FIREWALL E ROUTER

Vers. 1.2 del 20/12/2005

Premessa.

Questo documento contiene alcune raccomandazioni che l'Amministratore di Sistema dovrebbe tenere presente al momento della progettazione e configurazione di protezioni perimetrali, riguardanti cioè il punto di collegamento della LAN con la rete Internet.

Con il termine *firewall* si intende qualunque apparato o sistema (hardware e software) posto fra due reti, o all'interno di una rete, che svolge operazioni di filtraggio dei pacchetti che lo attraversano.

Oggi, molti dei firewall in commercio forniscono diversi servizi, anche piuttosto sofisticati, fra i quali software antivirus, sistemi anti-intrusione, server VPN, DHCP o NAT, software di analisi dei log, funzioni di traffic shaping e di controllo del contenuto dei pacchetti.
In questo documento ci si soffermerà soltanto sui sistemi di difesa perimetrali costituiti dai router di accesso ai PoP della rete GARR (border router) o da macchine dedicate e inserite subito dopo il router, in modo da analizzare i pacchetti IP provenienti dal router stesso.

La configurazione minima raccomandata è costituita da un router con capacità di controllo degli accessi tramite ACL. Per l'utilizzo di sistemi più complessi all'interno delle Unità Operative si veda il documento [3].

Breve descrizione

Il tipo base (fondamentale) di firewall è il "packet filter". Si tratta essenzialmente di un router dotato di funzionalità di controllo degli accessi tramite l'analisi di svariate informazioni contenute nei pacchetti (operando principalmente a livello 3, ma anche a livello 2 e 4 [1]):

- indirizzo IP sorgente
- indirizzo IP di destinazione
- tipo di traffico (protocollo utilizzato)
- caratteristiche delle sessioni, in particolare *porte* sorgente o destinazione (funzionalità di livello 4)
- MAC-address (funzionalità di Layer 2)

Il filtraggio dei pacchetti avviene attraverso una sequenza di regole (ACL, Access Control List). Per ogni pacchetto il firewall cerca in maniera sequenziale attraverso la lista se esista una regola specifica riguarda quel pacchetto; alla prima occorrenza l'analisi si interrompe e il firewall esegue l'operazione indicata dalla regola e che può essere:

- Accept
- Deny
- Discard

Il filtraggio può avvenire naturalmente sia sui pacchetti in ingresso che in uscita dalla LAN.

Due diversi punti di vista

La configurazione del firewall può seguire due diverse scuole, che l'Amministratore deve scegliere in base alle esigenze locali:

- può chiudere completamente l'accesso alla LAN, aprendo (permettendo) l'accesso soltanto verso macchine che forniscono servizi noti e registrati presso il Servizio, e tramite protocolli e porte ben note
- può chiudere soltanto gli accessi considerati pericolosi, lasciando aperto l'accesso a tutti gli altri host; in ogni caso, si raccomanda di chiudere e monitorare i tentativi di accesso via TCP e UDP verso:
    - le porte 0-1023, lasciando aperto l'accesso verso macchine che forniscono servizi o che sono appositamente registrate al Servizio
    - le porte utilizzate per exploit ben noti [App. B]
    - l'accesso verso macchine non aggiornate o non mantenute in sicurezza per motivi operativi.

La scelta fra i due approcci, o un approccio intermedio, spetta all'Amministratore locale, in base principalmente a:

- la sua capacità e disponibilità ad aggiornare velocemente in caso di necessità le ACL
- le esigenze di sicurezza della propria LAN
- lo stato di aggiornamento dei sistemi presenti sulla LAN

Nella configurazione delle ACL è consigliato rispettare le seguenti indicazioni:

- quando viene creato un filtro eliminare i filtri precedenti
- impostare il logging per ogni pacchetto rifiutato o bloccato
- proteggere la LAN dalla falsificazione di indirizzi IP (spoofing):
    - bloccare in ingresso:
        - localhost (127.x.x.x)
        - network riservate (10.x.x.x, 172.[16-31].x.x, 192.168.x.x)
        - indirizzi multicast ([224-239].x.x.x)
        - indirizzi della propria LAN
    - bloccare in uscita tutti i pacchetti che contengono un indirizzo IP esterno nel campo indirizzo IP di origine
- bloccare i pacchetti con indirizzo IP e porta di origine identici a indirizzo IP e porta destinazione (tipici di attacchi "Land attack" di DoS)
- proteggere l'apparato da attacchi TCP SYN
- proteggere la LAN da traffico ICMP inutile, sia in ingresso che in uscita, selezionando il tipo di messaggio ICMP che si considera legittimo
- proteggere la LAN da *traceroute* in ingresso

Si raccomanda inoltre di creare, salvare e mantenere i file di configurazione del router o firewall su un computer offline in formato ASCII.

Modalità di accesso per l'amministratore

L'accesso al router per gestione e configurazione dovrebbe, nei limiti del possibile, seguire le misure di sicurezza previste per le macchine che forniscono servizi

centralizzari, utilizzando cioè connessioni sicure e criptate; le modalità di accesso disponibili dipendono però dalla marca e dal modello in uso.

L'accesso tramite console attraverso una connessione seriale diretta è senz'altro quello da preferire; quando però sia indispensabile connettersi all'apparato da remoto, si raccomanda

- l'utilizzo di protocolli criptati (se previsti)
- la limitazione all'accesso solo da rete locale, comprendente filtraggio e logging delle connessioni.

Per aumentare la sicurezza dell'apparato si raccomanda inoltre di:

- spegnere i server TCP/UDP non utilizzati (es. *bootps*, *finger*) e limitare l'accesso ai server abilitati solo agli amministratori
- disabilitare i servizi non necessari (*source routing*, configurazione remota) e le porte di gestione non utilizzate
- disabilitare eventuali interfacce inutilizzate
- utilizzare password non banali, diverse per ogni apparato e cambiarle regolarmente
- filtrare e loggare eventuali accessi SNMP.

Per quanto riguarda la sicurezza fisica, si raccomanda che l'apparato venga installato in un luogo nel quale possa accedere solo personale autorizzato e nel quale siano installati sistemi di protezione fisica delle macchine:

- sistemi UPS
- sistemi di condizionamento dell'aria
- sistemi antincendio.

Controllo e monitoraggio

Si raccomanda di mantenere i log dei pacchetti rifiutati o rigettati, salvarli su una macchina esterna e possibilmente dedicata, sottoponendoli ad analisi periodica anche con l'aiuto di strumenti specifici. Si raccomanda inoltre di sincronizzare il sistema con uno o più server NTP per avere informazioni orarie più precise.

Con l'aiuto di software specifico (ad esempio mrtg o rrdtool+snmp) può essere utile monitorare l'occupazione di banda e il carico di CPU del sistema, in modo da rilevare variazioni anomale degli andamenti.

Esempi di configurazione di router Cisco

Sono disponibili in rete numerosi esempi di congurazioni raccomandate per router Cisco. Fra questi si segnalano:

- le Guide GARR [6]
- le Guide NSA "Cisco Router Guides" e "Supporting Documents N. 7- The 60 Minute Network Security Guide" [5]

BIBLIOGRAFIA on-line

1. http://csrc.nist.gov/publications/nistpubs/ (SP-800-41)
2. http://www.cert.org/security-improvement/
3. http://www.infn.it/netgroup/ (LAN Security)
4. http://www.iana.org/assignments/port-numbers
5. Router security configuration guide
   http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf
6. http://www.noc.garr.it/fdoc.htm
    a. Guida alla configurazione del router utente
    b. Guida alla configurazione delle Access List sul router utente

Abbreviazioni usate:

MAC	Media Access Control
LAN	Local Area Network
VPN	Virtual Private Network
DHCP	Dynamic Host Configuration Protocol
NAT	Network Address Translation
PoP	Point of Presence
GARR	Gruppo Armonizzazione Reti Ricerca
ACL	Access Control List
DoS	Denial of Service
TCP	Transport Control Protocol
SNMP	Simple Network Management Protocol
NTP	Network Time Protocol