Un eccellente gateway multifunzione

L'articolo descrive in modo dettagliato l'installazione di un gateway basato su Linux con la funzionalità di Mail Relay e DNS server in una rete dotata di un collegamento HDSL ad Internet ed una connessione dedicata ad una LAN remota.

Introduzione

In questo articolo, verrà descritta l'opera di installazione di un gateway multifunzione basato sul sistema operativo Linux. Tutti i componenti software utilizzati per implementare le funzioni del sistema aderiscono alla filosofia Open Source e risultano liberi nell'utilizzo, sia amatoriale che commerciale. L'installazione descritta è stata progettata e portata a compimento dall'autore in una media azienda industriale del Veneto. Seguendo la linea descritta nell'articolo, qualunque persona con un know-how appena sopra la media del mondo Linux, del protocollo TCP/IP e delle applicazioni più comuni di tale protocollo, può ottenere gli stessi risultati in situazioni analoghe e in tempi brevi; chiunque può dilettarsi per studio o per gioco e ripetere l'installazione sul proprio computer di casa (naturalmente in questo caso alcune funzionalità dovranno essere per forza di cose "simulate", non avendo a disposizione l'hardware necessario).

Se si cerca il significato letterale della parola "gateway" esso si riconduce essenzialmente a "strada" o in modo più generalizzato, "ingresso" o "uscita". In un certo senso, il significato della parola "gateway" dal punto di vista informatico, è lo stesso. Il significato che se ne dà parlando di internetworking è di strumento, hardware o software, per connettere due o più reti diverse [1]. In seguito, con l'avvento delle reti TCP/IP, il nome "gateway", usato nel mondo della ricerca è stato sostituito dal termine "router" da parte delle aziende produttrici di hardware. Lo stesso termine "gateway", comunque, è utilizzato anche per descrivere strumenti che forniscono funzioni di interconnessione (ad esempio "mail gateway" o "SMS gateway") tra sistemi software. Con "gateway multifunzione", quindi, si intende descrivere un prodotto hardware/software che fornisce sia la funzione propriamente svolta da un router, e cioè quella di instradamento di dati su reti diverse, che la funzione di interconnessione di sistemi software.

LA SITUAZIONE INIZIALE

L'azienda in cui è stato installato il sistema aveva la struttura riportata nella figura 1. La rete informatica è divisa in due parti: una dislocata in Veneto, comprendente circa 50 personal computer, due server con sistema operativo Windows NT e un IBM AS/400 per il sistema gestionale; l'altra in Lombardia, formata da circa 10 personal computer e un server Windows NT. Il collegamento fra le due reti è realizzato tramite un collegamento dedicato con una velocità di 128Kbps e due router IP. I due server della rete più grande, che in seguito chiameremo "principale", effettuano rispettivamente la funzione di file server, print server, proxy server e mail server il primo, fax server il secondo. I prodotti utilizzati sul primo server, che è l'unico che subirà modifiche con l'introduzione del gateway multifunzione, sono Microsoft Windows NT 4.0 Server, Microsoft Proxy Server 2.0 e Lotus Domino 4.5. Il server Domino viene utilizzato solo per la gestione della posta elettronica interna: ogni utente della rete ha una casella postale personale.

I client sono tutti PC con Microsoft Windows 95 e 98.

La funzione della interconnessione delle due reti LAN è quella di utilizzare lo stesso software gestionale che gira sull'unico AS/400 dislocato nella rete principale. La velocità offerta dal collegamento è buona, in quanto la banda necessaria per il collegamento con l'AS/400, utilizzando il software di emulazione terminale IBM Client Access, è molto ridotta. Il collegamento ad Internet è effettuato tramite un router ISDN collegato ad una seconda scheda di rete del primo server. Il router esegue il call on demand (chiamata su richiesta) quando il software Proxy Server ha bisogno di scaricare dati dalla rete per soddisfare le richieste dei client. Per un confronto preciso con la soluzione che verrà svolta dal gateway multifunzione, è necessario puntualizzare che, anche se il software di Microsoft permette di memorizzare in una cache le pagine web già viste in modo che un eventuale ulteriore richiesta delle stesse informazioni venga gestita localmente, in azienda tale funzionalità era disabilitata per non sprecare spazio su disco e per non rallentare il funzionamento del server che svolge altre funzioni ritenute più importanti, quali quelle di file server e print server. Il collegamento ad Internet viene utilizzato per consultare pagine web e soprattutto per ricevere ed inviare

la posta elettronica con caselle sul dominio della società, ospitate da un Internet Service Provider locale e gestite, con protocollo SMTP per la spedizione e POP3 per la ricezione, direttamente dai client di posta elettronica Lotus Notes. Le due reti utilizzano indirizzi facenti parte del pool di indirizzi riservati per l'uso interno; in particolare, la rete primaria ha indirizzi 192.168.100.0/24 e l'altra ha indirizzi 192.168.200.0/24. I default gateway delle due reti LAN sono rispettivamente i due router della connessione dedicata, 192.168.100.254 e 192.168.200.254. I client raggiungono Internet tramite il Proxy Server, che ha indirizzo 192.168.100.1, specificato nella configurazione di rete di Windows (il software del Proxy Server prevede un componente da installare sui client che redirige le richieste winsock verso il proxy server)[2].

OBIETTIVI

Nei primi tempi, l'azienda era soddisfatta della situazione in quanto lo scopo primario, di utilizzare lo stesso gestionale in entrambe le sedi, era raggiunto in modo efficiente e l'utilizzo della posta elettronica era sufficientemente ridotto da poter essere gestito tramite la linea ISDN con chiamate regolari al provider per l'invio e la ricezione dei messaggi. Naturalmente, con l'evolversi di Internet, l'uso da parte dell'azienda della posta elettronica e il numero stesso delle caselle, aumentò in modo considerevole. Si presentò quindi l'esigenza di migliorare la velocità di accesso ad Internet. Contemporaneamente, si notava che poteva essere altresì interessante gestire la posta elettronica interna in modo analogo a quella esterna, senza una inutile duplicazione di indirizzi che porta ad inefficienze e facili errori. Anche la navigazione sul web era aumentata a causa dell'uso massiccio dei siti web da parte dei fornitori. Come ultima esigenza, infine, era auspicabile una maggiore immediatezza nella ricezione dei messaggi di posta in arrivo dall'esterno.

LA SOLUZIONE PROPOSTA

La soluzione che è stata proposta per migliorare la situazione è stata quella di inserire nella struttura di rete un server Linux configurato come gateway multifunzione e l'installazione di una linea di connessione ad Internet ad alta velocità di tipo always-on. Ciò avrebbe garantito la possibilità di gestire in modo diretto la posta elettronica per il dominio della società e quindi a spedire e ricevere i messaggi email in tempo reale. La scelta è ricaduta su un collegamento HDSL con banda garantita di 1Mbps e picchi di 2Mbps e la disponibilità di 8 indirizzi IP pubblici statici (in realtà gli indirizzi utilizzabili dall'azienda sono solo 5, essendo il primo indirizzo riservato alla rete, l'ultimo al broadcast e uno al router HDSL). Con tale banda a disposizione, anche i siti più pesanti possono essere scaricati in poco tempo e i grossi messaggi di email non sono più un problema. La struttura della rete diventò quella attuale, riportata in figura 2.

IL SERVER LINUX EFFETTUA LE SEGUENTI FUNZIONI:

- Firewall
- DNS server
- Mail relay server
- Router con NAT

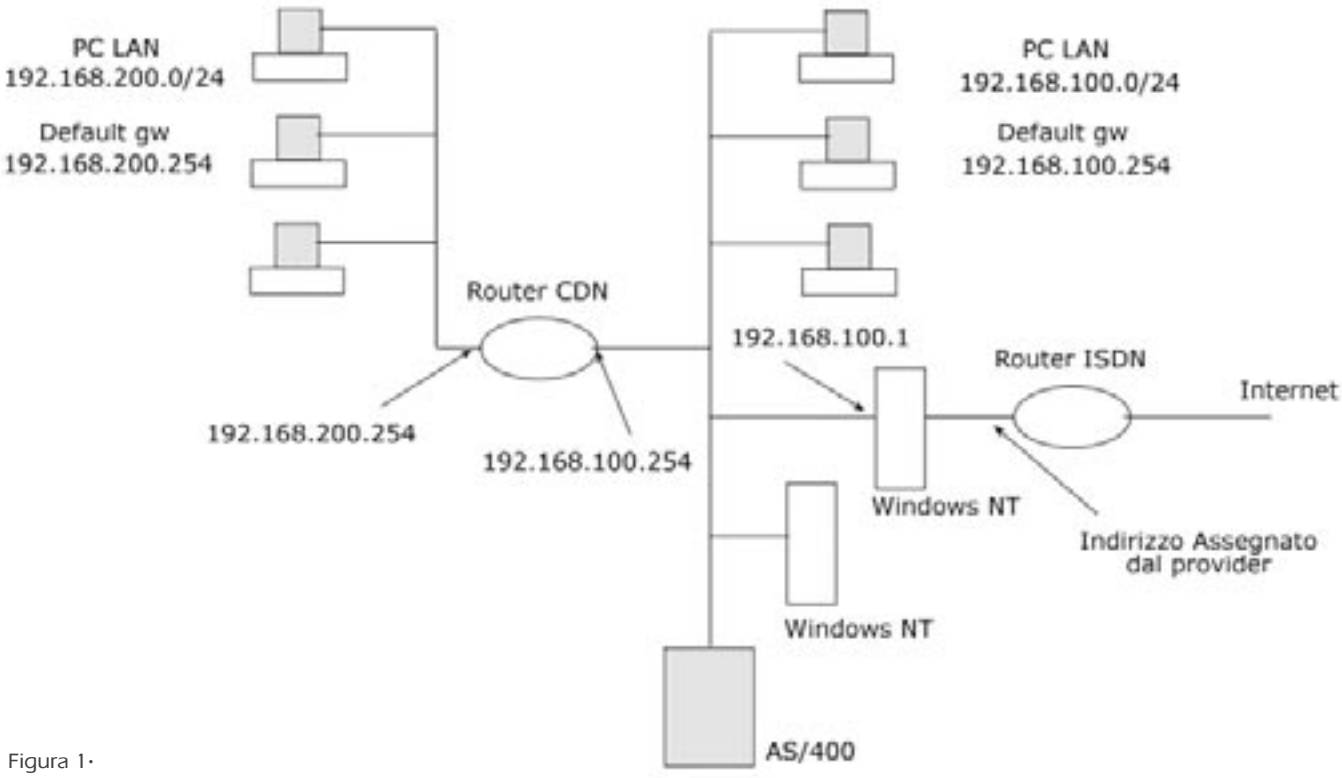

Figura 1·

I prodotti utilizzati per le funzioni sopraccitate sono: Kernel con Masquerading per la funzionalità di Router con NAT, ipchains e PortSentry per la funzionalità di Firewall, BIND 9 per la funzionalità di DNS server e Sendmail V8.9 per la funzionalità di Mail relay. E' stata utilizzata una distribuzione Redhat 6.1, con kernel 2.2.16 in quanto il kernel fornito con la distribuzione è affetto da un grave bug che ne compromette la sicurezza. Naturalmente sono stati utilizzati altri software di rifinitura che saranno descritti nella sezione relativa alla realizzazione del sistema. Sommariamente, l'installazione del sistema è consistita in: preparazione del server con l'installazione di due schede di rete, installazione del sistema operativo, installazione del nuovo kernel, ricompilazione del kernel, configurazione dei servizi, installazione dei software necessari allo svolgimento delle funzionalità server, configurazione del routing, configurazione del firewall, testing e messa in opera. Il tutto è stato svolto in due giorni di lavoro, creando minime disfunzioni agli utenti.

REALIZZAZIONE CONFIGURAZIONE HARDWARE

Prima di iniziare ad installare il software sono stati analizzati i requisiti hardware che il server utilizzato doveva avere. Il sistema operativo Linux non è molto esigente in termini di memoria RAM e pertanto è stato utilizzato un modulo da 128 MByte e una partizione di swap altrettanto grande.
Il processore del server è un Intel Pentium III con una frequenza di clock di circa 700Mhz, più che sufficiente per il carico di lavoro richiesto. Il disco utilizzato è un IDE con capacità di circa 20 GByte, molti dei quali inutilizzati.
Sono state installate due schede di rete uguali della 3COM, più precisamente due 3C905B-TX, da molto tempo riconosciute dal kernel di Linux. Una scheda di rete verrà utilizzata per il collegamento con la LAN principale, l'altra per il collegamento al router HDSL che instraderà il traffico verso Internet.
Dovendo fare un'analisi approfondita, data l'importanza della macchina, probabilmente potrebbe essere opportuno utilizzare un server con ridondanza, sia nei dischi che nell'alimentazione.

INSTALLAZIONE DEL SISTEMA OPERATIVO

L'installazione del sistema operativo utilizzando il CD-ROM di RedHat è molto semplice. E' stata utilizzata l'installazione di tipo 'Custom' che permette di selezionare i sottosistemi da installare. In particolare sono stati esclusi dall'installazione tutti i servizi server non richiesti (FTP, Samba, News, ecc.) e il sistema X Windows (davvero inutile su un server!). Il kernel è stato ricompilato escludendo le parti non utilizzate in modo da ridurne il peso. Tutte queste procedure sono probabilmente conosciute alla maggior parte degli utilizzatori del sistema operativo Linux e pertanto non saranno descritte nel dettaglio.

CONFIGURAZIONE DEL SISTEMA OPERATIVO

Terminata l'installazione del sistema, il primo passo necessario consiste nel configurare i sottosistemi che sono eseguiti all'avvio. Il sistema RedHat utilizza file di avvio di tipo System V con una suddi-

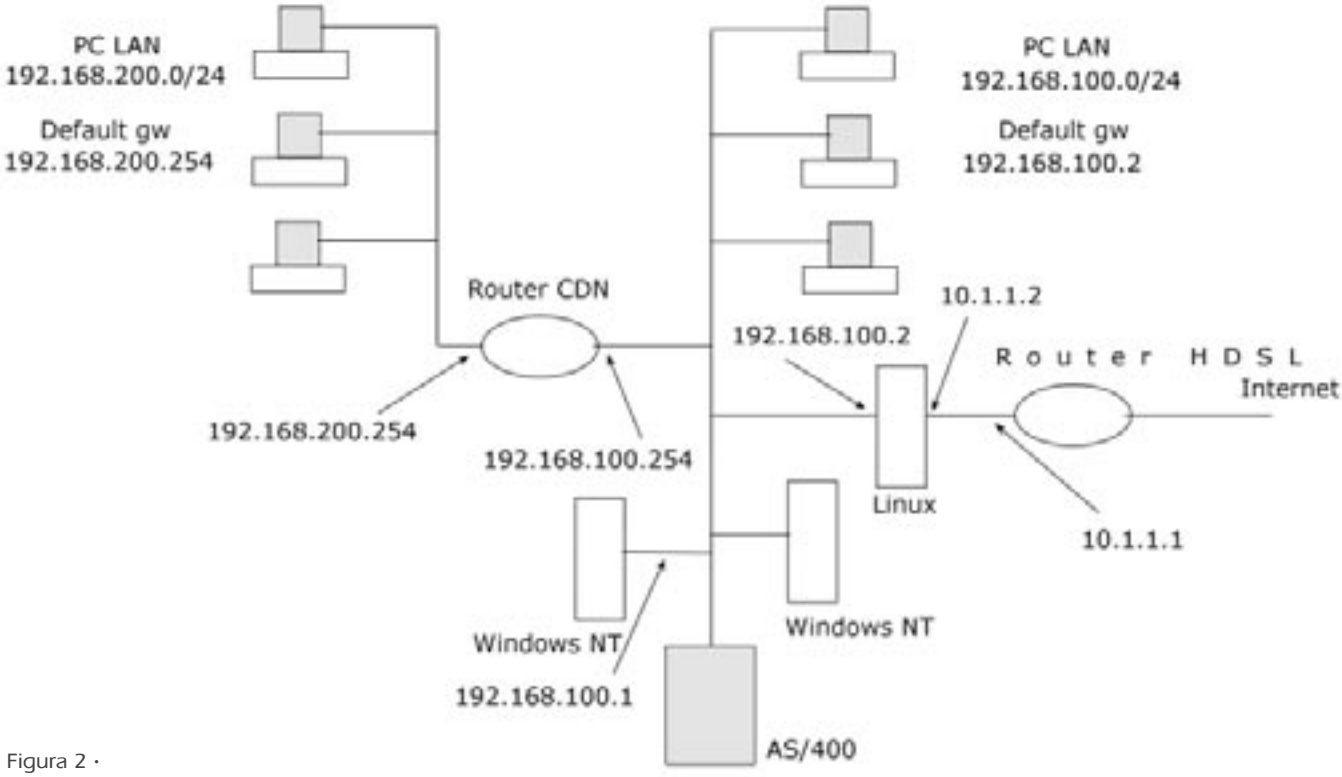

Figura 2 ·

visione in 'run-level' [3]. Ogni run-level corrisponde ad un tipo di utilizzo della macchina e prevede l'avvio di un ben definito gruppo di servizi. Generalmente nella cartella /etc/rc.d sono contenute alcune directory del tipo rcn.d ove 'n' e' il numero di run-level. I run-level che ci interessano sono 3, 6 e 0. Il run-level '3' generalmente corrisponde alla modalità 'multiutente testo'. Il run-level '6' rappresenta il reboot mentre lo '0' rappresenta l'arresto del sistema. All'interno delle directory rcn.d ci sono normalmente dei soft-link (i collegamenti ottenuti con il comando 'ln –s') a degli script contenuti in /etc/rc.d/init.d che hanno nomi del tipo Snnxxxx e Knnxxxx, ove 'nn' è un numero da 00 a 99 e 'xxxx' è una stringa di caratteri che identificano il servizio. Lo script di avvio, una volta determinato il run-level di default da utilizzare leggendo il file /etc/inittab esegue gli script contenuti nella corrispondente directory /etc/rc.d/rcn.d, in ordine di nome descrescente quelli con nome che inizia per 'K', e crescente quelli con nome che inizia per 'S'. Agli script 'K' viene passato in riga di comando un parametro 'stop' mentre ai file 'S' viene passato il parametro 'start'. In questo modo, è possibile decidere quali servizi sono eseguiti all'avvio del sistema, e in quale ordine. I file con nome che inizia per 'K' (Kill) sono eseguiti per primi e vengono utilizzati per terminare i processi che non devono girare nel run-level corrispondente. I file che iniziano per 'S' (Start) vengono eseguiti in seguito e servono per eseguire i processi che devono essere attivi nel run-level. I file sono marcati come eseguibili e per disattivarli è sufficiente marcarli come non eseguibili (chmod –x nomefile) oppure cancellarli, visto che in ogni caso, trattandosi solo di soft link, il file cui puntano non viene rimosso. Personalmente l'autore preferisce eliminarli, per avere una visione chiara dei processi che sono eseguiti all'avvio, facendo un list della directory corrispondente al run-level.
L'installazione di default esegue all'avvio molti sottosistemi, parecchi dei quali sono inutili o addirittura dannosi per la funzionalità che ci interessa. In particolare, sono stati disabilitati i servizi 'kudzu', 'portmap', 'nfslock', 'apmd', 'netfs', 'pcmcia', 'lpd', 'xfs', 'linuxconf'. Il servizio 'kudzu' permette il riconoscimento di nuovo hardware e la sua configurazione. Poiché può interrompere il boot del sistema, se vengono rilevate delle differenze hardware rispetto al boot precedente (per esempio se viene staccato il mouse), non è adatto ad un server che deve riprendere a funzionare immediatamente e senza l'intervento dell'utente dopo un eventuale spegnimento accidentale.
Il servizio 'portmap' è utilizzato dai software che fanno uso delle RPC (Remote Procedure Call) ed è stato per anni bersaglio di hacker a causa di alcuni famosi bug. Poiché nessun sottosistema installato fa uso di RPC è quindi bene disabilitarlo. Il servizio 'nfslock' viene utilizzato solamente se si installa il Network File System. Poiché non è il nostro caso, è stato rimosso. Lo script 'apmd' esegue del software per il controllo dei consumi (Advanced Power Management). In un server è sicuramente fuori luogo e pertanto viene disabilitato. Lo script 'netfs' esegue i server di Samba e di NFS, nel nostro caso non necessari.
Lo script 'pcmcia' è utilizzato solamente nel caso in cui vi siano delle schede PCMCIA nella macchina e generalmente nei server non viene utilizzato.
Un altro servizio affetto da bug legati alla sicurezza è il servizio 'lpd' utilizzato per la gestione della stampante. Il nostro server non ha alcuna necessità di stampare o di offrire servizi di stampa ad altre macchine e pertanto il servizio viene disabilitato. Lo script 'xfs' esegue il server dei font utilizzato dal sistema X Windows che non abbiamo neppure installato. Infine, 'linuxconf' è un software per la configurazione del sistema operativo, anch'esso affetto da bug molto ricercati dagli hacker. Visto che l'autore si trova più a suo agio con il 'vi', il servizio è stato disabilitato.
Dopo questa lunga descrizione dei servizi disabilitati, ecco l'elenco dei servizi che invece sono indispensabili e che pertanto sono lasciati inalterati: 'network', 'random', 'syslog', 'identd', 'atd', 'crond', 'inet', 'keytable', 'gpm', 'local'. Senza entrare nel dettaglio di ogni singolo servizio, essi sono tutti servizi indispensabili per un corretto funzionamento del sistema operativo e dei software che dovranno girare sul server. Unica concessione il servizio 'gpm', comodo per eseguire dei rapidi copia-incolla utilizzando il mouse.
L'operazione di pulizia non è ancora terminata in quanto alcuni servizi sono lanciati dal software 'inetd' che ha un suo specifico file di configurazione che è bene modificare. Il file in questione è /etc/inetd.conf e contiene un elenco di servizi di rete che sono eseguiti su richiesta e non all'avvio della macchina. Esempi tipici di server eseguiti dal servizio inetd sono finger, talk, pop3, ecc.
Nel nostro sistema, tutti i server presenti nel file inetd non sono utilizzati e pertanto disabilitiamo la loro esecuzione commentando nel file di configurazione le righe ad essi corrispondenti, anteponendone il carattere '#'. Ci si potrà chie-

```
options {
      directory "/var/named";
      allow-transfer {10.50.100.200;
10.50.100.201;};
      listen-on-v6 { none; };
};

zone "." {
      type hint;
      file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
      type master;
      file "named.local";
};

zone "100.168.192.in-addr.arpa" {
      type master;
      file "192.168.100";
};

zone "200.168.192.in-addr.arpa" {
      type master;
      file "192.168.200";
};

zone "1.1.10.in-addr.arpa" {
      type master;
      file "10.1.1";
};

zone "azienda.com" {
      type master;
      file "azienda.com";
};
```

Listato 1 · File /etc/named.conf

dere come mai il servizio 'inet' che esegue il server inetd viene utilizzato se tutti i suoi servizi sono disabilitati. Effettivamente, sarebbe possibile disabilitarlo (quindi rimuovere il link /etc/rc.d/rc3.d/Snninetd) se non sia ha bisogno di aggiungere servizi in seguito. Il principio di disattivare tutti i servizi non strettamente necessari è un vecchio principio della gestione della sicurezza ed è bene applicarlo su ogni macchina, connessa o meno ad Internet [4].

Installazione e configurazione dei software aggiuntivi

Come anticipato, è stato necessario scaricare alcuni software da Internet per poter completare l'installazione e rendere operativo il sistema.

SERVIZIO DNS

Il servizio DNS è uno dei servizi fondamentali di Internet. Una delle funzioni espletata dai server DNS è quella di permettere la risoluzione dell'indirizzo IP a partire da un nome con una struttura gerarchica. Anche i server DNS hanno una struttura gerarchica: vi sono server di primo livello, server di secondo livello, ecc. La risoluzione del nome viene effettuata facendo delle richieste ai server DNS dei vari livelli. Per esempio, per risolvere il nome 'azienda.com' la libreria software che effettua la risoluzione, prima effettua una richiesta ad uno dei server che gestisce il dominio di primo livello '.com'. Il server interpellato risponderà con un elenco di server DNS di secondo livello cui fa riferimento il dominio 'azienda.com'. A questo punto la libreria andrà ad interrogare uno dei server ottenuti per avere la risposta richiesta. Fortunatamente un server DNS può gestire più di un dominio, o addirittura più livelli. Un'altra funzione svolta dal server DNS viene utilizzata dai sistemi di gestione della posta elettronica. Vi siete mai chiesti come fa un server di posta a conoscere qual'è il server che gestisce la posta di un determinato dominio? La risposta è abbastanza semplice: basta chiederlo ad un server DNS!
Il sistema gateway è stato utilizzato come DNS server per entrambe le reti; in questo modo, eventuali richieste multiple di risoluzione di nomi vengono risolte con un unico accesso alla rete. Inoltre, il gateway svolge la funzione di DNS primario per il dominio Internet dell'azienda. Il software utilizzato come DNS server è BIND. La versione compresa nel CD del sistema operativo RedHat utilizzato è affetta da un grave bug inerente la sicurezza e poiché il gateway ha il servizio DNS esposto su Internet, è stata scaricata ed installata la versione 9 che corregge il problema. BIND è distribuito dall' Internet Software Consortium, all'indirizzo http://www.isc.org. Dopo aver scaricato i sorgenti e compilato il software, aiutati dall'immancabile file 'README', l'installazione prosegue con l'editing dei file di configurazione [5]. Vi sono alcuni files interessati dalle nostre modifiche; vediamo in dettaglio la struttura di tali files. Il file /etc/named.conf rappresenta la configurazione del server DNS. E' necessario editare tale file per configurare il servizio DNS. Il file utilizzato nell'installazione descritta in questo articolo è riportato nel listato 1. Nel seguito assumeremo che il dominio dell'azienda sia 'azienda.com' e che gli indirizzi pubblici offerti dal collegamento HDSL siano 10.1.1.0/24. Inoltre, assumiamo che l'indirizzo pubblico del gateway sia 10.1.1.2 . La prima parte del file, racchiusa dalla keywork options permette di specificare molte opzioni sul funzionamento del server, tra cui: le interfacce su cui dovrà collegarsi il servizio (in un server dotato di più indirizzi IP), il grado di sicurezza da utilizzare e cose più banali come la directory in cui sono contenuti i files citati nel seguito. Le opzioni utilizzate nella configurazione del gateway sono: directory "/var/named" che identifica la directory /var/named come directory di default per i files citati in seguito; allow-transfer {10.50.100.200; 10.50.100.201;}; che identifica l'IP 10.50.100.200 e 10.50.100.201 come gli unici indirizzi che possono effettuare un 'zone transfer', cioè un'interrogazione completa su tutta la zona; infine listen-on-v6 { none; }; configura il server per non utilizzare il protocollo IPv6. Vale la pena notare che l'opzione 'allow-transfer', utilizzata poco spesso dagli amministratori di sistema, è invece importante per non concedere troppe informazioni sulla rete ad un potenziale hacker che intende attaccarci. Infatti, l'operazione di zone transfer permette, con un solo comando, di ottenere tutti gli indirizzi IP e i relativi nomi della rete gestita dal server DNS, nonchè tutte le informazioni aggiuntive. Normalmente è bene abilitare al zone transfer solo altri server DNS che effettuano il back-up del dominio, ad esempio i DNS secondari.
Il file /etc/named.conf è poi suddiviso in sezioni, dette 'zone'. Ogni zona rappresenta una serie di indirizzi IP o il loro equivalente nome. Consultando il listato, si possono notare le seguenti zone: 0.0.127.in-addr.arpa, 100.168.192.in-addr.arpa, 200.168.192.in-addr.arpa, 0.1.1.10.in-addr.arpa, azienda.com.
La zona 'azienda.com' è utilizzata per la risoluzione dell'indirizzo IP a partire dal nome, per tutto il dominio azienda.com e per definire il server di posta per le caselle del tipo 'nome@azienda.com'.
Le altre zone sono utilizzate per la risoluzione inversa dal numero IP all'indirizzo per le reti 127.0.0.0/8, 192.168.100.0/24, 192.168.200.0/24 e 10.1.1.0/24. La struttura di un file di zona per la risoluzione dei nomi è rappresentata nel listato 2. Il file contiene informazioni relative ai nomi del dominio, ai name server, ai server di posta. Potrebbero essere inserite molte altre informazioni sulla struttura della rete che comunque, normalmente, non vengono utilizzate. La prima riga, $TTL 86400 definisce il Time To Live per il dominio, cioè il tempo massimo che un server DNS può mantenere in cache un dato relativo al dominio. Oltrepassato il TTL, il server che dovesse rispondere ad una interrogazione relativa al dominio, è costretto a reinterrogare il DNS che gestisce il dominio. La funzione del TTL è abbastanza ovvia, se un server mantenesse in cache per sempre i dati relativi ad un dominio, eventuali modifiche non sarebbero mai propagate al

resto della rete. Il tempo è espresso in secondi; 86400 secondi sono esattamente 24 ore. Le righe successive definiscono il record SOA (Start Of Authority) in cui sono presenti diverse informazioni. Innanzitutto si noti che il carattere '@' rappresenta il dominio, nel nostro caso azienda.com. La dicitura 'IN' sta per Internet e 'SOA' identifica il record SOA (banale no?). A seguire troviamo il nome del name server primario per questo dominio e l'indirizzo di posta elettronica dell'amministratore. Si notino due particolari: nell'indirizzo di posta elettronica, il carattere '@' è sostituito da un '.'; ogni nome di domino termina con un '.'. Se i nomi non dovessero terminare con un '.' verrebbe automaticamente aggiunto il nome di domino alla fine. Pertanto, scrivere 'gateway.azienda.com.' oppure 'gateway' è analogo mentre scrivendo 'gateway.azienda.com' (senza il punto finale) verrebbe interpretato come 'gateway.azienda.com.azienda.com' che non è esattamente quanto ci si potrebbe aspettare. L'elenco di numeri che seguono impostano alcuni parametri del record SOA. Il primo numero è il numero seriale del record; questo numero è utilizzato dal server DNS per verificare se ci sono state delle modifiche nel file che devono essere ricaricate. Generalmente viene utilizzato un numero del tipo yyyymmggss ove yyyy, mm, gg sono rispettivamente l'anno, il mese ed il giorno di modifica del file; ss è un progressivo che può essere usato nel caso in cui vengano effettuate più modifiche nello stesso giorno. Comunque l'importante è che il numero cresca quando il file viene cambiato, ed infatti alcuni amministratori usano un semplice contatore del tipo 1,2,3, ecc... Il secondo numero rappresenta il tempo dopo il quale i server DNS secondari devono rinfrescare la propria cache. Un tempo di 28800 secondi significa che ogni 8 ore i server DNS secondari per il dominio interrogheranno il server primario per ottenere le eventuali modifiche. Per completezza, è bene citare che a partire da BIND v8, quando un server primario rileva delle modifiche ad un dominio, viene inviato un segnale ai name server secondari per informarli delle modifiche. Il terzo numero rappresenta il tempo che un server secondario deve attendere prima di effettuare un altro refresh, nel caso in cui il refresh di cui sopra non dovesse avvenire per qualche malfunzionamento. Il quarto numero è il numero di secondi dopo i quali i server secondari smettono di rispondere a richieste inerenti al dominio nel caso in cui tutti i tentativi di refresh effettuati siano falliti. Nel nostro caso, 360000 secondi rappresentano 100 ore, cioè circa 12 tentativi di refresh. L'ultimo numero rappresenta il minimo TTL consentito. Scorrendo il contenuto del file, successivamente al record SOA troviamo i record NS (Name Server) che rappresentano i nomi dei name server del dominio. Nel nostro caso abbiamo citato il server primario, gatweway.azienda.com ed un name server secondario, dns.provider.it . Successivamente il record MX (Mail Exchange) identifica il server di posta per il dominio. E' possibile specificare diversi server distinti da una preferenza numerica. Numeri più bassi significano una preferenza maggiore. Nel caso in cui il server di preferenza maggiore non sia disponibile, la posta viene dirottata sugli altri sever, in ordine di preferenza. Nel nostro caso, l'unico server utilizzato è il nostro gateway. Si noti che nelle righe NS e MX non si è utilizzato il carattere '@'. Il fatto è dovuto all'utilizzo di un'altra abbreviazione che consente di lasciare in bianco il campo se è uguale a quello della riga precedente. Infine troviamo l'elenco dei record A (Address) che rappresentano gli indirizzi corrispondenti ai nomi. Nel nostro caso, il nome router.azienda.com corrisponde all'indirizzo 10.1.1.1 mentre il nome gateway.azienda.com corrisponde all'indirizzo 10.1.1.2 . La struttura di un file per la risoluzione inversa è riportata nel listato 3. Come si può facilmente notare, vi sono poche differenze tra i due tipi di file: non è presente il record MX e l'in-

```
$TTL 86400
@   IN   SOA   azienda.com. admin.azienda.com.  (
                          2002010101 ; Serial
                          28800      ; Refresh
                          14400      ; Retry
                          360000     ; Expire
                          86400 )    ; Minimum

      IN     NS      gateway.azienda.com.

1     IN     PTR     router.azienda.com.
2     IN     PTR     gateway.azienda.com.
```

Listato 2 · File /var/named/azienda.com

```
$TTL 86400
@       IN      SOA     gateway.azienda.com. admin.azienda.com.  (
                              2002010101 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              360000     ; Expire
                              86400 )    ; Minimum

            IN      NS      gateway.azienda.com.
            IN      NS      dns.provider.it.

            MX      10      gateway.azienda.com.

router.azienda.com.     IN          A       10.1.1.1
gateway.azienda.com.    IN          A       10.1.1.2
```

Listato 3 · File /var/named/10.1.1

dicazione della corrispondenza indirizzo-nome è descritta dai record PTR.
Rimane da configurare un ultimo parametro. Come anticipato in precedenza, un server DNS deve essere in grado di comunicare con speciali server DNS che contengono le informazioni relative ai domini di primo livello come, ad esempio, ".it", ".com", ecc… .
Esistono alcuni server DNS, detti 'root-servers' che svolgono esattamente questa funzione. L'elenco di tali server e' contenuto nel file che rappresenta la zona ".", nel nostro caso "named.ca".
Il contenuto del file è presentato nel listato 4. Il file è ottenibile facilmente utilizzando un programma distribuito insieme a BIND: il comando 'dig'. Lanciando il comando 'dig @a.root-servers.net . ns > named.ca' si ottiene proprio il file richiesto. I più attenti si staranno chiedendo come fa il server DNS a risolvere il nome a.root-servers.net se non ha ancora ottenuto il file che contiene i nomi dei root servers.
Effettivamente, la prima volta è necessario scaricare il file da un sito ftp, più precisamente 198.41.0.6 che corrisponde a ftp.rs.internic.net. Il comando dig è utile per mantenere valida la lista dei server e andrebbe utilizzato di tanto in tanto (oppure schedulato tramite crontab). La configurazione di BIND è terminata. E' ora possibile impostare nella struttura di avvio System V un collegamento che esegua il server all'avvio. Nella distribuzione installata, nella directory /etc/rc.d/init.d esiste un file 'named' cui bisogna effettuare un link simbolico nella directory /etc/rc.d/rc.3.d come descritto in precedenza.Una buona posizione per avviare il name server è dopo l'inizializzazione della rete TCP/IP ma prima di qualsiasi servizio che potrebbe richiedere la risoluzione di un nome. E' opportuno, inoltre, notare due cose: il nome del programma è named (name server daemon) e non bind; se nel sistema operativo era già stato installato BIND versione 8, bisogna fare attenzione nel lanciare il server corretto all'avvio. E' sufficiente verificare dove è stato installato BIND 9 e modificare di conseguenza lo script di avvio.

Ora che il DNS server è configurato è possibile contattare l'attuale gestore del dominio dell'azienda per accordarsi sullo spostamento del DNS primario sulla macchina gateway.

SERVER SMTP

Il protocollo SMTP, Simple Mail Transfer Protocol, viene utilizzato per scambiare messaggi di posta elettronica. Generalmente i server che gestiscono la posta elettronica si scambiano messaggi utilizzando il protocollo SMTP mentre i client spediscono la posta tramite SMTP ma la leggono tramite POP3 (Post Office Protocol) oppure IMAP (Internet Mail Application Protocol).
Un messaggio di posta elettronica, quando viene spedito dal mittente, attraversa un certo numero di server SMTP prima di giungere nella cassetta postale del destinatario. Nel caso più semplice, in cui sia il mittente che il destinatario operano su server direttamente collegati ad Internet, non ci sono passaggi intermedi a meno che non ci siano delle disfunzioni della rete di collegamento, nel qual caso un server di backup potrebbe essere utilizzato per la spedizione del messaggio. Nei casi più complessi, gli utenti potrebbero spedire messaggi ad un server non pubblico, il quale a sua volta smista la posta verso un 'relay' che si incarica della consegna del messaggio. Il messaggio potrebbe poi transitare su diversi server nel caso in cui vi siano situazioni in cui dominio principale ed eventuali sottodominii utilizzino server SMTP diversi. Per fare un esempio chiarificatore, supponiamo che l'utente con indirizzo info@azienda.com spedisca un messaggio alla casella persona@amm.fornitore.it . Nel nostro caso, il server interno Lotus Domino, rileva che la casella di destinazione non è una casella interna e pertanto dirotta il messaggio verso il server di 'relay', cioè gateway.azienda.com, usando il protocollo SMTP. A sua volta, il server SMTP inoltra una richiesta al server DNS chiedendo i record MX per il dominio amm.fornitore.it . Il nostro server DNS utilizzando la procedura già descritta precedentemente, esegue alcune interrogazioni fino a quando non riesce ad ottenere quanto richiesto, che supponiamo sia 'mail.fornitore.it' con preferenza 10 e 'backupmail.fornitore.it' con preferenza 20. Il nostro server SMTP, a questo punto, inizia una connessione SMTP verso mail.fornitore.it per lo scambio del messaggio. Se lo scambio avviene con successo, sarà compito del server mail.fornitore.it consegnare il messaggio al destinatario; se invece per qualche motivo il server mail non fosse raggiungibile, verrebbe tentata una connessione con il server backupmail. L'esempio descritto chiarisce quindi che la funzione del server SMTP è abbastanza complessa, soprattutto se si pensa che tale funzione può essere effettuata per diversi domini di posta elettronica e per diversi metodi di trasmissione dei messaggi (ad esempio: SMTP, UUCP, sistemi proprietari tipo Microsoft Exchange, Lotus Domino, ecc…). Il software utilizzato come server SMTP nell'installazione del gateway è sendmail, distribuito su http://www.sendmail.org [6]. Il programma Sendmail contenuto nel CD del sistema operativo utilizzato è la v8.9.
Sendmail è stato molto criticato nel tempo per i problemi di sicurezza che lo hanno sempre afflitto; a questo proposito vale la pena di notare che tali situazioni si riferiscono spesso a configurazioni errate del sistema che, data la complessità del software, a volte consentono agli hackers di ottenere privilegi molto elevati. Per esempio uno degli exploit utilizzati dal famoso "Morris worm" [7], che nel 1988 rallentò fino quasi alla paralisi diversi mail server di Internet, utilizzò, tra le altre cose, il fatto che la versione di sendmail distribuita con il sistema operativo SunOS aveva il debug abilitato per default (fortunatamente per gli utenti linux, ultimamente gli hacker si sono concentrati su Microsoft Internet Information Server…). Il file di configurazione primario del programma sendmail è molto complesso (vista anche l'inerente complessità del ruolo svolto dal programma). Sono stati quindi sviluppati alcuni strumenti per la configurazione semplificata. Quelli utilizzati nell'installazione del gateway sono le macro 'cf' e

il software m4 (anch'esso distribuito insieme al sistema operativo). E' stato necessario installare il pacchetto di macro utilizzando un file rpm scaricato dal sito ftp.redhat.com; il file normalmente viene chiamato sendmail-cf.rpm o con nomi analoghi. La directory di installazione di default è '/usr/lib/sendmail-cf' ove si trovano alcune sottodirectory tra cui 'cf' e un corposo file README che descrive tutte le opzioni e le macro che possono essere utilizzate.
Il programma m4 permette di elaborare uno o più file di testo in ingresso trasformando le macro in essi contenute e generando un file di testo di uscita. Il file di configurazione utilizzato è riportato nel listato 5. Normalmente il file di configurazione viene memorizzato all'interno della directory '/usr/lib/sendmail-cf/cf' ed ha estensione 'mc'. Nel nostro caso abbiamo utilizzato il nome 'azienda.com.mc'.
Vediamo il significato delle linee di configurazione del file utilizzato.
La macro include(`/usr/lib/sendmail-cf/m4/cf.m4') include alcune definizioni di default nel file.

La macro
define(`confDEF_USER_ID',``8:12'')
permette di specificare il nome utente ed il gruppo da utilizzare per default. Il programma sendmail svolge alcune delle sue attività come utente root, altre come l'utente cui è destinata la posta; quando i privilegi di root non sono necessari, ma non c'è alcun utente specifico da utilizzare per effettuare l'operazione in corso, sendmail utilizza l'utente ed il gruppo specificato da questa opzione. Nel nostro caso, lo userid 8 corrisponde all'utente 'mail'; il gruppo 12 al gruppo 'mail'.
La riga OSTYPE(`linux') serve per impostare alcuni parametri standard per i sistemi linux.
Le righe undefine(`UUCP_RELAY'), e undefine(`BITNET_RELAY') disattivano in sendmail il supporto per connessioni di tipo UUCP e BITNET.
La macro define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail') imposta il path per il programma 'procmail', utilizzato come local mailer cioè come software che si occupa della consegna dei messaggi destinati agli utenti locali.

La macro
FEATURE(`smrsh',`/usr/sbin/smrsh')
specifica che nelle operazioni che richiedano l'uso di una shell, deve essere utilizzata la shell smrsh (Sendmail Restricted Shell), una shell che non permette operazioni 'pericolose' dal punto di vista della sicurezza del sistema.
La riga FEATURE(`mailertable',`hash -o /etc/mail/mailertable') specifica che deve essere attivata la funzionalità 'mailertable' che permette di deviare la posta destinata su domini specifici verso agen-

```
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; End of File
```

Listato 4 - File /var/named/root.ca

ti di spedizione e server specifici. Questa è la funzione che sarà utilizzata per deviare tutta la posta in ingresso per azienda.com verso il server Lotus Domino interno. La configurazione di tale funzionalità è contenuta nel file /etc/mail/mailertable che vedremo in seguito. La riga FEATURE(local_procmail) consente di utilizzare il programma procmail come gestore della posta locale. Nel nostro caso, tale programma è usato solo per i messaggi che rimangono all'interno del gateway, ad esempio per i messaggi generati dal sistema cron verso l'utente root. Le righe MAILER(procmail) e MAILER(smtp) specificano che devono essere attivati gli agenti di spedizione procmail (per la posta locale) e smtp per la posta SMTP. Il file di configurazione di sendmail, normalmente '/etc/sendmail.cf', può essere generato con il comando 'm4 < azienda.com.mc > /etc/sendmail.cf' lanciato dalla directory '/usr/lib/sendmail-cf/cf'. Il file '/etc/mail/mailertable' contiene le istruzioni su come instradare la posta diretta verso il dominio azienda.com. Il file è costituito da una sola riga e precisamente 'azienda.com smtp:192.168.100.1'. Il significato di tale riga è che tutta la posta indirizzata al dominio 'azienda.com' deve essere instradata tramite SMTP al server 192.168.100.1, dove nel nostro caso gira Lotus Domino che naturalmente deve essere configurato per accettare la posta per il dominio azienda.com.
Un altro file importante è '/etc/mail/relay-domains' che contiene le righe
azienda.com
192.168.100.1

che significano che il server può essere utilizzato per spedire la posta da tutti gli IP del dominio azienda.com e dall'IP 192.168.100.1. Tale funzione è indispensabile per garantire la sicurezza del sistema e per non permettere ad estranei di usare il server di posta per spedire la propria posta o ancora peggio usare il nostro server per spamming. Ora che la configurazione di sendmail è terminata, è necessario configurare il suo avvio nella fase di bootstrap utilizzando il sistema già descritto per BIND. Sendmail può essere installato verso la fine della fase di boot, sicuramente dopo BIND. Naturalmente il sistema ottiene la piena funzionalità solo dopo che il dominio azienda.com è stato trasferito sul nostro server DNS (in alternativa è necessario far modificare il record MX al gestore del DNS). E' bene quindi, per non perdere messaggi di posta, controllare le caselle POP3 ancora per qualche giorno.

FIREWALL

Poichè il gateway è esposto su Internet 24 ore su 24 con un indirizzo IP pubblico, è buona cosa proteggerlo da tentativi di attacco tramite TCP/IP. Il software utilizzato a questo scopo è PortSentry, della Psionic Software Inc., distribuito su http://www.psionic.com/abacus/portsentry. Si tratta di un servizio che ascolta le comunicazioni su un certo numero di porte TCP e/o UDP ed esegue delle azioni se rileva connessioni su porte non consentite. L'installazione del gateway prevede una modalità in cui ogni attività, rilevata su porte di numero inferiore a 1024 e non abilitate a ricevere richieste, viene tracciata sul log di sistema e l'indirizzo IP da cui proviene la richiesta viene bloccato utilizzando una regola di IP Chains. Il software prevede alcune modalità operative su cui non ci soffermeremo molto visto che sono di semplice comprensione e sono dettagliate nei file di configurazione. Le tre modalità di risposta ad un tentativo di connessione sono le seguenti: ignora, blocca con TCP wrappers, blocca con IP Chains. E' inoltre possibile eseguire un programma esterno. Il software permette di ascoltare uno specificato insieme di porte, oppure di ascoltare tutte le porte in un certo intervallo, ad esclusione di quelle facenti parte di una apposita lista di esclusione e di quelle già utilizzate dai servizi attivi sul server. Dopo aver scaricato il software, è necessario compilarlo seguendo le istruzioni contenute nel file README. Una volta installato il programma, troveremo in /usr/local/psionic/portsentry alcuni files tra cui portsentry.conf che come è possibile immaginare è il file di configurazione del programma. Nel nostro caso, è stata usata la modalità di ascolto 'Advanced Stealth Scan Detection' che ascolta su un range di porte. Più precisamente, utilizzando la keyword ADVANCED_PORTS_TCP="nnnn", è possibile specificare l'ultima porta da ascoltare. La prima è la numero 1. Nel file di configurazione, quindi, deve essere presente una riga del tipo ADVANCED_PORTS_TCP="1023" che specifica l'ascolto sulle porte da 1 a 1023. E' opportuno disabilitare l'ascolto su alcune porte comuni tramite la keyword ADVANCED_EXCLUDE_TCP="n1,n2,n3,…". Ciò è necessario per non ricevere troppi allarmi nei file di log per applicazioni che non sono pericolose. Per esempio, è opportuno disabilitare l'ascolto sulla porta 113 (AUTH) e sulla porta 139 (NETBIOS) in quanto il transito di pacchetti su queste porte è abbastanza normale. La riga da utilizzare nel file di configurazione è ADVANCED_EXCLUDE_TCP="113,139". La modalità di risposta viene configurata con altre due keyword. Utilizzando la riga BLOCK_TCP=1 si specifica che gli indirizzi IP sorgenti dei pacchetti che giungono sulle porte abilitate alle rilevazioni devono essere filtrati. La riga KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l", invece, specifica che la modalità con cui filtrare l'indirizzo IP è quella di utilizzare una regola di IP Chains che filtra le connessioni provenienti dall'indirizzo sorgente del pacchetto e destinato al gateway, tenendone traccia nei log di sistema.
Vi sono alcune altre impostazioni da effettuare. La prima riguarda un file, normalmente /usr/local/psionic/portsentry/portsentry.ignore, che contiene gli indirizzi IP per i quali non bisogna mai intraprendere azioni nel caso in cui venisse rilevato un tentativo di comunicazione che ha uno di tali indirizzi come sorgente. E' opportuno inserire gli indirizzi della LAN all'interno di questo file per non consentire che un errore di configurazione o comunque una disattenzione nell'uso quotidiano dei sistemi porti al filtraggio di uno dei computer della rete

locale. Probabilmente, in situazioni in cui la sicurezza è di estrema importanza, è opportuno inserire in questo file solo l'indirizzo locale del server ma è bene tener presente che al minimo errore è necessario un intervento sul server per riportare in piena funzionalità il computer da cui è partito il tentativo di connessione. Se l'amministratore di rete non è sempre disponibile, questo può essere un problema. Nella stessa directory ci sono altri due files, portsentry.history e portsentry.blocked.atcp, che sono utilizzati per memorizzare lo storico degli IP bloccati e quelli bloccati a partire dall'ultimo reboot, rispettivamente. Infine l'opzione SCAN_TRIGGER="n" può essere utilizzata per consentire un numero 'n' di 'falsi allarmi' prima di lanciare l'azione di filtraggio. All'inizio della discussione del software Portsentry abbiamo specificato che ogni connessione su porte protette dal sistema avrebbe generato una riga di log di sistema. Per agevolare la consultazione di tali log, Portsentry può essere efficacemente affiancato dal programma LogCheck, distribuito sempre dalla Psionic, che permette di analizzare i file di log di sistema e di inviare una mail all'amministratore di rete contenente quanto rilevato. L'installazione del software pone in /usr/local/etc alcuni files. Il programma è costituito da uno shell script, logchech.sh, che deve essere modificato per impostare l'indirizzo di posta elettronica a cui spedire il report. E' sufficiente specificare nella riga SYSADMIN= l'indirizzo di posta ove si desidera spedire il report. Altri file specificano quali parole devono 'attirare' l'attenzione di logcheck. Nel file logcheck.hacking sono presenti le keyword che se trovate nel log file generano un allarme di tipo 'ACTIVE SYSTEM ATTACK!' che viene enfatizzato nel report; nel file logcheck.violations si trovano le parole che generano un allarme di tipo 'System Violations'. Nel file logcheck.violations.ignore e logcheck.ignore sono presenti le keyword che possono essere ignorate da logcheck. Per una descrizione più completa si può fare riferimento ai commenti nello stesso script logcheck.sh. Il file di configurazione portsentry.conf utilizzato nell'installazione del gateway è visibile nel listato 7. Per eseguire il programma portsentry all'avvio, è sufficiente inserire la riga /usr/local/psionic/portsentry –atcp all'interno del file /etc/rc.d/rc.local . E' buona cosa eseguire portsentry solo dopo aver avviato tutti i servizi del server. E' inoltre opportuno schedulare l'esecuzione di logcheck tramite il servizio cron. Per inserire una schedulazione ogni 4 ore, dalle 8:00 alle 20:00, si può inserire la riga 0 8,12,16,20 * * * /usr/local/etc/logcheck.sh nell'editor cron, crontab –e.

CONFIGURAZIONE DEL ROUTING

Come anticipato, il gateway svolge anche la funzione di router. Esso infatti instrada i pacchetti che hanno come sorgente un indirizzo della LAN e destinazione non locale verso Internet, dopo averne effettuato il masquerading, e i pacchetti verso la rete secondaria verso il router che governa la linea dedicata. Nel seguito descriveremo brevemente i passi da seguire per configurare il routing nel gateway. La discussione sarà meno dettagliata delle precedenti in quanto assumiamo un buona dimestichezza del lettore con il protocollo TCP/IP [8], i concetti di routing [9] e il software Ip Chains [4]. Prima di tutto è bene verificare che il kernel sia stato configurato abilitando il masquerading. Poi è necessario abilitare la funzione di forwarding, tramite il comando echo "1" > /proc/sys/net/ipv4/ip_forward
Il forwarding è utilizzato per instradare i pacchetti provenienti da un'interfaccia di rete verso un'altra interfaccia di rete. E' poi necessario abilitare il masquerading utilizzando IP Chains: /sbin/ipchains -A forward -i eth1 -s 192.168.100.0/24 -d ! 192.168.0.0/16 -j MASQ. In questo modo tutti i pacchetti che transitano attraverso il gateway provenienti da un indirizzo della rete principale e destinati ad un indirizzo non locale vengono mascherati e rediretti verso l'interfaccia eth1, che assumiamo sia l'interfaccia di rete con indirizzo 10.1.1.2 collegata al router HDSL. Per consentire l'utilizzo del protocollo FTP attraverso il masquerading è necessario eseguire il comando /sbin/modprobe ip_masq_ftp che attiva un plug-in per gestire il protocollo FTP; infatti il protocollo FTP utilizza due connessioni per il suo funzionamento e quindi il gateway deve predisporre l'accettazione di una connessione in ingresso a tale scopo. Per garantire la connettività con la rete secondaria, inoltre, è necessario impostare una route statica nella tabella di routing locale con il comando /sbin/route add -net 192.168.200.0 gw 192.168.100.254 netmask 255.255.255.0 che indirizza tutti i pacchetti destinati alla rete secondaria verso il router della linea dedicata. Per proteggere la rete interna, è bene bloccare il forwarding per default utilizzando il comando

```
include(`/usr/lib/sendmail-cf/m4/cf.m4')
define(`confDEF_USER_ID',``8:12'')
OSTYPE(`linux')
undefine(`UUCP_RELAY')
undefine(`BITNET_RELAY')
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')
FEATURE(`smrsh',`/usr/sbin/smrsh')
FEATURE(`mailertable',`hash -o /etc/mail/mailertable')
FEATURE(local_procmail)
MAILER(procmail)
MAILER(smtp)
```

Listato 5 · File /usr/lib/sendmail-cf/cf/azienda.com.mc

```
ADVANCED_PORTS_TCP="1023"
ADVANCED_EXCLUDE_TCP="113,139"
IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.ignore"
HISTORY_FILE="/usr/local/psionic/portsentry/portsentry.history"
BLOCKED_FILE="/usr/local/psionic/portsentry/portsentry.blocked"
BLOCK_TCP="1"
KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l"
SCAN_TRIGGER="0"
```

Listato 6 · File /usr/local/psionic/portsentry/portsentry.conf

/sbin/ipchains -P forward DENY. Se si utilizza ssh per l'accesso remoto al server dalla LAN e non si vuole esporre il servizio su Internet, è possibile filtrare le richieste provenienti dall'esterno e destinate sulla porta 22, utilizzata da ssh, con il comando /sbin/ipchains -A input –s ! 192.168.0.0/16 -d 10.1.1.2 22 -p tcp -j DENY –l. Ogni altro servizio che si desidera utilizzare sulla rete interna ma non esporre su internet dovrebbe essere trattato in modo analogo.

RAGGRUPPANDO QUANTO APPENA VISTO SI OTTIENE

```
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -i eth1 -s
192.168.100.0/24 -d ! 192.168.0.0/16 -j
MASQ
/sbin/ipchains -A input –s !
192.168.0.0/24 –d 10.1.1.2 22 -p tcp -j
DENY –l
echo "1" > /proc/sys/net/ipv4/ip_forward
/sbin/route add -net 192.168.200.0 gw
192.168.100.10 netmask 255.255.255.0
/sbin/modprobe ip_masq_ftp
```

che può essere inserito al termine del file /etc/rc.d/rc.local affinchè i comandi vengano eseguiti ad ogni boot. Si noti che il forwarding viene attivato solo dopo aver impostato i filtri necessari a garantire la sicurezza del sistema.

TESTING E MESSA IN OPERA

Al gateway è stato assegnato l'indirizzo locale 192.168.100.2. La messa in opera del sistema prevede la modifica dei default gateway sui PC della LAN. Il default gateway originario 192.168.100.254 deve essere sostituito con 192.168.100.2. In tal modo tutti i pacchetti non destinati alla rete LAN 192.168.100.0/24 vengono inviati al gateway che provvede a mascherarli e ad inviarli su Internet a meno che la destinazione non sia la rete secondaria, nel qual caso invia i pacchetti verso il router della linea dedicata. Sui PC della LAN è anche necessario configurare il server DNS con l'indirizzo IP del gateway.
Per testare il collegamento è sufficiente operare alcuni semplici comandi ping. Con ping 192.168.100.2 ci assicuriamo il funzionamento della connettività con la macchina gateway dal PC, con un ping su un'indirizzo della rete 192.168.200.0/24 controlliamo se viene effettuato il routing verso la LAN secondaria. Per testare la connessione verso Internet è sufficiente usare un browser e puntare sul nostro sito preferito … , non prima però di aver disinstallato il supporto per Microsoft Proxy Server da ogni client.

VANTAGGI OTTENUTI RISPETTO ALLA SOLUZIONE INIZIALE

Rispetto alla situazione iniziale sono stati ottenuti diversi miglioramenti:

- Velocità di accesso alla rete Internet
- Immediatezza nella ricezione e spedizione delle email
- Utilizzo di un unico server di posta interna/esterna.

Un fatto interessante che è stato rilevato riguarda le prestazioni del sistema di masquerading rispetto alla funzione svolta da Microsoft Proxy Server.
Inizialmente, essendo disponibile il collegamento HDSL prima dell'installazione del gateway, il server proxy era stato direttamente collegato al router HDSL in sostituzione del router ISDN.
La velocità di download di software, utilizzando siti "importanti" e quindi dotati di molta banda, aveva picchi di circa 110-120 Kbyte al secondo. Invece dopo l'installazione del gateway i picchi ottenuti sono stati di 190-200 Kbyte al secondo, quasi un 100% in più rispetto alla soluzione Microsoft e vicina ai limiti fisici della linea di trasmissione dati.
Come anticipato all'inizio dell'articolo, le funzionalità avanzate di Microsoft Proxy Server, quali la cache, erano disabilitate e pertanto le rilevazioni effettuate confermano che le prestazioni di Linux, nel controllo delle interfacce di rete, sono molto elevate rispetto agli altri sistemi disponibili.

Problemi riscontrati e soluzioni

Sono stati riscontrati alcuni problemi di ordine pratico e facilmente risolvibili che però è bene specificare.
Un primo problema riguarda l'identificazione delle schede di rete da parte del sistema operativo. Poiché si tratta di due schede identiche, per assegnare un nome di periferica e quindi identificare la funzione di scheda interna o scheda esterna è necessario effettuare alcune prove prima di configurare il sistema.
Collegando un cavo della rete LAN ad una delle schede ed effettuando dei ping è possibile rilevare quale delle due schede è stata configurata con gli indirizzi IP interni, inseriti in fase di installazione. A questo punto è sufficiente copiare e modificare gli script presenti in /etc/sysconfig/network per configurare anche la scheda esterna.
Un secondo possibile problema riguarda il fatto che per portare a termine la configurazione del gateway serve spesso una connessione ad Internet. Pertanto è necessario mantenere una connessione attiva da un PC oppure preparare tutto il software ed i files necessari in un CD.

Miglioramenti possibili

Possibili miglioramenti rispetto alla soluzione attuata riguardano l'eliminazione del server Lotus Domino e l'utilizzo di sendmail per la completa gestione della posta elettronica. In effetti questa è una direzione su cui l'azienda in cui è stata effettuata l'installazione si sta orientando, per due motivi:

- Scaricare il lavoro del file e print server;
- Eliminazione del client Lotus Notes dai PC e uso di Microsoft Outlook.

La scelta di utilizzare Microsoft Outlook, seppur "pericolosa" in quanto molti virus vengono scritti proprio per tale sistema di gestione di posta elettronica, consente agli utenti una maggiore semplicità d'uso in quanto utilizzerebbero lo stesso strumento che probabilmente usano nei propri PC di casa. ◀

L'autore

▸ ANDREA **VETTORI**

L'Autore Andrea Vettori, è Laureato in Ingegneria Informatica, utilizza Linux dal 1993. Nel 1999 fonda un Internet provider interamente basato su sistemi Linux. Attualmente fornisce consulenza su applicazioni Internet basate su sistemi Windows NT/2000 e Linux a medie aziende della provincia di Treviso.
Info:http://www.andreavettori.com