6
Sécurité

Dans un réseau câblé traditionnel, le contrôle d'accès est très simple: si une personne à un accès physique à un ordinateur ou à un concentrateur du réseau, alors elle peut utiliser (ou abuser) des ressources de ce réseau. Tandis que les mécanismes de logiciel sont une composante importante en sécurité de réseau, la limitation de l'accès physique aux appareils du réseau est le mécanisme ultime de contrôle d'accès. Si tous les terminaux et composantes du réseau sont uniquement accessibles par des individus de confiance, alors le réseau est probablement fiable.

Les règles changent de manière significative avec les réseaux sans fil. Même si la portée apparente de votre point d'accès peut sembler n'être que de quelques centaines de mètres, un usager avec une antenne à haut gain peut se servir du réseau à une distance de plusieurs pâtés de maison. Un usager non autorisé peut être détecté, mais il est impossible de retracer l'endroit où il se trouve. Sans transmettre un seul paquet, un usager malicieux peut même enregistrer toutes les données du réseau sur un disque. Ces données peuvent plus tard être employées pour lancer une attaque plus sophistiquée contre le réseau. Il ne faut jamais supposer que les ondes radio «s'arrêtent» simplement au bord de votre ligne de propriété.

Naturellement, même dans les réseaux câblés, il n'est jamais tout à fait possible de faire totalement confiance à tous les usagers du réseau. Les employés contrariés, les usagers connaissant peu les réseaux et les erreurs simples de la part d'usagers honnêtes peuvent causer des complications significatives au fonctionnement du réseau. En tant qu'architecte de réseau, votre but devrait être de faciliter la communication privée entre les usagers légitimes. Même si une certaine quantité de contrôle d'accès et d'authentification soit nécessaire dans n'importe quel réseau, vous aurez échoué dans votre travail si les usagers légitimes ont de la difficulté à utiliser le réseau pour communiquer.

Un vieil adage dit que la seule manière de rendre un ordinateur complètement sécuritaire est de le débrancher, l'enfermer dans un coffre-fort, détruire la clef et d'enterrer le tout dans le béton. Un tel système peut être complètement « sécuritaire » mais est inutile à la communication. Lorsque vous prenez des décisions de sécurité pour votre réseau, vous ne devez jamais

oublier ceci: le réseau existe afin que ses usagers puissent communiquer entre eux. Les considérations de sécurité sont importantes, mais ne devraient pas barrer la route aux usagers du réseau.

Sécurité physique

En installant un réseau, vous établissez une infrastructure dont les gens dépendront. Le réseau doit donc être fiable. Pour plusieurs installations, les pannes se produisent souvent en raison du trifouillage humain, accidentel ou pas. Les réseaux sont physiques, des câbles et des boîtes, c'est-à-dire des choses qui sont facilement déplacées et manipulées. Dans plusieurs installations, les gens ne sauront reconnaître l'équipement que vous aurez installé, ou encore, la curiosité les mènera à expérimenter. Ils ne se rendront pas compte de l'importance d'un câble qui va à un port. On pourraient déplacer un câble Ethernet afin d'y connecter un ordinateur portatif pendant 5 minutes ou déplacer un commutateur parce qu'il est dans leur chemin. Une prise pourrait être enlevée d'une barre de puissance parce que quelqu'un a besoin de ce réceptacle. Assurer la sécurité physique d'une installation est primordial. Les avertissements et les écriteaux ne seront utiles que pour certains, ceux qui peuvent lire ou parler votre langue. Placer les choses à l'écart et y limiter l'accès est le meilleur moyen d'empêcher les accidents ou le bricolage inopportun.

Au sein d'économies moins développées, les attaches et les boîtiers ne seront pas faciles à trouver. Cenpendant, vous devriez pouvoir trouver des alimentations électriques qui fonctionneront aussi bien. Les boîtiers personnalisés sont également faciles à fabriquer et devraient être considérés essentiels à n'importe quelle installation. Dans les pays du sud, il est souvent économique de payer un maçon pour faire des trous et installer un conduit, ce qui serait une option couteuse dans le monde développé. Du PVC peut être inséré dans des murs de ciment pour passer un câble d'une pièce à l'autre, ce qui évite de faire des trous chaque fois qu'un câble doit être passé. Pour isoler, des sachets en plastique peuvent être placés dans le conduit autour des câbles.

L'équipement de petite taille devrait être monté au mur et l'équipement plus grand devrait être placé dans un cabinet ou dans un coffret.

Commutateurs

Les commutateurs, les concentrateurs ou les points d'accès intérieurs peuvent, à l'aide d'une prise murale, être vissés directement sur un mur. Il est préférable de placer cet équipement aussi haut que possible afin d'éviter qu'une personne ne touche au dispositif ou à ses câbles.

Câbles

Les câbles devraient être cachés et attachés. Il est préférable d'enterrer les câbles plutôt que de les laisser pendre dans la cour où ils pourraient être utilisés pour suspendre des vêtements ou simplement être accrochés par une échelle, etc. Pour éviter la vermine et les insectes, vous devez trouver un conduit électrique en plastique. Ce sera une mince dépense qui vous évitera des ennuis. Le conduit devrait être enterré à environ 30 cm de profondeur (sous la glace dans le cas des climats froids). Il est également intéressant d'acheter un conduit plus grand que nécessaire de sorte que de futurs câbles puissent y être placés. Il est également possible de trouver un conduit pour câbles en plastique qui peut être utilisé à l'intérieur des bâtiments. Si non, des attaches de câble simples, clouées au mur peuvent être utilisées pour fixer le câble et pour s'assurer qu'il ne traîne pas là où il pourrait être accroché, pincé ou coupé.

Puissance

Il est préférable d'avoir des barres de puissance enfermées à clef dans un coffret. Si ce n'est pas possible, placez la barre de puissance sous un bureau ou sur le mur et utilisez de la bande adhésive toilée imperméable (*duct tape* en anglais, un ruban adhésif robuste) pour fixer la prise dans le réceptacle. Sur l'UPS et la barre de puissance, ne laissez pas de réceptacles vides. Au besoin, placez du ruban adhésif pour les couvrir. Les gens ont tendance à employer le réceptacle le plus accessible: rendez-les donc difficiles à utiliser. Si vous ne le faites pas, vous pourriez trouver un ventilateur ou une lumière branchée à votre UPS. Même s'il est bien d'avoir de la lumière, il est encore mieux de voir votre serveur fonctionner!

Eau

Protégez votre équipement contre l'eau et l'humidité. Dans tous les cas, veillez à ce que votre équipement, y compris votre UPS, est à au moins 30 cm de la terre, pour éviter les inondations. Essayez en outre de placer un toit sur votre équipement, de sorte que l'eau et l'humidité ne pénètrent pas dessus. Dans des climats humides, il est important de s'assurer que l'équipement ait la ventilation appropriée afin que l'humidité puisse être éliminée. Les petits cabinets doivent avoir de la ventilation, sans quoi l'humidité et la chaleur risquent de dégrader voire détruire votre équipement.

Mâts

L'équipement installé sur un mât est souvent sécuritaire face aux voleurs. Néanmoins, pour décourager les voleurs et pour maintenir votre équipement sécuritaire par rapport au vent, il est conseillé d'avoir des assemblages spé-

ciaux qui vont au delà de l'ingénierie. L'équipement devrait être peint d'une couleur mate, blanche ou grise pour refléter le soleil et le rendre ennuyeux et inintéressant. Les antennes plates sont beaucoup plus subtiles et moins intéressantes que les paraboliques et devraient donc être choisie de préférence. Toute installation placée au mur exige une échelle pour l'atteindre. Essayez de choisir un endroit bien éclairé mais non proéminent pour mettre l'équipement. Évitez en outre les antennes qui ressemblent à des antennes de télévision, car ce sont des articles qui attireront l'intérêt des voleurs. Une antenne WiFi sera inutile au plus commun des voleurs.

Menaces pour le réseau

Une différence critique entre Ethernet et la technologie sans fil est que les réseaux sans fil sont construits dans un ***milieu partagé***. Ils ressemblent plus étroitement aux vieux concentrateurs (*hub*) de réseau qu'aux commutateurs (switch) modernes, du fait que chaque ordinateur connecté au réseau « voit » le trafic de tout autre usager. Pour surveiller tout le trafic de réseau sur un point d'accès, on peut simplement synthoniser le canal qui est employé, placer la carte réseau dans le mode moniteur et prendre note de chaque trame. Ces données peuvent avoir beaucoup de valeur pour une oreille indiscrète (des données telles que le courriel, la voix ou des extraits de clavardages). Elles peuvent également fournir des mots de passe et d'autres données ayant une valeur importante, menaçant davantage le réseau. Nous le verrons plus tard dans ce chapitre, ce problème peut être atténué par l'utilisation du chiffrement.

Un autre problème sérieux avec les réseaux sans fil est que ses usagers sont relativement ***anonymes***. Même s'il est vrai que chaque dispositif sans fil possède une adresse MAC fournie par le fabriquant, ces adresses peuvent souvent être changées avec un logiciel. Même avec l'adresse MAC en main, il peut être très difficile de localiser l'emplacement d'un usager sans fil. Les effets par trajets multiples, les antennes à haut gain et les caractéristiques considérablement variables des transmetteurs radio empêchent de déterminer si un usager sans fil malveillant s'assied dans la salle contiguë ou se trouve dans un immeuble à plusieurs kilomètres de distance.

Même si le spectre sans licence fournit d'énormes économies à l'usager, il a l'effet secondaire malheureux de rendre très simple les attaques par ***déni de service*** (*Denial of Service- DoS* en anglais). Une personne malveillante peut causer des problèmes significatifs sur le réseau, simplement en mettant en marche un point d'accès à puissance élevé, un téléphone sans fil, un transmetteur vidéo ou tout autre dispositif à 2,4GHz. Plusieurs autres dispositifs réseau sont également vulnérables à d'autres formes d'attaques par déni de service, tels que les attaques de désassociassions et la corruption de la table ARP.

Voici plusieurs catégories d'individus qui peuvent poser des problèmes sur un réseau sans fil:

- ***Usagers involontaires***. Puisque de plus en plus de réseaux sans fil sont installés dans des secteurs très peuplés, il est courrant que des usagers d'ordinateur portatif s'associent accidentellement au mauvais réseau. Lorsque leur réseau préféré n'est pas disponible, la plupart des clients sans fil choisiront simplement n'importe quel autre réseau sans fil disponible. L'usager peut alors se servir de ce réseau comme d'habitude, en ignorant complètement qu'il peut être en train de transmettre des données de valeur sur le réseau de quelqu'un d'autre. Les personnes malveillantes peuvent même tirer profit de ceci en installant des points d'accès dans des endroits stratégiques, pour essayer d'attirer des usagers inconscients et pour saisir leurs données.

  Le premier pas pour éviter ce problème est d'instruire vos usagers et souligner l'importance de se connecter uniquement à des réseaux connus et fiables. Plusieurs clients sans fil peuvent être configurés pour se connecter seulement à des réseaux fiables ou pour demander la permission avant de joindre un nouveau réseau. Comme nous le verrons plus tard dans ce chapitre, les usagers peuvent se connecter sans risque à des réseaux publics ouverts en employant un chiffrement fort.

- ***Wardrivers***. Le phénomène du « *wardriving* » tire son nom du film populaire « Jeux de guerre » de 1983 sur des pirates informatiques. Le but des wardrivers est de trouver l'endroit physique des réseaux sans fil. Habituellement, ils conduisent autour d'une zone donnée avec un ordinateur portatif, un GPS et une antenne omnidirectionnelle, notant le nom et l'endroit de tous les réseaux qu'ils trouvent. Ces notations sont alors combinées avec les notations d'autres *wardrivers* et sont transformées en cartes graphiques localisant toute trace de réseau sans fil d'une ville particulière.

  La grande majorité des *wardrivers* ne constituent probablement aucune menace directe pour les réseaux, mais les données qu'ils assemblent pourraient être d'intérêt pour ceux qui désirent détruire un réseau donné. Par exemple, un point d'accès non protégé détecté par un *wardriver* pourrait être situé à l'intérieur d'un bâtiment stratégique, tel qu'un bureau gouvernemental ou corporatif. Une personne malveillante pourrait employer cette information pour accéder illégalement à ce réseau. On pourrait argumenter qu'un tel AP ne devrait jamais avoir été installé en premier lieu, mais le *wardriving* rend le problème encore plus urgent. Comme nous le verrons plus tard dans ce chapitre, les wardrivers qui emploient le programme de grande diffusion NetStumbler peuvent être détectés avec des programmes tels que Kismet. Pour plus d'informations sur le *wardriving*, visitez les sites Web tels que: *http://www.wifimaps.com/*, *http://www.nodedb.com/* ou *http://www.netstumbler.com/*.

- ***Points d'accès illicites***. Il y a deux classes générales de points d'accès illicites: ceux incorrectement installés par les usagers légitimes et ceux installés par les personnes malveillantes qui ont l'intention de rassembler des données d'autrui ou de nuire au réseau. Dans le cas le plus simple, un usager légitime du réseau peut vouloir une meilleure couverture sans fil pour son bureau, ou encore trouver que les restrictions de sécurité au réseau sans fil corporatif sont trop difficiles de satisfaire. En installant un point d'accès peu coûteux sans permission, l'usager ouvre le réseau entier et le rend susceptible de subir des attaques potentielles de l'intérieur. Même s'il est possible d'identifier les points d'accès non autorisés sur votre réseau câblé, il est extrêmement important de mettre en place une politique claire les interdisant.

  Il peut être très difficile de traiter avec la deuxième classe de point d'accès illicite. En installant une AP de haute puissance qui emploie le même ESSID comme réseau existant, une personne malveillante peut duper des personnes et les mener à utiliser leur équipement et noter ou même manipuler toutes les données qui passent à travers lui. Or, si vos usagers ont été formés pour employer un chiffrage fort, ce problème est sensiblement réduit.

- ***Oreilles indiscrètes***. Tel que mentionné précédemment, l'écoute clandestine est un problème très difficile à traiter sur les réseaux sans fil. En utilisant un outil de surveillance passif (tel que Kismet), une oreille indiscrète peut noter toutes les données d'un réseau à une grande distance, sans que personne ne puisse détecter leur présence. Des données mal chiffrées peuvent simplement être notées et déchiffrées plus tard, alors que des données non codées peuvent facilement être lues en temps réel.

  Si vous avez de la difficulté à convaincre les autres de l'existence de ce problème, vous pourriez vouloir faire une démonstration à l'aide d'outils tels qu'Etherpeg (*http://www.etherpeg.org/*) ou Driftnet (*http://www.ex-parrot.com/~chris/driftnet/*). Ces outils observent un réseau sans fil pour des données graphiques, telles que des fichiers GIF et JPEG. Tandis que d'autres usagers naviguent sur Internet, ces outils montrent tous les graphiques trouvés dans un collage graphique. J'utilise souvent des outils de ce type comme démonstration en parlant de la sécurité sans fil. Même si vous pouvez dire à un usager que leur courriel est vulnérable sans chiffrement, rien ne fait passer mieux le message que de leur montrer les images qu'ils sont en train de regarder dans leur navigateur Web.

  Même si elle ne peut être complètement éliminée, l'application appropriée du chiffrement fort découragera l'écoute clandestine.

Le but de cette introduction est de vous donner une idée des problèmes qui peuvent survenir en créant un réseau sans fil. Plus tard dans ce chapitre,

nous examinerons les outils et les techniques qui vous aideront à atténuer ces problèmes.

Authentification

Avant de pouvoir avoir accès aux ressources de réseau, les usagers devraient d'abord être ***authentifiés***. Dans un monde idéal, chaque usager sans fil aurait un identificateur qui est unique, inchangeable et qui ne peut pas être personnifié par d'autres usagers. Ceci s'avère être un problème très difficile à résoudre dans le vrai monde.

Ce que nous avons de plus semblable à un identificateur unique est l'adresse MAC. Celle-ci est un nombre de 48-bit qui a été donné par le fabricant à chaque dispositif sans fil et Ethernet. En utilisant le ***filtrage mac*** sur nos points d'accès, nous pouvons authentifier des usagers en nous basant sur leurs adresses MAC. Avec ce dispositif, le point d'accès garde une table interne d'adresses MAC qui ont été approuvées. Quand un usager sans fil essaye de s'associer au point d'accès, l'adresse MAC du client doit se trouver sur la liste d'adresses approuvées sans quoi l'association sera refusée. Comme alternative, l'AP peut garder une table de "mauvaises" adresses MAC et accorder l'accès à tous les dispositifs qui ne sont pas sur cette liste.

Malheureusement, ce n'est pas un mécanisme idéal de sécurité. Maintenir des tables d'adresses MAC sur chaque dispositif peut être encombrant, exigeant de tous les dispositifs de client d'avoir leur adresse MAC enregistrée et téléchargée aux APs. Pire encore, les adresses MAC peuvent souvent être changées par un logiciel. En observant des adresses MAC en service sur un réseau sans fil, une personne malveillante peut s'approprier de l'une d'entre-elles afin de s'associer à l'AP. Même si le filtrage MAC empêchera les usagers involontaires et la plupart des curieux d'accéder au réseau, il ne pourra pas à lui seul empêcher toutes les attaques éventuelles.

Les filtres MAC sont utiles pour limiter temporairement l'accès des clients qui agissent avec malveillance. Par exemple, si un ordinateur portatif a un virus qui envoie de grandes quantités de pourriel ou tout autre trafic, son adresse MAC peut être ajoutée à la table de filtre pour arrêter le trafic immédiatement. Ceci vous donnera le temps nécessaire pour retracer l'usager et régler le problème.

Un autre dispositif populaire d'authentification sans fil est le ***réseau fermé***. Dans un réseau typique, les APs annonceront leur ESSID plusieurs fois par seconde, permettant aux clients sans fil (ainsi que des outils tels que NetStumbler) de trouver le réseau et de montrer sa présence à l'usager. Dans un réseau fermé, l'AP ne transmet pas l'ESSID et les usagers doivent savoir le nom complet du réseau avant que l'AP permette l'association. Ceci

empêche les usagers occasionnels de découvrir le réseau et de le choisir dans leur client sans fil.

Ce dispositif pose un certain nombre d'inconvénients. Forcer les usagers à saisir l'ESSID complet avant de se connecter au réseau favorise les erreurs ce qui se traduit souvent en appels et en plaintes. Puisque le réseau n'est évidemment pas présent dans des outils tel que le NetStumbler, ceci peut empêcher que vos réseaux apparaissent sur les cartes de wardriving. Mais cela signifie également que d'autres concepteurs de réseaux ne pourront pas trouver facilement votre réseau et ne sauront pas spécifiquement que vous utilisez déjà un canal donné. Un voisin consciencieux peut exécuter une enquête d'emplacement, ne détecter aucun réseau voisin, et installer son propre réseau sur le même canal que vous utilisez. Ceci causera des problèmes d'interférence tant pour vous que pour votre voisin.

En conclusion, employer des réseaux fermés n'ajoute pas grand chose à la sécurité globale de votre réseau. En utilisant des outils de surveillance passifs (tels que Kismet), un usager habile peut détecter les trames envoyées par vos clients légitimes à l'AP. Ces trames contiennent nécessairement le nom du réseau. Un usager malveillant peut alors employer ce nom pour s'associer au point d'accès comme le ferait un usager normal.

Le chiffrement est probablement le meilleur outil que nous avons pour authentifier les usagers sans fil. Avec un chiffrement fort, nous pouvons donner une identité unique à un usager de sorte qu'il soit très difficile de la corrompre et employer cette identité pour déterminer les futurs accès au réseau. Le chiffrement a également l'avantage de préserver la confidentialité en empêchant les oreilles indiscrètes d'observer facilement le trafic du réseau.

La méthode de chiffrement généralement la plus appliquée sur les réseaux sans fil est le ***chiffrement WEP*** (l'acronyme WEP signifie en anglais ***wired equivalent privacy*** ou confidentialité équivalente au réseau filaire en français). Ce type de chiffrement fonctionne pratiquement avec tout l'équipement 802.11a/b/g. WEP emploie une clef 40-bit partagée pour chiffrer des données entre le point d'accès et le client. La clef doit être entrée sur l'AP ainsi que sur chacun des clients. Avec le chiffrement WEP activé, les clients sans fil ne peuvent s'associer à l'AP jusqu'à ce qu'ils emploient la clef correcte. Une oreille indiscrète écoutant un réseau auquel le WEP est activé verra le trafic et les adresses MAC, mais les données utiles de chaque paquet seront chiffrées. Ceci fournit un assez bon mécanisme d'authentification tout en ajoutant un peu de confidentialité au réseau.

Le WEP n'est certainement pas la solution de chiffrement la plus forte disponible actuellement. Ceci est dû au fait que la clef WEP est partagée par tous les usagers. Si la clef est compromise (par exemple si un usager donne le mot de passe à un ami ou si un employé est mis à la porte) alors changer

le mot de passe peut être très difficile puisque tous les APs et dispositifs de client doivent également être changés. Ceci signifie aussi que les usagers légitimes du réseau peuvent toujours écouter le trafic des autres clandestinement, puisqu'ils connaissent tous la clef partagée.

La clef elle-même est souvent très mal choisie rendant possible le piratage sans être connecté. Pire encore, l'implantation du WEP elle-même est souvent défectueuse dans plusieurs applications, ce qui rend encore plus facile d'abîmer certains réseaux. Même si les fabricants ont mis en application un certain nombre d'extensions à WEP (tel que de plus longues clefs à rotation rapide), ces prolongements ne font pas partie de la norme, et ne seront pas interopérables entre les équipements de différents fabricants. En mettant à jour les progiciels les plus récents pour tous vos dispositifs sans fil, vous pouvez empêcher certaines des premières attaques trouvées dans WEP.

WEP peut toujours être un outil utile d'authentification. En supposant que vos utilisateurs sont assez fiables pour ne pas donner le mot de passe, vous pouvez être certain que vos clients sans fil sont légitimes. Même s'il est possible de déchiffrer le WEP, ceci est encore au-delà de la compétence de la plupart des usagers. Le WEP est extrêmement utile pour rendre sécuritaire des liens point à point de longue distance, même des réseaux généralement ouverts. En employant WEP sur un tel lien, vous découragerez d'autres de s'associer au lien et ils emploieront probablement d'autres APs disponibles à la place. Le WEP est l'équivalent d'un écriteau « défense d'entrer » pour votre réseau. N'importe qui détectant le réseau verra qu'une clef est exigée, ce qui indique du fait même qu'ils ne sont pas les bienvenus.

La plus grande force du chiffrement WEP est son interopérabilité. Afin d'être conforme aux normes, tous les dispositifs sans fil fonctionnent avec un WEP de base. Même si ce n'est pas la méthode la plus forte disponible, c'est certainement le dispositif le plus couramment mis en application. Nous verrons d'autres techniques de chiffrement plus avancées plus tard dans ce chapitre.

Pour plus de détails sur le chiffrement WEP, voir les documents suivants:

- *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- *http://www.cs.umd.edu/~waa/wireless.pdf*
- http://www.crypto.com/papers/others/rc4_*ksaproc*.ps

Un autre protocole d'authentification de la couche de liaison est l'***Accès Protégé Sans fil*** (***Wi-Fi Protected Access -WPA*** en anglais). Le WPA a spécifiquement été créé pour traiter les problèmes que pose le chiffrement WEP que nous avons cités précédemment. Il fournit un schéma de chiffrement sensiblement plus fort et peut employer une clef privée partagée, des clefs uniques assignées à chaque utilisateur ou même des certificats SSL pour

authentifier le client et le point d'accès. L'authentification est vérifiée en utilisant le protocole 802.1X, qui peut consulter une base de données d'une tierce partie telle que RADIUS. En utilisant le Protocole Principal Temporel d'Intégrité (du sigle en anglais TKIP), des clefs peuvent rapidement être modifiées ce qui réduit la probabilité qu'une session particulière puisse être déchiffrée. De façon générale, le WPA fournit une authentification et une confidentialité sensiblement meilleures que le WEP standard.

La difficulté que pose actuellement le WPA est que l'interopérabilité entre les fournisseurs est encore très faible. Le WPA exige un équipement de point d'accès de dernière génération et des progiciels mis à jour sur tous les clients sans fil, ainsi qu'une quantité substantielle de configuration. Si vous installez un réseau dans un emplacement où vous contrôlez la plateforme entière d'équipements, le WPA peut être idéal. En authentifiant les clients et les APs, il résout le problème des points d'accès illicites et fournit plusieurs avantages significatifs par rapport au chiffrement WEP. Mais dans la plupart des installations de réseau où l'équipement est très varié et la connaissance des usagers sans fil est limitée, l'installation de WPA peut rapidement devenir un cauchemar. Pour toutes ces raisons, là où le chiffrement est effectivement employé, le WEP continue à être utilisé.

Portails captifs

Un outil d'authentification couramment utilisé sur les réseaux sans fil est le ***portail captif***. Un portail captif emploie un navigateur Web standard pour donner à un usager sans fil l'occasion de présenter son accréditation pour l'ouverture de la session. Il peut également être employé pour présenter à l'usager une certaine information (telle qu'une Politique d'Utilisation Acceptable) avant d'accorder l'accès total. Du fait qu'ils emploient un navigateur Web au lieu d'un programme personnalisé d'authentification, les portails captifs fonctionnent avec pratiquement tous les ordinateurs portatifs et les logiciels d'exploitation. Les portails captifs sont typiquement employés sur des réseaux ouverts sans d'autres méthodes d'authentification (tels que les filtres WEP ou MAC).

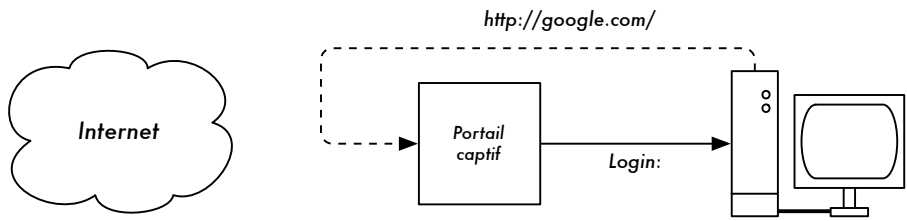

Figure 6.1: L'usager veut aller sur page Web et est redirigé.

Pour commencer, un usager sans fil ouvre son ordinateur portatif et choisit un réseau. Son ordinateur demande un bail DHCP, qui est accordé. L'usager emploie alors son navigateur Web pour visiter n'importe quel site sur Internet.

Au lieu de recevoir la page demandée, on présente un écran d'ouverture à l'usager. Cette page peut exiger de celui-ci qu'il entre un nom d'usager et un mot de passe, qu'il clique simplement sur un bouton d' « ouverture », qu'il saisisse les chiffres d'un ticket prépayé ou qu'il entre toute autre accréditation exigée par les administrateurs de réseau. L'usager entre alors son accréditation qui est vérifiée par un point d'accès ou un autre serveur sur le réseau. Tout autre accès au réseau est bloqué jusqu'à ce que ses accréditations soient vérifiées.

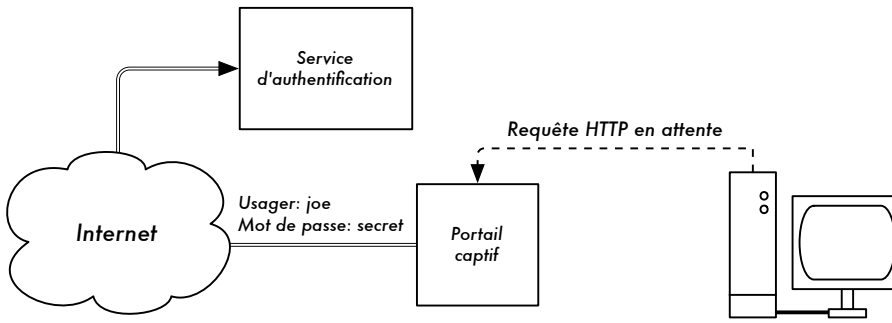

Figure 6.2: Les accréditations de l'usager sont vérifiées avant de lui permettre un accès complet. Le serveur d'authentification peut être le point d'accès lui-même, un autre ordinateur sur le réseau local ou un serveur n'importe où sur Internet.

Une fois authentifié, on permet à l'usager d'avoir accès à toutes les ressources du réseau et, normalement, on le redirige au site qu'il avait demandé au début.

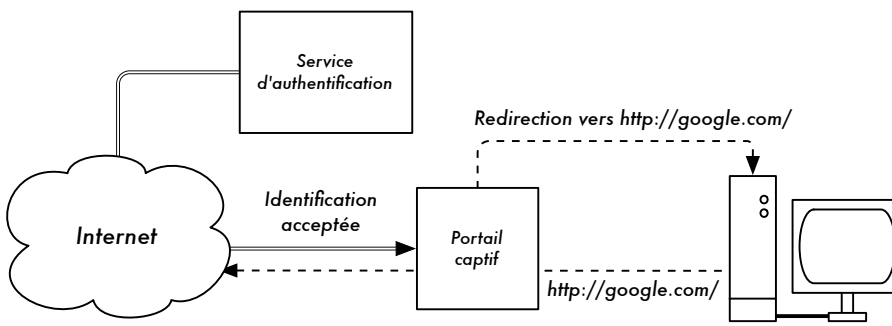

Figure 6.3: Une fois authentifié, l'usager peut avoir accès au reste du réseau.

Les portails captifs ne fournissent aucun chiffrement pour les usagers sans fil. Ils comptent plutôt sur les adresses MAC et IP comme unique identification. Puisque ceci n'est pas nécessairement très sécuritaire, on demandera à l'usager de s'authentifier à nouveau périodiquement. Ceci peut ce faire automatiquement en réduisant au minimum une fenêtre flottante ou pop-up spéciale du navigateur lorsque l'utilisateur entre pour la première fois.

Puisqu'ils ne fournissent pas de chiffrement fort, les portails captifs ne sont pas un très bon choix pour les réseaux qui doivent être fermés pour ne permettre l'accès qu'à des usagers fiables. Ils conviennent davantage aux cafés, aux hôtels et autres endroits d'accès publics utilisés par des usagers occasionnels de réseau.

Dans des installations de réseau publiques ou semi-publiques, les techniques de chiffrement telles que le WEP et le WPA sont inutiles. Il n'y a simplement aucune manière de distribuer des clefs publiques ou partagées aux membres du grand public sans compromettre la sécurité de ces clefs. Dans ces installations, une application plus simple telle qu'un portail captif fournit un niveau de service qui se trouve entre un service complètement ouvert et un service complètement fermé.

NoCatSplash et Chillispot sont deux logiciels libre de portails captifs.

NoCatSplash

Si vous devez simplement fournir à des usagers d'un réseau ouvert de l'information et une Politique d'Utilisation Acceptable, jetez un coup d'oeil à NoCatSplash. Il est disponible en ligne à l'adresse suivante: *http://nocat.net/download/NoCatSplash/*.

NoCatSplash fournit à vos usagers une page de présentation (ou page *splash*) personnalisable, exigeant qu'ils cliquent sur un bouton d' « ouverture » avant d'employer le réseau. Ceci est utile pour identifier les opérateurs du réseau et montrer les règles pour l'accès au réseau.

NoCatSplash en est écrit en C et fonctionnera sur à peu près tous les systèmes d'exploitation du type Unix, incluant Linux, BSD et même les plateformes embarquées telles qu'OpenWRT. Il présente un fichier simple de configuration et peut servir n'importe quel fichier HTML personnalisé comme page de présentation. Il fonctionne typiquement directement sur un point d'accès, mais également sur un routeur ou un serveur proxy. Pour plus d'informations, visitez l'adresse suivante: *http://nocat.net/*.

D'autres projets de points chauds populaires

NoCatSplash n'est qu'une application de portail captif. Il existe également plusieurs autres créations de source libre qui offrent une gamme diverse de fonctionnalités. En voici certaines:

- Chillispot (*http://www.chillispot.org/*). Chillispot est un portail captif conçu pour authentifier à l'aide d'une base de données d'accréditations d'usagers existante telle que RADIUS. Combiné avec l'application phpMyPrePaid, l'authentification basée sur les tickets prépayés peut être installée très fac-

ilement. Vous pouvez télécharger phpMyPrePaid à l'adresse suivante: *http://sourceforge.net/projects/phpmyprepaid/*.

- WiFi Dog (*http://www.wifidog.org/*). WiFi Dog fournit un paquet d'authentification de portail captif très complet dans un très petit espace (typiquement sous 30 kb). Du point de vue de l'usager, il n'exige aucun support pop-up ou Javascript, ce qui lui permet de fonctionner sur une plus grande variété de dispositifs sans fil.
- m0n0wall (*http://m0n0.ch/wall/*). Comme nous l'avons vu au chapitre cinq, m0n0wall est un système d'exploitation embarqué complet basé sur FreeBSD. Il inclue un portail captif avec support RADIUS, ainsi qu'un navigateur Web PHP.

Protection des renseignements personnels

La plupart des usagers ignorent que leur courriel, leurs clavardages et même leurs mots de passe privés sont souvent envoyés « dans l'espace libre » sur des douzaines de réseaux non fiables avant d'arriver à leur destination finale sur Internet. Même s'ils se trompent, les usagers espèrent toujours que leurs renseignements personnels seront protégés lorsqu'ils utilisent des réseaux informatiques.

Cette protection peut être réalisée même sur des réseaux qui ne sont pas fiables comme des points d'accès publics et Internet. La seule méthode efficace prouvée pour protéger les renseignements personnels est l'utilisation d'un ***chiffrement bout à bout*** fort.

Les techniques de chiffrement telles que WEP et WPA essayent d'aborder la question de la protection des renseignements personnels à la couche deux, la couche liaison. Même si ceci offre une protection contre les oreilles indiscrètes dans une connexion sans fil, la protection finit au point d'accès. Si le client sans fil emploie des protocoles peu sécuritaires (tels que le POP ou un simple SMTP pour recevoir et envoyer des courriels), alors des usagers en dehors de l'AP peuvent toujours se connecter à la session et voir les données personnelles. Comme cité précédemment, le WEP souffre également du fait qu'il emploie une clef privée partagée. Ceci signifie que les usagers légitimes sans fil peuvent s'écouter clandestinement les uns les autres puisqu'ils connaissent tous la clef privée.

En employant le chiffrement avec l'hôte distant de la connexion, les usagers peuvent habilement éluder le problème. Ces techniques fonctionnent bien même sur des réseaux publics peu fiables où les oreilles indiscrètes écoutent et manipulent probablement des données venant du point d'accès.

Afin d'assurer une protection des renseignements personnels, un bon chiffrement bout à bout devrait présenter les caractéristiques suivantes:

- ***Authentification vérifiée de l'hôte distant***. L'usager devrait pouvoir savoir sans aucun doute que l'hôte distant est bien ce qu'il prétend être. Sans authentification, un usager pourrait transmettre des données privées à tout ceux qui prétendraient être le service légitime.
- ***Méthodes fortes de chiffrement***. L'algorithme du chiffrement devrait être minutieusement examiné par le public et ne devrait pas être facilement déchiffré par un tiers. Il n'y a aucune sécurité par l'obscurité et le chiffrement fort est encore plus fort quand l'algorithme est largement connu et sujet à l'examen des pairs. Un bon algorithme avec une clef assez grande et protégée fournit un chiffrement qui sera peu susceptible d'être brisé malgré tout les efforts réalisés à l'aide de la technologie actuelle.
- ***Cryptographie à clef publique***. Même si ce n'est pas une condition absolue pour le chiffrement bout à bout, l'utilisation de la cryptographie à clef publique au lieu d'une clef partagée peut assurer que les données d'un usager demeurent privées, même si la clef d'un autre usager du service est compromise. Elle résout également certains des problèmes de la distribution de clefs aux usagers sur des réseaux peu fiables.
- ***Encapsulation des données***. Un bon mécanisme de chiffrement bout à bout protège autant de données que possible. Ceci peut aller de chiffrer une simple transaction de courriel à l'encapsulation de tout le trafic IP, y compris des consultations de DNS et d'autres protocoles de support. Certains outils de chiffrement fournissent simplement un canal sécuritaire que d'autres applications peuvent utiliser. Ceci permet aux usagers d'exécuter n'importe quel programme de leur choix en ayant toujours la protection du chiffrement fort, même si les programmes eux-mêmes ne la soutiennent pas.

Prenez en compte que les lois concernant l'utilisation du chiffrement sont considérablement différentes d'un endroit à l'autre. Certains pays considèrent le chiffrement comme des munitions et peuvent exiger un permis, bloquer des clefs privées ou même interdire complètement son utilisation. Avant de mettre en application n'importe quelle solution utilisant le chiffrement, soyez sûr de vérifier que l'usage de cette technologie est autorisé dans votre région.

Dans les sections suivantes, nous verrons certains outils spécifiques qui peuvent offrir une bonne protection pour les données de vos usagers.

Couche de sécurité SSL

La technologie de chiffrement bout à bout la plus largement disponible est la ***couche de sécurité SSL***. Elle est pratiquement installée dans tous les navigateurs Web et emploie la cryptographie à clef publique et une ***infrastructure à clef publique*** (***PKI***) fiable pour rendre plus sécuritaire la communication de données sur le Web. Toutes les fois que vous visitez un URL Web qui commence par https, vous employez la couche de sécurité SSL.

L'implantation SSL établie dans les navigateurs Web inclut une collection de certificats provenant de sources fiables, appelée les ***autorités de certificats*** (***CA***). Ces certificats sont des clefs cryptographiques qui sont employées pour vérifier l'authenticité des sites Web. Quand vous passez en revue un site Web qui emploie SSL, le navigateur et le serveur échangent d'abord des certificats. Le navigateur vérifie alors que le certificat fourni par le serveur correspond avec son nom d'hôte DNS, qu'il n'a pas expiré et qu'il est signé par une Autorité de Certification digne de confiance. De façon optionnelle, le serveur vérifie l'identité du certificat du navigateur. Si les certificats sont approuvés, le navigateur et le serveur négocient alors une clef principale de session en utilisant les certificats précédemment échangés pour la protéger. Cette clef est alors employée pour chiffrer toutes les communications jusqu'à ce que le navigateur se déconnecte. Ce genre d'encapsulation des données est connu sous le nom de ***tunnel***.

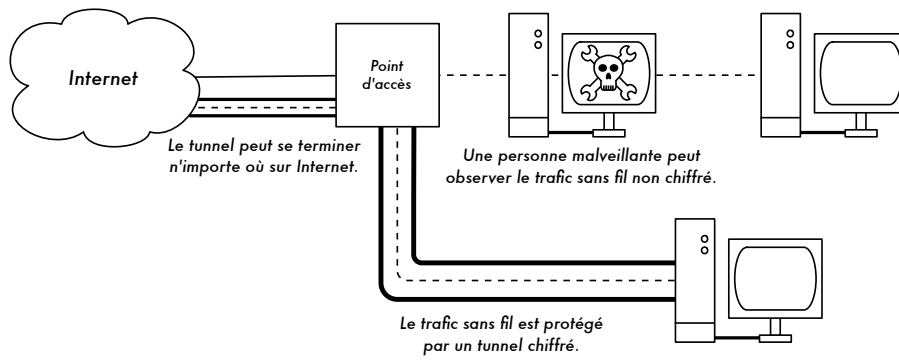

Figure 6.4: Les oreilles indiscrètes doivent rompre un chiffrement fort pour surveiller le trafic au sein d'un tunnel chiffré. La conversation à l'intérieur de ce tunnel est identique à n'importe quelle autre conversation non chiffrée.

L'usage de certificats avec un PKI protège non seulement la communication contre les oreilles indiscrètes, mais empêche également les ***attaques de l'homme au milieu*** (en anglais, ***man-in-the-middle -MITM***). Dans une attaque de l'homme au milieu, un usager malveillant intercepte toute la communication entre le navigateur et le serveur. En présentant des certificats faux au navigateur et au serveur, l'usager malveillant pourrait poursuivre simultanément deux sessions chiffrées. Puisque l'usager malveillant connaît le

secret des deux connexions, il est trivial d'observer et de manipuler des données passant entre le serveur et le navigateur.

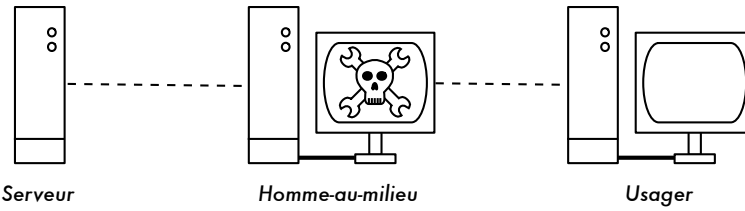

Figure 6.5: L'homme au milieu controle efficacement tout ce que l'usager voit et peut enregistrer ou manipuler tout le trafic. Sans infrastructure a clef publique pour vérifier l'authenticité des clefs, le chiffrement fort, employé seul, ne peut pas protéger contre ce genre d'attaque..

L'utilisation d'une bonne PKI empêche ce genre d'attaque. Afin de réussir son coup, l'usager malveillant devrait présenter un certificat au client qui est signé par une Autorité de Certificats fiable. À moins qu'une AC ait été compromise (ce qui est très peu probable) ou que l'usager ait été dupé et accepte le faux certificat, une telle attaque est impossible. C'est pourquoi il est extrêmement important que les usagers comprennent que le fait d'ignorer des avertissements sur des certificats expirés ou faux est très dangereux, particulièrement en utilisant des réseaux sans fil. En cliquant sur le bouton "ignorez", les usagers ouvrent leurs portes à plusieurs attaques potentielles.

SSL est non seulement employé pour naviguer sur le Web. Il est possible de rendre plus sécuritaires les protocoles de courriel peu sûrs tels que IMAP, POP et SMTP en les enveloppant dans un tunnel SSL. La plupart des clients de courriel actuels soutiennent IMAPS et POPS (IMAP et POP sécuritaires) ainsi que le SMTP protégé avec SSL/TLS. Si votre serveur de courriel ne fournit pas le support SSL, vous pouvez toujours le rendre plus sécuritaire avec SSL en employant un programme comme Stunnel (*http://www.stunnel.org/*). SSL peut être employé pour rendre plus sécuritaire presque n'importe quel service qui fonctionne sur TCP.

SSH

La plupart des personnes pensent à SSH comme remplacement sécuritaire de **`telnet`**, de la même façon que **`scp`** et **`sftp`** sont les contreparties sécuritaires de **`rcp`** et **`ftp`**. Mais SSH est plus qu'un *shell* (ligne de commande) distant chiffré. Comme le SSL, il emploie une forte cryptographie à clef publique pour vérifier le serveur à distance et pour chiffrer des données. Au lieu d'une PKI, il emploie une cache d'empreinte de clefs (*fingerprint key* en anglais) qui est vérifiée avant qu'une connexion soit autorisée. Il peut employer des mots de passe, des clefs publiques ou d'autres méthodes pour l'authentification des usagers.

Beaucoup de gens ne savent pas que SSH peut également agir en tant que tunnel de chiffrement tout usage ou même un chiffrement Web proxy. En établissant d'abord une connexion SSH à un site fiable près d'un (ou sur un) serveur à distance, des protocoles peu sûrs peuvent être protégés contre l'écoute clandestine et les attaques.

Tandis que cette technique peut être un peu avancée pour plusieurs usagers, les architectes de réseau peuvent employer SSH pour chiffrer le trafic à travers des liens peu fiables, tels que les liens point-à-point sans fil. Puisque les outils sont librement disponibles et fonctionnent sur le TCP standard, n'importe quel usager instruit peut mettre en application des connexions SSH sans l'intervention d'un administrateur en fournissant son propre chiffrement bout à bout.

OpenSSH (*http://openssh.org/*) est probablement la version la plus populaire sur les plateformes de type Unix. Les versions libres telles que Putty (*http://www.putty.nl/*) et WinSCP (*http://winscp.net/*) sont disponibles pour Windows. OpenSSH fonctionnera également sur Windows dans l'environnement Cygwin (*http://www.cygwin.com/*). Ces exemples supposent que vous employez une version récente d'OpenSSH.

Pour établir un tunnel chiffré d'un port sur l'ordinateur local à un port d'hôte distant, utilisez le commutateur **-L**. Par exemple, supposez que vous voulez expédier du trafic Web proxy sur un lien chiffré au serveur squid à squid.example.net. Redirigez le port 3128 (le port de proxy par défaut) avec la commande suivante:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

Les commutateurs **-fN** ordonnent à ssh de s'exécuter en tâche de fond après s'être connecté. Le commutateur **-g** permet à d'autres usagers sur votre segment local de se connecter à l'ordinateur local et à l'utiliser pour le chiffrement sur les liens de non-confiance. OpenSSH emploiera une clef publique pour l'authentification si vous en avez établie une ou demandera le mot de passe de l'hôte distant. Vous pouvez alors configurer votre navigateur Web pour vous connecter au port local 3128 comme son service web proxy. Tout le trafic Web sera alors chiffré avant d'être transmis à l'hôte distant.

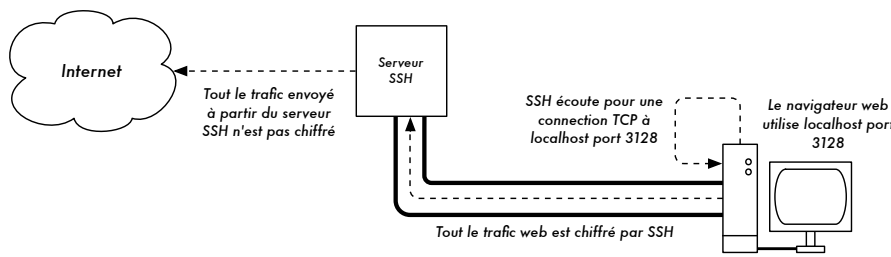

Figure 6.6: Le tunnel SSH protège le trafic Web au delà du serveur SSH lui-même.

SSH peut également agir en tant que proxy dynamique SOCKS4 ou SOCKS5. Ceci vous permet de créer un chiffrement Web proxy, sans avoir à installer squid. Notez que ce n'est pas un proxy à antémémoire; il chiffre simplement tout le trafic.

```
ssh -fN -D 8080 remote.example.net
```

Configurez votre navigateur web pour utiliser SOCKS4 ou SOCKS5 sur le port local 8080 et voilà, vous pourrez sortir.

SSH peut chiffrer des données sur n'importe quel port TCP, y compris des ports utilisés pour le courriel. Il peut même comprimer les données le long du chemin ce qui peut diminuer la latence sur des liens de basse capacité.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

Le commutateur **-C** met en marche la compression. En spécifiant commutateur **-L** plusieurs fois, vous pouvez ajouter autant de règles de redirection de port que vous le souhaitez. Notez qu'afin d'utiliser un port plus bas que 1024, vous devez avoir des privilèges de superutilisateur (*root*) sur l'ordinateur local.

Ceux-ci ne sont que quelques exemples de la flexibilité de SSH. En mettant en application des clefs publiques et en employant l'agent ssh de redirection, vous pouvez automatiser la création de tunnels chiffrés dans tout votre réseau sans fil et ainsi protéger vos communications avec un chiffrement et une authentification solides.

OpenVPN

OpenVPN est une implantation VPN gratuite et de source ouverte basée sur le chiffrement SSL. Il y a des implantations de client OpenVPN pour un éventail de systèmes d'exploitation, comprenant Linux, Windows 2000/XP (et plus récent), OpenBSD, FreeBSD, NetBSD, Mac OS X et Solaris. Étant un VPN, il encapsule tout le trafic (y compris DNS et tout autre protocole) dans un tunnel chiffré; et non un seul port TCP. La plupart des personnes le trouvent considérablement plus facile à comprendre et à configurer qu'IPsec.

OpenVPN présente également quelques inconvénients, tels qu'une latence assez élevée. Une certaine quantité de latence est inévitable puisque tout chiffrement/déchiffrement se réalise dans l'espace utilisateur mais à l'aide d'ordinateurs relativement nouveaux aux deux extrémité du tunnel il est possible de la réduire au minimum. Malgré qu'on puisse employer des clefs partagées traditionnelles, OpenVPN se démarque vraiment lorsqu'on l'utilise avec des certificats SSL et une Autorité de Certificat. OpenVPN présente

plusieurs avantages qui le rendent une bonne option pour fournir de la sécurité bout à bout.

- Il est basé sur un protocole de chiffrement robuste qui a fait ses preuves (SSL et RSA)
- Il est relativement facile à configurer
- Il fonctionne sur plusieurs plateformes différentes
- Il est bien documenté
- Il est gratuit et de source ouverte

Comme SSH et SSL, OpenVPN doit simplement se connecter à un port TCP de l'hôte distant. Une fois cette connexion établie, il peut encapsuler toutes les données de la couche de gestion de réseau ou même de la couche de liaison. Vous pouvez l'employer pour créer des connexions VPN robustes entre différents ordinateurs ou l'utiliser simplement pour connecter des routeurs sur des réseaux sans fil peu fiables.

La technologie VPN est un domaine complexe et dépasse un peu la portée de cet ouvrage. Il est important de comprendre comment les VPNs s'accommodent dans la structure de votre réseau afin d'assurer la meilleure protection sans ouvrir votre organisation à des problèmes involontaires. On retrouve plusieurs bonnes ressources en ligne qui se penchent sur la question de l'installation d'OpenVPN sur un serveur et un client. Je recommande particulièrement l'article suivant tiré du journal de Linux: *http://www.linuxjournal.com/article/7949* ainsi que le HOWTO officiel: *http://openvpn.net/howto.html*.

Tor et Anonymiseurs

L'Internet est fondamentalement un réseau ouvert basé sur la confiance. Quand vous vous connectez à un serveur Web à travers Internet, votre trafic traverse plusieurs routeurs différents appartenant à une grande variété d'établissements, d'associations et d'individus. En principe, n'importe quel de ces routeurs ont la capacité de regarder vos données de près, voyant au moins la source et les adresses de destination et, souvent aussi, le contenu réel de données. Même si vos données sont chiffrées en utilisant un protocole sécuritaire, il est possible pour votre fournisseur Internet de surveiller la quantité de données, la source et la destination de ces données. Souvent, ceci est assez pour rassembler une image assez complète de vos activités en ligne.

La protection des renseignements personnels et l'anonymat sont importants et étroitement liés entre eux. Il y a beaucoup de raisons valides qui peuvent vous pousser à protéger votre vie privée en ***anonymisant*** votre trafic de ré-

seau. Supposez que vous voulez offrir une connectivité Internet à votre communauté locale en installant un certain nombre de points d'accès pour que les personnes puissent s'y connecter. Que vous les fassiez payer pour l'accès ou pas, il y a toujours un risque que les gens qui utilisent le réseau le fassent pour quelque chose qui n'est pas légal dans votre pays ou région. Vous pourriez affirmer que cette action illégale particulière n'a pas été effectuée par vous-même et qu'elle a pu être accomplie par n'importe quelle personne se reliant à votre réseau. On pourrait éviter le problème s'il était techniquement infaisable de déterminer où votre trafic a été dirigé réellement. Que pensez-vous de la censure en ligne? Des pages Web anonymes peuvent également être nécessaires pour éviter la censure du gouvernement.

Il y a des outils qui vous permettent d'anonymiser votre trafic de différentes manières relativement faciles. La combinaison de ***Tor*** (*http://tor.eff.org/*) et de ***Privoxy*** (*http://www.privoxy.org/*) est une manière puissante de faire fonctionner un serveur local proxy qui fera passer votre trafic Internet par un certain nombre de serveurs à travers Internet, rendant très difficile de suivre la trace de l'information. Le Tor peut être exécuté sur un ordinateur local, sous Microsoft Windows, Mac OSX, Linux et une variété de BSDs où il anonymisera le trafic du navigateur sur cet ordinateur. Tor et Privoxy peuvent également être installés sur une passerelle ou même un petit point d'accès embarqué (tel que Linksys WRT54G) où ils fournit automatiquement l'anonymat à tous les usagers de ce réseau.

Tor fonctionne en faisant rebondir à plusieurs reprises vos connexions TCP à travers un certain nombre de serveurs répandus sur Internet et en emballant l'information de routage dans un certain nombre de couches chiffrées (d'où le terme ***routage en oignon***), qui vont être « épluchées » au cours du déplacement du paquet à travers le réseau. Ceci signifie qu'à n'importe quel point donné sur le réseau, la source et les adresses de destination ne peuvent pas être liées ensemble. Ceci rend l'analyse de trafic extrêmement difficile.

Le besoin du proxy de protection de la vie privée Privoxy lié à Tor est dû au fait que dans la plupart des cas les requêtes de nom de serveur (requêtes DNS) ne sont pas passées par le serveur proxy et quelqu'un analysant votre trafic pourrait facilement voir que vous essayiez d'atteindre un emplacement spécifique (par exemple, *google.com*) du fait que vous avez envoyé une requête DNS pour traduire google.com à l'adresse IP appropriée. Privoxy se connecte à Tor comme un proxy SOCKS4a, qui emploie des noms d'hôtes (et non des adresses IP) pour livrer vos paquets à la destination souhaitée.

En d'autres termes, employer Privoxy avec Tor est une manière simple et efficace d'empêcher l'analyse de trafic de lier votre adresse IP avec les services que vous employez en ligne. Combiné avec des protocoles chiffrés sé-

curitaires (du type que nous avons vu au sein de ce chapitre), Tor et Privoxy fournissent un niveau élevé d'anonymat sur l'Internet.

Surveillance

Les réseaux informatiques (et les réseaux sans fil en particulier) sont des inventions incroyablement divertissantes et utiles. Excepté, naturellement, quand ils ne fonctionnent pas. Vos usagers peuvent se plaindre que le réseau est « lent » ou « brisé », mais qu'est-ce que cela signifie vraiment? Sans pouvoir savoir ce qui se produit réellement, l'administration d'un réseau peut devenir très frustrante.

Afin d'être un administrateur de réseau efficace, vous devez avoir accès aux outils qui vous montrent exactement ce qui se produit sur votre réseau. Il y a plusieurs différentes classes d'outils de surveillance. Chacun vous montre un aspect différent de « ce qui se passe », de l'interaction physique par radio à la façon dont les applications des usagers interagissent les unes sur les autres. En observant comment le réseau fonctionne à travers le temps, vous pouvez avoir une idée de ce qui est « normal » pour votre réseau et même recevoir une annonce automatique lorsque les choses semblent sortir de l'ordinaire. Les outils énumérés dans cette section sont tous assez puissants et peuvent être gratuitement téléchargés à partir des adresses énumérées après chaque description.

Détection de réseau

Les outils de surveillance sans fil les plus simples fournissent simplement une liste de réseaux disponibles avec l'information de base (telle que la force et le canal du signal). Ils vous permettent de détecter rapidement les réseaux voisins et déterminer s'ils causent de l'interférence.

- **Ceux qui sont incorporés au client**. Tous les systèmes d'exploitation modernes fournissent un appui intégré aux réseaux sans fil. Ceci inclut typiquement la capacité de détecter les réseaux disponibles, permettant à l'usager de choisir un réseau à partir d'une liste. Même s'il est garanti que pratiquement tous les dispositifs sans fil ont une capacité simple de balayage, la fonctionnalité peut changer considérablement entre les différentes applications. En général, ces outils sont uniquement utiles pour configurer un ordinateur chez soi ou au bureau. Ils tendent à fournir peu d'informations outre les noms de réseau et le signal disponible au point d'accès actuellement en service.
- **Netstumbler** (*http://www.netstumbler.com/*). C'est l'outil le plus populaire pour détecter les réseaux sans fil en utilisant Microsoft Windows. Il fonctionne avec une variété de cartes sans fil et est très facile à utiliser. Il détectera les réseaux ouverts et chiffrés mais ne peut pas détecter les ré-

seaux sans fil fermés. Il possède également un mesureur de signal/bruit qui trace les données du récepteur radio sur un graphique au cours du temps. Il peut également être intégré à une variété de dispositifs GPS pour noter l'information précise concernant l'emplacement et la force du signal. Ceci rend Netstumbler un outil accessible pour effectuer le relevé informel d'un site.

- **Ministumbler** (*http://www.netstumbler.com/*). Ministumbler, fait par les concepteurs de Netstumbler, fournit presque la même fonctionnalité que la version de Windows mais fonctionne sur la plateforme Pocket PC. Ministumbler peut fonctionner sur un PDA de poche avec une carte sans fil pour détecter des points d'accès dans une zone donnée.
- **Macstumbler** (*http://www.macstumbler.com/*). Même s'il n'est pas directement relié au Netstumbler, Macstumbler fournit en grande partie la même fonctionnalité mais pour la plateforme Mac OS X. Il fonctionne avec toutes les cartes Airport de Apple.
- **Wellenreiter** (*http://www.wellenreiter.net/*). Wellenreiter est un détecteur graphique de réseau sans fil pour Linux. Il exige Perl et GTK et fonctionne avec des cartes sans fil Prism2, Lucent, et Cisco.

Analyseurs de protocoles

Les analyseurs de protocole de réseau fournissent beaucoup de détail au sujet de l'information traversant un réseau en vous permettant d'inspecter des paquets individuels. Pour des réseaux câblés, vous pouvez inspecter des paquets à la couche liaison ou à une couche supérieure. Pour les réseaux sans fil, vous pouvez inspecter l'information jusqu'aux trames 802.11. Voici plusieurs analyseurs populaires (et libres) de protocole de réseau:

- **Ethereal** (*http://www.ethereal.com/*). Ethereal est probablement l'analyseur de protocole le plus populaire disponible actuellement. Il fonctionne avec Linux, Windows, Mac OS X et divers systèmes BSD. Ethereal va capturer des paquets directement en provenance « du câble » et les montrer dans une interface graphique intuitive. Il peut décoder plus de 750 protocoles différents, des trames 802.11 aux paquets HTTP. Il peut rassembler des paquets fragmentés et suivre des sessions TCP entières facilement, même si d'autres données ont brisé l'échantillon. Ethereal est très utile pour dépanner des problèmes difficiles du réseau, ainsi que pour savoir exactement ce qui se produit quand deux ordinateurs conversent « sur le câble ».
- **Kismet** (*http://www.kismetwireless.net/*). Kismet est un analyseur de protocole sans fil puissant pour Linux, Mac OS X et même la distribution embarquée de Linux OpenWRT. Il fonctionne avec n'importe quelle carte sans fil qui supporte le mode moniteur passif. En plus de la détection de la pré-

sence du réseau, Kismet notera passivement chacune des trames 802.11 sur le disque ou sur le réseau dans le format standard PCAP, pour l'analyse postérieure avec des outils comme Ethereal. Kismet présente également de l'information associée au client; l'empreinte de l'équipement AP, la détection de Netstumbler et l'intégration GPS.

Puisque c'est un moniteur de réseau passif, il peut même détecter les réseaux sans fil « fermés » en analysant le trafic envoyé par les clients sans fil. Vous pouvez exécuter Kismet sur plusieurs ordinateurs à la fois et faire que ceux-ci informent à travers le réseau une interface usager centrale. Ceci permet la surveillance sans fil sur un large secteur, tel qu'un campus universitaire ou de corporation. Puisqu'il emploie le mode moniteur passif, il peut réaliser tout ceci sans transmettre aucune donnée.

- **KisMAC** (*http://kismac.binaervarianz.de/*). Kismac a été crée exclusivement pour la plateforme Mac OS X. Il fonctionne de façon très similaire à Kismet, mais avec une interface graphique Mac OS X très élaborée. C'est un module de balayage de données passif qui note l'information sur un disque de format PCAP compatible avec Ethereal. Malgré qu'il ne puisse pas fonctionner avec les cartes AirportExtreme (dues à des limitations du pilote sans fil), il le fait très bien avec une variété de cartes radio USB.
- **Driftnet** et **Etherpeg**. Ces outils décodent des données graphiques (telles que des fichiers GIF et JPEG) et les présentent dans un collage. Tel que mentionné précédemment, les outils de ce type ne sont pas très utiles pour le dépannage, mais sont très utiles pour démontrer l'insécurité des protocoles sans chiffrement. Etherpeg est disponible à l'adresse: *http://www.etherpeg.org/*, et Driftnet peut être téléchargé à l'adresse: *http://www.ex-parrot.com/~chris/driftnet/*.

Surveillance de la largeur de bande

Le réseau est lent. Qui est en train d'accaparer toute la largeur de bande? En employant un bon outil de surveillance de la largeur de bande, vous pouvez facilement déterminer la source des problèmes d'envoie massif de pourriel et de virus. De tels outils peuvent également vous aider à projeter la future capacité dont vous aurez besoin à mesure que la largeur de bande devient trop petite pour ses usagers. Ces outils vous donneront une représentation visuelle de la façon dont le trafic circule dans tout votre réseau, y compris le trafic venant d'un ordinateur ou d'un service particulier.

- **MRTG** (*http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*). La plupart des administrateurs de réseau ont fait la connaissance de MRTG à un certain moment dans leurs voyages. Écrit à l'origine en 1995, MRTG est probablement l'application de surveillance de la largeur de bande la plus largement répandue. En utilisant Perl et C, il établit une page Web remplie de graphiques détaillant le trafic entrant et sortant d'une interface réseau

particulière. Avec MRTG, il est simple de consulter des commutateurs de réseau, des points d'accès, des serveurs et d'autres appareils en montrant les résultats sous la forme de graphiques qui changent au cours du temps.

- **RRDtool** (*http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*). RRDtool a été développé par les mêmes personnes qui ont écrit mrtg mais c'est une application de surveillance générique plus puissante. RRD est l'abréviation en anglais de « *round-robin database* » (base de données à parcours circulaire). C'est un format de données générique qui vous permet de suivre facilement n'importe quel point de données comme un ensemble de moyennes au cours du temps. Tandis que rrdtool ne surveille pas directement les interfaces ou les dispositifs, plusieurs programmes de surveillance se basent sur lui pour stocker et montrer les données qu'ils rassemblent. Avec quelques simples scripts shell, vous pouvez surveillez facilement vos commutateurs de réseau et points d'accès et tracer la largeur de bande utilisée sous forme de graphique sur une page Web.
- **ntop** (*http://www.ntop.org/*). Ntop est utile pour une analyse historique de trafic et d'usage. Ce programme fournit un rapport détaillé en temps réel du trafic observé sur le réseau et le présente sur votre navigateur Web. Il s'incorpore à rrdtool pour faire des graphiques et des diagrammes dépeignant visuellement comment le réseau est employé. Sur les réseaux très occupés, ntop peut utiliser beaucoup de l'unité centrale de traitement et d'espace disque, mais il vous offre une vision précise de la façon dont votre réseau est employé. Il fonctionne sur Linux, BSD, Mac OS X et Windows.
- **iptraf** (*http://iptraf.seul.org/*). Iptraf est utile si vous désirez avoir un aperçu instantané de l'activité réseau sur un système Linux. C'est un utilitaire en ligne de commande qui vous donne un aperçu en quelques secondes des connexions et du flux réseau, y compris des ports et des protocoles. Il peut être très utile pour déterminer qui emploie un lien sans fil particulier, ainsi que pour voir son poids de chargement. Par exemple, en montrant une statistique détaillée de l'interruption du fonctionnement d'une interface, vous pouvez immédiatement repérer les usagers et déterminer exactement combien de largeur de bande ils emploient actuellement.

Dépannage

Que faites-vous lorsque le réseau se brise? Si vous ne pouvez pas accéder à une page Web ou au serveur de courriel et si en cliquant sur le bouton de rechargement vous ne réglez pas le problème, alors vous aurez besoin d'isoler l'endroit exact d'où il provient. Les outils suivants vous aideront à cerner le problème de connexion.

- **ping**. Presque tout système d'exploitation (incluant Windows, Mac OS X, et naturellement, Linux et BSD) inclut une version de l'utilitaire ping. Il util-

ise des paquets ICMP pour essayer d'entrer en contact avec l'hôte indiqué et affiche combien de temps a été nécessaire pour obtenir une réponse.

Savoir quoi contacter est aussi important que de savoir comment contacter. Si vous constatez que vous ne pouvez pas vous connecter à un service particulier par votre navigateur Web (exemple: *http://yahoo.com/*), vous pourriez essayer de le contacter:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Faites « control-C » lorsque vous avez fini de rassembler les données. Si les paquets prennent un long moment avant de revenir, il peut y avoir congestion de réseau. Si les paquets de retour ping ont un ttl inhabituellement bas, il peut y avoir des problèmes de routage entre votre ordinateur et l'hôte distant. Mais que se passe-t-il si le ping ne retourne aucune donnée du tout? Si vous contactez un nom au lieu d'une adresse IP, vous pouvez avoir des problèmes de DNS.

Essayez de contacter une adresse IP sur Internet. Si vous ne pouvez pas y accéder, c'est peut-être une bonne idée d'essayer si vous pouvez contacter votre routeur par défaut:

```
$ ping 216.231.38.1
PING 216.231.38.1 (216.231.38.1): 56 data bytes
64 bytes from 216.231.38.1: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 216.231.38.1: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 216.231.38.1: icmp_seq=2 ttl=126 time=13.897 ms
^C
--- 216.231.38.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms
```

Si vous ne pouvez pas contacter votre routeur par défaut, alors il y a des chances que vous ne pourrez pas non plus accéder à Internet. Si vous ne pouvez même pas connecter d'autres adresses IP sur votre LAN local, alors il est temps de vérifier votre connexion. Si vous utilisez un câble Ethernet, est-il branché? Si vous travaillez avec une connexion sans fil, êtes-vous connecté au réseau sans fil approprié? Celui-ci est-il à portée?

Dépanner un réseau à l'aide de ping relève en partie de l'art mais demeure un bon outil pédagogique. Puisque vous trouverez probablement l'utilitaire

ping sur presque tous les ordinateurs sur lesquels vous travaillerez, c'est une bonne idée d'apprendre à l'utiliser de manière appropriée.

- **traceroute** et **mtr** (*http://www.bitwizard.nl/mtr/*). Tout comme ping, traceroute est trouvé sur la plupart des systèmes d'exploitation (il se nomme **tracert** dans certaines versions de Microsoft Windows). En exécutant traceroute, vous pouvez trouver où se situent les problèmes entre votre ordinateur et n'importe quel point sur l'Internet:

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
 1  10.15.6.1  4.322 ms  1.763 ms  1.731 ms
 2  216.231.38.1  36.187 ms  14.648 ms  13.561 ms
 3  69.17.83.233  14.197 ms  13.256 ms  13.267 ms
 4  69.17.83.150  32.478 ms  29.545 ms  27.494 ms
 5  198.32.176.31  40.788 ms  28.160 ms  28.115 ms
 6  66.249.94.14  28.601 ms  29.913 ms  28.811 ms
 7  172.16.236.8  2328.809 ms  2528.944 ms  2428.719 ms
 8  * * *
```

Le commutateur **-n** indique à traceroute de ne pas prendre la peine de résoudre les noms DNS, en le faisant donc fonctionner plus rapidement. Vous pouvez voir qu'au saut sept, le temps de voyage bondit à plus de deux secondes, alors que les paquets sont jetés au saut huit. Ceci pourrait indiquer un problème à ce point dans le réseau. Si vous contrôlez cette partie du réseau, il pourrait être intéressant de commencer votre effort de dépannage à ce point là.

My TraceRoute (mtr) est un programme utile qui combine ping et traceroute dans un outil simple. En exécutant mtr, vous pouvez obtenir une moyenne continue de latence et de perte de paquet à un hôte donné au lieu de la présentation momentanée offerte par ping et traceroute.

```
                           My traceroute  [v0.69]
tesla.rob.swn (0.0.0.0)        (tos=0x0 psize=64 bitpatSun Jan  8 20:01:26 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                   Packets               Pings
 Host                            Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. gremlin.rob.swn               0.0%     4    1.9   2.0   1.7   2.6   0.4
 2. er1.sea1.speakeasy.net        0.0%     4   15.5  14.0  12.7  15.5   1.3
 3. 220.ge-0-1-0.cr2.sea1.speakeasy.  0.0%     4   11.0  11.7  10.7  14.0   1.6
 4. fe-0-3-0.cr2.sfo1.speakeasy.net   0.0%     4   36.0  34.7  28.7  38.1   4.1
 5. bas1-m.pao.yahoo.com          0.0%     4   27.9  29.6  27.9  33.0   2.4
 6. so-1-1-0.pat1.dce.yahoo.com   0.0%     4   89.7  91.0  89.7  93.0   1.4
 7. ae1.p400.msr1.dcn.yahoo.com   0.0%     4   91.2  93.1  90.8  99.2   4.1
 8. ge5-2.bas1-m.dcn.yahoo.com    0.0%     4   89.3  91.0  89.3  93.4   1.9
 9. w2.rc.vip.dcn.yahoo.com       0.0%     3   91.2  93.1  90.8  99.2   4.1
```

Les données seront constamment mises à jour et ramenées à une moyenne. Comme avec ping, vous devez faire « control-C » une fois que vous avez fini de regarder les données. Notez que pour exécuter mtr, vous devez avoir des privilèges de superutilisateur (*root*).

Tandis que ces outils ne révèlent pas avec précision ce qui ne fonctionne pas avec le réseau, ils peuvent vous fournir assez d'information pour savoir où vous devez continuer le dépannage.

Test de performance

À quelle vitesse peut aller le réseau? Quelle est la capacité utilisable réelle d'un lien particulier du réseau? Vous pouvez obtenir une très bonne évaluation de votre rendement en envoyant du trafic sur votre lien et en mesurant combien de temps prend le transfert des données. Même s'il y a des pages Web disponibles qui peuvent réaliser un « test de vitesse » sur votre navigateur (tel que *http://www.dslreports.com/stest*), ces test sont très imprécis si vous êtes loin de la source de test. Pire encore, ils ne permettent pas d'examiner la vitesse d'un lien particulier, mais uniquement la vitesse de votre lien à Internet. Voici deux outils qui vous permettront d'exécuter un test de rendement sur vos propres réseaux.

- **ttcp** (*http://ftp.arl.mil/ftp/pub/ttcp/*). Tccp fait actuellement partie de la plupart des systèmes de type Unix C'est un outil simple de test de rendement de réseau qui fonctionne sur chaque côté du lien que vous désirez examiner. Le premier noeud fonctionne en mode récepteur et l'autre transmet:

```
node_a$ ttcp -r -s

node_b$ ttcp -t -s node_a
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp -> node_a
ttcp-t: socket
ttcp-t: connect
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw
```

Après le rassemblement des données dans une direction, vous devriez renverser les rôles de transmission et réception pour examiner le lien dans l'autre direction. Il peut examiner les courants UDP et TCP et peut changer divers paramètres TCP et la grosseur des tampons pour donner au réseau un bon rendement. Il peut même employer un flux de données écrit par l'usager au lieu d'envoyer des données aléatoires. Rappelez-vous que l'afficheur de vitesse est en kilo-octets et non kilobits. Multipliez le résultat par 8 pour trouver la vitesse en kilobits par seconde.

Le seul inconvénient véritable de ttcp est qu'il n'a pas été développé durant des années. Heureusement, le code est de domaine public et est disponible gratuitement. Tout comme ping et traceroute, ttcp se trouve sur plusieurs systèmes comme outil standard.

- **iperf** (*http://dast.nlanr.net/Projects/Iperf/*). Tout comme ttcp, iperf est un outil de ligne de commande pour estimer le rendement d'une connexion réseau. Il a plusieurs des mêmes caractéristiques que ttcp, mais emploie un modèle « client » et « serveur » au lieu de « réception » et « transmission ». Pour exécuter iperf, initiez un serveur d'un côté et un client de l'autre:

```
node_a$ iperf -s

node_b$ iperf -c node_a
------------------------------------------------------------
Client connecting to node_a, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-11.3 sec   768 KBytes   558 Kbits/sec
```

  Le côté serveur continuera à écouter et à accepter des connexions de client sur le port 5001 jusqu'à ce que vous entriez la commande « control-c » pour l'arrêter. Ceci peut être plus simple si nous exécutons plusieurs tests à partir de divers endroits.

  La plus grande différence entre ttcp et iperf est que iperf est activement en cours de développement et présente plusieurs nouvelles caractéristiques (incluant le support IPv6). Il est un bon choix d'outil lors de la conception de nouveaux réseaux.

Santé du réseau

En suivant l'information à travers le temps, vous pouvez avoir une idée globale de la santé du réseau et de ses services. Ces outils présenteront les tendances de votre réseau et informeront lorsque des problèmes se présentent. Le plus souvent ces systèmes vont s'apercevoir qu'il y a un problème avant même que la personne ait la chance d'appeler le support technique.

- **cacti** (*http://www.cacti.net/*). Comme nous l'avons vu précédemment, beaucoup d'outils emploient RRDtool comme programme moteur (backend) pour créer des graphiques qui vont présenter les données accumulées. **Cacti** est de ce type. C'est un outil PHP de gestion de réseau qui simplifie l'accumulation de données et la production de graphiques. Il stocke sa configuration dans une base de données MySQL et est intégré avec SNMP. À l'aide de cet outil, il est très facile de situer tous les dispositifs sur votre réseau et de tout surveiller: des flux de réseau à la charge de l'unité centrale de traitement. Cacti a un schéma extensible de collecte de données qui vous permet d'accumuler presque n'importe quel genre de données (tel que le signal radio, le bruit ou les usagers associés) et de

tracer le tout sur un graphique en fonction du temps. Des imagettes de vos graphiques peuvent être présentées dans une page Web, vous permettant d'observer l'état global de votre réseau d'un seul coup d'oeil.

- **SmokePing** (h*ttp://people.ee.ethz.ch/~oetiker/webtools/smokeping/*). SmokePing est un autre outil créé par Tobias Oetiker. Il s'agit d'un outil écrit en Perl qui montre la perte de paquet et la latence sur un graphique simple. Il est très utile d'exécuter SmokePing sur un hôte ayant une bonne connectivité sur l'ensemble de votre réseau. Avec le temps, il révèle des tendances qui peuvent indiquer toutes sortes de problèmes de réseau. Combiné avec MRTG ou cacti, vous pouvez observer l'effet que la congestion de réseau a sur la perte de paquet et la latence. De façon optionnelle, SmokePing peut envoyer des alertes quand certaines conditions sont réunies, par exemple, lorsque l'on distingue une perte excessive de paquet sur un lien pendant une période prolongée.
- **Nagios** (*http://www.nagios.org/*). Nagios est un outil de surveillance du service. En plus de suivre la performance de simples pings (comme avec SmokePing), Nagios peut observer la performance des services réels sur n'importe quel nombre d'ordinateurs. Par exemple, il peut périodiquement interroger votre serveur Web pour s'assurer que celui-ci renvoie une page Web valide. Si un contrôle échoue, Nagios peut en informer une personne ou un groupe via courriel, SMS ou messagerie instantannée.

  Alors que Nagios aidera sans doûte un seul administrateur à surveiller un grand réseau, il est mieux utilisé lorsque vous avez une équipe de dépannage avec des responsabilités partagées entre les différents membres. Les événements problématiques peuvent être configurés pour ignorer les problèmes passagers en envoyant des avis uniquement aux personnes qui sont responsables de réparer ce problème en particulier. Si le problème continue pendant une période prédéfinie sans être reconnu, d'autres personnes peuvent alors en être informées. Ceci permet que les problèmes provisoires soient simplement notés sans déranger personne tandis que les problèmes réels sont portés à la connaissance de l'équipe.