Firewall/Router Configuration Guide

for Fusion Connect Voice Services

To ensure Fusion Connect VoIP traffic can pass between your network and ours, certain settings need to be applied on your firewall or router.

Depending on the make and model of your equipment some of these settings may not be present or necessary. If you have multiple routers or firewalls, you may need to apply these on each of them.

Begin by testing your service – if you find no problems, then no changes are needed. Fusion Connect VoIP works on most networks with no special configuration.

If you have problems, check the “Common Issues” section first, which will resolve most issues.

If you suspect your firewall, check the “Firewall Configuration” section for recommended settings.

Common Issue #1

UDP Timeout

This setting is known by multiple names, including:

- UDP timeout
- UDP session timeout
- UDP NAT timeout
- Session TTL

On most equipment it defaults to between 60 and 300 seconds. If yours is below 60 seconds it will result in reliability issues.

If your router/firewall can define this on a per-protocol basis, follow the “Protocol Setting” section.

If it does not have that capability (many small-business routers/firewalls do not), follow the “Global Setting” section.

Per-Protocol Fix

In your router/firewall configuration, build a rule as follows:

- **From**: LAN interface
- **To**: WAN interface
- **Protocol**: UDP
- **Destination port**: 5060 *or* 5089
- **UDP/session timeout**: 700 seconds

Apply this rule and restart your router/firewall to clear the network session list.

Global Fix

In your router/firewall configuration, locate the setting for UDP timeout. Set the value to 70 seconds. Save the setting and restart your router/firewall to clear the network session list.

Common Issue #2

Application Layer Gateway (ALG)

Many routers and firewalls have an ALG feature that can **interfere** with our traffic. It is known by several names, depending on manufacturer:

- SIP ALG
- Voice ALG
- VoIP ALG
- SIP Helper
- SIP Transformations

The location of the setting varies between manufacturers and models.

Some routers/firewalls have an entire configuration page dedicated to different Application Layer Gateway features. If yours has such a page, look for a “SIP” setting and disable it.

Check your router/firewall configuration for any setting matching this description and disable it if you are having **one-way audio, phone registration issues**, or other **unusual behavior**.

Common Issue #3

DNS SRV Resolution

Certain routers/firewalls have problematic DNS support. Specifically, they lack support for “SRV” type DNS records, which are rarely used outside of VoIP.

If your router/firewall cannot be configured to deliver DNS servers that support SRV, contact Fusion Connect Support. Depending on your service type, we can either switch to an “A record” or apply special configuration to resolve the issue.

The instructions below will allow you to test for SRV support from a PC.

Windows

1. Open the Command Prompt by either:
   - Locating it in the Start menu
   - Going to Start → Run and typing "cmd"

2. Enter this command and press enter:
   nslookup -type=all _sip._udp.ca01-access.megapathvoice.net

3. The results should look something like this:

```
Non-authoritative answer:

_sip._udp.ca01-access.megapathvoice.net SRV service location:
          priority       = 1
          weight         = 50
          port           = 5060
          svr hostname   = lsancagb-access01.megapathvoice.net
_sip._udp.ca01-access.megapathvoice.net SRV service location:
          priority       = 2
          weight         = 50
          port           = 5060
          svr hostname   = asbnvacz-access01-fo.megapathvoice.net
```

   Note that there are two entries that say "SRV service location". If you do not see any lines that say this, or if you get an error such as "non-existent domain," the router does not support SRV.

Mac / Linux

1. Open the Terminal app (Mac) or shell (Linux)

2. Enter this command and press enter:
   host -t SRV _sip._udp.ca01-access.megapathvoice.net

3. The output should look something like this:

```
_sip._udp.ca01-access.megapathvoice.net has SRV record 2 50 5060 asbnvacz-access01-
fo.megapathvoice.net.

_sip._udp.ca01-access.megapathvoice.net has SRV record 1 50 5060 lsancagb-
access01.megapathvoice.net.
```

4. Note there are two entries that say "has SRV record." If you do not see any lines that say this, or if you see "not found: 3(NXDOMAIN)," the router does not support SRV records.

Firewall Configuration

If your firewall is **highly restrictive**, it could block Fusion traffic. Note that this is **not usually the case** – the majority of firewalls permit most outbound traffic by default, and you should not need to make these changes.

If all else fails and you believe your firewall is at fault, you can **whitelist** traffic to Fusion's servers. The correct set of addresses varies based on your service type.

A note on hostnames: We provide hostnames when possible. If you can whitelist by hostname *and* IP address, do both, but if you can only do one, use IP addresses, which are more reliable with our service.

Microsoft Calling Services (Teams)

Please note: Parts of Teams service depend on systems provided by Microsoft, with which Fusion partners with, however we do not have any control. The information below may be changed at any time without notice; if you experience problems with chat, sharing, or other non-voice services, check for updated documentation from Microsoft which is located here - Skype for Business Online and Microsoft Teams.

Server Address	Ports
13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	UDP: 3478, 3479, 3480, 3481
*.lync.com, *.teams.microsoft.com, teams.microsoft.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443, 80
*.broadcast.skype.com, broadcast.skype.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443
*.sfbassets.com	TCP: 443, 80
*.keydelivery.mediaservices.windows.net, *.msecnd.net, *.streaming.mediaservices.windows.net, ajax.aspnetcdn.com, mlccdn.blob.core.windows.net	TCP: 443
aka.ms, amp.azure.net	TCP: 443
*.users.storage.live.com	TCP: 443
*.adl.windows.com	TCP: 443, 80
*.skypeforbusiness.com 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14, 52.238.119.141/32, 52.244.160.207/32, 2603:1027::/48, 2603:1037::/48, 2603:1047::/48, 2603:1057::/48, 2620:1ec:6::/48, 2620:1ec:40::/42	TCP: 443
*.msedge.net, compass-ssl.microsoft.com	TCP: 443

*.mstea.ms, *.secure.skypeassets.com, mlccdnprod.azureedge.net, videoplayercdn.osi.office.net	TCP: 443
*.tenor.com	TCP: 443, 80
*.skype.com	TCP: 443, 80

FusionWorks

The below applies to **Hosted** and **Trunking** products; if you are using **Webex**, ensure you follow that section as well as this one.

Primary VoIP Servers

64.190.143.0/24
50.20.30.0/24
216.86.44.0/24
50.21.36.0/24

Primary VoIP Provisioning Servers

72.245.184.0/24

Ports

It is safe to allow traffic on all ports to our servers. If you need to restrict it, use these ports:

Content	Protocol	Port
SIP Signaling	TCP/UDP	5060
SIP Signaling	TCP/UDP	5089
RTP Audio/Video	UDP	45000-65001

FusionWorks with Webex

Please note: Parts of Webex service depend on systems provided by Cisco Networks, with which Fusion partners, but over which we do not have any control. The information below may be changed at any time without notice; if you experience problems with chat, sharing, or other non-voice services, check for updated documentation from Cisco.

Ports

Content	Protocol	Port
TLS Signaling	TCP	443
TLS Signaling	TCP	444
SRTP Audio/Video	TCP/UDP	5004
SRTP Audio/Video	TCP/UDP	9000
SRTP Audio/Video	TCP/UDP	33434

Webex Service IP Addresses

IP subnets for media services		
3.22.157.0/26	18.181.204.0/25	69.26.160.0/19
3.25.56.0/25	18.230.160.0/25	114.29.192.0/19
3.101.70.0/25	20.50.235.0/24	150.253.128.0/17
3.101.71.0/24	20.53.87.0/24	170.72.0.0/16
3.101.77.128/28	20.68.154.0/24	170.133.128.0/18
3.235.73.128/25	23.89.0.0/16	173.39.224.0/19
3.235.80.0/23	40.119.234.0/24	173.243.0.0/20
3.235.122.0/24	44.234.52.192/26	207.182.160.0/19
3.235.123.0/25	52.232.210.0/24	209.197.192.0/19
18.132.77.0/25	62.109.192.0/18	210.4.192.0/20
18.141.157.0/25	64.68.96.0/19	216.151.128.0/19
18.181.18.0/25	66.114.160.0/20	
18.181.178.128/25	66.163.32.0/19	

FusionWorks Pro/FusionSIP

Primary VoIP Servers

sip.thevoicemanager.com	65.48.100.36
sip2.thevoicemanager.com	216.86.41.69
sip3.thevoicemanager.com	216.86.41.166
sip7.thevoicemanager.com	216.86.41.200
sipnyc.thevoicemanager.com	216.86.42.230

Config Servers

ftp.thevoicemanager.com	65.48.100.98
cpeprovprod.fusionconnect.com	216.132.113.168

NTP Server

ntp.thevoicemanager.com	65.48.98.50 – 65.48.98.52

Ports

It is safe to allow traffic on all ports to our servers. If you need to restrict it, use these ports:

Content	Protocol	Port
SIP Signaling	TCP/UDP	5060 -5061
SIP Signaling	TCP/UDP	5090 -5091
SIP Signaling	TCP/UDP	6000 -6001
RTP Audio	UDP	1024-65535
RTP Audio	UDP	10000 - 65000

Vendor Specific IP Information

Grandstream:

- https://www.gdms.cloud/server/info/index.html/#/

Poly:

- https://info.ztp.poly.com/assets/files/ip-ranges-085cb3501e6d53f36ac751b7684b60ed.json

Yealink:

- https://support.yealink.com/en/portal/knowledge/show?id=035c46eea77827eb20d53a4d

Readynet:

- Uses TR069 to the domain of acs.readynetsolutions.com (162.243.141.241)

DataRemote:

Inbound and Outbound Traffic

Purpose	Network Address	Protocol	Destination Ports
RTP ENHANCED MODEM/FAX/ALARM	12.44.197.0/24 12.11.243.0/24 12.22.54.0/24	UDP	10000-40000

Outbound Traffic Only

Purpose	Network Address	Protocol	Destination Ports
MANAGEMENT	142.215.242.0/24 12.44.197.0/24	TCP	443,8883
MANAGEMENT	0.0.0.0/0	TCP	443
EMAIL ALERTS	0.0.0.0/0	TCP	465,587,2525
WAN FAILOVER	8.8.8.8/32 8.8.4.4/32 1.1.1.1/32	ICMP	
DNS	8.8.8.8/32 8.8.4.4/32	TCP & UDP	53
DHCP	0.0.0.0/0	DHCP	67
NTP	0.0.0.0/0	UDP	123
RTP ENHANCED MODEM/FAX/ALARM	12.44.197.0/24 12.11.243.0/24 12.22.54.0/24	UDP	10000-40000