Seminario
“Sistemi per il rilevamento e la prevenzione delle intrusioni informatiche”

Università degli Studi di Bologna
DEIS - Laboratorio di Reti di Telecomunicazione
4 Giugno 2007

Ing. Vincenzo Vaccarino
Dipartimento Sistemi e Tecnologie - Settore Operazioni
CINECA

www.cineca.it

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Definizione di IDS

Un IDS è un dispositivo di monitoraggio il cui obbiettivo è individuare e segnalare le intrusioni.

Per *intrusione* si intende una qualsiasi violazione alla policy di sicurezza della rete considerata.

Non è necessariamente riferito ad un evento che parta dall'esterno della rete difesa e sia diretto verso il suo interno.

Collocazione nello schema di sicurezza

L'IDS è un dispositivo passivo, per cui si limita a segnalare le intrusioni all' amministratore.

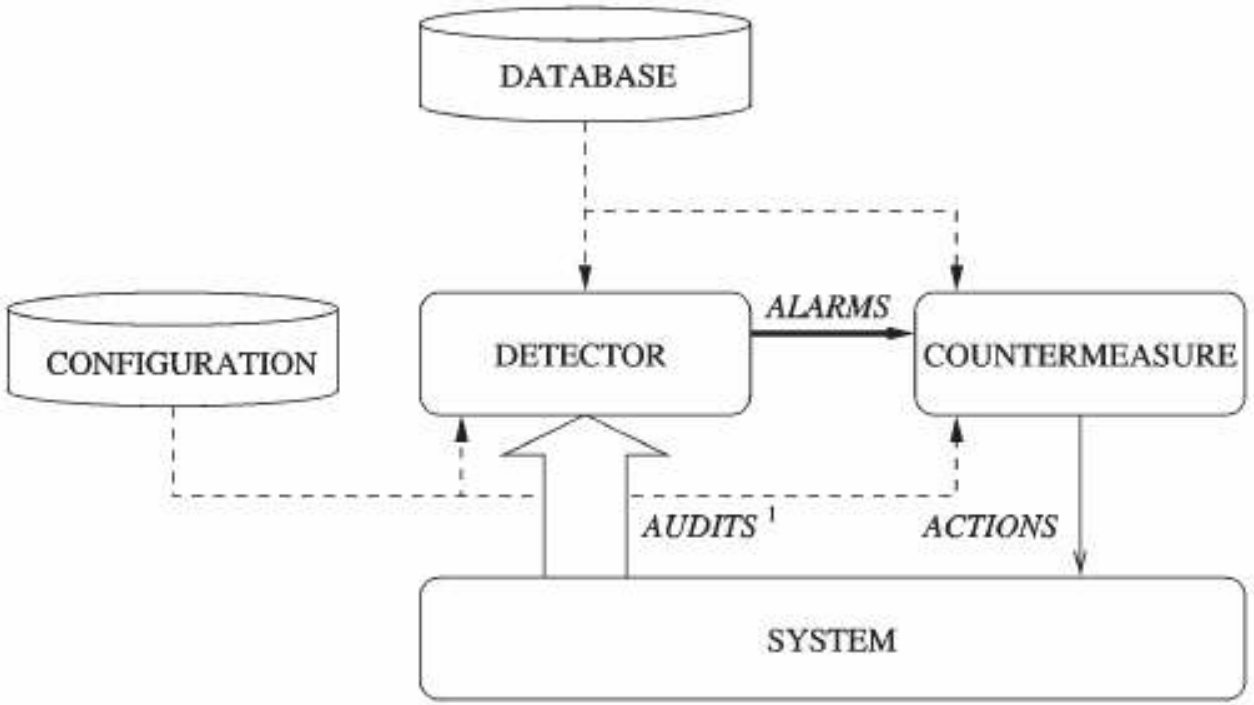
Se paragoniamo un firewall ad una porta blindata di una abitazione, l'IDS è un antifurto che comunica ad un responsabile la violazione del domicilio.

Le diverse componenti sono quindi complementari.

Necessità dell'IDS

- L'IDS non è un componente inutile o ridondante, anche per chi dispone già di firewall.
- Individua attacchi nel traffico che i dispositivi di frontiera lasciano passare
- Permette un controllo anche sui sistemi interni ai dispositivi di frontiera

Schema di principio (1)



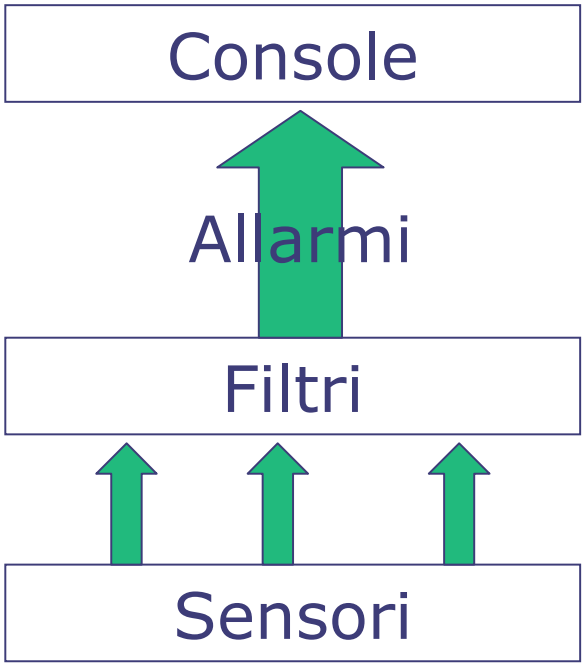
Schema di principio (2)

- *System* è il sistema di cui va operato il monitoraggio
- *Audit* è l'insieme delle grandezze che vengono valutate per il controllo
- *Detector* è il nodo centrale del sistema perché è il componente che effettua il controllo vero e proprio sui dati ricevuti

Schema di principio (3)

- *Alarms* è l'insieme degli allarmi attivati dal detector e registrati su database
- *Database* è il repository degli allarmi e delle tracce che permettono il confronto
- *Countermeasure* è il blocco che, negli IPS, mette in atto le contromisure previste
- *Configuration* definisce la configurazione di tutti i componenti

Componenti (1)



Componenti (2)

- I *sensori* acquisiscono i dati dal sistema sotto controllo e li inviano ai filtri perché ne venga determinata la natura

- I *filtri* operano la decisione riguardo la natura dei dati acquisiti, ed in base alle proprie regole stabiliscono se si tratti di eventi da registrare come allarmi

Componenti (3)

- Gli *allarmi* costituiscono il flusso di segnalazioni che i filtri inviano per un esame più approfondito e per l'eventuale decisione sulle contromisure

- La *console* permette di avere una visione d'insieme degli allarmi, per decidere le reazioni, e di configurare il sistema

Componenti (4)

- L'architettura può essere *distribuita*, ossia più blocchi *sensore+filtro* alimentano una singola console, essenziale per la correlazione degli eventi

- E' possibile utilizzare anche *preprocessori* che effettuano una prima elaborazione dei dati che poi i sensori passano ai filtri

Classificazione (1)

Esistono diversi metodi di classificazione degli IDS, ma i principali sono due:

- ***Obbiettivo protetto*** – si basa sulla natura del sistema protetto dall'IDS

- ***Metodo di rilevazione*** – individua le tipologie di analisi effettuata

Classificazione (2)

La classificazione in base all'obbiettivo protetto individua due categorie principali:

- NIDS – Network Based IDS
- HIDS – Host Based IDS

Meno diffusi sono gli IDS Ibridi, che uniscono caratteristiche di entrambi

Network IDS

I NIDS sono IDS che controllano interi segmenti di rete, prendendo quindi in esame il traffico di rete che vi passa

Per questo sono installati su macchine dedicate

Generalmente eseguono analisi ai livelli più bassi dello stack TCP/IP

Host IDS

Gli HIDS sono strumenti per il controllo dei singoli host su cui vengono installati

Vengono di solito monitorati i file di log, le chiamate di sistema, le modifiche al filesystem

Utilizzano le risorse hardware della macchina sotto controllo

Confronto NIDS-HIDS

- I NIDS non possono esaminare trasmissioni di rete criptate (almeno nella definizione classica)
- Gli HIDS devono impattare il meno possibile sulle prestazioni del sistema
- I NIDS hanno visibilità su eventuali attacchi portati in contemporanea a più sistemi
- Gli HIDS sono meno sensibili a fenomeni di saturazione

Hybrid IDS

Poco diffusi, sono prodotti che cercano di unire i pregi delle due tipologie HIDS e NIDS.

Sono costituiti da sensori di tipi diversi, che fanno riferimento ad un nucleo centrale per il filtraggio e la decisione.

Evoluzione : NNIDS

I Network Node IDS (NNIDS) nascono per ridurre i fenomeni di saturazione in ambiente Network based

I singoli sensori effettuano una prima scrematura dei dati, basandosi su criteri di massima

I risultati così ottenuti sono passati ad un centro di filtraggio, che lavora su una massa di dati minore

Classificazione (3)

Basandoci sull'analisi effettuata, anche in questo caso abbiamo due categorie :

- Sistemi basati su firme (*signature*)
- Sistemi basati sulla rilevazione di anomalie

Knowledge Based IDS

Con questo nome vengono identificati gli IDS in cui il criterio di decisione si basa su un archivio di tracce di attacco, o *firme*

Se i dati rilevati corrispondono alla traccia di un attacco noto, viene fatto scattare l'allarme

Per questo tipo di sistemi è essenziale un aggiornamento costante

Anomaly detection IDS

Questi IDS si basano su un modello che individua un comportamento normale, ed individuano come attacco ogni comportamento che si discosti da quello normale

Il modello può essere costruito in modo sintetico (*sistemi programmati*) o individuato dal sistema monitorato (*sistemi in autoapprendimento)*

Anomaly detection IDS (2)

I sistemi *programmati* sono più veloci da rendere operativi, ma non sempre è facile caratterizzare il traffico lecito.

I sistemi in *autoapprendimento* richiedono di solito lunghi periodi di esame della rete su cui sono installati.

Gli analizzatori di anomalie di protocollo si basano sugli standard dei vari servizi esistenti.

Confronto

- I sistemi basati su anomalie sono in grado di individuare anche attacchi sconosciuti, mentre quelli basati su firme solo quelli per cui sia stata determinata una traccia
- I sistemi basati su firme sono meno esposti al rischio di falsi positivi
- L'efficienza dei sistemi basati su anomalie dipende in modo determinante dalla qualità del modello

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Capacità di reazione

Tutti i sistemi visti finora hanno la comune caratteristica di essere passivi.

Negli ultimi anni è nata l'esigenza di avere a disposizione strumenti attivi, che permettano un certo grado di risposta, possibilmente in tempo reale, agli eventuali attacchi.

Dispositivi in grado di reagire, cioè di operare in maniera proattiva, in modo automatico sono detti **IPS** (Intrusion Prevention System).

IPS - Caratteristiche

I sistemi IPS devono essere in grado di impedire ad attacchi che riescano ad identificare di produrre danni.

E' quindi necessario che siano :

- molto veloci a prendere decisioni
- opportunamente integrati nella struttura di rete o del singolo sistema per poter intervenire a limitare l'azione dell'attacco in corso.

IPS – Classificazione

La principale classificazione esistente per gli IPS ricalca quella degli IDS :

- HIPS – Host based IPS
- NIPS – Network based IPS

Host IPS

Gli HIPS sono sistemi attivi sul singolo host che devono proteggere.

In tal senso, il monitoraggio può riguardare l' attività dei processi, le modifiche ai file, le chiamate di sistema e così via.

L'analisi in questo caso non avviene in un secondo momento sui log, ma monitorando l'attività il più possibile nel corso del suo svolgimento.

Host IPS

Le possibilità di reazione consistono in generale nel proibire la modifica di file e nel bloccare i processi che possano far parte di uno schema di attacco.

Solitamente viene comunque tenuto un log di tali operazioni e di quale ne sia stata la causa scatenante, in modo che l'amministratore di sistema possa comunque esaminarne l'attività.

Network IPS

Un NIPS è un dispositivo analogo al NIDS, da cui si differenzia per il fatto che è inserito nel cammino dei pacchetti di rete e la sua analisi è decisiva per il passaggio dei pacchetti da una rete all'altra.

Solo in questo modo si può garantire una vera protezione basata sul filtraggio del traffico di rete completo.

IPS - Vantaggi

I vantaggi dell'IPS rispetto all'IDS sono del tutto evidenti:

- Protezione reale del sistema
- Scarso bisogno di presidio umano

Pare quindi che sia la soluzione ideale….

IPS - Svantaggi

…ma la soluzione ideale purtroppo non esiste. Infatti l'IPS è un dispositivo critico:

- Risente dei falsi positivi
- Può diventare un collo di bottiglia per il sistema sotto controllo
- Può "bloccare" il sistema monitorato

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

IDS/IPS - Protezione

Il vantaggio dell'IPS è in questo caso evidente:

- l'IDS svolge un azione di monitoraggio che avverte l'amministratore spesso quando l'intrusione è già avvenuta
- l'IPS è anche in grado di evitare il completamento dell'intrusione

Questa forma di protezione si può ottenere sia con l'integrazione con altri dispositivi (es. firewall) sia mediante un'azione diretta dell'IPS

IDS/IPS - Presidio

Le analisi prodotte dagli IDS, per essere significative, devono essere analizzate dal personale preposto per capire cosa sia accaduto e come reagire.

E' quindi necessario presidiare quasi con continuità la console su cui vengono segnalati gli eventi.

L'IPS non richiede la stessa continuità in quanto comunque attiva le azioni di reazione in maniera autonoma.

IDS/IPS - Prestazioni

L'IDS non si interpone fra componenti di rete che debbano dialogare tra loro, per cui l'eventuale impossibilità di analizzare tutto il traffico comporta al più una perdita di efficienza.

L'IPS solitamente fa da filtro, per cui una sua saturazione a causa del troppo traffico può portare a rallentamenti nel funzionamento del sistema.

IDS/IPS – Falsi positivi (1)

Nel rilevamento delle intrusioni, un *falso positivo* rappresenta un evento attivato dal sistema che non sia in realtà corrispondente ad un vero attacco o comunque ad una attività considerata nociva.

Di solito il motivo di queste rilevazioni è legato ad errate configurazioni oppure a firme definite in maniera poco precisa.

IDS/IPS – Falsi positivi (2)

Nel caso degli IDS, la presenza di un falso positivo appesantisce le operazioni di analisi, aumentando il carico di lavoro degli operatori.

Nel caso degli IPS invece, il fatto che i falsi positivi attivino delle reazioni, può portare ad attivare contromisure in presenza di traffico legittimo, portando in molti casi a veri e propri DoS.

IDS/IPS – Rischi di blocco

IDS e IPS sono servizi a rischio di compromissione. Un eventuale blocco del sistema su cui girano ha però effetti diversi:

- IDS – viene a mancare il monitoraggio del sistema
- IPS – se l'IPS filtra tutto il traffico, la rete interna si trova isolata dall'esterno

IDS/IPS – Possibili soluzioni

Per evitare i rischi di eccessivi falsi positivi, molto spesso gli IPS vengono fatti funzionare con un insieme minimo di firme, che si sanno essere resistenti ai falsi positivi.

In parallelo, si fa analizzare il traffico anche ad un IDS, che identificherà i restanti attacchi.

La componente di IDS può essere anche già presente nel sistema IPS (solitamente questi sistemi presentano modalità di "simulazione" in cui gli allarmi vengono registrati senza ulteriori interventi).

Add-on (1)

In molti casi, il semplice nucleo dell'IDS non ne permette un utilizzo proficuo.

Infatti la norma prevede la registrazione in file di log e/o in database (con formati proprietari e non)

Per un utilizzo produttivo, il "cuore" dell' IDS è affiancato da tutta una serie di strumenti assolutamente necessari

Add-on (2)

La maggior parte di questi strumenti sono dedicati all'esecuzione di interrogazioni sui database degli allarmi e alla presentazione dei dati all'operatore in modo facilmente interpretabile.

Molto spesso questi strumenti di reportistica comprendono banche dati per la valutazione del rischio relativo ad un attacco ed interfacce specifiche per il database utilizzato

Add-on (3)

In un prodotto commerciale maturo questi strumenti sono assolutamente indispensabili, in quanto la loro assenza rende inutilizzabile anche il prodotto tecnicamente più avanzato.

Le analisi di mercato valutano quindi con grande attenzione l'utilizzabilità in un ambiente di produzione.

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Il mercato attuale

Negli ultimi anni il mercato relativo all' Intrusion Detection si è espanso in modo notevole.

Questo interesse del mercato ha spinto in particolare lo sviluppo degli IPS e di tool e prodotti che permettano analisi di elevata complessità.

Si è anche riscontrato un interesse per l'analisi di reti sempre più veloci, fino ad alcuni Gigabit

Il mercato attuale (2)

Inizialmente i prodotti IDS erano sviluppati da realtà piuttosto piccole ed erano prodotti di nicchia.

Molti di questi soggetti sono stati poi acquisiti dalle grandi case che si occupano di sicurezza, in modo da completare la propria offerta con queste linee.

Questo ha permesso inoltre una notevole accelerazione della ricerca in questo settore.

Mercato – Prodotti

Snort è un prodotto Open Source, nato nel 1998 e disponibile per le principali piattaforme esistenti. E' un NIDS basato su firme, anche se i tool sviluppati dalla comunità che lo sostiene ne hanno permesso l'utilizzo anche con funzioni di IPS (FlexResponse, Snort Inline).

http://www.snort.org

Mercato – Prodotti

Molte aziende operanti nell'ambito della sicurezza propongono gamme complete di prodotti IDS e IPS, spesso in modelli diversificati per quanto riguarda il dimensionamento dell'hardware, adatte a diverse situazioni di rete.

Nella maggior parte dei casi, i prodotti vengono forniti infatti completi di hardware (*appliance*), in modo da limitare al massimo i problemi per l'utenza.

Ulteriore vantaggio di questa situazione è che per il produttore è facile tenere sotto controllo le prestazioni che il prodotto può garantire, in quanto indipendenti da scelte hardware dell'utente.

Mercato – Aziende

Sourcefire è un'azienda che commercializza prodotti basati su Snort, di cui cura anche lo sviluppo. Dopo una fase concentrata sui NIDS, al momento propone NIPS sempre basati su Snort.Sta portando avanti ricerche sul Network Awareness per ottimizzare la raccolta dei dati.

ISS è stata la prima azienda a proporre NIDS commerciali, e la sua gamma RealSecure è ancora oggi un punto di riferimento per il mercato. Oggi si caratterizza per la serie Proventia, che fornisce soluzioni IPS destinate sia ai server, sia alle reti di diverse capacità. Dall'ottobre 2006 è stata acquisita da IBM.

Mercato – Aziende

CISCO è stata una delle prime aziende a fornire NIDS sotto forma di appliance complete di hardware e software. Al momento l'offerta è costituita da NIPS forniti sotto forma di *appliance*, completi di strumenti per l'integrazione dei sensori (anche con i prodotti di rete CISCO) e la loro amministrazione.

McAfee (precedentemente Network Associates) presenta una linea NIPS denominata IntruShield ed una serie di prodotti HIPS con soluzioni dedicate a server e desktop.

Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Snort

- E’ un Network IDS, basato su firme
- Nasce nel 1998, scritto da Martin Roesch
- Lo sviluppo oggi è coordinato da Sourcefire
- E’ rilasciato sotto licenza mista: il codice è sotto licenza GPL, mentre le firme sviluppate da Sourcefire sono sotto licenza proprietaria

Snort

La gratuità del prodotto e l'ampia comunità che lo segue e lo sviluppa lo rendono ideale per un primo approccio all'implementazione degli IDS.

D'altra parte, manca della maggior parte delle utility "accessorie" che abbiamo visto costituire una parte importante per un prodotto maturo.

Questi componenti sono spesso resi disponibili da soggetti esterni, solitamente con licenze Open Source.

Snort

Il sito ufficiale è http://www.snort.org

Oltre al programma nelle sue varie versioni, è disponibile una vasta documentazione

Molte notizie ed aggiornamenti si ricavano anche dalle mailing list di supporto, allo stesso sito

Snort - Firme

Snort, come molti altri IDS, permette agli utenti di scrivere le proprie firme, eventualmente adattando quelle già presenti. Anche sotto questo profilo la comunità è molto attiva, e nuove firme compaiono con una notevole prontezza all'apparire delle vulnerabilità, dei virus e degli exploit sulla scena pubblica.

La nuova forma di licenza per le firme ufficiali di Sourcefire, denominata VRT, impone delle limitazioni per quanto riguarda la redistribuzione delle firme (e dei loro derivati).

In sostanza, non è possibile utilizzare tali firme in prodotti commerciali, senza previa autorizzazione di Sourcefire.

Snort

- La versione più recente (stabile) è la 2.6.1.5
- Esistono versioni per Linux e per Windows
- Può funzionare come sniffer, come packet logger o come NIDS

Snort - Sniffer

I principali switch per il comando snort utilizzato come sniffer :

- -v : mostra indirizzi IP ed intestazioni TCP/UDP/ICMP
- -d : mostra il contenuto dei pacchetti dati
- -e : mostra i dati del livello Data Link

Snort – Packet Logger

In questo caso Snort registra il contenuto dei pacchetti esaminati :

- -l *dir* : registra sulla directory *dir*
- -L *file* : registra i dati nel file *file*
- -b : registra i dati in formato binario
- -r : modalità replay, mostra il contenuto di un file registrato

Il file in formato binario si può leggere con tcpdump o Ethereal

Snort - NIDS

Solitamente in questa modalità si preferisce attivarlo come servizio :

- -D : attiva snort in *daemon mode*
- snort.conf è il nome di default del file di testo che contiene la configurazione (è possibile forzarlo con -c *nomefile*)
- -A *[par]*: definisce le modalità di registrazione degli allarmi
- -s : gli eventi sono registrati nel syslog

Snort – Configurazione

La configurazione di Snort è determinata dal file snort.conf (o file diversi se esplicitamente indicati)

Si presenta come un file di testo, in cui sono presenti diverse sezioni che si occupano di definizioni preliminari, pre-processori, regole da utilizzare, plugin per l'output, etc.

Snort – Preprocessori (1)

I preprocessori permettono di effettuare operazioni sui dati prima che questi vengano esaminati dal motore di riconoscimento degli attacchi, ma dopo che il pacchetto è stato decodificato.

La forma generale è :

preprocessor <name>: <options>

Snort – Preprocessori (2)

Qualche preprocessore comunemente utilizzato :

- Stream4 – si occupa di riassemblare il flusso TCP
- Portscan – unifica le operazioni dovute ad un portscan, riducendo il numero di allarmi conseguenti

Snort – Preprocessori (3)

- [protocol] decode : esistono per diversi protocolli e si occupano di ricomporre i record relativi quando sono suddivisi in più pacchetti per facilitarne l'esame

- HTTP Inspect : opera su un flusso HTTP "ricostruito" e si occupa di effettuare una prima analisi ed eventualmente "normalizzare" campi che lo richiedano per l'esame

Snort – Regole (1)

Gli utenti possono scriversi le regole di Snort, con modalità descritte nella documentazione. Un esempio di regola :

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86
a5|"; msg "mountd access")↰
```

Snort – Regole (2)

Le regole predefinite sono separate in file per “argomento”. Il file di configurazione permette di definire quali di questi file vadano presi in considerazione, in modo, se necessario, da limitare il numero delle regole attive.

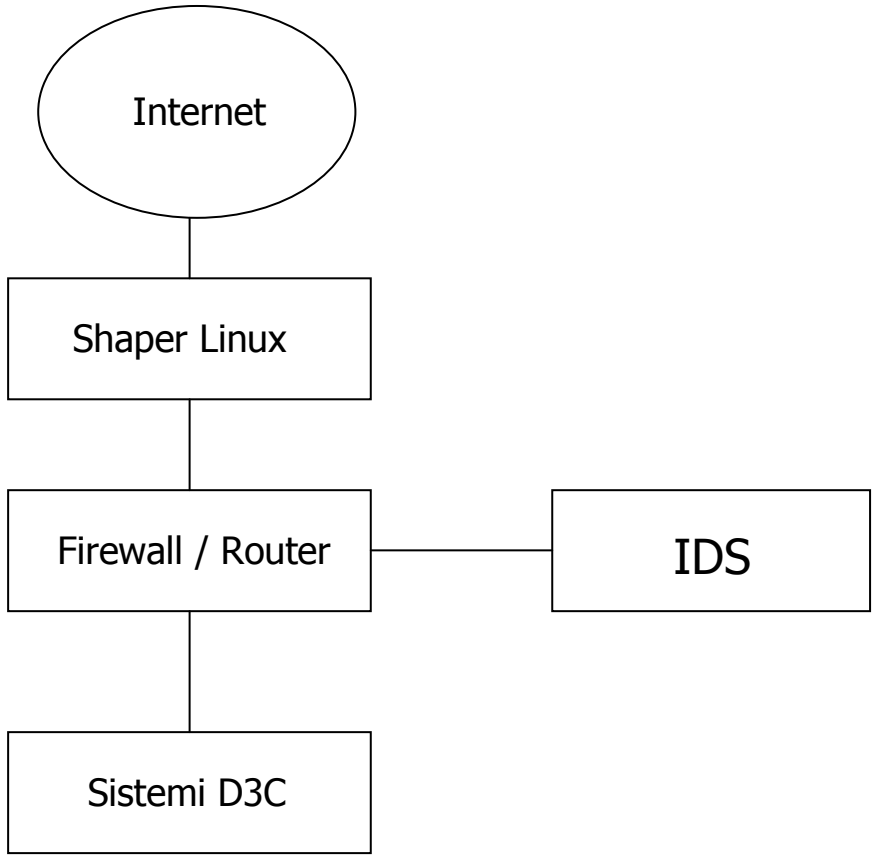
Le regole ufficialmente comprese nella distribuzione sono presenti anche in un database sul sito ufficiale.

Questo database è una delle fonti per la comprensione delle firme e del loro significato, insieme alla documentazione con cui di solito vengono pubblicate e commentate sulle mailing-list dedicate.

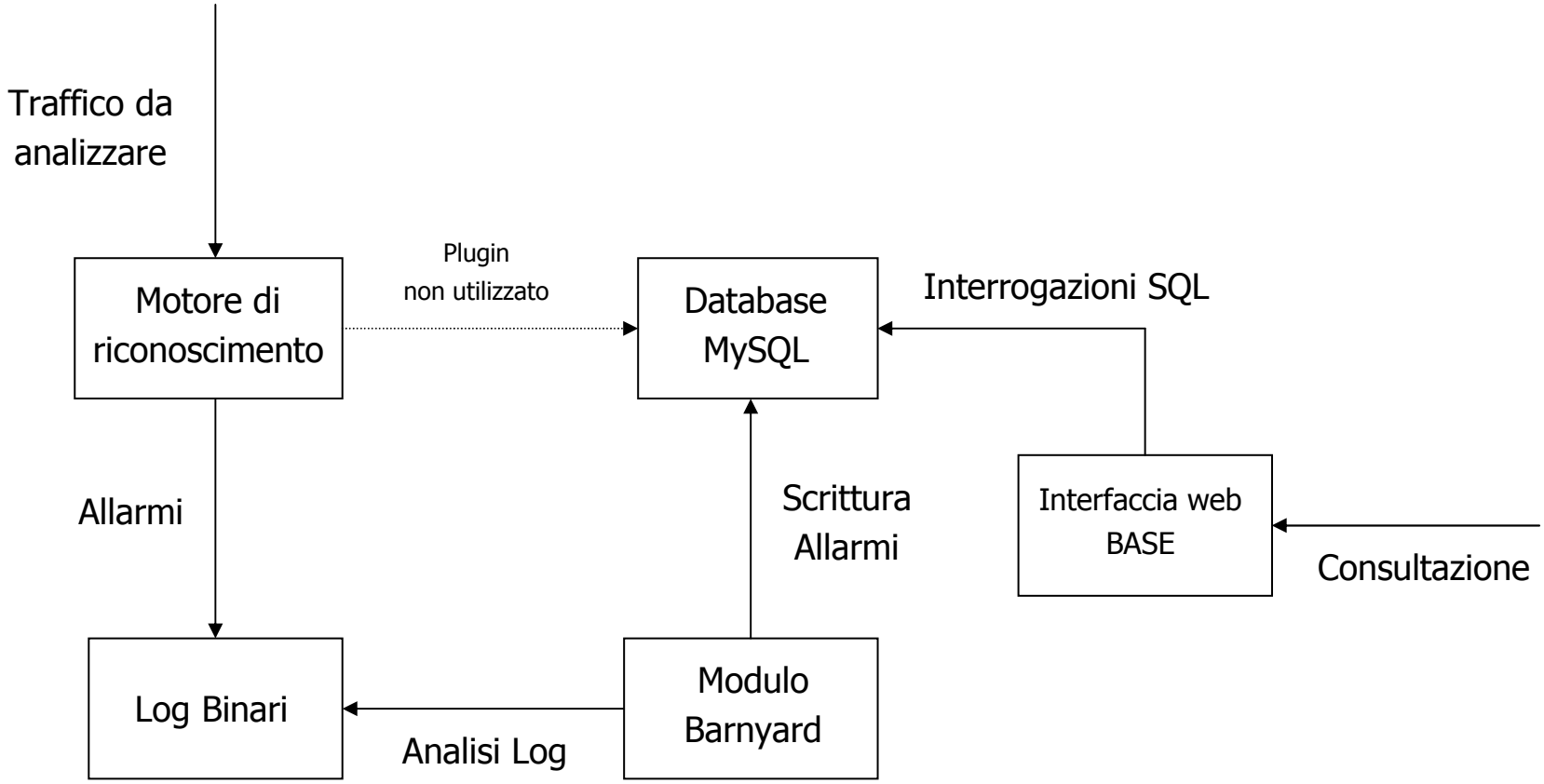
Agenda

- Definizione IDS
- Definizione IPS
- Confronto fra le soluzioni
- Stato del mercato
- Snort
- Un esempio pratico

Schema di rete generale



Schema funzionamento Server IDS



Link Prodotti

http://www.snort.org/
Sito ufficiale

http://www.tripwire.org/
Integrity checker per sistemi Linux

http://www.prelude-ids.org
IDS Ibrido

Link generici

http://www.security-focus.com/ids

http://www.security-focus.com/archive/96
Archivio della Mailing list relativa agli IDS

http://www.nss.co.uk
Prove comparative di prodotti commerciali appartenenti a diverse categorie

Riferimenti

Vincenzo Vaccarino

CINECA
Dipartimento Sistemi e Tecnologie

Tel. 051-6171411 (centralino)
e-mail: v.vaccarino@cineca.it

Domande ?