VPN RETI PRIVATE VIRTUALI:
ACCESSO REMOTO

Fondazione dell'Ordine degli Ingegneri della Provincia di Milano

Commissione per l'Ingegneria dell'Informazione

ing. Gianluca Sironi

FIREWALL:
LA PROTEZIONE PER GLI ACCESSI ESTERNI

GNU Free Documentation License

Via Stradella, 7 – 20129 Milano MI

gianluca.sironi @ gmail.com

agenda

- definizione e compiti di firewall
- tipologie a categorie di firewall
- funzionalità di sicurezza

perchè un firewall? / 1

quando si è connessi in rete (ad es. connessi ad internet) si fanno una serie di attività note:

- inviare e ricevere email
- navigare su siti web
- scaricare file
- utilizzare le chat

perchè un firewall? / 2

mentre si è connessi ad internet vi sono però una serie di attività “meno note”:

- Windows controlla sul sito di Microsoft se vi sono aggiornamenti per la sicurezza, ...
- software antivirus controllano se vi sono update
- applicazioni controllano se vi sono nuove versioni
- spyware che inviano dati
- worm che si propagano, ...

firewall

un firewall (*) è un dispositivo hardware o software in funzione in un ambiente di rete (ad es. internet) che ha lo scopo di controllare il traffico (permettere o negare particolari tipologie di traffico o canali di comunicazione) così come viene definito nelle politiche di sicurezza (security policy)

(*) il nome “firewall” è stato utilizzato per analogia con le pareti tagliafuoco del mondo delle costruzioni

compiti di un firewall

compito base di un firewall è filtrare il traffico in ingresso o in uscita tra "zone" a differente livello di fiducia (trust)

le tipologie di traffico sono tipicamente:
invio email (SMTP), ricezione email (POP/IMAP), navigazione siti web (HTTP), instant messaging, download o upload di file (FTP, P2P, ...), connessioni a Terminal Server ...

la zona internet è considerata "no trust";
una LAN (Local Area Network) o una zona intranet sono considerate tipicamente "very high trust"

suddivisione firewall in categorie

i firewall si possono suddividere in diverse categorie in base a caratteristiche quali:

- posizione (sul pc o su un dispositivo di rete)
- tipologia (software o hardware)
- livello di comunicazione filtrato (network layer, application layer, ...)
- funzionalità (NAT, VPN, proxy, ...)

posizione firewall / 1

Una suddivisione può essere fatta in base a dove è installato il firewall (sul pc o su un altro dispositivo):

- personal firewall
  una applicazione software installata
  su un singolo PC connesso ad internet

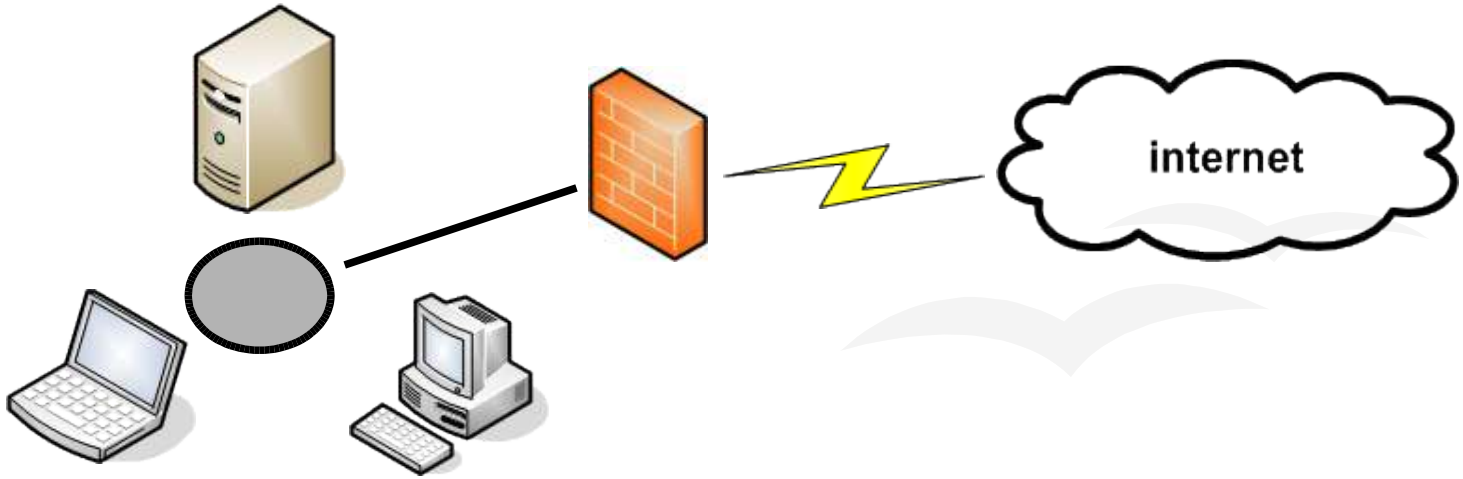
- network firewall:
  un dispositivo hardware, o una applicazione software installata su un apparato hardware dedicato, posizionato al confine tra due "zone"
  (tipico esempio fra una intranet ed internet)

posizione firewall / 2

Una suddivisione può essere fatta in base a dove è installato il firewall (sul pc o su un altro dispositivo):

- personal firewall

- network firewall



firewall software o hardware

I firewall si possono suddividere:

- applicazione software direttamente sul client:
  ad es. ZoneAlarm, CA, Symantec (Norton),
  McAfee, F-Secure, Tiny, ...

- applicazione software su un gateway
  (un server di connessione ad internet):
  ad es. Microsoft ISA, CheckPoint Firewall-1,
  SmoothWall, IPTables, IPCop, ...

- dispositivo hardware (appliance)
  (apparato dedicato con funzioni di firewall):
  ad es. dispositivi di Netgear, D-Link, Linksys,
  Zyxel, ... e di Cisco, Juniper, ...

packet inspection

Una suddivisione dei firewall può essere fatta in base alle funzionalità di controllo del traffico (in particolare l'ispezione dei pacchetti):

- packet filtering (stateless packet inspection)
  analizza il pacchetto

- statefull packet inspection (SPI)
  fa il monitor della connessione (e ne tiene traccia in una "state table")

Quasi tutti i firewall, anche router entry-level (per ambienti SOHO) hanno funzionalità di SPI

NAT

Una funzione presente nei network firewall
è il NAT (noto anche come IP-masquerading)

Attraverso il NAT (Network Address Translation)
il firewall “trasla” gli indirizzi IP privati dei client
e li rende non visibili dall'esterno (quindi non raggiungibili da port scanner, da accessi remoti non autorizzati, ...)

Quando ci si connette direttamente ad internet (con un modem) si è invece direttamente visibili (esposti):
l'interfaccia (del modem) ha un indirizzo IP pubblico

VPN e OpenVPN

Come VPN (Virtual Private Network) server si possono utilizzare prodotti proprietari come RRAS (una componente dei server Microsoft Windows)
o prodoti Open Source come OpenVPN

OpenVPN è un prodotto disponibile per molte piattaforme (Windows, Linux, Mac OS X, UNIX, ...)
Oltre a server VPN fornisce anche altre funzionalità di firewall come SPI (statefull packet inspection), ...

proxy firewall

A livello applicativo si possono avere funzioni di firewall attraverso l'utilizzo di proxy (application proxy)

Un proxy è un dispositivo che esegue un compito per qualcun altro; in genere lavora a livello applicativo: ad es. un proxy viene utilizzato per la navigazione web e si interpone tra client e server finale

su un proxy possono essere implementati controlli (in questo senso svolge compiti di tipo firewall) ma svolge anche funzione di caching e controllo conformità e l'esattezza dei pacchetti applicativi

vi sono molti proxy tra cui Microsoft ISA, Squid, ...

riferimenti

- SmoothWall
  http://www.smoothwall.org
- Squid
  http://www.squid-cache.org
- RFC 1631, The IP Network Address Translator (NAT)
  http://www.ietf.org/rfc/rfc1631.txt
- Firewalling and Proxy Server HOWTO
  http://www.linux.org/docs/ldp/howto/Firewall-HOWTO.html