Network Integration of Microsoft Office Server Products

High-level concepts for Lync, Exchange, SharePoint Server, and Office Web Apps

Users outside the network and cloud services

Authentication for external access

Gateway router with ACLs

Remote access servers for Lync and SharePoint

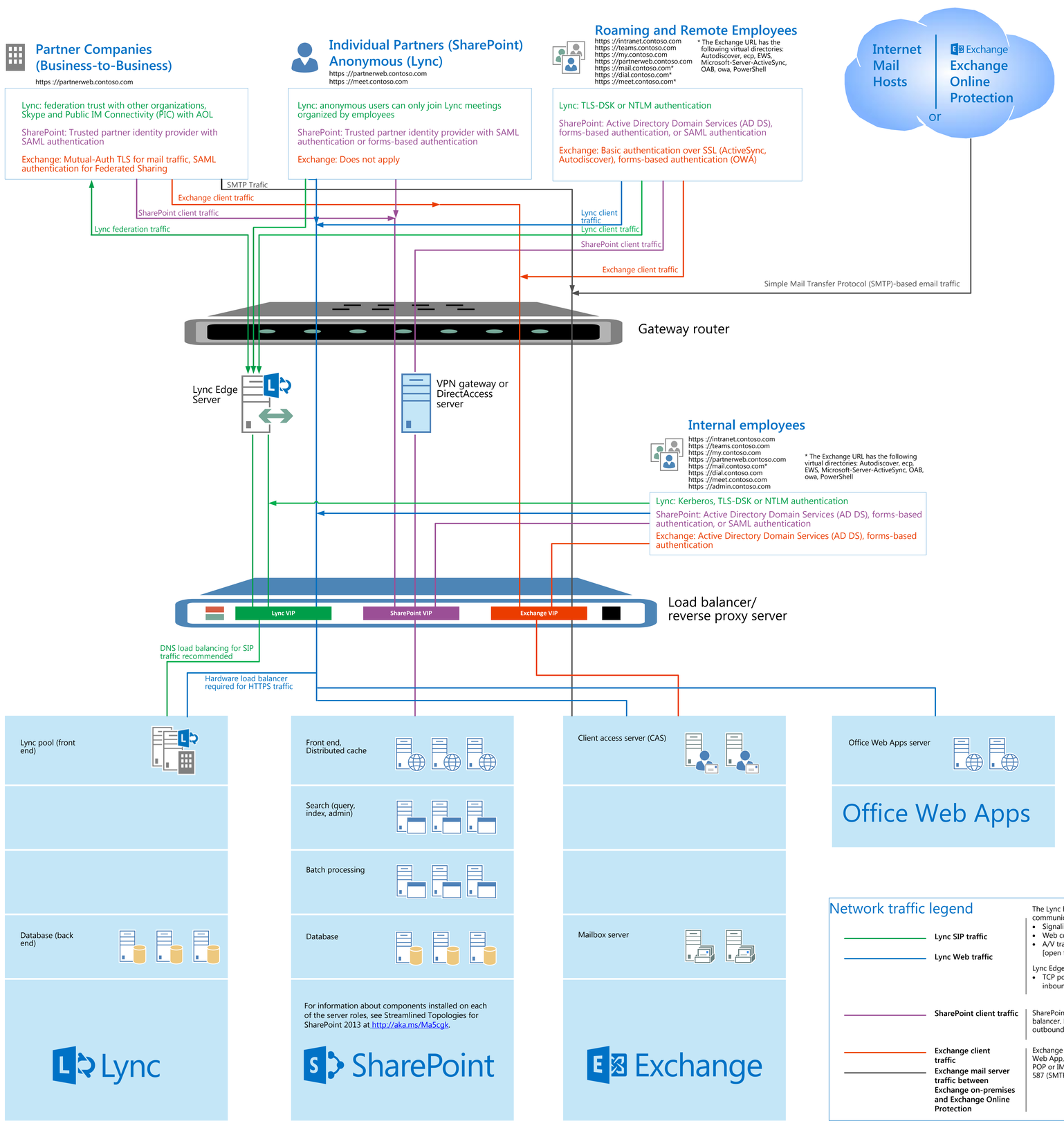
Internal users (far right)

Load balancer and reverse proxy device

Front-end, client-access tier

Application tier

Database/storage tier



About the design

Streamlined network design

This topology illustrates an on-premises network deployment of Microsoft SharePoint Server 2013, Microsoft Exchange Server 2013, and Microsoft Lync Server 2013. It also shows the use of the Microsoft cloud-based service, Exchange Online Protection, to provide anti-spam and malware protection for inbound SMTP traffic from the Internet.

This network design is streamlined to a minimum set of network components. The design does not take into account additional security or infrastructure features that might be required by some organizations.

This diagram:

- Provides a sample network topology illustrating inbound and outbound traffic through a gateway router and load balancing of client session traffic (external and internal) to the appropriate SharePoint, Exchange, and Lync server tiers.
- Shows the use of optional remote access servers, such as a third-party VPN gateway or DirectAccess server, to provide secure communication for roaming or remote employees.
- Details the SharePoint, Exchange, and Lync traffic flow from the client to each platform server tier.
- Identifies the type of remote or internal access connection based on client (such as partner or employee), and the authentication method used.
- Breaks down the SharePoint, Exchange, and Lync platforms by required server roles, identifying the front-end, application, database, and other levels.

Note: The architecture used here for SharePoint, Lync, and Exchange does not suggest a preferred way for implementing these platforms. It merely provides an example as topologies differ based on unique network requirements and security considerations.

Gateway router

For this topology, the gateway router sits at the edge of the network and routes all incoming and outgoing traffic to and from the intranet. Alternatively, there could also be other components that bridge the gap between the gateway router and the load balancer shown, such as multiple layers of firewalls. The topology shown represents just one way to deploy your network out of many. In this configuration, the gateway is configured with access control lists (ACLs) to permit very specific incoming and outgoing IP-based traffic on the router interfaces. ACLs, advanced inspection, or Network Address Translation (NAT) can also be performed on other devices, such as firewalls, throughout your network.

Load balancer and reverse proxy device

You can use hardware or software load balancing solutions to redirect traffic for segments including SharePoint front-end web Servers and Exchange Client Access Servers (CASs). In some cases it's optimal to use a layer-7 hardware-based load balancer for persistence requirements as it can make decisions based on information in the request, such as cookies or headers. However, factors like cost and increased utilization and workload from such a solution may not be desirable for your specific needs. Some points to consider for load balancing across SharePoint, Exchange, and Lync:

- **SharePoint** - For SharePoint 2013 you do not need to enable affinity for your front-end web servers. Normally this would be used for creating sticky sessions and avoiding multiple authentication requests from clients to each front end web server. The new Distributed Cache service in SharePoint 2013 stores and distributes logon tokens across the web servers of the SharePoint farm.
- **Exchange** - In Exchange 2013, the CAS role is designed to use Layer 4 load balancing, distributing requests at the Transport layer. This can significantly decrease load balancer utilization and workload.
- **Lync** – Domain Name System (DNS) load balancing is recommended for Session Initiation Protocol (SIP) traffic for Lync pools. Hardware load balancing (HLB) is required for Lync Web (HTTPS) traffic.

Remote access options

There are several options that can publish intranet resources for partners on the Internet or provide secure remote access for remote or roaming employees. Such examples include reverse proxies, DirectAccess, and third-party VPN gateways. The remote access solutions discussed below are possibilities for SharePoint, Lync, and Exchange, or any combination of these servers in an on-premises deployment. However, some remote options may not work with a particular solution.

Reverse Proxy - A reverse proxy supports traffic encryption, such as Secure Sockets Layer (SSL), and allows you to publish intranet applications and web resources to authenticated users and partners on the Internet. An example is Microsoft Forefront Unified Access Gateway (UAG).
Many hardware load balancers also support reverse proxy functionality. However, there are still valid scenarios for using a standalone solution based on your needs and requirements such as traffic isolation, security compartmentalization and performance optimization. Some benefits and considerations:

- Provides authenticated and secured access for partners or users accessing intranet resources (uses SSL (TCP 443) between the client and reverse proxy server).
- For Exchange, a benefit of using a reverse proxy such as Forefront UAG is pre-authentication before accessing the Exchange Client access server. Remote access users using published applications such as Outlook Web Access (OWA) could authenticate with the basic, NTLM, or Kerberos methods before reaching the internal network.
- For Exchange and SharePoint, solutions like Forefront UAG can terminate SSL connections and decrease the load off the intranet resources server, while providing a single point of management for certificates.
- For Lync, Web (HTTPS) traffic goes through the reverse proxy (TCP 443) for client communication. The reverse proxy proxies the HTTPS connection to Lync Web Services, Exchange CAS, and Office Web Apps. Lync Server 2013 does not support UAG.

DirectAccess – A remote access technology that relies on Internet Protocol security (IPsec) for authentication and for encrypting traffic between the DirectAccess client and server. DirectAccess provides simultaneous access to both Internet and intranet resources for roaming and remote employees without having to initiate a connection. Points to consider:

- DirectAccess uses IPsec protected traffic (protocol 50 and 51 and UDP 500) between the DirectAccess client and server.
- DirectAccess for Windows Server 2012 and Windows 8 does not need a public key infrastructure (PKI) deployment for server and client authentication.
- We recommend against using DirectAccess with Lync Server 2013 because of audio and video latency issues associated with IPsec encryption and decryption.

VPN Gateway – Typical VPN gateways provide a remote access connection, in which a remote access client computer is logically projected onto the intranet through a tunneled and user-initiated connection. You can use Unified Remote Access in Windows Server 2012 or several third-party solutions to provide secured access to the intranet for roaming or remote employees. VPN is not recommended for Lync. Remote Lync traffic should use the Edge Servers and split tunneling.

Domain Name System (DNS) considerations

You need to plan for the set of DNS records that allow both Internet and intranet users to resolve DNS names to the appropriate IP addresses.

- For Internet-based partners and roaming or remote employees, DNS records registered with Internet DNS servers provide resolution to the set of public IP addresses corresponding to the gateway router, the Lync Edge Server, the set of virtual IP addresses (VIPs) on the load balancer, and the DirectAccess or VPN gateway as needed.
- For intranet-based users, DNS records registered with intranet DNS servers provide resolution to the set of virtual IP addresses (VIPs) on the load balancer for access to SharePoint, Lync, and Exchange resources.
- DirectAccess clients use intranet DNS servers for names corresponding to the intranet DNS name space and Internet DNS servers for names that do not. To simplify the operation of DirectAccess, consider the use of a split DNS implementation that uses different DNS namespaces for intranet and Internet-based names. For example, use contoso.com for Internet namespace and corp.contoso.com for the intranet namespace.
- Exchange uses a split DNS model where host to IP resolution differs on publicly routed traffic than on the corporate network. At a minimum you need to have DNS records for OWA, Autodiscover, ActiveSync URLs for client traffic, and an MX record for inbound mail.
- If you are using Exchange Online Protection (EOP) your MX record points to that service instead of your Exchange farm.
- For Exchange you need a proof of ownership TXT record in your public DNS, and a Federation Org ID to set up federated sharing.
- Remote access VPN clients can be configured to use only intranet DNS servers when the remote access VPN connection is active.

Network traffic legend

Lync SIP traffic

Lync Web traffic

The Lync Edge Server uses the following ports for external user communication:

- Signaling/IM traffic (SIP/SIMPLE): TCP port 443 [open for inbound traffic]
- Web conferencing traffic (PSOM): TCP 443 [open for inbound traffic]
- A/V traffic (SRTP): TCP 443, UDP 3478 and TCP 50000-59999 (optional) [open for inbound and outbound traffic]

Lync Edge Server uses the following ports for federation communication:

- TCP ports 5061 (SIP), 5269 (XMPP), 443 and UDP 3478 (SRTP). [open for inbound and outbound traffic]

SharePoint client traffic

SharePoint can use TCP port 443 (SSL) for encrypted communication between the client and the load balancer. For external access from the Internet, this port needs to be opened for inbound and outbound traffic on the gateway router (or external firewall).

Exchange client traffic

Exchange mail server traffic between Exchange on-premises and Exchange Online Protection

Exchange uses TCP port 25 (SMTP) for server-to-server communications. Most client traffic (Outlook Web App, ActiveSync, Autodiscover, Outlook Anywhere) is handled over port 443 (HTTPS). If you have POP or IMAP clients, ports 110 (POP3), 995 (encrypted POP3), 143 (IMAP4), 993 (encrypted IMAP4), and 587 (SMTP) are also used to support these clients.

More on Lync network traffic?

Learn how Lync Server can help your organization provide instant messaging, web conferencing, application sharing, and voice communication.

Microsoft Lync Server 2013 Protocol Workloads Poster
http://aka.ms/G5jqjo

Microsoft