Revision 2.0
Date: 22.05.2017
Author: Daniel Henriksen

Atea Anywhere

Atea Anywhere

Firewall Requirements

This document describes required settings on customer firewalls to access Atea Anywhere services.

Atea Anywhere is available for Small Businesses and Enterprises. Companies within the SMB category (typically up to 100 user licenses) primarily access Atea Anywhere via internet.

Enterprises (100+ user licenses) normally connect to Atea Anywhere with MPLS/VPN when the staff is physically located in office premises. Mobile users and home office users can access Atea Anywhere services via internet.

1. General Requirements and recommendations

1.1. Firewall SIP inspection Rules

Atea Anywhere requires that SIP and H.323 inspection rules in firewalls are disabled as they likely will cause misbehavior of voice and video calls.

1.2. Jabber to Jabber Calls and Symantec Host IDS (HIDS)

Jabber to Jabber calls can trigger errors in Symantec HIDS. Symantec HIDS has a rule that disables connections from internet-based servers if it receives 5 connection requests from the same internet-based server within 200 seconds. For example, 3 Jabber to Jabber calls within 200 seconds will trigger Symantec HIDS. When this happens, ongoing Jabber to Jabber calls are dropped and Jabber to Jabber calls are disabled for 600 seconds.
To avoid this scenario, you must add Cisco Jabber to the Symantec exception list.

2. Access to Atea Anywhere services over MPLS/WAN – Enterprise

2.1. Outgoing from customer office site to Atea Anywhere (91.184.140.0/24)

Device endpoint types: Cisco Jabber, IP Phones, Telepresence systems.

Purpose	Transport	Protocol	Atea Anywhere (listening)
Trivial File Transfer Protocol (TFTP) used to download firmware and configuration files	UDP	TFTP	69, 6969
HTTP Access	TCP	HTTP	80
HTTPS Access	TCP	HTTPS	443
URLs for XML applications, authentication, directories, services, etc.	TCP	HTTP	8080
Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities	UDP	BFCP	5070
Skinny Client Control Protocol (SCCP)	TCP	SCCP	2000
Secure Skinny Client Control Protocol (SCCPS)	TCP	SCCPS	2443
Provide trust verification service	TCP		2445
Certificate Authority Proxy Function (CAPF) listening port for issuing Locally Significant Certificates (LSCs)	TCP	CAPF	3804
Session Initiation Protocol (SIP)	TCP +UDP	SIP	5060
Secure Session Initiation Protocol (SIPS)	TCP	SIPS	5061
HTTP-based download of firmware and configuration files	TCP	HTTPS	6970

Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)	UDP	RTP/SRTP	16384 - 32767
Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.	TCP	HTTPS	8443
Connects to the TFTP server to download client configuration files securely for Cisco Unified Communications Manager	TCP	HTTPS	6972
Connects to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.	TCP	XMPP	5222
Certificate Trust List (CTL) provider listening service in Cisco Unified Communications Manager	TCP	CTL-Client	2444
Computer Telephony Interface (CTI) used for desk phone control.	TCP	CTIQBE	2748
Internet Control Message Protocol (ICMP) This protocol number carries echo-related traffic. It does not constitute a port as indicated in the column heading.	ICMP	ICMP	

2.2. **Incoming traffic from Atea Anywhere (91.184.140.0/24) to customer devices**

Device endpoint types: Cisco Jabber, IP Phones, Telepresence systems

Purpose	**Transport**	**Protocol**	**Atea Anywhere (listening)**
Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)	UDP	RTP/SRTP	16384 - 32767
Session Initiation Protocol (SIP)	TCP and UDP	SIP	5060
Secure Session Initiation Protocol (SIPS)	TCP	SIPS	5061
Web Requests From Cisco Unified Communications Manager to Phone		HTTP	80
Secure FTP service, SSH access	TCP	SSH	22
Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities	UDP	BFCP	5070
Internet Control Message Protocol (ICMP) This protocol number carries echo-related traffic. It does not constitute a port as indicated in the column heading.	ICMP	ICMP	7

2.3. **Traffic between customer devices (Bi-Directional)**

Device endpoint types: Cisco Jabber, IP Phones, Telepresence systems.

Purpose	**Transport**	**Protocol**	**Atea Anywhere (listening)**
Real-Time Protocol (RTP), Secure Real-Time Protocol (SRTP)	UDP	RTP/SRTP	16384 - 32767
IM-Only Screen Share	TCP		49152 - 65535
Peer to peer file transfers. The client also uses this port to send screen captures.	TCP / UDP	SOCKS5 Bytestreams	37200

3. **Outgoing traffic to Atea Anywhere (88.151.163.0/24) over internet (MRA-mode)**
   Device endpoint types: Cisco Jabber, IP Phones, Telepresence systems.

Purpose	Protocol	Internet Endpoint (source)	Atea Anywhere (listening)
XMPP (IM and Presence)	TCP	>=1024	5222
HTTP proxy (UDS)	TCP	>=1024	8443
Media	UDP	>=1024	36002 - 59999
SIP signaling	TLS	>=1024	5061

4. **Outgoing traffic to Atea Anywhere VMR (Virtual Meeting Room) (88.151.163.0/24) over internet.**
   Required for device endpoint: Virtual Meeting Rooms via WEB Browser
   Outgoing traffic from the customer network to internet

Purpose	Protocol	Internet Endpoint (source)	Atea Anywhere (listening)
HTTPS	TCP	>=1024	443
Media	TCP + UDP	>=1024	40000 - 49999

##