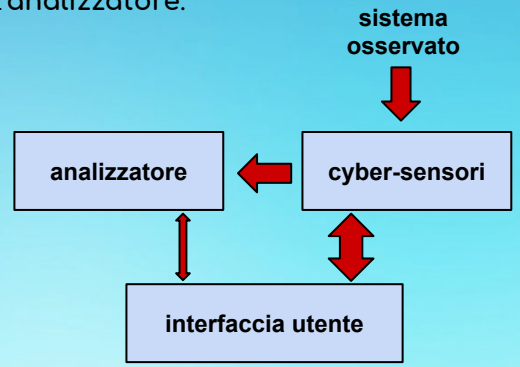
TECNOLOGIE DI RILEVAMENTO DI INTRUSIONI

Sono essenzialmente 3 le tecnologie di "*detection*" - rilevazione - che gli **IDPS** (*Intrusion Detection and Prevention Systems*) utilizzano in maniera combinata per fornire un maggior grado di accuratezza.

- **Signature-based**: in questo caso gli **IDPS** effettuano una comparazione fra le firme (o "*signatures*"), note e gestite tramite apposite regole dall'amministratore di rete, ed i pacchetti in transito. Sono molto efficaci nell'individuare minacce note che hanno un "pattern di attacco" statico ma sono quasi inutili nei confronti di minacce non note. L'analisi basata sulle firme non è inoltre in grado di tenere sotto controllo lo stato delle comunicazioni nel flusso di rete.
- **Statistical anomaly-based detection**: avendo a disposizione dati statistici riguardo i flussi di rete reputati normali, gli **IDPS** avvertono situazioni fuori dalla norma sulla base di quanto, determinati parametri, "deviano" dai propri valori standard. Questo metodo di "*detection*" necessita di una fase preliminare di studio della rete per stabilire quali sono i valori normali. Se in questa fase di taratura sono però già in corso attacchi o situazioni anomale, questi produrranno una definizione di stato normale di rete errata, portando in futuro a casi di falsi positivi o a ritenere innocue situazioni pericolose.
- **Stateful protocol analysis**: tecnologia in cui gli **IDPS** analizzano il flusso di rete, comparandolo con appositi profili che contengono azioni normalmente reputate non nocive nel contesto di specifici protocolli (detti *stateful protocols*). Questo tipo di analisi è molto sofisticata ma è al contempo molto difficile produrre profili per ogni protocollo, che comprendano tutti gli scenari possibili d'uso, leciti e non leciti.

LO SCENARIO NEI SISTEMI DI RILEVAMENTO DI INTRUSIONI

Nello scenario degli **IDPS** (*Intrusion Detection and Prevention Systems*) si hanno due entità principali (oltre al sistema osservato e all'interfaccia utente per riferire i dettagli dell'analisi), e sono: i "**cyber-sensori**" e l'**analizzatore**.



I "**cyber-sensori**", cioè macchine su cui sono in esecuzione i software di IDS / IPS, agiscono direttamente sul sistema osservato. Essi monitorano il traffico, analizzano la rete e riferiscono le statistiche misurate all'analizzatore.

L'**analizzatore** è un software che opera sul principio base del **test delle ipotesi**, secondo il quale l'amministratore della rete deve "tarare" il sistema per accettare un certo tasso di fallimento della rilevazione di minacce.

L'amministratore di rete usa l'interfaccia utente per comunicare per lo più con l'analizzatore, ma la può anche usare per controllare direttamente i sensori e configurare il sistema.

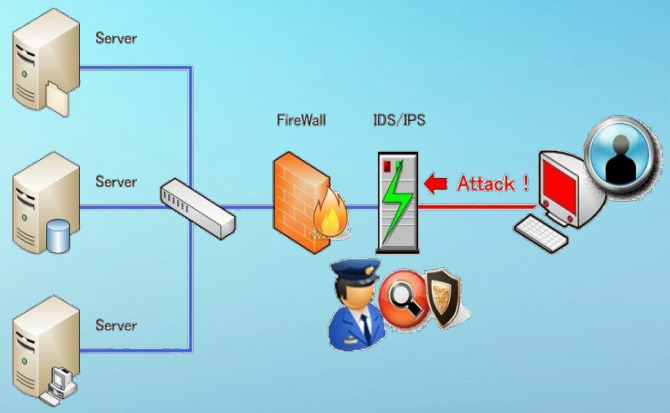
RIFERIMENTI

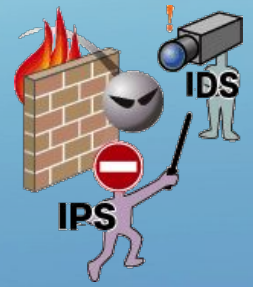
➢ https://www.c3t.it/projects/awareness/articoli&brochure/ids_ips/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

PREVENZIONE E RILEVAMENTO DI INTRUSIONI

Scopri cosa sono gli **Intrusion Detection and Prevention System** e come agiscono nella tua rete per proteggerti.





Intrusion Detection Systems

L'acronimo **IDS** sta per *Intrusion Detection System* (sistema di rilevamento di intrusione) e si riferisce ad una componente, hardware o software, atta ad analizzare il traffico in transito da e verso una specifica rete entro la quale viene installata.
Lo scopo di disporre un IDS in una rete è quello di monitorare il traffico al fine di rilevare eventuali attività sospette e/o malevole nei confronti di un qualunque componente della rete.

Intrusion Prevention Systems

L'acronimo **IPS** sta per *Intrusion Prevention System* (sistema di prevenzione di intrusione); come l'IDS, un sistema di prevenzione è una componente hardware o software disposta all'interno di una rete. Tuttavia, lo scopo di un IPS non è quello di tenere sotto controllo il flusso dei dati da e verso la rete in cui esso è collocato, ma quello di prevenire tentativi di attacco o movimenti sulla rete potenzialmente pericolosi per l'incolumità dei dispositivi che ne fanno parte.

IDS ed **IPS** sono tecnologie complementari nell'ambito della sicurezza delle reti e sono in grado di lavorare in sinergia. Entrambe sono accomunate dall'analisi del traffico di rete ed entrambe entrano in funzione sulla base del "*matching*" fra determinate regole fornite dall'amministratore di rete ed i pacchetti in transito. Proprio per questi motivi, diversi software implementano sia la funzione di **detection** che di **prevention** in un unico sistema, dando così origine a prodotti ibridi noti con l'acronimo di **IDPS** o *Intrusion Detection and Prevention System*.

Tipologie di Intrusion Detection and Prevention Systems (IDPS)

1. Network-Based IDPS

Monitorano il traffico, con particolare riguardo ai livelli di applicazione e di rete del **modello OSI** (*https://it.wikiped-ia.org/wiki/Modello_OSI*), in specifici segmenti della rete. Tipicamente i Network-Based IDPS vengono installati ai limiti topologici della rete, per esempio in prossimità dei **firewall** che antecedono i *gateway* (o porte di accesso) per altre reti o per Internet.

2. Wireless IDPS

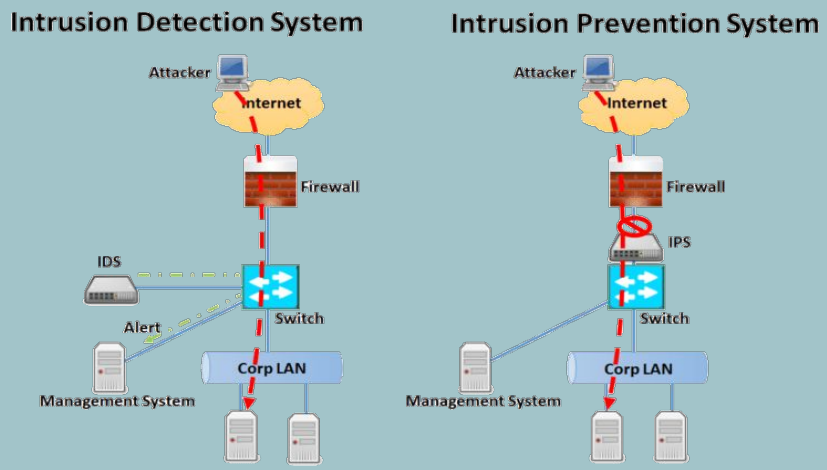
Monitorano il traffico wireless ed esclusivamente ciò che riguarda i protocolli di rete wireless. Non agiscono a livello applicativo o di rete.

3. Network Behaviour Analysis (NBA) IDPS

Esaminano il traffico per identificare minacce che generano traffico non comune per una rete, come nel caso di tentati attacchi **DDoS** (*Distributed Denial of Service*), in presenza di **malware** o violazioni di policy. Vengono spesso impiegati per monitorare il traffico interno alle stesse reti, o nel caso in cui si voglia rendere disponibile l'accesso alla propria rete da parte di terzi.

4. Host-Based IDPS

Monitorano tutto ciò che accade all'interno del singolo host su cui vengono installati. L'host su cui vengono installati è in genere un server accessibile dall'esterno della rete o un client di accesso pubblico.



Il contesto generale di utilizzo di questi **sistemi di intrusione e prevenzione** è quello aziendale. Il possesso ed il trattamento di dati sensibili da parte di aziende e organizzazioni, impone loro che vengano adoperati opportuni ed efficaci sistemi di sicurezza nelle loro reti interne onde evitare violazioni delle policy di sicurezza aziendali. Le tecnologie **IDPS** si vanno dunque ad affiancare (e mai a sostituire) ad altre tecnologie di sicurezza informatica quali **firewall** ed **antivirus**.