ASA firewall configuration for Expressway in dual NIC setup for WebRTC

Contents

Introduction

This document describes the configurational steps for ASA Firewall in an Expressway deployment with enabled dual NIC for WebRTC flow.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Cisco ASA (Cisco Adaptive Security Appliance) firewalls
- Administrative knowledge of Expressway servers
- Administrative knowledge of CMS (Cisco Meeting Server)
- Understanding of the Cisco CMS WebRTC application
- Network Address Translation (NAT)
- Traversal Using Relays around NAT (TURN)

Components Used

This document is not restricted to specific software and hardware versions, however the minimum software version requirements must be met.

- Expressway server
- CMS Server

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

WebRTC proxy support has been added to Expressway from version X8.9.2, which enables off-premises users to browse to a Cisco Meeting Server Web Bridge.

External clients and Guests can manage or join CMS coSpaces without the need of any software other than a supported web browser. List of supported browsers can be found [here](#).

The Expressway-E server can be configured with either single, or dual network interfaces (therefore having a pair of internally and externally-facing NICs). In the earlier Expressway versions, having a dual NIC with static NAT was not a mandatory requirement. When the WebRTC feature over Expressway was raised, it started to require a static NAT to be configured, even in the scenario of enabled dual NIC on the Expressway-E server. Expressway software version X12.5.3 is planned to contain a rework of the code's logic, which removes this requirement in almost all configurational scenarios. Refer to enhancement request [CSCve37570](#) for more information.

> **Note**: When Expressway-E in dual NIC configuration with static NAT is used as TURN server for the WebRTC traffic, and the only working media path is the relay candidate on both CMS and the WebRTC Client, the TURN server is sending RTP packets physically out to his own static NAT IP address. That is why NAT reflection must be configured on the external Firewall.

> **Caution**: Deployment of Expressway-E cluster with multiple TURN servers activated behind the same NAT continues to require NAT reflection to be configured.

Tech note

If you would like to learn more about the ICE, TURN and STUN processes, please watch the Cisco Life presentation [ICE / TURN / STUN Tutorial - BRKCOL-2986](#)

This session provides technical background and insights on Traversal Using Relay NAT (TURN) and Interactive Connectivity Establishment (ICE). It explains how these are used in the Collaboration Portfolio with some extra attention on the use case in Mobile and Remote Access (MRA). Participants in this session learned why TURN is needed and how ICE finds the optimal media path. Troubleshooting guidance was discussed, and the serviceability tools available together with best practices were demonstrated.

Configure

This chapter outlines the required steps to configure NAT reflection on the ASA firewall in the scenario of Expressway-E server with enabled dual NIC. Return traffic coming back from the firewall to the Expressway (after reflection) has as source address the public IP address of the server, where the request came from (to match the TURN permissions).

> **Note**: Firewalls typically mistrust packets that have the same source and destination

IP address. You must configure your external firewall to allow NAT reflection for the Expressway-E's public IP address.

Network Diagram

This image provides an example of a general WebRTC flow, in Expressway scenario with enabled dual NIC:

This image provides an example of connections flow and the required ports for it Web Proxy for CMS WebRTC: