IDS Intrusion Detection System

L'introduzione di tali sistemi in una rete locale richiede generalmente la configurazione degli apparato di rete (Lan Switch); per essere utile un **Network IDS** deve essere in grado di intercettare tutto il traffico di pacchetti scambiati tra i partecipanti.

In presenza di switch ciò può richiedere la trasformazione della interfaccia di rete utilizzata per connettere la piattaforma che svolge funzione di network IDS in porta di monitor; una porta di uno switch in stato di monitor invia una replica dei pacchetti in ingresso allo switch (oppure ad un sotto-insieme di porte dello switch) alla stazione direttamente connessa.

Per poter acquisire regolarmente i pacchetti, la scheda di rete del network IDS deve operare in modalità promiscua; non occorre comunque che la piattaforma con funzioni di network IDS abbia configurato lo stack TCP/IP sull'interfaccia usata per l'acquisizione; in assenza del TCP/IP il sistema risulta invisibile agli altri utenti attestati sulla rete locale.

Per assicurare che il sistema possa dialogare con altri sistemi locali, la stazione su cui viene installato il software deve essere dotata di più interfacce di rete.

Molto spesso il Network IDS è installato a ridosso dei gateway che interconnettono la rete aziendale al resto del mondo Internet pubblica.
Poiché un IDS acquisisce solo i pacchetti che attraversano lo switch cui è connesso, nel caso di Lan aziendale organizzata in più sottoreti logicamente separate, può essere necessario attivare più sistemi di rilevazione distribuiti; i dati raccolti da ciascun IDS possono poi essere esaminati da una console centralizzata in maniera sicura, previa realizzazione di una rete di management/monitoring dedicata e separata dal resto dell'infrastruttura di rete.

Un Network IDS poichè in grado di raccogliere informazioni direttamente a livello di rete può rilevare tentativi di attacco che si basano sulla manipolazione delle intestazioni dei pacchetti trasmessi oppure delle tabelle che mantengono informazioni di rete (ad es. tabelle ARP).
Una intrusione può essere rilevata a seguito di un pattern di attacco noto oppure a seguito alla registrazione di un numero troppo elevato di pacchetti "insoliti".

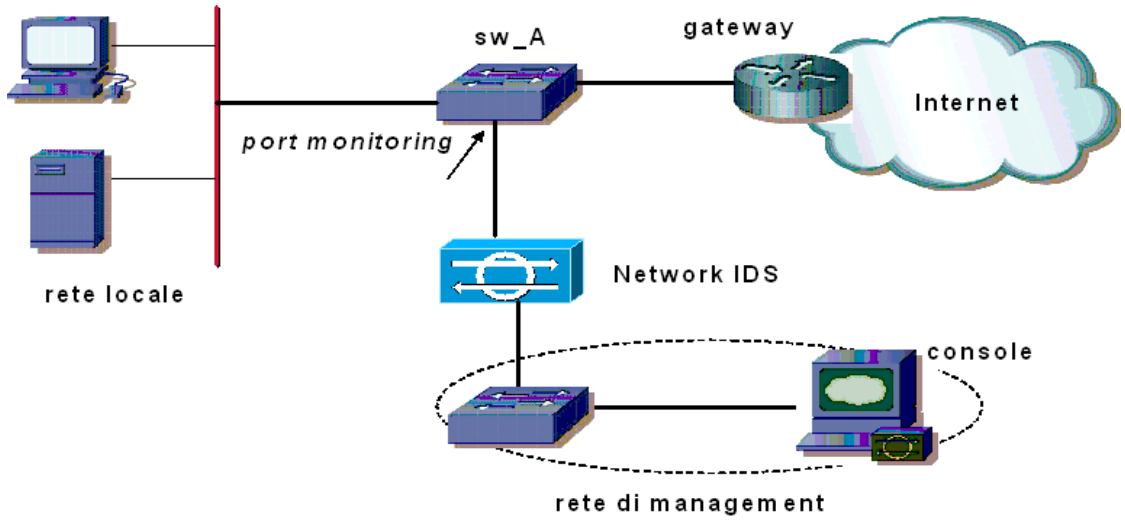
L'azione associata a tale evento risulta una trap o altro messaggio di segnalazione per l'amministratore di rete, oppure mediante interruzione automatica dell'attacco in corso.

Nel caso di sesioni TCP sospette, il sistema IDS può essere configurato per inviare dei RST ai due partecipanti (server locale e presunto client esterno); per poter effettuare questa operazione è condizione necessaria che la piattaforma IDS possa emulare un'entità IP in condizione ***"man in the middle"*** (è necessario che i pacchetti RST inviati emulino quelli prodotti dai sistemi finali coinvolti).

Nel caso di protocolli di tipo ***stateless*** un'intervento attivo dell'IDS si traduce nella ri-configurazione degli apparato di rete (router, firewall,etc…) imponendo delle politiche restrittive temporanee per bloccare l'inoltro dei pacchetti sospetti.
Comunque l'efficacia del sistema è condizionata alla quantità e qualità delle informazioni raccolte per effettuare l'analisi in tempo reale.

I principali inconvenienti possono nascere da un errato posizionamento della piattaforma IDS e dalla difficoltà di raccogliere tutte le evidenze di un attacco a partire dai pacchetti trasmessi sulla rete.

Inoltre un IDS non è esente da vulnerabilità che possono compromettere le capacità di monitorino; ad esempio attacchi DOS inviati numerosamente come ping flooding, syn flooding…. verso i sistemi presenti sulla rete locale. Un IDS è chiamato a gestire l'attacco secondo quanto configurato dall'amministratore e può essere indotto a consumare una quota significative delle proprie risorse per la sola registrazione di questo eventi ripetuti.
Un'altra limitazione può essere la non conoscenza della natura dei sistemi operativi che sono chiamati a proteggere.


sw_A
gateway
Internet
port monitoring
Network IDS
rete locale
console
rete di management