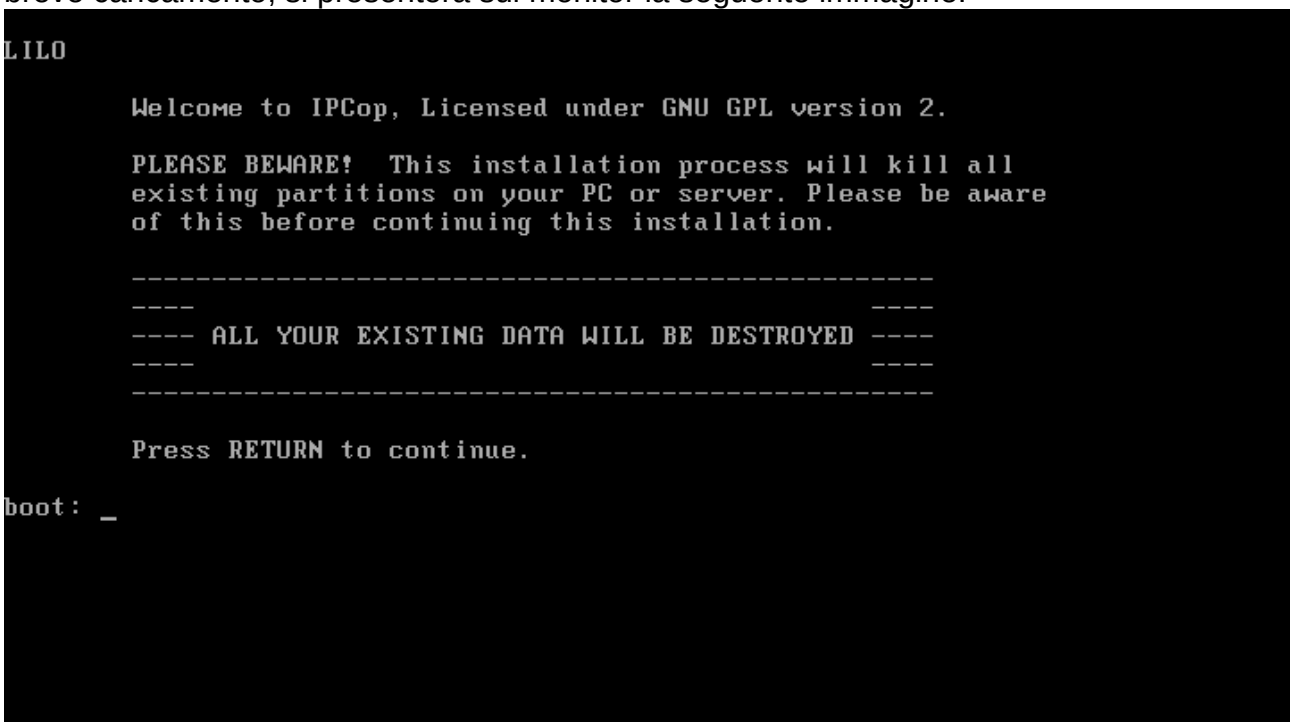
Proteggere il nostro personal computer da attacchi esterni è ormai diventata una priorità. Ciò è ancor più vero se a dover essere protetti sono diversi computer collegati in una rete LAN. Un sistema adottato per effettuare questa protezione e quello interporre tra Internet e il o i computer un firewall. Un firewall è sistema, hardware o software, che è in grado di filtrare le connessioni che avvengono tra la rete Internet e la rete interna e che permette la regolazione dei filtri e l'impostazione degli stessi in base alle esigenze dell'utente. Un sistema per effettuare questa funzione senza un elevato importo in costose licenze e hardware dedicato (anch'esso di elevato costo) è utilizzare macchine obsolete a causa della loro limitata capacità di calcolo ma sufficienti a gestire un sistema di filtri e un software il cui uso non è legato all'acquisto di licenze. Un ottimo risultato è stato ottenuto da chi scrive e da tanti altri utilizzando un firewall basato su un sistema linux. È per questo che ho deciso di scrivere una guida che potesse aiutare anche altri nell'installazione e configurazione di IpCop. Il firewall in oggetto (IpCop) è liberamente scaricabile dal sito http://www.ipcop.org dove è possibile trovare anche i manuali che ne descrivono l'installazione, il funzionamento ed eventuali modifiche specifiche per fargli eseguire determinate funzioni. È fornito con licenza GPL (GeneralPublicLicence) e quindi utilizzabile da chiunque e modificabile a piacimento in quanto si è in possesso dei sorgenti.

Ma andiamo per ordine; IpCop linux e una completa distribuzione linux il cui solo scopo è proteggere il network sul quale è installato implementando tecnologie esistenti per mettere in sicurezza una LAN o un singolo computer. Si può installare anche su un PC obsoleto (386, 486, ecc.) che abbia installato un HD anche di 500 Mb (ma va bene anche più piccolo) e due o tre schede di rete in base all'utilizzo che se ne vuole fare. Naturalmente non tutto l'hardware attualmente esistente viene supportato da IpCop, ma una lista può essere trovata nel sito a lui dedicato. Le funzioni principali sono:
Un sicuro, stabile ed altamente configurabile firewall basato sul linux.
Una amministrazione del firewall basata su delle pagine Web gestite da un server Web interno.
Un client DHCP che permette a IpCop di ottenere un indirizzo IP dall'ISP con il quale ci colleghiamo.
Un server DHCP che ci aiuta nella configurazione automatica delle macchine da proteggere.
Un proxy DNS per elevare la velocità nelle richieste DNS.
Un proxy Web altamente configurabile per elevare la velocità nel caricamento delle pagine Web.
Un sistema di "intrusion detection" che ci permette di determinare gli attacchi subiti.
L'abilità di dividere il nostro network in una zona VERDE, protetta da Internet e una zona ARANCIONE o DMZ (DeMilitarizedZone) che contiene i server ai quali si deve poter accedere da Internet.
La possibilità di creare una VPN (VirtualPrivateNetwork) che ci permette di collegare al network interno un altro network attraverso la rete Internet in maniera " sicura ".

Per effettuare l'installazione di IpCop è necessario scaricare l'immagine del CD dal sito di riferimento (circa 22Mb) e masterizzarla su un CD; il CD è bootable e quindi possiamo utilizzarlo per effettuare il boot nella macchina su cui andrà installato. Nel caso in cui non è possibile effettuare il boot nella macchina da CD è possibile trovare all'interno dello stesso un'immagine del floppy da utilizzare per il boot. Nel caso in cui la macchina in questione non abbia neanche un lettore CD collegato è comunque possibile effettuare l'installazione attraverso un server Web o FTP, ma tale opzione è un pò macchinosa.
Dobbiamo innanzitutto decidere quale sarà la configurazione del nostro network; IpCop

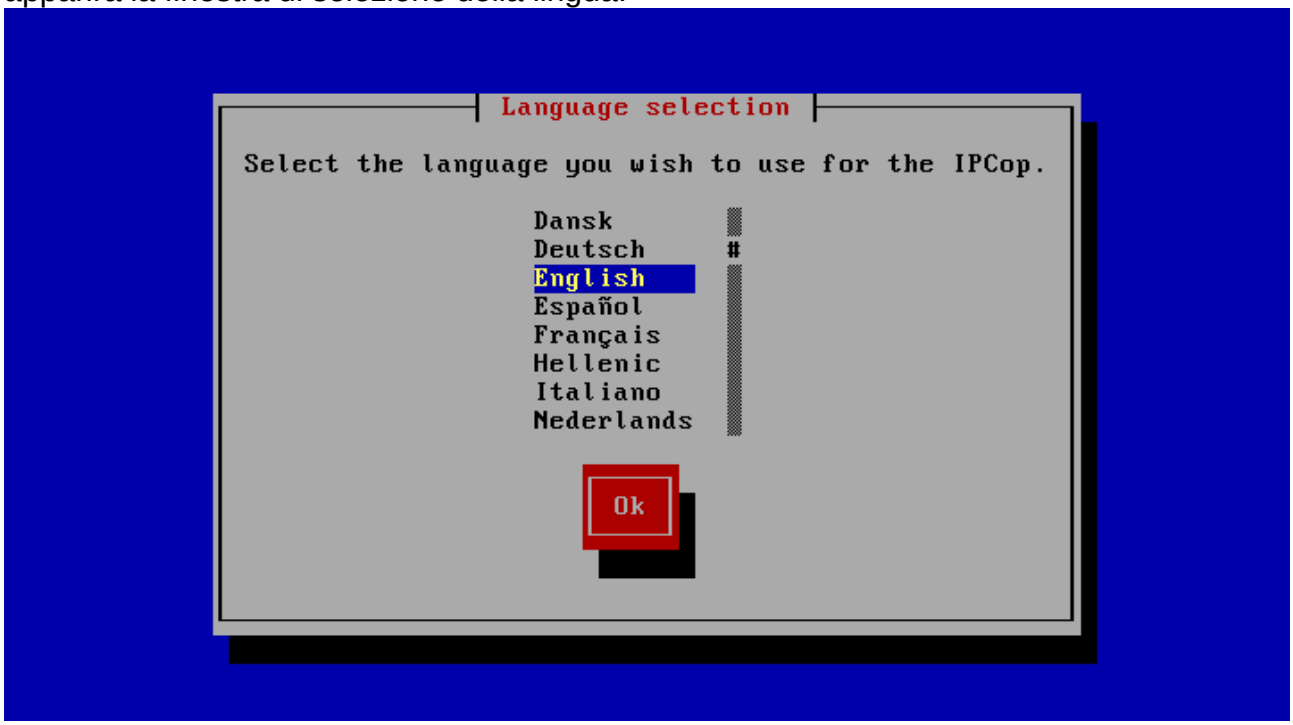
può dividere le tre interfacce di rete collegate in altrettanti network separati denominati VERDE, ARANCIONE e ROSSO. Il network verde sarà quello a cui andranno collegati i computer da proteggere; il firewall si occuperà di effettuare il routing e gestire le richieste provenienti da tale network da e verso Internet. Il network rosso sarà quello a cui andrà collegato l'accesso ad Internet. Il network arancione (opzionale) e quello parzialmente protetto da Internet ma che conterrà i server a cui si deve dare accesso da Internet. Le due configurazioni possibili sono quindi rosso e verde oppure rosso, arancione e verde. Assumiamo pertanto l'ipotesi di avere un modem o router collegato ad Internet con l'uscita RJ45; attacchiamo tale uscita all'interfaccia rossa (vedremo poi come assegnare un'interfaccia ad un network specifico). Il computer o la LAN da proteggere andranno collegati all'interfaccia denominata verde. Assumiamo inoltre che il PC in nostro possesso possa fare il boot da CD. Inseriamo pertanto il CD di avvio nella macchina e, dopo un breve caricamento, si presenterà sul monitor la seguente immagine.



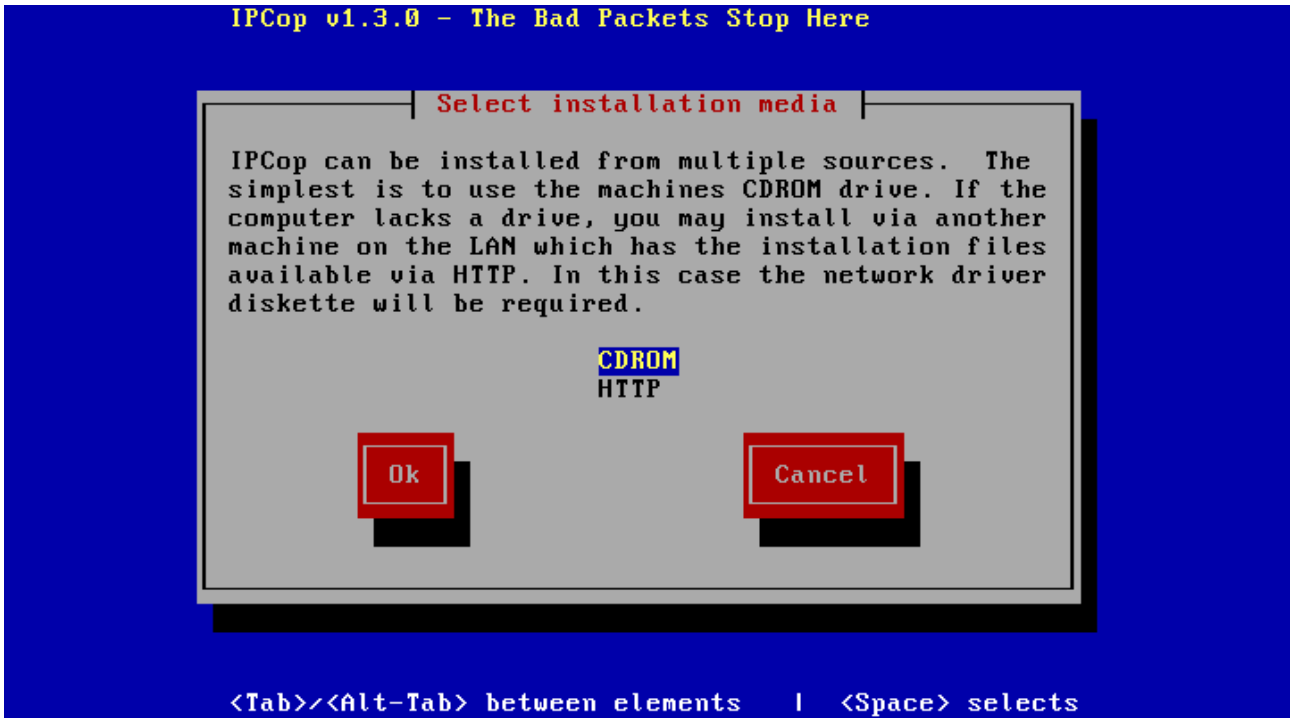
Premiamo invio ed il sistema effettuerà il caricamento del kernel linux, sullo schermo vedremo scorrere le informazioni e i messaggi di caricamento dello stesso così:

```
Limiting direct PCI/PCI transfers.
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
apm: BIOS version 1.2 Flags 0x03 (Driver version 1.16)
Starting kswapd
Journalled Block Device driver loaded
pty: 256 Unix98 ptys configured
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI en
abled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
ttyS02 at 0x03e8 (irq = 4) is a 16550A
ttyS03 at 0x02e8 (irq = 3) is a 16550A
Uniform Multi-Platform E-IDE driver Revision: 6.31
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller on PCI bus 00 dev 39
PIIX4: chipset revision 1
PIIX4: not 100% native mode: will probe irqs later
    ide0: BM-DMA at 0x10b0-0x10b7, BIOS settings: hda:DMA, hdb:pio
    ide1: BM-DMA at 0x10b8-0x10bf, BIOS settings: hdc:DMA, hdd:pio
hda: VMware Virtual IDE Hard Drive, ATA DISK drive
hdc: VMware Virtual IDE CDROM Drive, ATAPI CD/DVD-ROM drive
ide2: ports already in use, skipping probe
_
```

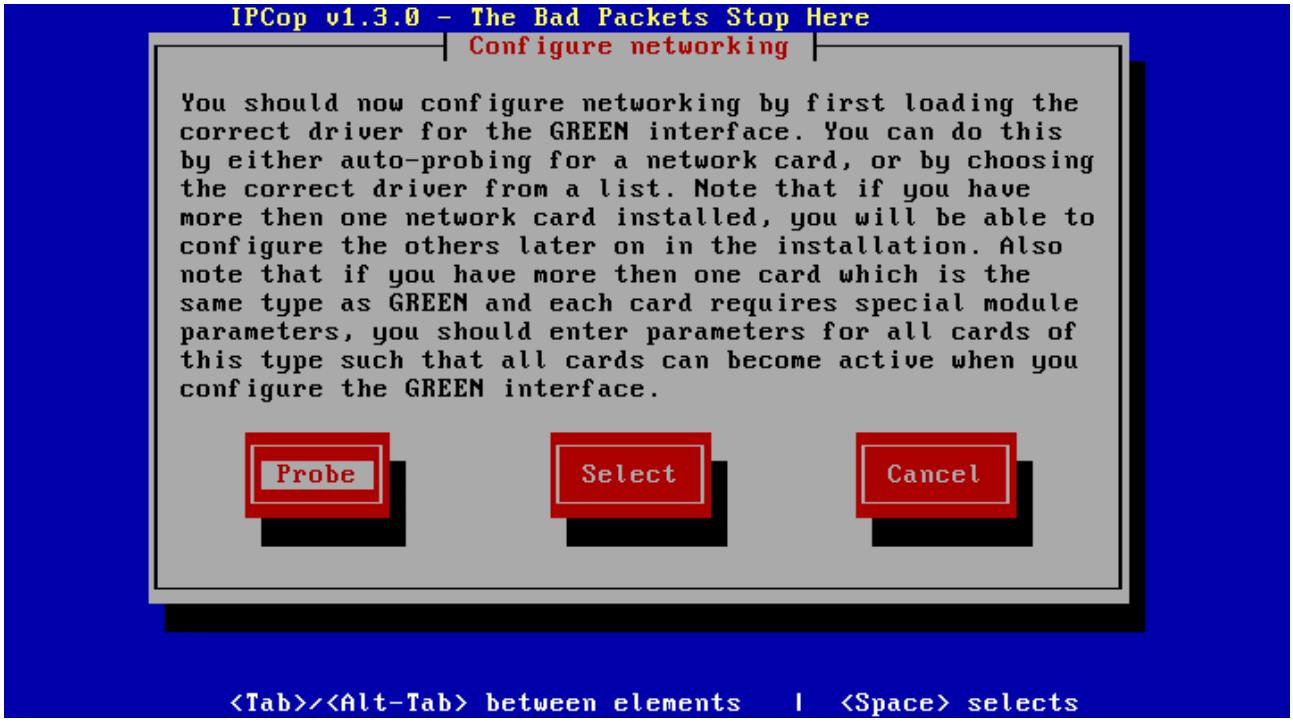
Nel caso in cui tutto l'hardware viene correttamente riconosciuto, e quindi in mancanza di errori che bloccherebbero la fase di boot e dei quali vedremmo descrizione sul monitor, apparirà la finestra di selezione della lingua.



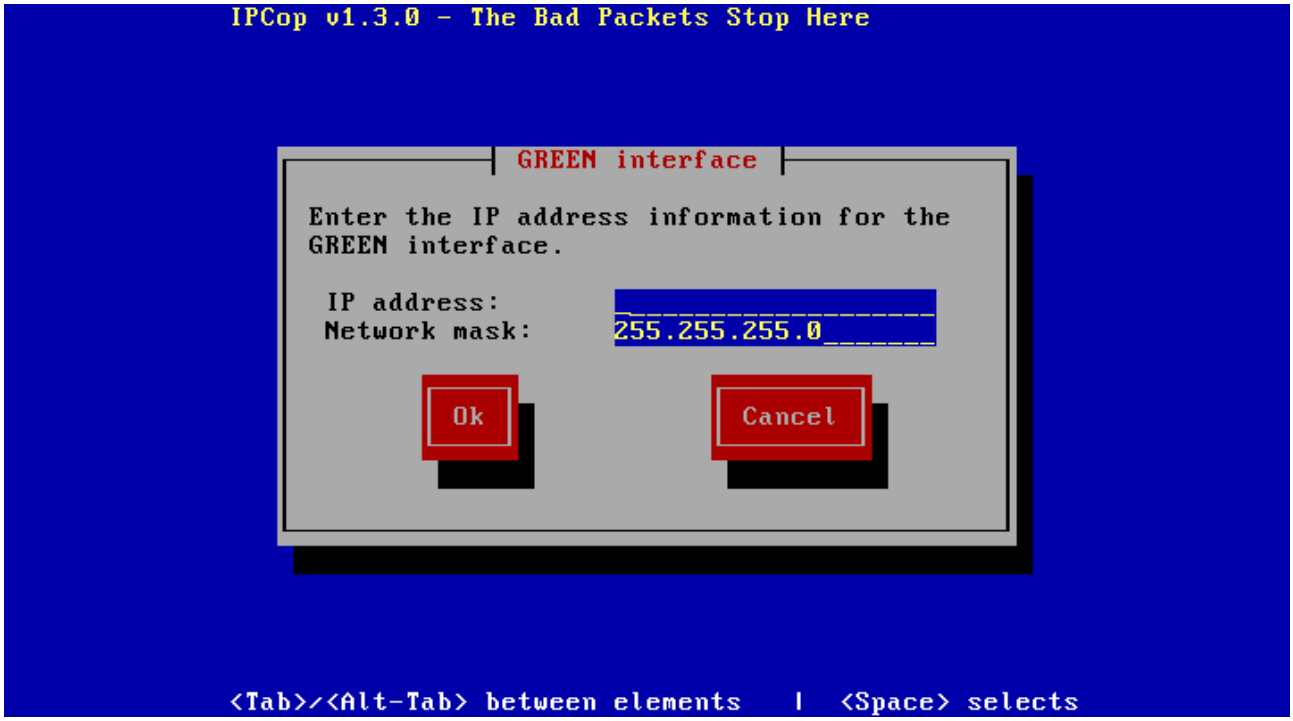
Dopo un'altra finestra che ci informa della possibilità di cancellare l'installazione si presenterà un box di dialogo che ci permetterà di decidere la sorgente di installazione.



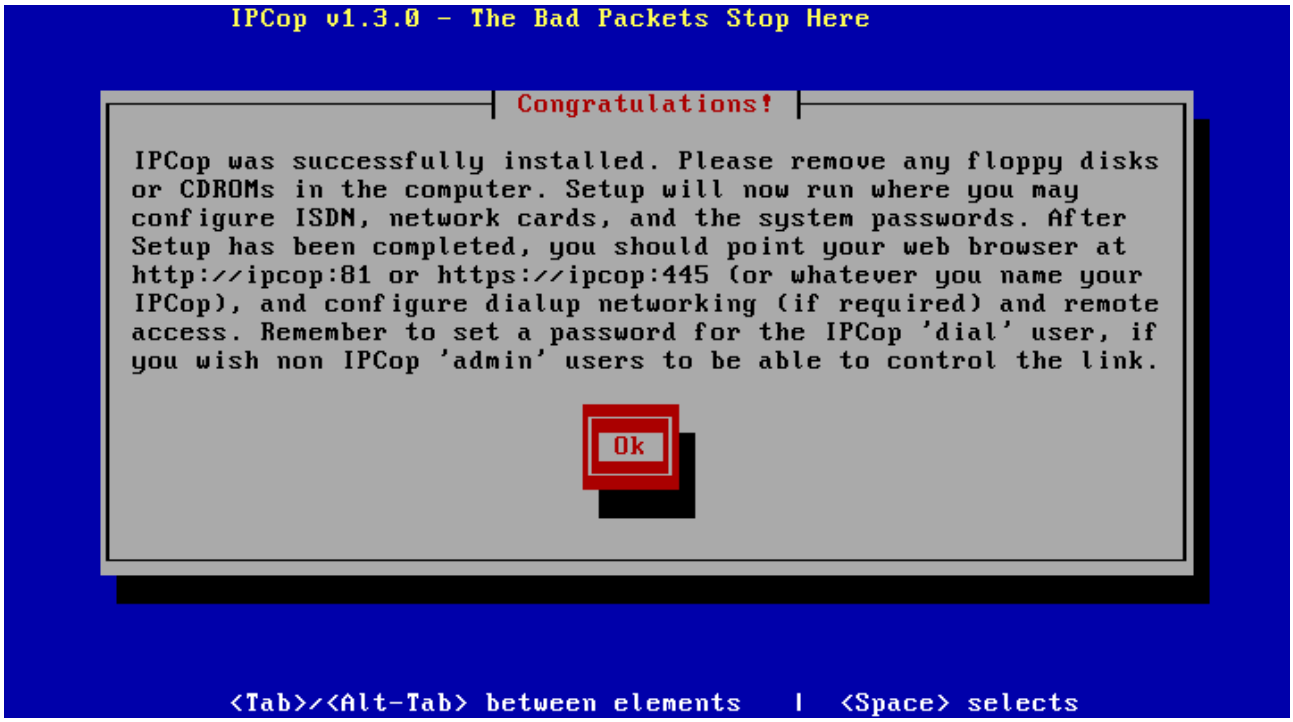
Selezioniamo CD rom e un box ci informerà che si stà procedendo alla preparazione dell'hard disk e che quindi ogni dato al suo interno verrà definitivamente cancellato; una volta confermato questo box partirà l'installazione vera e propria del firewall a questo punto si presenterà una finestra di selezione che ci permetterà di caricare il file di configurazione s'è precedentemente salvati su floppy. Questa funzione è utile nel caso in cui una macchina con il firewall installato si sia danneggiata; in tal caso la configurazione effettuata, s'è precedentemente salvata tramite un'apposita funzione del firewall, può essere ripristinata in un sol colpo su una nuova macchina senza perdita di tempo. Nel nostro caso selezioniamo"skip".
Successivamente il firewall passerà alla configurazione del network verde con il seguente box di selezione:



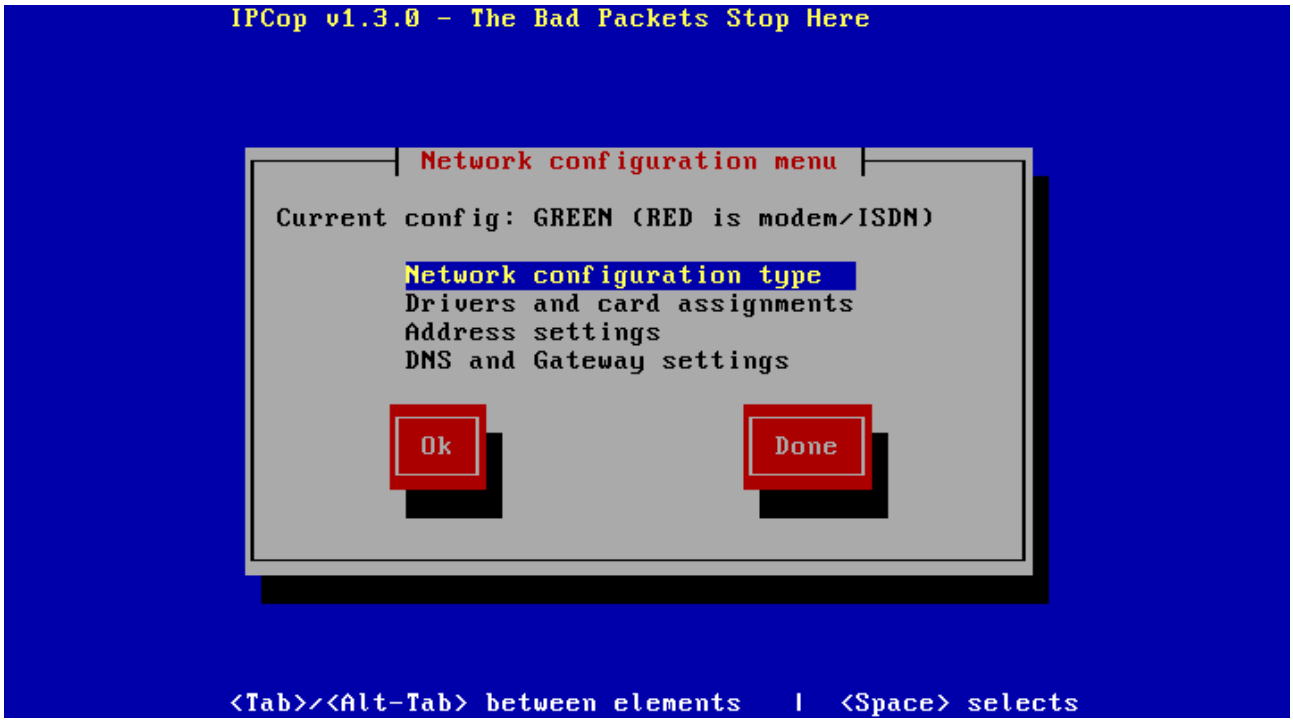
Selezioniamo "Probe" e di firewall tenterà di riconoscere automaticamente le schede di rete e assegnerà alla prima scheda trovata il network verde; assumiamo che le schede di rete siano tutte riconosciute correttamente dal firewall per semplificare, ma nel caso in cui queste non vengano riconosciute è possibile fargliele riconoscere installando dei driver appositi ed aggiornati per le schede in questione. Si presenterà il seguente box di selezione:



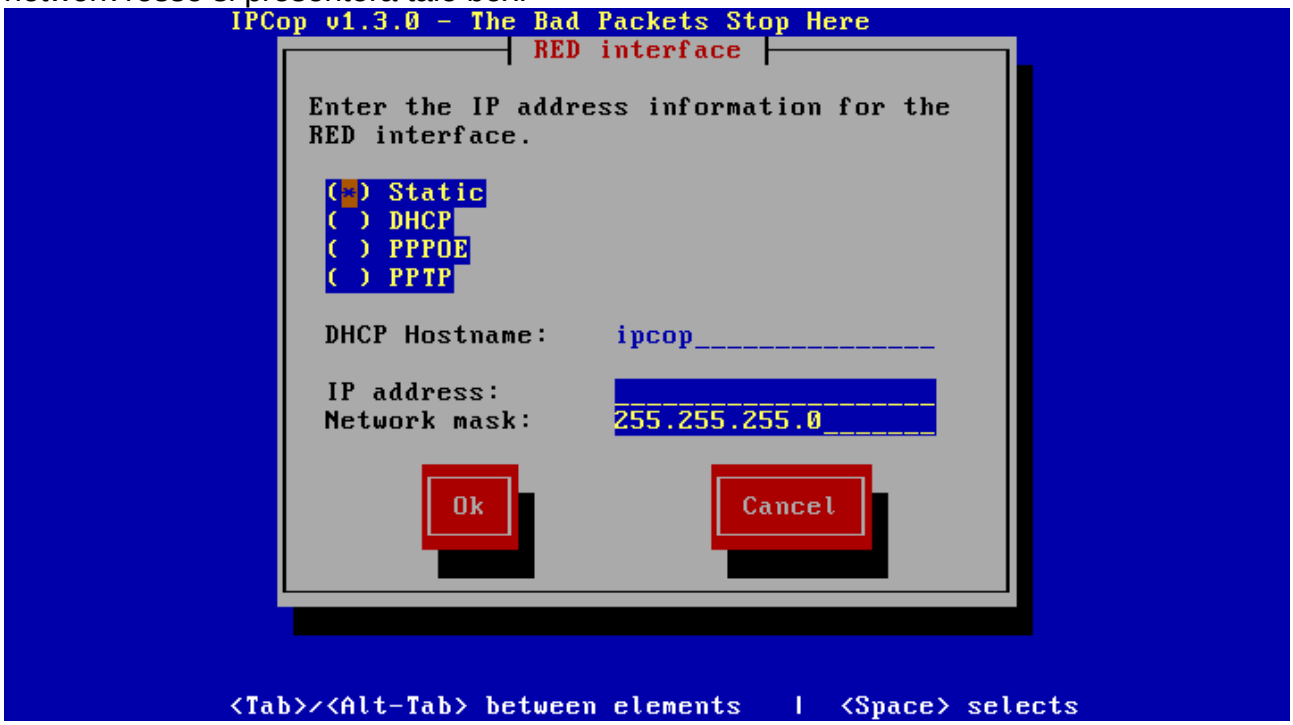
qui potremo inserire l'indirizzo IP che dovrà avere il firewall; tale indirizzo andrà deciso in base alla numerazione interna della nostra rete. Pertanto, assumendo che i nostri PC abbiano come indirizzo 192.168.1.x dove x è variabile da 0 a 255, dovremo scegliere come indirizzo 192.168.1.x dove x è un numero non presente nella numerazione interna dei PC e compreso nell'intervallo 0-255. Premiamo "OK" si presenterà la successiva immagine che ci informa che l'installazione e terminata ed è possibile rimuovere il CD e far partire il nostro firewall.



Se tutto è stato configurato correttamente sarà possibile accedere da qualunque computer della rete alle pagine Web di configurazione del firewall digitando su un browser Web l'indirizzo indicato nell'immagine; da notare che possibile collegarsi sia in sistema non protetto HTTP che è con un sistema protetto HTTPS. Non dimentichiamo di immettere i numeri indicati nell'immagine alla fine dell'indirizzo, pena l'impossibilità di accedere a dette pagine.
All'avvio del firewall si presenteranno dei box che ci permetteranno di scegliere la mappatura della tastiera (italiana, americana, ecc.) e il fuso orario. L'impostazione corretta di quest'ultimo box ci permetterà di registrare correttamente il log di sistema e di navigazione Internet ed inoltre sarà possibile utilizzare il firewall anche come "time server" installando opportuni Add-on; ma questo lo vedremmo dopo. Dovremo anche inserire il nome della macchina riconosciuto dalla rete interna; lasciamo stare l'opzione di default (ipcop) o cambiamola nel caso in cui vogliamo installare una VPN ed amministrare il firewall attraverso tale VPN. Si presenterà inoltre un box con la richiesta di configurazione ISDN. Infatti il firewall può anche gestire come network rosso modem ISDN o schede modem installate su slot PCI. Selezioniamo "Disable ISDN" e continuiamo l'installazione. Si presenterà a questo punto il box di configurazione dei network.

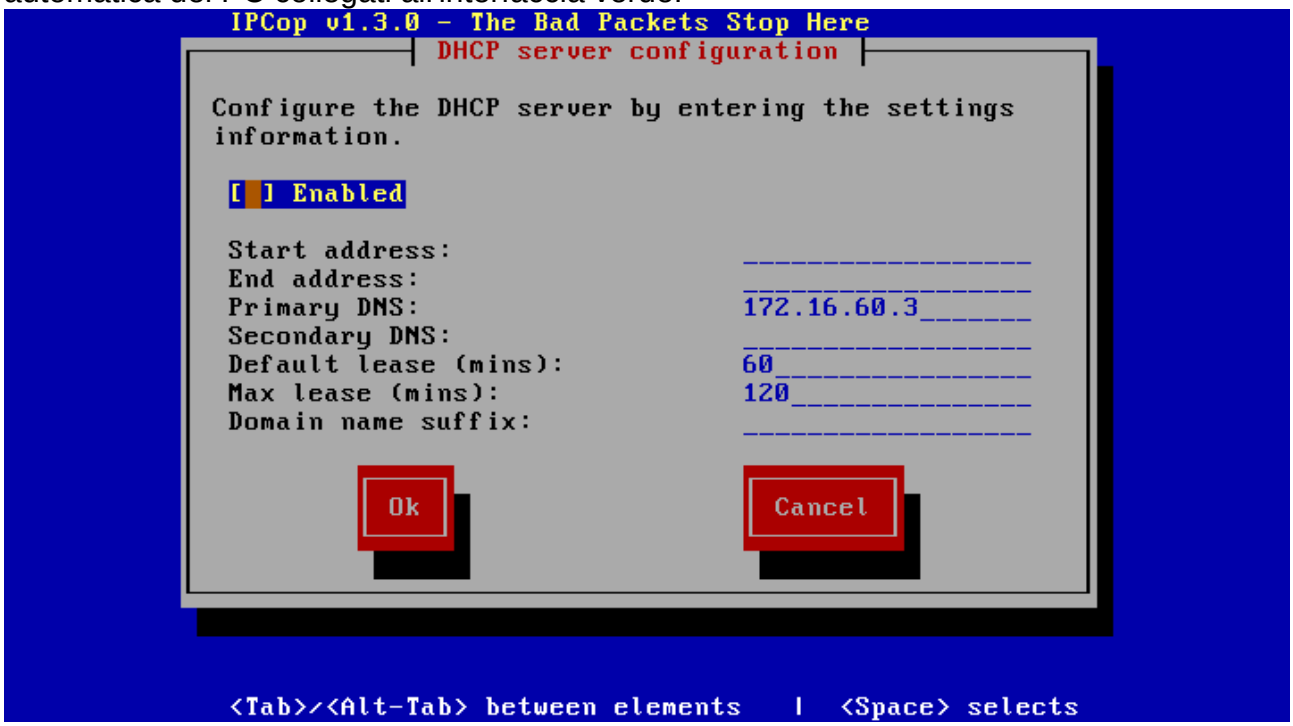


La prima opzione del menu ci permetterà di scegliere il tipo di configurazione; selezioniamo GREEN + RED e proseguiamo. La seconda opzione del menu ci permetterà di scegliere quale scheda assegnare a quale network. La terza opzione ci permetterà di scegliere per ogni tipo di scheda le configurazioni opportune; nel caso della scheda del network rosso si presenterà tale box:



Sceglieremo un indirizzo statico, che inseriremo sotto, nel caso in cui il fornitore di accesso ci abbia dato un indirizzo statico; il firewall ancora automaticamente la maschera da utilizzare. Utilizzeremo l'opzione DHCP nel caso in cui sarà possibile effettuare l'indirizzamento automatico delle firewall, per esempio nel caso in cui l'ISP ci abbia fornito un router con un server DHCP all'interno. La terza opzione andrà autorizzata nel caso in cui il modem che abbiamo sia del tipo che utilizza la connessione PPPoE, ossia nel caso

in cui è indispensabile fare una procedura di autenticazione che richieda l'inserimento di un username e una password. Vedremo dopo dove andranno inseriti tali dati. La quarta opzione ci sarà utile nel caso in cui la connessione sia PPTP e l'ISP ci abbia fornito un IP e una maschera fissi.
Dopo aver configurato correttamente il tutto potremo andare a configurare l'ultima opzione del menu di configurazione dei network; potremo andare ad inserire pertanto, se forniti dall'ISP, l'IP dei server DNS primario e secondario è l'eventuale gateway da utilizzare.
Fatto ciò selezioniamo "OK" e si presenterà il box di configurazione del server DHCP del network verde. Questo servizio potrà essere attivato per effettuare la configurazione automatica dei PC collegati all'interfaccia verde.

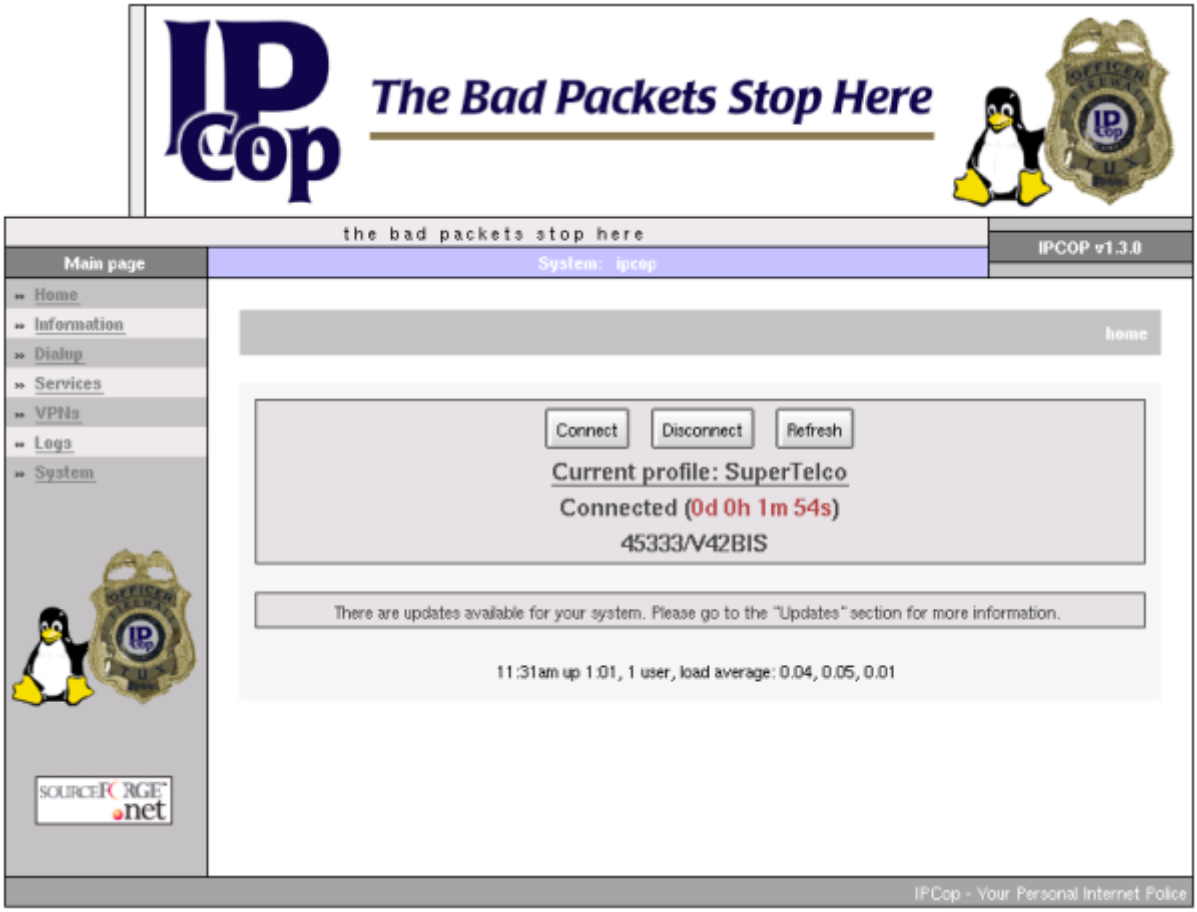


L'indirizzo di inizio e fine definisce il range di indirizzi che il server può assegnare ai client che ne facciano richiesta; gli indirizzi DNS primario e secondario possono essere lasciati in bianco in quanto andremo ad utilizzare il proxy DNS interno al firewall. La quinta e la sesta opzione di questo box ci permetteranno di settare il tempo entro il quale il computer client deve rispondere ad un assegnamento di indirizzo. Passato il tempo massimo impostato l'indirizzo assegnato non verrà più considerato tale ed il server potrà assegnarlo alla prossima richiesta. L'ultima opzione ci permetterà di inserire un suffisso alle richieste DNS.
Dopo aver premuto "OK" si presenterà un box con la richiesta di inserimento della password dell'utente "root". La successiva finestra ci richiederà di inserire la password per l'utente "setup". Occorre fare qui una precisazione; gli unici due utenti autorizzati ad accedere alla consolle di comando del firewall sono gli utenti "root" e "setup". Mentre il primo ha accesso totale al sistema, il secondo ha accesso alla sola finestra di configurazione. Un terzo box ci chiederà di inserire la password per l'amministrazione delle firewall via interfaccia Web.
A questo punto è terminata la configurazione del nostro firewall, premendo "OK" il sistema riavvierà ed il firewall entrerà in funzione. Sarà possibile effettuare il controllo della corretta configurazione del firewall facendo un ping della macchina da un qualunque PC connesso alla rete verde. In un sistema Windows si dovrà aprire una finestra MS-DOS e digitare "ping <indirizzo_firewall>", su un sistema Unix, linux o Macintosh OS X si digiterà "ping -n <indirizzo_firewall>". Se abbiamo fatto tutto correttamente tale operazione avrà esito

positivo.
Nell'appendice B del manuale di installazione delle firewall (in inglese) vengono riportati i codici di errore possibile che si possono presentare durante l'installazione o il boot della macchina; per ognuno di essi ne è descritta la causa ed è un utile guida nel caso si presentino problemi di qualunque sorta.

Accesso ed amministrazione del firewall via Web.

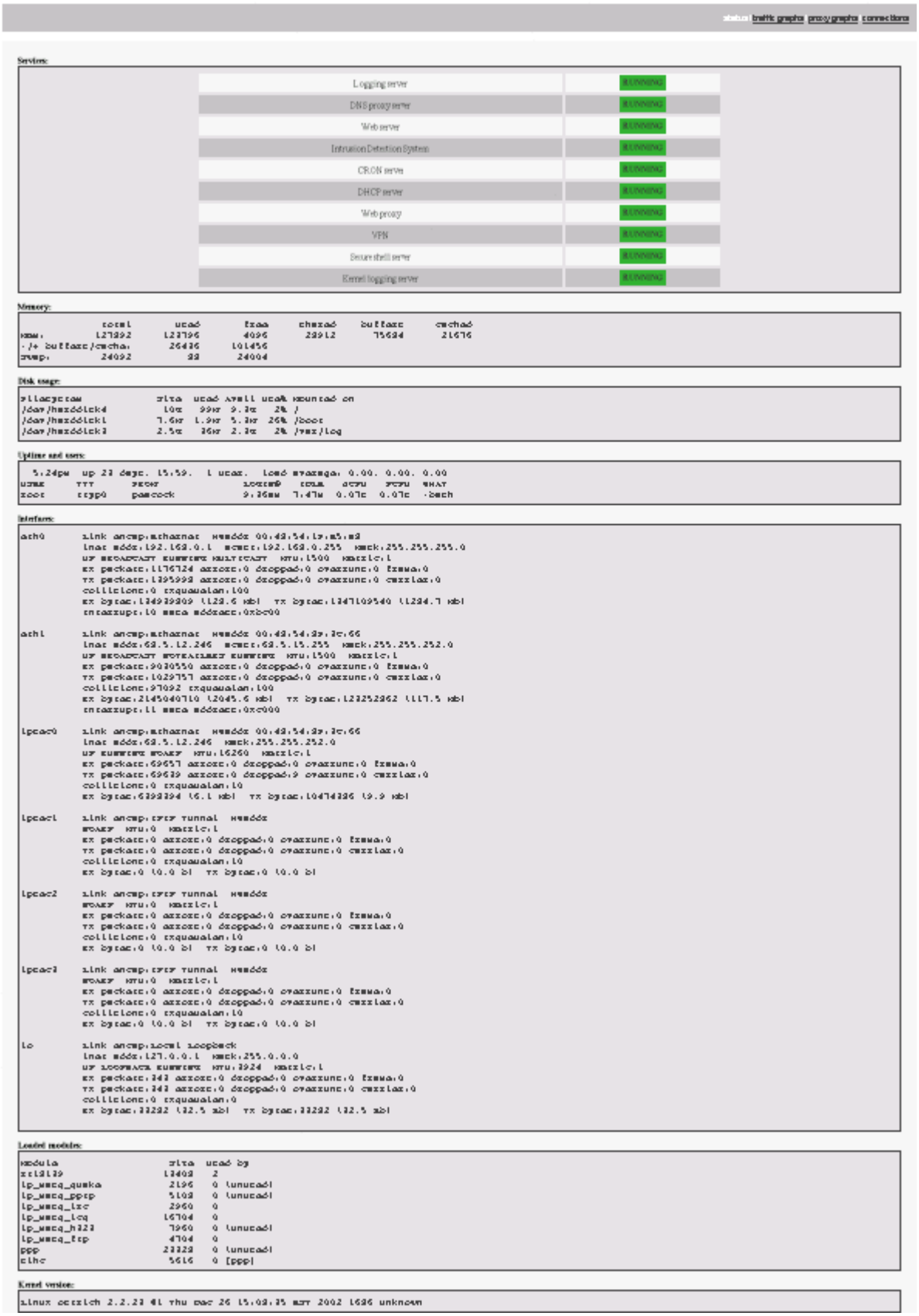
L'accesso alla GUI (GraphicsUserInterface) è semplicissimo; basta inserire in un browser Internet di un PC collegato al network verde l'indirizzo IP assegnato al firewall nella forma specificata nel box che si era presentato al primo riavvio delle firewall (quindi http://ip_firewall:81 per collegamenti normali e https://ip_firewall:445 per collegamenti protetti). Si presenterà una pagina simile a questa:



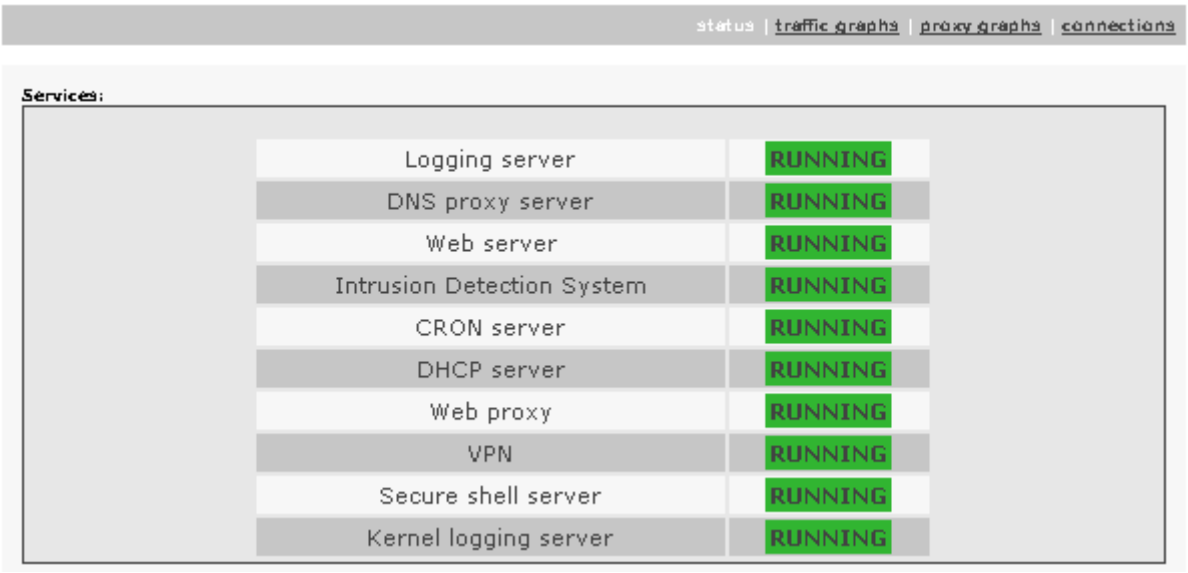
Le AWS (AdministrativeWebPages) saranno disponibili dal menu a sinistra. Da questa pagina iniziale (Home) sarà possibile controllare l'effettiva connessione ad Internet del firewall ed eventualmente connetterlo o disconnetterlo previo inserimento di username e password a suo tempo inseriti durante la fase di configurazione. L'inserimento di tali dati è richiesto inoltre per spostarsi attraverso le varie pagine di configurazione (AWS); facciamo quindi una breve descrizione delle funzioni che troveremo sotto ogni pagina.
Home: pagina iniziale.
Informazioni: saranno fornite tramite questa pagina di informazioni dettagliate sullo stato delle varie parti del firewall; grafici di traffico, del proxy, lista delle connessioni attive in quel momento, informazioni sui network e sul sistema in generale.
Connessione: usata per la configurazione e amministrazione della periferica utilizzata per

il network rosso (modem, PPPoE, ecc...)
Servizi: usata per la configurazione e amministrazione dei servizi che il firewall ci fornisce (DHCP, web proxy, port forwading, ecc...)
VPN: utilizzata per la configurazione di una o più VPN.
Log: pagina dalla quale è possibile visualizzare tutti i log che il firewall crea durante il suo normale funzionamento.
Sistema: configurazioni di sistema ed utility associate all'affare volle che ci permettono, ad esempio, di effettuare gli update di sistema in maniera semi-automatica, impostare l'orologio, selezionare il linguaggio, attivare l'accesso SSH e il servizio IDS (IntrusionDetectionSystem), effettuare il backup della configurazione attuale e spegnere o riavviare il firewall stesso.
Il firewall ha due user autorizzati ad accedere all'interfaccia Web. Il primo (admin) ha accesso totale a tutte le funzioni; il secondo (dial) è abilitato soltanto ad effettuare la connessione o la disconnessione da Internet. Tale funzionamento e utile per non lasciare ad utenti maldestri o malintenzionati la possibilità di variare i settaggi del firewall pur concedendo loro la possibilità di effettuare la connessione o disconnessione. Di default l'user "dial" è disabilitato; per abitarlo è necessario settare la password per questo user. Vedremo in seguito come effettuare tale operazione.

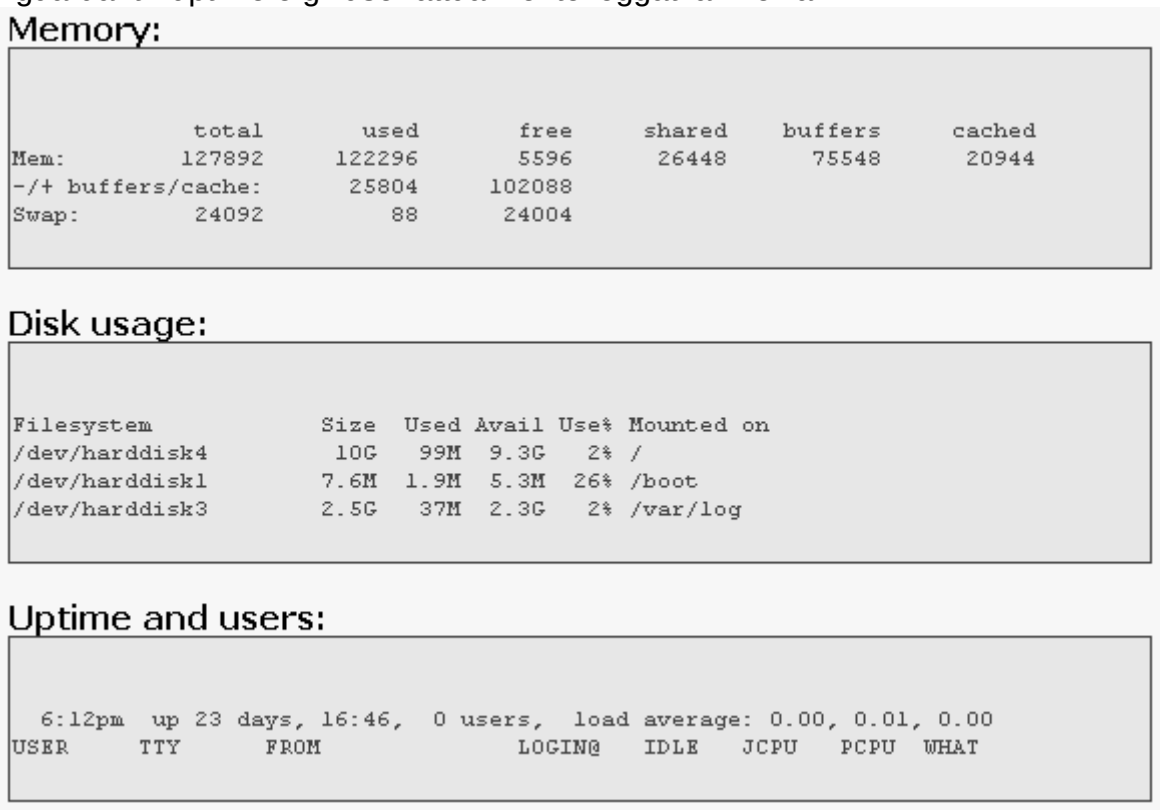
Pagina informazioni - sezione status



All'accesso a tale pagina vedremo che è divisa in quattro sottosezioni; disposta dall'una all'altra brani degli appositi link presenti in alto a destra. Nella sezione "Status" sarà possibile visualizzare i servizi attivi e non



lo stato della memoria, del disco fisso (che noteremo è stato diviso in tre partizioni) ed altri dati riguardanti l'uptime e gli user attualmente loggati al firewall



le interfacce collegate ed i dati caratteristici rispettivi di ogni interfaccia

Interfaces:

```
eth0      Link encap:Ethernet  HWaddr 00:48:54:1F:E5:B8
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1176562 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1395751 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:134924495 (128.6 Mb)  TX bytes:1347023823 (1284.6 Mb)
          Interrupt:10 Base address:0xbc00

eth1      Link encap:Ethernet  HWaddr 00:48:54:8F:3C:66
          inet addr:68.5.12.246  Bcast:68.5.15.255  Mask:255.255.252.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:9030208 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1029693 errors:0 dropped:0 overruns:0 carrier:0
          collisions:97092 txqueuelen:100
          RX bytes:2145000430 (2045.6 Mb)  TX bytes:123248449 (117.5 Mb)
          Interrupt:11 Base address:0xc000

ipsec0    Link encap:Ethernet  HWaddr 00:48:54:8F:3C:66
          inet addr:68.5.12.246  Mask:255.255.252.0
          UP RUNNING NOARP  MTU:16260  Metric:1
          RX packets:69657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69639 errors:0 dropped:9 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:6398394 (6.1 Mb)  TX bytes:10474386 (9.9 Mb)

ipsec1    Link encap:IPIP Tunnel  HWaddr
          NOARP  MTU:0  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

ipsec2    Link encap:IPIP Tunnel  HWaddr
          NOARP  MTU:0  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
```

i moduli caricati ed usati dal kernel e per ultimo le informazioni riguardanti il kernel stesso

Loaded modules:

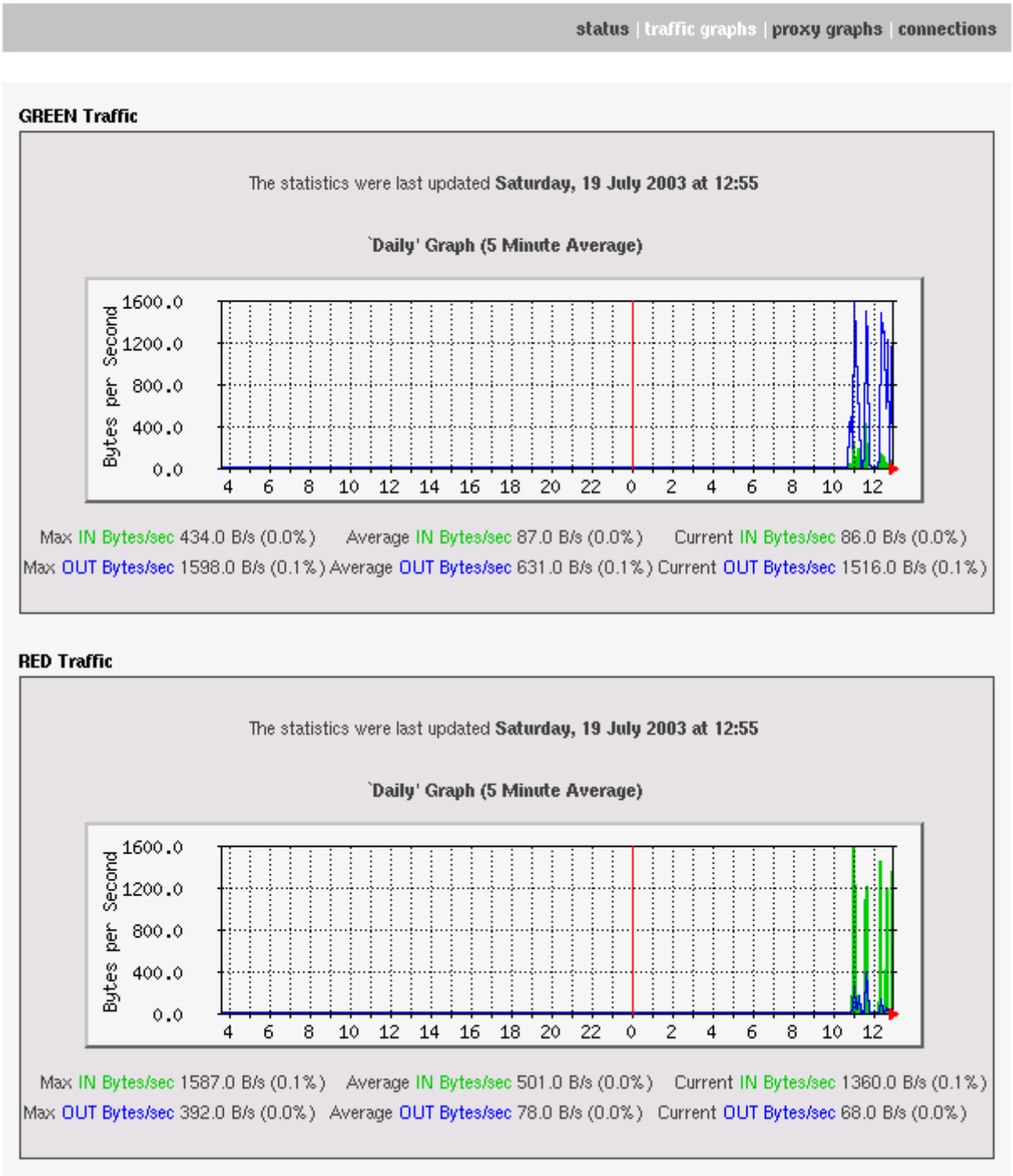
```
Module                  Size  Used by
rtl8139                13408   2
ip_masq_quake           2196   0 (unused)
ip_masq_pptp            5108   0 (unused)
ip_masq_irc             2960   0
ip_masq_icq            16704   0
ip_masq_h323            7960   0 (unused)
ip_masq_ftp             4704   0
ppp                    23328   0 (unused)
slhc                    5616   0 [ppp]
```

Kernel version:

```
Linux ostrich 2.2.23 #1 Thu Dec 26 15:08:35 EST 2002 i686 unknown
```

Pagina informazioni - sezione grafici traffico

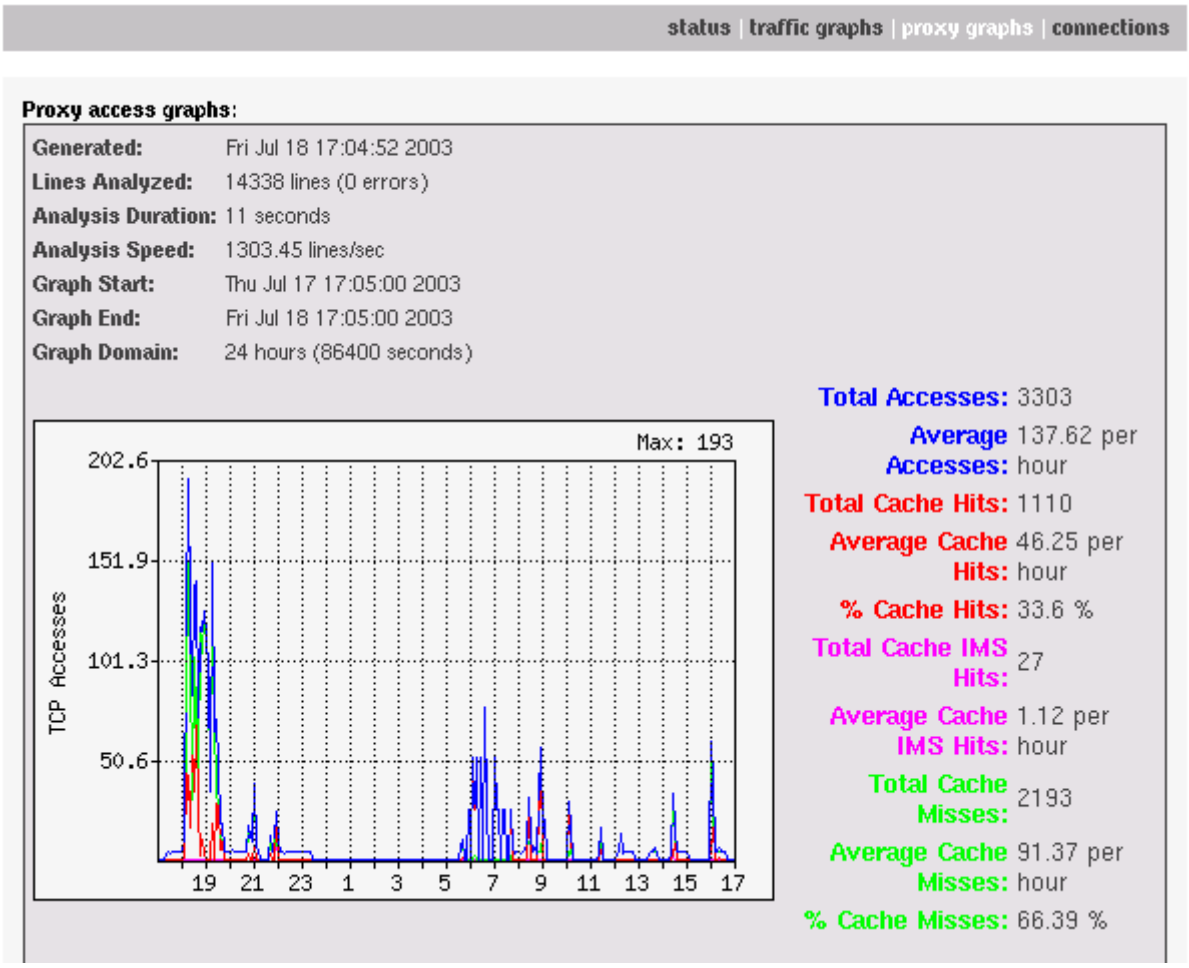
In tale pagina è possibile trovare in grafici del traffico effettuato nei network collegati per le ultime 24 ore; cliccando inoltre sulla freccia rossa in basso a destra di ogni grafico sarà possibile visualizzare in grafici specifici dell'interfaccia delle grafico selezionato di vigili per giorno, settimana, mese ed anno.



Pagina informazioni - sezione grafici proxy

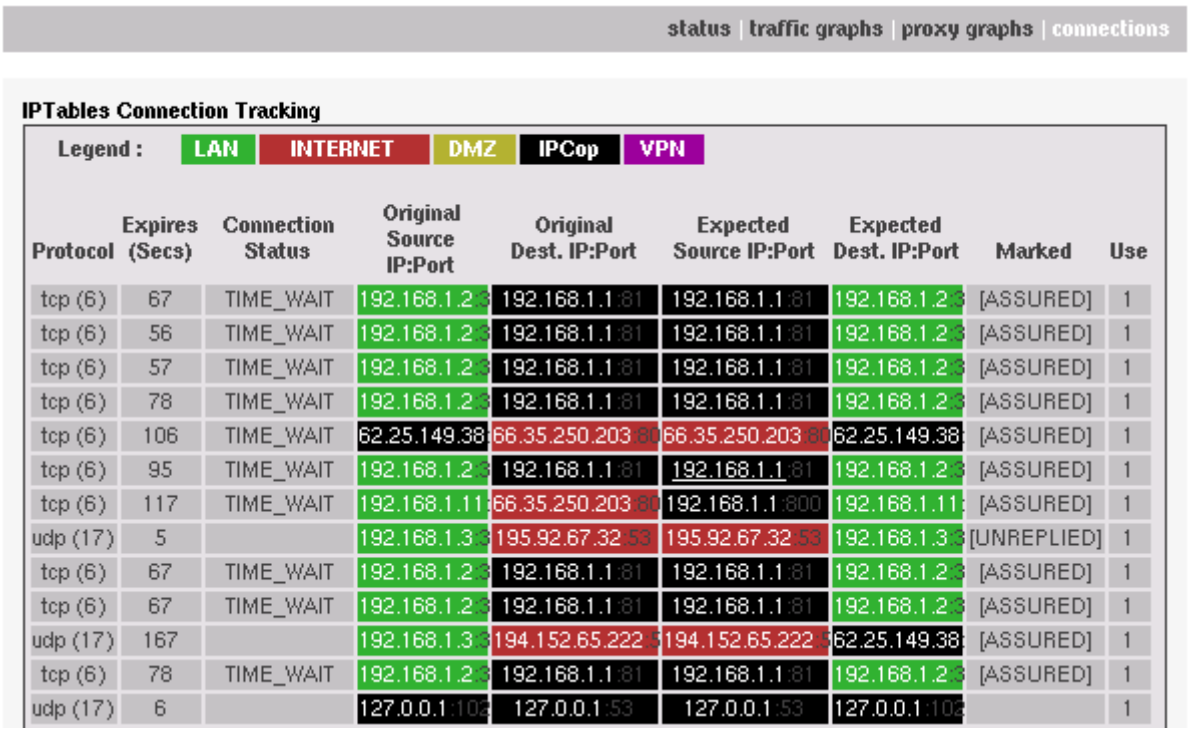
Qui vengono mostrati in grafici di accesso ed utilizzo dell'eventuale proxy abilitato con i

dati caratteristici che, in base all'esperienza, ci indicheranno la corretta o non corretta configurazione del nostro server proxy.



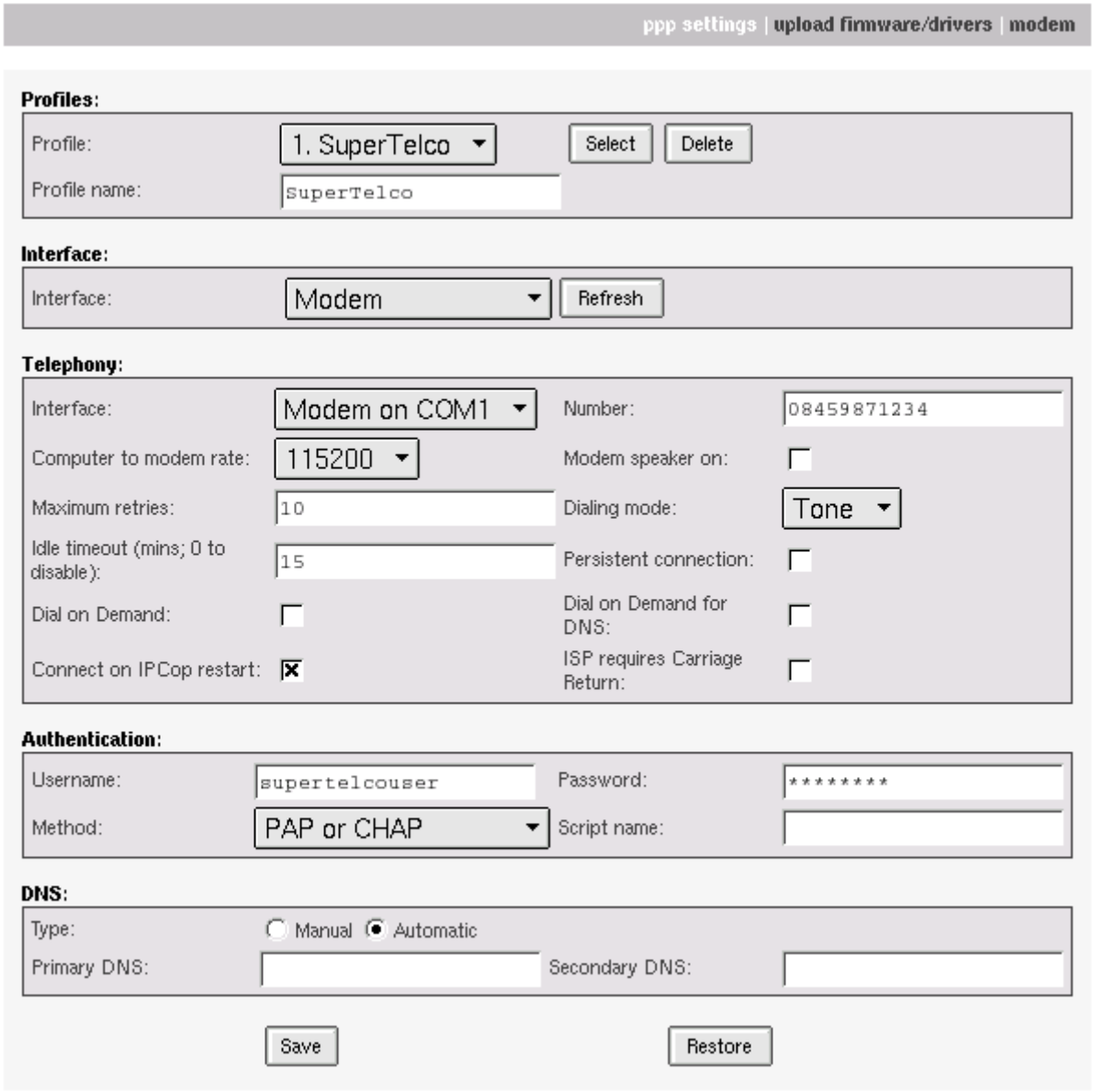
Pagina informazioni - sezione connessioni

Questo firewall usa le IPTables e/o Netfilter di linux per mantenere uno "Stateful firewall"; esso tiene traccia delle connessioni da e per ogni network collegato e c'è da un'indicazione in questa pagina fornendoci inoltre informazioni sul tipo di connessione effettuata. La diversa colorazione adottata ci indica inoltre dove sono situate (su quale network) le macchine oggetto del tracciamento.



Pagina Connessione - Sezione settaggi ppp

Questa pagina delle finestre di amministrazione della connessione è divisa in cinque differenti sezioni editabili e gioca un ruolo nella configurazione del firewall soltanto se il nostro accesso ad Internet avviene attraverso un modem analogico, un modem ISDN o una connessione DSL..



Profili

Nella prima sezione si possono selezionare gli eventuali profili registrati o eventualmente cancellarli; ad ogni profilo può essere associato un diverso sistema di collegamento ad Internet. Da notare che non è sempre possibile selezionare o modificare un profilo, non sarà possibile farlo quando il server è on-line o è in attesa di andare on-line che si trova nello stato di "Dial on Demand". Pertanto prima di utilizzare questa pagina bisogna andare nella pagina principale ed effettuare la disconnessione. Dopo aver selezionato il profilo di connessione desiderato si nuovamente tornare alla pagina principale e riconnettersi a Internet. Per salvare un profilo, dopo aver selezionato gli opportuni settaggi nelle sezioni seguenti, bisognerà premere il pulsante "SAVE" a fondo pagina; sarà comunque possibile ripristinare le eventuali modifiche fatte e non salvate per ogni profilo premendo il tasto "RESTORE".

Interfacce

Questa sezione della finestra ci permette di selezionare il device che noi utilizzeremo la

connessione. Potremmo trovare in tale sezione la possibilità di selezionare alternativamente modem, PPPTP, PPPoE e diversi altri sistemi in base a ciò che avremo specificato per l'interfaccia rossa nella precedente installazione del sistema.

Telefono

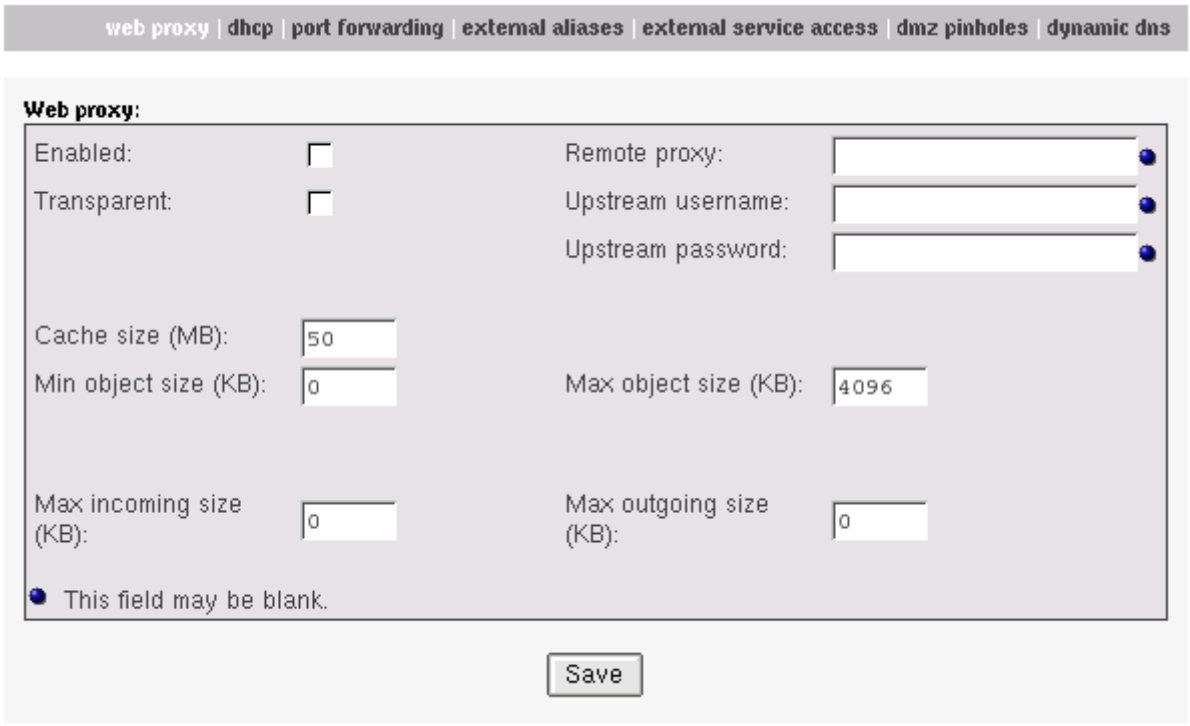
Questa sezione a diversi campi che devono essere riempiti o selezionati; bisogna quindi selezionare la corretta interfaccia di collegamento e, nel caso di collegamento tramite modem attaccato su porta seriale, bisognerà specificare la porta da utilizzare o, nel caso di connessione PPPoE, lasciare in bianco il campo. Nel caso di modem e quindi connessione, supponiamo, ISDN, bisognerà inserire il numero da chiamare e la velocità di collegamento dal modem con il PC. Nel caso di connessione tramite router e quindi, ad esempio, PPPoE, il campo andrà lasciato in bianco. Inseriamo inoltre il numero massimo di tentativi di collegamento da effettuare nel caso che il primo fallisca, e il tempo, in minuti, che deve passare senza che nessuno utilizzi la connessione prima che essa stessa sia chiusa (inserire zero nel caso di connessione flat).
I successivi flag ci permetteranno di rendere la connessione "persistente", e cioè fare in modo che il firewall mantenga attiva la connessione e che, anche in assenza di utilizzo, in caso di disconnessione tre commetta automaticamente se stesso ad Internet. Questa funzione può essere utile soprattutto nel caso in cui il sistema sia installato ed è in funzione 24/24h, in tal modo non ci sarà bisogno di nessuno che controlli l'effettiva connessione ad Internet anche, ad esempio, la notte. Precisiamo inoltre che i tentativi di riconnessione termineranno nel momento in cui raggiungeranno la cifra indicata poco più in alto che sarà necessario ricollegare il sistema di Internet tramite l'apposito tasto nella finestra di partenza. Ci sono poi i flag, utilizzati soprattutto con connessioni non flat, che ci permettono di effettuare automaticamente la connessione solo quando questa viene richiesta da un client servito dal sistema. Un altro flag ci permetterà di effettuare automaticamente il collegamento all'avvio della macchina, molto utile e con connessioni flat. In tal modo, settando opportunamente i flag ed eventualmente andando ad agire sul BIOS della macchina, sarà possibile fare in modo che nel caso venisse a mancare l'energia elettrica necessaria per il funzionamento automaticamente al ritorno dell'elettricità la macchina si accenda, carichi il sistema ed effettui automaticamente la connessione Internet senza che nessun operatore debba andare attivare alcunché.
Nella sezione di autenticazione andranno inseriti, se richiesti dal tipo di connessione, username e password forniti da chi ci ha dato l'accesso ad Internet. Potremmo altresì inserire uno script che andrà inserito nella directory "/etc/ppp" del sistema, nell'apposito campo inseriremo il solo nome senza percorso dello script. Un esempio di tale script si potrà trovare nella directory sopra citata.
Come ultima impostazione sarà possibile selezionare il tipo di DNS; automatico nel caso l'ISP ci dia questa possibilità, manuale nel caso, molto remoto, che tale possibilità non sia selezionabile.

Pagina Connessione - Sezioni "upload driver" e "modem"

Queste sezioni, delle quali tralasceremo di effettuare la descrizione in quanto di utilizzo intuitivo, ci permetteranno di effettuare un upgrade del firmware o del driver nei vari tipi di modem collegati ed anche di selezionare per alcuni di essi delle impostazioni particolari che ci permetteranno di utilizzare e configurare appieno il nostro hardware.

Pagina Servizi - Sezione proxy web

Questa sezione ci permetterà di configurare il proxy integrato nel firewall; non è necessario effettuare l'attivazione di tale servizio, il firewall funzionerebbe lo stesso anche senza. Abilitando però tale servizio sarà possibile, modificando opportunamente il sistema proxy installato, andare ad effettuare una gestione programmata di chi, come, quando deve accedere o no ad Internet.

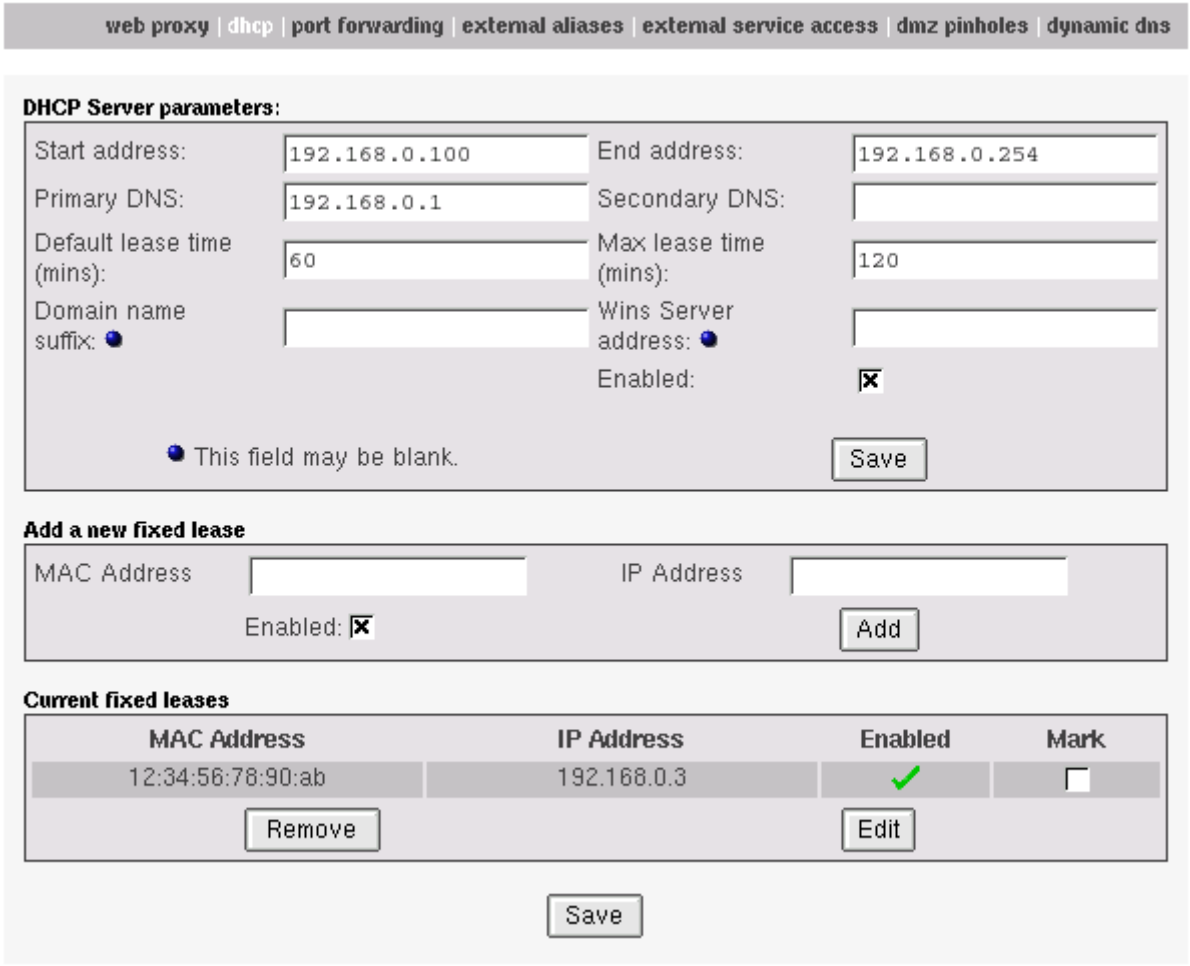


Il primo flag serve evidentemente per abilitare il sistema proxy, il secondo per rendere il funzionamento dello stesso trasparente all'utilizzatore. Questo funzionamento renderà quindi non necessaria la configurazione di ogni macchina collegata al network verde in quanto qualunque chiamata Internet verrà automaticamente gestita dal proxy senza che il sistema sia richiesta dei dati se ne accorga. Nel caso in cui la trasparenza non sia attivata bisognerà impostare manualmente sul sistema client l'indirizzo del firewall completo della porta utilizzata dal proxy nel formato "host_name:port_number"; nel caso, ad esempio, che il firewall presenti l'interfaccia sul network verde con indirizzi IP 192.168.1.100 si dovrà inserire nei client di utilizzare come proxy "192.168.1.100:800" in quanto la 800 e la porta utilizzata per i servizi proxy. Potremmo inoltre inserire in questa finestra il proxy che ci fornisce il nostro ISP; in tale situazione il proxy in locale farà richiesta al proxy che specificheremo nell'apposito campo, completo di username e password nel caso ciò venisse richiesto per il corretto accesso.
Potremmo inoltre andare a specificare la quantità di spazio sull'HD dedicata alla cache del proxy; attenzione che un valore troppo elevato, pur permettendo il salvataggio in locale di molti più dati, potrebbe rallentare la nostra navigazione se l'accesso a questi avvenisse in maniera più lenta che non scaricando direttamente da Internet. Precisiamo inoltre che, per problemi di privacy, non verranno salvate nella cache le pagine web con protocollo "https" e le pagine in cui vi sia un'immissione di username e password.
Potremmo inoltre variare le dimensioni minime e massime che possono avere gli oggetti salvati sulla cache; di default verranno salvati tutti i file con dimensione compresa tra 0 e 4 Mb (4096 Kb). Sarà inoltre possibile specificare la dimensione massima degli oggetti in ingresso e in uscita per impedire rispettivamente il download e l'upload di file di dimensioni

elevate che potrebbero compromettere il buon funzionamento dal network. Di default tali valori sono impostati a zero e non vi è quindi alcun vincolo a tale riguardo.

Pagina Servizi - Sezione DHCP

Questa sezione ci permetterà di configurare opportunamente il server DHCP del firewall utilizzato nel network verde; la sua mancata abilitazione non pregiudica il buon funzionamento del firewall stesso, se ne sistema è già presente un servizio di questo tipo si potrà tranquillamente lasciarlo disabilitato.

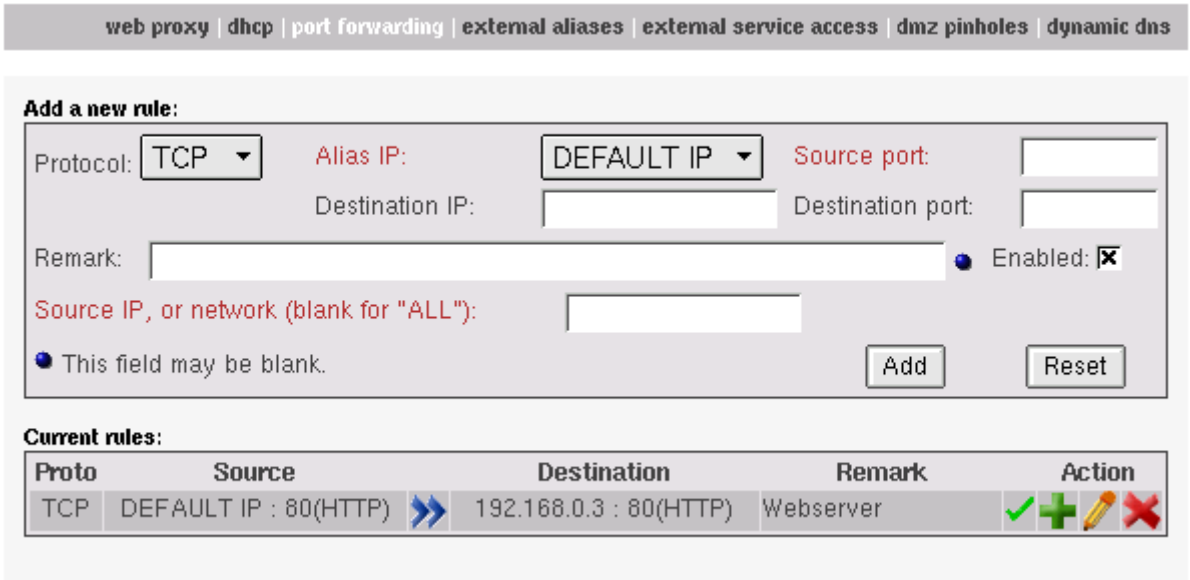


Tralasciando cos'è un server DHCP, diciamo solo che fornirà ai PC che ne faranno richiesta un indirizzo IP univoco; in questa finestra potremmo perciò inserire l'indirizzo IP di inizio e fine del range che ci interessa a segnare. Possiamo inoltre specificare l'indirizzo IP del server DNS; avendo il firewall stesso un DNS proxy potremmo inserire come indirizzo primario l'IP dello stesso firewall e come secondario quello di un altro server presente nel nostro network. Potremmo inoltre inserire il tempo di default e il tempo massimo entro il quale il client che faranno richiesta di indirizzo IP dovranno confermare l'avvenuta "presa" dell'IP stesso; se ciò avverrà quell'IP non verrà più fornito ad alcuna altro PC che ne faccia richiesta. Nel caso invece in cui si superi il tempo massimo di conferma quel indirizzo tornerà disponibile per una richiesta successiva. Potremmo inoltre inserire, se richiesto dal server DHCP dell'ISP, il nome del dominio, che verrà inserito come suffisso ad ogni richiesta effettuata all'ISP; ciò può essere utile nel caso in cui il nostro fornitore di accesso setti un nome di dominio di default nel network al quale ci si collega e non riconosca valide chiamate effettuate da computer che non siano inseriti nel dominio. Potremmo inoltre

inserire l'indirizzo del server Wins.
Potrebbe essere necessario in alcuni ambiti aziendali che determinati personal computer ricevano determinati IP fissi la cui mancanza potrebbe pregiudicare il corretto funzionamento degli stessi o dei programmi installati; a tale funzione serve la sezione seguente, che ci permetterà di assegnare alcuni indirizzi IP alle macchine che presentino un certo "MAC address". Ogni scheda di rete a un suo specifico "MAC address" e tramite tale valore potremo riconoscere il PC che ne farà richiesta e assegnargli il corretto indirizzo IP. Una lista dei IP assegnati verrà mostrata nella sezione subito dopo.

Pagina Servizi - Sezione port-forwading

Questa pagina ci permette di effettuare la gestione delle porte. È qui occorre fare qualche premessa:
La funzione di un firewall è quella di bloccare qualunque accesso dall'esterno verso l'interno della rete protetta; ciò viene fatto bloccando qualunque tentativo di accesso su tutte le porte esistenti. In alcuni casi questa situazione potrebbe andare un po' stretta. Nel caso in cui all'interno della rete sia presente un server che fornisce un servizio su richiesta e che tale server debba essere accessibile anche dall'esterno, ciò non potrà venire in quanto tutte le chiamate in entrata da Internet sulla porta utilizzata dal servizio su server interno verranno automaticamente bloccate dal firewall. Si pensi ad esempio a sistemi P2P, servizi di time server e tutti quei servizi che fanno utilizzo di porte TCP e UDP varie nel loro normale funzionamento; potrebbero verificarsi dei malfunzionamenti generici o addirittura dei mancati funzionamenti. Questa pagina ci permetterà di "deviare" una specifica porta dal network grosso verso una specifica porta e indirizzo IP dal network verde.



Innanzitutto dovremo selezionare il protocollo TCP o UDP da "fowardare"; lasceremo "Default IP" sul campo subito a destra ed andremo inserire in "Source port" il numero della porta cui avverrà il passaggio dati da Internet. Successivamente andremo ad inserire l'indirizzo IP e la porta di destinazione all'interno dal nostro network verde che dovrà gestire le chiamate e il traffico dati su quella porta. Nel campo "Remark" potremmo inserire un commento che ci ricordi il motivo per cui quella regola di forwading è stata creata. Potremmo settare più di una regola, quelle già settate si vedranno nella lista appena sotto. Potremmo inoltre specificare nel campo "Source IP" a quale indirizzo o range di indirizzi

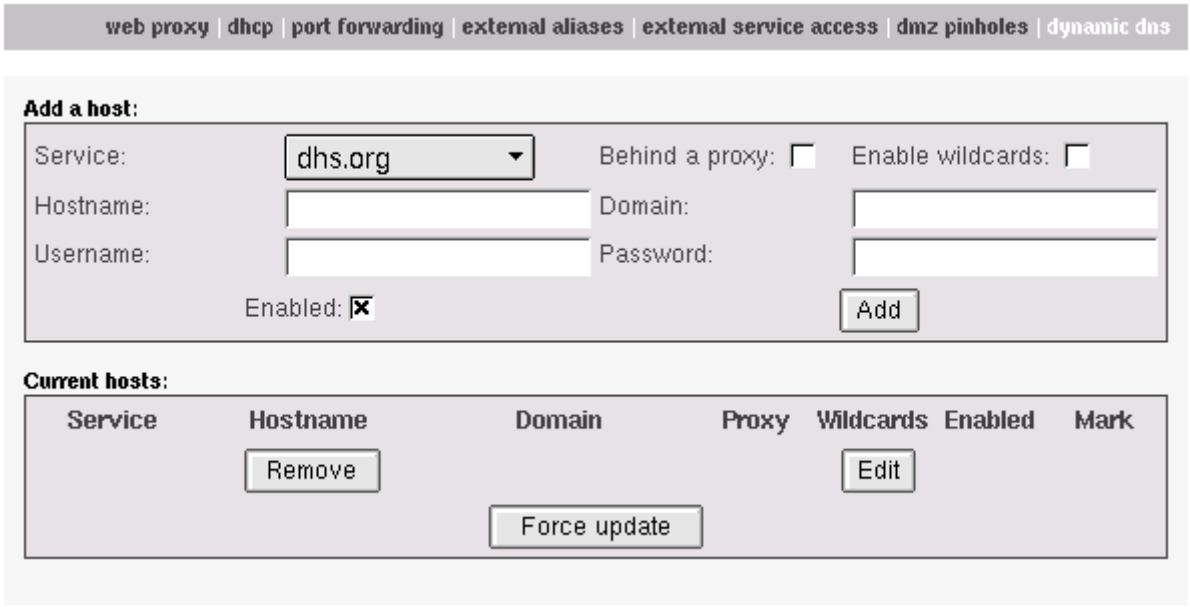
Internet ci riferiamo per l'applicazione di quella specifica regola.
Ci sono alcune note al riguardo di questo servizio; non viene ad esempio supportato il protocollo GRE. Nell'inserimento del numero della porta sono abilitate le wildcards; ad esempio la scritta "1-65535" significherà "dalla porta 1 alla porta 65535" ed altresì la scritta "*-500" significherà "tutte le porte fino alla 500". Alcune porte non potranno essere utilizzate con questo sistema in quanto già utilizzata dal firewall per alcuni servizi interni; esse sono la 67, 68,81, 222 e 445. Troveremo in ogni riga della lista sotto tre possibili azioni selezionabili rami di altrettanti tasti presenti sulla destra di ogni riga; tali tasti ci permetteranno, nell'ordine, di abitare e/o disabilitare la regola, modificarla o cancellarla.

Pagina Servizi - Sezioni "external aliases", "external service access" e "DMZ pinholes"

Le prime due sezioni ci serviranno per settare gli alias esterni e gli accessi esterni consentiti verso il nostro firewall. Essendo nostra intenzione rendere sicuro il sistema dirò solo che queste sezioni servono per attivare l'accesso alla macchina che ci funge da server da Internet e quindi dal network rosso; ciò potrebbe compromettere la sicurezza del sistema è pertanto non vanno utilizzati se non con la dovuta accortezza e dopo avere letto per bene, e soprattutto avere capito, il funzionamento degli stessi. Una descrizione esauriente del loro funzionamento si potrà trovare nel manuale in inglese fornito assieme al firewall.
La terza sezione ci permetterà di far funzionare correttamente il firewall nel caso si usi un sistema che preveda una DMZ. Come già detto in precedenza questa zona fa parte dell'opzionale network arancione su cui di solito andranno collegati i server che dovranno essere sempre accessibili da Internet ma non connessi alla LAN per ragioni di sicurezza. Andremo perciò a settare in questa pagina le opzioni che ci permetteranno di reindirizzare il traffico di determinate porta verso gli IP e porte oppurtuni dei server collegati al network arancione.

Pagina Servizi - Sezione dynamic dns

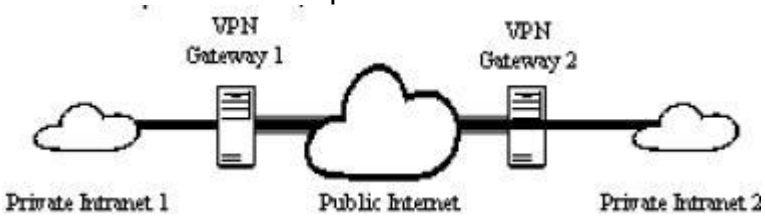
Questa pagina ci permetterà di utilizzare uno dei servizi di DNS dinamico che forniscono alcune società. Io personalmente ho utilizzato con successo il servizio di "NO-IP" e devo dire che funziona ottimamente.



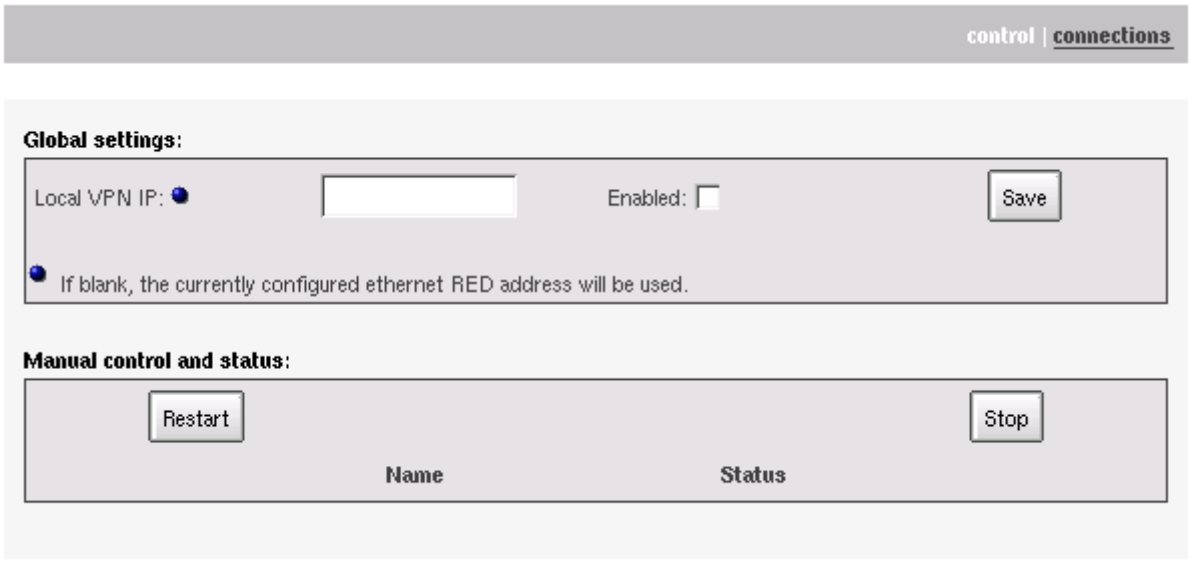
In termini pratici potremmo assegnare all'indirizzo IP che il nostro network detiene nell'accesso a Internet un indirizzo alfanumerico del tipo "miarete.no-ip.com" o simile nel caso si scelga un diverso fornitore del servizio; ciò risulta utile nel momento in cui dobbiamo ad esempio effettuare una chiamata su di una porta su cui abbiamo abilitato un servizio di reindirizzamento verso un server interno al network verde o a quello arancione. Piuttosto che dover digitare l'indirizzo IP e magari, nel caso in cui non abbiamo indirizzo statico, ciò sia variato nel tempo e quindi ci troveremo nell'impossibilità di accedere al servizio, potremo digitare l'indirizzo alfanumerico che ci permetterà di collegarci correttamente al servizio in quanto l'associazione tra indirizzo IP e indirizzo alfanumerico viene aggiornata ogni quindici minuti (se non ricordo male) dal firewall stesso. In questa pagina andranno perciò inseriti i dati di riconoscimento che vengono forniti dalle società che forniscono il servizio di DNS dinamico per un corretto funzionamento dello stesso.

Pagina VPN - Sezione controllo

Direi innanzitutto di riscrivere il concetto di VPN; è un sistema di comunicazione protetto tramite l'attivazione di un canale criptato e da cui si accede solo con opportune chiavi che permette il collegamento sicuro attraverso una rete insicura e pubblica quale può essere Internet. Graficamente può essere riassunta nell'immagine che segue.



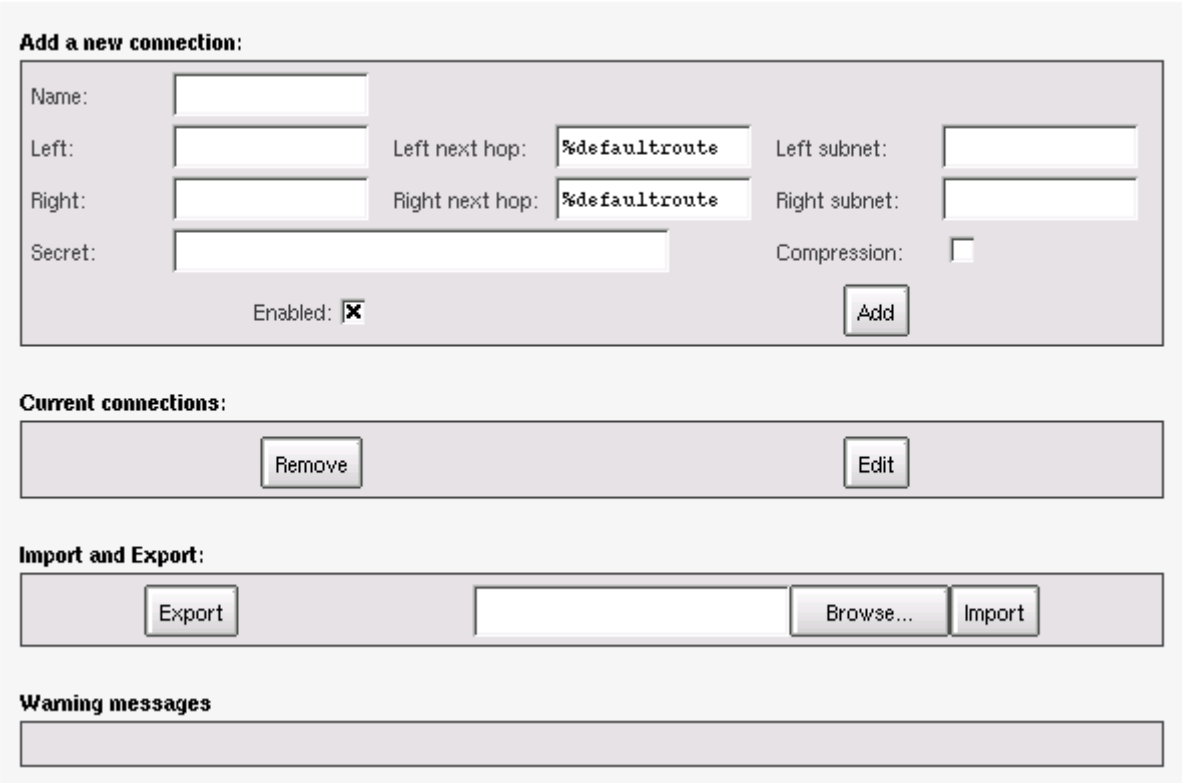
In questo diagramma ci sono due intranet collegate attraverso una VPN tramite alcuni gateway che si appoggiano sulla rete Internet esistente utilizzandola come canale di collegamento. Dal punto di vista lavorativo questo viene realizzato incapsulando i dati provenienti da una intranet e che devono arrivare all'altra in un pacchetto IP ordinario che verrà trasportato tramite Internet; tali dati verranno opportunamente criptati dal gateway di partenza prima dell'invio e decriptati all'arrivo automaticamente dal gateway di destinzione prima di raggiungere le macchine interne alla intranet. Perché ciò funzioni correttamente bisogna che ci sia una buona connessione tra i due gateway e i network collegati tramite VPN devono essere in spazi di indirizzi "non-overlapping" (non sarà quindi possibile collegare un network e che abbia indirizzi IP 192.168.0.0/24 ed un altro network e che abbia192.168.0.128/25). Una buona connessione è d'obbligo per evitare perdite di pacchetti o latenza troppo elevata degli stessi che se sarebbero molto sulla performance totale del sistema, come d'altronde sarebbe auspicabile una routing ad hoc.
Cominciamo comunque col descrivere il sistema del nostro firewall.



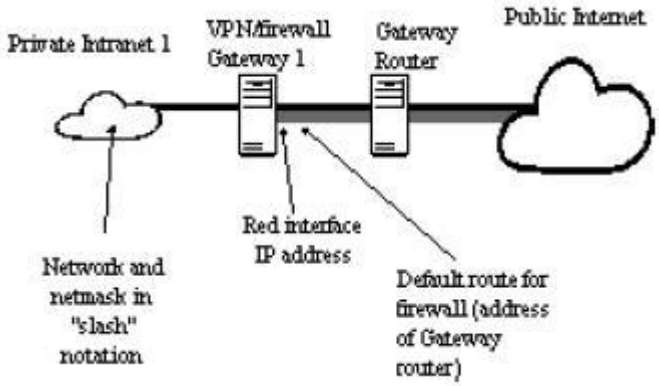
Questo firewall è in grado di stabilire connessioni VPN da e verso una rete remota. La VPN creata utilizza il supporto IPSec ed un sistema standard di tecnologia di criptazione denominato 3DES. Tramite questa pagina è possibile fermare, riavviare, attivare e disattivare una VPN. Nel campo dell'indirizzo IP è possibile specificare quale IP deve essere usato dal firewall come termine della connessione VPN; se il campo viene lasciato in bianco viene automaticamente utilizzato l'indirizzo dell'interfaccia rossa. Cliccando sul flag di abilitazione e successivamente sul tasto "SAVE" vengono salvati i settaggi creati. Nella sezione successiva vengono mostrati, nel caso di VPN attiva, lo status della stessa in quel momento e le eventuali connessioni esistenti.

Pagina VPN - Sezione connessioni

Per creare una VPN tra il firewall e un'altra VPN IPSec, quale potrebbe essere un altro firewall dello stesso tipo, occorrono alcune importanti informazioni che vanno inserite su questa finestra. Le informazioni inserite devono essere alquanto precise su entrambi i punti di accesso VPN, in quanto una non corrispondenza dei parametri porta all'impossibilità di creare una connessione correttamente. Maggiori informazioni sull'uso e la configurazione di questi parametri possono essere trovati nei siti di riferimento:
http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopDocumentationv01
http://www.freeswan.org/
http://jixen.tripod.com/
Non avendogli effettuato prove di collegamento VPN posso solo tentare di tradurre correttamente ciò che viene scritto nella guida ufficiale del firewall. Pertanto non prendete per oro colato ciò che scrivo ma spero possa essere un buon punto di partenza per chi voglia avventurarsi in tali test; sarebbe inoltre gradito da chi scrive e da chi legge successivamente che eventuali prove effettuate e andate a buon fine vengano documentate e illustrate per una maggiore comprensione del sistema.



Potremo innanzitutto inserire nella sito campo un nome da assegnare alla connessione e ai settaggi che andremo inserire; potremo così impostare diverse connessioni ed attivare quella che ci serve al momento che ci serve lasciando inalterati i settaggi e non dovendo di riscrivere ogni volta. I successivi campi "left" e "right" e di campi immediatamente al lato di questi ci permetteranno di inserire i parametri corretti che permettono la connessione vera e propria. Per sinistra e destra si intendono (presumo) i due punti della connessione VPN; andiamone ad analizzare un lato, che potremo riassumere nell'immagine seguente:



Sono tre le informazioni che ci bisognano: l'indirizzo IP dell'interfaccia rossa del firewall, l'indirizzo IP che ci fa il routing e l'indirizzo IP e la maschera del network da collegare (quindi il nostro caso l'indirizzo dell'interfaccia verde e la relativa netmask). L'indirizzo IP dell'interfaccia rossa si può tenere facilmente digitando, dopo essersi autenticati nel firewall come utente root, il comando "ifconfig" o "ifconfig eth2" nel caso in cui la nostra interfaccia rossa sia riconosciuta dal firewall come "eth2", ottenendo pressappoco il risultato di seguito illustrato

```
root@smoothwall~# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:40:05:74:35:12
          inet addr:64.131.159.150  Bcast:64.131.159.255  Mask:255.255.255.128
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259318 errors:0 dropped:0 overruns:0 frame:0
          TX packets:282351 errors:0 dropped:0 overruns:0 carrier:0
          collisions:13 txqueuelen:100
          Interrupt:10 Base address:0x240
```

nel quale risulta già evidenziato l'indirizzo che a noi interessa. Potremmo successivamente utilizzare il comando "netstat -nr" che ci permetterà di visualizzare le informazioni che ancora ci mancano, come illustrato in

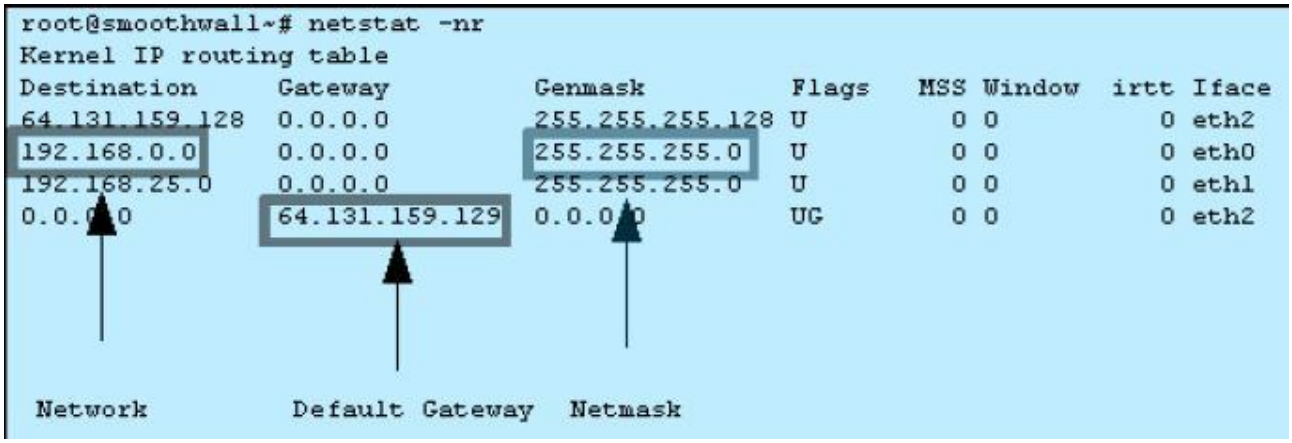


immagine. Bisogna precisare che la maschera dovrà essere inserita in "slash notation"; quindi una breve tabella per la conversione tra i due formati.

bitlength	netmask	IPs usable
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0 (point-to-point)
/32	255.255.255.255	0 (single-host netmask)

A dire il vero secondo la guida in inglese non è necessario inserire l'IP che ci fa il routing, basta lasciare la scritta che già si trova all'interno del campo "left next hop"; verrà utilizzato quello che ci fornisce il nostro ISP.
Successivamente andrà inserita la password che ci permetterà di criptare e decriptare i dati in partenza e in arrivo ed eventualmente attivare la compressione dei dati tramite l'apposito flag. Premendo a questo punto il tasto "ADD" verranno salvati i parametri inseriti che potranno poi eventualmente essere modificati o cancellati. Da notare la possibilità di esportare ed importare questi parametri da un firewall all'altro tramite un singolo file di configurazione.

Pagina Log

Questa sezione consiste in quattro sotto pagine: other, webproxy, firewall e IDS. È possibile da qui esaminare i log del firewall in alcune delle sue parti per effettuare dei controlli sull'utilizzo effettivo della rete, delle connessioni e così via. È anche possibile esportare i log visualizzati in dei file in formato testo e procedere alla loro analisi con programmi esterni che ci potranno facilitare nella nostra ricerca. Ma andiamo ad analizzare le quattro sotto pagine in maniera ordinata.

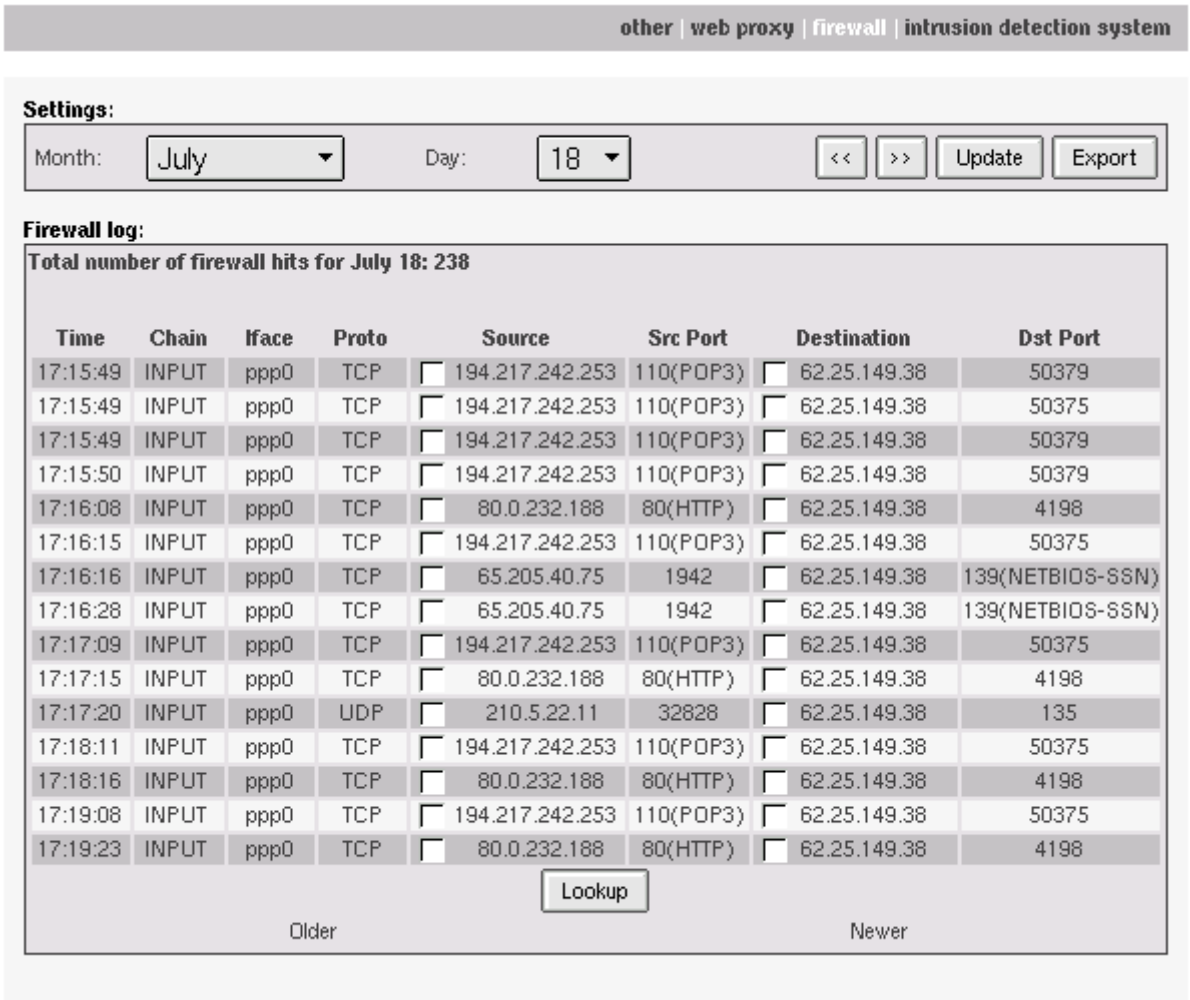
Pagina Log - Sezione Other

Questa pagina ci permette di visualizzare i log di sistema ed altri; in totale sono nove differenti categorie selezionabili tramite il comando a scomparsa "Section" e sono:
IPCop : in questo log potremo trovare informazioni standard fornite dal firewall quali ad esempio la connessione o disconnessione da Internet, l'aggiornamento del servizio di reindirizzamento (NO-IP e gli altri) e gli orari in quali questi avvenimenti sono caduti.
PPP : per potremo trovare log del traffico inviato attraverso l'interfaccia che provvede al collegamento PPP; questo include quindi gli eventuali messaggi di errore che ci potranno tornare molto utili nel caso in cui non riusciremo a collegarci correttamente ad Internet.
ISDN : verranno dimostrate le attività relative alla nostra unità ISDN.
DHCP : qui verrà indicato cosa il nostro server DHCP ha fatto per noi.
SSH : questo log ci permette di registrare quali utenti hanno avuto accesso al firewall e quando; saranno elencati gli utenti che hanno fatto i logon in remoto tramite interfaccia SSH (vedremo poi come si fà).
Login/Logout : qui troveremo gli stessi dati del precedente log aggiunti a quegli accessi fatti tramite la tastiera del firewall stesso.
Kernel : un registro delle attività del Kernel.
IPSec : un registro delle attività dell'IPSec utilizzato dalle connessioni VPN.
Update transcript : qui verranno visualizzati i log relativi alle attività di aggiornamento del firewall stesso disponibili nella successiva pagina servizi.
Potremmo inoltre, selezionando gli appositi comandi, effettuare la ricerca nel mese e nel giorno di nostro interesse e spostarci eventualmente con i tasti "<<" e ">>" avanti e indietro oltre a poter effettuare l'esportazione dei dati tramite l'apposito tasto.

Pagina Log - Sezione web proxy

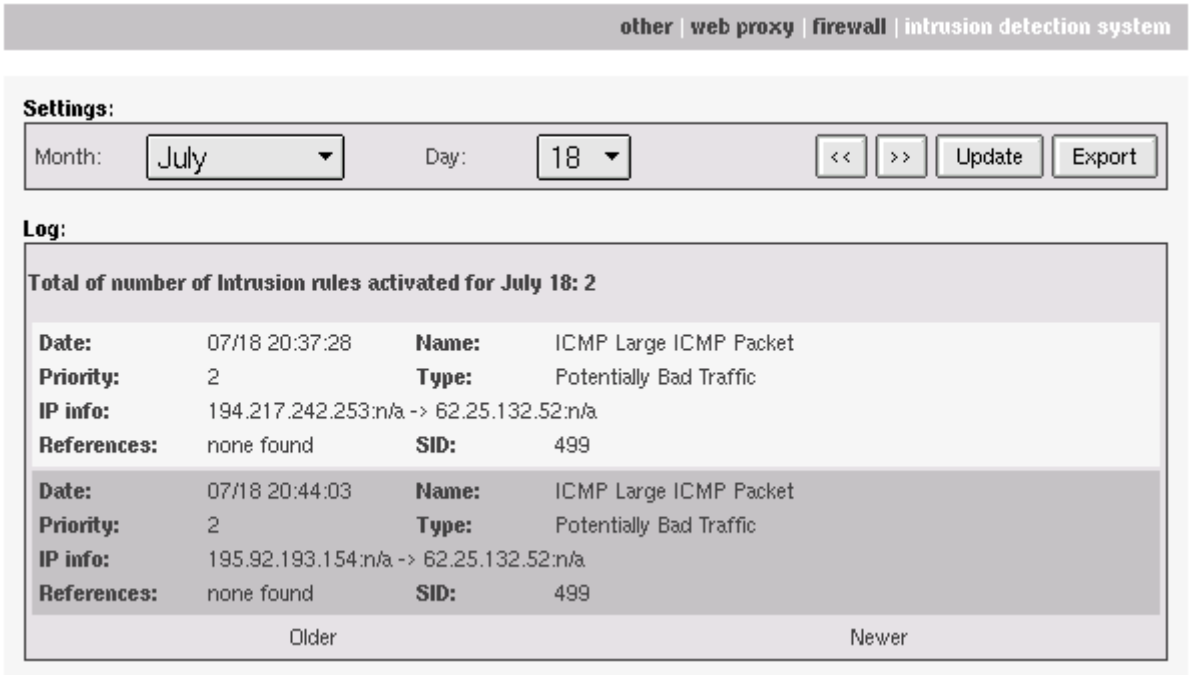
Questa pagina provvede a facilitarci la ricerca dei file che sono stati richiesti al proxy web se precedentemente attivato; sarà quindi possibile ottenere un log di tutte le richieste effettuate dal nostro network con l'indicazione per ogni richiesta dell'indirizzo IP del richiedente, l'orario e la richiesta effettivamente fatta. È inoltre possibile eliminare dal log le richieste di file con le estensioni più comuni che potrebbero disturbare la visione e l'analisi dei dati tramite l'apposito campo "Ignore filter". Attenzione deve essere prestata sull'uso di quanto qui visualizzato in quanto potrebbe andare in violazione dei diritti di privacy degli utilizzatori delle macchine interne alla nostra intranet.

Pagina Log - Sezione firewall



Questa pagina ci visualizza i pacchetti di dati bloccati dal nostro firewall. Ci viene quindi mostrato l'orario, il "chain", interfaccia, il protocollo, gli indirizzi IP di destinazione e di partenza, la porta originariamente aperta e quella aperta successivamente. Sarà possibile ottenere informazioni su uno specifico indirizzo IP in lista cliccando sul flag accanto lo stesso indirizzo e successivamente sul tasto "lookup".

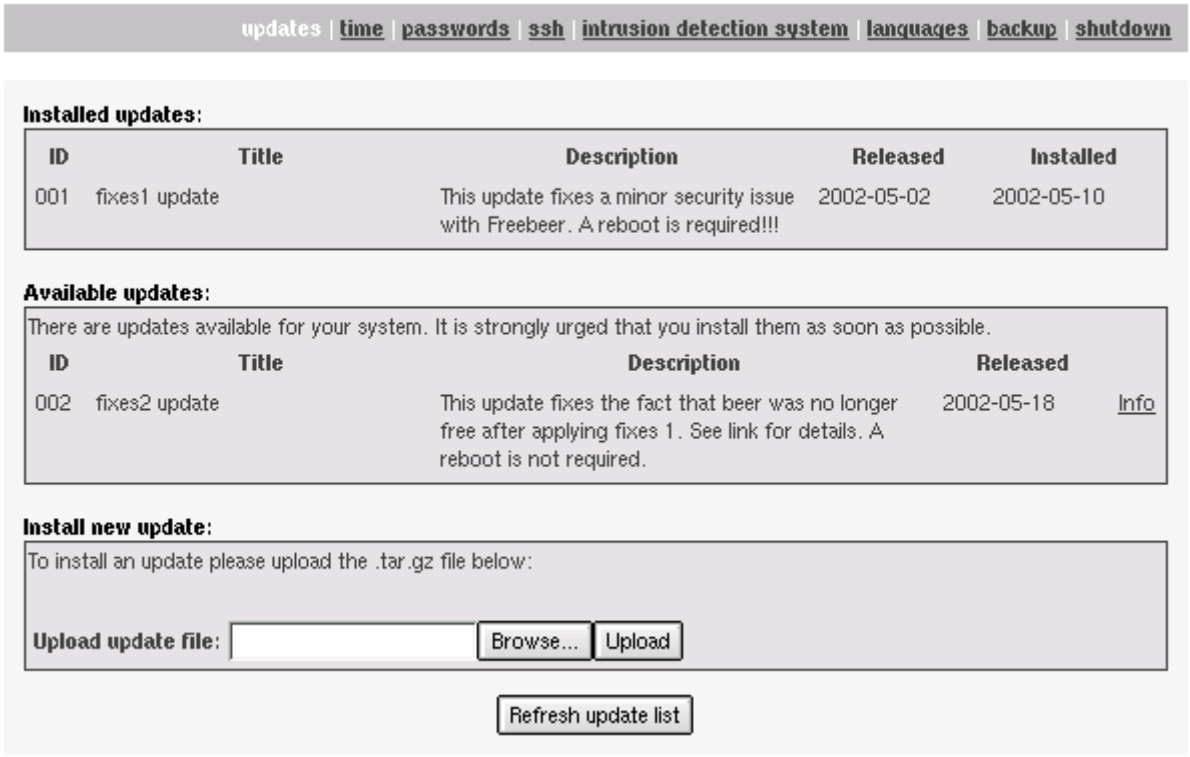
Pagina Log - Sezione Intrusion Detection System



Verranno qui elencati i tentativi di accesso registrati dall'IDS. Per ogni tentativo di accesso ci verrà fornita da data del tentativo, il nome del tipo di attacco subito, la priorità dello stesso espressa in gradi dal 1 al 3 (1 grave, 2 lievemente grave, 3 possibilmente grave), il tipo di attacco subito, gli indirizzi IP e l'eventuale netmask di provenienza dell'attacco, una eventuale link ad una pagina di riferimento sul tipo di attacco subito ed il numero SID. Quest'ultimo è lo "Snort ID"; Snort è il modulo software utilizzato dal nostro firewall per provvedere alle funzioni di IDS e tramite questo numero è possibile reperire molteplici informazioni sul tipo di attacco subito. Maggiori informazioni si potranno trovare sul sito di riferimento per Snort.

Pagina Sistema - Sezione update

Questa sezione ha tre precise funzioni: illustrarci le patch installate, informarci sulla disponibilità di nuove patch e applicare le stesse al nostro firewall.



Ogni volta che ci commettiamo ad Internet il nostro firewall fa un check per controllare che non ci siano nuovi update e patch disponibili; sarà comunque possibile fare un refresh della situazione tramite l'apposito tasto in fondo alla pagina. Avremo quindi un elenco delle patch installate e di quelle ancora da installare delle quali ci viene fornita la pagina di riferimento da cui scaricarle. Dopo aver effettuato il download delle stesse sulla macchina che utilizziamo per collegarci al firewall sarà possibile applicarle premendo il tasto "Browse"; si aprirà una maschera tipo "esplora risorse" che ci permetterà di andare a localizzare il file le precedentemente scaricato in formato ".tar", selezionarlo e cliccare "ok". Successivamente premere il tasto "upload" e la patch verrà applicata al firewall. Bisogna prestare attenzione al fatto che alcune di queste patch per essere funzionanti richiedono il riavvio del firewall stesso; inoltre, secondo quanto indicato nei manuali in inglese, il browser Opera non funziona correttamente nell'applicazione delle patch.

Pagina Sistema - Sezione time

Questa sezione ci serve per sincronizzare l'orologio della macchina firewall utilizzando un server NTP (Network Time Server). L'utilizzo di questa sezione è intuitivo, basterà inserire uno o due indirizzi di server NTP, abilitare il sistema, decidere ogni quanto deve essere effettuata la sincronizzazione e poi cliccare sul tasto "save".

Pagina Sistema - Sezione password

Questa sezione è utile nel caso in cui bisogna impostare le password degli utenti "admin" e "dial". Ricordiamo che mentre l'utente "admin" ha accesso completo alle pagine di amministrazione, l'utente "dial" può soltanto effettuare la connessione o disconnessione da Internet. Queste password sono valide solo per l'accesso via Web e non per l'accesso a linea di comando.

Pagina Sistema - Sezione SSH

Questa sezione ci permette di abilitare o di abilitare l'accesso SSH al nostro firewall dall'esterno (dal network verde); come per l'HTTP la porta è la n. 81 e per l'HTTPS la porta è la n. 445, per l'SSH la porta è la n. 222. Bisogna prestare attenzione all'abilitazione di questa opzione in quanto ci permette, senza possesso di user è password corretti, di accedere da remoto alla macchina firewall in maniera completa. Sarebbe perciò da abilitare solo se in caso di effettiva necessità e comunque solo per il tempo strettamente necessario alle operazioni da compiere.

Pagina Sistema - Sezione IDS

Questa sezione ci permetterà di abilitare l'intrusion detection system di cui abbiamo parlato precedentemente.

Pagina Sistema - Sezione languages

È intuitivo il fatto che questa sezione serba ad effettuare un cambio del linguaggio delle pagine Web di amministrazione del firewall; bisognerà caricare per alcune di queste gli opportuni update con i sistemi già precedentemente mostrati.

Pagina Sistema - Sezione backup

Questa sezione ci permette di effettuare un salvataggio dei file di configurazione del nostro firewall permettendoci quindi, nel malaugurato caso in cui il nostro hardware si guasti, di riattivare una nuova installazione su una nuova macchina con tutti i settaggi e parametri già impostati nella precedente, risparmiandoci quindi un bel po' di tempo lavorativo è permettendoci anche una veloce riattivazione del servizio Internet. Vi posso assicurare per esperienza personale che è una funzione utilissima.
Poniamo il caso di aver installato il firewall in un'azienda e che purtroppo si sia guastata la macchina e bisogna sostituirla; se avremmo precedentemente attuato il salvataggio dei dati di configurazione ci basterà inserire il floppy quando richiesto durante la nuova installazione ed automaticamente verranno caricati tutti parametri impostati precedentemente con notevole risparmio di tempo per la riattivazione dei servizi e conseguentemente minore fastidio per la mancanza di un servizio.
Per effettuare il salvataggio di questi dati bisognerà inserire nello lettore floppy della macchina firewall un dischetto già formattato da un sistema linux; il comando per effettuare ciò è "fdformat /dev/fd0". Dopo aver premuto il pulsante di salvataggio nella sezione informazioni poco sotto potremo vedere quali file siano stati salvati e il loro esito di salvataggio.

Pagina Sistema - Sezione shutdown

Anche per questa sezione l'uso è intuitivo, potremo andare a spegnere la macchina o effettuare il riavvio della stessa nel caso ad esempio di un'installazione di una patch che richiede il riavvio del firewall.

Termina qui la guida che mi ero prefissato di scrivere, varie parti della stessa sono state apprese dai relativi manuali di installazione e amministrazione del firewall in inglese, spero di aver fatto un lavoro corretto e sarò ben felice di accettare critiche o correzioni allo stesso in quanto non sono perfetto e quindi qualcosa di sbagliato sicuramente ci sarà. Nella speranza che quanto qui scritto possa servire a qualcuno e comunque nella certezza di essere personalmente appagato per il lavoro effettuato mi rimetto ai lettori per consigli, correzioni e soprattutto aggiunte alla guida scritta; come disse qualcuno più "acculturato" di me: "...ai posteri l'ardua sentenza, nui chiniam la fronte al massimo fattor...".

Russo Antonino
tonyfumetto@hotmail.com