Network Security: Firewalls

Luca Veltri

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

Corso di Sicurezza nelle reti, Reti di telecomunicazioni C, a.a. 2009/2010

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

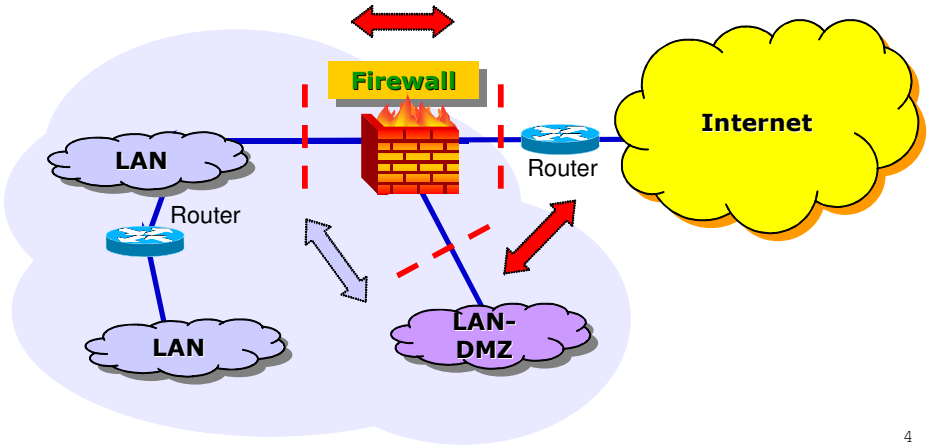
Che Cosa è un Firewall?

- 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

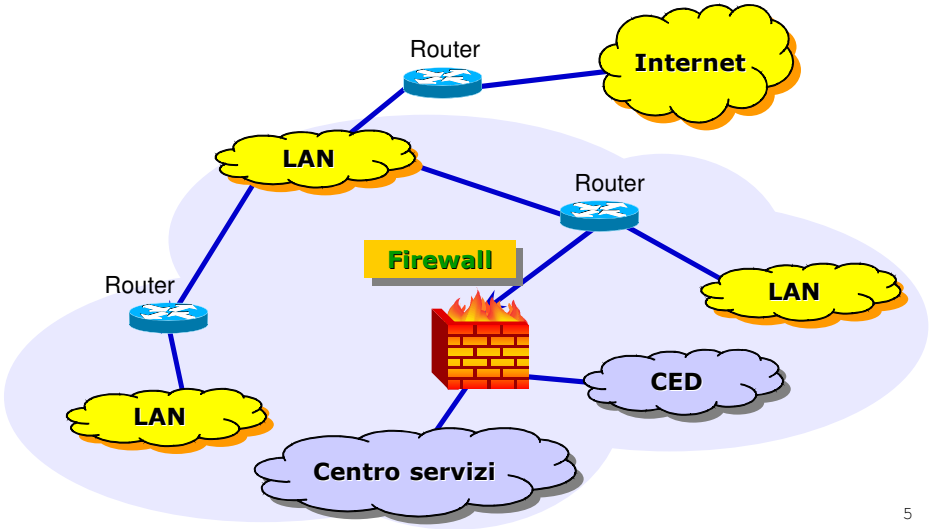
Dove si inserisce un Firewall

- 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**

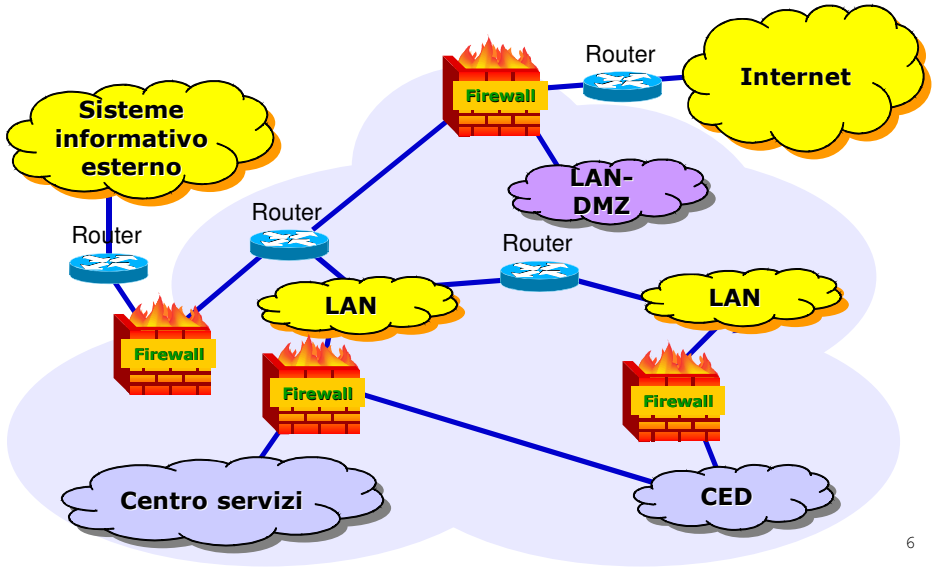
Esempio di protezione dalla rete pubblica



Esempio di protezione da accessi interni



Esempio di protezione multipla



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**
  - **Piu' in generale, le reti tra cui è interposto il firewall hanno ulteriori punti di congiunzione non protetti**
- In caso do 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 ininfluente:
  - **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.**

Politica di sicurezza implementata in un Firewall

- Una politica di sicurezza che regolamenta 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 filtraggi dei servizi definiti nella Politica di Accesso ai Servizi di Rete

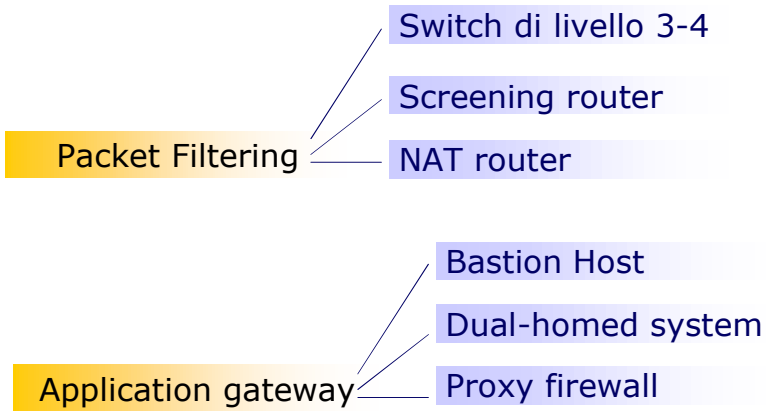
Network Service Access Policy

- 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**

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..

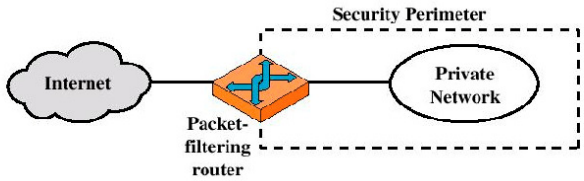
Tipologie di Firewall



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

Packet-filtering Router

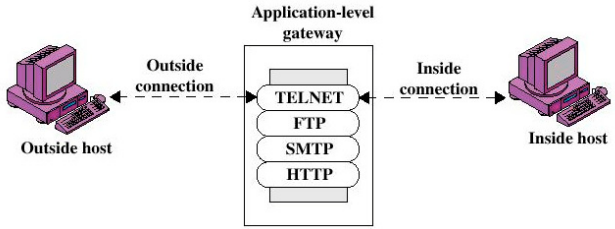


- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

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**

Application-level Gateway

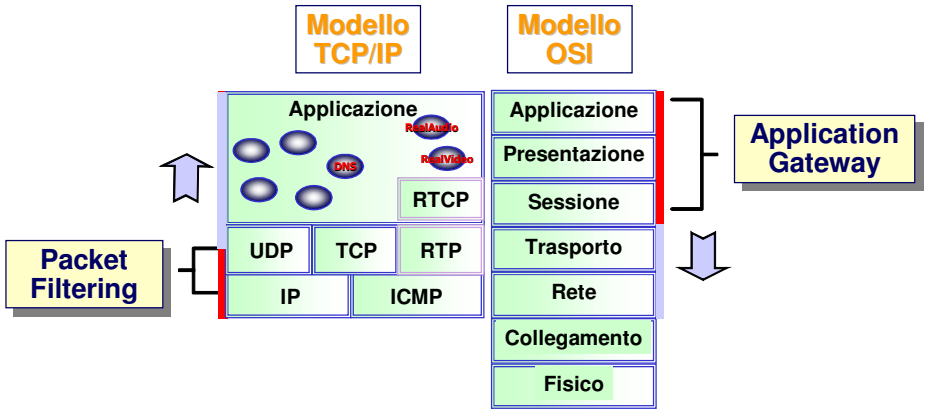


- Also called proxy server
- Acts as a relay of application-level traffic
- E.g. HTTP and FTP proxy, SMTP server, etc.

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)**

Packet Filtering vs. Application Gateway



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

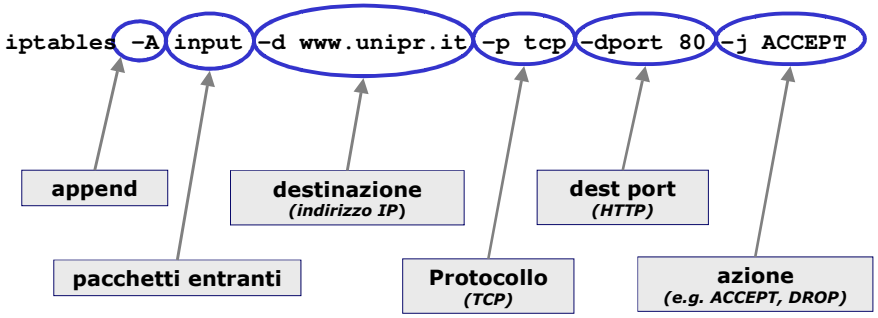
Informazioni strato applicativo

Regole di filtering: Esempio

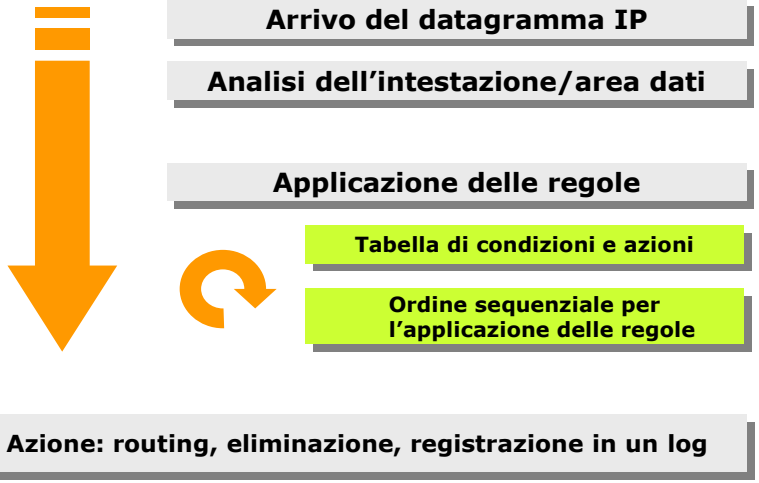
- Le regole di filtraggio sono ordinate in apposite liste o tabelle (Lists of rules), dette anche *Access control lists*, o *Chains*
- Esempio:
  - **abilitazione della posta elettronica (SMTP) e del web (HTTP)**

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

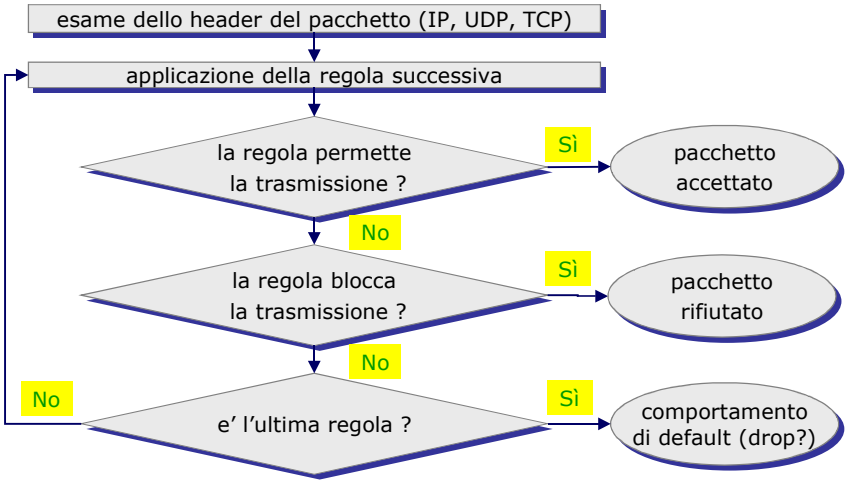
Esempio di inserimento di regole di filtering



Packet Filtering - Funzionamento



Logica delle regole di filtraggio



Modalità di filtraggio stateful/stateless

- Stafeful: con controllo di stato
- Stateless: senza controllo di stato

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)**

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]

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
```


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

Alcune complicazioni legate al packet filtering

- Protocolli applicativi che invertono la relazione tra client e server a livello di trasporto (e.g. FTP, SIP, etc.)
  - **la comunicazione a livello applicativo è di tipo client/server; a livello di trasporto la comunicazione iniziale è instaurata dal client applicativo (che sarà anche il client a livello di trasporto)**
  - **successivamente però è il server applicativo che instaura una nuova comunicazione a livello di trasporto; in questa comunicazione il server a livello di trasporto è il client applicativo**
  - **il nuovo numero di porta del server di trasporto può essere generato dinamicamente e scambiato durante la prima comunicazione**
  - **spesso si considerano politiche di inoltro in un firewall che abilitano la comunicazione client/server a livello applicativo in un solo verso; in questo caso diventa complicato individuare le eventuali porte da bloccare o abilitare**

Alcune complicazioni legate al packet filtering (cont.)

- Frammentazione dei pacchetti
  - **Per il protocollo IP un qualunque router può frammentare un pacchetto, che poi viene riassemblato a destinazione. Dopo la frammentazione solo il primo dei sotto-pacchetti contiene l'header con le informazioni necessarie per il packet filtering**
- Pericoli derivanti dall'utilizzo dell'IP source routing
  - **i pacchetto possono includere informazioni sul routing da seguire per arrivare a destinazione, anziché lasciare il cammino del routing a discrezione dei router da cui passa**
- Pericoli derivanti dall'IP spoofing
  - **nelle regole di filtraggio è quindi opportuno indicare anche l'interfaccia del router a cui arrivano i pacchetti**
  - **o prevedere opportune regole che bloccano eventuali tentativi di IP spoofing**

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
```


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 111 in
```


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
```

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**

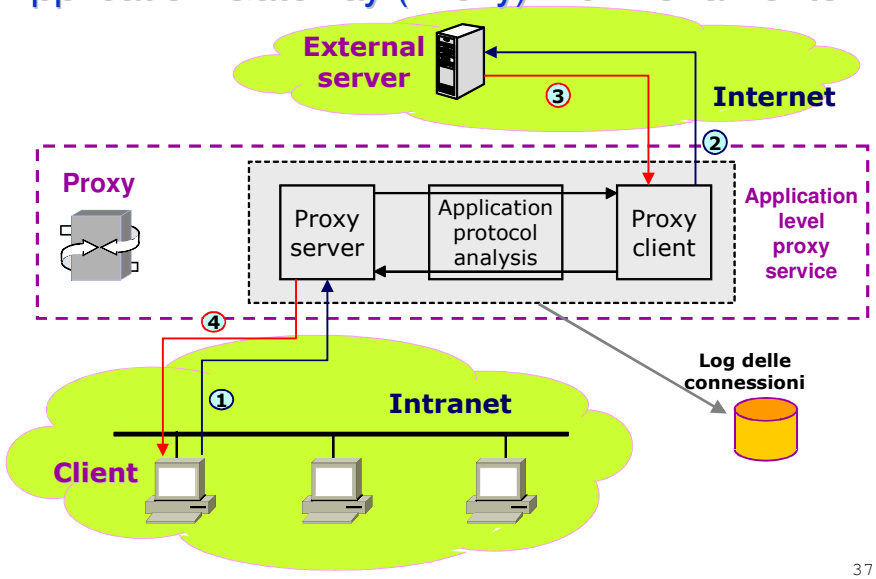
Bastion Host: servizi e vie di accesso

- 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/bachi 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**

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**

Application Gateway (Proxy): Funzionamento



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)**

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**

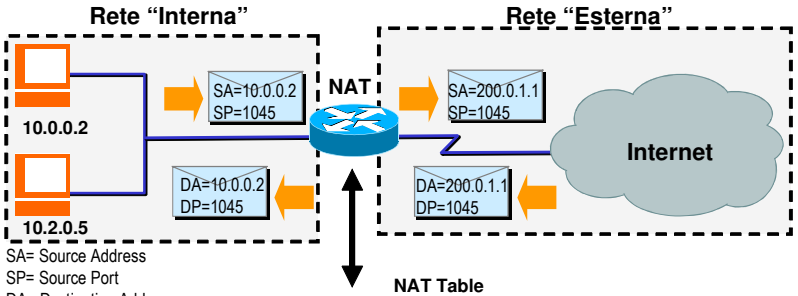
Quando si usa il NAT

- Un nodo NAT si usa quando si vuole:
  - **instradare verso la rete Internet del traffico proveniente da una rete interna (intranet) in cui si fa uso di indirizzamento privato**
    - lo scambio dei pacchetti deve essere bidirezionale
  - **semplificare lo spostamento (migrazione) di una rete (e.g. aziendale) da un un punto di accesso alla rete Internet ad un altro**
    - ad esempio a causa di cambio ISP
    - si vuole evitare la riconfigurazione di tutti i nodi (host e router) interni alla rete
  - **semplificare le tabelle di routing (avoidance of routing table explosion)**
    - isolando una porzione di rete dietro ad un router NAT e rendendo invisibile la sua struttura interna all’esterno
  - **nascondere l’indirizzamento utilizzato all’interno della propria rete**
  - **proteggere i nodi interni ad una rete da attacchi provenienti dall’esterno**

Tipologie di NAT

- Traslazione del tipo n↔n
  - **ciascun indirizzo IP interno ad una rete viene tradotto in un indirizzo IP esterno distinto, appartenente ad un pool di indirizzi predeterminato**
    - alcune volte riferito col termine "simple NAT"
    - NAT statico: la corrispondenza indirizzo interno e esterno è permanente, ovvero ogni indirizzo viene mappato sempre nel medesimo indirizzo esterno
    - NAT dinamico: la corrispondenza tra indirizzo interno e esterno è variabile, ovvero ogni indirizzo viene mappato in un indirizzo casuale prelevato d un insieme di indirizzi disponibili
- Traslazione del tipo n↔1
  - **tutti gli indirizzo IP interni ad una rete vengono tradotti in un medesimo indirizzo IP esterno**
    - per permettere il mappaggio inverso si deve far ricorso all'utilizzo delle informazioni di numero porta che vengono opportunamente modificate
    - più propriamente riferito col termine NAPT (Network Address and Port Translator)
    - è il tipo di NAT più utilizzato
- In entrambi i casi gli indirizzi "interni" hanno valore solo dietro al NAT e possono essere di tipo privato

Simple NAT

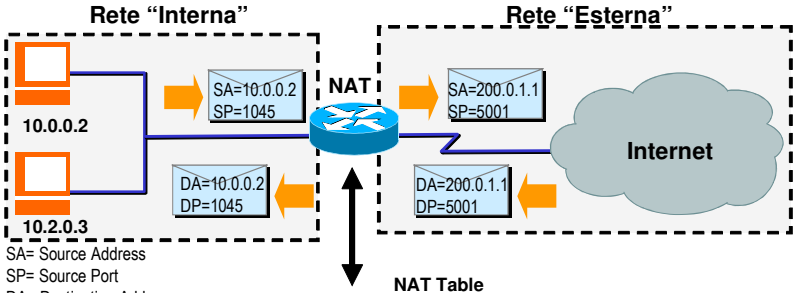


NAT Table

internal address	external address	remote address/port
10.0.0.2	200.0.1.1	*
10.0.0.3	200.0.1.2	*

- Funzionamento:
  - **viene tradotto il SA dei pacchetti uscenti (da sinistra a destra) da indirizzo interno a indirizzo esterno**
  - **viene tradotto il DA nei pacchetti entranti da indirizzo esterno a interno (mappaggio inverso)**
  - **tale mappaggio è mantenuto da una apposita tabella (NAT table)**

NAPT



NAT Table

internal address/port	external address/port	remote address/port
10.0.0.2:1045	200.0.1.1:5001	*
10.0.0.3:2340	200.0.1.1:5002	*

- Funzionamento:
  - **tutti gli host interni utilizzano un singolo indirizzo IP pubblico esterno**
  - **vengono utlizzate 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**

Vantaggi del NAPT

- Vantaggi:
  - **Indirizzamento:**
    - risparmio di indirizzi (un unico IP pubblico per un intera rete)
    - semplificazione tabelle di routing
    - configurazione della rete interna
  - **sicurezza:**
    - nascondere la struttura (e indirizzamento) di una rete interna
    - limitare (e proteggere) l'accesso verso una rete interna
    - intende nascondere il server che eroga un servizio, mediante ridirezione
  - **Load balancing:**
    - bilanciare il carico tra più server che erogano un servizio

Svantaggi del NAPT

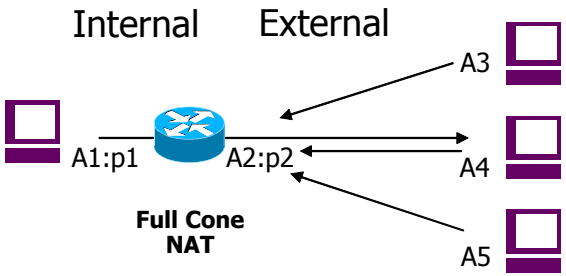
- Svantaggi:
  - **complicato l'impiego di server all'interno della rete accessibili dall'esterno**
    - in questi casi si ricorre al "static natting" o "destination NAT" (DNAT)
    - vengono configurati (staticamente) mappaggi tra porte esterne e coppie indirizzo/porta interne
    - il mappaggio viene fatto a partire da pacchetti entranti e in base alla potta di destinazione (destination NAT)
  - **complicato il funzionamento di alcuni applicativi che non mantengono una relazione fissa client/server a livello di trasporto, e.g. FTP, H323, SIP**
    - ad esempio quando gli indirizzi IP e porte dei nodi interni vengono inviati nel payload del messaggi applicativi per poi essere usati per instaurare comunicazioni nel verso opposto
    - In questi casi, sono necessari dei Application Level Gateway (ALG) implementati nel nodo NAPT che modificando il contenuto dati di livello applicativo dei pacchetti

Differenti tipi di NAPT

- Il NAT (e NAPT) non è un protocollo poiché non richiede un accordo tra due o più parti
  - **NAT opera il mappaggio nei due versi in modo trasparente agli altri nodi intermedi e terminali della comunicazione**
  - **ogni implementazione può utilizzare specifici meccanismi di mappaggio**
    - tipo di tabelle
    - informazione utilizzata per il mappaggio (e.g. solo gli indirizzi da mappare o anche l'indirizzo del host remoto)
    - supporto di eventuali protocolli applicaitvi che richiedono trattamento a parte (tramite appositi ALG)
- In letteratura i NAPT vengono comunque classificati come:
  - **Full cone NAT**
  - **Restricted cone NAT**
  - **Port restricted cone NAT**
  - **Symmetric NAT**

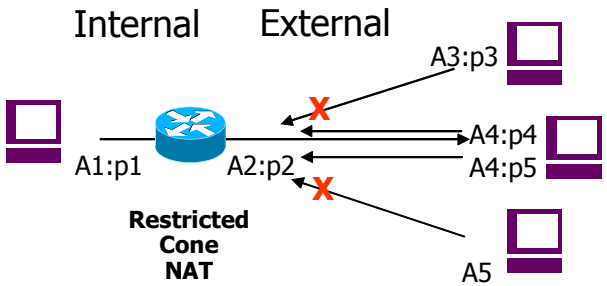
Tipi di NAT: Full Cone NAT

- 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**



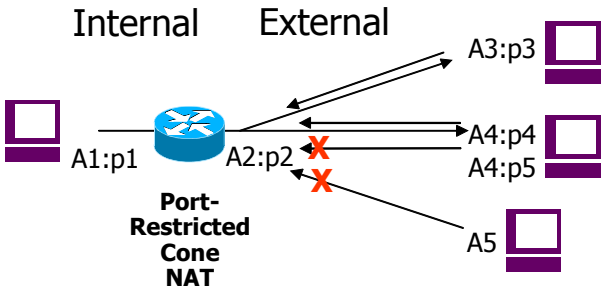
Tipi di NAT: Restricted Cone NAT

- Restricted cone NAT
  - **is like a restricted cone NAT, but it restricts the number of remote hosts that can send packets to the internal host**
  - **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**



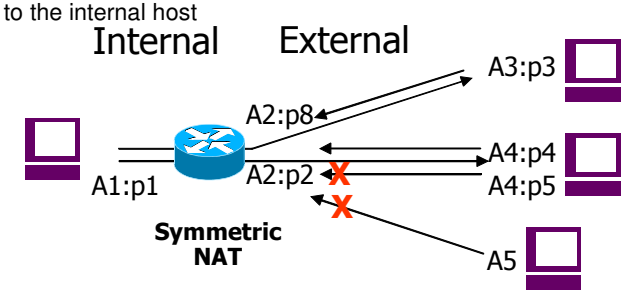
Tipi di NAT: Port Restricted Cone NAT

- 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**



Tipi di NAT: Symmetric NAT

- Symmetric NAT
  - **all requests from the same internal IP address/port to a specific destination IP address/port are mapped to specific external source IP address/port**
    - if the same 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 packet back to the internal host



NAT/FW traversal

- NAT router
  - **è dispositivo di sicurezza "leggera"**
    - nasconde la topologia fisica
    - puo' implementare funzionalita' di firewall di base
  - **il numero di NAT installati è in forte crescita (broadband at home, hot-spot, etc.)**
    - principalmente perché riduce il numero di indirizzi IP necessari
  - **anche con IPv6 è probabile che ci sia il bisogno di NAT ancora come dispositivi di sicurezza "leggera"**
- Packet filter firewall
  - **anche le resenze dei FW è in forte crescita soprattutto nelle reti aziendali ma anche per uso domestico/residenziale (includendo i FW personali)**
  - **le regole dei FW sono spesso molto restrittive (solo traffico da o verso indirizzi/porte note)**

NAT/FW traversal (cont.)

- Sebbene siano dispositivi diversi, questi hanno molte similitudini dal punto di vista del comportamento esterno
- In entrambi i casi si pone il problema per alcuni applicativi non NAT-friendly (o FW-friendly)
  - **applicazioni che non riescono ad attraversare facilmente NAT o Firewall senza opportuni interventi o modifiche**
    - applicazioni server
    - applicazioni che scambiano informazioni di indirzzamento IP e trasporto all'interno di messaggi applicativi (e.g. FTP, VoIP, P2P, Instant Messaging, etc.)

NAT/FW traversal: soluzioni

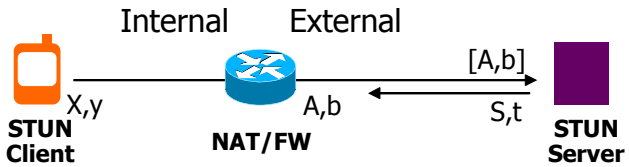
- Configurazione statica del NAT/FW
  - **apertura di specifici 'pinholes' statici**
  - **possibile rischio per la sicurezza**
  - **si devono conoscere gli specifici protocolli applicativi usati**
  - **difficile da configurare dato che molti protocolli applicativi negoziano le porte dinamicamente**
- Utilizzo di NAT Application Level Gateway (NAT ALG)
  - **funzionano a livello di pacchetto nel nodo NAT, ispezionando anche il contenuto dei messaggi applicativi**
  - **modificano eventuale informazione di indirzzamento IP e trasporto scambiata a livello applicativo e configurano dinamicamente opportune regole di inoltro**

NAT/FW traversal: soluzioni (cont.)

- Utilizzo di Proxy applicativi
  - **funzionano a livello applicativo, terminano e riaprono la comunicazione a livello IP (e trasporto)**
  - **possono essere posizionati su rete esterna o in apposita zona demilitarizzata (DMZ)**
  - **eventuali 'pinholes' devono essere configurati solo da o verso questi nodi**
  - **application-protocol specific: e.g. FTP proxy**
- Utilizzo di STUN/TURN/ICE
  - **funzionamento a livello applicativo utilizzando però meccanismi applicativi indipendenti dalle specifiche applicazioni (STUN/TURN/ICE)**
  - **tali protocolli devono essere inclusi all'interno delle applicazioni client**
  - **richiedono la presenza di appositi server esterni (STUN e/o TURN server)**
  - **STUN permette di scoprire che tipo di NAT o FW è presente e eventualmente quale indirizzo esterno viene mappato dal NAT**
  - **TURN permette di creare dei punti di rilancio esterni al NAT o FW, a livello di trasporto**
  - **soluzione ancora poco supportata**

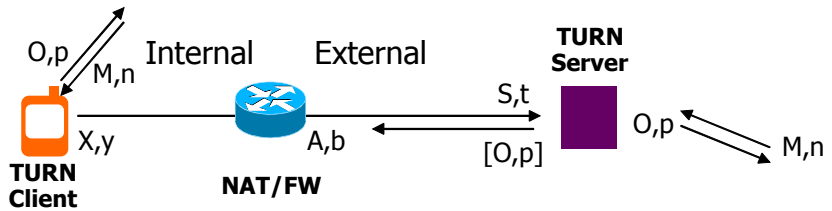
NAT/FW traversal: STUN

- Simple Traversal of User Datagram Protocol (UDP) Through NATs (STUN)
  - **scopre l'indirizzo IP pubblico (e le regole di mappaggio delle porte) del NAT tra il client ed il server inviando una serie di pacchetti di prova**
  - **non funziona con i NAT simmetrici utilizzati dalla maggior parte delle industrie per le loro reti**
  - **non funziona se i client sono dietro lo stesso NAT**
  - **necessita di uno STUN client nel client applicativo**
  - **richiede la messa in opera di un server STUN su di un nodo esterno**



NAT/FW traversal: TURN

- Traversal Using Relay NAT (TURN)
  - **protocollo che consente ad un client dietro un NAT o FW di ricevere a livello di trasporto rilanciati da apposito TURN server**
  - **funziona anche con i NAT simmetrici**
  - **necessita di uno TURN client nel client applicativo**
  - **richiede la messa in opera di un server TURN su di un nodo esterno**

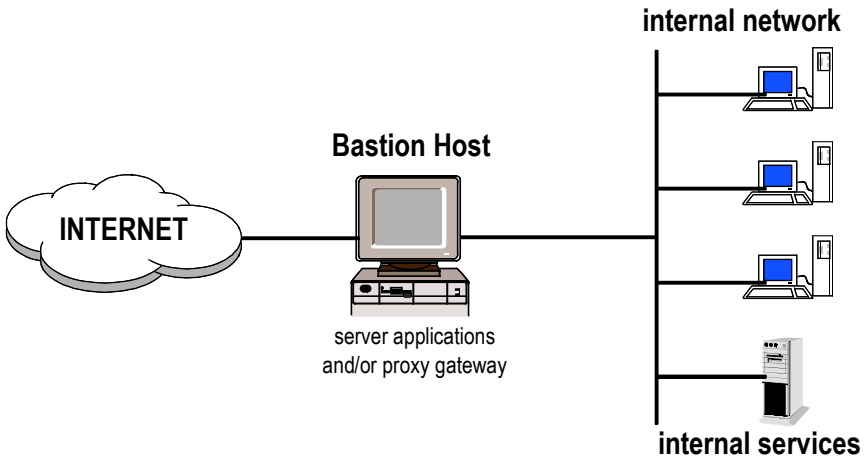


Configurazioni di firewall

Firewall configurations

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

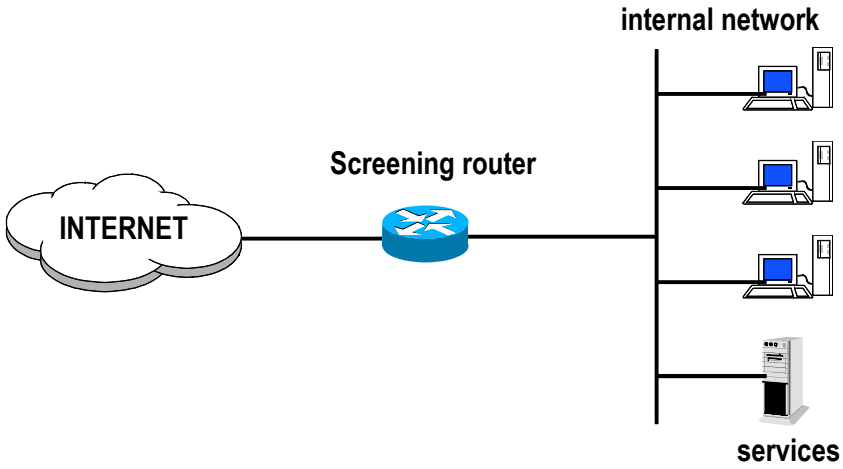
Dual-homed host firewall



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**

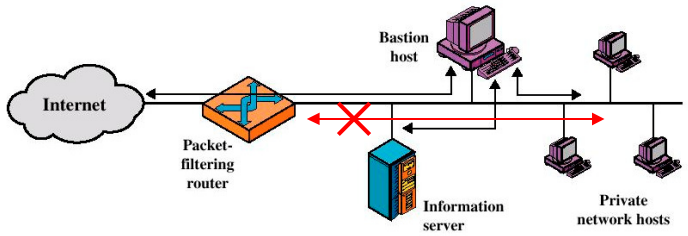
Screening router



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**

Screened host firewall (single-homed bastion host)

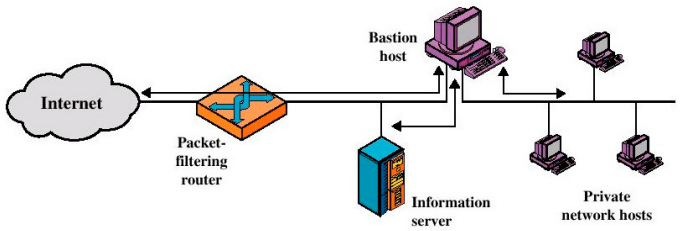


- Screened host firewall, single-homed bastion configuration
- Firewall may consist by two systems:
  - **A packet-filtering router**
  - **A bastion host**

Screened host firewall (single-homed bastion host)

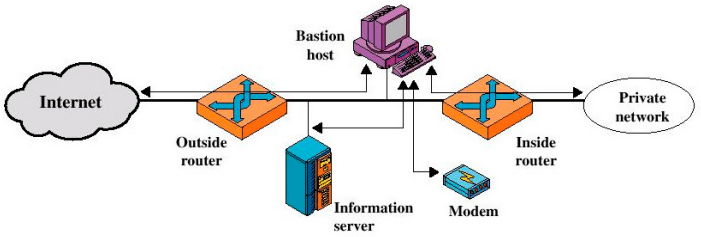
- Configuration for the packet-filtering router:
  - **Only packets from and to the bastion host are allowed to pass through the router**
- The bastion host performs authentication and proxy functions
- Greater security than single configurations because of two reasons:
  - **This configuration implements 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)

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**

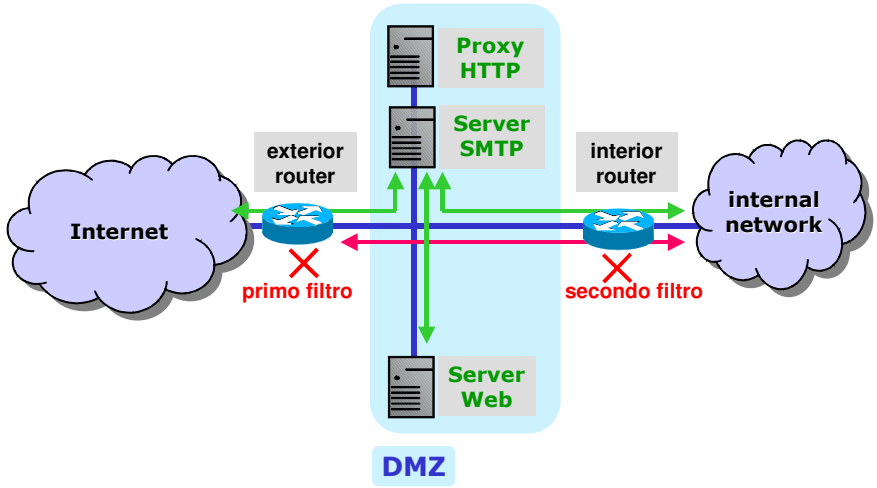
Screened-subnet firewall



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

Screened-subnet firewall (cont.)

- Demilitarized Zone

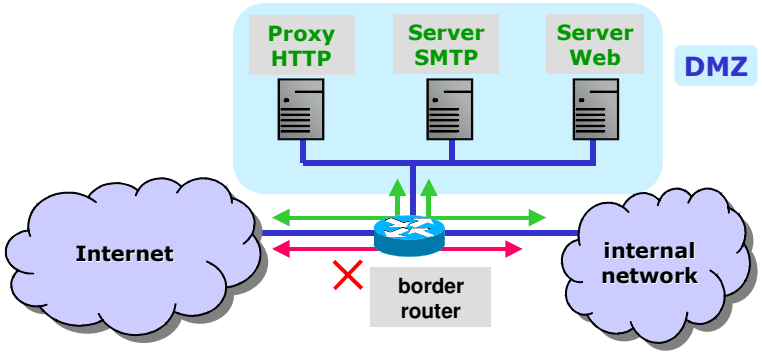


Screened-subnet firewall (cont.)

- 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)**

Screened-subnet firewall (cont.)

- Merging of interior/exterior router



Screened-subnet firewall (cont.)

- Può essere pericoloso:
  - **Unire bastion host e exterior router**
  - **Unire bastion host e interior router**
  - **Molteplicità di Interior routers**

- Non è pericoloso:
  - **Molteplicità di internal networks**
  - **Molteplicità di exterior routers**
  - **Molteplicità di DMZs**