Network Configuration Guide

FUSE NETWORKS

Cloud VoIP Network Configuration Guide

PURPOSE

This document outlines the recommended VoIP configuration settings for customer provided Firewalls and internet bandwidth requirements to support Mitel phones. The firewall should be able to protect the network from malicious Internet threats, prioritize VOIP traffic (via QOS), and allow access rules for Cloud VoIP services.

Internet Bandwidth & Calculations

Mitel phones are IP based and thus require a certain amount of internet bandwidth to function properly in a customer environment. The below calculation represents the total amount of bandwidth (Mbps) consumed per call. (Includes Ethernet overhead and encapsulation) It is recommended the overall site bandwidth assume 50% of the number of phones are simultaneously on a call.

Bandwidth Calculation	(100 kbps per call)*(2 rtp streams)/1000 kbps = .2 Mbps]

Cloud VoIP Phone Port Access

The following TCP/UDP ports are required, and must be permitted in the firewall access rules to allow the Mitel phones proper network communication (NAT port-forwarding is not to be configured). Typically, these ports are allowed access by default however, if stricter access rules are applied then, the following ports must be allowed:

Secure MiNet Remote Config	Multiple HTTPS connections over TCP port 443 to IP address 216.191.234.139
Secure MiNet Signaling	Multiple TCP connections must be allowed on ports 6801 and 6802. Heartbeat keep-alive every 30 seconds (TCP port 6801)
HTTP	Multiple HTTP connections over TCP ports 80, and 6880
HTTPS	Multiple HTTPS connections over TCP ports 80, 443, and 6880
TFTP	Multiple TFTP connections over UDP ports 69 and 20001 for Phone Firmware
SIP Signaling	Multiple TCP and UDP connections must be allowed on ports 5060 and 5061
SAC Signaling	Multiple TCP connections must be allowed on ports 3998, 3999, 6880 and 6881
App Signaling	Internally-initiated TCP requests must be allowed on ports 35,001 to 35,007 Internally-initiated TCP requests must be allowed on ports 36,000 to 36,009
RTP/Audio	Internally-initiated UDP requests must be allowed on ports 20,000 to 31,000

SIP Trunk Port Access

The following UDP ports are only for premise based SIP Trunks, and Cloud VoIP Enterprise customers with strict firewall policies (NAT port-forwarding is not to be configured):

SIP Trunk Signaling	Multiple UDP connections must be allowed on port 5060 SIP Trunk Registration Timer every 300 seconds *(destination IP address to be determined by your project/account manager*, UDP port 5060)
RTP/Audio	Internally-initiated UDP requests must be allowed on ports 20,000 to 52,500

Cloud VoIP IP Access

The following IPv4 address blocks must be permitted for Cloud VoIP Business or Enterprise services

Description	Block	Net mask	Wildcard
Seattle Block	63.232.60.64	255.255.255.192	0.0.0.63
Seattle Block	66.77.107.128	255.255.255.192	0.0.0.63

Cloud VoIP Enterprise Border Gateway IP Blocks

These subnets are exclusive to the virtual hosted environment, and will be provided by the System Implementation Specialist (SIS).

Description	Block	Net mask	Wildcard
Seattle Block	63.232.60.64	255.255.255.192	0.0.0.63
Seattle Block	66.77.107.128	255.255.255.192	0.0.0.63

SIP Trunk, Session Border Controller IP Blocks

These IP blocks are only for Premise based SIP Trunks, and Cloud VoIP Enterprise customers.

Description	Block	Net mask	Wildcard
Seattle Block	63.232.60.64	255.255.255.192	0.0.0.63
Seattle Block	66.77.107.128	255.255.255.192	0.0.0.63

Cloud VoIP Business Border Gateway Blocks

These blocks are for Cloud VoIP Business customers, and allow the Mitel Phones to communicate with Cloud VoIP Business services.

Description	Block	Net mask	Wildcard
Seattle Block	63.232.60.64	255.255.255.192	0.0.0.63
Seattle Block	66.77.107.128	255.255.255.192	0.0.0.63

Cloud VoIP DNS Requirements

For Mitel phones to register and communicate properly with Fuse Cloud VoIP Services, Mitel phones must be able to reach a primary DNS server that is capable of resolving external (public) DNS hostnames. (e.g. *.fusenetworks.com; *.fusevoip.net)

Cable or DSL Modems – Bridge Mode Required

ISPs providing Cable or DSL modem services must have the modem configured in “bridge mode” when connecting to the premise firewall. In “bridge mode,” the modem functions only as a modem (disabling duplicate NAT & Routing) and forwards all incoming traffic to the directly connected firewall.

NAT UDP Session Limits

When a call is placed with a Mitel phone, the local Firewall establishes a NAT session with the Cloud VoIP Border Gateways. If the firewall has aggressive NAT session timeout policies then, the Mitel phones will not function properly due to an untimely UDP session termination. The recommended NAT UDP session timeout is 300 seconds before the Firewall terminates the UDP session.

NAT Port Consistency

Best practice dictates to enable Consistent NAT for VoIP traffic on the firewall configuration. NAT consistently references a consistent map of the same Public IP address and Port pair to each phone’s internal private IP address and port pair during an NAT session.

SIP Applications Settings

Best practice is to disable any SIP assistance settings in the Firewall configuration (i.e. SIP ALG or SIP Transformations). When the Firewall attempts to manipulate VoIP/SIP traffic, this will often corrupt SIP messages, and cause the phones to not function properly.

Load Balancing & Failover Configuration

When a Mitel phone is powered-on, the phone will register the local Firewall’s Public NAT IP address with the Cloud VoIP Boarder Gateways. If load-balancing is configured on the Firewall with multiple ISP connections, then the Mitel phones might take a different path without registering the appropriate Public IP. This can cause a number of functionality problems, including one-way audio issues. For this reason, the following load-balancing configurations should not be used for VoIP traffic-

- ✓ Round-robin
- ✓ Spillover
- ✓ Percentage-based configurations

If the Firewall has multiple ISP connections then, an Active/Passive failover configuration is recommended for VoIP traffic with a 90 second timeout minimum.

Prioritization of VoIP Traffic (QOS)

All network traffic is subjected to bandwidth limitations, congestion, delay, and packet loss. When Voice over IP (VoIP) traffic travels across these network hazards, voice quality problems can occur. Quality of Service (QOS) is the set of techniques used to avoid the trenches of poor network performance, and ensure prioritization of Voice traffic.

Best practice is to implement QOS techniques on LAN and WAN connections. We recommend network segmentation of the voice traffic and then configuring priority Voice QOS policies.

Separating the LAN Traffic

There are a number of methods for separating voice and data traffic that might best fit the network environment and cost. The benefit of separating LAN traffic ensures data traffic will not affect voice traffic across the LAN connections.

QOS – DSCP & COS Values

The Mitel IP phones assign a DSCP & CoS value to voice traffic; these values are defined by the DHCP server option 125 or 43. If the Mitel IP Phone will not be using DHCP server options, the IP phone can be placed into Teleworker mode, and the DSCP value is set by default.

Firewalls and Router can be configured to honor OSI Layer 3 DSCP values. This is how traffic is managed on a shared WAN connection.

Switches are typically configured to honor OSI Layer 2 802.1p/CoS values. Some switches have the enhanced capability to map CoS to DSCP values, and honor Layer 3 values.

DSCP/COS Value Information Chart

Traffic Type	DSCP Value	802.1p/CoS Value
Secure Minet Signaling	26	6
SIP Signaling	26	6
RTP/Audio	46	6

DHCP Server Option 125 or 43

Mitel IP Phones use one of two vendor specific DHCP options- 43 or 125. Either can be used, it just depends upon the support capabilities of the DHCP server.
Refer to the DHCP server manufacturer's instructions for the process to add an option. If VLANs are configured, the DHCP option will need to be added in both the data and voice scope.

If VLANs are not configured, here is an example DHCP string:
id:ipphone.mitel.com;sw_tftp=63.232.X.X;call_srv=63.232.X.X;l2p=6v6s6;dscp=46v46s26

For deployments with VLANs configured, here is an example DHCP string:
id:ipphone.mitel.com;sw_tftp=63.232.X.X;call_srv=63.232.X.X;vlan=20;l2p=6v6s6;dscp=46v46 s26

String Information:

- ipphone.mitel.com; – Vendor ID
- sw_tftp; – TFTP server for firmware, MCD or MBG (assign same call_srv).
- call_srv; – MCD or MBG (must be same address as sw_tftp)
- vlan; – VLAN ID of the dedicated Voice VLAN for Mitel IP Phones.
- l2p; – COS/Layer2/Frame Priority, prioritizing voice traffic at the Switch layer.
- DSCP; – QOS/Layer3/Packet Priority, prioritizing voice traffic at the Firewall or Router layer.

Detailed Mitel Phone Port List

Destination Port	Transport	Description	Function	DSCP
80	TCP	HTTP - Browsing	Application	0
443	TCP	HTTPS - Browsing	Application	0
3998	TCP	SAC - Display phones	Signaling	26
5060	TCP	SIP - Signaling	Voice	46
5061	TCP	SIP - Signaling (TLS)	Voice	46
6050	UDP	VoIP Testing	Voice	46
6801	TCP	Secure MiNet	Signaling	26
6802	TCP	Secure MiNet	Signaling	26
6806	TCP	Console	Signaling	26
6807	TCP	Console	Signaling	26
6880	TCP	HTTPS - Browsing	Application	0
20000 - 31000	UDP	Voice Streaming	Voice	46
30000 - 60000	UDP	VoIP Testing	Voice	46
35001 - 35007	TCP	Handset Applications	Signaling	26
36001 - 36009	TCP	Handset Applications	Signaling	26
20001	UDP	TFTP	Application	0
48879		IPA Monitor	Application	0
50000 - 50511	UDP	Voice Streaming	Voice	46