AspenUC – Firewall Whitelist Rules

AspenUC UcaaS Firewall Requirements

LS Networks Engineering

Table of Contents

Document History

Version	Author	Date	Change Summary
1	Hugo Tinoco	October 22nd, 2019	Initial document creation

Document Overview

Document Identifier

AspenUC – Firewall Whitelist Rules

Description

Customers deploying AspenUC UcaaS behind a firewall, will be required to whitelist specific ports and services.

Document Scope

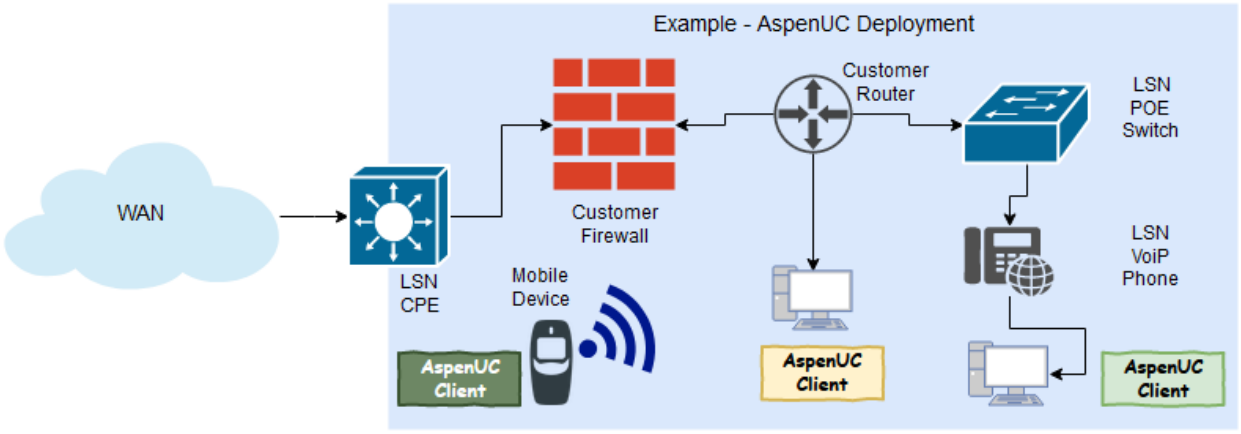
This document will focus on the necessary TCP/UDP ports, services and rules that must be whitelisted for an AspenUC thin client deployment. This is a general outline for customers utilizing WAN facing firewalls. This is NOT a guide for a security or network admin to follow when deploying AspenUC. If any further assistance is required with a complex firewall deployment, please contact the LS Networks Engineering team for assistance.

Classification

External. This document may be shared freely with LS Networks customers.

AspenUC – Thin Client

Below is an example deployment of AspenUC. The focus of this document is on the AspenUC Client on PCs or Mobile Devices.



Firewall Recommendations

The following are recommended ports and applications to allow through the on-site perimeter firewall for full functionality of the AspenUC UcaaS platform via the soft-client. A final decision on which ports and services to allow, will be determined by the Network/Security administrator for each individual location. However, majority of these services are critical for AspenUC's full functionality. The directionality of the firewall rules is assumed to be bi-directional.

Application	Port
SIP	TCP&UDP,5100,5060,5061
SSL/TLS	TCP/443
DNS	TCP/53
Jabber (XMPP)	TCP/443,5222,5223,5269,5270
Apple Push Notification (Mobile)	TCP/2195,2196,2197,5223,443
RTCP/rtb	Dynamic/(1024 to 65535)
Zoom	UDP,8801/8802

NGFW Considerations

Users behind a next generation firewall with application level inspection, should pay specific attention to the SIP port. Generally, default behavior under a SIP 'application' would allow or deny port 5060 and 5061. Ensure port 5100 is in the allowed list.

Please review the specified ports for all applications when using NGFW.

Summary:

The recommendations made on this document are to be reviewed by each individual entity's security and network team to properly asses the risk factor in considerations to their organization's needs. LS Networks does not assume any responsibility or liability for anyone following this document to make changes to their organizations firewall rules.

If customers would like to take extra precautions on identifying Source & Destination IP addresses, please contact the LS Networks engineering group.

This is a live document. As we extend the features of our AspenUC client, requirements and/or recommendations may change. For example, we are investigating the deployment of a Proxy server for file transfers between chat clients utilizing SOCKS5.

Glossary

- **SIP** - The Session Initiation Protocol is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
- **SSL** - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.
- **DNS** - The Domain Name System (DNS) stores and associates many types of information with domain names, it translates domain names (computer hostnames) to IP addresses, as the "phone book" for the Internet. It translates human-readable computer hostnames, e.g. www.paloaltonetworks.com, into the IP addresses that networking equipment needs for delivering information. It also stores other information such as the list of mail exchange servers that accept e-mail for a given domain.
- **Jabber** - Extensible Messaging and Presence Protocol (XMPP) is an open, XML-inspired protocol for near-real-time, extensible instant messaging (IM) and presence information (a.k.a. buddy lists). It is the core protocol of the Jabber Instant Messaging and Presence technology. The protocol is built to be extensible and has been used for publish-subscribe systems; signaling for VoIP, video, and file transfer; gaming; Internet of Things applications such as the smart grid; and Social networking services.
- **Apple-Push-Notifications** - The Apple Push Notification Service is a service created by Apple Inc. that was launched together with iOS 3.0 on June 17, 2009. It uses push technology through a constantly-open IP connection to forward notifications from the servers of third-party applications to the Apple devices; such notifications may include badges, sounds or custom text alerts. APNS was also added as an API to Mac OS X v10.7 - Lion for developers to take advantage of.

- **RTP** - Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet.
- **RTCP -** Real-time Transport Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP). RTCP provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP
- **Zoom -** Zoom is a meeting platform that unifies HD video conferencing, mobility and web meetings into a cloud service.

Source: Palo-Alto