



Network Security: Firewalls

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Corso di Sicurezza nelle reti di telecomunicazioni, a.a. 2008/2009

<http://www.tlc.unipr.it/veltri>

Che Cosa è un Firewall?

- Tradotto dalla lingua inglese il termine “firewall” significa muro di fuoco
- Un firewall rappresenta una configurazione HW e SW che viene interposta tra almeno una coppia di sottoreti IP
- Un firewall offre protezione analizzando e filtrando all'occorrenza tutto il traffico che transita tra le reti tra cui è interposto
- L'analisi ed il filtering del traffico avvengono a vari livelli, a seconda della tipologia e delle funzionalità implementate nel firewall

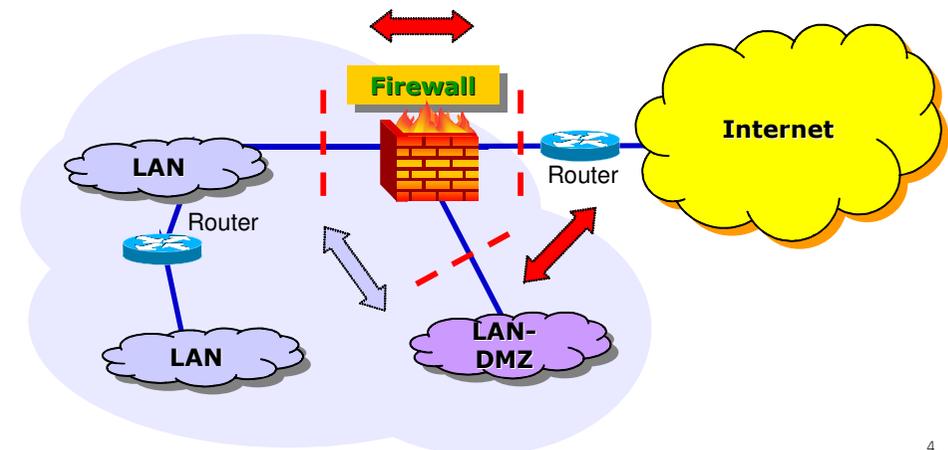
2

Dove si inserisce un Firewall

- Alla frontiera tra una rete interna da proteggere (anche un solo nodo) e la rete esterna (e.g. Internet):
 - per monitorare, limitare, autenticare l'accesso alla rete da proteggere nei confronti di accessi provenienti “dall'esterno”
 - per monitorare, limitare, autenticare gli accessi ad Internet o ad una sottorete/sistema esterna/o da parte dell'utenza interna
 - per realizzare reti virtuali private sicure su un backbone pubblico ritenuto intrinsecamente insicuro
- All'interno di una intranet:
 - per monitorare, limitare, autenticare l'accesso ad alcune risorse informatiche sensibili (Centro Servizi, CED, etc.)
- In generale, relativamente alla tipologia ed alla configurazione di un firewall, non esistono delle regole standard
 - la selezione ed implementazione di un firewall dipende dai requisiti che si intendono soddisfare

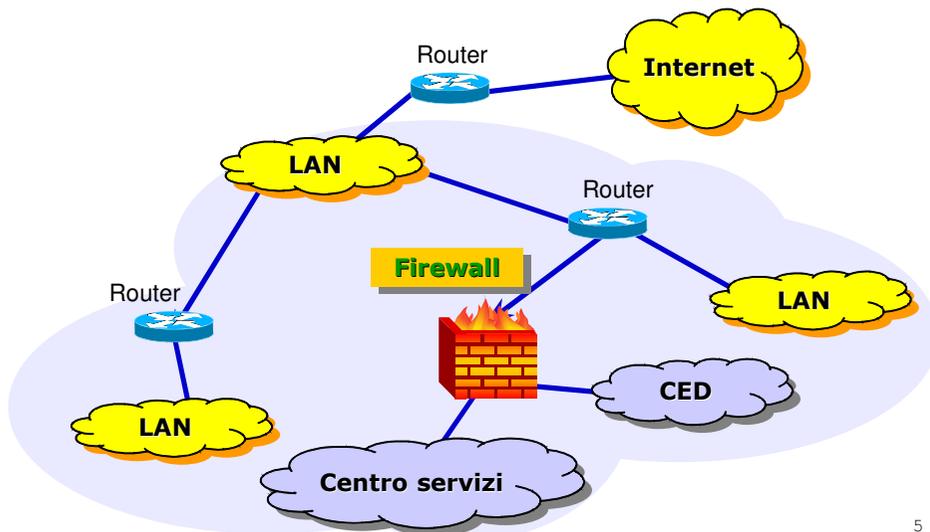
3

Esempio di protezione dalla rete pubblica



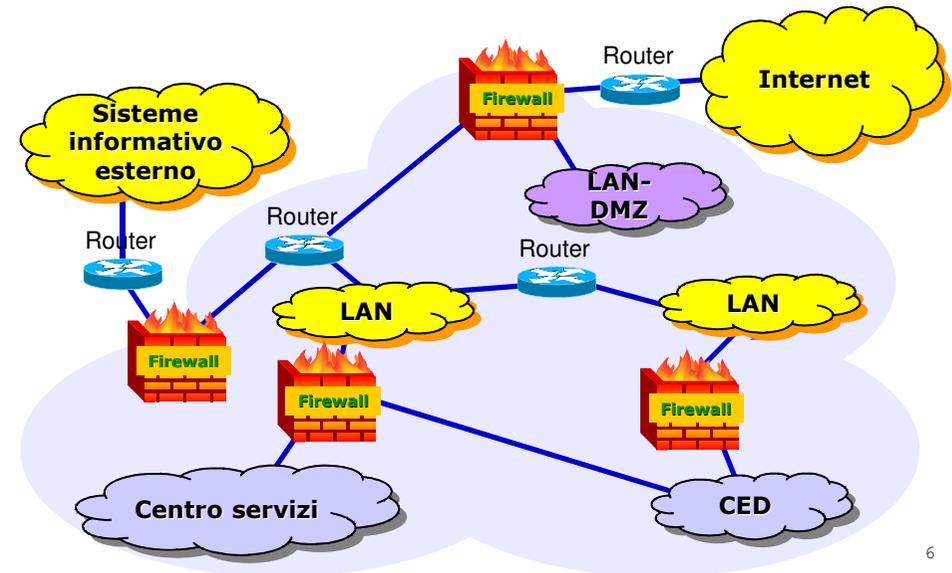
4

Esempio di protezione da accessi interni



5

Esempio di protezione multipla



6

Quando un Firewall non garantisce protezione

- Se esistono ulteriori percorsi di rete che consentono di by-passare il firewall:
 - Modem collegati a PC o server della intranet che consentono accessi dial-up dall'esterno
 - AP WiFi attivati e aperti, collegati all'interno della rete
 - Più in generale, le reti tra cui è interposto il firewall hanno ulteriori punti di congiunzione non protetti
- In caso di inconsistenza od errori nella configurazione:
 - Il firewall non implementa correttamente la politica di sicurezza stabilita
 - Il sistema su cui è installato il firewall è vulnerabile ad attacchi informatici a causa di bug del OS o, in genere, alla non perfetta configurazione dello stesso o perché ospita ulteriori applicativi che possono veicolare attacchi
- In presenza di tipologie di attacco per cui il firewall è influente:
 - attacchi informatici sferrati da host che sono attestati nella medesima sottorete a cui afferiscono le stazioni oggetto dell'attacco (ovvero non si transita per il firewall)
 - attacco sferrato mediante impiego di CD, dischi/memorie removibili, etc.

7

Politica di sicurezza implementata in un Firewall

- Una politica di sicurezza che regola il traffico attraverso un firewall viene definita a due livelli:
 - **Network Service Access Policy (Politica di Accesso ai Servizi di Rete - livello astrazione alto):**
 - Stabilisce:
 - quali servizi permettere e quali proibire
 - come i servizi saranno utilizzati
 - eventualmente, quali saranno le eccezioni permesse dalla politica
 - **Firewall Design Policy (Politica di progettazione del Firewall - livello astrazione basso):**
 - descrive come il firewall implementerà in pratica le restrizioni ed i filtri dei servizi definiti nella Politica di Accesso ai Servizi di Rete

8

Network Service Access Policy

- Politiche di accesso ai servizi di rete
- Equilibrio tra protezione dai rischi e possibilità di accedere alle risorse sulla rete
- Flessibilità perché:
 - Internet è in evoluzione continua
 - nuovi protocolli e servizi emergono su Internet
 - cambiamenti nelle necessità dell'azienda

9

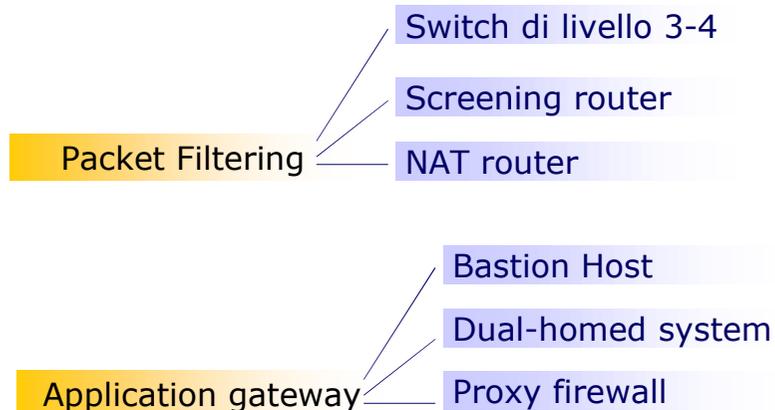
Firewall Design Policy

- Politica di progetto del Firewall
- Si specifica **come** implementare la politica di accesso ai servizi di rete
- I firewall generalmente implementano una delle due fondamentali politiche:
 - **Permettere ogni servizio, tranne quelli espressamente negati**
 - **Negare ogni servizio, tranne quelli espressamente permessi**
- E' più sicuro partire dalla politica di negazione di tutti i servizi tranne quelli esplicitamente permessi..



10

Tipologie di Firewall



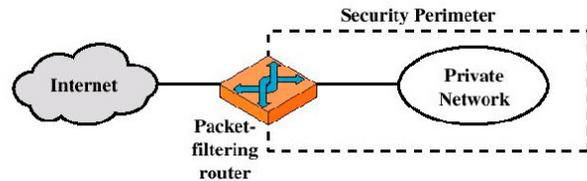
11

Tipologie di Firewall

- **Switch di livello 3-4**: dispositivo di rete che implementa funzionalità di livello fisico (rigenerazione del segnale tipico del media utilizzato), di livello data link (rigenera le trame di livello 2), di livello 3 (instradamento o filtraggio di datagrammi IP), di livello 4 (filtraggio di traffico in base al tipo di servizio Internet a cui si riferisce)
- **Screening router**: (packet-filtering router) un router configurato per svolgere funzionalità tipiche di un packet filtering
- **Bastion Host**: un host/server punto forte e critico per la sicurezza del sistema (in esso è concentrata la maggior parte della politica di sicurezza del sistema)
- **Dual Homed System**: un sistema (host, workstation, server) con due o più interfacce di rete
- **Proxy Firewall**: un sistema di tipo server proxy/relay con funzionalità di filtraggio tipiche di un firewall

12

Packet-filtering Router



- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

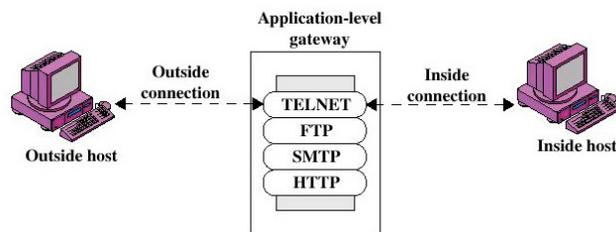
13

Packet-filtering Router

- Advantages:
 - **Simplicity**
 - **Transparency to users**
 - **High speed**
- Disadvantages:
 - **Difficulty of setting up packet filter rules**
 - **Lack of Authentication**
- Examples of attacks that can be prevented:
 - **IP address spoofing**
 - **Source routing attacks**
 - **Tiny fragment attacks**

14

Application-level Gateway



- Also called proxy server
- Acts as a relay of application-level traffic
- E.g. HTTP and FTP proxy, SMTP server, etc.

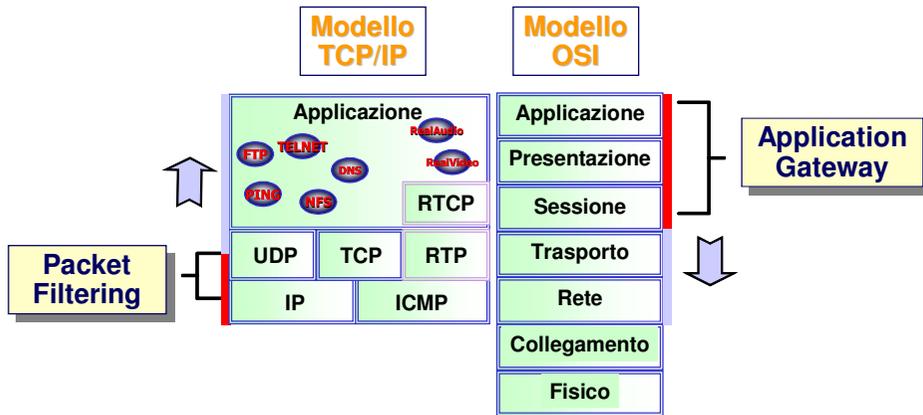
15

Application-level Gateway

- Advantages:
 - **Higher security than packet filters**
 - **Only need to scrutinize a few allowable applications**
 - **Easy to log and audit all incoming traffic**
- Disadvantages:
 - **Additional processing overhead on each connection (gateway as splice point)**

16

Packet Filtering vs. Application Gateway



17

Packet Filtering

- I pacchetti possono essere filtrati in base a:
 - Direzione del traffico (in/out/entrambe)
 - Riferimento temporale
 - Indirizzo MAC/DL destinazione
 - Indirizzo MAC/DL sorgente
 - Interfaccia
 - Indirizzo IP destinazione
 - Indirizzo IP sorgente
 - Campi TTL e TOS
 - Frammentazione IP
 - Opzioni IP
 - Tipo di protocollo (ICMP/TCP/UDP)
 - Tipo di messaggio ICMP
 - Range di porte TCP/UDP di destinazione
 - Range di porte TCP/UDP sorgente
 - Opzioni e flag TCP/UDP
 - Tipologia e contenuto dei protocolli applicativi
 - altro..
- Altre informazioni
Informazioni relative al protocollo di collegamento (data link)
Informazioni relative al protocollo IP
Informazioni ICMP
Informazioni TCP/UDP
Informazioni strato applicativo

18

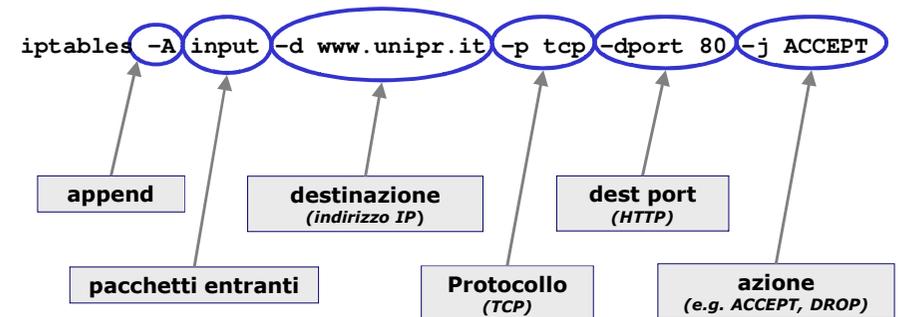
Regole di filtering: Esempio

- Le regole di filtraggio sono ordinate in apposite liste o tabelle (Lists of rules), dette anche *Access control lists*, o *Chains*
- Esempio:
 - abilitazione della posta elettronica (SMTP) e del web (HTTP)

IP source	IP dest	Proto	Sorce port	Dest port	Action
*	160.78.1.1	tcp	> 1023	25	permit
*	160.78.1.1	tcp	> 1023	80	permit
160.78.1.0/24	*	*	*	*	permit
*	*	*	*	*	deny

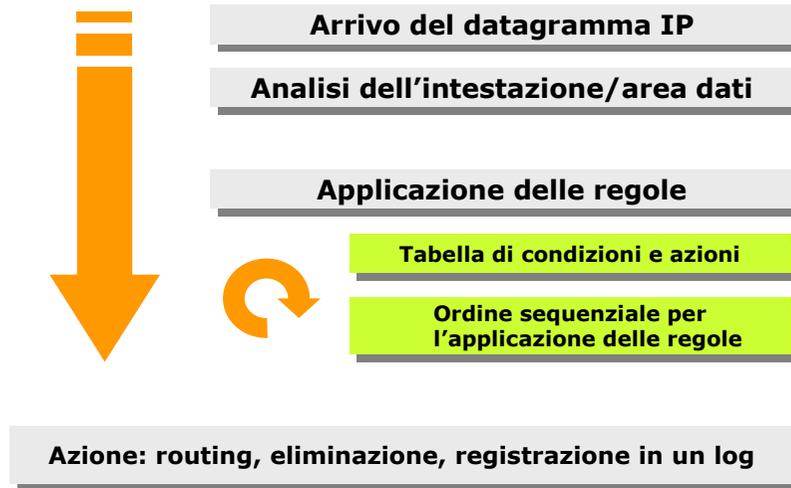
19

Esempio di inserimento di regole di filtering



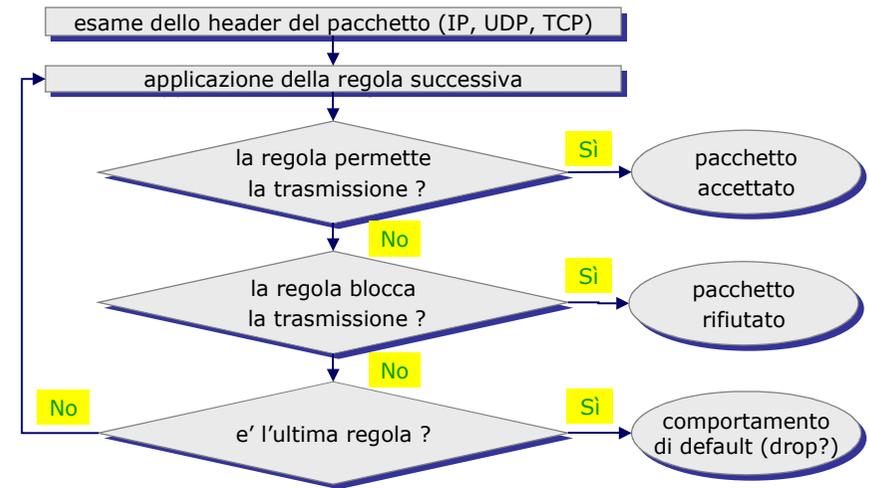
20

Packet Filtering - Funzionamento



21

Logica delle regole di filtraggio



22

Modalità di filtraggio stateful/stateless

- **Stateful**: con controllo di stato
- **Stateless**: senza controllo di stato

23

Access Control List CISCO

- Le Access Control List (ACL) costituiscono le regole per il filtro
- Possono definire controlli a livello di rete e trasporto
- Una ACL permette di abilitare/negare il flusso dei pacchetti, in funzione degli host/servizi interessati
- Per abilitare, ad esempio, il servizio di invio di email, una ACL potrebbe avere il seguente formato:

Type	Src_IP	Dst_IP	Src_Port	Dst_Port	Action
tcp	*	192.106.248.*	*	25	permit
*	*	192.106.248.*	*	*	deny

- Nota: di solito tutto quello che non è esplicitamente previsto è negato
- Due tipi di ACL
 - **Standard Access List (SAL)**
 - **Extended Access List (EAL)**

24

Extended Access List

```
access-list access-list-number {deny | permit} protocol source  
source-wildcard destination destination-wildcard [tos tos] [log |  
log-input]
```

```
no access-list access-list-number
```

100 ≤ list ≤ 199

For TCP/UDP:

```
access-list access-list-number {deny | permit} tcp/udp source  
source-wildcard [operator port [port]] destination destination-  
wildcard [operator port [port]] [established] [tos tos] [log | log-  
input]
```

25

Esempio di ACL

```
! NO IP SPOOFING  
access-list 100 deny ip 127.0.0.1 0.0.0.0 0.0.0.0 255.255.255.255  
access-list 100 deny ip 0.0.0.0 255.255.255.255 127.0.0.1 0.0.0.0  
access-list 100 deny ip 192.106.248.0 0.0.0.255 192.106.248.0 0.0.0.255  
!  
! TFTPD  
access-list 100 permit udp 192.106.248.24 0.0.0.0 192.106.248.1 0.0.0.0 eq 69  
!  
! NO r* commands  
access-list 100 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 512  
access-list 100 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 514  
!  
! CONNESSIONI TCP ATTIVE  
access-list 100 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established  
!  
! TELNET  
access-list 100 permit tcp 151.99.253.2 0.0.0.0 192.106.248.18 0.0.0.0 eq 23  
!  
! FTP  
access-list 100 permit tcp 146.48.2.1 0.0.0.0 192.106.248.1 0.0.0.0 eq 21  
...  
!  
! PERMETTE TUTTO IL RIMANENTE  
access-list 100 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

26

Modifica di Access List

- Creazione e Editing di Access List offline
- Aggiornamento di Access List mediante TFTP Server
 - Creazione delle access list mediante text editor (con commenti!)
 - salvaggio delle access list in ASCII su un TFTP server accessibile dal router,
 - sul router digitare `copy tftp running-config file_id` (comando per copiare l'access list sul router,
 - sul router digitare `copy running-config startup-config` (comando per salvare l'access list sulla memoria del router
- Oppure, tramite comandi di config

27

Alcune complicazioni legate al packet filtering

- IP Spoofing
 - Per questo si controlla anche l'interfaccia del router a cui arrivano i pacchetti
- Frammentazione dei pacchetti
 - Per il protocollo IP un qualunque router può frammentare un pacchetto, che poi viene riassembleto a destinazione. Dopo la frammentazione solo il primo dei sotto-pacchetti contiene l'header con le informazioni necessarie per il packet filtering
- Pericoli dell'IP source routing
 - Pacchetto che comprende le informazioni sul routing da seguire per arrivare a destinazione, anziché lasciare il cammino del routing a discrezione dei router da cui passa
- Gestione protocollo FTP
 - Il numero di porta della sessione dati del client viene generato dinamicamente, rendendo difficile definire le porte da bloccare.

28

AntiSpoofing – Filtro ingresso

- Gran parte degli attacchi in rete si basano sulla falsificazione fraudolenta degli indirizzi d'origine
- Il modo più semplice di proteggersi è quello di scartare, a livello di border router, tutto il traffico in ingresso con indirizzi sorgente manifestamente inammissibili rispetto alla provenienza

- **Esempio (Cisco)**

! Blocca il traffico dall'esterno con indirizzi sorgente interni

```
access-list 111 deny ip 160.78.0.0 0.0.255.255 any log
access-list 111 permit ip any any
```

```
interface Serial0
 ip access-group 111 in
```

- **Oppure (Linux)**

```
iptables -A FORWARD -i eth1 -s 160.78.0.0/16 -j DROP
iptables -A FORWARD -j ACCEPT
```

29

AntiSpoofing – Filtro ingresso

- E' opportuno bloccare anche tutto il traffico proveniente dall'esterno con indirizzi sorgente riservati (RFC 1918) o comunque non correttamente instradabili aggiungendo all'ACL in ingresso
- **Esempio**

```
access-list 101 deny ip host 0.0.0.0 any log
! Incoming with loopback source address
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
! Incoming with RFC 1918 reserved address
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
```

```
interface Serial0
 ip access-group 101 in
```

30

AntiSpoofing – Filtro uscita

- Per prevenire inoltre spoofing, volontari o involontari, dall'interno della propria rete verso l'esterno, analoghe misure di filtraggio vanno applicate sul border router in uscita
- **Esempio**

! Blocca il traffico uscente con indirizzi sorgente estranei

```
access-list 112 permit ip 192.1.2.0 0.0.0.255 any
access-list 112 deny ip any any log
```

```
interface Serial0
 ip access-group 112 out
```

31

Bastion Host, Application Gateway

Bastion Host

- Un sistema di computer che deve essere altamente sicuro poiché raggiungibile da attacchi
 - tipicamente è esposto alla rete Internet ed è il punto principale di contatto per gli utenti della rete interna
 - il nome deriva dalle fortificazioni delle mura esterne dei castelli medievali

33

Bastion Host: servizi e vie di accesso

- IP forwarding disabilitato
- Eliminare tool non necessari (compilatori, strumenti di amministrazione)
- Solo servizi essenziali
 - è più facile garantirne la sicurezza
 - meno servizi ⇒ più semplice ⇒ meno bug!
- Controllo degli script di avvio
- Controllo di software con difetti/buchi noti
- Procedure di backup
- Deve essere consentito l'accesso al bastion host solo tramite servizi sicuri (ssh), oppure da console locale (es. seriale)
- Ristrettezza sul controllo di accesso
 - non ci devono essere altri utenti fisici oltre all'amministratore

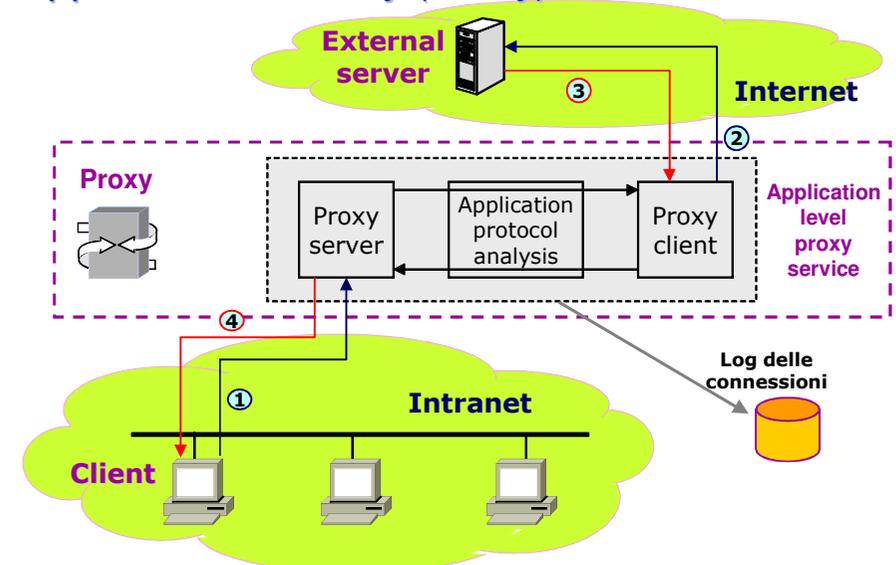
34

Application Gateway

- E' una macchina preposta a svolgere dei servizi per conto di altri applicativi, con controllo di accesso
- Si avvale di una logica del tipo store & forward, capace anche di processare il traffico dati a livello applicativo
- Impedisce il transito di molti protocolli "insicuri" risultando intrinsecamente più affidabile di un Packet Filtering
- Gli utenti che possono accedere ai servizi di proxy, non possono accedere all'application gateway (tramite login)
- Opzionalmente alcuni proxy prevedono la verifica dell'integrità dei dati ed il controllo antivirus dinamico
- Deve essere possibile tenere traccia, al suo interno, del traffico analizzato e filtrato (logs)
- Svantaggio: la specificità rispetto alle applicazioni
 - occorre installare un server proxy per ogni applicazione che si intende utilizzare, non esistono sistemi generici

35

Application Gateway (Proxy): Funzionamento



36

Application gateway vs. packet filtering

Pro

- ✓ **Pieno controllo a livello di applicazione**
- ✓ **Strong User authentication**
- ✓ **Full logging**
- ✓ **Nasconde, di default, gli indirizzi della rete interna**
- ✓ **Content filtering**
- ✓ **Caching**
- ✓ **Livello di sicurezza più elevato rispetto ad un packet filter**

Contro

- ✓ **Non supporta ogni possibile servizio (UDP, RPC, altri), ma soltanto quelli per cui esiste il relativo Security Proxy (FTP, Telnet, HTTP, SMTP, ...)**
- ✓ **Non adeguato a nuovi servizi**
- ✓ **Non utilizzabile in qualsiasi contesto**
- ✓ **Minori performance**
- ✓ **La sua introduzione richiede riconfigurazioni nelle postazioni di lavoro (configurazione dei client)**

37

Funzionalità aggiuntive di un FW: NAT

- RFC 2663 - "NAT Terminology and Considerations"
 - **Network Address Translation is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to end hosts**
 - **There are many variations of address translation that lend themselves to different applications**

38

Quando si usa il NAT

- Si deve instradare su Internet il traffico proveniente da una rete interna (intranet) in cui si è fatto uso di indirizzamento privato
- Si vuole nascondere l'indirizzamento della propria rete per scopi di sicurezza
- Si vuole semplificare lo spostamento di una rete intera
 - **nessuna riconfigurazione interna**
- Semplificazione delle tabelle di routing (avoidance of routing table explosion)
- Sicurezza

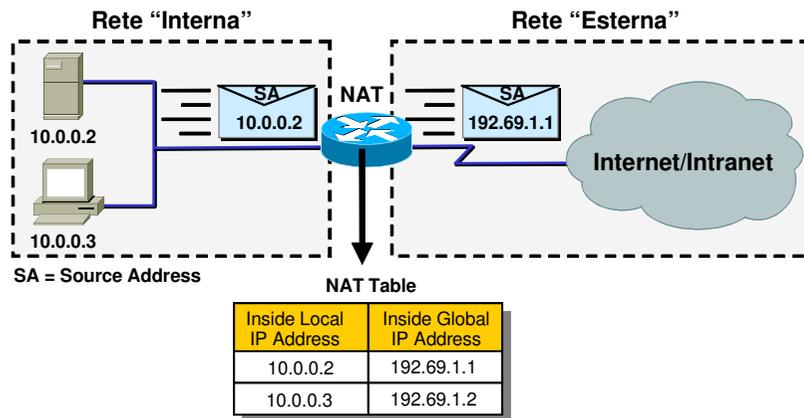
39

Tipologie di NAT

- **Traslazione del tipo $n \leftrightarrow n$ (NAT)**: ciascun indirizzo IP, appartenente al range a cui si intende applicare il NAT, viene traslato in un indirizzo IP distinto, appartenente ad un pool di indirizzi predeterminato
 - **NAT statico**: la corrispondenza indirizzo IP \leftrightarrow indirizzo IP traslato è permanente, ovvero ogni indirizzo IP viene traslato sempre con il medesimo indirizzo IP prelevato dal pool
 - **NAT dinamico**: la corrispondenza indirizzo IP \leftrightarrow indirizzo IP traslato è variabile, ovvero ogni indirizzo IP viene traslato con un indirizzo IP libero, ovvero non già precedentemente assegnato dal NAT, prelevato dal pool degli indirizzi IP configurati per il NAT
- **Traslazione del tipo $n \leftrightarrow 1$ (NAPT)**: ciascun indirizzo appartenente al range a cui si intende applicare il NAT viene traslato in un medesimo indirizzo IP fisso (normalmente lo stesso indirizzo del nodo NAT)

40

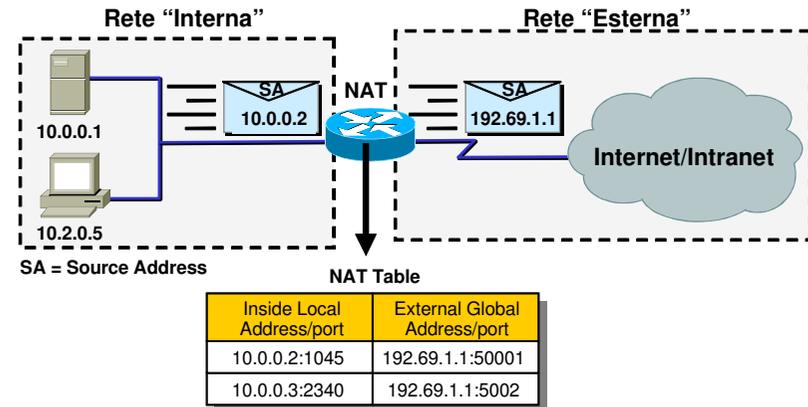
Simple NAT



- viene tradotto il SA dei pacchetti uscenti (da sinistra a destra) da indirizzo privato a indirizzo pubblico
- viene tradotto il DA nei pacchetti entranti da indirizzo pubblico a privato (mappaggio inverso)

41

Network Address Port Translation (NAPT)



- Tutti gli host interni utilizzano un singolo indirizzo IP pubblico esterno
- Vengono utilizzate le porte TCP/UDP per individuare il reale destinatario del pacchetto
- Nei pacchetti uscenti vengono modificate anche le S_port
- Nei pacchetti entranti vengono rimessi a posto sia il D_addr che il D_port

42

Network Address Port Translation (NAPT)

- Opera una traslazione di porte TCP/UDP oltre che di indirizzi IP
- Utilizzato per:
 - **Indirizzamento:**
 - risparmio di indirizzi (un unico IP pubblico per un'intera rete)
 - **Load balancing:**
 - si intende bilanciare il carico tra più server che erogano un servizio, sempre mediante l'impiego del meccanismo di redirect
 - **sicurezza:**
 - si intende nascondere la natura di un servizio, quando esportato su Internet
 - si intende nascondere il server che eroga il servizio, mediante ridirezione
- Svantaggi:
 - **Mancato funzionamento di alcuni applicativi di rete, e.g. FTP, H323(Netmeeting)..**
 - e.g. indirizzi IP e porte TCP/UDP privati inviati nel payload del messaggio TCP (non gestito dal NAPT)
 - se tale indirizzo viene usato dal host esterno, quest'ultimo non riuscirebbe ad estradare correttamente i pacchetti
 - **In questi casi, sono necessari dei Application Level Gateway (ALG) implementati nel nodo NAPT che modificando il contenuto dati di livello applicativo dei pacchetti**

43

Types of NAPT

- Full cone NAT
 - **also known as one-to-one NAT**
 - **all requests from the same internal IP address and port are mapped to the same external IP address and port**
 - **an external host can send a packet to the internal host, by sending a packet to the mapped external address**
- Restricted cone NAT
 - **all requests from the same internal IP address and port are mapped to the same external IP address and port**
 - **unlike a full cone NAT, an external host can send a packet to the internal host only if the internal host had previously sent a packet to it**

44

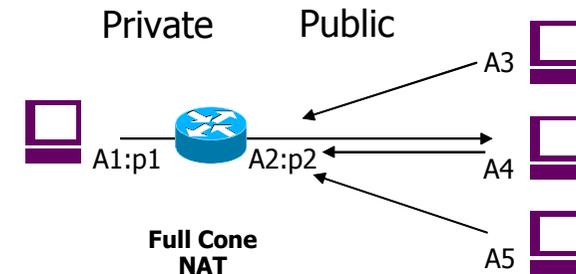
Types of NAT (cont.)

- Port restricted cone NAT
 - is like a restricted cone NAT, but the restriction includes port numbers
 - an external host can send a packet to a particular port on the internal host only if the internal host had previously sent a packet from that port to the external host
- Symmetric NAT
 - all requests from the same internal IP address and port to a specific destination IP address and port are mapped to that external source IP address and port
 - if the same internal host sends a packet with the same source address and port to a different destination, a different mapping is used. Only an external host that receives a packet can send a UDP packet back to the internal host

45

Tipi di NAT: Full Cone NAT

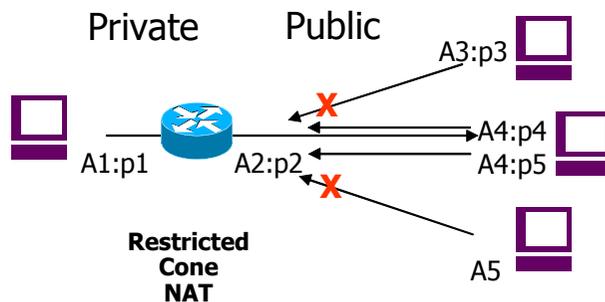
- Also known as one-to-one NAT
- All requests from the same internal IP address and port are mapped to the same external IP address and port
- An external host can send a packet to the internal host, by sending a packet to the mapped external address



46

Tipi di NAT: Restricted Cone NAT

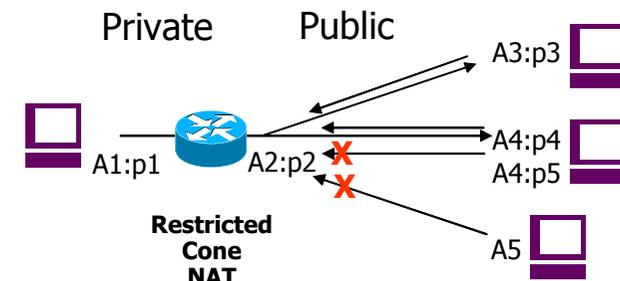
- Similar to full cone NAT
- Unlike a full cone NAT, an external host can send a packet to the internal host only if the internal host had previously sent a packet to it



47

Tipi di NAT: Port Restricted Cone NAT

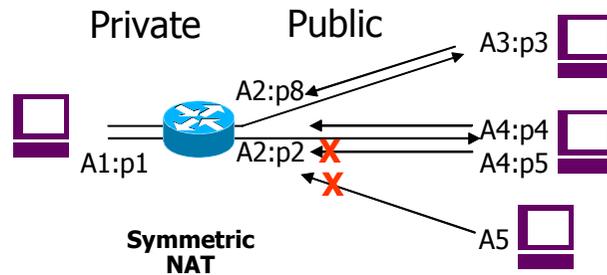
- Is like a restricted cone NAT, but the restriction includes port numbers
- An external host can send a packet to a particular port on the internal host only if the internal host had previously sent a packet from that port to the external host



48

Tipi di NAT: Symmetric NAT

- All requests from the same internal IP address and port to a specific destination IP address and port are mapped to that external source IP address and port
- If the same internal host sends a packet with the same source address and port to a different destination, a different mapping is used
- Only an external host that receives a packet can send a UDP packet back to the internal host



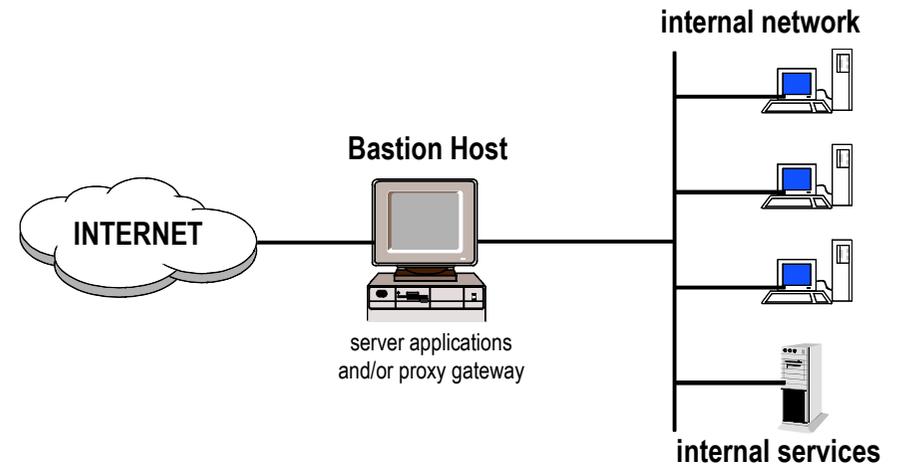
49

Configurazioni di firewall

Firewall configurations

- Single system
 - single gateway (bastion host), or
 - single packet filtering router
- More complex configurations

Dual-homed host firewall



51

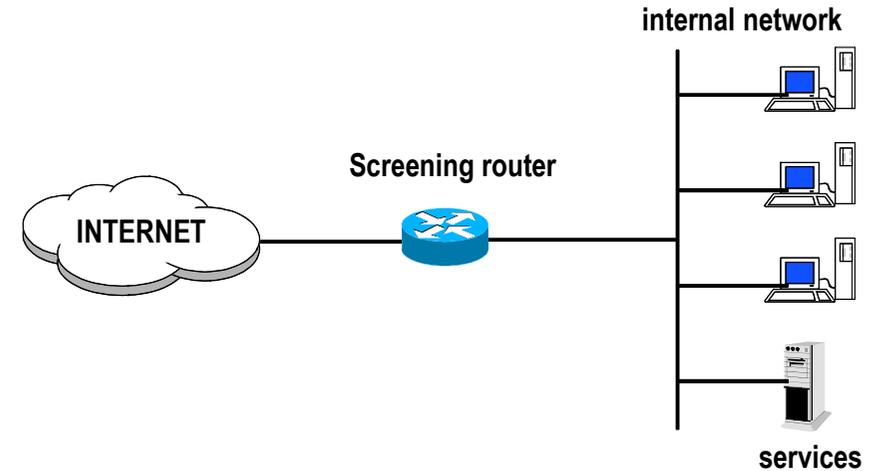
52

Dual-homed host firewall

- Bastion Host connesso ad entrambe le reti (esterna e interna)
- Eventuali applicazioni server accessibili da entrambe le reti
- Servizi esterni eventualmente accessibili tramite proxy gateway
- Pregi:
 - elevata sicurezza a livello di rete (isolamento tra reti IP differenti)
 - possibilità di utilizzo di indirizzamento interno privato
 - possibilità di implementare application level gateway (ALG) (i.e. proxy gateway)
 - semplicità di logging dei servizi
- Difetti:
 - possibilità di penetrazione tramite debolezze dell'host
 - accesso limitato ai soli servizi presenti sul bastion host e a quelli per cui è implementato un ALG

53

Screening router



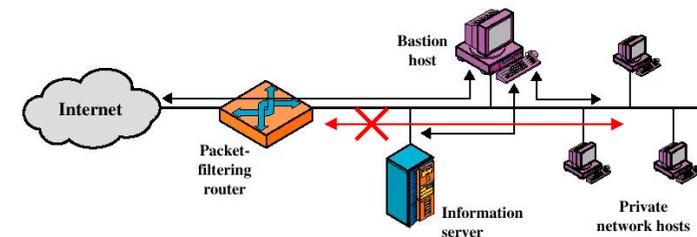
54

Screening router

- Router di confine con funzionalità di packet filtering
- Due possibilità per l'accesso ai servizi (interni/esterni)
 - Screened host firewall, single-homed bastion host
 - Screened host firewall, dual-homed bastion host

55

Screened host firewall (single-homed bastion host)



- Screened host firewall, single-homed bastion configuration
- Firewall may consist by two systems:
 - A packet-filtering router
 - A bastion host

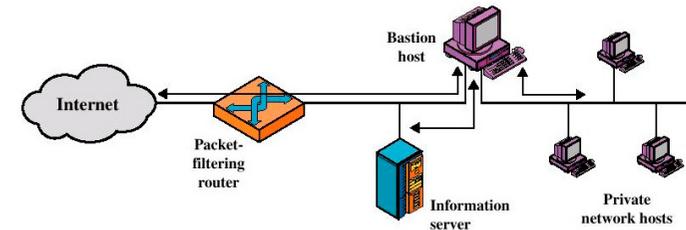
56

Screened host firewall (single-homed bastion host)

- Configuration for the packet-filtering router:
 - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions
- Greater security than single configurations because of two reasons:
 - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
 - An intruder must generally penetrate two separate systems
- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

57

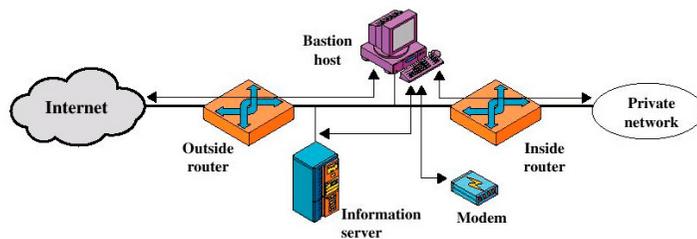
Screened host firewall (dual-homed bastion host)



- Screened host firewall, dual-homed bastion configuration
 - The packet-filtering router is not completely compromised
 - Traffic between the Internet and other hosts on the private network has to flow through the bastion host

58

Screened-subnet firewall

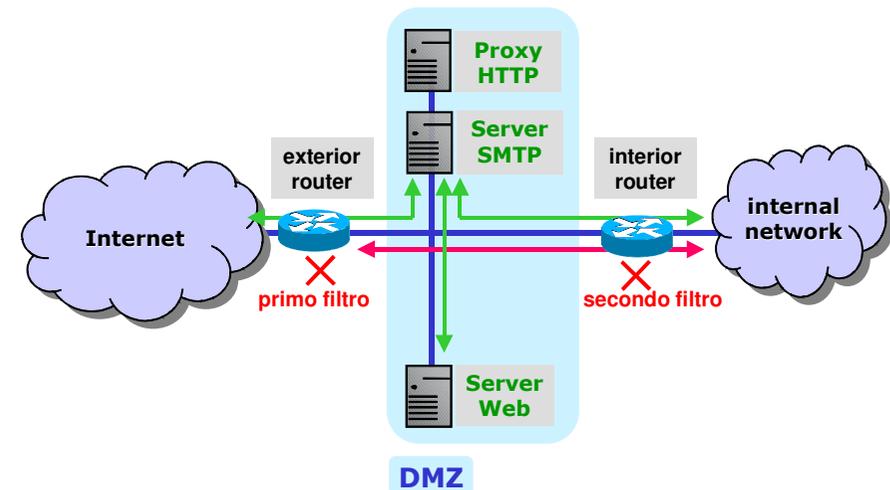


- Screened subnet firewall configuration
 - Most secure configuration
 - Two packet-filtering routers are used
 - Creation of an isolated sub-network (DMZ)

59

Screened-subnet firewall: DMZ

- Demilitarized Zone



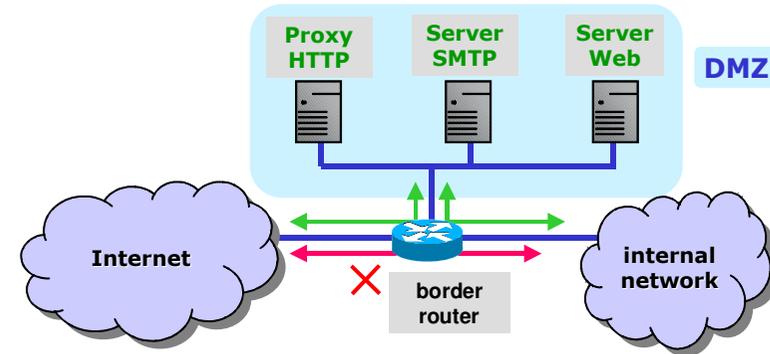
60

Screened-subnet firewall

- Advantages:
 - Three levels of defense to oppose to intruders
 - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)
 - The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

61

Merging of interior/exterior router



62

Architetture pericolose



- E' PERICOLOSO:
 - Unire bastion host e exterior router
 - Unire bastion host e interior router
 - Molteplicità di Interior routers



- NON E' PERICOLOSO:
 - Molteplicità di internal networks
 - Molteplicità di exterior routers
 - Molteplicità di DMZs

63