MiVoice Border Gateway Engineering Guidelines

Mitel®

Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

About this Document

Overview

The purpose of this document is to describe configuration rules, provisioning, and performance information for the MiVoice Border Gateway, and associated products in order to assist in sales and support of this product. This information is intended for Training, Sales and Product support staff and complements other sales material and product documentation.

NOTE: The Secure Recording Connector (SRC) has been consolidated into MBG. Accordingly, although this document discusses the SRC control interface and its protocol, it does not treat them SRC as a separate feature.

Prerequisites

The MiVoice Border Gateway application runs on the Mitel Standard Linux (MSL) Server. The reader should first become familiar with the *MSL Installation and Administration Guide* and the *MSL Qualified Hardware List*. These documents are available here.

About the MBG Documentation Set

Mitel documentation is available on mitel.com. The following guides provide complete information about MBG:

- The MBG Engineering Guidelines (this document).
- The MBG Installation and Maintenance Guide provides information about system requirements, installation of MBG, and configuration of MBG options and firewalls.
- The MiVoice Border Gateway Online Help provides information about MBG configuration and maintenance.
- The Remote IP Phones Configuration Guide provides information about configuring remote phones.

Supported Configurations

Services

MBG provides the following services:

- **Remote MiNet IP Phones**: The classic use of MBG, formerly known as the Teleworker Solution, permits remote MiNet phones to securely access the corporate phone network over the Internet.
- **Remote SIP IP Phones**: Permits Teleworker functionality for SIP hard or soft phones over the Internet.
- **SIP Trunking**: Allows a corporate phone switch to connect to a SIP Trunk provider, protecting the switch from malformed messages, unauthorized use, and various attacks, and providing an anchor point for media streams.
- **Call Recording**: Formerly the Secure Recording Connector, this service allows secure recording of phone calls by a third-party application.
- **WebRTC**: A gateway to support browser-based voice and video calling. This guide provides information about the requirements and installation procedures of the MiVoice Border Gateway.
- **Remote Proxy**:
  - **Web Proxy**: end-user access from the WAN to applications hosted inside the firewall
  - **Remote Management Service**: administrative access from the WAN to applications hosted inside the firewall

Refer to the Remote Proxy Services documentation for details. MBG can be deployed in several ways depending on the services required.

Teleworkers and Remote Offices

Overview

The original design intent of MBG is to provide a Teleworker solution. Once an MBG server is installed, extensions from the office PBX can be extended across the Internet to permit MiNet phones to work from homes, remote offices, hotels, and so on. As of MBG 10.1 Teleworkers can now be configured in a more flexible way for encrypted audio streaming (SRTP) or unencrypted audio streaming (RTP).

Each side of MBG can be configured independently as follows:

- SRTP on both sides
- SRTP on one side and RTP on the other side
- RTP on both sides

In Teleworker use-case, either the server-gateway profile or DMZ profile could be used depending where on the network MBG is to be deployed. If deploying behind an existing firewall on a DMZ, then a single network interface and DMZ profile is appropriate. If deploying beside an existing firewall, or if there is no existing firewall, then server-gateway profile is appropriate.

Failure to follow these guidelines will result in one-way or no-way audio.

WARNING: Some firewalls which use port-forwarding to simulate a DMZ are Port-forwarding Firewalls. See the *Common Requirements*chapter for full details.

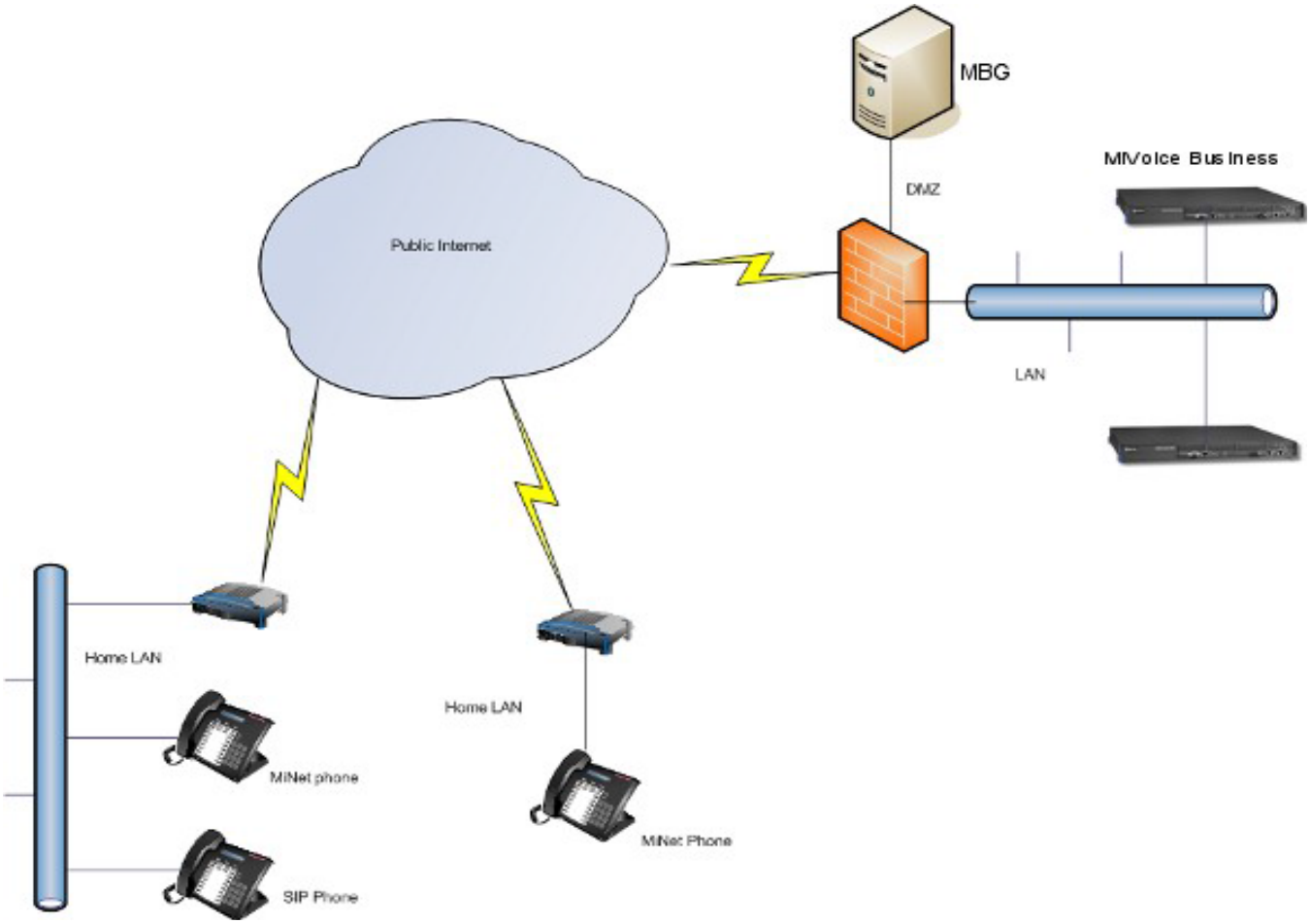


Figure 2.1: MBG in traditional Teleworker configuration

MiVoice Border Gateway as Internet Gateway

Mitel recommends deploying the Mitel Standard Linux server with MiVoice Border Gateway as the Internet gateway and firewall for any enterprise without an existing firewall. Figure 2 shows an example of this configuration using the MiVoice Border Gateway and a MiVoice Business (3300 ICP).

MBG requires two network interfaces and two addresses for this configuration. The external address must:

1. Be a static address that does not change
2. Be directly attached to a NIC on the MSL server
3. Be reachable from the public network/Internet
4. Be reachable from the internal network/LAN
5. Not be subject to NAT or behind another firewall

The interface may be configured via DHCP, PPPoA, PPPoE or similar technology, but the address it receives must always be the same.

WARNING: If the external address changes, all teleworker phones must be reprogrammed with the new address.

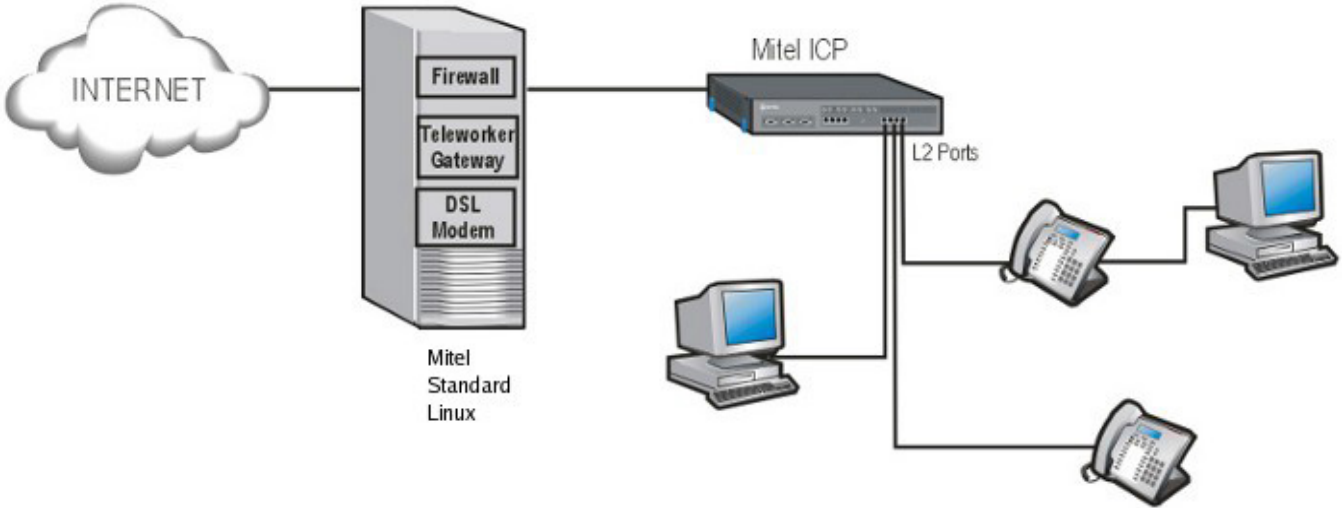


Figure 2.2: MBG as Internet Gateway (no enterprise firewall)

An enterprise can take advantage of the DSL, authenticated DHCP and PPPoE/PPPoA[1] capabilities of the MSL server. Additionally provides NAT for all devices at the enterprise, a stateful packet filter firewall, and optional port-forwarding.

NOTE: If desired and if hardware is available, a third interface may be configured in MSL. This interface might be useful as a dedicated interface for if a network between the MBG servers can be set aside for this purpose. Alternatively, the third interface could be put into bridged mode on MSL 9.2+ to permit an MBG server in parallel with an existing firewall to transparently handle all traffic from that firewall and accomplish traffic shaping. See Traffic Shaping for full details.

Additional Trusted Local Networks

Additional trusted internal networks or subnets that require access to the MiVoice Border Gateway can be added via the Networks panel of the server manager. This access can be limited to individual hosts, or large network blocks can be used. In all cases, the Router property should be set to the address of the router on the subnet attached to the MSL server's internal interface.

For example, to allow access from the single subnet 192.168.12.0/24, you would enter a network of 192.168.12.0 and a mask of 255.255.255.0 in the Local Networks panel, plus the address of the router on the local subnet through which this network can be reached.

If the customer's network has multiple subnets with a common prefix, access can be allowed from the prefix. For example, if the customer uses various subnets within the 192.168.0.0/16 network, enter a network of 192.168.0.0 and mask of 255.255.0.0 in the Networks panel, and allow the local router to determine the routing to the individual subnets.

In addition to providing application access control, the Networks panel can also be used to add static routes.

1. Limited support is provided for PPPoA. Mitel recommends the use of a D-Link DSL 300T modem at the enterprise site if PPPoA connectivity is required in gateway mode. Configure the modem to provide DHCP on the internal interface, and use DHCP on the MSL server to configure the public interface. The modem acts as a bridge. Note that PPPoA routers that provide NAT will not work here.

NOTE: Note: The Networks panel is a feature of MSL. Refer to the MSL documentation for a full description of its capabilities.

MiVoice Border Gateway in a DMZ

The MiVoice Border Gateway can also be deployed behind a customer-provided or customer-managed firewall as shown in Figure 3. This firewall must have 3 network interfaces (ports): WAN, LAN, and DMZ. Two-port firewalls are not supported. It should also be noted that some “DSL routers” with “DMZ” port forwarding are simply two-port NAT devices and should be treated as any other two-port firewall. Deployment of the MiVoice Border Gateway behind such devices is not supported.

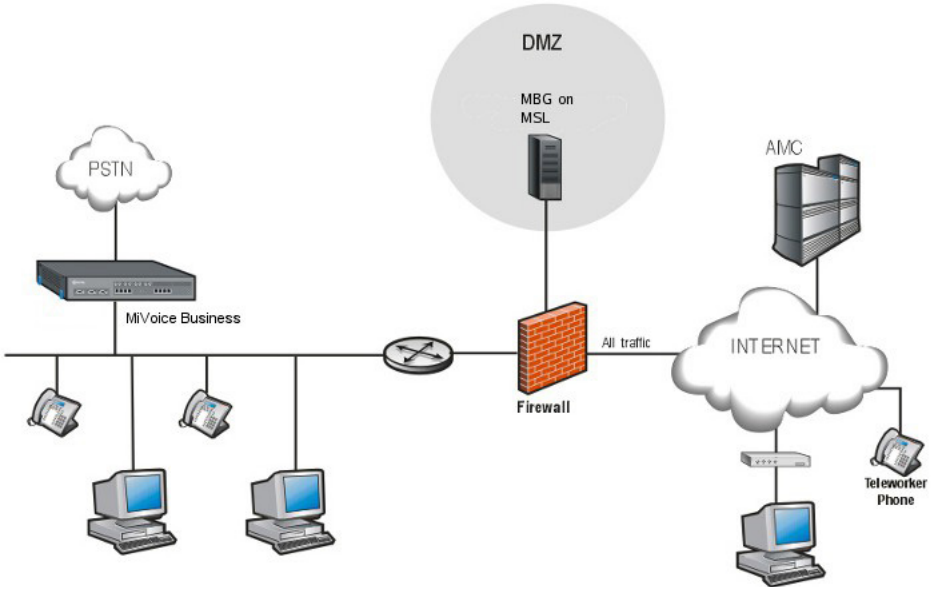


Figure 2.3: MBG deployed in a DMZ

MBG requires one network interface and two addresses for this configuration. The interface must be configured with a static address allocated from the DMZ network range. This is typically an RFC 1918 “private” address. The enterprise firewall must be configured with an address allocated from the public/Internet range. This address must be:

1. reachable from the public network/Internet
2. reachable from the internal network/LAN
3. able to reach the internal network/LAN
4. preferably dedicated solely to MBG, but also see Port-forwarding firewalls

NAT Traversal for Multi-instance MiVoice Business

In a multi-tenant Multi-instance MiVoice Business install, it is possible to find tenant sites with overlapped network ranges, and without NAT at the customer edge network. In this case, MBG can be used to perform between the tenant sets and the Multi-instance MiVoice Business solution.

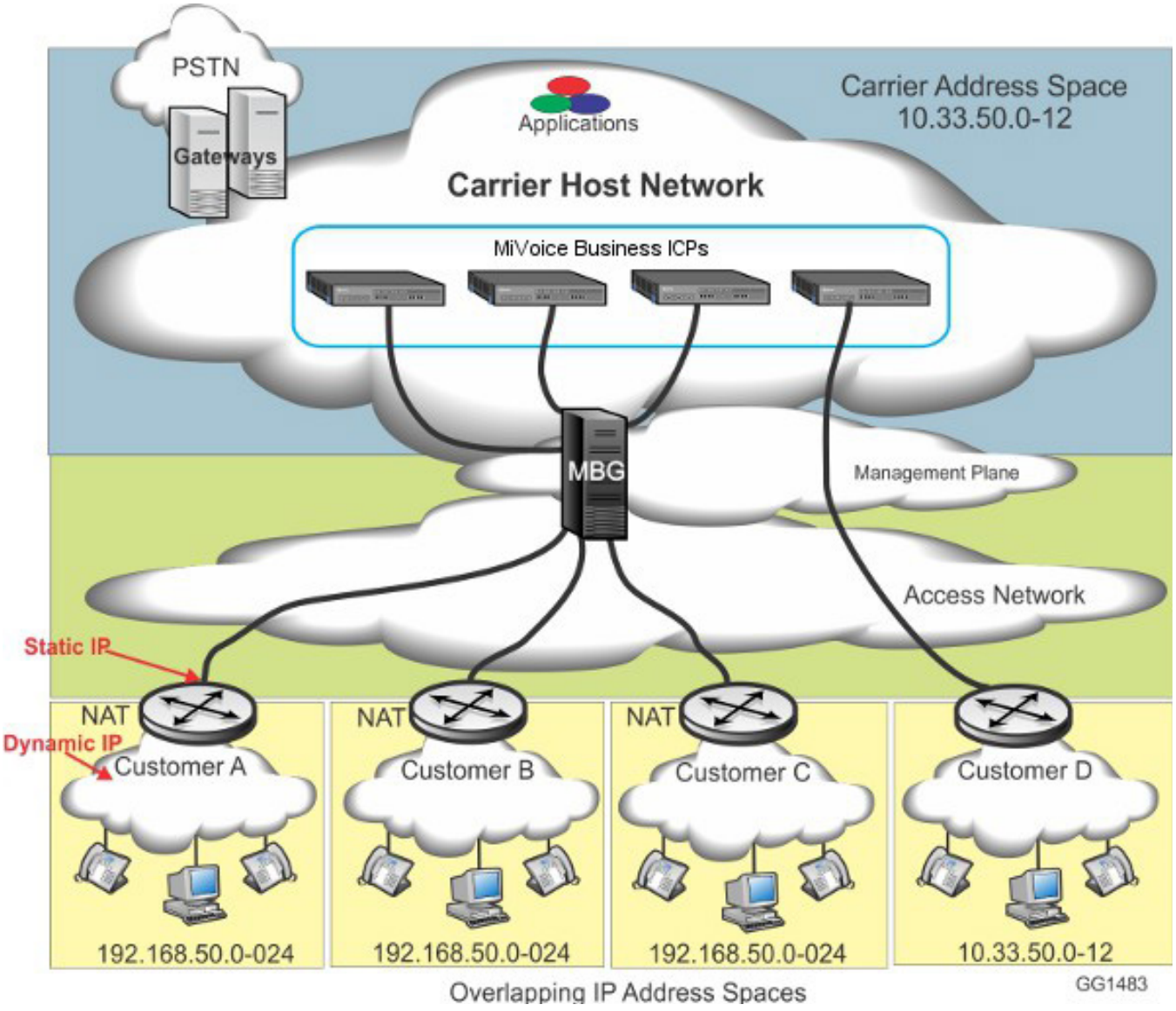


Figure 2.4: MBG providing NAT traversal for Multi-instance MiVoice Business

Secure Gateway for Broadview Networks Silhouette HKS

The Broadview Networks hosted key system provides service to various tenants across leased lines, MPLS circuits, or the Internet from a common carrier. Customers are provided with either MiNet or SIP sets, and the MBG acts as a Session Border Controller for both protocols. DNs are unique within each tenant but may overlap between tenants.

NOTE: Contact Broadview Networks to determine which MBG versions are compatible with silhouette, and for all support inquiries.

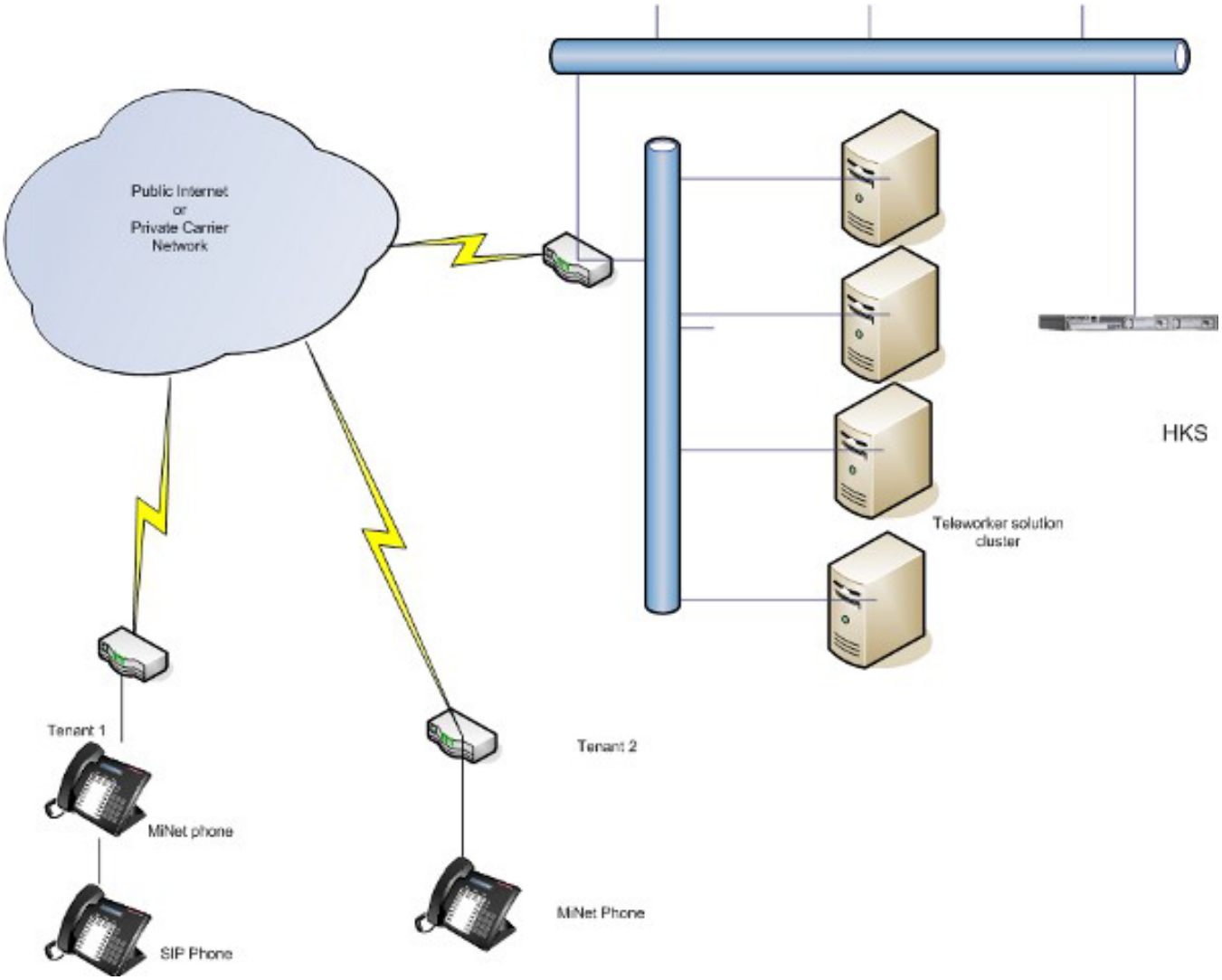


Figure 2.5: MBG as a Gateway for Broadview Networks silhouette

Secure Recording Environment

When MBG is provisioned with call recording licenses, it can provide a secure man-in-the-middle for call recording. This mode is supported only in a LAN environment.

It is advisable to disable MiNet restrictions on the MBG server providing call recording service, as having all LAN sets authenticate through MBG is likely not required.

Teleworker sets connected through an MBG at the network edge can be recorded as well, by configuring the edge MBG such that the desired sets point to the LAN MBG as if it was an ICP.

MBG Deployed on the LAN for Call Recording

When possible, Mitel recommends deploying the MBG call recording server on the same LAN segment as the ICP(s) with which it will be working. However, it is often practical to use a separate segment if not all devices should be recordable.

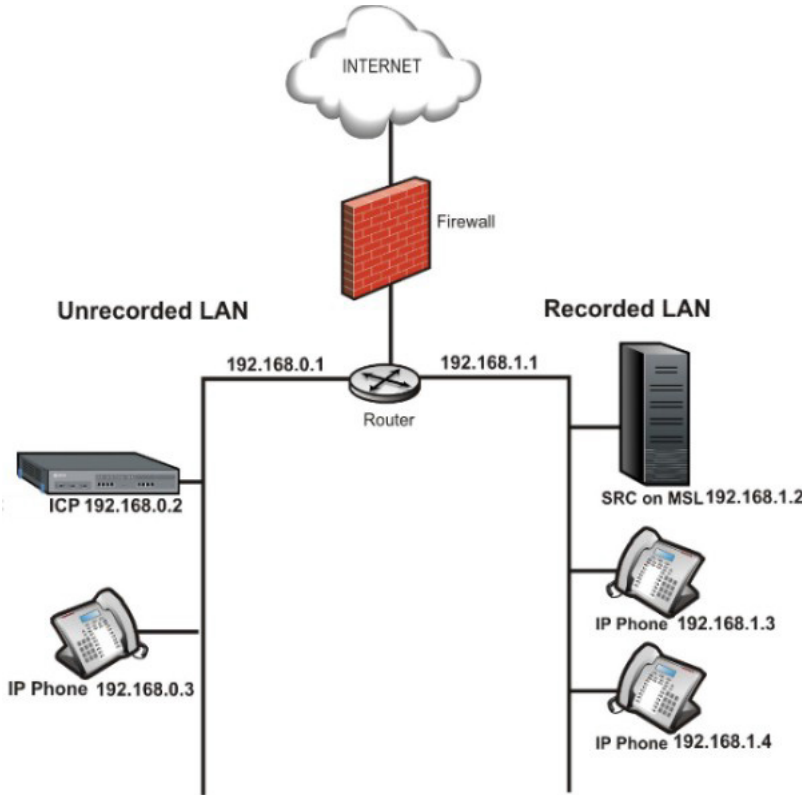


Figure 2.6: MBG Deployed on the LAN for Call Recording

The preceding image shows one sample configuration that could be used. IP phones that are to be recorded are on the same LAN segment as the MBG server. DHCP is enabled in MSL, and MBG provides DHCP configuration such that the sets use the MBG server as their TFTP server and as their ICP. MBG then proxies the set registrations to the real ICP on the other segment. Sets on a different LAN segment using the MiVoice Business DHCP server connect directly to the MiVoice Business and are therefore not recordable.

As an alternative to changing the network topology, each set that should be recordable can be individually programmed to connect to the MBG. Hold down the “7” key and put each set into Teleworker mode. At the prompt, enter the IP address of the MBG.

MBG servers can be chained together to allow recording of remote teleworker phones. Figure 7 below shows an example of a teleworker set connecting through the edge MBG to an MBG server for call recording (and finally to the MiVoice Business), so that it can be recorded along with the sets on the Recorded LAN. To configure this scenario, an “ICP” entry is added to the edge MBG containing the IP address of the LAN MBG used for recording. All remote sets that should be recordable must be configured with that “ICP”. The recording MBG will then proxy the remote sets to their real ICP.

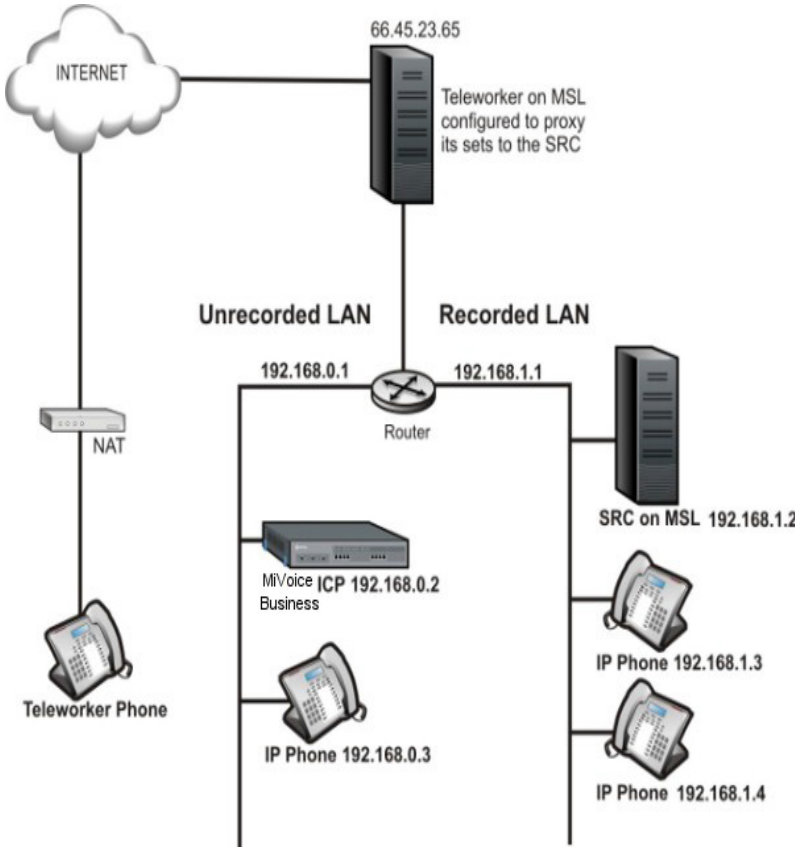


Figure 2.7: Recording Teleworker Sets

NOTE: CIS softphone (MiContact Center) can function properly in this configuration. However, only the signaling and voice should be proxied through the call recording MBG. Additional applications protocols should be proxied directly from the edge MBG to the CIS server.

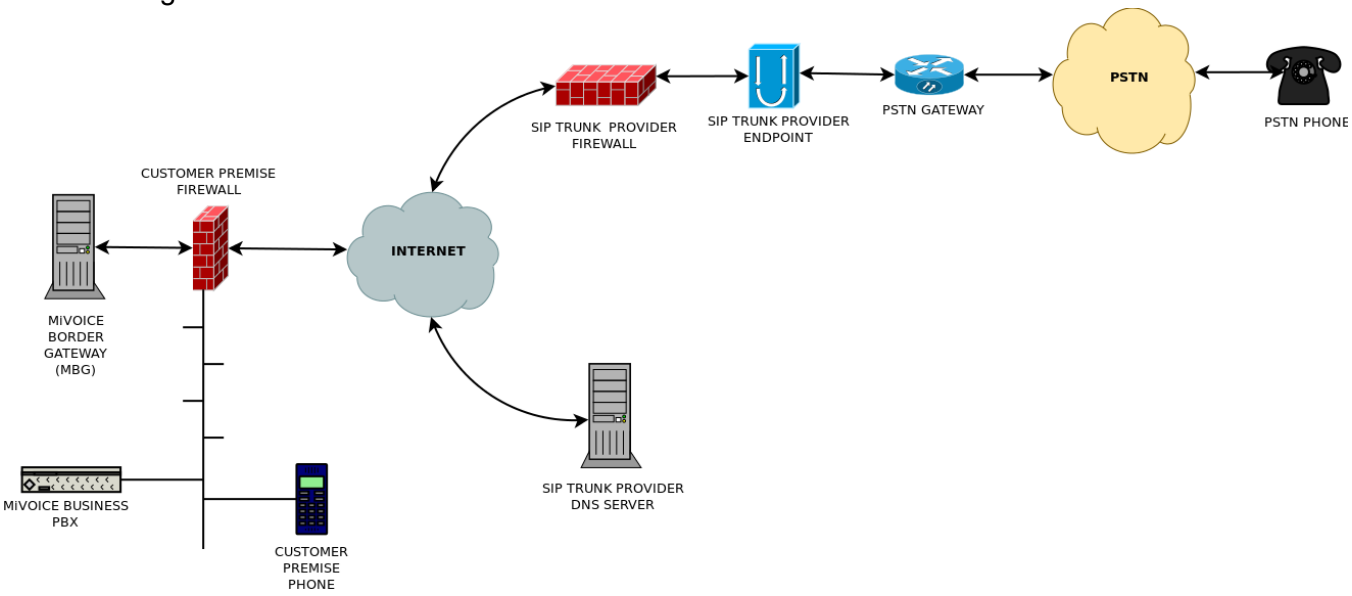
WARNING: This is the only supported way to have both teleworker sets and call recording of LAN sets. Combining teleworker service and call recording of LAN sets on a single server is not supported.

SIP Trunking

MBG introduced support for SIP trunks in release 5.1. The SIP trunk is established from MiVoice Business, MiVoice Office 250, MiVoice MX-One, or MiVoice Office 400 to the SIP trunk provider, using MBG as a SIP-aware firewall and proxy, as shown in figure below. MBG's SIP trunk service provides:

- Support for encrypted audio streaming (SRTP) on the TRUNK side of MBG if the remote TRUNK provider endpoint also supports it.
- Support for encrypted audio streaming (SRTP) on the ICP side of MBG if the remote ICP endpoint also supports it.
- NAT traversal of media and signaling
- Media anchoring for the remote provider, regardless of the internal device
- SIP adaptation and normalization to improve interoperability
- Protection from malformed & malicious requests, various types of attack, and request flooding

When providing SIP trunk service, MBG can be deployed either in the DMZ of, in parallel with, or in place of an existing firewall.



Some of the key benefits of using SIP trunks are:

- consolidation of capacity; all trunks come to one location, calls routed to branch offices over MPLS or VPN links already in place
- increased simplicity for bandwidth management
- local phone numbers from anywhere in the world to permit customers to reach the company in question easily
- cost savings over PRI/T1/POTS lines
- increased resiliency with the potential for disaster recovery configuration

Daisy Chain Deployments

“Daisy Chaining” is a technique of pointing one MBG at another that can work around certain bandwidth and routing restrictions. The servers are configured such that all traffic between the sets and ICPs traverses all MBG servers in series, like following links in a chain.

A “Daisy chained” MBG is one that is configured to accept all incoming requests (authentication is disabled) and pass them “upstream” to another MBG, where the standard authentication is performed.

NOTE: Note: In this context, “upstream” refers to the direction approaching the ICP on the LAN.

WARNING: Daisy-chaining is only supported for MiNet phones. SIP phones, SIP trunking and remote applications such as MiCollab Client are not supported with MBG daisy-chain deployments.

The two main applications of daisy-chaining are to comply with certain IT deployment policies and to reduce bandwidth for remote sites.

Special IT Policy Deployment

Daisy chaining the DMZ MBG server to a LAN MBG server minimizes the scope of the firewall rules required to facilitate communications between them. The firewall administrator can permit traffic only between those two servers instead of across the entire LAN where sets may be located.

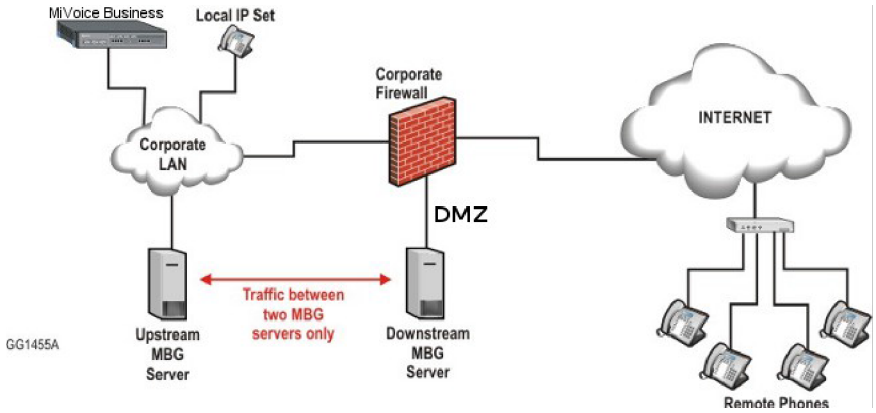


Figure 2.8: Daisy-chained MBGs for enhanced security

This configuration places the downstream server in the DMZ and the upstream server on the LAN. The servers should use the network profiles of DMZ mode and LAN mode, respectively.

NOTE: Authentication should be disabled on the downstream (DMZ) server, and adds/changes should be made only on the upstream (LAN) server.

Reduced Bandwidth for Remote Sites

If MBG is providing access for a remote office environment where the users often call one another, an MBG server can be provided on site and daisy chained to the MBG server at the main office. This is not needed for MiNet to MiNet calls behind the same remote NAT because the MBG local streaming feature will handle that case. However, this deployment can be used to keep MiNet to SIP calls in the remote office. This configuration, illustrated in Figure 10, can save bandwidth on the link between the remote and main offices.

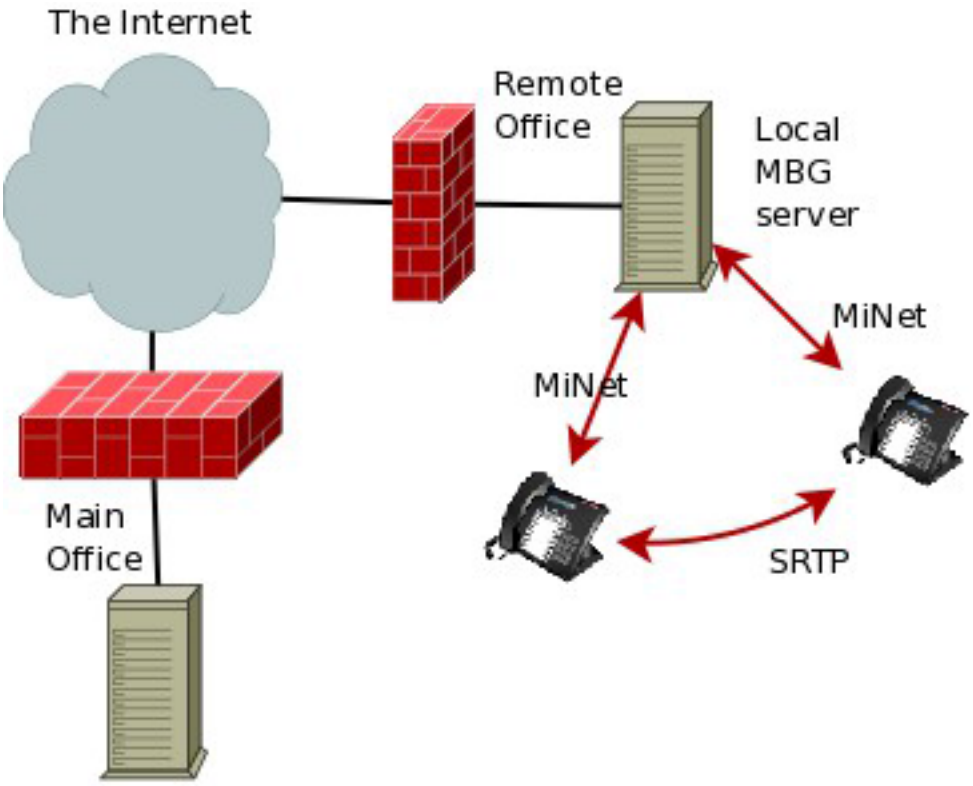


Figure 2.9: Daisy-chained MBGs to save bandwidth

The upstream server can be deployed in either a Gateway or a DMZ configuration.

The remote office (downstream) MBG can also be configured for either a Gateway or DMZ deployment. Note that there is no restriction on the location of the remote office sets; they do not have to be on the LAN. It may be desirable to configure certain teleworker sets to connect to remote office MBGs (rather than the main office MBG) in order to cause direct of those teleworkers' calls to sets in the remote office. This case requires Local streaming to be enabled on the upstream (main office) server.

It is even possible to deploy multiple downstream MBG servers at different remote offices. If upstream (main office) server has Local Streaming enabled, calls within each remote office remain local to that office: signaling still flows back to the main office, but voice streams for calls between offices will only traverse the path between the two MBGs. This minimizes bandwidth use on the main office's connection.

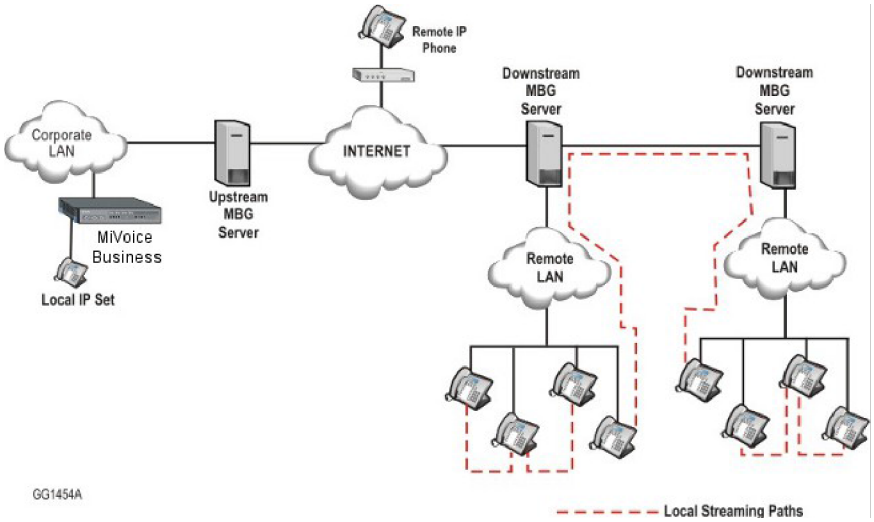


Figure 2.10: Multiple downstream MBGs

NOTE: All MBG servers in the daisy chain must be at the same release.

Refer to the *MBG Installation and Maintenance Guide* for a full description of setting up.

MBG in MiCollab

There are two supported deployments of MBG in MiCollab: on the LAN and on the network edge (Gateway mode). Deployment in the DMZ is not supported.

MiCollab on the LAN

The safest way to deploy MBG is to leave MiCollab and its applications on the LAN, and deploy a second server running MBG (either standalone or single-app MiCollab) in the DMZ or in Gateway mode at the network edge. Remote access to the LAN MiCollab can be provided via on Internet-facing MBG. If centralized management is desired, the two MBG applications can be clustered. All changes made on the LAN server will be reflected on the edge MBG. Refer to the MiCollab documentation set for details on clustering MBG with MiCollab.

MiCollab on the Network Edge

Although Mitel recommends the dual server approach for maximum security, a single MiCollab server with all applications can be deployed in Gateway mode at the network edge. In this configuration, all administrative and end-user web interfaces and all services are directly reachable from the public network; is not required to reach them.

MBG in MiVoice Business Express

The MiVoice Business Express product combines MiCollab and MiVoice Business on one virtual machine. Refer to the *MiVoice Business Express Deployment Guide* for a description of supported **MiVoice Business Express** configurations.

Support for an additional MBG deployment configuration is introduced for MiVoice Business Express environments only because of specific IT constraints imposed by some cloud providers. For MiVoice Business Express deployments only, MBG in server-gateway behind an existing firewall is supported with the constraint that phones must not connect to the MBG from the LAN side of the firewall. That is, this configuration is only supported for phones connecting to the MBG WAN interface via the existing firewall WAN interface.

Partial Service Configurations

All MBG services are not available in all supported configurations. This section identifies for each MBG service configurations where the service is not supported at the time of writing. In some cases the service may be technically possible but not currently supported pending further testing or to reduce complexity.

MBG provides the following services:

- **Remote MiNet IP Phones**
  - Connecting to MBG in MiVoice Business Express is not supported for LAN phones.
  - Connecting to MBG in MiCollab on the LAN is not supported for Internet phones.
- **Remote SIP IP Phones**
  - Connecting to MBG in MiVoice Business Express is not supported for LAN phones.
  - Connecting to MBG in MiCollab on the LAN is not supported for Internet phones.
- **SIP Trunking**
  - Connecting to a SIP trunk service provider from MBG in MiCollab on the LAN is not supported.
- **Call Recording**
  - Connecting to MBG in MiVoice Business Express is not supported for LAN phones.
  - Recording calls with MBG in MiCollab on the network edge is not supported for LAN phones.
  - Recording calls with standalone MBG on the network edge is not supported for LAN phones.
  - Call recording is not available with MBG for the following ICP types: MiVoice Office, silhouette
- **Remote Proxy Services**
  - Remote Proxy Services are not available with MBG in MiCollab.
  - Remote Proxy Services are not available with MBG in MiVoice Business Express.
  - Remote Proxy Services are not available with MBG for the following ICP types: MiVoice Office, silhouette.
- **Web Real-Time Communication (WebRTC)**
  - Browser-based voice and video calling using Google Chrome, Mozilla Firefox and Opera.

Common Requirements

This section provides general guidance common to all types of deployments and all services. Read this carefully.

Administrative Access

MBG provides a web-based management GUI for normal administration, log access, etc. This service can be accessed with any of the following supported web browsers:

- Microsoft Edge 20
- Internet Explorer 9 and higher (do not run in Compatibility View)
- Mozilla Firefox 41 and higher
- Google Chrome 46 and higher

Although not officially supported, the following browsers are tested occasionally and should also work:

- Apple Safari
- Any browser using the Mozilla Gecko engine or the Apple WebKit engine

NOTE: The MBG GUI requires a browser that supports JavaScript. The built-in MSL text-mode browser does not support JavaScript and cannot be used to manage MBG.

Some troubleshooting or advanced configuration requires command-line access. SSH is the only supported mechanism to reach the MSL command line remotely. On Microsoft Windows, Mitel recommends the use of PuTTY (a small, free SSH client). Open SSH is included with Apple Mac OS X (open Terminal and type “ssh”), and is included with or available for most flavors of Unix.

Firewalls (DMZ deployment)

MBG can be deployed into the DMZ of most third-party firewalls. However, a compatible firewall must have certain characteristics.

1. The firewall must provide at least three interfaces: external network, internal network, and DMZ.
2. The firewall must provide static 1:1 NAT between an externally-visible address and the DMZ address of the MBG server.
3. The public address used for MBG must be a static IP address visible from the external network (Internet). This should be a separate address from the external IP address of the firewall, although some firewalls that support port forwarding may allow sharing the address. It is vital that this address actually be static as any change of the address will cause remote sets to lose connectivity.
4. The firewall must preserve the TCP and UDP port numbers in packets exchanged between the MBG and the external network. In other words, only the address field may be changed.

For deployment in a DMZ, MSL must be installed in “server-only” mode with only a single NIC configured. This NIC should be given an address on the DMZ network. The firewall will map between this address and the external address used for MBG.

Details of the protocols that must be configured in the firewall are provided in Firewall Configuration. Particular attention should be paid to the requirement that all UDP ports >= 1024 on the LAN be permitted to reach the public IP of the MBG server.

WARNING: Failure to configure the firewall properly will result in audio problems (typically one-way audio).

Known Issues

Checkpoint “NG” Firewalls

Checkpoint “NG” firewalls (e.g. FireWall-1 NG) have a feature called “Smart Connection Re-use” that may interfere with older MiNet sets and some SIP sets that use a fixed source port for their outgoing connection. The feature should be disabled with older sets or if set connections to the MBG server cannot be maintained.

It is not a problem with newer sets that randomize the source port used for each new connection.

Port-Forwarding Firewalls

Use of MBG server with a port-forwarding firewall (where the external address of the firewall is shared between the MiVoice Border Gateway and other applications) is supported by MBG version 3.0 and higher. The firewall device must have at least 3 interfaces (external, internal, DMZ). This allows for a single external IP address to be assigned to the firewall. It does not eliminate the need for a separate DMZ network.

This special configuration is identical to a normal DMZ deployment with the exception that the MBG’s publicly-visible IP address will be the same as the firewall’s publicly-visible address (that is, the single public IP address is shared).

WARNING: Two-port firewall devices that simulate a DMZ through port forwarding are not supported, even if the device allows multiple external IP addresses.

SIP-Aware Firewalls

Many firewall devices today understand the SIP protocol and include some type of NAT traversal or rewriting of SIP packets. When MBG is used for connecting SIP clients (sets) and trunks, Mitel recommends turning off any SIP features of the main firewall. At best, it is redundant to have two devices performing the same job. In worse cases, they interfere with each other. Use of SIP over TLS can help prevent interference from SIP-aware firewalls.

UDP Flood Protection

UDP flooding protection and VoIP applications utilizing RTP do not work well together. It is recommended that UDP flooding protection in firewalls in the voice path be disabled.

Firewall Configuration Common to all Services

In a DMZ deployment, it is recommended that the administrator configure their firewall in the following way, regardless of the MBG feature set in use:

- Allow return traffic from established TCP connections
- From the server to the Internet allow traffic with
  - protocol TCP, destination port 22 (communications with Mitel AMC or SLS)
  - protocol UDP, destination port 53 (and return traffic) (DNS)
  - protocol TCP, destination port 443 to swdlgw.mitel.com (communications with Mitel Software Download Center)
  - protocol TCP, destination port 443 to swdl.mitel.com (communications with Akamai for content delivery/blades)
- From anywhere to the server allow traffic with
  - protocol UDP, destination port range 20000 to 30999 for Teleworker Network Analyzer, TFTP, voice and video
- From the server to anywhere allow traffic with
  - protocol UDP, destination port >= 1024 (RTP)

NOTE: This list is not exhaustive. Refer to the sections on individual services for the required ports and protocols of each. A more comprehensive set of firewall rules is given in *Appendix A*.

Remote Phone Access

A major purpose of the MBG is to allow remote MiNet IP and/or SIP phones to connect to the office PBX over an insecure wide-area network such as the Internet, as if they were physically in the office. Most current (and many older) models of IP sets are supported by MBG. However, please refer to the Remote IP Phones Configuration Guide for guidance on specific models. Most SIP devices, including all Mitel-branded SIP devices, can also be configured to work with MBG.

This section provides general guidelines for the Teleworker service. Refer to *Sizing your installation* to determine detailed requirements and performance limits.

Remote Site Requirements

Router

A set in a remote site (such as a home or branch office) is assumed to be part of a wired or wireless LAN behind a simple NAT router that provides access to the Internet, typically through a DSL or cable modem.

Mitel IP and SIP phones generally require a 10/100/1000 Mbps Ethernet connection, although some models can be configured for WiFi. (Refer to the device's documentation for configuration details.) All devices expect a TCP/IP network regardless of the link-layer technology.

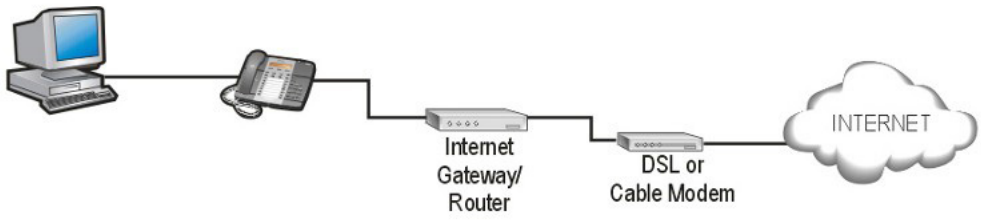


Figure 4.1: Example of a remote site

The remote site router must provide, at minimum:

- 10/100/1000 Mbps Ethernet with RJ45 connectors, for Mitel sets and connection to cable/DSL modem
- NAT from the internal network to the external network
- pass through of UDP and TCP protocols, including TFTP

The router should provide DHCP service, offering at least an IP address and default gateway. However, devices can be programmed with static IP addresses and settings in the absence of DHCP.

The router may need to support PPPoE/PPPoA when used with a DSL modem, and must be configured with the user name and password provided by the ISP.

The router may need to support Authenticated DHCP (client) when used with a cable modem, and must be configured with the user name and password provided by the ISP.

If WiFi sets are to be used, the router or a separate WiFi access point must also provide 802.11 b/g/n.

The router must control the Internet connection in order for multiple devices to share the connection. When using desktop phones, the use of USB PPPoE/PPPoA modems, USB 3G/4G modems, etc are not supported as they do not provide a port to plug in the phone. However, such devices can be used with s running on the PC if no other devices need to share the internet connection of the PC. A similar caveat applies to any service that requires software to be loaded on the PC, such as AOL Broadband. It cannot be used with a desktop device, but can possibly be used with a softphone application such as MiCollab Client.

NOTE: The remote site may have a dynamic IP address. However, if the address changes during a call, the call will drop and all devices at the site must re-register with MBG to restore service.

VPN Connectivity

Connecting a PC to the second Ethernet port on the back of a Mitel IP phone does not provide the PC with a VPN connection to the office network. That connection must still be made by use of the organization's supported VPN client software. This ensures that security of the corporate network is maintained when using MiVoice Border Gateway.

A gateway-to-gateway VPN can be constructed between branch offices (or homes) and the main office, if desired, such that all the PCs in the remote office have full access to the corporate LAN. However, Mitel advises that only non-voice traffic be routed across the VPN; voice traffic between sets and the MBG should traverse the Internet whenever possible. Routing real-time voice protocols across a VPN can result in degraded service.

MSL, upon which MBG runs, does provide a PPTP VPN service. If desired, the MBG server can be used as a VPN concentrator for access to the corporate network. However, a VPN is not required to use the features of MBG itself. For more details, see the *Mitel Standard Linux Installation & Administration Guide* (available in Mitel Document Center).

Using an Existing VPN

Using the MiVoice Border Gateway does not affect any existing VPN client software (for example, IPSEC road warrior connection) installed on the remote PC. The PC should be connected to either the second Ethernet port of the IP phone or directly to the router and the existing software should be used as before.

NOTE: VPN (for example, IPSEC) pass-through must be supported by the router at the remote site.

Corporate Firewall & Network Configuration for VPN Access

The corporate office firewall may need to be reconfigured to allow other traffic from the MSL server to the internal network if the MSL server is used as a VPN server. The ports and protocols required will depend on the applications used by the client PCs and this configuration is outside the scope of this document.

More information on firewall configuration can be found in *Firewalls DMZ* and *Appendix A*.

Bandwidth Requirements for the Remote Site

This section analyzes bandwidth requirements of the remote site using the MiVoice Border Gateway. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be provisioned as well. Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service provided by the MiVoice Border Gateway.

The table below shows examples of bandwidth required for various types of remote media streams.

Table 4.1: Bandwidth requirements of a single remote teleworker device

Voice	If compression (G.729a) enabled: 24 Kbps (bi-directional) If compression not enabled (): 80 Kbps (bi-directional)
MiCollab Audio, Web and Video Conferencing	192 Kbps (bi-directional)
MiCollab Client Video	256 Kbps – 1600 Kbps (bi-directional)
MiVoice Video Unit	512 Kbps – 1500 Kbps (bi-directional)

This table does not consider bandwidth requirements for PCs or other devices, which must be provisioned in addition to the IP Phone. If there is insufficient bandwidth, symptoms experienced by the IP phone user may include degraded voice quality, slow response, service interruption or loss of service. It also does not consider bandwidth requirements for additional applications. See the *Additional Application Requirements* section for more information.

NOTE: A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

A remote MiVoice Video Unit connecting to MBG over the Internet should be configured to disable the H.264 High Profile codec and to disable the Dynamic Bandwidth Allocation option. A video conference should not be initiated from a MiVoice Video Unit on the Internet because it would serve as a bridge and dramatically increase bandwidth requirements for the call.

Video calls between MiCollab Client 6.0 and MiVoice Video Unit 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a MiCollab Client on the Internet will receive video at the rate configured on a MiVoice Video Unit on the LAN even if the MiCollab Client is configured to use low bandwidth. This will be rectified in a future release of MiCollab Client and/or MiVoice Conference/Video Unit.

MiCollab Audio, Web and Video Conferencing between AWV clients via the AWV server is also supported through MBG. The bandwidth usage per video stream is configurable on the AWV client. An additional consideration is that an AWV client can receive multiple video streams, one for each video participant in the conference. That number can be reduced at the AWV client by minimizing or closing video windows.

For details and current values, please see the engineering guidelines for the devices/applications referenced as examples here (available in Mitel Document Center).

Bandwidth Usage and ISP Quotas

Many Internet Service Providers set quotas on the amount of IP bandwidth per month. As an aid in predicting whether a specific quota will be exceeded, this section provides the necessary data and a sample calculation.

Assumptions:

- Signaling channel requires 1 KByte per minute (average), based on 6 calls per hour, business usage, 15 minutes per hour
- Options keepalive and Gap registration enabled for SIP, at 20s and 300s respectively

Table 4.2: Bandwidth usage vs time for an IP or SIP phone

	Bandwidth Required	Hourly Usage (100%)	Monthly Usage (100%)
Signaling (MiNet)	1 KB/minute	60 KB	43.2 MB
Signaling (SIP)	1.75 KB/minute	105 KB	75.6 MB
G.711 voice stream (IP), 20ms	80 kbps	36 MB	25.92 GB
G.729a voice stream (IP), 20ms	24 kbps	10.8 MB	7.78 GB

NOTE: 20ms is the default RTP frame size, but the value is configurable in the MiVoice Border Gateway administration panel.

The data in the above table can be used to:

- estimate the available call time given a quota
- estimate the monthly bandwidth requirement for a given call volume

Example 1: Estimating Available Call Time

Given an ISP quota of 2 GB/month and continuous use:

- Call hours of G.729a = (2000 MB - 43.2 MB) / 10.8 MB per hour = 181 hours
- Call hours of G.711 = (2000 MB - 43.2 MB) / 36 MB per hour = 54 hours

Given the same 2 GB/month quota, and usage of 15 min/hr, 12 hours per day, 7 days per week:

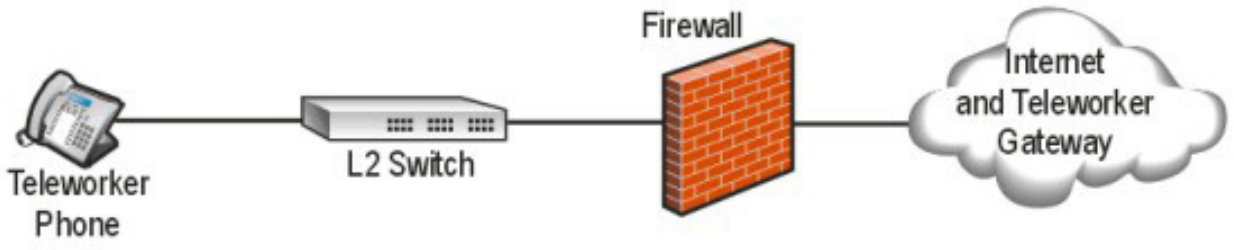
- Call hours of G.729a = (1448 hours or more than 1 month)
- Call hours of G.711 = (432 hours or roughly 18 days)

Example 2: Estimating Monthly Bandwidth Requirements

Given a user that averages 4 hours of phone calls per day, for 22 workdays in a month:

- Bandwidth Usage for G.729a = 43.2 MB + (10.8 MB x 4 hr per day x 22 days) = 994 MB
- Bandwidth Usage for G.711 = 43.2 MB + (36 MB x 4 hr per day x 22 days) = 3200 MB or 3.2 GB

Configuring the Remote Site Firewall



If the remote office has a firewall, it must be configured to allow the IP or SIP phone to connect through it to the MiVoice Border Gateway. The simplest approach is to permit all connections to or from the MBG's

IP address. A second very simple approach is to permit all outgoing connections and any responses to them. By default, most small office and home NAT routers allow outgoing connections and responses to those outgoing connections.

Sites with more restrictive security policies may wish to use the following rules:

- Allow bi-directional TCP connections to destination port 6881 on the MiVoice Border Gateway IP Address (for 6920, 6930, and 6940 avatar support)
- Allow TCP connections to destination port 6881 for Corporate Directory Access.
- Allow a bi-directional TCP connection to destination ports 6801 and 6802 on MiVoice Border Gateway IP address
- Allow bi-directional TCP connections to destination ports 3998 and 6881 on the MiVoice Border Gateway IP address (for 5235, 5330, 5340 and Navigator set features)
- Allow incoming UDP from source ports 20000 to 30999 on MiVoice Border Gateway IP address
- Allow outgoing UDP to destination ports 20000 to 30999 on MiVoice Border Gateway IP address
- Allow bi-directional TCP connections to destination port 36008 on the MiVoice Border Gateway IP address, if using Release 6.0 or later.
- Allow incoming and outgoing UDP and TCP to port 5060 on the MiVoice Border Gateway IP address, if non-encrypted IP support is desired for SIP devices.
- Allow incoming and outgoing TCP to port 5061 on the MiVoice Border Gateway IP address, if encrypted SIP support is desired for MiCollab Client devices.

Behavior

Mitel IP phones require a TFTP server that holds their set firmware and HTML applications. For remote phones, this TFTP service is provided by MBG.

Previous versions of MBG bundled a version of the HTML applications and served them directly. This caused some trouble with keeping versions in sync, especially with multiple ICPs. Since release 7.0, MBG does a proxy request to the appropriate ICP instead.

When an IP phone connects to its ICP, the ICP (MiVoice Business, MiVoice Office 250, MiVoice MX-One, and MiVoice Office 400) may issue a File Download directive over the SAC protocol connection. MBG intercepts these directives and downloads the file on behalf of the remote set. It then sends a modified directive to the set instructing it to download the cached file from MBG. This ensures that the set receives the same file that it would if it were directly connected to MiVoice Business. MBG will check periodically for updated HTML application files at the ICP. The frequency of checks depends on the feature set supported by the ICP. It could be as often as 10 minutes, and as infrequent as 24 hours.

NOTE: MBG's file downloader does not know about any ICPs until sets connect to MBG and thus get connected to an ICP. This step happens after a set has already retrieved its firmware load via TFTP. Due to that, set firmware loads are still bundled with MBG and are not fetched from the ICPs.

Firewall Configuration for Remote MiNet Devices

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Appendix A: Firewall Configuration Reference*.

From the Internet to the MBG server:

- allow protocol TCP, destination ports 6801, 6802[1], 3998 and 6881[2]
- allow protocol UDP, destination port 20001 (and return traffic)

From the MBG server to the LAN (or just ICPs):

- allow protocol TCP, destination ports 6800, 6801, 6802, 3998, 3999 and 6881
- allow protocol UDP, destination port 20001 (and return traffic)

NOTE: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

Configuring MBG for Remote SIP Devices

Remote SIP Device Limitations

The SIP protocol is limited in allowing device resiliency. While multiple DNS "A" records can be configured for an FQDN, which can be resolved to multiple MBG servers, this method provides no control over client behavior and therefore, does not guarantee resiliency.

Tuning Global Parameters

The default values for all parameters assume a Teleworking installation, with SIP devices being used over the Internet. In a LAN context, these parameters will work correctly but may be slightly aggressive.

By default, every 60 seconds MBG sends an Options request message to any SIP device that is:

- Connected over UDP.
- Behind a NAT device.

You can change this configuration, globally or for individual users, with the “Options keepalives” and “Options interval” parameters. For example, to force Options requests to be sent to all SIP devices (including devices that are connected using TCP or TLS, and devices that are connected using UDP but are not located behind NAT) set the “Options keepalives” parameter to “Always” on the Settings screen. To ensure that the SIP connection is maintained on a busy network, reduce the “Options interval” from its default value of 60 seconds to 20 seconds. Alternatively, on a quiet network, you may choose to increase the “Options interval” to its maximum value of 180 seconds. Note that frequent SIP traffic is required between the set and MBG in order to maintain NAT bindings on the remote NAT router. A device that times out due to inactivity may lose its NAT binding and the ability to receive calls from MBG.

On a “quiet” network it is sufficient to disable gapped registration and raise the options interval to its maximum value (180s at this time). If all remote SIP devices send their own keepalives or re-register at an interval less than 300s, MBG's Options Keepalives can be turned off.

1. Port 6802 is not required for Enhanced Security mode
2. The ports listed here correspond to services that have been enabled on MBG.

Support

While SIP clients can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System (DNS) that resolves to the public IP of the MBG server.

Advantages:

- The IP address of the MBG server can be changed, and the clients will not need to be reconfigured.
- DNS can provide a certain level of resiliency in case an MBG server experiences any kind of service outage. Simply configure the FQDN to resolve to multiple MBG servers. Please note that MBG cannot control how a SIP device behaves when it receives multiple IP addresses in a DNS response.

NOTE: A remote SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured "Allowed URIs" in the "SIP options" section of the Configuration tab.

WARNING: A SIP server requires functional DNS even if all devices are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working DNS resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

Firewall Configuration for Remote SIP Devices

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)*:

From the Internet to the MBG server:

- allow incoming and outgoing protocol UDP and TCP to port 5060[1]
- allow incoming and outgoing protocol TCP to port 5061

From the MBG server to the LAN (or just ICPs):

- allow incoming and outgoing protocol UDP and TCP to port 5060
- allow incoming and outgoing protocol TCP to port 5061

SIP over TLS (port 5061) is the default setting on MiCollab Client SIP softphones. This setting may be changed to SIP over TCP (port 5060) on the individual clients.

NOTE: This is a minimal configuration. Refer to *Firewalls (DMZ deployment)* for the full set of rules and optional settings.

1. The ports listed here correspond to services that have been enabled on MBG.

SIP Trunking

Overview

A “SIP trunk” in the context of MBG is simply a pair of endpoints, defined by their IP addresses and signaling ports. One of the endpoints is usually your ICP (MiVoice Business/3300 ICP, MiVoice Office 250, MiVoice MX-One, MiVoice Office 400, MiVoice Border Gateway, or Mitel 5000), and the other is your SIP provider’s firewall or SBC. These endpoints can be classified by the following modes:

- **Fixed Mode**: Pair of endpoints manually configured by the MBG administrator (addresses/ports are static).
- **SRV Mode**: Multiple endpoints automatically configured by MBG using the SIP Trunk Provider’s DNS server without any MBG administrator intervention (addresses/ports are dynamic).

A trunk can have any number of “channels,” each of which corresponds to an active media stream. A channel license is required for each active channel, so you will need enough channel licenses to cover the maximum number of active calls. As an analogy, an ISDN PRI link contains 23 B channels for audio and one D channel for signaling and can carry a maximum of 23 simultaneous calls. This would be equivalent to a SIP trunk with 23 channel licenses.

As of MBG 11.0:

- UDP, TCP and TLS transports in both Fixed and SRV mode are supported.
- transport protocol translation is not performed; that is, if TCP is selected as the transport protocol on MBG, both, the ICP as well as the service provider must also be using TCP to match with MBG; there cannot be any mismatch on each side of MBG. For example, there cannot be UDP on one end and TCP on the other end.
- encrypted audio streaming (SRTP) is now supported in TRUNK scenarios independently on either side of MBG:
  - On the TRUNK side of MBG if the remote TRUNK endpoint provider supports it.
  - On the ICP side of MBG if the remote ICP endpoint supports it.
- The following encrypted audio streaming (SRTP) cryptosuites are supported:
  - AES_CM_128_HMAC_SHA1_32
  - AES_CM_128_HMAC_SHA1_80

NOTE: On the MiVoice Business (3300 ICP), the MBG is configured as an outbound proxy in the Network Element form.

WARNING: In the 5.X releases, the SIP trunk connector listened on UDP port 5064 by default. As of MBG 6.0 the SIP connector can handle device endpoints and SIP trunks, so UDP port 5060 is used for both devices and SIP trunks. The Legacy Connector can no longer be re enabled as of MBG 8.0. If UDP port 5064 is in use, then you will need to contact your SIP Trunk provider to have their equipment changed to use MBG's UDP port 5060 before upgrading MBG to 8.0 or later.

WARNING: A SIP server requires functional DNS even if all devices are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working DNS resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

Send Options Keepalives

Fixed Trunk Mode

To maintain the availability of SIP trunks, you must configure MBG to keep the connection active by pinging the ICPs. For each SIP trunk, access the SIP trunking screen and program the following:

- Set **Options Keepalives** to **Always**.
- Set **Options Interval** to **20**.

NOTE: Ensure that this configuration is implemented for a resilient trunk configuration. Otherwise, in the event that an ICP becomes unavailable, the secondary connection may not be active and calls may fail.

SRV Trunk Mode

SRV Mode does not use Options Keepalives as it implements Trunk resiliency by design. When using SRV Mode Options Keepalives is automatically disabled and cannot be edited.

Bandwidth Requirements

Refer to *Sizing Your Installation* section.

Resilient ICP Configuration

NOTE: With MiVoice Business, set an **Invite Ringing Response Timer** value of **2** or **3** seconds (recommended) to fail an incoming call to the next route in the route list. The IRR value can be set under **SIP Device Capabilities**, in the **Timers** tab.

Configure Resiliency between the ICPs

On ICP “A”:

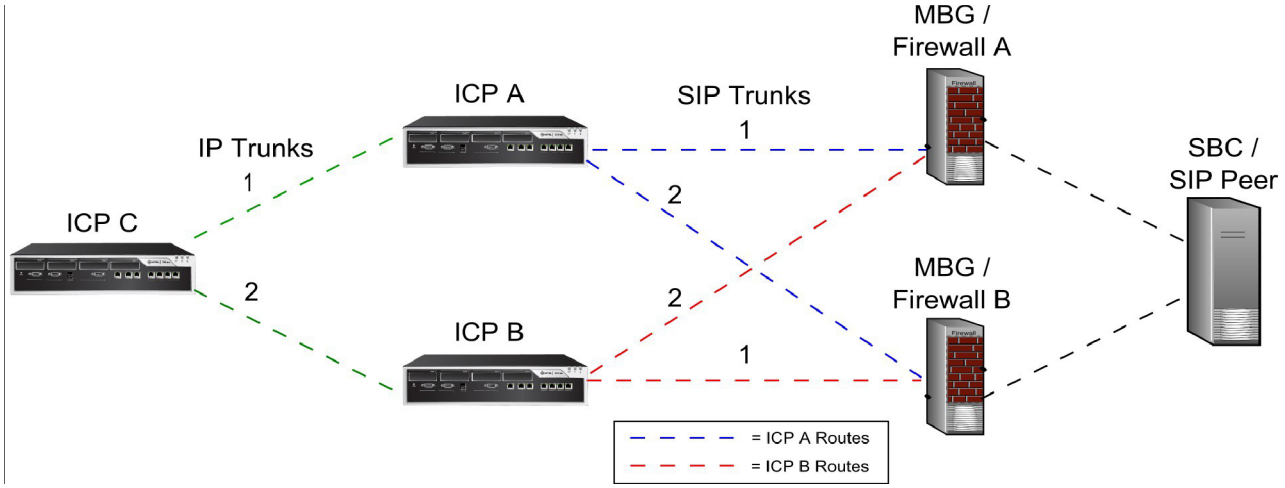
1. Create a Network Element Assignment for the MBG (as Type: Outbound Proxy), entering its address as a Fully Qualified Domain Name (FQDN) that resolves to MBG A and MBG B. In case one MBG fails, the FQDN enables the other MBG to be reached.
2. Create a Network Element Assignment for the SIP provider’s SBC (as Type: Other).
3. Create a SIP Peer Profile for the SBC, specifying the MBG as the Outbound Proxy.
4. Program a Route in ARS, specifying the SBC as the SIP peer.
5. Program ARS Digits Dialed such that outgoing calls use the new route.

On ICP “B”:

- Repeat steps 3, 4, and 5 (steps 1 and 2 are unnecessary because the network element information is shared between ICPs).

On Other nodes in the cluster (for example, ICP “C”):

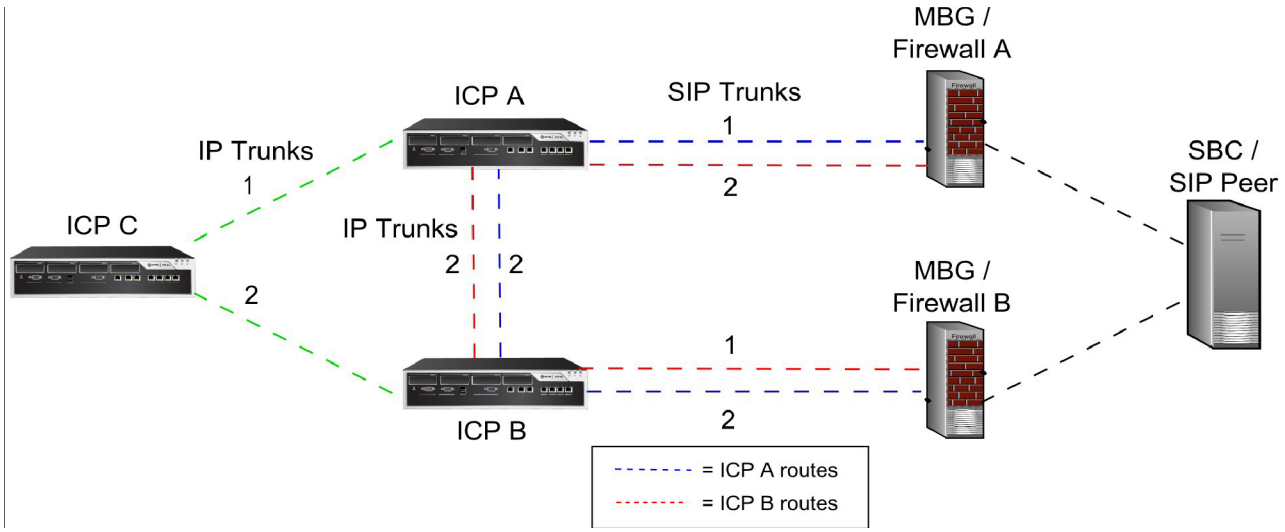
- Provision each element in the cluster with IP trunks with route lists to ICP A and ICP B.



Alternative Programming

If you cannot use an FQDN to reach MBG "A" and "B", do the following to achieve resiliency:

1. On ICP A, create a Network Element Assignment for MBG A (as Type: Outbound Proxy) and another for the SIP provider's SBC (as Type: Other). Create a SIP Peer Profile for the SBC, specifying MBG A as the Outbound Proxy.
2. On ICP B, add a Network Element Assignment for MBG B (as Type Outbound Proxy) and create another SIP Peer Profile for the SBC, specifying MBG B as the Outbound Proxy.
3. On ICP A, program a Route List in ARS with SIP peer A and a route to ICP B as an alternate. Then program ARS Digits Dialed.
4. On ICP B, program a Route List in ARS with SIP peer B and a route to ICP A as an alternate. Then program ARS Digits Dialed.



Configure MBG Clustering

1. On the master MBG, access the ICPs tab and add both ICP A and ICP B.
2. On the SIP trunking tab, configure a trunk profile for the remote SBC. Add a single routing rule of "*" with ICP A and ICP B as the targets of the rule. This configuration will propagate to the secondary MBG.

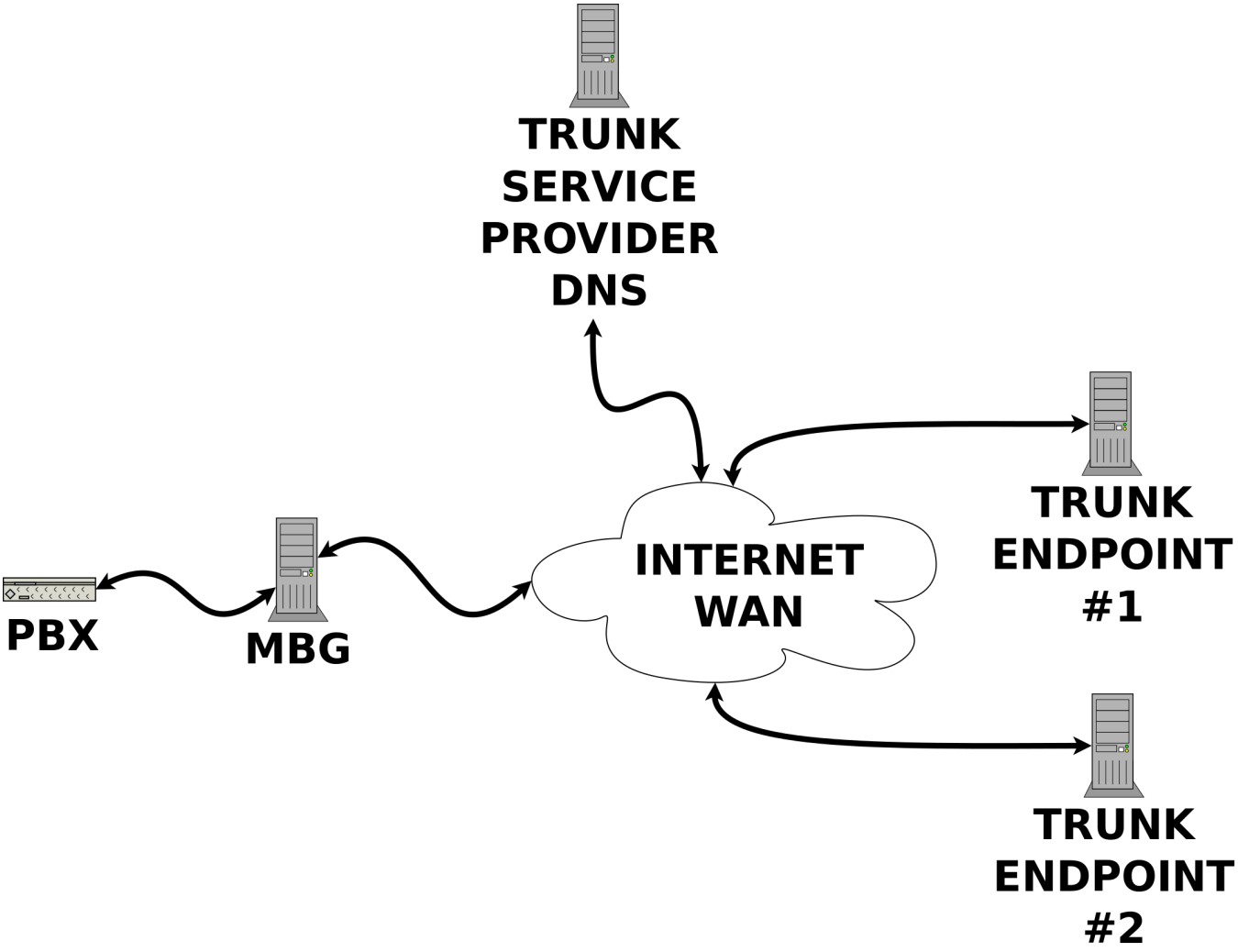
Incoming calls from the SBC will arrive at either MBG A or MBG B. From there, MBG routes an incoming call to ICP B only if ICP A is marked unavailable, unreachable, or down after failing to respond to three consecutive SIP option keepalives or to a SIP message within 32 seconds. Outgoing calls from either ICP can be routed through either MBG.

Resilient Trunk Configuration

NOTE: This section applies only to SRV mode Trunking.

A basic architecture for communication between a service provider and a client involves MiVoice Border Gateway (MBG) with SIP Trunks, normally a single Trunk Endpoint. This works well until the single trunk endpoint experiences an issue, such as being unreachable because of network issues, or has hardware or maintenance issues. During this downtime, the SIP Trunk Provider cannot provide service. Thus, the architecture does not provide resiliency.

The SIP Trunk Provider can implement resiliency by providing more than one trunk endpoints. When one trunk endpoint encounters an outage, services can be provided by switching to another trunk endpoint. However, in the absence of enabling a Transport protocol, the MBG administrator must manually create a Trunk entry for every Trunk Endpoint and enter the address and port of every Trunk Endpoint.



The function of Transport protocol is to automate the provision for resiliency. Select SRV from the Transport protocol drop-down to enable MBG to use SRV Trunking Mode for the Trunk Service Provider. When this option is enabled, the Remote Trunk endpoint port and Remote Trunk endpoint address fields are automatically configured and cannot be edited.

By default, this option is set to a non-SRV value (for example, UDP or TCP or TLS), and MBG uses Fixed Trunking Mode for the Trunk Service Provider. With Fixed Trunking Mode, you will need to manually configure the Remote Trunk endpoint port and Remote Trunk endpoint address fields.

MBG does not support transport protocol translation, which means, for example, if selecting TCP as the transport protocol, the ICP end points as well as the service provider, needs to be using TCP. One end cannot be UDP and the other end TCP.

Both SRV trunks and fixed trunks must use mutually exclusive addresses - a fixed trunk cannot use an IP address (or an FQDN that resolves into an IP address) that is also listed in at least one of the records of an SRV trunk service provider that is used by MBG and an SRV trunk that is used by MBG cannot use an IP address that is listed as one for a fixed trunk.

DNS Support

While the ICP can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System (DNS) that resolves to the public IP of the MBG server.

Advantage:

- The IP address of the MBG server can be changed, and the ICPs will not need to be reconfigured.

NOTE: An ICP SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured “Allowed URIs” in the “SIP options” section of the Configuration tab. Typically, the hostnames you add to the “Allowed URIs” list will be for the SIP service provider's session border controller or service domain.

WARNING: A SIP server requires functional even if ICPs are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

SIP Adaptation

It becomes necessary to make specific changes to the service itself for meeting the requirements of different providers to inter-operate between multiple SIP providers. One provider might want a header in a particular format while another provider wants the same header in a different format. Adding patches to the service itself in MBG to support such customized requests is not feasible because it requires too many patches to be managed.

The SIP Adaptation feature makes support for customized requests easy to implement and scalable. SIP Adaptation is done through a SIP Proxy that operates between two or more SIP endpoints. To accomplish this, a plug-in architecture was created in MBG's core service. This architecture permits plugins to act on SIP headers in MBG's SIP processing pipeline. An open-source scripting language, Lua, originally intended for embedding in a software application to provide customizable scripting support, was used for scripting the plugins. For information about scripting the plugins, see the MBG Lua API document in the Create Pipeline page in the MBG interface.

The SIP Adaptation page displays any configured adaptation pipelines in the Pipeline information table. This table is blank until you have created pipelines. Pipelines might have a global scope and apply to all SIP traffic, or they may be tied to a particular SIP trunk. After you have created a pipeline, apply the pipeline globally across all SIP trunks, or to specific SIP Trunks.

Firewall Configuration for SIP Trunking

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)*):

NOTE: Remember to turn off any UDP flooding protection and any SIP features of the DMZ firewall.

NOTE: As of MBG 10.0

- SIP Trunking is supported in both UDP and TCP in FIXED MODE and in SRV MODE.
- SRTP is supported over SIP Trunks.

From the Internet to the MBG server:

- allow protocol UDP, destination port 5060 (and return traffic) or

- allow protocol TCP, destination port 5060 (and return traffic) or
- allow protocol TCP, destination port 5061 (and return traffic)

From the MBG server to the LAN (or just ICPs):

- allow protocol UDP, destination port 5060 (and return traffic) or
- allow protocol TCP, destination port 5060 (and return traffic) or
- allow protocol TCP, destination port 5061 (and return traffic)

NOTE: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

Call Recording

The Mitel call recording solution encompasses multiple parts, including the MBG call recording service, a compatible call recording application, call manager platform and devices. Call recorders vary in their support of Mitel platforms and features. Configuring a solution line-up is beyond the scope of this document. Consult your recording vendor or Mitel sales engineering. Refer to the *MBG Online Help* for detailed information on the **Call Recording Service**.

MBG provides two services that allow an external Call Recording Equipment (CRE) to record audio calls:

- *Secure Recording Connector*(SRC): A Mitel proprietary service to record MiNET and SIP devices as well as SIP trunks.
- *SIPREC*: An industry standard protocol to record SIP devices.

NOTE: WebRTC calls cannot be recorded.

Mitel Secure Recording Connector

The Mitel Secure Recording Connector (SRC) behaves as a server, handling authenticated connections from Call Recording Equipment (CRE) and granting access to call setup information and copies of media streams (audio only).

The SRC allows a Call Recording Equipment (CRE) to record calls in one of the following modes:

Direct Call Recording

With direct call recording, the MBG server is positioned between the call server and the devices/trunks handling both signaling and media. This puts the MBG in a position to send a copy of the media streams to the CRE on request.

Indirect Call Recording

With indirect call recording, the remote devices are registered directly to MiVoice Business instead of the MBG. MBG acts as a broker between the call recorder, platform and devices. The device duplicates its audio stream and sends it to the CRE.

SIPREC

MBG's SIPREC service allows a CRE, referred to in RFC 7866 as a SIP Recording Server (SRS), to record audio calls to or from SIP devices connected to MBG. MBG provides the B2BUA Recording Model as described in RFC 7866 and is, oddly, referred to as an SRC (Session Recording Client).

SIPREC does not use TLS mutual authenticated connections, the CRE does not initiate connections to SRC. SRC is configured with the CRE addresses (see below) and it is the SRC that connects to the CRE.

SIPREC message flows follow the original SIP message flows through MBG. However, only call setup/teardown is shared. This takes the form of a SIP INVITE message, sent by SRC to CRE and a response to that INVITE from the CRE that will contain SDP (requesting a tap) or no SDP (not requesting a tap). Additional information about the call is sent from the SRC to the CRE in the form of extra “meta-data” attached to the SIP messages.

For more details about SIPREC refer to the *MBG Online Help*.

Refer to the *Sizing Your Installation* section to determine performance limits and resource requirements.

Requirements

This section contains software/hardware requirements necessary to support the Secure Recording Connector service.

Phones/Devices

For a complete list of devices that are supported by the secure recording connector service of MBG, please refer to the *MBG Remote Phone Configuration Guide* available at Mitel Document Center.

Firewall

The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that will permit return traffic on an existing established connection.

The following connections must be configured:

Port Range	Direction	Purpose and Details
For SRC		
TCP 6810	LAN ->Server	Call Recording Support. To enable a third-party call recording equipment (CRE) server to connect to the SRC control interface on MBG, this port must be enabled.
TCP 6815	Server ->ICPs	Indirect Call Recording support (Optional). To enable MBG to connect to the Indirect Call Recording connector on MiVoice Business systems which support it.
UDP 35000 to 35999	Server ->LAN	Voice Recording. For streaming voice streams from the MBG server to the CRE for recording purposes.
For SIPREC		
TCP <SRS port>	LAN -> SRS	SIP Signaling to SIPREC server.
UDP 35000 to 35999	Server -> LAN	Voice Recording. For streaming voice streams from the MBG server to the SRS for recording purposes.

Web Real-Time Communication (WebRTC)

WebRTC is an API definition drafted by the World Wide Web Consortium (W3C) that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities. MBG supports WebRTC for browser-based voice and video calling without the need of plug-ins using Google Chrome, Mozilla Firefox and Opera on all platforms except iOS.

WebRTC Gateway Supported Configurations

The WebRTC application offers a toolkit which you can use to add secured communication components to enterprise web pages. Two usage scenarios are available, for "anonymous" and "subscriber" calls.

Anonymous Call: In this scenario, an external user initiates a call to the enterprise by clicking a button on a web site and then providing minimal credentials (name and CAPTCHA phrase). The user, who is known as an "anonymous caller," is directed to an internal service such as a sales or product support hotline.

Subscriber Call: In this scenario, an external user logs in to MBG from a browser and then registers with the ICP. The user, who is known as a "subscriber," can perform a variety of tasks, such as looking up names in the company directory, accessing voicemail, and both placing and receiving calls.

ICP Support

The WebRTC gateway can be implemented with a MiVoice Business or MiVoice 5000 ICP. With a MiVoice Business, users can place anonymous calls over a SIP trunk. With a MiVoice 5000, users can place anonymous calls over a SIP trunk, log in as subscribers in order to place and receive calls, and access the company directory from an LDAP database.

WebRTC Architecture and Topology

The WebRTC solution consists of a gateway and a web application.

WebRTC Gateway (on MBG)

The WebRTC gateway is co-located with MBG and has two interfaces, LAN and WAN. The gateway has three complementary modules:

- **Web services**: Facilitates directory searches on the LDAP database.
- **SIP proxy**: Relays SIP signals between WebRTC clients and the ICP.
- **Media adaptor**: Relays media streams between WebRTC and LAN-based clients. Adapts formats (DTLS, codec).

WebRTC Web Pages (on Web Server)

A web server is required to host the WebRTC web pages. Although the web server can be co-located with the MBG, more typically it is hosted on a standalone system.

Default web pages are provided by MBG. These can be used without modification, or new web pages can be created that match the look and feel of the customer's website.

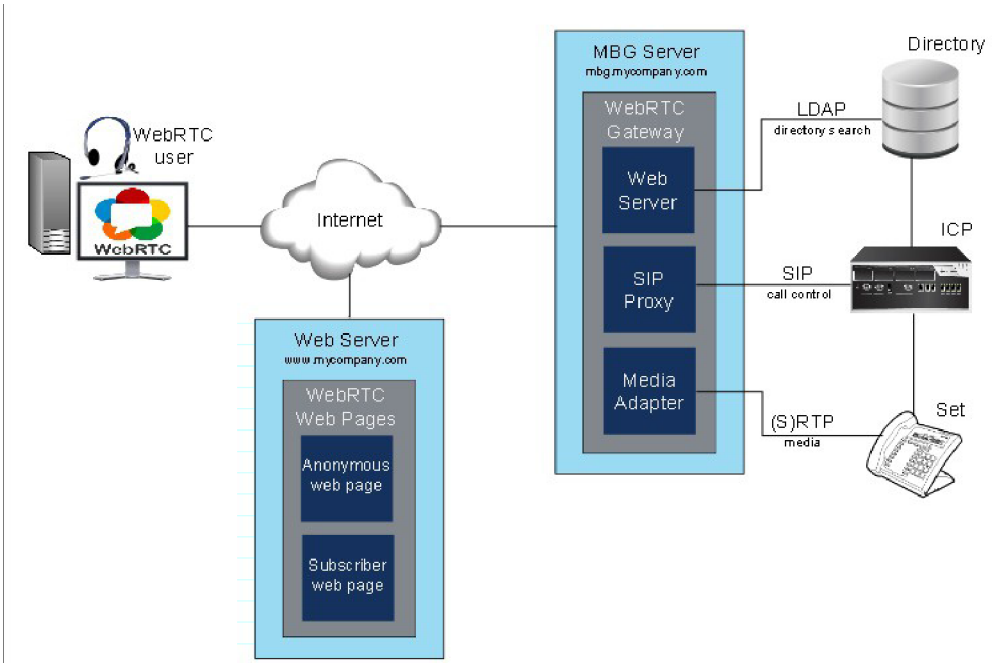


Figure 7.1: WebRTC Gateway and Web Pages Topology

Firewall Configuration for WebRTC Gateway

From the Internet to the MBG server:

- allow protocol TCP, destination port 5063 for SIP over TLS
- allow protocol UDP, destination ports 32000 to 32500 (and return traffic) for RTP media

From the MBG server to the LAN (or just ICPs):

- allow protocol TCP, destination port 389 for connection to LDAP database (MiVoice Business or MiVoice 5000 manager)
- allow protocol TCP, destination port 443 for connection to picture server (MiVoice Business, MiVoice 5000 manage, or dedicated picture server)
- allow protocol UDP, source port 5064 for unencrypted SIP trunk connection to MiVoice Business or MiVoice 5000 (anonymous calls)
- allow protocol TCP, source port 5065 for encrypted SIP trunk connection to MiVoice 5000 (anonymous calls)
- allow protocol TCP, source port 5066 for encrypted SIP user connections to MiVoice 5000 (subscriber calls)

From the MBG server to the LAN:

- allow protocol UDP, source ports 33000 to 33500 (and return traffic) for RTP media

Additional Application Requirements

MBG allows the use of several supported applications from remote sites, just as it allows use of IP phones. When MBG is deployed in the DMZ of a third-party firewall, that firewall must be configured to allow connections from these applications.

This section, plus the common rules in *Firewalls (DMZ deployment)*, gives a minimum configuration for each supported application. Refer to *Appendix A: Firewall Configuration Reference* for the full set of firewall rules.

MiCollab Client v6.0+

WARNING: MBG 7.0 required a port-forwarding rule for port 36008 that directed traffic to the MiCollab Client server. After upgrading to MBG 7.1 or higher, this rule must be removed from the MSL Port Forwarding panel.

The following additional rules are required, excluding the MiCollab Client softphones:

From the Internet to the MBG server:

- allow protocol TCP, destination port 36008

From the MBG server to the LAN:

- allow protocol TCP, destination ports 443, and 36008

NOTE: When the MiCollab Client server is behind MBG, remote MiCollab Clients require access via Web Proxy for MiCollab Client 5.1 and above. See *Web Proxy* for additional firewall rules.

MiCollab Clients also include MiNet and SIP softphones. For additional firewall rules covering the MiCollab Client softphones see *Firewall Configuration for Remote MiNet Devices* and *Configuring MBG for Remote SIP Devices*.

You can choose to have MBG present a built-in Mitel certificate or a trusted third-party certificate uploaded in the MSL Web Server panel to SIP TLS connections (TCP 5061). The default is Mitel certificate.

NOTE: Changing this setting breaks the trust model with the existing clients, which results in failures to connect until redeployment. Particularly, the MiCollab Client Deployment profile setting for TLS server certificate validation must match the MBG setting, such as,

- If the MBG setting is "Mitel", the deployment profile setting for TLS-server-certificate CA must be Mitel CA.
- If the MBG setting is "Web server", the deployment profile setting for TLS-server-certificate CA must be Public CA.

MiContact Center

The following additional rules are required:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 35001 – 35008 (inclusive), 36000 – 36004 (inclusive)

From the MBG server to the LAN:

- allow protocol TCP, destination ports 80, 443, 1443, 5024 – 5026 (inclusive), 5030, 7001, 7003, 8083, 8084, 8188, 42440

Web Proxy

The following additional rules are required, at minimum:

From the Internet to the MBG server:

- allow protocol TCP, destination port 443

From the MBG server to the LAN server:

- allow protocol TCP, destination port 443

MiCollab AWV Conferencing

In addition to rules under Web Proxy for HTTPS traffic, MiCollab AWV Conferencing requires passthrough of its ConnectionPoint traffic. This is supported with either:

- *an additional dedicated external IP address on TCP port 443* or
- *a dedicated TCP port on the primary external IP address*

Additional Dedicated External IP Address on TCP Port 443

In this configuration, the MiCollab AWV Conferencing server is usually configured with the internal port as 4443 and the external port as 443 in the Web Conferencing Setting page. The configured Web Conference Name fully qualified domain name (FQDN) must resolve externally to the dedicated external IP address. Following are the required rules:

From the Internet to the Firewall:

- allow protocol TCP, destination port 443 on the MiCollab AWV Conferencing IP address

From the Firewall to the Web Proxy (MBG):

- allow protocol TCP, destination port A, where A is the listen port for MiCollab AWV Conferencing configured by the administrator

From the Web Proxy (MBG) to the MiCollab AWV Conferencing server on the LAN:

- allow protocol TCP, destination port 4443

NOTE: The configuration method using two external IP addresses is helpful in preventing connectivity issues that may arise where AWV Clients are behind a corporate firewall with rules for outgoing traffic, where those rules may only allow web-based ports to be reached at a remote location. For example, a remote user is more likely to be able to make a connection to a server outside of their network using port 443, than port 4443.

Dedicated TCP Port on the Primary External IP Address

In this configuration, the MiCollab AWV Conferencing server must be configured with the same internal and external port, recommended is 4443. The configured Web Conference Name must resolve to the public IP of MBG and can be the MiCollab FQDN. Following are the required rules:

From the Internet to the MBG server:

- allow protocol TCP, destination port 4443 (or the external port configured on MiCollab AWV)

From the Web Proxy (MBG) to the MiCollab AWV Conferencing server on the LAN:

- allow protocol TCP, destination port 4443 (or the internal port configured on MiCollab AWV)

NOTE: The single IP address configuration will avoid the additional usage of a dedicated IP address (useful when IP addresses are expensive or simply not possible), however it should be noted that some external users sitting behind a firewall with restricting outgoing traffic rules at ports other than 80 and 443 may experience connectivity issues.

Additional Security Considerations

Due to the broad range of application types that can be deployed on the MSL operating system (formerly Managed Application Server), Mitel suggests that you read the **Security** section of the *MSL Installation and Administration Guide* before installing this application on the same server with other applications.

SIP Security

MBG supports the following forms of SIP security:

- Transport Layer Security (TLS) on both, the SET side and ICP side, with the option to present a Mitel built-in or a trusted third party certificate. TCP/TLS encrypts signaling between SIP devices, and is recommended if you enable set-side SRTP security.
- Secure Real-time Transport Protocol (SRTP) on the ICP side as well as the SET side. SRTP provide encryption, message authentication and integrity for the media stream between SIP devices and MBG.
- As of MBG 10.1 SRTP is supported for both TeleWorker SETs and TRUNK scenarios.
- As of MBG 11.0, SIP signaling for TRUNK scenarios is supported for all of UDP or TCP or TLS transports in Fixed and SRV mode.

Traffic Shaping

Overview

For small businesses with a simple setup to the Internet, sharing that upstream link between voice and data can be problematic. Users in the middle of calls to the PSTN via SIP trunks, for example, will find the voice quality of their calls greatly reduced if a member of the office were to suddenly start a large download from the Internet. To mitigate these issues, MBG has the capability to prioritize the IP traffic that it is handling. This technique is commonly known as traffic shaping.

To shape traffic, MBG must be in a position to handle all traffic to the organization's upstream link; specifically, it must be in gateway mode with a minimum of two network interfaces. In this mode, it can act as the organization's firewall. More commonly, however, the organization already has a firewall product of some kind, and would like to deploy MBG and use traffic shaping with a minimum of disruption. This "transparent" deployment is possible on servers with three network interfaces.

Using MSL 9.2+ the third interface can be put into bridged mode. The bridged interface can then be connected to the WAN interface on the existing firewall. This configuration transparently places MBG between the existing firewall and the WAN, and allows MBG to prioritize the organization's traffic, without requiring changes to the existing firewall.

Technical Details

Figure below illustrates the queuing discipline that MBG uses for traffic shaping. The hierarchical nature of the algorithm allows lower priority queues to use tokens available in higher priority queues, which means that when little VoIP traffic is available, lower priority data will not be unnecessarily constrained. Thus, the customer can make full use of their available bandwidth to the Internet.

The categorization of high priority vs. low priority traffic is performed based on two criteria:

1. **Source IP Address**: If the source IP address of the traffic belongs to any of the network interfaces on the MBG server, then it matches the first criteria. In other words, MBG must originate the traffic.
2. **DSCP value**: The second criteria of high priority traffic is a DSCP value of 46 decimal, 0x2E hex (Expedited Forwarding). This value must be set on packets that are considered high priority. MBG will set the value for its own VoIP-related traffic.

If both of these criteria are satisfied, then the traffic ends up in the high priority queue. Otherwise, it is considered low priority and will only be permitted through the HTB queue if the high priority queue has unused tokens.

This does mean that excessive high priority traffic can starve low priority data traffic. However, 10% of available bandwidth is reserved for low priority traffic (if it is present), so it should not starve completely.

This reservation does not waste bandwidth: it can be “borrowed” by the high priority queue if no low priority traffic is present.

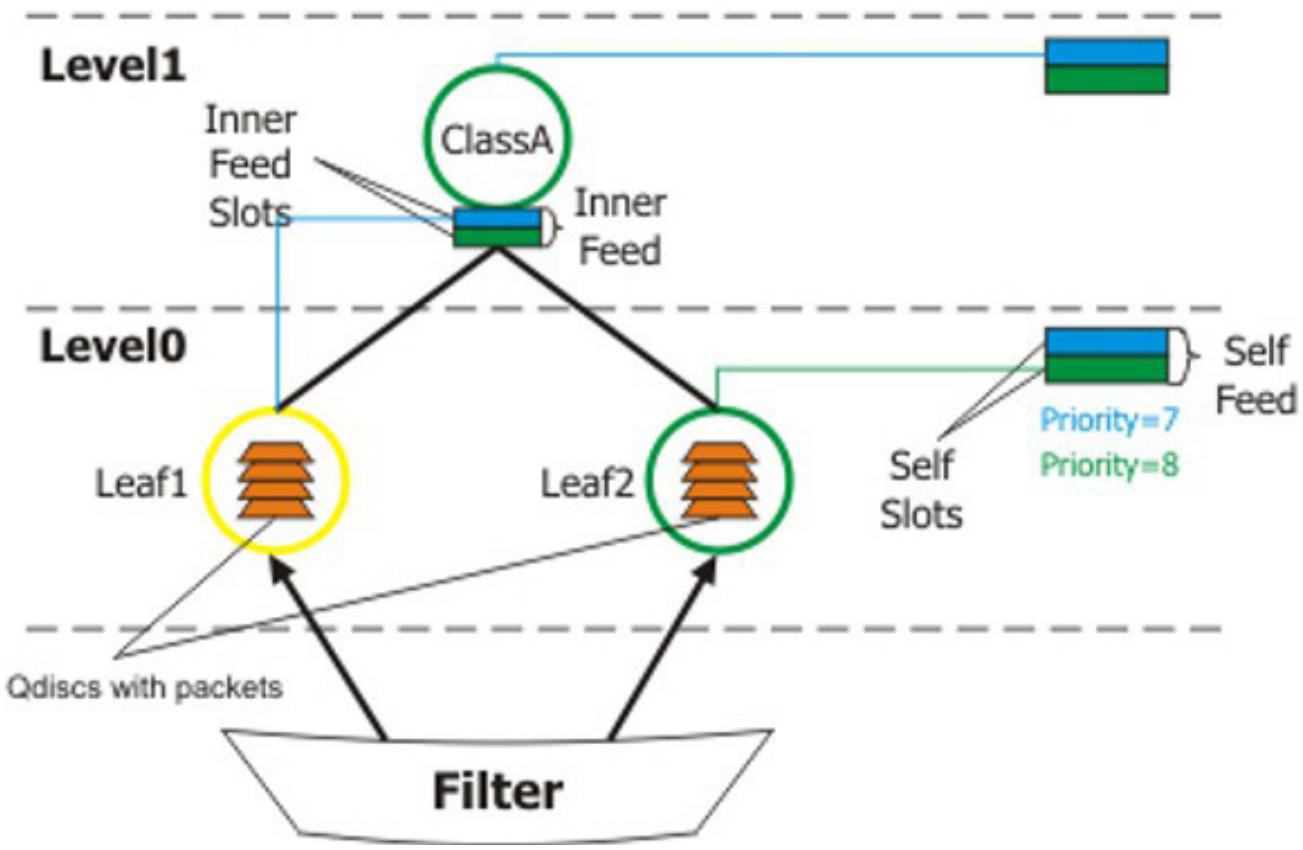


Figure 10.1: The Hierarchical Token Bucket Queue

Clustering

Overview

Clustering in this context refers to the ability of multiple MBG servers to communicate with one another via TCP, sharing data and providing the capability to manage multiple nodes thus joined as if they were a single unit.

Clustering also provides load balancing for supported MiNet devices, making the job of distributing devices across servers to share workload simple and effective. Set resiliency is also used within clustering, so that supported MiNet sets which can persistently store up to four IP addresses will have their resiliency list populated based on the cluster members. If a set loses its connection and cannot reconnect to its own node, it will try the next IP address on its list until it has exhausted all IP addresses on the resiliency list.

Clustering relies on a mesh of TCP connections between the nodes in the cluster. TCP port 6809 must be reachable between all nodes for cluster comms to be established. SSL/TLS is used to encrypt communications, so it is safe to use over the Internet.

Administrative access to each server in the cluster is required to establish a trust relationship between the nodes. The trust model is based on the IP addresses used to establish cluster comms. Each node is configured via the clustering tab to trust a connection coming in from a particular IP address. These addresses are shared across the cluster, so they must be reachable by all nodes involved, and any use of NAT will break the trust model. A summary of the steps to create a three-node cluster are shown below. Refer to the MiVoice Border Gateway Blade Installation and Maintenance Guide for full instructions on creating a cluster.

- Create the cluster from the master node, entering the IP address of the first slave node.
- Join the cluster from the first slave node, entering the IP address of the master node.
- Assuming no networking issues, the clustering tab will show established connections, and the slave node will show a backlog of events from the master (or it will finish too quickly to be seen).
- Add a node on the master, entering the IP address of the second slave node
- At this time, the first slave will receive the same data regarding the second slave via cluster comms.
- Join the cluster on the second slave, entering the IP address of the master node.
- Assuming no networking issues, the clustering tab on all nodes should show the peer nodes for that node.
- The three node cluster is now established.

NOTE: You can transform any member of a cluster into the master node. To do this, access the Clustering tab of the selected slave node and then click **Take Ownership**.

Once cluster communications are established, the master node will “push” data to the slaves until they are in sync with the master. Conflicting data is overwritten. When a slave joins the cluster, its existing database is deleted and a new database is provided by the master.

Cluster Zones

A cluster zone is a non-overlapping subset of nodes within an existing cluster. All nodes start out in the “Default” zone. The “Default” zone can be renamed but it cannot be deleted. It is easily identified because it appears first in the zone list, and has no “delete” link. Nodes can be left in the default zone if additional zoning is not required.

Additional zones can be created, and nodes can be moved to any zone. Zones can be created based on geographic location, the intended purpose for the nodes, or whatever reason the admin chooses. The purpose of zones is to provide device affinity.

By default all MiNet sets will be associated with the default zone. By editing the set, the set may have its affinity changed to a different zone. The implications of this are as follows:

- A set’s load-balancing list of nodes will always favor nodes in its zone
- The last entry in the load-balancing list will be a node from the default zone

This feature was introduced to support geographically dispersed clusters. For example, if there are three servers in North America and three in Asia, it makes little sense for Asian sets to be load balanced to North America unless all of the Asian servers are unreachable. Using cluster zones, a “North America” zone and an “Asia” zone could be created, and sets in Asia could be placed into the Asian zone. The sets in each region would then prefer the nodes in their region, reducing network latency and bandwidth use.

Similarly, zones can be created to segregate devices by function, such as keeping trials users on a separate node from regular users, or to split users by organizational group.

Node Weighting

Not all servers are created equal. If the hardware in the cluster is all equivalent, it is safe to leave the weight of each node in the cluster at its default value of 100. This ensures evenly-distributed load balancing.

To inform the cluster that a given node should handle more than an equal share of the load, increase its weight. If the server should handle less, lower the weight. For instance, assume there is a cluster of three nodes with weights of 50, 50, and 100. The two smaller servers (lower weights) will each handle roughly one quarter of the total load, while the third server handles the remaining half of the load.

Weights are not percentages[1]; they are simply a ratio of relative server power. Weights of 100,100,100 are equivalent to weights of 1,1,1. However, if the sum of all weights is 100 (or close to it), they can be treated as percentages of the total load and the system will behave as expected.

A weight of zero prevents any devices from connecting and will cause MBG to move all connected devices to other nodes.

Expressed mathematically, the above is simply: sets_on_a_node = total_sets x (node_weight / sum(node_weights))

NOTE: The distribution of devices will not be mathematically perfect. Some hysteresis is built in to the load-balancing algorithm to prevent devices from being redirected too often in a vain attempt to perfectly balance the cluster.

1. Note that using “total_sets = 100” in the formula below gives the percentage of total load handled by one node.

Note that weighting applies to zones, not to clusters. The “total load” is the load from devices configured with the same zone as the node. (In a cluster with only the Default zone, this distinction can be ignored.)

As an example, consider a cluster with five nodes and two zones. Two servers are in the “North America” zone and two servers are in the “Asia Pacific” zone. The remaining server is left in the Default zone.

The two North America servers are identical and have weights of 10. Each one will handle roughly one half of the total load of devices configured for the North America zone. One of the Asia Pacific servers is new and has more capacity; it has a weight of 20 and the other server has a weight of 10. The newer server will handle twice as much load (roughly two thirds) as the other server (one third). The fifth server handles 100% of the load in the Default zone, regardless of its weight.

WARNING: Not all devices can be load-balanced. See *Additional Considerations* for details.

Additional Considerations

While heterogeneous server capabilities are supported in a cluster thanks to the weighting mechanism, this weighting only affects the number of connected devices on each server. The cluster communications adds additional load on each server, so adding a node to the cluster does not, necessarily, linearly increase the capabilities of the cluster.

Furthermore, if the master node is used as the initial point of contact for all devices, then it should not be a “weak” server. There are many supported devices that do not support redirection, so the server they are programmed to contact will be the only server that they connect to. Setting a low weight on the main node will not change this. All SIP devices, MiNet softphones, and 5550 IP Console fall into this “non-redirectable” category. Such devices must be balanced manually by programming the devices to contact specific nodes. Setting a low weight, or a weight of zero, on nodes that handle non-redirectable devices can help with manual load balancing.

Firewall Configuration for Clustering

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)*):

From each MBG server to all other MBG servers in the cluster:

allow protocol TCP, destination port 6809

NOTE: Note: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

Advanced Options

Resiliency

MiNet devices are protected with two forms of resiliency: "Run time" and "Boot time".

Run Time Resiliency

Run time resiliency is required in case a MiNet device becomes disconnected from its current node due to a network problem or the node going offline. Should this occur, the device will attempt to reestablish a connection by consulting a "redirect list" of up to four IP addresses that it has received from MBG. The redirect list is comprised of the following:

- the device's current node
- up to two random, currently connected nodes in the device's own cluster zone
- one random, currently connected node in the backup zone (if a backup zone has not been defined, the Default zone is used instead)

For example, if the device is currently connected to MBG1, and MBG1 is taken offline for maintenance, calls that are in progress will be dropped (unless they are locally streamed) and the device will immediately consult the redirect list and attempt to reestablish the connection. First it will try to connect to MBG1, but because MBG1 is offline this attempt will fail. The device will then attempt to connect to up to two other nodes in its own cluster zone. If these attempts fail, finally the device will attempt to connect to a node in its backup cluster zone. ;

NOTE:

- Run time resiliency can only be used in a clustered environment.
- The redirect list is considered a "soft" list because it is stored in RAM. ;
- MBG re-sends the redirect list to MiNet devices whenever they are started or rebooted, and whenever the cluster configuration changes.
- The resiliency assignments do not in any way bind a given device to a specific node. Devices that do not support redirection (a subset of MiNet devices, plus any SIP devices) will stay with the server to which they initially connected. Clustering load balancing does consider devices that cannot be redirected.

Boot Time Resiliency

When any MiNet device (including a non-clustered device) starts or reboots, it employs boot time resiliency to connect to its own, local MBG. It does this by checking its network configuration, which stored in non-volatile FLASH memory, and employs this to search for MBG. The network configuration is comprised of the following:

- **Resiliency List**: An optional; Resiliency List;of up to four IP addresses can be configured on MBG and sent to 53xx Series IP Phones. In a clustered environment, these addresses are typically for nodes belonging to the device's own cluster zone.
- **Teleworker IP**: MiNet devices operating in teleworker mode will have a Teleworker IP address (programmed by pressing 7 key on bootup on most phones).

- **DHCP**: If the device does not have a Resiliency List or Teleworker IP, DHCP is used to obtain an IP address.

For example, when a user reboots her MiNet device, the device will first check whether it has received a Resiliency List. If the list has not yet been configured or downloaded, the device will then check whether it has a Teleworker IP address. If the Teleworker IP address has not been configured, the device will obtain an IP address from a DHCP server. ;

NOTE:

- Boot time resiliency can be used in either a clustered or non-clustered environment.
- In a clustered environment, Mitel recommends populating the Resiliency List with nodes in the cluster. If the cluster is spread across a subnet boundary, include nodes from each subnet to prevent a single point of failure.

IP Translations

Multiple servers deployed on the same DMZ need to each be addressable by individual public IPs so Teleworker clients can reach them. The IP addresses configured on their interfaces should be DMZ addresses, most likely from the RFC 1918 range to prevent routing to or from the DMZ without specific rules in the firewall and on the LAN. This presents a problem for MBG servers that need to stream to one another.

Consider an example of two servers, server A and server B, both installed in a DMZ configuration on the same DMZ.

	Public IP	**DMZ IP**
MBG A	66.46.21.11	192.168.0.5
MBG B	66.46.21.12	192.168.0.6

Set 1 connected to MBG-A calls set 2 connected to MBG-B. MBG-B intercepts the signaling and MBG-A sees a request to stream from set 1 to the public IP of MBG-B. If MBG-A streams to MBG-B via its public IP, there is a very strong possibility that the firewall will not permit the SRTP traffic to route back to the DMZ that it originated from, resulting in audio problems. Furthermore, it is a waste of bandwidth on the public side of the firewall to stream traffic out to it that is destined for a server on the same network once the firewall's NAT rules take effect.

The solution is simple. Both problems are solved by streaming directly from MBG-A's to MBG-B using their DMZ addresses. Unfortunately MBG-A is not aware of the existence of MBG-B. This is the purpose of the IP Translations feature.

In the MBG management GUI, choose Configuration and then IP Translations. In this example, the administrator would enter the following rule on MBG-A: Destination address: 66.46.21.12 Translation address: 192.168.0.6

Now when MBG-A encounters the IP address of 66.46.21.12 in the call setup, it translates it to 192.168.0.6 instead. For this to work in both directions, a reciprocal rule must be entered on MBG-B: Destination address: 66.46.21.11 Translation address: 192.168.0.5

Now a two-way call is properly routable between the two servers.

NOTE: This feature is suitable only for small numbers of servers. For N servers, each server requires a list of N-1 translation rules. This becomes difficult to manage for larger values of N. An auto-population feature, leveraging the clustering support, is being investigated for a future release.

Streaming Addresses

The MBG server will automatically determine the correct IP addresses to which endpoints must send their (S)RTP, if the server has been put into a standard, supported configuration and the correct network profile for that configuration has been chosen. See Services for full details on the supported configurations.

However, sometimes it is necessary to override the default streaming addresses, typically due to a non-standard configuration. When the admin views the Network profiles (under the Configuration tab), the current network profile will be shown with an interface to apply the supported network profiles.

Arbitrary addresses can be entered by selecting the Custom profile, if the “canned” configurations are not suitable. These addresses are used during signaling to inform the endpoints where to send RTP. If they are incorrect, there will be audio problems (typically one-way audio or no audio).

DMZ Deployment Profile

When the MBG server is deployed in a DMZ (see Figure 3 on page 5), all endpoints should send RTP to the IP address seen by the Mitel AMC or SLS during a sync operation. This is the MBG server's publicly-visible address after any NAT by the DMZ firewall. This address is configured automatically when DMZ mode is selected.

If this address is incorrect for some reason (such as multiple layers of NAT), use the Custom profile to enter the correct address.

Gateway Deployment Profile

A standard example of the gateway deployment is shown in Figure 2 on page 4. In this configuration, the WAN interface on the server is routable on the “public” network. This is referred to as the “set-side” streaming address, to which teleworker devices and service provider trunk equipment sends RTP. The “public” network is typically the Internet, but may instead be a managed service-provider network, MPLS LAN extension, corporate network, etc.

The LAN interface is attached to the private network. This is referred to as the “ICP-side” streaming address, to which LAN devices (phones), conference bridges, ICPs, voicemails, etc send RTP. The private and public addresses must be on different IP networks.

The defaults are usually acceptable. However, if not, they can be changed by using the Custom profile.

RTP Frame Size

By default, the RTP frame size is auto-negotiated between the endpoints. A size of 20 ms is common in North America, with 40 ms becoming common in Europe. If needed, the administrator can force use of a particular frame size. For example, some SIP trunk service providers insist on a particular RTP frame size.

The Configuration tab holds the global master setting. This setting is used as the default, and should be left on “Automatic” unless there is a pressing need to change it. Overrides can be placed on specific devices and trunks as required. For example, certain wireless networks handle RTP streams using larger (e.g. 40 ms) packets better than streams using smaller ones.

NOTE: The frame size override only affects the streams to and from devices. The ICP-side streaming is always auto-negotiated. On SIP trunks, both WAN and ICP sides can be specified separately.

TFTP Block Size

MiNet devices use the TFTP protocol to fetch their firmware from the MBG server. The Mitel TFTP server is slightly non-standard – it uses symmetric UDP to traverse NAT devices, and a “sliding window” to improve performance – but is otherwise RFC-compliant.

The default block size in the TFTP protocol is 512 bytes, and with large firmware loads in a lock-step protocol like TFTP[1] this can take a prohibitively long amount of time to download. MBG employs the TFTP “blksize” option to attempt to transfer 4096 byte blocks, if possible. Depending on one’s network this may or may not be possible: the large packets will require fragmentation on a standard Ethernet network with a 1500 byte MTU, and some ISPs do not permit this.

Set the global TFTP block size to the largest value that works. If your MiNet devices are experiencing issues downloading firmware or HTML applications, change the value to 1024 bytes.

Only the options in the pulldown (512, 1024, 2048 or 4096) are permitted.

Compression Codecs

MiNet devices

If you are doing secure call recording and the 3rd-party call recording equipment (CRE) only supports G.711 or G.729, you can restrict MBG to using those codecs. If you are not operating under these limitations, you should allow MBG to use an unrestricted range of codecs.

In addition, to reduce the amount of bandwidth consumed on the Internet side of the connection, you can force remote MiNet sets to use a specific codec. If bandwidth is not an issue, you can allow the sets to select a codec independently. Note that if this option is enabled, compression licenses are required to support transcoding from the Internet side to the ICP side of MBG.

SIP devices

If you are doing secure call recording and the 3rd-party call recording equipment (CRE) only supports G.711 or G.729, you can restrict MBG to using those codecs. If you are not operating under these limitations, you should allow MBG to use an unrestricted range of codecs.

1. Receipt of each block must be acknowledged before the next block is sent

SRTP Port Range

Each active call on the MBG requires four UDP ports: two for RTP and two for RTCP streams. Some SIP calls (video, T.38) might require eight or more ports. (Two ports for RTP plus two ports for RTCP per SDP media line are required). Ports are only used while calls are actually active, and are released upon the end of the call, or, for MiNet, end of the stream (which may be a hold or transfer, not actually the end of the "call").

The default voice port range of 20002-29999 provides enough ports for 2499 simultaneous voice calls, while the default video port range of 30000-30999 provides enough ports for 249 simultaneous video calls. These ranges can be reduced for smaller sites, if needed. The resulting ranges must be large enough to support all concurrent and transient calls. These ranges can also be moved for specific network requirements. However, be sure any third-party firewalls have the matching range programmed. Mismatches between a DMZ firewall and the MBG will result in some calls having no audio (or one-way audio).

DSCP

MBG allows configuration of a Differentiated Services Code Point (DSCP) to be inserted into the header of ip packets. A separate value can be configured for signaling and media packets. This is one of the tools available to help improve voice quality in some congested managed network environments.

As an example, consider a deployment with a managed WAN on the ICP side of MBG and the Internet on the sets side of MBG. Now consider a situation where a managed WAN Service Level Agreement (SLA) is purchased that divides traffic into classes, including an Expedited Forwarding (EF) queue with priority over other traffic classes. In this situation, MBG can be configured to insert an EF value (46 decimal) for voice packets as they pass from the Internet to the ICP side so that they can be protected on the managed WAN during periods of congestion.

If the remote VoIP devices are only using voice then the bandwidth purchased for the EF queue must be large enough to accommodate the total number of concurrent voice streams passing through the MBG from Internet to manage WAN. However, if the remote VoIP devices will also be using video in this example, then the bandwidth purchased for the EF queue must account for both voice and video, keeping in mind that a video call requires 10 to 20 times more bandwidth than a compressed audio call even when devices are configured with the lowest bandwidth settings. Refer to section *Determine Bandwidth Requirements* for guidance on calculating required bandwidth.

Alternatively, if the cost is prohibitive for provisioning enough EF queue bandwidth to support both voice and video needed for the deployment, then MBG should not be configured to insert an EF value (46 decimal) for voice/video packets. The reason for this is to prevent video passing through the MBG from impacting voice on a managed WAN where EF bandwidth has only been provisioned for voice. A future release of MBG will support configuring different values for voice and video to address this scenario.

Recommended settings when enough EF queue bandwidth has been provisioned to support both voice and video:

- voice/video: 46 decimal (Expedited Forwarding)
- signaling: 24 decimal (Class Selector 3)

Recommended settings when enough EF queue bandwidth has been provisioned to support voice only:

- voice: 46 decimal (Expedited Forwarding)

- video: 34 decimal (Assured Forwarding 41)
- signaling: 24 decimal (Class Selector 3)

Sizing Your Installation

MBG installations come in many sizes, from a handful of remote workers, to large call centers with recording requirements, to service providers with hundreds of SIP trunks routed to customer Virtual MiVoice Businesses. This section provides guidelines for selecting appropriate hardware and network capacity for any size of installation.

For site with fewer than 500 users and 100 simultaneous streams, skip to section *Determine Call Equivalents*.

NOTE: The calculations in this section assume that no other applications besides MBG will be running on the MSL server.

Determining Line Size for Large Sites

Step One: Determine Call Rate

The first step is to estimate how busy the site will be. Ideally, this figure will come from observations of actual usage, but it can be estimated. The services provided by the MBG server affect how much load it needs to handle.

Consider a typical teleworker scenario: 20 users working in a remote office. Assume that these users are on the phone about 10 minutes of each hour, or 6 CCS. If the users make two calls per hour, each call is 300s (5 minutes) long.

Multiply the average CPH rate by the total number of users to get the Erlang-B lambda value:

- λ = 2 CPH * 20 users = 40 CPH

A call center might have usage of 20 CCS per agent. Assume an average call time of 600s (10 minutes). If the agent is busy 2000 call-seconds (20 CCS) and each call is 600s, the agent is handling 3⅓ calls per hour. For a busy call center with 1000 agents, lambda is:

- λ = 3.3333 CPH * 1000 users = 3333.3 CPH

Step Two: Determine Service Rate

The service rate, represented by μ, is the mean number of calls the MBG can handle successfully per unit of time, without blocking. If it takes 20 minutes to service one call, then three calls can be serviced per hour, and the service rate is 3 CPH.

In the teleworker example above, the call duration is 300s, so MBG is processing 12 calls per hour:

- μ = 12

In the call center example, the call duration is 600s, so the MBG is processing 6 calls per hour:

- μ = 6

Step Three: Determine Grade of Service

The grade of service, represented by P(b), is the percentage of calls that are turned away (blocked) because of insufficient capacity. The nominal and recommended P(b) is 1%, or 0.01.

Step Four: Erlang-B Calculator

An Erlang-B calculator can now be used with the values above to find the number of lines required to handle the load. (Free Erlang-B calculators are widely available online.) Following the teleworker example above, the Erlang-B calculation is:

- λ = 40, μ = 12, P(b) = 0.01
- c = 9

The site will need 9 lines to handle the load. In MBG terms, this is 9 simultaneous calls. The number of simultaneous calls is the key value in determining MBG resource requirements.

For the call center example:

- λ = 3333.3, μ = 6, P(b) = 0.01
- c = 583

The call center would require 583 lines (and agents) to handle the call volume. Again, this is 583 simultaneous calls going through the MBG.

Determine Call Equivalents

The next step is to determine the impact of transcoding, taps, and codec choices on CPU load and network bandwidth. The baseline is a single non-transcoded call with one RTP stream. The procedure in this step applies a load factor to convert more complex calls into an equivalent number of simple calls.

Usage	Call Equivalent (CPU)
Basic (non-transcoded) call	1
Transcoded call	2.5
SIP trunk call	1
Tapped call	1.5

Example:

4 MiNet sets all in calls with other parties, plus 2 SIP trunk calls, and two of the calls being tapped, all using G.711, would constitute:

CPU use = (4 MiNet calls – 2 tapped) + 2 SIP trunk + 2 tapped

= 2 untapped + 2 trunk + 2 tapped

= 2 + 2 + 2*1.5

= 7 calls

Determine Bandwidth Requirements

VoIP devices, including phones and SIP trunks, use RTP/SRTP for voice communication. The bandwidth required for the RTP stream depends on the codec selected by the device. MiVoice Border Gateway supports the use of G.711, G.729, and G.722.1. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be considered as well.

Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service of the MiVoice Border Gateway.

The bandwidth figures for a single device are provided in *Bandwidth Requirements for the Remote Site*. For multiple devices, follow the procedure below.

Assumptions:

- Internet Service Providers specify bandwidth available to the user. i.e. PPPoE overhead does not need to be included in the provisioning of DSL bandwidth, but IP overhead does need to be included.
- RTP Bandwidth Requirements are as follows:
  - G.711 = 80 Kbps
  - G.729 = 24 Kbps
  - G.722.1 = 48 Kbps
- At 6 calls per hour Control stream bandwidth requirement is 20 Kbps peak for each 12 remote devices, and 1 Kbps idle for each remote device.
- The calculation below does not include bandwidth required for features such as paging. If group paging is enabled for teleworkers, an additional RTP stream should be provisioned for each remote member of the paging group.
- Whenever possible, transcoding should be performed by the ICP rather than the MiVoice Border Gateway, as this typically provides improved voice quality.
- If the mix of codecs in use cannot be reliably estimated, it is safest to assume G.711 for all calls.

NOTE: The actual bandwidth available will likely be less than the amount of bandwidth the ISP advertises. ; Also, the amount of available bandwidth may fluctuate throughout the day based on usage patterns of other subscribers.

The best way to determine the amount of available bandwidth is to use a speed test tool, preferably one provided by a third party rather than the ISP themselves – buyer beware.

G.711 Calculation

Bandwidth = number of users * idle control stream requirement

+ number of calls * RTP requirement

+ number of users / 12 * peak control stream bandwidth

For the teleworker example of 20 remote users:

20 * 1 Kbps + 9 * 80 Kbps + 20/12 * 20 Kbps

= 773 Kbps

For the call center example of 1000 remote agents:

1000 * 1 Kbps + 583 * 80 Kbps + 1000/12 * 20 Kbps

= 49307 Kbps or 48.15 Mbps

G.729a Calculation

Bandwidth = number of users * idle control stream requirement

+ number of calls * RTP requirement

+ number of users / 12 * peak control stream bandwidth

For the teleworker example:

20 * 1 Kbps + 9 * 24 Kbps + 20/12 * 20 Kbps

= 270 Kbps

For the call center example:

1000 * 1 Kbps + 583 * 24 Kbps + 1000/12 * 20 Kbps

= 16659 Kbps or 16.27 Mbps

Video Calculation

Some VoIP devices support video as well as voice, and extra bandwidth must be provisioned if video calls will be made. Although the exact bandwidth required depends on the content of the image, number of frames per second (fps), the codec and compression selected, and the video resolution, the list below gives approximations for some typical video streams.

<table>
<tr><th>Codec</th><th>Resolution</th><th>FPS</th><th>Bandwidth</th></tr>
<tr><td rowspan="2">H.263 or H.264
~ 384 kbps</td><td rowspan="3">QCIF (176x144)</td><td>15</td><td>~ 128 kbps</td></tr>
<tr><td>30</td><td>~ 256 kbps</td></tr>
<tr><td rowspan="3">CIF (352x288) or QVGA (320x240)</td><td>15</td></tr>
<tr><td>30</td><td>~ 768 kbps</td><td></td></tr>
<tr><td>MPEG-4
~ 128 – 360 kbps</td><td>CIF (352x288) or 320x240</td><td>15 – 30</td></tr>
</table>

This list shows the bandwidth required for video streams from some Mitel devices contrasted with bandwidth required for other types of media streams.

<table>
<tr><td rowspan="2">Voice
MiCollab Audio, Web and Video Conferencing</td><td>If compression (G.729a) enabled: 24 Kbps (bi-directional)
If compression not enabled (G.711): 80 Kbps (bi-directional)</td></tr>
<tr><td>192 Kbps (bi-directional)</td></tr>
<tr><td rowspan="2">MiCollab Client Video
MiVoice Video Unit</td><td>256 Kbps – 1600 Kbps (bi-directional)</td></tr>
<tr><td>512 Kbps – 1500 Kbps (bi-directional)</td></tr>
</table>

NOTE: A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

The Internet bandwidth provisioned at the MBG server must take into account the maximum number of simultaneous video calls from the remote devices and applications.

When a MiVoice Video Unit initiates a video conference it will also serve as the video bridge for the conference. For example, a MiVoice Video Unit that is acting as a video bridge for a 4 party conference will require three times the video bandwidth and three times the audio bandwidth required by a MiVoice Video Unit that is only a participant in the conference.

Video calls between MiCollab Client 6.0 and MiVoice Video Unit 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a MiCollab Client on the Internet will receive video at the rate configured on a MiVoice Video Unit on the LAN even if the MiCollab Client is configured to use low bandwidth. This will be rectified in a future release of MiCollab Client and/or MiVoice Conference/Video Unit.

MiCollab Audio, Web and Video Conferencing between AWV clients via the MiCollab AWV Conferencing server is also supported through MBG. The bandwidth usage per video stream is configurable on the AWV client. An additional consideration is that an AWV client can receive multiple video streams, one for each video participant in the conference. That number can be reduced at the AWV client by minimizing or closing video windows.

For details and current values, see the engineering guidelines for the devices/applications referenced as examples here (available in Mitel Document Center).

Fax Calculation

A fax call made over a SIP trunk or to a SIP device supporting fax will be either a G.711 voice stream or a T.38 fax session. For the purposes of bandwidth calculations, consider both cases to be an 80 kbps G.711 stream.

Call Recording Calculation

When using MBG's call recording services (Secure Call Recording or SIPREC), a third-party Call Recording Equipment (CRE) device requests “taps” of calls in progress. With Secure Call Recording (SRC), the control connection is an SSL-encrypted TCP stream authenticated by an X.509 client certificate provided by the CRE. With SIPREC, the control connection uses SIP TCP or TLS depending on CRE capabilities.

A small amount of bandwidth is used for the CRE control connection. However, it is usually insignificant when compared to the volume of voice traffic, and can be safely ignored. A small amount of CPU load is also incurred for the control connection. Again, it is usually insignificant compared to the load of processing voice signaling and RTP.

MBG makes a copy of the RTP streams for each call that is being recorded, and forwards them to the CRE. Therefore, each tapped call requires 50% more bandwidth than an untapped call. Only audio is recorded; any video or T.38 streams should be ignored when calculating call recording bandwidth requirements. Simply estimate the number of calls that will be recorded simultaneously, and multiply by the codec in use. When in doubt, it is safest to assume G.711 for all calls.

For example, assume that 10 calls will be recorded at a time. All calls are G.711.

Bandwidth = 10 calls * 80 kbps = 800 kbps

The site requires 800 kbps on top of the bandwidth used by the calls themselves.

NOTE: When transcoding, the bandwidth requirements are different on the two “sides” of the MBG.

Example Bandwidth Calculation

A site has 48 SIP trunks shared by remote and in-office users. Most users are in the office, but 100 work in various remote branch offices with Teleworker phones hosted on a MiVoice Business at the main office. Remote phones are configured for G.729 to save bandwidth, and all SIP trunk calls are G.711. (MiVoice Business handles any transcoding.) In addition, the site records up to 10 remote office calls at any given time.

At peak, the site uses 40 trunk channels and 75 of the remote users are in a call. Ten percent of the remote users are in MiCollab Client video calls configured to match the lowest bandwidth setting of a MiVoice Conference/Video Unit.

The system is deployed in gateway mode, in parallel with the company firewall.

Step one: G.711 trunk calls WAN BW = 40 channels * 80 kbps = 3200 kbps LAN BW = 40 channels * 80 kbps = 3200 kbps

Step two: Remote office calls; voice WAN BW = 75 * 24 kbps = 1800 kbps LAN BW = 75 * 24 kbps = 1800 kbps

Step three: Remote office calls; video 10% of 75 users = 7.5 WAN BW = 7.5 * 512 kbps = 3840 kbps LAN BW = 7.5 * 512 kbps = 3840 kbps

Step four: Recorded calls LAN BW = 10 tapped calls * 24 kbps = 240 kbps

Step five: Totals

Adding up the results from the four steps, the WAN bandwidth requirement is 3200 + 1800 + 3840 kbps for a total of 8840 kbps. The site will require at least a 9 megabit connection just for voice and video capacity. The LAN bandwidth, which includes tapped calls, is 3200 + 1800 + 3840 + 240, or 9080 kbps.

NOTE: For a server in LAN mode or in a DMZ (with a single NIC), calculate the bandwidth required for the WAN “side” (no tap streams) and LAN “side” (including tap streams) and add them together, since one NIC handles all of the traffic. In the example above, the network would have to handle 8840 + 9080 = 17920 kbps, or 17.9 Mbps. However, the WAN pipe still only has to handle 9 Mbps.

NOTE: See also sections *Web Proxy and Remote Management Service Requirements*, *MiCollab Client and MiCollab AWV Conferencing Requirements* and *MiContact Center Softphone Requirements*.

Hardware Selection

Installations with less than or equal to 500 users and up to 100 simultaneous streams can select any server on the MSL Qualified Hardware List. Larger sites can use the Call Equivalents obtained in section *Determine Call Equivalents* to determine the necessary number of servers.

Web Proxy and Remote Management Service Requirements

The bandwidth requirements for any and all applications proxied by Web Proxy and Remote Management Service are documented in their respective Engineering Guidelines, and are beyond the scope of this document. See *Web Proxy* for relevant firewall rules.

MiCollab Client and MiCollab AWV Conferencing Requirements

MiCollab Client with Softphone module counts as a remote IP set, with additional bandwidth required for its login and presence. The login and presence connections use negligible bandwidth and do not require real-time priority. The MiCollab Client SIP Softphone supports video calls, which requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings (see section 13.3 for examples).

MiCollab Audio, Web and Video Conferencing between AWV clients via the AWV server is also supported through MBG, which requires significantly more bandwidth than audio calls (see section 13.3 for examples).

A MiCollab AWV Conferencing connection can also require considerable bandwidth, based on the features used, the number of presenters, and the number of participants. The table below provides a typical use-case by number of presenters and participants, with the estimated bandwidth required. For more details, refer to the MiCollab Engineering Guidelines.

NOTE: The table assumes the following settings:

- **PowerPoint sharing**: enabled
- **Desktop/App Sharing**: disabled
- **Audio Setting**: good
- **Video Setting**: low

The collaboration bandwidth is in addition to that required for voice communications. Refer to *Additional Application Requirements* for the relevant firewall rules.

Table 13.1: Bandwidth Requirements for MiCollab AWV Conferencing Collaboration

Presenters	Participants	Bandwidth Required
1	1	192 Kbps
1	2	256 Kbps
1	5	448 Kbps
2	2	460 Kbps
2	5	736 Kbps
1	10	768 Kbps
2	10	1.2 Mbps
2	50	4.9 Mbps
5	100	18.7 Mbps

MiContact Center Softphone Requirements

MBG release 4.5 introduced support for the MiContact Center Softphone version 5.3. The softphone has multiple components. Bandwidth requirements of the voice component are identical to any other Mitel set

using G.711 or G.729 (compression). In addition to voice, MiContact Center Softphone supports the following connections through the MBG server:

MBG Server Port Used	Default Destination Port	Description
TCP 36000	TCP 80	HTTP authentication and user profile access
TCP 36001	TCP 443	HTTPS authentication and user profile access
TCP 36002	TCP 5024	Real-time client
TCP 36003	TCP 5025	Auditor connection
TCP 36004	TCP 5026	Telephony proxy

The “MBG Server Port Used” column indicates the port on which MBG listens, on its Internet-facing side, for the incoming connection. The “Default Destination Port” is the port on the MiContact Center server to which MBG routes the connection. Additional MiContact Center connections were added over multiple releases and as of MBG 8.0 also includes MBG Server TCP ports 35001 to 35008 inclusive. Refer to *MiContact Center* for firewall configuration instructions.

Bandwidth requirements will vary depending on the type of activity being performed. During installation of the client, software is downloaded and installed. The client periodically checks for updates and may download and install them. The bandwidth required by these tasks is not included in the tables below; it is assumed to be part of the bandwidth used by the user's PC.

When a user first launches the MiContact Center client and selects devices to view, there is a database transfer. The size of the database depends on the objects selected, as follows:

- 1 Queue (Q) = 65 KB
- 1 Agent (A) = 39 KB
- 1 Employee = 20 KB
- 1 Extension = 17 KB
- 1 Network Monitor (NM) (1 x MiVoice Business) = 56 KB

Refer to the following table to determine the size and download time for the database at various line speeds.

# of Devices	Config	Data Size	512 Kbps	1024 Kbps	1.54 Mbps	2.048 Mbps	10 Mbps
5	1Q, 1A 1Ex, 1Em, 1NM	157.6 KB	00:00:02	00:00:01	00:00:01	00:00:00	00:00:00
50	15Q, 11A, 11Ex, 12Em, 2NM	303.2 KB	00:00:04	00:00:02	00:00:01	00:00:01	00:00:00
100	25Q, 25A, 22Ex, 25Em, 3NM	348.8 KB	00:00:06	00:00:03	00:00:02	00:00:01	00:00:00
500	200Q, 100A, 92Ex, 100Em, 8NM	1.304 MB	00:00:20	00:00:10	00:00:06	00:00:05	00:00:01

# of Devices	Config	Data Size	512 Kbps	1024 Kbps	1.54 Mbps	2.048 Mbps	10 Mbps
1500	500Q, 300A, 385Ex 300Em 15NM	3.528 MB	00:00:55	00:00:27	00:00:18	00:00:13	00:00:02
5000	2086Q, 2379A, 247Ex, 322Em, 16NM	14.24 MB	00:03:42	00:01:51	00:01:13	00:00:55	00:00:11
8100	3036Q, 4379A, 247Ex, 322Em, 16NM	22.72 MB	00:05:55	00:02:57	00:01:57	00:01:28	00:00:18

NOTE: The use of traffic shaping (to prioritize RTP ahead of other packets) could be used to prevent data transfers, such as the initial DB transfer above, from affecting calls in progress.

The table below provides bandwidth requirements for a typical MiContact Center configuration at various call rates, in addition to the bandwidth required for voice communications.

Calls per Hour (CPH)	Bandwidth per ICP	Bandwidth per Real-Time Client
100	0.48 kbps	0.48 kbps
1000	4.88 kbps	4.72 kbps
2000	9.76 kbps	9.44 kbps
3000	14.72 kbps	14.16 kbps
4000	19.6 kbps	18.88 kbps
5000	24.48 kbps	23.6 kbps
6000	29.36 kbps	28.32 kbps

NOTE: This is a guideline only. Actual results may differ depending on the MiContact Center configuration.

Virtual MBG Considerations

Virtual MiVoice Border Gateway (vMBG) is the MBG software and supported Mitel Standard Linux (MSL) operating system bundled in a VMware Virtual appliance, to run in the VMware vSphere/ESX(i) hypervisor. The software is packaged in Open Virtualization Format (OVF) for deployment into a VMware environment.

MBG can also be installed on a Microsoft Hyper-V hypervisor. This type of virtual deployment is identical to a physical installation. The only limitations are that you can mount the ISO image from a network drive or CD/DVD, but not from a USB device, and that you require a virtual product license applied the ARID.

For detailed information concerning the VMware and Hyper-V deployments, including hardware and software requirements, refer to the *Virtual Appliance Deployment Guide*.

Licensing

The standard MBG base kit cannot be used to run an instance of vMBG. The “MiVoice Border Gateway Virtual Appliance” base kit (part number 54005339) must be used instead. An existing base kit can be converted.

WARNING: If the wrong base kit is used, the vMBG will have no licenses.

Upgrades

A virtual MBG can be upgraded just like a physical MBG, by visiting the MSL Blades panel and downloading the update from Mitel Software Download Center. Alternately, an MBG CD, available from Mitel MiAccess, can also be used via the VMware console.

MSL can also be upgraded either with the MSL ISO image available from Mitel MiAccess, or by clicking on the ServiceLink blade upgrade in the MSL Blades panel.

From time to time, Mitel releases new OVA files on Mitel MiAccess. The OVA must be used for initial deployment of a vMBG, but can also be used for upgrades by following the procedure below:

1. Back up[1] the current MBG using the application's back-up button.
2. Deploy the new OVA
3. Restore the backup file using the application's restore button

This procedure can also be used to convert a physical to a virtual MBG.

Alternately, a full backup of the MSL server can be performed, followed by deploying a new OVA, and then a restore of the backup using the MSL server console.

1. Mitel recommends making frequent backups of your important data

Host Server Requirements

Hardware

For information concerning hardware requirements and server capacities in VMware and Hyper-V deployments, refer to the *Virtual Appliance Deployment Guide*.

Software

For information concerning software requirements in VMware and Hyper-V deployments, refer to the *Virtual Appliance Deployment Guide*.

High-Availability

As with physical MBG servers, high-availability is achieved through MBG clustering. However, with virtual hardware, there is an additional consideration. To avoid a single point of failure, Mitel recommends using VMware anti-affinity rules to prevent all cluster nodes from running on the same physical host hardware. See the *Virtual Appliance Deployment Guide* for details.

Solutions to Common Problems

Changing a Cluster Node's IP Address

MBG clustering uses IP addresses to identify each node and to initiate cluster communications connections.

To change a node's IP address, Mitel recommends the following procedure:

1. Make sure that the node to be changed is not the master node. Take ownership from another node if required.
2. From the slave node to be changed, go to the clustering tab and click on the “Leave cluster” button.
3. Reconfigure the address via the MSL console, and follow the prompts to reboot.
4. Add the node on the master, and join the server to the cluster.

T.38 Faxing Does Not Work With NAT

Use of T.38 fax is not compatible with NAT. A fax device behind a NAT firewall/router that does not perform its own NAT traversal may not be able to receive T.38 faxes. It may be able to send them.

During the T.38 setup, the receiving fax listens for incoming tones from the sending fax (no-signal, v21-preamble, etc), then sends tones in response. However, MBG cannot send media to a device behind NAT until that device first sends at least one media packet to the MBG. In a T.38 setup, that will never happen, and the sender's tones are discarded. The call fails (after several retries by the sender).

If the sending fax is behind NAT and the receiving fax is not, the call should work.

It is possible to receive T.38 faxes when behind NAT with certain types of call setup. However, it is not wise to rely on a certain type of negotiation since T.38 calls can be set up in several ways.

Fax devices that support NAT traversal such as STUN should be able to work around this limitation. They appear to MBG as a device with a public address, and MBG can send to them without needing to receive a packet first. Use of G.711 faxing is another option, although it requires a very clean stream. Customers can also use a third-party fax to email or fax to web service.

NOTE: This problem does not apply to SIP trunks; there is no NAT on trunks.

Performance Characteristics and Limits

Mitel continually evaluates hardware and virtual hardware platforms with MBG to determine its maximum capacity. The following are the results of testing with MBG 10.1. These numbers assume a typical office call rate of 6 CCS.

Physical Hardware

CPUs: Dual Hex Core Intel® Xeon® CPU E5-2667 (Sandy Bridge) 2.9 GHz with Hyperthreading

Memory: 32 GB

Network: Gigabit (For details, see the note following the “MBG Capacities” table on the next page)

OS: Mitel Standard Linux

For information concerning supported hardware servers for the MiVoice Border Gateway, refer to the *MSL Qualified Hardware List* that is available in Mitel Document Center.

Virtual Hardware

Two deployment configurations are available—Small Business and Enterprise. For information concerning the capacities available with each configuration, refer to the *Virtual Appliance Deployment Guide* in Mitel Document Center.

MBG Capacities – Device (MiNet & SIP) and Trunking (SIP)

	System Type	Server Size	Protocol	Registered Devices	Concurrent ;G.711 Calls	Call Rate	Network	Network Card*
MiNet Set Capacity	Physical Limit	Enterprise	MiNet	5000	1600	6 ccs	1 x 10 GB	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
	Physical Limit	Enterprise	MiNet	10,000	1600	3 ccs	1 x 10 GB	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
	Physical Limit	Enterprise	MiNet	5000	3000	6 ccs	1 x 10 GB	Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
SIP Set Capacity	Physical Limit	Enterprise	SIP Sets	5000	800	6 ccs	1 x 10 GB	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
	Physical Limit	Enterprise	SIP Sets	5000	3000	6 ccs	1 x 10 GB	Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)

	System Type	Server Size	Protocol	Registered Devices	Concurrent ;G.711 Calls	Call Rate	Network	Network Card*
SIP Trunk Capacity	Physical Limit	Enterprise	SIP Trunking	—	800	6 ccs	1 x 10 GB	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
	Physical Limit	Enterprise	SIP Trunking	—	690	6 ccs	1 x 10 GB	Broadcom Corporation BCM57840 NetXtreme II 10/20-Gigabit Ethernet (rev 11)
	Physical Limit	Enterprise	SIP Trunking	—	1100	6 ccs	1 x 10 GB	Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)

NOTE:

- The capacity for concurrent calls is dependent on the network interface controller (NIC) being used. The maximum number of concurrent calls that can be sustained is directly dependent on the performance of the NIC that is installed on the server. In performance testing done by Mitel, bandwidth was typically not an issue (i.e. a 1GB NIC of any type was able to sustain 6 ccs and testing was done successfully with various 1GB and 10GB NICs). NICs with an on-board processor (such as the Intel 82599ES 10GB NIC shown above) can sustain over twice the number of concurrent calls than those without, such as the Broadcom BCM5719 10GB NIC. The Broadcom BCM5719 10GB NIC can Mitel tested could only sustain 1,600 concurrent calls compared to 3325 by the Intel 82599ES NIC. Mitel recommends the NIC selection be done with the expected traffic levels (concurrent calls) in mind.
- SIP Trunk Capacity is tested with zero registered devices. For a mixed-use system (SIP trunks and SIP or MiNet devices), use the MiNet Set Capacity figures.

MBG Capacities – WebRTC

	System Type	Server Size	Protocol	Audio	Audio and Video without transcoding	Audio and Video with transcoding	Network	Network Card*
WebRTC Capacity	Physical Limit	Enterprise	SIP	800	300	36	1 x 10 GB	Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe (rev 01)
	Physical Limit	Enterprise	SIP	2000	600	36	1 x 10 GB	Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)

NOTE:

- The capacities listed above require MBG to be dedicated to WebRTC calls. If the system is being used for other purposes, such as SIP trunking or call recording, the capacities will be reduced.
- Mitel recommends the use of Professional Services for any deployments with an expected number of concurrent WebRTC users greater than 500. This allows the appropriate deployment topology to be recommended.
- Transcoding video can be CPU intensive. To prevent your system from experiencing issues, instruct your users to limit the number of video calls that they place at any one time. Alternatively, enable transcoding only if your implementation includes devices which require it, such as the Mitel MiVoice Video Phone (UC360).

Web Proxy Capacities

System Type	Server Size	Protocol	Connections
Physical	Enterprise	MiContact Centre Ignite	1200
Virtual	Enterprise	MiContact Centre Ignite	1200

System Type	Server Size	Protocol	Connections
Virtual	Small Business	MiContact Centre Ignite	250

NOTE: Maximum MiCC Ignite connections per cluster:

- **No resiliency**: 7200 (1200 x 6 nodes)
- **Full resiliency**: 3600 (1200 x 3 nodes + 3 spares)

MBG System Capacities

	Limit	Configuration	Comment
Max Routing Rules	50000	Physical Enterprise	Up to 50,000 routing rules can be configured on a single MBG.
Maximum SIP Trunks	500	Physical Enterprise	Up to 500 SIP trunks can be configured on a single MBG.
Maximum PBX Connections	500	Physical Enterprise	Up to 500 PBXs can be connected to a single MBG.
Maximum Clustered MBGs	6	Any	Up to 6 MBG nodes can be clustered in a single cluster. The cluster must be configured as 5+1, with one MBG reserved for redundancy.
Maximum Devices in a Cluster	25,000 @ 6 ccs per device 50,000 @ 3 ccs per device	Physical Enterprise	An MBG cluster of 6 nodes supports up to 25,000 devices (5 x 5,000 devices, with one node reserved for redundancy) at 6 ccs per device, or up to 50,000 devices (5 x 10,000 devices with one node reserved for redundancy) at 3 ccs per device.

Appendix A: Firewall Configuration Reference

The information in this section is provided to allow configuration of a customer's firewall for the MiVoice Border Gateway in DMZ deployment. This configuration is automatic in the "MBG server as the gateway" deployment. In all cases below, "server" refers to the MiVoice Border Gateway server (that is, the MSL server). In the Direction column, the direction of the arrow indicates permission to initiate new connections in that direction. These rules assume a firewall that will permit return traffic on an existing established connection.

Port Range	Direction	Purpose and Description
AMC Communications		
TCP 22 (SSH)	Server -> Internet	AMC Communications. Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable server registration, software and license key downloads, alerts, and reporting.
UDP 53 (DNS)	Server -> Internet or Server -> Corporate DNS server	DNS. The server requires DNS to look up the IP addresses of the Mitel AMC and Software Download Center as well as for correct operation of SIP. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the *MSL Installation and Administration Guide* for details.
SLS Communications		
TCP 22 (SSH)	Server -> Internet	SLS Communications. Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable server registration, software and license key downloads, alerts, and reporting.
Mitel Software Download Center		
TCP 443 (HTTPS)	Server -> swdlgw.mitel.com 216.191.234.100	Blades download - access token for content delivery network
TCP 443 (HTTPS)	Server -> swdl.mitel.com port 443 (IP address based on location)	Blades download - access to content delivery/blades Akamai
Local and Remote Management		

TCP 443 (HTTPS)	LAN -> Server	Local Server Management. Allow inbound and outbound packets on TCP port 443 between the MBG Server and the LAN to allow for management of the server. HTTPS access to the manager on the external interface must also be explicitly enabled from the server-manager interface. The firewall should be configured to limit HTTPS access to desired management hosts.
TCP 443 (HTTPS)	Internet -> Server	Remote Server Management (Optional). Allow inbound and outbound packets on TCP port 443 between the MBG server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface. The firewall should be configured to limit HTTPS access to desired management hosts.
TCP 22 (SSH)	LAN -> Server	Remote SSH access (Optional). If the admin wishes to administer the MBG server remotely via the command line from the LAN, this rule is required.
TCP 22 (SSH)	Internet -> Server	Remote SSH access (Optional). If the admin wishes to administer the MBG server remotely via the command line over the Internet, this rule is required.
Clustering		
TCP 6809	Between servers in a cluster	Cluster Comms. If making use of clustering in MBG, this port must be open between the servers in the cluster to permit them to communicate with one another.
Voice and Video Communications for MiNET Devices, SIP Devices and SIP Trunking		
UDP 20000	Internet -> Server	Teleworker Analyzer Port. Allow incoming access to UDP port 20000 for the Teleworker Network Analyzer tool to run its diagnostics test.
UDP 20002-29999 (Configurable in MBG port range panel)	Internet -> Server LAN -> Server	Voice Communications. Allow incoming traffic on UDP ports 20002 to 29999 from all streaming devices on the LAN and the Internet. Misconfiguration here is a common cause of one-way audio issues. Note that the port boundary values (20002 to 29999) are configurable in the MBG interface. Mitel recommends keeping the default range when possible and avoiding the 50000-50999 range to reduce conflicts with other applications.
UDP 30000-30999 (Configurable in MBG port range panel)	Internet -> Server LAN -> Server	Video Communications. Allow incoming traffic on UDP ports 30000 to 30999 from all streaming devices on the LAN and the Internet. Misconfiguration here is a common cause of one-way audio issues. Note that the port boundary values (30000 to 30999) are configurable in the MBG interface. Mitel recommends keeping the default range when possible and avoiding the 50000-50999 range to reduce conflicts with other applications.

UDP 1024 - 65535 (RTP)	Server -> LAN Server -> Internet	Voice and Video Communications. Allow outgoing SRTP on UDP ports greater than, or equal to 1024 from the server to all streaming devices on the LAN and the Internet. Misconfiguration here is a common cause of one-way audio problems. Note that as of release 7.0, MBG defaults to using even-numbered ports for RTP, leaving the odd-numbered ports for RTCP. The Internet portion of this rule can be safely omitted in the absence of Internet traffic.
MiNET 52xx/53xx/69xx Basic		
UDP 20001	Internet -> Server LAN -> Server	TFTP server. Allow access to UDP port 20001 to allow MiNET devices to download their firmware and applications using TFTP
TCP 6800, 6801 and 6802	Server -> LAN Server -> ICP(s)	MiNet Call Control. Allow incoming and outgoing packets for TCP ports 6801 (MiNet-SSL) and 6802 (MiNet-Secure V1) between the server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNet), 6801 and 6802 between the server and the LAN and the server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN but ensure that the ICP(s) can communicate with the server's public address.
TCP 6801 and 6802	Internet -> Server	MiNet Call Control. Same as above. Port 6800 should not be used on the Internet as it is unencrypted. Port 6802 is not required with an Enhanced Security deployment.
TCP 3998, 6881	Internet -> Server	SAC Connection Support. Allow incoming TCP from the Internet to the MBG server, on ports 3998 and 6881, to support applications and web browsing, respectively, on the 5235, 5330, 5340 and Navigator sets. There is an additional LAN rule that follows this to complete the support.
TCP 3998, 3999 and 6881	Server -> ICP(s)	SAC Connection Support. Allow bidirectional TCP traffic on port 3999 to/from the ICP(s). This is to support the applications on the 5235, 5330, 5340 and Navigator sets. Note: 3998 and 6881 require an additional, MBG server on the LAN to which the Internet-facing server is daisy-chained.
TCP 80	Server -> LAN Server -> Internet	SAC Connection Support (Optional). Allow TCP port 80 from the server to the Internet, and to the LAN, to support web browsing on the 5235, 5330, 5340 and Navigator sets. Also required to the Internet to allow browsing of the Internet from the set.
UDP Port 20001	Server -> ICPs	HTML application autopopulation support (Optional). To permit MBG to autopopulate HTML applications from the ICPs, bidirectional traffic from a random UDP port on MBG to UDP port 20001 on the ICPs must be permitted.
MiNET 69xx Series enhanced feature support – MiNET Generic Plus		

TCP 6881	Internet -> Server	MiNet 69xx series IP Phones avatar, enhanced application or external LDAP server support (Optional). Allow incoming TCP from the internet to the MBG server on port 6881 to support avatars, enhanced applications or external LDAP server access on 6920, 6930, and 6940.
TCP 389	Server -> LAN	MiNet 69xx Series Phones (Optional). To enable 6920, 6930, 6940 phones to access the company directory, this port must be permitted from the Server to the LDAP database server on the LAN.
TCP 80	Server -> MiCollab Server	MiNet 69xx series IP Phones avatar support. Allow MiVoice Border Gateway to connect to the MiCollab server to retrieve avatars for 6920, 6930, 6940.
TCP 80 or TCP 443	Server -> Application Server	MiNet 69xx series IP Phones enhanced application support (Optional). Allow MiVoice Border Gateway to connect to the application server to provide enhanced features on 6920, 6930, 6940.
MiNET 5550 IP Console and MiVoice Business Console Support – MiNET Generic Plus		
TCP 6806	Internet -> Server	IP Console Support and MiVoice Business Console (Optional).
TCP 1606	Server -> LAN	IP Console Support and MiVoice Business Console (Optional).
TCP 6807	Internet -> Server	IP Console and MiVoice Business Console Support for presence (Optional).
TCP 18100	Server -> LAN (MiCollab Server)	IP Console and MiVoice Business Console Support for presence (Optional).
TCP 443	Server -> LAN	IP Console Support and MiVoice Business Console (Optional).
SIP Devices - Generic		
UDP 53	Server -> DNS server	DNS. The server requires DNS for correct operation of SIP.
UDP 5060	Server <-> ICPs Server <-> Internet	SIP UDP Support. If the SIP connector is enabled, then this port is required for non-encrypted SIP signaling between MBG and the set, between MBG and the ICP
TCP 5060	Server <-> Internet Server <-> ICPs	SIP TCP Support. Open this port for SIP signaling over TCP between MBG and SIP devices that have been updated to use TCP to port 5060. This port may also be opened between MBG and the ICPs.
TCP 5061	Server <-> Internet Server <-> ICPs	SIP TCP/TLS Support. This port is required for SIP signaling between MBG and SIP devices that have been configured to use TCP/TLS to port 5061 (the default client configuration). This port may also be opened between MBG and the ICPs.
SIP Devices - Mitel 68xx phones with MX-ONE (Optional)		

UDP 53	Server -> DNS server	DNS. The server requires DNS for correct operation of SIP.
TCP 5061	Internet -> Server	Support for Mitel 68xx/69xx SIP phones. This port is required for encrypted SIP signaling between Mitel 68xx phones and MBG
TCP 5060 or UDP 5060	Server -> LAN	Support for Mitel 68xx SIP phones. This port is required for SIP signaling between MBG and MX-ONE
TCP 22223	Internet -> Server	Support for Mitel 68xx phones with MX-ONE (Optional). This port must be permitted to enable encrypted XML connections from Internet-based 68xx phones to the server.
TCP 22222	Server -> LAN	Support for Mitel 68xx phones with MX-ONE (Optional). This port must be permitted to enable unencrypted XML connections from the server to the LAN-based MiVoice MX-ONE ICP.
TCP 4431	Internet -> Server	Support for Mitel 68xx SIP phones with configuration server (Optional). This port must be permitted to enable connections from Internet-based 68xx phones to the server.
TCP 80 or TCP 443	Server -> LAN	Support for Mitel 68xx SIP phones with configuration server (Optional). This port must be permitted to enable HTTP (TCP 80) or HTTPS (TCP 443) connections from the server to the LAN-based MiVoice MX-ONE configuration server.
SIP Device - Mitel 68xx/69xx Phones with MiVoice Office 400 (Optional)		
UDP 53	Server -> DNS server	DNS. The server requires DNS for correct operation of SIP.
UDP 69	Server -> LAN	Support for Mitel 68xx/69xx phones with MiVoice Office 400 (Optional). This port must be permitted to allow MBG to fetch initial startup.cfg, melody wave files and language files from MiVoice Office 400.
TCP 80	Internet -> Server	Support for Mitel 68xx/69xx phones with MiVoice Office 400 (Optional). This port must be permitted to allow phones to retrieve their initial startup.cfg, root certificates, melody wave files and language files from MBG.
TCP 5061	Internet -> Server	Support for Mitel 68xx/69xx SIP phones with MiVoice Office 400 (Optional). This port is required for encrypted SIP signaling between Mitel 68xx phones and MBG
TCP 5061 or TCP 5060	Server -> LAN	Support for Mitel 68xx/69xx SIP phones with MiVoice Office 400 (Optional). Either TCP 5060 or TCP 5061 (encrypted) is required for SIP signaling between Mitel 68xx/69xx and MiVoice Office 400.
TCP 4431	Internet -> Server	Support for Mitel 68xx/69xx phones with MiVoice Office 400 (Optional). This port must be permitted to enable encrypted XML connections from Internet-based phones to the server.

TCP 443	Server -> LAN	Support for Mitel 68xx/69xx phones with MiVoice Office 400 (Optional). This port must be permitted to enable encrypted XML connections from MBG to MiVoice Office 400. This port is also required for access to Self Service Portal
TCP 443	Internet -> Server	Support for Mitel 68xx/69xx phones with MiVoice Office 400 (Optional). This port must be permitted to allow end users to access the MiVoice Office 400 Self Service Portal via Remote Proxy.
SIP Device - MiVoice Conference Phone (Optional) See SIP devices – Generic Plus		
TCP 35010	Internet -> Server	Mitel MiVoice Conference Phone (Optional). The UC360 connects to the MBG on TCP port number 35010 to securely access an Active Directory server on the Customer's LAN.
TCP 389	Server -> LAN	MiVoice Conference Phone (Optional). To enable Conference Phone users to access the company directory, this port must be permitted from the Server to the LDAP database server on the LAN.
SIP Trunking		
UDP 53	Server -> DNS server	DNS. The server requires DNS for correct operation of SIP.
UDP 5060	Server <-> ICP Server <-> Internet	SIP UDP Support. If your SIP trunking provider supports SIP UDP enable this port for non-encrypted SIP signaling between MBG and the provider and between MBG and the ICP
TCP 5060	Server <-> Internet Server -<-> ICP	SIP TCP Support. If your SIP trunking provider supports SIP TCP, enable this port for non-encrypted SIP signaling between MBG and the provider and between MBG and the ICP
TCP 5061	Server <-> Internet Server -<-> ICP	SIP UDP Support. If your SIP trunking provider supports SIP TLS, enable this port for encrypted SIP signaling between MBG and the provider and between MBG and the ICP
Call Recording (Optional)		
TCP 80	Internet -> Server LAN -> Server	Certificate Management (Optional). On any server hosting clients that make use of MiSSL Tunnel with a client certificate (MiCollab Client, CIS, and so on), this port must be open to the Internet to permit the web service to submit a certificate signing request (CSR), check on the status of that request, and download the certificate. Also needed for CREs to register with SRC control interface.
TCP 6810	LAN -> Server	Call recording support (Optional). To enable a third-party call recording equipment (CRE) server to connect to the SRC control interface on MBG, this port must be enabled.
TCP 6815	Server -> ICPs	Indirect Call Recording support (Optional). To enable MBG to connect to the Indirect Call Recording connector on MiVoice Business systems which support it.

UDP 35000 to 35999	Server -> LAN	Voice Recording. For streaming voice streams from the MBG server to the CRE for recording purposes.
WebRTC Support (Optional)		
TCP 5063	Internet -> Server	WebRTC Support (Optional). To enable use of the WebRTC solution for SIP over TLS, this port must be permitted from the Internet to the server.
TCP 389	Server -> LAN	WebRTC Support (Optional). To enable WebRTC users to access the company directory, this port must be permitted from the Server to the LDAP database server on the LAN.
TCP 443	Server -> LAN	WebRTC Support (Optional). To enable access the user photos, this port must be permitted from the Server to the picture server on the LAN.
UDP 5064	Server <-> LAN	WebRTC Anonymous Mode Support with Security Profile Public (Optional). This port is required for unencrypted SIP signaling for the SIP trunk between MBG and the ICP (MiVoice Business or MiVoice 5000).
TCP 5065	Server <-> LAN	WebRTC Anonymous Mode Support with Security Profile Public and Private (Optional and only supported with MiVoice 5000). This port is required for encrypted SIP signaling for the SIP trunk between MBG and the ICP.
UDP 5066	Server <-> LAN	WebRTC Subscriber Support with Security Profile Public (Optional). This port is required for unencrypted SIP signaling between MBG and the ICP for subscriber mode support.
TCP 5066	Server <-> LAN	WebRTC Subscriber Support with Security Profile Public and Private (Optional and only supported with MiVoice 5000). This port is required for encrypted SIP signaling between MBG and the ICP for subscriber mode support.
UDP 32000 to 32500 (configurable in MBG interface)	Internet -> Server	WebRTC Voice and Video Communications. Allow incoming media on ports 32000 to 32500 from all streaming devices on the Internet to the Server. Note that the port boundary values (32000 to 32500) are configurable in MBG interface.
UDP 33000 to 33500 (configurable in MBG interface)	Server -> LAN	WebRTC Voice and Video Communications. Allow incoming media on ports 33000 to 33500 from the Server to the LAN. Note that the port boundary values (33000 to 33500) are configurable in MBG interface.

Remote Proxy (Optional)		
UDP 53 (DNS)	Server -> Corporate DNS server	DNS. The server requires DNS to look up the IP address of the internal server to proxy traffic to. See the *MBG Installation and Maintenance Guide* for details.
TCP 443 (HTTPS)	Internet -> Server Server -> LAN	Web Proxy client connections (Optional). If using the Web Proxy application, traffic must be permitted between the Internet and the proxy in the DMZ. The following applications are supported: MiCollab (MiCollab, MiCollab Client, MiCollab Unified Messaging, MiCollab Client Deployment Unit, MiCollab AWV Conferencing, Google Calendar Integration to AWV) MiVoice Business MiCollab Client MiCollab Unified Messaging Open Integration Gateway MiCloud Management Portal
TCP 443 (HTTPS)	Server -> LAN	Web Proxy client connections (Optional). If using the Web Proxy application, traffic must be permitted to and from the LAN to the proxy on the DMZ.
MiCollab Client (Optional) – See MiNET or SIP Devices for Softphone Plus		
TCP 443	Internet -> Server Server -> LAN	MiCollab Client support (Optional). To permit the MiCollab Client to connect to the MiCollab Client server for credentials, this port must be permitted.
TCP 36008	Internet -> Server Server -> LAN	MiCollab Client support (Optional). To permit the MiCollab Client to connect to the MiCollab Client server for presence information, this port must be permitted.
MiCollab AWV Conferencing		
TCP 443 (HTTPS)	Internet -> Firewall	MiCollab AWV Conferencing ConnectionPoint traffic with a dedicated second IP address (Optional). This traffic will arrive on TCP port 443 and be forwarded to the Proxy at the port configured in the Proxy interface to handle it. The Proxy then forwards this traffic to port 4443 on the LAN.
TCP <4443>	Firewall -> Server	MiCollab AWV Conferencing ConnectionPoint traffic with a dedicated second IP address (Optional). ConnectionPoint traffic from the Internet to each port configured to receive ConnectionPoint traffic in the Web Proxy must be permitted. The actual port number is defined when the administrator enables the “Listen port for MiCollab AWV (two WAN IPs)” on the Web Proxy. Port 4443 is recommended.
TCP 4443	Internet -> Server	MiCollab AWV Conferencing ConnectionPoint traffic with a dedicated TCP port and one IP address (Optional). The actual port number is defined when the administrator enables the “Listen port for MiCollab AWV (one WAN IP)” on Web Proxy. Port 4443 is recommended.

TCP 4443	Server -> LAN	MiCollab AWV Conferencing ConnectionPoint traffic (Optional). If using MiCollab AWV Conferencing through the Web Proxy, traffic to this destination port must be permitted between the proxy on the DMZ and the server on the LAN. For deployment using a dedicated TCP port and one IP address, use the port configured under the “Listen port for MiCollab AWV (one WAN IP)” on Web Proxy. Port 4443 is recommended.
MiContact Center (Optional) – See MiNET Support for Softphone Plus		
TCP 80	Internet -> Server	Certificate Management (Optional). On any server hosting clients that make use of MiSSL Tunnel with a client certificate (MiCollab Client, CIS, and so on), this port must be open to the Internet to permit the web service to submit a certificate signing request (CSR), check on the status of that request, and download the certificate. Also needed for CREs to register with SRC control interface.
TCP 36000	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 36003	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 5025	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36001	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 443	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36002	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 5024	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36004	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 5026	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.

TCP 35001	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 5030	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35002	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 7001	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35003	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 7003	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35004	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 8083	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35005	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 8084	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35006	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.
TCP 42440	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35007	Internet -> Server	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the Internet to the server.

TCP 1433	Server -> LAN	MiContact Center Support (Optional). To enable use of the MiContact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.

Glossary

APC	Application Processor Card
ATM	Asynchronous Transport Mode. A switching protocol that uses asynchronous time-division multiplexing (TDM) to put data into fixed-size cells. It is suitable for carrying real-time payloads such as voice and video.
CCS	Centrum Call Seconds. A unit of measurement used in traffic and queuing theory calculations that is equal to 100 seconds of conversation. One hour of telephone traffic on one line is equal to 36 CCS, which is equal to one erlang (a more common measurement).
CPH	Calls Per Hour
CRE	Call Recording Equipment
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol (RFC 1541)
DMZ	De-Militarized Zone. A portion of a network which is behind a firewall but has elements that are exposed to the Internet.
DSL	Digital Subscriber Line
Erlang	A unit of traffic density in a telecommunications system. One erlang is the equivalent of one call (including call attempts and holding time) in a specific channel for 3600 seconds in an hour. It is equal to one hour of conversation, or 36 CCS.
G.711	ITU-T codec audio standard, specifying an audio signal with a 3.4 KHz bandwidth (ordinary analog voice signal) over an A-law and μ-law digitized, linear PCM at 64Kbps. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.
G.729	This ITU-T standard describes CELP compression where voice is coded into 8-Kbps streams. The two variations of this standard (G.729A and G.729A Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-Kbps ADPCM.
ICP	IP Communications Platform
IETF	Internet Engineering Task Force. The official specification documents of the Internet Protocol suite are defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG). These specifications are recorded and published as standards track RFCs. (See RFC).
IP	Internet Protocol (RFC 1122 Section 3.)
IPSec	Internet Protocol Security

ISP	Internet Service Provider
MBG	MiVoice Border Gateway
MCA	Mitel Collaboration Advanced; now named MiCollab Audio, Web and Video Conferencing
MiNet	Mitel Network Layer Protocol. A signaling protocol used to transport messages between the PBX and all Mitel IP phones. MiNet is encapsulated in TCP.
MSL	Mitel Standard Linux. The standard Linux distribution used and maintained by Mitel as a platform for all applications
NAT	Network Address Translation. A technique for translating one set of IP addresses, often private, to another set, often public (RFC 1631)
PPP	Point-to-Point Protocol
PPPoA	Point to Point Protocol over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RFC	Request For Comments. A standards document for the public Internet. RFCs are produced by the IETF and its working groups, as well as other bodies, to define and ratify new Internet standards and changes to existing standards. RFCs must first be published as Internet Drafts.
RTP	Real-time Protocol (RFC 1889)
SIP	Session Initiation Protocol (RFC 3261 et al.)
SRC	Secure Recording Connector
SRS	SIP Recording Server
SRTP	Secure Real Time Protocol (RFC 3711)
SSL	Secure Socket Layer
TCP	Transmission Control Protocol (RFC 1122)
TDM	Time-Division Multiplexing. A system of carrying multiple signals on one carrier by dividing the multiple inputs into fixed-length (time) samples, and placing them one after the other onto the carrier medium.
TFTP	Trivial File Transfer Protocol (RFC 783). A simple file transfer protocol (no password protection or user directory services) that uses UDP to transfer files across a network
UDP	User Datagram Protocol (RFC 1122)
VoIP	Voice over IP
VPN	Virtual Private Network
WP	Web Proxy

Mitel
Powering connections

mitel.com