13 - Firewalls

La sicurezza su internet si basa su:

- crittografia:
  - IPSec
  - SSL
- exo strutture
  - firewall
  - VPN

Un firewall è la combinazione di software e hardware per regolare il traffico tra un ***internal network*** e un ***external network***
tecnologie

- packet sniffing
- stateful packet inspection
- application proxy
- network address translation
- VPN

Packet filtering

Implementato tramite uno screening router
- router: come indirizzare un pacchetto alla destinazione
- screening router: verificare se il pacchetto dovrebbe arrivare a destinazione
Applica un set di regole di filtraggio per il traffico in inbound e outbound e poi decide se scartarli o farli passare.
Filtri basati sulle informazioni nell' IP packet header:

- IP source address
- IP destination address
- Protocol type (TCP, UDP, ICMP)
- Source transport level address (numero della porta)
- destination transport level address (porta)
- packet size
  Informazioni aggiuntive:
- interfaccia in cui i pacchetti arrivano
- interfaccia in cui i pacchetti escono

Stateful packet inspection

Lo screening router può basare le decisioni di forwarding sullo state information che viene collegato e salvato durante le operazioni
Esempi:

- il pacchetto è la risposta ad un altro pacchetto?
- il numero di pacchetti visti dall'host supera un limite?
- il pacchetto è identico ad un già visto recentemente?
- è un frammento?

Vantaggi:

- uno screening router protegge l'intera rete
- molto efficiente
- molto disponibile
  Svantaggi:
- difficile da configurare
- riduce le performance del router
- visto che non può esaminare i dati di livello superiore le policy implementabili sono ridotte
- sono vulnerabili ad attacchi che si avvantaggiano dei problemi con TCP/IP come network layer address spoofing

Application proxy Firewall

Chiamato anche **application-level gateway**
Applicazioni specializzate per i servizi internet (HTTP, FTP, telnet, etc.)
Proxy client e proxy server
Necessita di un meccanismo per restringere le comunicazioni dirette tra reti interne ed esterne.
Combinato con cache per performance maggiori.
Effettivo solo se usato in congiunzione con meccanismi che restringono le comunicazioni dirette tra host interni ed esterni.

Vantaggi:

- Può eseguire autenticazioni livello utente
- può fare filtri intelligenti
- può essere combinato con caching
- ha un bun sistema di logging
  Svantaggi
- richiede server differenti per ogni servizio
- richiede modifiche ai clienti

Network address translation

Da la possibilità ad una rete di usare un set di indirizzi interno e un set differente esterno.
Inventato non per sicurezza ma per conservare l'IP address
implementato tipicamente da un router
Gli host dentro al dominio con NAT hanno assegnato un indirizzo privato che è unico localmente ma non globalmente

Vantaggi:

- Impone il controllo del firewall sul traffico in uscita
- restringe il traffico in ingresso (nessuna connessione spontanea)
- nasconde dettagli sulla sicurezza della rete interna
  Svantaggi:
- interferisce con alcune tecniche basate su crittografia
- Associazione dinamica degli indirizzi interferisce con i log
- Reti interne non possono hostare servizi visibili esternamente (port forwarding)

Architettura del firewall

- Host based e personale
- screening router
- dual-homed host
- screened host
- screened subnet

Host-based Firewalls

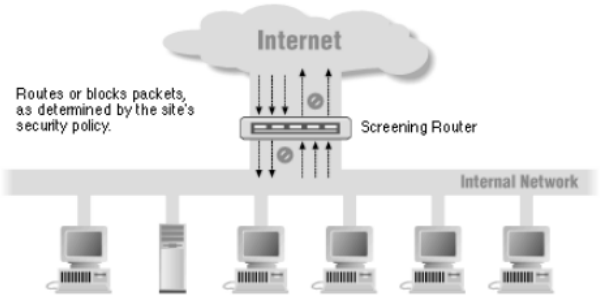
Rende sicuro un singolo host

- Disponibile in diversi OS
- comunemente usato per proteggere i server
  Vantaggi:
- molto perzonalizzabile
- topologia indipendente, tutti gli attacchi (interni ed esterni) devono passare attraverso il firewall
- Estensibile, nuovi server possono essere aggiunti alla rete con il proprio firewall senza il bisogno di modificare la rete

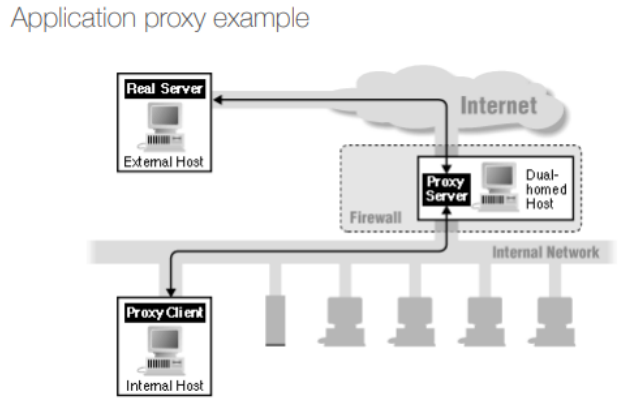
Personal firewalls

Controllano il traffico tra un pc e la rete

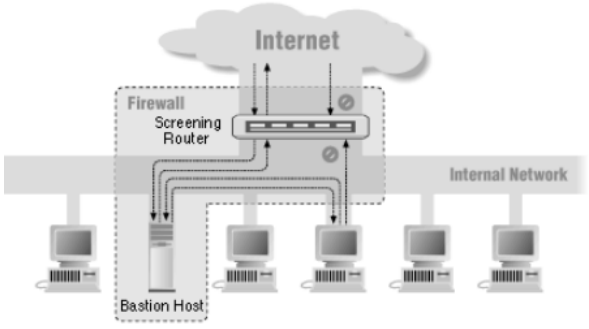
Screening router



Dual-Homed host



Screened host



Bastion host

Un computer in una rete disegnata e configurata specificatamente per resistere agli attacchi
Garantisce esposizione agli attacchi
Tutto il traffico incrocia il bastion host, che può bloccarlo o farlo passare
Normalmente esegue solo poche applicazioni, normalmente proxy

Regole basi da impostare

- nessun altro host può essere raggiunto dall'esterno
- OS fidati
- nessun software non necessario
- read only file system (tranne permessi molto stretti di lettura)
- solo servizi strettamente richiesti
- nessun account utente
- meccanismi di autenticazione aggiuntivi
- molti log

Screened subnet

Router esterno

- protegge le DMZ e reti interne dall'internet

- abilita i traffico in entrata solo per i servizi bastion/host
  Router interno
- protegge la rete interna dalla DMZ e internet
- esegue la maggior parte dei packet filtering
- permette solo sevizi selezionati dalla rete interna
- limita i servizi tra bastion host e la rete interna