xtendx®
corporate media solutions

Firewall-Konfiguration
Simplex Meeting

Kontakt xtendx:

support@xtendx.com

xtendx®
corporate media solutions

Benötigte Netzwerkeinstellungen für simplex Meeting

simplex Meeting nutzt im geeigneten Fall eine direkte Peer-to-Peer Verbindung. Dies verringert die Störungsanfälligkeit und die Verzögerung von Audio und Video Signalen.

Die Einstellungen sind üblicherweise in der Standardkonfiguration verbreiteter Router und Firewalls bereits standardmässig so gesetzt. Unter Umständen müssen jedoch bestimmte Netzwerk- und Firewall-Anpassungen vorgenommen werden.

Port Forwarding

Port Forwarding ist für die Verwendung von simplex Meeting nicht erforderlich. Es müssen keine Ports explizit für eingehenden Verkehr geöffnet werden.

Vorgehensweise

Bei optimaler Konfiguration besteht folgender Verbindungsverlauf:

1. Betreten des simplex Meeting Meetings
2. Kontakt zum simplex Meeting Server via TCP zur Aushandlung des Datenverkehrs
3. Direkter Kontakt zu den Teilnehmern via UDP.
4. Falls 3 fehlschlägt: Benutzung der simplex Meeting ICE/STUN/TURN Servers als Proxy mit UDP.

TCP ausgehend

Die ausgehende TCP Verbindung wird verwendet, um den nachfolgenden Datenverkehr auszuhandeln.

Für die Aushandlung wird das STUN Protokoll eingesetzt (RFC 5389).

Erlauben Sie ungefilterten*, ausgehenden Datenverkehr zu folgenden Adressen auf den Ports 80, 443 und 5349: 46.231.204.8 und 46.231.204.6

*) Das STUN Protokoll unterscheidet sich von dem HTTP Protokoll und kann durch Technologien wie DPI negativ beeinflusst werden.

UDP ausgehend

Die ausgehende UDP Verbindung wird für die eigentliche Audio- und Video-Kommunikation sowie für Peer-to-Peer Datenkanäle von simplex Meeting eingesetzt.

Ausgehende UDP Verbindungen sollte auf allen Ports aktiviert werden. Für das WebRTC Protokoll sind keine statischen Ports definiert. Die kommunizierenden Systeme suchen sich aus der lokalen Portliste einen freien Port für die Kommunikation aus. (Siehe https://en.wikipedia.org/wiki/Ephemeral_port).

Sollte es nicht möglich sein, ausgehendes UDP für alle Adressen zu aktivieren, so sollte es mindestens für die im Kapitel „TCP ausgehend“ angegebenen IP Adressen aktiviert werden.

Es müssen keine eingehenden Ports geöffnet werden.

UDP hole punching

Sitzungspartner kommunizieren wenn möglich mittels UDP hole punching (Siehe: https://en.wikipedia.org/wiki/UDP_hole_punching). Diese Vorgehensweise ist bei VoIP Applikationen verbreitet.

Diese Technologie funktioniert nicht wenn beide Partner symmetrisches NAT oder sog. „Restricted cone NAT“ einsetzen.

xtendx®
corporate media solutions

Firewall Anforderungen

Die unten beschriebenen Firewall-Einstellungen können je nach Anwendungsfall und Rechencenter-Umgebung weiter eingeschränkt werden. Sie sind nur indikativ. Bitte konsultieren Sie uns für weitere Details.

Web Server

Input

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[1]	Accept	TCP	Any	Any	Any	22
HTTP	Accept	TCP	Any	Any	Any	80
HTTPS	Accept	TCP	Any	Any	Any	443
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any

Output

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[2]	Accept	TCP	Any	22	Any	Any
HTTP	Accept	TCP	Any	80	Any	Any
HTTPS	Accept	TCP	Any	443	Any	Any
SMTP	Accept	TCP	Any	25	Any	Any
DNS	Accept	TCP	Any	53	Any	Any
DNS	Accept	UDP	Any	53	Any	Any
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any

Database Server

Input

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[3]	Accept	TCP	Any	Any	Any	22
MongoDB	Accept	TCP	Any	Any	Any	27017
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any

Output

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[4]	Accept	TCP	Any	22	Any	Any
MongoDB	Accept	TCP	Any	27017	Any	Any
DNS	Accept	TCP	Any	53	Any	Any
DNS	Accept	UDP	Any	53	Any	Any
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any

TURN and Video Bridge Server

Input

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[5]	Accept	TCP	Any	Any	Any	22
TURN	Accept	TCP	Any	Any	Any	80
TURN	Accept	UDP	Any	Any	Any	80
TURN	Accept	TCP	Any	Any	Any	443
TURN	Accept	UDP	Any	Any	Any	443
TURN	Accept	TCP	Any	Any	Any	3478-3479
TURN	Accept	UDP	Any	Any	Any	3478-3479
TURN	Accept	TCP	Any	Any	Any	32768-65535
TURN	Accept	UDP	Any	Any	Any	32768-65535
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any

Output

Description	Policy	Protocol	Source IP	Source Port	Destination IP	Destination Port
SSH[6]	Accept	TCP	Any	22	Any	Any
TURN	Accept	TCP	Any	80	Any	Any
TURN	Accept	UDP	Any	80	Any	Any
TURN	Accept	TCP	Any	443	Any	Any
TURN	Accept	UDP	Any	443	Any	Any
TURN	Accept	TCP	Any	3478-3479	Any	Any
TURN	Accept	UDP	Any	3478-3479	Any	Any

TURN	Accept	TCP	Any	32768-65535	Any	Any
TURN	Accept	UDP	Any	32768-65535	Any	Any
DNS	Accept	TCP	Any	53	Any	Any
DNS	Accept	UDP	Any	53	Any	Any
Loopback	Accept	TCP	127.0.0.1	Any	127.0.0.1	Any
Loopback	Accept	UDP	127.0.0.1	Any	127.0.0.1	Any
Default	Drop	Any	Any	Any	Any	Any