

Capitolo 16

I rischi di una rete senza fili **538**

Controllo delle connessioni a un punto di accesso senza fili **541**

Crittografia delle trasmissioni senza fili **544**

Protezione extra per reti senza fili **548**

I sì e i no dell'accesso remoto **549**

Reti e accesso remoto senza fili

Le reti *senza fili* o *wireless* un tempo costituivano una scelta costosa, esoterica, utilizzata solo in applicazioni aziendali specializzate, dove i vantaggi sopperivano al costo rilevante e alla notevole complessità proprie di questa soluzione. Negli ultimi anni, invece, il prezzo dell'hardware per reti senza fili è sceso, fino a giungere a livelli accettabili. La configurazione di una rete senza fili non richiede un'esperienza avanzata (se utilizzate Windows XP) gli adattatori di tipo wireless vengono configurati automaticamente, e l'impostazione di una rete senza fili avviene in genere in pochi minuti.

I vantaggi delle reti senza fili sono davvero molti: utilizzando un computer portatile con installazioni minime, dotato di un adattatore LAN senza fili non costoso, potete accedere al Web e ai file e le stampanti condivisi da qualsiasi posizione, sempre che vi troviate nel raggio d'azione del vostro punto di accesso (chiamato in gergo anche *access point*) senza fili. A casa potete utilizzare il computer sul divano sul balcone o a letto. In ufficio potete portare il computer a una conferenza e avere accesso da quella posizione alle informazioni dell'intranet della vostra società o del Web, e potete inviare per posta elettronica le minute della conferenza appena terminate.

Sfortunatamente tutti questi vantaggi prevedono seri problemi di protezione. Se potete connettervi alla rete a distanza, chiunque potrà farlo disponendo di un computer, un adattatore wireless e una certa determinazione. Potete implementare alcune misure di sicurezza, ma anche lo standard wireless più diffuso include alcune carenze di protezione che richiedono la vostra attenzione.

In questo capitolo spiegheremo cosa dovete e non dovete fare con una connessione senza fili. Spiegheremo inoltre come consentire l'accesso remoto alla vostra rete Windows senza compro-



Parte 3: Protezione di una rete

mettere la sicurezza. La forma di accesso remoto più sicura è dunque la rete privata virtuale o VPN (virtual private network), la quale costituisce comunque un eccellente supplemento anche per le reti senza fili.

Elenco di controllo sulla sicurezza

Se disponete di una rete senza fili, procedete come segue per salvaguardare le risorse condivise.

- Configurate il punto di accesso senza fili con una password sicura.
- Considerate di disabilitare l'amministrazione remota del punto di accesso; se dovete modificare queste impostazioni, potete farlo direttamente, utilizzando la connessione Ethernet o il cavo fornito in dotazione.
- Aggiornate il firmware di tutto l'hardware della rete senza fili con le versioni più recenti, che possono incorporare correzioni relative alla protezione.
- Sostituite il nome della rete (SSID) del vostro punto di accesso con uno che non corrisponda ai valori predefiniti hardware e non riveli informazioni vostre o dell'azienda.
- Utilizzate il controllo di accesso MAC, se è disponibile.
- Attivate Wired Equivalent Privacy (WEP) e impostate chiavi sicure.
- Cambiate le chiavi WEP almeno una volta al mese e preferibilmente ogni settimana.
- Sottoponete a scansione la rete senza fili per determinare se siete vulnerabili agli attacchi con gli strumenti più utilizzati dagli hacker.
- Considerate di utilizzare le reti private virtuali per connessioni senza fili.

I rischi di una rete senza fili

Per capire i problemi di protezione inerenti a una rete senza fili, dovete prima conoscere la struttura di base. Oggi le reti senza fili più diffuse presentano lo standard IEEE 802.11, adottato nel 1997. Tra le variazioni di questo standard troviamo IEEE 802.11b, anche noto come Wireless Ethernet, o Wi-Fi, che trasmette dati a una velocità massima di 11 Mbps, la stessa velocità di una connessione Ethernet convenzionale. I nuovi standard 802.11a e 802.11g utilizzano la stessa tecnologia Wi-Fi per trasferire i dati a velocità fino a 54 Mbps. Per ulteriori informazioni sulle differenze tra i vari componenti dello standard 802.11, consultate la sezione "802. eccetera: decodifica di standard senza fili", a pagina 540.



Capitolo 16: Reti e accesso remoto senza fili

Tutti gli standard 802.11 definiscono meccanismi con cui i dati di rete transitano nell'etere, utilizzando frequenze radio nell'intervallo di 2,4 GHz. Gli adattatori di rete con piccole antenne, in genere installate in uno slot PCMCIA su un computer portatile, o situate in una porta USB su un computer di tipo desktop, trasmettono e ricevono dati per comunicare con il resto della rete. Le configurazioni per reti senza fili più comuni prevedono una periferica hardware chiamata punto di accesso wireless (wireless access point), il quale incorpora un trasmettitore/ricevitore e viene connesso direttamente a Internet o a un concentratore (detto anche *hub*) o instradatore (detto anche *switch*) di rete, spesso agendo come ponte tra le reti con e senza fili. In realtà non è necessario un punto di accesso; le piccole reti possono funzionare mediante una "modalità ad hoc", in cui gli adattatori di rete comunicano direttamente l'un l'altro in una configurazione peer-to-peer.

Poiché la rete senza fili utilizza frequenze radio, chiunque disponga di un computer con un adattatore wireless e che si trovi nell'intervallo del punto di accesso o un singolo adattatore wireless può cercare di connettersi alla vostra rete. Con un modesto investimento in hardware e poche o nessuna abilità tecnica, un estraneo può compromettere la sicurezza della vostra rete in uno dei seguenti modi:

Furto di un servizio Anche se un intruso non può introdursi in singoli computer della rete, può ottenere l'accesso a Internet mediante la vostra connessione. Il risultato può degradare la qualità del servizio di connessione a Internet. Questo rischio è specialmente evidente in aree di alta densità, come condomini, in cui uno dei vostri vicini con un adattatore di rete senza fili può trovarsi nell'intervallo del vostro punto di accesso.

Negazione di un servizio Un intruso che non riesce a connettersi alla vostra rete può tuttavia provocare un arresto nella rete a causa delle richieste di connessione. Con una certa persistenza, un malintenzionato può negare completamente l'accesso alla rete agli utenti legittimi.

Furto o distruzione di dati Gli intrusi che riescono a connettersi alla vostra rete possono accedere alle cartelle e alle stampanti condivise. A seconda delle autorizzazioni assegnate a queste risorse, possono gestire, rinominare o eliminare file esistenti o aggiungerne nuovi.

Dominazione della rete Un intruso che riesce a connettersi alla rete e a utilizzare una vulnerabilità senza patch può installare un programma trojan o modificare le autorizzazioni, esponendo teoricamente i computer della LAN ad attacchi attraverso Internet.



Parte 3: Protezione di una rete

InsideOut

Non fate economia con la protezione

Avete seguito tutte le raccomandazioni di questo capitolo per assicurare il vostro punto di accesso senza fili, ma non potete ancora rilassarvi. Ricordate che le reti senza fili possono operare in una "modalità ad hoc", in cui l'adattatore di ogni computer serve come punto di accesso. Un malintenzionato che non riesce a infiltrarsi nel punto di accesso può cercare di colpire un singolo computer e entrare così nella rete. Per proteggervi, accertatevi di avere installato programmi come i firewall personali su ogni computer contenente un adattatore wireless.

In generale le reti senza fili sono state progettate per essere semplici da utilizzare, non per essere sicure. Una corretta protezione di una rete senza fili richiede molto sforzo extra. Se lavorate in una grande azienda, con accesso a un dominio Windows, più firewall, reti private virtuali e un server in grado di autenticare i computer su un database centrale, potete rendere sicura una rete senza fili con facilità. In una rete domestica o in una piccola rete, tuttavia, le opzioni sono considerevolmente limitate.

802.eccetera: decodifica degli standard di trasmissione senza fili

Il gruppo di lavoro 802.11 dell'Institute of Electrical And Electronic Engineers è responsabile delle specifiche per tutte le reti senza fili. Si tratta di un lavoro di dimensioni ciclopiche, al punto che il gruppo è stato diviso in una serie di piccoli gruppi che gestiscano singole parti del lavoro. Il risultato è una serie di standard, tutti a diversi gradi di complessità e con nomi confusi simili tra loro. Seguono le spiegazioni di quelli più utili per la pianificazione della protezione per la vostra rete senza fili.

- **802.11b**, anche noto come Wi-Fi, è l'attuale leader nella tecnologia delle reti senza fili. Utilizza la frequenza 2,4 GHz per inviare e ricevere dati a una velocità massima di 11 Mbps.
- **802.11a** utilizza un hardware simile a quello di 802.11b, ma trasmette a un intervallo di frequenza diverso, 5 GHz, e può raggiungere una velocità massima di 54 Mbps, cinque volte più veloce di Wi-Fi.
- **802.11g** è un'alternativa allo standard 802.11a che può anch'esso inviare dati lungo la rete a 54 Mbps. Poiché questo hardware utilizza lo stesso intervallo di frequenza degli adattatori Wi-Fi, ovvero 2,4 GHz, i produttori preferiscono periferiche che supportino entrambi gli standard, agevolando la transizione per coloro che dispongono già di molto hardware Wi-Fi e che preferiscono non dover gettare via.
- **802.1x** fornisce un meccanismo per l'autenticazione di computer che si connettono a un punto di accesso senza fili, in genere mediante un server Remo-



Capitolo 16: Reti e accesso remoto senza fili

te Authentication Dial-In User Service (RADIUS). Questo standard emergente è poco pratico per le piccole reti ma è ideale per grandi aziende che dispongono già di uno o più server di autenticazione. E il nome non presenta un errore tipografico: questo standard si applica a reti convenzionali con fili e a quelle senza fili, per cui il nome contiene solo un 1.

- **802.11i** è il successore di Wired Equivalent Privacy (WEP), il sistema di autenticazione costruito nello standard Wi-Fi, che è risultato essere troppo facile da individuare. Quando questo standard verrà terminato, incorporerà probabilmente una tecnica chiamata Temporal Key Integrity Protocol (TKIP).

Altri gruppi operativi stanno lavorando ad aspetti della tecnologia senza fili che riguardano la qualità del servizio (802.11e), le comunicazioni tra punti di accesso (802.11f) e reti ad alta velocità gestite dallo spettro (802.11h).

Un umorista tecnologico ha scritto, “La cosa migliore sugli standard è che ce ne sono così tanti”. Ciò è vero in modo particolare per le reti senza fili. Poiché diverse porzioni degli standard 802.11 sono in varie fasi di sviluppo, potete trovare prodotti che non presentano alcune tecnologie presenti invece in altre periferiche, e potete trovare altri produttori di hardware che introducono tecnologie basate su bozze di standard anziché sulla versione finale. Per ulteriori informazioni sui dettagli tecnici più recenti, consultate il sito ufficiale del gruppo di lavoro di 802.11, <http://www.ieee802.org/11>. Per un breve riassunto più facilmente leggibile, visitate il sito Web di Wireless Ethernet Compatibility Alliance, <http://www.wi-fi.org> (entrambe le fonti sono in inglese).

Controllo delle connessioni a un punto di accesso senza fili

La prima linea di difesa per proteggere una rete senza fili è rendere la connessione più difficile agli estranei, e non è un compito semplice. L'antenna in un punto di accesso senza fili può trasmettere il proprio segnale a centinaia di metri, in qualsiasi direzione. E se vivete in un grosso condominio ma non avete vicini nell'intervallo del punto di accesso, potete comunque essere vulnerabili. Una comunità entusiasta di hacker “drive by” (che girano per la città con un computer portatile cercando reti wireless non protette adeguatamente) ha trasformato l'irruzione in reti senza fili in un hobby, escogitando antenne potenziata e utilità software (con nomi pittoreschi come AirSnort e Network Stumbler, che in inglese significano rispettivamente Sbuffo d'aria e Peccatore della rete) che permettono loro di scoprire dettagli di reti non protette mentre si spostano in città o si siedono in aree pubbliche di un complesso di uffici.



Parte 3: Protezione di una rete

Suggerimento Non lasciate che persone sospette riconfigurino la vostra rete

Quando impostate per la prima volta un punto di accesso senza fili, accertatevi di modificare la password predefinita necessaria per sbloccare l'utilità di configurazione. Con questa precauzione fondamentale proteggerete il punto di accesso e il resto della rete, evitando che possano essere riconfigurati da un estraneo. Le password predefinite sono facili da individuare; cambiate la password predefinita utilizzando una facile da ricordare ma difficile da individuare. Per ulteriori informazioni su come creare una password efficace, consultate la sezione "Creazione di password sicure", a pagina 90. Se il vostro hardware supporta completamente la disabilitazione delle funzionalità di amministrazione con trasmissione senza filo, considerate di fare a meno di questa funzione, preferendogli una connessione diretta via Ethernet, USB o mediante una porta seriale.

In Windows XP, in particolare, il processo di connessione a una LAN senza fili è estremamente semplice, grazie a una funzione chiamata *wireless zero configuration* (ovvero rete senza fili priva di configurazione). La maggior parte dei punti di accesso trasmettono automaticamente la propria presenza, in modo che i computer client possano connettersi non appena entrano nell'intervallo. Quando connettete un adattatore di rete senza fili a un computer Windows XP, il sistema operativo automaticamente scopre il punto di accesso più vicino per quella rete e configura l'adattatore in modo che funzioni con esso. Queste informazioni vengono visualizzate nell'elenco di reti disponibili, come mostrato nella figura 16.1.

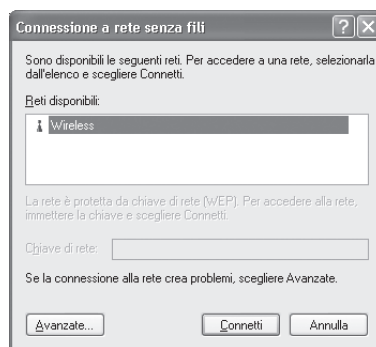


Figura 16.1 In Windows XP vengono individuate automaticamente le reti disponibili e avviene la connessione a esse automaticamente, a meno che non abbiate attivato Wired Equivalent Privacy (WEP).

Il nome della rete mostrato nell'elenco Reti disponibili (in questo caso Wireless) è chiamato anche *Service Set Identifier*, (SSID) o anche *Extended Service Set Identifier* (ESSID). In questo esempio è mostrato il nome SSID di un adattatore wireless USB di NetGear (modello MA101). Alcuni produttori utilizzano nomi predefiniti per il codice SSID; in



Capitolo 16: Reti e accesso remoto senza fili

questo caso, un possibile intruso che conosca il nome predefinito potrebbe connettersi al punto di accesso senza alcun impegno. Se vivete infatti in un condominio con pareti sottili e il vostro vicino utilizza lo stesso hardware da voi utilizzato, è possibile che uno o entrambi vi connettiate inavvertitamente alla rete errata!

Potete prendere una o tutte le seguenti misure di sicurezza per evitare che altre persone scoprano l'SSID della vostra rete e provino a connettersi a essa:

- **Scegliete un nuovo nome per la rete.** Questa è una buona idea se il vostro hardware assegna automaticamente un nome predefinito identico a quelli utilizzati da altre persone che dispongono dello stesso hardware. Qualsiasi casa facciate, non utilizzate un nome che vi identifichi o che identifichi la vostra azienda. Quelle poche informazioni possono incoraggiare gli hacker a provare con maggiore persistenza che non se utilizzaste una stringa numerica casuale.
- **Non trasmettete il nome della vostra rete.** Se il vostro hardware include un'opzione per impostare la rete come un sistema "chiuso", abilitatela. Chiunque desideri connettersi alla rete dovrà fornirne il nome manualmente, anziché trovarlo già immesso automaticamente dall'hardware senza fili e Windows XP; questa precauzione rende vane anche le utilità di scansione delle reti senza fili come Net Stumbler, che non sono in grado di scoprire automaticamente il nome della rete quando utilizzate questa configurazione.
- **Utilizzate indirizzi MAC per limitare l'accesso.** Non tutti i punti di accesso includono questa opzione, con cui potete specificare che gli adattatori wireless che possono connettersi al vostro punto di accesso siano solo quelli con indirizzi MAC nell'elenco immesso. Se la rete è piccola, potete gestire con facilità l'elenco manualmente. Per le reti che presentano più di cinque computer senza fili o che ospitano visite regolari, il peso amministrativo è inaccettabile. Un hacker esperto può ovviamente eludere un indirizzo MAC e saltare questa impostazione, ma può sempre essere un'utile barriera per ficcanaso casuali.

Se avete accesso a un efficace server di autenticazione aziendale, potete configurare la rete in modo che tutte le richieste di connessione siano costrette a essere autenticate con quel server. Questa opzione utilizza lo standard 802.1x e il protocollo Extensible Authentication Protocol (EAP). Nel mercato aziendale potete scegliere tra numerosi tipi di EAP, molti dei quali utilizzano un certificato o una password per autenticare il client della rete senza fili al punto di accesso. Utilizzato con un server RADIUS e una periferica fisica come una smart card, questa opzione può essere estremamente sicura.

Parte 3: Protezione di una rete

Il supporto per l'autenticazione 802.1x è incorporato in Windows XP. Per accedere a queste impostazioni, aprite la finestra di dialogo delle proprietà per la connessione della rete senza fili scegliete la scheda Autenticazione. La figura 16.2 mostra le impostazioni predefinite.

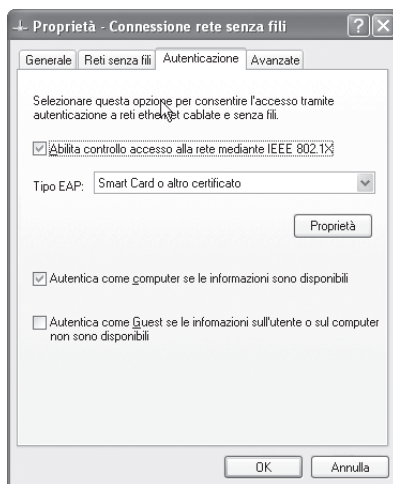


Figura 16.2 Se la vostra rete include un server di autenticazione, potete aumentare enormemente la protezione di una rete senza fili.

Se la vostra rete viene usata in una casa o in una piccola società, non dovete modificare queste impostazioni predefinite. In Windows XP l'autenticazione è possibile per impostazione predefinita, ma questa impostazione viene utilizzata solo quando è disponibile un server idoneo. Se il server di autenticazione utilizza il sistema MD5 challenge anziché un certificato, è vulnerabile ad attacchi di tipo “brute forcing” alla rete.

Crittografia delle trasmissioni senza fili

Dopo questi passaggi di configurazione, siete pronti per affrontare la funzione di protezione più controversa di una rete senza fili: l'attivazione del sistema Wired Equivalent Privacy (WEP). Nello standard originale 802.11b, WEP era definito come uno standard facoltativo, inteso a rendere le reti senza fili sicure quanto quelle cablate. Esso funziona crittografando la trasmissione dei dati tra i client mobili (un computer portatile con adattatore LAN senza fili, per esempio) e il punto di accesso. La maggior parte degli hardware su cui viene utilizzato WEP impiegano una singola chiave condivisa, utilizzata ovunque nella rete. Un difetto nello standard consente a questa chiave di essere facilmente scoperta da malintenzionati remoti, rendendo le implementazioni di WEP non sicure.

Capitolo 16: Reti e accesso remoto senza fili

Su molti prodotti senza fili per reti domestiche, la crittografia WEP è facoltativa. Su altri, tra cui la linea Agere Systems Orinoco, è abilitata per impostazione predefinita, con la serie economica Silver, la quale utilizza una debole crittografia a 40 bit, con una chiave composta da cinque caratteri di 8 bit, e la serie più costosa Gold in cui è utilizzata una crittografia a 104 bit, utilizzando una chiave di 13 caratteri. Se utilizzate hardware 802.11b, consigliamo di abilitare WEP come prima protezione e di aggiornare il suo livello a 104 bit. Per via delle vulnerabilità documentate di WEP, alcuni esperti di protezione consigliano di disabilitarla completamente. Pensiamo che il consiglio sia a breve termine. Sebbene WEP non fornisca alcuna protezione assoluta contro un malintenzionato sufficientemente determinato e debba essere affiancata da altre tecniche di protezione, abilitando questa opzione potrete arrestare hacker principianti e vicini fastidiosi. Alcuni produttori di hardware hanno inoltre risolto alcuni difetti di protezione nello standard WEP originale. Potete aggiornare il firmware nel vostro punto di accesso e negli adattatori LAN senza fili per incorporare questi miglioramenti.

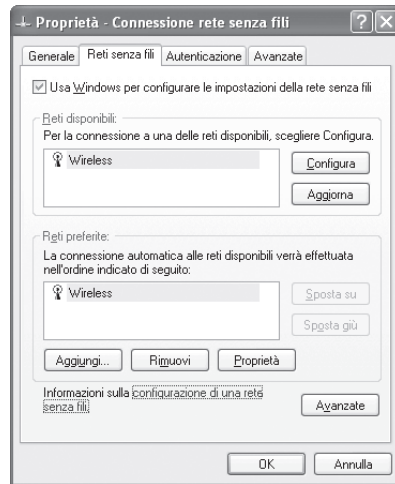
Nota Perché WEP utilizza dimensioni di chiavi particolari, come quelle a 40 e 104 bit? La chiave inviata per l'autenticazione include un *vettore di inizializzazione* di 24 bit, combinato con la chiave condivisa. Il risultato è una chiave che consiste di 64 bit (40+24) o 128 bit (104+24).

Per abilitare WEP sul vostro punto di accesso, dovete utilizzare l'apposita utilità di configurazione fornita con l'hardware del punto di accesso poiché in Windows non sono disponibili strumenti standard per configurarli. Se il vostro hardware comprende una opzione per aggiornare la crittografia da 40 bit a 104 bit, utilizzatela. Trascrivete la chiave condivisa e osservate con attenzione le altre impostazioni sul vostro punto di accesso.

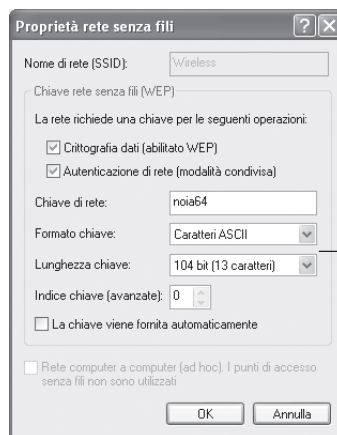
Dopo avere abilitato WEP su un computer Windows 2000, dovete utilizzare il software per il lato client per fornire la chiave condivisa. Se utilizzate Windows XP, il sistema operativo gestisce questa attività senza richiedere altro software e questa chiave dovrebbe essere richiesta alla prima connessione a una rete abilitata per WEP. Per immettere la chiave manualmente, procedete come segue (supponiamo che abbiate a disposizione un solo punto di accesso su una piccola rete):

- 1 Aprite la cartella Connessioni di rete, fate clic destro sull'icona dell'adattatore wireless e scegliete Proprietà. Se la scansione automatica è attiva, il nome della rete per il vostro punto di accesso dovrebbe essere visualizzato nell'elenco Reti disponibili e nell'elenco Reti preferite della scheda Retri senza fili.

Parte 3: Protezione di una rete



- 2 Selezionate la voce nell'elenco Reti preferite e scegliete Proprietà. Se avete disabilitato la scansione automatica sul vostro punto di accesso, fate clic sul pulsante Aggiungi.
- 3 Nella finestra di dialogo Proprietà rete senza fili mostrata nella figura 16.3, modificate le impostazioni come mostrato di seguito.



Controllate queste impostazioni prima di cambiare la chiave della rete

Figura 16.3 Per aumentare la protezione di una rete senza fili, modificate le impostazioni come mostrato qui. Fatelo dopo avere configurato il vostro punto di accesso.

Capitolo 16: Reti e accesso remoto senza fili

- Se è necessario, compilate la casella Nome di rete (SSID). Questo campo è automaticamente compilato e non disponibile se avete abilitato la scansione automatica sul punto di accesso.
 - Selezionate Crittografia dati (abilitato WEP). Con questa impostazione le trasmissioni dei dati sulla rete vengono crittografate.
 - Selezionate Autenticazione di rete (modalità condivisa). Questa impostazione richiede la chiave corretta prima di autenticare un computer.
 - Scegliete i valori per Lunghezza chiave (40 o 104 bit) e Formato chiave (Caratteri ASCII o Cifre esadecimali) in modo che corrispondano alle impostazioni del vostro punto di accesso.
 - Compilate il campo Chiave di rete utilizzando la stessa chiave impostata sul punto di accesso.
 - Deselezionate la casella La chiave viene fornita automaticamente. Questa impostazione viene utilizzata quando la chiave viene memorizzata sull'adattatore wireless.
- 4 Fate clic su OK per chiudere la finestra di dialogo e salvare le impostazioni.

Per via della debolezza nella crittografia WEP, gli esperti della protezione consigliano che modifichiate le chiavi WEP a intervalli regolari, almeno una volta al mese. Sebbene questo processo possa risultare noioso, è una precauzione necessaria su qualsiasi rete senza fili non compatibile con lo standard di autenticazione 802.11i.

Suggerimento Provate questa soluzione semplice e pratica

L'interruttore di accensione del vostro punto di accesso senza fili è uno strumento di protezione sorprendente. Se la maggior parte della vostra rete è composta da computer con fili e utilizzate funzioni senza fili solo occasionalmente, potete ridurre il rischio di intrusioni esterne disattivando il punto di accesso quando non dovete utilizzarlo. In una rete aziendale che opera solo durante il giorno, considerate di collegare la presa di alimentazione del punto di accesso a un timer, tramite il quale attiverete il punto di accesso solo durante gli orari d'ufficio. Questa soluzione "low-tech" è un'eccellente garanzia contro possibili intrusi che potrebbero essere tentati a provare a irrompere di notte, quando non potete notare il traffico indesiderato.



Protezione extra per reti senza fili

Su piccole reti le misure illustrate in questo capitolo dovrebbero essere sufficienti per proteggervi dalle più comuni forme di attacchi esterni verso la vostra rete senza fili. Ovviamente si suppone che abbiate protetto il resto della vostra rete utilizzando le precauzioni che sono descritte altrove in questo libro: implementando un criterio di protezione efficace, utilizzando password robuste, limitando l'utilizzo degli account di amministratore e impostando con cura l'accesso alle risorse condivise.

Nel mondo aziendale, in cui il valore delle informazioni memorizzate nella rete è alto, può essere necessario implementare ulteriori precauzioni per salvaguardare una rete senza fili. La maggior parte di questi passaggi comporta investimenti in fatto di software e hardware che provocano un notevole aumento del costo e della complessità della rete. Se la vostra azienda gestisce dati di routine estremamente delicati ed è soggetta ad adempimenti legali sul suo archivio (come le cartelle cliniche di un ospedale, o la corrispondenza di un cliente in un ufficio legale), dovete analizzare le attrezzature di protezione della rete senza fili prima di acquistarle e implementarle. L'investimento richiesto per salvaguardare i dati possono essere proibitivi.

Una discussione dettagliata di queste opzioni va oltre lo scopo di questo libro; le seguenti opzioni vi daranno un'idea dei fattori da considerare quando impostate una rete senza fili in un ambiente delicato:

- **Evitate la connessione della LAN senza fili a una LAN con fili.** Il punto di accesso senza fili deve essere connesso a un router su una rete separata o su un'interfaccia con firewall.
- **Utilizzate reti private virtuali per tutte le connessioni senza fili.** In questa configurazione il punto di accesso si connette al resto della rete mediante il server, agendo come gateway VPN. Gli intrusi provenienti dall'esterno possono raggiungere il punto di accesso, ma non potranno trasmettere o ricevere i dati senza autenticazione da parte del server VPN. Nella sezione che segue viene descritto come impostare un server VPN su un computer Windows XP o Windows 2000 Professional.
- **Utilizzate uno strumento di scansione per testare la vulnerabilità della vostra LAN senza fili.** Gli stessi strumenti che utilizzano gli hacker per introdursi in reti senza fili sono disponibili gratuitamente mediante download su Internet. Se amministrare una rete senza fili, scaricate una copia di AirSnort dal sito <http://airsnort.shmoo.com>. Troverete Network Stumbler sul sito <http://www.netstumbler.com>. Entrambi i programmi sono ben documentati e facili da utilizzare: potete scoprire un mondo di personaggi stravaganti.
- **Verificare i registri di controllo regolarmente.** Impostate il file registro Protezione per monitorare le connessioni alla vostra rete e rivederle regolarmente. Tenete d'occhio gli eventi di logon dell'account (connessioni realizzate sulla rete) che non corrispondono al comportamento normale degli utenti della rete. Per ulteriori informazioni su come impostare questo tipo di monitoraggio, consultate la sezione "Controllo degli eventi di protezione", a pagina 680.

I sì e i no dell'accesso remoto

Questo libro approfondisce le tecniche per mantenere altre persone lontane dal vostro computer e dalla vostra rete. Tuttavia è lecito voler consentire attente connessioni controllate alle risorse della rete. Per reti domestiche e di piccoli uffici, dove occorre soltanto una singola connessione d'ingresso, Windows XP e Windows 2000 dispongono di tutto il necessario.

Impostazione di una rete privata virtuale

Una *rete privata virtuale* (VPN) è uno strumento sicuro per connettere una rete privata, come una rete domestica o di un ufficio, mediante una rete pubblica (in genere Internet). Utilizzando una connessione VPN, potete accedere a tutte le risorse di rete come se foste connessi direttamente alla rete, e potete farlo da qualsiasi posizione in cui sia possibile realizzare una connessione a Internet.

Le connessioni VPN funzionano mediante il *tunneling* tra i due computer (o le due reti), che sono connessi a Internet. I protocolli per il tunneling viaggiano lungo la rete pubblica utilizzando protocolli standard, ma ogni pacchetto o frame IP (a seconda del protocollo) è crittografato e inserito in un altro pacchetto o frame con informazioni dell'intestazione che gli consente di spostarsi da un punto all'altro. Quando il nuovo pacchetto o frame raggiunge la propria destinazione, il software VPN elimina l'intestazione, decodifica i dati originali, e li indirizza alla destinazione finale. Se tentate di inviare dati "in chiaro" ovvero senza crittografia su Internet, chiunque potrebbe intercettare i pacchetti e leggerne il contenuto. In una connessione VPN, invece, i dati sono crittografati prima di essere immessi nella rete pubblica e decodificati solo dopo essere arrivati dietro il firewall di destinazione; chiunque intercettasse dunque i pacchetti vedrebbe solo dati crittografati e quindi illeggibili.

I protocolli di tunneling formano le basi delle connessioni VPN. Sebbene in Windows sia supportata una varietà di protocolli utilizzati da hardware di periferiche legacy, oggi vengono ampiamente utilizzati tre protocolli di tunneling:

- **Point-to-Point Tunneling Protocol (PPTP)**. Con PPTP potete crittografare frame IP, IPX o NetBEUI e inserirli in un'intestazione IP per inviarli lungo una rete intermedia.
- **Layer 2 Tunneling Protocol (L2TP)**. Con L2TP potete crittografare i frame IP, IPX o NetBEUI e quindi inviarli su una rete intermedia IP, X.25, Frame Relay, o ATM.
- **Modalità di tunneling IP Security (IPSec)**. Con IPSec Tunnel Mode i pacchetti IP possono essere crittografati e decodificati, quindi inseriti in un'intestazione IP per essere inviati in una rete intermedia. IPSec è spesso accoppiato con L2TP per scopi di crittografia, perché L2TP non supporta la crittografia di dati.



Parte 3: Protezione di una rete

Windows XP e Windows 2000 utilizzano PPTP o L2TP per connessioni di tunnel. Solo Windows 2000 Server o Windows .NET Server possono agire come server per connessioni VPN utilizzando L2TP. Con Windows XP e Windows 2000 Professional potete tuttavia connettervi a un server VPN utilizzando L2TP. Con Windows XP e Windows 2000 potete utilizzare IPSec per migliorare la protezione di tutte le interazioni di rete.

Con il minimo sforzo, potete impostare il computer come un server di accesso remoto, consentendo a chiunque disponga delle credenziali corrette (voi inclusi) di connettersi mediante un VPN. Dopo una autenticazione al VPN, potete accedere alle cartelle condivise sulle unità locali e accedere alla rete e alle risorse condivise altrove sulla rete stessa.

Nota Per creare o modificare connessioni in ingresso, dovete effettuare il login sul computer come membro del gruppo Administrators.

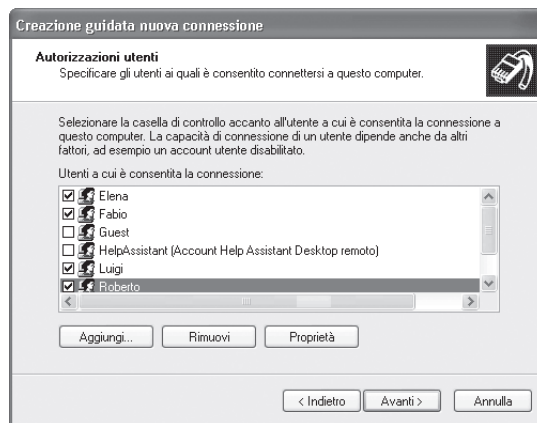
La procedura per impostare una connessione VPN in ingresso è pressoché identica in Windows 2000 e Windows XP. Nei passaggi che seguono, supponiamo che stiate utilizzando Windows XP, tuttavia sono riportate le differenze procedurali in Windows 2000 dove necessario:

- 1 Aprite la cartella Connessioni di rete. In Windows 2000 questa cartella è chiamata Rete e connessioni remote.
- 2 Scegliete File, Nuova connessione. Viene aperta la finestra della Creazione guidata nuova connessione. In Windows 2000 è chiamata Connessione guidata di rete. Se viene visualizzata la finestra di dialogo Informazioni sulla località di chiamata corrente, immettere il prefisso telefonico locale, anche se il computer non dispone di un modem o non avete intenzione di utilizzare il computer per una connessione remota, poi fate clic su OK per due volte.
- 3 Fate clic su Avanti per superare la finestra iniziale della procedura guidata.
- 4 Nella finestra Tipo di connessione di rete selezionate Installazione di una connessione avanzata. In Windows 2000 selezionate Accetta connessioni in ingresso. Fate clic su Avanti.
- 5 Nella finestra Opzioni di connessione avanzate selezionate Accetta connessioni in ingresso e fate clic su Avanti. Questo passaggio non è necessario per Windows 2000.
- 6 Se viene visualizzata una finestra Periferiche per chiamate in ingresso, fate clic su Avanti. Queste opzioni servono per impostare una connessione remota in ingresso, una connessione diretta via cavo, una connessione a raggi infrarossi. Questa finestra viene visualizzata solo se il computer dispone di un modem, di una porta seriale, una parallela o una IrDA.
- 7 Nella finestra Connessione di rete privata virtuale (VPN) in ingresso selezionate Consenti connessioni private virtuali e fate clic su Avanti. In Windows 2000, questa finestra è chiamata Connessione privata virtuale in ingresso.

Capitolo 16: Reti e accesso remoto senza fili

Per ricevere connessioni VPN su Internet, l'indirizzo IP della vostra connessione Internet deve essere noto in Rete. Se il vostro computer è direttamente connesso a Internet, utilizzate l'IP a voi assegnato dall'Internet service provider. Se siete connessi mediante un router o un gateway residenziale, gli utenti remoti specificeranno l'indirizzo IP del gateway; dovrete inoltrare la porta VPN al computer, come descritto nella sezione "Configurazione di un router o gateway residenziale", a pagina 526.

- 8 Nella finestra Autorizzazioni utenti, chiamata Utenti autorizzati in Windows 2000, selezionate la casella di fianco al nome di ogni utente che desiderate autorizzare per effettuare connessioni in ingresso. Verranno elencati tutti gli account utenti locali del computer. Utilizzate il pulsante Aggiungi per creare un nuovo account locale; fate clic sulla scheda Proprietà per creare o modificare una password.



Al termine dell'assegnazione di autorizzazioni utente fate clic su Avanti.

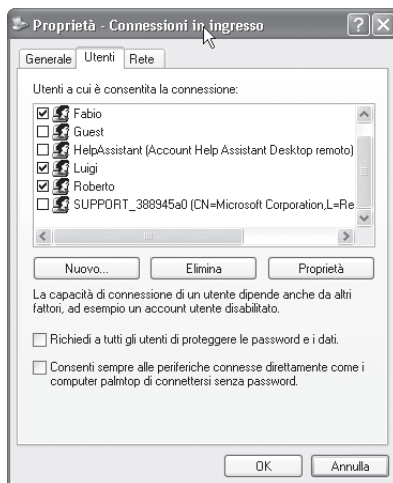
- 9 Nella finestra Software di rete, chiamata Componenti di rete in Windows 2000, selezionate la casella di fianco al nome di ogni componente di rete che desiderate utilizzare per una connessione in ingresso. Per la maggior parte degli utenti, le impostazioni predefinite (che comprendono il Protocollo Internet TCP/IP) sono corrette. Fate clic su Avanti per continuare.
- 10 In Windows 2000 avete l'opportunità di fornire alla connessione un nome descrittivo; in Windows XP no. Fate clic su Fine per salvare la nuova connessione.

Dopo avere creato la connessione in ingresso, potete modificare in qualsiasi momento le impostazioni, aggiungendo o rimuovendo utenti dall'elenco di utenti autorizzati a effettuare una connessione VPN. Aprite la cartella Connessioni di rete, Rete e connessioni remote in Windows 2000, fate clic destro sull'icona della connessione e scegliete Proprietà.

InsideOut

Aggiunta di crittografia a trasmissioni

Una modifica che consigliamo è quella di richiedere che tutti gli utenti della connessione VPN in ingresso effettuino la crittografia di tutti i dati e le password trasmessi. Per impostazione predefinita questa opzione è disattivata sulle connessioni VPN. Fate clic destro sull'icona della connessione in ingresso e scegliete Proprietà. Fate clic sulla scheda Utenti e selezionate la casella Richiedi a tutti gli utenti di proteggere le password e i dati. Prima che un utente possa connettersi a un VPN con questa opzione abilitata, deve aprire la finestra di dialogo delle proprietà per la connessione VPN in uscita, scegliere la scheda Protezione e selezionare Richiedi crittografia dati (disconnetti se non disponibile).



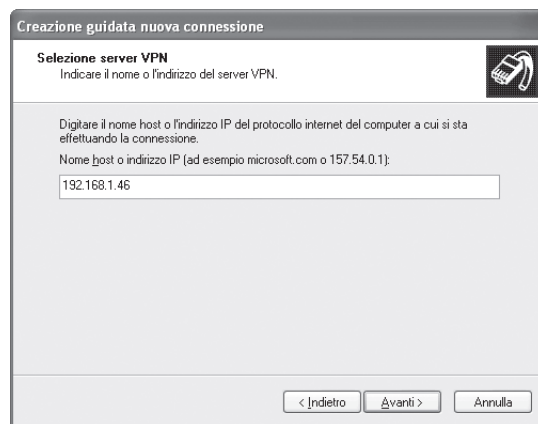
Connessione a una VPN

Dopo avere creato una connessione VPN in ingresso, dovete connetterla da qualsiasi computer Windows XP o Windows 2000. Utilizzate la procedura guidata per creare una nuova connessione di rete; dopo avere superato la schermata iniziale, procedete come segue in Windows XP:

- 1 Nella finestra Tipo di connessione di rete selezionate Connessione alla rete aziendale e fate clic su Avanti.
- 2 Scegliete Connessione VPN. Fate clic su Avanti.

Capitolo 16: Reti e accesso remoto senza fili

- 3 Nella finestra Nome connessione immettete un nome descrittivo; questo testo verrà utilizzato per identificare la connessione nella cartella Connessioni di rete. In Windows XP si suppone che siate connessi a una rete aziendale, ma potete immettere qualsiasi testo desideriate. Fate clic su Avanti.
- 4 Nella finestra Rete pubblica scegliete una delle seguenti opzioni, quindi fate clic su Avanti:
 - **Non effettuare prima alcuna connessione.** Selezionate questa opzione se il computer su cui state creando la connessione dispone di una connessione a Internet permanente ad alta velocità, o se desiderate connettervi sempre a Internet manualmente prima di connettervi alla VPN.
 - **Connetti automaticamente a.** Scegliete questa opzione e selezionate un'icona di connessione remota. Questa opzione è più appropriata su un computer che normalmente si connette a Internet utilizzando la stessa connessione remota.
- 5 Nella finestra Selezione server VPN immettete il nome o l'indirizzo IP del computer che è in grado di accettare le connessioni in ingresso. Per la maggior parte delle reti domestiche e di piccoli uffici, dovete immettere qui un indirizzo IP. Fate clic su Avanti.



- 6 Fate clic su Fine per salvare la connessione. Osservate la comoda opzione per creare un collegamento alla connessione sul desktop. Se avete intenzione di utilizzare spesso questa connessione VPN e desiderate evitare di doverla cercare sempre nella cartella Connessioni di rete, selezionate questa casella prima di fare clic su Fine.

In Windows 2000, la procedura è simile. Nella finestra Tipo di connessione di rete, scegliete Connessione a una rete privata attraverso Internet, quindi seguite la stessa procedura descritta per Windows XP.



Parte 3: Protezione di una rete

Le connessioni VPN funzionano in modo simile a una connessione remota. Quando fate doppio clic sull'icona per la connessione VPN, Windows contatta il nome del computer o l'indirizzo IP (stabilisce prima una connessione remota, se è necessario), quindi invia le credenziali che immettete. Se le credenziali vengono accettate, potete accedere alle risorse condivise dalla cartella Risorse di rete o immettendo gli indirizzi in formato UNC.

Soluzioni

Non riuscite a connettervi a VPN da un altro computer.

Dopo avere impostato una connessione VPN su un altro computer, potete non essere in grado di connettervi. Ciò può accadere se un firewall alla fine della connessione blocca il traffico VPN.

Quando utilizzate la procedura guidata Crea nuova connessione in Windows XP per creare una connessione VPN in ingresso, la procedura guidata configura correttamente in modo automatico il Firewall connessione Internet. Potete confermare ciò visitando la cartella Connessioni di rete, aprendo la finestra di dialogo delle proprietà per la connessione a Internet, facendo clic sulla scheda Avanzate, quindi clic su Impostazioni. Dovreste vedere le voci per Connessione VPN in entrata (L2TP) e Connessione VPN in entrata (PPTP): entrambe devono essere selezionate.

Se utilizzate un firewall di tipo software diverso da quello integrato in Windows XP, dovreste configurarlo in modo analogo. Per le connessioni PPTP (il tipo più utilizzato per le connessioni VPN in Windows XP), dovete far sì che la porta 1723 per comunicazioni TCP risulti aperta. Le connessioni L2TP, che utilizzano la porta 1701, richiedono un certificato di autenticazione del computer e sono disponibili solo quando il server VPN è su una rete con Windows .NET Server o Windows 2000 Server. Se state cercando di connettervi a un server utilizzando L2TP, dovreste richiedere l'aiuto dell'amministratore di rete per individuare e installare un certificato compatibile, per poter effettuare così una connessione.

Se il firewall installato sul computer client filtra il traffico esterno oltre alle connessioni in ingresso (ZoneAlarm si comporta in questo modo, per esempio), anche per quel computer dovreste far sì che anche la porta 1723 sia aperta.

Se siete certi che i firewall a ogni estremità della rete VPN non stiano bloccando il traffico, ma non riuscite a connettervi, il problema potrebbe trovarsi nel mezzo. Alcuni ISP (Internet Service Provider) bloccano il traffico VPN o lo consentono solo con alcuni tipi di account. Consultate il vostro ISP per informazioni su questi criteri.

Protezione di una connessione remota

Le connessioni VPN e le connessioni a Internet ad alta velocità sono state create l'una per l'altra. Impostare una connessione VPN sempre attiva a una linea DSL è semplice e rapido, e potete contare sul fatto che la connessione è sempre disponibile finché



Capitolo 16: Reti e accesso remoto senza fili

lasciate il computer acceso. In alcune circostanze, tuttavia, potreste non avere la possibilità di configurare un server VPN raggiungibile dall'esterno tramite Internet. È possibile che il vostro ISP blocchi il traffico sulla porta, oppure che il router usato non permetta di inoltrare porte a un computer sulla rete locale.

Inoltre, anche quando la configurazione di una connessione VPN in ingresso è tecnicamente fattibile, in effetti, potreste scegliere di non effettuarla per motivi di sicurezza. L'impostazione di una connessione VPN in ingresso che risponda al traffico sulla porta 1723 corrisponde a "bucare" (ovvero rendere vulnerabile) il firewall, e la porta aperta potrebbe richiamare l'attenzione di un utente non autorizzato e potreste non desiderare correre il rischio che un intruso possa sfruttare tale vulnerabilità o ottenere indebitamente una password facile da individuare.

In ogni caso, dovete considerare di utilizzare una connessione remota. Vi occorrerà un modem configurato per rispondere automaticamente, oltre a una linea telefonica che potete dedicare alle chiamate di dati in ingresso. Le velocità di trasmissione, ovviamente, saranno solo una frazione di ciò che potete aspettarvi da una connessione a banda larga. Il vantaggio è tuttavia che la connessione in ingresso sarà più sicura di una a cui avete accesso da Internet. Per realizzare una connessione, un utente remoto deve conoscere il numero di telefono corretto e disporre delle credenziali di accesso da voi definite per la connessione.

Per realizzare la connessione, seguite le istruzioni descritte nella sezione "Impostazione di una rete privata virtuale", a pagina 549, ma sostituite i passaggi da 6 a 8 con i seguenti:

- 6** Nella finestra Periferiche per chiamate in ingresso selezionate il modem da utilizzare.
- 7** Nella finestra Connessione di una rete privata virtuale (VPN) in ingresso, selezionate Non consentire connessioni private virtuali.
- 8** Nella finestra Autorizzazioni utenti selezionate la casella di fianco al nome di ogni utente che può effettuare una connessione in ingresso.

Come ulteriore precauzione (e misura di potenziale risparmio sulle bollette telefoniche), potete impostare le opzioni di richiamata. Per impostare tali opzioni per un determinato utente, selezionate il suo nome, fate clic su Proprietà, quindi clic sulla scheda Richiamata. Se selezionate un'opzione diversa da Non consentire la richiamata, quando il computer riceve una chiamata, autentica l'utente, effettua la disconnessione dello stesso, quindi effettua una chiamata telefonica verso il modem dell'utente. Procedete come segue per effettuare la selezione:

- Selezionate Non consentire la richiamata se desiderate che l'utente remoto effettui una connessione con una sola chiamata al vostro computer.
- Selezionate Consenti al chiamante di specificare un numero di richiamata se desiderate che il chiamante possa specificare un numero di telefono per una chiamata di ritorno.



Parte 3: Protezione di una rete

- Selezionate **Utilizza sempre il seguente numero** per la richiamata e specificate un numero di telefono se desiderate che il vostro computer chiami l'utente solo a un determinato numero telefonico. In questo modo si riduce la possibilità che un intruso che abbia scoperto un nome utente e una password validi possa accedere al sistema.