# Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2015/16







# Lezione VII: Tipologie di firewall





## Livelli firewall

In generale si possono avere firewall

- a livello applicativo (application gateway, proxy)
- a livello di trasporto (circuit gateway)
- a livello rete (packet filter)





## Livelli firewall

- Esistono anche ibridi: dynamic packet filter agiscono a livello rete e trasporto (e talvolta anche applicativo).
- Possono essere realizzati via software o hardware (piú veloci, ma piú costosi e meno flessibili nelle configurazioni).

## Stateless filtering

È il metodo piú semplice e piú comune

**Stateless filtering**

Ogni pacchetto (o comando protocollare, se a livello applicativo) è valutato in isolamento, senza tenere traccia di quelli precedenti





## ACL

In pratica si tratta di avere una Access Control List (ACL) che *filtra* i pacchetti o le richieste, uno alla volta

| int addr | int port | ext addr | ext port | action |
|---|---|---|---|---|
| * | * | a.b.c.d | * | block |
| 192.168.2.3 | 110 | * | 110 | allow |





## Digressione: ACL

Una ACL fissa la politica d'accesso: espressa in maniera compatta (e comprensibile). Come va interpretato *il silenzio* dell'ACL?

default deny Vietato tutto ciò che non è **esplicitamente** permesso

default permit Permesso tutto ciò che non è **esplicitamente** vietato





## Default deny

Normalmente l'ACL è una serie di regole che vengono esaminate dalla prima all'ultima, quindi se l'ultima regola è equivalente a

| int addr | int port | ext addr | ext port | action |
|---|---|---|---|---|
| * | * | * | * | block |

si ha *default deny*

# Stateful filtering



**Stateful filtering**

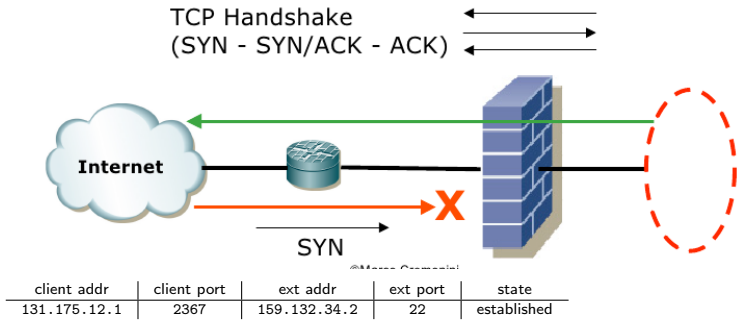
Si tiene traccia di uno *stato* del sistema e il filtraggio avviene sulla **storia** dei pacchetti o delle richieste.

Allo scopo occorre mantenere una tabella delle connessioni



# Stateful filtering






| client addr | client port | ext addr | ext port | state |
|---|---|---|---|---|
| 131.175.12.1 | 2367 | 159.132.34.2 | 22 | established |



# Deep packet inspection



Firewall stateful che operano filtraggio applicativo analizzando il **contenuto** dei pacchetti vengono talvolta detti deep packet filters.

- Analisi del traffico applicativo, la cui liceità va valutata caso per caso
- Generalmente basati su pattern matching di stringhe



# Riassumendo



I firewall si differenziano per

- il livello a cui agiscono
- il tipo di regole di filtraggio
  - stateless
  - stateful
  - "deep packet inspection"

## Configurazioni ricorrenti

SHBH *Single-homed bastion host*

DHBH *Double-homed bastion host*

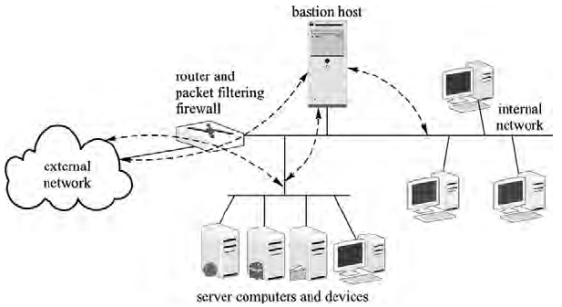
DMZ *Demilitarized zone* (o *screened subnet*)

Un *bastion host* è un nodo particolarmente protetto e capace di difesa prolungata che però può essere lasciato al nemico senza danni per la rete interna.





## Single-homed bastion host

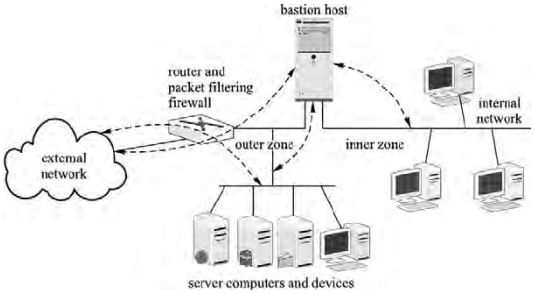



Nel caso il firewall venga compromesso, la rete interna rimane isolata (dal bastion host) dagli attacchi esterni.





## Double-homed bastion host

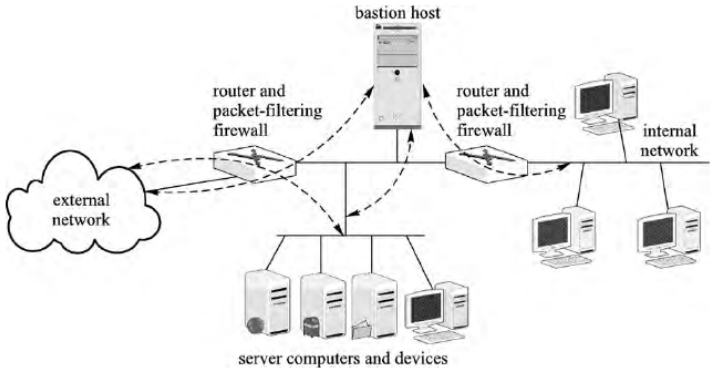



In questo caso si hanno due sottoreti: una "intima" inaccessibile dall'esterno e una piú esterna, ma sempre difesa dal bastion host.





## Screened subnet





Si usano **due** firewall per creare una zona di interdizione

## Effetti di un firewall

Grazie al firewall:

- separazione in zone aventi diverso grado di sicurezza
- solo i componenti esterni al firewall sono direttamente accessibili
- è possibile regolare la "direzionalità" delle connessioni (i socket rimangono bidirezionali, naturalmente)





## Riassumendo

- un firewall realizza una separazione in zone aventi diverso grado di sicurezza
- Alcune delle configurazioni piú comuni prevedono
  - bastion host
  - zone di interdizione





## Stateless filtering TCP

ACL per filtraggio:

| verso | IP src | IP dst | prot. | port src | port dst | flag | azione |
|---|---|---|---|---|---|---|---|
| | | | | | | | |





## Stateless filtering TCP

| | |
|---|---|
| verso | IN/OUT o le zone sorgente e destinazione (es. DMZ→Internet), o delle interfacce (es. eth0→eth1) |
| IP sorgente/destinatario | indirizzi (es. 159.149.10.1, 159.149.10.0/24) o *variabili* |
| protocollo | TCP, UDP, ICMP, IP |
| porta sorgente/destinazione | valore o range (es. $> 1023$) |
| flag | se è attivo ACK (solo TCP) |
| azione | permit, deny |

## Uso di variabili

- scrivere politiche di tipo generale, che possono essere *istanziate* sulla specifica topologia di rete
- modificare indipendentemente politiche e topologia

Esempio

DMZ := 159.149.70.0/24
Internal := 192.168.20.0/24
Private := 10.0.0.0/8
External := not(Internal or DMZ or Private)
WebServer := 159.149.70.11 and 159.149.70.12





## Protezione contro lo spoofing IP

ingress ed egress filtering.

| verso | IP src | IP dst | prot. | port src | port dst | flag | azione |
|---|---|---|---|---|---|---|---|
| OUT | Internal | Any | IP | Any | Any | * | Permit |
| IN | External | Internal | IP | Any | Any | * | Permit |
| Any | Any | Any | Any | Any | Any | * | Deny |





## SSH con stateless filtering

La politica da implementare autorizza solo connessioni SSH dall'interno della rete aziendale verso l'esterno.
**semplificazione: identifichiamo SSH con i pacchetti TCP con porta destinazione 22**(si noti che talvolta si cambia la porta proprio per ragioni di sicurezza!)

| verso | IP src | IP dst | prot. | port src | port dst | flag | azione |
|---|---|---|---|---|---|---|---|
| OUT | Internal | Any | TCP | $> 1023$ | 22 | * | Permit |
| IN | Any | Internal | TCP | 22 | $> 1023$ | * | Permit |
| Any | Any | Any | Any | Any | Any | * | Deny |





## SSH con stateless filtering

In realtà però possiamo notare che i pacchetti provenienti dall'esterno della rete dovrebbero essere solo risposte del server: quindi ACK deve essere settato.
Inoltre solo alcuni server ssh potrebbero essere autorizzati.

# SSH

sshSrvs := 159.149.70.13 and 159.149.70.42

| verso | IP src | IP dst | prot. | port src | port dst | flag | azione |
|---|---|---|---|---|---|---|---|
| OUT | Internal | sshSrvs | TCP | $> 1023$ | 22 | 1/0 | Permit |
| IN | sshSrvs | Internal | TCP | 22 | $> 1023$ | 1 | Permit |
| Any | Any | Any | Any | Any | Any | * | Deny |





# Riassumendo

- ingress ed egress filtering
- La scrittura delle regole di filtering impone di adattare la politica di sicurezza al *modello* imposto dal meccanismo di filtraggio
  - `SSH == tcp port 22`
- Occorre una conoscenza approfondita di protocolli e applicazioni