

Wireless (802.11)

e relative problematiche di security.

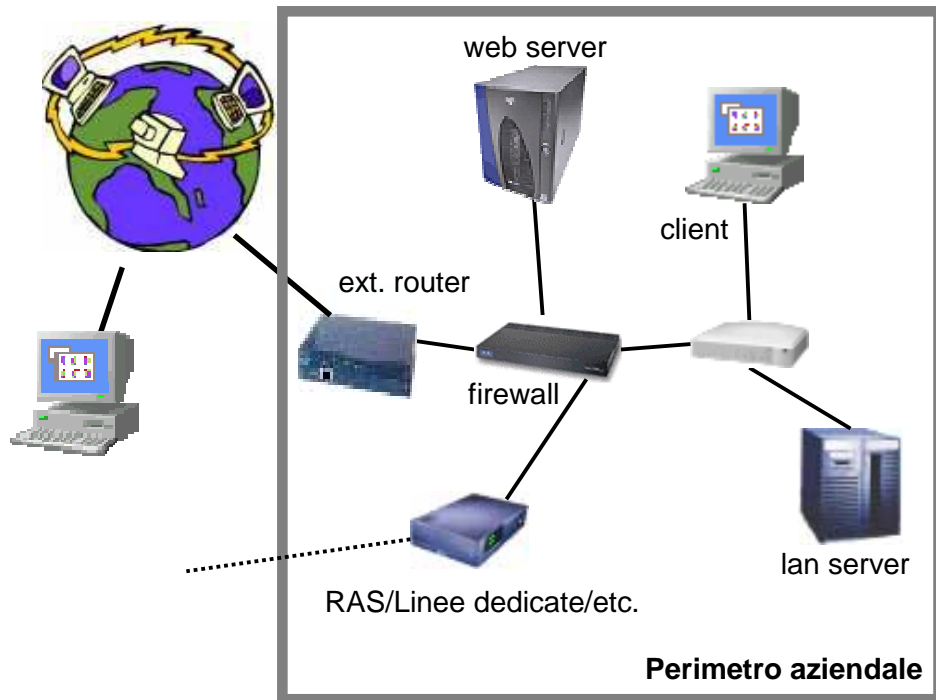


<http://www.infosec.it>

info@infosec.it

relatore: Igor Falcomatà

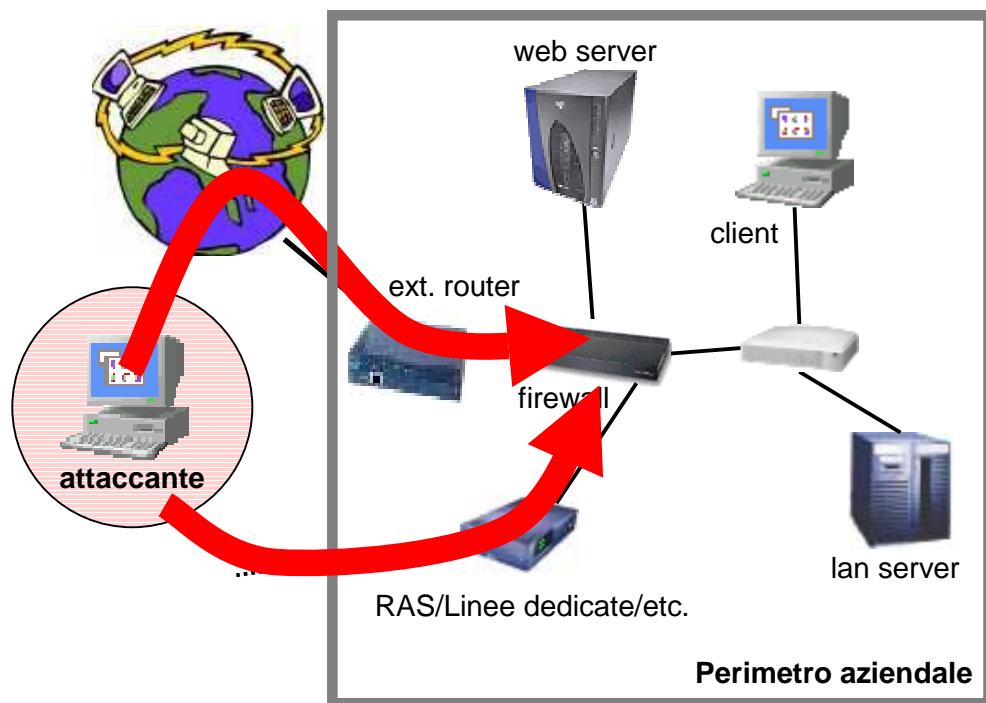
Rete "wired"



Esempio di rete aziendale "classica":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- RAS, Linee dedicate, VPN

Rete "wired"

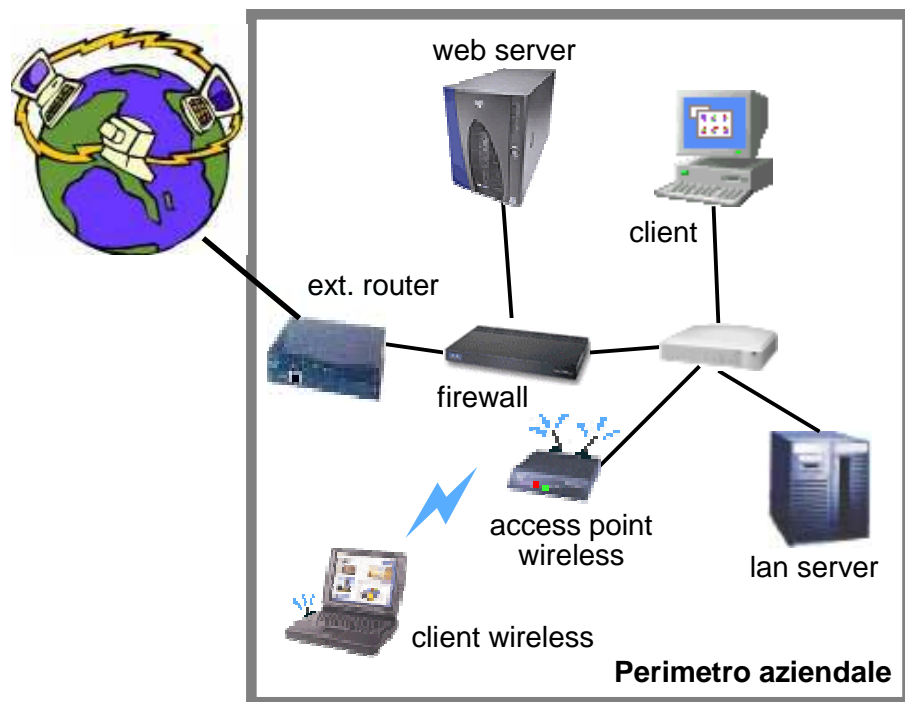


Esempio di rete aziendale "classica":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- RAS, Linee dedicate, VPN

Attacchi provenienti da Internet o tramite RAS/Linee dedicate, etc.

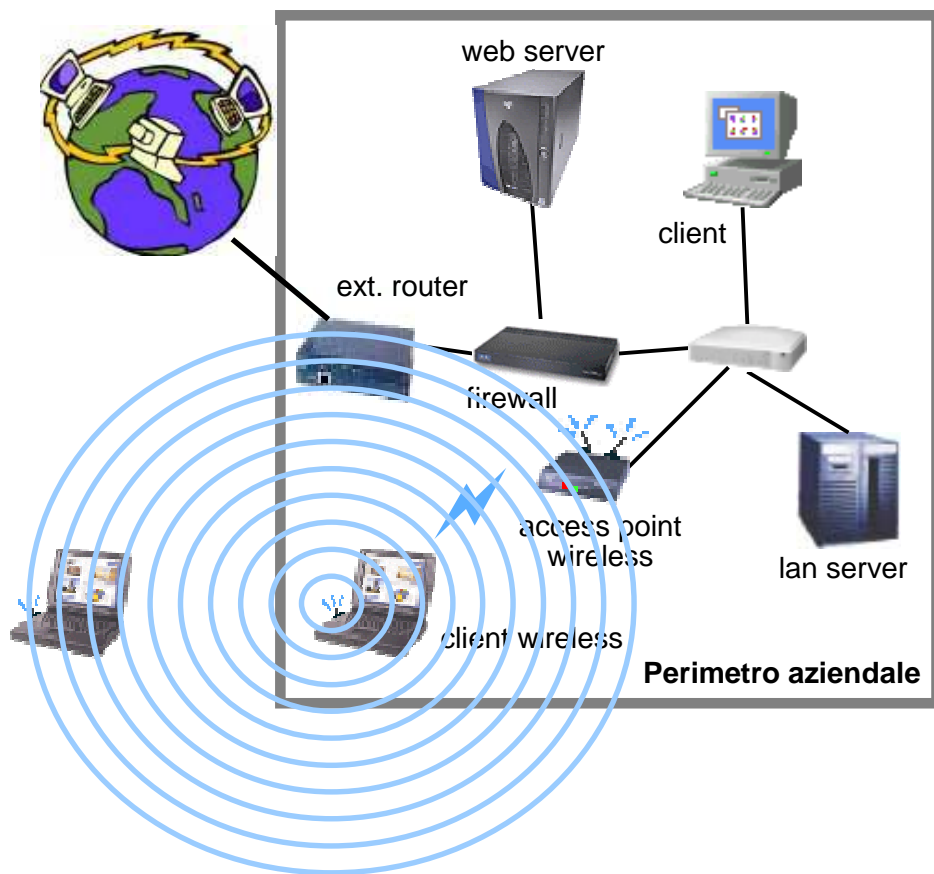
Rete "wireless"



Esempio di rete aziendale "wireless":

- rete privata (LAN)
- connessione ad Internet
- zona smilitarizzata (DMZ)
- access point wireless
- utenti wireless

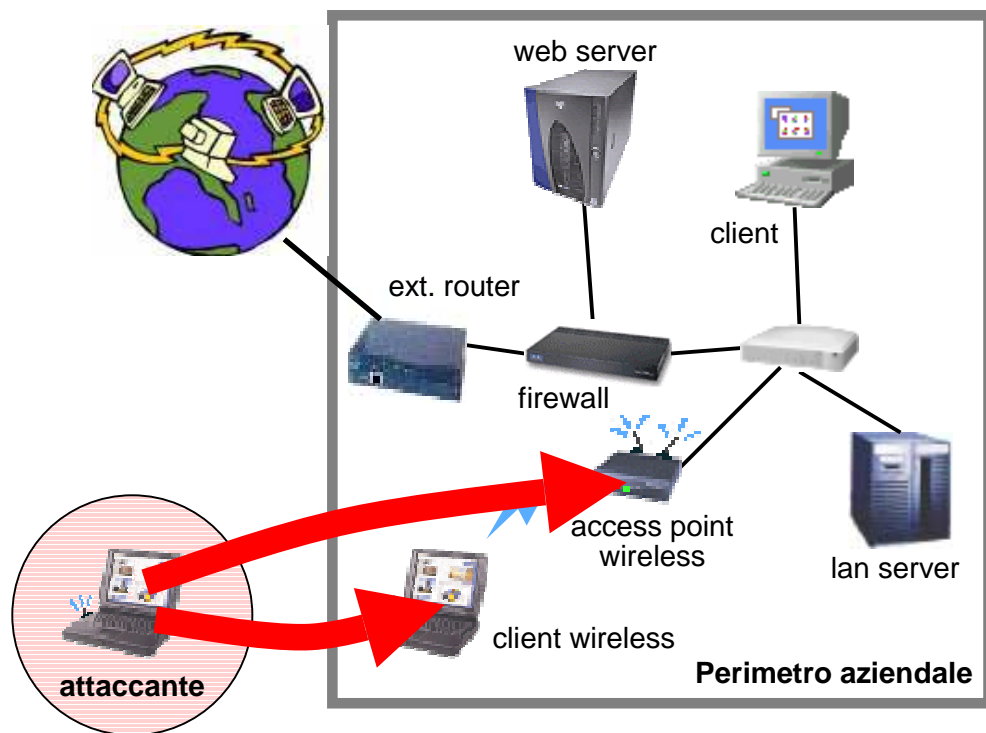
Rete "wireless"



Esempio di rete aziendale "wireless":

- i dati viaggiano nell'etere
- gli utenti si associano con gli "Access Point"
- per utilizzare il computer senza cavi in qualsiasi parte dell'azienda...
- ...o all'esterno dell'azienda

Rete "wireless"

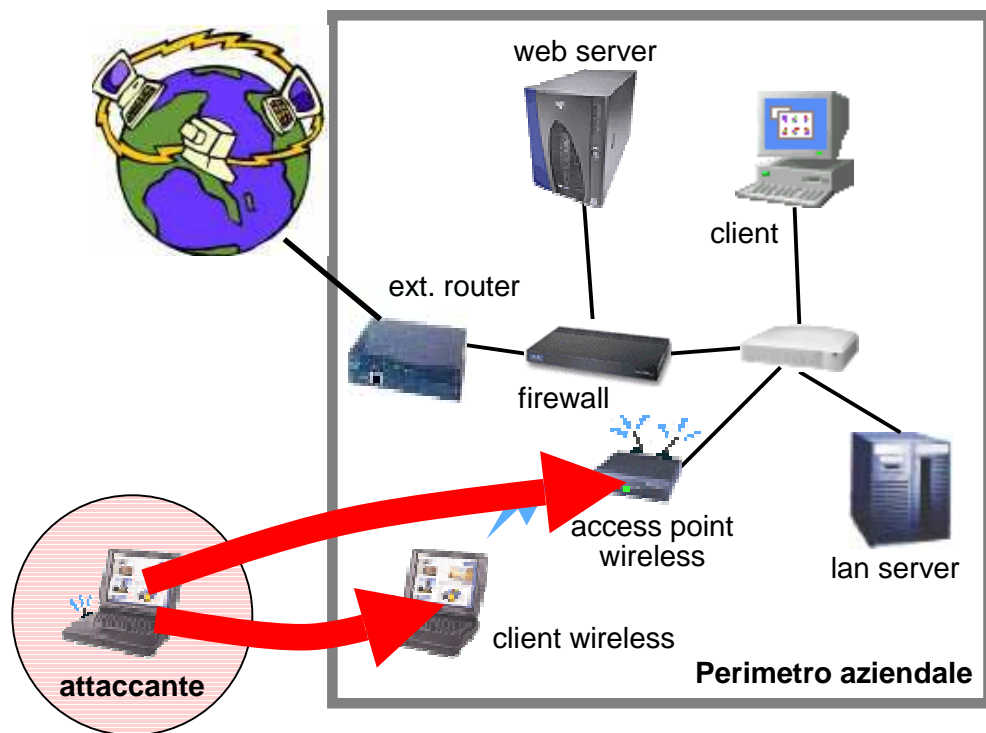


Esempio di rete aziendale "wireless":

- i dati viaggiano nell'etere
- gli utenti si associano con gli "Access Point"
- per utilizzare il computer senza cavi in qualsiasi parte dell'azienda...
- ...o all'esterno dell'azienda

Attacchi provenienti "dall'etere", per es. da un hacker posizionato all'esterno del perimetro aziendale.

Rete "wireless"

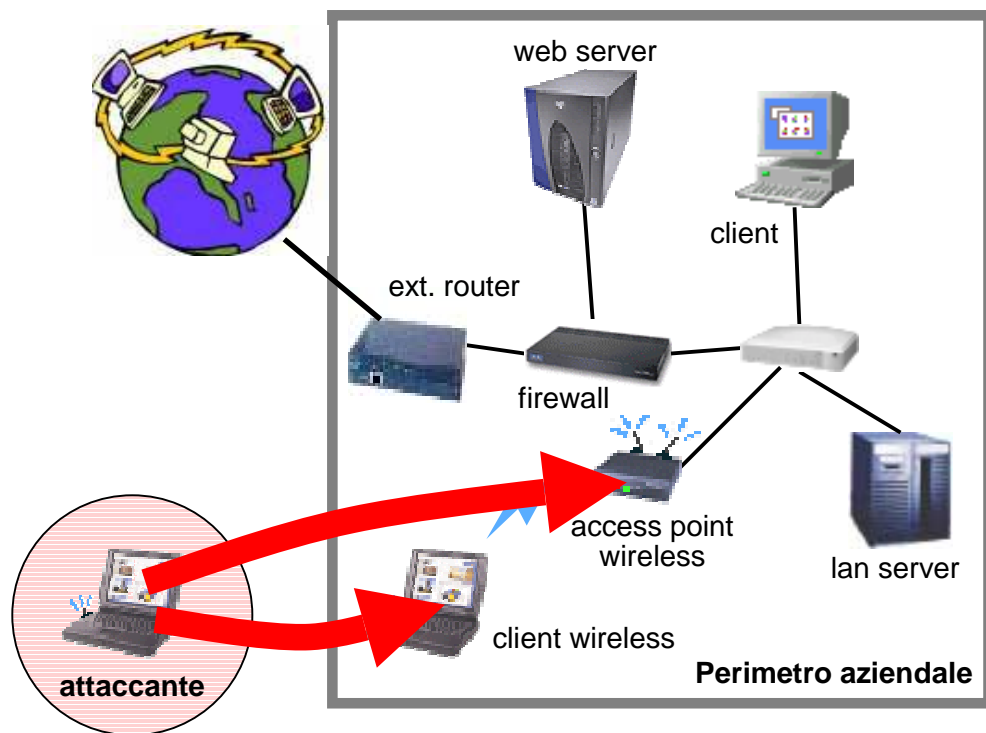


Perché insicure?

- dati non limitati al perimetro fisico (aria, finestre, muri, ...)
- dati viaggiano in chiaro
- associazione con AP senza autenticazione
- AP posizionati direttamente sulla LAN
- DoS

Nessuna misura di sicurezza...

Dati non limitati al perimetro fisico



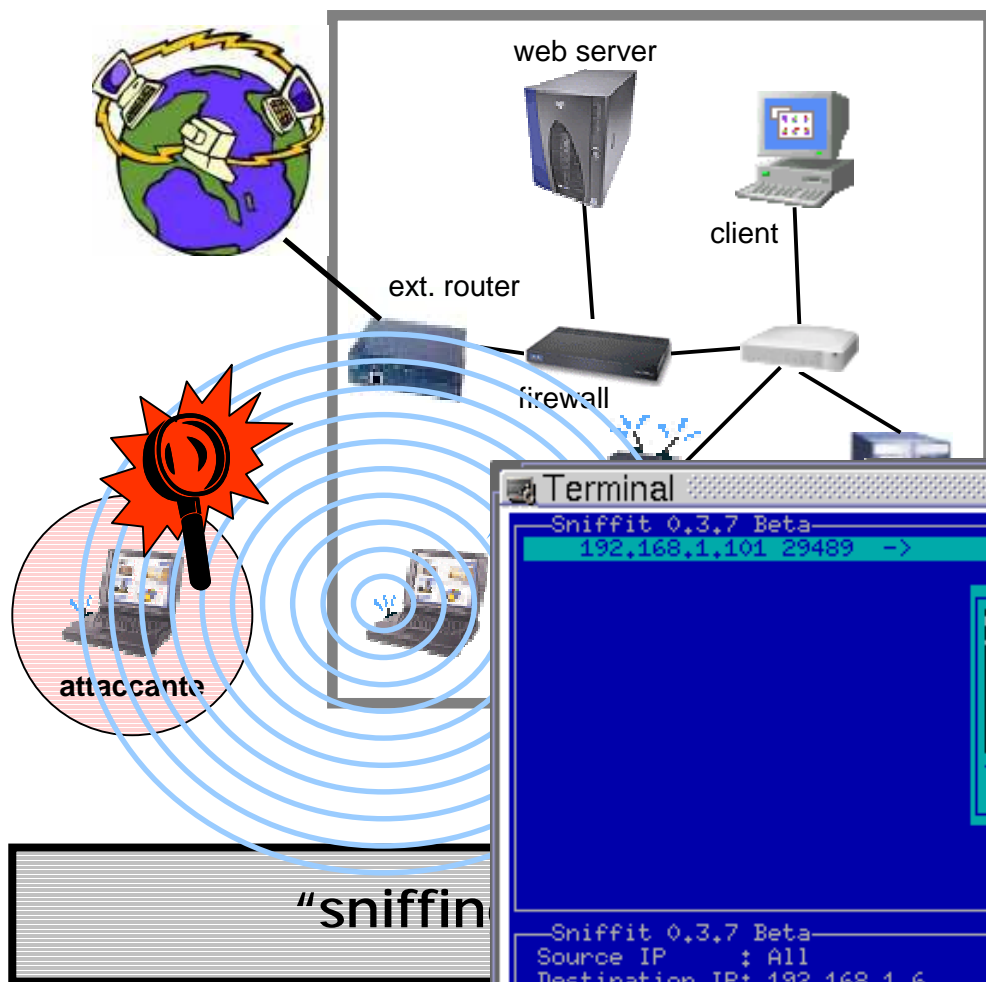
- per le loro caratteristiche, le onde radio attraversano muri, pareti, spazi aperti, vetri, etc.
- un attaccante che possa posizionarsi in un range fino a 30-50 metri da un AP può effettuare un apparecchiature standard
- con un antenna dedicata, il range aumenta

"Parking lot attack"

Dati viaggiano in chiaro



Dati viaggiano in chiaro



- se il traffico in transito non è cifrato, è possibile analizzarlo, in modalità "passiva" (semplicemente analizzando i pacchetti ricevuti senza inviarne)

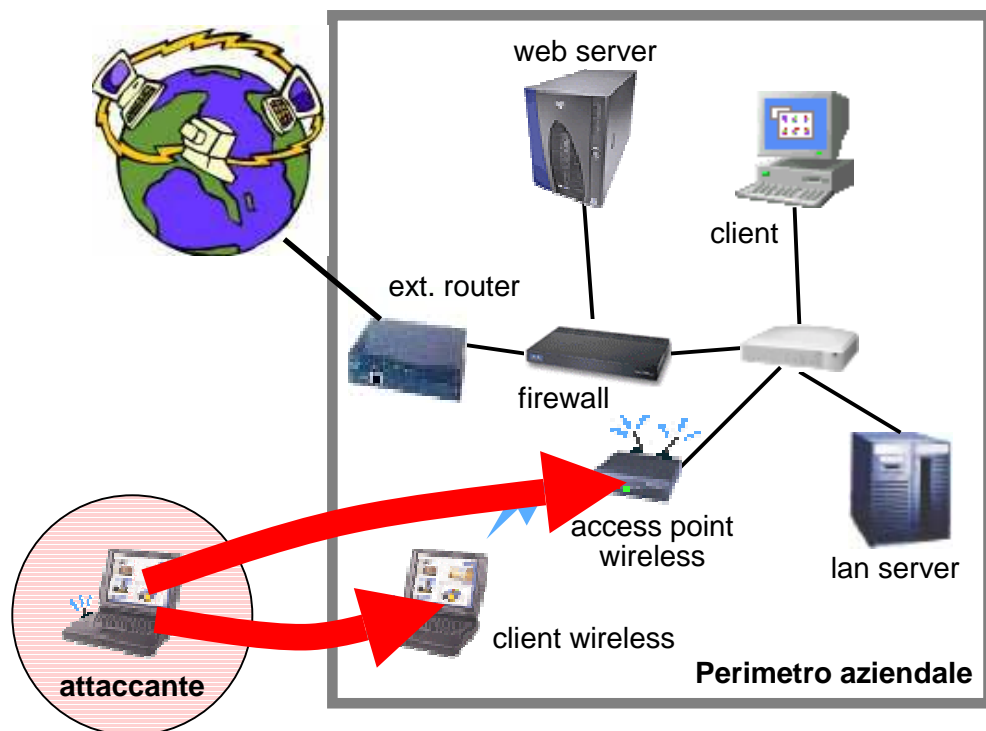
```
Terminal
Sniffit 0.3.7 Beta
192.168.1.101 29489 -> 192.168.1.6 23 [LOGGED]

utente,segreto,su -,supersegreto,passwd root,nuovapass,nuovapass,[]

192.168.1.101 29489 -> 192.168.1.6 23

Sniffit 0.3.7 Beta
Source IP : All Source PORT : All
Destination IP: 192.168.1.6 Destination PORT: 23
Masks: F1-Source IP F2-Dest. IP F3-Source Port F4-Dest. Port
```

Open System Authentication



"infrastructure"

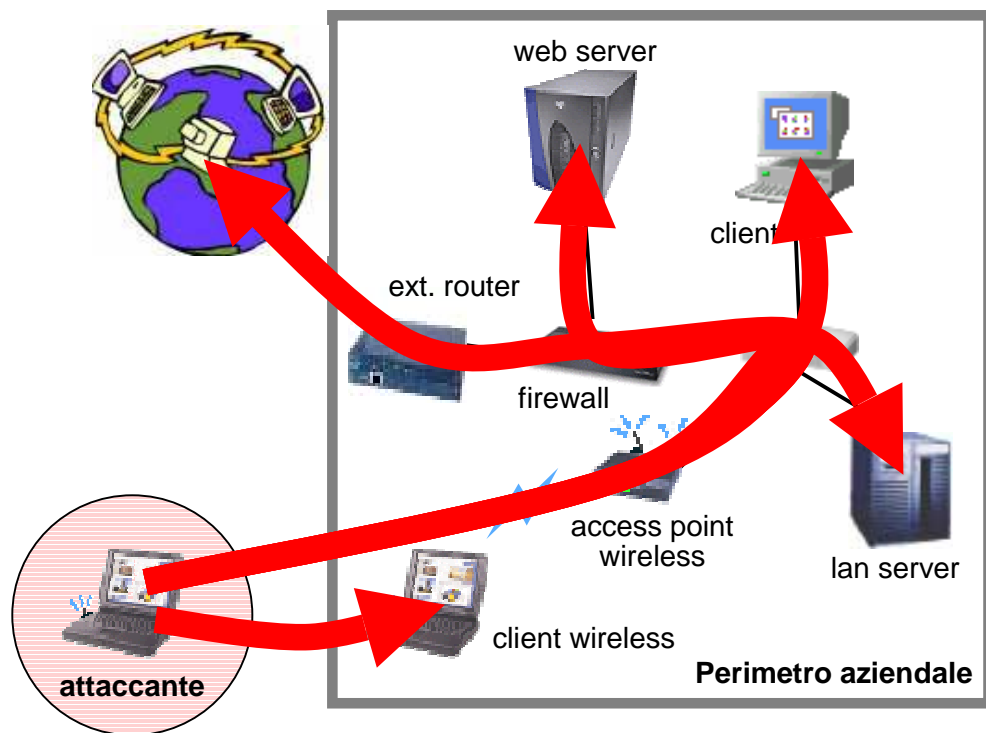
- raggiungere l'Access Point per entrare in rete
- simulare un AP e accettare connessioni dalle stazioni wireless

"ad hoc"

- attaccare direttamente altre stazioni

"NULL Authentication"

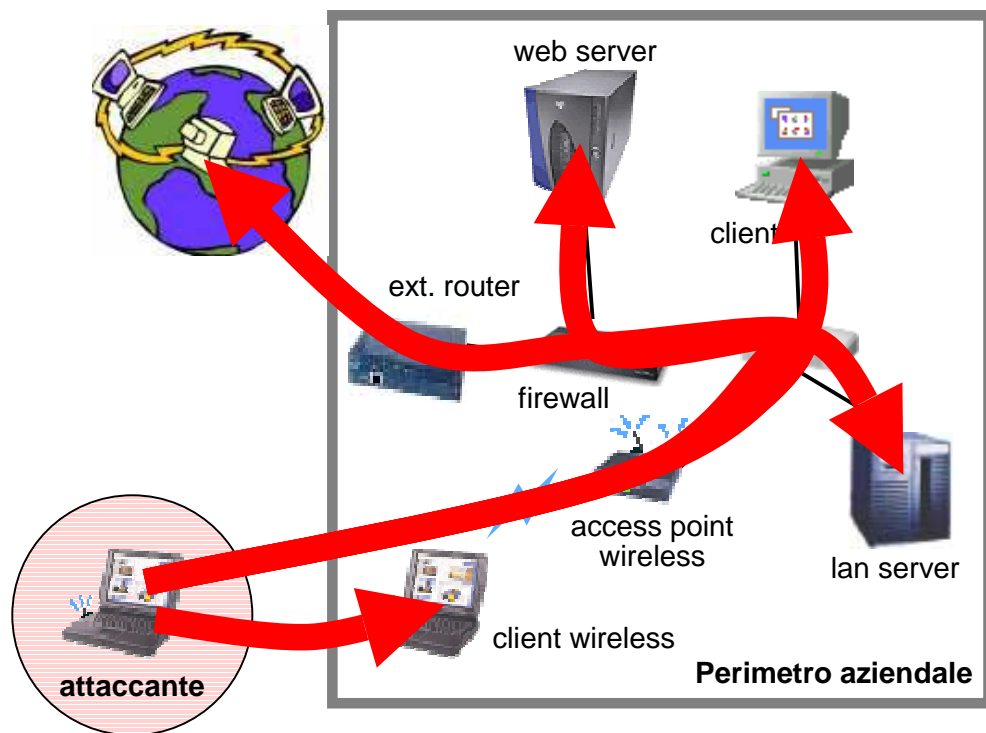
AP posizionati sulla rete interna



- attacco diretto ai server della rete interna
- attacco diretto alle stazioni sulla LAN
- attacco alle DMZ o altre stazioni da posizione privilegiata
- accesso ad Internet (attacco ad altri server, nascondendo la propria identità)

Le stesse possibilità di accesso di una stazione sulla LAN

Rete "wireless"

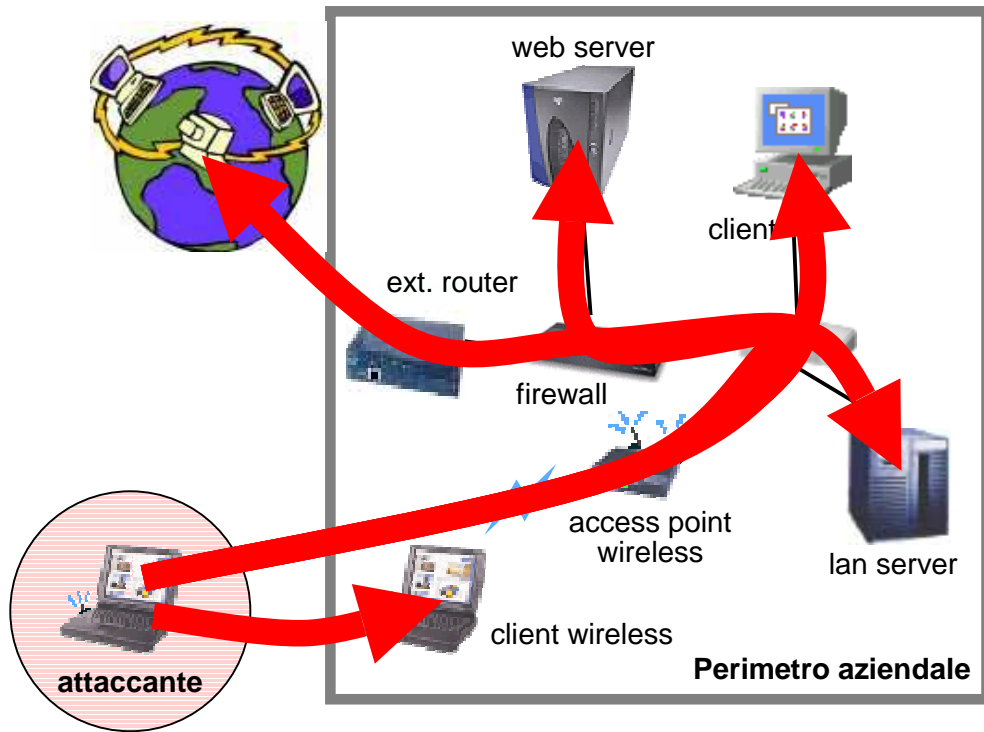


Perché insicure?

- conoscenza SSID
- filtro su MAC
- Wired Equivalency Privacy (WEP)
- Shared Key Authentication
- Varie estensioni proprietarie

Cattive misure di sicurezza...

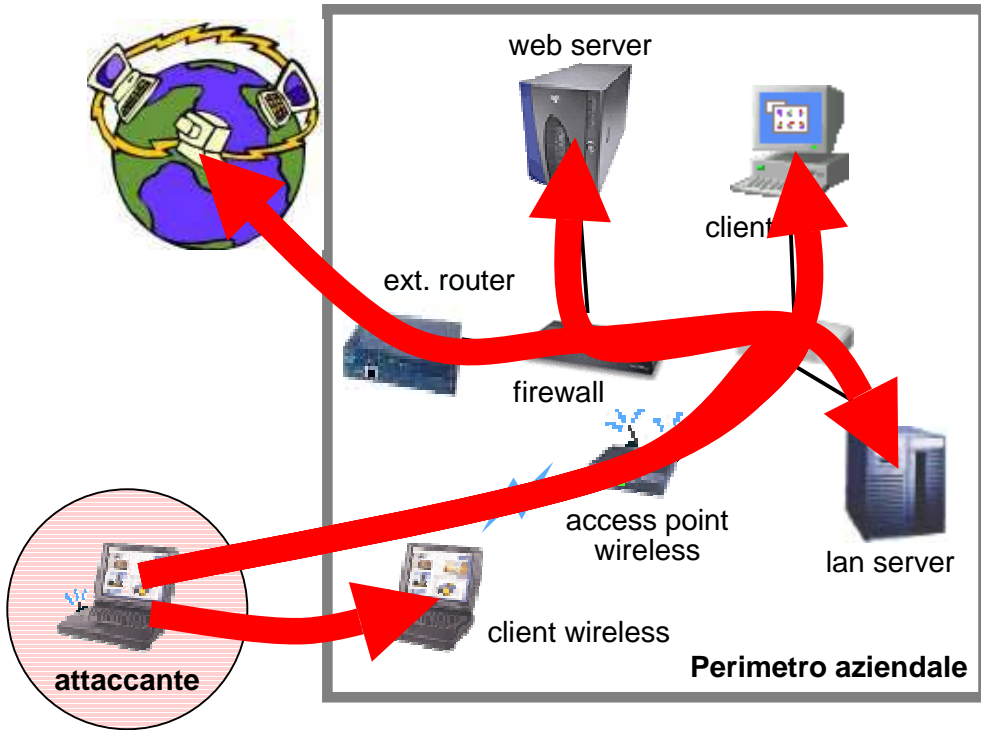
Conoscenza SSID



- per associarsi ad un AP è spesso sufficiente conoscere il SSID della rete
- SSID pre-impostati di default e non modificati
- il SSID viene inviato direttamente da molti AP nei "beacon" frame
- SSID trasmesso nei frame
- "probe" frame per verificare a quale AP corrisponda un SSID

SSID: service set identifier

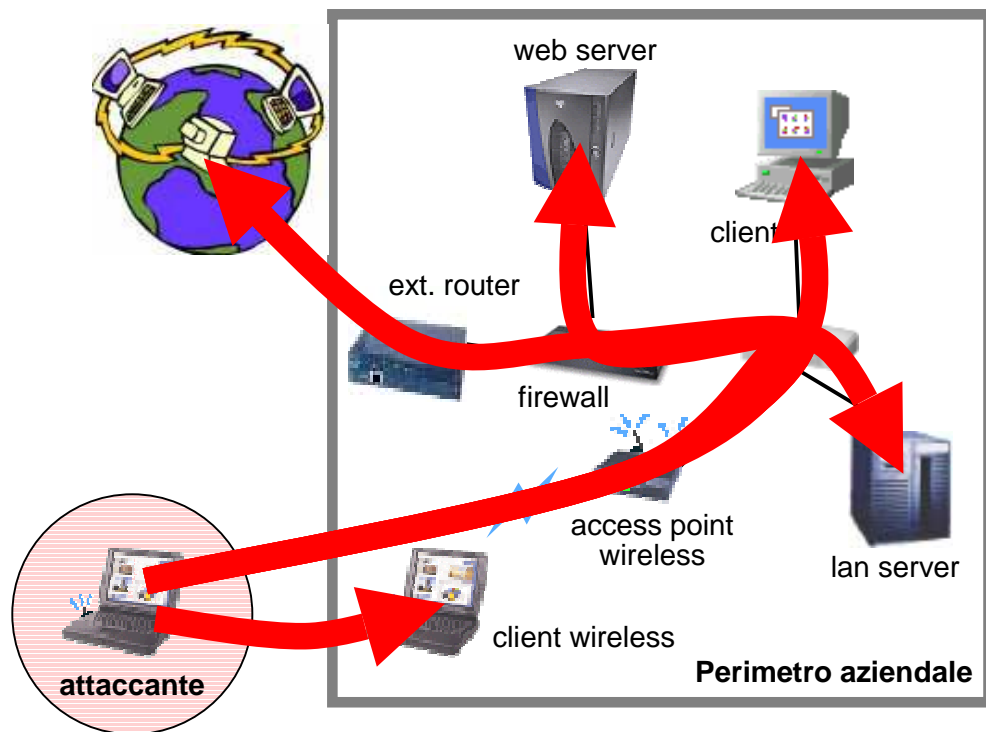
Filtro su MAC Address



- difficoltà di management per reti grandi
- MAC Address trasmesso nei frame dalle altre schede
- possibilità di cambiare con facilità il MAC Address della scheda

MAC: indirizzo hardware della eth

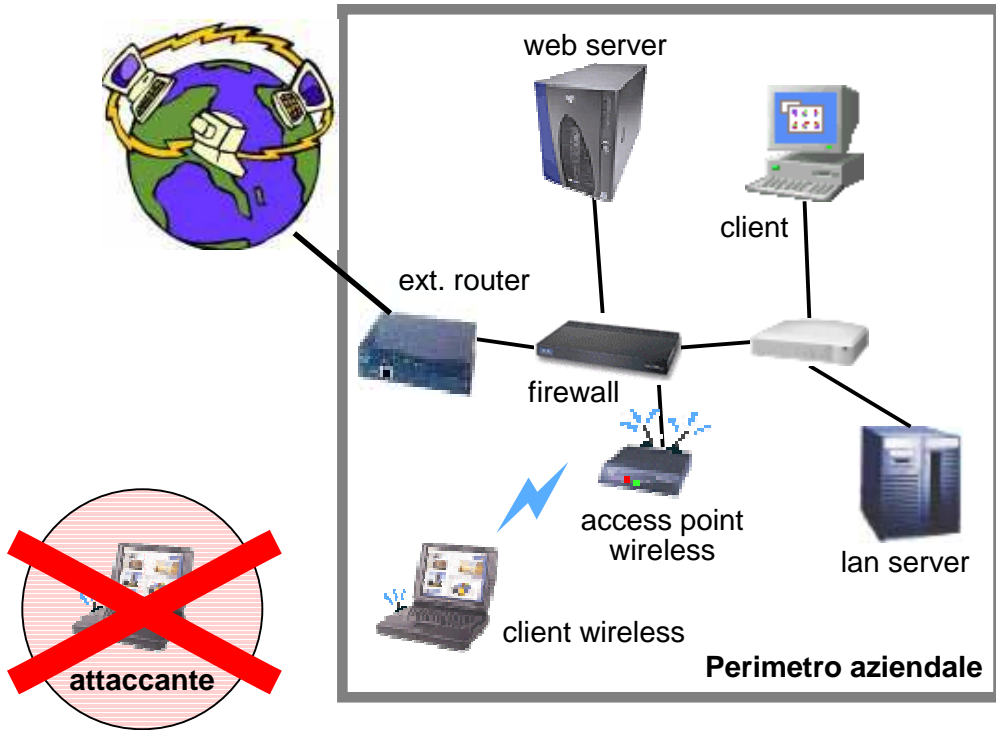
Wired Equivalency Privacy



- protocollo crittografico studiato per garantire la confidenzialità del traffico wireless da "sniffing" (Layer 2)
- chiave/i condivisa/e tra AP e client
- "Analysis of 802.11 Security or Wired Equivalency Privacy Isn't"
Nikita Borisov, Ian Goldberg, David Wagner:
- possibilità di scoprire le chiavi analizzando quantità sufficiente di traffico

cattiva implementazione di un buon algoritmo crittografico

Sicurezza nelle reti wireless



- WEP 128bit con chiavi diverse per ogni client, e rigenerazione delle chiavi frequente ed automatica
- partizionamento della rete wireless dalla LAN (FW)
- IPSec/VPN
- Corretta configurazione Access Point
- Corretta configurazione stazioni wireless

verifica delle vulnerabilità
Infosec Net Probing wireless

Is Your Business Wireless eXposed?



<http://www.infosec.it>

info@infosec.it

Possiamo aiutarvi!