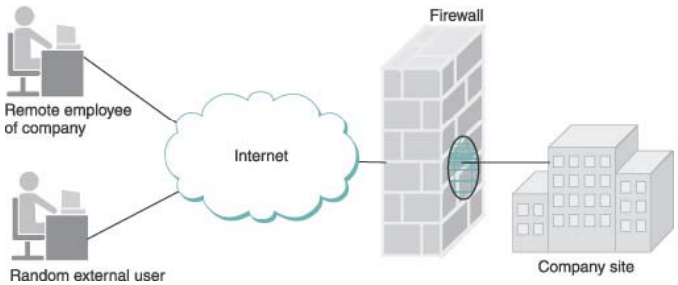
Firewall e IDS

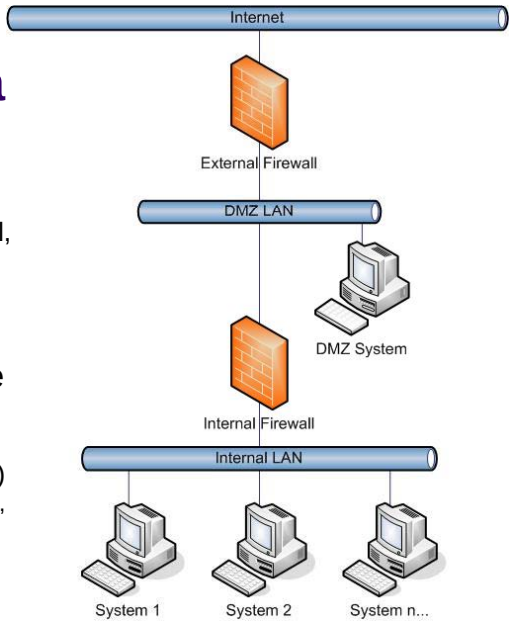
Firewall

- Sistema che costituisce l'unico punto di connessione tra una rete privata e il resto di Internet
  - Solitamente implementato in un router
  - Implementato anche su host (firewall personale)



Livelli di fiducia

- Un firewall suddivide la rete in
  - una zona interna al firewall, della quale si ha fiducia
  - una zona esterna, alla quale viene concessa una fiducia minore
- Si possono anche creare più zone di fiducia
  - rete interna
  - zona demilitarizzata (DMZ)
    - Ospita servizi pubblici (DNS, email, web)
  - resto di Internet



Tipi di firewall

- A filtraggio dei pacchetti (packet filter)
- A filtraggio dei pacchetti con memoria dello stato (stateful filter)
- A livello di applicazione (application gateway)

Filtraggio dei pacchetti

- Il firewall decide se consentire o negare l'accesso dei pacchetti entranti e uscenti in base a:
  - Indirizzo IP sorgente o destinazione
  - Porte sorgente e destinazione TCP o UDP
  - Tipo di messaggio ICMP
  - Bit TCP SYN o ACK
- Configurazione tipica: eliminare tutti i pacchetti che non sono esplicitamente consentiti

Esempi di regole di filtraggio

- Esempio
  - Regola: blocca i datagrammi in ingresso e uscita con IP protocol field = 17 e numeri di porta mittente o destinatario = 23
  - Effetto: tutti i flussi UDP e le connessioni telnet sono bloccate
- Esempio
  - Regola: Blocca i segmenti TCP in ingresso con ACK = 0
  - Effetto: Impedisce a client esterni di iniziare connessioni TCP con server interni ma lascia che tutti i client interni possano connettersi all'esterno
- Esempio
  - Regola: blocca tutti i datagrammi in ingresso tranne quelli con numeri di porta 80
  - Effetto: solo le richieste di client esterni al web server sono ammesse
  - Effetto collaterale: le risposte a richieste fatte da client interni a servizi esterni sono bloccate (un client comunica da porte non standard)

Politiche di accesso e configurazione dei firewall

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Table 8.4 ♦ Policies and corresponding filtering rules for a organization's network 130.27/16 with Web server at 130.207.244.203.

Implementazione delle regole mediante ACL

action	source address	dest address	protocol	source port	dest port	flag bit
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

Table 8.5 ♦ An access control list for a router interface

Filtraggio dei pacchetti con memoria dello stato

- Il firewall tiene traccia dello stato di tutte le connessioni TCP

source address	dest address	source port	dest port
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

Table 8.6 ♦ Connection table for stateful filter

- I pacchetti in entrata indirizzati a porte assegnate dinamicamente sono inoltrati solo se rappresentano risposte conformi allo stato di connessione associato alla porta

Filtraggio dei pacchetti con memoria dello stato

action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
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	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

Table 8.7 ♦ Access control list for stateful filter

Application gateway

- E' un intermediario (proxy) tra gli host della rete interna e quelli delle reti esterne
  - Non è possibile creare connessioni dirette tra host della rete interna e quelli delle reti esterne
  - Svolge contemporaneamente il ruolo di server per i client della rete interna e di client per i server delle reti esterne
- Conosce il funzionamento specifico del protocollo di livello applicazione

Application gateway

- Può essere usato in combinazione con un packet filter
  - Il router che implementa il packet filter esclude tutti i pacchetti in uscita che non originano e non terminano sull'host che implementa l'application gateway
  - Esempio: permette solo ad alcuni client interni autorizzati le connessioni Telnet ma impedisce il contrario

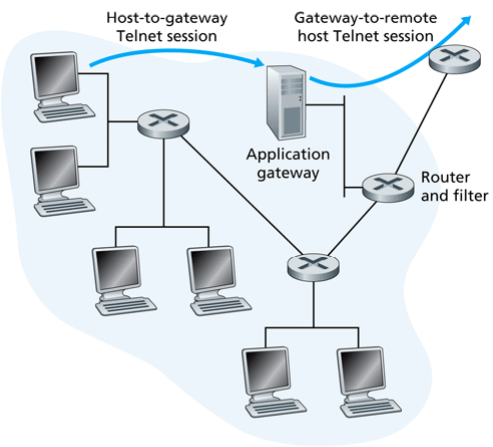


Figure 8.36 ♦ Firewall consisting of an application gateway and a filte

Sistemi di rilevamento delle intrusioni (IDS)

- Esaminano il contenuto dei pacchetti per rilevare pacchetti sospetti a livello di rete, di trasporto o di applicazione
- Rilevano un'ampia gamma di attacchi
  - Scansione della rete e delle porte
  - Attacchi DoS
  - Malware
- Standard de facto: Snort

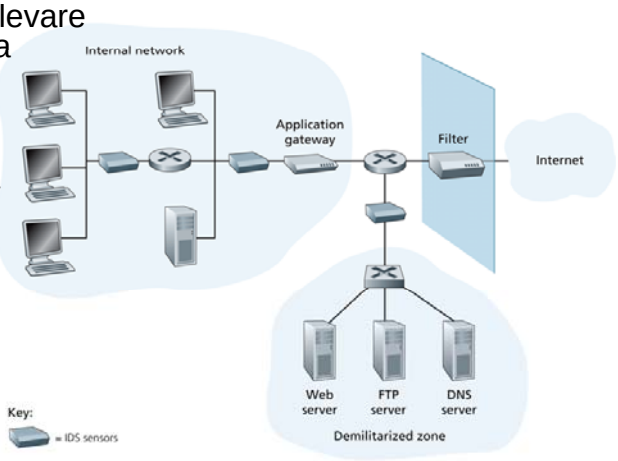


Figure 8.37 ♦ An organization deploying a filter, an application gateway, and IDS sensors

Tipi di IDS

IDS basati sulle firme

- Ampio database di firme (signature) degli attacchi
- Una firma è un insieme di regole associate a un'attività di intrusione
- Richiesta una conoscenza pregressa dell'attacco

IDS basati sulle anomalie

- Creano un profilo di traffico in situazioni "normali"
- Si accorgono di flussi di pacchetti statisticamente insoliti
- Non fanno affidamento sulla conoscenza di attacchi già avvenuti