Instuderingsuppgifter – VPN

Syfte

Denna instuderingsuppgift ska ge en **grundläggande och praktiskt användbar förståelse** för vad ett VPN (Virtual Private Network) är, varför det används och vilka typer av VPN-lösningar som är vanligast idag. Fokus ligger på **IPsec och SSTP**, men även öppna och moderna lösningar som **OpenVPN och WireGuard** introduceras.

Efter genomförd uppgift ska du kunna:

- Förklara vad ett VPN är och vilka problem det löser
- Beskriva skillnaden mellan vanliga VPN-typer
- Förstå grunderna i IPsec och SSTP
- Känna igen vanliga VPN-lösningar och tillverkare
- Resonera kring när olika VPN-lösningar används
- (Valfritt) Sätta upp eller skissa en enkel VPN-lösning

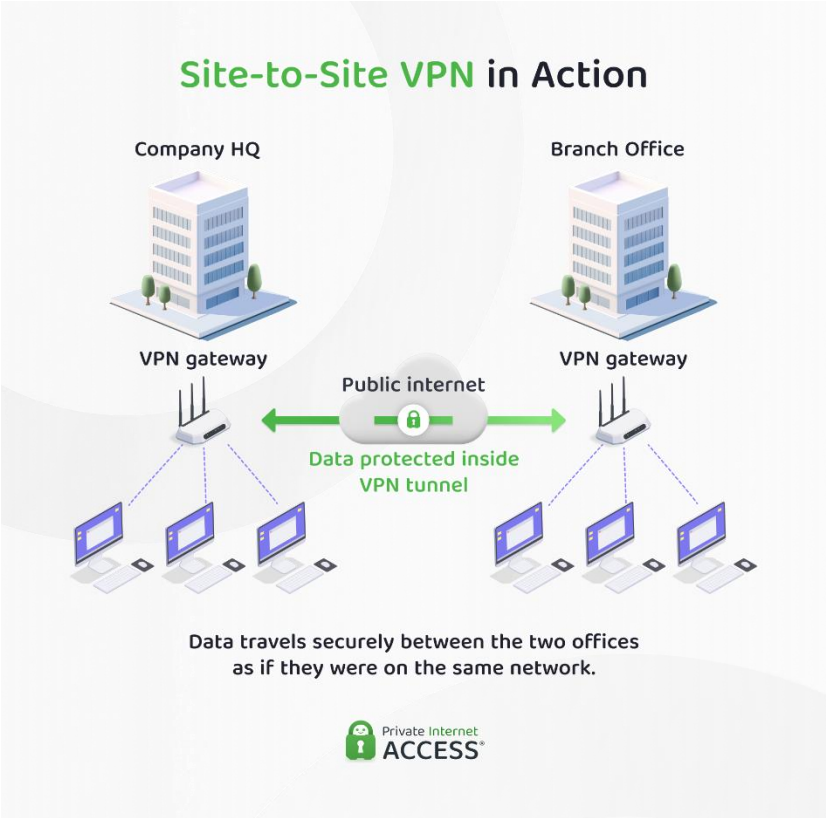
Del 1 – Vad är ett VPN?

Ett **VPN (Virtual Private Network)** skapar en **krypterad tunnel** över ett osäkert nät, oftast internet.

VPN används för att:

- Skydda data som skickas mellan användare och nätverk
- Ge fjärråtkomst till interna nätverk
- Koppla ihop kontor (site-to-site)
- Arbeta säkert hemifrån eller från publika nätverk

Förenklad bild:



Referens: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn
https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virtual-private-network-vpn.html

https://www.privateinternetaccess.com/blog/site-to-site-vpn/

Del 2 – Olika typer av VPN

2.1 Remote Access VPN även kallad P-2-S (Point to site)

- Används av **enskilda användare**
- Datorn ansluter till ett företags eller skolans nät
- Vanlig vid distansarbete

Exempel:

- Microsoft SSTP
- Cisco AnyConnect
- OpenVPN (client → server)

2.2 Site-to-Site VPN

- Kopplar ihop **två nätverk**
- Vanligt mellan kontor eller skolbyggnader

- Körs oftast alltid, utan användarinloggning

Exempel:

- IPsec mellan två brandväggar

Del 3 – IPsec (Internet Protocol Security)

3.1 Vad är IPsec?

IPsec är ett ramverk för att säkra IP-trafik och är **en av de vanligaste VPN-teknikerna i världen**.

Används ofta för:

- Site-to-site VPN
- Ibland remote access

3.2 Grundläggande begrepp

- **IKE / IKEv2** – används för nyckelutbyte
- **ESP** – krypterar trafiken
- **Tunnelläge** – vanligast i VPN

3.3 Fördelar

- Mycket säkert
- Stöd hos nästan alla tillverkare
- Standardiserat

3.4 Nackdelar

- Kan vara komplext att konfigurera
- Kan blockeras av brandväggar/NAT vid fel konfiguration

Del 4 – SSTP (Secure Socket Tunneling Protocol)

4.1 Vad är SSTP?

SSTP är ett VPN-protokoll utvecklat av **Microsoft**.

- Använder **HTTPS (TCP 443)**
- Vanligt i Windows-miljöer

4.2 Fördelar

- Fungerar nästan alltid genom brandväggar
- Enkelt i Windows-miljöer
- Bra för remote access

4.3 Nackdelar

- Proprietärt
- Begränsat stöd utanför Windows

Del 5 – Moderna och öppna VPN-lösningar

5.1 OpenVPN

- Öppen källkod
- Mycket vanligt i brandväggar och VPN-tjänster
- Körs över UDP eller TCP

Fördelar:

- Flexibelt
- Säkert
- Stöds av många leverantörer

5.2 WireGuard

- Nyare VPN-protokoll
- Mycket snabb och enkel design
- Blir allt vanligare

Fördelar:

- Hög prestanda
- Enkel konfiguration

Nackdelar:

- Färre företagsfunktioner än IPsec (än så länge)

Del 6 – Tillverkare och vanliga lösningar

Tillverkare / Lösning	Vanlig VPN-teknik
Cisco	IPsec, AnyConnect (SSL/IPsec)
Microsoft	SSTP, IKEv2
pfSense	IPsec, OpenVPN, WireGuard
Fortinet	IPsec, SSL-VPN

OpenVPN	OpenVPN
WireGuard	WireGuard

Del 7 – Jämförelse (översikt)

VPN-typ	Vanlig användning	Styrka
IPsec	Site-to-site	Standard, säkert
SSTP	Remote access	Fungerar genom brandväggar
OpenVPN	Både/både	Flexibelt
WireGuard	Både/både	Snabbt och enkelt

Del 8 – Valbar praktisk uppgift

Alternativ A – Skiss i Cisco Packet Tracer

En utmaning hade varit att skapa en Site to Site VPN koppling mellan två brandväggar i Packet Tracer. Detta kräver dock en hel del konfiguration och bör kompletteras med strukturerade laborationer.

Alternativ B – Enkel VPN med pfSense (översiktligt)

Något enklare att skapa en virtuell maskin och installera pfSense på den (eller liknande distribution) för att sedan installera en valfri VPN lösning samt om möjligt kontrollera denna med en klient.

Del 9 – Reflektionsfrågor

1. Varför används VPN istället för okrypterad trafik?
2. När är IPsec bättre än SSTP?
3. Varför blir WireGuard allt mer populärt?
4. Vilken VPN-lösning passar bäst för distansarbete i skolan?

Inlämning (förslag)

- Kort sammanfattning av VPN-typer (½ sida)
- En skiss eller Packet Tracer-fil
- Besvarade reflektionsfrågor