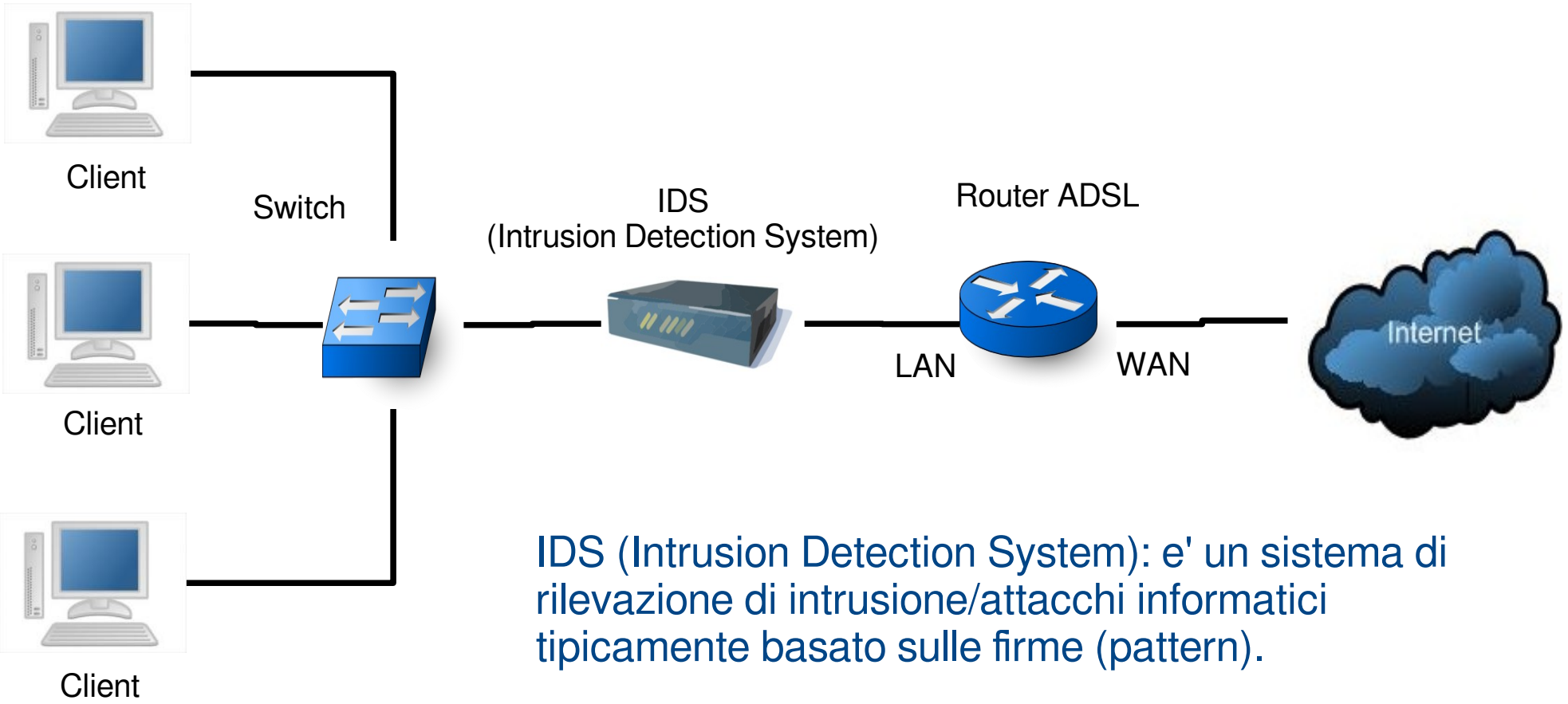
Introduzione ai Firewall e a PfSense

http://www.pfsense.org/

Novembre 2014

Sicurezza delle reti informatiche: rete di test

Rete connessa ad Internet tramite router ADSL e connessa ai client tramite switch con aggiunta di un IDS.



IDS (Intrusion Detection System): e' un sistema di rilevazione di intrusione/attacchi informatici tipicamente basato sulle firme (pattern).

Sicurezza delle reti informatiche: analisi attacco

- Primo attacco dopo meno di 10 minuti di connessione
- Sequenza di port scan
- Tentativi ripetuti di connessione alle porte:

  23/TELNET, 25/SMTP, 110/POP3, 80/HTTP, ...
- ICMP flood, tentativi di ARP Spoofing, ...
- In totale 12 attacchi nelle prime 24 ore, e 38 attacchi in 5 giorni

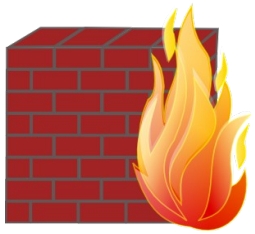
E stiamo parlando di una rete finta

senza nessuna attrattiva!!!

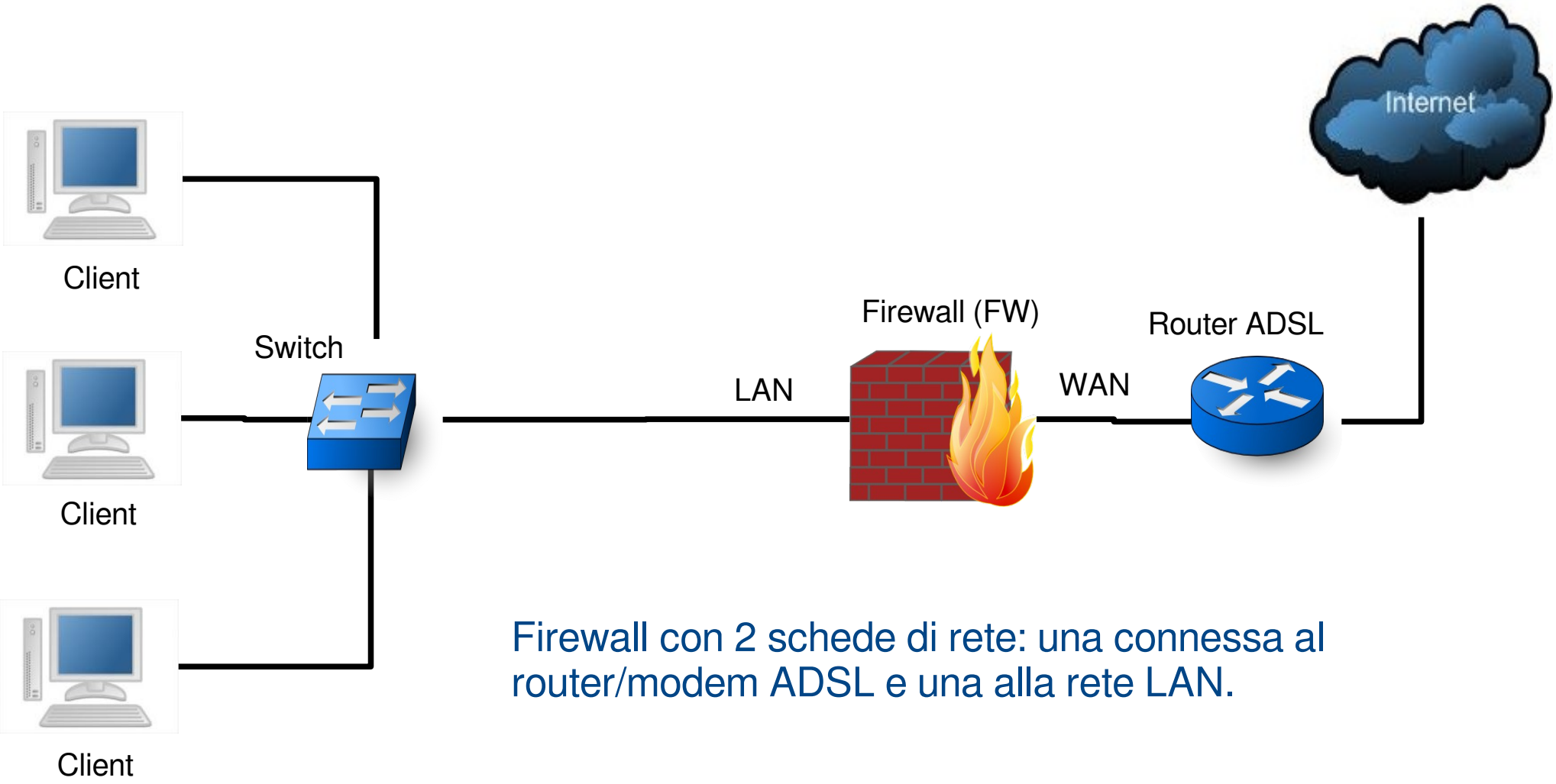
Firewall

- Nasce pertanto l'esigenza di aggiungere un dispositivo, posto immediatamente a valle del router di collegamento ad Internet, che permetta di configurare delle regole di controllo e filtraggio di tutto il traffico proveniente o diretto verso l'esterno.

Il Firewall

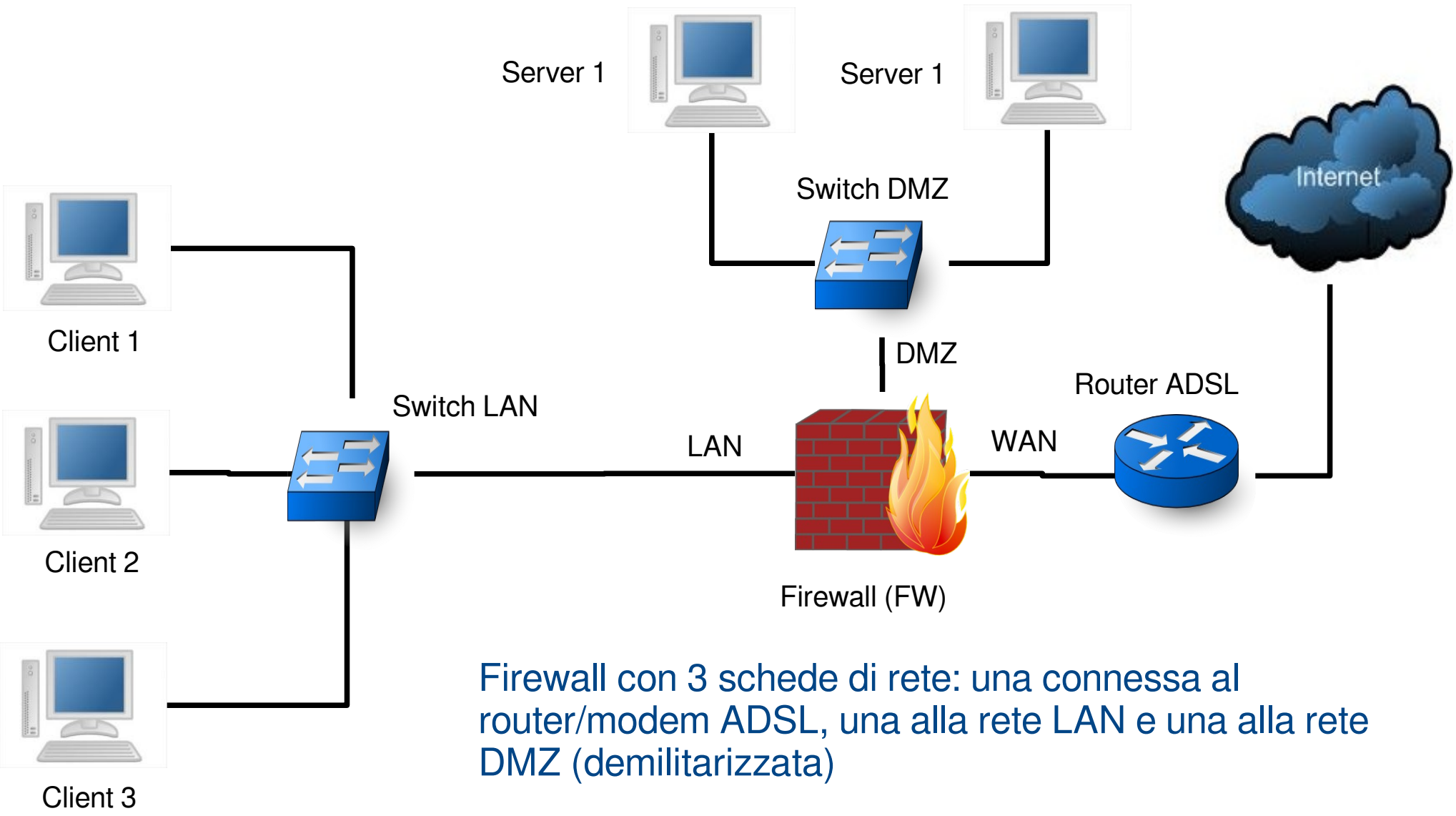


Firewall:
connessione tipica (1)



Firewall con 2 schede di rete: una connessa al router/modem ADSL e una alla rete LAN.

Firewall:
connessione tipica (2)



Firewall con 3 schede di rete: una connessa al router/modem ADSL, una alla rete LAN e una alla rete DMZ (demilitarizzata)

Firewall: definizione

- **Definizione :**

  E' un dispositivo che implementa un insieme di regole il cui scopo e' quello di garantire il controllo del traffico fra reti diverse.

- **Funzionalita' :**

  - Il FW analizza il traffico in transito e stabilisce se e' “ammissibile” ovvero in conformita' ad una policy di sicurezza o meno.

  - Il FW garantisce il controllo (e quindi il filtraggio) del solo traffico che lo attraversa.

    - Il traffico che viaggia internamente ai segmenti di rete ad esso connessi NON viene ispezionato.

Firewall:
cosa puo' fare (1)

- **Filtraggio dei pacchetti:**

  L'header di ogni pacchetto contiene informazioni riguardanti l'ip del mittente e del destinatario, il protocollo di rete utilizzato e altre informazioni che verranno processate a livello applicativo. Tramite queste informazioni un firewall può decidere se accettare o rifiutare il pacchetto.

- **Network Address Translation (NAT):**

  E' importante che dall'esterno non si possa risalire alla topologia della rete interna, così è opportuno che un firewall traduca gli ip interni in un unico ip pubblico. Questo permette inoltre di poter assegnare ad ogni scheda di rete interna un qualunque ip a scelta tra quelli predisposti per le reti private;

Firewall:
cosa puo' fare (2)

- **Inoltro dei pacchetti:**

  Il traffico destinato ad una certa porta può essere indirizzato verso un’altra porta o, ad esempio, verso un proxy server.

- **Filtraggio dei contenuti:**
  Un proxy server permette di filtrare il traffico web controllando gli url o i contenuti delle pagine prima che queste vengano restituite al browser per la visualizzazione.

- **Autenticazione avanzata:**

  Un’altra funzione molto comoda è la gestione dell’autenticazione degli utenti da parte dello stesso firewall.

Firewall:
cosa puo' fare (3)

- **Virtual Private Network (VPN):**

  Per poter collegare in modo sicuro due reti geograficamente lontane tra loro ormai si è soliti usare le VPN. Questa funzionalità, se inclusa direttamente nel firewall, rende molto semplice la creazione di queste connessioni.

- **Salvataggio e analisi dei file di log:**

  Per poter valutare l'operato del firewall è necessario analizzare scrupolosamente come questi ha agito durante la sua attività. In questo modo è possibile rivedere le regole di filtraggio modificandole opportunamente.

Firewall:
cosa non puo' fare (1)

- **Protezione da attacchi interni:**
  - Il firewall non e' piu' di nessuna utilita' quando:
    - il firewall è stato oltrepassato.
    - l'attacco nasce all'interno della rete protetta dal firewall.

      (il tipo di protezione che esso ci fornisce è perimetrale, quindi tutto ciò che è interno all'area è escluso dal filtraggio).
- **Social engineering:**
  - Usato per indicare coloro che spacciandosi per membri o organizzazioni autorevoli, estorcono preziose informazioni quali indirizzi ip, password, ecc.
  - In questo caso la soluzione è semplicemente quella di istruire il personale a non rispondere a tali domande se non in casi eccezionali.

Firewall:
cosa non puo' fare (2)

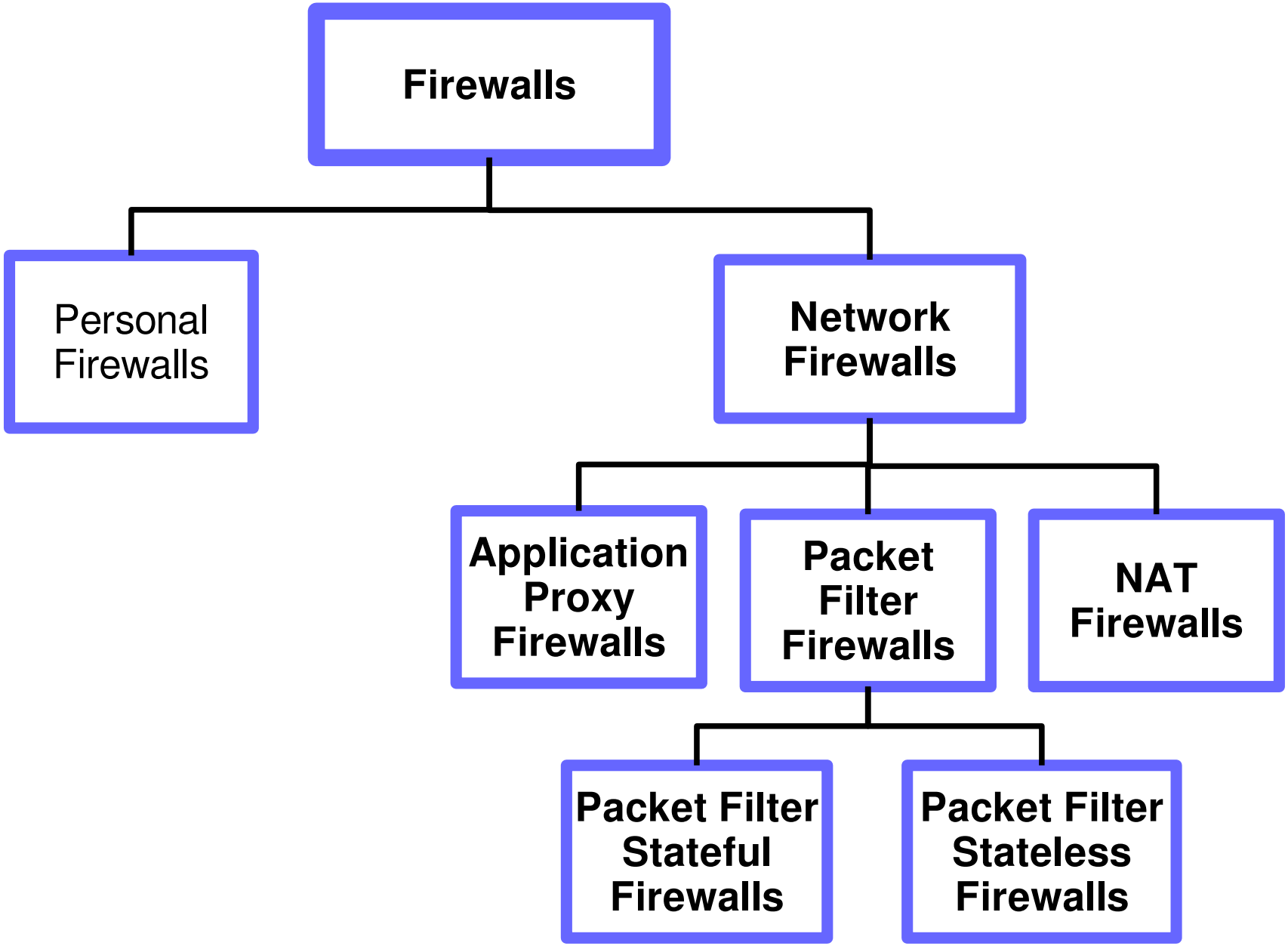
- **Integrità dei dati:**
  - I moderni firewall controllano costantemente la presenza di virus, ma non riescono a controllare tutti i pacchetti transitanti in rete alla ricerca di virus.
  - Ancora più difficilmente possono rilevare i cavalli di Troia, che non cercano di diffondersi verso altri file o computer, ma che si limitano ad aprire una back door nello stesso computer.

  Per venire a capo di queste situazioni è necessaria la presenza di un buon antivirus installato su tutti i client.

- **Cattiva configurazione:**

  Un firewall non è capace di distinguere da solo ciò che va bloccato e ciò che invece va accettato. La qualità del firewall deve essere supportata dalla qualità della sua configurazione da parte dell'amministratore.

Firewall:
Tassonomia



Firewall:
politiche e regole basi

Una delle decisioni più importanti durante la configurazione di un firewall è scegliere la strategia (politica) da applicare per la stesura delle regole.

- **Le due politiche piu' importanti:**
  - ➔ Allow-All : tutto ciò che non è espressamente negato è permesso.
  - ➔ Deny-All : tutto ciò che non è espressamente permesso è negato.

  In questo caso verrà bloccato tutto il traffico di rete, tranne quelle connessioni ritenute sicure dall'amministratore. Ciò si traduce in un minor numero di regole da gestire (e quindi un'efficienza maggiore) che devono essere aggiornate ogni qual volta viene modificata la lista delle connessioni sicure.
- **Le tre regole basi:**

1. Il firewall deve essere l'unico punto di contatto della rete interna con quella esterna.
2. Solo il traffico autorizzato può attraversare il firewall.
3. Il firewall deve essere un sistema altamente sicuro esso stesso.

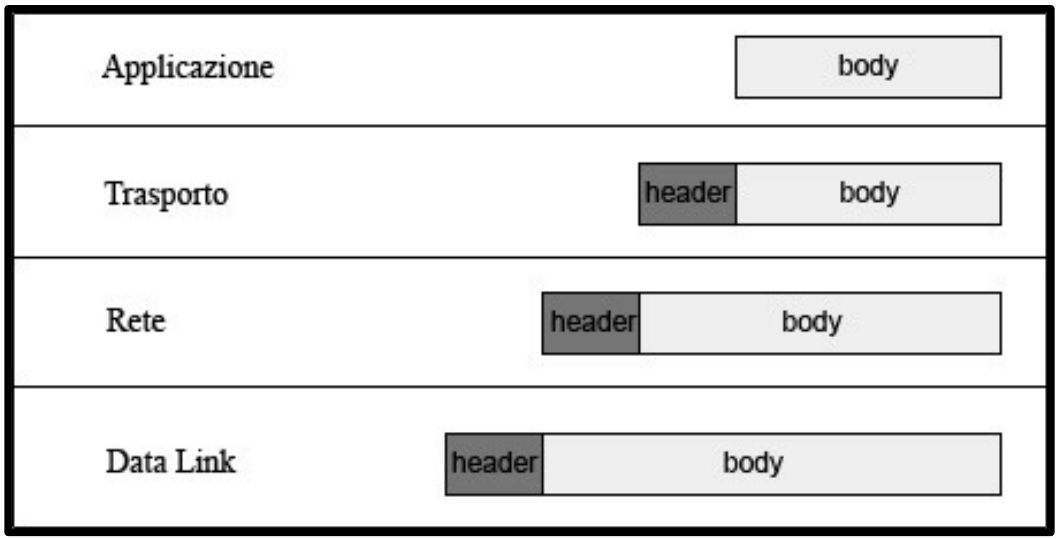
Firewall:
Open Systems Interconnect (ISO/OSI)

Application	Layer 7	→ HTTP, FTP, SSH, ecc...
Presentation	Layer 6	
Session	Layer 5	
Transport	Layer 4	→ TCP, UDP, ecc...
Network	Layer 3	→ IP, ICMP. ecc...
Data Link	Layer 2	→ Ethernet, Token Ring, ecc...
Physical	Layer 1	→ Collegamenti in rame, ottici, wireless, ecc...

Firewall:
Encapsulation

- Un pacchetto, a livello applicativo, è formato semplicemente dai dati da trasferire.
- Una volta che si scende di uno strato alla struttura del pacchetto viene aggiunto un **header** (contenente informazioni relative al livello), che nello strato sottostante verrà incapsulato nel body del pacchetto per poi aggiungere un altro header.

  Questo processo prende il nome di **encapsulation**.



Firewall:
porte TCP

- Le porte del protocollo TCP:

  - 0 -1023 **(System Ports)** : sono **assegnate** a specifici servizi dall'organismo IANA (Internet Assigned Numbers Authority)

    port 20 > FTP (control)
    port 21 > FTP (dati)
    port 22 > SSH
    port 23 > TELNET
    ecc...

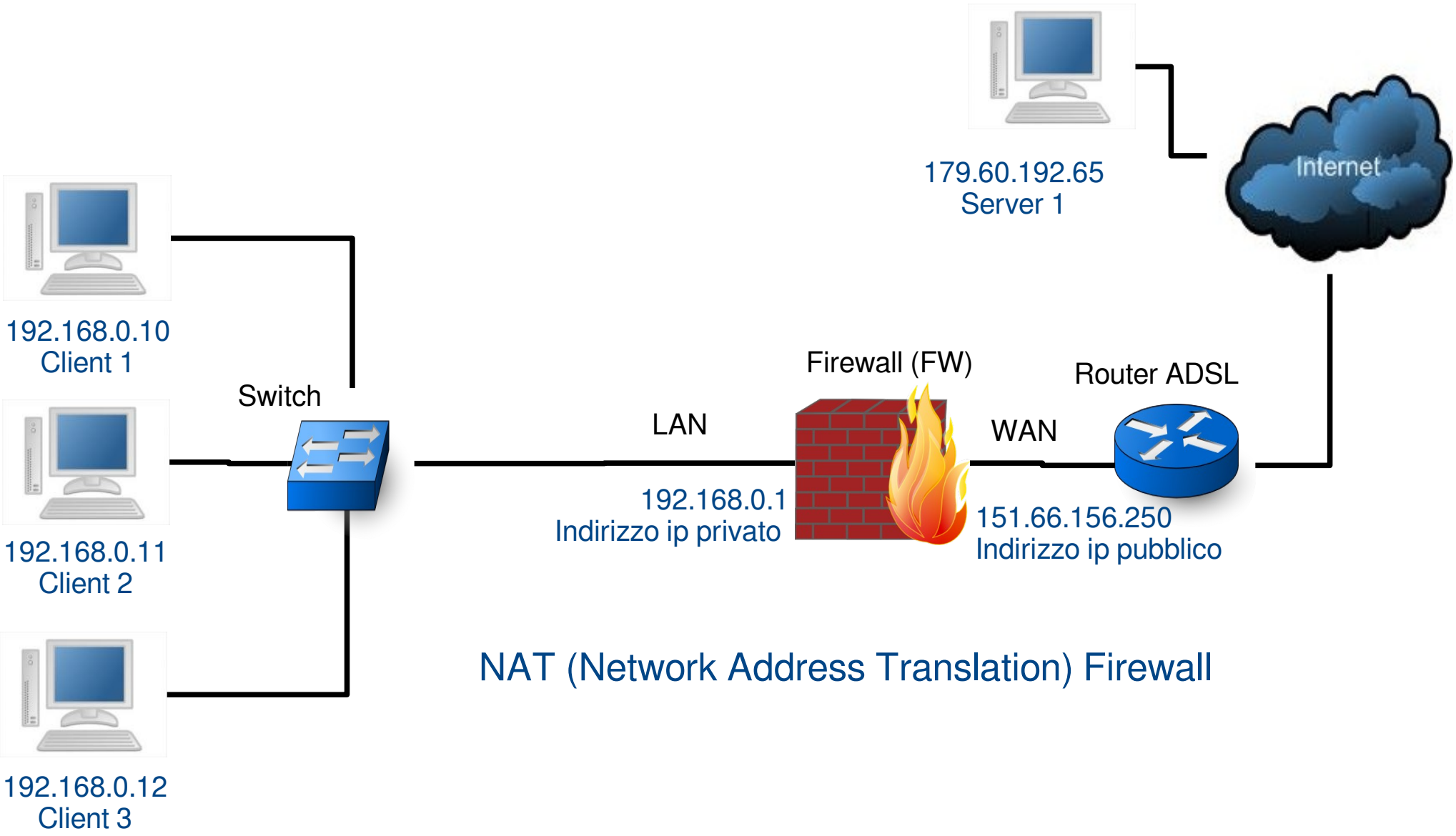
  - 1024 – 49151 **(User Ports)** : sono porte **registrate**

    port 1194 > OpenVPN
    port 3389 > Desktop Remoto SO Win
    port 5432 > PostgreSQL
    ecc...

  - 49152 – 65535 **(Dynamic Ports)** : sono porte di uso comune e quindi non sono utilizzate da applicazioni particolari

NAT Firewall

Firewall:
NAT firewall



NAT (Network Address Translation) Firewall

Firewall:
NAT firewall

- Il NAT (dinamico) viene chiamato anche IP masquerading e consiste nel presentare connessioni generate da n indirizzi IP, con un solo indirizzo IP verso l'eterno.
- La tecnica è detta anche Port Address Translation (PAT), in quanto vengono modificati non solo gli indirizzi IP ma anche le porte TCP e UDP delle connessioni in transito.
- Tipicamente e' una funzione del router (che effettui funzioni di NAT), per proteggere da accessi esterni, in quanto gli host interni possiedono indirizzi privati non accessibili da Internet.
- Un evidente limite dei firewall di tipo NAT è che non si effettua alcun controllo sul traffico verso l'esterno.
- Inoltre non si controlla il traffico a livello applicativo e quindi il NAT non impedisce il download di software pericoloso (virus).

Packet Filter Stateless

Firewall:
Packet Filter Stateless (1)

- Un packet filter FW analizza le informazioni contenute nell'header a livello Network (layer 3) e analizza anche gli header a livello Transport (layer 4) ma ignora le informazioni del protocollo applicativo al quale il pacchetto si riferisce.
- Viene quindi a conoscenza delle seguenti informazioni:
  - IP del mittente.
  - IP del destinatario.
  - Numero di porta del mittente e destinatario.
  - Protocollo.
- Il FW, dopo aver avuto accesso a tali informazioni, decide se il pacchetto può essere accettato o meno attraverso un algoritmo di scelta che si basa su una lista di regole (in ordine di priorità) precedentemente definite.
- I pacchetti vengono filtrati in base al servizio avvalendosi del fatto che le porte dei servizi TCP/UDP più conosciuti sono definite.

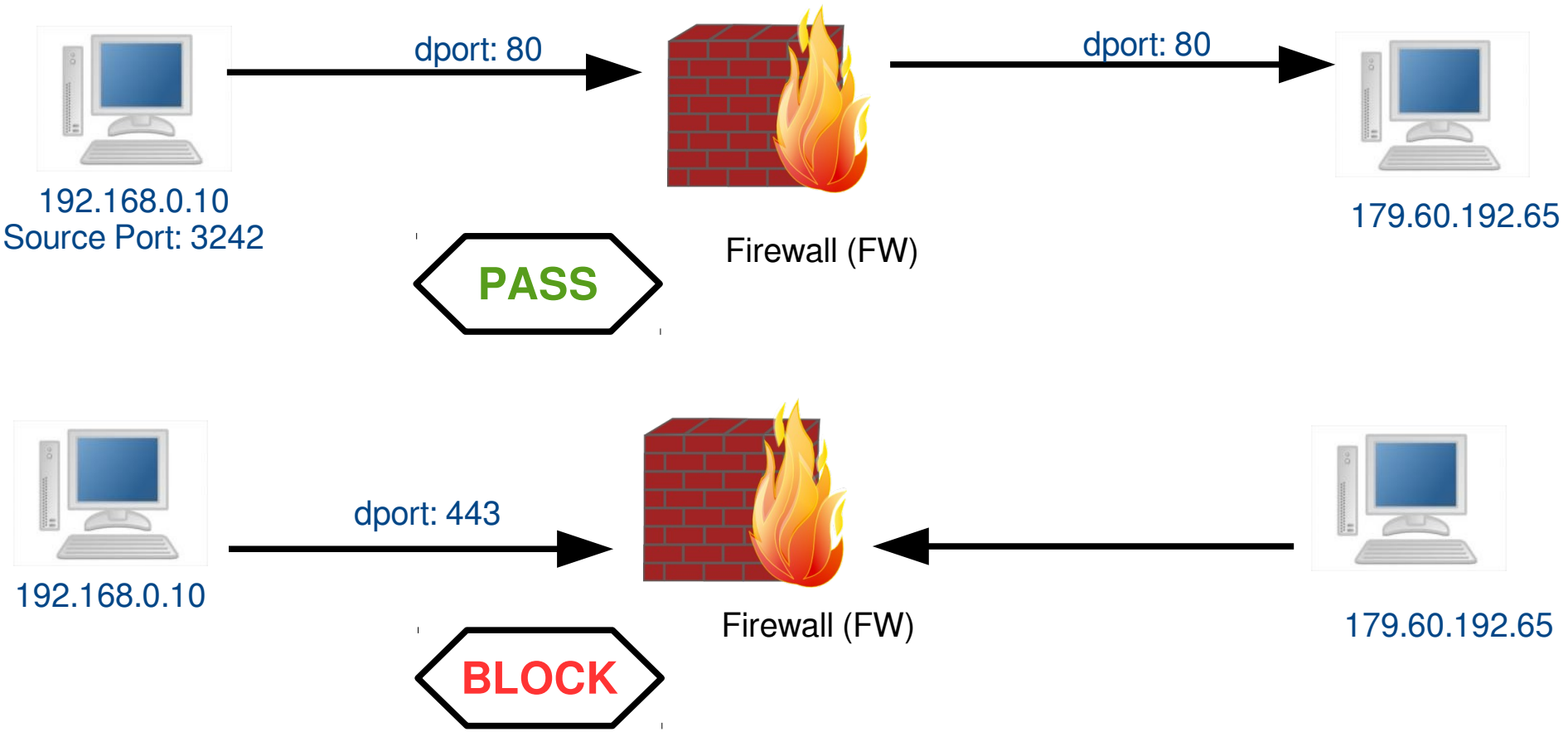
Firewall:
Packet Filter Stateless (2)

Esempio: se si vuole permettere soltanto il traffico da uno specifico indirizzo IP verso internet solo sulla porta 80, le regole di filtraggio dovranno essere del tipo:

N°	Azione	IP Source	Port Source	IP Dest.	Port Dest.	Descrizione
1	Accept	192.168.0.10	*	*	80	HTTP
2	Deny	*	*	*	*	ALL

- Quando il firewall riconosce che il traffico attuale trova riscontro in una delle regole di filtraggio presenti nella lista, i pacchetti possono essere gestiti in uno dei tre modi seguenti:
  - **Accept/Pass:** il firewall permette al pacchetto di raggiungere la sua destinazione. Quest'azione può generare delle entry nei log.
  - **Deny/Block:** il firewall scarta il pacchetto, senza che questo passi attraverso il firewall. Una volta che il pacchetto è stato scartato viene inviato un messaggio d'errore all'host sorgente. Quest'azione può generare delle entry nei log.
  - **Discard/Reject:** il firewall non solo scarta il pacchetto, ma non viene restituito nessun messaggio d'errore all'host sorgente. In questo modo si implementa una metodologia black hole attraverso la quale il firewall non rivela la sua presenza agli estranei. Questa azione può generare delle entry nei log.

Firewall:
Packet Filter Stateless (1)



FIREWALL RULE: PERMIT FROM ip: 192.168.0.10 Source Port: ANY TO ip: ANY Dest. Port: 80

Firewall:
Vantaggi Packet Filter Stateless (1)

- Trasparenza.
  Il firewall non lavora a livello applicativo, quindi non ostacola in alcun modo il normale utilizzo della rete, lavorando in maniera trasparente all'utente.
- Velocità.
  Il packet filtering è la tecnologia firewall che effettua meno controlli, e per questo è la più veloce. Per lo stesso motivo è semplice implementarla in soluzioni hardware.
- Immediatezza.
  Definendo una singola regola si può difendere un'intera rete dai pericoli derivanti da quel tipo di traffico.
- Gateway-only.
  I client non richiedono nessuna configurazione aggiuntiva.
- Topologia della rete interna invisibile dall'esterno.
  Con l'aggiunta di una NAT l'unico host visibile sarà il gateway/firewall.

Firewall:
Svantaggi Packet Filter Stateless (1)

- Basso livello.
  Lavorare a livello di network può essere positivo se il requisito fondamentale è la velocita' delle comunicazioni. Ma un packet filter non è in grado di elaborare le informazioni dei livelli superiori, quindi non è in grado di bloccare attacchi mirati a vulnerabilità di una specifica applicazione.
- Mancanza di servizi aggiuntivi.
  I firewall a filtraggio di pacchetti non permettono la gestione dell'autenticazione, l'http object caching ed il filtraggio di url e contenuti.
- Logging limitato.
  Le informazioni a cui il firewall può fare ricorso sono quelle presenti nell'header del pacchetto, quindi i file di log prodotti conterranno pochissime dati utili a fare auditing.
- Vulnerabile allo spoofing.
  Se il firewall opera filtrando i pacchetti in base alla loro provenienza, bisogna essere sicuri che quella sia la reale provenienza del pacchetto. Tramite una tecnica chiamata IP Spoofing è infatti possibile mentire sul proprio ip e aggirare le regole che altrimenti bloccherebbero l'accesso.

Packet Filter
Stateful Inspection

Firewall:
Packet Filter Stateful Inspection (1)

- **Il Packet Filter Stateful Inspection** sottolinea la novità più importante introdotta rispetto alla generazione precedente:

  il filtraggio non avviene più considerando in maniera isolata ogni singolo pacchetto, ma le decisioni saranno prese anche in base al contesto.

- Secondo il protocollo TCP/IP, quando un'applicazione richiede una connessione verso un altro host, sul sistema (mittente) viene aperta una porta che servirà per la ricezione del traffico. Questa porta sarà una di quelle comprese tra la 1024 e la 49151.
- Un Packet Filter Stateless per consentire queste connessioni dovrebbe permettere tutte quelle provenienti da una porta maggiore di 1023. Aprire così tante porte aumenterebbe la vulnerabilità della rete, quindi è bene cercare sempre di evitare questo approccio.

Firewall:
Packet Filter Stateful (2)

- Il Packet Filter Stateful, quando viene stabilita una connessione, se le regole di filtraggio non la bloccano, le informazioni relative ad essa sono inserite in una tabella di stato.
  I successivi pacchetti in ingresso saranno valutati in base all'appartenenza ad una delle connessioni consentite presenti nella tabella.
- Una volta che la connessione è conclusa la sua entry nella tabella sarà cancellata, così da evitare che questa si riempia completamente.

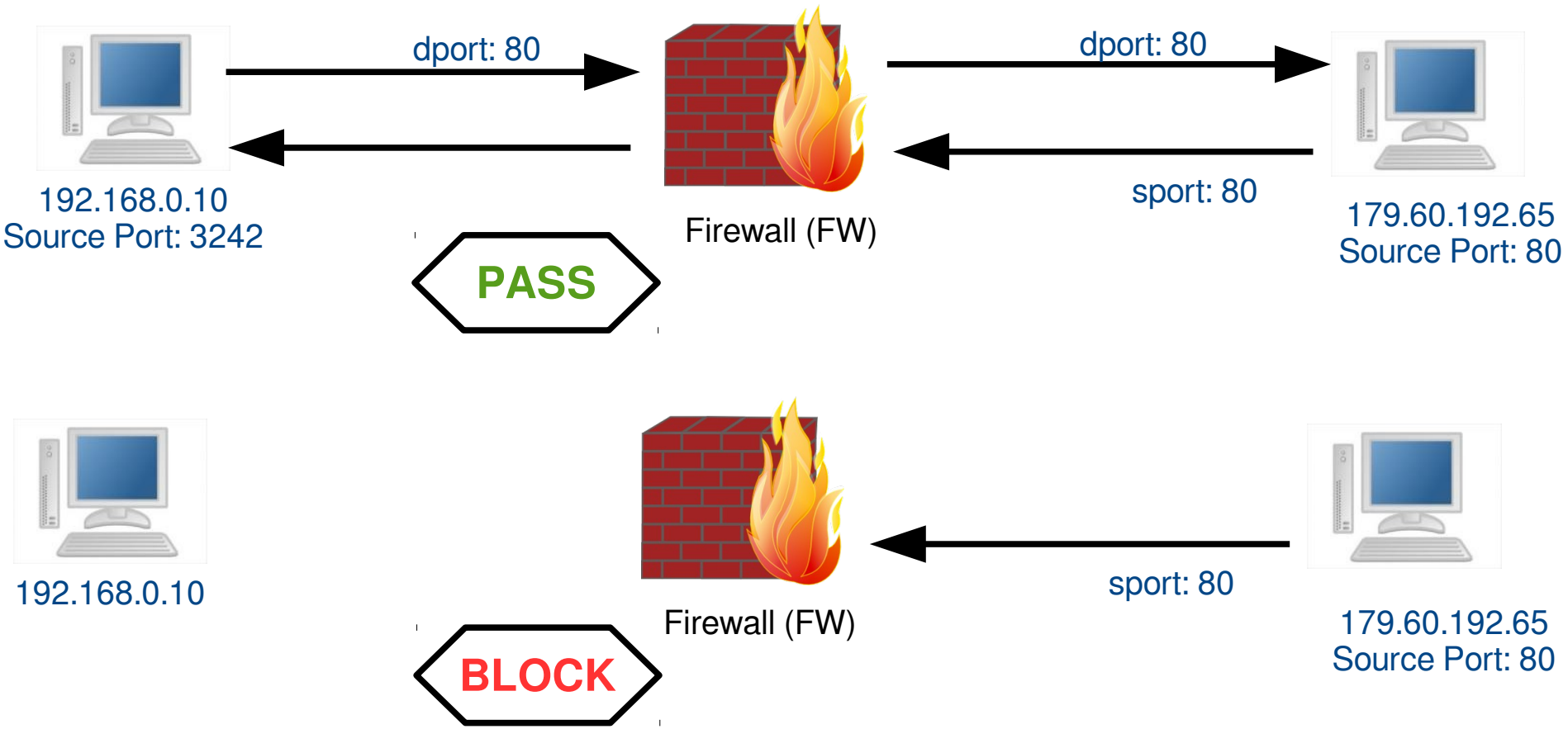
Firewall:
Packet Filter Stateful (3)

- Le informazioni riguardanti la connessione che verranno memorizzate saranno:
  - Un identificatore univoco del collegamento di sessione.
  - Lo stato della connessione. E' indicato come:
    - handshaking se si è nella fase iniziale, quella in cui si raccolgono le informazioni e si salvano nella tabella di stato,
    - established se la connessione è stata stabilita
    - closing se la connessione è terminata e si sta per eliminare la entry
  - Informazioni sulla sequenzialità dei pacchetti.
  - Gli indirizzi ip dell'host sorgente e di destinazione.
  - Le porte utilizzate dell'host sorgente e di destinazione.
  - Le interfacce di rete utilizzate.
- Utilizzando queste informazioni il firewall analizzerà ogni pacchetto per verificare se al computer che sta trasmettendo i dati è consentito effettuare una connessione col computer che deve riceverli (l'host protetto dal firewall).

Firewall:
Packet Filter Stateful

STATE TABLE:

FROM ip: 192.168.0.10 Source Port: 3242 TO ip: 179.60.192.65 Dest. Port: 80



FIREWALL RULE: PERMIT FROM ip: 192.168.0.10 Source Port: ANY TO ip: ANY Dest. Port: 80

Firewall: Vantaggi Packet Filter Stateful (1)

- Buon rapporto prestazioni/sicurezza.
  E' la tipologia di firewall con le più alte performance, perché è quella che effettua meno controlli durante la connessione. Nonostante questo è più affidabile di un Packet Filter Stateless.
- Protezione da IP Spoofing e Session Hijacking.
  Dato che il controllo non si limita al singolo ip o alla porta, è molto più difficile riuscire ad aggirare il firewall. Nel caso dello spoofing frammentare il più possibile il pacchetto in modo da aggirare la verifica delle informazioni dell'header non è efficace, perché le variabili in gioco sono molte di più. Lo stesso vale per il session hijacking, col quale si cerca di passare tramite una delle connessioni segnate come established.
- Tutti i vantaggi del packet filtering.
  Essendo una diretta evoluzione dei cosiddetti firewall di primo livello, gli stateful inspection packet filters ne ereditano tutti i fattori positivi (immediatezza, possibilità di natting...).

Firewall:
Svantaggi Packet Filter Stateful (1)

- Protocollo unico.
  Questa tecnica di firewalling sfrutta molte delle caratteristiche presenti nel protocollo tcp, e per questo motivo non può essere utilizzata all'interno di altre infrastrutture di rete.
- Servizio di auditing limitato.
  Il numero di informazioni salvate nei log è superiore rispetto ai packet filtering, ma non al punto che un amministratore possa ritenersi soddisfatto.
- Mancanza di servizi aggiuntivi.
  Si tratta dell'evoluzione del tipo di firewall precedente. Di conseguenza, non potendo agire a livello di applicazione non sono disponibili servizi come la gestione delle autenticazioni e il filtraggio dei contenuti.

Application Proxy

Firewall:
Application Proxy (1)

- Un **Application Proxy** (chiamato bastion host nel caso in cui rappresenta l'unico punto di contatto con la rete esterna, poiché appositamente corazzato e protetto per resistere agli attacchi) permette di realizzare una politica di sicurezza molto più severa di un semplice Packet Filter.
- Piuttosto che amministrare il flusso della comunicazione attraverso il filtraggio dei pacchetti si utilizza, per ogni applicazione desiderata, un programma mirato detto **proxy**.
- Un application proxy, più nello specifico, è un processo eseguito sul gateway che si interpone a livello di applicazione nella comunicazione fra componenti di una specifica applicazione per la quale è stato progettato. Nel caso di applicazioni client-server, ad esempio, un application proxy comunica con il client simulando di essere il server, e viceversa, comunica con il server simulando di essere il client.

Firewall:
Application Proxy (2)

- Mentre un packet filter è capace di utilizzare soltanto informazioni di basso livello come indirizzi ip e numero di porta, un application proxy è in grado di ispezionare l'intera porzione dati del pacchetto. Ad esempio un proxy FTP può bloccare pacchetti FTP che contengono certi nomi di file.
- Per comprendere il meccanismo di funzionamento di questo tipo di firewall analizziamo un esempio pratico:
  - Un computer della rete interna invia al firewall una richiesta di connessione con un server presente su Internet. Il proxy raccoglie la richiesta, controlla il set di regole per assicurarsi che essa sia lecita, per poi rigenerarla e inviarla al server. Quest'ultimo riceve la richiesta come se fosse partita dal proxy, ed invia la risposta. Questi pacchetti verranno nuovamente ispezionati e ricreati per poi essere inviati all'host interno.
- In nessun caso i pacchetti viaggiano direttamente fra client e server.

Firewall:
Vantaggi dell'Application Proxy (1)

- Controllo completo.
  Un application proxy non effettua verifiche relative soltanto alle informazioni contenute nell'header del pacchetto, ma utilizza anche quelle contenute nel body (la cosiddetta parte applicativa). Questo controllo avviene due volte: quando viene inviata la richiesta e quando si riceve la risposta.
- Log dettagliati.
  Le informazioni memorizzate sono molto accurate, perché oltre quelle contenute negli header dei pacchetti potranno essere utilizzate anche quelle di livello applicativo.
- Nessuna connessione diretta.
  Ogni volta i pacchetti in entrata e in uscita vengono totalmente rigenerati, quindi problemi tipo il buffer-overflow o simili non raggiungeranno l'host interno.
- Sicurezza anche in caso di crash.
  Un buon sistemista di rete cerca di evitare in ogni modo che avvengano, ma nel peggiore dei casi deve essere sicuro che le comunicazioni non avvengano in assenza del firewall. Un crash di un packet filter permetterebbe a qualunque pacchetto di viaggiare indisturbato, mentre un crash del proxy bloccherebbe completamente la connessione.

Firewall:
Vantaggi dell'Application Proxy (2)

- User-friendly.
  Le regole di filtraggio sono molto più facili da configurare rispetto a quelle di un Packet Filter.
- Autenticazione
  I gateway a livello di applicazione hanno la facoltà di supportare un’autenticazione dell'utente.
- Cache.
  I risultati delle varie richieste possono essere salvati in modo tale che se successivamente ne avverranno altre per gli stessi contenuti (nel caso di pagine web) sarà la cache a fornirli, liberando la rete da un carico supplementare. Sebbene molti siano convinti che questo sia lo scopo reale di un proxy, questo è soltanto un servizio secondario.

Firewall: Svantaggi dell'Application Proxy (1)

- Poco trasparente.
  I computer interni devono essere configurati per utilizzare il proxy invece di collegarsi direttamente al server.
- Un proxy per ogni applicazione.
  Per ogni servizio che si ha necessità di far passare attraverso il firewall che implementa questa tecnologia c'è bisogno di un proxy dedicato.
- Basse performance.
  E' probabilmente il maggior difetto di queste soluzioni firewall. La gestione della connessione attraverso il proxy richiede molto lavoro per la cpu, diversamente dai firewall di tipo Packet Filter.

PfSense

Firewall:
PfSense

- PfSense è un potente sistema firewall Open Source, basato su sistema operativo FreeBSD e che utilizza come sistema di filtraggio PF, ossia il Packet Filter di OpenBSD, uno dei sistemi più utilizzati nella realizzazione di sistemi di elevata sicurezza.
- Il progetto è iniziato nel 2004 come un fork del progetto m0n0wall, ma focalizzata verso le installazioni su PC piuttosto che su HW embedded.
- Sicuro e completamente configurabile tramite interfaccia web, può utilizzare per il suo funzionamento anche l'hardware di un comune PC.
- Include una lunga lista di funzionalità aggiuntive che permettono, grazie alla loro integrazione, di raggiungere un livello di protezione, sicurezza e controllo della rete estremamente elevato.
- pfSense è un progetto abbondantemente testato che conta ormai più di 1.000.000 (fine primo trimestre 2011) di download ed innumerevoli installazioni in tutto il mondo che variano dalla piccola e media azienda, fino alle grandi aziende, enti pubblici, ministeri, università ed altre organizzazioni che proteggono migliaia di dispositivi di rete.

Firewall:
PfSense - Architetture

- Architetture

  A partire da pfSense 2.0, ci sono versioni per:

  - i386 (32-bit)
  - amd64 (64 bit).

- Le CPU supportate (https://www.freebsd.org/relnotes/CURRENT/hardware/proc.html) sono quelle compatibili con FreeBSD 8.3 (PfSense 2.1.5) ovvero:
  - Amd64 > AMD Athlon™64, AMD Opteron™, AMD Sempron™, AMD Turion™, AMD Phenom™, multi-core Intel® Xeon™, The single-core Intel® Xeon™, Intel® Core™ 2 (not Core™ Duo) and later processors, Intel® Pentium® D processors, Intel® Centrino® Duo and Centrino® Pro, Intel® Pentium® 4 and Celeron® D, ecc...
  - I386
  - Pc98
  - Powerpc
  - Sparc64

Firewall:
PfSense – Tipologia installazione (1)

- Sono disponibili tre tipologie di installazioni:

  - Live CD o USB memory stick (senza installazione su HD o CF)

  La piattaforma Live CD consente di eseguire PfSense direttamente dal CD senza installare un disco rigido o scheda Compact Flash.

    - La configurazione può essere salvata su un disco floppy o un'unità flash USB.
    - Nella maggior parte dei casi, questo dovrebbe essere utilizzato solo come una valutazione del software con l'hardware particolare.
    - PfSense 2.0 Live CD è disponibile anche in una versione memstick USB che funziona in modo identico al Live CD.

  - Live CD o USB memory stick (con installazione su HD o CF)
    - Il Live CD (o USB memory stick) include un'opzione per installare il software pfSense sul disco rigido del sistema. Questo è il mezzo preferito per l'esecuzione di software pfSense.
      L'intero disco rigido viene sovrascritto, il dual boot con un altro sistema operativo non è supportato.

Firewall:
PfSense – Tipologia installazione (2)

- Versione NanoBSD

  La versione NanoBSD è studiato appositamente per l'utilizzo con la memoria flash (soprattutto Compact Flash), piuttosto che un disco rigido.

  - La memoria flash può gestire solo un numero limitato di scritture; il filesystem viene montato in sola lettura (viene abilitata la scrittura solo in certi casi - configurazione).
  - La versione NanoBSD ha due partizioni per il sistema operativo e una partizione per la configurazione.
    - Una partizione e' usata per il boot del SO
    - Una partizione e' usata per gli aggiornamenti o back-up
    - Una partizione e' usata per la memorizzazione della configurazione.

Firewall:
PfSense – Requisiti Hardware minimi

- Requisiti Hardware minimi (PfSense 2.x)
  - Requisiti generali per installazione su HD
    - CPU - Pentium II
    - RAM - 256 MB
    - Hard Disk 1 GB
    - Lettore CD-ROM
    - Porta USB
  - Embedded (nanoBSD)
    - 1 GB Compact Flash card
    - Porta seriale per la console o VGA

Firewall:
PfSense – Caratteristiche (1)

Tra le principali caratteristiche, troviamo (https://www.pfsense.org/about-pfsense/features.html):

- Un'avanzata funzionalità per impronte digitali che abilita il filtraggio in base al tipo di sistema operativo utilizzato dai pc della rete.
- Politiche di routing ad alta flessibilità per la selezione del gateway, per il bilanciamento del traffico, failover, WAN multiple, backup su più ADSL, etc...
- Rindondanza mediante protocollo CARP: due o più Firewall possono essere configurati per lavorare in coppia e simultaneamente. In caso di guasto/rottura di uno dei due Firewall, il traffico Internet ed i servizi correlati saranno gestiti automaticamente dal secondo Firewall in maniera del tutto trasparente e senza creare disservizi
- VPN: Per collegare tra loro sedi distaccate e utenti in mobilità (tramite Pc portatili o smartphone), pfSense offre tre tipologie per la connettività VPN: Ipsec, OpenVPN,PPTP,L2TP

Firewall:
PfSense – Caratteristiche (2)

- Raccolta statistiche sul traffico di rete (anche in tempo reale), generazione di grafici RRD, monitoraggio e generazione di report relativi alla navigazione in Internet da parte dei pc della rete.
- Dynamic DNS.
- Captive Portal.
- DHCP Server.
- Traffic Shaping
- Traffic Limiter

Riferimenti

PfSense	www.pfsense.org
PfSense Italy	www.pfsenseitaly.com
Forum PfSense	https://forum.pfsense.org/
Doc/tutorial PfSense	https://doc.pfsense.org/index.php/Main_Page
FreeBSD	www.freebsd.org
m0n0wall	www.m0n0.ch