Firewall - NAT: definizione e configurazione sulla rete ILC

ILC-CED-2002-03

Alessandro Enea

Consiglio Nazionale delle Ricerche

Istituto di **L**inguistica **C**omputazionale

Alessandro.Enea@ilc.cnr.it

Dicembre 2002

Indice

1. Introduzione

I firewall sono dispositivi software o hardware posti a protezione dei punti di interconnessione eventualmente esistenti tra una rete privata interna (ad es. una Intranet) ed una rete pubblica esterna (ad. es. Internet), oppure tra due reti differenti.
Il firewall, la cui traduzione letterale è "parete tagliafuoco", deve svolgere due compiti fondamentali: prevenire intrusioni dall'esterno ed eventuali fuoriuscite indesiderate di informazioni dall'interno.
In Figura 1 vediamo una semplice schematizzazione della posizione di un firewall:

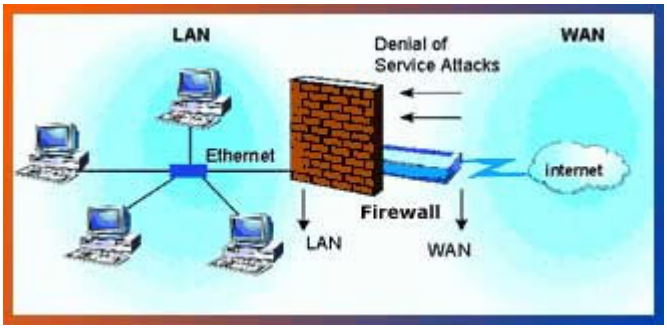

figura 1

In questo documento sono illustrate le funzioni fondamentali di un firewall e viene descritta la configurazione di un firewall con funzioni di NAT (Network Address Translation) attivo dal Maggio 2002 presso l'Istituto di Linguistica Computazionale.

2. Funzioni di un Firewall

Le diverse funzioni di un firewall possono essere raggruppate in queste categorie:

- Firewall per il Packet Inspection;
- Firewall come Filtro;
- Firewall come Gateway;
- Firewall per estensione della propria LAN.

Vediamole in dettaglio.

2.1 Firewall per il Packet Inspection

Un firewall è in genere in grado di analizzare il contenuto di ogni pacchetto che passa attraverso esso.
Questo è fondamentale per bloccare il traffico indesiderato o gli attacchi di hacker Internet senza complicare eccessivamente le configurazioni. Tipici esempi di Packet Inspection sono la possibilità di filtrare gli attacchi Internet di tipo "denial of service" (il firewall riconosce che è in corso un tentativo di attacco verso una macchina interna e lo blocca), la possibilità di verificare il sito in cui si sta navigando e il contenuto dello stesso per eventualmente bloccare o registrare comportamenti non consentiti. Il packet inspection è fondamentale per la realizzazione di un firewall di buon livello.

2.2 Firewall come Filtro

Un firewall è in grado di filtrare il traffico in base al tipo di protocollo, all'indirizzo della porta sorgente e all'indirizzo della porta di destinazione. Questa funzione è espletata anche da diversi tipi di router, per cui il vero vantaggio dei firewall in questo caso sta negli strumenti di

amministrazione e nel poter gestire tutte le varie funzionalità in modo centralizzato. In Figura 2 è schematizzato un esempio.

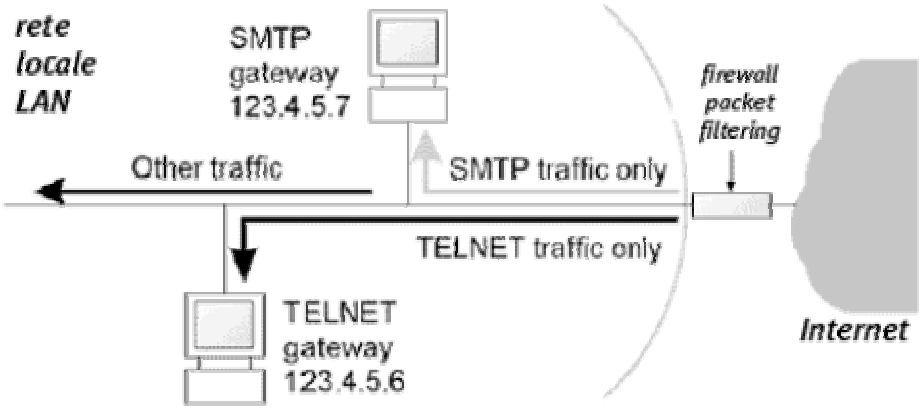

figura 2

2.3 Firewall come Gateway

I firewall possono essere usati come gateway verso Internet. In questa ottica il firewall viene visto dalla rete locale come "router", anche se generalmente sarà un altro router a realizzare la connessione fisica verso Internet. Se il firewall ha tre porte ethernet può gestire una rete sicura riservata ai propri server Internet e isolare la rete locale mediante la funzione NAT (Network Address translation). Con i classici firewall a due porte si può ottenere la stessa configurazione tramite due firewall (Figura 3).

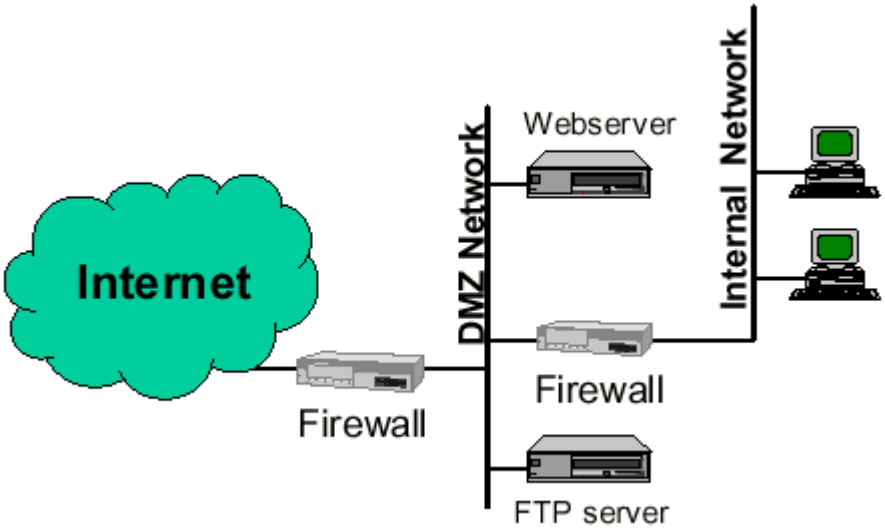

figura 3

2.4 Firewall per estensione della propria LAN

Una funzione che si ritrova in sempre più firewall è la possibilità di gestire le VPN (Virtual Private Network). Una VPN permette di estendere la propria rete privata (LAN) verso altre reti private utilizzando come dorsale una rete pubblica (e quindi intrinsecamente insicura). Questo è possibile perché i dati trasmessi da una rete privata all'altra vengono automaticamente crittografati e de-crittografati dai firewall, rendendo la trasmissione sicura in modo trasparente per gli utenti di una rete. La funzione di VPN è possibile anche tra la propria rete locale e un singolo computer (un portatile) in Internet: è sufficiente installare nel

portatile un apposito software che si occupi di crittografare / de-crittografare i dati provenienti dal firewall.
I vantaggi di questa tecnologia sono ovvi:

1. riduzione drastica dei costi per i collegamenti aziendali;
2. maggiore sicurezza nella trasmissione dei dati.

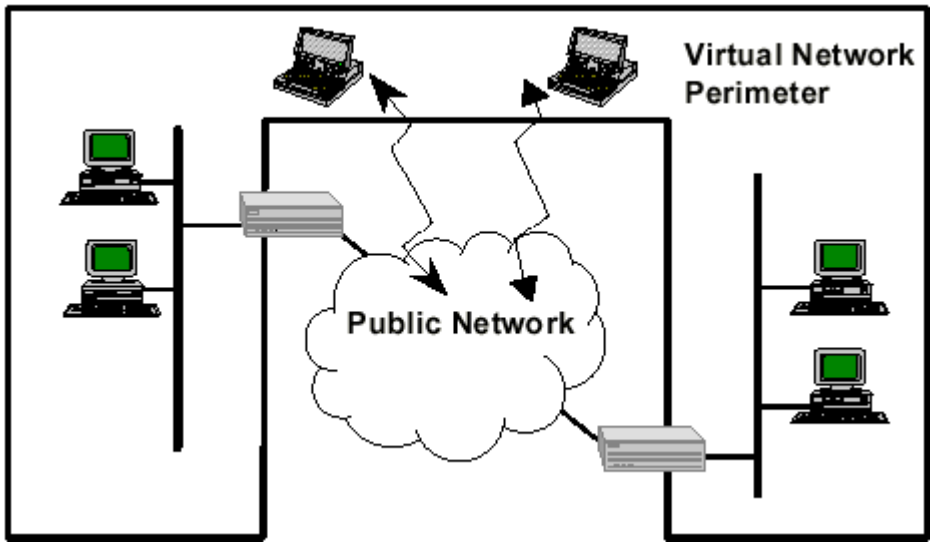

figura 4

3. Configurazione Hardware e Software

Il firewall attivo presso l'Istituto di Linguistica Computazionale ha una configurazione hardware che può essere così riassunta nelle sue componenti principali:

1. case con alimentazione ridondante;
2. processore AMD Athlon 1400 Mhz;
3. 2 schede di rete BROADCOM Corporation NetXtreme BCM5700 Gigabit Ethernet;
4. una coppia di hard disk da 60 Gb configurati in mirror software RAID1.

Il sistema operativo installato è Linux, distribuzione RedHat 7.3, con il kernel versione 2.4.9-21 opportunamente configurato come descritto nel documento "Firewall and Proxy Server HOWTO" [Firewall-HOWTO] nella sezione "Preparing the Linux system" (http://www.linux.org/docs/ldp/howto/Firewall-HOWTO-6.html).
Dopo aver modificato il kernel è stato installato il pacchetto RPM iptables-1.2.5-3.i386.rpm, che consente di utilizzare la tecnica di filtraggio denominata IPTABLES, descritta in dettaglio nel sito http://www.netfilter.org.
Come vedremo in dettaglio nel paragrafo successivo, esiste un solo file di configurazione (/etc/sysconfig/iptables) che può essere modificato con un editor testuale; in alternativa è possibile configurare e gestire completamente via WEB il firewall con il software WEBMIN (http://www.webmin.com).

4. NAT statica

L'idea seguita nella configurazione del firewall è quella di utilizzarlo con funzione principale di Gateway verso Internet (vedi paragrafo 2.3, pagina 4).
Rispetto a quanto illustrato nella precedente Figura 3 non è prevista una rete DMZ (Demilitarized Zone).

La funzione NAT (Network Address Translation) che viene utilizzata consiste nell'intervenire in tempo reale su ciascuna connessione tra una macchina della rete locale e una macchina esterna. Il router di confine (nel nostro caso il firewall-nat che stiamo descrivendo) traduce istantaneamente l'indirizzo di destinazione presente nei pacchetti in ingresso e l'indirizzo del mittente posto nei pacchetti in uscita dalla rete locale per ciascuna connessione, facendoli corrispondere entrambi a un indirizzo IP valido per la comunicazione su Internet.
Viene utilizzata la tecnica NAT statica che fa corrispondere indirizzi IP validi sulla rete esterna (Internet) ad alcuni indirizzi interni predefiniti, come mostrato nella Figura 5.

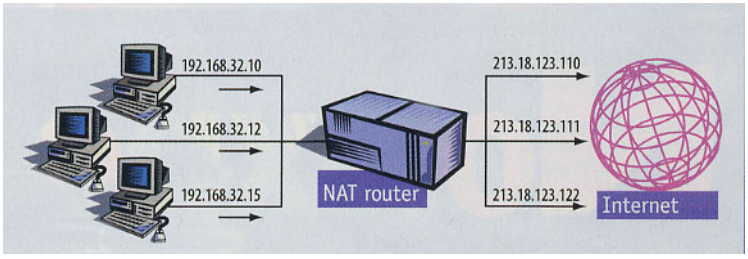

figura 5

Gli indirizzi interni predefiniti a cui si faceva riferimento prima sono illustrati in dettaglio nel documento "DHCP Server: definizione e configurazione sulla rete ILC" [ILC-CED-2002-02].
Per completezza accenniamo all'altra tecnica esistente, la NAT dinamica, dove il router di confine dispone di un piccolo pool di indirizzi validi di classe C, e li sostituisce automaticamente agli indirizzi originali (non validi) presenti nei pacchetti appartenenti alle connessioni che coinvolgono le macchine interne in uscita verso Internet. Una variante di questa tecnica, detta PAT o Port Address Translation, utilizza un solo indirizzo IP valido in luogo di un pool di indirizzi e fa corrispondere macchine interne diverse a diversi numeri di porta associati allo stesso indirizzo IP valido. Questa tecnica permette un risparmio in termini di indirizzi validi, ma rende difficoltosa la ricerca della macchina locale che può rendersi protagonista di una azione illecita sulla rete Internet.

5. Inserimento delle regole

Come abbiamo visto in precedenza, l'unico file di configurazione presente è /etc/sysconfig/iptables.
Non è nelle finalità di questo documento spiegare in dettaglio i parametri utilizzati all'interno delle regole inserite nel file di configurazione; per la spiegazione rimandiamo ai seguenti articoli presenti nel sito http://www.netfilter.org:

1. Linux 2.4 Packet Filtering HOWTO [Filtering-HOWTO] (http://www.netfilter.org/documentation/HOWTO/it/packet-filtering-HOWTO.html);
2. Linux 2.4 NAT HOWTO [NAT-HOWTO] (http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO.html).

Le regole che dobbiamo inserire all'interno del file di configurazione ci devono permettere di raggiungere queste due finalità:

1. gli utenti della rete locale privata devono utilizzare il firewall come Gateway verso Internet (vedi paragrafo 2.3, pagina 4);
2. il firewall deve agire da filtro e permettere l'ingresso nella rete privata solo verso determinati indirizzi IP e determinate porte di destinazione (vedi paragrafo 2.2, pagina 3).

Per raggiungere la prima finalità, se nella sezione nat del file /etc/sysconfig/iptables che inizia con:

**nat*

all'interno della catena dei pacchetti OUTPUT con azione predefinita ACCEPT, che inizia con:

:OUTPUT ACCEPT

inseriamo la regola:

-A POSTROUTING -s 192.168.92.98 -o eth1 -j SNAT --to-source 146.48.92.98

indichiamo così al firewall di tradurre i pacchetti provenienti dall'indirizzo IP sorgente 192.168.92.98 (ip di rete privata) utilizzando verso Internet (interfaccia eth1) l'indirizzo IP pubblico 146.48.92.98.

Una descrizione delle decisioni di instradamento programmabili con opportune regole si trova in: http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO-5.html.

Ulteriori spiegazioni sulla opzione POSTROUTING si possono trovare in:
http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO-6.html#ss6.1.

Ulteriori spiegazioni sulla opzione SNAT si possono trovare in:
http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO-3.html.

La Figura 6 mostra questa stessa regola inserita tramite l'interfaccia web del software Webmin:

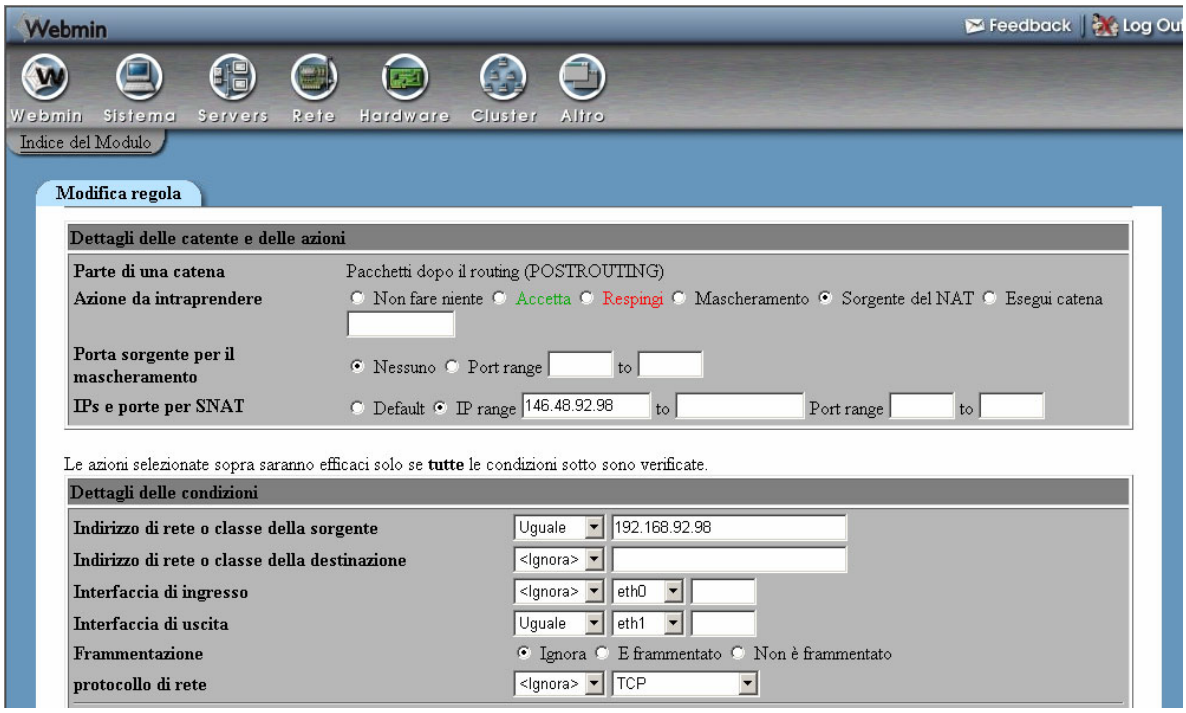

figura 6

Per raggiungere la seconda finalità, ossia utilizzare il firewall come filtro (paragrafo 2.2 pagina 3) per far accedere dalla rete Internet verso servizi e IP precisi situati all'interno della rete locale, se nella sezione nat del file /etc/sysconfig/iptables che inizia con:

**nat*

all'interno della catena dei pacchetti OUTPUT con azione predefinita ACCEPT, che inizia con:

:OUTPUT ACCEPT

inseriamo la regola:

-A PREROUTING -d 146.48.92.16 -i eth1 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.92.16:80

viene così permesso ai pacchetti che arrivano da Internet (interfaccia eth1) e destinati all'IP 146.48.92.16 porta 80 (Web server) di essere instradati verso l'IP 192.168.92.16 porta 80.

Ulteriori spiegazioni sulle opzioni PREROUTING e DNAT si possono trovare in: http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO-6.html#ss6.2.

La Figura 7 mostra questa stessa regola inserita tramite l'interfaccia web del software Webmin:

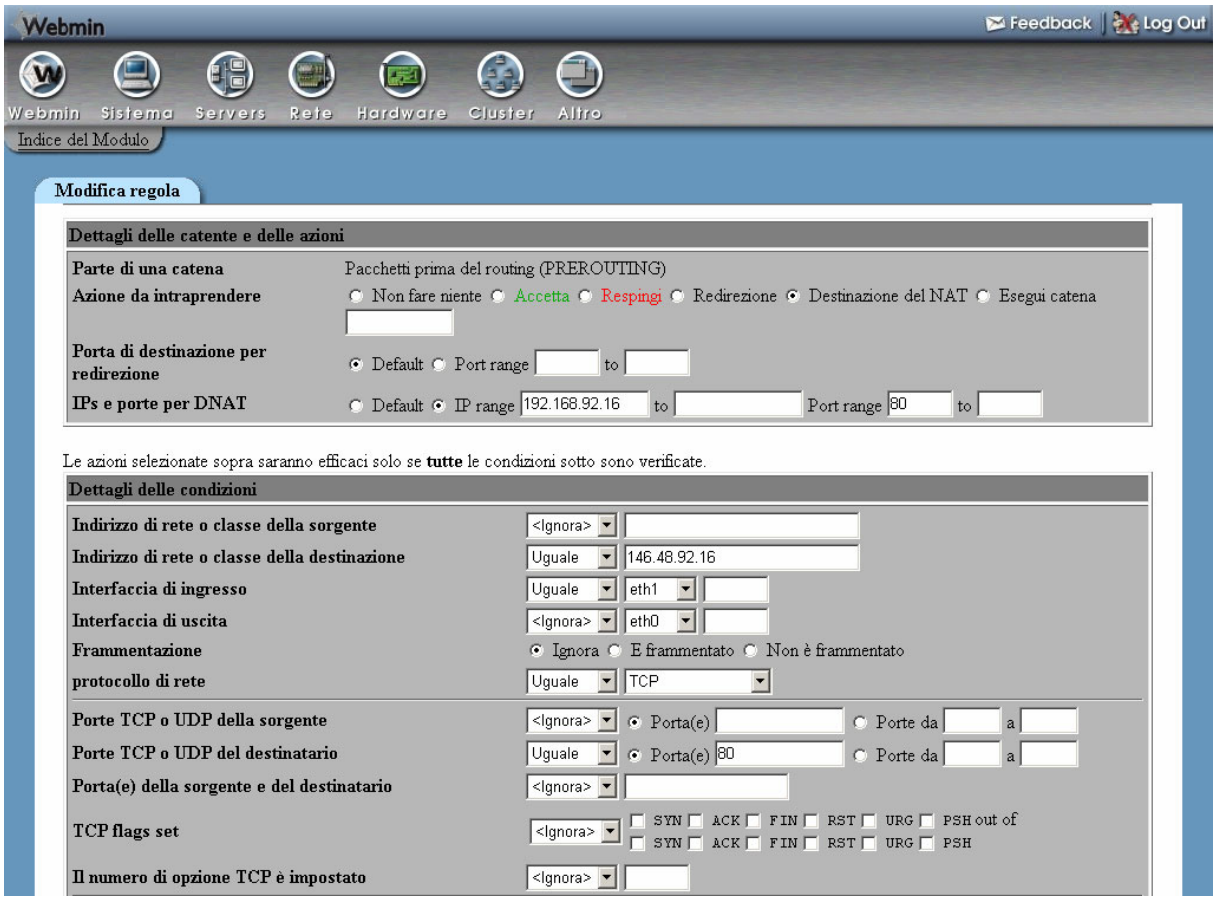

figura 7

6. Conclusioni

Concludiamo riassumendo i requisiti tecnici, le difficoltà incontrate e i benefici in termini di sicurezza raggiunti con l'adozione di un Firewall-NAT:

a) requisiti tecnici:

1. occorre utilizzare un calcolatore con una forte tolleranza ai guasti (alimentazione ridondante e dischi in RAID) ed una coppia di schede di rete molto veloci (1 Gbit/sec); i prezzi sul mercato di macchine con processore Intel/AMD idonee allo scopo non sono comunque elevati;
2. il sistema operativo è di pubblico dominio, dunque gratuito; può essere utilizzata una qualunque distribuzione di Linux perché è il kernel che gestisce il firewall.

b) difficoltà incontrate:

1. la documentazione su Internet è facilmente reperibile e ben dettagliata; occorre però sottolineare che lo strumento software è molto complesso per la miriade di parametri di configurazione presenti; questo impone un approfondito studio della terminologia adottata;
2. la documentazione riporta sempre regole da utilizzare nel file di configurazione attraverso un editor testuale; esistono però interfacce Web di configurazione che possono semplificarne la gestione.

c) benefici in termini di sicurezza:

1. la creazione di nuove regole e la loro modifica può essere fatta in breve tempo e l'applicazione è immediata senza interrompere il lavoro degli altri utenti;
2. il filtro dei pacchetti in ingresso da Internet verso la rete locale permette la distribuzione mirata dell'accesso a qualunque tipo di servizio (http, ftp, smtp, ecc..).

Bibliografia

[Firewall-HOWTO] Firewall and Proxy Server HOWTO. Mark Grennan, mark@grennan.com. February 2000. http://www.linux.org/docs/ldp/howto/Firewall-HOWTO.html, 2000.
[ILC-CED-2002-02] DHCP Server: definizione e configurazione sulla rete ILC. A. Enea. Dicembre 2002.
[Filtering-HOWTO] Linux 2.4 Packet Filtering HOWTO. Rusty Russell. May 2000. http://www.netfilter.org/documentation/HOWTO/it/packet-filtering-HOWTO.html, 2000.
[NAT-HOWTO] Linux 2.4 NAT HOWTO. Rusty Russell. May 2000. http://www.netfilter.org/documentation/HOWTO/it/NAT-HOWTO.html, 2000.