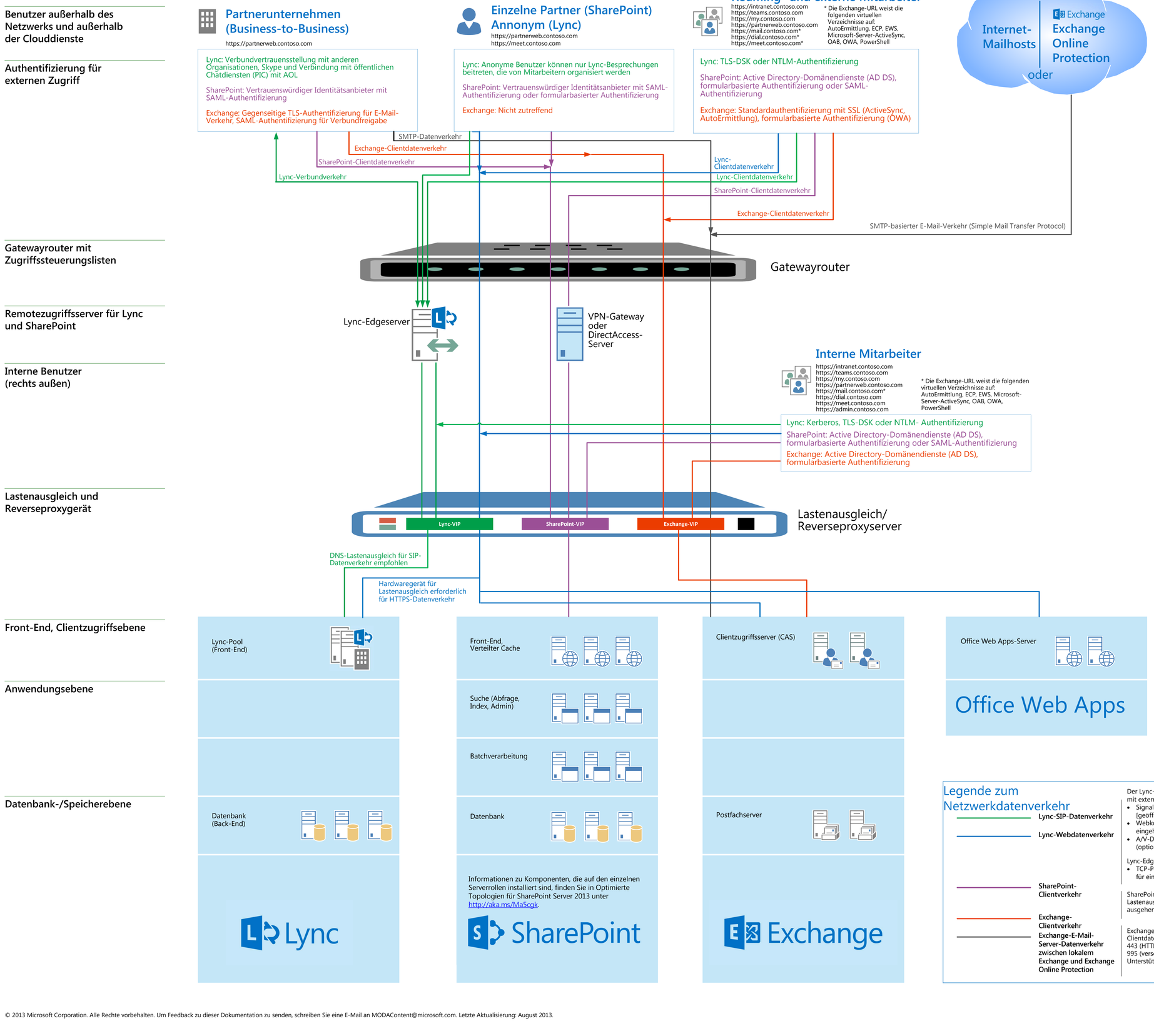
Netzwerkintegration von Microsoft Office-Serverprodukten

Allgemeine Konzepte für Lync, Exchange, SharePoint Server und Office Web Apps



Informationen zum Aufbau

Optimierter Netzwerkaufbau

In dieser Topologie ist eine lokale Netzwerkbereitstellung von Microsoft SharePoint Server 2013, Microsoft Exchange Server 2013 und Microsoft Lync Server 2013 dargestellt. Außerdem wird die Verwendung des cloudbasierten Microsoft-Diensts Exchange Online Protection veranschaulicht, um Antispam- und Malwareschutz für eingehenden SMTP-Datenverkehr aus dem Internet bereitzustellen.

Dieser Netzwerkaufbau ist so optimiert, dass es nur die minimal erforderlichen Netzwerkkomponenten umfasst. In dem Aufbau werden keine zusätzlichen Sicherheits- oder Infrastrukturfeatures berücksichtigt, die in manchen Organisationen möglicherweise erforderlich sind.

Dieses Diagramm:

- Stellt eine Beispielnetzwerktopologie dar, in der eingehender und ausgehender Datenverkehr über einen Gatewayrouter sowie der Lastenausgleich des Datenverkehrs der Clientsitzung (extern und intern) an den entsprechenden SharePoint-, Exchange- und Lync-Serverebenen veranschaulicht werden.
- Zeit die Verwendung optionaler Remotezugriffsserver, z. B. ein VPN-Gateway von einem Drittanbieter oder DirectAccess-Server, um sichere Informationen für das Roaming oder externe Mitarbeiter bereitzustellen.
- Zeigt den SharePoint-, Exchange- und Lync-Datenverkehrsfluss vom Client zu der Plattformserverebene im Detail.
- Identifiziert den Typ der Remote- oder internen Zugriffsverbindung basierend auf dem Client (z. B. Partner oder Mitarbeiter) sowie die verwendete Authentifizierungsmethode.
- Gliedert die SharePoint-, Exchange- und Lync-Plattformen nach erforderlichen Serverrollen auf und identifiziert dabei das Front-End, die Anwendung, die Datenbank und andere Stufen.

Hinweis: Die hier verwendete Architektur für SharePoint, Lync und Exchange stellt keine bevorzugte Implementierungsweise dieser Plattformen dar. Sie liefert lediglich ein Beispiel, da sich Topologien basierend auf einzigartigen Netzwerkanforderungen und Sicherheitsüberlegungen unterscheiden.

Gatewayrouter

Bei dieser Topologie befindet sich der Gatewayrouter am Rande des Netzwerks und leitet den gesamten eingehenden und ausgehenden Datenverkehr an das und aus dem Intranet weiter. Alternativ könnte es auch andere Komponenten geben, die die Lücke zwischen dem Gatewayrouter und dem angezeigten Lastenausgleich schließen, z. B. mehrere Ebenen von Firewalls. Die gezeigte Topologie stellt nur eine Möglichkeit der Bereitstellung Ihres Netzwerks von vielen dar. In dieser Konfiguration ist das Gateway mit Zugriffssteuerungslisten (ACLs) so konfiguriert, das sehr spezifischer eingehender und ausgehender Datenverkehr basierend auf IP-Adressen an den Routerschnittstellen zugelassen wird. ACLs, erweiterte Überprüfung oder Netzwerkadressübersetzung (NAT) können auch auf anderen Geräten, z. B. Firewalls, im gesamten Netzwerk ausgeführt werden.

Lastenausgleich und Reverseproxygerät

Sie können Hardware- oder Softwarelösungen für den Lastenausgleich verwenden, um Datenverkehr für Segmente, einschließlich SharePoint-Front-End-Webservern und Exchange-Clientzugriffsservern (CAS), umzuleiten. In manchen Fällen ist die Verwendung eines hardwarebasierten Layer 7-Lastenausgleichs für Persistenzanforderungen am besten geeignet, da Entscheidungen basierend auf Informationen in der Anforderung, z. B. Cookies oder Header, getroffen werden können. Es kann jedoch sein, dass Faktoren wie Kosten, gesteigerte Auslastung und höhere Arbeitslasten bei einer solchen Lösung für Ihre speziellen Anforderungen nicht erwünscht sind. Nachfolgend finden Sie einige Punkte, die für den Lastenausgleich bei SharePoint, Exchange und Lync berücksichtigt werden sollten:

- **SharePoint** – Für SharePoint 2013 müssen Sie die Affinität für Ihre Front-End-Webserver nicht aktivieren. Normalerweise würde diese für das Erstellen von so genannten "Sticky Session" und das Verhindern mehrerer Authentifizierungsanforderungen von Clients an die einzelnen Front-End-Webserver verwendet werden. Der neue Dienst für den verteilten Cache in SharePoint 2013 speichert und verteilt Anmeldetoken über die Webserver der SharePoint-Farm hinweg.
- **Exchange** – In Exchange 2013 ist die CAS-Rolle so konzipiert, dass ein Layer 4-Lastenausgleich verwendet wird, sodass Anforderungen auf der Transportebene verteilt werden. Dadurch kann die Auslastung des Lastenausgleichs sowie die Arbeitslast erheblich gesenkt werden.
- **Lync** – Für SIP-Datenverkehr (Session Initiation-Protokoll) für Lync-Pools wird der DNS-Lastenausgleich (Domain Name System) empfohlen. Für Lync Web-Datenverkehr (HTTPS) ist ein Hardwaregerät zum Lastenausgleich (HLB) erforderlich.

Remotezugriffsoptionen

Es gibt mehrere Optionen für das Veröffentlichen von Intranetressourcen für Partner im Internet oder das Bereitstellen von sicherem Remotezugriff für externe oder Roaming-Benutzer. Dazu gehören beispielsweise Reverseproxys, DirectAccess und VPN-Gateways von Drittanbietern. Die unten beschriebenen Remotezugriffslösungen sind Möglichkeiten für SharePoint, Lync und Exchange oder eine beliebige Kombination dieser Server in einer lokalen Bereitstellung. Manche Remoteoptionen funktionieren jedoch möglicherweise mit einer bestimmten Lösung nicht.

Reverseproxy – Ein Reverseproxy unterstützt die Verschlüsselung von Datenverkehr, z. B. Secure Sockets Layer (SSL), und ermöglicht eine Veröffentlichung von Intranet-Anwendungen und Webressourcen an authentifizierte Benutzer und Partner im Internet. Ein Beispiel ist Microsoft Forefront Unified Access Gateway (UAG).
Viele Hardwaregeräte für Lastenausgleich unterstützen auch die Reverseproxyfunktionalität. Es gibt jedoch immer noch gültige Szenarios für die Verwendung einer eigenständigen Lösung basierend auf Ihren Bedürfnissen und Anforderungen, z. B. Datenverkehrsisolation, Sicherheitsuntergliederung und Leistungsoptimierung. Nachfolgend finden Sie einige Vorteile und Überlegungen:

- Bietet authentifizierten und sicheren Zugriff für Partner oder Benutzer, die auf Intranet-Ressourcen zugreifen (verwendet SSL [TCP 443] zwischen dem Client und dem Reverseproxyserver).
- Bei Exchange besteht ein Vorteil der Verwendung eines Reverseproxys wie Forefront UAG in der Vorauthentifizierung, bevor auf den Exchange-Clientzugriffsserver zugegriffen wird. Remotezugriffsbenutzer, die veröffentlichte Anwendungen wie Outlook Web Access (OWA) verwenden, können sich mit der Standard-, NTLM- oder Kerberos-Methode authentifizieren, bevor sie in das interne Netzwerk gelangen.
- Bei Exchange und SharePoint können Lösungen wie Forefront UAG SSL-Verbindungen beenden und die Arbeitslast der Intranet-Ressourcenserver senken und dabei gleichzeitig einen einzigen Punkt für die Verwaltung von Zertifikaten bereitstellen.
- Bei Lync läuft der Webdatenverkehr (HTTPS) für die Clientkommunikation über den Reverseproxy (TCP 443). Der Reverseproxy überträgt die HTTPS-Verbindung an Lync Web Services, Exchange-CAS und Office Web Apps. Lync Server 2013 unterstützt UAG nicht.

DirectAccess – Eine Technologie für Remotezugriff, die auf IPsec (Internet Protocol Security) für die Authentifizierung und Verschlüsselung von Datenverkehr zwischen dem DirectAccess-Client und -Server basiert. DirectAccess bietet gleichzeitigen Zugriff auf Internet- und Intranet-Ressourcen für Roaming- und externe Benutzer, ohne dass hierfür eine Verbindung initiiert werden muss. Zu berücksichtigende Punkte:

- DirectAccess verwendet durch IPsec geschützten Datenverkehr (Protokoll 50 und 51 und UDP 500) zwischen dem DirectAccess-Client und -Server.
- DirectAccess für Windows Server 2012 und Windows 8 benötigt keine PKI-Bereitstellung (Public Key Infrastructure) für die Server- und Clientauthentifizierung.
- Die Verwendung von DirectAccess mit Lync Server 2013 wird aufgrund von Problemen mit der Audio- und Video-Wartezeit im Zusammenhang mit der IPsec-Entschlüsselung und -Verschlüsselung nicht empfohlen.

VPN-Gateway – Typische VPN-Gateways stellten eine Remotezugriffsverbindung bereit, bei der ein Remotezugriffs-Clientcomputer über eine Tunnelverbindung und eine benutzerinitiierte Verbindung logisch in das Intranet projiziert wird. Sie können Unified Remote Access in Windows 2012 oder mehreren Drittanbieterlösungen verwenden, um sicheren Zugriff auf das Intranet für Roaming- oder externe Mitarbeiter bereitzustellen. VPN wird für Lync nicht empfohlen. Lync-Remotedatenverkehr muss die Edgeserver und getrenntes Tunneln verwenden.

DNS-Überlegungen (Domain Name System)

Sie müssen den Satz von DNS-Datensätzen planen, über die sowohl Internet- als auch Intranet-Benutzer DNS-Namen in die entsprechenden IP-Adressen auflösen können.

- Für Internet-basierte Partner und Roaming- oder externe Mitarbeiter bieten DNS-Datensätze, die bei Internet-DNS-Servern registriert sind, eine Auflösung in den Satz öffentlicher IP-Adressen entsprechend dem Gatewayrouter, dem Lync-Edgeserver, dem Satz virtueller IP-Adressen (VIPs) auf dem Lastenausgleich und dem DirectAccess- oder VPN-Gateway, wenn erforderlich.
- Für Intranet-basierte Benutzer bieten DNS-Datensätze, die bei Intranet-DNS-Servern registriert sind, eine Auflösung in den Satz öffentlicher IP-Adressen (VIPs) auf dem Lastenausgleich für Zugriff auf SharePoint, Lync und Exchange-Ressourcen.
- DirectAccess-Clients verwenden Intranet-DNS-Server für Namen, die dem Intranet-DNS-Namespace entsprechen und Internet-DNS-Servern für Namen, die diesem nicht entsprechen. Um das Ausführen von DirectAccess zu vereinfachen, sollten Sie die Verwendung einer geteilten DNS-Implementierung in Betracht ziehen, die unterschiedliche DNS-Namespaces für Intranet- und Internet-basierte Namen verwendet. Verwenden Sie z. B. "contoso.com" für den Internet-Namespace und "corp.contoso.com" für den Intranet-Namespace.
- Exchange verwendet ein geteiltes DNS-Modell, bei dem sich die Auflösung von Host in IP für öffentlich weitergeleiteten Datenverkehr von der im Unternehmensnetzwerk unterscheidet. Sie benötigen mindestens DNS-Datensätze für OWA, AutoErmittlung, ActiveSync-URL für Clientdatenverkehr und einen MX-Datensatz für eingehende E-Mails.
- Wenn Sie Exchange Online Protection (EOP) verwenden, zeigt Ihr MX-Datensatz auf diesen Dienst und nicht auf die Exchange-Farm.
- Für Exchange benötigen Sie einen nachweisbar eigenen TXT-Datensatz in Ihrem öffentlichen DNS, sowie eine Verbundorganisations-ID, um Verbundfreigaben einzurichten.
- VPN-Clients für Remotezugriff können so konfiguriert werden, dass nur Intranet-DNS-Server verwendet werden, wenn die VPN-Verbindung für Remotezugriff aktiv ist.

Legende zum Netzwerkdatenverkehr

- **Lync-SIP-Datenverkehr**
- **Lync-Webdatenverkehr**
- **SharePoint-Clientverkehr**
- **Exchange-Clientverkehr**
- **Exchange-E-Mail-Server-Datenverkehr zwischen lokalem Exchange und Exchange Online Protection**

Der Lync-Edgeserver verwendet die folgenden Ports für die Kommunikation mit externen Benutzern:

- Signalisierung/IM-Datenverkehr (SIP/SIMPLE): TCP-Port 443 [geöffnet für eingehenden Datenverkehr]
- Webkonferenz-Datenverkehr (PSOM): TCP 443 [geöffnet für eingehenden Datenverkehr]
- A/V-Datenverkehr (SRTP): TCP 443, UDP 3478 und TCP 50000-59999 (optional) [geöffnet für eingehenden und ausgehenden Datenverkehr]

Lync-Edgeserver verwendet die folgenden Ports für Verbundkommunikation:

- TCP-Ports 5061 (SIP), 5269 (XMPP), 443 und UDP 3478 (SRTP). [geöffnet für eingehenden und ausgehenden Datenverkehr]

SharePoint kann TCP-Port 443 (SSL) für die verschlüsselte Kommunikation zwischen dem Client und dem Lastenausgleich verwenden. Für externen Zugriff aus dem Internet muss dieser Port für eingehenden und ausgehenden Datenverkehr am Gatewayrouter (oder der externen Firewall) geöffnet sein.

Exchange verwendet TCP-Port 25 (SMTP) für die Kommunikation zwischen Servern. Der Großteil des Clientdatenverkehrs (Outlook Web App, ActiveSync, Autodiscover, Outlook Anywhere) wird über Port 443 (HTTPS) verarbeitet. Wenn Sie POP- oder IMAP-Clients haben, werden auch die Ports 110 (POP3), 995 (verschlüsseltes POP3), 143 (IMAP4), 993 (verschlüsseltes IMAP4) und 587 (SMTP) zur Unterstützung dieser Clients verwendet.

Mehr zu Lync-Netzwerkdatenverkehr?

Erfahren Sie, wie Sie mit Lync Server Chats, Webkonferenzen, Anwendungsfreigabe und Sprachkommunikation in Ihrer Organisation bereitstellen können..

Microsoft Lync Server 2013 Poster zu Protokollarbeitsauslastung en http://aka.ms/G5jzjo

© 2013 Microsoft Corporation. Alle Rechte vorbehalten. Um Feedback zu dieser Dokumentation zu senden, schreiben Sie eine E-Mail an MODAContent@microsoft.com. Letzte Aktualisierung: August 2013.

Microsoft