

# I sistemi di Intrusion Detection: problemi e soluzioni

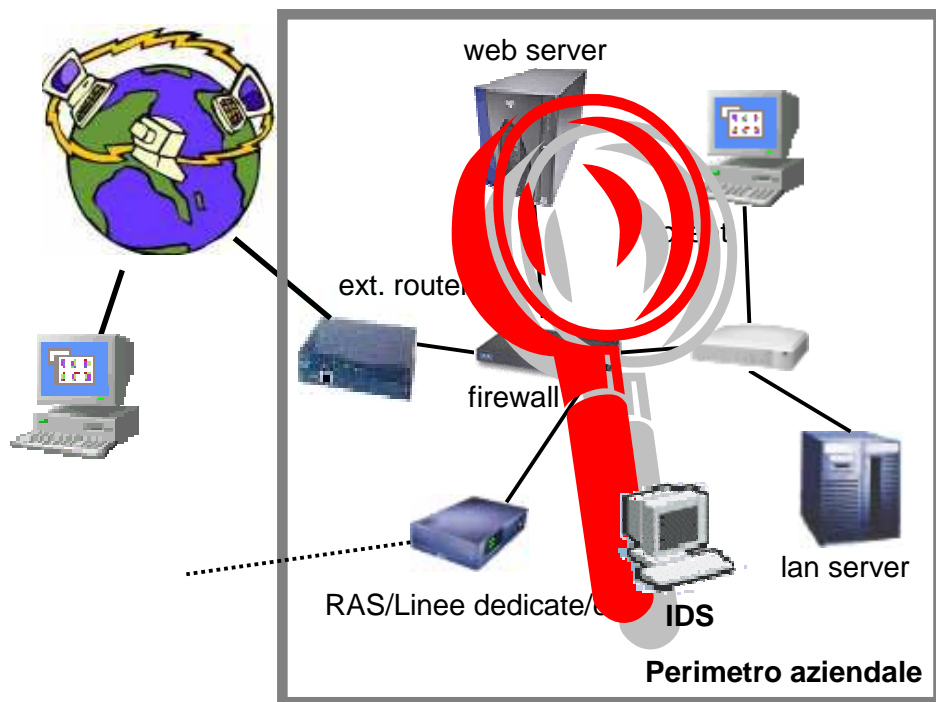


<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

Relatore: Igor Falcomatà

# Cos'è un'Intrusion Detection System ?

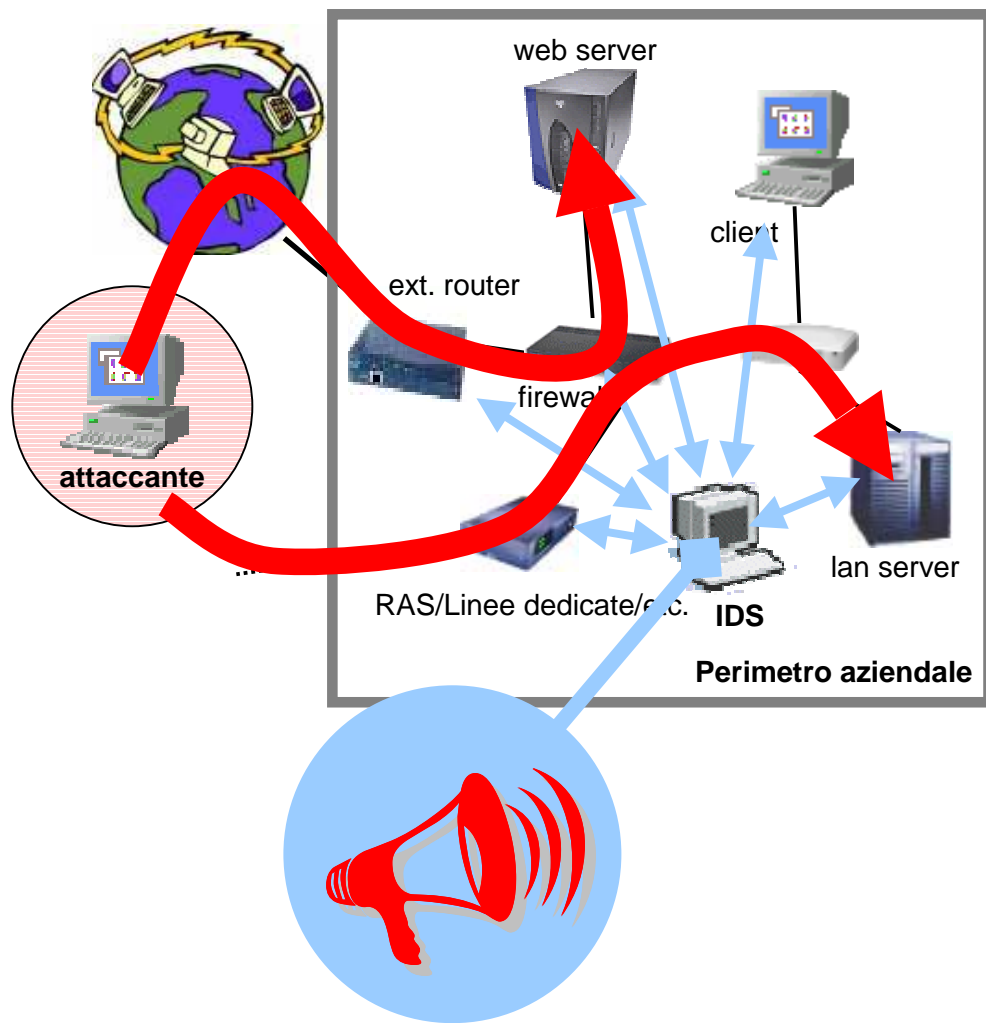


Esempio di rete aziendale "classica":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- RAS, Linee dedicate, VPN

Un IDS è un sistema per individuare e segnalare attacchi, intrusioni e violazioni delle policy.

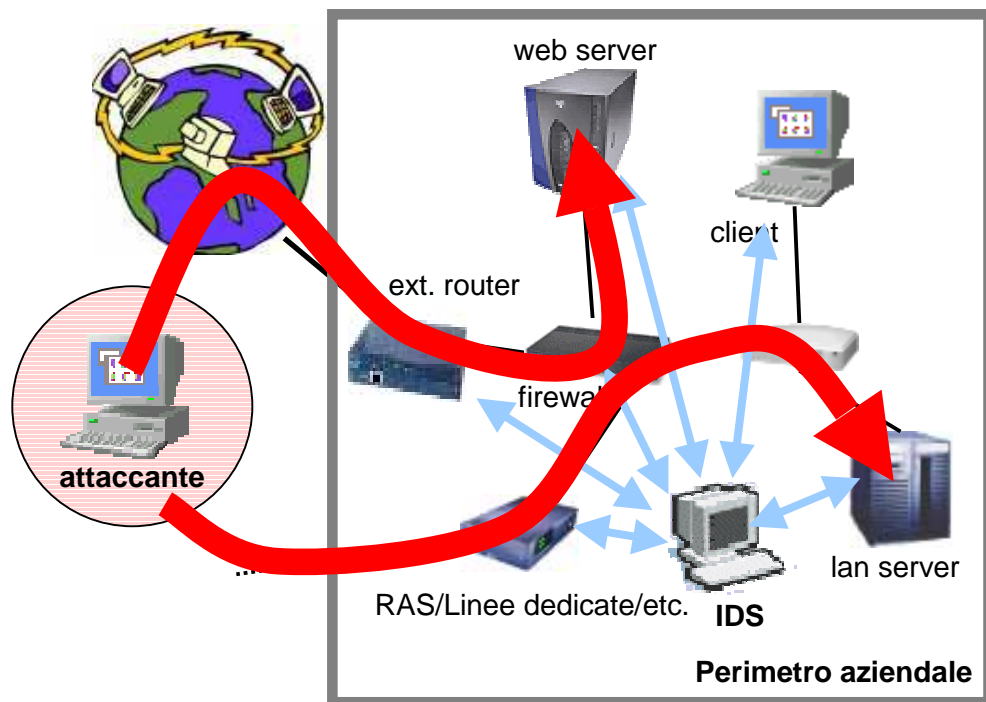
# Obbiettivi degli IDS



In teoria dovrebbero:

- monitorare ogni sistema e device
- essere affidabili al 100%
- riportare in tempo reale gli attacchi...
- ...con una diagnosi accurata del problema
- eventualmente segnalare o addirittura attivare le procedure per la soluzione

# Limiti degli IDS

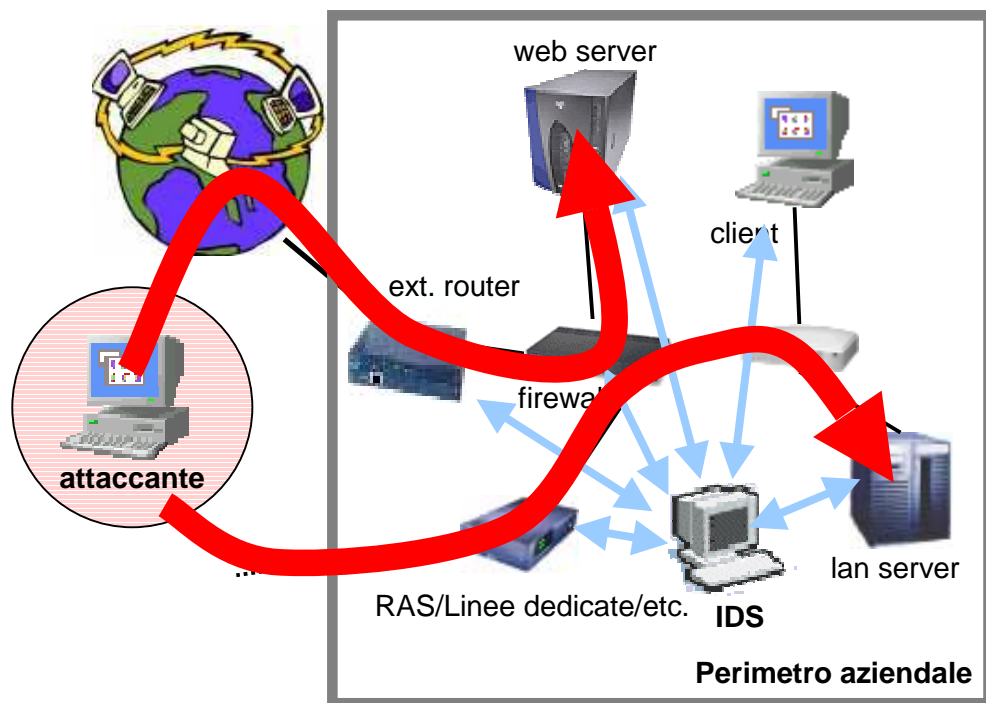


Ogni strumento ha dei limiti...  
...conoscerne le debolezze aiuta ad  
utilizzarli in maniera corretta ...

In pratica soffrono di:

- tipologie di attacco riconosciute spesso limitate agli attacchi già noti
- enorme numero di nuovi attacchi resi pubblici ogni giorno
- falsi positivi
- falsi negativi
- possibili errori di sviluppo o implementazione

# Funzionalità avanzate

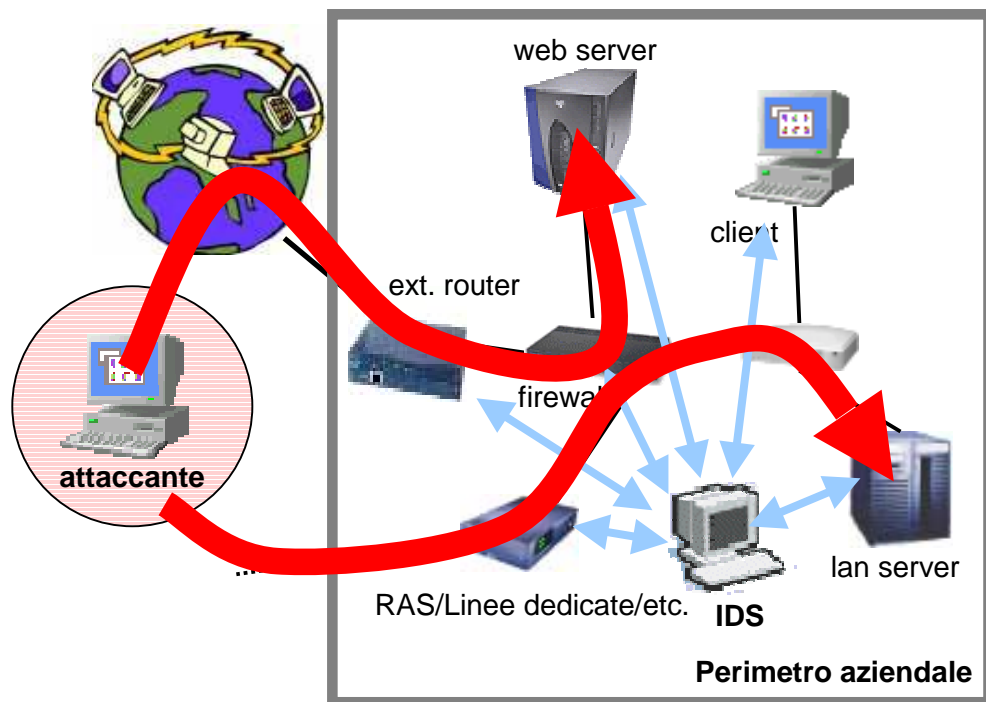


## I più avanzati

- permettono di personalizzare gli eventi da segnalare ed i report con linguaggi di scripting
- gestiscono un numero elevato di device e sistemi operativi
- sono in grado di collaborare utilizzando numerosi sensori
- sono in grado di pilotare Firewall e altri dispositivi di difesa per rispondere agli attacchi [1]

[1]: Si tratta di funzionalità da utilizzare con estrema precauzione, per non causare interruzioni alle attività legittime. E' una pessima pratica, purtroppo diffusa, abusare di queste funzionalità per non doversi curare di aggiornare sistemi sicuramente vulnerabili presenti sulla rete!

# Funzionamento degli IDS



## Come funzionano?

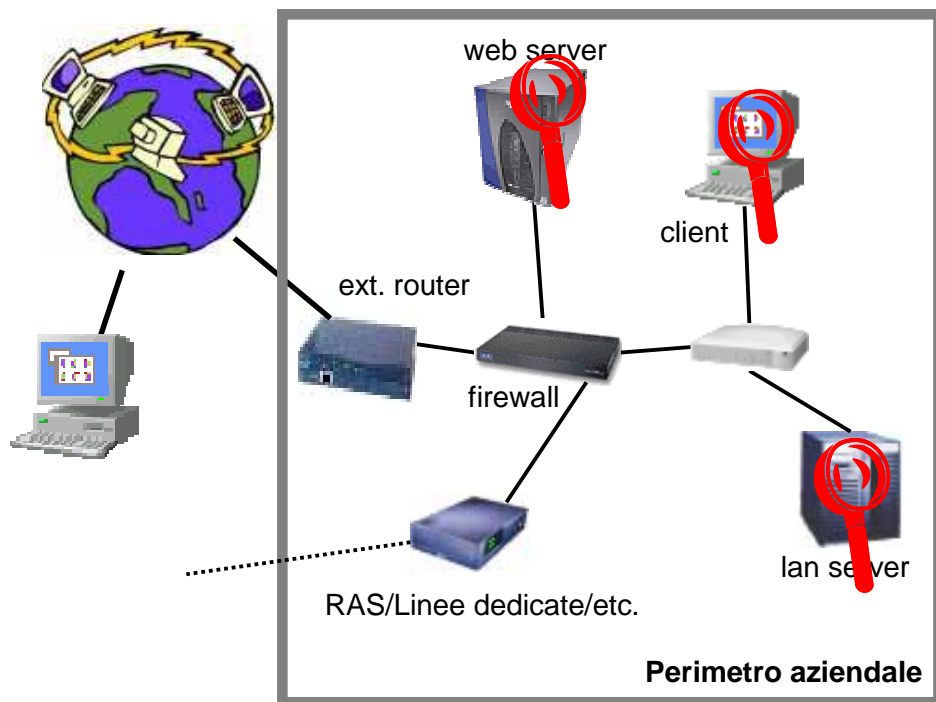
- analizzano in real-time una serie di eventi
- analizzano gli eventi in base a specifici parametri
  - attacco conosciuto
  - evento non permesso
  - evento anomalo
  - ...
- segnalano le anomalie secondo le configurazioni

NIDS -> Network Intrusion Detection System

HIDS -> Host Intrusion Detection System

DIDS -> Distributed Intrusion Detection System

# Host Intrusion Detection System

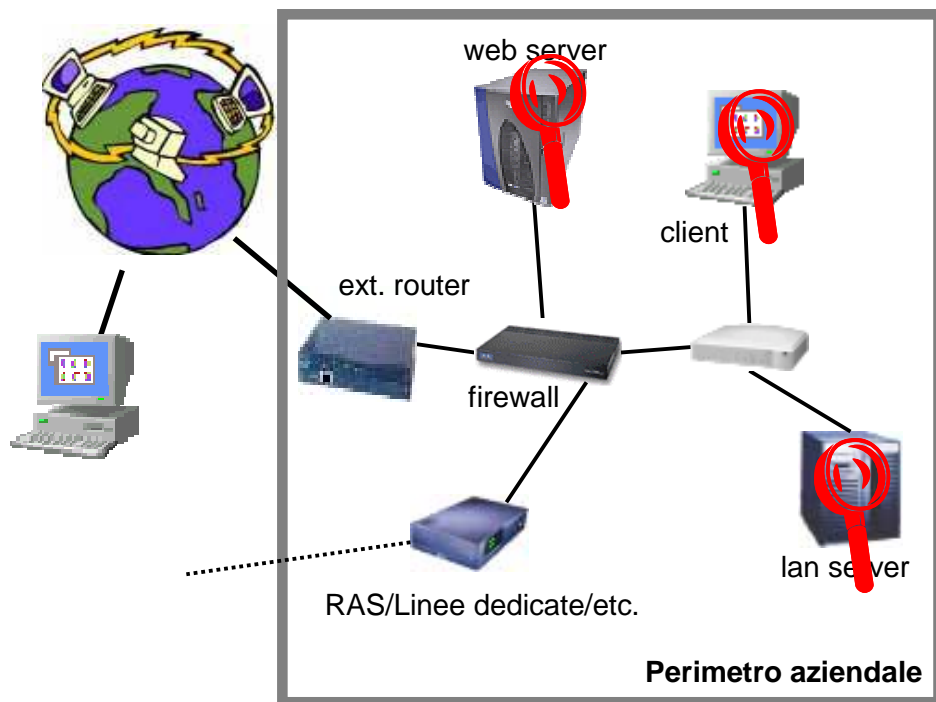


Basati su host e capaci di riconoscere una serie di attività interne al sistema.

## Come funzionano?

- sono installati sul sistema stesso (moduli kernel, etc.)
- analizzano in real-time le attività:
  - log
  - attività utenti
  - attività applicazioni
  - modifiche a file o documenti
  - ...
- segnalano le anomalie secondo le configurazioni

# Host Intrusion Detection System

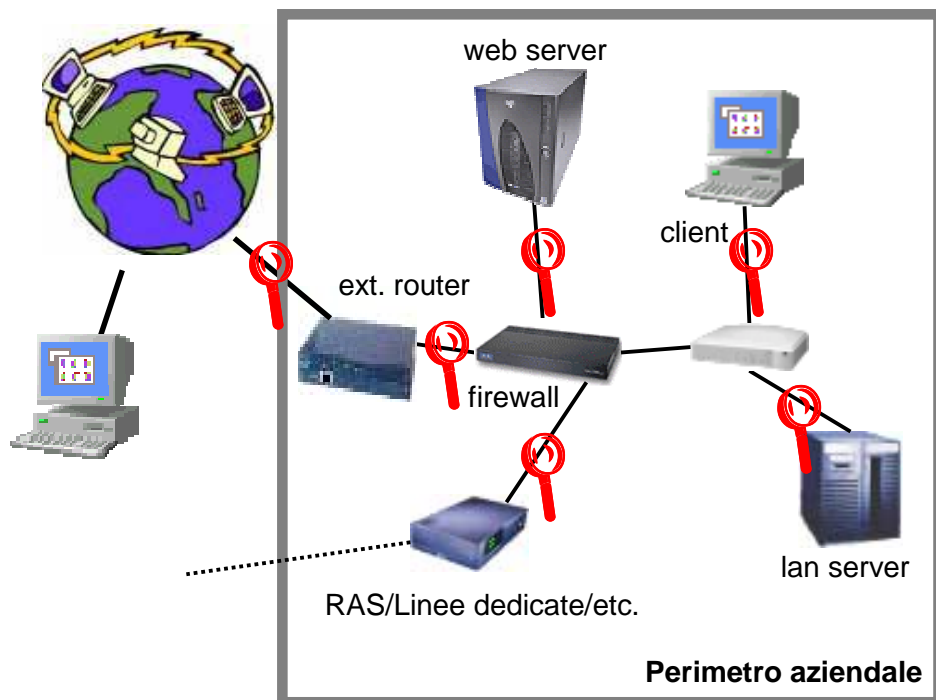


Sono utilizzati per il controllo avanzato delle attività del sistema, del software e degli utenti ospitati.

## Problematiche:

- Dipendenti dal sistema operativo  
(supporto, affidabilità)
- Licenze multiple  
(una per postazione)
- Visione ristretta  
(solo su quell'host)
- Utilizzo risorse  
(CPU, memoria, etc.)

# Network Intrusion Detection System

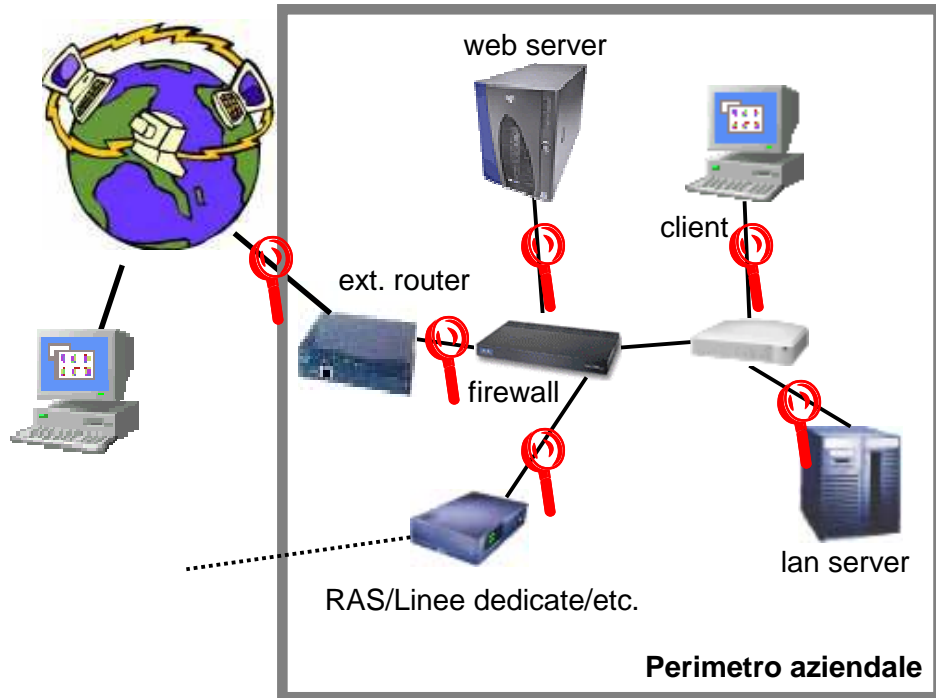


Basati sull'analisi del traffico in transito e capaci di riconoscere una serie di attività sulla rete.

## Come funzionano?

- sono sensori esterni che "sniffano" la rete (sistemi dedicati o appliance)
- analizzano in real-time il traffico in transito per individuare attacchi verso gli altri sistemi
- segnalano le anomalie secondo le configurazioni

# Network Intrusion Detection System

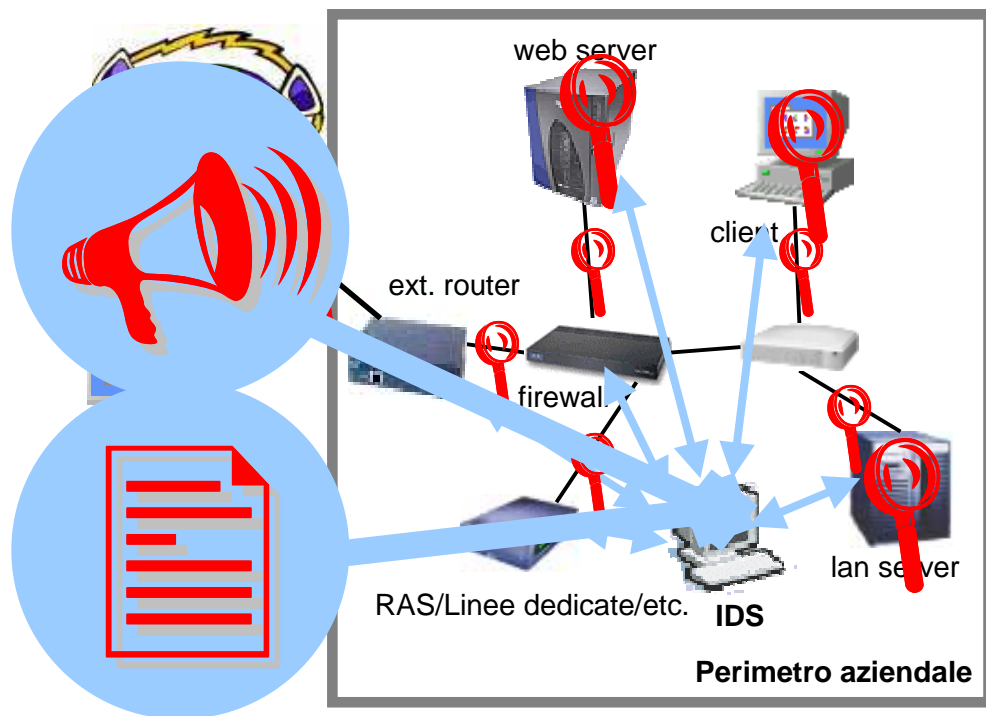


Sono utilizzati per il controllo avanzato del traffico e delle attività di altri sistemi sulla rete.

## Problematiche:

- limiti di analisi del traffico
  - reti segmentate
  - bandwidth troppo elevato
  - pacchetti frammentati
  - limiti dello stack TCP/IP
  - protocolli non riconosciuti
- difficilmente scalabili
- impossibilità di analizzare il traffico cifrato (SSL, IPsec, PGP, S/MIME, etc.)
- spesso basati su "signature" fisse

# Distributed Intrusion Detection System

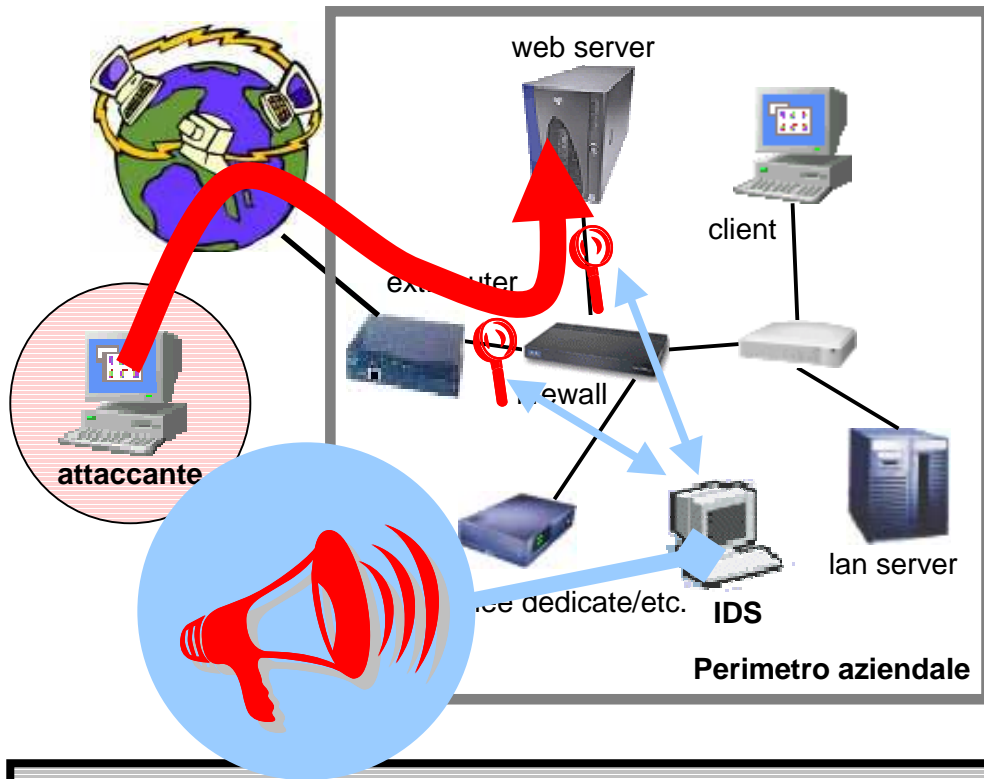


Sono utilizzati per integrare tutte le attività di Intrusion Detection di una rete.

## Come funzionano?

- Aggregano e analizzano i dati di vari sensori
  - NIDS
  - HIDS
  - log di sistema
- permettono una visione d'insieme delle attività di reti e sistemi
- gestiscono centralmente le configurazioni e i report
- segnalano le anomalie secondo le configurazioni

# Individuazione degli attacchi (NIDS)



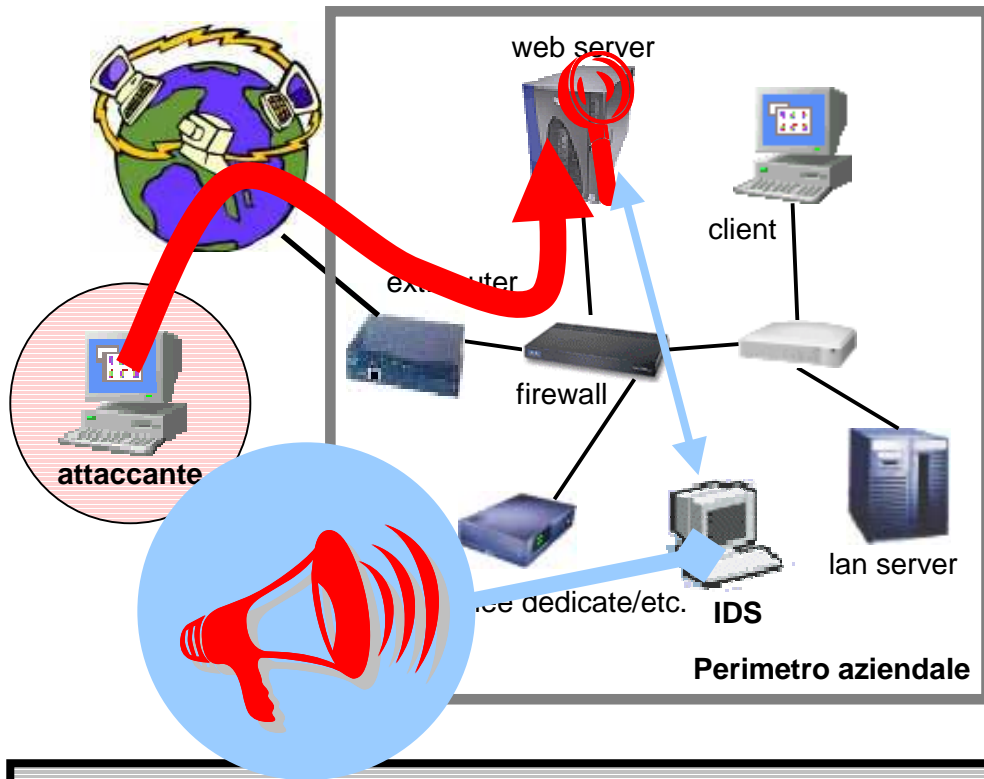
Utilizzando un sistema distribuito, sarà possibile analizzare il traffico di più sensori e correlarlo.

## Cosa è necessario?

- riconoscere la tipologia di attacco
- "intercettare" il traffico (posizionamento del sensore)
- esempio:

per individuare un attacco proveniente da Internet verso il web server sarà necessario posizionare un sensore su quel segmento di rete (sulla dmz o prima del firewall)

# Individuazione degli attacchi (HIDS)



Utilizzando un sistema distribuito avanzato, è possibile correlare i dati di NIDS e HIDS.

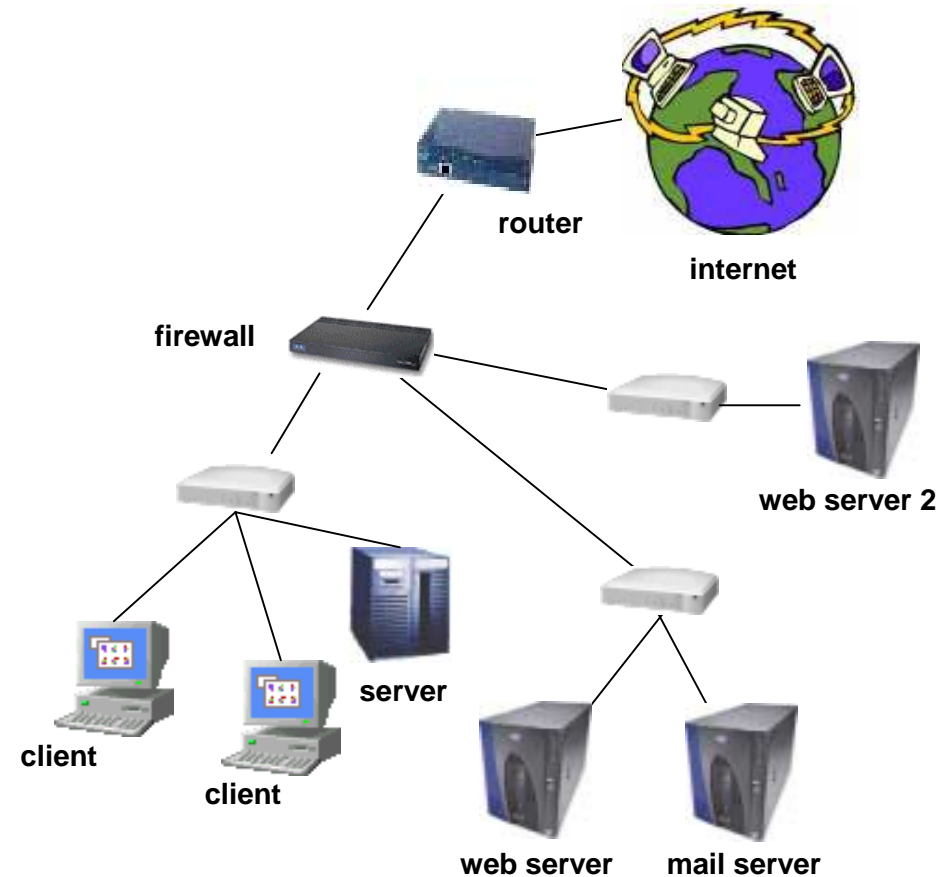
## Cosa è necessario?

- riconoscere la tipologia di attacco
- “intercettare” l'attacco (HIDS installato sul sistema)
- esempio:

per individuare un attacco proveniente da Internet verso il web server sarà necessario installare un sensore sul sistema stesso

# Come definire una struttura di base dei sensori

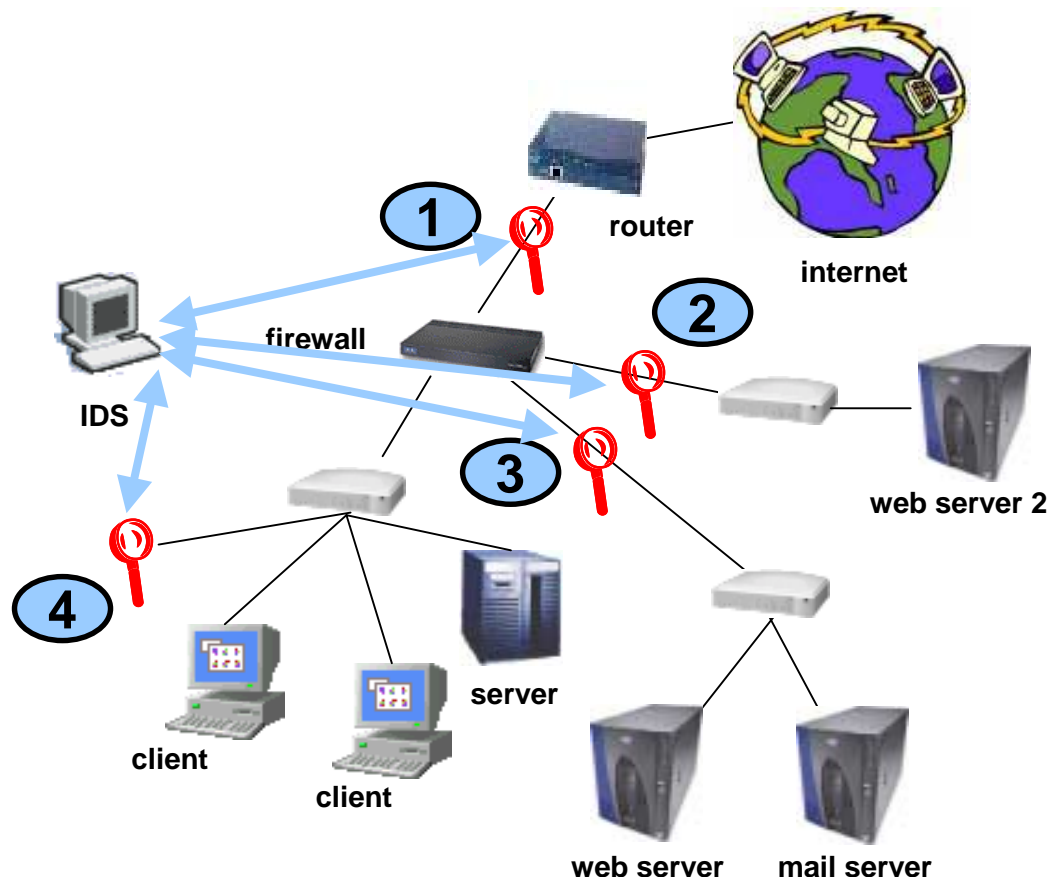
- spesso il partizionamento della rete non permette di monitorare l'intera struttura con un unico sensore
- per posizionare i sensori bisogna considerare il traffico nei vari segmenti
- se non è possibile analizzare tutto il traffico, i sensori andranno posizionati:
  - nei punti di passaggio (gateway, fw, etc.)
  - nei punti più vulnerabili (sistemi pubblici, etc.)
  - dove risiedono i dati maggiormente sensibili



# Come definire una struttura di base dei sensori

Nell'esempio:

- il sensore 1 analizza il traffico da e per Internet
- il sensore 2 analizza il traffico da e per il 2° web s.
- il sensore 3 analizza il traffico da e per il web ed il mail server
- il sensore 4 analizza il traffico sulla rete locale
- l'IDS  
esamina i dati forniti dai sensori, correla gli eventi, gestisce la configurazione e la reportistica centralizzate



I sensori e l'IDS utilizzano una rete separata per lo scambio dei dati (tra le due reti non ci sono collegamenti)

# Quali sono i principali sistemi di Intrusion Detection

I principali IDS (circa l' 80%) del mercato:

- Cisco: Secure IDS <http://www.cisco.com/go/ids>
- ISS: RealSecure <http://www.iss.net>
- Axent: Intruder Alert <http://www.axent.com>
- Intrusion.com: Secure Net Pro <http://www.intrusion.com>

Altri:

- Enterasys: Dragon <http://www.enterasys.com/ids>
- NFR Security: NID e HID <http://www.nfr.net>
- Marty Roesch: Snort <http://www.snort.org>

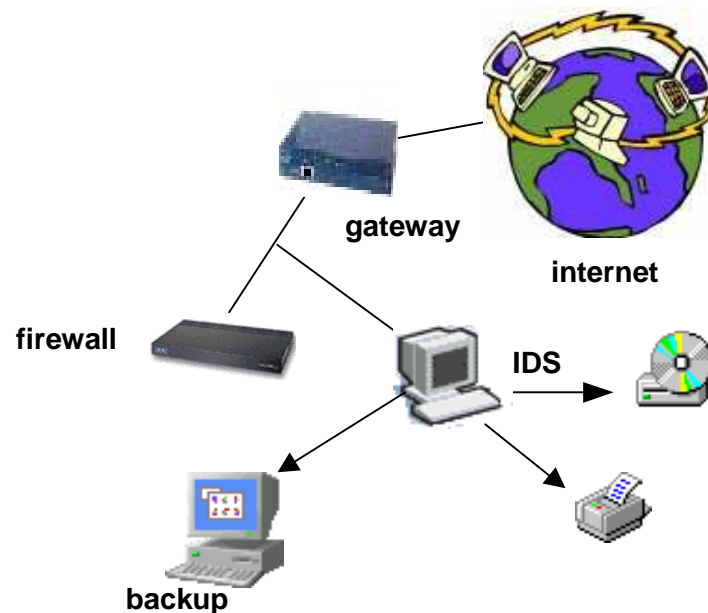
Secure IDS di Cisco e Real Secure di ISS tra i leader di mercato, Snort come alternativa open source e NFR perché ritenuto tecnologicamente il più avanzato.

# Come proteggere gli IDS

- E' consigliabile (per ragioni di performance e sicurezza) che i sensori di rete, le console di amministrazione ed i database degli IDS siano su sistemi dedicati e controllati da un'apposita rete di management, separata dalla rete di produzione
- qualora si utilizzi un OS ospite per installare un sensore NIDS, si applichino le stesse regole utilizzate per la protezione dei sistemi più sensibili :
  - tutti i servizi vanno disabilitati
  - tutti gli utenti superflui vanno rimossi
  - controlli di accesso alle risorse (file, registro, kernel, memoria)
  - "hardening" generale del sistema
  - quando possibile è comunque consigliabile utilizzare un appliance hardware con un OS appositamente preconfigurato
- come "punto di ascolto" sulla rete di produzione è consigliabile utilizzare un'interfaccia in modalità "stealth" e strumenti che impediscano l'invio di dati dal sensore ("receive-only")

# Come proteggere l'output degli IDS

- Per mantenere l'integrità dei dati raccolti è consigliabile utilizzare supporti "write-once", ovvero sistemi in cui i dati non possano essere alterati dopo che siano stati registrati
- alcune misure pratiche attuabili possono essere:
  - funzionalità "append-only" dell'OS
  - stampare l'output
  - utilizzare periferiche WORM (sola scrittura)
  - replicare i dati su altri sistemi in sola scrittura



- la scelta delle misure da implementare per la protezione degli output degli IDS varia in funzione della topologia di rete, dell'importanza dei dati e delle risorse a disposizione per proteggerli.

# Come gestire gli incidenti e le risposte agli incidenti

- Qualora venga identificata una intrusione in maniera inequivocabile, è possibile adottare soluzioni diverse in base alle esigenze:
  - reinstallare ex-novo il sistema
  - ripristinare il sistema cancellando eventuali modifiche effettuate indebitamente
  - congelare il sistema per permettere l'intervento di personale specializzato nell'individuazione di attività illecite

# Analisi e contenimento:

- Sono comunque da effettuare i seguenti passi:
  - identificare la provenienza degli intrusi
  - identificare le modalita dell'attacco e le sue implicazioni
  - identificare i sistemi coinvolti ed il livello di esposizione
  - iniziare delle misure di contenimento se l'attacco fosse ancora in atto

**Le procedure di reazione ad un attacco devono essere studiate preventivamente per non commettere errori in caso di emergenza**

# Reazione e risoluzione:

- Nel momento in cui l'emergenza viene ricondotta ad uno stato "controllato":
  - effettuare comunicazione dell'attacco subito
  - ripristinare l'operatività dei sistemi
  - patchare tempestivamente le vulnerabilità che hanno portato alla compromissione
  - mantenere un livello di monitoraggio elevato

**Dovrebbe essere preparato uno staff  
per limitare al minimo il disservizio**

# Cosa si può fare con un IDS

- Da Internet:
  - individuare un attacco → contromisure
  - individuare violazioni o tentate violazioni delle policy
  - statistiche utilizzo risorse in entrata
  - registrazione del traffico con finalità forensi
- Verso Internet:
  - individuare attacchi condotti dai dipendenti verso sistemi esterni
  - individuare invii non autorizzati di materiale aziendale
  - individuare violazioni o tentate violazioni delle policy
  - statistiche utilizzo risorse (web, mail, etc)
  - registrazione del traffico con finalità forensi

# Non dimentichiamoci

- Un IDS non deve essere accessibile, né dalla rete pubblica (Internet), né da altre reti (Lan, Dmz, Intranet, etc.)
- applicare la politica “un sensore per ogni segmento di rete”
- analizzare la maggior quantità di traffico possibile (soprattutto da e verso Internet)
- evitare di basarsi solo sul rilevamento degli attacchi conosciuti dall'IDS

# Conclusioni:

- L'impostazione di un sistema di sicurezza deve comprendere un piano complessivo:
  - Avere uno staff preparato e sensibile alla sicurezza
  - Utilizzare una varietà di strumenti coordinati (policy, antivirus, firewall, IDS)
  - Venire costantemente verificato ed aggiornato
  - Non affidarsi unicamente alla tecnologia

**La robustezza di un sistema di sicurezza viene misurata in base alla robustezza della sua componente più debole**

# Studio di fattibilità

- Concretamente, le possibilità per l'applicazione di un sistema di Intrusion Detection alla Vostra rete:
  - 1) acquisire la tecnologia e le competenze per utilizzarla
  - 2) acquisire la tecnologia ed appaltarne in outsourcing il controllo
  - 3) appaltare tutta la gestione dell'IDS (tecnologia, controllo, etc.) in outsourcing

# Tutti pensano di essere fuori pericolo, ma molto spesso ci si trova impreparati.

Capita troppo spesso che vengano ignorate totalmente le misure di sicurezza che potrebbero fare la differenza tra una rete violata ed una rete che passa indenne gli attacchi degli hackers.



# Is Your Business Internet eXposed?



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

## Possiamo aiutarvi!