

Perche' un Firewall non e' sufficiente?

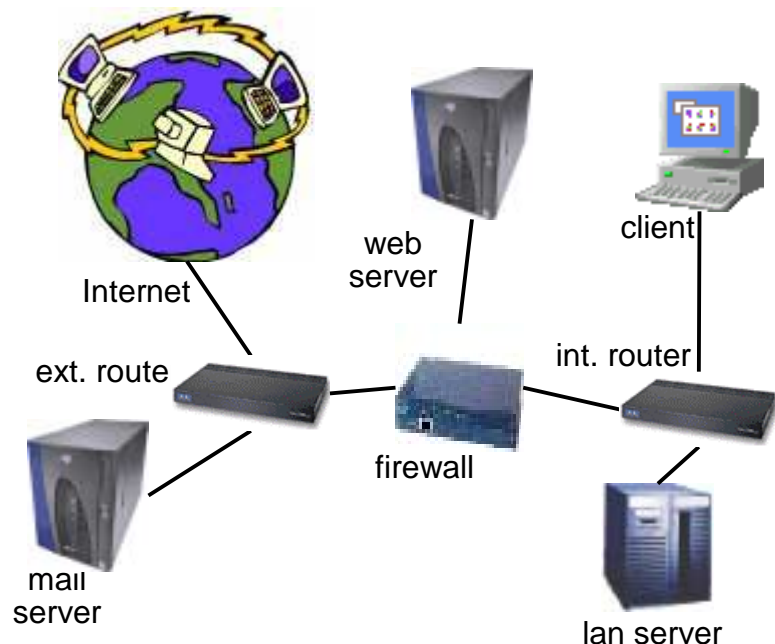


<http://www.infosec.it>

info@infosec.it

Attraversare un firewall

Cosa fa un firewall



Questo schema rappresenta una rete aziendale con le seguenti caratteristiche:

- collegamento ad Internet
- fornitura servizi Internet
- accesso del web server al lan server
- accesso del lan server al mail server
- rete interna connessa alle altre

N.B. Questa configurazione è una configurazione di esempio utilizzata per evidenziare delle casistiche.

In un cantiere edile, vengono poste delle guardie all'uscita per verificare che non venga rubato materiale di costruzione; tutte le sere le guardie controllano gli operai. Tutte le sere uno di questi esce tutto sporco e con una carriola vuota, le guardie lo lasciano passare. [L'operaio ruba indisturbato le carriere]

Lo schema di lato rappresenta una rete aziendale "comune" con alcune caratteristiche riassunte nel rettangolo in basso a sinistra, si adatta abbastanza bene ad una serie di considerazioni relative a sicurezza, funzionamento e complessità.

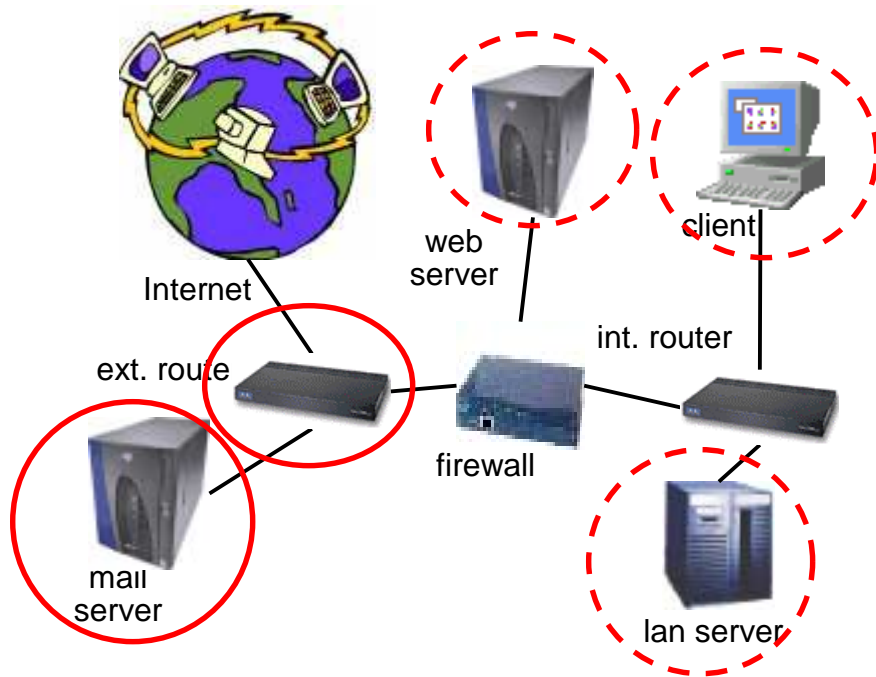
Gli attacchi a questa rete possono provenire da:

- Internet
- Sede remota
- Client remoto legittimo
- Client remoto illegittimo
- Client locale legittimo
- Client locale illegittimo

Nel caso in cui poi siano stati compromessi dei sistemi, è possibile che gli attacchi provengano da qualunque punto, compresi server, router o firewall stesso.

Un firewall è un apparecchio, o un insieme di apparati, configurato/i in modo da regolamentare il traffico in ingresso e uscita della rete o delle reti connesse.

I limiti di un firewall



Sono evidenziati in rosso i componenti della rete che non sono protetti dal firewall rispetto ad attacchi provenienti dal Internet (sono a monte del firewall).

A seconda delle tipologie di firewall e di traffico permesso nelle configurazioni è possibile che anche macchine difese dal firewall vengano attaccate con successo come verrà illustrato successivamente.

Vi sono due tipologie principali che generano problemi di sicurezza:

- configurazioni non corrette

si riscontrano problematiche che rientrano in questa categoria quando tramite una configurazione apposita del “sistema firewall” si sarebbero potuti evitare degli incidenti o quando si riscontrano impostazioni che forniscono dei punti di attacco superflui rispetto al funzionamento del sistema stesso.

[Questa tipologia è imputabile ad errori umani, errori di valutazioni e conseguente impostazione]

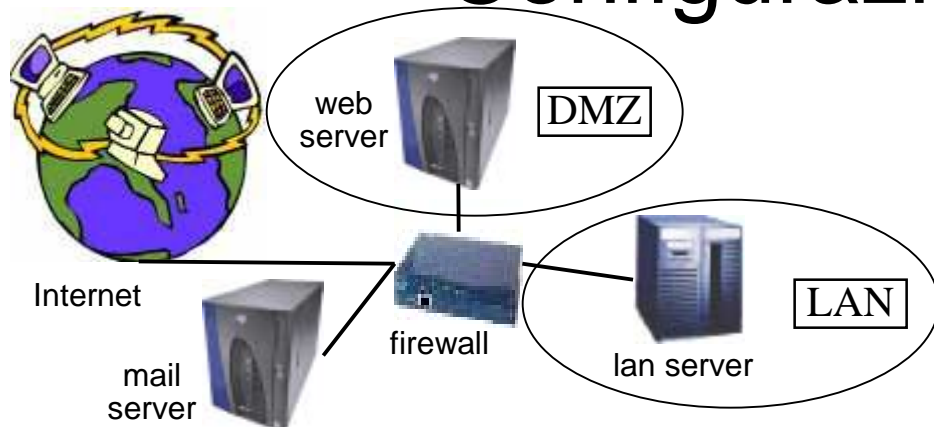
- problematiche tecniche

si riscontrano problematiche che rientrano in questa categoria quando nonostante siano state impostate le configurazioni a regola d’arte sul firewall e non vi siano punti di attacco superflui, sia possibile sfruttando degli errori di programmazione o delle vulnerabilità del firewall stesso forzare le regole impostate ed accedere indebitamente ad un componente che “teoricamente” si riteneva protetto.

[Questa tipologia è imputabile ad errori del firewall, errori di programmazione o limiti del sistema]

La configurazione di un firewall non deve essere esclusivamente operativa ma deve essere sicura.

Configurazioni non corrette



La struttura della rete è stata semplificata prendendo in considerazione i segmenti interessati da possibili errori di configurazione del firewall.

Queste possono rientrare nelle seguenti tipologie:

- configurazioni di default;
- configurazioni con specifiche negazioni e passaggio di quanto non specificatamente bloccato
- configurazioni non sufficientemente restrittive
- sistema ospite non sicuro
- relazioni di fiducia con host non protetti
- mancanza di comprensione delle problematiche di sicurezza inerenti una specifica configurazione
- errori di pianificazione della rete
- errori di valutazione dei servizi
- carenza di conoscenze avanzate su reti e protocolli

Esempi di configurazioni non corrette possono essere:

- permettere il traffico dal mail server (insicuro) al web server (DMZ) o alla rete interna (LAN)
- permettere traffici non specificatamente legati ai servizi che si vogliono fornire verso le macchine della rete pubblica (nel nostro esempio, traffico ftp, smtp, auth, smb verso la DMZ)
- permettere traffico verso eventuali servizi aperti sul firewall
- permettere traffico dalla DMZ server alla LAN (*)
- permettere traffico da Internet verso la LAN (**)

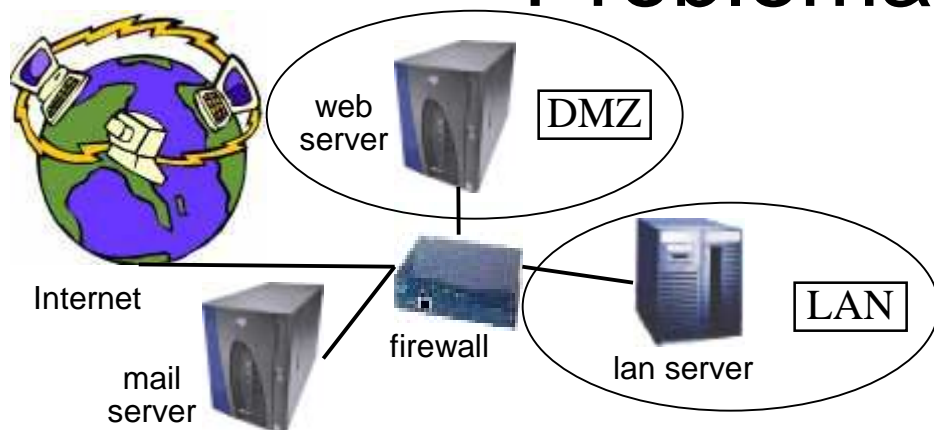
E' possibile anche essere vittime di errori più difficili da individuare come:

- errori di configurazione su servizi pubblici (verso i quali sia permesso l'accesso pubblico attraverso il firewall)
- vulnerabilità nei servizi pubblici o loro add-on insicuri
- installare agenti (cgi, asp o simili) insicuri che permettano operazioni non volute
- predefinire delle regole ed applicarle indiscriminatamente al firewall

* **Qualora vi siano servizi dinamici di consultazione di database deve essere studiato un meccanismo SICURO di consultazione delle informazioni.**

** **Qualora vi siano esigenze di telelavoro deve essere studiato un meccanismo SICURO di gestione**

Problematiche tecniche



La struttura della rete è stata semplificata prendendo in considerazione i segmenti interessati da possibili problematiche tecniche legate al firewall.

Queste possono rientrare nelle seguenti tipologie:

- limiti di configurazione e mancanza di flessibilità nell'impostazione delle regole volute
- suscettibilità a specifici attacchi
- lentezza negli aggiornamenti (anche relativamente a DoS e vulnerabilità)
- limiti di analisi del traffico (non tutti i firewall arrivano allo stesso livello..)
- mancanza di protezione del traffico "legittimo"
- reazione automatica a situazioni della rete
- accentramento delle difese della rete in un unico strumento

E' appurato che praticamente tutti i firewall abbiano avuto, essi stessi, problemi di sicurezza legati alla tecnologia utilizzata: errori di programmazione, errori di gestione delle eccezioni e quanti altri. Si rimanda al sito SecurityFocus e agli altri siti del settore per una trattazione esaustiva e aggiornamenti relativi ai problemi dei vari prodotti.

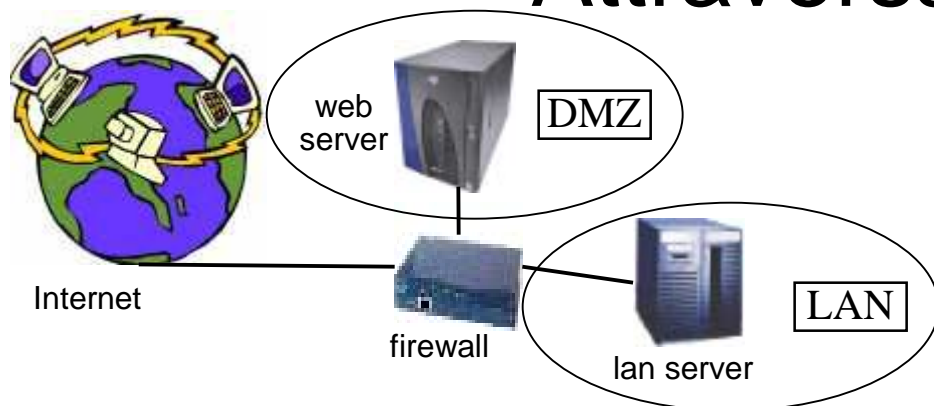
Una nota deve comunque essere fatta sulla gestione e sulla manutenzione del firewall:

- prevenire gli attacchi al sistema firewall verificandone l'efficacia periodicamente
- seguire e verificare gli aggiornamenti del sistema relativamente ai problemi di sicurezza riscontrati (con comunicazione dei produttori o pubblicazione su siti specializzati)
- analizzare i log comprendendo gli eventi della rete e la loro reale gravità
- aggiornare e mantenere gli host della rete, client compresi (che possono essere vulnerabili anche se difesi dal firewall)
- aggiornare e mantenere i servizi della rete (che possono essere vulnerabili anche se difesi dal firewall)

sono tutte attività necessarie ad una corretta amministrazione dei sistemi e ad una prevenzione degli incidenti.

E' doveroso ricordare che l'utilizzo di personale specializzato aiuta ad identificare e risolvere correttamente i problemi

Attraversare un firewall



La struttura della rete è stata semplificata prendendo in considerazione i segmenti interessati dalle regole impostate sul firewall in funzione del traffico da permettere e da negare.

Queste regole riconducono le tipologie di traffico alle seguenti:

- traffico negato
- traffico permesso

(di questo analizziamo ulteriormente le componenti)

- traffico legittimo (con trasporto legittimo)
- traffico legittimo (con trasporto illegittimo)
- traffico illegittimo (*)

* Questa categoria può esistere in funzione di particolari tecniche di generazione del traffico di rete.

Nell'analizzare un firewall di cui abbiamo descritto brevemente ragioni e limiti, nonché per comprenderne il funzionamento in una rete è interessante mettersi nell'ottica del traffico e "studiare le reazioni del firewall".

Faremo tre esempi di traffico permesso per vedere le reazioni sugli host dietro il firewall:

Esempio 1:

Da Internet un utente effettua una richiesta al web server:

```
"GET /cgi-bin/unsecure.cgi?cat%20/etc/passwd"
```

sul firewall questa richiesta viene considerata legittima ed inoltrata al web server che trasmette in chiaro la lista degli utenti e relative password criptate

Questo esempio è puramente indicativo, sebbene basato su un problema realmente esistito nel 1996.

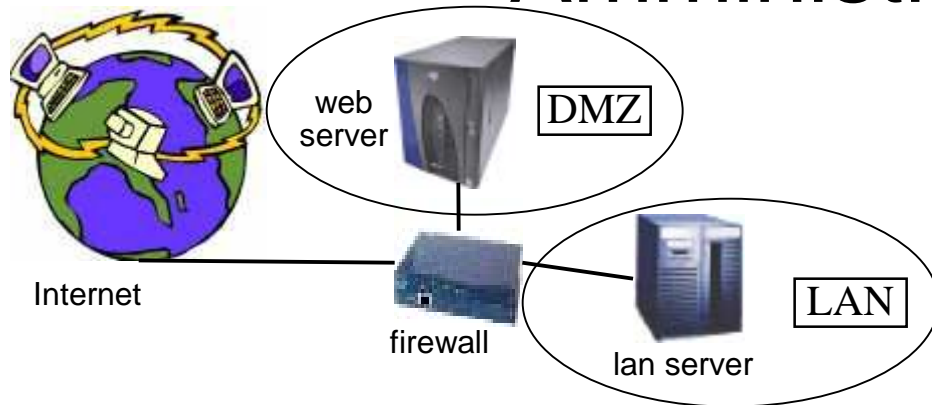
Esempio 2:

Da Internet è accessibile un servizio (ftp ?) sul server, questo servizio è vulnerabile ad attacchi e fornisce una shell da cui si può attraversando il firewall accedere alla rete.

Esempio 3:

Da Internet viene inviata una mail con un allegato che sfruttando un problema di sicurezza di un client di posta della rete interna si installa ed esegue una sequenza di comandi.

Amministrare un firewall



La struttura della rete è stata semplificata prendendo in considerazione i segmenti interessati dalle regole impostate sul firewall in funzione del traffico da permettere e da negare.

La parte più difficile nella progettazione di un firewall non è installarlo, ma configurarlo, mantenerlo e mantenere sicura la rete nel tempo. Specialmente al variare delle richieste e dei servizi forniti, avere chiari i possibili attacchi a cui potenzialmente è soggetta la rete.

Un firewall abbandonato a se stesso “invecchia” al progredire delle tecnologie di attacco e in funzione dello sviluppo delle risorse della rete, delle vulnerabilità dei client e dei protocolli che utilizzano. Presto o tardi un firewall “sicuro”, senza adeguata manutenzione diventerà “insicuro”.

Questa breve presentazione ha lo scopo di evidenziare il fatto che **i punti di forza di un firewall sono:**

- 1) corretto posizionamento nella rete
- 2) studio dei servizi che si vogliono fornire
- 3) impostazione delle regole pianificate
- 4) negazione di tutto il resto (prova del 9 degli studi fatti)
- 5) manutenzione e aggiornamento del firewall
- 6) manutenzione e aggiornamento della rete
- 7) verifica periodica dell'efficacia del sistema
- 8) consapevolezza dei limiti dei firewall

... **i punti di debolezza invece:**

- 1) configurazioni di default
- 2) mancanza di amministrazione
- 3) configurazioni troppo permissive verso host “insicuri”
- 4) installazione di applicazioni o estensioni insicure
- 5) stratificazione di situazioni non analizzate (insicure ?)
- 6) sovrabbondanza di servizi pubblicamente accessibili
- 7) concentrazione di sicurezza in un unico punto e dilagare di insicurezza circostante
- 8) suscitare un falso senso di sicurezza per il fatto di “esserci”

Un firewall risponde a delle regole, anche complesse, “come le guardie del cantiere” ma non risponde comunque a tutti i possibili problemi di sicurezza.