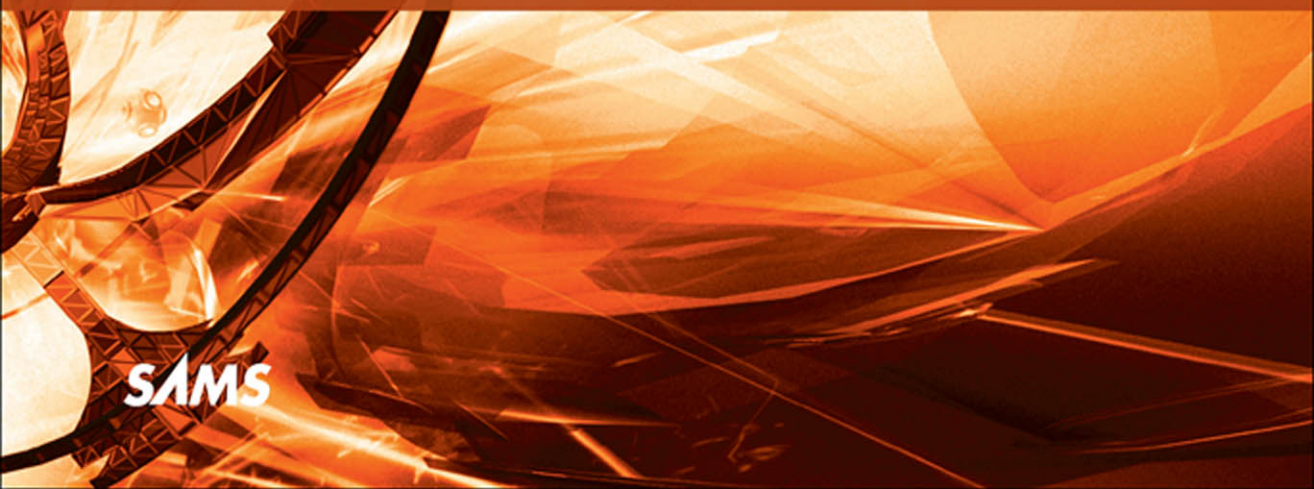
Alex Lewis
Pat Richard
Phil Sharp
Rui Young Maximo

Foreword by

Jamie Stark
Skype for Business Senior Product Manager, Microsoft

Skype® for Business

UNLEASHED



Alex Lewis, Pat Richard,
Phil Sharp, Rui Maximo

Skype for Business

UNLEASHED

SAMS | 800 East 96th Street, Indianapolis, Indiana 46240 USA

TABLE 11.2 (*Continued*)

Service	Protocol	Port	Direction	Description
Internal Edge Service	TCP	50001–50003	Inbound	This port must be opened to the Edge Server to allow the Central Logging Server (CLS) to collect logs from the Edge Server.

NOTE

The terms *inbound* and *outbound* refer to the direction between the Internet or internal network and the specified Edge service. For example, if the service is A/V Edge, and the column in the table says "Inbound," you must open the port with the destination address of the A/V Edge service IP address.

Using Network Address Translation (NAT) with Skype for Business Server 2015

Firewall NAT-ing of the external network interfaces is supported for single Edge Server deployments or Edge pool deployments that use DNS load balancing. NAT is not supported on the internal network interface of the Edge Server or Edge pool. NAT effectively takes packets bound for the firewall and forwards them to hosts inside the firewall based on port rules. This enables a company with limited numbers of routable IP addresses to support multiple services with fewer public IP addresses. In addition, it enables protected systems to hide their IP information because they never appear to be the source of a packet on the Internet; the firewall always appears to be the source. The NAT address for the A/V Edge must be specified in Topology Builder.

TIP

If you enable NAT for the external firewall, configure firewall filters that are used for traffic from the Internet to the Edge Server with Destination Network Address Translation (DNAT). Similarly, configure and filter for traffic going from the Edge Server to the Internet with Source Network Address Translation (SNAT). Note that the inbound and outbound filters for this purpose must use the same internal and external addresses. If externally the Edge is reachable at 11.22.33.44 and is mapped to an Edge Server internally at 10.1.1.44, outbound traffic from the Edge Server, 10.1.1.44, out to the Internet needs to come from the external IP address, 11.22.33.44. Although this might seem obvious, there are many situations in which all internal hosts appear to come from the same IP address. This is called PAT, or Port Address Translation, or is sometimes called NAT overload.

CAUTION

NAT-ing is not supported for Edge pool configurations that are load balanced using a hardware load balancer (HLB) because this would result in NAT-ing the connection twice, which is not supported for audio/video traffic. Therefore, the external firewall cannot be configured for NAT.

Reverse Proxy Requirements

Using reverse proxies such as F5, NetScaler, and A10 is an excellent way to securely publish applications such as Skype for Business Server 2015 to the Internet. Reverse proxies provide an intermediary layer between internal web servers and the Internet. Web requests from the Internet cannot reach internal web servers directly; they are proxied by reverse proxies. This best practice is recommended for exposing Skype for Business web services to the Internet. The following sections discuss how to configure reverse proxies to work with Skype for Business Server 2015.

Why a Reverse Proxy Is Required

It is important to understand why a reverse proxy solution is required for Skype for Business Server 2015. A reverse proxy is required to publish Skype for Business web services to external users. These web services are responsible for the following:

- **Autodiscover—**`lyncdiscover.<SIP domain>` is the preferred DNS record for Skype for Business clients to discover the organization's Skype for Business Server.
- **Simple URL publishing—**Allows users to join a Skype for Business meeting or obtain meeting dial-in information.
- **Meeting Web Scheduler—**This web service allows users to schedule a Skype for Business meeting without using the Skype for Business plug-in for Microsoft Outlook.
- **Web conferencing content—**Allows users to share collaboration content (application, desktop, whiteboard) during a Skype for Business meeting.
- **Address book and distribution list (DL) expansion—**Used by Skype for Business clients to download the Address Book and perform group expansion of distribution lists (DL). This enables users to search other internal users and groups.
- **Windows authentication—**Remote users can sign in to Skype for Business Server using NTLM authentication. Kerberos authentication is not possible for remote users.
- **Certificate provisioning—**Skype for Business Server supports client certificate authentication (TLS-DSK) to authenticate remote users. This web service allows remote clients to obtain a certificate from Skype for Business web services. Once obtained, the Skype for Business client can authenticate the user using the certificate instead of prompting for the user's username and password (NTLM).
- **Passive authentication—**Skype for Business Server supports OAuth to authenticate remote users. Skype for Business Server 2015 can be configured to enforce passive authentication for mobile clients only if desired. Passive authentication enables multifactor authentication (MFA) when integrated with a third security token service (STS).
- **Web ticket—**Once the remote user is authenticated using NTLM, TLS-DSK, or passive authentication, Skype for Business Server 2015 issues a compact web ticket (CWT) to the client. This CWT, similar to a cookie, allows the user to remain

authenticated for 8 hours without the server challenging the user to re-authenticate with each subsequent request. The Skype for Business client refreshes the CWT by TLS-DSK authentication using the client certificate before it expires in order to remain authenticated to the server.

- **Device updates—**Skype for Business Phone Edition devices require access to the Skype for Business Web Services to obtain software updates.
- **RGS client access—**This web service allows Skype for Business users to participate in a response group service remotely.
- **Web App—**This Skype for Business web service allows participants to join a Skype for Business meeting from a browser for those users who do not have a Skype for Business client.
- **Mobility—**Skype for Business clients on the mobile platforms Windows Phone, Android, and Apple iOS connect through the Skype for Business UCWA web services.

In addition to these Skype for Business web services that a reverse proxy exposes to the Internet, remote Skype for Business clients need access to Exchange Web Services (EWS) to obtain calendar information and join meetings. If the reverse proxy does not publish Exchange Autodiscover and EWS to the Internet, the functionality of remote Skype for Business clients will be impaired.

To share PowerPoint presentations, Skype for Business Server 2015 leverages Office Web Apps Server to enable this functionality. To allow remote Skype for Business clients to share PowerPoint presentations, Office Web Apps server must be published through the reverse proxy; otherwise, remote users will not be able to present or view PowerPoint presentations.

Deploying a reverse proxy solution with Skype for Business Server 2015 is absolutely critical in order to enable external user access. To deploy Skype for Business Web services, the reverse proxy solution must meet the following requirements:

- **HTTPS publishing—**Devices must be capable of securely publishing application content. Devices that support this functionality will specifically call this out as a feature.
- **SSL bridging—**Skype for Business Server 2015 requires the reverse proxy to listen for connections on TCP port 443 and bridge those connections to the Front End Web services on TCP port 4443. This is required because the Skype for Business web services contain separate virtual web directories. The external Skype for Business web services directory listens on port 4443 and should be used when publishing to the Internet.
- **Authentication bypass—**The reverse proxy should allow user authentication to occur at the Skype for Business Servers, not be authenticated by the reverse proxy itself.

CAUTION

It is not recommended (or supported by Microsoft) to deploy external web services without a reverse proxy solution. Do not use NAT as a replacement for a reverse proxy solution.

TIP

As a low-cost alternative, you can use Microsoft Application Request Routing (ARR) as a software-based reverse proxy. ARR is installed on a Windows Server with IIS configured.

Certificate Requirements

Chapter 10, "Dependent Services," covers certificate requirements in detail. In general, the reverse proxy certificate requires a public certificate with the following entries:

- **Skype for Business web services external FQDN—**This is defined in the topology and should be configured as the Subject Name (SN) of the certificate.
- **Simple URL entries—**There should be a certificate entry in the subject alternative name (SAN) field for every meeting and dial-in URL. There is typically a single dial-in FQDN, and there is a meeting FQDN for each SIP domain your organization is authoritative for.
- **LyncDiscover—**Skype for Business clients discover your Skype for Business Servers by querying for the DNS entry `lyncdiscover.<sipdomain>`. The first authentication is against this URL over HTTPS. As such, the reverse proxy certificate requires an entry for each SIP domain in the SAN.

Reverse Proxy Configuration

This section outlines tasks for configuring a reverse proxy for Skype for Business Server 2015.

Creating DNS Records for Reverse Proxy

To enable clients on the Internet to find Skype for Business Server 2015, add an address (A) record to an external DNS that is authoritative for your organization's domain. This includes (A) records, as described in Chapter 10.

NOTE

The procedure for creating records depends on the domain name server used. In the case of an externally hosted DNS, it might be as simple as calling your service provider and requesting the records.

Keep in mind that it might take several minutes to as much as a few hours for the new records to propagate and become available to clients.

On most reverse proxies, it is possible to have all external Skype for Business web services DNS records point to the same IP address.

Verifying Access to Skype for Business Web Services

Assuming that the firewall rules are in place and that the necessary DNS records are published externally, use the test connectivity tool (https://testconnectivity.microsoft.com)

from Microsoft to verify that your Skype for Business web services are accessible through your reverse proxy. This web-based utility will validate whether your Exchange Server and Skype for Business Server are correctly published to the Internet.

File Share Permissions

Skype for Business Server 2015 utilizes a file share for each pool. You can use the same file share for multiple pools or a separate file share per pool. This file share is used to store conferencing, CMS configuration replication, and address book information. This file share has strict permission requirements, and Skype for Business Server 2015 will assign permissions to these file shares during the deployment of your pools. Do not change the file share security permissions.

When deploying any Skype for Business Server 2015 topology changes, you must make sure that you have read/write access to the file shares in the topology. When you publish a topology change, Topology Builder will validate permissions on the file shares.

TIP

If the file-share permissions are ever changed by accident, simply publish the Skype for Business Server 2015 topology again and these permissions will be re-created.

Securing Service Accounts

When you are deploying Edge Servers in the DMZ, these Windows Servers are not domain-joined to the internal Active Directory Domain Services to maintain separation of access between the DMZ and the internal network. The same is true if using a Windows Server-based reverse proxy. Resources in the DMZ should not have direct or permissive access to the internal network unless explicitly permitted.

By limiting access to internal resources from the systems in the DMZ, you reduce the opportunities an attacker can leverage to access the internal network. This includes service accounts. The service account used by Skype for Business Server 2015 to run the Edge services are local accounts and not domain accounts. The Edge services use the Network Service account. This way, should the Edge Server become compromised, this service account doesn't have any permissions to internal resources.

Security Threats

Any server product that exposes services to the Internet is at risk of being compromised and becoming a conduit for unauthorized access into the organization's internal network. Skype for Business Server 2015 is no different. The primary entry points into a corporate network's Skype for Business Servers are the Edge Servers, reverse proxies, and the Session Border Controller (SBC).

The Edge Server is used for federation and remote user access. It allows Internet access to the following protocols:

- **SIP—**Used for signaling and IM traffic
- **SRTP—**Used for audio/video traffic
- **PSOM—**Used for web conferencing traffic

The reverse proxy provides access to Skype for Business mobile clients and Web App and other web services. It allows Internet access to internal Skype for Business web services over HTTPS.

The SBC is used as a point of demarcation between your network and the ITSP when connecting Enterprise Voice to the PSTN. The SBC, though generally connected to the ITSP through a private network, can use the Internet as an interconnect.

Each of the entry points (that is, ports) used by Skype for Business Server 2015 may be susceptible to attack, and the protocols used through these ports can be exploited. It is no longer sufficient to restrict port access as a security measure. All web services use the same port (443, for example). Therefore, blocking external access to port 443 is not a practical solution. In order to control access at a more granular level, it is necessary to secure access at the protocol level. Table 11.3 outlines the ports and protocols for all the functionality used by Skype for Business clients.

TABLE 11.3 Ports and Protocols for External Access to Skype for Business Server 2015 from the Internet

Functionality	Product	External Entry Point	Protocol	Port
Remote access	Skype for Business	Edge Server – Access Edge	SIP	TCP:443
Federation	Skype for Business	Edge Server – Access Edge	SIP	TCP:5061
Audio/video	Skype for Business	Edge Server – A/V Edge	SRTP	TCP:443, UDP:3478
Web conferencing	Skype for Business	Edge Server – Conf Edge	PSOM	TCP:443
File transfer	Skype for Business	Edge Server – A/V Edge	ICE	TCP:443
XMPP interop	Skype for Business	Edge Server – Access Edge	XMPP	TCP:5269
Application sharing	Skype for Business	Edge Server – A/V Edge	RDP	TCP:443
Dial-in	Skype for Business	Reverse Proxy	HTTPS	TCP:443
Address book	Skype for Business	Reverse Proxy	HTTPS	TCP:443
Certificate provisioning	Skype for Business	Reverse Proxy	HTTPS	TCP:443

(*Continued*)