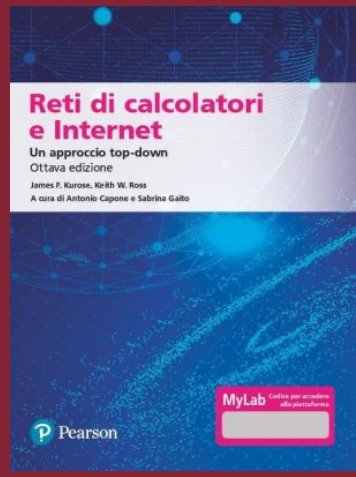
Reti di Elaboratori

Sicurezza nelle reti – WiFi, reti cellulari e firewall



SAPIENZA
UNIVERSITÀ DI ROMA

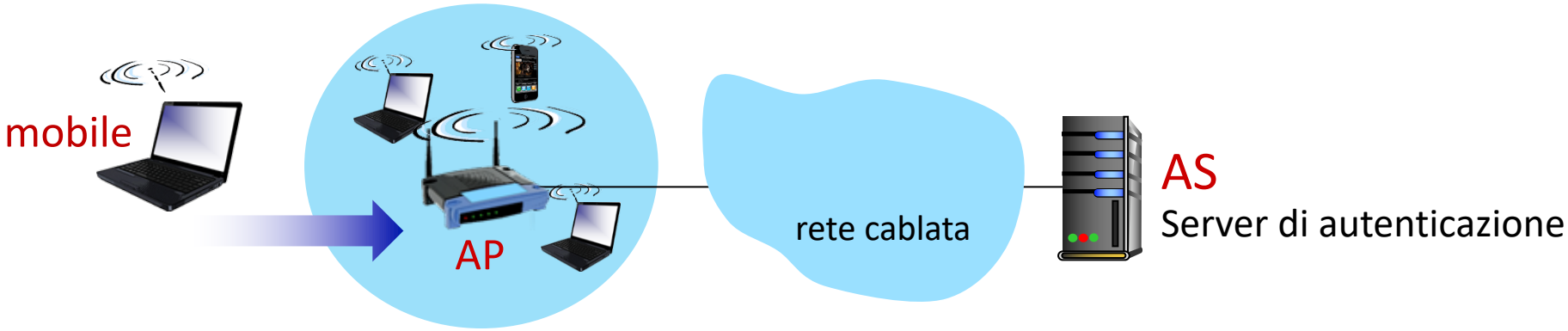
Alessandro Checco
alessandro.checco@uniroma1.it

Capitolo 8

Outline

- Che cos'è la sicurezza della rete?
- Principi di crittografia
- Autenticazione, integrità del messaggio
- Protezione della posta elettronica
- Protezione delle connessioni TCP: TLS
- Sicurezza a livello di rete: IPsec
- **Sicurezza nelle reti wireless e mobili**
  - 802.11 (WiFi)
  - 4G/5G
- Sicurezza operativa: firewall e IDS

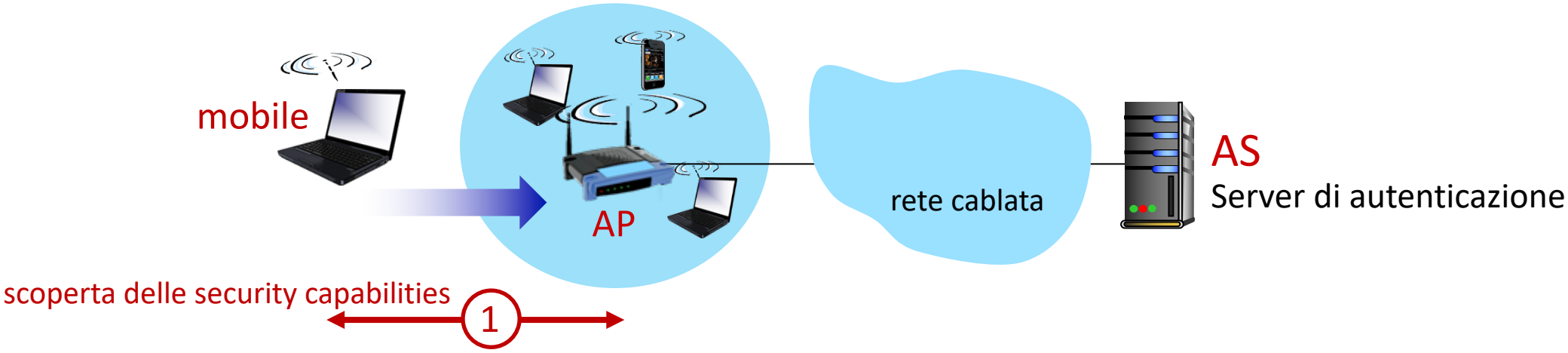
802.11: autenticazione, crittografia



Il cellulare in arrivo deve:

- associare al AP: (stabilire) la comunicazione tramite collegamento wireless
- autenticarsi alla rete

802.11: autenticazione, crittografia

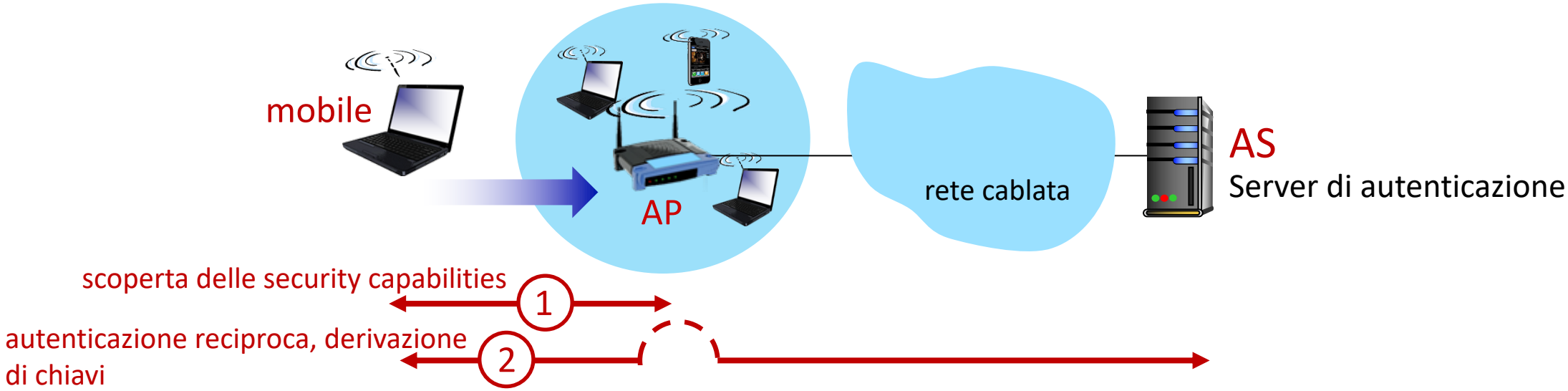


1 scoperta delle security capabilities:

- AP pubblicizza la sua presenza, le forme di autenticazione e crittografia supportate
- il dispositivo richiede moduli specifici di autenticazione, crittografia desiderata

sebbene dispositivo e AP stiano già scambiando messaggi, il dispositivo non è ancora autenticato, non dispone di chiavi di crittografia

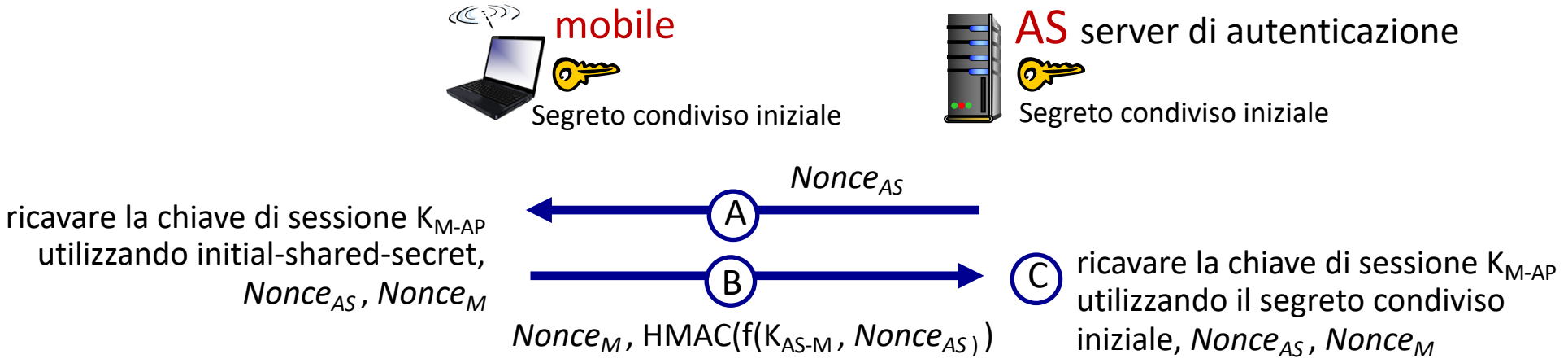
802.11: autenticazione, crittografia



2 autenticazione reciproca e derivazione a chiave simmetrica condivisa:

- AS e i dispositivi mobili hanno già un segreto comune condiviso (ad es. password)
- AS e dispositivo mobile usano segreto condiviso, nonces (previene gli attacchi replay), hashing crittografico (garantisce l'integrità del messaggio) per autenticarsi a vicenda
- AS e mobile derivano la chiave di sessione simmetrica

802.11: handshake WPA3

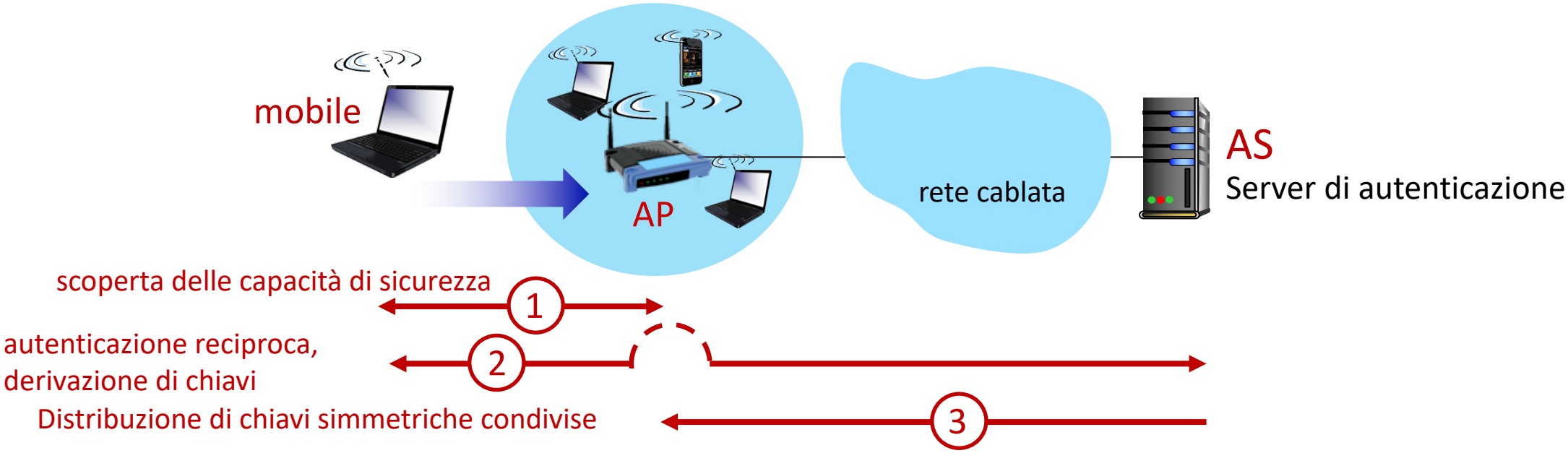


a) AS genera $Nonce_{AS}$, invia al mobile

b) mobile riceve $Nonce_{AS}$
- genera $Nonce_M$
- genera la chiave di sessione condivisa simmetrica $K_{M\text{-}AP}$ utilizzando $Nonce_{AS}$, $Nonce_M$ e il segreto condiviso iniziale
- invia $Nonce_M$, e Valore firmato da HMAC utilizzando $Nonce_{AS}$ e segreto condiviso iniziale

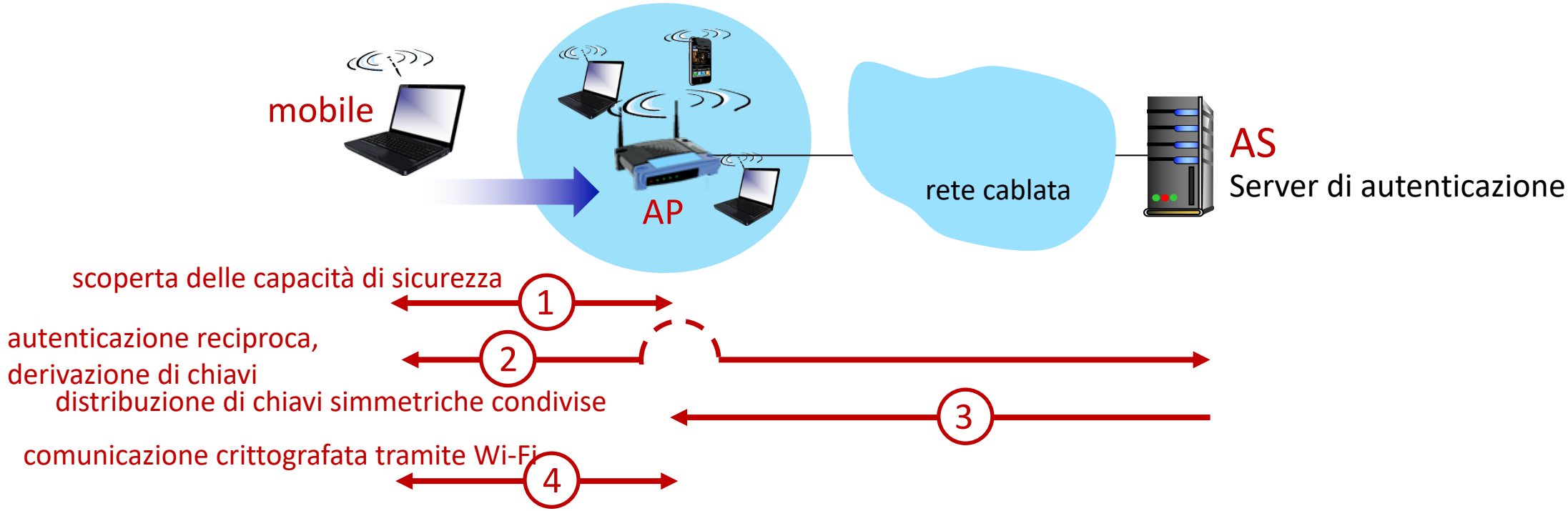
c) AS deriva la chiave di sessione condivisa simmetrica $K_{M\text{-}AP}$

802.11: autenticazione, crittografia



3. distribuzione della chiave di sessione simmetrica condivisa (ad esempio, per la crittografia AES)
   - stessa chiave derivata in mobile e AS
   - AS informa AP della sessione simmetrica condivisa

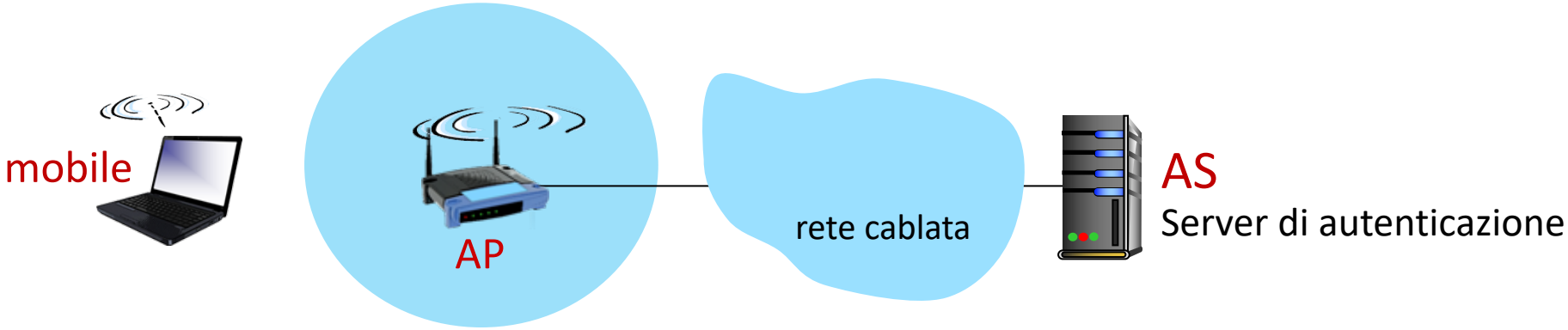
802.11: autenticazione, crittografia

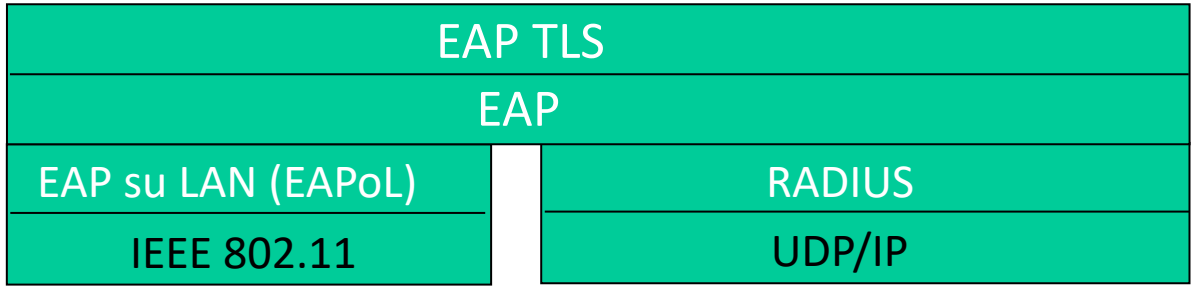


4 comunicazione crittografata tra host mobile e remoto tramite AP

- stessa chiave derivata tra mobile e AS
- AS informa AP della sessione simmetrica condivisa

802.11: autenticazione, crittografia



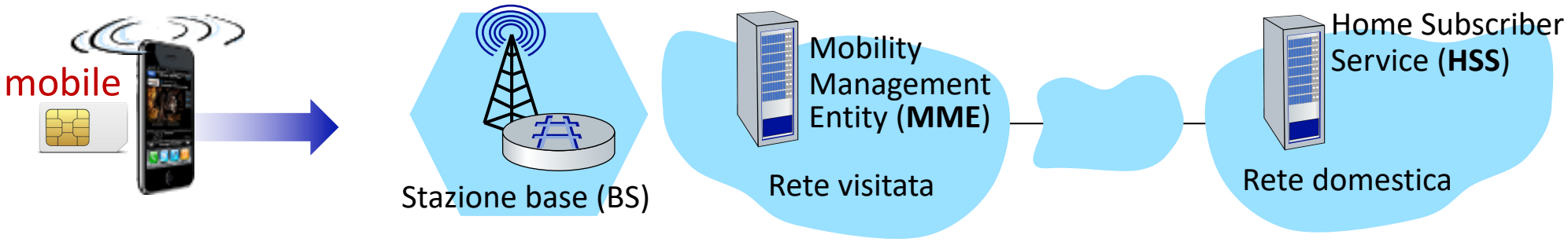


- Extensible Authentication Protocol (EAP) [RFC 3748] definisce il protocollo di richiesta/risposta end-to-end tra dispositivo mobile e AS

Outline

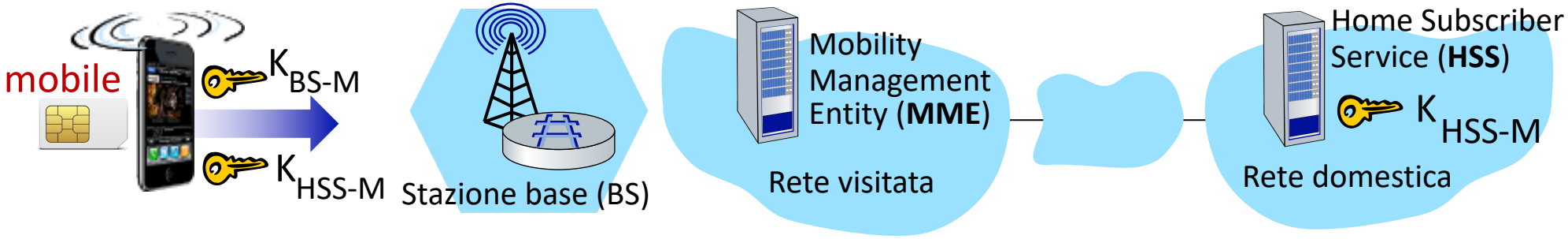
- Che cos'è la sicurezza della rete?
- Principi di crittografia
- Autenticazione, integrità del messaggio
- Protezione della posta elettronica
- Protezione delle connessioni TCP: TLS
- Sicurezza a livello di rete: IPsec
- **Sicurezza nelle reti wireless e mobili**
  - 802.11 (Wi-Fi)
  - 4G/5G
- Sicurezza operativa: firewall e IDS

Autenticazione, crittografia in 4G LTE



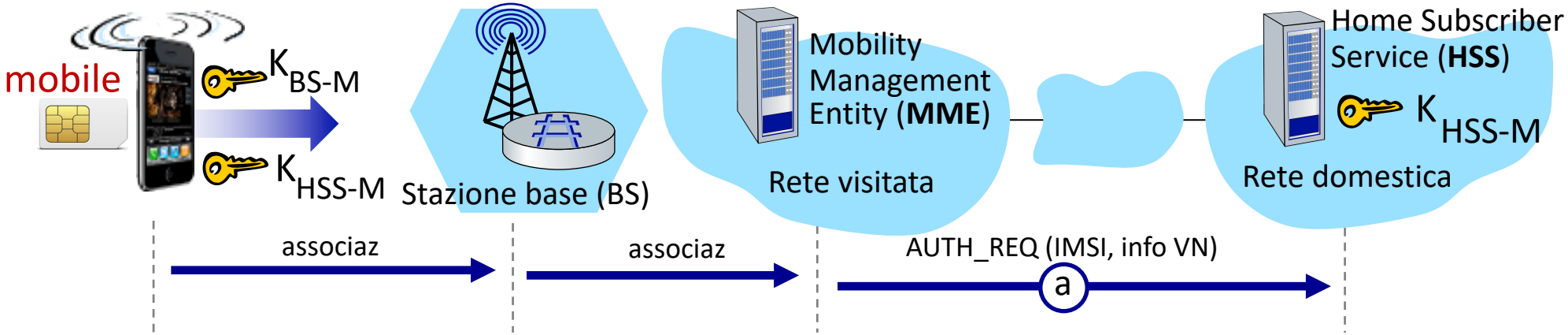
- il cellulare in arrivo deve:
  - associarsi a BS: (stabilire) la comunicazione tramite collegamento wireless 4G
  - autenticarsi alla rete e autenticare la rete
- notevoli differenze rispetto al WiFi
  - la carta SIM del cellulare fornisce un'identità globale, contiene chiavi condivise con la rete domestica (alla quale siamo abbonati)
  - i servizi nella rete visitata dipendono dall'abbonamento al servizio (a pagamento) nella rete domestica

Autenticazione, crittografia in 4G LTE



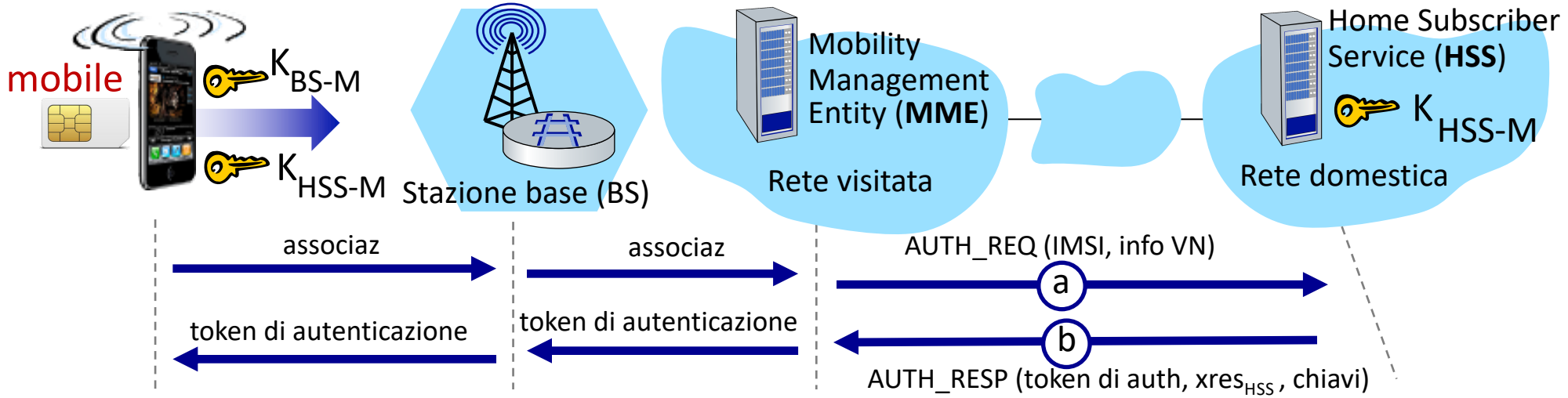
- mobile e BS utilizza la chiave di sessione K_{BS-M} per crittografare le comunicazioni tramite collegamento 4G
- MME nella rete visitata + HHS nella rete domestica, insieme svolgono il ruolo di WiFi AS
  - l'autenticatore finale è HSS
  - fiducia e relazione d'affari tra reti visitate e domestiche

Autenticazione, crittografia in 4G LTE



a) richiesta di autenticazione alla rete domestica HSS
   - il cellulare invia un messaggio di associazione (contenente il suo IMSI, le informazioni sulla rete visitata) inoltrato da BS a MME e infine a HHS
   - IMSI identifica univocamente il cellulare

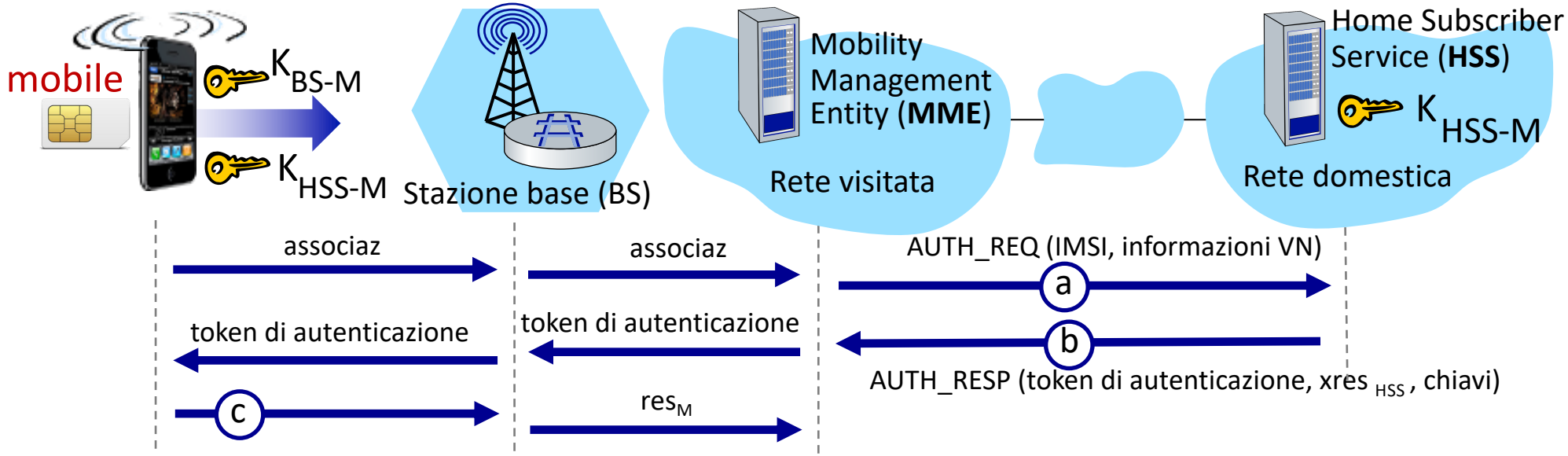
Autenticazione, crittografia in 4G LTE



b) HSS utilizza la chiave segreta condivisa in anticipo, K_{HSS-M} , per derivare il token di autenticazione, *auth_token* e il token di risposta di autenticazione previsto, $xres_{HSS}$

- *auth_token* contiene informazioni crittografate da HSS utilizzando K_{HSS-M} , consentendo al dispositivo mobile di sapere che chiunque abbia calcolato *auth_token* conosce il segreto condiviso in anticipo
- il cellulare ha una rete autenticata
- HSS visitato conserva $xres_{HSS}$ per un eventuale uso successivo

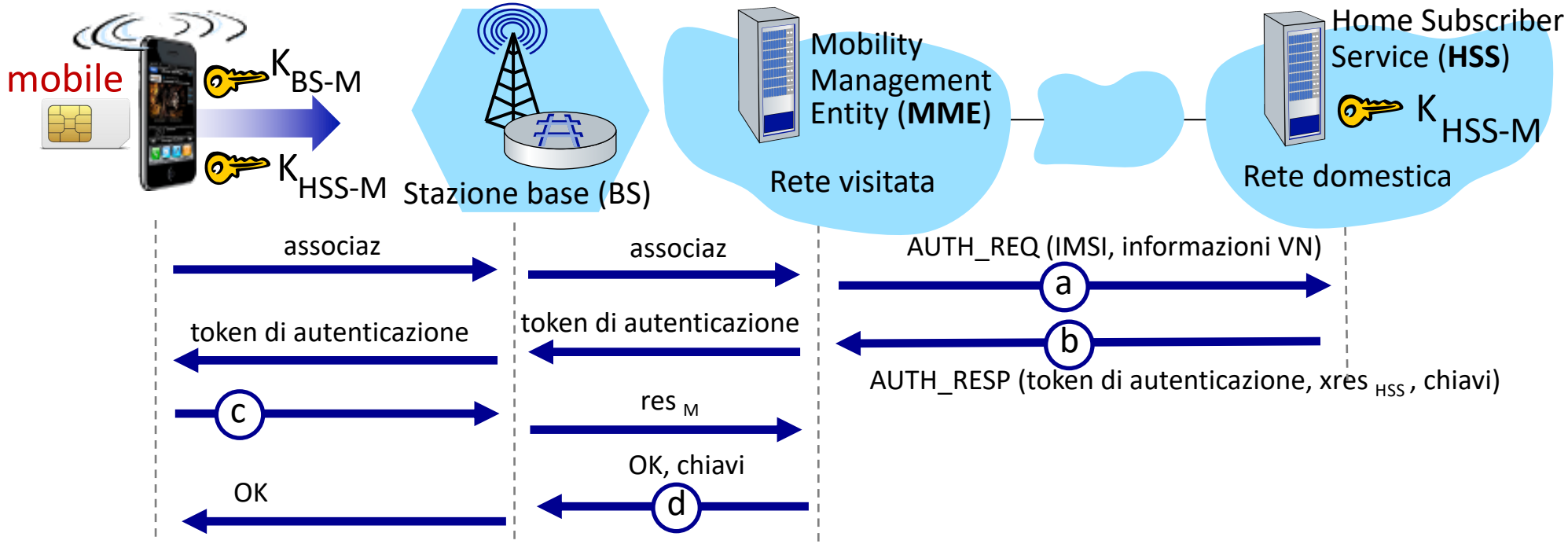
Autenticazione, crittografia in 4G LTE



c) risposta di autenticazione da cellulare:

- mobile calcola res_M utilizzando la sua chiave segreta per eseguire lo stesso calcolo crittografico che HSS ha effettuato per calcolare $xres_{HSS}$ e invia res_M a MME

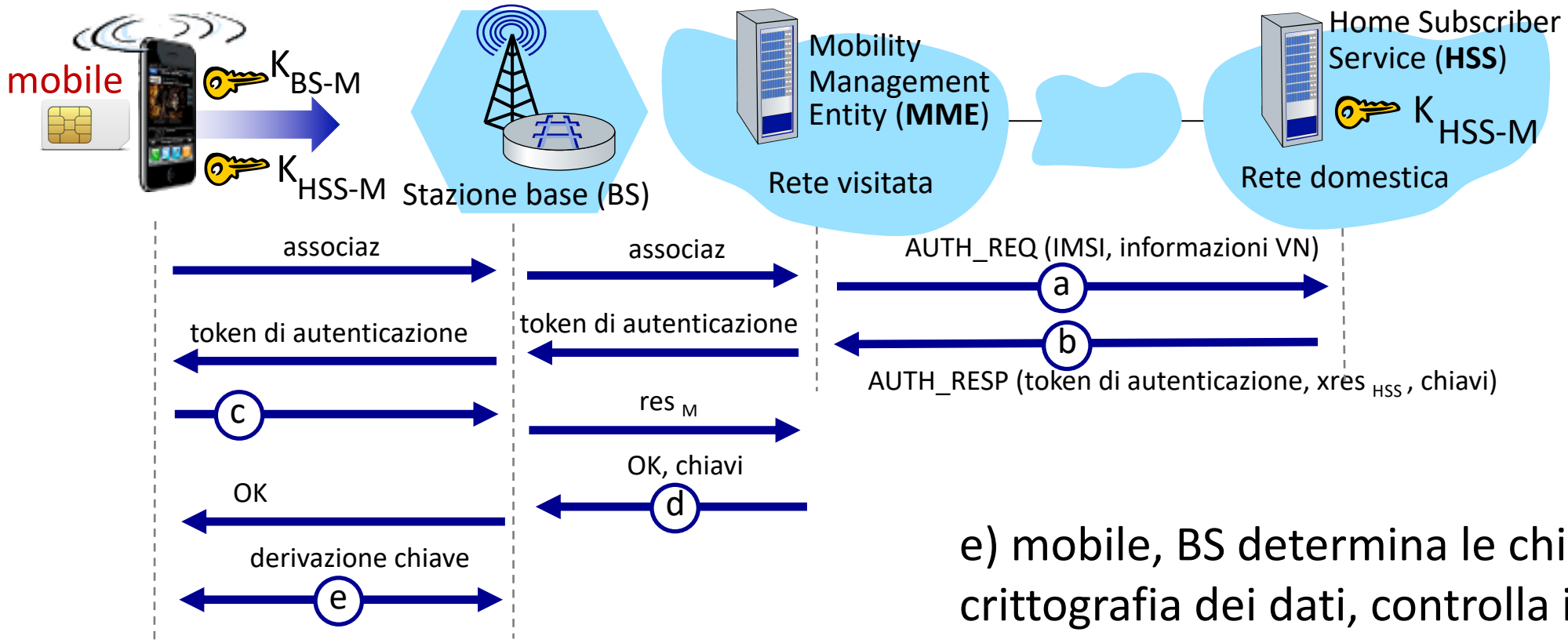
Autenticazione, crittografia in 4G LTE



d) il cellulare è autenticato dalla rete:

- MMS confronta il valore calcolato su dispositivi mobili di res_M con il valore calcolato da HSS di $xres_{HSS}$. Se corrispondono, il cellulare è autenticato!
- MMS informa BS che il cellulare è autenticato, genera chiavi per BS

Autenticazione, crittografia in 4G LTE



e) mobile, BS determina le chiavi per la crittografia dei dati, controlla i frame sul canale wireless 4G

- È possibile utilizzare AES

Autenticazione, crittografia: dal 4G al 5G

- 4G: MME nella rete visitata prende la decisione di autenticazione
- 5G: la rete domestica prende la decisione di autenticazione
  - MME visitato svolge il ruolo di "intermediario" ma può ancora rifiutare

- 4G: utilizza chiavi condivise in anticipo
- 5G: chiavi non condivise in anticipo per IoT

- 4G: dispositivo IMSI trasmesso in chiaro a BS
- 5G: crittografia a chiave pubblica utilizzata per crittografare IMSI

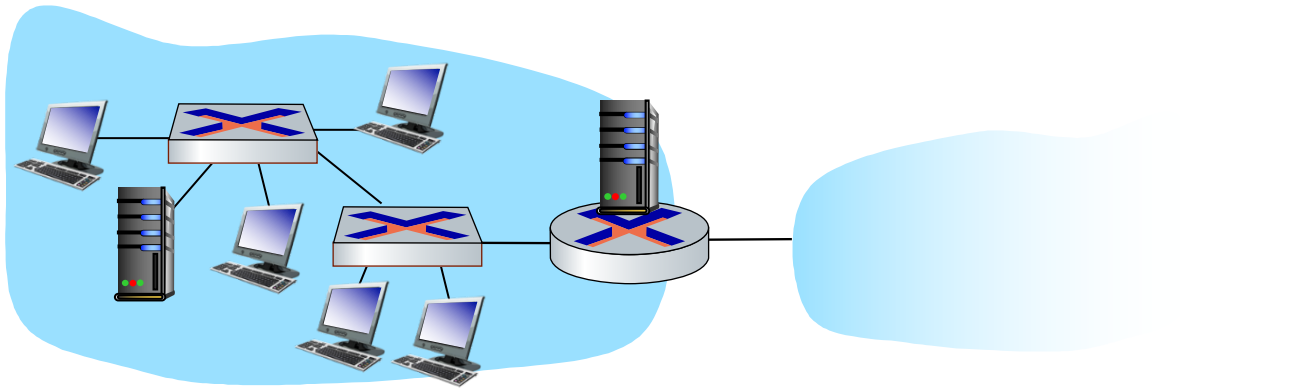
Outline

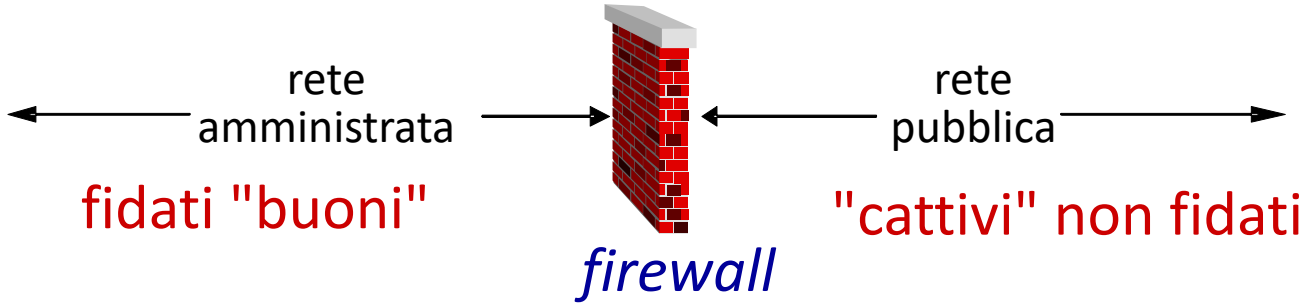
- Che cos'è la sicurezza della rete?
- Principi di crittografia
- Autenticazione, integrità del messaggio
- Protezione della posta elettronica
- Protezione delle connessioni TCP: TLS
- Sicurezza a livello di rete: IPsec
- Sicurezza nelle reti wireless e mobili
- Sicurezza operativa: firewall e IDS

Firewall

firewall

isola la rete interna dell'organizzazione dal resto di Internet, consentendo il passaggio di alcuni pacchetti e bloccandone altri





Firewall: perché

prevenire attacchi denial of service:

- SYN flooding: l'attaccante stabilisce molte connessioni TCP fasulle, nessuna risorsa rimasta per connessioni "reali".

impedire la modifica/l'accesso illegale ai dati interni

- ad esempio, l'attaccante sostituisce la home page della banca con qualcos'altro

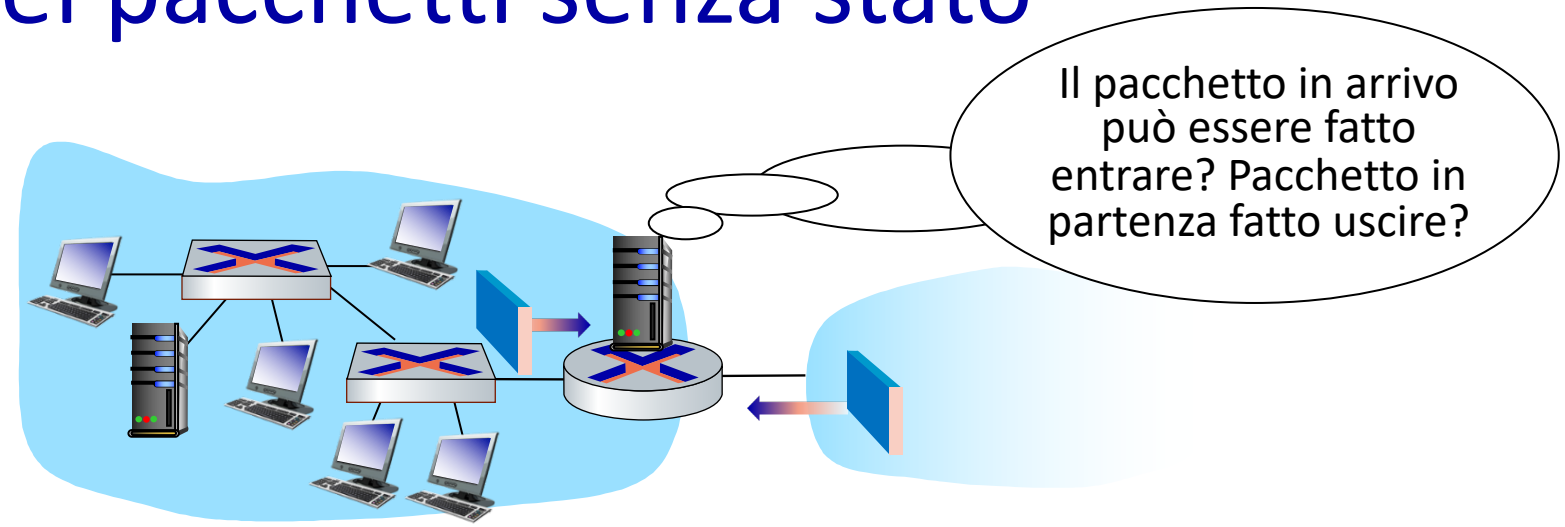
consentire solo l'accesso autorizzato alla rete interna

- set di utenti/host autenticati

tre tipi di firewall:

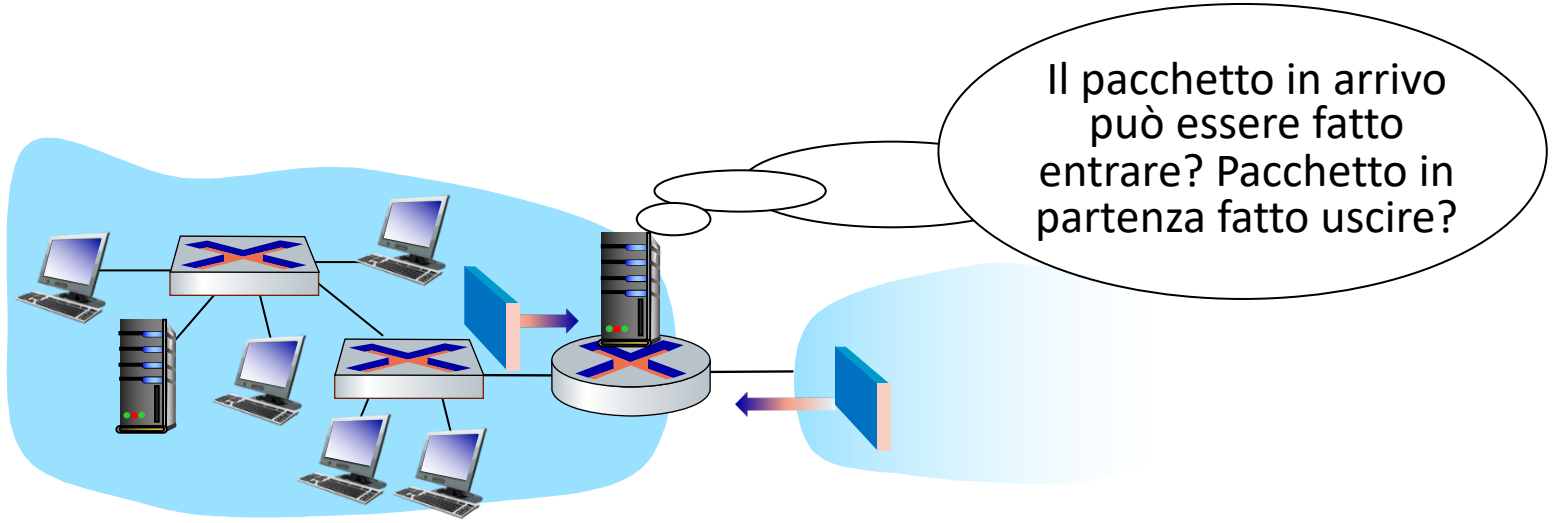
- filtri di pacchetti senza stato
- filtri di pacchetti con stato
- gateway applicativi

Filtraggio dei pacchetti senza stato



- rete interna connessa a Internet tramite router firewall
- filtra pacchetto per pacchetto , decisione di inoltrare/eliminare il pacchetto in base a:
  - indirizzo IP di origine, indirizzo IP di destinazione
  - Sorgente TCP/UDP, numeri di porta di destinazione
  - Tipo di messaggio ICMP
  - TCP SYN, ACK bit

Filtraggio dei pacchetti stateless: esempio



- esempio 1: bloccare i datagrammi in entrata e in uscita con il campo del protocollo IP = 17 e con la porta di origine o di destinazione = 23
  - risultato: tutti i flussi UDP in entrata e in uscita e le connessioni telnet vengono bloccati
- esempio 2: bloccare i segmenti TCP in entrata con ACK=0
  - risultato: impedisce ai client esterni di stabilire connessioni TCP con i client interni, ma consente ai client interni di connettersi all'esterno

Filtraggio dei pacchetti stateless: altri esempi

Politica	Impostazione firewall
nessun accesso Web esterno	blocca tutti i pacchetti in uscita a qualsiasi indirizzo IP, porta 80
nessuna connessione TCP in entrata, ad eccezione di quelle solo per il server Web pubblico dell'istituto.	blocca tutti i pacchetti TCP SYN in entrata su qualsiasi IP tranne 130.207.244.203, porta 80
impedire alle web-radio di consumare la larghezza di banda disponibile.	elimina tutti i pacchetti UDP in entrata, ad eccezione delle trasmissioni DNS e del router
impedisci che la tua rete venga utilizzata per un attacco smurf DoS.	eliminare tutti i pacchetti ICMP diretti a un indirizzo "broadcast" (ad es. 130.207.255.255)
impedire che la tua rete venga tracciata con traceroute	eliminare tutto il traffico ICMP TTL scaduto in uscita

Access Control List

ACL: tabella di regole, applicata dall'alto verso il basso ai pacchetti in arrivo: coppie (azione, condizione): simile a inoltro OpenFlow!

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

Filtraggio dei pacchetti con stato

- *filtraggio senza stato:* strumento rozzo
  - ammette pacchetti che "non hanno senso", ad esempio, porta dest = 80, bit ACK impostato, anche se non è stata stabilita alcuna connessione TCP:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *filtraggio stateful:* monitorare lo stato di ogni connessione TCP
  - track connection setup (SYN), teardown (FIN): determinare se i pacchetti in entrata e in uscita "hanno senso" (fanno parte di una connessione)
  - timeout per connessioni inattive al firewall: non ammette più pacchetti per connessioni scadute

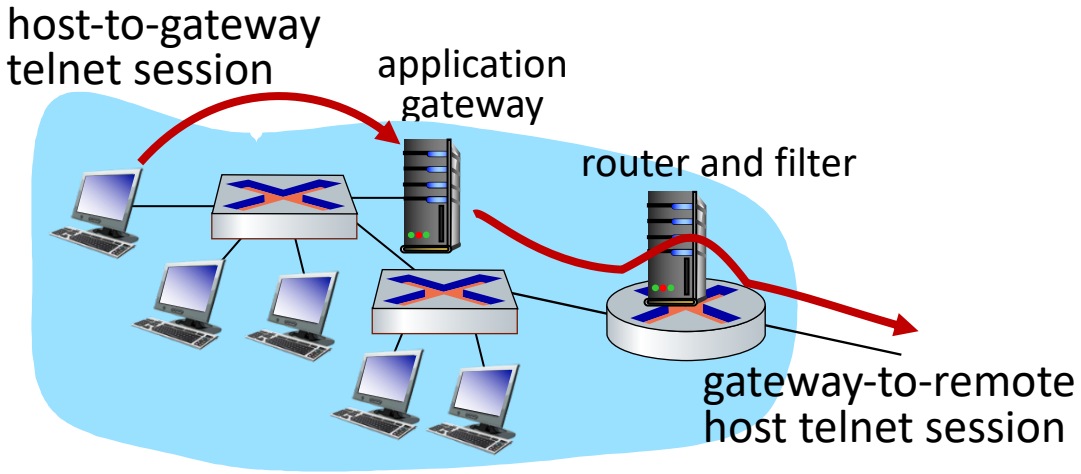
Filtraggio dei pacchetti con stato

ACL aumentato per indicare la necessità di controllare la tabella dello stato della connessione prima di ammettere il pacchetto

action	source address	dest address	proto	source port	dest port	flag bit	check connection
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	

Gateway applicativi

- filtra i pacchetti sui dati del livello applicazione e sui campi IP/TCP/UDP
- *esempio:* consenti a utenti interni selezionati di usare telnet verso l'esterno



1. richiedere a tutti gli utenti telnet di fare richieste tramite gateway
2. per gli utenti autorizzati, il gateway imposta la connessione telnet all'host di destinazione
   - il gateway inoltra i dati
3. il filtro del router blocca tutte le connessioni telnet che non provengono dal gateway

Limitazioni di firewall, gateway

- IP spoofing: il router non può sapere se i dati provengono “davvero” da una fonte dichiarata
- se più app necessitano di un trattamento speciale, ognuna ha bisogno del proprio application gateway (lento da implementare)
- il software client deve sapere come contattare il gateway
  - ad esempio, è necessario impostare l'indirizzo IP del proxy nel browser web

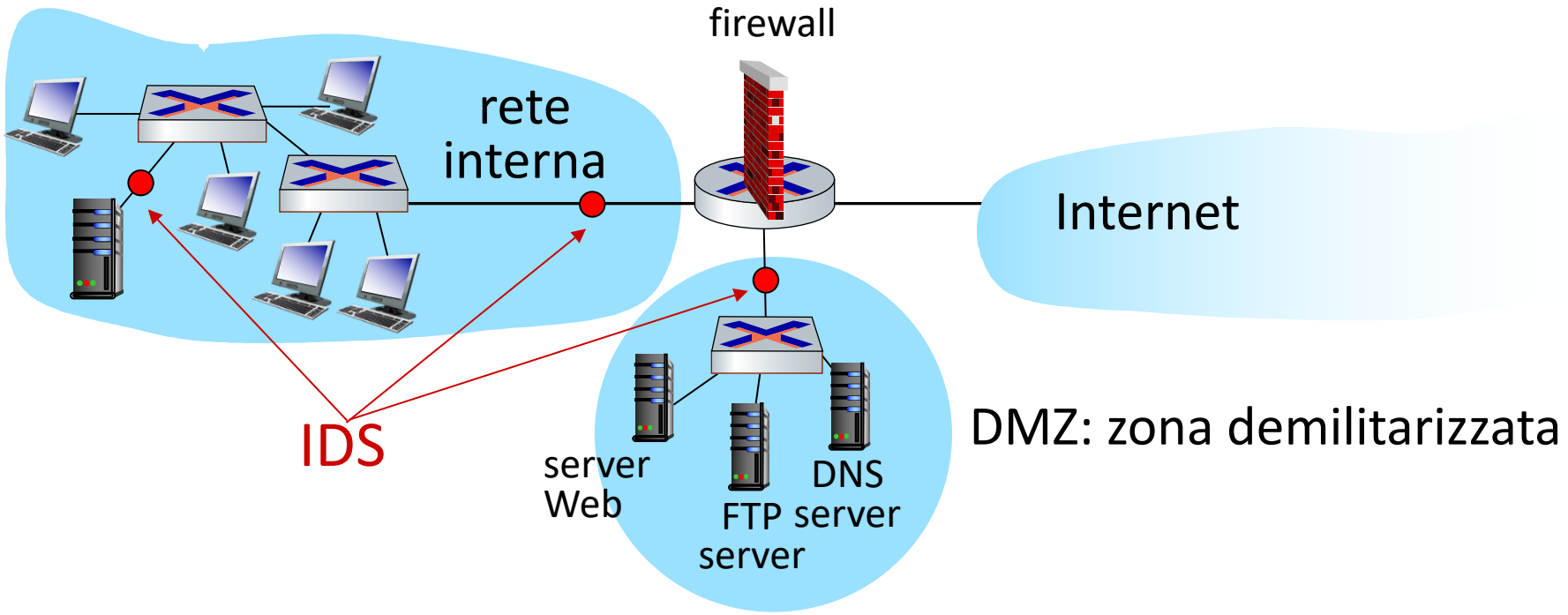
- i filtri usano spesso la politica tutto o niente per UDP
- *compromesso:* grado di comunicazione con il mondo esterno e livello di sicurezza
- molti siti altamente protetti subiscono ancora attacchi

Sistemi antintrusione

- filtraggio dei pacchetti che abbiamo visto finora:
  - funziona solo su intestazioni TCP/IP
  - nessun controllo di correlazione tra le sessioni
- IDS: sistema di rilevamento delle intrusioni
  - ispezione approfondita dei pacchetti: esaminare il contenuto dei pacchetti (ad esempio, controllare le stringhe di caratteri nel pacchetto rispetto al database di virus noti, stringhe di attacco e.g. SQL inject)
  - esaminare la correlazione tra più pacchetti
    - scansione delle porte (più pacchetti che insieme indicano questo comportamento)
    - mappatura della rete (tracerout analizzando i TTL)
    - Attacco DOS (traffico inusuale verso un IP interno)

Sistemi antintrusione (Intrusion Detection Systems)

più IDS: diversi tipi di controllo in punti diversi



Sicurezza di rete (riepilogo)

tecniche di base……

- crittografia (simmetrica e chiave pubblica)
- integrità del messaggio
- autenticazione end-point

…. utilizzato in molti diversi scenari di sicurezza

- e-mail sicura
- trasporto sicuro (TLS)
- IP sec
- 802.11, 4G/5G

sicurezza operativa: firewall e IDS