

Il firewall ipfw

- Introduzione ai firewall
 - classificazione
- Firewall a filtraggio dei pacchetti
 - informazioni associate alle regole
 - interpretazione delle regole
- ipfw
 - configurazione
 - impostazione delle regole

Introduzione ai firewall

Problema: sicurezza di una rete



- Internet è un ambiente insicuro
- Necessità di proteggere reti interne collegate ad Internet
 - imporre restrizioni sul tipo di traffico ammesso
 - definire delle policy di sicurezza
 - filtrare il traffico entrante e uscente

Definizione di firewall



- Firewall
 - dispositivo di sicurezza utilizzato in campo informatico per accettare, bloccare o mediare il traffico dati
 - può essere hardware o software
 - è configurato secondo le policy di sicurezza dell'organizzazione in cui si trova

Classificazione dei firewall



- Si possono individuare tre categorie contraddistinte da:
 - modalità di filtraggio delle comunicazioni
 - ⇒ tra un nodo e la rete o tra reti diverse
 - modalità di gestione dei pacchetti
 - ⇒ livello ISO/OSI dello stack di protocolli
 - capacità di tenere traccia dello stato delle connessioni

Classificazione: filtraggio comunicazione



- Firewall personale (personal firewall)
 - filtra il traffico che transita tra un singolo nodo e una rete
 - applicazione utilizzata in ambito desktop/office
 - ⇒ in esecuzione sullo stesso PC dell'utente
 - ⇒ esempi: Windows Firewall, Zone Alarm, Kerio PF
- Firewall di rete (network firewall)
 - filtra il traffico che transita tra le diverse reti che connette insieme
 - ⇒ dispositivo/computer dedicato
 - ⇒ situato al bordo di una rete (collegamento Internet)
 - ⇒ in genere indicato con il solo termine 'firewall'

Classificazione: gestione pacchetti



- Firewall a filtraggio di pacchetto (packet filtering)
 - operano a livello network/transport
 - ⇒ utilizzano gli header dei pacchetti IP/ICMP/TCP/UDP
- Gateway di applicazione (application gateway)
 - opera a livello applicazione
 - ⇒ proxy server, servizio che permette ai client di effettuare connessioni indirette ad altri servizi
 - tutti i dati sono vincolati a passare attraverso il gateway

Classificazione: stato della connessione



- Firewall stateless
 - ogni pacchetto viene trattato considerandolo singolarmente
 - semplice ma poco potente
- Firewall stateful
 - tiene traccia dello stato delle connessioni che lo attraversano
 - ⇒ flussi TCP, comunicazioni UDP
 - potente ma più complesso e lento
 - ⇒ richiede allocazione di risorse in memoria

Firewall a filtraggio dei pacchetti

Firewall a filtraggio dei pacchetti



- **Funzionamento**
 - accede alle intestazioni dei pacchetti
 - consulta una sequenza di regole (*rule chain*)
- **Insieme delle regole**
 - ogni regola
 - ⇒ è individuata da una serie di informazioni
 - ⇒ specifica l'azione da intraprendere quando le intestazioni dei pacchetti corrispondono alle informazioni specificate
 - ⇒ azioni possibili: accettare, scartare (senza notifica al mittente), scartare con notifica al mittente

Informazioni associate alle regole



- **Informazioni fondamentali utilizzate**
 - indirizzo e porta mittente
 - indirizzo e porta destinatario
 - esempio

Indice	IP sorgente	IP destinatario	Azione
1	131.114.0.0/16	131.114.29.9	Blocca

- **Informazioni aggiuntive**
 - numero della regola (ordine)
 - tipo protocollo e stato della connessione (stateful inspection)

Interpretazione delle regole



- **Il firewall**
 - controlla la corrispondenza delle intestazioni alle regole impostate
 - quando una regola viene soddisfatta allora viene applicata l'azione corrispondente
 - le regole sono processate nell'ordine in cui sono inserite all'interno della catena
 - solo la prima corrispondenza ha effetto

Importanza dell'ordine delle regole (1 di 2)



- L'amministratore di una rete aziendale con indirizzo 222.22.0.0/16 desidera
 - impedire l'accesso da Internet alla rete aziendale
 - consentire l'accesso dalla rete 111.11.0.0/16 (collaboratori esterni) alla sottorete interna 222.22.22.0/24
 - impedire alla singola sottorete 111.11.11.0/24 (collaboratore sgradito) di poter accedere alla sottorete interna 222.22.22.0/24

Importanza dell'ordine delle regole (2 di 2)



Errato!

Indice	IP sorgente	IP destinatario	Azione
1	111.11.0.0/16	222.22.22.0/24	Consenti
2	111.11.11.0/24	222.22.0.0/16	Blocca
3	0.0.0.0/0	0.0.0.0/0	Blocca

Corretto

Indice	IP sorgente	IP destinatario	Azione
1	111.11.11.0/24	222.22.0.0/16	Blocca
2	111.11.0.0/16	222.22.22.0/24	Consenti
3	0.0.0.0/0	0.0.0.0/0	Blocca

Regole default



- Caso in cui nessuna regola è soddisfatta
 - firewall inclusivo (inclusive)
 - ⇒ blocca tutto il traffico che non soddisfa le regole
 - ⇒ corrisponde ad avere come ultima regola 'blocca tutto'
 - ⇒ sicuro ma scomodo: senza definire le regole non si può accedere all'esterno
 - firewall esclusivo (exclusive)
 - ⇒ accetta tutto il traffico che non soddisfa le regole
 - ⇒ corrisponde ad avere come ultima regola 'accetta tutto'
 - ⇒ comodo ma insicuro

ipfw

■ ipfw versione 2

- firewall a filtraggio dei pacchetti con stateful inspection
- firewall presente in FreeBSD
 - ⇒ modulo del kernel
 - ⇒ utility a riga di comando ipfw
- caratteristiche aggiuntive
 - ⇒ accounting
 - ⇒ traffic shaping

■ In fase di compilazione del kernel

- opzioni di logging
- comportamento default
 - ⇒ firewall inclusivo o esclusivo
 - ⇒ in assenza di direttive esplicite il firewall è inclusivo (la regola di default è 'blocca tutto')

■ Dopo l'installazione

- file `/etc/rc.conf`
 - ⇒ direttiva `firewall_enable="YES"`
 - ⇒ direttiva `firewall_type=valore`
- file `/etc/rc.firewall`

- Attraverso il comando ipfw
- Operazioni principali
 - aggiunta/modifica di una regola
 - visualizzazione delle regole
 - cancellazione di una regola/dell'intera catena
- Insieme delle regole
 - valido finché la macchina rimane attiva
 - per sopravvivere al riavvio deve essere salvato in un file (in genere uno script)

■ Sintassi per l'aggiunta di regole

```
$ ipfw [-N] add [index] action [log] protocol pattern options
```

- unico flag `-N` per risolvere gli indirizzi numerici nell'output
- `index`, indice della regola specificata
- `log`, stampa sulla console le regole soddisfatte
- `action`, comportamento da adottare in caso di validità della regola
- `protocollo`, pacchetti su cui agire, opzioni

Indice della regola

```
$ ipfw [-N] add [index] action [log] protocol pattern options
```

- indica la posizione da assegnare alla regola specificata all'interno della catena
- sono disponibili 2^{16} possibili posizioni nella catena
 - ⇒ la regola 65535 è la policy di default (in genere 'blocca tutto')
- se omesso la regola viene collocata 100 posizioni sotto l'ultima regola inserita (esclusa la regola default)

Azione da svolgere

```
$ ipfw [-N] add [index] action [log] protocol pattern options
```

- allow (accept, pass, permit)
 - ⇒ lascia passare il pacchetto e *termina la ricerca*
- deny (drop)
 - ⇒ scarta il pacchetto e *termina la ricerca*
- reject
 - ⇒ scarta il pacchetto, invia al mittente un pacchetto ICMP host o port unreachable e *termina la ricerca*
- reset
 - ⇒ scarta il pacchetto, invia al mittente un messaggio di reset della connessione e *termina la ricerca*

Tipo di protocollo

```
$ ipfw [-N] add [index] action [log] protocol pattern options
```

- all
 - ⇒ tutti i pacchetti, altre opzioni IP nel campo *options*
- icmp
 - ⇒ singoli tipi ICMP nel campo *options*
- udp
- tcp
 - ⇒ opzioni relative allo stato nel campo *options*

Insieme di coppie host-porta

```
$ ipfw [-N] add [index] action [log] protocol pattern options
```

- ha la seguente forma

```
from addrspec [portspec] to addrspec [portspec]  
[via interface]
```

- dove
 - ⇒ *addrspec* specifica un indirizzo o una rete
 - ⇒ *portspec* specifica una o un insieme di porte
 - ⇒ *interface* descrive l'interfaccia da considerare

Campo pattern: formato indirizzo e porta



■ Formato dell'indirizzo

■ indirizzo singolo

- ⇒ address, es. 131.114.29.9
- ⇒ valori speciali any (0.0.0.0), me

■ rete con maschera (numero di bit)

- ⇒ address/mask-bits, es. 192.216.222.1/24

■ rete con maschera numerica

- ⇒ address:mask-pattern, es.
192.216.222.1:255.255.255.0

■ Formato della porta

■ porta singola o range di porte

- ⇒ es. 112, 113 oppure 1-1024

Campo options



■ Opzioni

```
$ ipfw [-N] add [index] action [log] protocol pattern  
options
```

■ direzione del pacchetto

- ⇒ entrante in o uscente out

■ stato della connessione TCP e flag

- ⇒ setup (inizializzazione) established (già attiva)
- ⇒ tcpflags flags (fin, syn, rst, psh, urg, ack)

■ tipo ICMP (numero)

- ⇒ icmp types types (es. 0 per echo reply e 8 per echo request)

■ altre opzioni IP

Visualizzazione delle regole



■ Sintassi per la visualizzazione delle regole

```
$ ipfw [-a] [-c] [-d] [-t] [-N] list
```

- opzione -a, mostra il contatore associato alla regola specificata
- opzione -c, utilizza la forma compatta
- opzione -t, mostra il timestamp relativo all'ultimo match della regola specificata
- opzione -N, risolve il nome degli host/servizi

Cancellazione delle regole



■ Sintassi per la cancellazione di una regola

```
$ ipfw [-q] delete index
```

- opzione -q, disabilita l'output dell'operazione

■ Sintassi per la cancellazione dell'intera catena

```
$ ipfw [-f] [-q] flush
```

- opzione -f, forza la cancellazione
- rimuove tutte le regole tranne la regola default



■ Regole semplici

- bloccare il traffico telnet proveniente dal sito evil.crackers.ru verso l'host trusted.host.org

```
$ ipfw add deny tcp from evil.crackers.ru to trusted.host.org 23
```

```
$ ipfw add deny tcp from evil.crackers.ru to trusted.host.org telnet
```

- bloccare l'intero traffico proveniente dalla rete 169.16.0.0/16 verso la macchina locale

```
⇒ ipfw add deny all from 169.16.0.0/16 to me
```



■ Regole con opzioni stateful

■ schema generale

```
$ ipfw add allow tcp from any to any established  
$ ipfw add allow tcp from trusted.net to my.net  
ports setup
```

...

```
$ ipfw add deny tcp from any to any
```

- la prima regola è soddisfatta per tutti i pacchetti TCP su connessione già stabilita
- la seconda regola è soddisfatta per connessioni TCP iniziate da trusted.net verso l'host my.net alle porte specificate
- l'ultima regola blocca il resto



■ Rispetto alla macchina locale

- bloccare tutto il traffico TCP in ingresso ad esclusione di quello diretto verso il webserver (supponendo che si trovi sulla porta 8080)
- consentire tutto il traffico TCP diretto in ingresso ad esclusione di quello diretto al web server, bloccando la fase di setup della connessione TCP
- bloccare il traffico ICMP in ingresso garantendo il funzionamento del comando ping sull'interfaccia locale