Progress®
Kemp® LoadMaster®

Technical Note MS Lync 2013 Server Security Guide

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Document Purpose 6

Intended Audience 6

About the Author 6

Chapter 2: Areas of Security Concerns 7

What is Unified Communication? 7

Mediation Server/Gateway 8

Isolated LAN 8

Consolidated LAN 9

Internal Lync Services Segregation 9

Logon Traffic Redirection 10

Internet-Based Access 12

Chapter 3: Security Requirements and Compliance 14

Lync External Facing Security Components 15

Reverse Proxy 15

Edge Server 15

Director Server 17

IIS Server 18

Security Topology 22

Minimal Deployment 23

Highly Secure Deployment 25

Highly Secure Deployment Multi-Pools 27

Chapter 4: Configure the Edge Security Pack (ESP) for Lync 29

Certificate Deployment 31

Rules or Regular Expressions 32

Adding a Virtual Service with ESP 32

Chapter 5: References 37

1

Introduction

Introduction

Microsoft always state the importance of security best practices in Lync environments. Taking this into consideration, the Lync environment is separated into different security areas and layers. It is not only based on Transport Layer Security (TLS) encryption (with certificate service and longer key length), it is well defined in other areas too.

In general, the key areas are:

- Internet-based access
- Logon traffic redirection
- Internal server service segregation
- Mediation server gateway communication

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience
- About the Author

Document Purpose

Document Purpose

The document focuses on the internet directed traffic and communication. This document does not cover other security mechanisms in depth. Also, two-factor authentication is not discussed in this document.

Intended Audience

Intended Audience

This document is intended to be read by anyone who is interested in finding out more about Lync 2013 server security.

About the Author

About the Author

Thomas Poett is a Microsoft MVP (Most Valuable Professional) for Lync. He is a professional, consistent and experienced expect who is technically savvy with over 20 years of experience in IT, telecommunication and software development. He also has extensive experience in business and market development. Thomas specializes in intercultural and business relationships in Asia. He has been very successful in providing leadership on new topics and complex global projects that require interfacing with internal/external teams and ecosystems. Thomas enjoys being an early adopter of visionary technologies.

Thomas can be reached at thomas.poett@live.de.

2

Areas of Security Concerns

Areas of Security Concerns

Refer to the following sections for details about areas of security concerns.

Related Links

For details, see the following topics:

- What is Unified Communication?
- Mediation Server/Gateway
- Internal Lync Services Segregation
- Logon Traffic Redirection
- Internet-Based Access

What is Unified Communication?

What is Unified Communication?

Unified communication includes all communications which could possibly be answered immediately, such as instant messaging, voice/video calls (phone calls) and conferencing, in addition to others such as desktop sharing or active file transfer.

With these communication channels, additional internal and external security is required. With unified communications, sensitive data such as files or shared desktops can be shared.

The sections below discuss four different key areas relating to security.

Mediation Server/Gateway

Mediation Server/Gateway

The Mediation Server component can be installed in two different ways – either consolidated on the Front End Server (being part of the Front End Pool), or installed as the dedicated pool with Mediation Server functionality only. In both scenarios, the audio path between the Mediation Server and Gateway(s) can be secured differently:

- The Mediation Server to Gateway network is dedicated – a physical isolated LAN on separate switches or cables
- The audio traffic is transmitted over the production LAN and TLS encryption is used

Isolated LAN

Isolated LAN

If the Mediation Server component is installed on the Front End Pool and has its own network card, or if the Mediation Server is its own Pool with a dual NIC, we have a dedicated LAN between the Mediation Server and the PSTN Gateway. In other words – a dedicated LAN cable to the PSTN.

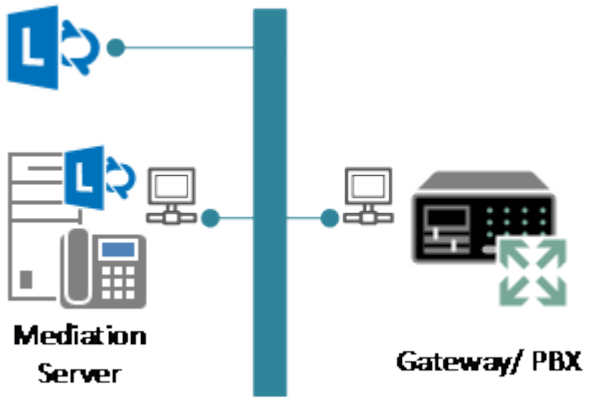


Some restrictions and possibilities related to this setup are outlined below:

As the LAN is isolated and not routed, it is possible to run IP traffic on this dedicated network segment without encryption. This reduces the CPU utilization on both the PSTN gateway and the Mediation Server pool. However, media-bypass is not possible in this configuration.

Consolidated LAN

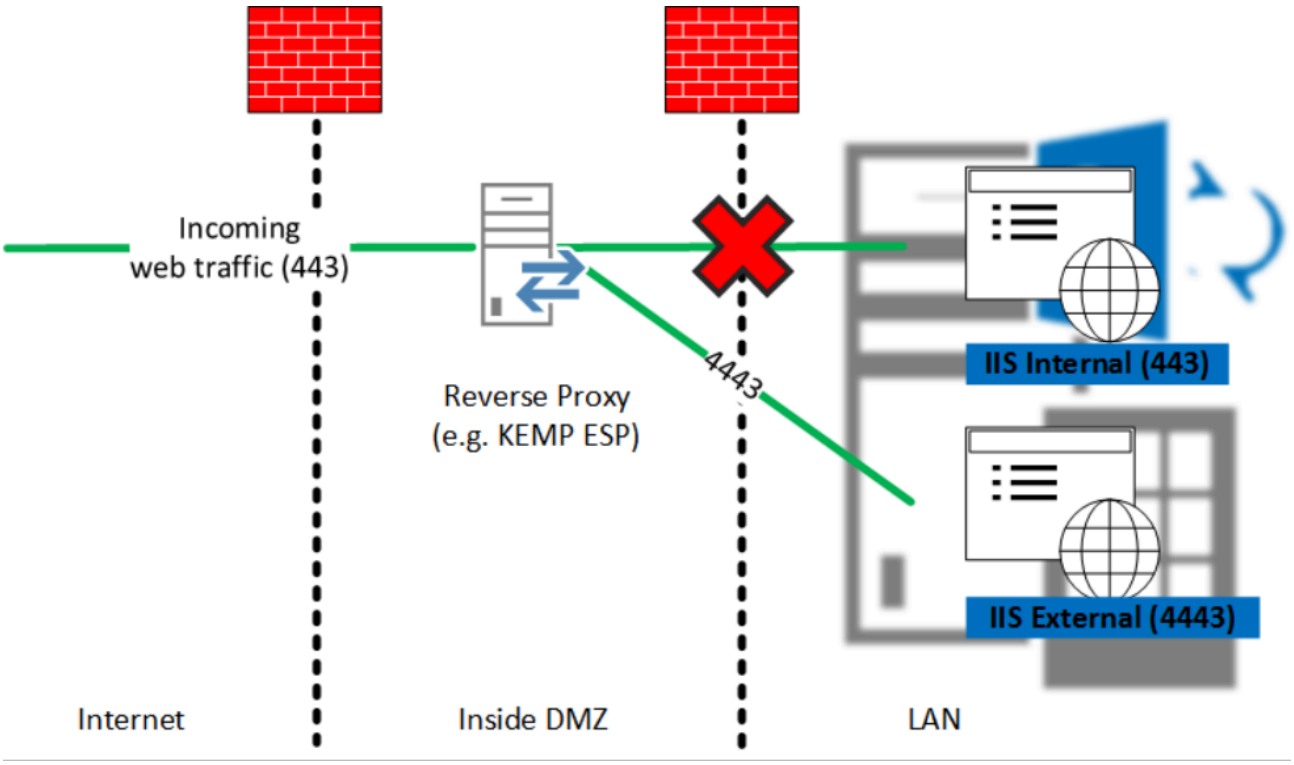
Consolidated LAN



In this topology design, the Mediation Server can be consolidated on the Front End Pool, or can be a dedicated role. Media-bypass is possible. Therefore, audio traffic is routed from/to all possible clients and is fully traceable on the network. TLS security can be required.

Internal Lync Services Segregation

Internal Lync Services Segregation



With this method, both the web and session traffic is encrypted. One obvious question is - if this traffic can reach the Lync servers from external clients, how do we ensure it is legitimate traffic?

The answer to this question is not simple – but since Microsoft improved IIS and security of Windows servers in general over the years, traffic can be segregated based on its origin to different targets, internal and external IIS websites (for example port segregation using 443/4443). Later in this document, we describe how it actually works.

Until the traffic reaches an internal Lync system – either the Director or Front End Server – the web traffic is not authenticated. Authentication must be carried out by the Domain Joined Lync Servers.

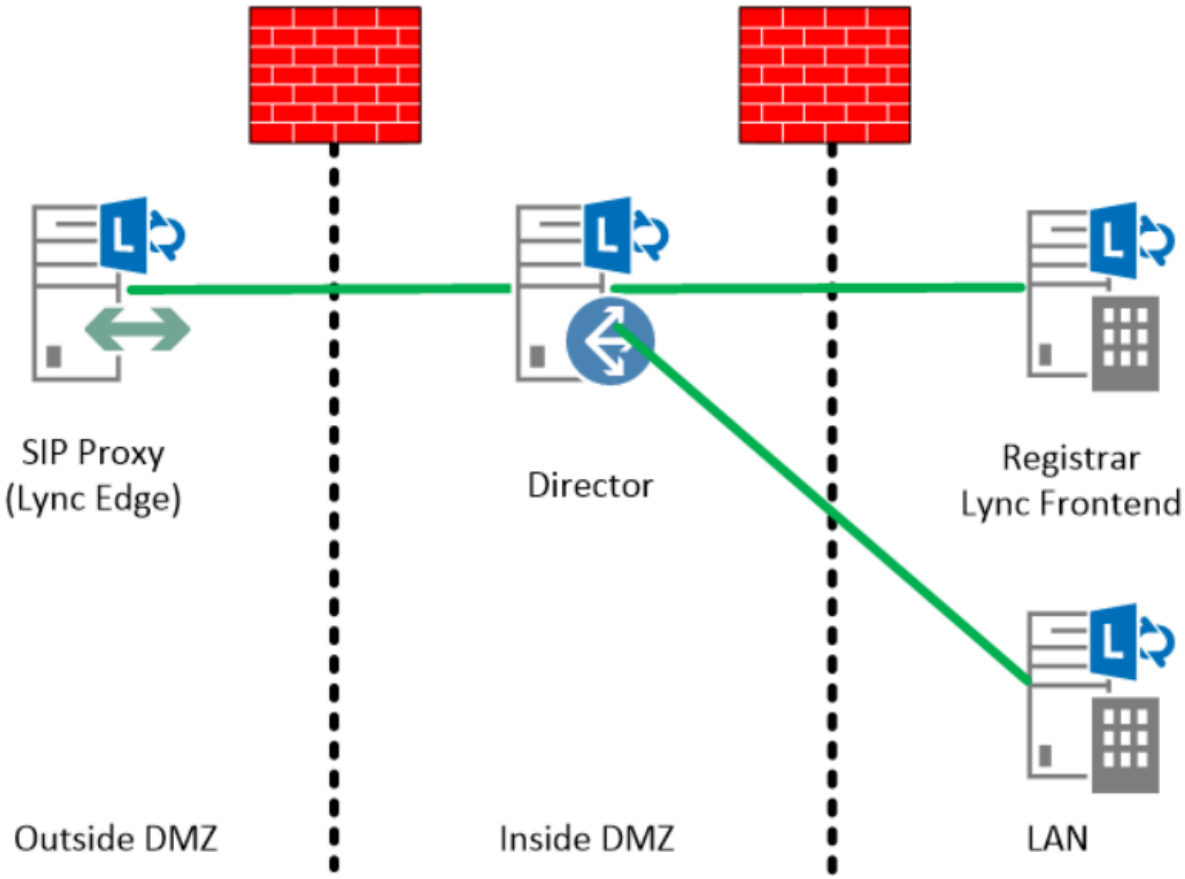
Session Initiation Protocol (SIP) is different to web traffic. Even when initiated from external networks, it will logically be seen as internal traffic. This behaviour is also discussed later in this document.

However, internal phone update and Certificate Revocation List (CRL) traffic cannot be encrypted – it needs to be HTTP rather than HTTPS.

Logon Traffic Redirection

Logon Traffic Redirection

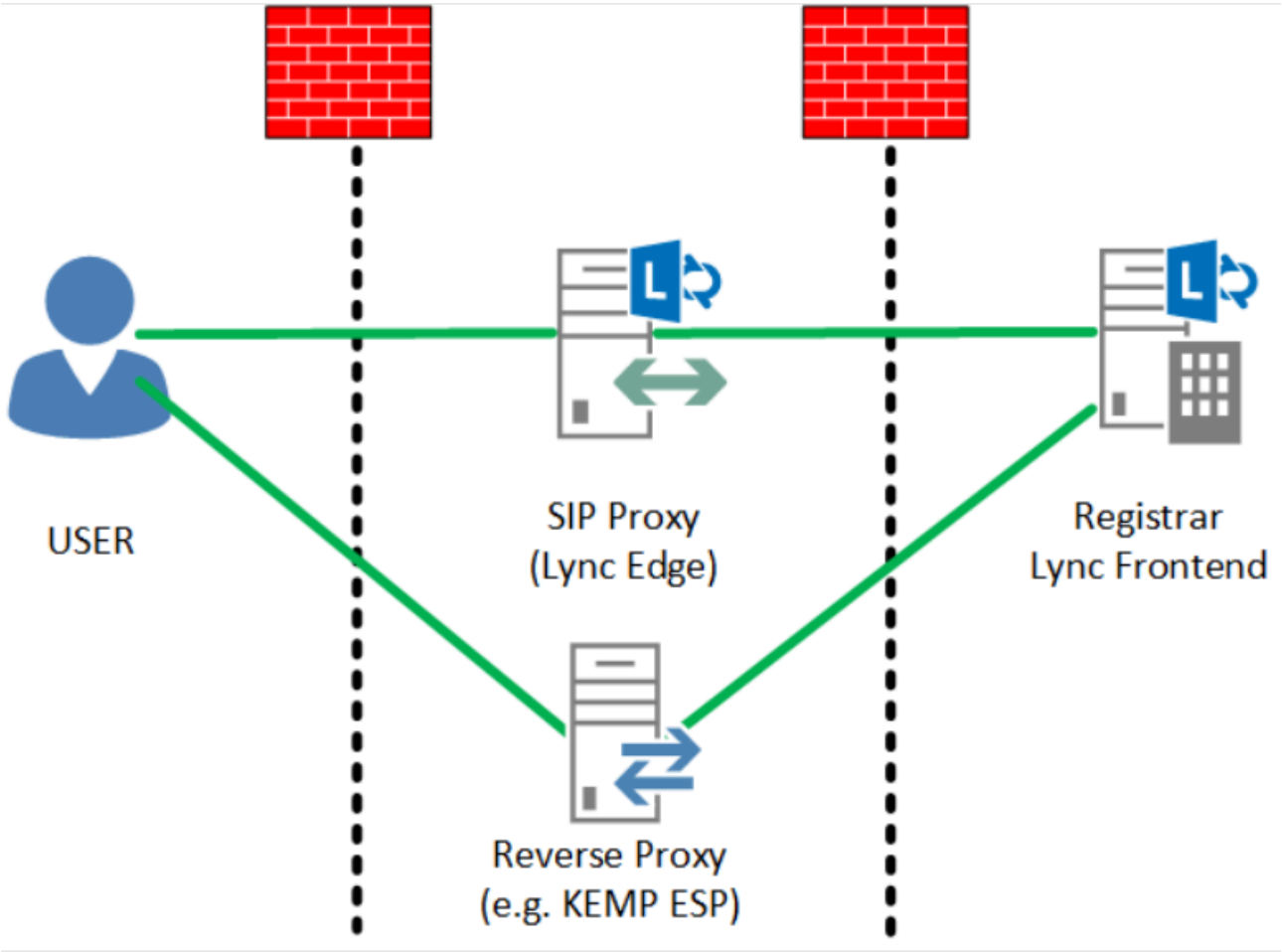
Lync offers support for larger deployments – offering increased security. This feature is supported by the Director Server role. This role is able to authenticate and then redirect incoming traffic to its intended destination.



In a multi-zone security model, it is possible to place the Director Servers in a DMZ which is supposedly in-between the Internet-facing DMZ and the LAN zone. This DMZ can be contacted internally and (indirectly) externally.

Internet-Based Access

Internet-Based Access



This is related to systems directly facing the internet. There must be two systems handling traffic coming from the internet:

- Reverse Proxy
- Lync Edge Server

Regarding the Reverse Proxy component – it is highly recommended to use solutions which are supported, either by Microsoft or the vendor. Microsoft only supports IIS Application Request Routing (ARR)/Wireless Application Protocol (WAP) [1] and Threat Management Gateway (TMG). The Edge Security Pack (ESP) is a non-Microsoft solution which will be discussed later in this document.

The Lync Edge Server is one of the most secure servers. The reverse proxy only handles web traffic – the Edge Server handles all SIP traffic. The Edge Server acts as a real application firewall.

[1]

At time of write this document, Windows Server 2012 R2 Web Application Proxy (WAP) is not supported, due to problems handling Lync deployments with multiple SIP domains.

3

Security Requirements and Compliance

Security Requirements and Compliance

Most customers require a strict traffic segregation and inspection on all traffic coming from and going to the Internet. This traffic must be fully inspected, at least on IP Layer 7. The ISO model describes Layer 7 as the IP application layer, which in our case is HTTP/HTTPS and SIP. In a Unified Communication solution – this is not enough.

Web traffic may be easier to analyse based on Reverse Proxy technologies, but how can SIP traffic be analysed? How can compliance of the policies (which are assigned to the users) be ensured?

Lync is a very sensitive communication system which operates with real time data. Real time data is time sensitive and session-aware. Web traffic also has its own uniqueness. In Lync there are web session tickets which must be kept intact. For example, these tickets ensures that the external client will receive the correct buddy list and not anything from another user.

Related Links

For details, see the following topics:

- Lync External Facing Security Components
- Security Topology

Lync External Facing Security Components

Lync External Facing Security Components

A handful of systems were identified in the Areas of Security Concerns section. There are two components facing the Internet directly and two components which are internal, LAN-based systems.

Reverse Proxy

Reverse Proxy

Reverse proxy is the system which handles the entire incoming HTTP(S) traffic. This incoming HTTP(S) traffic includes data such as address books, web services or distribution group expansion and other, supposed anonymous traffic such as access to dial-in conferences or meetings. User connections to these components are fronted with forms-based access pages. In total, there are three pages offering forms-based authentication; Dial-In, Meet and Scheduler.

Dial-In is the landing page for audio conferences. When a conference is planned and the link has been sent to possible participants, this page is accessed to find dial-in numbers. This webpage is accessible anonymously. However, there is a sign-in option that Lync users which are homed in this system can access to see their own dial-in parameters and preferences.

Meet is the landing page for the Lync Web App. If the page is accessed without a valid conferencing ID, Lync provides an error page. If a correct conference ID has been entered, it will either redirect the connection to a locally-installed Lync client or it will present the meeting login page. A forms-based login page for anonymous users provides only a naming identifier. The second option for Lync system-homed users allows the users to identify themselves with their Active Directory domain credentials.

Scheduler is the meeting planning landing page. If a user does not have the Outlook client installed, including a local Lync client installation, they need this (manually) configured web page to access and plan Lync meeting/conferences. It has a forms-based login page for domain-authenticated users.

Other web services consist of everything else that Lync, Mobil, App Store and Rich clients require. These services can only be accessed by users if they have authenticated themselves again in the Active Directory and if they have a valid session ticket assigned. Further details regarding the IIS components in Lync are discussed later in this document.

Note: Even though there is forms-based authentication, users cannot be pre-authenticated using Reverse Proxy. This is not a supported configuration. Lync-provided forms-based authentication simplifies the deployment – so a simple, but Lync-aware web traffic redirect can be used.

Edge Server

Edge Server

The Edge Server runs a Lync application for three services:

Access Edge Service: This application component is also called Access Proxy. It controls the remote user communication and passes through the authentication. Another feature of this component is the federation to other unified communication solutions, for example Lync or Office Communications Server (OCS), in addition to Public IM Connectivity (PIC) to MSN or Skype. The third component is Extensible Messaging and Presence Protocol (XMPP). Even though this is a dedicated service, it is related to Access Edge. The main purpose of this service is validating SIP connection between users inside and outside of the internal network.

Web Conferencing Edge Service: This is a dedicated service for web conferencing media distribution. The Edge Web Conferencing service proxies the conferencing data stream between the internal Front End Server hosting the conference and the external connected Lync client (rich and mobile).

Note: The Office Web Application Server is required for PowerPoint HTML5 rendering. This is not handled by the conferencing service.

Audio/Video Edge Service: The third core component in Lync Edge is the Audio/Video (A/V) component. This service does not only handle streams containing A/V only – it also proxies application/desktop sharing and file transfer to external users. The A/V Edge Service has two functions – the Audio/Video Edge Service and Audio/Video Authentication Service.

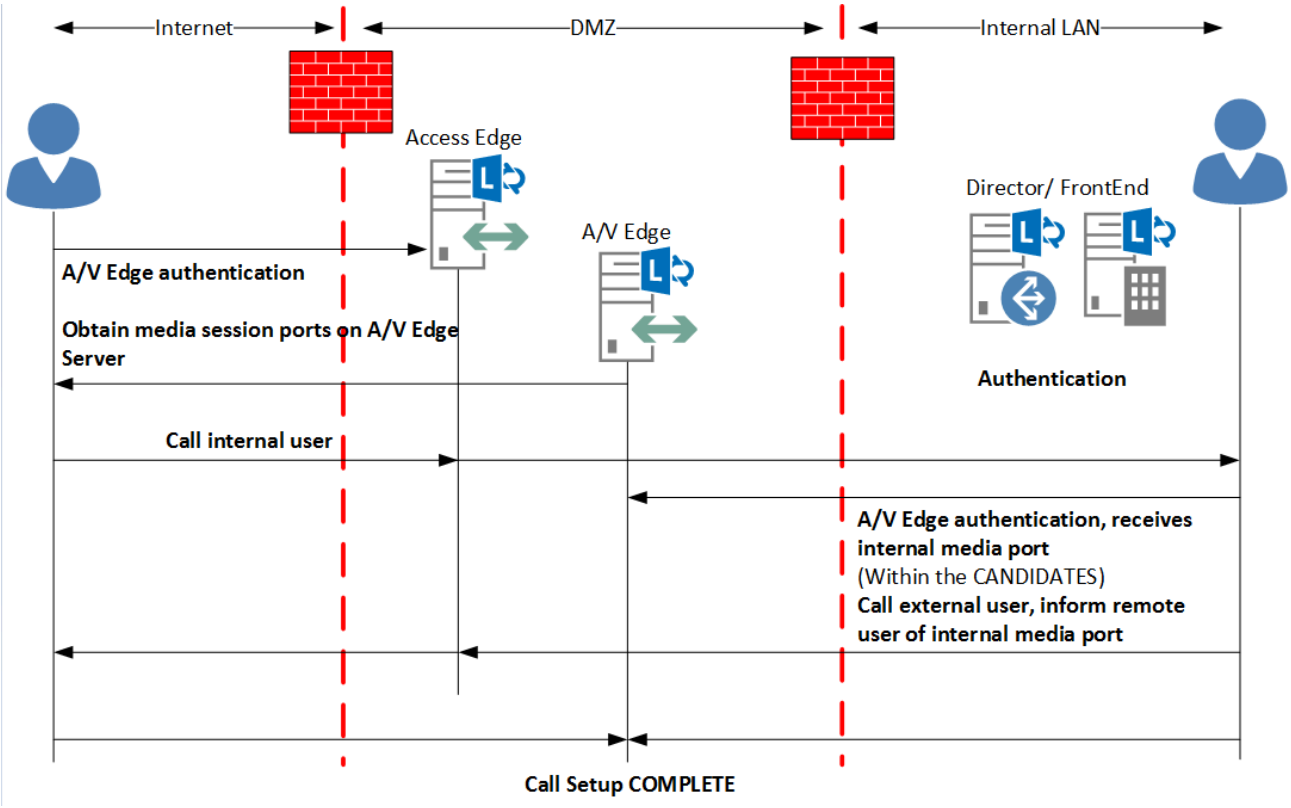
Note: All Edge server traffic must be encrypted using TLS. Public certificates need to be assigned to the Access Edge Service interface and Web Conferencing Edge Services interface. The A/V Edge Service does not need a certificate to be assigned to its interface – the certificate must be assigned to the A/V Authentication Service. The A/V Edge Service does not use the subject name or the Subject Alternative Name (SAN) entries.

Note: The A/V Authentication Service certificate in the Lync Edge Pool must share the same private key. The Edge Services are ignoring the Certificate's Subject Name – therefore, only the SAN names are used and important.

How does Lync Edge for Audio/Video Work?

The Lync A/V Edge Service is the MRAS (Media Relay Access Server) which lets the A/V traffic pass through. The A/V Authentication Service is an internal Lync component related to the internal deployment which authenticates media traffic coming from internal and travelling to external destinations.

Secure Real Time Protocol (SRTP) contains its own security. The SRTP protocol exchanges security keys (a master key which protects the session key) within the SIP protocol first. Further information about SRTP can be found in the related RFC. It is important to understand the Edge Server Service positioning, either the external interfaces or the internal interface.



The Edge Servers require two network interfaces. As the A/V site is segregated into two sites – security must be ensured.

Director Server

Director Server

As seen in the Edge Server section, the Edge Server is segregating SIP traffic but it is not responsible for authentication. There is unauthenticated traffic, for example presence status requests and traffic from remote users, which needs to be authenticated. Authentication can only be handled by a SIP Registrar, which is the Front End Server.

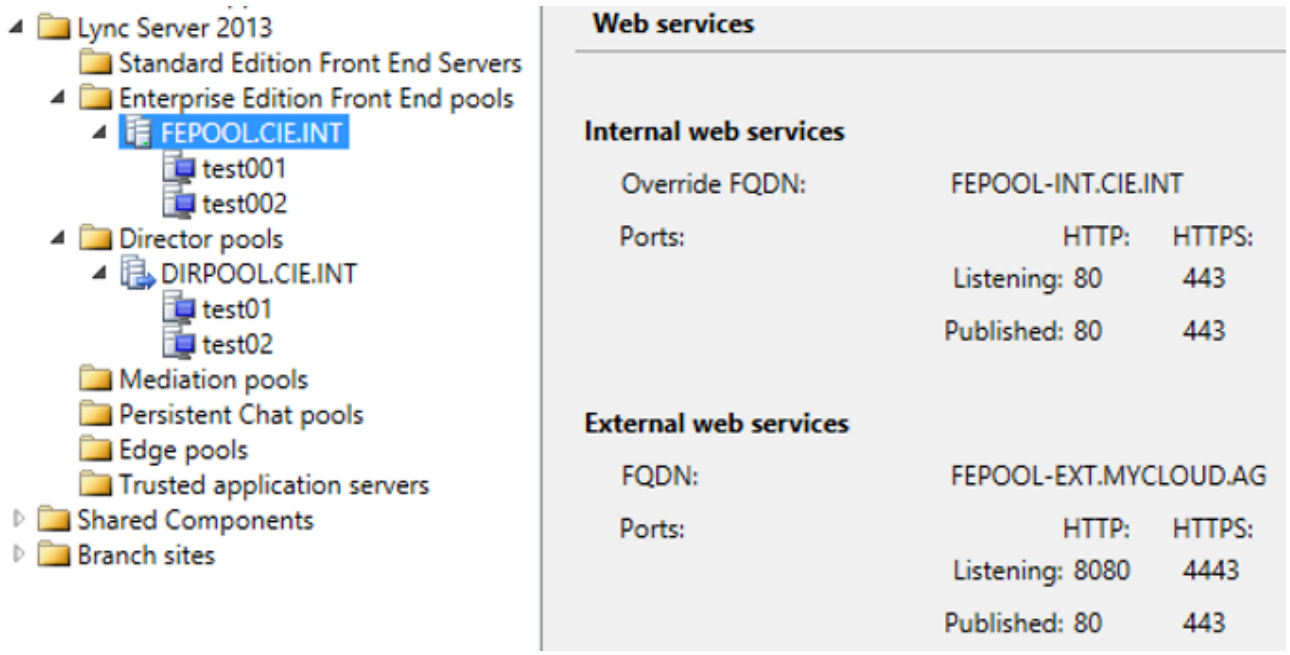
The Director role is another type of proxy server. It knows where a user is homed and can process the authentication. Afterwards, it will pass this authenticated traffic to the user's home pool.

The Director Server can also act as an additional security layer. As this authentication was taken over from the sensitive, data-homing Front End servers – if there is a denial-of-service attack, the attack will not be able to reach the internal Lync Front End servers. If the network is flooded with this invalid external traffic, it will simply be terminated here with no impact to any other internal system.

Note: Every Lync Front End Server has its own web services which need to be published using the Reverse Proxy. These services cannot be redirected via the Director Server.

IIS Server

The essential security part from Lync 2013 is the segregation of web services into internal and external IIS web pages. Therefore, if one service (or the entire web page) is compromised or crashes, the entire system will not run into issues.



Another security opportunity relates to the certificate assignment to the individual websites, along with dedicated Common Name (CN) assignments and separation with different TCP/IP ports.

IIS Web Services Security

The IIS serves several features and functions along with Lync, as listed below:

- Enable users to download files from the Address Book Service
- Enable clients to obtain updates
- Enable conferencing
- Enable users to download meeting content
- Enable users to expand distribution groups
- Enable phone conferencing
- Enable response group features

In addition, the cumulative update for Lync Server 2010: November 2011 installer - http://technet.microsoft.com/en-us/library/hh689988(v=ocs.14).aspx – creates virtual directories in IIS for the following purposes:

- On Front End Servers or Standard Edition Servers: support mobility functionality, such as Instant Messaging (IM) and presence on mobile devices
- On Front End Servers or Standard Edition Servers and on Directors: enable mobile devices to automatically discover mobility resources

In the table below, some of the most common services are addressed and described:

Lync Web Service	Address	Description
Address Book Server	https://<InternalFQDN>/ABS/int/ Handler	Location of Address Book Server downloaded files for internal users
Autodiscover Service	https://<InternalFQDN>/Autodiscover	Location of the Lync Server Autodiscover Service that locates mobility resources for internal mobile users
Client updates	http://<InternalFQDN>/Autodiscover	Location of update files for internal computer-based clients
Conf	http://<InternalFQDN>/AutoUpdate/Int	Location of update files for internal computer-based clients
Device updates	http://<InternalFQDN>/Conf/Int	Location of conferencing resources for internal users
Meeting	http://<InternalFQDN>/etc/place/null	Location of meeting content for internal users
Mobility Service	http://<InternalFQDN>/Mcx	Location of Mobility Service resources for internal mobile device users
Group Expansion and Address Book Web Query Service	http://<InternalFQDN>/ GroupExpansion/int/service.asmx	Location of the Web Service that enables group expansion for internal users. Also, the location of the Address Book Web Query service that provides global address list information to internal Mobile Microsoft Lync 2010 clients.
Phone Conferencing	http://<InternalFQDN>/PhoneConfere ncing/Int	Location of phone conferencing data for internal users

Lync Web Service	Address	Description
Device updates	http://<InternalFQDN>/RequestHandler	Location of the Device Update Web Service Request Handler that enables internal Unified Communication devices to upload logs and check for updates
Response Group application	http://<InternalFQDN>/RgsConfig http://<InternalFQDN>/RgsClients	Location of Response Group Configuration

DNS Mobility Setting for Internal Clients

Mobile users encounter various mobile application scenarios that require special planning. For example, a user might start using a mobile application while not in work by connecting via a 3G network, then switch to the corporate Wi-Fi network when arriving at work, and then switching back to 3G when leaving the building. The environment needs to support such network transitions and guarantee a consistent user experience. This section describes the infrastructure requirements that are needed to support mobile applications and automatic discovery of mobility resources.

Supporting the scenario outlined in the paragraph above can only be accomplished if the client stays connected with a single entity. This entity is the Reverse Proxy, regardless of whether the client is internally connected or connected via 3G/Internet.

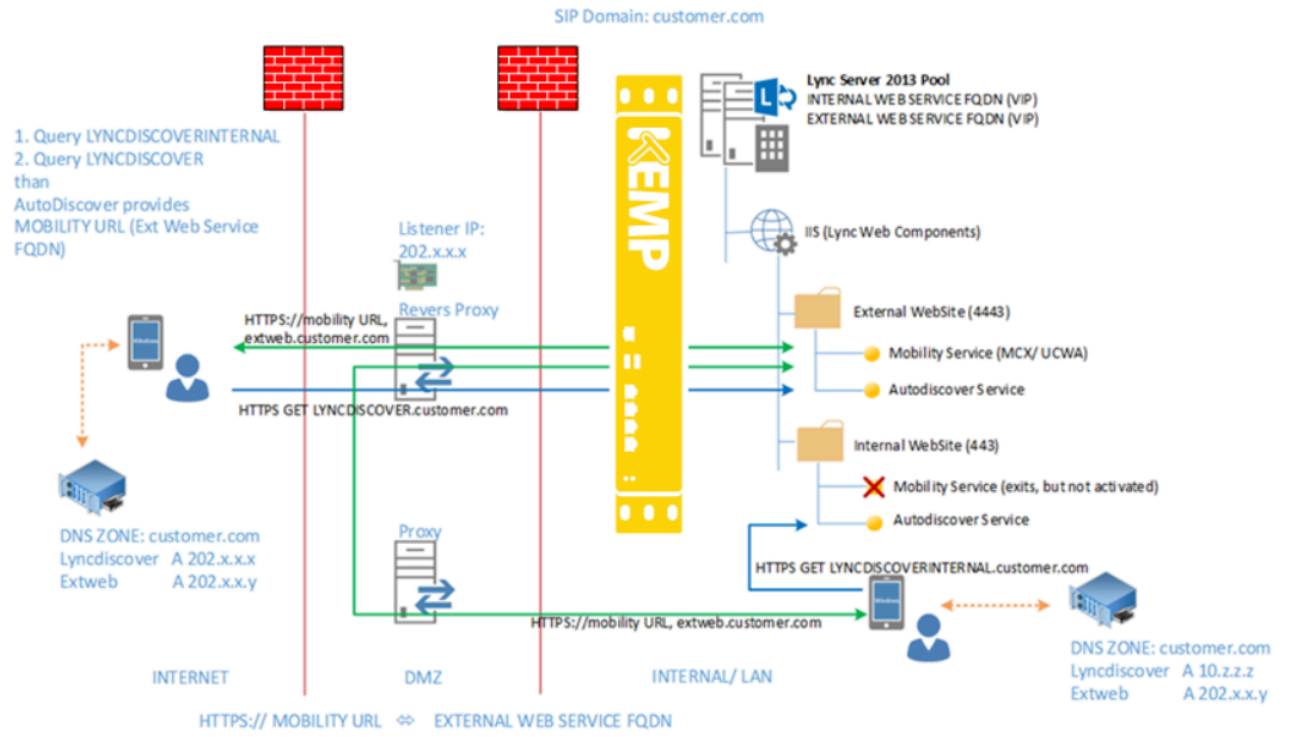
Note: The Discover URL (LYNCDISCOVERYINTERNAL) must point to the Front End Pool Web Service Virtual IP (VIPs) addresses.

Note: The Front End Server Internal Mobility URL must point to the Reverse Proxy external IP address.

Note: The Front End Server External Web Service URL must point to the Reverse Proxy external IP address.

Note: Although mobile applications can also connect to other Lync Server 2013 services, the requirement to send all mobile application web requests to the same external web FQDN applies only to the Lync Server 2013 Mobility Service. Other mobility services do not require this configuration.

Note: However, both the internal Mobility Service URL and the external Mobility Service URL are associated with the external Web Services FQDN.



Note: The internal Web Service (running on port 443) does not offer mobility services, as the diagram above is showing.

Load Balancing Requirements for Web Services

The hardware load balancer requirements for Director and Front End Pool Web Services are listed below:

- For internal Web Service Virtual IPs (VIPs), set source IP address persistence (internal port 80, 443) on the hardware load balancer. For Lync Server 15, source IP address persistence means that multiple connections coming from a single IP address are always sent to one server to maintain the session state.
- Set the TCP idle timeout to 1800 seconds.
- On the firewall between the reverse proxy and the next hop pool's hardware load balancer, create a rule to allow HTTPS traffic on port 4443 from the Reverse Proxy to the hardware load balancer. The hardware load balancer must be configured to listen on ports 80, 443 and 4443.

Summary of Hardware Load Balancer Affinity Requirements

The table below provides a summary of the hardware load balancer affinity requirements:

Client/user location	External web services FQDN affinity requirements	Internal web services FQDN affinity requirements
Lync web access (internal and	None required	Source address affinity

Client/user location	External web services FQDN affinity requirements	Internal web services FQDN affinity requirements
external users) Mobile device (internal and external users)		
Lync web access (external users only) Mobile device (internal and external users)	None required	Source address affinity
Lync web access (internal and external users) Mobile device (not deployed)	None required	Source address affinity

Security Topology

Security Topology

This section describes how to design Lync topologies based on several scenarios. The first question is – can Lync fulfil all of these requirements?

Lync definitely addresses all of these requirements with the Lync Edge server. The Edge server itself acts as a highly secure, real application proxy and is a non-domain joined system with incoming data replication only. The flow of an incoming SIP session is described below.

Arriving at the external Edge Server interface, external traffic is terminated, full application inspection, rights verification and user policy validation is started. After this inspection, the traffic will be sent via the internal network interface to the next network security layer which is the Lync Director Pool or the Front End Pool. In our example, we will assume that this additional security layer (in the form of Director Pool) was integrated.

User authentication requests will only be performed on a Director Pool and this traffic is redirected to the user's destination Front End pool. From there onwards, the traffic is treated as authenticated and a VIA (Path) is established between the Edge Pool, Director Pool, Front End Pool and the internal user client. This information is sent by a NOTIFY SIP command. The same principal is valid if users are homed on Survival Branch Appliances (SBAs).

SIP traffic is simple – SIP has the provisioning for VIA (Path) headers and therefore it is aware of the traffic flow.

The Web Service traffic is referring to the earlier mentioned topic of generic web traffic, for example meet or dial-in, and the web services homed on all Lync, Director and Front End Pools. The traffic flow for these must be taken into consideration.

The Director is not an additional security layer for Pool Web Services. This is where IIS website segregation comes into play.

The next section discusses the minimal deployment with an Edge Server and a Reverse Proxy.

Note: Starting with the initial principals – we will define the incoming protocols. Here we have SIP, Persistent Shared Object Model (PSOM), Session Traversal Utilities for NAT (STUN), RTP and HTTPS. HTTP is not relevant because, during the next topology definition, all unencrypted traffic will not be allowed. Additionally, in order to make the diagram below easier to understand – all Edge Server-relevant protocols have been consolidated in the word SIP.

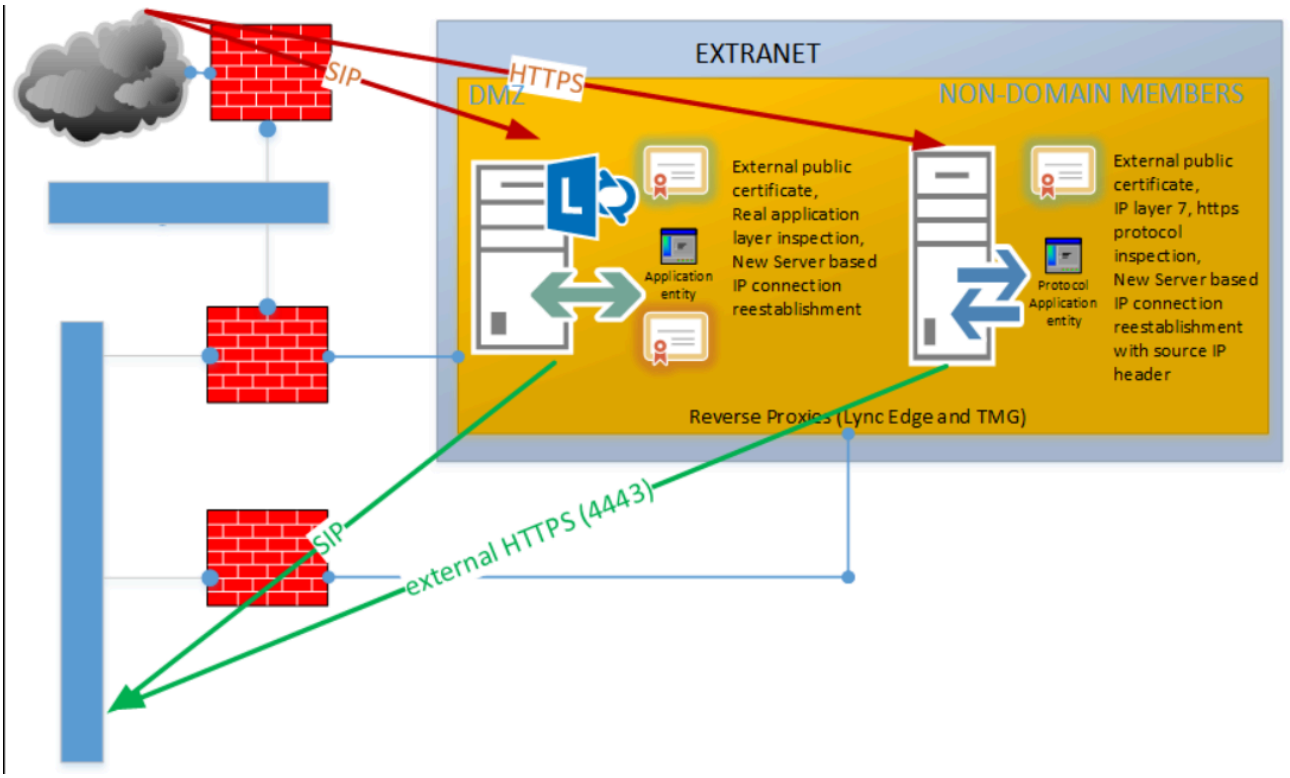
High Availability (HA) is not addressed in this document. Moreover, HA runs the Lync server in pools and initiates either Hardware Load Balancing (HLB) or a mixture of HLB and DNS load balancing.

Additionally, XMPP traffic cannot be directed via the Director Server – it is always a Front End – Edge communication.

Minimal Deployment

Minimal Deployment

Certificates are very important. Correct public certificates must be implemented on the Edge and the Reverse Proxy. The Edge Server additionally requires an internal certificate. This ensures the correct proxying, or better said the application firewall functionality. The Reverse Proxy also needs a public certificate and must be able to recognize the internal web services-assigned certificates. The correct infrastructure is needed to ensure the HTTPS and TLS traffic will work.



The minimal deployment consists of a single Lync Edge Server and a Reverse Proxy Solution as illustrated above.

Based on the DNS entries, the clients are enabled by accessing the associated component – the Edge or Reverse Proxy. The Reverse Proxy listens on TCP port 443 and simply redirects the traffic to the internal IIS server on TCP port 4443, while it inspects the HTTPS stream, repacks and re-encrypts the traffic with the certificate assigned to the external web service web site.

The Lync Edge server acts slightly differently. It still needs a valid public certificate so that the incoming, as well as the outgoing stream, can be decrypted. Clients or other Edge Servers need a certificate validation check before accepting TLS traffic encryption. The paragraphs below discuss how Lync handles this traffic.

For example, say that Lync has an incoming SIP request. The external client will contact the Access Edge, which then terminates the SIP connection on its external Access component. Next, the request is processed and the intent is validated. Assuming that it is a user authentication, the Edge server then initiates an outgoing session on its internal Access component, contacting the next hop which was defined in the Lync topology. If anything within this traffic does not match the Lync-specific traffic, for example if there are malformed packages, the Edge Server does not process the request. The Edge Server is a fixed component in this communication path. With the VIA parameter, internal and external (NAT) IP addresses can be seen.

Refer to the example below:

```
NOTIFY sip:172.28.91.102:63811;transport=tls;ms-opaque=4dc4459e44;ms-received-cid=41200;grid SIP/2.0
Via: SIP/2.0/TLS 172.28.11.222:5061;branch=z9hG4bKDFF54A39.668DC7A3C12F3034;branched=FALSE;ms-internal-
info="dg5Sh_HOLBeQIuW7aeLZXi-777RKXsH7J-Tz2_z9ka-12jx41mS2QnCAAA"
Via: SIP/2.0/TLS 172.19.13.12:55199;branch=z9hG4bKFF9150B3.158D61B2772D5034;branched=FALSE;ms-received-port=55199;ms-received-cid=35300
Via: SIP/2.0/TLS 172.19.45.67:60863;branch=z9hG4bK164F279A.0E2D7C239BB43033;branched=FALSE;ms-received-port=60863;ms-received-cid=5114F00
Via: SIP/2.0/TLS 10.11.10.84:56466;branch=z9hG4bKD73FF1C6.2C025539A8D9502C;branched=FALSE;ms-internal-
info="dkA2Nw9fhg7tfCPrevW7pFbiqu6LYV50XwzhmIoHvEKk45VQlsNq4BswAA";received=[redacted];ms-received-port=56466;ms-received-cid=100DD100
Via: SIP/2.0/TLS 10.10.10.128:62091;branch=z9hG4bK194A858B.6F070ABFD3B06035;branched=FALSE;ms-received-port=62091;ms-received-cid=27BB00
```

The example above shows the path from client 172.28.91.102 until 10.11.10.84, which is the NATed Access

IP of an Edge Server, including the external IP (which is blanked out in the screenshot above). 10.10.10.128 is the internal Front End server. The NOTIFY commands were received by the local client (172.28.91.102). The second Edge Server that is involved is 172.19.45.67, without a public IP address. This is because the log was collected on a Lync client in the internal LAN connecting the internal Edge Access interface and does not need to know any public associated IP addresses.

Two Edge Servers are involved. A SIP Proxy should look like another hop in the communication path. The Lync topology on both environments provides the Edge server with the necessary information relating to where the incoming SIP traffic should be routed first.

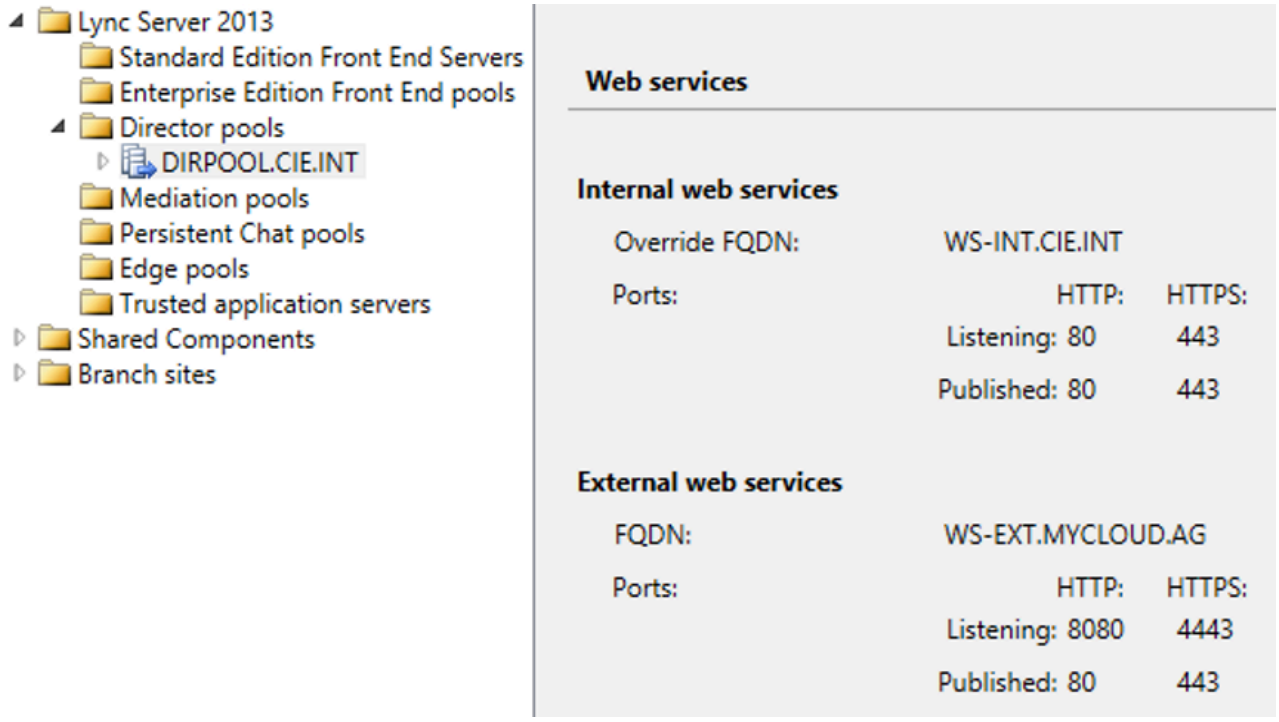
As the topology information is only replicated one way, and the Edge Server should be based on Microsoft best practice (meaning DNS should also only be configured on the external NIC and internally, the HOSTS file should be used) this scenario is considered as safe. Even if the Edge Server is compromised – no internal network information can be acquired.

Highly Secure Deployment

Highly Secure Deployment

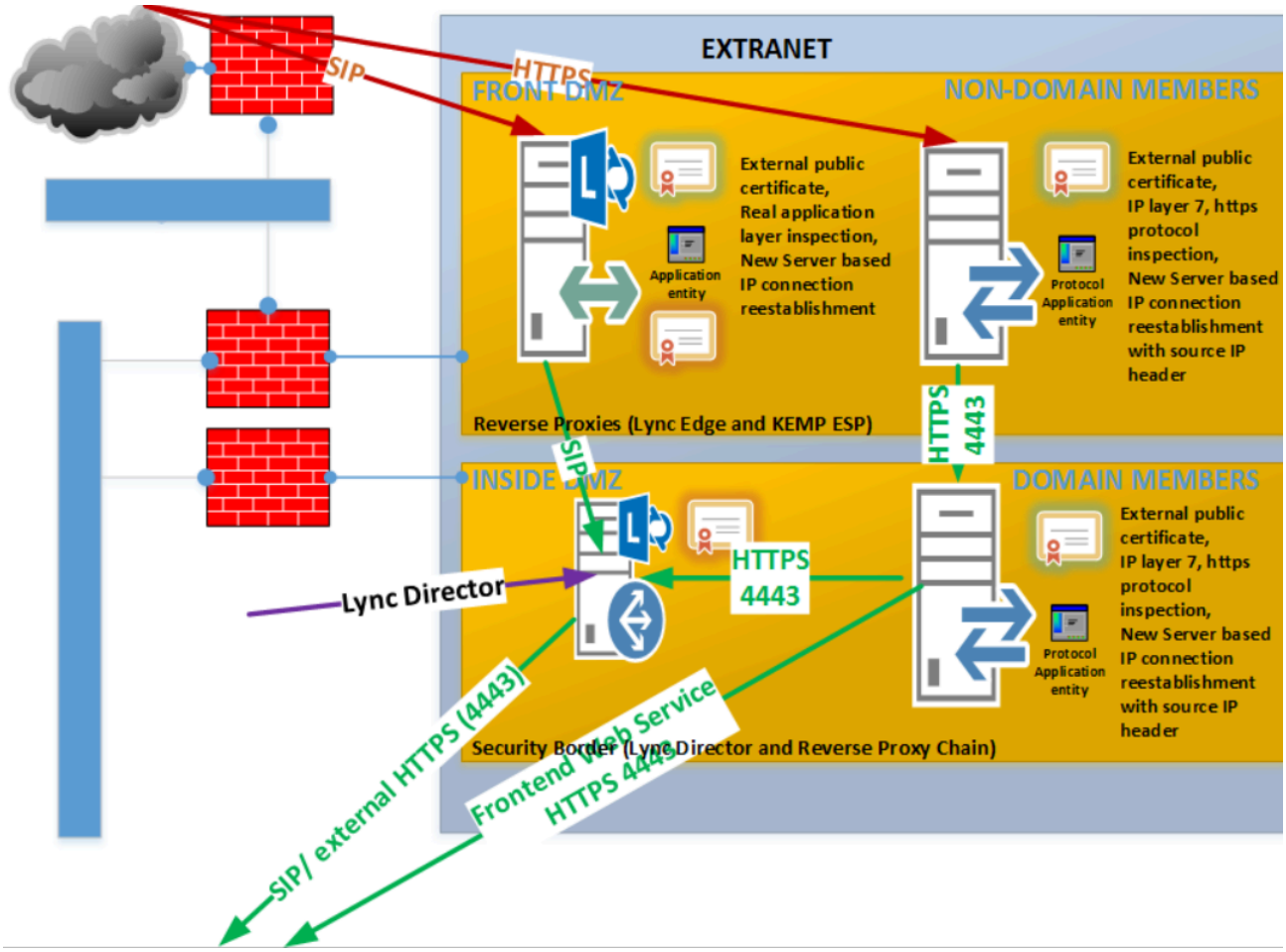
In a secure environment, Director Servers are recommended. They are the target for almost all Internet-related traffic, with a single exception – Front End Server Web Services traffic. This is acceptable due to the face that this traffic is only established once the initial SIP authentication is processed.

Web-based traffic does not require any authentication because Meet and Dial-In will be redirected to the Director Servers and therefore the security model becomes valid.



Note: If this security model is applied, please be aware that all internal DNS targets will have to point to this Director Pool too.

To separate this traffic, simply apply a second Director Pool and make this the preferred target for internal consolidated access. The DMZ-based Director Pool will then be the target defined in the Edge Server NEXT HOP parameter.



The diagram above offers a solution where the “INSIDE DMZ” zone is treated as the second defence zone and is allowed to be accessed from internal clients too. Beside the introduced Director Pool, there is a Reverse Proxy chain. A chain is when at least two Proxy Servers are configured in a row and depend on each other.

All external Web Services are published with a listener on the first, Internet-facing Reverse Proxy server. This points from there towards its chain member (the second Reverse Proxy) which then directs all requests to the designated destinations.

As described earlier, the Edge Server works in this scenario. The Edge Server acts as the NEXT HOP configuration point towards the Director Server. It is implemented as an additional security layer.

The Director now handles SIP and Web Service traffic and builds another line of defence.

Note: The Lync Mobility design is probably the most difficult of all designs. As defined in the prerequisites, the clients need access to the same Reverse Proxy entry point for internal (WLAN) and external (3G). Implementing this with a chained proxy can be difficult. How the internal WLAN client can establish those required connections should be discussed with your internal security officers.

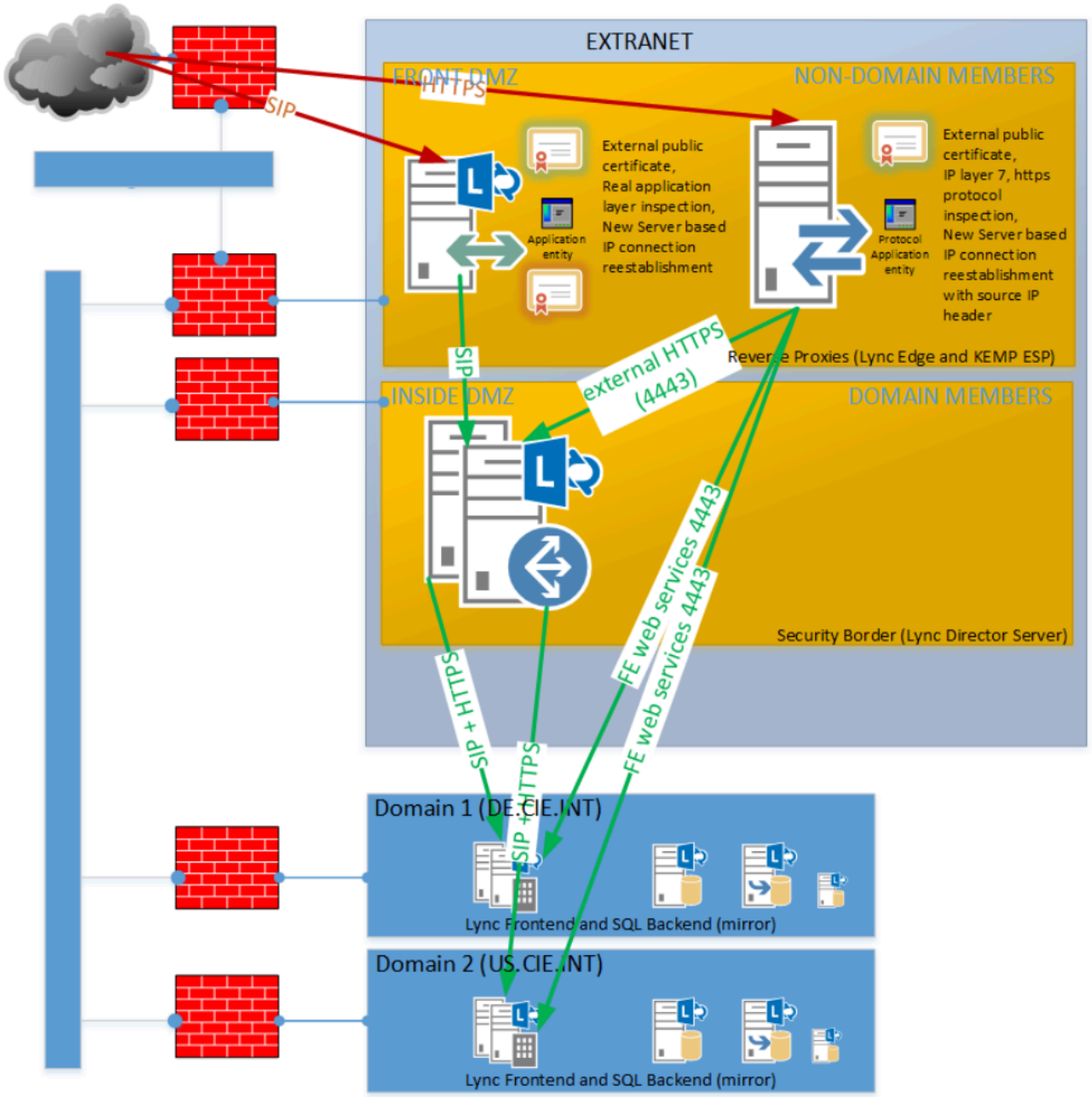
Highly Secure Deployment Multi-Pools

Highly Secure Deployment Multi-Pools

In this section, a highly secure and complex design will be discussed. In this scenario there is an Active Directory Forest with three domains; the Forest Root Domain (CIE.INT) and two sub-level domains (DE and US). Each domain contains Lync Server components and there are Administrators separated for each security area (this is not shown in the diagram).

The four security areas are:

- FO zone – the Internet-facing zone without domain members
- MO zone – a DMZ which contains the second defends line of Director Servers as Root domain Members
- Domain 1 as a user and resources domain
- Domain 2 as a user and resources domain



This is a real life scenario which was principally designed for a defense corporation with more than 8 domains, with highly secure backbone technologies, full administrative isolations and more requirement considerations.

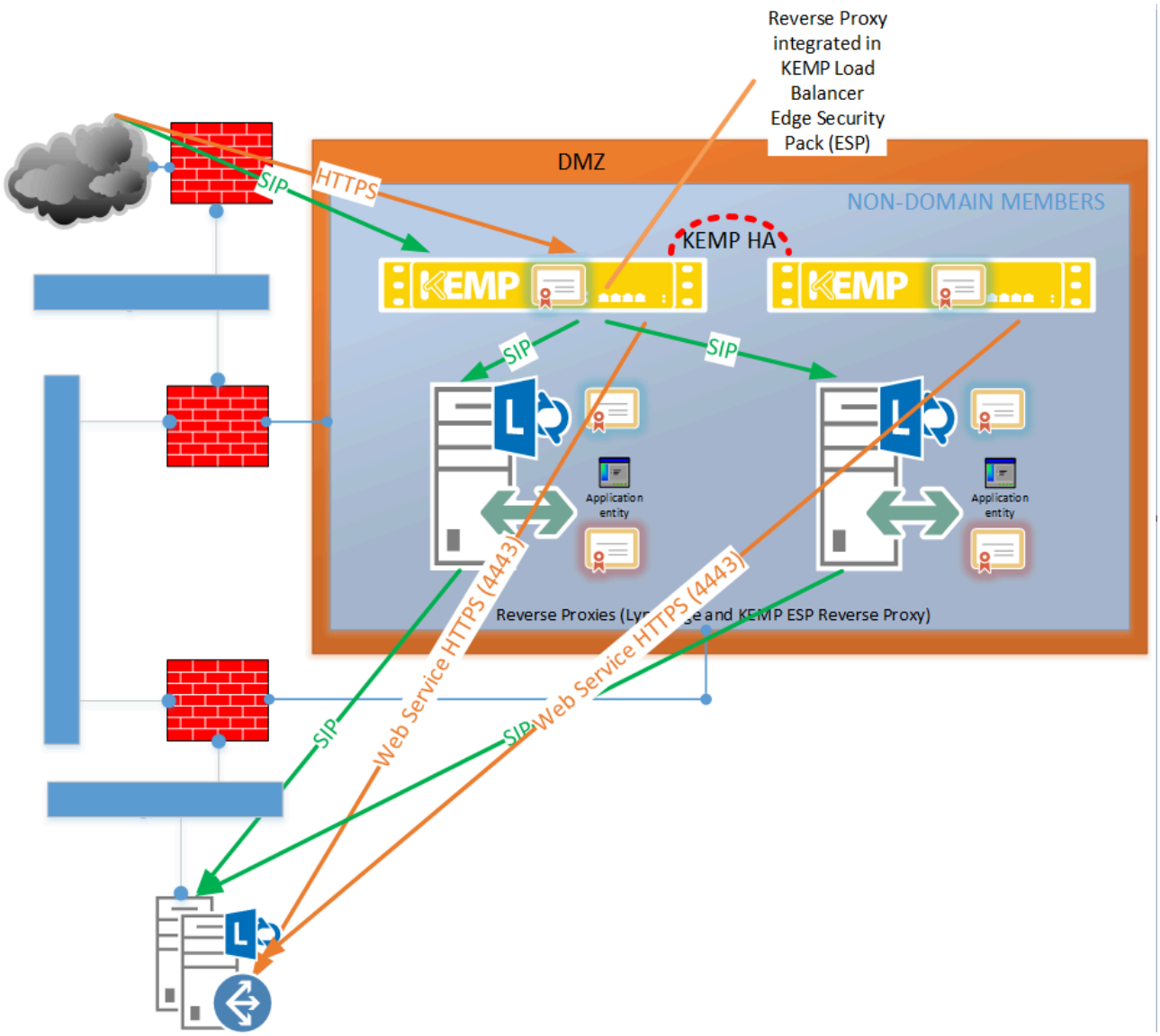
4

Configure the Edge Security Pack (ESP) for Lync

Configure the Edge Security Pack (ESP) for Lync

This section provides guidance on how to configure a Reverse Proxy solution.

In most cases, Lync is run in a High Availability (HA) configuration as a critical application. Therefore, use of a virtual or physical load balancer is required. The Virtual LoadMaster and hardware LoadMaster systems both provide a supported Reverse Proxy solution.



First, the necessary Lync Web Service information needs to be gathered, for example:

Address (FQDN and Listener IP)	Listener IP	Internal IP	Description
WS-EXT.MYCLOUD.AG	10.154.11.5		Lync external Web Service FQDN **Director Pool**
FEPOOL-EXT.MYCLOUD.AG	10.154.11.6	10.154.201.2 10.154.201.3	Lync external Web Service FQDN **Front End Pool**

Address (FQDN and Listener IP)	Listener IP	Internal IP	Description
LYNCDISCOVER.MYCLOUD.AG	10.154.11.5	10.154.201.2 10.154.201.3	Lync Mobility Services **Director Pool**
MEET.MYCLOUD.AG	10.154.11.5	10.154.201.2 10.154.201.3	Web Conferencing Landing Page **Director Pool**
DIALIN.MYCLOUD.AG	10.154.11.5	10.154.201.2 10.154.201.3	Dial-In Information Landing Page **Director Pool**
SCHEDULER.MYCLOUD.AG	10.154.11.5	10.154.201.2 10.154.201.3	Web Scheduler for Lync Conferences **Director Pool**

This example will demonstrate the Direct Setup only. All other services follow the same principles.

Related Links

For details, see the following topics:

- Certificate Deployment
- Rules or Regular Expressions
- Adding a Virtual Service with ESP

Certificate Deployment

Certificate Deployment

The service should not be transparent with ESP enabled. Therefore, a valid public certificate needs to be assigned to the Virtual Service.

For step-by-step instructions on how to import a certificate, refer to the SSL Accelerated Services, Feature Description.

Rules or Regular Expressions

Rules or Regular Expressions

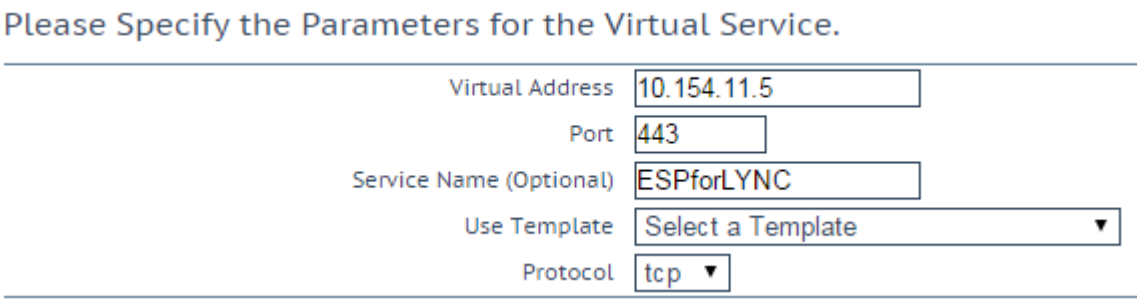
With Exchange publishing, there is a defined subset of rules. Generally, this is not necessary for Lync due to built-in security measures.

Adding a Virtual Service with ESP

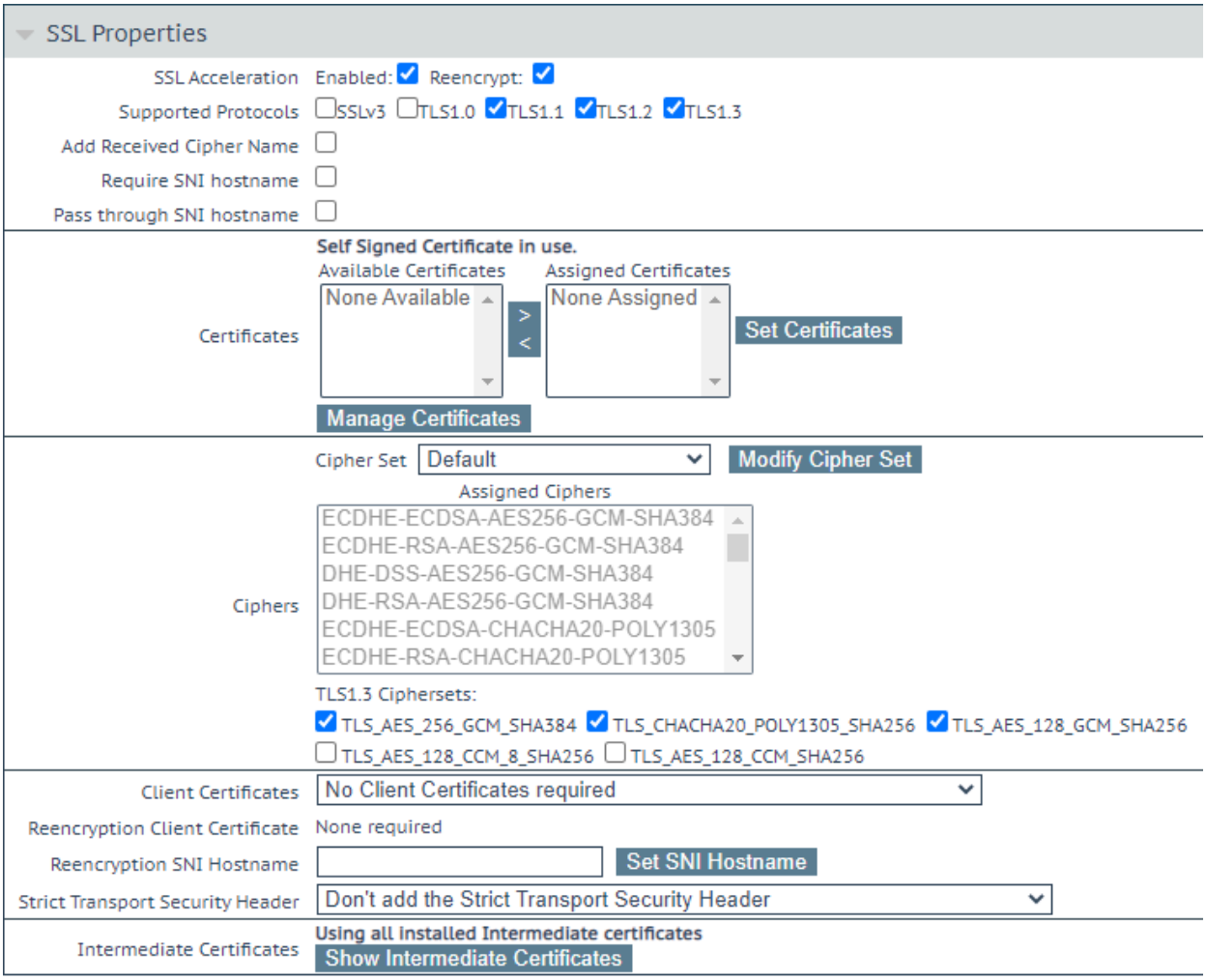
Adding a Virtual Service with ESP

At this point, the prerequisites should have been fulfilled and we can continue with the Reverse Proxy setup. This setup is similar to the setup for the Lync Internal Web Services.

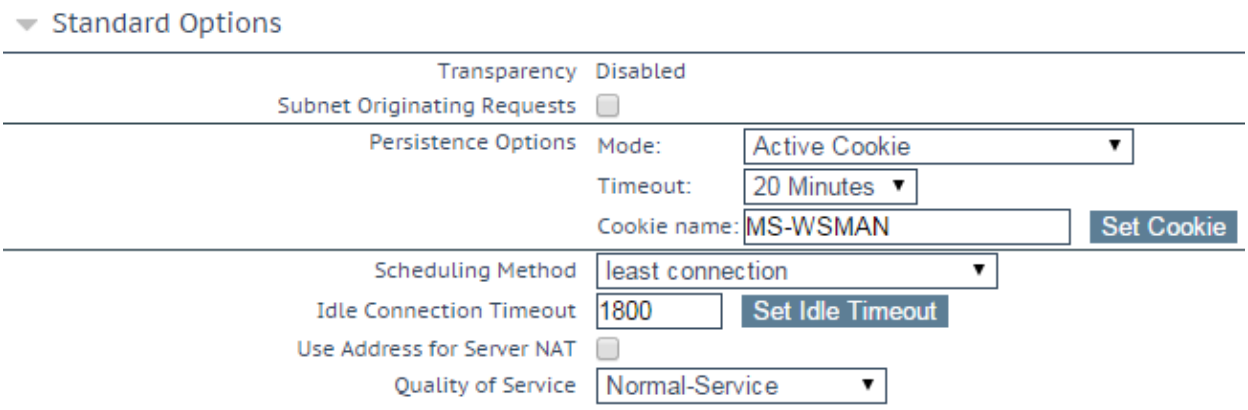
To configure the Virtual Service, follow the steps below:



1. Enter a valid **Virtual Address**. In our example, this is the NATed IP listener in the DMZ: **10.154.11.5**.
2. Enter **443** (HTTPS) as the **Port**.
3. Enter a recognizable **Service Name**, such as **ESPforLYNC**.
4. Click **Add this Virtual Service**.
5. Expand the **SSL Properties** section.



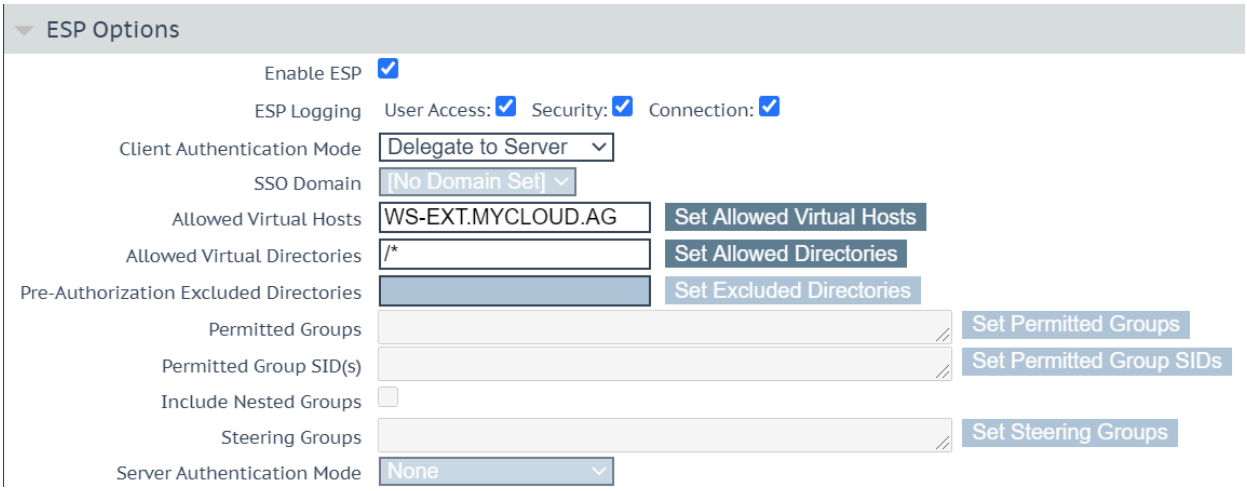
6. Select **Enabled**.
7. Click **OK**.
8. Select **Reencrypt**.
9. Select the relevant certificate in the **Available Certificates** box.
10. Click the right arrow to move the certificate to the **Assigned Certificates** box.
11. Click **Set Certificates**.
12. Expand the **Standard Options** section.



13. Set the **Persistence Options** as needed.

Note: In Lync 2013, cookie persistence is now optional. If you choose to use cookie persistence, set the parameters as follows: - Mode: **Active Cookie** - Cookie name: **MS-WSMAN**Alternatively, **Source IP Address** persistence can be used.

14. Set the **Timeout to 20 Minutes**.
15. Set the **Scheduling Method** to **least connection**.
16. Enter **1800** in the **Idle Connection Timeout** text box and click **Set Idle Timeout**.
17. Expand the **ESP Options** section.



18. Select **Enable**.

Note: The ESP options are what makes the LoadMaster act as a Reverse Proxy.

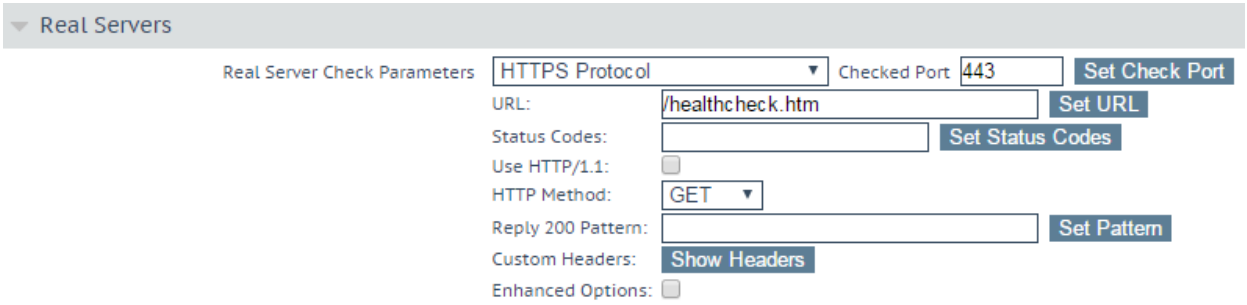
19. Ensure that each of the **ESP Logging** options are selected.

Note: As this acts as a security layer in-between, we recommend enabling all logging options for analysis.

20. Do not select an **SSO Domain**.

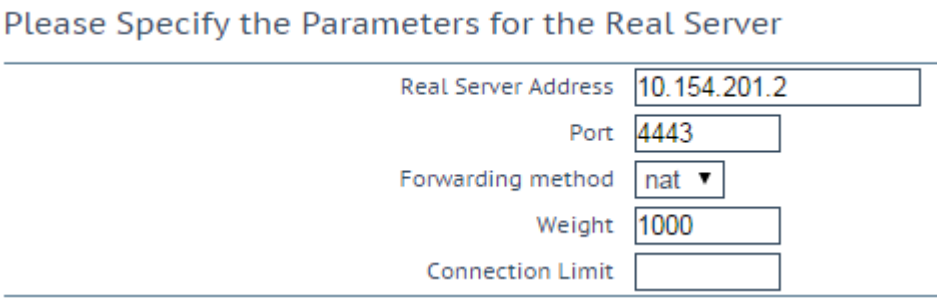
Note: An SSO domain should not be set because Lync does not support pre-authentication.

21. Enter the **Allowed Virtual Hosts**:
    - WS-EXT.MYCLOUD.AG
    - MEET.MYCLOUD.AG
    - DIALIN.MYCLOUD.AG
    - SCHEDULER.MYCLOUD.AG
    - LYNCDISCOVER.MYCLOUD.AG
22. Click Set Allowed Virtual Hosts.
23. Enter **/*** in the **Allowed Virtual Directories** text box.
24. Click **Set Allowed Directories**.
25. Expand the **Real Servers** section.



Note: The LoadMaster requires information on what it can check to see if the defined server/service is up and running. You can either copy your own HTML file on the external web service (IIS) or you can use a Lync defined path, for example /abs/handler.

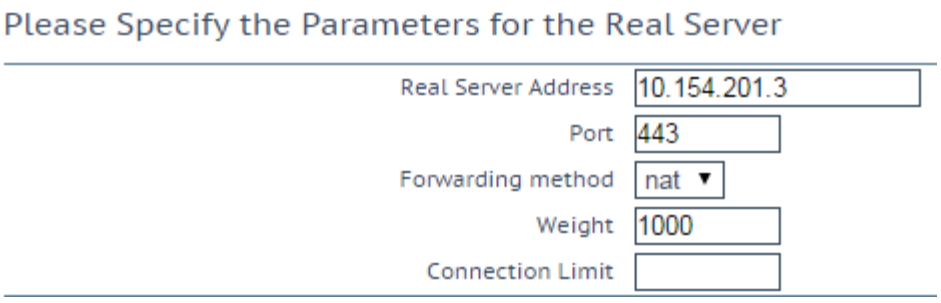
26. Enter **443** in the **Checked Port** text box.
27. Click **Set Check Port**.
28. Enter **/healthcheck.html** in the **URL** text box and click **Set URL**.
29. Click **Add New**.



30. Enter the **Real Server Address**.
31. Enter **4443** as the **Port**.

Note: The Reverse Proxy needs to address the correct internal IIS web page on the assigned port **4443**. This should be set the same for each Real Server.

32. Click **OK**.



33. Add the second Real Server.
34. Click **Back**.

Note: The Real Server details will be displayed at the bottom of the Virtual Service modify screen.

Id	IP Address	Port	Forwarding method
7	10.154.201.3	443	nat
6	10.154.201.2	4443	nat

35. Click the **View/Modify Services** link in the main menu.

Status	Real Servers	Operation
Up	10.154.201.2 10.154.201.3	Modify Delete

The Virtual Services will be displayed. The **Status** should be **Up**.

5

References

References

Some useful links are as follows:

MS Lync 2013, Deployment Guide

SSL Accelerated Services, Feature Description

Web User Interface, Configuration Guide

Thomas Poett's Blogs:

- http://lyncuc.blogspot.de/2014/04/internal-certificate-deployment-in-lync.html
- http://lyncuc.blogspot.de/2014/02/demystify-hlb-and-dns-load-balancing.html

TechNet article on Edge Server certificate planning:

http://technet.microsoft.com/en-us/library/gg413010.aspx

TechNet article on Edge Server certificate requirements:

http://technet.microsoft.com/en-us/library/gg398920.aspx

Lync 2013 LoadMaster Templates:

https://support.kemptechnologies.com/hc/en-us/sections/200428856