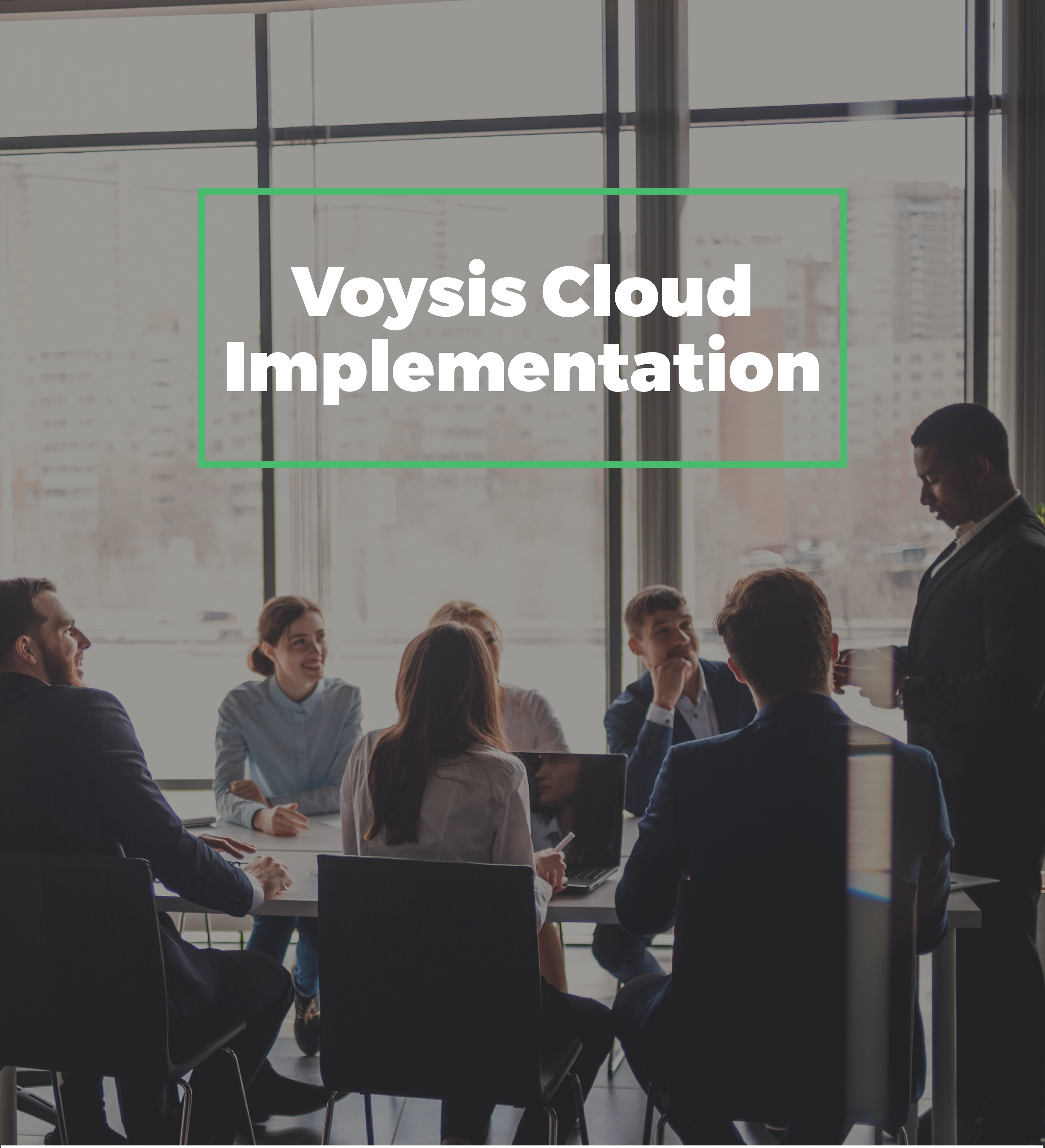


Voysis Cloud Implementation

VOYSIS
IP SOLUTIONS

Modernizing your Company's Services through VoysisCloud

On premise PBX systems, although come with a bevy of different features, are also limited when it comes to integrating other features and capabilities to meet the needs of current evolving technological advancements. This seems to be the driving force for many businesses wanting to migrate to the cloud.

Cloud telephony offers a cost-effective way to help improve your company's performance that reduces in-house infrastructure costs by allowing users to integrate and enhance their capabilities all while fostering productivity. Voysis IP Solutions can help you modernize your company's services through their VoysisCloud solution.

Voysis Features and Benefits

- VoysisCloud telephony systems connect to a secure data center dedicated to your company's own infrastructure.
- No need for on premise material or full-time staff.
- You will save on costs and increase your company's flexibility and productivity through technical modernization.
- You can configure your company's infrastructure easily and quickly and improve continuity of operations.

Migrating to the Mitel Cloud

In order to prepare for a successful VoIP cloud migration and to ensure that your network delivers optimal performance to your clients for cloud voice services, Voysis IP Solutions have prepared a simple yet effective best practices summary that you can follow.

Best Practices Summary

- Set priority to/from the MiVoice Border Gateway (MBG) and the Phones in the Router/firewall as QOS 6 (Voice) or DSCP value of 46 decimal, 0x2E hex
- Have the Firewall Voice rules as high in the processing list to reduce delay
- Set Firewall rules to Allow Any/Any to/from the MBG IP addresses and LAN for quick setup or troubleshooting.
- Disable any "SIP helpers" in Firewalls
- Disable UDP Flood Protection for Voice rules in Firewalls
- Have a single static Public IP to NAT. Changes to the IP address will cause the phones to reboot
- Disable CDP on Cisco switches
  MiVoice Border Gateway (MBG) IP Addresses (Provided by Voysis)

Remote Site Requirements

Router

A set in a remote site (such as a home or branch office) is assumed 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 Wi-Fi.

(Refer to the device's documentation for configuration details.) All devices expect a TCP/IP network regardless of the link-layer technology.

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 using a cable modem and must be configured with the user name and password provided by the ISP.

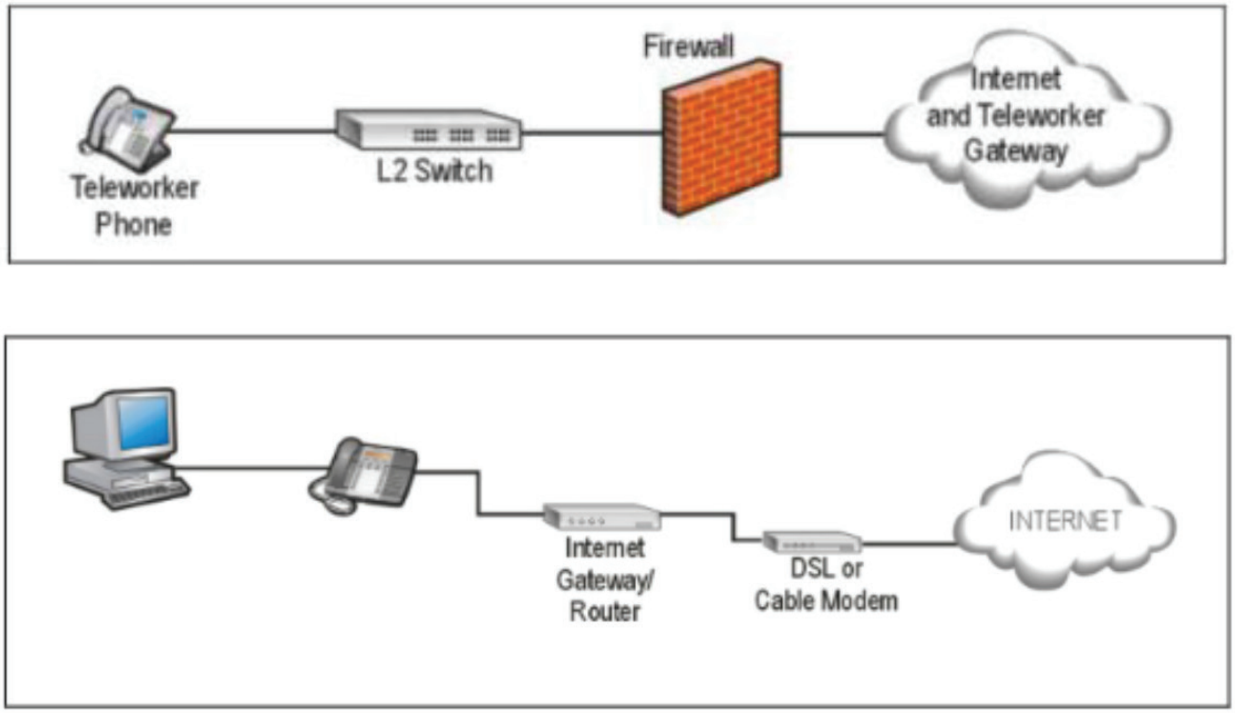
If you are using Wi-Fi sets, the router or a separate Wi-Fi access point must also provide 802.11 b/g/n.

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.

Configuring the Remote Site Firewall

If the remote office has a firewall, it configure it 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.



Example of a remote Site

Rules for sites with more restrictive security policies:

- 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 ports 36005, 36006, 36007, 36008 and 37000 on the MiVoice Border Gateway IP address, if using Release 5.0 or 5.1.
- 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 preferred for SIP devices.

- Allow incoming and outgoing TCP to port 5061 on the MiVoice Border Gateway IP address, if encrypted

- SIP support is preferred for MiCollab Client devices. MiVoice Border Gateway (MBG) IP Addresses (Provided by Voysis)

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. Disable the feature with older sets or if set connections to the MBG server cannot be maintained. With newer sets that randomize the source port used for each new connection, this should not be a problem.

SIP-Aware Firewalls

Many firewall devices today understand the SIP protocol and include some type of NAT traversal or rewriting of SIP packets. When using MBG 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 UDP flooding protection in firewalls in the voice path be disabled.

About Us

Incorporated in 2003, Voysis IP Solutions is a Mitel authorized reseller. Voysis IP Solutions supports the entire Mitel product portfolio and with our engineers, we create great solutions based on our customers' needs. Voysis IP Solutions supports both hosted and enterprise solutions.

We recognize that the value of a communications solution is different for every business. Our portfolio of solutions are highly scalable, secure, easily managed, and optimized to meet the evolving communications needs of our customers.

voysis.ca | **1-877.2voysis**