Engineer

VPN

ett logiskt avskilt nät över delad infrastruktur

Vad det är

Ett VPN, kort för virtuellt privat nätverk, är en uppsättning tunnlar eller märkta vägar som låter en sluten grupp maskiner nå varandra med sina egna adresser och rutter, vilka nät paketen än passerar på vägen. Terminologin från IETF ser det som en fråga om åtskillnad snarare än om sekretess: gruppen hålls isär från andra användare, och kryptering nämns som ett möjligt tillägg som ligger utanför arbetsgruppernas område. I vardagen dominerar två former. Ett VPN mellan platser (site-to-site) knyter ihop hela nät, t.ex. ett kontor och ett molnprojekt, genom en gateway i varje ände. Ett VPN för fjärråtkomst knyter en bärbar dator eller en telefon till ett nät som den befinner sig långt ifrån.

Mycket olika tekniker delar namnet. IPsec skyddar IP-paket inne i nätverksstacken på en värddator eller en säkerhetsgateway och använder vanligen IKEv2 för att förhandla fram sina nycklar. Det är vad de flesta brandväggar, routrar och hanterade gatewayer i molnet talar. WireGuard är en nyare tunnel som syns som ett vanligt nätverksgränssnitt, går över UDP, identifierar varje motpart med en publik nyckel och medvetet erbjuder en enda fast uppsättning chiffer i stället för en meny att förhandla om. OpenVPN körs som en process i användarrymden och sätter upp sina nycklar med TLS. Operatörernas VPN, byggda på BGP och MPLS, håller kunder isär inne i en leverantörs stamnät och ger enligt sin egen specifikation ingen kryptografisk sekretess alls. När ett avtal, en skiss eller en leverantör av brandväggar säger VPN lönar det sig att fråga vilket av dessa som avses.

Använd begreppet i ett beslut

Använd ”Vad är ett VPN?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Wi-Fi, brandväggar och fjärråtkomst uppsatta så att personalen kan arbeta varifrån som helst och bara rätt personer kommer in.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Förvaltade 30 VPS-instanser med Ubuntu Linux — 30 förvaltade Linux-servrar, med en plan för återställning

Förvaltade 30 VPS-instanser med Ubuntu Linux Hör av er →

Varför det spelar roll

Beslutet som ett VPN oftast avgör är hur två platser som behöver prata med varandra kan göra det utan att tjänsten mellan dem ligger öppet på internet. En databas som bara en datapipeline i ett annat moln läser, en intern adminpanel, ett mål för säkerhetskopior: var och en kan lyssna publikt bakom en inloggning, eller lyssna på en privat adress som bara tunneln gör nåbar. Det andra alternativet krymper det som en skanner kan hitta till en enda nätverksport på en gateway, och för förbindelser mellan platser är det fortfarande det enkla och välkända svaret.

WireGuard eller IPsec är nästa fråga, och den bortre änden avgör den oftast. Om den änden är en brandvägg i form av en apparat, en hanterad gateway hos en molnleverantör eller nätverksteamet hos en partner är IPsec ofta det enda som erbjuds, och samverkan väger tyngre än elegans. Om båda ändarna är Linux-maskiner som ni själva styr är WireGuard snabbare att sätta upp och lättare att resonera kring: en kort konfigurationsfil per sida, en publik nyckel per motpart och en lista över de adresser som varje motpart får skicka från. Designartikeln anger att implementationen för Linux är under 4 000 rader kod, liten nog att granska, medan en IPsec-uppsättning på Linux parar kärnans pakettransform med en separat daemon för nyckelutbyte och en längre lista med alternativ att komma överens om.

Driftkostnaden är sällan programvaran, som följer med Linux och med de flesta brandväggar. Kostnaden är uppmärksamhet. Tunnlar går ned på natten, nyckelbytet slutar fungera timmar efter att någon ändrade en inställning i den bortre änden, och det enda symtomet är tystnad: paket går in och ingenting kommer tillbaka. En tunnel förtjänar samma behandling som vilken annan produktionstjänst som helst, med en egen hälsokontroll, ett eget larm och en nedskriven notering om vem som äger varje ände.

Ett VPN är också fel verktyg på vissa ställen. Att ge varje anställd på distans en full tunnel in i kontorsnätet ger åtkomst till ett helt subnät när personen behövde en enda applikation, och väl ansluten blir personen gärna betrodd av allt på det subnätet. Åtkomst per applikation, där varje begäran autentiseras för sig och som oftast säljs under namnet zero trust, passar bättre när användarna är

människor och målen är webbapplikationer. Konsumentapparna som marknadsför ett VPN för integritetens skull är något tredje: de flyttar förtroendet från internetleverantören till VPN-företaget och kan dölja den ursprungliga käll-IP-adressen för mottagande webbplatser, men garanterar inte anonymitet i sig.

Så ser det ut i praktiken

Mellan 2022 och 2024 gick säker trafik mellan Google Cloud och lokalt driftade Linux-system över åtta tunnlar med WireGuard och IPsec, förvaltade och felsökta som en helhet. De hade varit bräckliga och långsamma att diagnostisera, och en död tunnel kunde bryta kommunikationen mellan miljöerna. Konfigurationen standardiserades så att ingen tunnel förblev ett specialfall, tunnlarnas tillstånd övervakades, och de återkommande problemen med routning och nyckelutbyte åtgärdades vid roten i stället för att rensas bort med en omstart. Därefter gick alla åtta tillförlitligt, och de återkommande anslutningsincidenterna upphörde.

Under samma år behövde en organisation data från ett fjärrbeläget analysdatalager som låg bakom ett IPsec-VPN. För sex ETL/ELT-pipelines som matade Google BigQuery var tunneln den första länken i kedjan: säkra anslutningar till den skyddade servern sattes upp så att hämtningen kunde köras utan tillsyn. Schemalagda jobb laddade sedan ned komprimerade arkiv med Parquet-, CSV- och .bak-filer, återställde och mellanlagrade dem i MSSQL och PostgreSQL och läste in resultatet i BigQuery. Manuellt arbete på minst tre timmar krympte till under 20 minuter för hela flödet, och synkroniseringen av data gick från veckovis till daglig. VPN:et är den minst synliga delen av det resultatet och den del som allt annat vilar på: en datapipeline som inte når sin källa stannar vid första steget, hur bra SQL-koden bakom den än är.

Var det går fel

Stora paket försvinner medan små kommer fram. Varje tunnel lägger till huvuden, så det största paket som får plats inuti är mindre än vad vägen utanför tillåter. Ett datameddelande i WireGuard lägger till 32 byte fast overhead före de yttre UDP- och IP-huvudena, totalt ungefär 60 byte över IPv4 och 80 över IPv6, utöver eventuell utfyllnad av paketet. När tunnelns MTU är satt för högt och vägen kastar de ICMP-meddelanden som skulle ha rapporterat det fungerar ping och en SSH-inloggning, medan filöverföringar och TLS-handskakningar hänger sig. Testa med ett paket i full storlek som förbjuder fragmentering, och sänk sedan gränssnittets MTU eller begränsa storleken på TCP-segmenten så att de får plats.

```
# When each WireGuard peer last completed a handshake, as Unix time
wg show wg0 latest-handshakes
# A 1,420-byte packet that may not be fragmented on the way
ping -M do -s 1392 -c 3 10.0.0.2
# Which interface and route the kernel picks for a remote host
ip route get 10.20.0.5
```

Två platser valde samma adresser. Privata intervall som 10.0.0.0/8 och 192.168.0.0/16 återanvänds överallt, och när två nät som båda använder 10.0.0.0/24 knyts ihop har en router inget sätt att avgöra vilken sida ett paket är avsett för. Planera intervallen före den första tunneln, eller acceptera adressöversättning i ena änden, vilket komplicerar varje loggrad och varje brandväggsregel efter den.

Tunneln är uppe och rutten är fel. En motpart kan visa en färsk handskakning medan trafiken ändå lämnar via standardrutten, eftersom rutten för det bortre subnätet saknas eller eftersom listan över tillåtna adresser för den motparten i WireGuard utelämnar det. I IPsec är motsvarigheten trafikväljare (traffic selectors) som skiljer sig mellan de två ändarna. IKEv2 smalnar antingen av dem till det som överlappar eller avvisar dem med notifieringen TS_UNACCEPTABLE, så en tunnel kan komma upp och bära mindre än någon av sidorna avsåg.

Nyckelbytet slutar fungera långt efter ändringen. Båda protokollen byter aktiva sessionsnycklar över tid, så en avvikelse som införs i ena änden, t.ex. ett redigerat förslag eller en roterad nyckel, kan märkas först när de aktuella nycklarna byts ut. WireGuard startar en ny session ungefär varannan minut medan trafik flödar. Livslängderna i IPsec är lokal policy i varje ände och behöver inte stämma överens. För WireGuard ska åldern på den senaste lyckade handskakningen tolkas tillsammans med förväntad trafik eller hälsokontroller: en gammal handskakning från en inaktiv motpart visar inte i sig att något har fallerat. Slå på livskontrollen i IKEv2, ofta kallad dead peer detection, så att en gateway märker en tyst motpart i stället för att skicka in i ett svart hål.

Ansluten blir betrodd. I många uppsättningar för fjärråtkomst behandlas en bärbar dator på VPN:et som om den satt på kontoret, så en enda stulen inloggningsuppgift når allt på det subnätet. Filtrera vad varje VPN-klient kan nå vid gatewayen, behåll autentiseringen på tjänsterna bakom den, och bestäm medvetet om namnuppslag och internettrafik går genom tunneln eller runt den.

Läs mer

- RFC 4026, section 3.10 — den generella definitionen av ett VPN från IETF, och noteringen om att kryptering ligger utanför arbetsgruppernas uppdrag.
- WireGuard: Next Generation Kernel Network Tunnel — designartikeln: routning via kryptonycklar, handskakningen och timrarna bakom nyckelbytet.
- RFC 4301 — säkerhetsarkitekturen för IP som varje implementation av IPsec följer.
- RFC 7296 — IKEv2, inklusive avsmalning av trafikväljare, livslängder som lokal policy och livskontrollen.
- RFC 4364 — BGP/MPLS IP VPNs, operatörernas sort, med överlappande adressrymder och ingen kryptografisk sekretess.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är ett VPN?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/vpn/