Engineer

Tor

ett nätverk som leder trafik via frivilliga reläer

Vad det är

Med Tor får den som avlyssnar en förbindelse inte veta vem som talar med vem. Varje anslutning skickas genom en kedja av maskiner, och ingen av dem känner till både var trafiken började och var den slutar. Kedjan väljs av klienten, ett program som heter tor och körs på läsarens egen dator, och den är oftast tre reläer lång: en vakt (guard) som klienten återanvänder som sin väg in, ett mellanrelä och ett utgångsrelä (exit) som öppnar den sista anslutningen till målet. Klienten bygger kretsen ett steg i taget och kommer överens om en separat nyckel med varje relä. Sedan lindar den in varje bit data i ett krypteringslager per steg. Varje relä skalar av sitt eget lager och får bara veta vilken granne som kom före och vilken som kommer efter. De kapslade lagren är löken i namnet på designartikeln, The Second-Generation Onion Router.
I vardagligt tal är reläerna tillsammans Tor-nätverket, tor med gemener är programmet och Tor Browser är webbläsaren som är paketerad för att använda det.

Data färdas i celler av fast storlek, så ett relä ser en ström av likformiga block i stället för formen på de ursprungliga paketen. Flera TCP-strömmar kan dela en krets när deras isoleringskrav är förenliga. Klienten bygger kretsar både i förväg och vid behov och tar dem ur bruk efter ålder och användning; en långlivad ström kan stanna på sin ursprungliga krets, och vissa isoleringsinställningar tillåter längre återanvändning. Applikationer når klienten via en lokal SOCKS-proxy, och bara TCP tar den vägen. Designartikeln säger rakt ut att den inte tunnlar protokoll som UDP. Frivilliga kör reläerna, och vart och ett publicerar en beskrivning med sina nycklar, sin adress, sin bandbredd och sin utgångspolicy. Ett litet antal katalogauktoriteter röstar om vilka reläer som ska listas och signerar resultatet som ett konsensusdokument, som varje klient hämtar innan den väljer väg.

Använd begreppet i ett beslut

Använd ”Vad är Tor?” 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

För den som driver en publik webbplats är Tor först och främst ett faktum om publiken. En läsare som kommer via Tor ser ut att komma från ett utgångsreläs adress och inte från sin egen, och listan över reläer är publik med flit, eftersom varje klient behöver den för att välja väg. En webbplats kan alltså känna igen trafik från Tor och behandla den annorlunda. Tor Project anser att den som driver en webbplats har rätt att blockera den, även om projektet hoppas att det inte sker. Beslutet som återstår gäller vad du gör med de läsarna: betjänar dem som alla andra, bromsar dem, ställer en utmaning framför dem eller ger dem en väg in som aldrig lämnar Tor-nätverket, vilket är precis vad en onion-adress gör.

Det lönar sig att vara noga med vad Tor lovar, eftersom designartikeln räknar upp vad den lämnar utanför. Den gör inte anspråk på att stå emot en observatör som kan se båda ändarna av en anslutning och jämföra tidpunkter och volym, och projektets dokumentation tillägger att forskarna inte känner till någon praktisk design med låg latens som klarar det på ett tillförlitligt sätt. Grundprotokollet döljer inte själva Tor-användningen; broar med pluggable transports ger fler sätt att maskera den trafiken. Och Tor krypterar inte den sista sträckan från utgångsreläet till målet: applikationen behöver egen kryptering för det steget.

Jämfört med ett VPN är förtroendet ordnat på ett annat sätt. En VPN-leverantör ser både användaren och målet och ombeds titta bort. I Tor ser inget enskilt relä båda. För de flesta vägar håller urvalsreglerna isär reläer ur samma deklarerade familj och undviker som standard ett gemensamt IPv4-/16- eller IPv6-/32-subnät; det finns dokumenterade undantag och konfigurerbara subnätsgränser. Priset är latens, eftersom en vanlig utgångskrets passerar tre maskiner som drivs av frivilliga, så sidor som är lätta och klarar sig med få förfrågningar fram och tillbaka fungerar bäst för läsare över Tor. En onion-adress kräver en tor-process och en privat nyckel att skydda, men ingen öppen inkommande port, och därför passar den på liten infrastruktur.

Så ser det ut i praktiken

Företagets egen webbplats går att läsa över Tor. Kommandoradssidan publicerar onion-adressen bredvid ett `curl` -kommando som hämtar texten i Markdown via en lokal tor-klient. Adressen är med avsikt vanlig `http://` : en onion-adress av version 3 kodar tjänstens publika identitetsnyckel tillsammans med en kontrollsumma och en versionsbyte. Tor autentiserar tjänsten och krypterar kretsen innan HTTP utbyts. Ett publikt webbcertifikat behövs inte för denna autentisering av onion-adressen.

En onion-tjänst behövde plats för en tor-process på värddatorn för företagets publika tjänster från september 2026: en kärna och ungefär 464 MB användbart minne, där TLS redan terminerades för sju domäner och en git-forge kördes. Utrymmet för den processen mättes i stället för att diskuteras, under ett dokumenterat dygn med stickprov på värddatorn med 512 MB: det lägsta uppmätta tillgängliga minnet var ungefär 310 MB av de 464, swapanvändningen var 2,6 procent och processorn var i vila 99,7 procent av tiden, så Tor fick plats bredvid resten.

Integritetssidan beskriver företagets val om att räkna läsare. Gemini- och Gopher-applikationerna för ingen åtkomstlogg, och deras dagliga räknare registrerar bara det sammanlagda antalet förfrågningar. Gopher har också en anslutningslogg i operativsystemet som innehåller källadressen; den loggen raderas efter 30 dagar. Företaget säger att det inte räknar något alls över Tor och inte erbjuder någon inställning för att aktivera det. Det är ett integritetsval från operatörens sida: Tor döljer läsarens nätverksadress men hindrar inte en tjänst från att räkna förfrågningar. Sidan säger att företaget hellre inte vill veta än kunna veta.

Var det går fel

Namnet slås upp utanför Tor. Ett program som skickar sina anslutningar till en SOCKS-proxy kan ändå slå upp värdnamnet själv först, via den vanliga resolvern, och den uppslagningen talar om för det lokala nätverket och DNS-leverantören vilken webbplats som besöks. Anslutningen går sedan genom Tor, men målet har redan läckt. I `curl` skiljer en enda flagga: med `--socks5` slås namnet upp lokalt, med `--socks5-hostname` lämnas det till proxyn och utgångsreläet slår upp det.

```
# Resolves the name locally, then connects through the proxy
curl -s --socks5 127.0.0.1:9050 https://example.org/
# Hands the name to tor; the exit relay looks it up
curl -s --socks5-hostname 127.0.0.1:9050 https://example.org/
```

Klartext efter utgången. Tor krypterar stegen mellan reläerna, inte det sista. Utgångsreläet öppnar en vanlig TCP-anslutning till målet och skickar det som applikationen gav det, så ett inloggningsformulär som skickas över vanlig HTTP kan läsas av den som driver utgångsreläet och av vem som helst i nätet bortom det. Leverera HTTPS för allt som lämnar Tor-nätverket. En onion-tjänst kringgår frågan, eftersom dess trafik aldrig lämnar nätverket.

En adress står för många läsare. Hastighetsbegränsningar och spärrar som utgår från klientens adress behandlar ett utgångsrelä som en enda besökare, fast många använder det samtidigt. En gräns som är inställd för en person stänger ute alla vars krets råkar sluta där, och en spärr som en enda missbrukare har förtjänat drabbar dem allihop. Bestäm medvetet hur utgångsadresser ska behandlas, i stället för att låta en generell regel per adress avgöra.

Identiteten färdas inuti kretsen. Tor döljer nätverksadressen och gör ingenting åt vad applikationen säger. En inloggning på ett personligt konto, en webbläsare med en särpräglad uppsättning eller ett dokument som hämtar något när det öppnas knyter sessionen till en person, hur många reläer som än ligger emellan. Projektets egen dokumentation påpekar att trafiken från applikationen fortfarande måste rensas på användarens sida. Det är det jobbet som Tor Browser tar på sig och som en vanlig webbläsare som pekas mot proxyn inte gör.

Ett utgångsrelä på en hemuppkoppling. Vakter och mellanreläer drar sällan på sig klagomål om missbruk. Utgången är det ställe som målen ser trafiken komma ifrån, så klagomålen och en och annan rättslig förfrågan hamnar hos den som driver den, och reläguiden från Tor Project säger att man inte ska köra ett utgångsrelä hemifrån. En frivillig med en enda hemadress kan köra en brygga (bridge) i stället, ett olistat relä som samma guide rekommenderar för just det läget.

Att räkna med att UDP fungerar. Röstsamtal, många spel och verktyg som skickar sina egna DNS-frågor bygger på UDP, och Tor bär bara TCP-strömmar. Sådana program fungerar inte genom Tor, och ett program som inte tvingas

genom proxyn kan helt enkelt ansluta direkt, utanför Tor, utan att säga något om det.

Läs mer

- Tor Specifications — protokollet, vägvalet, katalogen och specifikationerna för onion-tjänster samlade på ett ställe.
- Tor: The Second-Generation Onion Router — designartikeln: kretsar, celler, utgångspolicyer och en uttrycklig lista över vad designen inte försöker göra.
- Tor Path Specification — hur en klient väljer vakt, mellanrelä och utgång, och vilka reläer som inte får dela väg.
- Types of relays on the Tor network — vakter, mellanreläer, utgångsreläer och bryggor, med den rättsliga exponering som var och en innebär för den som driver den.
- HTTPS encryption and Tor — en interaktiv bild av vad en tjuvlyssnare ser med Tor, med HTTPS, med båda och med ingetdera.



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 Tor?” 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/tor/