MindLink

Product Overview

XMPP FEDERATION GATEWAY

Overview

This document describes the MindLink XMPP Federation Gateway for Skype for Business and Microsoft Teams.

The presumed audience is MindLink technology partners, and MindLink/Skype for Business/Teams customers.

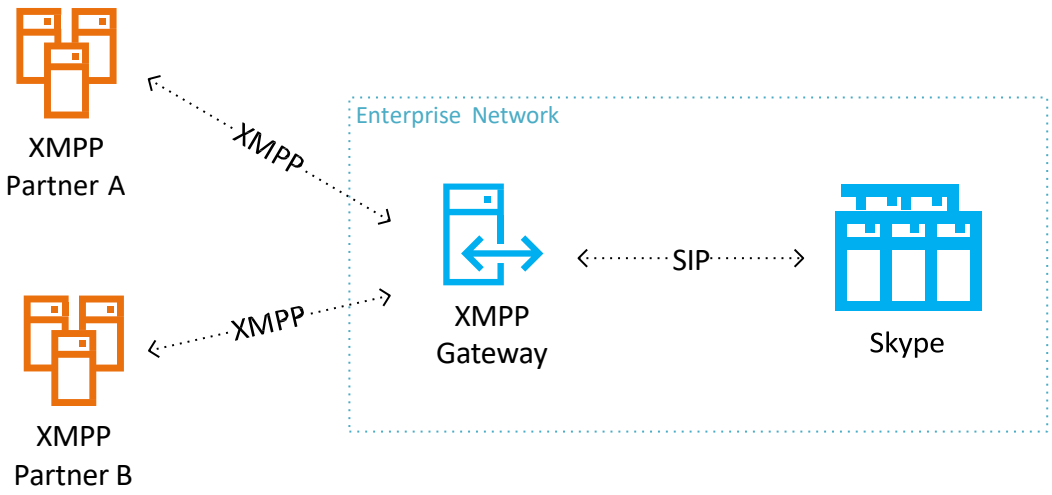
We describe the motivation behind the product and the technical architecture.

Background

Microsoft Skype for Business has historically offered an in-built XMPP gateway server component, such that users on XMPP-based chat systems can interact with Skype for Business users as externally federated contacts. This component is deployed, managed, and configured as part of the integrated Skype for Business on-premise topology.

The component effectively exposes the Skype for Business system as an externally-visible XMPP domain. Bi-directional server-server XMPP connectivity is achieved with a single remote federated XMPP server. This communication is over XMPP, according to the core XMPP specification.

External XMPP systems hence see and treat the Skype for Business system as a peer XMPP server. The translation to a SIP protocol behind the scenes for internal communication is opaque to external federated XMPP domains.



XMPP

Use of third-party XMPP chat systems is widespread across many sectors, in particular the Defense and Intelligence industries. The XMPP protocol is intrinsically suitable for use across low-bandwidth and constrained networks, such as in forward-deployed tactical scenarios.

XMPP systems are often in use as self-contained server clusters in disjoint remote networks such as ships or on the battlefield. These individual nodes communicate as a federated network with each other, and a centralized chat system in an enterprise datacenter – typically Skype for Business Server.

The open and standardised nature of the XMPP protocol also lends itself for use as a mutual interface between co-operating partner organisations, and as an interface into public chat services.

Skype for Business 2019

The component is deprecated by Microsoft in Skype for Business 2019.

Skype for Business customers require a supported and future-proofed alternative, with an active development roadmap and improved modern featureset.

Teams

There is no equivalent capability available for Microsoft Teams.

Teams users would currently need to use a third-party client/server to communicate with XMPP users. This is an awkward and disjoint end-user experience, and ultimately detracts from an organisation's investment in a unified cloud infrastructure.

Federation is intrinsically a two-party relationship. Customers that wish to use Teams cannot also coordinate that their federated partners also move to Teams in the same window – or indeed, at all. Interop with legacy external protocols is therefore important for business continuity during and after Teams migration.

Many customers are currently using XMPP systems and Skype for Business Server for specialised use cases. A clear, seamless and supported roadmap to Teams is a key challenge for migration of such environments.

Product Featureset

The MindLink XMPP Federation Gateway is a backend middle-tier server component that bridges bi-directionally between XMPP and Microsoft platforms.

Capabilities

The gateway is designed to support a full featureset capability for IM and Presence modalities:

- 1-2-1 IM and Presence (Implemented)
- 2-way federation (Implemented)
- Contact cards (Implemented)
- Contact list subscription notifications (Partial Implementation circa 2023)

Further roadmapped capabilities include multi-party IM and federated persistent chat rooms.

End User Experience

The end user experience for both Skype/Teams users and XMPP users is transparent – users see remote users in partner domains as standard federated users.

Both Skype/Teams and XMPP users are addressed using a <user>@<domain.com> format user name, these user names are mapped directly between SIP/XMPP identities bi-directionally across the gateway.

Technical Architecture

The gateway architecture is similar to the Skype for Business 2015 XMPP gateway component.

Terminology

The gateway is agnostic to the platforms it federates with. Each adapter communicates with the respective remote server to publish and read events from the broker. Each adapter is not aware of the other adapters that are being federated.

The gateway will communicate with an XMPP server in a single, remote, federated domain. These are deployed and managed by the external partners.

Chat system protocols typically involve flow of many aspects of communication information:

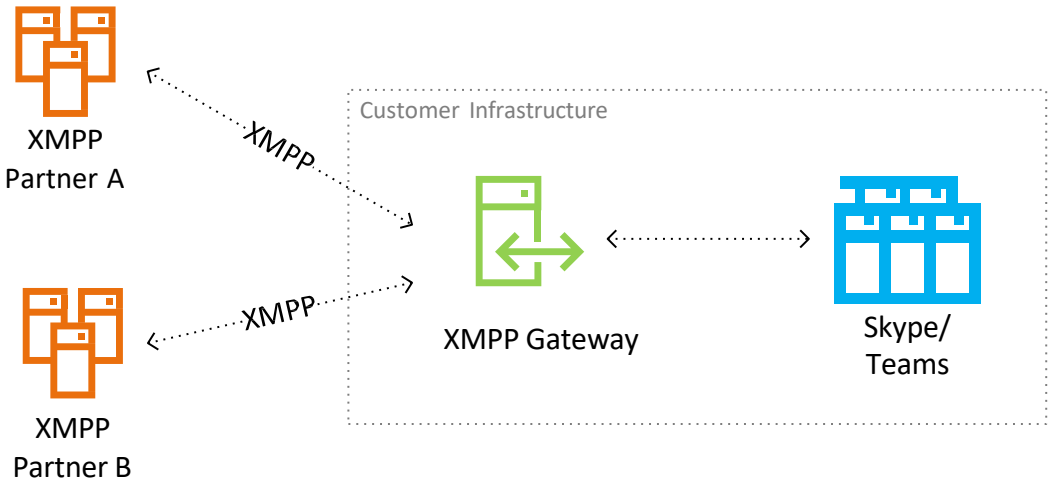
- Conversation state and signalling
- Conversation metadata
- Instant messages
- Presence subscription state and signalling
- Presence updates
- User directory queries

We refer to all of these different types of communication data at a generic protocol level as "message packets".

Server

The gateway is deployed as a standalone server component. Conceptually, the gateway is part of the Skype/Teams customer's infrastructure.

The server is a .NET Windows Service, installable on virtualizable Windows hardware. The compute hardware can be located in a private datacentre or public or private cloud.

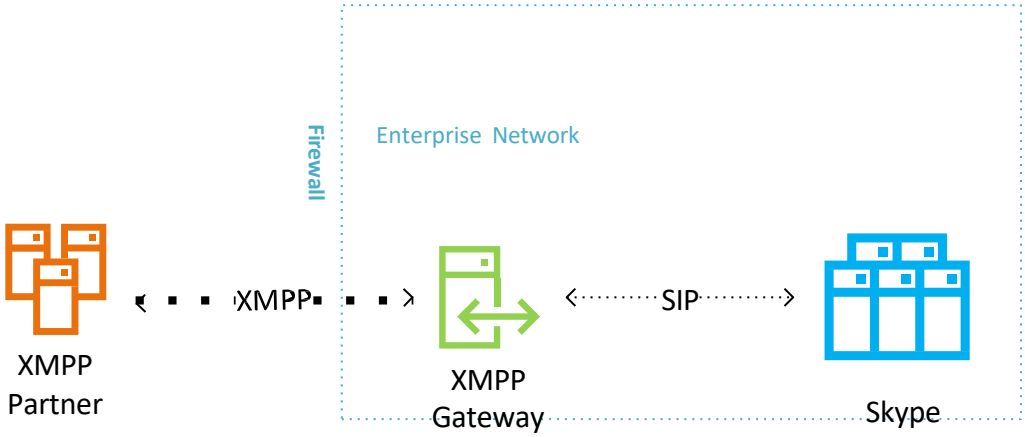


The server is intrinsically stateless – it will broker messages and transactions between protocols on either side, but not maintain or provide any specific application state or logic itself. However, a database is required for maintaining subscriptions across service restarts, this is not a hard requirement for deployment, but supports an improved user experience. Any in-flight transactions are short-lived, and automatic retry/resumption is afforded at the protocol layers in the case of node failure.

Physically, placement of the gateway differs for on-premise Skype domains vs Hybrid or Teams domains.

Skype for Business On-Premise

The server is deployed as part of the internal Skype for Business topology as a trusted application.

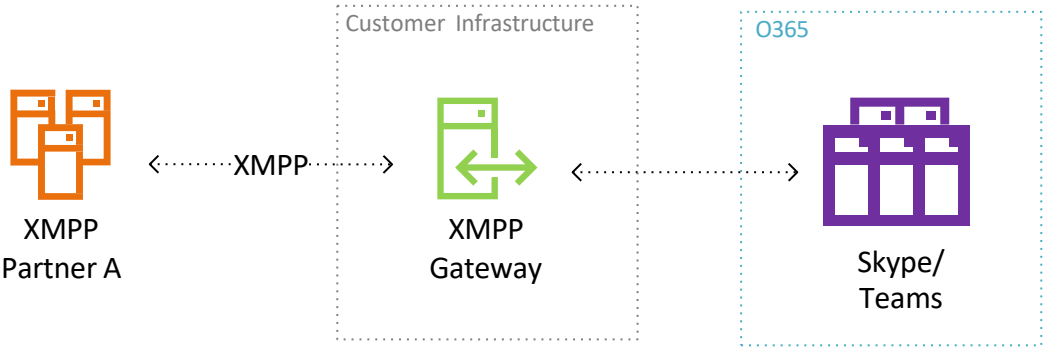


The server will communicate via SIP/TLS with the Skype for Business frontend pools over the internal network, and via server-server XMPP/TLS with remote XMPP domains.

A separate gateway installation is required for each on-premise Skype domain.

Hybrid Skype for Business or Teams

The server is deployed as a standalone gateway by the customer, managed by the customer as an external peer to the Microsoft-managed O365 cloud.



The server communicates with O365 components using O365 APIs and SIP via the public network, and via server-server XMPP/TLS with a remote XMPP domain.

Identities

The server understands SIP/O365 identities on the internal Skype/Teams side, and XMPP JID identities on the external XMPP side. It applies consistent bi-directional mapping logic to generate:

- An XMPP JID for an internal user's SIP address.
- A SIP address for an external user's XMPP JID.

On the internal side, the gateway impersonates external users as federated SIP identities. These identities do not actually exist in the internal directory, and no configuration of additional Skype/Teams-enabled accounts etc. is required.

Rights to "impersonate" external accounts are afforded to the gateway by the certificate-trust and routing mechanisms in the Skype and O365 platforms.

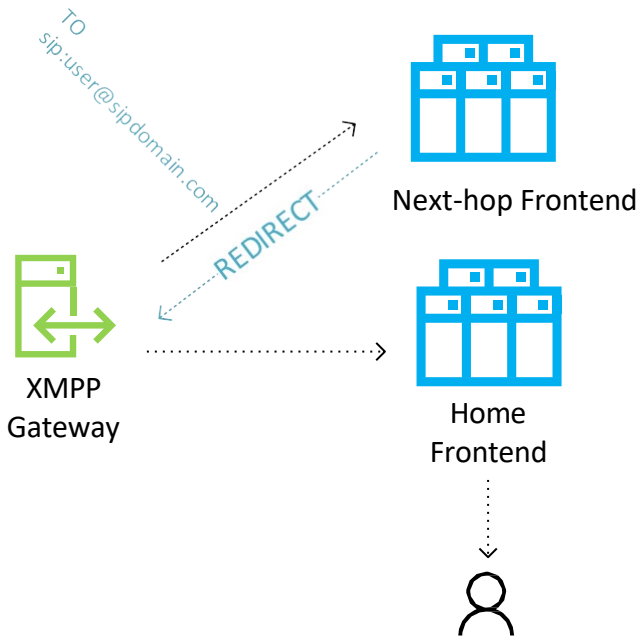
Routing

The gateway brokers message packets between SIP/Teams and XMPP components. All interaction between these components will be conducted via the gateway.

As such, both internal Skype/Teams components and external XMPP systems must be able to understand that messages for their counterparts should be routed through the gateway, and the gateway must understand correct forwarding routes for translated messages in each direction.

This is typically achieved on either side of the gateway using DNS records for discovery and certificates for authentication and trust.

Here, we discuss routing logic for message packets over the 4 unidirectional legs that the gateway will manage.



- Hybrid Skype/Teams – The gateway forwards the packets to the Skype edge services in the Hybrid/Teams environment. These are resolved via public DNS discovery records.

Scale Out

Capacity Model

Each gateway instance supports a minimum-hardware capacity model based on a maximum number of connected conversations and unidirectional presence subscriptions. The capacity model will be rated and tuned accordingly through planned load testing.

In terms of Skype/Teams users, the capacity model is translated based on an average number of XMPP-federated contacts and active XMPP-federated conversations per user, drawn from Microsoft modelling data.

Given a baseline minimum hardware specification:

- CPU: Quad core 2.4GHz
- RAM: 4GB
- Disk: 500MB

A single instance is rated for 2000 *concurrently active* users (TBC with planned load testing)

In future, further capacity can be achieved by adding more gateway nodes in a load-balanced pool configuration, or by increasing server resources.

Performance data is emitted by the server process to monitor system load, which can be used to more accurately assess required hardware resources in the given production environment.

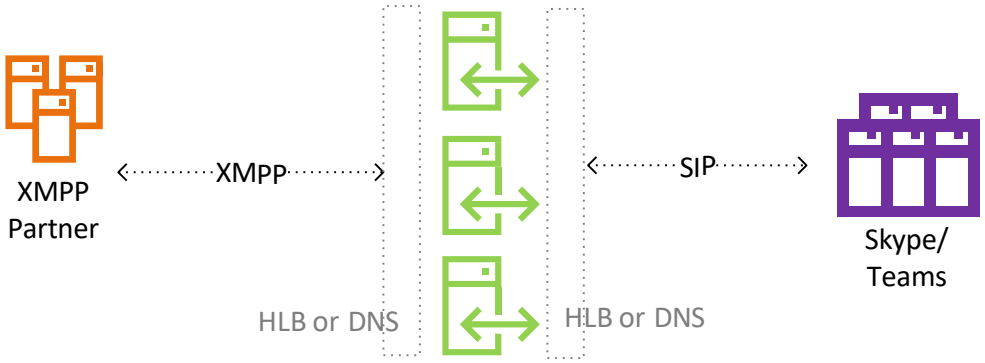
High Availability

Tolerance of node failures is handled by adding additional redundant nodes to the pool.

Load Balancing

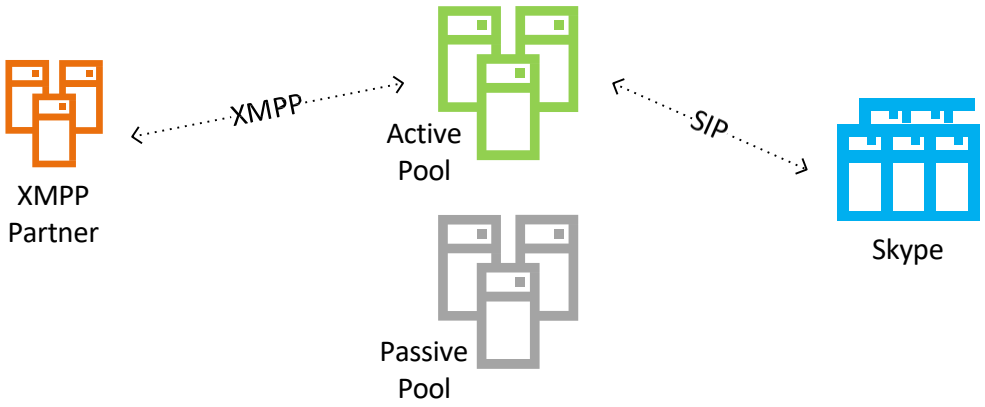
Load balancing of the internal surface is achieved via Skype for Business/SIP Federation pooling mechanisms – either a TLS-layer hardware load balancer or DNS load balancing.

Similarly, load balancing of the external XMPP surface is performed via a hardware load balancer, or DNS load balancing. Chosen mechanisms must be compatible with federated XMPP server implementations.



Failover

Disaster recovery failover is achieved via site-level redundancy. Active/passive pool failover is supported as a minimum basic strategy.



Failover of external XMPP connections is made by changing external DNS records and network configuration. Failover of internal SIP connectivity is made by the standard trusted application failover process.

Security

XMPP Domain Whitelisting

Allowed federated XMPP domains must be explicitly whitelisted in the gateway configuration. Messages forwarded to non-whitelisted domains will be dropped.

XMPP Transport Security

Server-server XMPP connections are secured over TLS. The TLS version is configurable – TLS 1.2 is supported, though negotiation of the effective TLS version does require mutual support from the federated XMPP components.

Server-server XMPP connections are authenticated via SASL handshake. Unauthenticated connections or unauthorized connections will be terminated.

SIP Transport Security

SIP connectivity with the Skype for Business topology is over TLS 1.2, secured and authenticated via mutual TLS, as prescribed by the Skype for Business trusted peer model.

Internal User Whitelisting

Skype/Teams users must be explicitly enabled via Active Directory config for access to federated XMPP users via the gateway. Messages to or from Skype/Teams users that are not enabled will be rejected.

Protocol Validation

XMPP packets are validated for structure and content. Connections sending invalid packets, or packets that are above a maximum size, will be immediately terminated.

Protocol Throttling

Packets are processed on a buffered queue with a maximum capacity. Processing of packets is throttled and the packet discarded if processing resources are overwhelmed.

Installation

The gateway server is delivered as a self-contained installer.

The gateway server should be installed on a Windows Server with bi-directional network connectivity, DNS resolution and certificate trust to the rest of the Skype for Business topology components.

The installer deploys the server binaries, configuration utilities, and registers the application as a Windows service.

The following pre-requisites must be in place:

- .NET Core 6
- Service account/application credentials

The installer also automates registration of the MSPL scripting overrides to the Skype default routing configuration, as appropriate.

In-place upgrade of the gateway component is supported for future versions.

Configuration

The gateway application is deployed with an accompanying graphical management interface.

Skype for Business On-Premise

The gateway should be configured as a trusted application in the Skype topology. The standard pre-requisites apply:

- Configuration of the Windows servers as a trusted application pool in the topology.
- Registration of a trusted application on the pool
- Acquisition of an appropriate trusted application pool certificate

Active Directory

The gateway should be configured with a connection to Active Directory. This is used to resolve and map internal user identities, and to determine whether a user is enabled for federated communication via XMPP.

The gateway service account should have rights to query Active Directory. For a hybrid or O365 installation, the service must be able to query the associated tenant users from the on-premise Active Directory or Azure AD components.

The gateway should be configured with a subset of Skype-enabled internal users that may bi-directionally communicate with external XMPP users via the gateway. This is done via query constructs over the directory.

XMPP Interface

The gateway should be configured with a whitelist of external XMPP domains with which it is allowed to communicate bi-directionally. Explicit server addresses may be configured for connections to each domain, otherwise dynamic DNS queries will be used to discover the servers.

The gateway should be provided an external certificate with which to authenticate to external XMPP servers. The subject of the certificate should meet the XMPP server-server validation requirements.

Edge Traversal

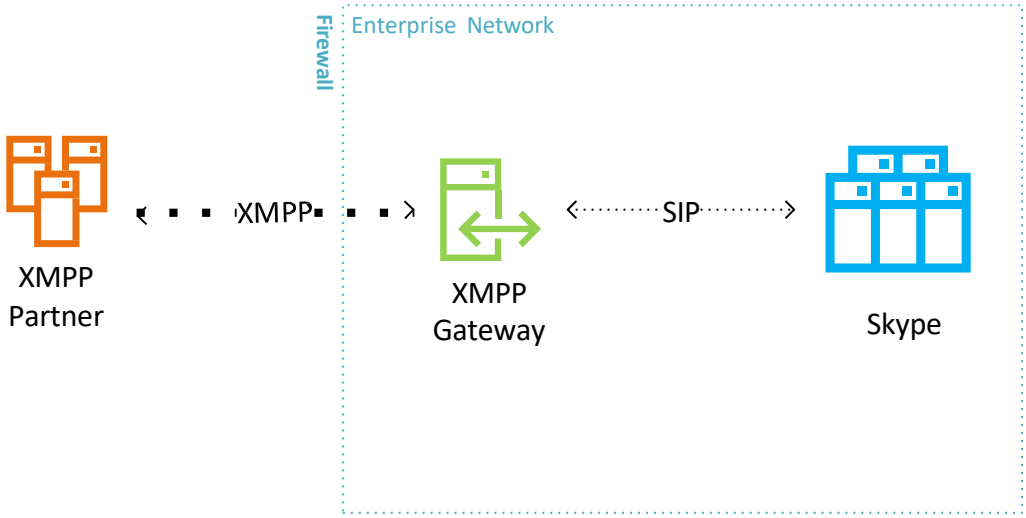
In an on-premises deployment, the gateway is deployed on the enterprise's internal network. To communicate with external federated XMPP servers, it must be able to communicate over the external network, typically on the default port 5269.

XMPP server-server connections are mutual and bi-directional – each server-server connection consists of two TLS connections, one established in each direction. The gateway must therefore be able to initiate connections to any whitelisted XMPP domain server, and be able to receive connections.

Every organisation has a different perimeter network architecture, and different security policies. The gateway is therefore designed to be as agnostic as possible in terms of how these connections are routed to and from the external network. It must be noted, however, that these connections are TCP/TLS connections, so HTTP proxy infrastructure cannot be leveraged.

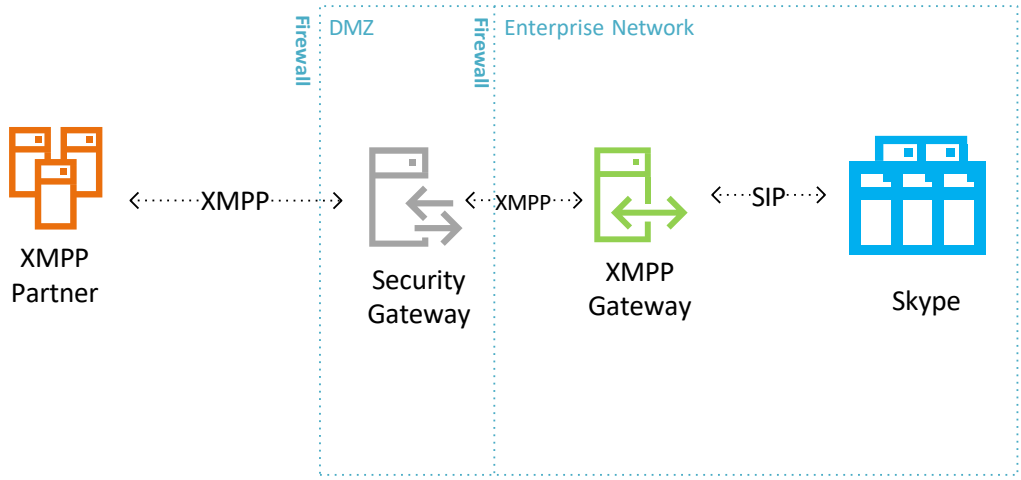
Single Firewall Architecture

The simplest case is direct connectivity through a single external firewall:



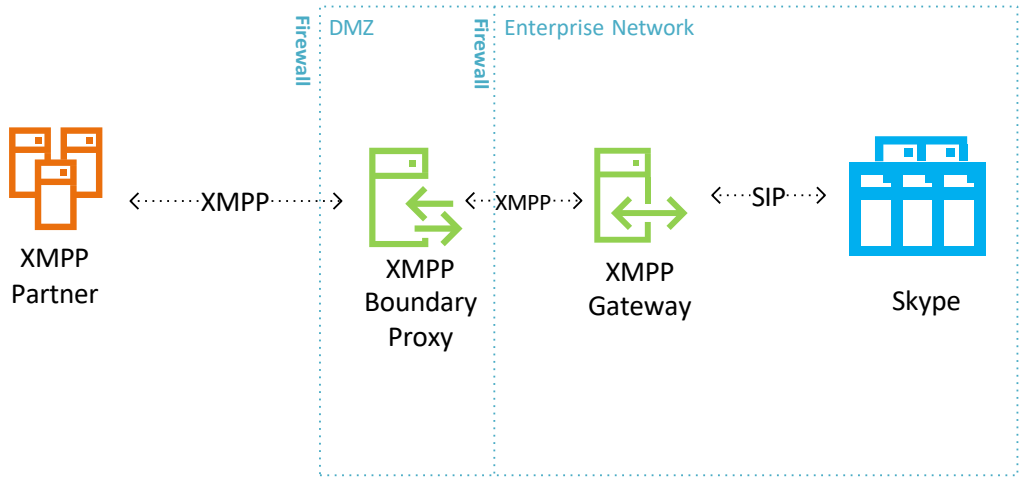
DMZ Architecture

Most organisations typically deploy a "DMZ" network area, between external and internal firewalls. Typically, a third-party network security appliance is deployed to proxy connections across this zone. We support any appliance that can proxy raw TLS connections:



Boundary Proxy

For highest-security deployments, application-level checking of all cross-boundary traffic is required. In this case, an XMPP proxy component is required in the DMZ, to explicitly validate and proxy all traffic.



MindLink are investigating development of such a proxy alongside the main gateway component, given customer need. This proxy would enforce protocol-level authentication and validation, before any traffic reaches the internal network.

It is also a candidate location to enforce additional whitelisting and DLP checks – for instance, dirty-word filtering.

Interop

MindLink assure interop with XMPP and Microsoft systems through automated and manual testing.

Skype for Business Server

The gateway supports Skype for Business Server 2015 and 2019. The gateway leverages UCMA versions 5 or 6 respectively, depending on the topology version.

MindLink typically support and test against the latest available cumulative updates for each major server version.

Skype for Business Clients

The gateway is compatible with any supported Skype for Business client, or third-party client (including MindLink Anywhere). All instant messaging is ultimately routed to and from the internal user's client through the Skype for Business frontend stack, and as such, all frontend-based messaging workloads – e.g. compliance archiving, server-side conversation history – are still compatible.

Teams

The gateway is supported with all production interop interfaces with the O365 cloud. MindLink will maintain support and issue compatibility updates as required, given notice from Microsoft support.

Again, interop is via backend services and compatibility concerns are largely insulated from client-specific changes.

XMPP

The gateway honours the latest XMPP-Core and XMPP-IM/P specifications. Nevertheless, interop with specific remote XMPP server implementations may require additional testing and logic, since there are typically nuanced behavioural differences between different implementations.

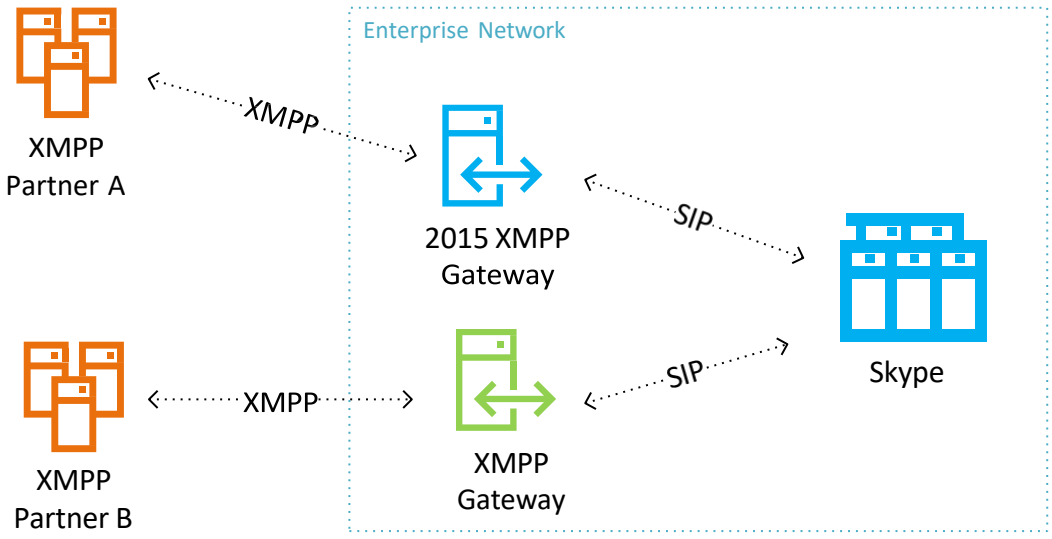
Initial development has been performed using the OpenFire implementation. Further discovery work against other XMPP implementations may be performed given customer requirements.

2015 XMPP Migration

The gateway sits alongside the Skype for Business topology as a third-party component. Therefore, it is able to co-exist alongside a deployed legacy Skype for Business XMPP gateway.

Only one gateway implementation will be able to service a given XMPP domain, however, since the internal Skype for Business and external XMPP servers must explicitly know which single gateway address to use for connectivity.

Low-risk POC and piece-meal migration is possible by migrating connectivity with a single federated XMPP domain at a time.



Diagnostics

The gateway produces log tracing at various configurable levels to its own logging stack. The logs contain diagnostic event and business logic information, not contain actual message content.

The Microsoft UCMA components of the gateway log to the Skype for Business ETW channel, capturable from the CLS logger.

The gateway publishes appropriate performance counter data, useful for performance and health monitoring.

Testing

The gateway is tested in-house by MindLink as part of the release cycle. This primarily involves automated acceptance testing via pre-defined simulated XMPP connections.

Manual testing against specific XMPP implementations is also be performed, based on customer requirements. Load tests to ascertain and verify capacity models are also be performed.

Certification of the gateway as a Microsoft-approved product will be performed if required.

Release Cycle

MindLink products are typically released on a 6-week cadence, based on incremental rolling improvements.

Licensing

Productization

The gateway is offered as a third-party product for Skype for Business and O365, purchasable directly from MindLink or via a MindLink reseller.

License Model

The licensing model is currently under review and MindLink endeavours to communicate this post-review.