Konfiguration und Fehlerbehebung für DNS- und Zertifikatsanforderungen auf Microsoft Federation über Expressway zum Cisco Meeting Server

Inhalt

Einführung

In diesem Dokument werden die DNS- und Zertifikatsanforderungen von Microsoft Lync/Skype for Business für eine Föderation zwischen verschiedenen Domänen über das Internet beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Expressway X8.9 oder spätere Version
- Cisco Meeting Server (CMS) 2.1.2 oder höher
- Microsoft Lync 2010-Server, Lync 2013-Server oder Skype for Business-Server - vor Ort oder in der Cloud gehostet (Office365)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

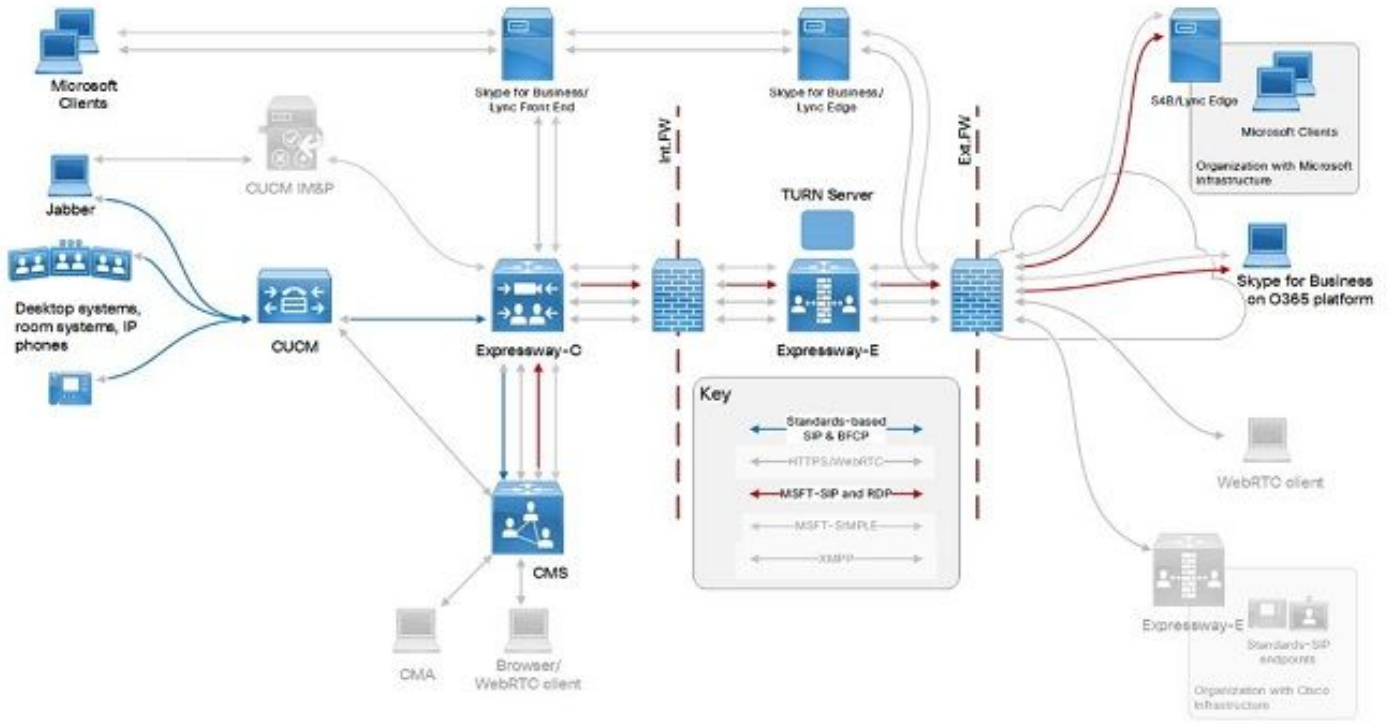
In diesem Dokument wird ein spezifischer Aspekt der Integration mit externen Microsoft-Clients in Ihre Cisco Infrastruktur mit Expressway und Cisco Meeting Server (CMS) beschrieben. Die Konfiguration für diese Integration wird in der Dokumentation der **Cisco Expressway-Optionen mit Cisco Meeting Server und/oder Microsoft-Infrastruktur** beschrieben, die für Ihre Version in der Liste der Konfigurationsleitfäden der Cisco Expressway-Serie verfügbar ist.

Das vorliegende Dokument konzentriert sich nur auf die DNS- und Zertifikatsanforderungen für Microsoft Lync oder Skype for Business für den externen Verbund. Die anderen Konfigurationen werden im oben genannten Konfigurationsleitfaden behandelt.

Konfigurieren

Ein Beispiel für den Anruffluss und seine Konfiguration kann ein CUCM-registrierter Endpunkt sein, der sich an einen Skype-Client anwählt (entweder vor Ort oder extern, oder in der Cloud mit Office365 registriert), oder umgekehrt - wobei das CMS für die Konvertierung zwischen Standard-SIP und Microsoft-Protokoll verwendet wird. Möglich wird dies durch die Integration und Anrufweiterleitung mithilfe von Expressway-Servern, wie in der Abbildung unten gezeigt, die aus dem **Cisco Expressway-Konfigurationsleitfaden mit Cisco Meeting Server und/oder der Microsoft-Infrastruktur** entnommen wird, auf den am Ende dieses Dokuments verwiesen wird.

Netzwerkdiagramm



Hinweis: Dies ist nur ein Beispielszenario für den Anruffluss. Andere Anrufszenarien sind ebenfalls möglich.

DNS

Microsoft Lync/Skype for Business verwendet den SRV-Datensatz **_sipfederationtls_tcp.<domain>**, um die externen Federationsserver zu ermitteln, an die die Anrufe gesendet werden sollen (sowie Anwesenheitsinformationen). oder für die Rückruffunktion basierend auf der Domäne, die im **Von/P-Asserted-Identity-Header** der eingehenden **SIP-INVITE** angegeben ist. In diesem Szenario müssen die DNS-Datensätze im öffentlichen DNS für beide Domänen verfügbar sein, um miteinander zu föderieren.

Der Domänenteil des **FQDN** (vollqualifizierter Domänenname), der von der SRV-Datensatzsuche für die Domäne zurückgegeben wird, muss genau übereinstimmen (keine anderen Domänen oder Subdomänen sind zulässig). Die folgende Tabelle zeigt ein Beispiel für die DNS-Konfiguration einer Domäne mit dem Namen **example.com**:

SRV-Datensatz	_sipfederationtls_tcp.example.com	expe.example.com
Ein Datensatz	expe.example.com	IP-Adresse von Expressway-E

Vorsicht: Der A-Datensatz, auf den die SRV auflöst, muss mit der konfigurierten Domäne übereinstimmen. Subdomänen (z. B. expe.sub.example.com) oder andere Domänen (expe.dummy.com) werden von Microsoft Lync/Skype for Business nicht als vertrauenswürdig eingestuft, was zu Anruffehlern führt, obwohl sie möglicherweise über entsprechende A-Datensätze verfügen und IP-Adressen korrigieren können.

Zertifikat

Microsoft Lync/Skype for Business richten eine TLS-Verbindung zwischen den auf der Lync- und

Expressway-Seite konfigurierten Domänen ein.Microsoft Lync/Skype for Business hat die folgenden Anforderungen an Serverzertifikate für den Verbund und die Server, mit denen er kommuniziert (Expressway-E in diesem Dokument):

- Das Serverzertifikat des Servers, das mit dem A-Datensatz übereinstimmt, muss diesen speziellen **FQDN** in seinem **Subject Alternative Name** (oder **Common Name**, wenn kein SAN verwendet wird) enthalten sein.
- Das vom Server präsentierte Serverzertifikat muss von den Microsoft Lync/Skype for Business-Servern als vertrauenswürdig eingestuft werden (entweder von einer öffentlichen Zertifizierungsstelle signiert oder von einer privaten Zertifizierungsstelle, deren Root-/Zwischenzertifikate in die **Liste** der **vertrauenswürdigen Zertifizierungsstellen** von Microsoft Lync/Skype für Business-Server importiert wurden). Beachten Sie, dass bei der Verwendung von Office365 Zertifikate mit öffentlicher Zertifizierungsstellenzahl erforderlich sind.

Beispiel:

Das Serverzertifikat des Expressway-E-Servers, das mit der Datei **expe.example.com** übereinstimmt, wie im obigen Beispiel gezeigt, muss mindestens folgende Einträge enthalten:

- (Nur wenn keine **Subject Alternative Names** vorhanden sind) **Common Name** muss **expe.example.com** sein**.**
- (Wenn **Subject Alternative Names** verfügbar sind) **Subject Alternative Name** muss einen **Eintrag expe.example.com** enthalten.
- Der Aussteller des obersten Zertifikatsbaums muss eine öffentliche Zertifizierungsstelle sein (oder die Zertifizierungsstelle muss in die **Liste** der **vertrauenswürdigen Zertifizierungsstellen** der Microsoft Lync-/Skype-Server aufgenommen werden).

Hinweis:

Die Domäne (example.com) selbst muss nicht als **Subject Alternative Name** eingeschlossen werden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Der Abschnitt enthält Protokollierungsinformationen und Ablaufverfolgungen, die in einer Testlabor-Bereitstellung mit den folgenden Spezifikationen entnommen wurden:

- Skype-Domäne ist skype.lab
- UC-Domäne (Expressway-E, Expressway-C und CUCM) ist steven.lab.
- Die CMS-Domäne für Benutzer und Leerstellen ist acano.steven.lab (auch cms.steven.lab ist verfügbar).

Da es empfohlen wird, eine separate Domäne für Ihren Cisco Meeting Server zu verwenden (die sich von Ihrer anderen UC-Domäne auf UCM/Expressway unterscheidet), ist es wahrscheinlich, dass Sie eine andere Domäne auf Ihrem Expressway-E-Server haben, und dies kann zu Integrationsproblemen im Zusammenhang mit den Anforderungen an den SIP-Verbund auf der Seite von Microsoft Lync/Skype für Business-Server führen.

Symptome und Protokollüberprüfung

Wenn die Anforderungen an DNS-Zertifikate auf der Microsoft Lync-/Skype-Server-Seite nicht erfüllt werden, bemerken Sie die folgenden Symptome:

- Wenn ein Anruf von Ihrer UC-Infrastruktur an Microsoft Lync/Skype erfolgt, sehen Sie den ausgehenden Anruf in der DNS-Zone Ihres Expressway-E zu Skype, aber sofort einen (504) Server-Timeout-Fehler, der auf der **Seite Status > Suchverlauf** von Expressway-E angezeigt wird:

- Wenn ein Anruf von Microsoft Lync/Skype an Ihre UC-Infrastruktur erfolgt, wird der Anruf, der auf dem Expressway-E eingeht, nicht angezeigt, wie auf der **Seite Status > Suchverlauf** von Expressway-E dargestellt.

In diesem Unterabschnitt wird erläutert, wie Sie dieses Szenario mithilfe der Protokollierung in weiteren Details überprüfen und überprüfen, was genau falsch konfiguriert ist.

Anruf bei Microsoft Lync/Skype

In diesem Anruffluss sehen Sie in der Diagnoseprotokollierung des Expressway-E, dass SIP INVITE zu Skype ausgeht (wenn es den **_sipfederationtls_tcp** SRV-Datensatz zu einem FQDN und IP auflösen kann), unmittelbar gefolgt von einer **504-Server-Timeout-**Antwort ohne weitere Details wie im folgenden Protokollausschnitt:

```
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
```

Die gleiche Antwort wird angezeigt (ohne weitere Informationen), unabhängig davon, ob es sich um einen Fehler in den DNS-Datensätzen oder im Serverzertifikat des Expressway-E handelt.

Um es genauer zu betrachten, müssen Sie sich die Lync-/Skype Edge-Serverprotokollierung ansehen, wo Sie die Warnungen und Fehler je nach den möglichen Fehlern sehen können:

- Mögliche Störung: Das FQDN-Ergebnis des SRV-Datensatzes stimmt nicht exakt mit der Domäne überein, wie es im **Von/P-Asserted-Identity-Header** der bei Skype eingehenden INVITE-Nachricht angegeben ist. In diesem Protokollausschnitt enthält der **Von/P-Asserted-Identity-Header** der **SIP-INVITE acano.steven.lab** als Domäne,

aber_sipfederationtls._tcp.acano.steven.lab nur vcse.steven.lab anstelle von vcse.acano.steven.steven. ven.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
```

- Mögliche Störung: Das Zertifikat des Expressway-E Servers enthält nicht den FQDN, der aus dem SRV-Datensatz _sipfederationtls_tcp entstanden ist. Dieselbe SIP-INVITE wird gesendet, und _sipfederationtls_tcp.acano.steven.lab verweist auf vcse.acano.steven.lab, aber dass FQDN nicht in der Zertifikatsliste des Expressway-E Servers enthalten ist:

```
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
```

Anruf von Microsoft Lync/Skype

Für diesen Anruffluss sehen Sie nicht viel in der Protokollierung des Expressway-E, da der Skype Edge-Server die INVITE-Nachricht nicht sendet und Sie sich auf die Skype-Protokollierung verlassen müssen. Verwenden Sie entweder die Lync/Skype (Edge)-Serverprotokollierung oder den Lync/Skype-Client, um das Problem genauer zu untersuchen.

Der Skype-Client, der sich auf einem Windows-PC anmeldet, ist über den folgenden Pfad verfügbar:

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

Sie kann für Office365-Skype-Benutzer nützlich sein, wenn kein direkter Zugriff auf die Skype-Server verfügbar ist. Bei dieser Protokollierung sehen Sie die vom Client gesendete SIP INVITE-Nachricht und die entsprechende Antwort.

Wenn bei Skype Probleme mit DNS- oder Zertifikatsanforderungen auftreten, erhalten Sie die 504 Server-Timeout-Antworten (einschließlich eines Fehlerurteils) von den Skype-Servern:

- Mögliche Störung: Das FQDN-Ergebnis des SRV-Datensatzes stimmt nicht exakt mit der Domäne überein, die aufgerufen werden soll. Dieser Protokollausschnitt zeigt den Versuch, mit der Domäne cms.steven.lab und der _sipfederationtls_tcp.cms.steven.lab einen Benutzer oder einen Leerraum zu wählen, und verweist auf 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"

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

- Mögliche Störung: Das Expressway-E Serverzertifikat enthält nicht den FQDN, der aus dem SRV-Datensatz **_sipfederationtls_tcp** stammt. Dieser Protokollausschnitt zeigt den Versuch, mit der Domäne **cms.steven.lab** eine Nummer zu wählen, für die **_sipfederationtls._tcp.cms.steven.lab korrekt in vcse.cms.steven.lab aufgelöst wird, dieser FQDN ist jedoch nicht im Subject Alternative Names auf dem Expressway-E-Serverzertifikat enthalten (mit** als **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"

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_PRINCIPAL)";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

Zugehörige Informationen

- Konfigurationsleitfäden für die Cisco Expressway Serie