FIREWALL

Separa la LAN aziendale dalla WAN filtrando i pacchetti con delle regole (policy)
La sicurezza di tutta la rete connessa ad Internet viene ricondotta alla sicurezza di un ristrettissimo numero di nodi, molto spesso solamente 1.

- Può essere realizzato con un PC (2 schede di rete in/out + software apposito)
- Nelle reti aziendali può essere incluso nel router o su hardware dedicato

Caratteristiche:

- Strumento efficace per la sicurezza delle reti
- Presenza di meccanismi per il controllo degli accessi
- Possibilità di gestire le regole per la sicurezza
- Configurazione di filtri per l'accesso dei computer di una rete ad Internet
- Protezione da attacchi (ARP spoofing, port scanning, DoS, SQL slammer)

Si possono distinguere in **3 categorie in base al livello TCP/IP** in cui operano:

- **Application Level Firewall**
- **Packet Filter Firewall**
- **Stateful Packet Inspection Firewall**

Application Level Firewall (+ protezione, - prestazioni)

- Intercetta le trasmissioni a livello Application (contenuto del pacchetto)
- Es. blocca i virus noti in una sessione HTTP o SMTP
- A questa categoria appartengono i **proxy** (che fa da tramite tra LAN e WAN)

Packet Filter Firewall (- protezione, + prestazioni)

- Intercetta le trasmissioni a livello Network (header del pacchetto)
- Es. una mail contenente virus può passare se è abilitato il traffico POP/SMTP
- I parametri che controlla sono:
  - IP di origine e di destinazione
  - Numero della porta TCP/UDP di origine e di destinazione)
  - Il protocollo di livello superiore usato

Stateful Packet Inspection Firewall (- protezione, + prestazioni)

- Intercetta le trasmissioni a livello Transport (analizza header e contenuto)
- Può controllare lo stato della connessione TCP e compilare le informazioni

ACL (Access Control List)

Le ACL permettono di esprimere delle **regole** che determinano o meno l'accesso ad alcune risorse, vengono modificate da parte dell'amministratore

- **white list** → indirizzi verso cui è consentito il transito dei dati (blocco altri)
- **black list** → indirizzi verso cui è bloccato il transito dei dati (consentito altri)

Le ragioni per adoperare le ACL sono:

- Fornire un livello base di sicurezza (restringere gli accessi ad una rete)
- Limitare il traffico
- Aumentare le prestazioni (alcuni pacchetti vengano processati prima di altri)
- Decidere quale tipo di traffico può essere trasmesso

Il router-firewall elabora le ACL in modo sequenziale → le + restrittive vanno prima
Appena un pacchetto soddisfa una delle condizioni la valutazione si interrompe
Il pacchetto viene quindi inoltrato o scartato a seconda dell'istruzione eseguita
Se il pacchetto non soddisfa nessuna condizione viene scartato (l'ultima è "deny all")

Esistono 2 tipologie di ACL:

- **Standard (1-99)**
  - Guardano l'indirizzo della sorgente
  - Vanno collocate vicine alla destinazione
- **Extended (100-199)**
  - Limitazioni ai pacchetti (protocollo, IP sorgente, IP destinazione, porta)

PROXY

è un programma (su computer o su apparato hardware) posto tra client e server

- Spesso lavorano a livello Application
- Il loro compito è garantire connettività e caching ai client (+ prestazioni)

Compiti:

- **Connettività** → permette ad una LAN di accedere ad Internet tramite un pc
- **Privacy** →maschera il vero indirizzo IP
- **Caching** → immagazzina per tot tempo dei dati (non si consulta il server)
- **Monitoraggio** → tiene traccia di tutte le operazioni effettuate (statistiche)
- **Amministrazione** → applica regole sui pacchetti o sulla banda
- **Filtraggio** → svolge le funzioni di firewall a livello Application
- **Restrizioni** → crea una zona neutra DMZ (DeMilitarized Zone)

Si possono individuare **3 categorie di utilizzo**:

- **Single Proxy Topology**
- **Multiple Proxy Vertical Topology**
- **Multiple Proxy Horizontally Topology**

Single Proxy Topology

- Utilizza 1 singolo proxy server per l'intera rete
- Configurazione sufficiente per un piccolo gruppo di client

Multiple Proxy Vertical Topology

- Utilizza più proxy secondary (uno per subnet) dipendenti da un proxy primario
- Reti medio/grandi
- I client possono avere il filtraggio dei pacchetti personalizzato

Multiple Proxy Horizontally Topology

- Utilizza più proxy secondari messi a pari livello
- Consente di bilanciare il carico in base alle richieste dei client
- Necessita di sincronizzazione (SVANTAGGIO)

NAT (Network Address Translation)

Tecnica adottata dal router che sostituisce, nell'intestazione del pacchetto, l'IP
socket = protocollo + indirizzo IP + porta

1. Quando un client richiede una pagina web ad un server esterno il suo IP e la sua porta vengono traslati e la corrispondenza viene registrata nella tabella.
2. Quando arriva la risposta dal server esterno la tabella permette di capire chi è che voleva quei dati → traslazione inversa → dati inviati al client
3. Tutte le comunicazioni provenienti dall'esterno non registrate → eliminate

Vantaggi:

- Limita il numero di IP pubblici necessari per collegare una LAN ad Internet

- Mantiene inalterata la configurazione degli host
- Non modifica il funzionamento dei protocolli e delle applicazioni della rete
- Flessibilità elevata → spazio molto ampio per gli IP privati
- Riduce i costi per l'accesso a Internet (gli IP pubblici sono a pagamento)
- Garantisce maggior sicurezza per i computer della LAN

Ha 3 funzionalità:
- **Static NAT** (usa 1 solo IP pubblico)
- **Dynamic NAT** (una un insieme di IP pubblici)
- **Port Address Translation o PAT** (traduce dinamicamente le porte)

PAT (Port Address Translation)

Consente al router di utilizzare un singolo indirizzo IP per gestire oltre 64000 (2^16) connessioni private contemporaneamente
Può traslare più IP client per lo stesso IP di destinazione cambiando solo la porta
Anche IPv6 implementa il NAT per mettere in comunicazione reti IPv6 con reti IPv4

Per la fase di transizione da IPv4 a IPv6, IETF ha ipotizzato **3 meccanismi:**
- **Dual-stack**
- **Conversion**
- **Tunneling per IPv6**

Dual-stack:
prevede l'utilizzo del doppio stack IP nella pila di protocolli TCP/IP
Questo permette di interpretare entrambe le versioni del protocollo IP e quindi di smistare ai livelli superiori il contenuto del pacchetto senza che questi sappiano da quale protocollo IP derivi.
Vantaggi:
- Semplicità di implementazione

Svantaggi:
- Aumento della complessità della rete (router e switch multiprotocollo)
- Non risolve il problema della scarsità degli indirizzi IP (sia l'IPv4 che l'IPv6)
- Routing più lento (entrambi gli IP devono essere annunciati)

Conversion:
- È considerato il NAT per IPv6
- È realizzato con il protocollo NAT-PT (PT = Protocol Translator)
  effettua la conversione IPv6 in IPv4 e viceversa secondo le tecniche NAT IPv4
- NAT-PT consente la comunicazione diretta tra reti solo IPv6 e reti IPv4

Tunneling: Incapsula un pacchetto IPv6 in un pacchetto IPv4

DMZ (DeMilitarized Zone)

Area in cui sia il traffico WAN sia quello LAN sono fortemente limitati e controllati

Permette ai server di fornire servizi all'esterno senza compromettere la sicurezza interna

- Posta elettronica
- Application Server

In DMZ si installano i server **front-end** a cui corrispondono i relativi **back-end** in LAN, il server front-end comunica con il suo back-end solo con le porte TCP/UDP necessarie. La

DMZ è una sottorete della rete aziendale accessibile ai dipendenti tramite LAN e da utenti esterni tramite Internet.

Una DMZ può essere:

- **Vicolo cieco**
- **Zona cuscinetto**

Vicolo cieco:

Realizzata mediante un firewall con 2 porte, 1 x la LAN e 1 x la DMZ, (+1 x la WAN)

Zona cuscinetto:

- **L'external firewall** separa la rete pubblica dalla DMZ
- **L'internal firewall** separa la DMZ dalla zona LAN vera e propria
- Sicurezza maggiore per i DB presenti in LAN
- Eventuali tentativi di intrusione in LAN devono superare un secondo firewall

VPN (Virtual Private Network)

Una VPN è una rete privata creata all'interno di un'infrastruttura di rete pubblica (Internet) Per un'azienda con diverse sedi dislocate può essere utile trattare tutte come un'unica rete LAN, la VPN permette di effettuare ciò andando a creare una sorta di WAN privata. Inoltre, può essere utile anche per chi lavora in teleworking o smartworking.

Le reti private vere e proprie collegano + sedi con canali dedicati (pagando gestori)

Vantaggi:

- Larghezza di banda sempre disponibile
- Nessun problema di accesso
- Nessuna congestione del traffico
- Prestazioni garantite
- Sicurezza garantita

Svantaggi:

- Alti costi di installazione
- Costi ricorrenti di manutenzione
- Tempi lunghi per la configurazione
- Mancanza di scalabilità
- Rischio di blocco del canale in caso di guasto (non c'è ridondanza)

Dal momento che la VPN viene creata sulla rete pubblica bisogna fare attenzione a:

- Variabilità del tempo di trasmissione (traffico, congestione, latenza)
- Controllo degli accessi (autenticazione)
- Sicurezza delle trasmissioni (cifratura e tunneling)

Tipi di VPN:

- **Remote-access VPN:** emula il desktop del computer dell'ufficio (homeworking)
- **Site-to-site VPN:** amplia le risorse di rete a filiali, uffici domestici e partner

Remote-access VPN:

- Consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale
- Realizzata con un server di accesso alla rete (**NAS**) e un software **VPN Client**
- Utilizzata per aziende con piccoli uffici o per i singoli dipendenti/utenti

Un **NAS** (Network Access Server o Nazz) è un server di accesso alla rete che richiede all'utente di inserire credenziali per connettersi. Può essere un server dedicato o un'applicazione software in esecuzione su un server. Il NAS utilizza il proprio processo di autenticazione o si avvale di un server AAA (Autenticazione/Autorizzazione/Accounting).

Un **VPN client** e un firewall che fornisce da barriera tra la LAN privata e Internet

Site-to-site VPN:

Permette di stabilire connessioni sicure su una rete pubblica ad aziende con tante sedi

Può essere **realizzata come:**

- **Intranet-based:** permette ad una società di unire reti di sede remoti in un'unica rete privata
- **Extranet-based:** per le società con rapporti stretti fra loro, permette di lavorare insieme in ambiente sicuro senza l'accesso preventivo alla propria rete

La sicurezza nelle VPN:

- **Autenticazione**
- **Cifratura**
- **Tunneling**

Autenticazione dell'identità:

Processo con cui un sistema informatico o un utente verifica la corretta identità di un altro sistema informatico che vuole comunicare attraverso una connessione, per poi concedergli l'autorizzazione a usufruire dei relativi servizi associati.

Questa procedura di autenticazione è detta **MultiFactor Authentication (MFA)**, per esempio dopo aver effettuato il login con username e password viene richiesto di immettere un codice generato con una chiave elettronica **(key fob)** che cambia ogni volta.

Al giorno d'oggi si utilizzano:

- **OTP (One-Time Password)**
- **Impronte digitali**
- **QR Code**

I protocolli per la sicurezza nelle VPN garantiscono anche **integrità** e **autenticità** dei dati (i pacchetti ricevuti non sono stati modificati e provengano da fonte certa). Per controllare che non siano state effettuate azioni indesiderate e non autorizzate, occorre prevedere **meccanismi di accounting** (azioni x documentare le risorse concesse a un utente durante un accesso come la durata della sessione di lavoro, il quantitativo dei dati (inviati e ricevuti) in una sessione).

Per cifrare il traffico utilizza diversi algoritmi di crittografia (3-DES, CAST, IDEA). Sia l'algoritmo da usare sia le chiavi segrete devono essere concordati e scambiati tra mittente e destinatario attraverso protocolli di sicurezza. Nel caso delle reti VPN, viene soprattutto utilizzato il protocollo **Internet Key Exchange (IKE)**, il cui compito principale è proprio implementare lo scambio delle chiavi per cifrare i pacchetti.

Lo scopo dei protocolli di tunneling è aggiungere un livello di sicurezza con l'incapsulamento al fine di proteggere ogni pacchetto nel suo viaggio su Internet.

Le VPN possono essere protette:

- In modalità trasporto → software impiegati
- In modalità tunnel (tunneling) → apparati (router e firewall)

I protocolli usati per il tunneling sono:

- IPsec (IP security)
- SSL/TLS (Secure Socket Layer / Transport Layer Security)
- BGP / MPLS (Border Gateway Protocol / Multiprotocol Label Switching)
- PPTP (Point-to-Point Tunnelling Protocol)
- IEEE 802.1Q (Ethernet VLANs)
- SSH (Secure SHell)
- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)

I protocolli per la sicurezza nelle VPN:

- IPsec
- SSL/TLS

IPsec non è un singolo protocollo, ma una architettura di sicurezza a livello network, composta da vari protocolli e da altri elementi.

I protocolli principali che lo costituiscono sono:

- **Authentication Header (AH):** garantisce autenticazione e integrità del messaggio ma non offre confidenzialità;
- **Encapsulating Security Payload (ESP):** fornisce autenticazione, confidenzialità e integrità del messaggio;
- **Internet Key Exchange (IKE):** implementa lo scambio delle chiavi per realizzare il flusso crittografato.

Nel momento in cui 2 host devono inviarsi dei dati, usando **AH o ESP**, è necessario instaurare prima una connessione logica, detta **Security Association** (SA) → per stabilirla viene usato **IKE**.

IKE è un protocollo a livello Application che usa UDP ma implementa un servizio affidabile, infatti, quando invia una richiesta per attivare una SA, la ritrasmette se non riceve risposta. In generale, le chiavi associate alle SA devono essere usate per un tempo limitato e per proteggere una quantità limitata di dati. Nel caso servisse trasferire altri dati, si instaura una nuova SA.

VPN Site-to-site con tunnelling IPsec

Le SA sono unidirezionali, per cui sono necessarie 2 SA per permettere a 2 host di comunicare tra di loro.

SAD (Security Association Database) → contiene tutte le Security Association attive su un host (o su un security gateway)

SPD (Security Policy Database) → contiene le politiche di sicurezza (tramite queste il sistema decide se un pacchetto deve essere scartato, lasciato passare in chiaro oppure elaborato tramite IPsec)

Il protocollo AH fornisce servizi di autenticazione, integrità e **protezione da attacchi di tipo replay**, in cui un intruso immette nella rete un pacchetto autentico precedentemente intercettato.

Protocolli per la sicurezza nelle VPN (AH):

- **Next header:** contiene l'ID del protocollo dell'header successivo (TCP, UDP, ICMP)
- **Payload length:** contiene la lunghezza dell'header AH
- **Reserved:** riservato per usi futuri, deve essere posto a zero.
- **Security Parameters Index (SPI):** contiene un numero che con l'IP di destinazione ed il protocollo (AH) identifica la SA utilizzata stabilito quando negoziata
- **Sequence number:** specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza tramite un meccanismo a finestra.
- **Authentication data:** contiene l'**Integrity Check Value (ICV)** del pacchetto. La lunghezza di questo campo è variabile ma deve essere un multiplo di 32 bit, per cui è possibile inserire un padding.

Protocolli per la sicurezza nelle VPN (ESP):

- **Next header:** contiene l'ID del protocollo dell'header successivo (TCP, UDP, ICMP) (se si utilizza il servizio di riservatezza, questo campo è cifrato)
- **Security Parameters Index (SPI):** contiene un numero che con l'IP di destinazione ed il protocollo (AH) identifica la SA utilizzata stabilito quando negoziata
- **Sequence number:** specifica il numero di sequenza del pacchetto all'interno della SA, per prevenire i replay attack. Il destinatario gestisce i numeri di sequenza tramite un meccanismo a finestra.
- **Payload data:** contiene il payload del pacchetto IP originale (modalità trasporto) oppure l'intero pacchetto IP originale (modalità tunnel), cifrato se si utilizza il servizio di riservatezza. Nel caso l'algoritmo di cifratura utilizzato necessiti di **Initialization Vector (IV)** (inserito all'inizio del payload).
- **Padding:** può essere necessario per
  - L'algoritmo di cifratura richiede un dimensione del testo multipla di tot
  - Assicurare il corretto allineamento dei campi successivi
  - Limitare gli effetti dell'analisi del traffico basata sulla dimensione
- **Pad length:** contiene la lunghezza del padding
- **Authentication data:** contiene il valore di controllo integrità **(ICV)** calcolato sull'intero pacchetto ESP escluso questo campo. È presente solo se si utilizza il servizio di autenticazione/integrità

Fornisce servizi di confidenzialità autenticazione, integrità e protezione da attacchi di tipo replay.

- A differenza di AH, l'autenticazione non copre l'header IP esterno
- Anche l'ESP presuppone che esista già una SA tra i due nodi

Protocolli per la sicurezza nelle VPN (IKE):

Realizza un collegamento peer-to-peer in due fasi:

- **1° fase** → i 2 host creano una SA per l'IKE stesso **(IKE SA)**, ovvero un canale sicuro da utilizzare per i messaggi di IKE.
- **2° fase** → utilizzano la SA appena creata per negoziare altre SA per altri protocolli (IPsec SA)

Protocolli per la sicurezza nelle VPN (SSL/TLS):

Le differenze da IKE sono poche e marginali, tuttavia sono non compatibili. In generale, vengono implementati entrambi e viene garantita l'interoperabilità.

TLS è un protocollo di livello Session dello stack ISO/OSI. Opera quindi al di sopra del protocollo di livello Transport. È uno standard IETF e deriva dal protocollo SSL. SSL è stato originariamente proposto da Netscape Communications, ma è un protocollo open

Composto da 2 livelli:

- **Record Protocol:** opera sopra un protocollo di liv. Transport (come TCP), è utilizzato per incapsulare protocolli di livello superiore
- **Handshake Protocol:** si occupa della fase di negoziazione in cui si autentica l'interlocutore e si stabilisce la crittografia comune

La realizzazione di una **VPN SSL/TLS-based** passa innanzitutto attraverso l'uso di **SSL/TLS** per l'**autenticazione** degli estremi del tunnel e la creazione delle **chiavi**.

SSL/TSL è un protocollo Client/Server che ha lo scopo di autenticare il server da parte del client (+ viceversa opzionale), e di creare un canale cifrato di comunicazione tra i 2.

L'autenticazione è basata sui certificati digitali riconosciuti da una **Certification Authority**. Il server invia il proprio certificato al client che ne verifica la validità (confronta la firma digitale con quella a lui nota). Se è valida → accetta il certificato e autentica il server. Analogamente il server può chiedere il certificato al client per verificarne la validità.

1) **Client** → **Server** il client invia al server:
- La richiesta di connessione
- La lista degli algoritmi di crittografia supportati
- Un valore random necessario a creare la pre-master-key
  (a sua volta servirà a generare la chiave privata di crittografia comune a entrambi)

2) **Server** → **Client** il server invia al client:
- Il proprio certificato digitale
- La scelta dell'algoritmo di crittografia
- Il proprio valore casuale per la pre-master-key
- La richiesta del certificato del client

3) **Client → Server** il client verifica il certificato del server
    - Se negativo → il protocollo fallisce
    - Se positivo → invia al server:
        - Il proprio certificato digitale
        - La pre-master-key cifrata con la chiave pubblica del server.

    Infine, il client accoda la richiesta di passare a comunicazioni cifrate

4) **Server → Client:** il server conferma al client di aver accettato il suo certificato digitale e passa alla fase di comunicazioni cifrate.

Dopo il punto 3 sia il client che il server hanno tutte le informazioni necessarie per calcolare la chiave, comune ad entrambi, e gli algoritmi a cui applicarla

SSL/TLS è adatto a proteggere la comunicazione tra due applicazioni (autentica l'applicazione o l'utente), **IPsec** può facilmente rendere sicuro il traffico tra host o tra intere sottoreti (autentica la macchina).

Principali differenze tra i due protocolli.

IPsec	SSL/TLS
Architettura complessa.	Singoli protocolli.
Peer-to-peer (IKE).	Client/Server.
Livello Network.	Livello Session.
Canale tra due macchine.	Canale tra due applicazioni.
Protezione di tutto il traffico IP.	Protezione solo del traffico TCP.
Protezione di tutto ciò che segue l'header IP.	Protezione dei dati del livello Application.
Impatto maggiore sul sistema operativo.	Impatto maggiore sulle applicazioni.

Le **reti** possono essere **classificate** per protocolli e grado di sicurezza **in 3 categorie:**

- **Trusted VPN**
- **Secure VPN**
- **Hybrid VPN**

Trusted VPN: (percorsi controllati)

- Riservatezza dei dati trasmessi controllata da un Internet Service Provider (ISP)
- Non utilizzano i protocolli che permettono la cifratura ed il conseguente tunneling
- L'ISP assicura una qualità del servizio (QoS) (controllo di percorsi dedicati)
- L'azienda che si rivolge all'ISP ha fiducia che i percorsi siano mantenuti sicuri

Secure VPN: (cifratura dei dati)

- Utilizzano protocolli che consentono la cifratura e il tunneling
- Per essere definita tale, una VPN deve garantire:
    - Sistema di autenticazione
    - Dati viaggiano criptati
    - Il livello di cifratura dei dati è elevato e modificabile nel tempo

Hybrid VPN: Tentativo di unire le caratteristiche delle Trusted VPN e delle Secure VPN

RETI WIRELESS

Le reti wireless possono utilizzare onde radio o segnali infrarossi per comunicare e vengono classificate in base alla loro estensione (come le reti wired)

- **WPAN** (Wireless Personal Area Network)
- **WLAN** (Wireless Local Area Network)
- **WMAN** (Wireless Metropolitan Area Network)
- **WWAN** (Wireless Wide Area Network)

WPAN

- Coprono il campo d'azione di una persona (fino a 10-15 metri)
- La maggior parte usa le onde radio
  - **Bluetooth** (frequenza libera ISM a 2,4 GHz), 2 Mb/s
- Altre usano gli infrarossi (fino a 3 metri, dispositivi **Line of Sight (LoS)**)
  - **IrDA** (Infrared Device Applcation), 4 Mb/s

WLAN

- Sono simili alle LAN cablate
- Lo standard più diffuso è IEEE 802.11
- Sono composte da:
  - **Wireless Terminal (WT)** → dispositivi mobile (pc, tablet, smartphone)
  - **Access Point (AP)** → agisce da bridge (wired-wireless) e da gateway

- AP + WT = **BSS (Basic Service Set)** → costituisce una **cella**
- È possibile collegare + più AP alla rete → **Wireless Distribution System**
- 2 o più BSS collegati da un WDS → **ESS (Extended Service Set)**

All'interno di un ESS **i diversi BSS possono essere collocati:**

- **BSS parzialmente sovrapposti** → copertura continua
- **BSS fisicamente disgiunti**
- **BSS co-locati** → diversi BSS nella stessa area (ridondanza / + prestazioni)

Lo standard 802.11 gestisce la mobilità delle stazioni distinguendo **3 tipi di transizioni:**

- **Transizione statica:** immobile o si sposta nell'area di 1 singolo BSS
- **Transizione tra BSS:** la stazione si sposta tra 2 BSS parzialmente sovrapposti
- **Transizioni tra ESS:** la stazione si sposta tra BSS appartenenti a 2 ESS diversi

La **configurazione di un AP:**

- **SSID (Service Set Identifier)**: nome assegnato alla WLAN, inviato con il beacon
- **Potenza**: **l'EIRP (Effective Isotropic Radiated Power)**, potenza dell'antenna
- **Canale:** (1-13), bisogna applicare la regola del 5 per non farli sovrapporre
- **Crittografia:** standard **WEP (Wireless Equivalent Privacy)**
- **Incapsulamento:** se l'AP è anche router
- **NAT e DHCP**

Oltre le WLAN aziendali e domestiche ci sono le **MANET (Mobile Ad hoc NETwork)**, usate dove non è possibile installare un AP (es. WI-FI Direct)

WMAN

- Distribuire dati tramite un'antenna
- Connessione di tipo:
  - Point-to-point (brighe → 2 antenna collegate alla rete cablata)
  - Point-to-multipoint (1 antenna omnidirezionale + N antenne unidirezionali)

WWAN

- Coprono uno spazio molto ampio come uno stato o un continente
- Queste tecnologie sono offerte da **WISP (Wireless Internet Service Provider)**

Attacchi nelle reti wireless

Sniffing: intercettazione passiva dei dati che transitano in rete. Usato per monitorare il traffico o intercettare in maniera fraudolenta i dati sensibili. Gli sniffer intercettano i singoli pacchetti, decodificano gli header dei vari livelli e ricostruiscono lo scambio di dati tra le applicazioni.

- **Scopi legittimi:** individuazione delle congestioni di rete o tentativi di intrusione
- **Scopi illeciti:** intercettazione di password, numeri di carte di credito, …

Accesso non autorizzato: a una rete privata senza autorizzazione. La tecnica più utilizzata è quella di servirsi di un **Access Point Rouge (APR)** cioè un AP non autorizzato. Per ostacolarlo è necessaria l'autenticazione reciproca tra i WT e gli AP. Inoltre, gli AP devono eseguire l'autenticazione con gli SW, impedendo la connessione di un APR.

I **wardriver** infrangono le scarse misure di sicurezza delle reti private per navigare gratis

Sostituzione del SID (Security IDentifier) (spoofing): Ad ogni account viene assegnato un identificativo SID a cui vengono associate autorizzazioni precise. La sostituzione del SID avviene posizionando un WTR intermedio tra un utente e AP. Questo tipo di attacco può sfruttare il protocollo ARP.

Lo **spoofing** è un tipo di attacco informatico in cui si realizza la falsificazione dell'identità. Questo attacco può avvenire in qualsiasi livello della pila ISO/OSI.

Per evitare lo spoofing, si può usare il protocollo **SARP (Secure ARP)**, che fornisce un tunnel protetto tra client e AP o router. Questo protocollo permette all'AP di ignorare ogni risposta non associata al client posto esattamente all'altra estremità.

Attacco DoS (Denial of Service): capace di paralizzare o disattivare una rete wireless, rendendola indisponibile per un periodo di tempo indeterminato. Usa attacchi **brute force**, oppure attacchi che utilizzano forti segnali radio che si sovrappongono ai segnali della rete rendendo inutilizzabili AP e WT

Crittografia WEP (Wired Equivalent Privacy):
WEP viene implementata a livello MAC ed è supportata dalla maggior parte dei dispositivi mobili e AP. Viene crittografato il payload del frame da trasmettere utilizzando l'algoritmo di cifratura a flusso (a chiave simmetrica) **RC4**.

Crittografia TKIP (Temporal Key Integrity Protocol):
Evoluzione del WEP, mantiene l'RC4, ma parte con una chiave temporale a 128 bit condivisa tra WT e AP (simmetrica). Alla chiave temporale combinata con l'indirizzo MAC del WT, si aggiunge un IV di altri 128 bit per creare la chiave di crittografia dei dati. Questa chiave viene rigenerata a ogni pacchetto o a ogni burst (raffica) di pacchetti inviati. **(distribuzione dinamica delle chiavi).**

TKIP > WEP → temporalità della chiave e > lunghezza dell'IV

Crittografia AES (Advanced Encryption Standard):
Alternativa a TKIP che garantisce una crittografia più sicura. AES è ritenuto indecifrabile **(uncrackable)** grazie all'utilizzo dell'algoritmo di **crittografia a blocchi Rijndael** al posto dell'RC4. Lo svantaggio di AES è che richiede una grande capacità di elaborazione (non tutti gli AP in commercio possono supportare).

WPA:

Nel 2018 la Wi-Fi Alliance ha introdotto un programma di certificazione per il WPA3, con l'obbietivo di fornire miglioramenti e nuove funzionalità di sicurezza, tra cui il blocco degli attacchi basati su KRAC (riusciti su WPA2).