IDS/IPS/Honeypot

IDS: Intrusion detection systems

- Tentano di rilevare:
  - attività di analisi della rete
  - tentativi di intrusione
  - intrusioni avvenute
  - comportamenti pericolosi degli utenti
  - traffico anomalo

Tecniche per IDS

- I sistemi di Intrusion Detection possono utilizzare diverse tecniche per rilevare un'intrusione:
  - verificare la presenza di schemi corrispondenti ad attacchi (pattern matching)
  - verificare la presenza di traffico "irregolare":
    - imparando qual è il traffico corretto e rilevando quello anomalo
    - in base a politiche che definiscono il traffico corretto/anomalo (es. violazioni di protocollo)

Tipologie di IDS

- NIDS: analizzano il traffico in rete (i sensori sono sniffer senza indirizzo IP)
- HIDS: analizzano le attività su un sistema
- Sistemi misti/ibridi (es. NIDS per singoli sistemi, architetture con HIDS/NIDS con un’unica console)

Network IDS (NIDS)

- Esaminano il traffico su un segmento di rete
- Vedono traffico che un HIDS potrebbe non vedere
- Non dipendono (molto) dagli OS dei sistemi
- Non hanno una visione del contesto in cui i dati saranno interpretati (OS, applicazione, ambiente…)
- Possono essere sovraccaricati con una certa facilità
- Ormai funzionalità comuni per diversi tipi di apparati
  - es. WAF (Web Application Firewalls)

HIDS: IDS per singoli sistemi

- Verificano tentativi di attacco al singolo sistema
- Possono:
  - esaminare i log del sistema e delle applicazioni
  - verificare lo stato dei file
  - controllare le attività dei processi (es. chiamate di sistema)
  - controllare il traffico di rete (sistemi ibridi, che possono anche bloccare il traffico come i personal firewall, a volte specializzati per applicazioni come http)
  - ...

HIDS vs. NIDS

- Sono meno pesanti per il sistema: possono essere installati su server e sistemi critici
- Se il sistema è compromesso, possono essere manomessi
- Hanno un'idea più chiara dell'ambiente in cui sono trattati i dati
- Sono sensibili ai DoS quanto il sistema su cui sono

Metodologie di analisi

- Tipo di analisi:
  - In base a database di attacchi noti
  - Euristiche
- Quando analizzare i dati?
  - Tempo reale?
  - Analisi successiva
  - Entrambe

IDS aggiornabili o programmabili?

- Aggiornabili con tecniche stile antivirus
  - Utile per attacchi noti, tipicamente pattern
  - Costo di gestione limitato
  - Debole su componenti legacy
- Personalizzabile
  - Flessibile ma oneroso
  - Duplicazione di sforzi già fatti?
- Ibridi: aggiornabili, ma con una certa flessibilità nella definizione di nuovi plug-in
  - es. Snort

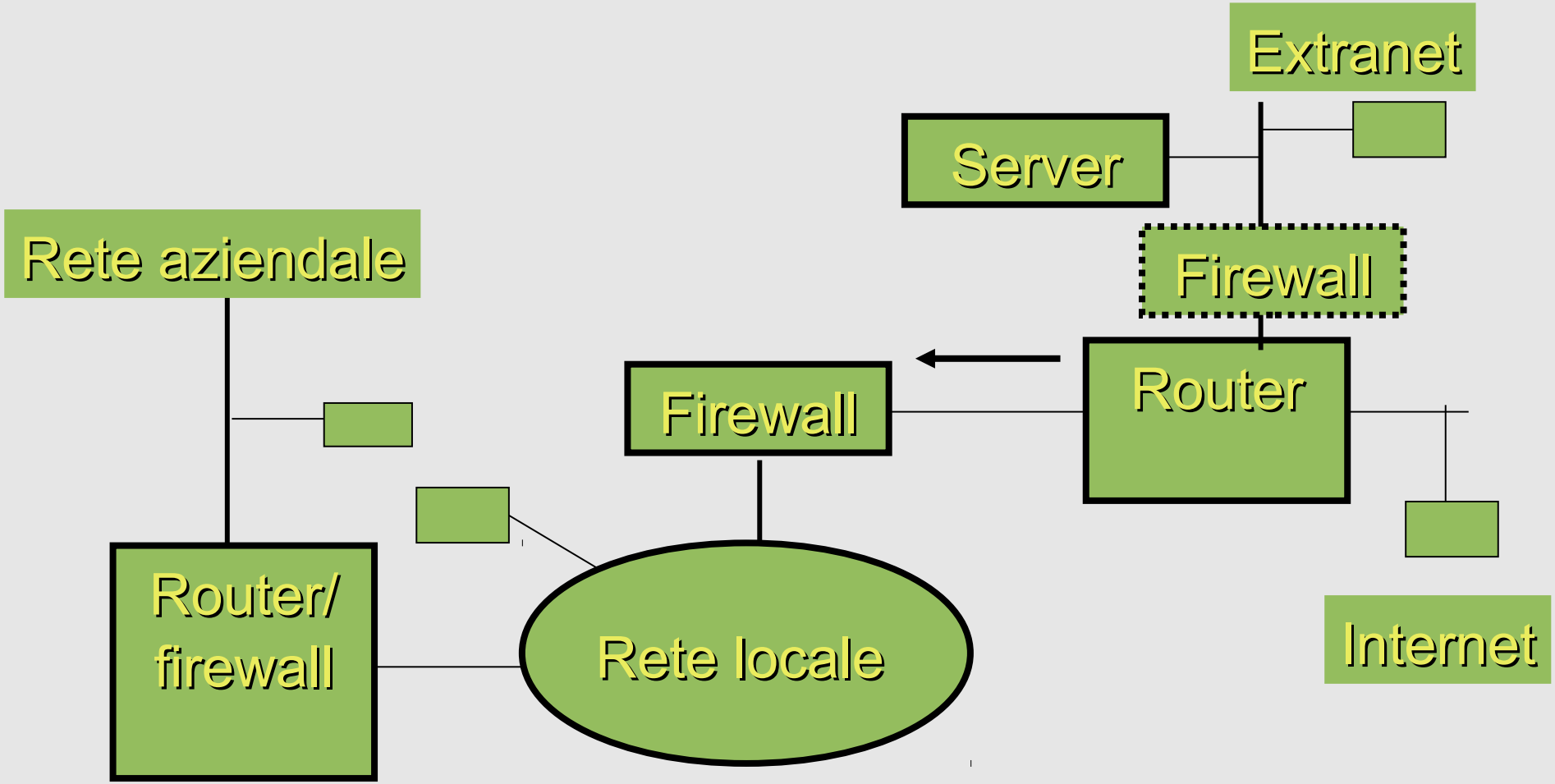
Uso dei sistemi di intrusion detection

- Non sostituiscono i firewall
- Interferiscono meno con il traffico di rete (è un vantaggio?)
- Possono essere utilizzati anche per monitorare il traffico interno
  - installazione/attivazione meno intrusiva
  - Attenzione alla capacità delle porte...
  - Network TAP
- Reactive IDS: abbattono le connessioni (o peggio?)

Gestione degli IDS

- Generalmente sono composti da:
  - agenti, da installare in punti critici della rete o su sistemi a rischio
  - console per la gestione e l'analisi
- Parte dell'elaborazione dei dati è fatta sull'agente
  - selezione dei dati interessanti
- Parte dell'elaborazione è fatta sul database presente sulla console
  - analisi a posteriori
  - visione globale

Dove mettere un IDS?



Attacchi agli IDS: input validation

- Gli IDS sono programmi eseguiti con privilegi elevati che leggono dei dati (i pacchetti) e li elaborano
- Se non sono realizzati con sufficiente cura, inviando pacchetti malformati è possibile avere anche qui dei buffer overflow
- Problemi analoghi (pubblici): ethereal, tcpdump…

Problemi tecnologici degli IDS

- Prestazioni (NIDS)
- Quanti protocolli e applicazioni devono conoscere?
- Falsi positivi?
- Falsi negativi (slow scans, traffico frammentato…)
- Aggiornamento
- Riconoscimento di attacchi inusuali

Problemi di uso degli IDS

- Lasciati a se stessi, gli IDS proteggono solo dagli attacchi banali
- Nella maggior parte dei casi, richiedono un'analisi e una decisione
- Sono necessari più dati del solo pattern che ha causato l'allarme:
- i dati possono essere incrociati con quelli del firewall
- può servire il traffico apparentemente legittimo o trascurabile di giorni precedenti
- interpretare i dati può essere difficile, specialmente se sembrano contraddittori o non decisivi

Integrazione con altri strumenti

- Integrazione con strumenti di scanning o gestione delle patch
  - permette di ridurre l'insieme di alert da monitorare, o di ridurre la gravità di una segnalazione
  - la presenza di un attacco può comunque essere un evento rilevante
- Integrazione con la gestione di firewall
  - da usare con cautela

Intrusion prevention

- Perché monitorare solamente il traffico e reagire solamente a posteriori e potenzialmente in ritardo?
- Gli strumenti di intrusion prevention si interpongono e bloccano l'attacco, anziché limitarsi al monitoraggio
  - potenziali problemi di prestazioni
  - più problemi con i falsi positivi
  - di fatto sono firewall specializzati

Honeypots/Honeynets

- Sono sistemi o reti “trappola”
- Generalmente più facili da attaccare, non hanno un uso reale: tutto il traffico è almeno anomalo
- Adatti a studiare gli attacchi... ma chi lo fa?
- L’attaccante può scoprirsi qui prima di attaccare i sistemi reali
- Non devono essere a loro volta fonte di attacco
- Potenziali problemi legali?