REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Come proteggere i sistemi informatici? Un approccio globale alla sicurezza!

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.

Agenda

- Sistemi sotto attacco.
  Chi minaccia i nostri sistemi?
- Difendere i sistemi!
  Quale approccio alla sicurezza?
- Gestione della sicurezza
- Meccanismi e strumenti di protezione
- Reagire ad un attacco

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

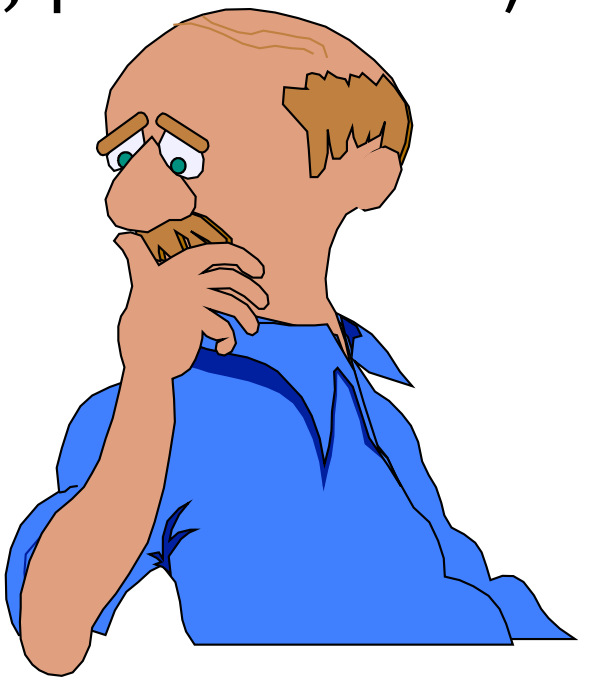
Sistemi sotto attacco. Chi minaccia i nostri sistemi?

Perché proteggersi?

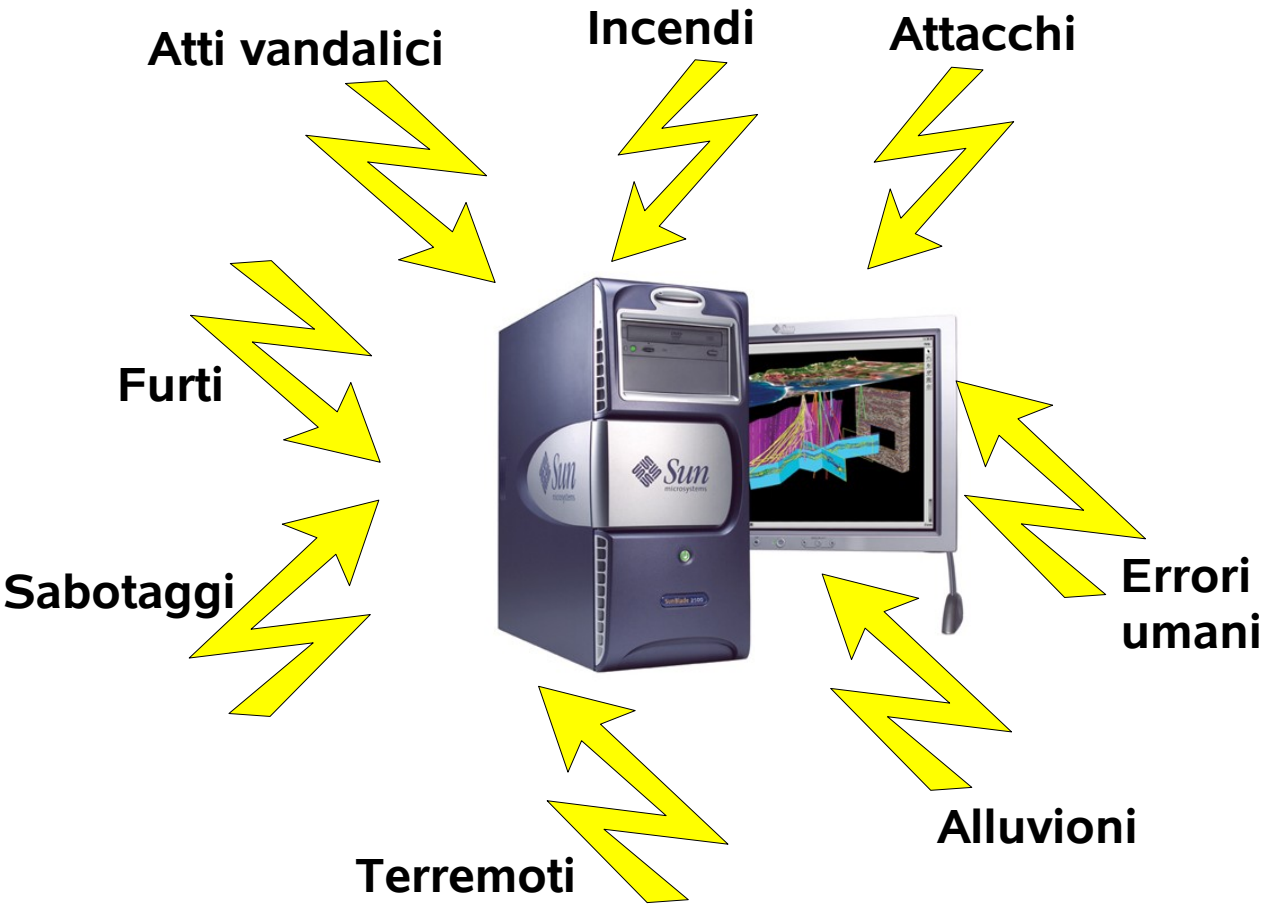
- Evitare incidenti
  - Cintura di sicurezza
  - Airbag (frontale/laterale)
  - Giuda prudente
  - Rispetto segnaletica
- Evitare furti
  - Antifurto
  - Posteggio a pagamento

Cosa proteggere?

- Sistemi, console, postazioni, periferiche...
- Software
- Le connessioni di rete
- Supporti removibili (CD, cassette, penne USB...)
- I dati, le informazioni e i file trattati dai sistemi....

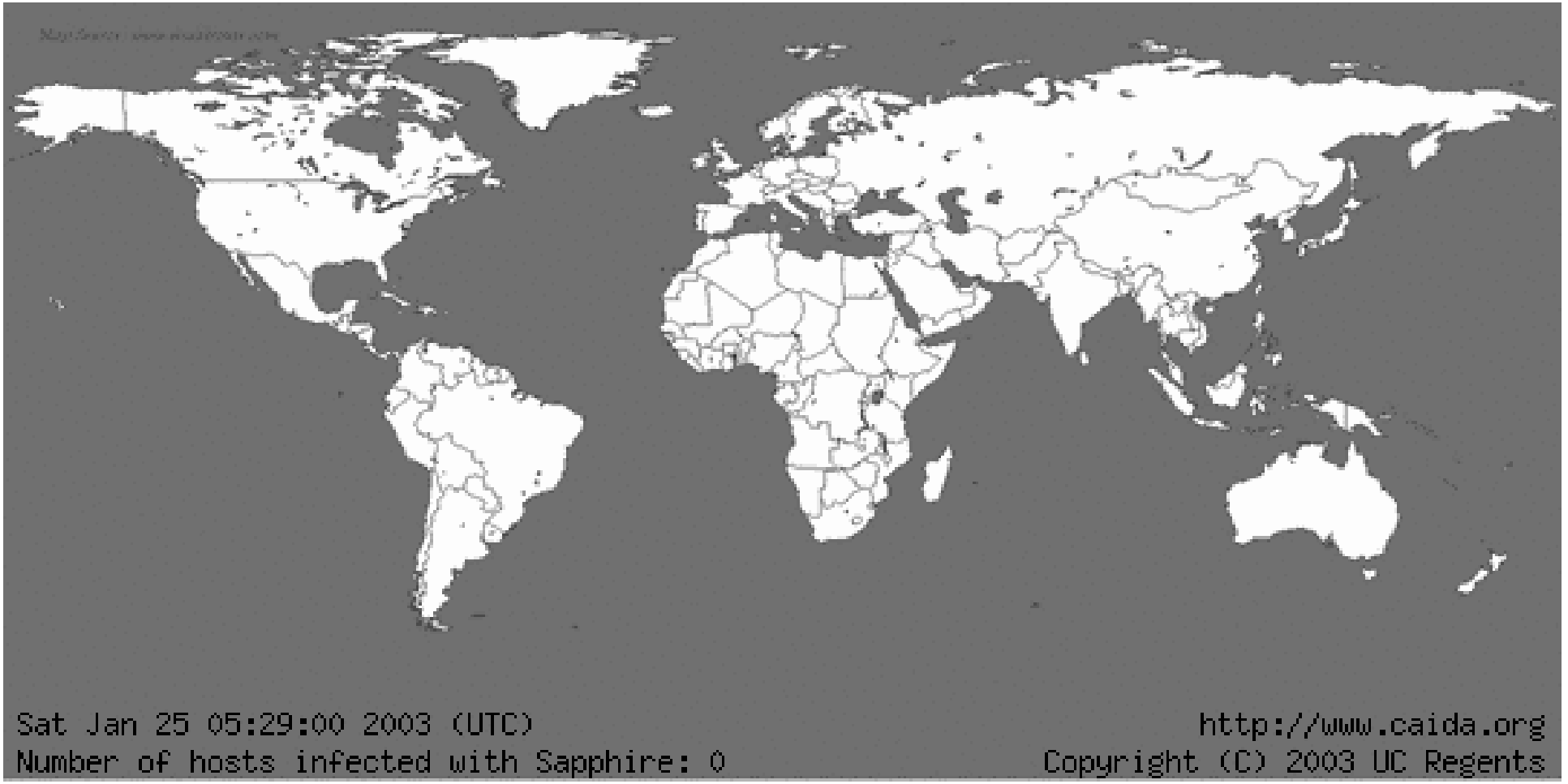


Proteggerlo, ma da che cosa?

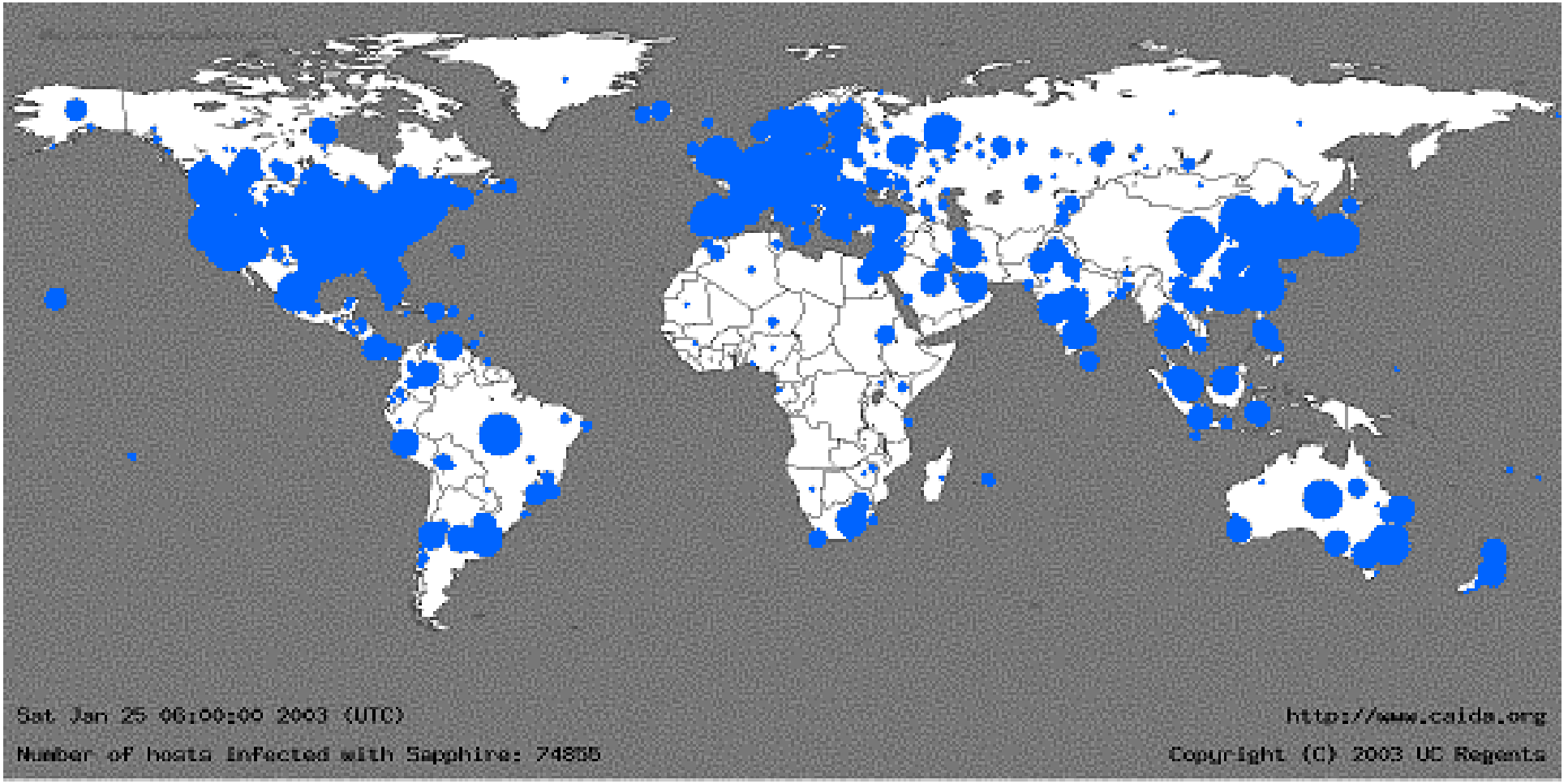


"I just wanted to prove how insecure these sites are"

SQL Slammer - prima



SQL Slammer - dopo



Quando un sistema è sicuro?

Attacchi fisici

- Il furto
  - Dischi USB, nastri, CD, DVD, documenti in formato cartaceo, portatili, agende - più in generale i piccoli oggetti - sono i più esposti ai furti

- Duplicazione non autorizzata
  - Solitamente non lascia tracce e quindi è molto difficile scoprirla.
- Danneggiamento o Vandalismo

Intercettazioni

- C'è molta più gente che ascolta di quanto pensi...
- Sniffing
  - analisi del traffico in transito sulla rete
  - non modificano il traffico
  - difficili da individuare

- Spoofing
  - impersonificazione di un apparato
  - Programma di emulazione di un servizio

Intercettazioni

- Contromisure
  - Protezione degli apparati e degli accessi di rete
  - Segmentazione delle reti
  - Limitare i diritti di installazione dei software
  - Prevedere comunicazioni crittate che rendono inservibili qualunque informazioni catturata sulla rete

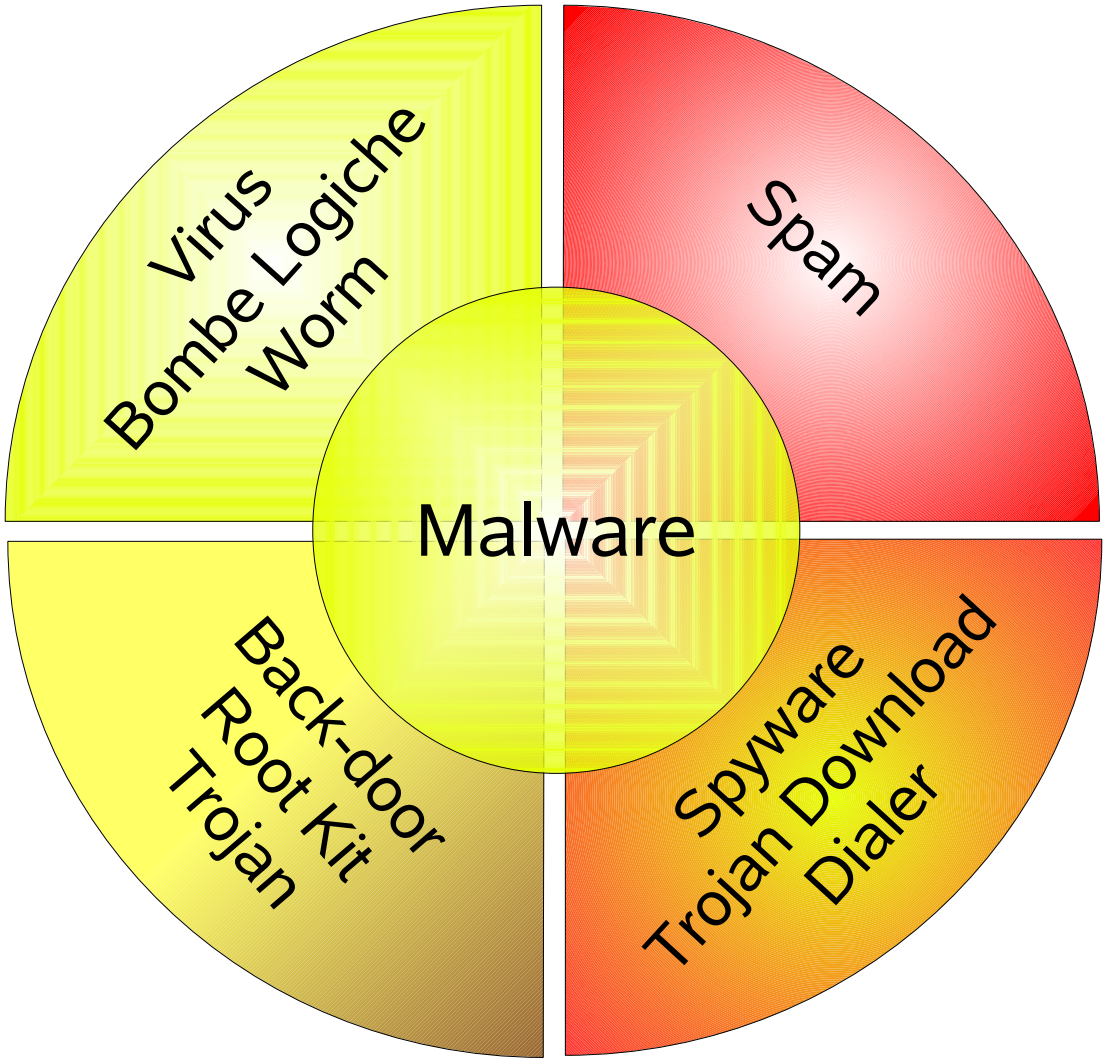
Intrusione

- Violazione delle credenziali degli utenze (ingresso privilegiato)
- Contromisure
  - Crittare le sessioni di autenticazione;
  - Sistemi robusti di autenticazione;
  - Regole scelta password
  - Formazione

Intrusione

- Bachi, errori di configurazione, servizi non protetti
- Contromisure
  - Disattivare i servizi inutili
  - Aggiornamento di patch, hot fix...
  - Configurare sistemi e i programmi
  - Restringere le politiche di accesso di firewall e router

Virus e company



Virus e company

- Come classificare un Virus
  - il tipo di danno che causano
  - modalità di infezione
  - modalità di mimetizzazione
- Contromisure:
  - Antivirus ed antispam
  - Aggiornamento dei sistemi
  - Firewall

Denail of services e Deduzione

- Saturare una risorsa rendendola indisponibile

- Contromisure
  - Configurazione degli apparati di rete
  - Segmentazione e filtri tra le varie sottoreti
- Attacchi di deduzione
  - Ricavare informazioni riservate sui sistemi incrociando dati provenienti da fonti lecite e illecite.

Social Engineering

- Il fattore umano risulta spesso essere l'anello più debole di un'architettura di sicurezza.
- Ricatto
- Corruzione
  - Chi accede a dati riservati ma ha una posizione minore
- Inganno
  - Sfruttare la buona fede e la disponibilità delle persone.

Social Engineering

- Contromisure
  - Un'adeguata formazione del personale
  - Politica gestione emergenze
  - Contatto per segnalazioni di richieste anomale

Eventi accidentali

- Guasto (rottura hardware o errore software)
- Errore umano
- Calamità naturale
- Contromisure
  - Limitare l'insieme di operazioni fornite agli utenti
  - Controllando la validità dei dati immessi
  - Salvataggio e ripristino dei dati
  - Business Continuity

REGIONE DEL VENETO

Direzione Sistema Informatico

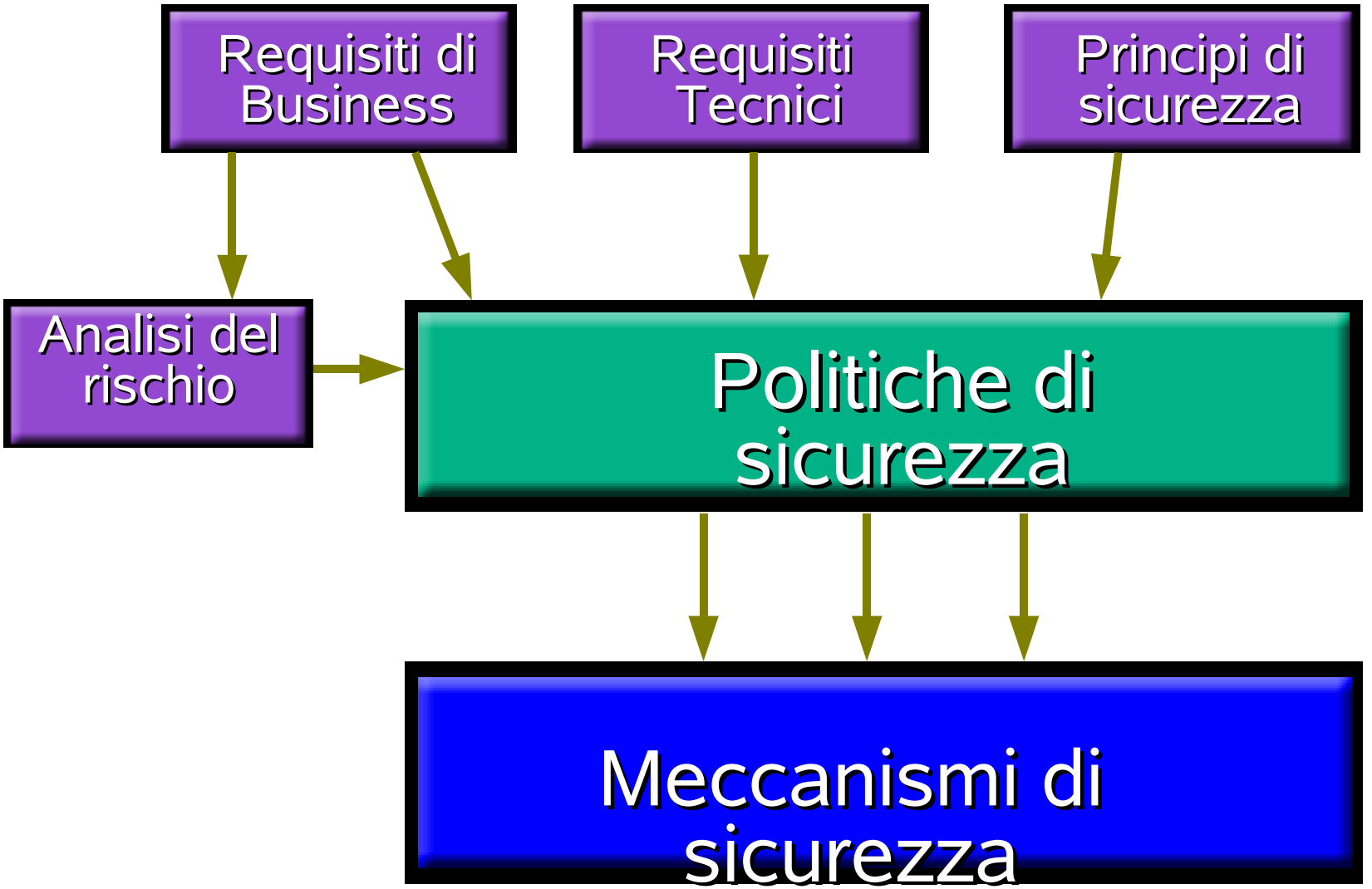
Sun microsystems

Difendere i sistemi! Quale approccio alla sicurezza?

Difendere i sistemi

- Prevenire
  - Prevenire e meglio che curare
- Controllare
  - Catturare gli intrusi con le mani nel sacco
- Ripristinare
  - Essere pronti al caso peggiore

Difendere i sistemi



Politica di sicurezza

- La “Politica di Sicurezza Informatica” è l'insieme organico delle regole formali che definiscono la modalità di gestione degli strumenti informatici e dei dati dell'azienda o dell'ente in esame.

- Le Politiche di Sicurezza decidono cosa sarà fatto.



Meccanismi di sicurezza

- I “Meccamismi di Sicurezza Informatica” sono l'insieme degli strumenti informatici che automatizzano le regole stabilite dalle politiche di sicurezza.
- I Meccanismi di Sicurezza decidono come sarà fatto.



Analisi del Rischio

Rischio = **Costo derivante da un evento indesiderato** * **Probabilità del verificarsi dell'evento**

Analisi del Rischio

- Identificare i requisiti di sicurezza
- Calcolare il rischio di violazione di tali requisiti
- Individuato i rischi è possibile scegliere le migliori contromisure
  - Risolvono il problema
  - Costo inferiore al rischio

- Tool e metodologie di supporto

Rischio residuo

Rischio residuo = Rischio - Contro-misure

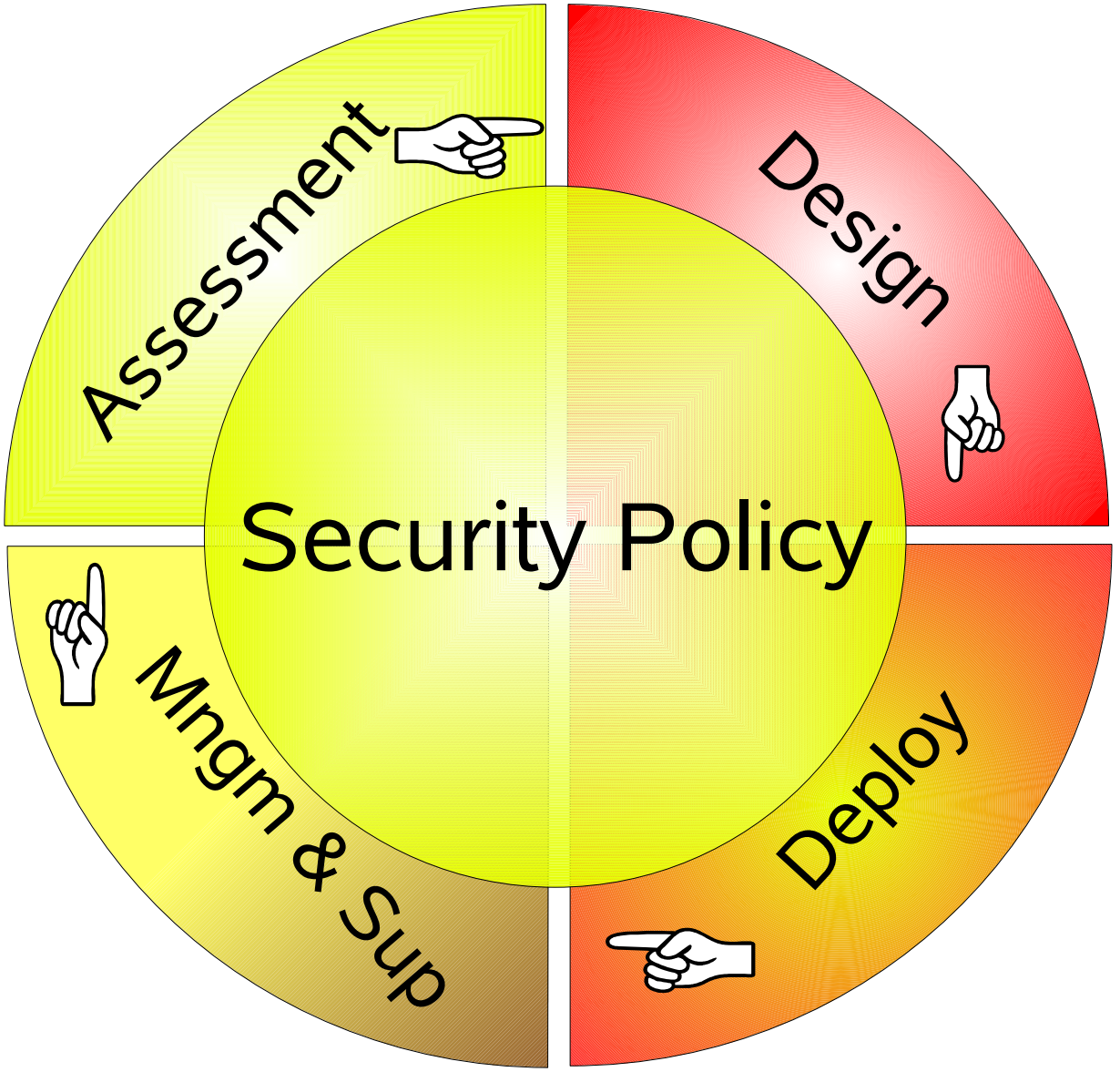
REGIONE DEL VENETO

Direzione Sistema Informatico

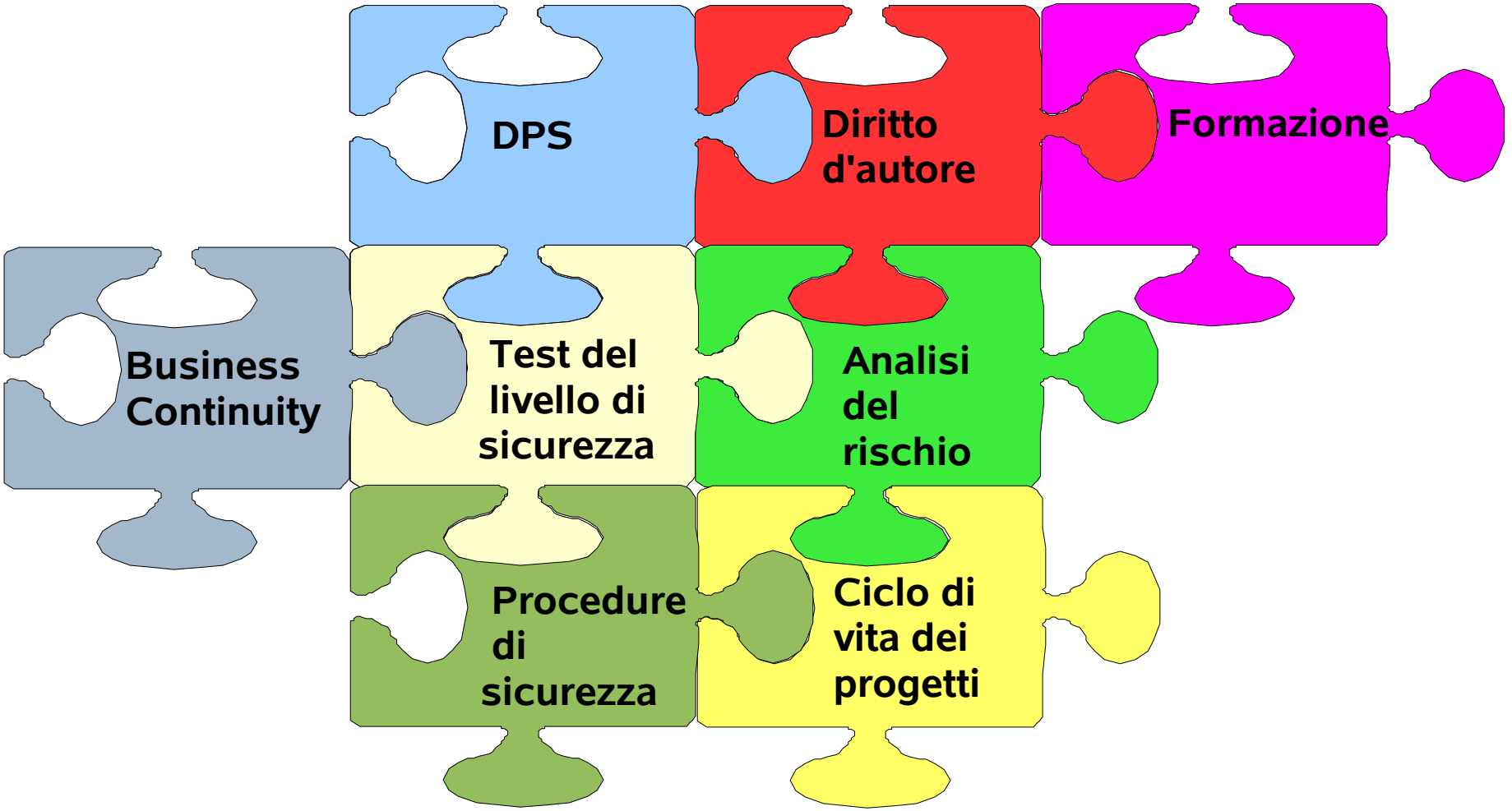
Sun microsystems

Gestione della sicurezza?

Ciclo di vita della sicurezza



Gestione della sicurezza



Politica di Sicurezza

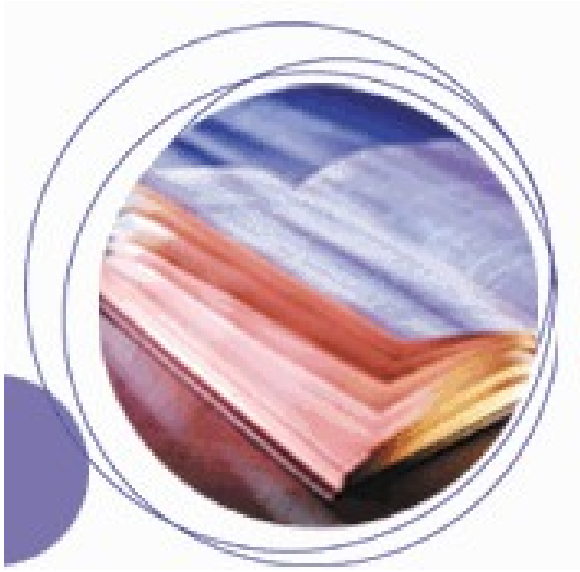
- Regole di riferimento per i nostri amministratori ed i nostri utenti
- Regole per la protezione da:
  - attacchi
  - errori umani e social engineer
  - disastri naturali
- Tiene conto delle tecniche di protezione

Politica di sicurezza

- Proporzionate al rischio
- La politica di sicurezza deve essere:
  - corretta
  - completa
  - comprendente gli aspetti gestionali
- Definisce le responsabilità personali
- Documentazione

Politica di Sicurezza: argomenti

- I principi e gli obiettivi di sicurezza.
- Le regole di sicurezza aziendale.
- Le attività consentite e quelle proibite.
- Le procedure operativo o modalità per applicare la politica all'ambiente.
- L'indicazione delle responsabilità dei singoli.



Modalità di cambio della Politica

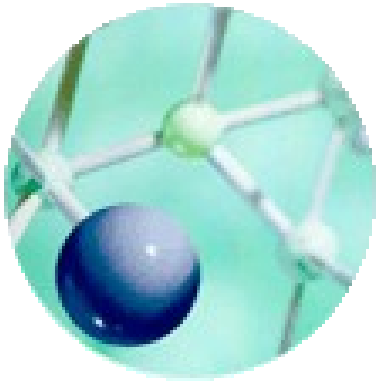
- Processo di aggiornamento:
  - Chi coinvolgere
  - Formazione del personale
  - Revisione periodica
- Allineamento alle nuove legislazioni
- Processo di verifica del reale stato della sicurezza dei sistemi

Documento Programmatico sulla Sicurezza

- Descrive:
  - le tipologie di dati trattati,
  - i sistemi coinvolti nel trattamento di questi dati,
  - le misure di sicurezza in essere e da adottare per proteggere questi dati,
  - gli strumenti tecnologici utilizzati,
  - gli interventi formativi per aggiornare il personale aziendale.
- Un costo o un opportunità?

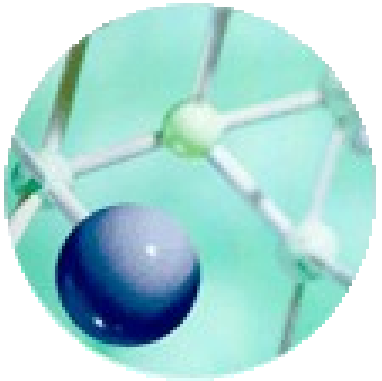
Architetture sicure

- Deve essere redditizio
  - Il costo di protezione delle risorse non deve avvicinarsi a o eccedere il costo della perdita potenziale ?
- Integrata e onnicomprensiva
- Realizzabile, estendibile, scalabile, gestibile e funzionalmente efficiente
- Aggiornabile a nuove tecnologie



Architetture sicure

- Supportare un modello di autenticazione robusta degli utenti
- Proteggere i dati in ogni fase della loro vita:
  - Creazione e modifica
  - Memorizzazione
  - Comunicazione (transito sulla rete)
  - Archiviazione
  - Dismissione
- Risponde alle minacce identificate

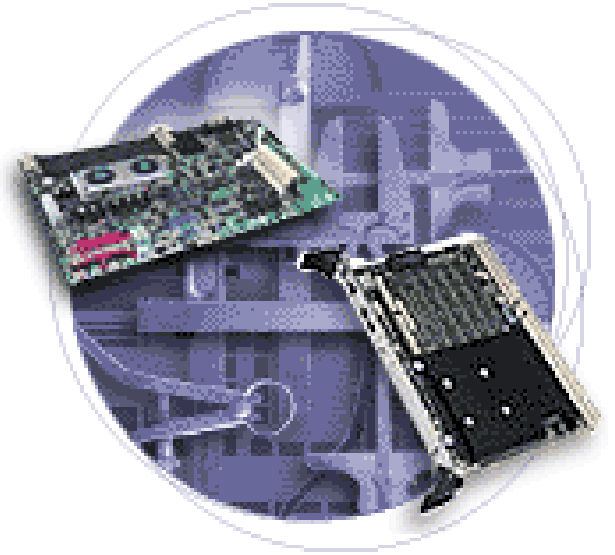


Raccomandazioni Pratiche

- Tutti i rischi identificati devono essere indirizzati
  - Attenuato
  - Accettato
  - Trasferito
- Tutte le architetture di sicurezza dovrebbero basarsi sul principio "Need-to-Know"
- Tutti le attività e i processi insicuri devono essere isolati
- Le attività critiche devono essere tracciate

Protezione a tutti i livelli

- Accessi remoti (sicurezza perimetrale)
- Rete
- Sistema operativo
- Applicativo
- Gestione degli accessi
- Archiviazione dei dati

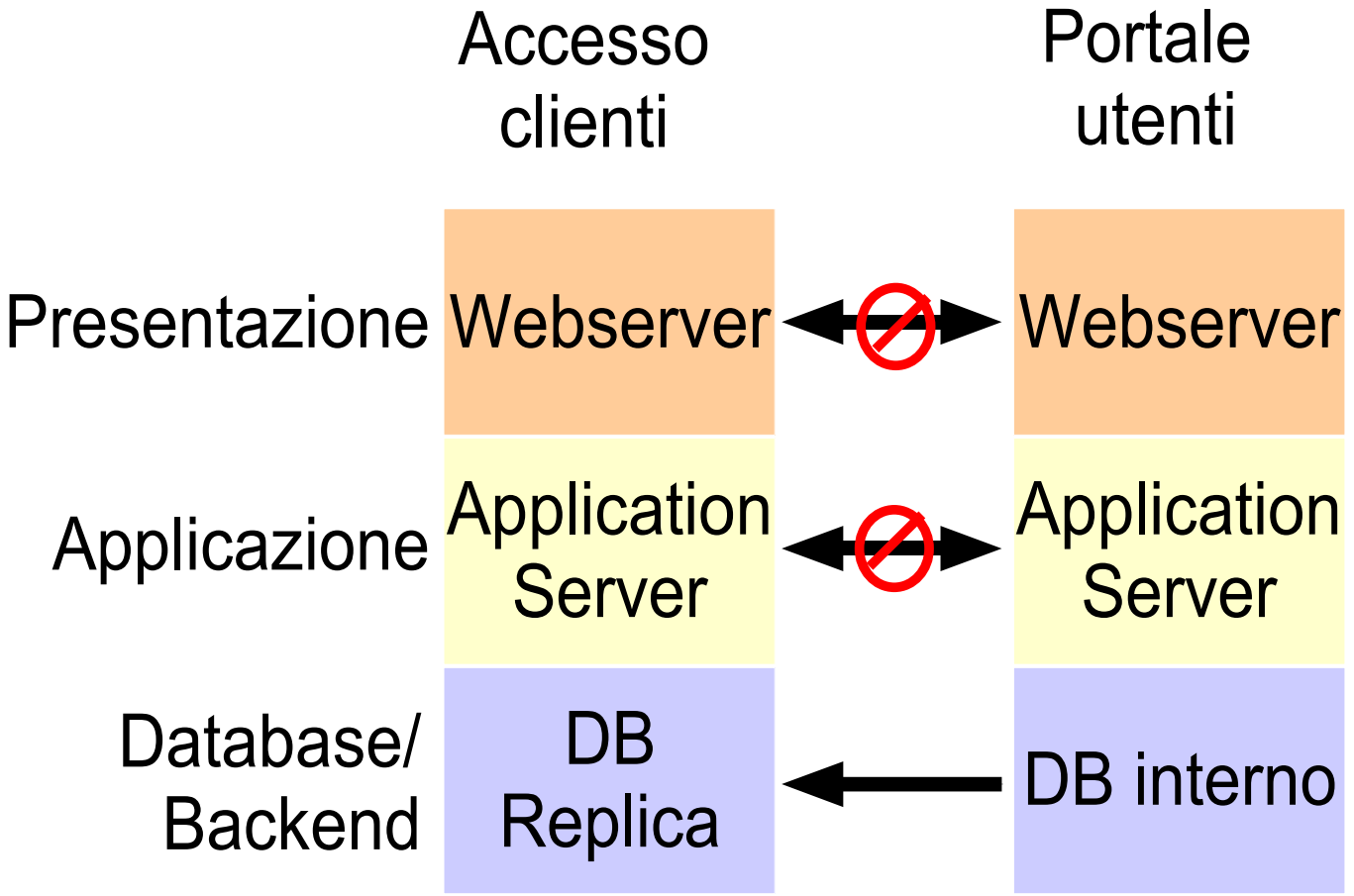


- Dismissione sistemi e supporti dati
- Protezione delle sessioni di amministrazione
- Formazione personale

Pensare al caso peggiore

- Una compromissione o un errore di un singolo punto non deve compromettere tutta l'infrastruttura.
- Prevedere strumenti di controllo per individuare tentativi di attacco
- Prevedere un piano di ripristino in caso di compromissione.

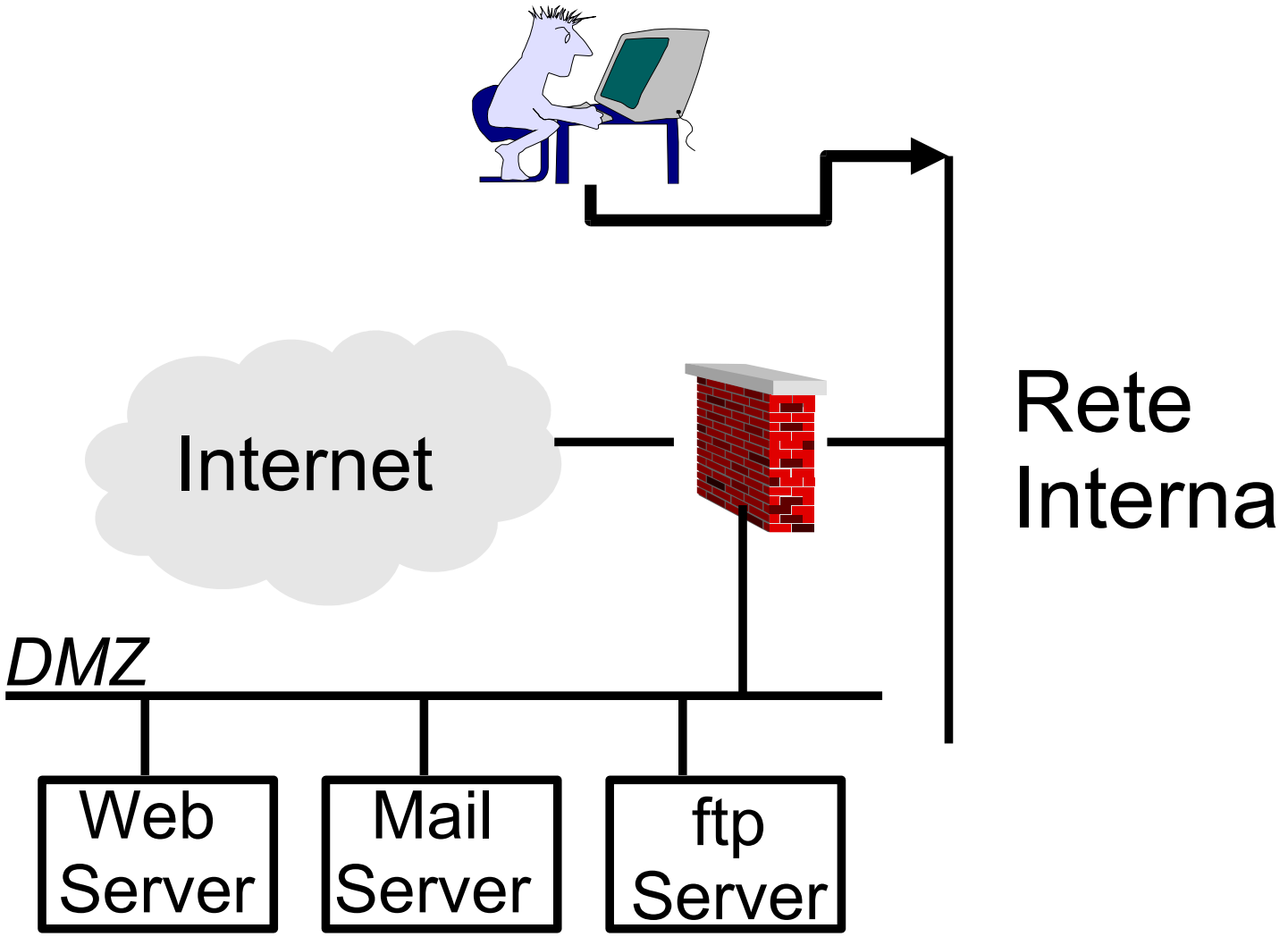
Protezione orizzontale e verticale



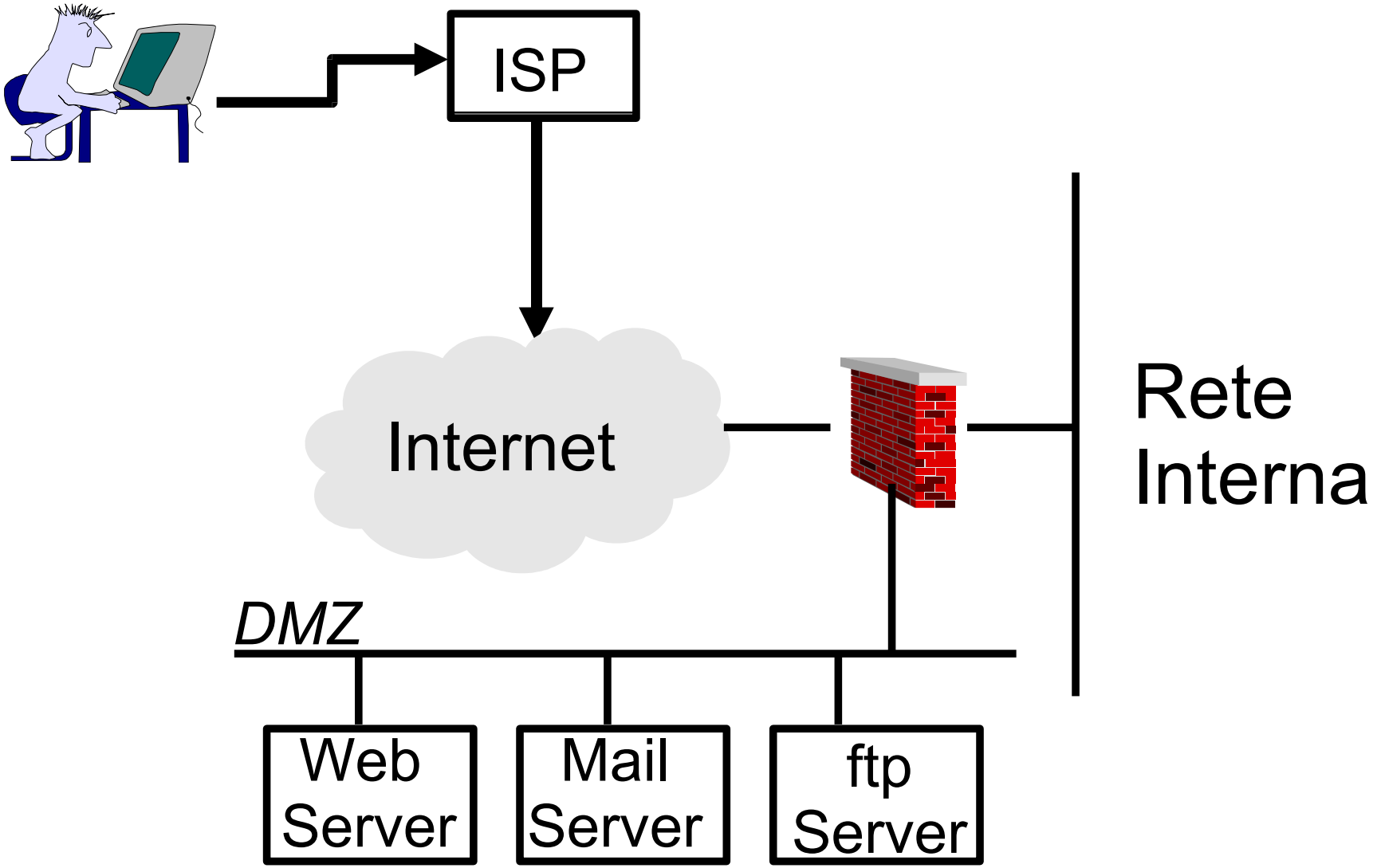
Verifica del livello di sicurezza

- Penetration Test
  - White hat
  - Black hat
- Eseguiti periodicamente
- Eseguiti da un esterno al progetto
- Test manuali e automatici
- Verifica sistemi di allarme

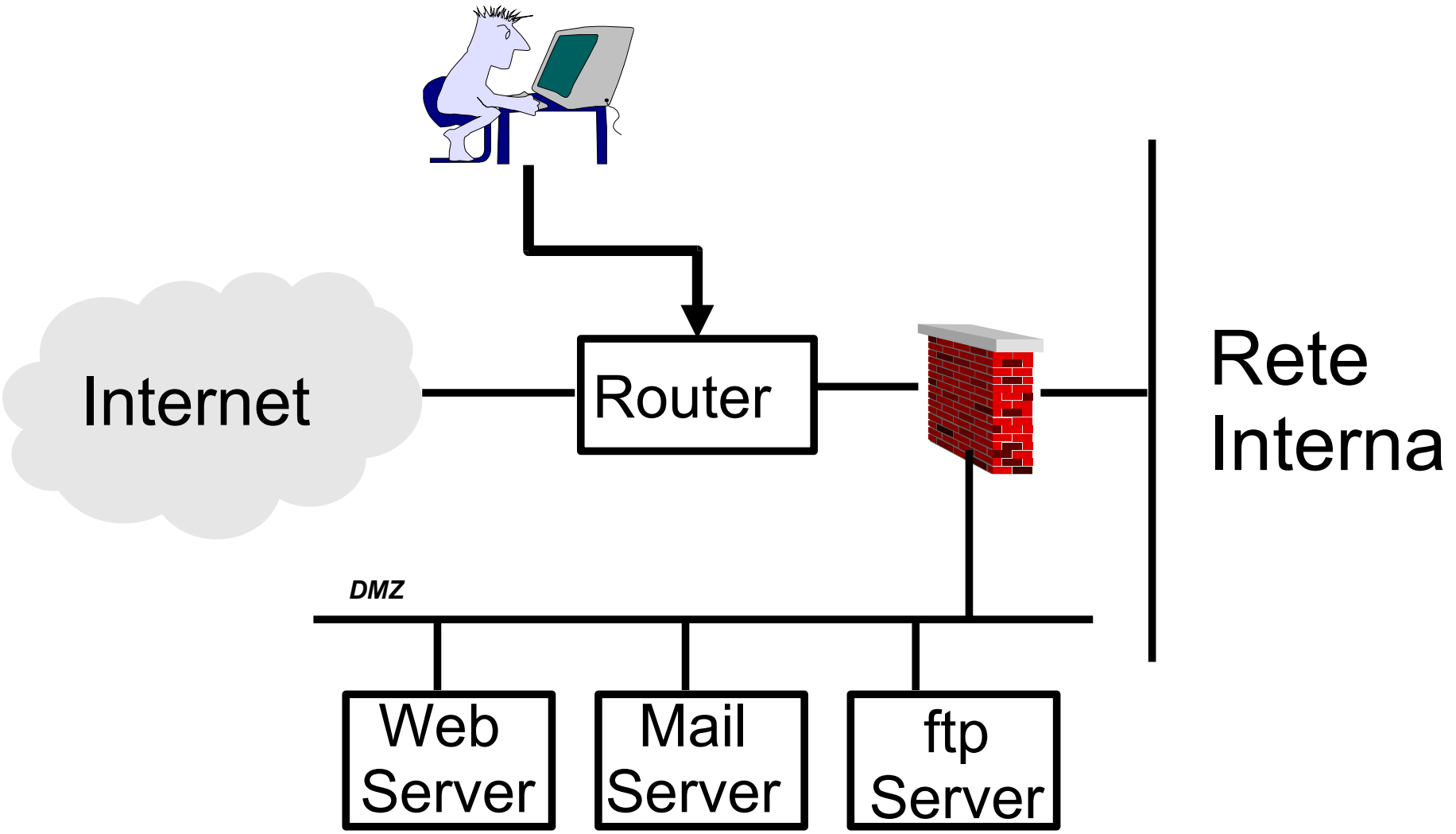
Probing dall'interno



Probing dall'esterno



Probing dall'esterno



Quali test

- Port-scanning
  - Operation System Identifications
- Network Mapping
- Vulnerability scanning
  - Web Vulnerability scanning
- Denial of Services test
- War-dialing
- Sniffing
- Social Engineering

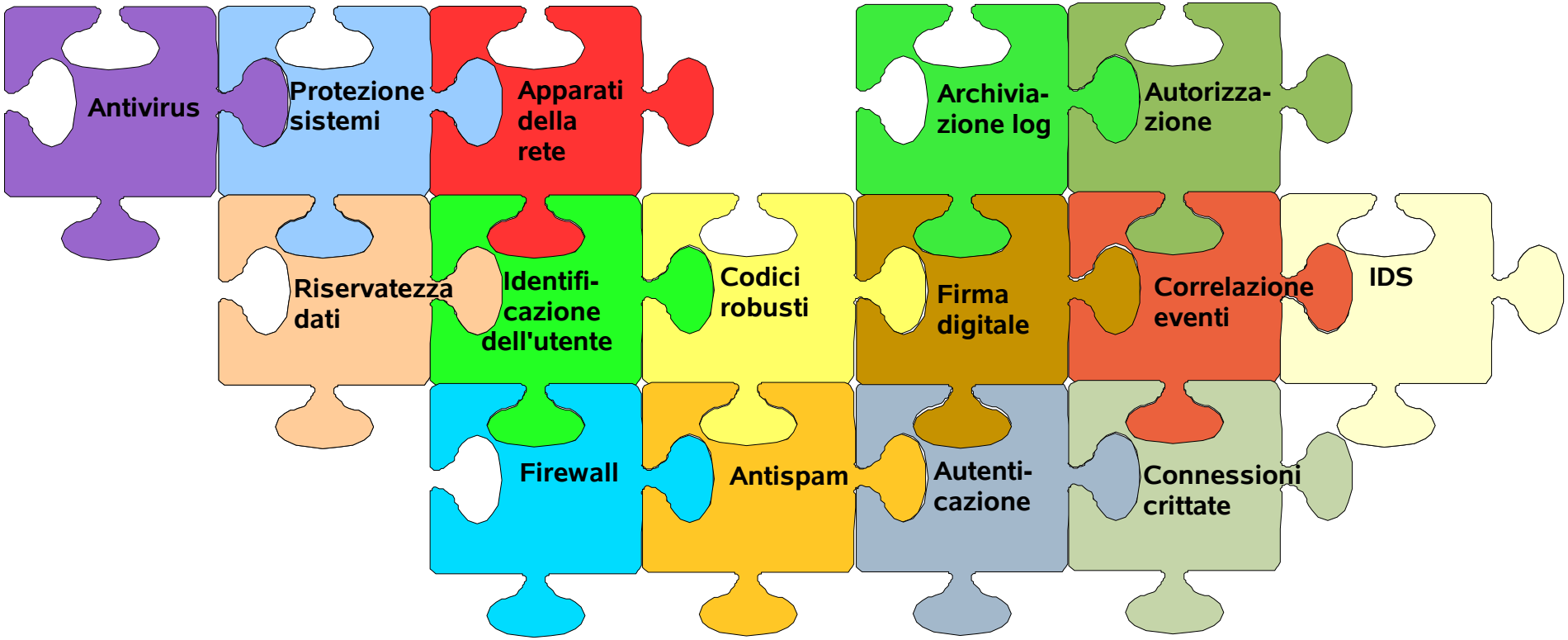
REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

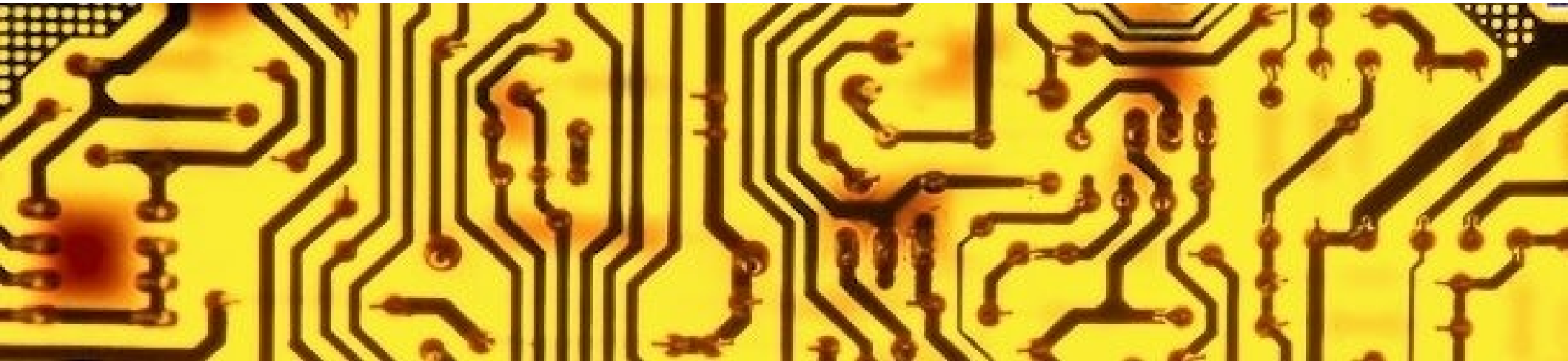
Meccanismi e strumenti di protezione

Meccanismi di sicurezza



Strumenti per la sicurezza

- Utilizziamo tecnologie di sicurezza
  - multiple
  - indipendenti
  - differenti
  - reciprocamente rinforzanti
  - semplici da amministrare

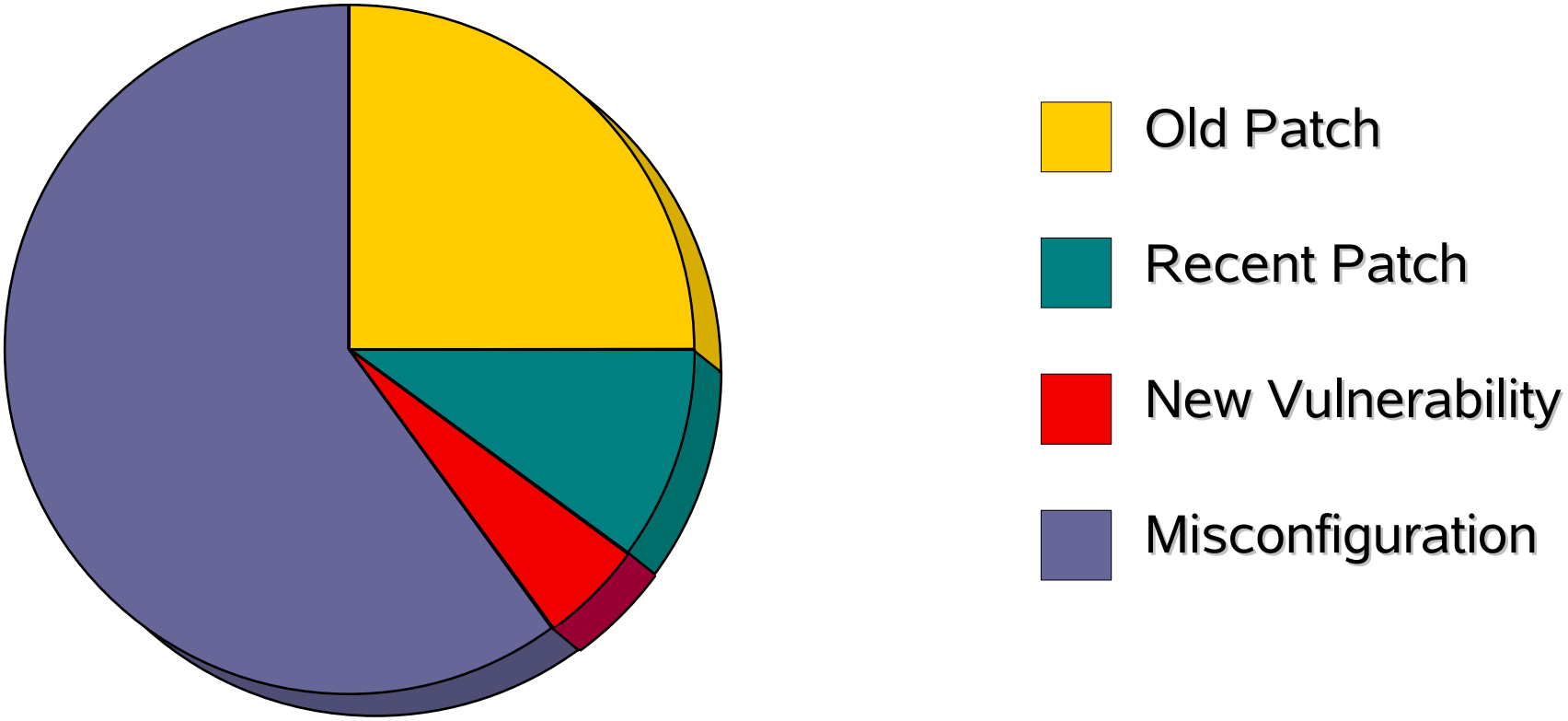


Strumenti per la sicurezza

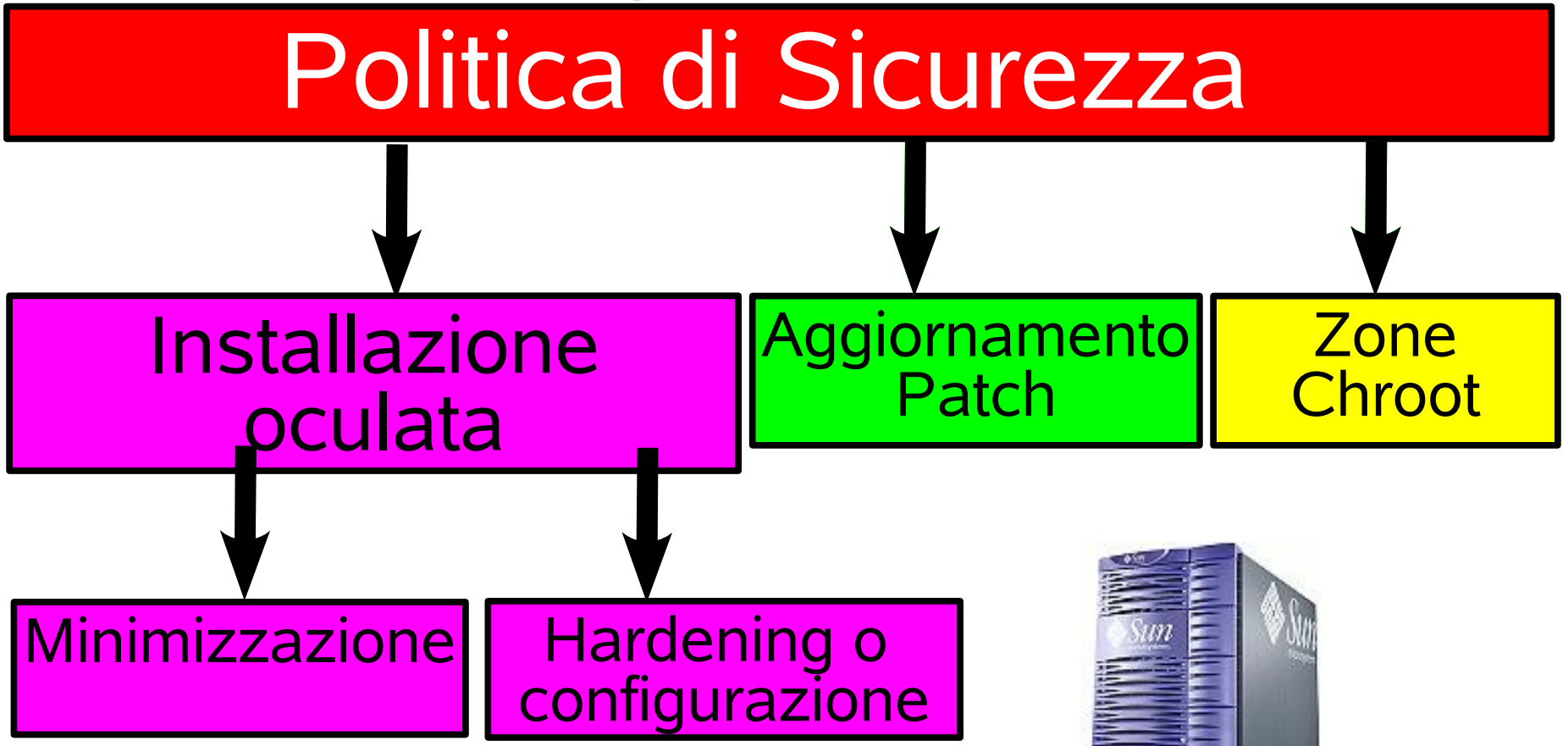
- Predisponiamo tutte le componenti in modo che siano:
  - Gestibili in modo “sicuro”
  - Disponibili quando servono
  - Configurate in modo razionale

- Utilizziamo un approccio di tipo “default-deny”
  - “é accedibile solo ciò che è espressamente autorizzato”

Le minacce ai sistemi



Sicurezza dei sistemi e degli applicativi



Hardening e Minimizzazione

- Analisi dei servizi erogati
  - requisiti tecnici
  - configurazione
  - strumenti di amministrazione e controllo.
- Analisi dei rischi
- Requisiti di sicurezza
  - Requisiti di legge

Hardening e Minimizzazione

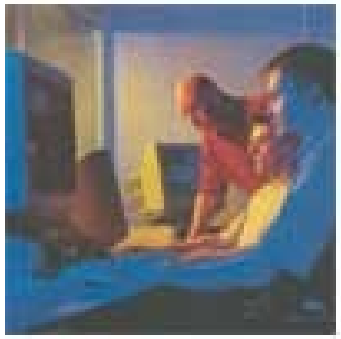
- Sviluppa e costruisce una configurazione del sistema e degli applicativi ad hoc
  - Installazione mirata delle componenti necessarie
  - Sistema chiuso intorno al servizio erogato
  - Configurazione documentata
  - Sistemi per la verifica e l'allineamento della configurazione
- L'hardening di un sistema è funzione del livello di sicurezza richiesto dal servizio erogato

Hardening metodologia

- Installare le patches e gli hot fix
- Disattivare, e possibilmente rimuovere, tutti i servizi TCP/IP non necessari.
- Configurare i servizi di rete necessari
  - Restringere gli accessi
  - Filtrare le connessioni
  - Attivare i meccanismi di sicurezza
- Amministrare sistemi/servizi su connessioni crittate

Hardening metodologia

- Configurare i metodi di autenticazione
- Personalizzare i parametri del sistema o dell'applicativo
- Configurare i file system e i permessi dei file di sistema
- Installare Firewall, IDS e altri meccanismi di protezione




Chroot e Zone

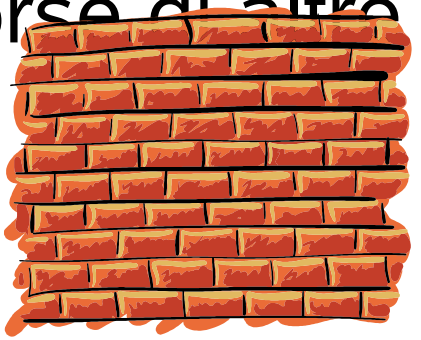
- Servizi eseguiti con utente non privilegiato
- Creare un ambiente chiuso dove eseguire gli applicativi
- Se l'applicativo è compromesso l'intruso non riesce ad uscire dall'area protetta

Zone: sicurezza

- Non accede ad altre Zone
- Accesso di root ristretto
- Non tutte le funzionalità di sistema sono incluse:
  - Accensione e spegnimento dell'intero sistema
  - Accesso ai parametri del Kernel,
  - Gestione della memoria e delle altre periferiche
  - Gestione delle interfacce di rete

Zone: isolamento

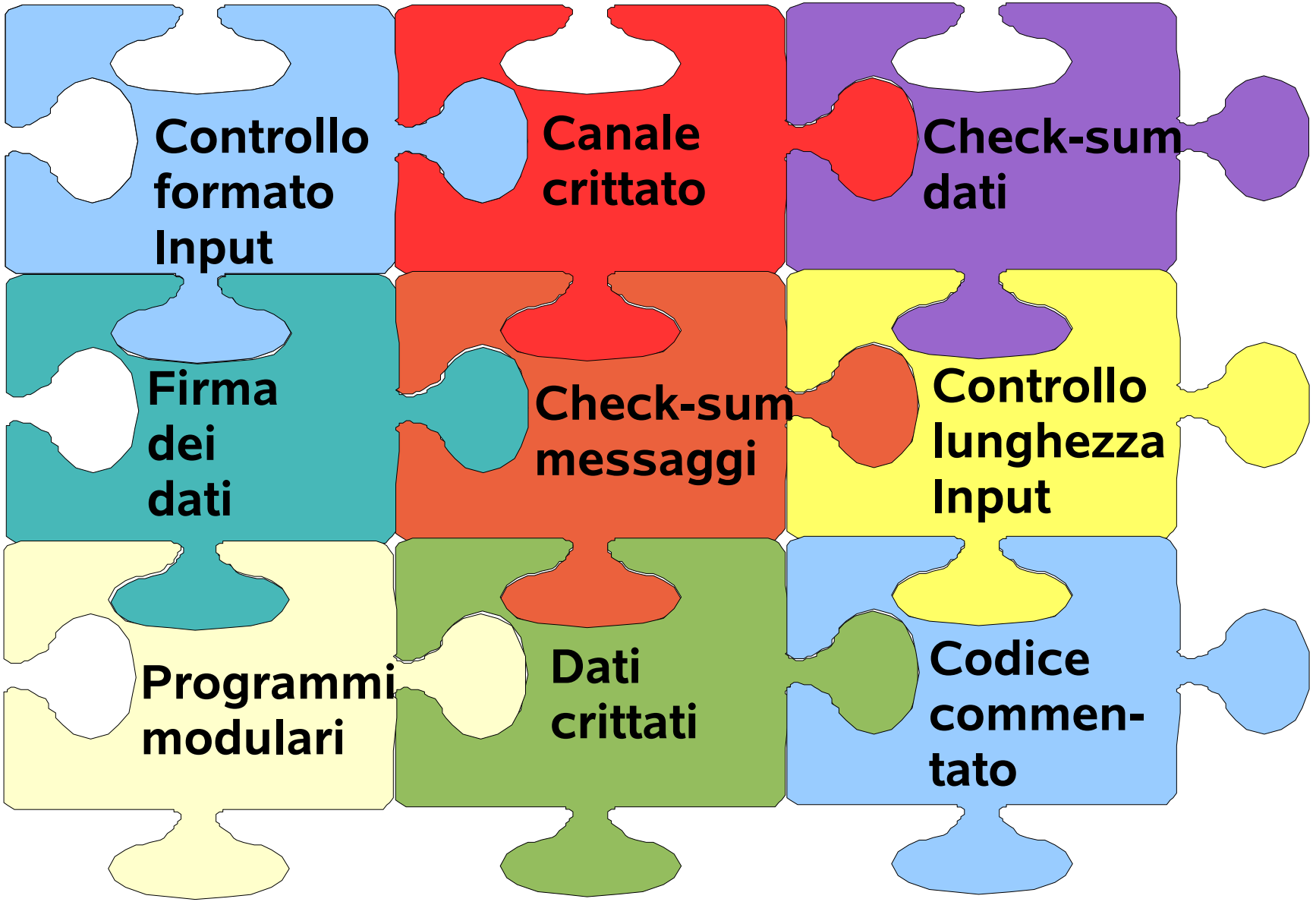
- FS ristretto
- Porte di rete condivise
  - Assegnazione di un indirizzo logico diverso per zona
- Impossibilità di vedere traffico di altre Zone
- Impossibilità di accedere alle risorse di altre Zone



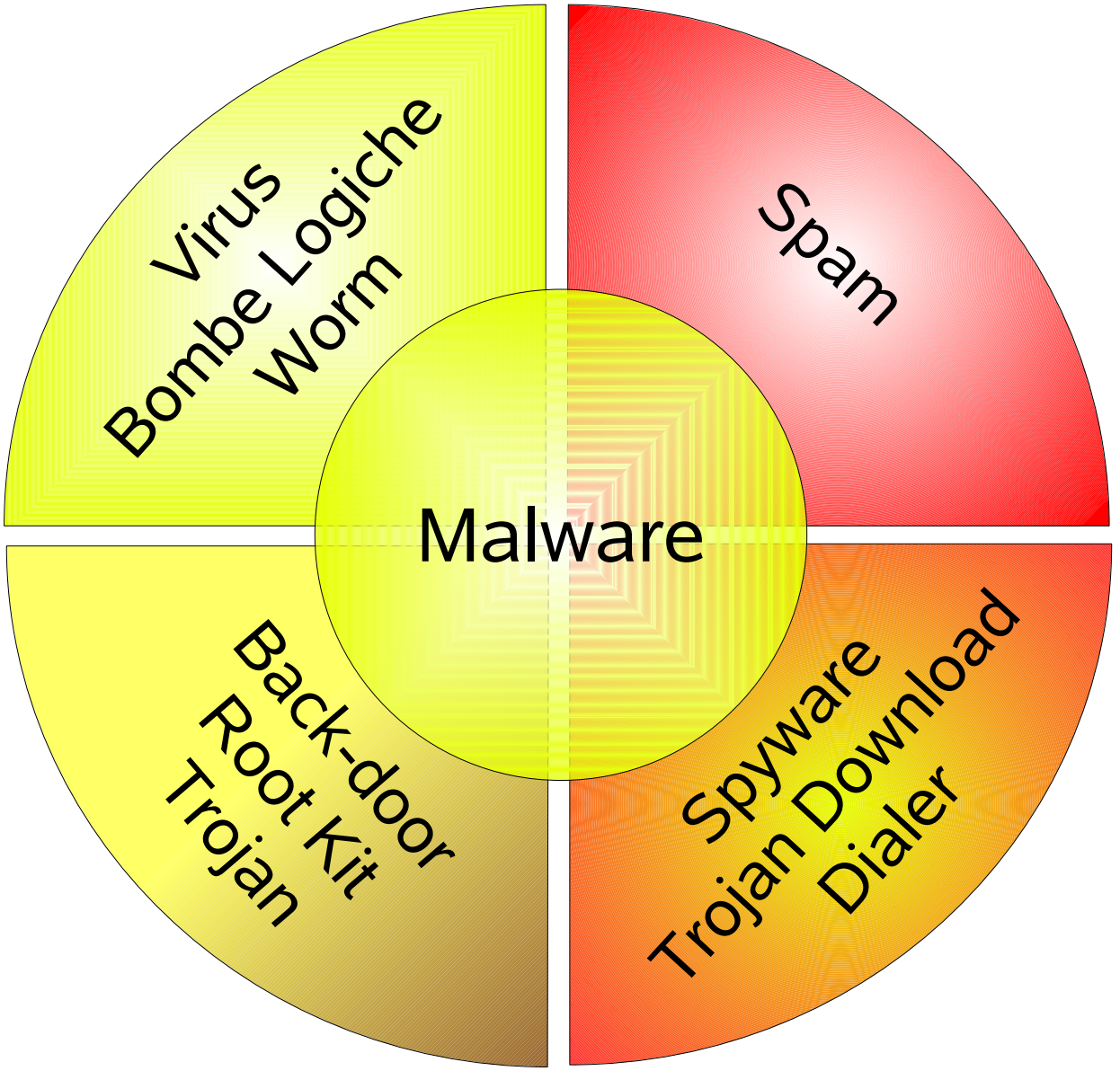
Benefici

- Ottenere la configurazione più appropriata per il sistema e i servizi
- Mitigare e gestire le potenziali criticitò di sicurezza (provenienti dall'esterno o dall'interno)
- Capire le potenzialità di sicurezza del software
- Aumentare la sicurezza con un costo limitato
- Massimizzare la disponibilità dei servizi

Codice robusto



Virus & Co.


Virus
Bombe Logiche
Worm
Spam
Malware
Back-door
Root Kit
Trojan
Spyware
Trojan Download
Dialer

Antivirus

- Antivirus
  - Scansione dei file di un sistema, dei messaggi di posta in arrivo, delle periferiche di sistema e di quant'altro alla ricerca di virus
  - Pulizia dei file e quarantena
- Firma dei virus
  - Intervallo tra diffusione virus e rilascio firma
- Filtri antispam
- Filtri sui Browser
- Formazione

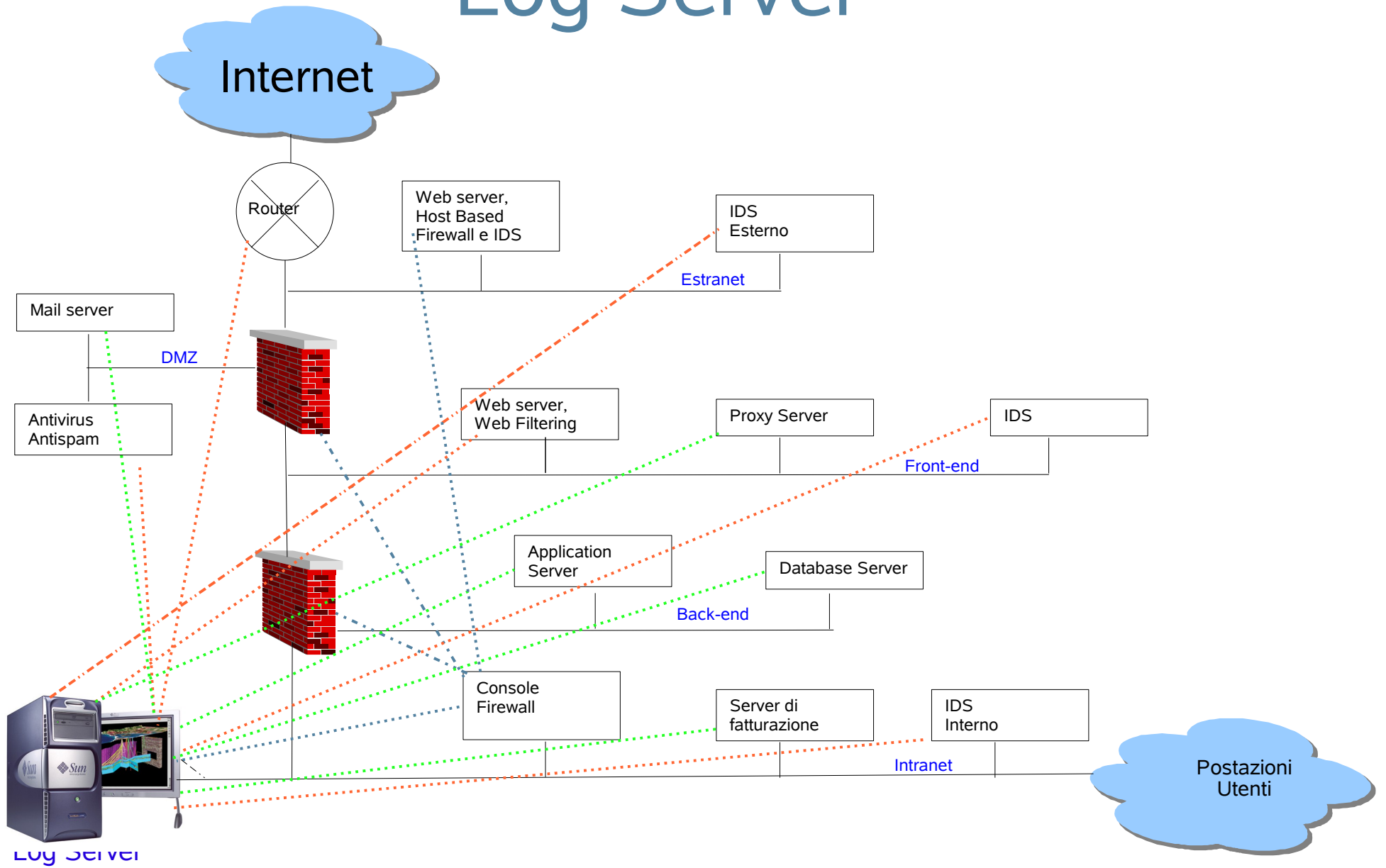
Sicurezza dei media rimovibili

- Il valore di un media è pari al valore del supporto fisico più il valore delle informazioni conservate.
- Conservazione
- Trasporto
- Dismissione
  - Sostituzione

Registrare le operazioni

- Scelta delle informazioni da registrare
  - L'importanza delle informazioni trattate
  - I rischi associati ai sistemi
  - Requisiti di legge
  - Capacità di archiviare informazioni
  - Capacità di analizzare i log prodotti

Log Server


Internet
Router
Web server,
Host Based
Firewall e IDS
IDS
Esterno
Estranet
Mail server
DMZ
Antivirus
Antispam
Web server,
Web Filtering
Proxy Server
IDS
Front-end
Application
Server
Database Server
Back-end
Console
Firewall
Server di
fatturazione
IDS
Interno
Intranet
Postazioni
Utenti

Registrare le operazioni

- Archiviazione centralizzata
- Analisi degli eventi
- Correlazione degli eventi
- Conservazione dei log
  - Obbligo di legge
  - Archiviazione crittata

Disegnare una rete sicura

- Un server = un servizio
- Disegnare una rete semplice
  - Segmentare in sottoreti
  - Proteggere le comunicazioni tra le varie sottoreti
  - Ambienti di sviluppo, collaudo e produzione
- Formalizzare tutto il flusso dati
- Analizzare il traffico
- Proteggere il traffico tramite connessioni crittate

Firewall: la prima barriera di protezione

- Controllano il traffico e scartano quello proibito
- Differenti livelli effettuati con differenti tecnologie
- Non solo protezione perimetrale ma anche

Packet filtering

- Filtra i pacchetti IP sulla base di:
  - indirizzi sorgente e destinatario
  - sul tipo di pacchetto (ad es. TCP o UDP)
  - sulle porte sorgente/destinataria

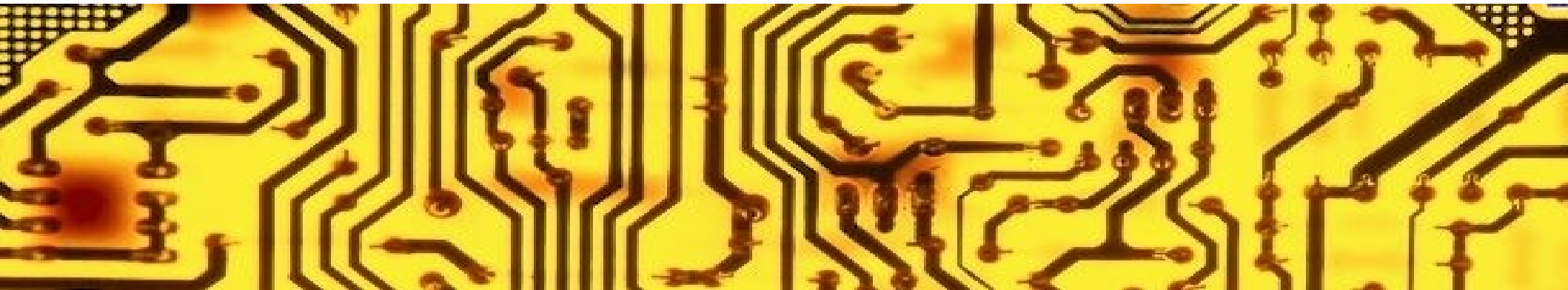
- Nella forma più semplice si può realizzare con le ACL di un router

Network Based Firewall

- Packet filtering Firewall
- Stateful Inspection Firewall
- Dedicated Proxy Server
- Application Proxy Gateway Firewall

Host Based Firewall

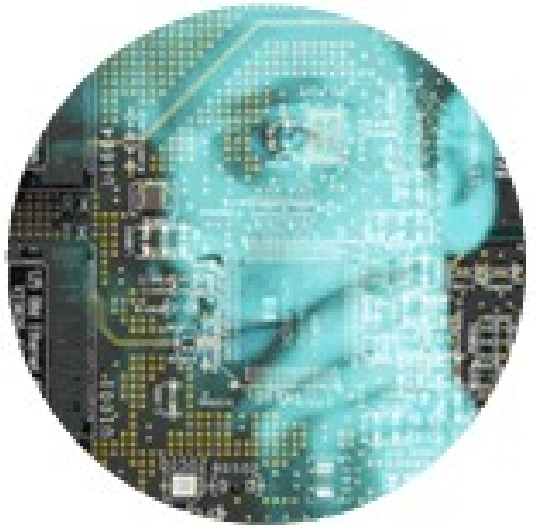
- Può integrare i controlli di rete con controlli sulla configurazione di sistema.
- Quando usare
  - Servizio critico
  - Server direttamente esposto su in Internet per aumentare la banda
  - Postazione portatile o remota



Servizi aggiuntivi dei Firewall

- Servizi aggiuntivi e integrati
  - NAT (Network Address Translation)
  - PAT (Port Address Translation)
  - VPN (Virtual Private Network) concentrator
  - DHCP (Dynamic Host Configuration Protocol)
  - IDS (Intrusion Detection System)
  - Antivirus, antispam o filtri a livello applicativo.
- Quando concentrare?

Come si rilevano gli intrusi?



- Analisi del traffico di rete
  - Firma dell'attacco
  - Anomaly detection
- Intrusion Detection System
  - Scoraggiare impiegati e consulenti maliziosi.
  - Individuare gli attacchi a servizi leciti.
  - Individuare le analisi preliminari.
  - Fornire informazioni utili sull'intruso e sulle azioni da esso compiute.

Intrusion Detection System

- Collezionare gli eventi in atto su una sorgente (calcolatore o rete)
- Analizzare i dati ricercando attacchi o anomalie
- Rispondere all'attacco con un allarme e con le opportune contromisure.

REGIONE DEL VENETO

Direzione Sistema Informatico

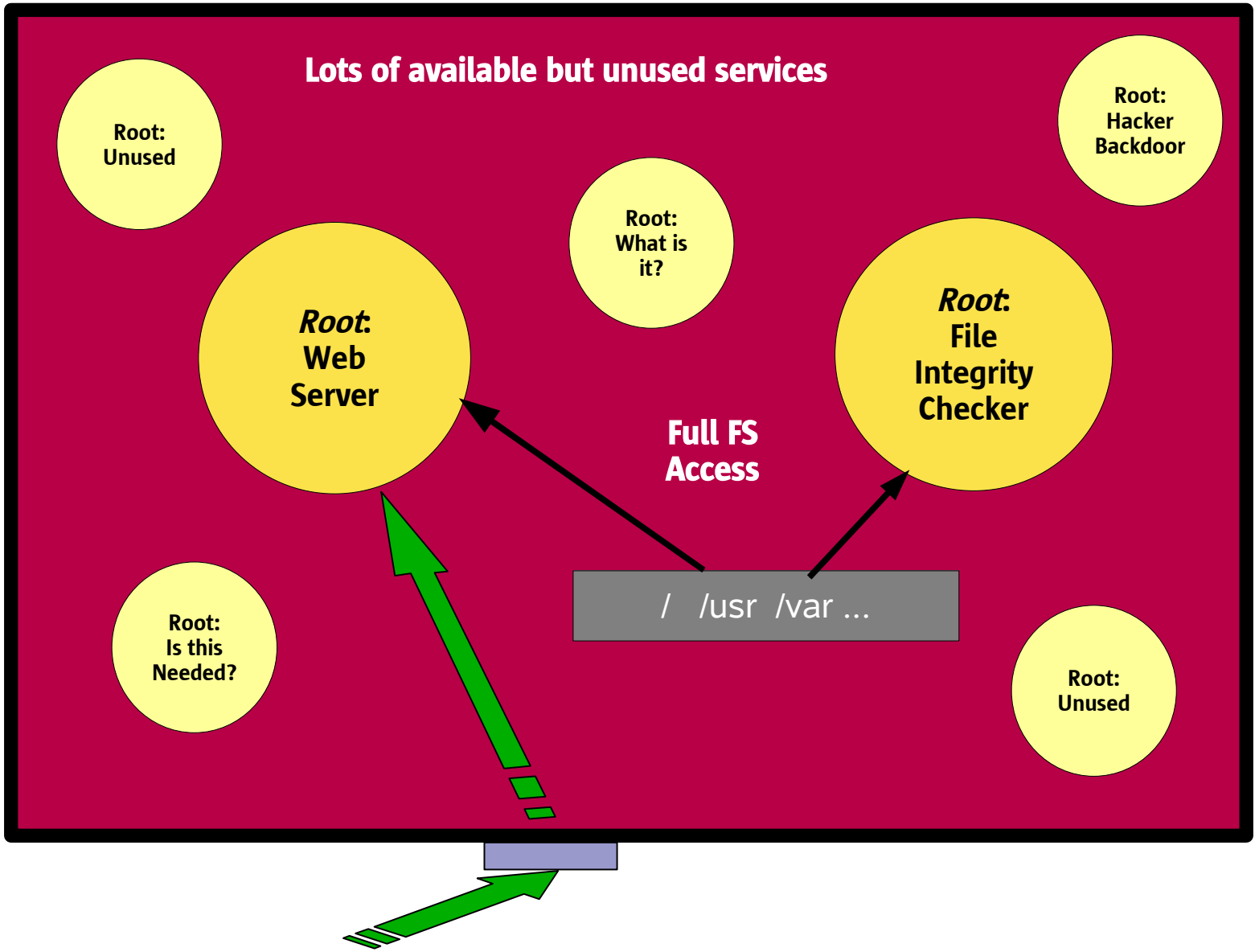
Sun microsystems

Defence in Depth

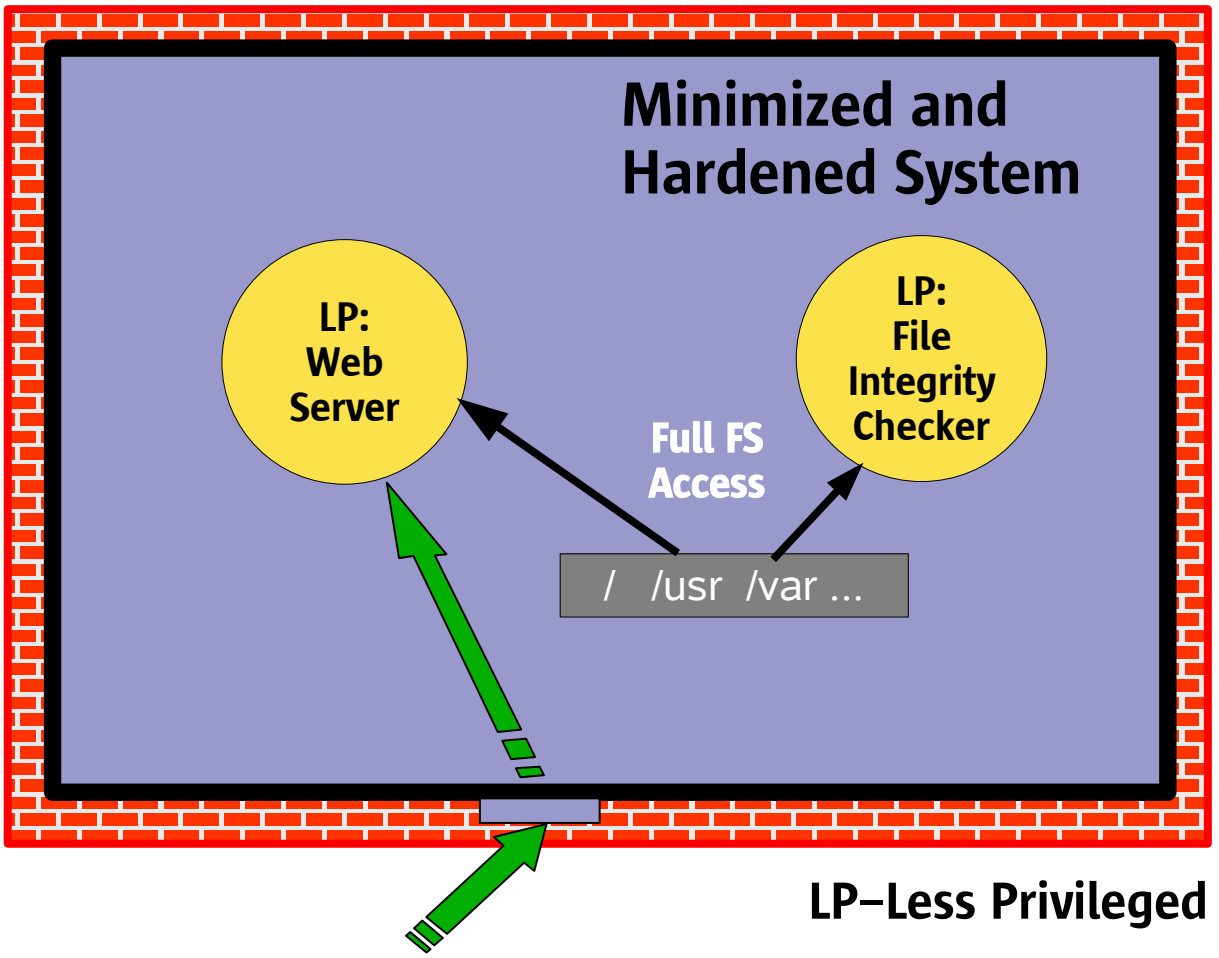
Defence in Depth

Defense in depth is the result of an aggregate set of solutions that work in a synergisitic, complimetary and mutually reinforcing manner

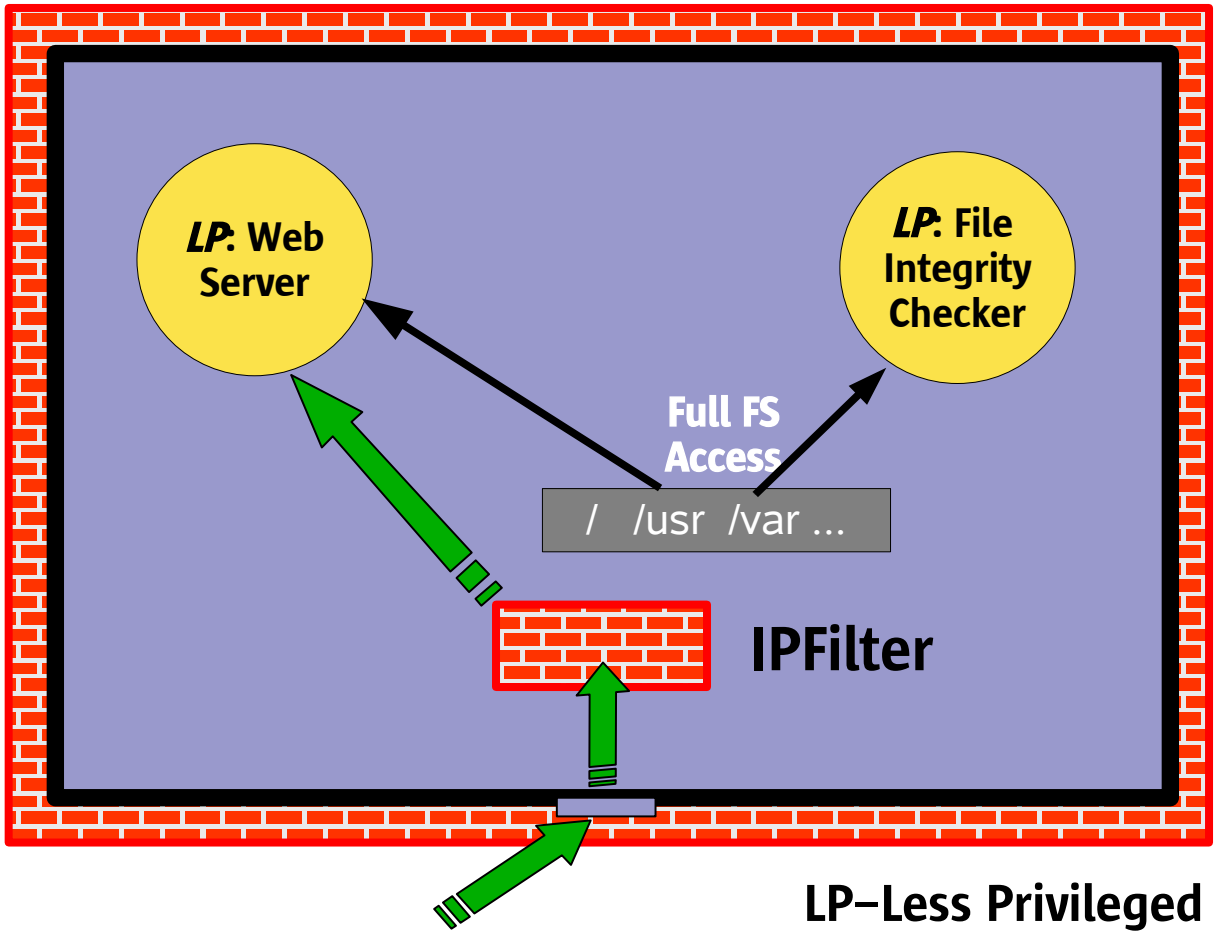
Protezione di un sistema, es.1



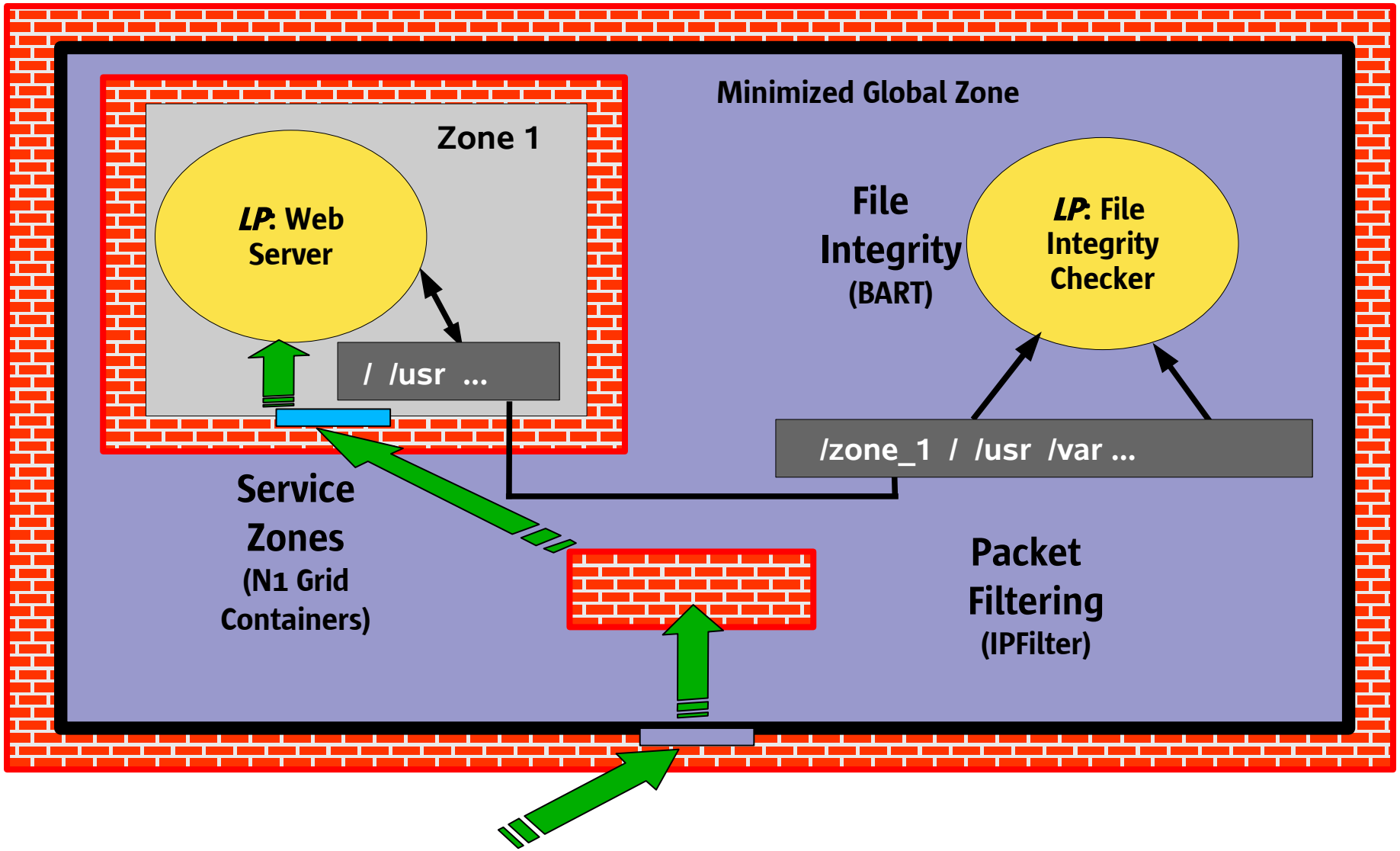
Protezione di un sistema, es.1



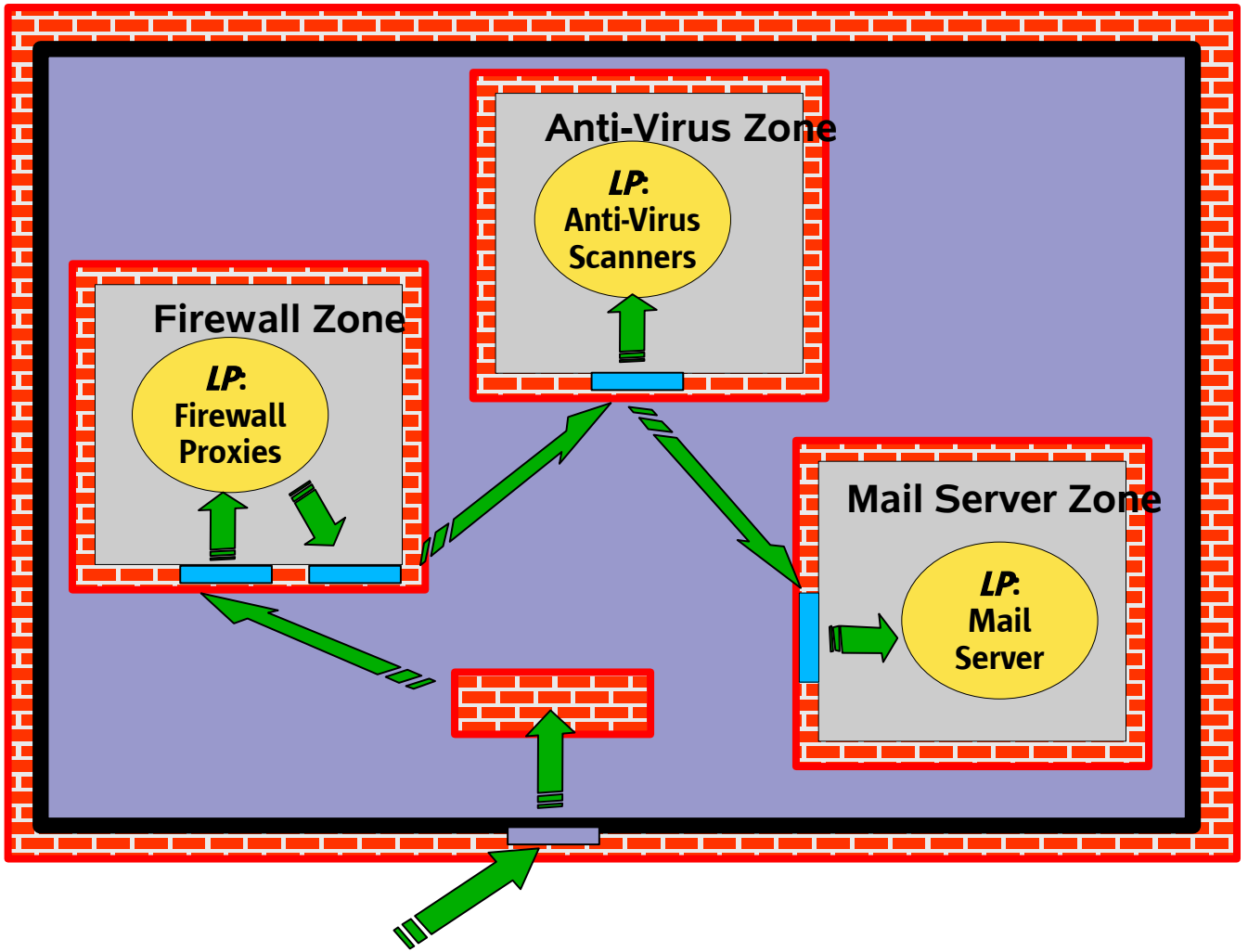
Protezione di un sistema, es.1



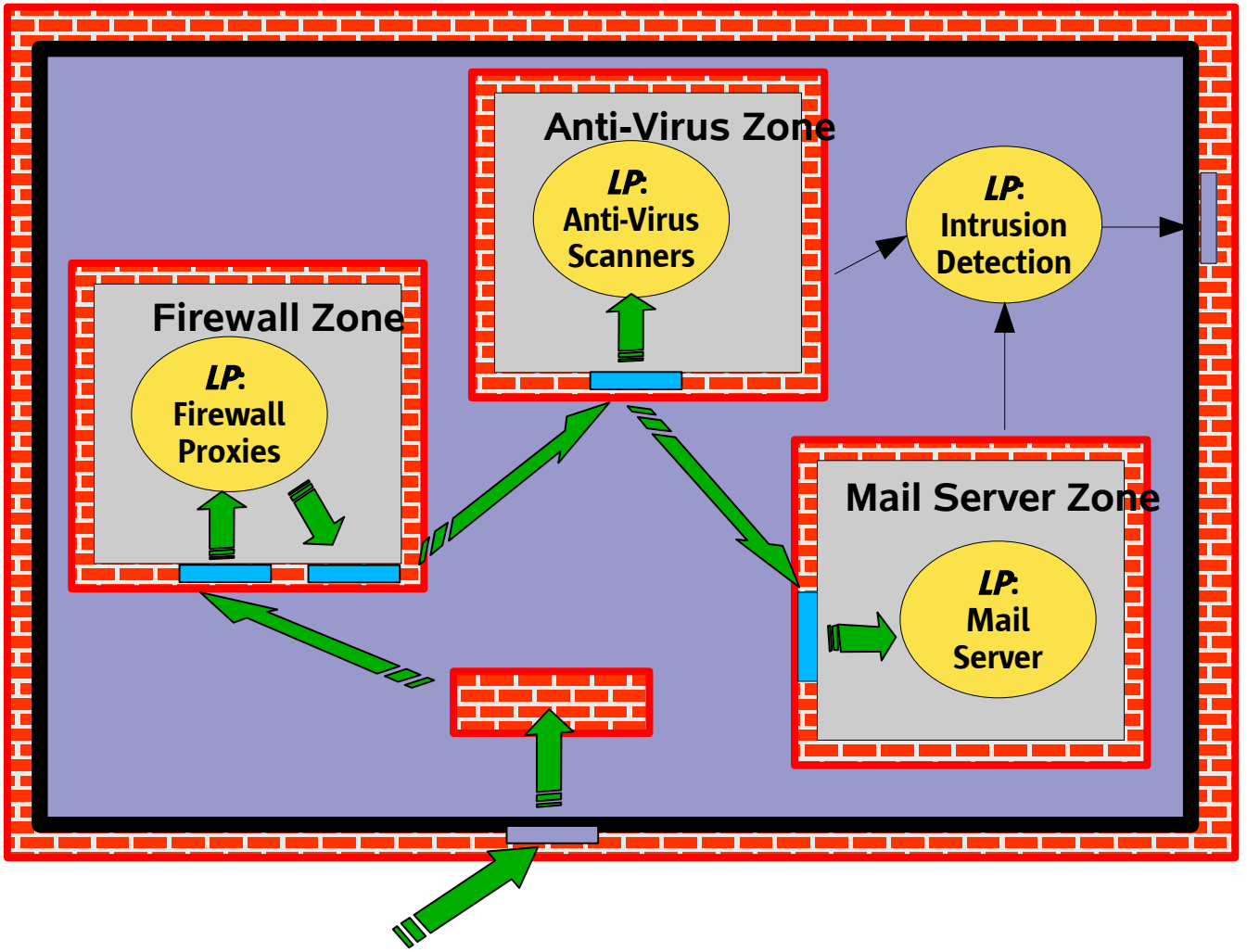
Protezione di un sistema, es.1



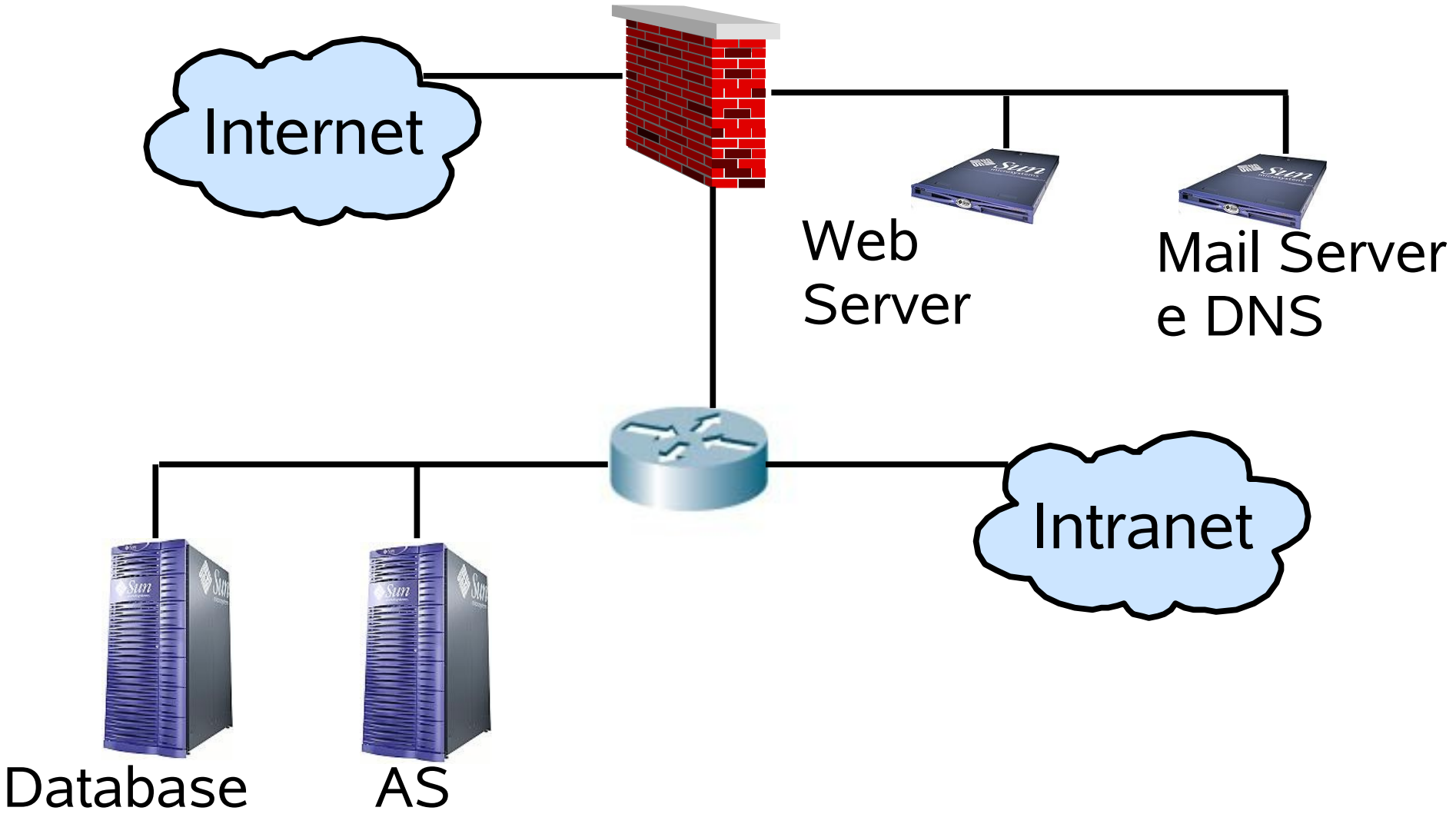
Protezione di un sistema, es.2



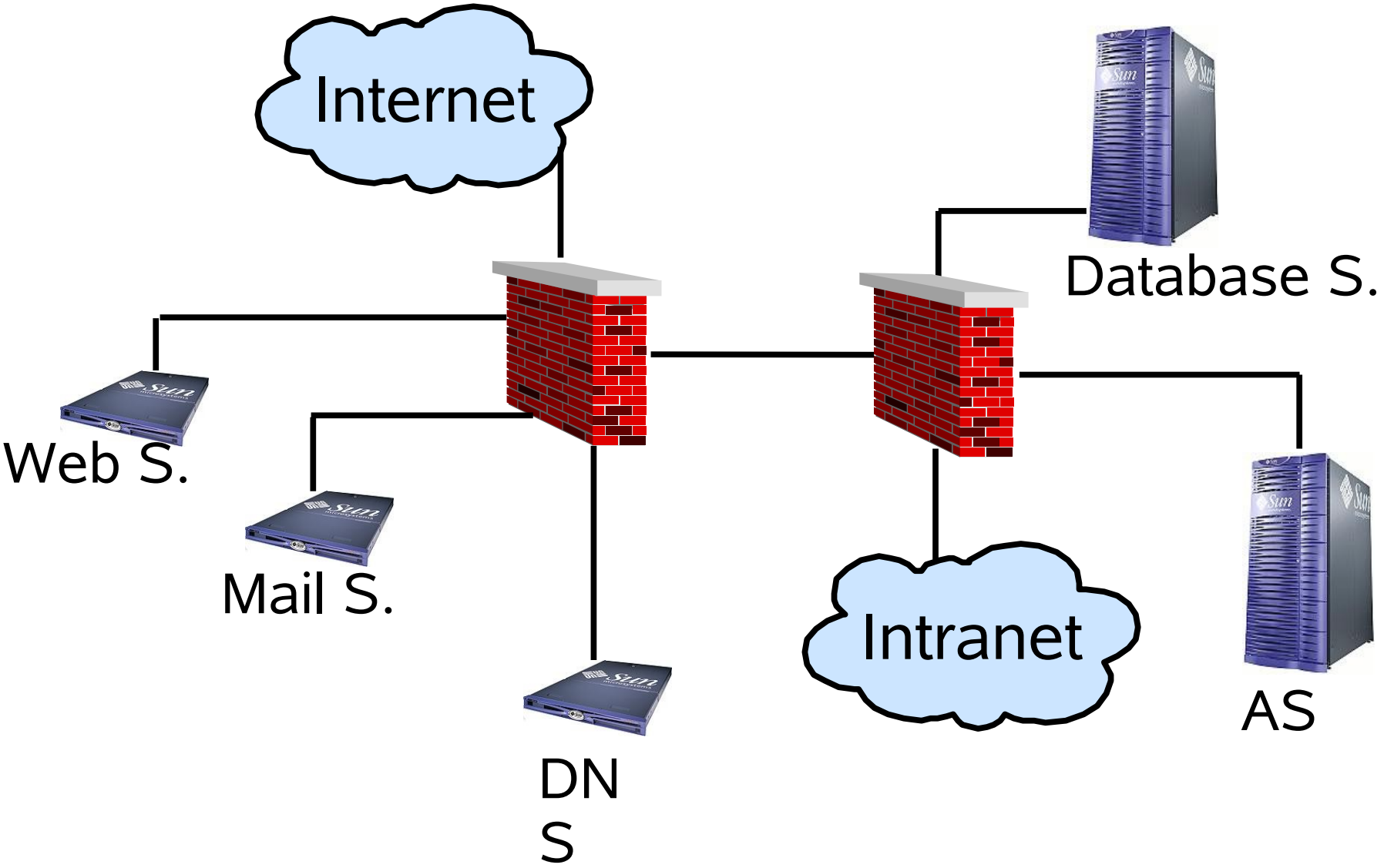
Protezione di un sistema, es.2



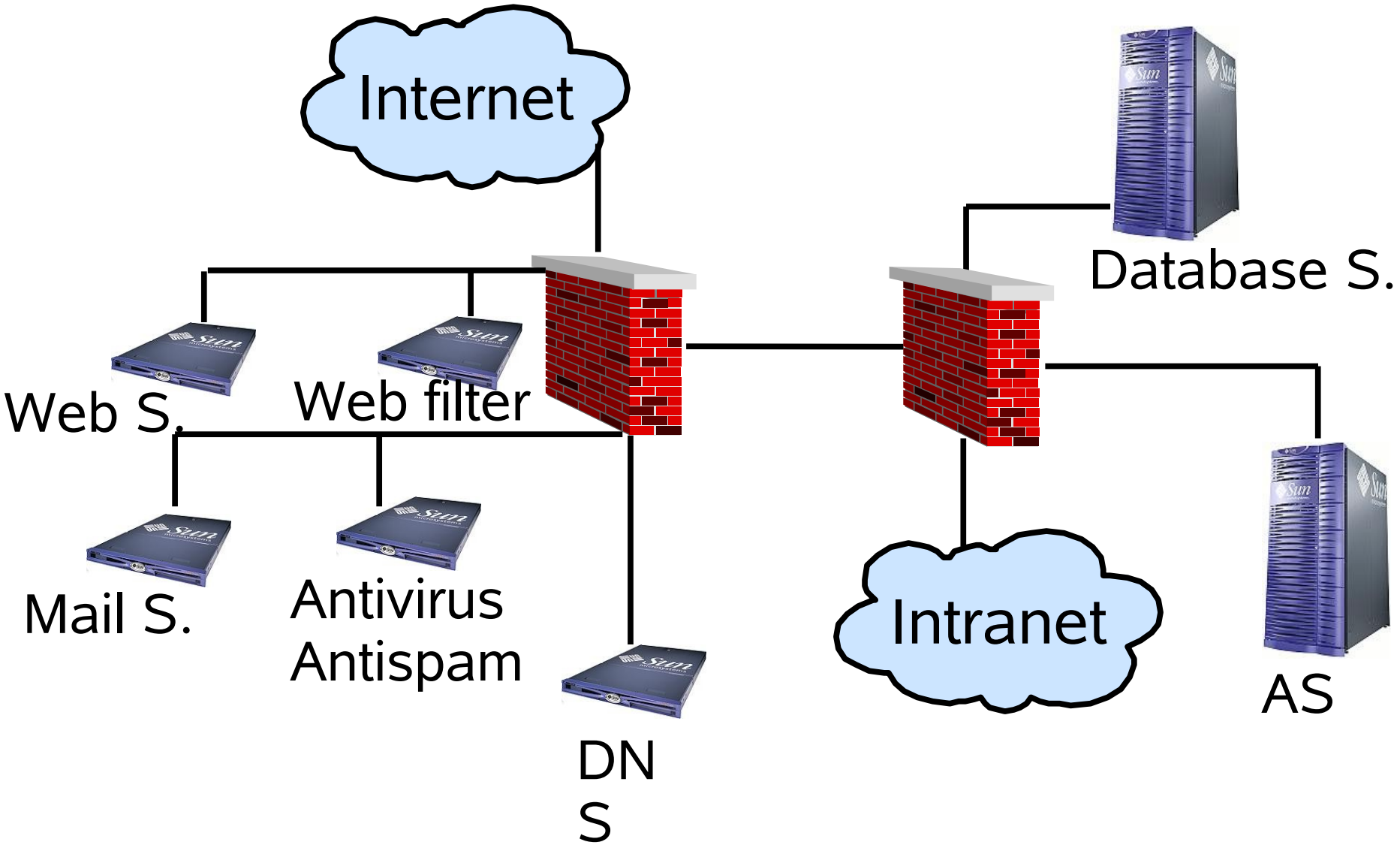
Protezione di una rete



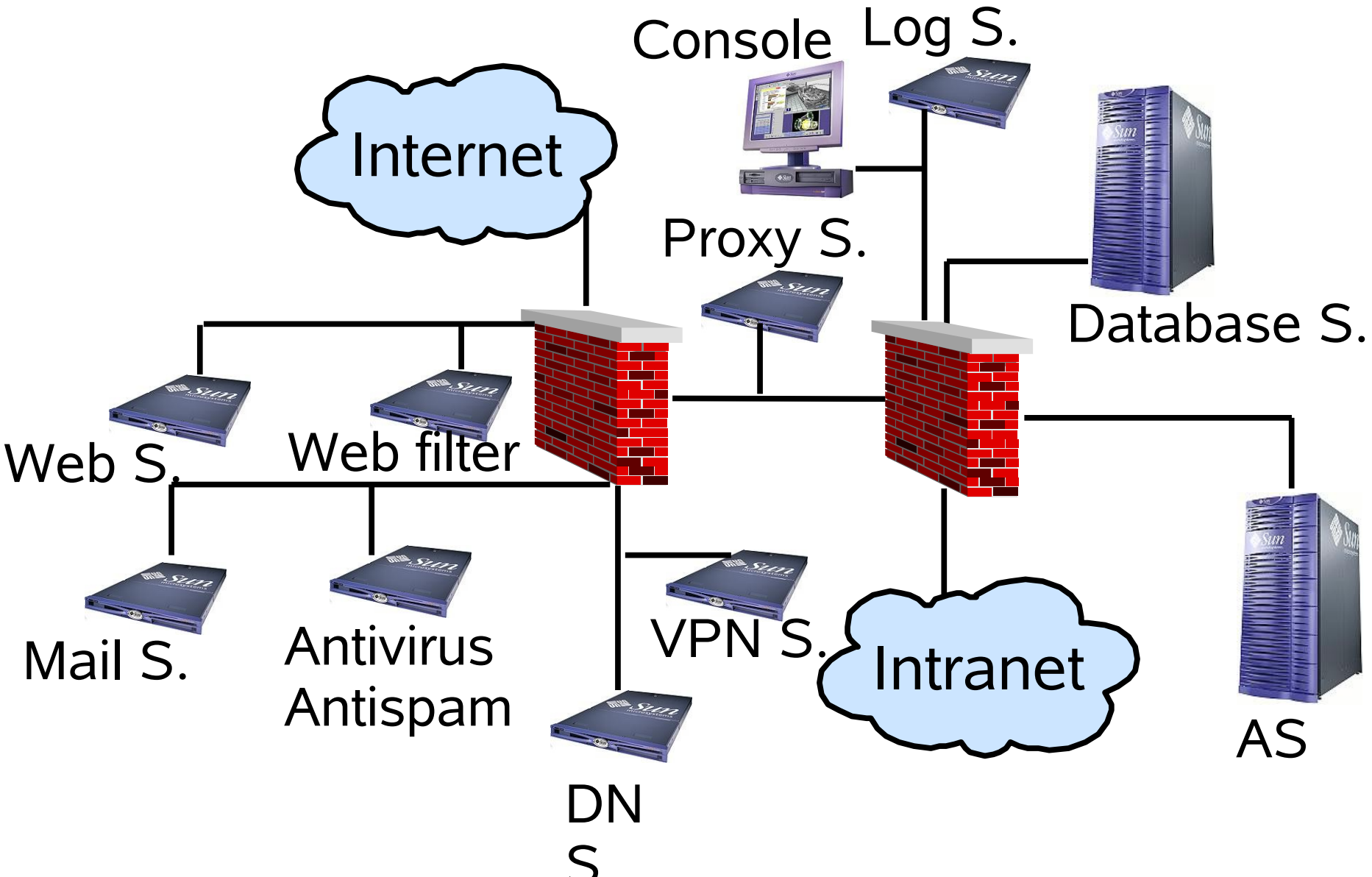
Protezione di una rete



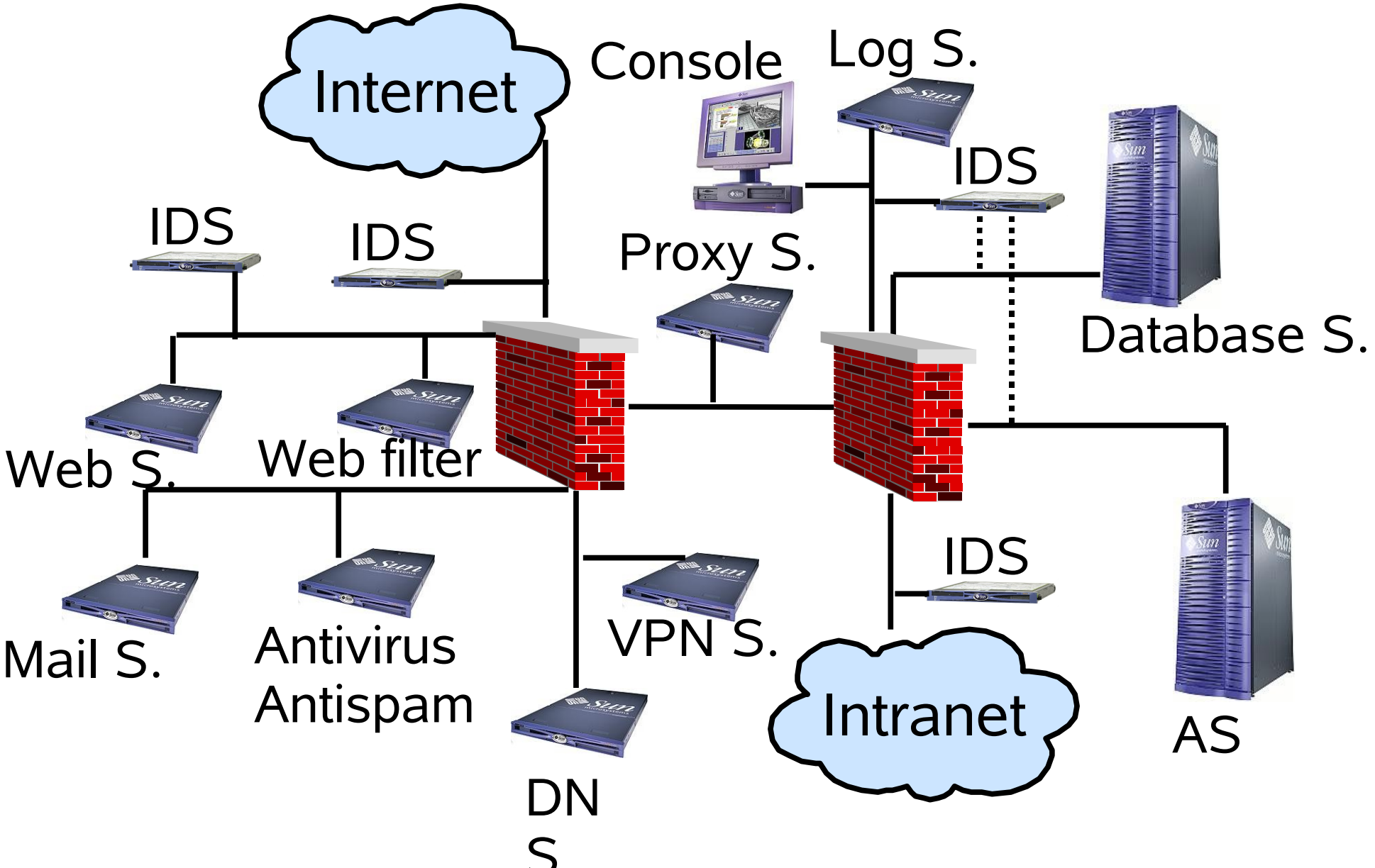
Protezione di una rete



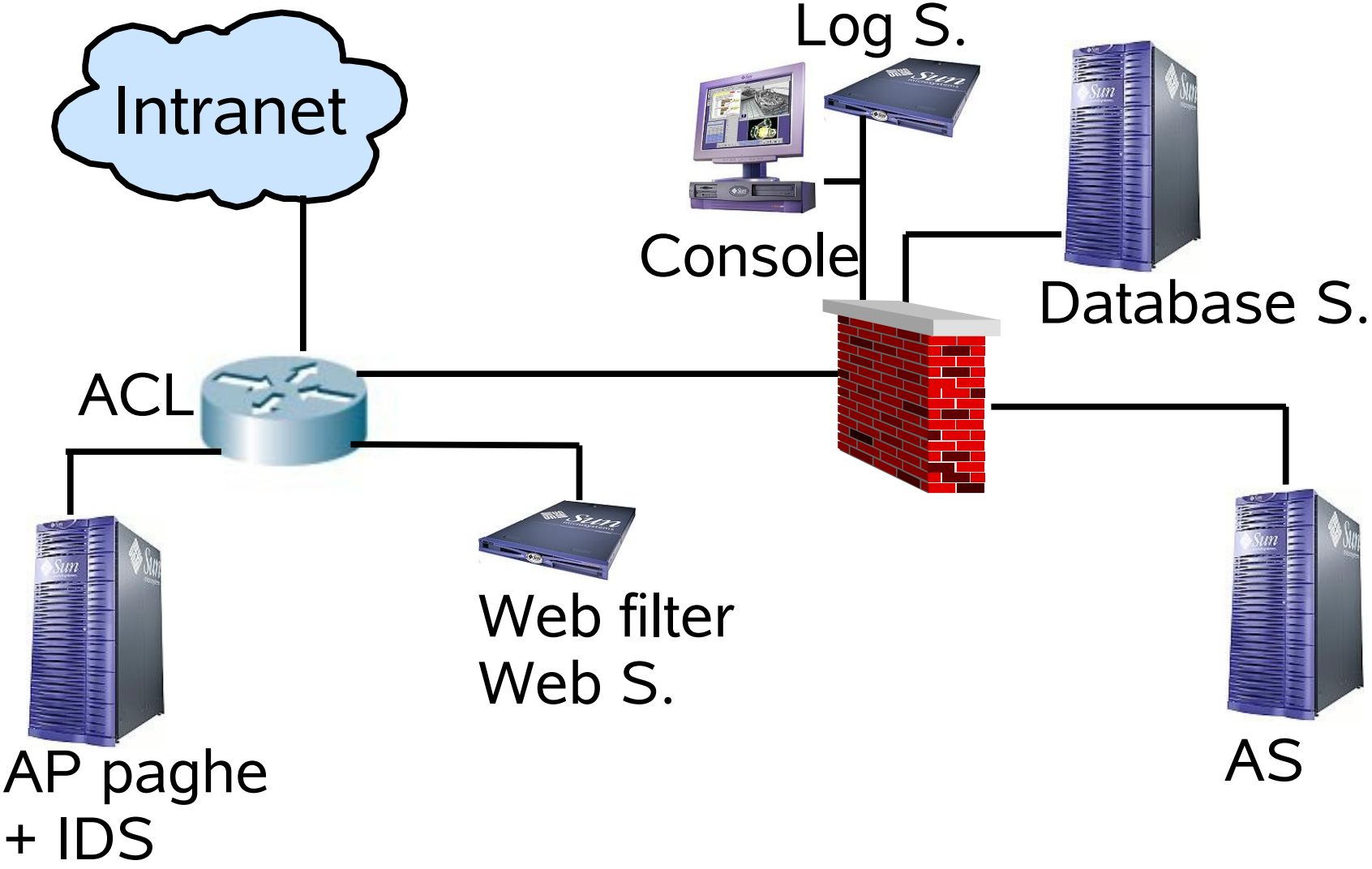
Protezione di una rete



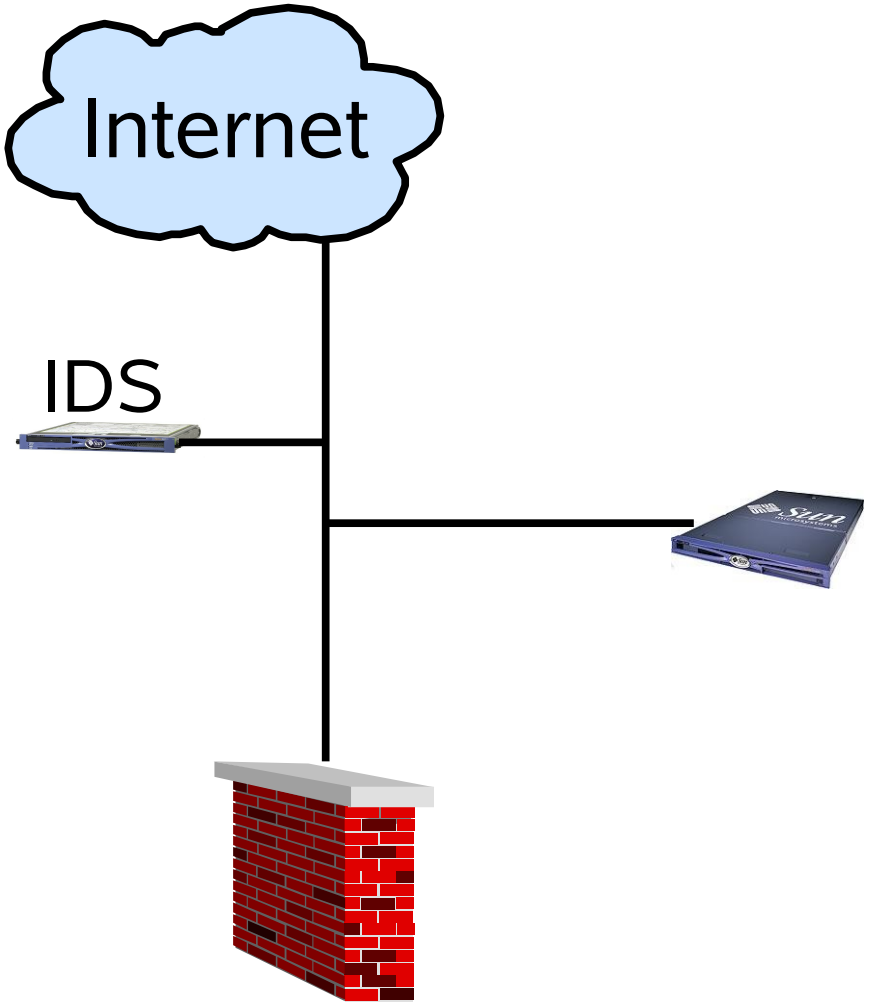
Protezione di una rete



Protezione di una rete



Protezione di una rete



Web Server
SO e SW con Patch
e hardenizzato.
Zone
Host Based Firewall
Host Based IDS
Web Filter

Benefici di questo approccio

- Esposizione minima alle minacce che arrivano dall'esterno/interno
- Elevata scalabilità orizzontale della soluzione
- Resistenza ad attacchi di tipo DDoS
- La presenza di sistemi load balancing ottimizza il consumo di banda dei singoli host
- Regole di filtering sui firewall più semplici
  - Gestione semplificata

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Reagire ad un attacco

Sono stato attaccato, panico... cosa faccio?

- Denunciare il reato alle forze dell'ordine
- Ricercare le eventuali manomissione dei dati
- Ricercare la vulnerabilità sfruttata e la conseguente chiusura della stessa
- Ricercare l'autore dell'attacco
- Rimettere in linea il servizio originale

Imparare dagli errori

- Per poter imparare dai propri errori occorre:
  1) individuare la causa dell'evento e le componenti coinvolte
  2) cercare i meccanismi capaci di prevenire tali incidenti e il motivo per cui non sono stati applicati
  3) verificare se gli strumenti di controllo hanno segnalato tempestivamente il problema
  4) adottare le contromisure individuate ed aggiornare le procedure

Nella Sicurezza la cooperazione responsabile fra tutte le componenti coinvolte consente di superare lo scoglio più alto.....

LA PARANOIA

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Gabriella Cattaneo

Security Technical Engineer

Sun Microsystems, Inc.