

Firewall Intrusion Detection System



Damiano Carra

Università degli Studi di Verona
Dipartimento di Informatica

Parte I: Firewall



Firewall

- ❑ I Firewall di rete sono apparecchiature o sistemi che controllano il flusso del traffico tra due reti con differenti livelli di sicurezza
 - Per prevenire accessi non autorizzati alla rete privata
 - Prevenire l'esportazione di dati dall'interno verso l'esterno
 - Schermare alcune reti interne e nasconderle agli altri
 - Bloccare alcuni accessi a servizi o ad utenti
 - Monitorare!
 - Log function importante!!

3



Problemi

- ❑ Si assume che gli attacchi avvengano dall'esterno
 - Ma possono anche iniziare dall'interno...
- ❑ Non difende contro nuovi rischi non ancora documentati nei protocolli
- ❑ I filtri sono difficili da settare e da mantenere perchè difficile compromesso tra libertà e sicurezza
- ❑ Può degradare le performance della rete

4



Due filosofie

☐ Default deny:

- *Tutto quello che non è espressamente ammesso è proibito*
 - Servizi sono abilitati caso per caso dopo una attenta analisi
 - Utenti sono molto ristretti e non possono facilmente rompere la policy di sicurezza

☐ Default permit:

- *Tutto quello che non è espressamente proibito è ammesso*
 - System administrator deve reagire prontamente ogni volta che un nuovo baco su un protocollo viene scoperto
 - Servizi sono rimossi/ridotti quando vengono scoperti pericolosi
 - Utenti sono meno ristretti



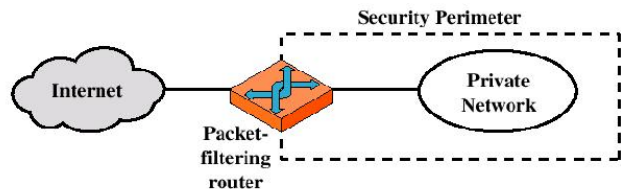
Tipologie di Firewall

☐ I firewall si suddividono in tre tipologie:

- Packet-Filtering router (1° generazione)
- Stateful Inspection (2° generazione)
- Gateway a livello di applicazione (o Proxy Server) (3° generazione)



Filtri a livello 3



- ☐ Source address del pacchetto (IP address)
- ☐ Destination address del pacchetto (IP address)
- ☐ Tipo del traffico (IP, ICMP, IPX se a livello 3, o anche protocolli di livello 2)
- ☐ Possibilmente, alcune caratteristiche del livello 4 (porta sorgente e destinazione)
- ☐ Talvolta, informazioni interne al router (quali informazioni circa l'interfacce sorgente e di destinazione del pacchetto, utile per routers con più interfacce)

7



Vantaggi e Limitazioni

- ☐ Vantaggi
 - E' disponibile in molti router
 - Costo d'acquisto contenuto
 - Trasparenza (non lavora a livello applicativo, quindi non ostacola il normale utilizzo della rete)
 - Velocità (effettua meno controlli, e per questo è la più veloce)
- ☐ Limitazioni
 - Regole difficili da configurare.
 - Può avere bug (più frequenti nel packet filtering rispetto al proxying)

8



Stateful Packet Filtering

- ❑ Quando viene stabilita una connessione, se le regole di filtraggio non la bloccano, allora le informazioni relative ad essa diventano entry di una tabella di stato
- ❑ Successivi pacchetti in ingresso saranno valutati in base all'appartenenza ad una delle connessioni consentite presenti nella tabella
- ❑ Quando la connessione è conclusa, la entry nella tabella sarà cancellata, per evitare che questa si riempia completamente

9



Stateful Packet Filtering

- ❑ Informazioni riguardanti la connessione che verranno memorizzate:
 - Identificatore univoco collegamento sessione
 - Stato connessione (handshaking se siamo in fase iniziale ovvero dove raccogliamo info e mettiamo in tabella stato, established, closing)
 - Informazioni sequenzialità pacchetti
 - Indirizzi IP host sorgente e destinazione
 - Interfacce di rete utilizzate

Source address	Source port	Dest. Address	Dest. Port	Connection state
192.168.0.199	1051	192.168.1.10	80	Handshaking
192.168.0.212	1109	192.168.1.23	25	Closing
192.168.3.105	1212	192.168.0.111	80	Established

10



Vantaggi e Limitazioni

☐ Vantaggi

- Tutti i vantaggi del packet filtering (essendone una evoluzione ne ereditano tutti i fattori positivi).
- Buon rapporto prestazioni/sicurezza (tipologia firewall con più alte performance, perché è quella che effettua meno controlli sulla connessione)
- Protezione da IP spoofing (il controllo non si limita al singolo IP o alla porta, è molto più difficile aggirare il firewall)

☐ Limitazioni

- Mancanza servizi aggiuntivi (non potendo agire a livello di applicazione non sono disponibili servizi come gestione delle autenticazioni)
- Testing complesso (verificare corretta configurazione firewall non è facile)



11

Filtri a livello 7

☐ Routing tra le due interfacce effettuato a livello applicazione dal software del firewall

- In caso di malfunzionamento del sw, il routing è disabilitato

☐ Possibilità di authentication

- UserId and password
- HW/SW token authentication
- Biometric authentication

☐ Filtri su specifici comandi

- Ad es. permettere get ma non put



12

Vantaggi e Limitazioni

❑ Vantaggi:

- Più sicuri dei packet filters
- Deve solo controllare un numero limitato di applicazioni (http, ftp, posta)
- Facile il log e il controllo del traffico

❑ Svantaggi:

- Processing overhead su ogni connessione
- Può solo controllare un numero limitato di applicazioni (http, ftp, posta)

13



Proxy server dedicati

❑ Specifici per ogni applicazione

❑ Aiutano l' application proxy gateway nel lavoro di contents-inspection

❑ Tipico uso:

- Antivirus
- Malicious code (applets java,activex, javascript, word)
- Usati spesso per outbound connections
 - Web cache proxy
 - Email proxy

14



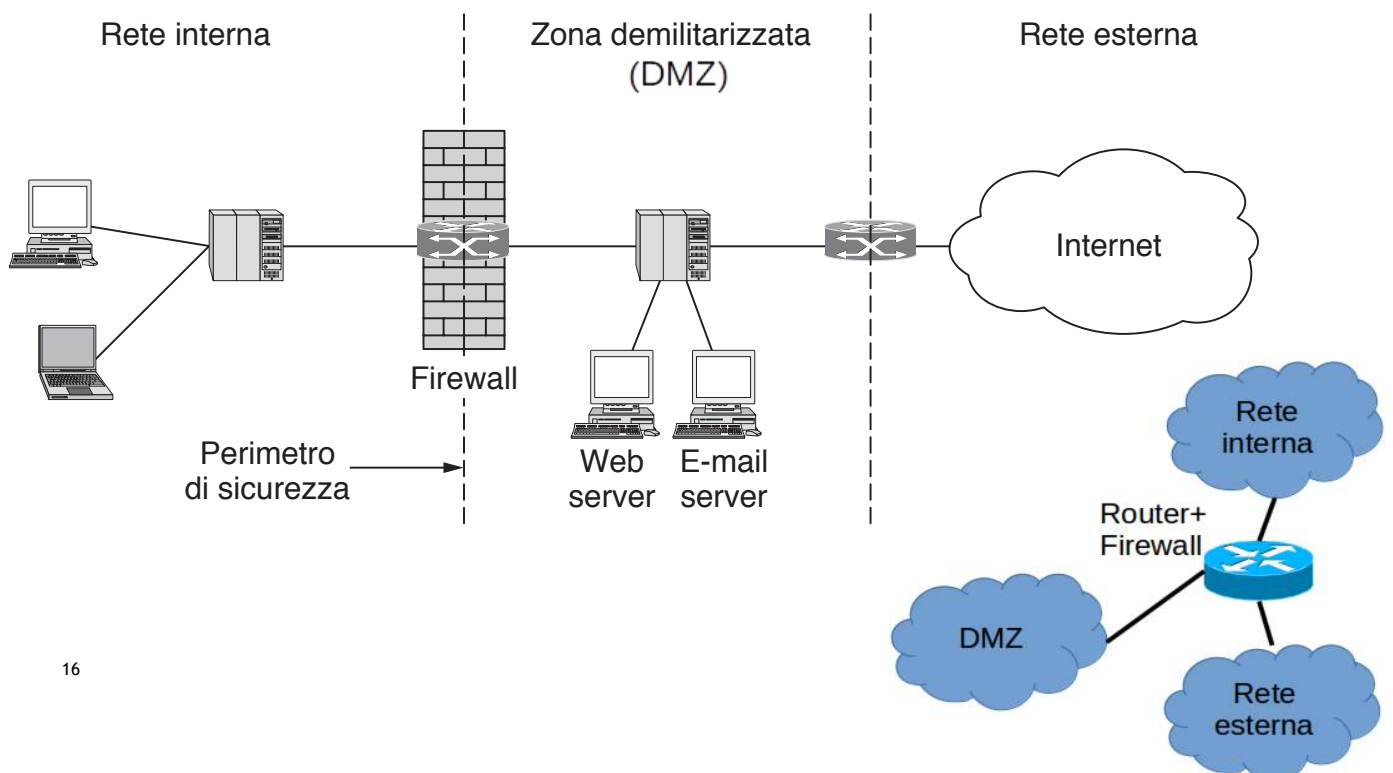
Personal firewalls

- ☐ Proteggono solo la macchina dove sono istallate
- ☐ Necessario, specie per mobile users
- ☐ Es:
 - winXp
 - Zonealarm
 - ...



15

Architettura



16

Parte II: Intrusion Detection System (IDS)



17

IDS - Sistema di rilevamento delle intrusioni

- ☐ Strumento, software o hardware, che automatizza il processo di monitoraggio impiegato per individuare eventi che rappresentano intrusioni non autorizzate
 - Ai computer
 - Alle reti locali

- ☐ Si può fare a livello di host (HIDS) e a livello di network (NIDS)



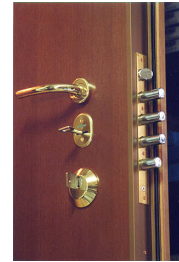
18

IDS vs Firewall

- ❑ Un IDS può essere considerato come un antifurto, cioè cerca di rilevarle eventuali intrusioni



- ❑ Un firewall può essere considerato come una porta blindata, serve bloccare le eventuali intrusioni



19



IDS perfetto e reale

- ❑ Un IDS perfetto dovrebbe riuscire ad individuare tutte le **reali** intrusioni
- ❑ Principali problemi:
 - Falsi positivi: IDS rileva un'anomalia, ma non è successo niente
 - Falsi negativi: IDS non rileva un'intrusione avvenuta
- ❑ Requisiti per un IDS reale
 - Scoprire un ampia gamma di intrusioni, sia già note che non note
 - Scoprirle velocemente, non necessariamente in tempo reale
 - Presentare i report delle analisi in formato semplice e facilmente comprensibile
 - Essere accurato

20



Principi di base

- ☐ Distinguere situazioni normali da quelle anomale
- ☐ L'utente in condizioni normali
 - Si comporta in modo più o meno prevedibile
 - Non compie azioni atte a violare la sicurezza
 - I propri processi compiono solo azioni permesse

21



Modelli per l'IDS

- ☐ Detection di anomalie
 - Sequenze di azioni non usuali possono essere intrusioni
- ☐ Detection di uso malevolo
 - Si conosce quali sequenze di azioni possono essere intrusioni
- ☐ Detection in base a specifiche
 - Si conoscono le situazioni derivanti da intrusioni
- ☐ I modelli possono essere statici o adattivi

22



Detection di anomalie

- ❑ Si analizzano insiemi di caratteristiche del sistema confrontando i valori con quelli attesi e segnalando quando le statistiche non sono paragonabili a quelle attese
 - Metriche a soglia
 - Momenti statistici
 - Modelli di Markov

23



Metriche a soglie

- ❑ Contare il numero di volte che un evento si presenta
 - Ci si aspetta tra m e n occorrenze
 - Se il numero cade al di fuori, c'è un'anomalia
- ❑ Esempio
 - Windows: blocco dopo k tentativi di login falliti. Il range è $(0, k-1)$.
 - k o più tentativi destano sospetto
- ❑ Problematiche
 - E' difficile trovare l'intervallo corretto
 - Talvolta si possono creare situazioni in cui l'intervallo diventa molto più grande
 - Esempio utenti francesi che usano una tastiera americana

24



Momenti statistici

- ❑ L'analizzatore calcola la deviazione standard (i primi due momenti) o altre misure di correlazione (momenti di ordine superiore)
 - Se i valori misurati di un certo momento cadono al di fuori di un certo intervallo vi è un'anomalia

- ❑ Problematiche
 - I profili possono evolvere nel tempo, si possono “pesare” opportunamente i dati o alterare le regole di detection

25



Modelli di Markov

- ❑ L'ipotesi è che la storia passata influenzi la prossima transizione di stato
- ❑ Le anomalie sono riconosciute da sequenze di eventi, e non sulle occorrenze di singoli eventi
- ❑ Il sistema deve essere addestrato per riconoscere sequenze valide
 - l'addestramento è svolto con utenti non anomali
 - l'addestramento produce migliori risultati con una quantità maggiore di dati
 - i dati dovrebbero coprire tutti le sequenze normali del sistema

26



Detection di uso malevolo

- ☐ Si controlla se una sequenza di istruzioni da eseguire è già nota per essere potenzialmente dannosa per la sicurezza del sistema
- ☐ La conoscenza è rappresentata mediante regole e il sistema controlla se la sequenza soddisfa una di queste regole
- ☐ Non si possono scoprire intrusioni non note precedentemente

27



Detection in base a specifiche

- ☐ Si determina se una sequenza di azioni viola una specifica di come un programma o un sistema dovrebbe funzionare

28



Architettura di un IDS

- ☐ E' essenzialmente un sistema di auditing sofisticato
- ☐ Tre attori principali
 - Agente
 - Sorta di logger
 - Direttore
 - Analizzatore
 - Notificatore
 - Esecutore

29



Agente

- ☐ Ottiene le informazioni e le invia al direttore
- ☐ Può mettere le informazioni in altre forme
 - Preprocessing dei record per estrarre parti rilevanti
- ☐ Può cancellare informazioni non necessarie
- ☐ Il direttore può richiedere all'agente ulteriori informazioni
- ☐ Si distinguono in agenti host e agenti network

30



Direttore

- ☐ Colleziona le informazioni inviate dagli agenti
 - Elimina i record ridondanti o non necessari
- ☐ Analizza le informazioni rimanenti per determinare se si è sotto attacco
 - Usa le tecniche viste prima
- ☐ Gira su un sistema separato
 - Non influenza le performance dei sistemi monitorati

31



Notificatore

- ☐ Ottiene i risultati e le informazioni dal direttore
- ☐ Prende le decisioni appropriate
 - Notificare messaggi agli amministratori
 - Riconfigurare gli agenti
 - Rispondere all'attacco

32



Combining Sources: DIDS

- ☐ I monitoraggi di host e di network non sono generalmente sufficienti da soli a scoprire alcuni tipi di attacchi
 - Un attaccante prova a fare telnet con vari login: gli IDS di rete lo possono scoprire, ma non gli IDS di host
 - L'attaccante prova entrare senza la password: gli IDS di host lo rilevano, ma non quelli di rete
- ☐ DIDS usa gli agenti sugli host da monitorare ed un monitor di rete



Risposte alle intrusioni

- ☐ Prevenzione: l'attacco deve essere scoperto prima del completamento
- ☐ Una tecnica è il Jailing: far credere all'attaccante che l'intrusione è andata a buon fine ma confinare le sue azioni in un dominio in cui non può fare danni (o causarne pochi)
 - Far scaricare file corrotti o falsi
 - Imitare il sistema vero



Materiale aggiuntivo: i falsi positivi

- ☐ Si consideri un test progettato per identificare una malattia rara
 - Malattia rara = intrusione
 - Ad esempio, incidenza della malattia (da dati storici): 1/10000
- ☐ Il test è accurato al 99%
 - Se somministrato ad una popolazione malata, il test risulta positivo nel 99% dei casi
 - Se somministrato ad una popolazione sana, il 99% risulta negativo

35



Materiale aggiuntivo: i falsi positivi

- ☐ Si supponga che il test venga somministrato a due persone, A e B con il seguente risultato:
 - A risulta positiva
 - B risulta negativa
- ☐ Qual è la probabilità che A abbia effettivamente la malattia?
 - Ovvero, che ci sia un'intrusione in corso?
- ☐ Qual è la probabilità che B non abbia effettivamente la malattia?
 - Ovvero che non ci sia un'intrusione in corso?

36



Soluzione: Bayes

$$P[pos | M] = 0.99$$

$$P[neg | S] = 0.99$$

$$P[M] = 10^{-4}$$

dati di partenza (M = Malato, S = Sano)

$$P[M | pos] = \frac{P[pos | M] P[M]}{P[pos | M] P[M] + P[pos | S] P[S]}$$

(formula di Bayes)

$$P[S] = 1 - P[M]$$

$$P[pos | S] = 1 - P[neg | S]$$

$$P[M | pos] = 0.0098$$

Probabilità che A sia
malato dato che il test è
risultato positivo

Probabilità che B sia sano
dato che il test è
risultato negativo

$$P[S | neg] = \frac{P[neg | S] P[S]}{P[neg | S] P[S] + P[neg | M] P[M]} = 0.999998$$

37



Considerazioni

- ☐ Quando il risultato è positivo, un singolo test non è sufficiente
 - Attenzione: le ipotesi di partenza è che la malattia sia rara
- ☐ La soluzione somministrare un nuovo test a chi è risultato positivo
 - Il test deve essere diverso, non necessariamente più accurato

38

