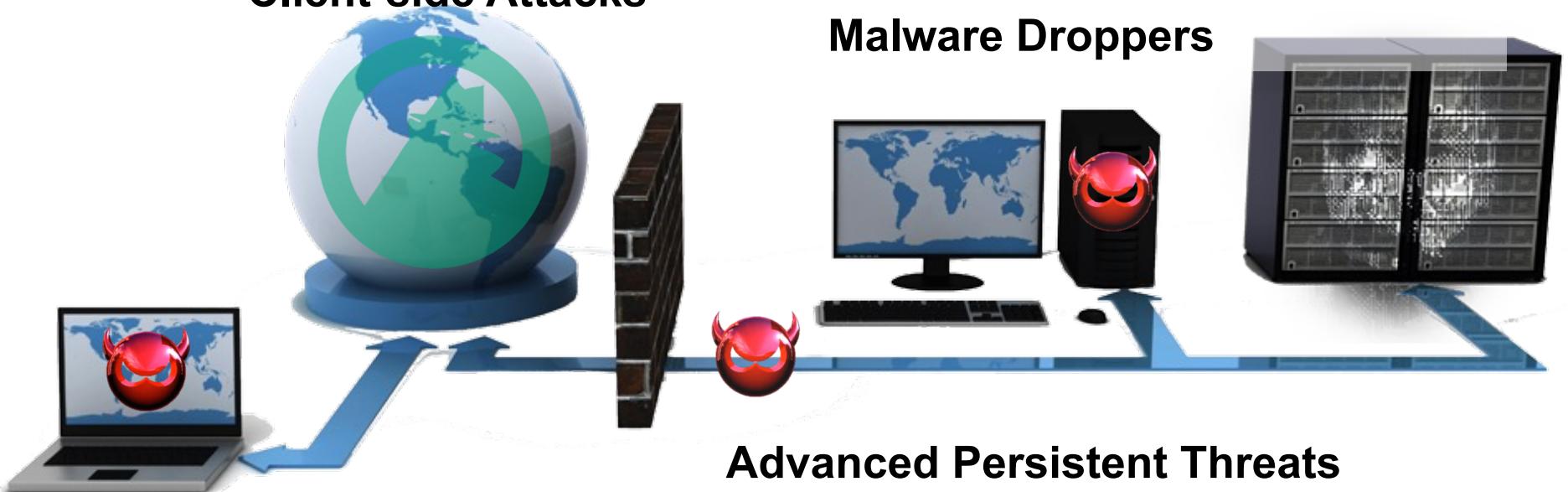


# **Next Generation Firewalls e Intrusion Detection Systems**

# Aumenta la complessità delle minacce

**Client-side Attacks**



**Malware Droppers**

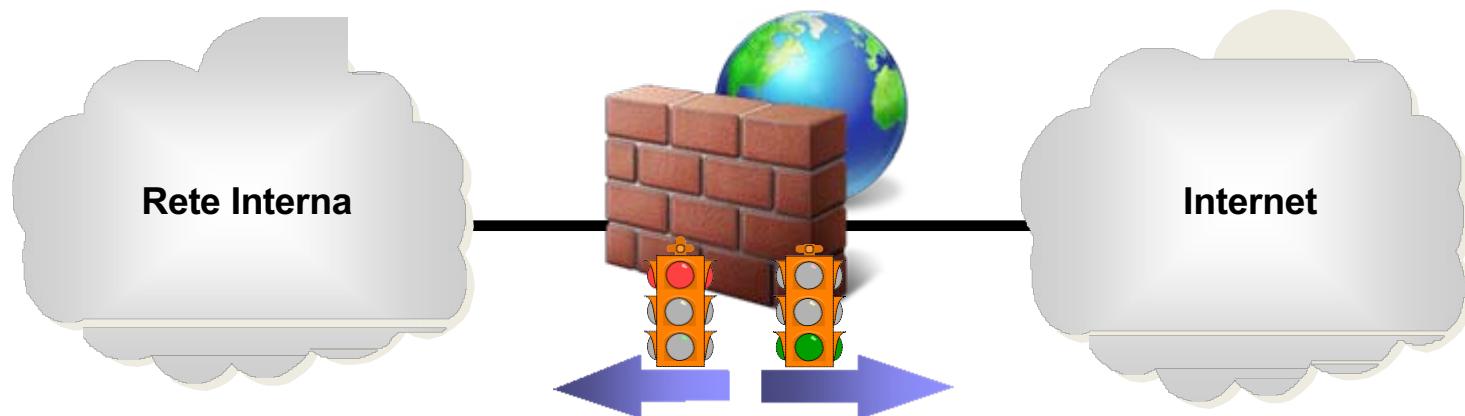
Attacchi sofisticati, ben finanziati e motivati, con serie ripercussioni socio-economiche e geopolitiche

# Limiti dei Firewall tradizionali

- Non protegge da virus e trojan
- Non protegge da attacchi nuovi (sconosciuti)
- Non protegge da connessioni che non lo attraversano (backdoor modem, HSDPA etc.)
- Non protegge da cattive o inesistenti policy
- Non protegge da attacchi interni (75%-80%)
- Non protegge da attacchi fisici
- **Non può fungere da unico punto di difesa**

# ACL e modello “fortezza”

- Sparisce il concetto di sicurezza totalmente (ed esclusivamente ) fondato su screening firewall posti sul bordo esterno della rete
- Le sole ACL diventano **poco flessibili** per definire le politiche di sicurezza



Filtraggio statico per porta di Protocolli:  
DNS (UDP/53), SMTP (TCP/25) , HTTP (TCP/80), FTP (TCP/21)

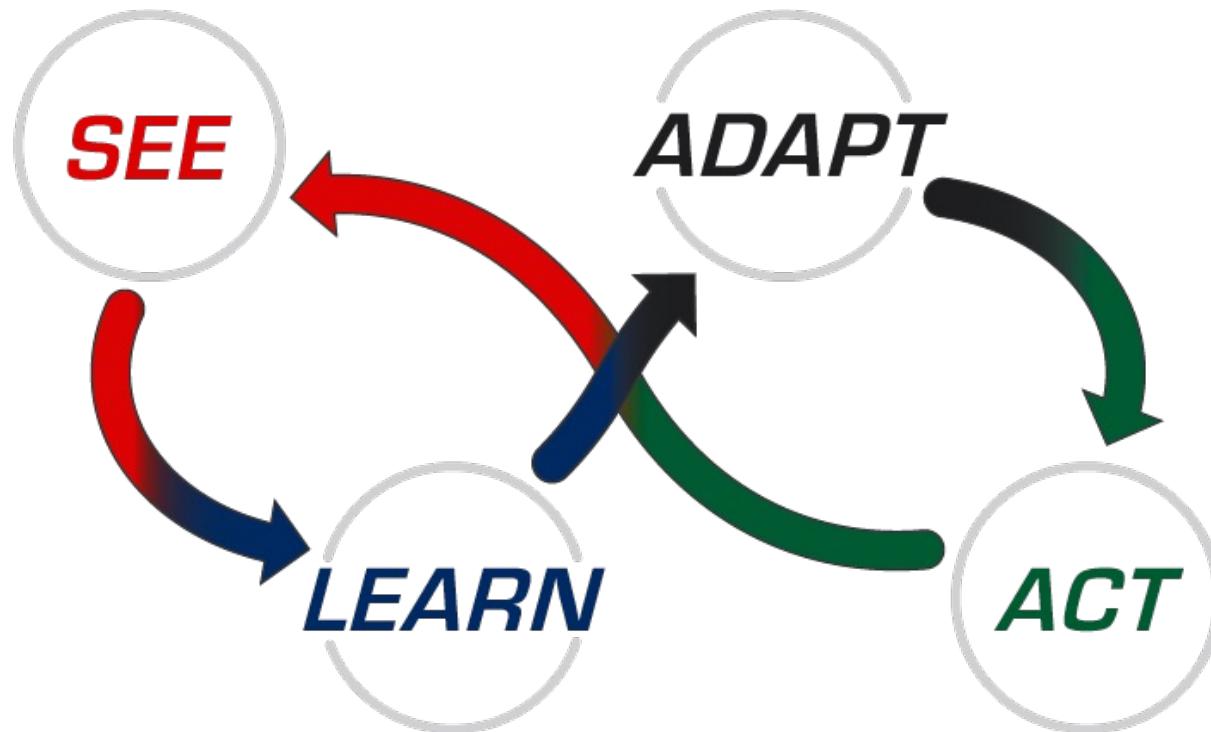
# Il filtraggio per porta non basta

- Non è più possibile applicare politiche di filtraggio basate su **parametri statici** del pacchetto IP o TCP/UDP



- Port  $\neq$  Applicazione (protocol obfuscation)
- IP address  $\neq$  Origine (IP spoofing)
- Payload  $\neq$  Contenuto (Encryption)

# Nuove necessità: Agile Security



...un processo in continua evoluzione per rispondere a cambiamenti continui.

# Difficile proteggere ciò che non vedi

- Ampiezza: chi, cosa, dove e quando
- Profondità: acquisire quanti più dettagli possibile
- Real-time data
- Visibilità completa concentrate in un punto solo



Threat



Device



Applications



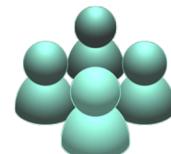
Network



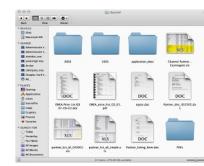
Vulnerabilities



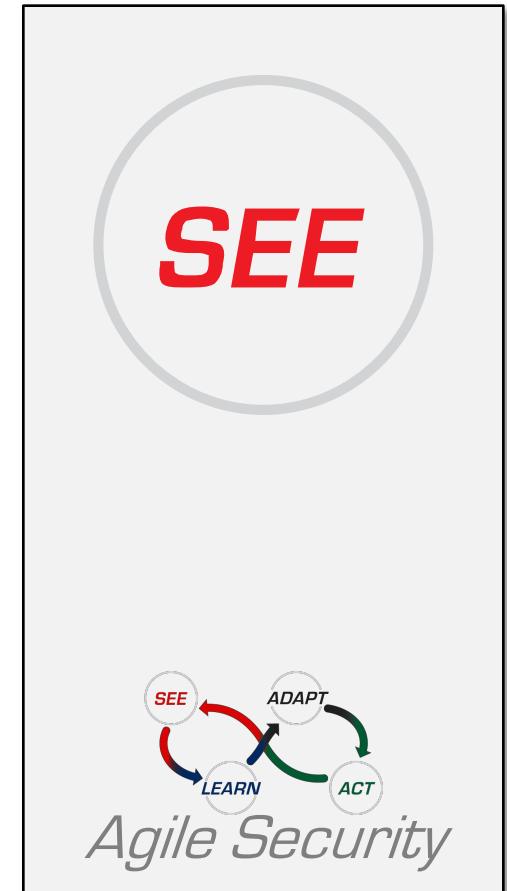
OS



Users



Files



La “Visibilità” garantisce il vantaggio della consapevolezza

# **LEARN**

- Ottieni informazioni dettagliate sulla realtà del tuo assetto IT e di sicurezza
- Diventa più intelligente applicando l'AI
- Correlare, dare priorità, decidere



# **ADAPT**

- Ottimizza automaticamente le difese
- Proteggiti in base alle norme
- Sfruttai vantaggi delle larchitetture aperte
- Misure e strategie di sicurezza su misura



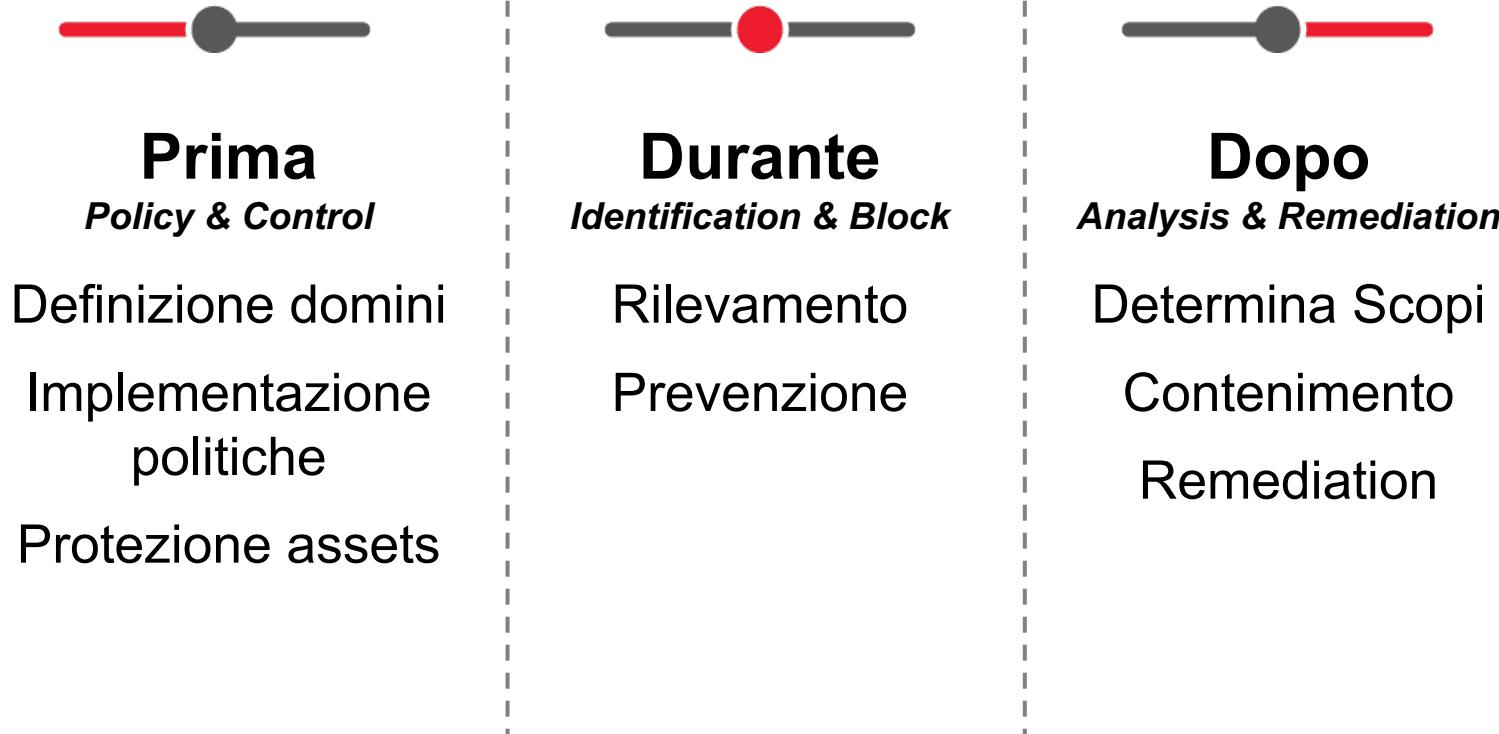
# **ACT**

- Blocca, avvisa, traccia, metti in quarantena, correggi
- Rispondi tramite automazione
- Riduci il "rumore"



**Strategia chiave: intelligenza & automazione**

# Sicurezza prima, durante e dopo gli attacchi

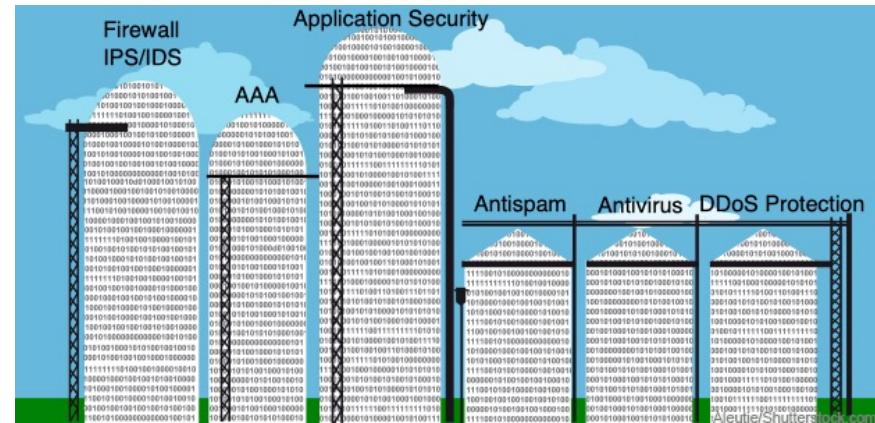


# Current trends

- E' necessario che i firewall si evolvano per essere più proattivi, bloccare i nuovi attacchi e fornire un controllo maggiore.
- Le aziende dovrebbero aggiornare i loro firewall e i sistemi di Intrusion Prevention per proteggere il sito e le attività di business, perché gli attacchi divengono sempre più sofisticati.
- Come potrebbe essere un Next-Generation Firewall?
- Il primo passo sostanziale è l' integrazione fra le funzionalità di firewall tradizionale (di prima generazione) e quelle di Intrusion Prevention. Inoltre tale sistema dovrà essere in grado di governare l' implementazione e l' applicazione delle policy di sicurezza anche a fronte dei cambiamenti nel modo di lavorare (es web 2.0) e nel modo in cui gli attacchi compromettono i sistemi.

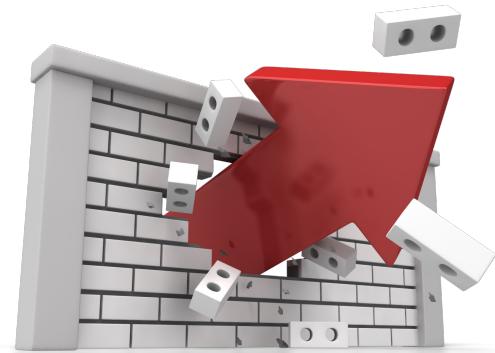
# Il problema: Siloed Security

- Nelle attuali organizzazioni coesiste un'eterogenità di sistemi e prodotti (spesso anche ridondanti) e approcci diversi alla sicurezza
  - Security Endpoints, Antivirus, antispyware,
  - Firewall, honeypot, Intrusion Detection System, Intrusion Prevention System, sistemi crittografici, sistemi di autenticazione
  - Soluzioni di backup o per resilienza/affidabilità
- Responsabilità differenziate
  - ognuno gestisce un pezzo di sicurezza
- Soluzioni integrate in tempi diversi
- Obiettivi di gestione diversi:
  - funzionamento delle reti e dei server
  - controllo accessi
  - operatività applicazioni etc.
- Limitata Interoperabilità
  - Soluzioni/interfacce legacy
  - Mancanza di standard



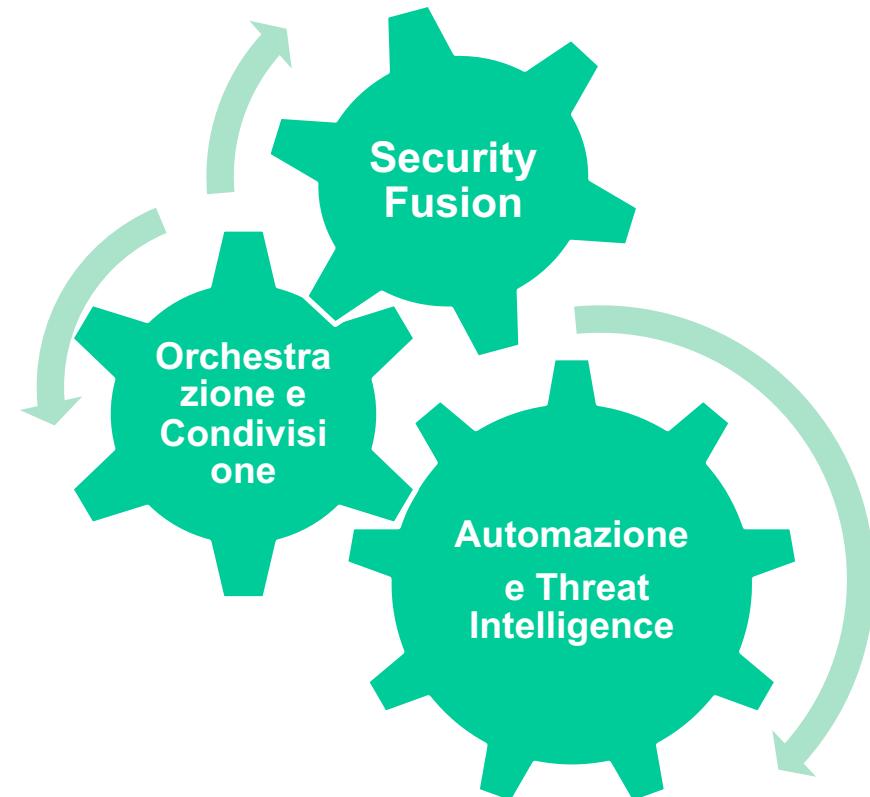
# Cambiare Vision e Approccio

- Bisogna partire da una nuova visione architetturale:
  - perimetro liquido
    - o fine concetto sicurezza perimetrale
  - utenti mobili
  - connettività ubiqua e erogata da soggetti multipli
    - o Scomparsa reti proprietarie
    - o Combinazione di fornitori accesso (e.g. 5G)
  - dati e applicazioni delocalizzati in cloud
    - o Problemi di sovvergnity
    - o Limitazioni capacità di intervento
- Approccio olistico e collaborativo alla sicurezza
  - **Consapevolezza** dei rischi e minacce
  - **Integrazione** fra sistemi di sicurezza
  - **Condivisione** informazioni per migliorare la visio
  - **Cooperazione** per un azione coordinata più efficace



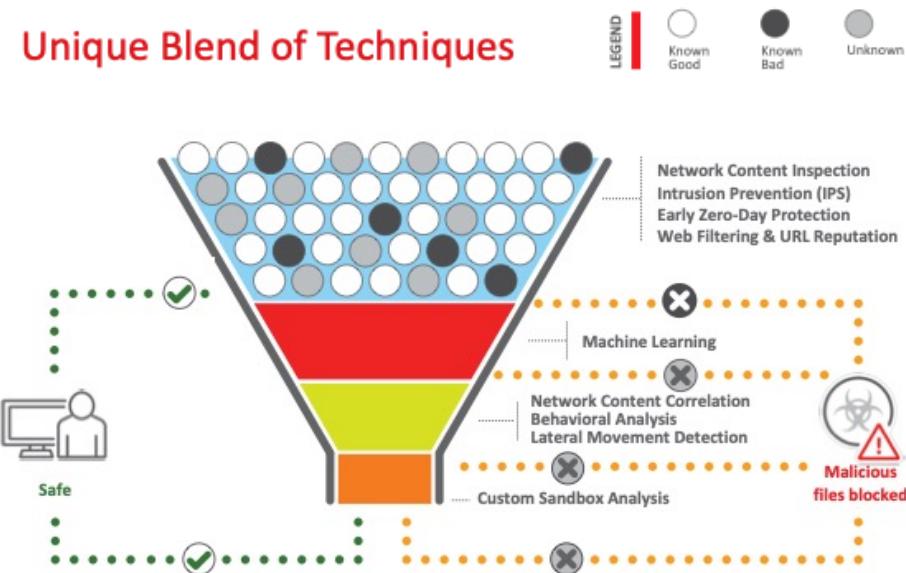
# Security by Design

- Concetto di sicurezza nativa, partendo dalle infrastrutture di rete e dagli oggetti connessi
  - Architetture e applicazioni vanno progettate ab inizio per offrire garanzie di sicurezza
  - Servono standard e interfacce comuni per garantire l'interoperabilità fra sistemi
  - L'integrazione fra prodotti deve avvenire attraverso l'utilizzo di API open
  - Va migliorata capacità di reazione attraverso principi di coalizione quali condivisione e correlazione di conoscenza
- **Security Fusion**
- **Orchestrazione e Condivisione**
- **Automazione e Threat Intelligence**



# Security Fusion

- Consolidamento di multipli componenti funzioni in una singola entità decisionale del punto di vista di gestione della sicurezza
  - Operazioni più coordinate ed efficienti
  - Tempi di reazione più veloci
  - Ogni computer, applicazione, agent, dispositivo, diventa un sensore connesso in grado di fornire informazioni utili alla sicurezza
- Integrazione funzioni gestionali e gruppi di lavoro
  - SoC,
  - NoC,
  - Application Security,
  - Developers



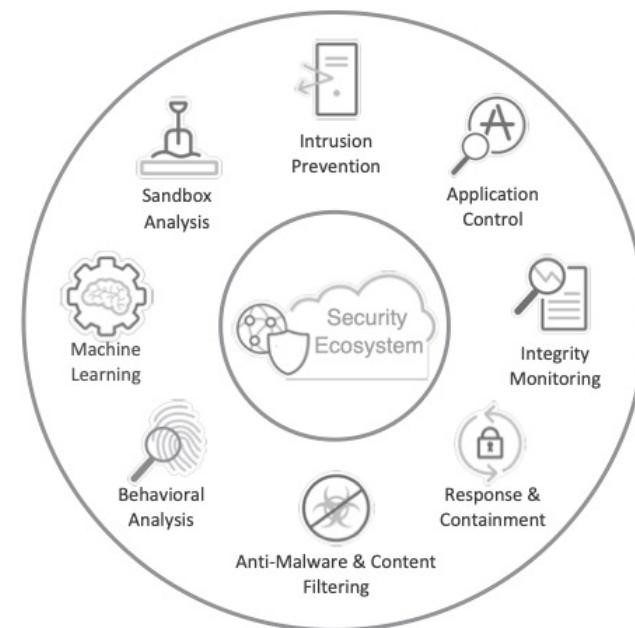
# Orchestrazione e Condivisione

- **Ecosistema di protezione** in grado di incrementare le difese in ottica di:
  - prevenzione, bloccare attacchi prima che raggiungano gli asset vulnerabili
  - identificazione delle minacce per bloccare attacchi prima che raggiungano gli asset vulnerabili
  - aggiornamenti in tempo reale delle contromisure e policy
- La **correlazione** di eventi rende possibile decisioni orientate da **context awareness**
  - visibilità centralizzata e integrata su tutti gli strati di sicurezza fornisce una vista più completa del problema
- Le decisioni nascono da **conoscenza collettiva e condivisa**
  - condividere le informazioni accelera i tempi di risposta
  - le informazioni condivise tra tutti i prodotti e gli ambienti consente una risposta cooperativa



# Ecosistema di Protezione

- **Firewall:** gestione centralizzata dei criteri/politiche di protezione
  - Implementazione politiche controllo accessi
  - Ispezione bidirezionale per filtraggio granulare del traffico
  - tracciamento e logging
- **Intrusion Detection/Prevention:** difesa da vulnerabilità note o zero day
  - Web App Protection e protezione applicazioni legacy
  - Ispezione del traffico per individuazione attacchi o violazione delle policy
  - Copertura vulnerabilità/exploit via Virtual Patching
  - Sandboxing per analisi cooperativa nuove minacce
- **Content filtering & Web Reputation:**
  - Blocco accesso a URL dannosi o contenuti non consentiti
- **Integrity Monitoring:** individuazione in tempo reale di cambiamenti sospetti
  - Monitoraggio sistemi e applicazioni critiche
  - Variazione a policy di sicurezza e controllo accessi
- **Log inspection:** automatizzare l'analisi dei Log e di generazione alert.
  - Ottimizzazione e generazione dinamica regole di filtraggio
  - Interfaccia con i sistemi SIEM
- **Antimalware:** protezione in tempo reale dispositivi e applicazioni
  - Real Time Scan
  - Remediation
- **Application Control:** gestione e controllo applicazioni
  - monitoraggio dell'esecuzione di software sui sistemi controllati
  - Controllo accessi e autorizzazioni via API



# Automazione e Threat Intelligence

- Piattaforme automatizzate che includono anche componenti di intelligenza artificiale per il supporto alle decisioni
  - Machine learning
  - Modelli evolutionary di DSS
  - Sentiment Analysis
  - Anomaly Detection
  - Agenti intelligenti e reazione autonoma
- Introduzione threat intelligence
  - Gestione e reporting degli incidenti
  - Security data Analytics
  - Assessment del rischio
  - Elaborazione modelli predittivi di attacco
  - Definizione strategie e tattiche di sicurezza



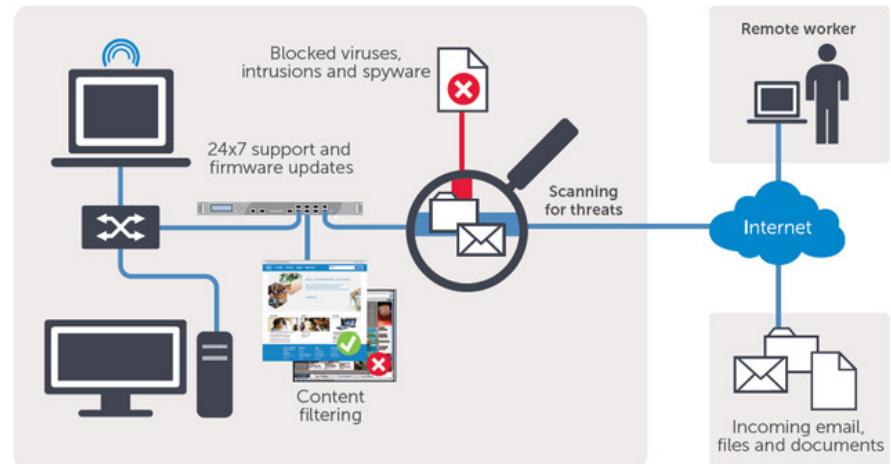
# UTM e Next Generation Firewalls

- Fra i componenti di base dei moderni ecosistemi per la gestione della sicurezza troviamo Next generation Firewall e soluzioni UTM (unified threat management)
- I due componenti non sono poi così differenti come si potrebbe pensare



# UTM

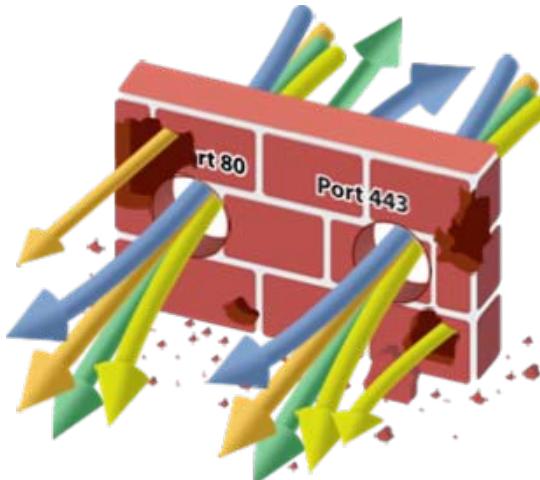
- Il concetto di UTM nasce per le piccole e medie organizzazioni per contenere la complessità dell'architettura di sicurezza
- Solitamente si riferisce a un singolo prodotto con diverse tecnologie di sicurezza integrate (gateway Antivirus, SPAM blocking, URL filtering, Intrusion Prevention, Data Loss Prevention, Reputation Authority, AAA, sandboxing, etc)
- E' semplice da implementare e garantisce tutte le tipiche funzionalità di sicurezza integrate in una sola piattaforma.



# Next Generation Firewalls

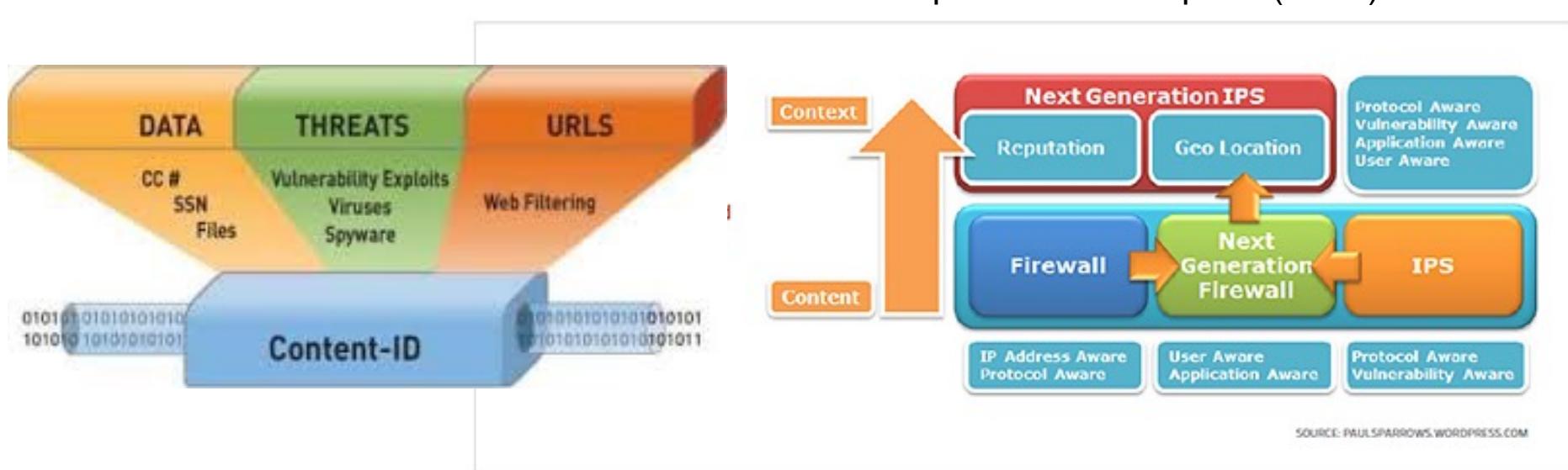
- Indipendentemente dalle dimensioni dell'organizzazione da proteggere può avere senso unificare motori di scansione multipla in una sola box.
- Non è necessario pagare per hardware aggiuntivo, licenze, contratti di manutenzione etc..
- Migliora la possibilità di combattere le attuali minacce multi-vettore
- Piuttosto che gestire strumenti di sicurezza separati, con box/console e policy differenti per ciascuna soluzione, è possibile unificare la gestione della sicurezza.
- La promessa di costi operativi più bassi, unita a livelli di sicurezza maggiori, è ciò che sta guidando la crescita del mercato della sicurezza integrata.

# Next Generation Firewalls



## Caratteristiche di base:

- compatibilità con firewall di prima gen.
  - funzionalità di Intrusion Prevention
  - full stack visibility & management
  - extra firewall intelligence (integrazione con sistemi di monitoraggio esterni)
  - Integrazione con user directories (LDAP, Radius etc.)
  - operatività wire speed (ASIC)



# Funzionalità Fondamentali

- Individuare le risorse più a rischio con informazioni dettagliate sul contesto
- Reagire tempestivamente agli attacchi grazie all'automazione intelligente della sicurezza che consente di impostare le policy e rafforzare le difese in modo dinamico
- Rilevare in modo più efficace le attività evasive o sospette tramite la correlazione degli eventi rilevati su rete e endpoints
- Ridurre notevolmente l'intervallo di tempo tra l'individuazione e l'intervento correttivo con soluzioni di sicurezza retrospettiva che monitorano costantemente la rete per rilevare attività e comportamenti sospetti anche dopo l'indagine iniziale
- Semplificare l'amministrazione e ridurre la complessità grazie a policy unificate che proteggono la rete in tutte le fasi dell'attacco

# Funzionalità Fondamentali

- Bloccare le minacce in tempo reale.
  - Garantire protezione in tutte le fasi di un attacco
  - Intercettare applicazioni pericolose, vulnerabilità, malware, URL ad alto rischio e file con contenuti dannosi.
- Semplificare la gestione dei criteri di filtraggio e delle policy
  - Abilitare le applicazioni in modo sicuro mediante strumenti grafici intuitivi e un editor di criteri/politiche di sicurezza
- Creare un perimetro logico.
  - Proteggere tutti gli utenti, fissi e mobili con una protezione uniforme in grado di estendersi dal perimetro fisico al perimetro logico
- Combinare HW e SW realizzati ad hoc per permettere performance multi-gigabit e bassa latenza

# Funzionalità Fondamentali

- Identificare le applicazioni, non le porte
  - Identificare la natura dell'applicazione, indipendentemente dal protocollo, dal tipo di cifratura oppure da tattiche evasive
  - utilizzare l'identità come elemento di base di tutti i criteri di sicurezza.
  - Identificare gli utenti, non gli indirizzi IP
  - Utilizzare le informazioni sugli utenti e sui gruppi provenienti dalle directory aziendali per:
    - acquisire visibilità,
    - creare criteri,
    - generare report
    - eseguire indagini forensi

# Stateful Inspection

## Traditional Applications

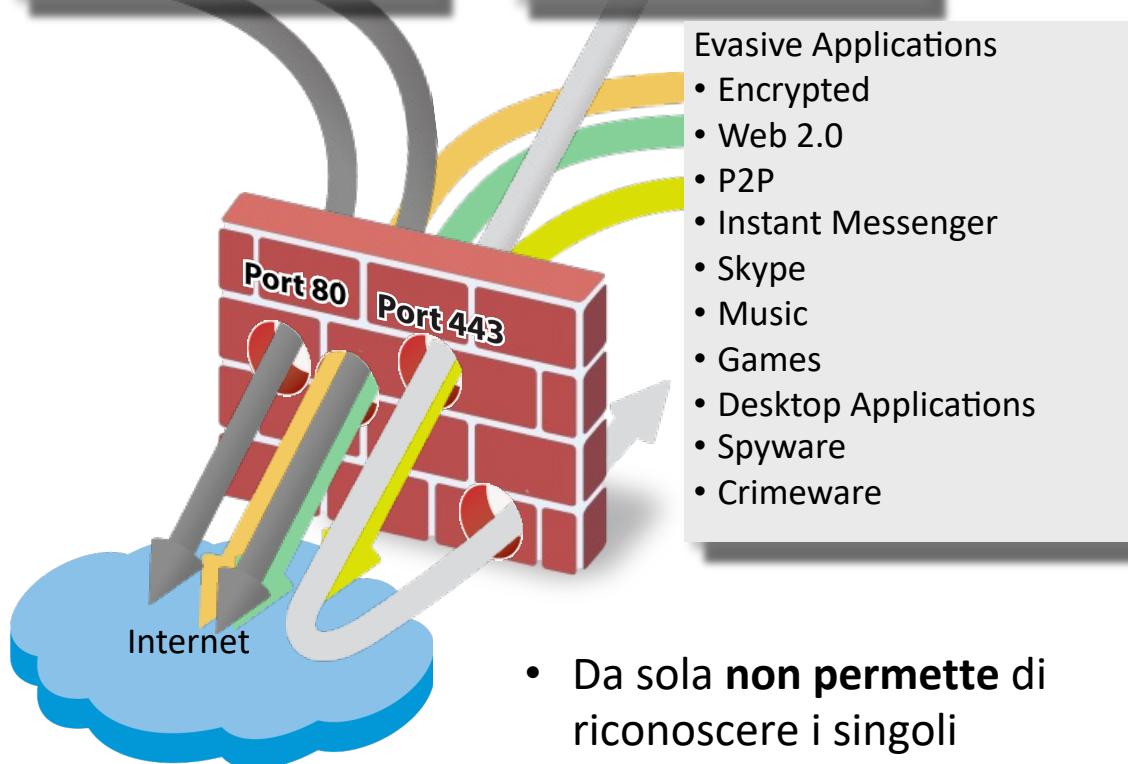
- DNS
- SSH
- SMTP
- HTTP

## Dynamic Applications

- FTP
- RPC
- Java/RMI
- Multimedia

## Evasive Applications

- Encrypted
- Web 2.0
- P2P
- Instant Messenger
- Skype
- Music
- Games
- Desktop Applications
- Spyware
- Crimeware



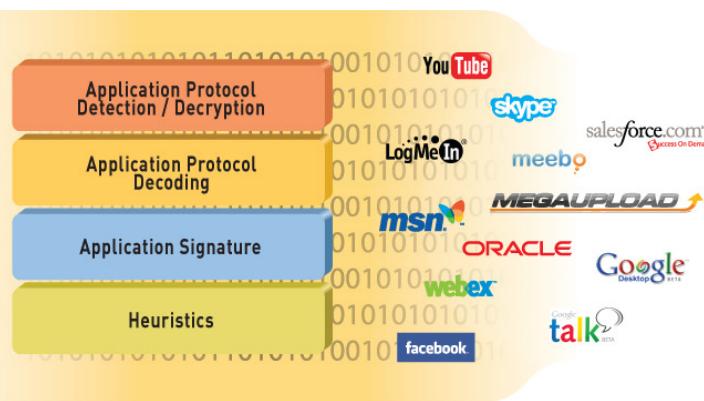
- Da sola **non permette** di riconoscere i singoli protocolli in presenza di tecniche di **offuscamento** o **evasione**

- IL FW tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP, permettendo ad esempio di riconoscere pacchetti TCP malevoli che non fanno parte di alcuna connessione.
- I firewall di questo tipo sono in grado anche di analizzare i protocolli che aprono più connessioni (ad esempio FTP), inserendo nel payload dei pacchetti informazioni di livello rete e trasporto

# Advanced (Deep) packet inspection

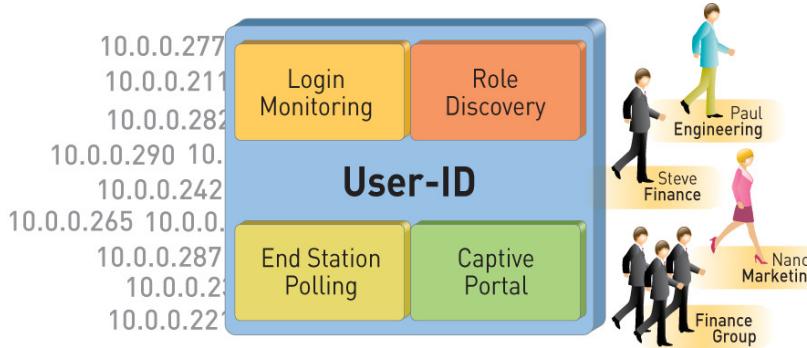
## **Riconoscere le applicazioni**

identificare le applicazioni e consentirle, bloccarle o limitarle in banda indipendentemente da porta, protocollo, codifica o qualsiasi altra tattica di elusione



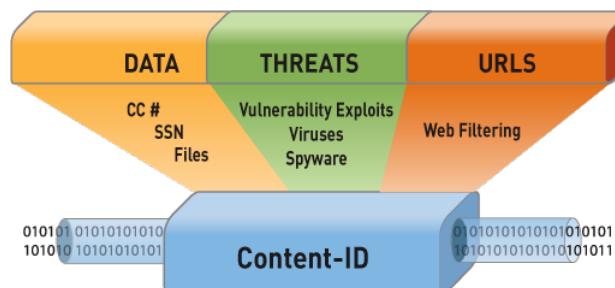
## **Identificare gli utenti**

indipendentemente da dispositivo o indirizzo IP, garantendo il controllo granulare delle applicazioni da parte di specifici utenti o gruppi di utenti e host per controllare i tipi di traffico a cui è consentito entrare e uscire dalla rete.



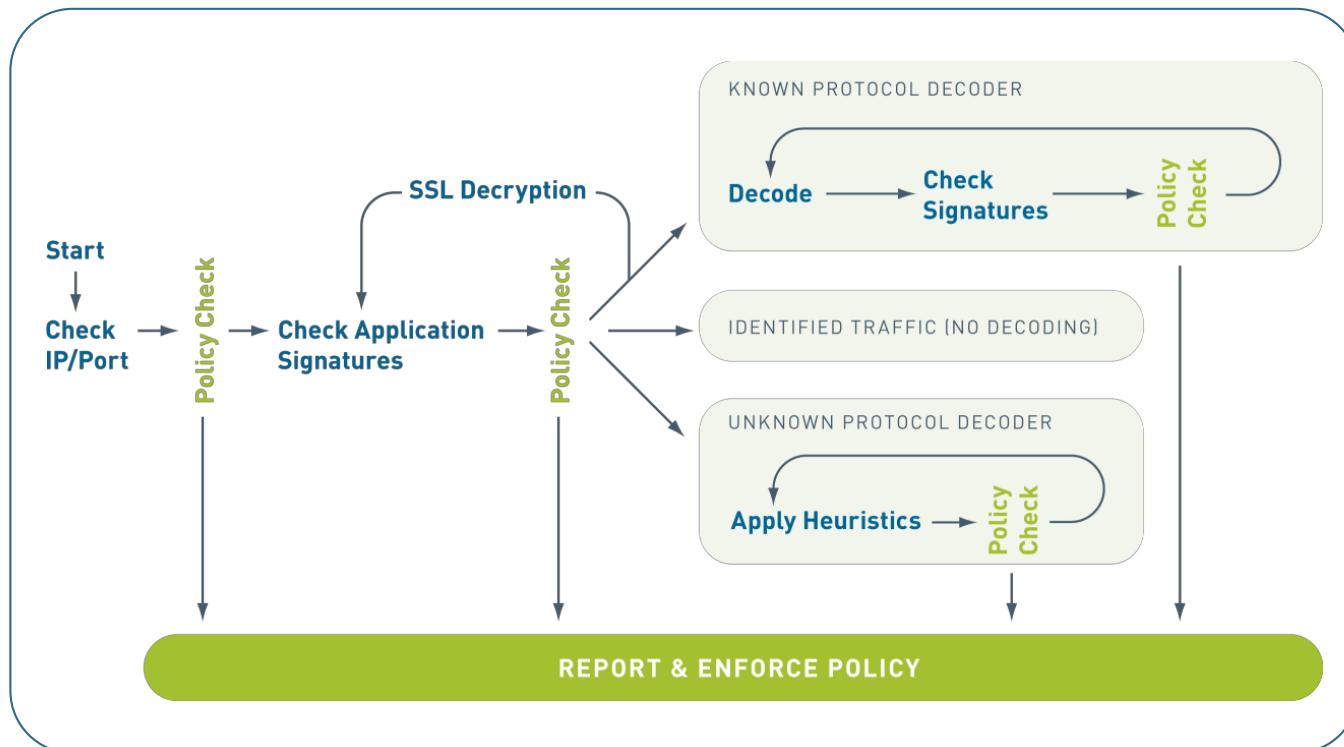
### ***Ispezionare e cercare contenuti***

Filtraggio avanzato dei contenuti per evitare accessi a siti inappropriate, ridurre le infezioni da malware, proteggersi dagli exploit più comuni etc.



# Come funziona?

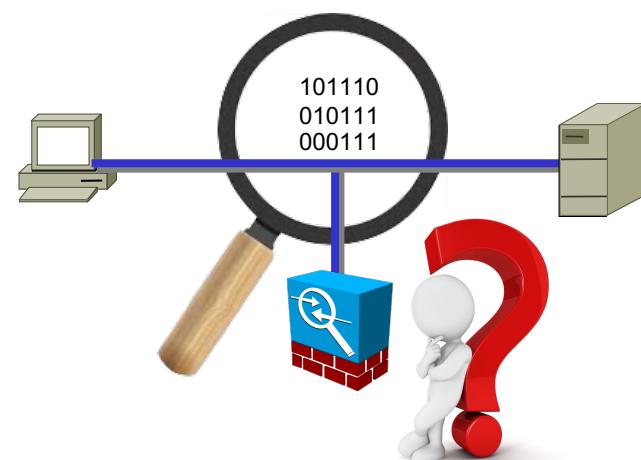
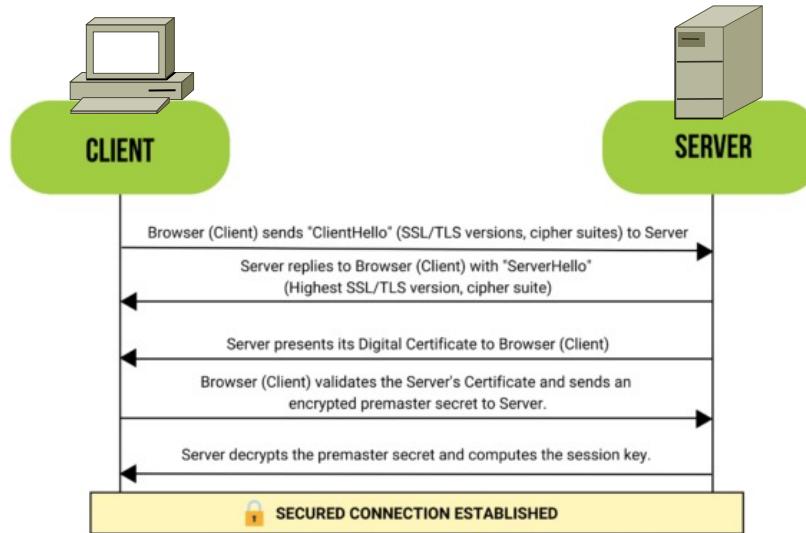
- Built-in intelligence e conoscenza dei protocolli e delle minacce
- Supportate da tecniche di decodifica avanzata e metodi euristici
- Potenziale uso di tecniche di AI/ML



Ben più sofisticato di un banale signature matching....

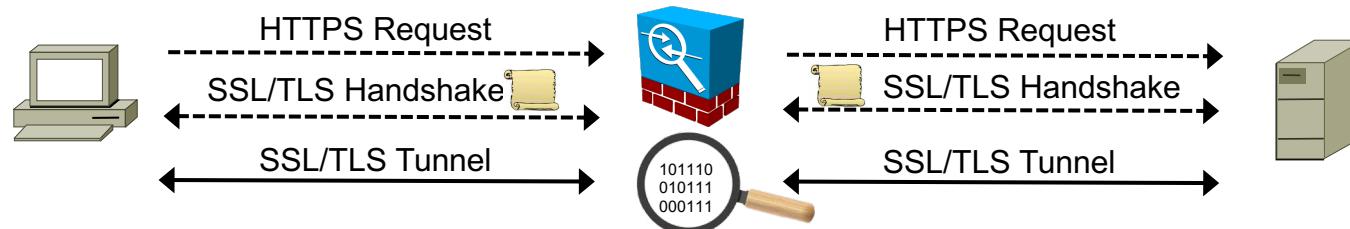
# HTTPS/SSL Inspection

- La maggioranza del traffico web è cifrata attraverso SSL o TLS
  - principalmente usando TLS 1.3 in ragione delle note vulnerabilità MITM di SSL (deprecato)
- I malware utilizzano sempre più frequentemente la crittografia per nascondere i propri exploit
- E' necessario ispezionare a livello NGFW il traffico cifrato per riconoscere eventuale malware ed evitare esfiltrazione
- Per realizzare l'ispezione il FW si introduce nella sessione HTTPS nella logica di un attacco man-in-the-middle



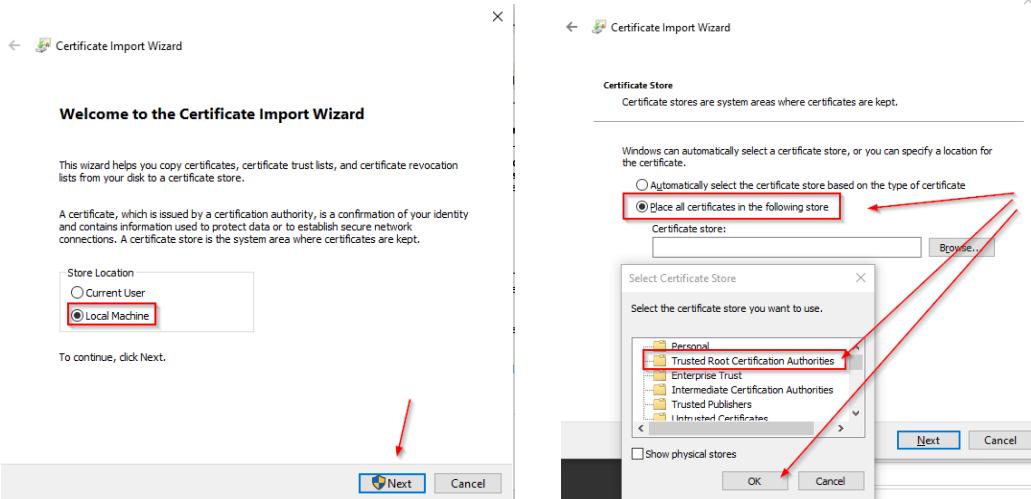
# Le fasi dell'SSL inspection

- Un utente apre un browser e invia una richiesta HTTPS.
- Il FW intercetta la richiesta e in un tunnel SSL/TLS separato, invia la propria richiesta HTTPS al server di destinazione e conduce la negoziazioni SSL/TLS.
  - Il server di destinazione invia al FW il suo certificato con la sua chiave pubblica.
  - Il FW e il server di destinazione completano l'handshake SSL/TLS.
  - I dati dell'applicazione e i messaggi successivi vengono inviati attraverso il tunnel SSL.
- Il FW conduce le negoziazioni SSL/TLS con il browser dell'utente.
  - Invia al browser il certificato intermedio o il root intermedio personalizzato dell'organizzazione, nonché un certificato server firmato da un'autorità di certificazione intermedia che garantisce l'affidabilità del FW.
  - Il browser convalida la catena di certificati nell'archivio certificati del browser.
  - Il FW e il browser completano l'handshake SSL/TLS.
  - I dati dell'applicazione e i messaggi successivi vengono inviati attraverso il tunnel SSL.



# Configurazione SSL Inspection

- Security Profiles -> SSL/SSH Inspection
  - Seleziona “Full SSL inspection”
- Il certificato CA di default è “Fortinet\_CA\_SSL”.
  - Selezionare “Download Certificate”
- Policy and Objects -> IPv4 Policy
  - creare la policy ‘SSL Inspection’,
- Seleziona la policy creata seguita da “Apply” o “Ok”



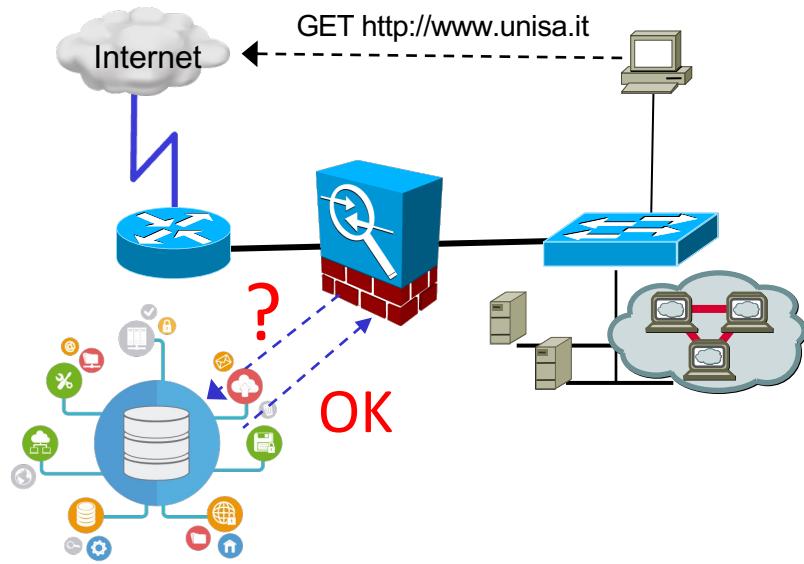
The screenshot shows the 'Edit SSL/SSH Inspection Profile' screen for 'deep-inspection'. The profile is described as a 'Read-only deep inspection profile'.

**SSL Inspection Options:**

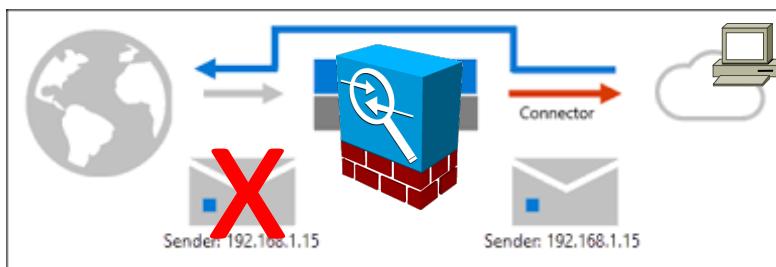
- Enable SSL Inspection of **Multiple Clients Connecting to Multiple Servers** Protecting **SSL Server**
- SSL Certificate Inspection: **Full SSL Inspection**
- CA Certificate: **Fortinet\_CA\_SSL** (selected)
- Untrusted SSL Certificates: **Allow**
- RPC over HTTPS: **Off**

**Policy & Objects** tab is selected in the navigation bar. Under 'IPv4 Policy', the 'SSL Inspection' section is highlighted and set to **deep-inspection**.

# Content filtering

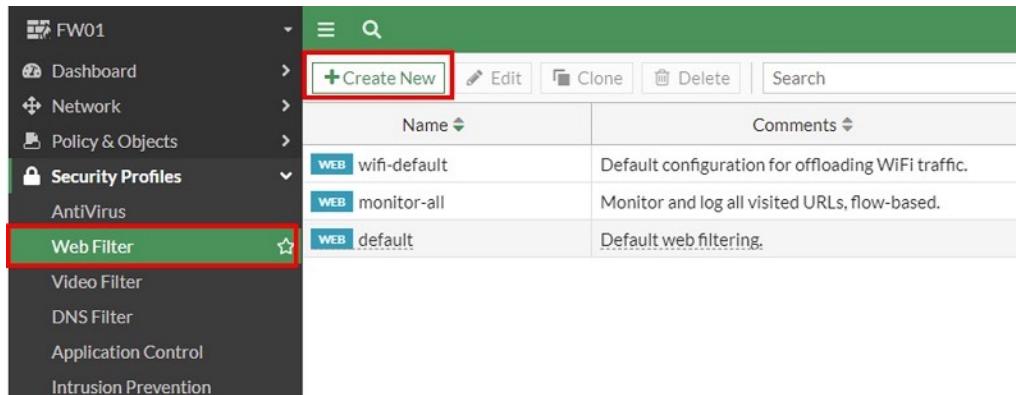


- Filtraggio di contenuti indesiderati, discutibili e dannosi attraverso l'ispezione dei pacchetti
- Richiede l'uso di basi di conoscenza/risorse di terze parti sempre aggiornate:
  - DB di classificazione delle risorse
  - Motori di categorizzazione
- Il firewall esegue l'ispezione del payload e prima di ammettere la sessione verifica il tipo di contenuto rispetto alle politiche locali
  - Es. blocco contenuti relativi a gioco d'azzardo, droghe, generiche attività correlate al crimine
- Il filtraggio può aver luogo anche a livello di
  - URL, accesso a siti WWW
  - risoluzione per domini DNS
  - Contenuti e-mail (attachments, header specifici etc.)
  - Risultati di ricerche a livello di motori specifici
- Il costo di una soluzione dipende dalle funzionalità, dalla qualità e dalla frequenza di aggiornamento del database, oltre che dal numero di utenti che deve servire.



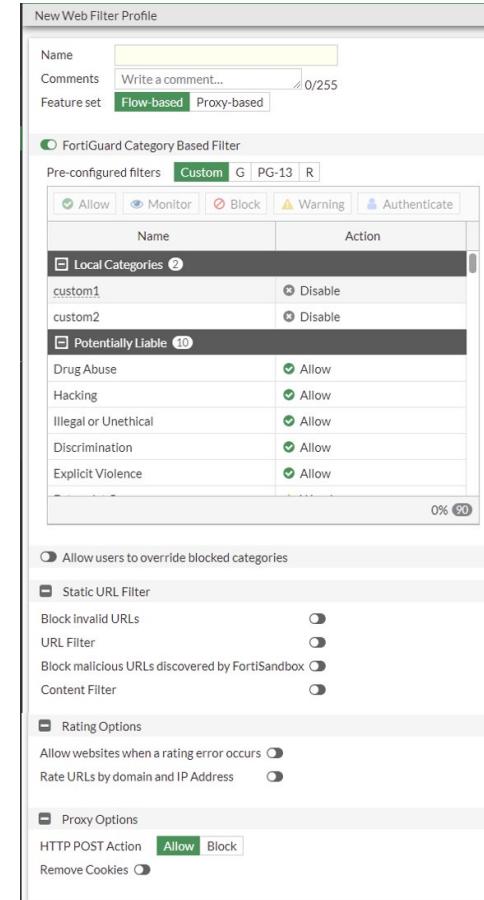
# Web Content Filtering su NGFW

- Di default ci sono 3 web filter profiles:
  - default
  - monitor-all
  - wifi-default
- Security Profiles > Web Filter
  - Creazione nuovo profilo



The screenshot shows the FortiGate management interface. On the left, there's a navigation sidebar with various security profiles like Dashboard, Network, Policy & Objects, AntiVirus, and others. The 'Web Filter' option is highlighted with a red box. Above the main content area, there's a toolbar with buttons for Create New, Edit, Clone, Delete, and Search. The main content area displays a table of existing Web Filter profiles:

Name	Comments
wifi-default	Default configuration for offloading WiFi traffic.
monitor-all	Monitor and log all visited URLs, flow-based.
default	Default web filtering.



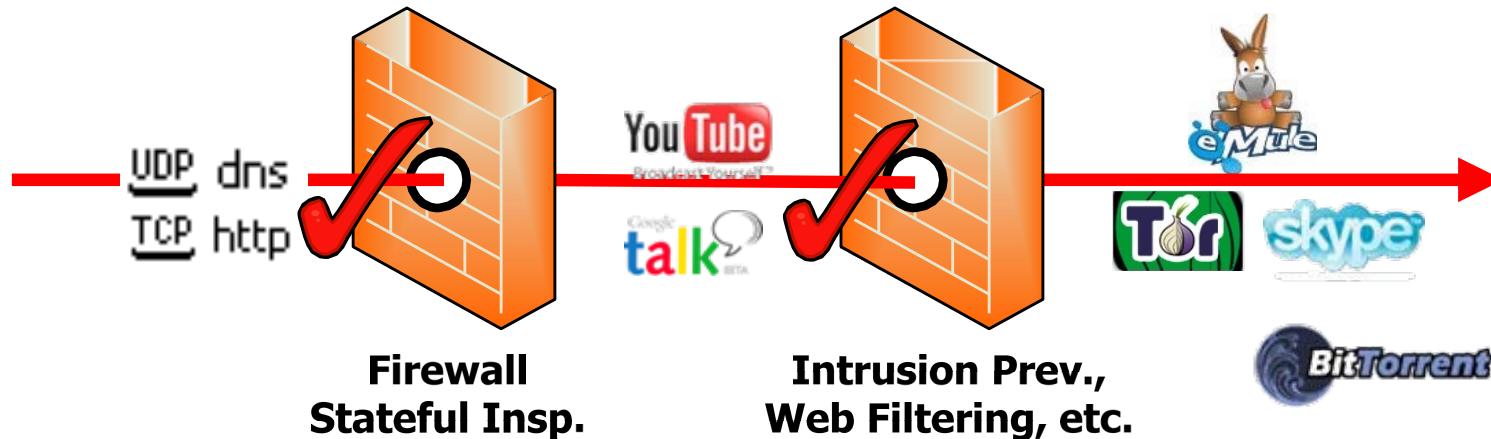
The screenshot shows the 'New Web Filter Profile' configuration dialog. At the top, there are fields for Name, Comments (with a placeholder 'Write a comment...'), and Feature set (set to 'Flow-based'). Below this is the 'FortiGuard Category Based Filter' section, which is expanded. It contains two tables:

Pre-configured filters	
Name	Action
Local Categories	Custom G PG-13 R
custom1	Allow
custom2	Allow
Potentially Liable	10
Drug Abuse	Allow
Hacking	Allow
Illegal or Unethical	Allow
Discrimination	Allow
Explicit Violence	Allow

Below this are other configuration sections:

- Allow users to override blocked categories
- Static URL Filter
  - Block invalid URLs
  - URL Filter
  - Block malicious URLs discovered by FortiSandbox
  - Content Filter
- Rating Options
  - Allow websites when a rating error occurs
  - Rate URLs by domain and IP Address
- Proxy Options
  - HTTP POST Action: Allow
  - Remove Cookies

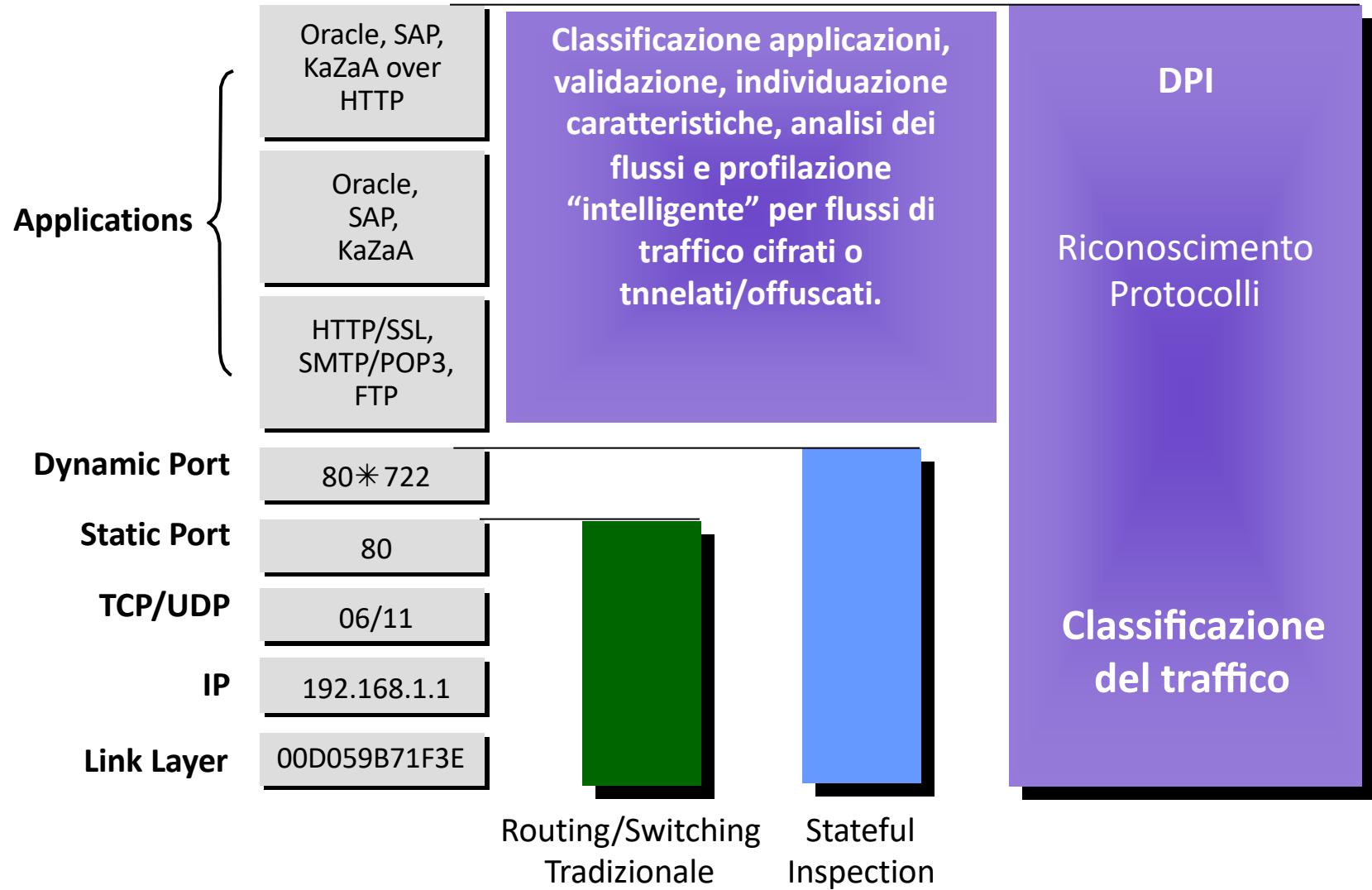
# Classificazione del traffico



Riconoscimento a livello protocollo di specifiche applicazioni

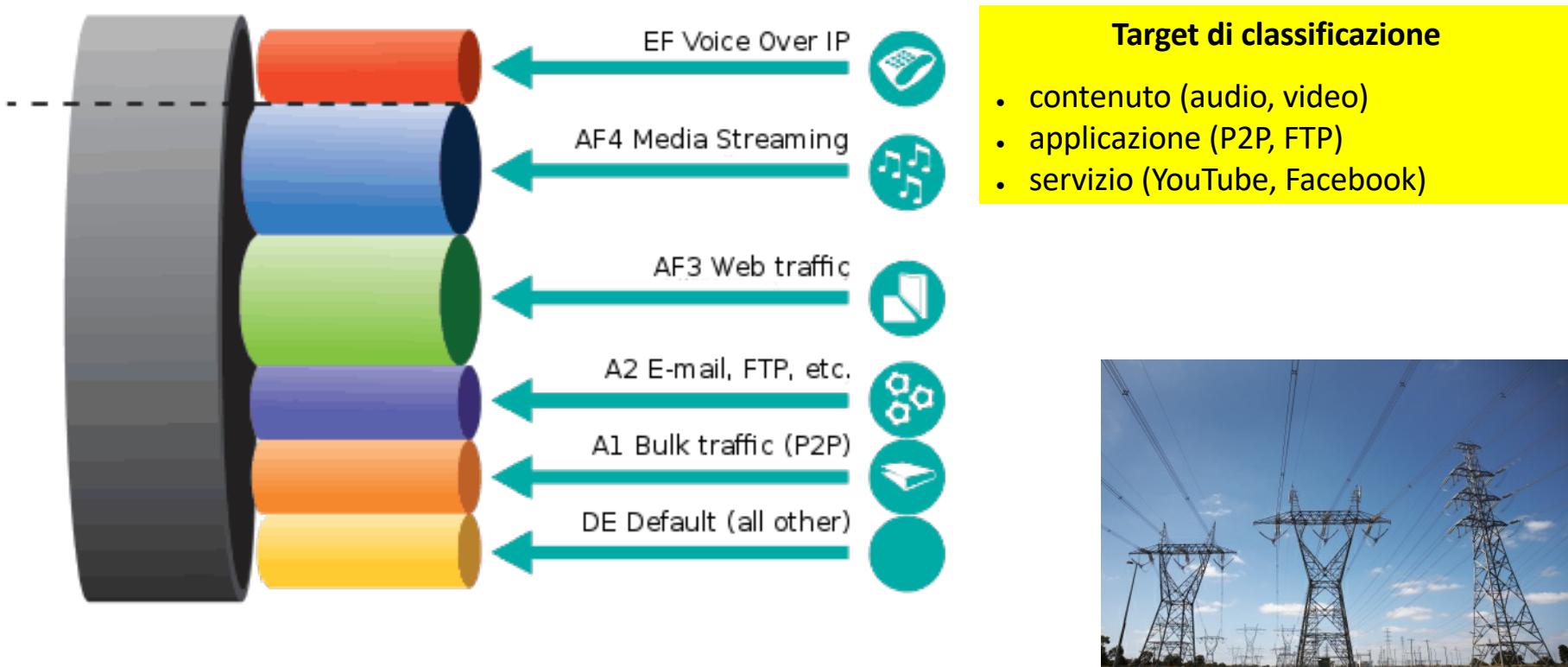
- I NG-firewalls sono in grado di riconoscere diverse applicazioni
- Alcune applicazioni usano meccanismi di protocol obfuscation e transitano indisturbate attraverso i firewalls su porte well-known (es. TCP/80, UDP/53)
- Molte applicazioni (e.g. P2P, Skype, Tor) usano la cifratura e non possono essere individuate attraverso IPS “signatures” e pattern di traffico noti
- E' necessario **classificare** efficacemente i flussi di traffico per riconoscere le applicazioni coinvolte end-to-end. Emerge il concetto di “**classi**” di traffico

# Classificazione dei flussi di traffico



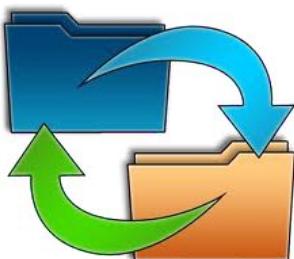
# Obiettivi Classificazione

- Essere in grado di individuare e riconoscere i vari flows nella rete a scopo di implementare politiche di filtraggio o Quality of Service



# Obiettivi Classificazione

- Acquisire conoscenza dei servizi usati maggiormente sulla rete a scopo di performance tuning o creazione di diversioni di traffico

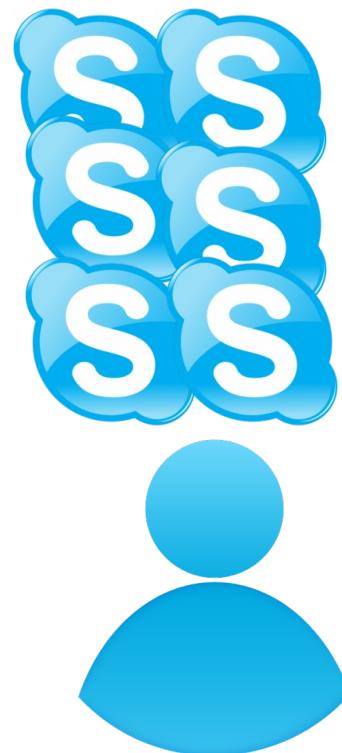


## Esempio

- application (Skype, HTTP)

# Obiettivi Classificazione

- Raggruppare utenti in vari profili (con trattamenti differenziati) in ragione delle applicazioni che utilizzano

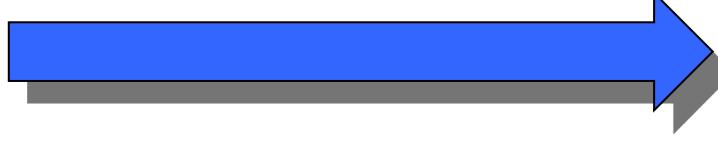


## Our interests

- application (Skype, BitTorrent)
- IP protocol (TCP / UDP)



# Associazione di applicazioni a utenti



# Controllo accessi a livello applicazioni

- Controllo accessi a livello di applicazione
  - “Gli interni possono consultare Facebook, ma solo il Marketing può usarlo attivamente (aggiungere contenuti)”
  - “Nessuno può usare applicazioni di file sharing”



# Classificazione applicazioni su NGFW

## Security Profiles > Application Control

- Associare un trattamento:
  - Monitor
  - Consenti
  - Blocco
  - Quarantena

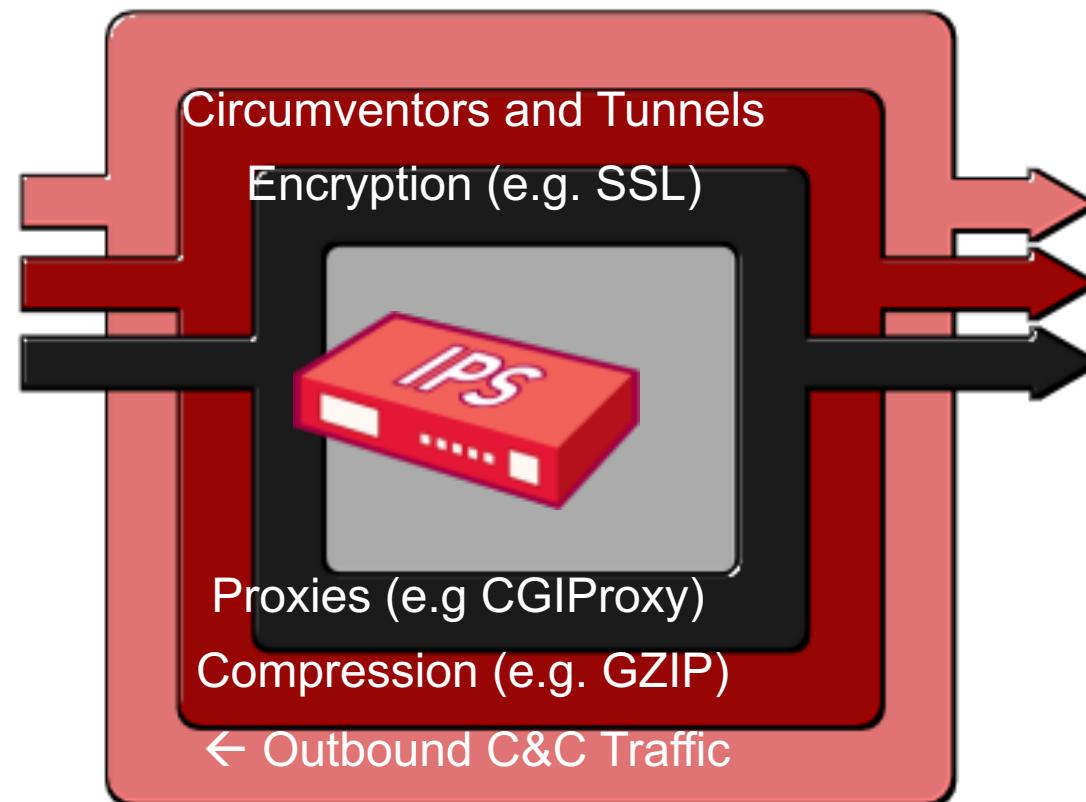
The screenshot shows the FortiGate Application Control interface. On the left, there's a sidebar with various security profiles like Antivirus, Web Filter, and Application Control. The main area has a tree view of application categories: Business, Cloud.IT, Game, Network.Service, Remote.Access, Update, Web.Client, and several others like P2P, Social.Media, Video/Audio, and Unknown Applications. Below the categories is a section for "Network Protocol Enforcement" which is currently disabled. At the bottom, there's a "Create New", "Edit", and "Delete" button, and a link to "View Signatures". A modal window titled "Add New Override" is open, showing a list of applications. The "Facebook" entry is selected, and the "Action" dropdown is set to "Block". To the right of the modal, a "Select Entries" sidebar lists many Facebook-related signatures, such as "Facebook.Application", "Facebook.AppName", etc.

This screenshot shows the FortiGate Application Sensor configuration. It includes sections for "Categories" (listing Business, Cloud.IT, Game, etc.), "Application and Filter Overrides" (with a table for priority, details, type, and action), and "Options" (allowing log DNS traffic, QUIC, and replacement messages). A modal window titled "Edit Application Sensor" is open, showing a list of applications under "Add New Override". The "Application" dropdown is set to "Facebook".

- Scelta applicazione da controllare ed il relativo trattamento
- E' possibile riferirsi a multiple signatures a livello del protocollo

# Problemi di offuscamento

**Non si può bloccare ciò che non si vede**



## Encrypted Traffic

SSL è il nuovo standard

## Proxies

I Reverse proxies sono usatissimi dagli hacker

## Remote Desktop

Usato sempre più frequentemente per il telelavoro

## Compressed Content

ZIP files, compressed HTTP

## Encrypted Tunnels

Hamachi, Ultrasurf, Tor

# Blocco di applicazioni che offuscano traffico

- E' opportune bloccare le applicazioni non necessarie e ad alto rischio

- Filtri (o limitazioni) sulle applicazioni peer-to-peer
- Blocco delle applicazioni non necessarie che possono eseguire il tunneling di altre applicazioni
- Esaminare la necessità di applicazioni note per essere utilizzate dal malware
- Blocco di anonimizzatori come Tor
- Blocco delle applicazioni di tunneling crittografate come UltraSurf
- Limitazione d'uso ai proxy approvati
- Limitazione d'uso del desktop remoto

Custom Only			Clear Filters	249 matching applications
Technology	Risk	Characteristic		
86 browser-based	12 <span style="background-color: green; border: 1px solid black; padding: 2px;">1</span>	508 Evasive		
109 client-server	41 <span style="background-color: blue; border: 1px solid black; padding: 2px;">2</span>	409 Excessive Bandwidth		
36 network-protocol	62 <span style="background-color: yellow; border: 1px solid black; padding: 2px;">3</span>	267 Prone to Misuse		
17 peer-to-peer	80 <span style="background-color: orange; border: 1px solid black; padding: 2px;">4</span>	627 Transfers Files		
	54 <span style="background-color: red; border: 1px solid black; padding: 2px;">5</span>	249 <b>Tunnels Other Apps</b>		
		267 Used by Malware		
		760 Vulnerability		
		805 Widely used		
Subcategory	Risk	Technology		
general-business	4	client-server	<span style="color: green;">+</span>	<span style="color: blue;">+</span>
internet-conferencing	5	browser-based	<span style="color: green;">+</span>	<span style="color: blue;">+</span>
office-programs	3	browser-based	<span style="color: green;">+</span>	<span style="color: blue;">+</span>

# Blocco violazioni protocollo su NGFW

Il meccanismo di «protocol enforcement» consente di usare servizi di rete (ad esempio HTTP, HTTPS) solo sulle porte previste (es. 80, 443)

In caso di violazione è possibile bloccare o monitorare il traffico

- Security Profiles > Application Control
  - Creazione «application sensor» o editing di uno già esistente
  - Abilitazione «Network Protocol Enforcement»

The screenshot shows the FortiGate 60E interface under the Application Control section. On the left, there's a sidebar with various security profiles like Antivirus, Web Filter, and DNS Filter. The main pane displays a list of application categories such as Business, Collaboration, Game, Mobile, P2P, Remote-Access, Storage, Backup, Video/Audio, and Web Client. Below this, a table lists network protocol enforcement rules:

Port	Enforce Protocols	Violation Action
Port 80	PROT HTTP	Block
Port 53	PROT DNS	Monitor

The screenshot shows the FortiGate 60E interface under the Application Control section, specifically the 'New Application Sensor' dialog. It allows setting a port (80) and specifying enforce protocols (HTTP). The violation action is set to 'Block'. A list of available protocols is shown on the right, with 'HTTP' selected.

Consenti HTTP solo su porta 80

# IP Reputation

Blacklist (13)		
 Global Blacklist (Any Zone)	X	
 Attackers (Any Zone)	X	
 Bogon (Any Zone)	X	
 Bots (Any Zone)	X	
 Cnc (Any Zone)	X	
 Google-Monitor (Any Zone)	X	
 Google-Not (Any Zone)	X	
 Malware (Any Zone)	X	
 Open_proxy (Any Zone)	X	
 Open_relay (Any Zone)	X	
 Phishing (Any Zone)	X	
 Spam (Any Zone)	X	
 Tor_exit_node (Any Zone)	X	

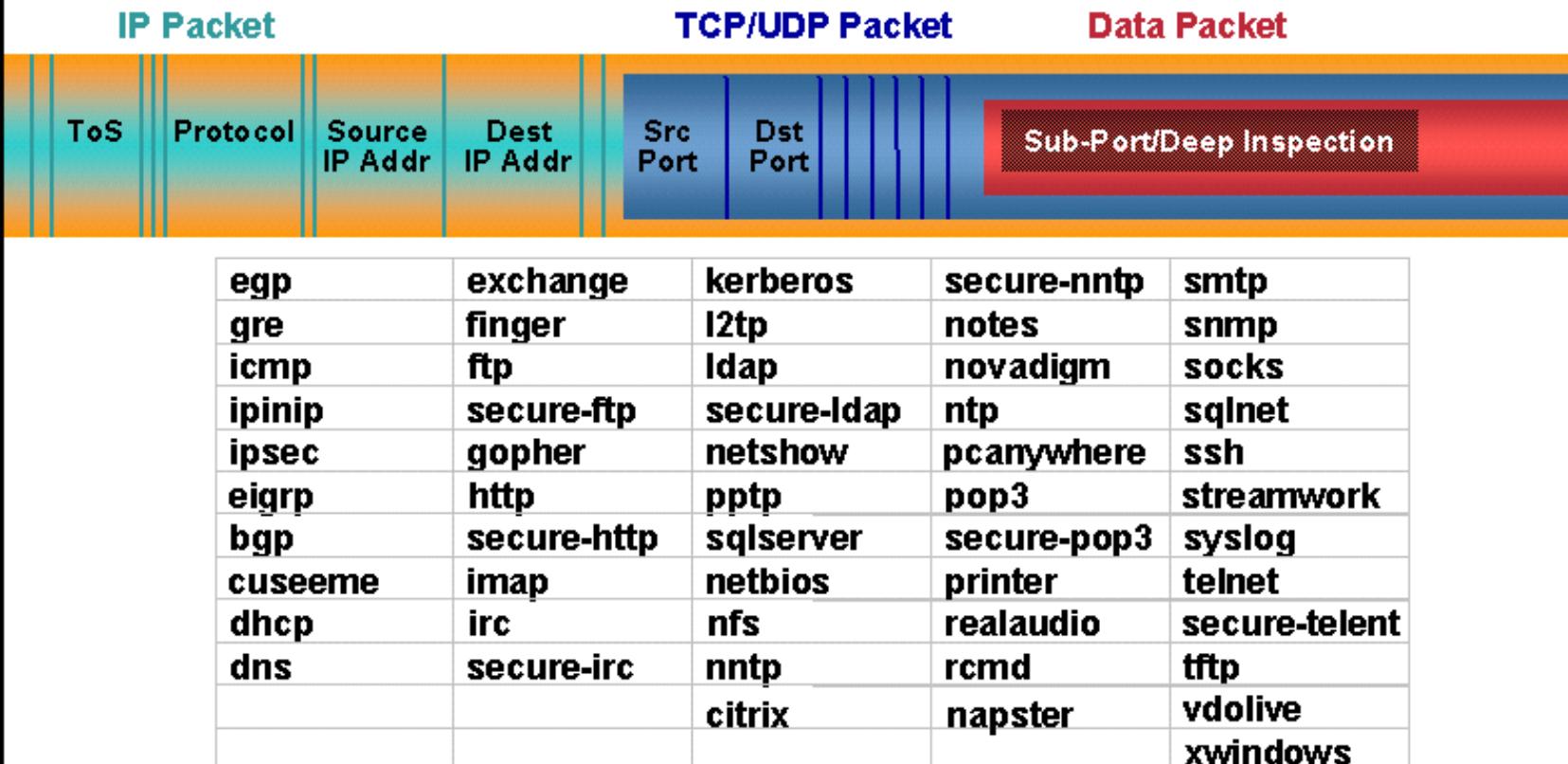
- Filtraggio e Alert su:
  - Botnet C&C Traffic
  - Attaccanti noti
  - Sorgenti di Malware, Phishing, e Spam
  - Open Proxies e open Relays

# Un esempio su router: NBAR

- Cisco NBAR (Network Based Application Recognition) è un motore proprietario Cisco per la classificazione del traffico disponibile anche a livello di router (e quindi verificabile in laboratorio GNS3)
- Esegue l'analisi dei modelli di traffico in real-time (basato su DPI e analisi del payload) in modo da riconoscere i protocolli
- Ha la capacità di classificare le applicazioni che hanno:
  - I numeri di porta UDP o TCP staticamente assegnati.
  - Protocolli che non sono TCP o UDP.
  - Numeri di porta UDP o TCP assegnati dinamicamente durante la connessione.
  - Classificazione basata su una ispezione profonda del pacchetto: NBAR può guardare all'interno di un pacchetto per identificare le applicazioni.
  - Identificare Traffico HTTP via URL, nome dell'host o tipo MIME usando le espressioni regolari (\*, ?, [ ]), Citrix ICA traffic, classificazione in base al tipo di payload RTP.
  - Attualmente supporta 88 protocolli/applicazioni.

# NBAR Packet Inspection

## Stateful & Dynamic Inspection



Supported protocols as of Cisco IOS Software Release 12.2(8)T:

[www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm) - 1031614

NBAR, 12/03

© 2003 Cisco Systems, Inc. All rights reserved.

# Configurazione NBAR

- Abilitazione funzionalità di protocol-discovery sull'interfaccia

```
int ethernet 0  
    ip nbar protocol-discovery
```

- Definizione di una classe di traffico via “class-map”

```
class-map match-any classe-di-prova  
    match protocol <espressione>
```

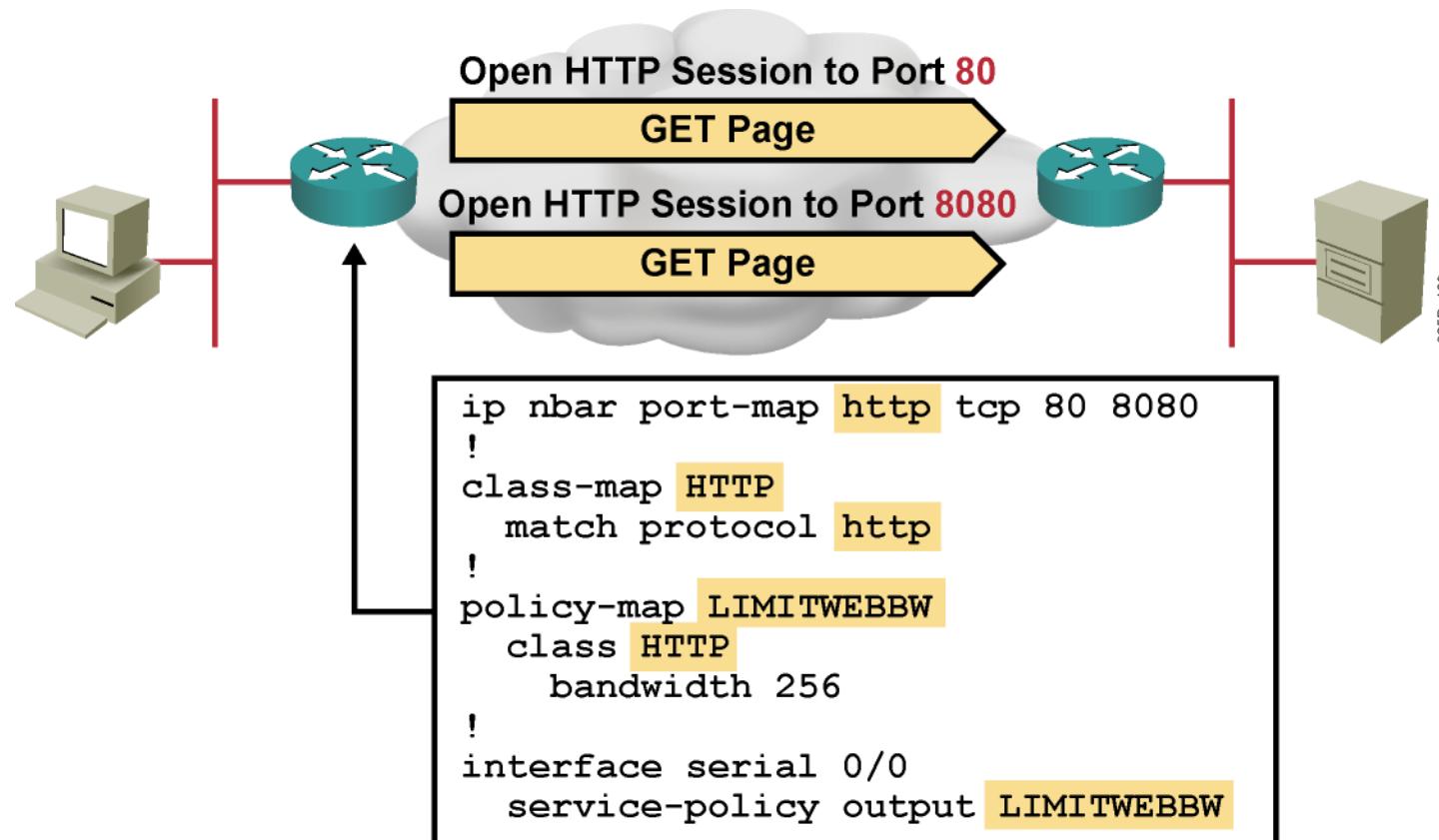
- Creazione di una policy di gestione della classe via “policy-map”

```
policy-map map-di-prova  
    class classe-di-prova  
        <azione (es. set ip dscp XXX) >
```

- Applicazione al'interfaccia di rete via “service-policy”

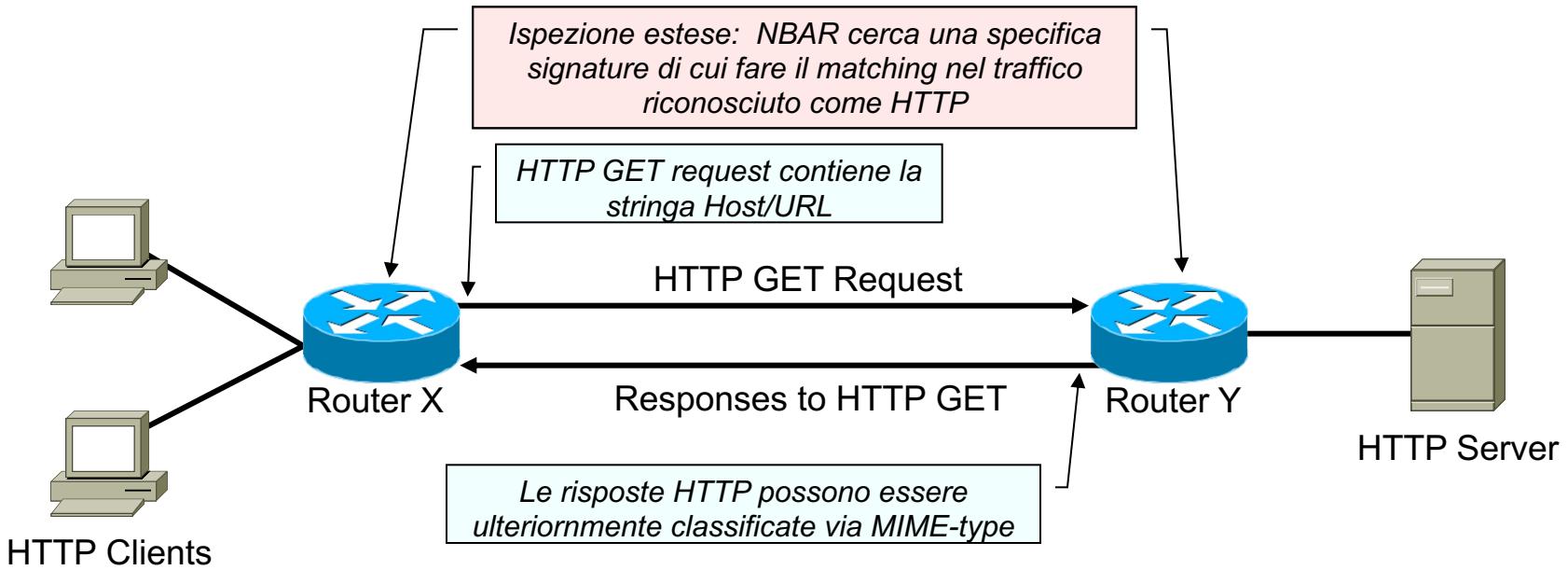
```
int ethernet 0  
    service-policy input mark-coded
```

# Limitazione in banda WWW



- Limitazione in banda traffico WWW
- Il comando **ip nbar port-map** definisce tutte le porte usate da HTTP.

# Ispezione transazioni HTTP



- (config-cmap)#match protocol http ?
  - host *host-name-string* -- Match Host Name
  - url *url-string* -- Match URL String
  - mime *MIME-type* -- Match MIME Type

E' possibile bloccare specifiche url o parti di esse (prefissi etc) oppure cercare keywords all'interno di url o specifici tipi MIME

# Blocco Code Red Worm

```
class-map match-any codered
    match protocol http url “*default.ida*”
    match protocol http url “*cmd.exe*”
    match protocol http url “*root.exe”

policy-map mark-codered
    class codered
        set ip dscp 1

int serial0
    ip nbar protocol-discovery
    service-policy input mark-codered

int ethernet0
    ip access-group 100 out

access-list 100 deny ip any any dscp 1
access-list 100 permit ip any any
```

# Blocco traffico P2P Kazaa

```
class-map match-any p2p
  match protocol fasttrack file-transfer *

policy-map block-p2p
  class p2p
    set ip dscp 1

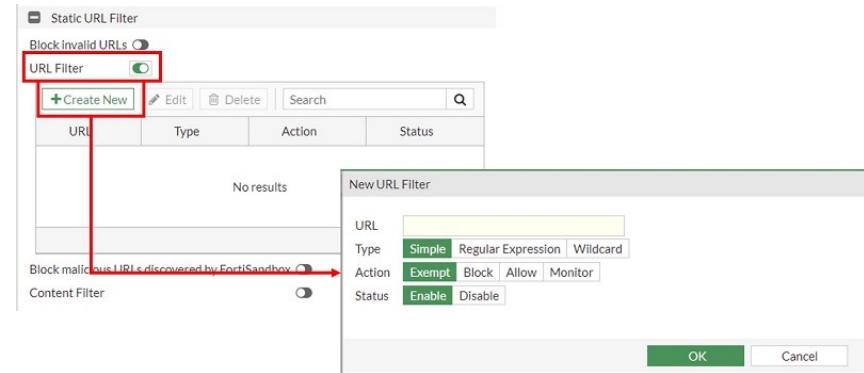
int FastEthernet0
  description PIX/Inside facing interface
  ip nbar protocol-discovery
  service-policy input block-p2p

int Serial0
  description Internet/Outside facing interface
  ip access-group 100 out

access-list 100 deny ip any any dscp 1
access-list 100 permit ip any any
```

# URL Filtering su NGFW

- Web Filter Menu
- Static URL Filter > URL Filter



The screenshot shows the 'Log & Report' section of the FortiGate interface. Under 'Web Filter', there is a table of log entries:

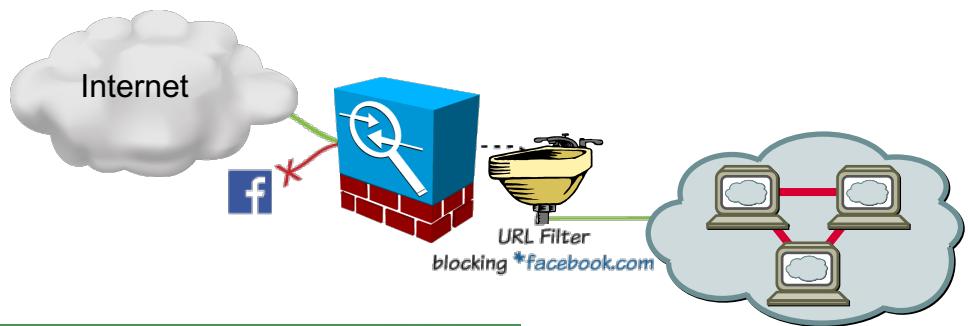
Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
6 seconds ago		10.1.10.3	blocked	http://yahoo.co.jp/favicon.ico			430 B / 0 B
6 seconds ago		10.1.10.3	blocked	http://yahoo.co.jp/			490 B / 0 B
40 seconds ago		10.1.10.3	blocked	https://pop.mail.yahoo.co.jp/			650 B / 0 B

Below the log table is a configuration section for 'Web Filter' with tabs for SSL, DNS Query, File Filter, and Web Application Firewall. The 'Web Filter' tab is selected.

# Blocco URL su NGFW

Semplice esempio:

- Blocco di qualsiasi accesso al dominio facebook.com
- Filtraggio a livello URL
- Uso di Web filtering policy



FW01

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Forward Traffic

Local Traffic

Sniffer Traffic

Events

AntiVirus

Web Filter

SSL

DNS Query

File Filter

Web Application Firewall

Add Filter

Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
6 seconds ago		10.1.10.3	blocked	http://yahoo.co.jp/favicon.ico		430 B / 0 B	
6 seconds ago		10.1.10.3	blocked	http://yahoo.co.jp/		490 B / 0 B	
40 seconds ago		10.1.10.3	blocked	https://pop.mail.yahoo.co.jp/		650 B / 0 B	

New URL Filter

URL: \*

Type: Simple

Action: Block

Status: Enable

OK Cancel

Crea una  
nuova policy  
che blocca  
\*facebook.com

Static URL Filter

Block invalid URLs:

URL Filter:

+ Create New	Edit	Delete	Search
URL	Type	Action	Status
*facebook.com	Wildcard	Block	Enable

Block malicious URLs discovered by FortiSandbox:

Content Filter:

System

Policy & Objects

IPv4 Policy

IPv6 Policy

NAT64 Policy

NAT46 Policy

Proxy Policy

Authentication Rules

Multicast Policy

Local In Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Security Profiles

Use Security Profile Group:

AntiVirus:

Web Filter:  WEB webfilter

DNS Filter:

Application Control:

IPS:

DLP Sensor:

VoIP:

ICAP:

Web Application Firewall:

SSL Inspection:

Mirror SSL Traffic to Interfaces:

SSL protocols:  SSL

Abilita la policy  
di web filtering

# Intrusion detection: concetti di base

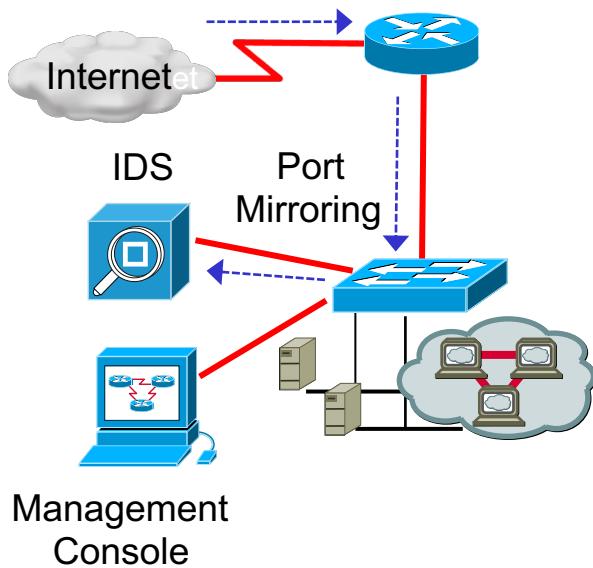
- Il concetto di «intrusione»
  - Insieme di azioni mirate a compromettere la sicurezza di uno specifico target o risorsa in rete ed in particolare:
    - Integrità (danneggiamento o modifica)
    - Confidenzialità (Violazione privaci ed esfiltrazione dati)
    - Disponibilità (Denial of service)
- Come rilevare un'intrusione?
  - L'unica possibilità è monitorare continuamente la rete e analizzare i log
  - Ovviamente questa soluzione non è molto scalabile.
  - L'analisi manuale delle informazioni di traffico o disponibili sui file di log è un'attività che richiede troppo rispetto ai tempi di reazione richiesti
    - Fornisce una visione limitata degli attacchi
    - Non è in grado di prevenire, al momento dell'analisi, l'attacco tipicamente è già iniziato.

# Intrusion Detection e Prevention

- E' necessario riconoscere istantaneamente e mitigare le minacce. Esistono due tecnologie:
  - Intrusion detection
    - Il processo di identificare e segnalare un attività di intrusione
  - Intrusion prevention
    - Estensione dei meccanismi di detection attraverso funzioni di controllo accessi avanzato per proteggere i target in tempo reale
- Assunzioni di base:
  - Le attività dei sistemi sono monitorabili
  - Le attività normali e quelle a seguito di intrusione presentano evidenze differenti

# Intrusion Detection Systems

- Un IDS monitora il traffico offline e genera un'allarme (log) quando rileva traffico dannoso,
- È un dispositivo passivo perché si limita ad analizzare il flusso di traffico attraverso un punto di intercettazione



- Non è quindi attraversato dal traffico
- Richiede solo un'interfaccia che opera in modalità promiscua.
- Non rallenta il traffico di rete
- Consente comunque il transito e l'attività del traffico dannoso

# Differenze fra IDS e Firewalls

- Entrambi preposti a controllare la sicurezza di una rete
- Un Next-Generation Firewall può rilevare attacchi o intrusioni provenienti dall'esterno ed intervenire per impedire che si verifichino.
- Tipicamente firewall limitano l'accesso tra segmenti di rete associate a domini di sicurezza differenti per prevenire intrusioni e non segnalano un attacco proveniente dall'interno.
- Viceversa un IDS è in grado di valutare una transazione sospetta una volta che la stessa ha avuto luogo e generare conseguenzialmente un allarme
- Un IDS quindi può rilevare anche gli attacchi che hanno origine all'interno

# Sistemi di difesa Passivi e Reattivi

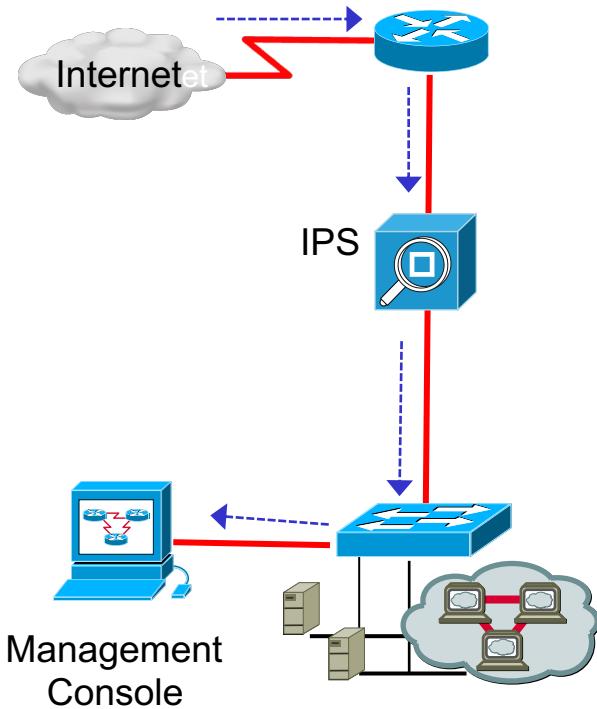
- Un sistema di difesa **passivo** quale ad esempio un IDS si comporta come un sensore in grado di
  - individuare una potenziale violazione della sicurezza,
  - tracciare la stessa
  - generare un allarme verso la security management console
- In un sistema **reattivo**, tipicamente un **Intrusion Prevention System (IPS)**, la componente IDS reagisce alla sospetta attività ostile resettando la connessione o riprogrammando il firewall per bloccare il traffico di rete dalla fonte potenzialmente dannosa.

# Intrusion Prevention

- Si definisce **Intrusion prevention** la capacità di bloccare dinamicamente gli attacchi e fornire i seguenti meccanismi di difesa attiva:
  - **Rilevamento**: identifica in tempo reale gli attacchi dannosi alla rete e alle risorse host.
  - **Prevenzione**: interrompe l'esecuzione dell'attacco rilevato.
  - **Reazione**: Immunizza il sistema da attacchi futuri da una fonte malevola.
- Entrambe le tecnologie (detection e prevention) possono essere implementate a livello di rete, a livello di host o entrambe per la massima protezione.

# Intrusion Prevention Systems

- Si basano sulla tecnologia IDS per rilevare gli attacchi.
- Tuttavia, possono anche affrontare immediatamente la minaccia.



- Un IPS è un dispositivo attivo perché tutto il traffico deve attraversarlo.
- Opera in linea in tempo reale per monitorare il traffico dal livello 2 al livello 7.
- Può anche impedire ai singoli pacchetti associati ad attacchi di raggiungere il sistema di destinazione (un IDS non può).

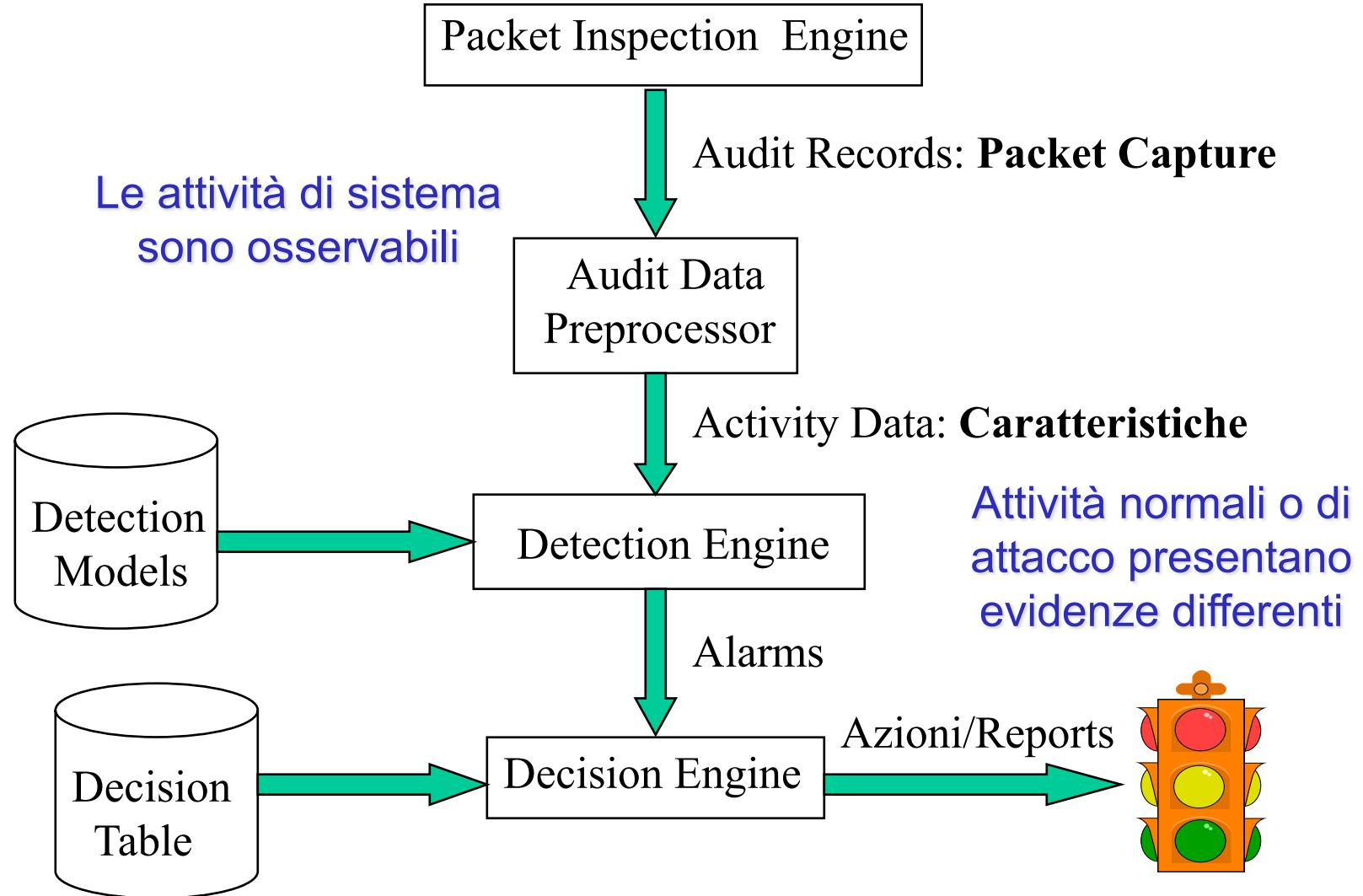
# IDS e IPS Vantaggi e Svantaggi

	<b>IDS (Promiscuous Mode)</b>	<b>IPS (Inline Mode)</b>
Vantaggi	<ul style="list-style-type: none"><li>Nessun impatto sulla rete in termini di prestazioni (latenza, jitter).</li><li>Nessun impatto sulla rete in caso di guasto del sensore o sovraccarico del sensore.</li></ul>	<ul style="list-style-type: none"><li>Blocca I pacchetti di attacco</li><li>Può usare tecniche di stream normalization</li></ul>
Svantaggi	<ul style="list-style-type: none"><li>Le reazioni (allarmi generati) non possono bloccare I pacchetti ostili.</li><li>Richiede un tuning sofisticato</li><li>Maggiormente vulnerabile a tecniche di network evasion</li></ul>	<ul style="list-style-type: none"><li>Qualche impatto sulle prestazioni di rete (latency, jitter).</li><li>Il guasto o il sovraccarico dell'IPS influiscono sulla funzionalità della rete</li></ul>

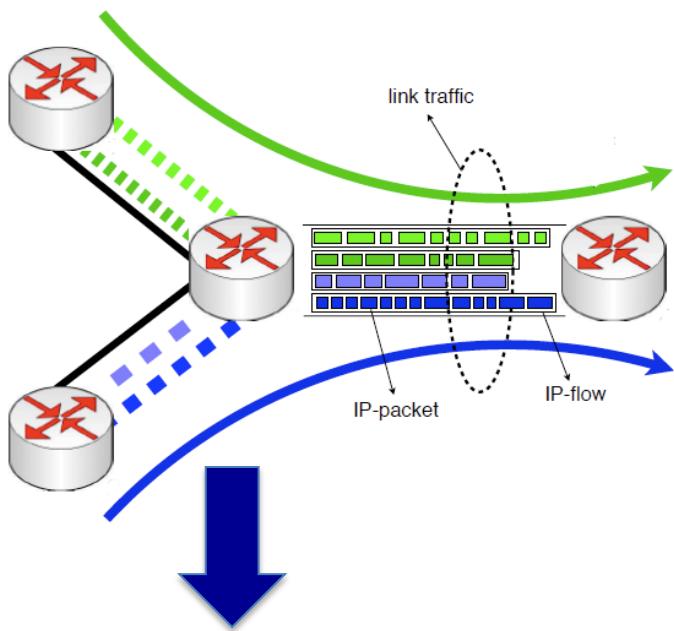
# Componenti Architetturali IDS/IPS

- Dal punto di vista algoritmico:
  - Caratteristiche
    - evidenze estratte da osservazioni (audit data)
    - elementi in grado di evidenziare intrusioni
  - Modelli – mettono insieme le evidenze
- Dal punto di vista architetturale:
  - packet inspection engine
  - audit data processor,
  - knowledge base,
  - decision engine,
  - sistemi di alarm generation e response management

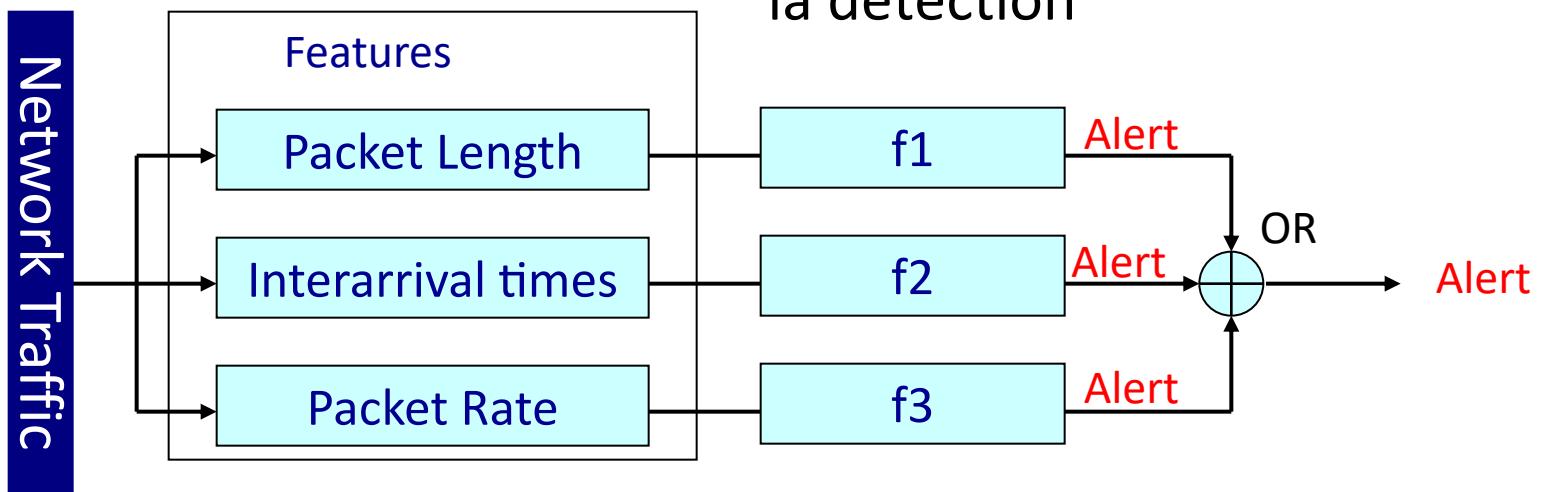
# Componenti Architetturali



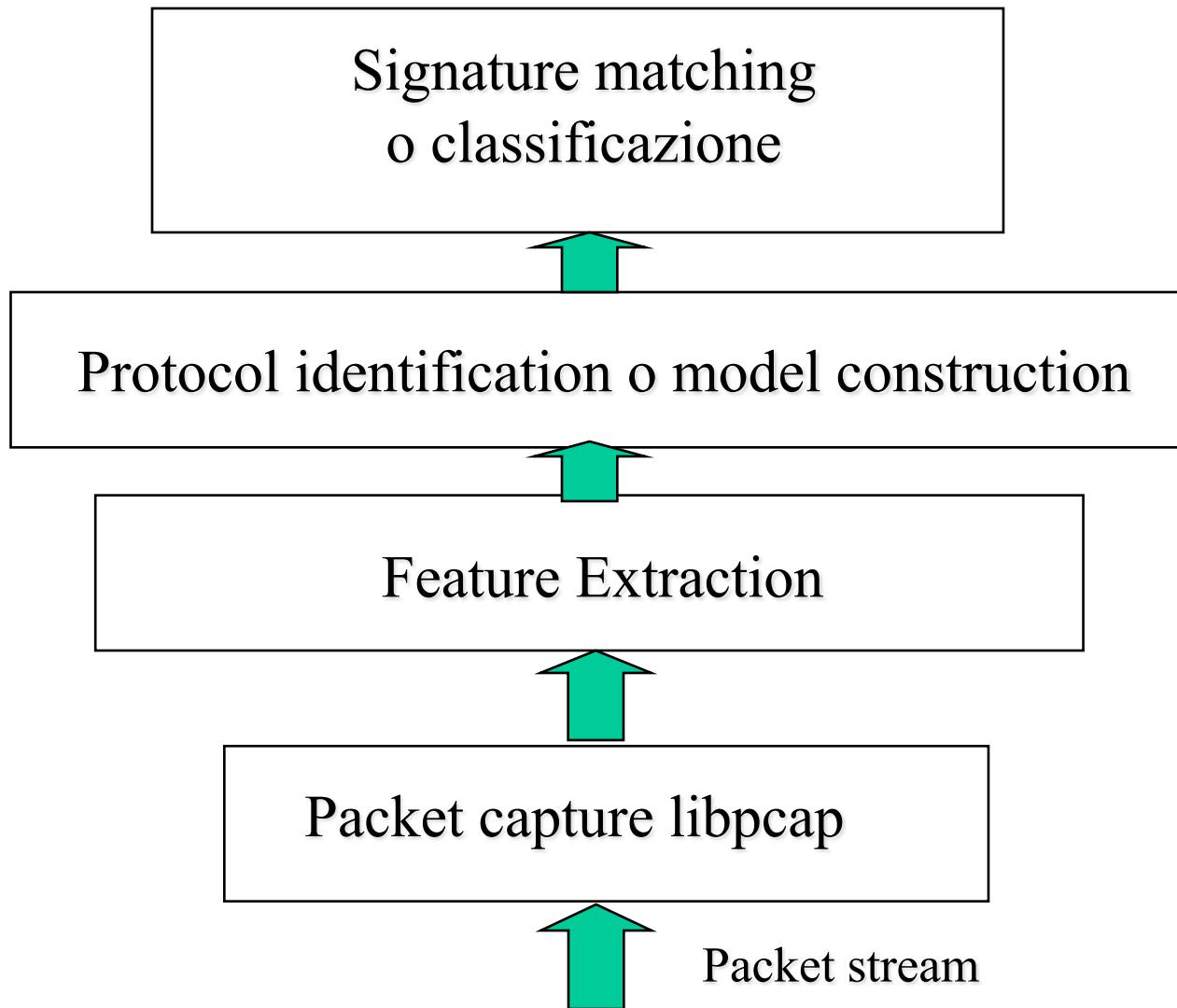
# Componenti Architetturali: caratteristiche



- Elementi descrittivi del traffico
  - Caratterizzano le dinamiche del traffico e ciò che ne descrive il cambiamento
  - Raccolte attraverso multipli punti di osservazione attraverso taps
- Usate per costruire modelli per la detection



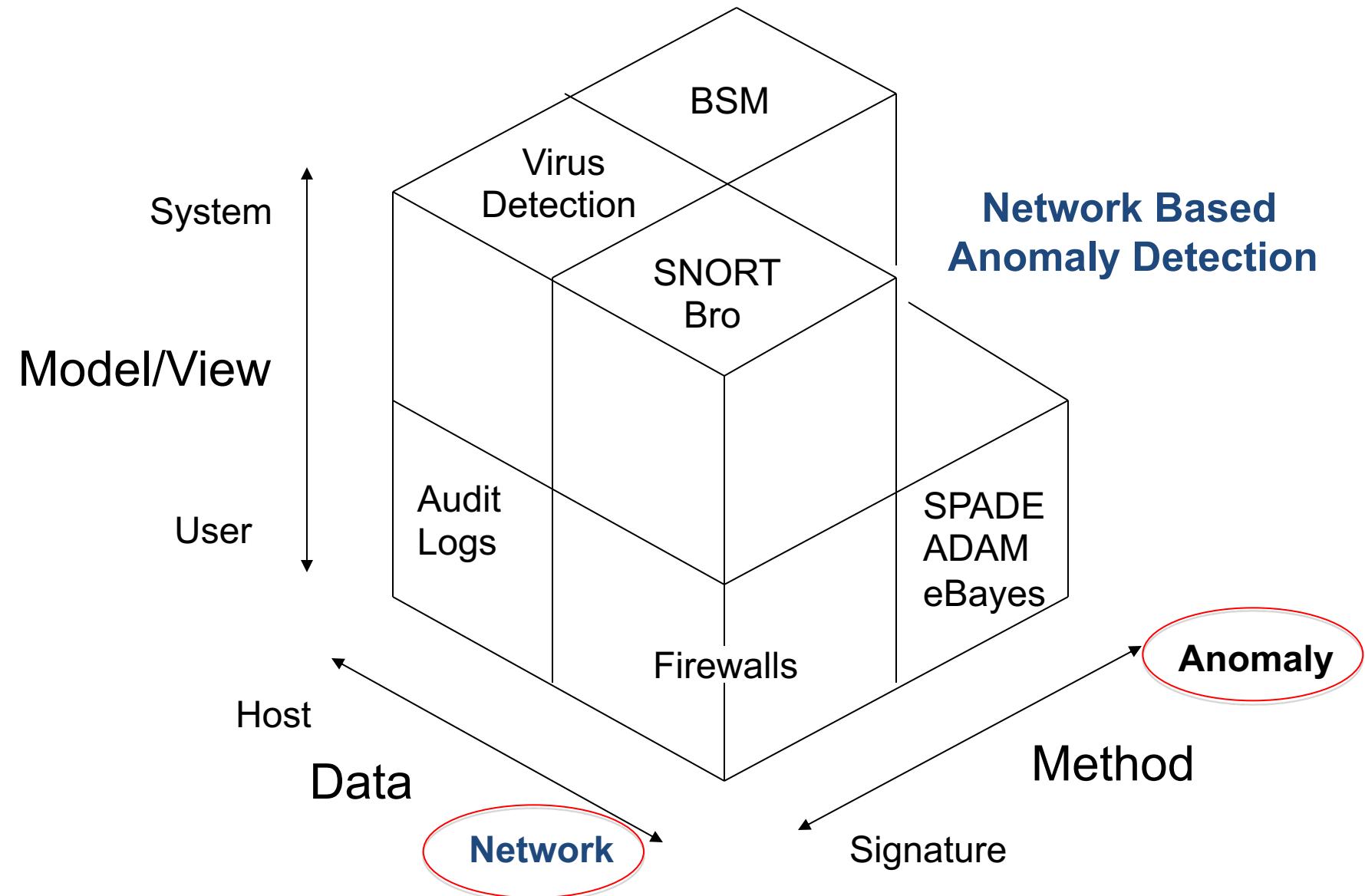
# Operatività IDS/IPS



# Approcci e implementazioni

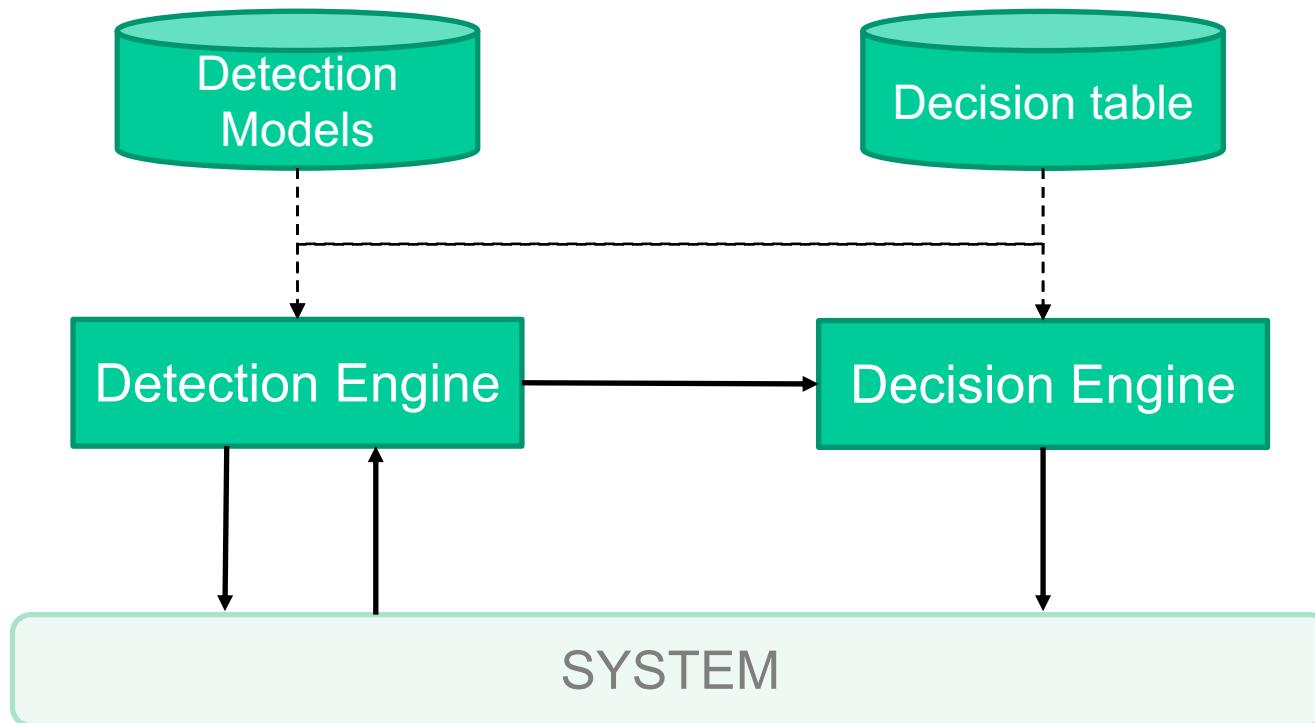
- Approccio Analitico: combinare le evidenze insieme a scopo di:
  - **Misuse detection**
    - Sistemi Knowledge-based (a.k.a. signature-based)
  - **Anomaly detection**
    - Sistemi Specification-based
    - Sistemi Behavior-based
- Implementazioni: Network-based o Host-based
  - **Network-based**: analizza il traffico di rete
  - **Host-based**: analizza l'attività dei processi

# Dimensioni della Detection



# Host-based IDS

- Basati su auditing and monitoring/analisi a livello di OS
  - Prevedono l'installazione di agents sui sistemi da monitorare
  - Profilano l'attività del sistema (system calls, accessi a disco etc., connessioni rete)
  - Possono eseguire analisi statica/dinamica di programmi per riconoscere malware
    - o Monitoraggio shell commands e system calls eseguite da applicazioni utente e di sistema
  - Richiedono informazioni estremamente accurate per una detection efficace



# Un esempio di Host-based IDS: EDR

- Gli EDR (Endpoint Detection and Response) sono strumenti cruciali nella difesa cibernetica proattiva di nuova generazione.
  - può migliorare significativamente la resilienza agli attacchi.
  - implementa una visibilità completa su tutti gli endpoint
- Un EDR è implementato attraverso un agent che ha il compito di rilevare, riconoscere e rispondere alle minacce a livello di ecosistema
- Le principali funzionalità sono:
  - Raccolta di dati dettagliati sull'attività degli endpoint e generazione di alert
  - Isolamento e rimozione automatizzata delle minacce (movimento laterale)
  - Analisi per comprendere la natura degli attacchi e raccoglierne le tracce utili
- L'EDR è in grado di cooperare con Firewall, SIEM e in genere con l'intero ecosistema di sicurezza

# Un esempio di Host-based IDS: EDR

Detect, Defuse, Respond and Remote Remediation

Pre-infection/ Pre-execution		Post-infection/Post-execution									
	Discover & Predict		Prevention		Detection		Defuse		Risposta e investigazione		Remediation & Roll back
Mitigazione rischio proattiva		Protezione pre-esecuzione		File-less e advanced threats	Blocco Data Breach e Ransomware			Piena visibilità attacchi		Disinfezione Automatizzata	
<ul style="list-style-type: none"><li>Individuazione rogue devices</li><li>Vulnerabilità</li><li>Virtual patching</li></ul>		<ul style="list-style-type: none"><li>ML AV</li><li>Threat Intelligence</li><li>Integrazione con Sandbox</li><li>Desktop firewall</li><li>Web filtering</li></ul>		<ul style="list-style-type: none"><li>Behavioral based</li><li>Riconoscimento attacchi memory-based</li><li>Classificazione minacce</li></ul>	<ul style="list-style-type: none"><li>Blocco di azioni ostili</li><li>Prevenzione Perdita dati</li><li>Zero Dwell time</li></ul>		<ul style="list-style-type: none"><li>Playbook automation</li><li>Cross platform response</li><li>Forensic data</li><li>Behavioral-based threat hunting</li><li>Built-in MITRE tags</li></ul>		<ul style="list-style-type: none"><li>Clean up / Roll back</li><li>Elimina re-image/rebuild</li><li>Minimizzazione business disruption</li></ul>		

Automazione | Cloud . Hybrid . | OS coverage

# Un esempio di Host-based IDS: EDR

- Gli EDR (Endpoint Detection and Response) sono strumenti cruciali nella difesa cibernetica proattiva di nuova generazione.
  - può migliorare significativamente la resilienza agli attacchi.
  - implementa una visibilità completa su tutti gli endpoint
- Un EDR è implementato attraverso un agent che ha il compito di rilevare, riconoscere e rispondere alle minacce a livello di ecosistema
- Le principali funzionalità sono:
  - Raccolta di dati dettagliati sull'attività degli endpoint e generazione di alert
  - Isolamento e rimozione automatizzata delle minacce (movimento laterale)
  - Analisi per comprendere la natura degli attacchi e raccoglierne le tracce utili
- L'EDR è in grado di cooperare con Firewall, SIEM e in genere con l'intero ecosistema di sicurezza

# Dagli EDR agli XDR

- Mentre gli EDR sono progettati per monitorare e proteggere gli endpoint tradizionali, le soluzioni XDR estendono l'ambito del rilevamento delle minacce i per includere altri livelli dello stack di sicurezza, ad esempio applicazioni, reti, server, carichi di lavoro e dispositivi IoT
- Le origini dei dati di interesse si differenziano tra EDR e XDR:
  - EDR si basa sui dati dei dispositivi endpoint,
  - XDR può raccogliere dati da tutto lo stack di sicurezza
- In termini di Scalabilità e adattabilità dato che i sistemi XDR possono connettersi a più livelli dello stack di sicurezza, sono più facili da ridimensionare e modellare in base a esigenze complesse
- XDR abbatte i silos nella logica di controllo distribuito fornendo una vista unificata su più strumenti e vettori di attacco.
- Tale visibilità migliorata fornisce il contesto completo delle minacce per ottimizzare il triage, l'indagine e gli sforzi di riparazione rapida.

# EDR/XDR Tools - Open Source

- Wazuh – OSSEC ++
- OSSEC – LIDS (xEndpoint), MW & RK detection, Automatable Actions, FIM, Inventory
- TheHive Cortex - IP, URL, domain, hashes, files, containment integration
- OSQuery – very generic host monitoring (configuration, performance , infrastructure health), + FIM, YARA (file artifacts) scanning, anomaly detection, process auditing, log settings, ...
- \*GRR – YARA, APIs, search and collect : files, reg, procs, mem cap, CPU, network, context ... all OSs, massive scale, full API, full cloud enablement/leveraging
- MIG – logs, files, memory, network, auditing, vulnerability mgmt, ... eroding forensics
- Volatility – digital forensics & incident response, EDR ++ (forensic dimension)

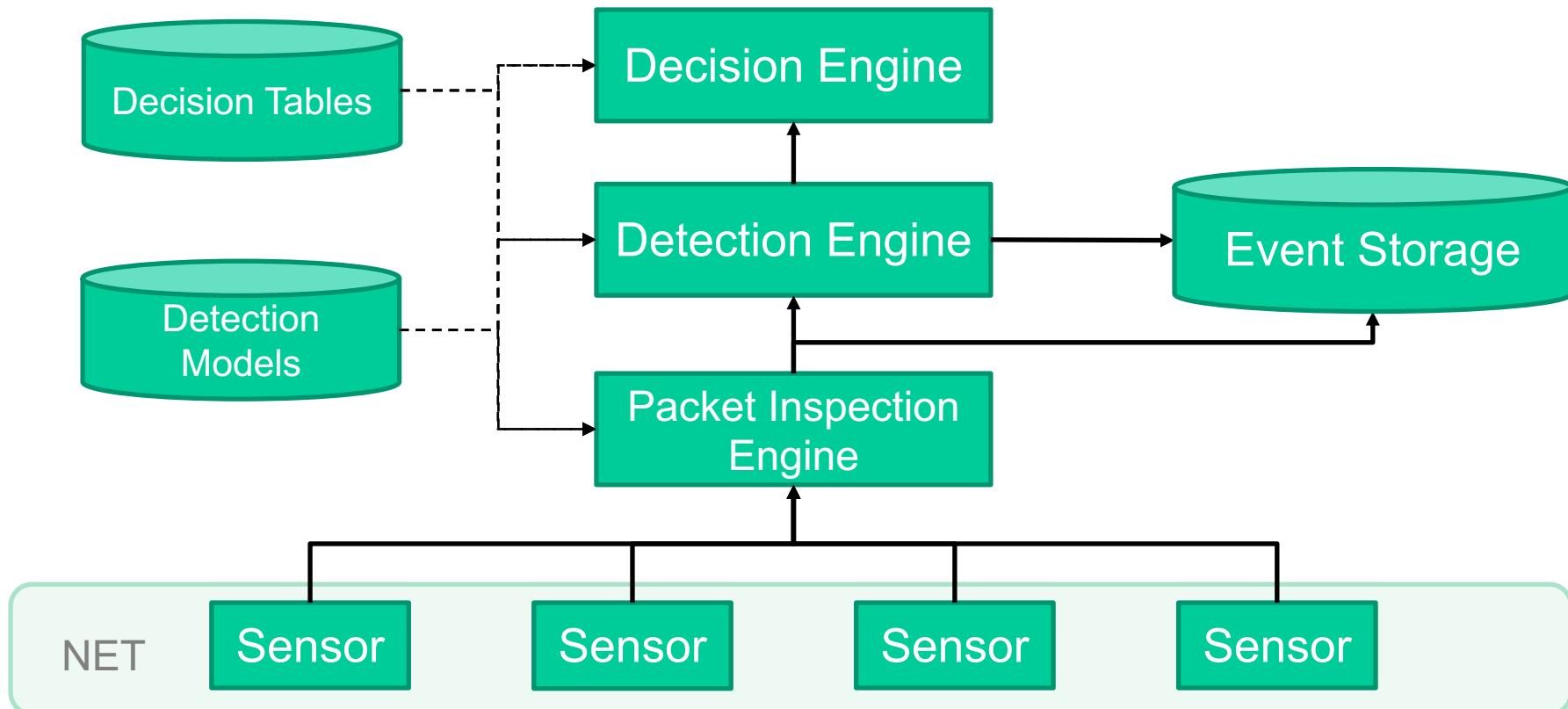
# EDR/XDR Tools - Commercial

## Gartner EPP MQ Leaders

- Microsoft - Defender for Endpoint
- CrowdStrike - Falcon
- Trend Micro Apex One – XDR for Cloud (Cloud One)
- SentinelOne - Singularity
- McAfee – MVISION EDR
- Sophos – Intercept-X
- Fortinet – FortiEDR
- BitDefender – GravityZone XDR
- Barracuda Managed XDR

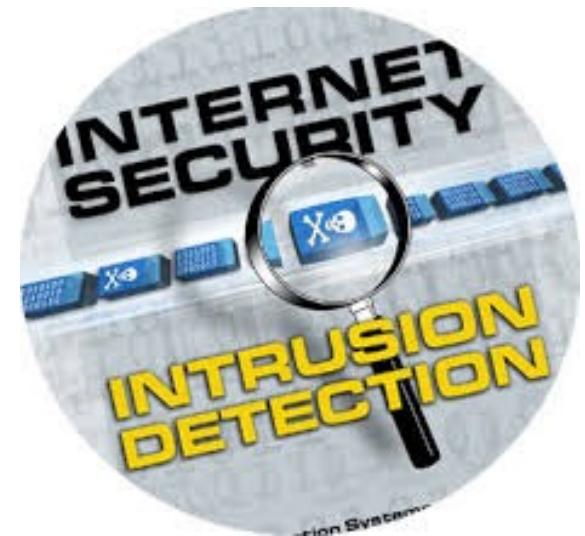
# Network-based IDS

- Basati su multipli sensori localizzati in punti strategici della rete
- Deep inspection del traffico di rete
  - Riconoscono la violazione di protocolli e l'occorrenza di pattern inusuali
  - Ispezionano il payload dei pacchetti per ricercare codice ostile
  - Generano allarmi in presenza di intrusioni/violazioni



# Problemi

- Non sono una panacea per tutti i problemi di sicurezza. In particolare *non* sostituiscono:
  - firewall ben configurati;
  - security audit regolari;
  - una politica di sicurezza “seria”.
- Producono falsi positivi.
- Possono essere “accecati” da attacchi DoS.
- Sono in difficoltà con reti veloci
  - rete di sensori (uno per macchina?).



# Problemi

- Sistemi Host-Based:
  - Dipendenza dall'utente: installazione/aggiornamento di un IDS agent (sensore) su tutte le macchine!
  - Se una macchina è violata, l'attaccante può modificare l'IDS e truccare i logs
  - La visione degli attacchi è solo locale
- Sistemi Network-Based
  - Non possono eseguire il payload o fare analisi del codice
  - DPI fornisce informazioni semantiche a livello di applicazione
  - Necessità di gestire grandi moli di traffico
  - Possono essere aggirati da tecniche crittografiche

# Approcci alla detection

- **Misuse detection o Knowledge-based:**
  - Richiedono la conoscenza pregressa della minaccia (misuse knowledge base)
  - Estremamente accurati ma poco completi
  - Richiedono aggiornamenti continui della knowledge based
  - Ottime prestazioni e minima richiesta di capacità computazionale
- **Anomaly-based**
  - Si basano sul riconoscimento di comportamenti che violano uno schema noto (outliers)
  - Estremamente completi ma poco accurati
  - In grado di riconoscere nuove minacce (0-day)
  - Estremamente impegnativi dal punto di vista computazionale (basati su AI e ML)

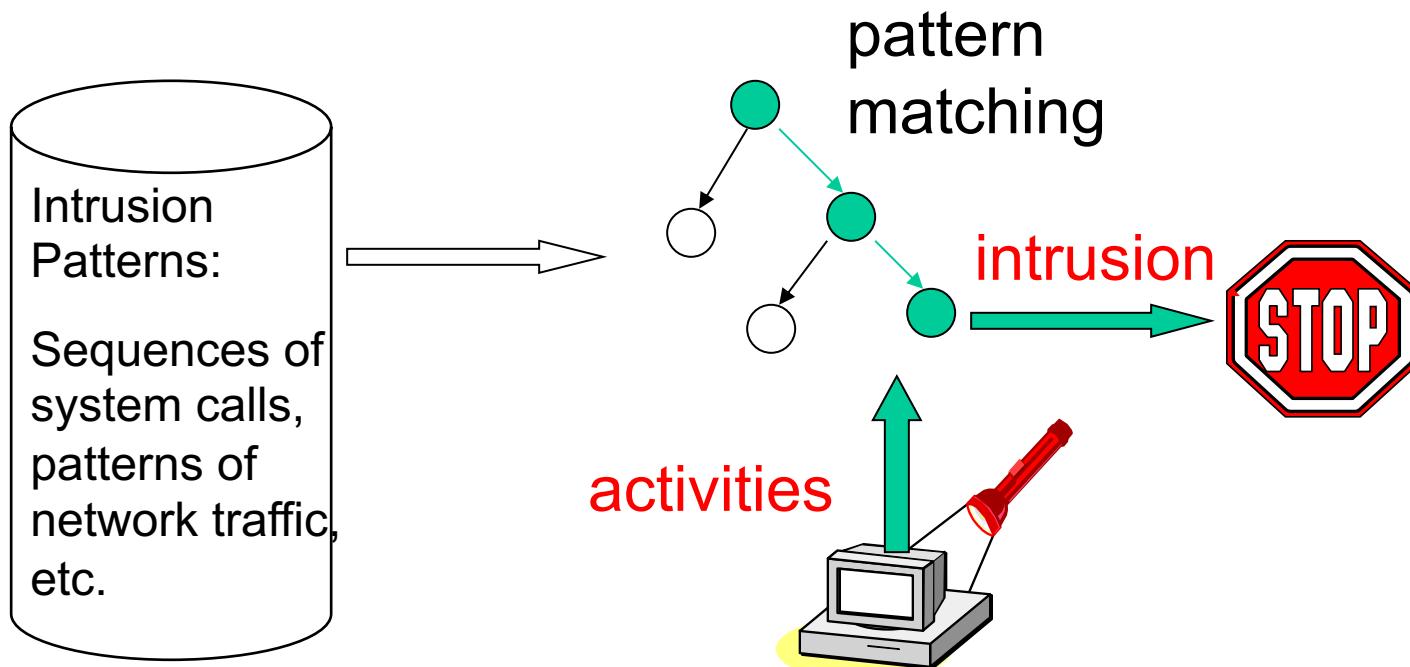
# Approcci Misuse detection

- Gli IPS/IDS che operano in logica misuse detection utilizzano serie di regole (**conoscenza pregressa**), per rilevare la tipica attività intrusiva in base ai pattern specifici di traffico che la caratterizzano (tipicamente chiamate “signatures”)
- Tali patterns possono essere descritti usando specifici linguaggi in grado di definire clausole di matching sia a livello di protocolli di rete/trasporto che di payload

Es. 1: `tcp $EXTERNAL_NET 1024: -> $HOME_NET 1024:  
(msg:"Skype client login -- reply from server";  
flags:AP,SUFR12; flow:to_client,established; dsiz  
e:5;  
content:"|17 03 01 00|"; depth:4; sid:1000010; rev:2; )`

Es. 2: `if (traffic contains "x90+de[\r\n]{30}")  
then "attack detected"`

# Approcci Misuse Detection



- Servono database di pattern di attacchi noti (signature DB) per generare allarmi o bloccare il flusso in caso di matching
  - Vantaggio: Buona accuratezza
  - Svantaggio: Non riconoscibili nuovi attacchi (0day)

# Signature

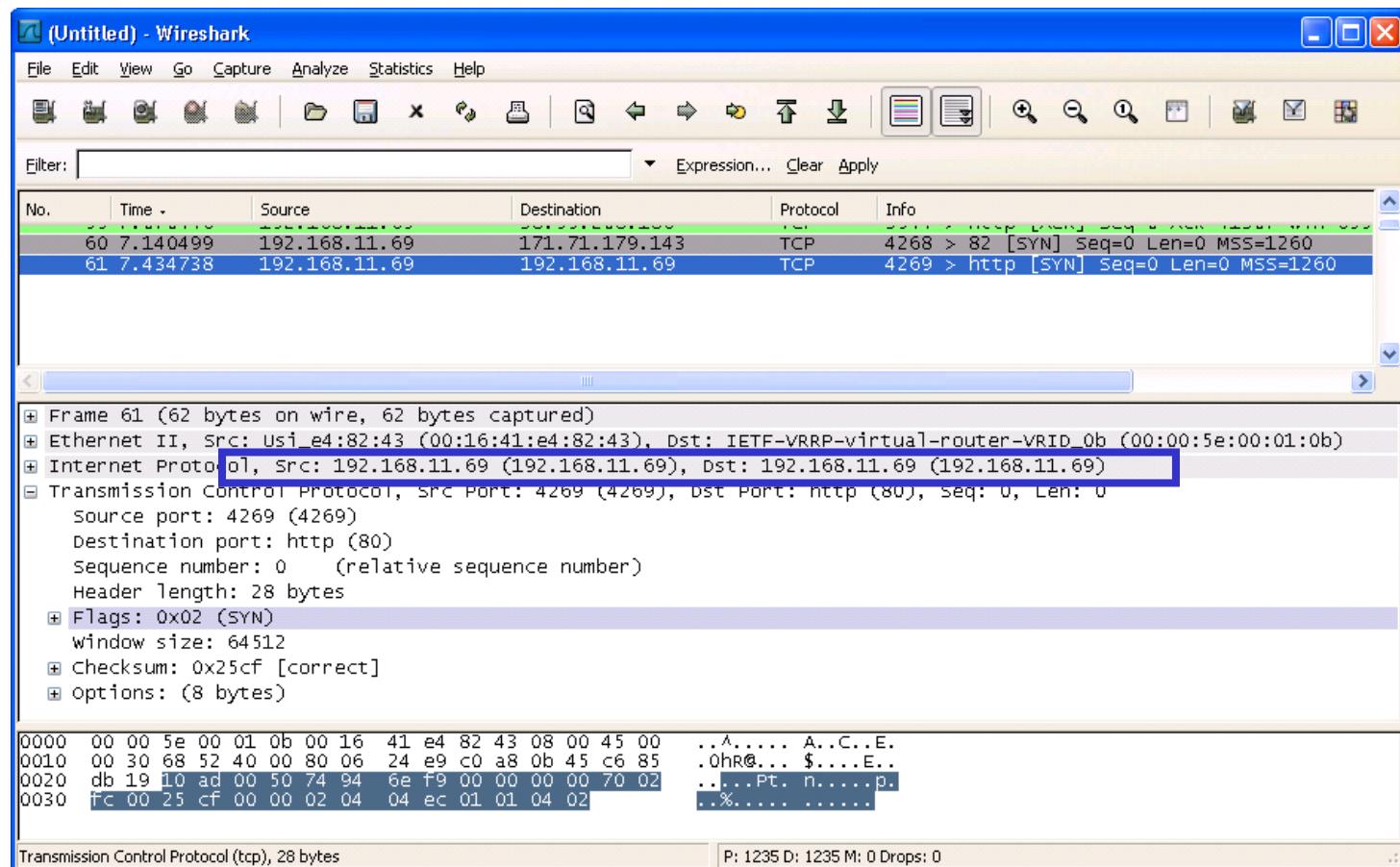
- Le Signatures sono caratterizzate da tre distinti attributi:
  - Tipo Signature
    - Atomiche (basta analizzare un solo pacchetto)
    - Composte (vanno ispezionati più pacchetti)
  - Trigger (allarme)
  - Action (risposta)

# Signature Atomiche

- Rilevano le forme più semplici di attacco individuabile dall'analisi di un singolo pacchetto, attività o evento da esaminare per determinare la corrispondenza con un pattern noto
  - In tal caso, viene attivato un allarme e viene eseguita un'azione associata al pattern
  - Non richiede alcuna conoscenza di attività passate o future (non sono richieste informazioni di stato sul flusso di pacchetti).

# Signature Atomiche: esempio

- Un attacco LAND contiene un pacchetto TCP SYN con indirizzi IP dell'host di origine e destinazione identici, facendo sì che la macchina risponda continuamente a se stessa.



# Signature Composte

- Definite anche come **stateful signature**, identificano una sequenza di operazioni distribuite su hosts multipli da riscontrare su un periodo di tempo specifico (orizzonte degli eventi).
  - **orizzonte degli eventi** : la durata dell'intervallo di tempo in cui va conservato lo stato per il matching della signature
- Tipicamente richiedono il matching di determinati pattern (payload o protocolli) su pacchetti/eventi differenti, per i quali il Sistema IDS/IPS deve conservare memoria dello stato nel contesto di una specifica transazione.

# Signature Composte: orizzonte eventi

- La durata dell'orizzonte degli eventi varia per ogni signature
  - Un IPS non può conservare le informazioni sullo stato indefinitamente senza esaurire le proprie risorse.
  - Pertanto, un IDS/IPS utilizza un orizzonte eventi propriamente configurato per la signature per determinare per quanto tempo va atteso il completamento di un pattern di attacco specifico quando viene rilevato un componente iniziale dello stesso
- La configurazione della durata dell'orizzonte degli eventi è un compromesso tra il consumo di risorse e la capacità di rilevare un attacco che si articola su un lungo periodo di tempo.

# Signature File

- Man mano che vengono identificate nuove minacce, è necessario creare e caricare nuove signatures nella base di conoscenza di un IDS/IPS
- Per semplificare questo processo, tutte le signatures da aggiungere possono essere inserite in un unico file di aggiornamenti da caricare su base periodica
  - Le soluzioni che aggiornano e distribuiscono i file delle signatures più frequentemente sono in grado di proteggere meglio la rete

# Esempi di Signature

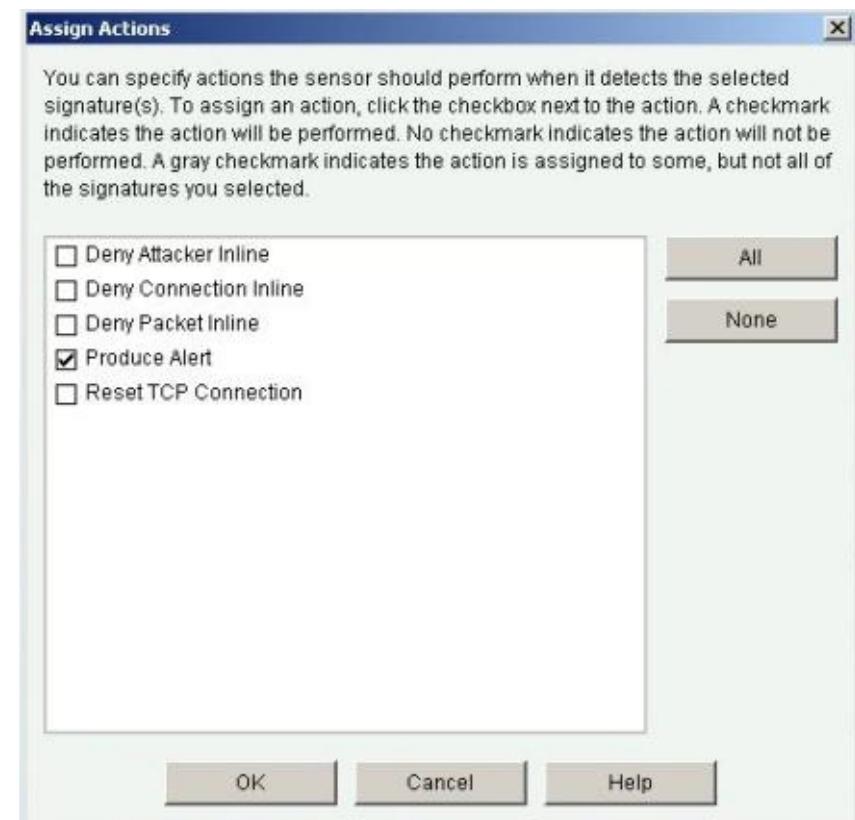
ID	Name	Description
1101	Unknown IP Protocol	Verificata quando viene ricevuto un datagramma IP con il campo protocollo impostato su 134 o superiore.
1307	TCP Window Size Variation	Verificata quando la TCP window size varia in maniera sospetta
3002	TCP SYN Port Sweep	Verificata quando una serie di pacchetti TCP SYN vengono inviati a un certo numero di porte di destinazione su un determinato host
3227	WWW HTML Script Bug	Verificata in presenza di un tentativo di visualizzare la presenza di files esternamente alla HTML root directory.

# Livelli di allarme associati a signature

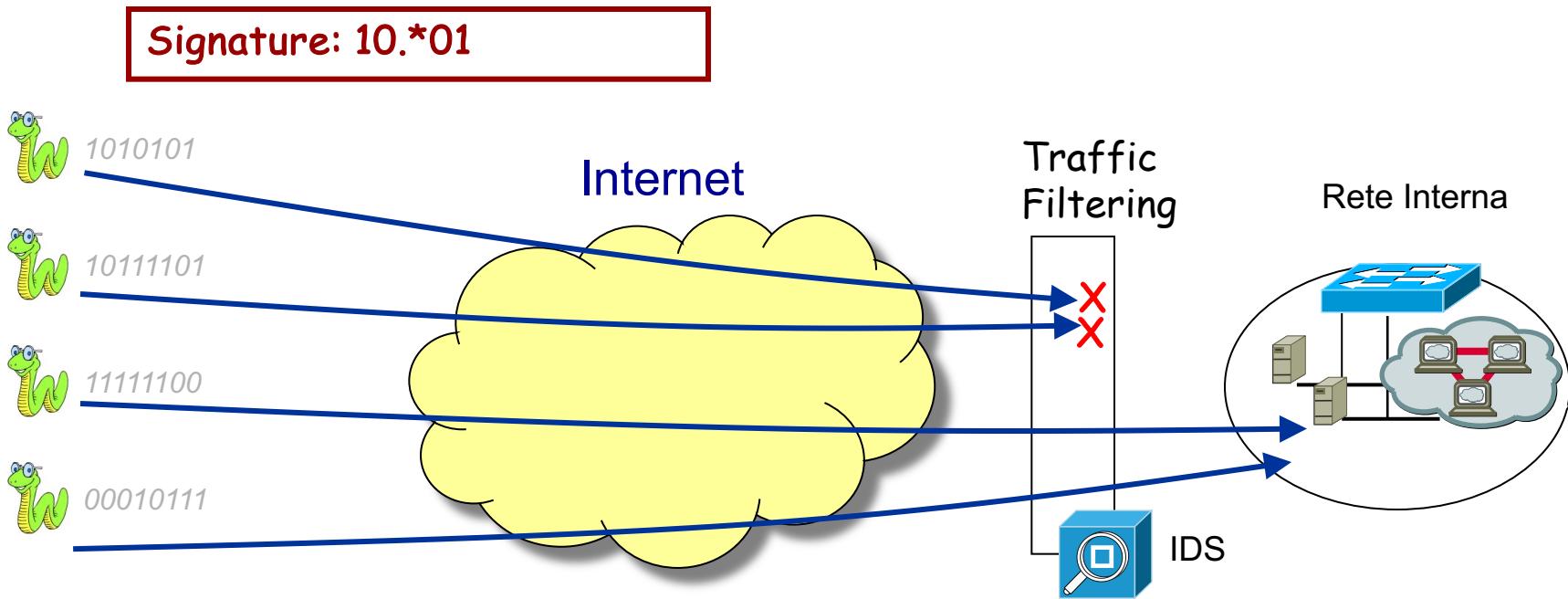
- A una signature può essere associato un livello di alert che è funzione della severità del problema individuato:
  - Basso
    - È stata rilevata un'attività di rete anomala che potrebbe essere percepita come dannosa, ma non è probabile una minaccia immediata.
  - Medio
    - È stata rilevata un'attività di rete anomala che potrebbe essere percepita come dannosa ed è probabile una minaccia immediata.
  - Alto
    - Rilevamento di un attacco mirato a ottenere l'accesso a risorse interne o DoS: una minaccia immediata è estremamente probabile.
  - Informativo
    - L'attività che attiva la signature non è considerata una minaccia immediata, ma le informazioni fornite sono utili.

# Signature Actions

- In presenza di matching di una signature, in ragione del livello di allarme e dell'attività ostile associata possono essere eseguite diverse azioni:
  - Consenti l'attività
  - Blocca immediatamente l'attività
  - Blocca attività future negando qualsiasi ulteriore traffico all'origine
  - Genera uno specifico allarme.

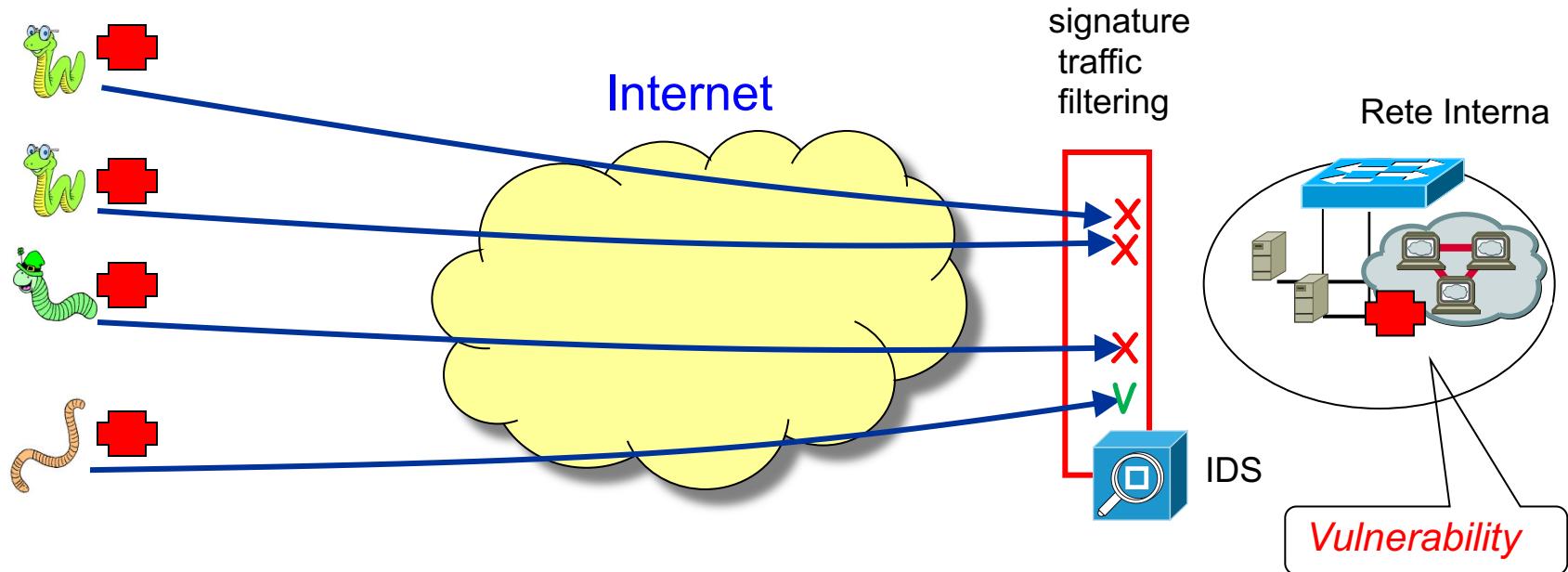


# Limitazioni delle Signatures Statiche



- Le signature usate nelle soluzioni basate su misuse detection sono tipicamente statiche
  - Basate esclusivamente sul matching esatto di specifici pattern
  - Rappresentate da espressioni regolari

# Il problema del polimorfismo

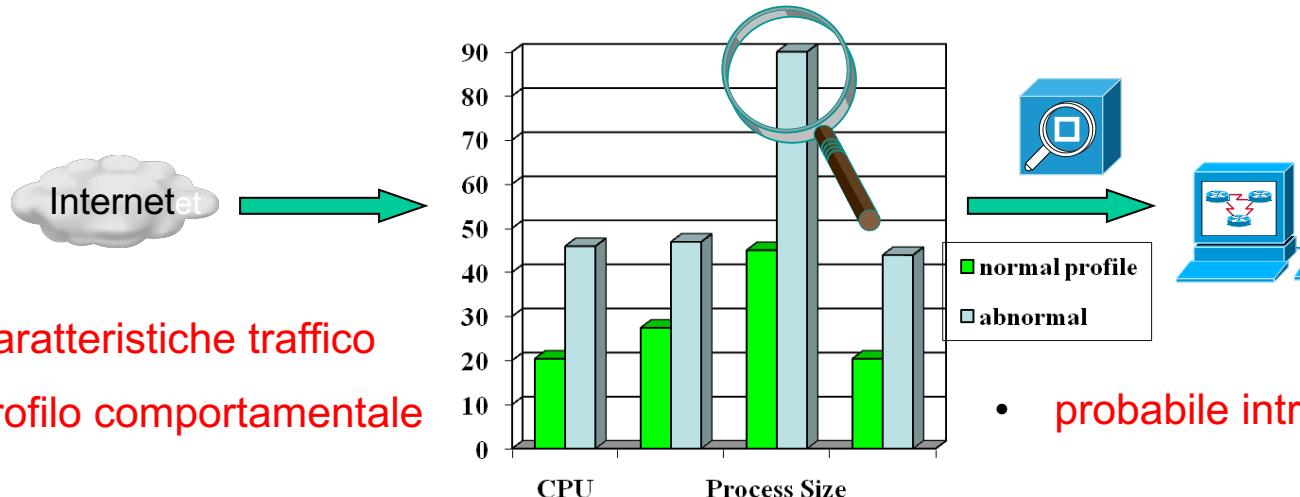


- Un malware polimorfo può cambiare frequentemente comportamento e signature
- Non è possibile rilevare malware polimorfi e tutte le minacce che esplorano vulnerabilità non note

# Approcci Anomaly-based

- **Sistemi Specification-based**
  - Basati sullo sviluppo di specifiche chiare (statistiche, soglie, proprietà matematiche) che definiscono il comportamento legittimo del sistema.
  - Qualsiasi deviazione è un intrusione.
- **Sistemi Behavior-based**
  - Costruiscono un modello di comportamento legittimo (o illegittimo)
  - individuano le intrusioni riconoscendo deviazioni (o conformità) rispetto al modello

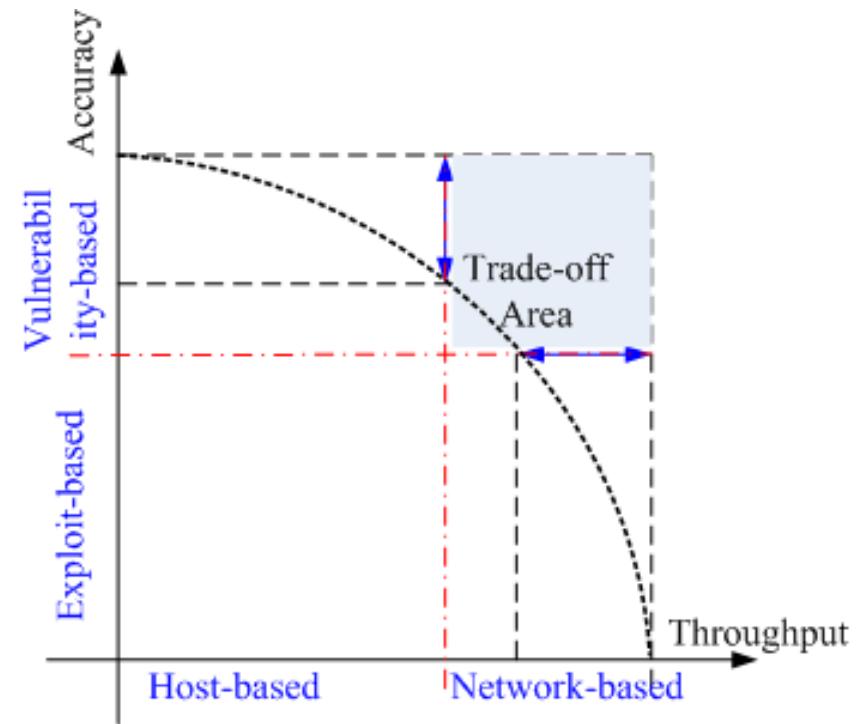
# Sistemi Specification-based



- Caratteristiche traffico
- Profilo comportamentale
  - probabile intrusione
- Un Sistema Specification-based definisce un **profilo** comportamentale in termini di **specifiche** e rileva le deviazioni rispetto ad esso
- Può potenzialmente individuare nuovi attacchi. Ma...
  - Si limitano il numero di falsi positivi (ma c'è dipendenza dalle specifiche)
  - Eventi rilevati come anomali possono essere attività normali riferite a usi precedentemente non previsti dalle specifiche
  - Sono molto difficili da sviluppare
- Man mano che la rete si evolve, il comportamento cambia, quindi la definizione delle specifiche va rivista periodicamente.

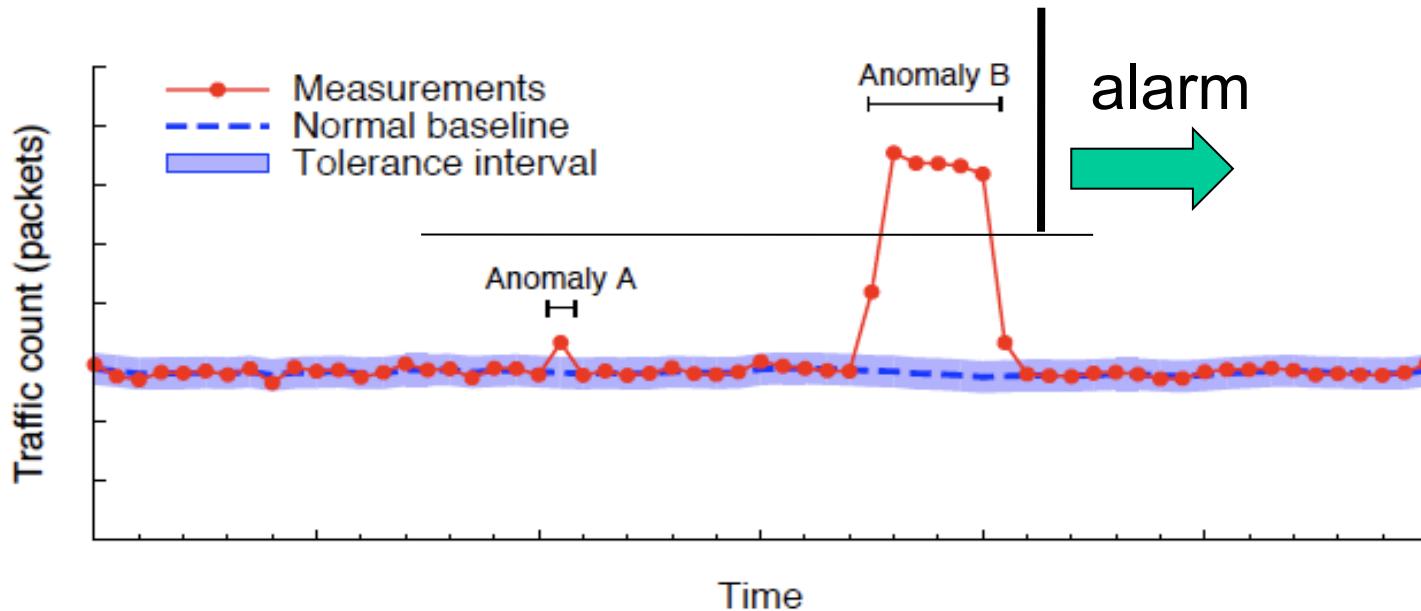
# Sistemi Behavior-based

- Maggiore Completezza
- Adattivi
  - Riconoscono e generano signatures (conoscenza) per attacchi 0day
- Reattività Scenario-based e situational-awareness
  - Correlazione di multiple sorgenti di osservazioni
  - Comportamento dipendente dalla situazione/scenario (botnet, DDoS)
  - Uso massiccio di tecnologie di Machine learning e AI



# Anomaly Detection

- Studio di un modello di comportamento normale
- Identificazione di violazioni a tale modello
- Divisione dei comportamenti in 2 spazi “*anomalo*” e “*normale*” e genera un allarme quando una specifica soglia di deviazione viene sorpassata (outlier)
- Non sappiamo in anticipo cosa è anomalo e cosa non lo è



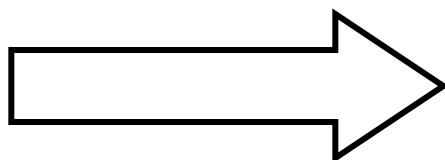
# Anomaly Detection

- Il rilevamento di anomalie può essere descritto come un problema di **classificazione binaria**: le attività sono divise in due classi
  - "normale" (negativo)
  - "non normale" (positivo).
- In situazioni più complesse si può arrivare a una classificazione multi-classe in cui il motore di detection è in grado di riconoscere oltre alla classe di traffic “normale” lo specific tipo di anomalia:
  - per macro-categoria: (es. scansione, DoS, buffer overflow)
  - per tipo di attacco: (es. SYN flood, smurfing, slowloris)

# Addestramento del modello

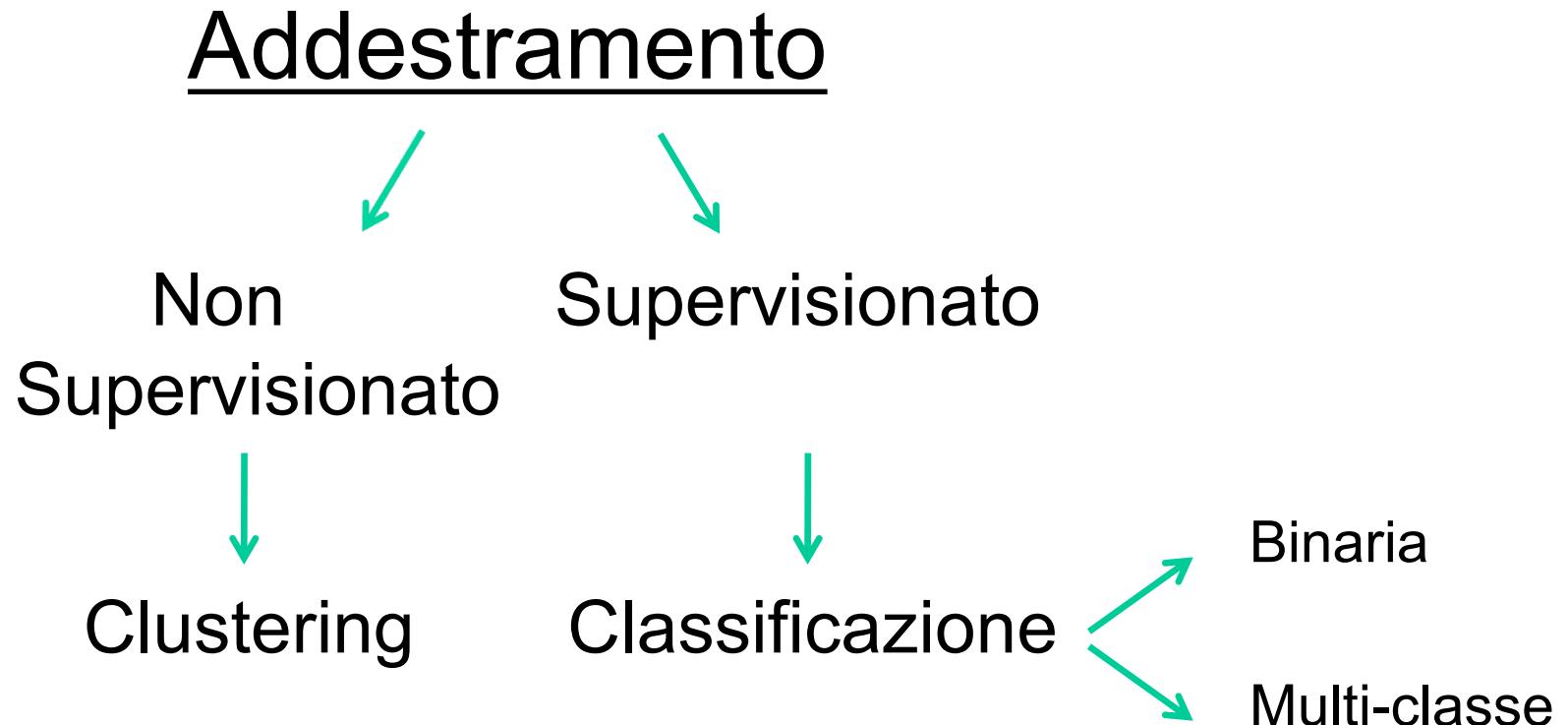
- Processo con il quale si utilizzano i dati a disposizione (*training set*) per la costruzione del modello
- L'attività di definizione di un modello comportamentale del traffico normale è nota come “baselining”

Esempi tratti dal  
problema  
(*Training Set*)  
Conoscenza a  
priori



Regole che  
governano il  
fenomeno

# Modalità di Addestramento



# Addestramento supervisionato

- Sinonimi: *supervised learning, classificazione*
- Idea e scopo:
  - di ogni elemento del training set si conosce l'esatta categoria.
  - L'obiettivo è quello di creare uno strumento in grado di classificare nuovi oggetti.
- Problemi:
  - capire se un algoritmo di training è capace di trovare la soluzione ottimale;
  - capire se converge, e se è sufficientemente scalabile;
  - capire se riesce a prediligere soluzioni semplice
  - Riconoscere situazioni mai affrontate (zero-day)

# Addestramento supervisionato

Apprendimento basato

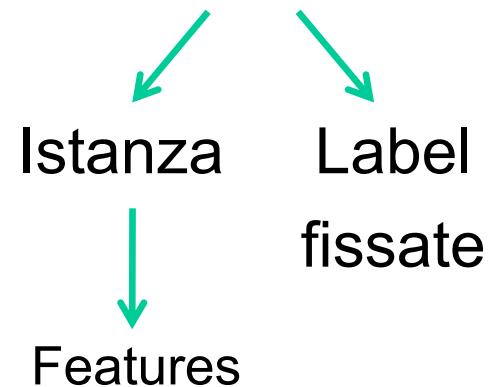
su Training Set → Insieme di coppie (esempi)



Costruzione classificatore



Test su nuove istanze

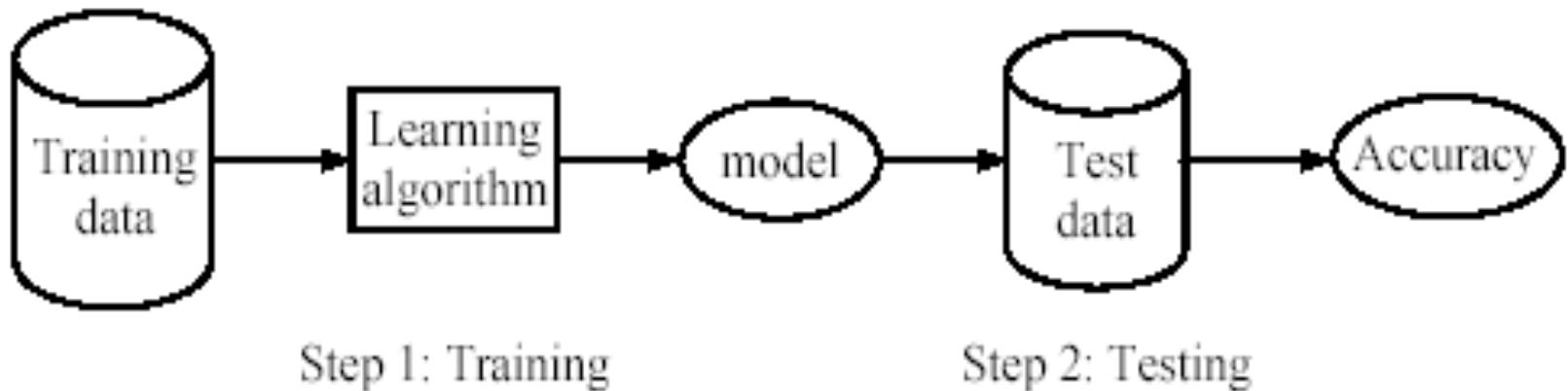


# Addestramento non supervisionato

- Sinonimi: *unsupervised learning, clustering*
- Idea e scopo:
  - nessuna informazione sulla categorizzazione degli elementi del training set.
  - Il sistema deve trovare i clusters (gruppi) “naturali” all’interno del training set, sulla base della “similarità” tra patterns
- Problemi:
  - intrinsecamente più difficile della classificazione
    - “naturali”?
    - “similarità”?

# Il processo di detection

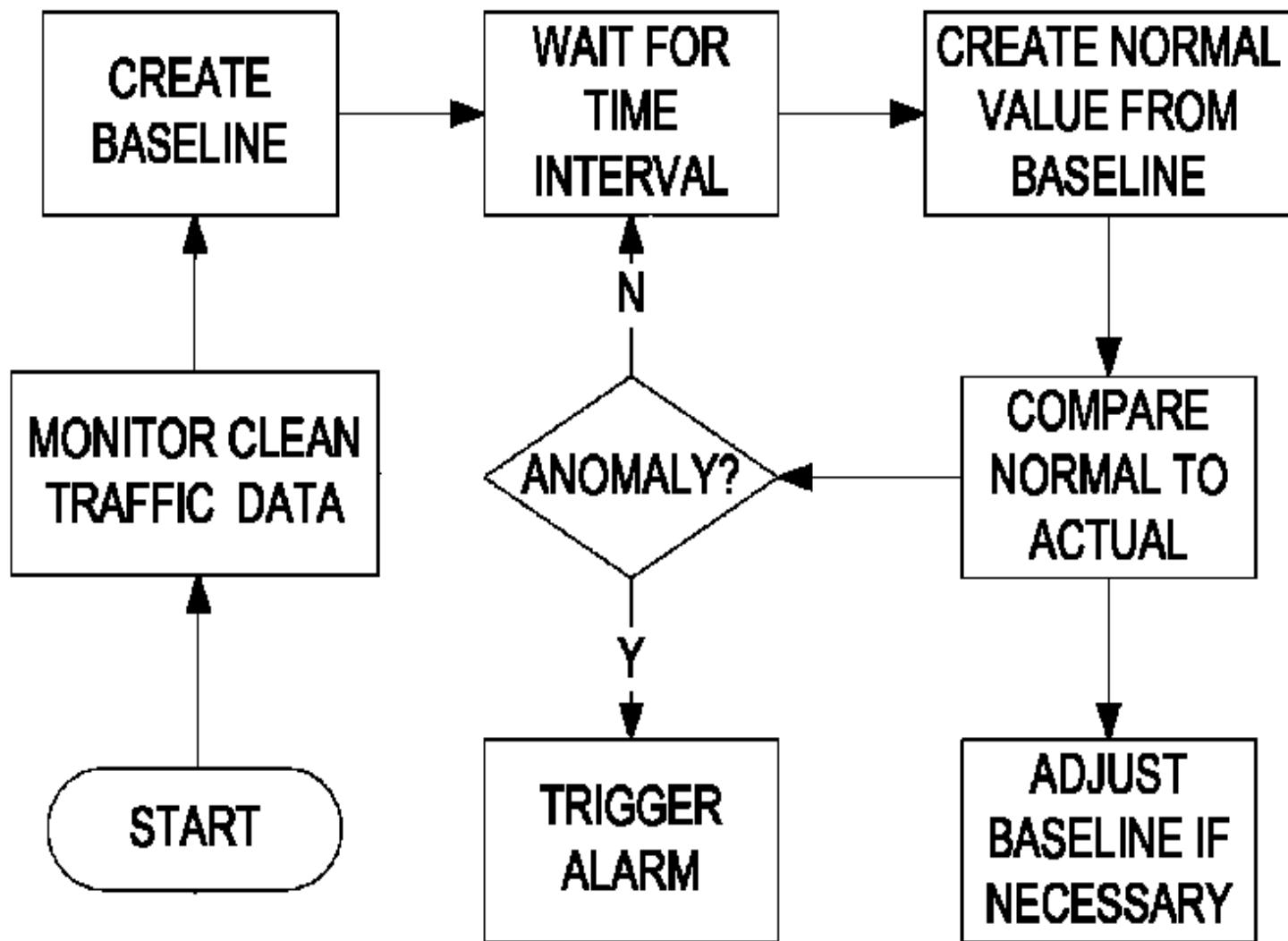
- L' anomaly detector è un classificatore a 2 classi che usa il **machine learning** per analizzare le deviazioni dal modello di normalità (baseline)
- Impara circa il verificarsi di specifici fenomeni via **inferenza induttiva**
- **Viene tipicamente addestrato solo sulla baseline**



# Il processo di training

- Utilizzando le caratteristiche estratte dal traffico opportunamente etichettato (pre-classificato) viene costruito il modello di classificazione.
- L'insieme delle label associate al traffico si definisce «**ground truth**»
- Utilizzando nuovi dati che includono nuovi tipi di attacchi è possibile riaddestrare o raffinare l'addestramento del modello.

# Il processo di detection



# *Sistemi di classificazione supervisionata*

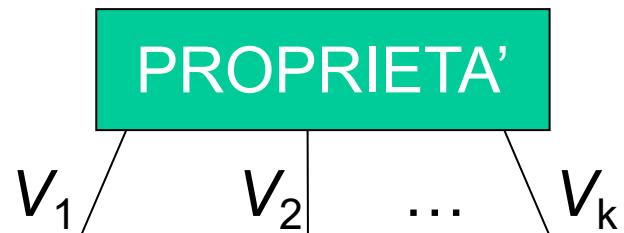
- Nella scelta di un sistema di classificazione supervisionato le opzioni più usate sono
  - **Alberi Decisionali**
  - **Reti Neurali**
  - **SVM (Support Vector Machines)**

# Alberi di Decisione

- Lo scopo è, come in tutti i modelli di apprendimento induttivo da esempi, **imparare la definizione di anomalia** espressa in termini di albero di decisioni
- Gli elementi da considerare in sede decisionale sono i valori delle caratteristiche
- Un albero di decisione può essere espressa come una disgiunzione (OR) di implicazioni, aventi il valore della decisione come conclusione.

# Alberi di Decisione

- Un albero di decisione prende in ingresso un elemento  $x \in X$  descritto mediante un insieme di proprietà (coppie attributo-valore) ed emette in uscita una "decisione" binaria ( positivo:anomalo o negativo:non anomalo)
- Nodi ed Archi: corrispondono al test della proprietà che può avere come risultato uno dei  $V_i$



# Alberi di Decisione

- La decisione deve basarsi sull'esame di esempi D:  $x \in X$ , che costituiscono il training set così descritti:
  - ogni esempio è rappresentato da un vettore che rappresenta i valori degli attributi prescelti per descrivere le istanze del dominio  $x: \langle v_1=val_i, v_2=val_j, \dots, v_n=val_m \rangle$  (utilizzando attributi booleani :  $\langle a_1, a_2, \dots, a_N \rangle$   $a_i = \{0, 1\}$  )
  - gli attributi sono proprietà che descrivono gli esempi del dominio
- Gli alberi di decisione hanno il potere espressivo dei linguaggi proposizionali, ovvero
  - qualsiasi funzione booleana può essere scritta come un albero di decisione (e viceversa).

# Alberi di Decisione

## Quando è appropriato usarli?

- L'uso di alberi di decisione è appropriato se:
  - Gli esempi (istanze) sono rappresentabili in termini di coppie attributo-valore.
    - Un albero di decisioni assegna classificazioni booleane ma può essere esteso al caso di funzioni a più valori.
    - Non è comune, ma possibile, l'utilizzo di questa tecnica per apprendere funzioni nel continuo (discretizzando i valori di  $f(x)$ ).
  - Si può rappresentare il concetto da apprendere mediante una forma normale disgiuntiva.
    - I dati di apprendimento possono contenere errori, oppure attributi di cui il valore è mancante.

# Alberi di Decisione: training set

- Il training set è l'insieme completo degli esempi sottoposti al sistema di apprendimento
- Una soluzione semplice sarebbe creare una espressione congiuntiva per ogni esempio e costruire una disgiunzione
  - In tal caso il sistema non avrebbe alcun potere predittivo su esempi non visti
  - L'obiettivo è estrarre uno schema dagli esempi, che sia in grado di estrapolare esempi non visti

# Alberi di Decisione: Algoritmo

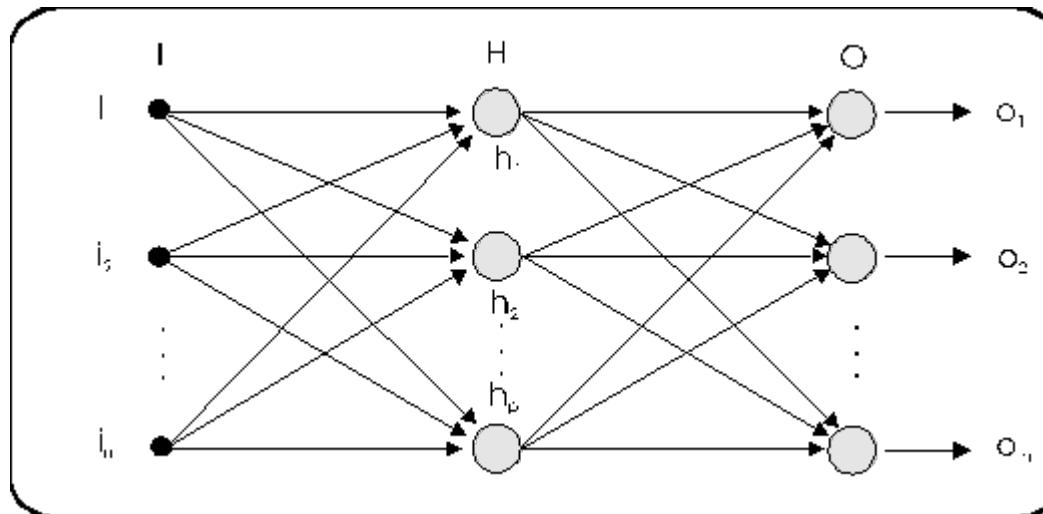
- L'obiettivo è di estrarre **uno schema coinciso**.
- Rasoio di Ockham: l'ipotesi più probabile è la più semplice che sia consistente con tutte le osservazioni.
- Il problema di identificare l'albero *più piccolo* è intrattabile. Tuttavia esistono euristiche che consentono di trovare alberi "abbastanza" piccoli.
- L'idea consiste nell'analizzare **dapprima gli attributi più importanti**, ovvero quelli che discriminano di più.
- Supponendo per ora di poter fare questa scelta ad ogni passo i, l'algoritmo di creazione di un albero delle decisioni da un set di esempi (**training**) è il seguente:

# Alberi di Decisione: Algoritmo

1. Scelgo l'attributo più importante come radice e suddivido gli esempi
2. Per ogni nodo successore:
  - Se ci sono sia es. positivi che negativi ricorsivamente applico l'algoritmo con un attributo in meno
  - Se sono tutti es. positivi metto la foglia SI:Positivo
  - Se sono tutti es. negativi metto la foglia NO:Negativo
  - Se non ci sono esempi restituisco un valore di default calcolato in base alla maggioranza del nodo progenitore
  - Se non ci sono più attributi ma ho ancora esempi misti ho una situazione di errore (rumore) o di reale non determinismo

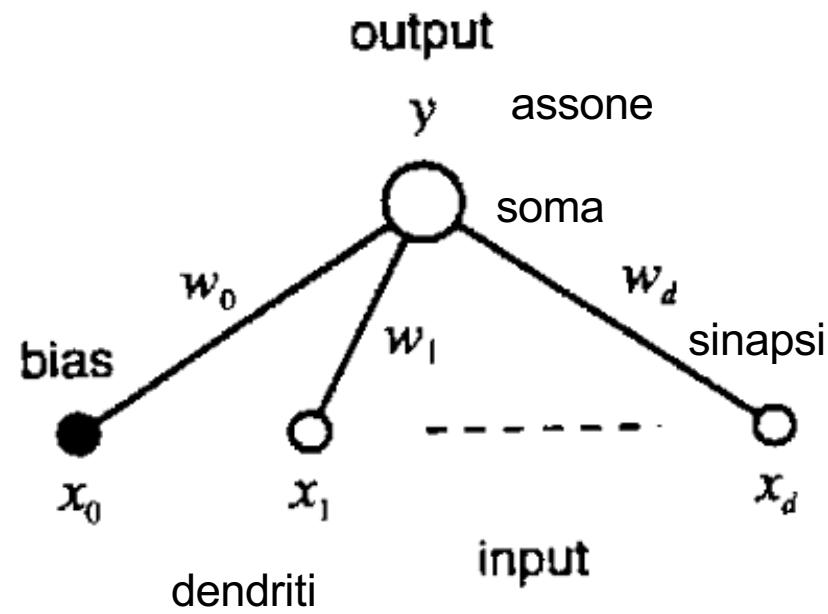
# Reti Neurali

- Hanno il vantaggio di essere sistemi di classificazione universali
- Sistema dinamico avente la topologia di un grafo orientato con nodi, i neuroni artificiali, ed archi, i pesi sinaptici. Il termine rete è riferito alla topologia dei collegamenti tra i neuroni.
- I sensori costituiscono l'input i risultati l'output



# Il neurone artificiale

- Le informazioni vengono elaborate in unità che imitano i neuroni.
- Modello matematico molto semplificato del neurone biologico.
- Ad ogni input  $x_i$  è associato un peso  $w_i$  con valore positivo o negativo per eccitare o inibire il neurone.
- Il bias varia secondo la propensione del neurone ad attivarsi, per variare la soglia di attivazione del neurone.



# Fuzionamento del neurone

1. caricare i valori degli input  $x_i$  e dei pesi relativi  $w_i$
2. calcolare la somma dei valori input pesata con i relativi pesi
3. calcolare il valore della funzione di attivazione  $g$  con il risultato della somma pesata
4. l'output del neurone  $y$  è il risultato della funzione di attivazione

$$y(x) = g\left(\sum_{i=1}^d w_i x_i + w_0\right) = \bar{w}^T \bar{x}$$

# Funzioni di attivazione

Determina la risposta del neurone.

A gradino

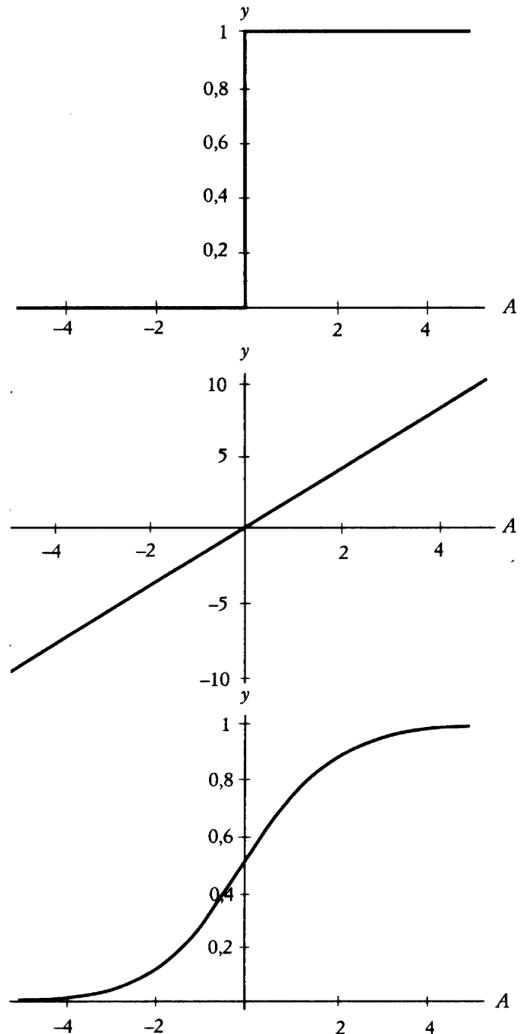
Lineare continua

$$g(A) = \begin{cases} 1 & \text{se } A > 0 \\ 0 & \text{altrimenti} \end{cases}$$

$$g(A) = kA$$

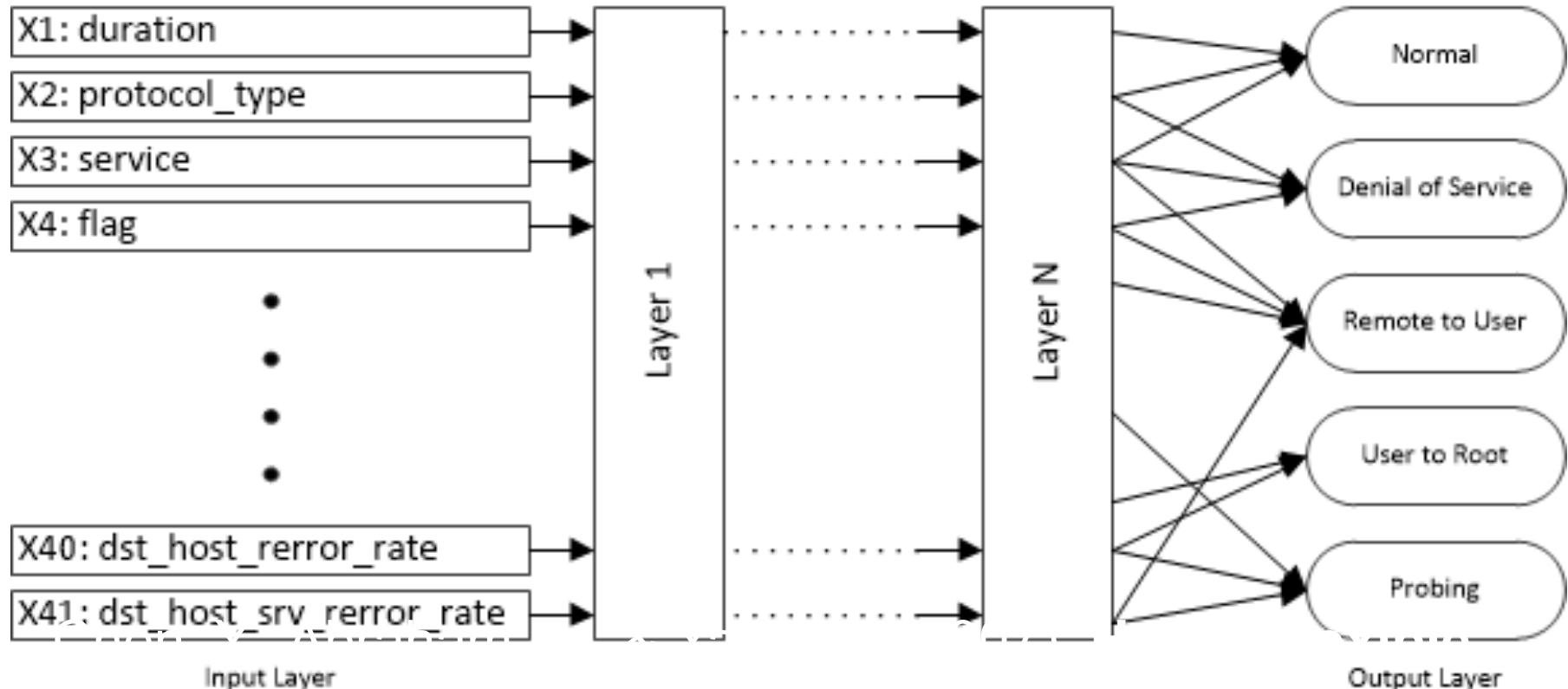
Sigmoide o logistica  
valori positivi, continua e derivabile

$$g(A) = \frac{1}{1 + e^{-A}}$$



# Esempio di rete neurale

Target della rete: individuazione della tipologia di attacco

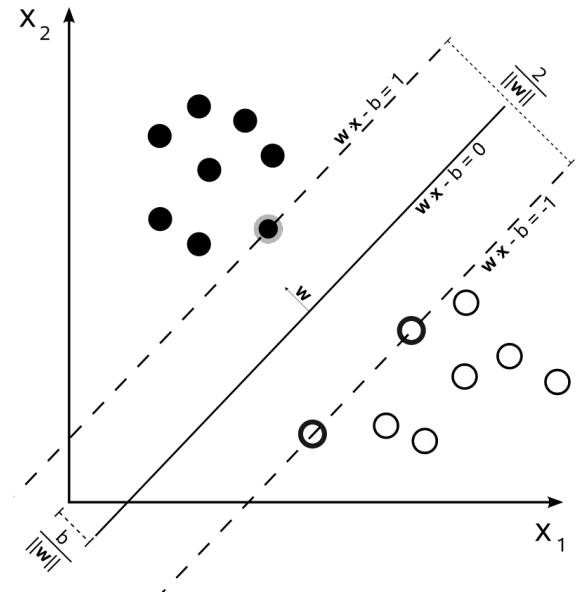


# Support Vector Machines

- Una SVM è un classificatore binario che apprende il confine fra esempi appartenenti a due diverse classi.
- Proietta gli esempi come punti in uno spazio multidimensionale e cercando un iperpiano di separazione in questo spazio.
- Gli iperpiani in uno spazio multidimensionale sono definiti come l'insieme di punti il cui prodotto scalare con un vettore in quello spazio è costante, dove tale insieme di vettori è un insieme ortogonale (e quindi minimale) di vettori che definiscono un iperpiano.
- L'iperpiano di separazione massimizza la sua distanza (il “margine”) dagli esempi di training più vicini.
  - gli esempi appartenenti a diverse categorie sono chiaramente separati da uno spazio il più possibile ampio.
  - I nuovi esempi sono quindi mappati nello stesso spazio e la predizione della categoria alla quale appartengono viene fatta sulla base del lato dell'iperpiano nel quale ricade.

# Support Vector Machines

- E' possibile per esempio realizzare una separazione lineare nello spazio
- I vettori che definiscono gli iperpiani possono essere scelti come combinazioni lineari con parametri  $\alpha_i$  delle immagini dei vettori delle caratteristiche  $x_i$
- Proprietà generali delle SVM:
  - Capacità di gestire dati con molte caratteristiche descrittive,
  - compattamento dell'informazione



# SVM, Uso

- Per usare una SVM si ha bisogna scegliere una funzione di *Kernel* che la corrispondente *funzione di trasferimento* nelle reti neurali
- In pratica, le mappature utilizzate dalle SVM sono fatte in modo tale che i prodotti scalari dei vettori delle coppie di punti in ingresso siano calcolati facilmente in termini delle variabili dello spazio originale, attraverso la loro definizione in termini della funzione kernel  $k(x, y)$ .
- La funzione Kernel va scelta accuratamente per un tipo di problema: è sempre possibile mappare l'input in uno spazio di dimensione maggiore del numero di punti del training set e produrre un classificatore perfetto

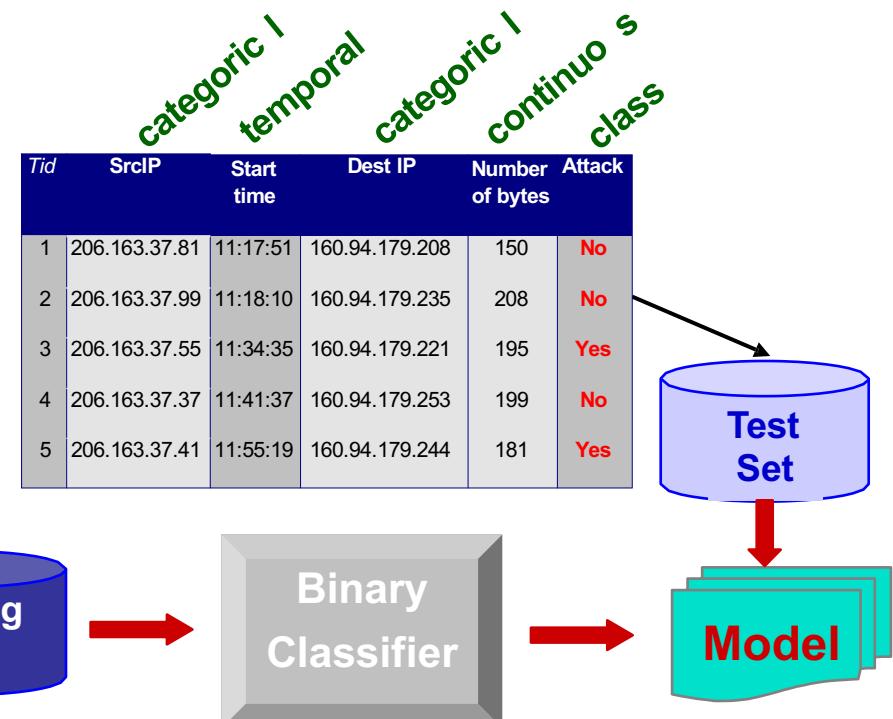
# Note sui Trainable Learners

- Sia le reti neurali che la SVM, prendono in input un insieme di etichette dei dati di training ed alcuni modelli parametri specializzati che devono essere settati.
- In generale i parametri specializzati, sono settati da un esperto umano o da un insieme di procedure automatiche usando cross-validation basate su parameter scanning

# Anomaly Detection all'opera

Tid	SrcIP	Start time	Dest IP	Dest Port	Number of bytes	Attack
1	206.135.38.95	11:07:20	160.94.179.223	139	192	No
2	206.163.37.95	11:13:56	160.94.179.219	139	195	No
3	206.163.37.95	11:14:29	160.94.179.217	139	180	No
4	206.163.37.95	11:14:30	160.94.179.255	139	199	No
5	206.163.37.95	11:14:32	160.94.179.254	139	19	Yes
6	206.163.37.95	11:14:35	160.94.179.253	139	177	No
7	206.163.37.95	11:14:36	160.94.179.252	139	172	No
8	206.163.37.95	11:14:38	160.94.179.251	139	285	Yes
9	206.163.37.95	11:14:41	160.94.179.250	139	195	No
10	206.163.37.95	11:14:44	160.94.179.249	139	163	Yes

*Misuse Detection – Costruzione di modelli predittivi*

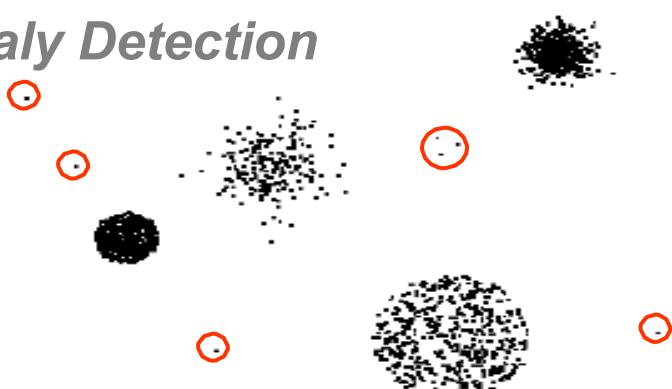


*Inferenza di attacchi tramite associazione di regole note*

Rules Discovered:

{Src IP = 206.163.37.95,  
Dest Port = 139,  
Bytes ∈ [150, 200]} --> {ATTACK}

*Anomaly Detection*

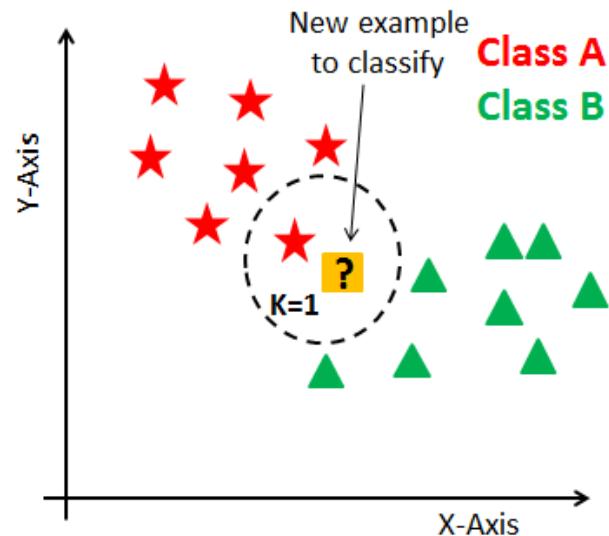


# Problemi nei modelli supervisionati

- Generare una ground truth affidabile, in grado di realizzare un buon modello di «normalità» o di «anomalia» è complicato
- E' difficile garantire che non vi siano attacchi nel periodo in cui si raccolgono i dati di traffico normale
- Spesso i dati di anomalia risentono di un certo grado di artificialità
- In genere il numero di eventi anomali raccolti è largamente inferiore al numero di osservazioni normali e questo può influenzare negativamente il classificatore

# Apprendimento instance-based: K-Nearest Neighbors (k-NN)

- Calcola una distanza approssimativa tra punti diversi identificati dai vettori di input e assegna i punti non etichettati alla classe dei suoi  $k$  vicini meno distanti.
- Il parametro  $k$  influenza le prestazioni e la precisione.
- k-NN prevede una logica di apprendimento instance-based (basata su esempi).
  - **Non è prevista alcuna fase di addestramento del modello**
  - Vengono solo individuati esempi (instances) di vettori di input pre-classificati sulla base dei quali vengono classificate nuove istanze.



# Clustering per Detection Non Supervisionata

~~Misuse Detection~~

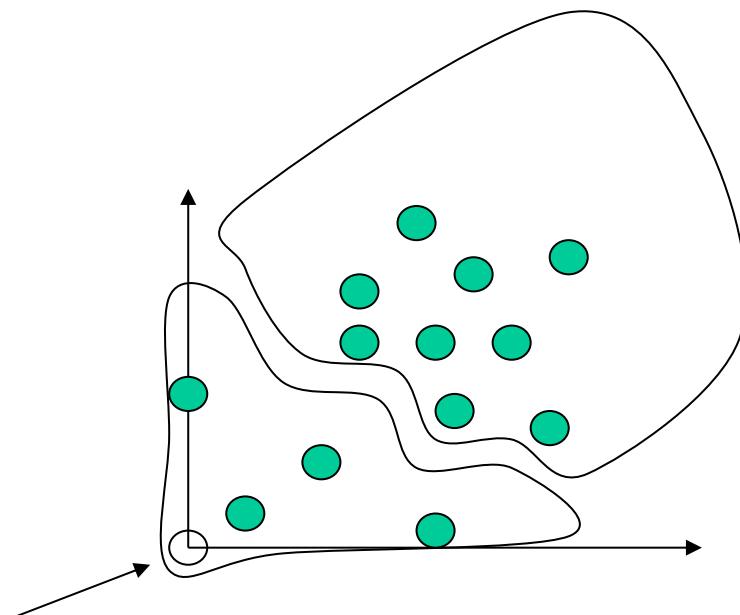
~~Anomaly Detection.~~



- Costruzione di un modello di training basato su dati non etichettati
- Determina outliers (anomalie) che si celano fra questi dati.

# Clustering

- Suddivide esempi non etichettati in sottoinsiemi disgiunti (**cluster**), tali che:
  - Gli esempi in uno stesso gruppo sono “molto” simili in termini di «distanza»
  - Gli esempi in gruppi diversi sono “molto” differenti
- Scopre **nuove categorie** in modo **non supervisionato**
  - No ground truth
  - No labels



# Metriche per la distanza

- Nota: se la distanza è normalizzata tra 0 e 1, la similarità  $sim(x, y)$  è data da  $1-d(x, y)$
- Distanza euclidea (norma  $L_2$ ):

$$L_2(\vec{x}, \vec{y}) = \sqrt{\sum_{i=1}^m (x_i - y_i)^2}$$

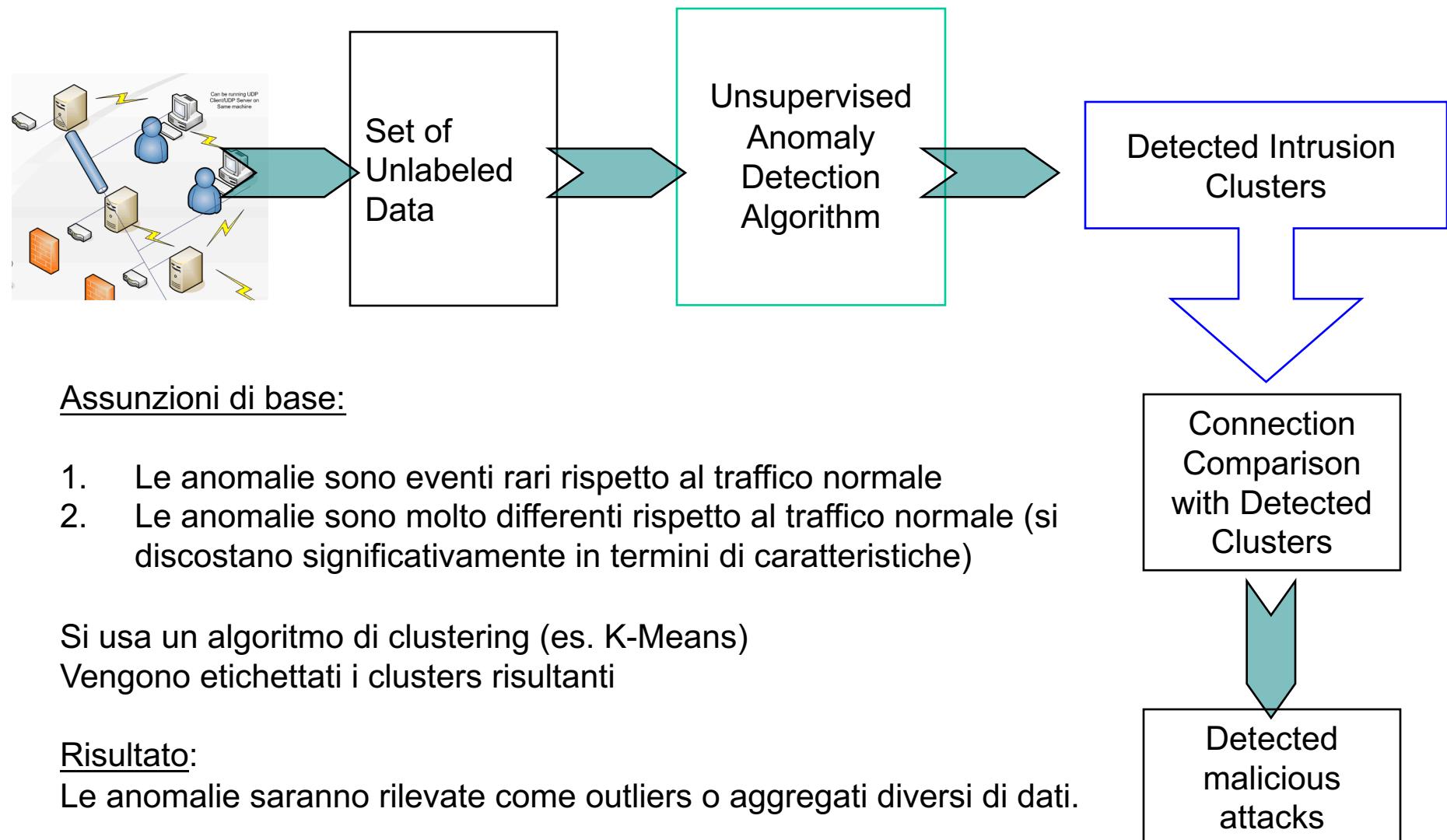
- Norma  $L_1$  (o distanza di Manhattan):

$$L_1(\vec{x}, \vec{y}) = \sum_{i=1}^m |x_i - y_i|$$

- Distanza di Mahalanobis:
  - dissimilarità tra due vettori aleatori  $x$  e  $y$  con stessa funzione di densità di probabilità e con matrice di covarianza  $S$

$$d(\vec{x}, \vec{y}) = \sqrt{(\vec{x} - \vec{y})^T S^{-1} (\vec{x} - \vec{y})}.$$

# Clustering per Intrusion Detection



# K-means

- Assume istanze a valori reali
- I cluster sono basati su **centroidi** o media dei punti in un cluster  $c$ :

$$\mu(c) = \frac{1}{|c|} \sum_{\vec{x} \in c} \vec{x}$$

- Le istanze vengono riassegnate ai cluster sulla base della distanza rispetto ai centroidi dei cluster attuali

# Algoritmo K-means

**K-means**(distanza  $d$ , insieme delle istanze  $X$ )

**Seleziona**  $k$  istanze a caso  $\{s_1, s_2, \dots, s_k\} \subseteq X$  come **semi**.

**Finché** il clustering non converge o si raggiunge criterio di stop:

Per ogni istanza  $x \in X$ :

**Assegna**  $x$  al cluster  $c_j$  tale che  $d(x, s_j)$  è minimale

**Aggiorna** i semi al centroide di ogni cluster, ovvero

per ogni cluster  $c_j$ :  $s_j = \mu(c_j)$

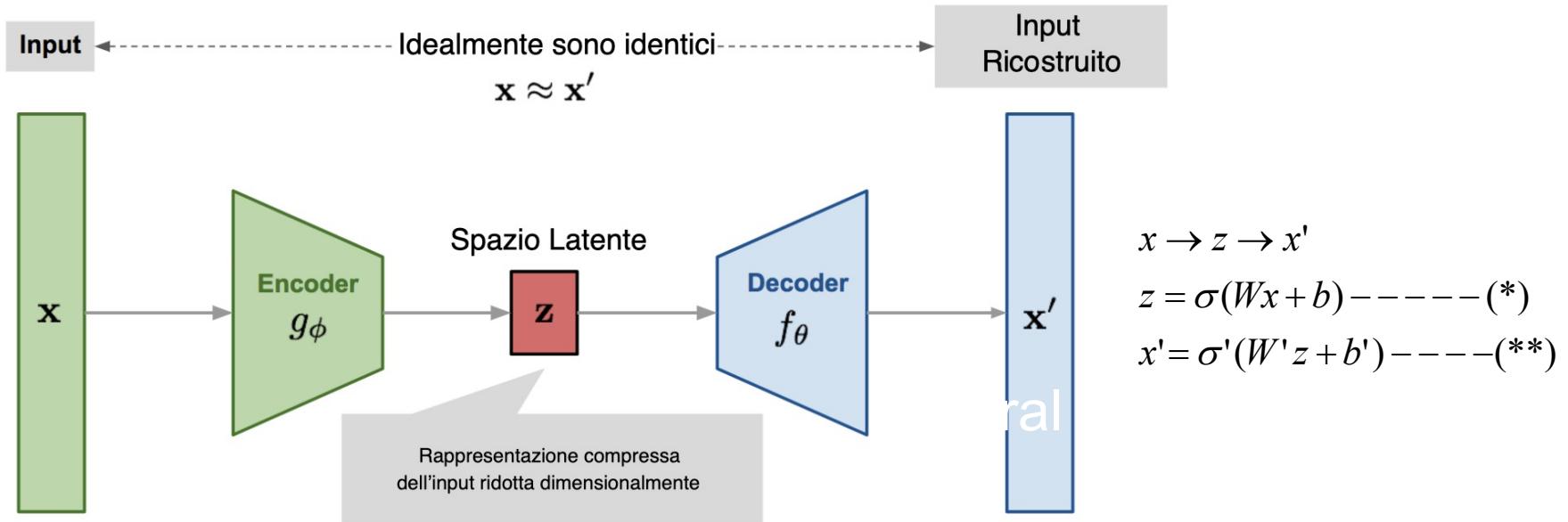
L'obiettivo di k-means è di **minimizzare la somma del quadrato della distanza** di ciascun punto in  $X$  rispetto al centroide del cluster cui è assegnato:

$$\sum_{i=1}^k \sum_{x \in c_i} d(\vec{x}, \mu_i)^2$$

# Autoencoder

Un autoencoder è una rete neurale feedforward che impara a ricostruire il proprio input (corrotto dal rumore) nel proprio output.

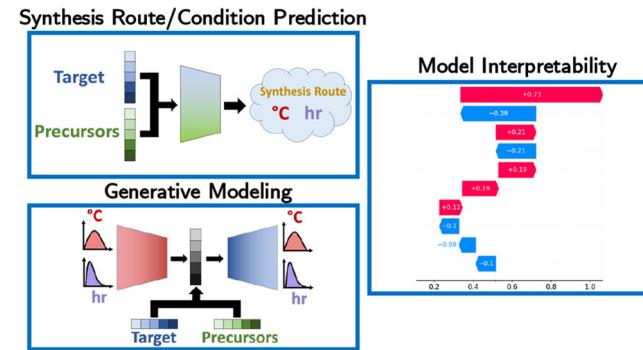
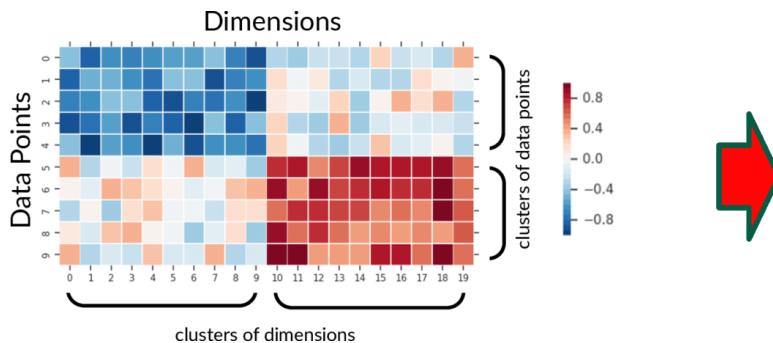
- Addestrato per minimizzare l'errore di ricostruzione
- La componente da input ai successivi layer nascosti fino allo spazio latente corrisponde a un codificatore
- I layer nascosti in uscita dopo lo spazio latente corrispondono a un decoder.
- Ingresso e uscita hanno la stessa dimensione.



# Autoencoder Variazionali

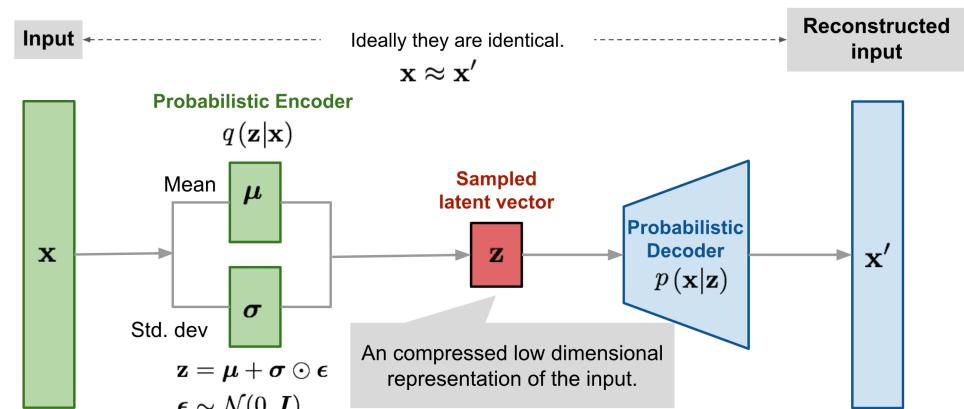
Idealmente, abbiamo bisogno di una soluzione in grado di:

- apprendere distribuzioni complesse di dati
- gestire dati ad alta dimensionalità
- catturare rappresentazioni latenti che sono interpretabili
- fornire approfondimenti sulle caratteristiche sottostanti che contribuiscono alle anomalie



# Variational Autoencoder (VAE)

- Idea di base: rendere **probabilistiche** le componenti encoder e decoder
- Ogni variabile  $z$  nello **spazio latente** è estratta da una **distribuzione di probabilità** dipendente dall' input,  $x$ , e la ricostruzione è effettuata in maniera probabilistica da  $z$ .
- Un **encoder probabilistico** dato un punto  $x$  produce una distribuzione  $q(z|x)$  su tutti i possibili valori di  $z$
- In maniera analoga un **decoder probabilistico**, data una rappresentazione latente  $z$  produce una distribuzione  $p(x|z)$  su tutti i possibili valori di  $x$
- Ottengo implicitamente una riduzione dimensionale



[1] Diederik P Kingma, Max Welling, Auto-Encoding Variational Bayes (2014) <https://arxiv.org/abs/1312.6114>

[2] Cinelli, L.P., Marins, M.A., Da Silva, E.A.B., Netto, S.L.: Variational Methods for Machine Learning with Applications to Deep Networks. Springer, Nature (2021)

# Features come distribuzioni di probabilità

L'apprendimento di un modello probabilistico di ciascuna caratteristica (espresso da un vettore di media e varianza logaritmica) facilita la comprensione della struttura e della variabilità sottostanti

- si possono dedurre relazioni complesse tra i dati di input e le variabili latenti che portano a una sorta di spiegabilità
- più parametri da regolare danno più controllo su come vogliamo modellare la nostra distribuzione latente

101110

010111

000111

101110

010111

000111

101110

010111

000111

101110

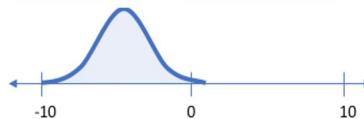
010111

000111

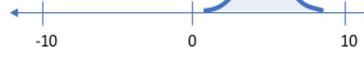
Packet Rate (discrete value)



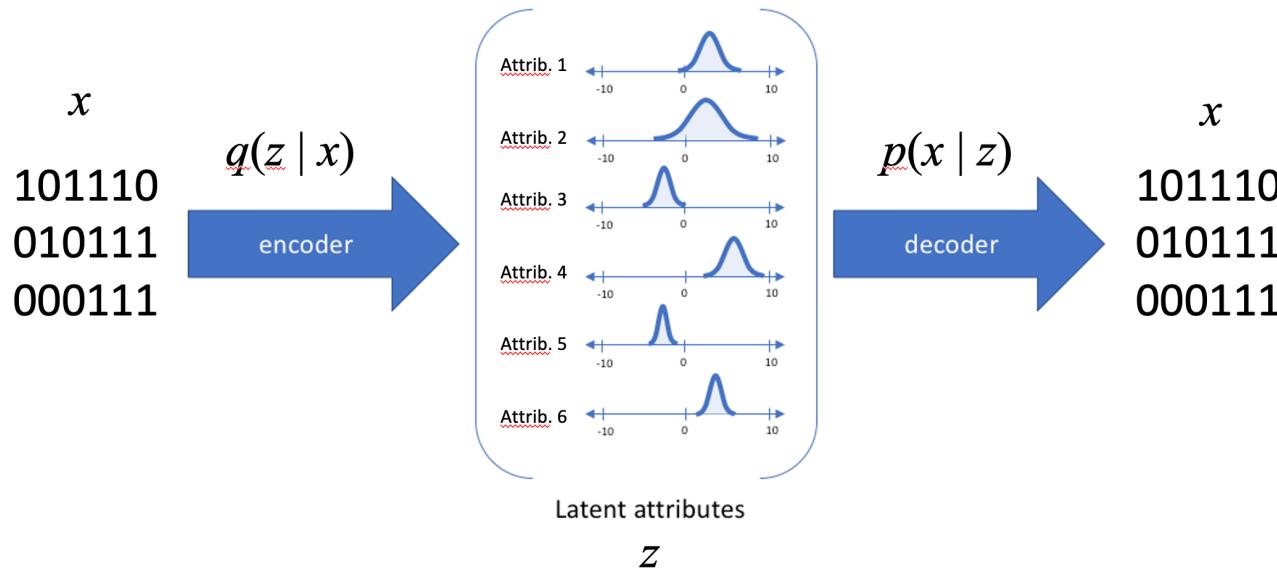
Packet Rate (distribution)



vs.

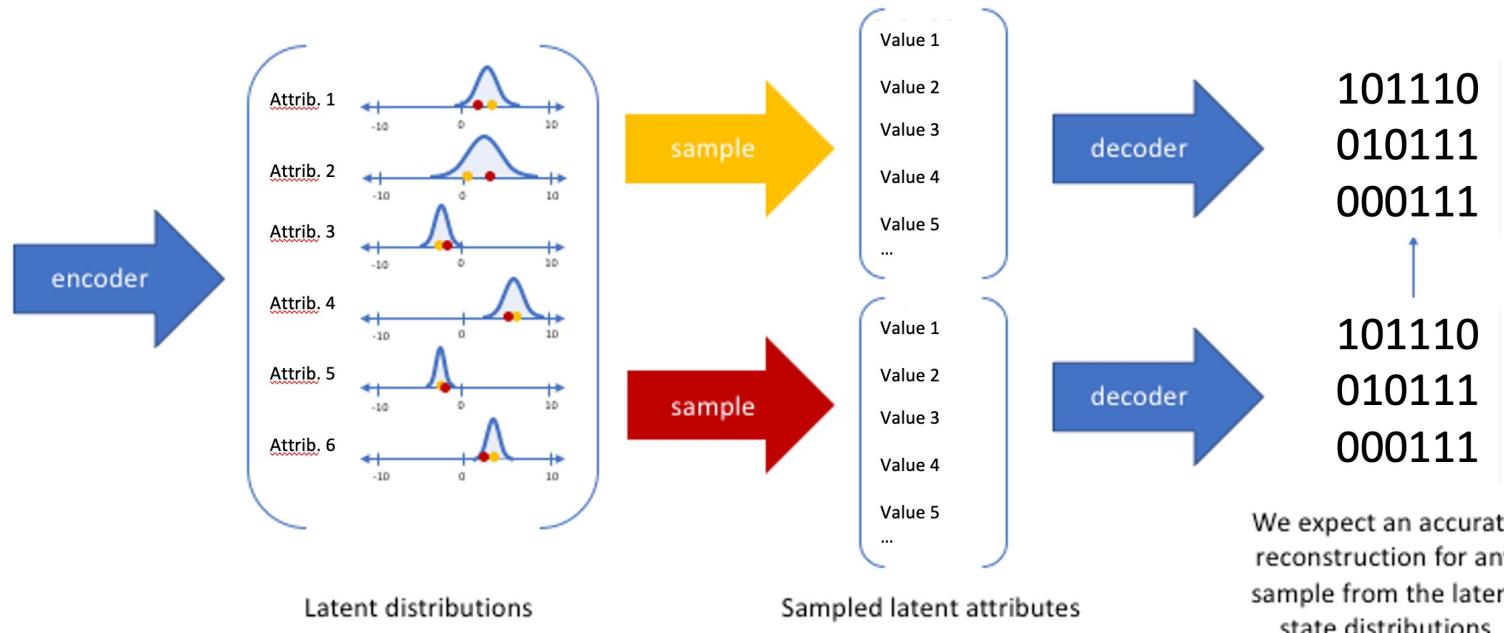


# VAEs come anomaly detectors



- Può essere facilmente utilizzato nel rilevamento di anomalie osservando l'errore di ricostruzione
- L'errore viene propagato all'indietro per correggere i parametri della rete
- L'addestramento è implicitamente regolarizzato per evitare overfitting e lo spazio latente è meglio organizzato
- La capacità di lavorare con uno spazio più fluido e continuo può portare a risultati più stabili e accurati

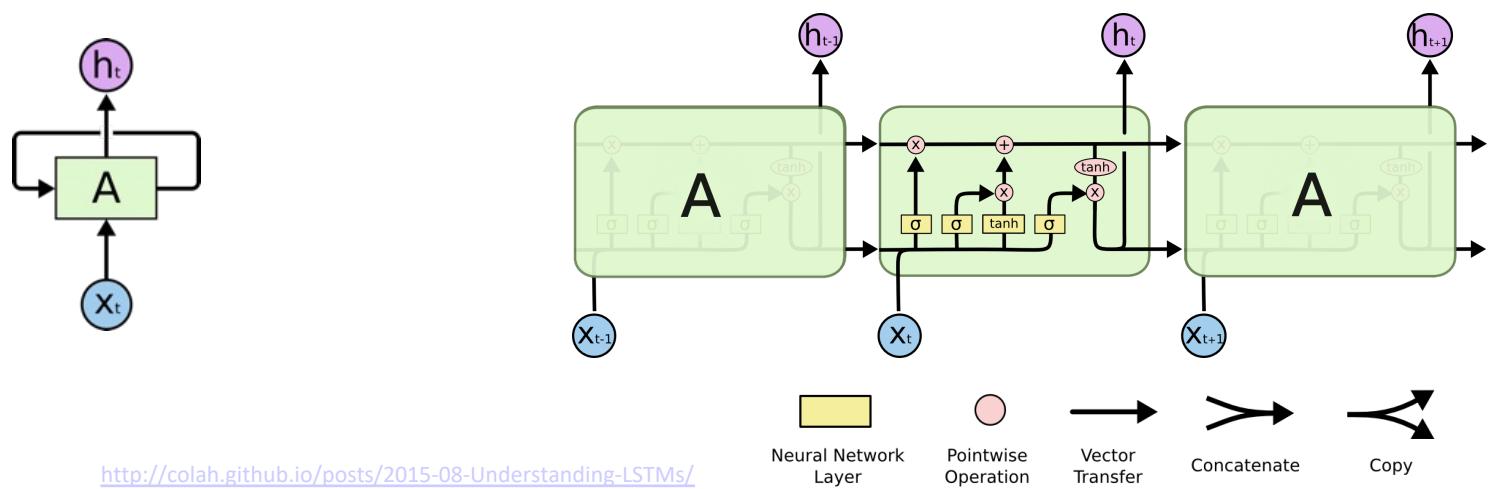
# Features come distribuzioni di probabilità



- Punti dati simili si trovano più vicini nello spazio latente rendendo le misure di somiglianza estremamente più affidabili.

# Riconoscere fenomeni temporali: LSTM

- La rete LSTM (Long Short-Term Memory) è un tipo di rete neurale ricorrente, ma ha una formulazione unica per affrontare il problema del vanishing gradient.
- L'obiettivo è fornire alle RNN una memoria a breve termine che possa durare migliaia di timestep, quindi una “memoria a breve termine lunga”, in modo che le reti risultanti siano particolarmente efficaci per lavorare con lunghe sequenze di dati.



# Anomaly Detection: problemi

- Ispezione dei flussi di traffico online e in tempo reale
- L' individuazione di eventi anomali da variazioni statistiche volumi rileva solo attacchi "noisy" (DDoS)
- Enormi quantità di dati da analizzare
- Meccanismi classification-based:
  - Supervised
  - Semi-supervised
  - Unsupervised (self learning)
- Riconoscimento nuovi attacchi (0-day)
- Detection, recovery & Prevention



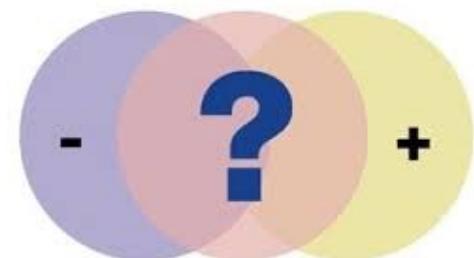
**“Individuare un'anomalia on-line su un interfaccia high-speed è come cercare un ago in un pagliaio in fiamme”**

# Prestazioni architetture di detection

- I parametri principali che caratterizzano le prestazioni di una soluzione di detection rispetto alla sua architettura sono relativi a:
  - Implementazione HW (ASIC)
  - Throughput di un tipico NIDS, nell'ordine delle decine di Gbps
    - E.g., 32 nsec per TCP SYN packet di 40 bytes
  - Scalabilità rispetto ai volumi di traffico
  - Resilienza nei confronti di attacchi
  - Presenza di SPOF

# Prestazioni algoritmi di detection

- I parametri prestazionali che caratterizzano un algoritmo di detection riguardano le situazioni di “falsi positivi” e di “falsi negativi”.
- Si ha un “falso positivo” quando il sistema rileva un attacco in situazione di traffico legittimo.
- D'altra parte la situazione di “falso negativo” si presenta in occasione di un reale attacco non rilevato. Tale situazione non è facilmente rilevabile, se non a posteriori, analizzando le evidenze dei sistemi che hanno subito l'attacco.
  - Allarme: A; Intrusione: I
  - Detection (true alarm) rate:  $P(A|I)$ 
    - o False negative rate  $P(\neg A|I)$
  - False alarm (aka, false positive) rate:  $P(A|\neg I)$ 
    - o True negative rate  $P(\neg A|\neg I)$
- È indispensabile che l'IPS non generi falsi negativi, perché significa che gli attacchi noti non vengono rilevati.



# Confusion matrix

- Consideriamo un classico problema di classificazione binario in cui riportiamo i risultati predetti dal classificatore rispetto alla situazione reale:
- Veri positivi (TP): esempi positivi correttamente classificati come positivi
- Veri negativi (TN): esempi negativi correttamente classificati come negativi
- Falsi positivi (FP): esempi negativi erroneamente classificati come positivi
- Falsi negativi (FN): esempi positivi erroneamente classificati come negativi

		Realtà	
		Positivo	Negativo
Predizione	Positivo	TP	FP
	Negativo	FN	TN

# Accuracy, precision, recall, F-score

Predizione

		Realtà	
		Positivo	Negativo
Predizione	Positivo	TP	FP
	Negativo	FN	TN

$$\text{Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}}$$

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$$

$$F1 - Score = 2 * \frac{\text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}}$$

## Accuracy

indica l'accuratezza del modello come dice il nome.

## Precision

è l'accuratezza della predizione delle classi positive.

## Recall o sensitivity

indica il rapporto di istanze positive correttamente individuate (sul totale dei casi)

## F-score

media armonica di precision e recall

- attribuisce un peso maggiore ai valori piccoli
- Questò fa sì che un classificatore ottenga un alto punteggio F1 solo quando precisione e recupero sono entrambi alti.

# Sandboxes

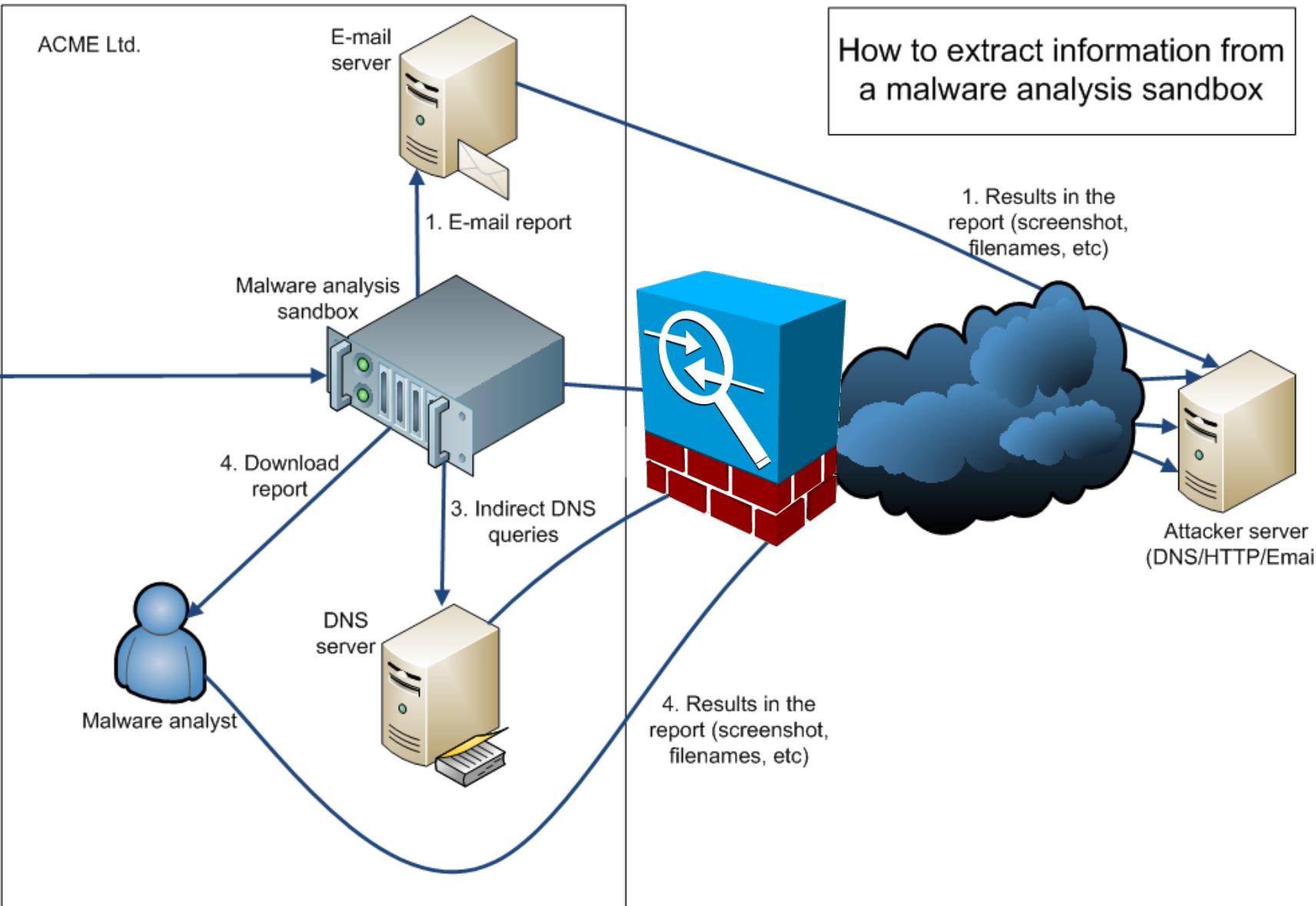
- Sistemi integrati con la soluzione FW che mettono a disposizione ambienti di virtualizzazione completamente isolati per l'individuazione dinamica del malware
- Cattura e blocco di potenziale malware
  - Il potenziale malware catturato viene eseguito su una VM isolate nel Sistema di sandboxing
  - La VM viene analizzata attraverso scansioni.
  - Memoria, chiamate di Sistema, connessioni di rete e accessi al filesystem vengono esaminate

The screenshot shows a web browser displaying the Anubis platform at [https://anubis.iseclab.org/?action=result&task\\_id=1efd374facec384d4d1edb0f5cf95dc8&call=first](https://anubis.iseclab.org/?action=result&task_id=1efd374facec384d4d1edb0f5cf95dc8&call=first). The interface includes a header with the Anubis logo and navigation links for Home, Advanced Submission, Clustering, News, About, Sample Reports, and Links. Below the header is a 'Task Overview' section containing the following information:

Task ID:	1efd374facec384d4d1edb0f5cf95dc8
URL:	<a href="http://myteenmovies.net/t.php?id=6113600">http://myteenmovies.net/t.php?id=6113600</a>
MDS:	b439e68c2cc0031c51bfe0c29ac1746
<b>Analysis Submitted:</b>	2011-08-28 07:10:46
<b>Analysis Started:</b>	2011-08-28 07:10:47
<b>Time Remaining:</b>	7 minutes and 50 seconds (0 jobs in queue)

A progress bar at the bottom indicates "2.08 %".

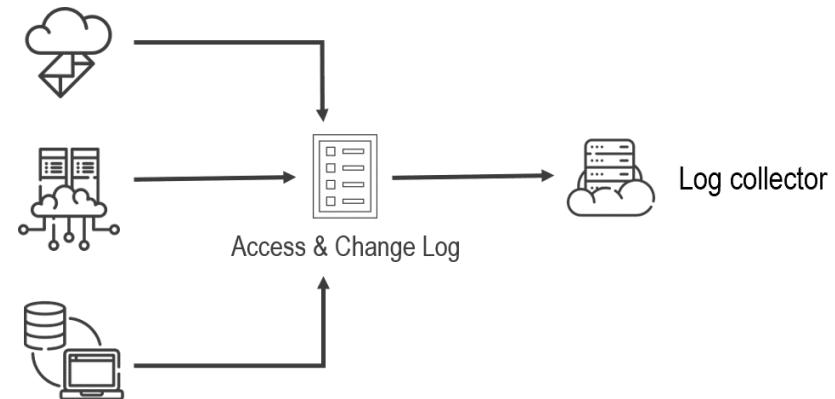
# Sandboxes



# Sistemi di Log Management

Sistemi di raccolta remota dei log da sistemi multipli:

- Controllo completo sullo stato degli host e dei servizi
  - Una suite di Log Management ti permette di notare eventuali comportamenti insoliti che potrebbero rivelarsi indizi di pericolo.
- Analisi dei problemi emersi nel sistema
  - Mediante una copia remota dei file di Log è possibile analizzare eventuali problemi riscontrati su di un dato sistema, anche se il sistema non dovesse risultare disponibile.
- Evita la perdita dei log
  - permette di non perdere mai nessun Log, anche a seguito di guasti HW o SW e di risalire alle criticità che hanno generato l'evento.
  - archiviazione legale a norma



# Security Information and Event Management (SIEM)

- Un SIEM è un sistema che combina le funzioni di Security Information Management (SIM) and Security Event Management (SEM).
- La componente SEM gestisce:
  - Monitoraggio in Real-time
  - Correlazione di eventi e threat intelligence
  - Notifiche
  - Console di management e visualizzazione dati
- La componente SIM tratta:
  - Raccolta e memorizzazione a lungo termine logs eventi
  - Analisi e reporting dei dati di logging



# SIEM Workflow



- L'attività di un sistema SIEM si articola in 5 fasi consecutive che partono dalla raccolta dei dati e che ne prevedono il successivo trattamento

# SIEM Workflow

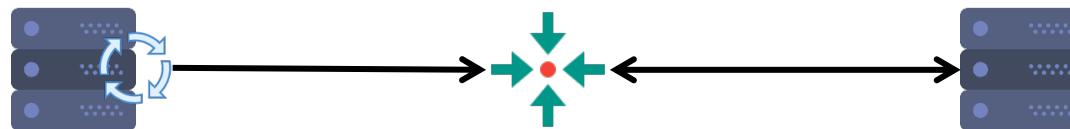


- Il SIEM acquisisce i dati degli eventi da un'ampia gamma di fonti nell'intera infrastruttura IT di un'organizzazione, compresi gli ambienti on-premises e cloud.
- I dati dei registri eventi di utenti, endpoint, applicazioni, origini dei dati, carichi di lavoro cloud e reti, nonché i dati provenienti da hardware e software di sicurezza quali firewall o software antivirus, vengono raccolti, correlati e analizzati in tempo reale.
- le soluzioni SIEM eseguono un certo numero di funzioni di aggregazione, consolidamento e ordinamento dei dati al fine di individuare le minacce e aderire ai requisiti di conformità delle informazioni.

# SIEM Workflow



- Metodi di raccolta dei dati dalle fonti



- **Aggregazione:** per raccogliere i dati insieme nel loro insieme in un unico repository
- **Normalizzazione:** per creare record coerenti per tipo e formato

# Normalizzazione

- **Formato di log originario da sorgente 1**

*10:32, 12/3/2017, alsuabim, ad.corporate.com, error, failed login attempt*

- **Formato di log originario da sorgente 2**

*12:45, 3/23/2017, malicious code detected, host1.corporate.com, alsuabim*

- **Log Normalizzato**

*10:32, 12/3/2017, alsuabim, ad.corporate.com, failed login attempt*

*12:45, 23/3/2017, alsuabim, host1.corporate.com, malicious code detected*

# SIEM Workflow



- Collega e correla gli eventi per identificare gli attacchi
- Utilizzando strumenti di analytics avanzata per individuare e comprendere modelli dati complessi, la correlazione eventi fornisce insight utili a individuare e mitigare rapidamente le potenziali minacce
- Alcune soluzioni SIEM integrano anche feed di threat intelligence di terza parte al fine di correlare i propri dati di sicurezza interna con firme e profili di minaccia precedentemente riconosciuti.
- L'integrazione in tempo reale con i feed di threat intelligence consente ai team di bloccare o rilevare nuove tipologie di firme utilizzate negli attacchi.

# SIEM Workflow



- Il SIEM nella sua attività di correlazione consente di costruire nuova conoscenza da multiple fonti di evidenze e rilievi
- Approccio Event based:
  - un singolo evento identifica un attacco
- Approccio Rule based:
  - Se X + Y + Z allora esegui A
  - Se X si ripete 3 volte in un ora, allora esegui Y
- Anomaly based:
  - Se il traffico sulla porta X supera la deviazione standard dei modelli di traffico storici, potrebbe esserci un problema

# SIEM Workflow



- Un SIEM consolida la sua analisi in un'unica dashboard centrale in cui i team di sicurezza monitorano l'attività, assegnano priorità agli avvisi, identificano le minacce e avviano la risposta o la correzione
  - Individuazione della **Severity**

Low	Medium	High	Critical
-----	--------	------	----------
  - **Notifica**: dopo aver identificato una minaccia, opportune notifiche vengono inviate ai security administrators (SOC)
  - **Reazione Automatica**: la maggioranza delle soluzioni SIEM può eseguire script esterni per reagire alle minacce individuate. (Cambio di regole su FW, emission di un Remediation ticket)

# Security Operations Center (SOC)

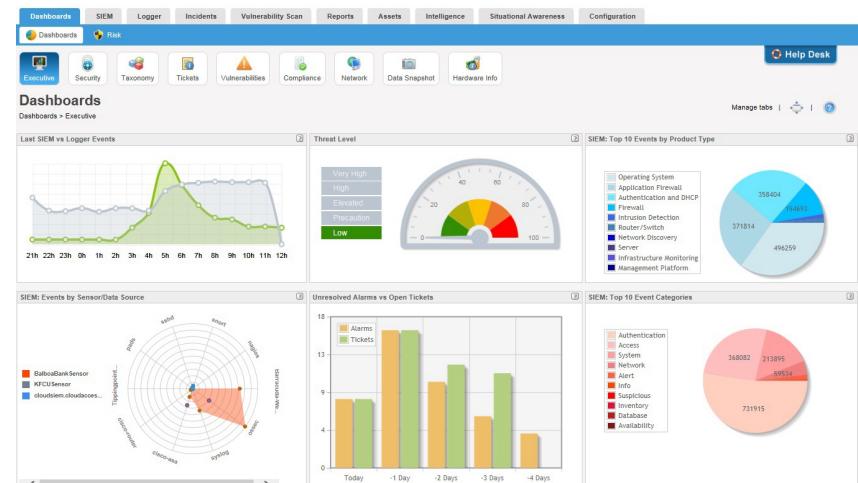


- Le soluzioni SIEM migliorano notevolmente il tempo medio di rilevazione (MTTD) e il tempo medio di risposta (MTTR) dei team di sicurezza IT, scaricando i workflow manuali associati all'analisi approfondita degli eventi di sicurezza.

# SIEM Workflow



- Le soluzioni SIEM possono generare report di conformità in tempo reale per PCI-DSS, GDPR, HIPPA, SOX e altri standard di conformità, riducendo l'onere della gestione della sicurezza e rilevando tempestivamente potenziali violazioni in modo da poterle affrontare.



# SIEM Workflow



- I dati di log raccolti vengono archiviati per future indagini forensi.
- Possono essere conservati i soli dati relativi a problemi di sicurezza
- L'archiviazione consente la conservazione a norma di legge e facilita l'analisi e la ricostruzione della timeline degli eventi associati a un incidente
  - Non equivalente a soluzioni di Log Management

# Funzionalità SIEM

- **Funzionalità di base**
  - Event Consolidation and Normalization
  - Log Retention
  - Alerting eCorrelazione Eventi
  - Dashboards
  - Reporting
- **Fuzionalità avanzate**
  - Threat Feeds
  - Verifiche Compliance
  - Situational Awareness
  - User Analytics
  - Riduzione Falsi Positivei
  - Packet Capture
  - File Integrity Monitoring
  - Geo Location
  - Gestione Workflows
  - Forensic Analysis
  - Ticketing
  - Long Term Retention

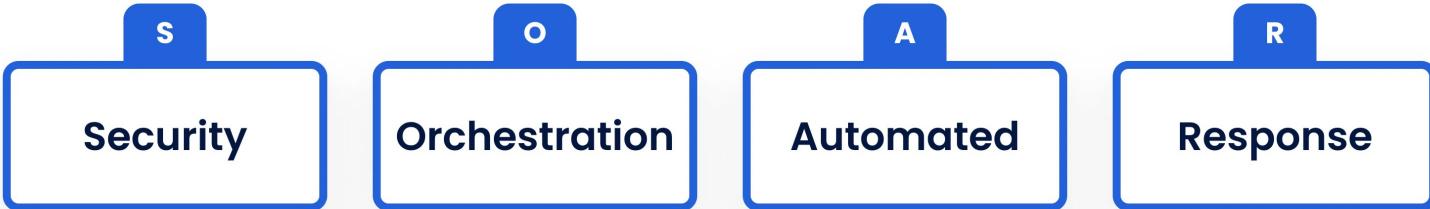
# Automazione basata su AI

- Le soluzioni SIEM di nuova generazione oggi si integrano con sistemi di orchestrazione della sicurezza, automazione e risposta (SOAR), risparmiando tempo e nella gestione della sicurezza
- Utilizzando modelli di deep learning che apprendono automaticamente dal comportamento della rete, queste soluzioni possono gestire complessi protocolli di identificazione delle minacce e di risposta agli incidenti in un tempo inferiore rispetto ai team fisici.
- Le capacità cognitive fornite dall'AI migliorano i processi decisionali del sistema consentendo ai sistemi di adattarsi e crescere man mano che il numero di endpoint aumenta.
- L'AI offre il potenziale per soluzioni che supportano più tipi di dati e una comprensione complessa delle minacce in continua evoluzione.

# SIEM vs. Log Management

Functionality	Security Information and Event Management	Log Management
<b>Log collection</b>	Security related logs	All logs
<b>Log pre-processing</b>	Parsing, normalization, categorization, and enrichment	Indexing, parsing, or none
<b>Log retention</b>	Retain parsed and normalized data	Retain raw log data
<b>Reporting</b>	Security focused reporting	Broad use reporting
<b>Analysis</b>	Correlation, threat scoring, event prioritization	Full text analysis, tagging
<b>Alerting and notification</b>	Advanced security focused reporting	Simple alerting on all logs
<b>Other features</b>	Incident management, analyst workflow, context analysis, etc.	High scalability of collection and storage

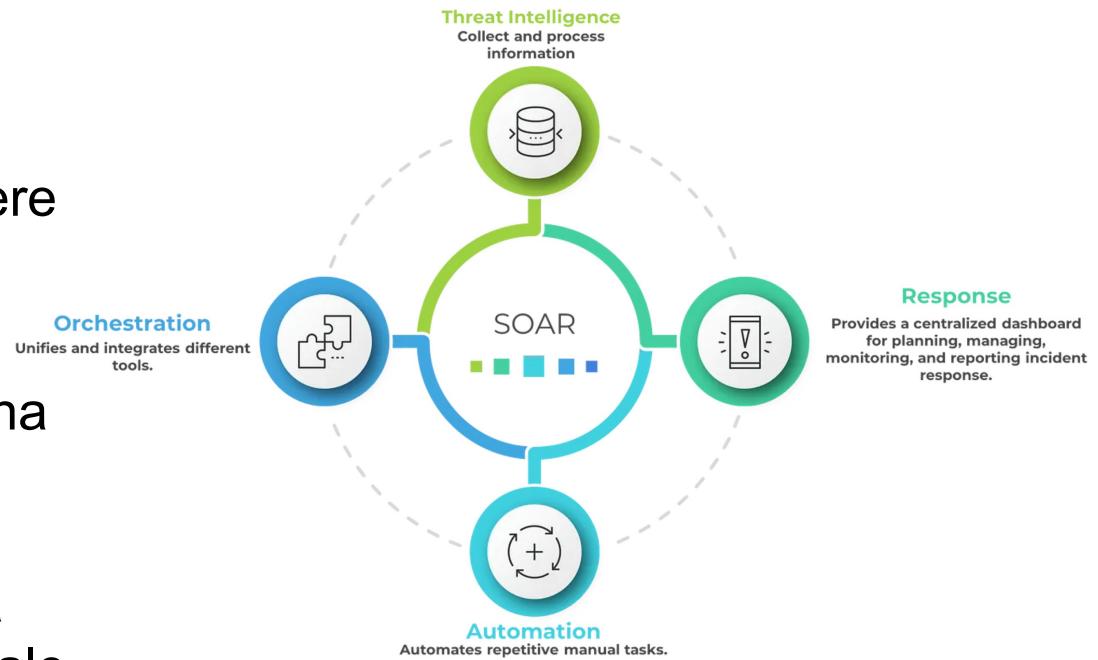
# SOAR



- Una soluzione SOAR ha lo scopo di orchestrare o dispositivi dell'ecosistema di sicurezza per gestire la reazione autonoma
- Può prendere decisioni automatiche su situazioni e incidenti più semplici (in accordo a workflow codificati) senza richiedere l'intervento dell'analista umano
  - Blocco IP, disabilita utenti, raccogli dati di traffico
- In pratica, all'interno dei workflows si concretizzano tutti i processi decisionali che riusciamo ad automatizzare in procedure specifiche
- L'effetto è risparmiare tempo nella reazione soprattutto nei task più ripetitivi in modo da concentrare la necessità di intervento umano solo dove maggiori doti di intuizione e creatività sono necessarie

# Componenti architettura SOAR

- **Threat Intelligence:** Raccoglie ed elabora informazioni per conoscere e prevedere le possibili minacce
- **Orchestrazione:** Combina diversi strumenti di sicurezza, facendoli lavorare insieme per una migliore sicurezza generale
- **Risposta:** Offre un punto di controllo centrale per pianificare, gestire, valutare e riferire su come vengono gestiti gli incidenti
- **Automazione:** Si occupa automaticamente delle attività di routine, rendendo il lavoro della sicurezza più veloce e con meno errori, in modo che il personale possa concentrarsi su attività più importanti.

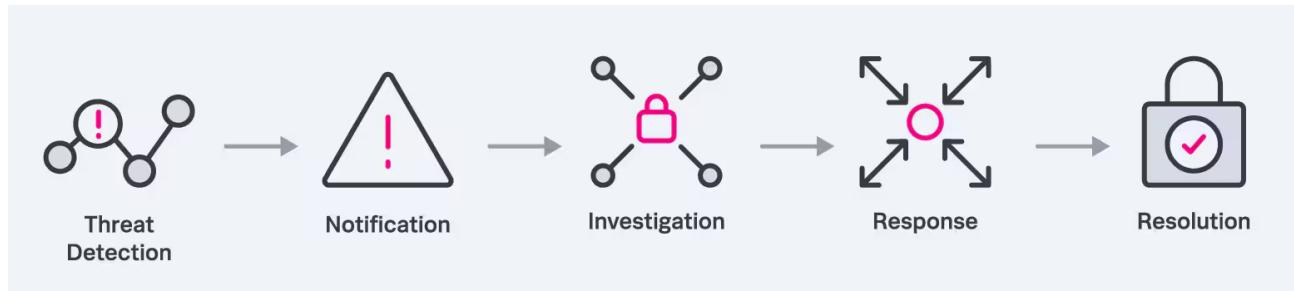


# Componenti architettura SOAR

- La Threat Intelligence è conoscenza aggregata basata su elementi derivati da varie fonti, come malware, traffico e attività utenti, che può aiutarci a decider in merito alle risposte a potenziali pericoli
  - Ad esempio per identificare il malware è possibile usare valori hash, come identificatori unici che rappresentano file o codici specifici.
  - In questo modo si può determinare rapidamente se un file è una minaccia confrontando l'hash con un DB di valori hash di malware noti
  - La combinazione di matching su entità diverse può darci ulteriori informazioni su attacchi in essere o minacce future
- L'efficacia delle azioni di orchestrazione e della loro automazione dipende dagli skill degli esperti che creano i vari playbooks
- L'efficacia della risposta è associata alla disponibilità di dati relativi allo specific caso che il workflow deve andare a gestire, soprattutto quando l'azione è governate da modelli di AI/ML

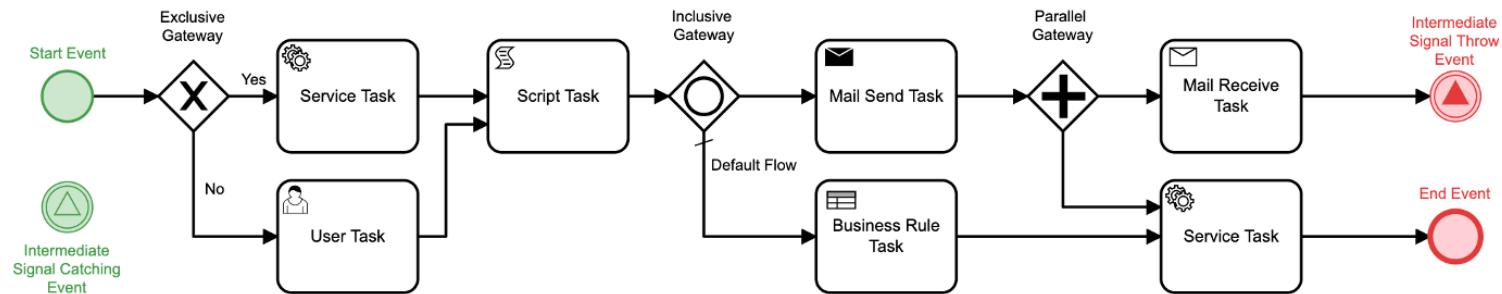
# SOAR Workflows

- Il SOAR lavora basandosi su workflows (chiamati playbooks) che permettono di collegare le azioni delle varie applicazioni e dei vari sistemi attraverso API opportune così come farebbe un analista
- Ogni evento (webhook o API call da una applicazione terza parte) innesca una serie di azioni in cascata per rispondere a un incidente codificato da gestire in accordo a un processo standardizzato
- Un workflow può anche attivare automaticamente altri workflows, creando una struttura di controllo articolata che prevede flussi interconnessi per rispondere a elevati bisogni di automazione
- Un workflow in taluni casi può prevedere la richiesta di conferma da un operatore umano (human in the loop)



# SOAR Workflows

- Per illustrare l'organizzazione di un workflow possiamo far riferimento alo schema seguente



Events		An Event is something that "happens" during the course of a Process.		
	Start Event	The Start Event indicates where a particular Process will start.		End Event
	Intermediate Signal Catching Event	Intermediate Event catching a signal from a preceding event in another workflow.		Intermediate Signal Throwing Event
Tasks		A Task is an atomic Activity within a Process flow. A Task is used when the work in the Process cannot be broken down to a finer level of detail.		
	Service Task	A Service Task is a Task that uses some sort of service, which could be a Web service or an automated application.		User Task
	Mail Send Task	Task where email is used to communicate a status indication or update.		Mail Receive Task
	Script Task	A Script Task defines a set of activities or actions which the task will execute.		Business Rule Task
Gateways		Gateways are used to control how Sequence Flows interact as they converge and diverge within a Process.		
	Exclusive Gateway	Only one of the paths can execute based on the decision logic. Often "yes/no" values.		Inclusive Gateway
	Parallel Gateway	Multiple paths execute without priority order.		Sequence Flow

# SOAR: Considerazioni

- **Principali benefici:**
  - Maggiore efficienza: L'automazione riduce lo sforzo manuale, migliorando la produttività.
  - Risposta rapida: Consente una risposta rapida agli incidenti di sicurezza, riducendo al minimo i danni potenziali.
  - Visibilità centralizzata: Fornisce un'unica piattaforma per il monitoraggio e la gestione degli incidenti di sicurezza, migliorando la consapevolezza della situazione.
- **Scenari d'uso**
  - Automazione della risposta agli incidenti: Automatizza l'intero processo di risposta agli incidenti, dal triage degli alert alla bonifica.
  - Threat Hunting: Automatizza il rilevamento e l'analisi delle minacce per identificare in modo proattivo le potenziali minacce alla sicurezza.
  - Lotta ai cyberattacchi: rilevamento e risposta a phishing, malware e altri attacchi, riducendo al minimo l'impatto su utenti e sistemi.