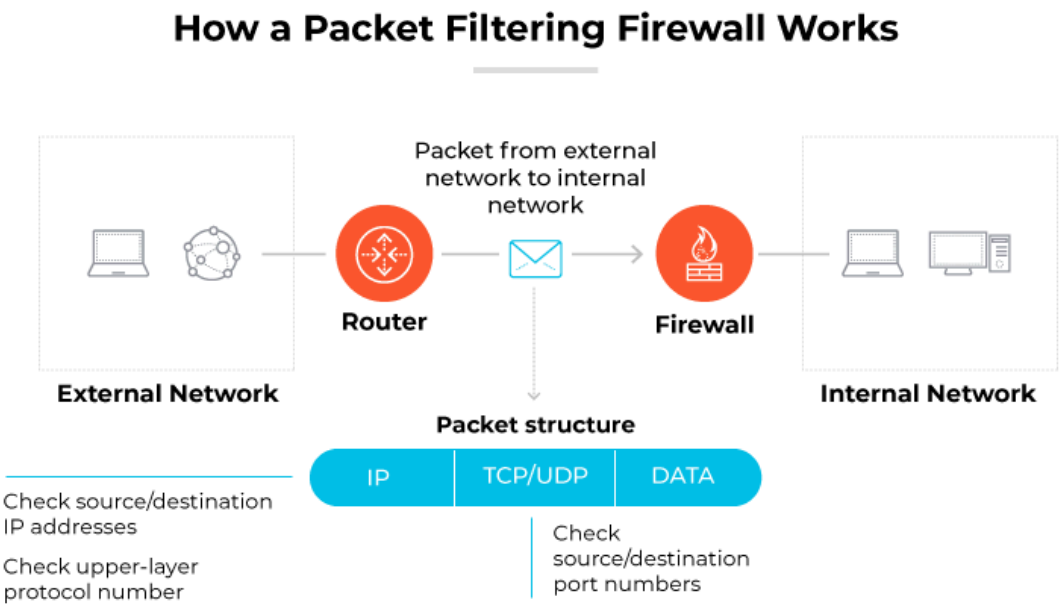
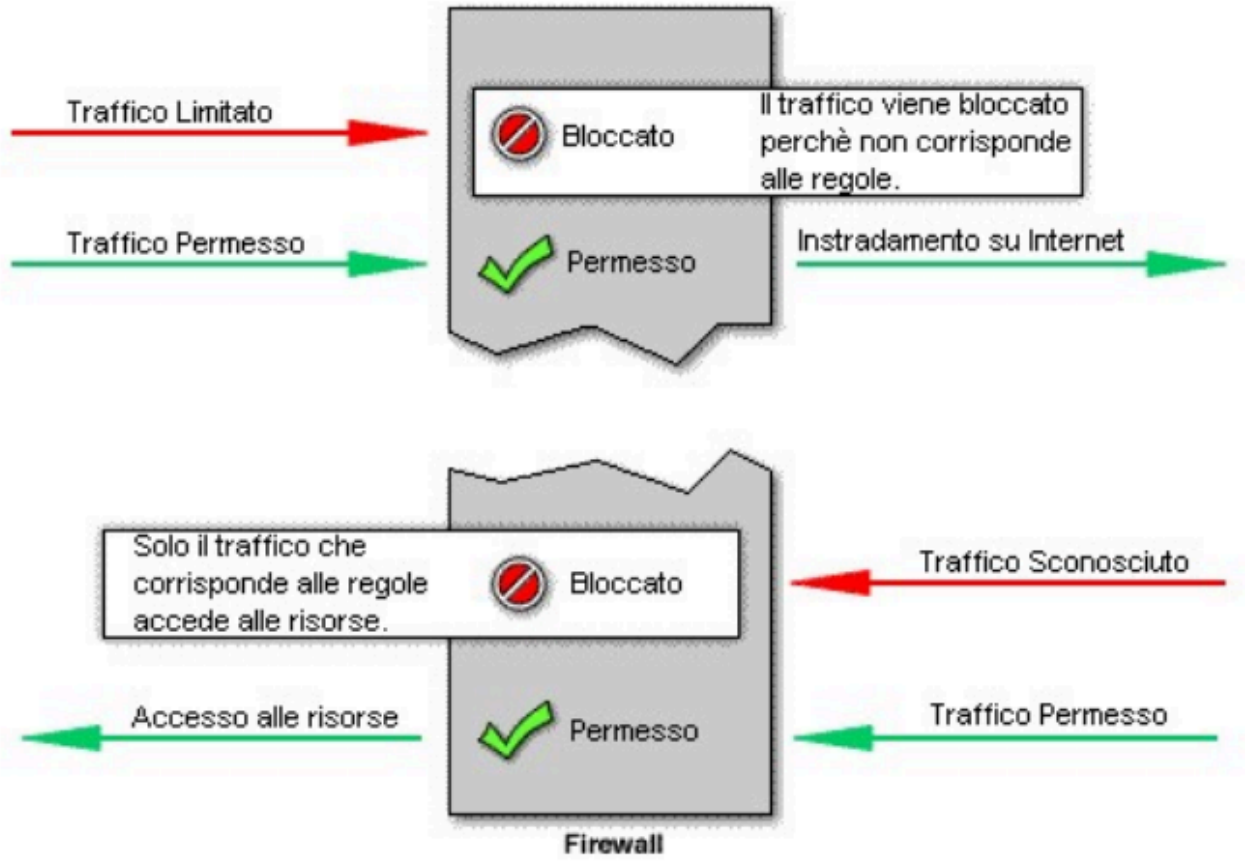
Packet Filter

- Software che guarda le intestazioni (*header*) dei singole pacchetti
- Agisce sulla base di regole definite dall'amministratore di rete (lista siti permessi / bloccati)
  - Ad esempio: sono a scuola, voglio accedere a un sito di streaming TV/serie
  - L'amministratore (admin) blocca l'accesso a quel sito
- Se un pacchetto ha il permesso, viene instradato (*routing*) a destinazione
- Una volta che li ha guardati, allora decide se
  - Accetta (*Accept*)
  - Scartare (*Deny*)
  - Rimandarlo indietro notificando il mittente (*Reject*)





Pro, Contro, Chi implementa

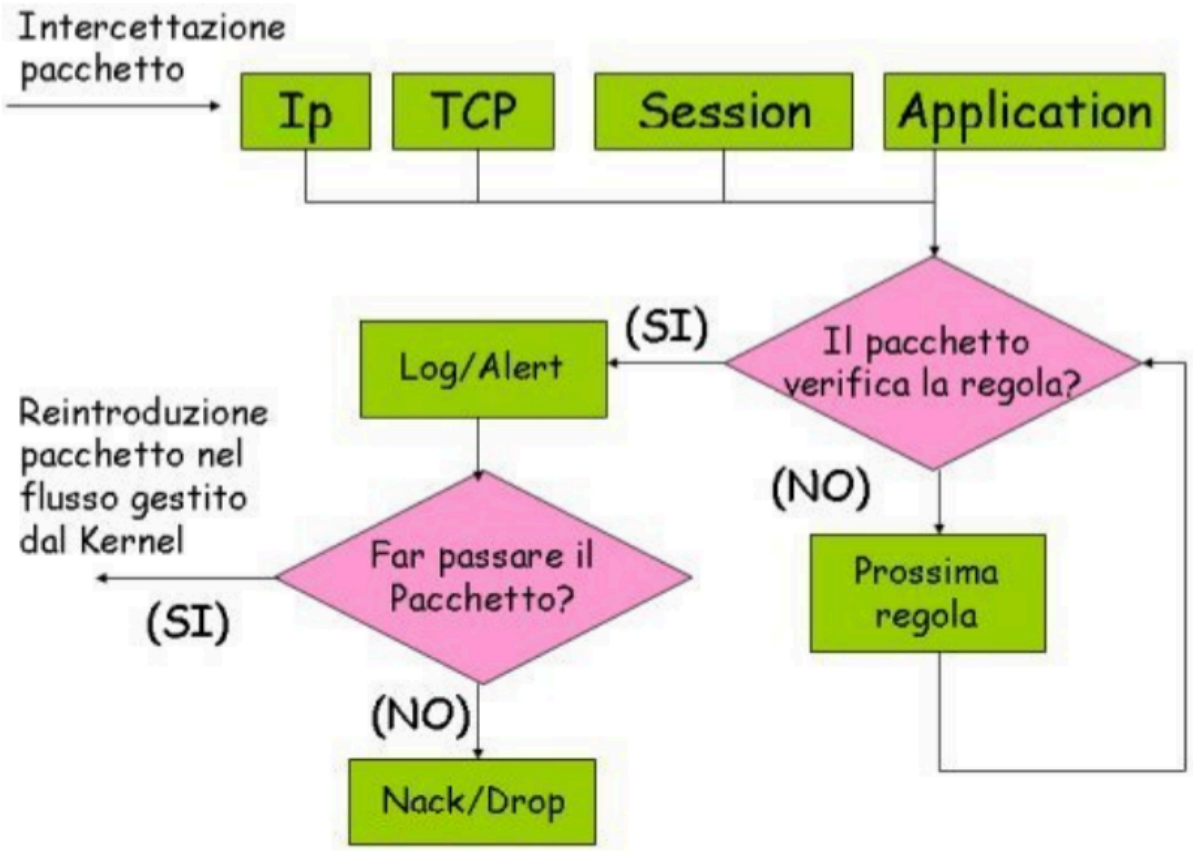
Chi implementa i packet filter?

- Normalmente, sono implementati dei *router*
- Siccome instradano i pacchetti, vogliamo capire come filtrare
  - Gli indirizzi IP (rete)
  - I numeri di porta (trasporto)

Pro/Contro dei Packet Filter:

- Pro: Sono veloci (ottime prestazioni)
- Contro: Controllano solo dove è diretto il pacchetto, non il contenuto del pacchetto (dati)

Schema Funzionamento Packet Filter



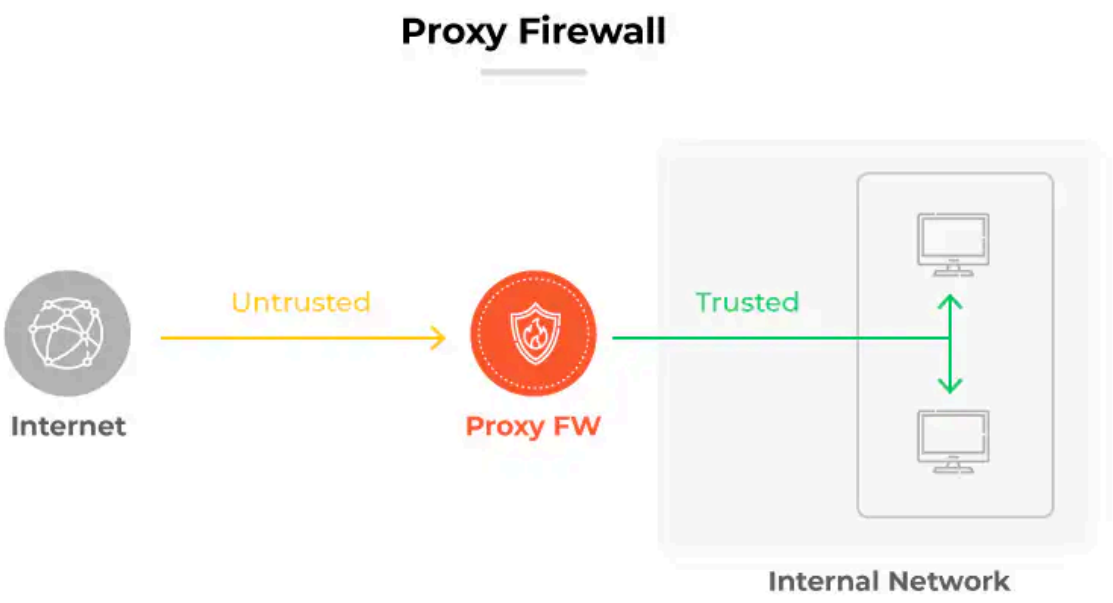
Ordine dello schema:

1. I vari livelli collaborano tra di loro
2. Il router usa il packet filter e verifica se il pacchetto rispetta le regole
    1. Se SI, allora vai avanti alla prossima
    2. Se NO, salvo il log (= informazioni su quello specifico accesso es. ora / disp. etc.)
        1. Verifico se far passare il pacchetto
            1. Se SI, proseguo e reintroduco il pacchetto nella rete
            2. Se NO, mando un ACK negativo (NACK = Negative ACKnoledgement = Risposta negativa al mittente) e poi "droppo" il pacchetto (cancello)

Application Proxy

Premesse e significati:

- Proxy = Intermediario = Filtri "in mezzo alla rete"
- Application proxy
    - Implementa regole a livello applicativo (*firewall*)
    - Controlli fatti "solo" a livello server (client - router - server)

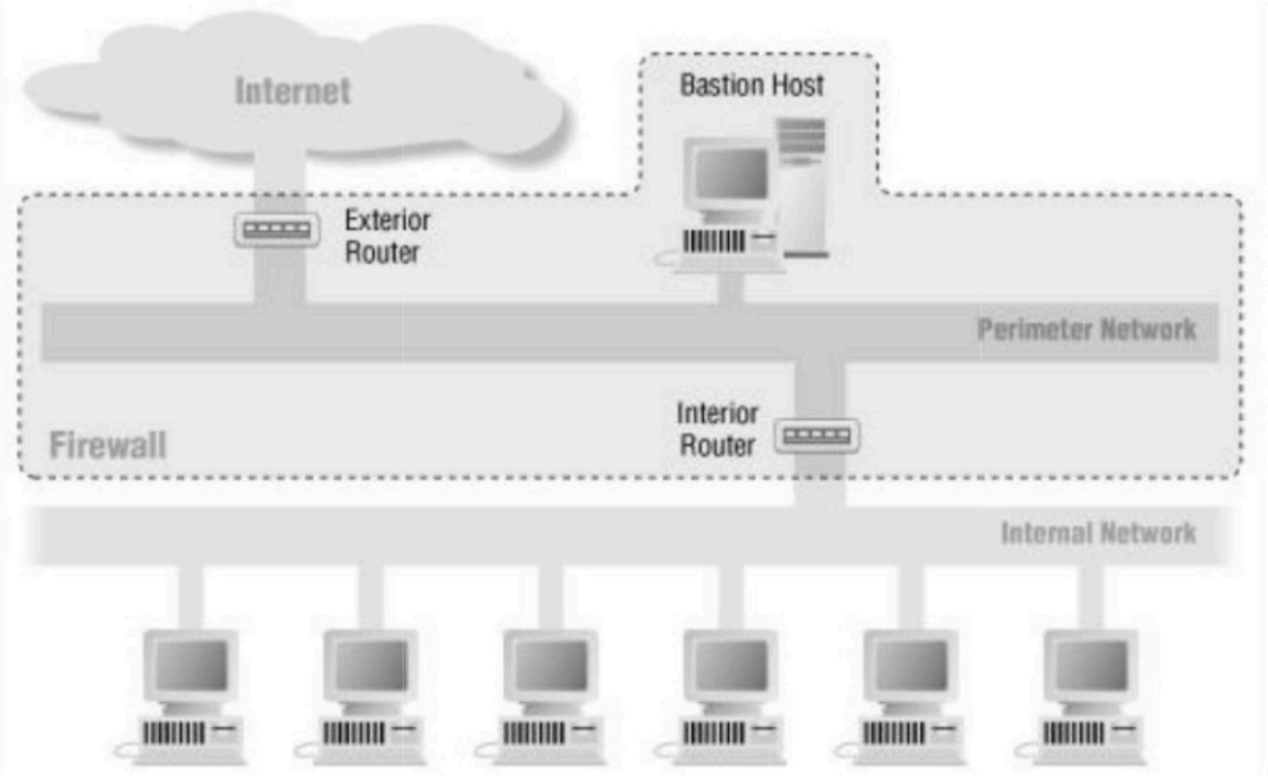


Logica schema:

- Usiamo un firewall per "regolare" l'accesso "al mondo esterno" (internet)
- Facciamo entrare solo il traffico "trusted"
- Ogni comunicazione di questo tipo richiede due connessioni:
  1. Una dal client al firewall e
  2. L'altra dal firewall al server

Firewall, Pro e Contro

> *Definizioni utili*:
>
> - Firewall = Insieme di regole hardware / software applicate in rete
> - Firewall Proxy = Blocca sulla base di regole indirizzi IP, protocolli e porte
> - Proxy Server = Connette il client al resto se le regole lo permettono



Contro:

1. Drastiche diminuzioni a livello prestazioni
    1. A causa del doppio traffico client-server e viceversa
2. Costrizione dell'utente alla configurazione del proxy
    1. Sforzo da parte dell'utente e consapevolezza
3. Ogni servizio (= applicazione) richiederebbe un firewall (=application proxy)

Pro:

1. Accesso preciso e controllato di ogni tipo di collegamento rete

Confronto Packet Filter e Application Proxy

Vantaggi

Packet Filter	Application Proxy
Basso utilizzo di risorse	Buon livello di sicurezza
Trasparente all'utente	Uso del livello applicazione
Buone Prestazioni	

Svantaggi

Packet Filter	Application Proxy
Basso livello di sicurezza	Proxy dedicato per ogni servizio
Accesso limitato all'header IP	Basse Prestazioni
Poca manipolazione informazioni	Vulnerabile a bug delle applicazioni

- Packet filter = Router che filtra le cose a livello 3 = network layer = rete
- Application proxy = Architettura client / server / firewall in cui filtriamo le cose a livello 7 = application layer = livello applicativo (= cambia in base al servizio usato)

Modello AAA

AAA = Autenthication / Authorization / Auditing

1. *Autenticazione*

Utente è rappresentato nel sistema in qualche modo che lo identifica *univocamente* (esiste solo lui). Ogni utente è rappresentato da uno ed un solo identificatore.

- Più identificatori per utente
- Più utenti per identificatore

2. *Autorizzazione*

Ad ogni utente vengono assegnati i *permessi* che servono.

- Controllo di accessi
- Controllo di autenticazione
- Autorizzazione richieste di accesso

3. *Audit (Adeguatezza)*

Operazione classica svolta nell'ambito cybersecurity che verifica che un certo tipo di sistema rispetti determinate specifiche (controllo ad alto livello) --> *adeguatezza*

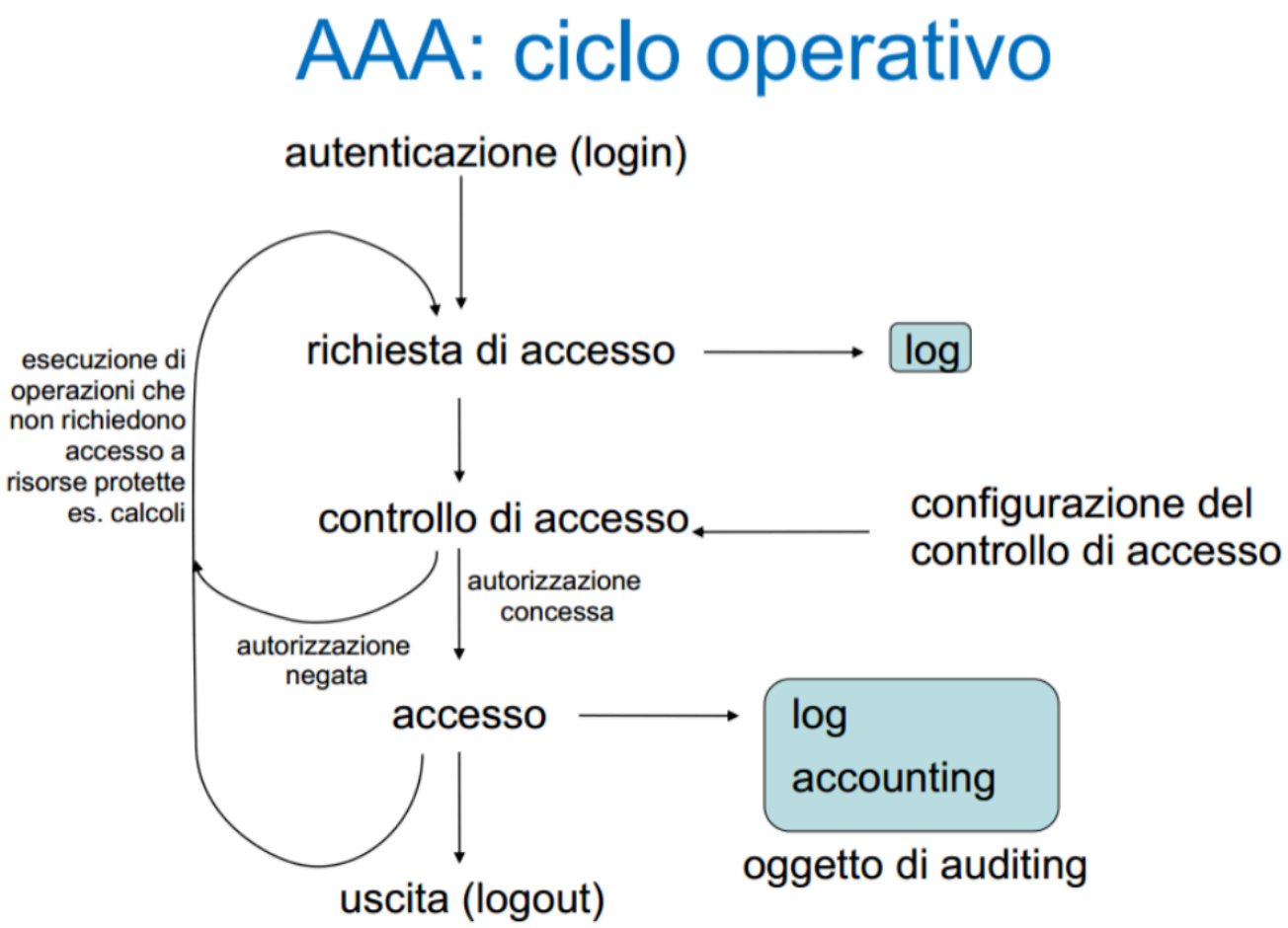
Cosa si controlla?

- Per ogni dispositivo, le richieste di autenticazione / accesso

- Per ogni dispositivo, il rispetto di determinate caratteristiche hardware / software

Esempio: Verifichi che un'azienda rispetti determinati requisiti --> Standard

- Access auditing
- Log auditing (log = informazioni)
- System security auditing (= sicurezza rete)



Politiche di accesso (Access Control)

1. DAC = Discretionary Access Control

Tipo di controllo dell'accesso in cui il proprietario di una risorsa limita l'accesso alla risorsa in base all'identità degli utenti -> discrezione in base alla persona.

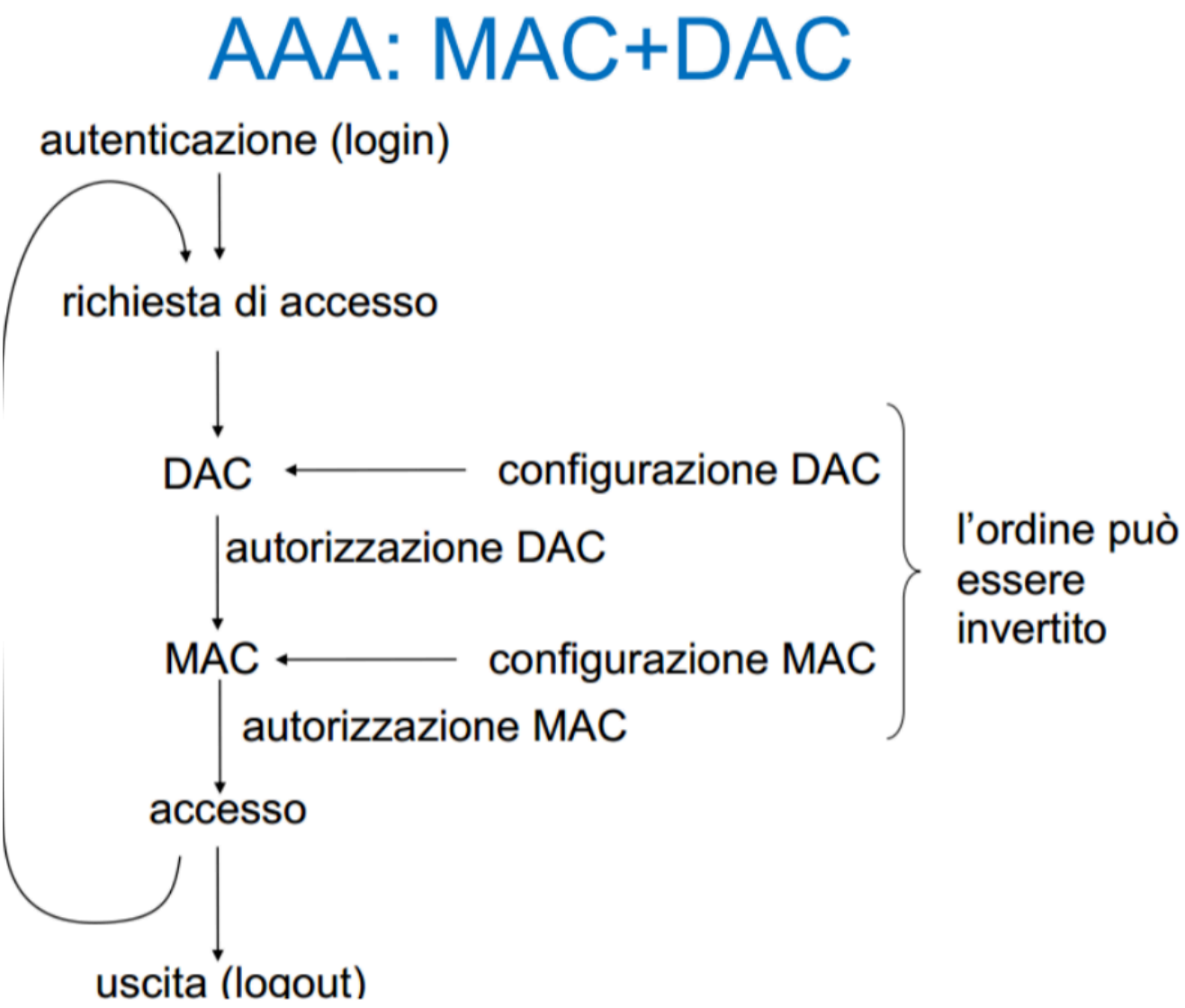
- Sicurezza delegati agli utenti
- Diffuso e flessibile

2. MAC = Mandatory Access Control

Tipo di controllo degli accessi che limita l'accesso alle risorse in base all'autorizzazione dei soggetti -> cambia in base al tipo di risorsa.

- Sicurezza delegata al solo amministratore

- Solo l'amministratore configura tutto



> MAC = Ci pensa l'admin
> DAC = Lo può gestire da solo l'utente

Le tre AAA vengono verificate a livello due (collegamento = data link) ISO/OSI, mentre ai livelli superiori bisogna garantire la segretezza dei dati

Accenni a fine appunti

Volendo, assieme ai precedenti, usiamo anche:

- CHAP / EAP = Controllo accessi univoci utenti con hash
- IPSec = Comunicazione sicura end-to-end per dispositivi e applicazioni
- SSL/TLS = Garantisce segretezza a livello trasporto
- RADIUS / Kerberos = Protocolli di autenticazione basati su crittografia nel livello 7