

Lug-ACROS presenta:

IpCop

...un firewall semplice.

Introduzione: che cosa è IpCop

- IpCop è una **distribuzione Linux** dedicata all'implementazione di un **firewall** per la messa in sicurezza di un'intera rete di pc e dei servizi da essa offerti. Per facilitare la gestione, la rete viene divisa in diversi “segmenti” a cui vengono assegnati diversi diritti di accesso, ogni “segmento” deve disporre di una scheda di rete dedicata.
- IpCop semplifica l'utilizzo del firewall: una volta installato è pronto per funzionare, la gestione “ordinaria” e la personalizzazione delle opzioni avvengono tramite un'interfaccia web accessibile da ogni pc della rete.
- IpCop **deve** essere installato su un pc dedicato.
- IpCop ha una struttura **estendibile**.

Come ottenere IpCop:

IpCop viene distribuito con licenza GPL. Può quindi essere liberamente scaricato dal sito <http://www.ipcop.org> ed installato un numero illimitato di volte su un numero a piacere di pc. Dal sito è possibile scaricare i files contenenti l'immagine del cd di installazione o i files di aggiornamento da una versione precedente della distribuzione, oltre a molti programmi che aggiungono funzionalità alla distribuzione di base. Questi programmi vengono denominati “addons”.

IpCop: boot, installazione e prima configurazione.

L'installazione di IpCop inizia facendo il boot dal cd ottenuto masterizzando il file dell'immagine iso scaricato dal sito. La prima schermata contiene un'avviso molto importante: proseguendo con l'installazione infatti

il disco rigido del pc verrà completamente cancellato!

Questa è una misura necessaria per garantire la sicurezza dell'installazione anche se di fatto **impedisce** di provare l'installazione sul pc che utilizziamo normalmente. E' comunque possibile, anzi consigliabile, effettuare un'installazione di test all'interno di una macchina virtuale, come vedremo successivamente, creata tramite software tipo VmWare o Qemu.

Premiamo invio per avviare l'installazione, quando appare la finestra relativa specifichiamo la lingua da utilizzare; dopo una fase di ricerca dei dispositivi il programma ci avvisa che procederà alla preparazione dell'hard disk del pc e successivamente verrà installato il sistema.

Nomenclatura delle connessioni:

IpCop divide ed isola il traffico di rete su schede distinte, a seconda della tipologia di rete che abbiamo scelto in fase di installazione. Tale scelta è comunque modificabile in qualsiasi momento semplicemente lanciando nuovamente il programma di configurazione.

La classificazione standard delle varie reti è la seguente:

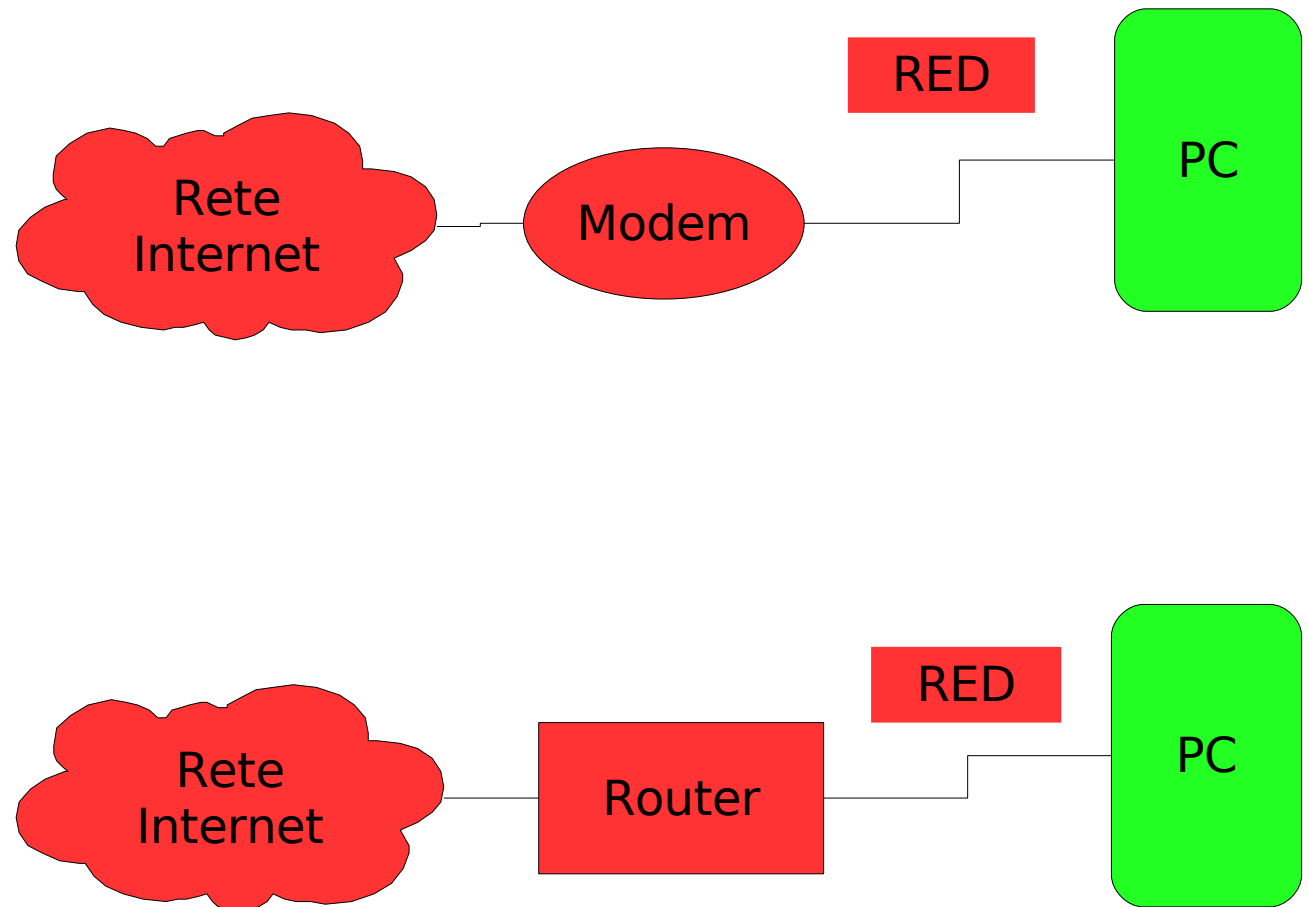
- Rete **RED** – la rete di connessione ad internet
- Rete **GREEN** – la rete interna di connessione tra i pc
- Rete **BLUE** – la rete di connessione senza fili (wifi)
- Rete **ORANGE** – la rete di connessione per i server raggiungibili da internet.

La rete **GREEN** ha libero accesso alle reti **RED**, **BLUE** ed **ORANGE**, le reti **BLUE** ed **ORANGE** possono accedere alla rete **RED** ma non possono accedere alla rete **GREEN**, la rete **RED** non ha di default nessun accesso alle reti **GREEN**, **BLUE** ed **ORANGE**.

Schemi di reti e connessioni ad internet

Pc singolo connesso tramite modem o tramite router.

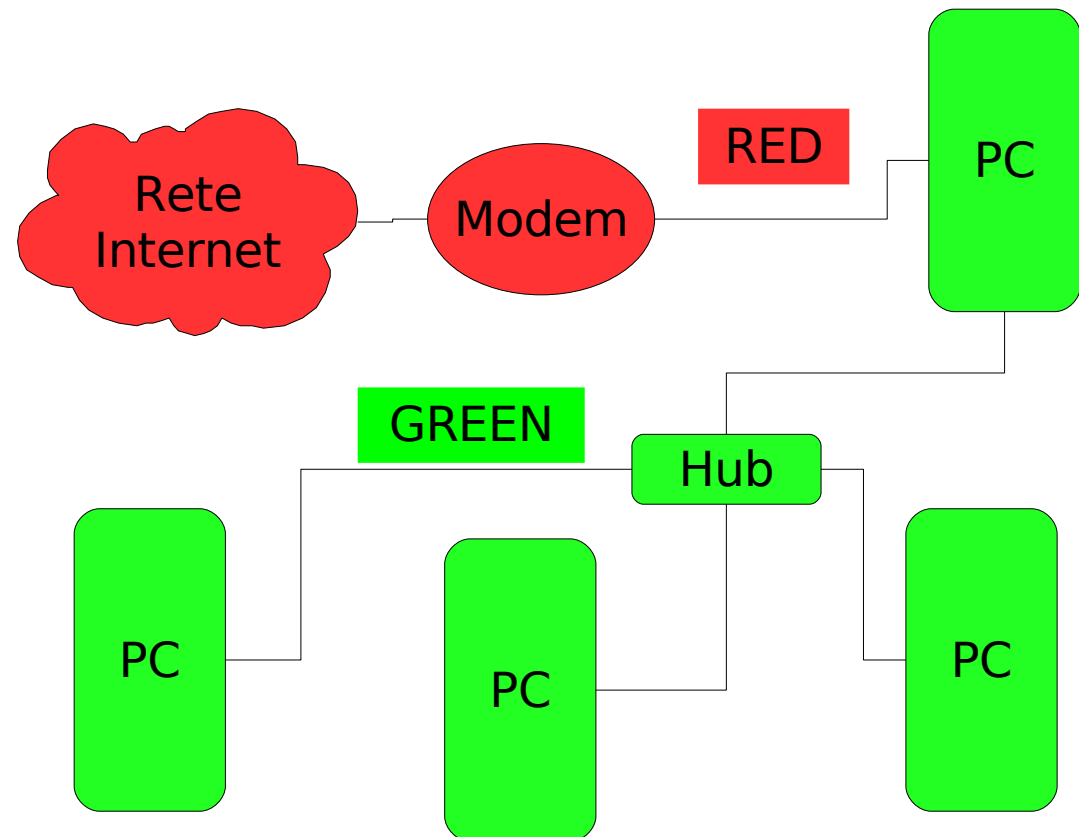
Le parti logiche sono comunque evidenziate dai colori utilizzati dalla nomenclatura standard.



Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet tramite un pc che condivide la sua connessione tramite modem.

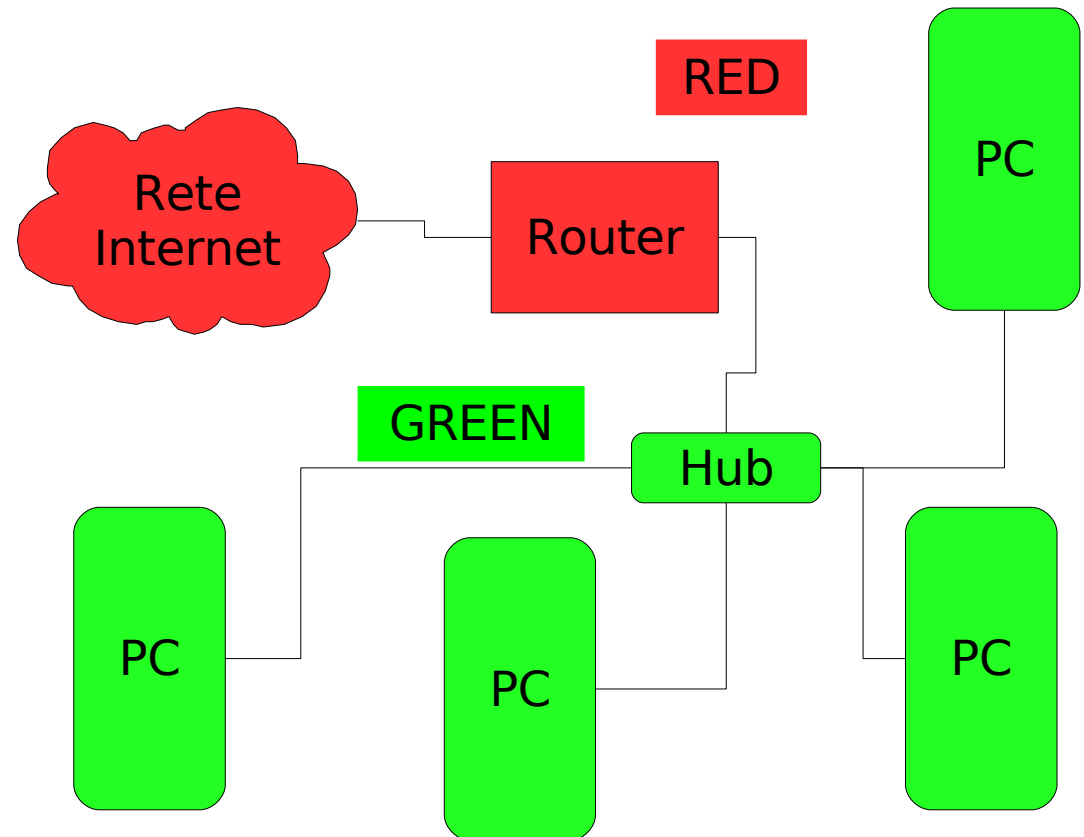
Rete **senza IpCop**, le parti logiche sono comunque evidenziate dai colori utilizzati dalla nomenclatura standard.



Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet tramite un router che condivide la connessione.

Rete **senza IpCop**, le parti logiche sono comunque evidenziate dai colori utilizzati dalla nomenclatura standard.

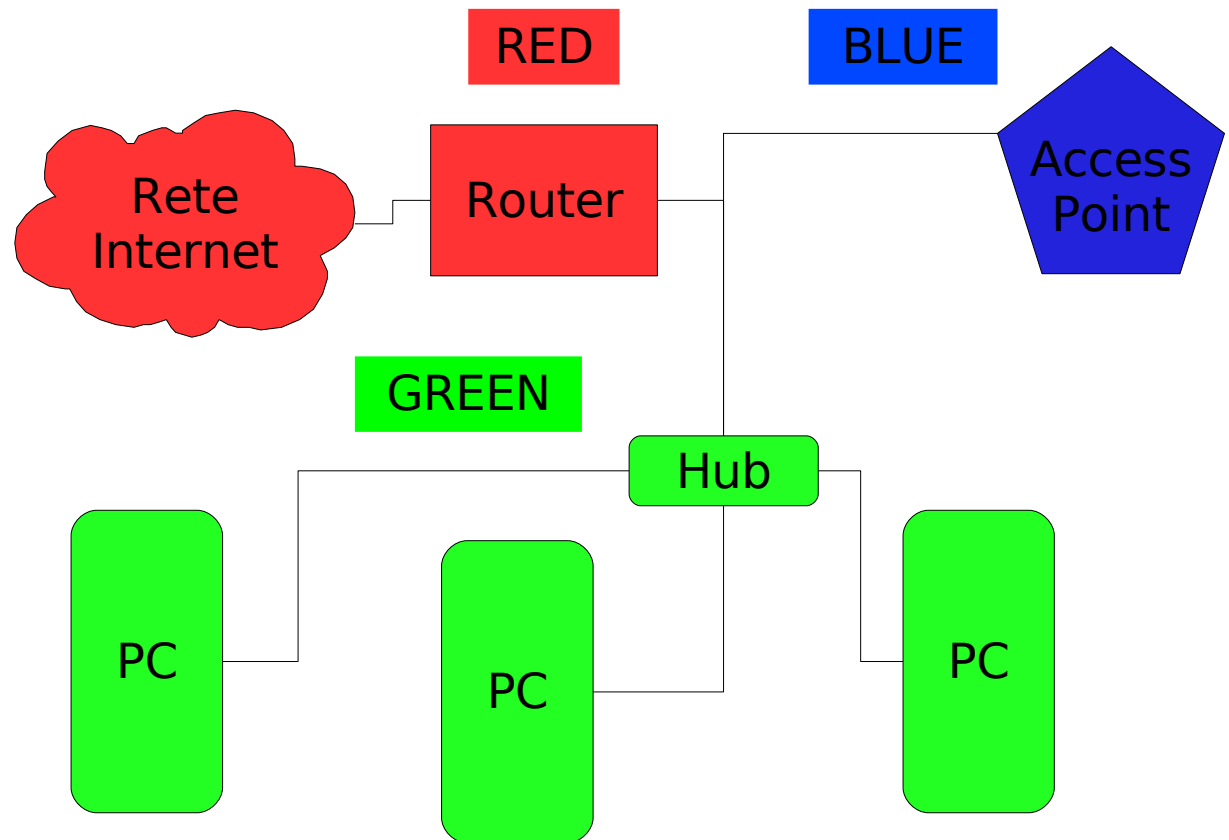


Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet tramite un router che condivide connessione.

E' inoltre presente un access point per l'accesso di rete senza fili.

Rete **senza IpCop**, le parti logiche sono comunque evidenziate dai colori utilizzati dalla nomenclatura standard.

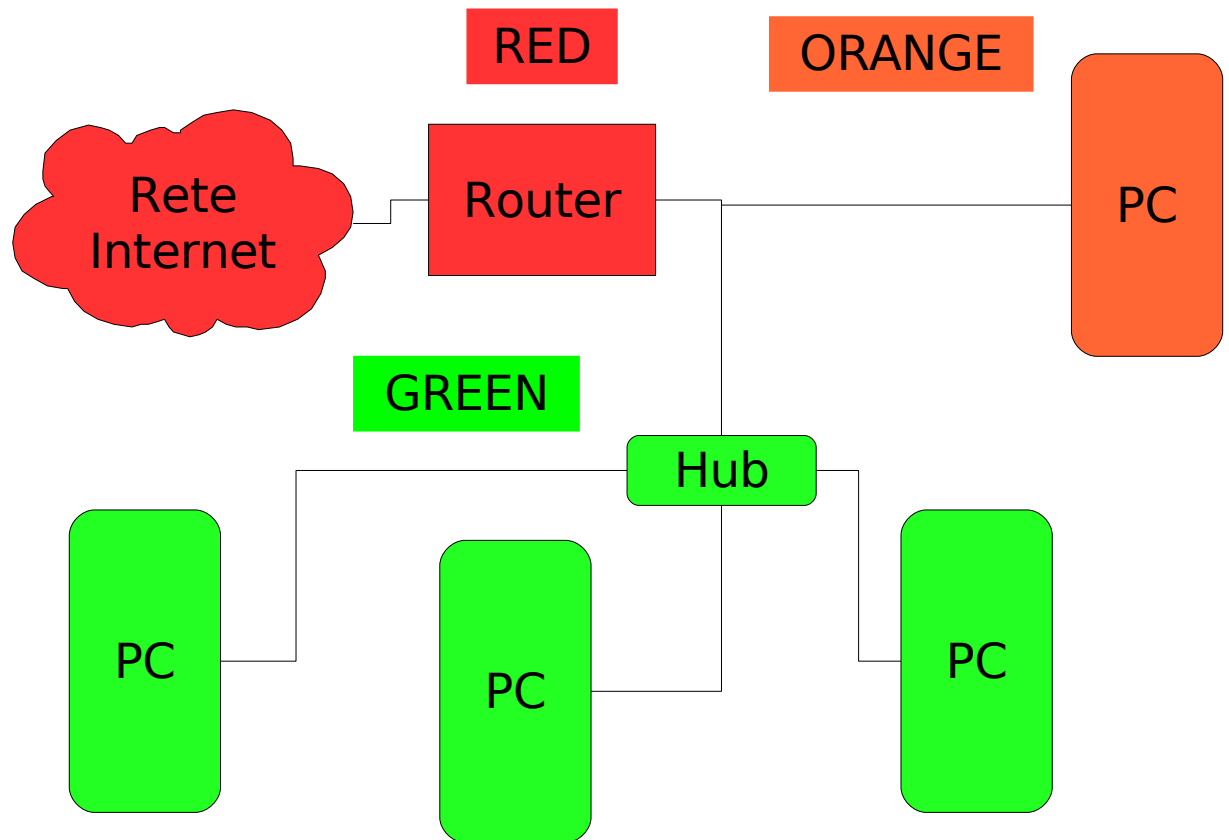


Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet tramite un router che condivide la connessione.

E' inoltre presente un server che offre servizi raggiungibili da internet.

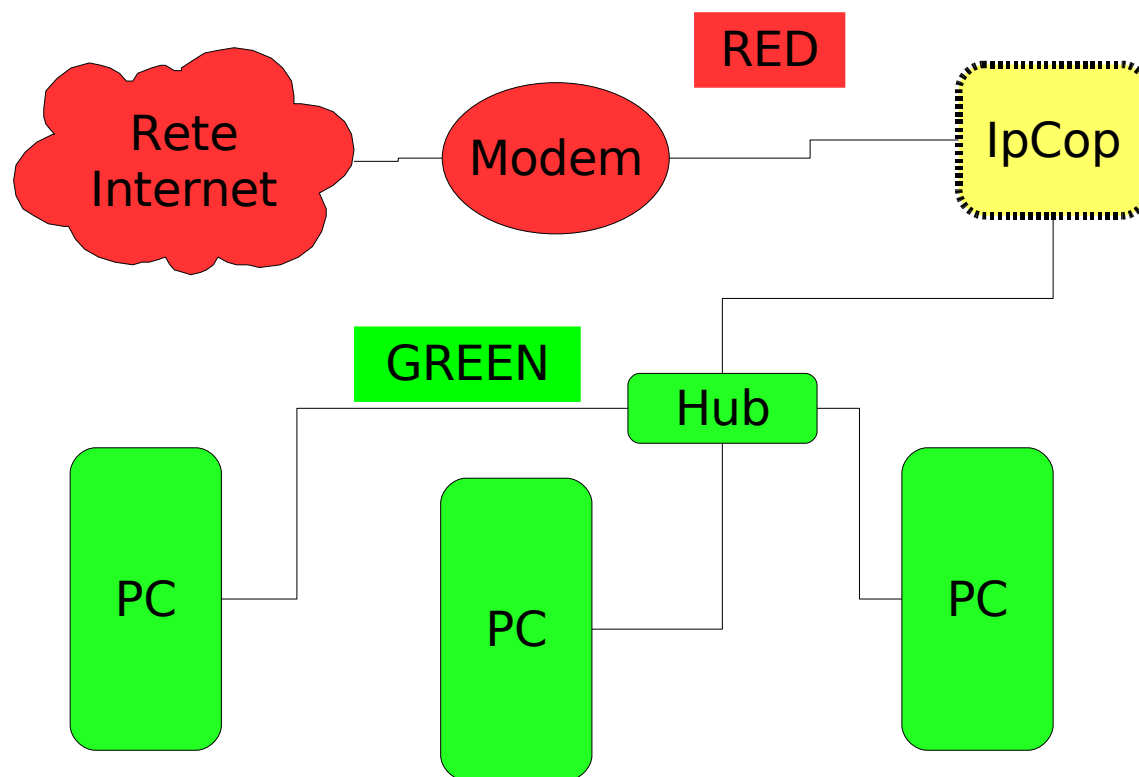
Rete **senza IpCop**, le parti logiche sono comunque evidenziate dai colori utilizzati dalla nomenclatura standard.



Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet **tramite IpCop** che condivide la connessione internet tramite modem.

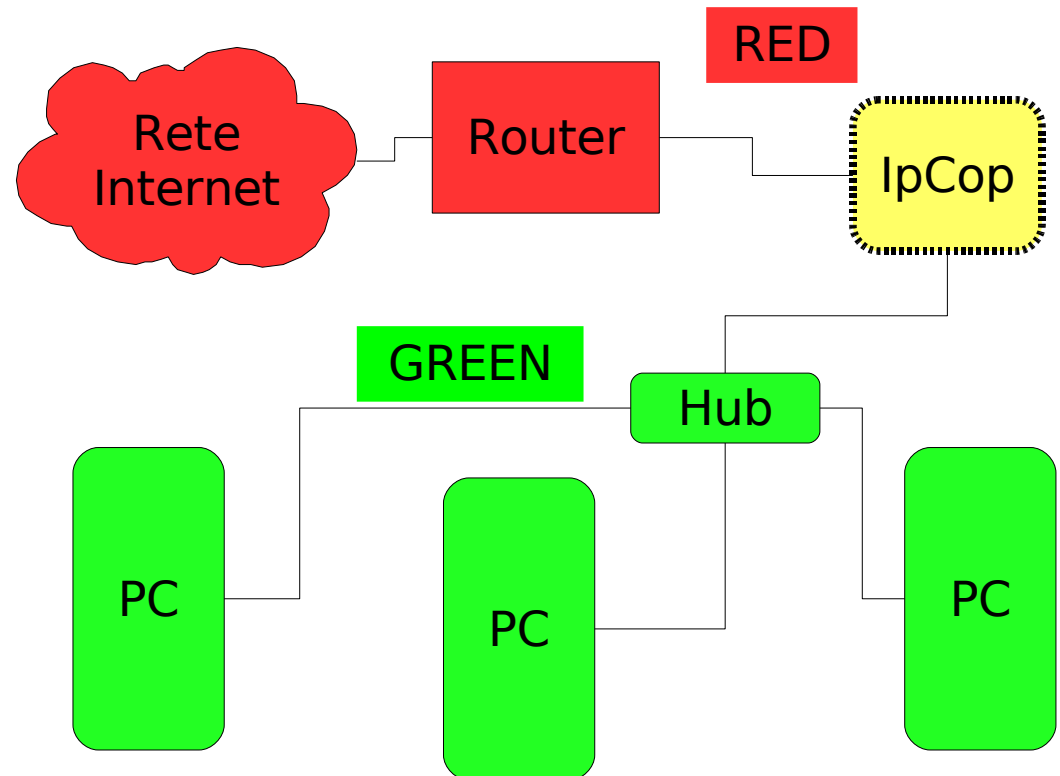
Le parti logiche sono evidenziate dai colori utilizzati dalla nomenclatura standard.



Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet **tramite IpCop** che condivide la connessione internet tramite router.

Le parti logiche sono evidenziate dai colori utilizzati dalla nomenclatura standard.



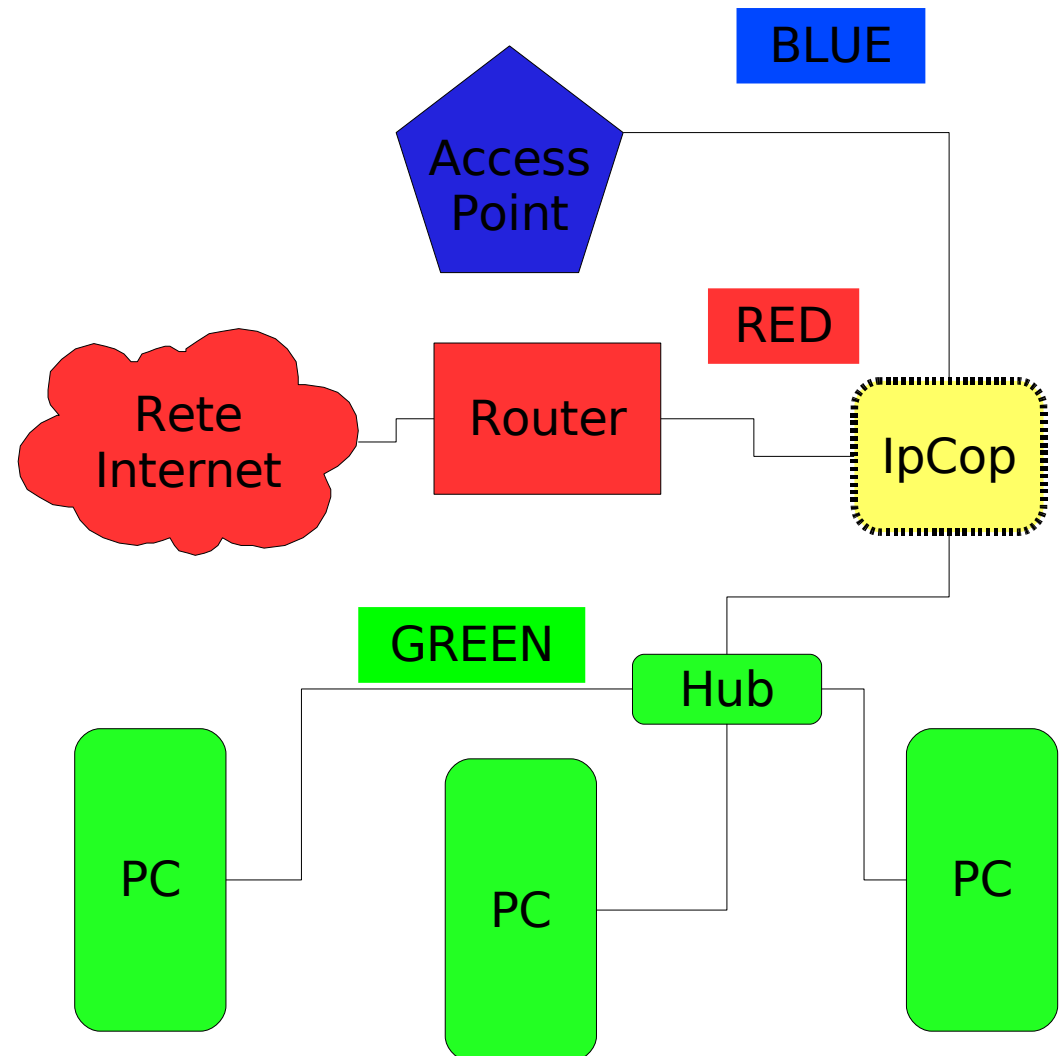
Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet **tramite IpCop** che condivide la connessione internet tramite router.

E' inoltre presente un access point per la connessione di rete senza fili.

La connessione alla rete cablata è gestita da **IpCop**.

Le parti logiche sono evidenziate dai colori utilizzati dalla nomenclatura standard.



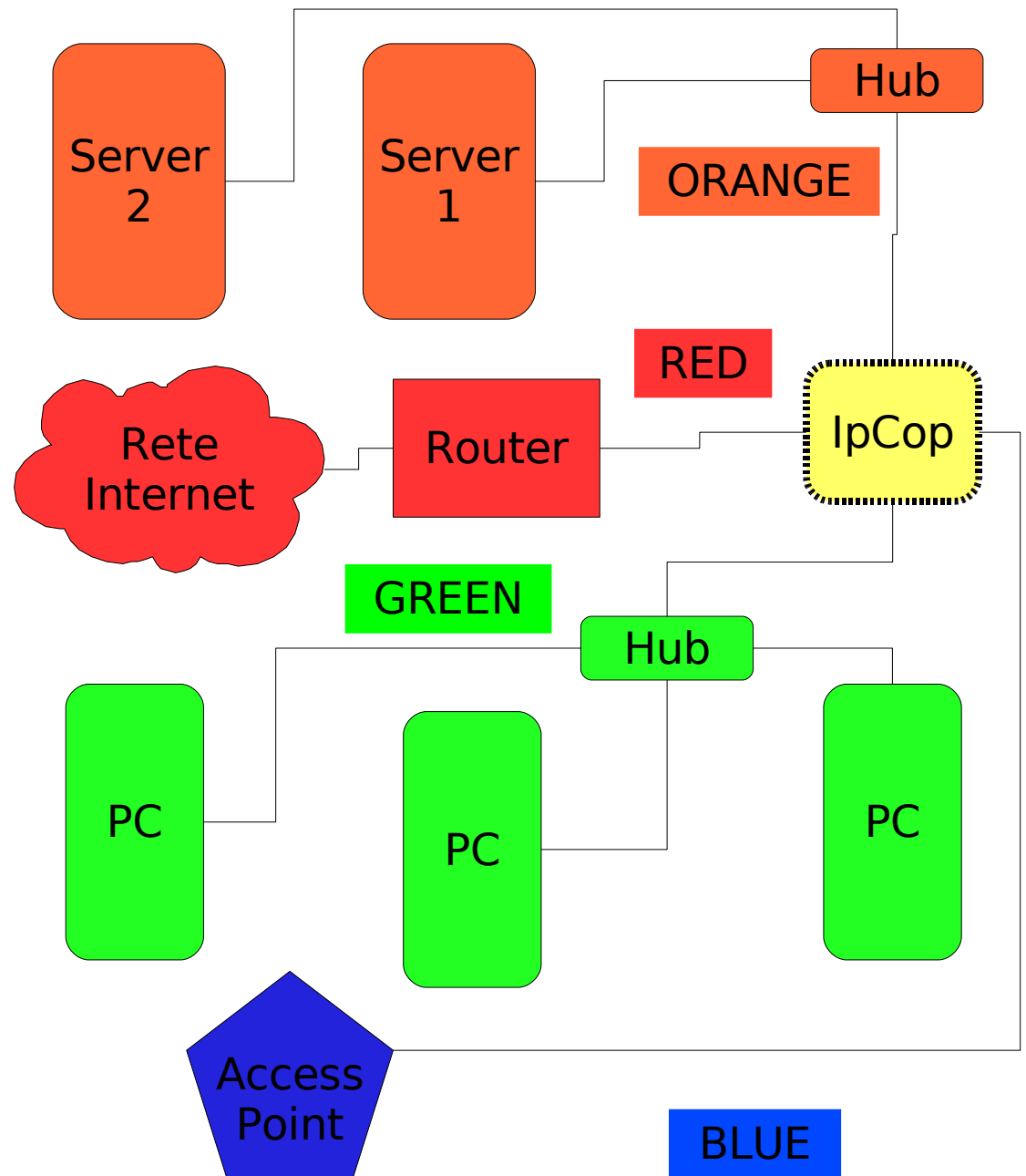
Schemi di reti e connessioni ad internet

Rete di pc connessi ad internet **tramite IpCop** che condivide la connessione internet tramite router.

E' presente un access point per la connessione di rete senza fili. La connessione alla rete cablata è gestita da **IpCop**.

E' inoltre presente una rete per i server che devono offrire servizi raggiungibili da internet.

Le parti logiche sono evidenziate dai colori utilizzati dalla nomenclatura standard.



Configurazione e gestione del firewall.

La configurazione e la gestione del firewall successive alla prima installazione avvengono in remoto, da un qualsiasi pc collegato alla rete GREEN, attraverso l'interfaccia web utilizzabile da qualsiasi browser oppure tramite la console testuale a riga di comando. La connessione avviene tramite protocolli sicuri e criptati, via web è possibile da qualsiasi sistema operativo, per la connessione alla console testuale da sistemi operativi diversi da Linux può essere necessaria l'installazione di un client ssh.

Da notare che per la maggior parte delle operazioni di configurazione è necessario l'utilizzo dell'interfaccia web, mentre l'utilizzo della riga di comando si rende indispensabile per l'installazione di alcuni addons.

Connessione all'interfaccia web.

Per la connessione all'interfaccia web è necessario aprire il browser web e digitare nella casella dell'indirizzo la stringa

https://<ip_del_firewall>:445 oppure http://<ip_del_firewall>:81

Connessione tramite riga di comando.

Per la connessione alla console da riga di comando è necessario prima di tutto attivare l'opzione relativa su IpCop tramite l'interfaccia web, successivamente su sistemi Linux si deve aprire una console testuale e digitare il comando

[ssh -p222 root@<ip_del_firewall>](#)

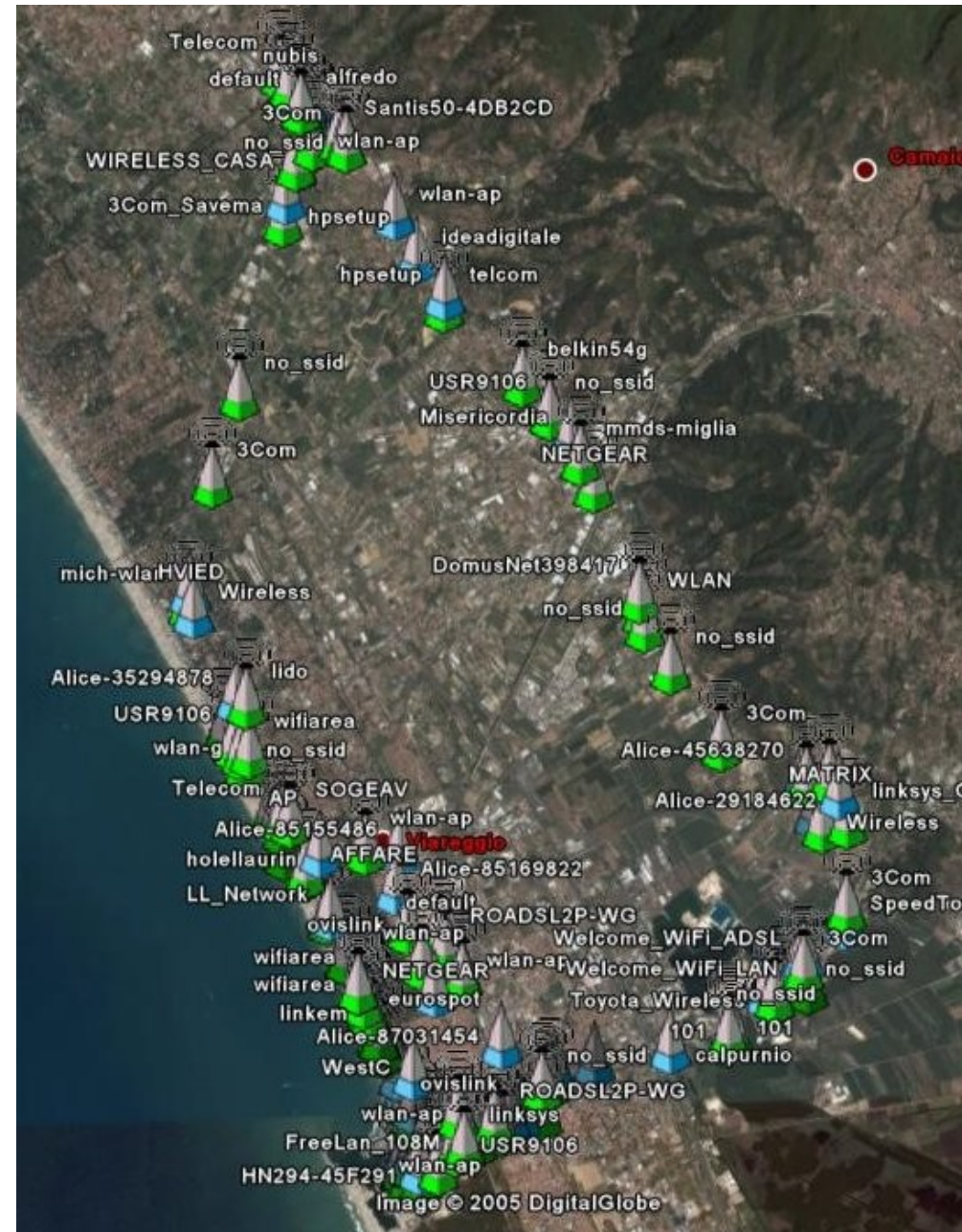
Per la connessione da sistemi Windows è consigliato l'uso del client Putty, configurato con gli stessi parametri indicati.

La protezione delle reti wireless.

Una funzione molto utile presente in maniera nativa in IpCop è la gestione dedicata alle reti wireless. L'argomento è delicato, in quanto spesso, per negligenza o scarsa conoscenza, vengono installati access point che non offrono nessun tipo di protezione, rendendo disponibile l'accesso alla rete a tutti quanti si trovassero a passare nel raggio d'azione del nostro access point. Da tenere presente che i sistemi di autenticazione presenti negli access point più datati (WEP) non assicurano una protezione adeguata.

IpCop permette di scegliere selettivamente a quali pc concedere l'accesso basandosi sul codice univoco della scheda di rete in uso; in ogni caso, anche se questo tipo di protezione venisse violato, all'eventuale intruso verrebbe concesso solo l'accesso ad internet mentre l'accesso alla rete GREEN interna sarebbe comunque impedito.

Nell'immagine a lato è possibile vedere il risultato di una ricerca degli access point presenti in zona: le icone azzurre rappresentano access point protetti, quelle verdi invece rappresentano access point non protetti che potrebbero permettere un accesso non controllato.



Pro e contro dell'utilizzo di IpCop

Pro:

- protegge tutta la rete da intrusioni provenienti da internet; impedisce agli utenti non autorizzati di modificare la configurazione.
- permette di proteggere ed isolare le connessioni provenienti dalla rete wifi dalla rete cablata. I pc collegati tramite la rete BLU possono accedere ad internet, l'accesso alla rete GREEN avviene preferibilmente configurando una connessione VPN.
- permette di proteggere ed isolare le connessioni dei server esposti su internet (rete ORANGE) da tutti gli altri pc in rete. L'eventuale compromissione di un server non consente all'attaccante l'accesso agli altri pc delle altre reti.
- può funzionare da proxy web per velocizzare l'accesso alle pagine, e da server dhcp per gestire la configurazione automatica di tutti i pc connessi in rete.
- include un sistema di analisi degli attacchi ricevuti (snort) e permette una visualizzazione semplificata di tutti i log, della configurazione e dello stato del sistema.
- attraverso l'installazione, in genere molto semplice, di addons permette di controllare l'accesso a siti non desiderati, filtrare oggetti non desiderati nelle pagine web, filtrare la posta elettronica da spam e virus, filtrare lo scaricamento di virus da siti web ed ftp, autorizzare l'accesso ad internet di determinati pc in orari prestabiliti, impedire o limitare l'uso verso l'esterno di programmi e servizi non desiderati come ad esempio il peer to peer.
- tutte le funzioni ed i servizi vengono gestite in maniera centralizzata, senza la necessità di configurare le singole postazioni.
- i costi: il pc da dedicare alle funzioni di firewall non deve avere prestazioni elevatissime o componenti "ultimo grido", le schede di rete aggiuntive costano ormai pochi euro, a parte la prima installazione il pc non necessita di monitor e tastiera, la licenza GPL del programma, ed in genere degli addons, permette l'installazione su un numero illimitato di pc senza nessun costo.

Pro e contro dell'utilizzo di IpCop

Contro:

- è necessario utilizzare un pc dedicato esclusivamente alle funzioni di firewall, tale pc deve essere sempre lasciato acceso e sarebbe preferibile, come per il router del resto, che fosse protetto da un gruppo di continuità.
- l'installazione di un nuovo pc con funzioni di firewall può creare problemi di spazio e la necessità di stendere nuovi cavi di rete ed alimentazione.
- è praticamente indispensabile una connessione adsl di tipo flat a canone fisso ed indipendente dal traffico, l'utilizzo di una connessione a consumo può far lievitare i costi di gestione in maniera difficilmente controllabile.
- è consigliabile, oltre che più semplice, utilizzare un router per la connessione ad internet; il software supporta l'utilizzo di alcuni modem usb ed alcuni adattatori isdn, ma in numero molto limitato, tale da non poterne garantire a priori il corretto funzionamento.
- sebbene l'installazione e la configurazione di base del sistema siano molto semplificate rispetto alla configurazione da zero di una distribuzione per ottenere risultati analoghi, è comunque necessaria una conoscenza di base delle reti e del loro funzionamento.
- potrebbe essere necessario riconfigurare il router per ottimizzarne il funzionamento con IpCop
- l'installazione e la configurazione di alcuni addons richiedono una conoscenza abbastanza approfondita del funzionamento delle reti, dei protocolli di comunicazione e dei software utilizzati.
- i costi: oltre al router, praticamente indispensabile, potrebbe essere necessario acquistare nuove schede di rete, hub/switch, cavi di rete ed access point. E' da notare che il costo di apparecchiature di rete di alto livello può inevitabilmente far lievitare il costo finale.

Esempio: IpCop all'opera

Connessione all'interfaccia web del firewall [IpCop](#) qui in uso.

Links e riferimenti

Il sito di IpCop:	http://www.ipcop.org	Download e documentazione del programma
Il sito di CopFilter:	http://www.copfilter.org	Un utile addon per IpCop
Il sito Grc	http://grc.com	Un sito per testare la protezione dei firewall
Siti di Addons per IpCop		
FirewallAddons		Addons installabili dall'interfaccia web
MhAddons		Addons installabili da linea di comando
Zerina OpenVPN		Ottimo addon per utilizzare OpenVPN

Esempio di installazione di IpCop

Se il tempo lo consente... vediamo adesso un esempio di installazione.

L'installazione verrà effettuata in una macchina virtuale realizzata con Qemu, il tempo necessario ad effettuare l'installazione potrebbe essere superiore al tempo impiegato per l'installazione su un pc reale.