Sicurezza Informatica PG
a.a. 2007-2008

Firewalls

Stefano Bistarelli
bista@sci.unich.it

Sommario

- Introduzione (Sicurezza e Firewall)
- Firewalls (Da bastion host a rete di difesa)
- Firewalls (Overview)
- 2 Filosofie ed 1 Principio
- Tipi di Firewalls
- Firewall environments
- Firewall security policy
- Tipiche configurazioni
- Un esempio
- Firewall Administration
- Raccomandazioni finali

Introduzione

Sicurezza e Firewalls

Come proteggersi?

- Physical security
  - Accesso fisico di utenti alle macchine
- Operational/Procedural security
  - Policy di sicurezza
- Personnel Security
  - …
- System Security
  - Acl, log, …
- Network Security
  - Firewall, IDS, buon routing e filtri

Come proteggersi?

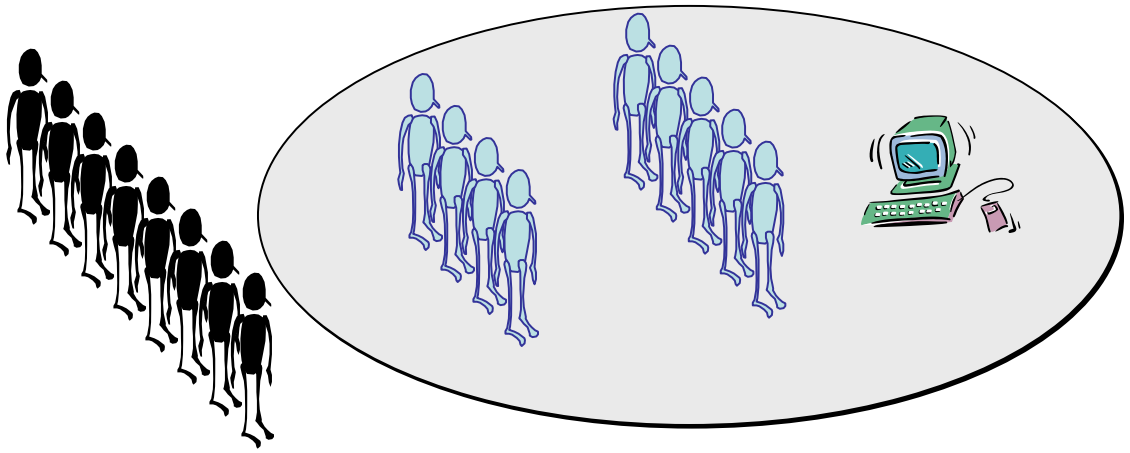
- Physical security
  - Accesso fisico di utenti alle macchine
- Operational/Procedural security
  - Policy di sicurezza
- Personnel Security
  - …
- System Security
  - Acl, log, …
- Network Security
  - Firewall, IDS, buon routing e filtri

Piano di Sicurezza

- Risk Avoidance (evitare rischi)
  - Necessitiamo di una connessione Internet permanente?
- Deterrence (deterrenza)
  - Pubblicizzare strumenti di difesa e di punizione
- Prevention (prevenzione)
  - Firewall
- Detection (detection)
  - IDS
- Recovery

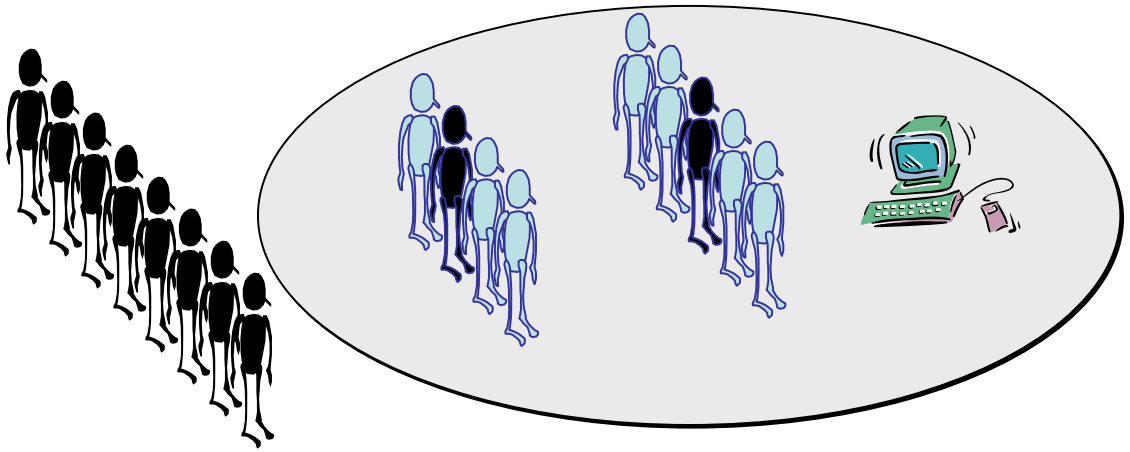
Firewalls???

- *Sicurezza non è sinonimo di Firewall!!*
- *Insiders and Outsiders!!*



Firewalls???

- *Sicurezza non è sinonimo di Firewall!!*
- *Insiders and Outsiders!!*



Firewalls

Da bastion host a rete di difesa

Firewalls oggi

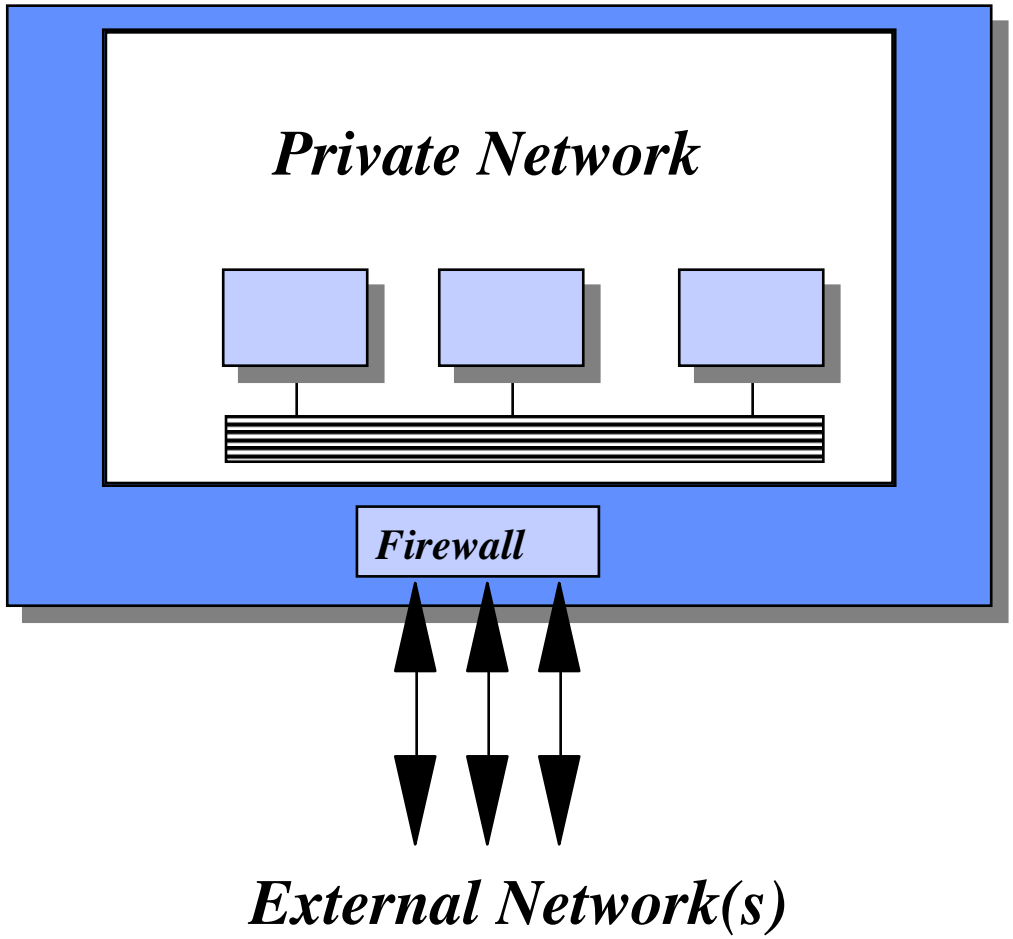
- Firewall non è un componente della rete ma un insieme di componenti che cooperano tra loro
  - Firewall e Intrusion Detection Systems (IDS)
  - Email/web content scanners per virus e malicious code (worms)
  - Personal firewalls
  - … a Policy!!
- Firewalls non come prima linea di difesa .. ma l'ultima!

Definizione

- *Network Firewalls are devices or systems that control the flow of network traffic between networks employing different security postures. (NIST)*
- *Firewalls di rete sono apparecchiature o sistemi che controllano il flusso del traffico di rete tra due reti con differenti livelli di sicurezza.*

Firewalls

- ***Firewall:*** *un metodo per prevenire accessi non autorizzati alla rete privata.*

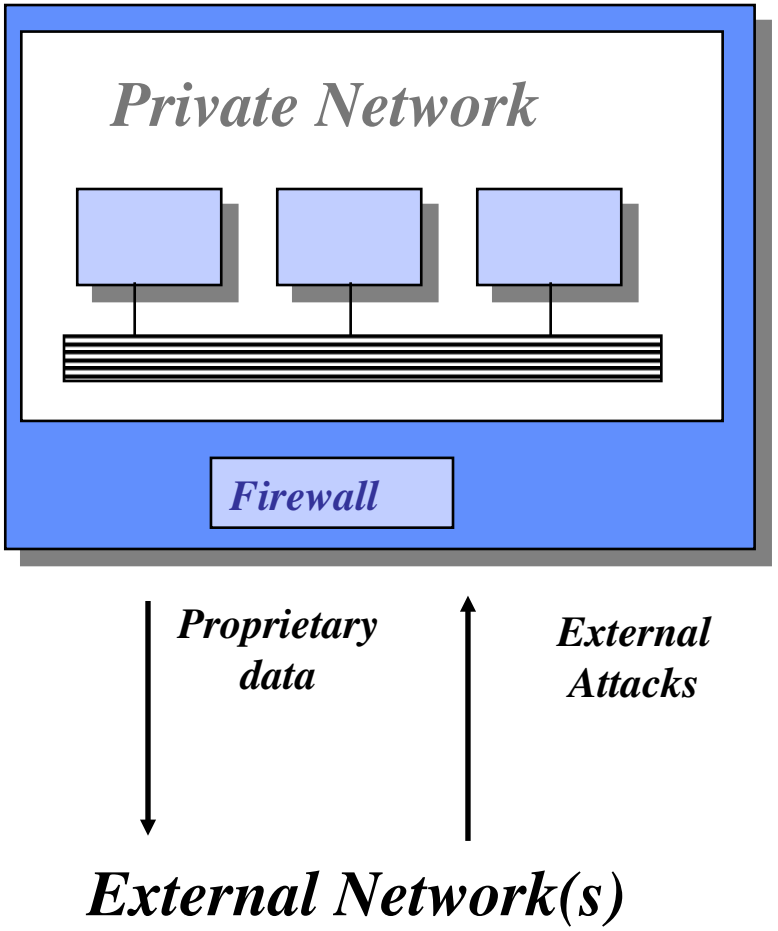


Firewalls

Overview

Cosa può fare un firewall

- Proteggere le risorse della rete privata da attacchi esterni.
- Prevenire l'esportazione di dati dall'interno verso l'esterno.
- Importante: usarlo insieme ad altri meccanismi di sicurezza!!



Vivere senza FW, …, si, … però

- *Riduce le possibilità di un external intruders di alterare la rete interna*
  - *Password vulnerability*
  - *Network probes for known flaws in services*
  - *Address (and other) spoofing*
  - *Details of the file system*
  - *Mail problems*
  - *Worms e virus*

Worms e virus

- Worms
  - Codice che si diffonde da un computer ad un altro usando una qualche vulnerabilità. Quando un computer ha un worm si dice "compromesso" ("compromised"). Una volta compromesso un computer inizierà ad infettare gli altri.
- Virus
  - Codice eseguito da un utente che fa qualcosa di inaspettato rispetto a quello che l'utente prevedeva. Spesso attachments di posta contengono virus. Un virus non usa una vulnerabilità del sistema, ma fa uso dell'utente!

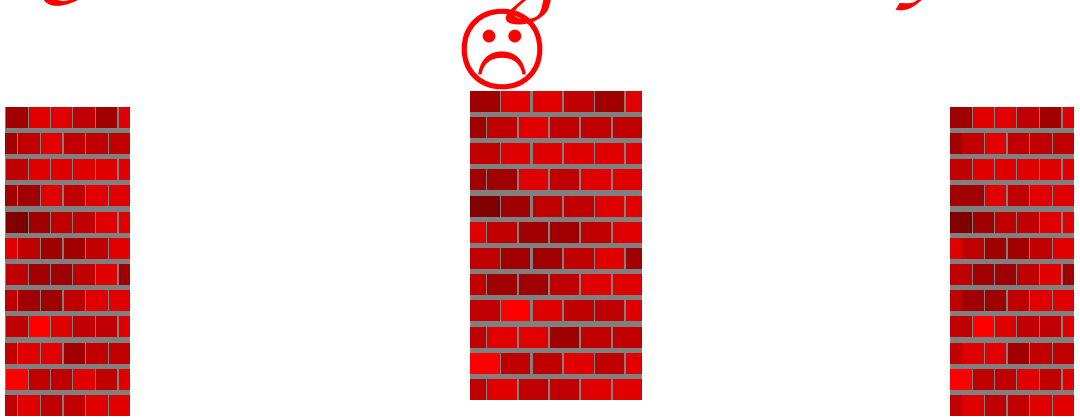
Cosa può fare un firewall, cont.

- Schermare alcune reti interne e nasconderle agli altri
- Bloccare alcuni accessi a servizi o ad utenti
- Monitorare!
  - Log function importante!!

Cosa può fare un firewall, cont.

- Virtual private networks (VPN)
  - Crittazione automatica dei dati tra i siti
  - Fornisce confidentialità dei dati inviati tra i due gateways
  - Le 2 reti appaiono come una singola rete, al di qua del firewall,
  - Buono per reti che si localizzano su più siti e collegate da una untrusted network (ex: Internet)
  - VPN permette l'uso remoto dei servizi locali

Alcuni Commenti negativi sui Firewalls



- *Firewalls sono l'approccio sbagliato: Non risolvono il problema, e rendono impossibile o molto difficile fare molte cose agli utenti interni.*
- *… d'altra parte, un responsabile di una rete interna non vivrebbe tranquillamente senza un firewall*

Più specificatamente ☹

- *Non difende contro nuovi bachi non ancora documentati nei protocolli*
- *I filtri sono difficili da settare e da mantenere perchè difficile compromesso tra libertà e sicurezza*
- *Può degradare le performance della rete*

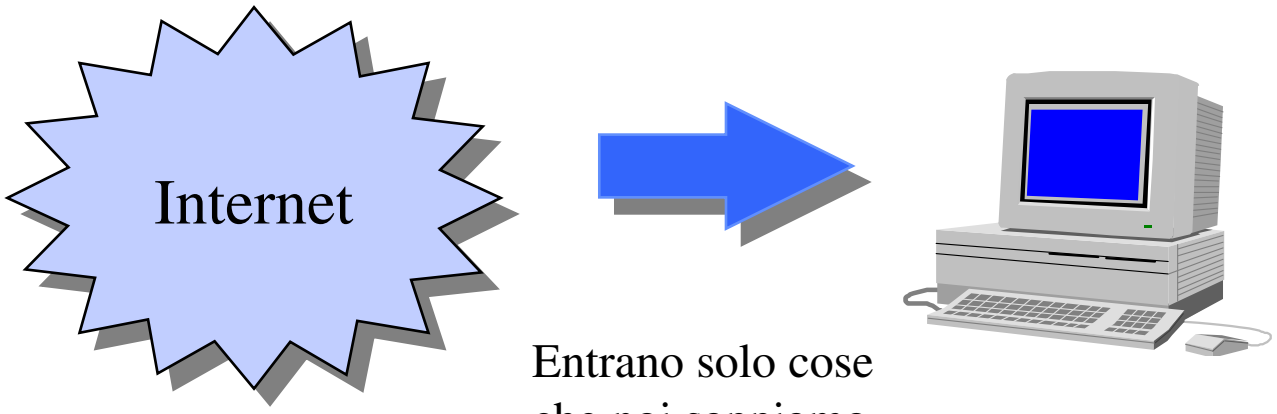
2 Filosofie ed 1 Principio

Due filosofie

- *Default deny:*
  - *Tutto quello che non è espressamente ammesso è proibito*
- *Default permit:*
  - *Tutto quello che non è espressamente proibito è ammesso*

Default deny

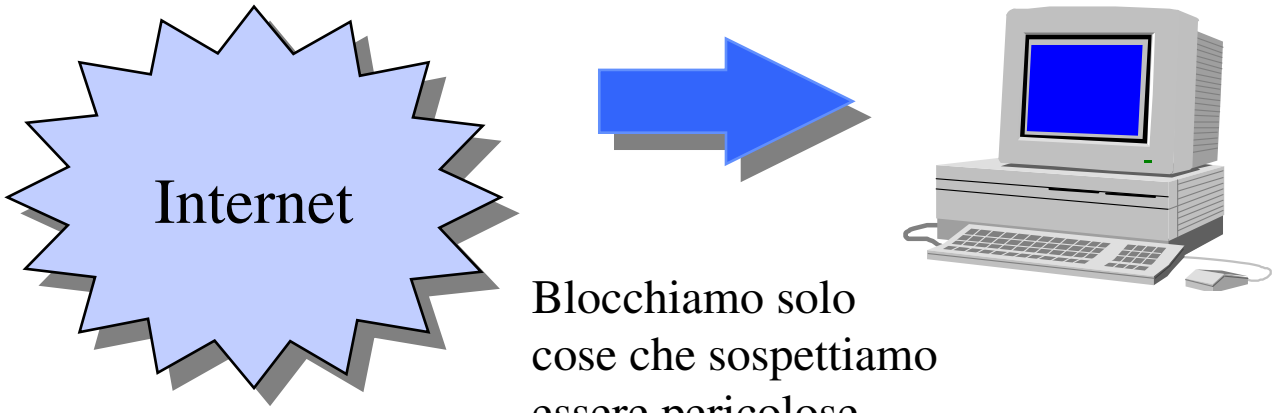
- *Firewall devono essere creati per bloccare tutto*
- *Servizi sono abilitati caso per caso dopo una attenta analisi*
- *Utenti sono molto ristretti e non possono facilmente rompere la policy di sicurezza*



Entrano solo cose
che noi sappiamo
essere non pericolose

Default permit

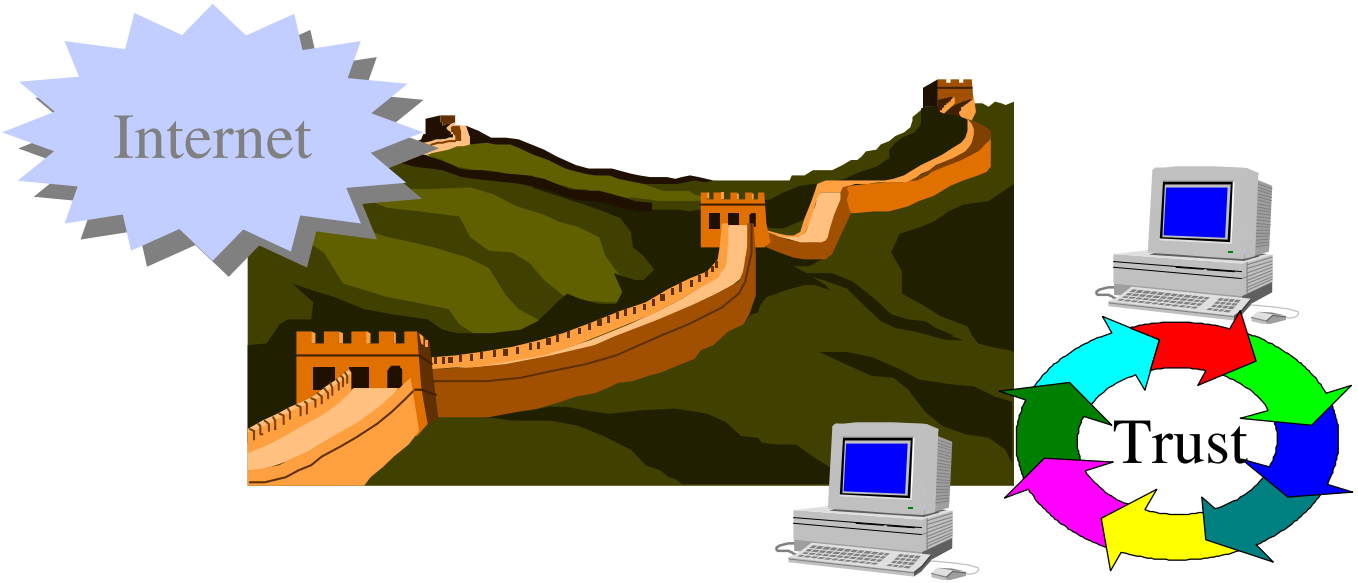
- *System administrator deve reagire prontamente ogni volta che un nuovo baco su un protocollo viene scoperto*
- *Servizi sono rimossi/ridotti quando vengono scoperti pericolosi*
- *Utenti sono meno ristretti*



Blocchiamo solo
cose che sospettiamo
essere pericolose

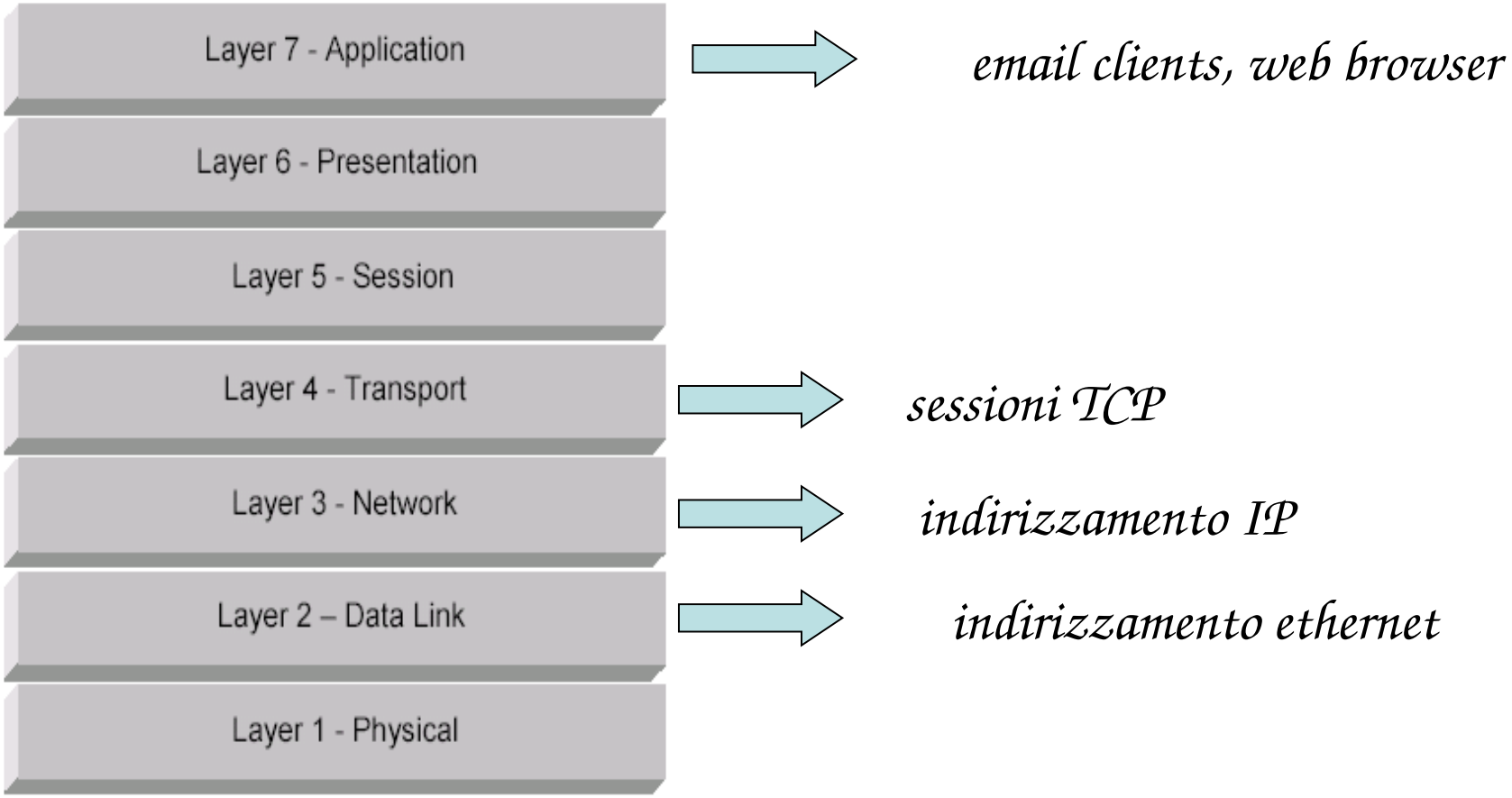
Il principio: La difesa perimetrale

1. Proteggi tutti I cammini di ingresso alla rete privata
   - Crea una sola porta di ingresso!
2. All'interno della rete gli host si fidano tra loro



Tipi di Firewalls

Classificazione dei firewalls



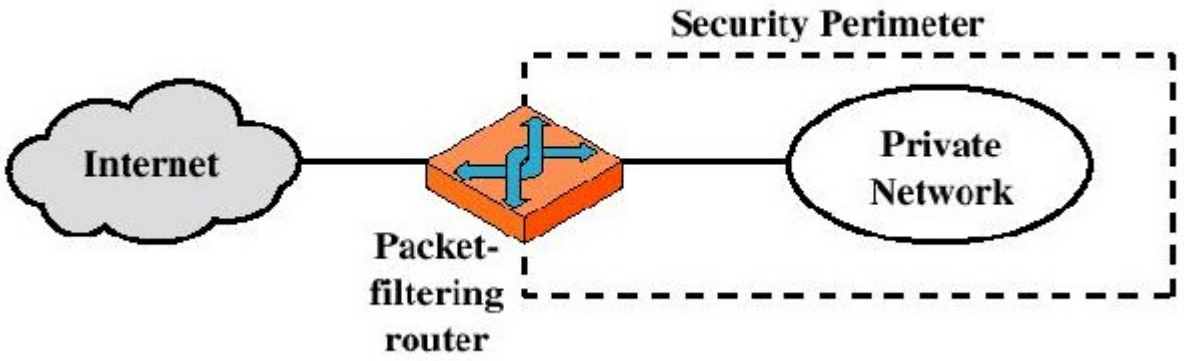
Servizi add-on

- NAT
  - Static translation
  - hiding translation
- DHCP
- Encryption functionality (VPNs)
- Application content filtering

Tipi di Firewalls

- *Packet-filtering routers*
- *Application-proxy gateways*

Packet Filter firewalls



Filtri a livello 3:

- Source address del pacchetto (IP address)
- Destination address del pacchetto (IP address)
- Tipo del traffico (IP,ICMP,IPX se a livello 3, o anche protocolli di livello 2)
- Possibilmente, alcune caratteristiche del livello 4 (porta sorgente e destinazione)
- Talvolta, informazioni interne al router (quali informazioni circa l'interfacce sorgente e di destinazione del pacchetto, utile per routers con più interfacce)

Boundary router: vantaggi/svantaggi

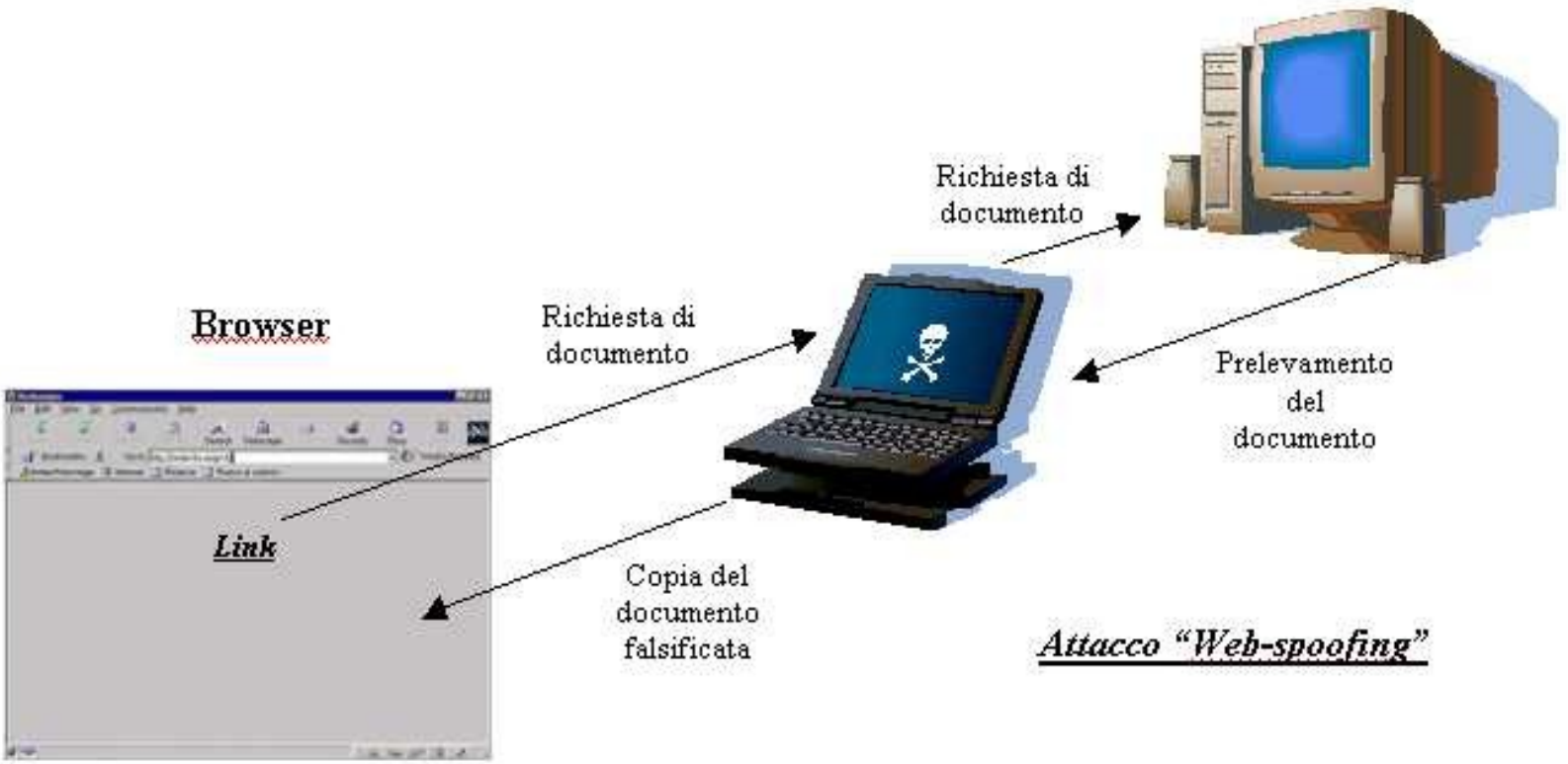
- Vantaggi:
  - Semplicità
  - Trasparente per l'utente
  - Alta velocità
- Svantaggi:
  - Nessun controllo per filtrare comandi/funzioni ai livelli più alti
    - Mancanza di user authentication
  - Funzioni di log praticamente inefficaci
  - Difficoltà nel creare buone regole

Packet filter rulesets

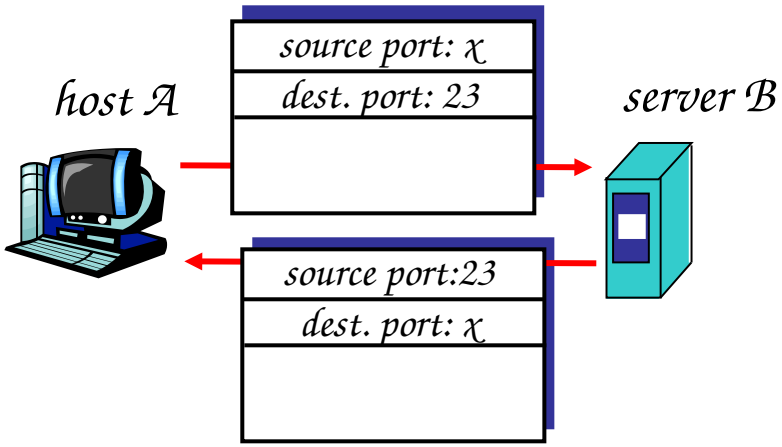
	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3	Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system.
4	192.168.1.0	Any	Any	Any	Allow	Internal Users can access External servers
5	Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email in
6	Any	Any	192.168.1.3	HTTP	Allow	Allow External Users to access WWW server
7	Any	Any	Any	Any	Deny	"Catch-All" Rule - Everything not previously allowed is explicitly denied

- *Accept*
- *Deny*
- *Discard*
  - *"Black hole" = trasparente all'esterno*

Regola 2:
Es. spoofing (Ip + TCP port 80)



Regola 1:
connessione TCP/UDP lato client



port use: simple telnet app

- Connessione a una porta (23) viene fatta creando lato cliente una porta (x>1023) a cui il server risponderà.
- Numeri di porte inseriti nel paccheto

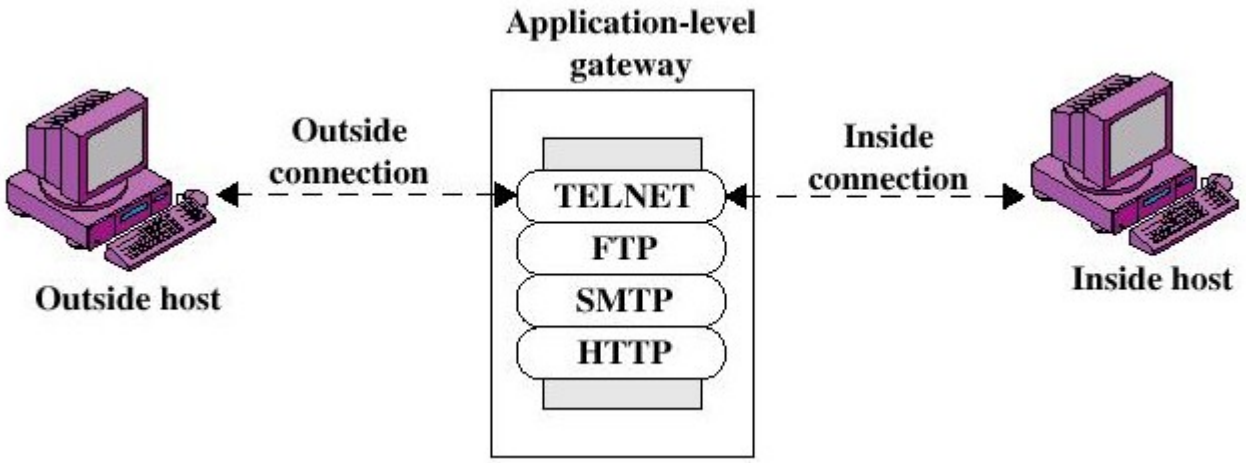
Stateful inspection firewalls

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet

- *Incorpora alcuni controlli a livello 4*
- *Crea dinamicamente una "state table" per validare inbound traffic*

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established

Application-proxy gateways



Filtri a livello 7

- Routing tra le due interfacce effettuato a livello applicazione dal software del firewall
  - In caso di malfunzionamento del sw, il routing è disabilitato
- Possibilità di authentication
  - userId and password
  - HW/SW token authentication
  - Biometric authentication (remota? Solo in aggiunta ad altri strumenti)
- Filtri su specifici comandi
  - (es. permetto get ma non put)

Proxi: vantaggi/svantaggi

- Vantaggi:
  - Più sicuri dei packet filters
  - Deve solo controllare un numero limitato di applicazioni (http, ftp, posta)
  - Facile il log e il controllo del traffico
- Svantaggi:
  - Processing overhead su ogni connessione
  - Può solo controllare un numero limitato di applicazioni (http, ftp, posta)

Proxy server dedicati

- *Specifici per ogni applicazione*
- *Aiutano l'application proxy gateway nel lavoro di contents-inspection*
- *Tipico uso:*
  - *Antivirus*
  - *Malicius code (applets java, activix, javascript, word)*
  - *Usati spesso per outbound connections*
    - *Web cache proxy*
    - *Email proxy*

Personal firewalls

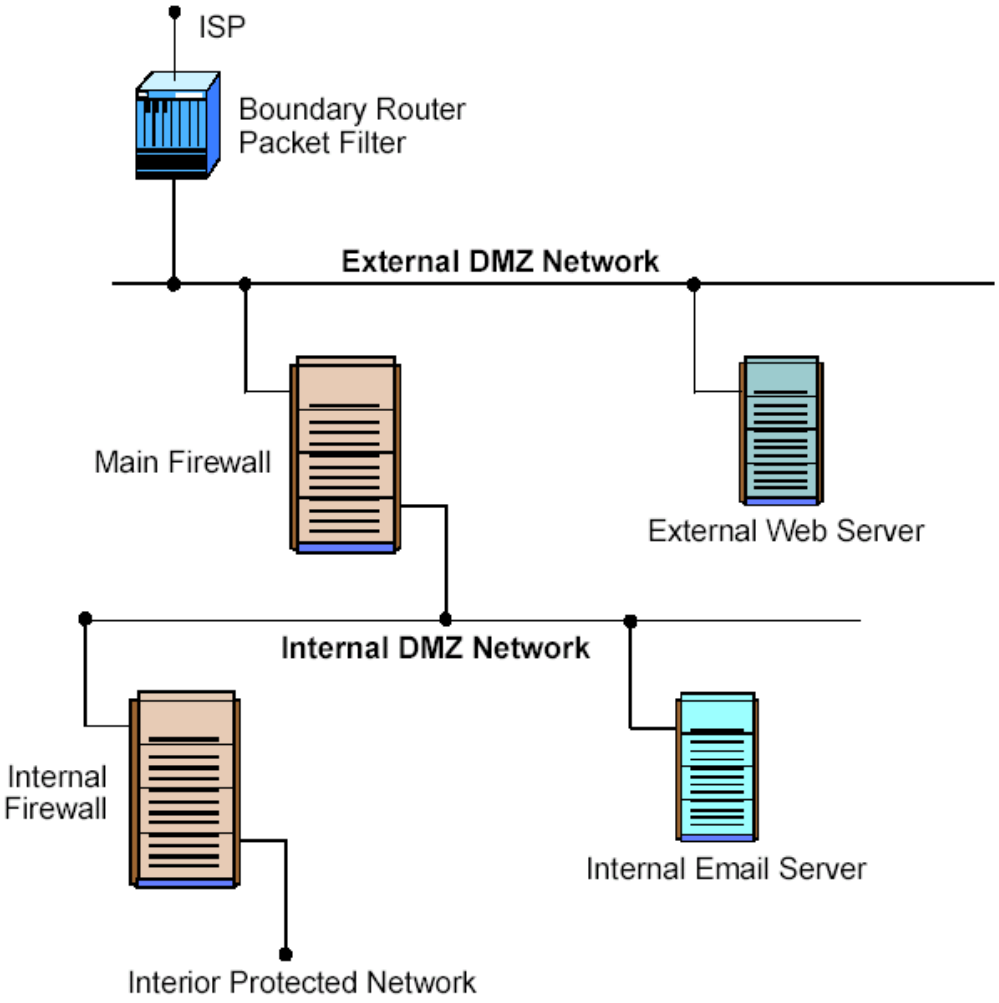
- Proteggono solo la macchina dove sono istallate
- Necessario, specie per mobile users
- Es:
  - winXp
  - Zonealarm
  - …

Firewall environments

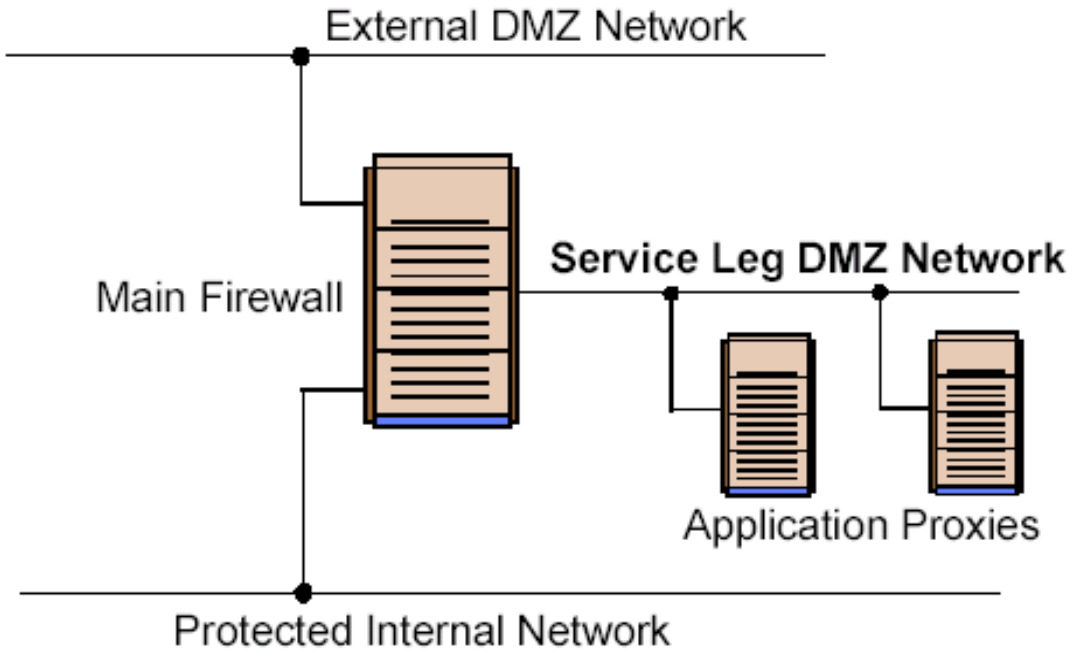
Linea guida per firewall environment

- *KISS principle (Keep It Simple Stupid!)*
- *Usa i devices per il loro scopo naturale!*
- *Sicurezza a piu' livelli (se più firewall in cascata possono essere usati, USARLI!)*
- *Attenzione agli attacchi dall'interno!* ☺

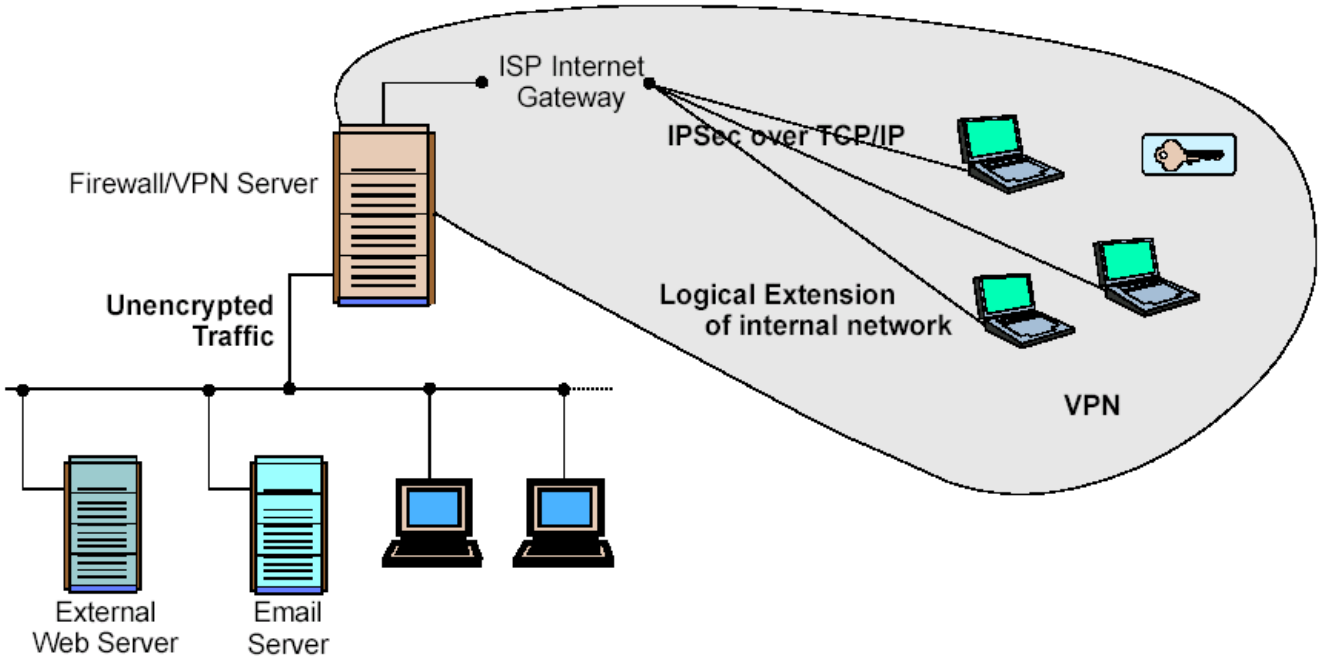
Environment 1: DMZ



Environment 1: DMZ
(service leg)

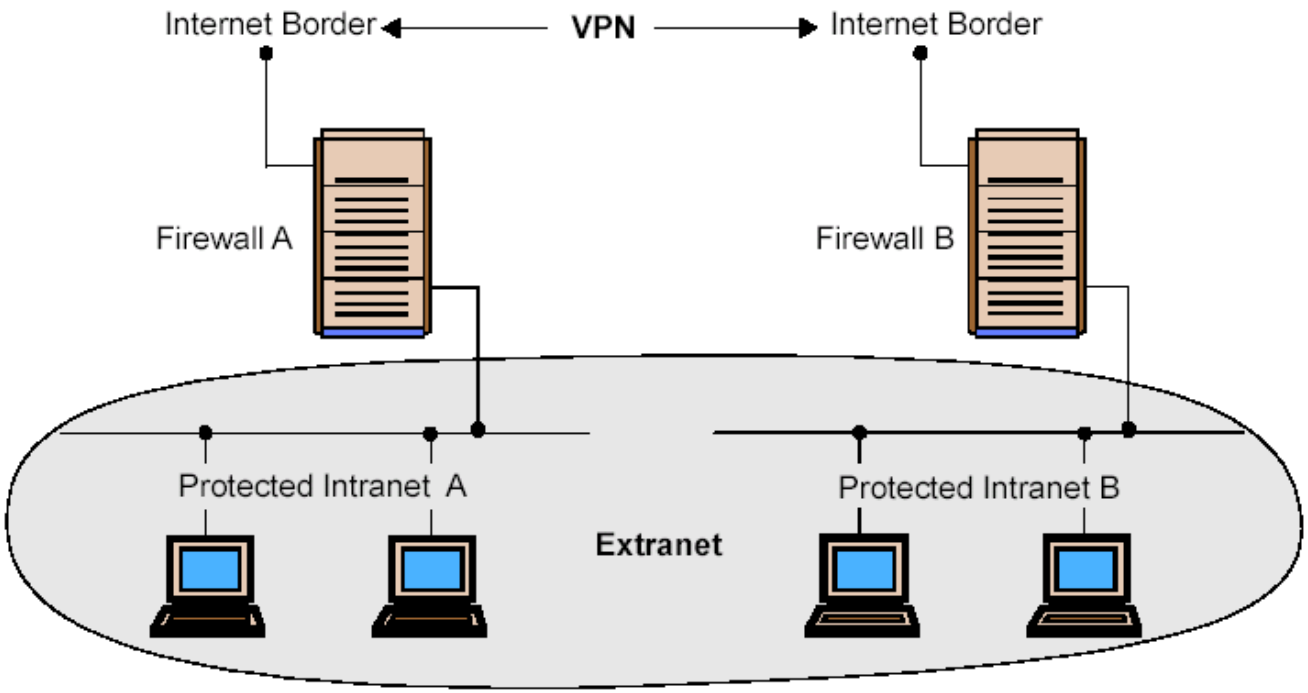


Environment 2: VPN



- VPN
  - IPSec
  - PPTP (by microsoft)
  - L2TP
- Firewall e VPN server insieme?
  - Si, ma
  - Prestazioni.. ☹

Environment 3: Intranet/extranet



Environment 4: Hubs/Switches

- Hubs
  - Devices a layer 1
  - Broadcast traffic
- Switches
  - Devices a layer 2
  - (essentially multiport bridges)
  - No possibilità di snif/eavesdrop tra porta e porta
    - OK per DMZ e Firewall environment
  - Isolamento delle subnets da tenere di conto nell'uso di IDSs

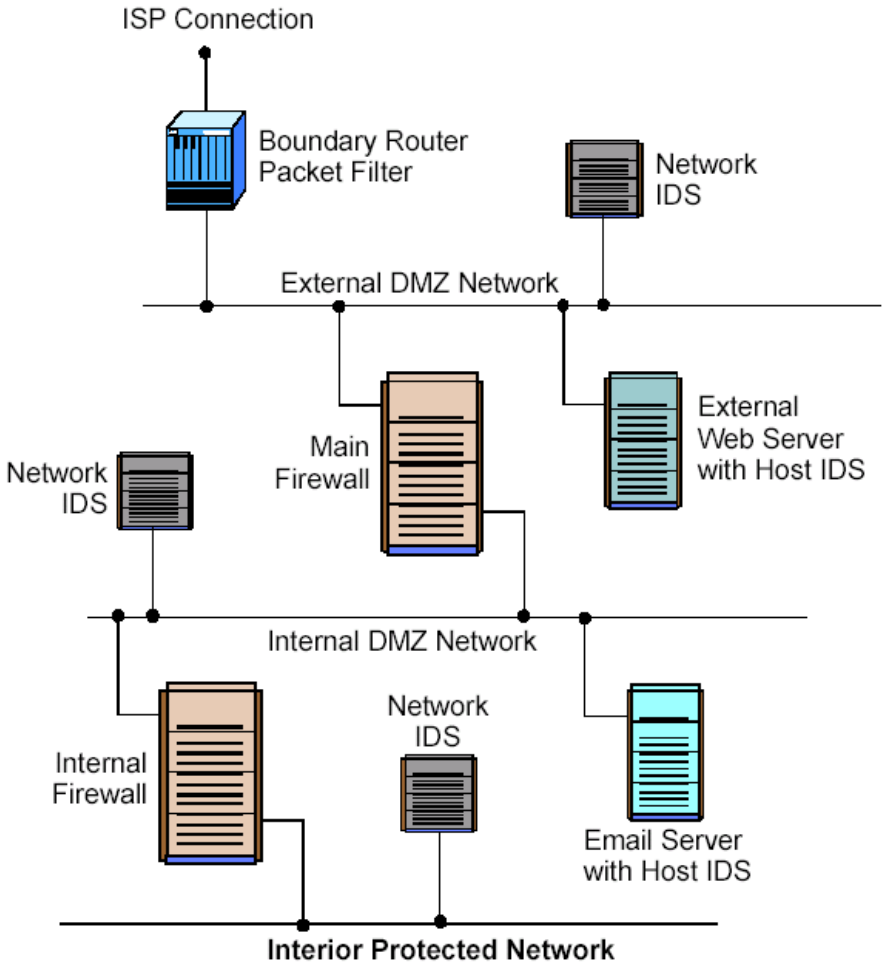
Environment 5: IDSs

- Per notificare (ed in alcuni casi prevenire) accesso a sistemi di rete
- Interazione con Firewalls per azioni reattive!!
  - Se IDS si accorge di un DoS attack, il firewall blocchera quell'accesso
- Due tipi di IDS
  - Host based
  - Network based

Environment 5: IDSs
(host IDS)

- Istallato sulle singole macchine da proteggere
- Strettamente dipendente dal OS della macchina
- Punti negativi:
  - Impatto su performance
  - Difficile riconoscere DoS
  - Impatto sulla stabilità del OS

Environment 5: IDSs
(Network based IDS)



- *Monitorano il traffico di rete cercando delle "tracce" (attack signature) che indicano un attacco in corso*
- *Più effettivo di un host-based IDS (un solo IDS monitorizza più macchine)*

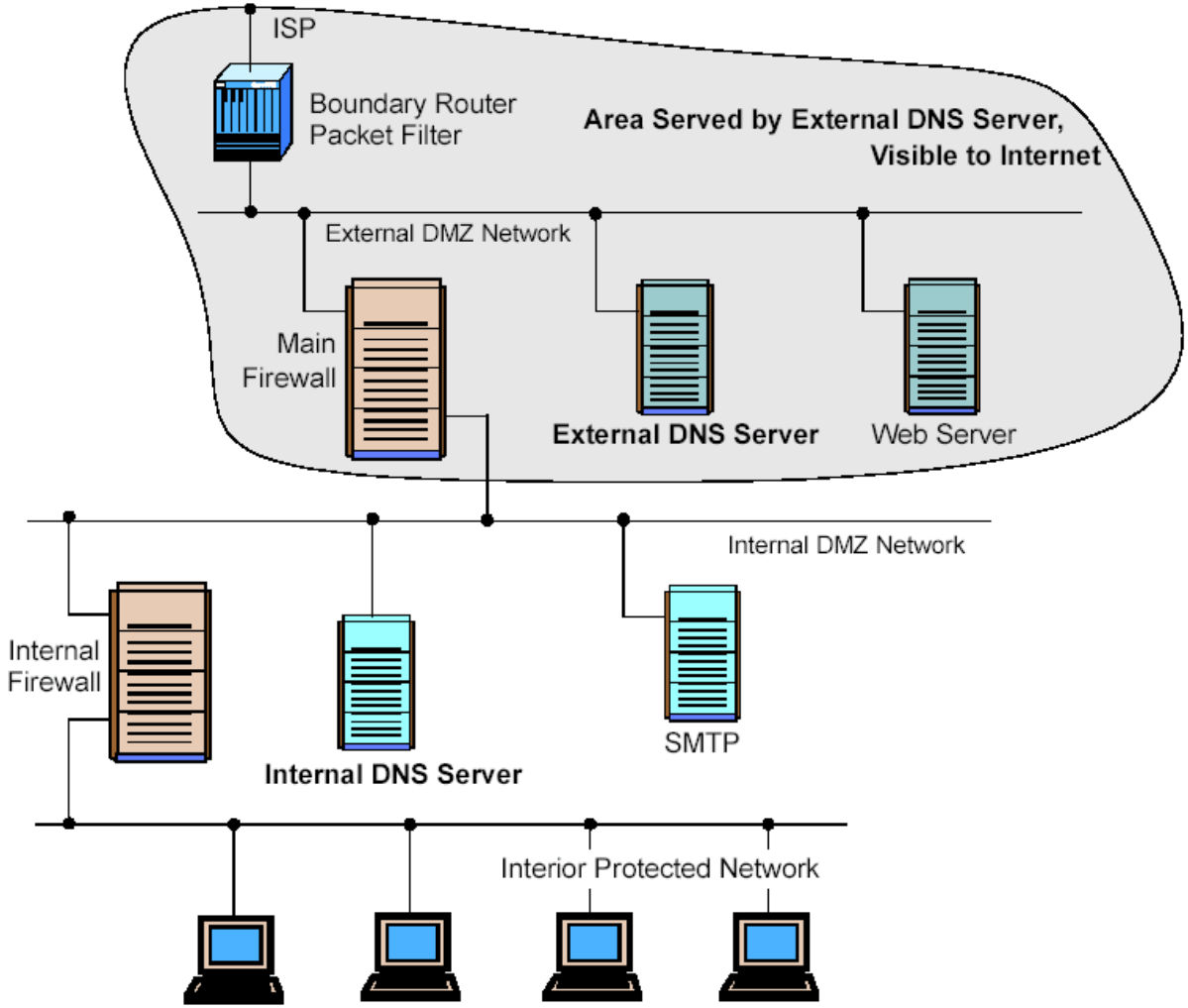
Environment 5: IDSs
(Network based IDS)

- Punti Negativi
  - Usualmente non riescono a riassemblare delle signature distribuite su più pacchetti
  - Necessitano switches con particolari funzionalità (port mirroring)
  - Interfacce in promiscuous mode (necessarie ai network-based IDSs) sono facilmente localizzabili e possono poi essere attaccate inviando grossi quantitativi di traffico inutile
  - Spesso sono essi stessi oggetto dell'attacco che dovrebbero monitorare (DoS)

Environment 6: DNSs

- Servizio critico per ogni ambiente che fa uso dell'Internet
- Split DNS
  - Separare su due server DNS la gestione dei nomi interni da quella dei nomi esterni
- Gestire traffico UDP/TCP separatamente
  - UDP: user lookup
  - TCP: Zone Transfer (solo dai secondari!)

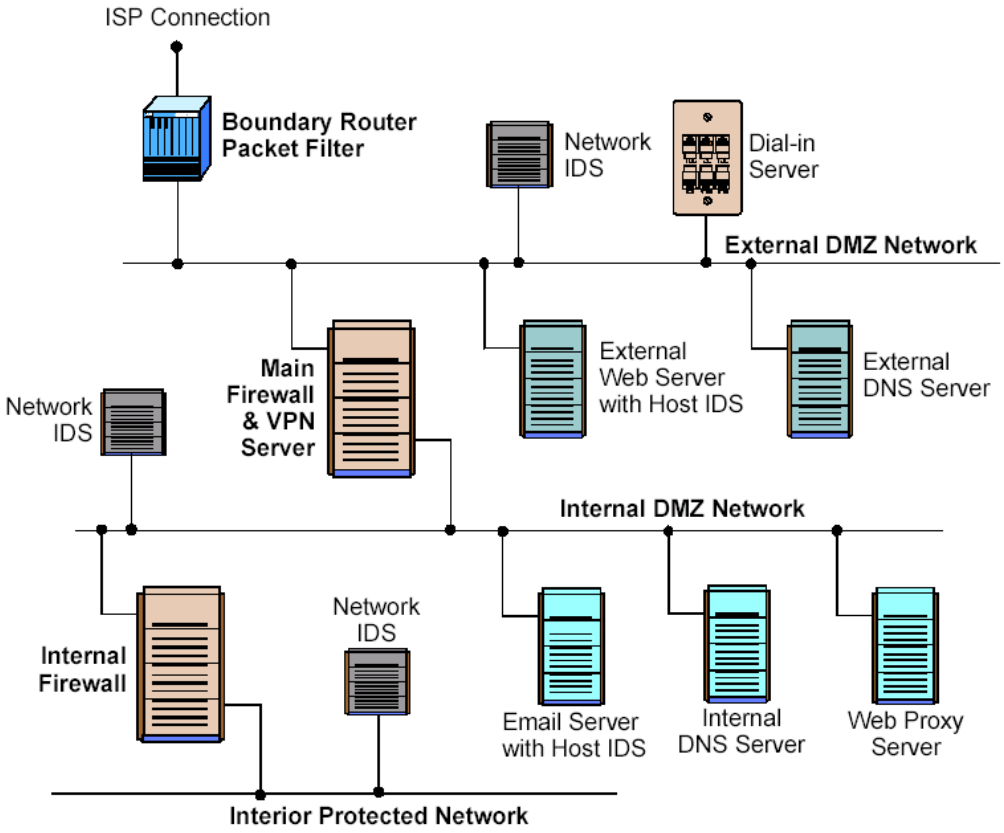
Environment 6: DNSs



Environment 7: Servers

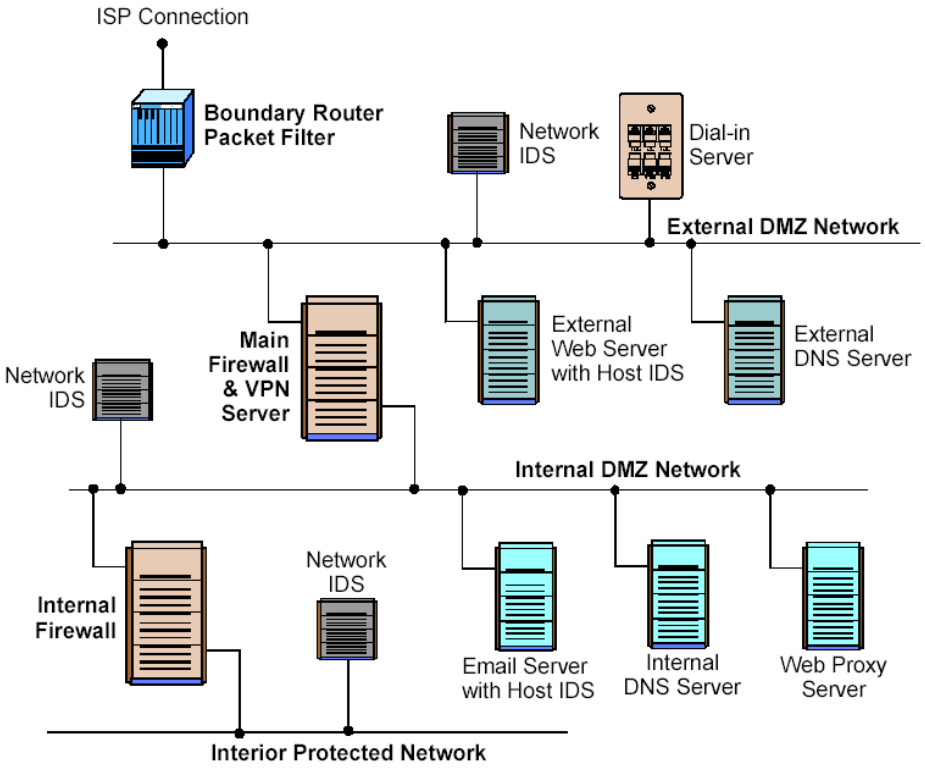
- Dove?
  - Chi deve accedervi?
  - Quanto sono importanti i dati contenuti?
- Regole generali
  - Server esterni protetti da un packet filter router
  - No server accessibili dall'esterno sulla rete interna!
  - Servers interni (al di qua del firewall interno) se importanza dati lo richiede (tante service legs?)
  - Isolare i servers (un attacco non impatta sul resto della rete)

Environment 7: Servers



- *Server esterni su external DMZ*
  - *DNS, web, directory server*
  - *Eventualmente su più DMZs per isolare i server*
  - *VPN, Dial-In server*
    - *Per controllare traffico prima che sia encrypted!*

Environment 7: Servers



- *Server interni su internal DMZ*
  - *DNS, web, directory server*
  - *Protetti anche da attacchi interni*
- *Mail servers*
  - *Se richiesto accesso dall'esterno, tramite ssl proxy sul firewall*

Firewall security policy

Firewall Policy

- Firewall policy è distinta dalla information security policy!
- Firewall policy descrive come sarà implementata la information security policy
- Detta le regole per gestire il traffico (web, email, …)
- Descrive come il firewall è gestito e aggiornato

Firewall Policy

- Risk analysis
  - Quali applicazioni?
  - Chi e da dove saranno usate?
  - Costi/benefici di ogni singola messa in sicurezza di macchina/servizio!!
  - Creare matrice traffico
  - Creare sulla base della matrice di traffico le regole da implementare sui vari firewalls!

Firewall Policy: … bloccare:

- Traffico in ingresso da sorgenti esterne non autenticate verso il firewall
  - Eccezione se proxy-email esterne (ma in questo caso accettare solo connessioni su porta 25!!)
- Traffico in ingresso … ma con pacchetti che mostrano la rete interna come sorgente ☹
- Traffico ICMP in ingresso
  - Firewalking! ☹
- Traffico SNMP da sorgenti non authenticate
  - Probing!! ☹

Firewall Policy: .. bloccare:

- Inbound/outbound traffic per pacchetti RFC1918-privati
  - 10.0.0.0 – 10.255.255.255 (classi A)
  - 172.16.0.0 - 172.16.255.255 (classi B)
  - 192.168.0.0 - 192.168.255.255 (classi C)
- Inbound/outbound traffic per pacchetti 127.0.0.1 o 0.0.0.0
  - Attacchi verso il firewall!!
- Inbound traffic contenente IP source routing informations!

Firewall Policy: .. bloccare:

- Inbound/outbound traffic per pacchetti contenenti directed broadcast address
  - Tipico uso per attacchi che implicano una risposta ad un diverso source address (DoS)
- Se possibile:
  - Usare user authentication
  - Usare quanto log possibile

Testing the policy!

- Quasi mai effettuato ☹

1. Semplice controllo tra quello che volevamo e quello che è stato implementato
2. Usando tools o specifici tiger-group che cercano di fare qualcosa vietato per policy
   - Penetration analysis
     - Seeded
     - blind

Implementazione del firewall e della policy

- Appliance-based firewalls
  - Scatole ad hoc che fanno solo questo
  - Piu' stabili e sicure dei firewall implementati on top di un OS
  - Di solito più performanti perché usano HW specifico
- OS based
  - Scalability
  - Presenza di vulnerabilità dell'OS ☹

Gestione e manutenzione del firewall

- CLI
  - Veloce ☺
  - A volte errori di battitura se non sono implementati dei controlli sintattici ☹
- GUI
  - Usabile anche da un novizio ☺
  - Usabile anche da un novizio ☹

Tipiche configurazioni

Firewall Configurations

- *In aggiunta alla semplice configurazione con un unico sistema (single packet filtering router or single gateway), sono possibili configurazioni più complicate*
- *tre tipiche configurazioni*

Firewall Configurations

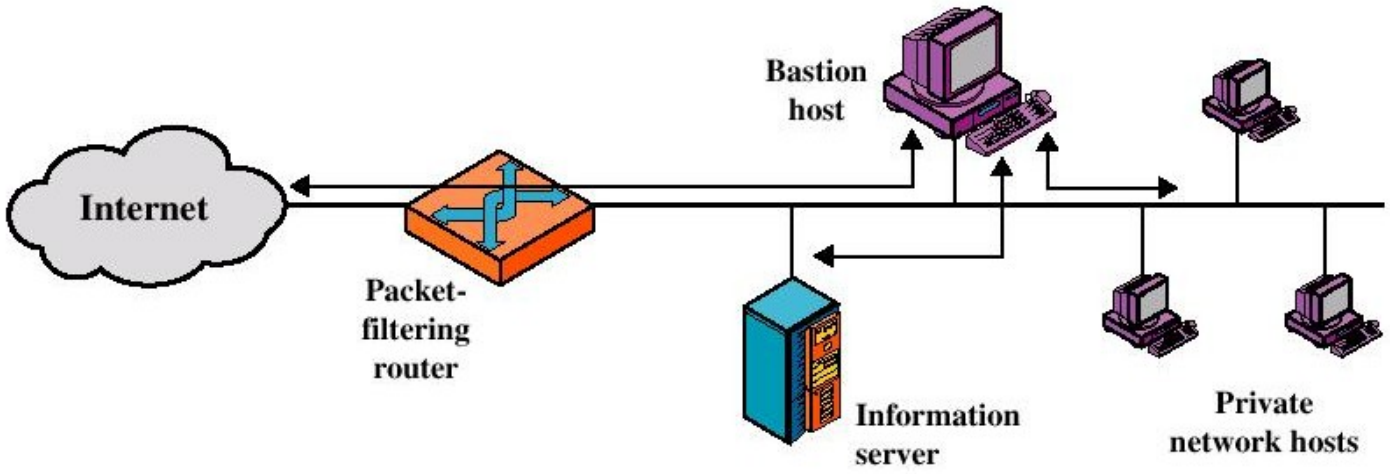
- *Screened host firewall system (single-homed bastion host)*
- *Screened host firewall system (dual-homed bastion host)*
- *Screened-subnet firewall system*

Firewall Configurations

- *Bastion Host*
  - *Un sistema identificato dal firewall administrator come un punto cruciale per la sicurezza della rete*
  - *il bastion host serve come a piattaform per un application-level o circuit-level gateway*

Firewall Configurations

- *Screened host firewall system (single-homed bastion host)*



Firewall Configurations

- Screened host firewall, single-homed bastion configuration
- Firewall considte di due sistemi:
  - un packet-filtering router
  - un bastion host

Firewall Configurations

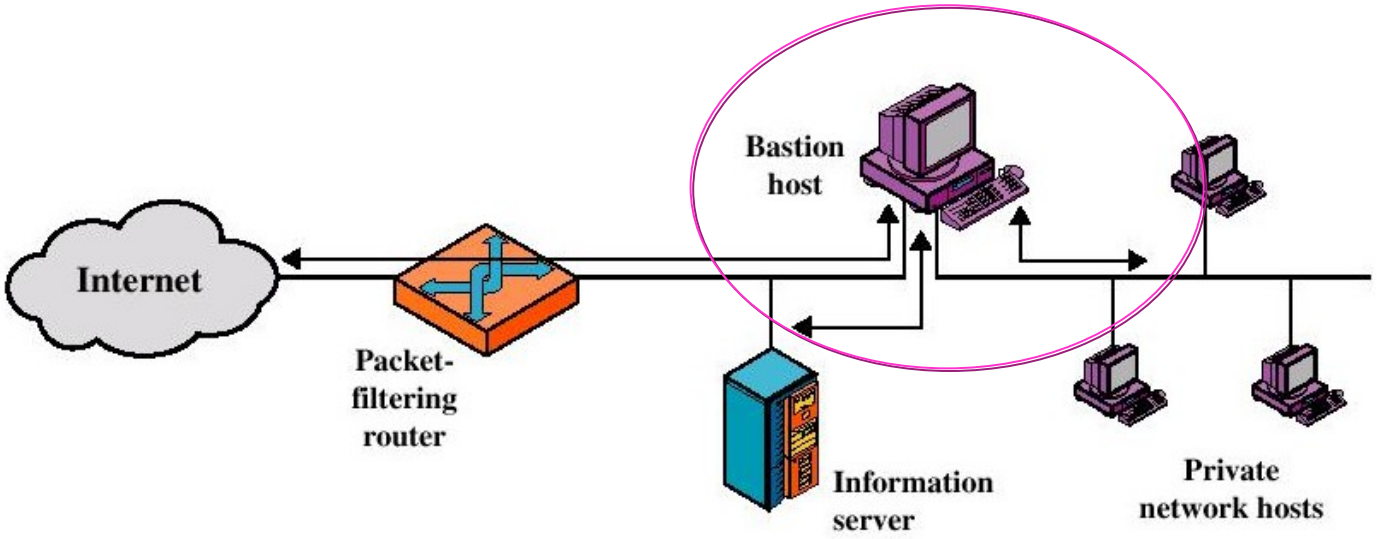
- Configurazione del packet-filtering router:
  - Solo I pacchetti da e per il bastion host sono permessi
- Il bastion host effettua funzioni di authentication and proxy (eventualmente caching)

Firewall Configurations

- *Più sicurezza di una configurazione con una sola macchina:*
  - *Implementa sia packet-level che application-level filtering (flessibilità nel definire una security policy)*
  - *Un intruder deve generalmente penetrare due sistemi separati*

Firewall Configurations

- *Screened host firewall system (dual-homed bastion host)*

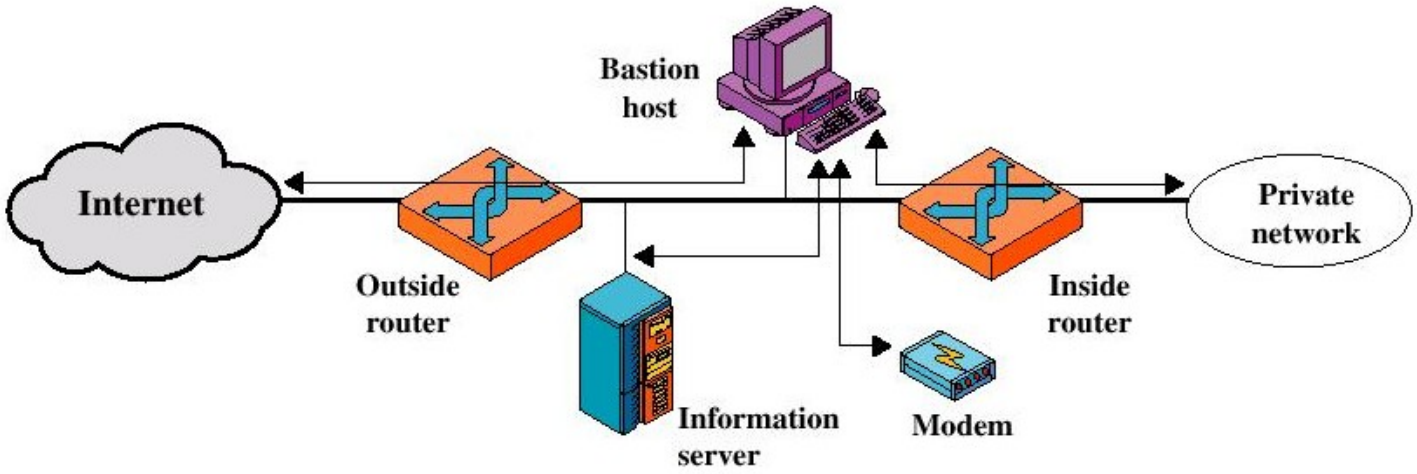


Firewall Configurations

- *Screened host firewall, dual-homed bastion configuration*
  - *Il traffico tra Internet e gli altri hosts sulla rete privata deve fisicamente passare attraverso il bastion host*

Firewall Configurations

- *Screened-subnet firewall system*



Firewall Configurations

- *Screened subnet firewall configuration*
  - *La più sicura delle tre configurazioni*
  - *Usati due packet-filtering routers*
  - *Creazione di una sub-network isolata*

Firewall Configurations

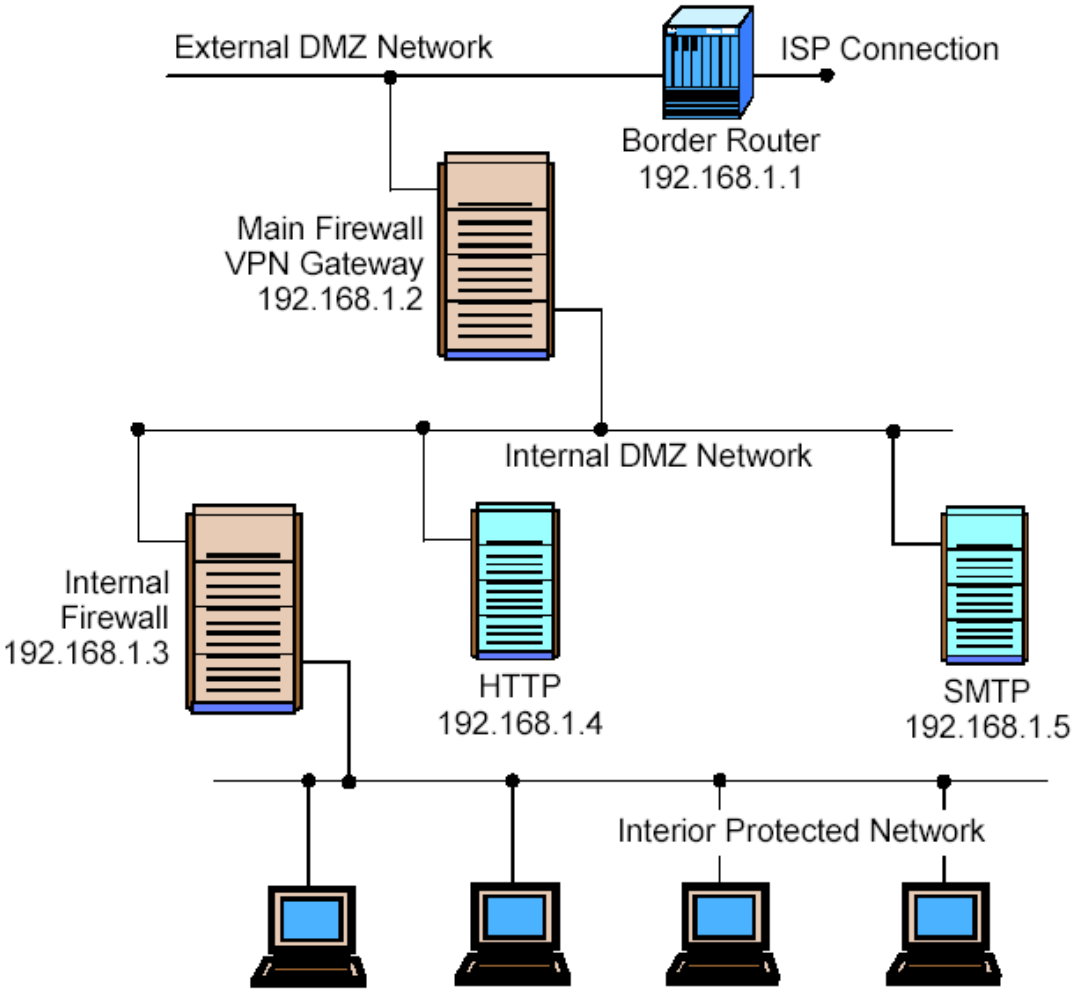
- *Vantaggi:*
  - *Tre livelli di difesa verso gli intruders*
  - *La rete interna è invisible all'Internet*
- *Svantaggi:*
  - *I systemi sulla rete interna non possono costruire cammini diretti verso l'esterno*

Un esempio

La Policy

- Tutto il traffico dall'interno è permesso
- Traffico web in uscita permesso tramite un http-proxy (magari cached and content filtered)
- Servizio SMTP in ingresso è passata ad un SMTP-proxy, e quindi ai client interni (i client interni possono ricevere email solo dal SMTP-proxy, magari dopo un controllo antivirus/antiworms)
- Traffico dall'esterno permesso sulla porta VPN del firewall (e poi passato all'interno)
- Tutto il resto è bloccato

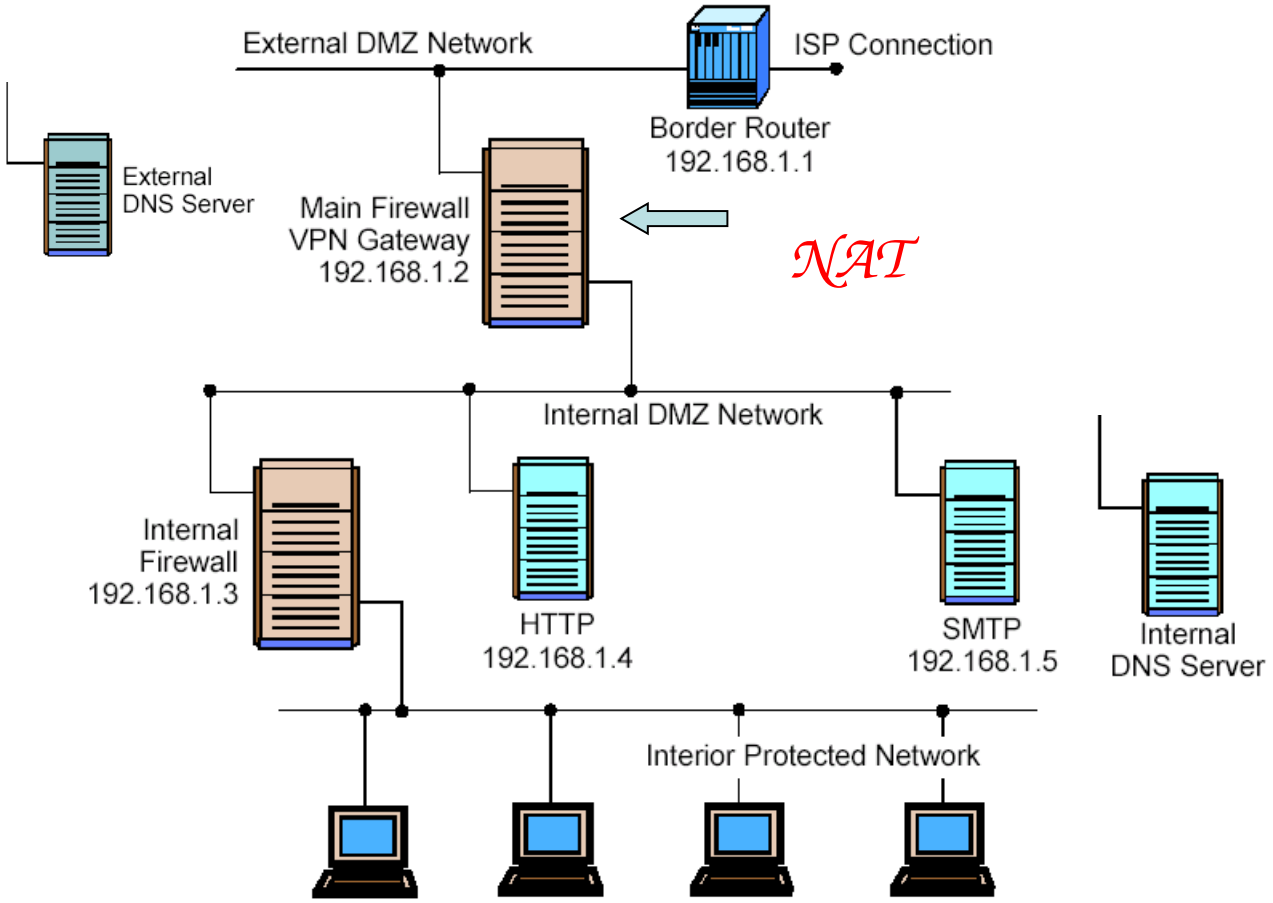
La rete


External DMZ Network
ISP Connection
Border Router
192.168.1.1
Main Firewall
VPN Gateway
192.168.1.2
Internal DMZ Network
Internal
Firewall
192.168.1.3
HTTP
192.168.1.4
SMTP
192.168.1.5
Interior Protected Network

possibili regole per il border router . . .

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3	Any	Any	192.168.1.2	VPN	Allow	Allow External users to connect to VPN server
4	Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email to proxy
5	Any	Any	192.168.1.2	HTTP	Allow	Send inbound HTTP to proxy
6	Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system.
7	192.168.1.0	Any	Any	Any	Allow	Internal Users can access External servers
8	Any	Any	Any	Any	Deny	"Catch-All" Rule - Everything not previously allowed is explicitly denied

Miglioramenti ...



Firewall Administration

Firewall Administration

- Accesso dalla console di gestione
  - Via specifici client ed encryption
  - Via SSH e http
  - Possibilmente anche una user authentication

Firewall OS

- Hardening the OS
  - Togliere protocolli, servizi e applicazioni di rete non usati
  - Togliere user/system account non usati
  - Applicare tutte le patch!!
    - Prima testarle in un ambiente di test
  - Disabilitazione interfacce non usate

Firewall Administration

- Strategie di disaster recovery
  - Swithes con capacità di Balancing/failover
    - Il tutto è trasparente
- Logging
  - Uso di un remote syslog server
    - Centralizzazionedi tutti i log
- Security incident!
  - Livelli/scala di importanza nella realtà!
  - La policy determina quali sono "gravi"
    - Mantenere logs per studi legali sull'attacco
    - Importante sincronizzazione con un time server!

Firewall Administration

- Strategie di backups
  - Day zero backup
  - No external backup!
    - Internal tape drive!
  - Copia del sistema su CD!

Raccomandazioni finali

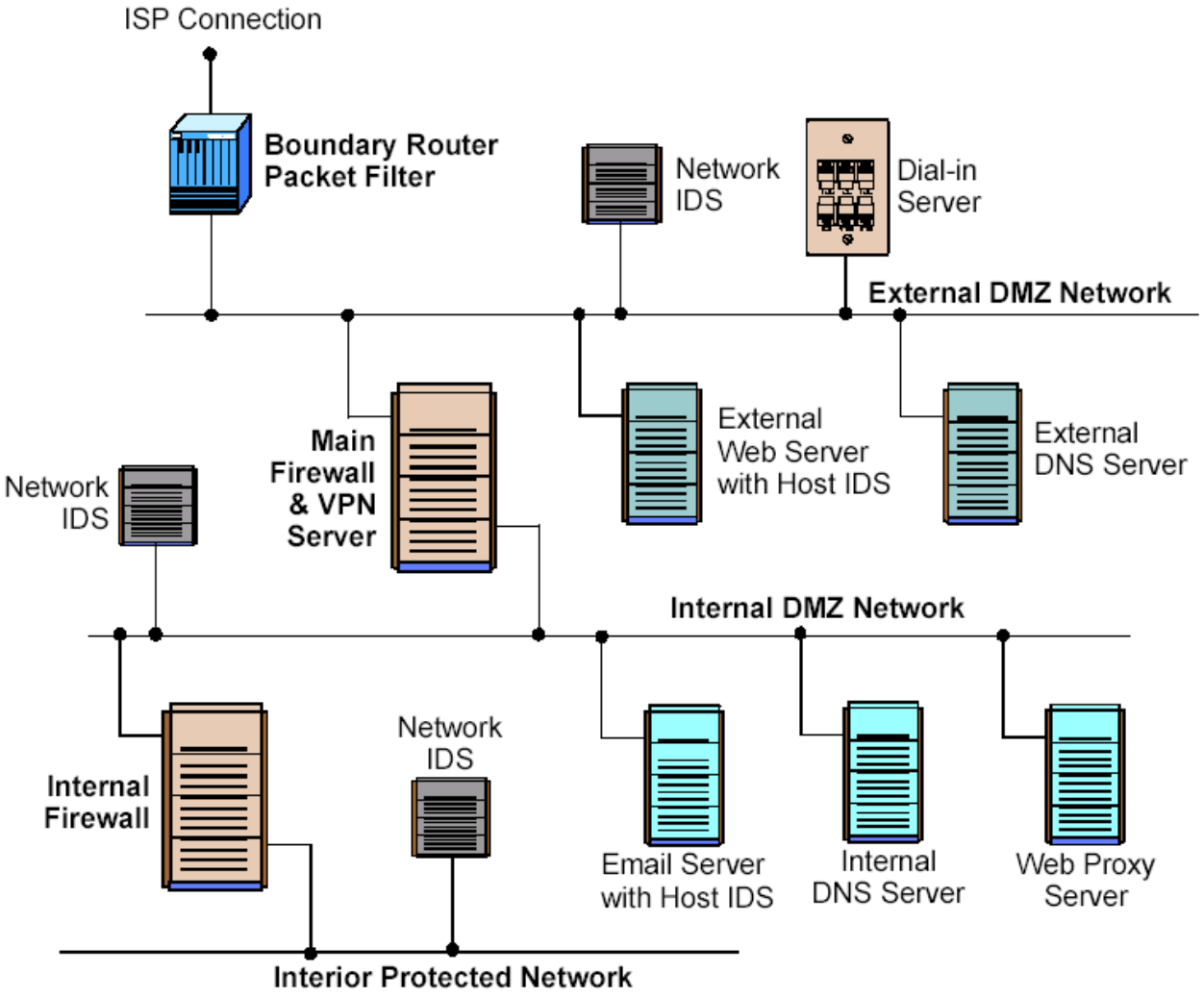
generali

- *Usare un firewall!!*
- *Su notebooks e a casa gli utenti devono usare un personal firewall*
- *Firewall: ultima linea di difesa! (gestire bene e proteggere singolarmente le macchine)*
- *Monitorare incidenti*
- *Aggiornare non appena esce una nuova patch*
- *Organizzare corsi aggiornamento periodici*

Scegliere un firewall

- Con almeno le seguenti funzioni
  - Packet filter
  - Stateful inspection
  - Proxy di selezionate applicazioni(web, posta)
  - Funzioni di log
  - Authenticazione dell'utente
  - Possibilità di controllo di
    - Interfaccia del firewall (sorgente e destinazione)
    - IP (sorgente e destinazione)
    - Porte (sorgente e destinazione)

Ricapitolando …



Ultima lezione

- *… siete stati bravissimi!!*
- *Mi avete fatto lavorare tanto …*
  - *Forse troppo!!* ☺

- *Spero che abbiate imparato tante cose*
- *.. E che vi ricorderete che l'avete imparate in questo corso!!* ☺*…*