Forum ICT Security

The Missing Link

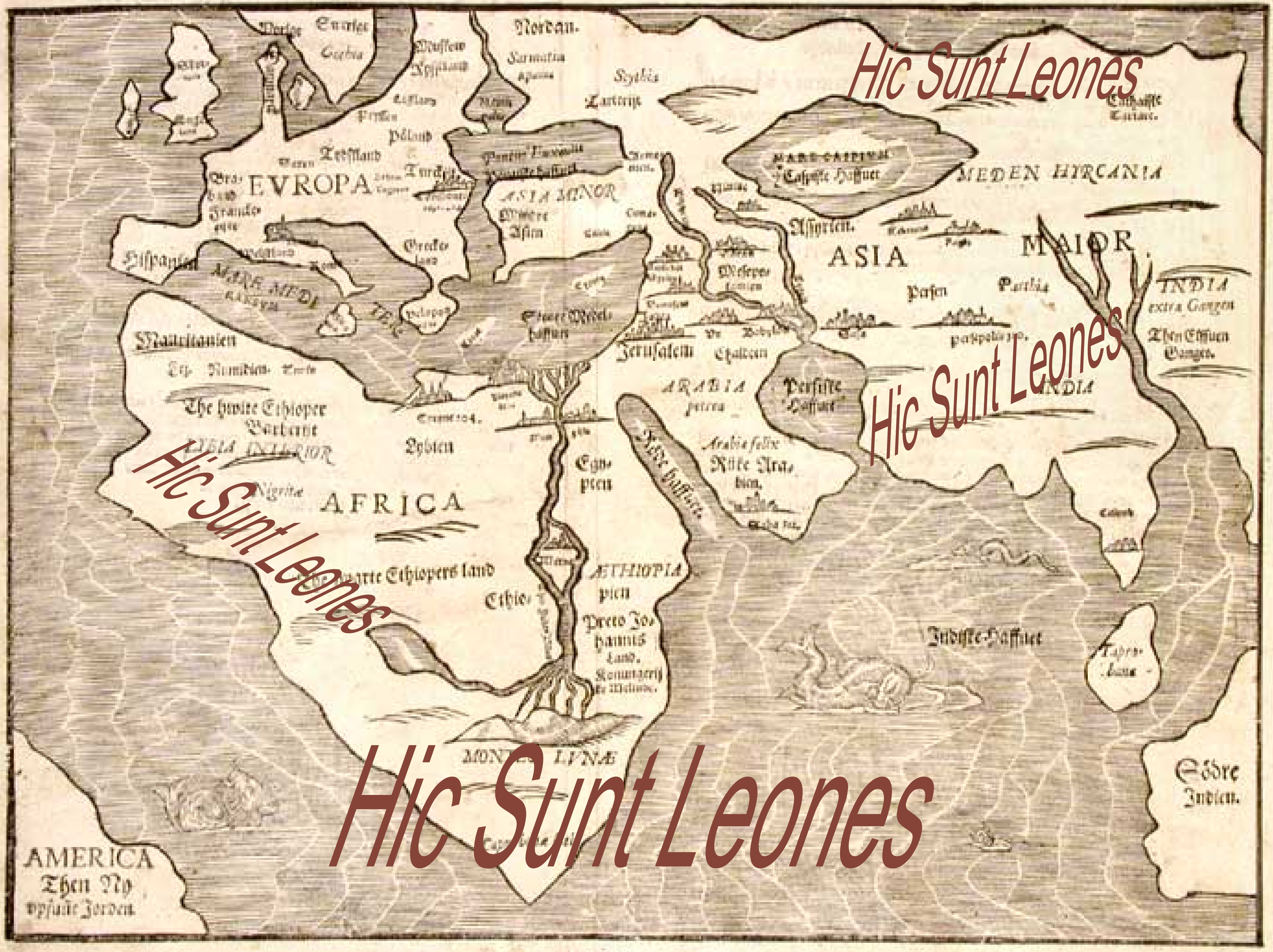
Sandro Fontana, CISSP

CEO Secure Edge

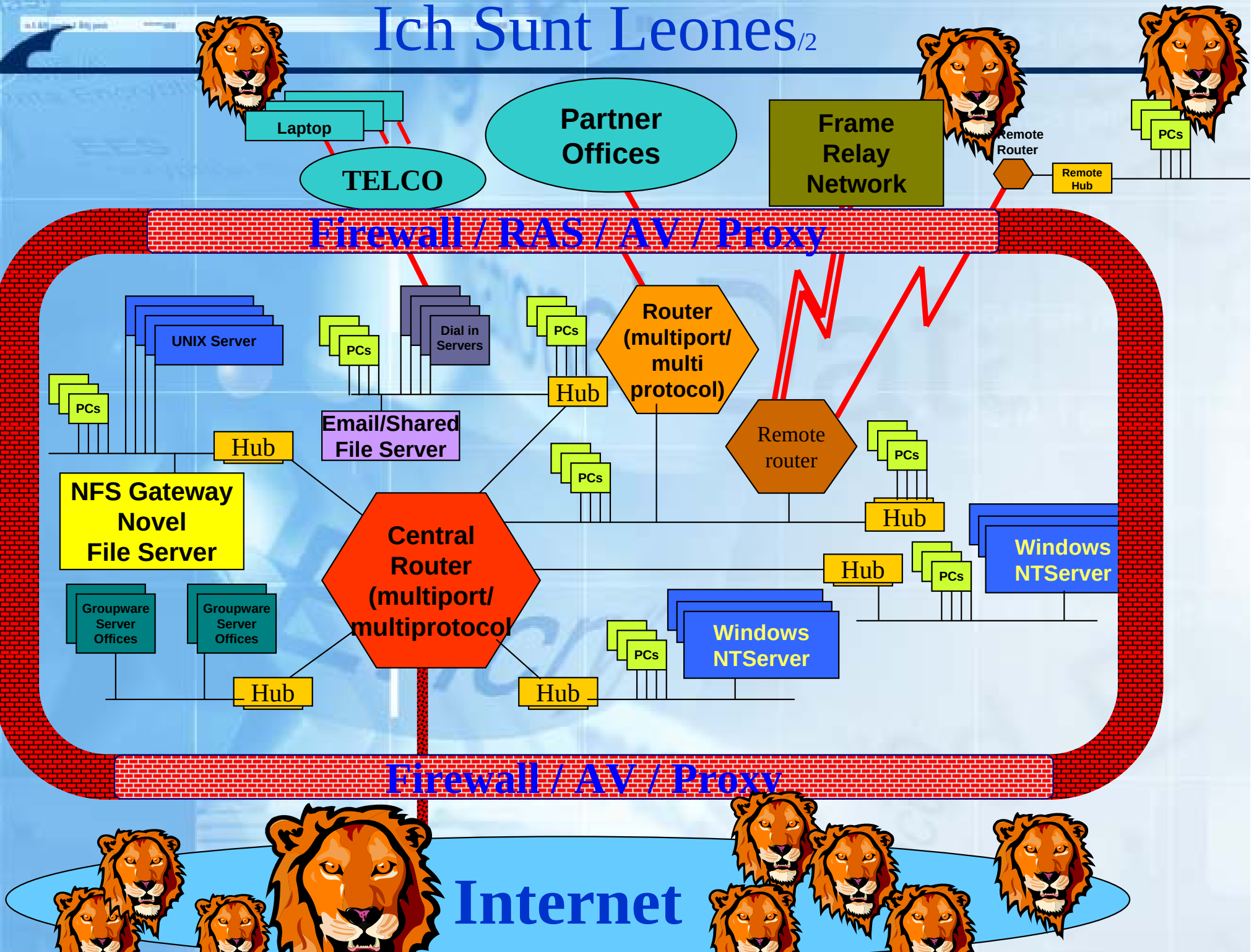
sfontana@secure-edge.com
s.fontana@computer.org

Roma 4 Novembre 2003

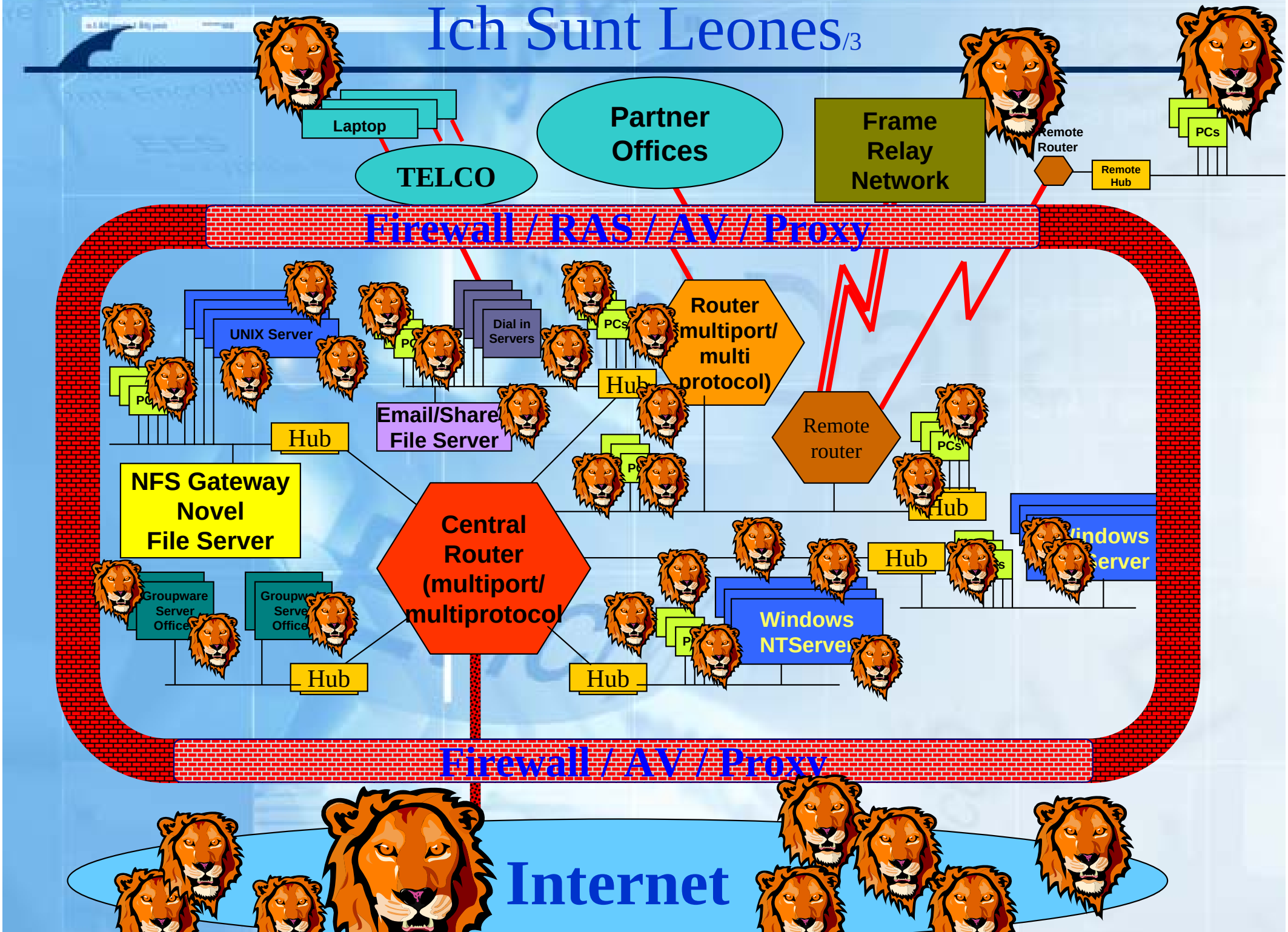
Premessa


Hic Sunt Leones
Hic Sunt Leones
Hic Sunt Leones
Hic Sunt Leones
Nordan.
EVROPA
ASIA MINOR
MARE CASPIVM
MEDEN HYRCANIA
Assyrien.
ASIA
MAIOR.
INDIA
extra Gangen
Then Floden Ganges.
Jerusalem
ARABIA
petrea
Arabia felix
Persiske Haffuet
Mauritanien
The hwite Ethioper
AFRICA
Egypten
ÆTHIOPIA
Preto Johannis land.
Indiske Haffuet
MONTES LVNÆ
Södre Indien.
AMERICA
Then Ny upfunde Jorden

Ich Sunt Leones/2



Ich Sunt Leones/3

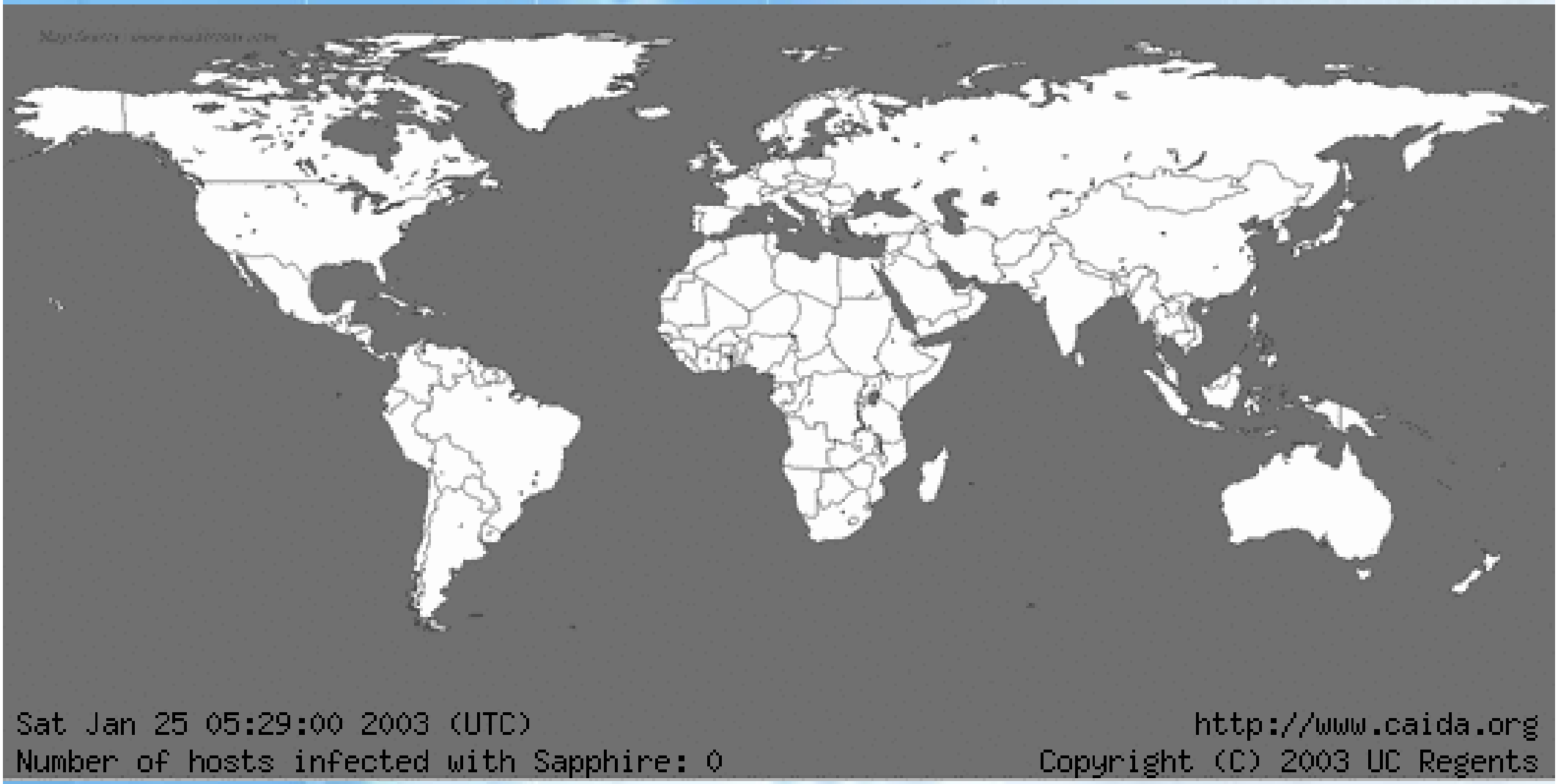


the speed of insecurity/1

"security works in an era of (computer) worms that can spread across the Internet in 10 minutes"

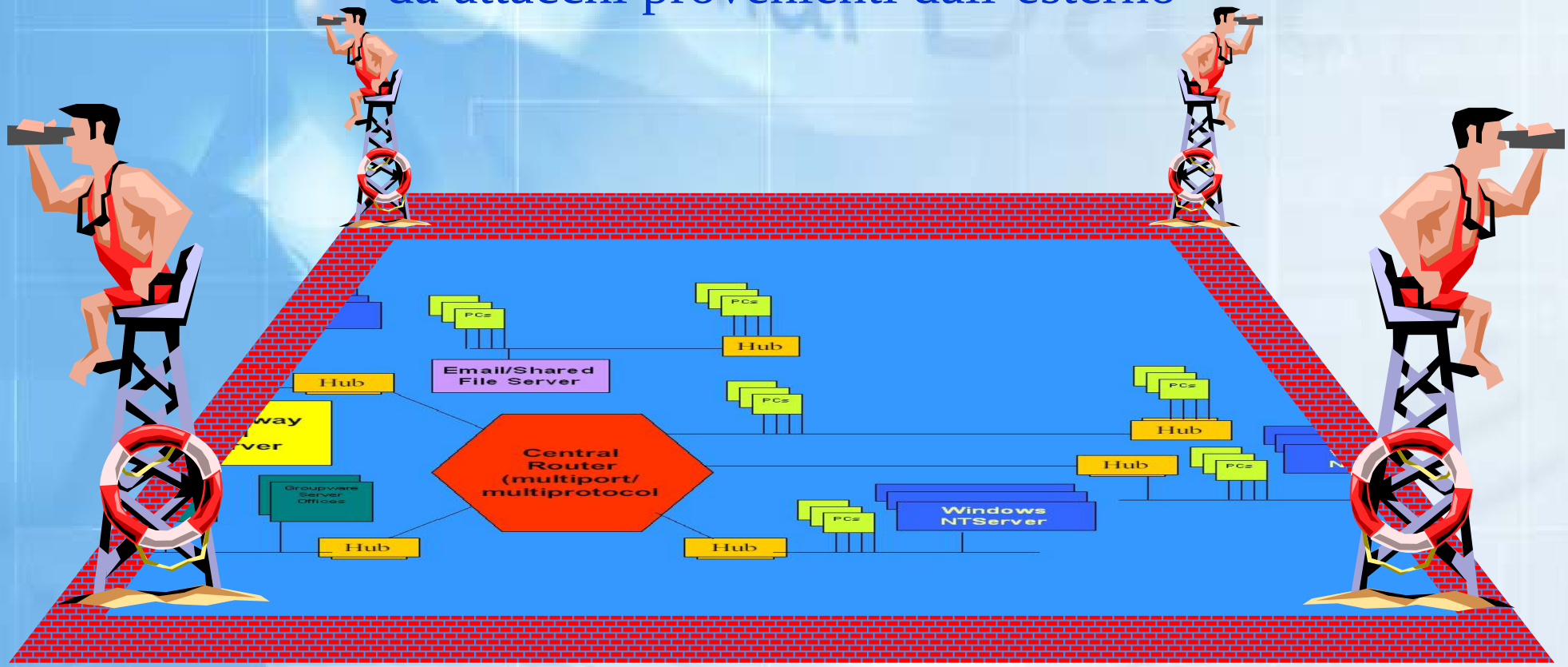
(Bruce Schneier - IEEE S&P, July/August 2003)

the speed of insecurity/2



change viewpoint

non si tratta più soltanto
di difendere i computer presenti nella rete aziendale
da attacchi provenienti dall'esterno

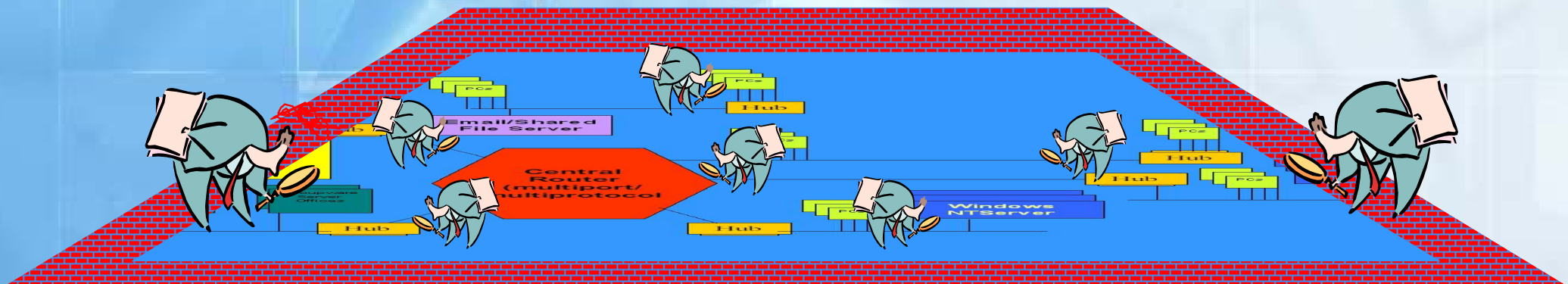


change viewpoint

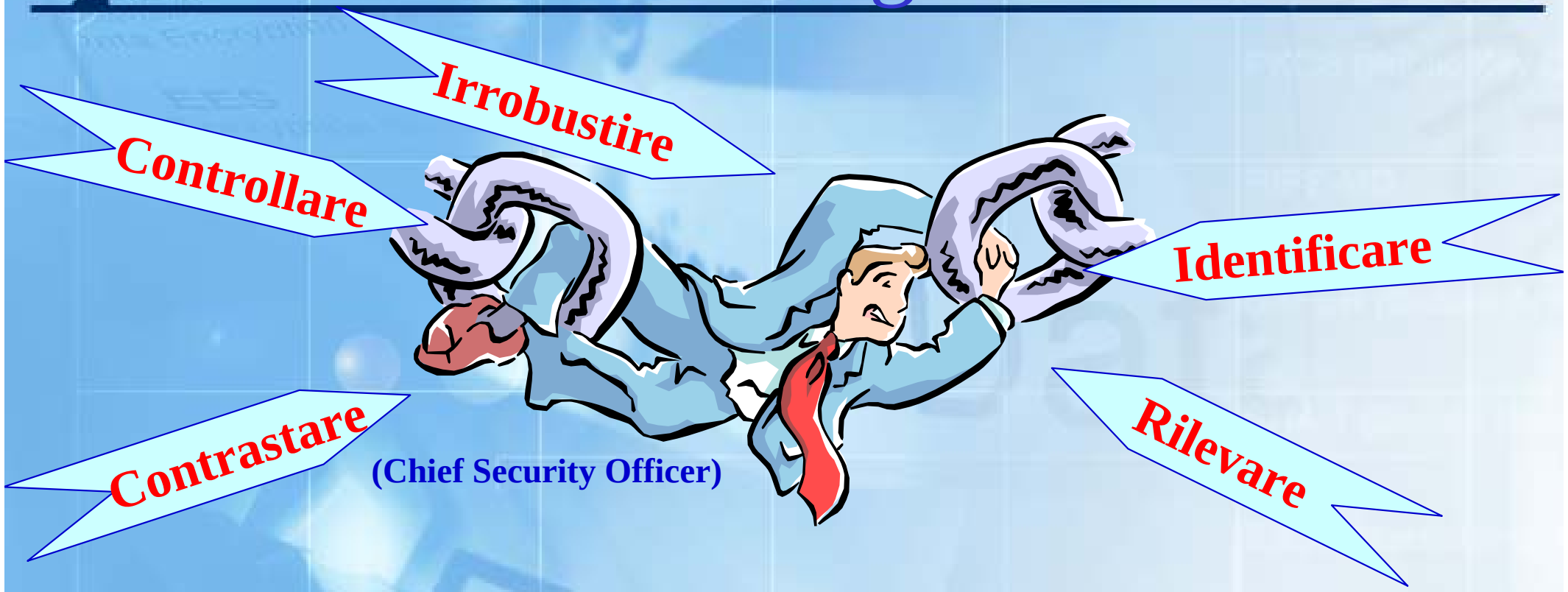
non si tratta più soltanto
di difendere i computer presenti nella rete aziendale
da attacchi provenienti dall'esterno

bisogna inoltre

difendere l'Enterprise Network da eventuali attacchi
provenienti dalle stazioni di lavoro e dai server interni.



the missing link



Nuova responsabilità:

proteggere l'Intranet
dagli attacchi provenienti da computer
attestati all'interno della stessa rete aziendale(*)

(*) (garantendo l'attuale flessibilità)

Mai dimenticare che …

“la sicurezza *è un processo,*
non è un prodotto”

(Bruce Schneier)

Goals

Worm confinement

- un Client od un Server, anche se compromesso, non deve divenire la fonte di ulteriore infezione all'interno dell'Azienda;

Request Verification

- ogni server deve poter qualificare la fonte del traffico di rete in ingresso

CentralManagement

- la gestione delle contromisure deve essere centralizzata

Una proposta

Secure Edge vede un percorso progettuale inserito all'interno del sistema di gestione della sicurezza ad es. l'ISMS della ISO/IEC 17799

Essential Point

- **Policy**
- **Requirements**
- **Management**
- **Tools**

Policy

NetAccess

- Per potere accedere alla intranet ed alle sue risorse ogni macchina, sia Client che Server ed ogni Utente, deve essere autorizzato

Verification

- il parco dei Client e Server installato ed attivo, deve essere tenuto sotto controllo, senza necessità di gestione IP address e/o ethernet address

Identification Authentication

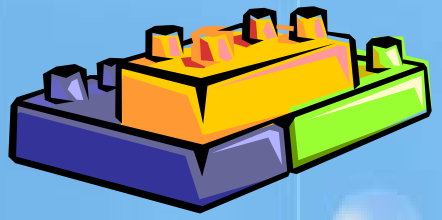
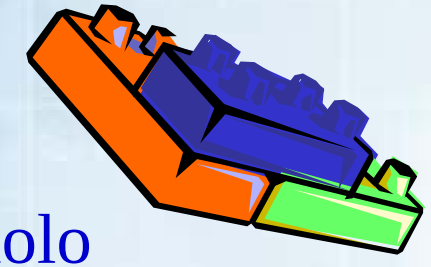
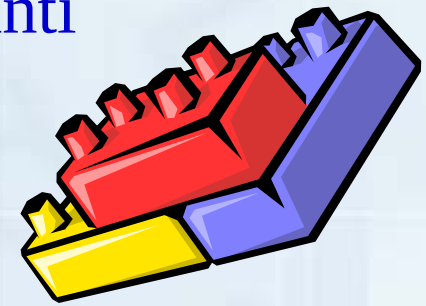
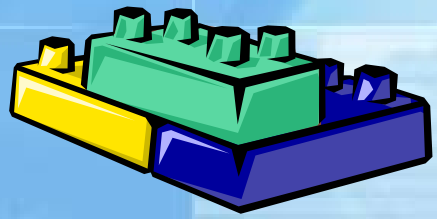
- ogni utente deve essere identificato ed autenticato con meccanismo forte

Effective RT-IDS

- Ogni violazione alle regole precedenti deve poter essere rilevata in tempo reale

Requirements

- Accesso alla intranet controllato tramite:
  - ✓Identificazione certa dei Client e Server connessi
  - ✓Autenticazione forte degli utenti
  - ✓firewall distribuito
- Profilo di accesso specializzato per ruolo
- Consolidamento centralizzato dei log
- Audit in tempo reale sugli eventi rilevanti
- Network Single SignOn®

Management

Policy Manager ☞ il responsabile della definizione dei profili e delle regole che devono essere applicate ai gruppi di macchine (client e server) ed ai ruoli aziendali (users)

Operation Manager ☞ controlla in tempo reale, lo stato delle singole macchine e dei singoli utenti attiva e gestisce gli alert, analizza i log provenienti dal parco macchine interno

Tools

Secure Edge

PcP Enterprise Edition

Gli strumenti/1

PcP-EE_DB

(RDBMS)

è il cuore informativo del sistema;
raccoglie tutti i dati dell'ambiente PcP Enterprise Edition :

- licenze Client e Server
- ruoli aziendali
- profili utenti
- certificati di chiave pubblica di tutti gli *attori* coinvolti
- regole di firewalling
- log globali di tutte le macchine controllate
- heart_beat in tempo reale

Gli strumenti/2

Policy Management Tool

(software client)

permette al Policy Manager la definizione di:

- gruppi di macchine: Client/Server
- ruoli aziendali
- profili
- regole di firewalling

Lavora in locale
con aggiornamento del PcP-EE_DB on demand

Gli strumenti/3

Monitor Console

E' l'interfaccia web al PcP-EE_ DB che
permette all'Operation Manager:

- l'interrogazione, l'elaborazione e la presentazione
delle informazioni generate dai software PcP-EE in esercizio
su tutte le macchine Client/Server Windows all'interno dell'Azienda;
- la configurabilità e la gestione di allarmi
- la memorizzazione di *query* ricorrenti

Gli strumenti/4

Policy Server

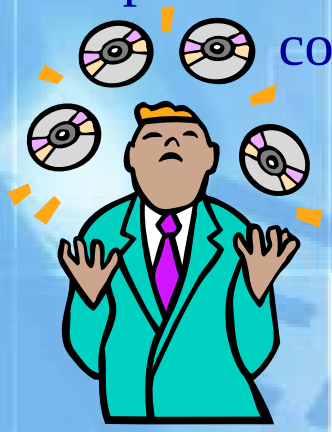
è un servizio presente su uno o più sistemi all'interno dell'azienda permette di:

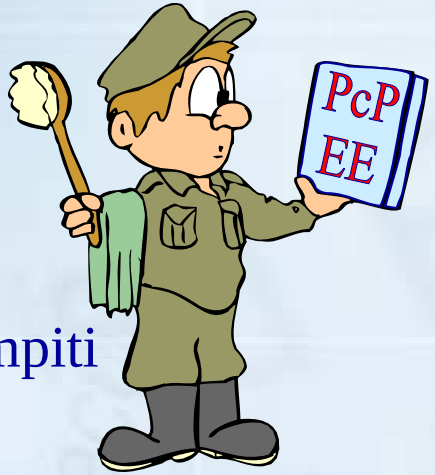
- autenticare le licenze PcP-EE ed i singoli Users;
- distribuire le Policy per i Server ed i Client oltre che le policy specifiche per lo User;
- acquisire i log dalle varie stazioni ed i pacchetti informativi (heart beat) relativi al traffico di rete dei singoli sistemi
- aggiornare PcP-EE_ DB centrale

Gli Strumenti/5

Distribuited Security Agent

é presente su ogni client ed ogni server aziendale
con sistema operativo Microsoft

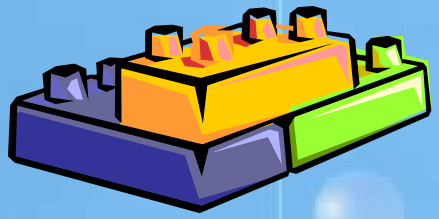


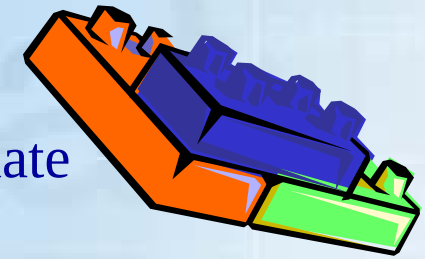


questo software assolve una serie di compiti

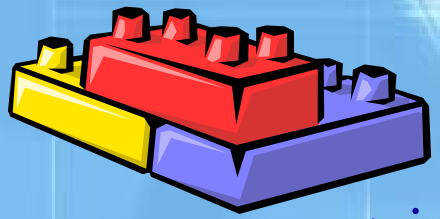
PcP-EE: duty/1

ogni macchina viene associata ad una licenza PcP-EE



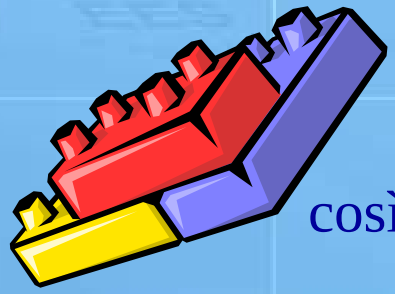


ad ogni macchina vengono assegnate
specifiche regole di firewalling
ed il profilo di protezione del gruppo a cui la macchina appartiene



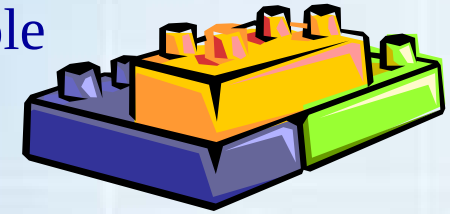
un utente che voglia lavorare su una macchina
viene prima identificato ed autorizzato,
quindi le regole di firewalling ed il profilo di protezione
associato al ruolo che l'utente, in quel momento, incarna in azienda
sono calate sulla macchina su cui opera

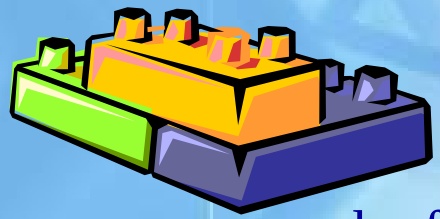
PcP-EE: duty/2



il traffico di rete viene bloccato/abilitato,
così come viene indicato dalle regole di firewalling

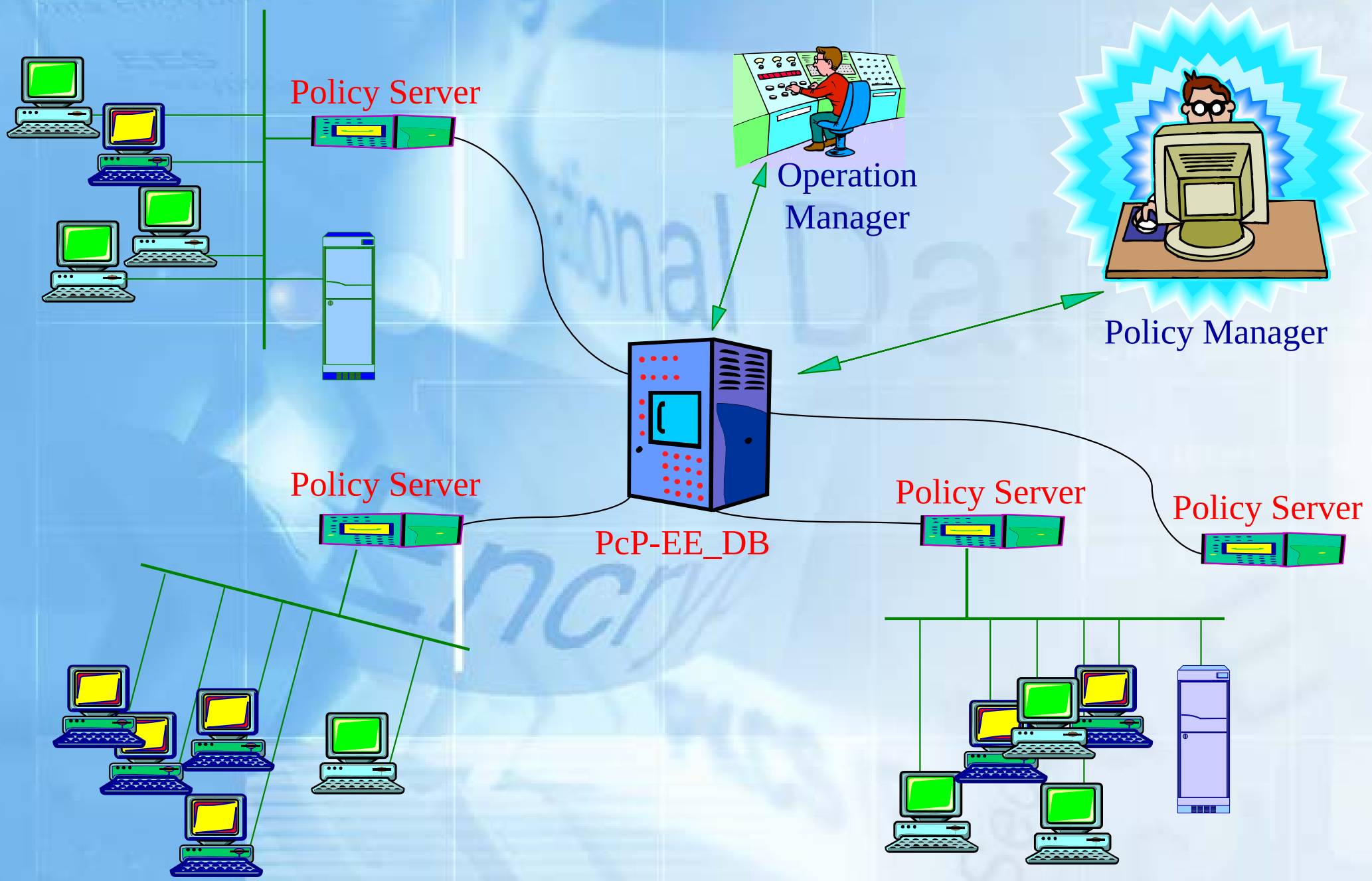
viene generato il log relativo al *matching* delle regole di firewalling,
se questa funzione è richiesta per queste regole





dichiara la propria *esistenza in vita*
tramite pacchetti statistici
che fungono da *HeartBeat* per PcP-EE stesso

Riepilogo


Policy Server
Operation Manager
Policy Manager
Policy Server
PcP-EE_DB
Policy Server
Policy Server

per concludere …

“la sicurezza *è un processo,*
non è un prodotto”

(Bruce Schneier)

Thank you for your attention