CIFRARI

Il **CIFRARIO** è un sistema che permette di:

- Cifrare
- Decifrare
- Generare e Gestire chiavi crittografiche.

Può essere:

- Aperto
- Chiuso

Definizioni

- **Plaintext** - testo prima della encryption
- **Ciphertext** - testo dopo l'encryption

SIMMETRICI (chiavi condivise)

Caratteristiche: - Mittente e Ricevente hanno la stessa chiave K - Cifratura e decifratura sono efficienti - Difficilissimo decifrare senza conoscere la chiave (essendo l'informazione necessaria)

Cifrari 'pre-informatici':

- **Character-oriented**
  - **Cifrario di Cesare**
    - monoalfabetici a 1 lettera
  - **Cifrario di Playfair** (monoalfabetico a 2 lettere)
  - **Cifrario di Vigenere** (polialfabetico)
- **Bit-oriented**
  - Cifrario di Vernam e one-time pad
- **A Sostituzione** - un gruppo di caratteri viene sostituito con un altro gruppo di caratteri
- **A Permutazione** - gruppi di caratteri vengono spostati nel testo
- Cifrari *monoalfabetici* a N lettere - Ogni N-upla di lettere del testo viene sostituita sempre dalla stessa sequenza di lettere
- Cifrari *polialfabetici* - Una lettere o N-upla di lettere può essere **cifrata diversamente** a seconda della sua posizione nel testo

Cifrari monoalfabetici a 1 lettera Come il cifrario di **Cesare**, ma la chiave K identifica una sostituzione per ciascuna lettera (es. a-q, b-q, c-f,...): *abcdefghilmnopqrstuvz qzfabdeohilmnprstcugv* **Esistono** $N!$ **diverse chiavi per** N **lettere.** - Non si può provare a decifrare manualmente (brute force) tutte le possibili chiavi (come in **Cesare**) - Molto deboli a causa di *regolarità* statistiche - **Crittanalisi Statistica** che considera la frequenza delle lettere del testo con la frequenza delle lettere in un linguaggio

Cifrari monoalfabetici a N lettere Ogni sequenza di N lettere viene sostituita con una sequenza fissata di N lettere. Per esempio (aa-qe, ab-zi, ba-df, ...) - Migliore di $N = 1$ (a una lettera) - Rimane possibile **Crittanalisi statistica** (più il testo è lungo e più facile sarà)

Cifrario di Playfair (monoalfabetico $N = 2$)

- Rimane possibile *Crittanalsi statistica*

Cifrari Polialfabetici

ASIMMETRICI (chiavi diversi per cifratore e decifratore)

FIREWALL

I Firewall vengono realizzati perche, in una rete, configurare e aggiornare ogni singolo computer e impossibile. Mantenere, invece, un singolo punto di controllo e piu facile. Quindi vengono usati per filtrare il traffico e proteggere i computer della rete.

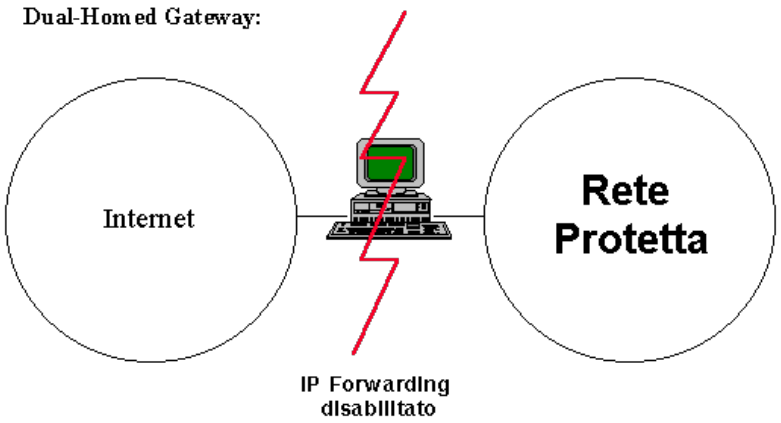
- il FW d l' i il FW deve essere l'unico punto di contatto della rete interna con quella esterna
- solo il traffico "autorizzato" può attraversare il FW
- il FW deve essere un sistema altamente sicuro esso stesso

Funzionalita:

1. Filtri sulla base di:
   - Destinazione
   - Servizi
   - Utente
2. Log di:
   - traffico complessivo
   - azioni dei singoli utenti
3. Generazione di allarmi

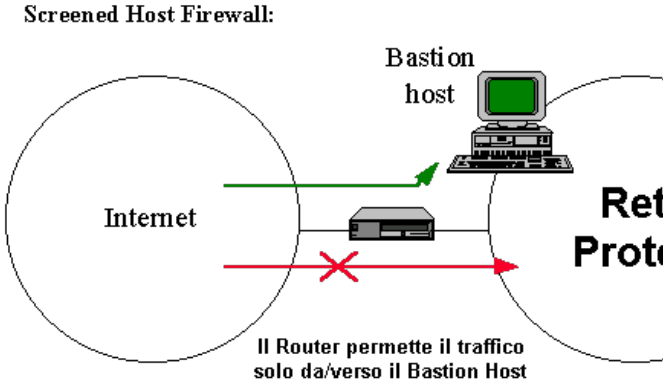
Tipi di configurazione:

1. **Screening Router**
   - uso del router per filtrare il traffico sia livello IP che superiore
   - non richiede hardware dedicato
   - non necessita di proxy (quindi di modifiche agli applicativi)
   - insicuro
   -
2. **Dual-homed gateway**
   - Facile realizzazione
   - richiede poco hardware (il SW firewall su PC o Calcolatore Custom0)
   - possibile mascherare la rete interna
   - scarsamente flessibile



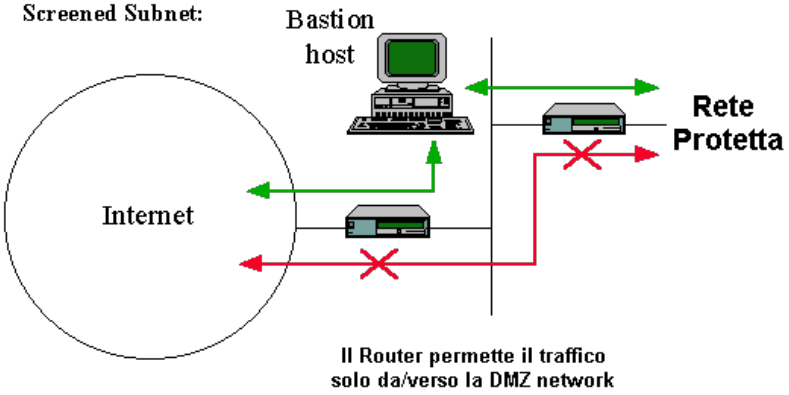
- grosso sovraccarico di lavoro

3. **Screened host gateway**
   - servizi forniti da un calcolatre (bastion host) con funzione di application gateway
   - separazione della rete interna viene realizzata dal router
   - router filtra i pacchetti in maniera tale che solo il bastion host possa aprire connessioni con la rete esterna.
   - tutti i sistemi esterni che desiderino collegarsi con la rete privata possono connettersi solo con il bastion host



   - Eccezioni: protocolli abilitati direttamente
4. **Screened subnet**
   - firewall viene realizzato utilizzando due router che creano una rete, compresa tra loro, detta rete perimetrale, su cui si trovano le macchine (bastion host)
   - **bastion host** forniscono i servizi (ad esempio l'application gateway e il server di posta elettronica)
   - router esterno filtra il traffico tra Internet e la rete perimetrale (in accordo con la politica di accesso ai servizi stabilita per la rete)
   - il router interno protegge la rete privata sia da Internet che della rete perimetrale consentendo esclusivamente il transito di pacchetti da e verso i bastion host.

- E' possibile configurare i due router in maniera tale da consentire il transito di traffico che si considera fidato tra Internet e la rete interna senza la mediazione di application gateway



Tipi di configurazione: 1. **Packet Filter** - Filtra in base a: - Direzione del pacchetto - Direzione della connessione - Indirizzo IP (sorgente e destinazione) - Servizio (porta sorgente e destinazione) - Difficolta' con alcuni protocolli - Non mantiene log - Difficile monitorare attacchi mentre avvengono Un **problema** importante nella configurazione di un firewall riguarda la **frammentazione IP**. Infatti se un pacchetto viene frammentato in pezzi molto piccoli, ogni parte può essere tanto ridotta da non includere neanche l'header TCP e quindi la porta utilizzata nel firewall per filtrare. Questo succede per frammenti di poco più di 20 byte, che sono comunque ingiustificati rispetto a qualsiasi MTU. Tali frammenti corti devono quindi essere tagliati.

Un'altra regola importante e' bloccare tutti i pacchetti con l'opzione di **source routing** perche' **permette IP spoofing** con TCP su WAN.

2. **Application Proxy**
   - Connessioni dirette tra interno ed esterno sono **proibite**
   - Possibili solo connessioni attraverso il firewall
   - Ogni servizio dev'essere configurato
   - Non trasparente
   - richiede host dedicato
   - Prestazioni medie
   - Sicuro
   - Mantiene log sofisticati
   - E' in grado di riferire il traffico agli utenti

Attenzione! Il firewall non risolve tutto: - non evita il problema di password deboli - non filtra traffico via modem - non tratta attacchi dall'interno - non evita problemi di sicurezza sui servizi e sui protocolli aperti verso l'esterno e, in generale, - non protegge da virus o simile portato su dischetto - evitare il 'denial of service'

NAT (Newtwork Address Translation)

NAPT (Networkd Adrress & Port Translation)

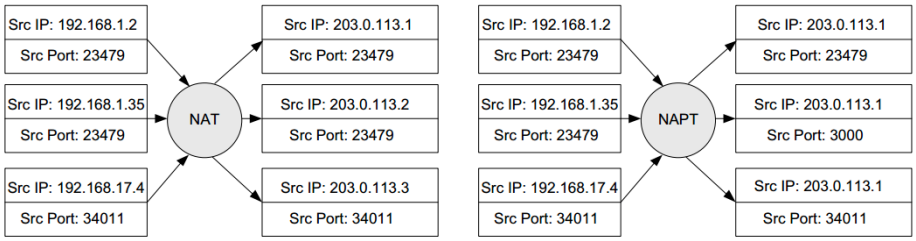


Figure 1: natnapt