Prime Call Cloud MeetMe 2.0

Firewall Traversal White Paper

This document describes the Prime Call Cloud MeetMe 2.0 firewall traversal solution. Outlined are the reasons for putting video systems behind a corporate firewall and the firewall configuration requirements for MeetMe 2.0.

Firewall Traversal

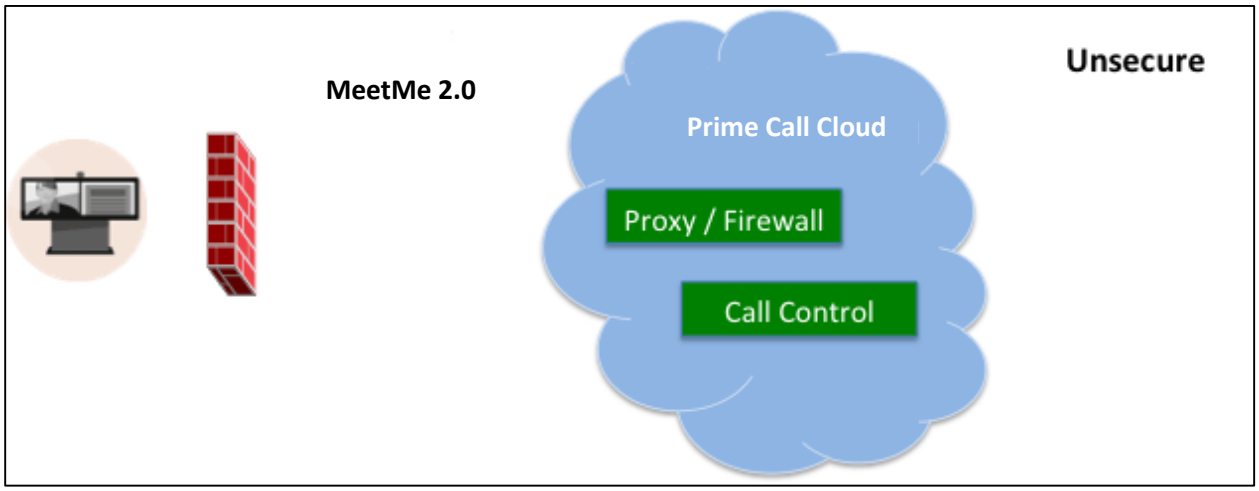
Putting video systems outside a corporate firewall introduces a range of security threats, including individuals potentially eavesdropping on highly sensitive conversations. Systems on public IP addresses also are vulnerable to denial-of-service (DoS) attacks.

With Prime Call Cloud, there is no need for endpoints to connect over the public Internet. Prime Call Cloud registered hard endpoints and soft clients instead are connected within the customer's private network and behind the resident firewall. The Prime Call Cloud firewall traversal solution provides direct video conference calling without compromising security.

Hard endpoints and soft clients registered to Prime Call Cloud automatically connect through firewalls to dedicated datacenters for a secure connection between endpoints and the cloud-based service. We ensure the privacy of video and audio calls with the default enablement of encrypted signaling using SIP TLS and encrypted media using Secure Real-Time Transport Protocol (SRTP).

The service filters and protects against incoming DoS attacks. With traffic monitoring, pattern recognition, and filtering, the MeetMe 2.0 Call Control Service also is designed to identify suspect traffic patterns, fraud attempts, and violations of service and breaches of policy.

Prime Call Cloud MeetMe 2.0 firewall traversal solution overview



Firewalls generally block unsolicited incoming requests so that calls originating from outside a network are prevented. Firewalls can be configured to allow outgoing requests and incoming responses from trusted destinations; this is how Prime Call Cloud makes the traversal of any firewall secure. The solution also keeps network security infrastructure intact so that business operations are not compromised when adding IP video capabilities.

The customer only needs to open a limited number of outgoing connections to a reduced set of specific IP addresses (see details at the end of this document). The Prime Call Cloud firewall traversal solution never allows inbound connections through the customer's firewall, and the client/server architecture makes outbound connections just like other traffic on the company network.

Firewall Configuration

Only a limited number of ports and destination addresses need to be configured in the firewall to be able to securely connect to Prime Call Cloud.

(Note: It is only required to open outgoing ports.)

IP whitelisting ensures that customers' systems are communicating with Prime Call Cloud and prevents traffic intended for the service from being hijacked or rerouted to a rogue website.

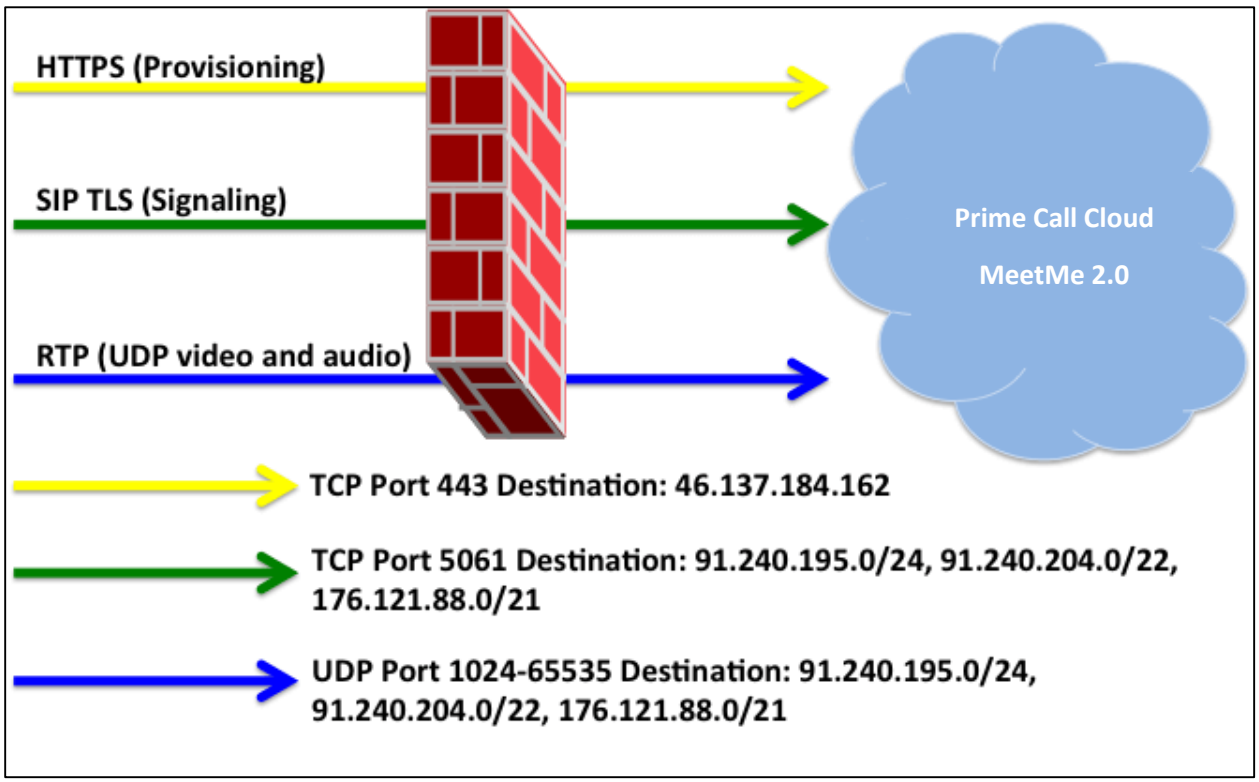
IP whitelisting can occur at several points on a customers' network, the most common of which is the firewall. When creating or updating an IP whitelist, IP restrictions on the firewall have to match our best practices described in this document.

The Prime Call Cloud firewall traversal solution is designed to work with standard firewalls. The following Network Address Translation (NAT) modes are supported:

- Symmetric NAT
- Full cone NAT
- Restricted cone NAT
- Port restricted cone NAT

The following diagram illustrates the recommended firewall configuration to take advantage of the Prime Call Cloud firewall traversal solution and redundant data centers located in Europe, North America, Middle East, Asia, and Australia.

Recommended firewall configuration for Prime Call Cloud MeetMe 2.0

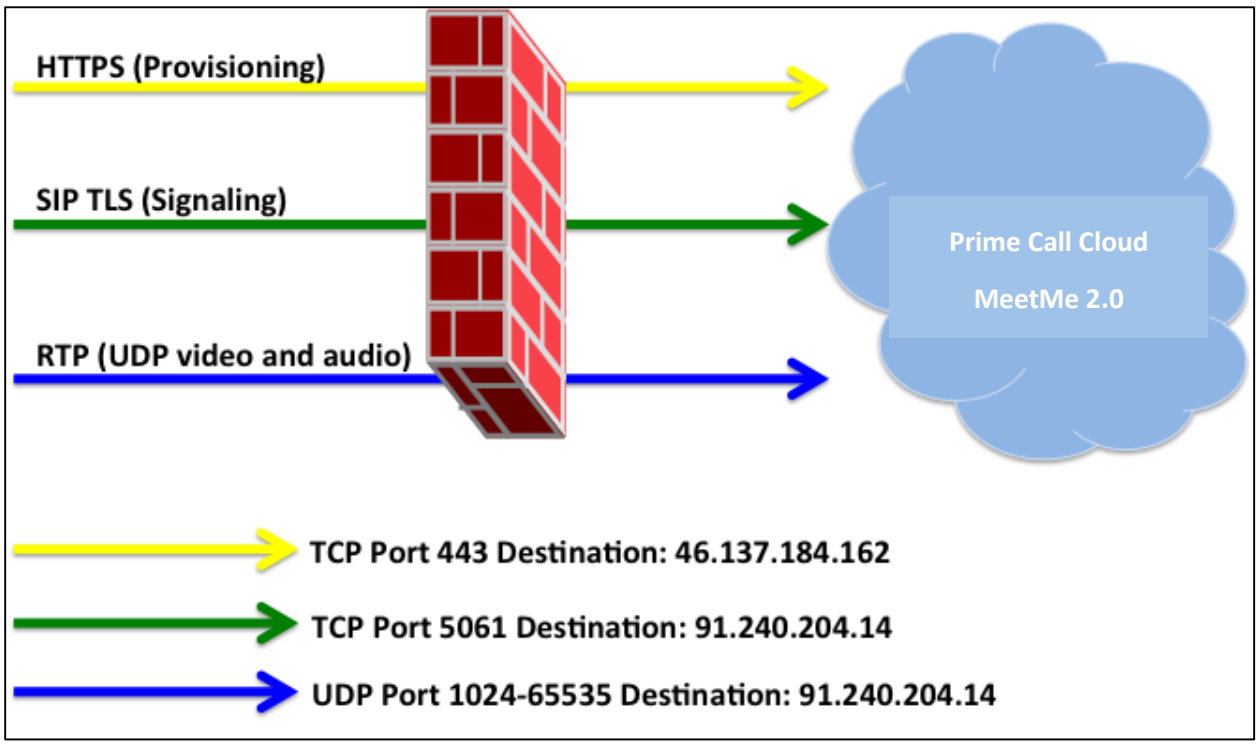


We recommends that the entire set of IP ranges is whitelisted to prevent accidental service interruptions. Doing this ensures that maintenance work or service disruptions do not cause unintentional downtime while using the service.

If the customer's security policy requires an even more limited setup, there also is a scaled-down configuration in which the customer only opens connections towards one dedicated data center and, in effect, connects to just one IP address. This configuration does not include a redundant solution with automatic failover if the data center you are connected to goes out of service.

Contact the support team before setting up this kind configuration (illustrated in the following diagram).

Scaled-down firewall configuration for Prime Call Cloud MeetMe 2.0



More Information

For more information, contact your Solutionz sales representative or use the MeetMe 2.0 video network assessment test application at *https://my.pcmm.vc/test*.