Configure and Troubleshoot DNS and Certificate Requirements on Microsoft Federation via Expressway to Cisco Meeting Server

Contents

Introduction

This document describes the DNS and certificate requirements of Microsoft Lync/Skype for Business for a federation between different domains over the Internet.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Expressway
- CMS (Cisco Meeting Server)
- Microsoft Lync or Skype for Business server
- CUCM (Cisco Unified Communications Manager)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Expressway X8.9 or later
- Cisco Meeting Server (CMS) 2.1.2 or later
- Microsoft Lync 2010 server, Lync 2013 server or Skype for Business server - on-prem or hosted in the cloud (Office365)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

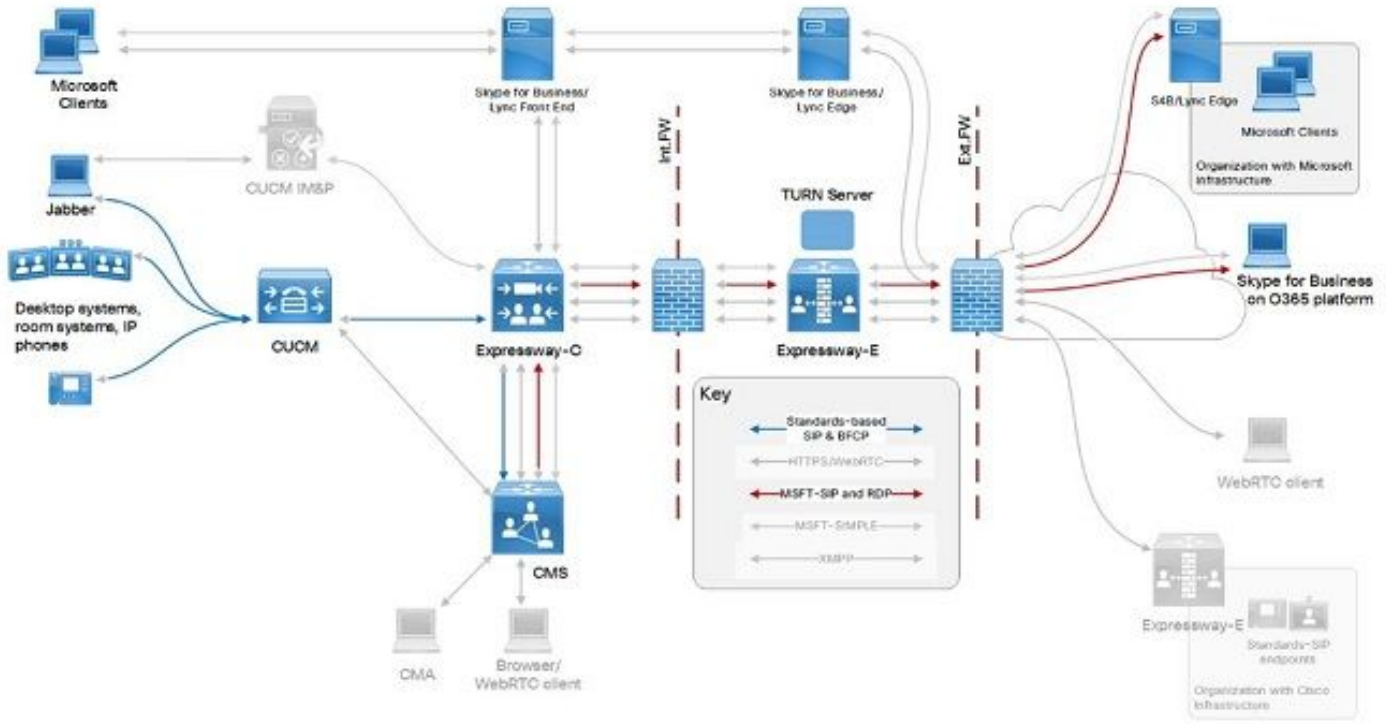
The document highlights a specific aspect of the integration with external Microsoft clients with your Cisco infrastructure using Expressway and Cisco Meeting Server (CMS). The configuration for this integration is as explained in the **Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure** documentation which is available for your version at the Cisco Expressway Series Configuration guides list.

The current document only focusses on the DNS and certificate requirements on the Microsoft Lync or Skype for Business end for external federation. The other configurations are covered in the above referenced configuration guide.

Configure

An example for the call flow and its configuration can be a CUCM registered endpoint which dials to a Skype client (either on-prem or off-prem, or registered in the Cloud using Office365), or vice versa - using the CMS for the conversion between Standard SIP and Microsoft protocol. This is possible through the integration and call routing using Expressway servers, as shown in the image below, which is taken from the **Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure configuration guide** referenced at the end of this document.

Network Diagram



Note: This is just an exemplary call flow scenario. Other call scenarios are also possible.

DNS

Microsoft Lync/Skype for Business uses the **_sipfederationtls._tcp.<domain>** SRV record in order to discover the external federation servers to which to send out the calls to (as well as presence information); or for the call-back functionality based on the domain which is specified in the **From/P-Asserted-Identity header** of the incoming **SIP INVITE**. In this scenario, the DNS records must be available at the public DNS for both domains in order to federate between each other.

The domain portion of the **FQDN** (Fully Qualified Domain Name) which is returned by the SRV record lookup for the domain must match exactly (no other domains or subdomains are allowed). The following table shows an example for DNS configuration for domain with name **example.com**:

SRV record	_sipfederationtls._tcp.example.com	expe.example.com
A record	expe.example.com	IP address of Expressway-E

Caution: The A record which the SRV resolves to, must be an exact match on the configured domain. Subdomains (for example expe.sub.example.com) or different domains (expe.dummy.com) will not be trusted by Microsoft Lync/Skype for Business and this will result in call failures even though they may have appropriate A records and resolve to correct IPs.

Certificate

Microsoft Lync/Skype for Business sets up a TLS connection between the domains configured on the Lync and Expressway sides.Microsoft Lync/Skype for Business has the following server

certificates requirements for the federation and the servers it is communicating with (Expressway-E in this document):

- The server certificate presented by the server matching the A record must have that particular **FQDN** contained in its **Subject Alternative Name** (or **Common Name**, if not using SAN)
- The server certificate presented by the server needs to be trusted by the Microsoft Lync/Skype for Business servers (either signed by a public CA, or by a private CA whose root/intermediate certificates got imported in the **Trusted CA list** of the Microsoft Lync/Skype for Business servers). Note that when using Office365, public CA signed certificates are required.

For example:

The server certificate of the Expressway-E server matching the **expe.example.com** as shown from the example above, must have the following minimum entries:

- (Only if no **Subject Alternative Names**) **Common Name** must be **expe.example.com**
- (If **Subject Alternative Names** are available) **Subject Alternative Name** must contain an **entry expe.example.com**
- Issuer of the top of the certificate tree must to be a public CA (or the CA would need to be added in the **Trusted CA list** of the Microsoft Lync/Skype servers)

Note:

The domain (example.com) on itself does not need to be included as a **Subject Alternative Name**.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

The section contains logging information and traces which are taken from a test lab deployment with the following specifications:

- Skype domain is skype.lab
- UC domain (Expressway-E, Expressway-C and CUCM) is steven.lab
- CMS domain for users and spaces is acano.steven.lab (cms.steven.lab is also available)

As it is recommended to use a separate domain for your Cisco Meeting Server (different from your other UC domain on UCM/Expressway), it is likely that you have a different domain on your Expressway-E server and this could lead to integration issues related with the requirements on SIP federation on the Microsoft Lync/Skype for Business server's side.

Symptoms and Log review

When the requirements on DNS certificates are not matched on the Microsoft Lync/Skype server side, you notice the following symptoms:

- When a call is made from your UC infrastructure out towards Microsoft Lync/Skype, you see the call outgoing on the DNS zone of your Expressway-E to Skype, but immediately throwing a (504) Server Timeout error, visible on the **Status > Search History** page of Expressway-E:

- When a call is made from Microsoft Lync/Skype towards your UC infrastructure, you do not see the call arriving on the Expressway-E as shown on the **Status > Search History** page of Expressway-E.

This sub-section explains how to verify this scenario using the logging in more details and check what exactly is misconfigured.

Call towards Microsoft Lync/Skype

In this call flow, you see in the diagnostic logging of the Expressway-E the SIP INVITE going out towards Skype (if it can resolve the **_sipfederationtls._tcp** SRV record to an FQDN and IP), immediately followed by a **504 Server time-out** response without any further details as shown on the following logging snippet:

```
2017-03-02T08:10:46.240+01:00 vcse tvcs: UTCTime="2017-03-02 07:10:46,240" Module="network.sip"
Level="DEBUG":  Action="Received" Local-ip="10.48.36.47" Local-port="25002" Src-ip="10.48.36.6"
Src-port="5061" Msg-Hash="13707918855517357847"
 SIPMSG:
 |SIP/2.0 504 Server time-out
 Via: SIP/2.0/TLS 10.48.36.47:5061;egress-
zone=DNSZone1;branch=z9hG4bK42ee6fd77d32cc8925196770b950b33554.731d73c3f4246d6a255e38a9f695bfc0;
proxy-call-id=6b2a018a-2da5-4013-a7e5-4e1455feadf7;rport;received=10.48.36.47;ms-received-
port=25002;ms-received-cid=100
 Via: SIP/2.0/TLS 10.48.36.46:5061;egress-
zone=TraversalZoneClient1;branch=z9hG4bK1f8bbe5926dc6abd06ea964d8fde1450156486;proxy-call-
id=e7e33845-c384-4c28-a42d-016863640fbb;received=10.48.36.46;rport=28119;ingress-
zone=TraversalZoneServer1
 Via: SIP/2.0/TLS
10.48.54.160:52768;branch=z9hG4bK6594a02846406f4a5459d5f58a8d26b3;received=10.48.54.160;ingress-
zone=NeighborZoneAcano1SIP
 Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960
 CSeq: 2066245576 INVITE
 From: "DX70 Steven" <sip:2000@acano.steven.lab>;tag=9fea3e7d70afd884
 To: <sip:stejanss@skype.lab>;tag=C65A7B0A8766A5F1D386474833D07882
 Server: RTC/6.0
 Content-Length: 0
```

The same response is shown (without any further information) regardless whether it is a fault on the DNS records, or on the server's certificate of the Expressway-E.

Thus to review it in more detail, you must look into the Lync/Skype Edge server logging, where you can see the warnings and errors depending on the possible occurring faults:

- Possible fault: FQDN outcome of SRV record does not match exactly on the domain as in the **From/P-Asserted-Identity header** of the INVITE incoming to Skype. In this log snippet, the **From/P-Asserted-Identity header** of the **SIP INVITE** contains **acano.steven.lab** as domain, but **_sipfederationtls._tcp.acano.steven.lab** is pointing to **vcse.steven.lab** instead of **vcse.acano.steven.lab**:

```
TL_WARN(TF_DIAG) [sfvedge\sfvedge]0584.0A44::03/02/2017-07:10:46.230.0000773E
(SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(830)) [156659184] $$begin_record
Severity: warning Text: The domain of the message resolved by DNS SRV but none of the FQDNs is
in the same domain
Result-Code: 0xc3e93d6f SIPPROXY_E_EPROUTING_MSG_ALLOWED_DOMAIN_NO_SRV_MATCH
SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0
SIP-Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960
SIP-CSeq: 2066245576 INVITE
Peer: vcse.steven.lab:25002
Data: domain="acano.steven.lab";fqdn1="vcse.steven.lab:5061"
```

```
$$end_record
```

- Possible fault: Expressway-E server's certificate does not contain the FQDN resulted from the **_sipfederationtls._tcp** SRV record. The same **SIP INVITE** is sent and **_sipfederationtls._tcp.acano.steven.lab**, but that FQDN is not contained in the Expressway-E server's certificate SAN list:

```
TL_ERROR(TF_DIAG) [sfvedge\sfvedge]0B60.0D6C::03/02/2017-06:30:40.025.00005602
(SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(833)) [3634190282] $$begin_record
Severity: error Text: Message cannot be routed because the peer's certificate does not contain a
matching FQDN
Result-Code: 0xc3e93d67 SIPPROXY_E_ROUTING_MSG_CERT_MISMATCH
SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0
SIP-Call-ID: e144704c-1dd0-4ea7-929f-77e7e071c24c
SIP-CSeq: 1567605805 INVITE
Peer: vcse.steven.lab:25001
Data: expected-fqdn="vcse.acano.steven.lab";certName="vcse.steven.lab";info="The peer
certificate does not contain a matching FQDN"
$$end_record
```

Call from Microsoft Lync/Skype

For this call flow you do not see much in the logging of the Expressway-E as the Skype Edge server does not send the INVITE out and you need to rely on the Skype logging. Use either the Lync/Skype (Edge) server logging, or the Lync/Skype client logging itself to investigate the issue in more depth.

The Skype client logging on a Windows PC is available at the following path:

C:\Users\<username>\AppData\Local\Microsoft\Office\16.0\Lync\Tracing\Lync-UccApi-x.UccApiLog

It can be useful in the case of Office365 Skype users when no direct access to the Skype servers is available. In this logging, you can see the **SIP INVITE** message sent out by the client and the appropriate response for that.

If you run into issues with DNS or certificate requirements on Skype as per this document, you receive the **504 Server time-ou**t responses (including a reason of the failure) from the Skype servers:

- Possible fault: FQDN outcome of SRV record does not match exactly on the domain tried to be called. This log snippet shows attempt to dial to a user or space with domain **cms.steven.lab** and the **_sipfederationtls._tcp.cms.steven.lab** is pointing to **vcse.sub.cms.steven.lab**:

```
SIP/2.0 504 Server time-out
Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="8168D157", snum="38",
rspauth="65d8d93b66e5b217115e3b1636bf433c9f5df54a", targetname="SfBFE.skype.lab", realm="SIP
Communications Service", version=4
From: "Steven Janssens"<sip:stejanss@skype.lab>;tag=280f2bf329;epid=c21eec507a
To: <sip:stejanss.space@cms.steven.lab>;tag=98283FD4A66E24FFB4967CDB73149B25
Call-ID: d0bce97cce8a45fcbb8cc973ba0282da
CSeq: 1 INVITE
Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00
ms-diagnostics: 1009;reason="No match for domain in DNS SRV
results";domain="cms.steven.lab";fqdn1="vcse.sub.cms.steven.lab:5061";source="sip.skype.lab"
Server: RTC/6.0
Content-Length: 0
```

- Possible fault: Expressway-E server certificate does not contain the FQDN resulted from the **_sipfederationtls._tcp** SRV record. This log snippet shows attempt to dial to a user or space with domain **cms.steven.lab** for which **_sipfederationtls._tcp.cms.steven.lab** resolves correctly to **vcse.cms.steven.lab** but this **FQDN** is not contained in the **Subject Alternative Names** on the Expressway-E server certificate (with **Common Name** as **vcse.steven.lab**):

```
SIP/2.0 504 Server time-out
Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="1D8F66EF", snum="49",
rspauth="67836c7ffc0f6132b2304006969a219d9252aabd", targetname="SfBFE.skype.lab", realm="SIP
Communications Service", version=4
From: "Steven Janssens"<sip:stejanss@skype.lab>;tag=a1ea5f9a46;epid=c21eec507a
To: <sip:stejanss.space@cms.steven.lab>;tag=B7D9BF35417873B07792AAD244E6B230
Call-ID: 5e38e39898cf40188170f0d70644a87b
CSeq: 1 INVITE
Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00
ms-diagnostics: 1010;reason="Certificate trust with another server could not be
established";ErrorType="The peer certificate does not contain a matching FQDN";tls-
target="vcse.cms.steven.lab";PeerServer="vcse.steven.lab";HRESULT="0x80090322(SEC_E_WRONG_PRINCI
PAL)";source="sip.skype.lab"
Server: RTC/6.0
Content-Length: 0
```

Related Information

- Cisco Expressway Series Configuration guides