Firewall

Protezione perimetrale e sistemi anti intrusione

Dispositivi di sicurezza

- Internet è un ambiente poco sicuro. Si rischia di subire ogni tipo di frode.
- Per l'amministratore della rete di una organizzazione ci sono
  - le persone autorizzate ad accedere alle risorse della rete
  - le persone che non devono assolutamente accedere alle risorse.
- Come in tutti gli edifici che ospitano uffici, c'è un solo punto di entrata-uscita, dal quale transitano sia le persone che lavorano per l'azienda sia gli utenti estranei all'azienda, ed entrambi i soggetti vengono controllati all'entrata e all'uscita.
- Anche in una rete di calcolatori, c'è un solo punto di accesso, dove il traffico entrante/uscente è controllato da dispositivi di sicurezza che provvedono a registrare il passaggio, scartare il traffico non autorizzato e smistare quello autorizzato.
- Questi dispositivi sono:
  - Firewall,
  - intrusion detection system (IDS),
  - intrusion prevention system (IPS).

Firewall

- Un **firewall è una combinazione di hardware e software che isola la rete interna di una organizzazione dalla rete Internet**, consentendo ad alcuni pacchetti di passare e bloccando altri.
- Un firewall permette all'amministratore di una rete di controllare il traffico, in entrambe le direzioni, tra il mondo esterno e le risorse interne.

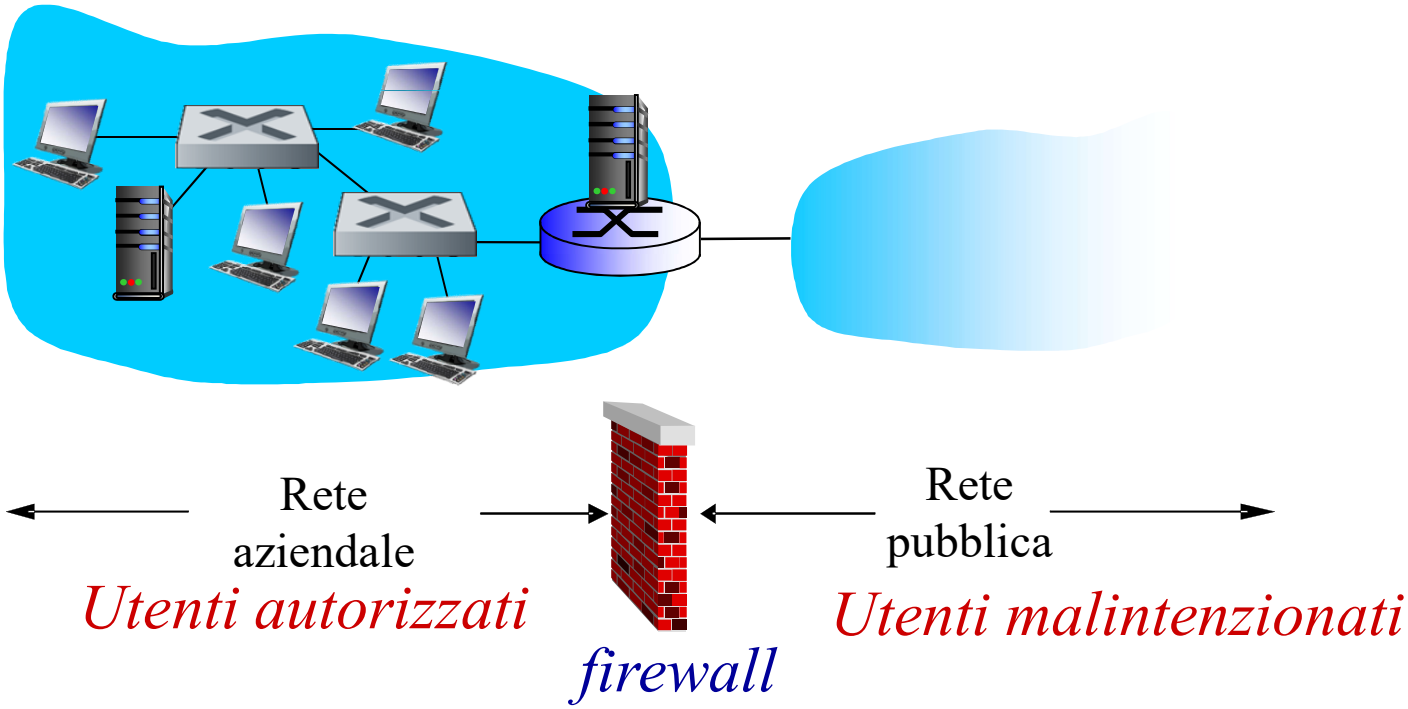
Scopi del firewall:

1) Tutto il traffico dall'esterno all'interno e viceversa, passa attraverso il firewall.
   - Il firewall si colloca al confine tra la rete amministrata e Internet. In questo modo è più semplice gestire la sicurezza ed imporre il rispetto di regole di sicurezza.
2) Solo il traffico autorizzato, elencato nelle politiche di sicurezza, sarà autorizzato a passare.
3) Il firewall è immune a ogni tentativo di penetrazione.
   - Il firewall è un dispositivo collegato alla rete. Se non viene configurato e installato correttamente fornisce solo un falso senso di sicurezza, che è peggio che non avere alcun firewall.

Firewall

firewall

I firewall di rete hanno lo scopo di proteggere l'area di una rete aziendale, impedendo agli utenti non autorizzati, che si trovano sulla rete pubblica, di accedere a risorse protette.



Scopi del Firewall

Impedire gli attacchi denial of service:

- SYN flood: l'attaccante apre molte connessioni TCP usando un indirizzo mittente inesistente, fino a saturare la memoria e non lasciando risorse per connessioni reali.

Impedire l'accesso o la modifica a dati riservati

- Ad esempio l'attaccante potrebbe sostituire una pagina web con un'altra

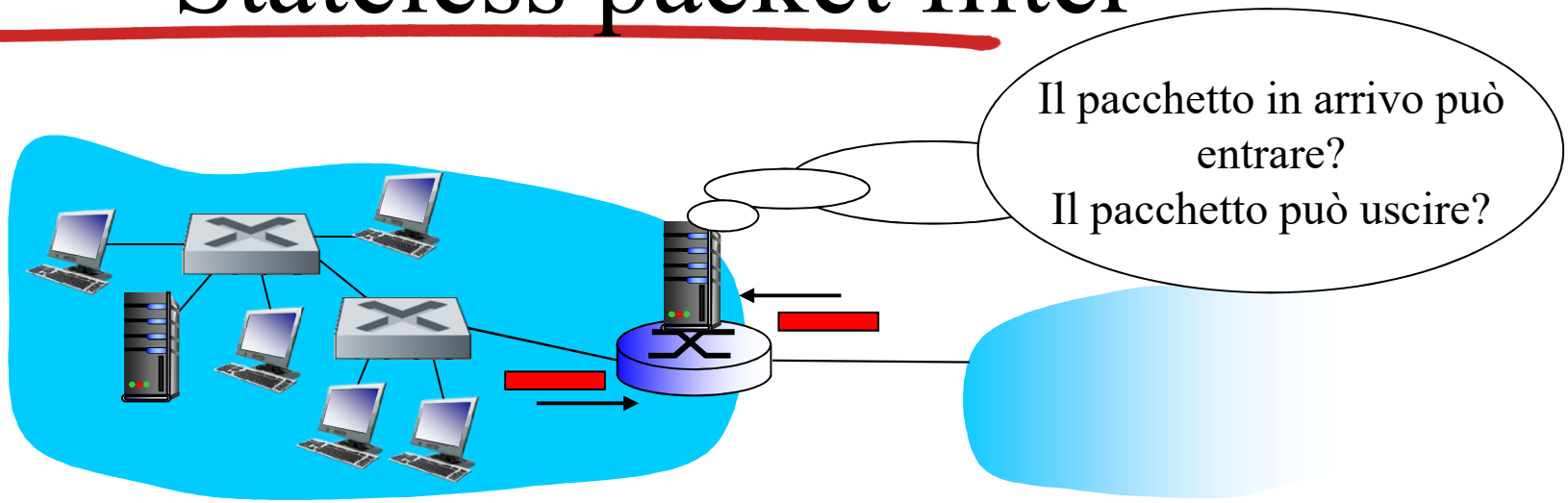
Consentire solo agli utenti autorizzati di accedere alla rete interna

- definire gli utenti e gli host autenticati

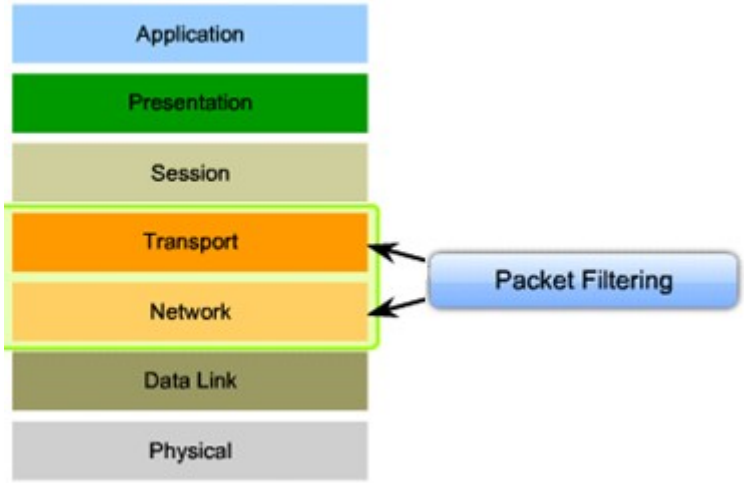
Esistono tre tipi di firewall:

- stateless packet filter
- stateful packet filter
- application gateway

Stateless packet filter



- La rete interna è connessa a Internet tramite un *router con funzionalità firewall*
- Il router *filtra pacchetto per pacchetto*, e decide di smistare o scartare il pacchetto secondo uno o più criteri, quali ad esempio:
  - Indirizzo IP sorgente, indirizzo IP destinazione
  - Numero di porta TCP o UDP sorgente o destinazione
  - Tipo di messaggio ICMP
  - Bit SYN e ACK nell'header del pacchetto TCP



Regole del firewall

- L'amministratore di una rete configura il firewall sulla base di criteri (policy) definiti dall'organizzazione.
- Le policy possono tener conto della produttività, dell'impegno di banda e di tutto ciò che riguarda la sicurezza dei dati dell'organizzazione.
- Ad esempio, se l'organizzazione non vuole che vengano stabilite connessioni TCP entranti, eccetto quelle dirette al suo server Web pubblico, può bloccare tutti i segmenti TCP SYN tranne i segmenti TCP SYN aventi porta destinazione 80 e indirizzo "IP destinazione" corrispondente al server Web.
- Se l'organizzazione vuole impedire che gli utenti interni occupino la banda con applicazioni radio o tv, può bloccare tutto il traffico UDP.
- Se l'organizzazione non vuole che un utente esterno scopra la mappa della rete interna, usando lo strumento "trace route", può bloccare i messaggi ICMP aventi il campo TTL = 0 in uscita dalla rete.

Stateless packet filter: esempio

- *esempio 1:* bloccare i pacchetti IP entranti e uscenti, aventi il campo protocollo = 17 e con porta sorgente o destinazione = 23
  - *risultato:* si blocca sia il flusso dei pacchetti UDP entranti e uscenti sia le connessioni telnet
- *esempio 2:* bloccare i segmenti TCP entranti aventi il bit ACK=0.
  - *risultato:* impedire ai client esterni di stabilire connessioni TCP con i client interni, ma consentire ai client interni di stabilire connessioni con client esterni.

Regole

- Una regola di filtraggio può essere basata su una combinazione di indirizzi e numeri di porta.
- (esempio) Un router potrebbe filtrare tutti i pacchetti Telnet (quelli con numero porta destinazione 23) scartando quelli destinati o provenienti da una lista di specifici indirizzi IP. Questa regola autorizza le connessioni Telnet con alcuni host.
- Ma, una regola che si basa su indirizzi esterni, non è pienamente affidabile perché non c'è alcuna protezione contro i pacchetti in cui l'indirizzo sorgente è stato contraffatto.

Regole

Il filtraggio dei pacchetti TCP può avvenire sulla flag ACK.

L'amministratore di rete consente che i client interni si connettano a server esterni, ma vuole impedire che un utente esterno si connetta ai server interni:

- L'apertura connessione inizia con un pacchetto che possiede la flag ACK = 0. In tutti pacchetti successivi la flag ACK = 1.
- Quindi per bloccare tutti i pacchetti di "apertura connessione" con server interni, la regola deve controllare la flag ACK dei pacchetti entranti.
- Questa policy impedisce che vengano stabilite connessioni da client esterni, ma permette connessioni che abbiano origine da client interni.

Stateless packet filtering: esempi

Policy	*Impostazioni del Firewall*
Impedire l'accesso a siti web esterni.	Scarta tutti i pacchetti destinati alla porta 80 verso qualsiasi indirizzo IP.
Rifiutare le richieste di apertura connessione TCP entranti, eccetto quelle verso il server Web aziendale.	Scarta i pacchetti entranti con la flag TCP SYN =1 eccetto quelli con IP destinazione = 130.207.244.203, porta 80
Impedire lo streaming del tipo Web-radio che assorbono la banda disponibile.	Scarta i pacchetti UDP entranti - eccetto se trasportano il protocollo DNS.
Prevenire l'attacco DoS.	Scarta I pacchetti di tipo ICMP trasmessi in "broadcast" (es. 130.207.255.255).
Impedire di conoscere la mappa della rete	Scarta tutti i pacchetti uscenti di tipo ICMP e con il campo TTL = 0

Access Contro List

- Nei router, le regole dei Firewall sono implementate con le **Access Control List**, per ciascuna interfaccia del router.
- La tabella che segue nella pagina successiva rappresenta una access control list per la rete 222.22/16. Questa access control list riguarda l'interfaccia che connette il router della rete al provider.
- Le regole vengono applicate, dall'alto verso il basso, ad ogni pacchetto che transita sull'interfaccia
- Le prime due regole consentono ad un utente interno di navigare sul Web:
  - La prima regola autorizza l'uscita dalla rete dei pacchetti con porta destinazione 80;
  - la seconda regola permette ai pacchetti con la flag ACK=1 di entrare nella rete.
- Se, dall'esterno, si tenta di aprire una connessione TCP con un host interno, la connessione verrà rifiutata.
- Le successive due regole consentono ai pacchetti DNS di entrare e uscire dalla rete.
- Questa Access Control List blocca tutto il traffico eccetto il traffico DNS e il traffico Web iniziato dall'interno della rete.

Access Control List

ACL: tabella di regole, applicate nell'ordine dall'alto al basso ai pacchetti entranti: sono coppie(azione, condizione)

azione	Indirizzo sorgente	Indirizzo dest	Protocollo	Porta sorgente	Porta dest	Flag
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filter

- Per comprendere gli stateful packet filter, si osservi la access control list.
- L'access control list permette a qualsiasi pacchetto entrante con ACK = 1 e porta sorgente 80 di superare il filtro. Un attaccante potrebbe usare questi pacchetti per inviare pacchetti dannosi, applicare l'attacco denial-of-service, o risalire alla mappa della rete interna.
- Se si bloccano i pacchetti TCP con la flag ACK=1, si impedisce agli utenti interni di aprire connessioni con server web esterni.

Azione	Indirizzo sorgente	Indirizzo destinazione	Protocollo	Porta sorgente	Porta destinazione	Flag
allow	Diverso da 222.22/16	222.22/16	TCP	80	> 1023	ACK

Stateful packet filter

- Gli Stateful filter risolvono questo problema memorizzando le connessioni TCP in una Tabella delle connessioni. Questo è possibile perché un firewall riconosce l'apertura di una connessione quando vede i segmenti di handshake (SYN, SYNACK, e ACK); e riconosce la chiusura della connessione quando vede un segmento con la flag FIN.
- Il firewall può anche stabilire che la connessione è chiusa quando non vede traffico sulla connessione per un certo tempo.

Indirizzo sorgente	Indirizzo destinazione	Porta sorgente	Porta destinazine
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Esempio di tabella di connessioni di un firewall.

Indica che ci sono tre connessioni TCP uscenti, Ognuna delle quali è stata aperta da un utente interno.

Stateful packet filtering

La access control list contiene una colonna, “controllo connessione”. In questa access control list, è specificato che la connessione deve essere controllata.

Azione	Indirizzo sorgente	Indirizzo destinazione	Proto	Porta sorgente	Porta dest	Flag	controllo conness
allow	222.22/16	Diverso da 222.22/16	TCP	> 1023	80	any	
allow	Diverso da 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	Diverso da 222.22/16	UDP	> 1023	53	---	
allow	Diverso da 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

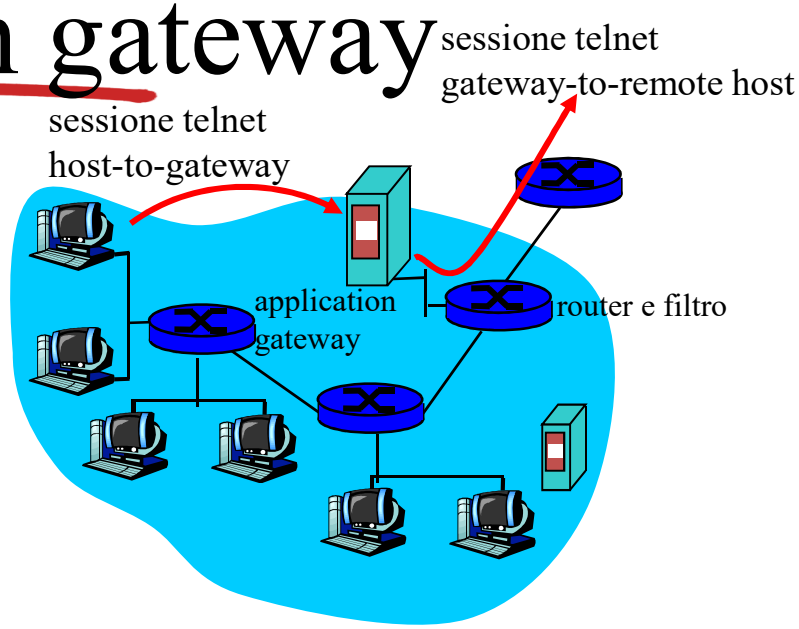
Esempio

- L'esempio seguente mostra come viene usata la tabella delle connessioni e la extended access control list.
- Un attaccante tenta di introdurre un pacchetto contraffatto nella rete dell'organizzazione inviando un pacchetto TCP con porta sorgente 80 e con la flag ACK=1.
- Questo pacchetto contiene indirizzo IP sorgente 150.23.23.155. Quando questo pacchetto giunge al firewall, il firewall controlla la access control list ed è costretto a verificare la tabella delle connessioni prima di autorizzare il pacchetto ad entrare. Dalla tabella delle connessione risulta che il pacchetto non appartiene ad una connessione uscente e lo scarta.
- Come secondo esempio, un utente interno vuole consultare un sito web esterno. Questo utente apre la connessione inviando un segmento TCP SYN, La connessione viee registrata nella tabella delle connessioni. Quando il server Web risponde (con un segmento avente il ACK = 1), il firewall, controllando la tabella delle connessioni vede che la connessione è registrata. Il firewall lascia passare questi pacchetti, senza interferire con la navigazione dell'utente interno.

Application Gateway

- Il filtraggio dei pacchetti consente ad una organizzazione di eseguire un controllo approfondito relativamente al contenuto dei campi Header dei pacchetti IP, TCP e UDP (IP sorgente e destinazione, numeri di porta sorgente e destinazione, valori delle flag, tipo di protocollo).
- Ma se l'organizzazione volesse concedere un servizio, ad esempio Telnet, ad un limitato numero di utenti (indipendentemente dagli indirizzi IP), i filtri non possono soddisfare questa esigenza.
- Se l'organizzazione vuole che gli utenti si autentichino il filtro non è capace di distinguere i permessi degli utenti.
- Le informazioni relative all'identità degli utenti sono dati del livello applicazione, non sono inserite nell'header dei pacchetti IP, TCP o UDP.
- Il firewall deve combinare il filtraggio dei pacchetti con l'application gateway. Gli Application gateways non leggono I campi dell'header dei pacchetti, la leggono il campo dati.
- Un **application gateway** è un server di una specifica applicazione attraverso cui devono passare tutti i dati (entranti e uscenti).
- Su uno stesso host ci possono essere più application gateways, ma ogni gateway riguarda un solo processo.

Application gateway

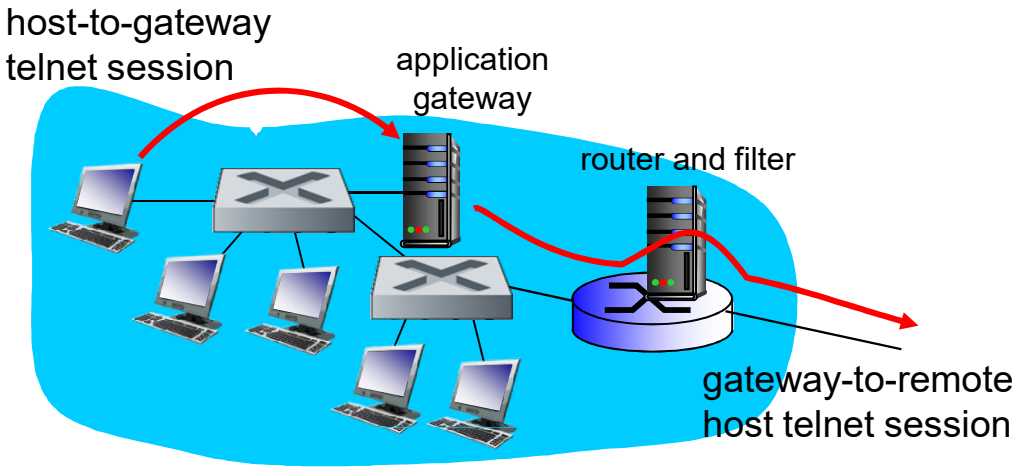


- filtra i pacchetti dei dati dell'applicazione contenuti nei pacchetti IP/TCP/UDP.
- *esempio:* permette di selezionare gli utenti interni autorizzati a usare telnet verso l'esterno.

1) Richiede che tutti gli utenti telnet passino attraverso il gateway.
2) Per gli utenti autorizzati, il gateway stabilisce una connessione telnet con l'host destinazione. Il gateway smista i dati tra le 2 connessioni
3) Il filtro del router blocca tutte le connessioni telnet che non hanno origine dal gateway.

Application gateway

Configurare un firewall che permette agli utenti autorizzati di usare Telnet verso l'esterno e impedire a utenti esterni di aprire connessioni Telnet con l'interno.
Si crea una combinazione di packet filter (in un router) ed una Telnet application gateway.

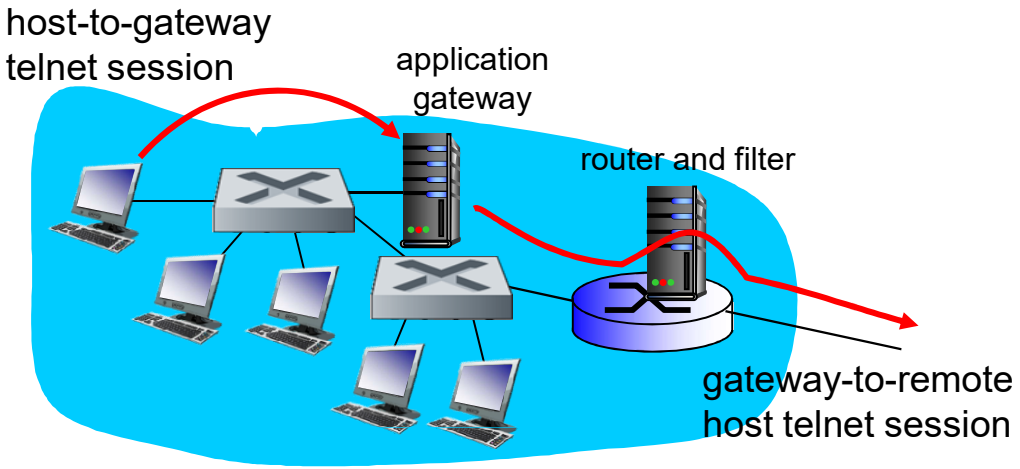


Il filtro del router è configurato per bloccare tutte le connessioni Telnet tranne quelle originate dall'indirizzo IP dell'application gateway. Questa configurazione obbliga tutte le connessioni Telnet uscenti a passare attraverso l'application gateway.

Application gateway

Un utente interno, che apre una connessione Telnet verso l'esterno, deve prima avviare una sessione Telnet con l'application gateway.

Una applicazione in esecuzione sul gateway, che ascolta le richieste di connessioni Telnet, chiede username e password. Quando l'utente le fornisce, l'application gateway verifica se l'utente ha il permesso di usare Telnet per connessioni uscenti



Se l'utente non possiede i requisiti la connessione viene chiusa dal gateway. Se l'utente ha il permesso allora il gateway:

(1) Chiede l'host name del computer esterno a cui l'utente vuole collegarsi,

(2) Imposta una sessione Telnet tra il gateway e l'host esterno,

(3) Invia all'host esterno tutti I dati provenienti dall'host utente, e consegna all'utente tutti I dati provenienti dall'host esterno.

Il Telnet application gateway non solo verifica I permessi dell'utente, ma agisce da Telnet server e Telnet client, tra l'utente e il server Telnet remoto

Limitazioni di firewall e gateway

- *IP spoofing:* i router non possono sapere se l'indirizzo sorgente appartiene ad un host reale
- Occorre avere un gateway per ogni applicazione
- I software dei client devono sapere come contattare il gateway.
  - Ad esempio, per un browser si deve impostare l'indirizzo IP del proxy

Sistemi di rilevamento Intrusioni

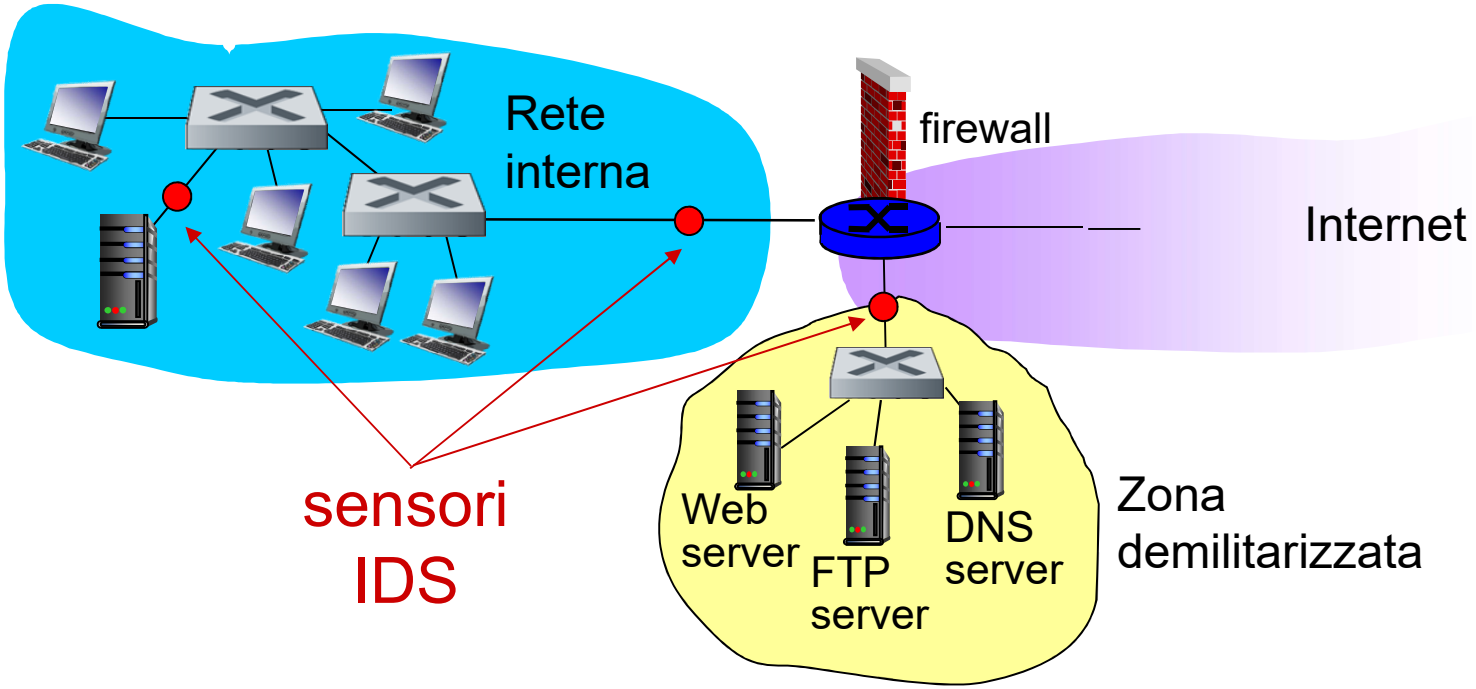
- Il filtraggio dei pacchetti:
  - opera solo sugli header TCP/IP
  - non c'è un controllo di correlazione tra le sessioni
- *IDS: intrusion detection system*
  - *Ispezione all'interno dei pacchetti:* osserva il contenuto dei pacchetti (esempio, cerca la stringa di caratteri "firma" nel database dei virus noti)
  - esamina la correlazione tra più pacchetti
    - port scanning
    - network mapping
    - DoS attack

Sistemi di riconoscimento intrusioni

Una organizzazione può installare uno o più sensori IDS nella sua rete. La rete in figura ha tre sensori IDS. I sensori lavorano in collaborazione, inviando informazioni sul traffico sospetto a un IDS centrale, questo raccoglie e integra queste informazioni e segnala l'evento all'amministratore.

L'organizzazione ha partizionato la sua rete in due regioni:

1. una ad elevata sicurezza, protetta da un packet filter ed un application gateway e monitorata dai sensori IDS;
2. ed una regione, denominata **demilitarized zone (DMZ)**, protetta solo dal packet filter, ma monitorata dai sensori IDS. Nella DMZ sono presenti i server aziendali che hanno necessità di comunicare con l'esterno.



Sistemi di riconoscimento intrusioni

- Si potrebbe osservare che basterebbe un solo sensore in prossimità del packet filter (o integrato nel packet filter.
- Un IDS non deve solo ispezionare il pacchetto al suo interno, ma deve cercare le stringhe contenute nel campo dati con le firme presenti nel database dei virus noti; questa ricerca spreca molto tempo di elaborazione, in particolare se la rete riceve alcuni gigabits/sec di traffico da Internet.
- posizionando opportunamente i sensori IDS, ognuno vede solo una parte del traffico.
- Comunque, attualmente sono disponibili IDS ed IPS ad elevate prestazioni che possono effettivamente svolgere il loro compito accanto al router di frontiera della rete, evitando di usare molti sensori.

Sistemi di riconoscimento intrusioni

- Gli IDS sono classificati come sistemi **signature-based** o come sistemi **anomaly-based.**
- Un IDS **signature-based** gestisce un database con le firme degli attacchi noti.
- Una firma (signature) è un insieme di regole tipiche di un'attività di intrusione.
- Una firma è un elenco delle caratteristiche di un pacchetto (ad esempio, numero porta sorgente e destinazione, protocollo, e una specifica stringa di caratteri nel payload del pacchetto), o potrebbe essere relativa ad una serie di pacchetti.
- Le firme sono create da tecnici esperti che studiano gli attacchi conosciuti.
- Un IDS signature-based sniffa ogni pacchetto in transito, ricercando nel database le stringhe che corrispondono alla firma. Se un pacchetto (o una serie di pacchetti) possiede una firma registrata nel database, l'IDS genera un allarme. L'allarme potrebbe essere inviato via mail all'amministratore, potrebbe essere inviato al sistema di gestione della rete, oppure potrebbe essere registrato in un file di log, che viene consultato periodicamente dall'amministratore.

Gli IDS Signature-based hanno delle limitazioni:

- Sono efficaci solo per gli attacchi conosciuti. Sono inefficaci per i nuovi attacchi.
- Anche se una firma viene rilevata, potrebbe non far parte di un attacco, e viene generato un falso allarme.
- Infine, poiché ogni pacchetto deve essere controllato in profondità, con numerose firme, l'IDS potrebbe impiegare molto tempo di elaborazione e addirittura non riconoscere i pacchetti dannosi.

Sistemi di riconoscimento intrusioni

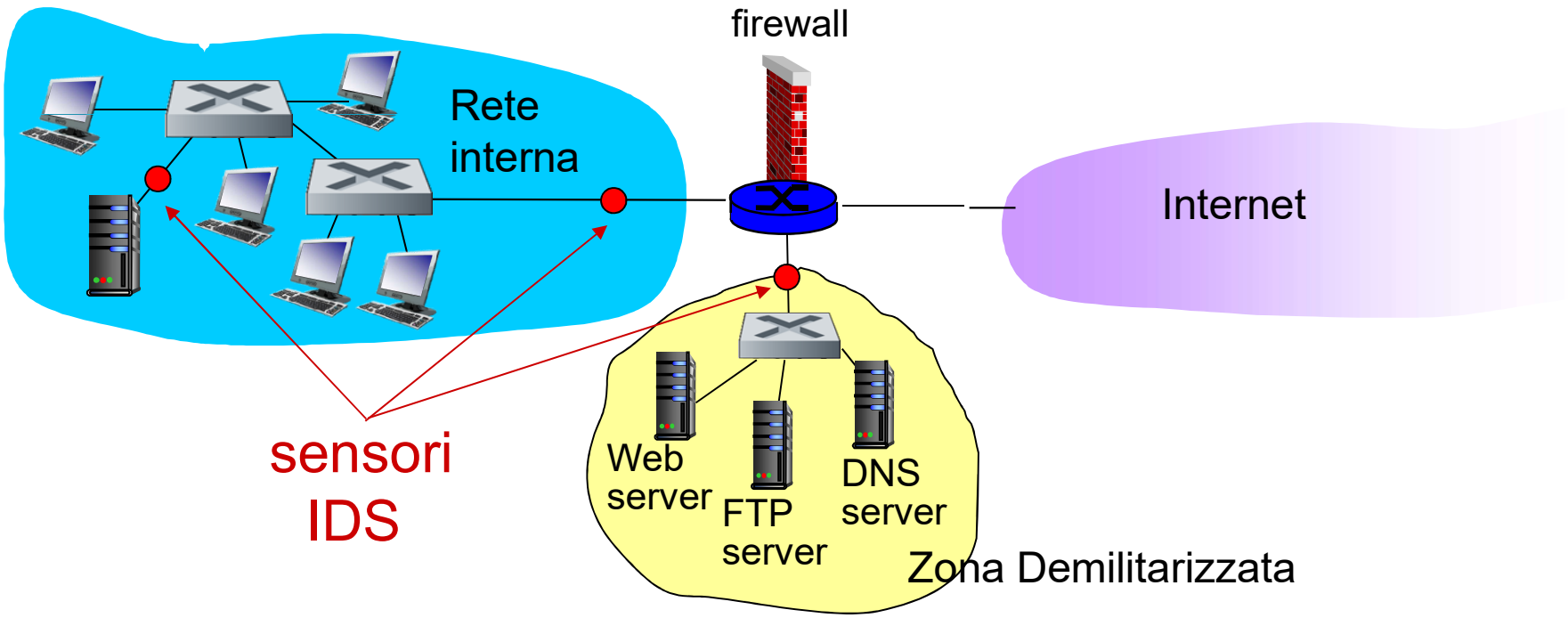
- Un IDS anomaly-based crea un profilo del traffico osservato durante la normale attività. Conteggia i flussi dei pacchetti per individuare qualcosa di insolito, ad esempio, una elevata percentuale di pacchetti ICMP o una rapida crescita di scansione delle porte e ping con indirizzi sempre diversi.
- Gli IDS non sfruttano una conoscenza relativa ad attacchi avvenuti. Potenzialmente potrebbero rilevare nuovi attacchi, non documentati.
- É estremamente difficile distinguere il traffico legittimo dal traffico insolito.

Snort

- Snort è un IDS di pubblico dominio, open source.
- Esiste nelle versioni per Linux e per Windows.
- Usa la stessa libreria libpcap usata da Wireshark per catturare ed analizzare pacchetti.
- Gestisce 100 Mbps di traffico.
- Quando il traffico è dell'ordine dei gibabit/sec, conviene usare più sensori Snort.
- Un esempio di firma Snort :
- `alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize: 0; itype: 8;)`
- Questa firma viene confrontata con ogni pacchetto ICMP di tipo 8 (ICMP ping), che entra nella rete dell'organizzazione ($HOME_NET) dall'esterno ($EXTERNAL_NET), ed ha la parte payload vuota (dsize = 0). Poiché nmap (il software usato per scandire le porte) genera pacchetti ping con queste caratteristiche, questa firma è progettata per riconoscere i tentativi di un attaccante di scoprire le porte aperte.
- Quando un pacchetto corrisponde a questa firma, Snort genera un allarme che include il messaggio "ICMP PING NMAP".
- In genere dopo poche ore da un attacco, la comunità Snort rilascia la firma dell'attacco e tutte le installazioni di Snort ne vengono a conoscenza automaticamente.

Intrusion detection system

- molti IDS: svolgono tipi differenti di controlli in posti diversi



Network Security (riepilogo)

tecniche di base ...

- criptografia (a chiave simmetrica e a chiave pubblica)
- integrità dei messaggi
- autenticazione delle parti

…. usate in molti differenti esigenze di sicurezza

- email
- livello trasporto (SSL)
- IP sec
- 802.11

Realizzate con firewalls e IDS