This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Web Real-Time Communications Deployment Guide

Private Cloud

12/19/2025

Contents

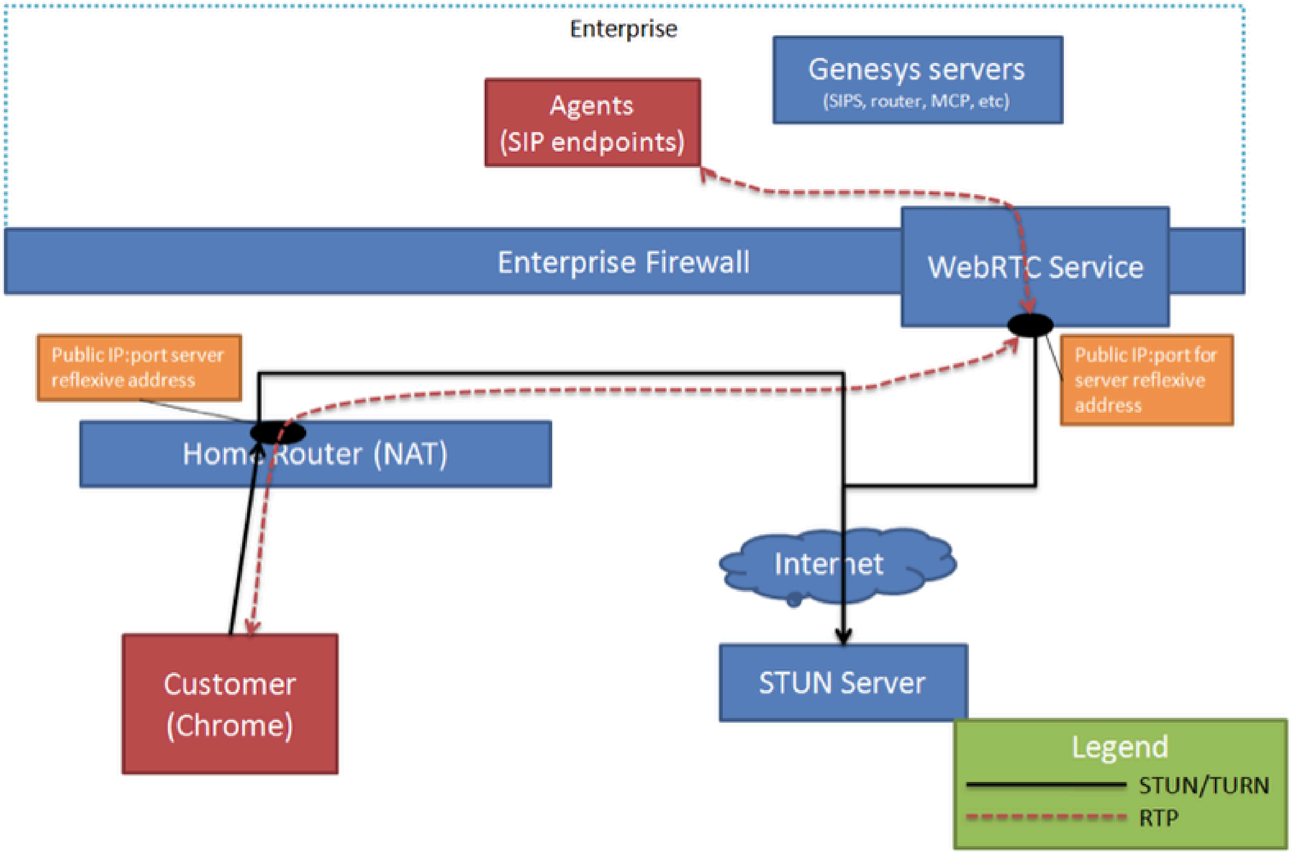
Private Cloud

In a private cloud, Genesys servers are generally deployed behind an enterprise firewall and are only able to access specific services from the Internet. The Genesys WebRTC Service is one of the servers that need to be accessible from the Internet for HTTP and SRTP. The WebRTC Service can then send SIP/RTP towards the enterprise network and is also able to bridge the media. In this type of deployment, the WebRTC Service must be deployed in the DMZ so that the component can handle inbound HTTP and SRTP traffic.

The following sections show the media path between customers and agents using various endpoints.

Customer (Browser) – Agent (SIP)

SIP agents are deployed within the enterprise. The WebRTC Service bridges media in from customers using browsers. To allow customers to connect to the WebRTC Service, the enterprise must deploy a STUN server on the public Internet so that the browser and the WebRTC Service can discover the server-reflexive address.



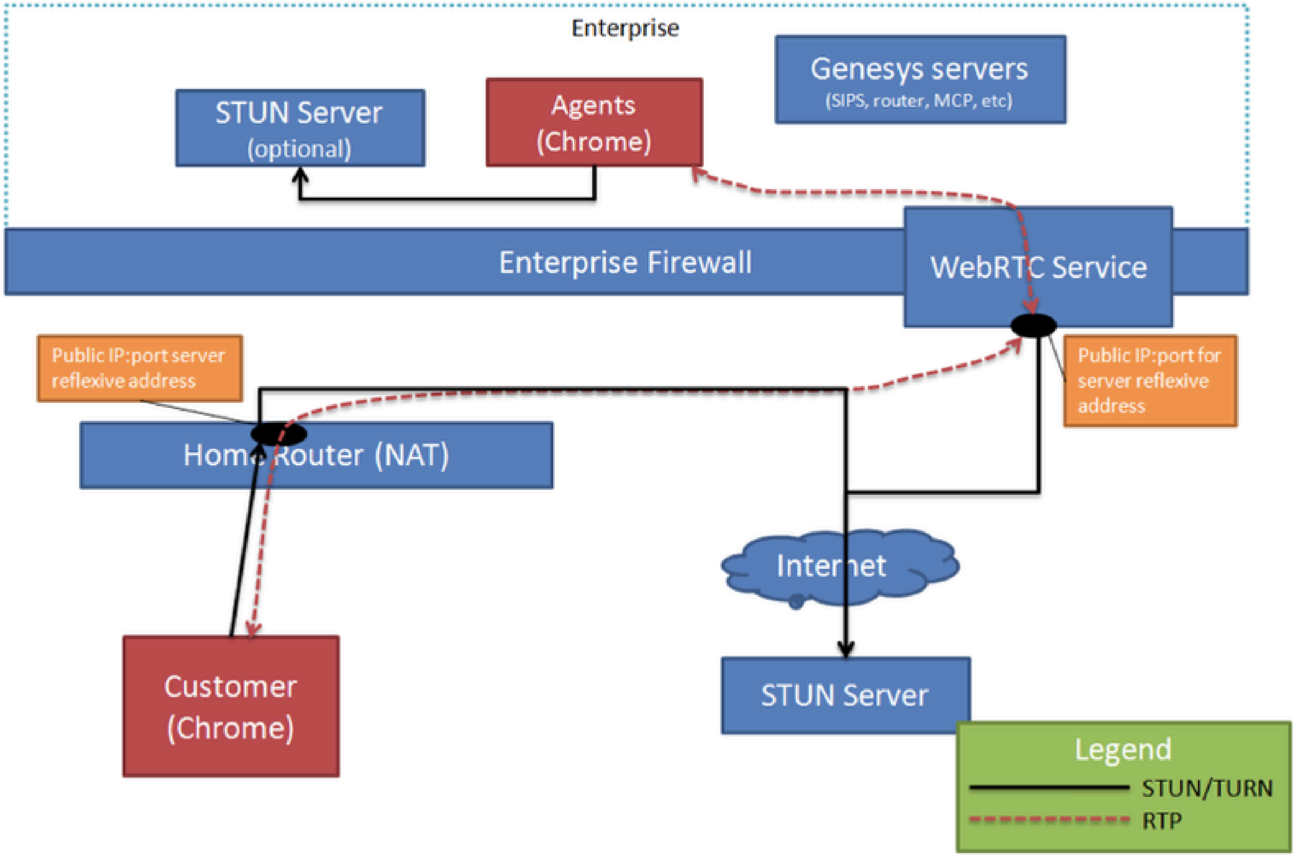
Customer (Browser) – Agent (Browser Inside the Enterprise)

Note: *A web-based agent desktop application implemented using the Genesys WebRTC JavaScript API could be used in this model. Genesys Workspace Web Edition is such a tool that supports audio-only calls, with no video support at this time.*

When agents use a browser as the endpoint to handle calls, the agent browser must be able to connect to the WebRTC Service in the DMZ. Since they are all hosted within the same enterprise network there are no restrictions about doing that. If NAT is deployed within the enterprise, then the enterprise must also deploy a STUN server within the enterprise network so that the browser and the WebRTC Service can resolve the server-reflexive address within the enterprise network.

On the customer-facing side, the media path is the same as described in the previous section; a STUN server must be deployed on the public network to allow customer browsers to resolve the server-reflexive address.

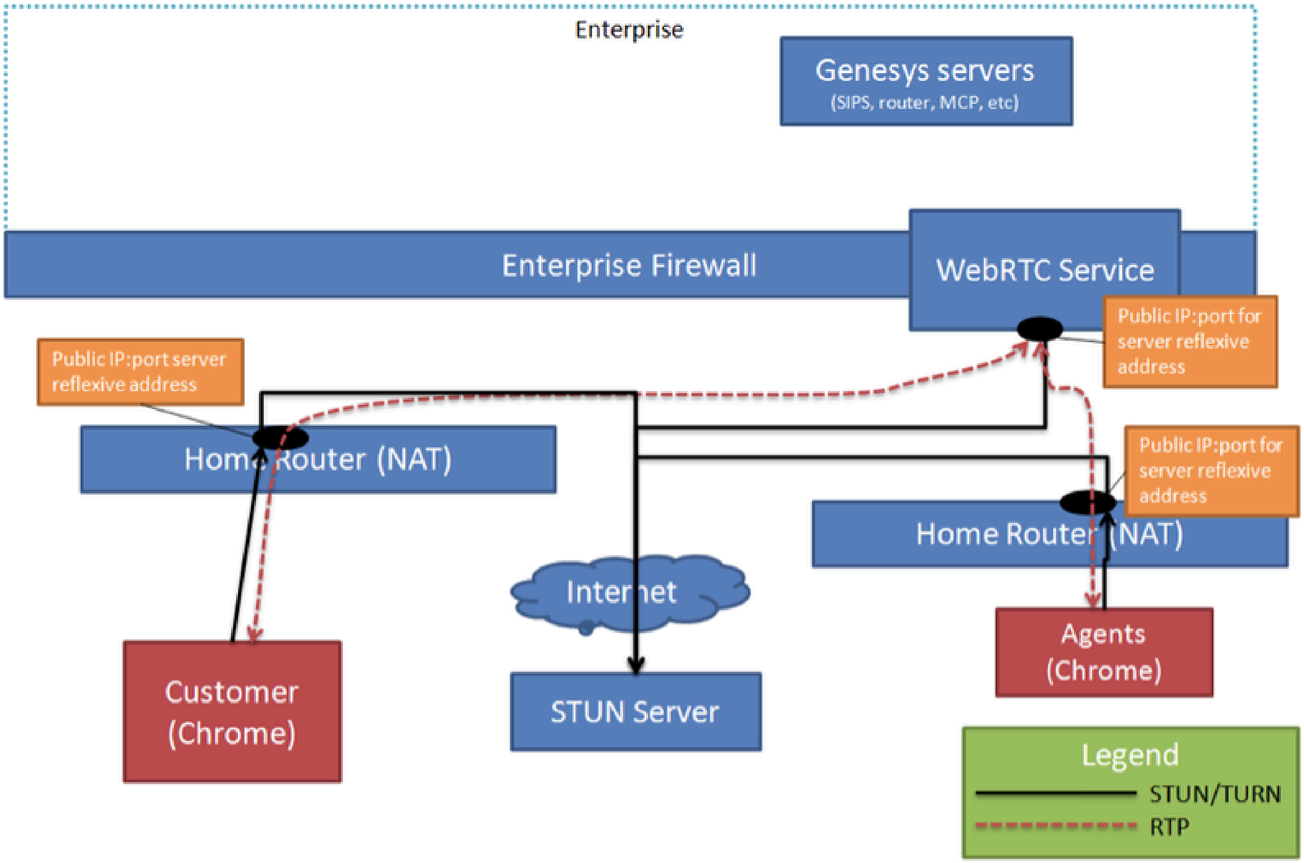
The WebRTC Service may still need to establish a media path to a Genesys server, such as a media server, for additional media services. It is therefore important to mention that the WebRTC Service is establishing the media path to the media server by means of the SIP/RTP path. Network address translation should not be configured between the WebRTC Service and the media servers, even though browser-using enterprise agents may be hosted in a subnet where NAT is enabled.



Customer (Browser) – Agent (Browser Outside the Enterprise)

Note: *A web-based agent desktop application implemented using the Genesys WebRTC JavaScript API could be used in this model. Genesys Workspace Web Edition is such a tool that supports audio-only calls, with no video support at this time.*

In deployments where remote agents are using a browser to handle calls, the remote agents connect their media paths to the WebRTC Service in the same manner as the customer browsers. The same public STUN server can service both customers and remote agents connecting to the WebRTC Service.


Enterprise
Genesys servers
(SIPS, router, MCP, etc)
Enterprise Firewall
WebRTC Service
Public IP:port for server reflexive address
Public IP:port server reflexive address
Home Router (NAT)
Public IP:port for server reflexive address
Home Router (NAT)
Internet
Customer (Chrome)
STUN Server
Agents (Chrome)
Legend
STUN/TURN
RTP