Engineer

VPN

🖧 et logisk atskilt nettverk over delt infrastruktur

Hva det er

VPN, i flertall VPN-er og kort for *virtual private network*, er et sett tunneler eller merkede stier som lar en lukket gruppe maskiner nå hverandre på egne adresser og ruter, uansett hvilke nettverk datapakkene krysser underveis. Terminologien fra IETF behandler det som et spørsmål om atskillelse heller enn hemmelighold: gruppen holdes adskilt fra andre brukere, og kryptering nevnes som et mulig tillegg som ligger utenfor arbeidsgruppenes mandat. I daglig bruk dominerer to former. Et VPN mellom lokasjoner (*site-to-site*) knytter sammen hele nettverk, f.eks. et kontor og et skyprosjekt, gjennom en gateway i hver ende. Et VPN for fjerntilgang (*remote access*) knytter én bærbar PC eller telefon til et nettverk den er borte fra.

Svært ulike teknologier deler navnet. IPsec beskytter IP-pakker inne i nettverksstakken til en vert eller en sikkerhetsgateway og bruker vanligvis IKEv2 til å forhandle nøklene sine; det er dette de fleste brannmurer, rutere og administrerte gatewayer i skyen snakker. WireGuard er en nyere tunnel som framstår som et vanlig nettverksgrensesnitt, går over UDP, identifiserer hver motpart med en offentlig nøkkel og bevisst tilbyr ett fast sett chiffer i stedet for en meny å forhandle om. OpenVPN kjører som en prosess i brukerrommet og setter opp nøklene sine med TLS. Operatør-VPN bygd på BGP og MPLS holder kunder adskilt inne i ryggradsnettet til en leverandør og gir, etter sin egen spesifikasjon, ingen kryptografisk konfidensialitet i det hele tatt. Når en kontrakt, et diagram eller en leverandør av brannmurer sier VPN, lønner det seg å spørre hvilken av disse som er ment.

Bruk begrepet i en beslutning

Bruk «Hva er VPN?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Wi-Fi, brannmurer og fjerntilgang satt opp slik at de ansatte kan jobbe hvor som helst, og bare de rette personene slipper inn.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Administrerte 30 Ubuntu Linux-VPS-instanser — 30 Linux-servere administrert, med gjenoppretting planlagt på forhånd

Administrerte 30 Ubuntu Linux-VPS-instanser Ta kontakt →

Hvorfor det er viktig

Beslutningen et VPN som regel avgjør, er hvordan to steder som må snakke sammen, kan gjøre det uten å legge tjenesten mellom dem ut på det åpne internett. En database som bare leses av en pipeline i en annen sky, et internt administrasjonspanel, et mål for sikkerhetskopier: hver av dem kan lytte offentlig bak en innlogging, eller lytte på en privat adresse som bare tunnelen gjør tilgjengelig. Det andre valget krymper det en skanner kan finne, til én nettverksport på gatewayen, og for forbindelser mellom lokasjoner er det fortsatt det enkle, godt forståtte svaret.

WireGuard eller IPsec er neste spørsmål, og den andre enden avgjør det som regel. Er den enden en ferdig brannmur fra en leverandør, en administrert gateway hos en skyleverandør eller nettverksteamet hos en partner, er IPsec ofte det eneste som tilbys, og samvirke veier tyngre enn eleganse. Er begge ender maskiner med Linux under din egen kontroll, er WireGuard raskere å sette opp og lettere å resonnere om: én kort konfigurasjonsfil per side, én offentlig nøkkel per motpart og en liste over adressene hver motpart får sende fra. Designartikkelen anslår implementasjonen for Linux til under 4 000 kodelinjer, lite nok til å revideres, mens et IPsec-oppsett på Linux kombinerer pakketransformasjonen i systemkjernen med en egen daemon for nøkkelutveksling og en lengre liste med valg å bli enige om.

Driftskostnaden er sjelden programvaren, som følger med Linux og med de fleste brannmurer. Kostnaden er oppmerksomhet. Tunneler faller ut om natten, ny nøkkelforhandling svikter timer etter at noen endret en innstilling på den andre siden, og det eneste symptomet er stillhet: pakker går inn, og ingenting kommer tilbake. En tunnel fortjener samme behandling som enhver annen tjeneste i produksjon, med egen helsesjekk, eget driftsvarsel og et skriftlig notat om hvem som eier hver ende.

Et VPN er også feil verktøy noen steder. Å gi hver ansatt som jobber utenfor kontoret, en full tunnel inn i kontornettet gir rekkevidde til et helt subnett når personen trengte ett program, og når forbindelsen først er oppe, har alt på det subnettet en tendens til å stole på vedkommende. Tilgang per applikasjon, der hver forespørsel autentiseres for seg og som oftest selges som nulltillit (*zero*

trust), passer bedre når brukerne er personer og målene er webapplikasjoner. Forbrukerappene som reklamerer med VPN for personvernets skyld, er enda en tredje ting: de flytter tilliten fra internettleverandøren til VPN-selskapet og kan skjule den opprinnelige kilde-IP-adressen for nettstedene trafikken sendes til, men garanterer ikke anonymitet i seg selv.

Slik ser det ut i praksis

I årene 2022–2024 gikk sikker trafikk mellom Google Cloud og lokale Linux-systemer over åtte WireGuard- og IPsec-tunneler, forvaltet og feilsøkt samlet. De hadde vært skjøre og trege å diagnostisere, og en død tunnel kunne bryte kommunikasjonen mellom miljøene. Konfigurasjonen ble standardisert slik at ingen tunnel lenger var et spesialtilfelle, helsen deres ble overvåket, og de gjentakende problemene med ruting og nøkkelutveksling ble løst ved roten i stedet for å bli ryddet bort med en omstart. Deretter kjørte alle åtte pålitelig, og de gjentakende tilkoblingshendelsene opphørte.

I de samme årene trengte en organisasjon data fra et eksternt datavarehus som lå bak et IPsec-VPN. For seks ETL/ELT-pipelines som matet Google BigQuery var tunnelen det første leddet i kjeden: sikre tilkoblinger til den beskyttede serveren ble satt opp slik at innhentingen kunne kjøre uten tilsyn. Planlagte jobber lastet deretter ned komprimerte arkiver med Parquet-, CSV- og .bak-filer, gjenopprettet og mellomlagret dem i MSSQL og PostgreSQL, og lastet resultatet inn i BigQuery. Med tunnelen oppe uten tilsyn gikk hele kjeden på under 20 minutter, der minst tre timer med manuelt arbeid hadde gått med før, og dataene ble hentet daglig i stedet for ukentlig. VPN-et er den minst synlige delen av det resultatet, og den delen alt annet hviler på: en pipeline som ikke når kilden sin, stopper på første trinn, uansett hvor god SQL-en bak den er.

Hvor det går galt

Store pakker forsvinner mens små kommer fram. Hver tunnel legger til headere, så den største pakken som får plass inni, er mindre enn stien utenfor tillater. En datamelding i WireGuard legger til 32 byte fast overhead før de ytre UDP- og IP-headerne, rundt 60 byte til sammen over IPv4 og 80 over IPv6, i tillegg til eventuell utfylling av pakken. Er MTU-en for tunnelen satt for høyt, og stien kaster ICMP-meldingene som skulle ha meldt fra om det, virker ping og en SSH-innlogging mens filoverføringer og TLS-håndtrykk henger. Test med en pakke i full størrelse som forbyr fragmentering, og senk så MTU-en på grensesnittet eller klem TCP-segmentstørrelsen ned til den passer.

```
# Når hver WireGuard-motpart sist fullførte et håndtrykk, som Unix-tid
wg show wg0 latest-handshakes
# En pakke på 1 420 byte som ikke får fragmenteres underveis
ping -M do -s 1392 -c 3 10.0.0.2
# Hvilket grensesnitt og hvilken rute kjernen velger for en fjern vert
ip route get 10.20.0.5
```

To lokasjoner valgte de samme adressene. Private adresseområder som 10.0.0.0/8 og 192.168.0.0/16 brukes om igjen overalt, og når to nettverk som begge bruker 10.0.0.0/24, kobles sammen, har en ruter ingen måte å avgjøre hvilken side en pakke skal til. Planlegg adresseområdene før den første tunnelen, eller godta adresseoversetting i den ene enden, noe som kompliserer hver logglinje og hver brannmurregel etter den.

Tunnelen er oppe, og ruten er feil. En motpart kan vise et ferskt håndtrykk mens trafikken fortsatt forlater verten gjennom standardruten, fordi ruten for det fjerne subnettet mangler, eller fordi listen over tillatte adresser som WireGuard holder for den motparten, utelater det. I IPsec er motstykket trafikkselektorer som er ulike i de to endene. IKEv2 snevrer dem enten inn til overlappen eller avviser dem med varselet TS_UNACCEPTABLE, så en tunnel kan komme opp og bære mindre enn noen av sidene hadde tenkt.

Ny nøkkelforhandling svikter lenge etter endringen. Begge protokollene bytter aktive øktnøkler over tid, så et avvik som innføres i den ene enden, f.eks. et redigert forslag eller en rotert nøkkel, kan vise seg først når de gjeldende nøklene byttes. WireGuard starter en ny økt omtrent annethvert minutt så lenge det går trafikk. Levetidene i IPsec er lokal policy i hver ende og trenger ikke å stemme overens. For WireGuard må alderen til det siste vellykkede håndtrykket tolkes sammen med forventet trafikk eller aktive helsesjekker: et gammelt håndtrykk fra en inaktiv motpart fastslår ikke alene at noe har sviktet. Slå på livssjekken i IKEv2, ofte kalt *dead peer detection*, så en gateway merker en taus motpart i stedet for å sende inn i et svart hull.

Tilkoblet blir betrodd. I mange oppsett for fjerntilgang behandles en bærbar PC på VPN-et som om den sto på kontoret, slik at stjålne påloggingsopplysninger gir tilgang til alt på det subnettet. Filtrer på gatewayen hva hver VPN-klient kan nå, behold autentiseringen på tjenestene bak den, og bestem bevisst om navneoppslag og internettrafikk skal gå gjennom tunnelen eller utenom.

Les mer

- RFC 4026, section 3.10 — den generelle definisjonen av VPN fra IETF, og merknaden om at kryptering ligger utenfor mandatet til arbeidsgruppene.
- WireGuard: Next Generation Kernel Network Tunnel — designartikkelen: kryptonøkkelruting, håndtrykket og tidtakerne bak ny nøkkelforhandling.
- RFC 4301 — sikkerhetsarkitekturen for IP som hver implementasjon av IPsec følger.
- RFC 7296 — IKEv2, med innsnevring av trafikkselektorer, levetider som lokal policy og livssjekken.
- RFC 4364 — BGP/MPLS IP VPN, operatørvarianten, med overlappende adresserom og uten kryptografisk konfidensialitet.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er VPN?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/vpn/