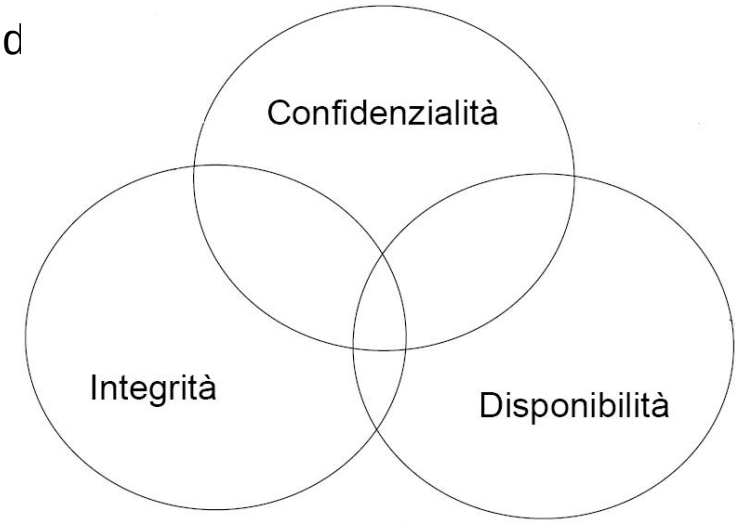
Sicurezza

IZ3MEZ
Francesco Canova
www.iz3mez.it
francesco@iz3mez.it

La sicurezza

- La Sicurezza informatica si occupa della salvaguardia d potenziali rischi e/o violazioni dei dati
- I principali aspetti di protezione del dato sono
  - Confidenzialità
  - Integrità
  - Disponibilità



- La protezione dagli attacchi informatici viene ottenuta agendo su più livelli:
  - a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi
  - a livello logico che prevede l'autenticazione e l'autorizzazione di un entità che rappresenta l'utente nel sistema
    - successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate in file di log
    - questo processo di monitoraggio delle attività è detto audit o accountability

Tipi di sicurezza

- Sicurezza passiva (usata contro gli “attacchi passivi”): tecniche e strumenti di tipo difensivo il cui scopo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata
  - Salvaguardano riservatezza e autenticazione
  - È più facile un intervento preventivo, che rilevare la presenza di un attacco
  - Spesso gli “attacchi passivi” sono effettuati per ottenere informazioni necessarie per un “attacco attivo”

- Sicurezza attiva (usata contro gli “attacchi attivi”): tecniche e strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi
  - dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità)
  - dalla possibilità che un utente non autorizzato possa modificarli (integrità)

Alcuni esempi di attacchi

- Attacchi passivi
  - Mapping e port scanning (esplorazione della rete)
    - Es mapping: uso del ping o di altre utility basate su ICMP per l'esplorazione di una rete
    - Es port scanning: uso di telnet o di di altre utility per la scansione delle porte
  - Sniffing (analisi del traffico)

- Attacchi attivi
  - Spoofing (sostituzione)
    - Es: Falsificazione dell'indirizzo di rete del mittente o falsificazione del nome simbolico
  - Exploit (sfruttamento dei bug dei software)
  - Malicious software
    - Es: Virus, Worm, Cavalli di Troia
  - DoS: Denial of Service (negazione del servizio)
    - Es: mail bombing (saturazione della posta

Come difendersi?

Alcune contromisure:

- Linee guida per la prevenzione dei problemi
- Sistemi di protezione di rete
- Sistemi di protezione a livello di host
  - ciascun host viene protetto separatamente, attraverso il sistema operativo o altro software locale
- Sistemi di protezione a livello applicativo
  - protezione dei dati attraverso meccanismi delle applicazioni stesse

Linee guida per la prevenzione dei problemi

- Aggiornamenti frequenti del software:
  - patch e service pack
- Monitoraggio tramite log
- Scansione delle porte
- Chiudere i processi in ascolto che non si intende utilizzare
- Politica di accessi autorizzati alle risorse
- Politica di gestione delle password
- Non operare quando non serve con diritti di root (administrator)

La Crittografia e l’autenticazione

- Sono tecniche fondamentali nelle strategie di protezione a livello di host e di applicazione
- Crittografia garantisce:
  - Riservatezza delle informazioni
  - Integrità dei dati
- Autenticazione garantisce:
  - Identità dell’interlocutore remoto
  - Autenticità delle informazioni
  - Paternità delle informazioni

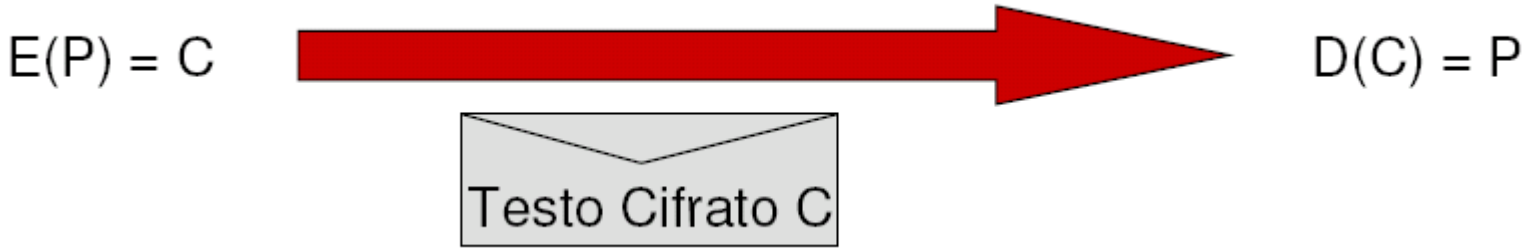
Crittografia

- Cos'è?
- Arte antica, e scienza moderna:
  - fino al 1600 – 1700: sostituzioni monoalfabetiche
  - sostituzioni polialfabetiche e sistemi simmetrici fino al 1975-76
  - crittografia a chiave pubblica e moderna

Scopo della crittografia: studiare metodi che consentano di memorizzare, elaborare e trasmettere informazioni in presenza di agenti ostili

Idea base della crittografia

- L’idea di base è quella di trasformare un messaggio in modo tale che solo utenti autorizzati riescano a leggerlo
  - P: testo in chiaro (plain text), comprensibile a tutti
  - C: testo cifrato (ciphertext), comprensibile solo al destinatario
  - E: funzione di cifratura, capace di rendere il messaggio decifrabile solo dal destinatario
  - D: funzione di decifrazione utilizzata dal destinatario per leggere il messaggio cifrato (solo il destinatario la conosce)



Tipi di algoritmi di cifratura

L'algoritmo di cifratura è la funzione matematica usata per cifrare e decifrare il messaggio

- Algoritmi basati su carattere
  - sostituzione
    - ogni simbolo si trasforma in un altro simbolo dell'alfabeto
    - cambiano i simboli ma non il loro ordine nel testo
  - trasposizione
    - i simboli vengono permutati in base ad una permutazione stabilita
    - i simboli dell'alfabeto non cambiano ma cambia l'ordine in cui compaiono nel messaggio
- Algoritmi basati su chiave
  - oltre a definire l'algoritmo, si usa una chiave per cifrare/decifrare
  - lo stesso algoritmo, con chiavi diverse, produce testi cifrati diversi a partire dallo stesso testo in chiaro

Algoritmi a chiave segreta (simmetrica)

- La chiave K è la stessa per cifrare e decifrare il testo e deve essere nota contemporaneamente a chi invia e a chi riceve il messaggio

- Le funzioni di cifratura e decifrazione sono una l'inversa dell'altra:
  - D(E(P,K) , K) = P
  - E(D(C,K) , K) = C

- Alcuni algoritmi a chiave segreta
  - DES (1977): chiave a 56 bit, ormai insicuro
  - Triple DES (1979): chiave a 168 bit
  - AES (1997): chiave a 128, 192 o 256 bit

Crittografia a chiave pubblica (asimmetrica)

- Si usano due chiavi K_1 e K_2, una usata per cifrare l'altra per decifrare:

- La chiave di cifratura K_1 è resa nota (chiave pubblica)
- La chiave di decifrazione K_2 è segreta (chiave privata)
- E' praticamente impossibile dedurre K_2 da K_1
- Naturalmente deve valere $D(E(P,K_1), K_2) = P$

- L'algoritmo più noto è conosciuto con l'acronimo RSA (da Rivest, Shamir, Adleman - 1978)

Certificazione

- La chiave pubblica può essere pubblicata in un apposito elenco oppure semplicemente inviata all'inizio della comunicazione
  - L'elenco delle chiavi pubbliche è un potenziale punto debole per la sicurezza del sistema
- Esiste il problema della autenticità delle chiavi pubbliche
  - un utente può in malafede pubblicare una chiave a nome di un altro ed utilizzarla per sostituirsi a lui
- Si ricorre a terze parti, dette Certification Authority, che garantiscono l'integrità e l'autenticità dell'elenco delle chiavi pubbliche (racc. ITU X.509)
  - la Certification Authority deve essere al di sopra di ogni sospetto, compatibilmente con il livello di sicurezza desiderato
  - la Certification Authority genera un certificato contenente la chiave pubblica dell'utente e lo firma con la propria chiave privata
  - qualunque altro utente può verificare che il certificato sia stato effettivamente firmato dall'Authority

Controllo degli accessi: sistemi di autenticazione

- Utilizzano meccanismi differenti (che possono anche essere combinati tra loro)
- qualcosa che io so
  - password, pin
- qualcosa che io posseggo
  - carta magnetica, smart card
- qualcosa che io sono (sistemi biometrici)
  - impronta digitale, retina, voce, viso
- L'affidabilità di un sistema di autenticazione è tanto più alta quanto più l'elemento identificativo è unico e riservato
  - falsificare una firma è più semplice che indovinare una password e, nello stesso ambito, password complicate sono più difficili da indovinare di password semplici
- La combinazione di più sistemi ne aumenta la sicurezza
  - bancomat = possesso + conoscenza

Controllo degli accessi: sistemi di autenticazione

- L'accesso ad informazioni protette deve essere ristretto alle sole persone autorizzate
  - Questo vale anche per i programmi che processano tali informazioni
- Questo richiede che vengano messi in atto meccanismi di controllo degli accessi per proteggere l'informazione
  - La sofisticatezza dipende dal "valore" delle informazioni
- I meccanismi di controllo degli accessi si basano su identificazione e autenticazione

Identificazione: è un'asserzione sull'identità di una persona.
"Salve, sono il sig. Pippo" … Ma sarà vero?

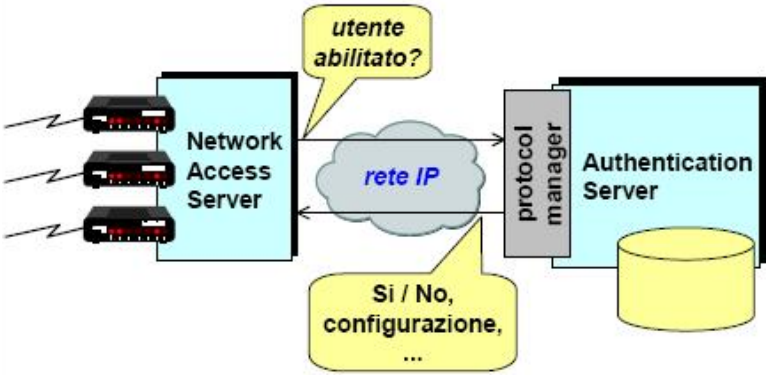
Autenticazione: è l'atto di verificare la veridicità di una identificazione
Verifico che chi dichiara di essere il Sig. Pippo sia veramente lui

Password

- In Internet sono più diffusi sistemi basati sulla conoscenza di qualcosa che sul possesso
  - difficoltà verificare se possesso e' lecito o legato a sottrazione
- Password statiche (nome account e password fissa)
  - in genere memorizzate nei sistemi sotto forma di hash
  - debolezze
    - scelta di password semplici (date nascita, matrimonio, nome figli, mogli,.)
    - furto per scrittura in luoghi accessibili (tastiera, cassetto, ...)
  - contromisure:
    - regole sulla complessità, aging, pwd history
- Password one time (password usate una sola volta in una comunicazione e poi scartate)
  - furto della password non consente utilizzi successivi
  - differenti modalità di generazione:
    - a partire da una chiave segreta S-key
    - a partire da una Smart Card)

NAS (Network Access Server)

- Un NAS è un singolo punto di accesso ad una risorsa remota
- Un NAS ha il compito di proteggere l'accesso a risorse
  - Esempi: stampanti, pc, Internet
- Funzionamento:
  - Un client si connette ad un NAS
  - Il NAS si appoggia ad un'altra "entità" per validare le credenziali fornite del client
  - Sulla base della risposta, il NAS permette o meno l'accesso alla risorsa protetta
- Il NAS non contiene pertanto nessuna informazione riguardo a
  - Quali client possono connettersi
  - Quali credenziali sono valide
- Il NAS si limita ad inviare ad un'altra entità in grado di processare le credenziali



… ma chi è l'entità che certifica?

Radius

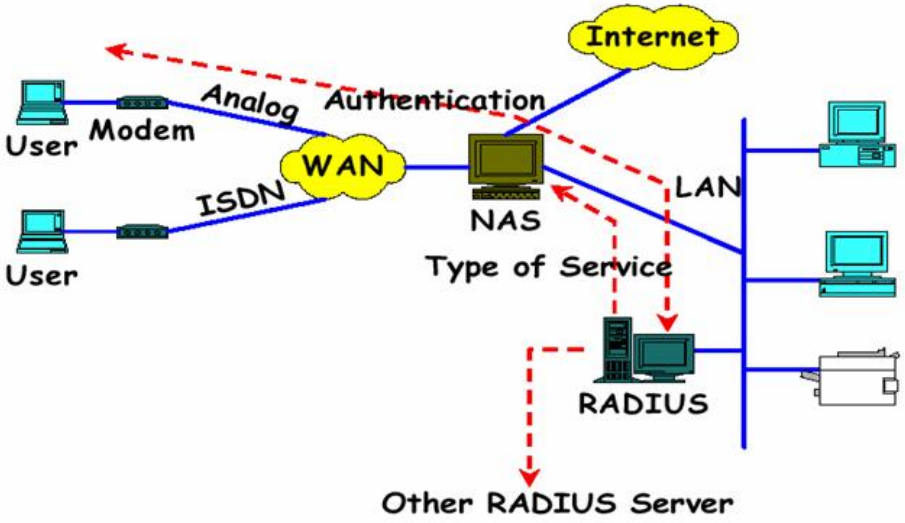
… generalmente un AAA server!

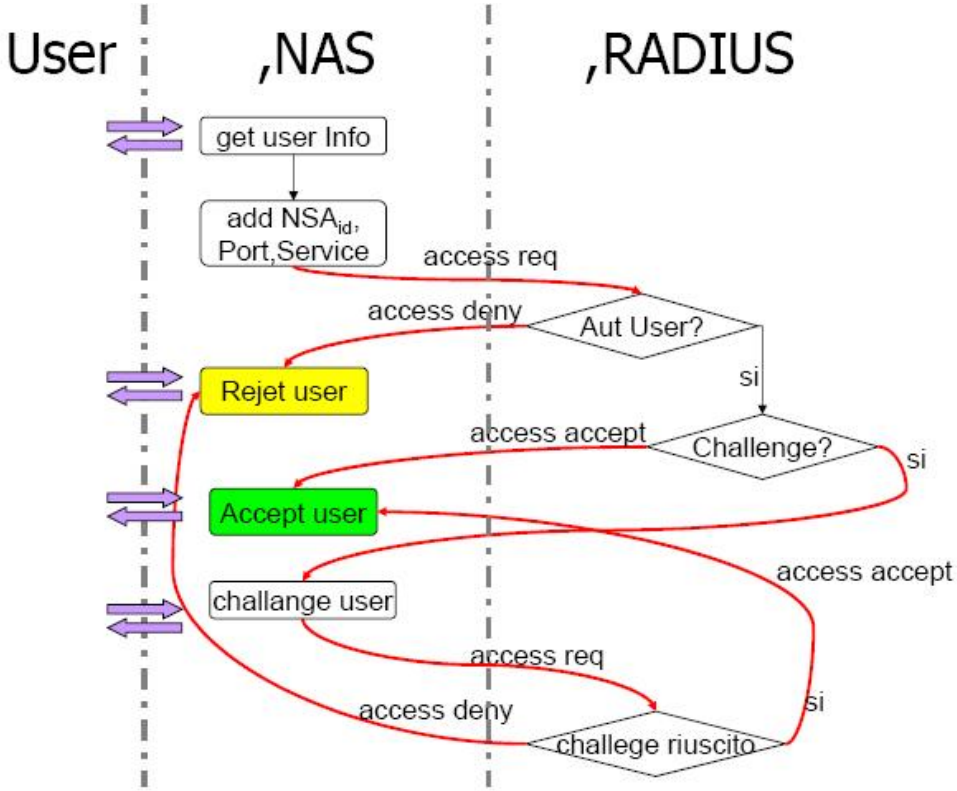
- Un AAA server è una entità che utilizza il protocollo AAA (Authentication, Authorization, Accounting) per effettuare autenticazione

- Per l'autenticazione remota, sia nei nuovi sistemi (mobili) che in quelli già esistenti, attualmente lo standard de-facto del protocollo AAA è RADIUS (Remote Access Dial-In User Service)
- RADIUS è utilizzato in applicazioni di accesso alle reti o di mobilità IP
  - è comunemente usato per dispositivi di rete integrati come router, server modem, switch, ecc…
  - utilizza pacchetti UDP
  - RADIUS fornisce alcuni livelli di protezione contro attacchi attivi e di sniffing

- Nonostante il suo buon funzionamento, è stato messo a punto un nuovo protocollo, Diameter, candidato a rimpiazzare RADIUS
  - utilizza infatti TCP anziché UDP ed è di conseguenza considerato più sicuro ed affidabile.

Funzionamento

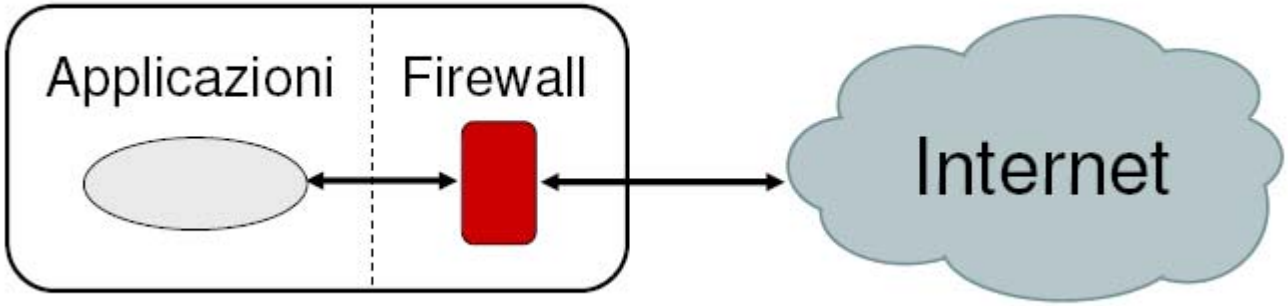




Firewall

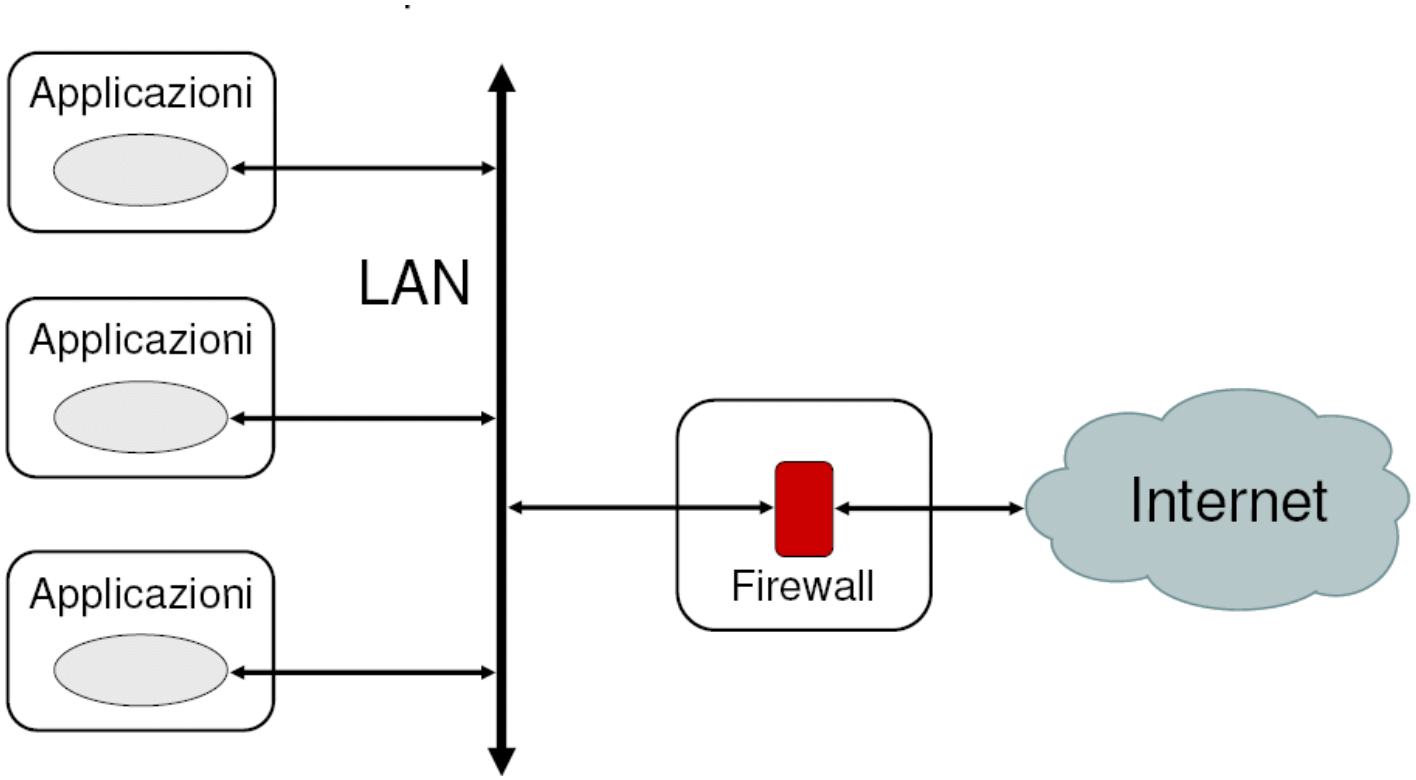
- Un firewall è un filtro software che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete
  - Processo che filtra il traffico in ingresso e in uscita da una rete
  - E' una barriera tra due reti

- Se si tratta di un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni, allora è considerabile come protezione di un host



Firewall

- Viene considerato una protezione di rete se il firewall è una macchina dedicata che filtra tutto il traffico da e per una rete locale



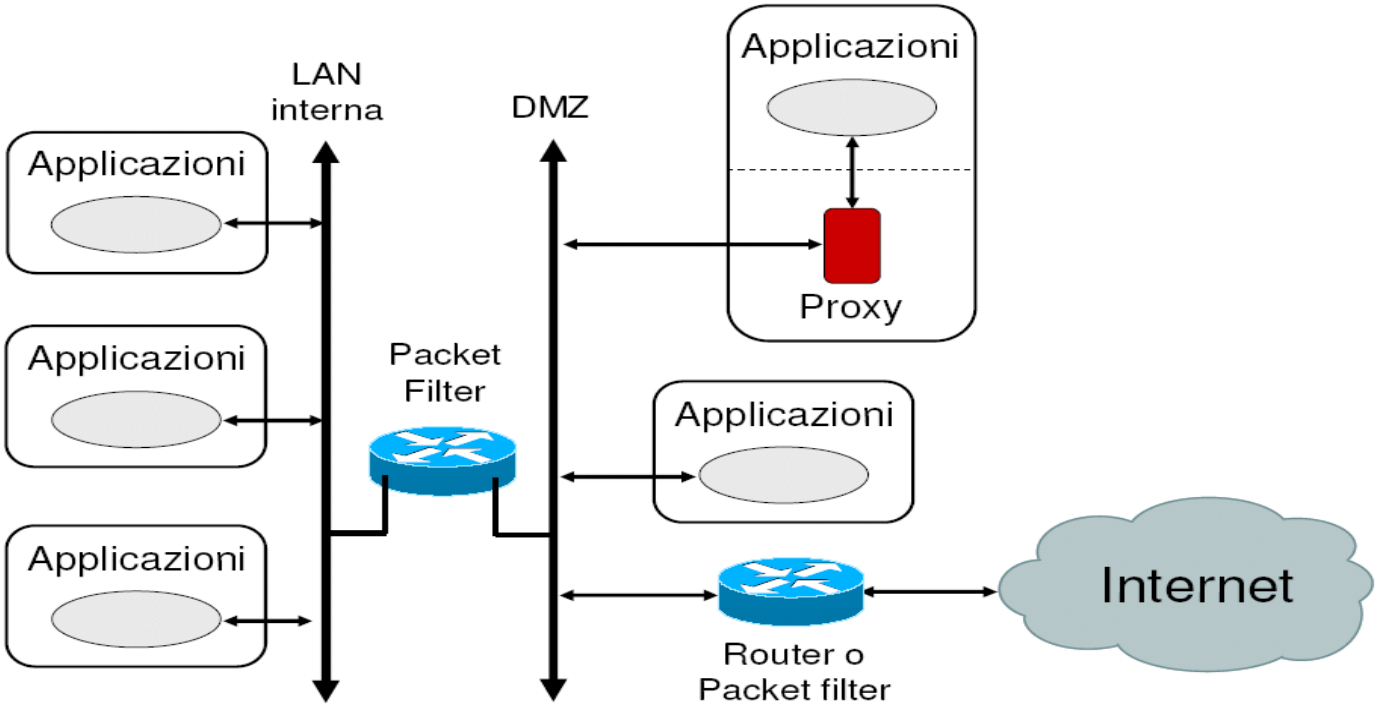
Packet Filter / Proxy Server

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
  - Solo il traffico autorizzato deve attraversare il firewall

- Un firewall può essere implementato come
  - packet filter
    - si interpone un router fra la rete locale ed Internet
    - sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
  - proxy server
    - esempio: nella rete protetta l'accesso ad Internet è consentito solo ad alcuni host
    - si interpone un server apposito detto proxy server per realizzare la comunicazione per tutti gli host
    - il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale

Esempio di configurazione firewall

- Quando una rete deve comprendere anche dei server che ospitano servizi pubblici (web, ftp, etc.), questi server sono collocati in una zona della rete chiamata DMZ (de-militarized zone)
- Una DMZ permette di creare un'area sicura della rete (su cui sono posti i server "pubblici") in cui far accedere il traffico esterno in maniera sicura e di evitare che questo traffico si diriga verso la rete di computer interna



I sistemi di rilevamento delle intrusioni (IDS)

- Studiati per rilevare attacchi tipici di Internet
- Forniscono diversi livelli di allarmi
- Possono bloccare i processi pericolosi
- Possono modificare la configurazione dei firewall
- Funzionamento:
  - Informazioni prelevate da “sensori” e da LOG
  - Rilevamento degli attacchi mediante il confronto con informazioni su data base (attack signature)
  - Rilevamento di situazioni anomale
    - eccessivo traffico di rete
    - protocolli anomali
    - atipica distribuzione statistica di valori (ad es.lunghezza pacchetti)

Considerazioni

- Classificazioni:
  - Network Intrusion Detection System (NIDS)
    - sono dotati di sensori sulla rete esterna
    - analizzano in tempo reale il traffico
    - non intercettano il traffico cifrato
  - Host Intrusion Detection System (HIDS)
    - sono installati sul sistema stesso
    - analizzano in tempo reale le attività
  - Distributed Intrusion Detection System (DIDS)
    - utilizzano vari tipi di sensori (reti, sistemi, LOG…)
    - individuano gli attacchi correlando informazioni di varia natura
- Limiti degli IDS
  - Grande quantità di informazioni aggiuntive
  - E’ necessario un esperto che sia in grado di intraprendere opportune azioni
  - Possibili disservizi per falsi positivi
  - I sensori devono essere opportunamente protetti

Fine