Web Real-Time Communications Deployment Guide

Firewalls and Restrictive NAT

12/16/2025

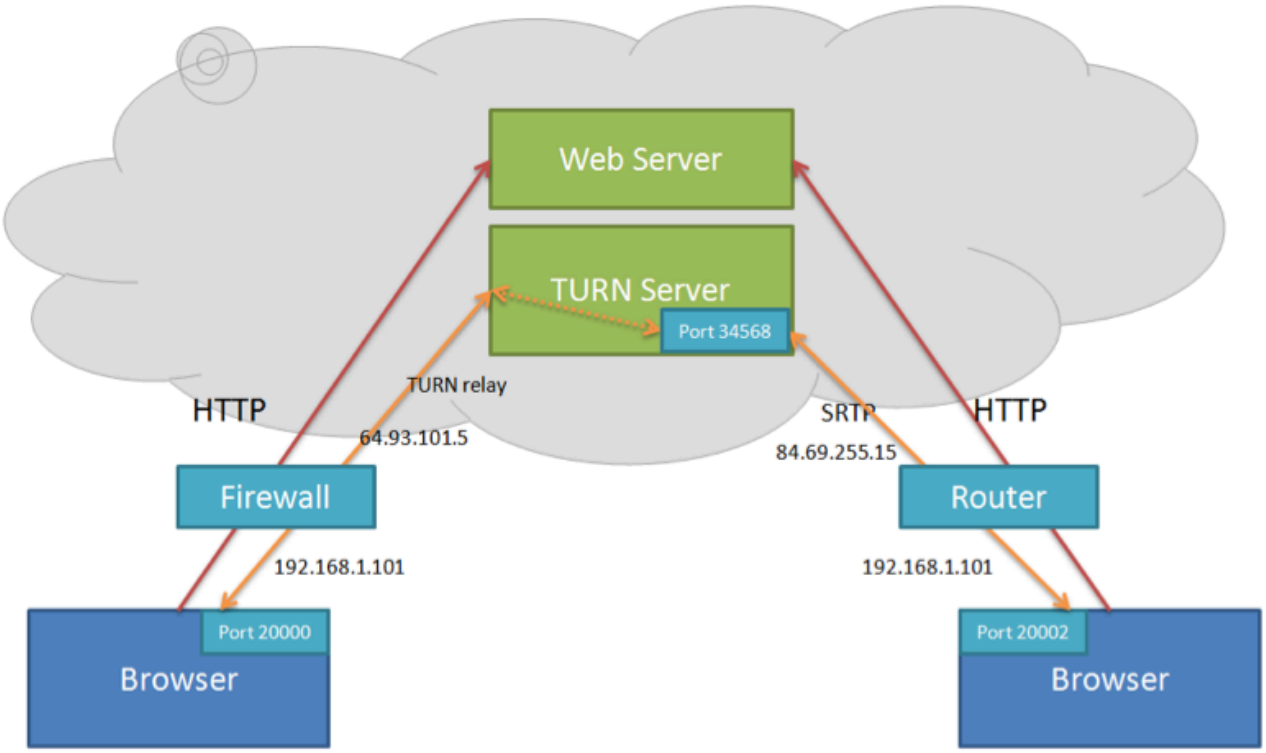
Firewalls and Restrictive NAT

In addition to dealing with NAT (Network Address Traversal), enterprise firewalls often implement restrictive access control as a means of protecting the enterprise network. A typical enterprise firewall might block all unknown ports from both inbound and outbound traffic. This means only a handful of known commonly used protocols, such as HTTP/HTTPS, ftp, and ssh, will be allowed to access the enterprise network.

Also, some routers may have a restrictive NAT translation policy that enforces address- and port-dependent mapping. This means the NAT binding can only be enabled for a specific address and port. When both endpoints are behind the same type of NAT, then both sides will be unable to find the actual binding outside of NAT.

In order to work with firewalls or restrictive NAT, ICE requires an additional intermediary called a Traversal Using Relays around NAT server (TURN server). This server, which is deployed on a public address, can relay media packets for a TURN client so that they are ultimately able to reach another endpoint. The browser that wants to send and receive media is considered as a TURN client and connects to the TURN server to acquire a relay address. Using this address the browser client can use this as a candidate in ICE negotiation during SDP offer/answer negotiation.

The following diagram shows an example where the browser client on the left is a TURN client and the TURN client is behind a restrictive firewall that blocks UDP traffic but allows a connection to the TURN server. The web application that offers the use of this TURN server would provide the TURN server address and a credential in the web page. The browser uses the TURN server address and the credential to initiate a request for relay ports on its behalf. In the following example, port 34568 is assigned to the TURN client and the browser can create an SDP offer with port 34568 on the TURN server address (a public address) as a candidate.


Web Server
TURN Server
Port 34568
TURN relay
HTTP
64.93.101.5
SRTP
84.69.255.15
HTTP
Firewall
Router
192.168.1.101
192.168.1.101
Port 20000
Browser
Port 20002
Browser