No pioneiro artigo *Characterization and Measurement of TCP Traversal through NATs and Firewalls,* os autores Saikat Guha e Paul Francis avaliam a probabilidade de sucesso no estabelecimento de conexões TCP atravessando gateways NAT (o chamado NAT transversal), quando ambos os *peer*s estão atrás das mesmas.

Estabelecer e manter conexões UDP atravessando NAT foi resolvido pelo protocolo STUN (RFC3489), mas o caso do protocolo TCP é um problema aberto ainda hoje. A gama de aplicações que se beneficiam ou são baseadas na comunicação confiável TCP é ampla (podemos citar acesso remoto, p2p, mensagens instantâneas e transmissão de voz e mídia em geral). A maioria das pessoas utiliza redes privadas atrás de dispositivos que efetuam NAT, como firewalls, justificando o trabalho. Há muito interessados em encontrar uma abordagem de sucesso, como os grandes provedores de mídia e jogos online.

Mediante revisão da literatura sobre o assunto, caracterizando e avaliando as diversas abordagens para obter atingir o objetivo, as falha e limitações (tanto dos artigos quando as apresentadas pelos sistemas operacionais, na verdade específicas do Windows XP). O experimento consistiu em avaliar uma série de roteadores disponíveis no mercado, tanto em laboratório (16 marcas e implementações) quanto em ambiente doméstico (83 em condições reais), utilizando drivers e ferramentas desenvolvidas pelos autores, principalmente o protocolo cliente-servidor STUNT (“sopa de letrinhas” que designa a adaptação do STUN para incluir TCP), quanto à capacidade de estabeleceram conexões TCP transversal sobre NAT.

O critério para obtenção dos dispositivos foi a “disponibilidade em lojas online nos Estados Unidos”, o que pode não representar bem a população de dispositivos pensando-se em comunicação mundial, principalmente em aplicações como comunicação online, que são relevantes quando consideramos países distintos com mercados distintos. Os próprios autores fazem essa ressalva pois a amostra de marcas e usuários testados em condições mais p´roximas às reais, além de pequena é concentrada em determindas marcas e um região específica.

O comportamento dos NAT avaliados foi separado e classificado em cinco característica gerais, para ser entrecruzado de acordo com as abordagem, inclusive se os dispositivos implementam o protocolo TCP corretamente para casos extremos (de borda/corta) . Cada característica de Os NAT comportam-se de maneiras distintas. Os autores utilizaram um fator de correção para as amostras que estavam sub-representadas, baseando-se em dados de pesquisa de mercado, o que pode ainda sim não refletir a realidade, pois tais pesquisas são fechadas. Uma ressalva é a mudança rápida do mercado e a impossibilidade de generalizar por marcas, pois há grande variação com relação a firmware e comportamento mesmo dentro da mesma marca.

As avaliações isoladas e em conjunto, estimam os sucesso das abordagens, bem como reportam o sucesso de estabelecimento de conexão TCP *peer-to-peer* atrás de NAT desde que pelo menos um dos pontos finais tenha comportamento previsível. Os autores fornecem uma discussão, baseados em uma aplicação peer-to-peer implementada e orientações para desenvolvedores sobre como obter com TCP transversal com altas taxas de sucesso em muitos cenários comuns.

Concluem reforçando que o STUN (RFC3489) já está padronizado e é antigo UDP, entretanto para TCP a área e nova. Protocolos como UPnP e MIDCOM permitem controle explícito do NAT por aplicações, mas o foco aqui é permitir que aplicações funcionem parao maior número de dispositivos, ao invés de restringí-las aos dispositivos compatíveis. Outra abordagem foi o estabelecimento do UPnP (embora não seja patrocinado pela IETF e seja necessário que ambos os hosts interessados na conexão sejam compatíveis com ele).

Os autores fazem uma série de ressalvas ao próprio estudo, como a questão das medições constituírem uma “fotografia” do período, a amostra ser enviesada e com escopo limitado, além da falta de avaliação de gateways que efetuam tradução IPv4 para IPv6. Tal ponderação ilustra a clareza dos autores ao delimitarem o problema. Não por acaso,

Em publicações mais recentes, verifica-se que há propostas de algoritmos para aumentar essa abrangência, como o e por fim a metodologia ICE (RFC5245), que estabelece mecanismos para NAT transversal referentes a multimídia. Os autores apontam que os resultados do artigo poderiam ser utilizados como referência para o processo de padronização de NAT e firewalls (que são um padrão de mercado, apesar de não serem consenso pois violam certas propriedades básicas da Internet) é justamente a falta de padronização de seu comportamento entre os diversos fabricantes). De fato os conceitos do artigo foram incorporados ao ICE-TCP[[1]](#footnote-1). A técnica ICE (Interactive Connectivity Establishment, no RFC5245) tem como meta obter comunicações altamente confiáveis que funcionem no maior número de configurações de rede possíveis, agregando diversas técnicas comprovadas.

Embora o protocolo e ferramentas tenham sido descontinuados em 2007, os dados dos testes e ferramentas estão disponíveis em domínio público. O trabalho é muito relevante por buscar interoperabilidade e soluções que atendam ao mercado e às pessoas e mesmo suas fraquezas são bem exploradas e esclarecidas pelos autores, fornecendo base para outro trabalhos.

1. <http://tools.ietf.org/html/draft-ietf-mmusic-ice-tcp-16> [↑](#footnote-ref-1)