I.D.S. Intrusion Detection Systems

Francesco Strappaveccia

Corso di Sicurezza

Corso di Laurea in Scienze e Tecnologie Informatiche Polo di Cesena

Università di Bologna

Anno Accademico 2007-2008

I.D.S : Cosa Sono?

- **DEFINIZIONE:** L'Intrusion Detection System o IDS è un dispositivo software e hardware (a volte la combinazione di tutti e due, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare (o prevenire) accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.
- **INTUITIVAMENTE:** Se un Firewall può essere paragonato ad una porta blindata che ”protegge” una casa o il caveau di una banca, l' I.D.S. è il sitema d'allarme che scatta nel momento in cui qualcuno o qualcosa riesce ad oltrepassare questo primo ”ostacolo” avvertendo il proprietario di casa o le forze dell'ordine, magari attuando esso stesso delle contromisure per ”combattere” tale intrusione
- **PRATICAMENTE:** L'I.D.S. non é altro che una suite di Hw e Sw dedicati che vengono installati nella rete che si vuole proteggere per individuare, notificare ed, eventualmente, combattere (automaticamente) attacchi da parte di soggetti con intenti maliziosi.

I.D.S : Obiettivi Teorici

- **Monitorare** ogni sistema e device
- Essere **affidabili** al 100%
- **Riportare** gli attacchi in tempo reale....
- ...con una **diagnisi accurata** del problema
- Eventualmente **segnalare** o addirittura **attivare** le procedure per contrastare tale attacco.

I.D.S. : Attacchi

- Attacchi alle reti informatiche tramite lo sfruttamento di un servizio vulnerabile (Exploit)
- Attacchi attraverso l'invio di dati malformati (Modificazione di pacchetti) e applicazioni malevole
- Tentativi di accesso agli host tramite innalzamento illecito dei privilegi degli utenti
- Accessi non autorizzati a computer e file
- programmi malevoli come virus, trojan e worm

I.D.S : Modus Operandi

- Analizzano in real-time una serie di eventi
- Analizzano gli eventi in base a specifici parametri (o pattern di attacco)
  - *Attacco conosciuto*
  - *Evento non permesso*
  - *Evento anomalo*
  - ...
- Segnalano le anomalie secondo le configurazioni

I.D.S. : Tipologie

- **NIDS:** Network Intrusion Detection System
- **HIDS:** Host Intrusion Detection System
- **DIDS(o HIDS):** Distribuited (o Hybrid) Intrusion Detection System

I.D.S. : I Componenti

- Uno o più **sensori** utilizzati per ricevere le informazioni dalla rete o dai computer ”piazzati” in punti strategici della rete o in macchine particolarmente soggette ad attacchi.
- Una **console** utilizzata per monitorare lo stato della rete e dei computer, tipicamente piazzata all'interno della rete e protetta dall'esterno.
- un **motore** che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle.
- Il motore di analisi si appoggia ad un **database** ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza o pattern di attacchi.

I.D.S : Meccanismi d'Individuazione

I metodi tramite i quali questi software operano sono quelli di analizzare determinate risorse del sistema al fine di trarne poi delle informazioni dalle quali enucleare dei ”comportamenti” non usuali da parte della risorsa monitorata.

Tipicamente vengono analizzati :

- log di sistema
- l'integrità dei file locali (modifiche sospette possono essere sintomo di una avvenuta irruzione)
- pacchetti destinati all'host, sia per reagire a pattern di attacco noti che per accorgersi di un port scan remoto, generalmente prologo di un tentativo di intrusione

Domanda??!!

- Ma **come** questi sistemi riescono a ”capire” che qualcosa ”non va per il verso giusto”??

- **Risposta:** esistono delle tecniche di rilevamento d'intrusione che,basandosi sui dati raccolti dai sensori, riescono a ”scoprire” se ci sono delle anomalie. Queste tecniche possono essere divise in due categorie:
- **Misuse Detection**
- **Anomaly Detection**.

I.D.S : Mimuse Detection I

- Identifica le intrusioni ricercando pattern nel traffico di rete o nei dati generati dalle applicazioni (**log analisys**)
- Codifica e confronta una serie di segni caratteristici (**signature action**) delle varie tipologie di scenari di intrusione conosciute(es.cambi di proprietà di un file, determinate stringhe di caratteri inviate ad un server, etc..)

I.D.S : Mimuse Detection II

- **Svantaggi:**
  - i pattern di intrusione conosciuti richiedono normalmente di essere inseriti manualmente nel sistema
  - non essere in grado di rilevare qualsiasi **futura** (quindi conosciuta) tipologia di intrusione se essa non è presente nel sistema (**0-Day Attack**)
- **Vantaggi:**
  - genera un numero relativamente basso di ”**falsi positivi**”
  - adeguatamente **affidabili** e **veloci**

I.D.S : Anomaly Detection I

- Nata al fine di sopperire alla **mancanza** della precedente di non riuscire a scovare un intruso nel caso questo non usi un attacco già conosciuto
- **Analizza** il sistema alla ricerca di anomalie.
- Vengono fatti dei profili dell'utilizzo normale del sistema ricavati da **misure statistiche** ed **euristiche** sulle caratteristiche dello stesso (es. Utilizzo della CPU di una macchina , traffico dati I/O di un particolare nodo, etc..)
- Stila una serie di **regole** che definiscono lo stato normale del sistema(es. il carico di rete, servizi attivi)

I.D.S : Anomaly Detection II

- **Svantaggi:**
  - selezione delle caratteristiche del sistema da adottare: *non sempre facilmente individuabili*
  - Il monitoraggio del sistema è molto pesante dato che è necessario tenere sottocontrollo molti fattori contemporaneamente per riuscire a classificare correttamente un attacco
- **Vantaggi:**
  - Estremamente flessibili.
  - Possono ”imparare”.

I.D.S. : Reazioni

Una volta scoperta l'intrusione quale è la **reazione** l'I.D.S.?

Gli approcci scelti dai progettisti sono fondamentalmente due:

- **I.D.S. Passivi:** rilevano una violazione della sicurezza informatica, provvedono a **notificarla** all'operatore tramite la console ed eventualmente gli inviano una email
- **I.D.S. Attivi**: provvedono a prendere delle opportune **contromisure** per **eliminare** o comunque **isolare** la violazione informatica

N.I.D.S : Network Intrusion Detection Systems

- Sono degli strumenti informatici, software o hardware, dediti ad **analizzare il traffico** di uno o piu segmenti di una LAN al fine di individuare **anomalie** nei flussi o probabili intrusioni informatiche.
- I piu comuni NIDS sono composti da una o piu **sonde**(**sensori**) dislocate sulla rete, che comunicano con un server (**motore**), che in genere si appoggia ad un **database**.
- Fra le attività anomale che possono presentarsi e venire rilevate da un NIDS vi sono: **accessi non autorizzati**, propagazione di software malevolo, acquisizione abusiva di privilegi appartenenti a soggetti autorizzati, **intercettazione del traffico** (**sniffing**), **negazioni di servizio** (**DoS**).

N.I.D.S. : Perchè?

Sopperiscono alle mancanze dei Firewall infatti:

- Un N.I.D.S. analizza il traffico in entrata ed in uscita che il Firewall **non blocca** classificandolo come ”**affidabile**” (es. impostazione di regole non troppo restrittive sui pacchetti)
- Analizza il traffico di rete **interno**, contrastando per quanto possibile attacchi avvenuti dalla rete locale.
- Sopperisce, se configurato opportunamente, ad **errori di configurazione** del Firewall stesso
- Crea un **log** da cui il sistemista può trarre delle **indicazioni** utili alla configurazione. (o anche lo stesso N.I.D.S.)

N.I.D.S. : Funzionamento I

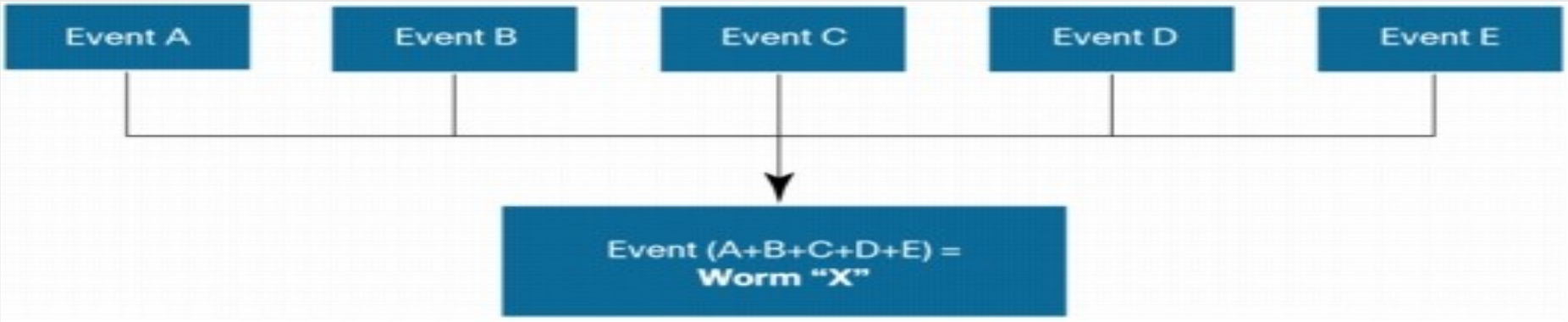
Le logiche su cui i NIDS si basano per riconoscere flussi non autorizzati si distinguono in:

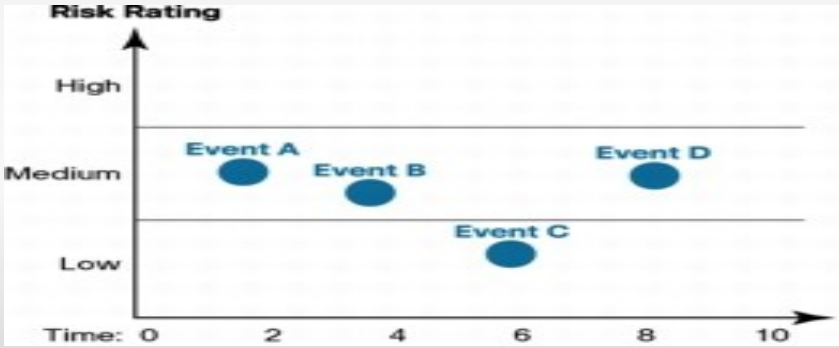
- **Pattern Matching:** il flusso dati viene confrontato con una *signature,* ossia un insieme di condizioni che fanno scattare ”l'allarme”

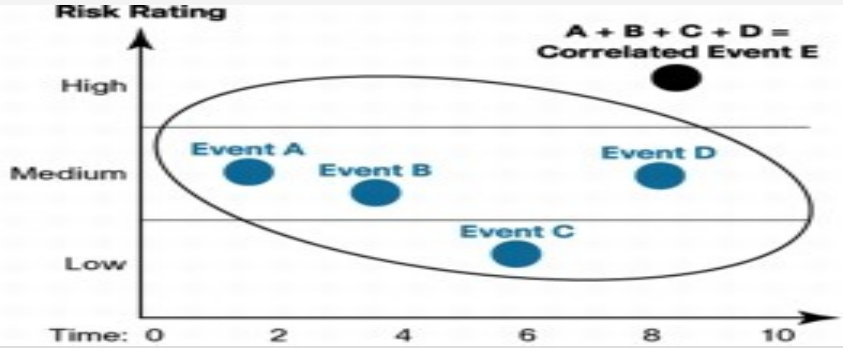
Es. Se un'applicazione sta cercando di connettersi alla porta **12345,** facendo una richiesta ogni 20 ms allora è un tentativo di attacco => Allertare l'amministratore

N.I.D.S. : Funzionamento II

Anomaly Detection: il riconoscimento di flussi sospetti grazie ad un sofisticato meccanismo di funzioni e algoritmi matematici (Es. Clustering). Se uno o piu flussi non rispettano gli standard, il sistema segnala l'errore con il consueto allarme.







N.I.D.S : I Sensori I

Critiche per questo tipo di I.D.S. sono l'**implementazione** e il **posizionamento** dei sensori, infatti:

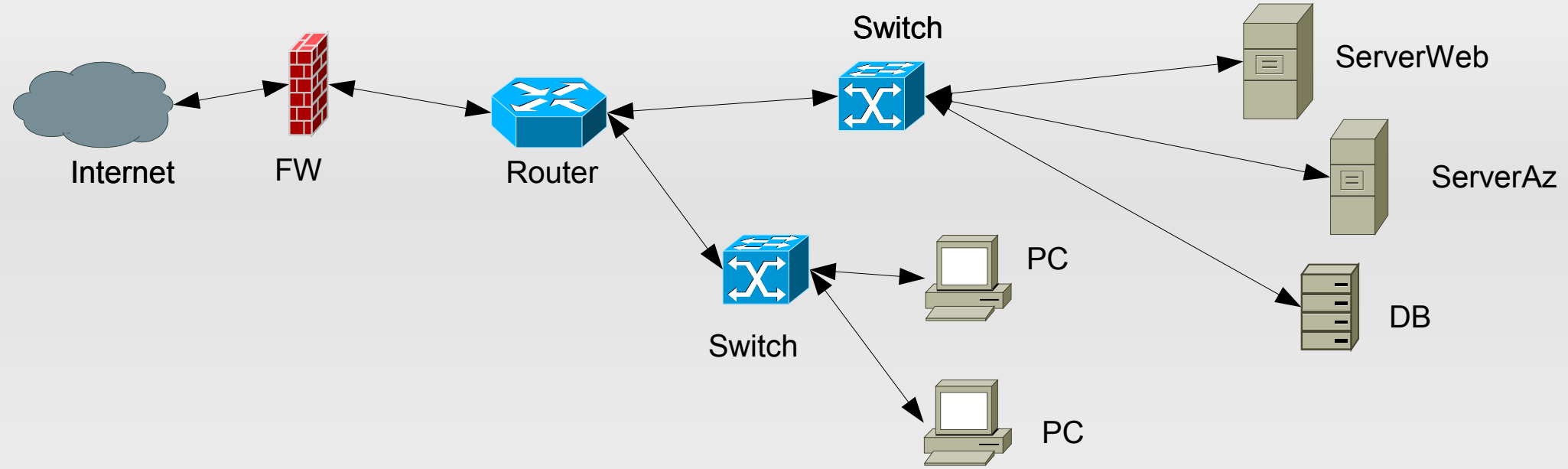
- **Implementazione:**
- In genere i sensori di rete che comunicano con il server centralizzato del NIDS effettuano un **monitoring full-duplex passivo** della rete.
- Praticamente questa operazione, **sniffing**, deve essere **trasparente** sulla rete. Infatti:
  - Permette di rendere i sensori **difficilmente individuabili** dall'esterno.
  - Evita colli di bottiglia che potrebbero ridurre le prestazioni della rete stessa.

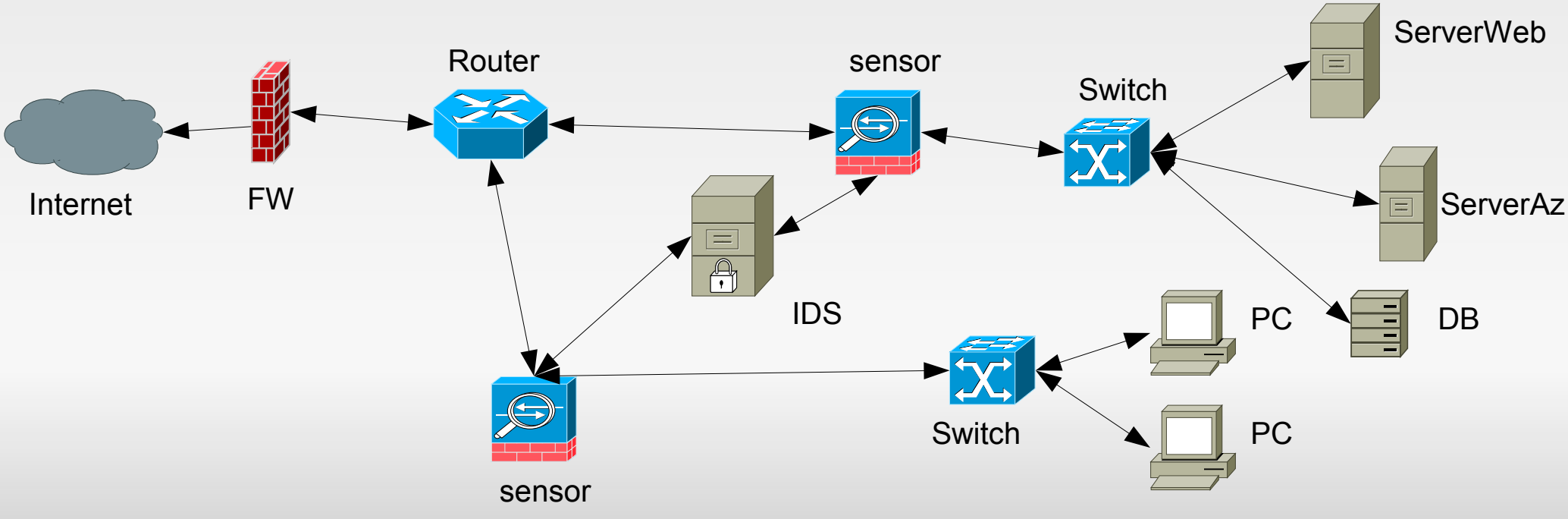
N.I.D.S : I Sensori II

- Tipicamente vengono posizionati dietro un **Network tap.**
- Le signature devo essere costantemente **aggiornate.**

- **Posizionamento:**
- Spesso il partizionamento della rete **non** permette di monitorare **l'intera struttura** con un **unico sensore**
- Per posizionarli è necessario **stimare** il traffico nei vari segmenti
- Se non è possibile monitorare tutto il traffico è necessario piazzare i sensori in punti strategici:
  - Punti di passaggio (**router**, **gateway**)
  - Punti vulnerabili (**server web**, **servizi esposti all'esterno**)
  - Nei Punti sensibili della rete (**DB aziendale**, **Servers interni**)

N.I.D.S : Topologia Sensori





N.I.D.S : Pro vs Contro

- **Pro**
  - sono **difficili** da **rilevare** in quanto agiscono passivamente
  - evidenziano eventuali **errori** nella **configurazione** del sistema
  - evidenziano eventuali **vulnerabilità** della rete
  - permettono di **monitorare** il **comportamento** degli **utent**i interni alla rete
  - rilevano eventuali attacchi provenienti dalla rete interna verso la rete esterna
- **Contro**
  - non sostituiscono l'esistente **staff di sicurezza** in quanto necessitano di costante monitoraggio.
  - non possono analizzare informazioni **criptate**
  - **incrementando** il numero delle **firme** , può essere **ridotta l'efficenza** del NIDS
  - richiedono **notevoli risorse** in termini di **spazio** per l'archiviazione dei log

I.P.S. : (Intrusion Prevention Systems)Uniamo le forze!!

- Come abbiamo notato dalle considerazioni precedenti un N.I.D.S sopperisce alle mancanze di un Firewall e questi alleggerisce, se opportunamente configurato, lo sforzo del sistema di intrusione, filtrando pacchetti e rifiutando connessioni che già dal loro primo tentativo di connessione si dimostrano palesi incipit di attentati maliziosi alla rete.
- Oltretutto questi due strumenti lavorano su **livelli diversi** della pila **ISO/OSI**, quindi la loro integrazione potrebbe essere una buona idea nell'ottica di migliorare la sicurezza di un sistema.
- Quindi One Secure, ora acquisita da Jupiter Networks, nella seconda metà degli **anni '90** realizza questo tipo di sistemi che al loro interno integrano le peculiarità dei Firewall e quelle dei N.I.D.S.

I.P.S. : Come Funzionano

- Il loro funzionamento e il loro comportamento in caso di allarme è del tutto simile a quell di un N.I.D.S solo che estende il suo campo d'azione su più livelli dello stack ISO/OSI.
- Infatti questo tipo di sistemi è in grado di riconoscere tentativi di attacchi malevoli sia a **livello 4**(quindi i classici **DoS**) che a **livello 7**(quindi attacchi basati su **malformazioni di dati** come **SQL Injection** e **Code Injection** in genere **HTML, SMTP...** etc).

I.P.S. : Tipologie I

- **Host based I.P.S. :** Sono tipicamente degli strumenti che sono installati su di una macchina e hanno lo scopo di proteggere in tutto e per tutto il PC interessato(**un ”super-antivirus”**). Integrano funzioni di Firewall, SandBoxing, etc..

  Sono usati principalmente per la protezione di macchine **mobile** come i Laptop che potrebbero trovarsi in ambienti pubblici soggetti ad attacchi su più fronti (es. Gli internet cafè con accesso wireless o gli Acces Point di un Aereoporto.)

I.P.S. : Tipologie II

- **Network I.P.S.**: Del tutto simili ai N.I.D.S, solo che con la possibilità, come detto prima, di controllare attacchi su più fronti e su più livelli
- **Content Based I.P.S.**: Basano il loro controllo sul confronto del traffico con signature tipiche di determinati attacchi
- **Protocol Analisys I.P.S.**: Basano il loro controllo sull'analisi dei protocolli di rete individuando violazioni su questi protocolli o anomalie(anche, eventualmente, bloccare traffico cifrato).

I.P.S. : Tipologie III

- **Rate Based I.P.S.:** Nati principalmente per analizzare il traffico di rete e bloccare sul nascere tentativi di **DoS.** Infatti viene posta particolare attenzione sull'analisi di determinati tipi di protocolli e sul loro carico di dati (**UDP**,**TCP, ARP**), numero di connessioni al secondo, pacchetti inviati e ricevuti per connessione e altri paramentri di rete.

Questo approccio potrebbe produrre una quantità enorme di **falsi positivi**, infatti la sua **qualità** è **direttamente proporzionale** alla qualità delle **statistiche** contenute nel **database** a cui si appoggia il suo motore.

H.I.D.S. : Host Intrusion Detection Systems

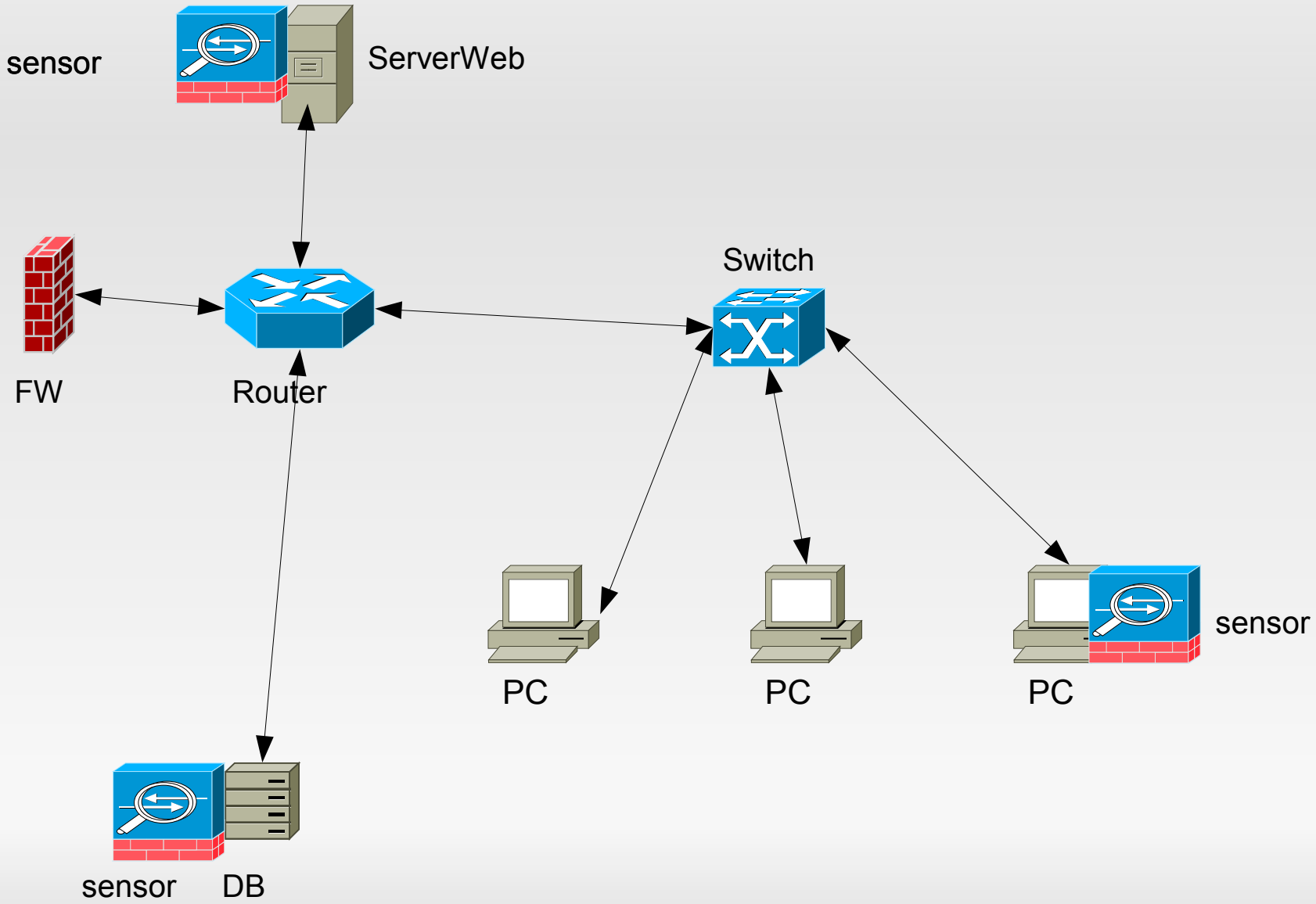
Sensori:

- Sono posizionati su **host** della rete **critici**
- Sono **moduli** del **sistema** residente della macchina(es. **Kernel Modules**)
- Analizzano in **real-time** funzioni come:
  - Log
  - **Attività utenti** (Privacy)
  - Attività applicazioni
  - Modifiche a file e documenti
  - .....

H.I.D.S : Detection

- Hanno un comportamento del tutto simile a quello di un **antivirus**
- Nel momento in cui viene riconosciuta la ”metrica” di un attacco reagiscono secondo diversi approcci:
  - **Isolando** la risorsa o l'applicazione attaccata
  - **Notificando** l'attacco
  - **Riavviando** il sistema(**provvedimento estermo**)

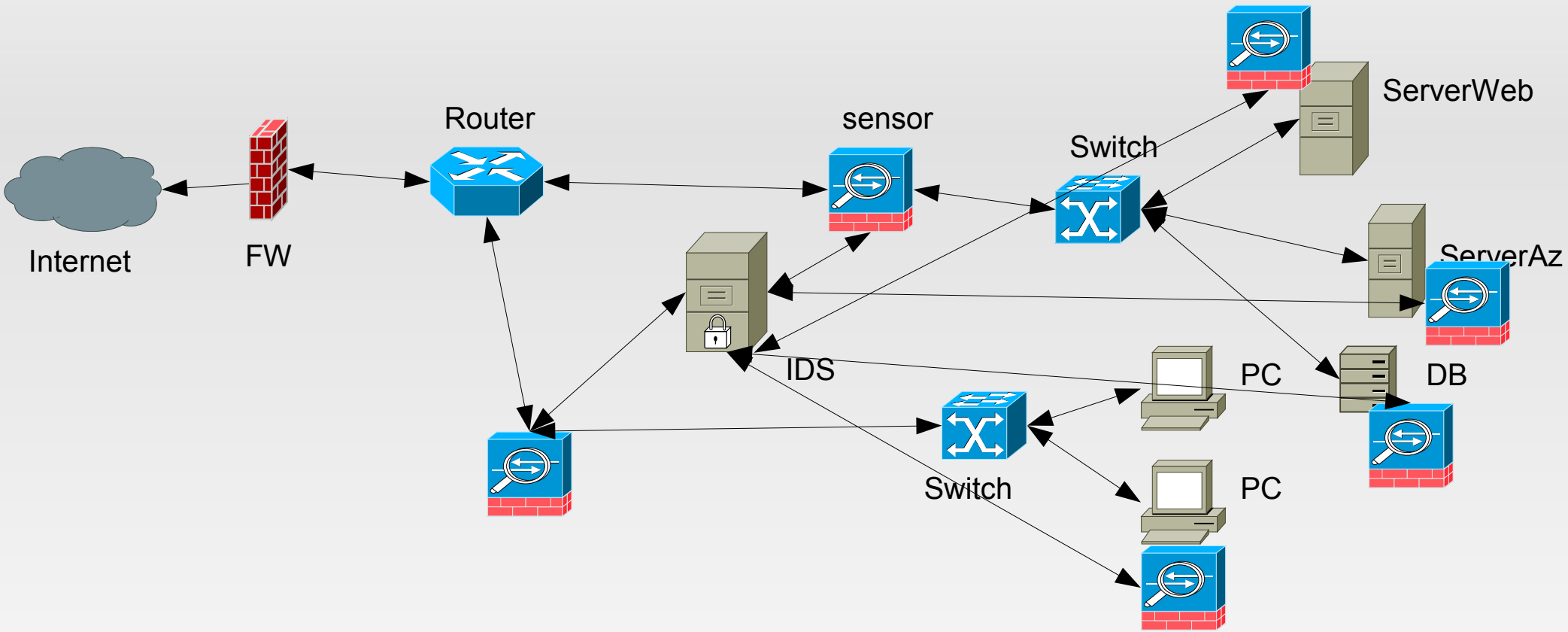
H.I.D.S. : Posizionamento



D(H).I.D.S : Distributed(Hybrid) Intrusion Detection Systems

- **Uniscono** ed **integrano** le peculiarità dei gli approcci visti in precedenza(N.I.D.S & H.I.D.S)
- Aggregano ed analizzano dati di vari sensori
  - NIDS
  - HIDS
  - Log di Sistema
- Permettono una visione globale ed approfondita delle attività all'interno di un sistema
- Gestiscono in maniera centralizzata le configurazioni e i report

D.I.D.S : Distributed Intrusion Detection Systems



I.D.S. : Vendor

- Principali produttori di I.D.S (80% del mercato):
  - **Cisco** Secure IDS
  - **ISS** RealSecure
  - **Axent** Intruder Alert
  - **Intrusion.com** Secure Net Pro
- Altri produttori(anche open source)
  - **Enterasys** Dragon
  - **NFR Security** NID e HID
  - **Marty Roesch** Snort

HONEYPOTS : Trick the Hacker

- **DEFINIZIONE:** un honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "**trappola**" o "**esca**" a fini di protezione contro gli attacchi informatici. Solitamente consiste in un **computer** o un **sito** che **sembra** essere **parte della rete** e contenere **informazioni preziose**, ma che in realtà è ben **isolato** e non ha contenuti **sensibili** o **critici**; potrebbe anche essere un file, un record, o un indirizzo IP non utilizzato.
- Il valore primario di un honeypot è l'informazione che esso dà sulla **natura** e la **frequenza** di eventuali attacchi subiti dalla rete. Gli honeypot non contengono informazioni reali e quindi non dovrebbero essere coinvolti da nessuna attività; rilevazioni in senso opposto possono rivelare intrusioni non autorizzate o malevole in corso.
- Gli honeypot possono portare dei rischi ad una rete, e devono essere maneggiati con cura. Se non sono ben protetti, un attacker potrebbe usarli per entrare in altri sistemi.

HONEYPOTS : Perchè?

- L'uso di questi strumenti è molto variegato, infatti una delle peculiarità degli honeypots e la loro **flessibilità** e la loro totale **configurabilità.**
- Posso essere utilizzati per diversi scopi come:
  - **Prevenzione degli attacchi**
  - **Riconoscimento degli attacchi**
  - **Risposta agli attacchi**
  - **Ricerca e individuazione di nuovi tipi di attacco**

HONEYPOTS : Tipologie

- Le ”filosofie” che caratterizzano l'implementazione e il funzionamento degli honeypots sono fondamentalmente due :
  - **High-interaction honeypots**
  - **Low-interaction honeypots**
- Come è facile intuire, questa differenza è data dalla maggiore o minore interazione che l'hacker può avere con questa ”trappola”.
- Ovviamente, maggiore è il grado di libertà che viene concesso all'hacker, maggiori sono i rischi che si corrono.

HONEYPOTS : Low Interaction

- Questo tipo di honeypot **emula** un sistema software con delle funzionalità ben **definite,** oltre le quali non è possibile andare.
- Infatti l'hacker che prova ad infiltrarsi in questo honeypot verrà **ingannato** pensando di avere veramente a che fare con il **servizio** di una vera macchina con un vero e proprio sistema operativo al suo interno.
- **Honeyd** è uno strumento software concepito per creare e gestire questo tipo di hp.
- Honeyd infatti permette di creare sulla stessa macchina più sistemi emulati con relativi servizi attivi al loro interno.
- Ovviamente l'attaccante non può andare oltre i servizi emulati, con il rischio di scoprire di essere stato ingannato.

HONEYPOTS : Low Interaction II

- **Pro:**
  - Facili da gestire e da creare
  - Non implicano una grande conoscenza dei diversi tipi di attacco.
  - La loro cattiva gestione non può causare danni ingenti
  - Ottimi per bloccare e riconosce attacchi portati da tool automatici.
- **Contro**
  - Facilmente riconoscibili
  - Non permettono di trarre informazioni esaustive su nuovi tipi di attacco
  - Di fronte a nuovi tipi di attacco che non conosce è totalmente inutile.

HONEYPOTS : High Interaction

- Questi hp non **emulano** una macchina, la rendono direttamente disponibile all'attaccante **virtualizzandola.**
- Fondamentalmente l'hacker si trova dentro un vero e proprio sistema, con tutte le sue feature attive, con il quale può interagire in piena libertà e senza limitazioni.
- In gergo viene creata una **Cage**(**Gabbia**) al cui interno viene osservato l'attaccante o gli attaccanti traendo importati informazioni sul loro modo di operare e la loro organizzazione
- Un tipico esempio di High Interaction Honeypot e quello che viene definito in gergo una ”**Honeynet**”. Praticamente un intero sistema virtuale con tanto di DB e WebServices al cui interno l'hacker può navigare indisturbato nel tentativo di portare a termine i suoi intenti.

HONEYPOTS : High Interaction II

- **Pro:**
  - Permettono di **osservare** e **comprendere** il comportamento di un hacker all'interno di un sistema
  - Permettono di carpirne i **software**, i **rootkit** e gli **exploit** che usano
  - Essendo degli end-point è possibile analizzare nel dettaglio gli attacchi portati con **dati malformati** o **criptati**
  - Possono essere usati per confondere l'attaccante
- **Contro:**
  - **Estremamente difficili da creare e gestire**
  - **La maggiore libertà potrebbe rivelarsi un'arma a doppio taglio. Infatti l'hp potrebbe essere usato dall'hacker, una volta che questi ha capito dove si trova e con cosa ha a che fare, per portare attacchi su altre reti.**
  - **E' nessaria una grande conoscenza sia dei sistemi sia del modus operandi di chi attacca.**

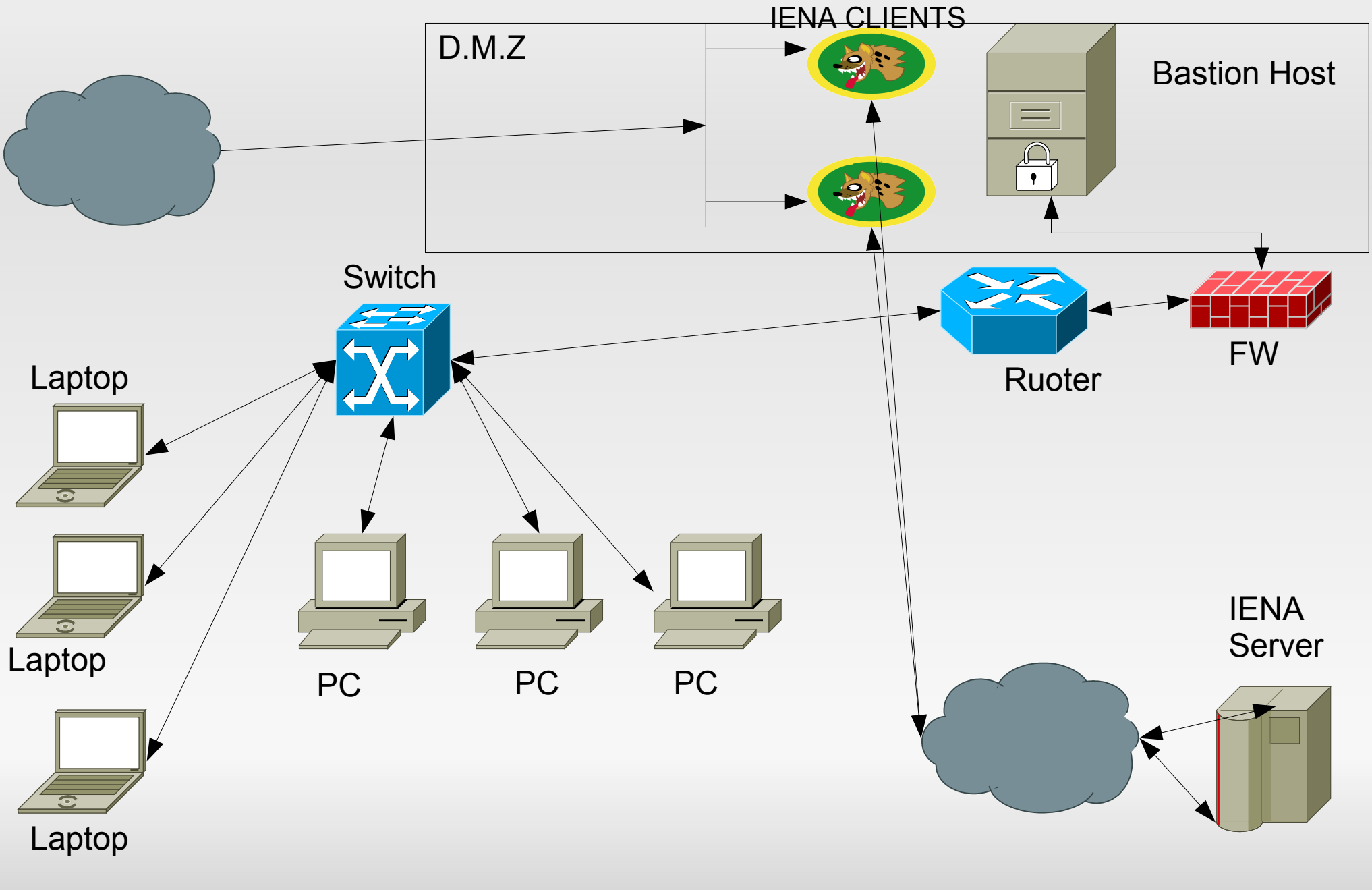
IENA

- **IENA** è il progetto **open source** che dà il nome all'omonimo software per la **prevenzione** delle intrusioni ideato e sviluppato all'interno del gruppo d'interesse per la sicurezza informatica **Ce.Se.NA** nella II Facoltà di Ingegneria dell'Università degli studi di Bologna.
- Il progetto **IENA** presenta una **nuova strategia** di prevenzione delle intrusioni nelle reti locali. L'originalità di **IENA** è rappresentata da una politica di totale **apertura.**

IENA II

- Obiettivo principe del software **IENA** è proteggere le risorse di una rete **bloccando sul nascere** eventuali attacchi esterni diretti alla **service exploitation**
- La difesa preventiva di **IENA** è basata totalmente sull'**inganno** dell'attaccante tramite un sistema di connessioni illecite che rappresentano delle **trappole.**
- L'attaccante che inconsapevolmente attiva una **trappola IENA**, viene immediatamente **espulso** dal sistema negando l'accesso dal suo indirizzo IP(IP Banning).

IENA. : Posizionamento



I.D.S. : Conclusioni

- Un sistema di sicurezza deve essere il **risultato** di un piano su **più livelli** e il più possibile **complessivo**
- Lo **staff** deve essere **preparato**
- Utilizzare più strumenti coordinati tra loro:
  - I.D.S
  - Firewall
  - Honeypots
  - Antivirus
  - Politiche aziendali
- Costante aggiornamento verifica del sistema
- Non affidarsi completamente alla tecnologia

Bibliografia e sitografia

- Siti:
  - www.wikipedia.org
  - http://it.wikipedia.org/wiki/Intrusion_detection_system
  - http://it.wikipedia.org/wiki/Network_Intrusion_Detection_System
  - http://sneakers.cs.columbia.edu/ids/index.html
  - http://www.auditmypc.com/freescan/readingroom/intrusion_detection.asp
  - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/pro
  - http://en.wikipedia.org/wiki/Intrusion-prevention_system
  - http://csrc.nist.gov/publications/PubsSPs.html
  - http://iena.sourceforge.net/
  - http://www.linux.com/articles/39244?page=1
  - http://www.honeypots.net/
  - http://www.honeyd.org/