Engineer

VPN

🖧 et logisk adskilt netværk over fælles infrastruktur

Hvad det er

En VPN, kort for virtuelt privat netværk, er et sæt tunneler eller mærkede stier, der lader en lukket gruppe maskiner nå hinanden på deres egne adresser og ruter, uanset hvilke net pakkerne krydser undervejs. IETF's terminologi ser det som et spørgsmål om adskillelse frem for hemmeligholdelse: gruppen holdes adskilt fra andre brugere, og kryptering nævnes som en mulig tilføjelse, der ligger uden for arbejdsgruppernes mandat. I hverdagen dominerer to former. En site-to-site-VPN forbinder hele netværk, for eksempel et kontor og et cloudprojekt, gennem en gateway i hver ende. En fjernadgangs-VPN, på engelsk remote access, forbinder én bærbar eller én telefon med et netværk, den befinder sig langt fra.

Meget forskellige teknologier deler navnet. IPsec beskytter IP-pakker inde i netværksstakken på en vært eller en sikkerhedsgateway og bruger typisk IKEv2 til at forhandle sine nøgler; det er den protokol, de fleste firewalls, routere og administrerede cloudgateways taler. WireGuard er en nyere tunnel, der viser sig som et almindeligt netværksinterface, kører over UDP, kender hver peer på en offentlig nøgle og bevidst tilbyder ét fast sæt krypteringsalgoritmer i stedet for en menu at forhandle om. OpenVPN kører som en proces i brugerrummet og etablerer sine nøgler med TLS. Operatørernes VPN'er, bygget på BGP og MPLS, holder kunderne adskilt i en udbyders backbone og giver ifølge deres egen specifikation ingen kryptografisk fortrolighed overhovedet. Når en kontrakt, et diagram eller en firewall-leverandør siger VPN, betaler det sig at spørge, hvilken af dem der menes.

Brug begrebet i en beslutning

Brug »Hvad er en VPN?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Wi-Fi, firewalls og fjernadgang sat op, så medarbejdere kan arbejde hvor som helst, og kun de rette kommer ind.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har administreret 30 Ubuntu Linux VPS-instanser — 30 Linux-servere driftet, med en plan for gendannelse

Har administreret 30 Ubuntu Linux VPS-instanser Kontakt os →

Hvorfor det betyder noget

Den beslutning, en VPN som regel afgør, er, hvordan to steder, der skal tale sammen, kan gøre det uden at lægge tjenesten imellem dem ud på det åbne internet. En database, som kun en pipeline i en anden cloud læser, et internt adminpanel, et backupmål: hver af dem kan lytte offentligt bag et login eller lytte på en privat adresse, som kun tunnelen gør tilgængelig. Den anden mulighed skærer det, en scanner kan finde, ned til én port på gatewayen, og til forbindelser mellem lokationer er det stadig det enkle og velkendte svar.

WireGuard eller IPsec er det næste spørgsmål, og som regel afgør den anden ende det. Er den ende en firewall-appliance, en cloududbyders administrerede gateway eller en partners netværksteam, er IPsec ofte det eneste, der er at vælge imellem, og interoperabilitet vejer tungere end elegance. Er begge ender Linux-maskiner, man selv har styr på, er WireGuard hurtigere at sætte op og lettere at gennemskue: én kort konfigurationsfil pr. side, én offentlig nøgle pr. peer og en liste over de adresser, hver peer må sende fra. Designartiklen opgør Linux-implementeringen til under 4.000 linjer kode, lille nok til at blive gennemgået linje for linje, mens en IPsec-opsætning på Linux parrer kernens pakketransformation med en separat dæmon til nøgleudveksling og en længere liste af valg, som begge sider skal være enige om.

Driftsomkostningen er sjældent softwaren, som følger med Linux og med de fleste firewalls. Omkostningen er opmærksomhed. Tunneler falder om natten, nøglefornyelsen går i stykker timer efter, at nogen har ændret en indstilling i den anden ende, og det eneste symptom er stilhed: pakker går ind, og intet kommer tilbage. En tunnel fortjener samme behandling som enhver anden produktionstjeneste, med sit eget sundhedstjek, sin egen alarm og en skriftlig note om, hvem der ejer hver ende.

En VPN er også det forkerte værktøj nogle steder. Giver man hver fjernmedarbejder en fuld tunnel ind i kontorets netværk, får personen adgang til et helt subnet, når behovet var én applikation, og når forbindelsen først er oppe, har alt på det subnet en tendens til at stole på dem. Adgang pr. applikation, hvor hver forespørgsel autentificeres for sig, og som oftest sælges under navnet zero trust, passer bedre, når brugerne er mennesker og målene er webapplikationer.

Forbrugerapps, der reklamerer med VPN for privatlivets skyld, er en tredje ting igen: de flytter tilliden fra internetudbyderen til VPN-firmaet og kan skjule den oprindelige afsender-IP-adresse for de websteder, trafikken sendes til, men garanterer ikke i sig selv anonymitet.

Sådan ser det ud i praksis

Fra 2022 til 2024 kørte sikker trafik mellem Google Cloud og on-premises Linux-systemer over otte WireGuard- og IPsec-tunneler, administreret og fejlfundet som ét sæt. De havde været skrøbelige og langsomme at diagnosticere, og en død tunnel kunne kappe kommunikationen mellem miljøerne. Konfigurationen blev standardiseret, så ingen tunnel forblev et særtilfælde, tunnelernes tilstand blev overvåget, og de tilbagevendende problemer med routing og nøgleudveksling blev rettet ved roden i stedet for at blive ryddet væk med en genstart. Derefter kørte alle otte pålideligt, og de tilbagevendende forbindelsesproblemer holdt op.

I de samme år havde en organisation brug for data fra et fjernt data warehouse, der lå bag en IPsec-VPN. For seks ETL/ELT-pipelines, der fodrede Google BigQuery, var tunnelen det første led i kæden: sikre forbindelser til den beskyttede server blev etableret, så hentningen kunne køre uden opsyn. Planlagte job hentede derefter komprimerede arkiver med Parquet-, CSV- og .bak-filer, gendannede dem, lagde dem i staging-skemaer i MSSQL og PostgreSQL og indlæste resultatet i BigQuery. Med alle led automatiseret tog hele kæden, fra download til BigQuery, under 20 minutter mod mindst 3 timers manuelt arbejde før, og dataene blev synkroniseret dagligt i stedet for ugentligt. VPN'en er den mindst synlige del af det resultat og den del, alt andet hviler på: en pipeline, der ikke kan nå sin kilde, stopper ved første trin, uanset hvor god SQL'en bag den er.

Hvor det går galt

Store pakker forsvinder, mens små kommer igennem. Hver tunnel lægger sine egne headere til, så den største pakke, der kan være inden i, er mindre end det, stien udenfor tillader. En WireGuard-datapakke lægger 32 byte fast overhead til før de ydre UDP- og IP-headere, omkring 60 byte i alt over IPv4 og 80 over IPv6, ud over eventuel padding af pakken. Når tunnelens MTU er sat for højt, og stien smider de ICMP-beskeder væk, der skulle melde det, virker ping og et SSH-login, mens filoverførsler og TLS-handshakes hænger. Test med en pakke i fuld størrelse, der ikke må fragmenteres, og sænk derefter interfacets MTU eller begræns TCP's segmentstørrelse, så pakkerne kan komme igennem.

```
# Hvornår hver WireGuard-peer sidst fuldførte et handshake, som Unix-tid
wg show wg0 latest-handshakes
# En pakke på 1.420 byte, der ikke må fragmenteres undervejs
ping -M do -s 1392 -c 3 10.0.0.2
# Hvilket interface og hvilken rute kernen vælger til en fjern vært
ip route get 10.20.0.5
```

To lokationer har valgt de samme adresser. Private intervaller som 10.0.0.0/8 og 192.168.0.0/16 bliver genbrugt overalt, og forbinder man to netværk, der begge bruger 10.0.0.0/24, kan en router ikke afgøre, hvilken side en pakke skal til. Planlæg intervallerne før den første tunnel, eller accepter adresseoversættelse i den ene ende, som gør hver loglinje og hver firewallregel derefter mere indviklet.

Tunnelen er oppe, og ruten er forkert. En peer kan vise et frisk handshake, mens trafikken stadig forlader maskinen ad standardruten, fordi ruten til det fjerne subnet mangler, eller fordi WireGuards liste over tilladte adresser for den peer udelader det. I IPsec er modstykket traffic selectors, der er forskellige i de to ender. IKEv2 snævrer dem enten ind til overlappet eller afviser dem med en TS_UNACCEPTABLE-meddelelse, så en tunnel kan komme op og bære mindre, end nogen af siderne havde tænkt sig.

Nøglefornyelsen fejler længe efter ændringen. Begge protokoller udskifter de aktive sessionsnøgler over tid, så en uoverensstemmelse, der er indført i den ene ende, for eksempel et redigeret forslag eller en roteret nøgle, først kan vise sig, når de aktuelle nøgler udskiftes. WireGuard starter en ny session cirka hvert andet minut, mens der går trafik. IPsec-levetider er lokal politik i hver ende og behøver ikke at være ens. For WireGuard skal alderen på det seneste vellykkede handshake vurderes sammen med den forventede trafik eller kontrolforespørgsler: et gammelt handshake fra en inaktiv peer er ikke i sig selv tegn på et svigt. Slå IKEv2's livstegnstjek til, ofte kaldet dead peer detection, så en gateway opdager en tavs peer i stedet for at sende ud i et sort hul.

Forbundet bliver til betroet. I mange fjernadgangsopsætninger bliver en bærbar på VPN'en behandlet, som om den stod på kontoret, så ét stjålet login når alt på det subnet. Filtrér på gatewayen, hvad hver VPN-klient kan nå, behold autentificeringen på tjenesterne bag den, og beslut bevidst, om navneopslag og internettrafik går gennem tunnelen eller uden om den.

Læs mere

- RFC 4026, section 3.10 — IETF's generelle definition af en VPN og bemærkningen om, at kryptering ligger uden for arbejdsgruppernes mandat.
- WireGuard: Next Generation Kernel Network Tunnel — designartiklen: cryptokey routing, handshaket og de timere, der styrer nøglefornyelsen.
- RFC 4301 — sikkerhedsarkitekturen for IP, som enhver IPsec-implementering følger.
- RFC 7296 — IKEv2, herunder indsnævring af traffic selectors, levetider som lokal politik og livstegnstjekket.
- RFC 4364 — BGP/MPLS IP VPNs, operatørvarianten, med overlappende adresserum og uden kryptografisk fortrolighed.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er en VPN?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/vpn/