Architetture per reti sicure
Terminologia

Non esiste una terminologia completa e consistente per le architetture e componenti di *firewall*. Per quanto riguarda i *firewall* sicuramente si può schematizzare quanto segue:

- *Firewall*: un componente o un insieme di componenti che limitano l'accesso tra una rete protetta ed Internet.
- *Host*: un *computer* connesso ad una rete.
- *Bastion host*: un *computer* che deve essere reso molto sicuro in quanto potrebbe essere oggetto di attacchi.
- *Dual-homed host*: un *computer* che ha almeno due interfacce di rete.
- *Network address translation*: una procedura mediante la quale un *router* modifica i pacchetti che lo attraverso cambiando gli indirizzi di rete in base ad una opportuna politica.
- Pacchetto: l'unità fondamentale di comunicazione in Internet.
- *Packet filtering*: l'azione intrapresa da un dispositivo per controllare in maniera selettiva il flusso dei dati proveniente e/o diretto verso la rete.
- Rete perimetrale: una rete aggiunta (interposta) tra una rete protetta ed una rete esterna (Internet) al fine di fornire un ulteriore livello di sicurezza. Una rete perimetrale viene qualche volta chiamata DMZ, *De-Militarized Zone* (Zona DeMilitarizzata, riferimento alla zona che separa le due Coree).
- *Proxy*: un'applicazione *software* che dialoga con *server* esterni per conto dei *client* interni.
- *Virtual Private Network* o VPN: una rete che trasporta pacchetti, appartenenti ad una rete privata implementata sull'infrastruttura pubblica, che non possono essere decifrati dagli attaccanti.

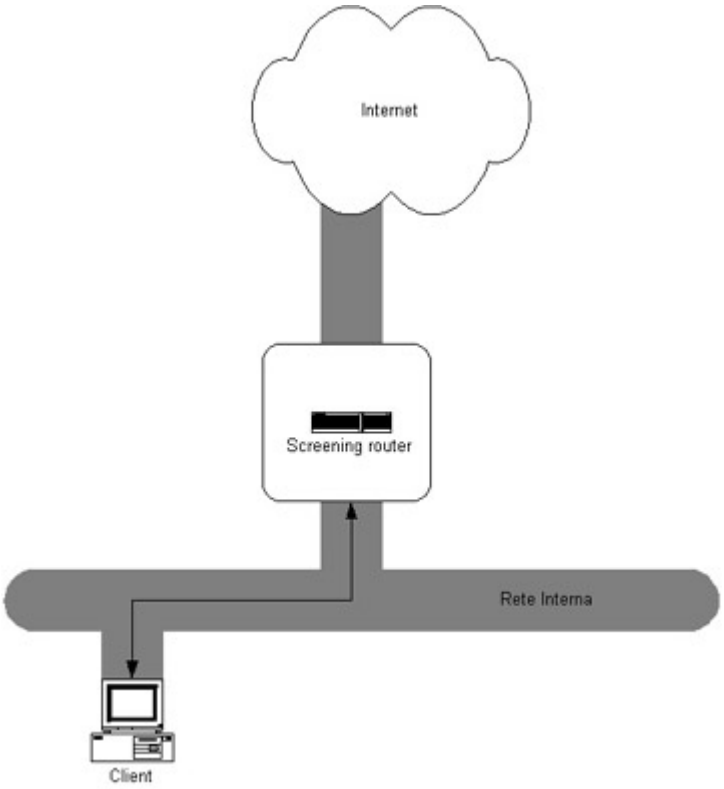
Packet filtering firewall 1

I sistemi per il *packet filtering* instradano in maniera selettiva i pacchetti tra *host* interni ed *host* esterni, vietando il passaggio a determinati tipi di pacchetti in conformità con la politica di sicurezza dell'organizzazione di appartenenza. Il *router* utilizzato come *packet filtering firewall* viene comunemente chiamato *screening router*.

Le informazioni di un pacchetto, elaborate dal *packet filter* sono:

- l'indirizzo IP di origine;
- l'indirizzo IP di destinazione;
- il protocollo a cui si riferisce il contenuto (TCP, UDP, ICMP, eccetera);
- la porta di origine TCP o UDP;
- la porta di destinazione TCP o UDP;
- il tipo di messaggio ICMP;
- la dimensione del pacchetto.

Il *router* è anche in grado di analizzare la parte dati di un pacchetto. Il *router* può anche assicurarsi che il pacchetto sia valido, impedendo la possibilità di attacchi basati su pacchetti incorretti.



Il *router* conosce altre informazione relative al pacchetto che si riferiscono a strati più bassi dell'architettura di comunicazione:

- l'interfaccia da cui proviene il pacchetto;
- l'interfaccia a cui è destinato il pacchetto.

Infine, un *router* può tenere traccia di una connessione, memorizzando, ad esempio:

- i pacchetti che costituiscono la risposta ad altri;
- il numero di pacchetti trasmessi o ricevuti da un *host*;
- eventi che indicano l'uguaglianza di pacchetti ricevuti in momenti diversi altro pacchetto;
- eventi che indicano la ricezione di pacchetti frammentati.

Packet filtering firewall 2

Per comprendere il funzionamento del *packet filtering* analizziamo le differenze tra un *router* ordinario e uno *screening router*. Un *router* ordinario controlla semplicemente l'indirizzo IP di destinazione di ogni pacchetto e seleziona il *path* ottimale per raggiungere la rete di destinazione, in base a politiche di *routing* preimpostate, in base all'indirizzo di destinazione, in base al contenuto delle tabelle di *routing*.

Uno *screening router* analizza i pacchetti molto più attentamente, decidendo se instradarlo o meno in base alle politiche di sicurezza dell'organizzazione a cui appartiene.

Le tecniche di *packet filtering* possono anche essere implementate da dispositivi che svolgono funzioni di *routing*; tali apparati prendono il nome di *packet filtering bridge*.

Una volta esaminate le informazioni di interesse, uno *screening router* compie una delle seguenti azioni:

- spedisce (*Permit*) il pacchetto verso la destinazione;
- scarta (*Drop*) il pacchetto, senza notificare l'evento al mittente;
- rifiuta (*Reject*) il pacchetto, ed invia un messaggio di errore al mittente;
- effettua il *logging* del pacchetto (registra l'evento);
- attiva un allarme per notificare ad un sistema di supervisione (*console* dello *screening router*) la presenza del pacchetto.

Router più sofisticati sono anche in grado di:

- modificare il pacchetto (ad esempio, per effettuare il *network address translation*);
- spedire il pacchetto ad una destinazione diversa da quella prevista (ad esempio, per forzare le transazioni attraverso un *proxy* oppure per effettuare un *load balancing*);
- modificare le regole di *filtering* (ad esempio, per bloccare tutto il traffico proveniente da un sito che ha spedito pacchetti ostili).

Packet filtering firewall 3

Una importante regola di filtraggio prevede l'utilizzo dei numeri di *port* associati ai servizi Internet e i *Flag* contenuti nei pacchetti TCP.

I dispositivi per il *packet filtering* che tengono traccia dei pacchetti analizzati sono di solito chiamati *statefull packet filter*, o *packet filter* dinamici, in quanto memorizzano lo stato delle connessioni, ovvero modificano il proprio comportamento in base alla storia del traffico. I filtri che operano azioni anche sul campo dati del pacchetto sono frequentemente chiamati *packet filter* intelligenti.

Un sistema per il *packet filtering* può costituire il punto in cui vengono forniti i servizi per realizzare reti private virtuali (VPN) e per il *network address translation*. Poiché il *packet filter* già analizza i pacchetti, può facilmente identificare i pacchetti che sono destinati ad un particolare *host* che si trovi nella VPN, cifrare tali pacchetti e spedirli verso la destinazione.

Packet filtering firewall 4

Vantaggi del packet filtering

- Un solo *screening router* può aiutare a proteggere una rete intera, purché ben collocato nella topologia della rete stessa.
- Semplici tecniche di *packet filtering* risultano molto efficienti. Poiché il *packet filtering* richiede l'elaborazione di un numero limitato di campi dei pacchetti, può essere utilizzato con un minimo *overhead*. L'uso di un *proxy* implica invece operazioni più complesse.
- Il *packet filtering* è disponibile in molti prodotti sia commerciali, sia *freeware*.

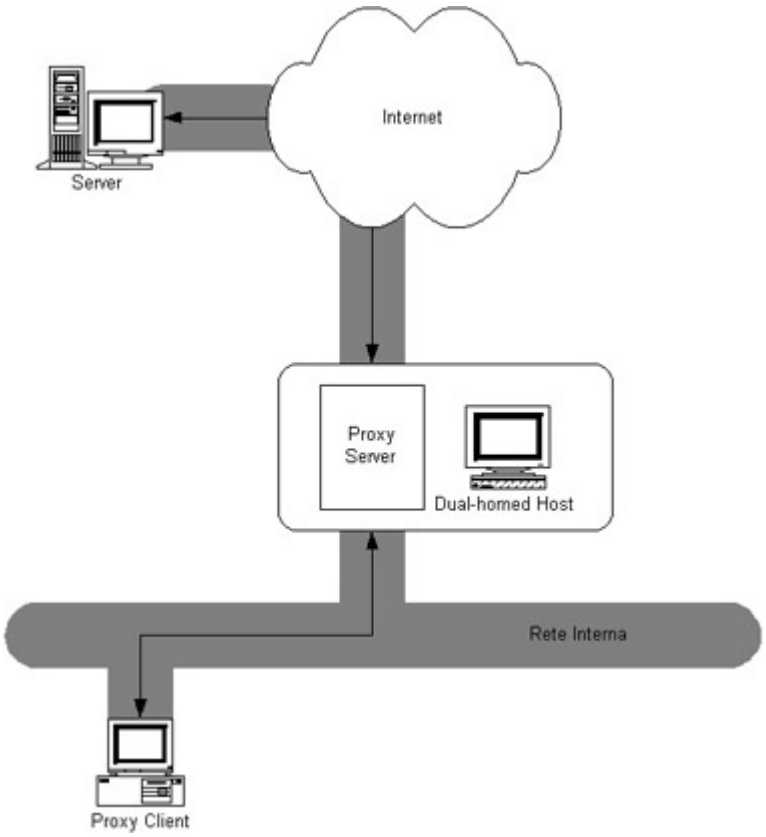
Packet filtering firewall 5

Svantaggi del packet filtering

- Gli strumenti di *packet filtering* non sono semplici da configurare, per via della complessità delle regole e delle difficoltà operative che occorre affrontare in fase di *testing*.
- Il *packet filtering*, se attivato su macchine per il *routing*, riduce le prestazioni, poiché determina un carico elaborativo aggiuntivo sul *router*.
- Alcune politiche non possono essere rafforzate da *screening router*. Ad esempio, i pacchetti possono essere associati agli *host* che li spediscono non agli utenti che ne hanno richiesto la trasmissione.

Proxy 1

Un *Proxy* è un oggetto che esegue delle azioni al posto di un altro oggetto.



Si tratta di applicazioni specializzate che ricevono richieste di servizi Internet da parte degli utenti e le inviano ai *server* reali. I sistemi *Proxy* possono essere utilizzati sia per ragioni di sicurezza, sia per ragioni di *performance*, sia per motivi di necessità.

I sistemi *Proxy* si collocano, più o meno trasparentemente, tra una rete di *client* interni ed i *server* esterni (es. Internet). La trasparenza è il maggior beneficio di un sistema *Proxy*; l'utente durante la navigazione sui *server Web*, ad esempio non percepisce la presenza del *proxy*.

Il *Proxy* opera funzioni di filtraggio; non inoltra cioé sempre le richieste all'esterno, soprattutto se la politica di sicurezza dell'organizzazione a cui appartiene prevede l'inibizione di alcuni siti *Web* o altro.

Proxy 2

Vantaggi dei sistemi Proxy

- Un sistema *Proxy* è adatto per il *logging*. Poiché un *Proxy* può comprendere il protocollo applicativo, tale sistema può effettuare un *logging* più efficiciente e completo.
- Un sistema *Proxy* consente operazioni di *caching*. Poiché tutte le richieste passano attraverso il *Proxy*, tale sistema può mantenere una copia locale dei dati richiesti. Se il numero delle richieste che si ripetono è significativo, allora il *caching* può migliorare le prestazioni.
- Un sistema *Proxy* consente una autenticazione a livello di utente.
- Un sistema *Proxy* è in grado di effettuare tecniche di *content filtering*.

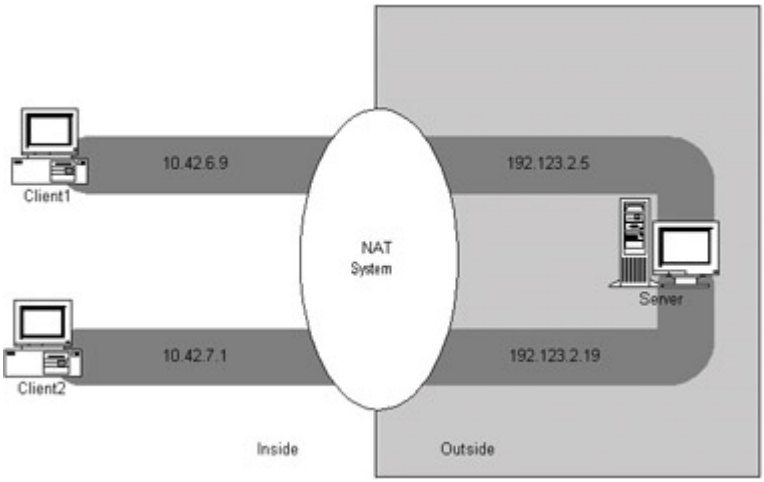
Proxy 3

Svantaggi dei sistemi Proxy

- Non tutti i servizi sono stati progettati per essere utilizzati facilmente attraverso un *Proxy*.
- I sistemi *Proxy* richiedono un differente applicativo *Proxy server* per ogni servizio.
- I sistemi *Proxy* solitamente richiedono di apportare modifiche ai *client*, alle applicazioni o alle procedure.

Network address translation 1

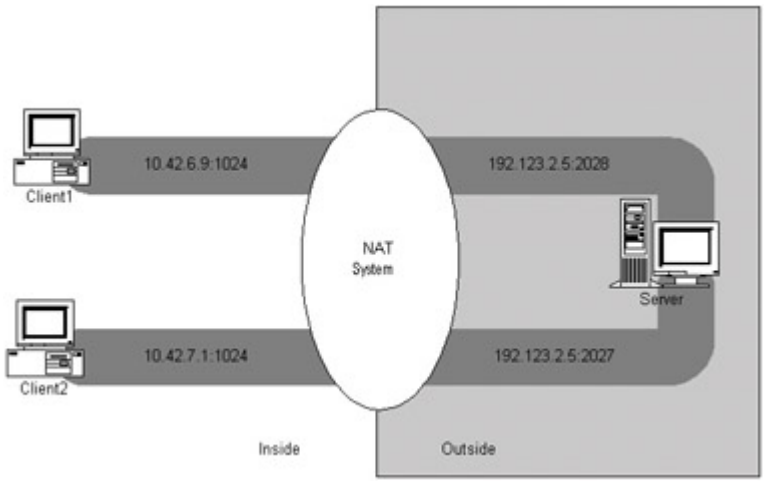
La prestazione *network address translation* consente ad una rete di usare internamente un insieme di indirizzi differente da quello utilizzato verso l'esterno. Un sistema per il NAT non fornisce sicurezza, ma aiuta a nascondere la struttura della rete interna e forza le connessioni a passare attraverso un *choke point*.



Come nel caso del *packet filtering*, anche il NAT richiede ad un *router* (in generale ad un *server*), di eseguire elaborazioni sui pacchetti. Nel caso di un *router* con funzionalità di NAT *server*, i pacchetti vengono analizzati, modificati ed istradati

Network address translation 2

Il NAT *server* è in grado di modificare anche i numeri di porta di origine e di destinazione; in questo caso viene chiamato PAT (*Port and Address Translation*).



I sistemi per il NAT possono usare differenti schemi per tradurre tra indirizzi interni ed indirizzi esterni:

- Assegnare staticamente un indirizzo esterno per ogni *host* interno, senza modificare i numeri di *port*. Questo approccio non fornisce alcun risparmio per quel che riguarda lo spazio di indirizzamento ed inoltre rallenta le prestazioni.
- Assegnare dinamicamente un indirizzo esterno ogni volta che un *host* interno inizia una connessione, senza modificare i numeri di porta.
- Creare un *mapping* fisso tra indirizzi interni ed indirizzi esterni, ma usare il *port mapping* per consentire a più macchine interne di usare uno stesso indirizzo esterno.
- Allocare dinamicamente una nuova coppia di indirizzo esterno-porta ogni qual volta che un *host* interno inizia una connessione.

Network address translation 3

Vantaggi del network address translation

Il *network address translation* consente di economizzare sul numero degli indirizzi esterni (pubblici) e determina vantaggi per la sicurezza:

- Migliora il controllo sulle connessioni in uscita, poiché tutti gli *host* possiedono un indirizzo che non funziona sulla rete esterna (tipicamente indirizzi interni sono quelli di classe C, B, A, di tipo privato).
- Limita il traffico in ingresso.
- Maschera la configurazione della rete interna. Tanto meno un attaccante conosce di una rete, tanto più la rete è sicura. Un sistema per il NAT rende molto difficile ad un attaccante la possibilità di determinare quanti *computer* comprende la rete, che tipo di macchine siano e le modalità di interconnessione.

Network address translation 4

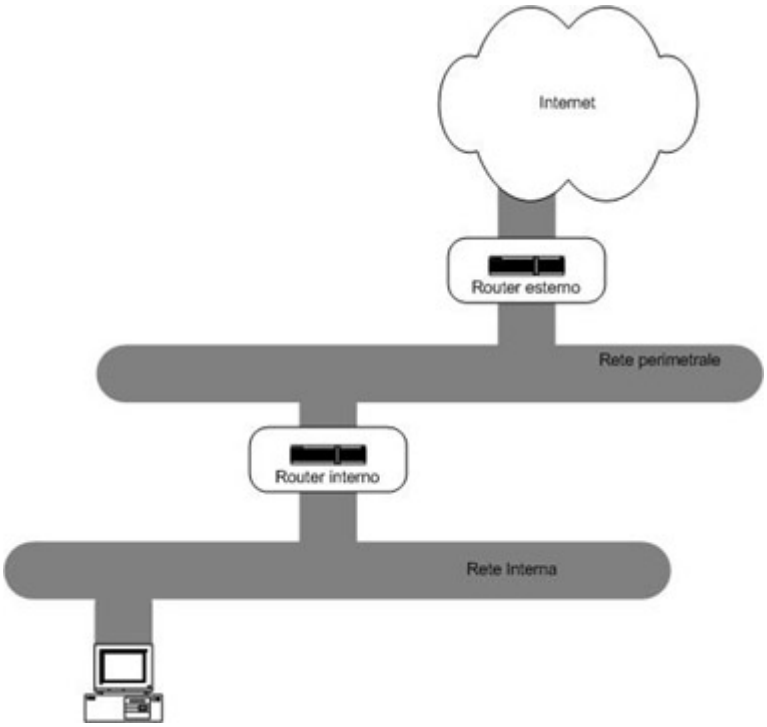
Svantaggi del network address translation

- L'allocazione dinamica richiede informazioni sullo stato che non sono sempre disponibili. Risulta molto semplice ad un sistema per il NAT sapere quando un *host* ha terminato di usare una connessione TCP, ma non esiste alcun modo per stabilire se un pacchetto UDP faccia parte di una nuova transazione o meno.
- Il NAT interferisce con alcuni sistemi di cifratura ed autenticazione. I sistemi che cifrano i dati spesso tentano di garantire anche la loro integrità in modo tale da assicurarsi che nessuno modifichi i pacchetti mentre sono in transito verso la destinazione.
- Non tutte le applicazioni funzionano correttamente se mediate dal NAT *server*.
- L'allocazione dinamica degli indirizzi interferisce con il *logging*. I *log* mostrano infatti gli indirizzi tradotti e quindi è necessario correlare le informazioni dei *log* con quelle gestite dal sistema per il NAT per poter interpretare correttamente gli eventi registrati.
- L'allocazione dinamica delle porte interferisce con il *packet filtering*. I sistemi per il *packet filtering* utilizzano le porte di origine e di destinazione per capire quale protocollo è coinvolto nell'interazione. Modificare la porta di orgine può influire sull'accettabilità dei pacchetti.

DMZ 1

L'architettura DMZ (*De-Militarized Zone*) aggiunge un ulteriore livello di sicurezza (rete perimetrale) all'architettura in cui si usa un *packet filtering*. La rete perimetrale infatti isola la rete interna dalla rete Internet. Il modo più semplice per realizzare una DMZ è quello di utilizzare due *screening router*. Uno risiede tra la rete perimetrale e la rete interna (*router* interno o *choke router*)

ed un altro risiede tra la rete perimetrale e la rete esterna (*router* esterno o *access router*). Per penetrare all'interno della rete privata è necessario violare due *router*.



La rete perimetrale comporta quindi un livello di sicurezza maggiore. Se qualcuno penetra all'interno di un *host* che si trova nella rete perimetrale può catturare solamente il traffico presente nella rete perimetrale, senza poter analizzare il traffico riservato della rete interna.

DMZ 2

router interno

Il *router* interno (o *choke router*) protegge la rete interna sia dagli attacchi provenienti da Internet che da quelli provenienti dalla rete perimetrale. Tale *router* effettua la maggior parte del *packet filtering*. Consente l'uso dei servizi esterni da parte dei siti interni (traffico di tipo *outbound*). Tali servizi possono essere tranquillamente utilizzati dall'organizzazione e facilmente gestiti da un *packet filter* piuttosto che da un *proxy server*. Il *router* interno permette anche l'accesso ai servizi attivi nella rete perimetrale, che potrebbero essere anche distinti da quelli a cui si accede nella rete esterna.

router esterno

Il *router* esterno (o *access router*) protegge sia la rete perimetrale che quella interna dagli attacchi provenienti da Internet. Permette il passaggio della maggior del traffico *outbound* ed effettua controlli solo sul traffico in ingresso (traffico *inbound*). Il tipo di attacco che solitamente viene controllato da tale *router* è quello relativo all'IP *spoofing*.