

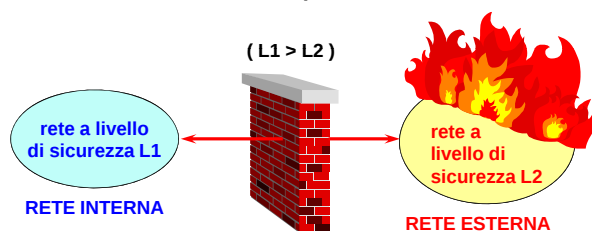
Firewall e IDS/IPS

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

Che cos'è un firewall?

- firewall = muro tagliafuoco
- collegamento controllato tra reti a diverso livello di sicurezza = sicurezza del perimetro



Ingress vs. Egress firewall

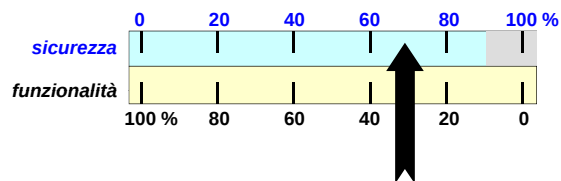
- **ingress firewall**
 - collegamenti incoming
 - tipicamente verso servizi offerti all'esterno
 - talvolta come parte di una comunicazione attivata dall'interno
- **egress firewall**
 - collegamenti outgoing
 - controllo dell'attività del personale
- **distinzione facile per servizi orientati al canale (es. applicazioni TCP), difficile per servizi basati su datagrammi (es. ICMP, applicazioni UDP)**

Progettazione di un firewall

Un firewall non si “compra”, si progetta
(si comprano i suoi componenti)

- si tratta di trovare il compromesso ottimale ...
- ... tra sicurezza e funzionalità
- ... col minimo costo

L'indice della sicurezza



I TRE PRINCIPI INDEROGABILI DEI FIREWALL

- I. il FW deve essere l'unico punto di contatto della rete interna con quella esterna
- II. solo il traffico “autorizzato” può attraversare il FW
- III. il FW deve essere un sistema altamente sicuro esso stesso

*D.Cheswick
S.Bellovin*

Politiche di autorizzazione

“Tutto ciò che non è espressamente permesso, è vietato”

- maggior sicurezza
- più difficile da gestire

“Tutto ciò che non è espressamente vietato, è permesso”

- minor sicurezza (porte aperte)
- più facile da gestire

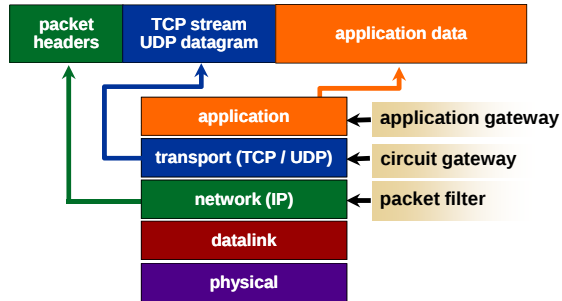
Considerazioni generali

- gli oggetti grossi sono più difficili da verificare
- se un processo non è stato attivato, i suoi banchi non ci riguardano
- “grande NON è bello” = configurazione minima
- un FW non è una macchina general-purpose (minimo del sw, no utenti)
- ognuno è colpevole finché non si dimostra innocente

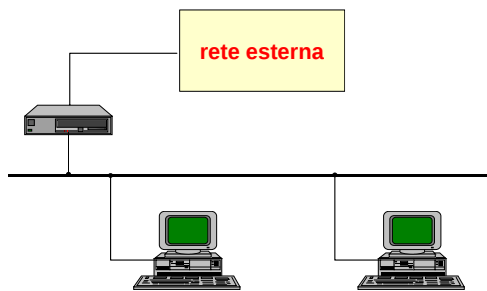
FW: elementi di base

- **screening router (choke)**
router che filtra il traffico a livello IP
- **bastion host**
sistema sicuro, con auditing
- **application gateway (proxy)**
servizio che svolge il lavoro per conto di un applicativo, con controllo di accesso
- **dual-homed gateway**
sistema con due connessioni di rete e routing disabilitato

A quale livello si fanno i controlli?

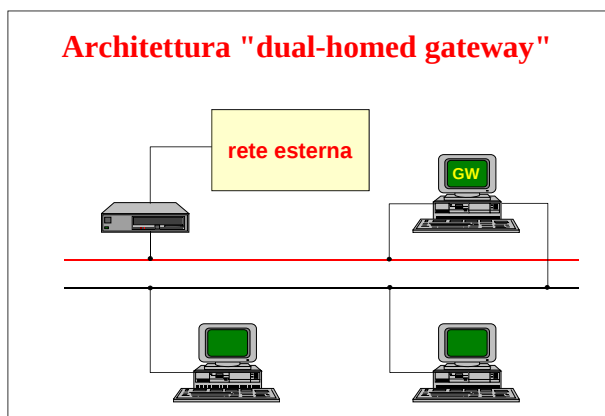


Architettura "screening router"



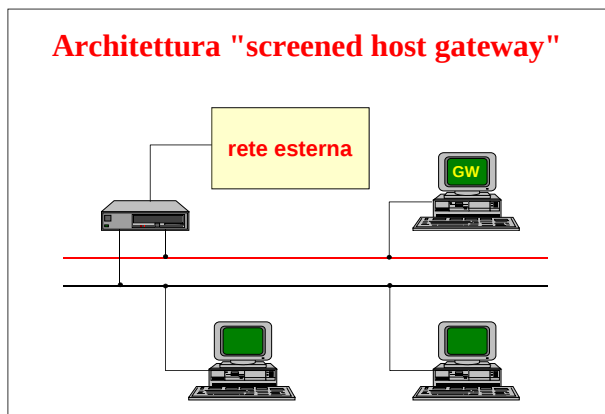
Architettura "screening router"

- usa il router per filtrare il traffico sia a livello IP che superiore
- non richiede hardware dedicato
- non necessita di proxy e quindi di modifiche agli applicativi
- facile, economico e ... insicuro!

Architettura "dual-homed gateway"

Architettura "dual-homed gateway"

- facile da realizzare
- richiede poco hardware
- possibile mascherare la rete interna
- scarsamente flessibile
- grosso sovraccarico di lavoro

Architettura "screened host gateway"

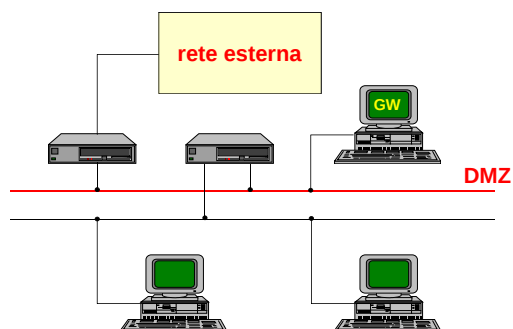
Architettura "screened host gateway"

- **router:**
 - blocca i pacchetti da INT a EXT a meno che arrivino dal bastion host
 - blocca i pacchetti da EXT a INT a meno che siano destinati al bastion host
 - eccezione: protocolli abilitati direttamente
- **bastion host:**
 - circuit/application level gateway per abilitare selettivamente dei servizi

Architettura "screened host gateway"

- più caro da realizzare
- più flessibilità
- complicato da gestire: due sistemi invece di uno
- si può selettivamente allentare il controllo su certi servizi / host
- si possono mascherare solo gli host/protocolli che passano dal bastion (a meno che il router abbia funzionalità NAT)

Architettura "screened subnet"

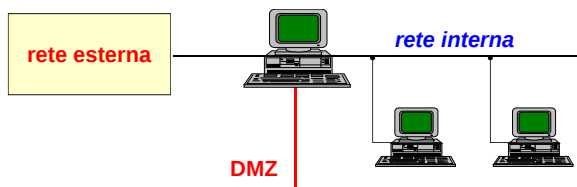


Architettura "screened subnet"

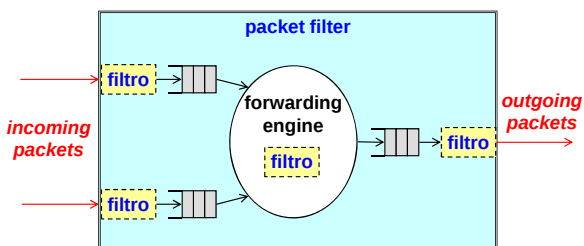
- DMZ (De-Militarized Zone)
- sulla DMZ - oltre al gateway - ci possono essere più host (tipicamente i server pubblici):
 - Web
 - accesso remoto
 - ...
- si può configurare il routing in modo che la rete interna sia sconosciuta
- soluzione costosa

Architettura "screened subnet" (versione 2)

- per motivi di costo e di semplicità di gestione spesso si omettono i router (e le loro funzioni sono incorporate nel gateway)
- anche noto come "firewall a tre gambe"



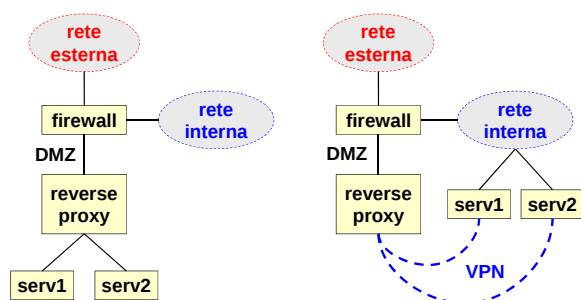
Punti di filtraggio



Reverse proxy

- un server HTTP che fa solo da front-end e poi passa le richieste al vero server
- benefici:
 - obfuscation (non dichiara il vero tipo di server)
 - load balancer
 - acceleratore SSL (con back-end non protetto ...)
 - web accelerator (=cache di contenuti statici)
 - compressione
 - spoon feeding (riceve dal server tutta una pagina creata dinamicamente e la serve poco per volta al client, scaricando così il server applicativo)

Configurazioni di reverse proxy



Architetture di firewall: quale scegliere? (1)

- in teoria, più alto il livello a cui il firewall opera:
 - più alto sarà il consumo di cicli macchina
 - più alto sarà il livello di protezione che offre
- la realtà:

Firewall customers once had a vote, and voted in favor of transparency, performance and convenience instead of security; nobody should be surprised by the results.
(Marcus J. Ranum, the "grandfather of firewalls", firewall wizard mailing list, oct 2000)

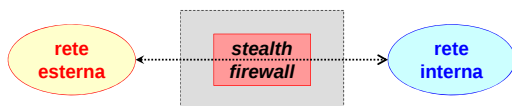
Architetture di firewall: quale scegliere? (2)

■ la scelta migliore:

- non un singolo prodotto, ma un'architettura di firewall robusta che supplisca alle carenze e eventuali vulnerabilità dei singoli dispositivi!!!
- per il singolo elemento richiedere se possibile il supporto ad architetture multiple: meglio poter scegliere che lasciar scegliere ad un vendor!!
- attenzione alle soluzioni che promettono di risolvere ogni vostro problema: forse si tratta di pubblicità ...

Stealth firewall

- firewall privo di un indirizzo di rete, così da non essere attaccabile direttamente
- intercetta i pacchetti fisicamente, mettendo la propria interfaccia di rete in modo promiscuo



Gestione di un firewall

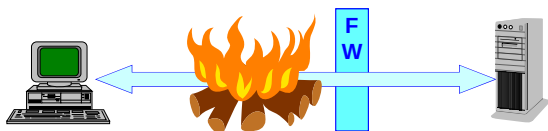
- manuale con politica di sicurezza della rete:
 - regola n. X
 - funzione richiesta
 - durata temporale della regola
 - richiedente e implementatore
 - regola/e del firewall n. Y
- controllo (semi-)automatico periodico della corrispondenza tra politica e regole implementate dal firewall:
 - dump + diff

Local / personal firewall

- firewall installato direttamente sul nodo da difendere
- tipicamente un packet filter
- rispetto ad un normale firewall in rete può controllare i programmi a cui è permesso:
 - aprire collegamenti in rete verso altri nodi (ossia agire come client)
 - ricevere richieste di collegamento / servizio (ossia agire da server)
- importante per limitare la diffusione di malware o trojan, o semplici errori di installazione
- gestione firewall distinta da gestione sistemistica

Protezione offerta da un firewall

- i firewall sono efficaci al 100% solo relativamente agli attacchi sui canali che sono bloccati
- per gli altri canali occorrono altre difese:
 - VPN
 - firewall "semantici" / IDS
 - sicurezza applicativa



Intrusion Detection System (IDS)

- definizione:
 - sistema per identificare individui che usano un computer o una rete senza autorizzazione
 - esteso anche all'identificazione di utenti autorizzati, ma che violano i loro privilegi
- ipotesi:
 - il "pattern" di comportamento degli utenti non autorizzati si differenzia da quello degli utenti autorizzati

IDS: caratteristiche funzionali

- **IDS passivi:**
 - uso di checksum crittografiche (es. tripwire)
 - riconoscimento di pattern ("attack signature")
- **IDS attivi:**
 - "learning" = analisi statistica del funzionamento del sistema
 - "monitoring" = analisi attiva di traffico dati, sequenze, azioni
 - "reaction" = confronto con parametri statistici (reazione scatta al superamento di una soglia)

IDS: caratteristiche topologiche

- **HIDS (host-based IDS)**
 - analisi dei log (del S.O. o delle applicazioni)
 - attivazione di strumenti di monitoraggio interni al S.O.
- **NIDS (network-based IDS)**
 - attivazione di strumenti di monitoraggio del traffico di rete

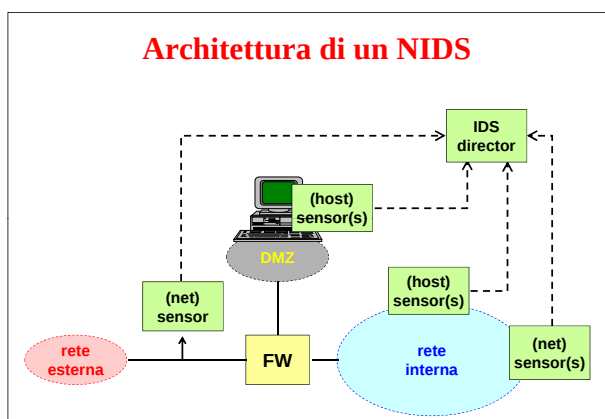
SIV e LFM

- **System Integrity Verifier**
 - controlla i file / filesystem di un nodo per rilevarne cambiamenti
 - es. rileva modifiche ai registri di Windows o alla configurazione di cron, cambio privilegi di un utente
 - es. tripwire
- **Log File Monitor**
 - controlla i file di log (S.O. e applicazioni)
 - rileva pattern conosciuti derivanti da attacchi o da tentativi di attacco
 - es. swatch

Componenti di un NIDS

- **sensor**
 - controlla traffico e log individuando pattern sospetti
 - attiva i security event rilevanti
 - interagisce con il sistema (ACLs, TCP reset, ...)
- **director**
 - coordina i sensor
 - gestisce il security database
- **IDS message system**
 - consente la comunicazione sicura ed affidabile tra i componenti dell'IDS

Architettura di un NIDS



IPS

- **Intrusion Prevention System**
- per velocizzare ed automatizzare la risposta alle intrusioni = IDS + firewall dinamico distribuito
- non un prodotto ma una tecnologia, con grosso impatto su tanti elementi del sistema di protezione
- pericolo di prendere la decisione sbagliata o di bloccare traffico innocuo

