Sicurezza delle reti[1]

Mattia Monga

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

a.a. 2010/11

[1]

Lezione VII: Sicurezza perimetrale

Sicurezza perimetrale

Poiché in Internet è una rete di reti (locali) si parla di protezione del perimetro di sottorete.

Firewall

Un firewall (*parete tagliafuoco*) è un dispositivo che:

- si trova al confine fra due reti A e B
- tutto il traffico in transito tra A e B (e viceversa) deve passare attraverso di esso
- filtra il traffico in transiti secondo una precisa politica d'accesso (*policy*)

Il compito dei firewall è stabilire quale traffico ha accesso alla rete (*policy*) e non controllare che il traffico permesso non faccia danni (*control*, intrusion detection).

Cosa sono i Firewall

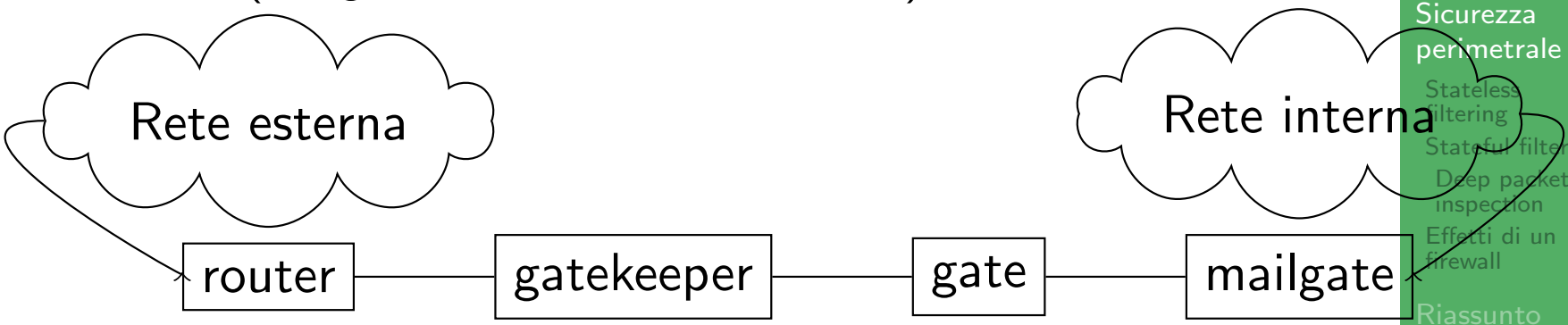
Tipicamente sono realizzati come

- Forwarding gateway
- Filtering router
- Proxy

E stabiliscono politiche (regole) ai livelli dello stack TCP/IP

Firewall a vari livelli

I primi firewall (Mogul, 1989 e Ranum, 1992) e



- Gatekeeper proxy applicativo: raccoglie le richieste applicative (Telnet, FTP, SMTP, ...) dall'interno e le manda verso l'esterno
- Gate filtra il traffico

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*)

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

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: generalmente però la si vuole specificare 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

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*

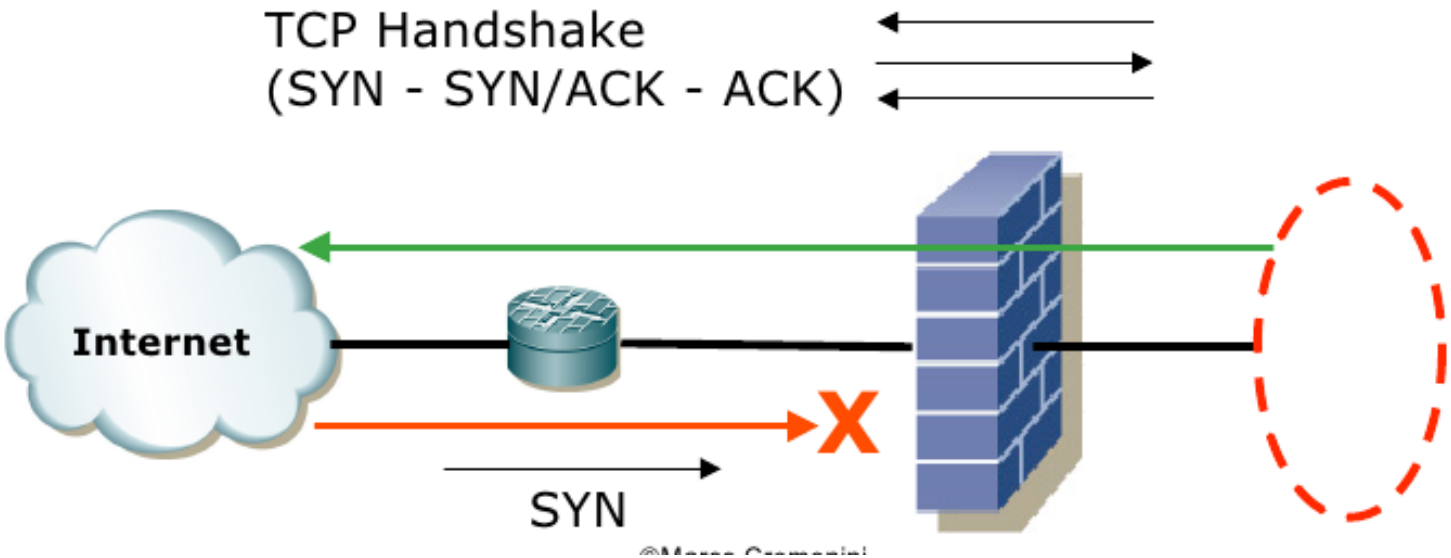
Stateful filtering

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
Naturalmente questo tipo di filtro è molto piú oneroso rispetto a quello *stateless*.

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

Configurazioni ricorrenti

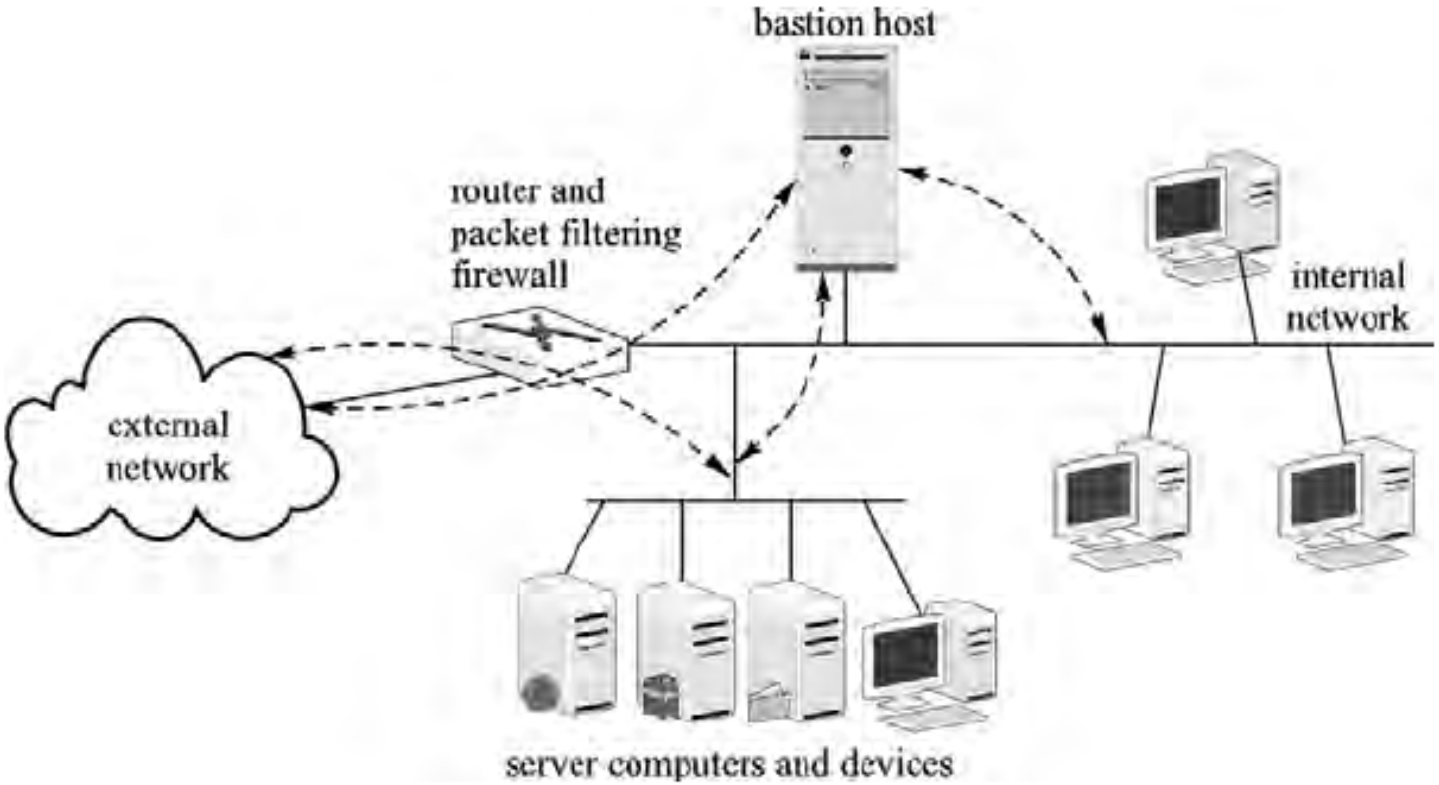
SHBH *Single-homed bastion host*

DHBH *Double-homed bastion host*

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

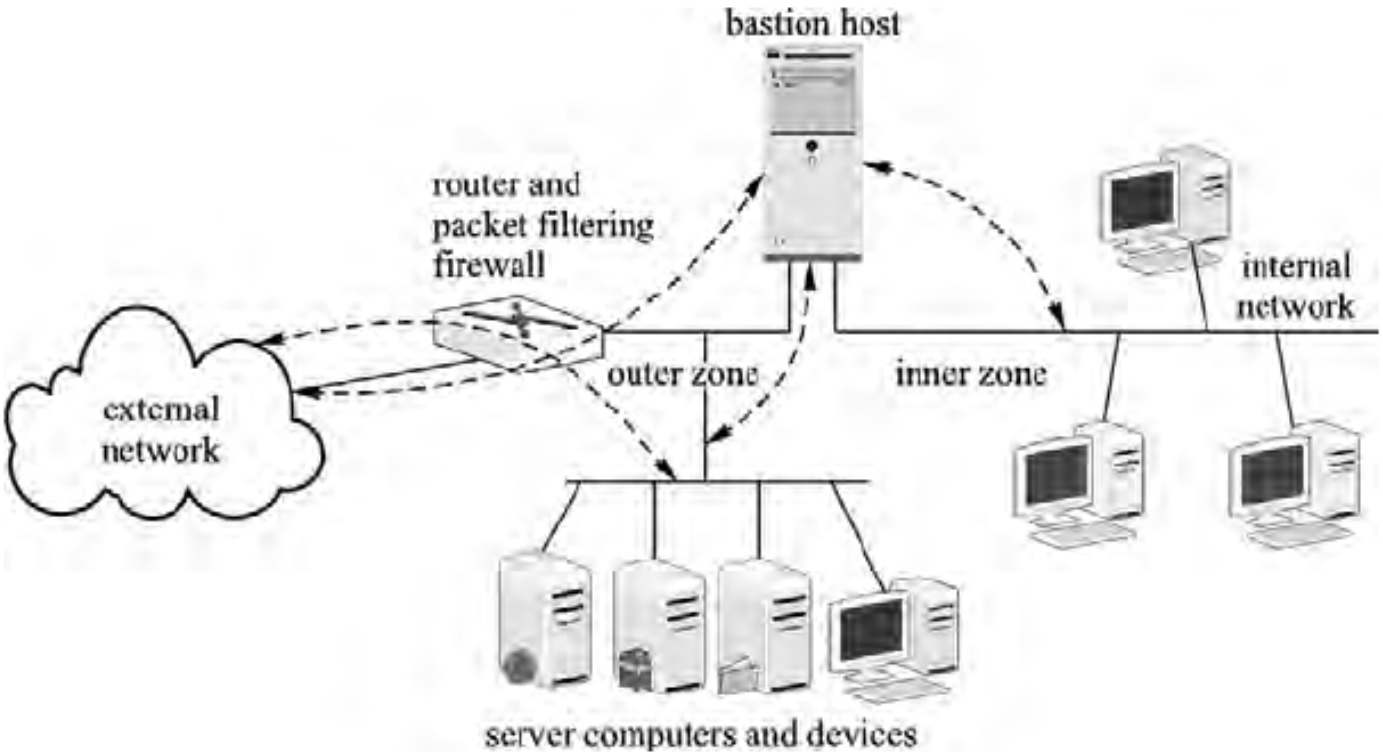
Un *bastion host* è un nodo particolarmente protetto e capace di difesa prolungata che però può essere lasciato al nemico senza danni per la rete interna.

Single-homed bastion host



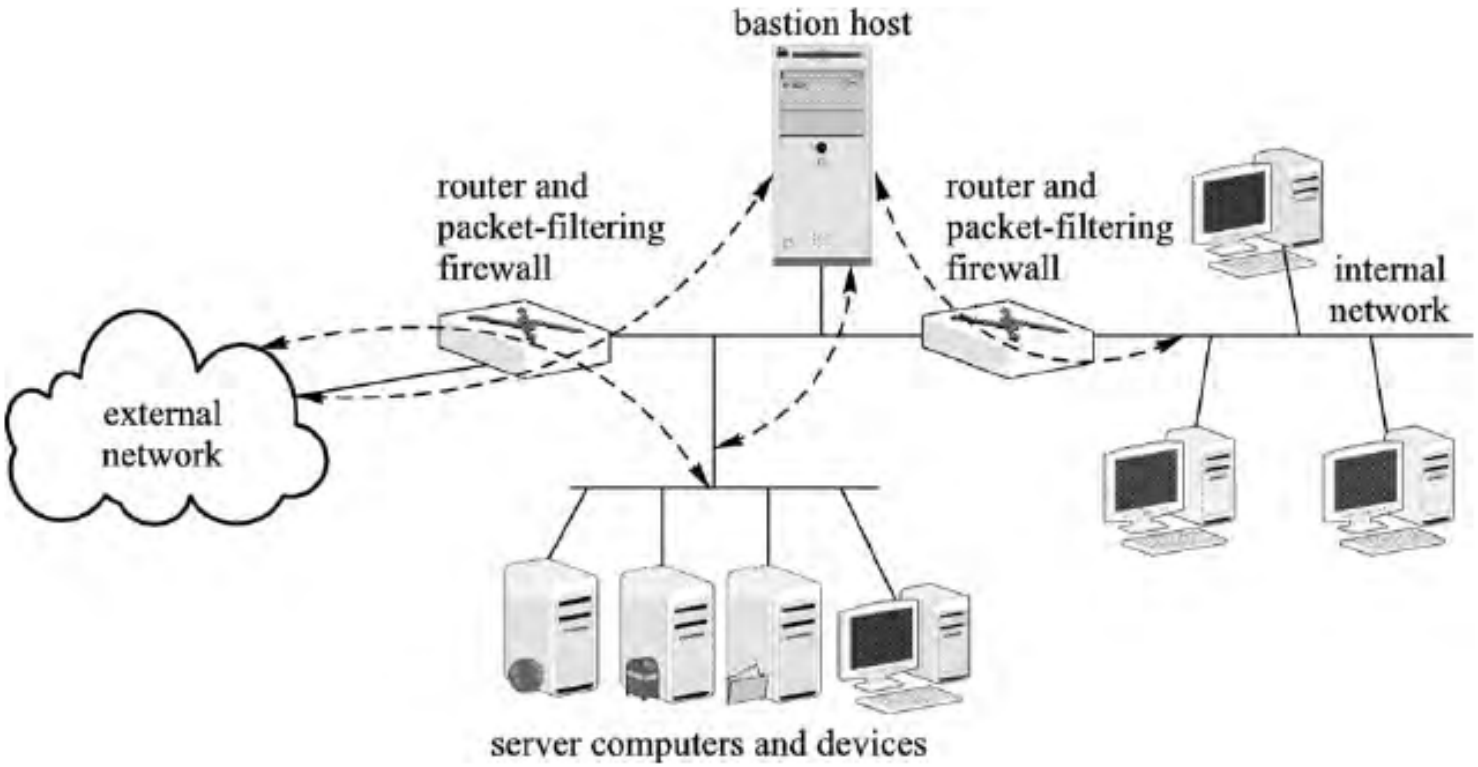
Nel caso il firewall venga compromesso, la rete interna rimane isolata (dal bastion host) dagli attacchi esterni.

Double-homed bastion host



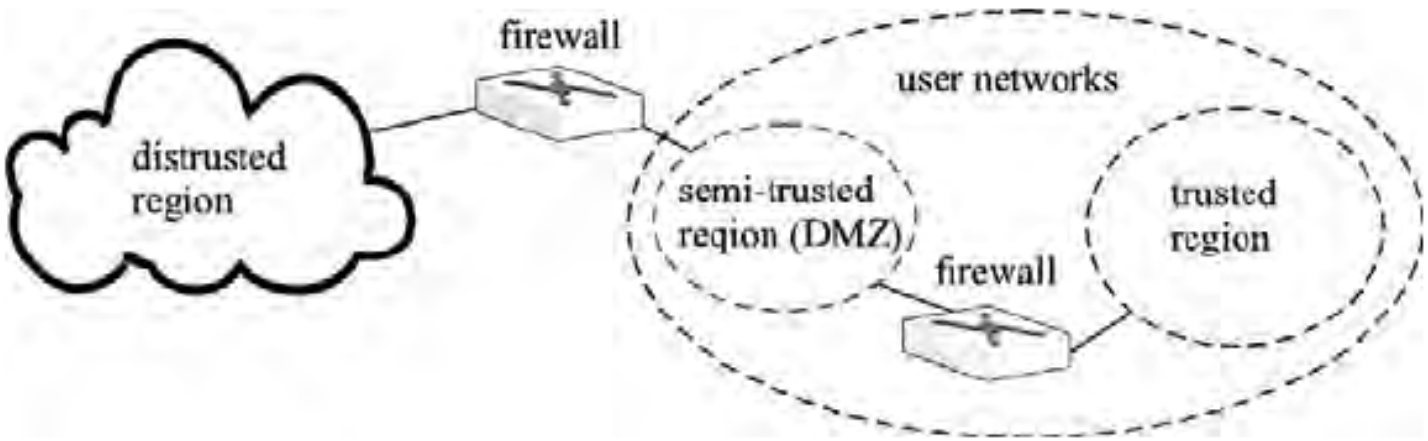
In questo caso si hanno due sottoreti: una "intima" inaccessibile dall'esterno e una piú esterna, ma sempre difesa dal bastion host.

Screened subnet



Si usano due firewall per creare una zona di interdizione

Screened subnet



Si usano due firewall per creare una zona di interdizione

Effetti di un firewall

Grazie al firewall:

- per tutte le sottoreti protette da un firewall si possono definire politiche di accesso
- solo i componenti esterni al firewall sono direttamente accessibili
- è possibile regolare la "direzionalità" delle connessioni (anche se i socket rimangono bidirezionali, naturalmente)
- realizza una separazione in zone aventi diverso grado di sicurezza nell'architettura di rete

Riassunto dei punti fondamentali

- Un firewall è un dispositivo capace di regolare il traffico fra due reti
- Il filtraggio può avvenire ad ogni livello
- I filtri possono essere
  - Stateless: semplici ed efficaci in molti casi comuni, ma rozzi nelle politiche
  - *Stateful*: piú onerosi, ma molto piú flessibili
- un firewall realizza una separazione in zone aventi diverso grado di sicurezza
- Alcune delle configurazioni piú comuni prevedono
  - bastion host
  - zone di interdizione