

# Analizzando il contenuto di Internet

La Total Filtering Solution di SurfControl

# Agenda

- Il problema Spam
- I rischi connessi all'uso della Mail e del Web in azienda
- Public Instant Messaging e P2P
  
- Le soluzioni SurfControl:
  - E-Mail Filter
  - Web Filter
  - Instant Message Filter

# L'epidemia dello Spam

## Una definizione:

“Qualunque contenuto non sollecitato che VOI ritene inappropriato o non necessario.”



## Chi spedisce spam e perché lo fa?

- I Virus vengono scritti da hacker e virus-writer: spesso per richiamare l'attenzione, acquisire fama o lanciare messaggi politici
- Lo Spam invece ha un carattere commerciale:
  - Le "Spam gangs" generano Mass Spam
  - In passato erano pagate per ogni indirizzo di email
  - Adesso sono pagate in base al numero di risposte
  - Ricevono 75c di \$ per risposta
  - Percentuale media di risposta: 0.00013 (500,000 messaggi = \$48)



## Chi sono gli spammer e dove sono?



Non più inefficienti e improvvisati  
Ora sono dinamici e sofisticati

... in grado di raggiungere chiunque!

Potrebbero essere ovunque  
Solo il 10% dello spam viene dall'Europa

Perciò le leggi della Comunità Europea non  
possono agire sul 90% del problema

E' una questione globale - non può essere  
risolta in ambito locale



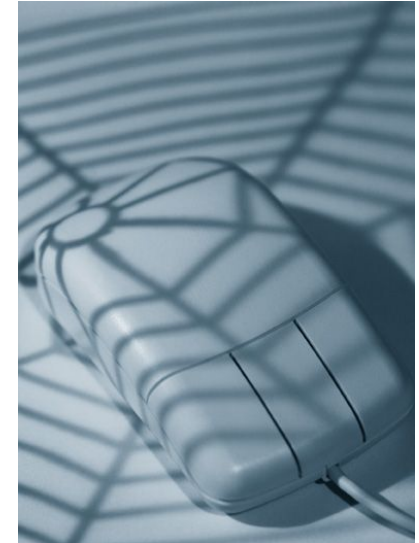
## I rischi del Contenuto su Internet

- Il **contenuto** su Internet comprende immagini, testo, pagine, file e oggetti che vengono prelevati da pagine web o recapitati via e-mail
- Questo **contenuto** può includere siti per Adulti, siti di Hacking, codice maligno, materiale riservato, Spam, linguaggio offensivo...
- Ciò espone le aziende a rischi legati alla produttività, alla sicurezza, all'uso improprio di risorse e a conseguenze legali
- Il controllo su Web e E-Mail riduce questi rischi



## Rischi - Responsabilità Legali

- Il contenuto non appropriato si trova ovunque su Internet e si diffonde velocemente via e-mail
- Questo può portare a querele, denunce per molestie e procedimenti legali
- Molte grandi aziende hanno speso milioni di dollari in cause legali, causate da materiale inappropriato rilevato nelle loro mail o traffico Web
- Il contenuto problematico tipicamente consiste in:
  - Materiale razzista, sessista, per adulti, incitante all'intolleranza o all'uso di droghe o materiale illegale
  - Immagini per adulti
  - Software e musica illegale o pirata




## Rischi - Perdita di Produttività




- Il 40% dell'utilizzo di Internet in azienda non è a fini lavorativi (IDC\*)
- In un'azienda da 1000 dipendenti, se ogni utente usasse il Web o la mail per fini non professionali per 30 minuti al giorno, si avrebbe un costo quotidiano di **25,000 Euro!**
- Distrazioni del Web - siti dedicati a sport, pornografia, shopping, finanze personali ecc.
- Distrazioni dell'E-mail - messaggi personali, chain letters, Spam


## Rischi - Sicurezza



 Il 90% delle proprietà intellettuali delle aziende è in formato digitale (SC Magazine)

- Un bersaglio per gli hackers
- Può uscire dall'azienda in una mail

 I virus nelle mail o nei documenti prelevati dal Web possono diffondersi nella rete aziendale nel giro di secondi

 La mail via Web è una porta aperta per fare entrare i virus e per fare uscire i documenti confidenziali

## Rischi - Risorse di Rete



- Il 35% delle mail non ha fini professionali, il 20% ha allegati
- Il 40% dell'utilizzo di Internet non è riferito al lavoro
- Streaming media, file di grandi dimensioni, freeware, pop-ups e banner occupano l'ampiezza di banda della rete
- Il mancato controllo sul Contenuto può impattare seriamente l'attività professionale

# Rischi Emergenti

L'Instant Messaging e il P2P pongono nuovi rischi di sicurezza su vasta scala



- Rischi legali
  - Regolamentazioni Industriali
  - Perdita di informazioni confidenziali
- Rischi per la Produttività
  - Tempo perso in chiacchiere
- Rischi per la Sicurezza
  - Infezioni Virali
  - Vulnerabilità Hacker
  - Aggiramento delle misure di sicurezza
- Rischi per la Rete
  - Spreco di banda
  - Nessun controllo

# Chi utilizza l'Instant Messaging e il Peer-to-Peer?

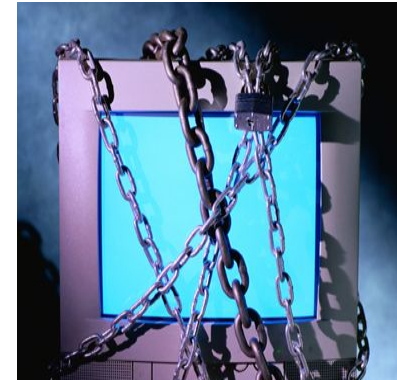
➤ Aumento del 300% nell'utilizzo dell' IM sul lavoro dal 2001 al 2002, saranno oltre 200 milioni di utenti entro il 2005 (IDC)

➤ Alla fine del 2002, gli impiegati nel 70% delle aziende USA utilizzavano applicazioni di IM come AIM, MSM e Yahoo (Gartner '03)

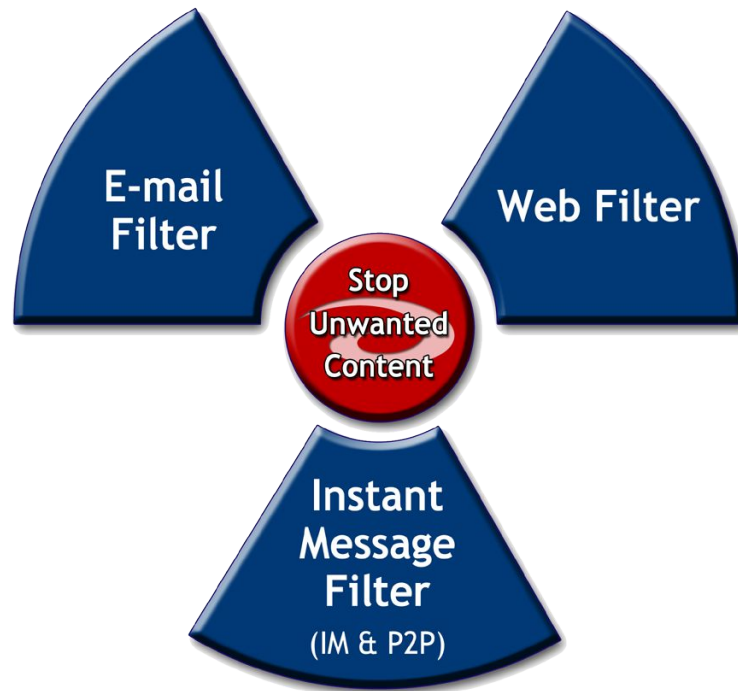
➤ Uno studio del traffico sulla rete di Gnutella ha evidenziato:

- 42% pornografia
- 97% potenziale ricaduta legale

(Palisade systems, riportato in e-marketer)







# La Soluzione Total Filtering SurfControl



- Aumenta la produttività
- Ottimizza le Risorse di Rete
- Incrementa la Sicurezza
- Limita la Responsabilità Legale

# Soluzioni per il controllo di Web & Mail

-  SurfControl fornisce una Soluzione per il Controllo Totale del Contenuto
-  Filtrare solo il contenuto Web o E-Mail lascia una falla che potrebbe essere sfruttata
  - uno senza l'altra è solo una mezza soluzione
-  SurfControl Web Filter è il prodotto numero 1 per il controllo del Web, con il 22% di market share (IDC Giugno 2002)
-  SurfControl è il fornitore #1 di soluzioni per il filtraggio di Web e E-mail (IDC Giugno 2002)



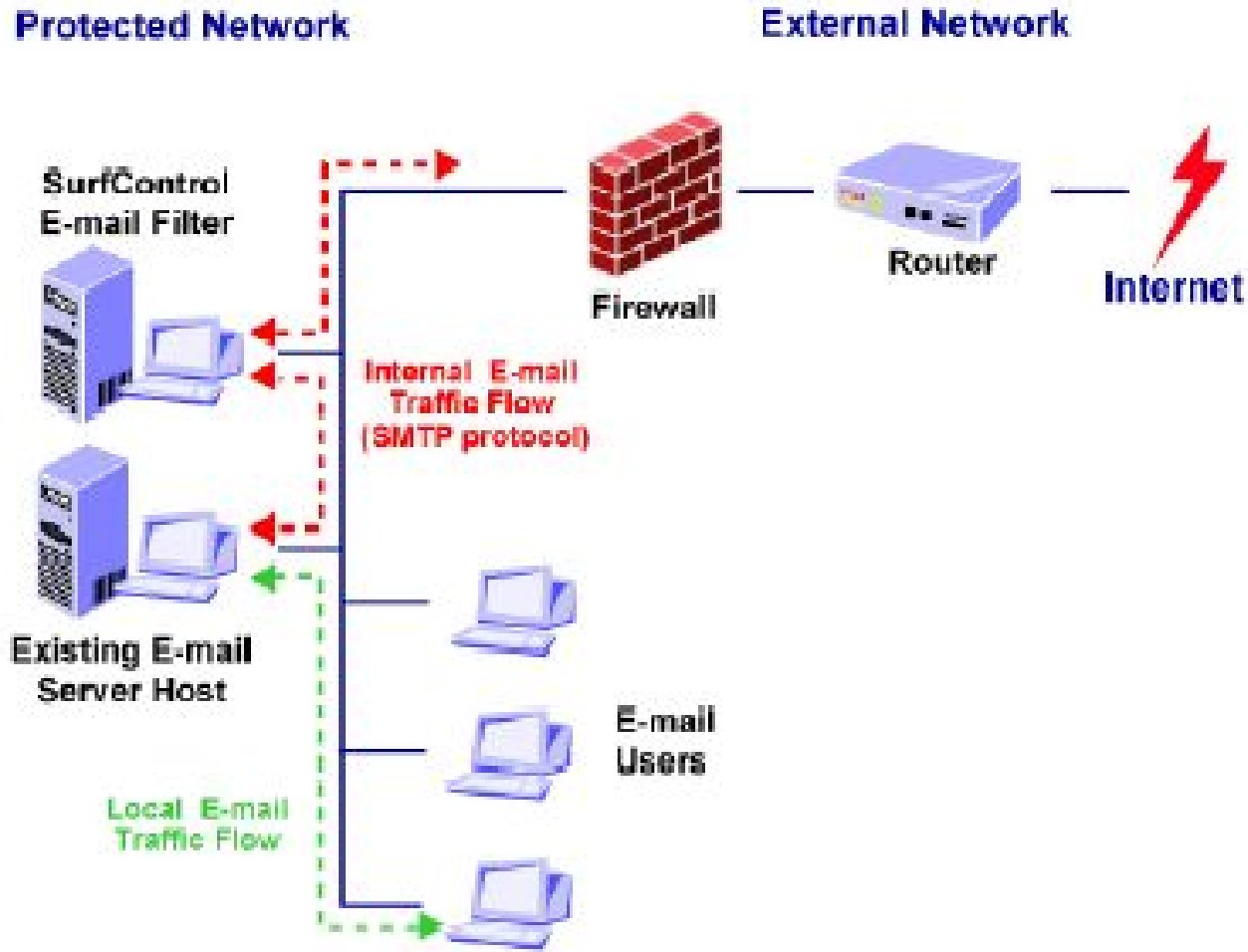
# E-mail Filter for SMTP



## Cos'è E-Mail Filter for SMTP

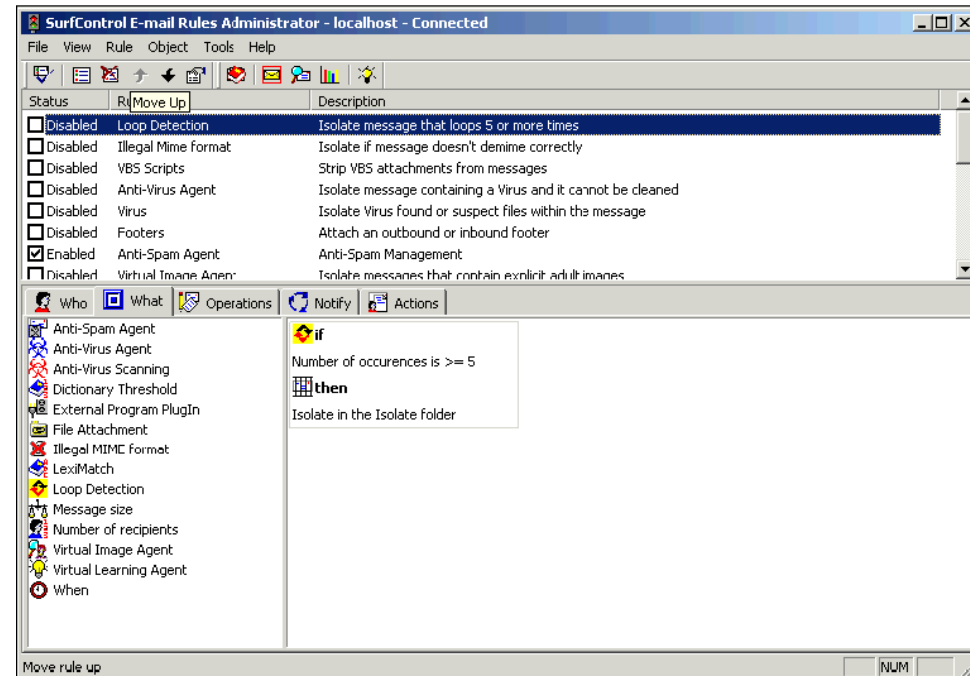
- Soluzione software, in ambiente Windows server, che permette l'applicazione delle Acceptable Usage Policy per la posta elettronica
- Analizza il contenuto delle mail (mittente, destinatario, allegati, corpo del messaggio...)
- L'amministratore può stabilire regole e azioni da eseguire su messaggi che presentino caratteristiche specifiche. Es:
  - Se un messaggio ha un allegato con estensione EXE, bloccalo
  - Se un messaggio contiene termini che ricorrono spesso nelle mail Spam, mettilo in quarantena
  - Se una mail ha un allegato, lancia un antivirus esterno per controllarlo

# Scenario: Server Dedicato



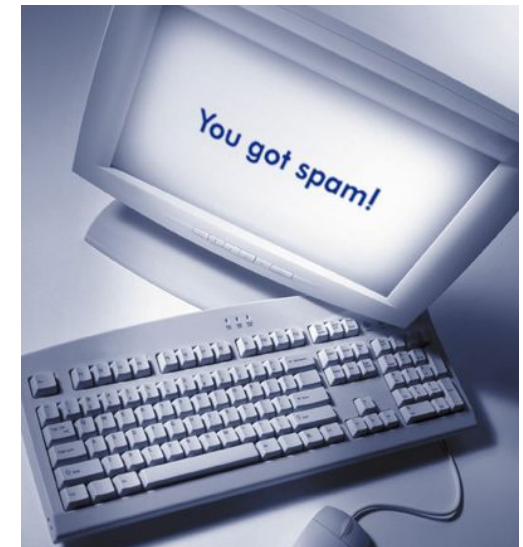
## Componenti:

- **Rules Administrator:** Strumento per creare le regole che compongono le Acceptable Usage Policies
- **Message Administrator:** Gestione e azioni su messaggi individuali e log
- **Monitor:** Controllo in tempo reale delle mail che vengono analizzate da E-Mail Filter
- **Administrator:** Amministrazione di E-Mail Filter tramite Browser
- **Scheduler:** Strumento per automatizzare i compiti ripetitivi (es: aggiornamento e gestione dei database)



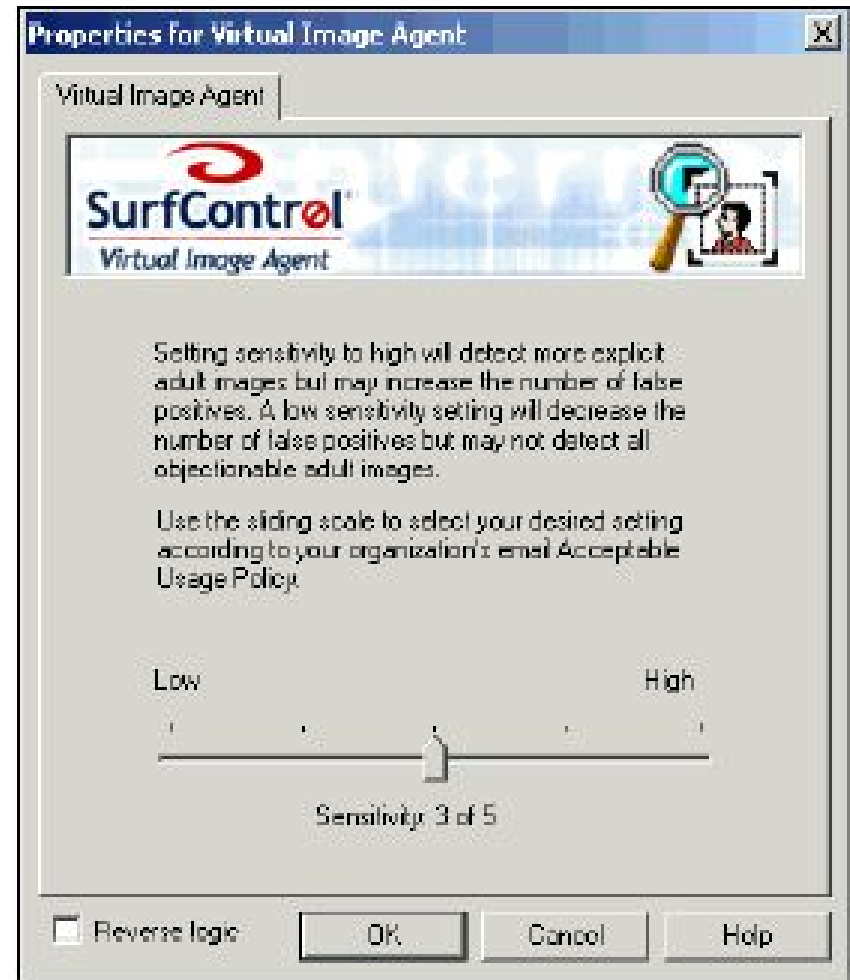
## Strumenti Anti-Spam

- **Anti-Spam Agent:** incorpora un database di Spam noto, permettendo all'amministratore di filtrare il contenuto non gradito
- **Dictionary Threshold:** consente di filtrare le mail in base alla frequenza e al tipo di parole che contengono - basato sui dizionari multilingue
- **LexiMatch:** permette di effettuare ricerche Booleane (AND, OR, NEAR...) sul contenuto delle mail - basato sui dizionari multilingue
- **Virtual Learning Agent:** mediante la tecnologia delle reti neurali, è in grado di "imparare" i termini del linguaggio in maniera contestuale - basato su Advanced Reasoning Technology. Capace di contrastare lo spam nuovo e di classificare dinamicamente le mail in base al contenuto



## Virtual Image Agent

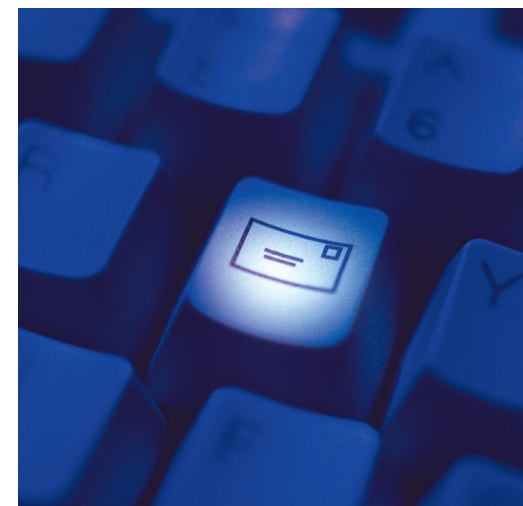
- Mediante la tecnologia delle reti neurali, analizza le immagini allegata alla mail
- Basandosi su colori e forme, è in grado di rilevare le immagini pornografiche
- Permette all'amministratore di bloccare selettivamente gli allegati "per adulti"
- Sensibilità regolabile



## Oggetti per la gestione della mail

- Loop Detection object
- Anti-Virus Agent
- Anti-Virus Scanning
- Strip Attachment
- HTML stripper
- Spoof Management

...



## Alcune feature significative

- Integrazione LDAP per creare più velocemente regole user-oriented
- Reportistica completa per avere un feedback sull'utilizzo della rete
- Fail Over e Load Balancing per gli ambienti corporate



# Web Filter for Windows



## Cos'è Web Filter for Windows 2000/2003

- Una soluzione software, a livello server, che permette di applicare policy e regole sul traffico Web
- Non è un proxy
- Utilizza un approccio simile a quella degli sniffer, catturando i pacchetti mediante la “pass-by” technology
- Consente di stabilire policy che permettono o negano l'accesso ai siti web per singoli utenti o gruppi di utenti
- La parola-chiave è **Categorizzazione**

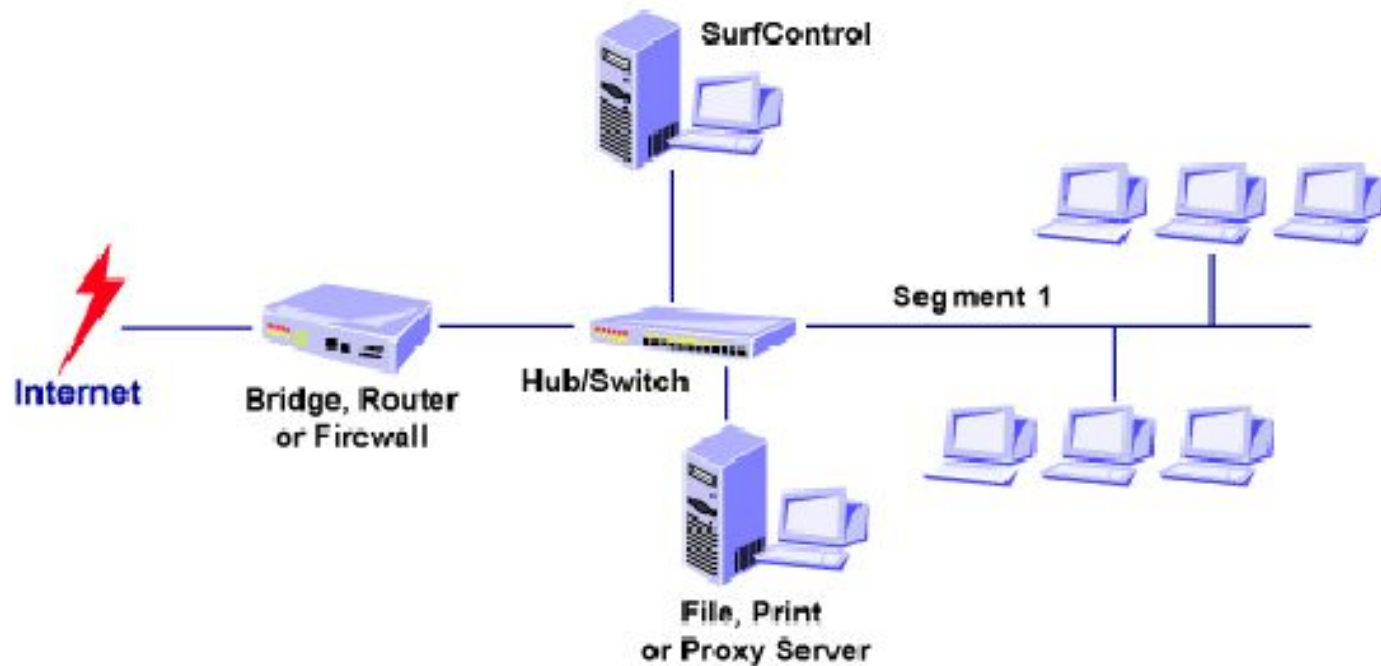
## Categorie e regole

- Oltre 6 milioni di URL categorizzati nel database Aura
- Oltre 1 miliardo di pagine Web
- 35,000 nuovi URL aggiunti ogni settimana
- 40 categorie di contenuti
- Il database di siti più ampio, più accurato e completo nel suo campo



- A ogni categoria, si possono applicare policy differenti
- Ad esempio:
  - I siti pornografici sono sempre vietati
  - I siti sportivi sono permessi solo in determinate fasce orarie

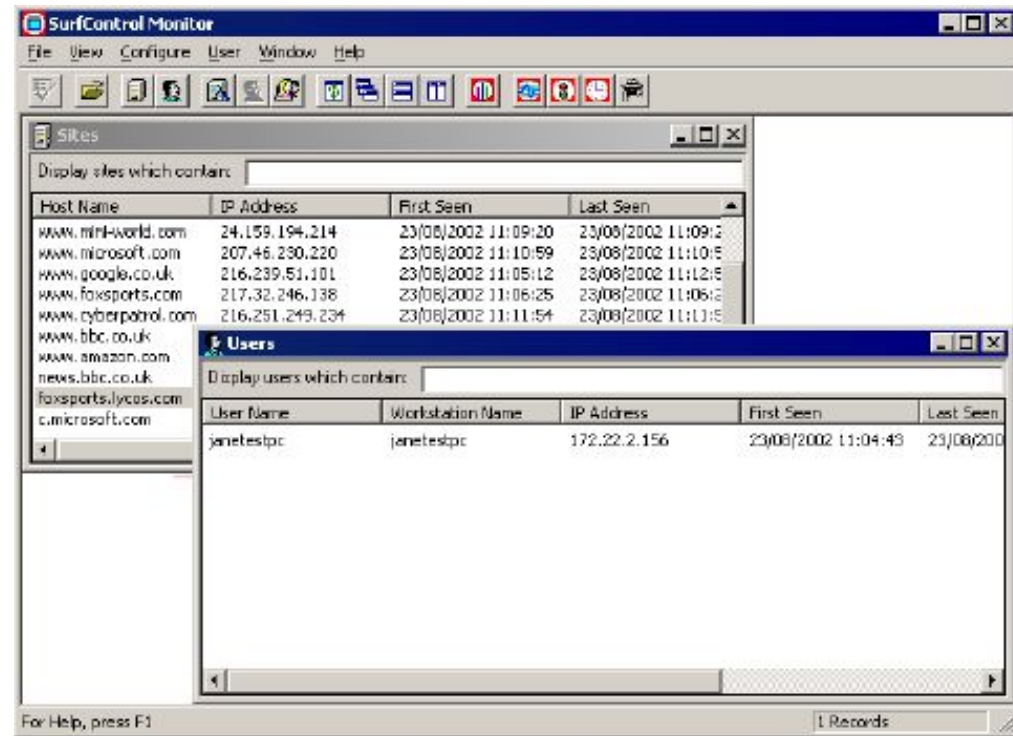
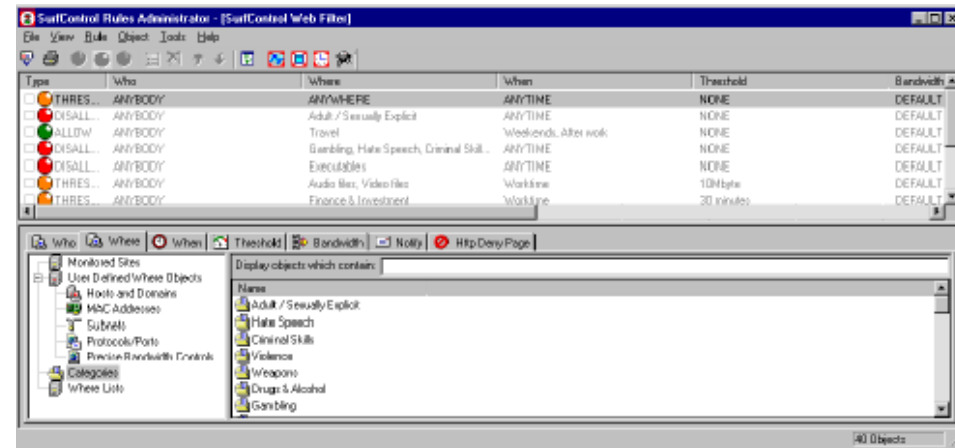
## Scenari: rete single-segment



Un singolo segmento, macchine connesse a un hub

## Componenti:

- **Rules Administrator:** Strumento per creare e applicare Regole e Policy
- **Monitor:** Verifica delle attività di utenti, host, gruppi
- **Real Time Monitor:** Mostra l'attività sulla rete in tempo reale
- **Virtual Control Agent:**
  - Basato sulla Advanced Reasoning Technology, oggetto in grado di categorizzare automaticamente i nuovi siti, analizzandone varie pagine di contenuto
  - Supporta inglese, spagnolo,



## Flessibilità e Scalabilità

### SurfControl Web Filter per:

- MS Windows
- Microsoft Proxy
- ISA Server
- CheckPoint FW-1
- VS per Linux
- VS per Nokia IPSO
- Novell BorderManager



### Web Filter può essere installato in ambienti con backbone

Gigabit Ethernet

# SurfControl Instant Message Filter





# Blocco basato sulle “impronte”



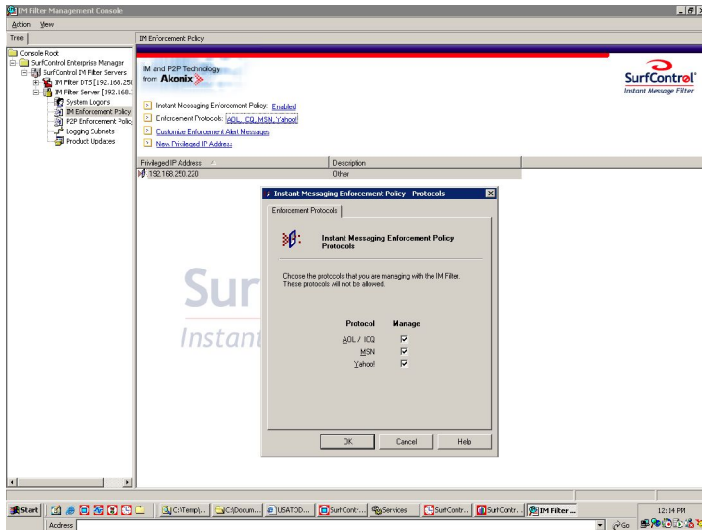
## Protocolli di IM Pubblico:

- AOL Instant Messenger
- MSN Messenger
- Yahoo Instant Messenger
- ICQ

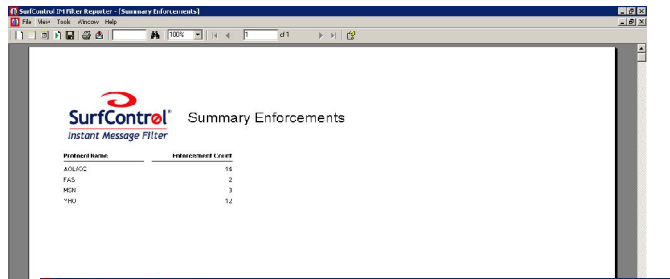


## Protocolli Peer-to-Peer

- Gnutella Network (BearShare, Phex, Gnucleaus, LimeWire, Morpheus, ecc.)
- FastTrack Network (Kazaa & Grokster)

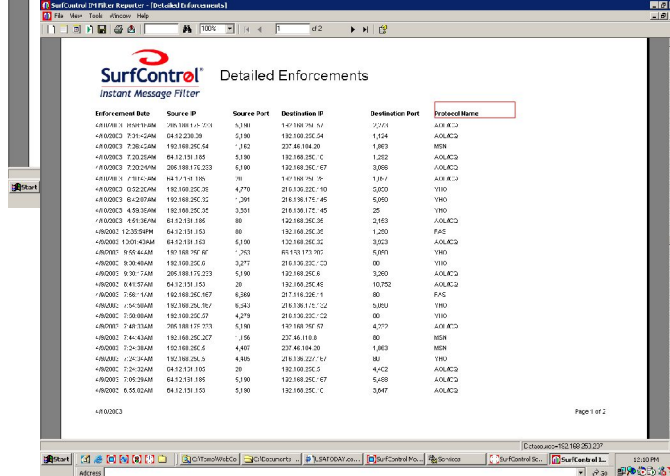


# Amministrazione completa



**SurfControl Summary Enforcements**  
Instant Message Filter

Protocol Name	Enforcement Count
ADSL2C	16
FA5	2
MSN	3
YHO	52

**SurfControl Detailed Enforcements**  
Instant Message Filter

Enforcement Info	Source IP	Source Port	Destination IP	Destination Port	Protocol Name
CR1088-1 105919AM	206.188.15.213	5390	192.168.255.54	2574	ADSL2C
*R000C3 7:31-5AM	64.12.238.29	5390	192.168.255.54	1554	ADSL2C
*R000C3 7:28-5AM	192.168.252.54	1362	227.84.184.20	1863	MSN
*R000C3 7:23-5AM	64.12.134.185	5390	192.168.255.54	1262	ADSL2C
*R000C3 7:20-5AM	206.188.15.213	5390	192.168.255.54	3066	ADSL2C
*R000C3 7:17-5AM	243.174.186	96	192.168.255.54	1397	ADSL2C
*R000C3 6:52-5AM	192.168.252.38	4770	214.139.227.10	6000	YHO
*R000C3 6:42-5AM	192.168.252.32	1261	214.139.174.45	6000	YHO
*R000C3 6:30-5AM	192.168.252.32	3201	214.139.174.45	26	YHO
*R000C3 6:19-5AM	192.168.252.32	5201	192.168.255.54	2453	ADSL2C
*R000C3 6:15-5AM	64.12.134.185	80	192.168.255.54	1200	FA5
*R000C3 1:20-5PM	64.12.134.185	5390	192.168.255.54	3023	ADSL2C
*R000C3 1:01-4PM	64.12.134.185	5390	192.168.255.54	6000	YHO
*R000C3 9:50-4AM	192.168.252.46	1263	65.153.173.100	6000	YHO
*R000C3 9:30-4AM	192.168.252.6	3277	214.139.227.10	00	YHO
*R000C3 9:30-7AM	206.188.15.213	5390	192.168.255.54	3200	ADSL2C
*R000C3 8:41-5AM	64.12.134.185	20	192.168.255.54	10762	ADSL2C
*R000C3 7:00-1AM	192.168.252.467	6369	217.118.206.1	80	FA5
*R000C3 7:00-9AM	192.168.252.767	6363	214.139.174.45	3000	YHO
*R000C3 7:00-8AM	192.168.252.27	4279	214.139.227.10	00	YHO
*R000C3 7:40-13AM	206.188.15.213	5390	192.168.255.54	4377	ADSL2C
*R000C3 7:40-4AM	192.168.252.207	1356	225.81.16.8	80	MSN
*R000C3 7:24-3AM	192.168.252.6	4407	227.46.184.20	1863	MSN
*R000C3 7:24-3AM	192.168.252.5	4365	214.139.227.10	80	YHO
*R000C3 7:24-2AM	64.12.134.185	20	192.168.255.54	4452	ADSL2C
*R000C3 7:05-3AM	64.12.134.185	5390	192.168.255.54	6488	ADSL2C
*R000C3 6:55-2AM	64.12.134.185	5390	192.168.255.54	3647	ADSL2C

 Specifico per ogni protocollo  
- Permetti o Blocca

 Aggiornamenti sui Protocolli

 Notifiche personalizzate

 Esclusione di indirizzi IP specifici dal bloccaggio

 Report

# Strategia di SurfControl Vs. Concorrenza

🌀 I concorrenti offrono:

- Riconoscimento di un minor numero di protocolli
- Soluzioni basate sul blocco delle porte
- Gestione a livello client

🌀 SurfControl - Sicurezza completa contro Public IM & P2P non autorizzati:

- Soluzione per server, efficiente e sicura
- Riconoscimento per impronte di tutti i principali protocolli di rete public IM e P2P

  
**SurfControl**<sup>®</sup>  
Instant Message Filter



  
**SurfControl**<sup>®</sup>

# SurfControl

## *The Total Leader in Filtering*



- Il fornitore #1 di soluzioni per il filtraggio di Web e E-mail
- Il leader globale del mercato
- Il marchio più riconosciuto nel Content Filtering