Tecniche di protezione delle reti Wireless

Sicurezza Nelle Wireless LAN

Giuseppe Paternò

Sicurezza Nelle Wireless LAN

Giuseppe Paternò

Sicurezza Nelle Wireless LAN

Prefazione di: Luca Sciortino

Autore ed Editore: Giuseppe Paternò

ISBN 88-901141-0-X

Edizioni:

Agosto 2003: Prima edizione

SOMMARIO

INDICE DELLE FIGURE

PREFAZIONE

Alcuni giorni or sono ho letto questo articolo su un famoso portale: "Presso dieci McDonalds di New York sarà possibile naviagare 1 ora gratis con il proprio portatile via Wi-Fi. Le ore successive costeranno $3.". Devo dire che mi è spuntato un sorriso sulle labbra... "le successive ore costeranno $3" !!!! La prima cosa che mi è balzata alla mente è che ad un utente un po' smaliziato non serve entrare da McDonalds e consumare per poter accedere alla wireless LAN, basta che ci si metta nel parcheggio di fronte. Vi immaginate la configurazione di quell'Access Point??? "Si accomodi pure questo è il menù e queste le sue chiavi Wep". Ma dai non scherziamo... chiavi WEP???

Per quanto riguarda la situazione italiana, il nostro ministro per le comunicazioni Maurizio Gasparri ha autorizzato in passato alcune società a fare delle sperimentazioni come servizio pubblico per capire l'impatto dal punto di vista tecnologico. Da poco il ministro ha firmato il decreto per la fruizione in ambito pubblico della tecnologia 802.11, a breve quindi il nostro paese si arricchirà ufficialmente di un nuovo strumento che è si sta già ampiamente diffondendo all'interno di edifici di proprietà, aziende, edifici statali ed edifici residenziali privati.

Sembra effettivamente tutto fantastico... niente più cablaggio, comodità per chi si sposta, costi contenuti, un business notevole! Come al solito però sembra che siano stati tralasciati gli aspetti più critici di tutto questo business... *la sicurezza*. Sebbene le Wireless LAN abbiano innumerevoli vantaggi, esistono delle nuove problematiche legate al mezzo trasmissivo via etere che hanno dei risvolti relativi alla sicurezza. L'etere è un mezzo trasmissivo pubblico: chiunque, con delle apparecchiature relativamente semplici, è potenzialmente in grado di captare il segnale delle Wireless LAN e introdursi nel sistema informativo di un'azienda.

I vendors si sono preoccupati solo in parte di questo aspetto, anche al di fuori dell'ambito wireless, del resto a loro importa la vendita dei loro prodotti. Qui invece dobbiamo lottare per rendere sicuri i nostri apparati, la cui responsabilità legale (altro aspetto di cui pochi si preoccupano) è solo ed esclusivamente nostra. Pensate all'utilizzo del wireless in campo medico in cui il dottore può tranquillamente accedere da qualsiasi punto dell' ospedale alla cartella medica del proprio paziente. Pensate però a quanto può essere pericoloso se nelle vicinanze

dell' ospedale si trovi un ragazzetto incauto e senza e scrupoli che si metta a giocare con lo stesso database dei pazienti solo perchè nell' impianto non è stato considerato l'aspetto della sicurezza.

Questo libro non vuole essere una guida di installazione e manutenzione delle singole applicazioni, ma vuole fornire al lettore idee e suggerimenti su come installare e proteggere la propria rete Wireless. È adatto ad un pubblico con una minima conoscenza sistemistica, approfondisce il funzionamento e gli aspetti tecnici legati alle reti Wireless, si consiglia la lettura a coloro che abbiano dimestichezza con le reti, l protocollo TCP/IP, ed un sistema operativo, sia esso Windows o Linux.

Luca Sciortino

Organizzazione del libro

Il libro è stato suddiviso in dieci capitoli, ognuno dei quali analizza e approfondisce le tecnologie che possono essere usate nell'ambito delle Wireless LAN. Partendo dal primo capitolo e proseguendo nella lettura, si passerà da concetti di base a livelli di implementazione sempre più complessi. Si consiglia di leggere ciascun capitolo prima di passare a quello successivo, ma la struttura di questa pubblicazione permette al lettore di consultare i singoli capitoli durante la fase implementativa nella propria rete senza fili.

Nel primo capitolo vengono analizzate le Wireless LAN ed i relativi problemi di sicurezza ad esse legati con un breve accenno alle tipologie di attacco.

Il secondo capitolo dà dei suggerimenti di base su come configurare in maniera efficace gli apparati wireless e quali strumenti e tecniche possono essere adottate a livello auditing di rete.

Il terzo capitolo tratta in modo approfondito l'integrazione di un proxy server in ambiente wireless su architetture Windows/Linux come gesione centralizzata rivolta ad una miglioria della sicurezza della LAN.

Il quarto capitolo si focalizza sulle tecnologie PPPoE e su come queste possono essere impiegate nell'ambito degli ISP per mettere in sicurezza le Wireless LAN. Vengono forniti esempi con i più diffusi server e client.

Nel quinto capitolo viene spiegato in modo esaustivo l'autenticazione IEEE 802.1x con particolare dettaglio sui metodi di autenticazione ed esempi su come realizzare l'infrastruttura per ospitare l'autenticazione basata su questo protocollo.

Nel sesto capitolo si introduce e si analizza il protocollo WI-FI Protected Access (WPA) e le motivazioni che hanno spinto i produttori ad implementare tale tipologia di protocollo.

Nel settimo capitolo si approfondisce il protocollo IPSEC quale integrazione sicura di un protocollo insicuro (TCP/IP). Inoltre si toccano concetti quale VPN (Virtual Private Network) con integrazioni in abito wireless ed esempi di configurazione nelle piattaforme piu' conosciute.

Nell' ottavo capitolo si cercherà invece di analizzare gli strumenti che ogni buon amministratore di sistema dovrebbe avere non solo in un ambiente wireless, ma anche in ambito di una normalissima LAN. Sono a tutti gli effetti strumenti che possono garantire un elevato controllo di quel che succede in una rete.

Il nono capitolo spiega in quali situazioni ed ambiti aziendali applicare le politiche di sicurezza fino a qui descritte. Fondamentale è la preparazione dell'autore che affronta le tematiche legate alla sicurezza in ambiente wireless con considerazioni personali legate alla propria esperienza lavorativa.

Il decimo capitolo vuole fornire dei brevi suggerimenti sulle azioni da intraprendere in caso di incidenti di sicurezza.

L’autore

Giuseppe Paternò ha conseguito la certificazione CCNP ed è membro di IEEE e della Italian Linux Society. La sua passione ha spinto Giuseppe ad esplorare fin da giovanissimo tutti i settori dell'informatica, con particolare riguardo al settore della sicurezza e delle reti, senza tralasciare le nuove sfide tecnologiche. Attualmente lavora come Senior Network and Security Architect presso Sun Microsystems, ma nel suo passato spiccano nomi eccellenti quali IBM e Infostrada. Questo libro scaturisce da una ricerca sulle Wireless LAN durata dieci mesi, in cui Giuseppe ha prodotto un Internet Draft dal titolo "Using PPP-over-Ethernet (PPPoE) in Wireless LANs".

Ringraziamenti

Un grazie enorme va a Luca Sciortino, buon amico e compagno di mille esperimenti informatici. Grazie anche a mia moglie Maria e ai miei genitori per avermi sopportato pazientemente mentre dedicavo il mio tempo all'informatica. Un ringraziamento va anche a chi, in qualche modo, ha contribuito alle ricerche e al presente libro: Gabriella Cattaneo, Silvio Danesi, Daniele Todde e Marco Misitano.

Convenzioni

Le seguenti convenzioni sono state adottate durante la stesura del presente libro:

Corsivo
: È usato per nomi di files, nomi di directory, comandi da eseguire e riferimenti a comandi/zone di una determinata finestra di Windows.

Sottolineato
: È usato per indicare URLs

`Testo a lunghezza costante`
: Per indicare esempi di codice o di configurazioni

Commenti e suggerimenti

Qualsiasi commento o suggerimento é benvenuto e può essere inviato al seguente indirizzo:

Giuseppe Paternò
Casella Postale 133
20090 Trezzano S/N (MI)
Italia

Oppure via e-mail a *info@gpaterno.com*. Successive edizioni ed eventuali correzioni di questa pubblicazione saranno disponibili sul sito Internet *http://www.gpaterno.com/*.

1. WIRELESS LAN

La necessità di mobilità e di copertura in ambienti aperti o difficili da raggiungere tramite cavi (es: ospedali, aereporti o palazzi antichi) hanno favorito la diffusione delle tecnologie wireless. Esistono diverse metodologie di trasmissione dati via etere, quali ad esempio il GPRS, Bluetooth e 802.11, detta anche Wireless Ethernet o Wi-Fi (Wireless Fidelty). La diffusione di quest'ultima sta aumentando notevolmente negli ultimi mesi presso le aziende e utenze private, data la facilità di installazione, le sue prestazioni (11Mbps o 54Mbps) e la sua flessibilità con costi ridotti.

Esistono però dei rischi di sicurezza collegati all'uso delle tecnologie wireless. Alcuni di questi rischi esistono anche nelle reti di tipo tradizionale, ma vengono esasperati dalla tipologia di collegamento senza fili. La trasmissione attraverso onde radio non è confinabile ad uno spazio ben definito, quale può essere quello della trasmissione via cavo: come per l'ascolto di una radio, è possibile per un potenziale intruso avvicinarsi all'esterno del palazzo e "captare" le onde radio. Così come per le reti cablate, attraverso appositi strumenti, è possibile visualizzare i dati che vengono ricevuti e inviati, rendendo disponibile all'eventuale intruso preziose informazioni quali utenze e password, e, in alcune situazioni, addirittura accedere ai database e corrompere i dati. Un altro fattore di rischio molto importante, ma spesso sottovalutato, è che un eventuale intruso non abbia nessun interesse a prendere informazioni sulla rete attaccata, ma voglia utilizzare la rete vittima come "ponte" per attaccare una terza entità, con cui spesso si ha una relazione di fiducia. L'intruso sarà solito usare il "ponte" per offuscare le proprie traccie: da un punto di vista puramente giuridico, l'amministratore della rete wireless violata sarà formalmente responsabile dell'atto di pirateria informatica nei confronti della terza entità, fino a quando le autorità giudiziali non troveranno prova dell'avvenuta intrusione.

La Wireless Ethernet dispone di un sistema di sicurezza che viene chiamato Wired Equivalent Privacy, detto comunemente WEP. Questa specifica, nata per garantire la privacy delle utenze, è basata però su di un sistema di crittografia debole che si è rilevata controproducente: attraverso un'analisi probabilistica di una piccola quantità di dati cifrati, è possibile risalire alla chiave di crittografia e pertanto accedere alla rete. Il rischio principale è che WEP dà una falsa sensazione di sicurezza agli utenti, conseguentemente i dati non cifrati possono essere

facilmente catturati da intrusi.

Questo libro ha lo scopo di evidenziare i problemi relativi alle wireless LAN e fornire opportuni suggerimenti su come migliorare la protezione della propria rete.

La tecnologia Wireless LAN

La tecnologia Wireless LAN più diffusa è basata sullo standard IEEE 802.11, in quanto più facile da configurare e più flessibile rispetto ad altre opzioni. Un fattore chiave che ne ha determinato il successo è la specifica 802.11b (conosciuta anche come 802.11 High Rate, Wireless Ethernet o Wi-Fi): attraverso questa rettifica al protocollo originale, la wireless LAN viene vista logicamente come una rete Ethernet tradizionale. In particolare, IEEE 802.11 definisce lo strato fisico e il livello MAC (Medium Access Control) per le reti wireless, ossia per reti locali viste come un'estensione o un'alternativa alle reti cablate. Inoltre la wireless LAN viene vista a livello LLC (Logical Link Layer) come una tradizionale rete Ethernet.

La tabella sottostante riporta le caratteristiche salienti dello strato fisico della Wireless Ethernet:

Livello fisico	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrarossi (IR)
Banda di frequenza	2.4GHz e 5GHz
Velocità di trasmissione	Fino a 11 Mb/s (802.11b) Fino a 54 Mb/s (802.11a e 802.11g)
Sicurezza	Wired Equivalent Privacy (WEP) basata su RC4.

Lo standard 802.11 utilizza un protocollo per la trasmissione dei dati al livello fisico denonimato CSMA/CA (Carrier-Sense, Multiple Access, Collision Avoidance), ossia un protocollo con rilevamento della portante, con accesso multiplo e con elusione delle collisioni. Questo protocollo evita le collisioni invece di rilevarle come nel caso dello standard 802.3. Nel protocollo CSMA/CA, quando un nodo deve trasmettere un pacchetto, si assicura che nessun altro nodo stia occupando il canale. Se il canale non dovesse risultare libero il nodo trasmittente sceglie un tempo casuale da attendere per ritentare la trasmissione. Poichè la probabilità che due nodi scelgano lo stesso fattore di tempo è molto bassa, in questo modo vengono minimizzate le collisioni tra pacchetti.

Lo standard IEEE 802.11 prevede due possibilità: *Reti Strutturate* e *Reti Ad-Hoc*.

La *rete strutturata* è suddivisa in celle (o BSS Basic Service Set), ognuna delle quali è controllata da una stazione base (o Punto di Accesso - AP). Sebbene la

rete possa essere formata da un'unica cella con un unico punto di accesso, la maggior parte delle installazioni sono formate da più celle, dove i punti di accesso sono collegati ad un altra rete che fornisce i servizi (denominata DS Distribution System), normalmente rappresentata da una rete Ethernet. Il sistema costituito dalle celle, dai punti di accesso e dalla rete esterna (DS) è visto come un unica rete 802 dai livelli più alti del modello OSI e viene denominato ESS (Extended Service Set). Lo standard 802.11 definisce anche il concetto di Portale, ossia un dispositivo che mette in comunicazione una rete wireless con un altra basata sugli standard 802, funzionalità che è attualmente integrata nei punti di accesso. Se le zone di copertura dei vari AP si sovrappongono può verificarsi il roaming del terminale attraverso i vari nodi, così come avviene nelle moderne reti per telefoni cellulari.

Una *rete ad-hoc* è composta da soli terminali wireless. Creata spontaneamente, non supporta l'accesso alla rete cablata e non necessita di punto di accesso. Non vi è una struttura nella rete wireless, nè postazioni assegnate da cui poter accedere, normalmente ogni nodo può comunicare con gli altri.

Quando un dispositivo wireless 802.11 vuole accedere in una BSS, esso deve ottenere le informazioni di sincronizzazione da un punto di accesso (o dalle altre stazioni se operante nella rete ad-hoc) per assicurarsi che tutte le stazioni operino con gli stessi parametri. I nodi possono ottenere tali informazioni in due modi:

- *Scansione Passiva*: la stazione attende che arrivi dal punto di accesso il pacchetto di sincronizzazione (Beacon Frame inviato a intervalli regolari).
- *Scansione Attiva*: in questo caso la stazione tenta di localizzare un punto di accesso e invia dei pacchetti sonda (probe packets), in attesa di una risposta dall AP. Questi tipi di pacchetti sono inviati dagli intrusi che tentano di ricavare informazioni sulla rete wireless.

Il pacchetto di sincronizzazione contiene informazioni per il livello fisico, ad esempio la sequenza per il salto di frequenza, il clock del punto di accesso e l'identificativo della BSS (SSID). In caso di sistema aperto il punto di accesso accetterà la connessione da qualsiasi client con una SSID vuota o impostata su *any*. In caso invece di sistema chiuso, l'AP rifiuterà le richieste di accesso che non provengono dai terminali con la corretta SSID impostata. Ogni stazione può essere associata ad un solo punto di accesso, ma i punti di accesso possono essere associati a più stazioni. Un nodo è in grado di trasmettere e ricevere soltanto quando il processo di associazione è terminato.

WEP e il pericolo delle Wireless LAN

Lo standard IEEE 802.11 definisce anche una cifratura opzionale dei dati trasmessi, chiamata Wired Equivalent Privacy (WEP). Come si evince dal suo acronimo, WEP è stato inizialmente concepito per dare una protezione all'utente finale simile a quella disponibile attraverso una rete cablata di tipo tradizionale.

Recenti studi (il più importante dei quali è "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" di Stubblefield, Ioannidis e Rubin) hanno dimostrato che si puo' ricavare la chiave di cifratura WEP dall'osservazione del traffico di rete. In dettaglio, la chiave WEP (da 40 o 104 bit) viene concatenata inizialmente ad un vettore di inizializzazione (IV) di 24 bit per formare una stringa da 64 o 128 bit, che sarà data in input all algoritmo RC4 per formare la chiave di cifratura dei dati. Parallelamente i dati da criptare vengono scomposti in blocchi e concatenati con i bit di checksum (ICV) per formare una stringa della stessa lunghezza della chiave RC4. Infine viene effettuato lo XOR tra la chiave RC4 e i blocchi dati ottenendo il testo cifrato, a cui viene aggiunto il vettore di inizializzazione. Proprio l'uso di quest'ultimo ha determinato la maggior debolezza del protocollo WEP: infatti l'algoritmo RC4 risulta vulnerabile se vengono utilizzate le chiavi più di una volta. Questo è esattamente quello che accade con il WEP: il vettore di inizializzazione è lungo soltanto 24 bit, quindi ammette uno spazio di 16777216 combinazioni (2^24). In aggiunta, il protocollo WEP prevede la reinizializzazione del IV ogni qual volta si origini una collisione nella trasmissione dei pacchetti dati. In una rete di medie dimensioni e con un discreto volume di traffico sono sufficienti pochi minuti affinché vengano riutilizzate le stesse chiavi di cifratura. Tramite meccanismi di criptoanalisi differenziata si può

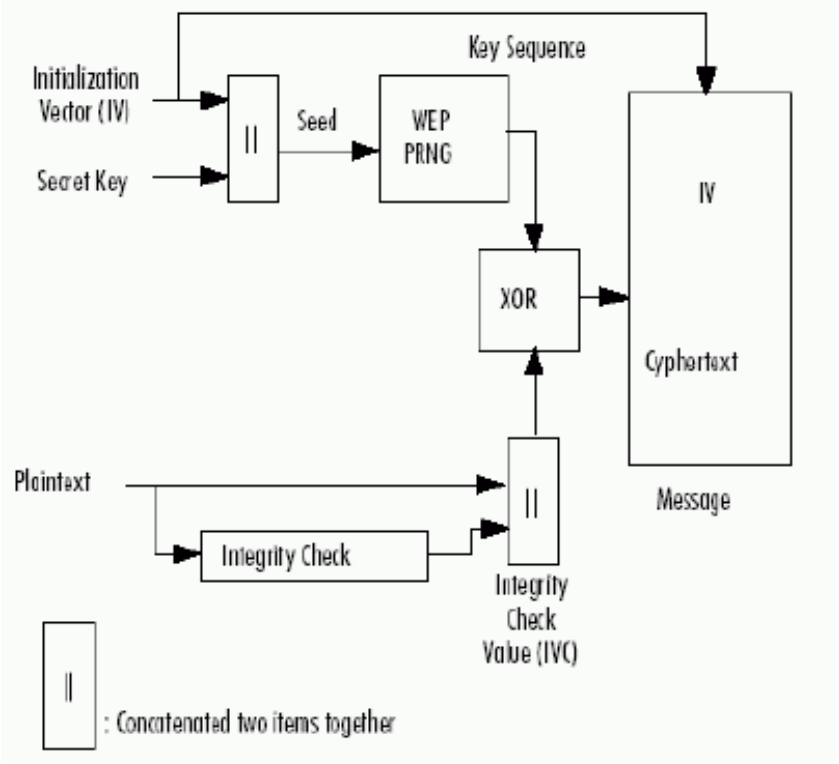

Fig. 1.1 - Sequenza di WEP

risalire in poco tempo alla chiave WEP e decifrare tutto il traffico tramite la chiave individuata. Oltre alle debolezze intrinseche del WEP, bisogna riscontrare che lo standard IEEE 802.11 non fornisce alcun meccanismo sulla custodia e configurazione delle chiavi WEP. Nei casi peggiori alcuni produttori hanno optato nel conservare la chiave WEP nel registro dei sistemi Windows o in un file di testo in Linux, completamente in chiaro; solo in pochi produttori hanno custodiscono la chiave WEP nel firmware della scheda di rete. È da sottolineare che la configurazione delle chiavi WEP è manuale, con un notevole sforzo da parte degli amministratori di sistema che sono costretti ad impostare la chiave WEP su ogni singola stazione wireless e punto di accesso. Questo implica una scarsa variazione nel tempo delle chiavi WEP, che è una delle cause principali di penetrazione nei sistemi per i motivi sopra discussi.

Il meccanismo WEP, quindi, dà una falsa sensazione di sicurezza all'utente finale, pertanto tutti i dati non criptati, ad esempio attraverso SSL, possono essere facilmente intercettati da eventuali intrusi.

Configurazioni standard

La configurazione standard delle case produttrici sono uno dei maggiori fattori di rischio per la sicurezza delle Wireless LAN. Gli amministratori di rete, molto spesso per mancanza di tempo, non configurano gli Access Point in maniera dettagliata.

I diversi produttori implementano lo standard IEEE 802.11 con caratteristiche differenti, alcune volte anche con estensioni proprietarie, e quindi con diversa modalità di configurazione. Le password degli Access Point, gli SSID e le chiavi WEP di default sono pertanto facile preda di potenziali aggressori.

Tipologie di attacchi

I rischi descritti nei paragrafi pecendenti possono rendere vulnerabile la propria rete ad attacchi. Possiamo evidenziare tre macro tipologie di attacchi: all'apparato radio, alla rete aziendale o interna e al client wireless.

Attacchi agli apparati radio. Le insicurezze del WEP permettono agli intrusi di eludere la crittografia dei dati trasmessi, così da poter analizzare il traffico wireless e da poter ricavare il contenuto dei dati trasmessi (es: login e password) per futuri attacchi. Inoltre, si possono eseguire attacchi più specifici, come la modifica dei dati in transito, il "replay" di sessioni eseguite dai client e il disturbo del segnale radio (Radio Jamming). Un altro tipo di attacco è l'inserimento di un finto Access Point. Per dirottare la connessione dei dispositivi wireless verso la rete pirata, gli hacker installano un punto di accesso con un segnale più potente

nelle loro vicinanze. Gli utenti tenteranno di collegarsi ai falsi server, fornendo nome utente e password e qualsiasi altra informazione riservata.

Attacchi alla rete aziendale o interna. Il WEP è l'unico modo protocollo nello standard IEEE 802.11 per autenticare gli utenti, pertanto un aggressore può facilmente entrare nella rete aziendale senza dover preoccuparsi di autenticarsi alla rete. Inoltre, non esiste nessun controllo di accesso verso le risorse della rete interna: un intruso puo' effettuare qualsiasi operazione sulla rete senza nessuna limitazione.

Attacchi ai client wireless. Molte architetture prevedono che i client wireless vengano visti come risorse interne, anzichè risorse esterne (o untrusted). Eventuali aggressori possono compromettere i client wireless per ottenere preziose informazioni o per usarli come "ponte" per penetrare nella rete aziendale.

2. PROTEZIONE DELLA RETE WIRELESS

Nel capitolo precedente si sono analizzati i possibili problemi di sicurezza relativi alle Wireless LAN, dovuti maggiormente sia alle limitazioni del protocollo IEEE 802.11 che alla configurazione non corretta degli apparati di rete. Uno dei primi passi per rendere sicura la wireless LAN è pertanto il procedere ad una corretta analisi della propria rete ed a configurare gli apparati in maniera adeguata. Questo capitolo propone dei suggerimenti in tal senso, descrivendo come l'amministratore di rete possa trarre vantaggio dall'aggregazione delle tecnologie esistenti.

Regole di base

Una corretta configurazione degli apparati è un buon inizio per proteggere la rete wireless. Grazie ad alcuni accorgimenti, è possibile "sviare" un eventuale intruso nascondendo dettagli preziosi e rendendo più difficile l'identificazione della rete su cui si sta collegando.

Cambiare gli SSID di default. Il Service Set Identifier (SSID) identifica univocamente ogni punto di accesso all interno della rete. Tramite una configurazione opportuna, soltanto i dispositivi che utilizzano la corretta SSID possono comunicare con i punti di accesso. Molti dei dispositivi hanno già preconfigurato un SSID di default: un intruso può usare questi nomi per cercare di accedere ad AP che hanno ancora la configurazione di fabbrica. Di seguito si riportano alcuni SSID di default:

SSID	Produttore
tsunami	Cisco
101	3Com
RoamAbout Default Network Name	Lucent/Cabletron
Compaq	Compaq
WLAN	Addtron
intel	Intel
linksys	Linksys
Default SSID	
Wireless	

Utilizzare SSID non descrittivi. Usare SSID descrittivi facilita il compito di un eventuale intruso nell'individuare luoghi o aziende e nel ricavare maggiori informazioni su come entrare. Si consiglia di utilizzare nomi anonimi o altamente scoraggianti come "AC01MLX", "HoneyPot01" o "GoAway01".

Disabilitare il Broadcast SSID. Gli AP mandano ad intervalli regolari Beacon Frames per la sincronizzazione con i client, i quali contengono il SSID. Queste frames servono ai client per configurarsi automaticamente la rete di accesso, ma servono anche a potenziali aggressori durante la ricerca delle reti wireless. È auspicabile disabilitare il Broadcast SSID qualora l'AP supporti questa opzione. Il client dovrà essere configurato manualmente con il SSID corretto per poter accedere alla rete.

Cambiare le password. Come per gli SSID, è importante cambiare le password di default degli AP. È buona norma che la password sia lunga almeno otto caratteri e che includa caratteri speciali e numeri.

Aggiornare il firmware. Nella scelta di un Access Point, è preferibile orientarsi verso un apparato che abbia la possibilità di aggiornare il suo firmware. È bene pertanto assicurarsi che l'Access Point abbia l'ultimo livello di firmware consigliato dal produttore.

Chiavi WEP. Anche se è stato dimostrato che WEP non è adeguato a proteggere una rete wireless, rappresenta comunque un deterrente per gli intrusi occasionali. Serve catturare dai 100 Mb a 1 Gb di traffico per provare a ricavare la chiave WEP, pertanto l'aggressore deve essere ben motivato per tentare l'intrusione. Cambiare spesso le chiavi WEP di crittografia sugli AP fa in modo che una rete compromessa, non lo sia a tempo indeterminato: un intruso, infatti, dovrebbe di fatto riprovare a ricavare la chiave WEP, scoraggiandolo da un secondo tentativo. Cambiare le chiavi WEP è abbastanza oneroso: alcuni Access Point supportano la dynamic WEP-key exchange per cambiare la chiave WEP per ogni adattatore. È consigiato controllare dal produttore degli Access Point la disponibilità di questa feature. Alcuni Access Points, ad esempio, non dispongono di questa feature, ma è possibile specificare fino a quattro differenti chiavi per facilitare il cambio periodico della chiave.

Abilitare il MAC filtering. Molti produttori includono nei loro Access Point la possibilità di abilitare soltanto alcune schede di rete, usando come metodo discriminatorio il loro MAC address. Alcuni Access Point permettono di fornire l'elenco dei MAC addresses abilitati attraverso una GUI, linea di comando o RADIUS. Si suggerisce di usare la GUI o la linea di comando nel caso di implementazione con pochi AP, RADIUS in un contesto più ampio. È necessario pero' comprendere che il MAC address di una scheda puo' essere facilmente cambiato, pertanto il MAC filtering non puo' essere usato come solo metodo di protezione.

Spegnere l'AP quando non serve. Gli intrusi agiscono solitamente durante la notte e il fine settimana, ovvero quando la rete ed i sistemi non sono controllati. È consigliato, quando possibile, collegare gli Access Point ad un timer, in modo da spegnerli quando non vengono utilizzati.

Minimizzare l'intensità del segnale. Gli intrusi sfruttano il fatto che le onde radio non si possono limitare a dei luoghi ben definiti, esempio l'ufficio vendite, ma riescono ad espandersi fuori dalle mura perimetrali dall'ufficio. Da qui la definizione del nome "parking lot attack", o più semplicemente attacchi provenienti dal parcheggio. È pertanto importante scegliere un'adeguata collocazione dell'Access Point all'interno dell'edificio, in modo che il segnale sia sufficiente a garantire il collegamento solo ed esclusivamente alla zona interessata. Attraverso appositi strumenti radio o di audit, è necessario verificare che il segnale non sia visibile all'esterno del palazzo o della zona identificata. Per minimizzare l'intensità del segnale, è sufficiente non posizionare l'AP vicino alle finestre e usare antenne direzionali con basso guadagno in decibel. Alcuni AP inoltre hanno la possibilità di definire l'intensità del segnale via software.

Cambiare le community di default di SNMP. Su molti AP risulta installato un agente SNMP (Simple Network Management Protocol). Se la community password non risulta correttamente configurata, un aggressore può leggere e scrivere dati di configurazione sull'AP, in maniera analoga ad altri sistemi che supportano SNMP.

Limitare il traffico di broadcast. Alcuni protocolli, in particolare il NetBIOS su TCP/IP usato da Windows, usano assiduamente i messaggi di broadcast. Questi messaggi di broadcast contribuiscono ad incrementare il valore IV del sistema WEP (si faccia riferimento al capitolo precedente), minimizzando per un intruso i tempi di raccolta dei dati per ricavare la chiave WEP. È consigliabile limitare il traffico di broadcast quando possibile, ad esempio disattivando il protocollo NetBIOS su TCP/IP dal binding con la scheda di rete Wireless.

Protezione del client. Alcuni attacchi sono mirati ai client wireless in quanto vengono usati come ponte per entrare nella rete interna e per ricavare preziose informazioni. Ad esempio, alcuni client wireless scrivono in chiaro, nel registry di Windows o in un file di testo, le chiavi WEP di crittografia. È preferibile usare un personal firewall sui client in modo da ridurre i rischi di attacchi.

Non utilizzare il DHCP. È consigliabile non utilizzare il DHCP per l'assegnazione dinamica degli indirizzi, ma considerare l'utilizzo di IP statici. Anche se è un ulteriore impegno per l'amministratore, è assai utile per evitare che la rete wireless attribuisca indirizzi IP validi a chiunque voglia associarsi con l'AP. Anche se un attaccante, utilizzando uno sniffer wireless, può facilmente ricavare gli IP, il fatto di non distribuirli via DHCP rappresenta un'ulteriore barriera. Inoltre, è consigliabile evitare di usare indirizzamenti di default facilmente intuibili come

192.168.1.0 o 192.168.0.0.

Uso di una VLAN separata. È consigliabile utilizzare una Virtual LAN separata per il traffico wireless, separandola dalla rete intranet. Esistono varie metodologie, che vedremo in seguito, per unire in maniera sicura le due LAN, tra le più semplici ricordiamo l'uso di un router/swich con capacità di filtro IP o un proxy.

In alcune piccole aziende e in ambienti SOHO (Small Office, Home Office) dove la protezione della rete non rappresenta un problema, queste semplici regole sono sufficienti a proteggere l'accesso wireless. In ambienti più critici, dove è necessario mantenere la confidenzialità dei dati, è necessario applicare delle regole più rigorose: vedremo nei prossimi capitoli quali sono le tecniche per proteggere tali ambienti.

Auditing

Uno dei principali meccanismi per conoscere lo stato del proprio livello di sicurezza è quello dell'audit. L'audit non viene eseguito una sola volta, ma è un processo che si ripete a cicli periodici, attraverso il quale gli amministratori di sistema e di rete possono capire la differenza fra il livello attuale di sicurezza e quello descritto nella policy aziendale, in modo da intervenire di conseguenza.

Analogamente, l'attività di auditing per le wireless LAN è un elemento chiave per verificare che la propria infrastruttura sia conforme alle proprie policy, che i parametri di configurazione siano stati impostati correttamente e che il segnale radio sia effettivamente limitato all'area che si intende coprire. È importante sottolineare che attraverso l'auditing è anche possibile rilevare eventuali Access Point non autorizzati che sono collegati alla rete aziendale: si provi ad immaginare ad esempio i possibili problemi di sicurezza legati ad un Access Point che un utente abbia collegato alla rete interna per sua "praticità".

Esistono software di auditing per le Wireless LAN, che richiedono l'uso di un PC portatile o di un palmare dotato di scheda compatibile con lo standard IEEE 802.11. I più usati sono Kismet e Airsnort per il sistema operativo Linux, Netstumbler per Windows e Ministumbler per PocketPC. Tutti i software sono in grado di effettuare le seguenti funzionalità:

- Esaminare i pacchetti di sincronizzazione (beacon packets) per trovare tutti i punti di accesso.
- Determinare l'SSID e il nome degli AP.
- Esaminare i pacchetti sonda (probe packets) e le risposte a questi.
- Esaminare i pacchetti dei dati.
- Determinare la presenza di meccanismi di cifratura.
- Esaminare i pacchetti di autenticazione ed il relativo metodo.
- Esaminare il numero di client nella rete.
- Determinare la versione di firmware presente sui singoli punti di accesso.
- Determinare la quantità dei dati trasmessi per eventuali attacchi al WEP

Kismet, inoltre, è in grado di intercettare i sistemi Cisco attraverso Cisco Discovery Protocol (CDP) e di trovare altri sniffer attivi sulla rete wireless. Questi programmi, in congiunzione con strumenti di sniffing e di WEP cracking, sono gli stessi adottati dai "wardrivers" o "warwalkers", ovvero coloro che sono alla ricerca di reti wireless.

L'hardware necessario

Per effettuare l'auditing della propria Wireless LAN é necessario disporre di un computer portatile o di un palmare, una scheda di rete Wireless compatibile IEEE 802.11a/b/g e di una eventuale antenna esterna. L'uso di un'antenna esterna é particolarmente raccomandato per effettuare rilevazioni quali l'individuazione della copertura di un HotSpot pubblico o capire se si é soggetti ad un attacco di tipo *parking lot*. In generale, si consiglia l'uso di un palmare con una PCMCIA wireless con antenna integrata per la sua praticità di utilizzo. Particolarmente adeguate ad un ambiente operativo Linux sono le schede wireless basate sul chipset *prism2* (es: alcune schede Dlink o Linksys) e le Cisco Aironet serie 350; queste ultime, inoltre, permettono una scansione contemporanea su tutte le frequenze, mentre le prime effettuano la scansione su ogni canale singolarmente. In ambito Windows, invece, si prediligono le card basate sul chipset *hermes* (es: Orinoco o Enterasys), ma é anche possibile effettuare scansioni attraverso le schede Cisco Aironet.

NetStumbler per Windows

Uno dei più diffusi software per l'auditing delle reti Wireless in ambiente Windows é *Network Stumbler* (chiamato anche NetStumbler) di Marius Milner, disponibile gratuitamente sul sito http://www.netstumbler.org. Alla release 0.3.30 il software non é in grado di supportare tutte le schede IEEE 802.11b/g, principalmente é in grado di operare con le schede basate sul chipset *hermes*, come ad esempio le schede Orinoco o le mini-PCI e PCMCIA della Toshiba: per maggiori informazioni sulle tipologie di schede supportate si faccia riferimento al file *readme.html* incluso con il pacchetto software. É possibile utilizzare le schede wireless Cisco Aironet con NetStumbler limitatamente al sistema operativo Windows XP.

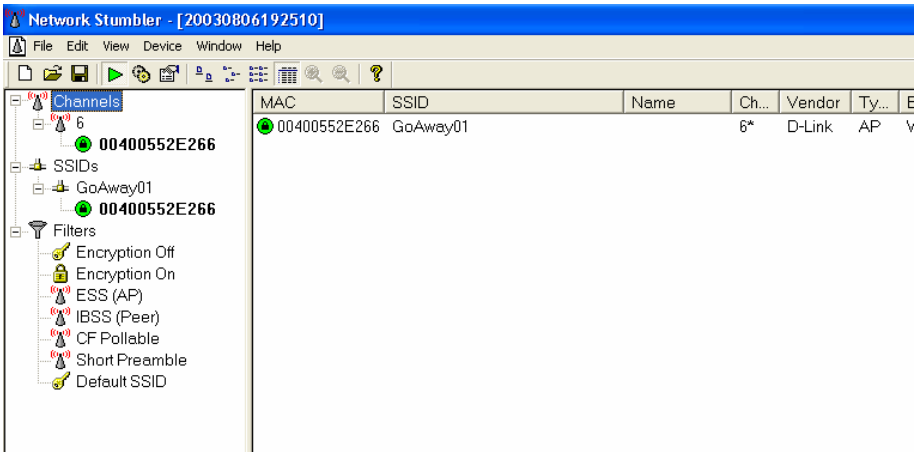

Fig. 2.2 – Console di NetStumbler

Il software viene distribuito come un file eseguibile e la sua installazione é simile a quella di altri software. É molto semplice effettuare auditing con NetStumbler: una volta rilevata automaticamente una scheda wireless disponibile, bisogna assicurarsi che il tasto *Scanning* della toolbar sia attivo (rappresentato da una freccia verde). Le reti wireless disponibili appariranno nel riquadro di destra, con le informazioni relative al SSID della rete wireless, il MAC address dell'Access Point, se si tratta di una rete crittografata, informazioni sul segnale e molto altro.

Kismet per Linux/FreeBSD

Esistono differenti tools per la rilevazione delle reti wireless e per l'analisi della crittografia, quali ad esempio *AirSnort* e *WepCrack*. Kismet é un software OpenSource che ha funzionalità simili a quelli di NetStumbler per Windows ed é in grado di collezionare ulteriori dati quali, ad esempio, le informazioni relative al Cisco Discovery Protocol (CDP), ed é inoltre capace di individuare programmi di scansioni quali NetStubler attivi sulla rete Wireless. Il software funziona principalmente con le schede wireless basate sul chipset *prism2*, sulle schede Cisco Aironet e Orinoco. Alcune distribuzioni recenti, ad esempio Debian, includono il pacchetto relativo a Kismet, ma é comunque disponibile il sorgente sul sito internet http://www.kismetwireless.net.

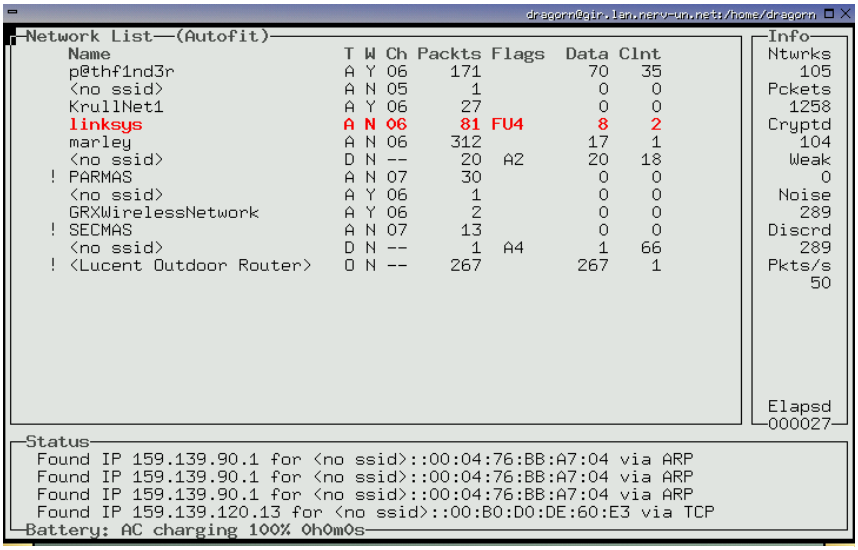

Fig. 2.2 – Console di Kismet

Prima di eseguire Kismet, é necessario modificare il suo file di configurazione *kismet.conf* (di default si trova in */usr/local/*etc) per indicare la scheda su cui eseguire le scansioni. In particolare é necessario modificare la riga contenente il parametro *source*. Ad esempio, per una scheda Cisco é necessario specificare:

```
source=cisco,eth0,Cisco
```

Per maggiori informazioni sui parametri e le schede, fare riferimento alle man pages *kismet.conf(5)* o alla documentazione allegata. Eseguire Kismet é molto semplice e immediato: la prima azione da effettuare é mettere la scheda wireless in modalità promiscua, eseguendo lo script *kismet_monitor*. Questo script non é valido per le schede Cisco Aironet, dove é necessario eseguire i seguenti comandi, ammettendo che la scheda sia la *eth0*:

```
iwconfig eth0 essid off
echo "Mode: r" > /proc/driver/aironet/eth0/Config
echo "Mode: y" > /proc/driver/aironet/eth0/Config
echo "XmitPower: 1" > /proc/driver/aironet/eth0/Config
ifconfig eth0 up
```

In seguito, é necessario avviare il server da root con il comando *kismet_server* e, da un'altra finestra, lanciare la User Interface (UI) con *kismet*. Le informazioni relative alle Wirleless LAN trovate verranno visualizzate nella UI, ad esempio l'SSID, gli IP trovati nella LAN, se si tratta di una rete crittografata, la qualità del segnale ed altro ancora.

3. PROXY

Durante i primi anni di diffusione di Internet come si conosce oggi, é nata la necessità di interconnettere le reti aziendali private, dette internet (con la "i" minuscola, ovvero Interconnected Networks) con la "big Internet". La necessità non era quella di un firewall, perché allora gli attacchi da intrusi erano esigui e non si percepiva il potenziale problema di sicurezza, ma quella di interconnettere la rete pubblica di accesso con quella privata. Oggi questo problema si sarebbe risolto attraverso il Network Address Translation (NAT), ma la tecnologia non era ancora disponibile: nascono così i proxy, ovvero software in grado di fare da "ponte" tra una rete e l'altra.

Esistono due tipologie di proxy, i *circuit-level* e gli *application-level*. I primi agiscono a livello UDP/TCP, creando un "circuito" tra il client e il server, senza però interpretare il protocollo applicativo: il più significativo esempio in questo campo é il protocollo *socks*. I secondi agiscono a livello applicativo, interpretando i dati e i comandi di una specifica applicazione, ad esempio HTTP o FTP. Il *socks* é documentato nell'RFC 1928 ed é disponibile attraverso diverse implementazioni, alcune di queste sono disponibili gratuitamente come *Dante* e il socks della *NEC*. Il grosso pregio del protocollo *socks* é che permette di fare da proxy per qualsiasi applicazione TCP o UDP, in quanto non interpreta il contenuto applicativo, e permette l'autenticazione degli utenti, ma il difetto é che bisogna aggiungere un ulteriore software nel client. Inoltre, non interpretando il contenuto degli applicativi, é impossibile avere delle policy su quali contenuti l'utente é abilitato, ad esempio non si può vietare l'utente alla navigazione sul di un sito di notizie, abilitando la webmail. Gli *application-level* proxy sono invece in grado di interpretare il contenuto del traffico, limitando o abilitando determinate URL, ed includono la possibilità di autenticare l'utente. Sono questi tipi di applicativi che vengono chiamati generalmente *proxy* e in particolare ci si riferisce ai proxy HTTP.

L’uso del Proxy in ambito wireless

L’adozione delle regole di base descritte nel capitolo precedente rendono più difficile l’intercettazione di una rete Wireless e più difficile l’accesso da parte di un intruso. Tuttavia esiste la possibilità che un intruso motivato possa accedere alla rete, grazie soprattuto ai problemi di WEP precedentemente esposti. La metodologia migliore pertanto é quella di dividere la rete wireless dalla rete interna, ad esempio attraverso l’adozione di un proxy che effetti l’autenticazione degli utenti. Nella figura successiva si illustra un esempio di struttura wireless con un proxy per la protezione della rete interna.

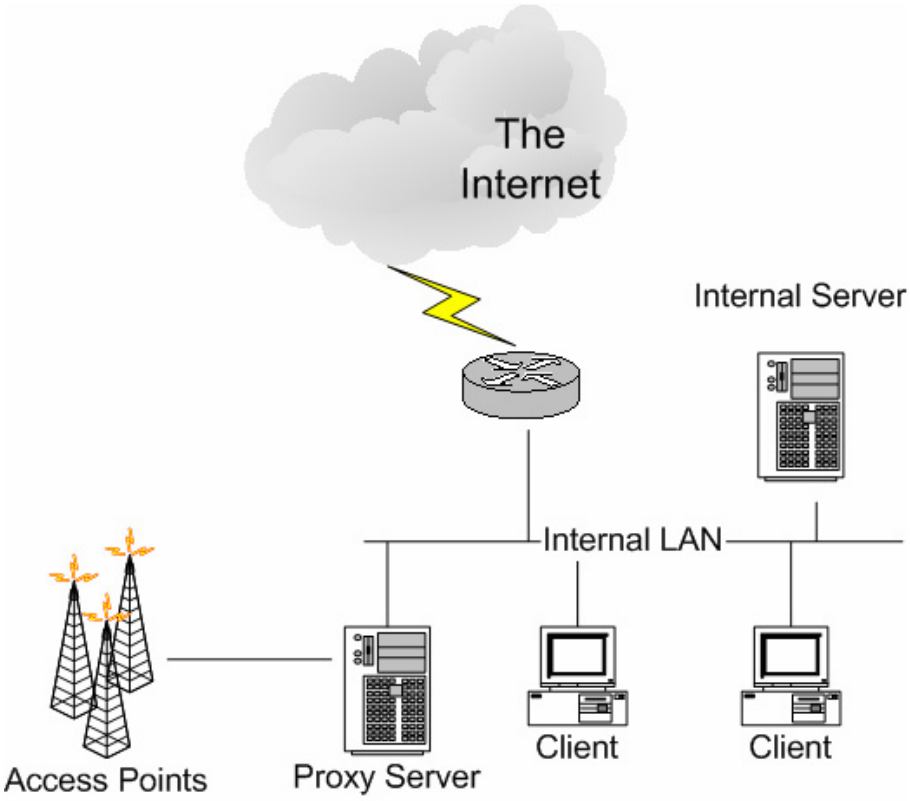

Fig. 3.1 - Esempio di architettura Proxy

La limitazione principale dell’adozione di un proxy é che tutti i protocolli non supportati dal proxy (ad esempio POP3 o IMAP) non possono essere utilizzati nell’ambito wireless. Pertanto, l’ambito di utilizzo di una simile architettura é ristretto a piccoli ambienti dove le applicazioni usate in ambito wireless sono principalmente di tipo Web-based. Qualora il proxy lo permette, é consigliabile attivare la funzionalità di *SSL accelerator*: con questo espediente, le richieste HTTP verranno incapsulate in SSL (HTTPS) e pertanto più difficili da intercettare in ambito wireless.

Squid

Il proxy server più popolare in internet é *Squid*. Si tratta di un proxy OpenSource ad alte prestazioni che supporta FTP, gopher, HTTP e HTTPS. Inoltre é dotato di un sistema di Access Control Lists (ACL) che permette di autenticare utenti e abilitare e/o disabilitare determinate URLs. Squid é stato concepito principalmente per ambienti Unix ed é disponibile sul sito Internet http://www.squid-cache.org/, ma esiste un ottimo porting anche su ambiente Windows NT/2000/XP/.NET grazie a Guido Serassio (http://www.serassio.it/). In questo paragrafo si intende fornire un esempio di configurazione effettuata con sistema operativo Linux e Windows, che sono tra i più diffusi. Qualsiasi sia il sistema operativo scelto su cui eseguire Squid, si consiglia di eliminare i servizi non usati, quali ad esempio FTP e TELNET su macchine Unix o la condivizione file e stampanti sotto windows: tale processo é detto di *hardening*. In questi esempi, si assume che l'utente abbia familiarità con gli ambienti operativi e che il server proxy disponga di due interfaccie di rete, una da collegare alla rete interna, l'altra verso la rete wireless.

Esempio con Linux

Il programma *Squid* é incluso in molte distribuzioni di Linux, é comunque possibile scaricare i sorgenti dal sito Internet menzionato precedentemente per quelle distribuzioni che non ne disponessero. Nel caso la distribuzione non comprendesse Squid, é sempre possibile scaricare i sorgenti dal sito ufficiale http://www.squid-cache.org/ e procedere alla sua compilazione e installazione, ad esempio con i seguenti comandi:

```
./configure    --prefix=/usr/local/squid  --enable-linux-netfilter  --
enable-ssl \
--enable-digest-auth-helpers=password \
--enable-external-acl-helpers=unix_group

make
make install
```

Il file di configurazione di squid é */etc/squid.conf* se si tratta di un pacchetto di distribuzione o solitamente */usr/local/etc/squid.conf* qualora fosse stato installato dai sorgenti con i parametri di default. Una semplice configurazione può prevedere che tutti gli utenti autenticati possano navigare liberamente, si veda il relativo *squid.conf*

```
## Porta di ascolto del proxy
http_port 8080

## Esegui Squid con le permission dell'utente "proxy"
cache_effective_user proxy
cache_effective_group proxy

## Non effettuare le cache dei CGI
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY

## Stabilisci una cache in RAM di 64 MB e su disco di 200 MB
## (primo parametro dopo la directory contenente la cache)
cache_mem 64 MB
cache_dir ufs /usr/local/squid/var/cache 200 16 256

## Tipo di autenticazione basic
auth_param    basic    program    /usr/local/squid/libexec/ncsa_auth
/usr/local/squid/etc/passwd
auth_param basic children 5
auth_param basic realm Proxy Authentication Required
auth_param basic credentialsttl 2 hours

## Refresh patterns
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320

## Inizio ACL di default, con autenticazione proxy richiesta
acl password proxy_auth REQUIRED
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow password
http_access deny all
http_reply_access allow all
icp_access allow all

## Nome visualizzato all'utente e directory di core dumps
visible_hostname proxy.azienda.it
coredump_dir /usr/local/squid/var/cache
```

Il file di configurazione é commentato per una più facile comprensione del suo contenuto. É preferibile eseguire Squid come utente non root, attraverso il parametro di configurazione *cache_effective_user* e *cache_effective_group*: nell'esempio citato Squid viene eseguito come utente *proxy*, pertanto sarà necessario creare tale utenza e gruppo nel proprio sistema prima di procedere. É altrettanto importante che l'utenza *proxy* sia effettivamente il proprietario delle directories che conterranno la cache e i files di log, di default rispettivamente */usr/local/squid/var/cache* e */usr/local/squid/var/log*. Per autenticare gli utenti in ambito unix si é scelto di usare un file di password esterno, in particolare si tratta del file */usr/local/squid/etc/passwd* che può essere creato e mantenuto attraverso l'utility *htpasswd* presente in apache (http://httpd.apache.org). Prima di eseguire Squid come proxy, é necessario inizializzare la directory di cache, eseguendo il comando *squid –z*. A questo punto, é possibile eseguire squid come daemon: lo script *RunCache* presente in */usr/local/squid/bin* permette di eseguire squid in modo corretto.

È anche consigliabile attivare il firewall di Linux, *iptables,* per proteggersi da eventuali tentativi di intrusione alla macchina proxy. Ammettendo che la rete interna sia collegata alla interfaccia *eth0* e la rete wireless a *eth1*, si proceda a proteggere la macchina con i seguenti comandi, che permetteranno di ricevere connessioni solo ed esclusivamente sulla porta del proxy (porta 8080/tcp):

```
iptables –P INPUT DROP
iptables –P FORWARD DROP
iptables –P OUTPUT ACCEPT
iptables –A INPUT –m state ––state ESTABLISHED,RELATED –j ACCEPT
iptables –A INPUT –i eth1 –p tcp –m tcp ––dport 8080 –j ACCEPT
```

Esistono differenti metodi per configurare Squid: quello illustrato in questo capitolo vuole fornire al lettore una idea che possa fungere da spunto per ulteriori approfondimenti. Per un ulteriore lettura, si consiglia l'ottima FAQ in italiano presente sul sito http://merlino.merlinobbs.net/Squid-Book/.

Esempio con Windows

Grazie a Guido Serassio, é disponibile un porting di Squid in ambiente Windows, che é possibile scaricare dal suo sito Internet http://www.serassio.it. Il file si presenta in formato ZIP e contiene al suo interno l'intera distribuzione che va decompressa, ad esempio nel drive *C:*. Da un punto di vista della configurazione, é molto simile a quella per Linux, con il vantaggio di potersi appoggiare alla gestione degli utenti di Windows, risultando in una più semplice amministrazione. Si veda un esempio di configurazione:

```
## Porta di ascolto del proxy
http_port 8080

## Non effettuare le cache dei CGI
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY

## Stabilisci una cache in RAM di 64 MB e su disco di 200 MB
## (primo parametro dopo la directory contenente la cache)
cache_mem 64 MB
cache_dir ufs C:/squid/var/cache 200 16 256

## Tipo di autenticazione basic
auth_param basic program c:/squid/libexec/nt_auth.exe
auth_param basic children 5
auth_param basic realm Proxy Authentication Required
auth_param basic credentialsttl 2 hours

## Refresh patterns
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern .               0       20%     4320

## Inizio ACL di default, con autenticazione proxy richiesta
acl password proxy_auth REQUIRED
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow password
http_access deny all
http_reply_access allow all
icp_access allow all

## Nome visualizzato all'utente e directory di core dumps
visible_hostname proxy.azienda.it
coredump_dir c:/squid/var/cache
```

La prima differenza fondamentale é relativa alla nomenclatura di files e directories, che sono simili a quelli di Windows ma con i forward-slashes ("*/*") al posto dei back-slashes ("\"). La seconda é il metodo di autenticazione, che si basa sulla gestione delle utenze di Windows, grazie al programma *nt_auth.exe.* Anche per la versione Windows di Squid, é necessario inizializzare la directory di cache eseguendo *c:\squid\sbin\squid –z*. Nella versione Windows, é possibile installare squid come servizio di Windows, invocando il comando *c:\squid\sbin\squid –i.* In questo modo, Squid viene eseguito come un servizio standard di Windows, pertanto basterà:

- Selezionare *Control Panel*
- Selezionare successivamente *Administrative Tools* e *Services*
- Selezionare SquidNT e, con il tasto destro del mouse, selezionare *Start*

Qualora si decidesse di implementare la soluzione di Squid installato su un sistema operativo Windows, é altamente consigliabile provvedere all'installazione di un personal firewalls, oppure di effettuare la rimozione dei servizi non necessari (hardening).

Microsoft ISA Server

Internet Security and Acceleration (ISA) Server di Microsoft non é solamente un proxy server, ma svolge anche funzioni di Firewall. Esso può essere configurato come soluzione integrata di firewall, proxy e IDS, oppure può essere solamente installato con funzioni di proxy. Una nota peculiare di ISA stà nel fatto che é capace di effettuare content inspection, di filtrare cioé il contenuto del traffico HTTP e negando quindi l'accesso a risorse protette. Inoltre, ISA server é in grado di svolgere la funzionalità di socks server, permettendo cioé anche l'uso di altre applicazioni TCP/IP. Come ogni prodotto Microsoft, é in grado di integrarsi perfettamente nel contesto dell'Active Directory, per poter implementare e distribuire le policy di accesso e integrarsi con la base utenti aziendali. Questa funzionalità, unita alla sua facilità di utilizzo e alla popolarità di Microsoft, hanno diffuso ISA Server soprattutto nella piccola e media impresa.

L'autore consiglia l'uso di Microsoft ISA Server in aggiunta ad altri accorgimenti per salvaguardare la rete aziendale da Internet, ad esempio configurando opportunamente le Access Control Lists sul router di accesso. In ambiente Wireless, una protezione equivalente alle ACL può essere rappresentata dall'uso di WEP e da quanto indicato nel capitolo precedente. ISA server é pertanto un ottimo sistema di protezione delle reti Wireless per chi ha già familiarita con questo strumento, oppure intende avvalersi degli ambienti Microsoft.

Per installare Microsoft ISA Server, é necessario avere un sistema operativo Windows 2000 Server Service Pack 1 o superore, oppure Windows 2003 Server (con esclusione della web server edition). Si assume che la macchina abbia almeno due interfaccie di rete, una per la rete interna e una per la rete wireless, che sia già installato il sistema operativo e che l'amministratore abbia familiarità con Windows Server.

Installazione

L'installazione di ISA Server é simile a quella di altri prodotti Microsoft. Durante l'installazione, il programma chiederà se questo server deve essere parte di un *array member*, premere *No* se non si dispone di altri ISA server. Successivamente verrà proposto come installare ISA Server tra *Firewall mode*, *Cache mode* e *Integrated mode*: sceglire *Integrated mode*, in quanto permette la funzione combinata delle prime due.

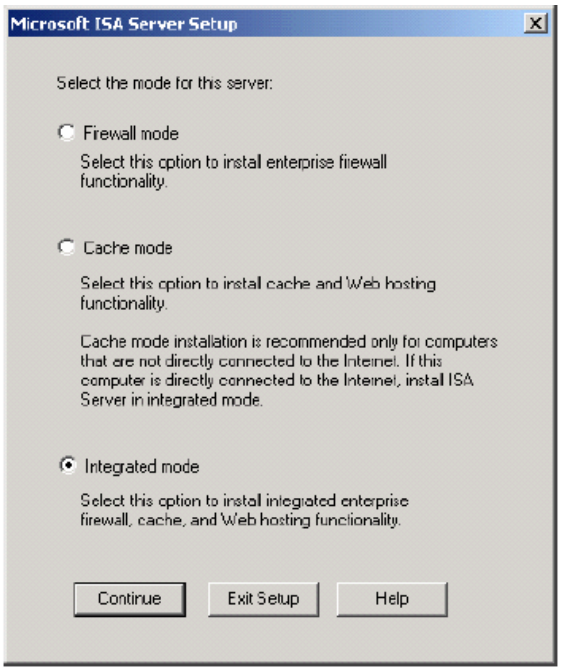

Fig. 3.2 – Selezione della modalità del server

L'ultima scelta durante l'installazione é relativa alla *Local Address Table* (LAT), ovvero l'intervallo di IP address considerati "interni": nel nostro caso, considereremo "interni" la LAN Wireless e successivamente modificheremo le opzioni per abilitare solo il traffico autenticato.

Utenti e Sicurezza di Windows Server

Prima di configurare ISA server é consigliabile creare gli utenti che saranno abilitati all'accesso, nel caso si trattase di un server standalone, e un gruppo per gli utenti Wireless. Una volta avvenuto l'accesso al sistema da utente "Administrator":

- Selezionare *Start*, *Programs, Administrative Tools* e *Computer Management*
- Selezionare *Local Users and Groups*
- Selezionare *Users*, e con il tasto destro del mouse, *New User*. Aggiungere pertanto gli utenti come consuetudine. Ripetere per ogni utente che debba avere accesso alla rete Wireless.
- Da *local Users and Groups*, selezionare *Groups* e, con il tasto destroy del mouse, *New Group*.
- Come *Group name* indicare *Wireless Users*, indicare una descrizione e aggiungere con il pulsante *Add* gli utenti definiti.

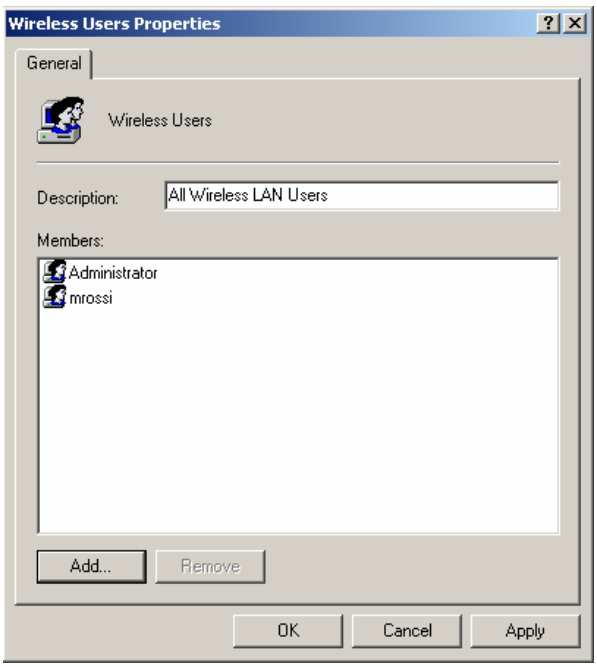

Fig. 3.2 – Creazione del gruppo di utenti Wireless

Nel caso si trattasse di un server collegato ad un dominio Active Directory, non é necessario provvedere alla creazione di utenti, in quanto valgono quelli già definiti, ma é comunque consigliabile creare un gruppo "*Wireless Users*" per una maggiore facilità di configurazione di ISA.

Grazie ad un tool di ISA Server, é possibile effettuare l'hardening del server ISA, ovvero la rimozione dei servizi non necessari, pertanto rendere più sicuro il computer che sarà destinato all'incarico di proxy. Questa opzione è disponibile aprendo *Programs, Microsoft ISA Server* e selezionando il *ISA Management.* Una

volta aperto questo programma, che è il centro di controllo del server, selezionare *Access Policy*, *IP Packet Filter* e successivamente l'icona *Secure your ISA Server Computer* dalla finestra principale. Il sistema proporrà tre opzioni di configurazione:

- **Dedicated.** Questa opzione è consigliata se la macchina su cui è installato ISA Server è dedicata alla sola funzionalità di firewall
- **Limited Services.** Questa opzione è valida per le macchine che fungono da Domain Controller o fanno parte dell'infrastruttura
- **Secure.** È una opzione per quei firewalls che sono anche database server o application server

Fig. 3.3 – Hardening di ISA Server

Per una migliore protezione, si consiglia che ISA Server sia installato su una macchina dedicata e che non funga ad altri servizi. A questo scopo, la prima opzione (*Dedicated*) è quella più opportuna.

Configurazione di ISA

Per procedere ad abilitare i client Wireless è necessario configurare Microsoft ISA Server dal suo tool di amministrazione, ovvero *ISA Management.* La prima azione da effettuare è quella di controllare la *Local Address Table* (LAT) configurata durante l'installazione di ISA Server. La LAT indica quali IP address sono da considerare "interni", e quindi affidabili: durante la configurazione verrà

modificato il comportamento di default, in modo da richiedere l'autenticazione dei clients. Per verificare la LAT, da ISA Management è necessario selezionare *Network Configuration* e successivamente *Local Address Table (LAT)* dal pannello alla sinistra. Nel pannello principale, verificare che vi sia un rigo con l'intervallo degli IP addresses assegnati ai client: per modificarli, selezionare il rigo e con il tasto destro del mouse selezionare *Properties*.

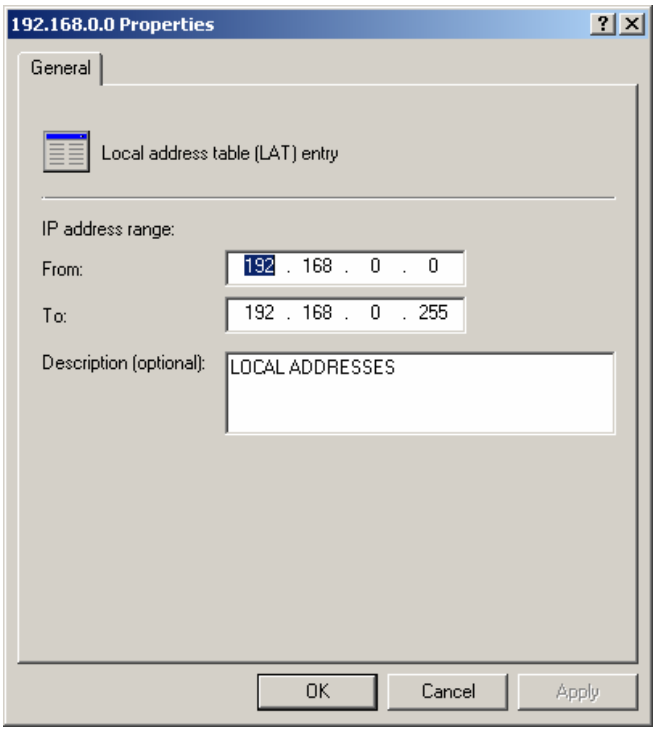

Fig. 3.4 –Definizione della LAT

Successivamente è necessario modificare le *Access Policy* per abilitare l'accesso Wireless. In ISA Server esistono due tipi di policy, il *Site and Content Rules* e i *Protocol Rules*. I primi riguardano principalmente HTTP e servono per la funzione di proxy cache vera e propria, in una maniera simile a quella di Squid, permettendo a client non-windows la "navigazione" HTTP. I Protocol Rules agiscono a livello circuit-level e abilitano la possibilità ad accedere ad altre applicazioni, quali ad esempio POP3 e IMAP, ma é una funzionalità disponibile ai soli client windows tramite un software da installare. È da sottolineare che le due policy sono totalmente indipendenti l'uno dall'altra, inoltre anche attraverso le Protocol Rules é possibile navigare in Internet (abilitare cioé HTTP), ma si perdono le funzionalità di cache e le funzioni di "inspection" all'interno di HTTP e la possibilità di navigazione per altri clients (es: Linux e Apple).

Site and Content Rules

Per configurare le *Site and Content Rules*, posizionarsi nell'apposita voce che si trova sotto la categoria *Access Policy*. Esiste una regola di default, chiamata *Allow Rule*, che bisogna disabilitare per funzionare in ambito Wireless. Selezionare questa regola e successivamente l'icona *Configure a Site and Content Rule*. Verrà proposta una finestra di dialogo, in basso disabilitare la checkbox contrassegnata

con *Enable*.

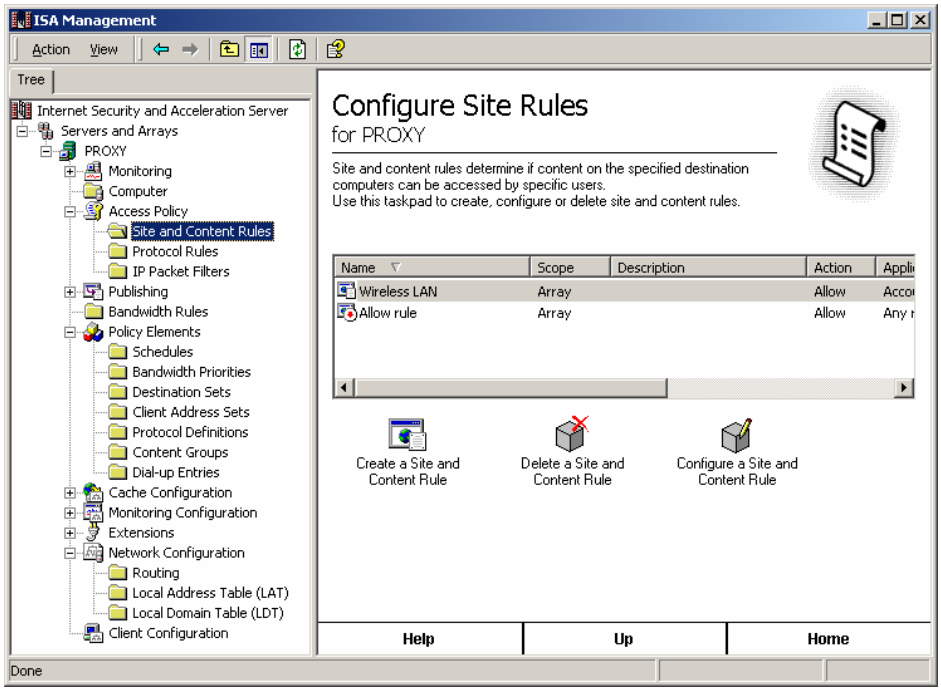

Fig. 3.5 – Console di configurazione Site and Content Rules

Successivamente selezionare l'icona *Create a Site and content Rule* per iniziare il wizard di configurazione. La prima schermata chiede il nome della regola, che verrà chiamata "Wireless LAN".

Fig. 3.6 – Site and Content Rule Wizard, nome della regola

Successivamente è necessario specificare il tipo di azione, ovvero se si tratta di una regola permissiva (*Allow)* o di diniego (*Deny)*, indicare *Allow* e premere *Next*.

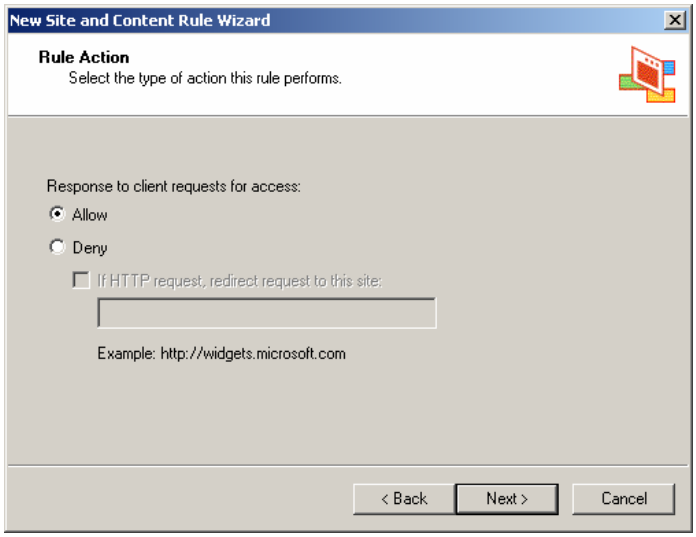

Fig. 3.7 – Site and Content Rule Wizard, azione

Il passo successivo indica il *Destionation Sets*, ovvero quale sia la destinazione della comunicazione. È necessario indicare tutte le destinazioni, quindi selezionare *All destinations* e il pulsante *Next.*

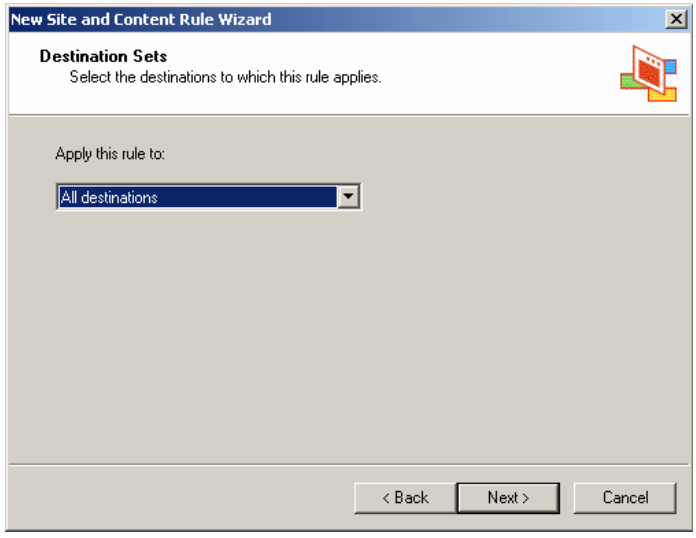

Fig. 3.8 – Site and Content Rule Wizard, destinazione

Nella sezione *Schedule*, ISA Server richiede all'amminstratore quando questa regola debba essere attivata. Potrebbe essere interessante abilitare l'accesso http soltanto negli orari di lavoro, in modo da evitare attacchi notturni, ma per facilitare la configurazione è preferibile che questa regola sia sempre attiva, quindi selezionare *Always* e premere *Next*.

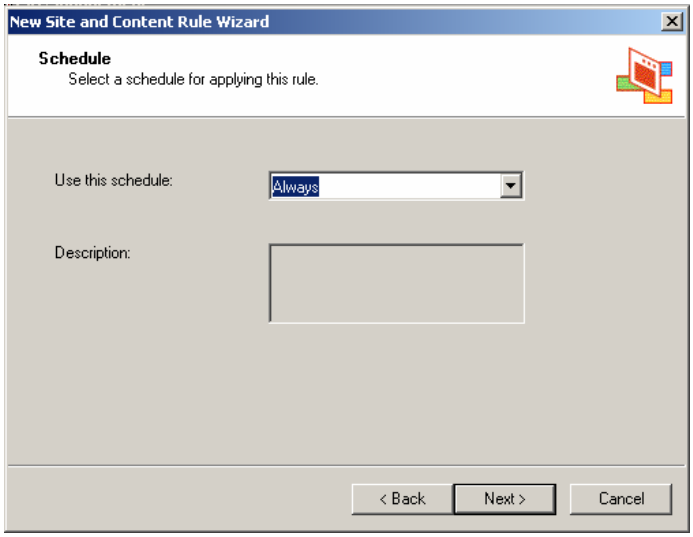

Fig. 3.9 – Site and Content Rule Wizard, tempo di attivazione

Successivamente viene proposto all'amministratore quali utenti o computer siano abilitati all'accesso. *Any request* indica tutti i client, *Specific computers* limita l'accesso a computer specifici, mentre *Specific users and groups* limita l'accesso a determinati utenti. Si consiglia quest'ultima opzione, in quanto è possibile tenere traccia degli accessi utente. Premere quindi *Next*.

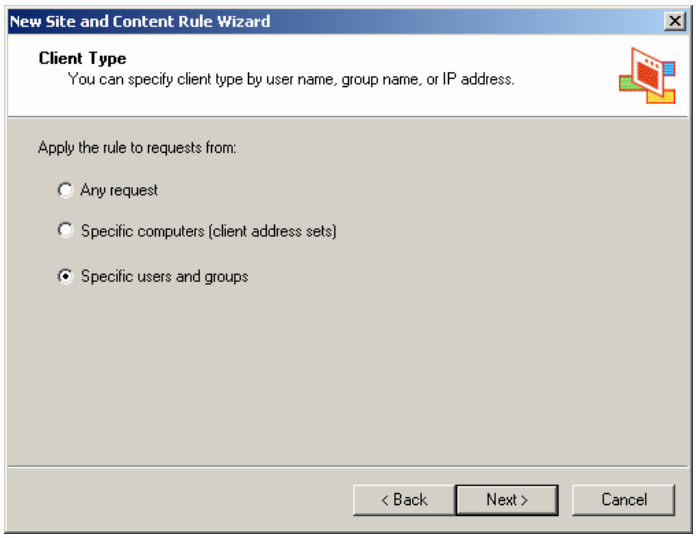

Fig. 3.10 - Site and Content Rule Wizard, tipo di client

Nella schermata successiva verrà richiesto quali utenti sono abilitati all'accesso via HTTP. Premere il pulsante *Add* e, dalla finestra di dialogo degli utenti e gruppi disponibili, selezionare il gruppo *Wireless Users* precedentemente creato sul sistema.

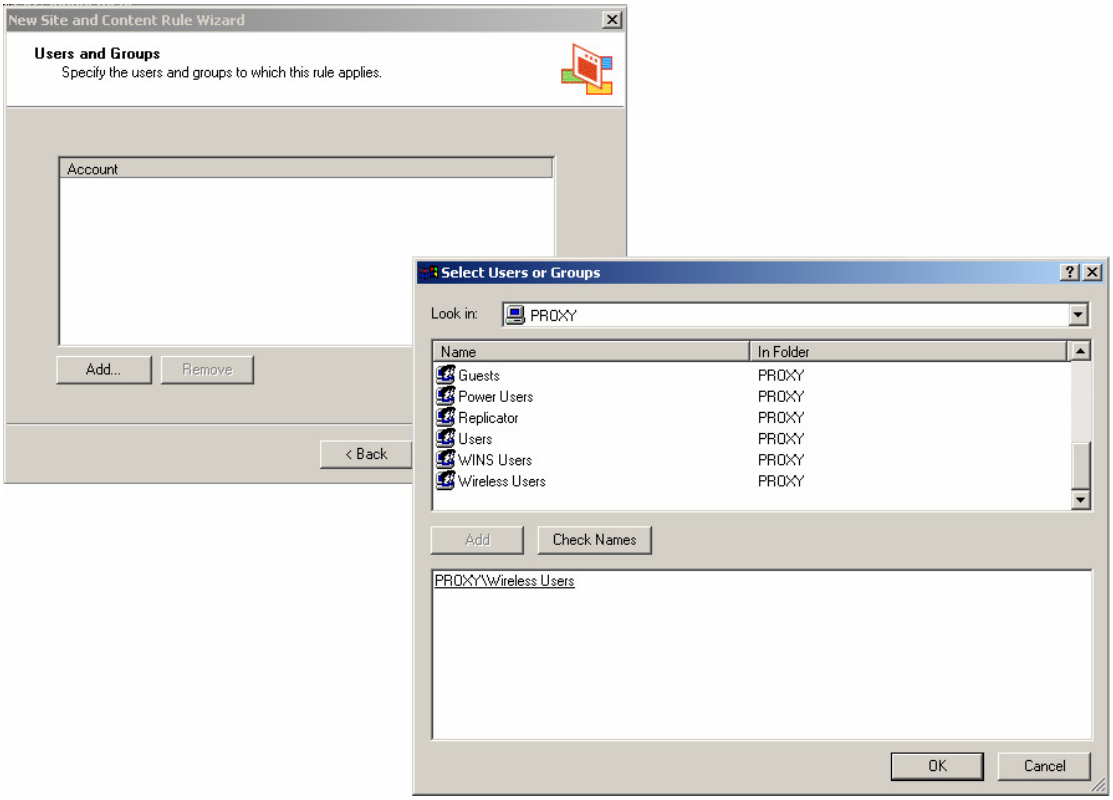

Fig. 3.31 - Site and Content Rule Wizard, aggiunta utenti

Non appena premuto *Ok* e successivamente il tasto *Next* verrà visualizzata una schermata riassuntiva. Premere *Finish* per applicare i cambiamenti.

Fig. 3.12 - Fine del Site and Content Rule Wizard

Protocol Rules

Come accennato precedentemente, i *Protocol Rules* sono indipendenti dai Site and Content Rules e non sussiste obbligo di configurare entrambe le regole, inoltre agiscono a livello circuit-level, permettendo l'utilizzo di altri protocolli (ad esempio Telnet e POP3). Il principale svantaggio di questa opzione è che il programma client è disponibile solo per ambienti Windows, ma è sicuramente una opzione interessante qualora tutti i client fossero della famiglia Windows. Per configurare questa opzione, dal tool *ISA Management* selezionare *Access Policy* e successivamente *Protocol Rules* come da figura sottostante.

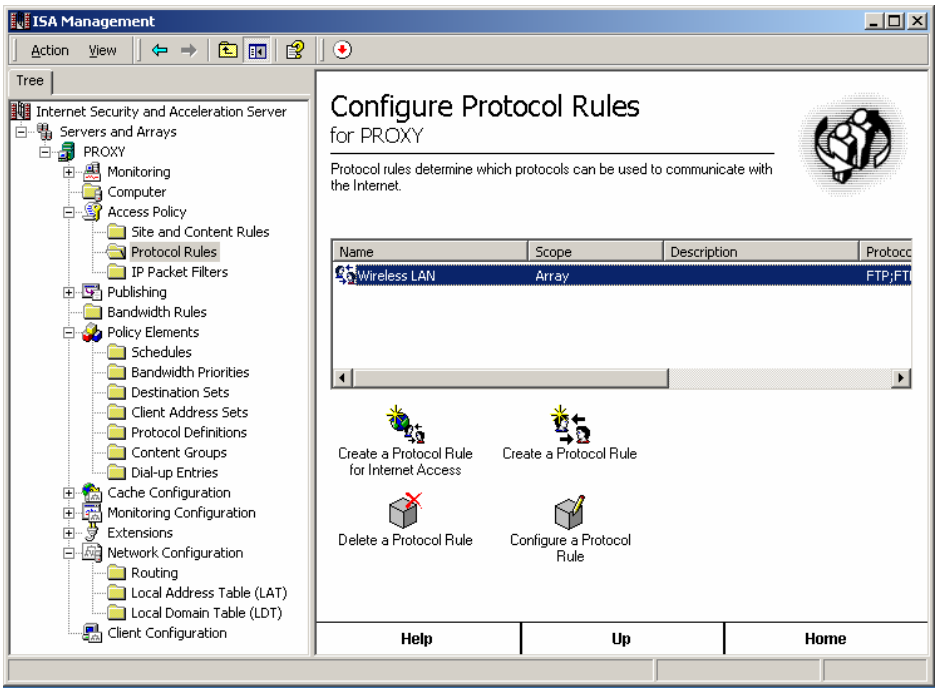

Fig. 3.13 - Console di configurazione Protocol Rule

Qualsiasi regola esistente va cancellata attraverso l'icona *Delete a Protocol Rule* e successivamente creandone una nuova con *Create a Protocol Rule*. Questo comando farà avviare un wizard che permette la configurazione di nuove Protocol Policies. Alla prima schermata indicare il nome della policy, ad esempio *Wireless LAN* e premere il pulsante *Next.*

Fig. 3.14 - Protocol Rule Wizard, nome della regola

La schermata successiva, *Protocols,* permette di selezionare i protocolli che vengono permessi. Per una ricerca migliore dei protocolli si consiglia di disattivare la checkbox *Show only selected protocols*, selezionare i protocolli prescelti (esempio Telnet, IMAP e FTP) e riselezionare la checkbox per effettuare una verifica finale dei protocolli selezionati. Non appena terminata la selezione dei protocolli, premere *Next*.

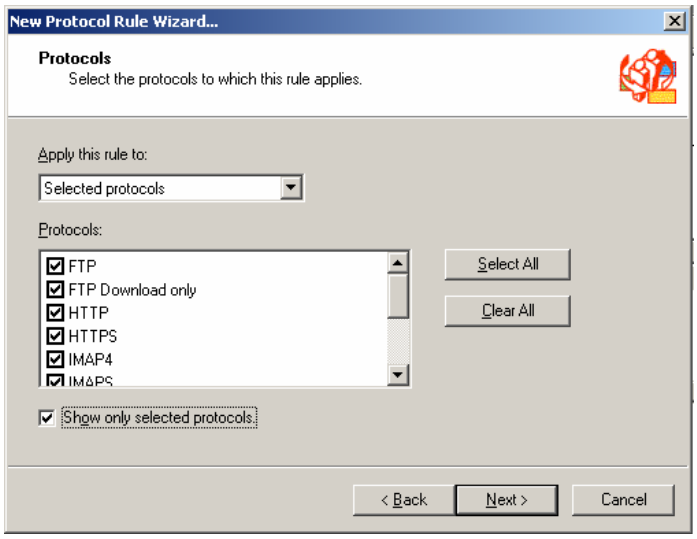

Fig. 3.15 - Protocol Rule Wizard, scelta dei protocolli

In maniera analoga alle Site and Content Rules, anche nei Protocol Rules è possibile indicare l'intervallo di tempo in cui si applicano queste regole. Qualora non si decidesse di limitare l'intervallo di tempo, lasciare il default *Always* e premere il pulsante *Next.*

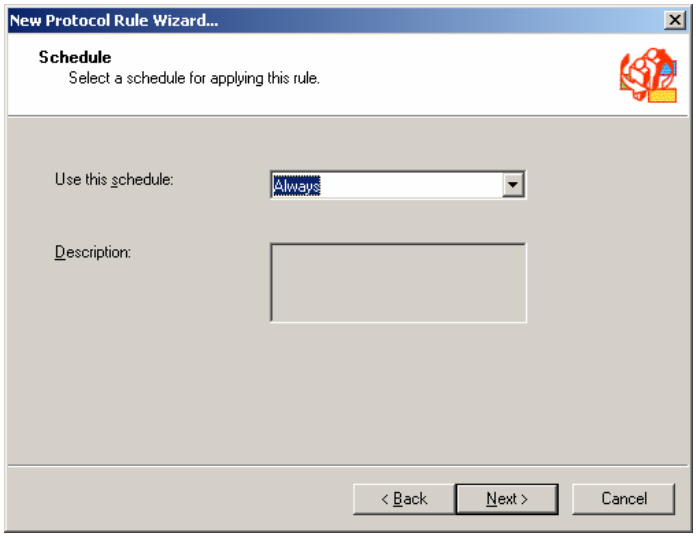

Fig. 3.16 - Protocol Rule Wizard, tempo di attivazione

Anche per Protocol Rules è possibile specificare quali utenti o computers siano abilitati all'accesso. In questo esempio, si è scelto di selezionare l'accesso in base agli utenti, quindi specificare *Specific users and groups* e premere *Next.*

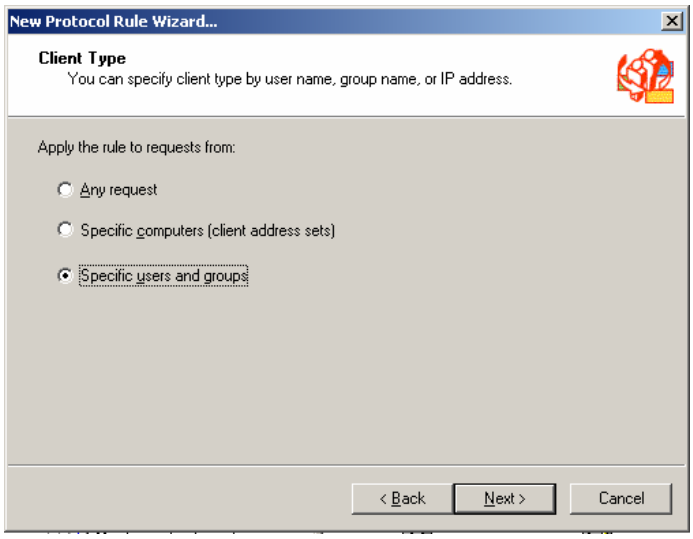

Fig. 3.17 - Protocol Rule Wizard, tipo di client

Analogamente a Site and Content Rules, è necessario selezionare quali utenti o gruppi di utenti concedere l'accesso alla rete locale. Agendo sul pulsante *Add* verrà presentata una finestra di dialogo con gli utenti e i gruppi presenti sul sistema, quindi selezionare il gruppo *Wireless Users* e premere *Ok*. Ritornati al Protocol Rule wizard, selezionare *Next*.

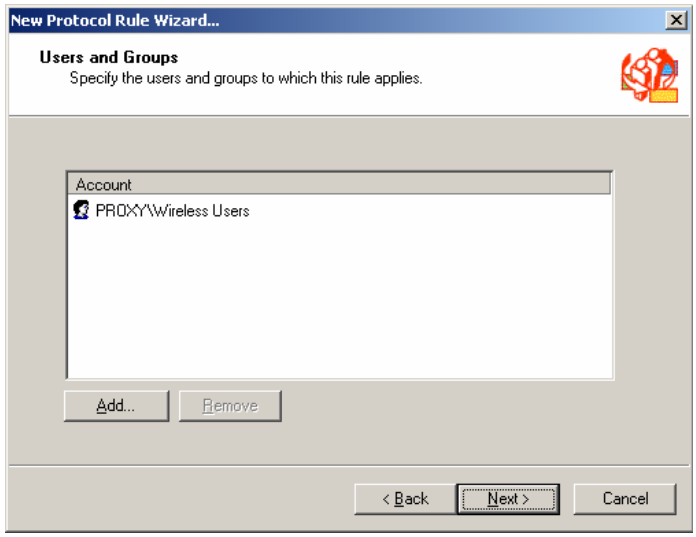

Fig. 3.18 - Protocol Rule Wizard, scelta degli utenti

La configurazione della regola di protocollo è terminata, premere quindi *Finish* per attivare i cambiamenti.

Fig. 3.19 - Fine del Protocol Rule Wizard

Configurazione del Firewall Client

Per sfruttare la Protocol Rule appena creata è necessario installare il programma *Firewall Client* di ISA Server. Prima di installare il client, è però necessario effettuare una configurazione su ISA Server. Dal tool *ISA Management*, selezionare la voce *Client Configuration*, nella finestra principale selezionare *Firewall Client* e, con il tasto destro del mouse, selezionare quindi *Properties*. È

probabile che sulla LAN connessa all'Access Point non vi sia un server DNS disponibile, pertanto è consigliabile specificare l'IP address anziché il DNS name e premere quindi *Ok*.

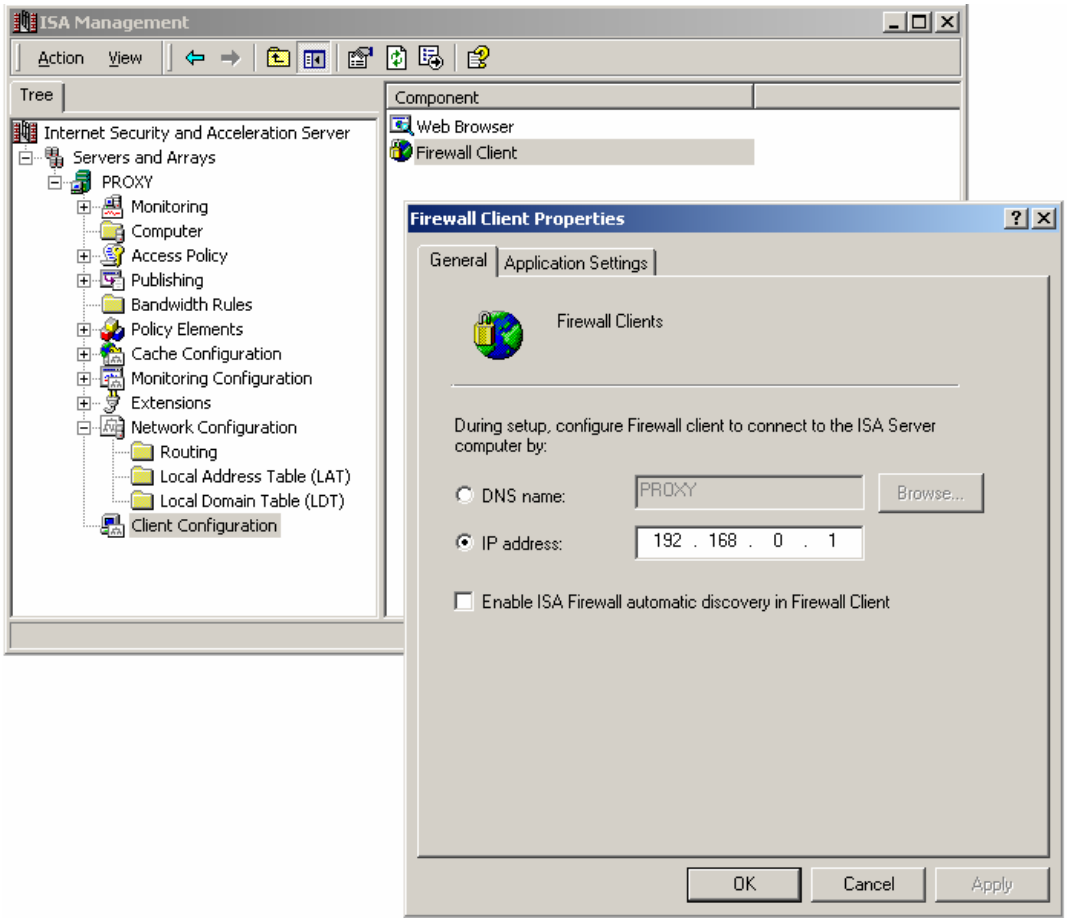

Fig. 3.20 - Configurazione del client da ISA Management

La seconda configurazione, opzionale, è quella relativa al *Web Browser*, che si trova al di sopra della voce *Firewall Client*: grazie a questa opzione, durante l'installazione del Firewall Client il browser del computer client verrà automaticamente configurato. Anche in questo caso, si consiglia di specificare l'IP address del server, anziché il DNS.

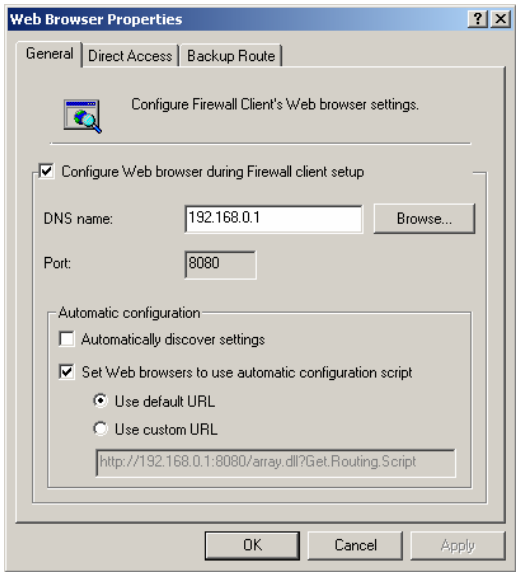

Fig. 3.41 – Specifica dell'IP address nel firewall client

Sebbene sul CD di ISA Server sia presente il Firewall Client da installare, questo si rifuterà di installarsi in quanto il client deve essere installato direttamente dal server ISA. Quando ISA Server si installa sul computer, crea una condivisione (*mspclnt*) che contiene una versione personalizzata del client, in base alle impostazioni sopra specificate. Ad esempio, se l'ISA Server avesse come IP address 192.168.0.1, da un client sarebbe sufficiente per iniziare l'installazione del client eseguire il comando:

\\192.168.0.1\mspclnt\setup.exe

L'installazione è simile a quella di altre applicazioni Windows, e nessun parametro di configurazione è richiesto, in quanto specificato direttamente dal server. Alla fine dell'installazione sarà necessario un riavvio della macchina per applicare i cambiamenti. Al riavvio, il client si presenterà come un'icona in basso a destra (a forma di mondo) e non è necessario configurare alcuna opzione.

Fig. 5.22- Particolare dell'icona del Firewall Client

È comunque sempre possibile visualizzare la configurazione del *Firewall Client,* selezionando l'icona con il tasto destro del mouse e successivamente l'opzione *Configure…* Il pannello di configurazione è anche richiamabile dal pannello di controllo di Windows.

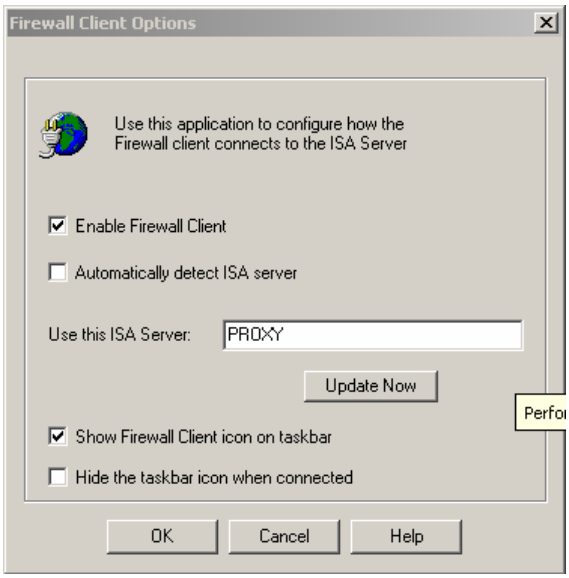

Fig. 3.23 - Opzioni del Firewall Client

4. PPPoE

Con l'introduzione delle tecnologie broadband come i cable modem, usati per far viaggiare Internet sulla TV via cavo e l'ADSL, gli Internet Service Providers hanno adottato una metodologia per risolvere il problema dell'autenticazione degli utenti nell'ambito broadband. Nella loro configurazione standard, L'ADSL e i cable modem sono in grado di emulare una rete ethernet: sebbene l'uso del DHCP avrebbe semplificato l'amministrazione lato ISP e la configurazione lato utente, non avrebbe permesso l'identificazione univoca dell'utente per l'erogazione dei servizi acquistati o per il pagamento in caso di "pay per use".

Questo problema è stato risolto con l'introduzione del protocollo Point-to-Point Protocol over Ethernet (PPPoE). In breve, questa tecnologia permette di incapsulare il protocollo PPP, usato nella sua accezione più comune sui collegamenti via modem, sul mezzo trasmissivo ethernet. In questo modo, traendo vantaggio della velocità del mezzo ethernet, è possibile riconoscere l'utente e fornire servizi adeguati, quali altri protocolli (ad esempio IPX e NetBIOS), e IP statici. Attraverso l'adozione di PPPoE è quindi possibile personalizzare i servizi erogati in base all'utente anziché in base all'ubicazione stessa dell'utente.

L'uso di PPPoE nell'ambito wireless

Analogamente alle tecnologie ADSL e cable modem, la wireless LAN è in grado di emulare una rete ethernet. Anche in ambito wireless è possibile sfruttare quindi la tecnologia PPPoE, con i benefici descritti precedentemente, ad esempio fornendo servizi personalizzati all'utente quali l'IP address fisso e access lists basate a livello utente.

PPPoE è paragonabile all'uso di IEEE 802.1x a livello autenticazione, ma offre alcuni vantaggi. Non tutti i produttori hanno scelto di implementare 802.1x nei loro Access Point, in special modo sugli AP a basso costo, pertanto tutti gli AP che non dispongono di funzionalità 802.1x devono essere sostituiti. Inoltre 802.1x

non copre la funzionalità di crittografia dati, mentre PPPoE offre un'architettura scalabile che vedremo in seguito. PPPoE, inoltre, non richiede l'uso di indirizzamenti a livello 3 (esempio IP) direttamente sulla ethernet, offuscando di fatto la topologia della rete interna, inoltre non richiede una infrastruttura PKI per l'autenticazione dell'utente. PPPoE, di contro ha un problema relativo alla lunghezza dei pacchetti trasmessi, chiamata Maximum Transmission Unit (MTU). In pratica la lunghezza dei pacchetti non può superare i 1492 bytes, causando problemi di performance su una grossa mole di dati trasmessi.

L'uso di PPPoE richiede che una macchina, sia essa un router od un server, funga da collegamento tra la rete interna e la rete Wireless. Questa macchina, denominata *Access Concentrator,* avrà il compito di autenticare e autorizzare in primo luogo l'utente, successivamente di codificare e decodificare il protocollo PPPoE.

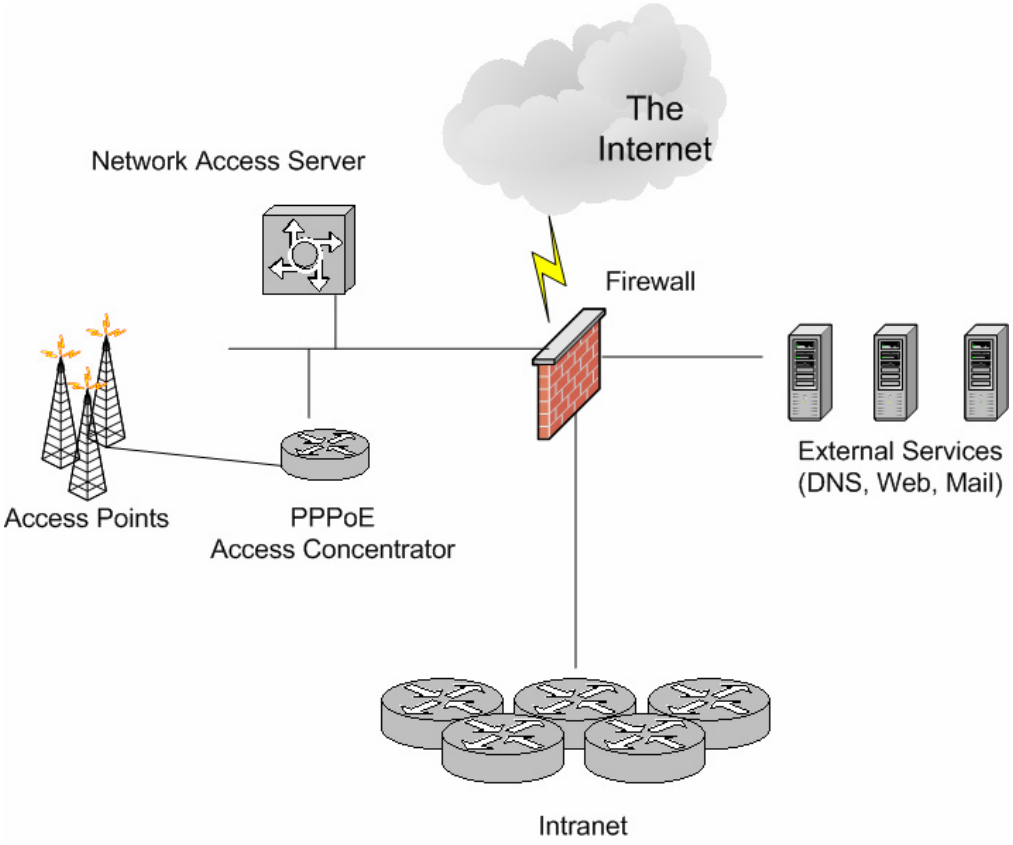

Fig. 4.1 - Esempio di Architettura PPPoE

È bene ricordare che durante la configurazione dell'Access Concentrator, lo scambio delle password tra il server e il client non deve essere di tipo Password Authentication Protocol (PAP), in quanto le password vengono scambiate in chiaro con questa metodologia. Si suggeriscono metodologie alternative, quali l'uso di CHAP e MS-CHAPv2.

L'uso di PPPoE in alcune tipologie di ambienti non ha vantaggi rispetto a IEEE 802.1x, ma la soluzione PPPoE è l'ideale qualora non si possa usare 802.1x congiuntamente ad IPSec, ad esempio dove 802.1x non è disponibile e negli

ambienti SOHO. Nei prossimi capitoli verranno descritti in maniera dettagliata quali ambienti possono essere l'ideale per la soluzione PPPoE.

Crittografia

Nel capitoli precedenti si è sottolineato quanto le onde radio siano difficili da controllare e quanto sia facile per un intruso intercettarle. Possiamo paragonare pertanto la wireless LAN a una rete pubblica di accesso. Ad esempio, nella Rete Telefonica Commutata (RTC), un aggressore può intercettare le password e i dati inserendosi nel sistema di distribuzione solitamente posizionato sulla strada. In quest'ottica, la wireless LAN è soggetta a vari attacchi ed è sempre suggeribile aggiungere un livello di crittografia in più rispetto a quanto offerto da WEP.

Il protocollo PPP e di conseguenza PPPoE, offre un'architettura di crittografia chiamata Microsoft Point-To-Point Encryption Protocol (MPPE). Questa estensione del Compression Control Protocol (CCP) è stata introdotta da Microsoft per applicare la sicurezza nel protocollo di VPN chiamato Point-to-Point Tunneling Protocol (PPTP). MPPE è basato sull'algoritmo Rivest-Shamir-Adleman (RSA) RC4 per effettuare la crittografia dei pacchetti e può usare una chiave crittografica fino a 128-bit. Inoltre MPPE può negoziare una modalità detta *stateless* che permette di cambiare la chiave di crittografia ogni qual volta esso si collega.

È abbastanza semplice introdurre l'uso di MPPE su collegamento basato su PPPoE, anche se non tutte le piattaforme supportano l'uso congiunto delle due tecnologie. PPPoE con l'estensione MPPE può essere un modo semplice per affrontare il problema di sicurezza in ambito wireless.

L'Access Concentrator

Nei paragrafi precedenti si è evidenziato come l'Access Concentrator (AC) funga da concentratore di accessi tra la rete wireless e la rete cablata, in maniera simile a quanto faccia un concentratore di accessi per i modem. In questo paragrafo si vuole fornire un esempio di come effettuare le configurazioni con i sistemi più diffusi quali i router Cisco e un server basato su Windows 2000.

Esempio con Windows 2000

L'esempio successivo descrive la configurazione di un Access Concentrator basato su tecnologia Windows 2000. Si assume che il computer abbia almeno queste caratteristiche:

- due schede di rete
- che il sistema operativo in uso sia Windows 2000 Professional/Server e che l'utente abbia familiarità con gli strumenti di amministrazione degli utenti e di rete.
- La configurazione è stata realizzata attraverso il programma *RASPPPOE* di Robert Schlabbach disponibile al sito Internet http://www.raspppoe.com/, da cui si può scaricare il driver. È necessario notare che il driver citato in questo esempio non supporta più di dieci connessioni in ingresso.

Distinguiamo la fase di installazione del driver, comune sia per il client che per il server, e la fase di configurazione della componente Remote Access Server (RAS) di Windows per agire come PPPoE Access Concentrator.

Preparazione all'installazione

Per installare il driver, si suggerisce di salvare i files aperti e di chiudere le applicazioni aperte, in quanto è possibile che l'installazione del driver richieda un riavvio del computer. È necessario che tutte le operazioni di configurazione vengano effettuate con un utente di classe "administrator".

Come descritto precedentemente si assume che il sistema operativo sia già stato installato e che vengano installati sia l'ultimo Service Pack disponibile che le HotFix di sicurezza specificate da Microsoft. Di default Windows 2000 è solito installare la feature *Remote Access and Internet Routing*: verificare che tale componente sia installato correttamente nel sistema e nel caso installarlo avendo cura di riapplicare il Service Pack o le HotFix. Per ragioni pratiche si suggerisce in questa fase di definire e configurare gli utenti da abilitare al collegamento remoto: è comunque possibile definire gli utenti anche in un secondo momento.

Successivamente è necessario collegare una interfaccia di rete sull'hub o switch della rete interna, l'altra sulla rete su cui sono attestati gli Access Point. Dal pannello *Network and Dial-Up Connections* aprire le proprietà della scheda di rete collegata verso la rete intranet e disabilitare tutti i servizi collegati (es: NetBIOS, File and Print services, Client for Microsoft Network), avendo cura di lasciare abilitato solamente il protocollo TCP/IP e configurandolo opportunamente.

Installazione del protocollo

Durante questa fase verrà installato il driver Point-to-Point over Ethernet sul sistema, configurandolo nella scheda di rete collegata verso la rete wireless.

- Scompattare il file ZIP del driver PPPoE in una directory temporanea
- Nel pannello *Network and Dial-Up Connections* aprire la proprietà della scheda di rete collegata verso la rete wireless e premere sul bottone *Install*
- Nella finestra *Select Network Component* selezionare *Protocol* e premere il bottone *Add*
- Nella finestra *Network Protocol* selezionare *Have Disk*
- Nella finestra *Install From Disk* selezionare la directory temporanea in cui si è scompattato il driver e premere *Ok*
- Selezionare *PPP over Ethernet Protocol* e premere *Ok*
- Durante l'installazione del protocollo verranno presentatate diverse finestre con il messaggio *Digital Signature Not Found*: premere sempre i pulsanti *Yes* o *Continue Anyway*
- Ritornati alla finestra delle proprietà della rete, togliere i checkbox a tutti i protocolli con l'esclusione di *PPP over Ethernet Protocol*

È probabile che il protocollo PPPoE venga anche abilitato sulla scheda di rete collegata verso la intranet pertanto è consigliabile controllare le proprietà di tale scheda e verificare che non ci sia *PPP over Ethernet Protocol.* Qualora ci fosse, assicurarsi che venga disabilitato su tale interfaccia.

A seguito di questa fase è suggerito effettuare un riavvio manuale del sistema, nel caso in cui non venga proposto da Windows.

Configurazione di Remote Access and Internet Routing

Durante questa fase si procederà a configurare *Remote Access and Internet Routing* per abilitare il sistema ad accettare le connessioni PPPoE, ovvero per fungere da PPPoE Access Concentrator. Il driver usato durante questo esempio usa il nome del computer come nome dell'Access Concentrator.

- Nel pannello *Network and Dial-Up Connections*, selezionare l'icona *Make New connection* per avviare il wizard di configurazione della rete.

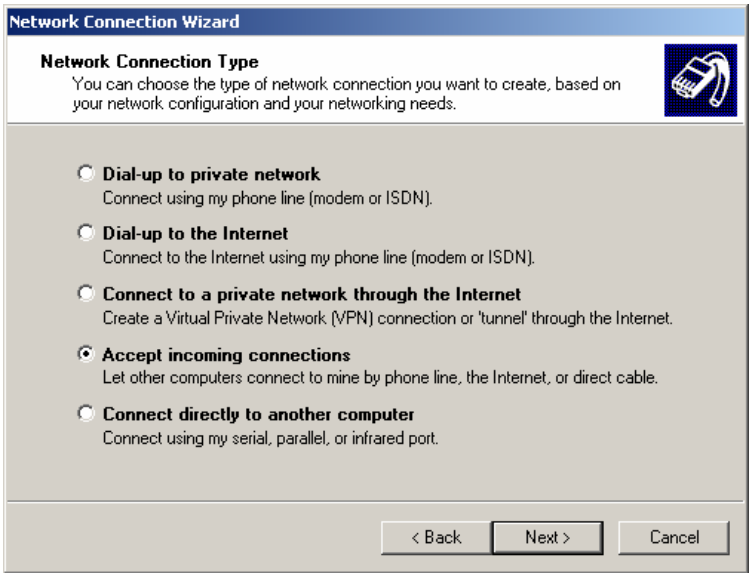

Fig. 4.2 - Configurazione di RAS per accettare connessioni

- Selezionare l'opzione *Accept incoming connections* e premere *Next*
- Nella lista dei devices dovrebbe apparire la scheda di rete collegata alla rete wireless, selezionarla e premere *Next*

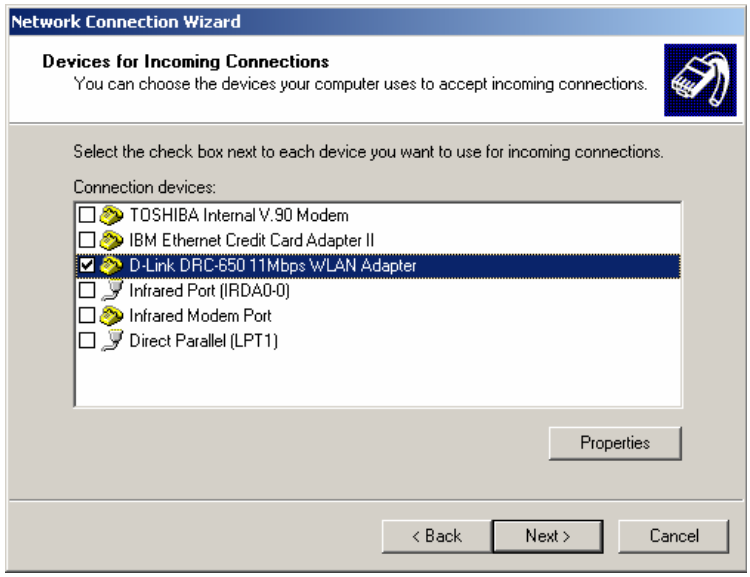

Fig. 4.3 - Scelta del device per le connessioni RAS

- Apparirà una schermata *Incoming Virtual Private Connection*, premere *Next*
- Alla schermata *Allowed User*, selezionare gli utenti di sistema che hanno il permesso di accedere in dial-in. Premere *Next*
- La finestra successiva è *Networking Components*. Si noterà che il *PPP over Ethernet Protocol* è nella lista, ma il checkbox è in grigio. Disabilitare tutti i protocolli con l'eccezione di TCP/IP e premere *Next*
- Nella finestra riassuntiva premere *Next* e successivamente *Finish*

Verrà create l'icona *Incoming Connections* nel pannello *Network and Dial-Up Connections,* selezionarla e premere *Properties.*

- Nella sezione *General*, selezionare la scheda di rete collegata alla rete wireless, avendo cura di deselezionare gli altri devices

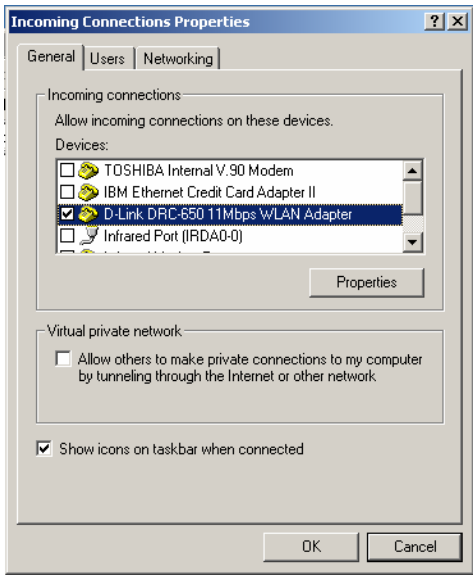

Fig. 4.4 - Propietà di Incoming Connections, General

- Nella sezione *Users* selezionare gli utenti da abilitare all'accesso PPPoE e selezionare *Require all users to secure their password and data*

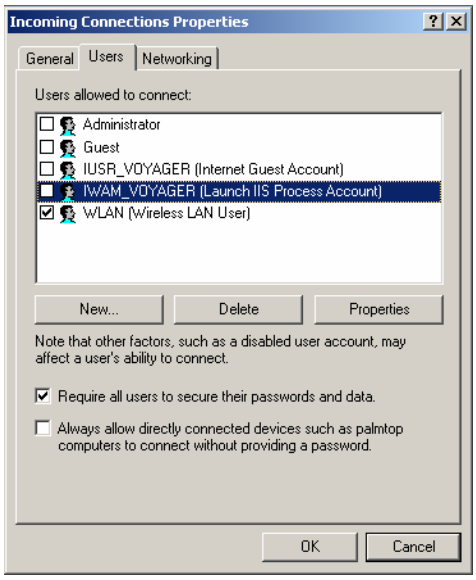

Fig. 4.5 - Propietà di Incoming Connections, Users

- Nella sezione *Networking* lasciare abilitato solamente il protocollo TCP/IP e disabilitare altri protocolli, ad esempio NetBEUI e *File and Printer Sharing for Microsoft Networks*
- Selezionare *PPP over Ethernet Protocol* e fare click due volte con il tasto sinistro del mouse. Una finestra di dialogo verrà aperta: nella sezione *General* aumentare il valore di *Number of lines (WAN endpoints)* fino al massimo consentito di 10. Premere *Ok*
- Selezionare *Internet Protocol (TCP/IP)* e premere il pulsante *Properties*.
- Selezionare *Allow callers to access my local area network*
- Selezionare *Assign TCP/IP address automatically using DHCP* qualora fosse disponibile un server DHCP sulla rete intranet.

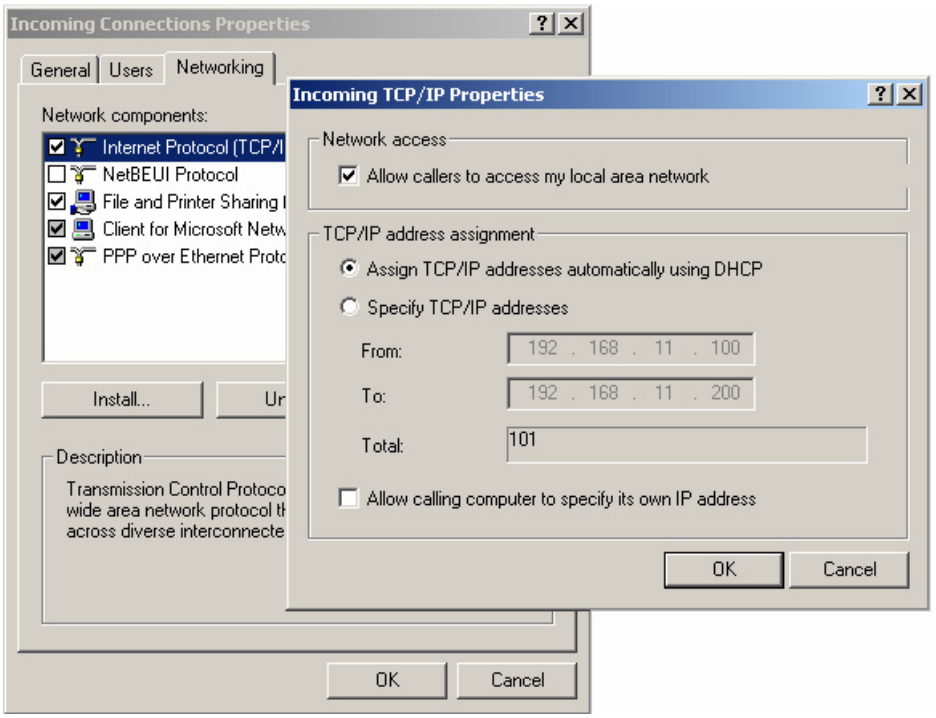

Fig. 4.6 - Propietà di Incoming Connections, Networking e definizione TCP/IP

- Qualora non fosse disponibile un DHCP server, selezionare un intervallo di indirizzi IP, avendo cura di selezionare pero' l'opzione Internet Connection Sharing (ICS) nella scheda di rete collegata alla Intranet. Questo è necessario per effettuare una riscrittura dell'header IP (NAT) quando si attraversa l'Access Concentrator.

Esempio con router Cisco

L'esempio precedente ha visto come configurare un server Windows 2000 per fungere da Access Concentrator. La limitazione dell'uso di Windows è sostanzialmente legata al massimo numero di collegamenti in ingresso, e la poca praticità di integrazione in un ambito più ampio, dove è già stata definita una politica di dial-up. È possibile sfruttare un router Cisco come Access Concentrator qualora sia presente in azienda. Tale router deve disporre di una interfaccia ethernet libera che dovrà essere collegata all'hub o switch su cui sono attestati gli Access Point. Si assume che si abbia familiarità con il sistema Cisco IOS e con la configurazione del dial-up.

L'esempio successivo è stato provato con una versione di IOS 12.2(11)T2.

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname myRouter
!
aaa new-model
!
aaa authentication ppp default local
aaa authorization network default local
aaa session-id common
enable secret 5 $1$5jXZ$ljbx2bPsFugsdD4WrHLSK.
!
username user1 password 0 user1
username user2 password 0 user2
memory-size iomem 5
ip subnet-zero
!
vpdn enable
!
vpdn-group PPPOE
 description Incoming PPPoE
 accept-dialin
  protocol pppoe
  virtual-template 10
!
interface Loopback1
 description Loopback interface for PPP
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 speed auto
!
interface Ethernet1/0
 no ip address
```

```
 half-duplex
 pppoe enable
!
interface Virtual-Template10
 description PPPoE General Template
 mtu 1492
 ip unnumbered Loopback1
 peer default ip address pool PPP_POOL
 ppp encrypt mppe 128
 ppp authentication ms-chapv2 ms-chap chap
!
ip local pool PPP_POOL 192.168.1.100 192.168.1.200
ip classless
no ip http server
ip pim bidir-enable
!
!
!
line con 0
line aux 0
line vty 0 4
 password mypassword
!
end
```

In questo esempio è da notare la configurazione del Virtual Template con i parametri *ppp encrypt mppe 128* e *ppp authentication ms-chapv2 ms-chap chap*, che consentono la crittografia a 128-bit la prima e lo scambio di password sicure la seconda.

È da notare che Cisco IOS supporta sia la possibilità di configurare l'autenticazione utenti attraverso RADIUS e Tacacs+ che la possibilità di assegnare gli IP addresses direttamente da un DHCP server. Si faccia riferimento alla Configuration Guide dell'IOS per avere maggiori informazioni sulla configurazione di tali opzioni.

Esempio con altri sistemi

È possibile usare altri sistemi operativi, al di fuori di quelli elencati precedentemente, per realizzare un Access Concentrator PPPoE. Questo capitolo vuole fornire, per completezza, un accenno alla loro configurazione, ma si sottolinea che questi esempi sono stati provati solo in parte, pertanto non privi di eventuali problematiche. Si assume che il lettore abbia esperienza nella configurazione dei sistemi operativi citati, compreso la ricompilazione di programmi, modifica del kernel e relativa ricompilazione.

FreeBSD

Aggiungere le seguenti linee nel file */etc/rc.conf*

```
### PPPOE
pppoed_enable="YES"
pppoed_interface="de0"
pppoed_flags="-P /var/run/ppoed.pid -l pppoein"
```

Definire nel file */etc/ppp/ppp.conf* la configurazione del ppp per l'accesso PPPoE:

```
pppoein:
 set ifaddr 10.0.2.1 10.0.2.20
 set dns 10.0.2.1
 set nbns 10.0.2.1
 disable utmp
 disable passwdauth
 enable lqr
 set cd 5!
 accept dns
 enable mschapv2 mppe
 disable deflate pred1
 deny deflate pred1
 set mppe 128 *
 set timeout 0
 set mru max 1400
 set mtu max 1400
 set speed sync
```

Linux

Verificare che nella propria distribuzione sia disponibile il software *Roaring Penguin PPPoE*, di solito contrassegnato come *rp-pppoe,* e installarlo. Qualora la distribuzione non abbia a disposizione il software, è possibile scaricare i binari ed i sorgenti dal sito http://www.roaringpenguin.com/pppoe.

È necessario inoltre scaricare le patch del kernel e le patch di PPPD 2.4.1 per abilitare l'uso del protocollo MPPE e, successivamente, applicarle. L'URL da cui si possono scaricare tali patch è http://public.planetmirror.com/pub/mppe/. Alcune distribuzioni forniscono il programma PPPD e il kernel con queste feature abilitate: si consiglia di verificare con il manuale o con le FAQ della propria distribuzione.

In seguito, configurare il file */etc/ppp/pppoe-server-options* in maniera simile a quanto segue:

```
debug
name *
lock
mtu 1490
mru 1490
proxyarp
auth
+chap
+chapms
+chapms-v2
ipcp-accept-local
ipcp-accept-remote
lcp-echo-failure 3
lcp-echo-interval 5
deflate 0
mppe-128
mppe-40
mppe-stateless
```

Configurare successivamente il file */etc/ppp/pppoe-server-pool-ip* con un intervallo di IP address da assegnare agli utenti wireless, e configurare il file */etc/ppp/chap-secrets.* Per eseguire il server PPPoE su Linux, eseguire il seguente comando:

pppoe-server -I ethX -C ACNAME-l 192.168.0.1 -p /etc/ppp/pppoe-server-pool-ip

dove *ethX* è l'interfaccia collegata alla rete Wireless, *ACNAME* è il nome dell'Access Concentrator e *192.168.0.1* è l'IP address da assegnare al server, che deve essere congruente con quanto specificato in */etc/ppp/pppoe-server-pool-ip*. Per maggiori informazioni sui parametri di configurazione, si faccia riferimento alle man pages o alla documentazione allegata con i programmi.

Il client

L'Access Concentrator è il punto più critico della configurazione di un accesso PPPoE e la maggioranza dei concetti e della configurazione di un Access Concentrator può essere applicata al client. È da notare che il supporto PPPoE client è molto più diffuso rispetto alla funzionalità di Access Concentrator, però non tutte le implementazioni client PPPoE accettano anche l'estensione MPPE per la crittografia. Nei paragrafi successivi si elencano alcuni esempi di configurazione di client Windows 2000, Linux e FreeBSD.

Esempio con Windows 2000

La scheda di rete wireless viene riconosciuta dal sistema operativo come una scheda di rete tradizionale, pertanto posta nel pannello di configurazione *Network and Dial-Up Connections*.

- Aprire le proprietà della scheda di rete e installare il protocollo *PPP over Ethernet* come indicato nel paragrafo "Esempio di AC con Windows 2000 - Installazione del protocollo".
- Successivamente, premere *Start,* selezionare *Run,* inserire il programma *RASPPPOE* e premere *Ok*.

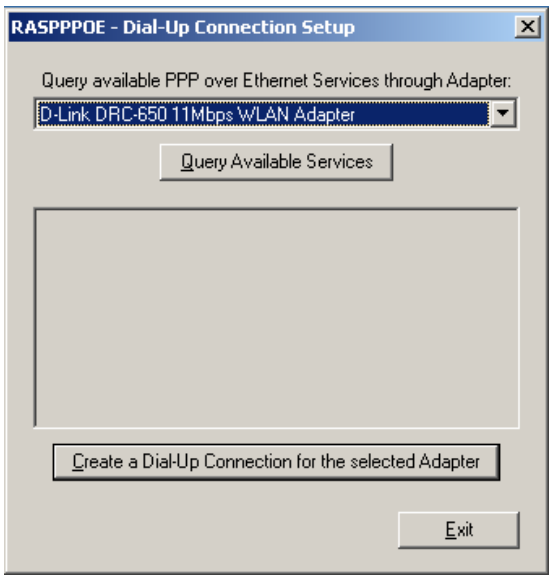

Fig. 4.7 - Query dei sevizi PPPoE disponibili

- Verrà presentata una finestra di dialogo. Selezionare la scheda di rete wireless dall'opzione *Query available PPP over Ethernet Services through Adapter*

qualora si abbiano più di una scheda di rete installata dalla macchina

- Premere il pulsante su *Create a Dial-Up Connection for the selected Adapter*
- Verrà creata un'icona chiamata *Connection through "Nome Adattatore"* nel pannello *Network and Dial-Up Connections*
- Selezionare la nuova icona e premere *Properties.*
- Nella sezione *Security*, selezionare *Required secured password* e selezionare *Require data encryption*

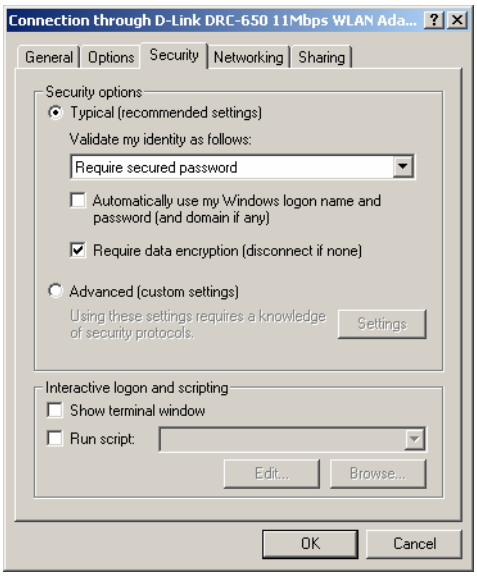

Fig. 4.8 – Selezione della cifratura MPPE

- Nella sezione *Networking*, selezionare unicamente il protocollo TCP/IP
- Premere *Ok*

Per eseguire la connessione, fare click due volte sulla nuova icona e fornire username e password, come definito sul server. È possibile configurare client con altre versioni di Windows con lo stesso driver PPPoE: si suggerisce di leggere il file di documentazione *readme9x.htm* per Windows 95/98/ME e *readment.htm* per Windows NT.

Esempio con altri sistemi

Analogamente per quanto specificato nell'Access Concentrator è possibile usare client non-Windows per collegarsi usando il protocollo PPPoE. Sebbene esistano implementazioni client in grado di supportare PPPoE, non tutti sono in grado di supportarlo congiuntamente a MPPE. Nei paragrafi successivi si daranno per completezza di informazione alcuni cenni su come configurare PPPoE su altri sistemi operativi, ma si sottolinea che è necessario avere esperienza nella configurazione dei sistemi operativi citati, compreso la ricompilazione di programmi, modifica del kernel e sua ricompilazione.

FreeBSD

Sul client andrà configurato il file */etc/ppp/ppp.conf* come da esempio:

```
connesione:
 set device PPPoE:wi0
 disable pap
 enable mschapv2
 enable lqr
 set cd 5
 set dial
 set login
 set redial 0 0
 set authname username
 set authkey password
```

Nell'esempio *username* e *password* vanno adattati in maniera adeguata. Per iniziare la connessione, è necessario eseguire il comando *ppp -ddial connessione*.

Linux

Verificare che, nella propria distribuzione, sia disponibile il software *Roaring Penguin PPPoE*, di solito contrassegnato come *rp-pppoe* e installarlo. Qualora la distribuzione non abbia a disposizione il software, è possibile scaricare i binari ed i sorgenti dal sito http://www.roaringpenguin.com/pppoe.

È necessario modificare il kernel di Linux e il programma PPPD anche per il client: si faccia riferimento al capitolo "Access Concentrator - Esempio con altri sistemi - Linux" per indicazioni su quali programmi sono necessari. Alcune distribuzioni forniscono il programma PPPD e il kernel con queste feature abilitate. Si consiglia di verificare con il manuale o con le FAQ della propria distribuzione.

È necessario modificare il file */etc/ppp/pppoe.conf* per riflettere i parametri di configurazione utente, in particolare il campo *USER*, che deve contenere un utente valido, e *PPPD_EXTRA="mppe-128 mppe-stateless require-chapms-v2"*. È necessario anche modificare il file */etc/ppp/chap-secrets* per inserire la coppia username e password. Il comando per avviare la connessione è *adsl-start* ed analogamente *adsl-stop* per terminarla.

5. IEEE 802.1x

Lo standard IEEE 802.1x permette di identificare in maniera sicura gli utenti, collegati ad una determinata porta ethernet o ad un Access Point, ed applicare di conseguenza il livello di sicurezza necessario: ad esempio ad un nostro partner possiamo dare la possibilità di navigare solamente su internet, mentre l'amministratore delegato può accedere al database principale. IEEE 802.1x è nato per l'identificazione e l'autorizzazione dell'utente su reti wireless e più in generale su reti ethernet, permettendo servizi personalizzati quali il raggruppamento di una classe di utenti in una determinata Virtual LAN.

Il protocollo è basato su Extensive Authentication Protocol Over Lan (EAPOL) che prevede differenti tipologie di autenticazione, tra cui MD5 e TLS. Sebbene questo protocollo sia l'ideale per riconoscere un utente e dare l'accesso alla rete, si possono evidenziare tre sue implicazioni. La prima é che IEEE 802.1x non definisce un sistema di crittografia: questo protocollo si limita ad autenticare l'utente, anche se in seguito verrà descritto in che modo é in grado di "integrarsi" con WEP. Il secondo problema é che molti degli Access Point esistenti non dispongono di 802.1x. Quegli AP che non dispongono della possibilità di essere aggiornati via software devono essere sostituiti. Inoltre é probabile che i futuri AP a basso costo, tipicamente pensati per l'utenza domestica e piccoli uffici, non disporranno di 802.1x, che necessita comunque di una infrastruttura RADIUS. Infine solamente alcuni sistemi operativi, ad esempio Windows 2000 e Windows XP, supportano nativamente IEEE 802.1x. I sistemi Apple con MacOS e chi dispone di sistemi Windows 95/98/ME/NT devono acquistare un client compliant con IEEE 802.1x, con costi aggiuntivi. Il costo potrebbe rappresentare un problema minore per una azienda con un numero definito di utenti, ma potrebbe essere un rischio di business per un ISP o un operatore mobile che decidesse di offrire accesso Wireless.

Sempre più produttori stanno sposando questa tecnologia, sia sulle reti ethernet tradizionali che su quelle wireless. Questa tipologia di autenticazione pone un ulteriore ostacolo tra il probabile intruso e la rete privata, pertanto è bene attivare questa caratteristica qualora si disponga di una infrastruttura PKI, e qualora gli Access Point siano compatibili con IEEE 802.1x. È bene verificare, sia sul manuale che con il produttore degli Access Point, la compatibilità a tale standard e le sue specifiche di configurazione.

IEEE 802.1x, EAP e le reti Wireless

Lo standard IEEE 802.1x é nato soprattutto per sopperire alla mancanza di autenticazione delle reti Wireless, ma i loro creatori hanno esteso il concetto di autenticazione anche per le reti tradizionali. Si pensi ad esempio ad un visitatore che entra nell'azienda e collega il suo portatile ad una presa ethernet: questa persona non deve avere gli stessi diritti di accesso alla rete di un amministratore di sistema. Il sistema 802.1x é un "Port-based access control mechanism", ovvero un sistema in grado di autenticare un utente collegato ad una determinata porta ethernet.

Al fine di poter identificare e autorizzare l'utente finale IEEE ha scelto di incapsulare su ethernet il protocollo Extensible Autentication Potocol. EAP é un framework di autenticazione inizialmente pensato per il Point-to-Point Protocol (PPP) che supporta differenti schemi di autenticazione. EAP non definisce uno specifico metodo di autenticazione, bensì permette di negoziare il protocollo di autenticazione tra i due interlocutori, ovvero l'utente e il server di autenticazione (tipicamente Radius). Sono stati definiti alcuni schemi di autenticazione EAP, i più famosi dei quali sono: MD5, TLS, TTLS, LEAP, PEAP, SecurID, SIM e AKA. Vediamone alcuni in dettaglio.

EAP-MD5. Si tratta di un'autenticazione basata su MD5, molto simile al protocollo CHAP, dove un algoritmo di hash *one-way* viene usato in combinazione ad uno *shared secret* e un *challenge*. Il suo uso é sconsigliabile in ambiente Wireless perché gli hash delle password possono essere soggetti ad un attacco di tipo "dictionary attack". Se un potenziale intruso riesce ad ottenere il *challenge* e l'hash fornito come riposta, questo può provare a ricavare la password off-line con appositi programmi. Inoltre, EAP-MD5 fornisce solo un'autenticazione del client non verificando la rete a cui ci si sta autenticando. In questo caso é possibile che un potenziale intruso, attraverso l'uso di un falso Access Point, possa redirigere l'utente in una falsa rete e prendere informazioni preziose.

EAP-TLS. Il Transport Layer Security (TLS) offre un'autenticazione sicura, che sostituisce le password con una autenticazione basata sui certificati digitali X.509. Al contrario di EAP-MD5, EAP-TLS supporta la "mutual authentication", ovvero sia il client che il server vengono verificati, evitando frodi relative all'inserimento di falsi Access Points. EAP-TLS é un'ottima scelta per la sicurezza dell'autenticazione in 802.1x quando una Public Key Infrastructure (PKI) é già stata adottata. Il grosso svantaggio di EAP-TLS é il costo elevato generato dalla manutenzione di una PKI: essa infatti richiede licenze software, personale qualificato e corsi di

formazione. Tra i vari meccanismi EAP, il TLS é lo standard più diffuso per l'autenticazione basata su 802.1x.

EAP-LEAP. Light EAP (LEAP), chiamato anche Cisco EAP, é una implementazione proprietaria di Cisco che permette la "mutual authentication" e permete di usare username e password come meccanismo di autenticazione. Anche se una buona politica delle password può fare di LEAP un protocollo sicuro, esso é soggetto ad attacchi di tipo "dictionary attack", così come EAP-MD5. Nonostante LEAP sia un protocollo proprietario di Cisco Systems, la casa di San Francisco si sta orientando verso i protocolli EAP-TLS e EAP-PEAP.

EAP-TTLS. Tunneled Transport Layer Security (TTLS) é un estensione di EAP-TLS che é stata creata per evitare la necessità di certificati per i client. Come per altri sistemi di autenticazione "tunneling" (PEAP é l'altro attualmente disponibile), TTLS é basato su un autenticazione a due fasi. Nella prima fase un algoritmo assimmetrico basato sulla chiave del server é usato per verificare le credenziali del server e la creazione di un tunnel sicuro. Nella seconda fase, il client viene riconosciuto usando un secondo metodo di autenticazione che verrà fatto passare attraverso il tunnel sicuro (da qui il termine "tunneling") creato precedentemente. Può essere usato un qualsiasi schema di autenticazione per la seconda fase, sia esso EAP-MD5, EAP-MSCHAPv2 o anche sistemi legacy quali PAP, CHAP, MS-CHAP o MS-CHAPv2.

EAP-PEAP. Il Protected EAP (PEAP) é un Internet Draft di Cisco, Microsoft e RSA. PEAP é simile al TTLS, in quanto sono gli unici due protocolli EAP di tipo "tunneling". Come per TTLS, viene creato un tunnel sicuro tra il server e il client in cui viene incapsulata l'autenticazione del client. Al contrario di TTLS, PEAP non supporta i sistemi legacy (PAP, CHAP, ecc...).

Attraverso EAP, lo standard IEEE 802.1x permette la distribuzioni di chiavi WEP attraverso la frame *EAPOL-Key*: questo tipo di messaggio EAP permette di inviare una o più chiavi WEP al client. Grazie a EAPOL-Key é possibile, su alcuni Access Point, usare chiavi WEP totalmente differenti per ogni sessione, ridimensionando il problema relativo alla derivazione delle chiavi WEP.

IEEE 802.1x é un ottimo protocollo, in quanto risolve problematiche relative all'autenticazione degli utenti e al cambio delle chiavi WEP, tuttavia i problemi relativi alla privacy dei dati inviati via Wireless rimangono. WEP ha una crittografia debole ed é possibile comunque derivare le chiavi su una sessione Wireless di lunga durata, pertanto sarebbe comunque necessaria una crittografia aggiuntiva quale IPSec. Inoltre é sempre possibile mandare pacchetti di disassociazione agli Access Point, falsificando gli header 802.11b.

Come funziona EAP-TLS

Come menzionato precedentemente, EAP-TLS é attualmente lo schema di autenticazione più diffuso per 802.1x/EAP. I componenti che svolgono un ruolo durante l'autenticazione 802.1x sono il *supplicant*, ovvero il computer dell'utente, l'*authenticator* (l'Access Point) ed infine l'*authentication server*, ovvero il RADIUS server. Durante l'autenticazione, sia il supplicant che il RADIUS devono supportare EAP-TLS, mentre l'Access Point deve supportare solamente 802.1x/EAP: l'AP non é a conoscenza del tipo di schema di autenticazione EAP.

Nella figura 5.1 é illustrato come funziona il processo di autenticazione 802.1x con EAP-TLS. É da notare che sia LEAP che MD5 usano lo stesso processo di autenticazione.

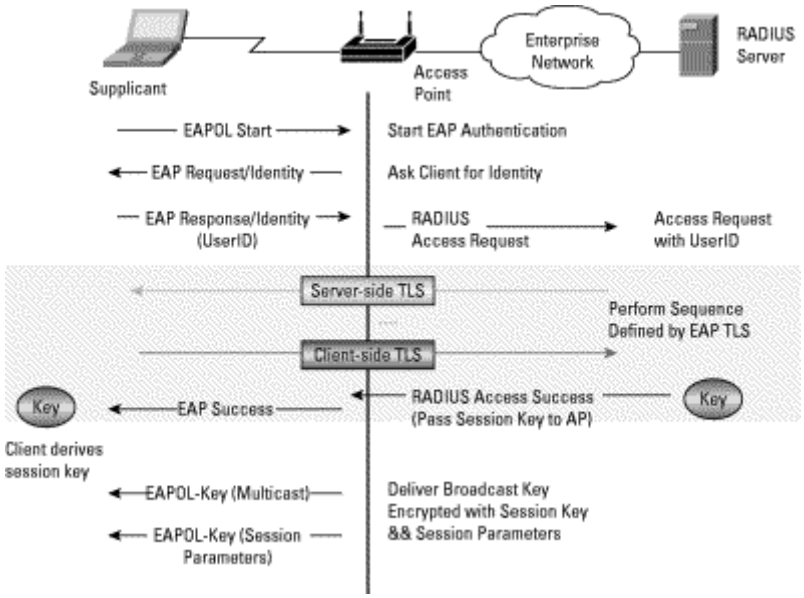

Fig. 5.1 –Processo di autenticazione 802.1x con EAP

In dettaglio, durante la conversazione EAP, il RADIUS server manda il proprio certificato al client e richiede il certificato del client. Il client valida il certificato del server e risponde con un messaggio EAP contenente il suo certificato. Il client inizia contestualmente anche la negoziazione per la crittografia, ovvero algoritmi di cifratura e compressione. Dopo che il certificato del client viene validato, il server risponde con le specifiche crittografiche della sessione. Nella figura 5.2 viene illustrata in dettaglio questa sequenza.

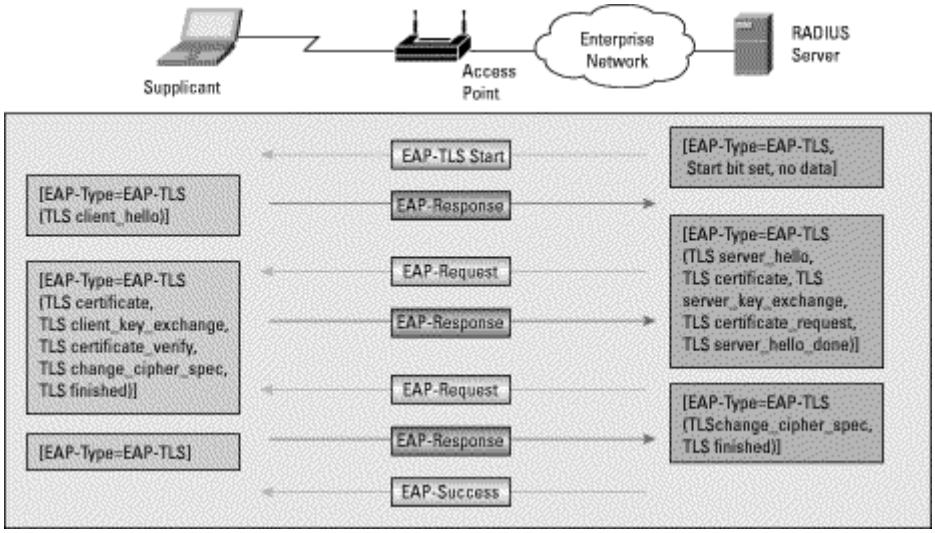

Fig. 5.2 - Dettaglio del processo di autenticazione 802.1x con EAP-TLS

Derivazione della chiave WEP in EAP-TLS

Durante l'handshake TLS tra client e server, il client genera un *pre-master secret* che viene crittografato con la chiave pubblica del server e lo manda successivamente al server. Il pre-master secret, dei valori casuali tra client e server e il *master secret* vengono usati per generare una chiave per la sessione. La *pseudo-random function* (PRF), che serve per generare la chiave della sessione é definita nel RFC 2246 (TLS), mentre l'RFC 2716 specifica come derivare la chiave della sessione. Successivamente viene riusata la funzione PRF insieme al *master secret*, congiuntamente a dei valori casuali (del server e del client) e alla stringa relativa al tipo di crittografia EAP proposta dal client per generare le chiavi di sessione, le chiavi Message Authentication Code (MAC) e il vettore di inizializzazione (IV). É importante sottolineare che sia il client che il RADIUS server derivano le chiavi di sessione in modo indipendente, anche se la lunghezza della chiave di sessione é determinata dall'Access Point ed é inviata attraverso un messaggio di tipo EAPOL-Key. La figura 5.3 riassume le fasi di derivazione della chiave WEP.

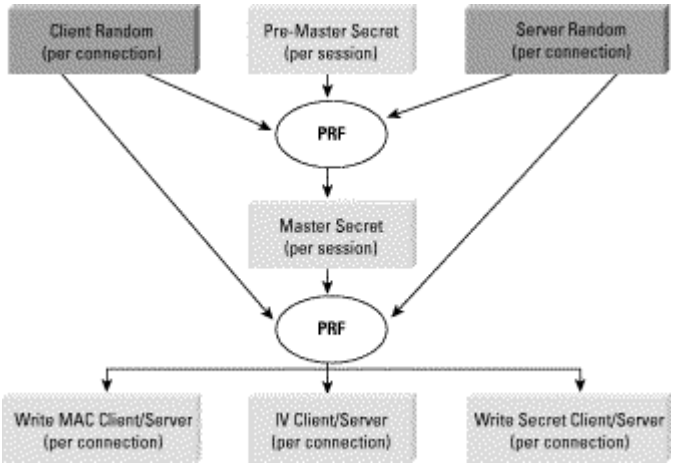

Fig. 5.3 – Uso della PRF per derivare le chiavi WEP

Configurazione del Radius Server

Per configurare IEEE 802.1x con EAP-TLS é necessario configurare per primo un RADIUS server che fungerà da server di autenticazione. Gli utenti wireless che si collegheranno all'access point verranno autenticati attraverso questo server, che deve supportare l'autenticazione di tipo EAP-TLS per poter permettere l'accesso. Si assume che l'amministratore abbia familiarità con il protocollo RADIUS ed inoltre si assume che si abbiano a disposizione i relativi certificati digitali, i quali devono essere rilasciati dall'amministratore della Certification Authority (sia essa interna o in outsourcing). Nei capitoli successivi si vuole fornire un esempio di due radius server che supportano l'autenticazione EAP-TLS, ovvero l'*Internet Authentication Service*, di Windows 2000 e 2003, e FreeRADIUS, disponibile per ambienti Unix.

Esempio di RADIUS con Windows (IAS)

L'esempio successivo descrive la configurazione di un RADIUS basato su tecnologia Windows. Per poter installare tale server é necessario avere installato Windows 2000 Server con Service Pack 3 o superiore, oppure Windows 2003 Server. Si assume che:

- il server DHCP sia già stato installato, o che esista già un server DHCP disponibile
- il certificato del server sia già installato e che l'utente abbia familiarità con gli strumenti di amministrazione degli utenti e di rete
- l'utente abbia familiarità con i tools di amministrazione

Per installare il RADIUS server, é necessario aprire il pannello di controllo ed eseguire *Add/Remove Programs*. Selezionare successivamente *Add/Remove Windows Components* e dalla categoria *Networking Services* selezionare *Internet Authentication Service*.

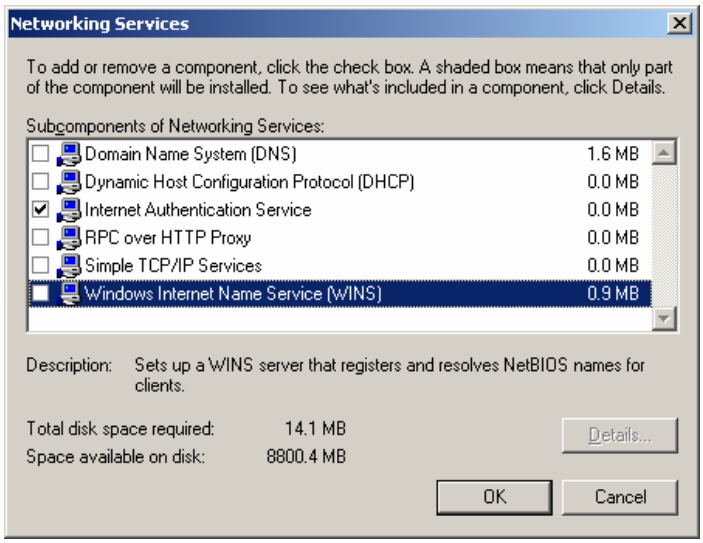

Fig .5.4 - Installazione del servizio IAS

Internet Authentication Service é stato installato, ma é necessario configuralo affinché sia possible l'autenticazione tramite IEEE 802.1x. Per fare ciò, é necessario aprire l'apposita icona *Internet Authentication Service* dalla voce del pannello di controllo *Administrative Tools*. Una volta aperto il programma si procederà come segue:

- Selezionare la cartella *Clients* e, con il tasto destro del mouse, selezionare *New Client*.
- Inserire il nome relative all'Access point e premere *Next.*

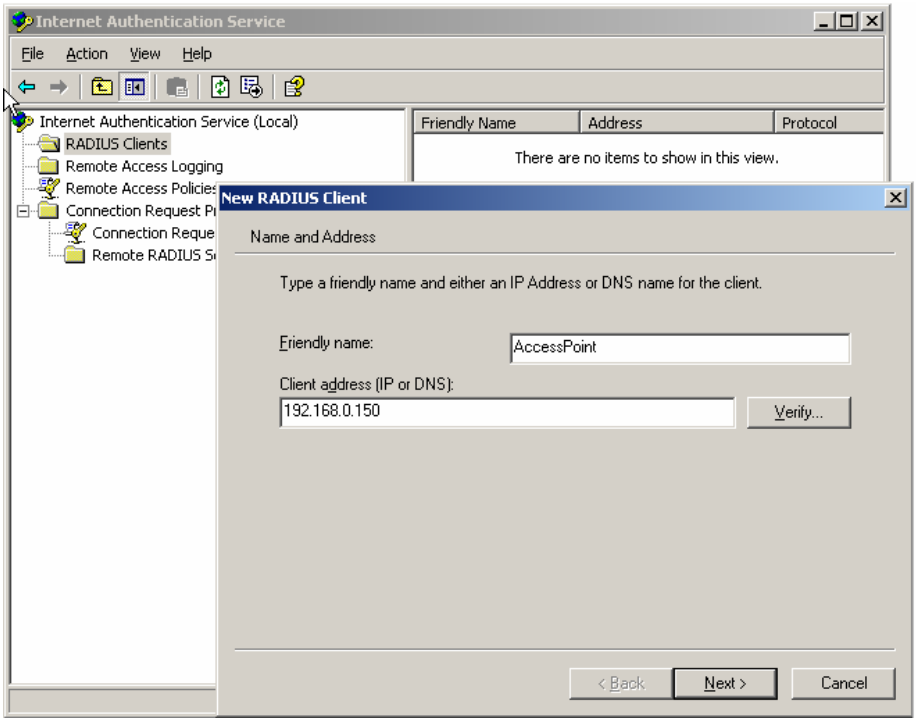

Fig. 5.5 - Configurazione di IAS, nuovo RADIUS client

- Inserire l'IP address dell'Access Point e uno shared secret (o parola d'accesso) e selezionare *Finish*. Il parametro *shared secret* servirà durante la configurazione dell'Access Point, pertanto é necessario ricordarsi tale password.
- Con il tasto destro del mouse, selezionare *Remote Access Policies* e successivamente *New Remote Access Policy*.
- Dare un nome alla policy, ad esempio *eap-tls*, e premere *Next*.
- Premere *Add.* In questa schermata si definiscono le condizioni valide affinché l'utente può accedere alla rete. A titolo di esempio si potrebbe restringere l'uso della wireless ai solo orari lavorativi con *Day-And-Time-Restrictions*, e premendo *Add.*
- Selezionare *Permitted*, poi *OK* e premere *Next*.
- Selezionare *Grant remote access permission*, e premere *Next*
- Fare click su *Edit Profile...* e selezionare la sezione *Authentication*. Assicurarsi che *Extensible Authentication Protocol* e *Smart Card or other Certificate* siano seleazionati. Rimuovere la selezione da altri sistemi di autenticazione e premere *OK.*

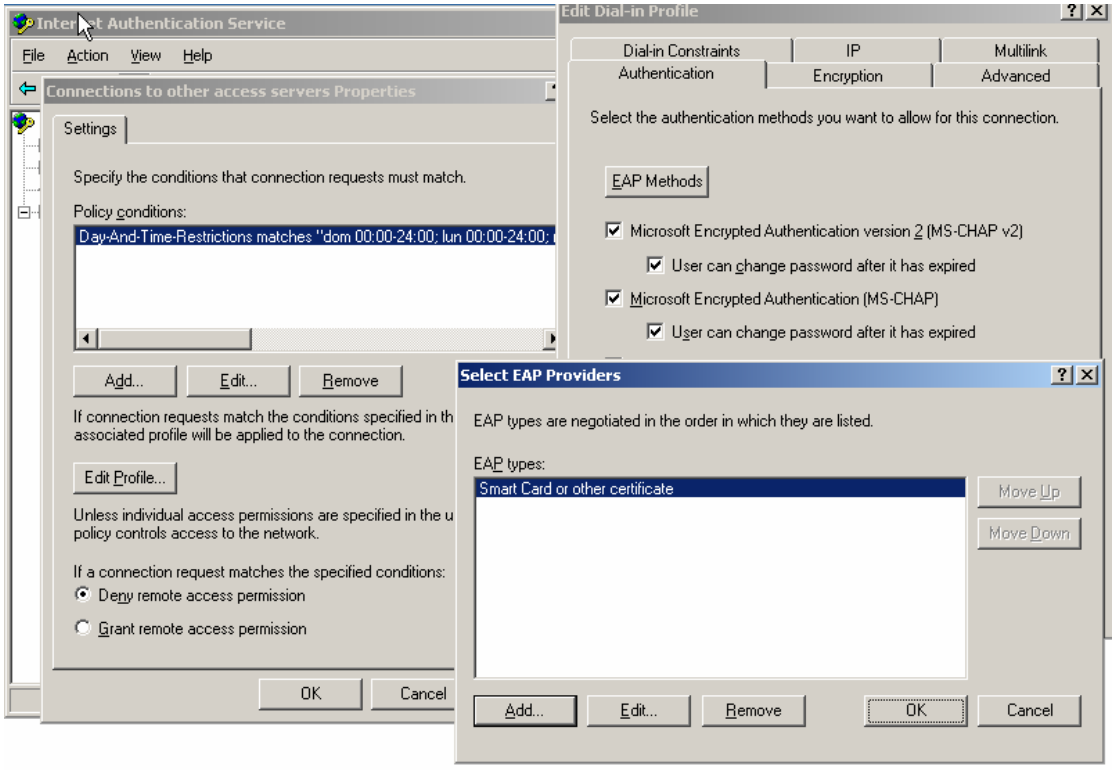

Fig. 5.6 - Creazione di una nuova policy di accesso remoto in IAS

Per completare l'installazione é necessario abilitare gli utenti all'accesso remoto. Tali passi sono già stati illustrati nel capitolo relativo al PPPoE.

Esempio di RADIUS con FreeRADIUS

Gli ambienti Unix sono tra i più usati come RADIUS server e uno dei software più popolari é FreeRADIUS. Tale software é compatibile con molte piattaforme Unix tra cui Linux, Solaris e Aix, ed é incluso in alcune distribuzioni Linux. É necessario verificare se la propria distribuzione Linux o il proprio sistema operative dispone di FreeRADIUS. Qualora non fosse disponibile, i sorgenti del programma possono essere scaricati dal sito http://www.freeradius.org/.

Per compilare FreeRADIUS nella maniera corretta, bisogna prima eseguire lo script *./configure* con i parametri desiderati e poi modificare il file *Makefile* nella sottodirectory *src/modules/rlm_eap/types/rlm_eap_tls/* alterando i seguenti valori:

```
TARGET = rlm_eap_tls
RLM_CFLAGS = $(INCLTDL) -I../.. -I/usr/local/openssl/include
RLM_LDFLAGS += -L/usr/local/openssl/lib
```

Facendo attenzione di sostituire */usr/local/openssl/include* e */usr/local/openssl/lib* rispettivamente con il percorso dei file include e le librerie di OpenSSL. Bisogna successivamente eseguire *make* per iniziare l'effettiva compilazione e, dopo aver compilato il programma, sarà sufficiente eseguire *make install* per effettuare l'installazione.

Affinché avvenga l'autenticazione IEEE 802.1x é necessario configurare il file *client.conf* con l'IP address e lo *shared secret* dell'Access Point. Inoltre, nel file *radiusd.conf* abilitare *default_eap_type = tls* e configurare la sezione TLS con i files relativi ai certificati per la 802.1x. Nel file *users*, per ogni utente che accederà alla rete Wireless, indicare *Auth-Type := EAP*. Il file di configurazione dir FreeRADIUS é molto complesso, si veda ad esempio un estratto esemplificato del file di configurazione per le sezioni che competono EAP:

```
modules {
          # Altri moduli del radius, come CHAP
          # LDAP o Unix

          eap {
                    # Abilito sia TLS che MD5, ma preferisco
                    # TLS
                    default_eap_type = eap-tls
                    md5 {
                    }

                    tls {
                              # Secret della chiave privata
                              private_key_password = mysecrete
                              # Chiave privata
                              private_key_file = /etc/raddb/priv.pem
                              # Chiave pubblica
                              certificate_file = /etc/raddb/pub.pem
                              # Chiave pubblica CA
                              CA_file = /etc/raddb/cacert.der
                              # Files da creare con testo random
                              dh_file = /etc/raddb/DH
                              random_file = /etc/raddb/random
                    }
          }
          ...
}

# Inserire EAP tra I moduli di autorizzazione
authorize {
          ...
          eap
}
# Inserire EAP tra I moduli di autenticazione
authenticate {
          eap
}
```

Infine, per avviare il radius server é sufficiente eseguire il seguente comando:
/usr/local/radius/sbin/radiusd -X -A

Configurazione dell'Access Point

Dopo aver configurato il RADIUS server é necessario abilitare il sistema di autenticazione 802.1x. Ogni Access Point é totalmente differente in questo, anche se i passi da seguire sono identici: l'abilitazione di 802.1x/EAP, inserimento del RADIUS server e relative porte di autenticazione/accounting (di default sono rispettivamente 1812 e 1813 su UDP), abilitazioni delle chiavi WEP. Per maggiori informazioni su come inserire questi parametri, si suggerisce di riferirsi al manuale del produttore dei propri Access Ponts.

A titolo di esempio, si vuole fornire una configurazione di Access Point Cisco, assumendo che la configurazione di base sia già stata effettuata (SSID, Frequenze, ecc..). Configurandolo attraverso un web browser, selezionare *Home*, *Setup*, *Security* ed infine *Authentication Server*. Assicurarsi che sia selezionato *Draft 10* nel campo *802.1x Protocol Version* ed inserire l'IP address del server RADIUS nella casella *Server Name/IP*. Si suggerisce di inserire l'IP address per evitare il tempo dovuto alla risoluzione del nome. Il parametro *Server Type* deve rimanere RADIUS, la porta deve essere impostata a *1812* e lo *Shared Secret* deve essere lo stesso impostato nel RADIUS server. Assicurarsi inoltre che la checkbox *EAP Authentication* sia abilitata.

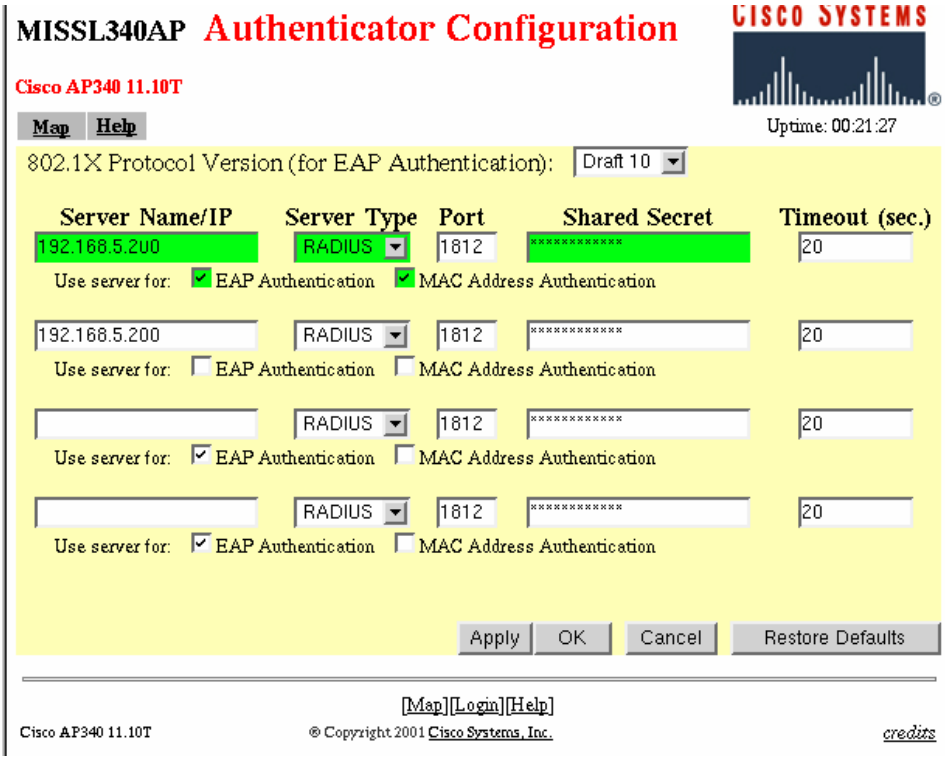

Fig. 5.7 - Configurazione del RADIUS su un AP Cisco

Ritornare successivamente al menù *Security* e selezionare il menù *Radio Data Encryption (WEP)*. Deselezionare tutti i tipi di autenticazione eccetto le opzioni *Open* nelle colonne *Accept Authentication Type* e *Require EAP* come da figura successiva.

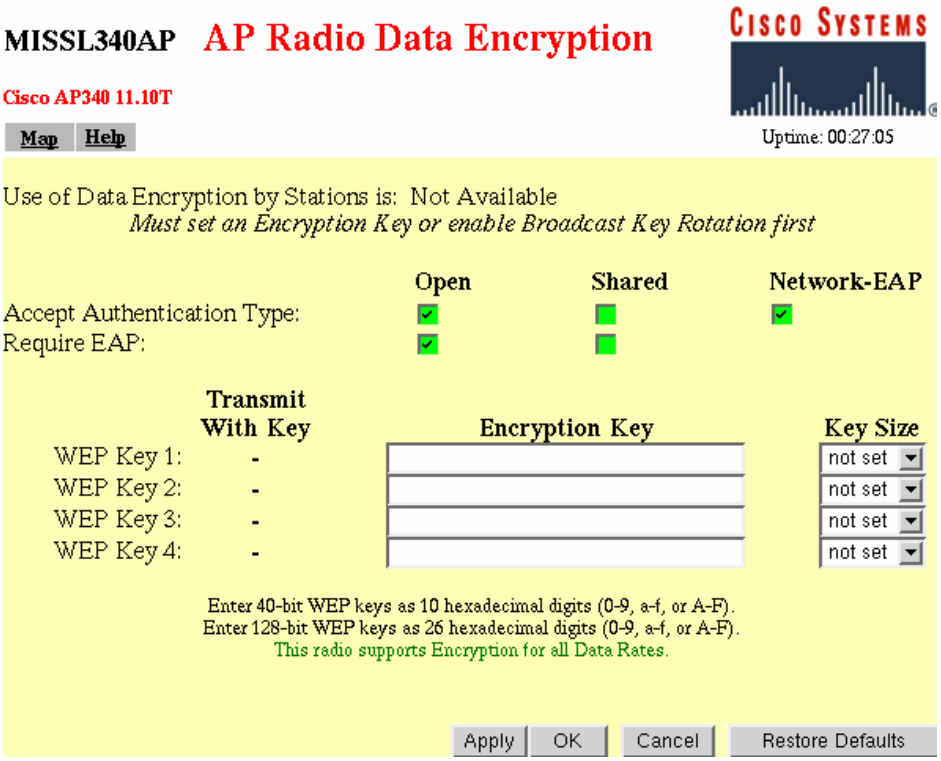

Fig. 5.8 - Abilitazione di EAP su un AP Cisco

Con l'Access Point Cisco e con il client 802.1x di Windows XP é possibile abilitare la generazione dinamica delle chiavi WEP per sessione. Come descritto nei paragrafi precedenti, l'abilitazione della generazione della chiave WEP per sessione (EAPOL-Key) possono mitigare i problemi di sicurezza relativi al WEP. Per abilitare tale funzione, sempre dal menù *Radio Data Encryption (WEP)* bisogna selezionare nella voce *Use of Data Encryption by Stations* il valore *Full Encryption.*

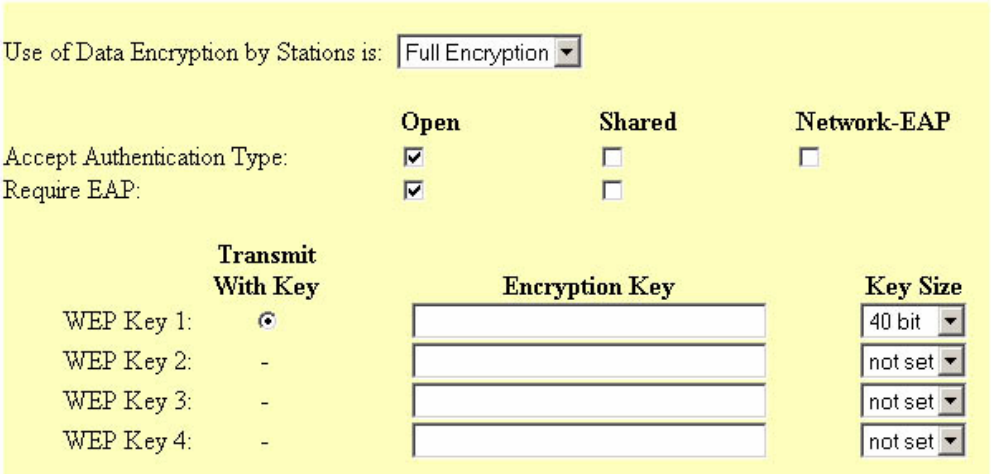

Fig. 5.9 - Configurazione di un AP Cisco per la distribuzione chiavi WEP

Configurazione del client

L'ultimo passo per la configurazione di IEEE 802.1x é quello di installare e configurare il client. Solo nelle recenti versioni dei sistemi operativi, quali ad esempio Windows XP é incluso un client per questo protocollo, mentre per altri sistemi operativi é necessiario disporre di un client separato, sia esso commerciale od OpenSource. Nei prossimi paragrafi verranno descritti tali client, assumendo che l'amministratore abbia buona familiarità con la configurazione del sistema operativo e della configurazione dei certificati digitali (per Windows XP).

Esempio con Windows XP e Windows 2000

Come accennato in precedenza, Windows 2000 e Windows XP sono attualmente gli unici sistemi operativi che dispongono del protocollo IEEE 802.1x. Su Windows 2000 è però necessario installare l'apposito client descritto Microsoft Knowledge Base Article numero *313664* e scaricabile gratuitamente sul sito internet http://support.microsoft.com/default.aspx?scid=kb;en-us;313664. Vedremo negli esempi successivi la configurazione attraverso Windows XP, che differisce da Windows 2000 dalla gestione nativa delle chiavi WEP e di WPA. Si assume che l'amministratore di sistema o l'utente abbia già scaricato ed installato il proprio certificato digitale X.509.

- Da *Control Panel*, selezionare *Network Connections* (si trova sotto *Network and Internet Connections*)
- Con il tasto destro del mouse su *Wireless Network Connection*, selezionare *Properties*

- Selezionare la sezione *Authentication*, selezionare *Enable network access control using IEEE 802.1X* e selezionare infine nel riquadro "EAP Type" *Smart Card or other Certificate*.

Fig. 5.10 - Windows XP, abilitazione di EAP

Solamente con Windows XP é possibile configurare la generazione della chiave WEP per sessione (EAPOL-Key), qualora l'Access Point lo supportasse. Per effettuare la configurazione, sempre dalle proprietà della *Wireless Network Connection*:

- Selezionare la sezione *Wireless Networks*
- Selezionare la rete in cui abilitare EAPOL-Key nel riquadro *Available Networks* e premere *Configure*

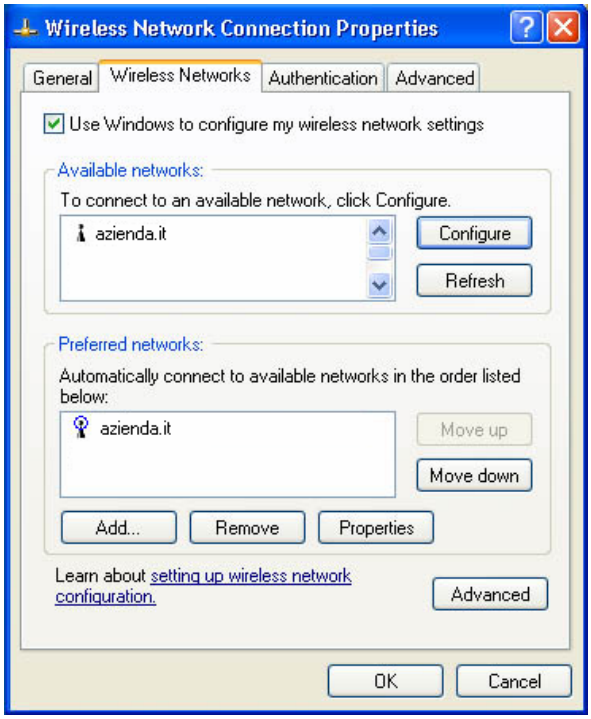

Fig. 5.11 - Windows XP, configurazione della rete wireless

- Selezionare l'opzione *Data encryption (WEP enabled)*
- Selezionare *The key is provided for me automatically*

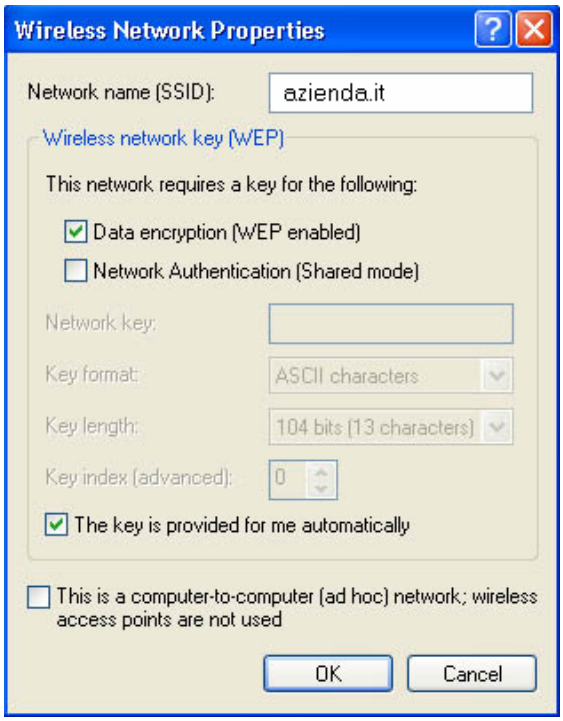

Fig. 5.12 - Windows XP, ricezione delle chiavi WEP dinamiche

Esempio con Windows 95/98/ME

La famiglia Windows 95/98/ME non dispone di un client nativo IEEE 802.1x. Uno dei client più popolari é *AEGIS Client* della società Meetinghouse Data Communication (MDC), disponibile anche per Linux e presto per MacOS X. Anche in questo caso é necessario che l'amministratore di sistema abbia installato prima i certificati all'interno di Windows.

Al primo avvio dopo l'installazione il software riconoscerà il primo avvio del client e proporrà di effettuare la configurazione.

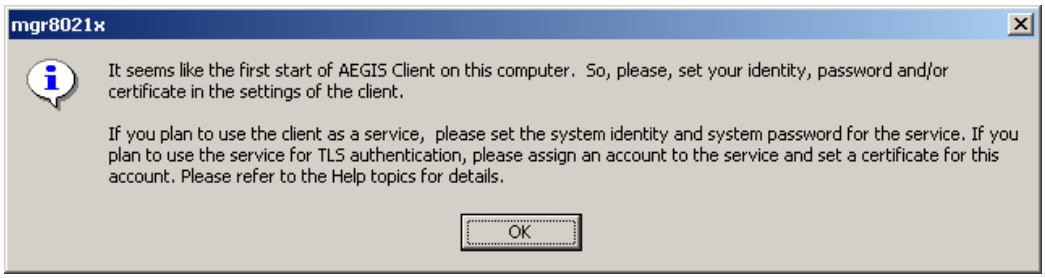

Fig. 5.13 - Primo avvio di AEGIS Client

Dopo aver premuto su *Ok*, una finestra di dialogo verrà presentata, consentendo l'immissione della configurazione utente (sezione *User settings)*.

- Selezionare in *Authentication type* il valore *TLS/Smart Card*
- Premere il pulsante *Change* nel riquadro *Client Certificate.*
- Verrà presentata una finestra *Select Certificate* che permette di selezionare il certificato dell'utente. Selezionare il certificato tra quelli disponibili e premere *Ok*
- Automaticamente il campo *Identity* verrà riempito con il nome del proprietario del certificato.

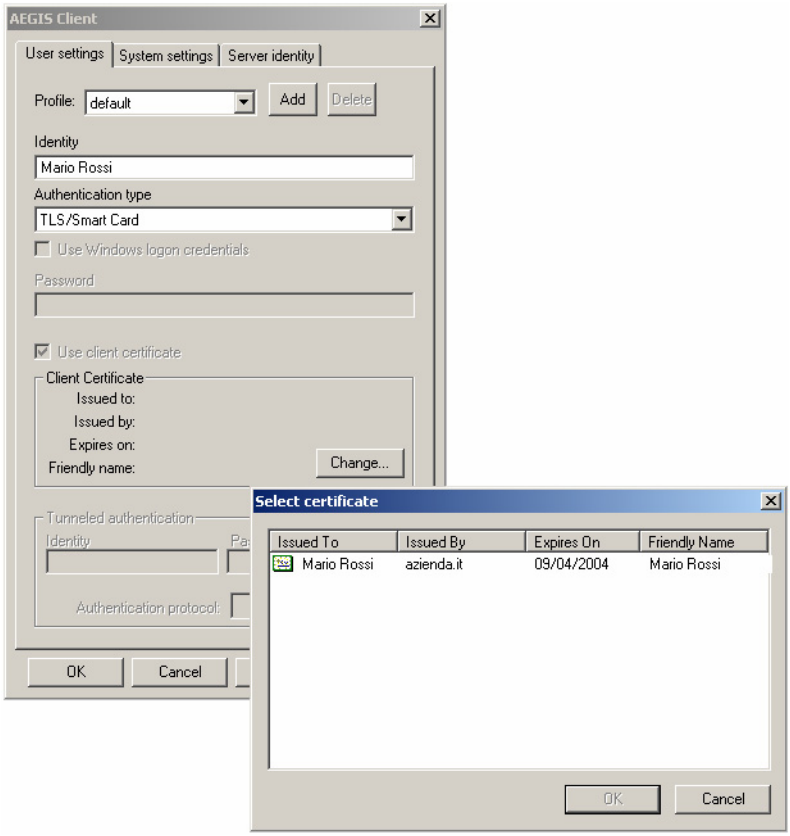

Fig. 5.14 - AEGIS Client, configurazione utente e certificato

- Selezionare successivamente la sezione *Server Identity*
- Nel riquadro *Certificate issuer must be*, selezionare la Certification Authority che ha rilasciato il certificato
- Nel riquadro *Server name must be* é suggeribile inserire solo il nome del dominio, ad esempio "azienda.it", anziché il nome completo del server. Questo é utile in caso si abbia più di un server RADIUS, ad esempio per una ragione di ridondaza. Selezionare anche *Domain name must end in specified name* e premere *Ok*.

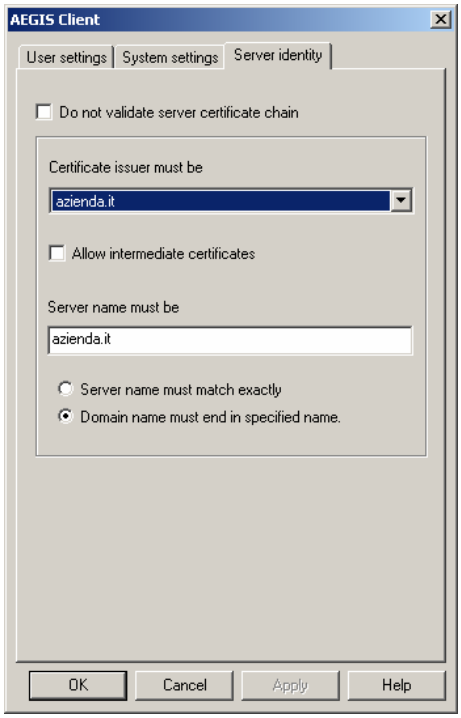

Fig. 5.15 - AEGIS Client, validazione del server

Per visualizzare lo stato del client, fare doppo click con il mouse sull'apposita icona del SysTray. Nella finestra di dialogo proposta sarà possibile visualizzare la scheda Wireless, lo stato dell'autenticazione IEEE 802.1x ed alte informazioni sulla rete Wireless quali il MAC address dell'Access Point a cui si é collegati.

Esempio con Linux

Il client più utilizzato per Linux é *xsupplicant*, un progetto di Open1X che ha come scopo fornire tools OpenSource per il protocollo IEEE 802.1x. É possibile scaricare l'ultima versione del client sul sito internet http://www.open1x.org, che ha come requisiti i pacchetti software OpenSSL 0.9.7, libpcap 0.7.1 e libdnet 1.6. Si faccia riferimento al file *README* incluso con xsupplicant per maggiori informazioni su come reperire i pacchetti software requisiti. Dopo aver decompresso il file di xsupplicant, entrare nella directory ed eseguire i comandi:

```
./configure
make
make install
```

I comandi elencati provvederanno ad autoconfigurare le dipendenze e le capacità del programma, a compilarlo ed installarlo. É necessario possedere i certificati X.509 nei seguenti formati:

Tipo di certificato	Formato
Pubblico dell'utente	DER
Privato dell'utente	PEM
Pubblico della CA	PEM

É possibile che il certificato pubblico/privato dell'utente sia distribuito in formato PKCS#12. I produttori di *xsupplicant* hanno messo a disposizione uno script chiamato *pkcs12toDERandPEM.sh* in grado di effettuare le opportune conversioni. Per configurare il programma é necessario agire sul file di configurazione */etc/1x/1x.conf.* In questo file é possibile specificare come il programma debba agire su reti differenti specificando un *network id*, il quale corrisponde in ambito wireless al valore dell'ESSID. Tale valore é espresso in ogni riga del file di configurazione prima del carattere ":". Nell'esempio sottostante si specifica un *network id* chiamato "myssid".

```
##################################################
## Collegamento alla rete Wireless
##################################################

## ID Utente
myssid:id = mrossi@azienda.it

## Certificato pubblico
myssid: cert = /etc/1x/certs/xsupplicant-public.cer

## Certificato privato
myssid: key = /etc/1x/certs/xsupplicant-private.pem

## Certificato della CA
myssid:root = /etc/1x/certs/CA.pem

## Autenticazione EAP
myssid:auth = EAP

## Dopo aver autenticato, prendi un IP da DHCP
myssid: first_auth = "/sbin/dhclient eth0"

## Messaggio utente
myssid: after_auth = "/bin/echo Autenticato alla rete"
```

Dopo aver effettuato la configurazione del programma xsupplicant, é sufficiente configurare l'ESSID corrispondente e eseguire il client come segue:

```
/sbin/iwconfig eth0 essid myssid
/sbin/ifconfig eth0 up
xsupplicant -i eth0
```

6. WI-FI PROTECTED ACCESS

Il protocollo Wi-Fi Protected Access (WPA) é uno sforzo dei produttori nel tentativo di colmare le lacune derivate da WEP. WPA é un sottoinsieme dello standard IEEE 802.11i; quest'ultimo chiamato anche WPA2 verrà rilasciato nel corso dell'anno 2004 e sarà pienamente compatibile con WPA. I produttori hanno disegnato questo protocollo per minimizzare l'impatto sulle performance e per permettere la sua distribuzione attraverso un aggiornamento software dei prodotti basati su IEEE 802.11b, come ad esempio Access Points e schede di rete. Alcuni produttori di hardware hanno ideato dei sistemi che permettono il "mixed mode", ovvero la possibilità di supportare contemporaneamente WPA e WEP per facilitare la migrazione a questo nuovo protocollo.

Il WPA richiede che un client si autentichi per accedere alla rete, sia esso attraverso un *Pre-Shared Key* (utenti SOHO) che attraverso *IEEE 802.1x/EAP*, e introduce un framework di crittografia per la confidenzialità dei dati che si appoggia ad algoritmi quali WEP, TKIP e AES. Il WEP usato in WPA ha un impatto minore rispetto al WEP tradizionale, in quanto le chiavi verranno cambiate in modo differente. Anche se WEP é supportato, WPA usa di default il *Temporary Key Integrity Protocol* (TKIP) per crittografare i dati, aumentando la chiave dai 104-bit di WEP, fino a 128-bit. Contrariamente a WEP, dove le chiavi venivano impostate staticamente, in TKIP vengono generate dinamicamente e distribuite attraverso il protocollo 802.1x/EAP. Inoltre TKIP include un *Message Integrity Check* (MIC) che permette di evitare le alterazioni dei pacchetti trasmessi attraverso la rete wireless. Il MIC viene calcolato separatamente dal client e dall'Access Point e se risultasse differente il pacchetto verrebbe scartato.

Il TKIP aumenta la difficoltà di decriptare i dati su una rete wireless: specialisti crittografi infatti hanno analizzato il Wi-Fi Protected Access e hanno affermato che i problemi legati al WEP sono stati risolti facendo di WPA un ottimo deterrente contro attacchi conosciuti.

La tabella successiva paragona le differenze tra WPA e WEP:

Protocollo	**WEP**	**WPA**
Crittografia	• Crittografia debole • Chiave a 40-bit o 104-bit • Chiavi statiche: tutti i client sulla rete hanno la stessa chiave • Distribuzione manuale della chiave	• Rimuove i problemi di WEP • Chiave a 128-bit • Chiavi dinamiche: ogni utente, ogni sessione e ogni pacchetto ha chiave differfente • Distribuzione automatica delle chiavi
Autenticazione	Debole: la chiave WEP viene usata come autenticazione	Attraverso IEEE 802.1x e EAP

WPA in dettaglio

Nel paragrafo precedente si é sottolineato quanto la vera forza di WPA stà nella sua forte integrazione con IEEE 802.1x/EAP e in una crittografia migliore. In dettaglio le caratteristiche di WPA si possono dividere in cinque categorie: *Network Capability Determination*, *Authentication*, *Key Management*, *Data Privacy* e *Data Integrity*.

Network Capability Determination. Agisce a livello 802.11 e comunica informazioni su WPA nei Beacon Packets, Probe Response e (Re) Association Requests. Queste informazioni includono il metodo di autenticazione (IEEE 802.1x o Pre-Shared Key) e il tipo di cifratura (WEP, TKIP o AES).

Authentication. Le due tipologie di autenticazione sono 802.1x/EAP e Pre-Shared Key, nel caso non si disponga di un RADIUS server (tipico ambiente SOHO). É da notare che la prima metodologia é quella preferita da WPA in quanto é in grado di distribuire chiavi differenti per sessione attraverso i messaggi EAPOL-Key.

Key Management. WPA ha un robusto sistema di generazione/manutenzione di chiavi che integra funzioni di autenticazione e privacy. Le chiavi sono generate dopo che il client si é autenticato alla rete e dopo un *4-way handshake* tra il client e l'Access Point.

Data Privacy (o critografia). Come agente crittografico WPA usa il Temporary Key Integrity Protocol (TKIP) per incapsulare WEP. Attraverso sofisticate tecniche di crittografia é possibile evitare i problemi di WEP.

Data Integrity. TKIP include un Message Integrity Code (MIC) alla fine di ogni messaggio non criptato per evitare che i pacchetti vengano modificati da un potenziale aggressore.

Network Capability Determination

Come accennato nel paragrafo precedente, la funzionalità di *Network Capability Determination* si basa su una modifica del formato delle frames di *Beacon*, *Probe Response* e *(Re) Association Request* di IEEE 802.11. Queste frames vengono ridefinite nel protocollo WPA per includere le caratteristiche della rete, ovvero per specificare la tipologia di autenticazione e di cifratura disponibile. I possibili metodi di autenticazione sono 802.1x e il Pre-Shared Key (PSK). Quest'ultimo metodo usa una chiave statica impostata manualmente, sia sui client che sugli Access Point, ed é l'ideale per coloro i quali non hanno un RADIUS server, ad esempio per utenze domestiche o per piccoli ambienti di lavoro. I possibili sistemi di cifratura sono WEP, TKIP e Advanced Encryption Standard (AES). Il client equipaggiato dell'apposito software (chiamato *supplicant*) usa le informazioni date dalla rete WPA per decidere quale metodo di autenticazione e cifratura scegliere. Per esempio, se l'Access Point usa il metodo PSK, allora il supplicant non userà 802.1x, ma sarà sufficiente provare all'AP di essere in possesso del PSK comune. Se il supplicant si accorge che non é in grado di supportare le metodologie offerte deve usare l'autenticazione 802.1x senza WPA per accedere alla rete: questo processo é detto *pre-WPA authentication*.

IEEE 802.1x é la metodologia di autenticazione preferita di WPA, in quanto é proprio grazie a questo protocollo che si ha la migliore resa di autenticazione e cifratura. WPA però necessita che il metodo EAP selezionato dall'amministratore supporti la *mutual authentication*, ad esempio TLS, TTLS, LEAP e PEAP. Durante il processo di autenticazione un *Pairwise Master Key* (PMK) viene generato sia sulla stazione che sul RADIUS server. Quest'ultimo manderà il PMK all'Access Point in maniera sicura. Questo processo é simile a quello della pre-WPA authentication, ma la differenza stà nel fatto che il *PMK* non é mai usato direttamente nelle funzioni di cifratura o di hash, ma viene usato per generare chiavi temporanee che verranno usate in queste funzioni. L'uso di chiavi temporanee é utile al fine di evitare attacchi alla chiave, come succede con WEP dove la chiave viene derivata dall'osservazione dei pacchetti in transito.

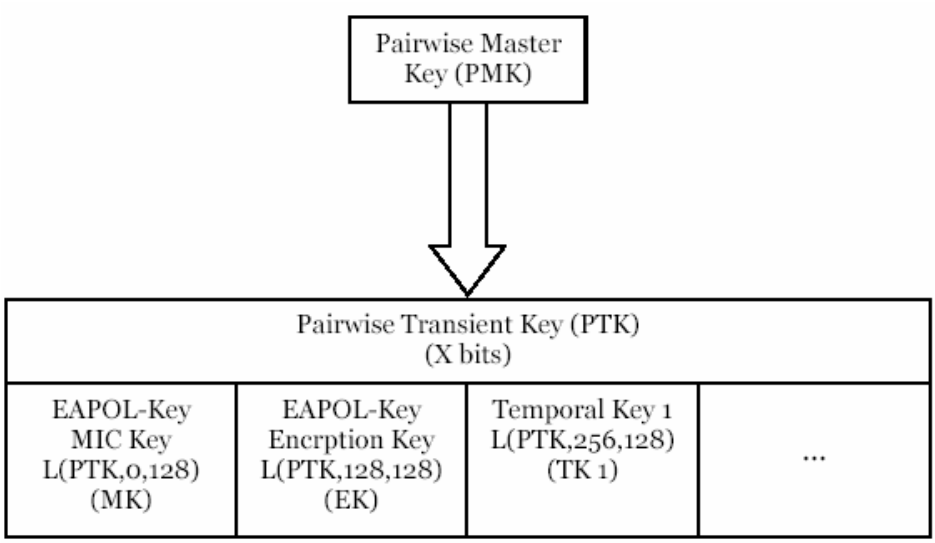

Fig. 6.1 – Uso del PMK per generare le chiavi TKIP

Le modifiche a 802.1x

Le maggiori modifiche apportate a IEEE 802.1x da parte del WPA sono relative al formato di EAPOL-key. Questo non significa che il processo di autenticazione 802.1x venga stravolto, ma vengono apportate modifiche alla distribuzione delle chiavi WPA che avvengono solamente dopo che un client si sia autenticato correttamente alla rete. Il processo dello scambio delle chiavi viene chiamato *4-way and Group Key Handshake.* Il 4-way handshake determina il PMK usato per il traffico unicast, mentre il Group Key handshake determina e distribuisce il PMK usato per il traffico di broadcast. Il processo di creazione delle chiavi é stato struttruato per evitare attacchi di tipo *man in the middle*, in dettaglio:

1. Gli indirizzi dell'Access Point e del client vengono usate in ogni calcolo del MIC durante il 4-way handshake. Questo restringe il processo di scambio di chiavi ad un determinato *authenticator* e *supplicant*.
2. Vengono usati gli *nonces* (valori usati una volta sola) durante il calcolo del MIC. Nuovi nonces vengono usati durante ogni 4-way handshake per generare le chiavi temporanee, congiuntamente al PMK.
3. Gli nonces assicurano che né il client né l'Access Point siano nella posizione di essere sotto attacchi di tipo replay. Ovvero, quando i nonces sono usati durante il processo di *key authentication*, il supplicant e l'authenticator devono essere in possesso del nuovo PMK dopo l'autenticazione, in modo da calcolare il valore corretto del MIC.

Un altro cambiamento é l'aggiunta del parametro *PortSecure*: quando questo valore é impostato, sia l'authenticator che il supplicant sanno che le chiavi per unicast e broadcast sono valide e pertanto possono essere programmate nel firmware della scheda di rete wireless, in modo da non sovraccaricare il

processore principale per la cirttografia. Dopo la programmazione della scheda di rete, le successive autenticazioni IEEE 802.1x avvengono in maniera cifrata. Prima dell'avvento di WPA, ogni autenticazione 802.1x avveniva in chiaro con l'effetto di essere soggetti ad attacchi di tipo *EAPOL Logoff messages*, con il risultato che il client veniva disconnesso dall'Access Point. Una volta che la scheda wireless ha le chiavi di crittografia inserite, tale tipologia di attacco non é più possibile.

Inoltre WPA definisce anche una frame di tipo *EAPOL MIC error*. Questo pacchetto permette al client di informare l'Access Point quando é soggetto ad un attacco. Questo pacchetto é inviato all'AP quando il client ha un errore durante a comparazione del MIC nei dati in transito. Quando il client riceve frequentemente pacchetti con errori, allora desume di essere sotto attacco e apposite contromisure vengono prese dall'Access Point, ad esempio attraverso la notifica ad un amministratore.

Crittografia

Nei paragrafi precedenti si é accennato che il metodo di cifratura preferito da WPA é TKIP. Il Temporary Key Integrity Protocol usa l'algoritmo RC4, lo stesso usato da WEP, ma ne aggiunge tecniche di protezione per evitare i problemi derivati da WEP. Ad esempio, viene aggiunto una funzione di cambio di chiavi ad ogni pacchetto un vettore di inizializzazione (IV) più lungo e un Message Integrity Code (MIC). La funzione di cambio di chiavi per ogni pacchetto (detta originariamente *key mixing*) viene usata nel TKIP per evitare gli attacchi su chiavi deboli. Durante la generazione del testo cifrato, la chiave di crittografia non é mai usata direttamente nella funzione RC4, ma viene usata una chiave temporanea per ogni pacchetto spedito. Per ovviare invece all'osservazione dei pacchetti con IV identico, TKIP aumenta la grandezza di IV da 24 a 48 bit. La funzione di hash usata per verificare l'integrità dei dati é detta Message Integrity Code (MIC o per gli addetti *Michael*), e la sua funzione é quella di verificare che i pacchetti non siano stati modificati da un client non autorizzato che finge di essere il legittimo client.

Oltre al TKIP, WPA supporta anche l'AES come metodo di cifratura, anche se inizialmente non é obbligatorio per la certificazione del consorzio Wi-Fi Alliance. Anche se AES é nettamente migliore rispetto a TKIP, esso necessita di nuovo hardware che lo supporti. TKIP invece é un buon compromesso che permette di avere una maggiore sicurezza rispetto a WEP, mentre i prodotti che supportano AES verranno immessi sul mercato e adottati dagli utenti.

I problemi di WPA

Anche il WPA non é senza problemi. Nel dettaglio, é soggetto ad attacchi di tipo Denial of Service (DoS); se l'Access Point riceve due pacchetti dati che falliscano la verifica del MIC entro 60 secondi, questo desume di essere sotto attacco e impiega contromisure come la disconnessione di tutti i client dall'Access Point. Questo fa sì che un intruso non possa risalire alle chiavi di crittografia, ma causa anche una perdita di connettività per 60 secondi.

Anche se WPA non é completamente invulnerabile, esso rappresenta la volontà dei produttori a risolvere i problemi delle tecnologie del Wireless. WPA con le opportune regole di base é un netto miglioramento della sicurezza rispetto al suo predecessore WEP.

7. IPSEC

Nel Giugno del 1994 la Internet Architecture Board (IAB) ha espresso, attraverso un documento (RFC 1636), la necessità di una migliore sicurezza in Internet, in particolare ha espresso la necessità di colmare le lacune del protocollo TCP/IP. Prendendo spunto da tale documento, sono state studiate e sviluppate delle tecnologie per rendere la comunicazione tra varie aziende sicura su un canale non sicuro quale Internet. Queste tecnologie sono meglio conosciute come Virtual Private Network o più semplicemente VPN.

L'IP Security Protocol, conosciuto come IPSec, è oggi la tecnologia più diffusa per lo scambio sicuro di dati tra aziende, o più comunemente fra due computer. IPSec è stato definito dall'Internet Engineering Task Force già dall'Agosto 1995 attraverso l'RFC 1825: sono passati otto anni da allora e IPSec è cresciuto notevolmente, affermandosi nel mercato come lo standard per la VPN, e fornendo al TCP/IP le funzionalità di autenticazione, integrità e crittografia di cui era sprovvisto. Uno dei fattori che ne hanno determinato la sua affermazione è che IPSec può essere inoltrato attraverso qualsiasi rete che supporta il protocollo IP, senza dover cambiare nessun nodo di rete, senza cambiare le applicazioni e senza cambiare in maniera sostanziale il sistema operativo dei nodi.

IPSec può operare in due modalità: *tunnel mode* e *transport mode*. La prima incapsula un intero datagramma IP al suo interno, rendendola ideale per l'uso con le VPN o per trasportare IP privati all'interno di IP pubblici, ad esempio per collegare una sede remota. La seconda invece incapsula solamente il protocollo TCP o UDP, rendendo sicura la sola comunicazione applicativa tra due nodi della rete Internet, ad esempio la comunicazione tra un web server e un database server.

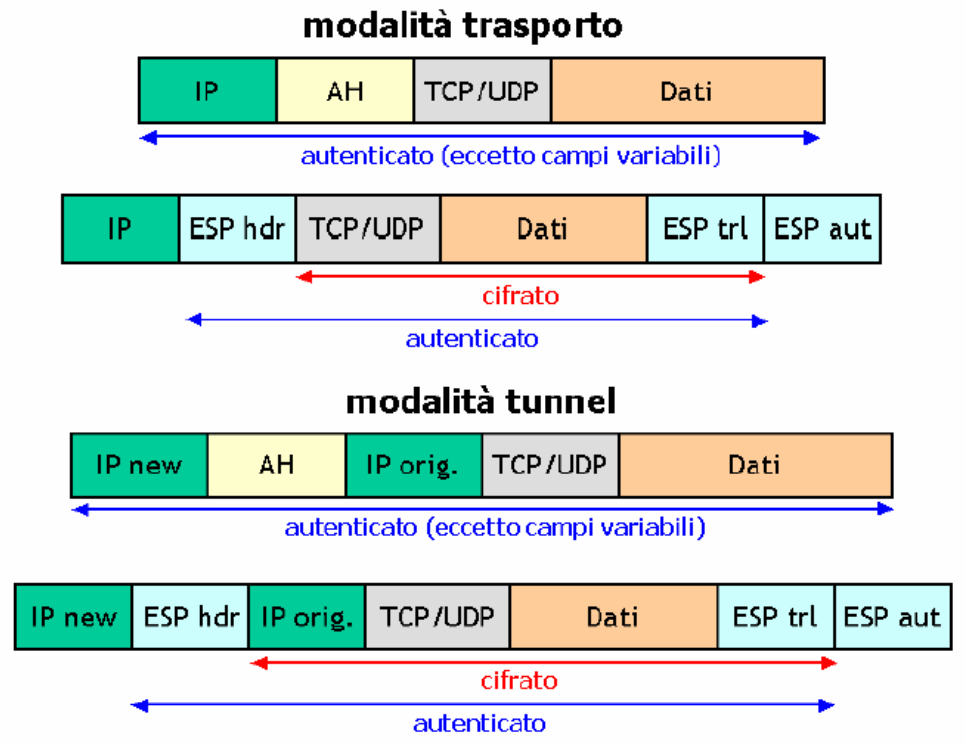

Fig. 7.1 - IPSec in modalità trasporto e modalità tunnel

Molti firewall e router hanno la funzionalità di IPSec Tunnel Mode per stabilire delle VPN, siano esse sedi remote, extranet o più semplicemente degli utenti interni collegati attraverso Internet. Come abbiamo sottolineato in precedenza, data la mancanza di un sistema sicuro di autenticazione e crittografia, le Wireless LAN sono da considerare *untrusted*, pertanto non differenti dalla rete Internet. In un ambiente quale quello aziendale, dove la sicurezza dei dati è molto importante, le Wireless LAN trovano un naturale complemento nella tecnologia IPSec. È da considerare che, se si dispone di una VPN per l'accesso tramite Internet, l'utente finale si troverà a suo agio attraverso l'uso di strumenti che già conosce. È consigliabile in questo scenario collegare gli Access Points a una rete demilitarizzata (DMZ) che sia riconducibile ad un firewall o ad un router di accesso, ad esempio quello collegato alla rete Internet.

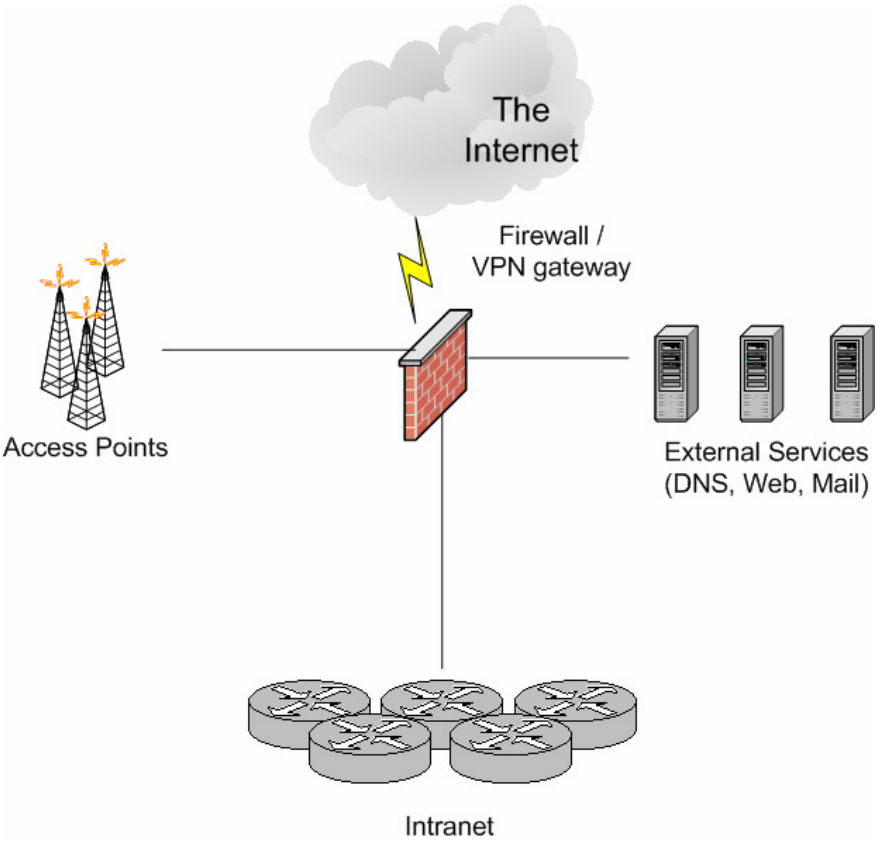

Fig. 7.2 - Esempio di architettura con IPSec

IPSec e lo scambio delle chiavi

La struttura di IPsec e` piuttosto complessa in quanto IPsec non e` un singolo protocollo, ma piuttosto un'architettura di sicurezza a livello IP composta da vari protocolli e da altri elementi. I protocolli principali che costituiscono IPsec sono tre:

- *AH* (Authentication Header) che fornisce servizi di autenticazione e integrità.
- *ESP* (Encapsulating Security Payload) che fornisce servizi di riservatezza, autenticazione e integrità.
- *IKE* (Internet Key Exchange) che gestisce lo scambio delle chiavi.

AH ed ESP non si preoccupano dello scambio delle chiavi e presumono che i due interlocutori si siano già accordati creando tra loro una Security Association (SA), ovvero una configurazione che specifica quali meccanismi di sicurezza utilizzare e con quali chiavi. Il compito di negoziare e gestire le Security Association secondo delle politiche definite localmente e` affidato a IKE.

La SA è un concetto fondamentale nell'ambito di IPSec in quanto specifica quali meccanismi di sicurezza, quali algoritmi e quali chiavi vengono utilizzati per proteggere il traffico TCP/IP. Tutte le Security Association attive sono contenute in un database detto Security Association Database (SAD), mentre esiste un altro database detto Security Policy Database (SPD) che contiene le politiche di sicurezza. Tramite esse il sistema decide se un pacchetto IP debba essere scartato, lasciato passare in chiaro oppure elaborato tramite IPsec, basandosi su parametri come l'indirizzo IP sorgente o destinazione, la porta sorgente o destinazione, il protocollo di trasporto.

Inizialmente le SA venivano generate e scambiate manualmente, ma la loro gestione è impraticabile su contesti più ampi, quali ad esempio quello di VPN gateway. Si è reso necessario pertanto l'uso di un meccanismo automatico per le gestioni delle chiavi... il protocollo IKE (Internet Key Exchange) è nato per questo scopo. IKE e` un protocollo ibrido, che integra ISAKMP (Internet Security Association and Key Management Protocol) e Oakley. Questi ultimi definiscono metodi differenti per stabilire una scambio di chiavi tra sistemi. Oakley definisce modi per costruire un percorso di relazioni sicure, mentre ISAKMP definisce le stesse fasi in modo gerarchico. Entrambi si riconducono in due fasi distinte di IKE: nella prima i due nodi creano una security association per IKE stesso (detta ISAKMP SA13), ovvero un canale sicuro da utilizzare per i messaggi di IKE, nella seconda fase utilizzano la ISAKMP SA per negoziare security association per altri protocolli. Esistono quattro metodologie più usate per l'autenticazione e lo scambio di chiavi attraverso IKE, ovvero:

- *Shared Secret,* dove entrambi i sistemi conoscono una password comune
- *Public/Private Key*, ovvero tramite chiavi asimmetriche pubbliche e private, ad esempio il PGP
- *Digital Certificates*, simile a Public/Private Key ma con chiavi aderenti allo standard X.509, ovvero esiste una verifica dell'utente o del sistema remoto tramite una Certification Authority (CA)
- *XAUT*, ovvero un estensione proprietaria di autenticazione. Alcuni vendor, quali Cisco e CheckPoint, includono questa funzionalità per autenticare un utente attraverso Username e Password. Si noti che questo è differente dallo Shared Secret che invece è legato ad una macchina e non ad un utente.

È consigliabile usare XAUT e i Certificati Digitali per autenticare un utente, mentre uno Shared Secret o Certificato Digitale è più adatto per autenticare due sistemi.

Protezione del client

Differentemente dal protocollo PPPoE, dove il client non aveva un IP address direttamente collegato alla scheda di rete, il protocollo IPSec viaggia su una rete IP esistente, per cui il client ha un IP address collegato alla scheda di rete Wireless. Come è stato menzionato nel primo capitolo, anche il client può essere il destinatario di un attacco da parte di un intruso, sia per "carpire" informazioni preziose che per essere usato come "ponte" per entrare nella rete privata. Per prevenire questo tipo di attacchi è consigliabile installare sui client un Personal Firewall e un Antivirus, ormai disponibili da diversi vendor e per diversi sistemi

operativi. Come per un firewall tradizionale, il Personal Firewall è in grado di monitorare il traffico IP in ingresso sul client, proteggendolo da eventuali attacchi quali i tentativi di accesso a backdoors (Back Orifice, Netbus, ecc...).

Un'altro passo per la protezione dei client basati su Windows è quello di limitare l'uso del registry per evitare la lettura remota. Dal programma *regedt32* è possibile posizionarsi sulle chiavi di registro di interesse e, con il tasto destro sulla cartella interessata si possono selezionare le autorizzazioni da concedere. Un'altra tecnica è quella di posizionare il file di registro di sistema in una partizione NTFS e limitare l'accesso alla directory tramite l'autorizzazione della directory dei files.

VPN Gateway

Come descritto in precedenza, è bene confinare gli Access Point in una rete separata non di fiducia (*untrusted*), e collegare questa rete alla rete Intranet attraverso un VPN gateway. La funzionalità di VPN server è presente in molti firewall e router, pertanto la realizzazione di questa topologia risulta semplificata qualora si disponga di tali apparecchiature. In particolare la rete wireless trova la sua naturale collocazione in una DMZ del firewall perimetrale di accesso a Internet, in quanto la pericolosità delle wireless LAN può essere paragonata alla stessa Internet. È possibile realizzare differenti tipologie di configurazioni e con diversi prodotti/programmi che supportano lo standard IPSec. A titolo di esempio nei prossimi paragrafi verrano presentati alcuni esempi di configurazione di VPN gateway, quali CheckPoint FW-1 e Cisco IOS, attraverso la metodologia di scambio di chiavi con certificati digitali X.509.

Esempio di VPN gateway con CheckPoint FW-1 NG

Per poter utilizzare CheckPoint FW-1 in modalità VPN gateway è necessario installare il modulo VPN-1 e acquistare la relativa licenza. Per abilitare tale opzione è necessario aprire le proprietà del Gateway CheckPoint e abilitare l'opzione *VPN-1 Pro* presente nelle *General Properties*, sezione *CheckPoint Products*. I seguenti passi sono stati realizzati con la versione VPN-1 NG Feature Pack 2. Si assume che CheckPoint FW-1 NG sia stato già installato sul firewall e che l'utente abbia familiarità con il prodotto e la sua GUI.

Preparazione della Certification Authority

Questo esempio è realizzato usando i certificati digitali X.509 come autenticazione del client. In CheckPoint VPN-1 è possibile sfruttare una Certification Authority esterna, qualora si disponga di una infrastruttura PKI, definendo un nuovo server di tipo *CA – OPSEC PKI*, importandone il certificato pubblico e definendo la modalità di accesso al Certificate Revocation List (CRL). Qualora non si avesse a disposizione una infrastruttura PKI esistente è possibile definire una Internal Certificate Autority (ICA) creando un nuovo server di tipo *CA – Local Management Server*. Per maggiori informazioni su come gestire in maniera approfondita le Certification Authority, si faccia riferimento al manuale *CheckPoint Virtual Private Networks* al capitolo Certification Authorities.

Definizione degli utenti

Un altro passo importante prima di configurare la VPN vera e propria è quello di configurare gli utenti che hanno accesso alla stessa. È pertanto necessario configurare in FW-1 un nuovo utente, e definire le seguenti proprietà:

- Nella sezione *Encryption* selezionare *IKE* e successivamente il pulsante *EDIT*

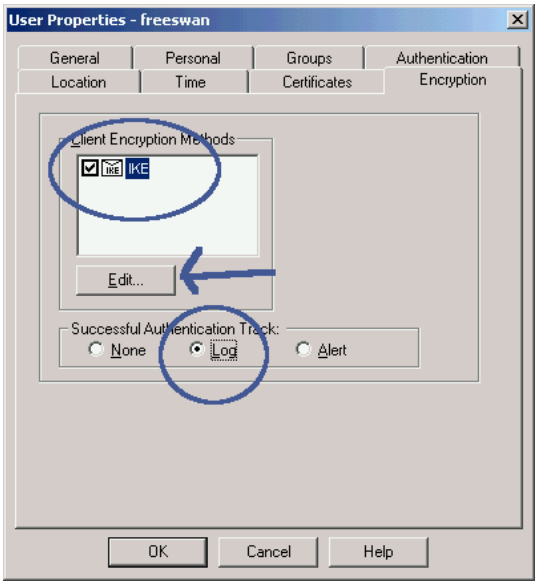

Fig. 7.3 - CheckPoint, propietà di encryption dell'utente

- Nella sezione *Authentication* selezionare *Public Key*

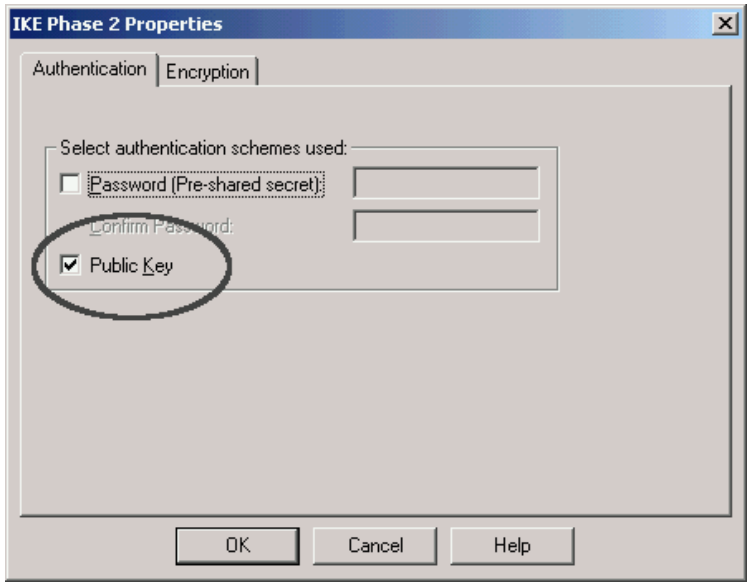

Fig. 7.4 - CheckPoint, uso della chiave pubblica in IKE per l'utente

- Nella sezione *Encryption* selezionare la checkbox *Defined Below,* in *Encryption Algorithm* selezionare *3DES* e in *Data Integrity* selezionare *MD5* e premere OK

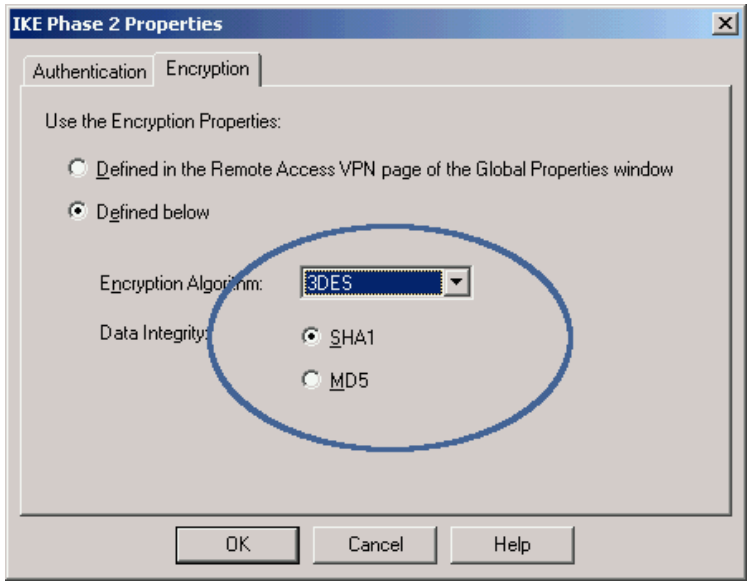

Fig. 7.5 – CheckPoint, uso dell'algoritmo di cifratura

- Premere *Generate and Save* per generare una nuova richiesta alla CA.

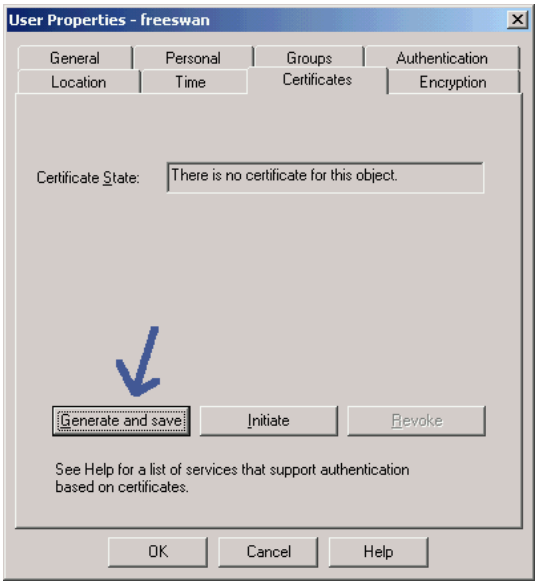

Fig. 7.6 - CheckPoint, generazione della chiave X.509 utente

Configurazione del modulo VPN

In questa fase si procede a configurare il modulo VPN su CheckPoint FW-1. A tale scopo nelle proprietà del gateway è necessario:

- Abilitare il modulo *VPN-1 Pro* nelle *General Properties*

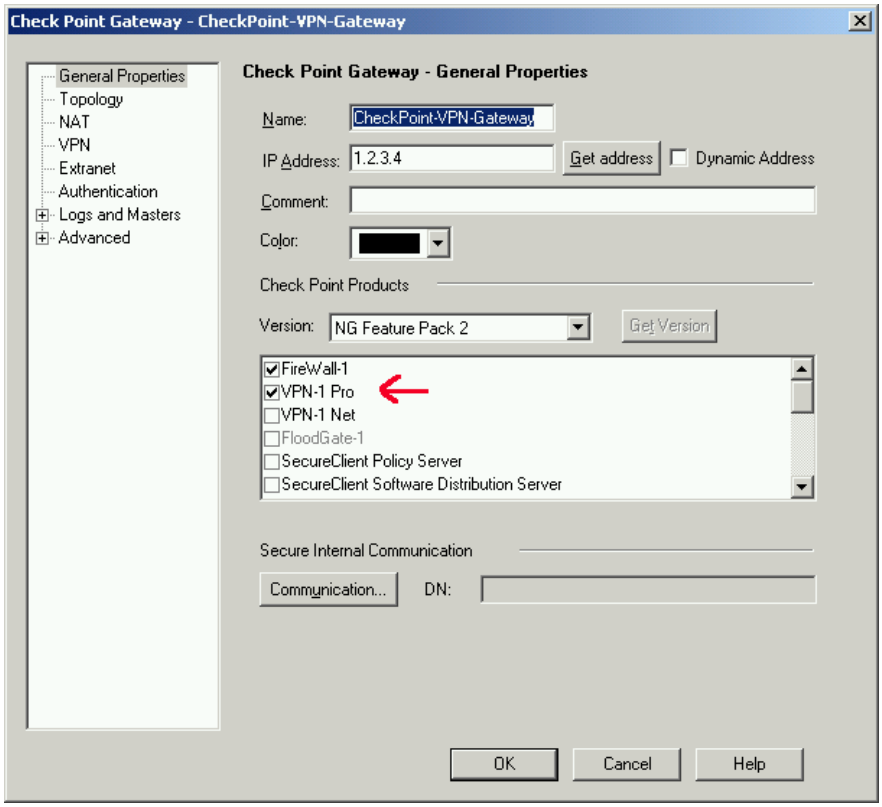

Fig. 7.7 - CheckPoint, abilitazione modulo VPN

- Nelle *Topology* definire manualmente l'oggetto che rappresenta la/e rete/i interna/e e abilitare l'opzione *Exportable for SecuRemote/SecureClient*

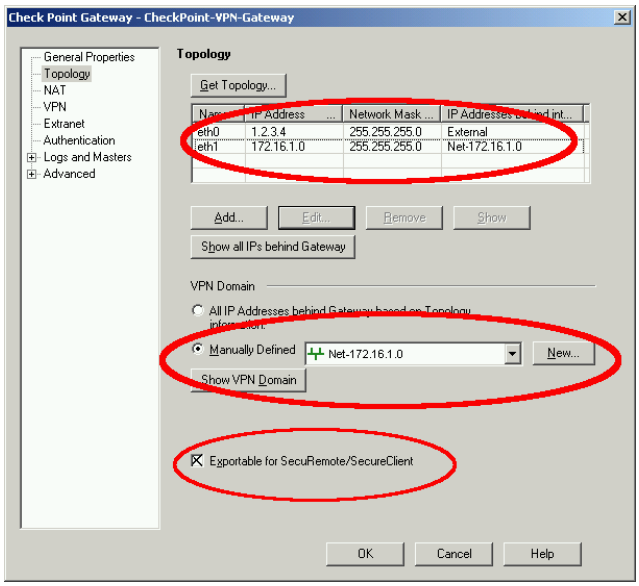

Fig. 7.8 - CheckPoint, definizione delle interfaccie di rete e della rete interna

- In *VPN*, selezionare *IKE* e successivamente premere *EDIT*

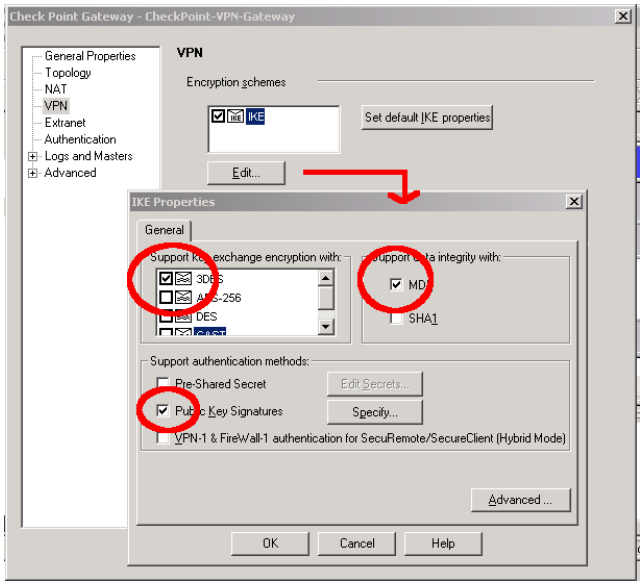

Fig. 7.9 - CheckPoint, configurazione algoritmo di cifiratura e di integrità

- Selezionare gli algoritmi di crittografia preferiti, ad esempio *3DES* e *AES-256*, selezionare come *Data Integrity* sia *MD5* che *SHA-1* e selezionare *Public Key Signatures*

È necessario successivamente selezionare il pannello delle *Global Properties* di CheckPoint, selezionare *VPN-1 Pro* e abilitare il *Traditional Mode*.

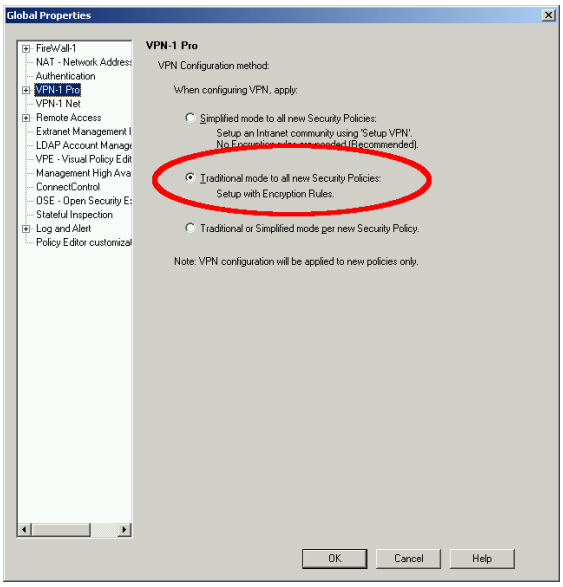

Fig. 7.10 - CheckPoint, selezione del Traditional Mode

Impostazione della VPN

L'ultima operazione da effettuare è quella dell'impostazione della regola di accesso VPN, aprendo la GUI sulle regole e definendo come sorgente gli utenti abilitati alla VPN, come destinazione la LAN interna, come servizio *Any* e come azione *Client Encrypt*. Con l'installazione di tale regola si è completata la configurazione della VPN su CheckPoint FW-1.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
1	All Users@Any	CheckPoint Net-172.16.1.0	* Any	Client Encrypt	Log	* Policy Targets

Fig. 7.10 - CheckPoint, definizione della policy VPN

Esempio di VPN gateway con Cisco IOS

Come per l'esempio di CheckPoint FW-1, questo descrive la configurazione di un gateway VPN usando i certificati digitali X.509. I router Cisco non dispongono di una Certification Authority, ma devono appoggiarsi su una CA esterna che supporti il protocollo Simple Certificate Enrollment Protocol (SCEP), come ad esempio Windows 2000, Entrust, VeriSign e OpenCA. Per supportare il servizio di VPN server, è necessario avere una versione di IOS 1.2.(8)T o superiore.

Enrollment del certificato

Il router deve scaricare il certificato digitale nella sua configurazione per permettere l'autenticazione del client. A tale scopo è necessario effettuare il processo di "Enrollment" come nell'esempio seguente

```
gw(config)#ip domain-name azienda.it
gw(config)#crypto key generate rsa
The name for the keys will be: gw.azienda.it
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

gw(config)#crypto ca trustpoint MYPKI
gw(ca-trustpoint)#enrollment url http://192.168.1.1
gw(ca-trustpoint)#enrollment mode ra
gw(ca-trustpoint)#crl query ldap://192.168.1.1
gw(ca-trustpoint)#serial-number none
gw(ca-trustpoint)#ip-address none
gw(ca-trustpoint)#password revokeme
gw(ca-trustpoint)#auto-enroll
gw(ca-trustpoint)#usage ike

gw(config)#crypto ca authen MYPKI
Certificate has the following attributes:
Fingerprint: 0D8E6CF8 C63D7068 3BA4B90A 16054812
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
gw(config)#

gw(config)#crypto ca enroll MYPKI
%
% Start certificate enrollment ..
% The subject name in the certificate will be: gw.azienda.it
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show
% the fingerprint.
```

```
gw(config)#    Fingerprint:  D9CE886E B4B76115 B7149128 6658E7CA
```

È necessario sostituire *gw.azienda.it* con il FQDN del gatway VPN, sostituire l'*enrollment url* e il *crl query* con quanto specificato dalla CA o dal suo amministratore qualora fosse interno all'azienda.

Configurazione della VPN

Quando il router ha scaricato il suo certificato è possibile procedere con la configurazione vera e propria della VPN. Di seguito viene fornito un esempio completo di configurazione:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname gw
!
aaa new-model
aaa authentication login ClientAuth local
aaa authorization network ClientAuth local
aaa session-id common
enable secret 5 $1$v49A$bfcGOf247dKQqZxCIN770
!
username vpnclient password 0 utente123
ip subnet-zero
!
ip domain-name azienda.it
!
crypto ca trustpoint MYPKI
enrollment mode ra
enrollment url http://192.168.1.1:80
usage ike
serial-number none
ip-address none
password 7 3305171D030F2F7741
crl query ldap://192.168.1.1
auto-enroll
crypto ca certificate chain MYPKI
certificate ca 3C9CC54B
308202E4  3082024D  A0030201  0202043C  9CC54B30  0D06092A  864886F7
0D010105
[...]
72AE135E 3B48662D
quit
certificate ra-encrypt 3C9CC573
308202E1  3082024A  A0030201  0202043C  9CC57330  0D06092A  864886F7
0D010105
[...]
30922C78 E6
quit
certificate ra-sign 3C9CC574
30820310  30820279  A0030201  0202043C  9CC57430  0D06092A  864886F7
0D010105
[...]
203E19C6 125AC104 608E37DF 600F97B9 B4DCF0CE
```

```
quit
certificate 3C9CC602
308202C0  30820229  A0030201  0202043C  9CC60230  0D06092A  864886F7
0D010105
[....]
A7E53742 75E1E403
quit
!
crypto isakmp policy 1
group 2
!
crypto isakmp identity hostname
crypto isakmp client configuration group People
dns 192.168.1.2
wins 192.168.1.2
domain azienda.it
pool VPN_POOL
acl 101
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map vpnclient 10
set transform-set myset
!
crypto map vpn client authentication list ClientAuth
crypto map vpn isakmp authorization list ClientAuth
crypto map vpn client configuration address respond
crypto map vpn 10 ipsec-isakmp dynamic vpnclient
!
interface Ethernet0/0
ip address 192.168.1.254 255.255.255.0
no keepalive
half-duplex
!
interface Ethernet0/1
ip address 10.1.1.1 255.255.255.240
half-duplex
crypto map vpn
!
ip local pool VPN_POOL 192.168.2.200 192.168.2.250
ip classless
no ip http server
ip pim bidir-enable
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
password cisco
!
end
```

È importante sottolineare alcuni passi della configurazione, in particolare nel parametro *crypto isakmp client configuration group People*, la stringa *People* rappresenta la Organizational Unit (OU) presente nel certificato del client. La configurazione *crypto ipsec transform-set myset esp-3des esp-md5-hmac* definisce invece i parametri di crittografia per la comunicazione tra il gateway e il client.

Il client

IPSec si è affermato come lo standard per la protezione dei dati su TCP/IP ed è presente nella maggioranza dei moderni sistemi operativi, seppur supportando diversi standard crittografici e modalità di configurazione, a volte con estensioni proprietarie. Esistono anche client "all purposes" che sono in grado di coprire la maggioranza delle funzionalità presenti sul mercato, come ad esempio SSH Sentinel, oppure client che sono in grado di integrarsi in una infrastruttura di policy più ampia, per esempio SecuRemote/SecureClient di CheckPoint che scaricano le loro policy da un firewall. È importante capire quali client andranno a collegarsi al VPN server e quali standard sono in grado di supportare, così da configurare il VPN gateway usando le migliori tecnologie comuni. Ad esempio, Linux con FreeS/WAN è in grado di supportare sia la crittografia AES 256-bit che 3DES, mentre Windows 2000 usa sia DES che 3DES. In tale scenario, il VPN gateway dovrà essere impostato per usare l'algoritmo 3DES, essendo comune ad entrambi.

Nei successivi paragrafi verranno descritti degli esempi di IPSec client, in particolare SSH Sentinel e Linux FreeS/WAN. È da sottolineare che MacOS X 10.2, cui nome in codice è "Jaguar", è basato su tecnologia BSD e incorpora la stessa implementazione IPSec di FreeBSD. Per maggiori informazioni sull'implementazione IPSec dei BSD si faccia riferimento al sito http://www.kame.net/.

Esempio di client con SSH Sentinel

Uno dei client IPSec più popolari in Internet è SSH Sentinel per Windows, dovuto al suo uso gratuito per fini non commerciali. Per configurare il programma è necessario disporre del certificato X509 dell'utente in formato PKCS#12 o PEM e un certificato pubblico della Certification Authority se questa non è pubblicamente riconosciuta (ad esempio Verisign).

Configurazione dei certificati

Il primo passo è quello della configurazione della Certification Authority comune.

- Aprire il programma *Policy Editor* e selezionare la sezione *Key Management*
- Selezionare *Trusted Certificates,* evidenziare *Certification Authorities* e con il tasto destro del mouse selezionare *Import*
- Selezionare il file contenente il certificato pubblico della CA e premere *Yes* fino ad importazione avvenuta

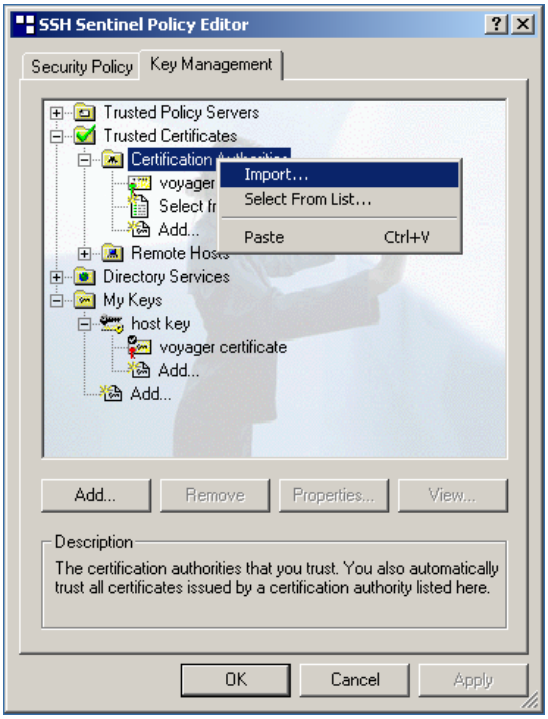

Fig. 7.11 - SSH Sentinel, importazione del certificato della CA

Poi è necessario importare il certificato dell'utente selezionando *My Keys,* con il tasto destro del mouse selezionando *Import* e selezionando il file del certificato. Durante l'importazione del certificato verrà chiesta la password per aprire il file con la chiave privata.

Configurazione della VPN

Per effettuare la configurazione della VPN è necessario selezionare la sezione *Security Policy*. È consigliabile creare una nuova policy, al fine di faciltitare la gestione utente, selezionando *New Policy Layer.* Nell'esempio successivo le connessioni ad altre reti non sono ammesse mentre è in uso la VPN, questo per proteggere il client da eventuali attacchi di intrusi mentre si è collegati attraverso la rete wireless. Per fare questo è necessario selezionare l'opzione *Deny Split Tunneling* nel pannello *Advanced* durante la definizione della VPN.

Per creare una VPN è necessario selezionare *VPN Connections* nella policy appena creata oppure su quella di Default, poi selezionare *Add* e specificare quanto segue.

- Security gateway: il nome o l'indirizzo IP del gateway VPN
- Remote network: any (0.0.0.0/0).
- Authentication key: La chiave privata o il certificato X.509
- Selezionare *legacy* quando si usa 3DES per la crittografia e normale quando si usa AES (Rijndael).
- Selezionare *Properties* per specificare altri parametri.
- Non selezionare *Aquire virtual IP address* qualora la rete wireless sia raggiungibile attraverso la rete interna. Selezionarla quando si desidera avere

un indirizzo IP virtuale.

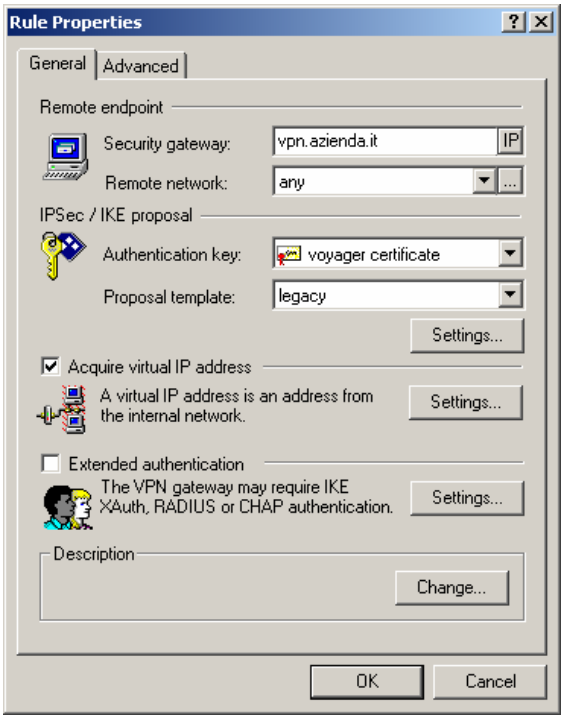

Fig. 7.12 – SSH Sentinel, configurazione della VPN

Esempio di client con Linux e FreeS/WAN

FreeS/WAN è il programma per Linux che si occupa di gestire IPSec. La sua installazione e configurazione è piuttosto complessa anche per i più esperti, in particolare se si tratta di usare congiuntamente la crittografia X.509 e il NAT Traversal. Molte distribuzioni Linux, quali Suse e Mandrake, includono anche il programma FreeS/WAN a cui pero' mancano le features di autenticazione a chiave digitale. É bene controllare nella propria distribuzione Linux se è presente FreeS/WAN con la patch per X.509. Qualora ne fosse sprovvisto, si consiglia l'ottimo sito http://www.freeswan.ca che distribuisce una versione di FreeS/WAN con le ultime patch disponibili, quali appunto l'estensione X.509, il NAT Traversal e l'algoritmo di crittografia AES. Per ricompilare il kernel di Linux con IPSec è necesario avere i sorgenti del kernel di Linux installati in */usr/src/linux*, successivamente entrare nella directory di freeswan e eseguire il comando *menugo*. Verrà presentata la usuale schermata dei parametri di configurazione del kernel: assicurarsi che all'interno di *Networking Support,* sia abilitato IPSec con i relativi moduli.

Certificati

È necessario avere un certificato X.509 in formato PEM o DER prima di procedere con la configurazione del client IPSec per Linux. Molte Certification Authorities sono solite rilasciare il certificato in formato PKCS#12, pertanto è necessario estrarre prima la chiave privata con il comando:

 # openssl pkcs12 -in freeswan.p12 -nocerts -out /etc/ipsec.d/private/freeswan-key.pem

e poi la chiave pubblica con:

 # openssl pkcs12 -in freeswan.p12 -nokeys -out /etc/ipsec.d/freeswan-pub.pem

È anche necessario includere il certificato pubblico della CA, sempre in formato PEM o DER, nella directory */etc/ipsec.d/cacerts*. Bisogna successivamente modificare il file */etc/ipsec.secrets* includendo il certificato privato appena generato, ad esempio inserendo la seguente linea:

: RSA /etc/ipsec.d/private/freeswan-key.pem "my password"

Dove "my password" è la password segreta che protegge la chiave privata.

File di configurazione

Di seguito si fornisce un esempio di file di configurazione /etc/ipsec.conf che permette sia di collegarsi solamente al gateway che alla intranet interna. Come indicato precedentemente, la configurazione di FreeS/WAN è piuttosto complessa ed è bene consultare anche la documentazione allegata al programma.

```
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        #interfaces=%defaultroute
        interfaces="ipsec0=eth0"
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=yes

## RoadWarrior to Gateway
conn freeswan-x509
        # Right side is FreeS/WAN RoadWarrior
        rightrsasigkey=%cert
        rightid="/O=id/OU=users/CN=freeswan"
        right=%defaultroute
        # Left side is VPN GATEWEAY
        left=1.2.3.4
        # leftid=  # !do not use for Check Point!
        # config
        type=tunnel
        keyingtries=0
```

```
        disablearrivalcheck=no
        authby=rsasig
        auth=esp
        keyexchange=ike
        auto=start

## RoadWarrior to Net behind Gateway: FreeS/WAN <-> Check Point
conn freeswan-x509-net
        # Right side is FreeS/WAN RoadWarrior
        rightrsasigkey=%cert
        right=%defaultroute
        rightid="/O=id/OU=users/CN=freeswan"
        left=1.2.3.4
        leftsubnet=172.16.1.0/24
        # config
        type=tunnel
        keyingtries=0
        disablearrivalcheck=no
        authby=rsasig
        auth=esp
        keyexchange=ike
        auto=start
```

In caso di problemi durante la configurazione di FreeS/SWAN, si consiglia la lettura di *SSL Certificates HOW-TO* (The Linux Documentation Project) e di *VPN Connection to FreeS/WAN IPSec Gateway* (SSH Communications Security).

8. CONTROMISURE

Come avviene su Internet, anche le reti wireless sono soggette a tentativi di accesso da parte di intrusi. L'attacco sulle reti wireless é contemporaneamente più grave di un tradizionale attacco via Internet, in quanto si riesce ad eludere i firewalls esterni, e molto più semplice, in quanto é sufficiente posizionarsi all'esterno dell'edificio per tentare di accedere, senza possibilità di essere rintracciati. Alcuni sistemi, ad esempio quelli di famose società o istituti di credito, sono più soggette a tentativi di accesso di quelle di medie e piccole imprese, che devono solamente evitare di essere usati come "ponti" per accedere a prede più ambite. Per le imprese soggette a tentativi indebiti di accesso, é necessario dotarsi di apposite contromisure che rilevano i tentativi di accesso e che sviano l'attenzione degli intusi dalle reti preziose. Tali metodi, che vedremo in dettaglio nei paragrafi successivi, sono gli *Intrusion Detection Systems* (IDS) e le reti trappola, chiamate *Honeynet*.

IDS

L'IDS (Intrusion Detection System) é un sistema di analisi del traffico in tempo reale che costituisce l'estensione logica delle capacità di un firewall. Questo strumento mette a disposizione dell'amministratore funzionalità oggi indispensabili nella gestione della sicurezza di rete, quali l'analisi e il riconoscimento degli attacchi o delle anomalie del traffico di rete. Il sistema di rilevazione delle intrusioni innalza il livello di protezione offerto dal firewall monitorando e analizzando in maniera preventiva il traffico di rete, al fine di identificare pattern sospetti che possano indicare un attacco proveniente sia dall'esterno che dall'interno della rete aziendale. Oltre al riconoscimento degli attacchi, l'IDS svolge anche funzioni di diagnostica di rete e di controllo sulla corretta applicazione delle policy di sicurezza. Segnalando infatti la presenza di traffico in contrasto con le policy stabilite, aiuta a individuare errori di configurazione delle stesse (ad esempio rilevando traffico che il firewall avrebbe

dovuto bloccare). L'uso di sistemi (o *sonde*) IDS è fortemente consigliabile nelle DMZ e a protezione di macchine sensibili. In tale ottica un IDS assume una importanza fondamentale in un ambito wireless al fine di individuare eventuali tentativi di accesso non autorizzato, ad esempio attraverso backdoors o buffer overflow. Alcuni IDS sono in grado di rispondere agli attacchi, ad esempio attraverso un pacchetto generato ad-hoc al fine di scoraggiare eventuali intrusi.

Una completa analisi del mondo "IDS" risulterebbe molto complessa e richiederebbe un libro separato per poter affrontare l'argomento. Questo paragrafo vuole comunicare al lettore l'importanza dei sistemi IDS anche in ambito wireless. Nei prossimi paragrafi verranno analizzati in modo superficiale gli IDS e una configurazione relativamente semplice di un IDS OpenSource.

Gli IDS in dettaglio

Lo scopo di un IDS é di fornire dettagli su un eventuale attacco. A tal fine gli IDS collezionano informazioni dai sistemi e dalle reti, ricercando problemi di sicurezza. In qualche caso, gli IDS riescono anche a reagire in tempo reale alle violazioni di sicurezza. Le funzioni salienti di un IDS sono

- Analisi delle attività di sistema e degli utenti.
- Analisi della configurazione di sistema e di eventuali vulnerabilità.
- Verifica dell'integrità dei files critici del sistema e dei dati.
- Analisi statistica di attività anomale.
- Riconoscimento di patterns relativi a determinati tipi di attacco.

Si possono distinguere due categorie di IDS: una *Host based*, a protezione dell'host su cui risiede l'IDS e molto spesso con funzioni caratteristiche dell'host quali l'auditing di comandi sospetti, l'altra è il *Network IDS*, che si occupa di monitorizzare il traffico di rete e rilevare eventuali tentativi di intrusione e di esecuzione di comandi sospetti. Esiste un'altro tipo di IDS, ma che può essere racchiusa sotto la categoria Host Based, ovvero il *File Integrity Checker* che é in grado di individuare i files cambiati nel sistema. Tra queste categorie, il Network IDS é quella più diffusa, in quanto permette il riconoscimento di attività sospette che passano sulla rete senza dover installare software aggiuntivo su ogni server.

Un IDS é in grado di analizzare eventi sospetti attraverso tre differenti tipologie di analisi, ovvero analisi basate su eventi o *signatures*, analisi statistiche e sistemi auto-adattanti. Nel caso di sistemi basati su signatures, il software IDS ragiona esattamente come un anti-virus. Il produttore del software produce un elenco di modelli (o *patterns*) che verranno ricercati all'interno del traffico di rete e, se questi verranno trovati, manderà un avvertimento all'amministratore. Questa é la tipologia di IDS più diffusa. Un sistema basato su analisi statistiche é in grado di costruirsi un "modello" dell'ambiente, ad esempio tenendo traccia di quanto duri una sessione telnet media. L'amministratore verrà notificato qualora il sistema riveli una sessione telnet differente dal suo modello. L'ultima tipologia di analisi é quella più complessa, dove la ricerca si sta concentrando, ovvero quella dei sistemi auto-adattanti. Questi sistemi partono con regole generiche sull'ambiente e iniziano ad imparare dall'ambiente circostante, quindi "adattandosi". Dopo aver

imparato le tipologie di traffico nell'ambiente di rete, questi sistemi notificano l'amministratore nel caso esista del traffico differente da quello che hanno imparato.

Qualsiasi sia il tipo di analisi che il sistema é in grado di effettuare, ogni IDS può non tenere traccia di eventi sospetti (detto anche *falsi negativi*) o può segnalare eventi sospetti anche quando non esiste nessun attacco (i *falsi positivi*). É importante capire che qualora un'organizzazione decida di installare un sistema IDS esso va costantemente analizzato da amministratori preparati.

Network IDS

I Network IDS (NIDS) sono divisi in due componenti logici: il sensore (o sonda) e la stazione di controllo (anche detta di *management*). La sonda viene installata in un segmento di rete e tiene traccia di eventi sospetti, mentre la stazione di management riceve gli allarmi dalle sonde e li visualizza su un monitor ad un operatore. I sensori sono sistemi dedicati al controllo del traffico di rete, che hanno una interfaccia di rete configurata in *promiscuous mode*: grazie a questa modalità, la scheda é in grado di ricevere ed analizzare tutto il traffico di rete. Qualora trovasse un'attività sospetta, la sonda manderà un allarme alla stazione di management. La stazione di controllo visualizza gli allarmi ed é solitamente in grado di effettuare delle ulteriori analisi. Alcune stazioni di management sono anche in grado di integrarsi con un framework di management più ampio, di solito adottati nei Network Operating Centre (NOC), quale ad esempio HP OpenView.

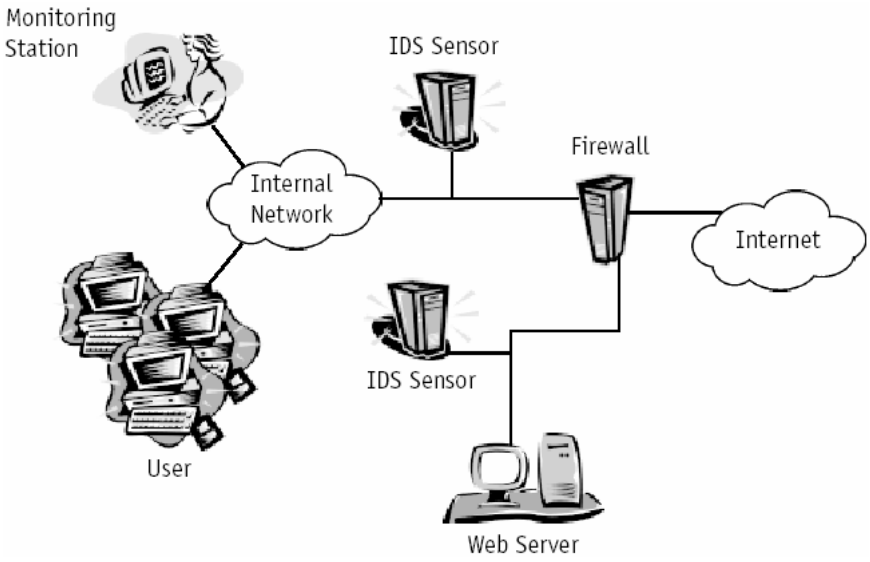

Fig. 8.1 - Architettura NIDS

Host IDS

Un sistema di IDS host-based ricerca segnali di intrusione nel sistema locale. Di solito questi sistemi si appoggiano ai sistemi di audit e di log del sistema operativo come fonte di informazioni per le analisi. In particolare analizzano attività sospette riguardanti il sistema locale, quali login sbagliate, tentativi di accesso a files protetti o alterazioni dei privilegi di sistema. Questo genere di IDS é di solito basato su regole, ad esempio il privilegio di amministratore può essere raggiunto soltanto attraverso il comando *su*. Ogni tentativo di accesso come root direttamente dal prompt di login può essere quindi considerato un attacco.

File Integrity Checkers

Un sistema File Integrity Checker esamina i files del computer per determinare se un file é stato alterato dall'ultima volta che il programma é stato eseguito. Il programma é basato su un database che tiene traccia del valore di hash di ciascun file del computer e ogni volta che viene eseguito paragona i files presenti nel sistema con quelli che ha nel database. Se il valore di hash differisce allora il file é da considerarsi modificato. Un valore di hash é dato da una funzione matematica che produce un valore a lunghezza fissa a partire da un file. Lo stesso file produrrà sempre lo stesso valore di hash ed un cambiamento a questo file produrrà un valore di hash differente. Esiste un caso raro in cui due files diversi producono lo stesso hash. Questa é una limitazione dei File Integrity Checkers che di solito viene sfruttata da potenziali intrusi per alterare i files di configurazione, senza però essere "visti" dal programma di controllo. Un esempio di File Integrity Checker é il famoso Tripwire (http://www.tripwire.org/).

Configurazione dello switch per un NIDS

Prima di configurare un NIDS, é necessario procedere ad una corretta configurazione dello switch su cui il sistema IDS verrà attestato. Un hub riceve un pacchetto su una porta e manda una copia, ripetendo il segnale, su ogni porta tranne quella da cui lo ha ricevuto. Uno switch, invece, analizza tutti i MAC address delle stazioni collegate alle sue porte e, quando un client manda un pacchetto destinato ad un'altro client, questo viene ripetuto soltanto sulla porta del client di destinazione. Questo comportamento, tipico dello switch, permette un significante incremento di prestazioni, ma lo rende inadatto ai sistemi IDS o, più semplicemente, a degli analizzatori di rete (o sniffer). Per esempio, se si vuole catturare il traffico ethernet mandato dall'host A all'host B, ed entrambi sono collegati ad un hub, é sufficiente collegare un analizzatore sull'hub per visualizzare il traffico che passa.

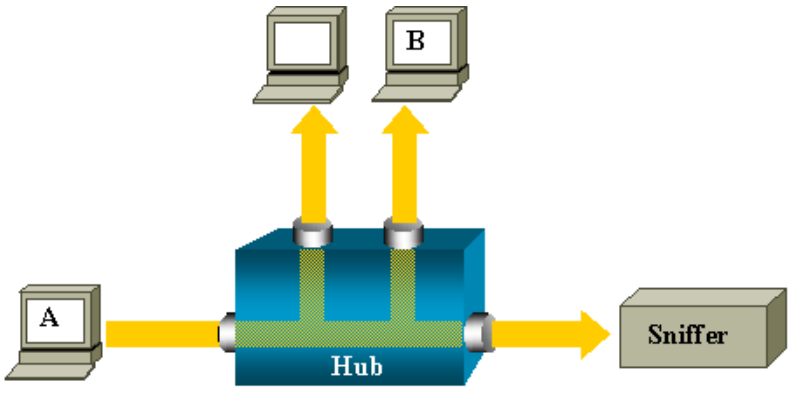

Fig. 8.2 – Schema di funzionamento di un hub

In uno switch, invece, il traffico tra l'host A e l'host B é solamente ripetuto sulla porta di B, pertanto il traffico non é catturabile dallo sniffer.

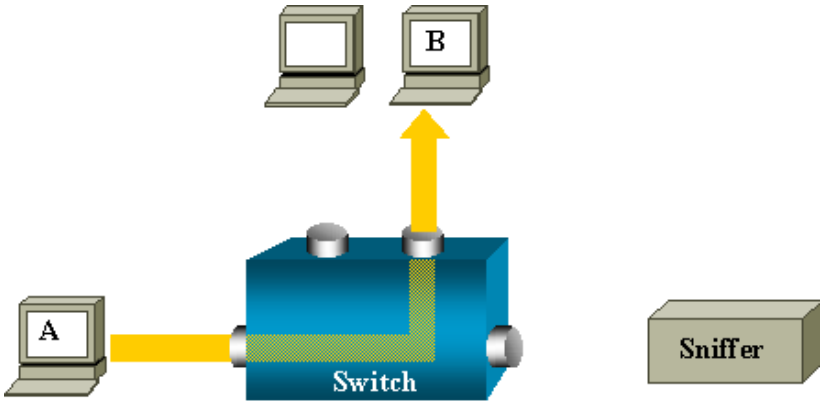

Fig. 8.3 - Schema di funzionamento di uno switch

Per poter analizzare il traffico é necessario abilitare una funzionalità detta *port monitor* o *port mirroring*. Non tutti gli switch dispongono di tale funzionalità: é necessario pertanto verificare con il produttore del proprio switch che il port mirroring sia disponibile. Negli switch Cisco questa caratteristica é detta *Switched Port Analyzer* (SPAN). Esistono due modi di attivare SPAN sui sistemi della Cisco dipendenti dal tipo di OS dello switch. Negli switch che montano i sistemi IOS, ad esempio la serie 2900XL, 3500XL e 4600, é necessario posizionarsi sulla interfaccia in cui é attestato l'IDS (esempio la *FastEthernet 0/10*) ed eseguire i seguenti comandi:

```
Switch(config)# int fa0/10
Switch(config)# port monitor FastEthernet 0/1
Switch(config)# port monitor FastEthernet 0/2
Switch(config)# port monitor VLAN 10
```

Il comando *port monitor* permette di analizzare una porta o una VLAN. In questo modo, tutto il traffico destinato a quella/e porta/e o VLAN verrà mandato alla sonda IDS. Sui sistemi che usano CatOS, ad esempio la serie 5000 e 6000, il comando é:

```
set span src_mod/src_port dest_mod/dest_port
set span src_vlans dest_mod/dest_port
```

il valore di dest_mod/dest_port é la porta dove é attestato l'IDS, ad esempio:

```
set span 0/1-2 0/10
set span 10 0/10
```

Il primo esempio é relativo al monitoring delle porte 0/1 e 0/2, mentre il secondo é quello della VLAN 10.

Esempio di IDS con Snort

Esistono differenti IDS, molti dei quali sono software commerciali come RealSecure di ISS. Una delle migliori sonde IDS é Snort, un software OpenSource capace di analizzare e tenere traccia del traffico IP in tempo reale. Snort é in grado di effettuare un'analisi del protocollo, ricerca ed individuazione di determinati contenuti e può essere usato per individuare diversi tipologie di attacchi, quali buffer overflow, scansioni stealth, attacchi ai CGI, tentativi sul protocollo SMB di Windows e i tentativi di determinare il sistemi operativo del server. Snort usa un linguaggio flessibile per le proprie regole. Queste ultime descrivono il traffico che deve essere identificato o che deve essere lasciato passare. Questo software ha la possibilità di mandare allarmi attraverso syslog, un file di log separato, di integrarsi con database relazionali come MySQL, di inviare un messaggio Windows (WinPopup) o un programma fatto ad-hoc. Tutte le principali distribuzioni Linux hanno tra i loro pacchetti il programma Snort, tuttavia alcune piattaforme (ad esempio Solaris o AIX) necessitano dei sorgenti del programma per essere compilato. É possibile scaricare tali sorgenti dal suo sito ufficiale http://www.snort.org/.

Snort può essere usato in tre modalità: come un packet sniffer (come *tcpdump* o *snoop*), come un packet logger (scrive i pacchetti in transito in un log) o come vero e proprio Network Intrusion Detection System. Per informazioni più estese sul funzionamento di Snort, si faccia riferimento al manuale utente di Snort.

Modalità sniffer

Per la modalità più semplice di sniffer é sufficiente eseguire Snort con l'opzione "*-v"*, che visualizza gli header dei pacchetti TCP/IP. Per visualizzare invece gli header dei pacchetti IP, TCP, UDP e ICMP é necessario invocarlo con l'opzione "*-vd"*. Con la modalità completa, ovvero con le opzioni "*-vde"*, é possibile visualizzare, oltre agli headers, anche i dati. Ad esempio:

```
/usr/local/sbin/snort -vde
```

Modalità packet logger

La modalità *packet logger* si attiva qualora si decida di salvare questi paccheti su disco. La modalità più semplice é quella di specificare una directory, attraverso l'opzione "*-l"*, dove verrano scritti i log. Ad esempio:

```
/usr/local/sbin/snort –vde –l /tmp/logs
```

É possibile limitare l'output dei log alla sola sottorete desiderata attraverso l'opzione "*-h"* come segue:

```
/usr/local/sbin/snort –vde –l /tmp/logs –h 192.168.0.0/24
```

Esiste un'altra opzione di Snort che permette di salvare i log in formato binario.

L'opzione *"-b"* é utile in caso di analisi con un programma esterno (ad esempio *tcpdump* o *ethereal*):

```
/usr/local/sbin/snort –vde –l /tmp/logs –b
```

Modalità Network IDS

Per abilitare questa modalità, é necessario disporre di un file con le regole, di solito si tratta del file *snort.conf*. Per usare Snort in modalita NIDS é sufficiente eseguire il comando:

```
/usr/local/sbin/snort –d –l /tmp/logs –h 192.168.0.0/24 –c snort.conf
```

Snort ha numerose opzioni di configurazione, incluso ad esempio una configurazione ad alte performance.

Questa sezione sui sistemi IDS ha voluto sottolineare l'importanza di tali strumenti in determinati ambienti e vuole invogliare l'amministratore ad un maggiore approfondimento sull'argomento.

HoneyNet

Una HoneyNet è una rete che funge da esca a potenziali aggressori. È una rete fittizia, deliberatamente aperta, che contiene pochi sistemi e il cui solo scopo è disorientare l'intruso e far perdere all'attaccante tempo prezioso. Tanto più è credibile la HoneyNet, tanto l'intruso non si accorgerà che si tratta di una rete fittizia e che è sotto osservazione. Una volta che l'intruso è intrappolato nella HoneyNet, è possibile studiarne il comportamento e le tipologie di attacco che è solito utilizzare. Inoltre è possibile identificarlo ed eventualmente coinvolgere le autorità competenti durante l'attacco.

L'uso di HoneyNet è utile quando la wireless è installata presso sedi importanti dove è fondamentale la confidenzialità delle informazioni, ma allo stesso tempo è palese al pubblico la conoscenza di tale sede. Ne sono un esempio le sedi principali degli istituti di credito, in quanto le informazioni sulla loro locazione sono di pubblico dominio.

Una HoneyNet wireless è facilmente costruibile semplicemente creando una nuova rete, completamente scollegata da qualsiasi altra su cui attestare un Access Point sufficientemente potente. Successivamente si configurerà l'Access Point semplicemente negando le regole basilari di configurazione indicate precedentemente, ad esempio impostando un SSID descrittivo quale "BancaABC" e non attivando le protezioni MAC. Come sottolineato precedentemente è importante che la HoneyNet sia credibile e che l'intruso non abbia il sospetto di essere intrappolato, pertanto é utile poter posizionare dei server, ad esempio web o database, che facciano sembrare "vera" la rete fittizia. Nella HoneyNet é importante posizionare un IDS che avverta l'amministratore quando una intrusione é in corso. L'intruso sarà così intrappolato in una rete fittizia e perderà tempo nel "carpire" informazioni che non riflettono la realtà aziendale. In questo modo l'amministratore potrà studiare il comportamento dell'intruso e, se necessario, avvertire le autorità competenti.

9. APPLICAZIONE DELLE TECNOLOGIE IN AMBITO WIRELESS

Per affrontare efficacemente il tema delle wireless LAN, è importante capire che non esiste "la soluzione", ma esistono varie tecniche e componenti che permettono congiuntamente di proteggere meglio il sistema. Analogamente alla rete Internet, non esiste la totale sicurezza, ma l'obbiettivo è quello di rendere talmente alto lo sforzo per riuscire ad entrare nel sistema, che il valore del contenuto stesso non abbia più senso. *Maggiore é il valore del contenuto da proteggere, maggiori devono essere le contromisure da adottare*. Vedendo ad esempio i due opposti, è inutile e ingestibile adottare un sistema di crittografia avanzato per una bacheca aziendale, quanto insicuro usare le password di default sul database centrale.

La protezione dei dati è tanto importante quanto importante è anche evitare l'uso improprio della propria LAN da parte di un intruso. Molto spesso, infatti, l'intruso non è interessato al contenuto di una rete (wireless o tradizionale), ma all'uso della stessa come "trampolino di lancio", sia per camuffare le proprie traccie, sia perchè la rete attaccata a una relazione di fiducia con una rete terza a cui l'intruso puo' essere interessato. Un intruso ad esempio potrebbe essere interessato a entrare nella rete wireless di una agenzia di viaggi per raggiungere ed attaccare la rete della compagnia aerea a cui l'agenzia viaggi è collegata. In questo esempio la responsabilità penale dell'attacco potrebbe ricadere sull'amministratore di sistema dell'agenzia di viaggi che è comunque responsabile della macchina da cui è partito l'attacco. Fino a che le autorità giudiziarie non avranno dimostrato che l'attacco è stato provocato da un intruso attraverso opportune indagini, l'amministratore di sistema sarà responsabile di tale attacco.

Nei capitoli precendenti abbiamo visto quali sono le "armi" tecnologiche che possono essere adottate per proteggere le wireless LAN. Tenendo conto del metro di giudizio relativo al contenuto da proteggere, si possono delineare quattro tipologie di ambienti. I primi due ambienti, che chiameremo *SOHO* (Small Office,

Home Office) e *PMI* (Piccola e Media Impresa), in cui la protezione delle wireless LAN è più focalizzata sulla problematica di evitare l'uso improprio della propria rete wireless, mantenendo comunque una certa confidenzialità dei dati. Nel terzo, che chiameremo *Corporate*, in cui non solo è importante evitare che un intruso entri nella rete wireless, ma soprattutto che la confidenzialità e la autenticazione dei dati siano parte essenziale della soluzione. Nel quarto caso, quello degli *ISP* (Internet Service Providers) e degli *Operatori Mobili* invece la confidenzialità dei dati non é importante quanto quello di identificare univocamente l'utente per fatturarne il consumo.

La suddivisione affrontata in questo capitolo é puramente indicativa e basata sull'esperienza dell'autore. Scegliere di adottare una soluzione rispetto all'altra è una questione meramente "filosofica" dell'amministratore di rete. Qualora si decida di sposare la soluzione *SOHO, PMI* o *Corporate* è bene applicare le regole basilari di sicurezza degli Access Point contenute nel paragrafo *Regole di base* del Capitolo 2 e fare periodici auditing della propria wireless LAN al fine di evitare che un utente colleghi alla rete interna Access Point non autorizzati.

Tecnologie/ Ambienti di utilizzo	*SOHO*	*PMI*	*Corporate*	*ISP/Operatori Mobili*
Regole di base	X	X	X	
Proxy	X	X		
PPPoE	X	X		X
IEEE 802.1x		X	X	X
WPA		X	X	X
IPSec			X	
IDS e HoneyNet			X	

Ambienti SOHO

Negli ambienti Small Office Home Office, tipicamente abitazioni private e piccoli uffici, è importante focalizzarsi nel mantenere privata la rete wireless. In particolare lo scopo è evitare che un intruso entri illegalmente nella propria rete e la sfrutti per attaccare altri siti. I dati contenuti solitamente in questa tipologia di ambiente non ha informazioni vitali, oppure non giustificano, sia da un punto di vista di set-up che di amministrazione, una infrastruttrara di sicurezza molto complessa.

Per le utenze domestiche e per alcuni piccoli uffici la semplice applicazione delle regole di base descritte nel Capitolo 2 sono sufficienti a proteggere la rete da intrusioni. Per i piccoli uffici che dispongono di uno o più server, ma che non hanno un dipartimento IT dedicato, è consigliabile unire alle tecniche di base degli Access Point anche un accesso tramite la tecnologia PPPoE, descritta nel capitolo 4, o tramite un Proxy (Capitolo 3). Questa tecnica offre agli utenti una buona protezione dagli accessi indesiderati, mantenendo comunque una sufficiente confidenzialità dei dati grazie a WEP.

Ambienti PMI

La Piccola e Media Impresa (PMI) é talmente diffiusa sul territorio che rappresenta la maggioranza delle imprese italiane. Le PMI possono arrivare fino ad oltre un centinaio di dipendenti e non é raro trovare un dipartimento IT dedicato, seppur formato da poche persone. Sebbene si tratti di aziende con una forte concorrenza nel loro settore, lo spionaggio informatico è raro in questo ambito. Analogamente ad un ambiente SOHO, l'obbiettivo è pertanto mantenere privata la rete wireless ed evitare di essere usati come "ponte", seppur mantanendo una certa confidenzialità dei dati.

In questo ambiente, è necessario coadiuvare le regole di base con un'altra tecnologia. Qualora si disponga di:

- un server Windows 2000 o superiore, tutti i client Windows 2000 o superiore, e uno o più Access Point che supportano IEEE 802.1x e/o WPA, sarebbe opportuno usare la tecnologia IEEE 802.1x descritta nel Capitolo 5.
- un proxy/firewall già installato con autenticazione dei client, ad esempio Microsoft ISA Server o Squid, é consigliabile usare la tecnologia Proxy descritta nel Capitolo 3.
- un Windows Server/Workstation o un router Cisco, client eterogenei tra di loro (Microsoft Windows, Linux, Apple MacOS, ecc...) e con la necessità di accedere a servizi non-web si consiglia di adottare la tecnologia PPPoE descritta nel Capitolo 4.

Ambienti Corporate

L'ambiente *Corporate* è costituito dalla grande impresa. In questa tipologia di ambiente ricadono coloro che necessitano di proteggere più il contenuto che un eventuale "join" alla rete wireless da parte di un intruso. Solitamente si tratta di un ambiente complesso, con amministratori di rete dedicati alla gestione dell'ambiente IT, e che molto spesso già dispongono di una VPN e di una infrastruttura PKI. Le persone che necessitano di accedere alla rete wireless hanno diverse esigenze e appartengono a diversi reparti, ad esempio i consulenti e il dipartimento vendite. Le informazioni a cui si ha accesso hanno un diverso grado di confidenzialità e sono solitamente ospitate su sistemi eterogenei, quali ad esempio Windows, Unix e Mainframe.

Per questo ambiente è consigliabile l'uso della tecnologia IPSec che fornisce sia controllo degli accessi, ma soprattutto offre un framework crittografico più ampio. Un gateway IPSec è in grado di fornire crittografia anche ai sistemi che non dispongono di tale tecnologia, ad esempio un AS/400 che con sistema operativo

versione V2R3M0 non dispone di IPSec. È bene collegare la rete wireless ad un firewall perimetrale di accesso Internet come spiegato nel Capitolo 4, la rete wireless puo' essere facilmente paragonata alla rete Internet, pertanto è necessario classificare gli utenti wireless come se si stessero collegando da un'altra località remota.

Nel caso di eterogeneità degli utenti che accedono alla rete wireless è suggeribile usare lo standard IEEE 802.1X, qualora gli Access Point siano in grado di supportarlo. È utile raggruppare le categoria di utenti in apposite VLAN perchè si possono assegnare permessi di accesso alle VPN o ad altre risorse. In particolare è utile quando la rete wireless è condivisa tra più entità o aziende. Ad esempio, tutte le aziende di un palazzo o di un campus decidono di offrire accesso wireless mantenendo una infrastruttura comune ad un minor costo di gestione con una maggiore copertura radio. Ogni utente di una determinata azienda sarà categorizzata in una VLAN ben separata che a sua volta verrà collegata al proprio firewall perimetrale. Nella stessa VLAN è consigliabile posizionare una sonda Network IDS per monitorare eventuali attività sospette e notificare pertanto l'amministratore di rete o di sistema che potrà prendere opportuni provvedimenti.

L'uso di una HoneyNet è consigliato in casi molto particolari perchè la sua gestione è piuttosto onerosa. É necessario disporre di un team ben preparato sulle problematiche di sicurezza, solitamente chiamato *Computer Incident Response Team (CIRT)* che controlli sempre la HoneyNet e correli altri eventi di sicurezza presenti in azienda. È consigliabile usare una HoneyNet nel caso esista una palese evidenza logistica dell'azienda, esempio attraverso cartelli all'esterno, e nel caso il contenuto dei dati da proteggere sia fortemente sensibile. Ad esempio è il caso delle banche o istituzioni pubbliche, in cui la loro sede principale è di pubblico dominio, il loro contenuto è indubbiamente interessante e la probabilità di trovare una wireless LAN è molto alta. È probabile che un eventuale intruso si apposti nelle vicinanze e che, attraverso antenne direttive e con alto guadagno, l'intruso tenti di individuare un accesso wireless. In questi casi l'uso di una HoneyNet potrebbe contribuire a disorientarlo e a distrarlo nel tentativo di rintracciare la sua provenienza.

Gli utenti

Alcune volte si tende a sottovalutare l'aspetto degli utenti, ma è importante *ascoltare* le esigenze degli utenti e coniugarle con i requisiti di sicurezza dell'azienda. Ad esempio se per proteggere la rete wireless l'utente deve "affrontare" complesse procedure è possibile che questo sia demotivato all'uso delle stesse tentando di eluderle con un Access Point collegato alla rete interna. È consigliabile usare programmi con cui l'utente già si sente familiare, ad esempio accesso remoto o il sofware VPN che già usa, oppure automatizzare la distribuzione delle policy attraverso il *Group and Policy Editor.* È importante anche assegnare i giusti permessi all'utente, senza troppo limitarlo nelle sue azioni e senza permettergli l'accesso a tutta la rete aziendale.

L'utente pertanto deve avere la sensazione che attraverso *pochi* cambiamenti gli venga garantita la *sua* sicurezza e quella aziendale, *senza avere ulteriori limitazioni.*

Ambienti ISP e Operatori Mobili

Gli operatori di telefonia mobile GSM/UMTS sono i migliori candidati per offrire accesso pubblico tramite 802.11, in quanto già dispongono dei mezzi, dell'infrastruttura e dell'esperienza necessaria. A titolo di esempio basti pensare che affiché la rete GPRS funzioni é necessario che la BSC, ovvero la "scatola" che gestisce le antenne GSM, abbia un collegamento IP con la sede centrale tipicamente in Frame Relay. La strada da percorrere tra avere un collegamento IP già presente nella BSC e l'installazione di antenne e Access Points per la fornitura di accesso Wi-Fi é pertanto molto breve. Analogamente, alcuni ISP e operatori telefonici che dispongono di fibra ottica potrebbero essere interessati ad estendere i loro servizi al Wi-Fi ad esempio come sostituzione del "local loop", ovvero dell'ultimo miglio in alternativa ai cavi in rame di Telecom Italia.

Qualsiasi sia lo scenario, l'uso pubblico della rete wireless é molto diverso dagli ambienti precedenti, dove é importante proteggere il contenuto dei dati in transito o l'accesso. Il modello di business legato agli operatori mobili e ISP é di identificare univocamente l'utente per motivi di billing, ad esempio un pay-per-use o la verifica che l'utente sia sottoscritto al servizio. Inoltre, non é possibile "offuscare" l'Access Point limitando la copertura radio, eliminando la propagazione del ESSID o usando chiavi WEP che cambiano continuamente. In uno scenario di copertura pubblica il segnale deve essere il più possibile diffuso, l'ESSID deve riflettere il nome dell'ISP (ad esempio: "TelecomLocale"), non devono esserci chiavi WEP impostate staticamente e non é possibile filtrare i MAC address dei client.

Tenendo conto dell'esigenze degli ISP e degli operatori mobili, le migliori tecnologie da poter utilizzare in questo ambito sono IEEE 802.1x e PPPoE. La scelta tra una delle due tecnologia è dettata da diversi fattori, tra cui il modello di business e i requisiti derivati dal marketing. Si vedano quali sono secondo l'esperienza dell'autore i vantaggi e gli svantaggi delle due soluzioni.

Tecnologia IEEE 802.1x

Pro	Contro
• IEEE 802.1x é il miglior metodo per l'autenticazione su reti Ethernet, in quanto non introduce overhead nella frame. • Si integra perfettamente con WEP per la distribuzione automatica delle chiavi attraverso la frame EAPOL-Key. • È alla base di WPA e IEEE 802.11i (WPA2).	• Il radius server deve supportare EAP. Inoltre deve supportare uno schema di autenticazione che permetta di usare le password, come ad esempio MD5 o PEAP. È sconsigliabile l'uso di TLS come metodo di autenticazione per il costo di produzione, distribuzione e mantenimento dei certificati X.509. • Gli unici OS che supportano nativamente IEEE 802.1x sono Windows 2000 e Windows XP. Altri sistemi operativi necessitano di appositi client con un costo aggiuntivo. • Nessuna possibilità di identificare univocamente un client attraverso un IP statico.

Tecnologia PPPoE

Pro	Contro
• Il client PPPoE è presente nella maggior parte dei sistemi operativi. Per gli OS in cui manca il client nativo, esistono versioni gratuite. • Nessun cambio dell'infrastruttura dial-up. Il PPPoE usa la stessa metodologia di accesso, quindi le stesse procedure di installazione, già in essere per i modem, ISDN e ADSL. • E' possibile assegnare un indirizzo IP statico. • È possibile crittografare la connessione attraverso MPPE.	• Non è possibile usare la crittografia WEP o WPA, ma si può sopperire usando l'estensione MPPE e raccomandando all'utente l'utilizzo di connessioni protette ai server (ad esempio HTTPS e IMAPS). • La grandezza del MTU non può essere maggiore di 1492, pertanto si hanno problemi di performance trasferendo una grossa mole di dati.

Il protocollo IEEE 802.1x é il migliore metodo per autenticare e profilare un utente su tecnologia ethernet. Inoltre é in grado di integrarsi con WEP, WPA e IEEE 802.11i (WPA2), offrendo una buona confidenzialità all'utente finale. Al contrario PPPoE deve avvalersi di MPPE per poter offrire un'analoga protezione dei dati dell'utente, di fatto escludendo a priori qualsiasi crittografia hardware come WEP o WPA.

Il grosso svantaggio di IEEE 802.1x é relativo soprattuto ai costi da affrontare per distribuire un software per l'autenticazione alla rete, in quanto al momento non tutti i sistemi operativi sono equipaggiati con tale client. Con PPPoE questo problema non esiste: tutti gli OS sono dotati di software per l'accesso PPPoE in quanto si tratta della stessa tecnologia usata nell'ADSL.

Sebbene la tecnologia IEEE 802.1x sia la soluzione perfetta per i client mobili quali portatili e PDA, potrebbe non esserla quando il Wi-Fi è usato come sostituto del "local loop". La tecnologia PPP offre la possibilità di avere un IP statico, pertanto è l'ideale per le piccole e medie aziende che intendono erogare servizi verso Internet, ad esempio un mail server. Un altro vantaggio di PPPoE rispetto a IEEE 802.1x é che PPPoE si integra perfettamente in una infrastruttura dial-up esistente, ovvero modem, ISDN e ADSL. Integrandosi in tale infrastruttura l'ISP o l'operatore mobile potrà erogare servizi di Virtual Private Dial-up Network (VPDN) anche attraverso il Wi-Fi, ampliando quindi l'offerta di affitto della propria rete ad ISP più piccoli o ad aziende.

10. GESTIONE DEGLI INCIDENTI

In questo libro si sono analizzati tutti i problemi relativi alle wireless LAN e sono stati forniti dei suggerimenti su come proteggere efficacemente la propria rete. Così come è importante proteggere la propria rete è importante anche capire cosa fare in caso di intrusione o di sospetta violazione di qualche sistema. Non si può rendere totalmente sicuro un sistema e bisogna tener presente che un aggressore piuttosto motivato potrebbe comunque violare il sistema. Molto spesso l'intruso non sfrutta solamente gli eventuali problemi di sicurezza di un applicativo, ma fa anche uso del *social engineering*, ovvero chiamare alcune persone che lavorano all'interno dell'azienda e usare la psicologia per ottenere informazioni preziose.

Un amministratore di sistema puo' insospettirsi di una intrusione da alcuni sintomi, quali ad esempio:

- Segnalazioni di attività sospette provenienti dalla sua macchina;
- La macchina si comporta in modo strano. Ad esempio: risulta molto lenta, ma il programma *top* non segnala nulla di particolare; uno o più filesystems sono pieni, ma non si riesce a scoprirne le cause;
- Il traffico in rete è molto elevato;
- Connessioni da locazioni insolite;
- I file di log sono incompleti o addirittura scomparsi;
- Alcune utility di sistema (o file di configurazione) sono state modificate

In questi casi potrebbe essere utile usare un rilevatore di *root kit*, quali ad esempio *chkrootkit*. È bene stare attenti perchè un eventuale intruso ben motivato potrebbe aver costruito il suo *root kit*, eludendo i rilevatori. Qualora si abbiano sospetti di intrusione è bene consultarsi con altri amministratori di sistema, di rete e di sicurezza per tentare di correlare tutti gli eventi sospetti.

In caso di incidente

Qualora si abbia avuto un intrusione, è bene non farsi prendere dal panico e razionalizzare nelle policy di sicurezza un eventuale processo di *Gestione degli incidenti*. Innanzi tutto è bene *staccare la macchina dalla rete*, procedere a raccogliere, a macchina accesa, prove che potrebbero rilevare tracce importanti dell'intruso. Alcune volte gli intrusi, per fretta o distrazione, dimenticano di cancellare le proprie traccie presenti nei log. Ad esempio è bene analizzare sempre il file di *messages, xferlog, wtmp, maillog* e per ogni utente guardare il contenuto del file di *history* della shell. Prima di spegnere la macchina è bene fare un backup completo che potrebbe servire ai fini legali. Una volta che si ha la conferma dell'intrusione può essere utile staccare il disco fisso e conservarlo per un'attività di analisi. Tale attività, detta *Forensic Analisys*, viene condotta da esperti di sicurezza e molto spesso è necessaria in caso di risvolti legali.

In caso di sospetta intrusione è buona norma notificare il fatto ai responsabili dei siti da cui è giunto l'attacco, il che dimostra inoltre una convivenza civile su Internet. Si riporta la seguente citazione dal RFC 1281 *Guidelines for the Secure Operation of the Internet*:

"The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations. "

Qualora il tentativo di accesso risulti piuttosto grave, o si ha semplicemente il sospetto che l'intruso abbia usato la propria rete per attaccare qualche altro sito è bene sporgere denucia alla *Polizia Postale*, presentando anche copia dei backup e dei log come prova dell'intrusione.

Ripristinare il servizio

Così come è importante trovare un intruso, è importante ripristinare il prima possibile il servizio agli utenti per diminuire i tempi di downtime. In questo caso è bene non fidarsi dei backup periodici, in quanto non si è a conoscenza del momento in cui l'intruso è penetrato nel sistema. È pertanto necessario reinstallare completamente il sistema operativo, avendo cura di applicare tutte le patch di sicurezza consigliate dal proprio produttore. Ripristinare dall'ultimo backup *solamente* i dati e la configurazione, avendo cura di rivedere dettagliatamente la configurazione stessa in quanto l'intruso potrebbe averla modificata a proprio giovamento. Una volta ripristinato il sistema è consigliabile cambiare tutte le password ed eventualmente installare un Host-based IDS per tracciare ulteriori tentativi di accesso.

GLOSSARIO

AC	Access Concentrator
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
BSC	Base Station Controller
BSS	Base Station System
BSS	Basic Service Set
BTS	Base Tranceiver Station
CA	Certification Authority
CDP	Cisco Discovery Protocol
CSMA/CA	Carrier Sense and Multiple Access with Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DSSS	Direct Sequence Spread Spectrum
EAP	Extensive Authentication Protocol
EAPOL	Extensive Authentication Protocol over Ethernet
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
GPRS	GSM Packet Radio Service
GUI	Graphical User Interface
IAB	Internet Architecture Board
ICA	Internal Certification Authority
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IPSEC	IP Security Protocol
IR	Infrarossi
ISAKMP	Internet Security Association and Key Management Protocol
IV	Initial Vector
LAN	Local Area Network
LEAP	Light EAP
LLC	Logical Link Control
MAC	Medium Access Control
MIC	Message Integrity Code
MPPE	Microsoft Point-to-Point Encryption Protocol
MTU	Maximum Transmission Unit

NAT	Network Address Translation
NIDS	Network IDS
PEAP	Protected EAP
PKI	Public Key Infrastructure
PMI	Piccola e Media Impresa
PMK	Pairwise Master Key
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PRF	Pseudo-Random Function
SA	Security Association
SAD	Security Association Database
SCEP	Simple Certificate Enrollment Protocol
SOHO	Small Office, Home Office
SPD	Security Policy Database
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TKIP	Temporary Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
VLAN	Virtual LAN
VPDN	Virtual Private Dial-up Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelty, o Wireless Ethernet (IEEE 802.11)
WLAN	Wireless LAN
WPA	Wireless Protected Access

BIBLIOGRAFIA

Giuseppe Paterno'
Using PPP-over-Ethernet (PPPoE) in Wireless LANs
Internet Draft, Maggio 2003

Kent & Atkinson
Security Architecture for the Internet Protocol
RFC 2401, Novembre 1998

R. Braden, D. Clark, S. Crocker, C. Huitema
Report of IAB Workshop on Security in the Internet Architecture February 8-10, 1994
RFC 1636, June 1994

Institute of Electrical and Electronics Engineers
Local and metropolitan area networks Port-Based Network Access Control
ANSI/IEEE Standard 802.1X, Ottobre 2001

R. Pethia, S. Crocker, B. Fraser
Guidelines for the Secure Operation of the Internet
RFC 1281, Novembre 1991

Uyless Black
Internet Security Protocols: Protecting IP Traffic
Pubblicato da Prentice Hall / Pearson Education nell'anno 2000

Stubblefield, Ioannidis, e Rubin
Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
AT&T Labs Technical Report TD-4ZCPZZ, Agosto 2001

M. Sutton, iDEFENSE Labs
Hacking the Invisible Network. Insecurities in 802.11x
WhitePaper, Luglio 2002

Giuseppe Paternò
Wireless Security:
A scalable solution for consumers, corporations, ISP and mobile operators
Whitepaper, Marzo 2003

SSH Communications Security
VPN Connection to FreeS/WAN IPSec Gateway
Manuale, Novembre 2002

Flavio Foschi
Le reti basate su standard IEEE 802.11b
Tesi di Laurea, anno 2002

Davide Cerri
Sicurezza a livello IP: IPsec e le reti private virtuali
Whitepaper

CheckPoint Software Technologies Ltd
CheckPoint Virtual Private Networks
Manuale, Marzo 2002

Mamakos, et. al
A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2516, Febbraio 1999

Institute of Electrical and Electronics Engineers
Local and metropolitan area networks Port-Based Network Access Control
ANSI/IEEE Standard 802.1X, Ottobre 2001

Simpson
PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 1994, Agosto 1996

Zorn
Microsoft PPP CHAP Extensions, Version 2
RFC 2759, Gennaio 2000

Aboba & Simon
PPP EAP TLS Authentication Protocol
RFC 2716, Ottobre 1999

Pall & Zorn
Microsoft Point-To-Point Encryption (MPPE) Protocol
RFC 3078, Marzo 2001

Kent & Atkinson
Security Architecture for the Internet Protocol
RFC 2401, Novembre 1998

Institute of Electrical and Electronics Engineers
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
ANSI/IEEE Standard 802.11, 1999 Edition

Institute of Electrical and Electronics Engineers
Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
IEEE Standard 802.11b, Settembre 1999

Pall
Microsoft Point-to-Point Compression (MPPC) Protocol
RFC 2118, Marzo 1997

D. Rand
The PPP Compression Control Protocol (CCP)
RFC 1962, Giugno 1996

W. Simpson
The Point-to-Point Protocol (PPP)
RFC 1661 / STD 51, Luglio 1994

RC4 é un algoritmo di crittografia proprietario disponibile sotto licenza da RSA Data Security Inc. Per informazioni sulla licenza contattare:

RSA Data Security, Inc.
100 Marine Parkway
Redwood City, CA 94065-1031

INDICE

Sicurezza Nelle Wireless LAN

Le Wireless LAN hanno portato una rivoluzione importante nel mondo dell'Information Technology. In questi anni abbiamo assistito ad una crescita esponenziale del mercato della telefonia mobile, che dimostra la necessità di comunicare in qualsiasi momento e da qualsiasi località. Analogamente al mercato della fonia, anche il mondo dei dati sta affrontando lo stesso trend di crescita, come dimostrato dall'interesse per il GPRS e per l'UMTS. Le Wireless LAN permettono di coniugare questa necessità di mobilità con le reti locali tradizionali, grazie soprattutto ai suoi costi contenuti e alla facilità di utilizzo.

Sebbene le Wireless LAN abbiano innumerevoli vantaggi, esistono delle nuove problematiche legate al mezzo trasmissivo via etere che hanno dei risvolti relativi alla sicurezza. L'etere è un mezzo trasmissivo pubblico: chiunque, con delle apparecchiature relativamente semplici, è potenzialmente in grado di captare il segnale delle Wireless LAN e introdursi nel sistema informativo di un'azienda. Questo libro vuole fornire al lettore alcuni suggerimenti su come rendere il collegamento wireless più sicuro.

Tra gli argomenti trattati:

- Problematiche di sicurezza delle Wireless LAN e tipologie di attacchi.
- Regole per la configurazione degli Access Point.
- Autenticazione e la segretezza dei dati con PPPoE ed esempi.
- Auditing, HoneyNet, IDS e autenticazione con IEEE 802.1x.
- Uso di proxy server per la protezione delle reti.
- Autenticazione e la segretezza dei dati con IPSec ed esempi.
- Suggerimenti di utilizzo delle tecnologie negli ambiti domestici, piccoli uffici, grandi aziende e ISP.
- Gestione degli incidenti e ripristino del servizio.

ISBN 88-901141-0-X

9788890114106