

### Introduzione

Internet sicura a scuola a costo zero. Questo documento presenta le istruzioni passo passo per installare e configurare il firewall Asso.Dschola con il filtro per la navigazione dell'Università di Tolosa.

Il filtro proposto si basa su Endian Firewall, una versione Italiana del firewall open source IPCop. Un utente esperto potrà utilizzare queste istruzioni anche per la configurazione di IPCop e di altri prodotti simili. La versione Asso.Dschola di Endian Firewall è già preconfigurata in molte parti per il pronto utilizzo a scuola ed è oggetto di queste istruzioni.

Il computer da destinare alle funzioni di firewall può anche essere un computer di recupero non troppo recente, ovviamente più il computer è obsoleto minori saranno le prestazioni del filtro. Con 256 Mb di RAM e un Processore di classe Pentium non avrete problemi sulle ADSL da 20MB con una cinquantina di computer. Attenzione a non utilizzare computer con problemi di raffreddamento o di consumi eccessivi perché il filtro, una volta configurato, dovrà rimanere sempre acceso.

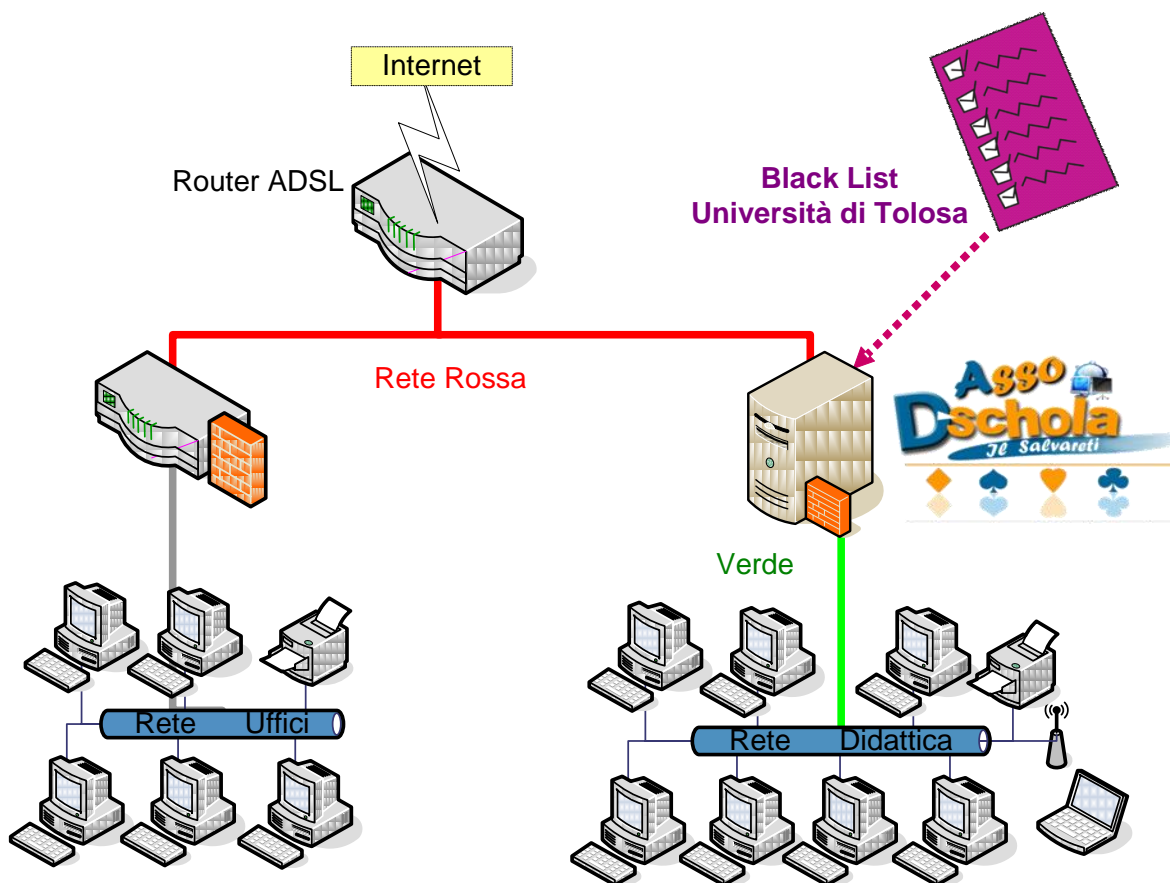
### Possibili configurazioni di installazione

La rete rossa è la rete di connessione ad Internet non protetta

La rete verde è la rete con la navigazione protetta.

Con questo firewall è possibile configurare e proteggere anche la rete della segreteria, una rete wireless e la rete dedicata ai server; ma queste istruzioni non trattano queste particolari configurazioni anche perché, in molte scuole, la rete della segreteria è già dotata di un proprio firewall.

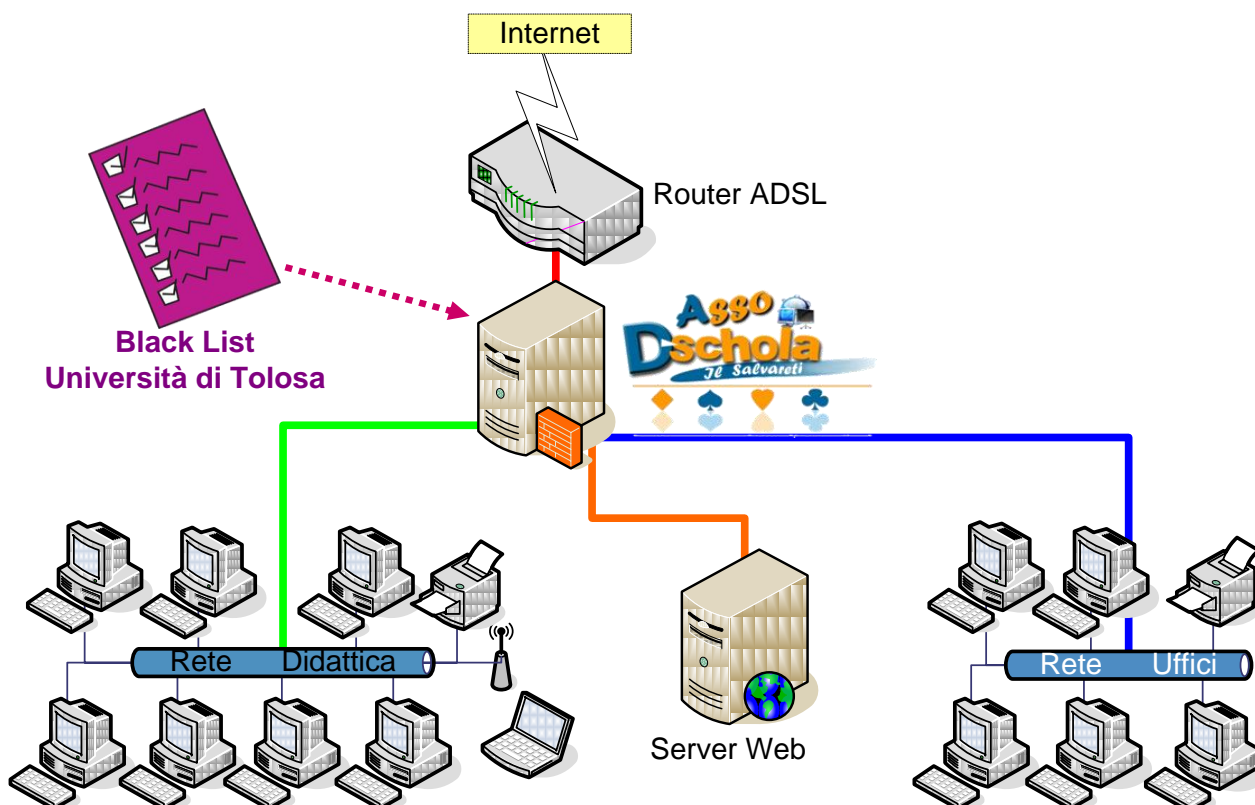
#### Rete uffici con firewall e rete didattica con navigazione protetta



### Solo rete didattica con navigazione protetta



### Rete didattica, uffici e server



### Procedura di installazione

Entrare nel bios del PC e disabilitare il controllo errore della tastiera e del monitor all'avvio (se presente) in modo da poter lasciare il computer senza mouse, monitor e tastiera. Nelle impostazioni di gestione alimentazione/risparmio energetico impostare l'opzione "power loss" (perdita alimentazione) su "Always on" (sempre acceso) in questo modo, dopo uno spegnimento accidentale o un black-out il computer con funzioni di filtro si riaccende automaticamente senza creare disservizi alla rete,

Avviare il computer inserendo il cd con Endian Firewall versione Asso.Dschola: procedere di default senza attivare la console.

Su INTERFACCIA GREEN inserire il seguente indirizzo IP del router 192.168.10.254 (Net mask 255.255.255.0) o un altro indirizzo scelto dalla scuola. Nella scelta prestare attenzione ad evitare conflitti con la rete che ci fornisce il router (di solito i router ADSL usano sottoreti a 192.168.1.x o 192.168.0.x).

L'installazione è terminata. ☺

### Connessione e configurazione

Collegare ad una delle schede di rete un PC per la configurazione. Se la connessione è diretta può essere utile un cavo cross (con le moderne schede di rete non è necessario).

Configurare il pc sul seguente indirizzo IP: 192.168.10.10; mask 255.255.255.0; gateway 192.168.10.254; dns 192.168.10.254 (o altro indirizzo compatibile con la sottorete scelta dalla scuola), con questa configurazione il pc non naviga ancora ma accede alle pagine di configurazione del filtro Endian Firewall.

Puntare il browser su <https://192.168.10.254:10443>. Se la pagina di amministrazione non risulta raggiungibile cambiare la connessione alla scheda di rete su Endian FW, attendere qualche secondo e riprovare.

In caso di problemi ad individuare la scheda di rete giusta lanciare dal prompt dei comandi MSDOS del PC utilizzato per la configurazione il seguente comando:

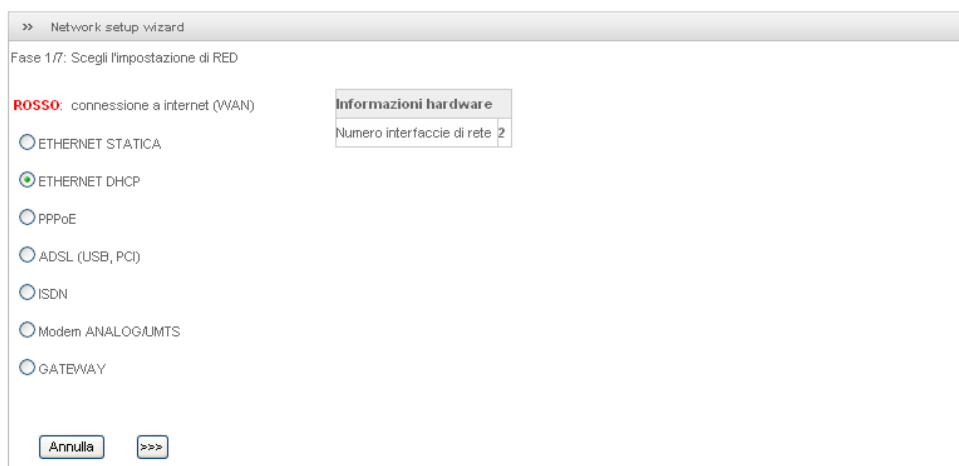
```
ping 192.168.10.254 -t
```

e provare a collegarsi sulle diverse schede di rete del filtro fino a quando non riceviamo risposta.

Una volta individuata la scheda verde, collegare l'altra scheda con un solo cavo al router (rete rossa).

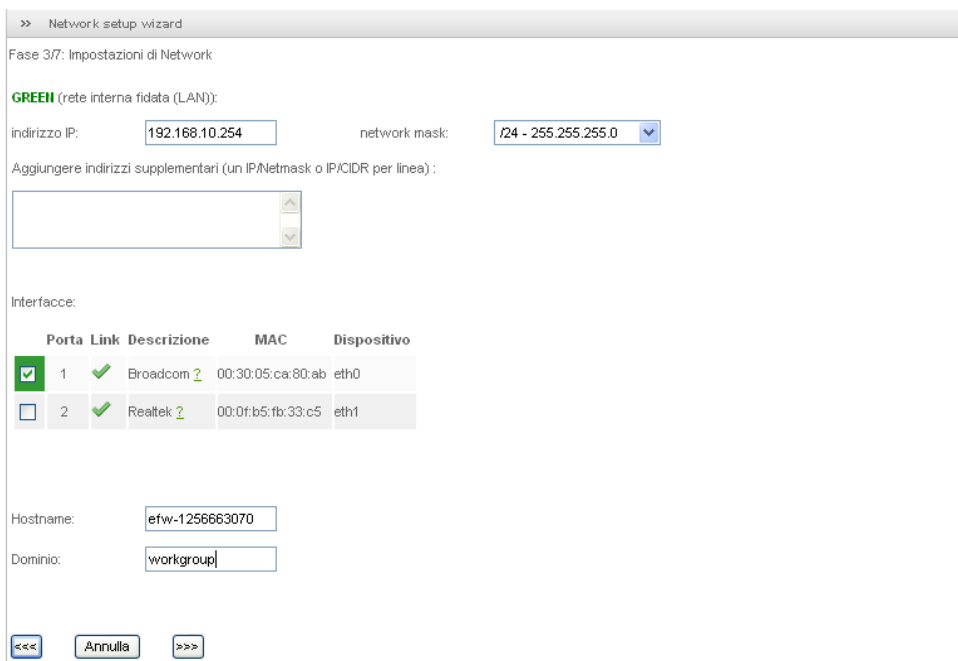
Accedere con il browser alla configurazione di Endian Firewall (Asso.Dschola), accettare la licenza GNU, scegliere la lingua, e inserire la password di Admin e di Root (consigliata una unica pw, differente da quelle già usate per altri dispositivi).

Selezionare l'indirizzo usato dalla rete rossa, nella maggior parte dei casi il router della ADSL ha il DHCP attivo e quindi non serve configurare la rete. Se invece manca il dhcp nel router, configurare la rete rossa con l'indirizzo preesistente di un computer della scuola (endian userà l'indirizzo del primo computer della rete).



Tipicamente non si usano le reti orange e blue, se non nelle scuole superiori o in grado di amministrarsi tale configurazione.

Confermare le impostazioni della rete green e impostare il nome gruppo di lavoro nel campo del dominio.



>> Network setup wizard

Fase 3/7: Impostazioni di Network

**GREEN** (rete interna fidata (LAN)):

indirizzo IP:  network mask:

Aggiungere indirizzi supplementari (un IP/Netmask o IP/CIDR per linea):

Interfacce:

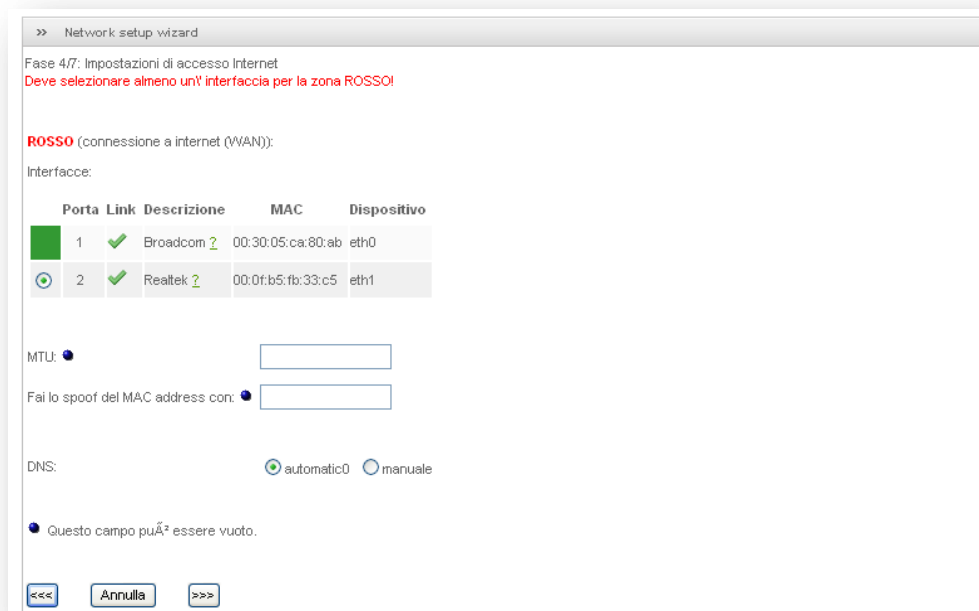
Porta	Link	Descrizione	MAC	Dispositivo
<input checked="" type="checkbox"/>	1	Broadcom	00:30:05:ca:80:ab	eth0
<input type="checkbox"/>	2	Realtek	00:0f:b5:fb:33:c5	eth1

Hostname:

Dominio:

<<< Annulla >>>

Selezionare scheda rete rossa, eventualmente inserire il DNS manualmente



>> Network setup wizard

Fase 4/7: Impostazioni di accesso Internet

**Deve selezionare almeno un' interfaccia per la zona ROSSO!**

**ROSSO** (connessione a internet (WAN)):

Interfacce:

Porta	Link	Descrizione	MAC	Dispositivo
<input checked="" type="checkbox"/>	1	Broadcom	00:30:05:ca:80:ab	eth0
<input type="checkbox"/>	2	Realtek	00:0f:b5:fb:33:c5	eth1

MTU:

Fai lo spoof del MAC address con:

DNS:  automatico  manuale

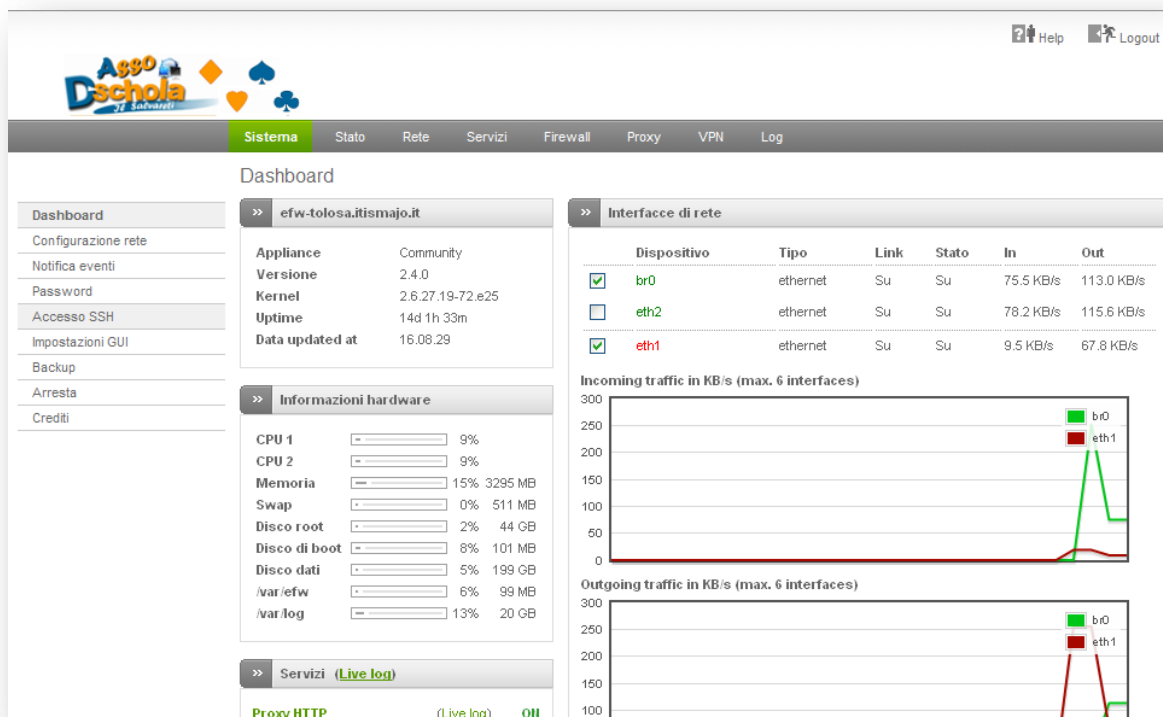
Questo campo può essere vuoto.

<<< Annulla >>>

Confermare e aspettare il riavvio di endian

### Configurazioni di base

Riconnettersi a: <https://192.168.10.254:10443> con username admin e password. (Se non è possibile riconnettersi, scambiare le due connessioni di rete sul firewall).



The screenshot shows the 'Sistema' page of the Dschola firewall management interface. The page is divided into several sections:

- Dashboard:** Shows system information for 'efw-tolosa.itismajo.it', including Appliance (Community), Version (2.4.0), Kernel (2.6.27.19-72.e25), Uptime (14d 1h 33m), and Data updated at (16.08.29).
- Informazioni hardware:** Displays hardware details for CPU 1 (9%), CPU 2 (9%), Memoria (15% 3295 MB), Swap (0% 511 MB), Disco root (2% 44 GB), Disco di boot (8% 101 MB), Disco dati (5% 199 GB), /var/efw (6% 99 MB), and /var/log (13% 20 GB).
- Servizi:** Shows the status of services, with Proxy HTTP (Live log) and Live log (Live log) both ON.
- Interfacce di rete:** A table showing network interfaces and their traffic statistics.

Dispositivo	Tipo	Link	Stato	In	Out
<input checked="" type="checkbox"/> br0	ethernet	Su	Su	75.5 KB/s	113.0 KB/s
<input type="checkbox"/> eth2	ethernet	Su	Su	78.2 KB/s	115.6 KB/s
<input checked="" type="checkbox"/> eth1	ethernet	Su	Su	9.5 KB/s	67.8 KB/s

Below the table are two line graphs: 'Incoming traffic in KB/s (max. 6 interfaces)' and 'Outgoing traffic in KB/s (max. 6 interfaces)'. Both graphs show traffic for br0 (green) and eth1 (red).

Nella pagina "sistema" attivare l'accesso SSH dal menu di sinistra



The screenshot shows the 'Accesso SSH' page of the Dschola firewall management interface. The page is divided into several sections:

- Impostazioni di Secure Shell Access:** A section with a toggle switch for 'Abilita Secure Shell Access' (Enable Secure Shell Access), which is currently turned off. Below the toggle is a text box with the following text: 'Utilizzare l'interruttore per abilitare l'accesso al Endian Firewall utilizzando Secure Shell. Per questioni di sicurezza Secure Shell è disabilitato di default.'

L'accesso SSH, ci consente di trasferire file e di utilizzare la console del firewall via rete senza bisogno di collegare fisicamente monitor e tastiera al computer che fa da filtro.

### Software per l'accesso remoto (facoltativo)

I software per amministrare i SSH il firewall con un computer Windows sono PuTTY e WinSCP, in questa fase dell'installazione la tastiera ed il monitor dovrebbero ancora essere collegati al filtro e quindi non sono

necessari. Si tratta, comunque, di funzionalità avanzate che non interessano la maggior parte degli utenti, se avete le conoscenze per utilizzare l'accesso remoto SSH potete scaricare:

PuTTY per la console remota: [www.putty.org](http://www.putty.org)

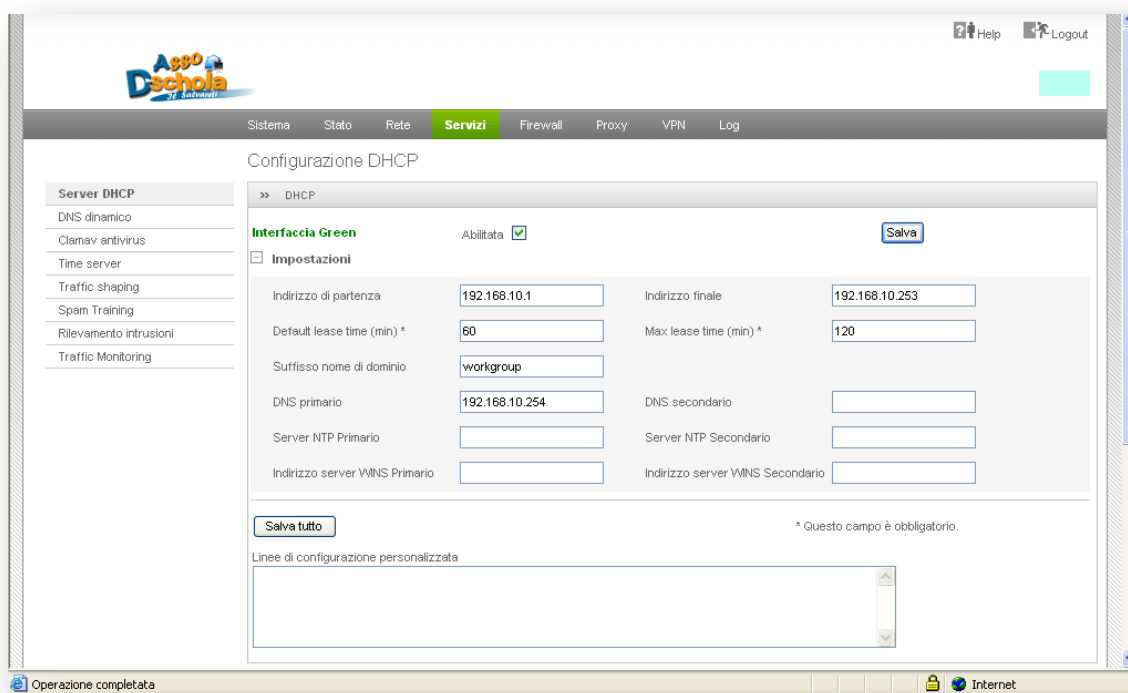
WinSCP per il trasferimento file: [www.winscp.net](http://www.winscp.net)

Trovate una copia degli stessi software anche nelle utility su [www.associazionedschola.it](http://www.associazionedschola.it)

### Configurazione servizi di rete

Adesso bisogna attivare i servizi sulla rete verde: dhcp, dns, proxy, filtro.

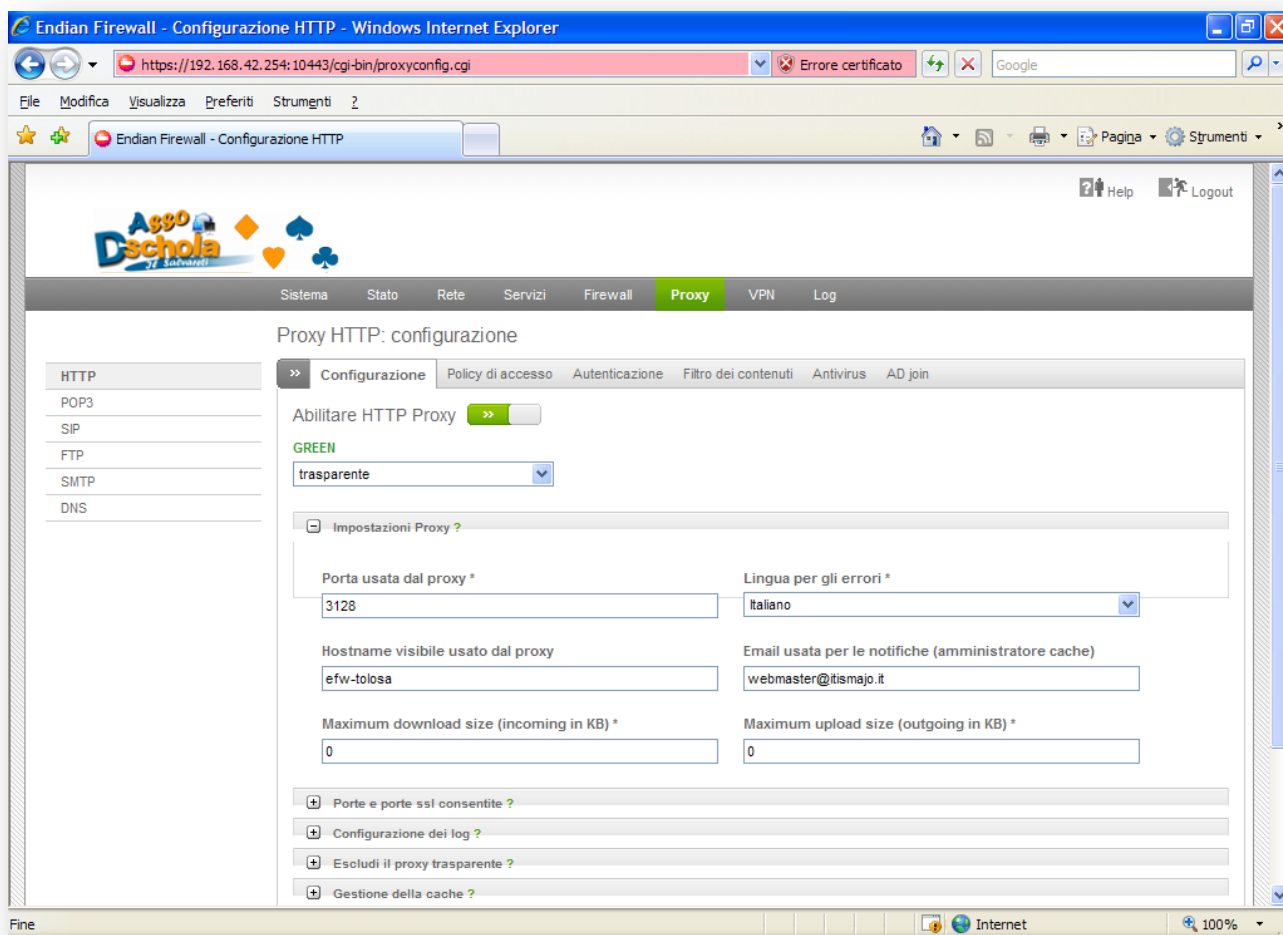
Fare clic su servizi, abilitare il dhcp su green e verificare o modificare le impostazioni del dhcp. Salva e salva tutto.



Se sono presenti dischi o stampanti di rete con indirizzo statico lasciare liberi alcuni indirizzi dalla assegnazione del DHCP. Ad esempio mettere come indirizzo finale 199 anziché 253. Così stampanti, dischi e server potranno utilizzare indirizzi statici da 200 a 253.

Andare su proxy e abilitare http proxy

Impostare proxy su green trasparente (in questo modo non è necessario configurare i browser dei diversi PC)



Impostare la lingua dei messaggi di errore in italiano

Eventualmente attivare i log del proxy della navigazione mettendo in guardia il responsabile della rete sui problemi di privacy (soprattutto per il "Log delle connessioni in uscita accettate").

Aumentare in gestione della cache le dimensioni del disco e del singolo file (x10 o x100). Questa opzione è molto utile per le connessioni lente perché mantiene nel disco rigido del filtro i file più scaricati senza prelevarli ogni volta da Internet.

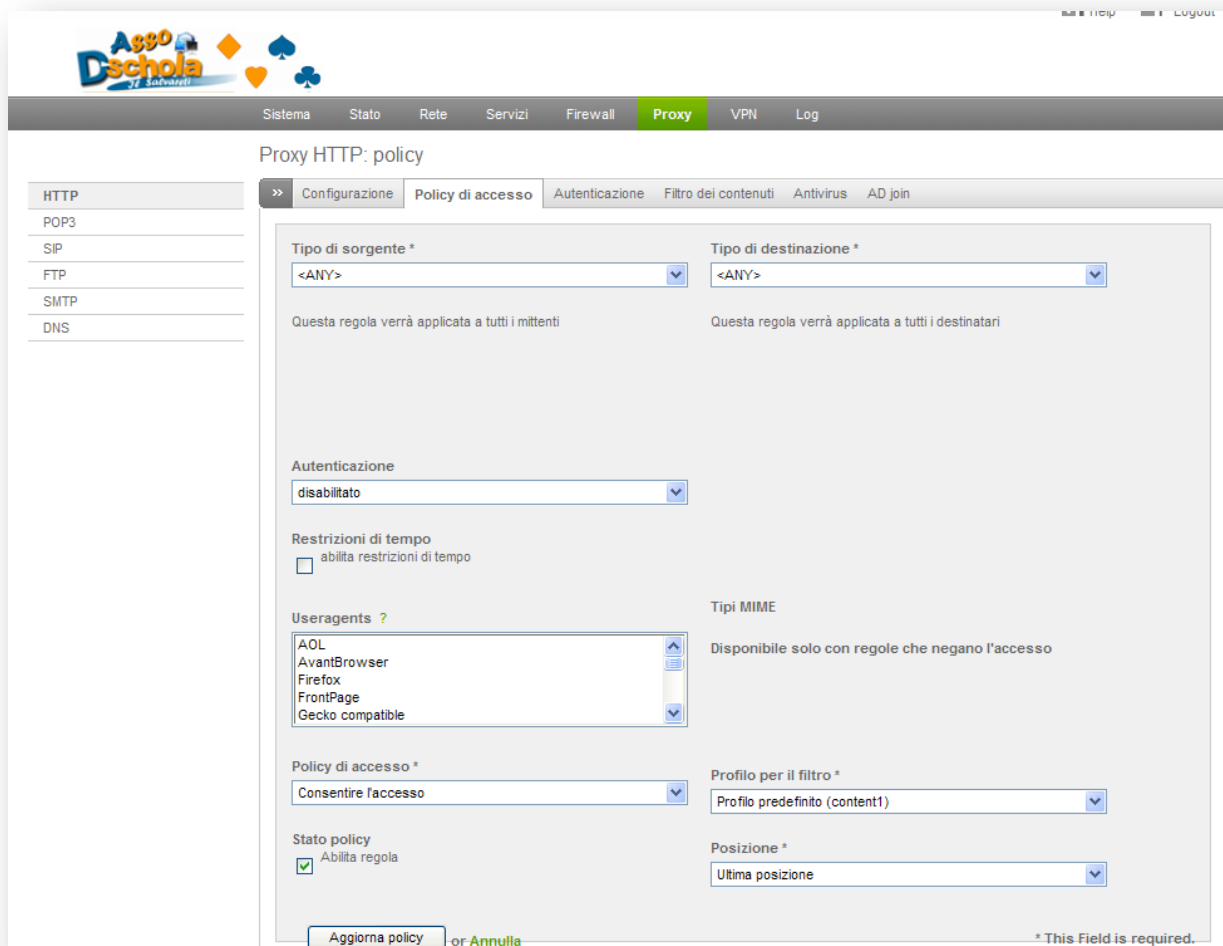
Per velocizzare il download di software e aggiornamenti mettere le seguenti dimensioni:

- 900MB per il singolo file (un intero CD/immagine ISO) se il pc è recente anche 5GB (un DVD)
- Almeno la metà del disco rigido come dimensione della cache su disco o anche più

### Filtro contenuti

Andare in policy di accesso e creare una nuova regola con filtro contenuti basato su "content1" (content1 è il profilo predefinito per il filtro).

La regola deve essere creata con sorgente/destinazione any, autenticazione disabilitata, policy di accesso "consentire accesso" e profilo per il filtro predefinito (content1).



The screenshot shows the configuration page for a Proxy HTTP policy. The interface includes a navigation menu at the top with options like Sistema, Stato, Rete, Servizi, Firewall, Proxy (selected), VPN, and Log. The main content area is titled "Proxy HTTP: policy" and contains several configuration sections:

- Configurazione:** Policy di accesso (selected), Autenticazione, Filtro dei contenuti, Antivirus, AD join.
- Tipo di sorgente \*:** Dropdown menu set to "<ANY>".
- Tipo di destinazione \*:** Dropdown menu set to "<ANY>".
- Autenticazione:** Dropdown menu set to "disabilitato".
- Restrizioni di tempo:** Checkbox "abilita restrizioni di tempo" is unchecked.
- Useragents ?:** List box containing AOL, AvantBrowser, Firefox, FrontPage, and Gecko compatible.
- Tipi MIME:** Note: "Disponibile solo con regole che negano l'accesso".
- Policy di accesso \*:** Dropdown menu set to "Consentire l'accesso".
- Profilo per il filtro \*:** Dropdown menu set to "Profilo predefinito (content1)".
- Stato policy:** Checkbox "Abilita regola" is checked.
- Posizione \*:** Dropdown menu set to "Ultima posizione".

At the bottom, there are buttons for "Aggiorna policy" and "Annulla", and a note: "\* This field is required."

Per migliori prestazioni e minore necessità di manutenzione disattivare o eliminare la regola dell'antivirus (la nostra esperienza ci dice che il filtro antivirus sul firewall, benché decisamente comodo, talvolta causa problemi dovuti al rapido cambio delle tecnologie di antivirus che possono diventare improvvisamente obsolete e impedire la navigazione in caso di mancato aggiornamento). Ricordiamo che l'antivirus sul firewall non ha nulla a che fare con gli antivirus presenti sui computer Client o Server, quindi la disattivazione di questo servizio accessorio di rete non pregiudica la funzionalità e la sicurezza offerta dalle soluzioni antivirus installate sui computer o dalle soluzioni di congelamento (Deep Freeze/Magic Card).

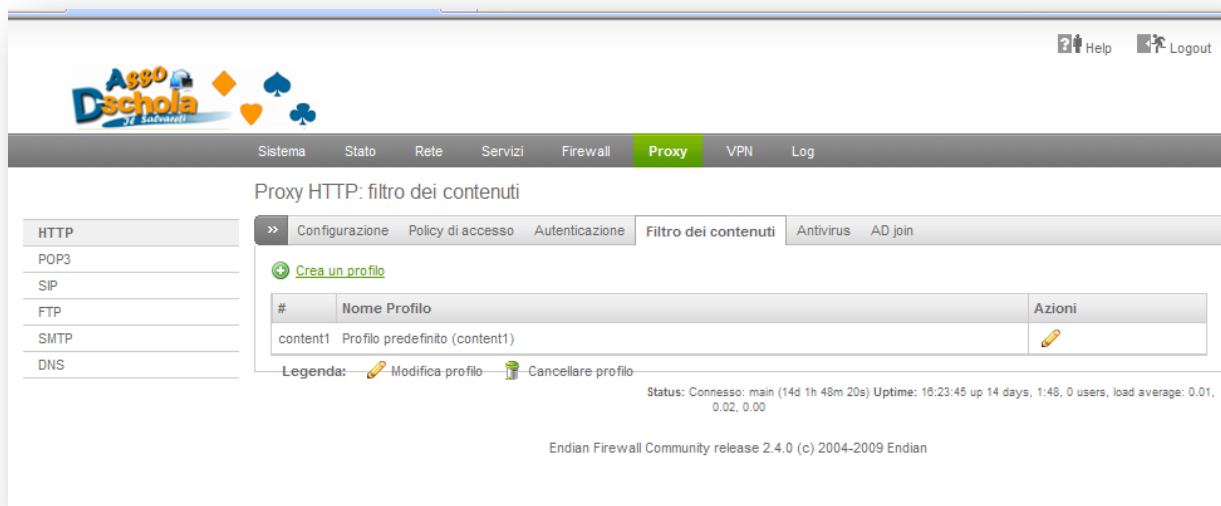
# NAVIGAZIONE PROTETTA CON ASSO.DSCHOLA

Istruzioni per l'installazione e configurazione di un filtro internet

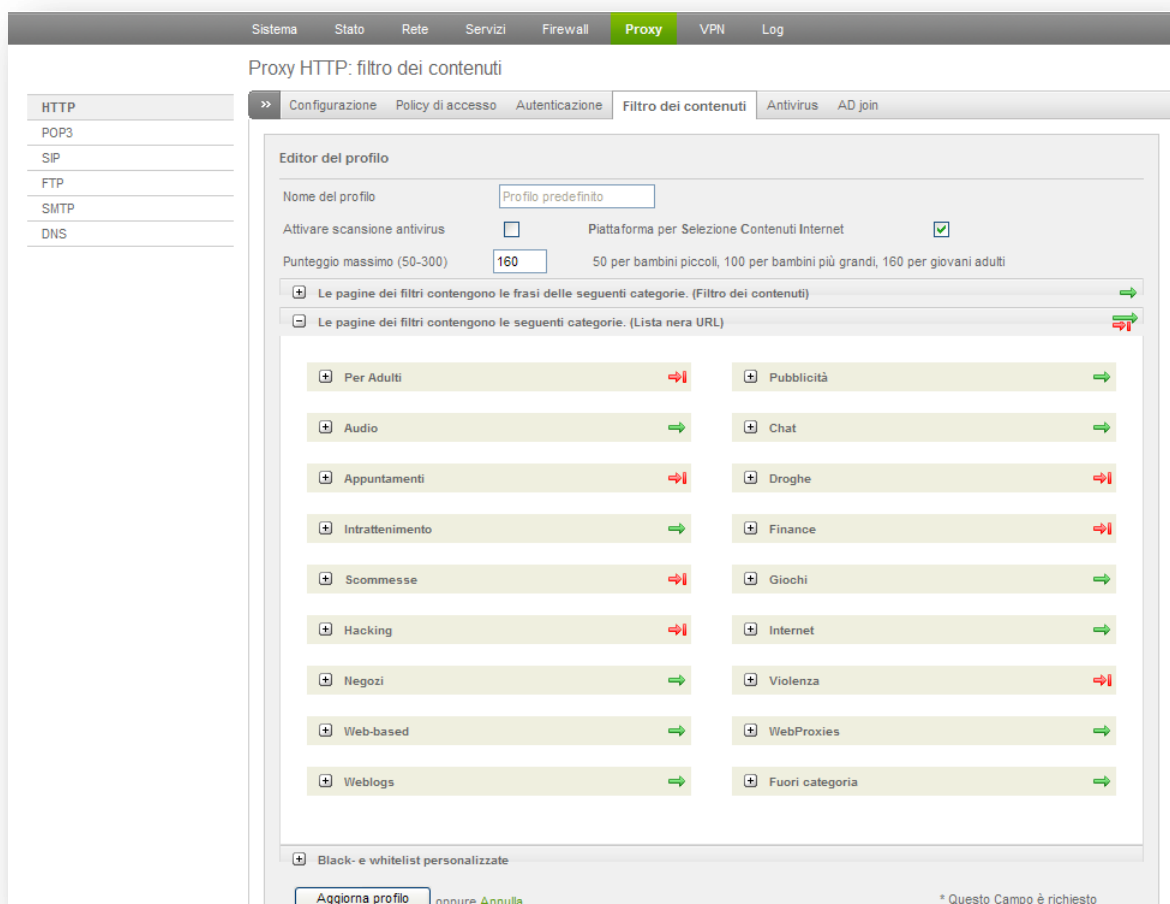


Ora rimane da impostare il filtro con le diverse categorie da bloccare:

Andare sulla voce filtro dei contenuti e modificare il profilo predefinito (content1):



Attivare la voce “piattaforma selezione contenuti internet”, disattivare la voce “scansione antivirus” e impostare le categorie da bloccare nella lista nera URL (blacklist Tolosa):





- il primo elenco di categorie si basa su parole chiave presenti nelle pagine web ed è più restrittivo e meno affidabile (conviene non usarlo a meno di non avere studenti particolarmente piccoli)
- il secondo (lista nera) si basa sulla blacklist dei siti web vietati, nel nostro caso l'elenco viene fornito gratuitamente dall'Università di Tolosa. Il catalogo è decisamente più affidabile

Il simbolo rosso indica che la categoria corrispondente è stata vietata, non è necessario vietare tutto ma solamente le categorie non adatte ai minori e all'utilizzo didattico. (ad esempio se vietate tutto non riuscirete ad usare neanche le web mail ed altri servizi che sono catalogati come web-based)

È inoltre possibile bloccare o abilitare singoli siti nelle Black e White list personalizzate.

La blacklist aggiornata viene scaricata automaticamente tutte le notti. Il filtro deve, quindi, rimanere sempre acceso.

N.B.

Durante la prima installazione è possibile che la black list non sia aggiornata, se non trovate tutte le categorie o se il filtro non vi sembra totalmente efficace potete procedere in due modi:

1. riavviare il firewall con il comando da tastiera o via browser dal menu sistema
2. attendere un giorno per consentire l'aggiornamento notturno

Completata la configurazione del filtro, selezionare il FTP (menu di sinistra) e disattivare il proxy FTP e il controllo antivirus su FTP. Il proxy trasparente su FTP, infatti, consente di accedere solamente ai server FTP in modalità anonima. Solo se non avete esigenze particolari di accesso ai server FTP potete lasciare queste opzioni attive.

Verificare che il proxy DNS (menu di sinistra) non sia attivato. Il proxy DNS è richiesto solo per particolari configurazioni tecniche. Endian Firewall è già dotato di un server DNS che è configurabile dal menu Rete per aggiungere eventuali host con relativi indirizzi IP.

### *Configurazione computer e collaudo*

Finite le configurazioni andare sulle impostazioni di rete del computer che stiamo usando e mettere indirizzo ip automatico e DNS automatico.

Verificare se il computer riesce ad accedere a internet e ripetere la configurazione su tutti i computer (Se già non sono tutti abilitati in automatico con DHCP)

Per verificare se il firewall è correttamente collegato ad internet è possibile entrare nella console digitando 0 sulla tastiera, nome utente: root e password; dopodiché provare a scrivere il seguente comando:

**ping www.libero.it**

A differenza di molti altri portali Libero risponde al ping. Se le risposte arrivano la connessione ad internet è ok. Fermare il ping con Control-C. e uscire dalla console con exit

Quando tutto funziona è possibile staccare tastiera e monitor e lasciare il filtro acceso per sempre.

La navigazione è ora protetta ☺



### Download

La versione Dschola di Endian firewall è scaricabile da: [www.associazionedschola.it/asso](http://www.associazionedschola.it/asso)

o [www.associazionedschola.it/majorana](http://www.associazionedschola.it/majorana) o [www.associazionedschola.it/avogadro](http://www.associazionedschola.it/avogadro) e utilizza la Blacklist di Tolosa più molte configurazioni già pronte per l'utilizzo nelle scuole. La versione 2 utilizza l'ultima e più recente versione di Endian Firewall. L'aggiornamento della blacklist viene effettuato alle 4.00 di tutti i giorni.

La versione ufficiale di Endian firewall è scaricabile da: [www.endian.com/en/community/download](http://www.endian.com/en/community/download)

La blacklist dell'Università di Tolosa 1 si può scaricare dal seguente URL:

<http://cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz>

### IPCop

Per realizzare la stessa configurazione con IPCop scaricare il firewall da <http://www.ipcop.org/index-pn.php> e il modulo di filtro con la blacklist di Tolosa da <http://franck78.ath.cx/> installare secondo le istruzioni (solo per utenti esperti).

### IPFIRE

La stessa configurazione è realizzabile con la distribuzione IPFIRE che è già preconfigurata per utilizzare la Black List di Tolosa e, a scelta, altre BlackList. Scaricare e installare IPFIRE da [www.ipfire.org](http://www.ipfire.org) (solo per utenti esperti)

### Team di Sviluppo

Ivan Bertotto	ITI Avogadro
Lorenzo Nazario	ITI Avogadro
Alberto Maccario	ITI Majorana
Dario Zucchini	ITI Majorana

[info@associazionedschola.it](mailto:info@associazionedschola.it)

[www.associazionedschola.it](http://www.associazionedschola.it)

Lasciate un vostro parere, commento o segnalazione su: [www.associazionedschola.it/asso](http://www.associazionedschola.it/asso)



Asso.Dschola by Associazione Dschola is licensed under a [Creative Commons Attribution - Non commerciale 2.5 Italia License](http://creativecommons.org/licenses/by-nc/2.5/it/).  
Permissions beyond the scope of this license may be available at [www.associazionedschola.it](http://www.associazionedschola.it).