrain. Plusieurs personnes ont plus particulièrement contribué à la relecture ou à la validation en laboratoire de ce document. Greg Abelar, Andy Balinsky, Brian Cox, Roland Saville et Ido Dubrawsky ont notamment constitué le cœur de ce groupe. Merci à tous de vos efforts.

1. Borisov et al., « Security of the WEP Algorithm »

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social Européen
Cisco Systems Europe
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www-europe.cisco.com
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :
www.cisco.com/go/offices.

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

BU/LW47840703