Squid

Come gestire e controllare gli accessi al Web dalle reti scolastiche

Giancarlo Dessì

E-mail: gian at cettolini.it

IPSAA "Sante Cettolini" Cagliari, Sede di Villacidro

http://www.cettolini.it

Indice

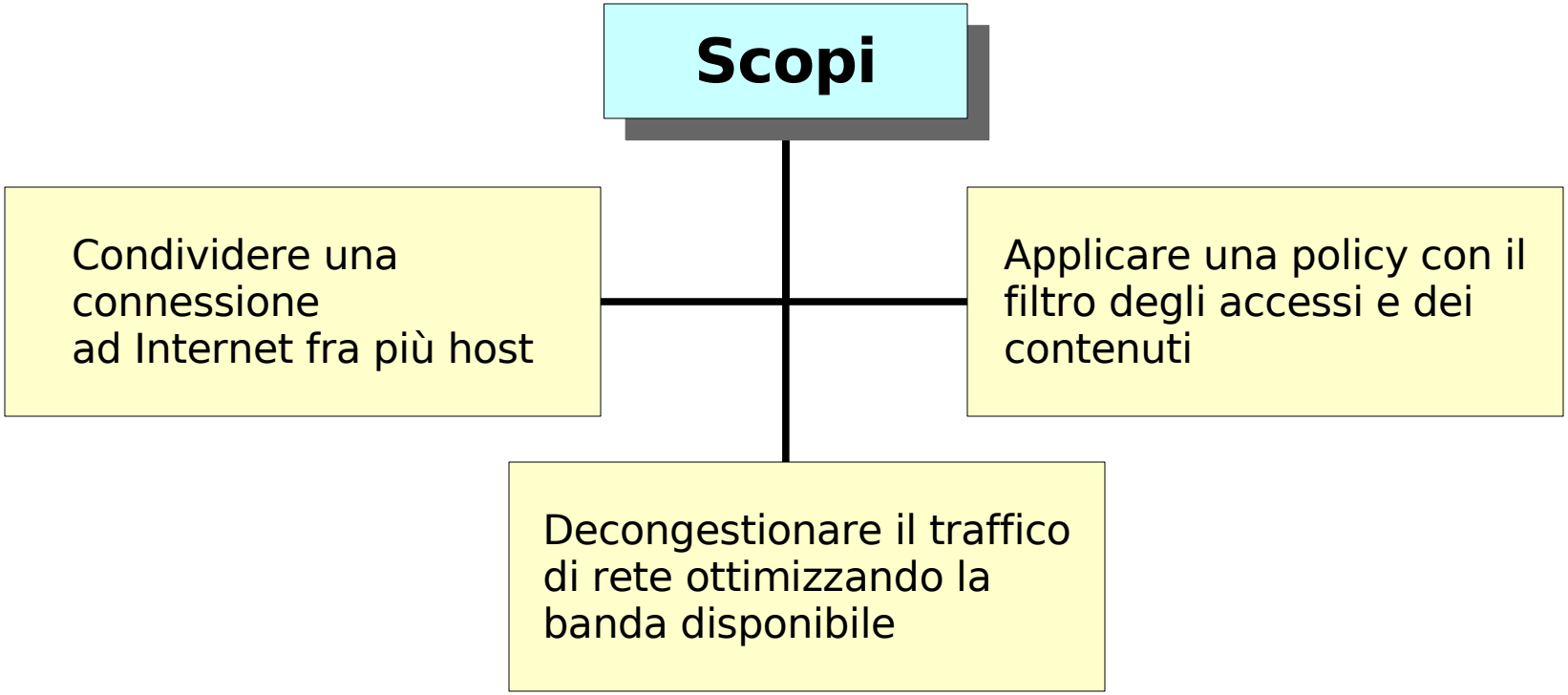
Squid e DansGuardian nelle reti scolastiche

In questa presentazione vedremo:

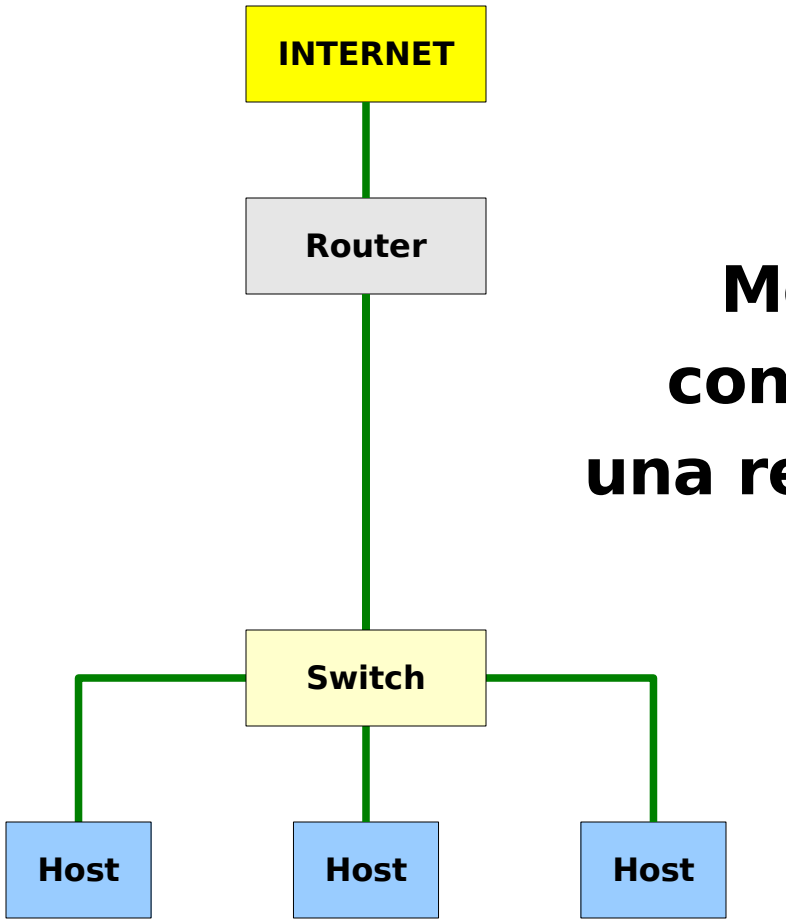
- Cos'è un servizio cache proxy
- I vantaggi rispetto alla connessione diretta
- Potenzialità di un cache proxy implementato
- Il cache proxy Squid
- Il *content filtering* DansGuardian
- Installazione e configurazione dei servizi in un sistema GNU Linux
- Analisi dei log
- Caso pratico: il controllo del traffico Web nella rete scolastica della scuola di Villacidro IPSAA Cettolini di Cagliari

Cos'è un cache proxy?

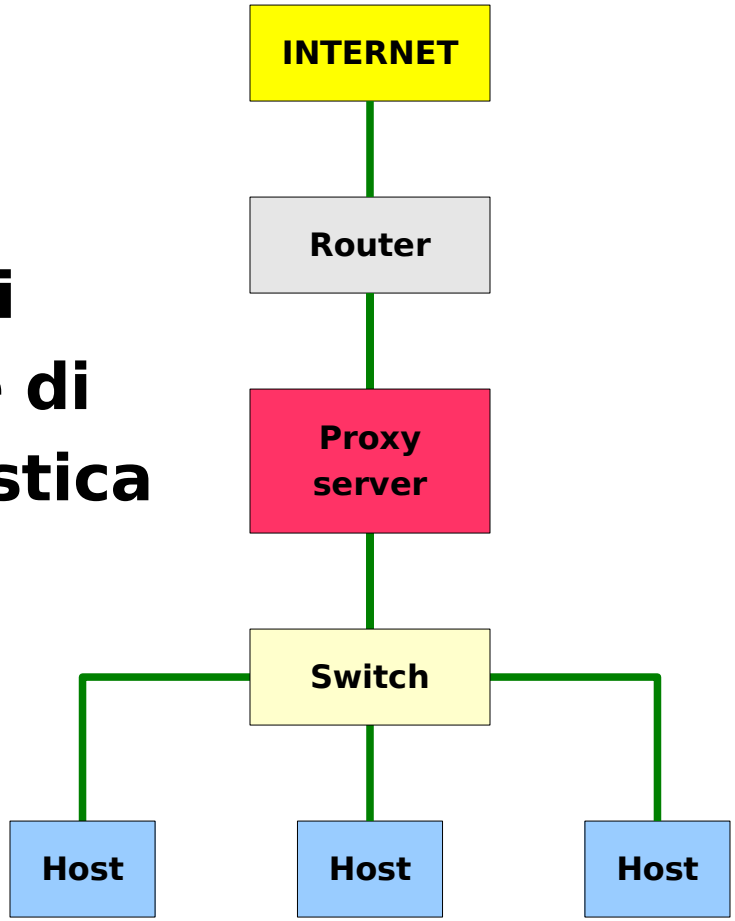
Servizio di memorizzazione locale delle risorse di rete richieste dai client



Modalità di connessione di una rete scolastica

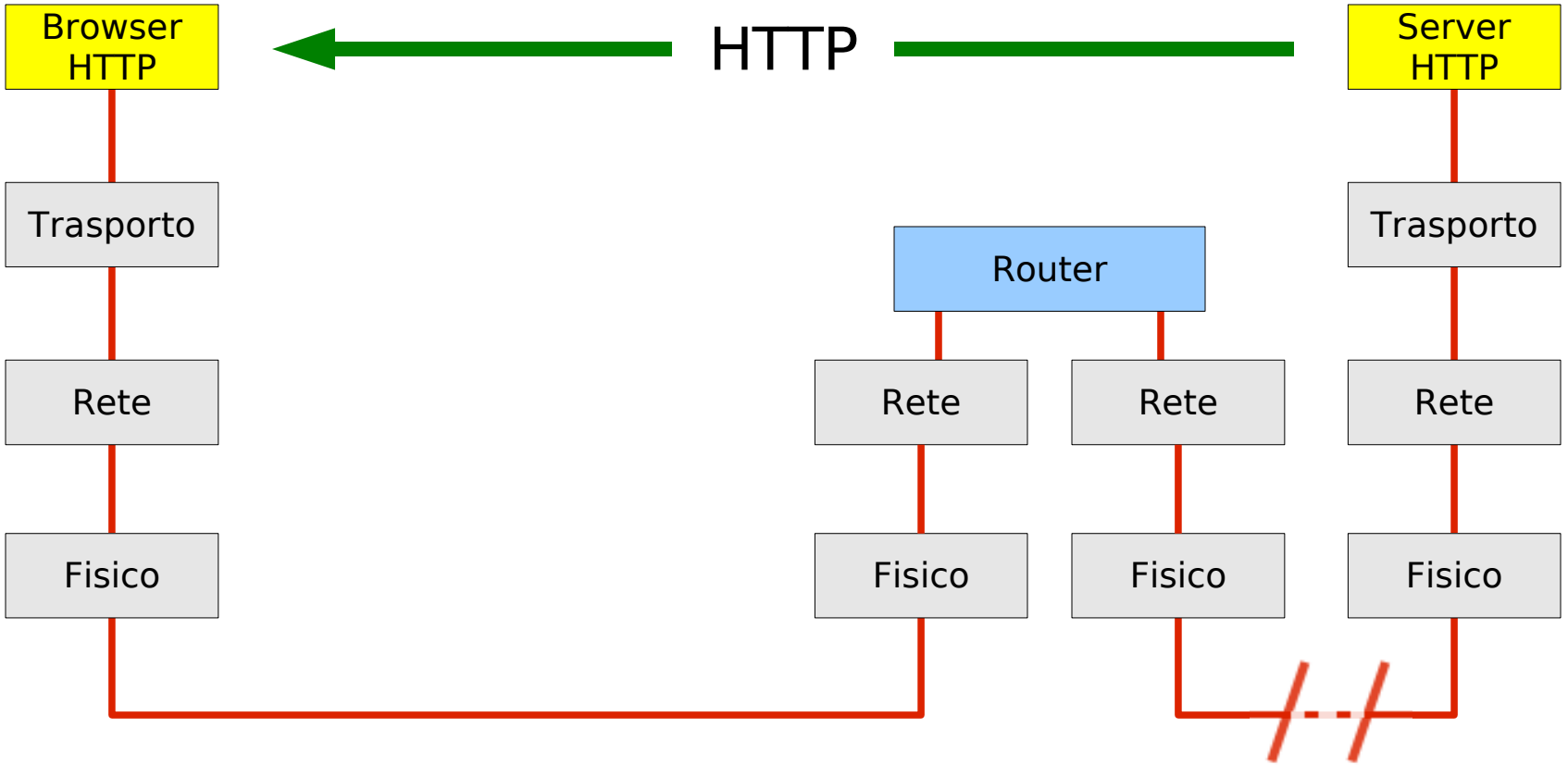


Connessione diretta

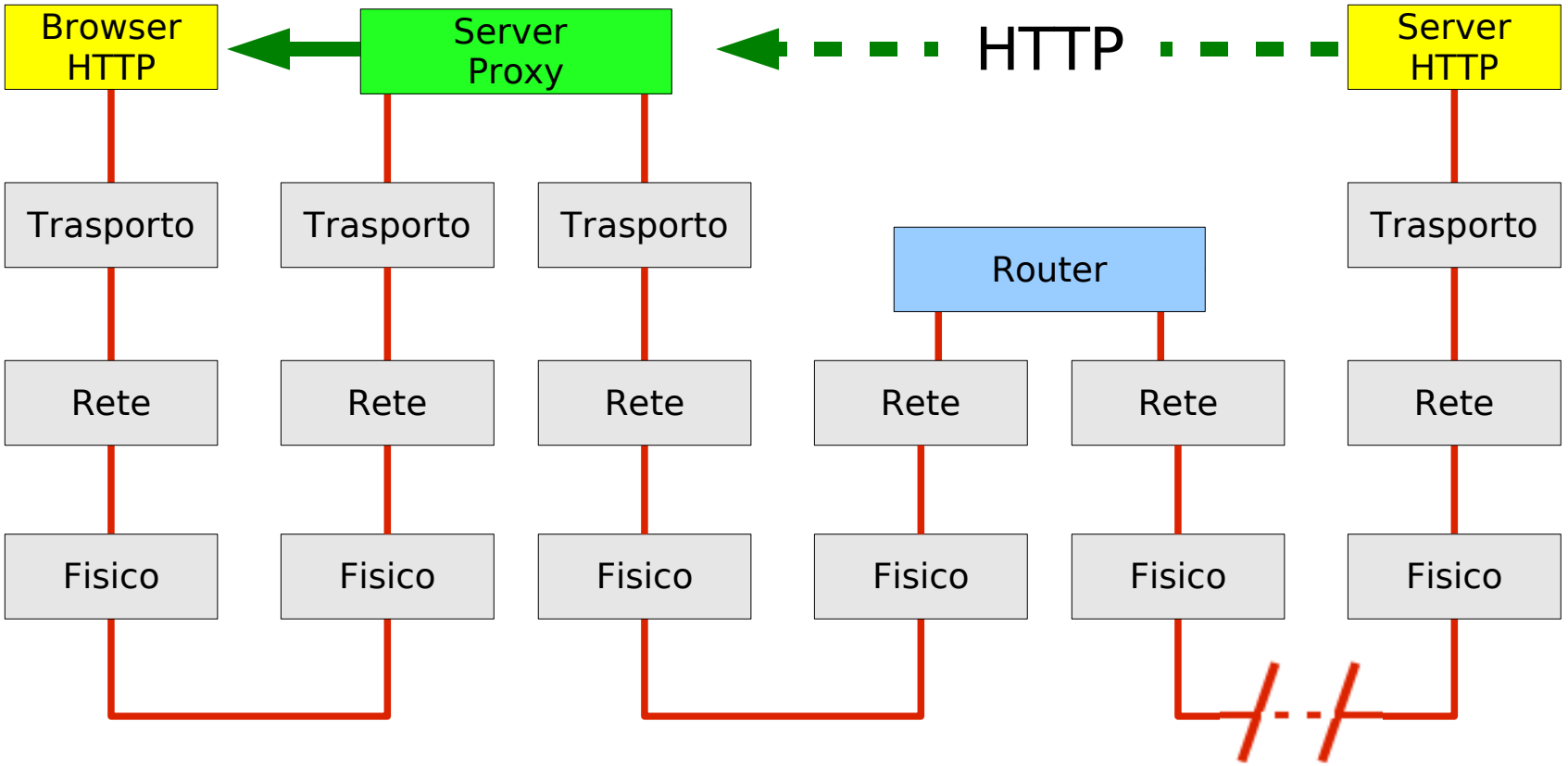


Connessione via proxy

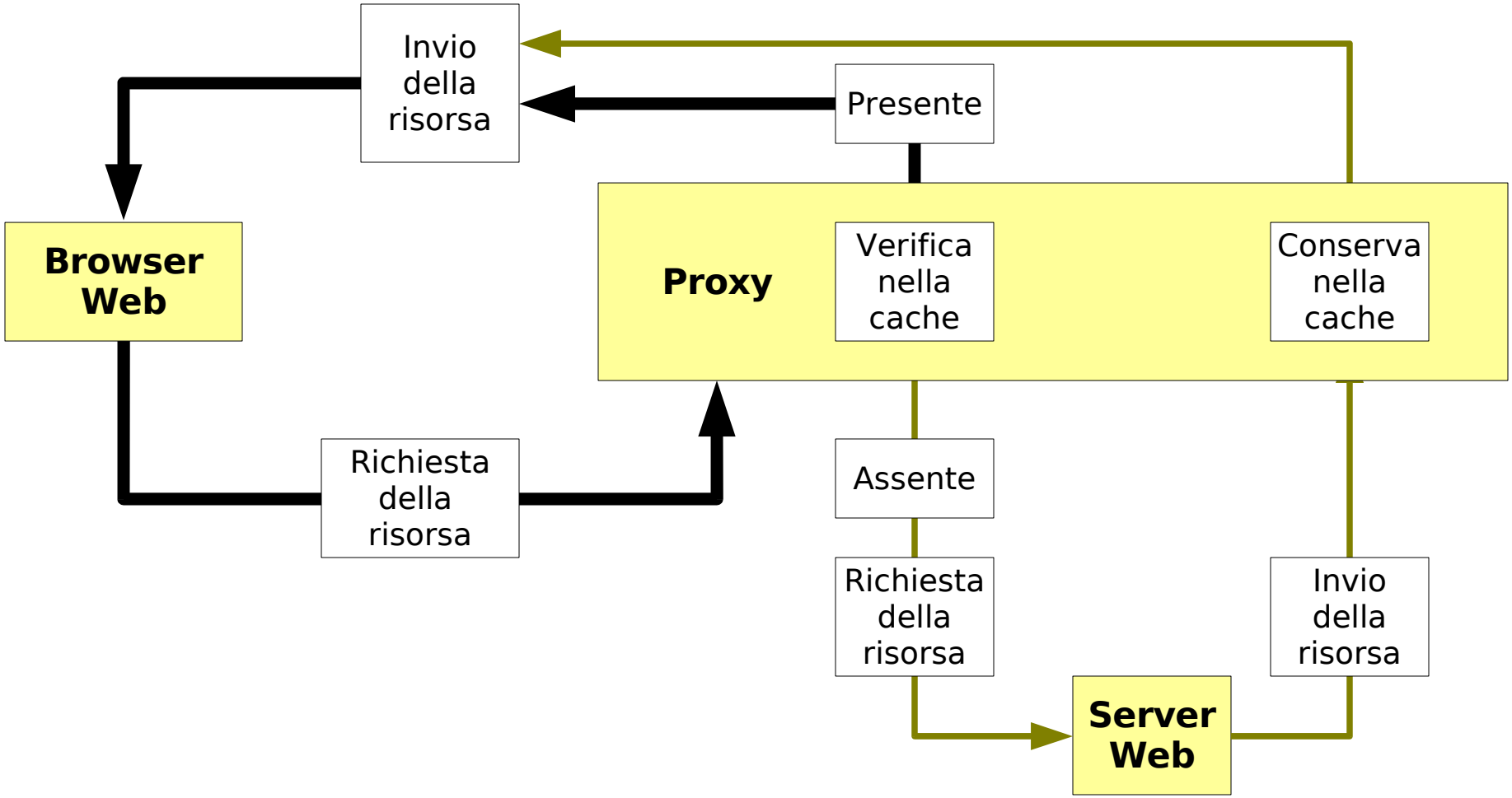
Architettura TCP/IP in una connessione diretta



Architettura TCP/IP in una connessione mediata dal proxy



Servizio HTTP offerto da un proxy



Funzionalità implementate	Accesso diretto	Accesso via proxy
Accessi multipli	Non sempre possibile	SI
Filtro delle utenze	NO	SI
Filtro dei contenuti	NO	SI
Decongestione del traffico in uscita	NO	SI
Controllo del traffico in uscita	NO	SI

Con un proxy è possibile:

- Condividere un'unica connessione fra più utenze
- Filtrare le utenze
- Filtrare i contenuti in download
- Liberare parte della banda di connessione disponibile
- Controllare il traffico in uscita grazie alla registrazione in un log

Squid

- E' il più noto e il più potente cache proxy nel panorama del software libero e open source.
- E' distribuito gratuitamente con licenza GNU General Public License
- Esiste un porting per sistemi Windows, ma espleta in pieno le sue potenzialità solo in un sistema GNU Linux soprattutto nell'integrazione con altri servizi di rete
- Supporta fra i principali protocolli HTTP e FTP
- Agisce come servizio in background sia su un server sia su una workstation
- E' di facile configurazione nelle funzionalità essenziali

DansGuardian

- E' un potente sistema di *content filtering* che migliora la policy di accesso di un proxy verificando le richieste su una banca dati pubblica, la ***blacklist***
- Se la richiesta non viola i vincoli impostati nella configurazione, DansGuardian la dirotta al proxy permettendo il download della risorsa
- La blacklist può essere scaricata da Internet e periodicamente aggiornata con un update automatico oppure con una procedura manuale

Dove reperirli

Squid

http://www.squid-cache.org

DansGuardian

http://dansguardian.org

Blacklist

http://urlblacklist.com/?sec=download (*)

(*) Disponibili diverse blacklist.

Installazione di Squid (Fase I)

Preparazione all'installazione

```
$ tar  xzvf squid-2.5.STABLE10.tar.gz
$ cd squid-2.5.STABLE10
$ less INSTALL
$ ./configure --help
```

Installazione indipendente dall'architettura (default)

Tutti i file saranno installati nella directory **/usr/local/squid** al cui interno saranno create le directory etc, bin, sbin, var, eccetera

```
$ ./configure
```

Installazione dipendente dall'architettura

Tutti i file saranno installati nella directory radice secondo lo standard unix (eseguibili in /bin e /sbin, file di configurazione in /etc, file di log in /var/log, eccetera

```
$ ./configure --prefix=/
```

Installazione di Squid (Fase II)

Compilazione

```
$ make
```

Installazione

```
$ su
password di root
# make install
```

Nelle prossime slide faremo riferimento all'installazione predefinita (architettura indipendente), con tutti i file di Squid posizionati in /usr/local/squid

Configurazione di Squid

L'installazione di Squid crea il file di configurazione generico

/usr/local/squid/etc/squid.conf

Il file va modificato togliendo i commenti o commentando le righe non necessarie e modificando gli argomenti delle direttive (o tag). Il numero di direttive da impostare dipende dal livello di personalizzazione che s'intende applicare al proxy

Sintassi

```
direttiva [argomenti]
```

1) Le righe vuote e gli spazi ripetuti sono ignorati
2) Le righe che iniziano con il carattere **#** sono trattate come commenti

Nell'esempio che segue Squid interpreterà solo le ultime due righe

```
# TAG: no_cache
# Lista di direttive ACL. Se collegate impongono che la richiesta non sia
# conservata nella cache. In altri termini, le richieste che rientrano nelle
# direttive ACL impostate con il parametro 'deny' saranno soddisfatte prelevando
# la risorsa dal Web e non dalla cache
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

Esempio di squid.conf

```
# Indirizzo IP e porta d'ascolto
http_port 192.168.10.1:3128

# Pagine Web dinamiche da non memorizzare nella cache
acl CGI urlpath_regex cgi-bin \?
acl ASP urlpath_regex asp \?
acl PHP urlpath_regex php \?
acl JSP urlpath_regex jsp \?
no_cache deny CGI ASP PHP JSP

# Dimensioni massime e minime delle risorse da memorizzare
maximum object size 10240 KB
minimum_object_size 10 KB

# individuazione delle reti da trattare nelle direttive d'accesso
acl all src 0.0.0.0/0.0.0.0
acl localnet src 192.168.10.0/255.255.255.0
acl localnet src 192.168.11.1-192.168.11.20/255.255.255.255
acl localhost src 127.0.0.1/255.255.255.255
acl manager proto cache_object
```

Esempio di squid.conf (continuazione)

```
# Definizione dei metodi di connessione trattati nelle direttive d'accesso
acl CONNECT method CONNECT

# Definizione delle porte TCP trattate nelle direttive d'accesso
acl SSL_ports  port 443 563
acl Safe_ports port 80                      # http
acl Safe_ports port 21                      # ftp
acl Safe_ports port 443 563                 # https, snews
acl Safe_ports port 70                      # gopher
acl Safe_ports port 210                     # wais
acl Safe_ports port 1025-65535              # unregistered ports
acl Safe_ports port 280                     # http-mgmt
acl Safe_ports port 488                     # gss-http
acl Safe_ports port 591                     # filemaker
acl Safe_ports port 777                     # multilink http
acl Safe_ports port 901                     # SWAT

# Definizione delle estensioni dei file trattai nelle direttive di accesso
acl banna_mp3 url_regex -i  \.mp3$   # per identificare i file mp3
acl banna_exe url_regex -i  \.exe$   # per identificare eseguibili per Windows
```

Esempio di squid.conf (continuazione)

```
# Definizione di un file di testo contenente una lista di espressioni regolari
acl forbidden url_regex "/usr/local/squid/etc/forbidden.txt"

# Direttive d'accesso (http_access): definiscono le regole di accesso al proxy
http_access allow manager localhost  # accesso locale in amministrazione
http_access deny manager             # nega l'accesso remoto in amministrazione
http_access deny !Safe_ports         # nega l'accesso alle porte non standard
http_access deny CONNECT !SSL_ports  # tuneling SSL solo sulle porte SSL
http_access deny banna_mp3           # nega l'accesso ai file mp3
http_access deny banna_exe           # nega l'accesso agli eseguibili Windows
http_access deny forbidden           # nega l'accesso alle chiavi in forbidden
http_access allow localnet           # permette l'accesso dalle reti locali
http_access allow localhost          # permette l'accesso dal loopback

# Accesso non consentito a tutti gli altri host
# Questa direttiva l'ultimo tag http_access
http_access deny all
```

Avvio di Squid

L'avvio del servizio si effettua avviando come root il binario squid

```
# /usr/local/squid/sbin/squid [opzioni]
```

Un elenco delle opzioni si ottiene digitando il comando con l'opzione **-h**

In questa sede concentriamo l'attenzione sulle seguenti opzioni:

-h : stampa sullo schermo l'elenco delle opzioni disponibili e una breve descrizione

-k reconfigure : riavvia Squid facendo rileggere la configurazione (da eseguire ogni volta che si modifica il file squid.conf)

-k check : verifica il funzionamento di Squid e la correttezza del file di configurazione

-D : avvia Squid disabilitando il controllo iniziale del DNS. Questa opzione può essere utile in caso di problemi quando si avvia Squid le prime volte

-z : opzione necessaria per l'avvio di Squid per la prima volta. Squid costruirà l'albero delle directory swap in [prefix]/var/cache

Verifica dell'esecuzione

Per verificare se il cache proxy è in esecuzione si può ricorrere al comando

```
$ pstree -p
```

Il comando stampa sullo schermo l'albero dei processi in esecuzione fra i quali dovremo trovare i riferimenti a Squid e ai due processi figli:

```
|-scsi_eh_1(1623)
|-squid(1446)---squid(1448)---unlinkd(1450)
|-syslogd(78)
|-udevd(175)
```

Se Squid o i suoi processi figli non sono in esecuzione, il processo è stato abortito per qualche errore. La causa dell'errore si accerta consultando i file di log con i comandi

```
$ tail /usr/local/squid/var/logs/cache.log

$ tail /var/log/syslog
```

Problemi di avvio

```
Nov  7 23:17:37 gian (squid): ipcache_init: DNS name lookup tests
failed
```

Causa

All'avvio Squid effettua un test della risoluzione dei nomi di dominio interrogando i DNS sui nomi elencati nella direttiva **dns_testnames**. Questa operazione fallisce se il Server DNS a cui si appoggia Squid non riesce a risolvere uno dei nomi oppure se il server di connessione non è collegato ad Internet

Soluzione:

Avviare squid con l'opzione -D

```
# /usr/local/squid/sbin/squid -D
```

Problemi di avvio

```
Nov  7 23:49:56 gian (squid): Cannot open
'/usr/local/squid/var/logs/access.log' for writing. ^IThe parent
directory must be writeable by the ^Iuser 'nobody', which is the
cache_effective_user ^Iset in squid.conf.
```

Causa

Per default il processo squid è avviato come utente nobody e non ha i privilegi di scrittura nelle directory di sistema (nella fattispecie /usr/local).
Squid non può pertanto inizializzare il sistema di cache proxy (creazione dei file di log e dell'albero delle directory swap)

Soluzione:

La soluzione più semplice consiste nell'assegnare la proprietà della directory /usr/local/squid/var all'utente nobody (l'operazione deve essere eseguita da root)

```
# chown -R nobody:nogroup /usr/local/squid/var
```

Problemi di avvio

```
Nov  8 00:12:16 gian (squid): ^IFailed to verify one of the swap
directories. Check cache.log ^Ifor details.  Run 'squid -z' to
create swap directories ^Iif needed, or if running Squid for the
first time.
```

Causa

All'avvio Squid verifica l'esistenza dell'albero delle directory swap in /usr/local/squid/var/cache. Se si avvia Squid per la prima volta, l'albero swap deve essere inizializzata

Soluzione:

Usare l'opzione -z quando si avvia Squid per la prima volta

```
# /usr/local/squid/sbin/squid -zD
```

Proxy caching avanzato: il *filtering* con DansGuardian

Nelle reti scolastiche è fondamentale applicare un sistema di *filtering*, intendendo con questo termine un insieme di funzionalità intrinseche o estese che permettono di amministrare gli accessi al Web differenziando le regole d'accesso in relazione al tipo di utenza, all'orario in cui si chiede l'accesso, alla funzione specifica dei client

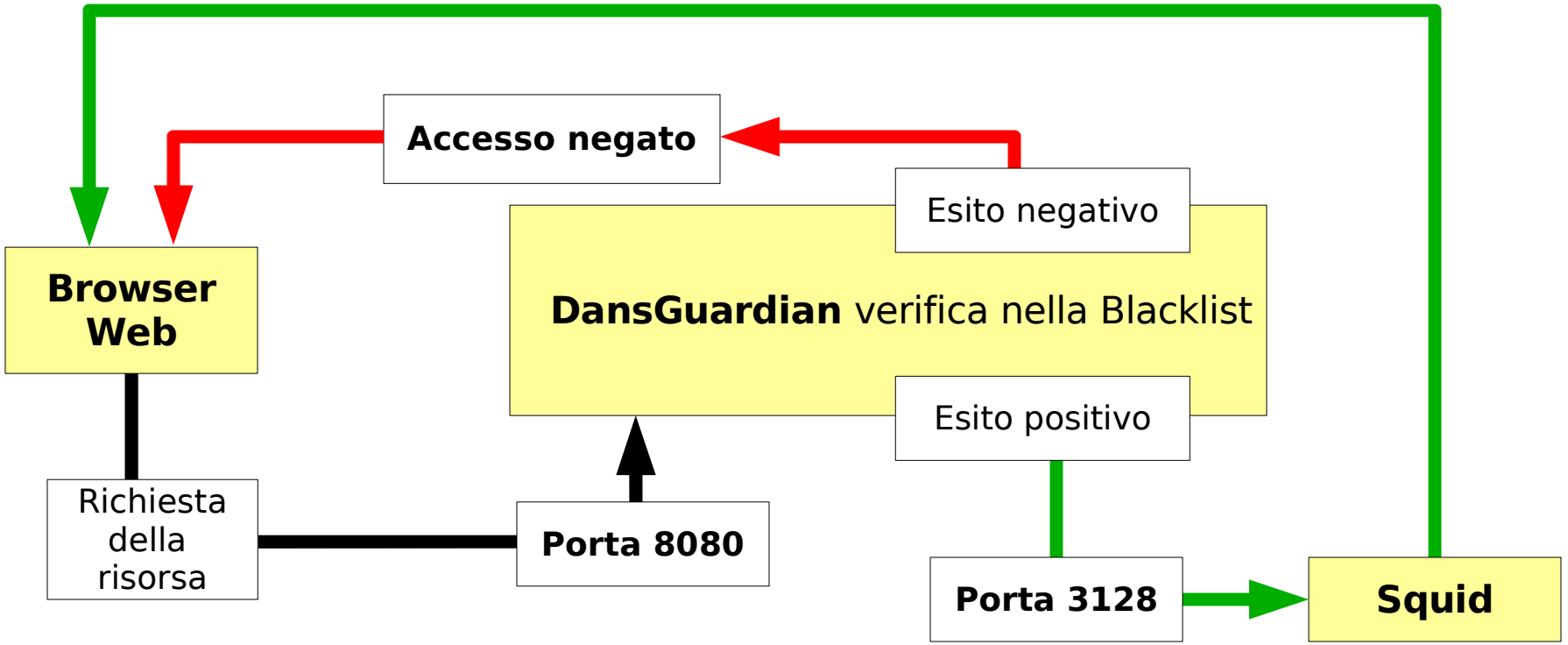
Squid supporta di per sé alcune di queste funzionalità in modo intrinseco, tuttavia può essere implementato associando il suo servizio ad altri servizi accessori:

- autenticazione degli utenti (es. Squid+MySQL): permette di associare il servizio ad un database degli utenti per differenziare la policy in funzione del tipo di utenza
- un servizio antivirus (es. Squid+DansGuardian+ClamAv): permette di filtrare i contenuti controllando la presenza di virus allo scopo di proteggere i client Windows della rete scolastica
- un servizio di *filtering* dei contenuti (es. Squid+DansGuardian): permette di filtrare i contenuti controllando la liceità delle risorse richieste dai client

In questa sede vedremo come installare uno dei più celebri sistemi di filtering dei contenuti Web: DansGuardian

Come opera DansGuardian

DansGuardian s'interpone fra il client e il proxy restando in ascolto per le richieste dei client e verifica nella blacklist se la richiesta è conforme alle direttive impostate. Se la richiesta è approvata la rendirizza al proxy vero e proprio, in caso contrario invia al client una pagina di accesso negato secondo le impostazioni della configurazione



Installazione di DansGuardian

Preparazione all'installazione

```
$ tar  xzvf dansguardian-2.8.0.6.source.tar.gz
$ cd dansguardian-2.8.0.6
$ less INSTALL
$ ./configure --help
```

Configurazione dell'installazione

Tutti i file saranno installati nella directory radice secondo lo standard Unix (eseguibile in /usr/sbin, file di configurazione in /etc/dansguardian, log in /var/log/dansguardian, eccetera

```
$ ./configure
```

Compilazione

```
$ make
```

Installazione

```
$ su
password di root
# make install
```

Configurazione di DansGuardian

L'installazione di DansGuardian crea il file di configurazione generico

/etc/dansguardian/dansguardian.conf

Il file va modificato adattando i valori impostati nelle direttive al contesto in cui si opera. Come già visto per squid.conf abbiamo già una configurazione predefinita, tuttavia può essere necessario personalizzare in vario modo la configurazione di DansGuardian

Sintassi

```
direttiva = [valore]
```

1) Le righe vuote e gli spazi ripetuti sono ignorati
2) Le righe che iniziano con il carattere **#** sono trattate come commenti

La configurazione di DansGuardian contempla una vasta casistica che non è possibile trattare in questa sede. Ci limitiamo pertanto all'esame di alcune impostazioni

Esempio di dansguardian.conf

Nell'esempio sono state omesse diverse direttive per concentrare l'attenzione su quelle che possono maggiormente interessare un'installazione di prova. Per ciò che non è contemplato in questo esempio si raccomanda di lasciare invariata la direttiva predefinita impostata dall'installazione di DansGuardian

```
# Azione eseguita da Dansguardian in caso di accesso negato
reportinglevel = 3

# Directory dei file HTML restituiti in caso di accesso negato
languagedir = '/etc/dansguardian/languages'

# Lingua utilizzata dalla directory languagedir (default: ukenglish)
language = 'italian'

# Formato del file di log
# L'opzione 3 imposta lo stesso formato del file access.log di Squid
logfileformat = 1

# Percorso del file di log
loglocation = '/var/log/dansguardian/access.log'
```

dansguardian.conf.... continuazione

```
# Indirizzo IP di DansGuardian
reportinglevel = 192.168.10.1

# Porta sulla quale DansGuardian resta in ascolto
filterport = 8080

# Indirizzo IP del proxy server (Squid). Per default è impostato il loopback
# con l'ipotesi che DansGuardian e Squid operino sullo stesso host. In
# alternativa impostare l'indirizzo del server di connessione
proxyip = 127.0.0.1

# Porta sulla quale il proxy resta in ascolto
proxyport = 3128

# URL di reindirizzamento se l'accesso negato reindirizza ad un CGI
# Lasciare l'impostazione di default se si usa il template statico
accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-bin/dansguardian.pl'

# Metodo di ponderazione delle pagine (il valore predefinito 2 fa sì che una
# frase venga conteggiata una sola volta se riscontrata nella pagina)
weightedphrasemode = 2
```

dansguardian.conf.... continuazione

```
# Creazione di una cache dei file e delle URI negate. L'impostazione
# predefinita (on) permette di triplicare la velocità del processo di
# scansione, pertanto è raccomandata se DansGuardian è in esecuzione su un
# computer lento
createlistcachefiles = on
```

Come già detto, diverse direttive sono state omesse.
In generale vanno usate per ottimizzare il funzionamento di DansGuardian adattandolo ad uno specifico contesto (es. differenziazione degli eventi in un sistema basato sull'autenticazione degli utenti).

E' consigliabile lasciare le impostazioni predefinite, soprattutto se non si ha cognizione di causa, e rimandare ad un secondo tempo l'implementazione della configurazione dopo aver acquisito un'adeguata esperienza.

In ogni caso, dopo aver impostato le direttive essenziali (es. indirizzi IP e porte di ascolto) DansGuardian è in grado di operare efficacemente anche con le impostazioni di default nella maggior parte dei contesti

Blacklist

La blacklist è il punto di forza dei servizi di filtering, che usano vere e proprie banche dati che riportano domini, indirizzi IP, URI ed espressioni regolari. Molte di queste banche dati sono aggiornate con una certa frequenza settimanale adattando la loro funzione al dinamismo della rete Internet.

Con un motore di ricerca possiamo reperire differenti blacklist libere o commerciali. La scelta può dipendere da vari fattori: l'esperienza del sistemista, l'affidabilità e il grado di completezza della blacklist, la frequenza di aggiornamento, il costo del servizio.

Un tutorial su Sistemistiindipendenti.org consiglia una specifica blacklist: oltre ad essere una corposa banca dati (oltre 20 MB), ha il vantaggio di includere un numero elevato di siti italiani, che in generale sono più facilmente raggiungibili dalle nostre reti scolastiche con una navigazione che si affida ai link associati ai banner pubblicitari dei portali in lingua italiana.

http://urlblacklist.com/?sec=download

http://urlblacklist.com/cgi-bin/commercialdownload.pl?type=information&file=bigblacklist

Installazione della blacklist

L'installazione si effettua scaricando l'archivio compresso nella directory /etc/dansguardian e scompattandolo con il comando tar
(operazione da eseguire come superutente)

```
# tar xzvf bigblacklist.tar.gz
```

L'operazione crea una directory contenente gli archivi sotto forma di file di testo (urls e domains) organizzati in directory secondo la categoria

La lista nera della banca dati si aggiunge alla funzione di ricerca, nelle pagine richieste, delle frasi significative eseguita da DansGuardian in base alla configurazione delle espressioni riportate nei file della directory /etc/dansguardian/phraselists, fornendo un sistema di filtering in grado di bloccare un altissimo numero di pagine non adatte ad una rete scolastica.

Per fruire della blacklist è necessario configurare DansGuardian specificando per quali categorie della blacklist deve essere attivato il filtro

Abilitazione delle categorie

L'abilitazione delle categorie si effettua configurando alcuni file contenuti nella directory **/etc/**dansguardian, in particolare i file **bannedsitelist** (relativo ai domini) e **bannedulrllist**. Questi file sono predisposti per l'inclusione di tutte le categorie, è sufficiente rimuovere il carattere di commento **#**.

Ad esempio, togliendo il commento alla seguente direttiva (in bannedsitelist), DansGuardian bloccherà tutti i domini elencati nel file domains contenuto in /etc/dansguardian/blacklists/warez

```
.Include</etc/dansguardian/blacklists/warez/domains>
```

E' possibile aggiungere nei suddetti file di configurazione altri indirizzi e altri domini non contemplati nella blacklist, indicando esclusivamente il dominio senza il www e senza http://. Ad esempio, per bloccare il dominio **http://www.pippo.it** si aggiunge in bannedsitelist la direttiva

```
pippo.it
```

Configurazione, c'è altro?

Una trattazione approfondita sulla configurazione di DansGuardian non può essere fatta in questa sede: questo sistema di filtering si adatta ad un ampio spettro di situazioni permettendo un livello di personalizzazione piuttosto spinto in grado di impostare un efficiente sistema di filtering adatto agli scopi di una scuola dell'infanzia (pornografia, pedofilia, chat) o di un istituto superiore ad indirizzo informatico (pornografia, warez, hacking, proxy anonimo).

Per rendersi conto delle potenziali configurazioni che DansGuardian prevede è sufficiente leggere il contenuto dei file di configurazione contenuti nella directory /etc/dansguardian. Si tratta di file di configurazione che sono applicati a cascata come estensioni del file principale (dansguardian.conf).

La modifica delle impostazioni può essere fatta agevolmente rimuovendo o applicando i caratteri di commento alle direttive già predisposte, oppure modificando il loro contenuto in funzione delle esigenze specifiche.

Con un po' di esperienza si potrà implementare il sistema di filtering con una configurazione ad hoc in grado di far dormire fra due guanciali sia il sysadmin sia il dirigente scolastico.

Avvio di DansGuardian

L'avvio del servizio si effettua mandando in esecuzione il binario dansguardian, che nell'installazione di default è posizionato nella directory /usr/sbin.
L'avvio deve essere fatto dall'utente root

```
# /usr/sbin/dansguardian
```

A questo punto, dopo aver configurato il browser Web per l'accesso al proxy attraverso DansGuardian (vedi slide successive) si può testare il funzionamento del sistema di filtering provando l'accesso a qualche sito vietato

Se il sistema è in esecuzione e correttamente configurato DansGuardian restituisce una pagina di accesso negato nella lingua impostata


DansGuardian - Accesso Negato - Mozilla Firefox
File Modifica Visualizza Vai Segnalibri Strumenti ?
http://www.playboy.com/
mozilla.org GULCh Seminario Appunti Linux NFS varie Mozilla Update NIS Squid Shell POSIX
L'ACCESSO E' STATO NEGATO -
L'accesso alla pagina:
http://www.playboy.com
... e' stato negato per il seguente motivo:
Sito vietato: playboy.com
Stai vedendo questo errore perche' la pagina che hai cercato di accedere contiene, o e' marcata come contenente, materiale che e' stato ritenuto non appropriato.
Se hai ulteriori domande, contatta il tuo coordinatore ICT o Network Manager.
Powered by DansGuardian
Completato
Inizio
Sali
AdBlock

Avvio automatico dei servizi di proxy cache e di content filtering

Come per tutti i servizi di rete che operano in background è utile avviare Squid e DansGuardian come demoni all'avvio del sistema, specie nei casi in cui il server di connessione viene riavviato ogni giorno.

Dopo aver verificato che i servizi sono correttamente installati e configurati e che funzionano regolarmente, è opportuno costruire gli script di avvio e inserirli nella directory di inizializzazione che secondo la distribuzione usata è **/etc/init.d** oppure **/etc/rc.d** oppure **/etc/rc.d/init.d**

A parte gli script, che sono basati sulla sintassi e la semantica standard della Shell Bourne, si faccia riferimento alla documentazione della distribuzione usata per sapere come avviare automaticamente gli script di inizializzazione.

A titolo d'esempio descrivo la procedura per l'avvio in una Slackware: dopo aver realizzato gli script, questi vanno posizionati nella directory **/etc/rc.d**, dopo di che si può modificare lo script **/etc/rc.M** inserendo i comandi di avvio degli script di inizializzazione di Squid e DansGuardian.

Slackware: chiamata degli script di avvio dallo script di inizializzazione

Inserire nel file /etc/rc.d/rc.M il seguente codice. Si consiglia di inserirlo dopo la chiamata ad altri servizi di rete eventualmente installati sul server di connessione (es. configurazione della connessione con il DHCP)

```
# Start Squid
if [ -x /etc/rc.d/rc.squid ]; then
  . /etc/rc.d/rc.squid start
fi

# Start DansGuardian
if [ -x /etc/rc.d/rc.dansguardian ]; then
  . /etc/rc.d/rc.dansguardian start
fi
```

Script di avvio di Squid

Aprire un editor di testo e trascrivere il seguente codice

```
#!/bin/sh
PREFIX=/usr/local/squid/sbin/
case "$1" in
start)
       if [ -f ${PREFIX}squid ]; then
          echo "Avvio di Squid Proxy Cache"
               ${PREFIX}squid -D
       fi
        ;;
stop)
       if ${PREFIX}squid -q 2> /dev/null; then
          echo "Arresto di Squid Proxy Cache"
               ${PREFIX}squid -k shutdown
          fi
        ;;
restart)
       $0 stop
       $0 start
       ;;
*)
       echo "Usa: $0 {start|stop|restart}" >&2
       ;;
esac
```

Script di avvio di Squid

Salvare il file nella directory con il nome rc.squid,
acquisire il privilegio di root e spostarlo nella directory /etc/rc.d.
Infine rendere eseguibile lo script con il comando

```
# chmod a+x /etc/rc.d/rc.squid
```

Script di avvio di DansGuardian

Nei sorgenti di DansGuardian è già predisposto uno script di avvio, **dansguardian.sysv**, posizionato nella directory radice dei sorgenti. E' perciò sufficiente copiarlo nella directory /etc/rc.d rinominandolo (in accordo con quanto impostato negli esempi precedenti) come rc.dansguardian

```
# cp -v [SOURCE_DIR]dansguardian.sysv /etc/rc.d/rc.dansguardian

# chmod a+x /etc/rc.d/rc.dansguardian
```

Naturalmente se l'installazione di DansGuardian si discosta da quella predefinita è necessario modificare il file rc.dansguardian attribuendo il valore corretto alle variabili CONFFILELOCATION e BINARYLOCATION, che indicano le directory in cui sono posizionati rispettivamente il file di configurazione dansguardian.conf e l'eseguibile dansguardian

Configurazione dei client

Sui client si dovrà impostare la connessione ad un proxy.
Questa operazione di norma si esegue sulle impostazioni del browser, perciò si rimanda alla guida del browser utilizzato sulla procedura da seguire, che in ogni caso è semplicissima.

Per impostare la connessione al proxy sarà necessario:
1. Specificare l'accesso al proxy per i protocolli HTTP e FTP
2. Specificare l'indirizzo IP del server di connessione
3. Specificare la porta di ascolto di DansGuardian (default: 8080) oppure, se non si è installato il sistema di filtering, quella di Squid (default: 3128)

Per ragioni di sicurezza è opportuno che sia prevenuta la possibilità che chiunque possa impostare il browser per accedere direttamente a Squid aggirando DansGuardian.
Questa eventualità è possibile se per ragioni di operatività la configurazione di Squid prevede l'accesso dai client della LAN (oltre che dal loopback) e non si sia predisposto un sistema di autenticazione degli utenti.
In questo caso non sarebbe male impostare una porta d'ascolto di Squid differente da quella di default e mantenerla segreta.

Consultiamo i log!!!

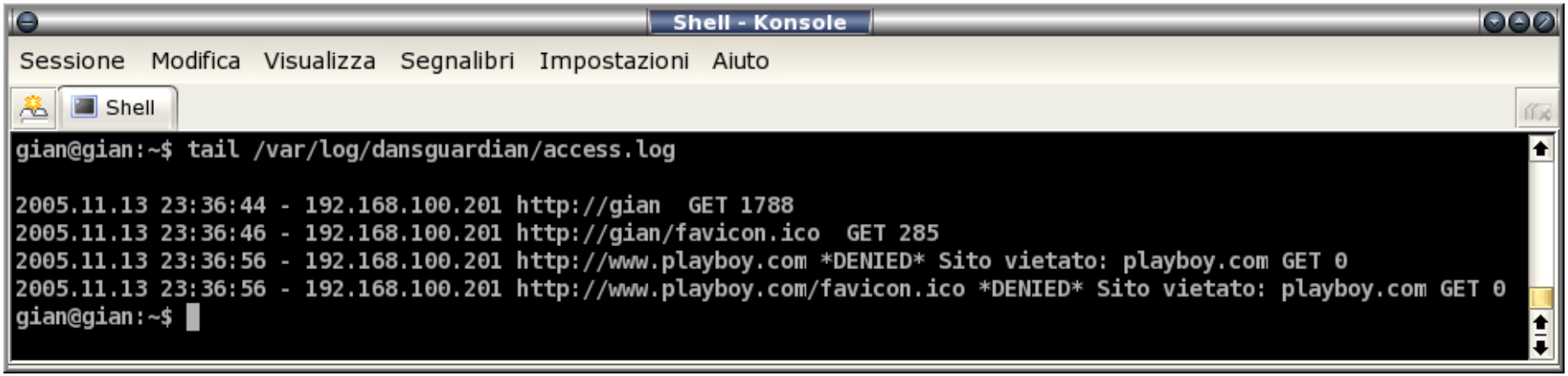
A prescindere da ogni considerazione relativa alla privacy (in ogni modo da prendere con riserva nell'ambito di una rete scolastica), il sysadmin coscienzioso consulta sempre i log per verificare se un servizio di rete funziona regolarmente, per accertare le eventuali violazioni di policy, per accertare l'esistenza di falle di sistema.

Per DansGuardian e Squid l'esame dei log è fondamentale soprattutto all'inizio per vari motivi.
In particolare, DansGuardian è un sistema di filtering sofisticato e la configurazione corrente va adattata *in itinere* proprio sulla base dei risultati ottenuti dai log nei primi tempi. In questo modo si potrà valutare la necessità di potenziare i vincoli della policy aggiungendo categorie o indirizzi non compresi nella blacklist, oppure adattando alcuni filtri che per qualche motivo bloccano l'accesso a siti utili.

Un solo esempio può darci un'idea sulla necessità di consultare i log: impostando un numero di pesi basso nella ricerca delle espressioni regolari si corre il rischio di bloccare una pagina che tratta dell'anatomia e della fisiologia dell'apparato genitale perché DansGuardian lo interpreta come una pagina dai contenuti pornografici. In questo caso si corregge la configurazione inserendo il sito nella lista delle eccezioni.

L'access.log di DansGuardian

Nell'installazione di default, il log degli accessi di DansGuardian si trova nella directory /var/log/dansguardian. Il file di log di DansGuardian può essere letto da una console con il comando tail usando l'opzione -x dove x è il numero degli ultimi x eventi

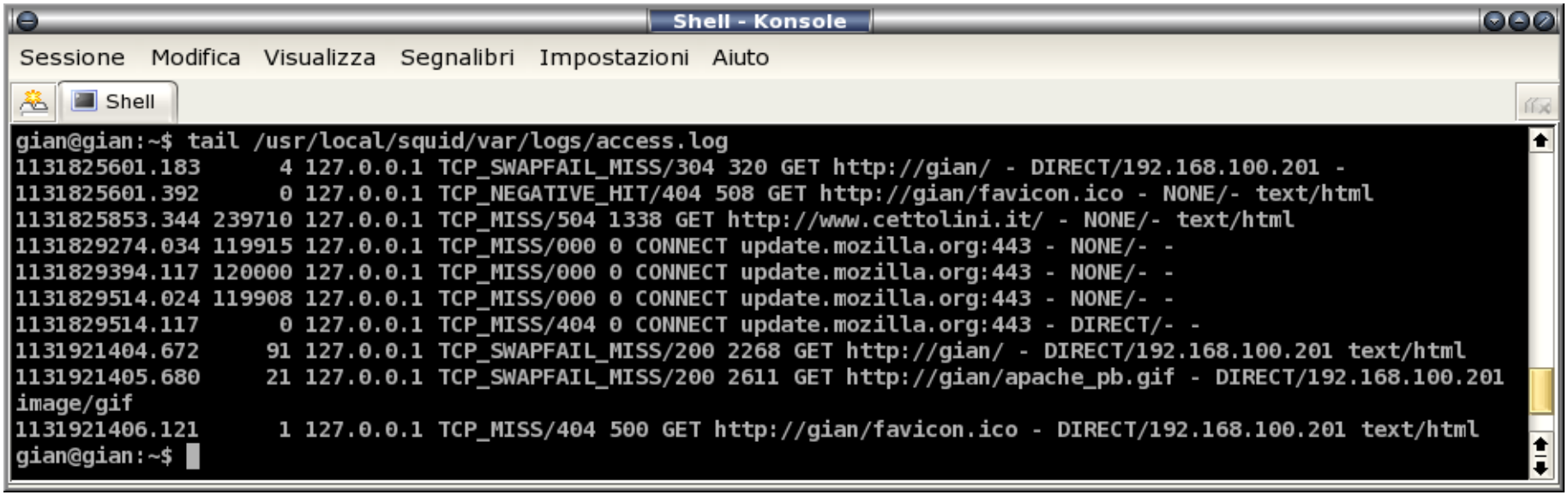


DansGuardian registra sul log l'evento e anche il motivo del blocco (nell'esempio si tratta di un sito segnalato nella blacklist). In questo modo l'amministratore ha anche le informazioni necessarie per poter apportare eventuali modifiche alla configurazione.

In rete sono in ogni caso disponibili strumenti di amministrazione che possono essere utilizzati per la lettura e l'analisi del log in modo più agevole rispetto a tail.

L'access.log di Squid

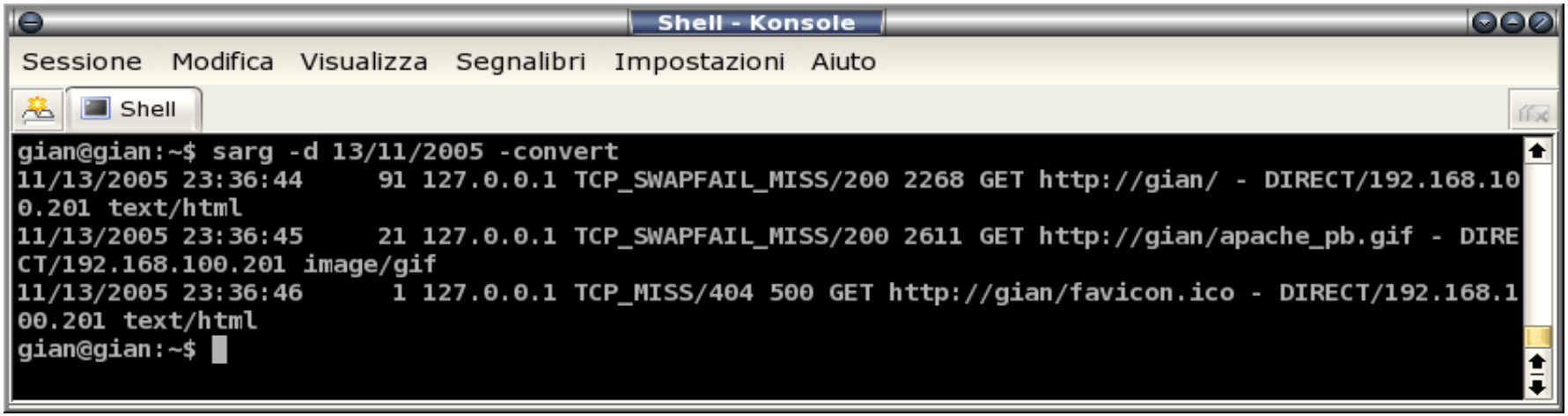
Il log degli accessi di Squid, nell'installazione predefinita, si trova invece nella directory /usr/local/squid/var/logs. Anche in questo caso si può ricorrere al comando tail per la lettura degli eventi



Come si può osservare, il formato del log degli accessi di Squid è tale da non rendere agevole la lettura immediata: l'ora e la data dell'evento sono registrate in un formato codificato perciò in questo caso è consigliabile utilizzare un analizzatore di log per ottenere nell'output la data e l'ora degli accessi in un formato leggibile.

L'access.log di Squid con Sarg

Un valido strumento per leggere i logo di Squid è **Sarg**, un altro progetto libero disponibile sul sito **http://sarg.sourceforge.net**. Sarg può essere usato per leggere da una comoda interfaccia HTML i log degli accessi di Squid e dei due content filtering più noti, SquidGuard e DansGuardian. Tralasciando la procedura d'installazione e configurazione, limitiamoci ad un semplice comando che dalla console ci permette di leggere il log degli accessi di Squid convertendo la data in un formato accessibile:



Come si può osservare, è possibile leggere gli eventi a partire da un determinato momento (opzione -d gg/mm/aaaa) e con data e ora in un formato leggibile (opzione -convert)

Un caso pratico:

L'IPSAA (*) “Cettolini” di Cagliari Scuola associata di Villacidro

(*)
Istituto Professionale Statale per l'Agricoltura e l'Ambiente

Il contesto

La nostra è una piccola scuola (attualmente circa 50 iscritti) in linea di massima composta da studenti abbastanza responsabili. Non ci sono pertanto grossi problemi di violazione della policy

- La scuola è cablata dal 2002
- Dispone di un accesso ad Internet da una sola postazione con connessione satellitare bidirezionale (ex Tiscalisat, ora gestita da Digiweb) condivisibile solo per mezzo di un proxy
- Dispone di un'aula MARTE (*) priva di connessione, utilizzata raramente per le scarse funzionalità offerte in quanto le direttive del progetto MARTE impongono la separazione fisica della rete MARTE dalle altre reti scolastiche
- Dispone di una piccola rete di workstation basata su piattaforma mista (Windows e Linux) con una significativa migrazione verso il software libero nel 2005
- Uso frequente della connessione al Web (pressoché quotidiano), principalmente basato sulla libera navigazione

(*) MARTE=Moduli di Apprendimento su Rete Tecno-Educativa
Progetto (in fase operativa) di interconnessione in una Intranet regionale di oltre 500 aule multimediali. Workstation e servizi di rete sono basati esclusivamente su piattaforma Microsoft

Configurazione iniziale

(dalla fine del 2002 alla fine del 2004)

- Rete prevalentemente Windows 98
- Alcuni sistemi configurati con GNU Linux in dual boot comunque poco usato
- Connessione Tiscalisat tramite modem satellitare con gestione basata su software compatibile solo con sistemi Windows
- Server di connessione Windows 2000 Server (licenza per 10 client)
- Proxy: Wingate (commerciale, licenza per 29 client)
- Protezione: Norton Antivirus (commerciale) e Sygate Firewall (freeware)
- Browser: Mozilla e Mozilla Firefox

Problemi:

- Non facile controllo di virus e worm sul server
- Frequenti tentativi di attacco (portscanner rilevati dal firewall)
- Frequenti accessi al proxy dall'esterno a causa della non facile configurazione
- Difficoltà di conservare i log degli accessi
- Nessun filtro dei contenuti

Note positive:

- Comportamento responsabile degli studenti: il numero di richieste non conformi alla policy era contenuto entro limiti fisiologici

Configurazione intermedia
(fino alla primavera del 2005)

Eventi:
- Sostituzione (fortuita ma felice) di Wingate con Squid per Windows
- Sostituzione di Norton Antivirus con ClamAV (GNU GPL)
- Migliore configurazione del firewall

Problemi:
- Stessi problemi legati all'uso di un server Windows
- Impossibilità d'impostare un servizio di filtering dei contenuti

Note positive:
- Facilità di configurazione del proxy
- Risoluzione del problema relativo agli accessi al proxy dall'esterno
- Conservazione del log degli accessi
- Miglioramento della sicurezza sul server
- Riduzione delle violazioni alla policy grazie ad un controllo più agevole dei log

Configurazione attuale
(in evoluzione dalla primavera del 2005)

Eventi:
- Passaggio dall'ISP Tiscali all'ISP Digiweb, incremento della banda, connessione satellitare bidirezionale basata su protocolli standard e compatibili con GNU Linux
- Acquisto di nuove macchine server e client senza licenze Windows
- Installazione di Slackware Linux sia sui client sia sui server (principale e server di connessione)

Problemi:
- Lento adattamento alla migrazione su Linux
- Difficoltà d'impostazione di un efficace filtering dei contenuti basato solo su Squid (ora risolto con l'installazione di DansGuardian)

Note positive:
- Uso prevalente di software libero
- Reazione positiva degli alunni (un po' meno dei docenti)
- Risolti tutti i problemi di sicurezza: il server di connessione resta costantemente acceso senza alcun problema di sicurezza
- Minor carico di lavoro nell'amministrazione della rete

Conclusioni

1. Cache proxy e Web Content filtering sono strumenti che migliorano la fruibilità della connessione al Web in una rete scolastica favorendo la libera navigazione senza violare i requisiti che deve rispettare una scuola nella sua funzione educativa e alleggerendo l'onere di vigilanza che grava sui singoli insegnanti

2. Gli strumenti disponibili per queste funzionalità nell'ambito del software proprietario(es. Windows 2003 Server + ISA Server), hanno costi elevati a causa dei vincoli sul numero delle licenze client, sono di non facile gestione perché richiedono una buona preparazione dell'amministratore di rete per garantire un buon livello di sicurezza, sono **probabilmente** poco compatibili (se non del tutto incompatibili) con l'adozione di reti miste comprendenti anche vecchi sistemi Windows e sistemi non Microsoft in un contesto che prevede l'autenticazione degli utenti

3. La combinazione GNU Linux + Squid + DansGuardian, eventualmente integrata da un sistema di autenticazione degli utenti basato su MySQL e altri servizi (Server HTTP per l'amministrazione e Clam AntiVirus per la protezione dei client Windows) offre un potente strumento integralmente libero e gratuito in grado di competere in efficacia, prestazione e portabilità con strumenti forse più sofisticati ma sicuramente più difficili da gestire e più onerosi per le modeste finanze della maggior parte delle scuole

Squid

DansGuardian

GNU Linux

Grazie per l'attenzione