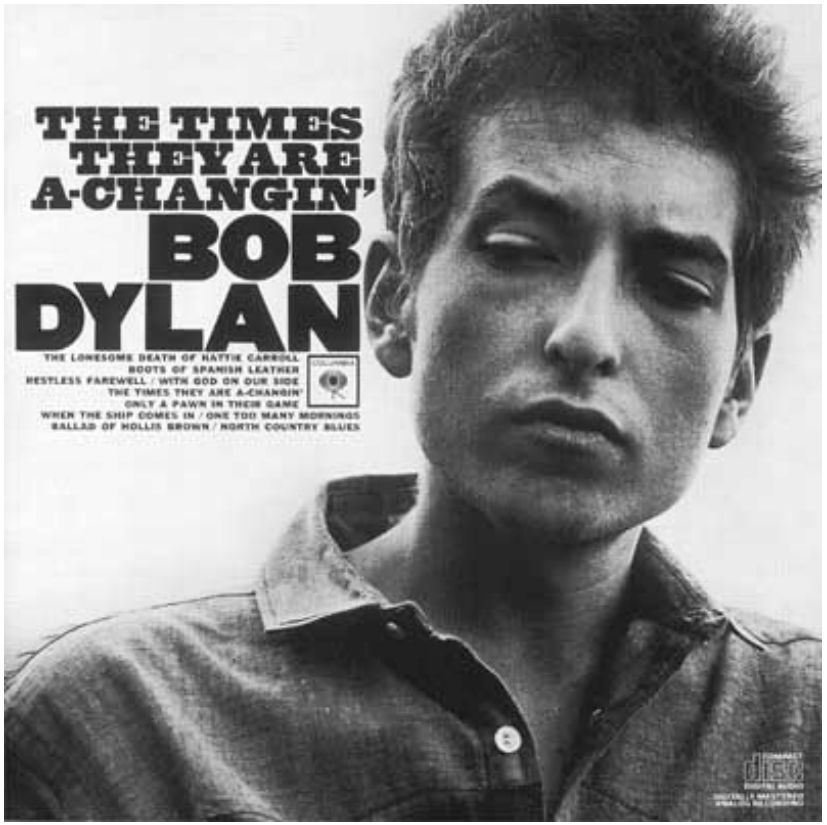

# La "ricetta" per mettere in sicurezza le proprie reti ai tempi di GARR-X

Francesco Palmieri

Università degli Studi di Napoli Federico II - GARR

# “The Times They Are a-Changin’”

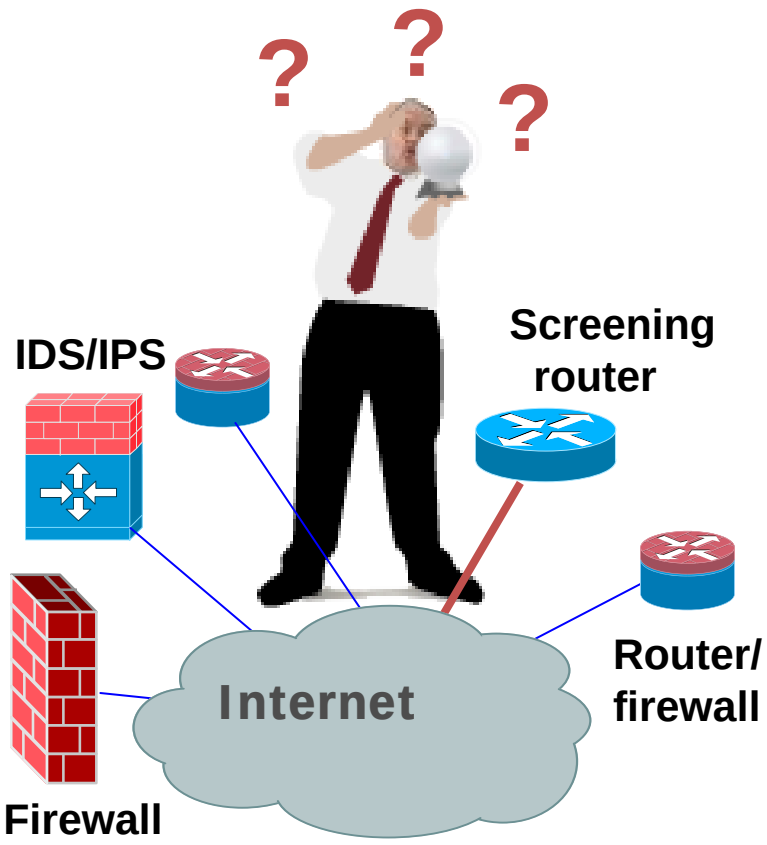
- Con l’avvento di GARR-X ed in particolare con l’introduzione di:
  - Servizi **pseudo-wire** e **VPLS**
  - **Bandwidth** e **connection** on demand
  - **Lambda dedicate**




- I confini fra WAN, MAN e LAN diventano **sempre più labili** … fino a scomparire quasi del tutto

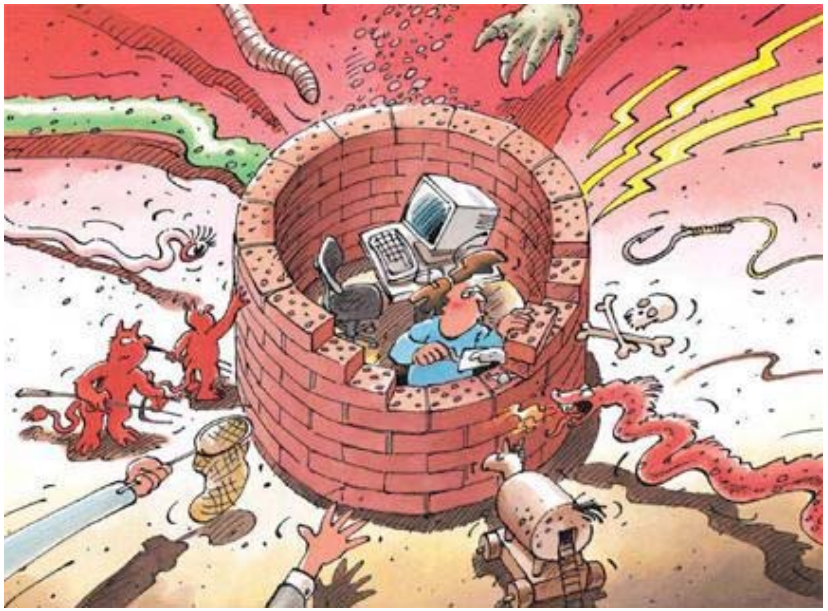
# Cambiano le architetture

- Tendono a **sparire** architetture e modelli di rete fortemente **strutturate su base layer**:
  - Layer 2 (switching) nella LAN
  - Layer 3 (routing) nella WAN
  - Firewall sul confine
- Andando verso **modelli dinamici** e flessibili che prevedono la localizzazione delle attività di routing e switching **dove servono** effettivamente



# Senza più confini!

- Con l'avvento delle tecnologie di nuova generazione (wireline e wireless) **si rilassa il concetto di "Perimetro"** della rete, e di conseguenza la logica di "**Demarcazione**"
- Ciò ha ovvie **conseguenze architetturali** su tutta la gestione della sicurezza della rete



# La borderless network

- L’avvento di nuove tecnologie ubiquitous/mobile wireless (3G cellular, Satellite, WiMax etc.) rende “**inconsistenti**” i confini delle infrastrutture di rete
- Reti LAN e MAN di cospicue dimensioni tendono a fondersi con tecnologie di livello 2 nella logica della “**Condominium Fiber**”

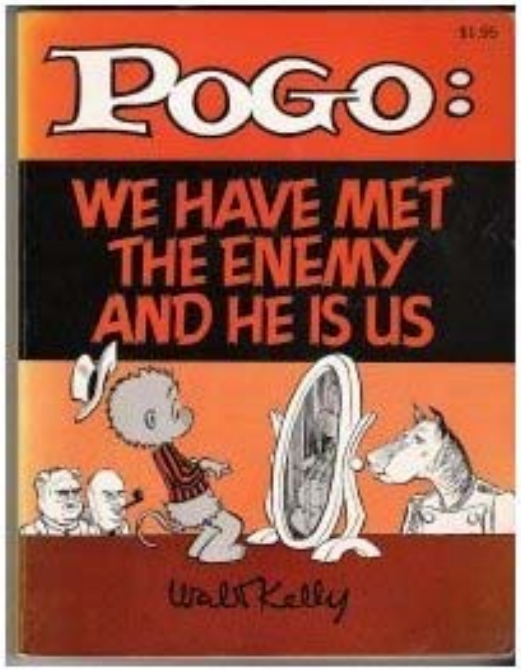
- Diventa quindi impossibile creare **barriere perimetrali** su cui concentrare gli sforzi e l’attenzione per la **security**

# Si confondono le idee …

- Vengono a **confondersi** ruoli, concetti, direttrici di azione e target fondamentali di difesa:
  - Cade completamente il paradigma: tutti “buoni” dentro (**inside**) e tutti cattivi fuori (**outside**)
  - Va riconsiderato il concetto di **security domain**

**IL “NEMICO” PUO’ ESSERE DENTRO LA NOSTRA INTRANET E IL NOSTRO “PERIMETRO” …**

**- EGLI E’ NOI -**

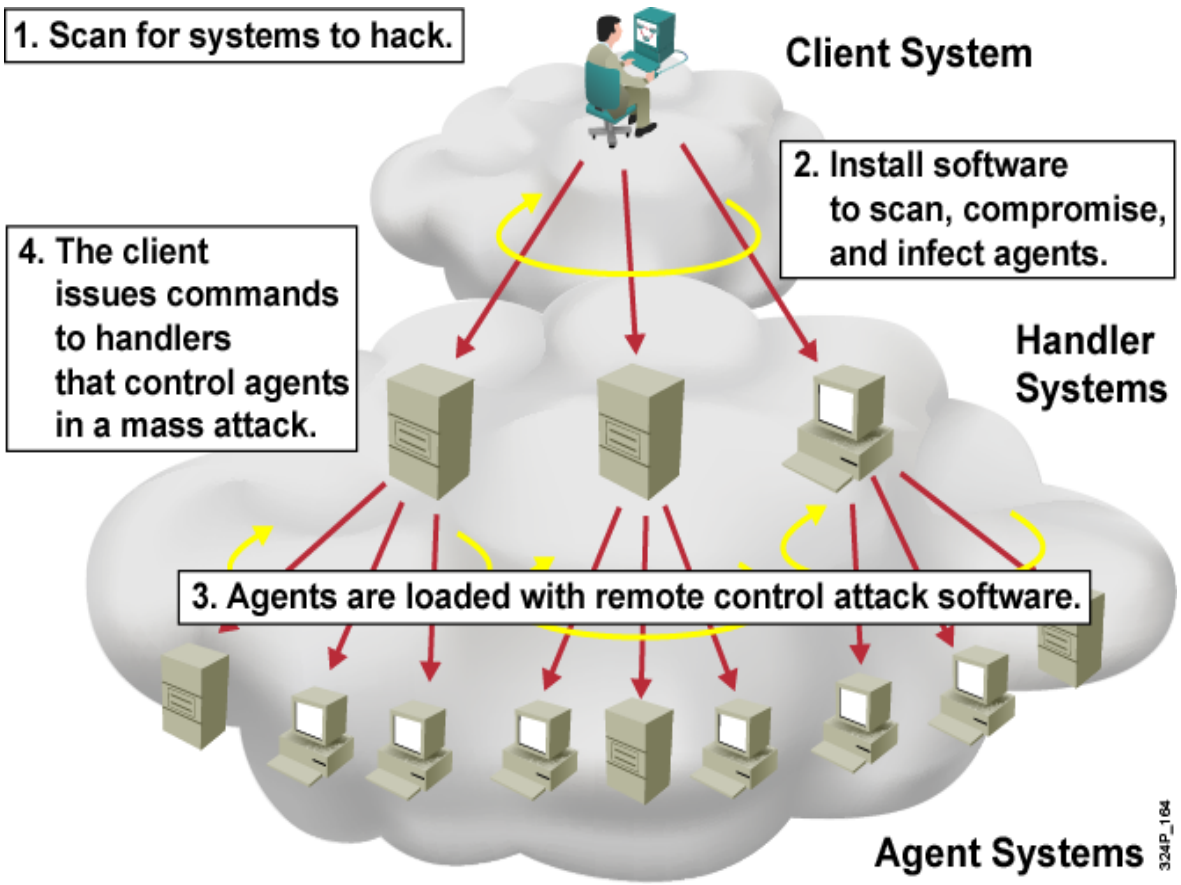


# … E gli obiettivi

- La risorsa da proteggere è la nostra rete interna dagli **attacchi esterni** (responsabilità interne) ? …
- … O le realtà esterne dagli attacchi/abusi **provenienti dalla nostra rete** (responsabilità legali) ?
- In virtù dell'**alta capacità di banda** le nostre reti diventano veicoli ideali e ambiti per:
  - Cyberterrorismo e cybercrime
  - Vandalismo informatico
  - Denial Of Service distribuiti
  - Grandi Botnets
  - Diffusione massiva Worms
- E' **strategico** proteggere:
  - La intranet dall'esterno
  - L'esterno dalla intranet

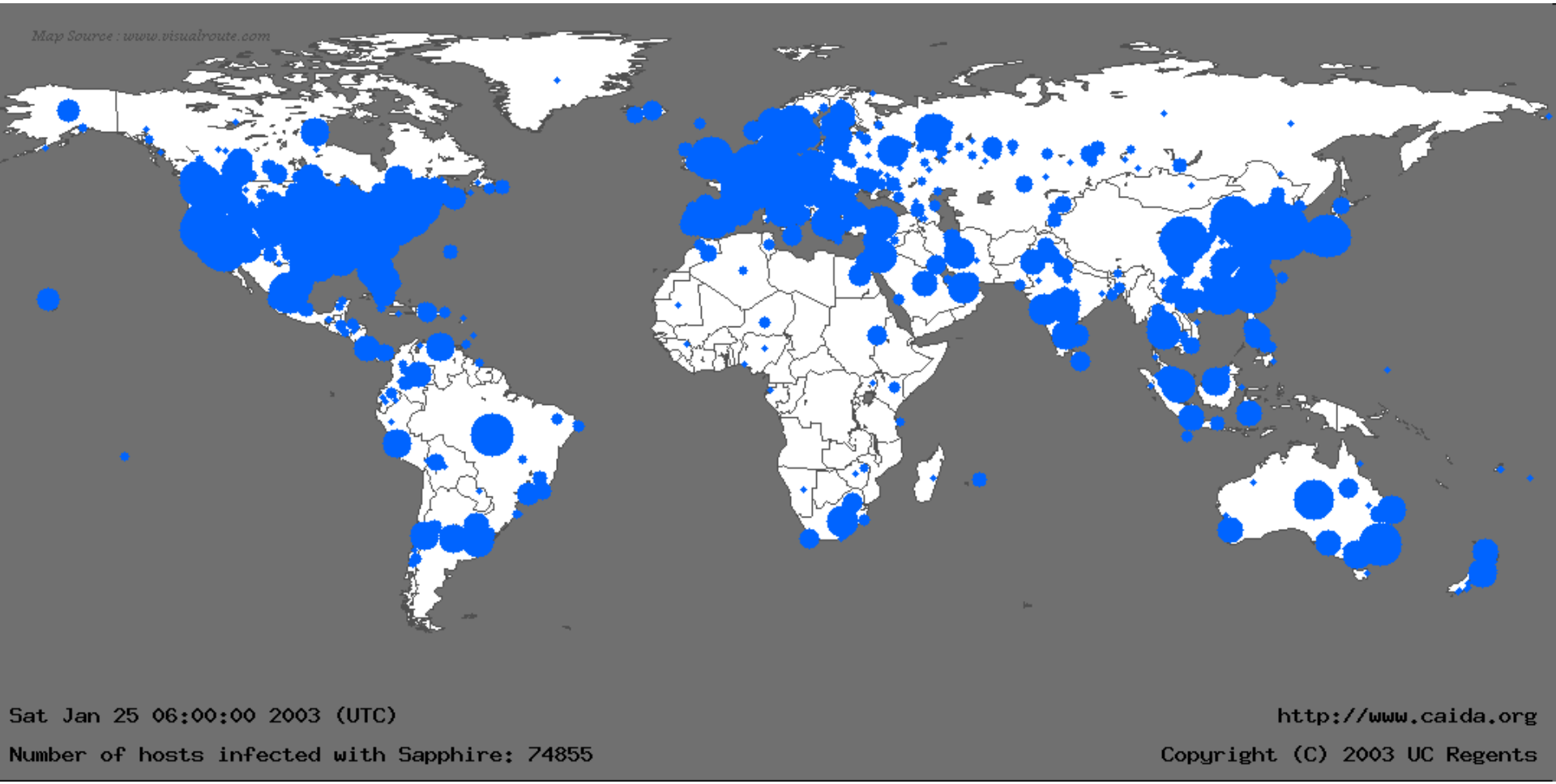
# Distributed DoS (DDOS)

- Non interessati all'accesso alla rete o a informazioni presenti su di essa
- Molto semplici da realizzare in disponibilità di risorse (banda)
- Molto complessi da tracciare e mitigare



# Flash Worms

- Hanno effetti devastanti sulla stabilità della rete Internet proporzionalmente alla loro velocità di propagazione

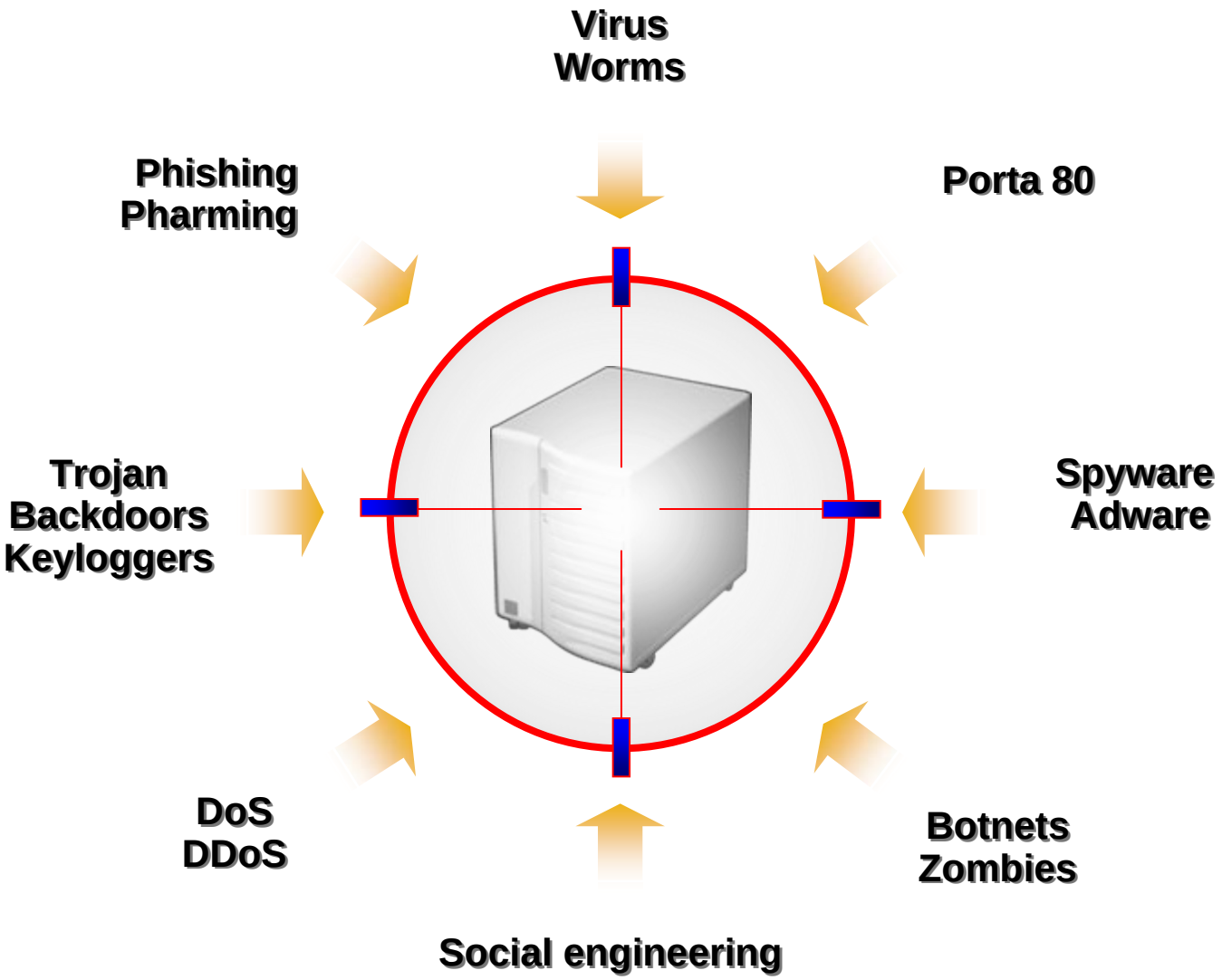


# Botnets in affitto

Fonte: Technology Review, 24 Settembre 2004

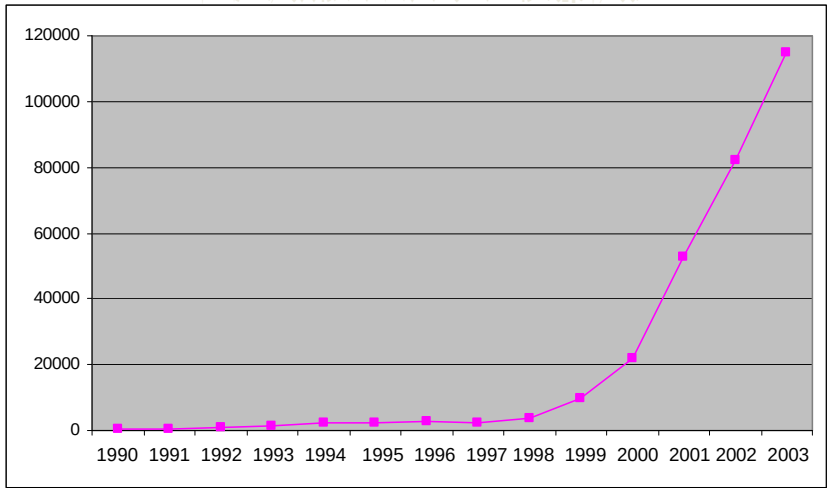
- Nasce un florido mercato delle macchine in rete compromesse
- Botnets di molte centinaia di hosts in affitto a circa 100$/ora
- Utilizzate per l'invio di SPAM, per sferrare attacchi DDOS, per distribuire materiale pedo-pornografico, etc.
- L'attività sta assumendo connotati professionali, anche grazie alla notevole domanda finalizzata a danneggiare il mondo dell'industria

# Aumentano i poblemi da gestire …

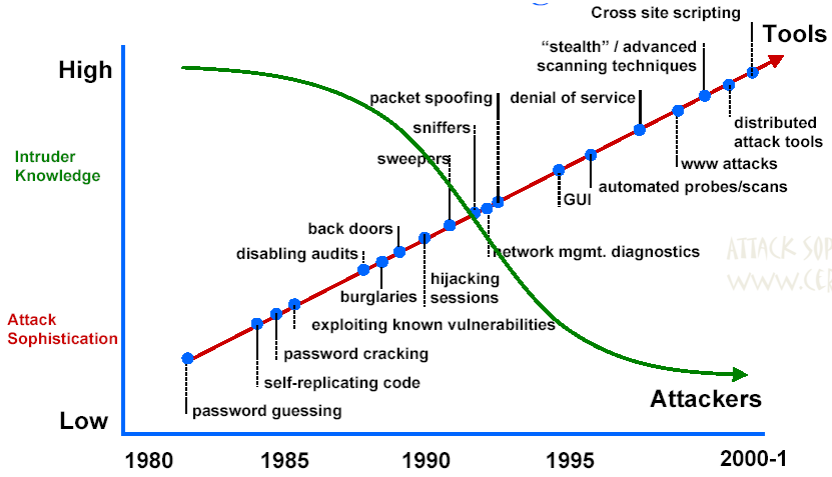


# … E quindi I soli firewalls non bastano

- E’ cresciuto **esponenzialmente** il numero di target vulnerabili
- Il grado di **sofisticazione** e la violenza degli attacchi è sempre più elevato

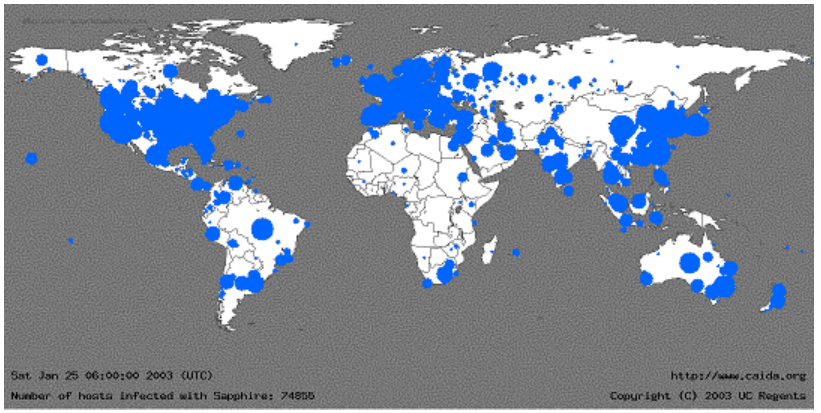



INCIDENTS REPORTED TO COMPUTER EMERGENCY RESPONSE TEAM/COORDINATION CENTER (CERT/CC)




ATTACK SOPHISTICATION VS. INTRUDER TECHNICAL KNOWLEDGE, SOURCE: WWW.CERT.ORG/ARCHIVE/PPT/CYBERTERROR.PPT

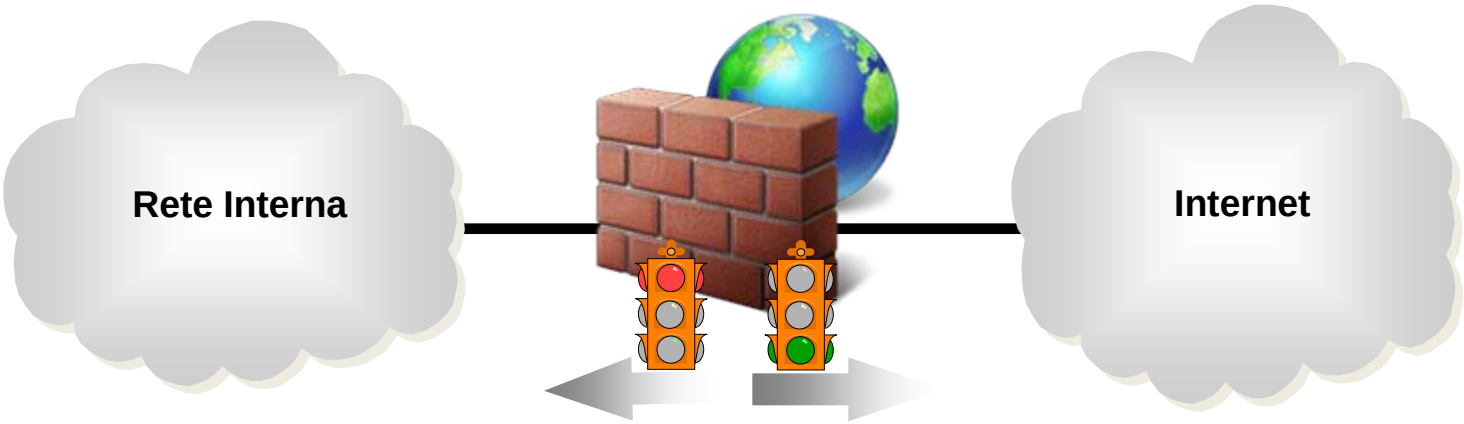
- Tutti I meccanismi di sicurezza disponibili hanno vulnerabilità **non** evitabili
- I firewalls **non** sono sufficienti per garantire la protezione delle reti a fronte di attacchi provenienti **dall’interno e dall’esterno**




THE GEOGRAPHIC SPREAD OF SAPPHIRE/SLAMMER WORM 30 MINUTES AFTER RELEASE (SOURCE: WWW.CAIDA.ORG)

# La fine del modello “fortezza”

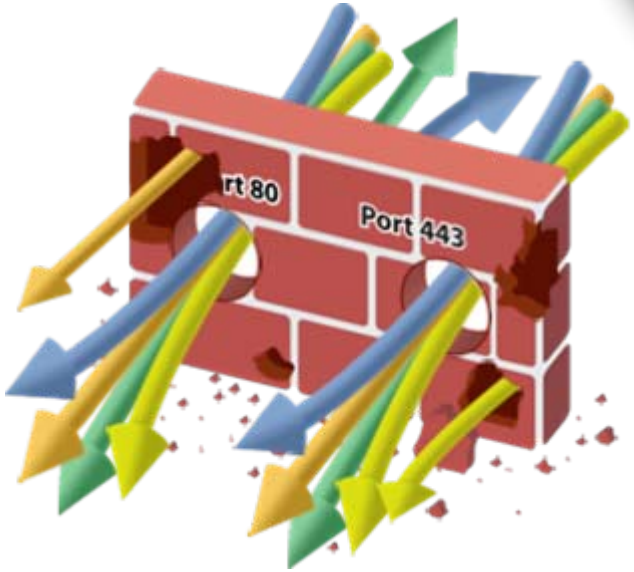
- **Sparisce** il concetto di sicurezza totalmente (ed esclusivamente ) fondato su screening firewall posti sul bordo esterno della rete
- Le sole ACL diventano **poco flessibili** per definire le politiche di sicurezza




**Filtraggio statico per porta di Protocolli:**
**DNS (UDP/53), SMTP (TCP/25) , HTTP (TCP/80), FTP (TCP/21)**

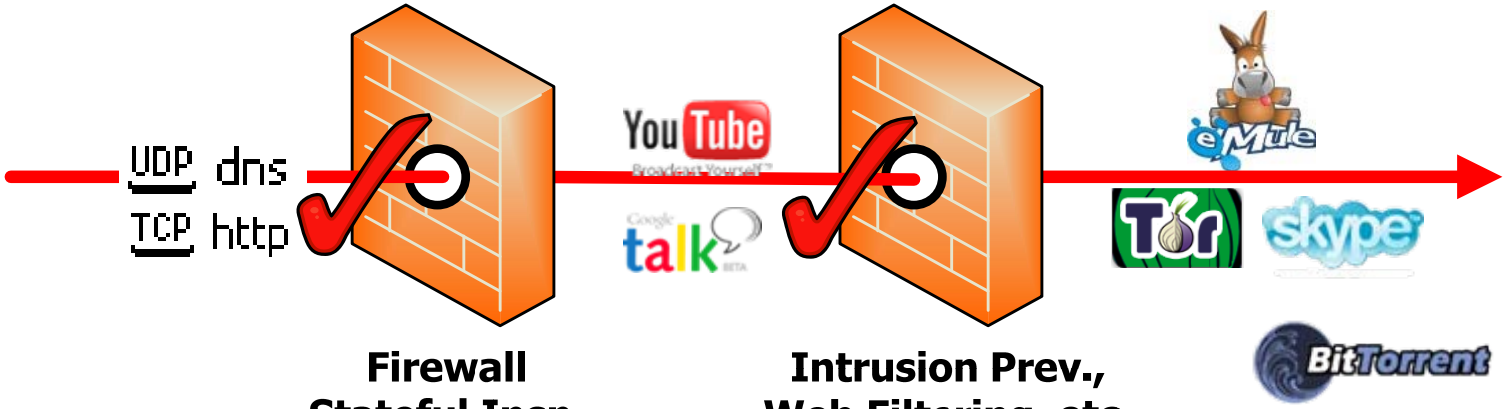
# Il filtraggio per porta non basta

- Non è più possibile applicare politiche di filtraggio basate su **parametri statici** del pacchetto IP o TCP/UDP


- Port ≠ Applicazione (protocol obfuscation)
- IP address ≠ Origine (IP spoofing)
- Payload ≠ Contenuto (Encryption)

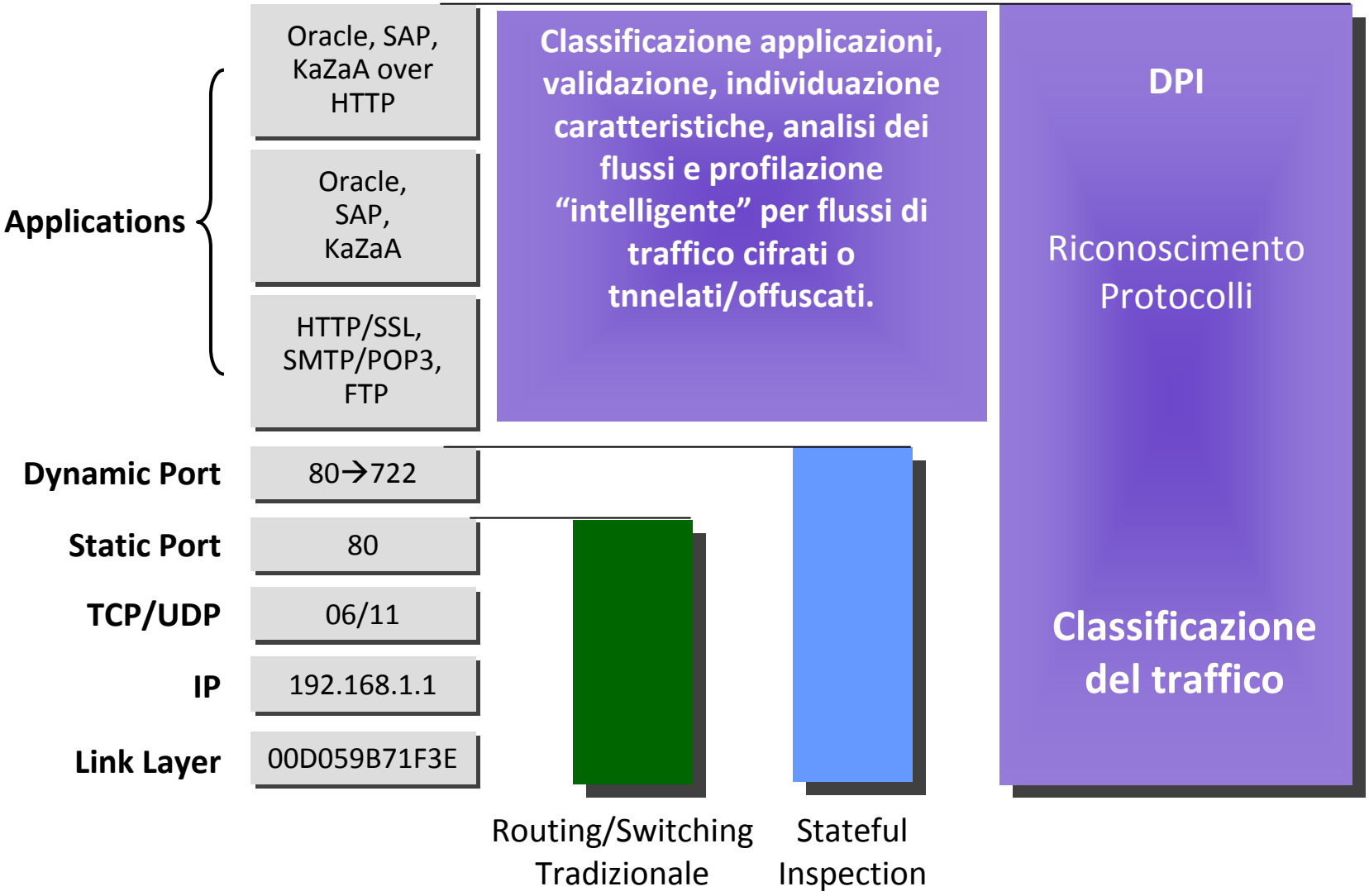
# Classificazione del traffico




**Più del 60% delle applicazioni non sono riconoscibili dai firewalls**

- I firewalls non sono in grado di riconoscere buona parte delle applicazioni
- Alcune aopplicazioni usano meccanismi di protocol obfuscation  e transitano indisturbate attraverso i firewalls su porte well-known  (es. TCP/80, UDP/53)
- Molte applicazioni (e.g. P2P, Skype, Tor) usano la cifratura e non possono essere individuate attraverso  IPS “signatures” e pattern di traffico noti
- E’ necessario **classificare** efficacemente i flussi di traffico per riconoscere le applicazioni coinvolte end-to-end. Emerge il concetto di **“classi” di traffico**

# Classificazione dei flussi di traffico

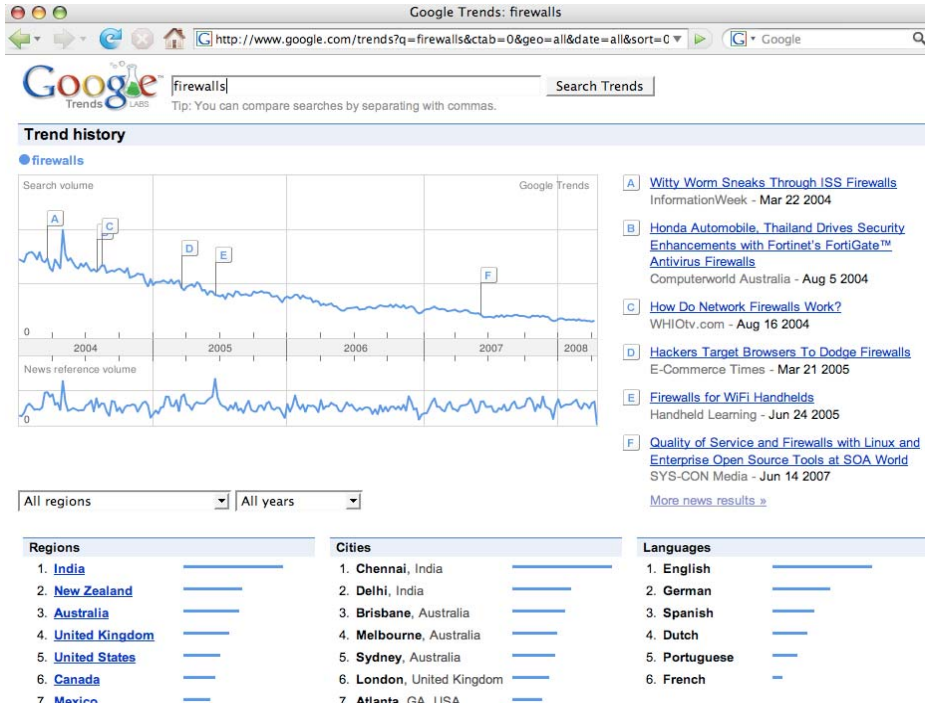


# Limiti di un firewall

- Non protegge da virus e trojan
- Non protegge da attacchi nuovi (sconosciuti)
- Non protegge da connessioni che non lo attraversano (backdoor modem, HSDPA etc.)
- Non protegge da cattive o inesistenti policy
- Non protegge da attacchi interni (75%-80%)
- Non protegge da attacchi fisici
- **Non può fungere da unico punto di difesa**

# Ma è ancora utile un firewall?

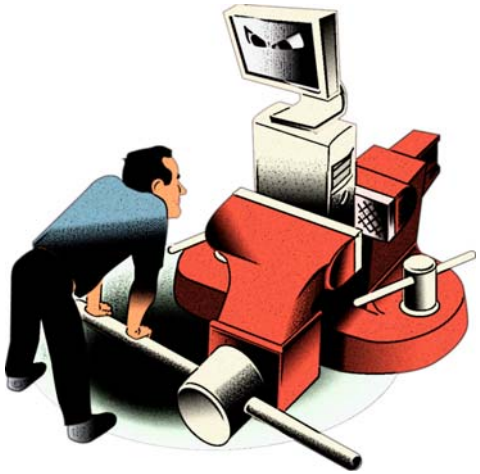
- Google Trends ci presenta un evidente **calo di interesse** nel mercato dei firewalls
- In ambito accademico un firewall aggressivo **può contrastare il processo di innovazione** e l'affermarsi di nuove applicazioni




- Durante RSA 2008 (San Francisco), Bill Cheswick autore della bibbia dei firewall (Cheswick, Bellovin and Rubin's - Firewalls and Internet Security: Repelling the Wily Hacker) ha asserito: "**I haven't used firewalls in, uh, well, mostly, for ten years or more." and "They still have their use, but I really want my hosts to be secure enough they don't need a firewall**"

# Si, ma al posto giusto!!!

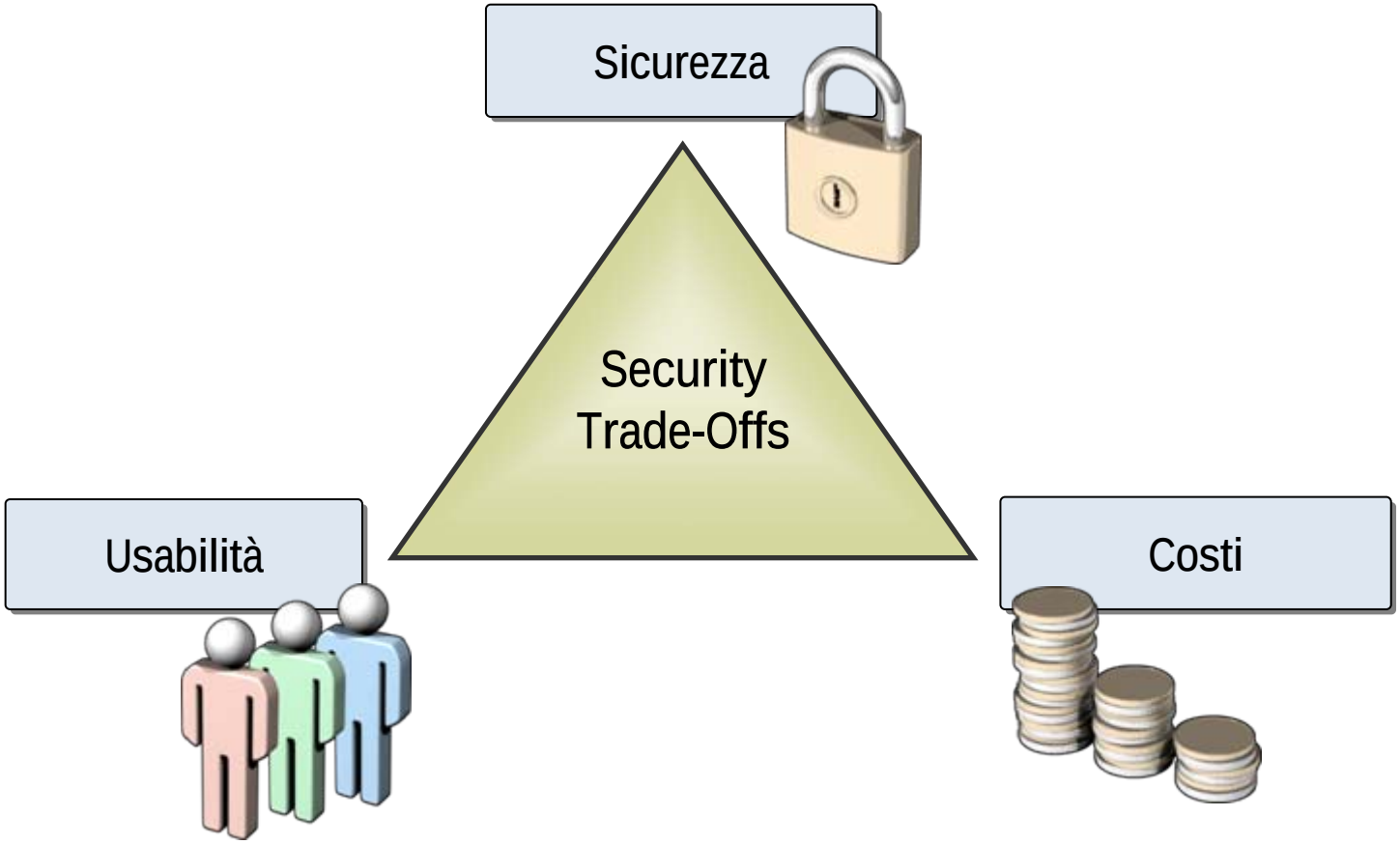
- Proteggere risorse critiche con firewall è più che mai necessario e **indispensabile**
- Vanno stabiliti perimetri interni di sicurezza di **minori dimensioni** e ben individuati
- Il confine da proteggere si sposta quanto possibile **vicino alle risorse interessate**



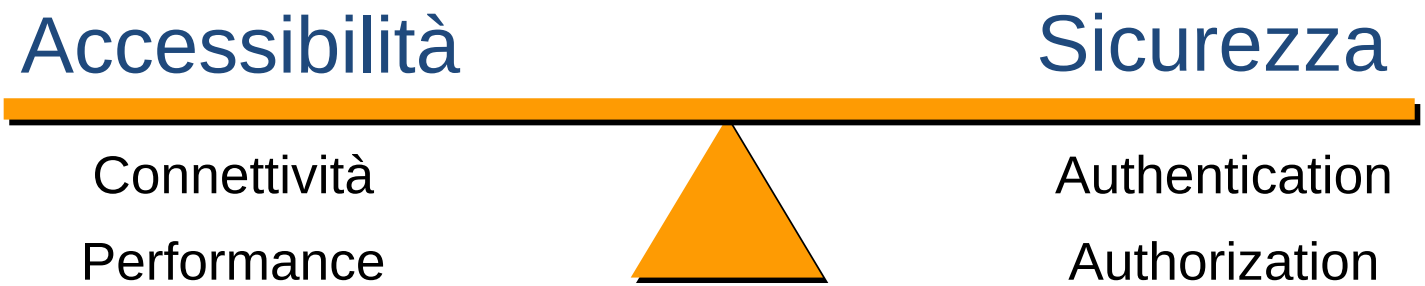
**E di conseguenza …**

- Prolifera il **numero di domini di sicurezza** (e spesso **di dispositivi di protezione**)
- **Aumentano i $$ costi $$** della sicurezza

# I compromessi fondamentali



# Sicurezza vs Prestazioni




Con l'aumentare delle prestazioni **le cose si complicano** considerevolmente

When the going gets tough the tough gets going

# Size matter!!!

- La **capacità di banda** dei link **può diventare** un problema
- La **potenza** richiesta aumenta
- **Non esistono** attualmente oggetti in grado di operare **wire-speed** su interfacce ad altissima velocità
- Firewalling e NAT possono **limitare** sostanzialmente la **scalabilità** e diventare veicolo di DoS a seguito di uno scan

# ACL troppo complesse … no grazie!!!

- Spesso i dati di targa in termini di throughput fanno riferimento al massimo conseguibile in condizioni ottimali – generalmente **conviene diffidare**
- ACL e politiche di filtraggio complesse possono **dimezzare** o **ridurre** a un terzo le prestazioni

GARR-CERT
servizio sicurezza GARR

alert documenti statistiche FAQ
mailing list membri PGP

**Incontri di GARR-B**

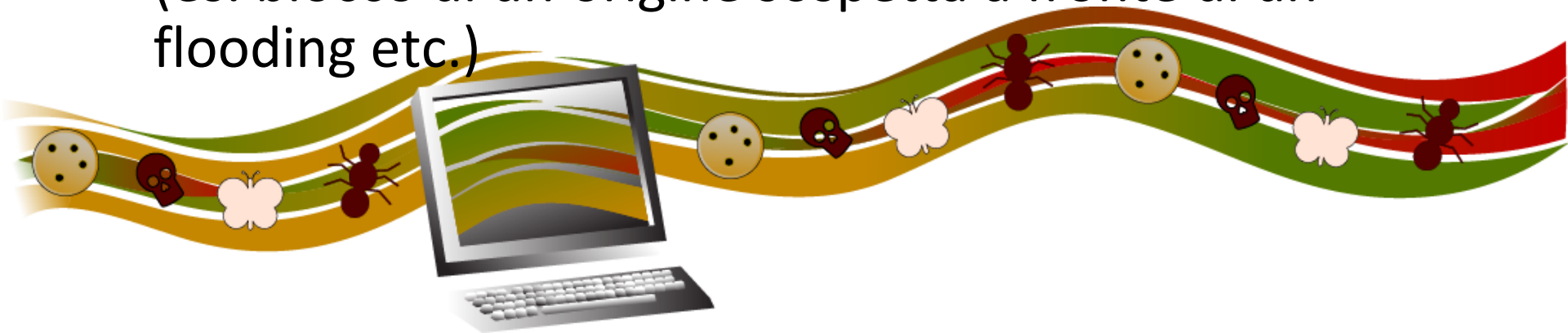
**Terzo Incontro: GARR-B, Stato ed Evoluzione**
**Firenze, 24-25 Gennaio 2001**

Sono disponibili le trasparenze di alcune presentazioni:

- Francesco Palmieri, *Advanced Network Security* (html, pdf)

# Intrusion Detection/Prevention

- Un IDS è un sistema atto ad individuare le intrusioni. E' un sistema, posizionato in punti strategici della rete, che analizza eventi sospetti al fine di individuare eventuali attacchi ("intrusion signatures").
- I sistemi IPS hanno la caratteristica di intervenire proattivamente a fronte di un'intrusione individuata attraverso l'applicazione automatica di contromisure (es. blocco di un'origine sospetta a fronte di un flooding etc.)



# Network-based IPS/IDS

- Un IDS/IPS è usualmente costituito da sniffer o sensori che vedono il traffico sul mezzo trasmissivo ed un motore (engine) per l'analisi e la gestione.
- I sensori operano  in modalità promiscua vedendo tutto il traffico. Non appena individuano qualcosa di sospetto inviano un messaggio di notifica alla stazione di analisi, che in base alla configurazione può inviare un alert, resettare la connessione, interagire con  firewall, router o switch per modificare o introdurre regole di filtraggio.

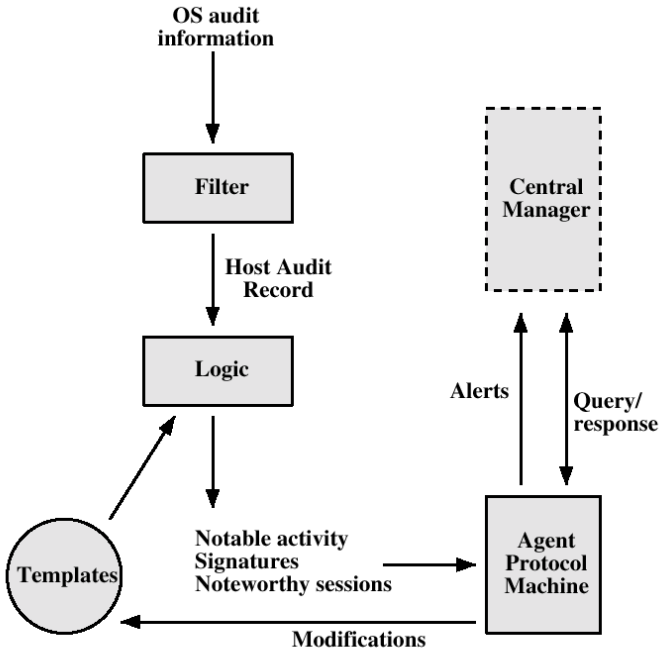



Figure 9.6 Agent Architecture

# Problemi comuni

- I principali problemi inerenti l'impiego di tali strumenti riguardano le situazioni di "falsi positivi" e di "falsi negativi".
- Si ha un "falso positivo" quando il sistema rileva un attacco in situazione di traffico legittimo.
- D'altra parte la situazione di "falso negativo" si presenta in occasione di un reale attacco non rilevato. Tale situazione non è facilmente rilevabile, se non a posteriori, analizzando le evidenze dei sistemi che hanno subito l'attacco.
- I sistemi basati su signature non sono in grado di rilevare nuovi attacchi (0day)

# Anomaly Detection

- Ispezione dei flussi di traffico online per individuazione di eventi anomali via:
  - Signature matching
  - Analisi variazioni statistiche volumi
- Enormi quantità di dati da analizzare
- Meccanismi classification-based:
  - Supervised
  - Semi-supervised
  - Unsupervised (self learning)
- Riconoscimento nuovi attacchi (0-day)
- Detection, recovery & Prevention

**“Individuare un’anomalia on-line su un interfaccia high-speed è come cercare un ago in un pagliaio in fiamme”**

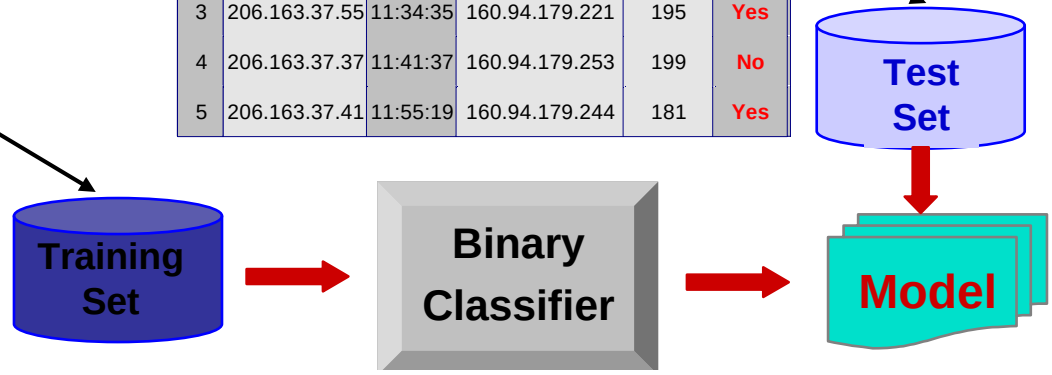
# Anomaly Detection all'opera

| Tid | SrcIP | Start time | Dest IP | Dest Port | Number of bytes | Attack |
|---|---|---|---|---|---|---|
| 1 | 206.135.38.95 | 11:07:20 | 160.94.179.223 | 139 | 192 | No |
| 2 | 206.163.37.95 | 11:13:56 | 160.94.179.219 | 139 | 195 | No |
| 3 | 206.163.37.95 | 11:14:29 | 160.94.179.217 | 139 | 180 | No |
| 4 | 206.163.37.95 | 11:14:30 | 160.94.179.255 | 139 | 199 | No |
| 5 | 206.163.37.95 | 11:14:32 | 160.94.179.254 | 139 | 19 | Yes |
| 6 | 206.163.37.95 | 11:14:35 | 160.94.179.253 | 139 | 177 | No |
| 7 | 206.163.37.95 | 11:14:36 | 160.94.179.252 | 139 | 172 | No |
| 8 | 206.163.37.95 | 11:14:38 | 160.94.179.251 | 139 | 285 | Yes |
| 9 | 206.163.37.95 | 11:14:41 | 160.94.179.250 | 139 | 195 | No |
| 10 | 206.163.37.95 | 11:14:44 | 160.94.179.249 | 139 | 163 | Yes |

*Misuse Detection – Costruzione di modelli predittivi*

categorical temporal categorical continuous class

| Tid | SrcIP | Start time | Dest IP | Number of bytes | Attack |
|---|---|---|---|---|---|
| 1 | 206.163.37.81 | 11:17:51 | 160.94.179.208 | 150 | No |
| 2 | 206.163.37.99 | 11:18:10 | 160.94.179.235 | 208 | No |
| 3 | 206.163.37.55 | 11:34:35 | 160.94.179.221 | 195 | Yes |
| 4 | 206.163.37.37 | 11:41:37 | 160.94.179.253 | 199 | No |
| 5 | 206.163.37.41 | 11:55:19 | 160.94.179.244 | 181 | Yes |

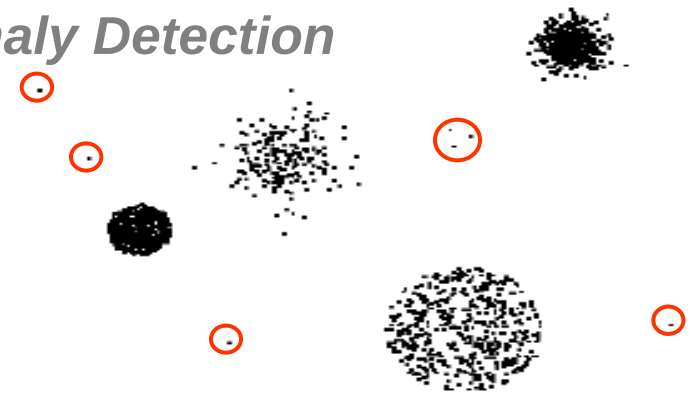



*Inferenza di attacchi tramite associazione di regole note*

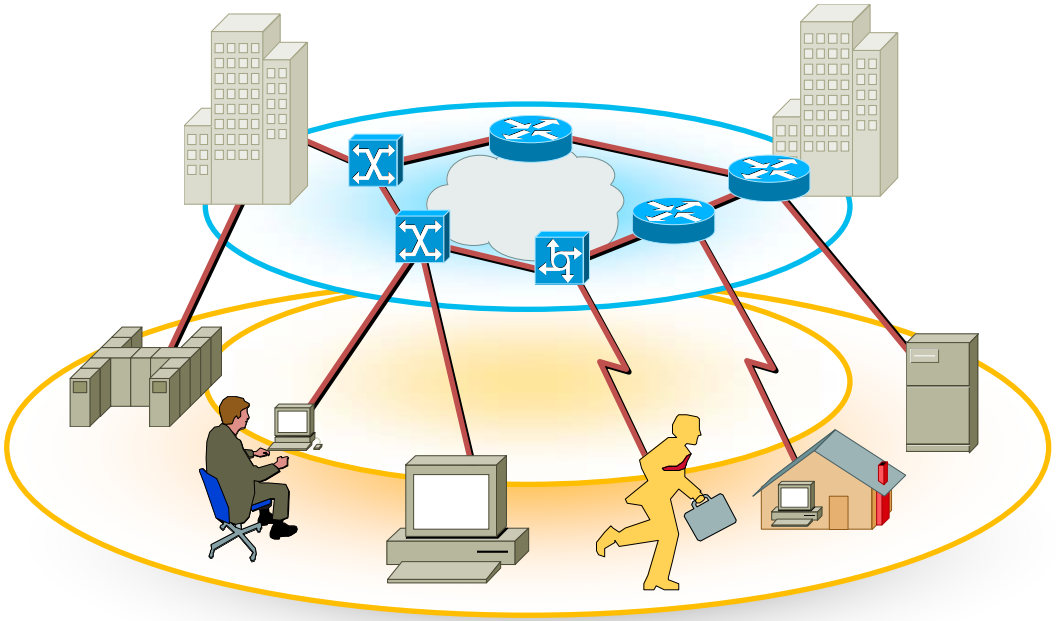
Rules Discovered:

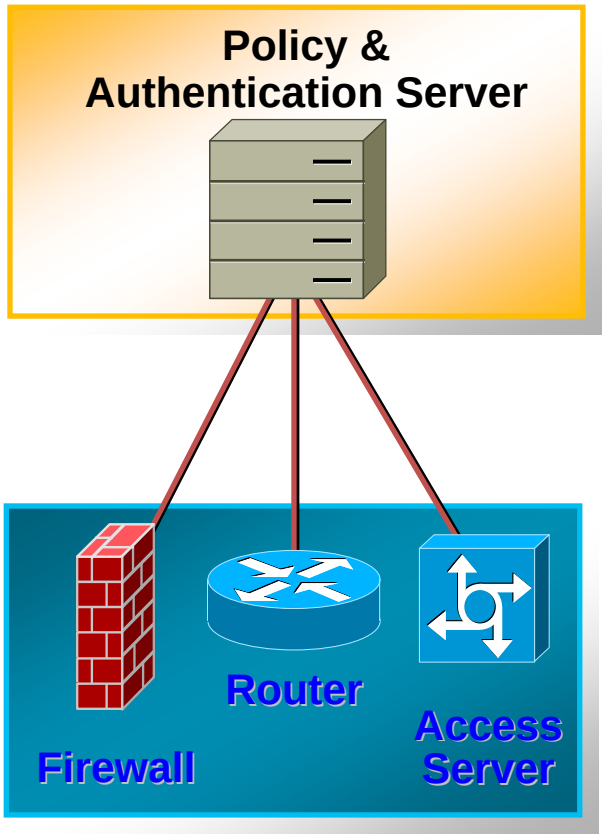
**{Src IP = 206.163.37.95,**
**Dest Port = 139,**
**Bytes ∈ [150, 200]} --> {ATTACK}**

*Anomaly Detection*



# Verso Architetture Security-aware






**UNA RETE SICURA E’ FRUTTO DELL’ARMONIZZAZIONE DI PIU’ COMPONENTI CIASCUNA COL PROPRIO RUOLO NEL CONTESTO DELL’ARCHITETTURA GLOBALE**

# Domande?