SBC for WRTC

In this section:

Related articles:

- Direct Media and Anti-trombone Support for ICE and DTLS
- Late Media Support for ICE and DTLS
- Pseudo Full ICE Support
- Signaling and Datachannel Pass-through With ICE Termination

Overview

The Sonus WebRTC Gateway (WRTC) technology enables web browsers to participate in audio, video, and data communications, without any kind of additional plug-ins or application downloads. Using a WRTC enabled browser, user can place a call, participate in multi-party video and audio conferencing, and engage in screen sharing collaboration. Sonus Web Service Solution bridges the web and SIP worlds to facilitate the integration of communications (voice, video, and data) in applications.

The Sonus SBC Core is a component of Sonus Web Service Solution. The SBC provides media service functionality when the WRTC endpoints are behind a NAT.

The SBC acts as a WRTC to SIP media gateway. It enables WRTC users to communicate to any back-end SIP system and PSTN. The SBC also provides routing, security, transcoding, and interworking. It supports the following functionalities:

- Relays and monitors the media streams.
- Inter-works WRTC media DTLS/SRTP to traditional RTP/UDP.
- Relays or transcodes opus to G7xx voice codecs.
- Relays VP8/VP9, and H.264 video codecs.
- Supports ICE and STUN procedures for NAT traversal.

ICE-Lite Support

Overview

Interactive Connectivity Establishment (ICE) is a protocol for Network Address Translator (NAT) traversal for multimedia sessions established with the offer/answer model. ICE uses the Session Traversal Utilities for NAT (STUN) protocol and its extension Traversal Using Relay NAT (TURN). ICE uses STUN and TURN servers to overcome network address translation issues that can occur when an endpoint is situated behind a NAT device. ICE solves the NAT issues for media streams. Support of the ICE specification is required by WebRTC (WRTC) endpoints.

The SBC is capable of acting as an ICE-Lite agent to allow the WRTC endpoints to connect to the existing VoIP network through the SBC using the DTLS-SRTP protocol. While acting as an ICE-Lite endpoint, the SBC interconnects with endpoints that have either ICE-Lite or full-ICE implementations. ICE-Lite is a lite version of the ICE protocol, which is defined to exchange media with each other. The interconnect with ICE-Lite end points is only for the purpose of IPv4 to IPv6 inter-working and no NAT traversal procedures are supported for ICE-Lite to ICE-Lite.

> ⚠ SBC implementation for ICE can be used with endpoints that are connected to the SBC through Sonus WRTC gateway and also WRTC endpoints connected from a third-party WRTC Gateway thereby presenting ICE in their SDP.

> ⚠ As SBC is not required to act as an ICE client (it is not located behind a NAT in current deployment models), the initial support for ICE is limited to the SBC acting as an ICE-Lite endpoint.

ICE-Lite key points:

STUN message processing:

- Decoding received messages on media port

- Validating the received messages
- Authenticating the received messages
- Encoding outgoing STUN Response messages and sending on allocated media port
- Encrypting outgoing STUN as per the configured username/password

Reachable IP address: an ICE-Lite agent has a reachable public IP address and can work with other agents that use ICE and are behind the NAT.

ICE-Lite Implementation

The ICE-Lite procedure starts with the offerer discovering all the IP port where it is reachable. These are known as local “candidates”. The “candidates” can be any or all of the following:

- Host candidates (Local IP port)
- Server Reflexive Candidates (External IP port allocated by NAT)
- Relay candidates (IP port on a media relay)

STUN is used to discover the Server Reflexive and Peer reflexive addresses on the NAT and TURN is used to discover the Relay candidates on the TURN relay. After the local candidates are discovered, the offerer (Full ICE Agent) sends them in the session description protocol (SDP) offer to the remote endpoints. The remote end point (SBC) discovers its own local candidates (which are only host candidates) and sends in the answer SDP to the offerer.

Once the offer/answer exchange is completed, Full ICE Agent takes the role of ICE controlling agent and performs connectivity check between the candidate pairs (from local candidate to remote candidate) by sending the STUN messages. SBC acts as controlled agent and responds to the STUN requests. Based on the success/failure of the connectivity check, a candidate pair is selected by the controlling agent to exchange the media and it sends a connectivity check on the selected pair with USE-CANDIDATE attribute to let the controlled agent know about the selected pair. The connectivity check may lead to the discovery of new local candidates due to the presence of Restricted or Symmetric NAT. These local candidates are also included in the procedure and are known as “Peer Reflexive Addresses”. SBC being a controlled ICE-Lite agent cuts thru the media after receiving USE-CANDIDATE on all components of the media stream (for example, if RTP and RTCP are required for a stream then media is only cut-through when USE-CANDIDATE is received for both RTP and RTCP).

The controlling agent sends an updated offer by using the selected local candidate in the default IP port of the media line and controlled agent (SBC) respond by sending its local candidate in the default IP port of the media line to complete the ICE-Lite procedure. The Ice-lite procedure can be restarted by the Full ice agent using ICE Restart procedures, if the Media ports changed during a call.

DTLS/SRTP Support

The Datagram Transport Layer Security (DTLS) protocol is designed to provide authentication, data integrity, and confidentiality for communications between two applications over an Unreliable Datagram Protocol (UDP). The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. DTLS-SRTP is an extension to the DTLS protocol, where DTLS acts as the key management protocol. DTLS protocol is also extended to negotiate the SRTP crypto suites and parameters for use with those keys.

The WRTC is a signaling protocol defined for the real time communication between the Web Browsers. The WRTC has assigned DTLS-SRTP protocol for the media exchange between the browsers. With the implementation of this feature, the SBC supports:

- Real time communication between the web browsers by using DTLS-SRTP while inter-working with SIP networks.
- DTLS on the media path for key management for the SRTP based media.
- The self-signed certificates to secure and authenticate DTLS associations. DTLS connections are secured by the two browsers sharing self-signed certificates as part of the media connection during a DTLS handshake between the browsers. The certificates are authenticated by checking a fingerprint, which is passed in the signaling path as part of the Session Description Protocol (SDP).

For configuration details, see Configuring SBC for WRTC.

Copyright © 2018 Sonus Networks. All rights reserved.