A MITEL
TECHNICAL PAPER

Security and the Mitel Teleworker

Date: July 2024

Notices

Trademarks

Contents

Introduction

The MiVoice Border Gateway teleworker solution is designed to take advantage of Mitel's security and reliability. The MiVoice Border Gateway (MBG) teleworker application enables remote workers to connect securely and conveniently to the corporate voice and data network without the use of a Virtual Private Network (VPN) across the Internet (or other network that requires Network Address Translation – NAT) to a Mitel IP PBX call control. This document provides an overview of the solution architecture and describes the protocols used to ensure the confidentiality of voice and data communications.

Solution Architecture

The solution consists of two elements. The first is the MiVoice Border Gateway (MBG) application (or "software blade") that is downloaded to the application server from the Mitel Software Download Center. Once the MBG software is installed and configured, the application allows the MBG to function as a proxy for remote phones requiring access to the corporate voice network. The solution offers several features that are designed both to improve voice quality over the Internet and to reduce bandwidth requirements between the corporate office and remote locations. The second element of the solution is the remote IP phone. All current Mitel IP phones are supported by the Teleworker Solution, including the Mitel 6900 and 6900w series, as well as Mitel Softphones and the MiVoice Business console. In addition, 3rd party SIP phones and softphones that have been tested successfully and certified for interoperation are also supported.

The MBG can be deployed on virtualized infrastructure (e.g. Nutanix, VMware) or physical servers as well as in cloud services such as those provided by Azure and AWS.

The following subsections describe the main supported deployment options.

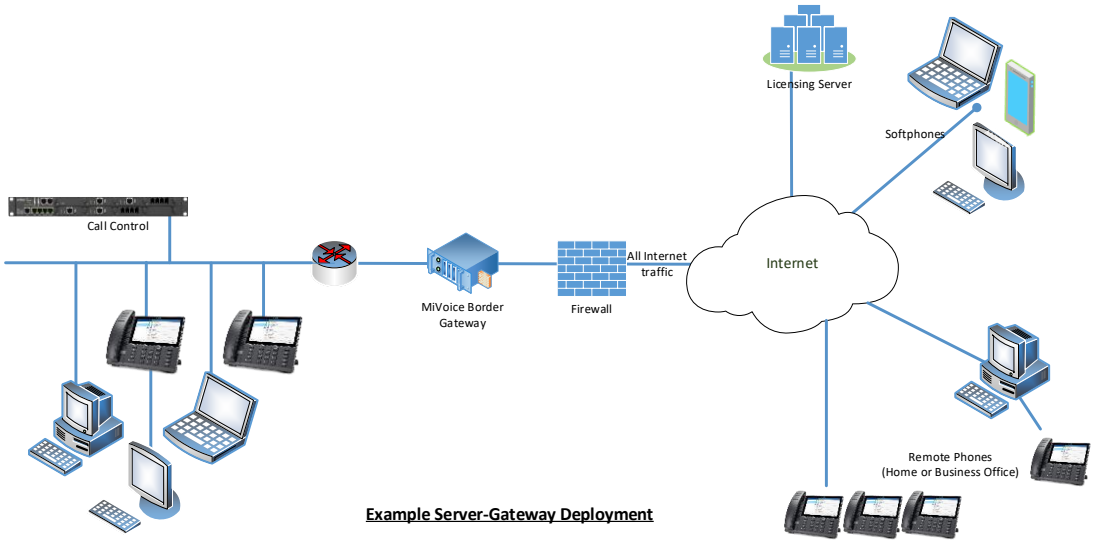
Server-Gateway Configuration Behind the Customer Firewall

In this configuration, the MBG functions as an Internet gateway with two Ethernet interfaces.
One interface is connected to the customer's Internet Firewall while the other is connected to the internal Local Area Network (LAN). Typically, this internal connection is isolated to Voice VLAN traffic only. Data traffic initiated inside the network is allowed while data traffic initiated outside the network is denied.

The external (WAN) IP address of the MBG server must be:

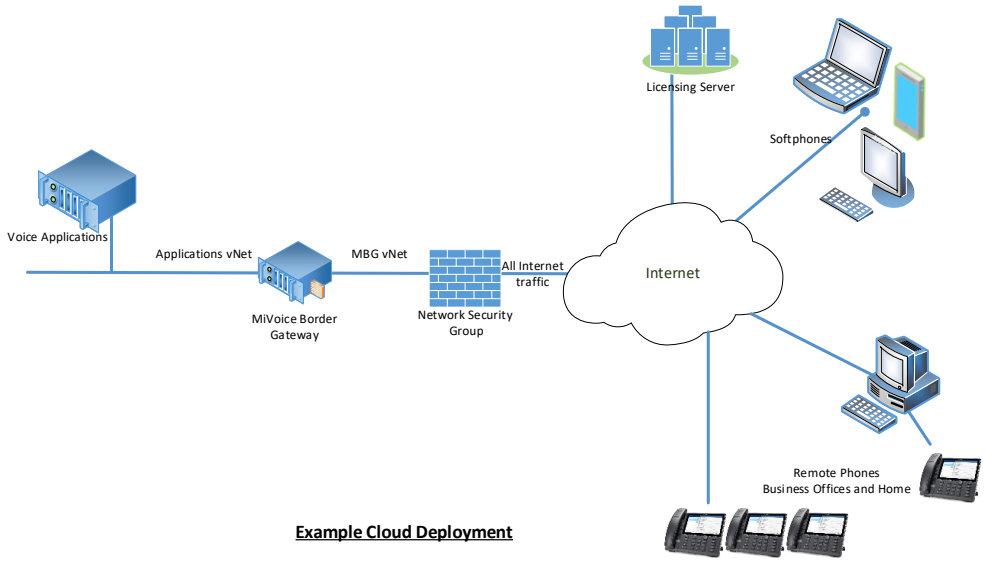
- dedicated to the MBG Solution
- reachable from the Internet via the customer's properly configured Firewall and the internal network (typically the voice VLAN)

In the server-gateway configuration the MBG server is the gateway to the Internet for MBG traffic via the customer's firewall. That is the MBG is configured to function as the voice firewall and gateway behind the corporate firewall. This configuration is a typical scenario in a small business setting and allows the customer to take advantage of the MBG capabilities.



Example Server-Gateway Deployment

Server-Gateway mode is also used with cloud deployments, such as AWS and Azure, where the MBG is situated behind the cloud providers Internet facing firewall (e.g. Azure Network Security Group) with one interface in the Applications vNet and the other in the MBG vNet.



Example Cloud Deployment

Server-only Configuration in Network DMZ

This option is intended for situations where there is an existing corporate De-Militarized Zone (DMZ), and the customer wants the MBG to be installed in the DMZ of the corporate firewall as illustrated.

The MBG acts only as a server and is protected from Internet exposure by the existing firewall.

On the MBG the network interface is configured with an IP address that is:

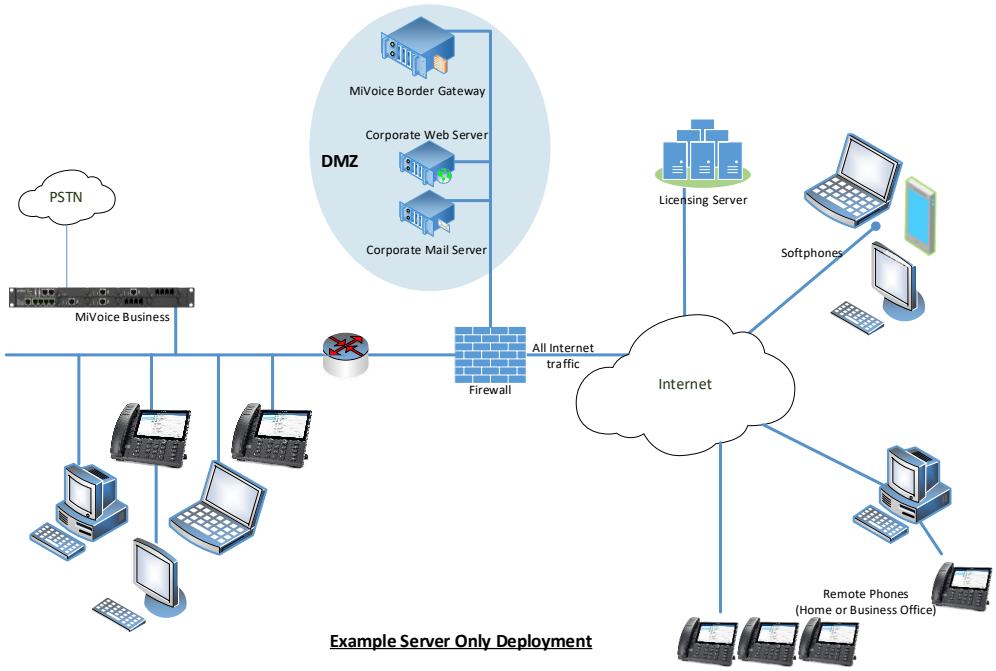
- dedicated to the MBG solution.
- private (allocated from the firewall's DMZ network range)
- reachable from the internal network

On the enterprise firewall, configure the WAN interface with an IP address that is:

- dedicated to the MBG Solution
- publicly routable via the firewall
- reachable from the Internet and the internal network.

When configuration is complete, the solution will use the public, post-NAT address of the MBG server for both the IP phone side and the Call Control (e.g. MiVoice Business, MX-ONE etc.) streaming addresses of the MBG.

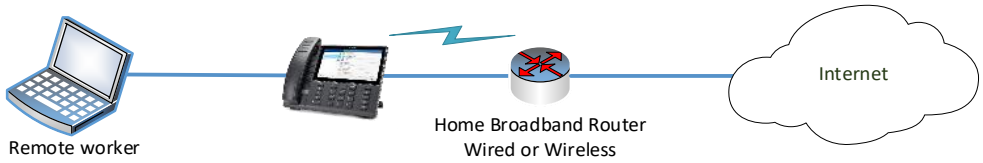
In a DMZ configuration, the firewall is the gateway for all traffic and has three interfaces (WAN, LAN, and DMZ).



Example Server Only Deployment

Remote User

The recommended configuration at the remote location is to connect the Mitel IP Phone to a standard broadband Internet router, providing Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP). Mitel provides an option for wireless connectivity via either a wireless adapter or with the current range of Mitel 6900(w) sets that have native wireless connectivity.



Example Remote Worker

Note: The IP desk phone requires power, which can be accomplished via a Power Injection Powerpack or an Ethernet switch or router capable of providing Power over Ethernet (PoE).

For a remote location which does not have any unused Ethernet ports, the IP phone can be connected to the router and the user's computer can be connected to the second Ethernet port on the back of the phone (if enabled) which provides pass-through communications to the Internet for the connected computer.

Connecting a PC to the second Ethernet port on the back of a Mitel IP desk phone does not provide the PC with a VPN connection to the office network. That connection must still be made using the organization's supported VPN client software. This ensures that security of the corporate network is maintained when using MBG as the Mitel Teleworker solution only provides a secure voice connection and not a data VPN (i.e. the PC cannot "ride" the phone's connection into the corporate network).

For PC's connected in this manner, the phone does not interfere with the data stream. The phone does, however, provide prioritization of the voice packets over data coming from the PC, ensuring better voice quality with minimal or no impact to the data connection.

Installation

Installation of the Teleworker Solution is simple and is typically accomplished in less than 30 minutes. The technician begins by loading the MBG application software, which includes the Linux operating system, onto a standard Intel-compatible computer or a virtual machine (OVA file is also available) onsite or in a data center. The installation is automatic and requires no Linux knowledge.

Once the operating system is installed the technician accesses the server's secure web-based management interface (the "server manager"), enters the application record ID number, which is provided as part of the ordering process, and downloads the Teleworker Solution application, which is then configured.

Mitel IP Phones

The configuration steps for placing a Mitel IP desk phone in Teleworker mode vary depending on the set type and call control being used.

6900 and 6900w IP Phones with MiVoice Business

To manually configure a 6900 or 6900w series IP phone press the settings key on the phone to view the services and static settings that allow the configuration of the phone. With the 6915, 6920(w), 6930(w) and 6940(w) IP Phones, select Voice Services followed by MiVoice Border Gateway. Or with the 6905, 6910 IP Phones, select User Settings first, followed by Voice Services and then MiVoice Border Gateway. Then enter the IP Address of MBG and press Save.

While brief steps of two examples with the MiVoice Business call control are provided below the document "MiVoice Border Gateway - Remote Phone Guide" should be consulted for the latest information.

In all scenarios the MBG administrator must authorize the specific phone to be allowed to connect to the MBG server. This authorization process is defined in more detail later in this document.

When powered up, the phone will first obtain a local IP address from the local DHCP server on the remote network (e.g. from the home broadband router) and, once configured, the phone will then automatically download its software from the MBG, previously programmed. The software load is stored in an encrypted form on the MBG server. The software is downloaded to the phone where it is decrypted, and an integrity check is performed to verify that it was not modified in transit. When the download completes the phone again connects to the MBG and the server in turn connects to the MiVoice Call Control (e.g. MiVoice Business) address, that was entered by the technician previously in the MBG administration interface. Under normal circumstances, this entire process is automatic and requires no special configuration at the remote location, within 2 minutes, dial tone is achieved.

Legacy 5300 IP Phones with MiVoice Business

To configure the 5300 IP phone power up the phone, holds down the “7” key for about 4 seconds and, when prompted to “Configure Teleworker” enters the Internet routable IP address of the MBG. This information is stored by the phone in NVRAM (Non-Volatile Random-Access Memory).

Voice Encryption

To ensure the confidentiality of communications all voice packets passed between the remote Mitel IP phone and the MBG are encrypted using the Secure Real-time Transport Protocol (SRTP) with 128-bit Advanced Encryption Standard (AES) cipher or better. SRTP adds confidentiality, message authentication and replay protection to all voice calls. Specifically, Secure RTP defines a set of default cryptographic transforms and allows new transforms to be introduced in the future.

The security benefits of SRTP include:

- Confidentiality of the voice media payloads as well as protection against replayed packets
- Low bandwidth cost, i.e., a framework preserving RTP header compression efficiency, and limited packet expansion.
- Low computational cost
- High tolerance to packet loss and re-ordering, and robustness to transmission bit errors in the encrypted payload

SRTP is ideal for protecting VoIP (Voice Over Internet Protocol) traffic because it can be used in conjunction with header compression and has no effect on IP Quality of Service (QoS). These attributes provide significant advantages, especially for voice traffic using low bit rate voice codecs such as G.729. To further enhance QoS and facilitate traffic management the MBG can be configured to insert Differentiated Services Code Points (DSCPs) in the IP headers of voice and signaling packets.

IP Phone Signaling Encryption

To protect the confidentiality and integrity of the IP Phone signaling, the signaling connection between the remote IP phone and the MBG server is fully encrypted using industry standard Transport Layer Security (TLS) encryption. The MBG can be configured to use specific TLS cipher suites to negotiate security settings and encrypt information for network connections including forcing TLS 1.2 or better.

Mitel MiNet IP Phone Authorization

In addition to protecting the confidentiality of the voice stream and the signaling, the Teleworker Solution is designed to prevent unauthorized remote phone users from gaining access to corporate voice resources. With MiVoice Business and MBG Teleworker sets this is accomplished by restricting access to specified IP Phones based on a unique identifier sent by the phone to the Teleworker Solution server in an encrypted control message. That unique identifier includes the MAC (Media Access Control) address of the phone. The first time an IP Phone attempts to send a registration message to the MBG, its MAC address is automatically logged and entered into a table that is displayed on the solution’s administration interface. It is important to note here that this MAC address is sent between the remote IP phone and the teleworker server over the encrypted signaling call control connection.

By default, the phone is disabled and therefore will not be able to connect to the MiVoice Business. To allow access, the MBG administrator must still set the phone’s entry to be enabled. It is also possible to enable specific phones by manually adding their MAC addresses to the table. Each phone’s MAC address is printed on a label on the back of the set. If many phones need to be installed, the administrator can enter an Installer Password in the configuration panel of the MBG. If such a password is set, the phone will prompt for it upon its initial connection to the MBG. The installer then enters the password using the phone keypad and the MBG then enables that phone’s MAC address for future connections. For convenience, the table also allows a description to be entered for each phone. If the entry is added

through the automatic registration process, the default description is the IP address of the phone. For bulk provisioning, the MBG administrator may also import from .CSV file.

SIP IP Phone Authorization

The MBG solution is designed to prevent unauthorized remote phone users from gaining access to corporate voice resources. This is accomplished with SIP phones by using unique usernames and complex password combinations. Two levels can be set up when being used in combination with the Mitel call control so that there is a unique username/password combination between the SIP phone and the MBG and a second unique combination between the MBG and the MiVoice Business system. Similar to MiNet IP phones the MBG administrator may also import from .CSV file for bulk provisioning.

Mitel publishes a document of successfully interoperability tested SIP devices on a regular basis as part of the “Mitel Third-Party Interoperability Reference Guide (IRG) for Mitel Products” document available via your Mitel Account Team or Channel Partner.

Check the vendor’s SIP device User Guide for instructions about configuring the SIP Registrar and/or SIP Proxy information for the SIP phone. Enter the following information:

- **Username**: Enter your username value provided by the MBG administrator.
- **Password**: Enter your password provided by the MBG administrator.
- **SIP Registrar** (or “Domain”): Enter the IP address or FQDN of the MBG server.
- **SIP Proxy** (if applicable): Enter the IP address or FQDN of the MBG server.

Web Real-Time Communication (WebRTC) _

WebRTC is an API definition that provides browsers and mobile applications with Real-Time Communications capabilities. The MBG provides WebRTC gateway functionality for browser-based voice and video calling, using HTTPS and DTLS-SRTP, without the need of plugins.

Two usage scenarios are available:

- An external user initiates a call to the enterprise by clicking a button on a web site and then providing minimal credentials (e.g. name and CAPTCHA phrase). The user is directed to an internal service such as a sales or product support hotline.
- An external user logs in to MBG from their browser and then registers with the call control. The user can then make and receive calls and access their voicemail.

Web Proxy Services

In addition to providing Teleworker services for communication endpoints, a Web Proxy Service is also included in the MBG, specifically for providing secure communications between Mitel Unified Communications Applications on the LAN and remote clients connecting via the Internet. The applications include:

- MiCollab Client for, Desktop, Web and Mobile
- MiCollab Unified Messaging (NuPoint)
- MiCollab Advanced Messaging Web Client
- MiContact Center Business
- Open Interface Gateway (OIG)
- Mitel Interaction Recorder (MIR)

An Internet published DNS entry is required in order for the remote clients to connect via the Web Proxy (e.g. MiCollab1@example.com).

For an application such as MiCollab to connect to the internal MiCollab Server, the following will occur:

- MiCollab client requests DNS resolution for MiCollab1@example.com
- The DNS server the PC/smartphone Phone is utilizing for its Internet connection will return the IP address of the Mitel.com corporate firewall.
- MiCollab Client connects to the corporate firewall.
- The corporate firewall routes the http request to the MBG Web Proxy.
- The Web Proxy requests resolution for MiCollab1.mitel.com from the customers Internal DNS server.
- The internal DNS server provides the IP address of the MiCollab1 server.
- The Web Proxy completes the connection to the MiCollab1 server.

The Web Proxy proxies the request to the MiCollab server along with the full URL requested by the client.

IP Blocking (Allow/Block IP Ranges)

The MBG IP Blocking feature monitors network activities in real-time and blocks or allows connections between the MBG and specific network blocks of IP addresses (netblocks) in Classless Inter-Domain Routing (CIDR) format further securing the MBG and Mitel solution.

CIDR lists are available on the Internet that contain netblocks for entire countries. These can be downloaded and modified for local requirements. CIDR lists can also be created from scratch. A list can be used to either block connections or allow connections). Use a text editor to create CIDR lists according to the following format:

```
# Block List Title

4.17.135.32/27 # Comment

4.17.143.0/28
```

Administration

Administration Access with the MBG is secured through encryption using HTTPS and is limited to only specified configured source hosts/networks during implementation. A secure, non-trivial password must be used for new installations. After the password is entered and confirmed the underlying operating system examines the password for strength. If it is found to be weak the user is notified and provided with the chance to change it.

Access to the web management (Server Manager) login is protected from brute force password attacks. By default, six consecutive failed login attempts within a 10-minute period locks out the IP address of the client for 30 minutes.

The MBG also provides support access to Secure Shell (SSH) for debugging purposes. SSH is disabled by default, but if required can be enabled temporarily. This temporary access can also be restricted to specific networks and/ hosts who are then able access the server via SSHv2. Once enabled SSH provides a secure, encrypted way to log in to the MSL server from a remote location. Typically, SSH access should only be used under instruction from Mitel technical support and should be disabled otherwise.

Summary

With the Mitel Teleworker solution, a user can take their Mitel communications device and applications virtually anywhere be it using their preferred communications device be it an IP desk phone, a softphone on their laptop, or mobile device.

The Mitel Teleworker solution provides a simple way to securely deploy remote teleworkers wherever an IP address and bandwidth can be found. The solution uses industry-standard protocols such as Secure RTP and TLS to ensure the confidentiality and integrity of all voice and signaling communication. Users can continue working away from the office without sacrificing in-office functionality or security. Enabling an in-office communications experience without being physically in the office.