IT-Politisk Forening
Jesper Lund
2972 7719
jesper@itpol.dk

22. november 2016

Notat om CG-NAT logning og privacy

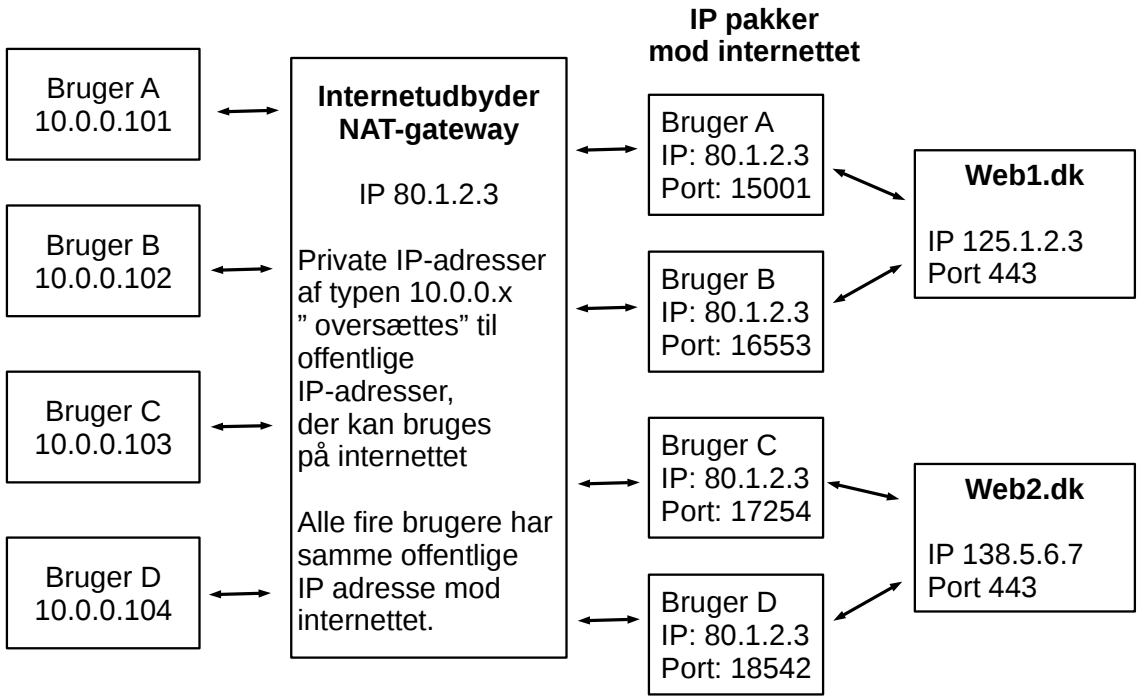
Formålet med dette notat er at redegøre for to forskellige metoder til CG-NAT logning af internetadgang med hensyn til efterforskningsmuligheder for politiet og omfanget af indgrebet i borgernes ret til privatliv og persondatabeskyttelse.

Notatet er skrevet som opfølgning på et møde hos Justitsministeriet den 18. november 2016, hvor Rigspolitiet og en række civilsamfundsorganisationer deltog. På mødet var der en diskussion af hvad CG-NAT logning konkret ville indebære.

Network Address Translation (NAT)

I mange situationer der er ikke unikke IPv4 adresser til alle brugere på et netværk. Network Address Translation (NAT) er en metode, som tillader flere brugere at dele en offentlig IP-adresse. Når NAT anvendes hos en internetudbyder (ISP), kaldes det normalt Carrier Grade NAT (CG-NAT).

Figuren nedenfor illustrerer hvordan GC-NAT fungerer. Der er fire abonnenter (brugere) med samme IP-adresse (80.1.2.3), som har HTTPS internettrafik til to websites (web1.dk og web2.dk).



En NAT-gateway er en server, som oversætter private IP-adresser (10.0.0.x i figuren) til offentlige IP-adresser på en sådan måde, at mange brugere kan dele den samme offentlige IP adresse.

Udfordringen i forhold til logning er at et potentielt stort antal abonnenter udadtil optræder med samme offentlige IP-adresse. ISP'erne skal efter logningsbekendtgørelsens § 5, stk. 1 registrere brugeridentiteten for en dynamisk tildelt IP-adresse. Når der anvendes CG-NAT, vil flere kunder imidlertid have tildelt den samme offentlige IP-adresse på et givent tidspunkt.[1]

Hvis politiet skal have oplyst hvem der anvendte en dynamisk tildelt IP-adresse på et bestemt tidspunkt, vil ISP'en ikke kunne oplyse identiteten på en specifik abonnent, men kun den samlede liste af abonnenter, som har brugt den pågældende IP-adresse på det pågældende tidspunkt. Det kan i nogle situationer være flere tusinde abonnenter.

For at identificere en konkret abonnent bag CG-NAT kræves logning af flere oplysninger hos ISP'en. Nedenfor skitseres to metoder baseret på henholdsvis registrering af anvendte source porte og registrering af internetforbindelsesoplysninger.[2]

Metode 1: Logning af source porte for den enkelte abonnent

På et givent tidspunkt vil kombinationen af source IP-adresse og source port-nummer være unik for den enkelte abonnent. Det skyldes at NAT-gateway'en bruger kombination af IP-adresse og port-nummer til at skelne mellem de enkelte brugere i den såkaldte NAT-tabel.

En logning af tildelte source porte kan gennemføres på to måder:

1. ISP'en registrerer alle NAT-sessioner med source port samt start- og sluttidspunkt, hvilket er oplysninger som allerede findes i NAT-tabellen. Denne tabel holder styr på de enkelte abonnenters internetpakker når der bruges NAT.
2. ISP'en kan holde abonnenterne inden for bestemte port-intervaller i NAT-gateway'en. I figuren ovenfor kunne portene 15000-15999 eksempelvis være reserveret til abonnent A, portene 16000-16999 til abonnent B, etc. Fordelen ved denne metode er at der ikke skal gemmes oplysninger om de enkelte NAT-sessioner.

Fra en privacy synsvinkel vil den første metode med logning af NAT-sessioner registrere oplysninger om intensiteten af internetforbruget for den enkelte abonnent, så den anden metode med faste port-intervaller er principielt at foretrække.[3] Det vigtigste er dog, at der i begge tilfælde ikke sker nogen registrering af destination IP-adressser, herunder besøgte websites.

Det fremgår af en skrivelse fra Rigspolitiets til fire internetudbydere af 6. november 2014,[4] at en logning af source porte allerede er implementeret på frivillig basis hos i hvert fald nogle af udbyderne, idet ”politiet har fået oplyst fra visse udbydere, at disse udbydere alene har mulighed for

1 Den private IP-adresse er unik for den enkelte bruger/abonnent, men logning af denne adresse har begrænset efterforskningsmæssig værdi, eftersom den private IP-adresse kun optræder i internetpakkerne til og med ISP'ens NAT-gateway, hvor den private IP-adresse omskrives til en offentlig IP-adresse.

2 Ved internetforbindelsesoplysninger forstås oplysninger om internetpakker til/fra den enkelte abonnent, som inkluderer destination IP-adressen og eventuelt yderligere oplysninger som source/destination porte. Ordet er en oversættelse af ”Internet Connection Records” som det er defineret i den britiske Investigatory Powers Act af 2016, se ”Factsheet – Internet Connection Records”, Investigatory Powers Bill.

3 For nogle ISP'er vil metode 2 med faste port-intervaller for den enkelte abonnent dog ikke være implementerbar, og i disse situationer er logning af NAT-sessioner den eneste mulighed.

4 IT-Politisk Forening har fået aktindsigt i denne skrivelse og svarene fra de fire internetudbydere. Dokumenterne kan ses her.

at identificere disse oplysninger, såfremt politiet udover IP-adresse og kommunikationstidspunkt tillige angiver portnummer".[5]

En del (web)servere på internettet registrerer formentlig kun source IP-adressen i deres logfiler. Hvis indehaverne af disse servere ønsker at kriminelle forhold skal kunne efterforskes af politiet, også når der er tale om brugere bag CG-NAT, skal de opfordres til også at registrere source porte. Der eksisterer hverken i dansk eller europæisk lovgivning en logningspligt for indholdstjenester (websites), så eventuelle logfiler (med eller uden source porte foruden IP-adresser) laves allerede i dag på frivillig basis.[6] På den baggrund bør det ikke være umuligt at gennemføre en informations-kampagne rettet mod indholdstjenester, således at de fremover registrerer source porte i deres logfiler.[7]

De begrænsninger som CG-NAT skaber for politiets efterforskning findes i alle andre lande, og derfor bør der være en fælles europæisk interesse for en sådan kampagne. I Europol rapporten "Internet Organised Crime Threat Assessment 2016" omtales source porten som den yderligere information (udover IP-adresse), som er påkrævet for at identificere abonnenter bag CG-NAT.[8]

Metode 2: Logning af internetforbindelsesoplysninger

Det fremgik af mødet hos Justitsministeriet den 18. november 2016, at Justitsministeriet og Rigspolitiet arbejder med denne model for CG-NAT logning.

Hvis politiet ikke kan oplyse den anvendte source port til ISP'en ved GC-NAT, vil logning af internetforbindelsesoplysninger hos ISP'en kunne bidrage til at indsnævre kredsen af mulige abonnenter, eventuelt til en enkelt abonnent i særligt gunstige situationer.

Kravet er nu at politiet foruden source IP-adresse og kommunikationstidspunkt (timestamp) kan oplyse IP-adressen på den server, som den mistænkte person (abonnent) har haft trafik til, dvs. destination IP-adressen.[9] På grundlag af logning af internetforbindelsesoplysninger kan ISP'en identificere de kunder, som på det pågældende tidspunkt har anvendt den pågældende source IP-adresse og haft trafik til/fra den pågældende server (destination IP-adresse).

Modsat hvad der er tilfældet hvis politiet kan oplyse source porten, vil den yderligere oplysning om destination IP-adressen ikke nødvendigvis identificere en unik abonnent. Der kan sagtens være situationer, hvor flere kunder har haft trafik til den samme server på det angivne kommunikationstidspunkt.

---

5 Den gamle sessionslogning, som blev ophævet i 2014, skulle efter den daværende logningsbekendtgørelse udføres ved overgangen mellem udbyderens eget net og et andet eller andre net ("på kanten"). Det vil i praksis være efter udbyderens NAT-gateway, hvilket betyder at flere abonnenters internettrafik optræder med samme source IP-adresse. Nogle udbydere (i hvert fald TDC) havde dog på frivillig basis implementeret en yderligere logning af NAT-sessioner i forbindelse med den gamle sessionslogning. Det fremgår af en aktindsigt i et notat fra Rigspolitiet af 26. marts 2014 (se side 9 her).

6 I C-582/14 har EU-domstolen fastslået, at dynamiske IP-adresser er personlige data for en 3. part som et website, men et website kan til IT-sikkerhedsformål registrere IP-adresser i logfiler uden samtykke i medfør artikel 7, litra f) i direktiv 95/46/EF (persondatadirektivet).

7 Internetstandarden RFC 6302 "Logging Recommendations for Internet-Facing Servers" fra Internet Engineering Task Force (IETF) anbefaler at servere medtager source porten i deres logning af indgående trafik. Begrundelsen for dette er den stigende brug af CG-NAT blandt internetudbydere.

8 IOCTA 2016, Internet Organised Crime Assessment, Europol 2016, side 58.

9 Ligesom at source porten ikke altid er tilgængelig, vil der utvivlsomt være situationer, hvor politiet ikke er i stand til at oplyse IP-adressen på serveren. Eksempler kunne være servere med skiftende (dynamiske) IP-adresser som styres via dynamisk-DNS, eller load-balancing via DNS hvor en indholdstjeneste har servere på flere IP-adresser.

I figuren (eksemplet) ovenfor vil abonnent A og B have trafik til web1.dk med IP-adresse 125.1.2.3, og hvis det sker på samme tid, vil ISP'en på grundlag af source IP-adresse, destination IP-adresse og kommunikationstidspunkt ikke kunne oplyse en unik abonnent, men kun to mulige abonnenter.

Hyppigheden af denne situation (hvor abonnenten ikke er unik) vil afhænge af "populariteten" af den pågældende server samt af hvordan logningen af internetforbindelsesoplysninger konkret gennemføres. Hvis der logges NAT-sessioner med start- og sluttidspunkt, kan disse sessioner være relativt lange afhængig af en række implementeringsmæssige detaljer på såvel klient- som serversiden af den anvendte software (samt timeout-værdier for NAT-sessioner i NAT-gateway). I så fald øges sandsynligheden for at flere kunder kan have sessioner til den pågældende server, som overlapper det kommunikationstidspunkt som politiet oplyser til ISP'en.

En 1:1 logning af internetforbindelsesoplysninger for alle pakker vil umiddelbart øge chancen for at identificere en unik kunde, men dette logningskrav vil antageligt være dyrere for ISP'erne, fordi der skal gemmes flere oplysninger. Derudover kan der stadig være flere kunder som har trafik til serveren på det givne kommunikationstidspunkt (sekund). Politiet kan heller ikke være sikker på at tidspunkterne hos den eksterne server og ISP'en er fuldt synkroniserede, og dermed øges risikoen for at den forkerte abonnent identificeres med 1:1 logning (logning af alle pakker).

Logning af internetforbindelsesoplysninger har den meget store ulempe, at der sker en fuldstændig kortlægning af den enkelte abonnents internettrafik, svarende til den sessionslogning som var gældende for alle abonnenter frem til 2014. Denne kortlægning vil i mange tilfælde omfatte oplysninger om borgerens politiske og religiøse præferencer og sundhedstilstand, hvilket er følsomme personoplysninger. For uddybning af denne problematik henvises til IT-Politisk Forenings høringssvar til Justitsministeriet af 25. august 2016 om de gældende logningsregler med henblik på udarbejdelse af evaluering (høringssvaret kan ses her).

Selv hvis Rigspolitiet kan argumentere for, at der er situationer hvor det vil være umuligt for politiet at oplyse source porten til ISP'en, og hvor den supplerende oplysning af destination IP-adressen kan indsnævre kredsen af mulige abonnenter til en enkelt eller i det mindste et begrænset antal personer, **bør Justitsministeriet i forbindelse med det kommende lovforslag stadigt overveje meget nøje, om denne yderligere efterforskningsmæssige fordel for politiet er proportional i forhold til det betydelige indgreb i borgernes ret til privatliv og persondatabeskyttelse, som en fuldstændig logning af internetforbindelsesoplysninger for alle CG-NAT abonnenter vil udgøre.**

I den forbindelse skal det anføres, at der kun vil være en efterforskningsmæssig værdi for politiet, hvis den mistænkte person tilgår internettet direkte. Hvis der gøres brug af VPN-forbindelser eller Tor-netværket, vil logning af internetforbindelsesoplysninger (destination IP-adressen) være omsonst. Der kan let opstå en situation, hvor den primære effekt af logningen er en meget indgribende kortlægning af uskyldige borgeres internettrafik, mens sikkerhedsbevidste kriminelle beskytter sig med VPN eller Tor. Det samme gælder selvfølgelig ved logning af source porte, men her er indgrebet i borgernes ret til privatliv og persondatabeskyttelse noget mindre, fordi de loggede oplysninger ikke direkte afslører destinationen for internettrafikken.

IT-sikkerhedseksperter råder i øvrigt allerede i dag almindelige (ikke-kriminelle) borgere til at beskytte deres mobiltelefon med en VPN-forbindelse, når de bruger offentlige WiFi hotspots og mobildata roaming i udlandet.[10] Det må antages, at kriminelle også læser sådanne anbefalinger.

10 Se for eksempel artiklen "Sådan undgår du hackere på din ferie", BT 16. juni 2016.

International sammenligning

Dette afsnit er skrevet på baggrund af oplysninger fra IT-Politisk Forenings internationale netværk, og listen nedenfor med EU-lande som har logning for at håndtere CG-NAT er derfor næppe komplet. Generelt må det dog antages at CG-NAT logning indtil videre kun forekommer i et begrænset antal EU-lande, fordi de fleste EU-lande indtil 2014 implementerede logningsdirektivet som ikke tog højde for CG-NAT, og i et antal EU-lande har nationale domstole efter EU-dommen i april 2014 om logningsdirektivet underkendt den nationale logningslov.

Storbritannien (UK)
Counter-Terrorism and Security Act 2015, Section 21(3) indførte en pligt for internetudbydere til at lave CG-NAT logning med source porte eller lignende information, som kan identificere en abonnent bag en delt IP-adresse. Det fremgår specifikt af sidste del af Section 21(3), at der ikke kan registreres oplysninger om besøgte websites. I november 2016 har parlamentet i UK vedtaget Investigatory Powers Act 2016 med krav om logning af internetforbindelsesoplysninger (Internet Connection Records), svarende til den danske sessionslogning som eksisterede frem til 2014, og Section 21 i Counter-Terrorism and Security Act 2015 ophæves i den forbindelse.

Internetforbindelsesoplysninger i Investigatory Powers Act har en bredere anvendelse end identifikation af en abonnent bag CG-NAT. Derudover kan forskellen mellem de to love uden tvivl henføres til, at det Konservative Parti efter valget i maj 2015 har flertal alene i Underhuset, mens partiet før valget indgik i en koalitionsregering med de Liberale Demokrater, som traditionelt har et større fokus på borgerrettigheder (herunder retten til privatliv) end det Konservative Parti.

Nederlandene (NL)
Parlamentet i Nederlandene behandler for tiden et lovforslag om en ny logningslov, som skal erstatte den tidligere logningslov der blev erklæret ugyldig af en domstol i marts 2015. Artikel I, punkt G i lovforslaget (side 4-5) kræver logning af tildelt IP-adresse samt yderligere unikke identifiers som port-numre, hvis det er nødvendigt for at identificere abonnenten.[11] Af lovforslagets bemærkninger side 41-42 fremgår det, at internetudbyderen skal gemme oplysninger om CG-NAT sessioner med port-numre samt start- og sluttidspunkt for sessionen, således at en abonnent kan identificeres ud fra source IP-adresse og source port.[12]

11 Lovforslaget om logning i NL kan ses her (på nederlandsk; Bits of Freedom takkes for oversættelse af de relevante dele af lovforslaget og bemærkningerne).
12 Bemærkninger til lovforslaget om logning i NL kan ses her (på nederlandsk).