

IPCop: *un pinguino come Firewall*

Rino Andriano

rino[at]lugbari[.]org

ottobre 2006



Copyright (C) 2006 Rino Andriano (rino at lugbari dot org)

La copia letterale e la distribuzione di questa presentazione nella sua integrità sono permesse con qualsiasi mezzo, a condizione che questa nota sia riprodotta.

Sommario

- 1 La sicurezza delle reti
 - I pericoli della rete
 - Il Firewall come strumento di difesa

Sommario

- 2 IPCop
 - Caratteristiche
 - Capire IPCop
 - Installazione e amministrazione

- 3 Addons
 - Estendere IPCop

Le informazioni

Oggi le informazioni sono sempre più importanti



Ormai è indispensabile proteggerle!

Rischi di Internet



- Quando si accede ad Internet si realizza sempre una **connessione bidirezionale**.
La connessione ci fornisce un *indirizzo IP* che può essere utilizzato da terzi per entrare nel nostro PC.
- Ciò significa che **il nostro computer può diventare a nostra insaputa Server** per altri utenti (cracker).

Rischi di Internet



- Ogni PC collegato in rete ha **65.536 porte** attraverso le quali può far **uscire** / **entrare** dati
- Ogni programma di un PC che abbia necessità di comunicare con la rete apre una porta di accesso al nostro calcolatore
- Le prime 1024 porte (*privilegiate*) sono assegnate in modo standard a servizi predefiniti (*25 SMTP, 80 HTTP, 110 POP3, ecc.*)

Tuttavia, tutte le porte possono essere aperte dinamicamente, a seconda delle necessità, dai programmi.

Principali pericoli della rete

Exploit
Shellcode
Cracking
Backdoor
Port scanning
Sniffing
Spoofing
Virus **DoS**
Worm **Trojan**



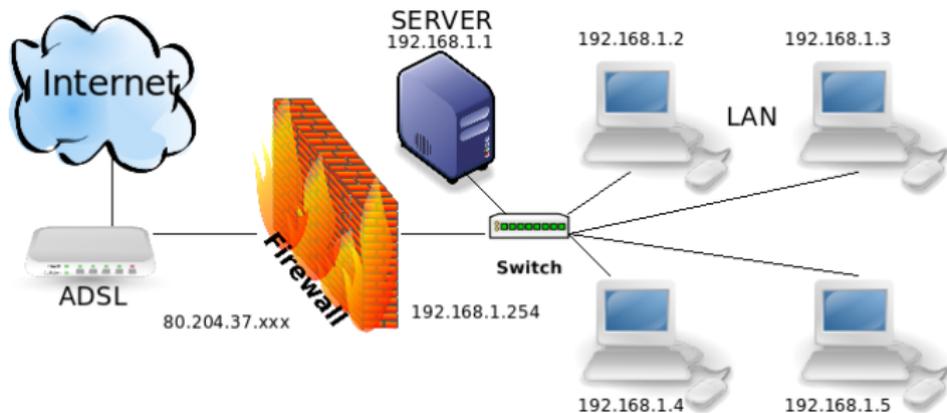
PC o LAN

La sicurezza di rete

Una **rete** possiamo ritenerla **sicura** quando:

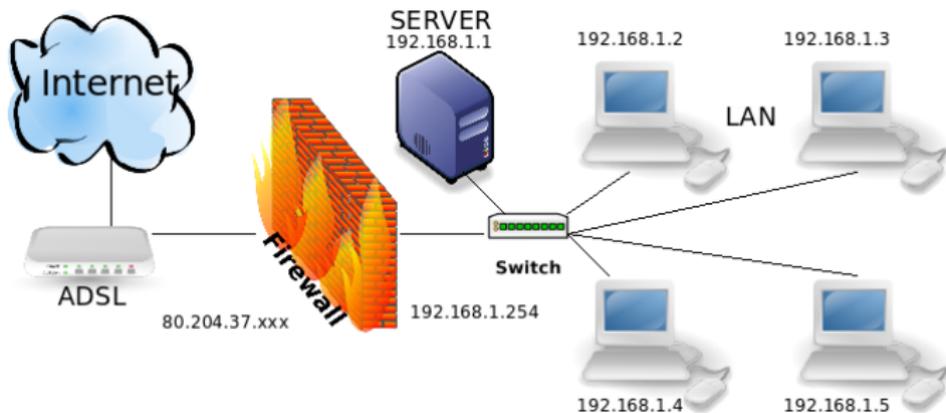
- Consente l'accesso a sistemi, servizi e risorse solo da e a persone autorizzate
- Protegge la sicurezza e la privacy delle transazioni da e verso Internet
- Evita di essere trampolini di lancio per attacchi alla rete

Firewall



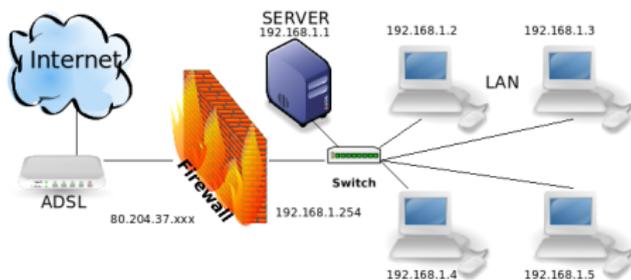
Il Firewall è uno degli strumenti più utili per contrastare i tentativi di intrusione su un PC o in una rete.

Firewall



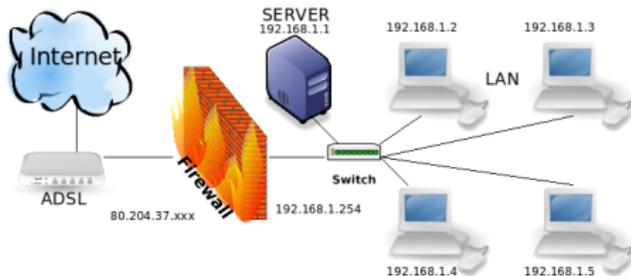
Il Firewall è un sistema particolare, che ha lo scopo di isolare i PC di una LAN da quelli di una WAN (es. Internet) creando una barriera *inattaccabile* e al contempo offrendo una connessione sicura ad Internet.

Firewall: che cosa è?



- Il Firewall è un sistema in grado di decidere quali informazioni far passare e quali fermare in una rete. Esso ispeziona il flusso di dati, intervenendo in base a regole che l'amministratore ha deciso.
- Può essere sia un **dispositivo fisico** esterno al PC, sia un **software** che collabora con il sistema operativo e i programmi installati.

Firewall: che cosa è?



- Tra i vantaggi di un Firewall è giusto annoverare anche la capacità di nascondere i singoli PC di una rete all'esterno.
- In altre parole un Firewall rende la vita difficile ai craker che desiderano raggiungere una determinata macchina, poiché le identità sono coperte e protette in maniera specifica.

Firewall: funzioni

Un Firewall svolge, normalmente, quattro funzioni:

- **INPUT**: determina cosa può ARRIVARE
- **OUTPUT**: determina cosa può USCIRE
- **FORWARDING**: prende un pacchetto in arrivo dall'interno e lo inoltra fuori, o viceversa
- **MASQUERADING**: utilizzando la tecnica **NAT** maschera l'indirizzo reale dei PC di una lan, con il suo

Firewall: come si configura

Un Firewall può essere configurato utilizzando due logiche opposte:

Tutto ciò che non è specificatamente permesso è **vietato**

- Il Firewall blocca tutto il traffico non previsto
- **VANTAGGI**: Maggiore sicurezza
- **SVANTAGGI**: Si limitano le scelte disponibili all'utente

Tutto ciò che non è specificatamente vietato è **permesso**

- Il Firewall lascia passare tutto il traffico e i servizi dannosi vanno bloccati individualmente
- **SVANTAGGI**: Difficoltà di amministrazione;
Rischio di lasciar transitare traffico indesiderato

Firewall: cosa NON può fare

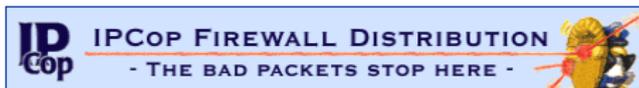
- Infine, è necessario ricordare ciò che un Firewall **NON può fare**. È giusto sapere anche questo, per evitare spiacevoli sorprese.
- Per esempio, **non protegge da attacchi iniziati** quando una rete è già stata compromessa.
- **Non protegge dai virus**
(ad eccezione dei Firewall *application gateway*)

Firewall: cosa NON può fare

- **Non protegge da intrusioni interne**, cioè da craker che hanno iniziato a danneggiare la rete dall'interno di un LAN.
- Soprattutto **non protegge dagli errori umani** (*causa principale degli incidenti legati alla sicurezza informatica*)

Parte II

IPCop-Firewall



IPCop: che cosa è

- IPCop è una mini-distribuzione **GNU/Linux** già configurata e pronta per realizzare un Firewall hardware/software.
- E' distribuita con licenza *GNU General Public Licence* ed è sviluppata, in perfetto stile Open Source, in collaborazione con la comunità degli utenti
- Non necessita di alcuna conoscenza pregressa di GNU/Linux in quanto si configura e si gestisce (aggiornamenti compresi) con una comoda interfaccia web anche da remoto
- Per utilizzarla è necessario solo un PC con almeno due schede di rete

IPCop: che cosa è

- IPCop può essere installato su hardware obsoleto. Gli sviluppatori hanno testato la versione 1.4 su un 486sx25Mhz con 12Mb di RAM e 273Mb di HD
- Una volta installato su un vecchio PC avrete recuperato hardware e avrete:
 - 1 Un ottimo Firewall **stateful inspection** (*tiene traccia delle relazioni tra i pacchetti che lo attraversano*) basato sul collaudatissimo **Netfilter/iptables** di GNU/Linux
 - 2 La possibilità di velocizzare la performance dei web browser attraverso l'attivazione del Proxy Server (*squid*)

IPCop: che cosa è

- L'interfaccia di installazione/gestione di IPCop è disponibile in 17 linguaggi (**compreso l'italiano**)
- È sviluppato dal 2001 e nelle ultime versioni è ormai un prodotto maturo che ha successo in una vasta comunità di utenti
- IPCop è un'ottima soluzione per piccole reti, aziendali SOHO, scuole, ecc.

IPCop: Mission del progetto

- Offrire una distribuzione Firewall GNU/Linux stabile, sicura e Open Source.
- Creare ed offrire una distribuzione Firewall GNU/Linux estremamente configurabile e di facile manutenzione.
- Offrire supporto affidabile agli utenti IPCop attraverso gradevoli forum pubblici di assistenza e discussione.
- Offrire un sistema stabile, sicuro e semplice per gli upgrades/patches di IPCop Linux.
- Sviluppare una relazione lunga e duratura con la comunità degli utenti
- Adattare IPCop all'evoluzione di Internet.
- Diffondere la conoscenza di GNU/Linux fra membri e utenti del progetto.

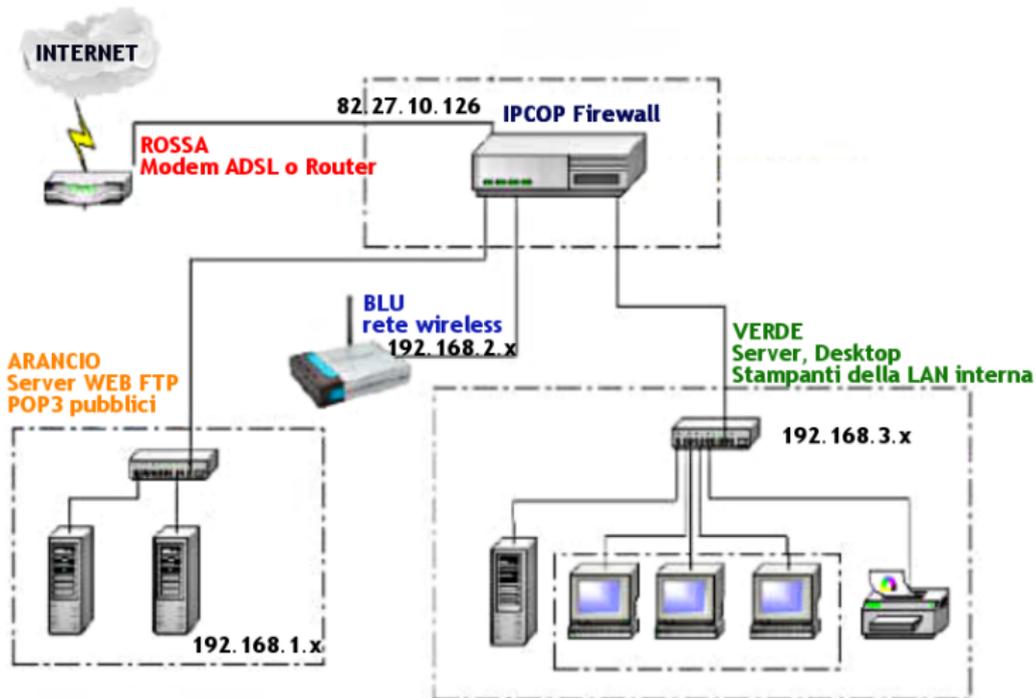
IPCop: Caratteristiche e funzionalità

- **GNU/Linux** con kernel 2.4.x
- **Linux Netfilter** con capacità di NAT/PAT e logging.
- Supporto per quattro schede di rete (*WAN, LAN, Wireless, DMZ*)
- Supporto **Client DHCP** su una scheda di rete per ricevere l'indirizzo IP dal Provider.
- Supporto **Server DHCP** per due schede di rete.
- Supporto **Server NTP** per sincronizzare la data e l'ora e per fornirla a due schede di rete.

IPCop: Caratteristiche e funzionalità

- **IDS** (*Intrusion detection system*) per tutte e quattro le schede di rete.
- Supporto per la **VPN** (rete privata virtuale).
- Supporto modem (analogici, ISDN, ADSL)
- **Proxy Server** per il Web.
- Amministrazione e controllo attraverso il browser con possibilità di patch/update
- Grafici sullo stato del sistema e sul traffico di rete
- Backup e Restore della configurazione
- Supporto server SSH per connessioni remote

IPCop: schema funzionale delle connessioni



IPCop: schede di rete

Riepilogando le schede di rete sono individuate da 4 colori differenti:

- **ROSSO** - rappresenta l'interfaccia connessa ad Internet.
- **VERDE** - rappresenta l'interfaccia per la rete interna.
- **BLU** - rappresenta l'interfaccia per una seconda rete interna o per una rete wireless.
- **ARANCIO** - rappresenta l'interfaccia per un'eventuale zona DMZ in cui si trovano server che offrono servizi all'esterno.

L'applicazione minima prevede due interfacce di rete, quella verso internet (**ROSSA**) e quella verso la rete locale (**VERDE**) da proteggere.

Nel caso in cui esistono due reti locali che devono rimanere separate (accesso consentito solo in VPN) si utilizza anche l'interfaccia **BLU**.

IPCop: Policy di default

IPCop utilizza, di default, per il traffico che lo attraversa le seguenti policy:

WAN	Rossa -> Firewall Bloccato , Utilizzare External Access
	Rossa -> Arancio Bloccato , Utilizzare Port Forwarding
	Rossa -> Blu Bloccato , Utilizzare Port Forwarding o VPN
	Rossa -> Verde Bloccato , Utilizzare Port Forwarding o VPN
DMZ	Arancio -> Firewall Bloccato (Non utilizzare IPCop come DNS o DHCP server per arancio)
	Arancio -> Rossa Permesso
	Arancio -> Blu Bloccato , Utilizzare DMZ Pinholes
	Arancio -> Verde Bloccato , Utilizzare DMZ Pinholes
Wireless 2^LAN	Blu -> Firewall Bloccato , Utilizzare Blue Access
	Blu -> Arancio Bloccato , Utilizzare Blue Access
	Blu -> Rossa Bloccato , Utilizzare Blue Access
	Blu -> Verde Bloccato , Utilizzare DMZ Pinholes o VPN
LAN	Verde -> Firewall Permesso
	Verde -> Rossa Permesso
	Verde -> Arancio Permesso
	Verde -> Blu Permesso

IPCop: come reperirlo

- L'immagine ISO si può scaricare liberamente dal sito <http://www.ipcop.org>
(ultima versione 1.4.11 - circa 43Mb)
- Se preferite una installazione con boot da dispositivi USB il sito IPCop vi mette a disposizione altre 3 immagini liberamente scaricabili:
 - 1 **fdd** - per dispositivi USB non partizionati
 - 2 **hdd** - per dispositivi USB partizionati come hard disk
 - 3 **zip** - per dispositivi ZIP o partizionati come ZIP

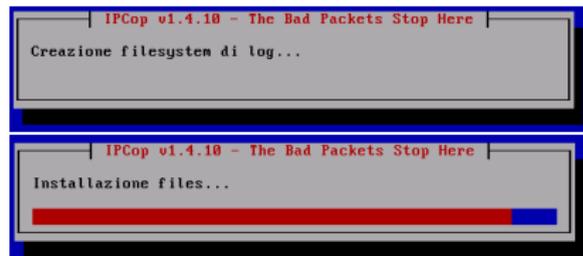
IPCop: fasi per l'installazione (1)

- Scarichiamo l'immagine ISO dal sito ufficiale www.ipcop.org (*verificandone l'impronta MD5*)
- Masterizziamo il file immagine ed effettuiamo il boot da CD-ROM (o USB drive)
- Selezioniamo la lingua preferita e la fonte di installazione



IPCop: fasi per l'installazione (2)

- Eseguiamo il partizionamento automatico del disco
(Attenzione:TUTTI I DATI SARANNO CANCELLATI!!)
- Segue la fase di installazione di IPCop



IPCop: fasi per l'installazione (3)

- Se si tratta di un ripristino, in fase di installazione, possiamo inserire il floppy con il backup della configurazione



IPCop: fasi per l'installazione (4)

- Selezioniamo i driver per l'interfaccia di rete GREEN (automatico o manuale).



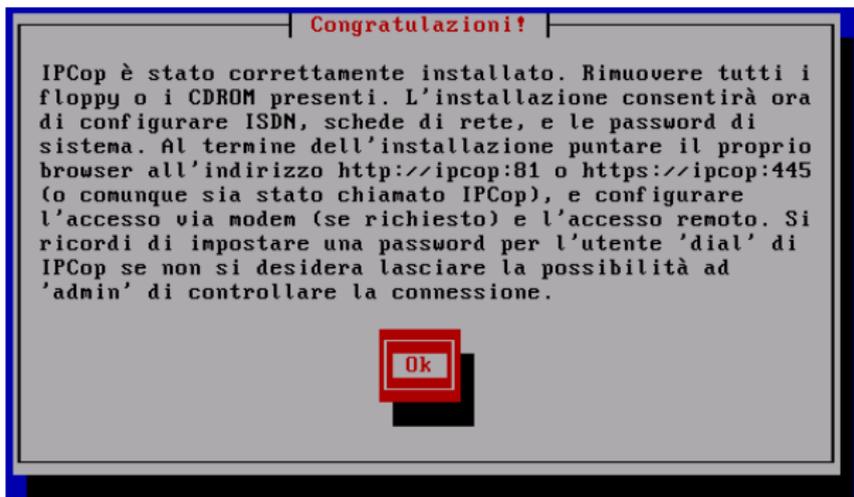
IPCop: fasi per l'installazione (5)

- Impostiamo l'indirizzo IP dell'interfaccia GREEN (Es. 192.168.1.254).



IPCop: fasi per l'installazione (6)

- Abbiamo finito la prima parte dell'installazione, rimuoviamo il CD e continuiamo



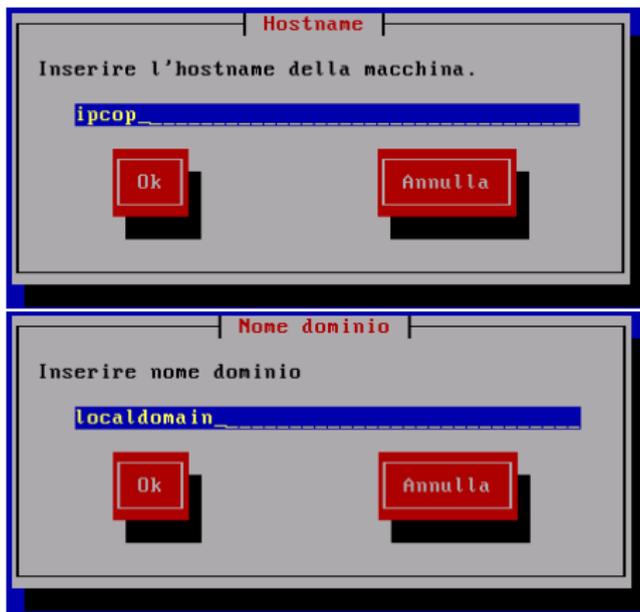
IPCop: fasi per l'installazione (7)

- Impostiamo i parametri di localizzazione
 (*tastiera, timezone*)



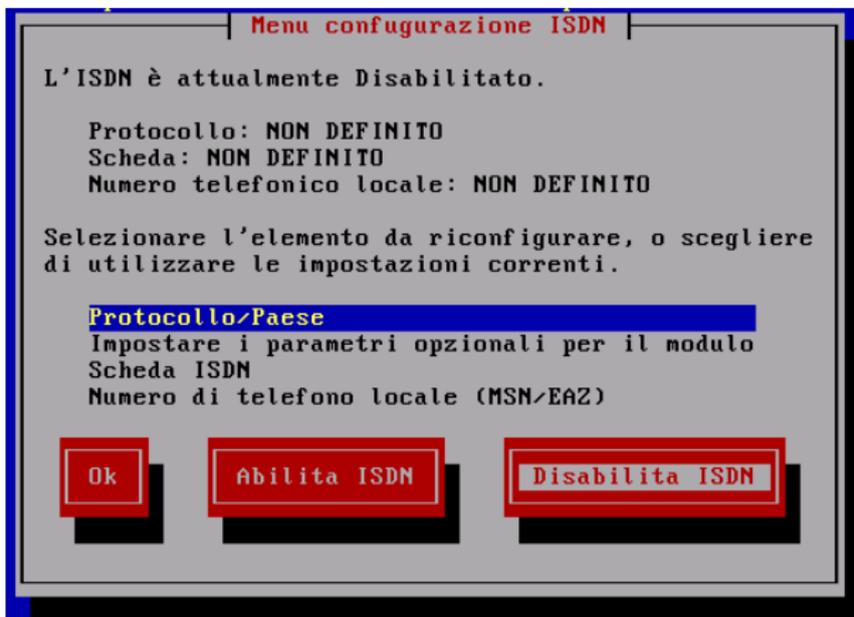
IPCop: fasi per l'installazione (8)

- Impostiamo il nome del sistema (*hostname*) e del dominio.



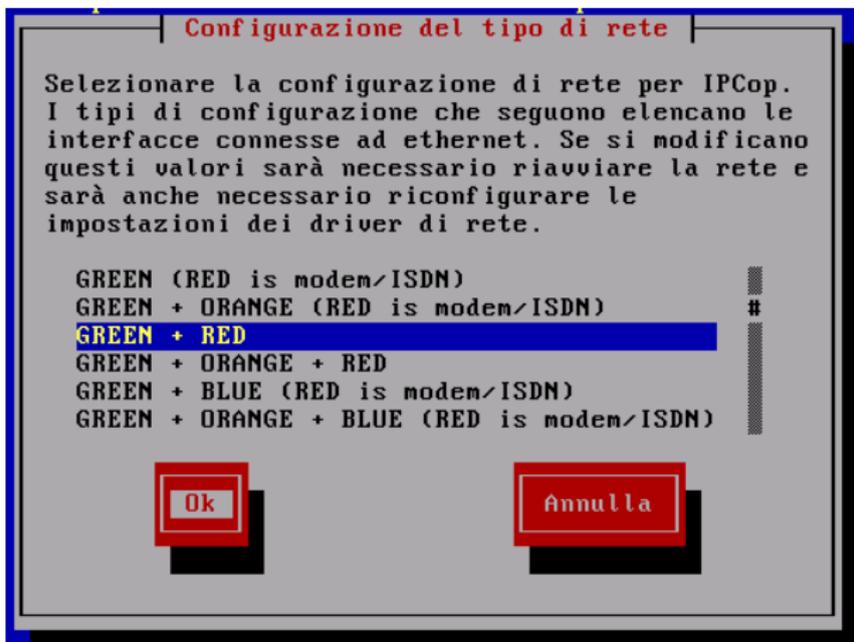
IPCop: fasi per l'installazione (9)

- Configuriamo il dispositivo ISDN
(*disabilitare se non interessa*)



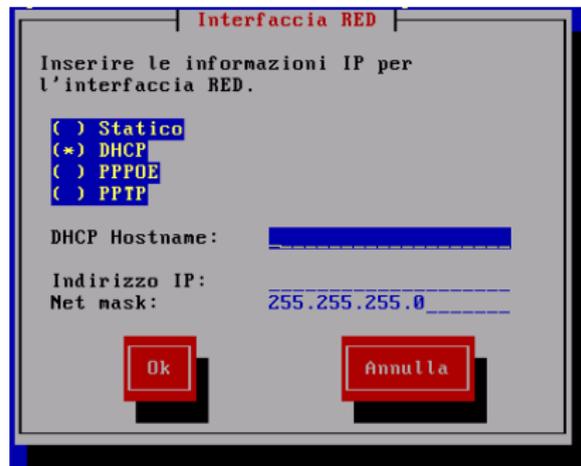
IPCop: fasi per l'installazione (10)

- Impostiamo il tipo di rete in base al numero delle interfacce presenti (Es. RED + GREEN)



IPCop: fasi per l'installazione (11)

- Configuriamo TUTTE le rimanenti interfacce di rete (la GREEN è stata già configurata).



IPCop: fasi per l'installazione (12)

- Inseriamo i DNS ed il Default Gateway.



IPCop: fasi per l'installazione (13)

- Configuriamo il server DHCP (saltare se non interessa).

Configurazione server DHCP

Configurare il server DHCP inserendo le seguenti informazioni.

Abilitato

Indirizzo iniziale: _____

Indirizzo finale: _____

DNS primario: 192.168.1.2 _____

DNS secondario : _____

Lease di default (min): 60 _____

Lease massimo (min): 120 _____

Suffisso nome dominio: localdomain _____

Ok

Annulla

IPCop: fasi per l'installazione (14)

- Impostiamo le password di **root** e dell'utente **admin**. Quest'ultimo è utilizzato per l'amministrazione via WEB di IPCop

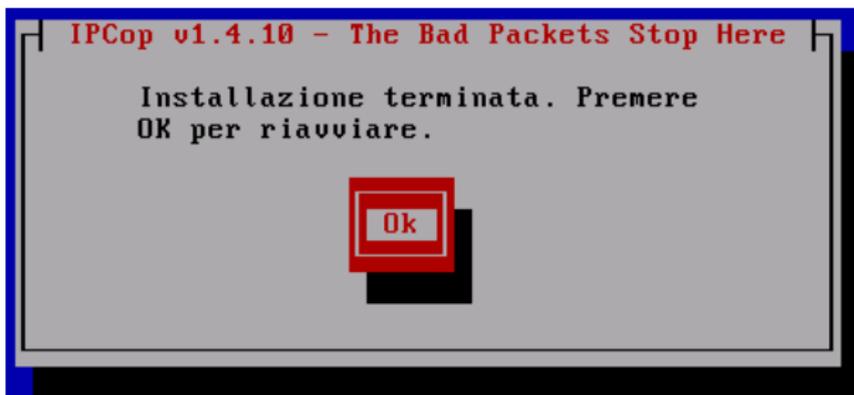
The image shows two screenshots of the IPCop v1.4.10 installation process. Both screenshots have a title bar that reads "IPCop v1.4.10 - The Bad Packets Stop Here".

The top screenshot is for setting the root password. It contains the text: "Inserire la password per l'utente 'root'. Accedere come 'root' per la riga di comando." Below this text are two input fields: "Password:" and "Conferma password:". At the bottom are two red buttons labeled "Ok" and "Annulla".

The bottom screenshot is for setting the admin password. It contains the text: "Inserire la password di 'admin' per IPCop. Questo utente sarà autorizzato ad accedere alle pagine web di amministrazione di IPCop." Below this text are two input fields: "Password:" and "Conferma password:". At the bottom are two red buttons labeled "Ok" and "Annulla".

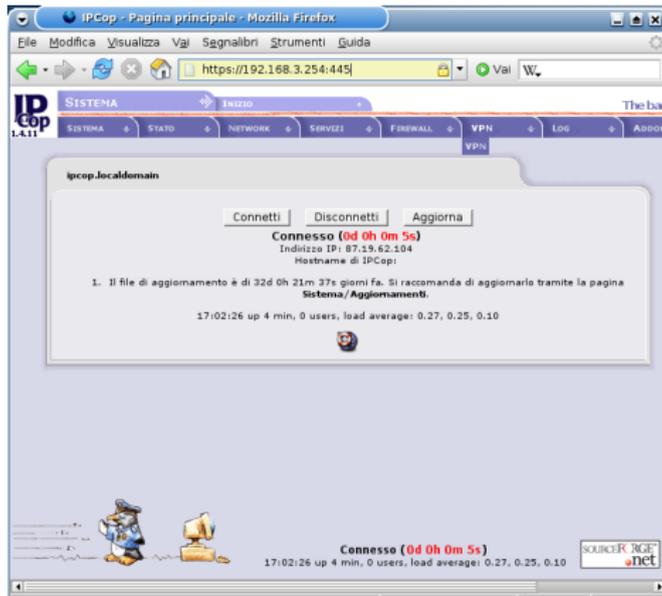
IPCop: fasi per l'installazione (15)

- L'installazione è terminata



IPCop: Amministrazione

Per gestire un Firewall IPCop è sufficiente utilizzare un browser
(da un client della LAN) scrivendo come URL
https://indirizzo-IPCop:445 (Es. *https://192.168.3.254:445*)



IPCop: Menu



Tramite comodi Menù (*dopo l'autenticazione*) possiamo gestire IPCop:

- 1 **Sistema** - Aggiornamenti, Password, SSH, Backup
- 2 **Stato** - Monitor e grafici sullo stato del sistema
- 3 **Network** - Configurazione modem
- 4 **Servizi** - Configurazione Proxy, DHCP, DNS dyn, Time server, IDS
- 5 **Firewall** - Personalizzazione Policy Firewall
- 6 **VPN** - Configurazione VPN
- 7 **Log** - Log di sistema, Firewall, IDS e Proxy

IPCop: Aggiornamenti

- La disponibilità di nuovi aggiornamenti sarà automaticamente verificata all'avvio del PC con IPCop, oppure può essere effettuata manualmente.
- Gli aggiornamenti potranno essere installati tramite interfaccia Web



Aggiornamenti disponibili:

Tutti gli aggiornamenti disponibili sono stati installati

Per installare un aggiornamento eseguire l'upload del file .tgz.gpg mediante il form sottostante:

Upload di un file di aggiornamento:

Utilizzo disco:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/root	799M	246M	545M	32%	/
/dev/harddisk2	2.2G	126M	2.0G	6%	/var/log



Aggiornamenti installati:

IPCop: Backup di sistema

Il Backup della configurazione di sistema può essere fatto:

- sull'Hard Disk di IPCop (scaricabile su altri PC)
- su Floppy (*drive di IPCop*)

The screenshot shows a web-based configuration window titled "Salvataggio". At the top, there is a "Backup su floppy" button and a text instruction: "Inserire un floppy formattato nel drive e cliccare il pulsante Backup su floppy per salvare la configurazione del sistema. Controllare il risultato dell'operazione attentamente." Below this, there are two main sections. The first is "Select media (only FAT supported for removable media)", where "Hard disk" is selected with a radio button. Underneath, it says "Plug in a device, refresh, select and mount before usage. Unmount before removal." and provides "Aggiorna", "Mount", and "Unmount" buttons. The second section is "Backup Encryption Key", which includes a "Backup password:" input field and an "Export backup key" button. At the bottom, it shows "Current media: Hard disk Liberti: 545 M" and a "Create a new backup set" section with a "Descrizione:" input field and a "Create a new backup set" button.

Per motivi di sicurezza, IPCop **crittografa i backup** con una chiave casuale generata al primo backup. Il restore di archivi sarà permesso solo sulla macchina IPCop che li ha creati

IPCop: Restore di sistema

Ripristinare un Firewall IPCop è un gioco da ragazzi se si dispone di una copia di backup della configurazione. Il Restore è disponibile:

- **durante l'installazione** se si dispone del Floppy di Backup
- **dopo l'installazione** utilizzando uno dei backup disponibili sull'Hard Disk di IPCop o un backup esterno da trasferire con upload su IPCop

Current media: **Hard disk** Liberi: 545 M

Create a new backup set

Descrizione:

Import a backup (.dat) file:

Insiemi di backup:

	Descrizione	Azione
2005-12-09 11:26:31		
2005-05-11 18:31:52		
2005-05-14 11:16:26		
2005-05-14 11:16:37		
2005-06-14 12:27:54		

IPCop: Monitor Sistema

IPCop mette a disposizione tanti report per monitorare lo stato del sistema e della rete. Ad esempio:

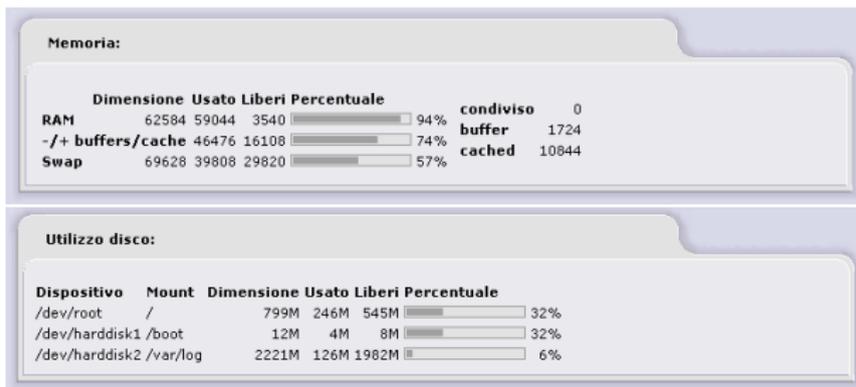
Servizi:

CRON server	AVVIATO
DNS proxy server	AVVIATO
Kernel logging server	AVVIATO
Log server	AVVIATO
Secure shell server	AVVIATO
Server DHCP	ARRESTATO
Server NTP	ARRESTATO
Sistema di rilevamento intrusioni (GREEN)	ARRESTATO
Sistema di rilevamento intrusioni (RED)	AVVIATO
VPN	ARRESTATO
Web proxy	ARRESTATO
Web server	AVVIATO

Stato dei servizi

IPCop: Monitor Sistema

IPCop mette a disposizione tanti report per monitorare lo stato del sistema e della rete. Ad esempio:



Stato della RAM e del disco

IPCop: Monitor Sistema

IPCop mette a disposizione tanti report per monitorare lo stato del sistema e della rete. Ad esempio:

```
Interfacce:

eth0      Link encap:Ethernet  HWaddr 00:30:84:3B:9F:9F
          inet addr:172.31.125.174  Bcast:172.31.125.175  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2801755 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2838931 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1788242543 (1705.4 MB)  TX bytes:2348498338 (2239.7 MB)
          Interrupt:11 Base address:0x7000

eth1      Link encap:Ethernet  HWaddr 00:00:B4:93:F1:8A
          inet addr:172.16.200.250  Bcast:172.16.200.255  Mask:255.255.255.0
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:2832832 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2769537 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2355609033 (2246.4 MB)  TX bytes:1783582570 (1700.9 MB)
          Interrupt:12 Base address:0x9000
```

Stato delle interfacce di rete

IPCop: Grafici Sistema

Attraverso i grafici avremo un'idea dello stato del sistema nel tempo. Ad esempio:

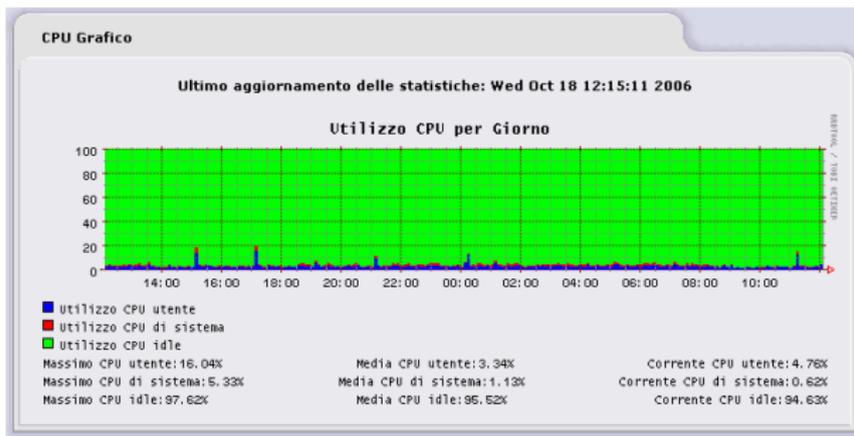


Grafico utilizzo CPU

IPCop: Grafici Sistema

Attraverso i grafici avremo un'idea dello stato del sistema nel tempo. Ad esempio:

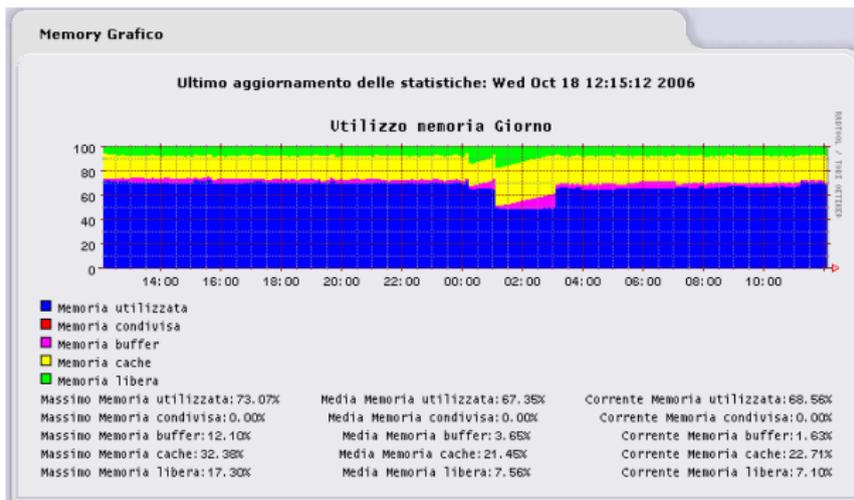


Grafico utilizzo RAM

IPCop: Grafici Sistema

Attraverso i grafici avremo un'idea dello stato del sistema nel tempo. Ad esempio:

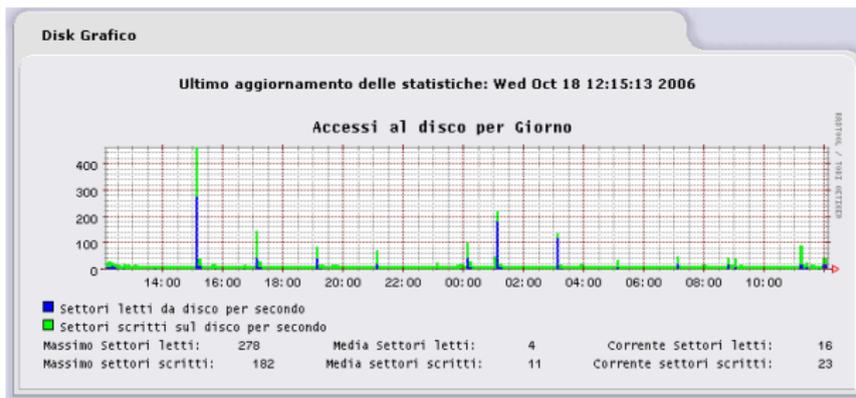


Grafico utilizzo Hard Disk

IPCop: Grafici Sistema

Attraverso i grafici avremo un'idea dello stato del sistema nel tempo. Ad esempio:

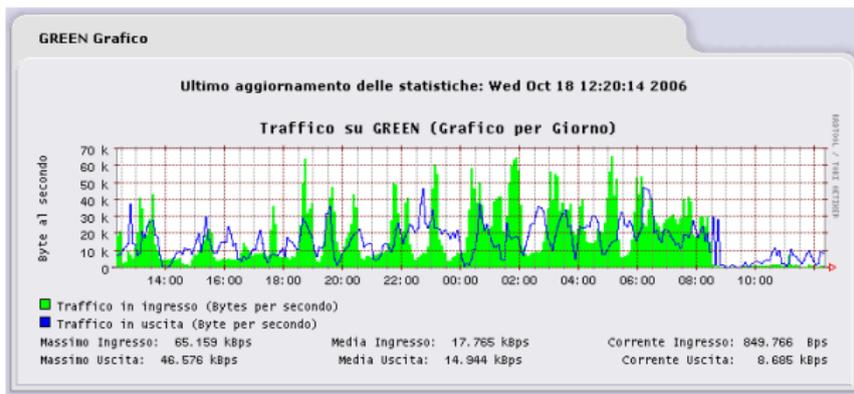


Grafico Traffico rete

IPCop: Grafici Sistema

Potremo poi avere statistiche sul traffico di rete

Traffico di rete nel periodo prescelto:

Data	Rete interna		Internet	
	In ingresso	In uscita	In ingresso	In uscita
2006-10-02	879.105	527.346	527.464	879.057
2006-10-03	1655.399	547.373	547.261	1655.367
2006-10-04	4.947	54.780	54.862	4.937
2006-10-05	11.430	478.206	478.246	11.430
2006-10-06	1773.896	1037.963	1037.961	1773.847
2006-10-07	1299.231	869.682	870.676	1299.141
2006-10-10	1299.958	1059.947	1059.959	1299.837
2006-10-11	1145.143	672.847	672.727	1145.121
2006-10-12	5.850	71.121	71.084	5.787
2006-10-13	16.722	138.161	138.085	16.701
2006-10-14	14.478	63.735	63.672	14.485
2006-10-16	133.761	787.251	794.973	133.815
2006-10-17	647.780	763.154	763.222	647.721
2006-10-18	876.224	647.161	646.262	876.080
Totale	9763.92 MB	7718.73 MB	7726.46 MB	9763.33 MB

IPCop: Grafici Sistema

Oppure verificare in tempo reale lo stato di tutte le connessioni sul Firewall

IPTables Connection Tracking

Legenda : LAN INTERNET DMZ Wireless IPCop VPN

Protocollo	Scade (Secondi)	Connessione Stato	Originale IP sorgente:Porta	Originale IP Dest.:Porta	Atteso IP sorgente:Porta	Atteso IP Dest.:Porta	Marcato	Usa
Tutti		Tutti	****	****	Ordinamento crescente: orgsip		Tutti	1
tcp (6)	431940	ESTABLISHED	172.31.125.163 :1457	213.175.4.43 :443	213.175.4.43 :443	172.16.200.250 :1457	[ASSURED]	1
tcp (6)	431942	ESTABLISHED	172.31.125.163 :1443	213.175.4.43 :443	213.175.4.43 :443	172.16.200.250 :1443	[ASSURED]	1
tcp (6)	260443	ESTABLISHED	172.31.125.168 :1042	86.83.146.66 :40390	86.83.146.66 :40390	172.16.200.250 :1042	[ASSURED]	1

IPCop: Servizi

Dal Menu SERVIZI accediamo alla loro amministrazione. Ad esempio:

Web proxy:

Abilita su Green :	<input type="checkbox"/>	Upstream proxy (host:port):	<input type="text"/>
Trasparente su Green :	<input type="checkbox"/>	Upstream username:	<input type="text"/>
Log abilitato:	<input type="checkbox"/>	Upstream password:	<input type="text"/>
		Porta del proxy:	<input type="text" value="800"/>
		Your extension_methods list:	<input type="text"/>

Gestione della cache

Dimensione cache (MB):	<input type="text" value="50"/>	<input type="button" value="Repair cache"/>
Min dim. oggetto (KB):	<input type="text" value="0"/>	<input type="button" value="Svuota cache"/>
Max dim. oggetto (KB):	<input type="text" value="4096"/>	

Limiti trasferimento

Max dim. ingresso (KB):	<input type="text" value="0"/>	Max dim. uscita (KB):	<input type="text" value="0"/>
-------------------------	--------------------------------	-----------------------	--------------------------------

This field may be blank.



Proxy Server - SQUID

IPCop: Servizi

Dal Menu SERVIZI accediamo alla loro amministrazione. Ad esempio:

DHCP

Interfaccia Verde Abilitato: Indirizzo IP/Netmask: **172.31.125.174/255.255.255.240**

Indirizzo di partenza:	<input type="text"/>	Indirizzo finale:	<input type="text"/>
Lease time di default (minuti):	<input type="text" value="60"/>	Lease time massimo (minuti):	<input type="text" value="120"/>
Suffisso nome di dominio:	<input type="text" value="mydomain"/>	Permetti client bootp:	<input type="checkbox"/>
DNS primario:	<input type="text" value="172.31.125.174"/>	DNS secondario:	<input type="text"/>
NTP Server Primario:	<input type="text"/>	NTP Server Secondario:	<input type="text"/>
WINS Server Primario:	<input type="text"/>	WINS Server Secondario:	<input type="text"/>

This field may be blank.



Server DHCP

IPCop: Servizi

Dal Menu SERVIZI accediamo alla loro amministrazione. Ad esempio:

Sistema di rilevamento intrusioni:

GREEN Snort
 RED Snort

Aggiornamento regole Snort

No
 Regole VRT di Sourcefire per utenti registrati
 Regole VRT di Sourcefire in abbonamento

Per utilizzare le Regole VRT di Sourcefire è necessario registrarsi su <http://www.snort.org>.

Accettare la licenza, attendere la password via email e connettersi al sito [USER PREFERENCES](#), premere il pulsante 'Get Code' in fondo e copiare l'Oink Code (40 caratteri)

Oink Code:

Regole già aggiornate

Intrusion Detection System - SNORT

IPCop: Firewall Policy

Con il Menu FIREWALL possiamo personalizzare le policy del Firewall. Ad esempio:

Aggiungi nuova regola:

Protocollo: Alias IP: Porta sorgente:

IP destinazione: Porta destinazione:

Note: Abilitato:

Indirizzo sorgente (IP o di rete, vuoto per "TUTTI"):

This field may be blank.



Port Forwarding

Per garantire dall'esterno l'accesso ad eventuali servizi interni.
(Es. Server WEB)

IPCop: Firewall Policy

Con il Menu FIREWALL possiamo personalizzare le policy del Firewall. Ad esempio:

Aggiungi nuova regola:

TCP Rete sorgente: ORANGE IP o NET sorgente: []
Rete Destinazione: VERDE IP o NET di destinazione: [] Porta destinazione: []
Note: [] Abilitato:

This field may be blank. 

DMZ Pinholes

Per permettere il traffico dalla **ARANCIO** e/o dalla **BLU** verso la **VERDE**

IPCop: VPN

Con IPCop è facilissimo realizzare VPN con altri Firewall IPCop o altri prodotti dotati di *IPSec* e *3DES*

Impostazioni globali

Hostname/IP VPN locale: Abilitato: VPN on GREEN: Abilitato:

Override default MTU:

Ritarda il lancio della VPN (secondi):

Restart net-to-net vpn when remote peer IP changes (dyndns), it helps DPD:

PLUTO DEBUG = crypt: , parsing: , emitting: , control: , klips: , dns: , nat_t:

- This field may be blank.
- Se necessario, questo ritardo puo' essere usato per permettere agli aggiornamenti del DNS dinamico di propagarsi correttamente. 60 è il valore comunemente utilizzato quando l'interfaccia RED utilizza un ip dinamico.

Controllo stato connessione:

Nome	Tipo	Nome Comune	Note	Stato	Azione
<input type="button" value="Aggiungi"/>					

Autorità di Certificazione:

Nome	Oggetto	Azione
Certificato Root:	Non presente	

IPCop: VPN

Infine tramite Menu LOG potremo controllare giorno per giorno cosa è successo. Ad esempio:

Impostazioni:

Mese: Giorno:

Log:

Numero totale di regole di intrusione attivate per Ottobre 18: 37

[Indietro](#) [Avanti](#)

Data:	10/18 06:16:08	Nome:	ICMP Destination Unreachable Communication Administratively Prohibited
Priorità:	3	Tipo:	Misc activity
IP info:	89.13.100.238:n/a -> 172.31.125.168:n/a		
Riferimenti:	vuoto	SID:	485
Data:	10/18 06:25:08	Nome:	ICMP Destination Unreachable Communication Administratively Prohibited
Priorità:	3	Tipo:	Misc activity
IP info:	89.13.100.238:n/a -> 172.31.125.168:n/a		

LOG Intrusioni

IPCop: VPN

Infine tramite Menu LOG potremo controllare giorno per giorno cosa è successo. Ad esempio:

Impostazioni:

Mese: Giorno:

Log:

Numero totale di connessioni bloccate per Ottobre 18, 2006: 207

Ora	Chain	Indietro			Src Port	Avanti		
		Iface	Prot.	Sorgente		Indirizzo MAC	Destinazione	Dst Port
00:01:16	NEW not SYN?	eth0	TCP	172.31.125.168	4669	:::::	84.76.156.1	4662
00:08:49	INPUT	eth1	UDP	83.93.160.229	5672	00:13:c3:f0:5d:2f	172.16.200.250	9485
00:09:04	INPUT	eth1	UDP	83.196.219.244	4672	00:13:c3:f0:5d:2f	172.16.200.250	9485

LOG Firewall

IPCop: Addons

È possibile estendere le funzionalità di IPCop tramite l'installazione di moduli/programmi aggiuntivi chiamati “**addons**”

ATTENZIONE!!!

Gli **addons** non sono ufficialmente riconosciuti
Alcuni di essi possono ridurre la sicurezza del Firewall

Sul sito di IPCop nella sezione “Addons” troviamo la lista dei siti web che li mettono a disposizione.

IPCop: Installazione degli Addons

Gli **addons** possono essere installati su IPCop in due modi:

- 1 tramite shell (*locale o remoto via SSH*)
- 2 tramite interfaccia WEB dopo aver installato **Addon Server**

Quest'ultimo è un modulo che facilita l'installazione e l'aggiornamento di numerosi addons reperibili sullo stesso sito di Addon Server

<http://firewalladdons.sourceforge.net>

IPCop: Addon Cop+

Tra i tanti addons disponibili segnalo Cop+ (*Copplus*) adatto a chi ha esigenze di **web content filtering**.

<http://home.earthlink.net/~copplus/>

Esso aggiunge a IPCop:

- Dansguardian content filter
- GUI per la gestione di Dansguardian
- Autenticazione utente a Squid (*Opzionale*)
- Aggiornamenti automatici delle Blacklist per Dansguardian

IPCop: Addon Copfilter

Un altro addon da segnalare è Copfilter.

<http://www.copfilter.org>

L'obiettivo del modulo è offrire un sistema facile, autoaggiornante, libero e gratuito per **filtrare** il traffico di rete (*FTP, HTTP, POP3, SMTP*) ed eliminare **virus** e **spam**.

Copfilter

Version: 0.83beta3a Documentation: [README](#) [CHANGELOG](#) [CREDITS](#) [BUGS](#)

WARNING: This package is NOT an official ipcop addon. It has not been approved or reviewed by the ipcop development team. It comes with NO warranty or guarantee, so use it at your own risk. This package adds firewall rules, proxies, filters and virus scanners to your ipcop machine. Do NOT use Copfilter if firewall security is an issue. With HAVP you could still [receive a virus](#).

Virus Quarantine (0x) Spam Quarantine (0x) [Monit Service Manager](#) [Copfilter Whitelist Manager](#) [Copfilter Spam Digest Manager](#)

Product	Description	Daemon	Version	Status	Manual Control*
monit	Monitoring Utility	monit	4.8.1	ON (PID 859 858 857)	<input type="button" value="Stop monit"/>
P3Scan	Transp. POP3 Proxy	p3scan	2.2.1	ON (PID 545)	<input type="button" value="Stop p3scan"/>
ProxSMTP	Transp. SMTP Proxy	proxsmtpd	1.4	OFF	<input type="button" value="Start proxsmtpd"/>
HAVP	Transp. HTTP Proxy	havp	0.82	OFF	<input type="button" value="Start havp"/>

IPCop: Addon Copfilter

CopFilter include famosi programmi Open Source già configurati come *SpamAssassin*, *Clamav Antivirus*, *P3scan*, *ProxSMTP*, *Privoxy*, *HAVP*, *frox*, *renattach*, *RoulesDuJour*, *Razor*, *monit*.

Copfilter

Version: 0.83beta3a Documentation: [README](#) [CHANGELOG](#) [CREDITS](#) [BUGS](#)

WARNING: This package is NOT an official ipcop addon. It has not been approved or reviewed by the ipcop development team. It comes with NO warranty or guarantee, so use it at your own risk. This package adds firewall rules, proxies, filters and virus scanners to your ipcop machine. Do NOT use Copfilter if firewall security is an issue. With HAVP you could still [receive a virus](#).

[Virus Quarantine \(0x\)](#) [Spam Quarantine \(0x\)](#) [Monit Service Manager](#) [Copfilter Whitelist Manager](#) [Copfilter Spam Digest Manager](#)

Product	Description	Daemon	Version	Status	Manual Control*
monit	Monitoring Utility	monit	4.8.1	ON (PID 859 858 857)	Stop monit
P3Scan	Transp. POP3 Proxy	p3scan	2.2.1	ON (PID 545)	Stop p3scan
ProxSMTP	Transp. SMTP Proxy	proxsmtpd	1.4	OFF	Start proxsmtpd
HAVP	Transp. HTTP Proxy	havp	0.82	OFF	Start havp

Bibliografia



IPCop

Documentazione ufficiale di IPCop.

<http://www.ipcop.org>



Wikipedia

L'enciclopedia libera.

<http://it.wikipedia.org/>

Links

-  Guida in italiano all'installazione di IPCop
<http://www.freedays.it/>
-  Sito di Addons-server e numerosi addons per IPCop
<http://Firewalladdons.sourceforge.net>
-  Sito di Cop+
<http://home.earthlink.net/~copplus>
-  Sito di CopFilter
<http://www.copfilter.org>

Questa presentazione è realizzata utilizzando esclusivamente Software Libero:



- **debian GNU/Linux** - <http://www.debian.org>
- **L^AT_EX** - <http://www.latex-project.org/>
- **Beamer** - <http://latex-beamer.sourceforge.net/>