Ottimizzazione Combinatoria
Appunti

Giovanni "Qua' Qua' dancer" Palma e Alex Basta

Contents

Chapter 1

Introduzione

Soccia che bononia

Chapter 2

Introduzione alla sicurezza di rete

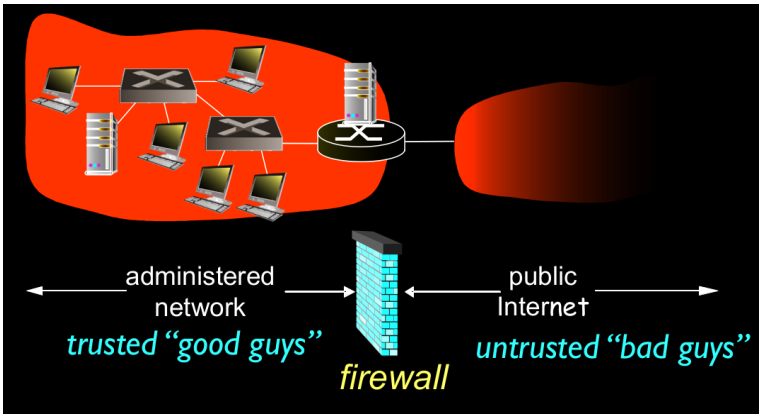
2.1 Firewall e IDS

Innanzi definiamo che cos'è un *Firewall*

Definition 2.1.1: Firewall

Si definisce **Firewall** un sistema di sicurezza che isola una rete interna di un'organizzazione da internet, controllando e filtrando il traffico di rete in entrata e uscita in base a regole di sicurezza definite dette di `ACCESS` o `DENIED`

L'idea del Firewall è che l'esterno di una rete è composta dai cosiddetti "cattivi ragazzi" che la mamma non vi raccomanderebbe come compagni d'uscita, mentre l'interno della rete è composta da "bravi ragazzi" di cui fidarsi, lo scopo del sistema è, quindi, separare i buoni dai cattivi



Il Firewall si rivela utile per principalmente tre motivi:

- **Prevenzione degli attacchi Denial of Service (Dos)**: tipologia di attacco informatico che mira a rendere inaccessibili o indisponibili i servizi di una rete ad utenti legittimi

  Un esempio è il **SYN flooding** in cui un attaccante invia molte richieste di connessione false, esaurendo le risorse del server sovraccaricandolo e impedendo connessioni legittime

- **Protezione dei dati interni da accessi non autorizzati**: ovvero impedisce che gli attaccanti possona *modificare o rubare dati sensibili*

  Un esempio classico è un attaccante che sostituisce il sito web di un'organizzazione con un contenuto malevolo.

- **Accesso selettivo e autorizzato alla rete interna**: Permette l'accesso solo a utenti o dispositivi autenticati, migliorando la sicurezza

Esistono tre tipi di tipoligie di Firewall che approfonoidremo nel dettaglio:

- **Stateless Packet Filter**: Controlla ogni pacchetto singolarmente, senza tenere traccia delle connessioni
- **Statefull Packet Filter**: Tiene traccia dello stato delle connessioni (es. richieste e risposte)
- **Application Gateway** (proxy Firewall): controlla il traffico a livello applicativo (es. HTTP, FTP, e.mail), filtrando così le informazioni che all'interno dei protocolli del livello (ad esempio il contenuto di una mail)

Si notino nel dettaglio

2.1.1 Stateless Packet Filtering

Definition 2.1.2: Stateless Packet Filtering

Lo **Stateless Packet Filtering** è una tecnica di sicurezza di rete in cui un firewall esamina ogni pacchetto individualmente, senza tener conto delle connessioni stabilite in precedenza. Questo significa che ogni pacchetto è valutato isolatamente sulla base di un insieme di regole predefinite

Di solito un firewall con filtraggio stateless è implementato su un router che collega una rete interna a internet. Il router analizza ogni pacchetto in ingresso e in uscita e decide se bloccarlo o lasciarlo in base a regole definite nelle cosiddette "**white list**" (pacchetti che possono passare) e o "**black list**" (lista di pacchetti da bloccare)
Il firewall prende decisioni basandosi su parametri del pacchetto, tra cui:

- **IP** del mittente e destinatario
- **Numero di porta TCP/UDP** del mittente e destinatario
- **Tipo di messaggio ICMP** bloccando, ad esempio, attacchi di scansione provenienti dall'esterno
- **bit SYN e ACK nei pacchetti TCP**: Il firewall può, ad esempio, bloccare pacchetti con SYN in entrata per impedire connessioni indesiderate dall'esterno

Qui degli esempietti:

Example 2.1.1 (Bloccare tutti i pacchetti con protocollo UDP o Telnet)

- **Regola**: blocca i pacchetti in entrata e in uscita se il protocollo IP è 17 (UDP) e se con la porta di origine o desitinazione è 23
- **Risultato**: Tutto il traffico UDP e telnet vengono bloccati

Example 2.1.2 (Bloccare pacchetti TCP in ingresso con ACK=0)

- **Regola**: blocca tutti i pacchetti TCP in ingresso se il bit ACK = 0
- **Risultato**:Le connessioni in entrata non possono essere iniziate da un host esterno verso la rete interna e le connessioni in uscita funzionano normalmente, perché il traffico di ritorno (che ha ACK=1) è consentito.

Riporto qui una tabella con altri esempi:

Politica	**Impostazione Firewall**
Nessun accesso Web esterno.	Elimina tutti i pacchetti in uscita verso qualsiasi indirizzo IP, porta 80
Nessuna connessione TCP in entrata, tranne quelle per il server Web pubblico dell'istituzione.	Elimina tutti i pacchetti TCP SYN in entrata verso qualsiasi IP tranne 130.207.244.203, porta 80
Impedisci alle Web-radio di consumare la larghezza di banda disponibile.	Elimina tutti i pacchetti UDP in entrata - tranne DNS e broadcast del router.
Impedisci alla tua rete di essere utilizzata per un attacco DoS smurf.	Elimina tutti i pacchetti ICMP diretti a un indirizzo di "broadcast" (ad esempio, 130.207.255.255).
Impedisci alla tua rete di essere tracciata	Elimina tutto il traffico ICMP TTL scaduto in uscita

Access control list

Definition 2.1.3: Liste di controllo d'accesso

Le **ACL** sono tabelle di regole applicate, *con priorità dall'alto verso il basso*, ai pacchetti in arrivo per decidere se consentire (allow) o bloccare (deny) il traffico di rete

Queste tabelle sono il vero e proprio cuore pulsante del Firewall e indicano quale pacchetto può passare e chi no

Example 2.1.3 (ACL)

azione	indirizzo sorgente	indirizzo destinazione	protocollo	porta sorgente	p
allow	222.22/16	outside of 222.22/16	TCP	> 1023	8
allow	outside of 222.22/16	222.22/16	TCP	80	>
allow	222.22/16	outside of 222.22/16	UDP	> 1023	5
allow	outside of 222.22/16	222.22/16	UDP	53	>
deny	all	all	all	all	a

Criticità

Un serio problema dei Firewall Stateless che potrebbero lasciare passare pacchetti che non hanno senso nel contesto di una connessione. Esempio:

- Un pacchetto con destinazione porta 80 (HTTP) e ACK=1 arriva dall'esterno
- Il firewall stateless lo accetta, anche se nessuna connessione HTTP è stata avviata da un client interno.
- Un attaccante potrebbe sfruttare questa debolezza per inviare pacchetti falsi alla rete interna

Per porre rimedio a questi tipi di problemi si veda la tipoligia di firewall sucessiva

2.1.2 Stateful packet filtering

Definition 2.1.4: Stateful packet filtering

Lo **Stateful packet filtering** è una tecnica di filtraggio di pacchetti tenendo traccia delle connessioni attive e delle loro fasi

Un firewall stateful tiene traccia di ogni connessione TCP attiva e controlla le tre fasi fondamentali della connessione TCP (assicurandosi che ogni pacchetto in entrata o uscita abbia senso):

- **Setup**: Il firewall rileva il pacchetto SYN iniziale, segnalando l'inizio di una connessione
- **Trasferimento dati**: I pacchetti con ACK vengono accettati solo se appartengono a una connessione già avviata
- **Chiusura**: Quando un pacchetto FIN o un timeout segna la fine di una connessione, il firewall non accetta più pacchetti fino a che non se apre un altro