Sicurezza nelle reti: protezione di LAN

Gaia Maselli
maselli@di.uniroma1.it

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 architettetture che siano immuni da attacchi

Cosa è un attacco?

- Spesso indicato anche come **intrusione**

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.

Un scenario di intrusione più complesso

- **Scansione della rete**: in questa fase si mira a recuperare più infomazioni possibili sulla rete obiettivo
  - Whois, dig, nslookup
  - Nmap (strumento di Network Mapping)

- **Identificazione delle vulnerabilità**: scansione a livello di singoli host (servizi disponibili sui vari host, versione di sistema operativo)
  - Port scanning

Un scenario di intrusione più complesso (cont.)

- **Attacco**: vengono sfruttate vulnerabilità scoperte nella fase precedente, creando un punto di appoggio per un accesso futuro
  - creando un account
  - installando una *backdoor*

- **Espansione dell'attacco**: l'intruso accede nuovamente al sistema per rubare dati confidenziali, cancellando file, mettendo fuori uso il sistema
  - Installazione di programmi dolosi
  - denial of service (DoS)

Network mapping

- Metodo per il recupero di informazioni sulla rete obiettivo, al fine di tracciare una mappa dei sistemi connessi e individuarne le vulnerabilità
- Per essere effettivo deve aggirare le regole adottate dai firewall (e progredire con il loro aggiornamento)
- Storicamente basato su *ping*, adotta meccanismi molto sottili per introdursi in una rete e ottenere un risultato analogo
- Obiettivo: ottenere in qualche modo una risposta dalle macchine sotto esame senza badare all'informazione ottenuta
- Si suddividono in
  - Metodi basati su richiesta valida
  - Metodi basati su richiesta non valida

Metodi di netwok mapping (1/2)

Basati su richiesta valida

- Invio di una richiesta valida verso un servizio che comporta una risposta da parte del server che offre tale servizio (Es. Richiesta orario corrente)
- Si suddividono in metodi che utilizzano
  - TCP
  - UDP
  - ICMP

Metodi che usano TCP

- Sfruttano caratteristiche delle procedure di apertura e chiusura di una connessione (3-way handshake)
- **Obiettivo: ricevere una qualche risposta (es. TCP ACK o TCP RST) che dimostri l'attività dell'host**

Metodi:

- Invio di TCP SYN verso una presunta porta aperta (ricevendo TCP SYN/ACK)
- Invio di TCP flag che causano il ritorno di un TCP RST
  - Invio di TCP ACK verso qualsiasi porta attiva
  - Invio TCP FIN verso una porta che si suppone chiusa
  - Invio di un TCP SYN/ACK (qualsiasi sia lo stato della porta)
  - Invio TCP XMAS su porta chiusa
  - Invio TCP NULL su porta chiusa

Metodi che usano UDP

- Meno utilizzato, meno affidabile

Metodi

- UDP/Echo port: invio di UDP echo request
- UDP Scan: invio pacchetto UDP verso porta chiusa causa risposta ICMP Port Unreacheable

Metodi che usano ICMP

- ICMP è largamente usato per i mezzi che offre nel verificare se una destinazione è raggiungibile
  - Icmp echo request (Ping)
  - Icmp timestamp request
  - Icmp information request
  - Icmp Address Mask request

Metodi di netwok mapping (2/2)

Basati su richiesta non valida

- Invio di una richiesta non valida che viola la specifica dell'IP per ricevere un messaggio di errore dalla macchina obiettivo
  - Invio di un primo frammento senza inviare i successivi → la macchina ricevente dopo un timeout risponde con un ICMP Fragment reassembly time exceeded
  - Specificando un valore non valido all'interno di uno qualsiasi dei campi dell'intestazione IP si ottiene un messaggio di errore ICMP dalla macchina destinataria

Port scanning

- Scansione dettagliata dei singoli host per scoprire i servizi attivi
- Conosciuta la lista dei servizi attivi si possono individuare vulnerabilità sfruttabili per eventuali connessioni o attacchi
- Metodi simili a quelli nel network mapping
  - TCP SYN
  - TCP SYN/ACK
  - TCP FIN
  - etc.

Tipi di attacchi

- Spiare la conversazione (*sniffing*)
  - Carta di credito
  - Comunicazioni con banca
  - Informazioni DNS e di routing
- Impersonare un altro soggetto (*spoofing*)
- Dirottare una sessione in corso (*hijacking*)
- Mettere fuori uso alcuni servizi (*Denial of service*)

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

I malintenzionati installano malware negli host attraverso Internet

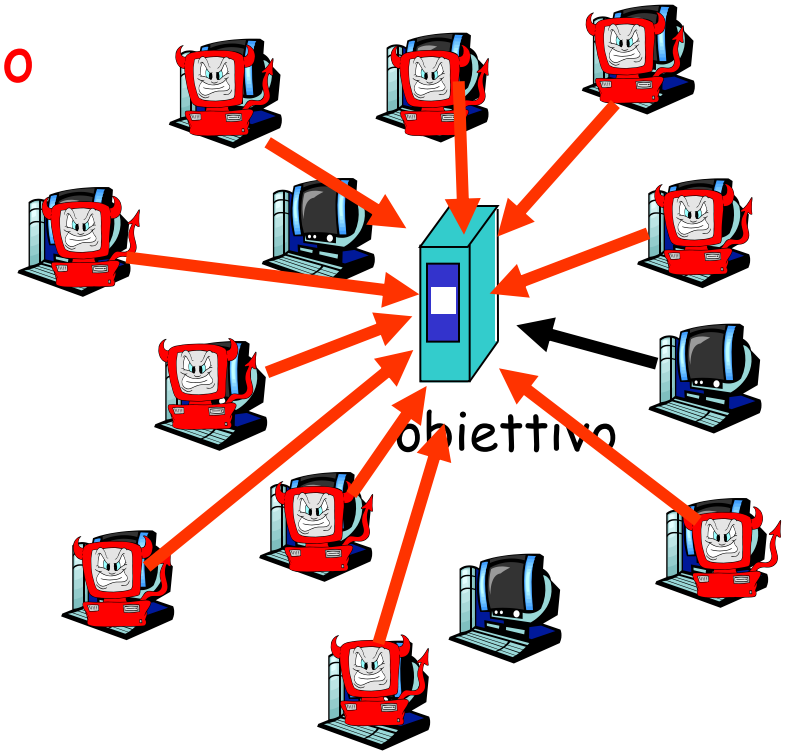
- Cavalli di Troia
  - Parte nascosta di un software utile
  - Oggi si trova spesso su alcune pagine web (Active-X, plugin)...
- Virus
  - L'infezione proviene da un oggetto ricevuto (attachment di e-mail), e mandato in esecuzione
  - Auto-replicante: si propaga da solo ad altri host e utenti
- Worm:
  - L'infezione proviene da un oggetto passivamente ricevuto che si auto-esegue
  - Auto-replicante: si propaga da solo ad altri host e utenti

I malintenzionati attaccano server e infrastrutture di rete

- Negazione di servizio (DoS): gli attaccanti fanno sì che le risorse (server, ampiezza di banda) non siano più disponibili al traffico legittimo sovraccaricandole di traffico artefatto

Denial of service distribuito

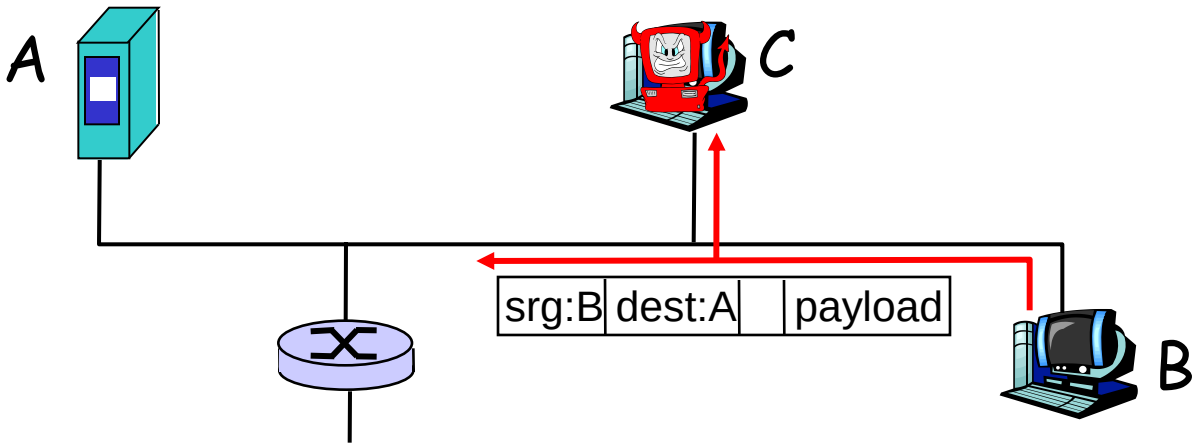
1. Selezione dell'obiettivo
2. Irruzione negli host attraverso la rete
3. Invio di pacchetti (**flooding**) verso un obiettivo da parte degli host compromessi



I malintenzionati analizzano i pacchetti

Analisi dei pacchetti *(packet sniffing)*:

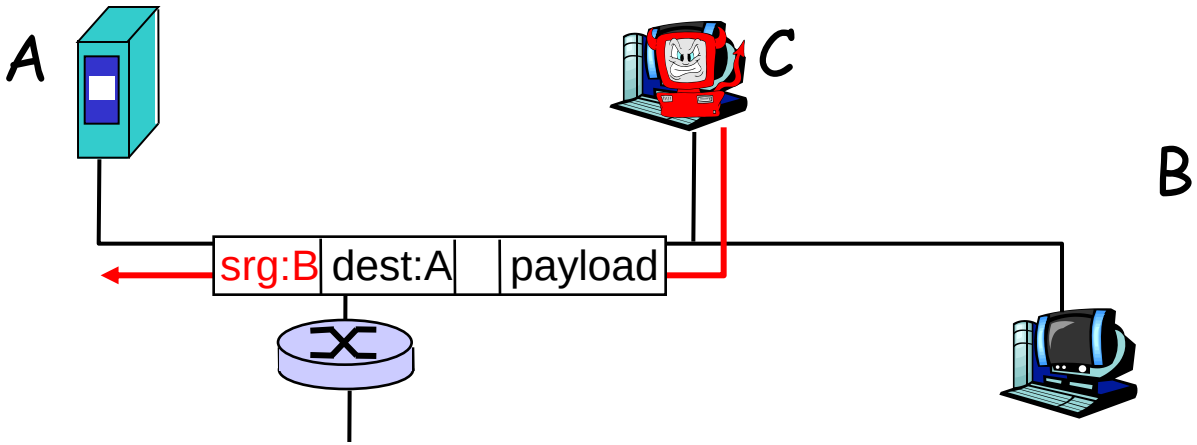
- Facile su mezzi broadcast (Ethernet condivisa, wireless)
- un'interfaccia di rete legge/registra tutti i pacchetti (password comprese!) che l'attraversano



- I packet sniffer sono **passivi**: non immettono paccheti sul canale, per cui sono difficili da individuare

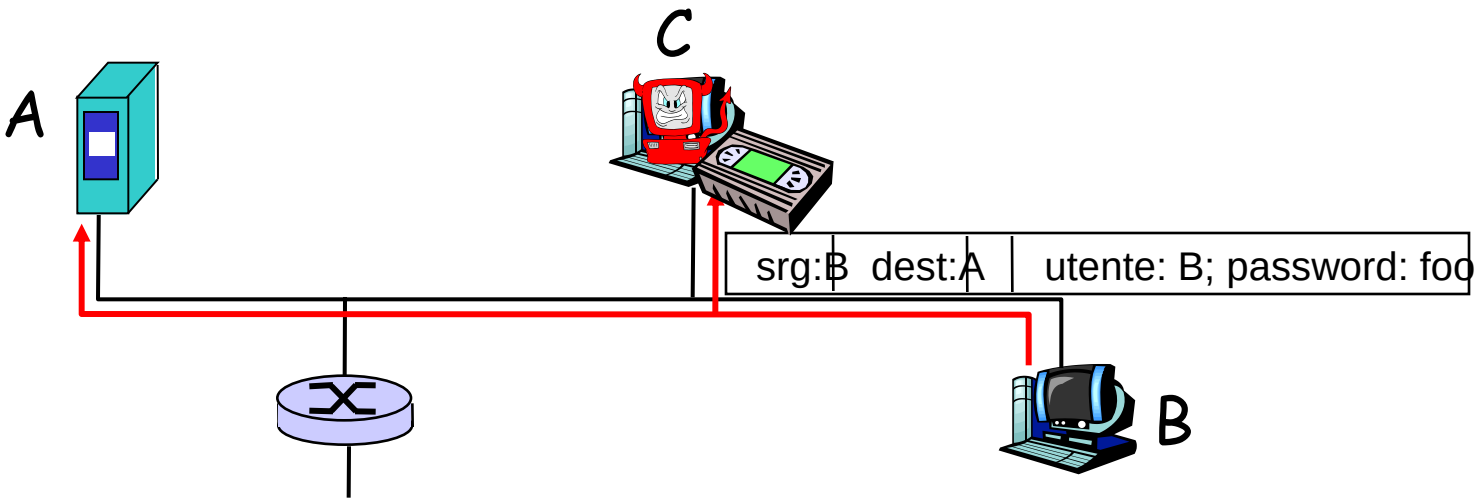
I malintenzionati usano indirizzi sorgente falsi

- *IP spoofing:* invio di pacchetti con un indirizzo sorgente falso



I malintenzionati registrano e riproducono

- *record-and-playback*: "sniffano" dati sensibili (password, ad esempio), per poi utilizzarli in un secondo tempo



Contromisure

- Antivirus
- Firewall
- Intrusion detection system
- Crittografia

Antivirus

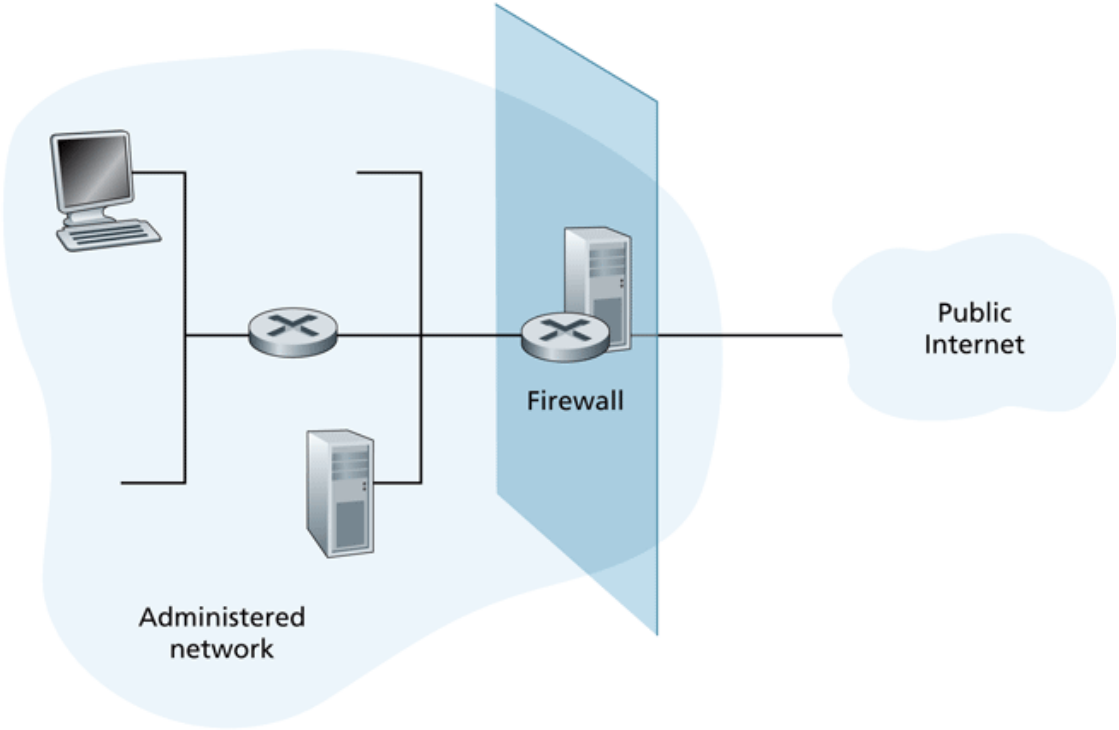
- Software atto a rilevare ed eliminare programmi dolosi (virus, worm, etc.)
- Viene installato sui singoli host per cui agisce localmente all'host
- Antivirus anche per server (mail server)
- Metodi
  - Esamina i dati interni al computer per rilevare presenza di programmi dolosi noti
  - Analizza il comportamento dei vari programmi alla ricerca di istruzioni sospette perché tipiche del comportamento dei virus
- Deve essere sempre aggiornato con la creazione di nuovi attacchi (sempre un passo indietro agli attacchi)

D: 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.

- Tutto il traffico verso l'interno e viceversa passa attraverso il firewall
- Solo al traffico autorizzato sarà consentito passare



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".

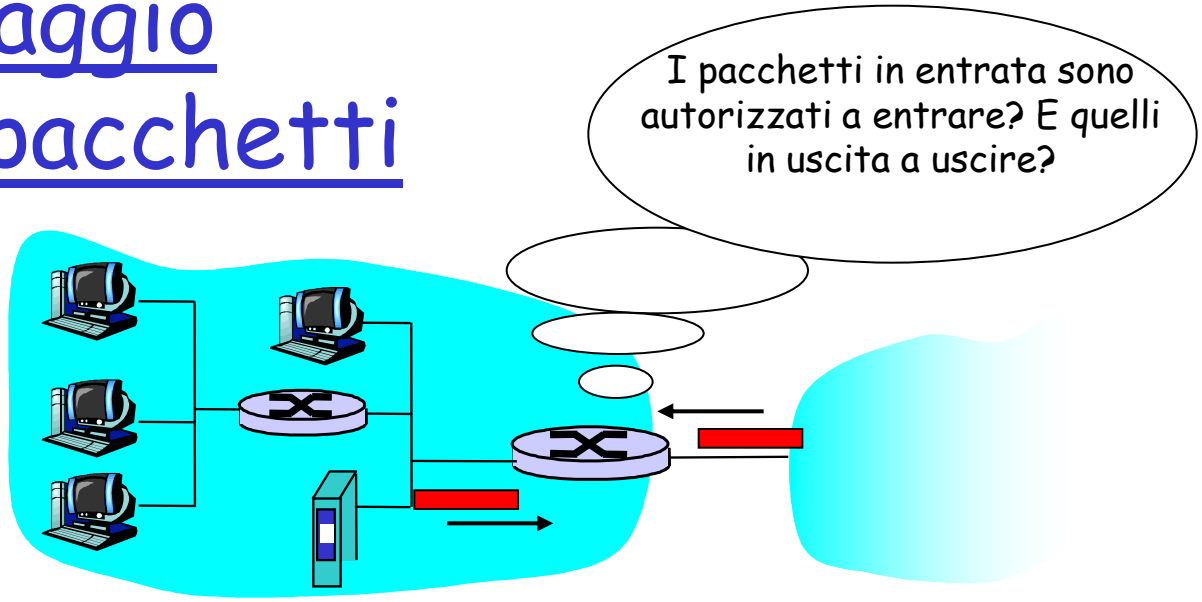
Prevenire modifiche/accessi illegali ai dati interni.

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

Tre tipi di firewall:

- A filtraggio dei pacchetti
- A filtraggio dei pacchetti con memoria dello stato
- A livello di applicazione (gateway)

Filtraggio dei pacchetti



- Una rete privata 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 in base a:
  - Indirizzo IP sorgente o destinazione
  - Porte sorgente e destinazione TCP o UDP
  - Tipo di messaggio ICMP
  - Bit TCP SYN o ACK

Filtraggio di pacchetti: un esempio

- Esempio 1: blocco sui datagrammi in entrata e in uscita con IP protocol field = 17 e il cui numero di porta sorgente o destinazione = 23.
  - Tutti i segmenti UDP e tutte le connessioni Telnet sono bloccate.
- Esempio 2: bloccare i segmenti delle comunicazioni TCP con ACK=0.
  - Espediente utile se si vuole che i client interni possano collegarsi a server esterni, evitando però l'operazione inversa.

Filtraggio di pacchetti: ulteriori 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

Access Control Lists (ACL)

- *ACL:* tabella di regole da applicare integralmente ai pacchetti entranti.
- Esempio di ACL per organizzazione 222.22/16

azione	indirizzo sorgente	indirizzo dest	protocollo	porta sorgente	porta destinaz.	bit di flag
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
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	----
blocca	tutto	tutto	tutto	tutto	tutto	tutto

Filtri di pacchetti con memoria dello stato

- 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

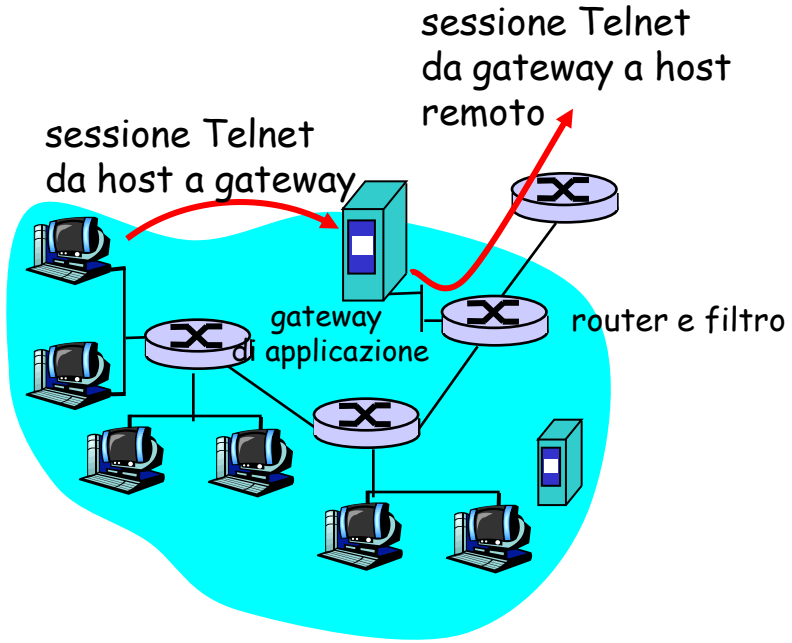
- *Filtraggio con memoria dello stato:* tiene traccia dello stato di tutte le connessioni TCP
  - Traccia l'impostazione del collegamento (SYN) e la terminazione (FIN): può così determinare se i pacchetti in entrata o in uscita "hanno senso" ovvero sono scambiati all'interno di connessioni esistenti

Filtri di pacchetti con memoria dello stato

- 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	

Gateway (proxy firewall)



- Il filtraggio dei pacchetti consente di effettuare un controllo sulle intestazioni IP e TCP/UDP.
- Esempio: permette ai client interni (autorizzati) le connessioni Telnet ma impedisce il contrario.
- Il gateway consente un filtraggio a livello di applicazione

1. Tutte le connessioni Telnet verso l'esterno devono passare attraverso il gateway.
2. Il gateway non solo concede l'autorizzazione all'utente ma smista anche le informazioni fra l'utente e l'host.
3. La configurazione del filtro del router blocca tutti i collegamenti eccetto quelli che riportano l'indirizzo IP del gateway.

Sistemi di intrusion detection

- IDS: *intrusion detection system*
  - *Sistema passivo che si basa sull'analisi del traffico di rete (non immette pacchetti in rete)*
  - *Rileva un'ampia gamma di attacchi:* guarda il contenuto dei pacchetti e li relaziona tra loro
  - Esamina le correlazioni among multiple packets
    - Scansione delle porte
    - Scansione della pila TCP
    - Attacchi DoS
  - Genera allarmi (ma non blocca il traffico)
  - Si basa su un packet sniffer + un insieme di regole

Network based intrusion detection

- ***Network-based***: il sistema cattura e analizza il traffico di rete
  - SNORT: sistema open source e pubblicamente disponibile

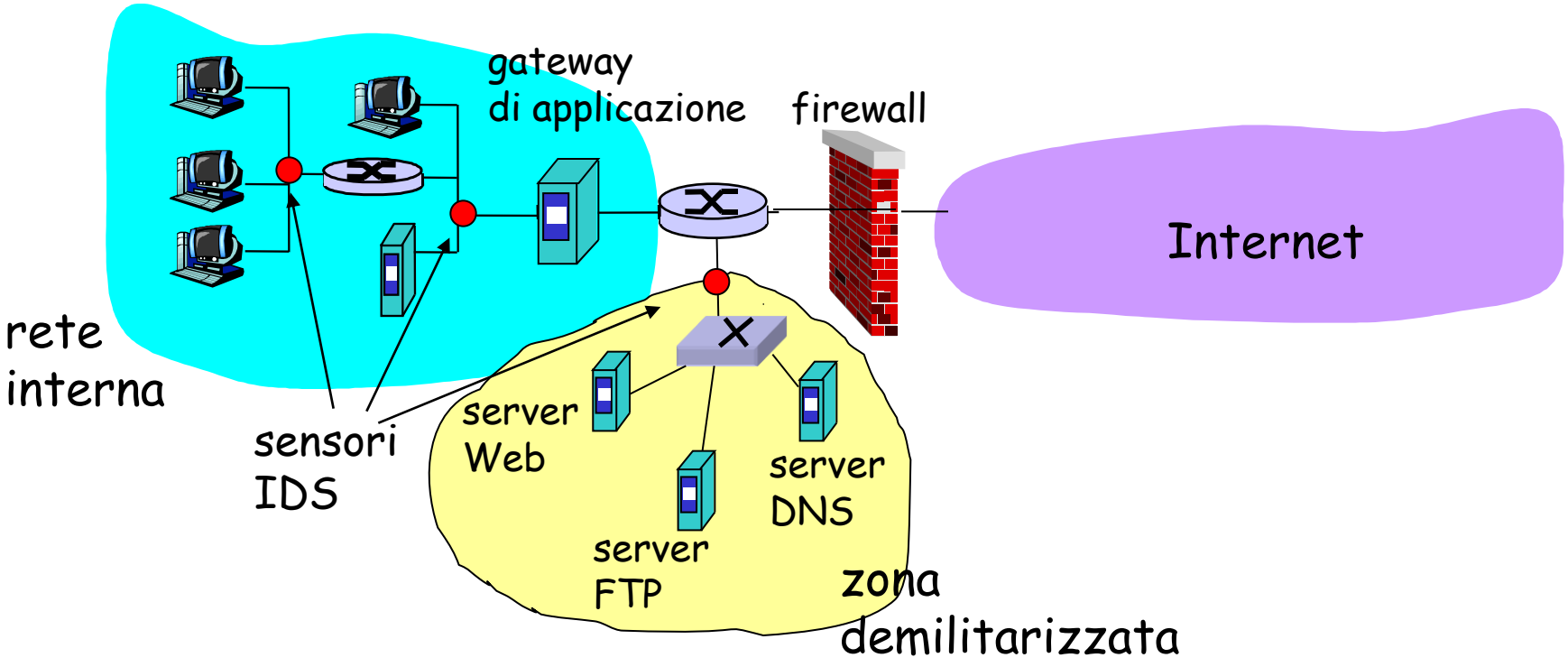
- Ci sono anche sistemi ***host-based***: la sorgente di informazione è locale e interna a un host, in generale a livello di sistema operativo (file di log)

Signature o anomaly based IDS

- ***Signature-based***: mantiene un database di firme degli attacchi (ovvero insieme di regole riguardanti un pacchetto o un insieme di pacchetti) e confronta ciascun pacchetto con le firme nel database
  - Se un pacchetto o una serie di pacchetti corrisponde a una firma nel database allora viene generato un allarme
  - Svantaggio: sempre un passo indietro rispetto a nuovi attacchi!!!
- ***Anomaly-based***: crea un profilo di traffico "normale" e genera un allarme quando rileva un comportamento (di rete) anomalo
  - Vantaggio: può rilevare nuovi attacchi
  - Svantaggio: può avere elevati falsi positivi e falsi negativi

Sistemi di rilevamento delle intrusioni

- L'IDS può essere composto da molteplici sistemi di rilevamento delle intrusioni: differenti tipi di controllo in punti diversi



La sicurezza nelle reti (riassunto)

- Sicurezza operativa
  - Antivirus
  - Firewall
  - Intrusion detection system
- Sicurezza della comunicazione
  - Crittografia, hash crittografica, firma digitale, … (prossima lezione)

D: quale meccanismo è migliore?