appunti_interrogazione_sistemi_4

Sicurezza

pg.232

Minacce

Le minacce si possono dividere in 2 tipi:

Naturali

Sono dovute a eventi naturali imprevedibili come tempeste, inondazioni, fulmini, incendi e terremoti.. eventi quasi impossibili da impedire e prevenire.

Per questo tipo di attacchi è necessario effettuare una **analisi dei rischi**, dato che potrebbero esserci solo periodi di inattività fino a danneggiamenti delle apparecchiature/infrastruttura o perdita di dati.

Oggi ci sono disposizioni legislative che prevedono la messa in atto di misure preventive, destinate alle operazioni di **disaster recovery**, cioè la predisposizione di piani di ripristino e emergenza.

Umane

Sono dovute a soggetti che hanno interesse nell'acquisire le informazioni di una azienda, o la limitazione della sua operatività tramite danneggiamenti ai suoi processi.
Possono essere causate da:

- *personale interno* (**attacchi interni**), come dipendenti scontenti o malintenzionati.
  Il tipo più pericoloso, dato che i dipendenti conoscono la struttura del sistema informativo e di quelli di sicurezza.
  Possono quindi facilmente inserire nei sistemi malware come *virus*, *trojan horse* e *worm*, o trasmettere informazioni verso l'esterno, tramite *spyware*, o creare una *backdoor*.
- *soggetti estranei* (**attacchi esterni**), con lo scopo di creare problemi / danneggiare l'organizzazione.

In rete

È soprattutto diventato oggi un grande pericolo perché basta infettare un dispositivo per infettare tutta la rete.

Sicurezza di un sistema informatico

Gli obiettivi della sicurezza dei dati si dividono in 3 parti, dette **CIA**:

- **Data *C*onfidentiality**, mantenere la segretezza dei dati
- **Data *I*ntegrity**, evitare che i dati vengano alterati
- **System *A*vailabity**, garantire il funzionamento del sistema

Questi obiettivi, strettamente connessi tra loro, sono garantiti tramite l'attenzione ad alcuni aspetti:

- **Autenticazione** (*Authentication*), con cui si intende il processo di riconoscimento delle credenziali di un utente.
- **Autorizzazione** (*Authorisation*), ogni utente deve essere associato ad un **insieme di autorizzazioni**, un elenco che specifica quali azioni sono permesse e quali negate, a quali risorse può accedere e quali modificare.
- **Riservatezza** (*Privacy*), le informazioni devono essere accessibili solo dagli utenti autorizzate. Gli altri utenti non devono avere modo di intercettarle.
- **Disponibilità** (*Availability*), un documento deve essere accessibile in qualsiasi momento alle persone autorizzate. È necessario garantire la continuità del sistema in ogni momento.
- **Integrità** (*Integrity*), si deve avere una garanzia e certezza che il documento sia l'originale, e che i contenuti non siano stati letti o alterati/modificati da persone non autorizzate. È anche necessario prevenire azioni che potrebbero causare il danneggiamento di dati/documenti.
- **Paternità**, ogni documento deve essere associato a un utente, il quale non deve poter ripudiare o negare messaggi rivolti o inviati da lui.
  È spesso anche necessario avere la **tracciabilità di un documento**, in modo da saper chi ha avuto accesso a questa risorsa.

Le misure da intraprendere per ottenere la **segretezza** possono essere affrontate anche a livelli diversi della **pila protocollare**:

- **A livello fisico** si può cercare di impedire intercettazioni di dati da intrusi.
- A **livello di data link** si possono introdurre codifiche e cifrature da rendere i dati quasi incomprensibili ai cracker.

Linee guida per lo sviluppo, uso e monitoraggio dei **sistemi di gestione della sicurezza delle informazioni** (**SGSI**) sono raggruppate nella certificazione **ISO/IEC 27001:2017**.

Tipi di minacce

Attacchi passivi

- Lettura dei contenuti, come lo *sniffing dei pacchetti* (**packet sniffing**)
- Analisi del sistema e del traffico di rete, senza analizzarne i contenuti

Attive

Intercettazione

A differenza del semplice *spionaggio/sniffing*, l'obiettivo è di intercettare password con le quali ottenere l'accesso ai sistemi.
È possibile che per eseguire questo attacco sia necessario un attacco preventivo, come l'installazione di componenti hardware (*dispositivi pirati*) o software specifici.
Per esempio: Si potrebbero inserire *server pirata* (**shadow server**) nella rete, che si spacciano per quelli originali, nei quali sono state modificate le tabelle di routing (**spoofing**), o tramite l'installazione di programmi che emulano i servizi del sistema, registrando le informazioni riservate.
es. il programma di login potrebbe essere sostituito in modo da intercettare la password (**password cracking**).

Sostituzione di un host

Sempre ottenuto tramite l'**IP spoofing**, qualcuno si sostituisce a un host falsificandone l'indirizzo di rete (generalmente si falsifica l'indirizzo di *livello 3 (ip)*, ma è anche possibile modificare quello di *livello 2*.) Questo tipo di attacco prende il nome di **source address spoofing**, con lo scopo di falsificare i dati tramite l'accesso non autorizzato.

Produzione

I malintenzionati producono nuovi componenti, i quali vengono inseriti nel sistema con lo scopo di arrecare danno e non di prelevare informazioni: sono veri e propri atti di sabotaggio, con lo scopo di ridurre la disponibilità di un sistema.
Le principali tecniche sono le seguenti:

- **attacchi virus**: un programma che provoca danni e si replica *infettando* gli altri host
- **attacchi worm**: la cui caratteristica è la replicazione senza bisogno di attaccarsi ad altri programmi, provocando danni come il consumo di risorse
- **attacchi DoS** (*Denial of Service*): Lo scopo è di tenere gli host occupati con operazioni inutili, in modo da impedire che possa offrire i propri servizi.
  Le principali tecniche di DoS sono:
  - Saturazione della posta/log
  - **ping flooding**
  - **SYN attack** (attacco al 3-way handshake)
  - **DDoS**, *distributed DoS*, che consise nell'installazione di un software per DoS su molti nodi, formando un *Botnet*, programmi detti **daemon, zombie o malbot**. (i *daemon* sono spesso controllati da un **master** tramite canali cifrati, e hanno la possibilità di auto-aggiornarsi)
- **Phishing**: attraverso uno spam di email si attira l'utente ad uno **shadow server**, in modo da catturarne le credenziali o altre informazioni personali, oppure di invitare l'installazione di plugin o estensioni che sono *virus/trojan mascherati*.

Una variante evoluta è lo **spear phishing**, che include nelle email dati personali per sembrare più credibili.
- **Intrusione**: consiste nel vero e proprio accesso non autorizzato a uno o più host, dove può modificare o cancellare le informazioni altrui, prelevare dati e introdurre dati falsi...

Sicurezza nei sistemi informativi distribuiti

Si divide in 2 parti:

- **Sicurezza nella rete**
- **Sicurezza sugli host**
  - A livello di *sistema operativo*
  - A livello di *applicazione*

L'obiettivo base è quello di garantire al sistema un **principio minimo di sicurezza**, che consiste nella protezione da attacchi passivi e nel riconoscimento degli attacchi attivi. Questo si realizza tramite l'analisi di tutti i componenti sia fisici che logici del sistema, e l'individuazione per ciascuno delle tecniche di attacco applicabili. (separate tra attive e passive)

I 3 punti principali della sicurezza sono:

- **La prevenzione** (*avoidance*), mediante protezione dei sistemi e della comunicazione (*crittografia, firewall, VPN...*)
- **La rilevazione** (*detection*), mediante il monitoraggio e il controllo degli accessi tramite autenticazione con password e certificati
- **Investigazione** (*investigation*) con l'analisi dei dati, il controllo interno e con il confronto e la collaborazione degli utenti

Prevenzione

Le tecniche principali adottate sono:

- **Uso della crittografia**, che garantisce la riservatezza delle informazioni e l'integrità dei dati, efficace contro gli attacchi di sniffing.
- **Autenticazione degli utenti**, a cui sono associate 3 problematiche diverse:
  - **Identificazione**
  - **Autenticazione**
  - **Autorizzazione**
- **Firma elettronica**, la quale garantisce l'autenticazione non falsificabile del documento, che garantisce che non sia stato alterato ed è quindi **non ripudiabile**
- **Connessioni TCP mediante SSL**, le connessioni sicure sono garantite da protocolli come il ***S*ecure *S*ocket *L*ayer** (*SSL*), che offre i servizi di sicurezza per l'autenticazione delle parti in comunicazione, garantendo integrità e riservatezza.
- **Firewall**, che permette il filtraggio dei pacchetti entranti/uscenti

- **Reti private e private virtuali**
  Possono essere delle reti pubbliche ad uso esclusivo dell'azienda, costose, oppure realizzate in *modo virtuale* tramite **VPN** (*Virtual Private Network*), più economico, creando tunnel protetti sulle infrastrutture mediante connessioni punto-punto di pacchetti autenticati incapsulati in pacchetti tradizionali

Firewall

Può essere sia un pezzo di **hardware** sia un **software** sul *router* (che causa però un rallentamento della velocità).
Permette il **filtraggio** dei pacchetti *entranti e uscenti*.
Il filtraggio viene eseguito secondo le *Access Control List*.

Può di prevenire attacchi DoS come il *SYN flooding*.
Ci sono 2 tipi di Firewall:

Personal Firewall

Firewall di tipo software presente sui singoli host, spesso fornito dal sistema operativo.
Controlla i dati in entrata e uscita del PC.
Non viene usato in ambiente aziendale dato che sarebbe necessario configurare manualmente ogni singolo host.

Network Firewall

Usati nelle aziende, spesso su una o più macchine dedicate, che eseguono il filtraggio del traffico di tutta la rete locale.

Packet-Filtering

Lavora al livello di rete e trasporto. (e di collegamento dati)
Dei pacchetti viene esaminato solamente l'header, e non i contenuti.
Esamina:

- Indirizzo IP e MAC del mittente e destinatario
- Numero di porta di destinazione
- Protocollo utilizzato (*TCP, UDP, ICMP*)

I **vantaggi** sono:

- **trasparenza**: dato che l'utente non si accorge del firewall dato che non viene ostacolato il normale uso della rete (non è necessario configurare i computer per l'uso del firewall)
- **velocità**: effettuando minori controlli rispetto ad altri firewall, è il più veloce e facile da implementare
  - **immediatezza**: si può facilmente difendere le reti con singole regole che bloccano tipi di traffici

- ***gateway-only***: non è necessaria configurazione sull'host
  Se viene aggiunto il NAT, la topologia interna della rete può diventare invisibile dall'esterno

Gli **svantaggi** sono:

- Lavora a **basso livello**, che rende impossibile bloccare il traffico di applicazioni specifiche
  - **Mancanza di servizi aggiuntivi**: non è possibile gestire servizi come quelli di autenticazione, l'*HTTP object caching* o il filtraggio di URL e dei contenuti delle pagine web
- **Logging limitato**: I firewall creano dei log dei pacchetti che vengono bloccati, ma a questo livello non è possibile creare log dettagliati a causa delle poche informazioni fornite dall'header
- **Vulnerabilità allo spoofing** (*IP*): I pacchetti sono filtrati in base alla provenienza, rendendolo quindi vulnerabile ai casi di spoofing
- **Testing complesso**: la prova delle regole è lunga e complicata

Il filtraggio tradizionale dei pacchetti non verifica lo stato della connessione.
Il malintenzionato si può quindi introdurre durante la creazione del canale di comunicazione tramite l'invio di pacchetti *ACK*, nonostante l'inizio dell'Handshake sia stato fatto da un altro host.

Per risolvere questo problema è stato creato lo *Stateful Inspection*

Stateful Inspection

Memorizza in una tabella tutte le sessioni *TCP* attive, tenendo traccia dello stato del three-way-handshake.

I **vantaggi** sono:

- Maggiore **sicurezza e velocità**, perché una volta che viene verificata la connessione è possibile effettuare meno controlli su quel traffico
- **Protezione da IP spoofing e session hacking**
- *Rimangono i vantaggi del packet filtering*

Gli **svantaggi** sono:

- **Protocollo unico** perché dipende da molte funzionalità specifiche al *protocollo TCP*, rendendone difficile l'uso in altre infrastrutture di rete
- *Rimangono gli svantaggi di logging limitato, mancanza di servizi aggiuntivi e il testing complesso*

È possibile essere sicuri da attacchi che *falsificano il source address IP* verificando che i pacchetti arrivino da interfacce verso l'interno del router, invece di quelle rivolte verso

l'esterno.

Circuit Gateway

Lavora al livello di sessione (e di trasporto), permette il controllo delle sessioni TCP.
Non più usato perché inglobato nella *stateful inspection*

Application Level Gateway (Proxy server)

Funziona come il *proxy*, che è un *man-in-the-middle* per velocizzare la connessione tra mittente e destinatario, ma introduce funzionalità avanzate del Firewall.
Lavora a livello applicativo, rendendo quindi possibile il controllo dei contenuti dei pacchetti.

I vantaggi sono:

- **controllo completo**: lavorando a livello applicativo, è possibile esaminare anche il *body* del pacchetto e, essendo *man-in-the-middle*, esegue un doppio controllo sia sulla richiesta che sulla risposta
    - Il livello applicativo rende anche possibile l'**autenticazione e filtraggio dei contenuti**
    - **cache**: come i proxy, effettua il caching delle pagine web, offrendo un ulteriore servizi di liberazione del traffico
- **logging dettagliato**, grazie alle informazioni fornite dal livello applicativo
- **nessuna connessione diretta** tra il malintenzionato e il server, rendendo possibile il blocco di tentativi di attacchi come il *buffer-overflow* prima che arrivino al server
    - **sicurezza anche in caso di crash**: dovesse fallire il proxy, la LAN rimane isolata dall'esterno, rimanendo quindi sicura
- **user-friendly**: la configurazione delle regole di filtraggio è più semplice

Gli **svantaggi** sono:

- **trasparenza minore**: richiede che ogni computer della LAN interna sia configurato per utilizzare il proxy
    - **è necessario un proxy per ogni applicazione**, per ogni servizio e, data la dinamicità dei servizi offerti in rete, è necessario un continuo aggiornamento
- **poco performante**: la gestione della connessione tramite il proxy richiede molte risorse della CPU e ha quindi prestazioni inferiori in confronto agli altri firewall

ACL

Sono le liste di regole utilizzate dai Firewall per il filtraggio dei pacchetti.
Quando vengono filtrati gli indirizzi IP, viene usata la **Wildcard Mask**, che indica i bit che possono variare nell'indirizzo. (Utile per bloccare/ammettere intervalli di IP. I bit che variano sono impostati a 1, quelli statici a 0)
Se viene omessa, sarà automaticamente impostata a 0.0.0.0 (bloccherà solo l'IP inserito)

Quando si creano le regole, si può specificare se devono essere applicate per i pacchetti **in entrata** o quelli **in uscita**.

In base al tipo di controllo che si vuole eseguire, ci sono più tipi:

Standard

Alle *ACL Standard* si può assegnare un numero da *0 a 99*.
Si può impostare in loro solamente l'indirizzo IP-sorgente e la usa *wildcard mask*.

Queste regole sono usate sul *router di confine* del network *destinatario* (che offre il servizio), perché permettono il filtraggio senza rallentare la rete.

Sintassi Cisco:

- Con il comando **ip access-list** si possono creare le liste.
- Con il comando **ip access-group**, mentre si è in configurazione dell'interfaccia del router, è possibile applicare la lista per i pacchetti entranti o uscenti.

```
ip access-list numero permit/deny IP-sorgente wildcard-mask
```

```
ip access-group numero in/out
```

Estese

Alle *ACL Estese* si può assegnare un numero da *100 a 199*.
Si possono impostare gli indirizzi IP sia del mittente che il destinatario, il protocollo e i numeri di porta.
Se si usa il TCP, è anche possibile aggiungere il blocco della connessione con il flag *established*.

Queste regole sono usate sul *router di confine* del network *mittente*, perché così si sanno a priori i pacchetti da scartare, senza che debbano viaggiare su internet, creando traffico inutile.

Sintassi Cisco:

```
ip access-list numero permit/deny protocollo IP-sorgente wildcard-mask
[porta] IP-destinazione wildcard-mask [porta] [established]
```

DMZ (*Demilitarized Zone*)

Le reti delle aziende sono spesso composte da *sistemi distribuiti*:

- Un *logic/data layer* composto dai database, che possono contenere informazioni private come le credenziali di autenticazione

- Un *presentation layer* che contiene informazioni pubbliche come le pagine del sito web o un server di posta elettronica, che può necessitare di informazioni presenti nel layer dati

È quindi opportuno separare l'accesso, separando i layer in 2 reti separate:

- La rete composta dai database privati non avrà accesso ad Internet, ma solo ai server pubblici
- Internet ha accesso solo ai server pubblici, e non può accedere ai server privati

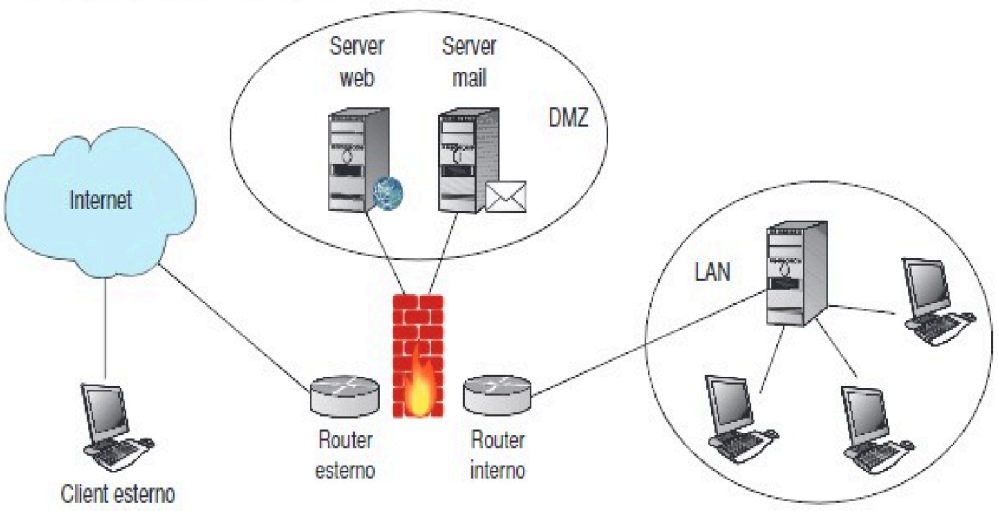
Con il NAT è possibile mascherare gli indirizzi interni e la tipologia della rete, dato che sarà usato solamente il gateway per la comunicazione con Internet.

Bastion Host

Il *Bastion Host* è il dispositivo più protetto della rete, spesso il singolo che necessita la connessione verso l'esterno.

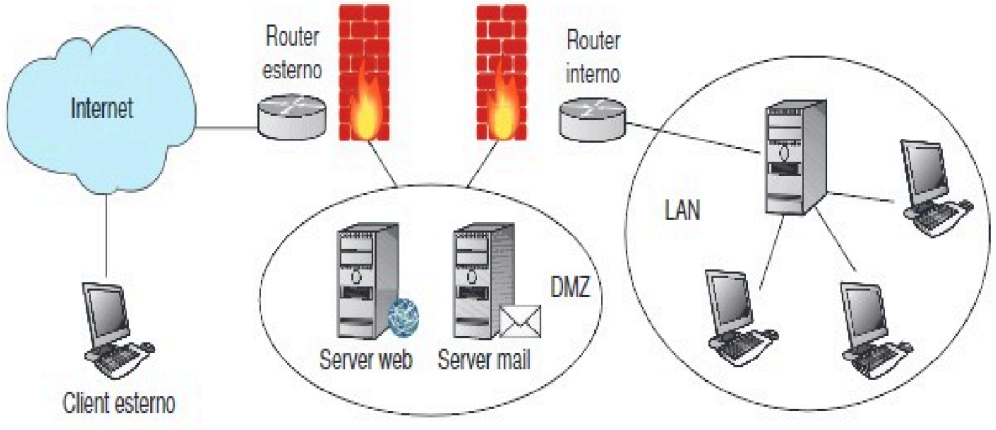
Architetture DMZ

1. Dentro un ramo del firewall

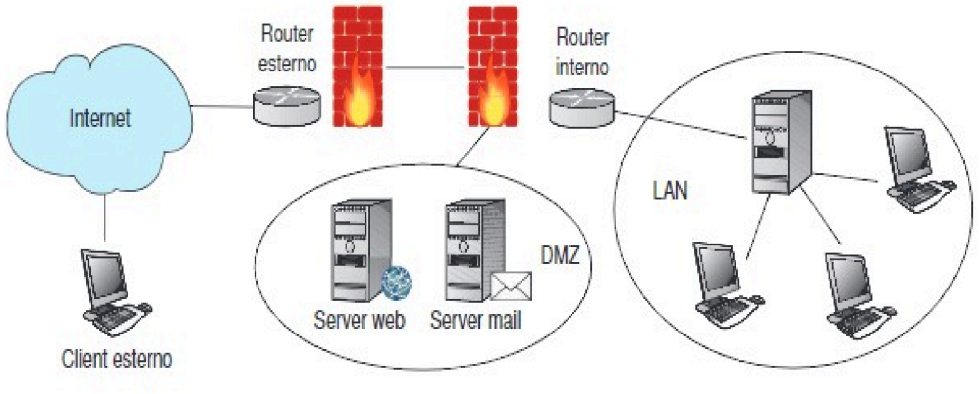


2. Tra due firewall

Architettura più sicura, perché per accedere alla rete privata bisogna rompere attraverso 2 firewall.



3. Sopra il firewall interno



NAT

Il *NAT* (*Network Address Translation*) è una tecnologia che è stata introdotta a causa della *carenza di indirizzi IPv4*.
traduce la comunicazione entrante e uscente in una rete verso l'esterno:
Quando una rete con indirizzo privato comunica verso Internet, il NAT in automatico esegue la conversione verso un'indirizzo pubblico.
Permette anche di mascherare la rete interna, perché è possibile utilizzare un solo indirizzo pubblico per tutti i dispositivi della rete. (spesso il *default gateway*)

Funzionando creando una tabella in cui crea la coppia di socket tra indirizzo privato-pubblico. (e il protocollo utilizzato)

I **vantaggi** sono:

- *Limita* gli IPv4 in Internet
- *Trasparenza*, perché non è necessario alterare la configurazione sugli host
  non bisogna nemmeno alterare il funzionamento di protocolli/applicazioni
- Maggiore *flessibilità* grazie all'uso di indirizzi privati
- Riduce i *costi* (Basta acquistare un solo indirizzo)
  Uno **svantaggio** del NAT è che non è in grado di gestire la *comunicazione contemporanea tra più host sulla stessa applicazione*. (*nel NAT semplice*)

Ci sono 3 tipi:

- **Static** *NAT*
  Converte gli indirizzi della rete in un solo indirizzo pubblico.
- **Dynamic** *NAT*
  Può convertire gli indirizzi della rete in più indirizzi pubblici diversi.
- **PAT** (*Port Address Translation*)
  Estensione del *NAT*, che esegue la traduzione (mascherazione) del **numero di porta**.

VPN

In passato, le aziende per avere una connessione privata tra più sedi utilizzavano una propria infrastruttura ad uso esclusivo, una **rete privata dedicata**.
Ha **vantaggi** come:

- Larghezza di banda *sempre disponibile*
    - *Prestazioni garantite*
- *Nessun problema di accesso*
    - *Sicurezza garantita*
      Ma ha anche **svantaggi** come:
- *Costi elevati*
- Necessita molta *banda*

Sono state successivamente sostituite dalle **VPN**, *Reti Private Virtuali*, che permettono un traffico *privato* sfruttando l'infrastruttura pubblica di Internet.
Ha **vantaggi** come:

- *Costi ridotti*
- *Multiplexing*
- *Trasparenza* (Non si necessita di autorizzazione, e può anche essere invisibile l'uso della VPN)
- *Capillarità* (Tramite la rete di Internet si ha un raggio che copre quasi tutto il mondo)
  Ha **svantaggi** come:
- *Necessità il controllo degli accessi*
- La *sicurezza delle trasmissioni* è garantita da protocolli, cifratura e tunneling.
- La Banda *non è sempre disponibile*

Le *VPN* eseguono il **Tunneling** sui pacchetti:
Consiste nell'**incapsulamento** dei pacchetti, creando all'interno del canale di comunicazione un *tunnel* in cui viaggiano i dati privati, *crittografati*, apparendo come se fossero pubblici.

Gli strati di tunneling possono essere creati a 2 livelli della pila:

- **Livello 2: strato di collegamento dati**, detti *Protocollo di tunneling punto-punto*
- **Livello 3: livello di rete**, dove l'*IPSec* può operare come protocollo VPN a livello di rete

Abbiamo 2 tipi di VPN:

- **Trusted VPN**, *VPN di fiducia*, dove la sicurezza viene affidata all'ISP della rete pubblica. L'ISP garantisce le proprietà del percorso, ma non viene garantito un alto livello di sicurezza.
- **Secure VPN**, dove vengono integrati protocolli di cifratura/tunneling come *IPSec* e *TLS/SSL*.
  Non sono garantite, però, le proprietà del percorso.

Protocolli

- **Protocollo PPTP** (*Point to Point Tunneling Protocol*) (lavora a livello 2)
  Vecchio protocollo Microsoft per la creazione dei Tunnel di comunicazione.
  È molto leggero, perché si occupa solo della creazione del tunnel, e necessita l'uso di protocolli aggiuntivi per la crittografia.
- **Protocollo L2TP** (*Level 2 Tunneling Protocol*)
  Protocollo che lavora al livello 2. (Successore del *PPTP*)
  Esegue la creazione del tunnel, ma esegue la crittografia solo sui messaggi di controllo.
  Viene successivamente integrato a livello 3 con protocolli come l'**IPSec**.
- **IPSec** (*Livello 3*)
  È un insieme di protocolli che permette di applicare la crittografia sui tunnel.
  Uno *svantaggio* è la maggiore *complessità*.
  È composto da 3 protocolli:
- **trasmissione di pacchetti**, dove è possibile usare uno dei due protocolli:
  - **Authentication Header**
  - **Encapsulation Security Payload**
- **Internet Key Exchange**, utilizzato per lo scambio delle chiavi

Viene creata una sessione per ogni connessione alla VPN, detta **Security Association** (**SA**), utilizzato per l'autenticazione.
È una *chiave unidirezionale* che identifica univocamente il *client* e il *server*.
Vengono memorizzate nel **Security Policy Database**, **SPD**.

Il monitoraggio del *traffico in uscita* viene controllato nelle seguenti fasi:

1. Viene controllato nell'SPD se è da scartare
2. Controllato se il pacchetto è incapsulato con l'IPSec
   Se non è presente, verrà ignorato
3. Se l'SA non esiste già, viene creato e aggiunto all'SPD

Il monitoraggio del *traffico in entrata*:

1. Controllato se è di tipo IPSec
2. Viene verificata l'SA
   - Se non esiste, il pacchetto viene scartato
   - Se esiste, viene elaborato l'IPSec
3. Se l'SA è valido il pacchetto passa ai livelli inferiori, altrimenti viene scartato

Il protocollo **Authentication Header**: (*AH*)
Include funzionalità di *autenticazione* e verifica dell'*integrità*.
Protegge dagli attacchi di tipo **relay**. (**DOS**, che consistono nella *duplicazione del pacchetto*)
Non garantisce *confidenzialità*. (Non viene eseguita la crittografia)

Alcuni campi dell'header IP, come il *time-to-live*, non vengono esaminati.
È **incompatibile con il NAT** perché il *checksum* di verifica viene calcolato anche in base ai

contenuti dell'header IP, modificato dal protocollo NAT.

Può funzionare in *2 modalità*:

1. **Trasporto**
   Il pacchetto finale incapsulato sarà composto in questo modo:

Authentication header		**Datagramma TCP**	
HeaderIP	AH	HeaderTCP	Payload

2. **Tunneling**

Authentication header		**Pacchetto IP**	**Datagramma TCP**	
HeaderIP	AH	HeaderIP	HeaderTCP	Payload

L'*Header di Autenticazione* contiene informazioni come i:

- *codici di autenticazione*
- *Informazioni per la verifica dell'integrità* (ICV)
- *Numero di sequenza*
  (Usato per combattere gli attacchi di duplicazione.
  Se quel numero di sequenza è di un pacchetto che è già stato accettato, verrà scartato)
- *SPI*, un codice che identifica l'SA.
  (*SPI* = Security Parameter Index)

Il protocollo **Encryption Security Protocol**: (*ESP*)
Include funzionalità di *autenticazione,* verifica dell'*integrità, protezione da attacchi relay* e **confidenzialità**.
Viene eseguita la *crittografia* solo sul payload. (Per i codici di verifica viene usato solo il payload, rendendolo compatibile con il *NAT*)

Ha *2 modalità*:

1. **Transport**

ESP		**Datagramma TCP**		**ESP**	
HeaderIP	HeaderESP	HeaderTCP	Payload	Trailer	Auth

2. **Tunneling**

ESP		**Pacchetto IP**	**Datagramma TCP**		**ESP**	
HeaderIP	HeaderESP	HeaderIP	HeaderTCP	Payload	Trailer	Auth

Il **Trailer ESP** contiene i *bit di padding* per garantire al cifrario che il blocchi siano della stessa lunghezza, e nasconde la lunghezza dal payload.
L'**Auth ESP** esegue il calcolo dell'hash usato per la verifica dell'integrità.

Il protocollo **Internet Key Exchange**: (*IKE*)

- Crea la trasmissione sicura utilizzata per lo scambio delle dell'SA.

Il **Server Radius** è un server per garantire le **AAA** di un utente che accede alla VPN.

- **Authentication**
- **Authorisation**
- **Accountability**

Applicazioni

Site to Site

consiste nel *collegamento di 2 o più reti aziendali tra loro*. (come quando si hanno più sedi distaccate)
Viene anche chiamato **VPN Lan to Lan**.
Ogni sede avrà un *router VPN* che rappresenta il tunnel tra le reti locali, che sfrutterà l'infrastruttura della rete pubblica.

End to Site

Consiste nell'*accesso ad una rete aziendale da una rete di casa o rete mobile*.
Il tunnel tra il terminale dell'utente e la rete aziendale viene realizzato da un *client VPN*, che sfrutta il canale della rete pubblica.

End to End

Consiste nell'*accesso remoto da un computer a un altro*.
Un uso comune di questo tipo è il protocollo **remote desktop**, utilizzato per visualizzare/gestire le applicazioni di un altro computer.
Il canale di trasmissione può essere una rete di qualunque tipo. (pubblica, aziendale, locale...)