Reti locali e architetture firewall

Gianni Bianchini
giannibi@dii.unisi.it

Master in Economia digitale & E-business

Centro per lo studio dei sistemi complessi - Università di Siena
Giugno 2004

Sommario

- Motivazioni. Servizi internet, tipologie di attacco, approcci alla sicurezza
- Progetto di un firewall per una rete aziendale
  - Architetture tipiche
  - Host bastione
  - Filtraggio e proxying
- Filtraggio del traffico di rete
  - Indirizzamento delle reti private
  - Filtraggio a livello applicazione e trasporto
    - Filtraggio stateless e stateful
    - Traffico TCP, UDP, ICMP, casi tipici
    - Attacchi
  - Il paradigma netfilter (kernel Linux)
- Esempio applicativo

Motivazioni

Molte problematiche di sicurezza dei sistemi informatici ed in particolare delle reti nascono dalla necessità di proteggere

- Dati
  - Privacy
  - Integrità
  - Disponibilità
- Risorse
  - Integrità hardware e software
  - Tempo di calcolo / memoria
- Reputazione
  - Furto di identità (es. accesso a chiavi private)
  - Catena di attacchi (mascheramento provenienza originaria)
  - Presenza materiale indesiderato in archivi pubblici
  - Web site defacement

Alcune tipologie di attacco

- Intrusione
  - Accesso non autorizzato
  - Scalata privilegi
  - Modifica dei sistemi (installazione backdoors)
- Denial of service
  - Network flooding
  - Resource exhaustion
  - Disabilitazione / danneggiamento dei servizi
- Furto di informazioni
  - Sfruttamento servizi per accesso ad informazioni addizionali
  - Accesso agli archivi
  - Intercettazione attività dei sistemi
  - Monitoraggio traffico di rete (sniffing)

Sicurezza: due filosofie

- Security through obscurity
  - Non rivelazione delle caratteristiche dei sistemi e degli algoritmi

    "The attacks to network-connected computers by hackers [...] aren't possible if you connect to Internet using a modem and XXX.it [...] No one will ever know which IP you will have next time you connect, and so you will be less vulnerable during your Internet connections using XXX.it" - Dal sito web di un noto ISP italiano, 1998
  - "Alibi" per l'attività di auditing/correzione di vulnerabilità
  - Inefficace sul lungo termine

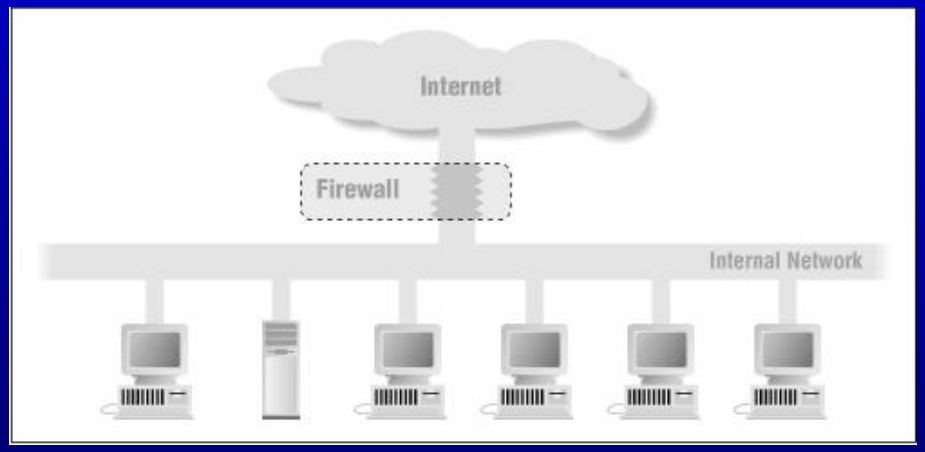
- Sicurezza "logica" e full disclosure
  - Il funzionamento del sistema, gli algoritmi impiegati e le soluzioni di protezione sono perfettamente note
  - La sicurezza è demandata alla segretezza delle informazioni di accesso (password, chiavi)
  - Eventuali vulnerabilità vengono rese pubbliche
  - Implica continue verifiche di affidabilità degli algoritmi e correzione dei problemi anche on-site

Sicurezza delle reti: approcci

- Sicurezza a livello singola macchina (“host level”)
  - Ogni sistema è dotato di misure di protezione individuali
  - Non scalabile e di difficile gestione
  - Schema prono ad errori
  - Non si adatta ad ambienti eterogenei per architetture e software
- Sicurezza a livello rete (“network level”)
  - Controllo d’accesso concentrato (hw/sw dedicato)
  - Scalabile, gestibile, adattabile
  - Minore flessibilità
- Problemi estranei ai modelli di sicurezza
  - Accesso fisico ai sistemi
  - Azioni dannose da parte di utenti legittimi
  - Essere comunque preparati ad intrusioni (IDS, sistemi di backup)

Che cos'è un firewall?

- Letteralmente: "muro ignifugo": insieme di apparati solitamente disposti all'interfaccia tra la rete locale e la rete Internet



- Funzioni logiche
  - ⋆ Separazione
  - ⋆ Restrizione
  - ⋆ Analisi
- Realizza il modello "network level"

Che cos'è un firewall?

- Funzioni fondamentali
  - ⋆ Definizione dei punti di ingresso/uscita dalla rete
  - ⋆ Definizione delle modalità di accesso alle risorse della rete
  - ⋆ Blocco di traffico e servizi non ammessi
  - ⋆ Analisi (logging) degli accessi e monitoraggio del traffico
  - ⋆ Separazione e mantenimento delle relazioni di fiducia (trust) tra porzioni diverse della stessa rete
  - ⋆ Modulazione del traffico (traffic shaping)

⇑

Politica di sicurezza (policy)

- Realizzazione hardware e software
  - ⋆ Routers, computers con software dedicato
  - ⋆ Soluzioni commerciali integrate

Che cos'è un firewall?

- Limitazioni
  - Nessuna protezione da utenti legittimi
  - Nessuna protezione in caso di punti d'accesso non controllati
  - Limitata protezione da tipi di attacchi non noti a priori
  - Limitata protezione da codice maligno che raggiunge la rete con modalità ammesse
    - Scaricamento software infetto (di difficile riconoscimento)
    - Introduzione di codice maligno codificato (es. email attachments) mitigabile con tecniche di content filtering anche a livello del firewall
  - Limitata protezione da attacchi a servizi pubblicamente accessibili
    - Sfruttamento (exploit) di vulnerabilità di programmi server mediante richieste legittime (necessari content filtering ed informazioni a priori)
    - Importante! Necessità di isolamento delle risorse potenzialmente compromissibili da quelle sensibili
  - Limitata protezione da worms che sfruttano traffico "ammissibile" (email, www)

Alcune regole d'oro

- Minimo privilegio
  - Ogni ente (sistema, utente, programma) non deve disporre di privilegi superiori a quelli strettamente necessari a svolgere le proprie funzioni
  - Limitazione possibili danni
  - Difficoltà a livello di progettazione, configurazione ed uso
- Difesa in profondità
  - Ridondanza, meccanismi di sicurezza multipli (sicurezza a livello rete + host)
  - Educazione dell'utente

    "I cretini sono sempre più ingegnosi delle precauzioni che si prendono per impedir loro di nuocere" (da "La legge di Murphy")
- Limitazione e monitoraggio dei punti d'accesso

Alcune regole d'oro

- Fail-safe defaults
  - In caso di malfunzionamento, il comportamento predefinito deve essere sicuro
  - Default = deny: "prima si chiude tutto, poi si apre solo ciò che serve"
  - Partecipazione universale: minimizzare le deroghe
- Diversificazione dei sistemi hw/sw
- Semplicità
  - Evitare l'uso di programmi complessi specialmente se non se ne sfruttano tutte le funzionalità

"Ogni catena è resistente quanto il suo anello più debole"

Progetto di un sistema firewall - Definizioni

- Firewall
  Insieme di componenti che regola gli accessi ed il traffico tra due o più reti

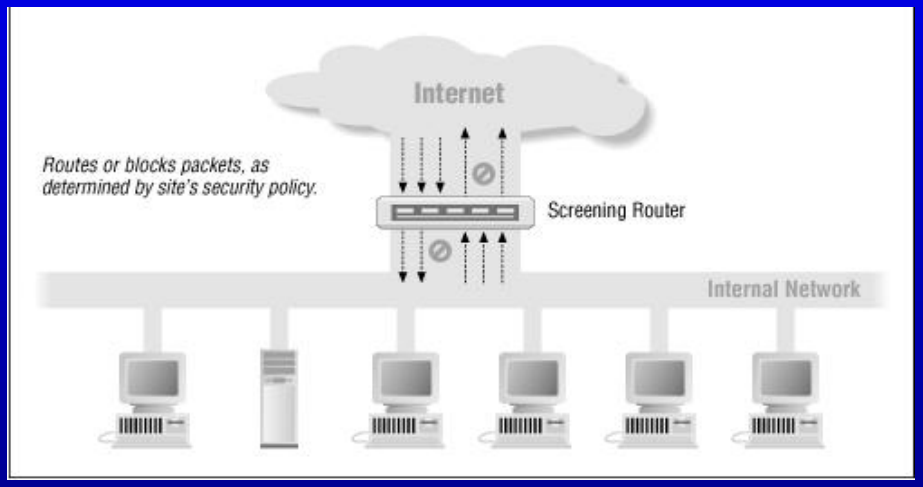
- Host bastione
  Sistema la cui sicurezza deve essere salvaguardata in modo particolare, poiché esposto ad attacchi (es. fornisce servizi pubblicamente accessibili o rappresenta il punto di interfaccia tra la rete Internet ed una rete interna)

- Host dual-homed
  Host interfacciato a più di una rete (es. accessibile tanto da Internet quanto da una rete interna)

- Router
  Apparecchio che effettua l'instradamento del traffico tra due o più reti

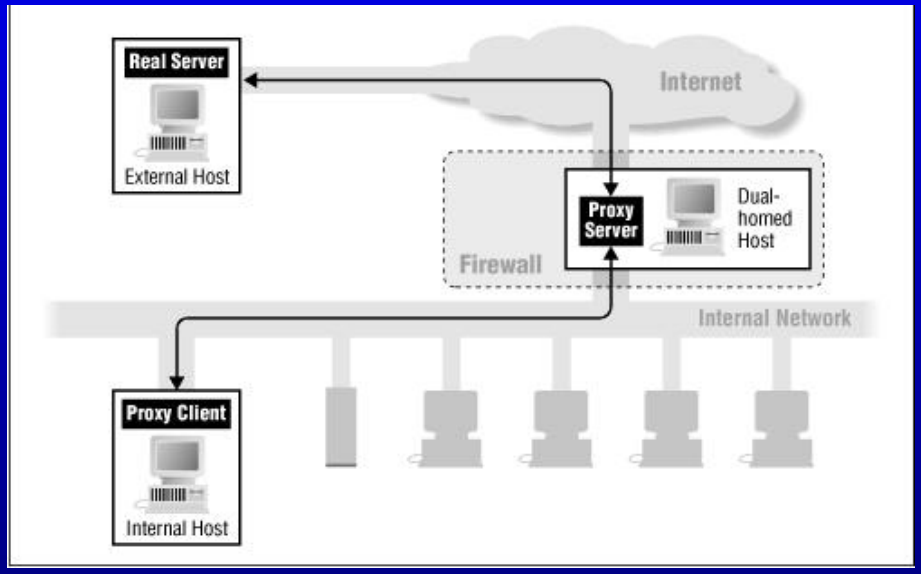
- Proxy server
  Sistema che prende in carico richieste a server esterni per conto di client interni, filtrando eventualmente tali richieste

Router filtrante (TCP/IP)



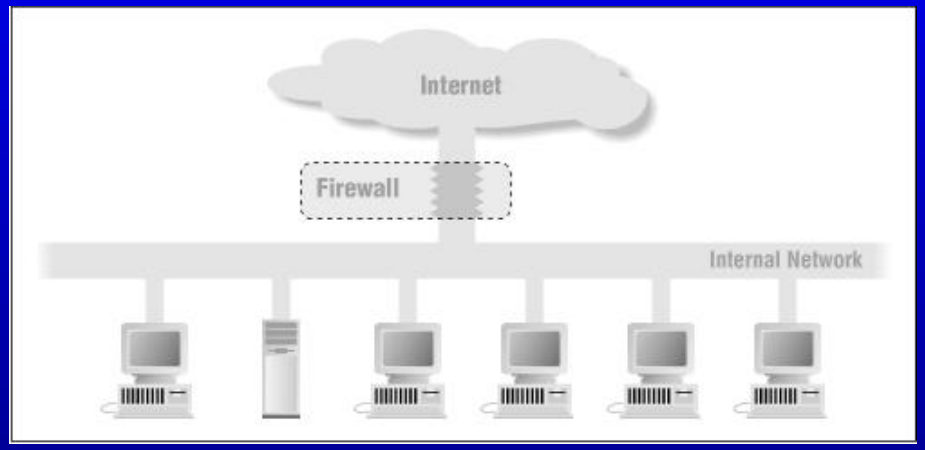
- Filtraggio sulla base dell'informazione contenuta nel singolo pacchetto
  - Indirizzo IP sorgente
  - Indirizzo IP destinazione
  - Tipo di protocollo di trasporto (TCP, UDP, ICMP, ...)
  - Porta TCP/UDP sorgente
  - Porta TCP/UDP destinazione
  - Tipo di messaggio ICMP
- Esempio: blocco connessioni entranti tranne quelle sulla porta `25/TCP` dell'host `mail-server` e su `80/TCP` dell'host `www-server`

Proxy server (Application gateway)



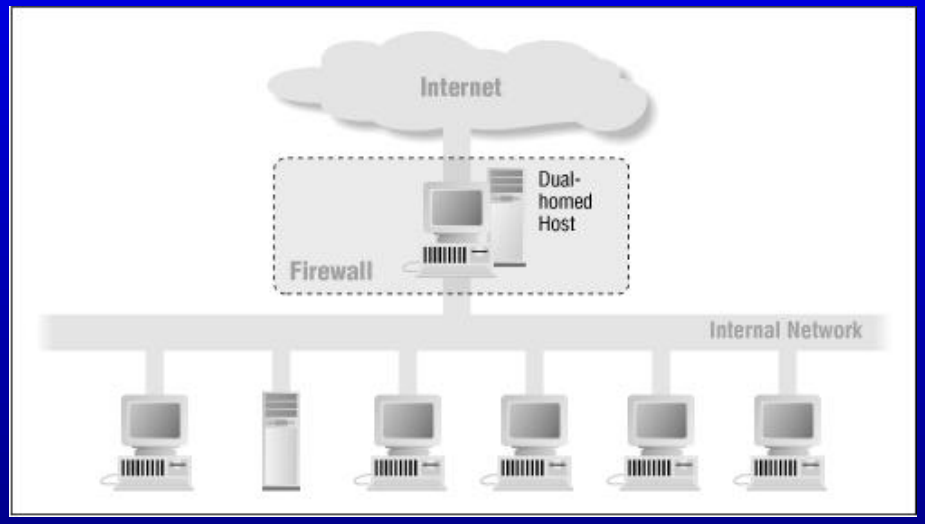
- Lavora a livello applicazione
- Funge da tramite fra client e server inoltrando le richieste e presentando le risposte
- Filtra le richieste in accordo con la policy di sicurezza
- Effettua funzioni di caching

Architetture



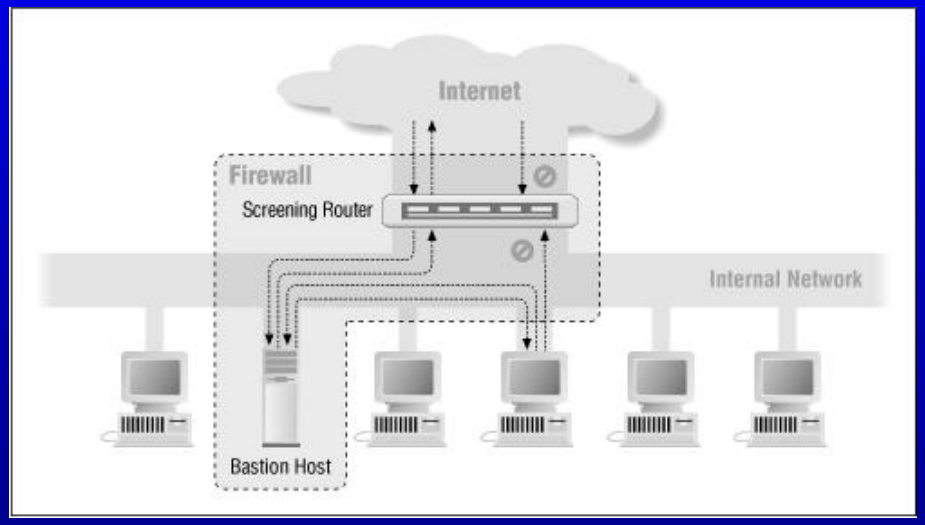
- Dual-homed host
- Screened host
- Screened subnet
- Architetture combinate

Architettura dual-homed host



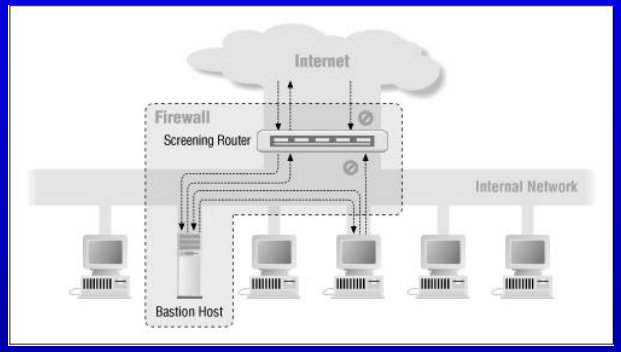
- No routing (traffico IP diretto non consentito)
  - ⋆ Accesso solo mediante application gateway (HTTP, SMTP, ...)
  - ⋆ Accesso mediante login esplicito sul dhh
    - ∗ Necessaria particolare attenzione agli account
- Non adeguata a fornire servizi pubblicamente disponibili
  - ⋆ Possibile compromissione diretta di host sulla rete interna

Architettura screened host



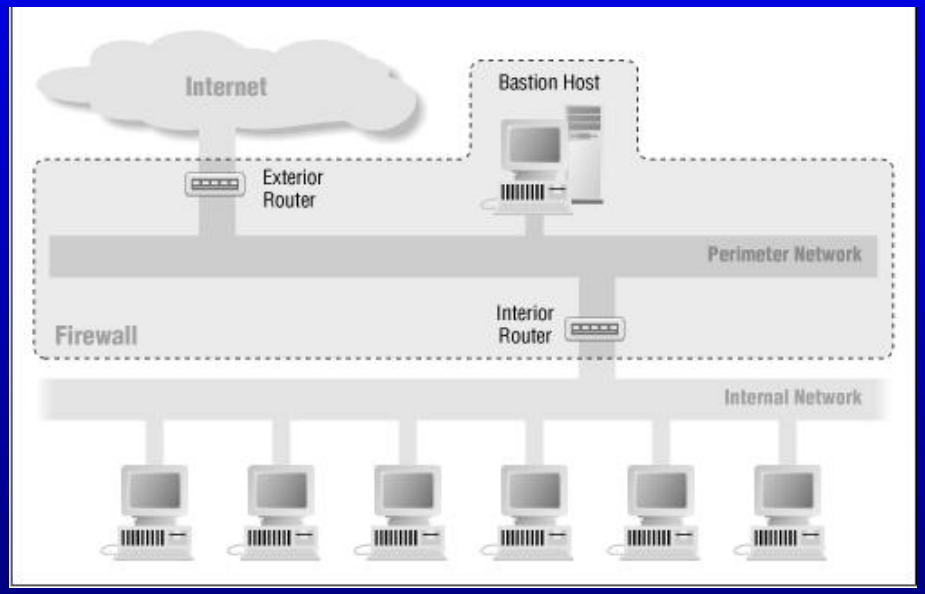
- Router filtrante + host bastione nella rete interna
- Servizi pubblicamente accessibili
  - ⋆ Connessioni dall'esterno permesse verso il solo bastione per i protocolli ammessi
- Accesso esterno
  - ⋆ Accesso diretto coi protocolli consentiti via packet filtering
  - ⋆ Accesso indiretto mediante proxy sul bastione

Architettura screened host



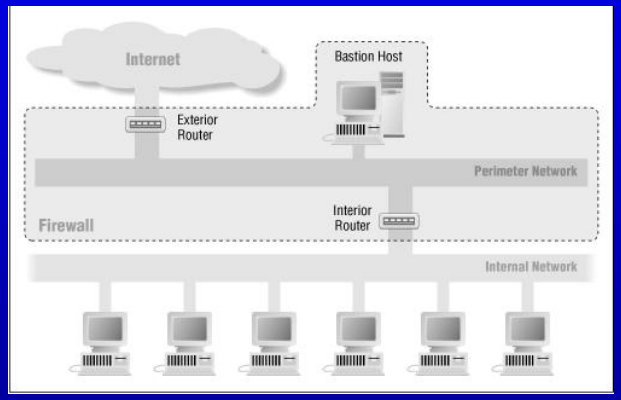
- Debolezze
  - La compromissione del bastione implica la compromissione della rete interna (single point of failure)
  - Necessarie forti misure di sicurezza host level
  - La compromissione del router implica la compromissione della rete interna
- Vantaggi
  - Configurazione del router meno prona ad errori rispetto a quella del dual-homed host

Architettura screened subnet



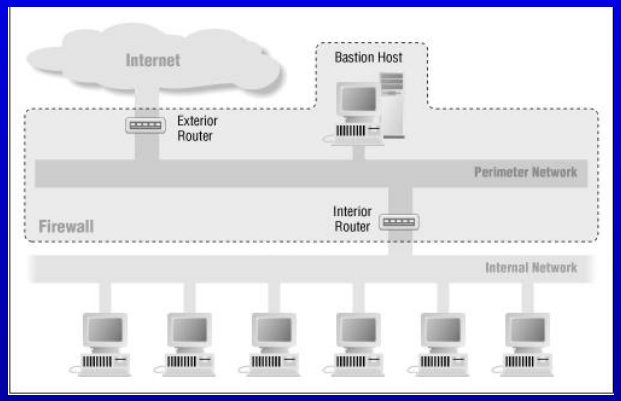
- Rete perimetrale (DMZ, DeMilitarized Zone)
- L'intrusione sugli host bastione NON dà accesso diretto alla rete interna (multiple points of failure)
- Possibilità strati multipli
  - ⋆ Strati più esterni: risorse più vulnerabili e/o meno critiche
  - ⋆ Strati più interni: risorse maggiormente critiche

Architettura screened subnet



- DMZ
  - ⋆ Impossibilità di intercettare il traffico sulla rete interna
  - ⋆ Possibile intercettazione del traffico Internet - rete interna e rete interna - bastione
- Bastione
  - ⋆ Fornisce i servizi esterni (HTTP, SMTP, ...)
  - ⋆ Può agire da proxy per connessioni uscenti (altrimenti possibili attraverso packet forwarding)

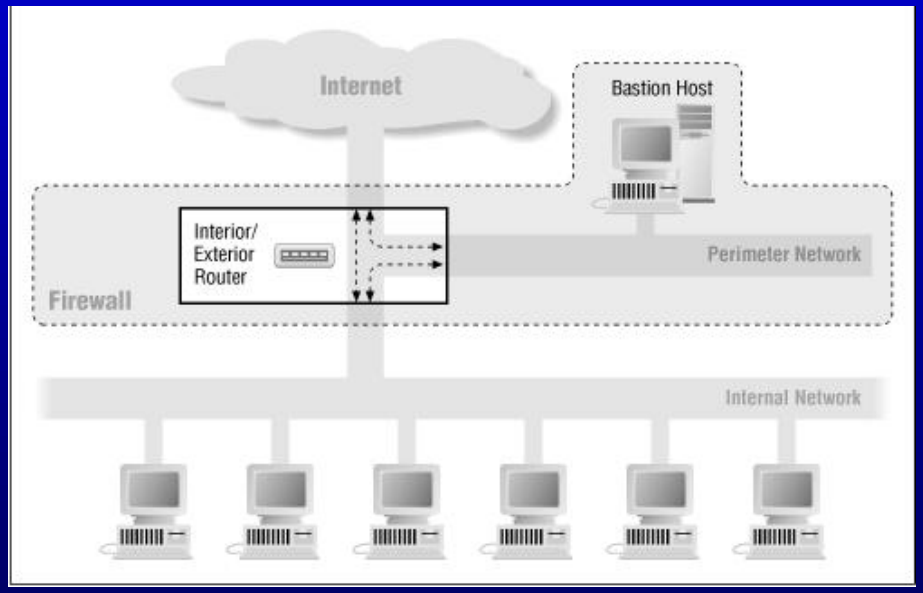
Architettura screened subnet



- Router interno
  - Protezione dell'accesso alla rete interna dall'esterno *e* dalla DMZ
  - Importante. Ridurre al minimo il livello di fiducia della rete interna nei confronti del bastione
    - No possibilità di connessione ai servizi interni
    - No possibilità di uso di risorse interne (es. file system condivisi)
- Router esterno
  - Protezione della DMZ e filtraggio ridondante dell'accesso alla rete interna
  - Prevenzione IP spoofing

Architettura screened subnet - varianti

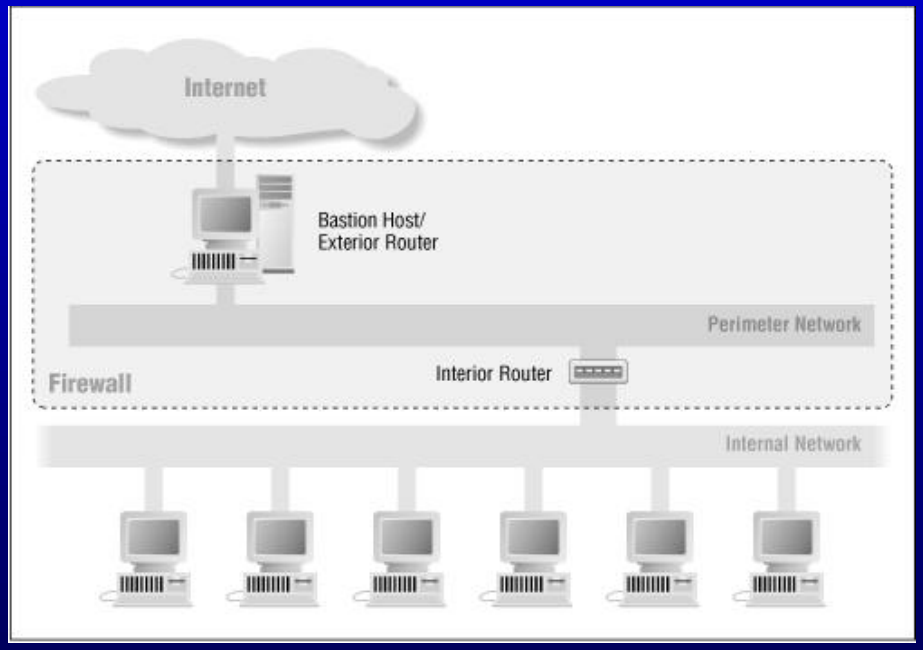
- Router unico



  - ⋆ Maggiore complessità del router
  - ⋆ Disponibili soluzioni commerciali

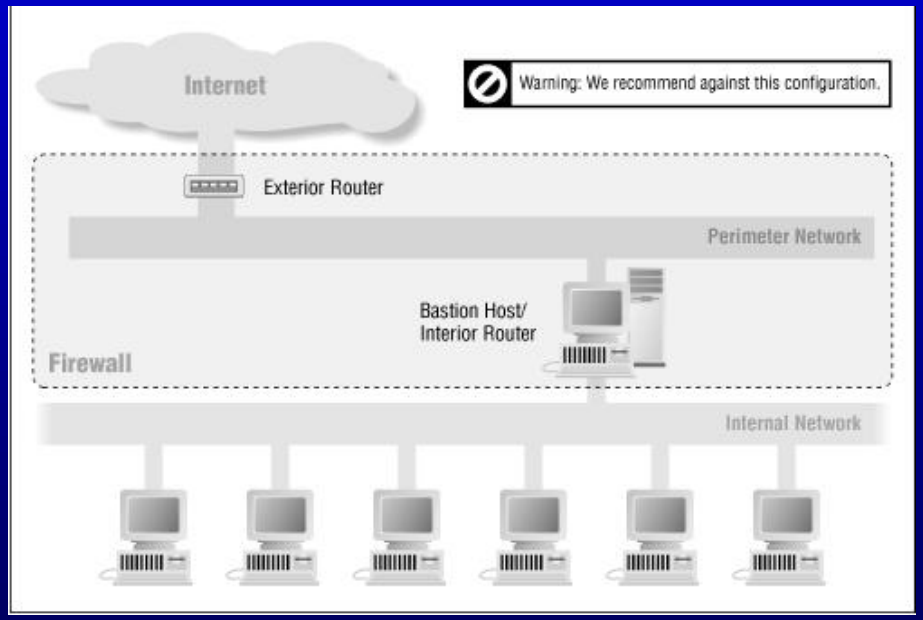
Architettura screened subnet - varianti

- Router e host bastione combinati



Screened subnet - Varianti pericolose

- Combinazione di bastione e router interno

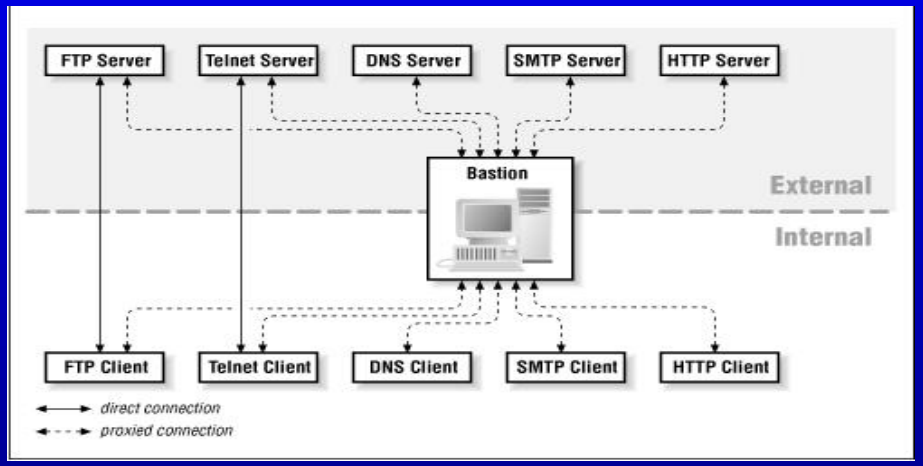


- ⋆ Espone la rete interna se il bastione è compromesso
- ⋆ Le regole di filtraggio del router possono venir modificate

Host bastione

- Configurazione tesa alla minimizzazione del danno in caso di compromissione
- Locazione fisica: prevenire intercettazione di informazioni riservate
  - Rete perimetrale (DMZ)
  - Rete interna dietro ethernet switch
    - Necessità di misure a livello host sui client della rete interna per limitare il trust nei confroni del bh

Host bastione - servizi



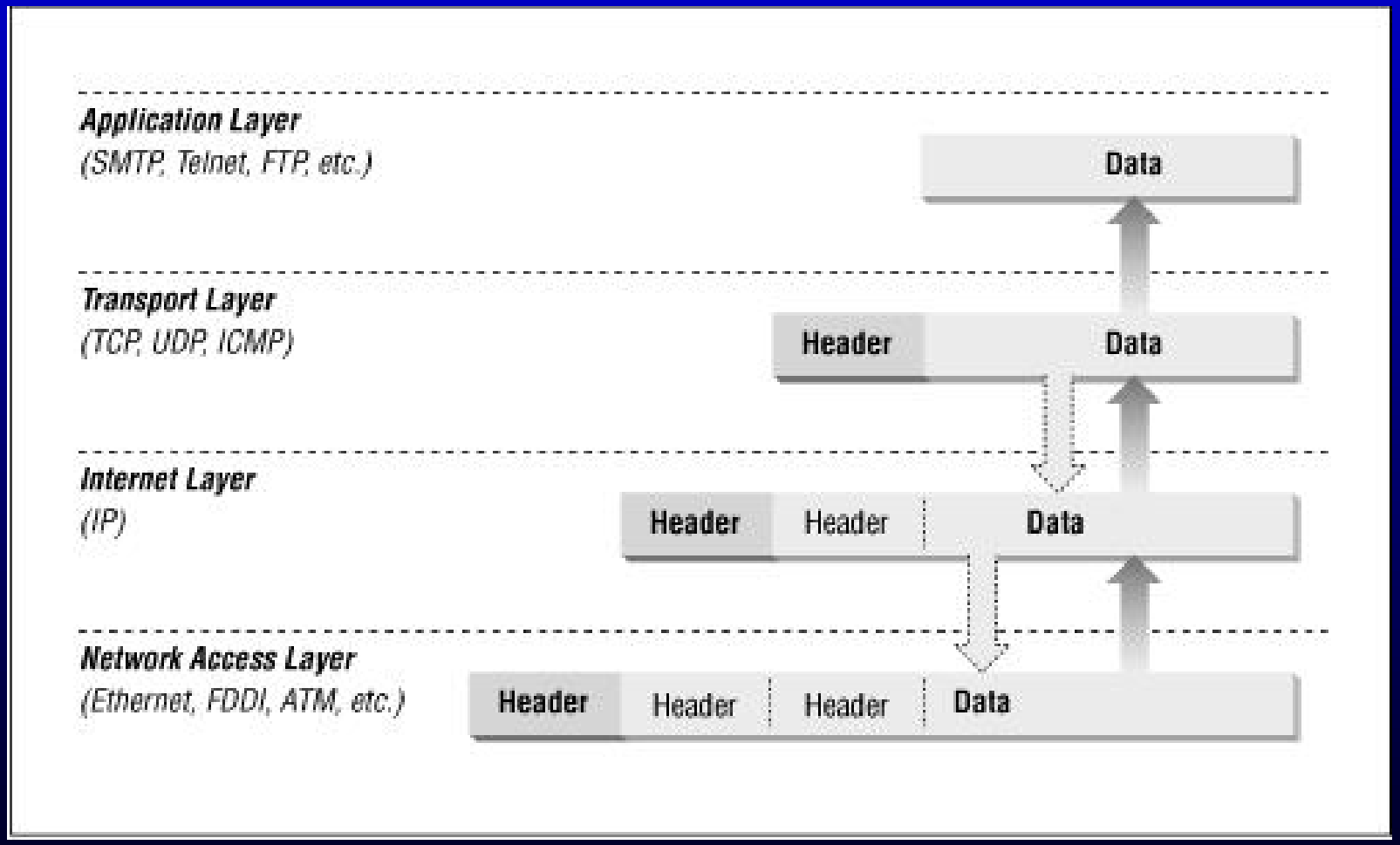
- Con accesso diretto (routing + packet filtering)
  - ⋆ Servizi “sicuri”, es. accesso interattivo SSH
- Via proxy
  - ⋆ HTTP, FTP, SMTP
  - ⋆ Accesso “non sicuro” alla rete interna (es. FTP, TELNET): evitare o usare misure addizionali (es. one-time passwords sul proxy)
- Evitare account utente sul bastione

Indirizzamento reti interne

- Indirizzi IP pubblicamente instradabili
  - Assegnazione da parte del Network Information Center (NIC) locale
- Indirizzi IP privati (RFC 1918)
  - `10.0.0.0/8`
  - `172.16.0.0/12`
  - `192.168.0.0/16`
- IP masquerading (source NAT)
  - Mappatura di più indirizzi privati su un unico indirizzo pubblico mediante riscrittura
  - Alternativa: proxying connessioni uscenti
- Forwarding (destination NAT)
  - Inoltro connessione esterna a indirizzo privato
  - Alternativa: proxying connessioni entranti

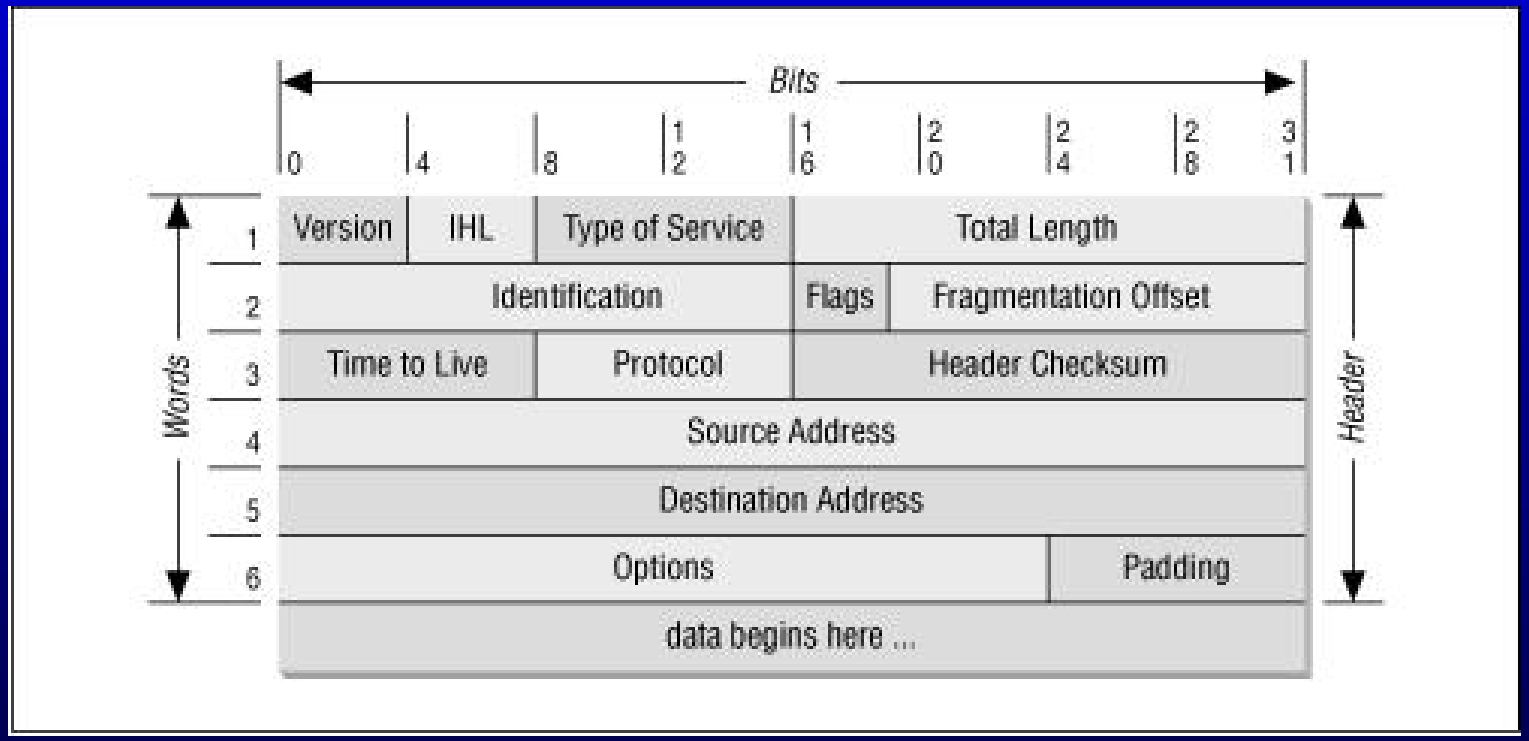
Packet filtering

- Incapsulamento dati



Packet filtering

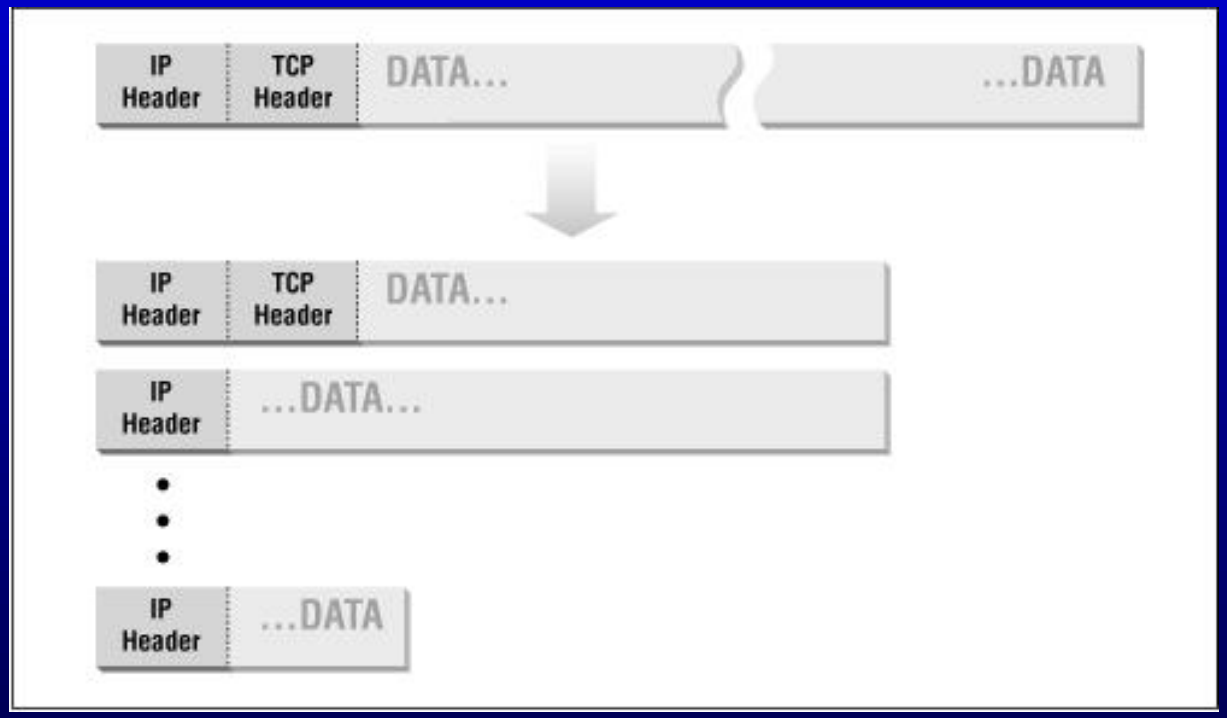
- IP: anatomia di un pacchetto



- Confronto delle informazioni contenute nell'header con regole assegnate
  - ⋆ Esempio: non inoltrare le connessioni dalla rete `192.168.0.0/16`
    - ∗ `DENY FWD src=192.168.0.0/16 dest=any`

Packet filtering

- IP: frammentazione



- I frammenti sono riassemblati a livello dell'host destinazione
- Campo header presente solo nel primo frammento
- I frammenti successivi al primo non vengono di solito filtrati
  - Possibilità di fuga di informazioni "non formattate"

Packet filtering - approcci

- Filtraggio stateless
  - La decisione sull'instradamento o meno di un pacchetto è presa esclusivamente sulla base della sola informazione contenuta nei campi header del pacchetto stesso
    - Indirizzo di provenienza/destinazione (`src/dest`)
    - Protocollo di trasporto (`proto=TCP/UDP/ICMP`)
    - Informazioni addizionali (porta sorgente/destinazione, flag)
- Stateful inspection
  - La decisione è presa sulla base dell'informazione del pacchetto e del traffico precedente, di cui è mantenuta memoria
- Content filtering
  - Viene esaminato il contenuto della comunicazione (non solo gli header) interpretando il traffico sulla base dei protocolli di livello applicazione

Packet filtering

- TCP (Transmission Control Protocol)
  - Connection-oriented, bidirezionale, stream
  - Reliable, controllo di integrità e sequenzialità
  - Usato dai servizi HTTP, FTP, SMTP, NNTP ed altri
  - Necessita lo stabilirsi di una connessione
  - Ogni servizio è identificato da una porta (port)
- Three-way handshake
- Filtraggio sulla base di porta (sorgente/destinazione), flag SYN e ACK
- Esempio: inoltrare solo connessioni da dovunque ad un server HTTP `www` (80/TCP)
  - `ALLOW FWD source=any dest=www proto=tcp dport=80`
  - `DENY FWD source=any dest=any proto=tcp flags=SYN`

Packet filtering

- UDP (User Datagram Protocol)
  - Non connection-oriented
  - Nessun controllo di integrità
  - Basso overhead
  - Usato da DNS, NFS, NetBIOS
  - Servizi identificati da porte
- Nel pacchetto non esistono informazioni sullo stato della connessione (non esiste connessione)
- Possibilità di filtraggio stateful, test di coerenza con traffico UDP precedente
- Esempio: permettere solo “connessioni” al server DNS `dnsserv` (53/UDP)
  - `ALLOW FWD source=any dest=dnsserv proto=UDP dport=53`
  - `ALLOW FWD source=any dest=any proto=UDP state=RELATED`
  - `DENY FWD source=any dest=any proto=UDP`

Packet filtering

- ICMP (Internet Control Message Protocol)
  - Echo request (type 8)
  - Echo reply (type 0)
  - Time exceeded (type 11)
  - Destination unreachable (type 3)
  - Redirect (type 5)
  - ...
- Filtraggio sul valore del campo `type`, anche stateful
- Esempio: accettare solo Echo request, Echo reply, Time exceeded, Destination unreachable
  - `ALLOW FWD src=any dest=any proto=ICMP type=8`
  - `ALLOW FWD src=any dest=any proto=ICMP type=11`
  - `ALLOW FWD src=any dest=any proto=ICMP type=3`
  - `ALLOW FWD src=any dest=any proto=ICMP state=RELATED`
  - `DENY FWD src=any dest=any proto=ICMP`

Packet filtering - attacchi

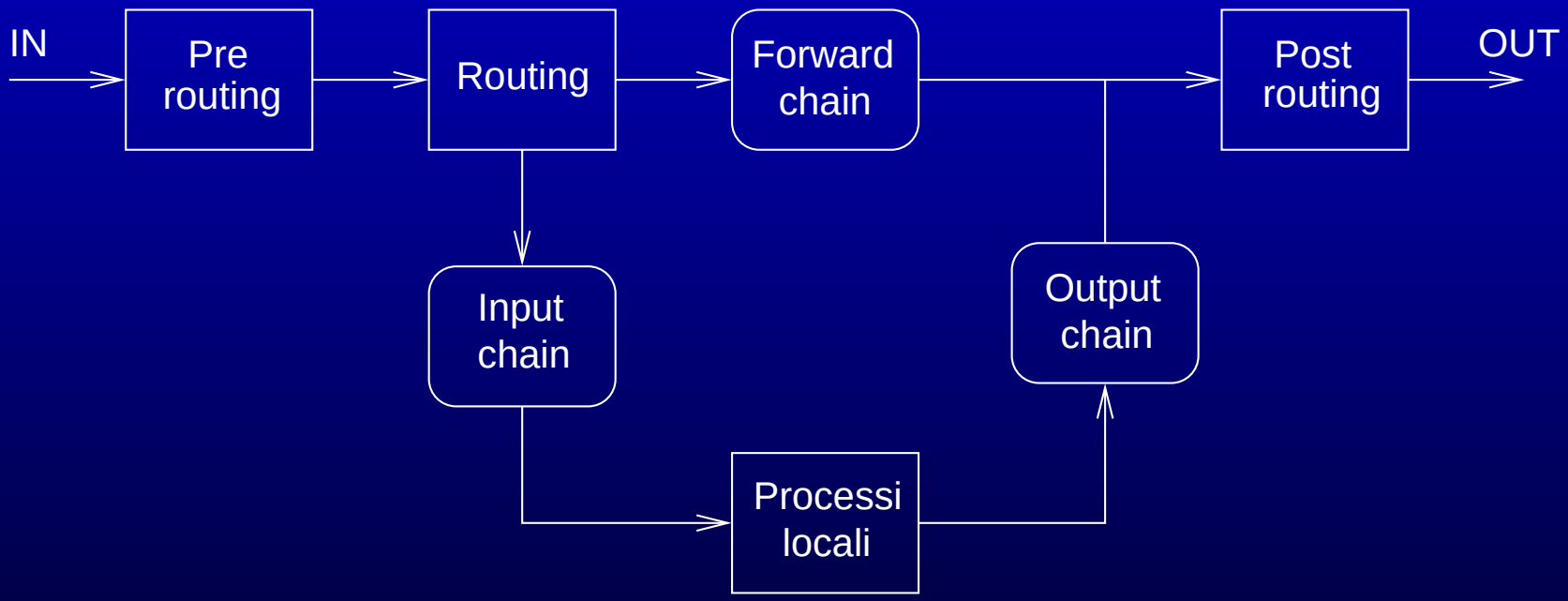
- Filtraggio su base indirizzo di origine
  - IP spoofing
    - UDP: immediato, es. NetBIOS
    - TCP: complesso (TCP sequence number prediction)
  - Man-in-the-middle
    - Necessità di intercettazione del traffico di risposta
    - Facilitato se l'attaccante appartiene alla rete del client oppure del server
  - Mitigabili con configurazione corretta dei router alle estremità
- Filtraggio su base protocollo/porta di origine
  - Esempio: bloccare tutto il traffico UDP, tranne il DNS

```
ALLOW FWD src=dnsserv sport=53 dest=any proto=UDP
ALLOW FWD dest=dnsserv dport=53 dest=any proto=UDP
 DENY FWD proto=UDP
```

  - Se `dnsserv` è compromesso può generare richieste UDP a qualunque tipo di servizio mascherandole da risposte DNS!

Un'implementazione reale: netfilter/iptables

- Parte del nucleo del sistema operativo Linux
- Paradigma di base



Un'implementazione reale: netfilter/iptables

- Ogni catena è una lista di regole, processata in ordine per ogni pacchetto
- Ogni regola è della forma

```
CONDIZIONE => AZIONE
```

  dove ad esempio

```
AZIONE = (ACCEPT|REJECT|DROP|LOG)
```

- Se un pacchetto non soddisfa una regola, si procede in cascata
- Se nessuna regola è soddisfatta, si applica una policy predefinita per la catena (`ACCEPT|REJECT|DROP`)

Un'implementazione reale: netfilter/iptables

- L'interfaccia al sistema netfilter è il comando `iptables`
- Esempi.
  - Aggiunta di una regola alla catena `FORWARD`
    ```
    iptables -A FORWARD -s 0/0 -d wwwsrv -p tcp --dport
    80 -j ACCEPT
    ```
  - Impostazione della policy della catena `INPUT`
    ```
    iptables -P INPUT DROP
    ```
- È possibile definire catene addizionali per semplificare la gestione
  - Esempio.
    ```
    iptables -N host-fidati
    iptables -P host-fidati DROP
    iptables -A host-fidati -s hostfidato -j ACCEPT
    iptables -A FORWARD -s 0/0 -d dnssrv -p udp --dport
    53 -j host-fidati
    ```

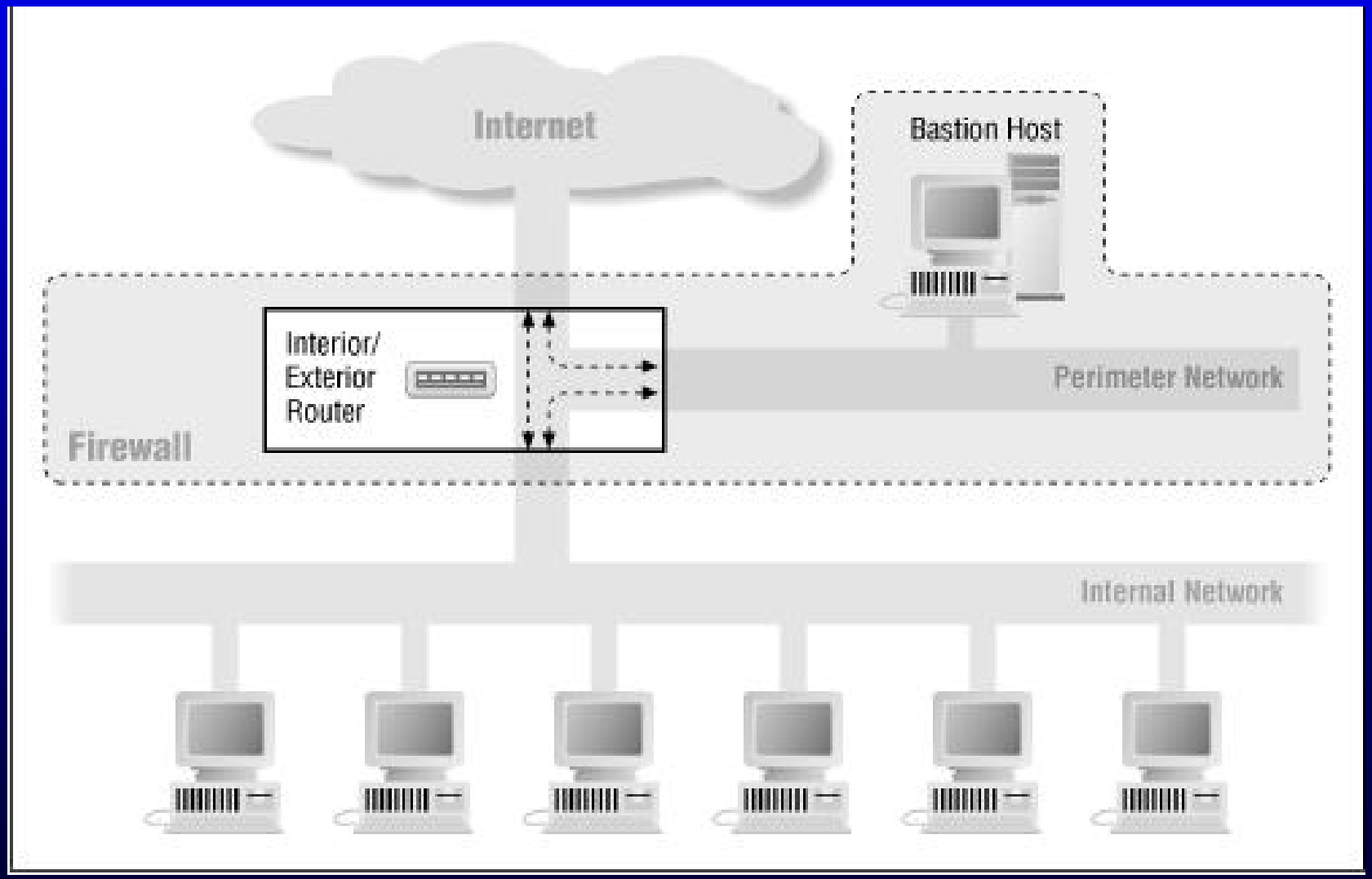
Un'implementazione reale: netfilter/iptables

- Stateful inspection (modulo state/conntrack)
  - Un pacchetto (TCP, UDP, ICMP) può essere riconosciuto in uno degli stati
    - `NEW`: inizia una nuova connessione
    - `ESTABLISHED`: appartiene ad una connessione esistente
    - `RELATED`: relativo, ma non parte di una connessione esistente (es. ICMP di errore)
    - `INVALID`: non identificato o errore non relativo ad alcuna connessione conosciuta

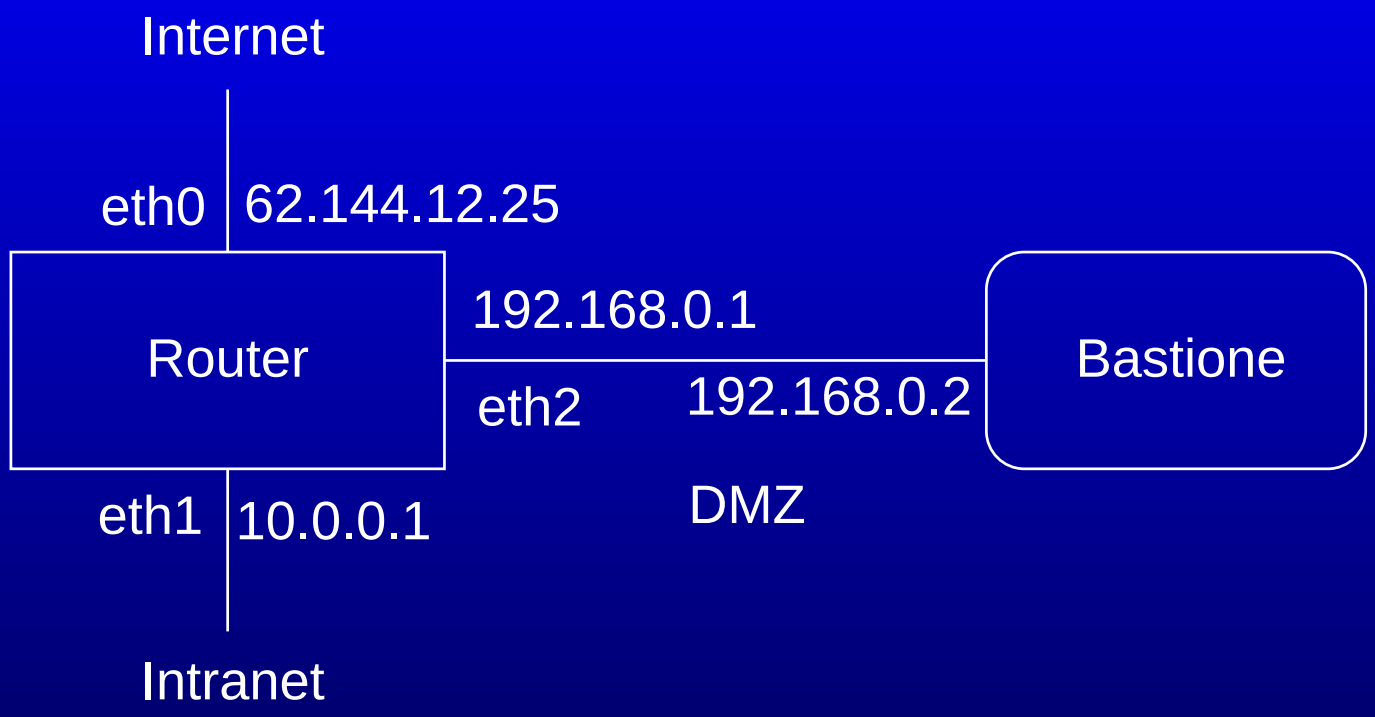
- Esempio: inoltrare solo connessioni da dovunque ad un server HTTP `www` (80/TCP)

```
iptables -A FORWARD -p tcp -d www --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d www -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -p tcp -j DROP
```

Esempio


Internet
Bastion Host
Interior/
Exterior
Router
Perimeter Network
Firewall
Internal Network

Esempio



- Specifiche:
  - ⋆ Accesso al solo servizio HTTP sul bastione da internet e dalla intranet
  - ⋆ Connessioni uscenti libere dalla intranet a internet
  - ⋆ Il bastione non può creare connessioni alla intranet
- N.B. Necessità di source e destination NAT

Esempio

- Impostazione policy di FORWARD

```
iptables -P FORWARD DROP
```

- Anti-spoofing

```
iptables -A FORWARD -s 10.0.0.0/8 -i eth0 -j DROP
iptables -A FORWARD -s 10.0.0.0/8 -i eth2 -j DROP
iptables -A FORWARD -s 192.168.0.0/16 -i eth0 -j DROP
iptables -A FORWARD -s 192.168.0.0/16 -i eth1 -j DROP
```

- Il traffico dalla intranet verso internet deve essere inoltrato (e mascherato)

```
iptables -A FORWARD -s 10.0.0.0/8 -d !  192.168.0.0/16
-j ACCEPT

iptables -A FORWARD -d 10.0.0.0/8 -m state --state
ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j
SNAT --to 62.144.12.25
```

Esempio

- DMZ

```
iptables -t nat -A PREROUTING -i eth0 -d 62.144.12.25
-p tcp --dport 80 -j DNAT --to 192.168.0.2:80

iptables -A FORWARD -d 192.168.0.2 -p tcp --dport 80 -j
ACCEPT

iptables -A FORWARD -s 192.168.0.2 -m state --state
ESTABLISHED,RELATED -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.0.2 -o eth0
-j SNAT --to 62.144.12.25
```

Bibliografia

- D. Brent Chapman, E. D. Zwicky, *Building internet firewalls*, O'Reilly, 1999
- Anonymous, *Maximum security*, SAMS, 1999
- W. R. Stevens, *TCP/IP Illustrated*, Addison Wesley, 1994
- R. Russell - *Packet filtering HOWTO* - `http://www.netfilter.org`
- Vari, *Firewalls FAQ*, `http://www.faqs.org/faqs/firewalls-faq`
- Vari, *Internet Firewalls - Resources*, `http://www.cerias.purdue.edu/coast/firewalls/fw-body.html`
- S. Piccardi, *GaPiL, Guida alla Programmazione in Linux*, `http://gapil.firenze.linux.it`