Università Politecnica delle Marche

Architetture e strumenti per la sicurezza informatica

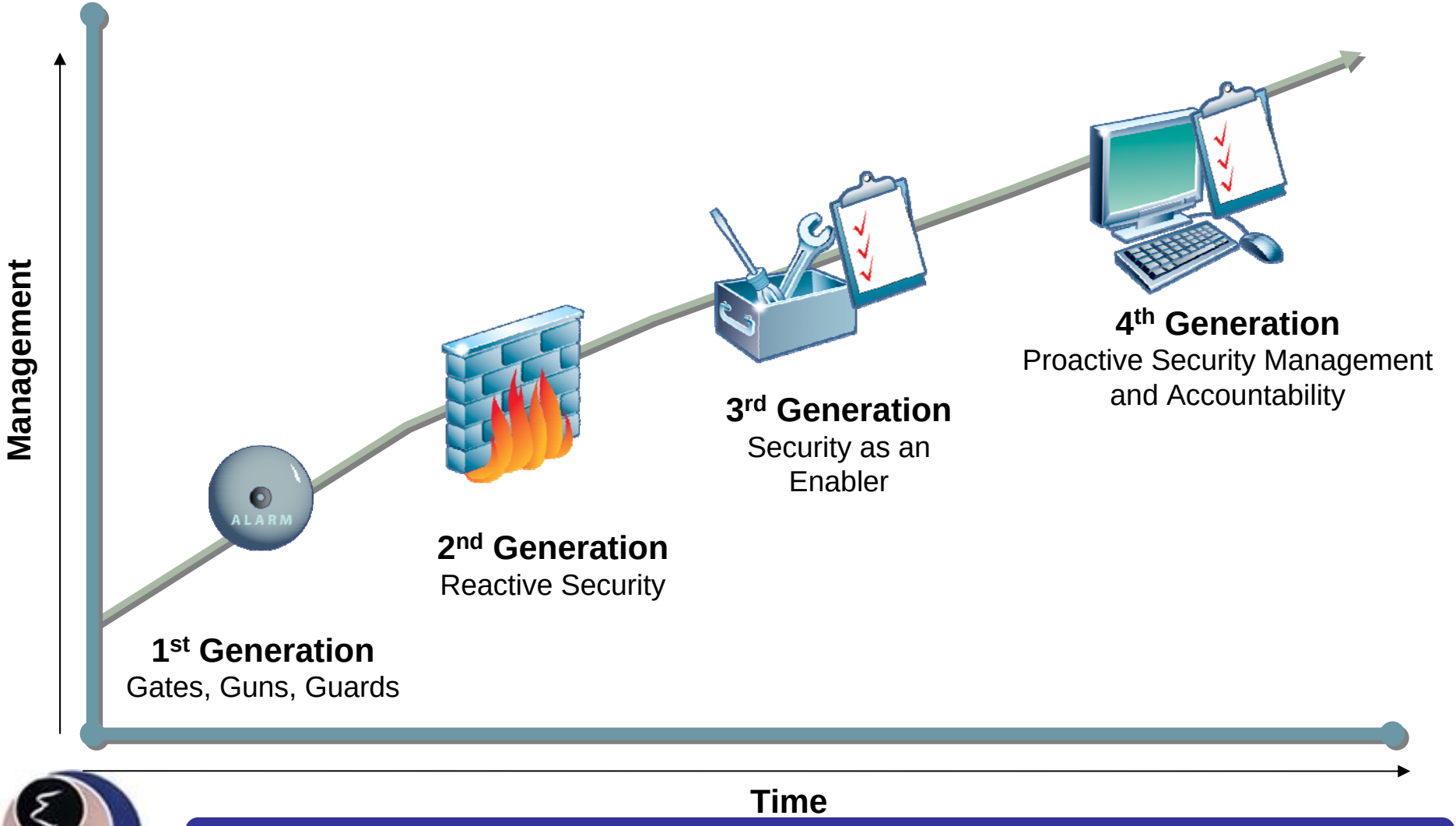
Ing. Gianluca Capuzzi

Dipartimento di Ingegneria Informatica, Gestionale e dell'Automazione

Agenda

- Premessa
- Firewall
- IDS/IPS
- Auditing
- Strumenti per l'analisi e la correlazione
- Strumenti e politiche di backup
- Cenni sulla risposta agli incidenti informatici

Evoluzione della sicurezza informatica



Suggerimenti

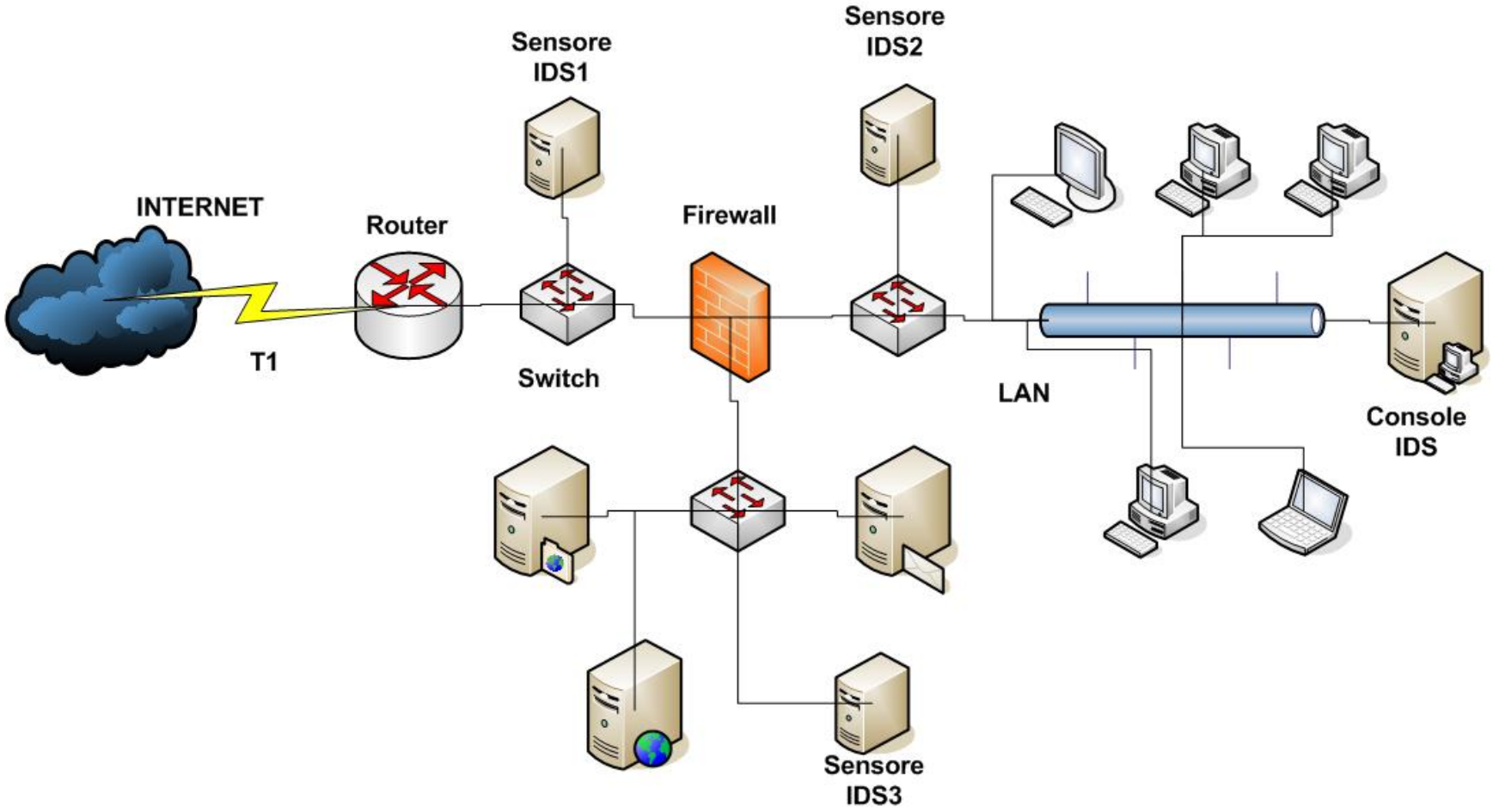
- Oggi si commette l'errore di affidarsi ad un unico strumento con tutte le funzionalità: ***appliance***
  - Se cade questo nodo, viene compromessa la sicurezza di tutta la rete
  - È preferibile un'architettura distribuita: i diversi strumenti ubicati in punti differenti della rete

Motivi

- L'IDS non può essere installato con Firewall perché deve essere "nascosto"

- Sarebbe meglio installare vari sensori IDS in diversi punti della rete per raccogliere un'informazione completa

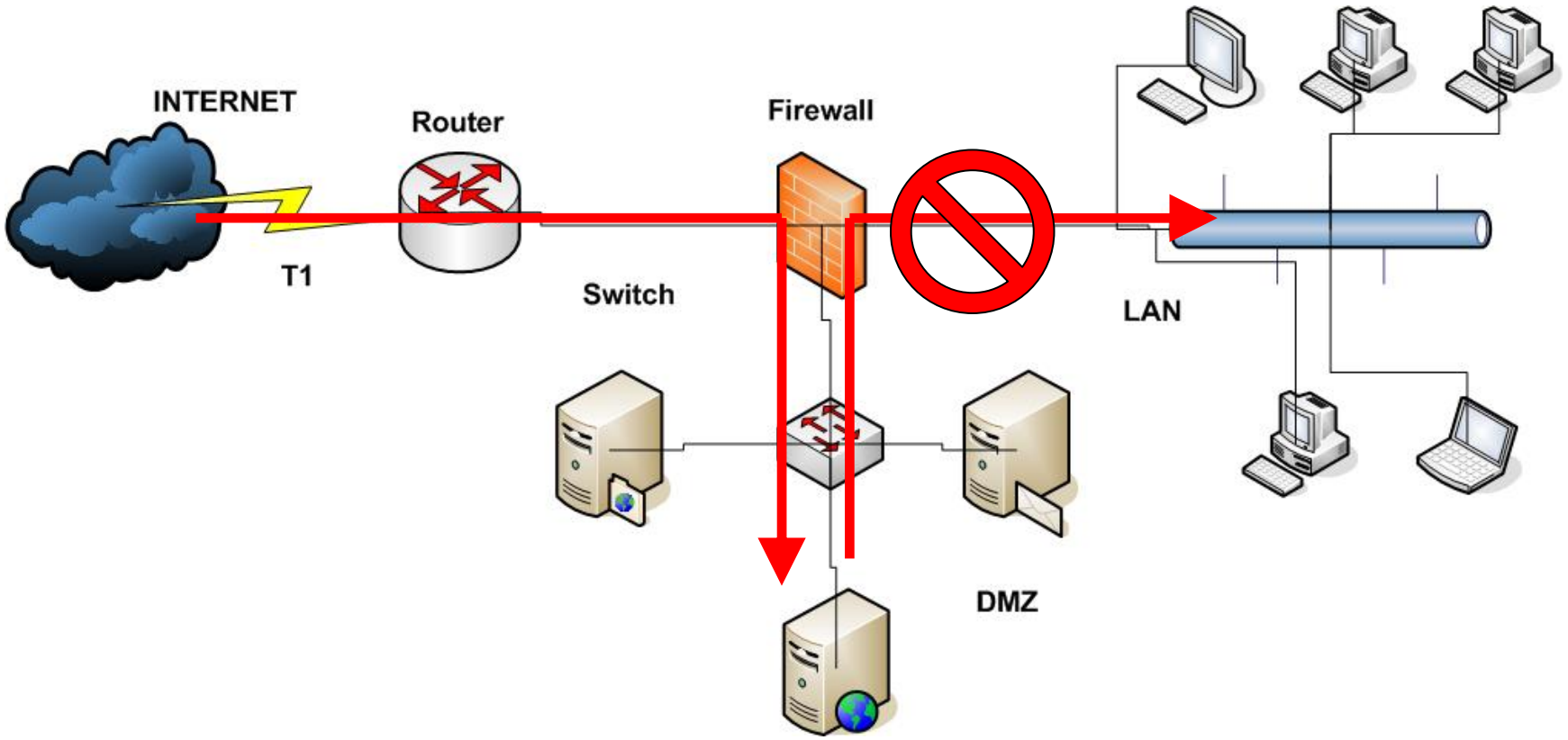
Esempio


Sensore
IDS1
Sensore
IDS2
INTERNET
Router
Firewall
T1
Switch
LAN
Console
IDS
Sensore
IDS3

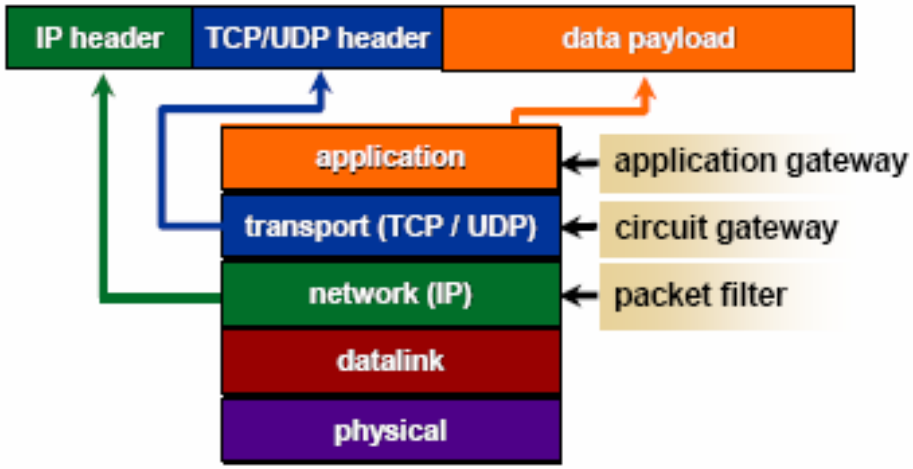
Firewall

- Filtri del traffico di rete
- Nati per risolvere il problema di connettere la LAN ad una rete non affidabile (internet)
- Per dare la possibilità ad utenti esterni di accedere a servizi interni si utilizzano le DMZ (reti “smilitarizzate”), dove vengono installati i server

Esempio

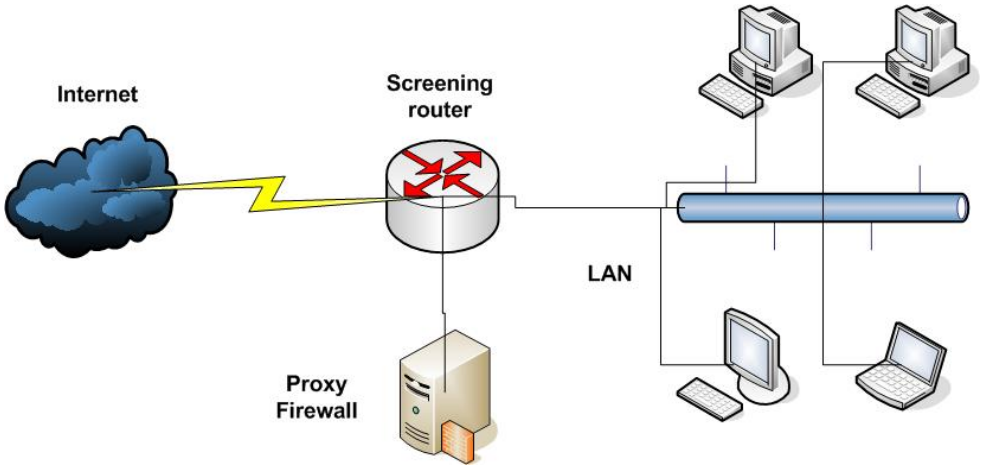


Classificazione



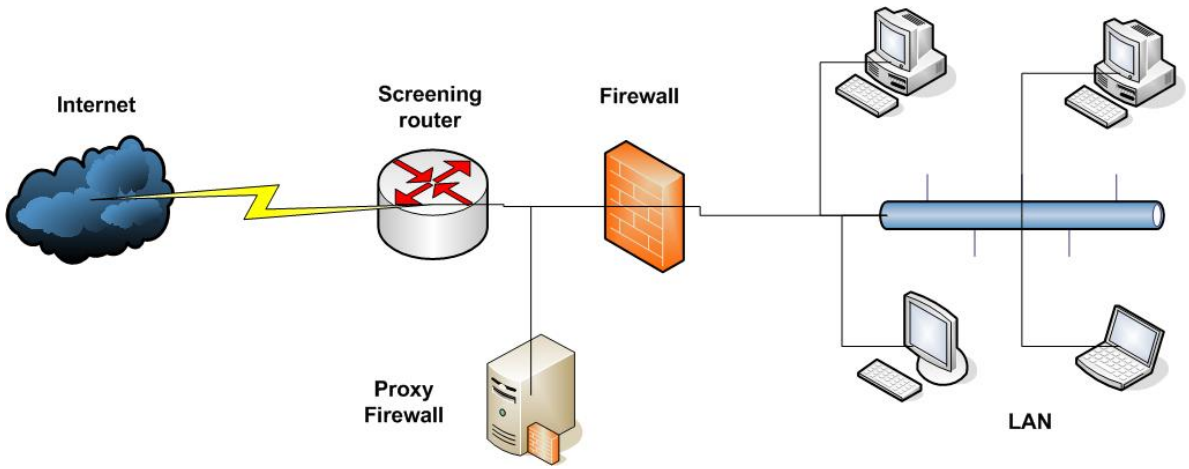
- Packet filter: agisce sul singolo pacchetto
- Circuit gateway e stateful firewall: riconoscono le sessioni aperte
- Application gateway: ha la possibilità di filtrare in base al contenuto

Architetture: dual-homed gateway



- È costituita da un router filtrante ed un proxy per il filtro degli accessi ai servizi offerti
- Il proxy ha la possibilità di filtrare basandosi sui contenuti

Architetture: screened network



- Più flessibile come architettura
- Più sicura: c'è un firewall che filtra le connessioni dalla DMZ verso la LAN interna
- Più costosa

Esempio

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:139 LOG fla
gs 0 level 4
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:139 reject-
with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:111 reject-
with icmp-port-unreachable
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21 LOG flag
s 0 level 4
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21 reject-w
ith icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:515 reject-
with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:143 reject-
with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:401 reject-
with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:6000 reject
-with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3000 reject
-with icmp-port-unreachable
REJECT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:2049 reject
-with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:2049 reject
-with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:5432 reject
-with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:110 reject-
with icmp-port-unreachable
REJECT     tcp  --  158.49.116.0/24      0.0.0.0/0           tcp dpt:22 reject-w
ith icmp-port-unreachable
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state ESTABLISHED
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 recent:
UPDATE seconds: 180 name: DEFAULT side: source
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x
16/0x02 recent: SET name: DEFAULT side: source

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

IDS

- Analogia: gli IDS possono essere visti come i sistemi di allarme delle abitazioni
- Lanciano allarmi in caso di attività sospette
- Sono passivi: a differenza dei firewall, hanno il compito di avvisare, non di intervenire

Anomaly detection

- Nella knowledge base mantengono il comportamento “normale”
- Effettuano un’analisi facendo un confronto col comportamento normale
- Tutto ciò che è diverso da questo è un comportamento anomalo

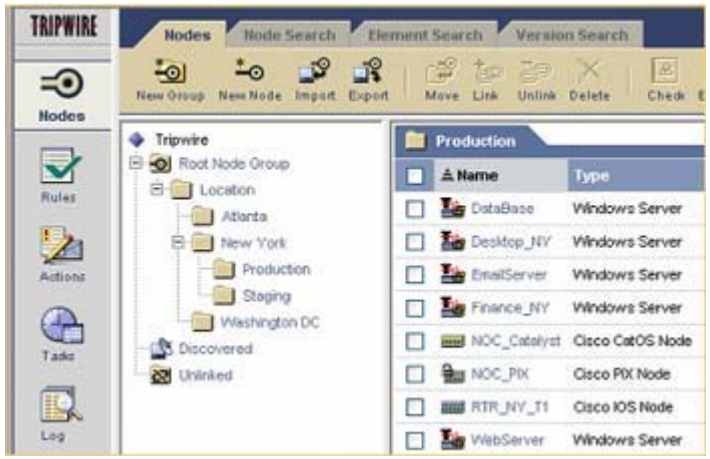
Misuse detection

- Nella KB mantengono il comportamento anomalo
- Effettuano un'analisi cercando i pattern dannosi: hanno un database di firme
- I più usati si basano sul pattern-matching

Anomaly vs Misuse: falsi allarmi

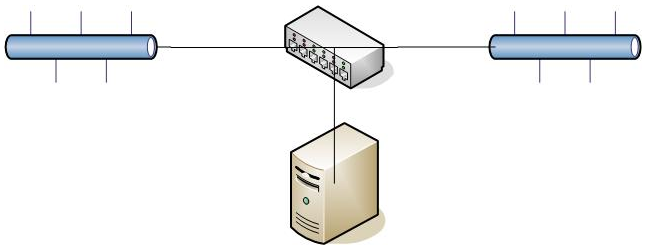
- Falsi negativi: attacchi non rilevati
- Falsi positivi: rilevamento errato
- Gli IDS di tipo anomaly producono un maggior numero di falsi positivi e meno falsi negativi
- Gli IDS di tipo misuse si comportano in maniera opposta

Host IDS



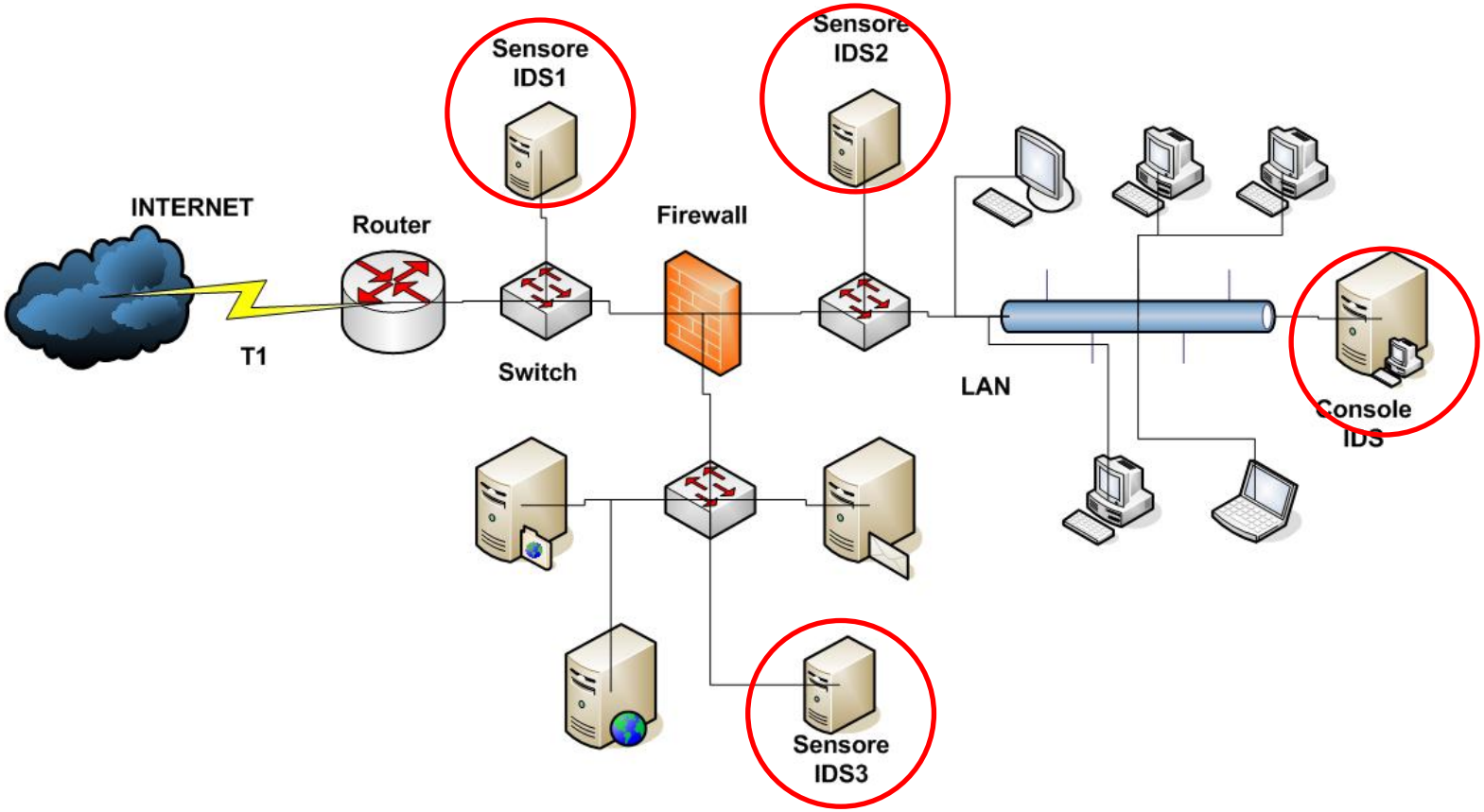
- Effettuano un'analisi sulla singola macchina host
- Possono essere configurati differentemente da un host all'altro: si guadagna in termini di precisione
- Non hanno una visione generale del comportamento della rete
- I più diffusi si basano sull'analisi del file system, per individuare modifiche non consentite

Network IDS



- Effettuano un'analisi sul traffico di rete, alla ricerca di pattern relativi ad azioni dannose
- Si installano sensori:
  - Nascosti
  - In modalità promiscua
  - Con raccolta ed analisi centralizzate

Strategie di inserzione



Strategie di inserzione

- A monte del firewall: analizzano tutto il traffico, compresi gli attacchi diretti al firewall
- Nella DMZ: rilevano gli attacchi ai servizi installati
- Nella LAN: analizzano il traffico interno

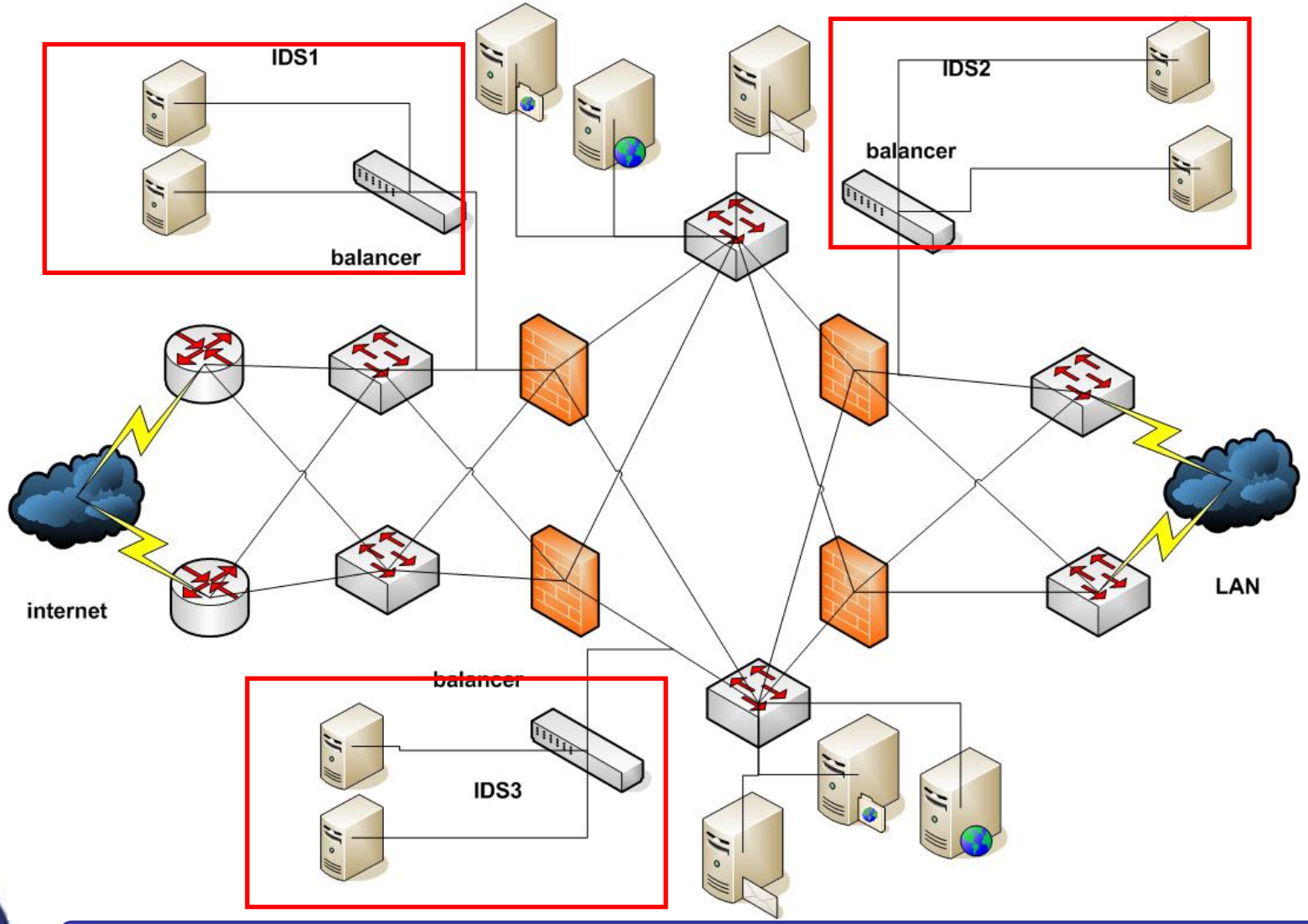
Tecnologia per l'inserzione

TAP

BALANCER

- TAP hanno 4 porte:
  - Una di input
  - La replica dell'input
  - Una di output
  - La replica dell'output
- Balancer:
  - Bilanciano il traffico sulle porte
  - Si evita che i sensori perdano pacchetti catturati in ingresso

Implementazione di un sistema di rilevamento delle intrusioni per reti

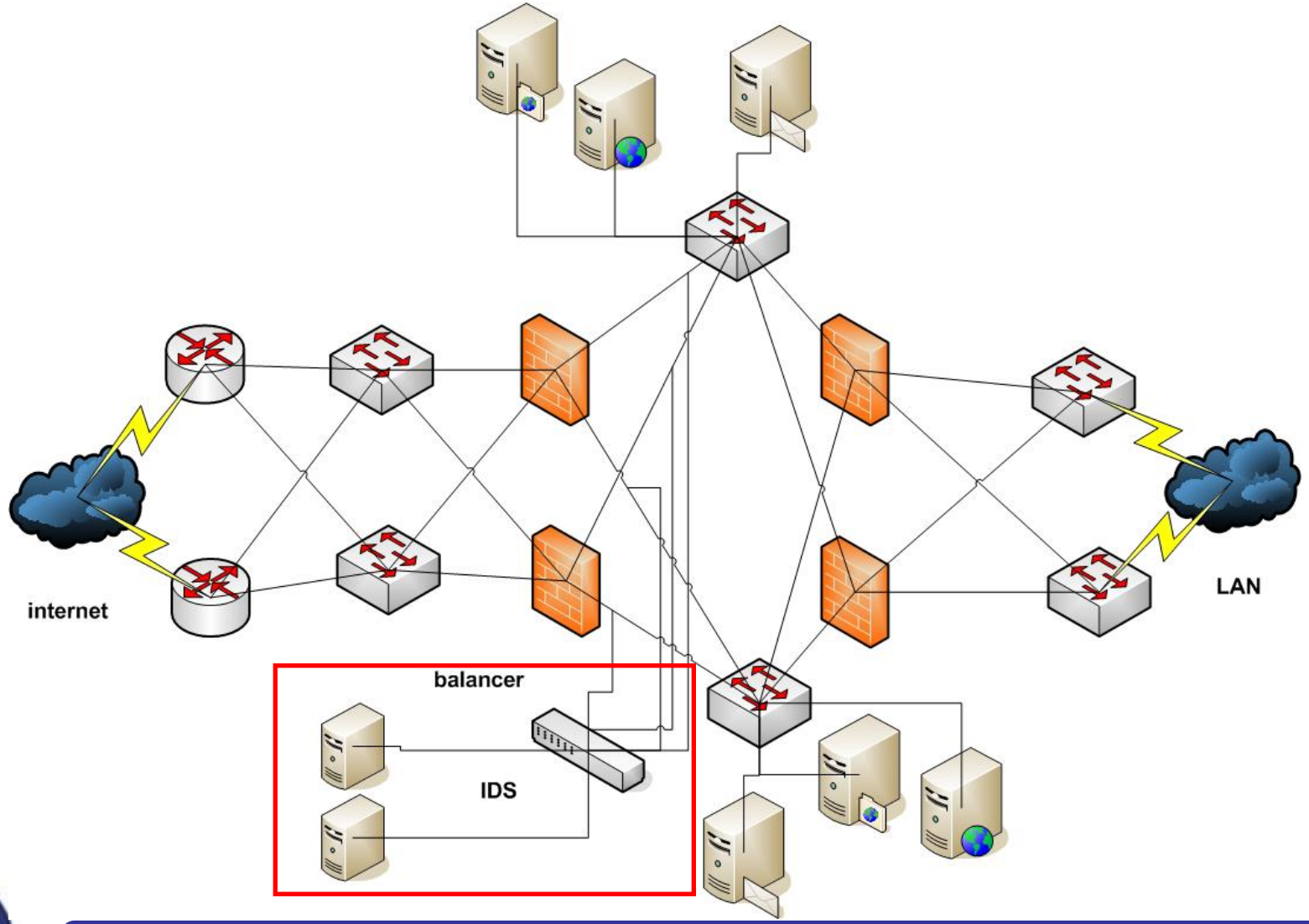


Dipartimento di Ingegneria Informatica, Gestionale e dell'Automazione

Problema: costi elevati

- Una soluzione di questo tipo comporta costi molto elevati:
  - 3 balancer
  - 6 sensori
  - 12 tap
- Si potrebbe pensare di utilizzare in tutto o in parte prodotti ***open source***

Implementazione di un sistema di rilevamento delle intrusioni per reti: ridotto



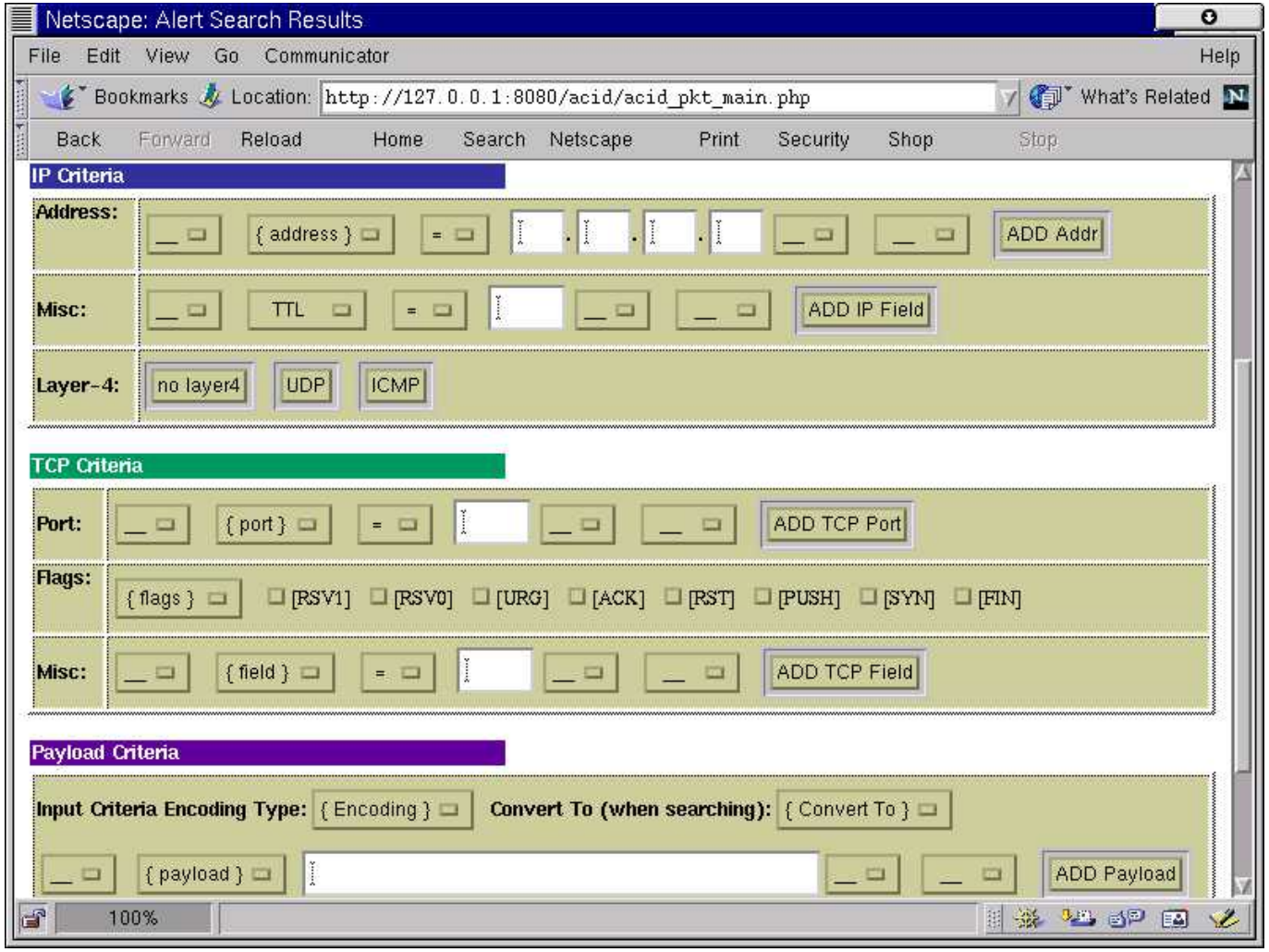
Intrusion Prevention System

- Gli IPS sono sistemi reattivi che agiscono nella fase di prevenzione degli attacchi
- Analizzano il traffico, come gli IDS, ma hanno la possibilità di filtrare pacchetti, come i firewall
- Problema: DoS indotto da un attaccante mediante spoofing di indirizzi consentiti
- Soluzione: blocco dinamico delle connessioni, filtri che agiscono sul singolo pacchetto

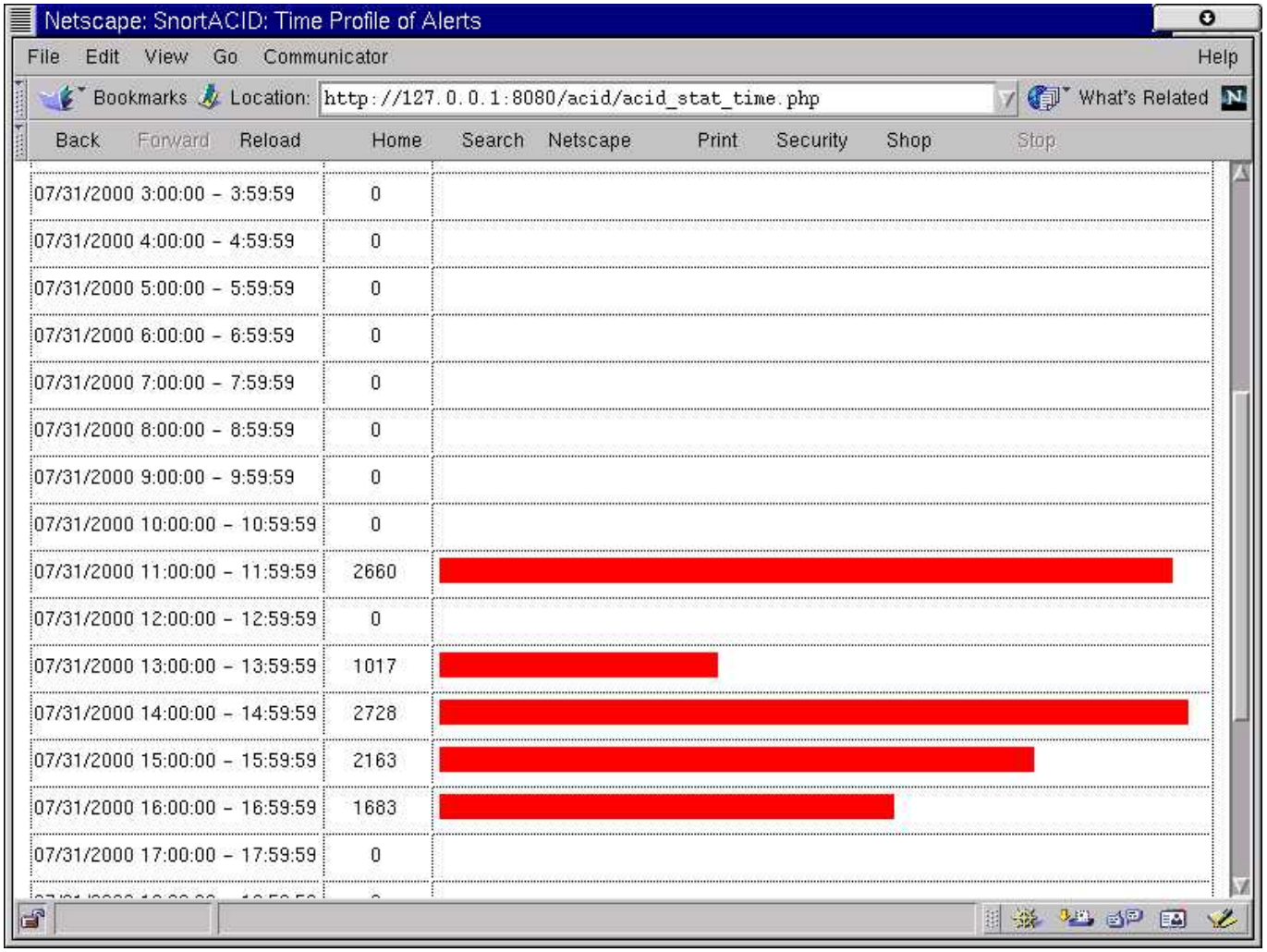
Analisi dei messaggi di log

- Quando si hanno diversi sensori, l'analisi dei messaggi di log diventa una procedura dispendiosa
- Si può utilizzare un sistema di raccolta ed analisi centralizzato
- Ad esempio, esistono console che forniscono strumenti per una lettura più agevole

Console per l'analisi degli allarmi: ACID



Console per l'analisi degli allarmi: ACID



07/31/2000 3:00:00 - 3:59:59	0
07/31/2000 4:00:00 - 4:59:59	0
07/31/2000 5:00:00 - 5:59:59	0
07/31/2000 6:00:00 - 6:59:59	0
07/31/2000 7:00:00 - 7:59:59	0
07/31/2000 8:00:00 - 8:59:59	0
07/31/2000 9:00:00 - 9:59:59	0
07/31/2000 10:00:00 - 10:59:59	0
07/31/2000 11:00:00 - 11:59:59	2660
07/31/2000 12:00:00 - 12:59:59	0
07/31/2000 13:00:00 - 13:59:59	1017
07/31/2000 14:00:00 - 14:59:59	2728
07/31/2000 15:00:00 - 15:59:59	2163
07/31/2000 16:00:00 - 16:59:59	1683
07/31/2000 17:00:00 - 17:59:59	0

Correlazione degli allarmi

- Altri allarmi e messaggi di log vengono prodotti da:
  - Sistema operativo
  - Altri strumenti di sicurezza
  - Applicativi
- Messaggi di log con livello di dettaglio differente e raccolti in punti differenti della rete
- Si può pensare di correlare i messaggi di log per avere una visione più generale e comunque completa

Correlazione degli allarmi

- Ad esempio si possono correlare gli allarmi in base:
  - Al timestamp: allarmi relativi ad eventi avvenuti in istanti di tempo vicini
  - Agli indirizzi IP sorgente e/o destinazione: allarmi relativi ad eventi generati dalla stessa sorgente e/o diretti alla stessa destinazione
  - Al tipo di messaggio: allarmi relativi ad eventi dello stesso tipo

Backup

- Le copie di backup possono essere utilizzate sia per risolvere problemi di sicurezza, sia per risolvere problemi di crash hw
- Servono:
  - Politiche di backup
  - Supporti hw
  - Utility sw

Politiche di backup

- Bisogna stabilire:
  - Quali sono i dati sensibili e dove si trovano
  - La frequenza con cui si vogliono effettuare i backup
  - Quando devono essere effettuati i backup e chi è responsabile di farlo
  - Il tipo di backup
  - Come vengono gestite le copie

Esempi

- Dati sensibili: dati privati di clienti e personale, dati necessari per i vari processi, altri dati utili al sistema informativo
- Si potrebbero effettuare backup in automatico, di notte
- Si potrebbero effettuare backup di sistemi ad intervalli di qualche settimana o un mese e backup incrementali o differenziali ogni settimana o quotidianamente (per i dati molto sensibili)

Supporti hw ed utility sw

- Si possono utilizzare CD o DVD, hard disk o dischi RAID
- Ci sono anche hw dedicati
- Esistono varie utility di supporto che forniscono:
  - Un'interfaccia friendly
  - Strumenti per l'esecuzione automatica
  - La scelta dei vari tipi di backup da effettuare

Consigli

- È utile conservarsi più copie effettuate in date differenti
- Si consiglia di separare il backup dei dati da quelli del sistema per gestirli separatamente
- Effettuare periodicamente copie del sistema su supporti non modificabili
- Fare attenzione alle copie per evitare di smarrirle o danneggiarle

Risposta agli incidenti informatici

- La risposta agli incidenti è composta da:
  - ***Analisi*** delle informazioni che vengono dalla fase di rilevamento (completate con altre raccolte al momento)
  - ***Intervento*** per evitare o ridurre al minimo i danni
  - ***Configurazione*** dei sistemi per eliminare le vulnerabilità
  - ***Ripristino*** del normale funzionamento

Direzione futura

- La tendenza attuale è quella di avere strumenti di analisi anche complessi
- Aiutano ad analizzare grandi moli di dati che riguardano l'attività
- L'evoluzione potrebbe essere un sistema che produce dei piani di soluzione, dopo aver riconosciuto il tipo di incidente
- Sistemi di questo tipo potrebbero essere di supporto ai security manager