# Seminario di approfondimento sulla sicurezza informatica

*Carmelo Floridia*
*c.floridia@idsunitelm.it*

# Agenda

## Strumenti per l'analisi della rete interna (rilevazione e soluzioni contro il P2P)

- Rete Tipo
- Considerazioni di carattere generale
- Monitorare la rete
- Analizzare il traffico di rete
  - Rilevare anomalie
  - Rilevare il P2P
  - Il problema della posta elettronica

## Ottimizzazione e protezione della navigazione web

- Utilizzo della banda
- Contrastare il P2P o altro download massivi
- URL filtering

## Aspetti normativi

- Per l'utilizzo di misure di sicurezza (URL Filtering)
- Per l'accesso a postazioni internet "aperte" (aule, biblioteche, oratorio..)

## Soluzioni per il collegamento in VPN

- Collegamento tra sedi e con utenti remoti
- Soluzioni con prodotti commerciali ed opensource
- Dettagli tecnici e punti di attenzione con il NAT

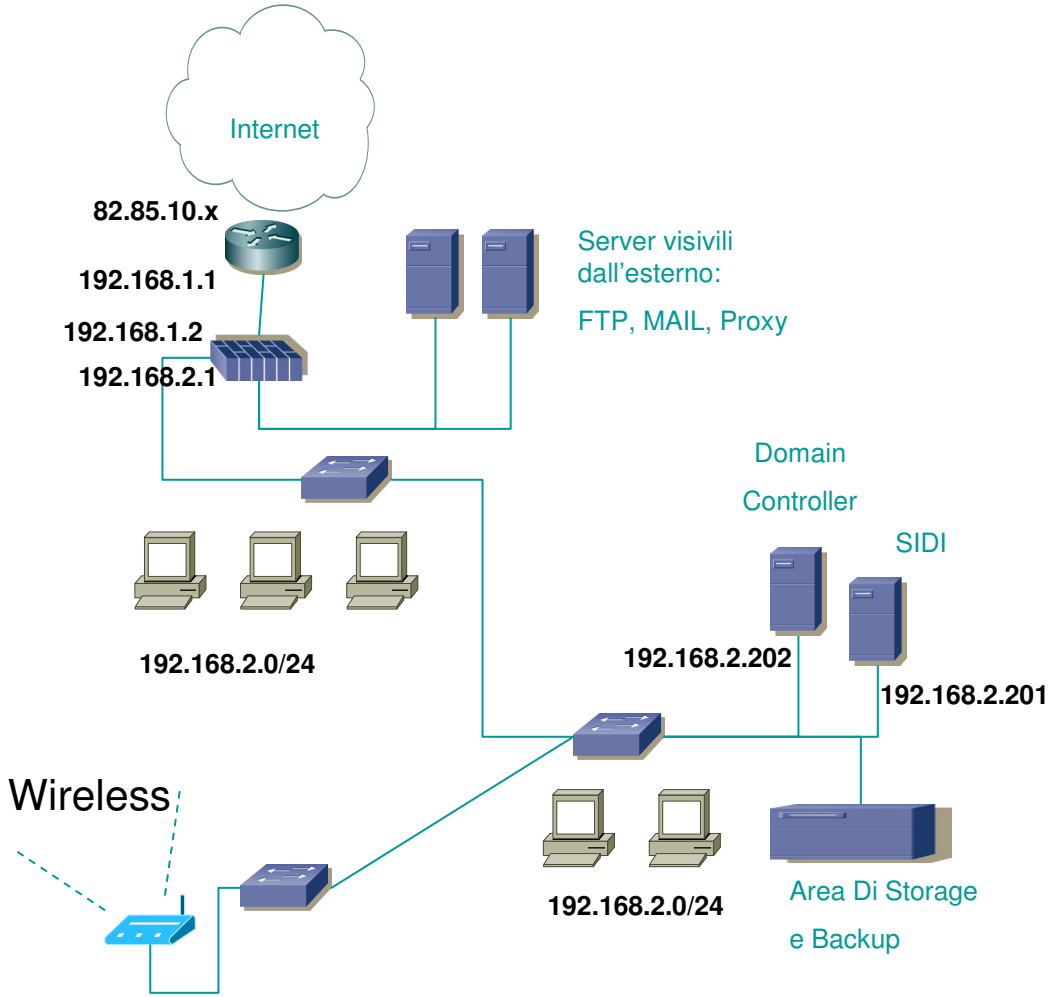
## Backup PC e server

- Individuazione dei dati da archiviare
- Tecnologie
- Prodotti commerciali ed opensource

## Utilizzo sicuro delle reti Wireless

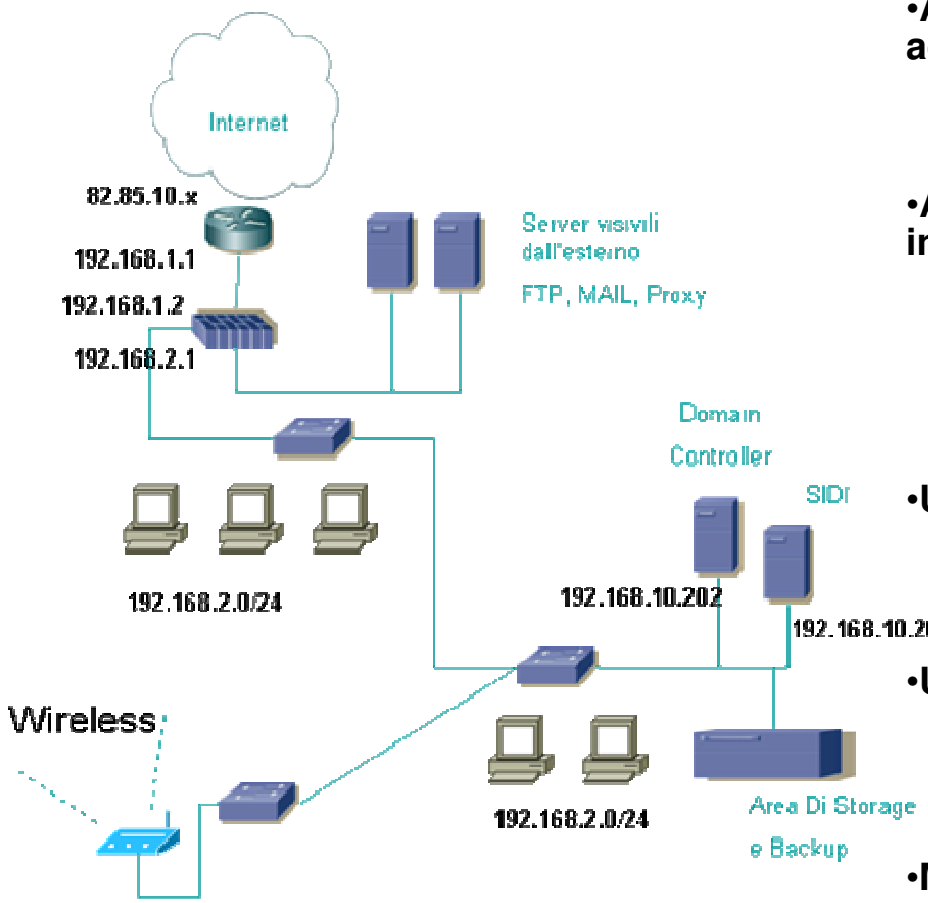
## Vademecum per l'utilizzo del PC di internet e della posta elettronica

# Architettura tipo di una rete diocesana




- **Architettura Tipo**
  - **Rete**
    - Router
    - Firewall
    - Switch
    - Access Point
  - **Sistemi**
    - Domain Controller
    - Area di Storage e Backup
    - Proxy
    - APPLICAZIONI
    - Postazioni CLIENTI
- **Cosa manca?**

# Architettura tipo di una rete diocesana




- Suggerimenti
  - **Avere sempre uno schema di rete ed un inventario aggiornato**
    - Utile per valutare upgrade, individuare problemi, valutare la sicurezza
  - **Avere un piano di indirizzamento (se si usano indirizzi statici)**
    - Stabilire quale range e' dedicato a PC, Server, Apparati
    - In caso di DHCP cominciare a valutare 802.1x per l'accesso sicuro
  - **Utilizzare Dominio Microsoft**
    - Upgrade e controllo centralizzato
    - File system distributo..
  - **Utilizzare le VLAN**
    - Separare rete client da server, voce da dati, etc (monitoraggio, sviluppo, aule informatiche, ospiti..)
  - **Mantenere aggiornati sistemi e rete**
    - Ultima volta upgrade router/firewall/switch?
    - Ancora qualche HUB?
  - **Apparati di scorta o soluzioni di backup**
    - che succede se salta uno switch o un router?

# Tenere sotto controllo la propria rete

- **E' opportuno avere sotto controllo lo stato di funzionamento della propria rete**
  - Quali sistemi HW inventory
  - Con quali programmi (sw inventory)
  - Sapere quali sistemi sono UP
  - Verificare l'occupazione di banda
  - Attivare alert in caso di fault

- **E' opportuno verificare la visibilità della propria rete**
  - Quali servizi e macchine sono accessibili dall'esterno
  - Visibilità delle macchine all'interno

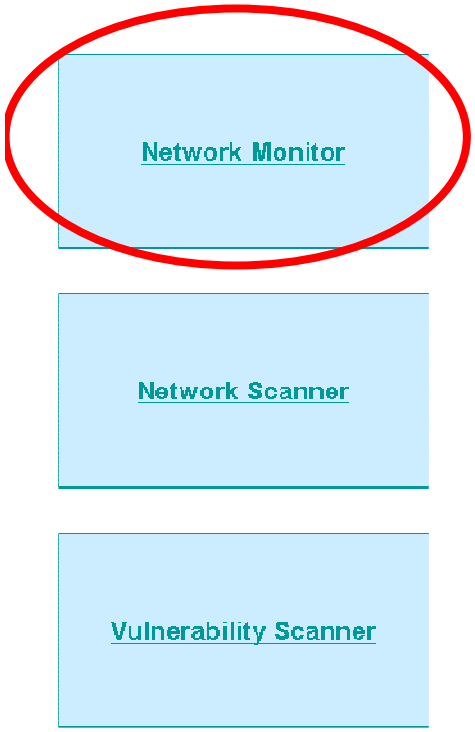
- **E' opportuno misurare periodicamente le vulnerabilità della propria rete**
  - A quali vulnerabiltà sono esposti i sistemi e gli apparati di rete

**Network Monitor**

**Network Scanner**

**Vulnerability Scanner**

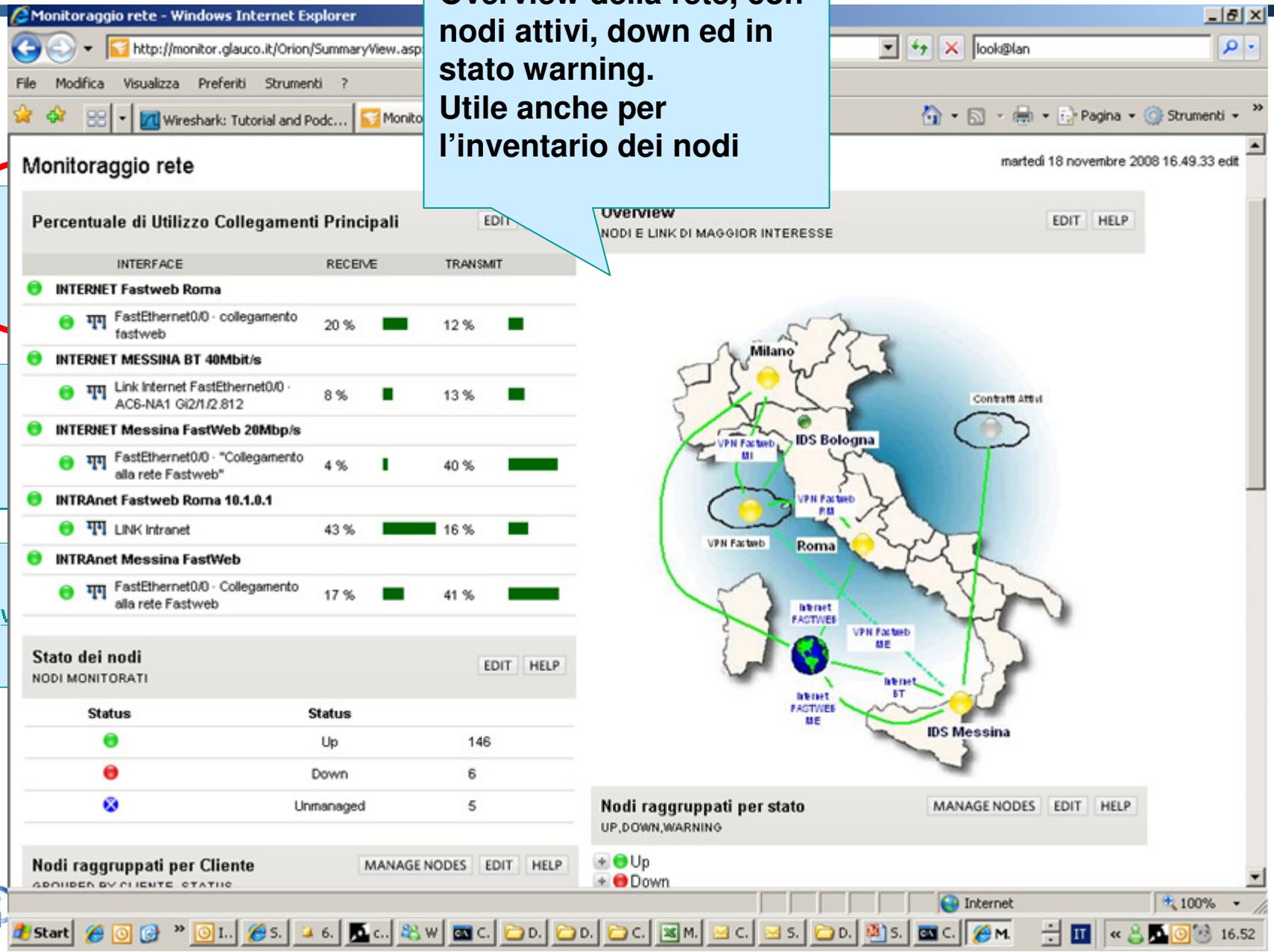
# Network Monitor



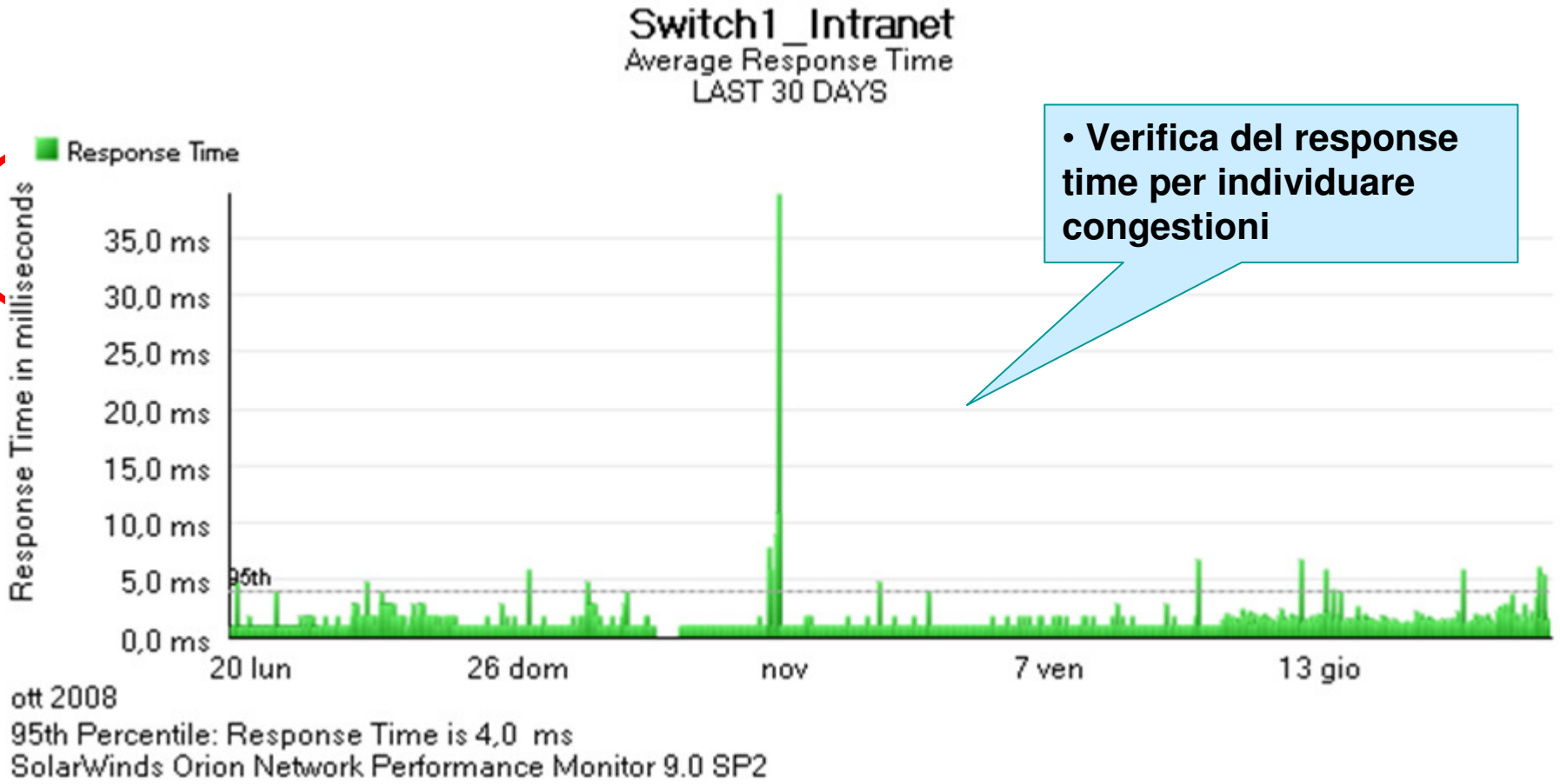

- Overview sullo stato di salute della rete
- Informazioni raccolte mediante ICMP (ping) e SNMP (Simple Network Management Protocol)
- Attenzione all'attivazione dell'SNMP
  - Utilizzare opportune ACL
  - utilizzare community RO altrimenti si rischia che da remoto puo' essere modificata la conf degli apparati di rete
- Diverse soluzioni sia commerciali che open source
  - www.solarwinds.net
  - Opensource
    - Zabbix
    - Nagios
- Demo
  - Http://monitor.glauco.it
    - Utilizzo interfacca
    - Mappa di roma
    - Alert
    - Eventi
    - Syslog

# Network Monitor

**Overview della rete, con nodi attivi, down ed in stato warning.**
**Utile anche per l'inventario dei nodi**

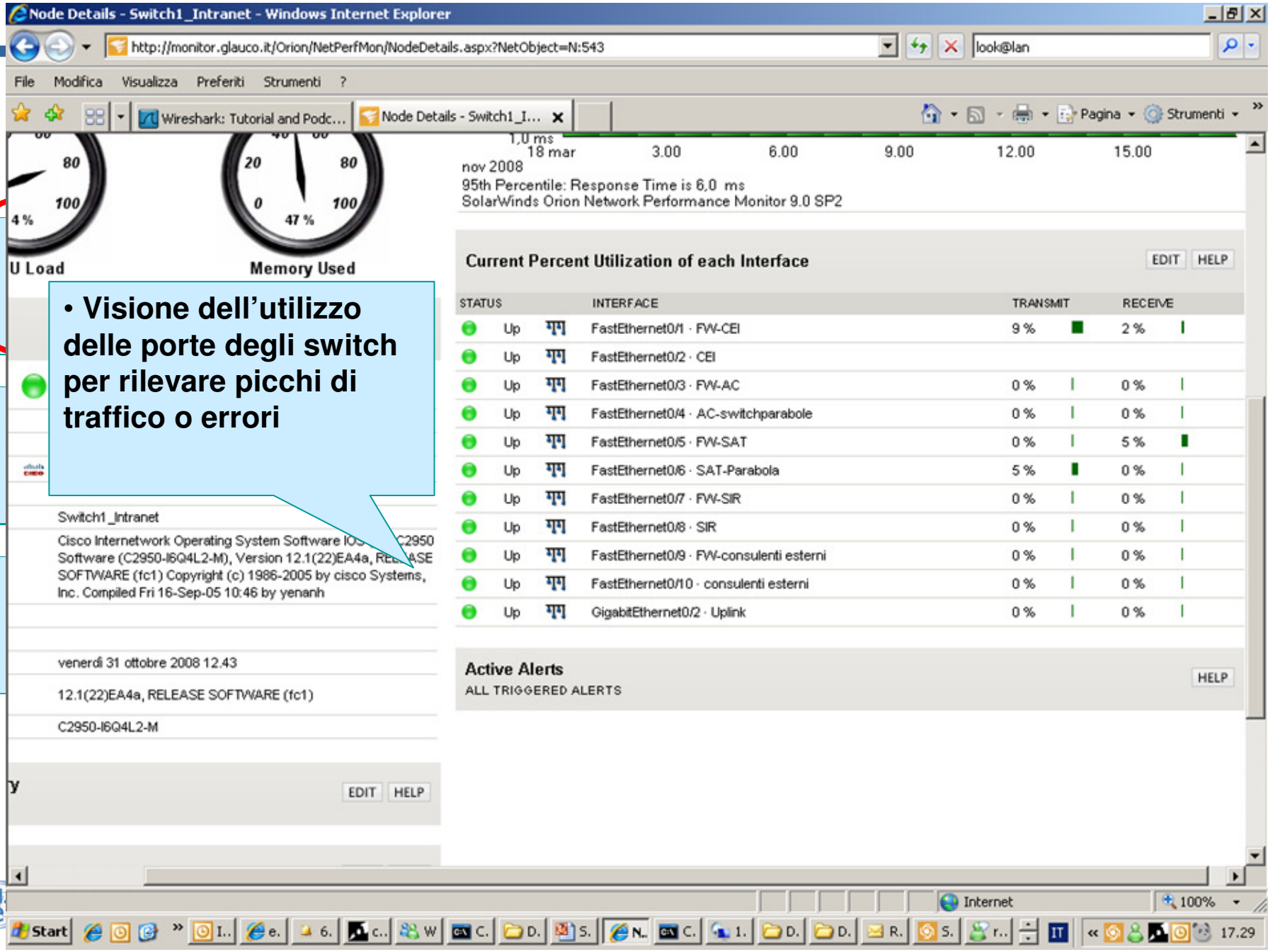


# Network Monitor

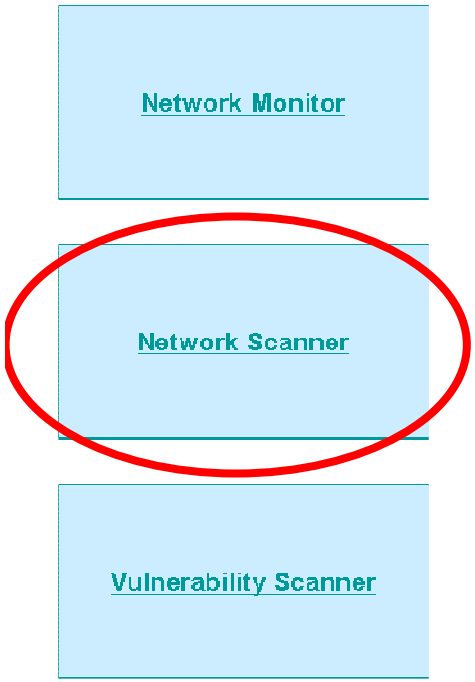



- **Verifica del response time per individuare congestioni**

# Network Monitor



# Network Scanner



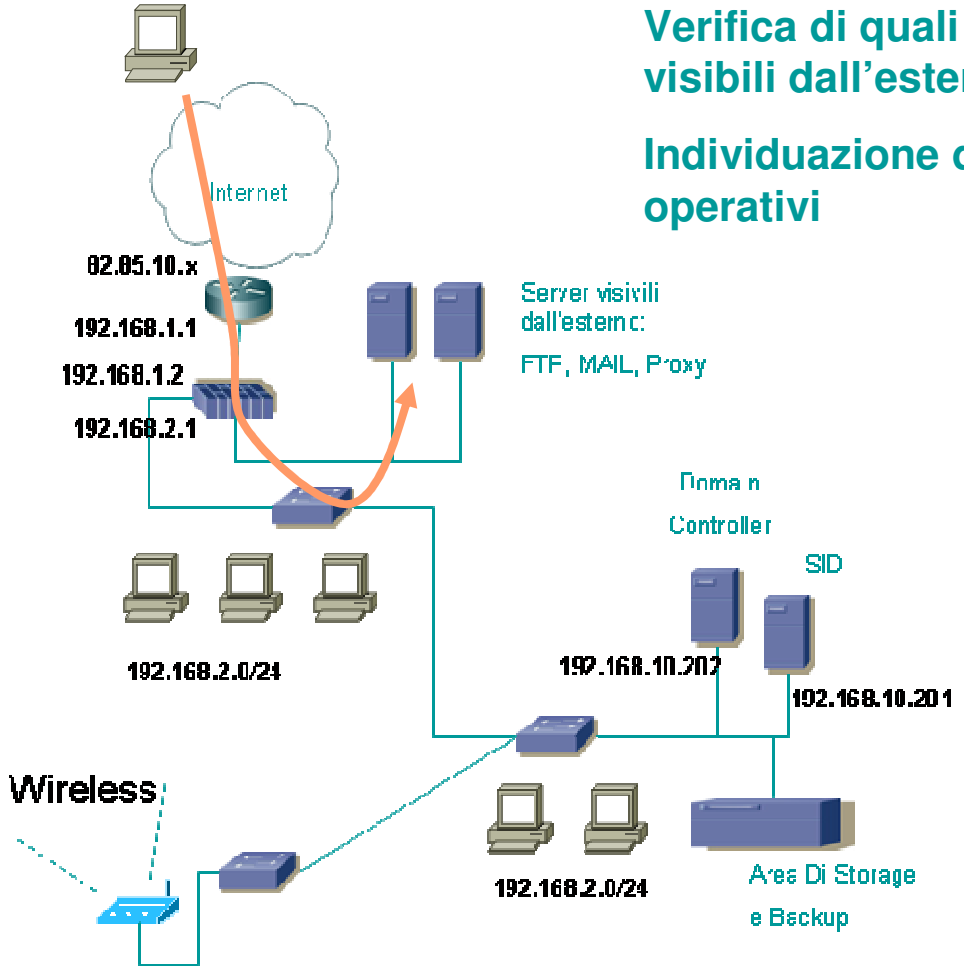

- **Verifica della visibilità della propria rete:**
  - Dall'esterno (anche per testare la configurazione del firewall)
  - Se si ritiene utile anche dall'interno soprattuto se vi sono VLAN distinte (ospiti, server, PC)
- **Obiettivo:**
  - Individuare quali servizi sono attivi sui server
  - Disabilitare i servizi non necessari
- **Strumenti**
  - Whois
  - PING , Traceroute
  - **!!NMAP!!**
    - **www.insecure.org**
  - DEMO su NMAP
    - Scansione IP IDS&Unitelm
      - nmap -T4 --version-light -sV -F -O 62.101.89.57
      - nmap -PI 62.101.89.*
    - Commenti sui risultati
    - Scansione di altri indirizzi

# Network Scanner

Network Monitor

Network Scanner

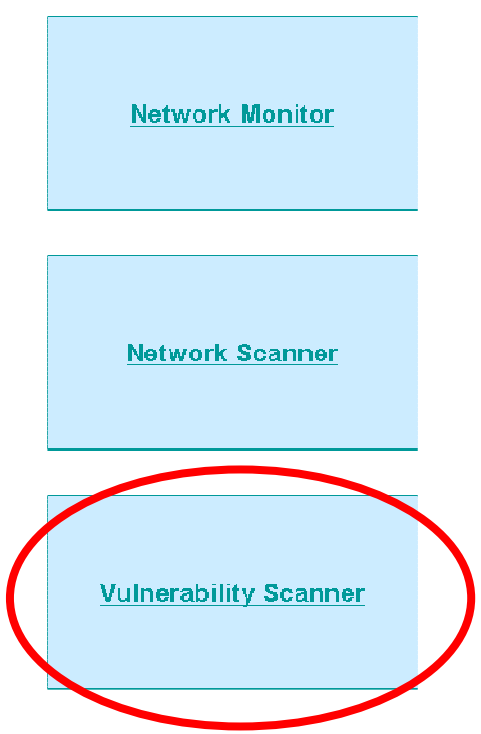
Vulnerability Scanner




**Verifica di quali porte sono visibili dall'esterno**

**Individuazione dei sistemi operativi**

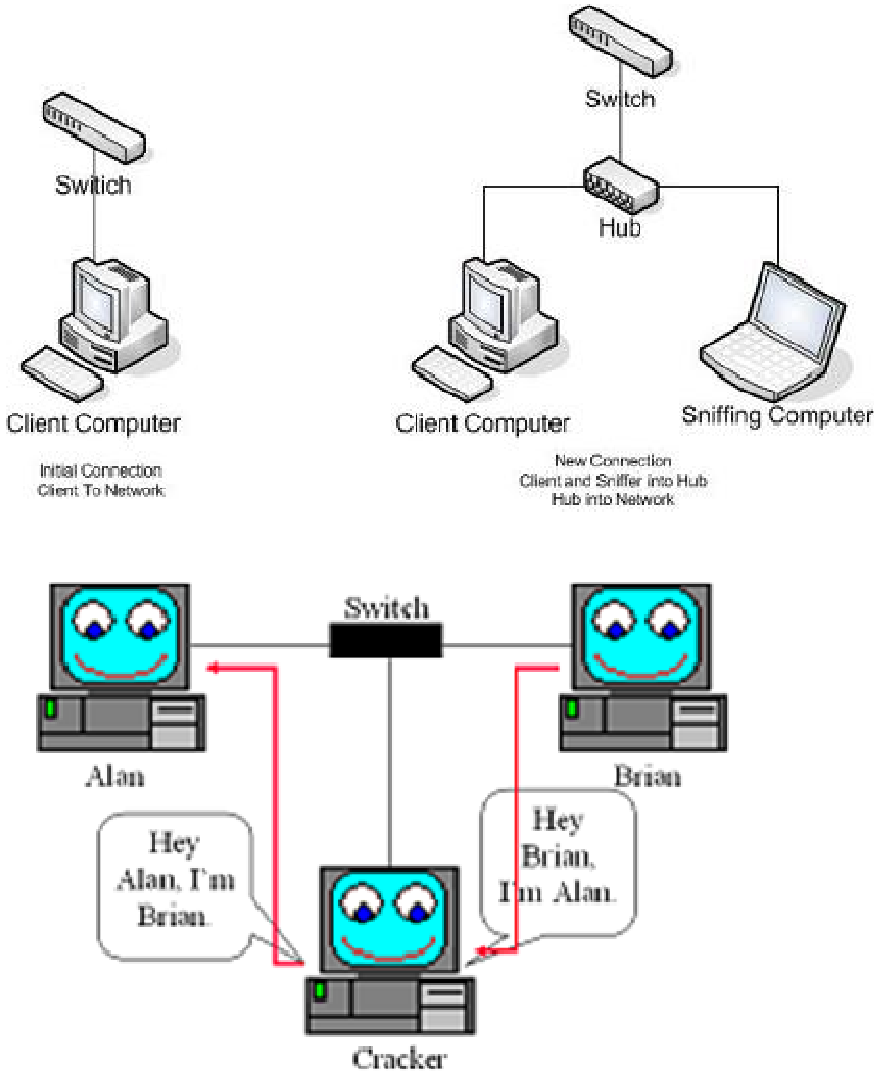
# Network Scanner




- **Verifica del livello di sicurezza**
  - Verificare a quali vulnerabilità note la rete ed i sistemi sono esposti
    - Le vulnerabilità possono essere tecnice ma anche organizzative (password deboli)
  - Giusto un accenno perche' l'argomento e' vario e merita di essere trattato con una sessione dedicata (magari un webcast dedicato sull'argomento)
- **Obiettivo:**
  - Rispetto ai servizi individuati al passo precedente, rilevare le vulnerabilità note
  - Definire una serie di attività per ridurre le vulnerabilità
- **Strumenti**
  - Diversi prodotti commeciali ed Opensource
    - IBM-ISS, Retina
    - Opensource: Nessus, Security Manager
  - Possibilità di usufruire di un servizio (che periodicamente effettua la scansione e fornice dei report e delle linee guida per ridurre le vulnerabilità)

**Report Demo**

# Analisi della rete con sniffer




- **Quando effettuarlo**
  - In caso di anomalie non rilevabili dall'analisi ad alto livello effettuata con gli strumenti di network monitor
- **Strumenti**
  - Opensource Wireshark (evoluzione di etherieal)
  - NTOP (www.ntop.org)
  - Diverse soluzioni a pagamento (iris, network associate..)
- Modalità
  - Con HUB (se si dispone di hub)
  - con ARP Poisoning e strumenti come CAIN

# Analisi della rete – Download Lento

- Prima dell'analisi della rete:
  - Individuare dove analizzare il trafico
  - Rete switchata?
    - ARP Poisoning
      - CAIN

- File di esempio: filedownload.dmp
  - Download di un file via http da due server distinti
    - Dall' I/O graph si nota la diversa velocità con cui sono scaricati i due file
    - Verifica dei due momenti di download
    - Poi da Analyze --> expert info altre considerazioni
      - **TCP window Update packets**: normale che in fase di trasferimento sia negoziata la dimensione della finestra TCP per ottimizzare i tempi di trasferimento
      - Individuare i primi problemi:
        - "Previous segment lost" : il client ha perso un pacchetto e rimanda dei "duplicate ack" finche' il server non rimanda il pacchetto mancante (identificato come "Fast retransmission" )
        - Inizialmente pochi "Duplicate Ack" , a seguire tanti messaggi di questo tipo in sequenza (signifca che c'e' maggiore latenza e problemi di rete), nel secondo download i duplicate ACK sono pochi (fisiologici)
      - Selezionare il pacchetto 1023 "Statistics" -> "TCP Stream Graph" -> "Round Trip Time Graph", si vede che il round trip time e' di 1 secondo (valore molto alto per i downlod)

# Analisi della rete – Problemi di collegamento

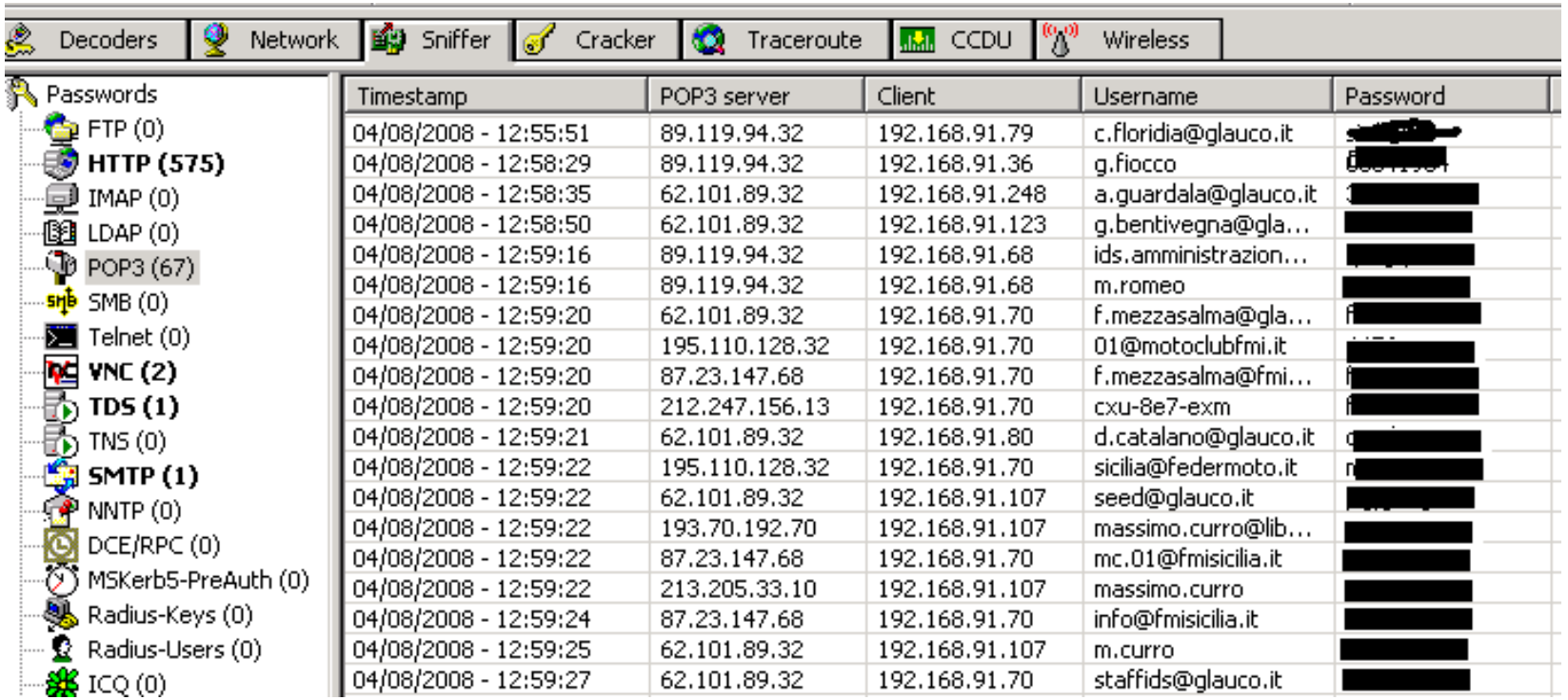
- Aprire con wireshark slowrouter.dmp
  - Prime considerazioni:
    - Tanti pacchetti ARP Broadcast (normali per il routing interlan), quindi mettere !arp per ridurre il numero di info visualizzate
    - Modificare l'impostazione per visualizzare l'intervallo di tempo tra un pacchetto e l'altro (View-> time display -> secondi dall'ultimo pacchetto)
      - Al pacchetto 18 (1 secondo per avere la risposta dal DNS!!!
      - In genere dopo la riposta dns ci dovrebbe essere subito il 3way handshake verso il server. In questo caso, il client fa il syn , ma il syn-'ack arriva in ritardo (mezzo secondo)
      - Arriva inoltre la risposta del dns che prima non aveva risposto, introducendo una ulteriore latenza
      - Ritrasmissione perche la pagina ancora non arriva (in totale 9 secondi di attesa)
      - Comportamenti di questo tipo possono far pensare ad un malfunzionamento del router (verificare dopo riavvio o firmware upgrade)

- Aprire spyware.dmp
  - ip.host==172.16.1.10
  - Tanti pacchetti RST perche' la macchina riceve connessioni che non si aspetta sulla porta 26452
  - Al pacchetto 70 analiz.exe via tftp (spyware in casa!!!)

## Analisi della rete – Altri esempi

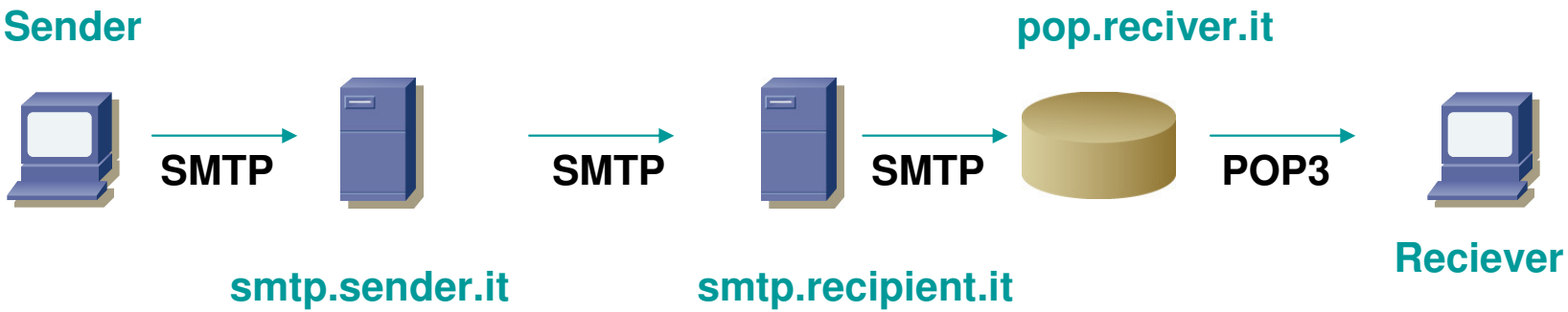
- Altri esempi
  - File: Emule.cap
    - Edit -> find pachet -> string EMULE
  - File posta.cap
    - ip.src == 192.168.91.79
    - Cattura messaggio normale, firmato (dal pacchetto 2382) , cifrato (pacchetto 3919) e con smtp ssl (6398)

# Dimostazione – 5 min di sniffing su rete




| Timestamp | POP3 server | Client | Username | Password |
|---|---|---|---|---|
| 04/08/2008 - 12:55:51 | 89.119.94.32 | 192.168.91.79 | c.floridia@glauco.it | [redacted] |
| 04/08/2008 - 12:58:29 | 89.119.94.32 | 192.168.91.36 | g.fiocco | [redacted] |
| 04/08/2008 - 12:58:35 | 62.101.89.32 | 192.168.91.248 | a.guardala@glauco.it | [redacted] |
| 04/08/2008 - 12:58:50 | 62.101.89.32 | 192.168.91.123 | g.bentivegna@gla... | [redacted] |
| 04/08/2008 - 12:59:16 | 89.119.94.32 | 192.168.91.68 | ids.amministrazion... | [redacted] |
| 04/08/2008 - 12:59:16 | 89.119.94.32 | 192.168.91.68 | m.romeo | [redacted] |
| 04/08/2008 - 12:59:20 | 62.101.89.32 | 192.168.91.70 | f.mezzasalma@gla... | [redacted] |
| 04/08/2008 - 12:59:20 | 195.110.128.32 | 192.168.91.70 | 01@motoclubfmi.it | [redacted] |
| 04/08/2008 - 12:59:20 | 87.23.147.68 | 192.168.91.70 | f.mezzasalma@fmi... | [redacted] |
| 04/08/2008 - 12:59:20 | 212.247.156.13 | 192.168.91.70 | cxu-8e7-exm | [redacted] |
| 04/08/2008 - 12:59:21 | 62.101.89.32 | 192.168.91.80 | d.catalano@glauco.it | [redacted] |
| 04/08/2008 - 12:59:22 | 195.110.128.32 | 192.168.91.70 | sicilia@federmoto.it | [redacted] |
| 04/08/2008 - 12:59:22 | 62.101.89.32 | 192.168.91.107 | seed@glauco.it | [redacted] |
| 04/08/2008 - 12:59:22 | 193.70.192.70 | 192.168.91.107 | massimo.curro@lib... | [redacted] |
| 04/08/2008 - 12:59:22 | 87.23.147.68 | 192.168.91.70 | mc.01@fmisicilia.it | [redacted] |
| 04/08/2008 - 12:59:22 | 213.205.33.10 | 192.168.91.107 | massimo.curro | [redacted] |
| 04/08/2008 - 12:59:24 | 87.23.147.68 | 192.168.91.70 | info@fmisicilia.it | [redacted] |
| 04/08/2008 - 12:59:25 | 62.101.89.32 | 192.168.91.107 | m.curro | [redacted] |
| 04/08/2008 - 12:59:27 | 62.101.89.32 | 192.168.91.70 | staffids@glauco.it | [redacted] |

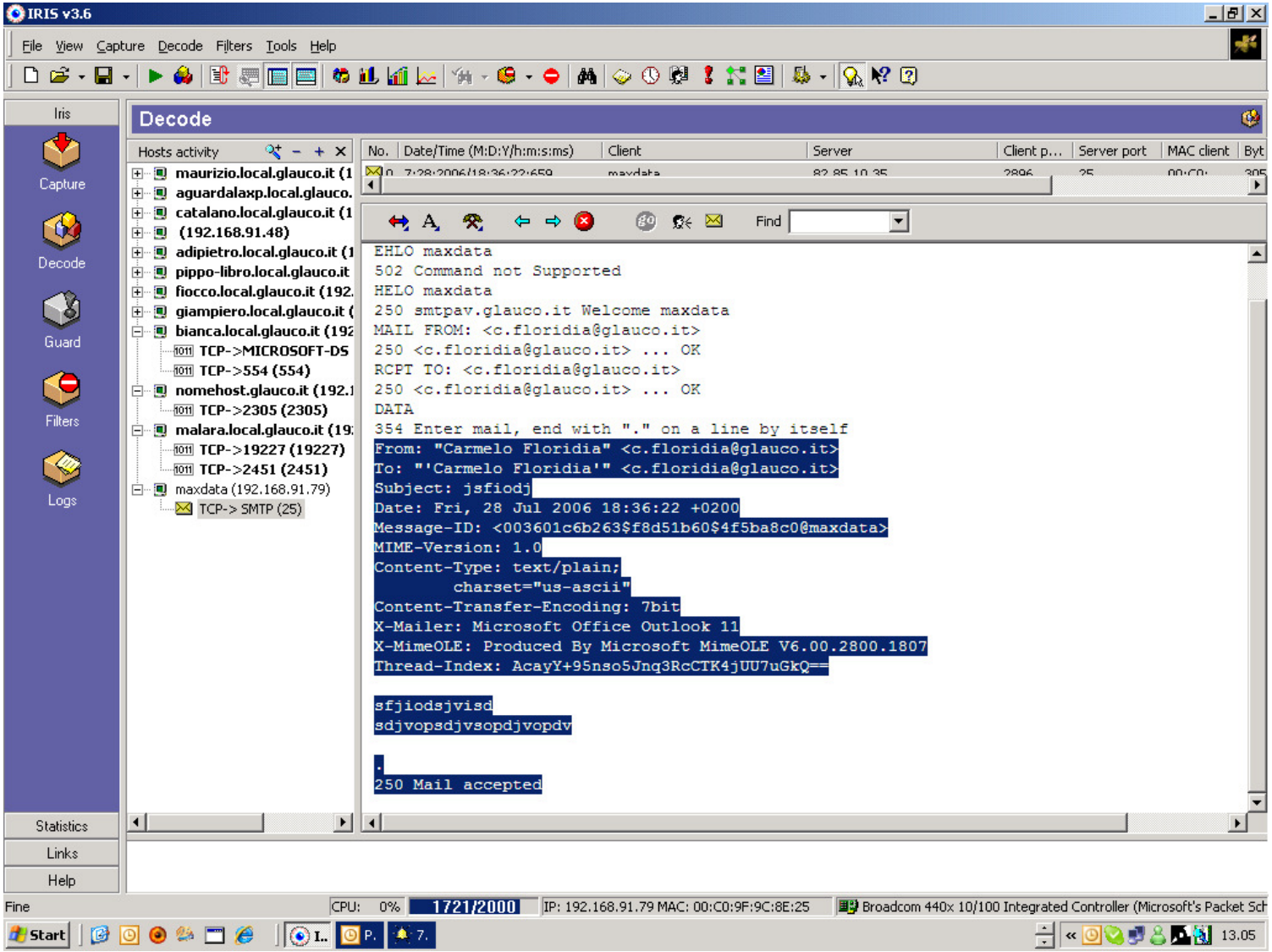
# Come funziona la posta elettronica



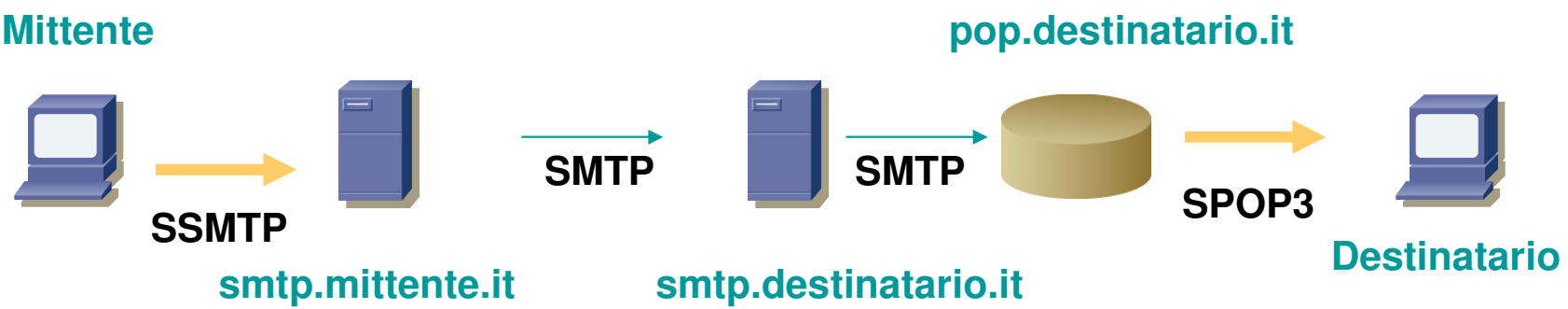

- **SMTP** Simple Mail Transfer Protocol
- **Il POP3** Post Office Protocol Version 3
- **IMAP4** Internet Message Access Protocol

- La password su questi protocolli viene trasmessa in chiaro

# Le email inviate sono catturabili



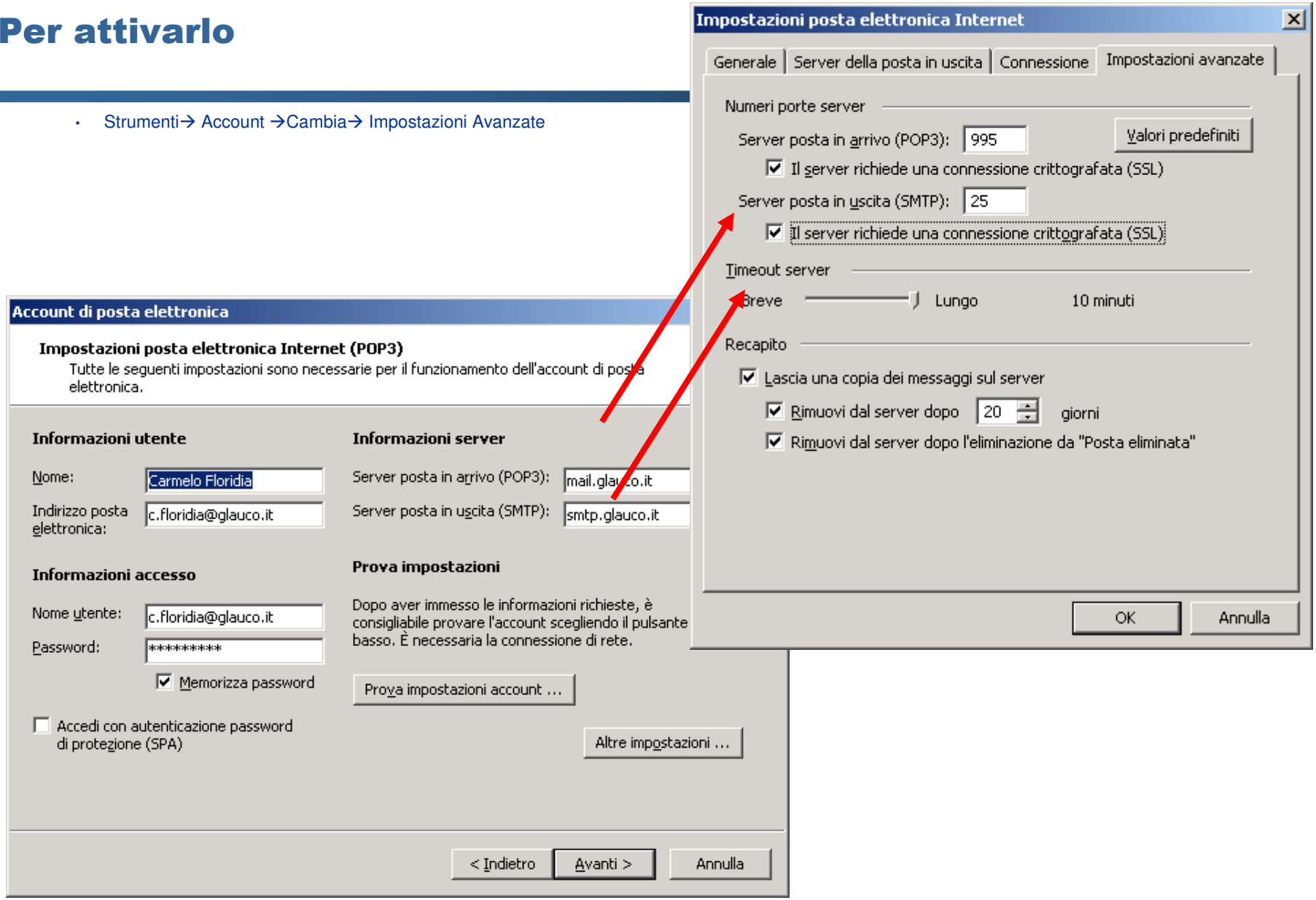
# Come funziona la posta elettronica protetta lato server



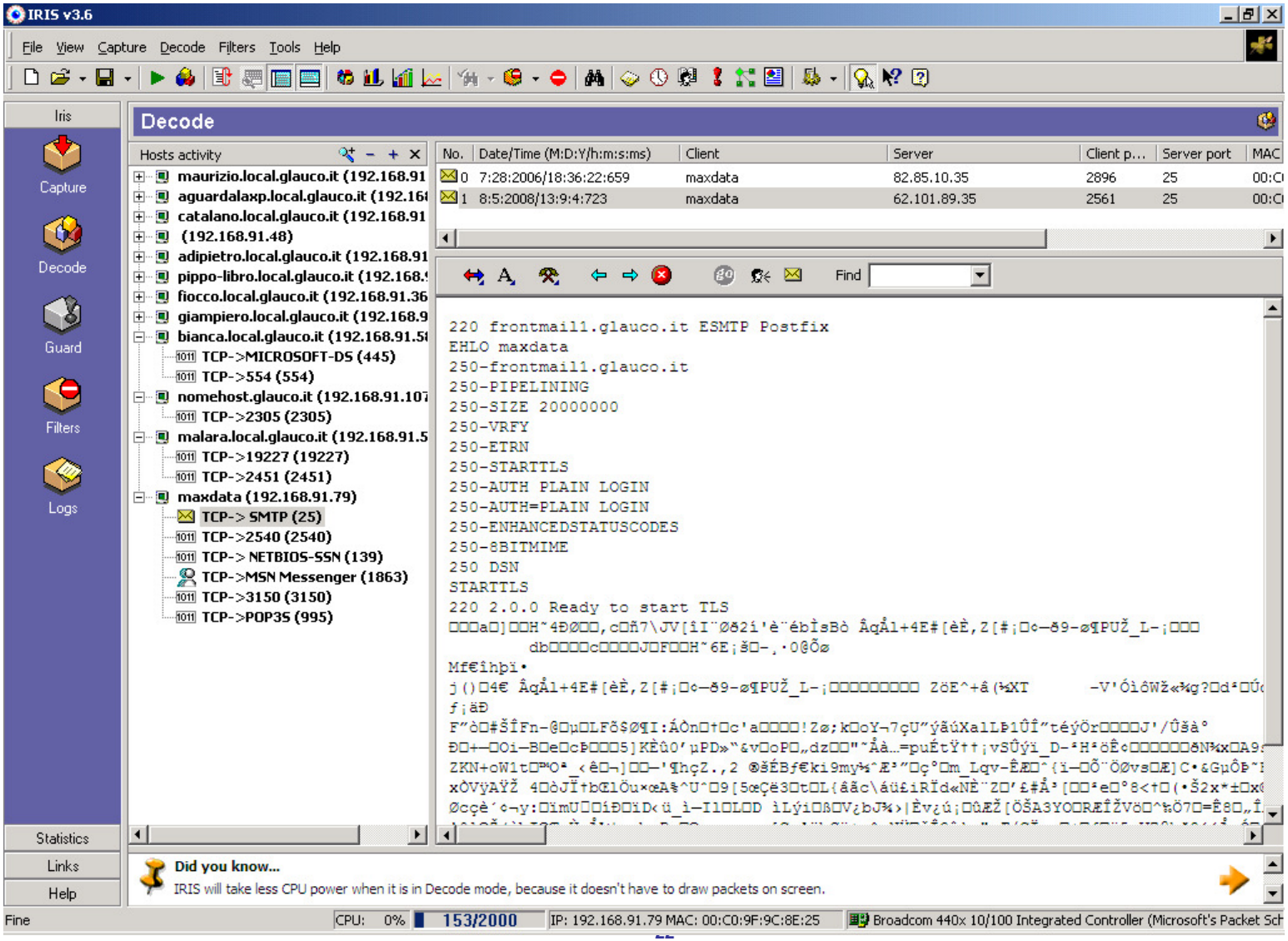

- **SSMTP** utilizza SSL per creare una connessione cifrata verso il server SMTP
- **SPOP3** utilizza SSL per creare una connessione cifrata tra il client ed il server POP
- Outlook ha gia la possibilità di utilizzare tali protocolli

# Per attivarlo

- Strumenti→ Account →Cambia→ Impostazioni Avanzate

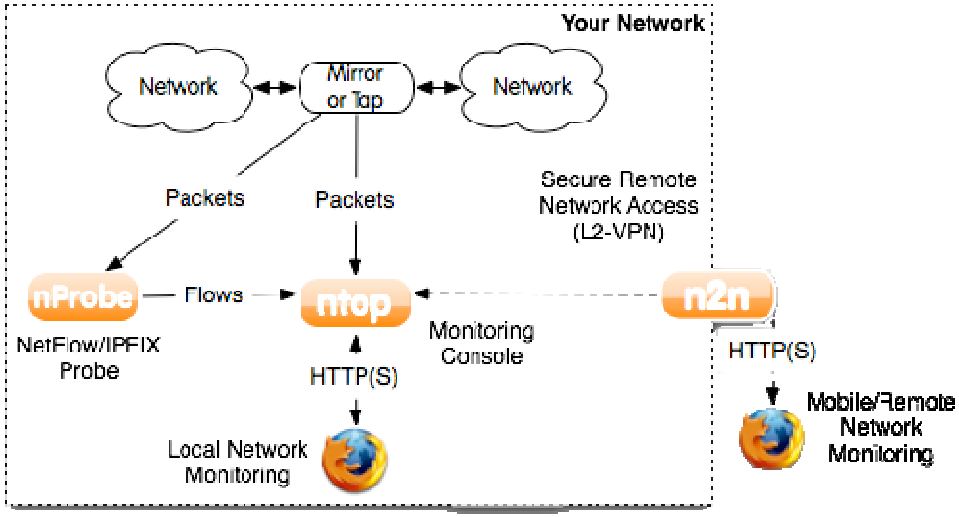


# La differenza



# Considerazioni finali sul monitoraggio

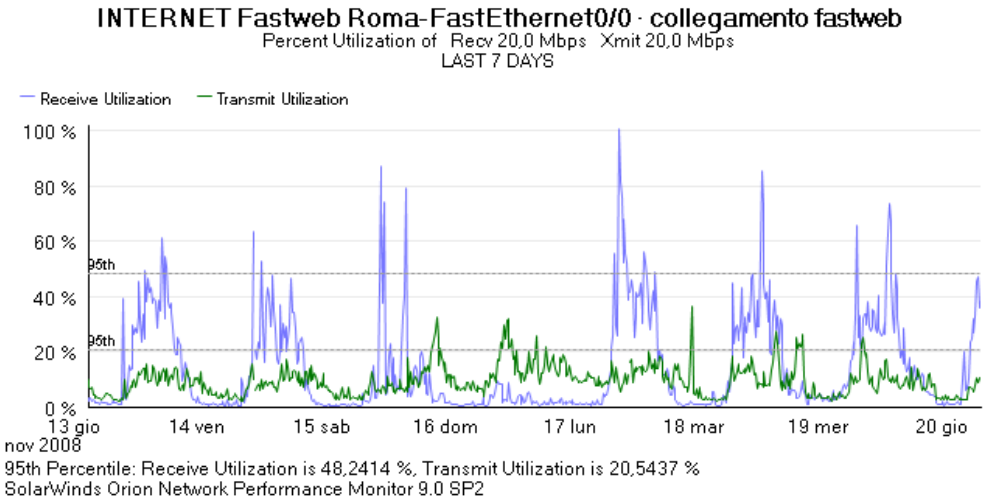
- In molti casi e' sufficiente il monitoraggio via SNMP e ping per rilevare anomalie di carattere macroscopico o per fornire elementi per avviare le attività di analisi con sniffer
- Mantenere aggiornato lo schema di rete e l'inventario puo' sembrare oneroso ma i benefici sono enorme
- Scorriamo insieme la SECTOOLS
  - http://sectools.org/
- Sniff sulla rete a seguito di segnalazione o costantemente (NTOP)
- Strumenti o Servizio?
  - Dipende dal tempo che si riesce a dedicare a queste attività che sono comunque impegnative e che hanno un beneficio indiretto (non direttamente percepito dall'utente finale)



# Protezione della navigazione e blocco del P2P

# Considerazioni sull'utilizzo della banda

- I sistemi di monitoraggio possono rilevare l'occupazione della banda.
- A seguito dell'analisi come abbiamo visto si puo' risalire alla tipologia di traffico
- Cosa fare In caso di abuso della banda dovuto a:
  - Download di file mediante p2p
  - Utilizzo di fileshareing su internet
    - Megaupload, rapidshare
  - Utilizzo di social network
    - Facebook, linked in



# Dal punto di vista tecnico:
# Introdurre meccanismi per ottimizzare l'utilizzo della banda

- Con i firewall tradizionali e' un po' complicato (si puo' ridurre marginalmente)
  - Non e' semplicissimo bloccare il P2P
    - Si possono bloccare le porte utilizzate dal p2p ma i sw cosentono il download anche dalla porta 80
  - Anche con i siti di filesharing la situazione non e' semplice
    - Si possono bloccare gli ip dei siti, ma ci sono mirror, proxy etc...
- I firewall di nuova generazione (UTM) consentono un analisi del traffico a livello di contenuto quindi:
  - Riconoscono se sulla porta 80 passa P2P
  - Hanno integrati o integrabili meccanimi di webfiltering per categoria con database aggiornati quotidianamente

**I firewall stabiliscono da che IP verso quale IP e su che porta**

**Gli UTM hanno maggiori funzionalità e potenzialità (tecnologia ASIC, elaborazione su HW)**

# Coinsiderazione sulle soluzioni

- **Prodotti commerciali**
  - Fortigate
  - Checkpoint
  - Zyxel
  - Sonicwall etc.

**L'aggiornamento e' automatico e prevede un canone annuo. Integrano in unica soluzine Firewall, VPN, IPS, AV, Web Filter e Antispam**

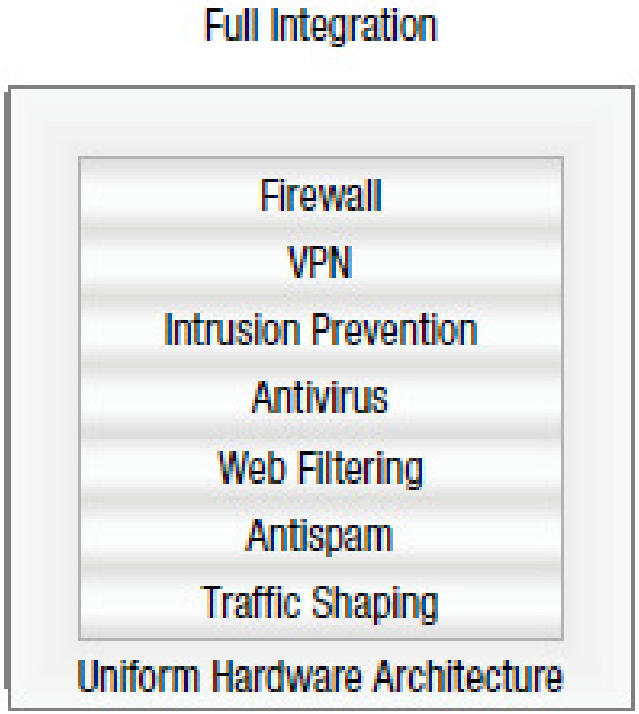
- **Prodotti Opensource**
  - ENDIAN
  - IPTABLES, DANSGUARDIAN, SQUID

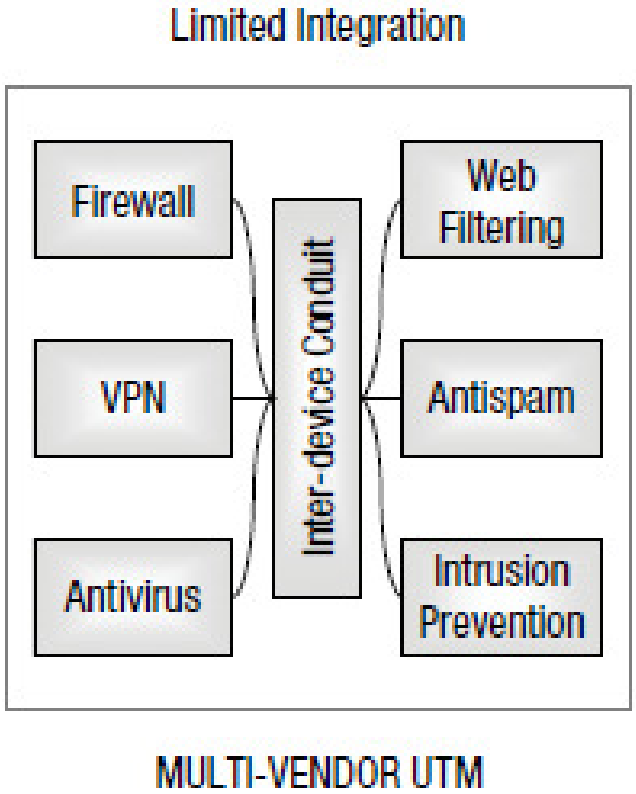
**Le versioni opensource non hanno l'upgrade automatico e l'integrazione deve essere fatta dall'utente finale. Ci sono versioni con supporto a pagamento**

- **Servizio**
  - Far gestire ad un centro specializzato le apparecchiature

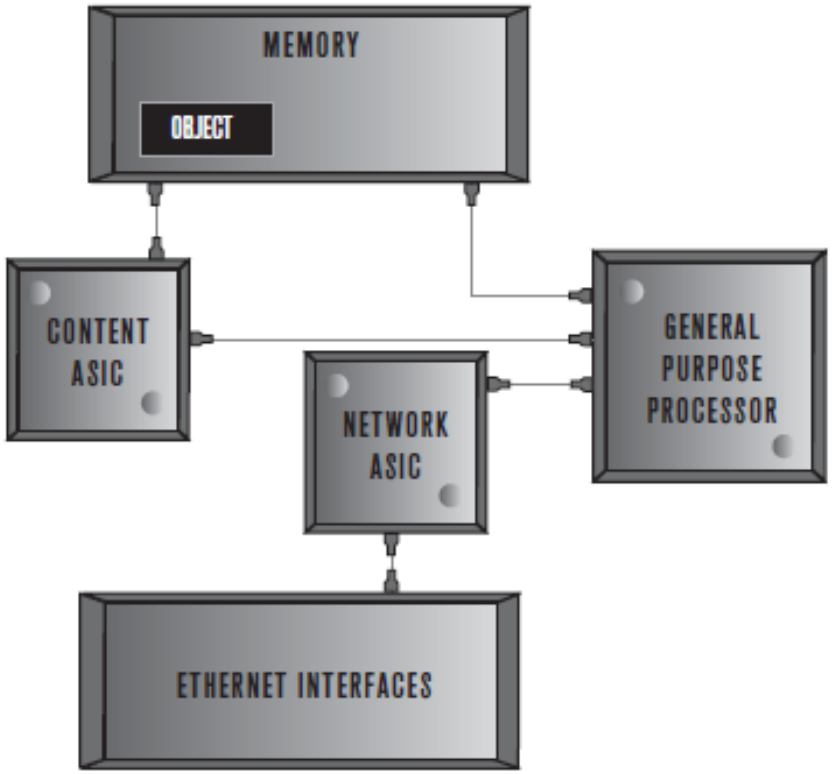
**Vantaggio di demandare a personale dedicato e qualificato questa attività. Possibilità di soluzini a 4 mani**

# Panoramica UTM Fortigate: tutto in un unico prodotto, no terze parti

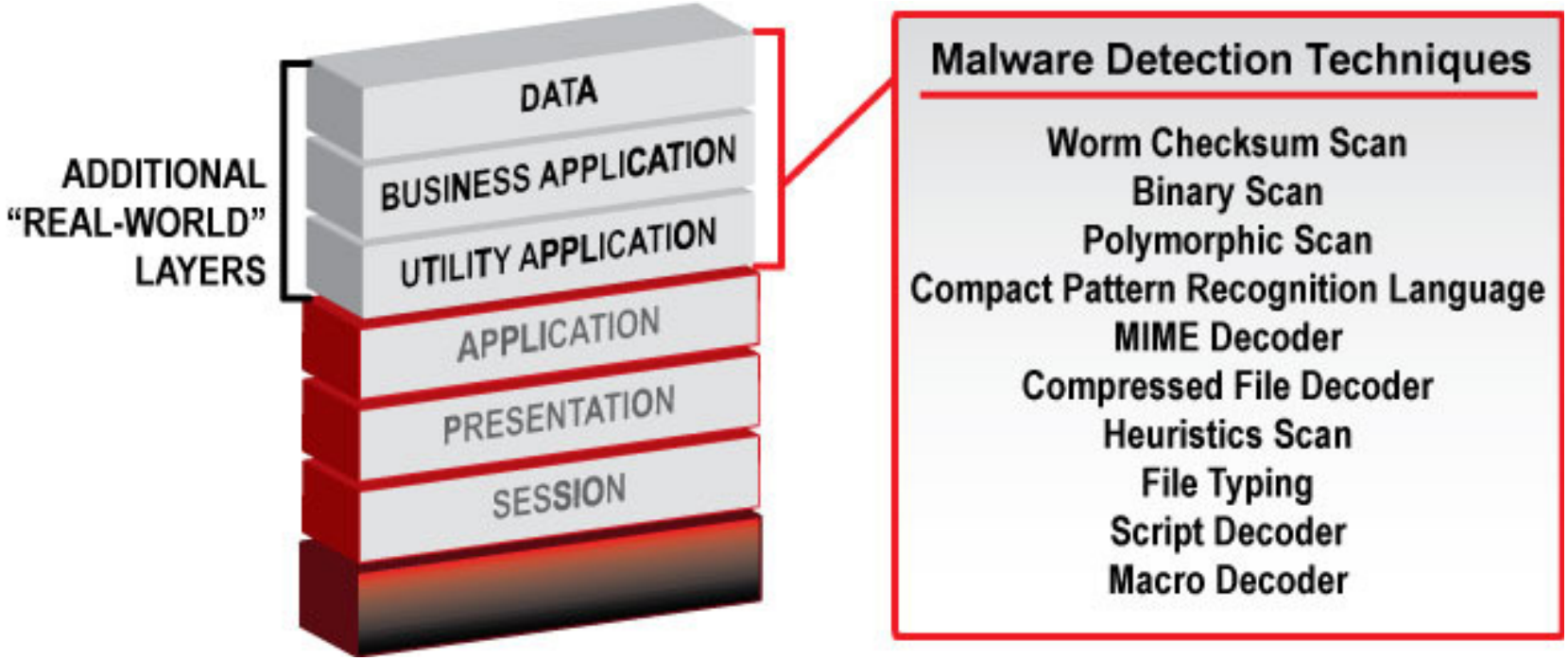


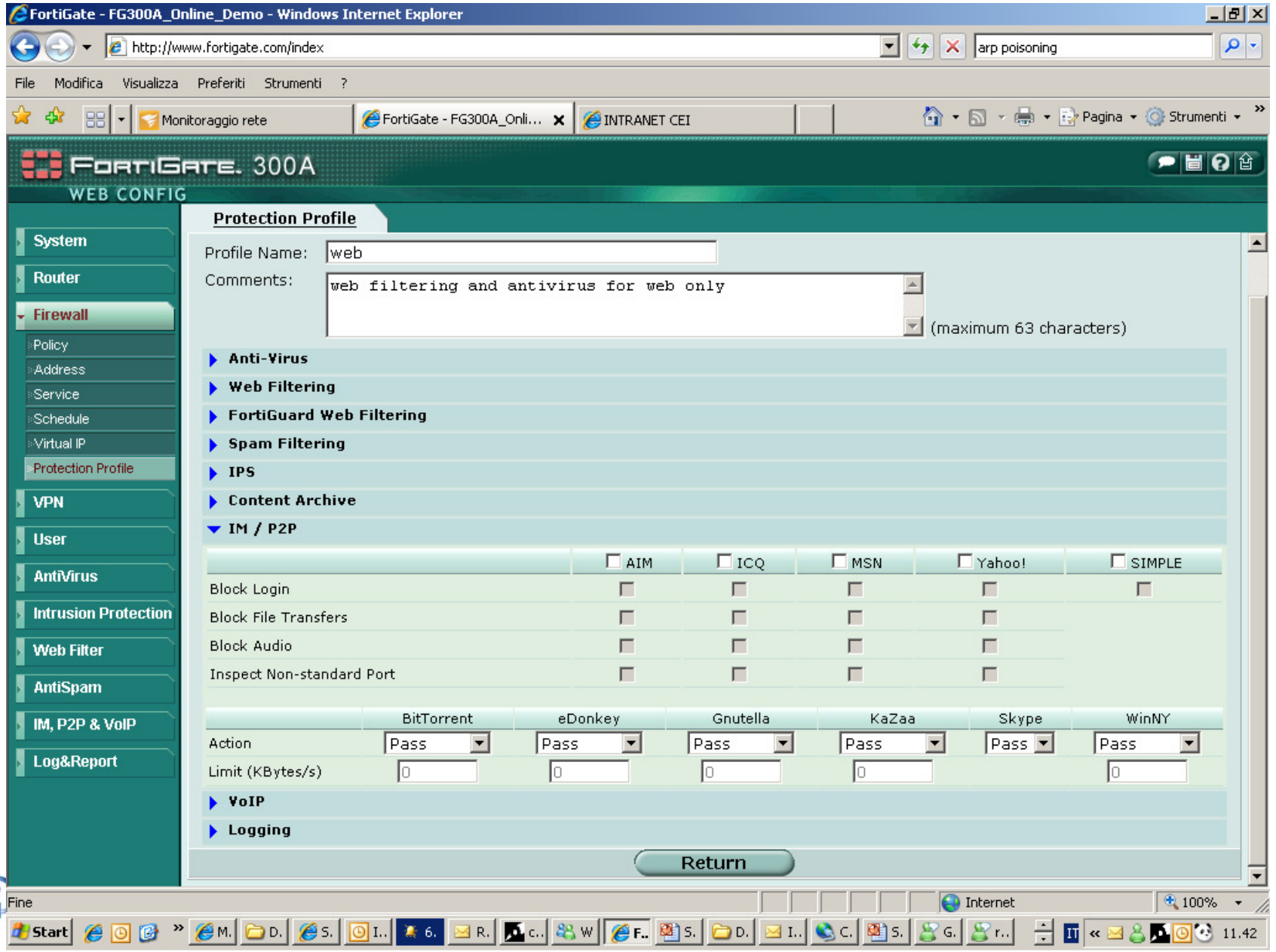
# Panoramica UTM Fortigate:Tecnologia ASIC -> maggiori prestazioni



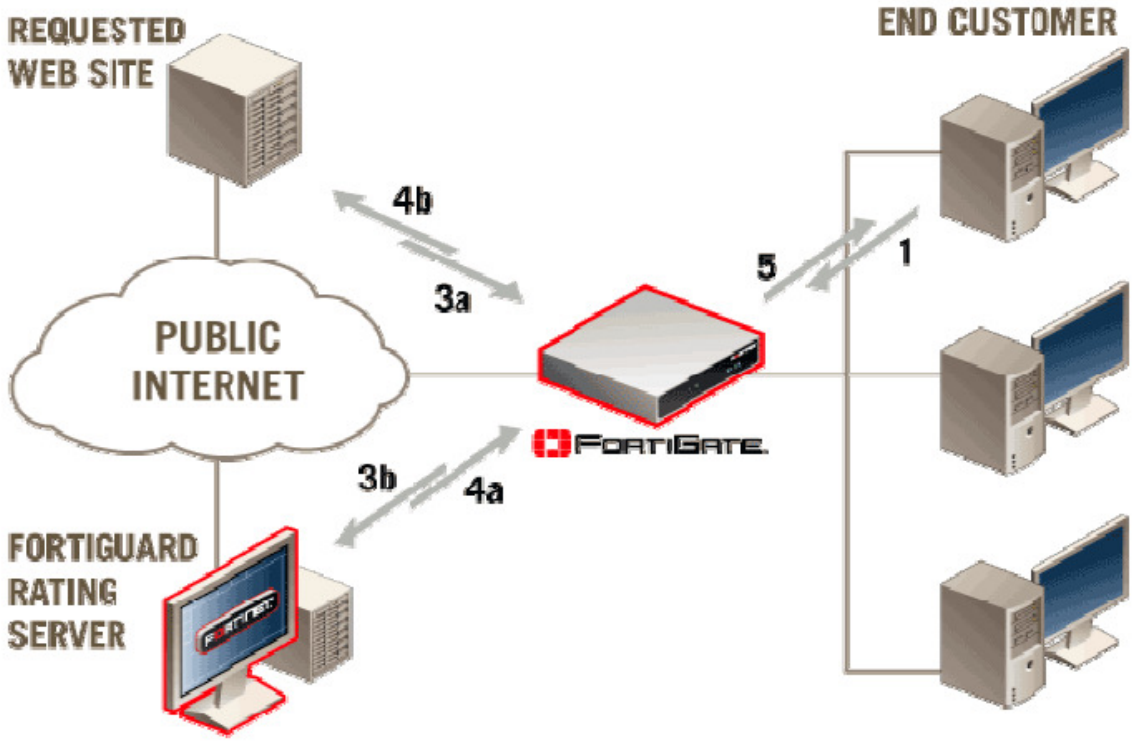
# Analisi piu' ad alto livello



# Possibilità di configurare il blocco o delle limitazioni sul P2P



# Web Filtering – Architettura con Fortigate

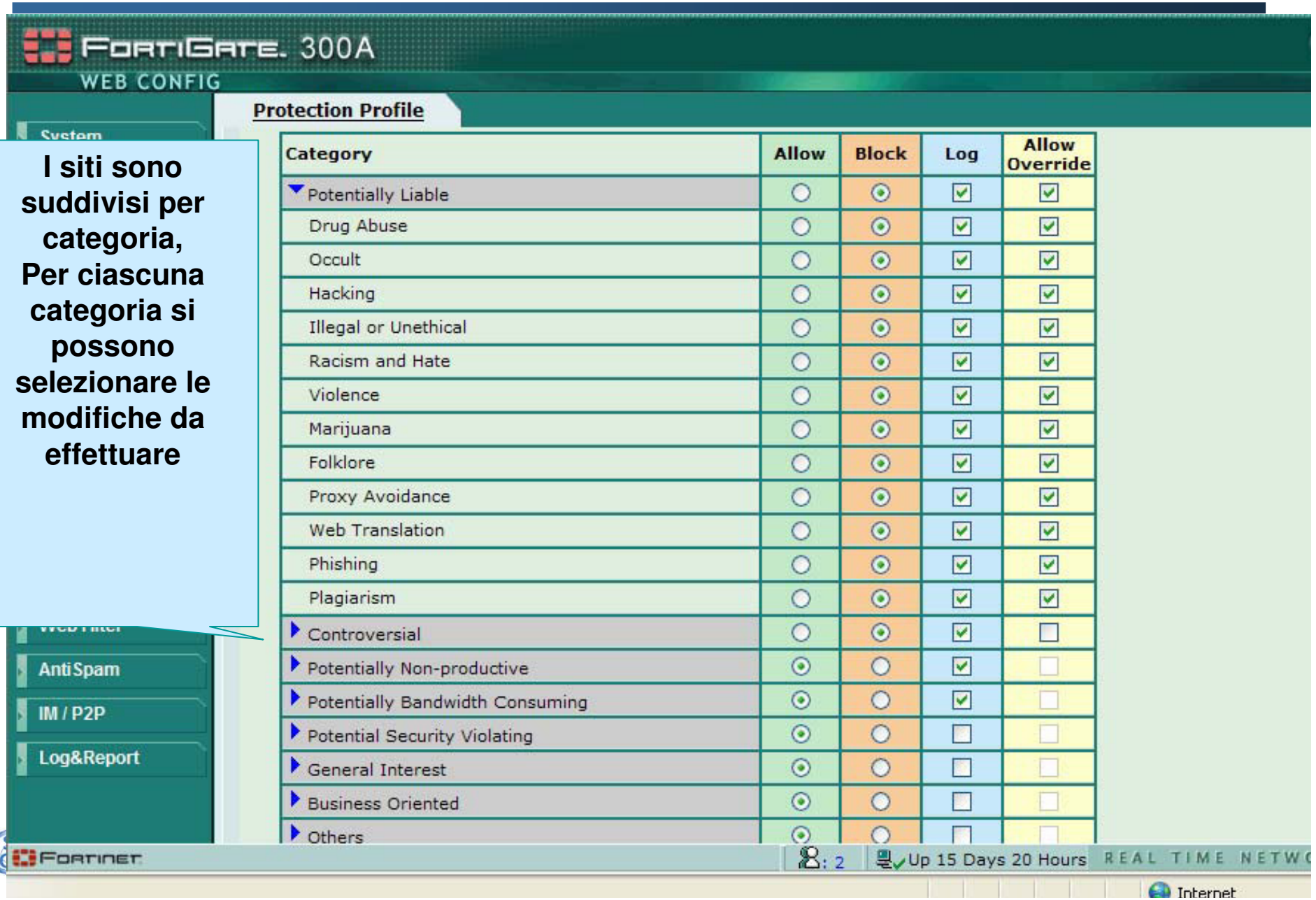



Le richieste sono inviate con datagram UDP al centro fortigate che manutiene un DB aggiornato.

La risposta viene tenuta in cache

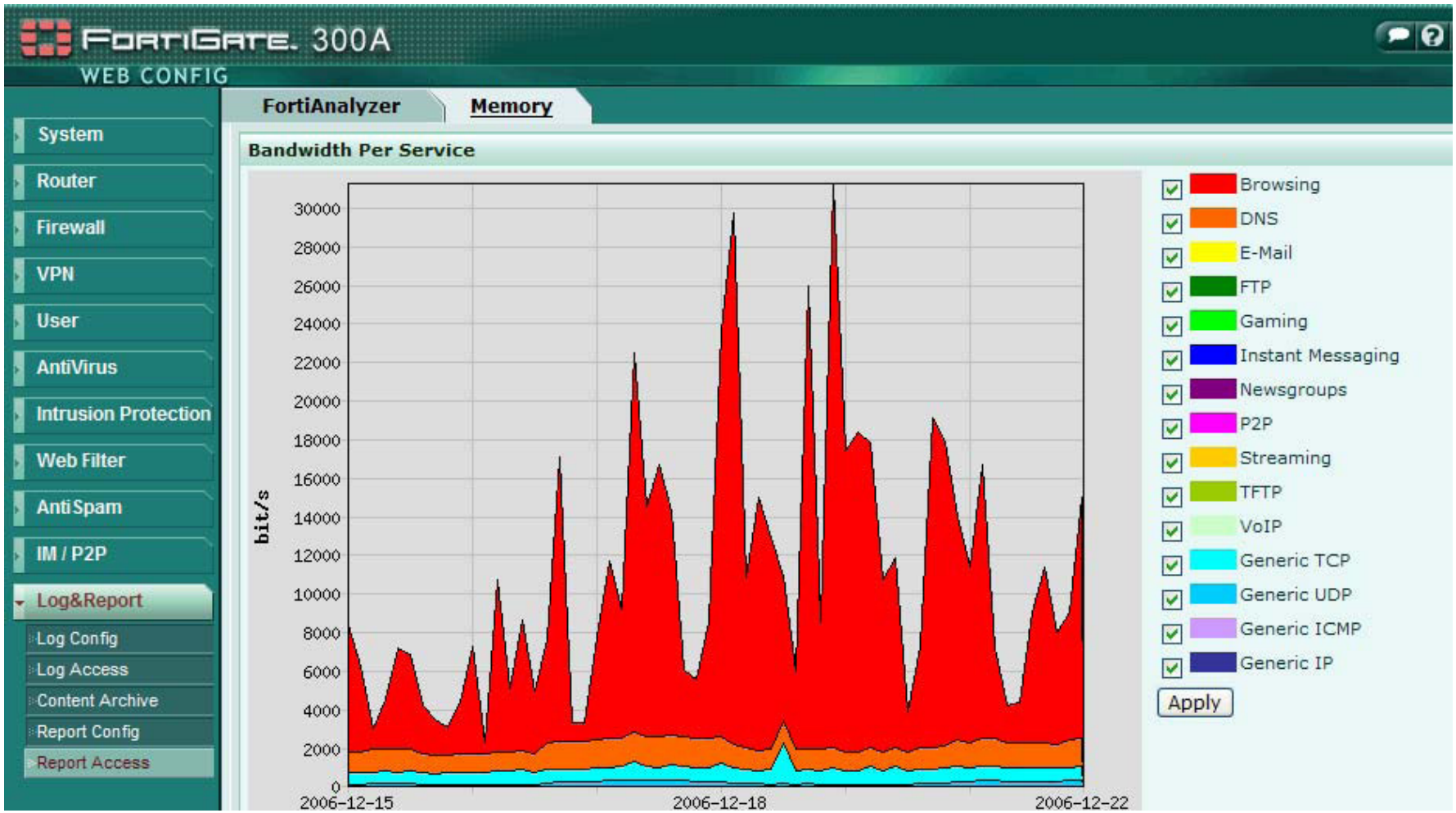
Il meccanismo e' simile al dns

# Web Filtering - Configurazione




I siti sono suddivisi per categoria,
Per ciascuna categoria si possono selezionare le modifiche da effettuare

# UTM – anche reportistica e monitoraggio

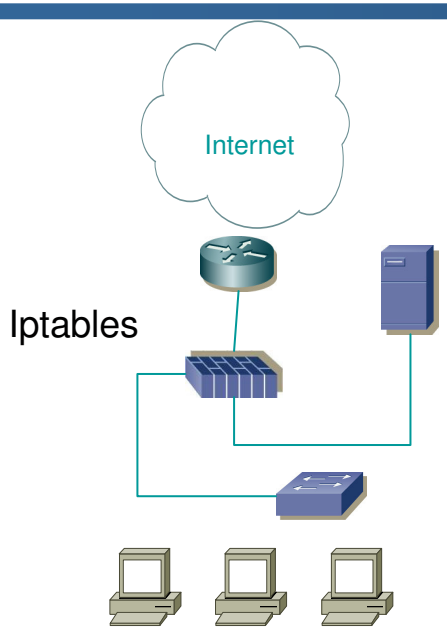


## DEMO On Line

- https://www.fortigate.com
- demo/fortigate

- http://demo.endian.com
  Your Login: admin
  Your Password: efw_demo

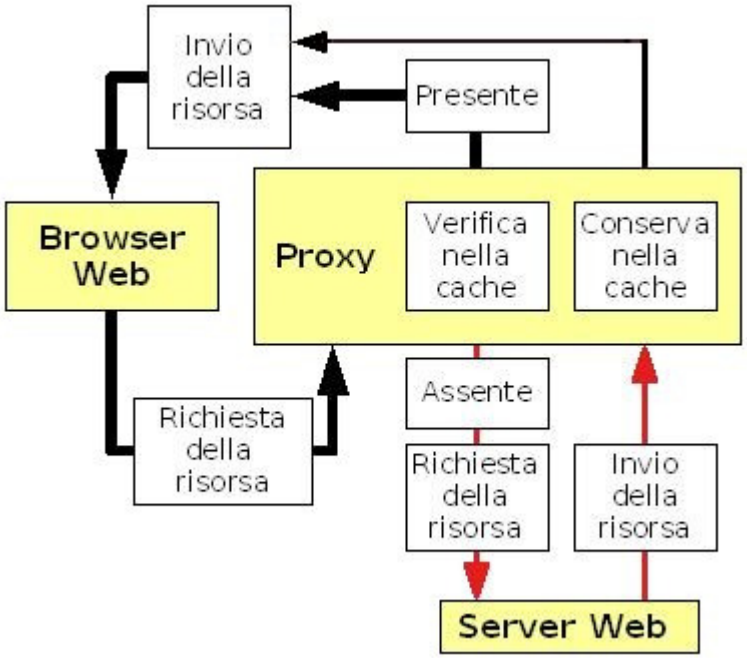
# Webfiltering: architettura con Opensource




Squid+

Dansguardian

(possono stare anche su macchine separate)




Configurazione:

-**Sul firewall**

-Tutto il traffico sulla porta 80 passalo sulla porta di dansguardian

-**Su dansguardian**

-Il traffico consentito mandalo a squid

- File di configurazione a riga di comando

- Possibilità di avere gli upgrade delle liste a pagamento

**http://dansguardian.org/**

**http://urlblacklist.com/**

# Aspetti legali

## Principale quadro normativo di riferimento

- D.lgs. 196/2003
- Misure minime di sicurezza Allegato B D.lgs. 196/2003
- *Legge 23 dicembre 1993 n.547 Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica“*
- Lavoro: le linee guida del Garante per posta elettronica e internet *Gazzetta Ufficiale n. 58 del 10 marzo 2007*

- **Garante Privacy - Deliberazione n.13 del 1 marzo 2007 (G.U. 10 marzo 2007 n.58)**

  Il Garante emana un provvedimento generale poiché "dall'analisi dei siti web visitati si possono trarre informazioni anche sensibili sui dipendenti e i messaggi di posta elettronica possono avere contenuti a carattere privato. Occorre prevenire usi arbitrari degli strumenti informatici aziendali e la lesione della riservatezza dei lavoratori" .

INTERESSI DA TUTELARE

Uso arbitrario degli strumenti aziendali (perdita di produttività e responsabilità)

Lesione della riservatezza dei lavoratori

## I 2 principi del bilanciamento degli interessi:

- Rilascio preventivo di idonea informativa:

  L'Autorità prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli

- Utilizzo di un disciplinare interno

  Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

## Preliminarmente dal punto di vista organizzativo è necessario che:

- si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
- si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

## Consigli sul modo di procedere:

1. Definire le modalità di utilizzo della rete internet;
2. Definire le modalità di utilizzo della posta elettronica e prefigurare delle soluzione atte a garantire la continuità dell'attività lavorativa;
3. Determinare la misura dei controlli del datore di lavoro;
4. Stabilire le conseguenze in caso di utilizzo indebito.

# Definire le modalità di utilizzo della rete internet

Definire nel documento di privacy policy per quali fini ed in che modo è utilizzabile il collegamento internet, per quali fini, cosa è assolutamente vietato e quali sono le responsabilità.

Nella Deliberazione n.13 del 1 marzo 2007 **il Garante prescrive di:**

- individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.

Nello stesso documento andranno specificati gli strumenti di web filtering adottati e come eventualmente sono trattati i dati acquisiti attraverso tali strumenti, distinguendo:

I dati trattati in forma aggregata

I dati trattati in forma individuale

## Definire le modalità di utilizzo della posta elettronica e prefigurare delle soluzione atte a garantire la continuità dell'attività lavorativa

La casella di posta elettronica aziendale *deve essere utilizzata* per finalità lavorative evitando l'invio di messaggi personali o la partecipazione a dibattiti, forum o mail list che non siano riconducibili alla stessa attività lavorativa.

In caso di assenze programmate (ferie, trasferte etc.) si dovrebbe mettere a disposizione una funzionalità di sistema che consenta di inviare automaticamente messaggi di risposta contenenti le coordinate(ulteriori indirizzi email, numeri telefonici etc.) di altro soggetto o, più in generale, dell'Azienda.

In caso di assenza non programmata(es. malattia), il lavoratore non sia in grado di attivare la succitata il Titolare del Trattamento, perdurando l'assenza per più giorni lavorativi dispone, se lo ritiene indispensabile per le esigenze dell'Azienda, l'attivazione di analogo accorgimento da parte del Responsabile del Trattamento dei dati designato, previa idonea informativa

## Determinare la misura dei controlli del datore di lavoro

Bisogna evitare qualsiasi interferenza ingiustificata sui diritti e sulle libertà dei lavoratori in relazione ai principi della:

PERTINENZA

NON ECCEDENZA

# QUANDO POSSONO ESSERE EFFETTUATI I CONTROLLI:

In caso di comportamenti anomali che espongano l'Azienda a situazioni di pericolo o eventi dannosi - non altrimenti impedibili con gli accorgimenti tecnici previsti dalla stessa azienda - adotta le misure di controllo atte a verificare codesti comportamenti, ovvero per le verifiche sulla funzionalità e la sicurezza del sistema.

**In prima istanza il datore di lavoro provvederà a un controllo generale su dati aggregati, riferiti all'intera struttura lavorativa od a una o più aree.**

I controllo: generale ed anonimo

Se accertato un utilizzo anomalo degli strumenti aziendali

un avviso generalizzato preannunciando successivi controlli, ancora generali, per verificare la correzione dell'anomalia(II controllo)..

**In assenza di successive anomalie no controlli su base individuale.**

III controllo: individuale

Se le anomalie non risultassero corrette, il datore di lavoro rilascerà preventiva e dettagliata informativa ai lavoratori interessati, chiarendo la necessità di effettuare controlli individuali e specificando i trattamenti dei dati che possono riguardarli.

## Stabilire le conseguenze in caso di utilizzo indebito

**Occorre prevedere prima le sanzioni eventuali in relazione alla condotta**

La violazione delle prescrizioni può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.

## Misure tecnologiche da applicarsi rispetto alla navigazione in internet:

- l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
- il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- la graduazione dei controlli.

## Misure tecnologiche da applicarsi rispetto alla posta elettronica:

- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli

## Punti di accesso internet:

- Autenticare
- Informare
- Regolamentare
- Conservare i dati acquisiti

# Autenticare

**Oggetto: Richiesta autorizzazione alla navigazione su INTERNET ed informativa ai sensi della legge196/2003**

Il sottoscritto……. Nato a ……..……il …….residente in……Via …….. numero di telefono……identificato a mezzo di ……..,in qualità di ******"), richiede l'abilitazione alla navigazione su INTERNET ed all'utilizzo della POSTA ELETTRONICA.

Il sottoscritto è a conoscenza del fatto che l'utilizzo di INTERNET e dei servizi **sono sotto la propria responsabilità**, ed esonera *** da ogni e qualsiasi responsabilità per un eventuale uso improprio di tali strumenti.

Il sottoscritto dichiara a tal fine**:**

**di aver preso visione dell'informativa ed aver prestato il consenso al trattamento dei dati personali** come specificato nell'allegato A

**di aver preso visione e di accettare integralmente le condizioni del regolamento interno** riguardante l'utilizzo delle postazioni di lavoro e della navigazione INTERNET e della POSTA ELETTRONICA (allegato B)

- Nome e Cognome (in stampatello)…….
- Documento di riconoscimento
- In qualità di ……..
- Firma leggibile……..
- Luogo, Data……..

# Informare:

***ALLEGATO A***

**INFORMATIVA ai sensi dell'art.13 D.lgs. 196/2003**

*** desidera preventivamente informarLa, ai sensi dell'art. 13 del D. Lgs. n.196/03, del fatto che il trattamento dei dati forniti, sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti. Pertanto Le forniamo le seguenti informazioni sul trattamento dei Suoi dati personali che intendiamo effettuare:

il trattamento dei dati richiesti ha le seguenti finalità:

- autorizzazione per la navigazione INTERNET;
- verifica utilizzo nel rispetto del regolamento interno (anche mediante l'utilizzo di strumenti informatici solo per inibire la navigazione verso siti ritenuti pericolosi e con contenuto immorale);
- comunicazione ai responsabili di *** dei risultati delle verifiche effettuate sul rispetto delle norme comportamentali.

il trattamento sarà effettuato ad opera di soggetti appositamente incaricati nel rispetto delle procedure previste nel Documento Programmatico sulla Sicurezza.

il conferimento dei Suoi dati è per Lei obbligatorio per i seguenti motivi: regole interne di buona condotta e sicurezza delle postazioni di lavoro. Il mancato conferimento comporta l'impossibilità di utilizzare la connessione internet offerta da *** durante lo svolgimento dei corsi.

i Suoi dati personali potranno essere comunicati a soggetti terzi, preventivamente individuati, che potranno avere il compito di collaborare con ***per le finalità di cui al punto 3 lett.a).Non saranno invece oggetto di diffusione.

il titolare del trattamento è *****.

Il responsabile del trattamento è ***

Lei potrà far valere i Suoi diritti, così come disciplinati dall'art.7 del D. Lgs. n. 196/03, che riportiamo sotto integralmente, rivolgendosi in qualunque momento al responsabile del trattamento come individuato nella presente informativa.

**CONSENSO PER IL TRATTAMENTO DEI DATI PERSONALI**

Il/La sottoscritto/a, acquisite le informazioni di cui all'articolo 13 del D. Lgs. n. 196/03, attesta il proprio libero consenso affinché il titolare proceda al trattamento dei propri dati personali come risultanti dalla presente scheda informativa.

Luogo e Data …….

Firma leggibile .....

***ALLEGATO B***

**REGOLAMENTO PER L' UTILIZZO DI POSTAZIONI DI LAVORO ED INTERNET**

La progressiva diffusione di nuove tecnologie informatiche e di INTERNET espone *** a rischi di un coinvolgimento legale. In particolare si segnalano i temi relativi alla diffamazione, alla discriminazione razziale, alla violazione dei diritti dei copyright, alle molestie sessuali, alla pubblicazione di materiale osceno, alla protezione dei dati e delle informazioni, alla negligente trasmissione di virus, alla involontaria formazione di contratti, ecc.

Per ridurre questi rischi *** ha già provveduto all'adozione delle misure di sicurezza informatica necessarie per la salvaguardia della sicurezza della rete, ed all'adozione delle misure minime previste per il trattamento di dati personali in conformità al testo unico 196/2003.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto con l'Ente stesso, si ritiene utile adottare un regolamento comune, diretto ad evitare comportamenti inconsapevoli e/o scorretti.

Sono quindi di seguito descritte le regole interne riguardanti l'utilizzo delle postazioni di lavoro e dei servizi INTERNET e POSTA ELETTRONICA.

La navigazione in INTERNET sarà consentita solo a chi abbia dato l'autorizzazione al trattamento dei nuovi dati con la firma e l'accettazione delle condizioni contenute nel presente documento. La navigazione effettuata senza aver preventivamente sottoscritto il presente documento è da ritenersi illecita e contro la volontà di **** ed esonera lo stesso Ente da ogni e qualsiasi responsabilità nascente dalla stessa.

Durante la navigazione in INTERNET e l'utilizzo della POSTA ELETTRONICA è vietato:

- Visitare siti con contenuto violento, immorale e pornografico e qualsiasi altro sito che offende il " normale senso del pudore" ;
- Fare o spedire osservazioni, proposte o materiali indecenti su INTERNET ;
- Comunicare in rete in modo offensivo, ingiurioso e diffamatorio;
- Scaricare qualsiasi software o file senza l'utilizzo di misure di sicurezza contro i virus approvate dall'Istituto ;
- Scambiare materiale contrario alla morale e all'ordine pubblico o con lo scopo di recare molestia alla quiete pubblica o privata , di recare offesa, o danno diretto o indiretto a chiunque;
- Intercettare, impedire, interrompere illecitamente comunicazioni informatiche o telelmatiche o rilevarne il contenuto;
- Violare, sottrarre o sopprimere la corrispondenza telematica tra terzi;
- Violare la privacy degli altri utenti della Rete ;
- Interferire intenzionalmente nelle normali operazioni dei sistemi, inclusa la propagazione di virus e la generazione di alti volumi di traffico di rete ( ad esempio utilizzando strecaming video o audio e software di connessione P2P quali Kazaa , WinMix, Emule e/o equivalenti ) che ostacolano sostanzialmente altri utenti nell'utilizzo della rete;
- Esaminare , cambiare o utilizzare file, username di altre persone senza esplicita autorizzazione .
- La navigazione in INTERNET, il caricamento e/o lo scaricamento di eventuali programmi, contenuti o informazioni della Rete avviene sotto la responsabilità dell'utilizzatore del servizio internet.
- Si ricorda che il software disponibile sulla rete INTERNET, nonché il file MP3, multimediali, fotografie, ecc, anche se accessibili e disponibili nelle diverse forme freeware, shareware, demo, trial, etc. sono soggetti alla normativa vigente sul trattamento dei diritti d'autore.
- Lo scarico e l'installazione di tale software, lo scarico di file MP3, multimediali, fotografie sulla propria postazione da parte degli utenti costituisce una presa in carico delle responsabilità legali implicite dell'atto sia sotto l'aspetto civile che penale.

## Conservare i dati acquisiti

- Archiviare e trattare i dati acquisiti secondo le previsioni del D.Lgs.196/2003 e in ossequio di quanto contenuto nell'informativa rilasciata

# Collegamento tra sedi remote (VPN)

# Collegamento remoto tra le sedi : Ipotesi

Altri uffici/enti collegati

Altri uffici/enti collegati

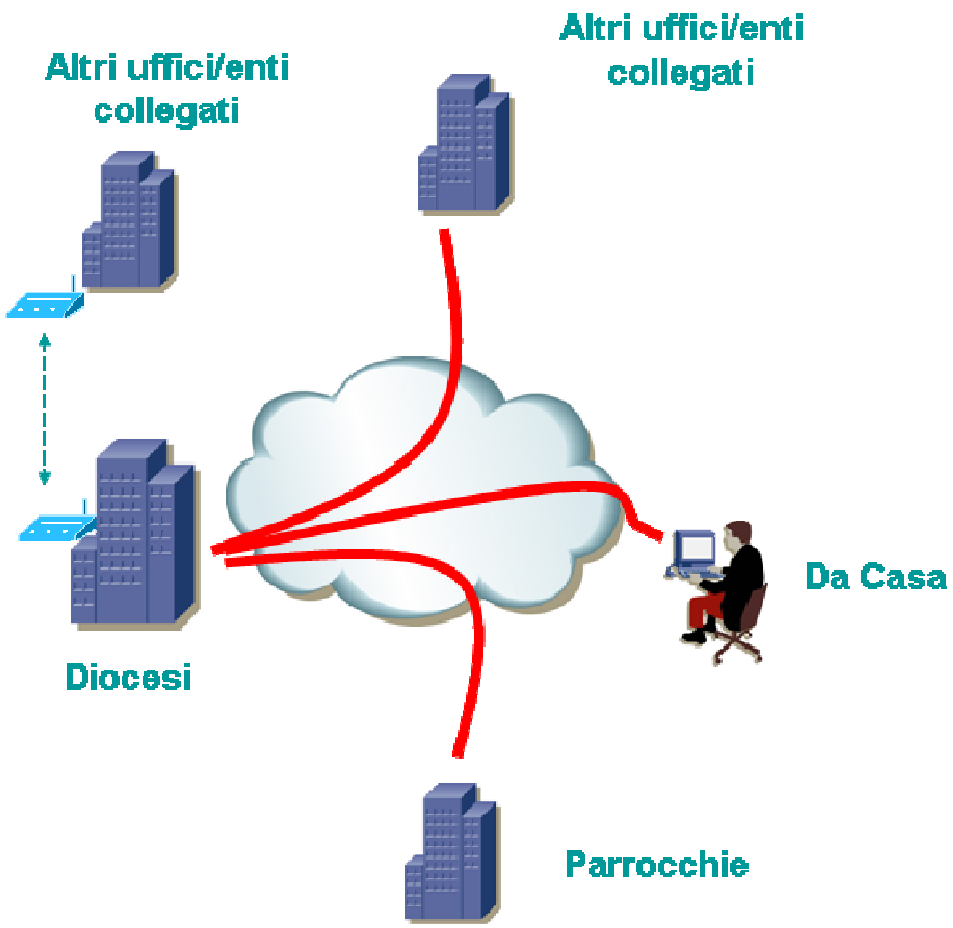
- Esigenza:
  - **Collegare le sedi tra di loro per:**
    - Condivisione documenti
    - Accesso servizi di rete locale (backup, antivirus…)
    - Accesso a Stampanti
  - **Accesso in modo sicuro da casa o da fuori ufficio**
    - Accesso a documenti su server
    - Accesso per interventi da remoto

Diocesi

Da Casa

Parrocchie

# Collegamento remoto tra le sedi : Ipotesi




- **Se la distanza lo permette e c'e' visibilità tra le sedi si puo' realizzare un bridge wireless**
- **Utilizzare il collegamento internet per realizzare una VPN**
  - **REQUISITI**
    - **Nella sede centrale:**
      - apparato su cui chiudere le VPN
      - Melgio IP pubblico riservato alla VPN
      - Attenzione al NAT
    - **Nelle sedi periferiche:**
      - Apparato per realizzare la VPN con la sede centrale
    - **Sui pc remoti**
      - Software per realizzare la VPN
- **VPN mediante MPLS**
- **Aprire gli IP pubblici**
  - Molto rischiosa (il traffico viaggia in chiaro su internet)
  - Servisi limitati
  - Opportuno avere ACL e limitare questa soluzione ad esigenze molto particolari

# Qualche dettaglio

Realizza VPN a livello **network** attraverso l'uso di tre protocolli

**IKE** (**Internet Key Exchange**):

- serve per autenticare l'interlocutore e per negoziare ed aggiornare gli algoritmi e le chiavi di crittografia/autenticazione da utilizzare nei dati da trasmettere in VPN
  - (porta UDP sorgente e destinazione = 500)

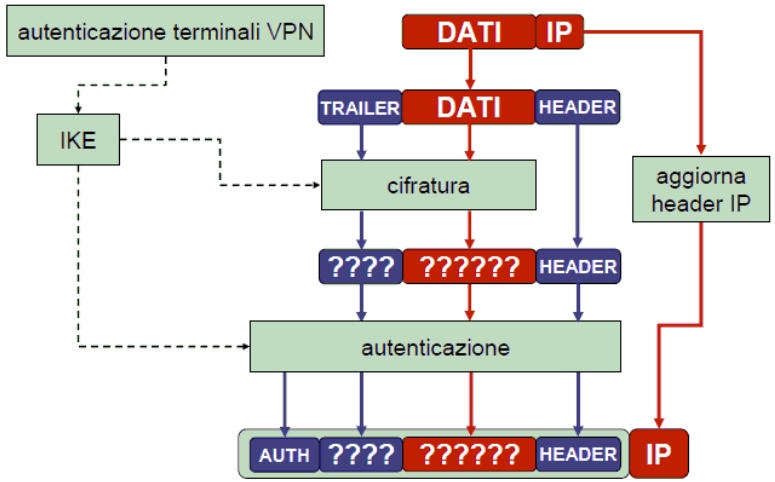
**AH** (**Authentication Header**)

- fornisce l'autenticazione dei pacchetti trasmessi in VPN garantendo
  - integrità ed autenticità dei dati
  - identità del mittente

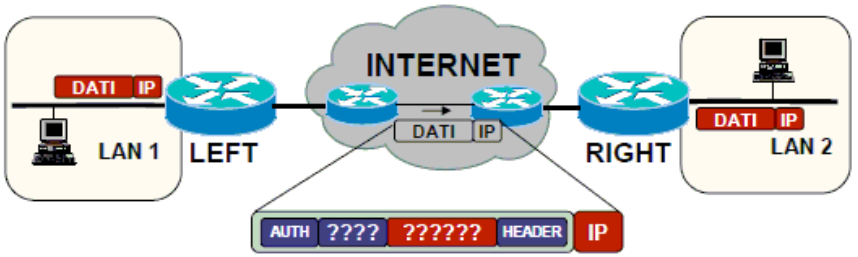
**ESP** (**Encapsulating Security Payload**)

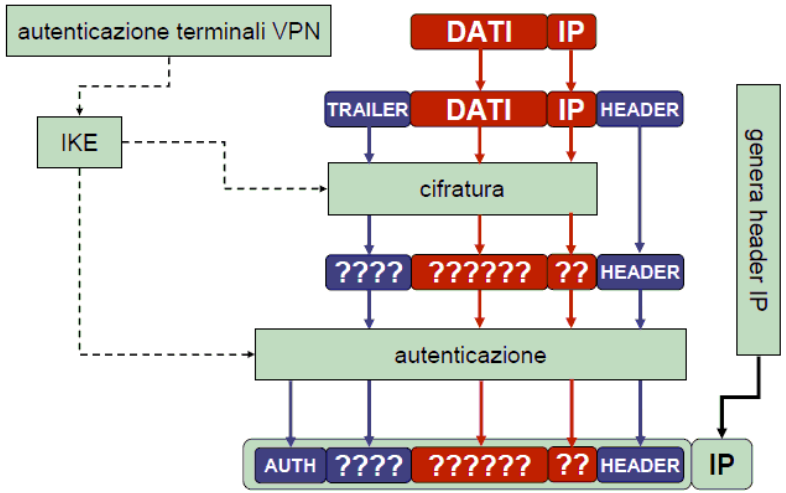
- oltre a fornire autenticazione come in AH, garantisce anche la
- riservatezza delle informazioni tramite crittografia
  - modalità **trasporto** o **tunnel**

# Tunneling e transport

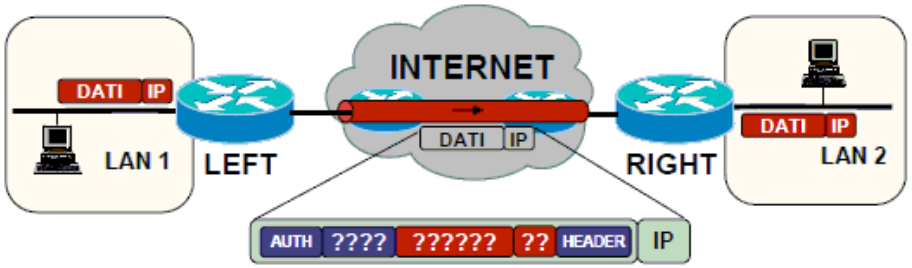



- **Transport (IP non incapsulato)**




- **Tunneling (IP Incapsulato)**



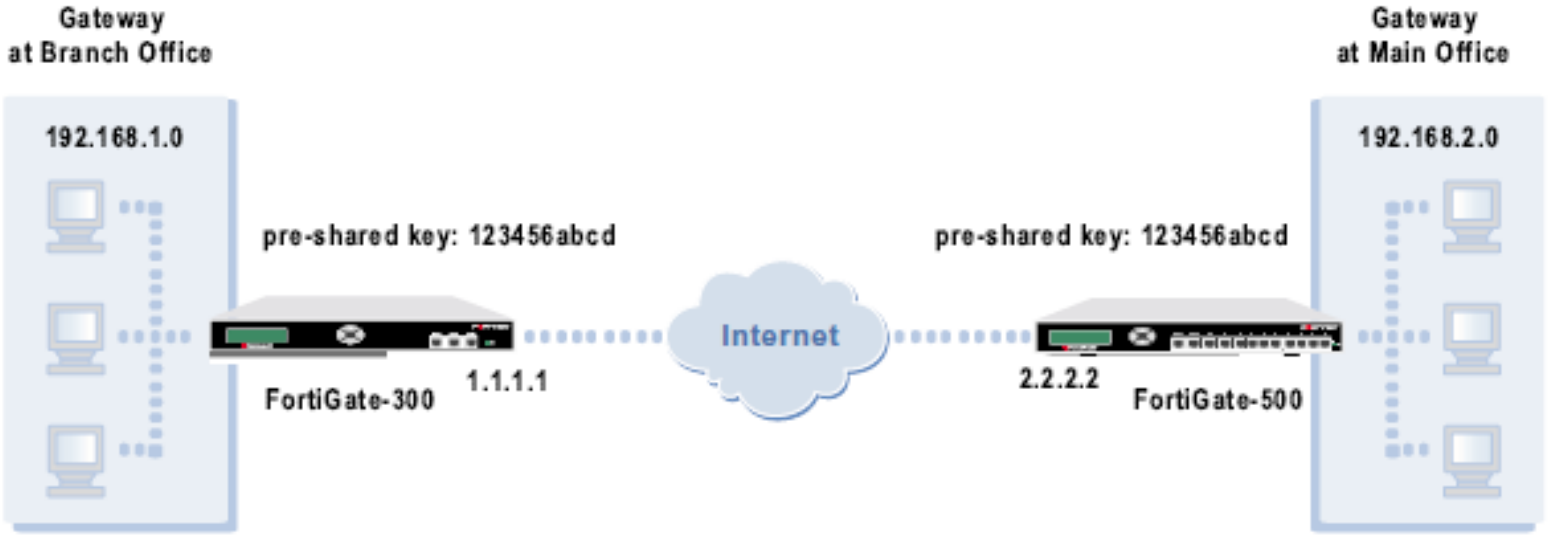
# Collegamento remoto tra le sedi : Tecnologia

Collegamento Site 2 Site tra la sede remota e la sede centrale:

-Attenzione all'indirizzamento per evitare overlap

-Considerazioni su banda e trasferimenti dati su collegamento asimmetrico

-Modalità di funzionamento con pre-shared key o anche con certificati



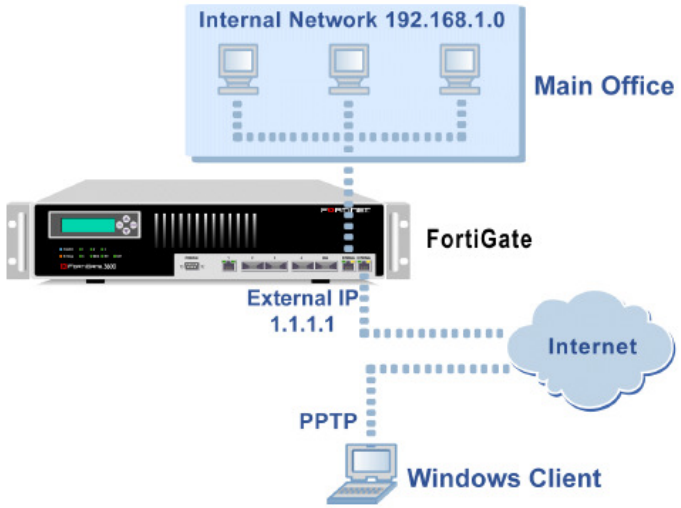
# Collegamento remoto tra le sedi : Tecnologia

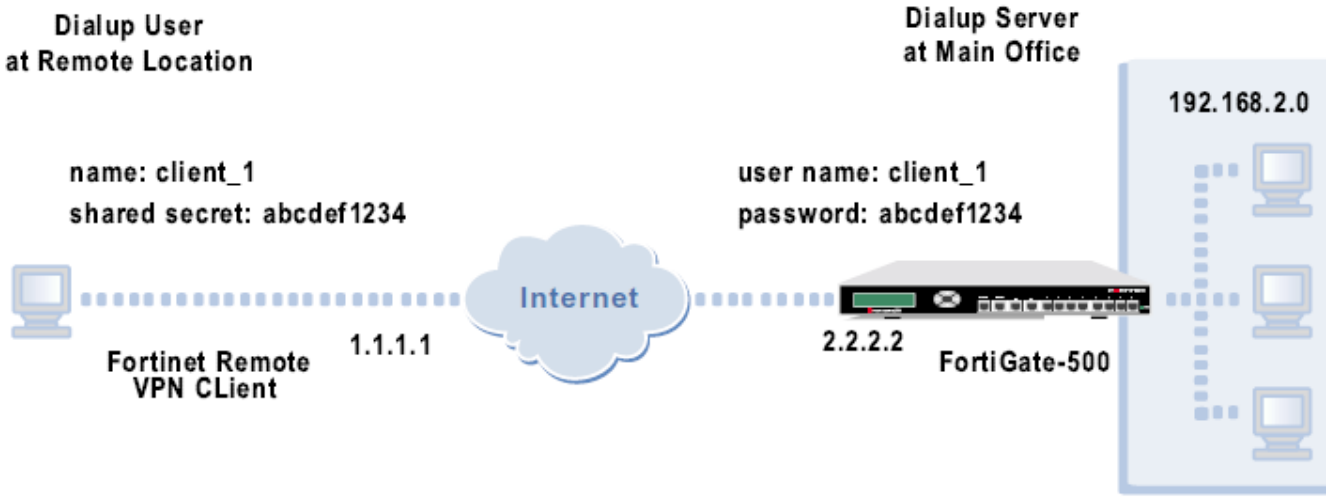
Collegamento da un client verso la sede (portatile, pc da casa, singola postazione su un ufficio distaccato):

-Utilizzo del PPTP

-Utilizzo dell'IPSEC

Figure 23: PPTP VPN between a Windows client and the FortiGate unit



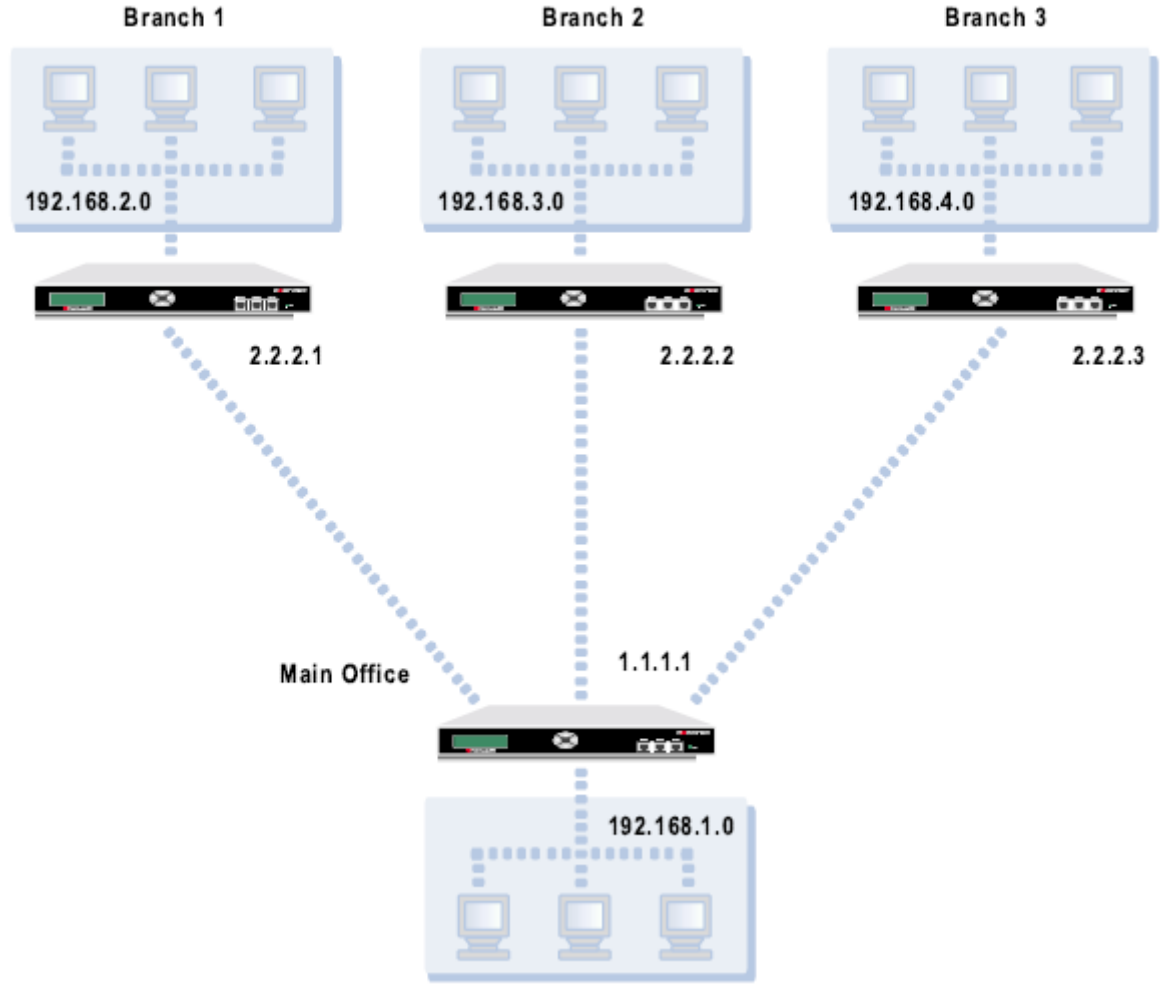



# IPSEC o PPTP

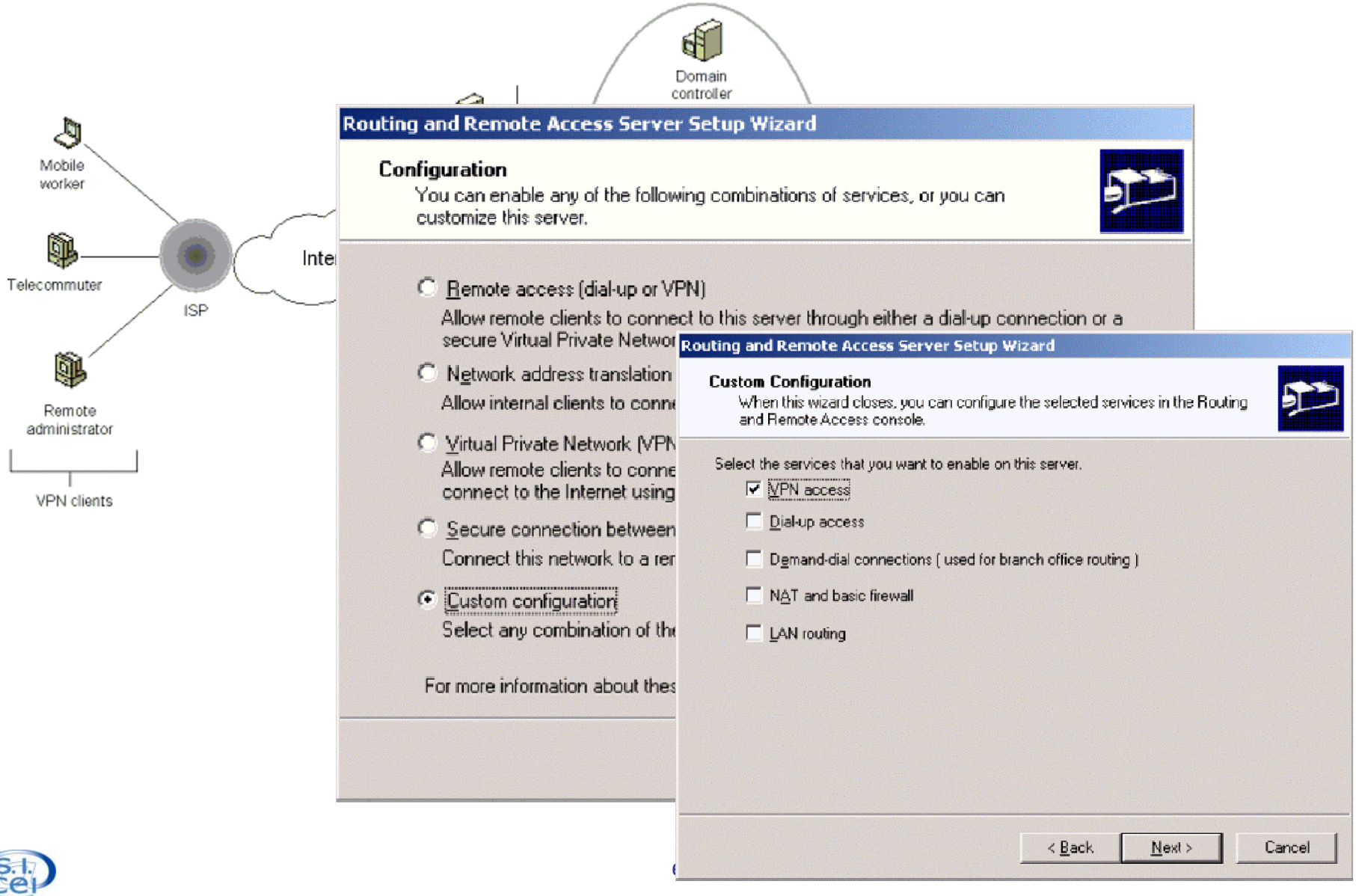
| | IPSec | PPTP |
|---|---|---|
| Pro | •Cifratura forte 168 bit 3DES<br>•Standard Internazionale | •Non richiede software aggiuntivo |
| Con | •Richiede software aggiuntivo | •Cifratura debole |

# Collegamento remoto tra le sedi : Tecnologia

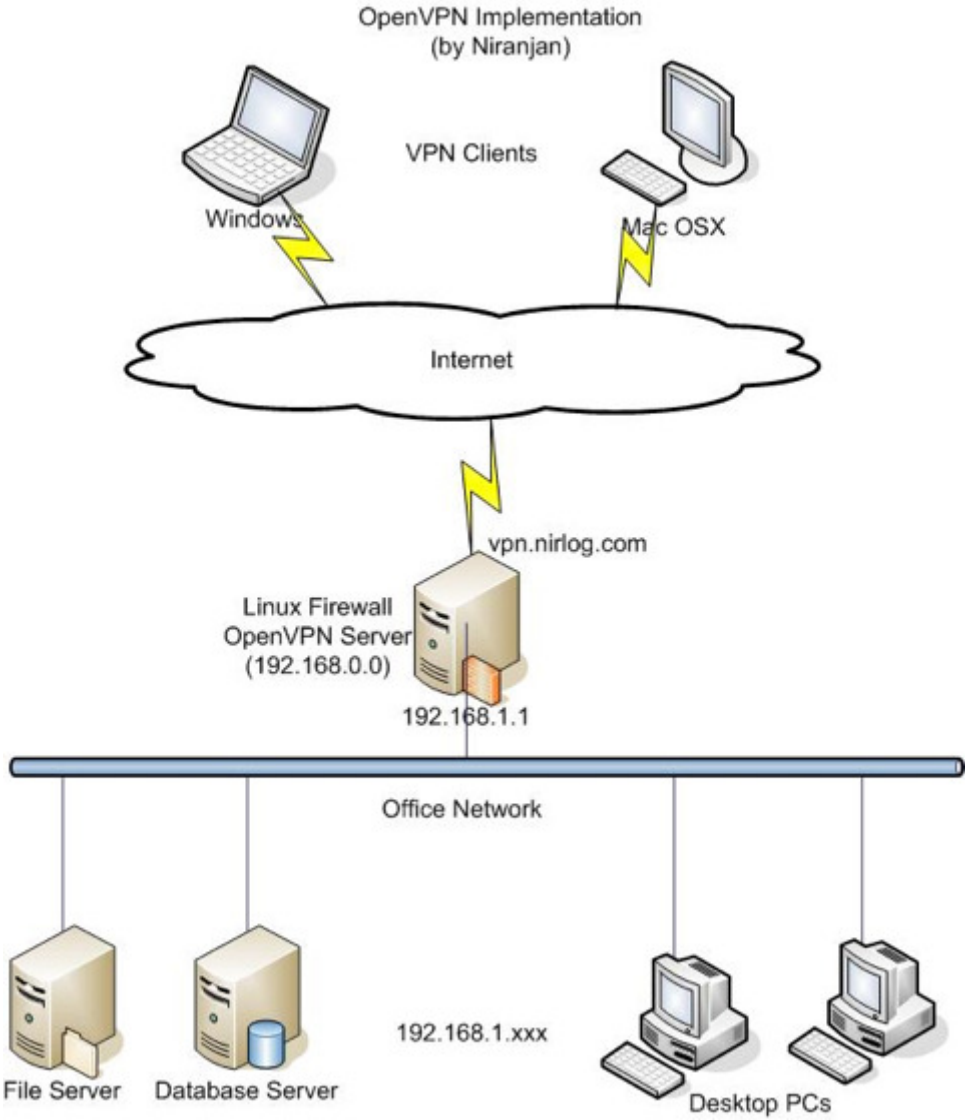
Figure 20: Hub and spoke configuration



# VPN: si può realizzare su un server Windows



# VPN : con OPEN VPN




Su Linux o Windows

Autenticazione con certificati, su token o su file

# Copie di sicurezza

# Attenzione al Backup

- **Esigenza**
  - **Rendere disponibile i dati a fronte di:**
    - Guasti
    - Virus
    - Cancellazioni errate
  - **Consentire all'utente di riprendere il lavoro tempestivamente**

- **Anche in questo caso mix di soluzione:**
  - **Tecnologica**
    - Aree per il backup
    - Software
  - **Procedurale/Oranizzativa**
    - Regole per il backup (un dato sul proprio pc se non portato sul server di backup non e' backuppato)

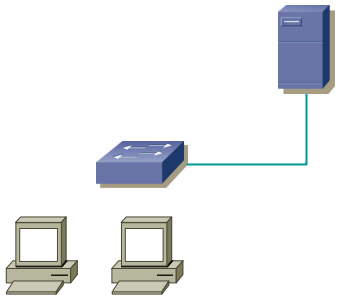
# Approccio al problema (1)

- **Identificare cosa archiviare e per quanto tempo**
  - Dati (sui pc e sul server)
  - Programmi e loro configurazione
  - Macchine per intero (immagini per ripristino in tempi brevi dell'operatività)
- **Stimare lo spazio necessario**
  - 1TB, 2TB, 10TB???
- **Disegnare la soluzione**
  - Dati **in line** (su server di backup ma comunque accessibili immediatamente in caso di fault) e/o **off line** (su nastro o DVD e quindi tempi di reperimento e caricamento)
    - L'archiviazione offline e' necessaria per quei dati per cui si vuole garantire la disponibilità anche a fronte di eventi localizzati che rovinano l'infrastruttura (le copie dovrebbero essere trasportate altrove)
  - Server di Backup, SAN o NAS
  - Scelta del software (funzionalità anche di ripristino su macchina virtuale?)
  - Impatto sulla rete

# Approccio al problema (2)

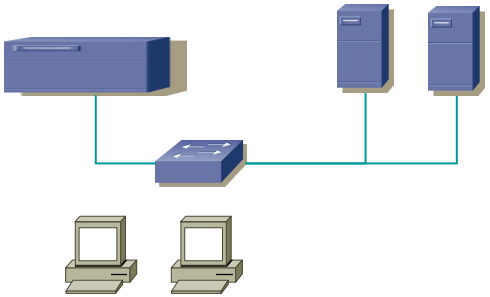
- **Implementare la soluzione**
  - Acquisto HW e SW
  - Installazione, configurazione ed avvio
  - Backup full ed incrementale
- **Manutenere la soluzione**
  - Monitorare il sistema per:
    - Capienza dischi
    - Esito dei backup (tutto e' andato a buon fine?)
  - Test periodici di ripristino
  - Integrazione nel sistema di backup dei nuovi programmi installati o dei nuovi server o dei nuovi pc
  - Etichettare e custodire in modo ordinato le copie di sicurezza

# Architettura tipo



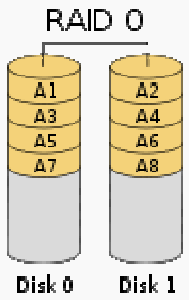
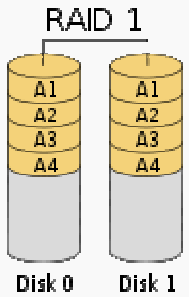
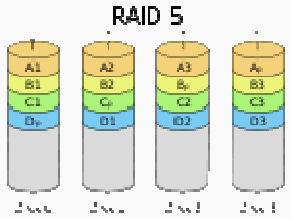
- **Soluzione piccole reti**:
  - Server con spazio disco e cartelle condivise
    - Configurato in Raid 1
    - Unità a nastro eventualmente collegata al server per i backup offline
  - Per il backup
    - In carico agli utenti con cartella documenti direttamente sul server

      oppure
    - Software
      - backup dei dati sul server
      - Immagine tipo dei PC con software di base



- **Soluzione piccole/medie**:
  - NAS dedicata al backup(fino a 4TB)
    - Raid 1 o 5
  - Eventuale unità a nastro
  - Software di backup
    - Sui PC (memento o acronis)
    - Sul server (acronis o l'open source backuppc o amanda)

# RAID (Redundant Array of Independent Disks)

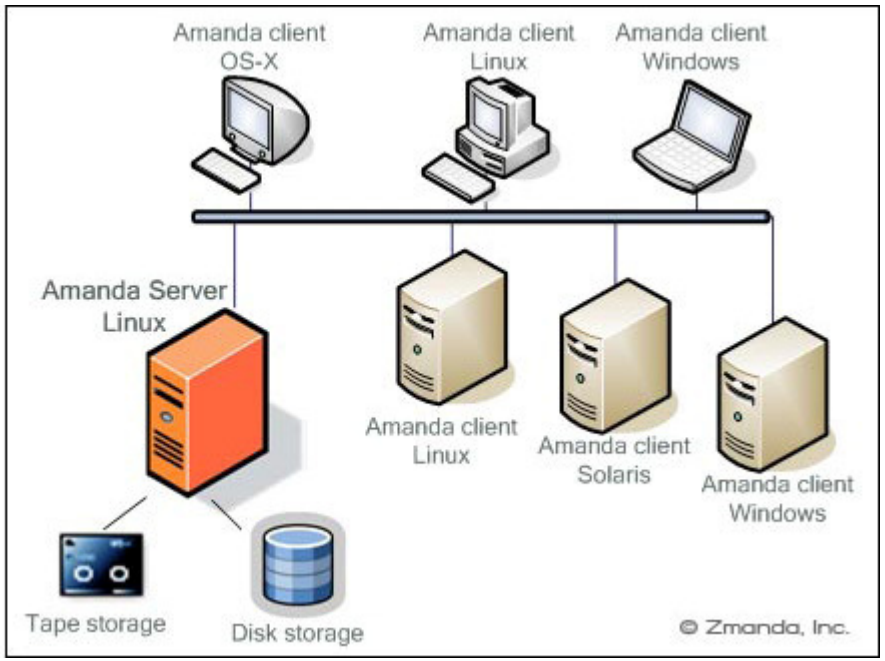
| | | |
|---|---|---|
| **RAID 0** |  | Il sistema RAID 0 divide i dati equamente tra due o più dischi con nessuna informazione di parità o ridondanza (operazione detta di *striping*).RAID-0 è usato generalmente per aumentare le prestazioni di un sistema, anche se è molto utile per creare un piccolo numero di grandi dischi virtuali da un grande numero di piccoli dischi fisici. |
| **RAID 1** |  | Il sistema RAID 1 crea una copia esatta (*mirror*) di tutti i dati su due o più dischi. È utile nei casi in cui la ridondanza è più importante che usare tutti i dischi alla loro massima capacità. |
| **RAID 5** |  | Un sistema RAID 5 usa una divisione dei dati a livello di blocco con i dati di parità distribuiti tra tutti i dischi appartenenti al RAID. Questa è una delle implementazioni più popolari, sia in hardware che in software. Virtualmente ogni sistema di *storage* permette il RAID-5 tra le sue opzioni. |

# Funzionalità del software Commerciale

- I costi (dal sito acronis)
  - 80€ a postazione
  - Per i server da 700 a 1000€
- Ci sono tante altre soluzioni,
- Questa e' presentata solo a titolo esempilificativo

# Funzionalità del software Opensource

- **Backup PC**
  - Da file server recupera i dati dai pc della rete
  - Deduplicazione
- **Amanda**
  - Vero e proprio software di ba con agenti per le varie tipolog server
- http://amanda.zmanda.com/



***Collaboration***

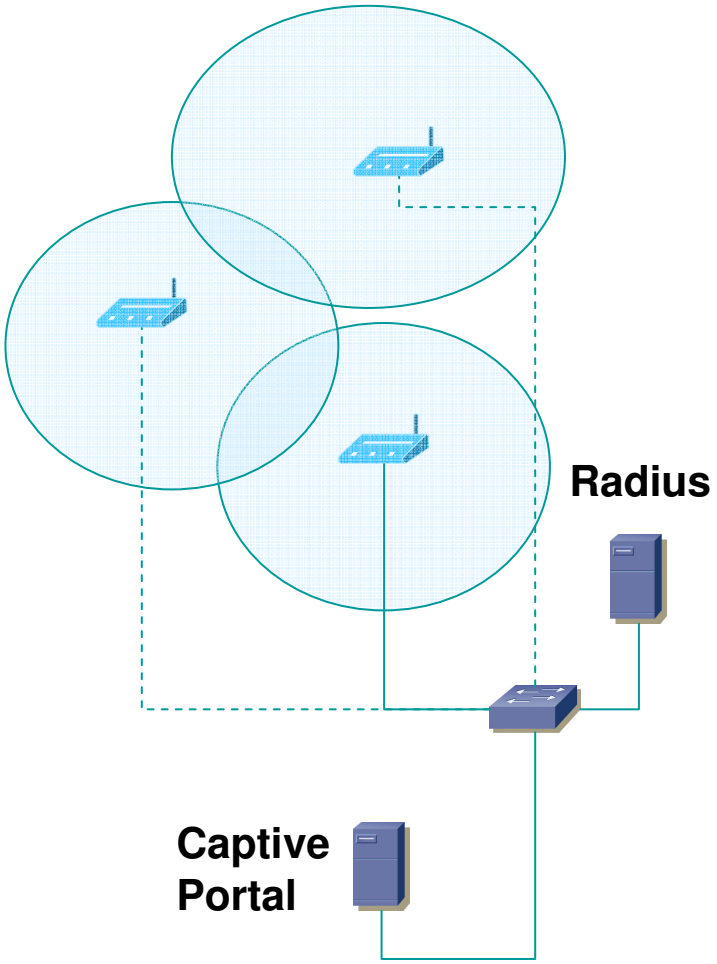
| **Applicazione** | Breeze | Elearing (copercom) | Microsoft Communicator+ Office Live | DIM DIM Open source / Enterprise |
|---|---|---|---|---|
| Instant Message | SI | SI | SI | SI |
| Stanza Chat | Si | SI , | SI | Si |
| Scambio Documenti | SI | NO | SI | SI |
| Audio/Video | SI | SI | SI | SI |
| Condivisione documenti e proprio schermo | SI | NO | SI | SI |
| Lavagna appunti | SI | NO | SI | SI |
| Requisiti Client | Browser con Flash Player | Browser | Client Communicator e software live meeting | Browser con Flash Player |
| Conferenza 1 a 1 | SI | NO | SI | SI |
| Conferenza 1 a N | SI | SI | SI | SI |
| Conferenza N a N | SI | NO | Solo video di 2 persone per volta | SI |
| Gestione partecipanti | Registrati o ospiti accettati dal moderatore | | Utenti su active directory o link per ospiti (che devono avere pero' installato il sw client) | Utenti a cui viene inviato il link con key |
| Integrazione con telefonia ( tradizionale e voip) | Modulo aggiuntivo mediante terze parti | NO | Altri elementi nell'architettura | SI (da testare) |
| Architettura | 1 server | | Almeno 4 server (virtuali) | 1 server |
| Vantaggi | Reqisiti client molto | Efficace per lo | Interoperabilità | Requisiti client molto leggeri |

# *Architetture Wireless*

# Utilizzo del Wireless

- **Reti wireless (diverse soluzioni architetturali)**
  - Nel piu' semplice dei casi tutto fatto con l'accesso point
  - Per maggiore controllo integrazione con server che gestisce l'autenticazione (radius con password o certificati)
  - Per gli ospiti una soluzione di captive portal con pagina web per l'autenticazione ed accesso ai servizi in base al profilo
  - 802.1x (maggiore sicurezza) non solo per l'accesso alle reti wireless ma anche alla rete fisica

- **Sicurezza (base)**
  - NO ssid in broadcast
  - Cifratura WPA-PSK (wep e' debole)



***Come valutare il livello di sicurezza della propria rete***

***Come proteggersi***

***Quanto spendere***

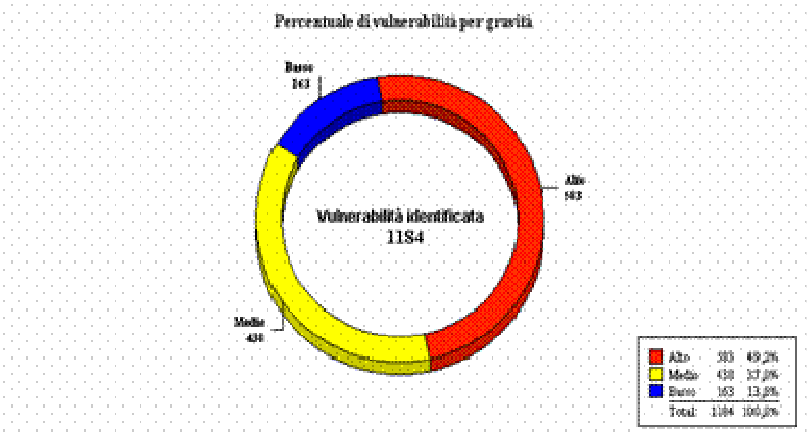
# Come valutare il livello di sicurezza della propria rete (1)

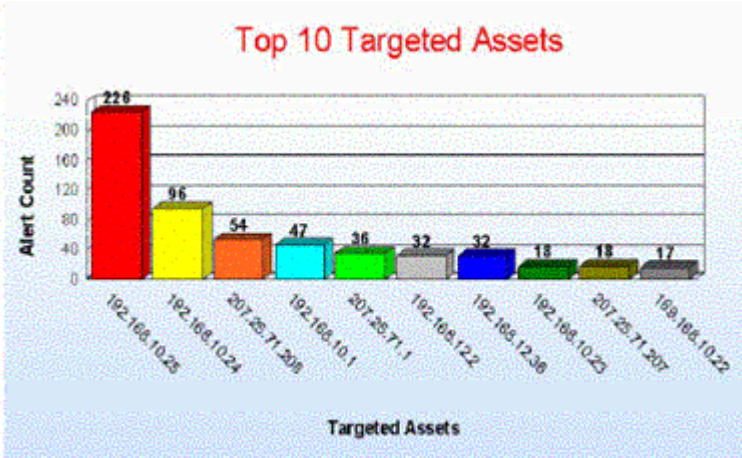
- Mediante il confronto con line guida sulla sicurezza

| Misura suggerita | Situazione attuale | Azioni da intraprendere | Priorità |
|---|---|---|---|
| Backup dei dati<br>-RAID<br>-Copia su DVD o Nastro in locali diversi | Copia dei dati su altro disco | Prevedere l'adozione di un sistema automatico per il ghost delle configurazioni e per la copia su supporti non riscrivibili | ALTA |
| Utilizzo di Firewall | Firewall per la connessione ad Internet | Rivedere le regole sul firewall e verificare l'aggiornamento della configurazione | MEDIA |
| Utilizzo di antivirus ed aggiornamento periodico | Antivirus centralizzato ed antivirus sui client | Nessuna | |
| Separazione rete client da rete server | Tutti sulla stessa LAN | Valutare l'adozione di VLAN | BASSA |

## Come valutare il livello di sicurezza della propria rete
### -L'importanza del Vulnerability Assessment-

- Mediante strumenti o servizi di analisi delle vulnerabilità che forniscono:
  - Livello di visibilità da internet
  - Vulnerabilità presenti
  - Livello di protezione delle proprie postazioni
  - Livello di protezione dei server
  - Report di sintesi e contromisure tecniche



# Come proteggersi:
# Innanzitutto analisi dei rischi e valutazione costi/benefici

- **Diverse modalità di protezione**
  - **Procedurali**
    - Regolamentazioni
    - Policy di sicurezza
    - Standard
    - Awareness
  - **Tecnici**
    - Firewall
    - Sistemi di autenitcazione
    - Antivirus
    - Antispam
  - **Fisici**
    - accesso ai locali
    - accesso ai server

Si….Ma cosa adottare?


**L'obiettivo è raggiungere un buon livello di sicurezza con un budget adeguato:**

*il costo dell'investimento in sicurezza non deve essere superiore alla perdita economica dovuta ad un problema di sicurezza*

# Vademecum

- Sui PC
  - Effettuare gli aggiornamenti di sicurezza
  - Mantenere attivo ed aggiornato l'antivirus
  - Impostare password robuste e cambiarle periodicamente
  - Disabilitare l'anteprima automatica
  - Attivare il blocco Popup
  - Click Ragionato
  - Se possibile limitare le capabilities dell'utente
- Sui server
  - Password robuste
  - Aggiornaemnti di sicurezza (previo backup)
  - Installare solo i servizi necessari (se non serve word non si installa)

## Conclusioni

- La soluzione ideale e generale non esiste ma..
  - Ci si può attrezzare per ottenere un adeguato livello di sicurezza senza dover acquistare necessariamente troppi prodotti
    - Configurando al meglio le proprie macchine
    - Mediante formazione e sensibilizzazione
  - Si possono acquistare prodotti di sicurezza, ma si devono mantenere aggiornati e configurati opportunamente
    - nel tempo altrimenti diventano inefficaci
  - Si puo' usufruire del servizio di sicurezza gestita
    - Per non preoccuparsi della sicurezza demandandola a terzi fidati. (questo perche' in genere il retferente informatico è superimpegnato nel quotidiano e difficilmente riesce a trovare il tempo per la gestione della sicurezza)

# *Promemoria servizi disponibili*

# Servizi disponibili

- **Antivirus Centralizzato (10€ a postazione)**
  - E' un servizio che prevede l'installazione di una versione del software che ha molte funzionalità rispetto al semplice antivirus desktop
    - Controllo centralizzato
    - Aggiornamenti in modalità push
- **Servizi di sicurezza UTM**
  - Gestione Firewall
  - Gestione Centralizzata VPN
  - Monitoraggio rete e sistemi IDS
  - URL Filtering
- **Supporto per l'implementazione delle soluzioni di Backup**
- **Per chi gestisce server di posta in casa**
  - Antispam di primo livello per chi ha i server di posta in casa
  - Backup Server mail
- **PUSH Mail**
- **WebMeeting**