Sicurezza

Problematiche con cui chiunque può aver avuto a che fare

- Danneggiamento dei computer connessi a internet mediante virus
- Violazioni di privacy
- Impossibilità di utilizzare servizi Internet

Occuparsi di sicurezza vuol dire:

- Studiare come un malintenzionato può attaccare la rete o un host
- Adottare metodi di difesa o progettare nuove architetture che siano immuni da attacchi

Cos'è un attacco?

Un qualsiasi insieme di azioni che tenta di

compromettere

*l'**integrità***

*la **confidenzialità***

*o la **disponibilità** di una risorsa*

Cosa vuol dire "comunicare in modo sicuro?"

Mantenere le comunicazioni segrete, protette da ogni possibile intrusione

Proprietà desiderabili:

- Riservatezza o confidenzialità: solo mittente e destinatario (che devono essere autenticati) devono essere in grado di comprendere il contenuto del messaggio che deve rimanere segreto
- Integrità: il contenuto della comunicazione non deve essere alterato
- Disponibilità: utenti legittimi devono poter usare i servizi di rete

Comuni scenari di intrusione

Programmi dolosi (virus, worm, etc.) possono introdursi all'interno di un host

- Tramite attachment in posta elettronica
- Scaricando programmi o applicazioni da Internet
- Sfruttando vulnerabilità di programmi già presenti sull'host
- Etc.

I malintenzionati installano malware negli host attraverso internet

Il malware (malicious software) può raggiungere gli host attraverso virus, worm, o cavalli di Troia

- Malware di spionaggio può registrare quanto viene digitato, i siti visitati e informazioni di upload.
- Gli host infettati possono essere “arruolati” in botnet, e usati per lo spamming e per gli attacchi di DDoS.
- Il malware è spesso auto-replicante: da un host infettato può passare ad altri host

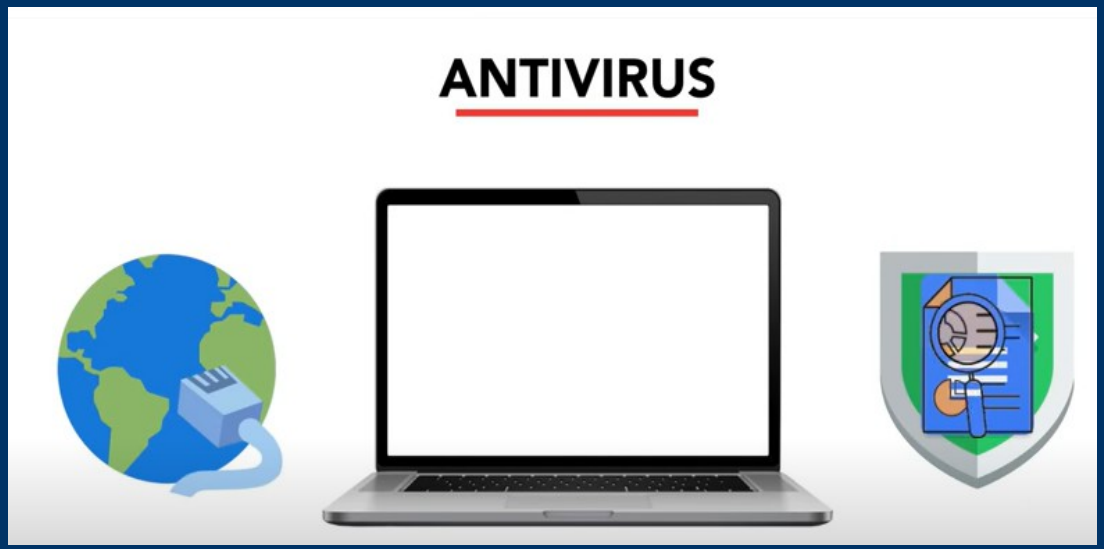
Contromisure

- Antivirus
- Firewall
- Intrusion Detection System
- Crittografia

Antivirus

L'antivirus analizza i **dati interni** al nostro pc.

E' un software che viene installato localmente e necessita di continui aggiornamenti (**è sempre un passo indietro agli attacchi!**)



Antivirus

Quando arriva un pacchetto l'antivirus svolge due azioni principali:

- Analizza il codice dei singoli file che arrivano e li confronta con un archivio che contiene tutti i virus conosciuti. Se trova una corrispondenza blocca quei dati.
- Analizza le azioni che quei file richiedono, cercando delle similitudini con malware già conosciuti. Se trova una qualche similitudine o se si trova davanti ad una richiesta potenzialmente dannosa come l'accesso ad un'area di memoria blocca l'azione.

E' possibile prevenire i virus ovvero impedire che entrino nel sistema ???

FIREWALL

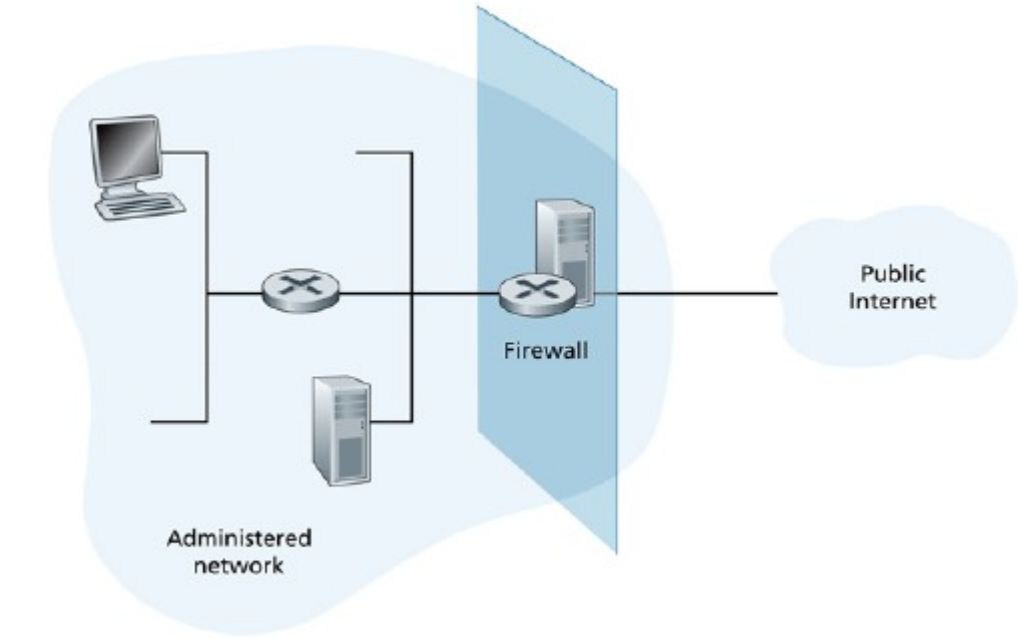
Struttura hardware e software che separa una rete privata dal resto di Internet e consente all'amministratore di controllare e gestire il flusso di traffico tra il mondo esterno e le risorse interne.

A cosa serve?

Permette di controllare i dati che **transitano** tra pc e rete Internet.

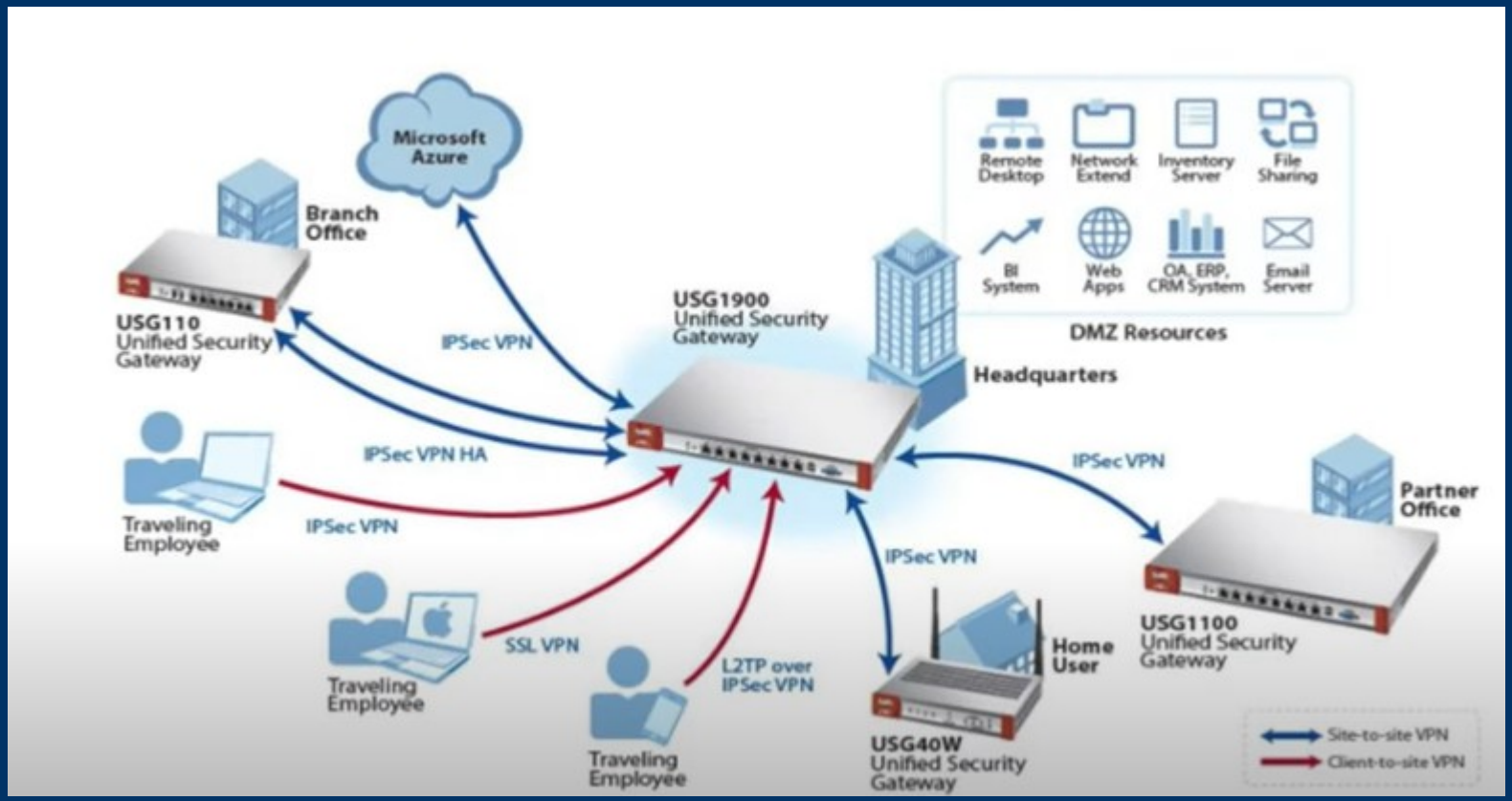
Tutto il traffico verso l'interno e viceversa passa attraverso il firewall

Solo al traffico autorizzato sarà consentito passare



Differenza tra firewall e antivirus

- Il firewall controlla i dati in transito dal nostro pc. Quando arriva una richiesta di collegamento da un server o da un sito web, il firewall si chiede chi è che vuole collegarsi?che tipologia di connessione o di servizio vuole effettuare?quanti dati vuole inviare?A quale porta vuole accedere?


Microsoft Azure
Branch Office
USG110 Unified Security Gateway
IPSec VPN
USG1900 Unified Security Gateway
Remote Desktop
Network Extend
Inventory Server
File Sharing
BI System
Web Apps
OA, ERP, CRM System
Email Server
DMZ Resources
Headquarters
IPSec VPN HA
Traveling Employee
IPSec VPN
IPSec VPN
Partner Office
USG1100 Unified Security Gateway
SSL VPN
Traveling Employee
L2TP over IPSec VPN
Traveling Employee
IPSec VPN
Home User
USG40W Unified Security Gateway
Site-to-site VPN
Client-to-site VPN

Firewall: perché

Consentire solo accessi autorizzati all'interno della rete (una serie di utenti/host autenticati)

Prevenire attacchi di negazione del servizio:

- SYN flooding: l'intruso stabilisce molte connessioni TCP fasulle per non lasciare risorse alle connessioni "vere".

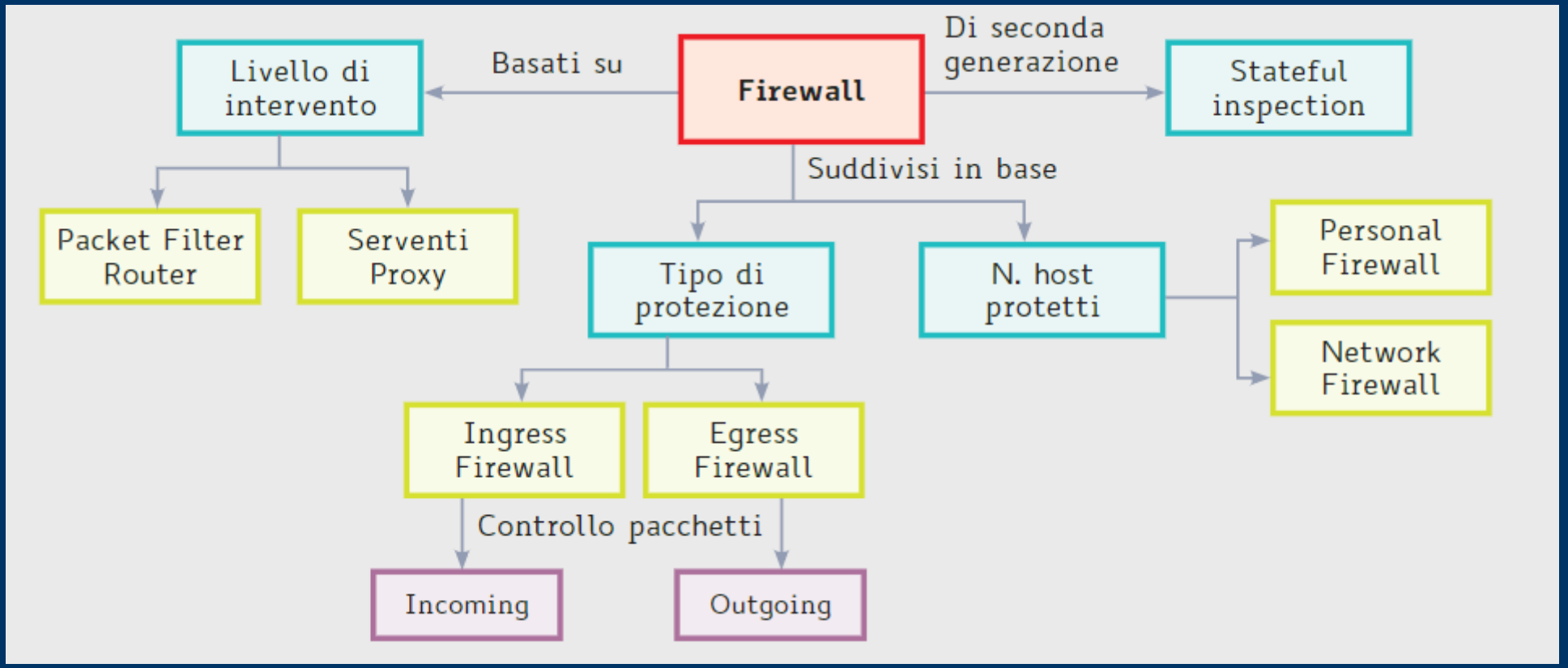
Prevenire modifiche/accessi illegali ai dati interni.

- es., l'intruso può sostituire l'homepage del MIUR con qualcos'altro.

Nella progettazione di un firewall bisogna tenere presente tre principi fondamentali:

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

Classificazione dei firewall



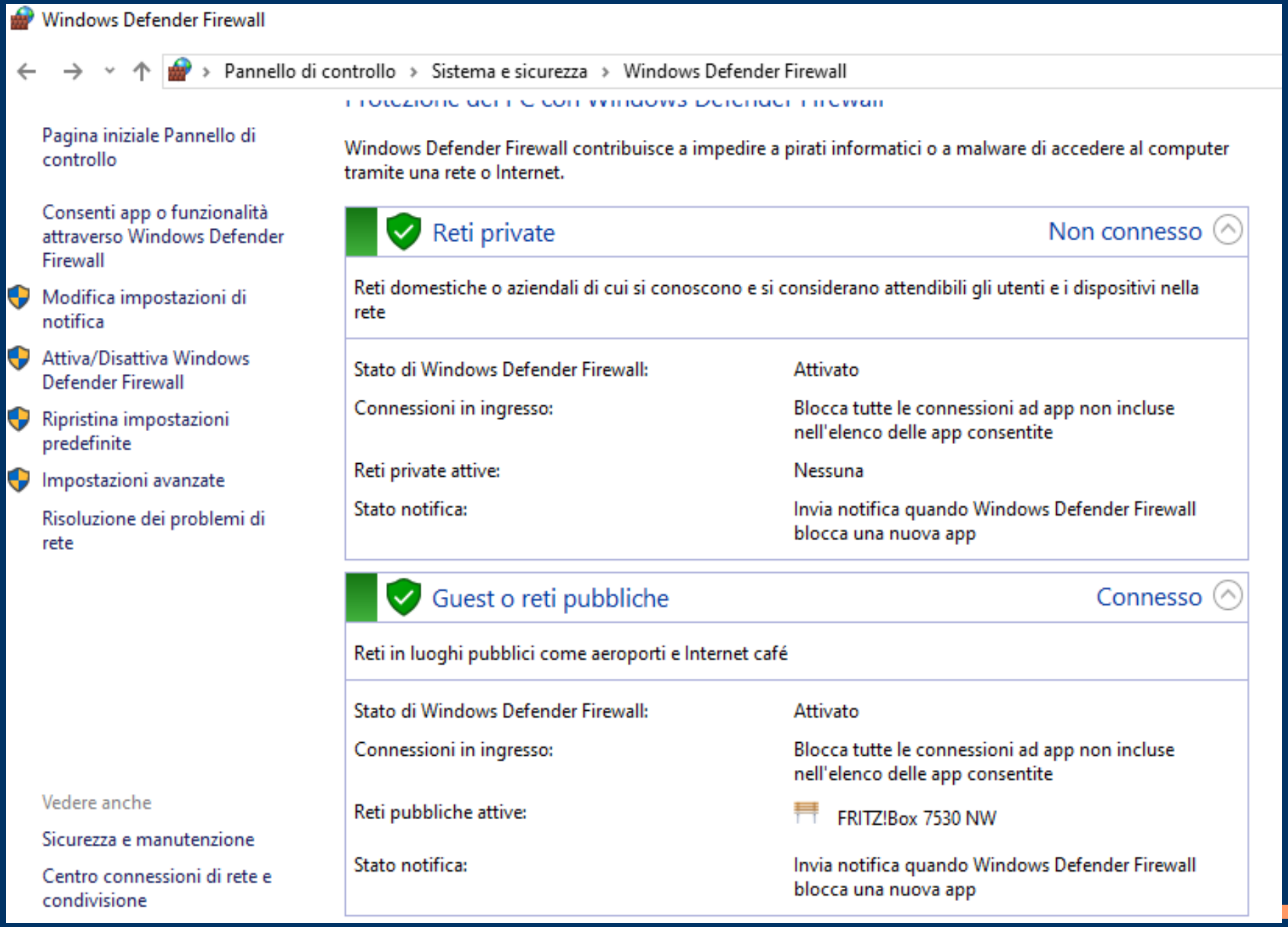
Personal Firewall

Classico Firewall che agisce sul singolo host: controlla i dati in entrata o in uscita dal pc.

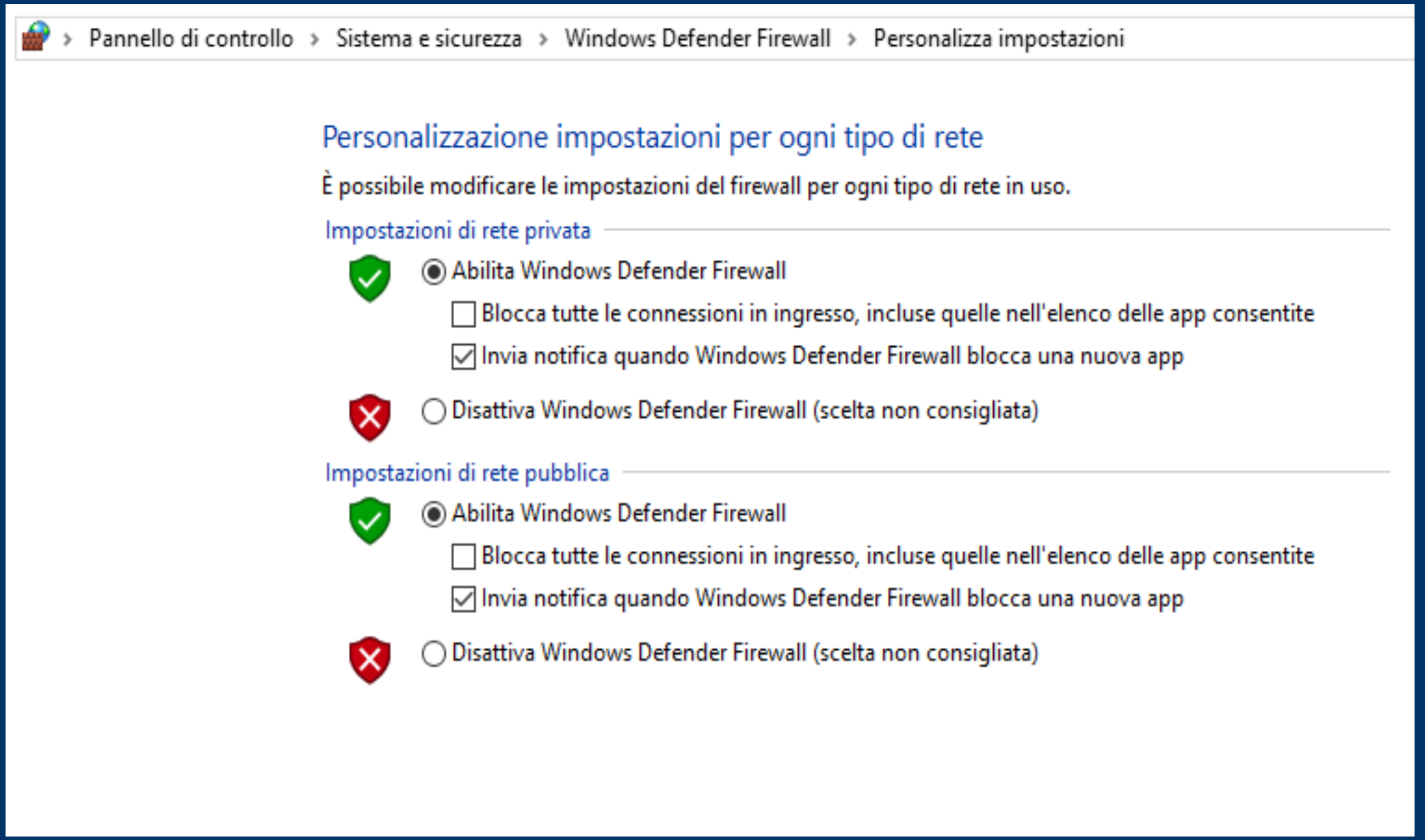
- Lo fornisce il sistema operativo (è solamente software da installare sull'host e protegge esclusivamente il dispositivo sul quale è installato)

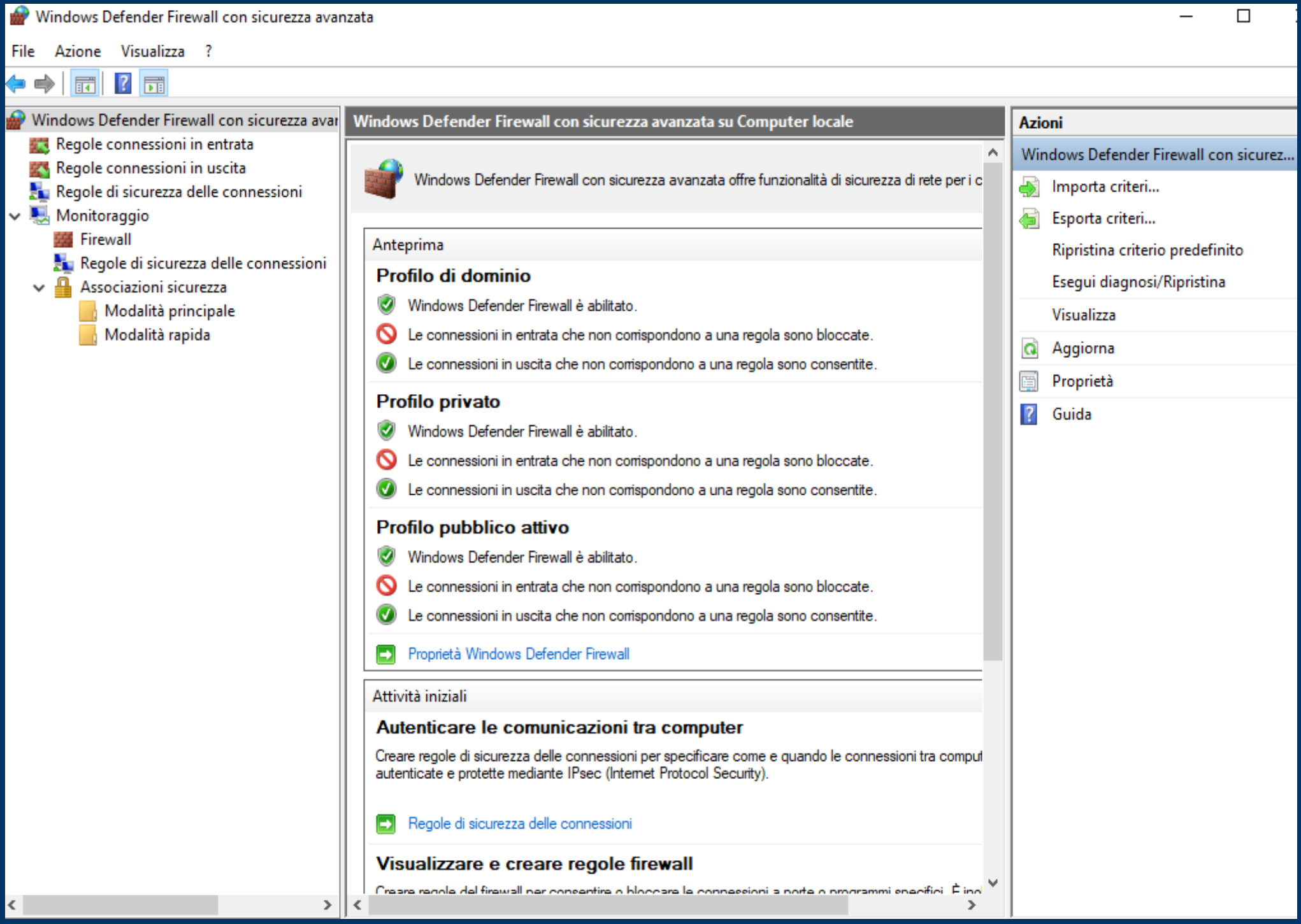
I personal firewall sono utilizzabili solo a scopo personale ma impensabili in una azienda in quanto risulterebbero economicamente non convenienti e inoltre sarebbe difficile implementare una politica comune delle policy, dovendo configurare ogni singolo host manualmente.

Personal Firewall : esempio pratico



Personal Firewall : esempio pratico




Windows Defender Firewall con sicurezza avanzata
File
Azione
Visualizza
?
Windows Defender Firewall con sicurezza avar
Regole connessioni in entrata
Regole connessioni in uscita
Regole di sicurezza delle connessioni
Monitoraggio
Firewall
Regole di sicurezza delle connessioni
Associazioni sicurezza
Modalità principale
Modalità rapida
Windows Defender Firewall con sicurezza avanzata su Computer locale
Windows Defender Firewall con sicurezza avanzata offre funzionalità di sicurezza di rete per i c
Anteprima
Profilo di dominio
Windows Defender Firewall è abilitato.
Le connessioni in entrata che non corrispondono a una regola sono bloccate.
Le connessioni in uscita che non corrispondono a una regola sono consentite.
Profilo privato
Windows Defender Firewall è abilitato.
Le connessioni in entrata che non corrispondono a una regola sono bloccate.
Le connessioni in uscita che non corrispondono a una regola sono consentite.
Profilo pubblico attivo
Windows Defender Firewall è abilitato.
Le connessioni in entrata che non corrispondono a una regola sono bloccate.
Le connessioni in uscita che non corrispondono a una regola sono consentite.
Proprietà Windows Defender Firewall
Attività iniziali
Autenticare le comunicazioni tra computer
Creare regole di sicurezza delle connessioni per specificare come e quando le connessioni tra comput
autenticate e protette mediante IPsec (Internet Protocol Security).
Regole di sicurezza delle connessioni
Visualizzare e creare regole firewall
Azioni
Windows Defender Firewall con sicurez...
Importa criteri...
Esporta criteri...
Ripristina criterio predefinito
Esegui diagnosi/Ripristina
Visualizza
Aggiorna
Proprietà
Guida

Personal Firewall

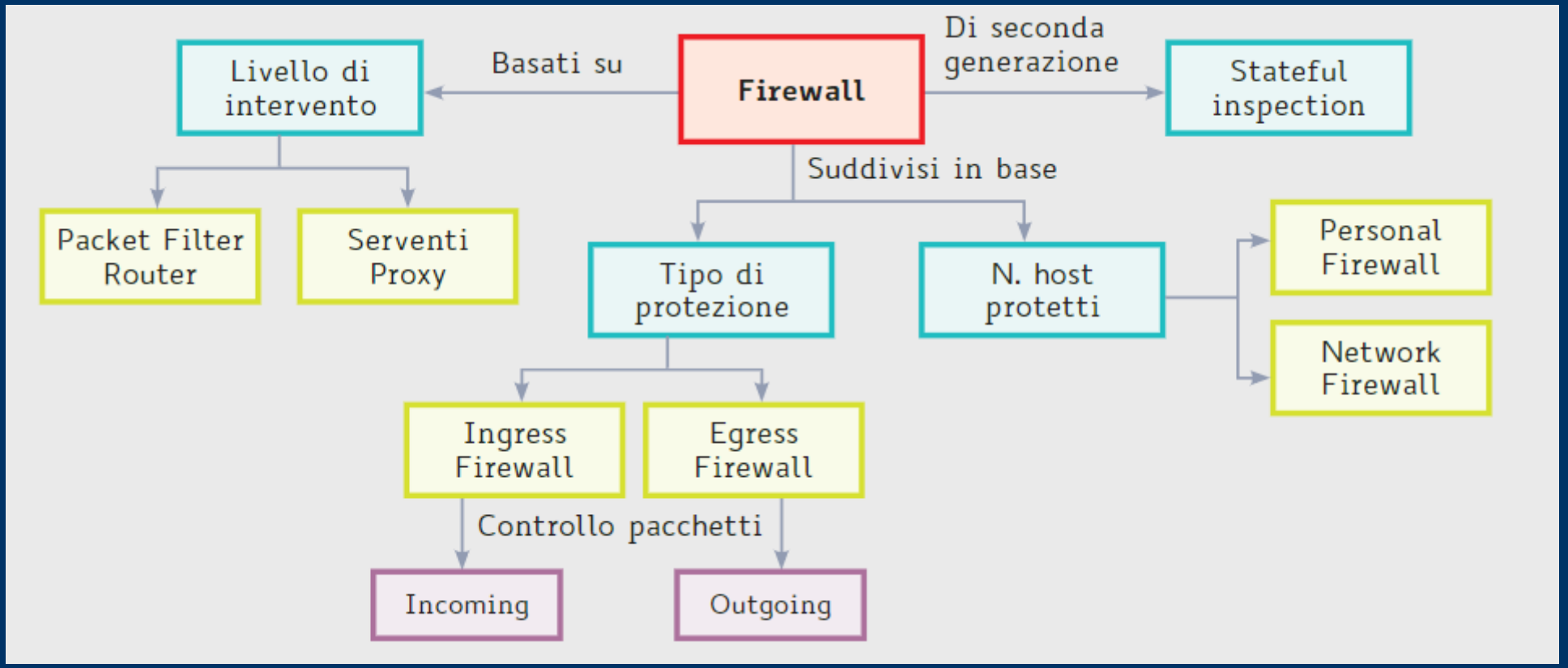
Quando un firewall analizza dei pacchetti applica una serie di regole che permettono o meno il verificarsi di quell'azione. Se, ad esempio, un software esterno alla rete chiede l'accesso a determinati dati o a posizioni di memoria che potrebbero compromettere l'uso del dispositivo il firewall riconosce un comportamento strano e blocca questo accesso. Può anche interagire con l'utente del PC chiedendo conferma di alcune azioni potenzialmente pericolose.

Personal Firewall

Il Personal Firewall, applica una serie di regole standard che sostanzialmente sono il risultato di quello che si è verificato negli anni. Ad esempio, immaginiamo che la porta xxx non appartiene a nessun servizio noto e non viene mai utilizzata per lo scambio dati.
Se ad un certo momento un software chiede di accedere proprio da quella porta, il firewall tenderà a bloccare l'accesso. Qual è lo svantaggio?

Può capitare che un firewall avverta un utente di un possibile pericolo, quando in realtà, la situazione in esame non presenta pericoli reali (falso allarme). In questi casi un utente inesperto potrebbe impedire una connessione utile al funzionamento del proprio PC!

Classificazione dei firewall



Network Firewall

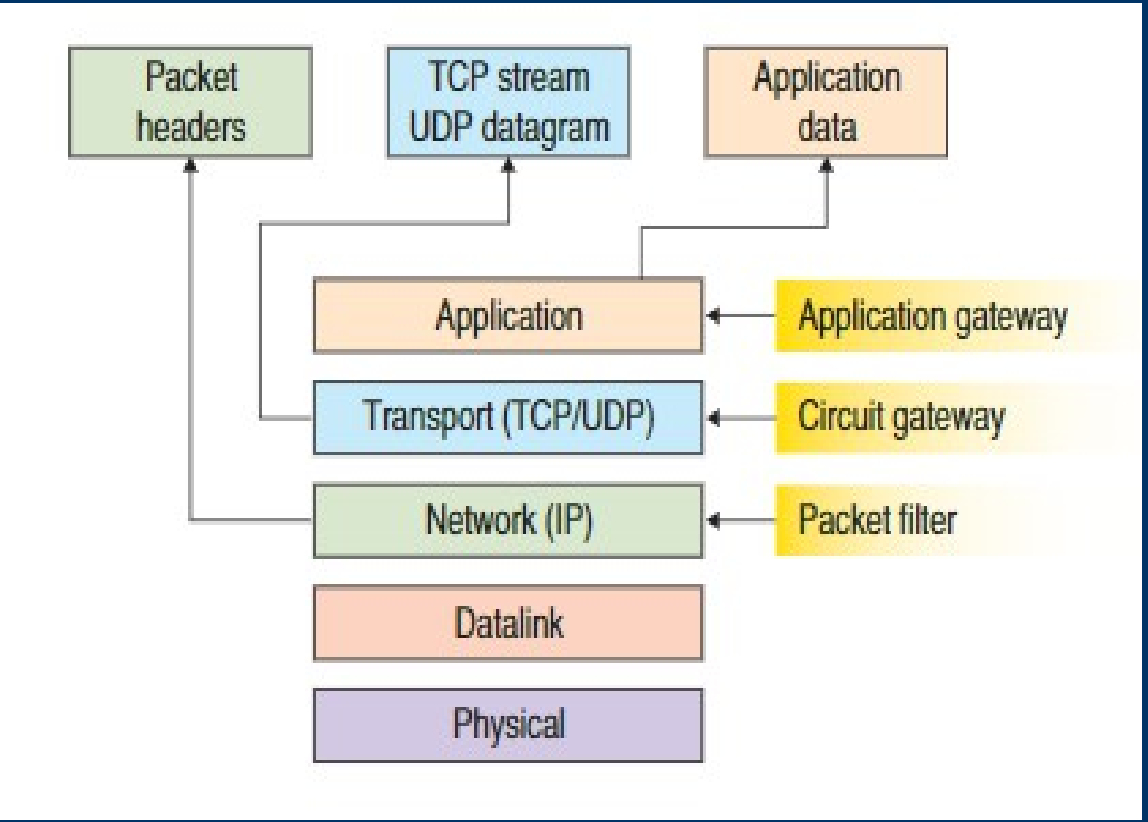
Sono i classici firewall aziendali dove una o più macchine sono dedicate al filtraggio di tutto il traffico da e per una rete locale e solo il traffico autorizzato può attraversare il firewall.

A seconda del livello della pila TCP/IP nel quale si fanno i controlli i network firewall si classificano:

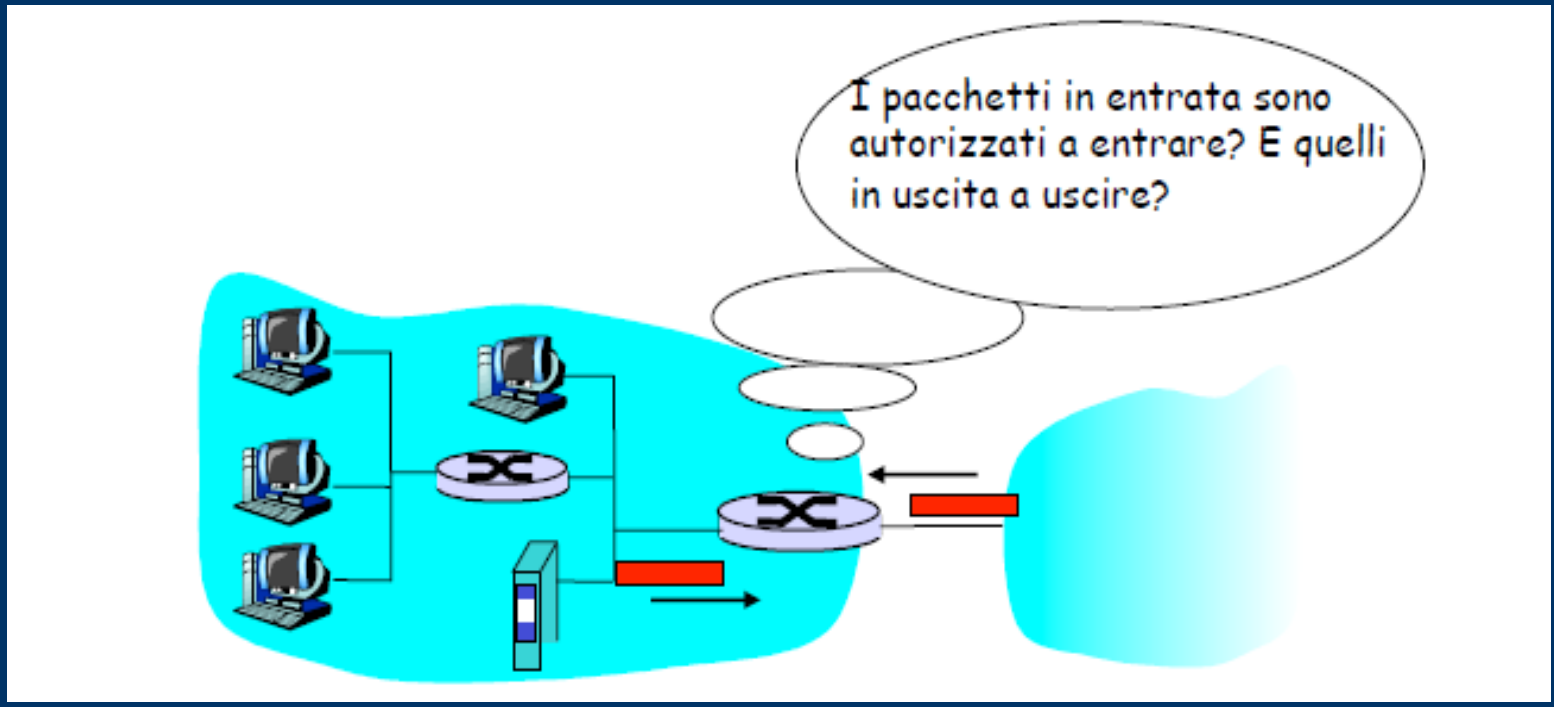
packet-filtering router

circuit gateway

proxy server



Packet Filtering



Una rete LAN è collegata a Internet mediante un router.

Il router è responsabile del filtraggio dei pacchetti e determina quali pacchetti devono essere bloccati o quali possono passare.

Packet Filtering

Un packet filtering router analizza le informazioni contenute nell'header TCP/IP a livello di rete e di trasporto (packet inspection) per individuare:

indirizzo IP del mittente o del destinatario;

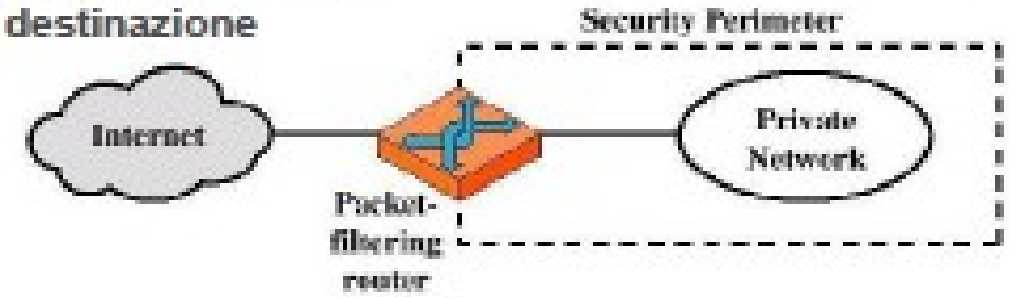
indirizzo MAC sorgente o di destinazione;

numero di porta verso cui è destinato il pacchetto;

protocollo da utilizzare (TCP, UDP, ICMP).

Packet Filtering

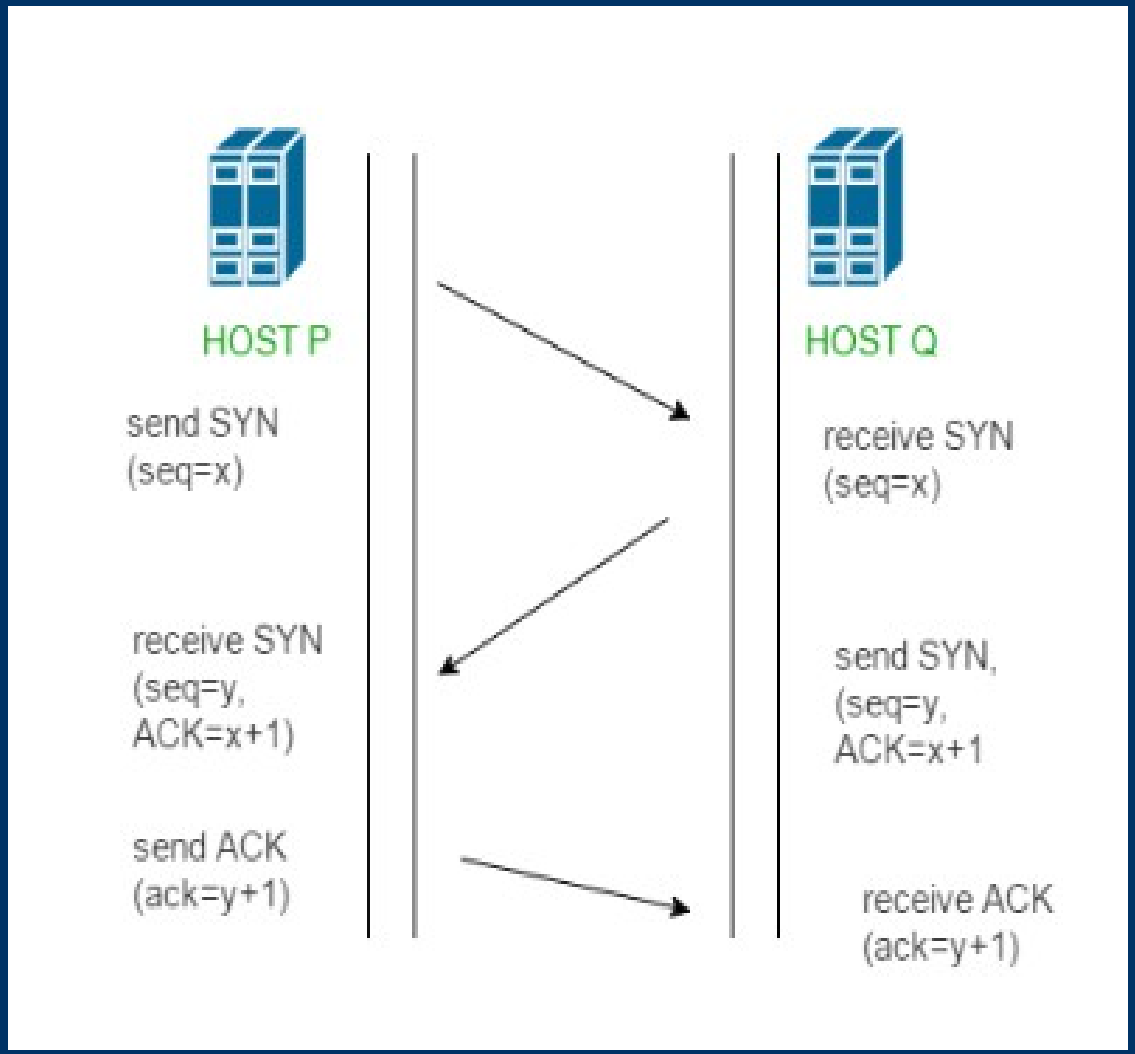
- Esamina unicamente l'header del pacchetto, es.:
  - Link layer:
    - Interfaccia fisica di ingresso o uscita
    - MAC address sorgente / destinazione
  - IP layer:
    - Indirizzi sorgente / destinazione
    - Protocollo trasportato (ICMP, TCP, UDP, AH, ESP, ...)
    - Opzioni IP (ECN, TOS, ...)
  - Transport layer:
    - TCP flags (SYN, ACK, FIN, RST, ...)
    - Porte sorgente / destinazione



Packet Filtering: esempi

Politica	Configurazione del firewall
Nessun accesso Web all'esterno.	Bloccare tutti i pacchetti IP uscenti con porta dest. 80 e qualsiasi indirizzo IP dest.
Nessuna connessione TCP entrante, eccetto quelle dirette al solo server Web pubblico dell'organizzazione	Bloccare tutti i pacchetti TCP SYN entranti verso quals.indirizzo IP 130.207.244.203, con porta destinazione 80
Evitare che le radio Web intasino la banda disponibile	Bloccare tutti i pacchetti UDP entranti, eccetto i pacchetti DNS
Evitare che la rete possa essere usata per un attacco DoS	Bloccare tutti i pacchetti ICMP ping diretti a un indirizzo broadcast (es. 130.207.255.255).
Evitare che la rete possa essere rilevata tramite Traceroute	Bloccare tutti i messaggi ICMP con TTL esaurito uscenti

TCP - Tree Way Handshake



Packet Filtering

Il firewall decide se il pacchetto può essere accettato o meno attraverso un algoritmo di scelta che si basa su una lista di regole (applicate in ordine di priorità) precedentemente definite.

Le ACL contengono, in questa tipologia di firewall, le regole da applicare ai pacchetti in transito.

Packet Filtering – Vantaggi

I principali vantaggi nell'utilizzo di un packet filtering router sono:

trasparenza: l'utente non si accorge della presenza del firewall dato che non lavora a livello applicativo e quindi non ostacola in alcun modo il normale utilizzo della rete;

velocità: effettuando minori controlli rispetto agli altri firewall che descriveremo in seguito risulta essere il più veloce e semplice da implementare;

immediatezza: tramite la definizione di una singola regola si può difendere un'intera rete dai pericoli derivanti da quel tipo di traffico;

gateway-only: non sono richieste ulteriori configurazioni aggiuntive per i client;

topologia della rete interna invisibile dall'esterno: se viene aggiunto un NAT, dall'esterno l'unico host visibile è il gateway.

Packet Filtering – Svantaggi

Gli svantaggi nell'uso di un packet filtering router sono:

basso livello: è veloce ma non è in grado di elaborare le informazioni dei livelli superiori a quello di rete e quindi non è in grado di bloccare attacchi mirati a vulnerabilità di una specifica applicazione;

mancanza di servizi aggiuntivi: non permettono la gestione di servizi quali l'autenticazione, l'HTTP object caching e il filtraggio di URL e dei contenuti delle pagine web;

logging limitato: analizzando solo i pochi campi presenti nell'header del pacchetto genera dei file di log con poche informazioni, insufficienti per verificare se il firewall compie sempre il proprio dovere;

vulnerabile allo spoofing: dato che vengono filtrati i pacchetti in base alla loro provenienza i casi di IP Spoofing non vengono riconosciuti;

testing complesso: è lungo e complicato effettuare le prove che ne verifichino il corretto funzionamento.

Packet Filtering – senza memoria?

- Filtraggio tradizionale: strumento poco flessibile
  - Ammette pacchetti che "non hanno senso," es. dest port = 80, bit ACK anche se non vi è alcuna connessione TCP.

azione	source address	indirizzo dest	protocollo	porta sorgente	porta destinaz	bit di flag
consenti	Al di fuori di 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *Filtraggio con memoria dello stato:* tiene traccia dello stato di tutte le connessioni TCP
  - Traccia l'impostazione del collegamento (SYN) e la terminazione (FIN): può così determinare se i pacchetti in entrata o in uscita "hanno senso" ovvero sono scambiati all'interno di connessioni esistenti

Stateful Inspection

- Nuova colonna di verifica della connessione + tabella delle connessioni attive

azione	indirizzo sorgente	indirizzo dest	Protoc	porta sorgente	porta destinaz.	bit di flag	controllo conness.
consenti	222.22/16	al di fuori di 222.22/16	TCP	> 1023	80	qualsiasi	
consenti	al di fuori di 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
consenti	222.22/16	al di fuori di 222.22/16	UDP	> 1023	53	---	
consenti	al di fuori di 222.22/16	222.22/16	UDP	53	> 1023	----	X
blocca	tutto	tutto	tutto	tutto	tutto	tutto	

Stateful Inspection - vantaggi

buon rapporto prestazioni/sicurezza: offre un ottimo compromesso fra prestazioni e sicurezza dato che effettua meno controlli durante la connessione ed è più affidabile di un filter router;

protezione da IP spoofing e session hacking: dato che il controllo viene effettuato sulla connessione è molto più difficile riuscire a violarlo;

tutti i vantaggi del packet filtering: ha anche tutti gli altri vantaggi dei packet filter dato che ne è una diretta evoluzione (immediatezza, possibilità di natting, gateway-only ...).

Statefull Inspection - svantaggi

protocollo unico: sfruttando molte delle caratteristiche proprie del protocollo TCP risulta difficilmente utilizzata all'interno di altre infrastrutture di rete;

servizio di auditing limitato: come per il packet filter le informazioni che registra nei file di log sono ancora insufficienti per una completa diagnostica;

mancanza di servizi aggiuntivi: lavorando ai livelli inferiori come il packet filter non permette servizi aggiuntivi come la gestione delle autenticazioni e il filtraggio dei contenuti;

testing complesso: è lungo e complicato effettuare le prove che ne verifichino il funzionamento e la sua corretta configurazione.

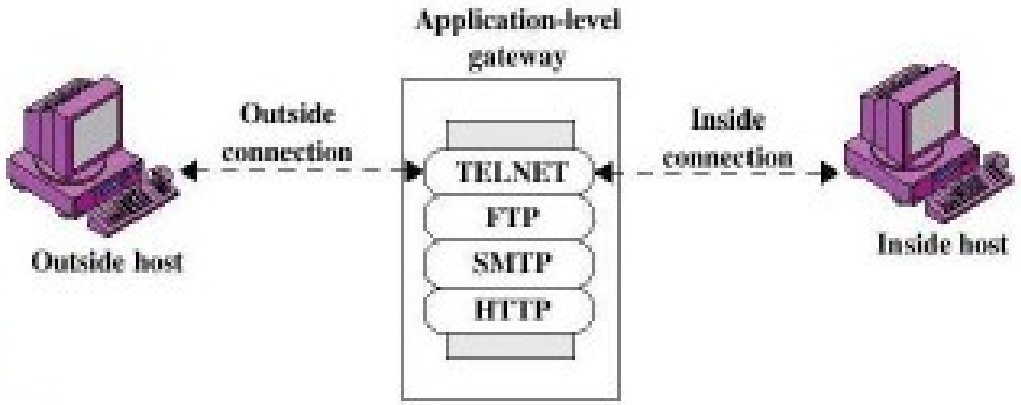
Packet Filtering - Efficacia

Esistono comunque tipi di intrusioni che sono difficili da identificare sfruttando le informazioni base sull'header del pacchetto perché gli attacchi sono indipendenti dal servizio:

- attacchi che falsificano il source address IP (IP Spoofing): tali attacchi possono essere sconfitti scartando semplicemente ciascun pacchetto con un source address IP interno ma proveniente da una delle interfacce del router che sono rivolte verso l'esterno;
- attacchi source routing: possono essere sconfitti semplicemente scartando tutti i pacchetti che contengono source route nel campo option del datagramma IP;
- attacchi con piccoli frammenti: un attacco con piccoli frammenti può essere sconfitto scartando tutti i pacchetti in cui il campo protocol type sia pari a 6 (cioè TCP) e l'IP fragment-offset sia pari a 1.

Application Level Gatway

- Anche chiamato *proxy server*
  - In questo ruolo può svolgere anche altre funzioni, es. caching
- Un ALG è un "man in the middle buono" che agisce da server nei confronti del client, e propaga la richiesta agendo da client nei confronti del server effettivo



Application Level Gatway - funzionamento

Vediamo praticamente come avviene il funzionamento in presenza di un proxy:

1. un host della LAN invia al firewall una richiesta di connessione con un sito web;

2. il proxy raccoglie la richiesta, controlla il set di regole per assicurarsi che essa sia lecita, per poi rigenerarla e inviarla al server;

3. quest'ultimo riceve la richiesta del proxy come se fosse partita dall' host e invia a esso la risposta;

4. risposta che viene nuovamente analizzata dal proxy prima di essere inviata all'host interno.

Application Level Gatway - vantaggi

controllo completo: dato che utilizza anche le informazioni contenute nel body, effettua un doppio controllo, sia quando viene inviata la richiesta sia quando si riceve la risposta;

log dettagliati: avendo a disposizione anche le informazioni di livello applicativo produce dei file di log molto accurati;

nessuna connessione diretta: tutti i dati in transito sono analizzati e ricostruiti: tentativi di buffer-overflow o simili sono intercettati e non vengono inoltrati all'host interno;

sicurezza anche in caso di crash: nel caso di un crash del proxy la LAN risulta isolata e quindi inaccessibile dall'esterno rimanendo protetta;

supporto per connessioni multiple: è in grado di gestire connessioni separate che appartengono alla stessa applicazione;

user-friendly: è semplice configurare le regole di filtraggio rispetto a quelle di un packet filtering router;

Application Level Gatway - vantaggi

user-friendly: è semplice configurare le regole di filtraggio rispetto a quelle di un packet filtering router;

autenticazione e filtraggio dei contenuti: offre anche il servizio autenticazione dell'utente e il riconoscimento dei contenuti;

cache: effettua il caching delle pagine web e quindi offre un ulteriore servizio liberando la rete da traffico inutile nel caso di richiesta della stessa pagina (lo analizzeremo più avanti quando faremo il protocollo HTTP).

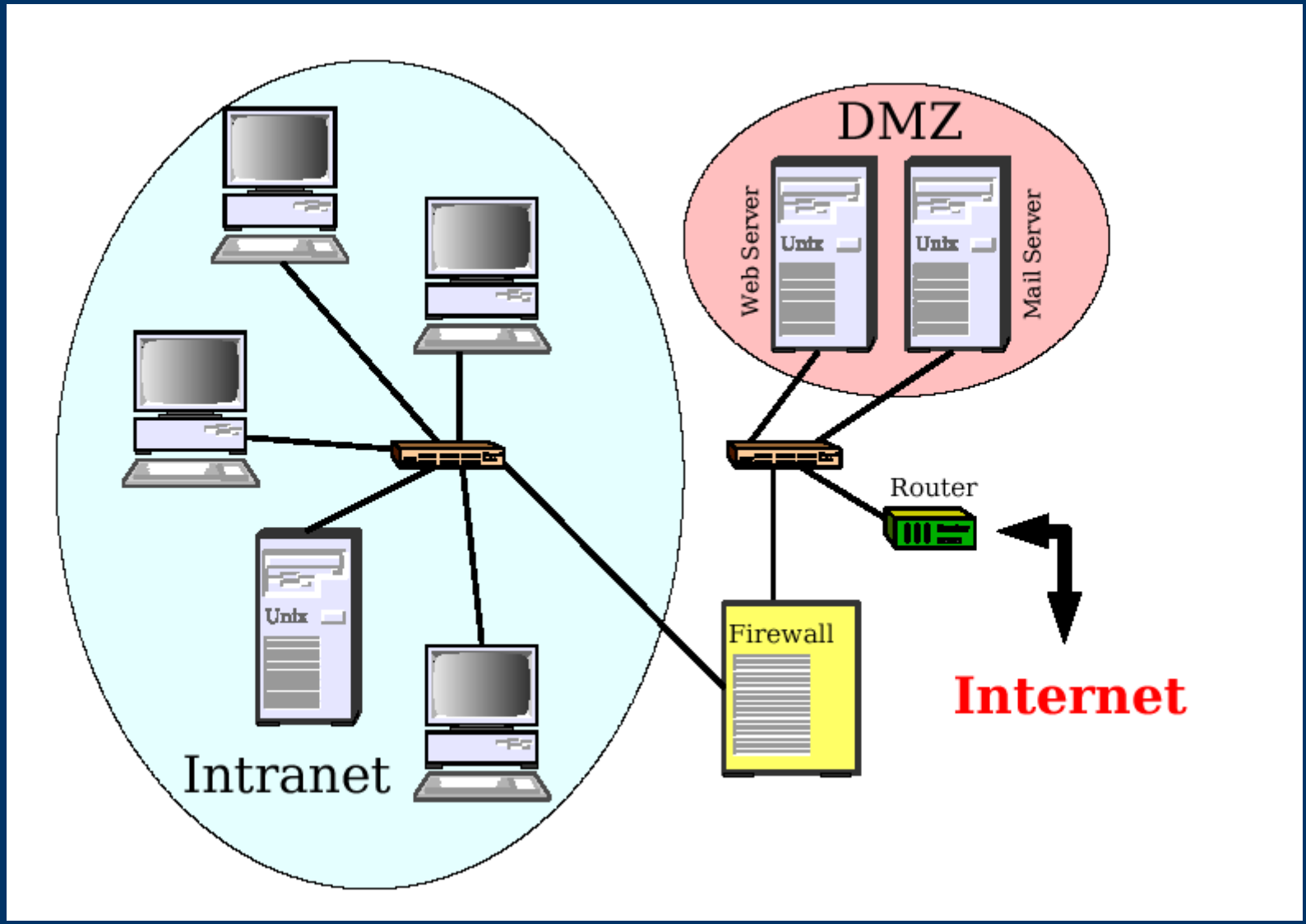
Application Level Gatway - svantaggi

è poco trasparente: richiede che ogni computer della LAN interna sia configurato per utilizzare il proxy;

richiede un proxy per ogni applicazione: è necessario dedicare un proxy a ogni servizio che si ha necessità di far passare attraverso il firewall e, data la dinamicità con la quale vengono offerti servizi in rete, è necessario il suo continuo aggiornamento;

ha basse performance: la gestione della connessione attraverso il proxy richiede molto lavoro per la CPU e quindi ha prestazioni molto inferiori rispetto ai firewall delle generazioni precedenti.

Demilitarized Zone - DMZ



Bastion Host

Bastion host

Con il termine **bastion host** indichiamo l'host configurato per respingere attacchi contro la rete interna e più in generale tutti quegli host che fungono da firewall critici per la sicurezza della rete stessa.
Il bastion host viene sempre associato a un packet filter con politiche di sicurezza opportunamente configurate. Possiede in genere le seguenti caratteristiche:

Bastion host
Quando l'application proxy rappresenta l'unico punto di contatto con la rete esterna prende il nome di bastion host, poiché è appositamente corazzato e protetto per resistere agli attacchi.

- unico calcolatore della rete interna raggiungibile da Internet e massicciamente protetto;
- dotato di software strettamente necessario, il più possibile privo di bug utilizzabili come vie di accesso preferenziali;
- proxy server in ambiente isolato (chrooting);
- file system a sola lettura;
- numero minimo dei servizi e nessun account utente;
- salvataggio e controllo dei log;
- eliminazione dei servizi non fidati e disattivazione del source routing.

DMZ – cos'è

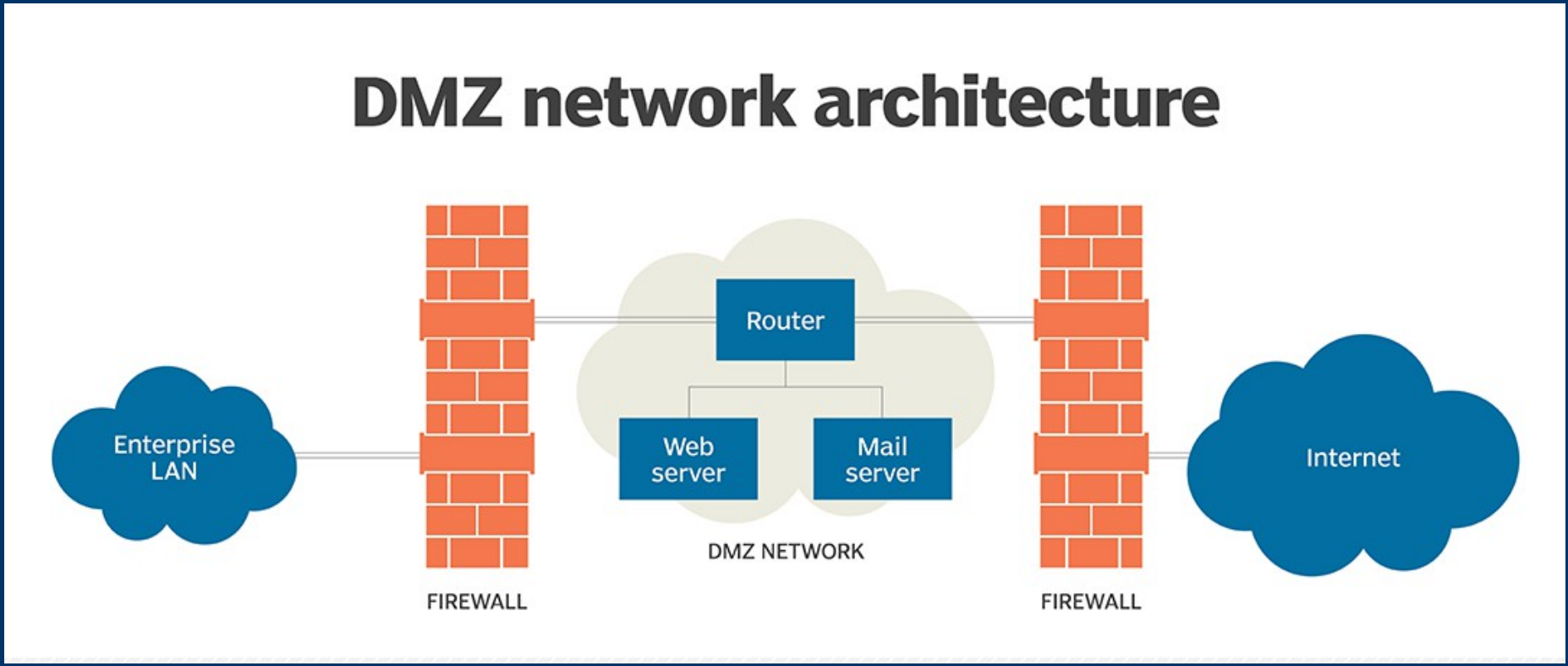
La DMZ è una zona che fa parte della rete LAN e che è progettata per fornire servizi alla rete Internet:

- server web
- server di posta elettronica
- Dns

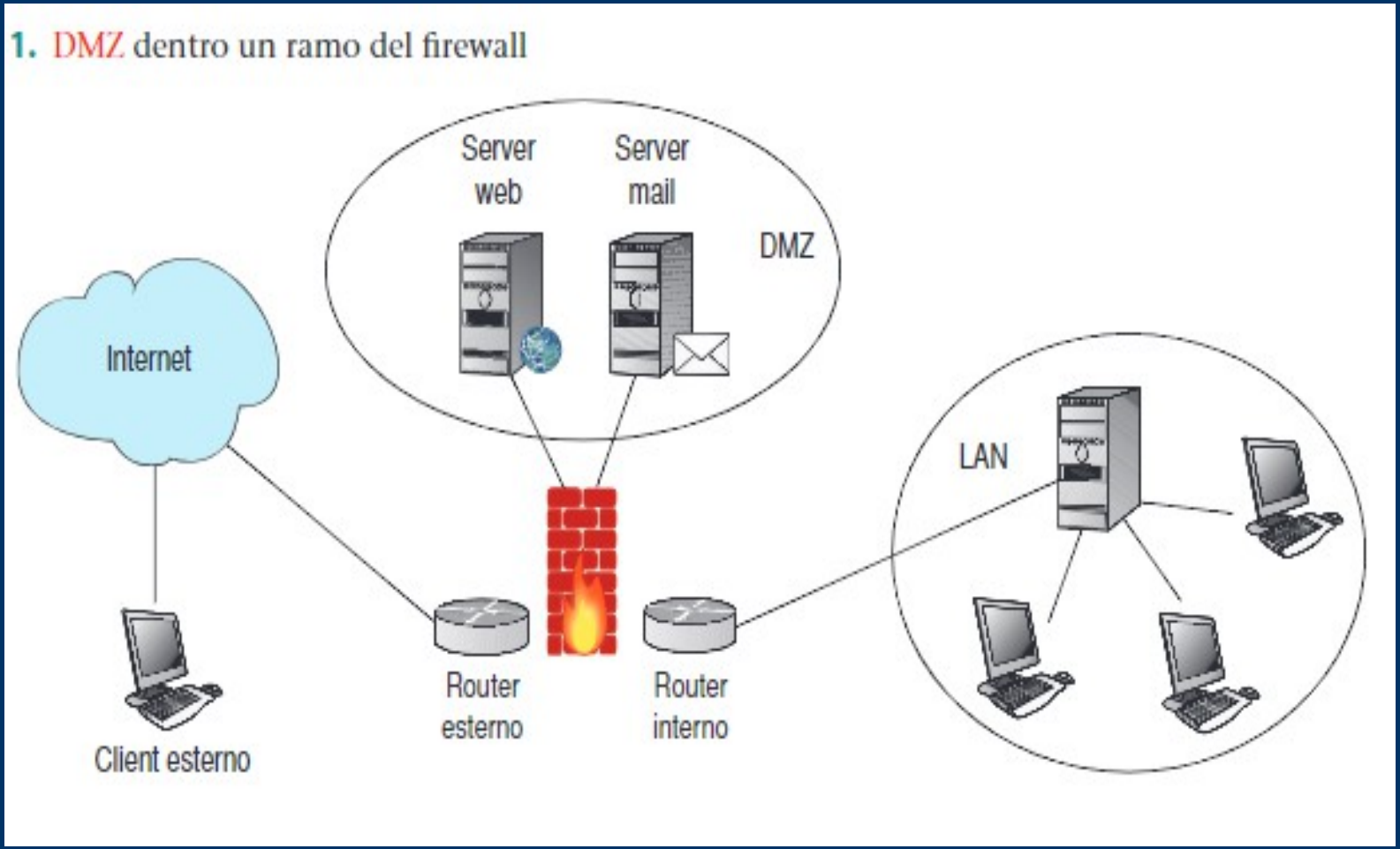
Per questo motivo, i criteri di sicurezza con la quale deve essere gestita sono differenti rispetto a tutta la rete LAN. Criteri di sicurezza meno stringenti.

DMZ cuscinetto

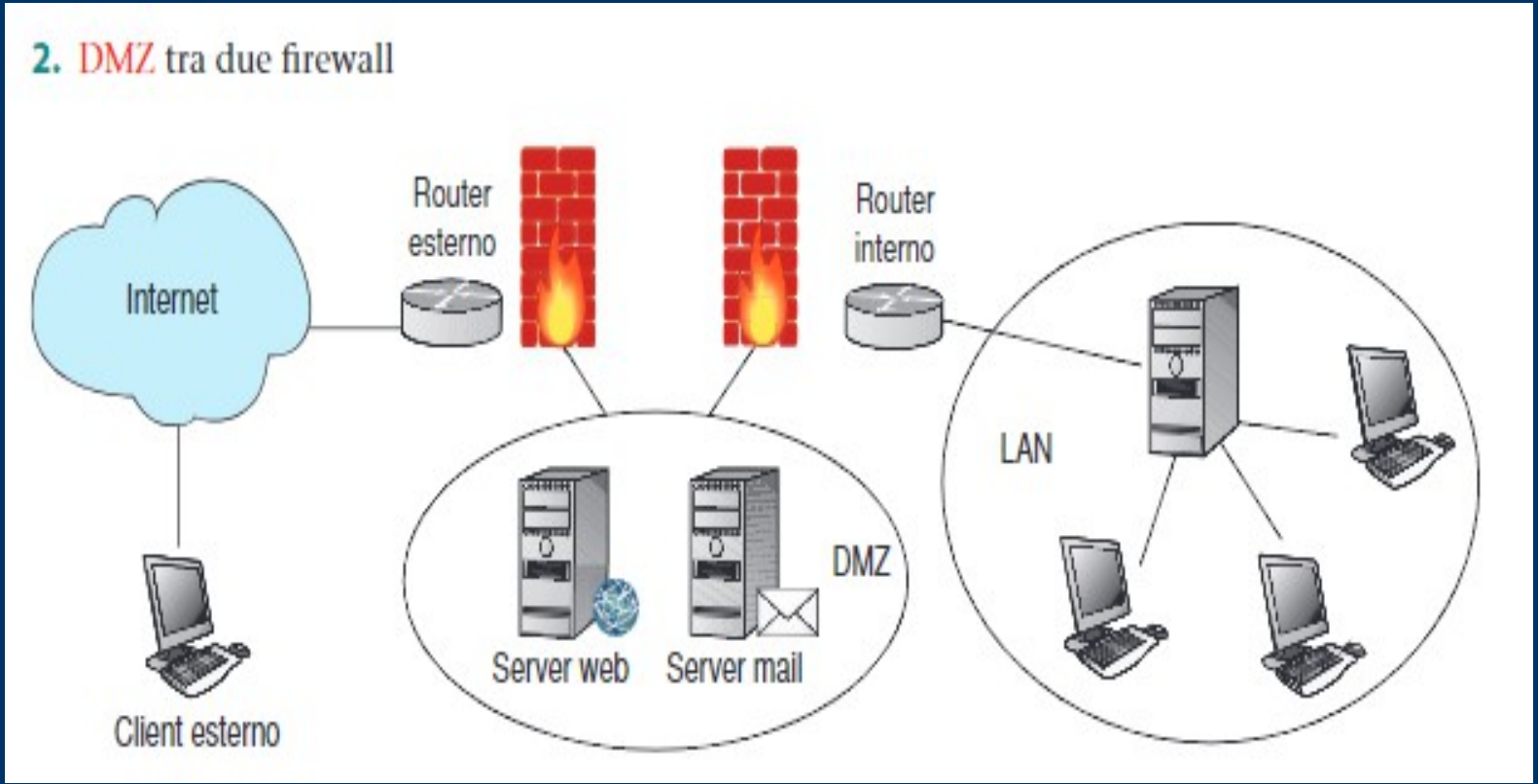
- Posso inserire un ulteriore livello di sicurezza: utilizzo due firewall



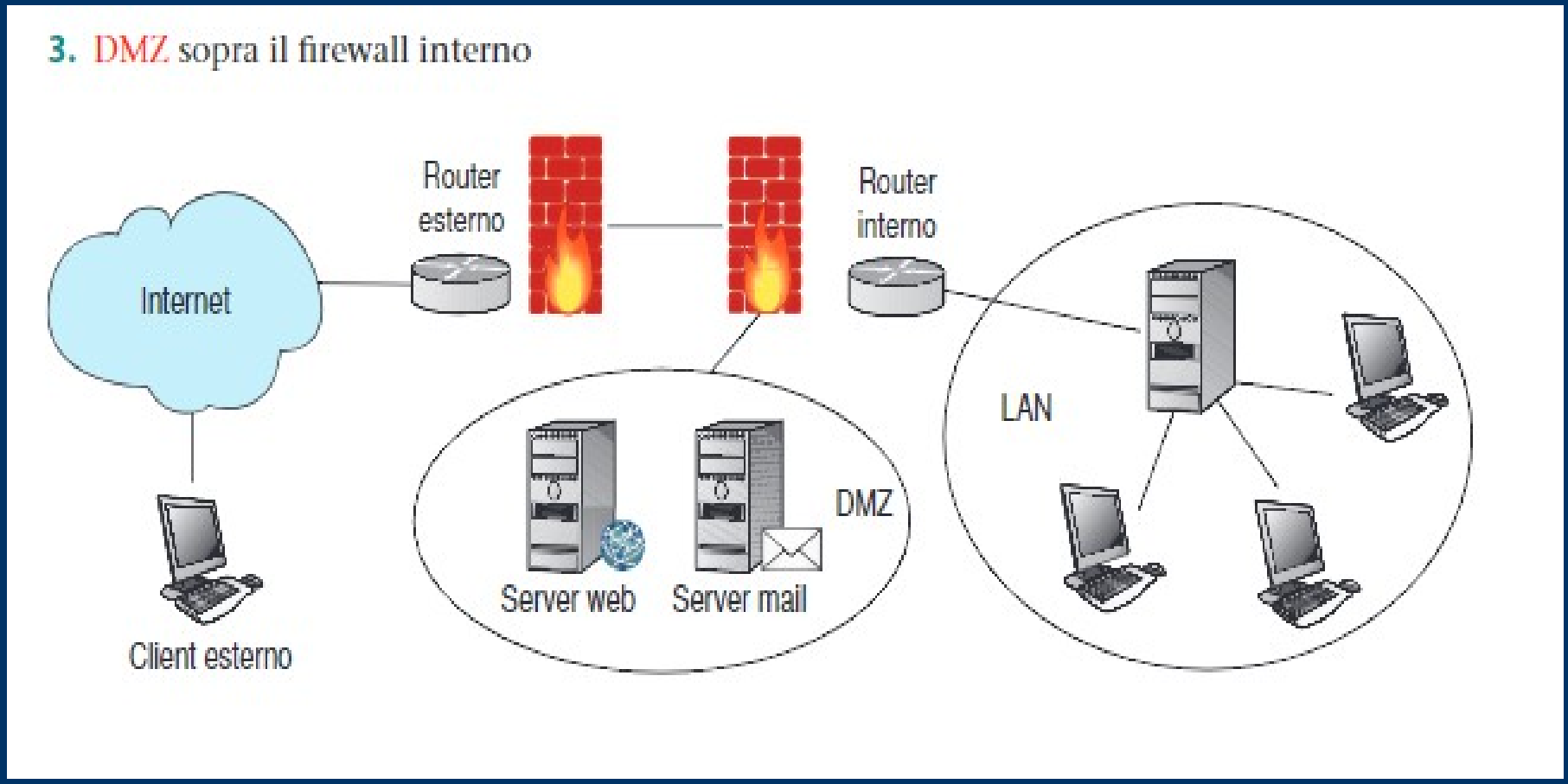
DMZ - possibili architetture



DMZ - possibili architetture



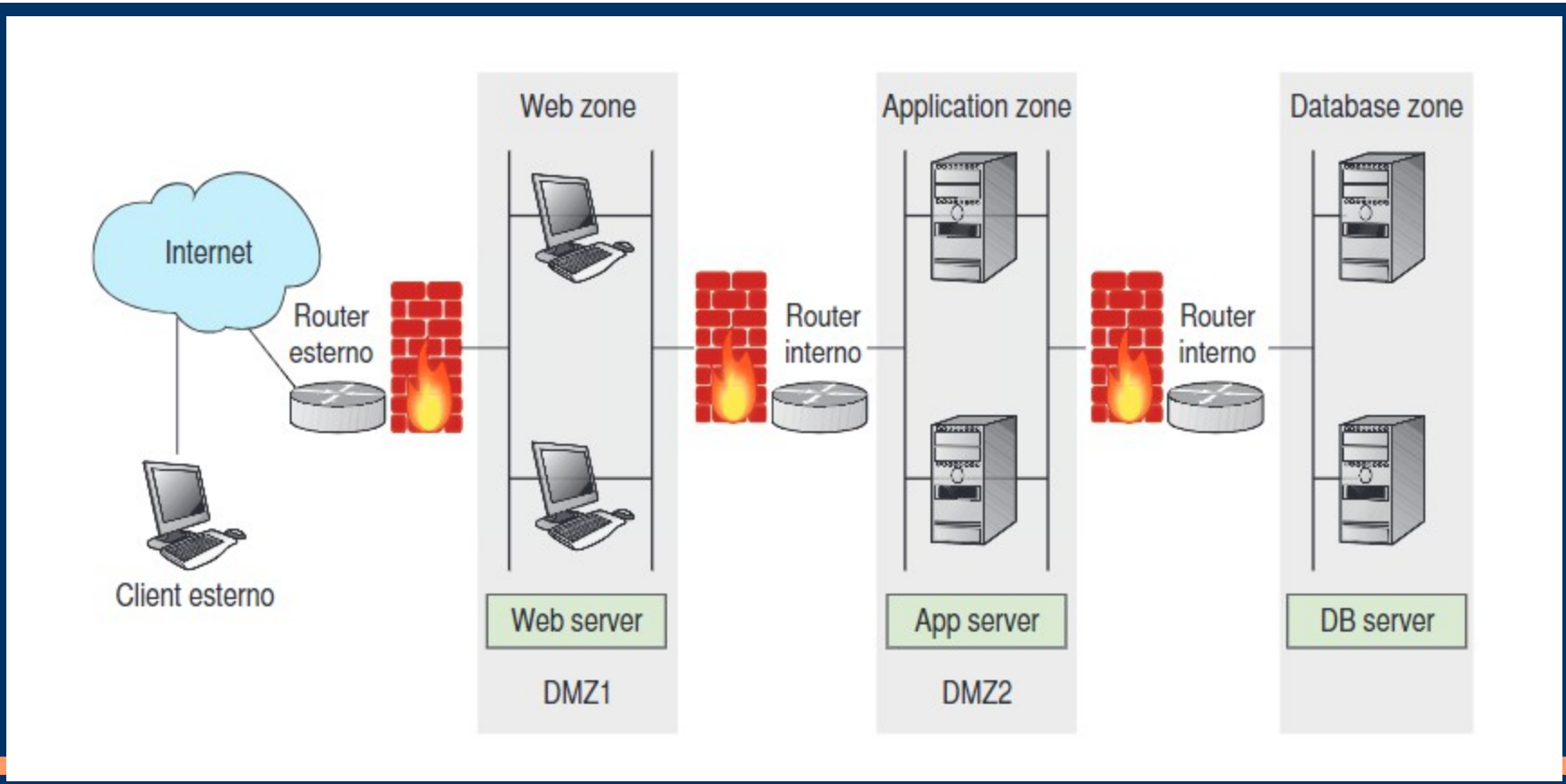
DMZ - possibili architetture



DMZ - possibili architetture

Utilizzando un'architettura 3-tier (n-tier), dove sono separati web server, application server e il database, è buona norma mettere il web server verso l'esterno e collocare nella DMZ l'application server, che di solito ospita la business logic e si collega al DB, che rigorosamente deve essere all'interno della LAN.

> Nelle ditte in cui la sicurezza dei dati è vitale è possibile introdurre un sistema di stratificazione della DMZ inserendo anche più di due firewall e più DMZ.



DMZ cuscinetto - vantaggi

- **Controllo di accesso**. Una rete DMZ fornisce il controllo dell'accesso ai servizi esterni al perimetro di rete LAN a cui si accede da Internet. Contemporaneamente introduce un livello di segmentazione della rete che aumenta il numero di ostacoli che un utente deve superare prima di ottenere l'accesso alla rete privata. In alcuni casi, una DMZ include un server proxy, che centralizza il flusso del traffico Internet interno, solitamente dei dipendenti, e semplifica la registrazione e il monitoraggio di tale traffico.
- **Prevenzione della ricognizione della rete**. Una DMZ impedisce a un utente malintenzionato di individuare potenziali obiettivi all'interno della rete. Anche se un sistema all'interno della DMZ viene compromesso, il firewall interno protegge comunque la rete privata, separandola dalla DMZ. Questa configurazione rende più difficile la ricognizione attiva esterna. Sebbene i server nella DMZ siano esposti pubblicamente, sono supportati da un altro livello di protezione interno.

DMZ cuscinetto

- **Protezione contro lo spoofing del protocollo Internet (IP)** . In alcuni casi, gli aggressori tentano di aggirare le restrizioni del controllo di accesso effettuando lo spoofing di un indirizzo IP autorizzato per impersonare un altro dispositivo sulla rete. Una DMZ può bloccare potenziali spoofer IP, mentre un altro servizio sulla rete verifica la legittimità dell'indirizzo IP testando se è raggiungibile.

DMZ – a cosa servono

Le reti DMZ rappresentano una parte importante della sicurezza delle reti aziendali quasi da quando vengono utilizzati i firewall. Vengono utilizzati per ragioni simili: proteggere i sistemi e le risorse organizzative sensibili. Le reti DMZ vengono spesso utilizzate per quanto segue:

- isolare e mantenere i potenziali sistemi bersaglio separati dalle reti interne;
- ridurre e controllare l'accesso a tali sistemi da parte di utenti esterni;
- ospitare risorse aziendali per renderne disponibili alcune ad utenti esterni autorizzati.