TERACOM MOBIL

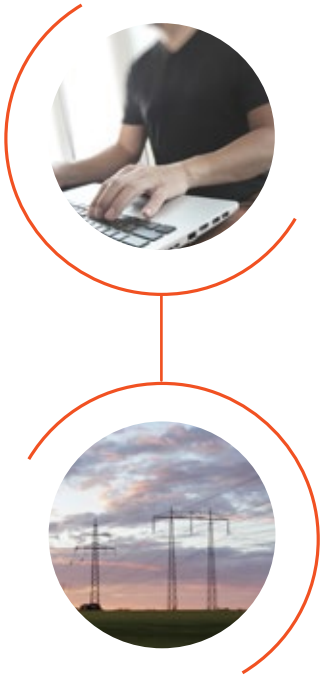
GUIDE

Din guide till en säkrare kommunikation

Internet genomsöks regelbundet i jakten på osäkra nätverk och enheter som saknar skydd för olika typer av exponering och intrång. Viktiga system kan slås ut genom attacker, fjärrstyras av obehöriga eller bli infekterade av virus. Rädslan för att ansluta lösningar direkt till internet blir därför allt större och efterfrågan på säkrare lösningar där enheterna går att fjärrstyras utan att de kan nås genom publika nätverk ökar.

Två nya regelverk

GDPR och NIS-direk-tivet trädde i kraft 2018. Två regelverk som ställer betydligt högre krav på företag och organisationer gällande IT-säkerhet och rapportering vid eventuella incidenter. Det gör att så gott som alla verksamheter måste se över sina processer kring IT-säkerhet och nu svämmar våra nyhetsflöden över med goda råd om hur man på bästa sätt ska säkerställa att kraven efterlevs.



Hur skyddar jag mig?

För att en IT-miljö ska vara ”säker”, krävs mer än bara punktinsatser – det är en fråga om att förändra hela sättet man ser på den digitala miljön. Men att försöka skapa en hel-täckande guide för denna förändringsresa skulle vara en alltför omfattande uppgift att ta sig an, och dessutom skulle den hamna ganska långt ifrån kärnan i den verksamhet som vi bedriver.

Därför har vi valt att fokusera på ett sätt, bland många, för att öka säkerheten i IT och kommunikationsnät. En metod som vi kan utan och innan och som vi har levererat till våra kunder under lång tid är privat nätverk. Den här guiden vänder sig till dig som överväger ett privat nätverk till din verksamhet, men som ännu är övertygad eller fullt ut medveten om de fördelar det medför. Här har vi samlat information om användningsområden, fördelar och vad du bör tänka på i valet av ett privat nätverk.

Vad är ett privat nätverk?

Med ett privat nätverk kan man skapa en säker förbindelse eller ”tunnel” mellan två eller flera punkter i ett icke-säkert datanätverk, för exempelvis fjärråtkomst över internet.

Isolerat nät skapar starkt skydd

Den grundläggande orsaken till att ett företag överväger ett privat nätverk är den ökade säkerhet det medför. I ett sådan nätverk upprättas nämligen ett nät som är isolerat från all annan trafik, vilket skapar ett starkt skydd mot eventuella angrepp – såsom spårnings- eller intrångsförsök.

Samordnat nätverk – oavsett var enheterna befinner sig

För företag har VPN – virtuellt privat nätverk – länge fungerat som ett säkert sätt låta anställda koppla upp sig mot sina nätverk, även då de inte fysiskt befinner sig i företagets lokaler.

VPN kan även användas då ett företag behöver koppla ihop kontorsnät (intranät) eller funktioner som är placerade på olika geografiska platser. Därigenom kan företagets nätverk på ett säkert sätt samordnas – trots att verksamheten är uppdelad på flera orter. På så sätt kan du exempelvis skapa en säker anslutning hela vägen från ditt interna företagsnätverk till uppkopplade enheter i fält. Oavsett geografisk placering.

Idag används VPN i större utsträckning för att koppla ihop affärskritisk kommunikation mellan maskiner eller maskiner till servrar (M2M-kommunikation).

Vilka är fördelarna med ett privat nätverk?

Ökad säkerhet

Genom att använda en VPN-lösning i ett publikt nätverk kan affärskritiska data separeras helt från all annan datatrafik och på så sätt skyddas från eventuella attacker utifrån.

Om förbindelsen dessutom är krypterad kan ingen avlyssna nätverket eftersom all sådan tillgång till datatrafiken i det privata nätverket kräver en krypteringsnyckel.

Koppla samman åtskilda nät

Ett VPN sammankopplar åtskilda nät som om de vore logiskt ihopkopplade – på samma sätt som om du vore ansluten till ett lokalt, fysiskt nätverk. Det gör att du, oberoende av var du befinner dig, kan koppla upp dig mot samma nät som dina kolleger – trots att du befinner utanför företagets väggar.

På samma sätt kan säkra anslutningar upprättas från ditt företagsnätverk till uppkopplade enheter i fält. Det innebär rent praktiskt att du kan förlänga ditt processnät till andra geografiska platser, oavsett var anslutningarna befinner sig. Det gör alltså att kommunikationen, och överföringen av affärskritiska data, mellan olika anläggningar säkras.

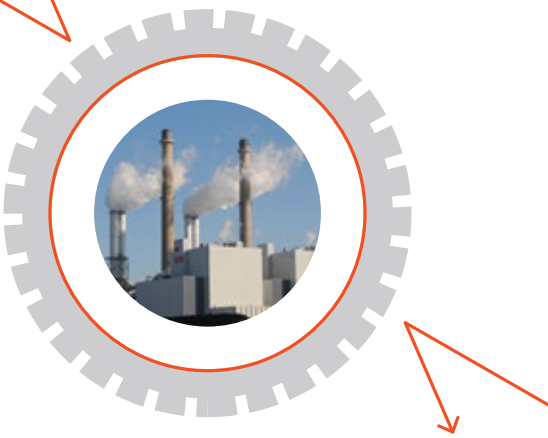
Segmentera nät – trots gemensam anslutning

Att använda VPN kan även vara ett enkelt sätt att segmentera flera olika nät, som har olika användningsområden, över en gemensam anslutning eller ett och samma öppna nätverk. Ett exempel på detta är om en verksamhet vill ansluta nät för flera olika funktioner, så kan de vara helt separerade, trots att de delar 4G-router.

Billigare och enklare

Ett VPN är dessutom betydligt billigare och enklare för företaget att använda, än att bygga och driva ett fysiskt, privat nät i egen regi.

Att tänka på när du väljer ett privat nät



Vad är syftet?

Som med alla investeringar är det viktigt att först och främst klargöra vad du vill uppnå med införandet av ett VPN. Vad är det bakomliggande behovet till att du överväger VPN som lösning? För de allra flesta är svaret: ökad säkerhet.

Vilken säkerhetsnivå krävs för din verksamhet?

Därefter bör man avväga vilken nivå av säkerhet som krävs. Somliga betraktar VPN som fullt tillräckligt för att täcka behovet av IT-säkerhet i företaget, medan andra ser det som ett av flera säkerhetslager i IT-miljön. Som med så mycket annat är IT-säkerheten även en budgetfråga, och då är VPN ett kostnadseffektivt alternativ.

Kommunikationen mellan ett företagets processystem och olika mätpunkter är ofta avgörande i samhällskritiska verksamheter, eftersom fel information kan leda till allvarliga konsekvenser. I dessa fall av särskilt känslig information bör man välja ett VPN som stödjer kryptering. Säkerställ även att de brandväggar som används ger stöd för den VPN-metod du väljer.

Hur ska åtkomst autentiseras?

För att säkerheten i nätverket ska kunna tryggas är åtkomsten till ett VPN begränsat till ett antal användare. På så sätt stärks skyddet för intrång från obehöriga. Det finns olika sätt att autentisera användare – att säkerställa deras identitet innan de får åtkomst till nätverket. Därför bör du i ett tidigt skede även tänka på vilken typ av autentisering som ska användas för ditt VPN. Om du inte själv vill hantera detta bör du välja en leverantör som kan erbjuda autentisering och tilldelning av IP-adresser.

Privat nätverk från Teracom Mobil

Skalbart och säkert

Mobilt VPN från Teracom Mobil öppnar möjligheter för bättre och säkrare kommunikation genom att enkelt och kostnads-effektivt koppla ihop mindre enheter av bolaget, lokalt eller spridda över landet, med företagets VPN.

Tjänsten är skalbar och flexibel, från några enstaka anslutningar till flera tusen och levereras över Teracom Mobils nät med valfria abonnemang, vilket ger en trygg och stabil uppkoppling.

Du bestämmer själv vilka enheter som ska få ansluta till nätet och trafiken är logiskt separerad från all annan trafik för maximal säkerhet.

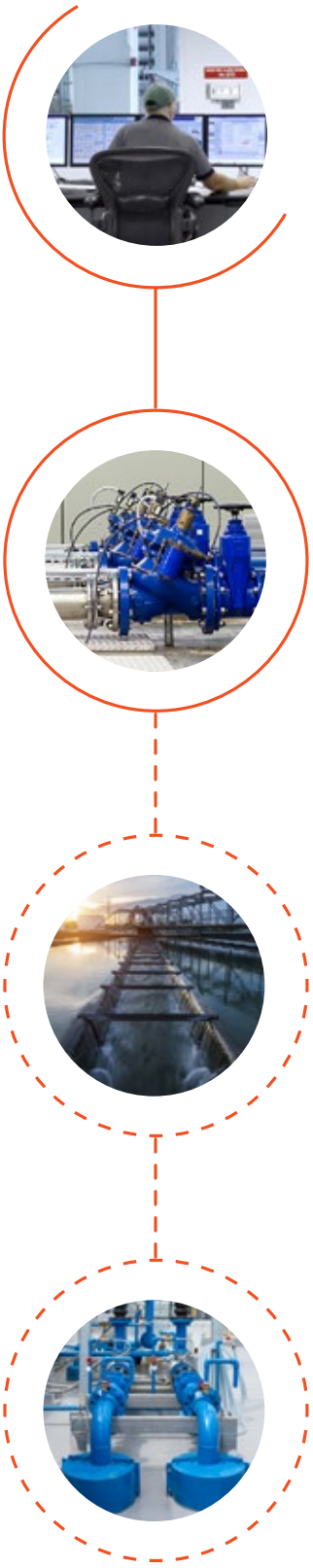
Genom att tjänsten inte är exponerad mot internet skyddas även datauppkopplingarna mot till exempel överbelastningsattacker.

Tekniken bakom tjänsten

Du som kund tilldelas ett eget APN (Access Point Name) dit bara dina egna abonnemang får ansluta. Autentisering kan ske både via SIM-kort och via företagets egen Radius-server. Utöver autentisering kan företagets Radius-server hantera annan konfiguration av routrarna, som till exempel tilldelning av IP-adresser.

Trafiken är separerad i nätet med hjälp av IP/MPLS genom hela Teracom Mobils nätinfrastruktur och via en avlämningsrouter varifrån kopplas företaget in, antingen via en fast anslutning separerad från internet, eller via en VPN-tunnel (IPSsec) över internet.

I grundpaketet ingår anslutning till en av våra serverhallar men för extra tillförlitlighet kan en ytterligare anslutning ske via två avlämningsroutrar i olika serverhallar (redundant transmission). Ofta väljer våra kunder att kombinera en fast anslutning och en IPSec-tunnel för att på ett kostnadseffektivt sätt uppnå en redundant anslutning mellan näten.



Managerat Mobilt VPN

För kunder som inte själva önskar hantera autentisering erbjuder vi en tilläggstjänst för Managerat Mobilt VPN, så att du snabbt och enkelt kan komma igång, där allt från konfiguration av hårdvara till övervakning och drift av uppkopplingen ingår.

Vi ser till att autentisering och tilldelning av IP-adresser sker korrekt och säkert, utan att du behöver investera i en egen RADIUS-infrastruktur. Allt du behöver göra är att koppla upp ditt företags nät till oss via en fast anslutning eller en VPN-tunnel och du är igång.

Vi hoppas att du har haft nytta av den här guiden och att den hjälpt dig att få en mer heltäckande bild av vad ett VPN kan bidra med till just din verksamhet.

Har du frågor och funderingar kring att välja rätt uppkoppling?

Teracom Mobil hjälper företag i hela Sverige att välja rätt uppkoppling. Våra företagskunder spänner från företag med anläggningar i hela landet till mindre kommuner. Kontakta oss för vidare rådgivning.

TERACOM
MOBIL