M11 SEGURETAT I ALTA DISPONIBILITAT

Administració de Sistemes Informàtics en Xarxa
IES de l'Ebre

UF2 – Seguretat Activa i Accés Remot

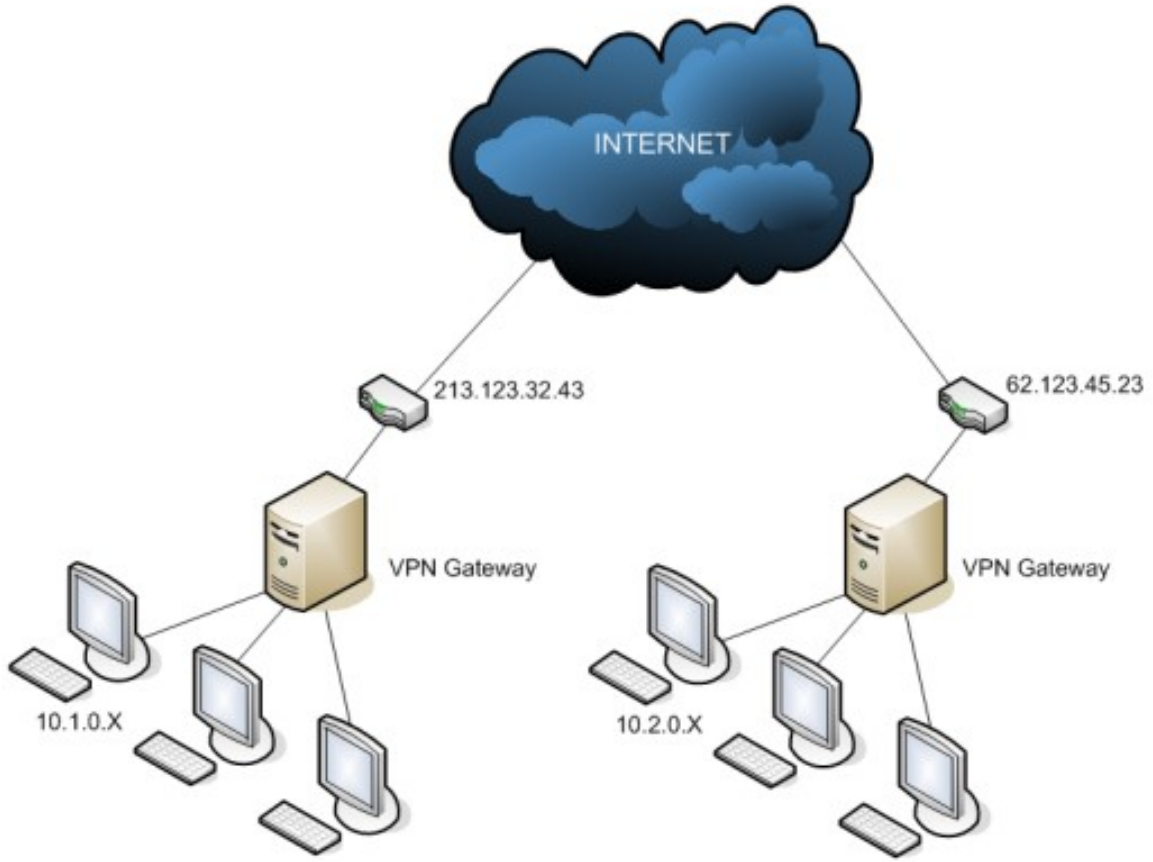
Xarxes Privades Virtuals. VPN

Xarxes Privades Virtuals

- Una **xarxa privada virtual** o VPN (*Virtual Private Network)* és una xarxa privada que s'estén a diferents punts remots mitjançant l'ús d'infraestructures públiques de transport (com per exemple, Internet).
- La transmissió de paquets de dades es realitza mitjançant un procés d'encapsulació i, per seguretat, de xifrat, ja que les dades circulen durant un temps per trams de xarxa pública.
- Aquests paquets de dades de la xarxa privada viatgen a través d'un "túnel". És a dir, s'aprofita el baix cost de l'accés a Internet, s'afegeixen tècniques de xifratge i se simulen les clàssiques connexions punt a punt.
- En el cas d'accés remot des d'un equip, la VPN permet a l'usuari accedir a la seva xarxa corporativa i li assigna al seu ordinador remot les adreces i privilegis d'aquesta xarxa, encara que la connexió s'hagi efectuat mitjançant una xarxa pública com Internet.

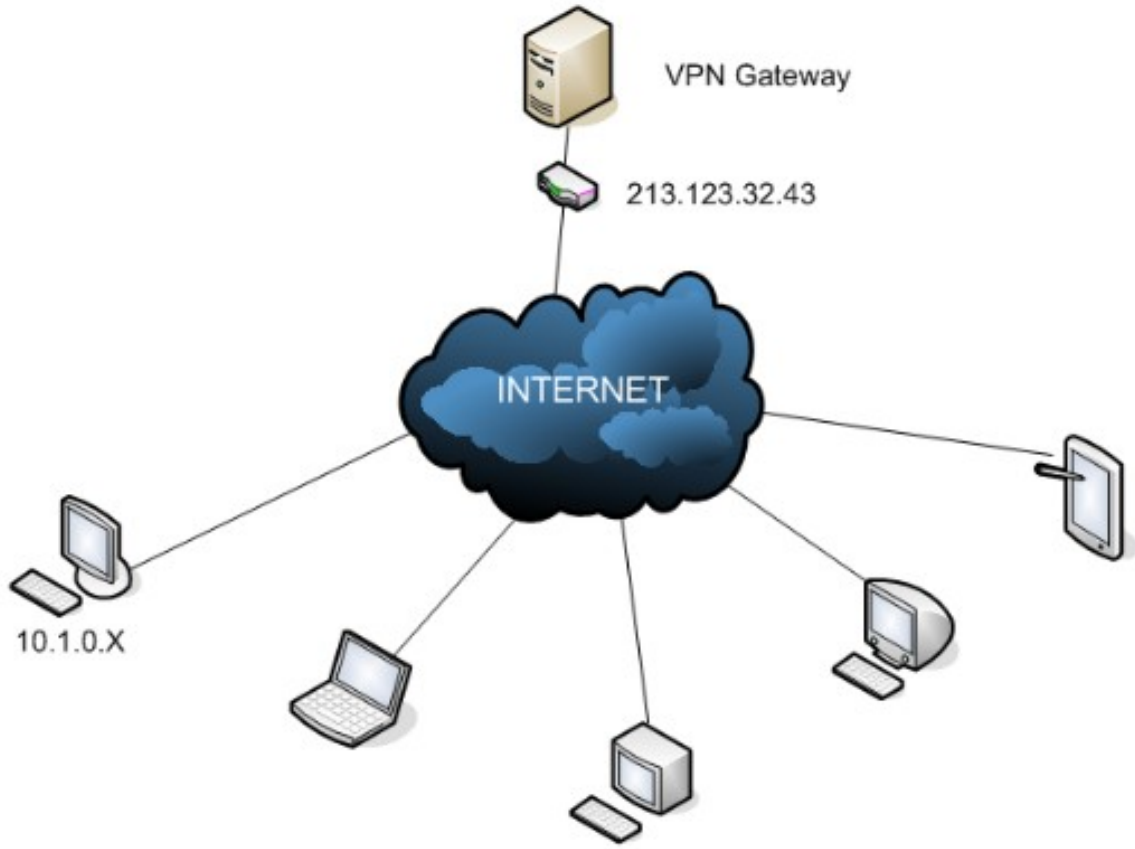
Interconnexió de xarxes

- Exemple: connexió de dues oficines d'una empresa
- S'estableix una VPN entre dos gateways, cadascun d'una xarxa privada
- Les màquines de les xarxes utilitzen aquests gateways com routers
- Quan una passarel·la rep un paquet dirigit a la xarxa privada l'altre extrem el s'envia a través de la VPN de manera segura
- Compte!, el trànsit només és protegit per la VPN al recorregut entre els dos gateways



Treballadors remots

- Exemple: treballadors remots (Road Warriors)
- Cada persona amb permís pot connectar des de qualsevol lloc.
- L'ordinador ha de comptar amb un client VPN, que estableix una connexió al concentrador de VPNs de la xarxa corporativa
- A partir d'aquest moment tot el trànsit des de l'ordinador a la xarxa corporativa queda protegit per la VPN



Avantatges i inconvenients VPN

Les xarxes privades ofereixen una sèrie d'avantatges, entre les que destaquen:

- **Seguretat**: és possible assegurar diversos serveis amb aquest mecanisme.
- **Mobilitat**: tenim una connexió segura entre usuaris mòbils i la nostra xarxa fixa, amb independència de la localització geogràfica
- **Transparència**: permet la interconnexió d'ordenadors en un sistema informàtic, però també de diferents xarxes. Tot transparent per a l'usuari, la configuració es pot fer només en l'entorn servidor.
- **Simplicitat**: una VPN aconsegueix que l'equip sigui vist per tota la xarxa, incloent servidors, la qual cosa simplifica l'administració d'equips remots.
- **Estalvi econòmic**: el trànsit segur de paquets per xarxes públiques té un cost econòmic sensiblement menor que la creació d'una xarxa dedicada.

Avantatges i inconvenients VPN

Per aconseguir tot això els paquets IP que es transmeten:

- S'han de **xifrar** per a garantir la **confidencialitat**
- S'han de **signar** per a garantir **l'autenticitat i la integritat**.

Pel que fa a possibles **inconvenients**:

- **Fiabilitat**: la dependència del proveïdor de xarxa (ISP) pot produir fallades en la xarxa que poden deixar incomunicats recursos de la nostra VPN.
- **Confiança**: si la seguretat d'un node o subxarxa que forma part d'una VPN queda compromesa es veurà afectada la seguretat de tots els components de la xarxa.

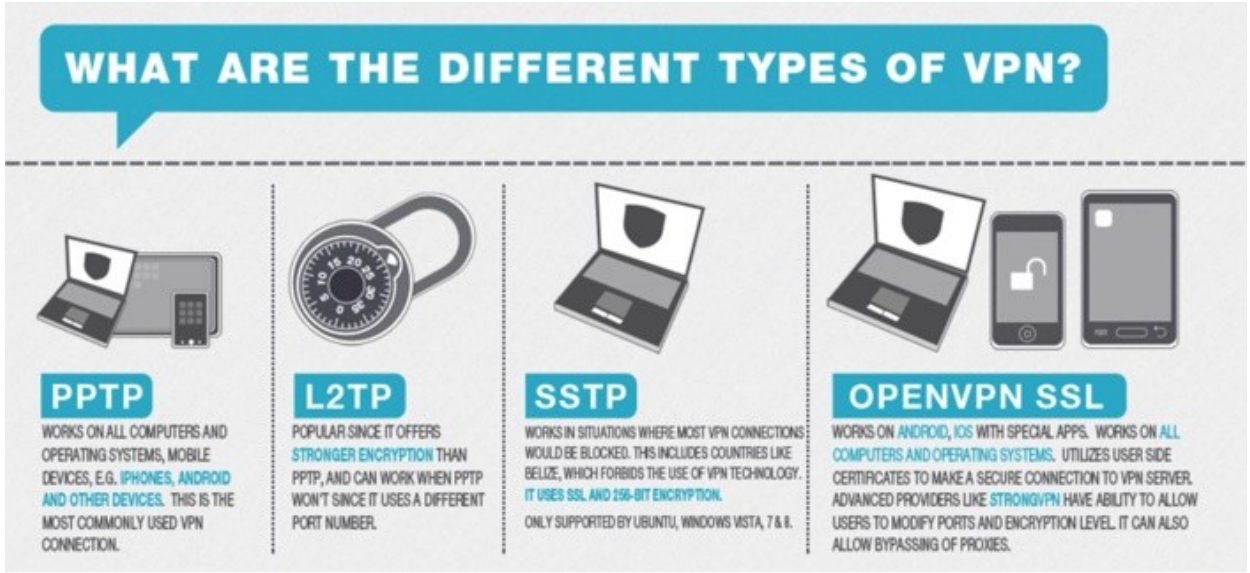
Tunneling

- Tunneling és un mètode que consisteix a **utilitzar la infraestructura** d'una xarxa de xarxes(com Internet), per **transportar** dades d'una **xarxa a una altra**.
- Les **dades** que han de ser transportades poden ser **paquets de protocol diferent** al que gestioni internet, és a dir, en lloc d'enviar un paquet tal com va ser produït pel node que el va originar, el **protocol de tunneling** (ja sigui L2TP, IPSec, etc) **l'encapsula en una capçalera addicional** que pertany al **protocol de transport d'Internet**, sobre la qual s'estableix el túnel (per exemple, IP).
- Els paquets encapsulats són llavors **encaminats sobre Internet** entre els extrems del túnel. A aquesta ruta lògica a traves de la qual viatgen els paquets encapsulats sobre Internet se l'anomena '**túnel**'.
- Quan els paquets (o quadres) encapsulats arriben al seu destí, el paquet és **desencapsula** i es reenviat al seu destí final.

Protocols de Tunneling

Els principals protocols de tunneling son:

- **IP Security (IPSec):** garanteix la seguretat de la transmissió i autenticació d'ususaris sobre xarxes públiques. Treballa a la cap de xarxa.
- **Protocol de Tunneling Punt a punt (PPTP):** és una alternativa a IPSec. Treballa en la capa d'enllaç i s'utilitza per a transmissions segures de tràfic basat en Windows.
- **Layer 2 Tunneling Protocol (L2TP):** es tracta d'una combinació de reenviament de capa 2 i PPTP, i es utilitzat per a encapsular trames de tipus PPP (Protocol Punt a Punt).
- **OpenVPN**: es un protocol de codi obert i s'ha convertit en un dels més utilitzats. Totes les dades son xifrades amb una clau AES-256 i autenticació RSA. Està disponible en gairebé totes les plataformes.



Secure Shell

- És un protocol que permet establir una connexió segura, de manera que un client pot obrir una sessió interactiva en una màquina remota per enviar ordres o fitxers a través d'un canal segur.
- Les dades que circulen estan **xifrades**, la qual cosa en garanteix la confidencialitat.
- **El client i el servidor s'autentifiquen mútuament** per assegurar que les dues màquines que es comuniquen són, de fet, aquelles que les altres parts creuen que són.
- Una connexió SSH s'estableix en diverses fases:
  - Es determina la **identitat** del servidor i del client (capa segura de transport). El client inicia sessió en el servidor.
  - Establiment d'un **canal segur**. Fase de negociació entre el client i el servidor per posar-se d'acord en els mètodes de xifratge que volen utilitzar.
  - **Autenticació**. Un cop s'ha establert la connexió segura entre el client i el servidor, el client s'ha de connectar al servidor per obtenir un dret d'accés. Hi ha diversos mètodes:
    - El mètode més conegut és la **contrasenya** tradicional.
    - Ús de **claus públiques**.